



ユーザーガイド

AWS Control Tower



AWS Control Tower: ユーザーガイド

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

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

AWS Control Tower とは	1
機能	1
AWS Control Tower が他のAWSサービスとやり取りする方法	2
AWS Control Tower を初めてお使いになる方に	3
仕組み	3
AWS Control Tower のランディングゾーンの構造	4
ランディングゾーンをセットアップした場合に起きること	4
共有アカウントとは	5
コントロールの仕組み	6
AWS Control Tower と StackSets が動作する仕組み	7
用語	9
料金	13
セットアップ	14
にサインアップする AWS	14
にサインアップする AWS アカウント	14
管理アクセスを持つユーザーを作成する	15
次のステップ	16
開始方法	17
クイックスタートガイド	17
起動前チェック	19
AWS IAM アイデンティティセンター (IAM Identity Center) のお客様に関する考慮事項	20
コントロール専用環境のセットアップ	21
開始方法	22
AWS Config に関する考慮事項	22
実装プロセス	22
重要な注意事項	22
コンソールからの開始方法	23
ランディングゾーン設定に対する想定	23
ステップ 1: 共有アカウントの E メールアドレスを作成する	24
ステップ 2: ランディングゾーンの設定と起動	26
ステップ 3: ランディングゾーンの確認とセットアップ	34
API を使用した開始方法	35
API を使用したランディングゾーン設定に対する想定	36
ステップ 1: ランディングゾーンを設定する	37

ステップ 2: AWS Control Tower APIs	41
ランディングゾーンを特定する	44
ランディングゾーンを更新する	45
ランディングゾーンをリセットしてドリフトを解決する	47
ランディングゾーンのマニフェストファイルの詳細を表示する	48
ランディングゾーンオペレーションのステータスを表示する	51
例: API のみを使用して AWS Control Tower ランディングゾーンを設定する	53
ランディングゾーンのスキーマ	61
CloudFormation を使用してランディングゾーンを起動する	84
次の手順	90
制限とクォータ	92
AWS Control Tower の既知の制限事項	92
クォータ引き上げをリクエストする	94
コントロールの制限事項	96
使用可能なコントロールとリージョンを確認する	97
基盤となる AWS サービスに基づく制限	97
リージョン間の違い	99
Controls Reference Guide	101
管理者向けのベストプラクティス	102
アクセスについてユーザーに説明する	102
リソースアクセスについて説明する	102
予防コントロールについて説明する	103
ランディングゾーンの計画	104
機能の比較	105
既存の組織での AWS Control Tower の起動	106
新しい組織での AWS Control Tower の起動	107
ベストプラクティス: AWS マルチアカウントランディングゾーンを設定する	107
AWS マルチアカウントガイダンスに合わせる	108
アーキテクチャが適切に設計された環境をセットアップするためのガイドライン	109
完全なマルチアカウント OU 構造を持つ AWS Control Tower の例	112
ルートについて	113
ランディングゾーンのセットアップに関する管理上のヒント	113
Landing Zone v4.0 移行ガイド	114
主な変更点	115
AWS Config の更新	117
グループ、ロール、ポリシーを設定する上での推奨事項	120

AWS Control Tower リソースに関するガイダンス	121
ルートのユーザーとしてサインインする場合	123
AWS Organizations ガイダンス	124
IAM Identity Center のガイダンス	125
Account Factory ガイダンス	127
SNS トピックのサブスクリプションに関するガイダンス	128
KMS キーのガイダンス	129
ランディングゾーンの更新	130
AI ベースのサービスのポリシー	132
設定更新管理	134
更新について	136
ランディングゾーンを更新する	137
標準的な更新手順	138
ランディングゾーンバージョンを選択する	138
アカウントの更新、ランディングゾーンバージョン、およびベースライン	140
アカウントの証跡を保持する	140
リセットと再登録でドリフトを解決する	142
自動化によるアカウントのプロビジョニングと更新	143
タスクの自動化	145
AWS CloudShellおよびAWS CLI	147
の IAM アクセス許可を取得するAWS CloudShell	148
AWS Control Towerを通じて を操作するAWS CloudShell	149
AWS CloudFormation リソース	152
AWS Control Tower および CloudFormation テンプレート	152
の詳細 CloudFormation	153
ランディングゾーンのカスタマイズ	154
AWS Control Tower コンソールからカスタマイズする	154
AWS Control Tower コンソールの外部でカスタマイズを自動化する	156
AWS Control Tower と LZA	156
AWS Control Tower のカスタマイズ (CfCT) のメリット	157
その他の CfCT の例	158
AWS Control Tower のカスタマイズ (CfCT) の概要	159
アーキテクチャ	159
Cost	162
コンポーネントサービス	162
AWS CodeCommit	162

AWS CodePipeline	163
AWS Key Management Service	163
AWS Lambda	163
Amazon Simple Notification Service	164
Amazon Simple Storage Service	164
Amazon Simple Queue Service	164
AWS Step Functions	165
AWS Systems Manager パラメータストア	165
デプロイに関する考慮事項	165
デプロイの準備	165
AWS Control Tower のカスタマイズを更新するには	167
テンプレートおよびソースコード	167
ソースコード	167
CfCT をデプロイする	168
前提条件	168
デプロイ手順	168
ステップ 1. スタックを起動する	168
ステップ 2. カスタムパッケージを作成する	172
スタックを更新する	173
スタックセットの削除	174
Simple Storage Service (Amazon S3) を設定ソースとしてセットアップする	175
GitHub を設定ソースとしてセットアップする	176
GitHub リポジトリを準備する	177
GitHub 接続を作成する	177
CloudFormationスタックをデプロイする	177
運用メトリクス	178
CfCT カスタマイズガイド	179
コードパイプラインの概要	179
カスタム設定の定義	181
ルート OU	189
ネストされた OU	190
独自のカスタマイズを構築する	191
CfCT マニフェストのバージョンアップグレード	198
ネットワーク	201
AWS Control Tower の VPCs とAWSリージョン	201
AWS Control Tower と VPC の概要	202

VPC と AWS Control Tower の CIDR とピア接続	203
AWS PrivateLink	205
考慮事項	205
インターフェイスエンドポイントの作成	206
エンドポイントポリシーを作成する	206
ルールとアクセス許可	208
ルールとアカウント	209
ルールとアカウントの作成	209
AWSControlTowerExecution ロール	209
ロールの信頼関係のオプションの条件	211
AWS Control Tower がアンマネージド OUsとアカウントで AWS Config ルールを集約する 方法	214
AWS Control Tower 監査アカウントのプログラムによるロールおよび信頼関係	217
IAM ロールを使用した自動アカウントプロビジョニング	221
リソースの管理	223
リージョンを設定する	224
AWS Control Tower リージョンの設定	225
リージョンを設定する際は混合ガバナンスを避ける	227
オプトインリージョンについて	229
リージョン拒否コントロールの設定	232
OU レベルでのリージョン拒否コントロールに関する考慮事項	233
アカウントについて	234
AWS Control Tower がアカウントを作成した場合に起きること	234
既存のセキュリティアカウントまたはログアカウントを使用する際の考慮事項	235
共有アカウントについて	236
管理アカウント	236
ログアーカイブアカウント	236
監査アカウント	237
共有アカウントのリソース	239
管理アカウントのリソース	239
ログアーカイブアカウントのリソース	243
アカウントリソースを監査する	246
メンバーアカウントについて	249
から AWS Control Tower アカウントを操作する AWS Service Catalog	249
アカウントの作成とプロビジョニング	250
Service Catalog API による AWS Control Tower のアカウントプロビジョニングの自動化 ..	251

Service Catalog でプロビジョニング済み製品を更新する	256
Service Catalog でアカウントの登録を解除する	257
アカウントのプロビジョニングと管理	259
必要なアクセス許可	259
プロビジョニングの方法	260
コンソールでアカウントをプロビジョニングする	262
アカウントの表示	263
アカウントの登録について	264
アカウント登録中の処理	265
VPC を使用して既存のアカウントを登録する	266
AWS Config リソースでアカウントを登録する	266
登録の前提条件	267
自動登録オプション	269
コンソールから登録する	271
アカウントが前提条件を満たしていない場合	274
必要な IAM ロールを既存の に手動で追加 AWS アカウント して登録する	276
既存の AWS Config リソースがあるアカウントを登録する	279
ステップ 1: サポートに連絡して、許可リストにアカウント (複数可) を追加する	281
ステップ 2: メンバーアカウントに新しい IAM ロールを作成する	282
ステップ 3: 既存のリソースがある AWS リージョンを特定する	283
ステップ 4: AWS Config リソースがない AWS リージョンを特定する	283
ステップ 5: 各 AWS リージョンの既存のリソースを変更する	283
ステップ 5a. AWS Config recorder リソース	284
ステップ 5b. AWS Config 配信チャネルリソースを変更する	284
ステップ 5c. AWS Config 集約認可リソースの変更	285
ステップ 6: AWS Control Tower が管理するリージョンで、リソースが存在しない場所にリ ソースを作成する	286
ステップ 7: OU を AWS Control Tower に登録する	287
Account Factory	287
アクセス許可	288
アカウントに関する考慮事項	289
アカウントの更新と移動	289
登録済みアカウントの E メールアドレスの変更	290
登録済みアカウントの名前を変更する	291
Amazon VPC の設定を構成する	292
アカウントを登録解除する	294

アカウントの解約	295
Account Factory のリソース	297
Account Factory Customization (AFC)	299
カスタマイズのための設定	301
ブループリントからカスタマイズされたアカウントを作成する	308
登録時に AFC を使用してアカウントをカスタマイズする	309
ブループリントを AWS Control Tower アカウントに追加する	310
ブループリントを更新する	310
アカウントからブループリントを削除する	311
パートナーのブループリント	311
Account Factory Customizations (AFC) に関する考慮事項	312
ブループリントエラーが発生した場合	312
CloudFormation に基づく AFC ブループリント用のポリシードキュメントのカスタマイズ	314
Terraform ベースの Service Catalog 製品の作成に必要な追加のアクセス許可	316
新しい External 製品タイプへの移行	317
AWS Control Tower Account Factory for Terraform (AFT)	318
前提条件	319
AFT の概要	320
AFT のデプロイ	323
新しいアカウントのプロビジョニング	332
複数のアカウントリクエスト	334
既存のアカウントの更新	334
サポートされるバージョン	337
機能オプションの有効化	340
AFT のリソース	344
必要なロール	349
コンポーネントサービス	352
AFT アカウントプロビジョニングパイプライン	354
アカウントのカスタマイズ	357
代替 VCS	363
データ保護	367
アカウントを削除する	368
運用メトリクス	370
トラブルシューティングガイド	371
Drift	375

ドリフトの検出	375
ドリフトの表示	377
ドリフトの解決	377
ドリフトスキャンと ポリシースキャンに関する考慮事項	378
すぐに解決すべきドリフトのタイプ	380
リソースへの修復可能な変更	381
ドリフトと新しいアカウントのプロビジョニング	381
ガバナンスドリフトのタイプ	382
移動されたメンバーアカウント	384
削除されたメンバーアカウント	386
計画外のマネージド SCP の更新	387
マネージド OU からデタッチされた SCP	388
削除された基礎 OU	389
Security Hub CSPM コントロールドリフト	389
コントロールポリシードリフト	391
信頼されたアクセスの無効化	392
有効なベースラインでの継承ドリフト	392
有効なコントロールの継承ドリフト	393
EventBridge の作成	394
AWS Control Tower の外部でリソースを管理する場合	396
AWS Control Tower の外部にあるリソースの参照	397
AWS Control Tower の外部でのリソース名の変更	397
セキュリティ OU の削除	398
セキュリティ OU からのアカウントの削除	399
自動的に更新される外部変更	401
組織	403
動画チュートリアル	404
トピック	404
ガバナンスを既存の組織に拡張する	404
動画: 既存の でランディングゾーンを有効にする AWS Organizations	406
IAM Identity Center および既存の組織に関する考慮事項	406
他の AWS サービスへのアクセス	406
ネストされた OU	406
動画チュートリアル	407
フラットな OU 構造からネストされた OU 構造への拡張	407
ネストされた OU の登録の事前チェック	408

ネストされた OU とロール	408
ネストされた OU とアカウントの登録時および再登録時の処理	408
ネストされた OU を登録する際の考慮事項	409
ネストされた OU の制限	409
ネストされた OU とコンプライアンス	410
ネストされた OU とドリフト	410
ネストされた OU とコントロール	411
ネストされた OU とルート	412
OU を登録して複数のアカウントを登録する	412
既存の OU の登録	414
新しい OU の作成	416
OU を削除する	416
登録時または再登録時に発生する障害のよくある原因	418
組織の更新	420
OU とアカウントを更新する場合	421
1つの OU 内の複数のアカウントの更新	421
再登録中の処理	422
1つのアカウントを更新するには	422
統合サービス	424
AWSバックアップ	424
CloudFormation	425
CloudTrail	425
CloudWatch	425
AWS Config	426
Control Tower ランディングゾーン 4.0 での AWS Config の統合	426
AWS Identity and Access Management	429
AWS Key Management Service	429
AWS Lambda	430
AWS Organizations	430
考慮事項	431
Simple Storage Service (Amazon S3)	431
Security Hub CSPM	431
AWS Service Catalog	431
Amazon SNS	432
ステップ関数	433
ID とアクセス管理	434

認証	434
アクセスコントロール	436
IAM Identity Center と AWS Control Tower	437
ユーザーグループ、ロール、アクセス許可セット	438
IAM Identity Center アカウントと AWS Control Tower に関する注意事項	439
AWS Control Tower の IAM Identity Center グループ	439
IAM によるリソースアクセス管理の概要	443
AWS Control Tower のリソースとオペレーション	444
リソース所有権について	444
リソースへのアクセスの管理	445
ポリシー要素を指定: アクション、効果、プリンシパル	455
ポリシーでの条件の指定	456
混乱した代理攻撃の防止	456
AWS Control Tower の IAM ポリシー	457
AWS Control Tower コンソールを使用するために必要なアクセス許可	457
AWS Control Tower 管理者ロール	459
AWS ControlTowerServiceRolePolicy	460
AWS ControlTowerIdentityCenterManagementPolicy	461
AWS ControlTowerStackSetRole	461
AWS ControlTowerCloudTrailRolePolicy	462
AWS ControlTowerBlueprintAccess ロールの要件	464
AWSServiceRoleForAWSControlTower	465
AWS ControlTowerAccountServiceRolePolicy	466
AWS Control Tower のマネージドポリシー	466
セキュリティ	478
データ保護	478
保管時の暗号化	480
転送時の暗号化	480
コンテンツへのアクセスの制限	480
コンプライアンス検証	480
耐障害性	481
インフラストラクチャセキュリティ	482
ログ記録とモニタリング	483
AWS Control Tower でのログ記録について	484
S3 バケットポリシー	485
モニタリングの概要	487

を使用した AWS Control Tower アクションのログ記録 AWS CloudTrail	488
CloudTrail での AWS Control Tower 情報	488
例: AWS Control Tower ログファイルのエントリ	491
でリソースの変更をモニタリングする AWS Config	492
設定コストを管理する	493
登録済みアカウントの AWS Config レコーダーデータを表示する	494
AWS Control Tower AWS Config でのトラブルシューティング	495
ライフサイクルイベント	496
CreateManagedAccount	500
UpdateManagedAccount	501
EnableGuardrail	502
DisableGuardrail	504
SetupLandingZone	505
UpdateLandingZone	507
RegisterOrganizationalUnit	509
DeregisterOrganizationalUnit	510
PrecheckOrganizationalUnit	511
EnableBaseline	513
ResetEnabledBaseline	515
UpdateEnabledBaseline	516
DisableBaseline	517
ユーザー通知	519
バックアップ	522
前提条件	523
バックアップの有効化	525
最初の部分: ランディングゾーンのバックアップを設定する	525
次のパート: OU でバックアップを有効化する	527
バックアップを無効にする	528
最初のステップ: OUのバックアップを無効にする	529
次のステップ: ランディングゾーン AWS Backup の をオフにする	529
移動したアカウント	530
バックアップドリフト	531
バックアップリソース	531
AWS バックアップのコントロール	535
ランディングゾーンを廃止する	536
廃止プロセスの概要	537

ランディングゾーンの廃止方法	538
API を使用してランディングゾーンを廃止する	539
廃止後に必要な手動クリーンアップタスク	540
廃止処理中に削除されないリソース	541
AWS Control Tower リソースを削除する	544
削除ではなく廃止が必要か	545
AWS Control Tower リソースの削除について	546
SCP の削除	546
StackSets およびスタックの削除	547
ログアーカイブアカウントでの Simple Storage Service (Amazon S3) バケットの削除	548
Account Factory ポートフォリオおよび製品を削除する	549
AWS Control Tower のロールとポリシーを削除する	550
AWS Control Tower リソースのヘルプ	552
ランディングゾーン廃止後のセットアップ	552
チュートリアル	554
チュートリアル: ALZ から AWS Control Tower に移行する	554
チュートリアル: VPC を使用せずに AWS Control Tower を設定する	554
AWS Control Tower VPC を削除する	555
オプションでアカウントの VPC リソースをクリーンアップする	556
AWS Control Tower で VPC なしのアカウントを作成する	556
チュートリアル: を使用して AWS Control Tower でセキュリティグループを設定する AWS Firewall Manager	557
AWS Firewall Manager でセキュリティグループを設定する	558
トラブルシューティング	559
ランディングゾーンの起動の失敗	559
ランディングゾーンの更新が KMS エラーで失敗した	560
ランディングゾーンを更新できない	561
ランディングゾーンが最新ではないエラー	562
新しいアカウントのプロビジョニングに失敗する	563
既存のアカウントを登録できない	564
Account Factory アカウントを更新できない	564
言及する失敗エラー AWS Config	566
起動パスが見つからないというエラー	568
許可不足のエラーを受け取った	568
検出コントロールがアカウントで有効になっていない	569
AWS Organizations API によって返されるレート超過エラー	569

ある AWS Control Tower ランディングゾーンから別の AWS Control Tower ランディングゾーンに Account Factory アカウントを直接移動できない	570
AWS サポート	572
ベースライン	573
OU レベルで適用されるベースラインタイプ	573
ランディングゾーンのセットアップ中に共有アカウントに適用できるベースラインタイプ	575
一部登録	576
コンソールと API の比較	577
有効なベースラインとメンバーアカウント	578
ベースラインとバージョニングのデフォルト	578
AWSControlTowerBaseline の表	578
例: API のみを使用して AWS Control Tower OU を登録する	584
ベースライン API の例	586
DisableBaseline	586
EnableBaseline	587
GetBaseline	589
GetBaselineOperation	590
GetEnabledBaseline	590
ListBaselines	591
ListEnabledBaselines	593
ResetEnabledBaseline	598
UpdateEnabledBaseline	598
追加情報	600
チュートリアルとラボ	600
ネットワーク	201
セキュリティ、アイデンティティ、ログ記録	601
リソースのデプロイとワークロードの管理	602
既存の組織とアカウントの操作	602
オートメーションと統合	602
ワークロードの移行	603
AWS の関連サービス	603
AWS Marketplace ソリューション	604
リリースノート	605
2026 年 1 月～現在	605
欧州の主権クラウドで利用可能な AWS Control Tower	605
2025 年 1 月～2025 年 12 月	606

AWS Control Tower ランディングゾーンバージョン 4.0	606
AWS Control Tower が Control Catalog に 279 個の AWS Config コントロールを追加	608
AWS Control Tower が、アジアパシフィック (ニューージーランド) リージョンで利用可能に	608
AWS Control Tower が自動アカウント登録をサポート	609
AWS Control Tower が Python バージョンを更新	609
AWS Control Tower がドリフトを低減	610
AWS Control Tower が IPv6 アドレスをサポート	610
Account Factory for Terraform バージョン 1.15.0 が利用可能に	610
Nitro インスタンスタイプでコントロールを更新	611
AWS Control Tower がアジアパシフィック (台北) リージョンで利用可能に	612
AWS Control Tower が PrivateLink をサポート	612
追加の業界フレームワークのサポート、メタデータの更新	612
サービスにリンクされた AWS Config コントロール	613
有効なコントロールコンソールビューによる一元的な可視性	615
Account Factory for Terraform (AFT) がデプロイ時に新しい設定をサポート	615
AWS Control Tower がベースライン API のアカウントレベルのレポートを導入	616
AWS アジアパシフィック (タイ) およびメキシコ (中部) リージョンで利用可能な AWS Control Tower	616
利用可能な追加の AWS Config コントロール	617
OU のアクションの登録解除と削除	617
Control Catalog が IPv6 アドレスをサポート	618
2024 年 1 月 ~ 12 月	618
AWS Control Tower CfCT が GitHub と RCP をサポート	619
AWS Control Tower に宣言型ポリシーを使用した予防コントロールを追加	619
AWS Control Tower に規範バックアッププランオプションを追加	620
AWS Control Tower は AWS Config コントロールを統合します	620
AWS Control Tower でフック管理を改善し、プロアクティブコントロールリージョンを追加	620
AWS Control Tower がマネージドリソースコントロールポリシーを起動	621
AWS Control Tower によるコントロールポリシードリフトの報告	622
新しい ResetEnabledControl API	622
コントロールカタログの GetControl API の更新	623
AWS Control Tower AFT が GitLab をサポート	623
AWS アジアパシフィック (マレーシア) リージョンで AWS Control Tower が利用可能に ...	624
AWS Control Tower が OU あたり最大 1000 アカウントをサポート	624

AWS Control Tower でランディングゾーンバージョンの選択が可能に	624
記述的なコントロール API が利用可能になり、リージョンとコントロールへのアクセスが 拡大	625
AWS Control Tower がオプトインリージョンで AFT と CfCT をサポート	626
AWS Control Tower に ListLandingZoneOperations API を追加	626
AWS Control Tower が最大 100 の同時コントロールオペレーションをサポート	627
AWS Control Tower が AWS カナダ西部 (カルガリー) で利用可能に	627
AWS Control Tower がセルフサービスのクォータ調整をサポート	629
AWS Control Tower の「Controls Reference Guide」をリリース	629
AWS Control Tower で 2 つのプロアクティブコントロールを更新し、名前を変更	629
非推奨のコントロールが使用不可に	630
AWS Control Tower が の EnabledControl リソースのタグ付けをサポート CloudFormation	630
AWS Control Tower がベースラインを使用した OU 登録と設定用の API をサポート	631
2023 年 1 月 ~ 12 月	632
新しい AWS Service Catalog 外部製品タイプへの移行 (フェーズ 3)	633
AWS Control Tower ランディングゾーンバージョン 3.3	634
新しい AWS Service Catalog 外部製品タイプへの移行 (フェーズ 2)	635
AWS Control Tower がデジタル主権を支援するコントロールを発表	635
AWS Control Tower ランディングゾーン API	639
AWS Control Tower コントロールのタグ付け API	639
AWS アジアパシフィック (メルボルン) で利用可能な AWS Control Tower	639
新しい AWS Service Catalog 外部製品タイプへの移行 (フェーズ 1)	639
AWS Control Tower で新しいコントロール API が追加されました	640
AWS Control Tower で新しいコントロールが追加されました	640
AWS Control Tower で信頼されるアクセスドリフトを検出する	640
AWS Control Tower が 4 つの追加で利用可能に AWS リージョン	641
AWS イスラエル (テルアビブ) で AWS Control Tower が利用可能に	641
AWS Control Tower に 28 個の新しいプロアクティブコントロールを追加	641
AWS Control Tower で 2 つのコントロールが廃止されます	642
AWS Control Tower ランディングゾーンバージョン 3.2	642
AWS Control Tower に IAM Identity Center の email-to-ID マッピングが追加されました	644
AWS Control Tower が AWS Security Hub CSPM コントロールを追加	644
AWS Control Tower が AWS Security Hub CSPM コントロールのメタデータを発行する ...	645
AWS Control Tower に Terraform 用の Account Factory Customization (AFC) を追加	645
AWS Control Tower にセルフマネージド IAM アイデンティティセンターを追加	645

AWS Control Tower に 混合ガバナンスの注意事項を追加	646
AWS Control Tower に新しいプロアクティブコントロールを追加	646
AWS Control Tower で Amazon EC2 コントロールを更新する	646
AWS Control Tower が 7 つの追加で利用可能に AWS リージョン	647
AWS Control Tower Account Factory Customization (AFC) とリクエストトレースが一般利 用可能	647
AWS Control Tower ランディングゾーンバージョン 3.1	647
AWS Control Tower プロアクティブコントロールが一般利用可能	649
2022 年 1 月 ~ 12 月	649
同時アカウント操作	650
Account Factory Customization (AFC)	650
包括的なコントロールは AWS リソースのプロビジョニングと管理に役立ちます	651
すべての AWS Config ルールでコンプライアンスステータスを表示可能	652
コントロールと新しい CloudFormation リソース用の API	652
CfCT がスタックセットの削除をサポート	653
カスタマイズされたログの保持	654
ロールドリフト修復可能	654
AWS Control Tower ランディングゾーンバージョン 3.0	654
OU とアカウントのビューが組み合わされた組織ページ	658
簡略化されたアカウントの作成と登録	658
AFT は、AWS Control Tower の共有アカウントの自動カスタマイズをサポートします	659
すべてのオプションのコントロールの同時操作	659
既存のセキュリティアカウントとログアカウント	660
AWS Control Tower ランディングゾーンバージョン 2.9	661
AWS Control Tower ランディングゾーンバージョン 2.8	661
2021 年 1 月 ~ 12 月	662
リージョン拒否機能	663
データ所在地機能	663
AWS Control Tower で、Terraform アカウントのプロビジョニングとカスタマイズが導入さ れました	664
新しいライフサイクルイベントが利用可能に	665
AWS Control Tower でネストされた OU が有効になりました	665
検出コントロールの同時実行性	666
2 つの新しいリージョンが利用可能に	666
リージョンの選択解除	667
AWS Control Tower が AWS キー管理システムと連携する	667

コントロールの名前が変更され、機能は変更されません	668
AWS Control Tower は SCP を毎日スキャンしてドリフトをチェックするようになりました	668
OU とアカウントのカスタマイズされた名前	669
AWS Control Tower ランディングゾーンバージョン 2.7	669
3 つの新しい AWS リージョンが利用可能に	671
選択したリージョンのみを管理	672
AWS Control Tower がガバナンスを AWS 組織内の既存の OUs に拡張	672
AWS Control Tower でアカウントの一括更新が可能になりました	673
2020 年 1 月 ~ 12 月	673
AWS Control Tower コンソールが外部 Config AWS ルールにリンクされるようになりました	674
AWS Control Tower が追加のリージョンで利用可能になりました	674
ガードレールの更新	675
AWS Control Tower コンソールに OU とアカウントの詳細が表示されます	675
AWS Control Tower を使用して 新しいマルチアカウント AWS 環境をセットアップする AWS Organizations	676
AWS Control Tower ソリューションのカスタマイズ	677
AWS Control Tower バージョン 2.3 の一般提供	677
AWS Control Tower でのシングルステップのアカウントプロビジョニング	678
AWS Control Tower の廃止ツール	679
AWS Control Tower のライフサイクルイベント通知	679
2019 年 6 月 ~ 12 月	680
AWS Control Tower バージョン 2.2 の一般提供	680
AWS Control Tower の新しい選択的コントロール	681
AWS Control Tower の新しい検出コントロール	681
AWS Control Tower は、管理アカウントとは異なるドメインを持つ共有アカウントの E メールアドレスを受け付けます	682
AWS Control Tower バージョン 2.1 の一般提供	682
ドキュメント履歴	684
AWS 用語集	707
.....	dccviii

AWS Control Tower とは

AWS Control Tower は、規範的なベストプラクティスに従って、AWSマルチアカウント環境をセットアップして管理するための簡単な方法を提供します。AWS Control Tower は、AWS Organizations、AWS Service Catalog、など、他のいくつかの [AWSサービスの機能](#) をオーケストレーションしてAWS IAM アイデンティティセンター、1 時間以内にランディングゾーンを構築します。リソースは、ユーザーに代わって設定および管理されます。

AWS Control Tower オーケストレーションは の機能を拡張しますAWS Organizations。組織やアカウントに、ベストプラクティスからの逸脱であるドリフトをさせないために、AWS Control Tower はコントロール (ガードレールと呼ばれることもあります) を適用します。例えば、コントロールを使用して、セキュリティログと必要なクロスアカウントアクセス許可が作成され、変更されないようにすることができます。

少数のアカウントをホストしている場合は、アカウントデプロイとアカウントガバナンスを容易にするオーケストレーションレイヤーを持つことは有益です。AWS Control Tower は、アカウントとインフラストラクチャをプロビジョニングする主な方法として採用できます。AWS Control Tower を使用すると、より簡単に企業基準を遵守し、規制要件を満たし、ベストプラクティスに従うことができます。

AWS Control Tower を使用すると、分散チームのエンドユーザーは、Account Factory で設定可能なAWSアカウントテンプレートを使用して、新しいアカウントをすばやくプロビジョニングできます。一方、中央のクラウド管理者は、すべてのアカウントが、確立された、会社全体のコンプライアンスポリシーと連携していることをモニタリングできます。

つまり、AWS Control Tower は、何千もの企業と連携することで確立されたベストプラクティスに基づいて、安全で準拠したマルチアカウントAWS環境を設定および管理する最も簡単な方法を提供します。AWS Control Tower の使用とAWS、マルチアカウント戦略で説明されているベストプラクティスの詳細については、「」を参照してください[AWS マルチアカウント戦略: ベストプラクティスガイド](#)。

機能

AWS Control Tower には次の機能があります。

- ランディングゾーン — ランディングゾーンは、セキュリティとコンプライアンスのベストプラクティスに基づく、優れたアーキテクチャ設計の[複数アカウントの環境](#)です。これは、すべての組織

単位 (OU)、アカウント、ユーザー、およびコンプライアンス規制の対象とするその他のリソースを保持するエンタープライズ全体のコンテナです。ランディングゾーンは、いずれの規模の企業のニーズに合わせてもスケーリングできます。

- **コントロール – コントロール** (ガードレールと呼ばれることもあります) は、AWS環境全体に継続的なガバナンスを提供する高レベルのルールです。これは、わかりやすい形式で表されます。予防コントロール、検出コントロール、プロアクティブコントロールの3種類があります。必須、強く推奨、選択的の3つのガイダンスカテゴリが適用されます。コントロールの詳細については、「[コントロールの仕組み](#)」を参照してください。
- **Account Factory** — Account Factory は、事前に承認されたアカウント設定で新規アカウントのプロビジョニングを標準化するのに役立つ、設定可能なアカウントテンプレートです。AWS Control Tower には、組織内でアカウントプロビジョニングワークフローの自動化を支援する、組み込みの Account Factory が用意されています。詳細については、「[Account Factory でのアカウントのプロビジョニングと管理](#)」を参照してください。
- **ダッシュボード** — このダッシュボードでは、中央のクラウド管理者のチームがランディングゾーンを継続的に監視できます。このダッシュボードを使用して、企業全体でプロビジョニングされているアカウント、ポリシーの適用に対して有効にされているコントロール、ポリシーの非準拠の継続的検出に対応するコントロール、およびアカウントと OU によって編成され非準拠リソースを確認できます。

AWS Control Tower が他のAWSサービスとやり取りする方法

AWS Control Tower はAWS Service CatalogAWS IAM アイデンティティセンター、やなどの信頼できるAWSサービス上に構築されていますAWS Organizations。詳細については、「[統合サービス](#)」を参照してください。

既存のワークロードの移行に役立つソリューションに、AWS Control Tower を他のAWSサービスに組み込むことができますAWS。詳細については、「[How to take advantage of AWS Control Tower and CloudEndure to migrate workloads to AWS](#)」(AWS Control Tower と CloudEndure を活用してワークロードを AWS に移行する方法) を参照してください。

構成、ガバナンス、拡張性

- **自動アカウント設定**: AWS Control Tower は、AWS Service Catalogのプロビジョニングされた製品の上に抽象化として構築された Account Factory (または「自動販売機」) を使用して、アカウントのデプロイと登録を自動化します。Account Factory はAWSアカウントを作成および登録でき、それらのアカウントにコントロールとポリシーを適用するプロセスを自動化します。アカウントの作成とプロビジョニングの詳細については、「[プロビジョニングの方法](#)」を参照してください。

- 一元化されたガバナンス: の機能を採用することでAWS Organizations、AWS Control Tower はマルチアカウント環境全体で一貫したコンプライアンスとガバナンスを確保するフレームワークをセットアップします。このAWS Organizationsサービスは、アカウントの中央ガバナンスと管理、AWS Organizations APIs からのアカウント作成、サービスコントロールポリシー (SCPs)、リソースコントロールポリシー (RCPs) など、マルチアカウント環境を管理するための重要な機能を提供します。
- 拡張性: AWS Control Tower コンソールだけでなく、で直接作業することでAWS Organizations、独自の AWS Control Tower 環境を構築または拡張できます。既存の組織を登録し、既存のアカウントを AWS Control Tower に登録すると、変更が AWS Control Tower に反映されていることがわかります。AWS Control Tower ランディングゾーンを更新して、変更を反映させることができます。ワークロードにさらに高度な機能が必要な場合は、AWS Control Tower とともに他のAWS パートナーソリューションを活用できます。

AWS Control Tower を初めてお使いになる方に

このサービスを初めて使用する方には、以下を読むことをお勧めします。

1. ランディングゾーンを計画および整理する方法の詳細については、「[AWS Control Tower ランディングゾーンの計画](#)」および「[AWS AWS Control Tower ランディングゾーンのマルチアカウント戦略](#)」を参照してください。
2. 最初のランディングゾーンを作成する準備ができている場合は、「[AWS Control Tower の使用開始方法](#)」を参照してください。
3. ドリフトの検出と防止の詳細については、「[AWS Control Tower でドリフトを検出および解決する](#)」を参照してください。
4. セキュリティの詳細については、「[AWS Control Tower のセキュリティ](#)」を参照してください。
5. ランディングゾーンおよびメンバーアカウントの更新方法については、「[AWS Control Tower で の設定更新管理](#)」を参照してください。

AWS Control Tower の仕組み

このセクションでは、AWS Control Tower がどのように動作するかを大まかに説明します。ランディングゾーンは、すべての AWS リソース用に適切に設計されたマルチアカウント環境です。この環境を使用して、すべての AWS アカウントにコンプライアンス規制を適用できます。

AWS Control Tower のランディングゾーンの構造

AWS Control Tower のランディングゾーンの構造は次のとおりです。

- ルート - ランディングゾーン内の他のすべての OU を含む親。
- セキュリティ OU - この OU には、ログアーカイブアカウントと監査アカウントが含まれています。これらのアカウントは、共有アカウントとも呼ばれます。ランディングゾーンを起動するときに、これらの共有アカウントのカスタマイズされた名前を選択できます。また、セキュリティとログ記録のために既存の AWS アカウントを AWS Control Tower に持ち込むオプションもあります。ただし、これらの名前を後で変更することはできません。また、初回起動後にセキュリティとログ記録のために既存のアカウントを追加することはできません。
- サンドボックス OU - サンドボックス OU は、ランディングゾーンを有効にしている場合にランディングゾーンを起動すると作成されます。このメンバー OU と他のメンバー OU には、ユーザーが AWS ワークロードを実行するために使用する登録済みアカウントが含まれています。
- IAM Identity Center ディレクトリ - デフォルトでは、このディレクトリには、IAM Identity Center ユーザーが格納されます。これは、各 IAM Identity Center ユーザーの許可の範囲を定義します。オプションで、ID とアクセスコントロールを自己管理することを選択できます。詳細については、[「IAM Identity Center と AWS AWS Control Tower の使用」](#)を参照してください。
- IAM Identity Center ユーザー - ランディングゾーンで AWS ワークロードを実行するためにユーザーが引き受けることができる ID です。

ランディングゾーンをセットアップした場合に起きること

ランディングゾーンをセットアップすると、ユーザーに代わって AWS Control Tower が管理アカウントで次のアクションを実行します。

- AWS Organizations 組織のルート構造に含まれるセキュリティとサンドボックス (オプション) の 2 つの組織単位 (OUs) を作成します。
- セキュリティ OU 内に共有アカウントを 2 つ作成または追加する (ログアーカイブアカウントと監査アカウント)。
- デフォルトの AWS Control Tower 設定を選択した場合や、ID プロバイダーを自己管理できる場合は、事前設定されたグループとシングルサインオンアクセスを使用して、IAM Identity Center にクラウドネイティブディレクトリを作成します。
- 必須の予防コントロールをすべて適用してポリシーを実施する。
- 必須の検出コントロールをすべて適用して設定違反を検出する。

- 予防コントロールは管理アカウントには適用されません。
- 管理コントロールを除き、ガードレールを組織全体に適用する。

AWS Control Tower ランディングゾーンおよびアカウント内のリソースの安全な管理

- ランディングゾーンを作成すると、多数の AWS リソースが作成されます。AWS Control Tower を使用するには、このガイドで説明されたサポートされている方法以外で、これらの AWS Control Tower マネージドリソースを変更または削除することはできません。これらのリソースを変更または削除すると、ランディングゾーンの状態が不明になります。詳細については、「[AWS Control Tower リソースの作成と変更に関するガイダンス](#)」を参照してください。
- オプションのコントロール (強く推奨または選択的ガイダンスを持つコントロール) を有効にすると、AWS Control Tower はアカウントで管理する AWS リソースを作成します。AWS Control Tower によって作成されたリソースを変更または削除しないでください。これにより、コントロールの状態が不明になる可能性があります。

共有アカウントとは

AWS Control Tower では、ランディングゾーンの共有アカウント (管理アカウント、ログアーカイブアカウント、および監査アカウント) がセットアップ時にプロビジョニングされます。

管理アカウントとは

これは、ランディングゾーン専用で作成したアカウントです。このアカウントは、ランディングゾーンでのすべての請求に使用されます。また、このアカウントは、OU とコントロールの管理だけでなく、アカウントの Account Factory プロビジョニングに使用することもできます。

Note

AWS Control Tower 管理アカウントから運用ワークロードを実行することはお勧めしません。ワークロードを実行する別の AWS Control Tower アカウントを作成します。

詳細については、「[管理アカウント](#)」を参照してください。

ログアーカイブアカウントとは

このアカウントは、ランディングゾーン内のすべてのアカウントからの API アクティビティとリソース設定に関するログのリポジトリとして使用されます。

詳細については、「[ログアーカイブアカウント](#)」を参照してください。

監査アカウントとは

監査アカウントは、セキュリティチームとコンプライアンスチームに対してランディングゾーンのすべてのアカウントへの読み書きアクセスを許可するように設計された制限付きのアカウントです。監査アカウントからは、Lambda 関数にのみ付与されるロールを使用して、アカウントをレビューするためにプログラムによってアクセスできます。監査アカウントでは、他のアカウントに手動でログインすることはできません。Lambda 関数とロールの詳細については、「[別の AWS アカウント から ロールを引き受けるように Lambda 関数を設定する](#)」を参照してください。

詳細については、「[監査アカウント](#)」を参照してください。

コントロールの仕組み

コントロールは、AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。各コントロールは 1 つのルールを適用します。これは、わかりやすい言語で示されます。有効になっている選択的コントロールまたは強く推奨されるコントロールを AWS Control Tower コンソールまたは AWS Control Tower API からいつでも変更できます。必須コントロールは常に適用され、変更することはできません。

予防コントロールにより、アクションの発生が防止されます。例えば、[Disallow Changes to Bucket Policy for Amazon S3 Buckets] (Amazon S3 バケットのバケットポリシーへの変更を不許可にする) という選択的コントロール (以前の名称は [Disallow Policy Changes to Log Archive] (ログアーカイブへのポリシーへの変更を不許可にする)) により、ログアーカイブ共有アカウント内で IAM ポリシーを変更できなくなります。禁止されたアクションを実行しようとする、拒否され、CloudTrail に記録されます。リソースもログインします AWS Config。

検出コントロールにより、特定のイベントが発生したときにそのイベントが検出され、アクションが CloudTrail に記録されます。例えば、[Detect Whether Encryption is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances] (Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームに対して暗号化が有効になっているかどうかを検出する) という強く推奨されるコントロールにより、暗号化されていない Amazon EBS ボリュームがランディングゾーンの EC2 インスタンスにアタッチされているかどうかを検出されます。

プロアクティブコントロールは、リソースがアカウントにプロビジョニングされる前に、リソースが会社のポリシーと目標に準拠しているかどうかを確認します。リソースがポリシーと目標に準拠していない場合、リソースはプロビジョニングされません。プロアクティブコントロールは、CloudFormation テンプレートを使用してアカウントにデプロイされるリソースをモニタリングします。

に精通しているユーザーの場合 AWS: AWS Control Tower では、予防コントロールはサービスコントロールポリシー (SCPs) とリソースコントロールポリシー (RCPs)。検出コントロールは AWS Config ルールで実装されます。プロアクティブコントロールは CloudFormation フックで実装されます。

関連トピック

- [AWS Control Tower でドリフトを検出および解決する](#)

AWS Control Tower と StackSets が動作する仕組み

AWS Control Tower は、デフォルトで CloudFormation StackSets を使用してアカウントのリソースを設定します。各スタックセットには、アカウントとアカウント AWS リージョン ごとに 1 つの StackInstances があります。AWS Control Tower は、アカウントとリージョンごとに 1 つのスタックセットインスタンスをデプロイします。

AWS Control Tower は、CloudFormation パラメータに基づいて、特定のアカウントおよび AWS リージョン 選択的に更新を適用します。更新が一部のスタックインスタンスに適用されると、他のスタックインスタンスが OUTDATED ステータスのままになることがあります。これは想定内の正常な動作です。

スタックインスタンスが OUTDATED 状態になった場合は通常、そのスタックインスタンスに対応するスタックがスタックセットの最新のテンプレートと合致していないことになります。スタックは古いテンプレートに残っているため、最新のリソースやパラメータが含まれていない可能性があります。スタックはまだ完全に使用可能です。

更新時に指定された CloudFormation パラメータに基づいて、想定される動作を簡単にまとめます。

スタックセットの更新にテンプレートへの変更が含まれている場合 (つまり、TemplateBodyまたは TemplateURL プロパティが指定されている場合)、または Parameters プロパティが指定されている場合、は、指定されたアカウントのスタックインスタンスを更新する前に、ステータスが Outdated のすべてのスタックインスタンスを CloudFormation マークします AWS リージョン。スタックセットの更新にテンプレートまたはパラメータの変更が含まれていない場合、は指定されたアカウントとリージョンのスタックインスタンス CloudFormation を更新し、他のすべてのスタックインスタンスは既存のスタックインスタンスのステータスのままにします。スタックセットに関連付けられたすべてのスタックインスタンスを更新するには、Accounts プロパティまたは Regions プロパティを指定しないでください。

詳細については、「CloudFormation ユーザーガイド」の [「スタックセットの更新」](#) を参照してください。

用語

ここでは、AWS Control Tower のドキュメントに表示されるいくつかの用語を簡単に確認します。

まず、AWS Control Tower は、このドキュメント全体に表示される組織および組織単位 (OU) という用語など、多くの用語をAWS Organizationsサービスと共有していることを知っておくとよいでしょう。

- 組織と OU の詳細については、「[AWS Organizationsの用語と概念](#)」を参照してください。AWS Control Tower を初めて使用する場合は、その用語を理解することから始めましょう。
- [AWS Organizations](#) は、ワークロードの拡大とスケーリングに合わせて環境を一元管理するためのAWSサービスです。AWS Control Tower はAWS Organizations、を使用してアカウントを作成し、OU レベルで予防コントロールを適用し、一元的な請求を行います。
- [AWS Account Factory アカウント](#) は、AWS Control Tower の Account Factory を使用してプロビジョニングされたAWSアカウントです。Account Factory は、アカウントの「自動販売機」と非公式に呼ばれることもあります。
- AWS Control Tower [ホームリージョン](#) は、AWS Control Tower ランディングゾーンがデプロイされたAWSリージョンです。ホームリージョンは、ランディングゾーン設定で表示できます。
- [AWS Service Catalog](#) では、一般的にデプロイされる IT サービスを一元管理できます。このドキュメントのコンテキストでは、Account Factory はAWS Service Catalogを使用して、カスタマイズされたブループリントからのAWSアカウントを含む新しいアカウントをプロビジョニングします。
- [AWS CloudFormation StackSets](#) は、スタックの機能を拡張するリソースのタイプで、1 回のオペレーションと 1 つの CloudFormation テンプレートで、複数のアカウントおよびリージョンにまたがるスタックを作成、更新、または削除できます。
- [スタックインスタンス](#) は、リージョン内のターゲットアカウントのスタックへの参照です。
- [Astack](#) は、単一のユニットとして管理できるAWSリソースのコレクションです。
- [アグリゲータ](#) は、組織内の複数のアカウントとリージョンからAWS Config設定とコンプライアンスデータを収集するAWS Configリソースタイプであり、1 つのアカウント内でこのコンプライアンスデータを表示およびクエリできます。
- [コンフォーマンスパック](#) は、アカウントとリージョン、または の組織全体に単一のエンティティとしてデプロイできるAWS Configルールと修復アクションのコレクションです。AWS Organizations。適合パックを使用して、AWS Control Tower 環境をカスタマイズできます。詳細を説明している技術的なブログについては、「[関連情報](#)」を参照してください。

- AWS Control Tower の[ベースライン](#)は、ターゲットに適用できるリソースと特定の設定のグループです。最も一般的なベースラインターゲットは、組織単位 (OU) です。例えば、AWSControlTowerBaseline というベースラインを使用して、OU を AWS Control Tower に登録することができます。ランディングゾーンの設定および更新時には、共有アカウント、またはランディングゾーン全体の特定の設定をベースラインターゲットとすることができます。
- ブループリント:ブループリントは、いくつかのメタデータをカプセル化するアーティファクトで、アカウント内にデプロイされるインフラストラクチャコンポーネントを定義します。たとえば、CloudFormationテンプレートは AWS Control Tower アカウントのブループリントとして機能します。
- ドリフト: AWS Control Tower によってインストールされ、設定されたリソースの変更。ドリフトのないリソースにより、AWS Control Tower が正常に機能できるようになります。
- 非準拠リソース: 特定の検出コントロールを定義するAWS Configルールに違反しているリソース。
- 共有アカウント: ランディングゾーンの設定時に AWS Control Tower によって自動的に作成される 3 つのアカウント (管理アカウント、ログアーカイブアカウント、監査アカウント) のうちの 1 つ。設定時に、ログアーカイブアカウントと監査アカウントのカスタマイズされた名前を選択できます。
- メンバーアカウント: メンバーアカウントは、AWS Control Tower 組織に属します。メンバーアカウントは、AWS Control Tower に登録または登録解除できます。登録された OU に、登録済みアカウントと未登録アカウントが混在している場合:
 - OU で有効になっている (または OU で継承された) 予防コントロールは、未登録アカウントを含む、その OU 内のすべてのアカウントに適用されます。これは、アカウントレベルではなく OU レベルの SCP、RCP、または宣言型ポリシーで予防コントロールが実施されるためです。詳細については、AWS Organizationsドキュメントの[サービスコントロールポリシーの継承](#)を参照してください。
 - OU で有効になっている検出コントロールは、未登録アカウントには適用されません。
 - プロアクティブコントロールはAWS CloudFormationフックによって補完されます。これらのコントロールは、OU に登録されていないアカウントには適用されません。

アカウントは一度に 1 つの組織のメンバーにしかなることができず、その料金はその組織の管理アカウントに請求されます。メンバーアカウントは、組織のルートコンテナに移動できます。

- accountAWS:AWSアカウントは、リソースコンテナとリソース分離の境界として機能します。AWSアカウントは、請求と支払いに関連付けることができます。AWSアカウントは、AWS Control Tower のユーザーアカウント ([IAM ユーザーアカウント](#)と呼ばれることもあります) とは異なります。Account Factory プロビジョニングプロセスによって作成されたアカウントは

AWS accounts です。AWSアカウントは、アカウント登録または OU 登録プロセスによって AWS Control Tower に追加することもできます。

- **コントロール:** コントロール (ガードレールとも呼ばれます) は、AWS Control Tower 環境全体に継続的なガバナンスを提供する高レベルのルールです。各コントロールは、1 つのルールを適用します。予防コントロールは、SCP で実装されます。検出コントロールはAWS Configルールで実装されます。プロアクティブコントロールはCloudFormationフックで実装されます。詳細については、「[コントロールの仕組み](#)」を参照してください。
- **Control Catalog:** AWS Control Tower コントロールカタログは、コンソールと API で AWS Control Tower を通して利用可能なすべてのコントロールの便覧です。以前は Control Library と呼ばれていました。用語を名前空間の名前 controlcatalog に一致させました。
- **ランディングゾーン:** ランディングゾーンは、デフォルトのアカウント、アカウント構造、ネットワークおよびセキュリティレイアウトなど、推奨される開始点を提供するクラウド環境です。ランディングゾーンから、ソリューションとアプリケーションを利用するワークロードをデプロイできます。
- **フレームワーク:** フレームワークは、特定の規制基準または業界要件です。Control Catalog オントロジーでは、フレームワークは標準コントロールで表されます。詳細については、Control Catalog の「[オントロジーの該当](#)」を参照してください。
- **ネストされた OU:** AWS Control Tower のネストされた OU は、別の OU に含まれる OU です。ネストされた OU は、厳密に親を 1 つ持つことができ、各アカウントを厳密に 1 つの OU のメンバーにすることができます。ネストされた OU は、階層を作成します。階層内の OU のいずれかにポリシーをアタッチすると、その配下にあるすべての OU とアカウントに適用されます。AWS Control Tower のネストされた OU 階層は、最大 5 レベルの深さになることができます。
- **親 OU:** 階層内の現在の OU のすぐ上にある OU。各 OU は、親 OU を 1 つだけ持つことができます。
- **子 OU:** 階層内の現在の OU より下にある OU。OU は、多数の子 OU を持つことができます。
- **OU 階層:** AWS Control Tower では、ネストされた OU の階層に最大 5 つのレベルを設定できます。ネストの順序は、レベルと呼ばれます。階層の最上位は、レベル 1 と呼ばれます。
- **最上位の OU:** 最上位の OU は、ルート自体ではなく、ルートの直下にある任意の OU です。ルートは、OU とは見なされません。
- **管理対象:** 管理対象リージョンは、組織が設定したガバナンスポリシーに従って、AWS Control Tower によって環境内で管理および制御されます。これらは、ベストプラクティスと組織ポリシーに準拠するようにモニタリングAWS リージョンされます。これらのリージョンのリソースは、AWS Control Tower コントロールを有効にすると保護されます。

- 管理対象外: ステータスが [管理対象外] と表示されるリージョンは、AWS Control Tower によって制御もモニタリングもされません。通常、これらのAWS リージョンは、AWS Control Tower が適用するのと同じガバナンスポリシーに準拠していません。これらのリージョンにリソースを作成することは可能ですが、作成したリソースは AWS Control Tower コントロールでは保護されません。
- 拒否済み: 拒否済みのリージョンは、AWS Control Tower によって明確にブロックされます。AWS Control Tower 環境内では、これらのAWS リージョンにリソースをプロビジョニングすることはできません。

料金

AWS Control Tower の使用に伴う追加料金はありません。AWS Control Tower で有効になっている AWS サービス、およびランディングゾーンで使用するサービスに対してのみ料金が発生します。例えば、Account Factory でアカウントをプロビジョニングするための Service Catalog と、ランディングゾーンで追跡されるイベント AWS CloudTrail に対して料金を支払います。AWS Control Tower に関する料金表や料金については、「[AWS Control Tower の料金](#)」を参照してください。

AWS Control Tower のアカウントからエフェメラルワークロードを実行している場合、関連するコストが増加する可能性があります AWS Config。詳細については、「[AWS Config 料金表](#)」を参照してください。これらのコストの管理の詳細については、AWS アカウント担当者にお問い合わせください。が AWS Control Tower と AWS Config どのように連携するかの詳細については、「[AWS Control Tower と AWS Config の連携](#)」を参照してください [でリソースの変更をモニタリングする AWS Config](#)。

AWS Control Tower の外部に AWS CloudTrail 証跡を実装する場合は、AWS Control Tower で使用できます。ただし、AWS Control Tower によって管理される証跡にもオプトインすると、重複した請求が発生する可能性があります。特別な要件がない限り、外部証跡を設定することはお勧めしません。ランディングゾーンのセットアップまたは更新時にオプトインすることを選択した場合、AWS Control Tower は管理アカウントで組織レベルの CloudTrail 証跡をセットアップしてアクティブ化します。CloudTrail のコスト管理については、「[CloudTrail のコストを管理する](#)」を参照してください。

セットアップ

AWS Control Tower を初めて使用する場合は、このセクションの手順に従って AWS アカウントを作成し、AWS Control Tower 管理アカウントを保護します。専用の追加のセットアップタスクについては AWS Control Tower、「」を参照してください[AWS Control Tower の使用開始方法](#)。

にサインアップする AWS

アマゾン ウェブ サービス (AWS) にサインアップすると、AWS アカウントは AWSを含む のすべてのサービスに自動的にサインアップされます AWS Control Tower。AWS アカウントがすでにある場合は、次のタスクに進んでください。AWS アカウントがない場合は、次の手順を使用してアカウントを作成します。

他のタスクで必要になるため、AWS アカウント番号を書き留めます。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. <https://portal.aws.amazon.com/billing/signup> を開きます。
2. オンラインの手順に従います。

サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

にサインアップすると AWS アカウント、AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、[ルートユーザーアクセスが必要なタスク](#)の実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。<https://aws.amazon.com/> の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、を保護し AWS IAM アイデンティティセンター、を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、AWS アカウント E メールアドレスを入力して、アカウント所有者[AWS マネジメントコンソール](#)として にサインインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、「AWS サインイン ユーザーガイド」の「[ルートユーザーとしてサインインする](#)」を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

手順については、IAM [ユーザーガイドの AWS アカウント「ルートユーザー \(コンソール\) の仮想 MFA デバイス](#)を有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「[AWS IAM アイデンティティセンターの有効化](#)」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法的チュートリアルについては、「AWS IAM アイデンティティセンター ユーザーガイド」の「[デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ](#)」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン「[ユーザーガイド](#)」の [AWS「アクセスポータルにサインインする](#)」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「[アクセス許可セットを作成する](#)」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「[グループを追加する](#)」を参照してください。

アカウントのセキュリティ

AWS Control Tower アカウントのセキュリティを保護するベストプラクティスを設定する方法に関する追加のガイダンスについては、AWS Organizations ドキュメントを参照してください。

- [管理アカウントのベストプラクティス](#)
- [メンバーアカウントのベストプラクティス](#)

次のステップ

[AWS Control Tower の使用開始方法](#)

AWS Control Tower の使用開始方法

この使用開始手順は、AWS Control Tower 管理者を対象としています。AWS Control Tower コンソールまたは API を使用してランディングゾーンをセットアップする準備ができたなら、この手順に従ってください。

現在、AWS Control Tower を初めてご利用の AWS お客様は、先に進む前に [AWS Control Tower ランディングゾーンの計画](#) というセクションを確認してください。

トピック

- [AWS Control Tower クイックスタートガイド](#)
- [前提条件: 管理アカウントの起動前自動チェック](#)
- [コントロール専用環境のセットアップ](#)
- [コンソールからの AWS Control Tower の開始方法](#)
- [API を使用した AWS Control Tower の開始方法](#)
- [次の手順](#)

AWS Control Tower クイックスタートガイド

AWS が初めての場合は、このセクションのステップに従うと、AWS Control Tower の使用をすばやく開始できます。AWS Control Tower 環境をすぐカスタマイズしたい場合は、「[ステップ 2. ランディングゾーンの設定と起動](#)」を参照してください。

Note

AWS Control Tower は、AWS CloudTrail、AWS Config、Amazon CloudWatch、Amazon S3、Amazon VPC などの有料サービスをセットアップします。これらのサービスを使用すると、[料金のページ](#)に示す費用が発生する場合があります。有料サービスの使用状況と発生した費用は、AWS マネジメントコンソールに表示されます。AWS Control Tower 自体に追加の費用が発生することはありません。

開始する前に

セットアッププロセスの開始前に行うべき最も重要な決定は、ホームリージョンを選択することです。ホームリージョンは、ほとんどのワークロードを実行したり、ほとんどのデータを保存したりす

る AWS リージョンです。AWS Control Tower ランディングゾーンをセットアップした後では、ホームリージョンを変更できません。ホームリージョンの選択方法の詳細については、「[ランディングゾーンのセットアップに関する管理上のヒント](#)」を参照してください。

 Note

デフォルトでは、AWS Control Tower は、アカウントを現在運用しているリージョンをホームリージョンとして選択します。現在のリージョンは、AWS マネジメントコンソール画面の右上で確認できます。

クイックスタート手順では、AWS Control Tower 環境のリソースのデフォルト値を受け入れることを前提としています。これらの選択肢の多くは後で変更できます。いくつかの 1 回限りの選択肢は「[ランディングゾーン設定に対する想定](#)」セクションに示しています。

新しい AWS アカウントを作成すると、AWS Control Tower のセットアップに必要な前提条件が自動的に満たされます。次の手順に進むことができます。

クイックスタート手順

1. 管理者ユーザー認証情報を使用して AWS マネジメントコンソールにサインインします。
2. AWS Control Tower コンソール (<https://console.aws.amazon.com/controltower>) に移動します。
3. 目的のホームリージョンで作業していることを確認します。
4. [Set up landing zone] (ランディングゾーンの設定) を選択します。
5. コンソールの指示に従い、すべてのデフォルト値を受け入れます。アカウント、ログアーカイブアカウント、監査アカウントの E メールアドレスを入力する必要があります。
6. 選択内容を確認して、[Set up landing zone] (ランディングゾーンの設定) を選択します。
7. AWS Control Tower は、ランディングゾーンのすべてのリソースをセットアップするのに約 30 分かかります。

環境をカスタマイズする方法など、AWS Control Tower のセットアップ方法の詳細については、次のいくつかのトピックの手順を参照して従ってください。

Note

初めて使用するとき、セットアップ問題が発生した場合は、[AWS サポート](#)に連絡し、診断の支援を要請してください。

前提条件: 管理アカウントの起動前自動チェック

AWS Control Tower では、ランディングゾーンをセットアップする前に、アカウントで一連の起動前チェックが自動的に実行されます。これらのチェックは、ランディングゾーンを確立する変更に管理アカウントが対応できることを確認するためのものであり、お客様側のアクションは必要ありません。ランディングゾーンをセットアップする前に AWS Control Tower が実行するチェックは次のとおりです。

- AWS Control Tower を起動するには、の既存のサービス制限で十分 AWS アカウント である必要があります。詳細については、「[AWS Control Tower の制限とクォータ](#)」を参照してください。
- は、次の AWS サービスにサブスクライブ AWS アカウント する必要があります。
 - 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

デフォルトでは、すべてのアカウントがこれらのサービスに登録されています。

AWS IAM アイデンティティセンター (IAM Identity Center) のお客様に関する考慮事項

- AWS IAM アイデンティティセンター (IAM Identity Center) が既に設定されている場合、AWS Control Tower ホームリージョンは IAM Identity Center リージョンと同じである必要があります。
- IAM Identity Center は、組織の管理アカウントにのみインストールできます。
- 選択した ID ソースに基づいて、次の 3 つのオプションが IAM Identity Center ディレクトリに適用されます。
 - IAM Identity Center ユーザーストア: SSO for AWS Control Tower が IAM Identity Center でセットアップされている場合、AWS Control Tower は IAM Identity Center ディレクトリにグループを作成し、メンバーアカウント用に選択したユーザーに対してこれらのグループへのアクセスをプロビジョニングします。
 - Active Directory: IAM Identity Center for AWS Control Tower が Active Directory でセットアップされている場合、AWS Control Tower は IAM Identity Center ディレクトリを管理しません。新規 AWS アカウントにユーザーやグループを割り当てません。
 - 外部 ID プロバイダー: AWS Control Tower for IAM Identity Center が外部 ID プロバイダー (IdP) でセットアップされている場合、AWS Control Tower は IAM Identity Center ディレクトリにグループを作成し、メンバーアカウント用に選択したユーザーに対してこれらのグループへのアクセスをプロビジョニングします。アカウントの作成時に Account Factory の外部 IdP から既存のユーザーを指定できます。AWS Control Tower は、IAM Identity Center と外部 IdP 間で同じ名前のユーザーを同期するときに、その新しく発行されたアカウントへのアクセス許可を指定されたユーザーに付与します。AWS Control Tower のデフォルトグループの名前と一致するように外部 IdP にグループを作成することもできます。これらのグループにユーザーを割り当てると、ユーザーが登録済みのアカウントにアクセスできるようになります。

IAM Identity Center および AWS Control Tower の使用に関する詳細については、「[IAM Identity Center アカウントと AWS Control Tower に関する注意事項](#)」を参照してください。

AWS Config および AWS CloudTrail のお客様に関する考慮事項

- では、組織の管理アカウントで信頼されたアクセスを有効にする AWS アカウント ことはできません AWS Config。信頼されたアクセスを無効にする方法については、[信頼されたアクセスを有効または無効にする方法に関する AWS Organizations ドキュメント](#)を参照してください。
- AWS Control Tower に登録する予定の既存のアカウントに既存の AWS Config レコーダー、配信チャネル、または集約設定がある場合は、ランディングゾーンの設定後にアカウントの登録を開始

する前に、これらの設定を変更または削除する必要があります。この事前チェックは、ランディングゾーンの起動時に AWS Control Tower 管理アカウントには適用されません。詳細については、「[既存の AWS Config リソースがあるアカウントを登録する](#)」を参照してください。

- AWS Control Tower のアカウントからエフェメラルワークロードを実行している場合、Config AWS に関連するコストが増加する可能性があります。これらのコストの管理の詳細については、AWS アカウント担当者にお問い合わせください。
- AWS Control Tower にアカウントを登録すると、アカウントは AWS Control Tower 組織の AWS CloudTrail 証跡によって管理されます。アカウントに CloudTrail 追跡の既存のデプロイがある場合、AWS Control Tower にアカウントを登録する前にアカウントの既存の追跡を削除しない限り、料金が重複して発生する可能性があります。組織レベルの追跡と AWS Control Tower の詳細については、「[料金](#)」を参照してください。

Note

起動時に、AWS Control Tower によって管理されるすべてのリージョンで、AWS Security Token Service (STS) エンドポイントを管理アカウントでアクティブ化する必要があります。この操作を行わないと、設定プロセスの途中で起動が失敗する可能性があります。

コントロール専用環境のセットアップ

AWS Control Tower ランディングゾーン 4.0 では、完全なランディングゾーンを実装することなく、コントロールのみの環境を作成できるようになりました。このデプロイオプションは、AWS Organizations のセットアップが確立されており、[AWS Control Tower Control Catalog](#) を介したマネージドコントロールの採用に集中したいお客様向けに設計されています。

トピック

- [開始方法](#)
- [AWS Config に関する考慮事項](#)
- [実装プロセス](#)
- [重要な注意事項](#)

開始方法

まず、ホームページから AWS Control Tower Control Catalog を確認して、利用可能なマネージドコントロール、関連するコンプライアンスフレームワーク、コントロールメタデータを理解します。AWS Control Tower でこのエクスペリエンスを有効にするには、既存の環境があり、コンソールで AWS マネージドコントロールを有効にすることを選択します。次に、ホームリージョンを確認し、必要に応じて追加の管理対象リージョンを選択します。セットアップ中に、自動アカウント登録を有効にできます。これにより、アカウントは OU 間で移動するときに、親組織単位 (OUs) からコントロールと設定を自動的に継承できます。

AWS Config に関する考慮事項

初期設定 AWS Config 時、または必要に応じて後で を有効にするオプションがあります。AWS Config は、環境で検出コントロールを使用する予定がある場合は必要です。を有効にする場合は AWS Config、設定とコンプライアンスデータを収集するアグリゲータアカウントを指定する必要があります。既存のアカウントを選択するか、セットアップ中に新しいアカウントを作成できます。その他のオプションには、AWS KMS キー暗号化の設定や、記録の Amazon S3 ログ保持期間の指定などがあります。

実装プロセス

なしで続行すると AWS Config、環境は Control Catalog 内の予防コントロールとプロアクティブコントロールをすぐに実行できるようになります。

ただし、最初の検出コントロールを有効にする準備ができたなら、ターゲット OUs で有効 Config Baseline になっている新しい を通じて AWS Config 記録を有効にする必要があります。これは OU あたりの 1 回限りのセットアッププロセスであり、OU あたりのアカウント数と AWS リージョンあたりのアカウントあたりのリソース数に基づいて AWS Config 料金が発生します。

重要な注意事項

AWS Control Tower 環境を作成すると、との信頼関係が確立され AWS Organizations、予防コントロールのドリフト検出が可能になり、アカウントと OU の変更を追跡できます。セットアップ中、AWS Control Tower はマネージドコントロール環境の基盤となるランディングゾーン設定を作成します。

APIs 「」を参照してください [API を使用した AWS Control Tower の開始方法](#)。マニフェストフィールドはランディングゾーン 4.0 ではオプションになりました。

コンソールからの AWS Control Tower の開始方法

この使用開始手順は、AWS Control Tower 管理者を対象としています。AWS Control Tower コンソールを使用してランディングゾーンをセットアップする準備ができたなら、この手順に従ってください。開始から完了まで、所要時間は約 30 分です。この手順は、いくつかの前提条件と 3 つの主なステップを必要とします。

現在、AWS Control Tower を初めてご利用の AWS お客様は、先に進む前に [AWS Control Tower ランディングゾーンの計画](#) というセクションを確認してください。

トピック

- [ランディングゾーン設定に対する想定](#)
- [ステップ 1: 共有アカウントの E メールアドレスを作成する](#)
- [ステップ 2. ランディングゾーンの設定と起動](#)
- [ステップ 3. ランディングゾーンの確認とセットアップ](#)

ランディングゾーン設定に対する想定

AWS Control Tower ランディングゾーンをセットアップするプロセスには、複数のステップがあります。AWS Control Tower ランディングゾーンには設定可能な側面があります。それ以外の選択肢は、セットアップ後に変更できません。

セットアップ時に設定する主な項目

- セットアップ時に最上位の OU 名を選択できます。また、ランディングゾーンのセットアップ後に OU 名を変更することもできます。デフォルトでは、最上位の OU 名は [Security] (セキュリティ) と [Sandbox] (サンドボックス) です。詳細については、「[アーキテクチャが適切に設計された環境をセットアップするためのガイドライン](#)」を参照してください。
- セットアップ時に、AWS Control Tower がデフォルトで作成する共有アカウントの名前 (デフォルトではログアーカイブと監査) をカスタマイズできますが、セットアップ後はこれらの名前を変更できません (これは 1 回限りの選択です)。
- セットアップ時に、オプションで AWS Control Tower の既存の AWS アカウントを指定して、監査およびログアーカイブアカウントとして使用できます。既存の AWS アカウントを指定し、それらのアカウントに既存の AWS Config リソースがある場合は、AWS Control Tower にアカウントを登録する前に既存の AWS Config リソースを削除する必要があります。(これは 1 回限りの選択です)。

- を初めて設定する場合、またはランディングゾーンバージョン 3.0 にアップグレードする場合は、AWS Control Tower が組織の組織レベルの AWS CloudTrail 証跡を設定できるようにするか、AWS Control Tower によって管理される証跡をオプトアウトして独自の CloudTrail 証跡を管理するかを選択できます。ランディングゾーンを更新するたびに、AWS Control Tower が管理する組織レベルの証跡をオプトインまたはオプトアウトできます。
- オプションで、ランディングゾーンを設定または更新する際、Amazon S3 ログバケットとログアクセスバケットにカスタマイズされた保持ポリシーを設定できます。
- オプションで、事前に定義したブループリントを指定して、AWS Control Tower コンソールでのカスタマイズされたメンバーアカウントのプロビジョニングに使用できます。使用できるブループリントがない場合は、後でアカウントをカスタマイズできます。「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。

元に戻すことができない設定の選択

- ランディングゾーンをセットアップした後で、ホームリージョンを変更することはできません。
- VPC で Account Factory アカウントをプロビジョニングしている場合、いったん作成した VPC CIDR を変更することはできません。

ステップ 1: 共有アカウントの E メールアドレスを作成する

新しいでランディングゾーンを設定する場合は AWS アカウント、「」を参照してください[セットアップ](#)。

- 新しい共有アカウントでランディングゾーンを設定するには、AWS Control Tower には、にまだ関連付けられていない 2 つの一意の E メールアドレスが必要です AWS アカウント。これらの E メールアドレスは、それぞれ共同受信箱として機能します。つまり、企業内で AWS Control Tower に関連する特定の作業を行うさまざまなユーザーの共有 E メールアカウントとなります。
- AWS Control Tower を初めて設定し、既存のセキュリティアカウントとログアーカイブアカウントを AWS Control Tower に持ち込む場合は、既存の AWS アカウントの現在の E メールアドレスを入力できます。

この E メールアドレスは以下に必要です。

- 監査アカウント - このアカウントは、AWS Control Tower によって提供される監査情報にアクセスする必要があるユーザーのチーム用です。また、環境のプログラムによる監査を実行してコンプラ

イアンス目的の監査に役立つサードパーティー製ツールのアクセスポイントとして、このアカウントを使用することもできます。

- ログアーカイブアカウント - このアカウントは、ランディングゾーンで登録済み OU 内のすべての登録済みアカウントに関するログ情報にアクセスする必要があるユーザーのチーム用です。

これらのアカウントは、ランディングゾーンの作成時にセキュリティ OU にセットアップされます。ベストプラクティスとして、これらのアカウントでアクションを実行するときは、適切なスコープの許可を持つ IAM Identity Center ユーザーを使用することをお勧めします。

Note

既存の AWS アカウントを監査アカウントおよびログアーカイブアカウントとして指定する場合、既存のアカウントは起動前のチェックに合格して、AWS Control Tower の要件と競合するリソースがないことを確認する必要があります。これらのチェックが成功しない場合、ランディングゾーンのセットアップは成功しない可能性があります。特に、アカウントには既存の AWS Config リソースがあってはなりません。詳細については、「[既存のセキュリティアカウントまたはログアカウントを使用する際の考慮事項](#)」を参照してください。

わかりやすくするために、このユーザーガイドでは常に共有アカウントをログアーカイブおよび監査というデフォルト名で参照しています。これらのアカウントをカスタマイズする場合は、このドキュメントを参照するときに、アカウントに付けたカスタマイズ後の名前に読み替えてください。[Account details] (アカウントの詳細) ページでは、カスタマイズした名前でアカウントを参照できます。

Note

マルチアカウント戦略に合わせて、一部の AWS Control Tower 組織単位 (OUs) AWS のデフォルト名に関する用語を変更しています。こうした名称をわかりやすくするための移行を進めていますが、まだ統一されていない部分もあります。セキュリティ OU は以前はコア OU と呼ばれていました。サンドボックス OU は、以前はカスタム OU と呼ばれていました。

ステップ 2. ランディングゾーンの設定と起動

AWS Control Tower ランディングゾーンを起動する前に、最も適切なホームリージョンを決定します。詳細については、「[ランディングゾーンのセットアップに関する管理上のヒント](#)」を参照してください。

Important

AWS Control Tower ランディングゾーンをデプロイした後にホームリージョンを変更するには、廃止と AWS サポートの支援が必要です。この方法は推奨されません。

AWS CLI で を使用してランディングゾーンを設定および起動する方法について説明します [API を使用した AWS Control Tower の開始方法](#)。

コンソールでランディングゾーンを設定して起動するには、次の一連のステップを実行します。

準備: AWS Control Tower コンソールに移動します。

1. ウェブブラウザを開き、AWS Control Tower コンソール (<https://console.aws.amazon.com/controltower>) に移動します。
2. コンソールで、AWS Control Tower の目的のホームリージョンで作業していることを確認します。次に、[Set up your landing zone] (ランディングゾーンを設定する) を選択します。

ステップ 2a. AWS リージョンを確認して選択する

ホーム AWS リージョンに選択したリージョンが正しく指定されていることを確認してください。AWS Control Tower をデプロイした後で、ホームリージョンを変更することはできません。

セットアッププロセスのこのセクションでは、必要な AWS リージョンを追加できます。必要に応じて後でリージョンを追加したり、管理対象からリージョンを除外したりできます。

管理する追加の AWS リージョンを選択するには

1. パネルに、現在選択しているリージョンが表示されます。ドロップダウンメニューを開いて、管理できる追加のリージョンのリストを表示します。
2. AWS Control Tower で管理できるようにするには、各リージョンの横にあるチェックボックスをオンにします。ホームリージョンの選択は編集できません。

特定のリージョンへのアクセスを拒否するには

特定の AWS リージョンの AWS リソースとワークロードへのアクセスを拒否するには、リージョン拒否コントロールの セクションで有効を選択します。デフォルトでは、このコントロールの設定は [Not enabled] (有効でない) になっています。

ステップ 2b. 組織単位 (OU) の設定

これらの OU のデフォルト名をそのまま使用する場合には、セットアップを続行するために必要なアクションはありません。OU の名前を変更する場合は、フォームフィールドに新しい名前を直接入力します。

- [Foundational OU] (基礎となる OU) - AWS Control Tower は、[Foundational OU] (基礎となる OU) (当初の名前は [Security OU] (セキュリティ OU)) を利用します。この OU の名前は、初期セットアップ時やその後に OU の詳細ページから変更できます。この [Security OU] (セキュリティ OU) には、2 つの共有アカウントが含まれています。デフォルトではログアーカイブアカウントと監査アカウントです。
- [Additional OU] (追加の OU) - AWS Control Tower では、ユーザーに代わって 1 つ以上の追加 OU をセットアップできます。ランディングゾーンに [Security OU] (セキュリティ OU) の他に少なくとも 1 つの [Additional OU] (追加の OU) をプロビジョニングすることをお勧めします。この追加の OU が開発プロジェクトを対象としている場合は、[「アーキテクチャが適切に設計された環境をセットアップするためのガイドライン」](#)で示すように、サンドボックス OU という名前にすることをお勧めします。に既存の OU がある場合は AWS Organizations、AWS Control Tower で追加の OU のセットアップをスキップするオプションが表示される場合があります。

ステップ 2c. 共有アカウント、ログ、および暗号化の設定

セットアッププロセスのこのセクションでは、共有 AWS Control Tower アカウントにデフォルトで選択される名前がパネルに表示されます。これらのアカウントは、ランディングゾーンに不可欠な要素です。これらの共有アカウントは移動または削除しないでください。セットアップ時に、監査アカウントとログアーカイブアカウントの名前をカスタマイズできます。または、1 回限りのオプションとして、既存の AWS アカウントを共有アカウントとして指定することもできます。

ログアーカイブアカウントと監査アカウントに一意の E メールアドレスを指定する必要があります。また、以前に管理アカウントに指定した E メールアドレスを確認できます。[Edit] (編集) ボタンをクリックして、編集可能なデフォルト値を変更します。

共有アカウントについて

- **管理アカウント - AWS Control Tower** 管理アカウントはルートレベルの一部です。管理アカウントでは、AWS Control Tower の請求が許可されています。また、ランディングゾーンの管理者許可もあります。AWS Control Tower では、請求用と管理者許可用に個別のアカウントを作成することはできません。

管理アカウントに表示される E メールアドレスは、セットアップのこのフェーズでは編集できません。これは確認として表示されます。そのため、複数のアカウントを持っている場合には、正しい管理アカウントを編集していることを確認できます。

- **2 つの共有アカウント** - この 2 つのアカウントの名前をカスタマイズできます。また、自分のアカウントを持ち込んで、新規または既存を問わず、アカウントごとに一意の E メールアドレスを指定することができます。AWS Control Tower で新しい共有アカウントを作成することを選択した場合、E メールアドレスにアカウントが関連付けられていることはできません AWS。

共有アカウントを設定するには、リクエストされた情報を入力します。

1. コンソールで、ログアーカイブという当初のアカウント名を変更して、新しい名前を入力します。このアカウント名は、多くのお客様がデフォルトのままにしています。
2. このアカウントの一意の E メールアドレスを指定します。
3. 監査という当初のアカウント名を変更して、新しい名前を入力します。このアカウント名は、多くのお客様がセキュリティという名前にすることを選択しています。
4. このアカウントの一意の E メールアドレスを指定します。

オプションでログの保持を設定する

このセットアップフェーズでは、AWS Control Tower にログを保存する Amazon S3 バケットの AWS CloudTrail ログ保持ポリシーを、日単位または年単位で、最大 15 年までカスタマイズできます。ログの保持をカスタマイズしない場合、デフォルト設定は、標準アカウントのログ記録で 1 年、アクセスログで 10 年です。この機能は、ランディングゾーンの更新またはリセット時にも使用できます。

オプションで自己管理 AWS アカウント アクセス

AWS Control Tower が (IAM) を使用して AWS アカウント AWS Identity and Access Management アクセスを設定するか、AWS アカウント アクセスを自己管理するかを選択できます。IAM AWS アイデンティティセンターのユーザー、ロール、アクセス許可を自分で設定してカスタマイズする

か、外部 IdP などの別の方法で、IAM アイデンティティセンターを使用して直接アカウントフェデレーションまたは複数のアカウントへのフェデレーションを行うことができます。この選択は後で変更できます。

デフォルトでは、AWS Control Tower AWS は、[「複数のアカウントを使用して AWS 環境を整理する」](#)で定義されているベストプラクティスのガイダンスに従って、ランディングゾーンに IAM アイデンティティセンターを設定します。ほとんどのお客様はデフォルトを選択します。特定の業界や国、または IAM Identity Center AWS AWS リージョン が利用できない での規制コンプライアンスのために、代替アクセス方法が必要になる場合があります。

アカウントレベルでの ID プロバイダーの選択はサポートされていません。このオプションはランディングゾーン全体にのみ適用されます。

詳細については、[「IAM Identity Center のガイダンス」](#)を参照してください。

オプションで AWS CloudTrail 証跡を設定する

ベストプラクティスとして、ロギングを設定することをお勧めします。AWS Control Tower に組織レベルの CloudTrail 証跡の設定と管理を許可する場合は、[Opt in] (オプトイン) を選択します。独自の CloudTrail 証跡またはサードパーティ製のログ作成ツールでログを管理する場合は、[Opt out] (オプトアウト) を選択します。コンソールで要求された場合は、選択を確認します。ランディングゾーンを更新する際、選択を変更したり、組織レベルの証跡をオプトイン/オプトアウトできます。

組織レベルおよびアカウントレベルの証跡を含め、独自の CloudTrail 証跡を随時設定および管理できます。重複した CloudTrail 証跡を設定すると、CloudTrail イベントがログに記録される時点で重複するコストが発生する可能性があります。

オプションで を設定する AWS KMS keys

暗号化キーを使用してリソースを AWS KMS 暗号化および復号する場合は、チェックボックスをオンにします。既存のキーがある場合は、ドロップダウンメニューに表示される識別子からキーを選択できます。[Create a key] (キーの作成) を選択して、新しいキーを生成できます。KMS キーは、ランディングゾーンを更新するたびに追加または変更できます。

[Set up landing zone] (ランディングゾーンの設定) を選択した場合、AWS Control Tower は KMS キーを検証するための事前チェックを実行します。キーは、以下の条件を満たす必要があります。

- 有効
- 対称
- マルチリージョンキーではない

- ポリシーに正しい許可が追加されている
- キーが管理アカウントにある

キーがこれらの要件を満たしていない場合は、エラーバナーが表示されることがあります。その場合は、別のキーを選択するか、キーを生成します。次のセクションで説明するように、必ずキーの許可ポリシーを編集してください。

KMS キーポリシーを更新する

KMS キーポリシーを更新する前に、KMS キーを作成する必要があります。詳細については、「AWS Key Management Service デベロッパーガイド」の「[キーポリシーの作成](#)」を参照してください。

AWS Control Tower で KMS キーを使用するには、AWS Config とに必要な最小限のアクセス許可を追加して、デフォルトの KMS キーポリシーを更新する必要があります AWS CloudTrail。ベストプラクティスとして、どのポリシーでも必要最小限のアクセス許可を付与することをお勧めします。KMS キーポリシーを更新する場合、権限を 1 つの JSON ステートメントまたは行単位でグループとして追加できます。

この手順では、AWS Config と CloudTrail が暗号化 AWS KMS に使用できるポリシーステートメントを追加して、AWS KMS コンソールでデフォルトの KMS キーポリシーを更新する方法について説明します。ポリシーステートメントには、次の情報を含める必要があります。

- **YOUR-MANAGEMENT-ACCOUNT-ID** – AWS Control Tower を設定する管理アカウントの ID。
- **YOUR-HOME-REGION** – AWS Control Tower をセットアップするときに選択するホームリージョン。
- **YOUR-KMS-KEY-ID** – ポリシーで使用される KMS キー ID。

KMS キーポリシーを更新するには

1. で AWS KMS コンソールを開く <https://console.aws.amazon.com/kms>
2. ナビゲーションペインで、[カスタマーマネージドキー] を選択します。
3. テーブルで、編集するキーを選択します。
4. [キーポリシー] タブで、キーポリシーを表示できることを確認します。キーポリシーが表示されない場合は、[ポリシービューへの切り替え] を選択します。
5. [編集] を選択し、AWS Config と CloudTrail の次のポリシーステートメントを追加してデフォルトの KMS キーポリシーを更新します。

AWS Config ポリシーステートメント

```
{
  "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 ポリシーステートメント

```
{
  "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. [Save changes] (変更の保存) をクリックします。

KMS キーポリシーの例

次のポリシー例は、AWS Config と CloudTrail に最低限必要なアクセス許可を付与するポリシーステートメントを追加した後、KMS キーポリシーがどのようになるかを示しています。サンプルポリシーには、デフォルトの KMS キーポリシーは含まれていません。

```
{
  "Version": "2012-10-17",
  "Id": "CustomKMSPolicy",
  "Statement": [
    {
      ... YOUR-EXISTING-POLICIES ...
    },
    {
      "Sid": "Allow Config to use KMS for encryption",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
    },
    {
      "Sid": "Allow CloudTrail to use KMS for encryption",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
      "Condition": {
        "StringEquals": {
```

```
        "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:cloudtrail:arn":
          "arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
      }
    }
  }
}
```

その他のポリシーの例については、以下のページを参照してください。

- 「[Granting encrypt permissions](#)」 (AWS CloudTrail ユーザーガイド)。
- 「[Required Permissions for the KMS Key When Using Service-Linked RolesS3 Bucket Delivery](#)」 (AWS Config デベロッパーガイド)。

攻撃者からの保護

ポリシーに特定の条件を追加することで、混乱した代理攻撃と呼ばれる特定のタイプの攻撃を防ぐことができます。これは、クロスサービス偽装など、エンティティが、より特権のあるエンティティにアクションを実行させる場合に発生します。ポリシー条件に関する一般的な情報については、「[ポリシーでの条件の指定](#)」も参照してください。

AWS Key Management Service (AWS KMS) では、マルチリージョン KMS キーと非対称キーを作成できますが、AWS Control Tower はマルチリージョンキーまたは非対称キーをサポートしていません。AWS Control Tower は、既存のキーの事前チェックを実行します。マルチリージョンキーまたは非対称キーを選択すると、エラーメッセージが表示されることがあります。その場合は、AWS Control Tower リソースで使用する別のキーを生成してください。

詳細については AWS KMS、「[AWS KMS デベロッパーガイド](#)」を参照してください。

AWS Control Tower の顧客データは、デフォルトでは SSE-S3 を使用して保存時に暗号化されます。

オプションでアカウントの自動登録を設定する

セットアップ中、またはそれ以降にこの機能を有効にすると、2つの登録済み OU 間で移動されたアカウント、または初めて AWS Control Tower 環境に移動されたアカウントは、継承ドリフトの状態を表示しなくなります。アカウントは、新しい OU で有効になっているベースラインとコントロールを自動的に継承します。前の OU のコントロールとベースラインは削除されます。

設定後に自動登録をオプトインするには、ランディングゾーンの [設定] ページに移動し、ランディングゾーンの [更新] を選択するか、AWS Control Tower UpdateLandingZone API を呼び出します。

API または AWS Control Tower コンソールを使用して AWS Organizations、OUs 間でアカウントを移動できます。登録されている OU の外部にアカウントを移動すると、AWS Control Tower はデプロイされたすべてのベースラインとコントロールを自動的に削除します。基本的に、AWS Control Tower からアカウントの登録を解除します。

Note

ランディングゾーンの初期設定後に自動登録機能を有効にする場合、AWS Control Tower は自動登録機能が有効になる前に OU 間でアカウントを移動したことが原因で発生した継承ドリフトを遡及的に解決しません。自動ドリフト解決は、この設定を有効にした後に移動されたアカウントに対して有効になります。

オプションで、カスタマイズされたメンバーアカウントを設定および作成する

[Create account] (アカウントの作成) ワークフローに従ってメンバーアカウントを作成する場合、オプションで、事前に定義したブループリントを指定して、AWS Control Tower コンソールでのカスタマイズされたメンバーアカウントのプロビジョニングに使用できます。使用できるブループリントがない場合は、後でアカウントをカスタマイズできます。「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。

ステップ 3. ランディングゾーンの確認とセットアップ

セットアップの次のセクションでは、AWS Control Tower がランディングゾーンに対して求める許可を示します。チェックボックスをオンにして各トピックを展開します。これらの許可に同意し (複数のアカウントに影響する可能性があります)、利用規約全体に同意するように求められます。

確定するには

1. コンソールでサービスアクセス許可を確認し、準備ができたら、AWS Control Tower が AWS リソースの管理とルール適用に使用するアクセス許可を理解します。
2. 選択を確定して起動を初期化するには、[Set up landing zone] (ランディングゾーンの設定) を選択します。

この一連のステップにより、ランディングゾーンセットアッププロセスが開始されます。完了するまでに 30 分ほどかかる場合があります。セットアップ時に、AWS Control Tower がルートレベル、セキュリティ OU、および共有アカウントを作成します。他の AWS リソースは作成、変更、または削除されます。

SNS サブスクリプションの確認

監査アカウントで指定した E メールアドレス宛に、AWS Control Tower でサポートしているすべての AWS リージョンから「AWS Notification - Subscription Confirmation」(通知 - サブスクリプション確認) という件名の E メールが届きます。監査アカウントでコンプライアンス E メールを受信するには、AWS Control Tower でサポートされている各 AWS リージョンから、各 E メール内のサブスクリプションの確認リンクを選択する必要があります。

API を使用した AWS Control Tower の開始方法

この使用開始手順は、AWS Control Tower 管理者を対象としています。この手順は、いくつかの前提条件と 2 つの主なステップを必要とします。

この手順では、AWS Control Tower およびその他の AWS サービスの APIs を使用してランディングゾーンを設定および起動します。これらの APIs を使用すると、[CloudFormation コンソールまたはを使用して](#)、プログラムで AWS Control Tower 環境を作成できます AWS CLI。

AWS Control Tower のランディングゾーンを起動する前に、以下の前提条件のタスクを実行してください。

- 最も適切なホームリージョンを決定します。詳細については、「[ランディングゾーンのセットアップに関する管理上のヒント](#)」を参照してください。
- 「[前提条件: 管理アカウントの起動前自動チェック](#)」で起動前自動チェックを参照し、ランディングゾーンを確立する変更に対して管理アカウントが対応できることを確認します。

トピック

- [API を使用したランディングゾーン設定に対する想定](#)
- [ステップ 1: ランディングゾーンを設定する](#)
- [ステップ 2: AWS Control Tower APIs](#)
- [ランディングゾーンを特定する](#)
- [ランディングゾーンを更新する](#)
- [ランディングゾーンをリセットしてドリフトを解決する](#)
- [ランディングゾーンのマニフェストファイルの詳細を表示する](#)
- [ランディングゾーンオペレーションのステータスを表示する](#)
- [例: API のみを使用して AWS Control Tower ランディングゾーンを設定する](#)
- [ランディングゾーンのスキーマ](#)
- [CloudFormation を使用してランディングゾーンを起動する](#)

API を使用したランディングゾーン設定に対する想定

AWS Control Tower ランディングゾーンをセットアップするプロセスには、複数のステップがあります。AWS Control Tower ランディングゾーンには設定可能な側面があります。それ以外の選択肢は、セットアップ後に変更できません。

セットアップ時に設定する主な項目

- セットアップ時に基礎となる OU 名を選択できます。また、ランディングゾーンのセットアップ後に OU 名を変更することもできます。デフォルトでは、基礎となる OU 名は [セキュリティ] と [サンドボックス] です。詳細については、「[アーキテクチャが適切に設計された環境をセットアップするためのガイドライン](#)」を参照してください。
- セットアップ時に、AWS Control Tower がデフォルトで作成する共有アカウントの名前 (デフォルトではログアーカイブと監査) をカスタマイズできますが、セットアップ後はこれらの名前を変更できません (これは 1 回限りの選択です)。
- APIs のセットアップ時に、AWS Control Tower が監査およびログアーカイブ AWS アカウントとして使用する既存のアカウントを指定する必要があります。既存の AWS アカウントを指定するには、それらのアカウントに既存の AWS Config リソースがある場合は、AWS Control Tower にアカウントを登録する前に、既存の AWS Config リソースを削除または変更する必要があります。 (これは 1 回限りの選択です)。

- を初めて設定する場合、またはランディングゾーンバージョン 3.0 にアップグレードする場合は、AWS Control Tower が組織の組織レベルの AWS CloudTrail 証跡を設定できるようにするか、AWS Control Tower によって管理される証跡をオプトアウトして独自の CloudTrail 証跡を管理するかを選択できます。ランディングゾーンを更新するたびに、AWS Control Tower が管理する組織レベルの証跡をオプトインまたはオプトアウトできます。
- オプションで、ランディングゾーンを設定または更新する際、Amazon S3 ログバケットとログアクセスバケットにカスタマイズされた保持ポリシーを設定できます。

元に戻すことができない設定の選択

- ランディングゾーンをセットアップした後で、ホームリージョンを変更することはできません。
- VPC で アカウントをプロビジョニングしている場合、いったん作成した VPC CIDR を変更することはできません。

次のセクションでは、セットアップの前提条件と詳細なステップを説明および注意事項とともに示します。その他のコード例については、「[例: API のみを使用して AWS Control Tower ランディングゾーンを設定する](#)」を参照してください。

ステップ 1: ランディングゾーンを設定する

AWS Control Tower ランディングゾーンをセットアップするプロセスには、複数のステップがあります。AWS Control Tower ランディングゾーンの特定の要素は設定可能ですが、それ以外はセットアップ後に変更できません。ランディングゾーンを起動する前に、これらの重要な考慮事項の詳細については、[ランディングゾーン設定の期待値](#)を参照してください。

AWS Control Tower ランディングゾーン APIs を使用する前に、まず他の AWS サービスから APIs を呼び出して、起動前にランディングゾーンを設定する必要があります。このプロセスには、3 つの主要なステップが含まれます。

1. 新しい AWS Organizations 組織の作成
2. サービス統合アカウントの設定
3. ランディングゾーン API の呼び出しに必要なアクセス許可を持つ IAM ロールまたは IAM アイデンティティセンターユーザーを作成する。

ステップ 1. ランディングゾーンを含む組織を作成する:

AWS Organizations CreateOrganization API を呼び出し、すべての機能を有効にして基礎 OU を作成します。AWS Control Tower では、指定されたセキュリティ OU を作成することもお勧めします。このセキュリティ OU には、すべてのサービス統合アカウントが含まれている必要があります。これらは、以前のランディングゾーンバージョンのログアーカイブアカウントと監査アカウントになります。

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

AWS Control Tower では、1 つ以上の追加の OU をセットアップできます。ランディングゾーンに [Security OU] (セキュリティ OU) の他に少なくとも 1 つの [Additional OU] (追加の OU) をプロビジョニングすることをお勧めします。この追加 OU が開発プロジェクトを対象としている場合は、[AWS Control Tower ランディングゾーンの AWS マルチアカウント戦略](#)に記載されているように、サンドボックス OU に名前を付けることをお勧めします。

ステップ 2. 必要に応じてサービス統合アカウントをプロビジョニングします。

ランディングゾーンをセットアップするために、AWS Control Tower では AWS サービス統合を設定できます。これらのサービス統合ごとに、1 つ以上のサービス統合中央アカウントが必要になる場合があります。ランディングゾーン APIs を使用して AWS Control Tower を初めてセットアップする場合は、有効な AWS サービス統合ごとに中央統合アカウントを指定する必要があります。既存の AWS アカウントを使用するか、AWS Control Tower コンソールまたは AWS Organizations APIs を使用してこれらのアカウントをプロビジョニングできます。これらのサービス統合アカウントが、組織内のルートレベルの指定されたセキュリティ OU にあることを確認します。

1. AWS Organizations CreateAccount API を呼び出して、セキュリティ OU にログアーカイブアカウントと監査アカウントを作成します。

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

(オプション) AWS Organizations DescribeAccount API を使用して CreateAccount オペレーションのステータスを確認します。

2. プロビジョニングされたサービス統合アカウントを指定されたセキュリティ OU に移動する

```
aws organizations move-account --account-id 0123456789012
--source-parent-id r-examplerootid111 --destination-parent-id ou-examplerootid111-
security
```

ステップ 3. 必要なサービスロールを作成する

/service-role/ IAM パスの次の IAM サービスロールを作成して、AWS Control Tower がランディングゾーンのセットアップに必要な API コールを実行できるようにします。

- [AWSControlTowerAdmin](#)
- [AWSControlTowerCloudTrailRole](#)
- [AWSControlTowerStackSetRole](#)
- [AWSControlTowerConfigAggregatorRoleForOrganizations](#)

これらのロールとポリシーの詳細については、「[AWS Control Tower でアイデンティティベースのポリシー \(IAM ポリシー\) を使用する](#)」を参照してください。

IAM ロールを作成するには:

すべてのランディングゾーン API を呼び出すために必要なアクセス許可を持つ IAM ロールを作成します。または、IAM アイデンティティセンターユーザーを作成して、必要なアクセス許可を割り当てることもできます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "backup:UpdateGlobalSettings",
        "controltower:CreateLandingZone",

```

```

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

```


Note

Config 統合を有効にしてランディングゾーンバージョン 4.0 AWS にアップグレードする場合は、アクセスorganizations:ListDelegatedAdministrators許可が必要です。

ステップ 2: AWS Control Tower APIs

AWS Control Tower APIs を使用してランディングゾーンを起動できます。このセクションでは、必要なランディングゾーンマニフェストファイルを作成し、CreateLandingZoneAPI オペレーションで使用する方法について説明します。

マニフェストファイルの作成

マニフェストファイルは、ランディングゾーン設定を指定する JSON ドキュメントです。ランディングゾーンバージョン 4.0 では、多くのコンポーネントがオプションとなり、より柔軟なデプロイが可能になりました。

マニフェスト構造

以下は、使用可能なすべての設定を含むマニフェストファイルの完全な構造です。

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

```

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

```

重要な注意事項

- マニフェストにはすべてのenabledフラグが必要です。
- AWS Config 統合 ("config.enabled": false) を無効にする場合は、次の統合も無効にする必要があります。
 - セキュリティロール ("securityRoles.enabled": false)
 - アクセス管理 ("accessManagement.enabled": false)

- バックアップ ("backup.enabled": false)
- アカウント IDsは有効な 12 桁の AWS アカウント IDsである必要があります。
- KMS キー ARNs は有効な AWS KMS キー ARNsである必要があります。
- 保持期間は 1 日以上である必要があります。

CreateLandingZone API の使用

API を使用してランディングゾーンを作成するには:

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

API はランディングゾーン作成の進行状況を追跡するために使用できるランディングゾーンオペレーション ID を返します。レスポンス例:

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

、SUCCEEDED、または のステータスを返す GetLandingZoneOperation API を使用してFAILED、オペレーションのステータスをモニタリングできますIN_PROGRESS。

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

ランディングゾーンバージョン 4.0 での変更点

マニフェストの構造と要件の重要な変更:

- 組織構造
 - organizationStructure 定義がマニフェストから削除されました

- 顧客が独自の組織構造を定義できるようになりました
- 要件のみ: サービス統合アカウントは、ルートの下にある同じ OU 内に存在する必要があります
- 有効なフラグ
 - すべてのサービス統合設定には、必須フィールドとなる `enabled` フラグがあります。
 - お客様は常にブール値を指定する必要があります。デフォルト値は指定されません。
 - お客様は、マニフェストの各サービス統合設定を明示的に有効化/無効化する必要があります。
 - `accessManagement`
 - `backup`
 - `centralizedLogging`
 - `config`
 - `securityRoles`
- セキュリティロール
 - セキュリティロールの統合がオプションになりました
 - `securityRoles` デプロイを管理するために導入された新しい `enabled` フラグ
 - 無効にすると、関連するセキュリティ機能は実装されません
- AWS Config 統合
 - 新しい AWS Config サービス統合セクションが、次のフィールド `config` とともに マニフェストに追加されました。
 - `enabled`: AWS Config 統合デプロイを管理するために必要なブールフラグ
 - `accountId`: AWS Config アグリゲータの AWS アカウント ID
 - 設定:
 - `accessLoggingBucket.retentionDays`: アクセスログの保持期間
 - `loggingBucket.retentionDays`: AWS Config ログの保持期間
 - `kmsKeyArn`: 暗号化用の KMS キー

ランディングゾーンを特定する

`ListLandingZones` を呼び出すと、アカウントに既に AWS Control Tower が設定されているかどうかを確認できます。この API は、ランディングゾーンのホームリージョンに関係なく、すべての商業リージョンにわたって 1 つのランディングゾーン識別子 (ARN) を返します。ランディング

ゾーン ARN は特定リージョンごとに異なります。

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

[オブテインリージョン](#)の場合、ListLandingZones API は、API のホームリージョンと同じリージョンで呼び出された場合にのみランディングゾーン識別子を返します。例えば、ランディングゾーンが af-south-1 にセットアップされている場合に、af-south-1 で ListLandingZones を呼び出すと、API はランディングゾーン識別子を返します。ランディングゾーンが af-south-1 にセットアップされている場合に、ap-east-1 で ListLandingZones を呼び出すと、API はランディングゾーン識別子を返しません。

出力:

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

ランディングゾーンを更新する

新しいランディングゾーンバージョンが利用可能になった場合や、ランディングゾーン設定にその他の更新を加える場合は、UpdateLandingZone API を呼び出して、更新されたランディングゾーンのマニフェストファイルを参照できます。この API は OperationIdentifier を返します。これを使用して GetLandingZoneOperation API を呼び出し、更新オペレーションのステータスを確認できます。

ランディングゾーンを更新するには

1. AWS Control Tower の UpdateLandingZone API を呼び出して、更新されたランディングゾーンバージョンまたは更新されたランディングゾーンのマニフェストを参照します。

```
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
```

リージョンと一元化されたログを使用した LandingZoneManifest.json ファイルの例:

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

```

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

```

出力:

```

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

```

- i** オプションで [Re-register OU] (OU の再登録) を使用してアカウントを更新する
 アカウント数が 1000 未満の登録済み AWS Control Tower OUs の場合、AWS Control Tower コンソールを使用してダッシュボードの OU ページにアクセスし、OU の再登録を選択してその OU のアカウントを更新できます。

ランディングゾーンをリセットしてドリフトを解決する

ランディングゾーンを作成するとき、ランディングゾーンとすべての組織単位 (OU)、アカウント、リソースは、選択したコントロールによって適用されるガバナンスルールに準拠します。ユーザーおよび組織のメンバーがランディングゾーンを使用する際、コンプライアンスステータスが変更されることがあります。これらの変更はドリフトと呼ばれます。

ランディングゾーンがドリフト状態かどうかを確認するには、GetLandingZone API を呼び出すことができます。この API は、ランディングゾーンのドリフトステータスとして DRIFTED または IN_SYNC を返します。

ランディングゾーン内のドリフトを解決するには、ResetLandingZone API を使用してランディングゾーンを元の設定にリセットできます。例えば、AWS Control Tower はデフォルトで IAM Identity Center を有効にして を管理できるようにします AWS アカウントが、IAM Identity Center を無効にして元のランディングゾーンパラメータを設定すると、 を呼び出すResetLandingZoneと IAM Identity Center の設定が無効になります。

ResetLandingZone API を使用できるのは、利用可能な最新のランディングゾーンバージョンを使用している場合のみです。GetLandingZone API を呼び出して、ランディングゾーンバージョンを利用可能な最新バージョンと比較できます。必要に応じて、「[ランディングゾーンを更新する](#)」を行うことで利用可能な最新バージョンをランディングゾーンで使用できます。これらの例では、バージョン 3.3 を最新バージョンとして使用しています。

1. GetLandingZone API を呼び出します。API がドリフトステータスとして DRIFTED を返した場合、ランディングゾーンはドリフト状態です。
2. ResetLandingZone API を呼び出して、ランディングゾーンを元の設定にリセットします。

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

出力:

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


Note

ランディングゾーンをリセットしても、ランディングゾーンバージョンは更新されません。ランディングゾーンバージョンの更新の詳細については、「[ランディングゾーンを更新する](#)」を参照してください。

ランディングゾーンのマニフェストファイルの詳細を表示する

AWS Control Tower ランディングゾーンマニフェストファイルは、AWS Control Tower リソースについて説明するテキストファイルです。以下のセクションでは、ランディングゾーンマニフェストファイルのエントリの詳細定義を示します。

ランディングゾーンスキーマの完全な例については、「[ランディングゾーンのスキーマ](#)」を参照してください。

governedRegions - 管理下に置かれるリージョン

- タイプ: 文字列のリスト
- 必須: いいえ
- 例:

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

organizationStructure - 組織内に作成するセキュリティおよびサンドボックス OU の名前を選択します

- タイプ: オブジェクト
- 必須: はい
- プロパティ:
- 例:
 - security - 1 つの必須プロパティ name を持つオブジェクト。String を渡します
 - sandbox - 1 つの必須プロパティ name を持つオブジェクト。String を渡します

```
"organizationStructure": {  
  "security": {  
    "name": "CORE"
```

```

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

```

centralizedLogging – の設定AWS CloudTrail

- タイプ: オブジェクト
- 必須: はい
- プロパティ:
 - accountId - はString、ログ記録リソースをデプロイするAWSアカウントを表します。
 - 設定 - 3 つのプロパティを持つ Object。
 - loggingBucket - 1 つのプロパティ retentionDays を持つオブジェクト。Number を渡します
 - accessLoggingBucket - 1 つのプロパティ retentionDays を持つオブジェクト。Number を渡します
 - kmsKeyArn - String (オプション)
 - 有効 - Boolean (オプション)
- 例:

```

"centralizedLogging": {
  "accountId": "222222222222",
  "configurations": {
    "loggingBucket": {
      "retentionDays": 60
    },
    "accessLoggingBucket": {
      "retentionDays": 60
    },
    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX"
  },
  "enabled": true
}

```

securityRoles - ログ記録リソースをデプロイする場所を選択します

- タイプ: オブジェクト
- 必須: はい
- プロパティ: accountId - ログ記録リソースをデプロイするAWSアカウントStringを表す。
- 例:

```
"securityRoles": {  
    "accountId": "333333333333"  
}
```

accessManagement – アクセス管理を有効にするには、whether を選択します

- タイプ: オブジェクト
- 必須: いいえ
- プロパティ: 有効 - ブール値
- 例:

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

backup – AWS Control Tower によるAWSバックアップの設定

- タイプ: オブジェクト
- 必須: いいえ
- プロパティ:
 - 設定 - 3 つのプロパティを持つ Object。
 - centralBackup - 1 つのプロパティ accountId を持つオブジェクト。String を渡します
 - backupAdmin - 1 つのプロパティ accountId を持つオブジェクト。String を渡します
 - kmsKeyArn - String (オプション)
 - 有効 - Boolean
- 例:

```
"backup": {  
    "configurations": {
```

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

ランディングゾーンオペレーションのステータスを表示する

ListLandingZoneOperations API を使用すると、ランディングゾーンに対してアクションを実行する AWS Control Tower オペレーションのステータスを表示できます。

この API オペレーションの詳細については、「[ListLandingZoneOperations](#)」を参照してください。

ListLandingZoneOperations

ListLandingZoneOperations の入出力の例。

この例は、パラメータなしで API を呼び出す方法を示しています。

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

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

```

        "status": "SUCCEEDED"
      },
      {
        "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
        "operationType": "CREATE",
        "status": "FAILED"
      }
    ]
  }
}

```

この例は、API を呼び出し、結果の最大数を指定する方法を示しています。

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

```

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
      "operationType": "CREATE",
      "status": "FAILED"
    }
  ],
  "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTW0nfb1Up_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wd14J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}

```

この例は、API を呼び出し、nextToken でページ分割された結果を取得する方法を示しています。

```

aws controltower --region us-east-1 list-landing-zone-operations --next-token
AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTW0nfb1Up_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wd14J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",

```

```

        "operationType": "DELETE",
        "status": "SUCCEEDED"
    },
    {
        "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
        "operationType": "CREATE",
        "status": "SUCCEEDED"
    },
    {
        "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
        "operationType": "CREATE",
        "status": "FAILED"
    }
]
}

```

この例は、フィルターを指定して API を呼び出す方法を示しています。

```

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

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

```

例: API のみを使用して AWS Control Tower ランディングゾーンを設定する

この例によるチュートリアルは、付随的なドキュメントです。説明、注意事項、および詳細については、「[Getting started with AWS Control Tower using APIs](#)」を参照してください。

前提条件

AWS Control Tower ランディングゾーンを作成する前に、組織、2 つの共有アカウント、いくつかの IAM ロールを作成する必要があります。このチュートリアルでは、CLI コマンドと出力の例とともに、これらのステップについて説明します。

ステップ 1. 組織と 2 つの必要なアカウントを作成します。

```
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"
```

ステップ 2. 必要な IAM ロールを作成します。

AWSControlTowerAdmin

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



```

        "Resource": "*"
    }
]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

```

AWSControlTowerCloudTrailRole

```

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

```

```
}
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

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

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file:///config_trust.json
aws iam attach-role-policy --role-name
AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

ステップ 3. アカウント ID を取得し、ランディングゾーンのマニフェストファイルを生成します。

次の例の最初の 2 つのコマンドは、ステップ 1 で作成したアカウントのアカウント ID を変数に保存します。これらの変数は、ランディングゾーンのマニフェストファイルを生成するのに役立ちます。

```
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
```

Step 4. 最新バージョンでランディングゾーンを作成します。

マニフェストファイルと最新バージョンでランディングゾーンを設定する必要があります。この例は、バージョン 3.3 を示しています。

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

次の例に示すように、出力には `arn` と `operationIdentifier` が含まれます。

```
{
  "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNU0L2AXXX",
  "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

ステップ 5. (オプション) ループを設定して、ランディングゾーン作成オペレーションのステータスを追跡します。

ステータスを追跡するには、前の `create-landing-zone` コマンドの出力にある `operationIdentifier` を使用します。

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

サンプルステータス出力:

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

次のサンプルスクリプトを使用すると、ログファイルのように、オペレーションのステータスを何度もレポートするループを設定できます。こうすれば、コマンドを繰り返し入力する必要はありません。

```
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
```

ランディングゾーンに関する詳細情報を表示するには

ステップ 1. ランディングゾーンの ARN を特定する

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

出力には、次の出力例に示すように、ランディングゾーンの識別子が含まれます。

```
{
  "landingZones": [
    {
      "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX"
    }
  ]
}
```

ステップ 2. 情報を取得する

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX
```

以下は、表示される出力の例です。

```
{
  "landingZone": {
    "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX",
    "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"  
}  
}
```

ステップ 6: (オプション) **ListLandingZoneOperations** API を呼び出して、ランディングゾーンを変更するオペレーションのステータスを表示します。

ランディングゾーンオペレーションのステータスを追跡するには、[ListLandingZoneOperations](#) API を呼び出します。

ランディングゾーンのスキーマ

ランディングゾーンは、スキーマによって作成される AWS リソースです。AWS Control Tower ランディングゾーンバージョンには、それぞれ一意のスキーマがあります。

AWS Control Tower ランディングゾーンのバージョン 3.1 以降のスキーマは、互換性のあるバージョンの選択に役立つように、このリファレンスセクションで公開されています。

Note

ランディングゾーンバージョン 3.0 には、不要なアクセスログ記録に関する既知の問題があります。この問題はランディングゾーンバージョン 3.1 で解決されています。変更の詳細については、「[AWS Control Tower ランディングゾーンバージョン 3.1](#)」を参照してください。

ランディングゾーン 4.0 スキーマ

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

```

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

```



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



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

```
        "type": "number",
        "minimum": 1,
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  },
  "SecurityRoles": {
    "type": "object",
    "required": [
      "enabled"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      },
      "enabled": {
        "type": "boolean",
        "additionalProperties": false
      }
    },
    "additionalProperties": false,
    "if": {
      "properties": {
        "enabled": {
          "const": true
        }
      }
    },
    "then": {
      "required": [
        "accountId"
      ]
    }
  },
  "Config": {
    "type": "object",
    "required": [
      "enabled"
    ],
```

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

```

        "additionalProperties": false
      }
    }
  }
}

```

ランディングゾーン 3.3 のスキーマ

```

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

```

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

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



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

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

```

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

```

ランディングゾーン 3.2 のスキーマ

```

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

```

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

```

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

```

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

```

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

```

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


ランディングゾーン 3.1 のスキーマ

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

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

```

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

```

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

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

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

CloudFormation を使用してランディングゾーンを起動する

ランディングゾーンは、CloudFormation コンソールまたは AWS CLI を通じて CloudFormation で設定および起動できます。このセクションでは、API を通じて CloudFormation でランディングゾーンを起動する手順と例を示します。

トピック

- [CloudFormation でランディングゾーンを起動するための前提条件](#)
- [CloudFormation を使用して新しいランディングゾーンを作成する](#)
- [CloudFormation を使用して既存のランディングゾーンを管理する](#)

CloudFormation でランディングゾーンを起動するための前提条件

1. AWS CLI から、AWS Organizations CreateOrganization API を使用して組織を作成し、すべての機能を有効にします。

詳細な手順については、「[ステップ 1: ランディングゾーンを設定する](#)」を参照してください。

2. CloudFormation コンソールまたは AWS CLI を使用して、CloudFormation テンプレートをデプロイし、管理アカウントに以下のリソースを作成します。
 - ログアーカイブアカウント (「ログ記録」アカウントと呼ばれることもあります)
 - 監査アカウント (「セキュリティ」アカウントと呼ばれることもあります)

- AWSControlTowerAdmin、AWSControlTowerCloudTrailRole、AWSControlTowerConfigAggregatorRole および AWSControlTowerStackSetRole サービスロール。

AWS Control Tower がこれらのロールを使用してランディングゾーン API コールを実行する方法については、「[ステップ 1: ランディングゾーンを設定する](#)」を参照してください。

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
```

CloudFormation を使用して新しいランディングゾーンを作成する

CloudFormation コンソールまたは AWS CLI を使用し、次の CloudFormation テンプレートをデプロイしてランディングゾーンを作成します。

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: Array
    Description: List of governed regions
  SecurityOunName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOunName:
    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
```

CloudFormation を使用して既存のランディングゾーンを管理する

CloudFormation を使用して、新規または既存の CloudFormation スタックにランディングゾーンをインポートすることで、既に起動しているランディングゾーンを管理できます。詳細と手順については、「[既存リソースを CloudFormation 管理に取り込む](#)」を参照してください。

[AWS Control Tower でドリフトを検出および解決する](#)には、AWS Control Tower コンソール、AWS CLI、または [ResetLandingZone API](#) を使用できます。

次の手順

これで、ランディングゾーンがセットアップされ、使用する準備ができました。

AWS Control Tower の使用方法の詳細については、次のトピックを参照してください。

- 推奨される管理方法については、「[ベストプラクティス](#)」を参照してください。
- 特定のロールと許可を持つ IAM Identity Center ユーザーとグループをセットアップできます。推奨事項については、「[グループ、ロール、ポリシーを設定する上での推奨事項](#)」を参照してください。
- AWS Organizations デプロイから組織とアカウントの登録を開始するには、「[既存の組織とアカウントの管理](#)」を参照してください。
- エンドユーザーは Account Factory を使用してランディングゾーン AWS に独自のアカウントをプロビジョニングできます。詳細については、「[アカウントの設定とプロビジョニングのためのアクセス許可](#)」を参照してください。
- [AWS Control Tower のコンプライアンス検証](#) を確保するために、中央クラウド管理者はログアーカイブアカウントのログアーカイブを確認できます。また、指定されたサードパーティー監査人はセキュリティ OU のメンバーである監査 (共有) アカウントの監査情報を確認できます。
- AWS Control Tower の機能の詳細については、「[関連情報](#)」を参照してください。
- 場合によっては、最新のバックエンド更新プログラムと最新のコントロールを入手してランディングゾーンを最新の状態に維持するために、ランディングゾーンを更新する必要があります。詳細については、「[AWS Control Tower での設定更新管理](#)」を参照してください。
- AWS Control Tower の使用中に問題が発生した場合は、「[トラブルシューティング](#)」を参照してください。

⚠ Important

アカウントのルートユーザーの MFA をまだ有効にしていない場合は、すぐに有効にしてください。ルートユーザーのベストプラクティスの詳細については、「[アカウントのルートユーザーを保護するためのベストプラクティス](#)」を参照してください。

AWS Control Tower の制限とクォータ

この章では、AWS Control Tower を使用する際に留意すべき AWS サービスの制限とクォータについて説明します。サービスクォータの問題によりランディングゾーンをセットアップできない場合は、[AWS サポート](#) にお問い合わせください。

コントロール固有の制限の詳細については、「[コントロールの制限事項](#)」を参照してください。

Controls Reference Guide

AWS Control Tower のコントロールに関する詳細情報は、「[AWS Control Tower Controls Reference Guide](#)」に移動されました。

AWS Control Tower の既知の制限事項

このセクションでは、AWS Control Tower の既知の制限事項とサポートされていないユースケースについて説明します。

- AWS Control Tower には全体的な同時実行数の制限があります。通常、一度に実行できるオペレーション数は 1 つです。この制限には次の 2 つの例外があります。
- オプションのコントロールは、非同期プロセスを通じて同時にアクティブ化および非アクティブ化できます。呼び出し元がコンソールか API に関係なく、一度に合計最大 100 のコントロール関連オペレーションを実行できます。
- アカウントは、非同期プロセスを通じて Account Factory で同時にプロビジョニング、更新、登録でき、アカウント関連のオペレーションは同時に 5 つまで実行できます。アカウントの管理を解除するには、一度に 1 つのアカウントを実行する必要があります。
- Account Factory for Terraform (AFT) には、デプロイ中に追加の同時実行パラメータが設定されています。AWS は、次のデフォルト値を使用して AFT をテストしています。
 - `concurrent_account_factory_actions`: 5 (アカウントのプロビジョニング)
 - `maximum_concurrent_customizations`: 5 (カスタマイズパイプライン)

これらの制限をテスト済みのデフォルトを超えて増やすと、安定性が低下する可能性があります。

- セキュリティ OU の共有アカウントの E メールアドレスは変更できますが、これらの変更を AWS Control Tower コンソールで確認するには、ランディングゾーンを更新する必要があります。

- AWS Control Tower ランディングゾーンの OU には、OU あたり 5 個の SCP という制限が適用されます。
- AWS Control Tower は、ランディングゾーンの組織で、すべての OU 間で分けられたアカウントを最大 10,000 個までサポートします。
- 直接ネストされたアカウントの数が 1000 を超える既存の OU は、AWS Control Tower に登録または再登録することはできません。OU の登録に伴う制限の詳細については、「[基盤となる AWS サービスに基づく制限](#)」を参照してください。
- 一部の依存関係は使用できないため AWS リージョン、AWS Control Tower (CfCT) のカスタマイズはこれらでは使用できません。
 - 欧州 (チューリッヒ) eu-central-2
 - 欧州 (スペイン) eu-south-2
 - カナダ西部 (カルガリー) ca-west-1
 - アジアパシフィック (メルボルン) ap-southeast-4
 - アジアパシフィック (マレーシア)、ap-southeast-5
 - アジアパシフィック (タイ)、ap-southeast-7
 - メキシコ (中部)、mx-central-1

CfCT を AWS Control Tower のホームリージョンにデプロイする場合、CfCT を使用してこれらのリージョンにリソースをデプロイおよび管理できますが、これらのリージョンに CfCT を構築することはできません。

- 一部の依存関係は使用できないため AWS リージョン、AWS Control Tower Account Factory for Terraform (AFT) は以下では利用できません。
 - 欧州 (チューリッヒ) eu-central-2
 - 欧州 (スペイン) eu-south-2
 - カナダ西部 (カルガリー)、ca-west-1
 - アジアパシフィック (メルボルン) ap-southeast-4
 - アジアパシフィック (マレーシア)、ap-southeast-5
 - アジアパシフィック (タイ)、ap-southeast-7
 - メキシコ (中部)、mx-central-1
- サードパーティーのバージョン管理システム (VCS) への接続には AWS CodeConnections 接続を使用できないため、AFT の新規のお客様が AWS Control Tower Account Factory for Terraform (AFT) を以下のリージョンにデプロイすることはできません。

- アジアパシフィック (香港)、アフリカ (ケープタウン)、中東 (バーレーン)、欧州 (チューリッヒ)、アジアパシフィック (ジャカルタ)、アジアパシフィック (ハイデラバード)、アジアパシフィック (大阪)、アジアパシフィック (メルボルン)、イスラエル (テルアビブ)、欧州 (スペイン)、中東 (アラブ首長国連邦)、アジアパシフィック (タイ)、メキシコ (中部)
- 以下のリージョンは AWS Service Catalog をサポートしていません。
 - カナダ西部 (カルガリー)、ca-west-1
 - アジアパシフィック (マレーシア)、ap-southeast-5
 - アジアパシフィック (タイ)、ap-southeast-7
 - メキシコ (中部)、mx-central-1

Note

Service Catalog をサポートしていないリージョンは、Account Factory Customizations for AWS Control Tower (AFC) をサポートしていません。

サポートされていないリージョンの AWS Control Tower 機能の詳細については AWS Service Catalog、「 [」を参照してください](#)[AWS Control Tower が AWS カナダ西部 \(カルガリー\) で利用可能に。](#)

- コントロール API を呼び出してコントロールをアクティブ化または非アクティブ化する場合、AWS Control Tower での EnableControl と DisableControl の更新の同時オペレーションの上限は 100 です。10 個のオペレーションを同時に実行でき、残りのオペレーションはキューに入れます。完了するまでコードを調整する必要がある場合があります。
- Terraform をベースにしたブループリントを使用して、Account Factory Customizations (AFC) でアカウントをプロビジョニングする場合、それらのブループリントは 1 つの AWS リージョンにしかなデプロイできません。デフォルトでは、AWS Control Tower はホームリージョンにデプロイします。

クォータ引き上げをリクエストする

Service Quotas コンソールは、AWS Control Tower のクォータに関する情報を提供します。Service Quotas コンソールを使用して、デフォルトのサービスクォータを表示したり、調整可能なクォータの[クォータの引き上げをリクエスト](#)したりすることができます。

Note

新しく作成されたアカウントや Organizations では、デフォルトの 10 アカウントを下回るクォータが発生する可能性があります。

Service Quotas コンソールから次のクォータを表示できます

- 同時アカウントオペレーションのクォータ: 同時に実行できる同時アカウントオペレーションの最大数。デフォルト: 5、最大: 10、調整可能
- 1 つの OU 内のアカウント数: 1 つの OU に存在することができる AWS Control Tower 管理アカウントの最大数。この上限を超えるアカウントを追加すると、AWS Control Tower での OU 登録プロセスは実行できません。OU あたりのアカウント数の詳細については、AWS Control Tower ドキュメントの「[基盤となる AWS サービスに基づく制限](#)」を参照してください。デフォルト: 1000、調整不可。
- 組織単位 (OU) の同時オペレーション: 同時に実行できる OU 関連の同時オペレーションの最大数。デフォルト: 1、調整不可。

例えば、アカウント関連の同時オペレーションのクォータを 5 から 10 に引き上げるようにリクエストできます。AWS Control Tower の一部のパフォーマンス特性がクォータの引き上げ後に変化する場合があります。たとえば、OU のアカウント数が多いと、OU の更新に時間がかかることがあります。または、SCP が 5 つある OU でのアクションの完了には、SCP が 3 つある場合よりも時間がかかる可能性があります。

Note

サービスクォータの引き上げリクエストは、実行されるまでに最大 2 日かかる場合があります。クォータの引き上げは、必ず AWS Control Tower のホームリージョンからリクエストしてください。

別の方法として、[AWS サポート](#)に連絡し、AWS Control Tower の一部のリソースについてクォータの引き上げをリクエストすることもできます。または、以下のビデオを見て、特定のサービスクォータの引き上げを自動化する方法を確認することもできます。

ビデオ: AWS Control Tower に関連するサービスでのサービスクォータ引き上げのリクエストを自動化する

この動画 (7:24) では、AWS Control Tower でのデプロイに基づいて、関連する統合 AWS サービスのサービスクォータの増加を自動化する方法について説明します。また、組織の AWS エンタープライズサポートへの新しいアカウントの登録を自動化する方法も示します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower でのクォータの引き上げに関する動画チュートリアル。](#)

この環境で新しいアカウントをプロビジョニングしているときに、ライフサイクルイベントを使用して、指定された AWS リージョンでのサービスクォータ引き上げの自動リクエストをトリガーできます。

AWS クォータの詳細については、[AWS 全般のリファレンス](#)を参照してください。

コントロールの制限事項

AWS Control Tower は、サービスコントロールポリシー (SCPs)、AWS Config ルール、CloudFormation フックなど、さまざまな形式で実装されるコントロール AWS を使用して、で安全なマルチアカウント環境を維持するのに役立ちます。

Controls Reference Guide

AWS Control Tower のコントロールに関する詳細情報は、「[AWS Control Tower Controls Reference Guide](#)」に移動されました。

SCP などの AWS Control Tower リソースを変更したり、Config レコーダーやアグリゲータなどの AWS Config リソースを削除したりすると、AWS Control Tower はコントロールが設計どおりに機能することを保証できなくなります。このため、マルチアカウント環境のセキュリティが危険にさらされる可能性があります。セキュリティ AWS [の責任共有モデルは](#)、お客様が行う可能性のある変更に応用されます。

Note

AWS Control Tower は、ランディングゾーンを更新したときに予防コントロールの SCP を標準設定にリセットすることで、環境の完全性が維持されるように支援します。SCP に加えられた可能性がある変更は、設計により、標準バージョンのコントロールに置き換えられます。

リージョン別の制限事項

AWS Control Tower の一部のコントロールは、AWS Control Tower が利用可能な特定の AWS リージョン 場所で動作しません。これらのリージョンは、必要な基盤となる機能をサポートしていないためです。したがって、そのコントロールをデプロイしても、AWS Control Tower で管理しているすべてのリージョンで動作しない可能性があります。この制限は、Security Hub CSPM Service-managed Standard: AWS Control Tower の特定の検出コントロール、特定のプロアクティブコントロール、および特定のコントロールに影響します。リージョン別の利用可能性の詳細については、「[Security Hub controls](#)」を参照してください。また、[リージョンサービスリストドキュメント](#)と[Security Hub CSPM コントロールリファレンスドキュメント](#)も参照してください。

混合ガバナンスの場合、コントロールの動作も制限されます。詳細については、「[リージョンを設定する際は混合ガバナンスを避ける](#)」を参照してください。

AWS Control Tower がリージョンとコントロールの制限を管理する方法の詳細については、「[AWS オプトインリージョンをアクティブ化する際の考慮事項](#)」を参照してください。

Note

コントロールとリージョンのサポートに関する最新情報については、[GetControl](#) および [ListControls](#) API オペレーションを呼び出すことをお勧めします。

使用可能なコントロールとリージョンを確認する

各コントロールの使用可能なリージョンは、AWS Control Tower コンソールで表示できます。AWS Control Catalog の [GetControl](#) および [ListControls](#) APIs を使用して、利用可能なリージョンをプログラムで表示できます。

特定の でサポートされていないサービスマネージドスタンダード: AWS Control Tower の AWS Security Hub CSPM コントロールについては AWS リージョン、[Security Hub CSPM 標準の](#)「サポートされていないリージョン」を参照してください。

基盤となる AWS サービスに基づく制限

このページでは、他の AWS サービスの制限が原因で生じる可能性のある制限と、AWS Control Tower がそれらのサービスとどのように連携するかについて説明します。

一般的なガイドライン

原則として、OU の登録時にサポートされるアカウントの数は、その OU に対して管理されるリージョンの数と有効なコントロールの数が増えるにつれて減少すると予想されます。これらの一般的なガイドラインは、15 個のオプションコントロールが有効になっていることを前提としています。OU で有効になっているコントロールの数がそれより多くても少なくても、登録時の OU あたりのアカウント数の上限は異なります。

- 管理対象リージョン数が 15 である場合、最大 1000 のアカウントを持つ OU がサポートされます。
- 管理対象リージョン数が 16～21 である場合、サポートされる OU の最大サイズは 600～1000 アカウントの範囲です。
- 管理対象リージョン数が 22 である場合、最大 680 のアカウントを持つ OU がサポートされます。
- 管理対象リージョン数が 23 以上である場合、サポートされる OU の最大サイズは 680 アカウント未満です。

エラーが発生した場合

登録に失敗した場合は、OU を再登録できます。また、ネストされた OU を使用するか、別の OU にアカウントを移動することで、OU を小さくすることもできます。

Note

AWS Control Tower が常に適用する必須コントロールは、登録の目的で OU で有効にしたコントロールの数にはカウントされません。

CloudFormation スタックセットの制限

複数の にまたがって多数のアカウントを登録する予定の場合 AWS リージョン、組織の全体的なサイズに対して CloudFormation スタックセットによって制限が発生することがあります。次の計算式で制限を見積もることができます。

組織内の管理されたアカウントの数 x 管理対象リージョンの数 $\leq$ 150,000

この制限は、OU の登録プロセスで表面化します。例えば、15 のリージョンが管理され、15 のオプションコントロールが有効になっている場合、OU 登録の上限は 1000 アカウントです。しかし、1000 を超えるアカウントを持つ OU を登録する必要がある場合、または多数のオプションコントロールを有効にしている場合は、管理対象リージョンの数を 15 未満に減らす必要があります。この減少は、スタックセットの制限によるものです。

AWS Config 制限事項

多数のアカウントで OUs を登録する場合、すべてのアグリゲータで[毎週 が作成または削除 AWS Config できるアカウントの最大数](#)に制限が発生することがあります。登録済みアカウントはこの制限にカウントされません。毎週最大 1000 の新しいアカウントを AWS Control Tower に登録できます。

アカウントとオプトインリージョンに関する初回の制限事項

複数のオプトインリージョンにまたがる多数のアカウントを持つ OU を初めて登録する場合、[アカウント管理クォータ](#) による制限が生じ、レイテンシーが長くなることがあります。レイテンシーが原因で OU 登録中にエラーが発生する可能性があります。

AWS Control Tower 機能のリージョン間の違い

AWS Control Tower は他の AWS サービスの動作を調整するため AWS リージョン、AWS Control Tower の動作には特定の違いがあります。例えば、次のようになります。

- AWS Service Catalog は、AWS Control Tower が利用可能なすべての AWS リージョン で利用できるわけではなく、それらのリージョンでの Account Factory の動作が変更されます。
- 一部のリージョンでは、ブループリントの基盤となる機能をサポートする Service Catalog が使用できないため、Account Factory Customizations (AFC) を使用できません。
- 基盤となる機能がないため AWS リージョン 、一部のコントロールはすべての で利用できるわけではありません。
- AFT と CfCT は、基盤となる機能がないため、すべての AWS リージョン で利用できるわけではありません。

AWS Control Tower 環境の動作を的確に判断するには、ホームリージョンを確認します。次に、以下の項目を評価します。詳細については、「[Limitations and quotas in AWS Control Tower](#)」を参照してください。

- 希望するホームリージョンで AWS Service Catalog 利用できますか？
- 必要なコントロールを使用できるか？「[Control limitations](#)」を参照してください。
- 目的のホームリージョンで IAM アイデンティティセンターを使用できるか？

コントロールのデプロイ可能なリージョン

AWS Control Tower は、基盤となる依存関係がないため、特定のリージョンにデプロイするときに特定のコントロールをアクティブ化できません。ListControls および GetControl API を呼び出して、任意のコントロールのデプロイ可能なリージョンに関する最新情報を確認できます。AWS Control Tower コンソールでデプロイ可能なリージョンを表示することもできます。

AWS Control Tower によって管理される OU でコントロールをアクティブ化する場合、コントロールの影響領域は、AWS Control Tower によって管理されるリージョンとコントロールのデプロイ可能なリージョンの共通部分です。

例えば、コントロールは、管理対象リージョン X、Y、Z で動作する OU で有効化できます。ただし、有効化すると、コントロール自体がリージョン Y をサポートしていないため、同じコントロールはリージョン X と Z にのみデプロイされます。

AWS リソースの保護にギャップが発生しないように、デプロイするコントロールと AWS Control Tower でワークロードを運用するリージョン間の関係をモニタリングすることが重要です。

保護されたリージョンを確認する方法

- AWS Control Tower コンソールでは、有効化されたコントロールセクションで有効化されたコントロールとリージョンを表示できます。
- GetEnabledControl API を呼び出すと、targetRegions パラメータには、デプロイ不可能なリージョンではなく、コントロールを効果的にデプロイできるリージョンのみが表示されます。

AWS Control Tower Controls Reference Guide

AWS Control Tower のコントロールに関する詳細情報は、「[AWS Control Tower Controls Reference Guide](#)」に移動されました。

AWS Control Tower 管理者向けのベストプラクティス

このトピックは、主に管理アカウントの管理者を対象としています。

管理アカウントの管理者には、AWS Control Tower のコントロールによってメンバーアカウント管理者が実行できなくなるタスクについて説明する責任があります。このトピックでは、この知識を伝えるためのベストプラクティスと手順について説明し、AWS Control Tower 環境を効率的に設定して維持するためのその他のヒントを示します。

アクセスについてユーザーに説明する

AWS Control Tower コンソールは、管理アカウントの管理者権限を持つユーザーだけが使用できます。それらのユーザーだけが、ランディングゾーン内で管理作業を実行できます。これは、ベストプラクティスに従って、ほとんどのユーザーとメンバーアカウント管理者に AWS Control Tower コンソールが表示されることがないことを意味します。管理アカウントの管理者グループのメンバーは、必要に応じて、ユーザーとメンバーアカウントの管理者に次の情報を説明する必要があります。

- ユーザーと管理者がランディングゾーン内でアクセスできる AWS リソースについて説明します。
- 他の管理者がそれに応じて AWS ワークロードを計画して実行できるように、各組織単位 (OU) に適用される予防コントロールを一覧表示します。

リソースアクセスについて説明する

一部の管理者および他のユーザーは、ランディングゾーン内でアクセスできる AWS リソースの説明が必要になる場合があります。このアクセスには、プログラムによるアクセスとコンソールベースのアクセスが含まれます。一般的に、AWS リソースの読み取りアクセスと書き込みアクセスが許可されます。内で作業を実行するには AWS、ユーザーがジョブを実行するために必要な特定のサービスにある程度のアクセスが必要です。

AWS 開発者などの一部のユーザーは、エンジニアリングソリューションを作成できるように、アクセスできるリソースについて知っておく必要がある場合があります。AWS サービスで実行されるアプリケーションのエンドユーザーなどの他のユーザーは、ランディングゾーン内の AWS リソースについて知る必要はありません。

AWS には、ユーザーの AWS リソースアクセスの範囲を特定するためのツールが用意されています。ユーザーのアクセスの範囲を特定したら、組織の情報管理ポリシーに従って、その情報をユーザーと共有できます。これらのツールの詳細については、以下のトピックを参照してください。

- AWS アクセスアドバイザー – AWS Identity and Access Management (IAM) アクセスアドバイザー ツールを使用すると、ユーザー、ロール、グループなどの IAM エンティティが AWS サービスを呼び出したときの最後のタイムスタンプを分析することで、デベロッパーが持つアクセス許可を判断できます。サービスアクセスを監査して不要な許可を削除したり、必要に応じてプロセスを自動化したりできます。詳細については、[AWS セキュリティブログ記事](#)を参照してください。
- IAM Policy Simulator - IAM Policy Simulator では、IAM およびリソースベースのポリシーをテストし、トラブルシューティングできます。詳細については、「[IAM Policy Simulator を使用した IAM ポリシーのテスト](#)」を参照してください。
- logsAWS CloudTrail – AWS CloudTrail ログを確認して、ユーザー、ロール、またはによって実行されたアクションを確認できます AWS のサービス。CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

AWS Control Tower ランディングゾーン管理者が実行したアクションは、ランディングゾーン管理アカウントで確認できます。メンバーアカウント管理者およびユーザーが実行したアクションは、共有ログアーカイブアカウントで確認できます。

AWS Control Tower イベントのサマリーテーブルは、[\[Activity\]](#) (アクティビティ) ページで確認できます。

予防コントロールについて説明する

予防コントロールにより、組織のアカウントが企業ポリシーへの準拠を維持できるようになります。予防コントロールのステータスは、適用または無効です。予防コントロールは、サービスコントロールポリシー (SCP)、リソースコントロールポリシー (RCP)、または宣言型ポリシーを使用して、ポリシー違反を防止します。これに対して、検出コントロールは、定義された AWS Config ルールを使用して、存在するさまざまなイベントまたは状態を通知します。

AWS 開発者などの一部のユーザーは、エンジニアリングソリューションを作成できるように、使用するアカウントや OUs に適用される予防コントロールについて知っておく必要がある場合があります。次の手順では、組織の情報管理ポリシーに従って、適切なユーザーにこの情報を提供する方法に関するガイダンスを示します。

Note

この手順では、ランディングゾーン内に少なくとも 1 つの子 OU と少なくとも 1 人の AWS IAM アイデンティティセンター ユーザーがすでに作成されていることを前提としています。

例: 知っておく必要があるユーザーに予防コントロールを示すには

1. <https://console.aws.amazon.com/controltower/> で AWS Control Tower コンソールにサインインします。
2. 左側のナビゲーションから、[Organization] (組織) を選択します。
3. 表から、該当するコントロールに関してユーザーが情報を必要としているいずれかの OU の名前を選択します。
4. OU の名前と、この OU に適用されるコントロールを書き留めます。
5. ユーザーが情報を必要としている OU ごとに、前の 2 つのステップを繰り返します。

コントロールとその機能の詳細については、「[About controls in AWS Control Tower](#)」を参照してください。

AWS Control Tower ランディングゾーンの計画

セットアッププロセスを完了すると、AWS Control Tower によって、ランディングゾーンと呼ばれる、アカウントに関連付けられたリソースが起動されます。このリソースは、組織とそのアカウントのホームとして機能します。

Note

組織ごとに 1 つのランディングゾーンをセットアップできます。

ランディングゾーン計画とセットアップ時に従うベストプラクティスについては、「[AWS AWS Control Tower ランディングゾーンのマルチアカウント戦略](#)」を参照してください。

AWS Control Tower をセットアップする方法

既存の組織に AWS Control Tower ランディングゾーンをセットアップすることも、AWS Control Tower ランディングゾーンが含まれる新しい組織を作成することから始めることもできます。

- [既存の組織での AWS Control Tower の起動](#): このセクションは、既存の が AWS Control Tower によってガバナンスを開始する AWS Organizations 準備ができているお客様を対象としています。
- [新しい組織での AWS Control Tower の起動](#): このセクションは AWS Organizations、既存の、OUs。

 Note

ラン AWS Organizations デイニングゾーンがすでにある場合は、AWS Control Tower ガバナンスを既存のランディングゾーンから組織内の既存の OUs とアカウントの一部またはすべてに拡張できます。「[既存の組織とアカウントの管理](#)」を参照してください。

機能の比較

ここでは、AWS Control Tower を既存の組織に追加する場合と、AWS Control Tower ガバナンスを OU およびアカウントに拡張する場合の違いを簡単に比較します。また、AWS ランディングゾーンソリューションから AWS Control Tower に移行する場合は、いくつかの特別な考慮事項が適用されます。

既存の組織への追加について: 既存の組織への AWS Control Tower の追加は、AWS コンソール内で行うことができます。この場合、AWS Organizations サービスで作成した組織がすでにあり、その組織は現在 AWS Control Tower に登録されておらず、後でランディングゾーンを追加する必要があります。

ランディングゾーンを既存の組織に追加すると、AWS Control Tower は AWS Organizations レベルで並列構造を設定します。既存の組織内の OU とアカウントは変更しません。

ガバナンスの拡張について: ガバナンスの拡張は既に AWS Control Tower に登録されている 1 つの組織内にある特定の OU とアカウントに適用されます。つまり、その組織にはランディングゾーンが既に存在していることになります。ガバナンスの拡張とは、登録済みの組織内にある特定の OU とアカウントに制約が適用されるように AWS Control Tower コントロールを拡張することです。この場合、新しいランディングゾーンを起動するのではなく、組織の現在のランディングゾーンを拡張するだけです。

 Important

特別な考慮事項: 現在の [AWS Landing Zone ソリューション \(ALZ\)](#) を使用している場合は AWS Organizations、組織で AWS Control Tower を有効にする前に、AWS ソリューションアーキテクトに確認してください。AWS Control Tower は、AWS Control Tower がランディングゾーンの現在のデプロイと干渉する可能性があるかどうかを判断する事前チェックを実行できません。詳細については、「[チュートリアル: ALZ から AWS Control Tower に移行する](#)」を参照してください。また、ランディングゾーン間でのアカウントの移動については、「[アカウントが前提条件を満たしていない場合](#)」を参照してください。

既存の組織での AWS Control Tower の起動

既存の組織で AWS Control Tower ランディングゾーンを設定することで、既存の AWS Organizations 環境と並行してすぐに作業を開始できます。内に作成された他の OUs AWS Organizations は AWS Control Tower に登録されていないため、変更されません。これらの OU とアカウントは、そのまま使用できます。

AWS Control Tower は、その管理アカウントとして既存の組織の管理アカウントを使用して統合を図ります。新しい管理アカウントは不要です。既存の管理アカウントから AWS Control Tower ランディングゾーンを起動できます。

Note

既存の組織で AWS Control Tower をセットアップするには、サービスの制限により、少なくとも 2 つの追加のアカウントの作成が許可されている必要があります。

AWS Control Tower を既存の組織に追加した場合の影響

AWS Control Tower は、組織に 2 つのアカウント (監査アカウントとログ記録アカウント) を作成します。これらのアカウントは、チームが行ったアクションの記録を個々のエンドユーザーアカウントに保持します。[Audit] (監査) アカウントと [Log archive] (ログアーカイブ) アカウントは、AWS Control Tower ランディングゾーン内の [Security] (セキュリティ) OU に表示されます。

ランディングゾーンを設定すると、AWS Control Tower によって追加されたアカウントは既存の一部になり AWS Organizations、既存の組織の請求の一部になります。

機能の概要

既存の AWS Organizations 組織で AWS Control Tower を有効にすると、組織にいくつかの主要な機能強化がもたらされます。

- AWS Control Tower によって追加されたアカウントは既存の組織の一部になるため、組織のグループ全体で一括請求が可能になります。
- これにより、OU の 1 つの管理アカウントからすべてのアカウントを管理できます。
- また、既存のアカウントと新しいアカウントにセキュリティとコンプライアンスに関するコントロールを適用する方法がシンプルになります。

⚠ Important

既存の AWS Organizations 組織で AWS Control Tower ランディングゾーンを起動しても、その組織から AWS Control Tower に登録されていない他の OUs またはアカウントに AWS Control Tower ガバナンスを拡張することはできません。

既存の組織で AWS Control Tower を起動するには、「[AWS Control Tower の使用開始方法](#)」で説明されているプロセスに従います。

AWS Control Tower が既存の AWS Organizations 組織とやり取りする方法の詳細については、「」を参照してください[AWS Control Tower で組織とアカウントを管理する](#)。

新しい組織での AWS Control Tower の起動

AWS Control Tower を初めて使用し、まだ使用していない場合は AWS Organizations、[セットアップ](#) ドキュメントから始めることをお勧めします。

AWS Control Tower は、組織がまだセットアップされていない場合には自動的にセットアップします。

AWS AWS Control Tower ランディングゾーンのマルチアカウント戦略

AWS Control Tower のお客様は、最良の結果を得るために AWS 環境とアカウントを設定する方法についてのガイダンスを求められることがよくあります。AWS は、AWS Control Tower ランディングゾーンを含む AWS リソースを最大限に活用できるように、マルチアカウント戦略と呼ばれる統合された推奨事項のセットを作成しました。

基本的に、AWS Control Tower は他の AWS サービスと連携するオーケストレーションレイヤーとして機能し、AWS アカウントと の AWS マルチアカウントレコメンデーションを実装するのに役立ちます AWS Organizations。AWS Control Tower は、ランディングゾーンをセットアップした後も、複数のアカウントとワークロードにわたって企業のポリシーとセキュリティプラクティスを維持する場合に役立ちます。

ほとんどのランディングゾーンは時間の経過と共に拡大します。AWS Control Tower ランディングゾーン内の組織単位 (OU) とアカウントの数が増加するのに合わせて、ワークロードを効果的に編成できるように AWS Control Tower のデプロイを拡張できます。この章では、AWS マルチアカウン

ト戦略に沿って AWS Control Tower ランディングゾーンを計画およびセットアップし、時間の経過と共に拡張する方法について規範的なガイダンスを提供します。

組織単位のベストプラクティスに関する一般的な説明については、「[を使用した組織単位のベストプラクティス AWS Organizations](#)」を参照してください。

AWS マルチアカウント戦略: ベストプラクティスガイダンス

AWS 適切に設計された環境の ベストプラクティスでは、リソースとワークロードを複数の AWS アカウントに分割することをお勧めします。AWS アカウントは独立したリソースコンテナと考えることができます。ワークロードを分類する機能と、問題が発生した場合の影響範囲を小さくする機能を備えています。

AWS アカウントの定義

AWS アカウントは、リソースコンテナとリソース分離の境界として機能します。

Note

AWS アカウントは、フェデレーションまたは AWS Identity and Access Management (IAM) を介して設定されたユーザーアカウントとは異なります。

AWS アカウントの詳細

AWS アカウントは、リソースを分離し、AWS ワークロードのセキュリティ脅威を封じ込める機能を提供します。また、請求のメカニズムと、ワークロード環境を管理するためのメカニズムも備えています。

AWS アカウントは、ワークロードにリソースコンテナを提供するための主要な実装メカニズムです。環境が適切に設計されている場合は、複数の AWS アカウントを効果的に管理できるため、複数のワークロードと環境を管理できます。

AWS Control Tower は、アーキテクチャが適切に設計された環境をセットアップします。アカウントに依存し AWS Organizations ているため、複数の AWS アカウントにまたがる環境への変更を管理するのに役立ちます。

アーキテクチャが適切に設計された環境の定義

AWS は、適切に設計された環境をラン ディングゾーンで始まる環境として定義します。

AWS Control Tower には、自動的にセットアップされるランディングゾーンがあります。これにより、環境内の複数のアカウントにわたって企業ガイドラインが確実に遵守されるようにコントロールが適用されます。

ランディングゾーンの定義

ランディングゾーンは、デフォルトアカウント、アカウント構造、ネットワーク、セキュリティレイアウトなど、推奨される開始点を提供するクラウド環境です。ランディングゾーンから、ソリューションとアプリケーションを利用するワークロードをデプロイできます。

アーキテクチャが適切に設計された環境をセットアップするためのガイドライン

次のセクションで説明するように、アーキテクチャが適切に設計された環境には次の 3 つの主要なコンポーネントがあります。

- 複数の AWS アカウント
- 複数の組織単位 (OU)
- よく計画された構造

複数の AWS アカウントの使用

アーキテクチャが適切に設計された環境をセットアップするには、1 つのアカウントでは不十分です。複数のアカウントを使用することで、セキュリティ目標とビジネスプロセスを最適にサポートできます。マルチアカウントアプローチを使用する利点は次のとおりです。

- セキュリティコントロール - アプリケーションによってセキュリティプロファイルが異なるため、アプリケーションごとに異なるコントロールポリシーとメカニズムが必要です。例えば、監査人と話をして、ペイメントカード業界 (PCI) ワークロードをホストしている単一のアカウントを参照した方がはるかに簡単です。
- 分離 - アカウントは、セキュリティ保護の単位です。潜在的なリスクとセキュリティの脅威は、他のユーザーに影響を与えることなく、アカウント内に封じ込めることができます。したがって、セキュリティのニーズによっては、アカウントを互いに分離する必要があります。例えば、チームによってセキュリティプロファイルが異なる場合を考えてみます。
- 多数のチーム — チームごとに責任とリソースニーズが異なります。複数のアカウントをセットアップすることで、同じアカウントを使用することがあっても、チームが互いに干渉することはありません。

- データの分離 - データストアとアカウントを分離することで、データにアクセスしてデータストアを管理できるユーザーの数を制限できます。この分離により、高度にプライベートなデータの不正漏洩を防ぐことができます。例えば、データを分離すると、一般データ保護規則 (GDPR) の遵守をサポートできます。
- ビジネスプロセス - ビジネス単位または製品によって目的とプロセスがまったく異なることがあります。ビジネス固有のニーズに合わせて個々のアカウントを確立できます。
- 請求 - 転送料金など請求レベルで項目を分けるには、アカウントが唯一の方法です。マルチアカウント戦略は、ビジネス単位、職務チーム、または個々のユーザー間で個別に請求対象項目を作成する場合に役立ちます。
- クォータ割り当て - AWS クォータはアカウントごとに設定されます。アカウントごとにワークロードを分けると、明確に定義された個別のクォータが各アカウント (プロジェクトなど) に与えられます。

複数の組織単位の使用

AWS Control Tower およびその他のアカウントオーケストレーションフレームワークでは、アカウント境界を越えて変更を加えることができます。したがって、AWS ベストプラクティスはクロスアカウントの変更に対処します。これにより、環境が破壊されたり、セキュリティが損なわれたりする可能性があります。場合によっては、変更の影響がポリシーを超えて環境全体に及ぶことがあります。そのため、少なくとも本番稼働とステージングという 2 つの必須アカウントをセットアップすることをお勧めします。

さらに、ガバナンスとコントロールの目的で AWS、アカウントは多くの場合、組織単位 (OUs) にグループ化されます。OU は、複数のアカウントにわたるポリシーの適用を処理するように設計されています。

最低でも、個別のコントロールとポリシーを使用して、本番稼働環境とは別に本番稼働前 (またはステージング) 環境を作成することをお勧めします。本番稼働環境およびステージング環境は、個別の OU として作成して管理し、個別のアカウントとして請求できます。また、コードのテスト用にサンドボックス OU をセットアップすることをお勧めします。

ランディングゾーンでの OU 向けに適切に計画された構造の使用

AWS Control Tower では、いくつかの OU が自動的にセットアップされます。ワークロードと要件が時間の経過と共に拡大するのに伴い、ニーズに合わせて当初のランディングゾーン設定を拡張できます。

Note

例に示す名前は、マルチアカウント AWS 環境を設定するための推奨 AWS 命名規則に従います。ランディングゾーンのセットアップ後に OU の名前を変更するには、OU の詳細ページで [Edit] (編集) を選択します。

レコメンデーション

AWS Control Tower で最初の必須の OU (セキュリティ OU) をセットアップした後、ランディングゾーンに追加の OU をいくつか作成することをお勧めします。

AWS Control Tower でサンドボックス OU と呼ばれる追加の OU を少なくとも 1 つ作成できるようにすることをお勧めします。この OU は、ソフトウェア開発環境用です。サンドボックス OU のセットアップを選択していれば、AWS Control Tower がランディングゾーンの作成時にセットアップします。

ユーザー自身がセットアップできるその他の推奨される OU が 2 つあります。共有サービスとネットワークアカウントが含まれるインフラストラクチャ OU と、本番稼働用ワークロードが含まれるワークロード OU です。AWS Control Tower コンソールから [Organizational units] (組織単位) ページで他の OU をランディングゾーンに追加できます。

自動的にセットアップされるものを除く推奨される OU

- インフラストラクチャ OU - 共有サービスとネットワークアカウントが含まれます。

Note

AWS Control Tower は、インフラストラクチャ OU を自動的にセットアップしません。

- サンドボックス OU - ソフトウェア開発 OU。例えば、この OU は使用量に固定制限がある場合や、本番稼働ネットワークに接続されていない場合があります。

Note

AWS Control Tower ではサンドボックス OU をセットアップすることをお勧めします。ただし、これは任意です。ランディングゾーン設定の一環として、自動的にセットアップできます。

- ワークロード OU - ワークロードを実行するアカウントが含まれます。

 Note

AWS Control Tower は、ワークロード OU を自動的にセットアップしません。

詳細については、「[Production starter organization with AWS Control Tower](#)」(AWS Control Tower を使用して作成された本番稼働用スターター組織) を参照してください。

完全なマルチアカウント OU 構造を持つ AWS Control Tower の例

AWS Control Tower はネストされた OU 階層をサポートしています。つまり、組織の要件を満たす階層 OU 構造を作成できます。AWS マルチアカウント戦略ガイダンスに合わせて AWS Control Tower 環境を構築できます。

また、AWS マルチアカウントガイダンスに従って適切に機能するシンプルでフラットな OU 構造を構築することもできます。階層 OU 構造を構築できるからといって、必ずそうしなければならないわけではありません。

- AWS マルチアカウントガイダンスを使用して、拡張されたフラットな AWS Control Tower 環境の OUs [「例: フラット OU 構造のワークロード」](#) を参照してください。
- AWS Control Tower でネストされた OU 構造を使用する方法の詳細については、「[AWS Control Tower のネストされた OU](#)」を参照してください。
- AWS Control Tower が AWS ガイダンスと連携する方法の詳細については、AWS ホワイトペーパー [「Organizing Your AWS Environment Using Multiple Accounts」](#) を参照してください。

リンク先のページにある図表は、他にも多くの基礎 OU と追加 OU が作成されていることを示しています。これらの OU は、大規模にデプロイする場合に追加で求められるニーズに対応します。

基礎 OU 列では、次の 2 つの OU が基本構造に追加されています。

- Security_Prod OU - セキュリティポリシーの読み取り専用領域と、ブレイクガラスのセキュリティ監査領域を提供します。
- インフラストラクチャ OU - 以前に推奨されていたインフラストラクチャ OU を Infrastructure_Test (本番稼働前のインフラストラクチャ用) と Infrastructure_Prod (本番稼働のインフラストラクチャ用) の 2 つの OU に分けることをお勧めします。

追加 OU 領域では、基本構造にさらにいくつかの OU が追加されています。環境の拡大に合わせて次に作成することが推奨されている OU は以下のとおりです。

- ワークロード OU - ワークロード OU は、以前は推奨されていましたが、現在は任意となった OU です。Workloads_Test (本番稼働前のワークロード用) と Workloads_Prod (本番稼働のワークロード用) の 2 つの OU に分離されました。
- ポリシーステージング OU - システム管理者はコントロールとポリシーに対する変更をテストしてからそれらを完全に適用できます。
- 停止 OU - 一時的に無効になっている可能性のあるアカウント用のロケーションを提供します。

ルートについて

ルートは OU ではありません。ルートとは、管理アカウント、および組織内のすべての OU とアカウントのコンテナです。概念的には、ルートにはすべての OU が含まれます。ルートは削除できません。AWS Control Tower 内のルートレベルでは、登録済みアカウントを管理することはできません。代わりに、OU 内の登録済みアカウントを管理します。役立つ図については、[AWS Organizations ドキュメント](#)を参照してください。

ランディングゾーンのセットアップに関する管理上のヒント

ランディングゾーンをセットアップして設定するためのヒントをいくつか示します。

- 作業を最も多く行う AWS リージョンは、ホームリージョンである必要があります。
- ランディングゾーンを設定し、ホームリージョン内から Account Factory アカウントをデプロイします。
- 複数の AWS リージョンに投資する場合は、クラウドリソースがクラウド管理作業のほとんどを行い、ワークロードを実行するリージョンにあることを確認してください。
- ワークロードとログを同じ AWS リージョンに保持することで、リージョン間のログ情報の移動と取得に関連するコストを削減できます。
- 監査およびその他の Amazon S3 バケットは、AWS Control Tower を起動するのと同じ AWS リージョンに作成されます。これらのバケットを移動しないことをお勧めします。
- ログアーカイブアカウントで独自のログバケットを作成できますが、お勧めできません。AWS Control Tower によって作成されたバケットは、必ず残してください。
- Amazon S3 アクセスログは、ソースバケットと同じ AWS リージョンに存在する必要があります。

- 起動時に、AWS Control Tower でサポートされているすべてのリージョンで、AWS Security Token Service (STS) エンドポイントを管理アカウントでアクティブ化する必要があります。この操作を行わないと、設定プロセスの途中で起動が失敗する可能性があります。
- AWS Control Tower では、有効になっているコントロールのみのタグ付けがサポートされます。詳細については、「[AWS Control Tower コントロールのタグ付け API](#)」を参照してください。
- AWS Control Tower が管理するすべてのアカウントで、多要素認証 (MFA) を有効にすることをお勧めします。
- または、AWS ルートアクセス管理機能を使用して、メンバーアカウントでルートアクションを実行でき、すべてのアカウントで MFA を有効にする必要がなくなります。詳細については、「[AWS Organizationsを使用するお客様のルートアクセスの集中管理](#)」を参照してください。

VPC に関する考慮事項

- AWS Control Tower によって作成された VPC は、AWS Control Tower が利用可能な AWS リージョンに限定されます。サポート対象外のリージョンでワークロードを実行する一部のお客様は、Account Factory アカウントで作成された VPC を無効にすることをお勧めします。この場合、Service Catalog ポートフォリオを使用して新しい VPC を作成するか、必要なリージョンでのみ実行されるカスタム VPC を作成することもできます。
- AWS Control Tower によって作成された VPC は、すべての AWS アカウント用に作成されたデフォルト VPC とは異なります。AWS Control Tower がサポートされているリージョンでは、AWS Control Tower は AWS Control Tower VPC の作成時にデフォルトの VPC を削除します。
- ホーム AWS リージョンでデフォルトの VPC を削除する場合は、他のすべての AWS リージョンで削除することをお勧めします。

Landing Zone v4.0 移行ガイド

AWS Control Tower ランディングゾーン 4.0 では、ランディングゾーンアーキテクチャの大幅な見直しを導入され、柔軟な専用コントロールエクスペリエンスと完全にオプションのサービス統合が提供されます。主な機能強化には AWS Config、AWS CloudTrail、SecurityRoles、および AWS Backup 統合を選択的に有効にする機能が含まれ、AWS Config および AWS CloudTrail 専用のリソースを使用して分離を改善します。

このリリースでは、必須の組織構造要件が削除され、お客様が独自の を定義できるようになりました。また、包括的な ConfigBaseline を必要とせずに、検出コントロールをサポートする新しいが導入されましたAWSControlTowerBaseline。サービスにリンクされた Config Aggregator は、以前の集約メソッドを置き換え、コンプライアンスデータ収集を合理化します。

さらに、マニフェストフィールドはオプションになり、統合と制御の有効化のみに焦点を当てた AWS Organizations 最小限のランディングゾーンデプロイが可能になります。これらの変更により、堅牢なガバナンス機能を維持しながら、より大きなカスタマイズオプションが提供され、お客様は特定のニーズに合わせて AWS Control Tower をより効果的に調整できます。

トピック

- [主な変更点](#)
- [AWS Config の更新](#)

主な変更点

Note

- 「登録済み」と「登録済み」の定義は、この新しいバージョンの AWS Control Tower に移行しました。アカウント/OU で AWS Control Tower リソースが有効になっている場合 (コントロールやベースラインなど)、管理対象リソースと見なされます。定義は、AWSControlTowerBaselineベースラインの存在によって駆動されなくなります。
 - サービスにリンクされたロールはすべてのランディングゾーンバージョンにわたって保持され、OUs」になったときに削除されなくなります。
 - サービスにリンクされたロールは、ランディングゾーンの廃止後にのみ手動で削除できます。
-
- ランディングゾーン 4.0 の前提条件: API 経由でバージョン 4.0 にアップグレードする場合は、AWSControlTowerCloudTrailRoleサービスロールが既存のインラインポリシーAWSControlTowerCloudTrailRolePolicyではなく新しい管理ポリシーを使用していることを確認します。[ドキュメント](#)の説明に従って、現在のインラインポリシーをデタッチし、新しい管理ポリシーをアタッチします。
 - オプションのマニフェスト: ランディングゾーン API のマニフェストフィールドがオプションになりました。お客様は、サービス統合なしでランディングゾーンを作成できます。マニフェストフィールドを既に使用している既存の顧客には影響しません。
 - オプションの組織構造: AWS Control Tower は、お客様が独自の組織構造を定義および管理できるように、セキュリティ OU の作成を強制または管理しなくなりました。ただし、AWS Control Tower では、各 AWS サービス統合に設定されたすべてのアカウントを同じ親 OU の下にする必要があります。AWS Control Tower を既にセットアップしていて、セキュリティ OU を持ってい

るお客様には影響はありません。AWS Control Tower は、Security OU でサービス統合アカウントを管理するために必要なリソースとコントロールを自動的にデプロイします。たとえば、AWS Config 統合が有効になっている場合、AWS Config の記録はすべてのサービス統合アカウントで有効になります。AWS Control Tower ベースラインと AWS Config ベースラインは、セキュリティ OU および統合アカウントには適用されません。サービス統合を変更するには、ランディングゾーンの設定を更新します。

 Note

- AWS Control Tower ランディングゾーン 4.0 の組織構造設定が以前のランディングゾーンバージョンから変更されました。AWS Control Tower は、指定されたセキュリティ OU を作成しなくなります。サービス統合アカウントを持つ OU は、指定されたセキュリティ OU になります。
 - メンバーアカウントが、各統合のアカウントが存在する OU に移動すると、自動登録がオンまたはオフになっているかどうかに関係なく、その OU で有効なコントロールがドリフトします。
- ドリフト通知: AWS Control Tower は、AWSControlTowerBaselineを有効にせずにランディングゾーン 4.0 のすべてのお客様の SNS トピックへのドリフト通知の送信を停止し、代わりに管理アカウントの EventBridge へのドリフト通知の送信を開始します。EventBridge を介してドリフト通知を受信する方法に関するサンプライベントとガイダンスを確認するには、[このガイド](#)を確認してください。
 - オプションのサービス統合: AWS CloudTrail、SecurityRoles、など AWS Config、すべての AWS Control Tower 統合を有効または無効にできるようになりました AWS Backup。これらの統合には、API でオプションに必要なenabledフラグも追加されました。ランディングゾーンまたは共有アカウントに適用されるベースラインが相互に依存するようになりました。統合固有の依存関係は次のとおりです。
 - 有効化:
 - CentralSecurityRolesBaseline → を有効にするCentralConfigBaseline必要があります
 - IdentityCenterBaseline → を有効にするCentralSecurityRolesBaseline必要があります
 - BackupCentralVaultBaseline → を有効にするCentralSecurityRolesBaseline必要があります

- BackupAdminBaseline → を有効にするCentralSecurityRolesBaseline必要があります
- LogArchiveBaseline → 独立 (依存関係なし)
- CentralConfigBaseline → 独立 (依存関係なし)
- 無効化:
 - CentralConfigBaseline
は、CentralSecurityRolesBaseline、IdentityCenterBaselineBackupAdminBaselineおよび BackupCentralVaultBaselineベースラインが最初に無効になっている場合にのみ無効にできます。
 - CentralSecurityRolesBaseline
は、IdentityCenterBaseline、BackupAdminBaselineおよび BackupCentralVaultBaselineベースラインが最初に無効になっている場合にのみ無効にできます。
 - IdentityCenterBaseline は個別に無効にできます。
 - BackupAdminBaseline および BackupCentralVaultBaselineベースラインは個別に無効にできます
 - LogArchiveBaseline は個別に無効にできます

AWS Config の更新

- AWS Config および AWS CloudTrail 専用リソース: AWS Config および AWS CloudTrail では、共有リソースの代わりに個別の専用 S3 バケットと SNS トピックを使用するようになりました。お客様は、複数の統合に単一または個別のアカウントを使用する柔軟性を制限されています。
- AWS Control Tower ランディングゾーンバージョン 4.0 にアップグレードする場合、既存のデータと S3 バケットは移動されません。AWS CloudTrail 統合では、プレフィックスが付いた既存の S3 バケットが引き続き使用されますaws-controltower-logs。更新オペレーション後の新しい AWS Config データは、AWS Control Tower aws-controltower-configが CentralConfigBaseline に指定されたアカウントに作成するプレフィックスを持つ新しい S3 バケットに保存されます。

Note

ランディングゾーン 4.0 で AWS CloudTrail 統合を初めて有効にすると、プレフィックスを持つたびに新しい S3 バケットが作成されます。aws-controltower-cloudtrail

- データの場所の変更: 以前に共有されたリソースから専用リソースにアップグレードした既存のお客様は、異なる S3 バケットに AWS Config および AWS CloudTrail データを持つことになります。確立されたお客様のワークフローとツールでは、新しいバケットの場所のデータにアクセスするために更新が必要になる場合があります。
- AWS CloudTrail は引き続き同じ既存のバケットに留まりますが、AWS Config データは AWS Control Tower によって作成された新しい S3 バケットに保存されます。
- 異なるログを 1 つのバケットに一元化する場合は、クロスバケットレプリケーションを設定できます。詳細については、[S3 ドキュメント](#)を参照してください。
- AWS Control Tower によって管理されるリージョンで AWS Control Tower によって作成されていない既存の AWS Config 配信チャネルを持つアカウントを登録している場合は、ランディングゾーン 4.0 aws-controltower-config-logs-の AWS Control Tower 設定と一致するように、配信チャネルの S3 バケット名を AWS Config 統合アカウントのプレフィックスが付いた新しい S3 バケットに更新します。詳細については、「[既存の AWS Config リソースがあるアカウントを登録する](#)」を参照してください。
- AWS Config ランディングゾーンバージョン 4.0 での統合: AWS Config 統合を有効にしてランディングゾーン 4.0 に移行すると、次の変更が表示されます。
 1. 既存の監査アカウントは、委任管理者として登録されています AWS Config。
 2. サービスにリンクされた Config Aggregator は、監査アカウント (新規顧客の AWS Config 中央アグリゲータアカウントと既存顧客の監査アカウント) にデプロイされます。新しいアグリゲータは、Control Tower 以外のマネージドアカウントを含め、組織内の任意の AWS Config レコーダーからデータを集約できます。
 3. 既存のアグリゲータは削除されます - 管理アカウント (aws-controltower-ConfigAggregatorForOrganizations) の組織アグリゲータと監査アカウント (aws-controltower-GuardRailsComplianceAggregator) のアカウントアグリゲータは削除されます。
 4. Configuration Aggregator はサービスにリンクされているため、削除されたアグリゲータに関連付けられたコントロールは自動的に削除されます。
 - a. [AWS Config リソースの AWS Control Tower によって作成されたタグの変更を禁止する](#)

b. [AWS Control Tower によって作成された AWS Config 集約認可の削除を禁止する](#)

- 新しい**ConfigBaseline**ベースライン: 包括的な を必要とせずに、検出コントロールをサポートする ConfigBaseline OU レベルに別の が追加されましたAWSControlTowerBaseline。詳細については、[「OU レベルのベースラインタイプのリスト」](#)を参照してください。デフォルトのランディングゾーンを使用している既存のお客様では、すべてのサービス統合がオプションになりました。依存関係要件については、「」で説明しています[主な変更点](#)。
- サービスにリンクされた Config Aggregator: AWS Config 中央アグリゲータアカウントの組織とアカウントのアグリゲータを置き換えます。
- AWS Config 統合を有効にしてランディングゾーン 4.0 にアップグレードする場合、お客様は `アクセスorganizations:ListDelegatedAdministrators`許可が必要です

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "backup:UpdateGlobalSettings",
        "controltower:CreateLandingZone",
        "controltower:UpdateLandingZone",
        "controltower:ResetLandingZone",
        "controltower>DeleteLandingZone",
        "controltower:GetLandingZoneOperation",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "controltower:ListLandingZoneOperations",
        "controltower:ListTagsForResource",
        "controltower:TagResource",
        "controltower:UntagResource",
        "servicecatalog:*",
        "organizations:*",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "logs:*",
        "cloudformation:*",
        "kms:*",
```

```
        "iam:GetRole",
        "iam:CreateRole",
        "iam:GetSAMLProvider",
        "iam:CreateSAMLProvider",
        "iam:CreateServiceLinkedRole",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:AttachRolePolicy",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": "*"
  }
]
```

グループ、ロール、ポリシーを設定する上での推奨事項

ランディングゾーンを設定する際には、どのユーザーが特定のアカウントにアクセスする必要があるのか、その理由を事前に決定することをお勧めします。例えば、セキュリティアカウントはセキュリティチームだけがアクセスできるようにし、管理アカウントはクラウド管理者のチームのみがアクセスできるようにする必要があります。

このトピックの詳細については、「[AWS Control Tower の Identity and Access Management](#)」を参照してください。

推奨される制限事項

管理者が AWS Control Tower アクションのみを管理できるようにする IAM ロールまたはポリシーを設定することで、組織への管理アクセスの範囲を制限できます。推奨されるアプローチは、IAM ポリシー `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy` を使用することです。AWSControlTowerServiceRolePolicy ロールを有効にすると、管理者は AWS Control Tower のみを管理できます。各アカウントには、予防コントロールを管理する AWS Organizations ための への適切なアクセス、検出コントロールを管理する AWS Config ための SCPs、 へのアクセスを必ず含めてください。

ランディングゾーンで共有監査アカウントを設定する場合は、アカウントの第三者監査人に `AWSecurityAuditors` グループを割り当てることをお勧めします。このグループは、メンバーに読み取り専用アクセス許可を与えます。アカウントには、監査対象の環境に対する書き込みアクセス許可があってはなりません。これは、監査人の職務分離要件の遵守に違反する可能性があるためです。

AWS Control Tower の特定のロールとやり取りするアカウントとリソースを制限するために、ロールの信頼ポリシーに条件を課すことができます。AWSControlTowerAdmin ロールは幅広いアクセスを許可するため、このロールへのアクセスを制限することを強くお勧めします。詳細については、「[Optional conditions for your role trust relationships](#)」を参照してください。

AWS Control Tower リソースの作成と変更に関するガイダンス

AWS Control Tower でリソースを作成および変更する場合は、次のベストプラクティスをお勧めします。このガイダンスは、サービスが更新されたときに変更される可能性があります。AWS Control Tower 環境には[責任共有モデル](#)が適用されることに注意してください。

一般的なガイダンス

- 管理アカウント、共有アカウント、メンバーアカウントのリソースなど、AWS Control Tower によって作成されたリソースを変更または削除しないでください。これらのリソースを変更すると、ランディングゾーンの更新または OU の再登録が必要になる場合があります。また、変更によってコンプライアンスレポートが不正確になる可能性があります。

特に、次のことに注意してください。

- アクティブな AWS Config レコーダーを保持します。Config レコーダーを削除すると、検出コントロールはドリフトを検出して報告することができません。非準拠のリソースが、情報不足が原因で [Compliant] (準拠) として報告される可能性があります。
- セキュリティ組織単位 AWS Identity and Access Management (OU) の共有アカウント内で作成された (IAM) ロールを変更または削除しないでください。これらのロールの変更には、ランディングゾーンの更新が必要になる場合があります。
- 登録されていないアカウントであっても、メンバーアカウントから `AWSControlTowerExecution` ロールを削除しないでください。削除した場合、これらのアカウントを AWS Control Tower に登録したり、直接の親 OU を登録したりすることができなくなります。
- SCPs または AWS Security Token Service () AWS リージョン を介した の使用を許可しないでくださいAWS STS。禁止した場合、AWS Control Tower が未定義の状態になります。でリージョ

ンを許可しない場合 AWS STS、認証はそれらのリージョンで使用できないため、機能はそれらのリージョンで失敗します。代わりに、コントロールに示すように、AWS Control Tower のリージョン拒否機能、ランディングゾーンレベルで機能する [リクエスト AWS された に基づく へのアクセスを拒否 AWS リージョン](#) する、または [OU に適用されるコントロールリージョン拒否コントロール](#) に依存して、リージョンへのアクセスを制限します。

- SCP AWS Organizations FullAWSAccess は適用する必要がある、他の SCPs とマージしないでください。この SCP への変更はドリフトとして報告されません。ただし、特定のリソースへのアクセスが拒否された場合、一部の変更が AWS Control Tower の機能に予期しない影響を与える可能性があります。例えば、SCP がデタッチまたは変更された場合、アカウントは AWS Config レコーダーへのアクセスを失うか、CloudTrail ログにギャップが生まれます。
- API を使用して AWS Organizations DisableAWSServiceAccess、ランディングゾーンを設定した組織への AWS Control Tower サービスアクセスをオフにしないでください。オフにした場合、AWS Organizations からのメッセージサポートがないと、特定の AWS Control Tower ドリフト検出機能が正しく動作しなくなる可能性があります。これらのドリフト検出機能により、AWS Control Tower は組織内の組織単位、アカウント、統制のコンプライアンスステータスを正確に報告できます。詳細については、[API_DisableAWSServiceAccessAWS Organizations API リファレンスの「」](#)を参照してください。
- 通常、AWS Control Tower は一度に 1 つのアクションを実行します。1 つのアクションを完了してから、別のアクションを開始する必要があります。例えば、コントロールを有効にするプロセスが進行中にアカウントをプロビジョニングしようとする、アカウントのプロビジョニングは失敗します。

例外:

- AWS Control Tower は、オプションコントロールをデプロイする同時アクションを許可します。詳細については、「[Concurrent deployment for optional controls](#)」を参照してください。
- AWS Control Tower は、Account Factory を使用して、アカウントに対して最大 10 の作成、更新、または登録の同時アクションを許可します。

Note

AWS Control Tower によって作成されたリソースの詳細については、「[共有アカウントとは](#)」を参照してください。

アカウントと OU に関するヒント

- 登録した各 OU は最大 1000 アカウントに設定することをお勧めします。これにより、新しいリージョンをガバナンス用に構成する場合など、アカウントの更新が必要なときはいつでも [OU を再登録] 機能によってこれらのアカウントを更新できます。
- OU あたりのアカウント数は 1000 に制限されていますが、OU の登録にかかる時間を短縮するには、OU あたりのアカウント数を 680 程度にしておくことをお勧めします。原則として、OU の登録に必要な時間は、OU が運用しているリージョンの数に、OU のアカウント数を掛けた数に応じて増加します。
- 概算で、680 個のアカウントを持つ OU の場合、コントロールの登録と有効化に最大 2 時間、再登録に最大 1 時間かかります。また、コントロールが多い OU は、コントロールが少ない OU よりも登録に時間がかかります。
- OU の登録に長い期間かかることに関する懸念事項の 1 つは、このプロセスが他のアクションをブロックすることです。お客様によっては、各 OU でより多くのアカウントを許可したいため、OU の登録や再登録に時間がかかっても構わない場合があります。

ルートユーザーとしてサインインする場合

特定の管理タスクでは、ルートユーザーとしてサインインする必要があります。AWS Control Tower の Account Factory によって AWS アカウント 作成された にルートユーザーとしてサインインできます。

次のアクションを実行するには、ルートユーザーとしてサインインする必要があります。

- アカウント名、ルートユーザーのパスワード、E メールアドレスなど、特定のアカウント設定を変更する。詳細については、「[AWS Control Tower でアカウントを更新して移動する](#)」を参照してください。
- [を閉じる AWS アカウント](#)には。
- ルートユーザーログイン認証情報を必要とするアクションの詳細については、「AWS アカウント管理 リファレンスガイド」の「[ルートユーザー認証情報が必要なタスク](#)」を参照してください。

Note

[AWS サポートプランを変更または有効にするには、ルートユーザーとしてサインインするか、または適切な IAM アクセス許可を持つユーザーになる必要があります。](#)

ルートユーザーとしてサインインするには

1. AWS サインインページを開きます。

アクセス AWS アカウント が必要な の E メールアドレスがない場合は、AWS Control Tower から取得できます。管理アカウントのコンソールを開き、[Accounts] (アカウント) を選択し、E メールアドレスを探します。

2. アクセス AWS アカウント が必要な の E メールアドレスを入力し、次へを選択します。

3. [Forgot password?] (パスワードを忘れた場合) を選択して、パスワードリセット手順をルートユーザーの E メールアドレスに送信します。

4. ルートユーザーのメールボックスからパスワードリセットの E メールメッセージを開き、指示に従ってパスワードをリセットします。

5. AWS サインインページを開き、リセットしたパスワードでサインインします。

または、AWS ルートアクセス管理機能を使用して、ルートとしてサインインしなくても、メンバーアカウントでルートアクションを実行できます。詳細については、「[AWS Organizationsを使用するお客様のルートアクセスの集中管理](#)」を参照してください。

AWS Organizations ガイダンス

AWS Control Tower は密接に関連付けられています AWS Organizations。AWS 環境を保護するための最適な連携方法に関する具体的なガイダンスをいくつか示します。

- AWS Control Tower 管理アカウントとメンバーアカウントのセキュリティを保護するためのベストプラクティスに関するガイダンスについては、AWS Organizations ドキュメントを参照してください。
 - [管理アカウントのベストプラクティス](#)
 - [メンバーアカウントのベストプラクティス](#)
- AWS Control Tower に登録済みの OU にアタッチされている既存のサービスコントロールポリシー (SCP) を更新しないでください。これを行うと、コントロールが不明な状態になり、AWS Control Tower でランディングゾーンのリセットや OU の再登録を行う必要が生じます。代わりに、AWS Control Tower が作成した SCPs を編集するのではなく、を使用して新しい SCPs AWS Organizations を作成し、それらを OUs にアタッチできます。
- 登録済み OU の外部から個々の登録済みアカウントを AWS Control Tower に移動すると、解決が必要なドリフトが発生します。「[ガバナンスドリフトのタイプ](#)」を参照してください。

- AWS Organizations を使用して AWS Control Tower に登録されている組織内でアカウントを作成、招待、または移動する場合、それらのアカウントは AWS Control Tower に登録されず、それらの変更は記録されません。SSO を使用してこれらのアカウントにアクセスする必要がある場合は、「[メンバーアカウントアクセス](#)」を参照してください。
- AWS Organizations を使用して OU を AWS Control Tower によって作成された組織に移動する場合、外部 OU は AWS Control Tower によって登録されません。
- AWS Control Tower は、アクセス許可のフィルタリングをとは異なる方法で処理 AWS Organizations します。アカウントが AWS Control Tower Account Factory でプロビジョニングされている場合、エンドユーザーは、AWS Control Tower コンソールですべての OUs の名前と親を確認できます。これらの名前と親 AWS Organizations を から直接取得するアクセス許可がない場合も同様です。
- AWS Control Tower は、OU の親は表示できるが OU の名前は表示できない許可など、組織に対する混合アクセス許可をサポートしていません。このため、AWS Control Tower の管理者は完全なアクセス許可を持つことが期待されます。
- SCP AWS Organizations FullAWSAccess は適用する必要がある、他の SCPs とマージしないでください。この SCP への変更はドリフトとして報告されません。ただし、特定のリソースへのアクセスが拒否された場合、一部の変更が AWS Control Tower の機能に予期しない影響を与える可能性があります。例えば、SCP がデタッチまたは変更された場合、アカウントは AWS Config レコーダーへのアクセスを失うか、CloudTrail ログにギャップが生まれます。
- API を使用して AWS Organizations DisableAWSServiceAccess、ランディングゾーンを設定した組織への AWS Control Tower サービスアクセスをオフにしないでください。オフにした場合、AWS Organizations からのメッセージサポートがないと、特定の AWS Control Tower ドリフト検出機能が正しく動作しなくなる可能性があります。これらのドリフト検出機能により、AWS Control Tower は組織内の組織単位、アカウント、統制のコンプライアンスステータスを正確に報告できます。詳細については、[API_DisableAWSServiceAccessAWS Organizations API リファレンスの「](#)」を参照してください。

IAM Identity Center のガイダンス

AWS Control Tower では、AWS Identity and Access Management (IAM) を使用してへのアクセスを規制することをお勧めします AWS アカウント。ただし、AWS Control Tower に IAM Identity Center をセットアップさせるか、ビジネス要件を最も効果的に満たす方法で IAM Identity Center を自分でセットアップするか、またはアカウントアクセスに別の方法を選択するかを選ぶことができます。

Note

SSO は、テクノロジー業界でシングルサインオンを表すために使用される略語です。一般的に、SSO はセッションとユーザー認証のサービスです。これにより、ユーザーは 1 つのログイン認証情報を使用して多くのアプリケーションにアクセスできます。のシングルサインオン機能を参照する場合 AWS、という AWS サービスを参照し AWS Identity and Access Management、IAM または IAM Identity Center と略します。

デフォルトでは、AWS Control Tower AWS は、[「複数のアカウントを使用して AWS 環境を整理する」](#)で定義されているベストプラクティスのガイダンスに従って、ランディングゾーンに IAM アイデンティティセンターを設定します。ほとんどのお客様はデフォルトを選択します。特定の業界や国、または IAM Identity Center AWS AWS リージョン が利用できない地域での規制コンプライアンスのために、代替のアクセス方法が必要になる場合があります。

オプションの選択

コンソールから、AWS Control Tower にセットアップさせるのではなく、ランディングゾーンのセットアッププロセス中に IAM Identity Center を自己管理することを選択できます。ランディングゾーンの設定を変更し、ランディングゾーンの [設定] ページでランディングゾーンを更新することで、後でいつでもこの選択を変更できます。

AWS Control Tower AWS で IAM Identity Center を停止するか、IAM Identity Center AWS の使用を開始するには

1. ランディングゾーンの [設定] ページに移動する
2. [設定] タブを選択します。
3. 次に、適切なラジオボタンを選択して、IAM Identity Center AWS の選択を変更します。

IdP として AWS IAM アイデンティティセンターを自己管理することを選択すると、AWS Control Tower は やなどの AWS Control Tower の管理に必要なロール `AWSControlTowerAdmin` とポリシーのみを作成します `AWSControlTowerAdminPolicy`。自己管理型のランディングゾーンの場合、AWS Control Tower は、ランディングゾーンのセットアッププロセス中や Account Factory でのアカウントプロビジョニング中に、お客様固有の用途の IAM ロールおよびグループを作成しなくなります。

Note

AWS Control Tower AWS ランディングゾーンから IAM Identity Center を削除しても、AWS Control Tower が作成したユーザー、グループ、およびアクセス許可セットは削除されません。これらのリソースを削除することをお勧めします。

Azure AD、Ping、Okta などの代替 ID プロバイダー (IdPs) を持つ Account Factory のお客様は、IAM Identity Center AWS [プロセス](#)に従って外部 ID プロバイダーに接続し、IdP をオンボードできます。ランディングゾーンの設定を変更することで、いつでも AWS Control Tower がグループとロールを生成するように戻すことができます。

- ID ソースに基づいて AWS Control Tower が IAM Identity Center と連携する方法の詳細については、このユーザーガイドの開始方法ページの「[起動前チェック](#)」セクションの AWS IAM アイデンティティセンター「お客様向けの考慮事項」を参照してください。
- AWS Control Tower が IAM Identity Center やさまざまなアイデンティティソースとやり取りする動作の詳細については、「IAM Identity Center ユーザーガイド」の「[アイデンティティソースの変更に関する考慮事項](#)」を参照してください。
- AWS Control Tower および IAM Identity Center の使用に関する詳細については、「[IAM Identity Center AWS と AWS Control Tower の使用](#)」を参照してください。

Account Factory ガイダンス

Note

単一アカウントのプロビジョニング、更新、カスタマイズは、AWSControlTowerBaseline を有効にした組織単位 (OU) をターゲットにする必要があります。OU で AWSControlTowerBaseline が有効になっていない場合は、アカウントの自動登録を有効にするか、EnabledBaseline で ResetEnabledBaseline API と ResetEnabledControl APIs を使用してアカウント EnabledControls を登録できます。EnabledBaselines AWSControlTowerBaseline の詳細については、「」を参照してください[OU レベルで適用されるベースラインタイプ](#)。

Account Factory を使用して AWS Control Tower で新しいアカウントをプロビジョニングする際に、問題が発生する可能性があります。これらの問題のトラブルシューティング方法については、

「AWS Control Tower ユーザーガイド」で「[トラブルシューティング](#)」の「[新しいアカウントのプロビジョニングに失敗する](#)」セクションを参照してください。

IAM ユーザーの代わりにフェデレーションユーザーまたは IAM ロールを作成することをお勧めします。フェデレーションユーザーと IAM ロールは一時的な認証情報を提供します。IAM ユーザーは長期認証情報を持っているため、管理が難しい場合があります。詳細については、「IAM ユーザーガイド」の「[IAM アイデンティティ \(ユーザー、ユーザーグループ、ロール\)](#)」を参照してください。

Account Factory で新しいアカウントをプロビジョニングするとき、またはアカウント登録機能 AWS Control Tower を使用するとき、IAM ユーザーまたは IAM Identity Center ユーザーとして認証されている場合は、ユーザーが AWS Service Catalog ポートフォリオにアクセスできることを確認します。アクセスできない場合は、Service Catalog からのエラーメッセージが表示されることがあります。詳細については、「AWS Control Tower ユーザーガイド」で「[トラブルシューティング セクション](#)」の「[起動パスが見つからないというエラー](#)」を参照してください。

 Note

一度にプロビジョニングできるアカウントは最大 5 個です。

SNS トピックのサブスクリプションに関するガイダンス

SNS トピックをサブスクライブして、AWS Control Tower 環境に関する情報を入手します。

 Note

AWS Control Tower は、LZ4.0 以降のすべてのお客様の SNS トピックへのドリフト通知の送信を停止します。

- SNS トピックは、コンプライアンス通知や Amazon CloudWatch イベント通知など AWS Config、aws-controltower-AllConfigNotifications によって発行されたすべてのイベントを受け取ります。例えば、このトピックでは、コントロール違反が発生したかどうかを示します。また、他のタイプのイベントに関する情報も提供します (このトピックが構成されたときに公開する内容については、「[AWS Config](#)」を参照してください。)
- aws-controltower-BaselineCloudTrail 追跡の[データイベント](#)は、aws-controltower-AllConfigNotifications SNS トピックにも公開されるように設定されています。

- 詳細なコンプライアンス通知を受け取るには、aws-controltower-AllConfigNotifications SNS トピックをサブスクライブすることをお勧めします。このトピックでは、すべての子アカウントからのコンプライアンス通知を集約します。
- ドリフト通知やその他の通知、コンプライアンス通知を受信して、全体的な通知を少なくするには、aws-controltower-AggregateSecurityNotifications SNS トピックをサブスクライブすることをお勧めします。
- AWS Control Tower Account Factory for Terraform (AFT) のエラーに関する通知を受け取るには、AFT リポジトリの [aft_failure_notifications](#) という SNS トピックにサブスクライブできます。例えば、次のようになります。

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

- 保管中の SNS トピックは、ディスク暗号化を使用してすべて暗号化されています。詳細については、「[Data encryption](#)」を参照してください。

SNS トピックとコンプライアンスの詳細については、「[Prevention and notification](#)」を参照してください。

KMS キーのガイダンス

AWS Control Tower は AWS Key Management Service () で動作しますAWS KMS。オプションで、管理する暗号化キーを使用して AWS Control Tower リソースを暗号化および復号化する場合は、AWS KMS keysを生成して構成できます。KMS キーは、ランディングゾーンを更新するたびに追加または変更できます。ベストプラクティスとして、独自の KMS キーを使用し、時々変更することをお勧めします。

AWS KMS では、マルチリージョン KMS キーと非対称キーを作成できます。ただし、AWS Control Tower は、マルチリージョンキーまたは非対称キーをサポートしていません。AWS Control Tower は、既存のキーの事前チェックを実行します。マルチリージョンキーまたは非対称キーを選択すると、エラーメッセージが表示されることがあります。その場合は、AWS Control Tower リソースで使用する別のキーを生成してください。

AWS CloudHSM クラスターを運用する顧客の場合: CloudHSM クラスターに関連付けられたカスタムキーストアを作成します。次に、作成した CloudHSM カスタムキーストアにある KMS キーを作成できます。この KMS キーを AWS Control Tower に追加できます。

KMS キーのアクセス許可ポリシーを AWS Control Tower で動作させるには、特定の更新を行う必要があります。詳細については、「[KMS キーポリシーを更新する](#)」セクションを参照してください。

ランディングゾーン更新のベストプラクティス

このセクションでは、AWS Control Tower でのランディングゾーンバージョンのアップグレードを検討する際に留意すべき考慮事項とベストプラクティスについて説明します。2.0 ランディングゾーンバージョンシリーズから 3.0 ランディングゾーンバージョンシリーズへの変更は特に重要です。ランディングゾーンをアップグレードすると、AWS Control Tower は自動的に利用可能な最新バージョンになります。

Note

最新バージョンのランディングゾーンに更新するのがベストプラクティスです。

このセクションで説明するベストプラクティスの概要

- ベストプラクティス: セキュリティと監査上の理由から、すべてのアカウントで全面的なログを有効にし、ログ情報を一元的な場所に送信することを強くお勧めします。AWS Control Tower では、この一元的な場所はログアーカイブアカウントであり、このアカウントが Amazon S3 ログバケットを提供します。
- ベストプラクティス: AWS Control Tower で組織レベルの CloudTrail 証跡をオプトアウトする場合は、独自の証跡をセットアップして管理します。
- ベストプラクティス: AWS Control Tower 環境を操作する際には、テスト環境をセットアップします。

2.x ランディングゾーンバージョンから 3.x ランディングゾーンバージョンに移行する利点

- ホームリージョンでのみ AWS Config リソースを記録するため、グローバルリソースを管理するとコスト削減につながります。
- 独自の KMS キーを使用して AWS CloudTrail 証跡を暗号化する
- ログの保持期間をカスタマイズできる
- 必須コントロールが強化される
- 利用可能なコントロールの数が増える
- と統合 AWS Security Hub CSPM

- Python ランタイムの更新

2.x ランディングゾーンバージョンから 3.x ランディングゾーンバージョンに移行する際の注意事項

- ランディングゾーン 3.0 以降では、AWS Control Tower は が AWS 管理するアカウントレベルの AWS CloudTrail 証跡をサポートしなくなりました。
- AWS Control Tower が管理する組織レベルの証跡を選択するか、それをオプトアウトして独自の CloudTrail 証跡を管理するかを選択できます。
- OU 内の一部のアカウントが AWS Control Tower に登録されておらず、アカウントレベルの独自の証跡を保持する必要がある場合は特に、コストが二重に発生する可能性があります。

組織レベルの CloudTrail 証跡の選択に関する考慮事項

- 3.0 以降にアップグレードすると、AWS Control Tower は最初に作成したアカウントレベルの証跡を 24 時間後に削除します。[\[例外\]](#)
- これらの証跡のデータは失われません。既存のログは、証跡が削除されても保持されます。
- AWS Control Tower は、アカウントレベルの証跡を組織レベルの証跡と区別するために、同じ Amazon S3 バケットに証跡の新しいパスを作成します。
 - アカウントの証跡ログのパスは、/orgId/AWSLogs/... という形式を取ります。
 - 組織の証跡ログのパスは、/orgId/AWSLogs/orgId/... という形式を取ります。
- ユーザーがデプロイした追加の CloudTrail 証跡 (AWS Control Tower によってデプロイされていない証跡) はそのままになります。
- 登録済み OU に未登録のアカウントがある場合、AWS Control Tower に登録されていないアカウントも含めて、すべてのアカウントが組織レベルの証跡に含まれます。
- 連結アカウントの Amazon CloudWatch アラームはトリガーされません。
- 組織レベルの証跡をオプトアウトしても、AWS Control Tower は証跡を作成しますが、そのステータスを [オフ] に設定します。
- ベストプラクティスとして、AWS Control Tower で組織レベルの証跡をオプトアウトする場合は、独自の CloudTrail 証跡をセットアップして管理する必要があります。

組織レベルの証跡の利点

- 組織の証跡は、OU 内のすべてのアカウントで機能します。
- ログに記録された項目は標準化されており、アカウントユーザーが変更することはできません。

テスト環境を検討する

ランディングゾーンをアップグレードすると、AWS Control Tower は共有アカウントと基礎 OU のみを変更します。ワークロードアカウントや OU は変更しません。ただし、ベストプラクティスとして、AWS Control Tower 環境を操作する際には、テスト環境をセットアップすることをお勧めします。隔離されたテスト環境内では、AWS Control Tower ランディングゾーンのアップグレードやサービスコントロールポリシー (SCP) に加える変更をテストしたり、環境に適用するコントロールをテストしたりすることができます。この推奨事項は、規制対象の業界で事業を行っている場合に特に役立ちます。

更新時の一般的なエラーのチェックリスト

AWS Control Tower ランディングゾーンを 2.x バージョンから 3.x バージョンに更新する際の一般的なエラーを回避するために実行できるタスクの短いリストを次に示します。

基本的な更新チェックリスト

- ランディングゾーンを確認します。
 - AWS Control Tower サービスに移動し、組織単位とアカウントページを確認し、アカウントの状態が登録済みと登録済みに設定されていることを確認します。
 - 該当する場合は、カスタマイズパイプラインの最後の実行が成功したことを確認します。
 - 以前にバケットポリシーに加えられた変更は上書きされるため、監査アカウントの Amazon S3 集中ロギングバケットを確認します。
- AWS Control Tower によって所有されていない SCP が、更新を実行している管理ロールのメンバーアカウントまたは管理アカウントのアクションの実行から `AWSControlTowerExecution` ロールを制限しないことを確認します。

AI ベースのサービスと AWS Control Tower

AWS上の AI ベースのサービスによるデータの保存をオプトアウトするためのサービスコントロールポリシー (SCP) を作成できます。これらの SCP ポリシーは、Amazon Rekognition や Amazon CodeWhisperer などの AI ベースのサービスが、他の AI ベースの AWS サービスを改善するためにデータを保存して使用できないことを指定します。

これらの AI オプトアウト SCP ポリシーは、組織全体、OU、または特定のアカウントに適用できます。ポリシーはグローバルに有効です。これらのポリシーの詳細については、AWS Organizations ドキュメントの [AI サービスのオプトアウトポリシー](#) を参照してください。

AI を使用する AWS サービスのリストとポリシーの例については、AWS Organizations 「ユーザーガイド」の [「AI サービスのオプトアウトポリシーの構文と例」](#) を参照してください。

AWS Control Tower での設定更新管理

ランディングゾーンを最新の状態に保つのは、中央クラウド管理者のチームのメンバーの責任です。ランディングゾーンを更新すると、AWS Control Tower にパッチが適用され、更新されます。さらに、潜在的なコンプライアンスの問題からランディングゾーンを保護するために、中央クラウド管理者のチームのメンバーは、ドリフトの問題が検出され、報告されたらすぐに解決する必要があります。

Note

AWS Control Tower コンソールは、ランディングゾーンを更新する必要があるときを示します。更新するオプションが表示されていない場合、ランディングゾーンは既に最新です。

次の表に、AWS Control Tower ランディングゾーン更新リリースのリストと、各リリースの説明へのリンクを示します。

バージョン	リリース日	説明
4.0	11-17-2025	ランディングゾーンバージョン 4.0
3.3	12-12-2023	ランディングゾーンバージョン 3.3
3.2	6-09-2023	ランディングゾーンバージョン 3.2
3.1	2-09-2023	ランディングゾーンバージョン 3.1
3.0	7-26-2022	ランディングゾーンバージョン 3.0
2.9	4-22-2022	ランディングゾーンバージョン 2.9

バージョン	リリース日	説明
2.8	2-10-2022	ランディングゾーンバージョン 2.8
2.7	4-8-2021	ランディングゾーンバージョン 2.7
2.6	12-29-2020	ランディングゾーンバージョン 2.6
2.5	11-18-2020	ランディングゾーンバージョン 2.5
2.4	なし	なし
2.3	3-5-2020	ランディングゾーンバージョン 2.3
2.2	11-13-19	ランディングゾーンバージョン 2.2
2.1	6-24-19	ランディングゾーンバージョン 2.1

ランディングゾーンを更新するたびに、ランディングゾーンの設定を変更する機会があります。

更新の利点

- 管理対象リージョンを変更できる
- ログの保持ポリシーを変更することができる
- リージョン拒否コントロールを追加または削除できる
- KMS AWS 暗号化キーを適用できます
- 組織レベルの CloudTrail 証跡をアクティブ化または非アクティブ化できる
- [ランディングゾーンのドリフト](#)を解決できる

ランディングゾーンを更新すると、AWS Control Tower の最新機能が自動的に提供されます。[Landing zone settings] (ランディングゾーン設定) ページで現在のランディングゾーンのバージョンを確認してください。

更新が失敗しても、AWS Control Tower は以前のランディングゾーンバージョンにロールバックしません。ランディングゾーンが不確定な状態になる場合があります。その場合は、AWS サポートにお問い合わせください。更新の失敗をトラブルシューティングする方法の詳細については、「[ランディングゾーンを更新できない](#)」を参照してください。

ランディングゾーンを更新するときに、未使用の AWS アイデンティティセンター (旧称 SSO) AWS マッピングをクリアする場合があります。詳細については、「[Field Notes: Clear Unused IAM Identity Center Mappings Automatically During AWS Control Tower Upgrades](#)」(フィールドノート:AWS Control Tower のアップグレード中に未使用の IAM ID Center のマッピングを自動的に消去する) を参照してください。

更新とリセットの前提条件 — リクエスト支払いをオフにする

ランディングゾーンを更新またはリセットする前に、ログアーカイブアカウントの Amazon S3 ログ記録バケットで、[リクエスト支払い] 機能が有効になっていないことを確認します。[更新] または [リセット] プロセスを開始する前に、この機能をオフにする必要があります。AWS Control Tower がログ記録バケットを設定するときに、この機能は有効化されません。したがって、この機能をオフにする必要があるのは、後でユーザーがリクエスト支払い機能を有効にした場合のみです。詳細については、「[CloudTrail の Amazon S3 バケットポリシー](#)」と「[リクエスト支払いバケットの使用](#)」を参照してください。

ランディングゾーンの更新について

ガバナンスのドリフトを修正するには、または AWS Control Tower の新しいバージョンに移動するには、更新が必要です。AWS Control Tower の完全な更新を実行するには、最初にランディングゾーンを更新してから、登録済みアカウントを個別に更新する必要があります。3 種類の更新を異なるタイミングで実行することが必要になる場合があります。

- ランディングゾーンの更新: ほとんどの場合、この種類の更新は、[Landing zone settings] (ランディングゾーン設定) ページで [Update] (更新) を選択して実行します。特定の種類のドリフトを解決するには、ランディングゾーンの更新が必要になる場合があります。必要に応じて [リセット] を選択できます。

- 1 つ以上の個々のアカウントの更新: 関連する情報が変更された場合、または特定の種類のドリフトが発生した場合は、アカウントを更新する必要があります。アカウントが更新を必要とする場合、アカウントのステータスは [Accounts] (アカウント) ページで [Update available] (更新プログラムが利用できます) と表示されます。

1 つのアカウントを更新するには、アカウントの詳細ページに移動し、[Update account] (アカウントの更新) を選択します。アカウントを更新するには、[Re-register OU] (OU を再登録) を選択して手動プロセスを使用するか、このページの後のセクションで説明する自動スクリプティングアプローチを使用することもできます。

- 完全な更新: 完全な更新には、ランディングゾーンの更新が含まれ、その後に登録済み OU に登録されているすべてのアカウントの更新が続きます。3.0、3.2 などの AWS Control Tower の新しいリリースでは、完全な更新が必要です。完全な更新プロセスを容易にするために、アカウント数が 1000 以下の OU の場合は、[OU を再登録] を選択してその OU 内のすべてのアカウントを更新し、OU ごとに [OU を再登録] コマンドを繰り返します。

ランディングゾーンの更新の詳細については、「[ランディングゾーンの更新のベストプラクティス](#)」を参照してください。

Note

ランディングゾーンの更新が完了した後で、更新を元に戻したり、以前のバージョンにダウングレードしたりすることはできません。

ランディングゾーンを更新する

AWS Control Tower ランディングゾーンを更新する最も簡単な方法は、[Landing zone settings] (ランディングゾーン設定) ページを使用することです。このページは、AWS Control Tower ダッシュボードの左側ナビゲーションで [Landing zone settings] (ランディングゾーン設定) を選択すると表示されます。

[Landing zone settings] (ランディングゾーン設定) ページには、ランディングゾーンの現在のバージョンが表示され、利用可能な更新バージョンが一覧表示されます。バージョンを更新する必要がある場合は、[Update] (更新) ボタンを選択できます。

Note

または、ランディングゾーンを手動で更新することもできます。[Update] (更新) ボタンを使用するか手動で処理するかにかかわらず、更新にはほぼ同じ時間がかかります。ランディングゾーンのみを手動で更新するには、以下のステップ 1 と 2 を参照してください。

標準的な更新手順

以下に示しているのは、コンソールから AWS Control Tower の完全な更新を行うステップです。個々のアカウントを更新するには、「[コンソールでアカウントを更新する](#)」を参照してください。

OU ごとに任意の数のアカウントを使用してランディングゾーンを更新するには

1. ウェブブラウザを開き、AWS Control Tower コンソール (<https://console.aws.amazon.com/controltower/home/update>) に移動します。
2. ウィザードの情報を確認し、[Update] (更新) を選択します。これにより、ランディングゾーンのバックエンドおよび共有アカウントが更新されます。このプロセスには 30 分と少しかかる可能性があります。
3. メンバーアカウントを更新します (1000 を超えるアカウントを含む OU の場合、この手順に従う必要があります)。
4. 左側のナビゲーションペインから、[Organization] (組織) を選択します。
5. 各アカウントを更新するには、[コンソールでアカウントを更新する](#) に記載されている手順に従います。

オプションで [Re-register OU] (OU の再登録) を使用してアカウントを更新する

アカウント数が 1000 未満の登録済み AWS Control Tower OUs の場合は、ダッシュボードの OU ページに移動し、OU の再登録を選択してその OU のアカウントを更新できます。

ランディングゾーンバージョンを選択する

AWS Control Tower ランディングゾーンバージョン 3.1 以降を実行している場合は、ランディングゾーン設定の更新またはリセットオペレーションを実行するときに、現在のバージョンを維持する

か、新しいバージョンにアップグレードするかを選択できます。ほとんどの場合、ドリフトを修復するのに最適な方法はリセットオペレーションです。

ランディングゾーンバージョンは、AWS Control Tower コンソールで、または AWS Control Tower API を使用して選択できます。

 Note

中間バージョンをスキップするランディングゾーンバージョンをデプロイすることを選択した場合、例えば 3.1 から 3.3 に移行すると、AWS Control Tower は更新オペレーションの一環として中間バージョンを自動的にデプロイします。

会話の中では、新しいバージョンに移行することを、単なる更新ではなくアップグレードと呼ぶことがよくあります。この 2 つの概念は異なります。新しいバージョンにアップグレードしなくても、例えば管理するリージョンを変更することで、ランディングゾーン設定を更新できるためです。コンソールで [更新] ボタンを選択すると、現在のランディングゾーンバージョンとデプロイするランディングゾーンバージョンに基づいて、インプレース更新またはアップグレードオペレーションが実行されます。

ランディングゾーンバージョンの選択 – コンソールでの手順

1. AWS Control Tower コンソールから [ランディングゾーン設定] ページに移動します。使用可能なランディングゾーンの表で、新しいバージョンを選択します。バージョン 3.1 以降を選択することに注意してください。3.1 より前のバージョンは、この機能と互換性がありません。
2. 表からバージョンを選択すると、実行可能なアクションが表示されます。[更新] は、現在のバージョンが選択したバージョンより前の場合に実行できます。[リセット] は、現在のバージョンが 3.1 以降の場合に実行できます。
3. バージョンを選択したら、画面の右上の領域にある [更新] ボタンまたは [リセット] ボタンを選択します。
4. デプロイ用に選択したランディングゾーンバージョンを示す確認画面が表示されます。続行するには、右下の [次へ] を選択します。更新オペレーションには数分以上かかる場合があります。
5. ランディングゾーンの更新後、アカウントの更新が必要になる場合があります。アカウントの更新を行う最も簡単な方法は、登録された OU ごとに [OU を 再登録] プロセスを実行することです。

アカウントの更新、ランディングゾーンバージョン、およびベースライン

AWS Control Tower ランディングゾーンは、一連のベースライン設定に対応する AWS リソースです。ベースラインとランディングゾーンバージョンが 1 対 1 で対応しているわけではありません。[OU ベースラインとランディングゾーンバージョンの互換性](#)を示す表を参照できます。

ベースラインバージョンを飛ばすときは、ランディングゾーンの更新後にアカウントを更新する必要があります。例えば、3.1 から 3.2 にアップグレードする場合、これらのランディングゾーンバージョンは同じベースラインを共有しているため、アカウントを更新する必要はありません。

これに対して、3.1 から 3.3 にアップグレードする場合、ベースラインバージョンは 3.2～3.3 に対応する 4.0 であるため、アカウントを更新する必要があります。

ランディングゾーンバージョンとベースラインの関係の詳細については、「[OU ベースラインとランディングゾーンバージョンの互換性](#)」を参照してください。

ランディングゾーンの更新中に AWS CloudTrail 証跡を保持する

AWS Control Tower でランディングゾーンバージョンをアップグレードするときにアカウントレベルの AWS CloudTrail の証跡を保持することを選択します。

前提条件

- ランディングゾーンのバージョンが 3.0 より小さい。
- 最新の作成または更新オペレーションが成功している。

アカウントレベルの証跡を保持し、組織レベルの CloudTrail 証跡にオプトインするには

- アカウントを許可リストに登録するには、AWS サポートにお問い合わせください。
- サポートチームは、ターゲットアカウントがいつ許可リストに登録されたかを確認します。
- 確認後、ランディングゾーンをバージョン 3.1 以降に更新し、AWS CloudTrail 設定 – 有効を選択します。

アカウントレベルの証跡を保持し、AWS Control Tower によって管理される CloudTrail の証跡をオプトアウトするには

- アカウントを許可リストに登録するには、AWS サポートにお問い合わせください。

2. サポートチームは、ターゲットアカウントがいつ許可リストに登録されたかを確認します。
3. 確認後、ランディングゾーンをバージョン 3.1 以降に更新し、AWS CloudTrail 設定 – 有効でないを選択します。

⚠ Important

アカウントレベルの CloudTrail 証跡が保持されると、許可リストから証跡を削除したり、アカウントを削除したりすることはできません。

アカウントレベルの証跡を保持するためのサポートリクエストを行う方法

ランディングゾーンの更新中にアカウントレベルの証跡を保持する必要がある場合は、AWS サポートに問い合わせ、AWS Control Tower の許可リストにアカウントを追加する必要があります。サポートチケットを送信するには、以下の手順に従います。

1. AWS マネジメントコンソールにサインインします。
2. AWS サポートセンターに移動します。
3. [ケースを作成] を選択します。
4. [ケースタイプ] で、[テクニカルサポート] を選択します。
5. [サービス] で、[AWS Control Tower] を選択します。
6. [カテゴリ] で、[一般的なガイダンス] を選択します。
7. [件名] 行には、以下のフレーズを含めます。

Allow retention of account-level trails during Landing Zone update

8. [説明] フィールドで、以下の詳細を指定します。
 - AWS 管理アカウント番号
 - 選択した AWS Control Tower 環境のホームリージョン
9. サポートケースフォームの他の必須フィールドに入力します。
10. [送信] を選択してサポートケースを作成します。

チケットを送信すると、AWS サポートはリクエストを確認し、必要に応じてアカウントを許可リストに追加します。サポートケースのコミュニケーションチャンネルを通じて、詳細な手順と確認を受け取ります。

Note

許可リストに登録された後にアカウントレベルの証跡を削除するには、管理アカウントを使用して CloudFormation スタックセットまたは特定のスタックインスタンスを削除します。スタック内のすべてのリソースが削除されます。

リセットと再登録でドリフトを解決する

ドリフトは、ユーザーおよび組織のメンバーがランディングゾーンを使用する際に発生することが多いです。

ドリフト検出は、AWS Control Tower で自動的に行われます。SCP の自動スキャンは、ドリフトを解決するために行う必要のある変更や構成の更新を必要とするリソースを特定するのに役立ちます。

多くの種類のドリフトを修復するには、コンソールの [ランディングゾーン設定] ページで [リセット] を選択します。また、コンソールで OU の [再登録] を選択することで、いくつかの種類のドリフトを解決することもできます。コントロールの場合、ResetEnabledControl API を呼び出すことで、ドリフトをプログラムで解決できます。ドリフトの種類とその解決方法の詳細については、「[ガバナンスドリフトのタイプ](#)」と「[AWS Control Tower でドリフトを検出および解決する](#)」を参照してください。

ドリフトの解決が発生する特殊なケースの 1 つにロールドリフトがあります。必要なロールが利用できない場合、コンソールに警告ページと、ロールを復元する方法に関するいくつかの指示が表示されます。ロールドリフトが解決されるまで、ランディングゾーンは利用できません。このドリフトのリセットは、ランディングゾーンの完全なリセットと同じではありません。ドリフトの詳細については、[すぐに解決すべきドリフトのタイプ](#) というセクションの「必要なロールを削除しない」を参照してください。

⚠ ランディングゾーンバージョンのドリフトを解決するアクションを実行する際には、2 つの動作が可能です。

- 最新のランディングゾーンバージョンを使用している場合、[リセット] を選択してから[確認] を選択すると、ドリフトしたランディングゾーンリソースは保存済みの AWS Control Tower 設定にリセットされます。ランディングゾーンバージョンは変わりません。

- 最新バージョンでない場合は、[更新] を選択する必要があります。ランディングゾーンは最新のランディングゾーンバージョンにアップグレードされます。このプロセスの一環としてドリフトが解決されます。

自動化によるアカウントのプロビジョニングと更新

Note

単一アカウントのプロビジョニング、更新、カスタマイズは、AWSControlTowerBaseline を有効にした組織単位 (OU) をターゲットにする必要があります。OU で AWSControlTowerBaseline が有効になっていない場合は、アカウントの自動登録を有効にするか、EnabledBaseline で ResetEnabledBaseline API と ResetEnabledControl APIs を使用して、その OU EnabledControls でアカウントを登録できます。EnabledBaselines AWSControlTowerBaseline の詳細については、「」を参照してください[OU レベルで適用されるベースラインタイプ](#)。

AWS Control Tower の各アカウントは、いくつかの方法でプロビジョニングまたは更新できます。

- アカウントは、AWS Control Tower Account Factory for Terraform (AFT) により、プロビジョニングおよび更新できます。詳細については、「[AWS Control Tower Account Factory for Terraform \(AFT\) の概要](#)」を参照してください。
- アカウントは、Customizations for AWS Control Tower (CfCT) を使用して更新できます。詳細については、「[AWS Control Tower のカスタマイズ \(CfCT\) の概要](#)」を参照してください。
- スクリプト自動化: API アプローチを使用してアカウントを更新する場合は、Service Catalog の [API フレームワーク](#) と AWS CLI を使用して一括処理でアカウントを更新できます。各アカウントの Service Catalog の [UpdateProvisionedProduct](#) API を呼び出します。この API を使用して、アカウントを 1 つずつ更新するスクリプトを書くことができます。このアプローチの詳細については、ガバナンス用のリージョンを追加するときに、ブログ記事「[新しい AWS リージョンでのガードレールの有効化](#)」を参照してください。

一度に 5 つまでアカウントを更新できます。少なくとも 1 つのアカウントの更新を無事に完了してから、次のアカウントの更新を開始してください。したがって、アカウントが多くある場合は、処理に時間がかかることはありますが、複雑ではありません。この方法の詳細については、「[Service Catalog API による AWS Control Tower のアカウントプロビジョニングの自動化](#)」を参照してください。

動画チュートリアル

[動画チュートリアル](#) は、スクリプトによるアカウントの自動プロビジョニング用に設計されていますが、この手順はアカウントの更新にも適用されます。ProvisionProduct API の代わりに UpdateProvisionedProduct API を使用します。

スクリプトによるオートメーションの追加のステップとして、AWS Control Tower UpdateLandingZone ライフサイクルイベントの [Succeed] (成功) ステータスを確認します。これは、動画で説明されているように個々のアカウントの更新を開始するためのトリガーとして使用します。ライフサイクルイベントは一連のアクティビティの完了を示すため、このイベントが発生するとランディングゾーンの更新が完了したことを意味します。アカウントの更新を開始する前に、ランディングゾーンの更新が完了している必要があります。ライフサイクルイベントの操作の詳細については、「[ライフサイクルイベント](#)」を参照してください。

以下も参照してください。

- [AWS CloudShellを使用して を操作するAWS Control Tower.](#)
- [AWS Control Tower でのタスクの自動化.](#)

AWS Control Tower でのタスクの自動化

多くのユーザーは、アカウントのプロビジョニング、コントロールの割り当て、監査など、AWS Control Tower のタスクを自動化することを好みます。これらの自動アクションは、次のコールを使って設定できます。

- [AWS Service Catalog API](#)
- [AWS Organizations API](#)
- [AWS Control Tower API](#)
- [AWS CLI](#)

[追加情報とリンク](#) ページには、AWS Control Tower でタスクを自動化するのに役立つ多くの優れた技術ブログ記事へのリンクが含まれています。次のセクションでは、タスクの自動化を支援する、この「AWS Control Tower ユーザーガイド」の領域へのリンクを示します。

コントロールタスクの自動化

AWS Control Tower API を使用して、コントロール (ガードレールとも呼ばれます) の適用や削除に関するタスクを自動化できます。詳細については、「[AWS Control Tower API リファレンス](#)」を参照してください。

AWS Control Tower API を使用してコントロールオペレーションを実行する方法の詳細については、ブログ記事「[AWS Control Tower releases API, pre-defined controls to your organizational units](#)」を参照してください。

ランディングゾーンタスクの自動化

AWS Control Tower ランディングゾーン API は、ランディングゾーンに関連する特定のタスクを自動化するのに役立ちます。詳細については、「[AWS Control Tower API リファレンス](#)」を参照してください。

OU 登録の自動化

AWS Control Tower ベースライン API は、OU の登録などの特定のタスクを自動化するのに役立ちます。詳細については、「[AWS Control Tower API リファレンス](#)」を参照してください。

アカウントの自動解約

AWS Organizations API を使用して、AWS Control Tower メンバーアカウントの閉鎖を自動化できます。詳細については、「[を使用して AWS Control Tower メンバーアカウントを閉鎖する AWS Organizations](#)」を参照してください。

アカウントのプロビジョニングと更新の自動化

AWS Control Tower Account Factory Customization (AFC) は、AWS Control Tower コンソールからアカウントを作成するのに役立ちます。カスタマイズした CloudFormation テンプレートはブループリントと呼ばれます。このプロセスは、1 つのブループリントを設定した後はパイプラインを維持しなくても、新しいアカウントを作成したり、アカウントを繰り返し更新したりできるという意味では、自動化されています。

AWS Control Tower Account Factory for Terraform (AFT) は、GitOps モデルに従い、AWS Control Tower でのアカウントプロビジョニングとアカウント更新のプロセスを自動化します。詳細については、「[AWS Control Tower Account Factory for Terraform \(AFT\) によるアカウントのプロビジョニング](#)」を参照してください。

AWS Control Tower (CfCT) のカスタマイズは、AWS Control Tower ランディングゾーンをカスタマイズし、AWS ベストプラクティスとの整合性を保つのに役立ちます。CfCT カスタマイズは、AWS CloudFormation テンプレート、サービスコントロールポリシー (SCPs)、リソースコントロールポリシー (RCPs)。詳細については、「[AWS Control Tower のカスタマイズ \(CfCT\) の概要](#)」を参照してください。

自動アカウントプロビジョニングの詳細と動画については、「[チュートリアル: AWS Control Tower を使用した自動アカウントプロビジョニング](#)」および「[IAM ロールを使用した自動アカウントプロビジョニング](#)」を参照してください。

[スクリプトによるアカウントの更新](#)も参照してください。

プログラムによるアカウントの監査

プログラムによるアカウントの監査の詳細については、「[Programmatic roles and trust relationships for the AWS Control Tower audit account](#)」(AWS Control Tower 監査アカウントのプログラムによるロールと信頼関係) を参照してください。

その他のタスクの自動化

自動リクエストという方法で特定の AWS Control Tower Service Quotas を増やす方法については、「[Automate Service Limit Increases](#)」(サービス制限引き上げの自動化) というビデオをご覧ください。

オートメーションと統合のユースケースについて説明している技術的なブログについては、「[Automation and integration](#)」(オートメーションと統合)を参照してください。

GitHub では 2 つのオープンソースのサンプルが用意されており、セキュリティに関連する特定のオートメーションタスクに役立ちます。

- [aws-control-tower-org-setup-sample](#) というサンプルでは、セキュリティ関連サービスの委任管理者として監査アカウントの設定を自動化する方法について説明しています。
- [aws-control-tower-account-setup-using-step-functions](#) というサンプルでは、新規アカウントのプロビジョニングおよび設定時に、ステップ関数を使用してセキュリティのベストプラクティスを自動化する方法について説明しています。このサンプルには、組織共有 AWS Service Catalog ポートフォリオにプリンシパルを追加したり、組織全体の AWS IAM アイデンティティセンターグループを新しいアカウントに自動的に関連付けたりすることが含まれます。また、各リージョンのデフォルトの VPC を削除する方法についても説明します。

「AWS セキュリティリファレンスアーキテクチャ」には、AWS Control Tower に関連するタスクを自動化するためのコード例が含まれています。詳細については、「[AWS 規範的ガイダンス](#)」のページと[関連付けられた GitHub リポジトリ](#)を参照してください。

CLI での作業を容易にする AWS サービスである AWS CloudShell で AWS Control Tower AWS を使用する方法については、[AWS CloudShell と AWS CLI](#)」を参照してください。

AWS Control Tower は のオーケストレーションレイヤーであるため AWS Organizations、APIs と AWS CLI を使用して他の多くの AWS サービスを利用できます。詳細については、「[関連 AWS サービス](#)」を参照してください。

AWS CloudShellを使用して を操作するAWS Control Tower

AWS CloudShellは、CLI AWSでの作業を容易にするAWSサービスです。これは、 から直接起動できるブラウザベースの事前認証済みシェルですAWS マネジメントコンソール。コマンドラインツールをダウンロードまたはインストールする必要はありません。AWS Control Towerおよびその他のAWSサービスのAWS CLIコマンドは、任意のシェル (Bash、PowerShell、または Z シェル) から実行できます。

[から を起動AWS CloudShellAWS マネジメントコンソール](#)すると、コンソールへのサインインに使用したAWS認証情報が新しいシェルセッションで使用できます。AWS Control Towerおよびその他のAWSサービスとやり取りするときに設定認証情報の入力をスキップできます。シェルのコン

コンピューティング環境にプリインストールされているAWS CLIバージョン 2 を使用します。事前認証済みですAWS CloudShell。

の IAM アクセス許可を取得するAWS CloudShell

AWS Identity and Access Managementは、管理者が IAM ユーザーと IAM Identity Center ユーザーにアクセス許可を付与できるようにするアクセス管理リソースを提供しますAWS CloudShell。

管理者がユーザーにアクセス権を付与する最も簡単な方法は、AWS管理ポリシーを使用することです。[AWSマネージドポリシー](#)は、AWSが作成および管理するスタンドアロンポリシーです。CloudShell の次のAWS管理ポリシーを IAM ID にアタッチできます。

- `AWSCloudShellFullAccess`: すべての機能へのフルアクセスAWS CloudShellで を使用するアクセス許可を付与します。

IAM ユーザーまたは IAM Identity Center ユーザーが実行できるアクションの範囲を制限する場合はAWS CloudShell、`AWSCloudShellFullAccess`管理ポリシーをテンプレートとして使用するカスタムポリシーを作成できます。CloudShell でユーザーが使用できるアクションの制限の詳細については、AWS CloudShell「ユーザーガイド」の「[IAM ポリシーによるAWS CloudShellアクセスと使用状況の管理](#)」を参照してください。

Note

IAM アイデンティティには、AWS Control Towerへの呼び出しを行うアクセス許可を付与するポリシーも必要です。詳細については、「[AWS Control Towerコンソールを使用するために必要なアクセス許可](#)」を参照してください。

起動AWS CloudShell

からAWS マネジメントコンソール、ナビゲーションバーで使用する以下のオプションを選択してCloudShell を起動できます。

- CloudShell アイコンを選択します。
- 検索ボックスに「cloudshell」を入力し始めてから [CloudShell] オプションを選択します。

CloudShell を起動したので、操作に必要なAWS CLIコマンドを入力できますAWS Control Tower。たとえば、AWS Configステータスを確認できます。

AWS Control Towerを通じて を操作するAWS CloudShell

AWS CloudShellから起動するとAWS マネジメントコンソール、コマンドラインインターフェイス、AWS Control Towerからすぐに のやり取りを開始できます。AWS CLIコマンドは CloudShell で標準的に機能します。

Note

AWS CLIで を使用する場合AWS CloudShell、追加のリソースをダウンロードまたはインストールする必要はありません。ユーザーはシェル内で既に認証されているので、呼び出しを行う前に認証情報を設定する必要はありません。

AWS CloudShellを使用して をセットアップするAWS Control Tower

これらの手順を実行する前に、特に明記されていない限り、ランディングゾーンのホームリージョンAWS マネジメントコンソールの にサインインし、ランディングゾーンを含む管理アカウントの管理権限を持つ IAM Identity Center ユーザーまたは IAM ユーザーとしてサインインする必要があります。

1. ランAWS Control Towerランディングゾーンの設定を開始する前に、 でAWS Config CLI コマンドを使用して設定レコーダーと配信チャネルのステータスAWS CloudShellを確認する方法は次のとおりです。

例:AWS Configステータスを確認する

表示コマンド:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-records`
- 通常の応答は "name": "default" のようになります。

2. AWS Control Towerランディングゾーンを設定する前に削除する必要がある既存のAWS Config レコーダーまたは配信チャネルがある場合は、入力できるコマンドをいくつか次に示します。

例: 既存のAWS Configリソースを管理する

削除コマンド:

- `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

のAWS Control Towerリソースを削除しないでくださいAWS Config。これらのリソースが失われAWS Control Towerと、 が整合性のない状態になる可能性があります。

詳細については、AWS Configドキュメントを参照してください。

- [設定レコーダーの管理 \(AWS CLI\)](#)

-

[配信チャネルの管理](#)

3. この例では、信頼されたアクセスを有効または無効にAWS CloudShellするために から入力するAWS CLI コマンドを示していますAWS Organizations。の信頼されたアクセスを有効または無効にする必要AWS Control TowerがないためAWS Organizations、これは一例にすぎません。ただし、アクションを自動化またはカスタマイズする場合は、他のAWSサービスの信頼されたアクセスを有効または無効にする必要がある場合がありますAWS Control Tower。

例: 信頼されたサービスのアクセスを有効化または無効化する

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

例: を使用して Amazon S3 バケットを作成するAWS CloudShell

次の例では、AWS CloudShellを使用して Amazon S3 バケットを作成し、PutObject メソッドを使用してコードファイルをそのバケットのオブジェクトとして追加できます。

1. 指定されたAWSリージョンにバケットを作成するには、CloudShell コマンドラインに次のコマンドを入力します。

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

コールが成功すると、コマンドラインに次の出力に似たサービスからのレスポンスが表示されます。

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

 Note

[バケット名の命名規則](#)に従わない (小文字しか使用しないなどの) 場合、以下のようなエラーが表示されます: CreateBucket オペレーションの呼び出し時にエラー (InvalidBucketName) が発生しました。指定されたバケットは有効ではありません。

2. ファイルをアップロードし、作成したばかりのバケットにオブジェクトとして追加するには、PutObject メソッドを呼び出します。

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

オブジェクトが Simple Storage Service (Amazon S3) バケットに正常にアップロードされると、コマンドラインに次の出力に似たサービスからのレスポンスが表示されます。

```
{
  "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebee56\""
}
```

ETag は、格納されているオブジェクトのハッシュです。[これを使用して、Simple Storage Service \(Amazon S3\) にアップロードされたオブジェクトの整合性を確認できます。](#)

を使用して AWS Control Tower リソースを作成する AWS CloudFormation

AWS Control Tower はと統合されています。これは AWS CloudFormation、AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップに役立つサービスです。controls. CloudFormation provisions AWS::ControlTower::EnabledControl など、必要なすべての AWS リソースを記述するテンプレートを作成します。

を使用すると CloudFormation、テンプレートを再利用して AWS Control Tower リソースを一貫して繰り返しセットアップできます。リソースを一度記述し、複数の AWS アカウント およびリージョンで同じリソースを何度もプロビジョニングします。

AWS Control Tower および CloudFormation テンプレート

および関連サービスのリソースをプロビジョニング AWS Control Tower および設定するには、[CloudFormation テンプレート](#)を理解する必要があります。テンプレートは、JSON や YAML でフォーマットされたテキストファイルです。これらのテンプレートは、CloudFormation スタックでプロビジョニングするリソースを記述します。JSON または YAML に慣れていない場合は、CloudFormation デザイナーを使用して CloudFormation テンプレートの使用を開始できます。詳細については、「AWS CloudFormation ユーザーガイド」の「[CloudFormation Designer とは](#)」を参照してください。

AWS Control Tower は、での AWS::ControlTower::EnabledControl (コントロールリソース)、AWS::ControlTower::LandingZone (ランディングゾーン)、AWS::ControlTower::EnabledBaseline (ベースライン) の作成をサポートしています CloudFormation。これらのリソースタイプの JSON テンプレートと YAML テンプレートの例を含む詳細情報については、「AWS CloudFormation User Guide」の「[AWS Control Tower](#)」を参照してください。

Note

の EnableControl および DisableControl の更新の制限 AWS Control Tower は、100 の同時オペレーションです。

CLI とコンソール AWS Control Tower の例については、「[でコントロールを有効にする CloudFormation](#)」を参照してください。

の詳細 CloudFormation

詳細については CloudFormation、次のリソースを参照してください。

- [AWS CloudFormation](#)
- [AWS CloudFormation ユーザーガイド](#)
- [CloudFormation API リファレンス](#)
- [AWS CloudFormation コマンドラインインターフェイスユーザーガイド](#)

AWS Control Tower のランディングゾーンのカスタマイズ

AWS Control Tower のランディングゾーンでは、リージョンの選択やオプションのコントロールなどの特定の要素をコンソールで設定することができます。その他の変更は、コンソールではなくオートメーションを通じて行うことができます。

例えば、AWS CloudFormation テンプレートや AWS Control Tower ライフサイクルイベントと連携する GitOps スタイルのカスタマイズフレームワークである AWS Control Tower のカスタマイズ機能を使用して、ランディングゾーンのより広範なカスタマイズを作成できます。GitOps

AWS Control Tower コンソールからカスタマイズする

ランディングゾーンに対して以下のカスタマイズを行うには、AWS Control Tower コンソールで指定される手順に従います。

セットアップ時にカスタマイズした名前を選択する

- セットアップ時に最上位の OU 名を選択できます。AWS Organizations コンソールを使用している場合でも OUs の名前を変更できますが、で OUs を変更すると、修復可能な [ドリフト](#)が発生する AWS Organizations 可能性があります。
- 共有の [Audit] (監査) および [Log Archive] (ログアーカイブ) アカウントの名前を選択できますが、セットアップ後に名前を変更することはできません (これは 1 回限りの選択です)。

ヒント

で OU の名前を変更 AWS Organizations しても、Account Factory の対応するプロビジョニング済み製品は更新されないことに注意してください。プロビジョニングされた製品を自動的に更新し、ドリフトを回避するには、OU の作成、削除、再登録などの OU の操作を、AWS Control Tower から実行する必要があります。

AWS リージョンの選択

- ガバナンスの特定の AWS リージョンを選択することで、ランディングゾーンをカスタマイズできます。AWS Control Tower コンソールの手順に従います。
- ランディングゾーンを更新するときに、ガバナンスの AWS リージョンを選択または選択解除できます。

- リージョン拒否コントロールを有効または無効に設定し、管理されていない AWS リージョンのほとんどの AWS サービスへのユーザーアクセスを制御できます。

CfCT にデプロイの制限 AWS リージョン がある場所については、「」を参照してください[コントロールの制限事項](#)。

オプションのコントロールを追加してカスタマイズする

- 強く推奨されるコントロールと選択的コントロールはオプションです。つまり、どのコントロールを有効にするかを選択することで、ランディングゾーンのエンフォースメントレベルをカスタマイズできます。[オプションのコントロール](#)はデフォルトでは有効になっていません。
- オプションの[データレジデンシーコントロール](#)では、データを保存し、アクセスを許可するリージョンをカスタマイズできます。
- 統合された Security Hub CSPM 標準の一部であるオプションのコントロールを使用すると、AWS Control Tower 環境をスキャンしてセキュリティリスクを確認できます。
- オプションのプロアクティブコントロールを使用すると、プロビジョニング前に CloudFormation リソースをチェックして、新しいリソースが環境のコントロール目標に準拠していることを確認することができます。

AWS CloudTrail 証跡をカスタマイズする

- ランディングゾーンをバージョン 3.0 以降に更新する場合、AWS Control Tower によって管理される組織レベルの CloudTrail 証跡をオプトインするかオプトアウトするかを選択できます。この選択は、ランディングゾーンを更新するたびに変更できます。AWS Control Tower は管理アカウントに組織レベルの証跡を作成し、その証跡のステータスはユーザーの選択に基づいてアクティブまたは非アクティブのどちらかになります。ランディングゾーン 3.0 は、アカウントレベルの CloudTrail 証跡をサポートしていません。ただし、これらが必要な場合は、独自の証跡を設定および管理できます。証跡が重複すると、追加料金が発生する場合があります。

コンソールでカスタマイズされたメンバーアカウントを作成する

- AWS Control Tower コンソールから、カスタマイズされた AWS Control Tower メンバーアカウントを作成したり、既存のメンバーアカウントを更新してカスタム設定を追加したりできます。詳細については、「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。

AWS Control Tower コンソールの外部でカスタマイズを自動化する

一部のカスタマイズは AWS Control Tower コンソールでは利用できませんが、他の方法で実装することができます。例:

- GitOps スタイルのワークフローで、[Account Factory for Terraform \(AFT\)](#) を使用してプロビジョニング中にアカウントをカスタマイズできます。

AFT は、[AFT リポジトリ](#) で使用可能な Terraform モジュールでデプロイされます。

- テンプレート AWS CloudFormation とサービスコントロールポリシー (SCPs) に基づいて構築された機能のパッケージである [Customizations for AWS Control Tower \(CfCT\)](#) を使用して、[AWS Control Tower](#) ランディングゾーンをカスタマイズできます。CfCT カスタムのテンプレートとポリシーを組織内の個々のアカウントと組織単位 (OU) にデプロイできます。

CfCT のソースコードは [GitHub リポジトリ](#) にあります。

- Landing Zone Accelerator (LZA) on AWS を使用して、AWS Control Tower ランディングゾーンをカスタマイズできます。LZA ソリューションは、AWS ベストプラクティスに合致し、複数のグローバルコンプライアンスフレームワークに準拠するように設計されています。AWS Control Tower を基礎ランディングゾーンとしてデプロイし、必要に応じて LZA でランディングゾーンの機能を強化することをお勧めします。詳細については、「[AWS Control Tower and Landing zone accelerator](#)」を参照してください。

AWS Control Tower と Landing Zone Accelerator

このセクションでは、AWS Control Tower と Landing Zone Accelerator (LZA) ソリューションを併用する利点について説明します。

Landing Zone Accelerator (LZA) on AWS を使用して、AWS Control Tower ランディングゾーンをカスタマイズできます。

LZA は、AWS ベストプラクティスや複数のグローバルコンプライアンスフレームワークに合わせて設計された基本的な機能をデプロイし、マルチアカウント環境の管理と管理を支援するソリューションです。LZA は AWS Cloud Development Kit (CDK) を使用して構築されています。

LZA は、安全なワークロードのホスティングに適したクラウド環境を自動的に設定します。このソリューションは、運用とガバナンスの一貫性を維持するために AWS リージョン、すべてにデプロイ

できます。LZA ソリューションは、AWS ベストプラクティスに合致し、複数のグローバルコンプライアンスフレームワークに準拠するように設計されています。

AWS Control Tower を基礎ランディングゾーンとしてデプロイし、必要に応じて LZA でランディングゾーンの機能を強化することをお勧めします。LZA と AWS Control Tower を組み合わせることで、マルチアカウント環境の管理とガバナンスに役立つ包括的なノーコードソリューションが得られます。これは、規制の厳しいワークロードと複雑なコンプライアンス要件をサポートするように設計されています。AWS Control Tower と Landing Zone Accelerator を併用すれば、セキュリティ、コンプライアンス、運用機能も含めて、プラットフォームの準備を確実なものとすることができます。

LZA のソースコードは [GitHub リポジトリ](#) にあります。

LZA と AWS Control Tower を組み合わせる方法の詳細については、「[LZA Implementation Guide](#)」を参照してください。

AWS Control Tower のカスタマイズ (CfCT) のメリット

AWS Control Tower のカスタマイズ (CfCT) と呼ばれる機能パッケージを使用すると、AWS Control Tower コンソールで作成できるものよりも広範なカスタマイズをランディングゾーンのために作成することができます。これは GitOps スタイルの自動化されたプロセスを提供します。ビジネス要件を満たすようにランディングゾーンを作り直すことができます。

このinfrastructure-as-codeのカスタマイズプロセスは、AWS CloudFormation テンプレートを AWS サービスコントロールポリシー (SCPs) および AWS Control Tower [ライフサイクルイベント](#)と統合し、リソースのデプロイがランディングゾーンと同期されたままになるようにします。例えば、Account Factory を使用して新しいアカウントを作成すると、アカウントおよび OU にアタッチされたリソースを自動的にデプロイできます。

Note

Account Factory および AFT とは異なり、CfCT は新しいアカウントの作成専用ではなく、指定したリソースをデプロイしてランディングゾーン内のアカウントと OU をカスタマイズすることを目的としています。

Note

CfCT で設定されたターゲット組織単位 (OU) では、AWS Control Tower で AWSControlTowerBaseline が有効になっている必要があります。AWSControlTowerBaseline の詳細については、「」を参照してください [OU レベルで適用されるベースラインタイプ](#)。

利点

- カスタマイズされた安全な AWS 環境の拡張 – マルチアカウント AWS Control Tower 環境をより迅速に拡張し、AWS ベストプラクティスを反復可能なカスタマイズワークフローに組み込むことができます。
- 要件のインスタンス化 – ポリシーの目的を表す AWS CloudFormation テンプレートとサービスコントロールポリシーを使用して、ビジネス要件に合わせて AWS Control Tower ランディングゾーンをカスタマイズできます。
- AWS Control Tower のライフサイクルイベントで自動化を進める — ライフサイクルイベントを使用すると、以前の一連のイベントの完了に基づいてリソースをデプロイできます。ライフサイクルイベントを使用して、アカウントや OU にリソースを自動的にデプロイできます。
- ネットワークアーキテクチャを拡張する - トランジットゲートウェイなど、接続性を向上させて保護するカスタマイズされたネットワークアーキテクチャをデプロイできます。

その他の CfCT の例

- AWS Control Tower のカスタマイズ (CfCT) を使用したネットワーキングのユースケースの例は、「アーキテクチャブログ記事」の「[サービスカタログを使用した一貫した DNS のデプロイ](#)」と「[AWS Control Tower のカスタマイズ](#)」に記載されています。CfCT AWS
- [CfCT と Amazon GuardDuty に関連する](#) 具体的な例については、[aws-samples リポジトリ](#)の GitHub で入手できます。
- CfCT に関するその他のコード例は、[aws-samples リポジトリ](#)の AWS セキュリティリファレンスアーキテクチャの一部として入手できます。これらの例の多くで、サンプルの manifest.yaml ファイルが customizations_for_aws_control_tower という名前のディレクトリに含まれています。

AWS セキュリティリファレンスアーキテクチャの詳細については、[AWS 「規範ガイダンス」 ページ](#)を参照してください。

AWS Control Tower のカスタマイズ (CfCT) の概要

AWS Control Tower (CfCT) のカスタマイズは、AWS Control Tower ランディングゾーンをカスタマイズし、AWS ベストプラクティスとの整合性を保つのに役立ちます。CfCT カスタマイズは、AWS CloudFormation テンプレートとサービスコントロールポリシー (SCPs)。

この CfCT 機能は AWS Control Tower のライフサイクルイベントと統合されているため、リソースのデプロイはランディングゾーンと同期したままになります。例えば、Account Factory を使用して新しいアカウントを作成すると、アカウントにアタッチされたすべてのリソースが自動的にデプロイされます。カスタムのテンプレートとポリシーを組織内の個々のアカウントと組織単位 (OU) にデプロイできます。

Note

CfCT で設定されたターゲット組織単位 (OU) では、AWS Control Tower で `AWSControlTowerBaseline` が有効になっている必要があります。`AWSControlTowerBaseline` の詳細については、「」を参照してください [OU レベルで適用されるベースラインタイプ](#)。

次のビデオでは、スケーラブルな CfCT パイプラインをデプロイするためのベストプラクティスと一般的な CfCT カスタマイズについて説明しています。

次のセクションでは、AWS Control Tower のカスタマイズ (CfCT) をデプロイするための、アーキテクチャ上の考慮事項と設定手順について説明します。これには、セキュリティと可用性に関する AWS ベストプラクティスに従って、必要な AWS サービスを起動、設定、実行する [AWS CloudFormation](#) テンプレートへのリンクが含まれています。

このトピックは、IT インフラストラクチャアーキテクトと、AWS クラウドでアーキテクチャの設計の実務経験を持つ開発者を対象としています。

AWS Control Tower のカスタマイズ (CfCT) の最新の更新および変更については、GitHub リポジトリの [CHANGELOG.md ファイル](#) を参照してください。

アーキテクチャの概要

CfCT をデプロイすると、Amazon S3 バケットを設定ソースとして AWS クラウドに次の環境を構築します。

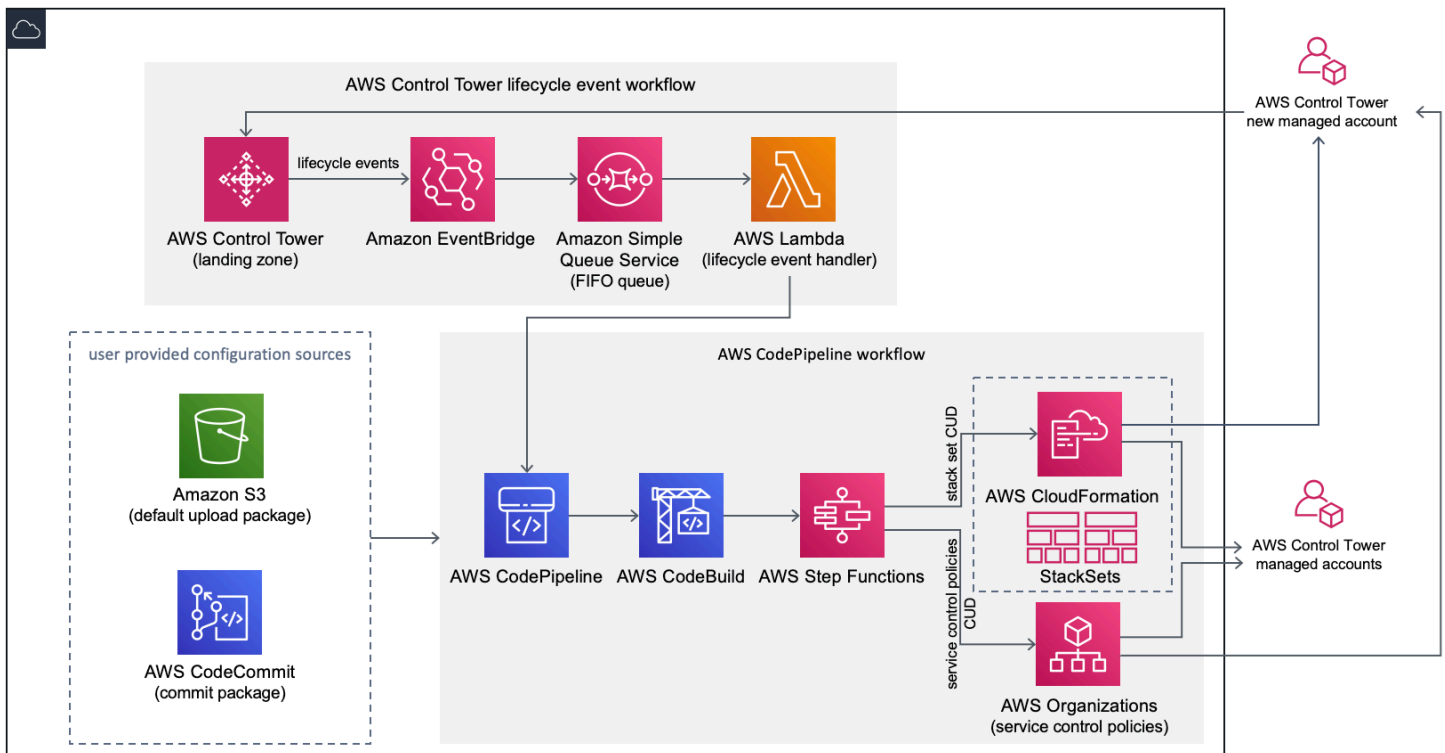


図 1: AWS Control Tower のカスタマイズに関するアーキテクチャ

CfCT には、AWS Control Tower 管理アカウントにデプロイする AWS CloudFormation テンプレートが含まれています。このテンプレートはワークフローを構築するために必要なすべてのコンポーネントを起動するため、AWS Control Tower のランディングゾーンをカスタマイズできます。

i 注意

CfCT は AWS Control Tower のホームリージョンと AWS Control Tower 管理アカウントにデプロイする必要があります。これは、AWS Control Tower のランディングゾーンがデプロイされる場所であるためです。AWS Control Tower のランディングゾーンの設定については、「[開始方法](#)」を参照してください。

CfCT をデプロイすると、[Amazon Simple Storage Service](#) (Amazon S3) によってカスタムリソースがパッケージ化され、コードパイプラインソースにアップロードされます。アップロードプロセスは、サービスコントロールポリシー (SCP) ステートマシンと [AWS CloudFormation StackSets](#) ステートマシンを自動的に呼び出して、OU レベルで SCP をデプロイするか、OU レベルまたはアカウントレベルでスタックインスタンスをデプロイします。

📘 メモ

デフォルトでは、CfCT はパイプラインソースを格納するために Amazon S3 バケットを作成します。既存の AWS CodeCommit リポジトリがある場合は、場所を [CodeCommit](#) リポジトリに変更できます。詳細については、「[Set up Amazon S3 as the configuration source](#)」(Simple Storage Service (Amazon S3) を設定ソースとしてセットアップする) を参照してください。

CfCT は次の 2 つのワークフローをデプロイします。

- [AWS CodePipeline](#) ワークフロー
- AWS Control Tower ライフサイクルイベントワークフロー

AWS CodePipeline ワークフロー

AWS CodePipeline ワークフローは AWS CodePipeline、組織内の AWS CloudFormation StackSets と SCPs の管理 [AWS Step Functions](#) を調整する、[AWS CodeBuild](#) プロジェクト、および [AWS IAM](#) を設定します。

設定パッケージをアップロードすると、CfCT はコードパイプラインを呼び出して 3 つのステージを実行します。

- 構築ステージ — AWS CodeBuild を使用して設定パッケージの内容を検証します。
- SCP ステージ — サービスコントロールポリシーステートマシンを呼び出し、AWS Organizations API を呼び出して SCPs を作成します。
- CloudFormation ステージ — スタックセットステートマシンを呼び出して、[マニフェストファイル](#) で指定したアカウントまたは OUs のリストで指定されたリソースをデプロイします。

各段階で、コードパイプラインはスタックセットおよび SCP ステップ関数を呼び出します。これにより、カスタムスタックセットと SCP がターゲットとなる個々のアカウントまたは組織単位全体にデプロイされます。

📘 注意

設定パッケージのカスタマイズの詳細については、「[CfCT カスタマイズガイド](#)」を参照してください。

AWS Control Tower ライフサイクルイベントワークフロー

AWS Control Tower で新しいアカウントが作成されると、[ライフサイクルイベント](#)が AWS CodePipeline ワークフローを呼び出すことができます。このワークフローを使用して、設定パッケージをカスタマイズできます。このパッケージは、[Amazon EventBridge](#) イベントルール、[Amazon Simple Queue Service](#) (Amazon SQS) 先入れ先出し (FIFO) キュー、および [AWS Lambda](#) 関数で構成されます。

Amazon EventBridge イベントルールが一致するライフサイクルイベントを検出すると、Amazon SQS FIFO キューにイベントを渡し、AWS Lambda 関数を呼び出し、コードパイプラインを呼び出してスタックセットと SCPs のダウンストリームデプロイを実行します。

Cost

CfCT を実行するコストは、AWS CodePipeline 実行数、AWS CodeBuild 実行期間、AWS Lambda 関数の数と期間、および発行された Amazon EventBridge イベントの数によって異なります。例えば、build.general1.small を使用して 1 か月で 100 ビルドを実行し、各ビルドが 5 分間実行される場合、CfCT の実行にかかるおおよそのコストは月額 3.00 ドルになります。詳細については、実行している AWS サービスそれぞれの価格を示した Web ページを参照してください。

Amazon Simple Storage Service (Amazon S3) バケットと AWS CodeCommit Git ベースのリポジトリリソースは、設定情報を保護するために、テンプレートを削除した後も保持されます。選択したオプションに応じて、Amazon S3 バケットに格納されているデータの量と Git リクエストの数 (Amazon S3 リソースには適用されません) に基づいて課金されます。詳細については、[Amazon S3](#) と [AWS CodeCommit](#) の価格設定を参照してください。

コンポーネントサービス

以下の AWS サービスは、AWS Control Tower のカスタマイズ (CfCT) のコンポーネントです。
CfCT

AWS CodeCommit

既存の AWS CodeCommit リポジトリがある場合は、Amazon S3 の代わりにパイプラインのソースとして設定できます。

CloudFormation テンプレートへの入力に基づいて、CfCT は Amazon Simple Storage Service セクションで説明されているのと同じサンプル設定で [AWS CodeCommit](#) リポジトリを作成できます。

CfCT AWS CodeCommit リポジトリをローカルコンピュータにクローンするには、[AWS CodeCommit ユーザーガイド](#)で説明されているように、リポジトリへの一時的なアクセスを許可する認証情報を作成する必要があります。バージョンの互換性については、「[AWS CodeCommitのセットアップ](#)」を参照してください。

Note

CodeCommit をまだ使用していない場合、Amazon S3 バケットを設定パッケージの保存場所としてセットアップすることしかできません。CodeCommit は、CfCT を初めてデプロイする場合は使用できません。

AWS CodePipeline

AWS CodePipeline は、デフォルトの Amazon S3 バケットまたは AWS CodeCommit リポジトリで実行する設定パッケージの更新に基づいて、変更を検証、テスト、実装します。設定ソースコントロールの詳細については、「[Using Amazon S3 as the Configuration Source](#)」を参照してください。パイプラインには、設定ファイルとテンプレート、コアアカウント、AWS Organizations サービスコントロールポリシー、AWS CloudFormation StackSets を検証および管理するためのステージが含まれています。パイプラインのステージの詳細については、「[CfCT カスタマイズガイド](#)」を参照してください。

AWS Key Management Service

CfCT では、[AWS Key Management Service](#) (AWS KMS) CustomControlTowerKMSKey 暗号化キーが作成されます。このキーは、Simple Storage Service (Amazon S3) 設定バケット、Amazon SQS キュー、および AWS Systems Manager パラメータストアの機密パラメータ内のオブジェクトを暗号化するために使用されます。デフォルトでは、CfCT によってプロビジョニングされたロールだけが、このキーを使用して暗号化または復号化操作を実行する許可を持ちます。設定ファイル、FIFO キュー、またはパラメータストアの SecureString 値にアクセスする場合は、管理者を CustomControlTowerKMSKey ポリシーに追加する必要があります。デフォルトで、自動キーローテーションが有効になっています。

AWS Lambda

CfCT は AWS Lambda 関数を使用して、AWS Control Tower ライフサイクルイベント中の AWS CloudFormation StackSets または AWS Organizations SCPs中にインストールコンポーネントを呼び出します。

Amazon Simple Notification Service

CfCT では、ワークフロー中に、パイプラインの承認などの通知を [Amazon Simple Notification Service](#) (Amazon SNS) のトピックに発行できます。Amazon SNS は、パイプラインの承認通知を受信することを選択した場合にのみ起動されます。

Amazon Simple Storage Service

CfCT をデプロイすると、CfCT によって一意の名前を持つ Amazon Simple Storage Service (Amazon S3) バケットが作成されます:

例: Amazon S3 バケット名

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

このバケットには、「_custom-control-tower-configuration.zip」という名前のサンプル設定ファイルが含まれています。

ファイル名の先頭にアンダースコアがあることに注意してください。

この zip ファイルには、サンプルマニフェストと、必要なフォルダ構造が記述された関連するサンプルテンプレートが用意されています。これらのサンプルは、AWS Control Tower のランディングゾーンをカスタマイズするための設定パッケージの開発に役立ちます。サンプルマニフェストは、カスタマイズを実装する際に必要となるスタックセットとサービスコントロールポリシー (SCP、Service Control Policies) に必要な設定を示します。

このサンプル設定パッケージをモデルとして使用して、カスタムパッケージを開発およびアップロードできます。これにより、CfCT 設定パイプラインが自動的にトリガーされます。

設定ファイルのカスタマイズの詳細については、「[CfCT カスタマイズガイド](#)」を参照してください。

Amazon Simple Queue Service

CfCT では、Amazon Simple Queue Service (Amazon SQS) FIFO キューを使用して、Amazon EventBridge からライフサイクルイベントをキャプチャします。AWS Lambda 関数をトリガーし、を呼び出し AWS CodePipeline で AWS CloudFormation StackSets または SCPs。SCP の詳細については、「[AWS Organizations](#)」を参照してください。

AWS Step Functions

CfCT は、カスタマイズのデプロイをオーケストレーションするために Step Functions を作成します。これらの Step Functions は設定ファイルを変換し、必要に応じて環境全体にカスタマイズをデプロイします。

AWS Systems Manager パラメータストア

[AWS Systems Manager Parameter Store](#) は CfCT 設定パラメータを格納します。このパラメータを使用すると、関連する設定テンプレートを統合できます。たとえば、一元化された Amazon S3 バケットに AWS CloudTrail データをログ記録するように各アカウントを設定できます。また、Systems Manager パラメータストアは、管理者が CfCT の入力とパラメータを表示できる一元的な場所を提供します。

デプロイに関する考慮事項

AWS Control Tower のカスタマイズ (CfCT) は、AWS Control Tower のランディングゾーンがデプロイされているものと同じアカウントとリージョンで起動してください。つまり、cfcT は AWS Control Tower のホームリージョンの AWS Control Tower 管理アカウントにデプロイする必要があります。デフォルトでは、CfCT は、そのアカウントとリージョンに設定パイプラインを設定することで、ランディングゾーンの設定パッケージを作成して実行します。

デプロイの準備

CloudFormation テンプレートを初期デプロイ用に準備するときは、いくつかのオプションがあります。設定ソースを選択し、パイプラインのデプロイの手動承認を許可できます。次の 2 つのセクションでは、これらのオプションについて詳しく説明します。

設定ソースを選択します。

デフォルトでは、テンプレートによって、サンプル設定パッケージを `_custom-control-tower-configuration.zip` と呼ばれる .zip ファイルとして保存する Amazon Simple Storage Service (Amazon S3) バケットが作成されます。Amazon S3 バケットはバージョン管理されており、必要に応じて設定パッケージを更新できます。設定パッケージの更新については、「[Using Amazon S3 as the Configuration Source](#)」(Simple Storage Service (Amazon S3) を設定ソースとして使用する) を参照してください。

アンダースコアを必ず削除する

サンプル設定パッケージファイル名はアンダースコア (_) で始まるため AWS CodePipeline は自動的に開始されません。設定パッケージのカスタマイズが完了したら、AWS CodePipelineでデプロイを開始するようにするため、アンダースコア (_) を付けずに `custom-control-tower-configuration.zip` をアップロードしてください。

既存の AWS CodeCommit Git リポジトリがある場合は、設定パッケージのストレージ場所を Amazon S3 バケットから AWS CodeCommit Git リポジトリに変更できます。これを行うには、CloudFormation パラメータで CodeCommit オプションを選択します。

圧縮の必要性の有無

デフォルトの S3 バケットを使用する場合は、設定パッケージが .zip ファイルとして利用できることを確認します。AWS CodeCommit リポジトリを使用する場合は、必ず、ファイルを圧縮せずに設定パッケージをリポジトリに配置してください。の設定パッケージの作成と保存については AWS CodeCommit、「」を参照してください [CfCT カスタマイズガイド](#)。

サンプル設定パッケージを使用して、独自のカスタム設定ソースを作成できます。カスタム設定をデプロイする準備ができたなら、設定パッケージを Simple Storage Service (Amazon S3) バケットまたは AWS CodeCommit リポジトリに手動でアップロードします。設定ファイルをアップロードすると、パイプラインが自動的に開始されます。

パイプライン設定の承認パラメータの選択

AWS CloudFormation テンプレートには、設定変更のデプロイを手動で承認するオプションがあります。デフォルトでは、手動承認は有効になっていません。詳細については、「[ステップ 1 スタックを起動する](#)」を参照してください。

手動承認が有効になっている場合、設定パイプラインは AWS Control Tower ファイルマニフェストとテンプレートに対して行われたカスタマイズを検証し、手動承認が許可されるまでプロセスを一時停止します。承認後、デプロイは必要に応じて残りのパイプラインステージの実行に移り、AWS Control Tower のカスタマイズ (CfCT) 機能を実装します。

手動承認パラメータを使用して、パイプラインでの最初の実行を拒否することで、AWS Control Tower のカスタマイズ設定が実行されないようにすることができます。このパラメータを使用する

と、実装前の最終確認として、AWS Control Tower のカスタマイズの設定変更を手動で検証することもできます。

AWS Control Tower のカスタマイズを更新するには

以前に CfCT をデプロイしたことがある場合は、CfCT フレームワークの最新バージョンを取得するように CloudFormation スタックを更新する必要があります。詳細については、「[スタックの更新](#)」を参照してください。

テンプレートおよびソースコード

AWS Control Tower のカスタマイズ (CfCT) は、AWS CloudFormation テンプレートを起動した後に管理アカウントにデプロイされます。GitHub から [テンプレート](#) をダウンロードし、このテンプレートを [AWS CloudFormation](#) で起動してください。

customizations-for-aws-control-tower.template では以下をデプロイします。

- AWS CodeBuild プロジェクト
- AWS CodePipeline プロジェクト
- Amazon EventBridge ルール
- AWS Lambda 関数
- Amazon Simple Queue Service キュー
- Amazon Simple Storage Service バケットとサンプル設定パッケージ
- AWS Step Functions

Note

テンプレートは特定の要件に基づいてカスタマイズできます。

ソースコードリポジトリ

[GitHub リポジトリ](#) では、CfCT のテンプレートとスクリプトをダウンロードし、ランディングゾーンのカスタマイズ内容を他のユーザーと共有できます。

自動デプロイ

自動デプロイを開始する前に、「[考慮事項](#)」を確認してください。このセクションのステップバイステップの手順に従って、ソリューションを設定し、AWS Control Tower 管理アカウントにデプロイします。

デプロイ時間: 約 15 分

前提条件

CfCT は、AWS Control Tower の管理アカウントと AWS Control Tower のホームリージョンにデプロイする必要があります。ランディングゾーンを設定していない場合は、「[開始方法](#)」を参照してください。

デプロイ手順

CfCT をデプロイする手順は、2 つの主要なステップで構成されます。詳細な手順については、各ステップのリンクをクリックしてください。

[ステップ 1. スタックを起動する](#)

- CloudFormation テンプレートを管理アカウントに起動します。
- テンプレートパラメータを確認して、必要に応じて調整します。

[ステップ 2. カスタムパッケージを作成する](#)

- カスタム設定パッケージを作成します。

Important

正しい AWS CloudFormation をダウンロードして CfCT を起動するには、このセクションに示している GitHub リンクに従ってください。以前に指定した S3 バケットへの古いリンクは使用しないでください。

ステップ 1. スタックを起動する

このセクションの CloudFormation テンプレートによって、AWS Control Tower のカスタマイズ (CfCT) がアカウントにデプロイされます。

i 注意

CfCT の実行中に使用される AWS サービスのコストは、お客様の負担となります。詳細については、「[Cost](#)」を参照してください。

1. AWS Control Tower のカスタマイズを起動するには、[GitHub からテンプレートをダウンロード](#)し、[AWS CloudFormation](#) から起動します。
2. テンプレートはデフォルトで米国東部 (バージニア北部) リージョンで起動します。別の AWS リージョンで CfCT を起動するには、コンソールナビゲーションバーのリージョンセクターを使用します。

i Note

CfCT は、AWS Control Tower のランディングゾーン (ホームリージョン) をデプロイしたものと同一リージョンおよびアカウントで起動する必要があります。

3. [Create stack] (スタックの作成) ページで、正しいテンプレート URL が [URL] テキストボックスに表示されていることを確認し、[Next] (次へ) を選択します。
4. [Specify stack details] (スタックの詳細を指定) ページで、CfCT スタックに名前を割り当てます。
5. [Parameters] (パラメータ) で、次のパラメータを確認し、必要に応じてテンプレート内で変更します。

パイプラインの設定

パラメータ	デフォルト	説明
Pipeline Approval Stage] (パイプライン承認ステージ	No	パイプライン設定をデフォルトの自動承認ステージから手動承認ステージに変更するかどうかを選択します。詳細については、「 the section called “CfCT カスタマイズガイド” 」を参照してください。

パイプラインの設定		
パラメータ	デフォルト	説明
Pipeline Approval Email Address] (パイプライン承認メールアドレス	<オプション入力>	承認通知用の電子メールアドレス。このパラメータを使用するには、[Pipeline Approval Stage] (パイプライン承認ステージ) パラメータを Yes に設定する必要があります。
AWS CodePipeline	Amazon S3	AWS CodePipeline のソースは、CfCT のカスタマイズを保存および設定する場所を選択するのに役立ちます。
AWS CodeCommit のセットアップ		
パラメータ	デフォルト	説明
[Existing CodeCommit Repository?] (既存の CodeCommit リポジトリを使用しますか?)	No	既存の CodeCommit Git リポジトリを使用するかどうかを選択します。Yes を選択する場合、[CodePipeline Source] (CodePipeline ソース) パラメータを AWS CodeCommit に設定する必要があります。
CodeCommit Repository Name] (CodeCommit リポジトリ名	custom-control-tower-configuration	既存の Git リポジトリの名前を指定する場合は、[既存の CodeCommit リポジトリを使用しますか?] パラメータを Yes に設定し、そのリポジトリの正確な名前を入力する必要があります。

AWS CodeCommit のセットアップ

パラメータ	デフォルト	説明
CodeCommit Branch Name] (CodeCommit ブランチ名	main	カスタマイズパッケージが格納される Git ブランチ。このパラメータを使用するには、[CodePipeline Source] (CodePipeline ソース) パラメータを AWS CodeCommit に設定する必要があります。

CloudFormation StackSets の設定

パラメータ	デフォルト	説明
Region Concurrency Type] (リージョンの同時実行タイプ	PARALLEL	リージョンで StackSets オペレーションをデプロイする同時実行タイプを選択します。この設定は、ワークフローの作成、更新、削除に適用されます。その他の許容値は SEQUENTIAL です。
Max Concurrent Percentage] (最大コンカレントパーセンテージ	100	このオペレーションを一度に実行するアカウントの最大の割合。許容される最大値は 100 です。詳細については、 「スタックセットオペレーションのオプション」 を参照してください。

CloudFormation StackSets の設定

パラメータ	デフォルト	説明
Failure Tolerance Percentage (フォールトトレランスパーセンテージ)	10	AWS CloudFormation がリージョンでのオペレーションを停止するまでに、各リージョンでこのスタックオペレーションの失敗を許容するアカウントの割合 (%)。許容される最小値は 0 で、最大値は 100 です。詳細については、「 スタックセットオペレーションのオプション 」を参照してください。

6. [Next] (次へ) を選択します。
7. [スタックオプションの設定] ページで、[次へ] を選択します。
8. [Review] (確認) ページで、設定を確認して確定します。このテンプレートが AWS Identity and Access Management (IAM) リソースを作成することを確認するボックスに必ずチェックを入れてください。
9. [Create stack] (スタックの作成) を選択してスタックをデプロイします。

CloudFormation コンソールの [Status] (ステータス) 欄でスタックのステータスを表示できます。約 15 分で CREATE_COMPLETE のステータスが表示されます。

ステップ 2. カスタムパッケージを作成する

スタックを起動したら、付属の設定パッケージをカスタマイズして、AWS Control Tower のランディングゾーンとサービスコントロールポリシー (SCP) をカスタマイズできます。カスタムパッケージを作成する詳細な手順については、「[CfCT カスタマイズガイド](#)」を参照してください。

注意

パイプラインは、カスタム設定パッケージをアップロードしないと実行されません。

スタックを更新する

AWS Control Tower のカスタマイズ (CfCT) を以前にデプロイしたことがある場合、手順に従って AWS CloudFormation スタックを CfCT フレームワークの最新バージョンに更新します。

Important

以下の手順を完了する前に、[GitHub の最新のテンプレート](#)を Amazon Simple Storage Service (Amazon S3) バケットにアップロードする必要があります。Amazon S3 の使用を開始する方法については、「Amazon Simple Storage Service ユーザーガイド」の「[Amazon S3 の開始方法](#)」を参照してください。

1. [AWS CloudFormation コンソール](#) にサインインします。
2. 既存の AWS Control Tower のカスタマイズ (CfCT) CloudFormation スタックを選択し、[更新] を選択します。
3. [前提条件 – テンプレートの準備] で、[既存テンプレートを置き換える] を選択します。
4. [テンプレートの指定] ページで、以下を実行します。
 - a. [テンプレートソース] で、[既存テンプレートを置き換える] を選択します。
 - b. Amazon S3 URL で、以前に GitHub から Amazon S3 にアップロードしたテンプレートのテンプレート URL を入力し、[次へ] を選択します。
 - c. テンプレート URL が正しいことを確認します。[次へ] を選択し、もう一度 [次へ] を選択します。
5. [パラメータ] で、テンプレートのパラメータを確認し、必要に応じて変更します。パラメータの詳細については、「[ステップ 1. スタックを起動する](#)」を参照してください。
6. [Next] (次へ) を選択します。
7. [スタックオプションの設定] ページで、[次へ] を選択します。
8. [レビュー] ページで、設定を確認して確定します。このテンプレートが AWS Identity and Access Management (IAM) リソースを作成することを確認するボックスに必ずチェックを入れてください。
9. [変更セットの表示] を選択して、変更を確認します。
10. [スタックの更新] を選択してスタックをデプロイします。

AWS CloudFormation コンソールの [Status] (ステータス) 欄でスタックのステータスを表示できます。約 15 分で UPDATE_COMPLETE のステータスが表示されます。

スタックセットの削除

マニフェストファイルでスタックセットの削除を有効にしている場合は、スタックセットを削除できます。デフォルトでは、`enable_stack_set_deletion` パラメータが `false` に設定されています。この設定では、リソースが CfCT マニフェストファイルから削除されていると、関連するスタックセットを削除するアクションは実行されません。

マニフェストファイルで `enable_stack_set_deletion` の値を `true` に変更すると、マニフェストファイルから関連するリソースを削除したときに、CfCT はスタックセットとそのすべてのリソースを削除します。

この機能は、マニフェストファイルの v2 でサポートされています。

Important

最初に `enable_stack_set_deletion` の値を `true` に設定すると、次回 CfCT を呼び出したときに、プレフィックス `CustomControlTower-` で始まるすべてのリソースのうち、キータグ `Key:AWS_Solutions, Value: CustomControlTowerStackSet` が関連付けられているリソースと、マニフェストファイルに宣言されていないリソースは、削除対象としてステージングされます。

このパラメータを `manifest.yaml` ファイルで設定する方法の例を次に示します。

```
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
```

Simple Storage Service (Amazon S3) を設定ソースとしてセットアップする

AWS Control Tower のカスタマイズをセットアップすると、`_custom-control-tower-configuration.zip` ファイルと呼ばれる初期設定ファイルが、`custom-control-tower-configuration-account-ID-region` ファイルという名前の Amazon Simple Storage Service (Amazon S3) バケットに格納されます。

注意

このファイルをダウンロードして変更する場合は、変更を圧縮し、`custom-control-tower-configuration.zip` という名前を付けて新しいファイルとして保存してから、同じ Simple Storage Service (Amazon S3) バケットにアップロードします。

Simple Storage Service (Amazon S3) バケットは、パイプラインのデフォルトのソースです。デフォルト設定が指定されている場合、ファイル名にアンダースコアプレフィックスを含まない設定 zip ファイルを S3 バケットにアップロードすると、パイプラインが自動的に開始されます。

zip ファイルは [Server-Side Encryption](#) (SSE) と AWS Key Management Service (AWS KMS)、および KMS キーの [denial of use](#) によって保護されています。zip ファイルにアクセスするには、KMS キーポリシーを更新して、アクセスを許可するロールを指定する必要があります。ロールは、管理者ロール、ユーザー、またはその両方とすることができます。次の手順に従ってください。

1. [AWS Key Management Service コンソール](#) に移動します。

2. [Customer Managed Keys] (カスタマーマネージドキー) で、CustomControlTowerKMSKey を選択します。
3. [Key policy] (キーポリシー) タブを選択します。次に、[Edit] (編集) を選択します。
4. [Edit key policy] (キーポリシーの編集) ページで、コード内の [Allow Use of the key] (キーの使用を許可) セクションを開き、次のいずれかのアクセス許可を追加します。
 - 管理者ロールを追加する場合:

```
arn:aws:iam::<account-ID>:role/<administrator-role>
```
 - ユーザーを追加する場合:

```
arn:aws:iam::<account-ID>:user/<username>
```
5. [Save Changes] (変更を保存) をクリックします。
6. [Simple Storage Service \(Amazon S3\) コンソール](#)に移動し、設定 zip ファイルが含まれている S3 バケットを探して、[download] (ダウンロード) を選択します。
7. マニフェストファイルとテンプレートファイルに対して必要な設定変更を行います。マニフェストファイルとテンプレートファイルのカスタマイズについては、「[the section called “CfCT カスタマイズガイド”](#)」を参照してください。
8. 変更をアップロード:
 - a. 変更された設定ファイルを圧縮し、ファイルに custom-control-tower-configuration.zip という名前を付けます。
 - b. SSE を AWS KMS master-key:CustomControlTowerKMSKey と一緒に使用して Simple Storage Service (Amazon S3) にファイルをアップロードします。

GitHub を設定ソースとしてセットアップする

このセクションでは、GitHub をソースとして AWS Control Tower (CfCT) のカスタマイズをデプロイする方法を説明します。このプロセスには、3 つの主要なステップがあります。

- GitHub リポジトリを準備する
- GitHub コード接続を作成する
- CloudFormationスタックをデプロイする

GitHub リポジトリを準備する

GitHub アカウント内にリポジトリを作成します。テンプレートで使用するデフォルト名は `custom-control-tower-configuration` です。ターゲットリポジトリをプライベートにすることを検討してください。カスタマイズは、CfCT リポジトリの [デプロイフォルダ](#)にある `manifest.yaml` という yaml ファイルで定義します。

[CfCT カスタマイズガイド](#)には、カスタマイズを設定する `manifest.yaml` の作成に関する詳細なガイドランスが記載されています。

GitHub 接続を作成する

Github のデベロッパーツール --Connections インスタンスから、次の手順を実行します。

1. [Create connection] を選択し、プロバイダーとして GitHub を選択します。
2. [Create a GitHub App connection] を選択し、[Connection name] フィールドに GitHub CfCT または任意の名前を入力します。
3. [Connect to GitHub] を選択し、[Install a new app] を選択します。
4. リポジトリの GitHub ユーザーまたは組織を選択する
5. [Repository access] で、[Only select repositories] を選択し、前に作成したリポジトリを選択して作業を保存します。
6. コード接続 ARN を書き留めます。CloudFormationスタックをデプロイするときに必要になります。

CloudFormationスタックをデプロイする

- リポジトリから `custom-control-tower-initiation.template` ファイルをダウンロードします。
- `custom-control-tower-initiation.template` ファイルを使用して新しいCloudFormationスタックを作成します。
- [AWS CodePipeline Source] で、[GitHub (via Code Connection)] を選択します。
- [GitHub Setup] で、以下のフィールドを指定します。
 - [ARN of the Code Connection] には、コード接続 ARN を指定します。
 - [GitHub User or Organization] には、リポジトリを作成した GitHub ユーザーまたは組織の名前を入力します。

- [GitHub Repository Name] には、リポジトリ名を入力します (デフォルトは custom-control-tower-configuration)。
- [GitHub Branch Name] には、ブランチ名を入力します (デフォルトは main)。

運用メトリクスの収集

AWS Control Tower のカスタマイズ (CfCT) には、匿名の運用メトリクスを AWS に送信するオプションが含まれています。AWS ではこのデータを使用して、お客様が CfCT をどのように使用しているか、および関連するサービスや製品を把握します。データ収集が有効になっていると、次の情報が AWS に送信されます。

- ソリューション ID: AWS ソリューション識別子
- 一意の ID (UUID): デプロイごとにランダムに生成された一意の識別子
- タイムスタンプ: データ収集タイムスタンプ
- ステートマシンの実行回数: このステートマシンが実行された回数を増分カウントします。
- マニフェストのバージョン: 設定で使用するマニフェストバージョン

Note

AWS は収集したデータを所有します。データ収集には、[AWS プライバシーポリシー](#)が適用されます。

匿名の運用メトリクスを AWS に送信しないようにするには、次のいずれかのタスクを実行します。

- AWS CloudFormation テンプレートマッピングセクションを次のように更新します。

from

```
AnonymousData:
  SendAnonymousData:
    Data: Yes
```

~

```
AnonymousData:
```

```
SendAnonymousData:  
  Data: No
```

- CfCT をデプロイしたら、パラメータストアコンソールで `/org/primary/metrics_flag` SSM パラメータキーを見つけ、値を **No** に更新します。

CfCT カスタマイズガイド

AWS Control Tower のカスタマイズ (CfCT) ガイドは、AWS Control Tower 環境を会社または顧客向けにカスタマイズおよび拡張することを希望する管理者、DevOps プロフェッショナル、独立系ソフトウェアベンダー、IT インフラストラクチャアーキテクト、システムインテグレーターを対象としています。このガイドでは、CfCT カスタマイズパッケージを使用して AWS Control Tower 環境をカスタマイズおよび拡張する際に役立つ情報を提供します。

Note

(CfCT) をデプロイして設定するには、設定パッケージをデプロイして処理する必要があります AWS CodePipeline。以下のセクションではこのプロセスを詳しく説明します。

コードパイプラインの概要

設定パッケージには、Amazon Simple Storage Service (Amazon S3) と が必要です AWS CodePipeline。設定パッケージには、次の項目が含まれています。

- マニフェストファイル
- 付随するテンプレートのセット
- AWS Control Tower 環境のカスタマイズを記述および実装するためのその他の JSON ファイル

デフォルトでは、`_custom-control-tower-configuration.zip` 設定パッケージは、次の命名規則に従って Simple Storage Service (Amazon S3) バケットにロードされます。

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

Note

デフォルトでは、CfCT はパイプラインソースを格納するために Amazon S3 バケットを作成します。ほとんどのお客様は、このデフォルトのままで構いません。既存の AWS

CodeCommit リポジトリがある場合は、ソースの場所を AWS CodeCommit リポジトリに変更できます。詳細については、「AWS CodePipeline ユーザーガイド」の「[CodePipeline でパイプラインを編集する](#)」を参照してください。

マニフェストファイルは、ランディングゾーンをカスタマイズするためにデプロイできる AWS リソースについて記述するテキストファイルです。CodePipeline は次のタスクを実行します。

- マニフェストファイル、それに付随するテンプレートのセット、およびその他の JSON ファイルを抽出する
- マニフェストとテンプレートの検証を実行する
- CfCT マニフェストファイル内のセクションを呼び出して特定の[パイプラインステージ](#)を実行する。

マニフェストファイルをカスタマイズし、設定パッケージのファイル名からアンダースコア (_) を削除して設定パッケージを更新すると、AWS CodePipeline が自動的に開始されます。

アンダースコアを覚えておく

設定パッケージのサンプルファイル名はアンダースコア (_) で始まるため、AWS CodePipeline は自動的に開始されません。設定パッケージのカスタマイズが完了したら、AWS CodePipeline でデプロイをトリガーするため、アンダースコア (_) を付けずにファイル `custom-control-tower-configuration.zip` をアップロードします。

AWS CodePipeline ステージ

CfCT パイプラインでは、AWS Control Tower 環境を実装および更新するためにいくつかの AWS CodePipeline ステージが必要です。

1. ソースステージ

ソースステージは最初のステージです。カスタマイズされた設定パッケージによって、このパイプラインステージが開始されます。のソースは、設定パッケージをホストできる Amazon S3 バケットまたは AWS CodeCommit リポジトリのいずれか AWS CodePipeline です。

2. ビルドステージ

ビルドステージでは AWS CodeBuild 、設定パッケージの内容を検証する必要があります。これらのチェックには、 `および` を使用して、`manifest.yaml` ファイルの構文とスキーマ、パッケージに含まれるすべての CloudFormation テンプレート、またはリモートでホストされているすべてのテンプレートのテスト `CloudFormation validate-template` が含まれます `cfn_nag`。マニフェストファイルと CloudFormation テンプレートがテストに合格すると、パイプラインは次のステージに進みます。テストに不合格だった場合は、CodeBuild ログを確認して問題を特定し、必要に応じて設定ソースファイルを編集できます。

3. 手動承認ステージ (オプション)

手動承認ステージはオプションです。このステージを有効にすると、設定パイプラインをさらに制御できます。承認が得られるまで、デプロイ中のパイプラインは一時停止します。手動承認をオプトインするには、スタックを起動したときに、[Pipeline Approval Stage] (パイプライン承認ステージ) パラメータを [Yes] (はい) に変更します。

4. ポリシーステージ

ポリシーステージは、サービスコントロールポリシー (SCP) またはリソースコントロールポリシー (RCP) ステートマシンを呼び出して、SCP または RCP を作成する AWS Organizations APIs を呼び出します。RCPs

5. CloudFormation リソースステージ

CloudFormation リソースステージは、スタックセットステートマシンを呼び出して、マニフェストファイルで指定したアカウントまたは組織単位 (OUs) のリストで指定されたリソースをデプロイします。ステートマシンは、マニフェストファイルで指定された順序で CloudFormation リソースを作成します。リソースの依存関係を指定するには、マニフェストファイルでリソースが指定されている順序を調整します。マニフェストファイル内のリソースの順序は、依存関係を指定する唯一の方法です。

カスタム設定の定義

CfCT マニフェストファイル、付随するテンプレートのセット、およびその他の JSON ファイルを使用して、カスタム AWS Control Tower 設定を定義します。これらのファイルをフォルダ構造にパッケージ化し、次のコード例に示すように、Simple Storage Service (Amazon S3) バケット内に `.zip` ファイルとして配置します。

カスタム設定フォルダ構造

```
- manifest.yaml
```

```
- policies/ [optional]
  - service control policies files (*.json)
- templates/ [optional]
  - template files for AWS CloudFormation Resources (*.template)
```

前の例は、カスタム設定フォルダの構造を示しています。Amazon S3 または AWS CodeCommit リポジトリをソースストレージの場所として選択した場合でも、フォルダ構造は変わりません。Simple Storage Service (Amazon S3) をソースストレージとして選択した場合は、すべてのフォルダとファイルを `custom-control-tower-configuration.zip` ファイルをアップロードし、`.zip` ファイルのみを指定された Simple Storage Service (Amazon S3) バケットにアップロードします。

Note

を使用している場合は AWS CodeCommit、ファイルを圧縮せずにリポジトリにファイルを配置します。

CfCT マニフェストファイル

CfCT `manifest.yaml` ファイルは、AWS リソースを記述するテキストファイルです。次の例は、CfCT マニフェストファイルの構造を示しています。

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

resources:
  #set of CloudFormation resources, SCP policies, or RCP policies
...
```

前のコード例で示したように、マニフェストファイルの最初の 2 行は、`region` と `version` キーワードの値を指定します。これらのキーワードの定義は次のとおりです。

region — AWS Control Tower のデフォルトリージョンのテキスト文字列。この値は、有効な AWS リージョン名 (`us-east-1`、`eu-west-1` など) である必要があります `ap-southeast-1`。AWS Control Tower のホームリージョンは、リソース固有のリージョンが指定されていない限り、カスタム AWS Control Tower リソース (CloudFormation StackSets など) を作成するときのデフォルトです。


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

version — マニフェストスキーマのバージョン番号。サポートされている最新バージョンは 2021-03-15 です。

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

Note

最新バージョンの使用をお勧めします。マニフェストプロパティを最新バージョンに更新するには、「[CfCT マニフェストのバージョンアップグレード](#)」を参照してください。

前の例で示した次のキーワードは、resource キーワードです。マニフェストファイルの [resources] (リソース) セクションは高度に構造化されています。これには、CfCT パイプラインによって自動的にデプロイされる AWS リソースの詳細なリストが含まれています。次のセクションで、リソースとその使用可能なパラメータについて説明します。

CfCT マニフェストファイルの [リソース] セクション

このトピックでは、CfCT マニフェストファイルの [リソース] セクションについて説明します。このセクションでは、カスタマイズに必要なリソースを定義します。CfCT マニフェストファイルのこのセクションは、キーワード resources から始まり、ファイルの末尾まで続きます。

マニフェストファイルのリソースセクションでは、コードパイプラインを介して CfCT が自動的にデプロイする StackSets、または AWS Organizations SCPs と RCPs を指定します CloudFormation。OU、アカウント、およびリージョンを一覧表示してスタックインスタンスをデプロイできます。

スタックインスタンスは OU レベルではなくアカウントレベルでデプロイされます。SCP と RCP は OU レベルでデプロイされます。詳細については、「[独自のカスタマイズを構築する](#)」を参照してください。

次のサンプルテンプレートには、マニフェストファイルの [リソース] セクションで利用可能なエントリが説明されています。

```
resources: # List of resources
```

```

- name: [String]
  resource_file: [String] [Local File Path, S3 URI, S3 URL]
  deployment_targets: # account and/or organizational unit names
    accounts: # array of strings, [0-9]{12}
      - 012345678912
      - AccountName1
    organizational_units: #array of strings
      - OuName1
      - OuName2
  deploy_method: scp | stack_set | rcp
  parameters: # List of parameters [SSM, Alfred, Values]
    - parameter_key: [String]
      parameter_value: [String]
  export_outputs: # list of ssm parameters to store output values
    - name: /org/member/test-ssm/app-id
      value: ${output_ApplicationId}
  regions: #list of strings
    - [String]

```

このトピックの残りの部分では、前のコード例で示したキーワードの詳しい定義について説明します。

name — CloudFormation StackSets に関連付けられた名前。指定する文字列は、スタックセットに対してよりわかりやすい名前を割り当てます。

- **タイプ:** 文字列
- **必須:** はい
- **有効な値:** a~z、A~Z、0~9、およびハイフン (-)。名前はアルファベット文字で始まる必要があります。

説明: リソースの説明。

- **タイプ:** 文字列
- **必須:** いいえ

resource_file – このファイルは、マニフェストファイルへの相対的な場所、CloudFormation リソース、SCPs、または RCPs を作成するための JSON の CloudFormation テンプレートまたは AWS Organizations サービスコントロールポリシーを指す Amazon S3 URI または URL として指定できます。

- タイプ: 文字列
- 必須: はい

1. 次の例で示している `resource_file` は、設定パッケージ内のリソースファイルへの相対的な場所として指定されます。

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

2. 次の例は、Amazon S3 URI として指定されているリソースファイルを示しています。

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

3. 次の例は、Simple Storage Service (Amazon S3) HTTPS URL として指定されているリソースファイルを示しています。

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

Note

Simple Storage Service (Amazon S3) URL を指定する場合は、バケットポリシーで、CfCT のデプロイ元となる AWS Control Tower 管理アカウントの読み取りアクセスが許可されていることを確認します。Simple Storage Service (Amazon S3) HTTPS URL を指定する場合は、パスがドット表記を使用していることを確認します。例えば、`S3.us-west-1`。CfCT は、S3 とリージョンの間にダッシュを含むエンドポイントをサポートしていません (`S3-us-west-2` など)。

4. 次の例は、リソースを保存する Simple Storage Service (Amazon S3) バケットポリシーと ARN を示しています。

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

```
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::my-bucket/*"
  }
]
```

この例では、*AccountId* 変数を、CfCT をデプロイしている管理アカウントの AWS アカウント ID に置き換えます。その他の例については、「Amazon Simple Storage Service ユーザーガイド」の「[バケットポリシーの例](#)」を参照してください。

parameters — CloudFormation パラメータの名前と値を指定します。

- タイプ: MapList
- 必須: いいえ

[parameters] (パラメータ) セクションには、キー/値パラメータのペアが含まれます。次の疑似テンプレートは、[parameters] (パラメータ) セクションの概要を示します。

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

- parameter_key — パラメータに関連付けられたキー。
 - タイプ: 文字列
 - 必須: はい (パラメータプロパティの下)
 - 有効な値: a~z、A~Z、0~9
- parameter_value - パラメータに関連付けられた入力値。
 - タイプ: 文字列
 - 必須: はい (パラメータプロパティの下)

deploy_method — アカウントにリソースをデプロイするためのデプロイ方法。現在、deploy_method は、CloudFormation StackSets を介したリソースデプロイ stack_set のオプション

ション、SCP をデプロイする場合は scp オプション、RCPs をデプロイする場合は rcp オプションを使用してリソースのデプロイをサポートしています。SCPs

- タイプ: 文字列
- 有効な値: stack_set | scp | rcp
- 必須: はい

deployment_targets – CfCT がアカウントまたは organization_units として指定された CloudFormation リソースをデプロイするアカウントまたは組織単位 (OUs) のリスト。

 Note

SCP または RCP をデプロイする場合、ターゲットはアカウントではなく OU である必要があります。

- タイプ: このリソースが特定のアカウントリストにデプロイされることを示す文字列 account name または account number、あるいはこのリソースが指定された OU リストにデプロイされることを示す OU names のリスト。
- 必須: accounts または organizational_units のうち少なくとも 1 つ
- accounts:

タイプ: このリソースが特定のアカウントリストにデプロイされることを示す文字列 account name または account number のリスト。

- organizational_units:

タイプ: このリソースが特定の OU リストにデプロイされることを示す文字列 OU names のリスト。アカウントを含まない OU を指定し、accounts プロパティを追加していない場合、CfCT はスタックセットのみを作成します。

 Note

組織の管理アカウント ID が許可されている値ではありません。デフォルトでは、CfCT は、組織の管理アカウントへのスタックインスタンスのデプロイをサポートしていません。特別なユースケースがある場合は、「[ルート OU](#)」を参照してください。

`export_outputs` — SSM パラメータキーを表す名前/値のペアのリスト。これらの SSM パラメータキーを使用すると、テンプレート出力を SSM パラメータストアに格納できます。出力は、先にマニフェストファイルで定義済みの他のリソースから参照されることになります。

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

- タイプ: name および value キーペアのリスト。name には SSM パラメータストアキーの name 文字列が含まれ、value にはパラメータの value 文字列が含まれています。
- 有効な値: 任意の文字列、または `CfnOutput-Logical-ID` がテンプレート出力変数に対応する `[$[output_CfnOutput-Logical-ID]]` 変数。CloudFormation テンプレートの出力セクションの詳細については、CloudFormation 「ユーザーガイド」の「[出力](#)」を参照してください。
- 必須: いいえ

例えば、次のコードスニペットは、`/org/member/audit/vpc_id` という名前の SSM パラメータキーにテンプレート VPCID の出力変数を保存します。

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

Note

`export_outputs` キー名には、`output` 以外の値を含めることができます。例えば、name が `/org/environment-name` の場合、value は `production` とすることができます。

`regions` – CfCT が CloudFormation スタックインスタンスをデプロイするリージョンのリスト。

- タイプ: AWS 商用リージョン名のリスト。このリソースが指定されたリージョンリストにデプロイされることを示します。このキーワードがマニフェストファイルに存在しない場合、リソースはホームリージョンにのみデプロイされます。
- 必須: いいえ

ルート OU

マニフェスト V2 バージョン (2021-03-15) では、CfCT は `organizational_units` の組織単位 (OU) の値としてのルートをサポートしています。

- `scp` または `rcp` のデプロイ方法を選択した場合、`organizational_units` でルートを追加すると、AWS Control Tower はルートの下にあるすべての OU にポリシーを適用します。`stack_set` のデプロイ方法を選択した場合、`organizational_units` でルートを追加すると、CfCT は、管理アカウントを除き、AWS Control Tower に登録されているルートの下にあるすべてのアカウントにスタックセットをデプロイします。
- AWS Control Tower のベストプラクティスに従って、管理アカウントはメンバーアカウントの管理と請求のみを目的としています。AWS Control Tower 管理アカウントで本番ワークロードを実行しないでください。

ベストプラクティスのガイダンスに従って、AWS Control Tower のデプロイでは、管理アカウントはルート OU の下に置かれています。これにより、フルアクセス権を付与しながら、管理アカウントが追加のリソースを実行しないようにします。この理由のため、`AWSControlTowerExecution` ロールは管理アカウントにデプロイされません。

- 管理アカウントについては、次のベストプラクティスに従うことをお勧めします。特定のユースケースで、管理アカウントにスタックセットをデプロイする必要がある場合は、`accounts` をデプロイターゲットとして含め、管理アカウントを指定します。それ以外の場合は、`accounts` をデプロイターゲットとして含めないでください。必要な IAM ロールなど、不足しているリソースを管理アカウントで作成する必要があります。

管理アカウントにスタックセットをデプロイするには、`accounts` をデプロイターゲットとして含め、管理アカウントを指定します。それ以外の場合は、`accounts` をデプロイターゲットとして含めないでください。

```
---
region: your-home-region
version: 2021-03-15

resources:

  ...truncated...

  deployment_targets:
    organizational_units:
```

- Root

Note

ルート OU 機能は、V2 バージョンのマニフェストファイル (2021-03-15) でのみサポートされます。organizational_units の OU として [Root] (ルート) を追加する場合、他の OU は追加しないでください。

ネストされた OU

CfCT では、1 つ以上のネストされた OU をマニフェスト V2 バージョン (2021-03-15) の organizational_units キーワードでリストすることができます。

OU 間の区切り文字としてコロンを使用した、ネストされた OU の完全なパス (ルートを除く) が必要です。scp または rcp のデプロイ方法では、AWS Control Tower は、ネストされた OU パスの最後の OU に SCP または RCP をデプロイします。デプロイ方法 stack_set では、AWS Control Tower は、ネストされた OU パスの最後の OU のすべてのアカウントに、スタックセットをデプロイします。

例えば、パス OUName1:OUName2:OUName3 について考えてみましょう。パス内の最後の OU は OUName3 です。CfCT は SCP または RCP を OUName3 にデプロイし、スタックセットを OUName3 の直下にあるすべてのアカウントにデプロイします。

```
---
region: your-home-region
version: 2021-03-15

resources:

  ...truncated...

  deployment_targets:
    organizational_units:
      - OuName1:OUName2:OUName3
```


Note

ネストされた OU 機能は、V2 バージョンのマニフェストファイル (2021-03-15) でのみサポートされます。

独自のカスタマイズを構築する

独自のカスタマイズを構築するには、サービスコントロールポリシー (SCPs)、リソースコントロールポリシー (RCPs)、および CloudFormation リソースを追加または更新することで、CfCT manifest.yaml ファイルを変更します。デプロイする必要があるリソースについては、アカウントと OU を追加または削除できます。パッケージフォルダ内のテンプレートを追加または変更したり、独自のフォルダを作成したり、テンプレートまたは manifest.yaml ファイル内のフォルダを参照したりできます。

このセクションでは、独自のカスタマイズを構築する際の 2 つの主要部分について説明します。

- サービスコントロールポリシー用に独自の設定パッケージをセットアップする方法
- AWS CloudFormation スタックセット用に独自の設定パッケージを設定する方法

SCP または RCP の設定パッケージを設定する

このセクションでは、サービスコントロールポリシー (SCP) または リソースコントロールポリシー (RCP) 用の設定パッケージを作成する方法を説明します。このプロセスの 2 つの主要部分は、(1) CfCT マニフェストファイルの準備、(2) フォルダ構造の準備です。

ステップ 1: manifest.yaml ファイルを編集する

サンプル manifest.yaml ファイルを出発点として使用します。必要な設定をすべて入力します。resource_file および deployment_targets の詳細を追加します。

次のスニペットは、デフォルトマニフェストファイルを示しています。

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

resources: []
```

region の値は、デプロイ時に自動的に追加されます。これは CfCT をデプロイしたリージョンと一致する必要があります。このリージョンは AWS Control Tower リージョンと同じものにする必要があります。

Amazon S3 バケットに格納されている zip パッケージ内の example-configuration フォルダにカスタム SCP または RCP を追加するには、example-manifest.yaml ファイルを開き、編集を開始します。

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

...truncated...
```

次のスニペットは、カスタマイズされたマニフェストファイルの例を示しています。1 回の変更で複数のポリシーを追加できます。

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

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

ステップ 2: フォルダ構造を作成する

リソースファイルに Simple Storage Service (Amazon S3) URL を使用していて、キーと値のペアの parameters を使用している場合、このステップを省略できます。

マニフェストファイルは JSON ファイルを参照するため、マニフェストをサポートするには、SCP ポリシーまたは RCP ポリシーを JSON 形式で含める必要があります。マニフェストファイルに指定されたパス情報とファイルパスが一致していることを確認します。

- policy JSON ファイルには、OU にデプロイされる SCP または RCP が含まれています。

次のスニペットは、サンプルマニフェストファイルのフォルダ構造を示しています。

```
- manifest.yaml
- policies/
  - block-s3-public.json
```

以下のスニペットは、block-s3-public.json ポリシーファイルの一例です。

JSON

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

CloudFormation StackSets の設定パッケージを設定する

このセクションでは、CloudFormation StackSets の設定パッケージを設定する方法について説明します。このプロセスの 2 つの主要部分は、(1) マニフェストファイルの準備、(2) フォルダ構造の更新です。

ステップ 1: 既存のマニフェストファイルを編集する

以前に編集したマニフェストファイルに新しい CloudFormation StackSets 情報を追加します。

次のスニペットには、確認のため、SCP または RCP 用の設定パッケージをセットアップするために前述したものと同一カスタマイズされたマニフェストファイルが含まれています。このファイルをさらに編集して、リソースの詳細を含めることができるようになりました。

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

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp / rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
      - OUName1
      - OUName2
```

次のスニペットは、resources の詳細を含む編集済みのサンプルマニフェストファイルを示します。resources の順序は、resources の依存関係を作成するための実行順序を決定します。次のサンプルマニフェストファイルをビジネス要件に応じて編集できます。

```
---
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

```

次の例は、マニフェストファイルに複数の CloudFormation リソースを追加できることを示しています。

```

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

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings

```

```
- Custom
- Sandbox

- name: transit-network
  resource_file: templates/transit-gateway.template
  parameter_file: parameters/transit-gateway.json
  deploy_method: stack_set
  deployment_targets:
    accounts: # array of strings, [0-9]{12}
      - Prod
      - 123456789123 #Network
    organizational_units: #array of strings
      - Custom
  export_outputs:
    - name: /org/network/transit-gateway-id
      value: ${output_TransitGatewayID}
  regions:
    - us-east-1
```

ステップ 2: フォルダ構造を更新する

フォルダ構造を更新するときは、マニフェストファイルにあるすべてのサポート CloudFormation テンプレートファイルと SCP または RCP ポリシーファイルを含めることができます。ファイルパスがマニフェストファイルで指定したものと一致していることを確認します。

- テンプレートファイルには、OUs とアカウントにデプロイされる AWS リソースが含まれています。
- policy ファイルには、テンプレートファイルで使用する入力パラメータが含まれます。

次の例は、[ステップ 1](#) で作成したサンプルマニフェストファイルのフォルダ構造を示しています。

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

「alfred」ヘルパーと CloudFormation パラメータファイル

CfCT には、CloudFormation テンプレートで定義されている [SSM パラメータストア](#) キーの値を取得するための alfred ヘルパーと呼ばれるメカニズムが用意されています。alfred ヘルパーを使用す

ると、CloudFormation テンプレートを更新せずに、SSM パラメータストアに保存されている値を使用できます。詳細については、「[CloudFormation ユーザーガイド](#)」の [CloudFormation 「テンプレートとは」](#) を参照してください。

Important

alfred ヘルパーには 2 つの制限があります。パラメータは、AWS Control Tower 管理アカウントのホームリージョンでのみ使用できます。ベストプラクティスとして、スタックインスタンスごとに変わらない値を使用することを検討してください。「alfred」ヘルパーがパラメーターを取得すると、変数をエクスポートするスタックセットからランダムなスタックインスタンスを選択します。

例

CloudFormation スタックセットが 2 つあるとします。スタックセット 1 には 1 つのスタックインスタンスがあり、1 つのリージョンの 1 つのアカウントにデプロイされます。アベイラビリティーゾーンに Amazon VPC とサブネットが作成されます。VPC ID と subnet ID をパラメータ値としてスタックセット 2 に渡す必要があります。VPC ID と subnet ID をスタックセット 2 に渡す前に、AWS::SSM::Parameter を使用して VPC ID と subnet ID をスタックセット 1 に保存する必要があります。詳細については、CloudFormation ユーザーガイドの [AWS::SSM::Parameter](#) を参照してください。

CloudFormation スタックセット 1:

次のスニペットでは、alfred ヘルパーは、パラメータストアから VPC ID と subnet ID の値を取得し、それらの値を StackSet ステートマシンに入力として渡すことができます。

```
VpcIdParameter:
  Type: AWS::SSM::Parameter
  Properties:
    Name: '/stack_1/vpc/id'
    Description: Contains the VPC id
    Type: String
    Value: !Ref MyVpc

SubnetIdParameter:
  Type: AWS::SSM::Parameter
  Properties:
    Name: '/stack_1/subnet/id'
    Description: Contains the subnet id
```

```
Type: String
Value: !Ref MySubnet
```

CloudFormation スタックセット 2:

スニペットには、CloudFormation スタック 2 manifest.yaml ファイルで指定されたパラメータが表示されます。

```
parameters:
  - parameter_key: VpcId
    parameter_value: $[alfred_ssm_/stack_1/vpc/id]
  - parameter_key: SubnetId
    parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

CloudFormation スタックセット 2.1:

このスニペットは、ユーザーが CommaDelimitedList 型のパラメータをサポートする alfred_ssm プロパティを一覧表示できることを示しています。詳細については、CloudFormation ユーザーガイドの [Parameters](#) を参照してください。

```
parameters:
  - parameter_key: VpcId # Type: String
    parameter_value: $[alfred_ssm_/stack_1/vpc/id']
  - parameter_key: SubnetId # Type: String
    parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
  - parameter_key: AvailabilityZones # Type: CommaDelimitedList
    parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
  - "$[alfred_ssm_/availability_zone_2]"
```

カスタマイズパッケージの JSON スキーマ

CfCT のカスタマイズパッケージの JSON スキーマは、[GitHub のソースコードリポジトリ](#)にあります。このスキーマはほとんどの開発ツールで使用でき、独自の CfCT manifest.yaml ファイルを構築する際のエラーを減らすのに役立ちます。

CfCT マニフェストのバージョンアップグレード

AWS Control Tower のカスタマイズ (CfCT) の最新バージョンについては、GitHub リポジトリの [CHANGELOG.md ファイル](#)を参照してください。

Warning

AWS Control Tower のカスタマイズ (CfCT) のバージョン 2.2.0 では、関連する AWS サービス API に合わせて CfCT マニフェストスキーマ (バージョン 2021-03-15) が導入されました。APIs マニフェストスキーマを使用すると、単一の manifest.yaml ファイルで、分離された DevOps ワークフローを通じてサポートされているリソース (CloudFormation テンプレート、SCPs、RCPs) を管理できます。

CfCT マニフェストスキーマのバージョン 2020-01-01 を、バージョン 2021-03-15 以降に更新することを強くお勧めします。

CfCT は、引き続き manifest.yaml ファイルのバージョン 2021-03-15 および 2020-01-01 をサポートします。既存の設定を変更する必要はありません。ただし、バージョン 2020-01-01 はサポート終了になります。バージョン 2020-01-01 に更新プログラムを提供したり、拡張機能を追加したりすることはありません。ルート OU およびネストされた OU 機能は、バージョン 2020-01-01 ではサポートされていません。

CfCT マニフェストバージョン 2021-03-15 で廃止されたプロパティ:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

必須の CfCT アップグレードステップ

CfCT マニフェストのスキーマバージョンを 2021-03-15 にアップグレードするときに、ファイルを更新するために必要な変更は次のとおりです。次のセクションでは、移行時の必須の推奨および推奨される変更について概説します。

組織ポリシー

1. SCP または RCP を新しいプロパティ resources の下にある organization_policies に移動します。
2. policy_file プロパティを新しいプロパティ resource_file に変更します。

3. `apply_to_accounts_in_ou` を新しいプロパティ `deployment_targets` に変更します。OU リストは、サブプロパティ `[organizational_units]` で定義する必要があります。accounts サブプロパティは、組織ポリシーではサポートされていません。
4. 新しいプロパティ `deploy_method` を、値 `scp` または `rcp` を指定して追加します。

CloudFormation リソース

1. CloudFormation リソースを新しいプロパティ `resources` の下にある `cloudformation_resources` に移動します。
2. `template_file` プロパティを新しいプロパティ `resource_file` に変更します。
3. `deploy_to_ou` を新しいプロパティ `deployment_targets` に変更します。OU リストは、サブプロパティ `[organizational_units]` で定義する必要があります。
4. `deploy_to_accounts` を新しいプロパティ `deployment_targets` に変更します。アカウントリストは、サブプロパティ `accounts` で定義する必要があります。
5. `ssm_parameters` プロパティを新しいプロパティ `export_outputs` に変更します。

強く推奨される CfCT アップグレードステップ

CloudFormation パラメータ

1. `parameter_file` プロパティを新しいプロパティ `parameters` に変更します。
2. `parameter_file` プロパティの値にあるファイルパスを削除します。
3. 既存のパラメータ JSON ファイルのパラメータキーとパラメータ値を、`parameters` プロパティの新しいフォーマットにコピーします。この操作により、マニフェストファイルでこれらの値を管理することができます。

Note

`parameter_file` プロパティは CfCT マニフェストバージョン 2021-03-15 でサポートされています。

AWS Control Tower のネットワーク

AWS Control Tower は、VPC を介したネットワークの基本的なサポートを提供します。

AWS Control Tower VPC のデフォルト設定または機能がニーズを満たさない場合は、他のAWSサービスを使用して VPC を設定できます。VPCs [「スケーラブルで安全なマルチ VPC AWS ネットワーク インフラストラクチャの構築」](#) を参照してください。

AWS Control Tower は、デュアルスタック IP アドレスを使用して IPv4 および IPv6 プロトコルをサポートします。詳細については、「[AWS Control Catalog のエンドポイントとクォータ](#)」および「[AWS Control Tower のエンドポイントとクォータ](#)」を参照してください。

関連トピック

- 既存の VPC があるアカウントを登録する場合の AWS Control Tower の動作の詳細については、「[VPC を使用して既存のアカウントを登録する](#)」を参照してください。
- Account Factory では、AWS Control Tower VPC を含むアカウントをプロビジョニングしたり、VPC なしでアカウントをプロビジョニングしたりできます。AWS Control Tower VPC を削除する方法、または VPC なしで AWS Control Tower アカウントを設定する方法については、「[チュートリアル: VPC を使用せずに AWS Control Tower を設定する](#)」を参照してください。
- VPC のアカウント設定の変更方法については、アカウントの更新に関する「[Account Factory のドキュメント](#)」を参照してください。
- AWS Control Tower のネットワークと VPC を使用方法の詳細については、このユーザーガイドの関連情報ページで「[ネットワーク](#)」のセクションを参照してください。

AWS Control Tower の VPCs と AWS リージョン

アカウント作成の標準的な部分として、は、AWS Control Tower AWS で管理していないリージョンであっても、すべてのリージョンにデフォルト VPC AWS を作成します。このデフォルト VPC は、AWS Control Tower がプロビジョニングされたアカウント用に作成する VPC とは異なりますが、非管理リージョンの AWS デフォルト VPC には IAM ユーザーがアクセスできる場合があります。

管理者は、リージョン拒否コントロールを有効にして、エンドユーザーが AWS Control Tower がサポートするリージョンの VPC に接続する権限を持たないようにできます。ただし、管理対象外のリージョンです。リージョン拒否コントロールを設定するには、[Landing zone settings] (ランディングゾーン設定) ページに移動し、[Modify settings] (設定を変更する) を選択します。

リージョン拒否コントロールは、管理対象外のAWS リージョンにおけるほとんどのサービスへのAPI コールをブロックします。詳細については、[「リクエストされたAWSに基づいて へのアクセスを拒否する」](#)を参照してくださいAWS リージョン。

Note

リージョン拒否コントロールでは、AWS Control Tower がサポートされていないリージョンで IAM ユーザーがAWSのデフォルト VPC に接続することを妨げない場合があります。

必要に応じて、非管理リージョンのAWSデフォルト VPC を削除できます。VPCs リージョンのデフォルト VPC をリストするには、次の例と同様の CLI コマンドを使用できます。

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

AWS Control Tower と VPC の概要

AWS Control Tower VPC に関する重要な事実を以下に示します。

- Account Factory でアカウントをプロビジョニングするときに AWS Control Tower によって作成された VPC は、AWSデフォルトの VPC と同じではありません。
- AWS Control Tower がサポートされているAWSリージョンに新しいアカウントを設定すると、AWS Control Tower は自動的にデフォルトのAWS VPC を削除し、AWS Control Tower によって設定された新しい VPC を設定します。
- 各 AWS Control Tower アカウントには、AWS Control Tower で作成された 1 つの VPC が許可されます。アカウントは、アカウント制限内に追加のAWS VPCs を持つことができます。
- すべての AWS Control Tower VPC には、米国西部 (北カリフォルニア) リージョン、us-west-1、us-west-1 の 2 つのアベイラビリティゾーンを除くすべてのリージョンに 3 つのアベイラビリティゾーンがあります。デフォルトでは、各アベイラビリティゾーンに 1 つのパブリックサブネットと 2 つのプライベートサブネットが割り当てられます。したがって、米国西部 (北カリフォルニア) 以外のリージョンの場合、各 AWS Control Tower VPC には、デフォルトで 9 つのサブネットが含まれ、3 つのアベイラビリティゾーンに分かれています。米国西部 (北カリフォルニア) では、6 つのサブネットが 2 つのアベイラビリティゾーンで分割されます。
- AWS Control Tower VPC 内のサブネットのそれぞれに、同サイズの一意的 IP アドレス範囲が割り当てられます。

- VPC 内のサブネットの数は設定可能です。VPC のサブネット設定の変更方法の詳細については、「[Account Factory トピック](#)」を参照してください。
- IP アドレスが重複しないため、AWS Control Tower VPC 内の 6 または 9 つのサブネットは無制限に相互通信できます。

VPC を使用する場合、AWS Control Tower はリージョンレベルで区切りません。すべてのサブネットは、指定した正確な CIDR 範囲から割り当てられます。VPC のサブネットは、どのリージョンにも存在できます。

Notes (メモ)

VPC コストを管理する

新しいアカウントをプロビジョニングするときにパブリックサブネットが有効になるように Account Factory の VPC 設定を定義すると、Account Factory によって VPC が設定されて、NAT ゲートウェイが作成されます。料金は Amazon VPC による使用量に対して請求されます。

VPC とコントロールの設定

VPC インターネットアクセス設定を有効にして Account Factory アカウントをプロビジョニングすると、その Account Factory 設定によってコントロール「[顧客が管理する Amazon VPC インスタンスのインターネットアクセスを許可しない](#)」が上書きされます。新しくプロビジョニングされたアカウントのインターネットアクセスを有効にしないようにするには、Account Factory で設定を変更する必要があります。詳細については、「[Walkthrough: Configure AWS Control Tower Without a VPC](#)」を参照してください。

VPC と AWS Control Tower の CIDR とピア接続

このセクションは、主にネットワーク管理者を対象としています。通常、会社のネットワーク管理者は、AWS Control Tower 組織の全体的な CIDR 範囲を選択する担当者です。ネットワーク管理者は、特定の目的のために、その範囲内からサブネットを割り当てます。

VPC の CIDR 範囲を選択すると、AWS Control Tower は RFC 1918 仕様に従って IP アドレス範囲を検証します。Account Factory は、以下の範囲で最大 /16 の CIDR ブロックを許可します。

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10 (インターネットプロバイダーがこの範囲の使用を許可している場合のみ)

/16 区切り記号を使用すると、最大 65,536 個の IP アドレスを指定できます。

以下の範囲から有効な IP アドレスを割り当てることができます。

- 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 (192.168 範囲外の IP はありません)

指定した範囲がこれらの範囲外である場合、AWS Control Tower はエラーメッセージを表示します。

デフォルトの CIDR 範囲は 172.31.0.0/16 です。

AWS Control Tower は、選択された CIDR 範囲を使用して VPC を作成する際に、組織単位 (OU) 内に作成した各アカウントのすべての VPC に対して、同じ CIDR 範囲を割り当てます。IP アドレスのデフォルトオーバーラップのため、この実装では、OU 内のいずれかの AWS Control Tower VPC 間のピア接続が最初は許可されません。

サブネット

各 VPC 内で、AWS Control Tower は指定された CIDR 範囲を 9 つのサブネット間に均等に分割します (6 つのサブネットがある米国西部 (北カリフォルニア))。VPC 内のサブネットは重複しません。したがって、それらはすべて VPC 内において相互間で通信できます。

つまり、デフォルトでは VPC 内のサブネット通信は制限されません。VPC サブネット間の通信を制御するためのベストプラクティスは、必要に応じて、許可するトラフィックフローを定義するルールを使用してアクセスコントロールリストを設定することです。特定のインスタンス間のトラフィックを制御するには、セキュリティグループを使用します。AWS Control Tower でセキュリティグループとファイアウォールを設定する方法の詳細については、[「チュートリアル:AWS Firewall Manager を使用して AWS Control Tower でセキュリティグループを設定する」](#)を参照してください。

ピア接続

AWS Control Tower は、複数の VPC 間で通信するための VPC と VPC 間のピア接続を制限しません。ただし、デフォルトでは、すべての AWS Control Tower VPC のデフォルトの CIDR 範囲は同じです。ピア接続をサポートするために、IP アドレスが重複しないように Account Factory の設定で CIDR 範囲を変更できます。

Account Factory の設定で CIDR 範囲を変更すると、以降に AWS Control Tower で (Account Factory を使用して) 作成されるすべての新しいアカウントに新しい CIDR 範囲が割り当てられます。古いアカウントは更新されません。例えば、アカウントを作成し、CIDR 範囲を変更して新しいアカウントを作成すると、これら 2 つのアカウントに割り当てられた VPC 間はピア接続できます。IP アドレス範囲が同じではないため、ピア接続が可能です。

インターフェイスエンドポイントを使用して AWS Control Tower にアクセスする (AWS PrivateLink)

を使用して AWS PrivateLink、VPC と AWS Control Tower の間にプライベート接続を作成できます。インターネットゲートウェイ、NAT デバイス、VPN 接続、または Direct Connect 接続を使用せずに、VPC 内にあるかのように AWS Control Tower にアクセスできます。VPC のインスタンスは、パブリック IP アドレスがなくても AWS Control Tower にアクセスできます。

このプライベート接続を確立するには、AWS PrivateLink を利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、AWS Control Tower 宛てのトラフィックのエントリポイントとして機能するリクエスト管理型ネットワークインターフェイスです。

詳細については、「AWS PrivateLink ガイド」の [「Access AWS のサービス through AWS PrivateLink」](#) を参照してください。

AWS Control Tower に関する考慮事項

AWS Control Tower のインターフェイスエンドポイントを設定する前に、「AWS PrivateLink ガイド」の「[考慮事項](#)」を確認してください。

AWS Control Tower は、インターフェイスエンドポイントを介してすべての API アクションの呼び出しをサポートしています。

AWS Control Tower のインターフェイスエンドポイントを作成する

Amazon VPC コンソールまたは AWS Command Line Interface () を使用して、AWS Control Tower のインターフェイスエンドポイントを作成できますAWS CLI。詳細については、「AWS PrivateLink ガイド」の「[インターフェイスエンドポイントを作成](#)」を参照してください。

以下のサービス名を使用して、AWS Control Tower のインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.controltower
com.amazonaws.region.controltower-fips
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、リージョンのデフォルト DNS 名を使用して、AWS Control Tower への API リクエストを実行できます。例えば、controltower.us-east-1.amazonaws.com。

インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイント経由での AWS Control Tower へのフルアクセスが許可されています。VPC から AWS Control Tower に許可されるアクセスを制御するには、カスタム・エンドポイント・ポリシーをインターフェースのエンドポイントにアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、AWS PrivateLink ガイドの[Control access to services using endpoint policies \(エンドポイントポリシーを使用してサービスへのアクセスをコントロールする\)](#)を参照してください。

例: AWS Control Tower アクション用の VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。インターフェイスエンドポイントにアタッチされると、このポリシーは、すべてのリソースですべてのプリンシパルに、リストされている AWS Control Tower アクションへのアクセス権を付与します。


```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "controltower:ListEnabledControls",
        "controltower:ListLandingZones"
      ],
      "Resource": "*"
    }
  ]
}
```

 Note

AWS Control Tower API オペレーションの完全なリストについては、「[AWS Control Tower API リファレンス](#)」を参照してください。

必要なロールと許可

AWS Control Tower は IAM ロールを使用してリソースへのアクセスを管理します。

ロールの一般情報については、「[User groups, roles, and permission sets](#)」を参照してください。

アクセス許可について

- AWS Control Tower での IAM グループとそのアクセス許可の詳細については、「[IAM Identity Center groups for AWS Control Tower](#)」を参照してください。
- アカウントのプロビジョニングに必要なアクセス許可の詳細については、「[Permissions required for accounts](#)」を参照してください。
- AWS Control Tower に必要なコンソールアクセス許可の詳細については、「[Permissions required to use the AWS Control Tower console](#)」を参照してください。

ロールについて

- プログラムによるアクセス用に設計されたアクセス許可も含め、ロールの作成方法については、「[Create roles and assign permissions](#)」および「[Programmatic roles and trust relationships for the AWS Control Tower audit account](#)」を参照してください。
- AWS Control Tower がアカウントの管理に使用するその他のロールの詳細については、「[Using identity-based policies \(IAM policies\) for AWS Control Tower](#)」および「[Managed policies for AWS Control Tower](#)」を参照してください。
- AWS Control Tower と AWS Config ロールの詳細については、「[AWS Control Tower ConfigRecorderRole](#)」を参照してください。
- AWS Control Tower がアカウントの AWS Config 情報を集約するために使用するロールの詳細については、「[AWS Control Tower がアンマネージド OU とアカウントで AWS Config ルールを集約する方法 OUs](#)」を参照してください。
- ロールとアクセス許可を割り当てるときにリソースを保護する方法については、「[ロールの信頼関係のオプション条件](#)」、「[オプションで AWS KMS キーを設定する](#)」、「[サービス間のなりすましを防ぐ](#)」を参照してください。
- IAM ロールによる AWS Control Tower での自動アカウントプロビジョニングに関する具体的な情報については、「[Automated Account Provisioning with IAM Roles](#)」を参照してください。
- AWS Config SNS トピックを保護するポリシーを表示するには、「[SNS AWS Config トピックポリシー](#)」を参照してください。

AWS Control Tower がロールと連携してアカウントを作成および管理する方法

一般に、ロールは AWS における Identity and Access Management (IAM) の一部です。の IAM とロールに関する一般的な情報については AWS、[IAM AWS ユーザーガイドの「IAM ロール」トピック](#)を参照してください。

ロールとアカウントの作成

AWS Control Tower は、AWS Organizations の CreateAccount API を呼び出して、顧客のアカウントを作成します。がこのアカウント AWS Organizations を作成すると、そのアカウント内にロールが作成されます。このロールは、AWS Control Tower が API にパラメータを渡して名前を付けます。ロールの名前は AWSControlTowerExecution です。

AWS Control Tower は、Account Factory によって作成されたすべてのアカウントの AWSControlTowerExecution ロールを引き継ぎます。このロールを使用して、AWS Control Tower は、アカウントにベースライニングを行い、必須の (およびその他有効な) コントロールを適用します。これにより、他のロールが作成されます。これらのロールは、次に AWS Config などの他のサービスによって使用されます。

Note

アカウントのベースライニングとは、そのリソースを設定することです ([Account Factory テンプレート](#)を含む)。これはブループリントまたはコントロールと呼ばれることもあります。ベースライニングのプロセスでは、テンプレートのデプロイの一部として、一元化されたログ記録とセキュリティ監査のロールもアカウントにセットアップします。AWS Control Tower ベースラインは、登録されているすべてのアカウントに適用するロールに含まれています。

アカウントとリソースの詳細については、「[AWS Control Tower AWS アカウント の について](#)」を参照してください。

AWSControlTowerExecution ロールについての説明

AWSControlTowerExecution ロールは、登録されたすべてのアカウントに存在する必要があります。これにより AWS Control Tower が個々のアカウントを管理し、それらのアカウントに関する情報を監査アカウントおよびログアーカイブアカウントに報告できるようにするものです。

AWSControlTowerExecution ロールは、次のように、いくつかの方法でアカウントに追加できます。

- セキュリティ OU のアカウント (コアアカウントと呼ばれることもあります) の場合、AWS Control Tower は、AWS Control Tower の初期セットアップ時にロールを作成します。
- AWS Control Tower コンソールで作成された Account Factory アカウントの場合、AWS Control Tower は、アカウント作成時にこのロールを作成します。
- アカウント登録が 1 つの場合は、ロールを手動で作成し、AWS Control Tower にアカウントを登録するようお客様に依頼します。
- ガバナンスを OU に拡張する場合、AWS Control Tower は、StackSet-AWSControlTowerExecutionRole を使用して、その OU 内のすべてのアカウントにロールを作成します。

 Note

アカウントの登録を解除すると、手動で作成されたか、AWS Control Tower 自体によって作成されたかにかかわらず、AWS Control Tower は AWSControlTowerExecution ロールを削除します。

AWSControlTowerExecution ロールの目的:

- AWSControlTowerExecution では、スクリプトと Lambda 関数を使用して、アカウントを自動的に作成および登録できます。
- AWSControlTowerExecution では、各アカウントのすべてのログがロギングアカウントに送信されるよう、組織のロギングを設定できます。
- AWSControlTowerExecution では、AWS Control Tower に個別のアカウントを登録できます。最初に、そのアカウントに AWSControlTowerExecution ロールを追加する必要があります。ロールの追加手順については、「[必要な IAM ロールを既存の に手動で追加 AWS アカウント して登録する](#)」を参照してください。

AWSControlTowerExecution ロールと OU の連携方法:

AWSControlTowerExecution ロールは、選択した AWS Control Tower コントロールが自動的に、組織内の各 OU の個々のアカウントに適用され、AWS Control Tower で作成したすべての新規アカウントにも適用されるようにします。結果として、以下のようになります。

- AWS Control Tower [コントロール](#)によって具体化される監査機能とロギング機能に基づいて、コンプライアンスレポートとセキュリティレポートをより簡単に提供できます。
- セキュリティチームとコンプライアンスチームは、すべての要件が満たされていること、組織ドリフトが発生していないことを確認できます。

ドリフトの詳細については、「[Detect and resolve drift in AWS Control Tower](#)」(AWS Control Tower でドリフトを検出して解決する)を参照してください。

つまり、AWSControlTowerExecution ロールとその関連ポリシーを使って、組織全体のセキュリティとコンプライアンスを柔軟に管理できるということです。したがって、セキュリティまたはプロトコルの違反が発生する可能性が低くなります。

ロールの信頼関係のオプションの条件

AWS Control Tower 環境に追加のセキュリティレイヤーを追加するには、AWS Control Tower の特定のロールとやり取りするアカウントとリソースを制限するために、ロールの信頼ポリシーに条件を課すことができます。例えば、広範なアクセス許可を許可するために、AWSControlTowerAdmin ロールへのアクセスをさらに制限できます。

脅威アクターがリソースにアクセスできないようにするには、AWS Control Tower の信頼ポリシーを手動で編集して、ポリシーステートメントに `aws:SourceArn` 条件または `aws:SourceAccount` 条件を少なくとも 1 つ追加します。追加のセキュリティのベストプラクティスとして、`aws:SourceArn` 条件を追加することができます。これは `aws:SourceAccount` より具体的であり、特定のアカウントと特定のリソースへのアクセスを制限するためです。

リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合は、`aws:SourceArn` 条件を使用し、ARN の未知の部分にワイルドカード (*) を使用できます。例えば、`arn:aws:controltower:*:123456789012:*` は、リージョンを指定しない場合に機能します。

以下の例では、IAM ロールの信頼ポリシーと共に `aws:SourceArn` IAM 条件を使用しています。AWSControlTowerAdmin ロールの信頼関係に条件を追加します。これは、AWS Control Tower サービスプリンシパルがこのロールとやり取りするためです。

例に示すように、ソース ARN の形式は次のとおりで

す。 `arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:`

文字列 `${HOME_REGION}` および `${CUSTOMER_AWSACCOUNT_id}` を、自身のホームリージョンと呼び出しアカウントのアカウント ID で置き換えます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

この例では、arn:aws:controltower:us-west-2:012345678901:* と指定されているソース ARN が、sts:AssumeRole アクションの実行を許可される唯一の ARN となります。つまり、us-west-2 リージョンで、アカウント ID 012345678901 にサインインできるユーザーのみが、controltower.amazonaws.com と指定された AWS Control Tower サービスのこの特定のロールと信頼関係を必要とするアクションの実行を許可されます。

次の例は、ロールの信頼ポリシーに適用される aws:SourceAccount 条件と aws:SourceArn 条件を示しています。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
```

```
        "controltower.amazonaws.com"
    ],
    },
    "Action": "sts:AssumeRole",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "012345678901"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
    }
}
]
```

この例は、aws:SourceAccount 条件ステートメントが追加された、aws:SourceArn 条件ステートメントを示しています。詳細については、「[クロスサービス偽装の防止](#)」を参照してください。

AWS Control Tower のアクセス許可ポリシーの一般的な情報については、「[リソースへのアクセスの管理](#)」を参照してください。

推奨事項:

AWS Control Tower が作成するロールに条件を追加することをお勧めします。このロールは他の AWS のサービスによって直接引き受けられるためです。詳細については、このセクションで前に示した AWSControlTowerAdmin の例を参照してください。AWS Config レコーダーロールについては、aws:SourceArn 条件を追加し、許可されたソース ARN として Config レコーダー ARN を指定することをお勧めします。

すべての管理アカウントの AWSControlTowerExecution などのロール、または AWS Control Tower 監査アカウントが[引き受け可能なその他のプログラムによるロール](#)については、これらのロールの信頼ポリシーに aws:PrincipalOrgID 条件を追加することをお勧めします。これにより、リソースにアクセスするプリンシパルが正しい AWS 組織のアカウントに属していることが検証されます。aws:SourceArn 条件ステートメントは期待どおりに機能しないため、追加しないでください。

Note

ドリフトの場合は、特定の状況で AWS Control Tower ロールがリセットされる可能性があります。ロールをカスタマイズしている場合は、ロールを定期的に再確認することをお勧めします。

AWS Control Tower がアンマネージド OUsとアカウントで AWS Config ルールを集約する方法

- AWS Control Tower 管理アカウントは、外部 AWS Config ルールの検出を支援する組織レベルのアグリゲータを作成します。これにより、AWS Control Tower はアンマネージドアカウントにアクセスする必要はありません。AWS Control Tower コンソールには、特定のアカウントに対して外部で作成された AWS Config ルールが表示されます。これらの外部ルールの詳細は、[アカウントの詳細] ページの [外部の Config ルールのコンプライアンス] タブで確認できます。
- アグリゲータを作成するために、AWS Control Tower は、組織について記述し、そのアカウントを一覧表示するために必要な許可を持つロールを追加します。AWSControlTowerConfigAggregatorRoleForOrganizations ロールには、AWSConfigRoleForOrganizations マネージドポリシーと、config.amazonaws.com との信頼関係が必要です。

Note

ランディングゾーンバージョン 4.0 を使用しているお客様は、AWS Control Tower が既存の組織レベルの設定アグリゲータからサービスにリンクされた設定アグリゲータに移行したため、このロールは必要ありません。

Note

ランディングゾーンを含む組織で信頼されたアクセスを有効にすると、AWS Control Tower は組織内のすべてのアカウントのロールの作成、リソースの管理、データの読み取りを行うことができます。信頼されたアクセスを通じて、組織内のアカウントまたは OU は、登録済みか登録済みかにかかわらず、AWS Control Tower で利用できます。

ロールにアタッチされた IAM ポリシー (JSON アーティファクト) は次のとおりです。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSControlTowerConfigAggregatorRoleForOrganizations の信頼関係は次のとおりです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

管理アカウントにこの機能をデプロイするには、管理ポリシーに次のアクセス許可が追加されます。これはAWSControlTowerServiceRolePolicy、AWS Config アグリゲータの作成時にAWSControlTowerAdminロールによって使用されます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:PutConfigurationAggregator",
        "config>DeleteConfigurationAggregator",
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:role/service-role/AWSControlTowerConfigAggregatorRoleForOrganizations",
        "arn:aws:config:us-east-1:123456789012:config-aggregator/"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "organizations:EnableAWSServiceAccess",
      "Resource": "*"
    }
  ]
}
```

新しいリソース、AWSControlTowerConfigAggregatorRoleForOrganizations および aws-controltower-ConfigAggregatorForOrganizations が作成されました。

準備ができたら、アカウントを個別に登録するか、OU を登録してグループとしてアカウントを登録することができます。アカウントを登録すると、でルールを作成すると AWS Config、AWS Control Tower は新しいルールを検出します。アグリゲータは外部ルールの数を表示し、アカウントの各外部ルールの詳細を表示できる AWS Config コンソールへのリンクを提供します。AWS Config コンソールと AWS Control Tower コンソールの情報を使用して、アカウントで適切なコントロールが有効になっているかどうかを判断します。

AWS Control Tower 監査アカウントのプログラムによるロールおよび信頼関係

監査アカウントにサインインし、他のアカウントをプログラムで確認するロールを引き受けることができます。監査アカウントでは、他のアカウントに手動でログインすることはできません。

監査アカウントは、AWS Lambda 関数にのみ付与される一部のロールを使用して、他のアカウントへのプログラムによるアクセスを許可します。セキュリティ上の理由から、これらのロールには他のロールとの信頼関係があります。つまり、ロールを利用できる条件が厳密に定義されていることを意味します。

AWS Control Tower スタック `StackSet-AWSCoontrolTowerBP-BASELINE-ROLES` は、監査アカウントに次のプログラム専用のクロスアカウント IAM ロールを作成します。

- `aws-controltower-AdministratorExecutionRole`
- `aws-controltower-ReadOnlyExecutionRole`

AWS Control Tower スタック `StackSet-AWSCoontrolTowerSecurityResources` は、監査アカウントに次のプログラム専用のクロスアカウント IAM ロールを作成します。

- `aws-controltower-AuditAdministratorRole`
- `aws-controltower-AuditReadOnlyRole`

`ReadOnlyExecutionRole`: このロールは、監査アカウントが、組織全体の Amazon S3 バケット内のオブジェクトを読み取ることを許可する点に注意してください (メタデータアクセスのみを許可する `SecurityAudit` ポリシーとは対照的です)。

`aws-controltower-AdministratorExecutionRole`:

- 管理者権限があります
- コンソールから引き受けることはできません
- 監査アカウントのロール (`aws-controltower-AuditAdministratorRole`) でのみ引き受けることができます

次のアーティファクトは、`aws-controltower-AdministratorExecutionRole` の信頼関係を示しています。プレースホルダー番号 `012345678901` は、監査アカウントの `Audit_acct_ID` 番号に置き換えられます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-AuditAdministratorRole:

- AWS Lambda サービスでのみ引き受けることができます
- 文字列 log で始まる名前を持つ Simple Storage Service (Amazon S3) オブジェクトに対して読み取り (Get) 操作および書き込み (Put) 操作を実行する許可があります

アタッチされるポリシー:

1. AWSLambdaExecute AWS 管理ポリシー

2. AssumeRole-aws-controltower-AuditAdministratorRole – インラインポリシー – AWS Control Tower によって作成されます。アーティファクトは次のとおりです。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```
]
}
```

次のアーティファクトは、aws-controltower-AuditAdministratorRole の信頼関係を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-ReadOnlyExecutionRole:

- コンソールから引き受けることはできません
- 監査アカウントの別のロール (AuditReadOnlyRole) でのみ引き受けることができます

次のアーティファクトは、aws-controltower-ReadOnlyExecutionRole の信頼関係を示しています。プレースホルダー番号 012345678901 は、監査アカウントの Audit_acct_ID 番号に置き換えられます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-AuditReadOnlyRole:

- AWS Lambda サービスでのみ引き受けることができます
- 文字列 log で始まる名前を持つ Simple Storage Service (Amazon S3) オブジェクトに対して読み取り (Get) 操作および書き込み (Put) 操作を実行する許可があります

アタッチされるポリシー:

1. AWSLambdaExecute AWS 管理ポリシー

2. AssumeRole-aws-controltower-AuditReadOnlyRole – インラインポリシー – AWS Control Tower によって作成されます。アーティファクトは次のとおりです。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

次のアーティファクトは、aws-controltower-AuditAdministratorRole の信頼関係を示しています。

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

```
    },
    "Action": "sts:AssumeRole"
  }
]
}
```

IAM ロールを使用した自動アカウントプロビジョニング

Account Factory アカウントの設定をさらに自動化するには、メンバーアカウントの [AWSControlTowerExecution ロールを引き受ける](#) AWS Control Tower 管理アカウントで Lambda 関数を作成します。次に、管理アカウントが、ロールを使用して、各メンバーアカウントで必要な設定手順を実行します。

ただし、Lambda 関数を使用してアカウントをプロビジョニングする場合、この作業を実行するアイデンティティには `AWSServiceCatalogEndUserFullAccess` に加え、次の IAM アクセス許可ポリシーが必要です。

JSON

```
{
  "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: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": "*"
}
]
}

```

アクセス許可

sso:GetPeregrineStatus、sso:ProvisionApplicationInstanceForAWSAccount、sso:ProvisionApplicationProfileForAWSAccount、sso:ProvisionSAMLProvider、および sso:ProvisionSAMLProvider は、AWS Control Tower Account Factory が IAM Identity Center AWS とやり取りするために必要です。

AWS Control Tower のリソース

- AWS Control Tower のリソース所有権に関する一般情報については、「[AWS Control Tower リソースに対するアクセス許可の管理の概要](#)」を参照してください。
- AWS Control Tower が共有アカウントに作成するリソースの詳細については、「[共有アカウントについて](#)」を参照してください。
- AWS Control Tower が Account Factory を通じてアカウントをプロビジョニングするときに作成するリソースの詳細については、「[Account Factory のリソースに関する考慮事項](#)」を参照してください。
- AWS Control Tower で定義されている AWS リソースタイプの詳細を表示するには、AWS CloudFormation 「ユーザーガイド」の「[AWS Control Tower リソースタイプのリファレンス APIs](#)」を参照してください。 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_ControlTower.html

AWS リージョンと AWS Control Tower の連携方法

AWS Control Tower は、次の AWS リージョンでサポートされています。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (オレゴン)
- カナダ (中部)
- アジアパシフィック (シドニー)
- アジアパシフィック (シンガポール)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ストックホルム)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (東京)
- 欧州 (パリ)
- 南米 (サンパウロ)
- 米国西部 (北カリフォルニア)
- アジアパシフィック (香港)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (大阪)
- 欧州 (ミラノ)
- アフリカ (ケープタウン)
- 中東 (バーレーン)
- イスラエル (テルアビブ)
- 中東 (アラブ首長国連邦)
- 欧州 (スペイン)
- アジアパシフィック (ハイデラバード)
- 欧州 (チューリッヒ)

- アジアパシフィック (メルボルン)
- カナダ西部 (カルガリー)
- マレーシア (クアラルンプール)
- アジアパシフィック (タイ)
- メキシコ (中部)
- アジアパシフィック (台北)

ホームリージョンについて

ランディングゾーンを作成すると、AWS マネジメントコンソールへのアクセスに使用しているリージョンが AWS Control Tower のホーム AWS リージョンになります。作成プロセス中に、一部のリソースがホームリージョンにプロビジョニングされます。その他のリソース (OU や AWS アカウント) はグローバルです。

いったん選択したホームリージョンは変更できません。

コントロールとリージョン

現在、予防コントロールはすべてグローバルに使用できます。一方、検出およびプロアクティブコントロールは、AWS Control Tower がサポートされているリージョンでのみ機能します。新しいリージョンで AWS Control Tower を有効にした場合のコントロールの動作の詳細については、「[AWS Control Tower リージョンの設定](#)」を参照してください。

AWS Control Tower リージョンの設定

このセクションでは、AWS Control Tower ランディングゾーンを新しい AWS リージョンに拡張したり、ランディングゾーン設定からリージョンを削除したりする場合に想定される動作について説明します。このアクションは通常、AWS Control Tower コンソールの [Update] (更新) 機能を使用して実行します。

Note

ワークロードの実行を必要としない AWS リージョンに AWS Control Tower ランディングゾーンを拡張しないでください。リージョンをオプトアウトしても、そのリージョンへのリソースのデプロイを阻止できませんが、デプロイしたリソースは AWS Control Tower によって管理されません。

新しいリージョンの設定時に、AWS Control Tower はランディングゾーンを更新します。つまり、ランディングゾーンをベースラインとして次のことを行います。

- 新たに選択されたすべてのリージョンでアクティブに動作します。
- 選択解除されたリージョンのリソースの管理を停止します。

AWS Control Tower が管理する組織単位 (OU) 内の個々のアカウントは、このランディングゾーンの更新プロセスの一環として更新されません。そのため、OU を再登録してアカウントを更新する必要があります。

AWS Control Tower リージョンを設定するときは、次のレコメンデーションと制限事項に注意してください。

- AWS リソースまたはワークロードをホストする予定のリージョンを選択します。
- リージョンをオプトアウトしても、そのリージョンへのリソースのデプロイを阻止できませんが、デプロイしたリソースは AWS Control Tower によって管理されません。

新しいリージョンのランディングゾーンを設定するときに、AWS Control Tower 検出コントロールは次のルールに従います。

- 既存のものに変更はありません。検出コントロールでも予防コントロールでも、その動作は、既存のリージョンの既存の OU における既存のアカウントでは変わりません。
- 更新されていないアカウントが含まれている既存の OU に新しい検出コントロールを適用することはできません。新しいリージョンに AWS Control Tower ランディングゾーンを設定したら (ランディングゾーンを更新することによって)、既存の OU および既存のアカウントで新しい検出コントロールを有効にする前に、既存の OU で必ず既存のアカウントを更新してください。
- 既存の検出コントロールは、アカウントを更新するとすぐに新しく設定したリージョンで機能し始めます。AWS Control Tower ランディングゾーンを更新して新しいリージョンを設定し、アカウントを更新すると、OU で既に有効になっている検出コントロールが、新しく設定したリージョン内のそのアカウントで機能し始めます。

AWS Control Tower リージョンの設定

1. <https://console.aws.amazon.com//controlltower> で AWS Control Tower コンソールにサインインします。

2. 左ペインのナビゲーションメニューで、[Landing zone settings] (ランディングゾーン設定) を選択します。
3. [Landing zone settings] (ランディングゾーン設定) ページの [Details] (詳細) セクションで、右上の [Modify settings] (設定を変更する) ボタンを選択します。ランディングゾーン更新ワークフローに移動します。新しいリージョンを管理したり、リージョンを管理対象から除外したりするには、最新のランディングゾーンバージョンに更新する必要があるためです。
4. ガバナンスの追加 AWS リージョンで、管理するリージョンを検索します (または管理を停止します)。[State] (状態) 列に、現在管理対象となっているリージョンと管理対象になっていないリージョンが表示されます。
5. 追加で管理対象とする各リージョンのチェックボックスをオンにします。管理対象から除外する各リージョンのチェックボックスをオフにします。

 Note

リージョンを管理対象にしないことにした場合、引き続きそのリージョンにリソースをデプロイできますが、そのリソースは AWS Control Tower の管理対象外になります。

6. 残りのワークフローを完了し、[Update landing zone] (ランディングゾーンの更新) を選択します。
7. ランディングゾーンのセットアップが完了したら、OU を再登録して新しいリージョンのアカウントを更新します。詳細については、「[AWS Control Tower の OU とアカウントを更新する場合](#)」を参照してください。

新しいリージョンの設定後に個々のアカウントをプロビジョニングまたは更新するには、[Service Catalog の API フレームワーク](#)と [AWS CLI](#) を使用してバッチ処理でアカウントを更新する方法もあります。詳細については、「[自動化によるアカウントのプロビジョニングと更新](#)」を参照してください。

リージョンを設定する際は混合ガバナンスを避ける

AWS Control Tower ガバナンスを新しいリージョンに拡張した後、およびリージョンから AWS Control Tower ガバナンスを削除した後 AWS リージョン、OU 内のすべてのアカウントを更新することが重要です。

混合ガバナンスは、OU を管理するコントロールが OU 内の各アカウントを管理するコントロールと完全に一致しない場合に発生する可能性がある望ましくない状況です。AWS Control Tower がガ

バナンスを新しい に拡張した後、またはガバナンスを削除した後にアカウントが更新されない場合 AWS リージョン、混合ガバナンスは OU で発生します。

このような状況では、OU 内の特定のアカウントが、OU 内の他のアカウントと比較されたり、ランディングゾーンの全体的なガバナンス体制と比較されたりすると、リージョンごとに異なるコントロールが適用されることがあります。

ガバナンスが混在している OU では、新しいアカウントをプロビジョニングすると、その新しいアカウントには、ランディングゾーンと同じ (更新された) リージョンと OU のガバナンス体制が適用されます。ただし、まだ更新されていない既存のアカウントには、更新されたリージョンガバナンス体制は適用されません。

一般に、混合ガバナンスでは、AWS Control Tower コンソールのステータスインジケータが矛盾したり不正確になったりすることがあります。たとえば、混合ガバナンスの場合、まだ更新されていないアカウントについては、登録済み OU のオプトインリージョンが「管理なし」ステータスで表示されます。

Note

AWS Control Tower は、混合ガバナンスの状態ではコントロールを有効にすることはできません。

混合ガバナンスにおけるコントロールの動作

- 混合ガバナンス中、AWS Control Tower は、OU の一部のアカウントが更新されていないため、OU が既に管理対象として表示しているリージョンに、AWS Config ルールに基づくコントロール (検出コントロール) を一貫してデプロイできません。FAILED_TO_ENABLE エラーメッセージが表示されることがあります。
- 混合ガバナンスの場合、OU 内のアカウントがまだ更新されていない状態でランディングゾーンのガバナンスをオプトインリージョンに拡張すると、OU の EnableControl API 操作は検出および予防コントロールについては失敗します。OU 内の更新されていないメンバーアカウントはまだそれらのリージョンにオプトインされていないため、FAILED_TO_ENABLE エラーメッセージが表示されます。
- 混合ガバナンス中、Security Hub CSPM Service-managed Standard: AWS Control Tower の一部であるコントロールは、ランディングゾーン設定と更新されていないアカウントの間に不一致があるリージョンでは、コンプライアンスを正確に報告できません。

- 混合ガバナンスによって SCP ベースのコントロール (予防コントロール) の動作が変わることはなく、すべての管理対象リージョンの OU 内のすべてのアカウントに一律に適用されます。

Note

混合ガバナンスはドリフトとは異なり、ドリフトとして報告されません。

混合ガバナンスを修復するには

- お客様は、リージョン別コントロールをリセットすることで、混合ガバナンスを修復できるようになりました。グローバル以外のコントロールはすべてリージョン (検出的コントロールとプロアクティブコントロール) です。アラートバナーを通じて、OU が混合ガバナンスにあることが警告されます。

AWS オプトインリージョンをアクティブ化する際の考慮事項

のほとんどの AWS リージョン はデフォルトでアクティブですが AWS アカウント、特定のリージョンは手動で選択した場合にのみアクティブになります。このドキュメントでは、これらのリージョンをオプトインリージョンと呼んでいます。対照的に、 が作成されるとすぐに、デフォルトでアクティブなリージョン AWS アカウント は、商用リージョン、デフォルトリージョン、または単にリージョンと呼ばれます。

オプトインという用語には歴史的な根拠があります。2019 年 3 月 20 日以降に導入された AWS リージョン はすべてオプトインリージョンとしてデプロイされます。オプトインリージョンでは、そのリージョンの使用をオプトインしない限り、アカウントはそのリージョン内で有効になっておらず、ID はリージョンにレプリケートされません。ユーザー、グループ、ロール、ポリシー、ID プロバイダー、関連データ (X.509 署名証明書やコンテキスト固有の認証情報など)、パスワードポリシーやアカウントエイリアスなどの他のアカウントレベルの設定を含む、IAM サービスを通じて管理されるすべてのデータは ID データと見なされます。

オプトインリージョンは、ランディングゾーン設定時に選択することで自動的にアクティブ化できます。ランディングゾーンは、選択したすべてのリージョンで有効になります。

AWS Control Tower ホームリージョンとしてオプトインリージョンを選択する場合は、まず AWS マネジメントコンソールにサインインしたときに [リージョンを有効にする](#) のステップに従ってアクティブ化します。オプトインリージョンから既存のログアーカイブアカウントと監査アカウントを取得するには、まずそのリージョンを手動でアクティブ化します。

AWS オプトインリージョンには、AWS Control Tower が利用可能な複数のリージョンが含まれています。

- アジアパシフィック (香港) リージョン、ap-east-1
- アジアパシフィック (ジャカルタ) リージョン、ap-southeast-3
- 欧州 (ミラノ) リージョン、eu-south-1
- アフリカ (ケープタウン) リージョン、af-south-1
- 中東 (バーレーン) リージョン、me-south-1
- イスラエル (テルアビブ)、il-central-1
- 中東 (UAE) リージョン、me-central-1
- 欧州 (スペイン) リージョン、eu-south-2
- アジアパシフィック (ハイデラバード) リージョン、ap-south-2
- 欧州 (チューリッヒ) リージョン、eu-central-2
- アジアパシフィック (メルボルン) リージョン、ap-southeast-4
- カナダ西部 (カルガリー) リージョン、ca-west-1
- アジアパシフィック (タイ)、ap-southeast-7
- メキシコ (中部)、mx-central-1
- アジアパシフィック (台北)、ap-east-2
- アジアパシフィック (ニュージーランド)、ap-southeast-6

AWS Control Tower には、オプトインリージョンとデフォルトリージョン (他の商用リージョン) では動作が異なるコントロールがいくつかあります。詳細については、「[コントロールの制限事項](#)」を参照してください。オプトインリージョンにワークロードをデプロイする際に留意すべき点をいくつか紹介します。

管理がアクティブ化か？

リージョンの管理は AWS Control Tower コンソールから選択できるアクションであるため、リージョンにコントロールを適用できることを忘れないでください。オプトインリージョンをアクティブ化または非アクティブ化することは、AWS コンソールで選択できるもう 1 つのアクションです。これにより、リージョンがアカウントで開かれ、そのリージョンにリソースとワークロードをデプロイできるようになります。

動作に関する注意事項

- オプトインリージョンを管理する場合は、ワークロードの障害につながる可能性があるため、管理対象のオプトインリージョンを非アクティブ化 (オプトアウト) しないことをお勧めします。AWS Control Tower では、AWS Control Tower コンソール内から管理対象リージョンを非アクティブ化することはできませんが、AWS 請求コンソールや AWS SDK などの AWS Control Tower 外のソースから管理対象リージョンを非アクティブ化しないでください。
- AWS Control Tower がガバナンスをオプトインリージョンに拡張すると、すべてのメンバーアカウントでそのリージョンがアクティブ化 (オプトイン) されます。リージョンを管理から削除しても、AWS Control Tower はメンバーアカウントのリージョンを非アクティブ化 (オプトアウト) しません。
- リージョンの選択解除中、AWS Control Tower は、AWS 請求コンソールや AWS SDK などの AWS Control Tower 外のソースからアカウントに対してそのリージョンを手動で非アクティブ化した場合、オプトインリージョンからのリソースの削除をスキップします。非アクティブ化したリージョンからはリソースを削除することをお勧めします。そうしないと、それらのリソースに対して予想外の請求が発生する可能性があります。
- ランディングゾーンが廃止された場合、AWS Control Tower はオプトインリージョンを含むすべての管理対象リージョンのリソースをクリーンアップします。ただし、AWS Control Tower では、オプトインリージョンが非アクティブ化されません。廃止後の追加手順として、オプトインリージョンを非アクティブ化できます。
- ホームリージョンがオプトインリージョンで、既存のアカウントをログアーカイブアカウントと監査アカウントとして登録する場合、オプトインリージョンをランディングゾーンのホームリージョンとして選択する前に、オプトインリージョンを手動でアクティブ化する必要があります。[リージョンを有効にする](#)を参照
- AWS Control Tower がオプトインリージョンをホームリージョンとして設定されていて、他のリージョンの AWS コンソールから AWS Control Tower サービスにアクセスすると、コンソールは自動的にホームリージョンにリダイレクトされません。
- 基盤となる API には容量制限があり、リージョンの数、アカウント数、サービスの負荷によっては、レイテンシーが数分から数時間に増加する可能性があります。ベストプラクティスとして、ワークロードを実行する AWS リージョン のみにオプトインし、一度に 1 つのリージョンにオプトインします。

管理とアカウントに関する重要な制限

- AWS Control Tower が利用可能な 16 を超える商用リージョン (オプトインリージョンを含む) が管理されている場合、OU を登録する際の組織単位 (OU) あたりのアカウント数の上限が引き下げられます。詳細については、[「基盤となる AWS サービスに基づく制限」](#) を参照してください。

リージョン拒否コントロールの設定

AWS Control Tower には 2 つのリージョン拒否コントロールがあります。1 つのコントロール `GRREGIONDENY` を有効にすると、ランディングゾーン全体に適用されます。別のコントロール `CTMULTISERVICEPV1` を有効にすると、指定した特定の OU に適用できます。詳細については、[「リクエストされた AWS に基づいて へのアクセスを拒否する AWS リージョン」](#) および [「OU に適用されたリージョン拒否コントロール」](#) を参照してください。

ランディングゾーンのリージョン拒否コントロールに関する考慮事項

リージョン拒否コントロールである `GRREGIONDENY` は独特のコントロールです。特定の OU ではなく、ランディングゾーン全体に適用されるためです。リージョン拒否コントロールを設定するには、[Landing zone settings] (ランディングゾーン設定) ページに移動し、[Modify settings] (設定を変更する) を選択します。

- この設定は後で変更できます。
- 有効にすると、このコントロールが登録済みのすべての OU に適用されます。
- このコントロールは個々の OU には設定できません。

Note

リージョン拒否コントロールを有効にする前に、適用するリージョンに既存のリソースがないことを確認してください。コントロールを適用すると、以後そのリージョン内のリソースにアクセスできなくなるためです。このコントロールが有効になっている間は、拒否したリージョンにリソースをデプロイできません。

リージョン拒否コントロールを有効にすると、このコントロールは階層の最上位にある登録済みのすべての OU に適用され、それが階層の下位にある OU に継承されます。コントロールを削除すると、登録済みのすべての OU でコントロールが削除され、AWS Control Tower の管理対象でないす

すべてのリージョンが [Not Governed] (管理対象外) ステータスのままになり、AWS Control Tower が利用できないリージョンにリソースをデプロイできるようになります。

例外

ホームリージョンへのアクセスを拒否することはできません。IAM や などの特定のグローバル AWS サービスは AWS Organizations、リージョン拒否コントロールから除外されます。詳細については、「[Deny access to AWS based on the requested AWS リージョン](#)」を参照してください。

- 完全なコントロール名: リクエスト AWS されたリージョン AWS に基づいて へのアクセスを拒否する
- コントロールの説明: 指定されたリージョンの外部にあるグローバルサービスおよびリージョンサービスでは、リストされていない操作へのアクセスを禁止します。
- これは、予防ガイダンスによる選択的コントロールです。

リージョン拒否コントロール SCP のテンプレートを表示するには、「AWS Control Tower Control reference」の「[Deny access to AWS based on the requested AWS リージョン](#)」を参照してください。AWS Control Tower SCP は [の SCP AWS Organizations](#) と似ていますが、同一ではありません。

[リージョンサービスページ](#)でリージョンサービスエンドポイントを設定できます。

OU レベルでのリージョン拒否コントロールに関する考慮事項

OU レベルのリージョン拒否コントロールに関する主な考慮事項は、ランディングゾーンのリージョン拒否コントロールも有効になっている場合に、それがランディングゾーンのリージョン拒否コントロールとどのように相互作用するかを判断することです。詳細については、「[Region deny control applied to the OU](#)」を参照してください。

また、「[Configure the Region deny control](#)」を確認することもできます。

AWS Control Tower AWS アカウント の について

AWS アカウント は、所有するすべてのリソースのコンテナです。これらのリソースには、アカウントによって受け入れられる AWS Identity and Access Management (IAM) ID が含まれます。これは、そのアカウントにアクセスできるユーザーを決定します。IAM アイデンティティには、ユーザー、グループ、ロールなどがあります。AWS Control Tower で IAM、ユーザー、ロール、およびポリシーを使用する方法の詳細については、「[AWS Control Tower の Identity and Access Management](#)」を参照してください。

リソースとアカウントの作成時間

AWS Control Tower は、アカウントを作成または登録するときに、アカウントに必要な最小限のリソース設定をデプロイします。たとえば、[Account Factory テンプレート](#)の形式のリソースや、IAM ロール、AWS CloudTrail 証跡、[Service Catalog プロビジョニング済み製品](#)、IAM Identity Center ユーザーなどのランディングゾーン内の他のリソースが含まれる場合があります。AWS Control Tower は、コントロール設定に応じて、新しいアカウントがメンバーアカウントになることになっている組織単位 (OU) のリソースもデプロイします。

AWS Control Tower は、ユーザーに代わってこれらのリソースのデプロイをオーケストレーションします。デプロイを完了するにはリソースごとに数分かかる場合があるため、アカウントを作成または登録する前に作業の合計時間を考慮してください。アカウントのリソースの管理の詳細については、「[AWS Control Tower リソースの作成と変更に関するガイダンス](#)」を参照してください。

AWS Control Tower がアカウントを作成した場合に起きること

AWS Control Tower の新しいアカウントが作成され、AWS Control Tower 間のやり取りによってプロビジョニングされます AWS Organizations AWS Service Catalog。AWS Control Tower コンソールからアカウントを作成し、既存のアカウントを登録できます。AWS Control Tower コンソール AWS アカウント を使用して既存のを登録する詳細な手順については、「」を参照してください [AWS Control Tower コンソールから既存のアカウントを登録する](#)。

アカウント作成の舞台裏

1. たとえば、AWS Control Tower Account Factory ページから、コンソールから直接 AWS Service Catalog、または Service Catalog ProvisionProduct API を呼び出してリクエストを開始します。
2. AWS Service Catalog は AWS Control Tower を呼び出します。

3. AWS Control Tower はワークフローを開始し、最初のステップとして CreateAccount API を AWS Organizations 呼び出します。
4. がアカウント AWS Organizations を作成すると、AWS Control Tower はブループリントとコントロールを適用してプロビジョニングプロセスを完了します。
5. Service Catalog が引き続き AWS Control Tower をポーリングして、プロビジョニングプロセスが完了したことを確認します。
6. AWS Control Tower でのワークフローが完了すると、Service Catalog がアカウントの状態を確定し、結果をユーザー (リクエスト) に通知します。

既存のセキュリティアカウントまたはログアカウントを使用する際の考慮事項

をセキュリティ (デフォルト名: 監査) またはログ記録 (デフォルト名: ログアーカイブ) アカウント AWS アカウント として受け入れる前に、AWS Control Tower はアカウントで AWS Control Tower の要件と競合するリソースをチェックします。例えば、ロギングバケットの名前が AWS Control Tower が必要とする名前と同じである場合があります。また、AWS Control Tower は、アカウントがリソースをプロビジョニングできることを検証します。たとえば、AWS Security Token Service (AWS STS) が有効になっていること、アカウントが停止されていないこと、AWS Control Tower がアカウント内でリソースをプロビジョニングするアクセス許可を持っていることを確認します。

AWS Control Tower は、お客様が指定したログアカウントやセキュリティアカウント内の既存のリソースを削除しません。ただし、有効にすると、AWS Control Tower リージョン拒否コントロールにより、拒否されたリージョン内のリソースへのアクセスが禁止されます。

アカウントのセキュリティ

AWS Control Tower の管理アカウントおよびメンバーアカウントのセキュリティを保護するためのベストプラクティスに関するガイダンスについては、AWS Organizations ドキュメントを参照してください。

- [管理アカウントのベストプラクティス](#)
- [メンバーアカウントのベストプラクティス](#)

共有アカウントについて

AWS Control Tower には、管理アカウント、監査アカウント、ログアーカイブアカウントの 3 つの特別な AWS アカウント が関連付けられています。これらのアカウントは通常、共有アカウントと呼ばれ、場合によってはコアアカウントと呼ばれることもあります。

- ランディングゾーンのセットアップ時に、監査アカウントとログアーカイブアカウントの名前をカスタマイズすることを選択できます。アカウント名の変更については、「[AWS Control Tower の外部でのリソース名の変更](#)」を参照してください。
- 最初のランディングゾーンのセットアッププロセス中に、既存のを AWS Control Tower セキュリティまたはログ記録アカウント AWS アカウント として指定することもできます。このオプションを使用すると、AWS Control Tower で新しい共有アカウントを作成する必要がなくなります (これは 1 回限りの選択です)。

共有アカウントおよび関連リソースの詳細については、「[共有アカウントで作成されたリソース](#)」を参照してください。

管理アカウント

これにより、AWS Control Tower が AWS アカウント 起動します。デフォルトでは、このアカウントのルートユーザーおよびこのアカウントの IAM ユーザーまたは IAM 管理者ユーザーは、ランディングゾーン内のすべてのリソースへのフルアクセス権を持っています。

Note

ベストプラクティスとして、AWS Control Tower コンソール内で管理機能を実行するときには、このアカウントのルートユーザーまたは IAM 管理者ユーザーとしてサインインするのではなく、管理者権限を持つ IAM Identity Center ユーザーとしてサインインすることをお勧めします。

管理アカウントで利用できるロールとリソースの詳細については、「[共有アカウントで作成されたリソース](#)」を参照してください。

ログアーカイブアカウント

ログアーカイブ共有アカウントは、別の AWS アカウントを特に持ち込まない場合、ランディングゾーンの作成時に自動的に設定されます。

このアカウントには、ランディングゾーン内の他のすべてのアカウントのすべての AWS CloudTrail と AWS Config ログファイルのコピーを保存するための中央 Amazon S3 バケットが含まれています。ベストプラクティスとして、ログアーカイブアカウントへのアクセスを制限することをお勧めします。コンプライアンスと調査を担当し、それに関連するセキュリティツールまたは監査ツールを使用するチームに制限します。このアカウントは、自動セキュリティ監査、または Lambda 関数 AWS Config ルールなどのカスタムをホストして修復アクションを実行するために使用できます。

Amazon S3 バケットポリシー

AWS Control Tower ランディングゾーンバージョン 3.3 以降では、アカウントは監査バケットへの書き込みアクセス許可のために、aws:SourceOrgID 条件を満たす必要があります。この条件によってのみ、CloudTrail は組織内のアカウントに代わってお客様の S3 バケットへログを書き込めるようになり、組織外の CloudTrail ログによるお客様の AWS Control Tower S3 バケットへの書き込みを防ぎます。詳細については、「[AWS Control Tower ランディングゾーンバージョン 3.3](#)」を参照してください。

ログアーカイブアカウントで使用可能なロールとリソースの詳細については、「[ログアーカイブアカウントのリソース](#)」を参照してください。

Note

これらのログは変更できません。アカウントアクティビティに関連する監査とコンプライアンス調査の目的で、すべてのログが保存されます。

監査アカウント

特に別のアカウントを使用しない場合、この共有アカウントは、ランディングゾーンの作成時に自動的にセットアップされます。

監査アカウントは、セキュリティとコンプライアンスのチームに制限することをお勧めします。チームは、ランディングゾーン内のすべてのアカウントに対して監査人 (読み取り専用) と管理者 (フルアクセス) というアカウント横断的なロールを持ちます。このようなロールは、セキュリティとコンプライアンスのチームが次の目的で使用するためのものです。

- カスタム AWS Config ルールの Lambda 関数のホスティングなどの AWS メカニズムを使用して監査を実行します。

- 修復アクションなど、自動化されたセキュリティ操作を実行します。

また、監査アカウントは Amazon Simple Notification Service (Amazon SNS) サービスから通知を受け取ります。次の 3 つのカテゴリの通知を受け取ることができます。

- すべての設定イベント – このトピックでは、ランディングゾーン内のすべてのアカウントからのすべての CloudTrail と AWS Config 通知を集約します。
- セキュリティ通知の集約 — このトピックでは、特定の CloudWatch イベント、AWS Config ルール コンプライアンスステータス変更イベント、および GuardDuty 検出結果から受け取ったすべてのセキュリティ通知が集約されます。
- ドリフト通知 - このトピックでは、ランディングゾーン内のすべてのアカウント、ユーザー、OU、および SCP で検出されたすべてのドリフト警告が集約されます。ドリフトの詳細については、「[AWS Control Tower でドリフトを検出および解決する](#)」を参照してください。

メンバーアカウント内でトリガーされる監査通知では、ローカルの Amazon SNS トピックにアラートを送信することもできます。この機能により、アカウント管理者は個々のメンバーアカウントに固有の監査通知をサブスクライブできます。そのため、管理者は個々のアカウントに影響する問題を解決しながら、一元管理された監査アカウントにすべてのアカウント通知を集約できます。詳細については、「[Amazon Simple Notification Service デベロッパーガイド](#)」を参照してください。

監査アカウントで使えるロールとリソースの詳細については、「[アカウントリソースを監査する](#)」を参照してください。

プログラムによる監査の詳細については、「[Programmatic roles and trust relationships for the AWS Control Tower audit account](#)」を参照してください。

Important

監査アカウントに指定した E メールアドレス宛てに、AWS Control Tower でサポートされているすべての AWS リージョン から「AWS 通知 – サブスクリプションの確認」という件名の E メールが届きます。監査アカウントでコンプライアンス E メールを受信するには、AWS Control Tower で AWS リージョン サポートされている各 E メールから、各 E メール内のサブスクリプションの確認リンクを選択する必要があります。

共有アカウントで作成されたリソース

このセクションには、ランディングゾーンを設定するときに AWS Control Tower が共有アカウントに作成するリソースが表示されます。

メンバーアカウントリソースの詳細については、「[Account Factory のリソースに関する考慮事項](#)」を参照してください。

管理アカウントのリソース

ランディングゾーンを設定すると、管理アカウント内に次の AWS リソースが作成されます。

AWS のサービス	リソースタイプ	リソース名
AWS Organizations	アカウント	audit
		log archive
AWS Organizations	OU	Security
		Sandbox
AWS Organizations	サービスコントロールポリシー	aws-guardrails-*
AWS CloudFormation	スタック	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER
		AWSControlTowerBP-BASELINE-CONFIG-MASTER (バージョン 2.6 以降)
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL (3.0 以降にはデプロイされません)
		AWSControlTowerBP-BASELINE_SERVICE_L

AWS のサービス	リソースタイプ	リソース名
		INKED_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
		AWSControlTowerSecurityResources
		AWSControlTowerExecutionRole

AWS のサービス	リソースタイプ	リソース名
AWS Service Catalog	製品	AWS Control Tower Account Factory
AWS Config	アグリゲータ	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	追跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrail Logs
AWS Identity and Access Management	ロール	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	ポリシー	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWS のサービス	リソースタイプ	リソース名
AWS IAM アイデンティティセンター	ディレクトリグループ	AWSAccountFactory
		AWSAuditAccountAdmins
		AWSControlTowerAdmins
		AWSLogArchiveAdmins
		AWSLogArchiveViewers
		AWSSecurityAuditors
		AWSSecurityAuditPowerUsers
		AWSServiceCatalogAdmins
AWS IAM アイデンティティセンター	許可セット	AWSAdministratorAccess
		AWSPowerUserAccess
		AWSServiceCatalogAdminFullAccess
		AWSServiceCatalogEndUserAccess
		AWSReadOnlyAccess
		AWSOrganizationsFullAccess

 Note

CloudFormation StackSet BP_BASELINE_CLOUDTRAILは、ランディングゾーンバージョン 3.0 以降ではデプロイされません。ただし、ランディングゾーンを更新するまでは、ランディングゾーンの以前のバージョンに引き続き存在します。

ログアーカイブアカウントのリソース

ランディングゾーンを設定すると、ログアーカイブアカウント内に次の AWS リソースが作成されます。

AWS のサービス	リソースタイプ	リソース名
AWS CloudFormation	スタック	StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC- READ-PROHIBITED-
		StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC-WRI TE-PROHIBITED
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDWATCH-
		StackSet-AWSContro ITowerBP-BASELINE- CONFIG-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDTRAIL-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-ROLES-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-LINKED-ROLE-(In 3.2 and later)

AWS のサービス	リソースタイプ	リソース名
		StackSet-AWSContro ITowerBP-BASELINE-ROLES-
		StackSet-AWSContro ITowerLoggingResources-
AWS Config	AWS Config ルール	AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_READ_PROHIBITED AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	追跡	aws-controltower-BaselineCl oudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComp lianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	/aws/lambda/aws-controltowe r-NotificationForwarder

AWS のサービス	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	ポリシー	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	トピック	aws-controltower-SecurityNotifications
AWS Lambda	アプリケーション	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	関数	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	バケット	aws-controltower-logs- aws-controltower-s3-access-logs-

アカウントリソースを監査する

ランディングゾーンを設定すると、監査アカウント内に次の AWS リソースが作成されます。

AWS のサービス	リソースタイプ	リソース名
AWS CloudFormation	スタック	StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC- READ-PROHIBITED-
		StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC-WRI TE-PROHIBITED-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDWATCH-
		StackSet-AWSContro ITowerBP-BASELINE- CONFIG-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDTRAIL-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-ROLES-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-LINKED-ROLE-(In 3.2 and later)

AWS のサービス	リソースタイプ	リソース名
		StackSet-AWSControlTowerBP-SECURITY-TOPICS-
		StackSet-AWSControlTowerBP-BASELINE-ROLES-
		StackSet-AWSControlTowerSecurityResources-*
AWS Config	アグリゲータ	aws-controltower-GuardrailsComplianceAggregator
AWS Config	AWS Config ルール	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	追跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	/aws/lambda/aws-controltower-NotificationForwarder

AWS のサービス	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	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	ポリシー	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	トピック	aws-controltower-AggregateSecurityNotifications
		aws-controltower-AllConfigNotifications
		aws-controltower-SecurityNotifications
AWS Lambda	関数	aws-controltower-NotificationForwarder

メンバーアカウントについて

メンバーアカウントは、ユーザーが AWS ワークロードを実行するアカウントです。AWS Control Tower メンバーアカウントは、自動化された手法を含むさまざまな方法で作成およびカスタマイズできます。場合によっては、既存の を AWS Control Tower AWS アカウント に取り込むことができます。メンバーアカウントが作成、または登録されるとき、AWS Control Tower コンソールで作成された組織単位 (OU) または AWS Control Tower に登録された組織単位 (OU) に存在している必要があります。詳細については、次の関連トピックを参照してください。

- [プロビジョニング方法](#)
- [Account Factory でのアカウントのプロビジョニングと管理](#)
- [AWS Control Tower でのタスクの自動化](#)
- [自動登録でアカウントを移動して登録する](#)
- [AWS Control Tower Account Factory for Terraform \(AFT\) によるアカウントのプロビジョニング](#)
- 「AWS Organizations ユーザーガイド」の「[AWS Organizations の用語と概念](#)」。

アカウントとコントロール

メンバーアカウントは、AWS Control Tower で登録することも、未登録にしておくこともできます。登録済みのアカウントと未登録のアカウントには、それぞれ異なる方法でコントロールが適用されます。また、ネストされた OU のアカウントには、継承に基づいてコントロールが適用されることもあります。

AWS Control Tower が割り当てるメンバーアカウントリソースの詳細については、「[Account Factory のリソースに関する考慮事項](#)」を参照してください。

から AWS Control Tower アカウントを操作する AWS Service Catalog

このセクションでは、 の機能を使用して AWS Control Tower アカウントを処理する方法について説明します AWS Service Catalog。

トピック

- [Account Factory を使用して Service Catalog コンソールでアカウントをプロビジョニングする](#)

- [Service Catalog API による AWS Control Tower のアカウントプロビジョニングの自動化](#)
- [Service Catalog でプロビジョニング済み製品を更新する](#)
- [Service Catalog でアカウントの登録を解除する](#)

Account Factory を使用して Service Catalog コンソールでアカウントをプロビジョニングする

次の手順では、を使用して IAM アイデンティティセンターでユーザーとしてアカウントを作成してプロビジョニングする方法について説明します AWS Service Catalog。この手順は、アドバンストアカウントプロビジョニングまたはマニユアルアカウントプロビジョニングとも呼ばれます。必要に応じて、プログラム、AWS CLI、Service Catalog APIs、または AWS Control Tower Account Factory for Terraform (AFT) を使用して、AWS Control Tower アカウントをプロビジョニングできます。以前にカスタムブループリントを設定したことがある場合は、カスタマイズされたアカウントをコンソールでプロビジョニングできる場合があります。カスタマイズの詳細については、「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。

Account Factory でユーザーとしてアカウントをプロビジョニングするには

1. ユーザーポータル URL からサインインします。
2. [Your applications] (お申込み内容) から、[AWS Account] (アカウント) を選択します。
3. アカウントのリストで、管理アカウントのアカウント ID を選択します。この ID には、[(Management)] ((管理)) などのラベルが付いている場合もあります。
4. [AWSServiceCatalogEndUserAccess] から [Management console] (マネジメントコンソール) を選択します。これにより、このアカウントの AWS マネジメントコンソール このユーザーの が開きます。
5. アカウントのプロビジョニング AWS リージョン に正しい を選択していることを確認します。これは AWS Control Tower リージョンである必要があります。
6. [Service Catalog] を検索して選択し、Service Catalog コンソールを開きます。
7. ナビゲーションペインで、[Products] (製品) を選択します。
8. [AWS Control Tower Account Factory] を選択してから、[Launch product] (製品の起動) ボタンを選択します。この選択により、新しいアカウントをプロビジョニングするウィザードが開始されます。
9. 情報を入力し、以下の点に注意してください。

- [SSOUserEmail] は新しい E メールアドレスか既存の IAM Identity Center ユーザーに関連付けられた E メールアドレスのいずれかです。どちらを選択しても、このユーザーにはプロビジョニングするアカウントへの管理者アクセスが許可されます。
 - [AccountEmail] は、AWS アカウントにまだ関連付けられていない E メールアドレスでなければなりません。[SSOUserEmail] で新しい E メールアドレスを使用する場合は、ここでもそのアドレスを使用できます。
10. [TagOptions] を定義しないでください。また、[Notifications] (通知) を有効にしないでください。これらの操作を行うと、アカウントのプロビジョニングに失敗する可能性があります。完了したら、[Launch product] (製品の起動) を選択します。
 11. アカウント設定を確認し、[Launch] (起動) を選択します。アカウントのプロビジョニングに失敗するため、リソースプランを作成しないでください。
 12. これで、アカウントのプロビジョニングが開始されます。この処理には数分かかることがあります。ページをリフレッシュして、表示されたステータス情報を更新できます。

 Note

一度にプロビジョニングできるアカウントは最大 5 個です。

Service Catalog API による AWS Control Tower のアカウントプロビジョニングの自動化

AWS Control Tower は、など、他のいくつかの AWS サービスと統合されています AWS Service Catalog。APIs を使用して、AWS Control Tower でメンバーアカウントを作成およびプロビジョニングしたり、既存のメンバーアカウントを登録したりできます。

 Note

ランディングゾーン設定で IAM Identity Center をオプトアウトした場合、AWS Service Catalog APIs またはコンソールを使用したアカウントプロビジョニング中に指定した値は使用されません。

この動画では、AWS Service Catalog を呼び出すことによって、自動化されたバッチ方式でアカウントをプロビジョニングする方法について説明します。プロビジョニングでは、AWS コマンドラインインターフェイス (CLI) から [ProvisionProduct](#) API を呼び出し、セットアップする各アカ

ウントのパラメータを含む JSON ファイルを指定します。この動画では、[AWS Cloud9](#) 開発環境をインストールして使用し、この作業を実行する方法を説明します。AWS Cloud9 の代わりに AWS Cloudshell を使用する場合、CLI コマンドは同じになります。

 Note

また、各アカウントの の [UpdateProvisionedProduct](#) API を呼び出すことで、アカウントの更新を自動化 AWS Service Catalog するためにこのアプローチを適応させることもできます。アカウントを更新するスクリプトを 1 つずつ作成できます。

Terraform を使い慣れている場合は、まったく異なるオートメーションの方法として、[provision accounts with AWS Control Tower Account Factory for Terraform \(AFT\)](#) (AWS Control Tower Account Factory for Terraform (AFT) でアカウントをプロビジョニングする) ことができます。

オートメーションの管理ロールのサンプル

次に示すのは、管理アカウントでオートメーションの管理ロールを設定するために使用できるサンプルテンプレートです。このロールは、ターゲットアカウントの管理者アクセスを使用してオートメーションを実行できるように、管理アカウントで設定します。

```
AWS::Template::FormatVersion: 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"
```

オートメーションの実行ロールのサンプル

次に示すのは、オートメーションの実行ロールを設定するために使用できるサンプルテンプレートです。このロールは、ターゲットアカウントで設定します。

```
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"

```

これらのロールを設定したら、AWS Service Catalog APIsを呼び出して自動タスクを実行します。CLI コマンドは、動画で説明されています。

Service Catalog API のプロビジョニング入力のサンプル

API を使用して新しい AWS Control Tower アカウントをプロビジョニングしたり、既存のメンバーアカウントを登録ProvisionProductしたりする場合に、Service Catalog API に渡すことができる入力の例を次に示します。

Note

ProvisionProduct API を使用して既存のメンバーアカウントを登録するには、API `AWSControlTowerExecution` を呼び出す前に IAM ロールがターゲットアカウントに存在する必要があります。新しいアカウントプロビジョニングと既存のアカウント登録の両方に、次の例に示す同じ入力パラメータを使用できます。

```

{
  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"
}
```

詳細については、「[API reference for Service Catalog](#)」 (Service Catalog の API リファレンス) を参照してください。

Note

ManagedOrganizationalUnit の値の入力文字列の形式が OU_NAME から OU_NAME (OU_ID) に変更されていることに注意してください。続く動画では、この変更については言及していません。

動画チュートリアル

この動画 (6:58) では、AWS Control Tower のアカウントのデプロイを自動化する方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower での自動アカウントプロビジョニングに関する動画チュートリアル。](#)

Service Catalog でプロビジョニング済み製品を更新する

次の手順では、Service Catalog を使用して、アカウントのプロビジョニング済み製品を更新することにより、Account Factory のアカウントを更新したり、新しい OU に移動したりする方法を示します。

Note

ランディングゾーン設定で IAM Identity Center をオプトアウトした場合、AWS Service Catalog APIs またはコンソールを使用したアカウントプロビジョニング中に指定した値は使用されません。

Account Factory アカウントを更新したり、Service Catalog からその OU を変更したりするには

1. AWS マネジメントコンソールにサインインし、<https://console.aws.amazon.com/servicecatalog/> で AWS Service Catalog コンソールを開きます。

Note

Service Catalog で新しい製品をプロビジョニングする許可を持つユーザーとしてサインインする必要があります (例えば、AWSAccountFactory グループまたは AWSServiceCatalogAdmins グループの IAM Identity Center ユーザー)。

2. ナビゲーションペインで [Provisioning] (プロビジョニング) を選択し、次に [Provisioned products] (プロビジョニング済み製品) を選択します。
3. 一覧表示されているメンバーアカウントごとに以下のステップを実行して、すべてのメンバーアカウントを更新します。
 - a. メンバーアカウントを選択します。そのアカウントの [Provisioned product details] (プロビジョニングされた製品の詳細) ページが表示されます。
 - b. [Provisioned product details] (プロビジョニングされた製品の詳細) ページで、[Events] (イベント) タブを選択します。
 - c. 以下のパラメータを書き留めます。
 - [SSOUserEmail] (プロビジョニングされた製品の詳細で利用可能)
 - [AccountEmail] (プロビジョニングされた製品の詳細で利用可能)
 - SSOUserFirstName(IAM Identity Center で利用可能)

- SSOUSerLastName(IAM Identity Center で利用可能)
 - AccountName(IAM Identity Center で利用可能)
- d. [Actions] (アクション) で、[Update] (更新) を選択します。
- e. 更新する製品の [Version] (バージョン) の横にあるボタンを選択して、[Next] (次へ) を選択します。
- f. 前に説明したパラメータ値を入力します。
- 既存の OU を保持する場合は、[ManagedOrganizationalUnit] で、アカウントが既に存在している OU を選択します。
 - アカウントを新しい OU に移行する場合は、[ManagedOrganizationalUnit] で、そのアカウントの新しい OU を選択します。

中央のクラウド管理者は、この情報を AWS Control Tower コンソールの [Organization] (組織) ページで見つけることができます。

- g. [次へ] を選択します。
- h. 変更内容を確認し、[Update] (更新) を選択します。このプロセスには、アカウントごとに数分かかることがあります。

Service Catalog でアカウントの登録を解除する

アカウントの登録解除は、Service Catalog コンソールで AWSAccountFactory グループの IAM アイデンティティセンターユーザーがプロビジョニング済み製品を終了する方法で行えます。IAM Identity Center ユーザーまたはグループの詳細については、[「ユーザーとアクセスの管理 AWS IAM アイデンティティセンター」](#)を参照してください。Service Catalog でメンバーアカウントを登録解除する手順を以下に説明します。

Service Catalog を使用して登録済みアカウントの登録を解除するには

1. ウェブブラウザで Service Catalog コンソール (<https://console.aws.amazon.com/servicecatalog>) を開きます。
2. 左のナビゲーションペインで [Provisioned products list] (プロビジョニング済み製品リスト) を選択します。
3. プロビジョニングされるアカウントのリストから、今後 AWS Control Tower による管理を希望しないアカウントの名前を選択します。

4. [Provisioned product details] (プロビジョニングされた製品の詳細) ページの [Actions] (アクション) メニューから、[Terminate] (終了) を選択します。
5. 表示されるダイアログボックスで [Terminate] (終了) を選択します。

 Important

terminate (終了) という単語は Service Catalog に固有のものです。Service Catalog Account Factory でアカウントを終了しても、アカウントは解約されません。このアクションにより、アカウントの OU およびランディングゾーンからアカウントが削除されます。

6. アカウントが登録解除されると、ステータスが [未登録] に変わります。
7. このアカウントが不要になった場合は、解約します。AWS アカウントの閉鎖の詳細については、「[AWS Billing ユーザーガイド](#)」の「[アカウントの閉鎖](#)」を参照してください。

 Note

アカウントのステータスが [未登録] と表示されるまで待ちます。

AWS Control Tower でのアカウントのプロビジョニングと管理

この章では以下について説明します。

- AWS Control Tower で新しいメンバーアカウントをプロビジョニングおよび管理するための概要と手順。
- 既存の AWS アカウントを AWS Control Tower に登録するための概要と手順。

AWS Control Tower のアカウントの一般情報については、「[AWS Control Tower AWS アカウントのについて](#)」を参照してください。AWS Control Tower で複数のアカウントを登録する方法については、「[AWS Control Tower への既存の組織単位の登録](#)」を参照してください。

Note

単一アカウントのプロビジョニング、更新、カスタマイズは、AWSControlTowerBaseline を有効にした組織単位 (OU) をターゲットにする必要があります。OU で AWSControlTowerBaseline が有効になっていない場合は、アカウントの自動登録を有効にするか、EnabledBaseline で ResetEnabledBaseline API と ResetEnabledControl APIs を使用してアカウント EnabledControls を登録できます。EnabledBaselines AWSControlTowerBaseline の詳細については、「」を参照してください [OU レベルで適用されるベースラインタイプ](#)。

Note

プロビジョニング、更新、登録など、最大 5 つのアカウント関連のオペレーションを同時に実行できます。

アカウントのプロビジョニングに必要なアクセス許可

適切なユーザーグループの許可があれば、組織内のすべてのアカウントに対して標準化されたベースラインとネットワーク設定を指定できます。

Account Factory を使用して AWS Control Tower コンソールからアカウントを作成する場合は、AWS Control Tower コンソールを使用するアクセス許可と共に、AWSServiceCatalogEndUserFullAccess ポリシーが有効になっている IAM ユーザーとしてアカウントにサインインする必要があります。ルートユーザーとしてサインインすることはできません。

Note

アカウントをプロビジョニングする場合、アカウントのリクエストには必ず CreateAccount および DescribeCreateAccountStatus アクセス許可が必要です。このアクセス許可セットは Admin ロールの一部であり、リクエストが Admin ロールを受けると自動的に付与されます。アカウントをプロビジョニングするアクセス許可を委任する場合、これらのアクセス許可をアカウントリクエストに直接追加する必要がある場合があります。

AWS Control Tower で必要な許可の全般的な情報については、「[AWS Control Tower でアイデンティティベースのポリシー \(IAM ポリシー\) を使用する](#)」を参照してください。AWS Control Tower のロールとアカウントについては、「[Roles and accounts](#)」を参照してください。

AWS Control Tower 内のアカウントのプロビジョニング

AWS Control Tower には、メンバーアカウントを作成および更新するための方法が複数用意されています。一部の方法は主にコンソールベースで、一部の方法は主に自動化されています。

概要:

AWS Control Tower のメンバーアカウントを作成する標準的な方法の 1 つは、Account Factory を使用することです。Account Factory は、Service Catalog に含まれるコンソールベースの製品です。ランディングゾーンがドリフト状態でない場合は、AWS Control Tower コンソールから、[アカウントを作成] をメソッドとして使用して新しいアカウントをプロビジョニングしたり、[アカウントの登録] を使用して既存の AWS アカウントを AWS Control Tower に登録したりできます。

Account Factory を使用すると、AWS Control Tower のデフォルト設定に基づいてベーシックアカウントをプロビジョニングできます。また、特殊なユースケースの要件を満たすカスタマイズされたアカウントをプロビジョニングすることもできます。

[Account Factory Customization \(AFC\)](#) は、カスタマイズされたアカウントを AWS Control Tower コンソールからプロビジョニングする手段を提供し、アカウントのカスタマイズとデプロイを自動化し

ます。1 回限りのセットアップのためのいくつかのステップを実行すると、コンソールベースの自動プロビジョニングを使用できるようになり、スクリプトの作成やパイプラインの設定は不要となります。詳細については、「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。

自動登録

ランディングゾーン設定の自動アカウント登録機能にオプトインすると、継承ドリフトを作成せずに、AWS Control Tower AWS アカウント の外部で作成し、AWS Control Tower に登録されている OU に移動することもできます。詳細については、「[自動登録でアカウントを移動して登録する](#)」を参照してください。

コンソールベースの方法:

- 基本アカウントまたはカスタマイズされたアカウントについては AWS Service Catalog、の一部である Account Factory コンソールを使用します。詳細と手順については、「[Account Factory でアカウントのプロビジョニングと管理](#)」を参照してください。
- 自動登録を通じて、コンソールから OU にアカウントを移動します。「[自動登録でアカウントを移動して登録する](#)」を参照してください。
- AWS Control Tower 内の [Enroll account] (アカウントの登録) 機能を使用します (ランディングゾーンがドリフト状態でない場合)。「[AWS Control Tower コンソールから既存のアカウントを登録する](#)」を参照してください。
- AWS Control Tower コンソールでは、Account Factory を使用して、同時に最大 5 つのアカウントを作成、更新、または登録できます。

自動化された方法:

- Lambda コード: AWS Control Tower ランディングゾーンの管理アカウントから、Lambda コードと適切な IAM ロールを使用します。「[Automated Account Provisioning with IAM Roles](#)」を参照してください。
- Terraform: AWS Control Tower Account Factory for Terraform (AFT) から、Account Factory と GitOps モデルを利用して、アカウントのプロビジョニングと更新のオートメーションが可能です。「[AWS Control Tower Account Factory for Terraform \(AFT\) によるアカウントのプロビジョニング](#)」を参照してください。

- 自動登録を通じ、API を使用して OU に既存のアカウントを移動します。「[自動登録でアカウントを移動して登録する](#)」を参照してください。
- AWS Control Tower コンソールの Account Factory Customization: セットアップのステップの実行後は、カスタマイズされたアカウントの今後のプロビジョニングで、設定を追加したり、パイプラインを維持したりする必要はありません。アカウントは、ブループリントと呼ばれる AWS Service Catalog 製品によってプロビジョニングされます。ブループリントでは、CloudFormation テンプレートまたは Terraform テンプレートを使用できます。

Note

CloudFormation ブループリントは、リソースを複数のリージョンにデプロイできます。Terraform ブループリントでは、1 つのリージョンにのみリソースをデプロイできます。デフォルトでは、それはホームリージョンです。

AWS Control Tower コンソールでのアカウントのプロビジョニング

次の手順では、AWS Control Tower コンソールを使用して、アカウントを IAM Identity Center のユーザーとして作成およびプロビジョニングする方法について説明します。この手順は、マニユアルアカウントプロビジョニングとも呼ばれます。必要に応じて、プログラム、CLI、Service Catalog APIs、または AWS Control Tower Account Factory for Terraform (AFT)AWSを使用して AWS Control Tower アカウントをプロビジョニングしたり、既存のアカウントを登録済みの OU に自動的に登録したりできます。以前にカスタムブループリントを設定したことがある場合は、カスタマイズされたアカウントをコンソールでプロビジョニングできる場合があります。カスタマイズの詳細については、「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。

ユーザーとして AWS Control Tower コンソールでアカウントを個別にプロビジョニングするには

1. にサインインAWSし、AWS Control Tower コンソールに移動します。
2. 左のナビゲーションから、[組織] を選択して [組織] ページを表示します。
3. 右上の [リソースを作成] を選択します。
4. ドロップダウンメニューで、[アカウントを作成] を選択します。
5. そのページで情報を入力し、次の点に注意してください。

- [アカウント E メール] は、AWS アカウントにまだ関連付けられていない E メールアドレスでなければなりません。
 - 表示名は、このアカウントに表示する名前です。
6. IAM Identity Center の E メールアドレスとユーザー名を使用して、[アクセス設定] を定義するフィールドに入力します。
 7. ドロップダウンリストから登録済み OU を選択して、アカウントをプロビジョニングする OU を指定します。
 8. 必要に応じて、定義済みのブループリントを使用して、カスタマイズされたリソースでアカウントをプロビジョニングします。このタスクは後で実行できます。
 9. アカウントの選択を確認し、右下の [アカウントを作成] を選択します。
 10. これで、アカウントのプロビジョニングが開始されます。この処理には数分かかることがあります。ページをリフレッシュして、表示されたステータス情報を更新できます。

Note

一度にプロビジョニングできるアカウントは最大 5 個です。

アカウントの表示

[Organization] (組織) ページには、AWS Control Tower での OU や登録のステータスに関係なく、組織内のすべての OU とアカウントが一覧表示されます。各アカウントが登録の前提条件を満たしていれば、AWS Control Tower でメンバーアカウントを個別または OU グループ別に表示および登録できます。

特定のアカウントを表示するには

- [Organization] (組織) ページに移動します。
- 右上のドロップダウンメニューから [アカウントのみ] を選択できます。
- 次に、テーブルからアカウントの名前を選択します。
- テーブルから親 OU の名前を選択して、その OU の [詳細] ページで、その OU 内のすべてのアカウントのリストを表示することもできます。

[組織] ページと [アカウントの詳細] ページで、アカウントの [状態] を表示できます。これは、次のいずれかです。

- [Not enrolled] (未登録) - アカウントは親 OU のメンバーですが、AWS Control Tower によって完全には管理されていません。親 OU が登録されている場合、アカウントはその登録済みの親 OU に設定された予防コントロールによって管理されますが、OU の検出コントロールはこのアカウントに適用されません。親 OU が未登録の場合は、どのコントロールもこのアカウントに適用されません。
- Enrolling (登録中) - アカウントは、AWS Control Tower の管理対象になっています。親 OU のコントロール設定に適合するようにアカウントが調整されます。このプロセスには、アカウントリソースごとに数分かかる場合があります。
- [Enrolled] (登録済み) - アカウントは、その親 OU 用に設定されたコントロールによって管理されています。AWS Control Tower によって完全に管理されています。
- Enrollment failed (登録に失敗しました) - アカウントを AWS Control Tower に登録できませんでした。詳細については、「[登録の失敗の一般的な原因](#)」を参照してください。
- Update available (更新が利用可能) - アカウントには利用可能な更新があります。この状態のアカウントは登録済みですが、環境に加えられた最近の変更を反映するには、アカウントを更新する必要があります。単一のアカウントを更新するには、アカウントの詳細ページに移動し、[Update account] (アカウントの更新) を選択します。

1 つの OU の下にこの状態のアカウントが複数ある場合は、OU を再登録することを選択し、これらのアカウントをまとめて更新できます。

既存のアカウントの登録について

AWS Control Tower ガバナンスは、AWS Control Tower によって既に管理されている組織単位 (OU) に登録 AWS アカウント するときに、既存の個人に拡張できます。対象アカウントは、AWS Control Tower OUs と同じ AWS Organizations 組織に属する未登録の OU に存在します。

AWS Control Tower にアカウントを登録するには、さまざまな方法があります。このページの情報は、すべての登録方法に適用されます。

Note

ランディングゾーンの初期セットアップ時を除き AWS、監査またはログアーカイブアカウントとして機能する既存のアカウントを登録することはできません。

アカウント登録中の処理

登録プロセス中に、AWS Control Tower は以下のアクションを実行します。

- アカウントのベースラインを作成します。これには、以下のスタックセットのデプロイが含まれます。
 - 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

これらのスタックセットのテンプレートで既存のポリシーとの競合がないことを確認することをお勧めします。

- AWS IAM アイデンティティセンター または を通じてアカウントを識別します AWS Organizations。
- 指定した OU にアカウントを配置します。現在の OU に適用されているすべての SCP を適用して、セキュリティ体制の整合性を保ってください。
- 選択した OU 全体に適用される SCP を使用して、必須のコントロールをアカウントに適用します。
- アカウント内のすべてのリソースを記録するように有効に AWS Config して設定します。
- AWS Control Tower の検出コントロールをアカウントに適用する AWS Config ルールを追加します。

アカウントと組織レベルの CloudTrail 証跡

ランディングゾーンバージョン 3.1 以降で、ランディングゾーン設定でオプションの AWS CloudTrail 統合を選択した場合:

- OU 内のすべてのメンバーアカウントは、登録されているかどうかにかかわらず、OU の AWS CloudTrail 証跡によって管理されます。
- AWS Control Tower にアカウントを登録すると、そのアカウントは新しい組織の AWS CloudTrail 追跡によって管理されます。CloudTrail 追跡の既存のデプロイがある場

合、AWS Control Tower にアカウントを登録する前にアカウントの既存の追跡を削除しない限り、料金が重複して発生する可能性があります。

- AWS Organizations コンソールや APIs などを使用してアカウントを登録済みの OU に移動する場合は、アカウントの残りのアカウントレベルの証跡を削除できます。CloudTrail 証跡の既存のデプロイがある場合は、CloudTrail の料金が重複して発生します。

ランディングゾーンを更新して組織レベルの証跡をオプトアウトすることを選択した場合、またはランディングゾーンがバージョン 3.0 より古い場合、組織レベルの CloudTrail 証跡はアカウントには適用されません。

VPC を使用して既存のアカウントを登録する

AWS Control Tower は、Account Factory で新しいアカウントをプロビジョニングするときに、既存のアカウントを登録するときとは異なる方法で VPC を処理します。

- 新しいアカウントを作成すると、AWS Control Tower は自動的に AWS のデフォルト VPC を削除し、そのアカウントの新しい VPC を作成します。
- 既存のアカウントを登録する場合、AWS Control Tower はそのアカウントの新しい VPC を作成しません。
- 既存のアカウントを登録しても、AWS Control Tower はアカウントに関連付けられた既存の VPC または AWS デフォルト VPC を削除しません。

Tip

Account Factory を設定して新規アカウントに対するデフォルトの動作を変更でき、AWS Control Tower の組織内のアカウントに対して VPC がデフォルトで設定されないようにできます。詳細については、「[AWS Control Tower で VPC なしのアカウントを作成する](#)」を参照してください。

AWS Config リソースでアカウントを登録する

登録するアカウントには、既存の AWS Config リソースがあってはなりません。「[既存の AWS Config リソースがあるアカウントの登録](#)」を参照してください。

以下は AWS Config 、設定レコーダーや配信チャネルなど、既存のアカウント AWS Config リソースのステータスを判断するために使用できる CLI コマンドの例です。

表示コマンド:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

通常の応答は "name": "default" のようになります。

削除コマンド:

- `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`

登録の前提条件

このセクションでは、ランディングゾーン設定ページでオプションの自動登録機能を選択していない場合、または 3.1 より前のランディングゾーンバージョンで動作している場合に、既存の AWS アカウントを AWS Control Tower に登録する方法について説明します。

AWS Control Tower AWS アカウント に既存の を登録する前に、次の前提条件が必要です。

Note

ランディングゾーンの [設定] ページで AWS Control Tower 自動登録機能をアクティブ化した場合、または登録 OU プロセスの一部としてアカウントを登録する場合は、AWSControlTowerExecution ロールを追加する前提条件は必要ありません。ただし、いずれの場合も、登録するアカウントには既存の AWS Config リソースがない可能性があります。[「既存の AWS Config リソースがあるアカウントの登録」](#)を参照してください。

1. 既存のを登録するには AWS アカウント、AWSControlTowerExecutionロールが登録するアカウントに存在する必要があります。詳細と手順については、「[アカウントを登録する](#)」で参照できます。
2. AWSControlTowerExecution ロールに加えて、登録する既存の AWS アカウント には、以下のアクセス許可と信頼関係が必要です。それ以外の場合、登録は失敗します。

ロールのアクセス許可: AdministratorAccess (AWS 管理ポリシー)

ロールの信頼関係:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. アカウントには AWS Config 設定レコーダーまたは配信チャネルを持たないことをお勧めします。アカウントを登録する前に、AWS CLI を使用してこれらを削除または変更できます。それ以外の場合は、[既存の AWS Config リソースを変更する方法については、既存のリソースがあるアカウントの登録](#)を参照してください。
4. 登録するアカウントは、AWS Control Tower 管理アカウントと同じ AWS Organizations 組織に存在する必要があります。既存のアカウントは、AWS Control Tower 管理アカウントと同じ組織にのみ、AWS Control Tower に既に登録されている OU で登録できます。

登録に関するその他の前提条件を確認するには、「[AWS Control Tower の開始方法](#)」を参照してください。

Note

AWS Control Tower にアカウントを登録すると、そのアカウントは AWS Control Tower 組織の AWS CloudTrail 追跡によって管理されます。CloudTrail 追跡の既存のデプロイがある場

合、AWS Control Tower にアカウントを登録する前にアカウントの既存の追跡を削除しない限り、料金が重複して発生する可能性があります。

AWSControlTowerExecution ロールでの信頼されるアクセスについて

既存の AWS アカウント を AWS Control Tower に登録する前に、AWS Control Tower がアカウントを管理または管理するアクセス許可を付与する必要があります。具体的に CloudFormation は、AWS Control Tower には、 が選択した組織のアカウントにスタックを自動的にデプロイできるように、AWS Organizations ユーザーに代わって AWS CloudFormation と の間に信頼されたアクセスを確立するためのアクセス許可が必要です。この信頼されたアクセスでは、AWSControlTowerExecution ロールは、各アカウントを管理するために必要なアクティビティを実行します。そのため、登録する前にこのロールを各アカウントに追加する必要があります。

信頼されたアクセスが有効になっている場合、 は 1 回のオペレーション AWS リージョン で複数のアカウントおよび のスタックを作成、更新、または削除 CloudFormation できます。AWS Control Tower はこの信頼機能を使用して既存のアカウントにロールとアクセス許可を適用します。その後、それらを登録済み組織単位に移動して、管理下に置くことができます。

信頼されたアクセスと の詳細については AWS CloudFormation StackSets、 「」 および [AWS CloudFormationStackSetsAWS Organizations](#) 「」を参照してください。

自動登録でアカウントを移動して登録する

アカウントの自動登録機能は、バージョン 3.1 以降のランディングゾーンで利用可能です。

オプションでこの機能を有効にする場合は、AWS Organizations APIs とコンソールを使用して、[継承ドリフト](#)を作成せずにアカウントを AWS Control Tower に移動できます。アカウントは、AWS Control Tower の送信先の組織単位 (OU) からベースラインリソースとコントロール設定を自動的に受け取ります。このオプション機能を使用すると、2 つの OU が同じベースライン設定を持ち、同じコントロールが有効になっている場合、継承ドリフトを作成せずに、AWS Control Tower 内の OU 間でアカウントを移動することもできます。

自動登録を有効にするには: AWS Control Tower コンソールのランディングゾーンの [設定] ページでアカウントの自動登録を選択するか、RemediationType パラメータの値を継承ドリフトに設定して AWS Control Tower CreateLandingZone または UpdateLandingZone API を呼び出します。

自動登録を適用するには: 設定ページでこのオプションを選択したら、AWS Organizations コンソール、API、AWS Organizations MoveAccountまたは AWS Control Tower コンソールを使用してアカウントを移動できます。

自動登録を使用してアカウントの登録を解除するには: 登録されている OU の外部にアカウントを移動すると、AWS Control Tower はデプロイされたすべてのベースラインとコントロールを自動的に削除します。

Note

AWS Control Tower のソースと送信元 OU の設定が異なる場合、アカウントで [移動されたメンバーアカウント](#) ドリフトが表示されることがあります。

前提条件: 自動登録用に設定する

- AWS Control Tower ランディングゾーンバージョン 3.1 以降を実行している必要があります。
- コンソールのランディングゾーンの [設定] ページ、または RemediationTypes パラメータの値を Inheritance Drift に設定して AWS Control Tower ランディングゾーン API を使用して、AWS Control Tower 自動登録機能にオプトインします。オプトインすると、AWS Control Tower はユーザーに代わっての move account イベントに対応し AWS Organizations、移動したアカウントの継承ドリフトを直ちに修正します。

必要なアクセス許可

CreateAccount API と MoveAccount API を使用するには AWS Organizations、特定のロールとアクセス許可が必要です。AWS Control Tower AWS Organizations で 使用方法の詳細については、[「AWS Control Tower と AWS Organizations」](#)を参照してください。

API の使用状況に関する例

これらの API に関する詳細と例については、「AWS Organizations API リファレンス」の[「CreateAccount」](#)と[「MoveAccount」](#)を参照してください。

考慮事項

- 登録タイムライン: AWS Control Tower に登録されている OU に移動したアカウントは、結果整合性モデルで登録されます。このプロセスは通常、移動するアカウントの数に応じて数分、最大数時間かかります。
- 登録解除プロセス: AWS Control Tower の外部の OU に移動することで、同じプロセスを使用して AWS Control Tower からアカウントの登録を解除できます。このプロセスでは、AWS Control

Tower によってデプロイされたロールとリソース、および AWS Control Tower で有効になっているコントロールがすべて削除されます。

AWS Control Tower コンソールから既存のアカウントを登録する

個人を AWS Control Tower に登録 AWS アカウント するには、2 つの一般的な方法があります。

1. 設定ページで自動登録機能を選択したら、AWS Control Tower の AWS アカウント 外部で を作成し、登録済みの OU に直接移動できます。詳細については、「[自動的にアカウントを移動し、登録する](#)」を参照してください。このオプションは、ランディングゾーンバージョン 3.1 以降でのみ有効です。
2. AWS Control Tower コンソールから既存のアカウントを手動で登録できます。

以下のセクションでは、2 つ目のオプションについて説明します。これは、AWS Control Tower 環境の以前の設定を必要としません。は、必要な[前提条件](#)を満たす AWS アカウント 必要があります。

コンソールで対象となるアカウントを表示します。

1. AWS Control Tower の [Organization] (組織) ページに移動します。
2. 登録するアカウントの名前を見つけます。見つけるには、アカウント名は、右上にあるドロップダウンメニューから [Accounts only] (アカウントのみ) を選択し、フィルターされたテーブルで探してください。

次に、[アカウントを手動で登録する手順](#) セクションで示されているように、個々のアカウントを登録する手順に従います。

コンソールからの登録に関する考慮事項

- AWS Control Tower コンソールで利用できるアカウント登録機能は、AWS Control Tower によって管理 AWS アカウント されるように既存の を登録することを目的としています。詳細については、「[既存の AWS アカウントの登録](#)」を参照してください。
- コンソールベースの [アカウントの登録] 機能は、ランディングゾーンが[ドリフト](#)状態でないときに使用できます。ランディングゾーンがドリフト状態にある場合は、[Enroll account] (アカウントの登録) 機能を正常に使用できないことがあります。ランディングゾーンのドリフトが解決されるまで、Account Factory または他の方法を使用して新しいアカウントをプロビジョニングする必要があります。

- AWS Control Tower コンソールからアカウントを登録する場合は、AWS Control Tower コンソールを使用する管理者権限と共に、AWSServiceCatalogEndUserFullAccess ポリシーが有効になっているユーザーでアカウントにサインインする必要があり、ルートユーザーとしてサインインすることはできません。
- 登録するアカウントは、他のアカウントを更新する場合と同様に、および AWS Control Tower Account Factory を使用して更新できます。更新手順については、「[AWS Control Tower でアカウントを更新して移動する](#)」セクションを参照してください。

Note

既存の E メールアドレスを登録するときは AWS アカウント、必ず既存の E メールアドレスを確認してください。それ以外の場合は、新しいアカウントが作成されます。

アカウントを手動で登録する手順

既存の AWS アカウント アカウントで AdministratorAccess アクセス許可 (ポリシー) を設定したら、次のステップに従ってアカウントを登録します。

コンソールから AWS Control Tower に個別のアカウントを登録するには

- AWS Control Tower の [Organization] (組織) ページに移動します。
- [Organization] (組織) ページで、登録できるアカウントでは、セクション上部の [Actions] ドロップダウンメニューから [Enroll] を選択できます。これらのアカウントには、[Account details] (アカウントの詳細) ページでも [Enroll account] (アカウントの登録) ボタンが表示されます。
- [Enroll account] (アカウントの登録) を選択した場合、[Enroll account] (アカウントの登録) ページが表示され、AWSControlTowerExecution ロールをアカウントに追加するよう促されます。手順については、「[必要な IAM ロールを既存の に手動で追加 AWS アカウント して登録する](#)」を参照してください。
- 次に、ドロップダウンの一覧から登録された OU を選択します。アカウントが既に登録済みの OU にある場合、このリストには OU が表示されます。
- [[Enroll account (アカウントの登録)]] を選択します。
- AWSControlTowerExecution ロールを追加するためのモーダルリマインダーが表示されるので、アクションを確認します。
- [Enroll] (登録する) を選択します。

- AWS Control Tower は登録プロセスを開始し、[Account details] (アカウントの詳細) ページに戻ります。

登録の失敗の一般的な原因

- 既存のアカウントを登録するには、登録するアカウントに `AWSControlTowerExecution` ロールが存在する必要があります。
- IAM プリンシパルに、アカウントをプロビジョニングするアクセス許可がない可能性があります。
- AWS Security Token Service (AWS STS) は、ホームリージョンの AWS アカウント、または AWS Control Tower でサポートされている任意のリージョンで無効になっています。
- AWS Service Catalog の Account Factory ポートフォリオに追加する必要があるアカウントにサインインしている場合があります。アカウントを AWS Control Tower で作成または登録できるように、Account Factory にアクセスする前に、アカウントを追加する必要があります。適切なユーザーまたはロールが Account Factory ポートフォリオに追加されていない場合、アカウントを追加しようとするとエラーが発生します。AWS Service Catalog ポートフォリオへのアクセスを許可する方法については、[「ユーザーへのアクセスを許可する」](#)を参照してください。
- root としてサインインしている可能性があります。
- 登録しようとしているアカウントには、残っている AWS Config 設定がある可能性があります。特に、アカウントに設定レコーダーや配信チャネルを持たないようにできます。これらは、アカウントを登録する AWS CLI 前に、[「既存の AWS Config リソースがあるアカウントを登録する」](#) および [「AWS Control Towerを通じて操作するAWS CloudShell」](#)を参照してください。
- アカウントが別の AWS Control Tower OU を含む管理アカウントを持つ別の OU に属している場合、別の OU に参加する前に、現在の OU のアカウントを終了する必要があります。元の OU で既存のリソースを削除する必要があります。それ以外の場合、登録は失敗します。
- 目的の OU の SCP で、そのアカウントに必要なすべてのリソースの作成が許可されていない場合、アカウントのプロビジョニングと登録は失敗します。例えば、目的の OU 内の SCP は、特定のタグのないリソースの作成をブロックする場合があります。この場合、AWS Control Tower はリソースのタグ付けをサポートしていないため、アカウントのプロビジョニングまたは登録は失敗します。サポートについては、アカウント担当者または サポートにお問い合わせください。

新しいアカウントを作成するとき、または既存のアカウントを登録するときに、AWS Control Tower でロールをどのように使用するかの詳細については、[「Roles and accounts」](#)を参照してください。

i Tip

既存の が登録の前提条件 AWS アカウント を満たしていることを確認することができない場合は、登録 OU を設定し、その OU にアカウントを登録できます。登録が成功したら、アカウントを目的の OU に移動できます。登録に失敗しても、他のアカウントや OU は障害の影響を受けません。

既存のアカウントとその設定が AWS Control Tower に対応しているかどうか疑問がある場合は、次のセクションで推奨されるベストプラクティスに従うことができます。

推奨: アカウントの登録に 2 段階のアプローチを設定する

- まず、コン AWS Config フォーマンスパックを使用して、アカウントがいくつかの AWS Control Tower コントロールによってどのように影響を受けるかを評価します。AWS Control Tower への登録がアカウントにどのように影響するかを確認するには、「[コンフォーマンスパックを使用した AWS Control Tower AWS Config ガバナンスの拡張](#)」を参照してください。
- 次に、アカウントを登録できます。コンプライアンスの結果が満足のいくものであれば、予想しない結果を招くことなくアカウントを登録できるため、移行パスが簡単になります。
- 評価が完了したら、AWS Control Tower ランディングゾーンを設定する場合は、評価用に作成された AWS Config 配信チャネルと設定レコーダーを削除する必要がある場合があります。そうすれば、AWS Control Tower を正常にセットアップできるようになります。

i Note

コンフォーマンスパックは、AWS Control Tower によって登録された OUs にアカウントがあるが、ワークロードは AWS Control Tower がサポートしていない AWS リージョン内で実行される状況でも機能します。適合パックを使用して、AWS Control Tower がデプロイされていないリージョンに存在するアカウントのリソースを管理できます。

アカウントが前提条件を満たしていない場合

前提条件として、AWS Control Tower ガバナンスに登録できるアカウントは、同じ組織全体に属している必要があります。アカウント登録の前提条件を満たすには、以下の準備のステップに従って、AWS Control Tower と同じ組織にアカウントを移動できます。

AWS Control Tower と同じ組織にアカウントを移動するための準備のステップ

1. 既存の組織からアカウントを削除します このアプローチを使用する場合は、別の支払い方法を指定する必要があります。
2. アカウントを AWS Control Tower の組織に参加するように招待します。詳細については、「[ユーザーガイド](#)」の「[組織に参加する AWS アカウントを招待する](#)」を参照してください。AWS Organizations
3. 招待を受け入れます アカウントは組織のルートに表示されます。このステップでは、アカウントを AWS Control Tower と同じ組織に移動し、SCP および一括請求を確立します。

Tip

アカウントが古い組織から削除される前に、新しい組織への招待を送信できます。招待は、アカウントが既存の組織から正式に削除されるのを待機します。

残りの前提条件を満たすステップ:

1. 必要な AWSControlTowerExecution ロールを作成します。
2. デフォルト VPC をクリアします (これはオプションです。AWS Control Tower は既存のデフォルト VPC を変更しません)。
3. または を使用して、既存の AWS Config 設定レコーダーまたは配信チャネルを削除 AWS CLI または変更します AWS CloudShell。詳細については、「[AWS Config リソースでアカウントを登録する](#)」および「[既存の AWS Config リソースがあるアカウントを登録する](#)」を参照してください。

これらの準備手順が完了したら、AWS Control Tower にアカウントを登録できます。詳細については、「[アカウントを手動で登録する手順](#)」を参照してください。このステップにより、アカウントが AWS Control Tower の完全な管理下に入ります。

アカウントのプロビジョニングを解除して、アカウントを登録しスタックを維持できるようにするための任意のステップ

1. 適用された CloudFormation スタックを保持するには、スタックセットからスタックインスタンスを削除し、インスタンスのスタックを保持を選択します。

2. AWS Service Catalog Account Factory でアカウントプロビジョニング済み製品を削除します。(このステップでは、プロビジョニングされた製品が AWS Control Tower から削除されるだけです。アカウントは削除されません。)
3. 必要に応じて、組織に属していないアカウントに必要な請求の詳細を使用してアカウントを設定します。次に、組織からアカウントを削除します (これを行うと、アカウントは AWS Organizations クォータの合計に対してカウントされません)。
4. リソースが残っている場合はアカウントをクリーンアップし、「[アカウントを登録解除する](#)」のアカウント閉鎖のステップに従って、アカウントを閉鎖します。
5. コントロールが定義された [Suspended] (停止状態) の OU がある場合、ステップ 1 を実行する代わりに、その OU にアカウントを移動できます。

必要な IAM ロールを既存の に手動で追加 AWS アカウント して登録する

AWS Control Tower のランディングゾーンを既に設定している場合は、AWS Control Tower に登録されている OU に組織のアカウントを登録できます。ランディングゾーンをまだ設定していない場合は、「AWS Control Tower ユーザーガイド」の「[はじめに](#)」の **ステップ 2** に記載されているステップに従います。ランディングゾーンの準備ができたなら、次のステップを実行して、手動で既存のアカウントを AWS Control Tower による管理下に入れます。

この章で前述した [登録の前提条件](#) を必ず確認してください。

AWS Control Tower にアカウントを登録する前に、そのアカウントを管理するアクセス許可を AWS Control Tower に付与する必要があります。これを行うには、次のステップに示すように、アカウントへのフルアクセス権を持つロールを追加します。これらのステップは、登録するアカウントごとに実行する必要があります。

アカウントごとに次の手順を実行します。

ステップ 1: 登録するアカウントが現在含まれている組織の管理アカウントに、管理者アクセス権を使ってサインインします。

例えば、このアカウントを から作成 AWS Organizations し、クロスアカウント IAM ロールを使用してサインインする場合、次の手順を実行できます。

1. 組織の管理アカウントにサインインします。
2. AWS Organizations に移動します。
3. [Accounts] (アカウント) で、登録するアカウントを選択し、アカウント ID をコピーします。

4. 上部のナビゲーションバーのアカウントドロップダウンメニューを開き、[Switch Role] (ロールの切り替え) を選択します。
5. [Switch Role] (ロールの切り替え) フォームで、次のフィールドに入力します。
 - [Account] (アカウント) に、コピーしたアカウント ID を入力します。
 - [Role] (ロール) に、このアカウントへのクロスアカウントアクセスを有効にする IAM ロールの名前を入力します。このロールの名前は、アカウントの作成時に定義されています。アカウントの作成時にロール名を指定していない場合は、デフォルトのロール名、OrganizationAccountAccessRole を入力します。
6. [Switch Role] (ロールの切り替え) を選択します。
7. これで、子アカウント AWS マネジメントコンソール として にサインインします。
8. 完了したら、次の手順を実行するために子アカウントにとどまります。
9. 管理アカウント ID は次のステップで入力する必要があるため、メモしておきます。

ステップ 2: AWS Control Tower にアカウントを管理する許可を付与します。

1. [IAM] に移動します。
2. [Roles] (ロール) に移動します。
3. [ロールの作成] を選択してください。
4. ロールの対象となるサービスの選択を求められたら、[カスタム信頼ポリシー] を選択します。
5. ここに示すコード例をコピーして、ポリシードキュメントに貼り付けます。文字列 *Management Account ID* を、管理アカウントの実際の管理アカウント ID に置き換えます。貼り付けるポリシーは次のとおりです。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

```
}  
]  
}
```

6. ポリシーをアタッチするよう求められたら、[AdministratorAccess] を選択します。
7. [Next:Tags] (次へ: タグ) を選択します。
8. [Add tags] (タグを追加する) というタイトルのオプションの画面が表示されることがあります。[Next:Review] (次へ: レビュー) を選択して、この画面をスキップします。
9. [Review] (確認) 画面の [Role name] (ロール名) フィールドに、AWSControlTowerExecution と入力します。
10. [Description] (説明) ボックスに、登録のためのフルアカウントアクセスを許可などの短い説明を入力します。
11. [ロールの作成] を選択してください。

ステップ 3: 登録された OU に移動してアカウントを登録し、登録を確認します。

ロールを作成して必要なアクセス許可を設定したら、次のステップに従ってアカウントを登録し、登録を確認します。

1. 管理者として再度サインインし、AWS Control Tower に移動します。
2. アカウントを登録します。
 - AWS Control Tower の [Organization] (組織) ページでアカウントを選択し、右上にある [Actions] (アクション) ドロップダウンメニューから [Enroll] (登録) を選択します。
 - [アカウントを手動で登録する手順](#) ページで示されているように、個々のアカウントを登録する手順に従います。
3. 登録を確認します。
 - AWS Control Tower から、左側のナビゲーションの [Organization] (組織) を選択します。
 - 最近登録したアカウントを探します。初期状態では、[Enrolling] (登録中) のステータスが表示されます。
 - 状態が [Enrolled] (登録済み) に変わったら、移動は成功です。

このプロセスを続行するには、AWS Control Tower に登録する組織内の各アカウントにサインインします。各アカウントについて、前提条件のステップと登録のステップを繰り返します。

AWSControlTowerExecution ロールを追加する例

次の YAML テンプレートを使用すると、アカウントに必要なロールを作成してプログラマ的に登録できます。

```
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
```

既存の AWS Config リソースがあるアカウントを登録する

このトピックでは、既存の AWS Config リソースを持つアカウントを登録する方法をステップバイステップのアプローチを使って説明します。既存のリソースを確認する方法の例については、「[AWS Config リソースでアカウントを登録する](#)」を参照してください。

AWS Config リソースの例

アカウントがすでに持っている可能性のある AWS Config リソースのタイプを次に示します。AWS Control Tower にアカウントを登録できるようにするには、これらのリソースの変更が必要になる場合があります。

- AWS Config レコーダー
- AWS Config 配信チャネル
- AWS Config 集約認可

制限事項

- 既存の AWS Config リソースを使用してアカウントを登録することは、ランディングゾーンで設定された管理アカウントまたはサービス統合アカウント (複数可) ではサポートされていません。
- アカウントは、 を有効にする OU 登録または再登録ワークフローを使用してのみ登録できますAWSControlTowerBaseline。アカウントは、 を有効化またはリセットして登録することはできませんConfigBaseline。
- 既存の AWS Config リソースを持つアカウントは、 ではサポートされていません [自動登録でアカウントを移動して登録する](#)。
- リソースが変更され、アカウントにドリフトが生じてても、AWS Control Tower はリソースを更新しません。
- AWS Config AWS Control Tower によって管理されていないリージョンの リソースは変更されません。

引き受け

- AWS Control Tower ランディングゾーンをデプロイしました。
- アカウントがまだ AWS Control Tower に登録されていないこと。
- アカウントには、AWS Control Tower によって管理されるリージョンの少なくとも 1 つに、少なくとも 1 つの既存の AWS Config リソースがあります。
- アカウントでガバナンスドリフトが発生していないこと。

Note

既存の Config リソースを持つアカウントを、許可リストに追加せずに登録しようとする、登録は失敗します。後で、同じアカウントを許可リストに追加しようとしても、AWS Control Tower はアカウントが正しくプロビジョニングされていることを検証できません。許可リストをリクエストして登録する前に、AWS Control Tower からアカウントをプロビジョニング解除する必要があります。アカウントを別の AWS Control Tower OU に移動し

ただけでは、ガバナンスドリフトが発生し、アカウントを許可リストに追加できなくなります。

既存の AWS Config リソースにアカウントを登録する自動アプローチを説明するブログについては、[「AWS Control Tower への既存の AWS Config リソースを持つアカウントの登録を自動化する」](#)を参照してください。

このプロセスには主に次の 5 つのステップがあります。

1. AWS Control Tower 許可リストにアカウント (複数可) を追加します。
2. アカウントで新しい IAM ロールを作成します。
3. 既存の AWS Config リソースを変更します。
4. リソースが存在しない AWS リージョンに AWS Config リソースを作成します。
5. AWS Control Tower にアカウントを登録します。

先に進む前に、このプロセスに関する次の期待事項を考慮してください。

- AWS Control Tower はこのアカウントに AWS Config リソースを作成しません。
- 登録後、AWS Control Tower コントロールは、新しい IAM ロールを含む、作成した AWS Config リソースを自動的に保護します。
- 登録後に AWS Config リソースに変更があった場合は、アカウントを再登録する前に、AWS Control Tower の設定に合わせてリソースを更新する必要があります。

ステップ 1: サポートに連絡して、許可リストにアカウント (複数可) を追加する

チケットの件名には次の文章を使用してください。

既存の AWS Config リソースがあるアカウントを AWS Control Tower に登録する

チケットの本文に以下の詳細を記載してください。

- 管理アカウント番号
- 既存の AWS Config リソースを持つメンバーアカウントのアカウント番号。登録するすべてのアカウントのサポートケースを作成できます。

- AWS Control Tower のセットアップで選択したホームリージョン

 Note

アカウントを許可リストに追加するのに必要な時間は 2 営業日です。

ステップ 2: メンバーアカウントに新しい IAM ロールを作成する

1. メンバーアカウントの CloudFormation コンソールを開きます。
2. 次のテンプレートを使用して新しいスタックを作成します。

```
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. スタックの名前を CustomerCreatedConfigRecorderRoleForControlTower とします。
4. スタックを作成します。

Note

作成する SCP は `aws-controltower-ConfigRecorderRole*` ロールを除外する必要があります。AWS Config ルールが評価を実行する機能を制限するアクセス許可を変更しないでください。

Config の呼び出しから `aws-controltower-ConfigRecorderRole*` をブロックする SCP がある場合に `AccessDeniedException` を受信しないよう、次のガイドラインに従ってください。

ステップ 3: 既存のリソースがある AWS リージョンを特定する

アカウント内の管理対象リージョン (AWS Control Tower 管理対象) ごとに、前述の既存の AWS Config リソースサンプルタイプが少なくとも 1 つあるリージョンを特定してメモします。

ステップ 4: AWS Config リソースがない AWS リージョンを特定する

アカウント内の管理対象リージョン (AWS Control Tower 管理対象) ごとに、前述のサンプルタイプの AWS Config リソースがないリージョンを特定してメモします。

ステップ 5: 各 AWS リージョンの既存のリソースを変更する

このステップでは、AWS Control Tower のセットアップに関する次の情報が必要です。

- `AUDIT_ACCOUNT` - AWS Config サービス統合アカウント (以前は監査アカウントと呼ばれていた) ID
- `CONFIG_BUCKET` - AWS Config が設定スナップショットと設定履歴ファイルを配信する AWS S3 バケット。次のステップに進む前に、AWS S3 バケットがあることを確認します。
 - ランディングゾーンバージョン 3.3 以前では、AWS S3 バケットの名前は `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`、ログ記録アカウントにあります。
 - ランディングゾーンバージョン 4.0 以降では、AWS S3 バケットの名前は `aws-controltower-config-logs-AUDIT_ACCOUNT-<REGION_STRING>-<SUFFIX_STRING>`、AWS Config サービス統合アカウント (以前の監査アカウント) にあります。
- `IAM_ROLE_ARN` - ステップ 2 で作成した IAM ロール ARN
- `ORGANIZATION_ID` - 管理アカウントの組織 ID

- MEMBER_ACCOUNT_NUMBER - 変更対象のメンバーアカウント
- HOME_REGION - AWS Control Tower のセットアップのホームリージョン

次のセクション 5a～5c の指示に従って、既存のリソースを変更します。

ステップ 5a. AWS Config recorder リソース

AWS リージョンごとに存在できる AWS Config レコーダーは 1 つだけです。それが存在する場合は、次のように設定を変更します。ホームリージョンでは項目 GLOBAL_RESOURCE_RECORDING を true に置き換えます。AWS Config レコーダーが存在する他のリージョンの項目を false に置き換えます。

- Name: 変更なし
- RoleARN: IAM_ROLE_ARN
 - RecordingGroup:
 - AllSupported: true
 - IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
 - ResourceTypes: 空欄

この変更は、次のコマンドを使用して AWS CLI から行うことができます。文字列を既存の AWS Config レコーダー名 RECORDER_NAME に置き換えます。

```
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
```

ステップ 5b. AWS Config 配信チャネルリソースを変更する

リージョンごとに存在できる AWS Config 配信チャネルは 1 つだけです。2 つ以上存在する場合は、次のように設定を変更します。

- Name: 変更なし
- ConfigSnapshotDeliveryProperties: TwentyFour_Hours

- S3BucketName: *CONFIG_BUCKET*
- S3KeyPrefix: *ORGANIZATION_ID*
- SnsTopicARN: 次の形式の、監査アカウントからの SNS トピック ARN。

```
arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-  
AllConfigNotifications
```

この変更は、次のコマンドを使用して AWS CLI から行うことができます。文字列を既存の AWS Config レコーダー名 *DELIVERY_CHANNEL_NAME* に置き換えます。

```
aws configservice put-delivery-channel --delivery-channel  
name=DELIVERY_CHANNEL_NAME,s3BucketName=CONFIG_BUCKET,s3KeyPrefix="ORGANIZATION_ID",configSnap  
controltower-AllConfigNotifications --region CURRENT_REGION
```

ステップ 5c。AWS Config 集約認可リソースの変更

Note

ランディングゾーンバージョン 4.0 以降では、このステップは必要ありません。

リージョンごとに複数の集約認証が存在できます。AWS Control Tower には、監査アカウントを認可済みアカウントとして指定し、AWS Control Tower のホームリージョンを認可リージョンとして指定する集約認可が必要です。存在しない場合、次の設定を使用して新しく作成します。

- AuthorizedAccountId: 監査アカウント ID
- AuthorizedAwsRegion: AWS Control Tower セットアップのホームリージョン

この変更は、次のコマンドを使用して AWS CLI から行うことができます。

```
aws configservice put-aggregation-authorization --authorized-account-  
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region  
CURRENT_REGION
```

ステップ 6: AWS Control Tower が管理するリージョンで、リソースが存在しない場所にリソースを作成する

次の例GLOBAL_RESOURCE_RECORDINGに示すように、ホームリージョンで IncludeGlobalResourceTypes パラメータの値が になるように CloudFormation テンプレートを改訂します。また、このセクションで指定している、テンプレートの必須フィールドを更新します。

ホームリージョンでは項目 GLOBAL_RESOURCE_RECORDING を true に置き換えます。AWS Config レコーダーが存在しない他のリージョンの場合は、項目を false に置き換えます。

1. 管理アカウントの CloudFormation コンソールに移動します。
2. CustomerCreatedConfigResourcesForControlTower という名前の新しい StackSet を作成します。
3. 次のテンプレートをコピーして更新します。

Note

テンプレートの CustomerCreatedAggregationAuthorization リソースは、ランディングゾーンバージョン 4.0 以降では必要ありません。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
```



```
S3BucketName: CONFIG_BUCKET
S3KeyPrefix: ORGANIZATION_ID
SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
CustomerCreatedAggregationAuthorization:
  Type: "AWS::Config::AggregationAuthorization"
  Properties:
    AuthorizedAccountId: AUDIT_ACCOUNT
    AuthorizedAwsRegion: HOME_REGION
```

必須フィールドを使用してテンプレートを更新します。

- a. S3BucketName フィールドで、**CONFIG_BUCKET** を置き換えます。
 - b. [S3KeyPrefix] フィールドで、**ORGANIZATION_ID** を置き換えます。
 - c. [SnsTopicARN] フィールドで、**AUDIT_ACCOUNT** を置き換えます。
 - d. [AuthorizedAccountId] フィールドで、**AUDIT_ACCOUNT** を置き換えます。
 - e. [AuthorizedAwsRegion] フィールドで、**HOME_REGION** を置き換えます。
4. CloudFormation コンソールでのデプロイ中に、メンバーアカウント番号を追加します。
 5. ステップ 4 で特定した AWS リージョンを追加します。
 6. スタックセットをデプロイします。

ステップ 7: OU を AWS Control Tower に登録する

AWS Control Tower のダッシュボードで OU を登録します。

Note

アカウントの登録ワークフローは、このタスクでは成功しません。[Register OU] (OU の登録) または [Re-register OU] (OU の再登録) を選択する必要があります。

Account Factory でのアカウントのプロビジョニングと管理

Note

単一アカウントのプロビジョニング、更新、カスタマイズは、AWSControlTowerBaseline を有効にした組織単位 (OU) をターゲットにする必要があります。OU で

AWSControlTowerBaseline が有効になっていない場合は、アカウントの自動登録を有効にするか、EnabledBaseline で ResetEnabledBaseline API と ResetEnabledControl APIs を使用し、その OU で EnabledControls を使用してアカウントを登録できます。EnabledBaselines AWSControlTowerBaseline の詳細については、「」を参照してください[OU レベルで適用されるベースラインタイプ](#)。

この章では、Account Factory を使用して AWS Control Tower ランディングゾーンに新しいメンバーアカウントをプロビジョニングするための概要と手順について説明します。

アカウントの設定とプロビジョニングのためのアクセス許可

AWS Control Tower Account Factory を使用すると、 のクラウド管理者とユーザーがランディングゾーンにアカウント AWS IAM アイデンティティセンター をプロビジョニングできます。デフォルトでは、IAM Identity Center ユーザーは AWSAccountFactory グループまたは管理グループに属している必要があります。

Note

組織全体で許可を持つアカウントを使用する場合と同様に、管理アカウントから作業するときには注意が必要です。

AWS Control Tower 管理アカウントには AWSControlTowerExecution ロールとの信頼関係があります。これにより、一部の自動アカウント設定も含めて、管理アカウントからのアカウント設定が可能になります。AWSControlTowerExecution ロールの詳細については、「[Roles and accounts](#)」を参照してください。

Note

既存の AWS アカウント を AWS Control Tower に登録するには、そのアカウントでAWSControlTowerExecutionロールが有効になっている必要があります。既存のアカウントを登録する方法の詳細については、「[既存のアカウントの登録について](#)」を参照してください。

権限の詳細については、「[アカウントのプロビジョニングに必要なアクセス許可](#)」を参照してください。

Account Factory アカウントの管理に関する考慮事項

Account Factory を使用して作成およびプロビジョニングしたアカウントは、更新、登録解除、および閉鎖できます。転用したいアカウントのユーザーパラメータを更新することで、アカウントを再利用できます。アカウントの組織単位 (OU) を変更することもできます。

Note

Account Factory が供給するアカウントに関連付けられているプロビジョニング済み製品を更新するときに、新しいユーザーの E メールアドレスを指定すると AWS IAM アイデンティティセンター、AWS Control Tower は IAM Identity Center に新しいユーザーを作成します。以前に作成したアカウントは削除されません。IAM Identity Center から以前の IAM Identity Center ユーザーの E メールアドレスを削除する方法については、「[Disabling a User](#)」(ユーザーを無効にする) を参照してください。

AWS Control Tower でアカウントを更新して移動する

登録したアカウントを更新する最も簡単な方法は、AWS Control Tower コンソールから行うことです。個々のアカウントの更新は、[移動されたメンバーアカウント](#) のようなドリフトを解決するのに役立ちます。ランディングゾーンの完全な更新の一部として、アカウントの更新も必要です。

コンソールでアカウントを更新する

AWS Control Tower コンソールでアカウントを更新するには

1. AWS Control Tower の [Organization] (組織) ページに移動します。
2. OU のリストで、更新するアカウントの名前を選択します。更新可能なアカウントには、[Update available] (更新可能) のステータスが表示されます。
3. 次に、選択したアカウントのページの [Account details] (アカウントの詳細) が表示されます。
4. 右上の [Update account] (アカウントの更新) を選択します。

ある組織単位 (OU) から別の OU にアカウントを移動する場合、新しい OU によって適用されるコントロールが以前の OU のコントロールとは異なる場合があることに注意してください。新しい OU のコントロールがアカウントのポリシー要件を満たしている必要があります。

AWS Control Tower アカウントは、アカウントの自動登録をオプトインしたかどうかによって変更されます。自動登録の詳細については、「[オプションでアカウントの自動登録を設定する](#)」を参照してください。

自動登録を使用して、アカウントが OU 間を移動するときの動作を制御する

アカウントを新しい OU に移動するとき、AWS Control Tower は OU で有効なベースラインとコントロールをアカウントに適用します。前の OU のコントロールとベースラインは削除されます。登録されている OU の外部にアカウントを移動すると、AWS Control Tower はデプロイされたすべてのベースラインとコントロールを削除します。

自動登録を使用しないで、アカウントが OU 間を移動するときの動作を制御する

アカウントを OU 間で移動するとき、宛先 OU のコントロールがアカウントに適用されます。ただし、以前の OU のアカウントに適用されていたコントロールは削除されません。コントロールの正確な動作は、以前の OU と宛先 OU でアクティブなコントロールの実装に固有です。

- AWS Config ルールで実装されたコントロールの場合: 前の OU のコントロールは削除されません。このようなコントロールは手動で削除する必要があります。
- SCP を使用して実装されたコントロールの場合: 以前の OU の SCP ベースのコントロールは削除されます。宛先 OU の SCP ベースのコントロールがこのアカウントで有効になります。
- CloudFormation フックを使用して実装されたコントロールの場合: この動作は、新しい OU のコントロールのステータスによって異なります。
 - 宛先 OU でフックベースのコントロールが有効になっていない場合: 古いコントロールは、手動で削除しない限り、移動したアカウントに対して有効なままとなります。
 - 宛先 OU でフックのコントロールが有効になっている場合: 古いコントロールは削除され、宛先 OU のコントロールがアカウントに適用されます。

登録済みアカウントの E メールアドレスの変更

AWS Control Tower で登録されたメンバーアカウントの E メールアドレスを変更するには、このセクションの手順に従います。

Note

以下の手順では、管理アカウント、ログアーカイブアカウント、または監査アカウントの E メールアドレスを変更することはできません。詳細については、[AWS 「アカウントに関連](#)

[付けられた E メールアドレスを変更するにはどうすればよいですか？](#)」または「サポート」にお問い合わせください AWS。

AWS Control Tower によって作成されたアカウントの E メールアドレスを変更するには

1. アカウントのルートユーザーパスワードを回復します。[「紛失または忘れた AWS パスワードを復元するにはどうすればよいですか？」の記事の手順に従います。](#)
2. ルートユーザーパスワードでアカウントにサインインします。
3. E メールアドレスを他のメールアドレスと同じように変更し AWS アカウント、変更が反映されるまで待ちます AWS Organizations。E メールアドレスの変更による更新が完了するまで、遅延が発生する可能性があります。
4. アカウントに以前にあった E メールアドレスを使用して、Service Catalog でプロビジョニング済み製品を更新します。プロビジョニング済み製品を更新するプロセスには、新しい E メールアドレスのプロビジョニング済み製品への関連付けが含まれます。これにより、E メールアドレスの変更が AWS Control Tower で有効になります。今後プロビジョニングされる製品の更新には、新しい E メールアドレスを使用します。

AWS Organizationsで作成したメンバーアカウントのパスワードまたは E メールアドレスを変更するには、「AWS Organizations ユーザーガイド」の「[ルートユーザーとしてのメンバーアカウントへのアクセス](#)」を参照してください。

または、ルートユーザーとしてログインしなくても、AWS Organizations コンソールから Account Factory または他のメンバーアカウントの E メールアドレスを更新できます。詳細については、「AWS Organizations User Guide」の「[Updating the root user email address for a member account with AWS Organizations](#)」を参照してください。

登録済みアカウントの名前を変更する

このセクションの手順に従って、登録された AWS Control Tower アカウントの名前を変更します。

Note

AWS 管理者アカウントの名前を変更するには、管理者権限があり、アカウントのルートユーザーとしてログインしている必要があります。

AWS Organizations コンソールまたは APIs を使用して AWS Control Tower によって作成されたアカウントの名前を変更するには

- 「AWS アカウント管理リファレンスガイド」に[記載されている手順](#)に従ってください。

AWS Control Tower によって作成されたアカウントの名前を変更する代替方法

1. アカウントの root パスワードを回復します。この記事で説明されている手順に従います。[紛失または忘れた AWS パスワードを復元するにはどうすればよいですか？](#)
2. root パスワードでアカウントにサインインします。
3. AWS Billing コンソールで、アカウント設定ページに移動します。
4. その他の AWS アカウントの場合と同様に、[Account settings] (アカウント設定) で名前を変更します。
5. AWS Control Tower が自動的に更新され、名前の変更が反映されます。この更新は、AWS Service Catalogのプロビジョニング済み製品には反映されません。

Amazon Virtual Private Cloud の設定を使用して Account Factory を構成する

Account Factory により、組織内のアカウントに対して、事前承認済みのベースラインと設定オプションを作成できます。AWS Service Catalogを通じて新しいアカウントを設定し、プロビジョニングできます。

Account Factory ページに、組織単位 (OU) のリストとその許可リストのステータスが表示されます。デフォルトでは、すべての OU が許可リストに表示されます。つまり、アカウントは OU の下でプロビジョニングできます。アカウントプロビジョニングのために特定の OUsを無効にすることができます AWS Service Catalog。

エンドユーザーが新しいアカウントをプロビジョニングするときに使用できる Amazon VPC 設定オプションを表示できます。

Account Factory で Amazon VPC 設定を構成するには

1. 中央のクラウド管理者として、管理アカウントの管理者権限で AWS Control Tower コンソールにサインインします。
2. ダッシュボードの左側から [Account Factory] を選択し、Account Factory ネットワーク設定ページに移動します。そこに、デフォルトのネットワーク設定が表示されます。編集するに

は、[Edit] (編集) を選択し、編集可能なバージョンの Account Factory ネットワーク設定を表示します。

- 必要に応じて、デフォルト設定の各フィールドを変更できます。エンドユーザーが作成できるすべての新しい Account Factory アカウントに指定する VPC 設定オプションを選択し、該当する設定をフィールドに入力します。
- [disabled] (無効) または [enabled] (有効) を選択して、Amazon VPC にパブリックサブネットを作成します。デフォルトでは、インターネットにアクセス可能なサブネットは許可されません。

 Note

新しいアカウントをプロビジョニングするときにパブリックサブネットが有効になるように Account Factory の VPC 設定を定義すると、Account Factory によって Amazon VPC が設定されて、[NAT ゲートウェイ](#)が作成されます。料金は Amazon VPC による使用量に対して請求されます。詳細については、「[Amazon VPC の料金](#)」を参照してください。

- リストから、Amazon VPC のプライベートサブネットの最大数を選択します。デフォルトでは、[1] が選択されています。許可されるプライベートサブネットの最大数は、アベイラビリティゾーンごとに 2 です。
- アカウントの VPC を作成するための IP アドレスの範囲を入力します。この値は、クラスレスドメイン間ルーティング (CIDR) ブロックの形式 (例: デフォルトは 172.31.0.0/16) であることが必要です。この CIDR ブロックは、アカウント用に Account Factory が作成する VPC の全範囲のサブネット IP アドレスを提供します。VPC 内では、サブネットは指定した範囲から自動的に割り当てられ、各サブネットは同じサイズになります。デフォルトでは、VPC 内のサブネットは重複しません。ただし、プロビジョニングされたすべてのアカウントの VPC 間ではサブネット IP アドレス範囲が重複する場合があります。
- アカウントのプロビジョニング時に VPC を作成する 1 つのリージョンまたはすべてのリージョンを選択します。デフォルトでは、すべての使用可能なリージョンが選択されます。
- リストから、各 VPC にサブネットを設定するアベイラビリティゾーンの数を選択します。デフォルト値および推奨値は 3 です。
- [Save] (保存) を選択します。

これらの設定オプションを設定して、VPC を含まない新しいアカウントを作成できます。詳しくは「[チュートリアル](#)」を参照してください。

アカウントを登録解除する

Account Factory でアカウントを作成したか、を登録し AWS アカウント、ランディングゾーンでアカウントを AWS Control Tower によって管理する必要がなくなった場合は、AWS Control Tower コンソールからアカウントを登録解除できます。

AWS Control Tower アカウントを登録解除すると、AWS Control Tower によってプロビジョニングされたすべてのリソースがコントロールとブループリントも含めて削除されます。アカウントは AWS Control Tower OU からルートエリアに移動されます。アカウントは登録済み OU の一部ではなくなり、AWS Control Tower の SCP の対象ではなくなります。アカウントは を通じて閉鎖できます AWS Organizations。

AWS Control Tower コンソールから登録済みアカウントの登録を解除するには

1. ウェブブラウザで AWS Control Tower コンソール (<https://console.aws.amazon.com/controltower>) を開きます。
2. 左側のナビゲーションペインから、[組織] を選択します。
3. [組織] ページで、OU の近くにある + ボタンを選択して、アカウントを含む OU を展開します。
4. アカウントを選択し、[管理を解除] を選択します。

Note

アカウントのステータスが [未登録] と表示されるまで待ちます。

このアカウントが不要になった場合は、解約します。AWS アカウント解約の詳細については、「AWS Billing ユーザーガイド」の「[アカウントの解約](#)」を参照してください。

自動登録がアクティブになったときにアカウントの登録を解除する

[設定] ページで自動登録機能が有効になっている場合は、AWS Control Tower に登録されていない OU に移動してアカウントの登録を解除することもできます。すべての AWS Control Tower リソースが削除されます。この方法で誤ってアカウントの登録を解除しないように注意してください。ただし、OU に戻すことでアカウントを再登録できます。

カスタマイズされたアカウントの登録を解除すると、ランディングゾーンによってデプロイされたリソースと、AWS Control Tower がアカウント内に作成したその他のリソースが AWS

Control Tower によって削除されます。手動で追加された場合でも、AWS Control Tower は AWSControlTowerExecution ロールも削除します。このロールを削除すると、サービス実行ロールは管理対象外のアカウントに残らないため、最小特権の原則に一致します。

アカウントを登録解除したら、アカウントを閉鎖できます AWS Organizations。

Note

登録解除されたアカウントは解約も削除もされていません。アカウントが登録解除されても、Account Factory でアカウントを作成する際に選択した IAM アイデンティティセンターユーザーは引き続きこのアカウントに対する管理者権限を保持します。このユーザーに管理者権限を持たせないようにするには、Account Factory でアカウントを更新し、このアカウントの IAM Identity Center ユーザー E メールアドレスを変更して、IAM Identity Center のこの設定を変更する必要があります。詳細については、「[AWS Control Tower でアカウントを更新して移動する](#)」を参照してください。

動画チュートリアル

この動画 (3 分 25 秒) では、AWS Control Tower からのアカウントの削除、アカウントへのルートアクセスの取得、最後に AWS アカウントの解約を行う方法を示します。アカウントを解約するには、[AWS Organizations API](#) を使用することもできます。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower でのアカウントの解約方法に関する動画チュートリアル。](#)

AWS Control Tower の一般的なタスクを説明する AWS [YouTube 動画](#) のリストを表示できます。

Account Factory で作成されたアカウントを解約する

Account Factory で作成されたアカウントは、AWS アカウントです。AWS アカウントの解約の詳細については、「[AWS Account Management Reference Guide](#)」の「[Closing an account](#)」を参照してください。

Note

の閉鎖 AWS アカウント は、AWS Control Tower からのアカウントの登録解除とは異なります。これらは個別のアクションです。アカウントを解約する前に、アカウントを登録解除する必要があります。

を使用して AWS Control Tower メンバーアカウントを閉鎖する AWS Organizations

組織の管理アカウントから AWS Control Tower メンバーアカウントを閉鎖できます。ルート認証情報を使用して各メンバーアカウントに個別にサインインする必要はありません AWS Organizations。ただし、この方法で管理アカウントを解約することはできません。

AWS Organizations [CloseAccount API](#) を呼び出すか、AWS Organizations コンソールでアカウントを閉じると、メンバーアカウントは AWS アカウント 90 日間分離されます。アカウントのステータスは、AWS Control Tower と AWS Organizations で [Suspended] (停止) となります。この 90 日間にアカウントを操作しようとする、AWS Control Tower からエラーメッセージが表示されます。

Note

OU がアカウントを停止した場合、ターゲットのリージョンコントロールの EnabledControl オペレーションは失敗します。

90 日が経過する前に、メンバーアカウントを復元できます AWS アカウント。90 日が過ぎると、アカウントのレコードは削除されます。

ベストプラクティスとして、メンバーアカウントを解約する前に、そのアカウントを登録解除することをお勧めします。メンバーアカウントを最初に管理解除せずに解約すると、AWS Control Tower でアカウントのステータスは [Suspended] (停止) とともに [Enrolled] (登録済み) と表示されます。その結果、この 90 日の期間中にアカウントの OU を再登録しようとする、AWS Control Tower からエラーメッセージが表示されます。停止中のアカウントは、基本的に、事前チェックに失敗した再登録アクションをブロックします。OU からアカウントを削除すると、OU を再登録できますが、アカウントの支払い方法がないとエラーが発生する AWS 可能性があります。この制約を回避するには、別の OU を作成し、この OU にアカウントを移動してから再登録を試みます。この OU の名前は、Suspended OU とすることをお勧めします。

Note

アカウントを解約する前に登録を解除しない場合は、その 90 日が経過 AWS Service Catalog した後に でアカウントのプロビジョニング済み製品を削除する必要があります。

詳細については、[CloseAccount API](#) に関する AWS Organizations ドキュメントを参照してください。

Account Factory のリソースに関する考慮事項

アカウントが Account Factory でプロビジョニングされると、アカウント内に次の AWS リソースが作成されます。

AWS サービス	リソースタイプ	リソース名
AWS CloudFormation	スタック	StackSet-AWSContro ITowerBP-BASELINE- CLOUDTRAIL-*
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDWATCH-*
		StackSet-AWSContro ITowerBP-BASELINE- CONFIG-*
		StackSet-AWSContro ITowerBP-BASELINE-ROLES- *
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-ROLES-*
AWS CloudTrail	追跡	aws-controltower-BaselineCl oudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComp lianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrail Logs
		/aws/lambda/aws-controltowe r-NotificationForwarder

AWS サービス	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	aws-controltower-AdministratorExecutionRole
		aws-controltower-CloudWatchLogsRole
		aws-controltower-ConfigRecorderRole
		aws-controltower-ForwardSnsNotificationRole
		aws-controltower-ReadOnlyExecutionRole
		AWSControlTowerExecution
AWS Identity and Access Management	ポリシー	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	トピック	aws-controltower-SecurityNotifications
AWS Lambda	アプリケーション	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	関数	aws-controltower-NotificationForwarder
Amazon EventBridge	ルール	AWSControlTowerManagedRule
Amazon EventBridge	ルール	aws-controltower-ConfigComplianceChangeEventRule

Account Factory Customization (AFC) を使用したアカウントのカスタマイズ

Note

単一アカウントのプロビジョニング、更新、カスタマイズは、AWSControlTowerBaseline を有効にした組織単位 (OU) をターゲットにする必要があります。OU で AWSControlTowerBaseline が有効になっていない場合は、アカウントの自動登録を有効にするか、EnabledBaseline で ResetEnabledBaseline API と ResetEnabledControl APIs を使用してアカウント EnabledControls を登録できます。EnabledBaselines AWSControlTowerBaseline の詳細については、「」を参照してください[OU レベルで適用されるベースラインタイプ](#)。

AWS Control Tower では、AWS Control Tower コンソールからリソースをプロビジョニング AWS アカウント するとき、新規および既存の をカスタマイズできます。AWS Control Tower では、Account Factory Customization を設定すると、今後のプロビジョニングに備えてこのプロセスが自動化されるため、パイプラインを維持する必要がなくなります。カスタマイズされたアカウントは、リソースがプロビジョニングされるとすぐに使用できます。

ブループリントを使用して新しいアカウントをプロビジョニングする

カスタマイズされたアカウントは、AWS Control Tower Account Factory、CloudFormation テンプレート、または Terraform を使用してプロビジョニングされます。カスタマイズされたアカウントのブループリントとして機能するテンプレートは、ユーザーが定義します。ブループリントでは、アカウントのプロビジョニング時に必要な特定のリソースと設定が記述されています。AWS パートナーによって構築および管理される事前定義されたブループリントも利用できます。パートナーが管理するブループリントの詳細については、「[AWS Service Catalog 入門ライブラリ](#)」を参照してください。

既存のアカウントにブループリントを適用

AWS Control Tower コンソールのアカウント更新ステップに従って、カスタマイズされたブループリントを既存のアカウントに適用することもできます。詳細については、「[コンソールでアカウントを更新する](#)」を参照してください。

定義: ハブアカウント

アカウントのブループリントは に保存されます。このため AWS アカウント、ハブアカウントと呼ばれます。ブループリントは Service Catalog 製品の形式で保存されます。他の Service Catalog 製品と区別するために、この製品をブループリントと呼びます。Service Catalog 製品の作成方法の詳細については、「AWS Service Catalog 管理者ガイド」の「[製品の作成](#)」を参照してください。

Note

AWS Control Tower にはプロアクティブコントロールが含まれており、AWS Control Tower で CloudFormation リソースを監視します。オプションで、これらのコントロールをランディングゾーンでアクティブ化できます。プロアクティブコントロールを適用すると、アカウントにデプロイするリソースが組織のポリシーと手順に準拠しているかどうかチェックされます。プロアクティブコントロールの詳細については、「[Proactive controls](#)」を参照してください。

AFC との連携の詳細については、「[Automate account customization using Account Factory Customization in AWS Control Tower](#)」(AWS Control Tower の Account Factory Customization を使ったアカウントのカスタマイズの自動化) を参照してください。

前提条件

カスタマイズされたアカウントの作成を AWS Control Tower の Account Factory を使用して開始する前に、AWS Control Tower のランディングゾーン環境をデプロイし、新しく作成したアカウントを配置する組織単位 (OU) を AWS Control Tower に登録しておく必要があります。

カスタマイズの準備

- ハブアカウントを指定する: ハブアカウントとして機能する新しいアカウントを作成するか、既存のを使用できます AWS アカウント。AWS Control Tower 管理アカウントをブループリントハブアカウントとしては使用しないことを強くお勧めします。
- 必要なロールを追加する: AWS Control Tower AWS アカウント に登録してカスタマイズする場合は、AWS Control Tower に登録する他のアカウントと同様に、まずロールをAWSCloudControlTowerExecutionそれらのアカウントに追加する必要があります。
- パートナーのブループリントの設定 (オプション): マーケットプレイスサブスクリプション要件を持つパートナーのブループリントを使用する予定の場合は、これらのブループリントを AWS

Control Tower 管理アカウントから設定した後に Account Factory Customization ブループリントとしてデプロイする必要があります。

トピック

- [カスタマイズのための設定](#)
- [ブループリントからカスタマイズされたアカウントを作成する](#)
- [登録時に AFC を使用してアカウントをカスタマイズする](#)
- [ブループリントを AWS Control Tower アカウントに追加する](#)
- [ブループリントを更新する](#)
- [アカウントからブループリントを削除する](#)
- [パートナーのブループリント](#)
- [Account Factory Customizations \(AFC\) に関する考慮事項](#)
- [ブループリントエラーが発生した場合](#)
- [CloudFormation に基づく AFC ブループリント用のポリシードキュメントのカスタマイズ](#)
- [Terraform ベースの Service Catalog 製品の作成に必要な追加のアクセス許可](#)
- [AWS Service Catalog 外部製品タイプへの移行](#)

カスタマイズのための設定

次のセクションでは、カスタマイズプロセスのために Account Factory を設定する手順について説明します。これらの手順を開始する前に、ハブアカウントを[委任管理者](#)として設定することをお勧めします。

概要

- ステップ 1. 必要なロールを作成します。Service Catalog 製品 (ブループリントとも呼ばれます) が保存される (ハブ) アカウントにアクセスする許可を AWS Control Tower に付与する IAM ロールを作成します。
- ステップ 2. AWS Service Catalog 製品を作成します。カスタムアカウントのベースライン化に必要な AWS Service Catalog 製品 (「ブループリント製品」とも呼ばれます) を作成します。
- ステップ 3. カスタムブループリントを確認します。作成した AWS Service Catalog 製品 (ブループリント) を検査します。

- Step 4. ブループリントを呼び出して、カスタマイズされたアカウントを作成します。アカウントの作成時、ブループリント製品の情報とロール情報を AWS Control Tower コンソールの Account Factory の適切なフィールドに入力します。

ステップ 1. 必要なロールを作成する

アカウントのカスタマイズを開始する前に、AWS Control Tower とハブアカウント間の信頼関係を含んでいるロールを設定する必要があります。このロールが継承されると、ハブアカウントのリソースを管理するためのアクセス権を AWS Control Tower に付与できます。ロールの名前は `AWSControlTowerBlueprintAccess` にする必要があります。

AWS Control Tower はこのロールを引き受けて、ユーザーに代わってポートフォリオリソースを作成し AWS Service Catalog、ブループリントを Service Catalog 製品としてこのポートフォリオに追加し、アカウントプロビジョニング中にこのポートフォリオとブループリントをメンバーアカウントと共有します。

以下のセクションの説明に従って、`AWSControlTowerBlueprintAccess` ロールを作成します。ロールは、登録済みアカウントまたは未登録アカウントで設定できます。

 IAM コンソールに移動して、必要なロールを設定します。

登録されている AWS Control Tower アカウントで `AWSControlTowerBlueprintAccess` ロールを設定するには

1. AWS Control Tower 管理アカウントにプリンシパルとしてフェデレートまたはサインインします。
2. 管理アカウントのフェデレーションプリンシパルから、ブループリントハブアカウントとして機能するように選択した登録済みの AWS Control Tower アカウントの `AWSControlTowerExecution` ロールを継承するか、ロールを切り替えます。
3. 登録した AWS Control Tower アカウントの `AWSControlTowerExecution` ロールから、適切な権限と信頼関係を持つ `AWSControlTowerBlueprintAccess` ロールを作成します。

⚠ Important

AWS ベストプラクティスのガイダンスに準拠するには、AWSControlTowerExecution ロールの作成直後に AWSControlTowerBlueprintAccess ロールからサインアウトすることが重要です。AWSControlTowerExecution ロールは、リソースの意図しない変更を防ぐために、AWS Control Tower でのみ使用することを目的としています。

ブループリントハブアカウントが AWS Control Tower に登録されていない場合は、AWSControlTowerExecution ロールがアカウントに存在しないため、AWSControlTowerBlueprintAccess ロールのセットアップを続行する前にロールを継承する必要があります。

未登録のメンバーアカウントで AWSControlTowerBlueprintAccess ロールを設定するには

1. 推奨されている方法で、ハブアカウントとして指定したいアカウントにプリンシパルとしてフェデレートまたはサインインします。
2. アカウントにプリンシパルとしてログインしたら、適切な権限と信頼関係を持つ AWSControlTowerBlueprintAccess ロールを作成します。

AWSControlTowerBlueprintAccess ロールは、次の 2 つのプリンシパルに信頼を付与するように設定する必要があります。

- AWS Control Tower 管理アカウントで AWS Control Tower を実行するプリンシパル (ユーザー)。
- AWS Control Tower 管理アカウントの AWSControlTowerAdmin という名前のロール。

次に信頼ポリシーの例を示します。これは、ロールに含める必要があるポリシーと似ています。このポリシーは、最小特権アクセスの付与のベストプラクティスを示しています。独自のポリシーを作成する場合は、*YourManagementAccountId* を AWS Control Tower 管理アカウントの実際のアカウ
ント ID で置き換え、*YourControlTowerUserRole* を管理アカウントの IAM ロールの識別子で置
き換えます。

JSON

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

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:role/service-role/
AWSControlTowerAdmin",
        "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
      ]
    },
    "Action": "sts:AssumeRole"
  }
]
```

必要なアクセス許可ポリシー

AWS Control Tower では、AWSServiceCatalogAdminFullAccess という名前の管理ポリシーを AWSControlTowerBlueprintAccess ロールにアタッチする必要があります。このポリシーは、AWS Control Tower がポートフォリオと AWS Service Catalog 製品リソースを管理できるようにするときに AWS Service Catalog が探すアクセス許可を提供します。このポリシーは、IAM コンソールでロールを作成するときにアタッチできます。

追加のアクセス許可が必要な場合があります

- ブループリントを Amazon S3 に保存する場合、AWS Control Tower には AWSControlTowerBlueprintAccess ロールの AmazonS3ReadOnlyAccess アクセス許可ポリシーも必要です。
- デフォルトの管理者ポリシーを使用しない場合、AWS Service Catalog Terraform タイプの製品では、AFC カスタム IAM ポリシーにいくつかのアクセス許可を追加する必要があります。Terraform テンプレートで定義するリソースを作成するために必要なアクセス許可に加えて、これらが必要です。

ステップ 2. AWS Service Catalog 製品を作成する

AWS Service Catalog 製品を作成するには、「AWS Service Catalog 管理者ガイド」の「[製品の作成](#)」のステップに従います。AWS Service Catalog 製品を作成するときに、アカウントのブループリントをテンプレートとして追加します。

⚠ Important

HashiCorp が Terraform ライセンスを更新した結果、Terraform Open Source 製品とプロビジョニング済み製品のサポートが External という新しい製品タイプ AWS Service Catalog に変更されました。この変更が AFC に与える影響の詳細 (既存のアカウントのブループリントを External 製品タイプに更新する方法など) については、「[External 製品タイプへの移行](#)」を参照してください。

ブループリントを作成する手順の概要

- アカウントのブループリントとなる CloudFormation テンプレートまたは Terraform tar.gz 設定ファイルを作成またはダウンロードします。いくつかのテンプレートの例については、このセクションの後半に示します。
- Account Factory ブループリント AWS アカウント を保存する にサインインします (ハブアカウントと呼ばれることもあります)。
- AWS Service Catalog コンソールに移動します。次に、[Product list] (製品リスト) を選択し、[Upload new product] (新しい製品をアップロード) を選択します。
- [Product details] (製品詳細) ペインに、名前や説明など、ブループリント製品の詳細を入力します。
- [Use a template file] (テンプレートファイルの使用)、[Choose file] (ファイルの選択) の順に選択します。ブループリントとして使用するために作成またはダウンロードしたテンプレートや設定ファイルを選択または貼り付けます。
- コンソールページの下部にある [Create product] (製品を作成する) を選択します。

テンプレートは、AWS Service Catalog リファレンスアーキテクチャリポジトリ CloudFormation からダウンロードできます。[そのリポジトリの例は、リソースのバックアッププランを設定するのに役立ちます。](#)

以下は、Best Pets という架空の会社向けのテンプレートの例です。これは、ペットのデータベースへの接続を設定するのに役立ちます。

Resources:

```
ConnectionStringGeneratorLambdaRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
```

```

    Version: "2012-10-17"
    Statement:
      - Effect: Allow
        Principal:
          Service:
            - lambda.amazonaws.com
        Action:
          - "sts:AssumeRole"
ConnectionStringGeneratorLambda:
  Type: AWS::Lambda::Function
  Properties:
    FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]
    Description: Retrieves the connection string for this account to access the Pet
Database
    Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
    Runtime: nodejs22.x
    Handler: index.handler
    Timeout: 5
    Code:
      ZipFile: >
        export const handler = async (event, context) => {
          const awsAccountId = context.invokedFunctionArn.split(":")[4]
          const connectionString= "fake connection for account " + awsAccountId;
          const response = {
            statusCode: 200,
            body: connectionString
          };
          return response;
        };

ConnectionString:
  Type: Custom::ConnectionStringGenerator
  Properties:
    ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

PetDatabaseConnectionString:
  DependsOn: ConnectionString
  # For example purposes we're using SSM parameter store.
  # In your template, use secure alternatives to store
  # sensitive values such as connection strings.
  Type: AWS::SSM::Parameter
  Properties:
    Name: pet-database-connection-string

```

Description: Connection information for the BestPets pet database
Type: String
Value: !GetAtt ConnectionString.Value

ステップ 3. カスタムブループリントを確認する

ブループリントは AWS Service Catalog コンソールで表示できます。詳細については、「Service Catalog 管理者ガイド」の「[製品の管理](#)」を参照してください。

ステップ 4. ブループリントを呼び出して、カスタマイズされたアカウントを作成する

AWS Control Tower コンソールの[Create account] (アカウントの作成) ワークフローに従うと、オプションのセクションが表示され、アカウントのカスタマイズに使用できるブループリントに関する情報を入力できます。

前提条件

カスタマイズするハブアカウントを設定し、ブループリント (Service Catalog 製品) を少なくとも 1 つ追加してから、その情報を AWS Control Tower コンソールに入力して、カスタマイズされたアカウントのプロビジョニングを開始する必要があります。

AWS Control Tower コンソールで、カスタマイズされたアカウントを作成または更新します。

1. ブループリントを含んでいるアカウントのアカウント ID を入力します。
2. そのアカウントから、既存の Service Catalog 製品 (既存のブループリント) を選択します。
3. 複数のバージョンのブループリント (Service Catalog 製品) がある場合は、適切なバージョンを選択します。
4. (オプション) プロセスのこの時点で、ブループリントプロビジョニングポリシーを追加または変更できます。ブループリントプロビジョニングポリシーは、JSON で記述され、IAM ロールにアタッチされている場合、ブループリントテンプレートで指定されたリソースをプロビジョニングします。AWS Control Tower は、Service Catalog が CloudFormation スタックセットを使用してリソースをデプロイできるように、メンバーアカウントにこのロールを作成します。ロールの名前は AWSControlTower-BlueprintExecution-bp-**xxxx** です。デフォルトでは、AdministratorAccess ポリシーがここに適用されます。
5. このブループリントに基づいてアカウントをデプロイする AWS リージョン または リージョンを選択します。

6. ブループリントにパラメータが含まれている場合は、パラメータの値を AWS Control Tower ワークフローの追加フィールドに入力できます。追加する値には、GitHub リポジトリ名、GitHub ブランチ、Amazon ECS クラスター名、およびリポジトリ所有者の GitHub ID が含まれる場合があります。
7. ハブアカウントまたはブループリントの準備がまだ整っていない場合は、アカウントの更新プロセスに従って後からアカウントをカスタマイズできます。

詳細については、[ブループリントからカスタマイズされたアカウントを作成する](#)を参照してください。

ブループリントからカスタマイズされたアカウントを作成する

カスタムブループリントを作成すると、AWS Control Tower の Account Factory でカスタムアカウントの作成を開始できます。

新しい AWS アカウントを作成するときにカスタムブループリントをデプロイするには、次の手順に従います。

1. の AWS Control Tower に移動します AWS マネジメントコンソール。
2. [Account Factory] と [Create account] (アカウントの作成) を選択します。
3. アカウント名や E メールアドレスなどのアカウントの詳細を入力します。
4. E メールアドレスとユーザー名で IAM Identity Center の詳細を設定します。
5. アカウントが追加される登録済みの OU を選択します。
6. [Account Factory Customization] セクションを展開します。
7. Service Catalog 製品が含まれているブループリントハブアカウントのアカウント ID を入力し、[Validate] (検証) を選択します。ブループリントハブアカウントの詳細については、「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。
8. Service Catalog 製品リスト (すべてのカスタムブループリント、パートナーブループリント) から、すべてのブループリントが含まれているドロップダウンメニューを選択します。ブループリントと対応するバージョンを選択してデプロイします。
9. ブループリントにパラメータが含まれている場合は、これらのフィールドが表示されて入力できます。事前にデフォルト値が入力されています。
10. 最後に、ブループリントをデプロイする場所を [Home Region] (ホームリージョン) または [All governed Regions] (すべての管理対象リージョン) から選択します。Route 53 や IAM な

どのグローバルリソースは、単一のリージョンのみにデプロイする必要がある場合があります。Amazon EC2 インスタンスや Amazon S3 バケットなどのリージョン別リソースは、すべての管理対象リージョンにデプロイできます。

11. すべてのフィールドに入力したら、[Create account] (アカウントの作成) を選択します。

Note

Terraform で作成されたブループリントは 1 つのリージョンにのみデプロイでき、複数のリージョンにはデプロイできません。

アカウントプロビジョニングの進捗状況は、[Organization] (組織) ページで確認できます。アカウントのプロビジョニングが完了すると、ブループリントで指定されたリソースはすでにそのアカウント内にデプロイされています。アカウントとブループリントの詳細を表示するには、[Account details] (アカウント詳細) ページに移動します。

登録時に AFC を使用してアカウントをカスタマイズする

以下は、AWS Control Tower コンソールで、アカウントを登録およびカスタマイズする方法を示しています。

1. AWS Control Tower コンソールに移動し、左側のナビゲーションから [Organization] (組織) を選択します。
2. 使用可能なアカウントのリストが表示されます。カスタムブループリントを使用して登録するアカウントを特定します。そのアカウントの [State] (状態) 列に、[Not enrolled] (未登録) ステータスのアカウントが反映されています。
3. アカウントの左側にあるラジオボタンを選択し、画面右上の [Actions] (アクション) ドロップダウンメニューを選択します。ここで、[Enroll] (登録) オプションを選択します。
4. [Access configuration] (アクセス設定) セクションにアカウントの IAM Identity Center 情報を入力します。
5. アカウントがメンバーとなる登録済みの OU を選択します。
6. アカウント作成手順の 7~12 と同じ手順を使用して、[Account Factory Customization] (Account Factory のカスタマイズ) セクションを完了します。詳細については、[「Account Factory アカウントをプロビジョニング AWS Service Catalogする」](#)を参照してください。

アカウントの進捗状況は、[Organization] (組織) ページで確認できます。アカウントの登録が完了すると、ブループリントで指定されたリソースはすでにそのアカウント内にデプロイされています。

ブループリントを AWS Control Tower アカウントに追加する

既存の AWS Control Tower メンバーアカウントにブループリントを追加するには、AWS Control Tower コンソールの [Update account] (アカウントの更新) ワークフローに従い、アカウントに追加する新しいブループリントを選択します。詳細については、「[AWS Control Tower または AWS Service Catalog で Account Factory アカウントを更新して移動する](#)」を参照してください。

Note

アカウントに新しいブループリントを追加すると、既存のブループリントは上書きされます。

Note

AWS Control Tower アカウントごとに 1 つのブループリントをデプロイできます。

ブループリントを更新する

以下の手順では、カスタムブループリントの更新方法とデプロイ方法について説明します。

カスタムブループリントを更新するには

1. CloudFormation テンプレートまたは Terraform tar.gz ファイル (ブループリント) を新しい設定で更新します。
2. 更新したブループリントを新しいバージョンとして AWS Service Catalog に保存します。

更新したブループリントをデプロイするには

1. AWS Control Tower コンソールの [Organization] (組織) ページに移動します。
2. [Organization] (組織) ページをブループリント名とバージョンでフィルタリングします。
3. アカウントの更新プロセスに従い、アカウントに最新バージョンのブループリントをデプロイします。

ブループリントの更新に失敗した場合

AWS Control Tower では、プロビジョニングされた製品が AVAILABLE 状態になると、ブループリントを更新できます。プロビジョニングされた製品が TAINTED 状態である場合、更新は失敗します。次の回避策を推奨します。

1. AWS Service Catalog コンソールで、TAINTEDプロビジョニング済み製品を手動で更新して、状態を に変更しますAVAILABLE。詳細については、「[プロビジョニングされた製品の更新](#)」を参照してください。
2. 次に、AWS Control Tower のアカウント更新プロセスに従って、ブループリントのデプロイエラーを修正します。

この手動ステップを推奨する理由は、次のとおりです。ブループリントを削除すると、メンバーアカウントのリソースが削除される可能性があります。リソースの削除は、既存のワークロードに影響する場合があります。このため、特に実稼働ワークロードを実行している場合には、ブループリントを更新する別の方法 (元のブループリントを削除して置換する) ではなく、この方法をお勧めします。

アカウントからブループリントを削除する

アカウントからブループリントを削除するには、アカウントの更新ワークフローに従ってブループリントを削除し、アカウントを AWS Control Tower のデフォルト設定に戻します。

コンソールでアカウントの更新ワークフローを開始すると、アカウントの詳細がすべて入力されます。カスタマイズの詳細は入力されません。これらの AFC の詳細を空白のままにすると、AWS Control Tower ではアカウントからブループリントが削除されます。このとき、アクションが開始される前に、警告メッセージが表示されます。

Note

AWS Control Tower は、アカウントの作成またはアカウントの更新プロセス中にブループリントを選択した場合にのみ、ブループリントをアカウントに追加します。

パートナーのブループリント

AWS Control Tower Account Factory Customization (AFC) は、AWS パートナーによって構築および管理される事前定義されたカスタマイズブループリントへのアクセスを提供します。このようなパートナーブループリントは、特定のユースケースに合わせてアカウントをカスタマイズするのに役立ち

ます。各パートナーのブループリントは、特定のパートナーからの製品提供と連携するように事前に設定してカスタマイズされたアカウントの作成に役立ちます。

AWS Control Tower のパートナーのブループリントの完全なリストを表示するには、コンソールで Service Catalog の「入門ライブラリ」に移動します。ソースタイプ [AWS Control Tower Blueprints] (AWS Control Tower ブループリント) を検索します。

Account Factory Customizations (AFC) に関する考慮事項

- AFC は、単一の AWS Service Catalog ブループリント製品を使用したカスタマイズのみをサポートしています。
- AWS Service Catalog ブループリント製品は、ハブアカウントと AWS Control Tower ランディングゾーンのホームリージョンと同じリージョンに作成する必要があります。
- AWSControlTowerBlueprintAccess IAM ロールは、適切な名前、権限、信頼ポリシーを使用して作成する必要があります。
- AWS Control Tower は、ホームリージョンのみにデプロイするか、またはAWS Control Tower によって管理されているすべてのリージョンにデプロイするかという 2 つのブループリントのデプロイオプションをサポートしています。リージョンの選択はできません。
- メンバーアカウントのブループリントを更新すると、ブループリントハブアカウント ID と AWS Service Catalog ブループリント製品を変更することはできません。
- AWS Control Tower では、1 回のブループリント更新操作で既存のブループリントの削除と新しいブループリントの追加を同時に行うことはできません。ブループリントを削除してから、別の操作で新しいブループリントを追加できます。
- AWS Control Tower は、作成または登録するアカウントがカスタマイズされているか、またはカスタマイズされていないかに基づいて動作を変更します。カスタマイズされたアカウントをブループリントを使用して作成または登録しない場合、AWS Control Tower は AWS Control Tower 管理アカウントで (Service Catalog を通じて)、Account Factory によってプロビジョニングされた製品を作成します。ブループリントを使用してアカウントを作成または登録する際にカスタマイズを指定する場合は、AWS Control Tower は AWS Control Tower 管理アカウントで、Account Factory でプロビジョニングされた製品を作成しません。

ブループリントエラーが発生した場合

ブループリントの適用中のエラー

新しいアカウント、または AWS Control Tower に登録している既存のアカウントのいずれの場合も、ブループリントをアカウントに適用する過程でエラーが発生した場合の復旧手順は同じです。アカウントは存在したままですが、カスタマイズされず、AWS Control Tower に登録されていません。続行するには、次の手順に従って、AWS Control Tower にアカウントを登録し、登録時にブループリントを追加します。

AWSControlTowerBlueprintAccess ロール作成中のエラーと回避策

AWS Control Tower アカウントから AWSControlTowerBlueprintAccess ロールを作成する場合、AWSControlTowerExecution ロールを使用してプリンシパルとしてサインインする必要があります。他のユーザーとしてサインインすると、次のアーティファクトに示すように、CreateRole オペレーションは SCP によって妨げられます。

```
{
  "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"
```

```
}
```

以下の回避策を使用できます。

- (最も推奨)AWSControlTowerExecution ロールを継承して、AWSControlTowerBlueprintAccess ロールを作成します。この回避策を選択した場合、リソースの意図しない変更を防ぐために、ロールの作成後すぐに AWSControlTowerExecution ロールからサインアウトしてください。
- AWS Control Tower に登録されていないため、この SCP の対象ではないアカウントにサインインします。
- この SCP を一時的に編集して、オペレーションを許可します。
- (あまり推奨しない) AWS Control Tower 管理アカウントをハブアカウントとして使用すると、SCP の対象になりません。

CloudFormation に基づく AFC ブループリント用のポリシードキュメントのカスタマイズ

Account Factory でブループリントを有効にすると、AWS Control Tower はユーザーに代わって StackSet を作成する CloudFormation ように指示します。は、StackSet にスタックを作成 CloudFormation するためにマネージドアカウントへのアクセス CloudFormation を必要とします。CloudFormation にはすでに AWSControlTowerExecutionロールを通じてマネージドアカウントの管理者権限がありますが、このロールは によって引き受けることはできません CloudFormation。

ブループリントの有効化の一環として、AWS Control Tower によってメンバーアカウントにロールが作成されます。このロールは CloudFormation によって継承され、StackSet の管理タスクが完了する場合があります。Account Factory を使用してカスタマイズ済みブループリントを有効にする最も簡単な方法は、allow-all ポリシーを使用することです。このようなポリシーはすべてのブループリントテンプレートと互換性があるためです。

ただし、ベストプラクティスでは、ターゲットアカウントの CloudFormation のアクセス許可を制限する必要があります。カスタマイズされたポリシーを提供できます。このポリシーは、AWS Control Tower が用いて作成するロールに適用 CloudFormation します。例えば、ブループリントによって something-important という名前の SSM パラメータが作成された場合、次のポリシーを指定できます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudFormationActionsOnStacks",
      "Effect": "Allow",
      "Action": "cloudformation:*",
      "Resource": "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid": "AllowSsmParameterActions",
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParameter",
        "ssm:GetParameters"
      ],
      "Resource": "arn:*:ssm:*:*:parameter/something-important"
    }
  ]
}
```

AllowCloudFormationActionsOnStacks ステートメントはすべての AFC カスタムポリシーに必要です。このロール CloudFormation を使用してスタックインスタンスを作成するため、スタックで CloudFormation アクションを実行するためのアクセス許可が必要です。AllowSsmParameterActions セクションは、有効になっているテンプレートに固有です。

権限に関する問題の解決

制限付きポリシーを使用してブループリントを有効にするとき、ブループリントを有効にする権限が不足していることがあります。このような問題を解決するには、ポリシードキュメントを改訂し、修正されたポリシーを使用するようにメンバーアカウントのブループリント設定を更新します。ポリシーがブループリントを有効にするのに十分であることを確認するには、CloudFormation アクセス許可が付与され、そのロールを使用してスタックを直接作成できることを確認します。

Terraform ベースの Service Catalog 製品の作成に必要な追加のアクセス許可

AFC の Terraform 設定ファイルを使用して AWS Service Catalog 外部製品を作成する場合、AWS Service Catalog では、テンプレートで定義されたリソースの作成に必要なアクセス許可に加えて、特定のアクセス許可を AFC カスタム IAM ポリシーに追加する必要があります。デフォルトのフル Admin ポリシーを選択した場合は、これらの追加のアクセス許可を追加する必要はありません。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "resource-groups:CreateGroup",
        "resource-groups:ListGroupResources",
        "resource-groups>DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "tag:GetResources",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
        }
      }
    }
  ]
}
```

```
}  
}  
}  
]  
}
```

の外部製品タイプを使用して Terraform 製品を作成する方法の詳細については AWS Service Catalog、「Service Catalog 管理者ガイド」の [「ステップ 5: 起動ロールを作成する」](#) を参照してください。

AWS Service Catalog 外部製品タイプへの移行

AWS Service Catalog は、Terraform Open Source 製品とプロビジョニング済み製品のサポートを External という新しい製品タイプに変更しました。この移行の詳細については、「AWS Service Catalog 管理者ガイド」の [「既存の Terraform オープンソース製品およびプロビジョニングされた製品から External 製品タイプへの更新」](#) を参照してください。

この変更は、AWS Control Tower アカウントファクトリーのカスタマイズを使用して作成または登録した既存のアカウントに影響します。これらのアカウントを External 製品タイプに移行するには、AWS Service Catalog と AWS Control Tower の両方で変更を行う必要があります。

新しい External 製品タイプに移行するには

1. 既存の Terraform リファレンスエンジンを にアップグレード AWS Service Catalog し、External 製品タイプと Terraform Open Source 製品タイプの両方のサポートを含めます。Terraform Reference Engine の更新方法については、[AWS Service Catalog GitHub リポジトリ](#) を参照してください。
2. で AWS Service Catalog、新しい External 製品タイプを使用して、既存の Terraform Open Source 製品 (ブループリント) を複製します。既存の Terraform Open Source ブループリントを削除しないでください。
3. AWS Control Tower で、Terraform オープンソースブループリントを使用している各アカウントを更新し、新しい External ブループリントを使用するようにします。
 - a. ブループリントを更新するには、まず Terraform オープンソースブループリントを完全に削除する必要があります。詳細については、「[アカウントからブループリントを削除する](#)」を参照してください。
 - b. 新しい External ブループリントを同じアカウントに追加します。詳細については、「[ブループリントを AWS Control Tower アカウントに追加する](#)」を参照してください。

4. Terraform Open Source ブループリントを使用するすべてのアカウントが外部ブループリントに更新されたら、Terraform Open Source を製品タイプとして使用する製品に戻って AWS Service Catalog 終了します。
5. 今後、AWS Control Tower アカウントファクトリーのカスタマイズを使用して作成または登録するすべてのアカウントは、CloudFormation または External 製品タイプを使用するブループリントを参照する必要があります。

External 製品タイプを使用して作成したブループリントの場合、AWS Control Tower は Terraform テンプレートと Terraform リファレンスエンジンを使用するアカウントのカスタマイズのみをサポートします。詳細については、「[カスタマイズのための設定](#)」を参照してください。

Note

AWS Control Tower は、新しいアカウントの作成時に Terraform オープンソースを製品タイプとしてサポートしていません。これらの変更の詳細については、AWS Service Catalog 管理者ガイドの「[既存の Terraform オープンソース製品とプロビジョニング済み製品を外部製品タイプに更新する](#)」を参照してください。AWS Service Catalog は、必要に応じてこの製品タイプの移行を通じてお客様をサポートします。アカウント担当者を通じて支援をリクエストしてください。

AWS Control Tower Account Factory for Terraform (AFT) によるアカウントのプロビジョニング

AWS Control Tower Account Factory for Terraform (AFT) は、AWS Control Tower でのアカウントプロビジョニングとアカウント更新のプロセスを自動化する GitOps モデルを採用します。

AFT では、AFT ワークフローを呼び出す入力を含むアカウントリクエスト Terraform ファイルを作成します。AFT のワークフローは、AFT のアカウントプロビジョニングフレームワークとアカウントカスタマイズステップを実行します。

AFT は、AWS Control Tower のワークフローパフォーマンスに影響しません。Account Factory または AFT によってアカウントをプロビジョニングした場合、同じバックエンドワークフローが発生します。

前提条件

Note

AFT アカウントプロビジョニングは、AWS Control Tower で AWSControlTowerBaseline が有効になっている組織単位 (OU) をターゲットにする必要があります。AWSControlTowerBaseline の詳細については、「」を参照してください[OU レベルで適用されるベースラインタイプ](#)。

AFT を開始するとき、次を作成します。

- AWS Control Tower で OU、次に AFT 環境の AFT 管理アカウントを作成します。アカウント ID をメモしておき、後で Terraform モジュールで AFT をデプロイするときに main.tf ファイルに入力できるようにします。このアカウント ID は、AWS Control Tower [コントロールの詳細] ページで確認できます。詳細については、「[Terraform のドキュメント](#)」を参照してください。
- 完全にデプロイされた AFT 環境内の 1 つ以上の git リポジトリ。詳細については、「[Post-deployment steps for AFT](#)」を参照してください。
- 完全にデプロイされた AFT 環境。詳細については、「[AWS Control Tower Account Factory for Terraform \(AFT\) の概要](#)」および「[AWS Control Tower Account Factory for Terraform \(AFT\) のデプロイ](#)」を参照してください。[Terraform のドキュメント](#)も参照してください。

Tip

[アカウントを作成] を使用して AWS Control Tower コンソールから AFT 管理アカウントを作成できます。詳細については、「[プロビジョニングの方法](#)」を参照してください。オプションで、aft-account-customizations リポジトリにアカウントテンプレートフォルダーを作成し、追加したアカウントを定義しやすくなります。

自動登録を介して登録されたアカウントの場合:

- AFT による新しいアカウントの作成は引き続き正常に機能します。
- 既存のアカウントのインポートには、追加のステップが必要です。
 - OU を登録して、インポートする前に必要なプロビジョニング済み製品を作成します。

- 登録 OU は イベント `CreateManagedAccount` と `UpdateManagedAccount` イベントを出力し、AFT のカスタマイズを有効にします。

AFT にデプロイの制限 AWS リージョン がある場所については、[AWS Control Tower の制限とクォータ](#)「」および「」を参照してください[コントロールの制限事項](#)。

[Terraform のドキュメント](#)には、AWS Control Tower Account Factory for Terraform (AFT) を設定する方法の概要が含まれています。

AWS Control Tower Account Factory for Terraform (AFT) の概要

Account Factory for Terraform (AFT) は、AWS Control Tower でアカウントのプロビジョニングとカスタマイズに役立つ Terraform パイプラインを設定します。AFT は、お客様のアカウントの AWS Control Tower を管理できるようにしながら、Terraform ベースのアカウントプロビジョニングの利点を提供するように設計されています。

AFT でアカウントリクエスト Terraform ファイルを作成して、アカウントプロビジョニングの AFT ワークフローをトリガーするために必要な入力を取得します。アカウントのプロビジョニング段階が完了すると、AFT はアカウントのカスタマイズ段階が始まる前に一連のステップを自動的に実行します。詳細については、「[AFT アカウントプロビジョニングパイプライン](#)」を参照してください。

AFT は、Terraform Cloud、Terraform Enterprise、Terraform Community Edition をサポートしています。AFT では、入力ファイルと簡単な `git push` コマンドを使用してアカウントの作成を開始したり、新規または既存のアカウントをカスタマイズしたりできます。アカウントの作成には、AWS Control Tower ガバナンスに関するすべてのメリット、および組織の標準的なセキュリティ手順とコンプライアンスガイドラインを満たすのに役立つアカウントのカスタマイズが含まれます。

AFT はアカウントのカスタマイズリクエストの追跡をサポートしています。アカウントのカスタマイズリクエストを送信するたびに、AFT は AFT カスタマイズ AWS Step Functions ステートマシンを通過する一意のトレーストークンを生成し、実行の一部としてトークンをログに記録します。その後、Amazon CloudWatch Logs Insights クエリを使用してタイムスタンプを範囲指定して検索し、リクエストトークンを取得できます。その結果、トークンに関連付けられたペイロードを確認し、AFT ワークフロー全体を通じてアカウントカスタマイズリクエストを追跡することができます。CloudWatch Logs と Step Functions の詳細については、以下を参照してください。

- Amazon CloudWatch Logs ユーザーガイドの「[Amazon CloudWatch Logs とは](#)」
- 「AWS Step Functions デベロッパーガイド」の「[AWS Step Functions の概要](#)」

AFT は [コンポーネントサービス](#)、他の AWS サービスの機能を として組み合わせ、Terraform Infrastructure as Code (IaC) をデプロイするパイプラインを使用してフレームワークを構築します。AFT により、次のことが可能になります。

- GitOps モデルでアカウントプロビジョニングと更新リクエストを送信する
- アカウントのメタデータと監査履歴を保存する
- アカウントレベルのタグを適用する
- すべてのアカウント、一連のアカウント、または個々のアカウントにカスタマイズを追加する
- 機能オプションの有効化

AFT は、AFT 管理アカウントと呼ばれる別のアカウントを作成して、AFT 機能をデプロイします。AFT を設定する前に、既存の AWS Control Tower ランディングゾーンが必要です。AFT 管理アカウントは、AWS Control Tower 管理アカウントと同じではありません。

AFT が提供する柔軟性

- プラットフォームに対する柔軟性: AFT は、Community Edition、Cloud、Enterprise の初期デプロイおよび継続的な運用のための Terraform ディストリビューションをサポートしています。
- バージョン管理システムの柔軟性: AFT は をサポートし AWS CodeCommit、 を介した代替バージョン管理ソースをサポートします AWS CodeConnections。

AFT が提供する機能オプション

ベストプラクティスに基づいて、いくつかの機能オプションを有効にできます。

- データイベントをログ記録するための組織レベルの CloudTrail の作成
- アカウントの AWS デフォルト VPC の削除
- プロビジョニングされたアカウントを AWS エンタープライズサポートプランに登録する

Note

AFT パイプラインは、アカウントがアプリケーションの実行に必要とするリソース (Amazon EC2 インスタンスなど) をデプロイするためのものではありません。AWS Control Tower アカウントの自動プロビジョニングとカスタマイズのみを目的としています。

動画チュートリアル

このビデオ (7:33) では、AWS Control Tower Account Factory for Terraform を使用してアカウントをデプロイする方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower での自動アカウントプロビジョニングに関する動画チュートリアル。](#)

AFT アーキテクチャ

オペレーションの順序

AFT 管理アカウントで AFT オペレーションを実行します。完全なアカウントプロビジョニングワークフローの場合、図表の左から右に示されているステージの順序は次のとおりです。

1. アカウントリクエストが作成され、パイプラインに送信されます。一度に複数のアカウントリクエストを作成して送信できます。Account Factory は、先入れ先出しの順序でリクエストを処理します。詳細については、「[複数のアカウントリクエストを送信する](#)」を参照してください。
2. 各アカウントがプロビジョニングされます。このステージは AWS Control Tower 管理アカウントで実行されます。
3. グローバルカスタマイズは、発行された各アカウントごとに作成されたパイプラインで実行されます。
4. 最初のアカウントプロビジョニングリクエストでカスタマイズが指定されている場合、カスタマイズは対象アカウントでのみ実行されます。アカウントが既にプロビジョニングされている場合は、そのアカウントのパイプラインでさらにカスタマイズを手動で開始する必要があります。

AWS Control Tower Account Factory for Terraform – アカウントのプロビジョニングワークフロー

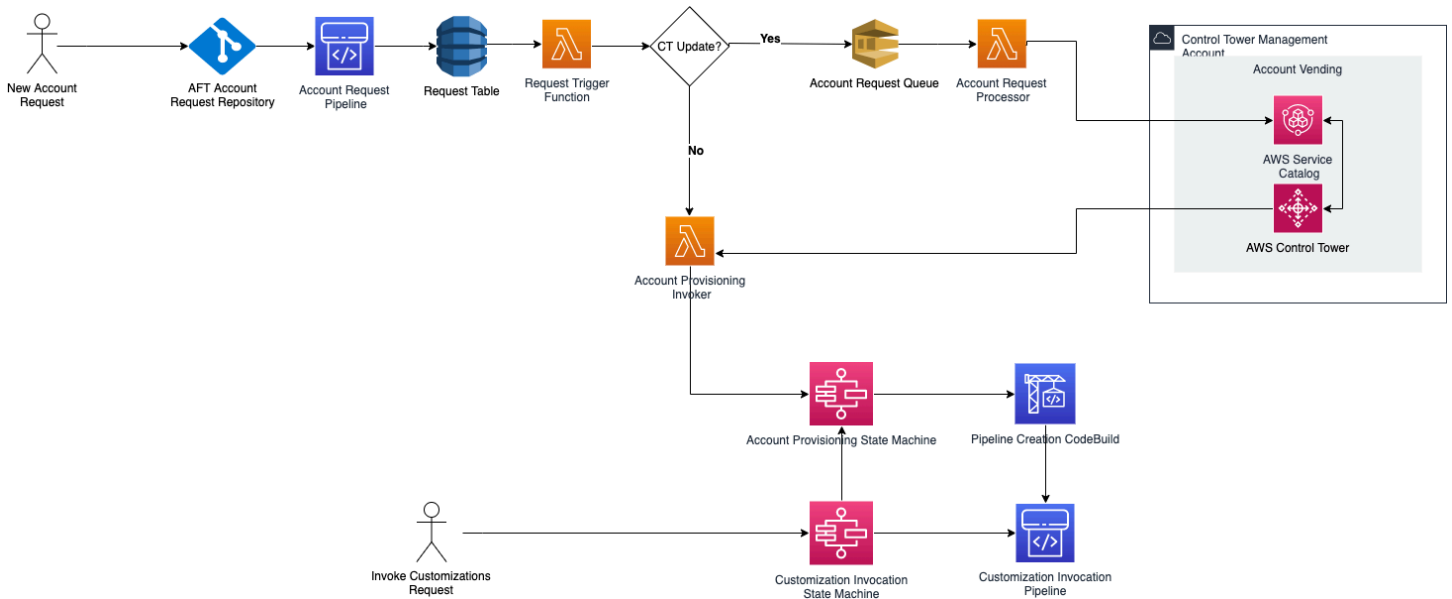


図 1: AWS Control Tower Account Factory for Terraform

Cost

AFT に伴う追加料金はありません。AFT によってデプロイされたリソース、AFT によって有効化された AWS サービス、および AFT 環境にデプロイされたリソースに対してのみ料金が発生します。

デフォルトの AFT 設定には、データ保護とセキュリティを強化するための AWS PrivateLink エンドポイントの割り当て、および AWS CodeBuild のサポートに必要な NAT ゲートウェイが含まれます。このインフラストラクチャの料金の詳細については、[AWS PrivateLink の料金](#)と [NAT ゲートウェイの Amazon VPC の料金](#)を参照してください。これらのコストの管理の詳細については、AWS アカウント担当者にお問い合わせください。AFT のこれらのデフォルト設定は変更できます。

AWS Control Tower Account Factory for Terraform (AFT) のデプロイ

このセクションは、既存の環境で Account Factory for Terraform (AFT) を設定する AWS Control Tower 環境の管理者を対象としています。ここでは、新しい専用の AFT 管理アカウントを使用して、Account Factory for Terraform (AFT) 環境を設定する方法について説明します。

Note

Terraform モジュールは AFT をデプロイします。このモジュールは GitHub の [AFT リポジトリ](#)で入手可能で、AFT リポジトリ全体がモジュールと見なされます。

AFT リポジトリのクローンを作成する代わりに、GitHub の AFT モジュールを参照することをお勧めします。これにより、モジュールが利用可能になったときにその更新を管理して使用することができます。

AWS Control Tower Account Factory for Terraform (AFT) 機能の最新リリースの詳細については、この GitHub リポジトリの [リリースファイル](#) を参照してください。

デプロイの前提条件

AFT 環境を設定して起動する前に、次のリソースが利用可能であることが必要です。

- AWS Control Tower ランディングゾーンのホームリージョン。詳細については、「[AWS Control Tower で AWS リージョン を使用する方法](#)」を参照してください。
- AWS Control Tower ランディングゾーン。詳細については、「[AWS Control Tower のランディングゾーンを計画する](#)」を参照してください。
- AFT 管理アカウント。AWS Control Tower または他の方法でプロビジョニングして AWS Control Tower に登録することができます。
- Terraform のバージョンとディストリビューション。詳細については、「[Terraform と AFT のバージョン](#)」を参照してください。
- コードやその他のファイルへの変更を追跡および管理するための VCS プロバイダー。デフォルトでは、AFT は AWS CodeCommit を使用します。詳細については、「AWS CodeCommit ユーザーガイド」の「[What is AWS CodeCommit?](#)」を参照してください。

AFT を初めてデプロイする場合に、既存の CodeCommit リポジトリがないときは、GitHub や BitBucket などの外部 VCS プロバイダーを選択する必要があります。詳細については、「[Alternatives for version control of source code in AFT](#)」を参照してください。

- AFT をインストールする Terraform モジュールを実行できるランタイム環境。
- AFT 機能のオプション。詳細については、「[機能オプションを有効にする](#)」を参照してください。

AWS Control Tower Account Factory for Terraform を設定して起動する

以下の手順は、Terraform のワークフローに精通していることを前提としています。AFT のデプロイの詳細については、AWS Workshop Studio ウェブサイトの「[AFT 入門ラボ](#)」を参照してください。

ステップ 1: AWS Control Tower ランディングゾーンを起動する

「[AWS Control Tower の開始方法](#)」のステップを完了します。ここで、AWS Control Tower 管理アカウントを作成し、AWS Control Tower ランディングゾーンを設定します。

 Note

AdministratorAccess 認証情報を持つ AWS Control Tower 管理アカウントのロールを必ず作成してください。詳細については次を参照してください:

- 「AWS Identity and Access Management IAM ユーザーガイド」の「[IAM ID \(ユーザー、ユーザーグループ、ロール\)](#)」
- 「AWS マネージドポリシーリファレンスガイド」の「[AdministratorAccess](#)」

ステップ 2: AFT の新しい組織単位を作成する (強く推奨)

AWS Control Tower ランディングゾーンに別の OU を作成することをお勧めします。この OU に AFT 管理アカウントをプロビジョニングします。AWS Control Tower 管理アカウントから新しい OU と AFT 管理アカウントを作成します。詳細については、「[新しい OU を作成する](#)」を参照してください。

ステップ 3: AFT 管理アカウントをプロビジョニングする

AFT では、AFT 管理オペレーション専用の AWS アカウントをプロビジョニングする必要があります。AWS Control Tower ランディングゾーンに関連付けられている AWS Control Tower 管理アカウントにサインインしているときに、AFT 管理アカウントを作成します。AWS Control Tower コンソールから AFT 管理アカウントをプロビジョニングするには、[組織] ページで [アカウントを作成] を選択するか、他の方法を選択します。詳細については、[AWS Service Catalog 「Account Factory でアカウントをプロビジョニングする」](#)を参照してください。

 Note

AFT 用に別の OU を作成した場合は、AFT 管理アカウントを作成するときに必ずこの OU を選択してください。

AFT 管理アカウントを完全にプロビジョニングするには、最大 30 分かかる場合があります。

ステップ 4: Terraform 環境がデプロイに使用可能であることを検証する

このステップは、Terraform の使用経験があり、Terraform を実行するための手順を適切に行っていることを前提としています。詳細については、HashiCorp Developer ウェブサイトの「[Command: init](#)」を参照してください。

Note

AFT は Terraform バージョン 1.6.0 以降をサポートしています。

ステップ 5: オプション 設定

- オプションで仮想プライベートクラウド (VPC) 設定を設定する

AFT モジュールには、AWS Control Tower が中央 AFT 管理アカウントの VPC 内にアカウントリソースをプロビジョニングするかどうかを指定する `aft_enable_vpc` パラメータが含まれています。デフォルトでは、パラメータは `true` に設定されています。このパラメータを `false` に設定すると、AWS Control Tower は VPC やプライベートネットワークリソース (NAT ゲートウェイや VPC エンドポイントなど) を使用せずに AFT をデプロイします。`aft_enable_vpc` を無効にすると、一部の使用パターンで AFT の運用コストを削減できる場合があります。VPC 設定を追加すると、`false` に設定されている `aft_enable_vpc` パラメータが上書きされます。

Note

`aft_enable_vpc` パラメータを再度有効にする (値を `false` から `true` に切り替える) には、`terraform apply` コマンドを 2 回連続して実行する必要があります。

新しい VPC をプロビジョニングする代わりに、アカウント内の既存の VPC を使用するように AFT を設定できます。独自の VPC を使用するには、次の VPC 設定パラメータを指定します。

- `aft_customer_vpc_id` - 既存の VPC の ID
- `aft_customer_private_subnets` - VPC 内のプライベートサブネット ID のリスト

設定例:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # VPC configuration
```



```
aft_customer_vpc_id = "vpc-0123456789abcdef0"
aft_customer_private_subnets = ["subnet-0123456789abcdef0",
"subnet-0123456789abcdef1"]

# Other AFT parameters...
}
```

Important

既存の AFT デプロイがある場合は、カスタム VPC オプションを使用することはお勧めしません。基盤となる既存の VPC 内のリソースに応じて、Lambda 関数または CodePipeline との依存関係がある場合があります。

- オプションで Terraform プロジェクト名を設定する

terraform_project_name パラメータを設定することで、AFT で使用される Terraform プロジェクト名をカスタマイズできます。デフォルトでは、AFT はデプロイを Terraform Cloud または Terraform Enterprise の「デフォルト」プロジェクトに配置します。

設定例:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Project name configuration
  terraform_project_name = "my-organization-aft"

  # Other AFT parameters...
}
```

Note

このパラメータは、Terraform Enterprise または Terraform Cloud のデプロイにのみ適用されます。

- オプションで AFT リソースにカスタムタグを適用する

tags パラメータを使用して、すべての AFT リソースにカスタムタグを適用できます。これらのタグは、リソースの整理、コスト配分、アクセスコントロールに役立ちます。

設定例:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Custom tags configuration
  tags = {
    Environment = "Production"
    CostCenter  = "IT-12345"
    Project     = "AFT-Deployment"
    Owner       = "platform-team@example.com"
  }

  # Other AFT parameters...
}
```

これらのタグは、AFT モジュールによって作成されたすべてのリソースに適用されます。AFT は、カスタムタグで上書きできない `managed_by = "AFT"` タグを自動的にすべてのリソースに追加します。

 Note

カスタムタグは、最初のデプロイ中だけでなく、いつでも追加できます。

- 必要に応じて、AWS KMS カスタマーマネージド暗号化キー (CMK) を CloudWatch ロググループと SNS トピックに適用する

ロググループと SNS トピックの KMS CMK 暗号化を有効化するには、`cloudwatch_log_group_enable_cmk_encryption` と `sns_topic_enable_cmk_encryption` の変数を設定します。

これらの設定をオプトインすると、AFT は既存の CMK、`alias/aft` を使用して CloudWatch ログと SNS トピックを暗号化します。この CMK は、AFT が AFT 管理アカウントにデプロイされたときに作成され、ロググループと SNS トピックに適用されます。

- 変数 `cloudwatch_log_group_enable_cmk_encryption` が `true` に設定されている場合、AFT の CloudWatch ロググループは CMK を使用して暗号化されます。変数がデフォルト値である `false` に設定されている場合、ログは [CloudWatch ログのデフォルトによるサーバー側の暗号化](#) を使用して暗号化されます。
- 変数 `sns_topic_enable_cmk_encryption` が `true` に設定されている場合、AFT SNS トピック (`aft-notifications` および `aft-failure-notifications`) に送信される通知は、CMK を使用して暗号化されます。変数がデフォルト値である `false` に設定されている場合、SNS メッセージは AWS マネージドキー `alias/aws/sns` で暗号化されます。詳細については、「[SSE の重要な用語](#)」を参照してください。
- オプションで CodeBuild コンピューティングタイプを変更する

デプロイ中に、AFT が CodeBuild に使用するコンピューティングタイプを変更するには、変数 `aft_codebuild_compute_type` を設定します。

受け入れられるコンピューティングタイプの詳細については、「[オンデマンド環境のタイプについて](#)」を参照してください。デフォルトのコンピューティングタイプは `BUILD_GENERAL1_MEDIUM` です。

- オプションで Terraform の OpenID Connect (OIDC) を設定する

Terraform Enterprise または HCP Terraform (以前の Terraform Cloud) を使用しているお客様は、OIDC プロトコル上に構築された Terraform のワークロード ID トークン (または動的プロバイダー認証情報) を使用して、AFT でワークスペースを安全に接続および認証できます。

`terraform_oidc_integration` パラメータを `true` に設定することで、AFT ワークスペースの OIDC 統合を有効にできます。デフォルトでは、このパラメータは `false` に設定されます。このパラメータを有効にする場合、デフォルト (`aws.workload.identity` `terraform_oidc_aws_audience` と) が環境と一致しない場合は `app.terraform.io`、および `terraform_oidc_hostname` パラメータを確認して設定する必要があります。

設定例:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Terraform distribution must be "tfc" or "tfe" for OIDC
  terraform_distribution = "tfc"

  # Terraform OIDC Configuration
```

```
terraform_oidc_integration = true
terraform_oidc_aws_audience = "aws.workload.identity" # default
terraform_oidc_hostname     = "app.terraform.io"       # default; set to your TFE
hostname if applicable

# Other AFT parameters...
}
```

Note

このパラメータは、Terraform Enterprise または HCP Terraform デプロイにのみ適用されます。

Note

現在、AFT 管理アカウントで Terraform の OIDC プロバイダーを利用している場合は、この統合にオプトインする前にそのプロバイダーを削除する必要があります。AFT は、デプロイ時にそのプロバイダーを再作成します。

ステップ 6: Account Factory for Terraform モジュールを呼び出して AFT をデプロイする

AdministratorAccess 認証情報を持つ AWS Control Tower 管理アカウント用に作成したロールで、AFT モジュールを呼び出します。AWS Control Tower は、AWS Control Tower 管理アカウントを通じて、AWS Control Tower Account Factory リクエストをオーケストレーションするために必要なすべてのインフラストラクチャを確立する Terraform モジュールをプロビジョニングします。

GitHub の [AFT リポジトリ](#) で AFT モジュールを表示できます。GitHub リポジトリ全体が AFT モジュールと見なされます。AFT モジュールの実行と AFT のデプロイに必要な入力については、[README ファイル](#) を参照してください。または、[Terraform レジストリ](#) で AFT モジュールを表示することもできます。

環境で Terraform を管理するために確立されたパイプラインを持っている場合は、この AFT モジュールを既存のワークフローに統合できます。それ以外の場合は、必要な認証情報で認証された環境から AFT モジュールを実行します。

タイムアウトするとデプロイが失敗します。(AWS Security Token Service STS) 認証情報を使用して、完全なデプロイに十分なタイムアウトを確保することをお勧めします。AWS STS 認証情報の

最小タイムアウトは 60 分です。詳細については、「AWS Identity and Access Management ユーザーガイド」の「[IAM の一時的な認証情報](#)」を参照してください。

Note

AFT が Terraform モジュールを使用してデプロイを完了するまで最大 30 分かかる場合があります。

ステップ 7: Terraform 状態ファイルを管理する

AFT をデプロイすると、Terraform 状態ファイルが生成されます。このアーティファクトは、Terraform が作成したリソースの状態を記述します。AFT バージョンを更新する予定がある場合は、必ず Terraform 状態ファイルを保存するか、Amazon S3 と DynamoDB を使用して Terraform バックエンドをセットアップします。AFT モジュールはバックエンドの Terraform 状態を管理しません。

Note

Terraform 状態ファイルを保護するのはユーザーの責任です。一部の入力変数には、プライベートの ssh キーまたは Terraform トークンなどの機密値が含まれる場合があります。デプロイ方法によって、これらの値は Terraform 状態ファイルにプレーンテキストとして表示されることがあります。詳細については、HashiCorp ウェブサイトの「[Sensitive data in State](#)」を参照してください。

デプロイ後のステップ

AFT インフラストラクチャのデプロイが完了したら、次の追加ステップに従って設定プロセスを完了し、アカウントをプロビジョニングする準備を整えます。

ステップ 1: 目的の VCS プロバイダーとの CodeConnection を完了する

サードパーティーの VCS プロバイダーを選択した場合、AFT によって CodeConnection が確立されるので、その CodeConnection を確認します。希望する VCS を使用して AFT を設定する方法については、「[AFT での代替のソースコードバージョン管理](#)」を参照してください。

AWS CodeStar 接続を確立する最初のステップは、AFT によって行われます。接続を確認する必要があります。

ステップ 2: 各リポジトリを設定する

AFT では、次の [4 つのリポジトリ](#) を管理する必要があります。

1. アカウントリクエスト — このリポジトリは、アカウントリクエストの配置または更新を処理します。[使用可能な例](#)。AFT アカウントリクエストの詳細については、「[AFT による新しいアカウントのプロビジョニング](#)」を参照してください。
2. AFT アカウントプロビジョニングのカスタマイズ — このリポジトリは、グローバルカスタマイズステージを開始する前に、AFT で作成され、管理されるすべてのアカウントに適用されるカスタマイズを管理します。[使用可能な例](#)。AFT アカウントプロビジョニングのカスタマイズを作成するには、「[AFT アカウントプロビジョニングのカスタマイズのステートマシンを作成する](#)」を参照してください。
3. グローバルカスタマイズ — このリポジトリは、AFT で作成され、管理されるすべてのアカウントに適用されるカスタマイズを管理します。[使用可能な例](#)。AFT グローバルカスタマイズを作成するには、「[グローバルカスタマイズの適用](#)」を参照してください。
4. アカウントのカスタマイズ — このリポジトリは、AFT で作成され、管理される特定のアカウントにのみ適用されるカスタマイズを管理します。[使用可能な例](#)。AFT アカウントのカスタマイズを作成するには、「[アカウントカスタマイズの適用](#)」を参照してください。

AFT は、これらの各リポジトリが特定のディレクトリ構造に従うことを期待しています。リポジトリの入力に使用されるテンプレート、およびそれらのテンプレートの設定方法については、[AFT GitHub リポジトリ](#) の Account Factory for Terraform モジュールで入手できます。

AFT による新しいアカウントのプロビジョニング

このセクションでは、AFT と AFT 管理アカウントをすでに設定しており、追加のアカウントをプロビジョニングしていることを前提としています。

AFT で新しいアカウントをプロビジョニングするには、アカウントリクエストの Terraform ファイルを作成します。このファイルには、aft-account-request リポジトリ内のパラメータの入力が含まれています。アカウントリクエストの Terraform ファイルを作成したら、git push を実行してアカウントリクエストの処理を開始します。このコマンドは、`ct-aft-account-request` オペレーションを呼び出します。これは AWS CodePipeline、アカウントのプロビジョニングが完了した後に AFT 管理アカウントで作成されます。詳細については、「[AFT アカウントプロビジョニングパイプライン](#)」を参照してください。

アカウントリクエスト Terraform ファイルのパラメータ

アカウントリクエストの Terraform ファイルには、次のパラメータを含める必要があります。[アカウントリクエストの Terraform ファイルの例](#)は GitHub で確認できます。

- `module name` の値は、AWS アカウント リクエストごとに一意である必要があります。
- `module source` の値は、AFT が提供するアカウントリクエスト Terraform モジュールへのパスです。
- `control_tower_parameters` の値は、AWS Control Tower アカウントの作成に必要な入力をキャプチャします。値には次の入力フィールドが含まれます。
 - `AccountEmail`
 - `AccountName`
 - `ManagedOrganizationalUnit`
 - `SSOUserEmail`
 - `SSOUserFirstName`
 - `SSOUserLastName`

Note

`control_tower_parameters` に対して入力した内容は、アカウントのプロビジョニング中に変更することはできません。

`aft-account-request` リポジトリの `ManagedOrganizationalUnit` の指定にサポートされている形式には、`OUnitName` および `OUnitID` (OU-ID) があります。

- `account_tags` は、ビジネス基準 AWS アカウント に従ってタグ付けできるユーザー定義のキーと値をキャプチャします。詳細については、AWS Organizations ユーザーガイドの [AWS Organizations リソースへのタグ付け](#)を参照してください。
- `change_management_parameters` の値には、アカウントリクエストが作成された理由やアカウントリクエストを開始したユーザーなどの追加情報が含まれます。値には次の入力フィールドが含まれます。
 - `change_reason`
 - `change_requested_by`

- `custom_fields` は、`/aft/account-request/custom-fields/` で発行されたアカウントに SSM パラメータとしてデプロイするキーと値を持つ追加メタデータをキャプチャします。アカウントのカスタマイズ中にこのメタデータを参照すると、適切なコントロールをデプロイできます。例えば、規制コンプライアンスの対象となるアカウントは、追加の をデプロイする場合があります AWS Config ルール。 `custom_fields` で収集したメタデータは、アカウントのプロビジョニングおよび更新中に追加の処理を引き起こす可能性があります。アカウントリクエストからカスタムフィールドを削除すると、そのカスタムフィールドは発行されたアカウントの SSM パラメータストアから削除されます。
- (オプション) `account_customizations_name` は、`aft-account-customizations` リポジトリ内のアカウントテンプレートフォルダをキャプチャします。詳細については、「[アカウントのカスタマイズ](#)」を参照してください。

複数のアカウントリクエストの送信

AFT はアカウントリクエストを 1 つずつ処理しますが、AFT パイプラインには複数のアカウントリクエストを送信できます。AFT パイプラインに複数のアカウントリクエストを送信すると、AFT はアカウントリクエストを先入れ先出しの順序でキューに入れ、処理します。

Note

AFT がプロビジョニングするアカウントごとに 1 つのアカウントリクエスト Terraform ファイルを作成することも、1 つの Terraform ファイルに複数のリクエストをカスケードすることもできます。

既存のアカウントの更新

⚠ 自動登録の互換性

組織で自動登録を使用して自動アカウント登録を行う場合、AFT にはこれらのアカウントのインポートに関する制限があることに注意してください。自動登録を通じて登録されたアカウントには、AFT のインポートワークフローに必要な Service Catalog でプロビジョニングされた製品がありません。

回避策: OU の登録機能を使用して、自動的に登録されたアカウントのプロビジョニング済み製品を作成します。これにより、AFT のカスタマイズに必要なライフサイクルイベントが可能になります。

以前に送信されたアカウントリクエストを更新するして `git push` を実行することで、AFT がプロビジョニングしたアカウントを更新できます。このコマンドは、アカウントプロビジョニングワークフローを起動し、アカウント更新リクエストを処理できます。ManagedOrganizationalUnit の入力を更新できます。これは `control_tower_parameters` に必要な値の一部です。

ManagedOrganizationalUnit は、すべての `control_tower_parameters` の中で唯一の更新可能なパラメータです。ただし、`custom_fields` など、アカウントリクエストの Terraform ファイルに含まれるその他のパラメータは更新できます。詳細については、「[AFT による新しいアカウントのプロビジョニング](#)」を参照してください。

例えば、AFT アカウントの名前または E メールアドレスを更新するには、アカウントリクエストファイルで `custom_fields` として詳細を定義できます。このように、グローバルカスタマイズ中に `aws_account_alternate_contact` リソースに渡すことができる SSM パラメータを作成します。

```
resource "aws_account_alternate_contact" "operations" {

  alternate_contact_type = "OPERATIONS"

  name          = "Example"
  title         = "Example"
  email_address = "someone@example.com"
  phone_number  = "+1234567890"
}
```

オペレーションやセキュリティなど、他の問い合わせタイプにも同様のフィールドを追加できます。グローバルカスタマイズで、各カスタムフィールドのデータルックアップを追加して、アカウントリクエストで作成したすべてのフィールドを検索できるようにします。

```
data "aws_ssm_parameter" "billing_name" {
  name = "/aft/account-request/custom-fields/billing_name"
}

data "aws_ssm_parameter" "billing_title" {
  name = "/aft/account-request/custom-fields/billing_title"
}

data "aws_ssm_parameter" "billing_email_address" {
  name = "/aft/account-request/custom-fields/billing_email_address"
}
```

```
data "aws_ssm_parameter" "billing_phone_number" {
  name = "/aft/account-request/custom-fields/billing_phone_number"
}
```

最後に、グローバルカスタマイズファイルでも、代替連絡先リソースを作成します。アカウントリクエストで作成した連絡先のタイプごとに、次のいずれかのブロックを定義する必要があります。

```
resource "aws_account_alternate_contact" "billing" {

  alternate_contact_type = "BILLING"

  name          = data.aws_ssm_parameter.billing_name.value
  title         = data.aws_ssm_parameter.billing_title.value
  email_address = data.aws_ssm_parameter.billing_email_address.value
  phone_number  = data.aws_ssm_parameter.billing_phone_number.value
}
```

Note

`control_tower_parameters` に対して入力した内容は、アカウントのプロビジョニング中に変更することはできません。
`aft-account-request` リポジトリの `ManagedOrganizationalUnit` の指定にサポートされている形式には、`OUName` および `OUID` (OU-ID) があります。

AFT がプロビジョニングしていないアカウントを更新する

AFT の外部で作成された AWS Control Tower アカウントを更新するには、`aft-account-request` リポジトリにアカウントを指定します。

Note

すべてのアカウントの詳細が正しく、AWS Control Tower 組織およびそれぞれの AWS Service Catalog プロビジョニング済み製品と一致していることを確認します。

AFT AWS アカウント で既存の を更新するための前提条件

- は AWS Control Tower に登録 AWS アカウント する必要があります。
- は AWS Control Tower 組織の一部 AWS アカウント である必要があります。

Terraform と AFT バージョン

Account Factory for Terraform (AFT) は、Terraform バージョン 1.6.0 以降をサポートしています。次の例に示すように、AFT デプロイプロセスの入力パラメータとして Terraform のバージョンを指定する必要があります。

```
terraform_version = "1.6.0"
```

Terraform ディストリビューション

AFT は、次の 3 つの Terraform ディストリビューションをサポートしています。

- Terraform Community Edition
- Terraform Cloud
- Terraform Enterprise

これらのディストリビューションについては、以降のセクションで説明します。AFT ブートストラッププロセス中に、選択した Terraform ディストリビューションを入力パラメータとして指定します。AFT デプロイと入力パラメータの詳細については、「[AWS Control Tower Account Factory for Terraform \(AFT\) のデプロイ](#)」を参照してください。

Terraform Cloud または Terraform Enterprise ディストリビューションを選択した場合、`terraform_token` に指定する [API トークン](#) は、ユーザーまたはチーム API トークンである必要があります。組織トークンは、すべての必須 API でサポートされているわけではありません。セキュリティ上の理由から、次の例に示すように [terraform 変数](#) を割り当てることによって、このトークンの値をバージョン管理システム (VCS、Version Control System) にチェックインしないようにする必要があります。

```
# Sensitive variable managed in Terraform Cloud:  
terraform_token = var.terraform_cloud_token
```

Terraform Community Edition

ディストリビューションとして Terraform Community Edition を選択すると、AFT は AFT 管理アカウントで Terraform バックエンドを管理します。AFT は、AFT デプロイメントおよび AFT パイプラインフェーズ中に実行する、指定された Terraform バージョンの `terraform-cli` をダウンロード

します。結果の Terraform 状態設定は、次の形式の名前で Simple Storage Service (Amazon S3) バケットに格納されます。

```
aft-backend-[account_id]-primary-region
```

AFT は、災害対策のために、次の形式の名前で、別の AWS リージョンに Terraform 状態設定をレプリケートする Simple Storage Service (Amazon S3) バケットも作成します。

```
aft-backend-[account_id]-secondary-region
```

これらの Terraform 状態の Simple Storage Service (Amazon S3) バケットの削除機能に対しては、多要素認証 (MFA、Multi-Factor Authentication) を有効にすることをお勧めします。Terraform Community Edition の詳細については、[Terraform のドキュメント](#)を参照してください。

ディストリビューションとして Terraform OSS を選択するには、次の入力パラメータを指定します。

```
terraform_distribution = "oss"
```

Terraform Cloud

ディストリビューションとして Terraform Cloud を選択すると、AFT は Terraform Cloud 組織内に次のコンポーネントのワークスペースを作成し、API 駆動型のワークフローを開始します。

- アカウントリクエスト
- AFT がプロビジョニングしたアカウントの AFT カスタマイズ
- AFT がプロビジョニングしたアカウントのアカウントカスタマイズ
- AFT がプロビジョニングしたアカウントのグローバルカスタマイズ

Terraform Cloud が、結果の Terraform の状態設定を管理します。

ディストリビューションとして Terraform Cloud を選択するときは、次の入力パラメータを指定します。

- `terraform_distribution = "tfc"`
- `terraform_token` – このパラメータには、Terraform Cloud トークンの値が含まれます。AFT は、その値を機密としてマークし、AFT 管理アカウントの SSM パラメータストアに Secure String として保存します。会社のセキュリティポリシーとコンプライアンスガイドラインに従っ

て、Terraform トークンの値を定期的にローテーションすることをお勧めします。Terraform トークンは、ユーザーレベルまたはチームレベルの API トークンでなければなりません。組織トークンはサポートされていません。

- `terraform_org_name` — このパラメータには、Terraform Cloud 組織の名前が含まれます。

Note

単一の Terraform Cloud 組織で複数の AFT デプロイメントはサポートされていません。

Terraform Cloud の設定方法の詳細については、[Terraform のドキュメント](#)を参照してください。

Terraform Enterprise

ディストリビューションとして Terraform Enterprise を選択すると、AFT は Terraform Enterprise 組織内に次のコンポーネントのワークスペースを作成し、結果の Terraform の実行に対して API 駆動型のワークフローをトリガーします。

- アカウントリクエスト
- AFT によってプロビジョニングされたアカウントの AFT アカウントプロビジョニングカスタマイズ
- AFT によってプロビジョニングされたアカウントのアカウントカスタマイズ
- AFT によってプロビジョニングされたアカウントのグローバルカスタマイズ

結果の Terraform の状態設定は Terraform Enterprise セットアップによって管理されます。

ディストリビューションとして Terraform Enterprise を選択するには、次の入力パラメータを指定します。

- `terraform_distribution = "tfe"`
- `terraform_token` — このパラメータには、Terraform Enterprise トークンの値が含まれます。AFT は、その値を機密としてマークし、AFT 管理アカウントの SSM パラメータストアに `secure string` として保存します。会社のセキュリティポリシーとコンプライアンスガイドラインに従って、Terraform トークンの値を定期的にローテーションすることをお勧めします。
- `terraform_org_name` — このパラメータには、Terraform Enterprise 組織の名前が含まれます。
- `terraform_api_endpoint` — このパラメータには、Terraform Enterprise 環境の URL が含まれます。このパラメータの値は、次の形式であることが必要です。

```
https://{fqdn}/api/v2/
```

Terraform Enterprise の設定方法の詳細については、[Terraform のドキュメント](#)を参照してください。

AFT バージョンを確認する

デプロイした AFT のバージョンを確認するには、AWS SSM パラメータストアキーをクエリできます。

```
/aft/config/aft/version
```

レジストリメソッドを使用すると、バージョンをピン留めできます。

```
module "control_tower_account_factory" {  
  source = "aws-ia/control_tower_account_factory/aws"  
  version = "1.3.2"  
  # insert the 6 required variables here  
}
```

AFT バージョンの詳細については、[AFT リポジトリ](#)を参照してください。

AFT バージョンを更新する

AWS Control Tower 管理アカウントにサインインして、この AFT の更新を開始します。

デプロイした AFT のバージョンを更新するには、main リポジトリブランチからバージョンをプルできます。

```
terraform get -update
```

プルが完了したら、Terraform プランを再実行するか、[適用] を実行して AFT インフラストラクチャを最新の変更で更新できます。

機能オプションの有効化

AFT は、ベストプラクティスに基づいた機能オプションを提供します。AFT のデプロイ中に、機能フラグを使用して、これらの機能にオプトインできます。AFT 入力設定パラメータの詳細については、「[AFT による新しいアカウントのプロビジョニング](#)」を参照してください。

デフォルトでは、これらの機能は有効になっていません。環境でそれぞれの機能を明示的に有効にする必要があります。

トピック

- [AWS CloudTrail データイベント](#)
- [AWS エンタープライズサポートプラン](#)
- [AWS デフォルトの VPC を削除する](#)

AWS CloudTrail データイベント

有効にすると、AWS CloudTrail データイベントオプションによってこれらの機能が設定されます。

- CloudTrail の AWS Control Tower 管理アカウントに組織の証跡を作成します。
- Simple Storage Service (Amazon S3) および Lambda データイベントのログ記録をオンにします。
- AWS KMS 暗号化を使用して、すべての CloudTrail データイベントを暗号化し、AWS Control Tower Log Archive アカウントの `aws-aft-logs-*` S3 バケットにエクスポートします。
- [Log file validation] (ログファイルの検証) 設定をオンにします。

このオプションを有効にするには、AFT デプロイ入力設定で次の機能フラグを [True] に設定します。

```
aft_feature_cloudtrail_data_events
```

前提条件

この機能オプションを有効にする前に、の信頼されたアクセス AWS CloudTrail が組織で有効になっていることを確認してください。

CloudTrail の信頼されたアクセスのステータスを確認するには、次の手順に従います。

1. AWS Organizations コンソールに移動します。
2. [Services] (サービス) > [CloudTrail] を選択します。
3. 次に、必要に応じて、右上の [Enable trusted access] (信頼されたアクセスを有効にする) を選択します。

AWS CloudTrail コンソールを使用するように指示する警告メッセージが表示される場合がありますが、この場合は警告を無視してください。AFT は、信頼されたアクセスを許可した後、この機能オプションの有効化の一環として証跡を作成します。信頼されたアクセスが有効になっていない場合は、AFT がデータイベントの証跡を作成しようとしたときにエラーメッセージが表示されます。

Note

この設定は組織レベルで機能します。この設定を有効にすると、AFT によって管理されているかどうかにかかわらず AWS Organizations、のすべてのアカウントに影響します。有効化時の AWS Control Tower ログアーカイブアカウントのすべてのバケットは、Simple Storage Service (Amazon S3) データイベントから除外されます。CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

AWS エンタープライズサポートプラン

このオプションを有効にすると、AFT パイプラインは AFT によってプロビジョニングされたアカウントの AWS エンタープライズサポートプランを有効にします。

AWS アカウントには、デフォルトで AWS 基本サポートプランが有効になっています。AFT は、AFT がプロビジョニングするアカウントのエンタープライズサポートレベルへの自動登録を提供します。プロビジョニングプロセスにより、アカウントのサポートチケットが開き、AWS エンタープライズサポートプランへの追加がリクエストされます。

エンタープライズサポートオプションを有効にするには、AFT デプロイ入力設定で次の機能フラグを [True] に設定します。

```
aft_feature_enterprise_support=false
```

[AWS サポートプランの詳細については、「サポートプランの比較」](#)を参照してください。AWS

Note

この機能を使用するには、支払いアカウントを Enterprise Support プランに登録する必要があります。

AWS デフォルトの VPC を削除する

このオプションを有効にすると、AWS Control Tower リソースが にデプロイされていない場合でも AWS リージョン、AFT は AFT 管理アカウントとすべての AWS デフォルト VPCs を削除します AWS リージョン。

AFT は、AFT がプロビジョニングする AWS Control Tower アカウント、または AFT を介して AWS Control Tower に登録する既存の AWS アカウントについて、AWS デフォルトの VPCs を自動的に削除しません。

デフォルトでは AWS リージョン、各 に VPC が設定された新しい AWS アカウントが作成されます。エンタープライズには VPCs を作成するための標準プラクティスがある場合があります。そのため、特に AFT 管理アカウントでは、AWS デフォルトの VPC を削除し、有効にしないようにする必要があります。

このオプションを有効にするには、AFT デプロイ入力設定で次の機能フラグを [True] に設定します。

```
aft_feature_delete_default_vpcs_enabled
```

以下は、AFT デプロイの入力設定の例です。

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"
  ct_management_account_id    = var.ct_management_account_id
  log_archive_account_id      = var.log_archive_account_id
  audit_account_id            = var.audit_account_id
  aft_management_account_id   = var.aft_management_account_id
  ct_home_region               = var.ct_home_region
  tf_backend_secondary_region = var.tf_backend_secondary_region

  vcs_provider                = "github"
  account_request_repo_name    = "${var.github_username}/learn-terraform-aft-account-request"
  account_provisioning_customizations_repo_name = "${var.github_username}/learn-terraform-aft-account-provisioning-customizations"
  global_customizations_repo_name = "${var.github_username}/learn-terraform-aft-global-customizations"
  account_customizations_repo_name = "${var.github_username}/learn-terraform-aft-account-customizations"

  # Optional Feature Flags
```

```
aft_feature_delete_default_vpcs_enabled = true
aft_feature_cloudtrail_data_events      = false
aft_feature_enterprise_support          = false
}
```

デフォルト VPC の詳細については、「[Default VPC and default subnets](#)」(デフォルト VPC とデフォルトサブネット) を参照してください。

AWS Control Tower Account Factory for Terraform のリソースに関する考慮事項

AWS Control Tower Account Factory for Terraform を使用してランディングゾーンを設定すると、AWS アカウント内にいくつかのタイプの AWS リソースが作成されます。

リソースの検索

- タグを使用して、AFT リソースの最新リストを検索できます。検索のキーと値のペアは次のとおりです。

Key: managed_by | Value: AFT

- タグをサポートしないコンポーネントサービスの場合は、リソース名で aft を検索してリソースを特定できます。

Note

AFT は、管理アカウントに AWS Backup リソースを作成しません。

最初に作成されたリソースのテーブル (アカウント別)

AWS Control Tower Account Factory for Terraform 管理アカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTAdmin
		AWSAFTExecution
		AWSAFTService

AWS service	リソースタイプ	リソース名
		ct-aft-*
		aft-*
		codebuild_trigger_role
		python-layer-builder-aft-common-*
AWS Identity and Access Management	ポリシー	aft-*
CodeCommit	リポジトリ	aft-*
CodeBuild	ビルドプロジェクト	aft-*
		ct-aft-*
		python-layer-builder-aft-common-*
コードパイプライン	パイプライン	<i>YourAccountId</i> -customizations-pipeline
Simple Storage Service (Amazon S3)	バケット	aft-*
Lambda	関数	aft-*
Lambda	レイヤー	aft-common-*
DynamoDB	テーブル	aft-request
		aft-request-audit
		aft-request-metadata
		aft-controltower-events

AWS service	リソースタイプ	リソース名
Step Functions	ステートマシン	aft-account-provisioning-customizations aft-account-provisioning-framework aft-feature-options aft-invoke-customizations
VPC	VPC	aft-management-vpc
Amazon SNS	トピック	aft-notifications aft-failure-notifications
Amazon EventBridge	イベントバス	aft-events-from-ct-management
Amazon EventBridge	イベントルール	aft-account-provisioning-customizations-trigger aft-account-request-codepipeline-trigger aft-lambda-account-request-processor aft-controltower-event-logger
Key Management Service (KMS)	カスタマーマネージドキー	aft-backend-*-kms-key aft
AWS Systems Manager	パラメータストア	/aft/*
Amazon SQS	キュー	aft-account-request.fifo aft-account-request-dlg.fifo

AWS service	リソースタイプ	リソース名
CloudWatch	ロググループ	/aws/*/ct-aft-* /aws/*/aft-* /aws/codebuild/python-layer-builder-aft-common-*
AWS バックアップ	ボールド	aft-controltower-backup-vault
AWS バックアップ	プラン	aft-controltower-backup-plan
AWS サポートセンター (オプション)	サポートプラン	Enterprise

AWS AWS Control Tower Account Factory for Terraform を通じてプロビジョニングされたアカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecution
AWS サポートセンター (オプション)	サポートプラン	Enterprise

AWS Control Tower 管理アカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecution AWSAFTService aft-controltower-events-rule
AWS Systems Manager	パラメータストア	/aft/*

AWS service	リソースタイプ	リソース名
EventBridge	イベントルール	aft-capture-ct-events
CloudTrail (オプション)	追跡	aws-aft-CustomizationsCloud Trail
AWS Support Center (オプション)	サポートプラン	Enterprise

AWS Control Tower ログアーカイブアカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecution AWSAFTService
Key Management Service (KMS)	カスタマーマネージドキー	aft
Simple Storage Service (Amazon S3)	バケット	aws-aft-logs-* aws-aft-s3-access-logs-*
AWS サポートセンター (オプション)	サポートプラン	Enterprise

AWS Control Tower 監査アカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecution AWSAFTService
AWS サポートセンター (オプション)	サポートプラン	Enterprise

必要なロール

一般に、ロールとポリシーは AWS の Identity and Access Management (IAM) の一部です。詳細については、「[AWS IAM ユーザーガイド](#)」を参照してください。

AFT は、AFT パイプラインのオペレーションをサポートするために、AFT 管理アカウントと AWS Control Tower 管理アカウントに複数の IAM のロールとポリシーを作成します。これらのロールは、最小特権アクセスモデルに基づいて作成されます。このモデルは、各ロールおよびポリシーで最小限必要なアクションとリソースのセットに対する許可を制限します。これらのロールとポリシーには、識別 managed_by:AFT のために AWS タグ key:value ペアが割り当てられます。

これらの IAM ロールの他に、AFT は 3 つの重要な役割を作成します。

- AWSAFTAdmin ロール
- AWSAFTExecution ロール
- AWSAFTService ロール

これらのロールについては、以降のセクションで説明します。

AWSAFTAdmin ロールについての説明

AFT をデプロイすると、AWSAFTAdmin ロールが AFT 管理アカウントで作成されます。このロールにより、AFT パイプラインは、AWS Control Tower および AFT でプロビジョニングされたアカウントで AWSAFTExecution ロールを引き受けることができるため、アカウントのプロビジョニングとカスタマイズに関連するアクションを実行できます。

AWSAFTAdmin ロールにアタッチされたインラインポリシー (JSON アーティファクト) は次のとおりです。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
```

```

        "arn:aws:iam::*:role/AWSAFTExecution",
        "arn:aws:iam::*:role/AWSAFTService"
    ]
}

```

次の JSON アーティファクトは、AWSAFTAdmin ロールの信頼関係を示しています。プレースホルダー番号 012345678901 は、AFT 管理アカウント ID 番号に置き換えられます。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

AWSAFTExecution ロールについての説明

AFT をデプロイすると、AWSAFTExecution ロールが AFT 管理アカウントと AWS Control Tower 管理アカウントで作成されます。後ほど、AFT パイプラインが、AFT アカウントのプロビジョニング段階で、AFT でプロビジョニングされた各アカウントに AWSAFTExecution ロールを作成します。

AFT は、最初に AWSControlTowerExecution ロールを使用して、指定されたアカウントに AWSAFTExecution ロールを作成します。AWSAFTExecution ロールを使用すると、AFT パイプラインは、AFT でプロビジョニングされたアカウントと共有アカウントに対して、AFT フレームワークのプロビジョニングとプロビジョニングのカスタマイズの段階で実行されるステップを実行できます。

個別のロールは範囲を制限するのに役立つ

ベストプラクティスとして、カスタマイズ権限は、リソースの初期デプロイ時に許可されるアクセス許可とは別にしておきます。AWSAFTService ロールはアカウントのプロビジョニングを目的としており、AWSAFTExecution ロールは、アカウントのカスタマイズを目的としていることを忘れないようにしてください。この分離により、パイプラインの各フェーズで許可されるアクセス許可の範囲が制限されます。この区別は、AWS Control Tower の共有アカウントをカスタマイズする場合に特に重要です。共有アカウントには、請求の詳細やユーザー情報などの機密情報が含まれている場合があります。

AWSAFTExecution ロールのアクセス許可: AdministratorAccess – AWS マネージドポリシー

次の JSON アーティファクトは、AWSAFTExecution ロールにアタッチされた IAM ポリシー (信頼関係) を示しています。プレースホルダー番号 012345678901 は、AFT 管理アカウント ID 番号に置き換えられます。

AWSAFTExecution の信頼ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTService ロールについての説明

AWSAFTService ロールは、共有アカウントと管理アカウントを含むすべてのマネージドアカウントに AFT リソースをデプロイします。リソースは、以前は、AWSAFTExecution ロールによるみデプロイされていました。

AWSAFTService ロールは、プロビジョニング段階でリソースをデプロイするためにサービスインフラストラクチャで使用することを目的としており、AWSAFTExecution ロールは、カスタマイズのデプロイにのみ使用するためのものです。この方法でロールを引き受けると、各ステージでより詳細なアクセス制御を維持できます。

AWSAFTService ロールのアクセス許可: AdministratorAccess – AWS マネージドポリシー

次の JSON アーティファクトは、AWSAFTService ロールにアタッチされた IAM ポリシー (信頼関係) を示しています。プレースホルダー番号 012345678901 は、AFT 管理アカウント ID 番号に置き換えられます。

AWSAFTService の信頼ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

コンポーネントサービス

AFT をデプロイすると、コンポーネントはこれらの各AWSサービスからAWS環境に追加されます。

- [AWS Control Tower](#) - AFT は、AWS Control Tower 管理アカウントで AWS Control Tower Account Factory を使用して、アカウントをプロビジョニングします。
- [Amazon DynamoDB](#) - AFT は AFT 管理アカウントに Amazon DynamoDB テーブルを作成します。このテーブルには、アカウントリクエスト、アカウント更新の監査履歴、アカウントメタデータ、および AWS Control Tower ライフサイクルイベントが保存されます。AFT は、AFT アカウントプロビジョニングワークフローの開始など、ダウンストリームプロセスを開始するための DynamoDB Lambda トリガーも作成します。

- [Amazon Simple Storage Service](#) - AFT は、AFT 管理アカウントと AWS Control Tower ログアーカイブアカウントに Amazon Simple Storage Service (S3) バケットを作成し、AFT パイプラインが必要とするAWSサービスによって生成されたログを保存します。AFT は、プライマリとセカンダリに Terraform バックエンド S3 バケットを作成しAWS リージョン、AFT パイプラインワークフロー中に生成された Terraform 状態を保存します。
- [Amazon Simple Notification Service](#) - AFT は、AFT 管理アカウントに Amazon Simple Notification Service (SNS) トピックを作成します。このトピックには、すべての AFT アカウントリクエストの処理後に成功と失敗の通知が保存されます。任意のプロトコルを使用して、これらのメッセージを受信できます。
- [Amazon Simple Queue Service](#) - AFT は、AFT 管理アカウントに Amazon Simple Queue Service (Amazon SQS) FIFO キューを作成します。キューを使用すると、複数のアカウントリクエストを並行して送信できますが、順次処理する場合には AWS Control Tower Account Factory に一度に 1 つのリクエストを送信します。
- [AWS CodeBuild](#) - AFT は、AFT 管理アカウントに AWS CodeBuild ビルドプロジェクトを作成して、さまざまなビルドステージで AFT ソースコードの Terraform プランを初期化、コンパイル、テスト、および適用します。
- [AWS CodePipeline](#) - AFT は、AFT 管理アカウントに AWS CodePipeline パイプラインを作成して、AFT ソースコード用に選択したサポート対象の AWS CodeStar 接続プロバイダーと統合し、AWS CodeBuild でビルドジョブをトリガーします。
- [AWS Lambda](#) - AFT は、AFT 管理アカウントに AWS Lambda の関数とレイヤーを作成して、アカウントリクエスト、AFT アカウントプロビジョニング、およびアカウントカスタマイズの各プロセス中にステップを実行します。
- [AWS Systems Manager Parameter Store](#) - AFT は、AFT 管理アカウントに AWS Systems Manager Parameter Store をセットアップして、AFT パイプラインプロセスに必要な設定パラメータを保存します。
- [Amazon CloudWatch](#) - AFT は、AFT 管理アカウントに Amazon CloudWatch ロググループを作成して、AFT パイプラインで使用する AWS のサービスによって生成されたログを保存します。CloudWatch ログの保持期間は、Never Expire に設定されています。
- [Amazon VPC](#) - AFT は、セキュリティを強化するために、Amazon Virtual Private Cloud (VPC) を作成して、AFT 管理アカウントのサービスとリソースを個別のネットワーク環境に分離します。
- [AWS KMS](#) - AFT は、AFT 管理アカウントと AWS Control Tower ログアーカイブアカウントで AWS Key Management Service (KMS) を使用します。AFT は、Terraform の状態、DynamoDB テーブルに保存されるデータ、および SNS トピックを暗号化するためのキーを作成します。これらのログとアーティファクトは、AWS のリソースとサービスが AFT によってデプロイされたとき

に生成されます。AFT で作成された KMS キーは、デフォルトで 1 年ごとのローテーションが有効になっています。

- [AWS Identity and Access Management \(IAM\)](#) – AFT は、推奨される最小特権モデルに従います。これにより、AFT パイプラインワークフロー中に必要なアクションを実行するために、AFT 管理アカウント、AWS Control Tower アカウント、および AFT プロビジョニング済みアカウントに AWS Identity and Access Management (IAM) ロールとポリシーが必要に応じて作成されます。
- [AWS Step Functions](#) – AFT は、AFT 管理アカウントに AWS Step Functions ステートマシンを作成します。これらのステートマシンは、AFT アカウントプロビジョニングフレームワークおよびカスタマイズに必要なプロセスとステップをオーケストレートおよび自動化します。
- [Amazon EventBridge](#) – AFT は、AFT および AWS Control Tower 管理アカウントに Amazon EventBridge イベントバスを作成して、AWS Control Tower ライフサイクルイベントを AFT 管理アカウントの DynamoDB テーブルにキャプチャして長期間保存します。AFT は、AFT 管理アカウントと AWS Control Tower 管理アカウントに Amazon CloudWatch イベントルールを作成して、AFT パイプラインワークフローの実行中に必要な複数のステップをトリガーします。
- [AWS CloudTrail \(オプション\)](#) – この機能を有効にすると、AFT は Amazon S3 バケットと AWS Lambda 関数のデータイベントを記録するための AWS CloudTrail 組織の証跡を AWS Control Tower 管理アカウントに作成します。AFT は、これらのログを AWS Control Tower ログアーカイブアカウントで一元管理される S3 バケットに送信します。
- [AWS サポート \(オプション\)](#) – この機能を有効にすると、AFT は AFT によってプロビジョニングされたアカウントの AWS エンタープライズサポートプランを有効にします。デフォルトでは、AWS アカウントは AWS 基本サポートプランを有効にして作成されます。

AFT アカウントプロビジョニングパイプライン

パイプラインのアカウントプロビジョニングステージが完了した後も、AFT フレームワークは続行されます。これにより、一連のステップが自動的に実行され、[アカウントのカスタマイズ](#)ステージが開始される前に、新しくプロビジョニングされたアカウントに詳細が設定されるようになります。

次に、AFT パイプラインが実行される次のステップを示します。

1. アカウントリクエストの入力を検証します。
2. プロビジョニングされたアカウント (アカウント ID など) に関する情報を取得します。
3. アカウントメタデータを AFT 管理アカウントの DynamoDB テーブルに保存します。

4. 新しくプロビジョニングされたアカウントに [AWSAFTExecution] IAM ロールを作成します。AFT は、このロールが Account Factory ポートフォリオへのアクセスを許可するために、アカウントのカスタマイズステージを実行するこのロールを引き受けます。
5. アカウントリクエスト入力パラメータの一部として指定したアカウントタグを適用します。
6. AFT デプロイ時に選択した AFT 機能オプションを適用します。
7. 指定した AFT アカウントプロビジョニングのカスタマイズを適用します。次のセクションでは、git リポジトリで、AWS Step Functions ステートマシンを使用してこれらのカスタマイズを設定する方法の詳細について説明します。このステージは、アカウントプロビジョニングフレームワークステージと呼ばれることもあります。これはコアプロビジョニングプロセスの一部ですが、アカウントプロビジョニングワークフローの一部としてカスタマイズされた統合を提供するフレームワークをあらかじめ設定してから、次のステージで追加のカスタマイズをアカウントに追加します。
8. プロビジョニングされたアカウントごとに、AWS CodePipeline AFT 管理アカウントに が作成されます。これは (次のグローバル) [アカウントのカスタマイズ](#) ステージを実行するために実行されます。
9. プロビジョニングされた (およびターゲットの) アカウントごとに、アカウントカスタマイズパイプラインを呼び出します。
10. 成功または失敗の通知を SNS トピックに送信し、そこからメッセージを取得できます。

ステートマシンを使用したアカウントプロビジョニングフレームワークのカスタマイズの設定

アカウントをプロビジョニングする前に Terraform 以外のカスタム統合を設定した場合、これらのカスタマイズは AFT アカウントのプロビジョニングワークフローに含まれます。例えば、AFT によって作成されたすべてのアカウントがセキュリティ標準などの組織の標準やポリシーに準拠していることを確認するために、特定のカスタマイズが必要になる場合があります。これらの標準は、追加のカスタマイズの前にアカウントに追加できます。これらのアカウントプロビジョニングフレームワークのカスタマイズは、グローバルアカウントのカスタマイズステージが次に開始される前に、プロビジョニングされたすべてのアカウントに実装されます。

Note

このセクションで説明する AFT 機能は、AWS Step Functions の機能を理解している上級ユーザーを対象としています。代替として、アカウントのカスタマイズステージでグローバルヘルパーを操作することをお勧めします。

AFT アカウントプロビジョニングフレームワークは、ユーザーが定義した AWS Step Functions ステートマシンを呼び出して、カスタマイズを実装します。可能なステートマシン統合の詳細については、「[AWS Step Functions のドキュメント](#)」を参照してください。

一般的な統合を次に示します。

- 任意の言語での AWS Lambda 関数
- Docker コンテナを使用した、AWS ECS または AWS Fargate タスク
- AWS またはオンプレミスでホストされるカスタムワーカーを使用した AWS Step Functions アクティビティ
- Amazon SNS または SQS 統合

AWS Step Functions ステートマシンが定義されていない場合、ステージはノーオペレーションで渡されます。AFT アカウントプロビジョニングのカスタマイズのステートマシンを作成するには、[AFT アカウントプロビジョニングのカスタマイズのステートマシンを作成する](#)の手順に従います。カスタマイズを追加する前に、前提条件を満たしていることを確認してください。

これらのタイプの統合は AWS Control Tower の一部ではないため、AFT アカウントカスタマイズのグローバルな事前 API ステージの間は追加できません。代わりに、AFT パイプラインを使用して、プロビジョニングプロセスの一部としてこれらのカスタマイズを設定できます。これらは、プロビジョニングワークフローで実行されます。次のセクションで説明するように、AFT アカウントプロビジョニングステージを開始する前に、事前にステートマシンを作成して、これらのカスタマイズを実装する必要があります。

ステートマシンを作成するための前提条件

- AFT が完全にデプロイされていること。AFT デプロイの詳細については、「[AWS Control Tower Account Factory for Terraform \(AFT\) のデプロイ](#)」を参照してください。
- AFT アカウントプロビジョニングのカスタマイズのために、環境に git リポジトリを設定します。詳細については、「[デプロイ後のステップ](#)」を参照してください。

AFT アカウントプロビジョニングのカスタマイズのステートマシンを作成する

ステップ 1: ステートマシンの定義を変更する

例の `customizations.asl.json` ステートマシンの定義を変更します。この例は、[デプロイ後のステップ](#)において、AFT アカウントプロビジョニングのカスタマイズを保存するために設定した

git リポジトリで使用できます。ステートマシンの定義の詳細については、「[AWS Step Functions デベロッパーガイド](#)」を参照してください。

ステップ 2: 対応する Terraform 構成を含める

カスタム統合のためのステートマシンの定義を使用して、.tf 拡張子を持つ Terraform ファイルを同じ git リポジトリに含めます。例えば、ステートマシンのタスク定義で Lambda 関数を呼び出す場合は、lambda.tf ファイルを同じディレクトリに保存します。カスタム設定に必要な IAM ロールと許可を含めてください。

適切な入力を指定すると、AFT パイプラインは自動的にステートマシンを呼び出し、AFT アカウントプロビジョニングフレームワークステージの一部としてカスタマイズをデプロイします。

AFT アカウントプロビジョニングのフレームワークとカスタマイズを再開するには

AFT は、AFT パイプラインを介して発行されたすべてのアカウントについて、アカウントプロビジョニングのフレームワークとカスタマイズの手順を実行します。アカウントプロビジョニングのカスタマイズを再開するには、次の 2 つの方法のいずれかを使用できます。

1. アカウントリクエストリポジトリの既存のアカウントに変更を加えます。
2. AFT で新しいアカウントをプロビジョニングします。

アカウントのカスタマイズ

AFT は、プロビジョニングされたアカウントに標準の設定またはカスタマイズされた設定をデプロイできます。AFT 管理アカウントでは、AFT はアカウントごとに 1 つのパイプラインを提供します。このパイプラインを使用すると、すべてのアカウント、一組のアカウント、または個々のアカウントにカスタマイズを実装できます。Python スクリプト、bash スクリプト、および Terraform 設定を実行したり、アカウントカスタマイズステージの一部として AWS CLI を操作したりできます。

概要

選択した git リポジトリでカスタマイズを指定した後、グローバルカスタマイズを保存する場所またはアカウントカスタマイズを保存する場所のいずれかで、アカウントカスタマイズステージが AFT パイプラインによって自動的に完了します。アカウントを遡及的にカスタマイズするには、「[カスタマイズの再呼び出し](#)」を参照してください。

グローバルカスタマイズ (オプション)

AFT によってプロビジョニングされているすべてのアカウントに特定のカスタマイズを適用することもできます。例えば、特定の IAM ロールを作成する必要がある場合やすべてのアカウントにカスタムコントロールをデプロイする必要がある場合、AFT パイプラインのグローバルカスタマイズステージでその操作を自動的に行うことができます。

アカウントカスタマイズ (オプション)

AFT でプロビジョニングされた他のアカウントとは異なる個別のアカウント、または一組のアカウントをカスタマイズするには、AFT パイプラインのアカウントカスタマイズ部分を使用して、アカウント固有の設定を実装します。例えば、特定のアカウントでのみ、インターネットゲートウェイへのアクセスが必要になる場合があります。

カスタマイズの前提条件

アカウントのカスタマイズを開始する前に、次の前提条件が満たされていることを確認してください。

- AFT が完全にデプロイされていること。デプロイ方法については、「[AWS Control Tower Account Factory for Terraform を設定して起動する](#)」を参照してください。
- 環境内のグローバルカスタマイズおよびアカウントカスタマイズ用の git リポジトリに必要な情報が事前入力されていること。詳細については、「[デプロイ後のステップ](#)」の「ステップ 3: (必須) 各リポジトリを設定する」を参照してください。

グローバルカスタマイズの適用

グローバルカスタマイズを適用するには、選択したリポジトリに特定のフォルダ構造をプッシュする必要があります。

- カスタム設定が Python プログラムまたはスクリプトの形式である場合は、それらをリポジトリ内の [api_helpers/python] フォルダに配置します。
- カスタム設定が Bash スクリプトの形式である場合は、それらをリポジトリ内の [api_helpers] フォルダに配置します。
- カスタム設定が Terraform の形式である場合は、それらをリポジトリ内の [terraform] フォルダに配置します。
- カスタム設定の作成の詳細については、グローバルカスタマイズの README ファイルを参照してください。

Note

グローバルカスタマイズは、AFT パイプラインの AFT アカウントプロビジョニングフレームワークステージの後で自動的に適用されます。

アカウントカスタマイズの適用

選択したリポジトリに特定のフォルダ構造をプッシュすると、アカウントカスタマイズを適用できます。アカウントカスタマイズは、AFT パイプラインのグローバルカスタマイズステージの後で自動的に適用されます。アカウントカスタマイズリポジトリに、さまざまなアカウントカスタマイズを含む複数のフォルダを作成することもできます。必要なアカウントカスタマイズの実装ごとに、以下のステップを使用します。

アカウントカスタマイズを適用するには

1. ステップ 1: アカウントカスタマイズ用のフォルダを作成する

選択したリポジトリで、AFT が提供する ACCOUNT_TEMPLATE フォルダを新しいフォルダにコピーします。新しいフォルダの名前は、アカウントリクエストで指定した `account_customizations_name` と一致する必要があります。

2. 特定のアカウントカスタマイズフォルダの設定を追加する

設定の形式に基づいて、アカウントカスタマイズフォルダに設定を追加できます。

- カスタム設定が Python プログラムまたはスクリプトの形式である場合は、リポジトリ内にある **[`account_customizations_name`]/api_helpers/python** フォルダに配置します。
- カスタム設定が Bash スクリプトの形式である場合は、それらをリポジトリ内にある **[`account_customizations_name`]/api_helpers** フォルダに配置します。
- カスタム設定が Terraform の形式である場合は、それらをリポジトリ内の **[`account_customizations_name`]/terraform** フォルダに配置します。

カスタム設定の作成の詳細については、アカウントカスタマイズの README ファイルを参照してください。

3. アカウントリクエストファイルの特定の `account_customizations_name` パラメータを参照する

AFT アカ운トリクエストファイルには、入力パラメータ `account_customizations_name` が含まれています。このパラメータの値として、アカウントカスタマイズの名前を入力します。

Note

環境内のアカウントに対して複数のアカウントリクエストを送信できます。異なるまたは類似のアカウントカスタマイズを適用する場合は、アカウントリクエストの `account_customizations_name` 入力パラメータを使用してアカウントのカスタマイズを指定します。詳細については、「[複数のアカウントリクエストを送信する](#)」を参照してください。

カスタマイズの再呼び出し

AFT には、AFT パイプラインでカスタマイズを再呼び出しする方法が用意されています。この方法は、新しいカスタマイズステップを追加した場合や、既存のカスタマイズを変更する場合に便利です。再呼び出しすると、AFT によってカスタマイズパイプラインが開始されて、AFT でプロビジョニングされたアカウントに変更が加えられます。イベントソースベースの再呼び出しを使用すると、個々のアカウント、すべてのアカウント、OU に応じたアカウント、またはタグに従って選択されたアカウントにカスタマイズを適用できます。

AFT でプロビジョニングされたアカウントのカスタマイズを再呼び出しするには、次の 3 つのステップに従います。

ステップ 1: グローバルカスタマイズまたはアカウントカスタマイズの **git** リポジトリに変更をプッシュする

必要に応じてグローバルカスタマイズおよびアカウントカスタマイズを更新し、変更を git リポジトリに再度プッシュします。この時点では何も起こりません。次の 2 つのステップで説明するように、イベントソースによってカスタマイズパイプラインを呼び出す必要があります。

ステップ 2: カスタマイズを再呼び出しするための AWS Step Functions の実行を開始する

AFT では、AFT 管理アカウントに `aft-invoke-customizations` という AWS Step Functions が用意されています。この関数の目的は、AFT でプロビジョニングされたアカウントのカスタマイズパイプラインを再呼び出しすることです。

次に、`aft-invoke-customizations` AWS Step Functions に入力を渡すために作成できるイベントスキーマ (JSON 形式) の例を示します。

```
{
  "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"]
    }
  ]
}
```

このイベントスキーマの例に示すように、再呼び出しプロセスに対して含めたり除外したりするアカウントを選択できます。組織単位 (OU)、アカウントタグ、およびアカウント ID でフィルタリングできます。フィルターを適用せず、ステートメント "type": "all" を含めた場合は、AFT でプロビジョニングされたすべてのアカウントのカスタマイズが再呼び出しされます。

Note

AWS Control Tower Account Factory for Terraform (AFT) のバージョンが 1.6.5 以降の場合は、ネストされた OU を構文 OU Name (ou-id-1234) を使用してターゲットにできます。詳細については、次の [GitHub](#) に関するトピックを参照してください。

イベントパラメータを入力すると、Step Functions が実行され、対応するカスタマイズが呼び出されます。AFT では、一度に最大 5 つのカスタマイズを呼び出すことができます。Step Functions は、イベント条件に一致するすべてのアカウントが完了するまで待機してループします。

ステップ 3: AWS Step Functions の出力をモニタリングし、AWS CodePipeline の実行を監視する

- Step Functions で生成される出力には、Step Functions 入力イベントソースと一致するアカウント ID が含まれています。
- [Developer Tools] (開発者用ツール) の下にある AWS CodePipeline に移動して、アカウント ID に対応するカスタマイズパイプラインを表示します。

AFT アカウントカスタマイズリクエストの追跡によるトラブルシューティング

AWS Lambda に基づいてアカウントカスタマイズワークフローが出力するログには、ターゲットアカウント ID とカスタマイズリクエスト ID が含まれます。AFT では、カスタマイズリクエストに関連する CloudWatch Logs をターゲットアカウントまたはカスタマイズリクエスト ID でフィルタリングするために使用できる CloudWatch Logs Insights クエリを提供することで、Amazon CloudWatch Logs によるカスタマイズリクエストの追跡とトラブルシューティングを行うことができます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「[Amazon CloudWatch Logs を使用したログデータの分析](#)」を参照してください。

AFT で CloudWatch Logs Insights を使用するには

1. CloudWatch コンソールの <https://console.aws.amazon.com/cloudwatch/> を開いてください。
2. ナビゲーションペインで、[ログ]、[ログのインサイト] の順に選択します。
3. [クエリ] を選択します。
4. [サンプルクエリ] で [Account Factory for Terraform] を選択し、次のクエリのいずれかを選択します。

- アカウント ID 別のカスタマイズログ

Note

必ず **"YOUR-ACCOUNT-ID"** をターゲットアカウント ID に置き換えてください。

```
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/
```

- カスタマイズリクエスト ID 別のカスタマイズログ

Note

必ず **"YOUR-CUSTOMIZATION-REQUEST-ID"** をカスタマイズリクエスト ID に置き換えてください。カスタマイズリクエスト ID は、AFT アカウントプロビジョニングフレームワーク AWS Step Functions ステートマシンの出力にあります。AFT アカウントプロビジョニングフレームワークの詳細については、「[AFT アカウントプロビジョニングパイプライン](#)」を参照してください。

```
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. クエリを選択したら、必ず時間間隔を選択し、[クエリの実行] を選択します。

AFT での代替のソースコードバージョン管理

AFT はソースコードバージョン管理システム (VCS) AWS CodeCommit に を使用し、ビジネス要件または既存のアーキテクチャを満たす他の [CodeConnections](#) を許可します。

AFT を初めてデプロイする場合に、既存の CodeCommit リポジトリがないときは、AFT デプロイの前提条件の一部として外部 VCS プロバイダーを指定する必要があります。

AFT では、次のソースコード管理の代替方法がサポートされています。

- GitHub
- GitHub Enterprise Server
- Bitbucket
- GitLab
- GitLab セルフマネージド

 Note

VCS AWS CodeCommit として を指定した場合、追加のステップは必要ありません。AFT は、環境内に必要な git リポジトリ (デフォルト名を使用) を作成します。ただし、組織の標準に準拠するように、必要に応じて CodeCommit のデフォルトのリポジトリ名をオーバーライドすることができます。

AFT で代替のソースコードバージョン管理システム (カスタム VCS) を設定する

AFT デプロイ用の代替のソースコードバージョン管理システムを設定するには、次のステップに従います。

ステップ 1: サポートされているサードパーティーのバージョン管理システム (VCS、Version Control System) で **git** リポジトリを作成する

を使用していない場合は AWS CodeCommit、以下の項目について、AFT がサポートするサードパーティーの VCS プロバイダー環境で git リポジトリを作成する必要があります。

- AFT アカウントリクエスト。 [サンプルコードがあります](#)。AFT アカウントリクエストの詳細については、「[AFT による新しいアカウントのプロビジョニング](#)」を参照してください。
- AFT アカウントプロビジョニングのカスタマイズ。 [サンプルコードがあります](#)。AFT アカウントプロビジョニングのカスタマイズの詳細については、「[AFT アカウントプロビジョニングのカスタマイズのステートマシンを作成する](#)」を参照してください。
- AFT グローバルカスタマイズ。 [サンプルコードがあります](#)。AFT グローバルカスタマイズの詳細については、「[アカウントのカスタマイズ](#)」を参照してください。
- AFT アカウントのカスタマイズ。 [サンプルコードがあります](#)。AFT アカウントのカスタマイズの詳細については、「[アカウントのカスタマイズ](#)」を参照してください。

ステップ 2: AFT デプロイに必要な VCS 設定パラメータを指定する

AFT デプロイの一部として VCS プロバイダーを設定するには、次の入力パラメータが必要です。

- `vcs_provider`: を使用していない場合は AWS CodeCommit、ユースケースに基づいて VCS "bitbucket" "github"プロバイダーを "gitlab"、"githubenterprise"、またはとして指定します。
- `github_enterprise_url`: GitHub Enterprise の顧客のみを対象に、GitHub の URL を指定します。
- `account_request_repo_name`: AWS CodeCommit ユーザーの場合、この値は に設定されます `aft-account-request`。AFT でサポートされるサードパーティー VCS プロバイダー環境では、この入力値を実際のリポジトリ名で更新します。Bitbucket、GitHub、GitHub Enterprise、GitLab、および GitLab セルフマネージドの場合、リポジトリ名は `[Org]/[Repo]` という形式である必要があります。
- `account_customizations_repo_name`: AWS CodeCommit ユーザーの場合、この値は に設定されます `aft-account-customizations`。AFT でサポートされるサードパーティー VCS プロバイダー環境では、この入力値をお使いのリポジトリ名で更新します。Bitbucket、GitHub、GitHub Enterprise、GitLab、および GitLab セルフマネージドの場合、リポジトリ名は `[Org]/[Repo]` という形式である必要があります。
- `account_provisioning_customizations_repo_name`: AWS CodeCommit ユーザーの場合、この値は `aft-account-provisioning-customizations` に設定されます。AFT でサポートされるサードパーティー VCS プロバイダー環境では、この入力値をお使いのリポジトリ名で更新します。Bitbucket、GitHub、GitHub Enterprise、GitLab、および GitLab セルフマネージドの場合、リポジトリ名は `[Org]/[Repo]` という形式である必要があります。
- `global_customizations_repo_name`: AWS CodeCommit ユーザーの場合、この値は に設定されます `aft-global-customizations`。AFT でサポートされるサードパーティー VCS プロバイダー環境では、この入力値をお使いのリポジトリ名で更新します。Bitbucket、GitHub、GitHub Enterprise、GitLab、および GitLab セルフマネージドの場合、リポジトリ名は `[Org]/[Repo]` という形式である必要があります。
- `account_request_repo_branch`: ブランチはデフォルトで `main` ですが、この値はオーバーライドできます。

デフォルトでは、AFT のソースは各 git リポジトリの `main` ブランチです。ブランチ名の値は、追加の入力パラメータでオーバーライドできます。入力パラメータの詳細については、[AFT Terraform モジュール](#)の README ファイルを参照してください。

既存の AWS CodeCommit お客様向け

AFT 用に新しい名前で作成する場合は、これらの入力パラメータの値を更新することでリポジトリ名を更新できます。

ステップ 3: サードパーティーの VCS プロバイダー AWS CodeCommit の接続を完了する

デプロイを実行すると、AFT は必要な AWS CodeCommit リポジトリを作成するか、選択したサードパーティー VCS プロバイダー AWS CodeCommit の接続を作成します。後者の場合は、AFT 管理アカウントのコンソールに手動でサインインして、保留中の CodeCommit 接続を完了する必要があります。CodeCommit 接続を完了する詳細な手順については、「[AWS CodeCommit のドキュメント](#)」を参照してください。

AFT を AWS CodeCommit から別の VCS プロバイダーに移動する

このセクションでは、AWS Control Tower Account Factory for Terraform (AFT) をバージョン管理システム (VCS) として AWS CodeCommit から別の VCS プロバイダーに移動する方法の概要を説明します。

ステップ 1. 選択した VCS に新しいリポジトリを設定します。

ステップ 2. これらのリポジトリを新しいリモートとして git に追加します。

ステップ 3. 新しい VCS プロバイダーに git push を実行します。

Note

作成するリポジトリ構造は in AWS CodeCommit と同じである必要があります。構造を変更すると、AFT の目的のコードの実行に影響が出ます。

リポジトリ構造:

- aft-account-request
- aft-account-customizations
- aft-global-customizations
- aft-account-provisioning-customizations

Step 4. 次の例に示すように、AWS Control Tower 管理アカウントで、VCS プロバイダーを指すように Terraform モジュール (ブートストラップ) を更新します。

例: [GitLab と Terraform OSS](#)

- terraform plan を実行して変更をプレビューし、次に terraform apply を実行します。

ステップ 5. CodeConnection (以前は CodeStar と呼ばれていました) の設定を完了するには、各ステップを完了します。

1. AFT 管理アカウントにサインインする
2. 「保留中 [の接続の更新](#)」、またはコンソール「[\[\]](#)」の説明に従って、新しい VCS プロバイダーの [pendingCodeConnections](#) AWS CodeConnections を見つけて完了します <https://us-east-1.console.aws.amazon.com/codesuite/settings/connections>。AWS
3. リファレンス: 「[Post-deployment steps](#)」

Note

アカウントパイプラインは、aft-invoke-customizations ステップ関数が呼び出されるまで以前のソースを保持します。この呼び出しは、アップグレードの一部として、または次のカスタマイズ呼び出しの一部として実行できます。

詳細については、このブログ [AWS CodeCommit リポジトリを別の Git プロバイダーに移行する方法](#) を参照してください。

データ保護

AFT でのデータ保護には、[AWS 責任共有モデル](#)が適用されます。データ保護のため、セキュリティについては、次のベストプラクティスをお勧めします。

- AWS Control Tower で提供されるデータ保護ガイドラインに従ってください。詳細については、「[AWS Control Tower のデータ保護](#)」を参照してください。
- AFT デプロイ時に生成された Terraform 状態設定を保持します。詳細については、「[AWS Control Tower Account Factory for Terraform \(AFT\) のデプロイ](#)」を参照してください。
- 組織のセキュリティポリシーの指示に従って、機密性の高い認証情報を定期的にローテーションします。シークレットの例としては、Terraform トークン、git トークンなどがあります。

保管時の暗号化

AFT は、保管時に AWS Key Management Service キーで暗号化される Amazon S3 バケット、Amazon SNS トピック、Amazon SQS キュー、Amazon DynamoDB データベースを作成します。AFT で作成された KMS キーは、デフォルトで 1 年ごとのローテーションが有効になっています。Terraform の Terraform Cloud または Terraform Enterprise ディストリビューションを選択した場合、AFT には、機密性の高い Terraform トークン値を保存する AWS Systems Manager SecureString パラメータが含まれます。

AFT は、で説明 [コンポーネントサービス](#) されている AWS サービスを使用します。デフォルトでは、保管時に暗号化されます。詳細については、AFT の各コンポーネント AWS サービスの AWS ドキュメントを参照し、各サービスのデータ保護プラクティスについて説明します。

転送時の暗号化

AFT は、デフォルトで転送中の暗号化を使用する で説明 [コンポーネントサービス](#) されている AWS サービスに依存します。詳細については、AFT の各コンポーネント AWS サービスの AWS ドキュメントを参照し、各サービスのデータ保護プラクティスについて説明します。

Terraform Cloud または Terraform Enterprise ディストリビューションの場合、AFT は Terraform 組織にアクセスするための HTTPS エンドポイント API を呼び出します。AWS CodeStar 接続でサポートされているサードパーティーの VCS プロバイダーを選択した場合、AFT は HTTPS エンドポイント API を呼び出して VCS プロバイダー組織にアクセスします。

AFT からアカウントを削除する

このトピックでは、AFT からアカウントを削除して、AFT パイプラインでアカウントのデプロイと更新を停止する方法について説明します。

Important

AFT パイプラインからアカウントを削除すると、元に戻すことはできず、状態が失われる可能性があります。

AFT からアカウントを削除するのは、廃止したアプリケーションのアカウントを閉鎖する場合、漏洩したアカウントを隔離する場合、またはアカウントをある組織から別の組織に移動する場合です。

Note

AFT からアカウントを削除することは、AWS Control Tower アカウントまたは AWS アカウントを削除することと同じです。AFT からアカウントを削除しても、引き続き AWS Control Tower がアカウントを管理します。AWS Control Tower アカウントまたは を削除するには AWS アカウント、以下を参照してください。

- 「Control Tower ユーザーガイド」の「[Unmanage a member account](#)」(メンバーアカウントの管理を解除する)を参照してください。
- 「AWS Billing ユーザーガイド」の「[アカウントの解約](#)」

AFT パイプラインからアカウントを削除するには

AFT からアカウントを削除する手順を以下に説明します。

1. アカウントリクエストを保存する **git** リポジトリからアカウントを削除する

アカウントリクエストを保存する git リポジトリで、AFT から削除するアカウントのアカウントリクエストを削除します。

アカウントリクエストリポジトリからアカウントリクエストを削除すると、AFT はカスタマイズパイプラインとアカウントのメタデータを削除します。詳細については、GitHub の AFT の「[1.8.0 リリースノート](#)」を参照してください。

2. Terraform ワークスペースを削除する (Terraform Cloud および Terraform Enterprise のお客様のみ)

AFT から削除するアカウントのグローバルカスタマイズとアカウントカスタマイズのワークスペースを削除します。

3. Amazon S3 バックエンドから Terraform の状態を削除する

AFT 管理アカウントで、AFT から削除するアカウントの、Amazon S3 バケット内のすべての関連フォルダを削除します。

Tip

以下の例では、**012345678901** を AFT 管理アカウント ID 番号に置き換えます。

例: Terraform OSS

Terraform OSS を選択すると、aft-backend-**012345678901**-primary-region および aft-backend-**012345678901**-secondary-region Amazon S3 バケットに 3 つのフォルダがアカウントごとに表示されます。これらのフォルダは、カスタマイズパイプラインの状態、アカウントのカスタマイズ状態、およびグローバルカスタマイズ状態に関連しています

例: テラフォームクラウドまたはテラフォームエンタープライズ

Terraform Cloud または Terraform Enterprise を選択した場合、aft-backend-**012345678901**-primary-region および aft-backend-**012345678901**-secondary-region Amazon S3 バケットには、アカウントごとにフォルダがあります。これらのフォルダは、カスタマイズパイプラインの状態に関連しています。

運用メトリクス

デフォルトでは、Account Factory for Terraform (AFT) は匿名の運用メトリクスを AWS に送信します。このデータは、ソリューションの品質と機能を向上させる目的で、お客様が AFT をどのように使用しているかを理解するために使用されます。AFT のデプロイ中にパラメーターを変更することで、データ収集をオプトアウトできます。データ収集が有効になっていると、次のデータが AWS に送信されます。

- ソリューション: AFT 固有の識別子
- バージョン: AFT のバージョン
- UUID (Universally Unique Identifier): 個々の ATF のデプロイに対してランダムに生成された一意の識別子
- タイムスタンプ: データ収集タイムスタンプ
- データ: お客様が行った AFT の設定とアクション

収集したデータの所有権は AWS が有します。データ収集には、[AWS プライバシーポリシー](#)が適用されます。

Note

1.6.0 より前のバージョンの AFT では、使用量メトリクスは AWS にレポートされません。

レポートメトリクスをオプトアウトするには:

- 次の例に示すように、Terraform 入力設定ファイルで `aft_metrics_reporting` の入力値を `false` に設定し、AFT を再デプロイします。明示的に設定しない場合、この値は、デフォルトで `true` に設定されます。

例をコピーする場合は、x の部分の文字列を実際の ID とリージョン値で置き換えてください。

```
module "control_tower_account_factory" {
  source = "aws-ia/control_tower_account_factory/aws"

  # Required Vars
  ct_management_account_id      = "xxxxxxxxxxxx"
  log_archive_account_id       = "xxxxxxxxxxxx"
  audit_account_id             = "xxxxxxxxxxxx"
  aft_management_account_id     = "xxxxxxxxxxxx"
  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
}
```

Account Factory for Terraform (AFT)

このセクションは、Account Factory for Terraform (AFT) 使用時に直面する可能性のある一般的な問題をトラブルシューティングするのに役立ちます。

トピック

- [一般的な問題](#)
- [アカウントのプロビジョニング/登録に関連する問題](#)
- [カスタマイズの呼び出しに関する問題](#)
- [アカウントカスタマイズのワークフローに関連する問題](#)

一般的な問題

- AWS リソースクォータの超過

ロググループで AWS リソースクォータを超過したことが示された場合は、[AWS サポート](#)にお問い合わせください。Account Factory は AWS CodeBuild、AWS Organizations、を含むリソースクォータ AWS のサービス で 使用します AWS Systems Manager。詳細については次を参照してください:

- 「CodeBuild ユーザーガイド」の「[AWS CodeBuildとは](#)」。
- Organizations ユーザーガイドの「[とは AWS Organizations](#)」。
- Systems Manager ユーザーガイドの「[AWS Systems Managerとは](#)」。
- Account Factory バージョンが古い

問題が発生した際、それがバグであることを確かめるには、Account Factory が最新バージョンであることを確認します。詳細については、「[Updating the Account Factory version](#)」(Account Factory バージョンの更新)を参照してください。

- Account Factory ソースコードにローカルな変更が加えられている

Account Factory は、オープンソースプロジェクトです。AWS Control Tower は Account Factory コアコードをサポートしています。Account Factory コアコードにローカルな変更を加える場合、AWS Control Tower は Account Factory デプロイをベストエフォートベースでのみサポートします。

- Account Factory ロールのアクセス許可が不十分

Account Factory では、IAM ロールとポリシーを作成して、発行されたアカウントのデプロイとカスタマイズを管理します。このようなロールまたはポリシーを変更すると、Account Factory パイプラインで特定のアクションを実行できなくなる可能性があります。詳細については、「[Required roles](#)」(必要なロール)を参照してください。

- アカウントリポジトリに情報が正しく入力されていない

アカウントをプロビジョニングする前に、必ず「[デプロイ後の手順](#)」に従ってください。

- 手動による OU の変更後、ドリフトが検出されなくなる

Note

ドリフト検出は、AWS Control Tower で自動的に行われます。ドリフトの解決の詳細については、「[Detect and resolve drift in AWS Control Tower](#)」(AWS Control Tower でドリフトを検出して解決する)を参照してください。

組織単位 (OU) が手動で変更されると、ドリフトが検出されなくなります。これは、イベント駆動型の Account Factory が持つ性質によるものです。アカウントリクエストが送信されるとき、Terraform によって管理されるリソースは Amazon DynamoDB アイテムであり、直接のアカウントではありません。アイテムが変更されると、リクエストはキューに入れられ、AWS Control Tower によって (アカウントの詳細を管理するサービス) を通じて処理されます。OU を手動で変更すると、アカウントリクエストが変更されないため、ドリフトは検出されません。

アカウントのプロビジョニング/登録に関連する問題

- アカウントリクエスト (メールアドレス/名前) がすでに存在する

この問題は通常、プロビジョニング中または `ConditionalCheckFailedException` 発生時に、Service Catalog 製品の障害を引き起こします。

この問題の詳細情報は、次のいずれかを実行することで確認できます。

- Terraform または CloudWatch Logs ロググループを確認する。
- Amazon SNS トピックに発行されたエラー `aft-failure-notifications` を確認する。
- 不正な形式のアカウントリクエスト

アカウントリクエストが期待されるスキーマに従っていることを確認します。例については、GitHub の [terraform-aws-control_tower_account_factory](#) を参照してください。

- AWS Organizations リソースクォータを超えました

アカウントリクエストが AWS Organizations リソースクォータを超えていないことを確認します。詳細については、[AWS「組織のクォータ」](#)を参照してください。

カスタマイズの呼び出しに関する問題

- ターゲットアカウントが Account Factory にオンボードされていない

カスタマイズリクエストに含まれるすべてのアカウントが Account Factory にオンボードされていることを確認します。詳細については、「[Update an existing account](#)」(既存のアカウントの更新)を参照してください。

- カスタマイズリクエストのターゲットとなるアカウントが DynamoDB テーブル `aft-request-metadata` には存在するが、アカウントリクエストリポジトリに存在しない

次のいずれかを実行して、問題のあるアカウントを除外するようにカスタマイズ呼び出しリクエストを書式設定します。

- DynamoDB テーブル `aft-request-metadata` で、アカウントリクエストリポジトリに存在しないアカウントを参照するエントリを削除する。
- 「all」をターゲットとして使用しない。
- アカウントが属する OU をターゲットにしない。
- アカウントを直接ターゲットにしない。
- Terraform Cloud に使用されたトークンが誤っている

正しいトークンを設定していることを確認します。Terraform Cloud はチームベースのトークンのみをサポートし、組織ベースのトークンをサポートしていません。

- アカウントカスタマイズパイプラインが作成される前にアカウントを作成できなかった。アカウントをカスタマイズできない

アカウントリクエストリポジトリのアカウント仕様を変更します。アカウントのタグ値を変更するなどの変更を加えると、パイプラインが存在しない場合でも、Account Factory はパイプラインの作成を試みるパスをたどります。

アカウントカスタマイズのワークフローに関連する問題

アカウントカスタマイズのワークフローに関連する問題が発生した場合は、AFT のバージョンが 1.8.0 以上であることを確認し、DynamoDB リクエストテーブルからアカウント関連のメタデータのインスタンスをすべて削除してください。

AFT バージョン 1.8.0 の詳細については、GitHub の「[リリース 1.8.0](#)」を参照してください。

AFT のバージョンを確認および更新する方法については、以下を参照してください。

- [AFT バージョンを確認する](#)
- [AFT バージョンを更新する](#)

Amazon CloudWatch Logs Insights クエリを使用して、ターゲットアカウントとカスタマイズリクエスト ID を含むログをフィルタリングすることで、カスタマイズリクエストの追跡とトラブルシューティングを行うこともできます。詳細については、「[AFT アカウントカスタマイズリクエストの追跡によるトラブルシューティング](#)」を参照してください。

AWS Control Tower でドリフトを検出および解決する

ドリフトの特定と解決は、AWS Control Tower 管理アカウント管理者の通常の運用タスクです。ドリフトを解決することで、ガバナンス要件のコンプライアンスを確保できます。

ランディングゾーンを作成するとき、ランディングゾーンとすべての組織単位 (OU)、アカウント、リソースは、選択したコントロールによって適用されるガバナンスルールに準拠します。ユーザーおよび組織のメンバーがランディングゾーンを使用する際、コンプライアンスステータスが変更されることがあります。一部の変更は偶発的になされますが、時間的制約のある操作上のイベントに対応するために意図的になされる場合もあります。

ドリフト検出は、ドリフトを解決するために変更や設定更新が必要になるリソースを識別するのに役立ちます。

ドリフトの検出

ドリフト検出は、AWS Control Tower で自動的行われます。ドリフトを検出するには、AWS Control Tower が AWS Organizations への読み取り専用 API コールを行えるようにするため、AWSControlTowerAdmin ロールに管理アカウントへの永続的アクセス権が必要です。これらの API コールは、AWS CloudTrail イベントとして表示されます。

メンバーアカウントのドリフトは、監査アカウントに集約された Amazon Simple Notification Service (Amazon SNS) 通知に表示されます。各メンバーアカウントの通知を介して、アラートがローカルの Amazon SNS トピック、および Lambda 関数に送信されます。

Note

[設定] でアカウントの自動登録機能が有効になっている場合、これらの SNS 通知は使用できません。

AWS Security Hub CSPM サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールの場合、ドリフトは AWS Control Tower コンソールのアカウントとアカウントの詳細ページ、および Amazon SNS 通知によって表示されます。

メンバーアカウント管理者は、特定のアカウントの SNS ドリフト通知にサブスクライブできます (ベストプラクティスとしてもサブスクライブをお勧めします)。例えば、aws-controltower-AggregateSecurityNotifications SNS トピックはドリフト通知を提供します。ドリフトが発

生すると、AWS Control Tower コンソールから管理アカウント管理者に通知されます。ドリフトの検出と通知に関する SNS トピックの詳細については、「[Drift prevention and notification](#)」を参照してください。

ドリフト通知の重複除外

同じタイプのドリフトが同じリソースセットで複数回発生した場合、AWS Control Tower はドリフトの初回インスタンスに対してのみ SNS 通知を送信します。AWS Control Tower は、このドリフトのインスタンスが修復されたことを検出した場合、それらの同一のリソースに対してドリフトが再発生した場合にのみ、別の通知を送信します。

例: SCP ドリフトは以下の方法で処理されます

- 同じマネージド SCP を複数回変更した場合、初めて変更したときに通知が届きます。
- マネージド SCP を変更し、ドリフトを修正してから再度変更すると、2 回通知が届きます。

アカウントドリフトのタイプ

- OU 間でのアカウントの移動 (「[有効なベースラインでの継承ドリフト](#)」と「[有効なコントロールの継承ドリフト](#)」を参照)
- アカウントが組織から削除

Note

アカウントを 1 つの OU から別の OU に移動しても、以前の OU のコントロールは削除されません。移動先 OU で新しいフックベースのコントロールを有効にすると、古いフックベースのコントロールがアカウントから削除され、新しいコントロールに置き換わります。SCPs と AWS Config ルールで実装されたコントロールは、アカウントが OUs を変更するときに常に手動で削除する必要があります。

ポリシードリフトの例

- SCP の更新
- SCP が OU からデタッチされた

詳細については、「[Types of Governance Drift](#)」を参照してください。

ドリフトの表示

コンソールまたは API を使用して、アカウントと OU のドリフトステータスを表示し、アカウントと OU の設定がドリフトしている、または同期していないタイミングを特定できます。ドリフトステータスは SNS メッセージでも伝えられます。これらの SNS メッセージの受信の詳細については、「[SNS トピックのサブスクライブのガイド](#)」を参照してください。

コンソールで OU とアカウントドリフトのステータスを表示するには、[組織] ページに移動し、検査する OU またはアカウントを選択します。

OU とアカウントのドリフトステータスをプログラムで表示するには、[ListEnabledBaselines](#) API を呼び出して、有効なベースラインのステータスを表示します。ListEnabledBaselines API を使用して個々のアカウントのステータスをプログラムで表示するには、includeChildren フラグを使用します。これらのステータスでフィルタリングし、注意が必要なアカウントと OU のみを表示できます。

Note

AWS Control Tower は、各ドリフト修復オペレーションが完了すると[ライフサイクルイベント](#)を生成します。

ドリフトの解決

検出は自動で行われますが、ドリフトを解決するステップはコンソールまたは API を使用して行う必要があります。(移動されたアカウントで自動登録が有効化されている場合を除く。)

例えば、[ResetEnabledControl](#) API を呼び出すことにより、コントロールのポリシードリフトをプログラムで解決できます。

OU の設定ベースラインドリフトを解決するには、コンソールで [OU を再登録] を選択します。1 つのアカウントによってドリフトが発生している場合は、コンソールで [アカウントを更新] を選択できます。API を使用してベースラインドリフトを解決するには、OU で [ResetEnabledBaseline](#) API を呼び出すことができます。

概要

- [Landing zone settings] (ランディングゾーン設定) ページでは、さまざまなタイプのドリフトを解決できます。これらのタイプのドリフトを解決するには、[バージョン] セクションの [リセット] ボタンを選択します。

- OU のアカウント数が 1000 未満の場合は、[組織] ページまたは [OU の詳細] ページで [OU を再登録] を選択することで、Account Factory でプロビジョニングされたアカウントのドリフト、または SCP のドリフトを解決できます。
- 個々のアカウントを更新することで、[移動されたメンバーアカウント](#) などのアカウントドリフトを解決できる場合があります。詳細については、「[コンソールでアカウントを更新する](#)」を参照してください。
- コントロールの場合、[ResetEnabledControl API](#) を呼び出して多くの種類のドリフトを解決できます。
- OU とアカウントのベースラインドリフトは、[ResetEnabledBaseline API](#) を呼び出すか、AWS Control Tower コンソールで [OU を再登録] または [アカウントを更新] を選択することで解決できます。
- OUs 間でアカウントを移動したときに発生する継承ドリフトを解決するには、自動登録機能を有効にします。自動登録を有効にすると、AWS Control Tower はベースラインリソースとコントロール設定を送信先 OU から移動したアカウントに適用することで、継承ドリフトを自動的に修復します。コンソールのランディングゾーン設定ページで自動登録を有効にするか、RemediationTypeパラメータを Inheritance Drift に設定して [UpdateLandingZone API](#) を呼び出します。詳細については、「[自動登録でアカウントを移動して登録する](#)」を参照してください。

⚠ ランディングゾーンバージョンのドリフトを解決するアクションを実行する際には、2 つの動作が可能です。

- 最新のランディングゾーンバージョンを使用している場合、[リセット] を選択してから[確認] を選択すると、ドリフトしたランディングゾーンリソースは保存済みの AWS Control Tower 設定にリセットされます。ランディングゾーンバージョンは変わりません。
- 最新バージョンでない場合は、[更新] を選択する必要があります。ランディングゾーンは最新のランディングゾーンバージョンにアップグレードされます。このプロセスの一環としてドリフトが解決されます。

ドリフトスキャンと ポリシースキャンに関する考慮事項

AWS Control Tower は、マネージド SCP、RCP、宣言型ポリシーを毎日スキャンして、対応するコントロールが正しく適用され、ドリフトが発生していないことを確認します。これらのリソースを

取得してチェックを実行するために、AWS Control Tower は管理アカウントのロールを使用して、AWS Organizations ユーザーに代わって を呼び出します。

AWS Control Tower のスキャンでドリフトが検出された場合は、通知が届きます。AWS Control Tower は、ドリフトの問題ごとに通知を 1 つだけ送信するため、ランディングゾーンが既にドリフト状態にある場合、新しいドリフトアイテムが見つからない限り、追加の通知が送信されることはありません。

AWS Organizations は、各 APIs を呼び出す頻度を制限します。この制限は、1 秒あたりのトランザクション (TPS) 単位で表され、TPS 制限、スロットリングレート、または API リクエストレートと呼ばれます。AWS Control Tower が AWS Organizations を呼び出して SCP、RCP、宣言型ポリシーを監査する場合、AWS Control Tower が行う API コールは TPS 制限にカウントされます。これは、AWS Control Tower が管理アカウントを使用してコールを行うためです。

まれに、サードパーティーのソリューションまたは作成したカスタムスクリプトを使用して、同じ API を繰り返し呼び出すと、この制限に達することがあります。たとえば、ユーザーと AWS Control Tower が同時に (1 秒以内に) 同じ AWS Organizations APIs を呼び出し、TPS 制限に達した場合、それ以降の呼び出しはスロットリングされます。つまり、これらのコールは Rate exceeded のようなエラーを返します。

API リクエストレートを超えた場合

- AWS Control Tower が上限に達してスロットリングされた場合、監査の実行が一時停止され、後で再開されます。
- ワークロードが制限に達してスロットリングされた場合、その結果は、ワークロードの構成方法に応じて、わずかな遅延からワークロードの致命的なエラーにまで及ぶ可能性があります。このエッジケースには注意が必要です。

日次 SCP スキャンは、

1. 最近アクティブな OU が取得されます。
2. 登録された OU ごとに、OU にアタッチされている AWS Control Tower によって管理されているすべての SCP が取得されます。マネージド SCP には、aws-guardrails で始まる識別子があります。
3. OU で有効な予防コントロールごとに、コントロールのポリシーステートメントが OU のマネージド SCP に存在することを確認します。

OU には、マネージド SCP が 1 つ以上ある場合があります。

すぐに解決すべきドリフトのタイプ

ほとんどのタイプのドリフトは、管理者が解決できます。ただし、AWS Control Tower ランディングゾーンに必須の組織単位を削除したなど、即時解決しなければならないタイプのドリフトもあります。回避すべき重要なドリフトの例を以下に示します。

- セキュリティ OU を削除しないでください。AWS Control Tower によるランディングゾーンのセットアップ中に元々セキュリティと名付けられていた組織単位は削除しないでください。削除すると、ランディングゾーンをすぐにリセットするように指示するエラーメッセージが表示されます。リセットが完了するまで、AWS Control Tower で他のアクションを実行することはできません。
- 必要なロールを削除しないでください。AWS Control Tower は、IAM ロールのドリフトについてコンソールにログインするときに、特定の AWS Identity and Access Management (IAM) ロールをチェックします。これらのロールが見つからないかアクセス可能でない場合は、ランディングゾーンをリセットするように指示するエラーページが表示されます。これらのロールは、AWSControlTowerAdmin AWSControlTowerCloudTrailRole AWSControlTowerStackSetRole です。

これらのユーザーロールの詳細については、「[AWS Control Tower コンソールを使用するために必要なアクセス許可](#)」を参照してください。

- すべての追加の OU を削除しない: AWS Control Tower の運用には少なくとも 1 つの追加の OU が必要ですが、それがサンドボックス OU である必要はありません。
- 共有アカウントを削除しない: セキュリティ OUs からログアカウントを削除するなど、AWS Organizations コンソールまたは APIs を使用して Foundational OU から共有アカウントを削除した場合。これらのアカウントを移動すると、修正が必要なアカウントの移動ドリフトのタイプが作成されます。このタイプのドリフトを修正するには、ランディングゾーンを更新する必要があります。

Note

ベストプラクティスとして、これらの共有アカウントを Foundational OU 外に移動しないでください。

リソースへの修復可能な変更

以下に示しているのは、AWS Control Tower リソースに許可された変更のリストです。ただし、それらの変更により、解決可能なドリフトが発生します。これらの許可されたオペレーションの結果は AWS Control Tower コンソールで表示できますが、更新が必要な場合があります。

発生したドリフトを解決する方法の詳細については、「[AWS Control Tower の外部でのリソースの管理](#)」を参照してください。

AWS Control Tower コンソールの外部で許可される変更

- 登録済み OU の名前変更。
- セキュリティ OU の名前変更。
- 基礎 OU 以外のメンバーアカウントの名前変更。
- セキュリティ OU での AWS Control Tower の共有アカウントの名前変更。
- 基礎以外の OU の削除。
- 基礎以外の OU からの登録済みアカウントの削除。
- セキュリティ OU での共有アカウントのメールアドレスの変更。
- 登録された OU 内のメンバーアカウントのメールアドレスの変更。

Note

OU 間でのアカウントの移動はドリフトと見なされ、解決する必要があります。

ドリフトと新しいアカウントのプロビジョニング

ランディングゾーンがドリフト状態である場合、AWS Control Tower 内の [Enroll account] (アカウントの登録) 機能は動作しません。その場合、AWS Service Catalogを使用して新しいアカウントをプロビジョニングする必要があります。手順については、「[Account Factory を使用して Service Catalog コンソールでアカウントをプロビジョニングする](#)」を参照してください。

特に、ポートフォリオの名前変更など、Service Catalog を使用してアカウントに特定の変更を加えた場合、[Enroll account] (アカウントの登録) 機能は動作しません。

ガバナンスドリフトのタイプ

ガバナンスドリフトは組織ドリフトとも呼ばれ、OU、SCP、およびメンバーアカウントが変更または更新されたときに発生します。AWS Control Tower で検出できるガバナンスドリフトのタイプは次のとおりです。

- アカウントと OU ガバナンスのドリフト
- ランディングゾーンのドリフト
- 非 SCP コントロールのコントロールドリフト
- ベースラインとコントロールの継承ドリフト

次のセクションでは、AWS Control Tower が報告するこれらのタイプのドリフトの詳細と、それらの解決方法を説明します。

Note

AWS Control Tower は、LZ4.0 以上のお客様の SNS トピックへのドリフト通知の送信を停止し、代わりに管理アカウントの EventBridge へのドリフト通知の送信を開始します。EventBridge を介してドリフト通知を受信する方法に関するサンプルイベントとガイドランスについては、EventBridge の作成に関する以下のセクションを参照してください。

アカウントと OU ガバナンスのドリフト

- [移動されたメンバーアカウント](#)
- [削除されたメンバーアカウント](#)
- [計画外のマネージド SCP の更新](#)
- [マネージド OU からデタッチされた SCP](#)

ランディングゾーンのドリフト

別のタイプのドリフトはランディングゾーンドリフトで、これは管理アカウントを通じて見られます。ランディングゾーンドリフトは、IAM ロールドリフト、または基礎 OU と共有アカウントに特に影響を与えるあらゆるタイプの組織ドリフトで構成されます。

- [削除された基礎 OU](#)

- [信頼されたアクセスの無効化](#)

ランディングゾンドリフトの特殊なケースは、ロールドリフトで、必要なロールが利用できない場合に検出されます。このようなドリフトが発生すると、コンソールに警告ページと、ロールを復元する方法に関するいくつかの指示が表示されます。ロールドリフトが解決されるまで、ランディングゾーンは利用できません。ドリフトの詳細については、[すぐに解決すべきドリフトのタイプ](#) というセクションの「必要なロールを削除しない」を参照してください。

非 SCP コントロールのコントロールドリフト

AWS Control Tower は、リソースコントロールポリシー (RCP) で実装されたコントロール、宣言型ポリシー、およびAWS Security Hub CSPM サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールに関するコントロールドリフトについて報告します。

- [Security Hub CSPM コントロールドリフト](#)
- [コントロールポリシードリフト](#)

ベースラインとコントロールの継承ドリフト

- 有効なベースラインドリフト

メンバーアカウントのベースライン設定が親 OU に適用されているものと異なる場合、AWS Control Tower はそれらの OU とアカウントで有効なベースライン (リソース設定) の継承ドリフトを報告します。ベースラインの詳細については、「[ベースラインのタイプ](#)」を参照してください。

- [有効なベースラインでの継承ドリフト](#)
- 有効なコントロールドリフト

メンバーアカウントの有効なコントロールの設定が親 OU に適用されているものと異なる場合、AWS Control Tower はそれらの OU とアカウントで有効なコントロールの継承ドリフトを報告します。

- [有効なコントロールの継承ドリフト](#)

報告されないドリフト

- AWS Control Tower は、Amazon CloudWatch、IAM Identity Center など AWS CloudTrail、管理アカウントで動作する他のサービスに関するドリフトを探しません CloudFormation AWS Config。

- AWS Control Tower は、ベースラインに含まれるリソースを変更した場合に発生する可能性のあるリソースドリフト、または他の種類のドリフトを検出しません。

移動されたメンバーアカウント

Note

LZ 4.0 以降のお客様の場合、AWS Control Tower は AWSControlTowerBaseline なしで Account Factory アカウントの移動ドリフト通知を送信しません。

このタイプのドリフトは、OU ではなくアカウントで発生します。このタイプのドリフトは、AWS Control Tower メンバーアカウント、監査アカウント、またはログアーカイブアカウントが、登録された AWS Control Tower OU から他の OU に移動されたときに発生する可能性があります。多くの場合、[設定] ページでアカウントの自動登録機能を有効化すると、このタイプのドリフトを回避できます。詳細については、[自動登録でアカウントを移動して登録する](#)を参照してください。

このタイプのドリフトが検出された場合のドリフト通知の例を次に示します。

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more than 1000 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

解決策

最大 1000 のアカウントを持つ OU の、Account Factory でプロビジョニングされたアカウントでこのタイプのドリフトが発生した場合は、次の方法で解決できます。

- AWS Control Tower コンソールの [Organization] (組織) ページに移動し、アカウントを選択して、右上の [Update account] (アカウントの更新) を選択します (個々のアカウントでは最速のオプション)。
- AWS Control Tower コンソールの [Organization] (組織) ページに移動して、アカウントが含まれている OU の [Re-register] (再登録) を選択します (複数のアカウントでは最速のオプション)。詳細については、「[AWS Control Tower への既存の組織単位の登録](#)」を参照してください。
- Account Factory でプロビジョニングされた製品を更新する。詳細については、「[AWS Control Tower でアカウントを更新して移動する](#)」を参照してください。

Note

更新する個々のアカウントが複数ある場合は、スクリプト [自動化によるアカウントのプロビジョニングと更新](#) を使用して更新を行う方法も参照してください。

- 1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合、ドリフトの解決は、次の段落で説明するように、移動されたアカウントのタイプによって異なる場合があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。
 - Account Factory でプロビジョニングされたアカウントが移動された場合 — アカウントが 1000 未満の OU では、Account Factory でプロビジョニングされた製品を更新するか、OU を再登録するか、ランディングゾーンを更新することで、アカウントドリフトを解決できます。
- 1,000 を超えるアカウントを持つ OU では、OU を再登録しても更新が実行されないため、AWS Control Tower コンソールまたはプロビジョニングされた製品のいずれかを使用して、移動した各アカウントを更新することによりドリフトを解決する必要があります。詳細については、「[AWS Control Tower でアカウントを更新して移動する](#)」を参照してください。
- 共有アカウントが移動された場合 — ランディングゾーンを更新することで、監査またはログアーカイブアカウントの移動によるドリフトを解決できます。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。

⚠ 廃止されたフィールド名

ガイドラインに準拠ManagementAccountIDするため、フィールド名MasterAccountIDはに変更されました AWS。古い名前は廃止されました。2022 年以降、廃止されたフィールド名を含むスクリプトは機能していません。

削除されたメンバーアカウント

このタイプのドリフトは、登録された AWS Control Tower 組織ユニットからメンバーアカウントが削除されたときに発生する可能性があります。次の例は、このタイプのドリフトが検出されたときのドリフト通知を示しています。

```
{
  "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"
}
```

解決策

- このタイプのドリフトがメンバーアカウントで発生した場合は、AWS Control Tower コンソールまたは Account Factory でアカウントを更新することによりドリフトを解決できます。例えば、Account Factory の更新ウィザードから、別の登録された OU にアカウントを追加できます。詳細については、「[AWS Control Tower でアカウントを更新して移動する](#)」を参照してください。
- 共有アカウントが基礎 OU から削除された場合、ランディングゾーンをリセットしてドリフトを解決する必要があります。このドリフトが解決されるまで、AWS Control Tower コンソールを使用することはできません。
- アカウントと OU のドリフトの解決の詳細については、「[AWS Control Tower の外部でリソースを管理する場合](#)」を参照してください。

Note

Service Catalog では、Account Factory でプロビジョニングされた製品のうちアカウントを表すものは、アカウントを削除するために更新されません。代わりに、プロビジョニングされた製品は TAINTED として表示され、エラー状態になります。クリーンアップするには、Service Catalog に移動し、プロビジョニングされた製品を選択してから、[Terminate] (終了) を選択します。

計画外のマネージド SCP の更新

このタイプのドリフトは、コントロールの SCP がコンソール AWS Organizations で更新されたとき、または AWS CLI またはいずれかの AWS SDKs を使用してプログラムで更新されたときに発生する可能性があります。このタイプのドリフトが検出された場合のドリフト通知の例を次に示します。

```
{
  "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"
}
```

解決策

最大 1000 アカウントの OU でこのタイプのドリフトが発生した場合は、次の方法で解決できます。

- AWS Control Tower コンソールで [Organization] ページに移動して OU を再登録する (最も時間がかからないオプション)。詳細については、「[AWS Control Tower への既存の組織単位の登録](#)」を参照してください。
- ランディングゾーンを更新する (時間のかかるオプション)。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。

1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合は、ランディングゾーンを更新して解決してください。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。

マネージド OU からデタッチされた SCP

このタイプのドリフトは、AWS Control Tower によって管理される OU からコントロールの SCP がデタッチされた場合に発生する可能性があります。AWS Control Tower コンソールの外部から作業している場合に発生するのが特に一般的です。このタイプのドリフトが検出された場合のドリフト通知の例を次に示します。

```
{
  "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"
}
```

解決策

最大 1000 アカウントの OU でこのタイプのドリフトが発生した場合は、次の方法で解決できます。

- AWS Control Tower コンソールで OU に移動して OU を再登録する (最も時間がかからないオプション)。詳細については、「[AWS Control Tower への既存の組織単位の登録](#)」を参照してください。
- ランディングゾーンを更新する (時間のかかるオプション)。ドリフトが必須コントロールに影響を与えている場合、更新プロセスによって新しいサービスコントロールポリシー (SCP) が作成され、それを OU にアタッチすることでドリフトを解決します。ランディングゾーンを更新する方法については、「[ランディングゾーンを更新する](#)」を参照してください。

1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合は、ランディングゾーンを更新して解決してください。ドリフトが必須コントロールに影響を与えている場合、更新プロセス

スによって新しいサービスコントロールポリシー (SCP) が作成され、それを OU にアタッチすることでドリフトを解決します。ランディングゾーンを更新する方法については、「[ランディングゾーンを更新する](#)」を参照してください。

削除された基礎 OU

このタイプのドリフトは、セキュリティ OU などの AWS Control Tower の基礎 OU にのみ適用されます。これは、AWS Control Tower コンソールの外部で基礎 OU が削除された場合に発生する可能性があります。このタイプのドリフトが発生させずに基礎 OU を移動することはできません。OU の移動は、OU を削除してから別の場所に追加するのと同じだからです。ランディングゾーンを更新してドリフトを解決すると、AWS Control Tower は元の場所にある基礎 OU を置き換えます。次の例は、このタイプのドリフトが検出されたときに受け取る可能性のあるドリフト通知を示しています。

```
{
  "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"
}
```

解決策

このドリフトは基礎 OU に対してのみ発生するため、ランディングゾーンを更新することで解決できます。他のタイプの OU が削除されると、AWS Control Tower は自動的に更新されます。

アカウントと OU のドリフトの解決の詳細については、「[AWS Control Tower の外部でリソースを管理する場合](#)」を参照してください。

Security Hub CSPM コントロールドリフト

このタイプのドリフトは、AWS Security Hub CSPM サービスマネージドスタンダード: AWS Control Tower に含まれるコントロールがドリフト状態を報告したときに発生します。AWS Security Hub CSPM サービス自体は、これらのコントロールのドリフト状態を報告しません。代わりに、サービスは検出結果を AWS Control Tower に送信します。

Security Hub CSPM コントロールドリフトは、AWS Control Tower が Security Hub CSPM から 24 時間以上ステータス更新を受信していない場合にも検出できます。検出結果が正常に受信されない場合、AWS Control Tower はコントロールのドリフトが発生していないかどうかを確認します。次の例は、このタイプのドリフトが検出されたときに受け取る可能性のあるドリフト通知を示しています。

```
{
  "Message" : "AWS Control Tower has detected that an AWS Security Hub control
    was removed in your account example-account@amazon.com <mailto:example-
    account@amazon.com>. The artifact deployed on the target OU and accounts does not match
    the expected template and configuration for the control. This mismatch indicates that
    configuration changes were made outside of AWS Control Tower. For more information,
    view Security Hub standard",
  "MasterAccountId" : "123456789XXX",
  "ManagementAccountId" : "123456789XXX",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
  "RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
    and enable it again. If the problem persists, contact AWS support.",
  "AccountId" : "7876543219XXX",
  "ControlId" : "SH.XXXXXXX.1",
  "ControlName" : "EBS snapshots should not be publicly restorable",
  "ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
  "EnabledControlIdentifier": "arn:aws:controltower:us-
    east-1::enabledcontrol/<UNIQUE_ID>".
  "Region" : "us-east-1"
}
```

解決策

アカウント数が 1000 未満の OU、推奨される解決策は、ドリフトされたコントロールに対して ResetEnabledControl API を呼び出すことです。コンソールで、OU の再登録を選択すると、コントロールが元の状態にリセットされます。または、どの OU でも、コンソールまたは AWS Control Tower API を使用して、コントロールを削除して再度有効にすることができます。これにより、コントロールもリセットされます。

アカウントと OU のドリフトの解決の詳細については、「[AWS Control Tower の外部でリソースを管理する場合](#)」を参照してください。

コントロールポリシードリフト

このタイプのドリフトは、リソースコントロールポリシー (RCP) または宣言型ポリシーで実装されたコントロールがドリフトの状態をレポートするときに発生します。これは、AWS Control Tower コンソールとドリフトメッセージで表示できる CONTROL_INEFFECTIVE の状態を返します。このタイプのドリフトのドリフトメッセージには、影響を受けるコントロールの EnabledControlIdentifier も含まれます。

このタイプのドリフトは、SCP ベースのコントロールでは報告されません。

次の例は、このタイプのドリフトが検出されたときに受け取る可能性のあるドリフト通知を示しています。

```
{
  "Message": "AWS Control Tower detects that a policy it owns was updated unexpectedly. This mismatch indicates that configuration changes were made outside of AWS Control Tower.",
  "MasterAccountId": "123456789XXX",
  "ManagementAccountId": "123456789XXX",
  "OrganizationId": "o-123EXAMPLE",
  "DriftType": "CONTROL_INEFFECTIVE",
  "RemediationStep": "To remediate the issue, Reset the DRIFTED enabled control if permitted or Re-register the OU. If the problem persists, contact AWS support.",
  "TargetIdentifier": "arn:aws::organizations/o-123456/ou-1234-4567",
  "ControlId": "CT.XXXXXXX.PV.1",
  "ControlName": "EBS snapshots should not be publicly restorable",
  "ApiControlIdentifier": "arn:aws:controlcatalog::control/<UNIQUE_ID>",
  "EnabledControlIdentifier": "arn:aws:controltower:us-east-1::enabledcontrol/<UNIQUE_ID>"
}
```

解決策

AWS Control Tower で有効になっている RCP コントロール、宣言型ポリシーコントロール、Security Hub CSPM コントロールに対するコントロールポリシードリフトの最も簡単な解決策は、ResetEnabledControl API を呼び出すことです。

アカウント数が 1000 未満の OU の場合、コンソールまたは API からの他の解決策は OU を再登録することです。これにより、コントロールは元の状態にリセットされます。

どの個々の OU でも、コンソールまたは AWS Control Tower API を使用して、コントロールを削除して再度有効にすることができます。これにより、コントロールもリセットされます。

アカウントと OU のドリフトの解決の詳細については、「[AWS Control Tower の外部でリソースを管理する場合](#)」を参照してください。

信頼されたアクセスの無効化

このタイプのドリフトは、AWS Control Tower のランディングゾーンに適用されます。これは、AWS Control Tower ランディングゾーンを設定 AWS Organizations した後に、で AWS Control Tower への信頼されたアクセスを無効にしたときに発生します。

信頼できるアクセスを無効にすると、AWS Control Tower は AWS Organizations から変更イベントを受信しなくなります。AWS Control Tower は、これらの変更イベントを使用して同期を維持します AWS Organizations。その結果、AWS Control Tower はアカウントと OU の組織的な変更を見逃す可能性があります。そのため、ランディングゾーンを更新するたびに、各 OU を再登録することが重要です。

例: ドリフト通知

このタイプのドリフトが発生したときに受け取るドリフト通知の例を次に示します。

```
{
  "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."
}
```

解決策

この種のドリフトが AWS Control Tower コンソールで発生すると、AWS Control Tower から通知されます。解決策は、AWS Control Tower のランディングゾーンをリセットすることです。詳細については、「[ドリフトの解決](#)」を参照してください。

有効なベースラインでの継承ドリフト

このタイプのドリフトは、AWS Control Tower の OU とアカウントで発生する可能性があります。

解決策

このタイプのドリフトが発生すると、AWS Control Tower から通知されます。継承ドリフトのほぼすべてのケースで、移動したメンバーアカウントのドリフトに関するドリフト通知を受け取ります。これは、通常、アカウントが移動されたとき、またはアカウントが登録に失敗したときに、このタイプのドリフトが発生するためです。

コンソールでドリフトを表示し、解決する

AWS Control Tower コンソールで、[組織] ページの [ベースライン状態] 列にこの継承されたドリフトステータスを表示できます。コンソールからの解決策は、OU を再登録するか、アカウントを更新することです。

プログラムを使用してドリフトを表示し、解決する

ドリフトステータスをプログラムで表示するには、[ListEnabledBaselines](#) API を呼び出して、OU の有効なベースラインのステータスを表示します。ListEnabledBaselines API を使用して個々のアカウントのステータスをプログラムで表示するには、includeChildren フラグを使用します。

このタイプのドリフトは、[ResetEnabledBaseline](#) API を呼び出すことでプログラムで解決できます。

有効なコントロールの継承ドリフト

このタイプのドリフトは、AWS Control Tower の OU とアカウントで発生する可能性があります。

解決策

このタイプのドリフトが発生すると、AWS Control Tower から通知されます。継承ドリフトのほぼすべてのケースで、移動したメンバーアカウントのドリフトに関するドリフト通知を受け取ります。これは、通常、アカウントが移動されたとき、またはアカウントが登録に失敗したときに、このタイプのドリフトが発生するためです。

コンソールでドリフトを表示し、解決する

AWS Control Tower コンソールでは、[組織] ページ、[有効化されたコントロール] ページ、[アカウントの詳細] ページで、この継承されたドリフトステータスを表示できます。コンソールからの解決策は、OU を再登録するか、アカウントを更新することです。

プログラムを使用してドリフトを表示し、解決する

有効なコントロールの継承されたドリフトステータスをプログラムで表示するには、[ListEnabledControls](#) API を呼び出して、OU の有効なコントロールのステータスを表示します。ListEnabledControls API を使用して個々のアカウントのステータスをプログラムで表示するには、includeChildren フラグを使用します。

このタイプの継承ドリフトは、[ResetEnabledControl](#) API を呼び出すことでプログラムで解決できます。

EventBridge の作成

Note

EventBridge は LZ4.0 以上のお客様に対してのみ有効です。

AWS Control Tower の EventBridge 形式の例

```
{
  "version": "0",
  "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
  "detail-type": "Drift Detected",
  "source": "aws.controltower",
  "account": "111122223333",
  "time": "2018-03-22T00:38:11Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "message" : "AWS Control Tower has detected that your member account 'account-email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/move-account'",
    "managementAccountId" : "012345678912",
    "organizationId" : "o-123EXAMPLE",
    "driftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
    "remediationStep" : "Re-register this organizational unit (OU), or if the OU has more than 1000 accounts, you must update the provisioned product in Account Factory.",
  }
}
```

```
"accountId" : "012345678909",  
"sourceId" : "012345678909",  
"destinationId" : "ou-3210-1EXAMPLE"  
}  
}
```

ドリフト通知を受信するための EventBridge ルールを作成するガイダンス:

ドリフト通知の EventBridge ルールを作成するには

1. Amazon EventBridge コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. [ルールの作成] を選択します。
4. ルールの名前と説明を入力します。
5. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
6. イベントソースを定義します。
 - 「イベントソース」で、イベントソースとして AWS サービスを選択します。
 - AWS 「サービス名」で、AWS Control Tower を選択します。
 - 「イベントタイプ」で、ドリフト検出を選択
7. ターゲットを選択します。
 - ターゲットタイプでAWS サービスを選択し、ターゲットの選択でドリフト通知トピックや Lambda 関数などのターゲットを選択します。ターゲットは、ルールで定義したイベントパターンに一致するイベントが返されたときにトリガーされます。
 - 選択したターゲットに応じて、Lambda 関数名やドリフト通知トピック ARN など、必要な設定の詳細を指定します。
8. ルールを確認して作成します。
 - ルールの詳細を確認し、必要な変更を加えます。
 - 問題がなければ、ルールの作成をクリックして新しい EventBridge ルールを保存します。

ルールを作成すると、指定された AWS Control Tower イベントのモニタリングが開始され、ドリフトイベントが発生したときに選択したターゲットアクションがトリガーされます。

AWS Control Tower の外部でリソースを管理する場合

AWS Control Tower はお客様に代わってアカウント、組織単位、その他のリソースをセットアップしますが、これらのリソースの所有者はお客様です。これらのリソースは、AWS Control Tower の内部または外部で変更できます。AWS Control Tower の外部でリソースを変更する最も一般的な場所は、AWS Organizations コンソールです。このトピックでは、AWS Control Tower の外部で変更を行う場合に、AWS Control Tower リソースへの変更を調整する方法について説明します。

AWS Control Tower コンソールの外部でリソースの名前変更、削除、移動を行うと、コンソールが同期しなくなります。変更の多くは自動的に調整されます。変更によっては、ランディングゾーンをリセットして、AWS Control Tower コンソールに表示される情報を更新する必要があります。

一般に、AWS Control Tower コンソールの外部で AWS Control Tower リソースに加えた変更により、ランディングゾーンで解決可能なドリフトの状態が発生します。これらの変更の詳細については、「[リソースへの修復可能な変更](#)」を参照してください。

ランディングゾーンのリセットが必要なタスク

- セキュリティ OU の削除 (特殊なケースであるため、不用意に行わないでください)
- セキュリティ OU からの共有アカウントの削除 (非推奨)
- セキュリティ OU に関連付けられた SCP の更新、アタッチ、またはデタッチ。

AWS Control Tower によって自動的に更新される変更

- 登録済みアカウントの E メールアドレスの変更
- 登録済みアカウントの名前変更
- 新しい最上位の組織単位 (OU) の作成
- 登録済み OU の名前変更
- 登録済み OU の削除 (更新が必要なセキュリティ OU は除きます)
- 登録済みアカウントの削除 (セキュリティ OU の共有アカウントは除きます)

Note

AWS Service Catalog は、AWS Control Tower とは異なる方法で変更を処理します。変更を調整すると、ガバナンス体制に変更が生じる AWS Service Catalog 可能性があります。プロ

ビジョニング済み製品の更新の詳細については、AWS Service Catalog ドキュメントの「[プロビジョニング済み製品の更新](#)」を参照してください。

AWS Control Tower の外部にあるリソースの参照

AWS Control Tower の外部で新しい OU とアカウントを作成した場合は、それらが表示されていても、AWS Control Tower の管理対象外となります。

OU の作成

AWS Control Tower の外部で作成された組織単位 (OU) は未登録と見なされます。そうした OU は、[Organization] (組織) ページに表示されますが、AWS Control Tower コントロールの管理対象外となります。

アカウントの作成

AWS Control Tower の外部で作成されたアカウントは未登録と見なされます。AWS Control Tower に登録済みの OU に属する登録済みアカウントと未登録アカウントは、[Organization] (組織) ページに表示されます。登録済み OU に属していないアカウントは、AWS Organizations コンソールを使用して招待できます。この招待の目的は、アカウントを AWS Control Tower に登録したり、AWS Control Tower の管理対象をアカウントに拡大したりすることではありません。アカウントを登録して管理対象を拡大するには、AWS Control Tower で [Organization] (組織) ページまたは [Account detail] (アカウント詳細) に移動し、[Enroll account] (アカウントを登録) を選択します。

AWS Control Tower の外部でのリソース名の変更

AWS Control Tower コンソールの外部で組織単位 (OU) とアカウントの名前を変更できます。変更すると、その変更を反映するためにコンソールが自動的に更新されます。

OU の名前変更

では AWS Organizations、AWS Organizations API またはコンソールを使用して OU の名前を変更できます。AWS Control Tower の外部で OU 名を変更すると、AWS Control Tower コンソールに名前の変更が自動的に反映されます。ただし、AWS Service Catalogを使用してアカウントをプロビジョニングする場合は、AWS Control Tower と AWS Organizationsとの間で整合性が保たれるようにランディングゾーンをリセットする必要もあります。[リセット] ワークフローにより、基礎 OU と追加 OU のサービス間で整合性が保たれます。このタイプのドリフトは、[ランディングゾーン設定] ページから解決できます。「[AWS Control Tower でドリフトを検出および解決する](#)」の「ドリフトの解決」を参照してください。

AWS Control Tower ダッシュボードの [Organization] (組織) ページに OU の名前が表示されます。ランディングゾーンのリセットオペレーションが正常に完了したことを確認できます。

登録済みアカウントの名前変更

各 AWS アカウントには、AWS Billing and Cost Management コンソールでアカウントのルートユーザーが変更できる表示名があります。AWS Control Tower に登録されているアカウントの名前を変更すると、その名前変更が AWS Control Tower に自動的に反映されます。アカウント名の変更の詳細については、AWS 「Billing User Guide」の「[Managing an AWS account](#)」を参照してください。

セキュリティ OU の削除

このタイプのドリフトは特殊なケースです。セキュリティ OU を削除すると、ランディングゾーンのリセットを求めるエラーメッセージページが表示されます。AWS Control Tower で他のアクションを実行する前に、ランディングゾーンをリセットする必要があります。

- AWS Control Tower コンソールでアクションを実行することはできず、AWS Service Catalog リセットが完了するまで新しいアカウントを作成することはできません。
- [ランディングゾーン設定] ページを開いても、そのページに [リセット] ボタンは表示されません。

この状況では、ランディングゾーンのリセットプロセスによって、新しいセキュリティ OU が作成され、2 つの共有アカウントが新しいセキュリティ OU に移動されます。AWS Control Tower は、ログアーカイブアカウントと監査アカウントをドリフト済みとしてマークします。どちらのアカウントでも同じプロセスでドリフトが解決されます。

[Security] (セキュリティ) OU を削除する必要があると判断した場合は、次の点に留意してください。

[Security] (セキュリティ) OU を削除する前に、その OU にアカウントが含まれていないことを確認する必要があります。具体的には、OU からログアーカイブアカウントと監査アカウントを削除する必要があります。これらのアカウントを別の OU に移動することをお勧めします。

Note

セキュリティ OU を削除するアクションは不用意に実行しないでください。ログが一時的に停止されている場合、一部のコントロールが適用されない可能性があるため、このアクションによりコンプライアンスの問題が発生することがあります。

ドリフトに関する一般的な情報については、「[AWS Control Tower でドリフトを検出および解決する](#)」の「ドリフトの解決」を参照してください。

セキュリティ OU からのアカウントの削除

組織から共有アカウントを削除したり、[Security] (セキュリティ) OU から共有アカウントを移動したりすることはお勧めしません。誤って共有アカウントを削除した場合は、このセクションの修復ステップに従ってアカウントを復元できます。

- AWS Control Tower コンソール内から: 修復プロセスを開始するには、半手動修復ステップに従います。AWS Control Tower コンソールへのアクセスに使用するユーザーまたはロールに、`organizations:InviteAccountToOrganization` を実行する許可があることを確認します。このようなアクセス許可がない場合は、AWS Control Tower コンソールと AWS Organizations コンソールの両方を使用する手動修復ステップに従います。
- AWS Organizations コンソールから開始: この修復プロセスは少し長く、完全に手動の手順です。手動修復手順に従うと、AWS Organizations コンソールと AWS Control Tower コンソールが切り替わります。で作業するときは AWS Organizations、`AWSOrganizationsFullAccess` 管理ポリシーまたは同等の を持つユーザーまたはロールが必要です。AWS Control Tower コンソールで作業するときは、`AWSControlTowerServiceRolePolicy` マネージドポリシーまたは同等のものと、すべての AWS Control Tower アクションを実行する許可 (`controtower: *`) を持つユーザーまたはロールが必要です。
- 修復ステップでアカウントが復元されない場合は、AWS サポートにお問い合わせください。

以下を通じて共有アカウントを削除した結果 AWS Organizations。

- AWS Control Tower の必須のコントロールのサービスコントロールポリシー (SCP) によってアカウントが保護されなくなります。結果: AWS Control Tower によってアカウント内に作成されたりソースが変更または削除される場合があります。
- アカウントが AWS Organizations 管理アカウントに含まれなくなりました。結果: AWS Organizations 管理アカウントの管理者は、アカウントの支出を把握できなくなりました。
- アカウントが によってモニタリングされることは保証されなくなりました AWS Config。結果: AWS Organizations 管理アカウントの管理者は、リソースの変更を検出できない場合があります。
- アカウントが組織内に存在しなくなります。結果: AWS Control Tower の更新とリセットが失敗します。

AWS Control Tower コンソールを使用して共有アカウントを復元するには (半手動の手順)

1. <https://console.aws.amazon.com/controltower> で AWS Control Tower コンソールにサインインします。organizations:InviteAccountToOrganization を実行する許可を持つ IAM ユーザー、IAM Identity Center のユーザー、またはロールとしてサインインする必要があります。このような許可がない場合は、このトピックで後述する手動修復ステップを使用してください。
2. [Landing zone drift detected] (ランディングゾーンのドリフトが検出されました) ページで、[Re-Invite] (再招待) を選択して、共有アカウントを組織に再招待することで共有アカウントの削除を修復します。自動的に生成された E メールが、アカウントの E メールアドレスに送信されます。
3. 招待を承諾して、共有アカウントを組織に戻します。以下のいずれかを実行します。
 - 削除された共有アカウントにサインインし、<https://console.aws.amazon.com/organizations/home#/invites> に移動します。
 - アカウントを再招待したときに送信された E メールメッセージにアクセスできる場合は、削除したアカウントにサインインし、メッセージ内のリンクをクリックして、アカウントの招待に直接移動します。
 - 削除された共有アカウントが別の組織にない場合は、アカウントにサインインし、AWS Organizations コンソールを開いて招待に移動します。
4. 管理アカウントに再度サインインするか、AWS Control Tower コンソールが既に関いている場合は再ロードします。[Landing zone drift] (ランディングゾーンドリフト) ページが表示されます。[リセット] を選択してランディングゾーンを修復します。
5. リセットプロセスが完了するまで待ちます。

修復が成功すると、共有アカウントが通常の状態およびコンプライアンスで表示されます。

修復ステップでアカウントが復元されない場合は、AWS サポートにお問い合わせください。

AWS Control Tower と AWS Organizations コンソールを使用して共有アカウントを復元するには (手動修復)

1. で AWS Organizations コンソールにサインインします <https://console.aws.amazon.com/organizations/>。AWSOrganizationsFullAccess マネージドポリシーまたは同等のものを持つ IAM ユーザー、IAM Identity Center のユーザー、またはロールとしてサインインする必要があります。

2. 共有アカウントを組織に招待し直します。アカウントを に招待する要件、前提条件、手順については AWS Organizations、[「ユーザーガイド」の「組織への AWS アカウントの招待」](#)を参照してください。AWS Organizations
3. 削除された共有アカウントにサインインし、<https://console.aws.amazon.com/organizations/home#/invites> に移動して、招待を承諾します。
4. 管理アカウントにもう一度サインインします。。
5. AWSControlTowerServiceRolePolicy マネージドポリシーまたは同等のものと、すべての AWS Control Tower アクションを実行する許可 (controltower:*) を持つユーザーまたはロールとして、AWS Control Tower コンソールにサインインします。
6. [ランディングゾーンのドリフト] ページが表示されます。ここには、ランディングゾーンをリセットするオプションがあります。[リセット] を選択してランディングゾーンを修復します。
7. リセットプロセスが完了するまで待ちます。

修復が成功すると、共有アカウントが通常の状態およびコンプライアンスで表示されます。

修復ステップでアカウントが復元されない場合は、AWS サポートにお問い合わせください。

自動的に更新される外部変更

アカウントの E メールアドレスに加えた変更は、AWS Control Tower では自動的に更新されますが、Account Factory では自動的に更新されません。

管理対象アカウントの E メールアドレスの変更

AWS Control Tower は、コンソールエクスペリエンスから求められた E メールアドレスを取得して表示します。したがって、共有アカウントおよびその他のアカウントの E メールアドレスは、変更後も常に更新され、AWS Control Tower に表示されます。

Note

では AWS Service Catalog、プロビジョニング済み製品の作成時にコンソールで指定されたパラメータが Account Factory に表示されます。ただし、元のアカウントの E メールアドレスは変更されても、自動的に更新されません。これは、アカウントがプロビジョニングされた製品に概念的に含まれているためです。プロビジョニングされた製品とは異なります。この値を更新するには、プロビジョニングされた製品を更新する必要があります。これにより、ガバナンス体制が変更される可能性があります。

外部 AWS Config ルールの適用

AWS Control Tower は、AWS Control Tower コンソールの外部でアクティブ化された AWS Config ルールを含め、AWS Control Tower に登録された組織単位にデプロイされたすべてのルールのコンプライアンスステータスを表示します。

AWS Control Tower の外部での AWS Control Tower リソースの削除

AWS Control Tower で OU とアカウントを削除でき、これ以上のアクションを実行することなく更新を確認できます。Account Factory は、OU を削除したときには自動的に更新されますが、アカウントを削除したときには更新されません。

登録済み OU の削除 (セキュリティ OU は除きます)

内では AWS Organizations、API または コンソールを使用して空の組織単位 (OUs) を削除できます。アカウントを含む OU は削除できません。

OU が削除され AWS Organizations すると、AWS Control Tower は から通知を受け取ります。また、Account Factory の OU リストが更新されて、登録済み OU のリストの整合性が保たれます。

Note

では AWS Service Catalog、Account Factory が更新され、アカウントをプロビジョニングできる利用可能な OU のリストから削除された OUs が削除されます。

OU からの登録済みアカウントの削除

登録済みアカウントを削除すると、AWS Control Tower に通知が届いて更新が行われます。これにより、情報の整合性が保たれます。

Note

では AWS Service Catalog、管理対象アカウントを表す Account Factory プロビジョニング済み製品は、アカウントを削除するために更新されません。代わりに、プロビジョニングされた製品は TAINTED として表示され、エラー状態になります。クリーンアップするには、AWS Service Catalogに移動し、プロビジョニングされた製品を選択してから、[Terminate] (削除) を選択します。

AWS Control Tower で組織とアカウントを管理する

AWS Control Tower で作成するすべての組織単位 (OU) とアカウントは、AWS Control Tower によって自動的に管理されます。また、AWS Control Tower の外部で作成された既存の OU とアカウントがある場合は、それらを AWS Control Tower の管理下に入れることができます。

既存の アカウント AWS Organizations と AWS アカウントの場合、ほとんどのお客様は、アカウントを含む組織単位 (OU) 全体を登録することで、アカウントのグループを登録することを好みます。アカウントを個別に登録することもできます。個々のアカウント登録の詳細については、「[既存のアカウントの登録について](#)」を参照してください。

用語

- 既存の組織を AWS Control Tower に登録することは、組織の登録、または組織へのガバナンスの拡張と呼ばれます。
- AWS Control Tower に AWS アカウントを持ち込むと、アカウントの登録と呼ばれます。

OU とアカウントを表示する

AWS Control Tower の [Organization] (組織) ページでは、AWS Control Tower に登録済みの OU や未登録の OU を含め、AWS Organizations内のすべての OU を表示できます。ネストされた OU は階層の一部として表示できます。右上のドロップダウンから [Organizational units only] (組織単位のみ) を選択すると、[Organization] (組織) ページで組織単位を表示できます。

[Organization] (組織) ページには、AWS Control Tower での OU や登録のステータスに関係なく、組織内のすべてのアカウントが一覧表示されます。右上のドロップダウンから [Organization only] (アカウントのみ) を選択すると、[Organization] (組織) ページでアカウントを表示できます。アカウントが登録の前提条件を満たしている場合は、OU 内でアカウントを個別に表示、更新、登録できます。

フィルタリングを選択しない場合、[Organization] (組織) ページにアカウントと OU が階層表示されます。このページは、すべての AWS Control Tower リソースを監視し、アクションを実行する中心的な場所です。[Organization] (組織) ページの詳細については、動画チュートリアルをご覧ください。

Note

ランディングゾーンを含む組織で信頼されたアクセスを有効にすると、AWS Control Tower は組織内のすべてのアカウントのロールの作成、リソースの管理、データの読み取りを行うことができます。信頼されたアクセスを通じて、組織内のアカウントまたは OU は、登録済みか登録済みかにかかわらず、AWS Control Tower で利用できます。

動画チュートリアル

この動画 (4:01) では、AWS Control Tower の [Organization] (組織) ページの使用方法について説明しています。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower の \[Organization\] \(組織\) ページの使用方法の動画チュートリアル](#)

トピック

- [AWS Control Tower への既存の組織単位の登録](#)
- [既存のアカウントの登録について](#)

ガバナンスを既存の組織に拡張する

AWS Control Tower のガバナンスを既存の組織に追加するには、「AWS Control Tower ユーザーガイド」の「[はじめに](#)」のステップ 2 に記載されているように、ランディングゾーン (LZ) を設定します。

既存の組織に AWS Control Tower ランディングゾーンをセットアップするときは、以下のことが想定されます。

- AWS Organizations 組織ごとに 1 つのランディングゾーンを設定できます。
- AWS Control Tower は、既存の AWS Organizations 組織の管理アカウントを管理アカウントとして使用します。新しい管理アカウントは不要です。
- AWS Control Tower は登録済み OU に 2 つの新しいアカウントとして、監査アカウントとログ記録アカウントを設定します。
- 組織のサービスの制限により、これら 2 つの追加のアカウントの作成が許可されている必要があります。

- ランディングゾーンを起動するか、OU を登録すると、その OU に登録されているすべてのアカウントに AWS Control Tower コントロールが自動的に適用されます。
- AWS Control Tower によって管理される OU AWS に既存のアカウントを追加で登録して、それらのアカウントにコントロールを適用できます。
- AWS Control Tower に OU を追加したり、既存の OU を登録したりできます。

登録に関するその他の前提条件を確認するには、「[AWS Control Tower の開始方法](#)」を参照してください。

AWS Control Tower ランディングゾーンがセットアップされていない AWS Organizations の OU には、AWS Control Tower コントロールが適用されません。ここでは、その仕組みについて詳しく説明します。

- AWS Control Tower Account Factory の外部で作成された新しいアカウントは、登録済み OU のコントロールによって制限されません。
- AWS Control Tower に未登録の OU で作成された新しいアカウントは、特に [Enroll] (登録) で AWS Control Tower に登録していない限り、コントロールによって制限されません。アカウントの登録の詳細については、「[既存のアカウントの登録について](#)」を参照してください。
- 追加の既存の組織、既存のアカウント、新しい OU、または AWS Control Tower の外部で作成したアカウントは、個別に OU を登録するか、アカウントを登録しない限り、AWS Control Tower コントロールによって制限されません。

既存の OU とアカウントに AWS Control Tower を適用する方法の詳細については、「[AWS Control Tower への既存の組織単位の登録](#)」を参照してください。

既存の組織に AWS Control Tower ランディングゾーンをセットアップするプロセスの概要については、次のセクションの動画を参照してください。

Note

セットアップ中、AWS Control Tower は一般的な問題を回避するために事前チェックを実行します。ただし、現在 AWS ランディングゾーンソリューションを使用している場合は AWS Organizations、組織で AWS Control Tower を有効にして、AWS Control Tower が現在のランディングゾーンのデプロイを妨げる可能性があるかどうかを判断する前に、AWS ソリューションアーキテクトに確認してください。また、ランディングゾーン間でのアカウ

ントの移動については、「[アカウントが前提条件を満たしていない場合](#)」を参照してください。

動画: 既存の でランディングゾーンを有効にする AWS Organizations

この動画 (7:48) では、既存の AWS Organizations 構造で AWS Control Tower ランディングゾーンをセットアップして有効にする方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[既存の組織で AWS Control Tower を有効にする](#)

IAM Identity Center および既存の組織に関する考慮事項

- AWS IAM アイデンティティセンター (IAM Identity Center) が既に設定されている場合、AWS Control Tower ホームリージョンは IAM Identity Center リージョンと同じである必要があります。
- AWS Control Tower は、既存の設定を削除しません。
- IAM Identity Center が既に有効になっており、IAM Identity Center ディレクトリを使用している場合、AWS Control Tower は許可セット、グループなどのリソースを追加し、通常どおり続行します。
- 別のディレクトリ (外部、AD、マネージド AD) が設定されている場合、AWS Control Tower は既存の設定を変更しません。詳細については、「[AWS IAM アイデンティティセンター \(IAM Identity Center\) のお客様に関する考慮事項](#)」を参照してください。

他の AWS サービスへのアクセス

組織を AWS Control Tower ガバナンスに導入した後も、コンソールと APIs を使用して AWS Organizations AWS Organizations 、 を通じて利用可能な AWS サービスにアクセスできます。詳細については、「[AWS の関連サービス](#)」を参照してください。

AWS Control Tower のネストされた OU

この章では、AWS Control Tower でネストされた OU を操作する際に留意すべき想定事項と考慮事項を示します。ネストされた OU での操作は、ほとんどの点でフラットな OU 構造での操作と同じです。[Register] (登録) 機能と [Re-register] (再登録) 機能はネストされた OU で動作しますが、変更された動作もあり、それについてはこの章で説明します。

動画チュートリアル

この動画 (4:46) では、AWS Control Tower でネストされた OU デプロイを管理する方法について説明しています。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower でのネストされた OU の管理に関する動画チュートリアル。](#)

ネストされた OU とランディングゾーンのベストプラクティスに関するガイダンスについては、ブログ記事の「[Organizing your AWS Control Tower landing zone with nested OUs](#)」(ネストされた OU による AWS Control Tower ランディングゾーンの編成) を参照してください。

フラットな OU 構造からネストされた OU 構造への拡張

フラットな OU 構造で AWS Control Tower ランディングゾーンを作成した場合は、それをネストされた OU 構造に拡張できます。

このプロセスには主に次の 4 つのステップがあります。

1. AWS Control Tower で目的のネストされた OU 構造を作成します。
2. AWS Organizations コンソールに移動し、一括移動機能を使用して、アカウントをソース OU (フラット) から宛先 OU (ネスト) に移動します。その方法は次のとおりです。
 - a. アカウントの移動元となる OU に移動します。
 - b. OU 内のすべてのアカウントを選択します。
 - c. [Move] (移動) を選択します。

Note

AWS Control Tower には Move 機能がないため、このステップは AWS Organizations コンソールで実行する必要があります。

3. AWS Control Tower のネストされた OU に移動し、[Register] (登録) または [Re-register] (再登録) の操作を行います。ネストされた OU 内のすべてのアカウントが登録されます。
 - AWS Control Tower に OU を作成した場合は、OU の [Re-register] (再登録) を行います。
 - で OU を作成した場合は AWS Organizations、OU を初めて登録します。
4. アカウントを移動して登録したら、AWS Organizations コンソールまたは AWS Control Tower コンソールから空の最上位 OU を削除します。

ネストされた OU の登録の事前チェック

ネストされた OU とそのメンバーアカウントを正常に登録できるように、AWS Control Tower では一連の事前チェックが実行されます。これと同じ事前チェックが、最上位の OU またはネストされた OU を登録するときにも実行されます。詳細については、「[Common causes of failure during registration or re-registration](#)」を参照してください。

- すべての事前チェックにパスすると、AWS Control Tower が自動的に OU の登録を開始します。
- 事前チェックが失敗した場合、AWS Control Tower は登録プロセスを停止し、OU を登録する前に修正する必要がある項目のリストを示します。

ネストされた OU とロール

AWS Control Tower は、ターゲット OU の下にあるアカウントと、ターゲット OU の下にネストされたすべての OU にあるアカウントに対して、AWSControlTowerExecution ロールをデプロイします。これは、ターゲット OU のみを登録する場合でも同様です。管理アカウント [Administrator] (管理者) のすべてのユーザーに、AWSControlTowerExecution ロールを持つアカウントに対する許可が付与されます。このロールを使用すると、AWS Control Tower コントロールでは通常許可されないアクションを実行できます。

このロールは、登録する予定がない未登録のアカウントから削除できます。このロールを削除すると、ロールをアカウントに復元しない限り、AWS Control Tower にアカウントを登録したり、直接の親 OU を登録したりすることはできません。アカウントから AWSControlTowerExecution ロールを削除するには、AWSControlTowerExecution ロールでサインインする必要があります。他の IAM プリンシパルには AWS Control Tower で管理されるロールの削除が許可されていないためです。

ロールのアクセスを制限する方法については、「[Optional conditions for your role trust relationships](#)」を参照してください。

ネストされた OU とアカウントの登録時および再登録時の処理

ネストされた OU を登録または再登録すると、AWS Control Tower がターゲット OU の未登録アカウントをすべて登録し、登録済みのアカウントをすべて更新します。以下のような処理が発生すると想定されています。

AWS Control Tower が次のタスクを実行する

- この OU の下にあるすべての未登録アカウントと、そのネストされた OU 内にあるすべての未登録アカウントに対して、AWSControlTowerExecution ロールを追加します。
- 未登録のメンバーアカウントを登録します。
- 登録済みのメンバーアカウントを再登録します。
- 新しく登録されたメンバーアカウントの IAM Identity Center ログインを作成します。
- 既存の登録済みのメンバーアカウントを更新して、ランディングゾーンへの変更を反映します。
- この OU とそのメンバーアカウント用に設定されているコントロールを更新します。

ネストされた OU を登録する際の考慮事項

- コア OU (セキュリティ OU) の下に OU を登録することはできません。
- ネストされた OU は個別に登録する必要があります。
- 親 OU が登録されていない限り、OU を登録することはできません。
- ツリー内で上位にあるすべての OU がある時点で正常に登録されていない限り (既に削除されたものも含めます)、OU を登録することはできません。
- 上位にあるドリフトされた OU の下に OU を登録することはできますが、そのアクションによってドリフトが修復されることはありません。

ネストされた OU の制限

- OU は、ルートの下に最大 5 レベルの深さでネストできます。
- ターゲット OU の下にネストされる OU は、個別に登録または再登録する必要があります。
- ターゲット OU が階層内のレベル 2 以下にある場合、つまり最上位の OU でない場合、上位にある OU で有効な予防コントロールが、この OU とその下位にあるすべての OU に自動的に適用されます。
- OU 登録の失敗は、階層ツリーの上位に伝播されません。親の OU 詳細ページで、ネストされた OU の状態に関する詳細を確認できます。
- OU 登録の失敗は、階層ツリーの下位に伝播されません。
- AWS Control Tower は、新規または既存のアカウントの VPC 設定を変更しません。

ネストされた OU とコンプライアンス

AWS Control Tower コンソールから、[Organization] (組織) ページで非準拠の OU とアカウントを表示できるため、広範囲にコンプライアンスを把握できます。

ネストされた OU およびアカウントのコンプライアンスに関する考慮事項

- OU のコンプライアンスは、その下にネストされた OU のコンプライアンスに基づいて決定されません。
- コントロールのコンプライアンスステータスは、ネストされた OU を含め、コントロールが有効になっているすべての OU で計算されます。「[OU とアカウントの AWS Control Tower コンプライアンスステータス](#)」を参照してください。
- OU は、OU 階層内のどこに配置されているかにかかわらず、非準拠のアカウントがある場合にのみ非準拠として表示されます。
- ネストされた OU が非準拠の場合、その親 OU は自動的に非準拠とは見なされません。
- [OU detail] (OU の詳細) または [Account detail] (アカウントの詳細) ページで、OU またはアカウントが非準拠ステータスを示す原因となっている可能性のある非準拠リソースのリストを表示できます。

ネストされた OU とドリフト

状況によっては、ドリフトのためにネストされた OU を登録できないことがあります。

ドリフトとネストされた OU に対する想定

- ドリフトされた親を持つ OU に対してコントロールを有効にすることはできますが、ドリフトされた OU に対して直接ガードレールを有効にすることはできません。
- ドリフトされた OU の下で検出コントロールを有効にすることができます。ただし、最上位のドリフトされた OU でない場合に限られます。
- 必須コントロールは、最上位の OU でのみ有効になります。ネストされた OU を登録するときには、必須コントロールはスキップされます。
- 1 つの必須コントロールは AWS Config リソースを保護するため、ネストされた OUs を登録するには、そのコントロールがドリフトしない状態である必要があります。ドリフトされている場合、AWS Control Tower はネストされた OU の登録をブロックします。

- 最上位の OU がドリフトしている場合、AWS Config リソースを保護するコントロールはドリフトしている可能性があります。この場合、AWS Control Tower は検出コントロールの適用など、AWS Config リソースの作成または更新を必要とするアクションをブロックします。

ネストされた OU とコントロール

登録済みの OU でコントロールを有効にした場合、予防コントロールと検出コントロールでは動作が異なります。ネストされた OU の場合、プロアクティブコントロールは検出コントロールと同様に動作します。

予防コントロール

- 予防コントロールは、ネストされた OU に適用されます。
- 必須の予防コントロールは、OU とそのネストされた OU の下にあるすべてのアカウントに適用されます。
- 予防コントロールは、ターゲット OU の下にネストされたすべてのアカウントと OU に影響します。そのアカウントと OU が登録されていない場合でも影響を受けます。

検出コントロールとプロアクティブコントロール

- ネストされた OU は、検出コントロールまたはプロアクティブコントロールを自動的に継承しません。個別に有効にする必要があります。
- 検出コントロールとプロアクティブコントロールは、ランディングゾーンの運用リージョンに登録されているアカウントにのみデプロイされます。

コントロールの状態と継承を有効化

[OU details] (OU 詳細) ページでは、継承されたコントロールを OU ごとに表示できます。

Tip

コントロールの継承を利用して、OU の SCP クォータ内に収めることができます。例えば、ネストされた OU に対してコントロールを直接有効にする代わりに、OU 階層の最上位の OU で有効にすることができます。

ステータスの継承

- ステータスが [Inherited] (継承済み) の場合、コントロールが継承によってのみ有効になり、OU に直接適用されていないことを示します。
- ステータスが [Enabled] (有効) の場合、他の OU での状態に関係なく、コントロールがこの OU に適用されることを示します。
- ステータスが [Failed] (失敗) の場合、他の OU での状態に関係なく、コントロールがこの OU に適用されないことを示します。

Note

ステータスが [Inherited] (継承済み) の場合、コントロールがツリー内の上位の OU に適用されたことと、この OU に適用されるものの直接には追加されなかったことを示します。

ランディングゾーンが現在のバージョンでない場合

[Enabled controls] (有効なコントロール) 表内の各行は、1 つの個別の OU にある 1 つの有効なコントロールを表します。

ネストされた OU とルート

ルートは OU ではなく、登録や再登録ができません。ルートにアカウントを直接作成することもできません。ルートが非準拠になったり、登録済みやドリフトなどのライフサイクル状態になったりすることはありません。

一方で、ルートはすべてのアカウントと OU の最上位のコンテナです。ネストされた OU のコンテキストでは、これは他のすべての OU がネストされているノードです。

AWS Control Tower への既存の組織単位の登録

複数の既存の AWS アカウントを AWS Control Tower に取り込む効率的な方法は、AWS Control Tower によるガバナンスを組織単位 (OU) 全体に拡張することです。

で作成された既存の OU AWS Organizations とそのアカウントに対する AWS Control Tower ガバナンスを有効にするには、AWS Control Tower ランディングゾーンに OU を登録します。最大 1000 のアカウントが含まれている OU を登録できます。1000 を超えるアカウントが含まれている OU は、AWS Control Tower に登録できません。

OU を登録すると、そのメンバーアカウントが AWS Control Tower ランディングゾーンに登録されます。メンバーアカウントは、OU に適用されるコントロールによって管理されます。

Landing Zone バージョン 4.0 以降では、OU でコントロールを直接有効にできます。検出コントロールには、OU を登録するか、OU で AWS Config 記録を有効にすることでアクティブ化できる AWS Config 記録が必要です。登録 OU は を有効にしますAWSControlTowerBaseline。AWS Config 記録を有効にすると、 が有効になりますConfigBaseline。詳細については、「[ベースラインのタイプ](#)」および「[AWS Control Tower Controls Reference Guide](#)」を参照してください。

Note

AWS Control Tower ランディングゾーンをまだお持ちでない場合は、まず、AWS Control Tower によって作成された新しい組織または既存の AWS Organizations 組織のいずれかでランディングゾーンを設定します。ランディングゾーンのセットアップ方法の詳細については、「[AWS Control Tower の使用開始方法](#)」を参照してください。

OU の登録によるアカウントの処理

AWS Control Tower では、AWS CloudFormation が組織内のアカウントにスタックを自動的にデプロイできるように、AWS Organizations ユーザーに代わって AWS CloudFormation と の間に信頼されたアクセスを確立するためのアクセス許可が必要です。

- ステータスが [Not enrolled] (未登録) であるすべてのアカウントに AWSControlTowerExecution ロールが追加されます。
- OU を登録すると、デフォルトでは OU に対して必須のコントロールが有効になります。

OU 登録後の一部のアカウントの登録

OU を正常に登録できても、一部のアカウントが未登録のままになることがあります。その場合、未登録のアカウントは登録の前提条件の一部を満たしていません。[Register OU] (OU の登録) プロセスの一環としてアカウントの登録が失敗した場合は、アカウントページのアカウントステータスに [Enrollment failed] (登録に失敗しました) と表示されます。OU ページでは、アカウントフィールドに [4 of 5] (4/5) といったアカウント情報が表示されることもあります。

例えば、[4 of 5] と表示されている場合は、[Register OU] (OU の登録) プロセスを実行したところ、OU に全部で 5 個あるアカウントのうち 4 個は正常に登録されたものの、1 個が失敗したということになります。アカウントを登録するには、アカウントが登録の前提条件を満たしていることを確認した後で [Re-Register OU] (OU を再登録) を選択します。

IAM ユーザーが OU を登録するための前提条件

アクセスAdmin許可がすでにある場合でも、Register OU オペレーションを実行するときは、AWS Identity and Access Management (IAM) ID (ユーザーまたはロール) または IAM Identity Center ユーザー ID を適切な Account Factory ポートフォリオに含める必要があります。そうしないと、登録時にプロビジョニング済み製品の作成が失敗します。失敗するのは、AWS Control Tower が OU の登録時に IAM ユーザーまたは IAM Identity Center ユーザー ID の認証情報を利用するためです。

これに関連するポートフォリオは、AWS Control Tower Account Factory Portfolio という AWS Control Tower によって作成されたものです。このポートフォリオに移動するには、[Service Catalog] > [Account Factory] > [AWS Control Tower Account Factory Portfolio] を選択します。次に、[グループ、ロール、およびユーザー] というタブを選択して、IAM または IAM Identity Center ID を表示します。アクセス権を付与する方法の詳細については、「[AWS Service Catalogのドキュメント](#)」を参照してください。

既存の OU の登録

AWS Control Tower コンソールの [Organization] (組織) ページでは、AWS Control Tower に登録済みの OU や未登録の OU を含め、組織のすべての OU とアカウントを階層で表示できます。

一般に、未登録の OUs は 1000 以下で作成され AWS Organizations、他のランディングゾーンによって管理されません。最大 1000 のアカウントが含まれている既存の OU を登録できます。1000 を超えるアカウントが含まれている OU は、AWS Control Tower に登録できません。

コンソールから既存の OU を登録するには

1. <https://console.aws.amazon.com/controltower> で AWS Control Tower コンソールにサインインします。
2. 左ペインのナビゲーションメニューで、[Organization] (組織) を選択します。
3. [Organization] (組織) ページで、登録する OU の横にあるラジオボタンを選択し、右上の [Actions] (アクション) ドロップダウンメニューから [Register organizational unit] (組織単位の登録) を選択します。または、OU の名前を選択すると、その OU の [OU details] (OU の詳細) ページが表示されます。
4. [OU details] (OU の詳細) ページで、右上の [Actions] (アクション) ドロップダウンメニューから [Register OU] (OU の登録) を選択できます。

登録プロセスでは、管理対象を OU に拡大するのに少なくとも 10 分かかり、アカウントを追加するたびに最大 2 分かかります。

API を使用して既存の OU を登録するには

AWS Control Tower API を使用して既存の OU を登録するには、`baselineIdentifier` フィールドの `AWSControlTowerBaseline` を使用して `EnableBaseline` API を呼び出します。詳細については、「[API のみを使用した AWS Control Tower OU の登録](#)」を参照してください。

既存の OU を登録した場合の結果

既存の OU を登録すると、`AWSControlTowerExecution` ロールにより、AWS Control Tower の管理対象を個々のアカウントに拡大できます。ガードレールが適用され、アカウントアクティビティに関する情報が監査およびログ記録のアカウントに報告されます。

他には以下のような結果があります。

- `AWSControlTowerExecution` を使用すると、AWS Control Tower 監査アカウントによる監査が可能になります。
- `AWSControlTowerExecution` では、各アカウントのすべてのログがログ記録アカウントに送信されるように組織のログ記録を設定できます。
- `AWSControlTowerExecution` により、選択した AWS Control Tower コントロールが OU 内の個々のアカウントと AWS Control Tower で作成したすべての新規アカウントに自動的に適用されるようになります。

登録済み OU の場合、AWS Control Tower コントロールによって具体化される監査機能とログ記録機能に基づいて、コンプライアンスレポートとセキュリティレポートを提供できます。セキュリティチームとコンプライアンスチームは、すべての要件が満たされていること、組織ドリフトが発生していないことを確認できます。ドリフトの詳細については、「[AWS Control Tower でドリフトを検出および解決する](#)」を参照してください。

Note

AWS Control Tower に OU とそのアカウントが表示されるときに、ある異常な状況が発生することがあります。登録済み OU にアカウントを作成した後、登録済みのアカウントを別の未登録の OU に移動すると (特に AWS Organizations を使用してアカウントを移動すると)、OU の詳細ページに「1/0」アカウントという結果が表示されることがあります。また、その未登録の OU に別の未登録のアカウントを作成した可能性もあります。未登録のアカウントがある場合、コンソールではその OU に対して「1/1」などと表示されます。単一の (新規作成の) アカウントが登録されているように見えますが、実際には登録されていません。新しいアカウントを登録する必要があります。

新しい OU の作成

AWS Control Tower で OU またはネストされた OU を作成する方法は次のとおりです。

AWS Control Tower で新しい OU を作成するには

1. [Organization] (組織) ページに移動します。
2. 右上の [Create resources] (リソースの作成) ドロップダウンメニューから [Create organizational unit] (組織単位の作成) を選択します。
3. [OU name] (OU 名) フィールドに名前を指定します。
4. [Parent OU] (親 OU) ドロップダウンに、登録済み OU の階層が表示されます。作成している新しい OU の親 OU を選択します。
5. [Add] (追加) を選択します。

Tip

ネストされた OU をより少ない手順で追加するには、[組織] ページのテーブルに表示される親 OU の名前を選択し、親 OU の [OU] ページを表示します。次に、右上にある [アクション] ドロップダウンメニューから [OU の追加] を選択します。新しい OU が、選択した OU の下にネストされた OU として自動的に作成されます。

Note

ランディングゾーンが最新でない場合は、ドロップダウンメニューに階層ではなくフラットリストが表示されます。ランディングゾーンにネストされた OU が含まれている場合でも、L5 OU の下に新しい OU を作成できないため、ドロップダウンに L5 OU は表示されません。AWS Control Tower のネストされた OU の詳細については、「[AWS Control Tower のネストされた OU](#)」を参照してください。

OU を削除する

AWS Control Tower は、OU を登録解除し、OU を削除する別のコンソールアクションをサポートしています。

OU の削除は最終的なものです。元に戻すことはできません。

考慮事項

- 削除および登録解除オペレーションが成功するには、OU のアカウントが空である必要があります。
- すべてのオプションのコントロールを OU から削除する必要があります。
- OU を削除する前に、登録を解除する必要があります。
- 削除ではなく、登録を解除することによって、AWS Control Tower から OU を削除できます。

AWS Control Tower から OU を削除するには

1. <https://console.aws.amazon.com/controltower> で AWS Control Tower コンソールにサインインします。
2. [Organization] (組織) ページに移動します。
3. OU の名前を選択して [OU の詳細] ページを表示し、すべてのアカウントが OU から削除されていることを確認します。
4. また、[OU の詳細] ページで、すべてのオプションのコントロールが OU から削除されていることを確認してください。
5. [組織] ページに戻り、OU の横にあるラジオボタンを選択します。
6. 右上の [アクション] ドロップダウンメニューから [組織単位を登録解除] を選択します。
7. OU を完全に削除しない場合は、ここで停止し、AWS Control Tower から登録解除するだけにします。OU を完全に削除するには、次のステップに進みます。
8. 続行するには、右上の [アクション] ドロップダウンメニューから [削除] を選択します。

別の OU の登録を解除するには、登録解除プロセスが完了するまで待つ必要があります。

Note

AWS Control Tower によって管理されているアカウントを削除するには、AWS Control Tower コンソールの左のナビゲーションペインから [アカウントファクトリー] に移動します。AWS Control Tower によって管理されていない OU 内のアカウントを削除するには、AWS Organizations コンソールに移動します。

プログラムで OU の登録を解除するには、[DisableBaseline API](#) を呼び出します。

登録時または再登録時に発生する障害のよくある原因

一般に、OU を登録または再登録すると、その OU 内のすべてのアカウントが AWS Control Tower に登録されます。ただし、OU 全体が正常に登録されても、一部のアカウントが登録に失敗する場合があります。このような場合は、そのアカウントに関連する事前チェックの失敗を解決して、そのアカウントまたは OU を再登録する必要があります。

OU またはそのメンバーアカウントの登録 (または再登録) が失敗した場合、AWS Control Tower は影響を受けるメンバーアカウントについてエラーメッセージを返します。エラーメッセージは [OU の詳細] ページで確認できます。このページでは、事前チェックとアカウントのエラーメッセージが表にまとめられています。[OU を登録] オペレーションが失敗した場合、表には OU に属するすべてのアカウントのエラーメッセージがすべて表示されます。必要に応じて、[アカウントの詳細] ページで各アカウントのエラーメッセージを確認することもできます。

オプションで、どの事前チェックに合格しなかったかを示す詳細なレポートを含むファイルをオフライン分析用にダウンロードできます。登録領域の右上に表示される [Download] (ダウンロード) ボタンを選択すると、ダウンロードを完了できます。

このセクションでは、事前チェックが失敗した場合に発生する可能性があるエラーの種類とそのエラーの修正方法について説明します。

ランディングゾーンのエラー

- ランディングゾーンの準備ができていない

現在のランディングゾーンをリセットするか、最新バージョンに更新してください。

OU エラー

- SCP の最大数を超過している

OU あたりのサービスコントロールポリシー (SCP) の制限を超過しているか、別のクォータに達している可能性があります。AWS Control Tower ランディングゾーンのすべての OU には、OU あたり 5 個の SCP という制限が適用されます。クォータの許容数を超過する SCP がある場合は、SCP を削除または結合する必要があります。

- SCP の競合

既存の SCP が OU またはアカウントに適用されているために、AWS Control Tower がアカウントを登録できない可能性があります。適用された SCP を調べて、AWS Control Tower の動作を妨げ

るポリシーがないか確認してください。階層の上位にある OU から継承された SCP を確認してください。

- スタックセットのクォータを超えている

スタックセットのクォータを超えている可能性があります。クォータの許容数を超えるインスタンスがある場合は、スタックインスタンスをいくつか削除する必要があります。詳細については、「AWS CloudFormation ユーザーガイド」の「[AWS CloudFormation のクォータ](#)」を参照してください。

- アカウントの上限を超えている

AWS Control Tower では、登録時に各 OU を 1000 アカウントに制限しています。

アカウントエラー

- アカウントで事前チェックが禁止されている

OU 上の既存の SCP が原因で、AWS Control Tower が OU メンバーアカウントに対して事前チェックを実行できません。この事前チェックの失敗を解決するには、OU を更新するか、OU から SCP を削除します。

- E メールアドレスのエラー

アカウントに指定した E メールアドレスが命名基準に準拠していません。許可される文字を正規表現 (regex) で指定するは、`[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+` を使用します。

- 設定レコーダーまたは配信チャネルが有効

アカウントには、既存の AWS Config 設定レコーダーまたは配信チャネルがある場合があります。これらは、アカウントを登録する前に、AWS Control Tower 管理アカウントがリソースを管理しているすべての AWS リージョン AWS CLI で、を通じて削除または変更する必要があります。

- STS が無効

AWS Security Token Service (AWS STS) はアカウントで無効にすることができます。AWS STS エンドポイントは、AWS Control Tower でサポートされているすべてのリージョンのアカウントでアクティブ化する必要があります。

- IAM Identity Center の競合

AWS Control Tower ホームリージョンが AWS IAM アイデンティティセンター (IAM Identity Center) リージョンと同じではありません。IAM Identity Center が既にセットアップされている場

合、AWS Control Tower ホームリージョンは IAM Identity Center リージョンと同じである必要があります。

- SNS トピックが競合している

アカウントには、AWS Control Tower で使用する必要がある Amazon Simple Notification Service (Amazon SNS) トピック名があります。AWS Control Tower は、特定の名前を付けてリソース (SNS トピックなど) を作成します。このような名前が既に取得されている場合は、AWS Control Tower のセットアップが失敗します。こうした状況は、AWS Control Tower に以前に登録されたアカウントを再利用している場合に発生する可能性があります。

- 一時停止中のアカウントが検出される

このアカウントは停止しています。AWS Control Tower に登録することはできません。アカウントをこの OU から削除してから再試行してください。

- IAM ユーザーがポートフォリオにない

OU を登録する前に AWS Identity and Access Management、(IAM) ユーザーを Service Catalog ポートフォリオに追加します。このエラーは、管理アカウントにのみ関係します。

- アカウントが前提条件を満たしていない

アカウントがアカウント登録の前提条件を満たしていません。例えば、アカウントに AWS Control Tower に登録するために必要なロールと許可が不足している可能性があります。ロールを追加する手順については、「[必要な IAM ロールを既存の に手動で追加 AWS アカウント して登録する](#)」を参照してください。

AWS Control Tower に登録すると、すべての AWS アカウントで AWS CloudTrail が自動的に有効になります。登録前のアカウントで CloudTrail が有効になっている場合は、登録プロセスを開始する前に CloudTrail を非アクティブ化しない限り、二重請求が発生する可能性があります。

組織の更新

組織単位 (OU) を更新する、または OU 内の複数のアカウントを更新する最も簡単な方法は、次のいずれかのアクションを実行することです。

- が有効になっている場合AWSControlTowerBaselineは、OU を再登録します。
- が有効になっていない場合は、有効なベースラインをリセットするかAWSControlTowerBaseline、有効なコントロールをリセットします。

AWS Control Tower の OU とアカウントを更新する場合

ランディングゾーン更新を実行するときは、登録済みのアカウントを更新して、そのアカウントに新しいコントロールを適用する必要があります。

- 再登録またはリセットオプションを使用して、OU のすべてのアカウントの更新を実行できます。
- ランディングゾーンに複数の OU が登録されている場合は、すべての OUs を再登録またはリセットして、すべてのアカウントを更新します。
- 1 つのアカウントを更新するには、AWS Control Tower コンソールから を更新するか、アカウントで AWSControlTowerBaseline が有効になってい AWS Service Catalog 場合は、 でプロビジョニング済み製品の更新オプションを選択します。「[コンソールでアカウントを更新する](#)」を参照してください。

同じ OU 内の複数のアカウントの更新

すべてのアカウントと OU を更新する必要がある場合は、これらのステップを AWS Control Tower 組織の各 OU に対して繰り返します。

1 つの操作で 1 つの OU 内の複数のアカウントを更新するには

1. <https://console.aws.amazon.com/controltower> で AWS Control Tower コンソールにサインインします。
2. 左ペインのナビゲーションメニューで、[Organization] (組織) を選択します。
3. [Organization] (組織) ページで、OU を選択して [OU details] (OU の詳細ページ) を表示します。
4. OU で AWSControlTowerBaseline が有効になっている場合は、「アクション」で「OU の再登録」を選択します。OU で AWSControlTowerBaseline が有効になっていない場合は、Actions の「Reset AWS Config baseline」を選択し、「Enabled controls」セクションの「Reset control」を選択します。

または、[更新プログラムが利用できます] のステータスが表示されているアカウントを必要な数だけ選択して、[アカウントの更新] を選択することもできます。

再登録中の処理

OU を再登録すると、次のような処理が行われます。

- [State] (状態) フィールドは、アカウントが現在 AWS Control Tower に登録されているか ([Enrolled] (登録済み))、アカウントが一度も登録されたことがないか ([Not enrolled] (未登録))、以前に登録に失敗したか ([Enrollment failed] (登録に失敗しました)) を示します。
- OU を再登録すると、ステータスが [Not enrolled] (未登録) または [Enrollment failed] (登録に失敗しました) であるすべてのアカウントに AWSControlTowerExecution ロールが追加されます。
- AWS Control Tower は、それらの新規登録アカウントに Single Sign-On (IAM Identity Center) ログインを作成します。
- [Enrolled] (登録済み) のアカウントは、AWS Control Tower に再登録されます。
- SCP がデフォルトの定義に戻されるため、OU に適用されている予防コントロールのドリフトが修正されます。
- 最新のランディングゾーンの変更を反映するように、すべてのアカウントが更新されます。

詳細については、「[既存のアカウントの登録について](#)」を参照してください。

Tip

OU を再登録するときや、ランディングゾーンバージョンと複数のメンバーアカウントを更新するときに、StackSet-AWSControlTowerExecutionRole と記述されたエラーメッセージが表示されることがあります。管理アカウントのこの StackSet は、登録済みのすべてのメンバーアカウントに AWSControlTowerExecution IAM ロールが既に存在するために失敗することがあります。このエラーメッセージは想定される動作であり、無視してもかまいません。

1 つのアカウントを更新するには

Note

単一アカウントのプロビジョニング、更新、カスタマイズは、AWSControlTowerBaseline を有効にした組織単位 (OU) をターゲットにする必要があります。OU で AWSControlTowerBaseline が有効になっていない場合は、アカウントの自動登録を有効にするか、EnabledBaseline で ResetEnabledBaseline API と ResetEnabledControl APIs を使用して、その OU EnabledControls でアカウントを登録できます。EnabledBaselines

AWSControlTowerBaseline の詳細については、「」を参照してください[OU レベルで適用されるベースラインタイプ](#)。

AWS Control Tower コンソールの AWS Control Tower アカウント、または Service Catalog コンソールで、個々の AWS Control Tower アカウントを更新できます。

AWS Control Tower コンソールで 1 つのアカウントを更新するには、「[コンソールでアカウントを更新する](#)」を参照してください。

で 1 つのアカウントを更新するには AWS Service Catalog

1. AWS Service Catalog に移動します。
2. 左ペインのナビゲーションメニューで、[Provisioned products] (プロビジョニングされた製品) を選択します。
3. [Provisioned products] (プロビジョニングされた製品) ページで、更新するプロビジョニングされた製品の横にあるラジオボタンを選択します。
4. 右上の [Actions] (アクション) ドロップダウンから [Update] (更新) を選択して更新します。

での更新の詳細については AWS Service Catalog、「Service Catalog 管理者ガイド」の[Service Catalog でプロビジョニング済み製品を更新する](#)「」および「[製品の更新](#)」を参照してください。

統合サービス

AWS Control Tower は、適切に設計された環境のセットアップを支援するために、他のAWSサービス上に構築されたサービスです。この章では、基盤となるサービスの設定情報と AWS Control Tower で動作する仕組みなど、これらのサービスの概要を示します。

アーキテクチャが適切に設計された環境の評価方法の詳細については、「[AWS Well-Architected Tool](#)」を確認してください。「[管理とガバナンスクラウド環境ガイド](#)」も参照してください。

トピック

- [AWS使用可能なバックアップオプション](#)
- [を使用して環境をデプロイするCloudFormation](#)
- [CloudTrail によるイベントのモニタリング](#)
- [CloudWatch によるリソースとサービスのモニタリング](#)
- [を使用したリソース設定の管理AWS Config](#)
- [IAM によるエンティティの許可の管理](#)
- [AWS Key Management Service](#)
- [Lambda によるサーバーレスコンピューティング関数の実行](#)
- [を使用してアカウントを管理するAWS Organizations](#)
- [Simple Storage Service \(Amazon S3\) によるオブジェクトの保存](#)
- [Security Hub CSPM を使用して環境をモニタリングする](#)
- [を使用してアカウントをプロビジョニングするAWS Service Catalog](#)
- [Amazon Simple Notification Service によるアラートの追跡](#)
- [を使用して分散アプリケーションを構築するAWS Step Functions](#)

AWS使用可能なバックアップオプション

AWS Backup を使用すると、AWS Control Tower ランディングゾーンのバックアッププランを作成できます。データバックアップとリカバリのワークフローをランディングゾーンに直接組み込むことができます。バックアッププランには、保持日数、バックアップの頻度、バックアップが発生する時間枠などの事前定義済みのルールが含まれます。詳細については、「[AWS Backup と AWS Control Tower](#)」を参照してください。

を使用して環境をデプロイするCloudFormation

CloudFormationを使用すると、AWSインフラストラクチャのデプロイを予測どおりに繰り返し作成およびプロビジョニングできます。これにより、基盤となるAWSインフラストラクチャの作成と設定を心配することなく、AWS製品を活用して、信頼性とスケーラビリティに優れたコスト効率の高いアプリケーションをクラウドで構築できます。テンプレートファイルを使用して、リソースのコレクションを1つのユニット (スタック) としてまとめて作成および削除CloudFormationできます。詳細については、「[AWS CloudFormationユーザーガイド](#)」を参照してください。

AWS Control Tower はCloudFormationスタックセットを使用してアカウントにコントロールを適用します。CloudFormationと AWS Control Tower の連携の詳細については、「[を使用して AWS Control Tower リソースを作成する AWS CloudFormation](#)」を参照してください。

CloudTrail によるイベントのモニタリング

AWS Control Tower は、一元的なログ記録と監査を有効にするAWS CloudTrailように を設定します。CloudTrail では、管理アカウントが管理アクションとライフサイクルイベントを確認できます。

CloudTrail は、アカウントのAWS API コールの履歴を保持することで、クラウド内のAWS環境をモニタリングするのに役立ちます。例えば、CloudTrail をサポートするサービスのAWS APIsを呼び出したユーザーとアカウント、呼び出し元のソース IP アドレス、呼び出しが発生した時間を特定できます。API を使用して CloudTrail をアプリケーションに統合したり、組織用の追跡作成を自動化したり、追跡の状態を確認したり、CloudTrail のログ記録のオン/オフを管理者が切り替える方法を制御したりすることもできます。詳細については、「[AWS CloudTrailユーザーガイド](#)」を参照してください。

CloudWatch によるリソースとサービスのモニタリング

Amazon CloudWatch は、信頼性、拡張性、柔軟性に優れた数分で使用を開始できるモニタリングソリューションです。お客様はもはや、独自のモニタリングシステムやインフラストラクチャをセットアップ、管理、拡張する必要はありません。詳細については、「[Amazon CloudWatch ユーザーガイド](#)」を参照してください。

AWS Control Tower で Amazon CloudWatch を使用方法の詳細については、「[Monitoring](#)」 (モニタリング) を参照してください。

を使用したリソース設定の管理AWS Config

AWS Configは、AWSアカウントに関連付けられたリソースの詳細ビューを提供します。これには、リソースの設定方法、相互の関係、設定とその関係が時間の経過とともにどのように変化したかが含まれます。詳細については、「[AWS Configデベロッパーガイド](#)」を参照してください。

AWS Control Tower によってプロビジョニングされたAWS Configリソースには、aws-control-tower および値 managed-by-control-tower が自動的にタグ付けされます。

が AWS Control Tower でリソースをAWS Configモニタリングおよび記録する方法、およびリソースに対して請求する方法の詳細については、「」を参照してください[でリソースの変更をモニタリングする AWS Config](#)。

AWS Control Tower はAWS Config ルールを使用して検出コントロールを実装します。詳細については、「[About controls in AWS Control Tower](#)」を参照してください。

Control Tower ランディングゾーン 4.0 での AWS Config の統合

サービスにリンクされた Config Aggregator (SLCA)

AWS Control Tower は、ランディングゾーン 4.0 以降の一部としてサービスにリンクされた Config Aggregator (SLCA) を実装するようになりました。この変更は、組織全体での AWS Config データの集約と管理方法の大幅な改善を表します。

主な変更点

新しいサービスにリンクされた Config Aggregator のデプロイ

- サービスにリンクされた Config Aggregator は、指定された AWS Config 統合アカウントにデプロイされます。
- 既存の顧客の場合、これは監査アカウントになります
- 新規のお客様の場合、これはマニフェストの config.accountIdフィールドで指定されたアカウントになります。

委任された管理者

- AWS Config アグリゲータアカウントが AWS Config の委任管理者になる
- AWS Control Tower は委任管理者設定を自動的に設定します

- これにより、組織全体で AWS Config を一元管理できます。

レガシーアグリゲータからの移行

ランディングゾーン 4.0 へのアップグレード中:

- 管理アカウントの組織アグリゲータが削除されます。
- 監査アカウントのアカウントアグリゲータは削除されます。
- これらは、AWS Config 統合アグリゲータアカウントの新しいサービスにリンクされた Config アグリゲータに置き換えられます。

拡張データ集約

サービスにリンクされた Config Aggregator は、Config データ集約の機能を改善しました。

- 組織内の任意の AWS Config レコーダーからデータを集約できます
- Control Tower によって管理されていないアカウントのデータが含まれます
- 組織全体の設定項目の包括的なビューを提供します。
- 拡張データ境界コントロールをサポート

重要な考慮事項

委任管理者設定

- AWS Control Tower は、AWS Config 統合のマニフェストで指定されたアカウントを使用します。
- このアカウントは、委任管理者として自動的に設定されます。
- この設定では、顧客からの追加のアクションは必要ありません。
- 既存のお客様の場合、以前のセキュリティロール統合アカウント (監査アカウント) は、ランディングゾーン 4.0 のアップグレード中に AWS Config 中央アグリゲータアカウントとして設定されます。

データ集約範囲

- サービスにリンクされた Config Aggregator は、以下から設定データを集約できます。
 - Control Tower マネージドアカウント

- Control Tower 以外のマネージドアカウント
- 組織内でアクティブな Config レコーダーを持つすべてのアカウント

アクセスコントロール

- 集約データへのアクセスは IAM ポリシーを通じて管理されます
- AWS Config 中央アグリゲータアカウントは、すべての集約データに一元的にアクセスできます
- メンバーアカウントは、個々の AWS Config レコーダーを維持します。

ベストプラクティス

Config セントラルアグリゲータアカウントの選択

- セキュリティとコンプライアンスのモニタリング専用のアカウントを選択する
- 適切なアクセスコントロールが設定されていることを確認する
- 既存の監査アカウントまたはセキュリティアカウントの使用を検討する

データ管理

- 集約された設定データを定期的に確認する
- 適切な保持ポリシーを実装する
- アカウント間で AWS Config レコーダーのステータスをモニタリングする

移行の影響

ランディングゾーン 4.0 にアップグレードする場合:

移行前

- 既存の AWS Config ルールとアグリゲータを文書化する
- 現在の AWS Config データアクセスパターンを確認する
- 必要な IAM ポリシーの更新を計画する

移行中

- レガシー AWS Config アグリゲータは自動的に削除されます
- サービスにリンクされた Config Aggregator がデプロイされます
- 委任された管理者が設定されます

移行後

- サービスにリンクされた Config Aggregator が正しく機能することを確認する
- メンバーアカウントからのデータ集約を確認する
- 必要に応じてモニタリングツールとレポートツールを更新する

IAM によるエンティティの許可の管理

AWS Identity and Access Management(IAM) は、他のAWSサービスへのアクセスを制御するためのAWSサービスです。IAM を使用すると、ユーザー、アクセスキーなどのセキュリティ認証情報、およびアクセス許可を一元管理して、ユーザーとアプリケーションにアクセス権が付与されるAWSリソースを指定できます。

ランディングゾーンのセットアップ時に、ID プロバイダーとして IAM を選択すると、AWS IAM アイデンティティセンターに対して多数のグループを自動的に作成できます。これらのグループには、IAM から事前定義された許可ポリシーである許可セットがあります。また、エンドユーザーも IAM を使用して、IAM ユーザーおよびメンバーアカウント内のその他のエンティティに許可の範囲を定義できます。

AWS Identity and Access Management(IAM) は、AWSアカウントとビジネスアプリケーションへのアクセスを管理する方法を簡素化します。AWS Control Tower 内のすべての AWS アカウントについて、IAM Identity Center へのアクセスとユーザーアクセス許可を制御できます。

詳細については、「[AWS IAM アイデンティティセンターユーザーガイド](#)」を参照してください。

IAM をサポートAWS リージョンしていない を拠点としている場合は、別の ID プロバイダーを導入して、独自のユーザーとグループを手動で設定および維持できます。

AWS Key Management Service

AWS Key Management Service(AWS KMS) では、データを保護するキーを作成および制御できます。AWS Control Tower では、オプションで暗号化キーを使用してデータをAWS KMS暗号化できます。詳細についてはAWS KMS、[AWS KMS デベロッパーガイド](#)を参照してください。

AWS Control Tower でAWS KMSキーを設定する方法については、[「オプションでAWS KMSキーを設定する」](#)を参照してください。

Lambda によるサーバーレスコンピューティング関数の実行

を使用するとAWS Lambda、サーバーのプロビジョニングや管理を行わずにコードを実行できます。余分な管理オーバーヘッドが発生することなく、多くのタイプのアプリケーションやバックエンドサービスのコードを実行できます。コードをアップロードすると、Lambda が高い可用性でコードを実行および拡張できます。他のAWSのサービスから自動的にトリガーするようにコードをセットアップすることも、ウェブやモバイルアプリケーションから直接コードを呼び出すこともできます。

例えば、AWS Control Tower 監査アカウントでは特定のロールをプログラムで引き受けることができるため、Lambda を使用して他のアカウントを確認できます。また、AWS Control Tower ラifecycleイベントを使用して、Lambda 関数をトリガーすることもできます。

を使用してアカウントを管理するAWS Organizations

AWS Organizationsは、作成して一元管理する組織に複数のAWSアカウントを統合することができるアカウント管理サービスです。Organizations では、メンバーアカウントを作成して、既存のアカウントを組織に招待できます。それらのアカウントをグループ分けしたり、ポリシーに基づいて管理したりできます。詳細については、「[AWS Organizationsユーザーガイド](#)」を参照してください。

AWS Control Tower では、Organizations は請求の一元管理、アクセス、コンプライアンス、セキュリティの制御、メンバーAWSアカウント間でのリソースの共有に役立ちます。アカウントは、組織単位 (OU) と呼ばれる論理グループに分類されます。Organizations の詳細については、「[AWS Organizationsユーザーガイド](#)」を参照してください。

AWS Control Tower は、次の OU を使用します。

- Root - すべてのアカウントおよびランディングゾーンにある他のすべての OU の親コンテナです。
- Security - この OU には、ログアーカイブアカウント、監査アカウント、および所有されているリソースが含まれます。
- Sandbox - この OU は、ランディングゾーンをセットアップすると作成されます。この OU とランディングゾーンにあるその他の子 OU には、メンバーアカウントが含まれています。エンドユーザーは、AWSリソースで処理を実行するためにこれらのアカウントにアクセスします。

Note

AWS Control Tower コンソールから [Organizational units] (組織単位) ページで他の OU をランディングゾーンに追加できます。

考慮事項

AWS Control Tower によって作成された OU にコントロールを適用できます。AWS Control Tower の外部で作成された OU には、デフォルトでは適用できません。ただし、そのような OU を登録できます。OU を登録したら、その OU とそのアカウントにコントロールを適用できます。OU の登録については、「[Register an existing organizational unit with AWS Control Tower](#)」を参照してください。

Simple Storage Service (Amazon S3) によるオブジェクトの保存

Amazon Simple Storage Service (Amazon S3) は、インターネット用のストレージです。Simple Storage Service (Amazon S3) を使用すると、いつでもウェブ上の任意の場所から任意の量のデータを保存および取得できます。AWS マネジメントコンソールのシンプルかつ直感的なウェブインターフェイスを使用して、これらのタスクを実行できます。詳細については、「[Amazon Simple Storage Service ユーザーガイド](#)」を参照してください。

ランディングゾーンのセットアップ時に、ランディングゾーン内にあるすべてのアカウントのすべてのログを含めるための Simple Storage Service (Amazon S3) バケットがログアーカイブアカウントに作成されます。

Security Hub CSPM を使用して環境をモニタリングする

AWS Control Tower はAWS、サービスマネージドスタンダード: AWS Control Tower と呼ばれる Security Hub CSPM 標準によって Security Hub CSPM と統合されています。詳細については、「[Security Hub standard](#)」を参照してください。

を使用してアカウントをプロビジョニングするAWS Service Catalog

AWS Service Catalogを使用すると、IT 管理者は承認された製品のポートフォリオを作成、管理、配布し、エンドユーザーはパーソナライズされたポータルで必要な製品にアクセスできます。一般的な

製品には、AWSリソースを使用してデプロイされるサーバー、データベース、ウェブサイト、またはアプリケーションが含まれます。

特定の製品にアクセスできるユーザーを制御できます。これにより、組織のビジネス標準へのコンプライアンスを実現したり、製品のライフサイクルを管理したり、ユーザーが確実に製品を見つけて起動したりできるようにすることが可能です。詳細については、「[Service Catalog 管理者ガイド](#)」を参照してください。

AWS Control Tower では、中央クラウド管理者とエンドユーザーは、カスタムブループリントと呼ばれるAWS Service Catalog製品を使用して、ランディングゾーンにカスタムアカウントをプロビジョニングできます。詳細については、「[Step2.AWS Service Catalog製品を作成します](#)」。

AWS Service Catalogコンソールと APIs を使用して AWS Control Tower アカウントとやり取りできます。詳細については、[から AWS Control Tower アカウントを操作する AWS Service Catalog](#)を参照してください。

AWS Control Tower は、Service Catalog API を使用して、アカウントのプロビジョニングと更新をさらに自動化することもできます。詳細については、「[AWS Service Catalogデベロッパーガイド](#)」を参照してください。

Amazon Simple Notification Service によるアラートの追跡

Amazon Simple Notification Service (Amazon SNS) は、アプリケーション、エンドユーザー、およびデバイスでクラウドから通知を瞬時に送受信できるようにするウェブサービスです。詳細については、「[Amazon Simple Notification Service デベロッパーガイド](#)」を参照してください。

AWS Control Tower では、Amazon SNS を使用して、管理アカウントおよび監査アカウントの E メールアドレスにプログラムによるアラートを送信します。これらのアラートは、ランディングゾーン内でのドリフトの防止に役立ちます。詳細については、「[AWS Control Tower でドリフトを検出および解決する](#)」を参照してください。

また、Amazon Simple Notification Service を使用してコンプライアンス通知を送信しますAWS Config。

Tip

AWS Control Tower コントロールのコンプライアンス通知を (監査アカウントで) 受信する最良の方法の 1 つは、AggregateConfigurationNotifications をサブスクライブすることです。コンプライアンスの検査に役立つサービスです。これは、コンプライアンスから外

れるルールに関するAWS Config実際のデータを提供します。は、OU 内のアカウントのリストAWS Configを自動的に維持します。

Eメールを使用するか、SNS が許可する任意のタイプのサブスクリプションを使用して、手動でサブスクライブする必要があります。ステートメント `arn:aws:sns:homeregion:account:aws-controltower-AggregateSecurityNotifications` により、監査アカウントにつながります。

を使用して分散アプリケーションを構築するAWS Step Functions

AWS Step Functionsを使用すると、分散アプリケーションのコンポーネントをビジュアルワークフローの一連のステップとして簡単に調整できます。ステートマシンをすばやく構築および実行し、アプリケーションのステップを信頼性が高くスケーラブルな方法で実行できます。詳細については、「[AWS Step Functionsデベロッパーガイド](#)」を参照してください。

AWS Control Tower の Identity and Access Management

Account Factory でのアカウントのプロビジョニングや AWS Control Tower コンソールでの新しい組織単位 (OUs) の作成など、ランディングゾーンでオペレーションを実行するには、AWS Identity and Access Management (IAM) または承認済み AWS ユーザーであることを認証 AWS IAM アイデンティティセンター する必要があります。例えば、AWS Control Tower コンソールを使用している場合は、管理者から提供された AWS 認証情報を指定して ID を認証します。

ID を認証すると、IAM は特定のオペレーションとリソースに対する一連の定義されたアクセス許可 AWS を使用して へのアクセスを制御します。アカウント管理者である場合、IAM を使用して、アカウントに関連付けられたリソースへの他の IAM ユーザーのアクセスをコントロールできます。

トピック

- [認証](#)
- [アクセスコントロール](#)
- [IAM Identity Center AWS と AWS Control Tower の使用](#)
- [AWS Control Tower リソースに対するアクセス許可の管理の概要](#)
- [クロスサービス偽装の防止](#)
- [AWS Control Tower でアイデンティティベースのポリシー \(IAM ポリシー\) を使用する](#)

認証

には、次のいずれかのタイプの ID AWS としてアクセスできます。

- AWS アカウントルートユーザー – AWS アカウントを初めて作成するときは、アカウント内のすべての AWS サービスとリソースへの完全なアクセス権を持つ ID から始めます。このアイデンティティは、AWS アカウントのルートユーザーと呼ばれます。アカウントの作成に使用した E メールアドレスとパスワードでサインインすると、このアイデンティティにアクセスできます。日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことを強くお勧めします。代わりに、[最初の IAM Identity Center ユーザー \(推奨\) または IAM ユーザー \(ほとんどの場合にベストプラクティスではない\) を作成するためにのみ、ルートユーザーを使用するというベストプラクティス](#)に従います。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。詳細については、「[ルートユーザーとしてサインインする場合](#)」を参照してください。

- IAM ユーザー – [IAM ユーザー](#)は、特定のカスタマイズされたアクセス許可を持つ AWS アカウント内の ID です。IAM ユーザー認証情報を使用して、マネジメントコンソール、AWS ディスカッションフォーラム、AWS サポートセンターなどの AWS 安全な AWS ウェブページにサインインできます。AWS のベストプラクティスでは、IAM ユーザーではなく IAM Identity Center ユーザーを作成することをお勧めします。これは、長期的な認証情報を持つ IAM ユーザーを作成すると、セキュリティ上のリスクが高くなるためです。

特定の目的で IAM ユーザーを作成する必要がある場合は、サインイン認証情報に加えて、IAM ユーザーごとにアクセスキーを作成できます。これらのキーは、複数の SDKs のいずれかを介して、または コマンドラインインターフェイス (CLI) AWS を使用して、プログラムで AWS サービスを呼び出すときに使用できます。SDK と CLI ツールでは、アクセスキーを使用してリクエストが暗号で署名されます。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。AWS Control Tower では、署名バージョン 4 がサポートされています。これは、インバウンド API リクエストを認証するためのプロトコルです。リクエストの認証の詳細については、AWS 全般のリファレンスの[署名バージョン 4 の署名プロセス](#)を参照してください。

- IAM ロール – [IAM ロール](#)は、アカウントで作成して特定の許可を付与できる IAM ID です。IAM ロールは、AWS アイデンティティであるという点で IAM ユーザーと似ており、アイデンティティが **できることとできないこと**を決定するアクセス許可ポリシーがあります AWS。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。IAM ロールと一時的な認証情報は、次の状況で役立ちます:
- フェデレーティッドユーザーアクセス – IAM ユーザーを作成する代わりに、Directory Service、エンタープライズユーザーディレクトリ、またはウェブ ID プロバイダーから既存の ID を使用できます。これらはフェデレーティッドユーザーと呼ばれます。は、ID プロバイダーを介してアクセスがリクエストされると、フェデレーティッドユーザーにロールを AWS 割り当てます。フェデレーションユーザーの詳細については、「IAM ユーザーガイド」の「[フェデレーションユーザーとロール](#)」を参照してください。
- AWS サービスアクセス – サービスロールは、サービスがユーザーに代わってアカウントでアクションを実行するために引き受ける IAM ロールです。一部の AWS サービス環境を設定するときは、サービスが引き受けるロールを定義する必要があります。このサービスロールには、サービスが必要な AWS リソースにアクセスするために必要なすべてのアクセス許可が含まれている必要があります。サービスロールはサービスによって異なりますが、多くのサービスロールでは、そのサービスの文書化された要件を満たしている限り、許可を選択することができます。サービスロールは、お客様のアカウント内のみでアクセスを提供します。他のアカウントのサー

ビスへのアクセス権を付与するためにサービスロールを使用することはできません。IAM 内部からサービスロールを作成、修正、削除できます。例えば、Amazon Redshift がユーザーに代わって Simple Storage Service (Amazon S3) バケットにアクセスし、そのバケットのデータを Amazon Redshift クラスターにロードすることを許可するロールを作成できます。詳細については、IAM ユーザーガイドの「[AWS サービスにアクセス許可を委任するロールの作成](#)」を参照してください。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、Amazon EC2 インスタンスで実行され、CLI または AWS API AWS リクエストを行っているアプリケーションの一時的な認証情報を管理できます。これは、Amazon EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを Amazon EC2 インスタンスに割り当て、そのすべてのアプリケーションで使えるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、Amazon EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得することができます。詳細については、「IAM ユーザーガイド」の「[Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する](#)」を参照してください。
- IAM Identity Center ユーザー IAM Identity Center ユーザーポータルに対する認証は、IAM Identity Center に接続したディレクトリによって制御されます。ただし、ユーザーポータル内からエンドユーザーが利用できる AWS アカウントへの認可は、次の 2 つの要因によって決まります。
- IAM Identity Center コンソールで AWS それらの AWS アカウントへのアクセス権が割り当てられているユーザー。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「[シングルサインオンアクセス](#)」を参照してください。
- それらの AWS アカウントに適切なアクセス権を許可するために、AWS IAM Identity Center コンソールでエンドユーザーにどのレベルのアクセス許可が付与されているか。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「[許可セット](#)」を参照してください。

アクセスコントロール

ランディングゾーンで AWS Control Tower リソースまたは他の AWS リソースを作成、更新、削除、または一覧表示するには、オペレーションを実行するためのアクセス許可と、対応するリソースにアクセスするためのアクセス許可が必要です。また、プログラムでオペレーションを実行するには、有効なアクセスキーが必要です。

以下のセクションでは、AWS Control Tower の許可を管理する方法について説明します。

トピック

- [AWS Control Tower リソースに対するアクセス許可の管理の概要](#)
- [AWS Control Tower でアイデンティティベースのポリシー \(IAM ポリシー\) を使用する](#)

IAM Identity Center AWS と AWS Control Tower の使用

AWS Control Tower では、IAM Identity Center により、中央のクラウド管理者とエンドユーザーが複数の AWS アカウントとビジネスアプリケーションへのアクセスを管理できます。デフォルトでは、ID とアクセス制御を自己管理するオプションを選択していない限り、AWS Control Tower はこのサービスを使用して、Account Factory を通じて作成されたアカウントへのアクセスを設定および管理します。

ID プロバイダーの選択については、「[IAM Identity Center のガイダンス](#)」を参照してください。

AWS Control Tower での IAM Identity Center ユーザーおよび許可のセットアップ方法に関する簡単なチュートリアルについては、こちらの動画 (所要時間: 6 分 23 秒) をご覧ください。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower AWS での IAM Identity Center のセットアップのビデオチュートリアル。](#)

IAM Identity Center での AWS Control Tower のセットアップについて

AWS Control Tower の初期セットアップの時点では、ルートユーザーと適切な許可を持つ IAM ユーザーのみ、IAM Identity Center ユーザーを追加できます。ただし、エンドユーザーが [AWSAccountFactory] グループに追加されると、Account Factory ウィザードから新しい IAM Identity Center ユーザーを作成できるようになります。詳細については、「[Account Factory でのアカウントのプロビジョニングと管理](#)」を参照してください。

推奨されるデフォルトを選択した場合、AWS Control Tower は、ランディングゾーンを事前設定済みディレクトリでセットアップするため、ユーザーがアカウント間でフェデレーティッドアクセスを持つように、ユーザーアイデンティティとシングルサインオンを管理できます。ランディングゾーンのセットアップ時に、このデフォルトディレクトリはユーザーグループと許可セットを含むように作成されます。

Note

IAM Identity Center の委任管理者機能を使用して、組織 AWS IAM アイデンティティセンター内の管理を管理アカウント以外のアカウントに委任できます。この機能を使用する

場合、メンバーシップを管理するアクセス権を持つ管理者は、管理アカウントに割り当てられたグループも管理できることに注意してください。詳細については、ブログ記事「[Getting started with AWS SSO delegated administration](#)」を参照してください。

ユーザーグループ、ロール、アクセス許可セット

ユーザーグループは、共有アカウント内で定義された特殊なロールを管理します。ロールは、一緒に属する許可のセットを確立します。グループのすべてのメンバーは、グループに関連付けられた許可セットやロールを継承します。メンバーアカウントのエンドユーザー用に新しいグループを作成して、グループが実行する特定のタスクに必要なロールのみをカスタムに割り当てることができます。

使用できる許可セットは、読み取り専用アクセス、AWS Control Tower 管理アクセス、Service Catalog アクセスなど、異なるユーザー許可の幅広い要件に対応しています。これらのアクセス許可セットにより、エンドユーザーはエンタープライズのガイドラインに従って、ランディングゾーンに独自の AWS アカウントをすばやくプロビジョニングできます。

ユーザー、グループ、および許可の割り当てを計画するためのヒントについては、「[グループ、ロール、ポリシーを設定する上での推奨事項](#)」を参照してください。

AWS Control Tower のコンテキストでこのサービスを使用する方法の詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」で次のトピックを参照してください。

- ユーザーを追加するには、「[ユーザーを追加する](#)」を参照してください。
- グループにユーザーを追加するには、「[グループにユーザーを追加する](#)」を参照してください。
- ユーザーのプロパティを編集するには、「[ユーザーのプロパティの編集](#)」を参照してください。
- グループを追加するには、「[グループの追加](#)」を参照してください。

Warning

AWS Control Tower は、ホームリージョンに IAM Identity Center ディレクトリをセットアップします。ランディングゾーンを別のリージョンにセットアップして IAM Identity Center コンソールに移動する場合は、そのリージョンをホームリージョンに変更する必要があります。ホームリージョンの IAM Identity Center 設定は削除しないでください。

IAM Identity Center アカウントと AWS Control Tower に関する注意事項

ここでは、AWS Control Tower で IAM Identity Center ユーザーアカウントを使用する際の注意事項をいくつか紹介します。

- IAM Identity Center ユーザーアカウントが無効になっている場合、Account Factory AWS で新しいアカウントをプロビジョニングしようとする、エラーメッセージが表示されます。IAM Identity Center コンソールで IAM Identity Center ユーザーを再度有効にすることができます。
- Account Factory によって発行されたアカウントに関連付けられたプロビジョニング済み製品を更新するときに、新しい IAM Identity Center ユーザーの E メールアドレスを指定すると、AWS Control Tower によって新しい IAM Identity Center ユーザーアカウントが作成されます。以前に作成したユーザーアカウントは削除されません。AWS IAM Identity Center から以前の IAM Identity Center ユーザーの E メールアドレスを削除する場合は、[Disabling a User](#) (ユーザーを無効にする) を参照してください。
- AWS IAM Identity Center は [Azure Active Directory と統合](#)されており、既存の Azure Active Directory を AWS Control Tower に接続できます。
- AWS Control Tower の動作が IAM Identity Center およびさまざまな ID ソースと AWS どのように相互作用するかの詳細については、IAM Identity Center ドキュメントの「[ID ソースの変更に關する考慮事項](#)」を参照してください。AWS

AWS Control Tower の IAM Identity Center グループ

AWS Control Tower では、アカウントで特定のタスクを実行するユーザーを編成するために事前設定されたグループを利用できます。ユーザーを追加して、IAM Identity Center で直接これらのグループに割り当てることができます。これにより、アカウント内では許可セットがグループのユーザーに一致します。グループの設定に関する最新のガイダンスとベストプラクティスについては、「IAM Identity Center ユーザーガイド」の「[ベストプラクティス](#)」を参照してください。

ランディングゾーンをセットアップすると、以下のグループが作成されます。

AWSAccountFactory

アカウント	許可セット	説明
管理アカウント	AWSServiceCatalogE ndUserAccess	このグループは、Account Factory を使用して新しいアカウントをプロビジョニングす

アカウント	許可セット	説明
		るためにこのアカウントでのみ使用されます。

AWSServiceCatalogAdmins

アカウント	許可セット	説明
管理アカウント	AWSServiceCatalogAdminFullAccess	このグループは、Account Factory で管理者権限を変更するためにこのアカウントでのみ使用されます。このグループのユーザーは、AWSAccountFactory グループにも含まれていない限り新しいアカウントをプロビジョニングできません。

AWSControlTowerAdmins

アカウント	許可セット	説明
管理アカウント	AWSAdministratorAccess	AWS Control Tower コンソールにアクセスできるのは、このアカウントのこのグループのユーザーのみです。
ログアーカイブアカウント	AWSAdministratorAccess	ユーザーは、このアカウントで管理者アクセスが与えられます。
監査アカウント	AWSAdministratorAccess	ユーザーは、このアカウントで管理者アクセスが与えられます。

アカウント	許可セット	説明
メンバーアカウント	AWSOrganizationsFullAccess	ユーザーは、このアカウントで Organizations へのフルアクセスが与えられます。

AWS Security Audit Power Users

アカウント	許可セット	説明
管理アカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行し、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。
ログアーカイブアカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行し、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。
監査アカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行し、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。
メンバーアカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行し、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。

AWSSecurityAuditors

アカウント	許可セット	説明
管理アカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースに読み取り専用でアクセスできます。
ログアーカイブアカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースに読み取り専用でアクセスできます。
監査アカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースに読み取り専用でアクセスできます。
メンバーアカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースに読み取り専用でアクセスできます。

AWSLogArchiveAdmins

アカウント	許可セット	説明
ログアーカイブアカウント	AWSAdministratorAccess	ユーザーは、このアカウントで管理者アクセスが与えられます。

AWSLogArchiveViewers

アカウント	許可セット	説明
ログアーカイブアカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスと

アカウント	許可セット	説明
		リソースに読み取り専用でアクセスできます。

AWSAuditAccountAdmins

アカウント	許可セット	説明
監査アカウント	AWSAdministratorAccess	ユーザーは、このアカウントで管理者アクセスが与えられます。

AWS Control Tower リソースに対するアクセス許可の管理の概要

すべての AWS リソースは、によって所有され AWS アカウント、リソースを作成またはアクセスするためのアクセス許可はアクセス許可ポリシーによって管理されます。アカウント管理者は、IAM アイデンティティ (つまり、ユーザー、グループ、ロール) に許可ポリシーをアタッチできます。一部のサービス (など AWS Lambda) では、リソースへのアクセス許可ポリシーのアタッチもサポートされています。

Note

アカウント管理者 (または管理者) は、管理者権限を持つユーザーです。詳細については、「IAM ユーザーガイド」の「[IAM のベストプラクティス](#)」を参照してください。

ユーザーまたはロールに権限を付与する責任を負う場合は、権限を必要とするユーザーとロール、各ユーザーとロールが権限を必要とするリソース、およびそれらのリソースを操作するために許可する必要がある特定のアクションを把握して追跡する必要があります。

トピック

- [AWS Control Tower のリソースとオペレーション](#)
- [リソース所有権について](#)
- [リソースへのアクセスの管理](#)
- [ポリシー要素を指定: アクション、効果、プリンシパル](#)

- [ポリシーでの条件の指定](#)

AWS Control Tower のリソースとオペレーション

AWS Control Tower では、プライマリリソースはランディングゾーンです。AWS Control Tower では、追加のリソースタイプ、コントロール (ガードレールと呼ばれることもあります) もサポートされています。ただし、AWS Control Tower では、既存のランディングゾーンのコンテキストでのみコントロールを管理できます。コントロールはサブリソースと呼ぶことができます。

のリソースとサブリソース AWS には、次の例に示すように、一意の Amazon リソースネーム (ARNs) が関連付けられています。

AWS Control Tower には、AWS Control Tower リソースと連携するための一連の API オペレーションが用意されています。利用可能なオペレーションのリストについては、「[AWS Control Tower API リファレンス](#)」の「AWS Control Tower」を参照してください。

AWS Control Tower の CloudFormation リソースの詳細については、[ユーザーガイドを参照してください AWS CloudFormation](#)。

リソース所有権について

AWS アカウントは、リソースを作成したユーザーに関係なく、アカウントで作成されたリソースを所有します。具体的には、リソース所有者は、リソース作成リクエストを認証する[プリンシパルエントティ](#) (AWS アカウント ルートユーザー、IAM アイデンティティセンターユーザー、IAM ユーザー、または IAM ロール) の AWS アカウントです。次の例は、この仕組みを示しています。

- AWS アカウントのアカウントルートユーザー認証情報を使用してランディングゾーン AWS を設定する場合、AWS アカウントはリソースの所有者です。
- AWS アカウントに IAM ユーザーを作成し、そのユーザーにランディングゾーンを設定するアクセス許可を付与する場合、そのユーザーは、アカウントが前提条件を満たしている限り、ランディングゾーンを設定できます。ただし、ユーザーが属する AWS アカウントがランディングゾーンリソースを所有しています。
- ランディングゾーンを設定するアクセス許可を持つ AWS アカウントに IAM ロールを作成すると、そのロールを引き受けることのできるすべてのユーザーがランディングゾーンを設定できます。ロールが属する AWS アカウントは、ランディングゾーンリソースを所有します。

リソースへのアクセスの管理

アクセス権限ポリシー では、誰が何にアクセスできるかを記述します。以下のセクションで、アクセス許可ポリシーを作成するために使用可能なオプションについて説明します。

Note

このセクションでは、AWS Control Tower のコンテキストでの IAM の使用について説明します。IAM サービスに関する詳しい説明はしません。完全な IAM ドキュメンテーションについては、「IAM ユーザーガイド」の「[IAM とは](#)」を参照してください。IAM ポリシー構文の詳細と説明については、「IAM ユーザーガイド」の「[AWS IAM ポリシーリファレンス](#)」を参照してください。

IAM アイデンティティにアタッチされているポリシーは、アイデンティティベースのポリシー (IAM ポリシー) と呼ばれます。リソースにアタッチされたポリシーは、リソースベースのポリシーと呼ばれます。

Note

AWS Control Tower では、アイデンティティベースのポリシー (IAM ポリシー) のみサポートされます。

トピック

- [アイデンティティベースのポリシー \(IAM ポリシー\) について](#)
- [ロールを作成して、アクセス許可を割り当てる](#)
- [リソースベースのポリシー](#)

アイデンティティベースのポリシー (IAM ポリシー) について

ポリシーを IAM アイデンティティにアタッチできます。例えば、次の操作を実行できます。

- アカウントのユーザーまたはグループに許可ポリシーをアタッチする – ランディングゾーンのセットアップなどの AWS Control Tower リソースを作成するユーザー許可を付与するために、ユーザーまたはユーザーが所属するグループに許可ポリシーをアタッチできます。

- 許可ポリシーをロールにアタッチする (クロスアカウントの許可を付与) – アイデンティティベースのアクセス許可ポリシーを IAM ロールにアタッチして、クロスアカウントの許可を付与することができます。たとえば、ある AWS アカウントの管理者 (アカウント A) は、別のアカウント (AWS アカウント B) にクロスアカウントアクセス許可を付与するロールを作成したり、別の AWS サービスにアクセス許可を付与するロールを作成したりできます。
- アカウント A の管理者は IAM ロールを作成し、そのロールに、アカウント A のリソースを管理する許可を付与する権限ポリシーをアタッチします。
 - アカウント A の管理者は、ロールに信頼ポリシーをアタッチします。ポリシーは、ロールを引き受けることのできるプリンシパルとしてアカウント B を識別します。
 - プリンシパルとして、アカウント B の管理者は、アカウント B のすべてのユーザーにそのロールを引き受ける権限を与えることができます。このロールを引き受けることで、アカウント B のユーザーはアカウント A のリソースを作成したり、アクセスしたりできます。
 - AWS サービスにロールを引き受ける機能 (アクセス許可) を付与するには、信頼ポリシーで指定するプリンシパルを AWS サービスにすることができます。

ロールを作成して、アクセス許可を割り当てる

ロールとアクセス許可により、AWS Control Tower や AWS の他のサービスのリソースにアクセスできます。これにはリソースへのプログラムによるアクセスも含まれます。

アクセスを提供するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM アイデンティティセンター:

アクセス許可セットを作成します。「AWS IAM アイデンティティセンター ユーザーガイド」の「[アクセス許可セットを作成する](#)」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

ID フェデレーションのロールを作成します。詳細については IAM ユーザーガイドの [サードパーティー ID プロバイダー \(フェデレーション\) 用のロールを作成する](#) を参照してください。

- IAM ユーザー:

- ユーザーが担当できるロールを作成します。手順については IAM ユーザーガイドの [IAM ユーザーのロールの作成](#) を参照してください。

- (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。IAM ユーザーガイドの [ユーザー \(コンソール\) へのアクセス許可の追加](#) の指示に従います。

IAM を使用した許可の委任の詳細については、「IAM ユーザーガイド」の「[アクセス管理](#)」を参照してください。

 Note

AWS Control Tower のランディングゾーンを設定するときは、AdministratorAccess 管理ポリシーを持つユーザーまたはロールが必要です。(arn: aws: iam:: aws: policy/ AdministratorAccess)

のロールを作成するには AWS のサービス (IAM コンソール)

1. にサインイン AWS マネジメントコンソール し、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
4. [サービスまたはユースケース] でサービスを選択し、次にユースケースを選択します。ユースケースは、サービスに必要な信頼ポリシーを含める定義になります。
5. [次へ] を選択します。
6. [アクセス許可ポリシー] では、オプションは選択したユースケースによって異なります。
 - サービスがロールのアクセス許可を定義している場合、アクセス許可ポリシーを選択することはできません。
 - 制限されたアクセス許可ポリシーのセットから選択します。
 - すべてのアクセス許可ポリシーから選択します。
 - アクセス許可ポリシーを選択するのではなく、ロールの作成後にポリシーを作成し、そのポリシーをロールにアタッチします。
7. (オプション) [アクセス許可の境界](#)を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。
 - a. [アクセス許可の境界の設定] セクションを開き、[アクセス許可の境界を使用してロールのアクセス許可の上限を設定する] を選択します。

IAM には、 アカウントの AWS 管理ポリシーとカスタマー管理ポリシーのリストが含まれます。
 - b. アクセス許可の境界として使用するポリシーを選択します。

8. [次へ] を選択します。
9. [ロール名] では、オプションはサービスによって異なります。
 - サービスでロール名が定義されている場合、ロール名を編集することはできません。
 - サービスでロール名のプレフィックスが定義されている場合、オプションのサフィックスを入力できます。
 - サービスでロール名が定義されていない場合、ロールに名前を付けることができます。

 Important

ロールに名前を付けるときは、次のことに注意してください。

- ロール名は 内で一意である必要があり AWS アカウント、大文字と小文字を区別することはできません。

例えば、**PRODRROLE** と **prodrole** の両方の名前でロールを作成することはできません。ロール名がポリシーまたは ARN の一部として使用される場合、ロール名は大文字と小文字が区別されます。ただし、サインインプロセスなど、コンソールにロール名がユーザーに表示される場合、ロール名は大文字と小文字が区別されません。

- 他のエンティティがロールを参照する可能性があるため、ロールを作成した後にロール名を編集することはできません。

10. (オプション) [説明] にロールの説明を入力します。
11. (オプション) ロールのユースケースとアクセス許可を編集するには、[ステップ 1: 信頼されたエンティティを選択] または [ステップ 2: アクセス権限を追加] のセクションで [編集] を選択します。
12. (オプション) ロールの識別、整理、検索を簡単にするには、キーと値のペアとしてタグを追加します。IAM でのタグの使用の詳細については、IAM ユーザーガイドの [AWS Identity and Access Management 「リソースのタグ」](#) を参照してください。
13. ロールを確認したら、[ロールを作成] を選択します。

JSON ポリシーエディタでポリシーを作成するには

1. にサインイン AWS マネジメントコンソール し、 <https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

初めて [ポリシー] を選択する場合には、[管理ポリシーによるこそ] ページが表示されます。今すぐ始める を選択します。

3. ページの上部で、[ポリシーを作成] を選択します。
4. ポリシーエディタ セクションで、JSON オプションを選択します。
5. JSON ポリシードキュメントを入力するか貼り付けます。IAM ポリシー言語の詳細については、「[IAM JSON ポリシーリファレンス](#)」を参照してください。
6. [ポリシーの検証](#)中に生成されたセキュリティ警告、エラー、または一般警告をすべて解決してから、[次へ] を選択します。

 Note

いつでも [ビジュアル] と [JSON] エディタオプションを切り替えることができます。ただし、[ビジュアル] エディタで [次へ] に変更または選択した場合、IAM はポリシーを再構成してビジュアルエディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「[ポリシーの再構成](#)」を参照してください。

7. (オプション) でポリシーを作成または編集するときに AWS マネジメントコンソール、テンプレートで利用できる JSON または YAML ポリシー CloudFormation テンプレートを生成できます。

これを行うには、ポリシーエディタで [アクション] を選択し、次に [CloudFormation テンプレートを生成] を選択します。詳細については CloudFormation、「AWS CloudFormation ユーザーガイド」の「[AWS Identity and Access Management リソースタイプのリファレンス](#)」を参照してください。

8. ポリシーにアクセス権限を追加し終えたら、[次へ] を選択します。
9. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。このポリシーで定義されているアクセス許可を確認して、ポリシーによって付与されたアクセス許可を確認します。
10. (オプション) タグをキーと 値のペアとしてアタッチして、メタデータをポリシーに追加します。IAM でのタグの使用の詳細については、IAM ユーザーガイドの[AWS Identity and Access Management 「リソースのタグ」](#)を参照してください。
11. [ポリシーを作成] をクリックして、新しいポリシーを保存します。

ビジュアルエディタを使用してポリシーを作成するには

1. にサインイン AWS マネジメントコンソール し、 <https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

初めて [ポリシー] を選択する場合には、[管理ポリシーによるこそ] ページが表示されます。[Get Started] (今すぐ始める) を選択します。

3. [Create policy] (ポリシーを作成) を選択します。
4. [ポリシーエディタ] セクションで、[サービスを選択] セクションを見つけて、AWS のサービスを選択します。上部の検索ボックスを使用して、サービスのリストの結果を制限することができます。ビジュアルエディタのアクセス許可ブロック内で選択できるサービスは 1 つだけです。複数のサービスにアクセス許可を付与するには、[さらにアクセス許可を追加する] を選択して、複数のアクセス許可ブロックを追加します。
5. [許可されるアクション] で、ポリシーに追加するアクションを選択します。アクションは次の方法で選択できます。
 - すべてのアクションのチェックボックスをオンにします。
 - [アクションを追加] を選択して、特定のアクションの名前を入力します。ワイルドカード文字 (*) を使用すると、複数のアクションを指定できます。
 - [アクセスレベル] グループの 1 つを選択して、アクセスレベルのすべてのアクション ([読み取り]、[書き込み]、または [リスト] など) を選択します。
 - それぞれの [アクセスレベル] グループを展開して、個々のアクションを選択します。

デフォルトでは、作成しているポリシーが選択するアクションを許可します。その代わりに選択したアクションを拒否するには、[Switch to deny permissions (アクセス許可の拒否に切り替え)] を選択します。[IAM はデフォルトでは拒否](#) されるため、ユーザーが必要とするアクションとリソースのみに対してアクセス許可を許可することを、セキュリティのベストプラクティスとしてお勧めします。別のステートメントまたはポリシーによって個別に許可されるアクセス許可を上書きする場合のみ、アクセス許可を拒否する JSON ステートメントを作成します。これにより、アクセス許可のトラブルシューティングがより困難になる可能性があるため、拒否ステートメントの数は最小限に制限することをお勧めします。

6. [リソース] では、前のステップで選択したサービスとアクションが [特定のリソース](#) の選択をサポートしていない場合は、すべてのリソースが許可され、このセクションを編集することはできません。

[リソースレベルのアクセス許可](#)をサポートする 1 つ以上のアクションを選択した場合、ビジュアルエディタでそれらのリソースが一覧表示されます。[リソース] を展開して、ポリシーのリソースを指定できます。

リソースは次の方法で指定できます。

- [ARN を追加] を選択して、それらの Amazon リソースネーム (ARN) 別にリソースを指定します。ビジュアル ARN エディタを使用するか、ARN を手動でリストすることが出来ます。ARN 構文の詳細については、「IAM ユーザーガイド」の「[Amazon リソースネーム \(ARN\)](#)」を参照してください。ポリシーの Resource 要素で ARN を使用する方法については、「IAM ユーザーガイド」の「[IAM JSON ポリシー要素: Resource](#)」を参照してください。
 - リソースの横にある [このアカウント内のすべて] を選択して、そのタイプのすべてのリソースにアクセス許可を付与します。
 - [すべて] を選択し、そのサービスのすべてのリソースを選択します。
7. (オプション) [リクエスト条件 - オプション] を選択して、作成するポリシーに条件を追加します。条件によって JSON ポリシーステートメントの効果が制限されます。例えば、特定の時間範囲内でそのユーザーのリクエストが発生した場合にのみ、ユーザーがリソースに対してアクションを実行できるように指定できます。また、一般的に使用される条件を使用して、多要素認証 (MFA) デバイスでユーザーを認証する必要があるかどうかを制限することもできます。または、リクエストの発行元を特定範囲内の IP アドレスに限定できます。ポリシー条件で利用できるすべてのコンテキストキーのリストについては、「サービス認可リファレンス」の「[AWS サービスのアクション、リソース、および条件キー](#)」を参照してください。

条件は次の方法で選択できます。

- 一般的に使用される条件を選択するには、チェックボックスを使用します。
- 他の条件を指定するには、[別の条件を追加] を選択します。条件の [条件キー]、[修飾子]、[演算子] を選択し、[値] に入力します。複数の値を追加するには、[追加] を選択します。値は、論理 OR 演算子によって接続されていると見なすことができます。完了したら、[条件を追加] を選択します。

複数の条件を追加するには、[別の条件を追加] を選択します。必要に応じて操作を繰り返します。各条件は、この 1 つのビジュアルエディタのアクセス許可ブロックにのみ適用されます。アクセス許可ブロックが一致すると見なされるためには、すべての条件が満たされている必要があります。つまり、論理 AND 演算子によって接続される条件を考慮します。

Condition 要素の詳細については、「IAM ユーザーガイド」の「[IAM JSON ポリシー要素: Condition](#)」を参照してください。

- さらにアクセス許可ブロックを追加するには、[さらにアクセス許可を追加] を選択します。各ブロックに対して、ステップ 2 から 5 を繰り返します。

 Note

いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[ビジュアル] エディタで [次へ] に変更または選択した場合、IAM はポリシーを再構成してビジュアルエディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「[ポリシーの再構成](#)」を参照してください。

- (オプション) でポリシーを作成または編集するときに AWS マネジメントコンソール、テンプレートで利用できる JSON または YAML ポリシー CloudFormation テンプレートを生成できます。

これを行うには、ポリシーエディタで [アクション] を選択し、次に [CloudFormation テンプレートを生成] を選択します。詳細については CloudFormation、「AWS CloudFormation ユーザーガイド」の「[AWS Identity and Access Management リソースタイプのリファレンス](#)」を参照してください。

- ポリシーにアクセス権限を追加し終えたら、[次へ] を選択します。
- [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認し、意図したアクセス許可を付与したことを確認します。
- (オプション) タグをキーと 値のペアとしてアタッチして、メタデータをポリシーに追加します。IAM でのタグの使用の詳細については、IAM ユーザーガイドの[AWS Identity and Access Management 「リソースのタグ」](#)を参照してください。
- [ポリシーを作成] をクリックして、新しいポリシーを保存します。

プログラマ的なアクセス権を付与するには

ユーザーが の AWS 外部で を操作する場合は、プログラムによるアクセスが必要です AWS マネジメントコンソール。プログラムによるアクセスを許可する方法は、 がアクセスするユーザーのタイプによって異なります AWS。

ユーザーにプログラムによるアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラムによるアクセス権を必要とするユーザー	目的	方法
IAM	(推奨) コンソール認証情報を一時的な認証情報として使用して AWS CLI、AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、AWS Command Line Interface 「ユーザーガイド」のAWS「ローカル開発用ログイン」を参照してください。 • AWS SDKs 「SDK およびツールリファレンスガイド」の「Login for AWS local development」を参照してください。AWS SDKs
ワークフォースアイデンティティ (IAM アイデンティティセンターで管理されているユーザー)	一時的な認証情報を使用して AWS CLI、AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、AWS Command Line Interface ユーザーガイドの「を使用する AWS CLI ように AWS IAM アイデンティティセンターを設定する」を参照してください。 • AWS SDKs、ツール、API については、AWS APIs 「SDK およびツールリファレンスガイド」の「IAM アイデンティティセンター認証」を参照してください。AWS SDKs

プログラムによるアクセス権を必要とするユーザー	目的	方法
IAM	一時的な認証情報を使用して AWS CLI、AWS SDKs、または AWS APIs。	「IAM ユーザーガイド 」の「 AWS リソースでの一時的な認証情報の使用 」の手順に従います。
IAM	(非推奨) 長期認証情報を使用して、AWS CLI、AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs 「SDK とツールリファレンスガイド」の「長期認証情報を使用した認証」を参照してください。AWS SDKs • API AWS APIs 「IAM ユーザーのアクセスキーの管理」を参照してください。

攻撃者からの保護

他の AWS サービスプリンシパルにアクセス許可を付与するときに攻撃者から保護する方法の詳細については、「[ロールの信頼関係のオプション条件](#)」を参照してください。ポリシーに特定の条件を追加することで、混乱した代理攻撃と呼ばれる特定のタイプの攻撃を防ぐことができます。これは、クロスサービス偽装など、エンティティが、より特権のあるエンティティにアクションを実行させる場合に発生します。ポリシー条件に関する一般的な情報については、「[ポリシーでの条件の指定](#)」も参照してください。

AWS Control Tower でアイデンティティベースのポリシーを使用する場合の詳細については、「[AWS Control Tower でアイデンティティベースのポリシー \(IAM ポリシー\) を使用する](#)」を参照し

てください。ユーザー、グループ、ロール、アクセス許可の詳細については、「IAM ユーザーガイド」の「[アイデンティティ \(ユーザー、グループ、ロール\)](#)」を参照してください。

リソースベースのポリシー

Simple Storage Service (Amazon S3) などの他のサービスでは、リソースベースの許可ポリシーもサポートされています。例えば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス許可を管理できます。AWS Control Tower では、リソースベースのポリシーはサポートされていません。

ポリシー要素を指定: アクション、効果、プリンシパル

AWS Control Tower コンソール、または[ランディングゾーン API](#) を使用して、ランディングゾーンを設定および管理できます。ランディングゾーンを設定するには、IAM ポリシーで定義された管理者権限を持つ IAM ユーザーである必要があります。

ポリシーで識別できる最も基本的な要素は次の通りです。

- リソース – ポリシーで Amazon リソースネーム (ARN) を使用して、ポリシーを適用するリソースを識別します。詳細については、「[AWS Control Tower のリソースとオペレーション](#)」を参照してください。
- アクション – アクションのキーワードを使用して、許可または拒否するリソースオペレーションを識別します。実行可能なアクションのタイプについては、「[AWS Control Tower で定義されたアクション](#)」を参照してください。
- 効果 – ユーザーが特定のアクションを要求する際の効果を指定します。許可または拒否のいずれかになります。リソースへのアクセスを明示的に付与 (許可) していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- Principal – ID ベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的なプリンシパルとなります。リソースベースのポリシーでは、権限 (リソースベースのポリシーにのみ適用) を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。AWS Control Tower では、リソースベースのポリシーはサポートされていません。

IAM ポリシーの構文と記述の詳細については、「IAM ユーザーガイド」の「[AWS IAM ポリシーリファレンス](#)」を参照してください。

ポリシーでの条件の指定

許可を付与するとき、IAM ポリシー言語を使用して、ポリシーが有効になる必要がある条件を指定できます。例えば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、「IAM ユーザーガイド」の「[条件](#)」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。AWS Control Tower に固有の条件キーはありません。ただし、必要に応じて使用できる AWS 広範な条件キーがあります。AWS 全体のキーの完全なリストについては、IAM ユーザーガイドの「[条件に使用可能なキー](#)」を参照してください。

クロスサービス偽装の防止

では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。あるサービスが別のサービスを呼び出すとき、あるサービスが別のサービスを操作し、それ以外では許可されていない方法で、お客様のリソースに影響を及ぼす許可を使用した場合、クロスサービス偽装が発生します。この攻撃を防ぐために、は、正当なアクセス許可を持つサービスのみがアカウント内のリソースにアクセスできるように、データを保護するのに役立つツール AWS を提供します。

ポリシーで `aws:SourceArn` 条件および `aws:SourceAccount` 条件を使用して、お客様のリソースにアクセスするために AWS Control Tower が別のサービスに付与する許可を制限することをお勧めします。

- クロスサービスのアクセスにリソースを 1 つだけ関連付けたい場合は、`aws:SourceArn` を使用します。
- クロスサービスが使用できるように、アカウント内の任意のリソースを関連付けたい場合は、`aws:SourceAccount` を使用します。
- `aws:SourceArn` の値に Simple Storage Service (Amazon S3) バケットの ARN などのアカウント ID が含まれていない場合は、両方の条件を使用して、許可を制限する必要があります。
- 両方の条件を使用する場合、および `aws:SourceArn` の値にアカウント ID が含まれている場合は、`aws:SourceAccount` の値と、`aws:SourceArn` の値のアカウントは、同じポリシーステートメントで使用する時、同じアカウント ID を示している必要があります。

詳細な説明と例については、「<https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html>」を参照してください。

AWS Control Tower でアイデンティティベースのポリシー (IAM ポリシー) を使用する

このトピックでは、アカウント管理者がどのようにして IAM アイデンティティ (ユーザー、グループ、ロール) に許可ポリシーをアタッチし、それによって AWS Control Tower リソースでのオペレーションを実行する許可を付与する方法を示す、アイデンティティベースのポリシーの例を示します。

Important

初めに、AWS Control Tower リソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要トピックをお読みになることをお勧めします。詳細については、「[AWS Control Tower リソースに対するアクセス許可の管理の概要](#)」を参照してください。

AWS Control Tower コンソールを使用するために必要なアクセス許可

AWS Control Tower は、ランディングゾーンを設定するときに、3 つのロールを自動的に作成します。コンソールアクセスを許可するには、3 つのロールすべてが必要です。AWS Control Tower では、アクションおよびリソースの最小セットへのアクセスを制限するためのベストプラクティスとして、アクセス許可が 3 つのロールに分割されます。

ランディングゾーンのアクセスに必要な 3 つのロール

- [AWS Control Tower 管理者ロール](#)
- [AWS ControlTowerStackSetRole](#)

これらのロールのロール信頼ポリシーへのアクセスを制限することをお勧めします。詳細については、「[Optional conditions for your role trust relationships](#)」を参照してください。

コンソールで Control Catalog を表示する

AWS Control Tower コンソールでコントロール情報を表示するには、IAM ポリシーに `controlcatalog` のアクセス許可を追加する必要があります。これらのアクセス許可は次のとおりです。

- `controlcatalog:GetControl`
- `controlcatalog:ListControls`

- `controlcatalog:ListControlMappings`
- `controlcatalog:ListCommonControls`

ポリシーで更新されたアクセス許可の例を次に示します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "controlcatalog:GetControl",
        "controlcatalog:ListControls",
        "controlcatalog:ListControlMappings",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

AWS Control Tower は `controlcatalog` API を呼び出して特定のコントロールメタデータを取得するため、これらのアクセス許可を追加する必要があります。AWS Control Tower のアクセス許可では不十分です。

アクセス許可を更新する方法の詳細については、「[ロールを作成して、アクセス許可を割り当てる](#)」を参照してください。

`controlcatalog` IAM アクションの詳細については、「[AWS Control Catalog のアクション、リソース、および条件キー](#)」を参照してください。

Note

コントロール情報は、[Control Catalog API](#) を介して利用できます。

AWS Control Tower 管理者ロール

このロールは、ランディングゾーンの維持にきわめて重要なインフラストラクチャへのアクセス権を持つ AWS Control Tower を提供します。AWS ControlTowerAdmin ロールには、アタッチされたマネージドポリシーと、IAM ロールのロール信頼ポリシーが必要です。ロール信頼ポリシーは、リソースベースのポリシーで、どのプリンシパルがロールを引き受けることができるかを指定します。

このロールの信頼ポリシーのサンプルスニペットを次に示します。

JSON

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

AWS CLI からこのロールを作成し、 という名前のファイルに配置するには `trust.json`、CLI コマンドの例を次に示します。

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-role-policy-document file:///trust.json
```

このロールには 2 つの IAM ポリシーが必要です。

1. インラインポリシー。次に例を示します。

JSON

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

```
        "Effect": "Allow",
        "Action": "ec2:DescribeAvailabilityZones",
        "Resource": "*"
      }
    ]
  }
}
```

2. 次を示すマネージドポリシー。これは AWS ControlTowerServiceRolePolicy です。

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicy は、CloudFormation スタックセットとスタックインスタンス、AWS CloudTrail ログファイル、AWS Control Tower の設定アグリゲータ、AWS Control Tower によって管理される AWS Organizations アカウントと組織単位 (OUs) などの AWS AWS Control Tower リソースを作成および管理するためのアクセス許可を定義する AWS マネージドポリシーです。

この管理ポリシーの更新は、表 [AWS Control Tower のマネージドポリシー](#) にまとめられています。

詳細については「AWS マネージドポリシーリファレンスガイド」の「[AWS ControlTowerServiceRolePolicy](#)」を参照してください。

ロール信頼ポリシー:

JSON

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

インラインポリシーは AWS ControlTowerAdminPolicy です。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "ec2:DescribeAvailabilityZones",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

AWS ControlTowerIdentityCenterManagementPolicy

このポリシーは、AWS Control Tower に登録されているメンバーアカウントの IAM アイデンティティセンター (IdC) リソースを設定するアクセス許可を提供します。AWS Control Tower でランディングゾーンの設定 (または更新) 中に ID プロバイダーとして IAM Identity Center を選択すると、このポリシーが AWS ControlTowerAdmin ロールにアタッチされます。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「[AWS ControlTowerIdentityCenterManagementPolicy](#)」を参照してください。

AWS ControlTowerStackSetRole

CloudFormation は、AWS Control Tower によって作成されたアカウントにスタックセットをデプロイするためにこのロールを引き受けます。インラインポリシー:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],

```

```
        "Resource": [
            "arn:aws:iam::*:role/AWSControlTowerExecution"
        ],
        "Effect": "Allow"
    }
}
```

信頼ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS ControlTowerCloudTrailRolePolicy

AWS Control Tower は、ベストプラクティスとして CloudTrail を有効にし、CloudTrail にこのロールを提供します。CloudTrail は CloudTrail ログを作成し公開するために、このロールを引き受けます。

管理ポリシー: AWS ControlTowerCloudTrailRolePolicy

このロールはAWS ControlTowerCloudTrailRolePolicy、AWS Control Tower に代わって Amazon CloudWatch Logs に監査ログを発行するために必要なアクセス許可を CloudTrail に付与する AWS マネージドポリシーを使用します。この管理ポリシーは、このロールに以前使用されていたインラインポリシーを置き換え、AWS が顧客の介入なしにポリシーを更新できるようにします。

詳細については、「AWS マネージドポリシーリファレンスガイド」の[AWS ControlTowerCloudTrailRolePolicy](#)を参照してください。

この管理ポリシーの更新は、表 [AWS Control Tower のマネージドポリシー](#) にまとめられています。

Note

管理ポリシーの導入前は、このロールは同等のアクセス許可を持つインラインポリシーを使用していました。インラインポリシーが マネージドポリシーに置き換えられ、シームレスな更新が可能になりました。

以前のインラインポリシー (参照用):

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"
    }
  ]
}
```

信頼ポリシー

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
]
```

AWS ControlTowerBlueprintAccess ロールの要件

AWS Control Tower では、同じ組織内の指定されたブループリントハブアカウントに AWS ControlTowerBlueprintAccess ロールを作成する必要があります。

ロール名

ロールタイプは、AWS ControlTowerBlueprintAccess である必要があります。

ロール信頼ポリシー

ロールは、以下のプリンシパルを信頼するように設定する必要があります。

- 管理アカウントで AWS Control Tower を使用するプリンシパル。
- 管理アカウントの AWS ControlTowerAdmin ロール。

以下の例は、最小特権の信頼ポリシーを示しています。独自のポリシーを作成する場合は、*YourManagementAccountId* を AWS Control Tower 管理アカウントの実際のアカウント ID で置き換え、*YourControlTowerUserRole* を管理アカウントの IAM ロールの識別子で置き換えます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

        "Principal": {
            "AWS": [
                "arn:aws:iam::111122223333:role/service-role/AWSControlTowerAdmin",
                "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
            ]
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
    }
}

```

ロールのアクセス許可

管理ポリシーの `AWSServiceCatalogAdminFullAccess` をロールにアタッチする必要があります。

AWSServiceRoleForAWSControlTower

このロールは、ランディングゾーンの維持に不可欠な操作 (ドリフトしたリソースの通知など) のために、Log Archive アカウント、監査アカウント、およびメンバーアカウントへのアクセス権を AWS Control Tower に 付与します。

AWS `ServiceRoleFor AWS ControlTower` ロールには、アタッチされたマネージドポリシーと、IAM ロールのロール信頼ポリシーが必要です。

このロールのマネージドポリシー: `AWS ControlTowerAccountServiceRolePolicy`

ロール信頼ポリシー:

JSON

```

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

```

```
}  
]  
}
```

AWS ControlTowerAccountServiceRolePolicy

この AWS 管理ポリシーにより、AWS Control Tower は自動アカウント設定と一元化されたガバナンスを提供する AWS サービスをユーザーに代わって呼び出すことができます。

このポリシーには、Security Hub CSPM Service-managed Standard: AWS Control Tower の一部である Security Hub CSPM コントロールによって管理されるリソースの結果転送を AWS Control Tower が実装 AWS Security Hub CSPM するための最小限のアクセス許可が含まれており、カスタマーアカウントを管理する機能を制限する変更が防止されます。これはバックグラウンド AWS Security Hub CSPM ドリフト検出プロセスの一部であり、お客様が直接開始することはありません。

このポリシーは、各メンバーアカウントで、特に Security Hub CSPM コントロール用に Amazon EventBridge ルールを作成するアクセス許可を付与します。これらのルールでは、正確な EventPattern を指定する必要があります。また、ルールはサービスプリンシパルが管理するルールにのみ適用されます。

サービスプリンシパル: `controltower.amazonaws.com`

詳細については、「AWS マネージドポリシーリファレンスガイド」の「[AWS ControlTowerAccountServiceRolePolicy](#)」を参照してください。

この管理ポリシーの更新は、表 [AWS Control Tower のマネージドポリシー](#) にまとめられています。

AWS Control Tower のマネージドポリシー

AWS は、によって作成および管理されるスタンドアロン IAM ポリシーを提供することで、多くの一般的なユースケースに対処します AWS。マネージドポリシーは、一般的ユースケースに必要な許可を付与することで、どの許可が必要なのかをユーザーが調査する必要をなくすることができます。詳細については、「IAM ユーザーガイド」の「[AWS マネージドポリシー](#)」を参照してください。

変更	説明	日付
AWS ControlTowerAccountServiceRolePolicy - 既存ポリシーへの更新	AWS Control Tower は、サービスにリンクされたフックの内部改善BatchDescriptorTypeConfiguration	2026 年 3 月 23 日

変更	説明	日付
	ions のために、AWS Control Tower が AWS CloudFormation サービス API を呼び出すことを可能にする新しいアクセス許可を追加しました。	
AWS ControlTowerAccountServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、Amazon EventBridge ルール条件の検証精度を向上させるために既存のポリシーを更新しました。更新によりevents:detail-type 、条件が から に移動StringEquals されForAllValues:StringEquals 、同じ機能アクセス許可を維持しながら、イベントパターンマッチングの制御が向上します。	2025 年 12 月 30 日

変更	説明	日付
AWS ControlTowerAccountServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、次のアクセス許可を拡張する新しいポリシーを追加しました。 • AWS Config サービスにリンクされた設定アグリゲータを作成、タグ付け、削除、管理、および読み取るアクセス許可 • AWS Config すべての設定アグリゲータを記述するアクセス許可 • AWS Organizations の委任管理者を一覧表示する アクセス許可 AWS Config • AWS Organizations 組織を記述するアクセス許可 • CloudFormation サービスにリンクされたフックを管理するアクセス許可	2025 年 11 月 10 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 管理ポリシーの更新	AWS Control Tower は、AWS ControlTowerServiceRolePolicy の Amazon CloudWatch Logs リソースパターンを更新し、ランディングゾーン 4.0 のオプション AWS CloudTrail の統合をサポートしました。パターンが <code>aws-controltower/CloudTrailLogs:*</code> に変更され <code>aws-controltower/CloudTrailLogs*:*</code>、の後にワイルドカード文字が追加され <code>CloudTrailLogs</code>、任意のサフィックスを持つロググループを管理できるようになりました。 この更新により、ランディングゾーン 4.0 のオプション AWS CloudTrail の統合が有効になり、お客様は AWS CloudTrail 統合を複数回有効または無効にできます。統合を有効にするたびに、Amazon CloudWatch Logs ロググループは一意的なサフィックスで再作成され、名前の競合を回避します。更新は、既存のデプロイと下位互換性があります。	2025 年 10 月 31 日

変更	説明	日付
AWS ControlTowerCloudTrailRolePolicy – 新しいマネージドポリシー	AWS Control Tower は AWS ControlTowerCloudTrailRolePolicy マネージドポリシーを導入しました。これにより、CloudTrail はログストリームを作成し、Control Tower が管理する Amazon CloudWatch Logs ロググループにログイベントを発行できます。 この管理ポリシーは、以前 AWS ControlTowerCloudTrailRole で使用されていたインラインポリシーを置き換え、お客様の介入なしにポリシーを更新 AWS できるようにします。ポリシーは、パターン に一致する名前を持つロググループに限定されま すaws-controltower/CloudTrailLogs* 。	2025 年 10 月 31 日

変更	説明	日付
AWS ControlTowerIdentityCenterManagementPolicy - 新しいポリシー	AWS Control Tower は、お客様が AWS Control Tower に登録されているアカウントで IAM Identity Center リソースを設定できるようにする新しいポリシーを導入し、アカウントの自動登録時に AWS Control Tower が一部のタイプのドリフトを修正できるようにします。 この変更は、お客様が AWS Control Tower で IAM アイデンティティセンターを設定し、AWS Control Tower が自動登録ドリフトを修正できるようにするために必要です。	2025 年 10 月 10 日
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、アカウントを AWS Control Tower に自動登録するときに、AWS Control Tower がスタックセットリソースをクエリしてメンバーアカウントにデプロイできるようにする新しい CloudFormation アクセス許可を追加しました。	2025 年 10 月 10 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、お客様がサービスにリンクされた AWS Config ルールを有効または無効にできるようにする新しいアクセス許可を追加しました。 この変更は、お客様が Config ルールによってデプロイされるコントロールを管理できるようにするために必要です。	2025 年 6 月 5 日
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、AWS Control Tower が AWS CloudFormation サービス APIs <code>ActivateType</code>、<code>DeactivateType</code> および <code>SetTypeConfiguration</code> を呼び出すことを許可する新しいアクセス許可を追加しました <code>AWS::ControlTower::types</code>。 この変更により、お客様はプライベート CloudFormation フックタイプのデプロイなしでプロアクティブコントロールをプロビジョニングできます。	2024 年 12 月 10 日

変更	説明	日付
AWS ControlTowerAccountServiceRolePolicy - 新しいポリシー	AWS Control Tower は、AWS Control Tower がイベントルールを作成および管理し、それらのルールに基づいて Security Hub CSPM に関連するコントロールのドリフト検出を管理できるようにする新しいサービスにリンクされたロールを追加しました。 この変更は、これらのリソースが Security Hub CSPM サービスマネージドスタンダード: AWS Control Tower の一部である Security Hub CSPM コントロールに関連している場合に、お客様がドリフトしたリソースをコンソールで表示できるようにするために必要です。	2023 年 5 月 22 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、ランディングゾーンの顧客アカウント (管理アカウント、ログアーカイブアカウント、監査アカウント、OU メンバーアカウント) がオプトイン AWS リージョン を利用できるように、AWS Control Tower が AWS アカウント管理サービスにより実装された EnableRegion 、ListRegions 、およびGetRegionOptStatus API を呼び出すための新しい権限を追加されました。 この変更は、お客様が AWS Control Tower によるリージョン管理をオプトインリージョンに拡張するために必要です。	2023 年 4 月 6 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower では、AWS Control Tower がブループrint (ハブ) アカウントで AWSControlTowerBlueprintAccess ロールを引き受けることができる新しいアクセス許可が追加されました。ブループrint (ハブ) アカウントは、組織内の専用アカウントであり、1 つ以上の Service Catalog 製品に保存されている事前定義済みのブループrintを含みます。AWS Control Tower は、Service Catalog ポートフォリオの作成、リクエストされたブループrint製品の追加、およびアカウントプロビジョニング時にリクエストされたメンバーアカウントへのポートフォリオの共有という 3 つのタスクを実行するために AWSControlTowerBlueprintAccess ロールを引き受けます。 この変更は、お客様が AWS Control Tower Account Factory を通じてカスタマイズされたアカウントをプロビジョニングするために必要です。	2022 年 10 月 28 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、ランディングゾーンバージョン 3.0 以降、お客様が組織レベルの AWS CloudTrail 証跡を設定できるようにする新しいアクセス許可を追加しました。 組織ベースの CloudTrail 機能を使用するには、お客様が CloudTrail サービスに対して信頼されたアクセスを有効にする必要があります。また、IAM ユーザーまたはロールが、管理アカウントで組織レベルの追跡を作成するアクセス許可を持っていることが必要です。	2022 年 6 月 20 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存のポリシーを更新します	AWS Control Tower では、お客様が KMS キー暗号化を使用できるようにする新しいアクセス許可が追加されました。 KMS 機能を使用すると、お客様独自の KMS キーを提供して AWS CloudTrail ログを暗号化できます。また、お客様は、ランディングゾーンの更新または修復中に KMS キーを変更することもできます。KMS キーを更新する場合、AWS CloudFormation には AWS CloudTrail PutEventSelector API を呼び出すためのアクセス許可が必要です。ポリシーの変更は、AWS ControlTowerAdmin ロールが API を呼び出せるようにすることです AWS CloudTrail PutEventSelector 。	2021 年 7 月 28 日
AWS Control Tower は変更の追跡を開始しました	AWS Control Tower は、AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 5 月 27 日

AWS Control Tower のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、AWS お客様とお客様の間の責任共有です。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ - AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。は、安全に使用できるサービス AWS も提供します。セキュリティの有効性は、[AWS コンプライアンスプログラム](#)の一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。AWS Control Tower に適用されるコンプライアンスプログラムの詳細については、「[コンプライアンスプログラムによる対象範囲内のAWS のサービス](#)」を参照してください。
- クラウド内のセキュリティ - お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、AWS Control Tower を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するよう AWS Control Tower を設定する方法について説明します。また、AWS Control Tower リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

AWS Control Tower のデータ保護

責任 AWS [共有モデル](#)、AWS Control Tower でのデータ保護に適用されます。このモデルで説明されているように、AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「AWS のサービス」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、[データプライバシーに関するよくある質問](#)を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された「[AWS 責任共有モデルおよび GDPR](#)」のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント、AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の[CloudTrail 証跡の使用](#)を参照してください。
- AWS 暗号化ソリューションと、内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「[連邦情報処理規格 \(FIPS\) 140-3](#)」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して AWS Control Tower AWS CLI または他の AWS のサービス を操作する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

Note

を使用したユーザーアクティビティのログ記録 AWS CloudTrail は、ランディングゾーンを設定すると AWS Control Tower で自動的に処理されます。

データ保護の詳細については、AWS セキュリティブログ のブログ投稿「[AWS の責任共有モデルと GDPR](#)」を参照してください。AWS Control Tower には、ランディングゾーンに存在するコンテンツを保護するために使用できる次のオプションがあります。

トピック

- [保管時の暗号化](#)
- [転送時の暗号化](#)

• [コンテンツへのアクセスの制限](#)

保管時の暗号化

AWS Control Tower では、ランディングゾーンを支援するために Simple Storage Service (Amazon S3) マネージドキー (SSE-S3) を使用して保管時に暗号化される Simple Storage Service (Amazon S3) バケットおよび Amazon DynamoDB データベースを使用します。デフォルトでは、この暗号化はランディングゾーンのセットアップ時に設定されます。必要に応じて、KMS 暗号化キーでリソースを暗号化するようにランディングゾーンを構成できます。また、ランディングゾーンでそれをサポートするサービス用に使用するサービスに対して保管時の暗号化を確立することもできます。詳細については、そのサービスのオンラインドキュメントでセキュリティに関する章を参照してください。

転送時の暗号化

AWS Control Tower では、ランディングゾーンを支援するために転送中の暗号化に Transport Layer Security (TLS) とクライアント側の暗号化を使用します。さらに、AWS Control Tower へのアクセスには、HTTPS エンドポイント経由でのみアクセスできるコンソールを使用する必要があります。デフォルトでは、この暗号化はランディングゾーンのセットアップ時に設定されます。

コンテンツへのアクセスの制限

ベストプラクティスとして、適切なユーザーのサブセットへのアクセスを制限する必要があります。AWS Control Tower でこれを行うには、集中型クラウド管理者とエンドユーザーが適切な IAM アクセス許可を持ち、IAM Identity Center ユーザーの場合は、適切なグループに存在している必要があります。

- IAM エンティティのロールとポリシーの詳細については、「[IAM ユーザーガイド](#)」を参照してください。
- ランディングゾーンのセットアップ時に作成された IAM Identity Center グループの詳細については、「[AWS Control Tower の IAM Identity Center グループ](#)」を参照してください。

AWS Control Tower のコンプライアンス検証

AWS Control Tower は、組織がコントロールおよびベストプラクティスでコンプライアンスのニーズを満たすのに役立つ優れた設計のサービスです。さらに、サードパーティーの監査者が、複数の AWS コンプライアンスプログラムの一部としてランディングゾーンで利用できる

多くのサービスのセキュリティおよびコンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、[AWS「コンプライアンスプログラムによる対象範囲内のサービス」](#)を参照してください。一般的な情報については、「[AWSコンプライアンスプログラム](#)」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「[AWS Artifact ユーザーガイド](#)」の [AWS「アーティファクトでのレポートのダウンロード」](#)を参照してください。

AWS Control Tower を使用する場合のお客様のコンプライアンス責任は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- [セキュリティとコンプライアンスのクイックスタートガイド](#) – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイする手順について説明します AWS。
- [アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- [AWSコンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- [AWS Config](#) – この AWS サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。
- [AWS Security Hub CSPM](#) – この AWS サービスは、内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

AWS Control Tower の耐障害性

AWS グローバルインフラストラクチャは、AWS リージョンとアベイラビリティゾーンを中心に構築されています。

AWS リージョンは、物理的に分離および分離された複数のアベイラビリティゾーンを提供します。アベイラビリティゾーンは、低レイテンシー、高スループット、および高度に冗長なネットワークによって接続されます。複数のアベイラビリティゾーンがあることで、アベイラビリティゾーン間で自動的にフェイルオーバーして中断することなく動作するアプリケーションとデータベ

スを設計して運用できます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、フォールトトレランス、および拡張性が優れています。

AWS Control Tower が利用可能な AWS リージョン のリストについては、「」を参照してください [AWS リージョンと AWS Control Tower の連携方法](#)。

ホームリージョンは、ランディングゾーンが設定された AWS リージョンとして定義されます。

AWS リージョンとアベイラビリティーゾーンの詳細については、[AWS 「グローバルインフラストラクチャ」](#) を参照してください。

AWS Control Tower のインフラストラクチャセキュリティ

AWS Control Tower は、ホワイトペーパー「[Amazon Web Services: セキュリティプロセスの概要](#)」に記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

ネットワーク経由でランディングゾーン内の AWS サービスやリソースにアクセスするために、AWS 公開された API コールを使用します。Transport Layer Security (TLS) 1.2 が必要であり、Transport Layer Security (TLS) 1.3 以降が推奨されています。また、一時的ディフィー・ヘルマン Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service](#) (AWS STS) を使用して、テナンタリセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Control Tower ランディングゾーンワークロードのネットワークインフラストラクチャセキュリティを強化するようにセキュリティグループを設定できます。詳細については、「[チュートリアル: を使用して AWS Control Tower でセキュリティグループを設定する AWS Firewall Manager](#)」を参照してください。

AWS Control Tower でのログ記録とモニタリング

モニタリングを使用すると、潜在的なインシデントに対して計画を立て、対応することができます。モニタリングアクティビティの結果が、ログファイルに保存されます。したがって、ログ記録とモニタリングは密接に関連した概念であり、AWS Control Tower における Well-Architected の重要な要素です。

ランディングゾーンをセットアップすると作成される共有アカウントの 1 つが、ログアーカイブアカウントです。これは、すべての共有アカウントとメンバーアカウントのログを含む、すべてのログを一元的に収集することに特化しています。ログファイルは Amazon S3 バケットに保存されます。これらのログファイルを参照することで、管理者と監査人は発生したアクションとイベントを確認できます。

ベストプラクティスとして、マルチポイント障害が発生した場合に簡単にデバッグできるように、AWS セットアップのすべての部分からモニタリングデータをログに収集することをお勧めします。AWS には、ランディングゾーンのリソースとアクティビティをモニタリングするためのツールがいくつか用意されています。

例えば、コントロールのステータスは常にモニタリングされます。このステータスは、AWS Control Tower コンソール内で、または [AWS Control Tower API](#) を使用してプログラムにより、一目で確認できます。Account Factory でプロビジョニングしたアカウントの正常性とステータスも常にモニタリングされます。

ログに記録されたアクションを [アクティビティ] ページから表示する

AWS Control Tower コンソールの [アクティビティ] ページには、AWS Control Tower 管理アカウントのアクション概要が表示されます。AWS Control Tower の [Activities] (アクティビティ) ページに移動するには、左側のナビゲーションから [Activities] (アクティビティ) を選択します。

アクティビティページに表示されるアクティビティは、AWS Control Tower の AWS CloudTrail イベントログで報告されたアクティビティと同じですが、テーブル形式で表示されます。特定のアクティビティの詳細を表示するには、表からアクティビティを選択し、[View details] (詳細の表示) を選択します。

メンバーアカウントのアクションとイベントは、ログアーカイブファイルで表示できます。

以下のセクションでは、AWS Control Tower のモニタリングとログインについて詳しく説明します。

トピック

- [統合されたモニタリング用ツール](#)
- [を使用した AWS Control Tower アクションのログ記録 AWS CloudTrail](#)
- [AWS Control Tower でのライフサイクルイベント](#)
- [でのAWSユーザー通知の使用AWS Control Tower](#)

AWS Control Tower でのログ記録について

AWS Control Tower は、 および との統合を通じてアクションAWS CloudTrailとイベントのログ記録を自動的に実行しAWS Config、CloudWatch に記録します。AWS Control Tower の管理アカウントや組織のメンバーアカウントのアクションなど、すべてのアクションがログに記録されます。管理アカウントのアクションとイベントは、コンソールの [Activities] (アクティビティ) ページに表示されます。メンバーアカウントのアクションとイベントは、ログアーカイブファイルで表示できます。

組織レベルの証跡

ランディングゾーンをセットアップすると、AWS Control Tower が新しい CloudTrail 証跡をセットアップします。これは組織レベルの証跡で、組織内の管理アカウントとすべてのメンバーアカウントの全イベントがログされます。この機能は、各メンバーアカウントで証跡を作成する管理アカウントアクセス許可を付与するのに信頼されたアクセスに依存します。

AWS Control Tower および CloudTrail 組織証跡についての詳細は、[組織の証跡の作成](#)を参照してください。

Note

ランディングゾーンバージョン 3.0 より前の AWS Control Tower リリースでは、AWS Control Tower で各アカウントのメンバーアカウントの証跡が作成されていました。リリース 3.0 に更新すると、CloudTrail 証跡が組織証跡になります。証跡を移行する際のベストプラクティスについては、「CloudTrail ユーザーガイド」の「[証跡の変更のベストプラクティス](#)」を参照してください。

AWS Control Tower にアカウントを登録すると、アカウントは AWS Control Tower 組織のAWS CloudTrail証跡によって管理されます。アカウントに CloudTrail 追跡の既存のデプロイがある場合、AWS Control Tower にアカウントを登録する前にアカウントの既存の追跡を削除しない限り、料金が重複して発生する可能性があります。

Note

ランディングゾーンバージョン 3.0 に更新すると、AWS Control Tower は登録済みアカウントの (AWS Control Tower が作成した) アカウントレベルの証跡をユーザーに代わって削除します。既存のアカウントレベルのログファイルは、Amazon S3 バケットに保存されます。

監査アカウントの Amazon S3 バケットポリシー

AWS Control Tower では、リクエストが組織または組織単位 (OU) から発信された場合にのみ、AWS サービスはリソースにアクセスできます。書き込みアクセス許可のために、aws:SourceOrgID 条件を満たす必要があります。

aws:SourceOrgID 条件キーを使用して、Amazon S3 バケットポリシーの条件要素で [組織 ID] の値を設定できます。この条件によってのみ、CloudTrail は組織内のアカウントに代わってお客様の S3 バケットへログを書き込めるようになり、組織外の CloudTrail ログによるお客様の AWS Control Tower S3 バケットへの書き込みを防ぎます。

このポリシーは、既存のワークロードの機能には影響しません。このポリシーを以下の例に示します。

```
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: AWSS3BucketPermissionsCheck
          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
```

この条件キーの詳細については、IAM ドキュメントと「リソースにアクセスするAWSサービスにスケーラブルなコントロールを使用する」というタイトルの IAM ブログ投稿を参照してください。

統合されたモニタリング用ツール

モニタリングは、AWS Control Tower およびその他のAWSソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。には、AWS Control Tower をモニタリングし、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツールAWSが用意されています。

- Amazon CloudWatch は、AWSリソースと で実行されるアプリケーションをAWSリアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、CloudWatch で Amazon EC2 インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「[Amazon CloudWatch ユーザーガイド](#)」を参照してください。
- Amazon CloudWatch Events は、AWSリソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。CloudWatch Events で自動イベント駆動型コンピューティングを有効にすると、特定のイベントをモニタリングするルールを記述し、そのイベントが発生したときに他のAWSのサービスで自動アクションをトリガーできます。詳細については、「[Amazon CloudWatch Events ユーザーガイド](#)」を参照してください。
- Amazon CloudWatch Logs では、Amazon EC2 インスタンス、CloudTrail、およびその他のソースからのログファイルをモニタリング、保存、およびアクセスできます。CloudWatch Logs は、ログファイル内の情報をモニタリングし、特定のしきい値が満たされたときに通知します。高い耐久性を備えたストレージにログデータをアーカイブすることも可能です。詳細については、「[Amazon CloudWatch Logs ユーザーガイド](#)」を参照してください。
- AWS CloudTrail は、AWSアカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。呼び出し元のユーザーとアカウントAWS、呼び出し元の送信元 IP アドレス、呼び出しの発生日時を特定できます。

ヒント: CloudWatch Logs と CloudWatch Logs インサイトを使用して、アカウントに対する CloudTrail アクティビティを表示およびクエリできます。このようなアクティビティには、AWS

Control Tower ライフサイクルイベントなどがあります。CloudWatch Logs の機能を使用すると、CloudTrail を使用して通常作成できるクエリよりも詳細で緻密なクエリを実行できます。

詳細については、「[を使用した AWS Control Tower アクションのログ記録 AWS CloudTrail](#)」を参照してください。

を使用した AWS Control Tower アクションのログ記録 AWS CloudTrail

AWS Control Tower は AWS CloudTrail、AWS Control Tower のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、AWS Control Tower のアクションをイベントとしてキャプチャします。追跡を作成する場合は、AWS Control Tower のイベントを含めた CloudTrail イベントの Simple Storage Service (Amazon S3) バケットへの継続的な配信を有効にすることができます。

追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、AWS Control Tower に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエストが行われた日時、および追加の詳細を確認できます。

設定や有効化の方法など、CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

CloudTrail での AWS Control Tower 情報

CloudTrail は、AWS アカウントの作成時にアカウントで有効になります。AWS Control Tower でサポートされているイベントアクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) で AWS のその他サービスのイベントと共に CloudTrail イベントに記録されます。AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、[CloudTrail イベント履歴でのイベントの表示](#)を参照してください。

Note

ランディングゾーンバージョン 3.0 より前の AWS Control Tower リリースでは、AWS Control Tower でメンバーアカウントの証跡が作成されていました。リリース 3.0 に更新すると、CloudTrail 証跡が更新されて組織証跡になります。証跡を移行する際のベストプラクティスについては、「CloudTrail ユーザーガイド」の「[メンバーアカウントの証跡から組織の証跡への移行に関するベストプラクティス](#)」を参照してください。

推奨: 証跡の作成

AWS Control Tower のイベントなど、AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、ログファイルを CloudTrail で Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。証跡は、AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- [証跡の作成のための概要](#)
- [証跡の作成を準備する](#)
- [CloudTrail コストの管理](#)
- [CloudTrail がサポートするサービスと統合](#)
- [CloudTrail 用 Amazon SNS 通知の構成](#)
- 「[複数のリージョンから CloudTrail ログファイルを受け取る](#)」および「[複数のアカウントから CloudTrail ログファイルを受け取る](#)」

AWS Control Tower は、以下のアクションをイベントとして CloudTrail ログファイルに記録します。

パブリック API

- AWS Control Tower パブリック API の一覧と各 API の詳細については、「[AWS Control Tower API Reference](#)」を参照してください。これらのパブリック APIs は、によってログに記録されません AWS CloudTrail。

その他の API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- GetLandingZoneStatus
- GetHomeRegion

- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。
- リクエストがアクセス拒否として拒否されたか、正常に処理されたか。

詳細については、「[CloudTrail userIdentity 要素](#)」を参照してください。

例: AWS Control Tower ログファイルのエントリ

追跡は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できるものです。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報があります。ログファイルに CloudTrail イベントが特定の順序で表示されるわけではありません。

次の例は、アクションを開始したユーザーの ID のレコードなど、SetupLandingZone AWS Control Tower イベントの一般的なログファイルエントリの構造を示す CloudTrail ログエントリを示しています。

```
{
  "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"
}
```

でリソースの変更をモニタリングする AWS Config

AWS Control Tower は、すべての登録済みアカウント AWS Config で を有効にします。これにより、検出コントロールによるコンプライアンスのモニタリング、リソースの変更の記録、ログアーカイブアカウントへのリソース変更ログの配信が可能になります。

ランディングゾーンのバージョンが 3.0 より前の場合: 登録済みアカウントの場合、 は、アカウントが動作するすべてのリージョンのリソースに対するすべての変更を AWS Config ログに記録します。各変更は、リソース識別子、リージョン、各変更が記録された日付、および変更が既知のリソースまたは新しく検出されたリソースに関連するかどうかなどの情報を含む構成項目 (CI) としてモデル化されます。

ランディングゾーンバージョンが 3.0 以降の場合: AWS Control Tower は、IAM ユーザー、グループ、ロール、カスタマー管理ポリシーなどのグローバルリソースの記録をホームリージョンのみに制限します。グローバルリソースの変更のコピーは、すべてのリージョンに保存されるわけではありません。このリソース記録の制限は AWS Config [ベストプラクティス](#) に準拠しています。[グローバルリソースの完全なリスト](#) は、AWS Config ドキュメントで入手できます。

- 詳細については AWS Config、[「AWS Config の仕組み」](#) を参照してください。
- がサポート AWS Config できるリソースのリストについては、[「サポートされているリソースタイプ」](#) を参照してください。
- AWS Control Tower 環境でリソース追跡をカスタマイズする方法については、ブログ記事 [「AWS Control Tower で AWS Config リソース追跡をカスタマイズする」](#) を参照してください。

AWS Control Tower は、すべての登録済みアカウントに AWS Config 配信チャネルを設定します。この配信チャネルを通じて、AWS Config によってログアーカイブアカウントに記録されたすべての変更がログに記録され、Amazon Simple Storage Service バケットのフォルダに保存されます。

AWS Control Tower で AWS Config コストを管理する

このセクションでは、AWS Control Tower アカウントのリソースの変更 AWS Config を記録して請求する方法について説明します。この情報は、AWS Control Tower AWS Configを使用する際に関連するコストの管理方法を理解するのに役立ちます。AWS Control Tower では追加費用が不要です。

Note

ランディングゾーンのバージョンが 3.0 以降の場合: AWS Control Tower は、IAM ユーザー、グループ、ロール、カスタマー管理ポリシーなどのグローバルリソース AWS Config の記録をホームリージョンのみに制限します。したがって、このセクションの情報の一部がランディングゾーンに適用されない場合があります。

AWS Config は、アカウントが動作する各リージョンの各リソースに対する各変更を、設定項目 (CI) として記録するように設計されています。は、生成する設定項目ごとに AWS Config 請求します。

AWS Config の仕組み

AWS Config は、各リージョンのリソースを個別に記録します。IAM ロールなどの一部のグローバルリソースは、リージョンごとに 1 回記録されます。たとえば、5 つのリージョンで運用されている登録済みアカウントに新しい IAM ロールを作成すると、はリージョンごとに 1 つずつ、5 CIs AWS Config を生成します。Route 53 ホストゾーンなどの他のグローバルリソースは、すべてのリージョンで 1 回だけ記録されます。たとえば、登録済みアカウントで新しい Route 53 ホストゾーンを作成すると、そのアカウントに選択されているリージョンの数に関係なく、AWS Config が CI を 1 回生成します。これらのタイプのリソースを区別するのに役立つリストについては、「[同じリソースが複数回記録されている](#)」を参照してください。

Note

AWS Control Tower が と連携する場合 AWS Config、リージョンは AWS Control Tower によって管理されるか、管理解除され、アカウントがそのリージョンで動作している場合は変更が記録され AWS Config ます。

AWS Config がリソース内の 2 種類の関係を検出する

AWS Config は、リソース間の直接関係と間接関係を区別します。リソースが他のリソースの Describe API 呼び出しで返された場合、それらのリソースは直接的な関係として記録されます。別のリソースと直接関係にあるリソースを変更しても、AWS Config は両方のリソースの CI を作成しません。

たとえば、Amazon EC2 インスタンスを作成し、API でネットワークインターフェイスを作成する必要がある場合、AWS Config では、Amazon EC2 インスタンスはネットワークインターフェイスと直接的な関係があると見なされます。その結果、は 1 つの CI のみ AWS Config を生成します。

AWS Config は、間接的な関係であるリソース関係の個別の変更を記録します。たとえば、セキュリティグループを作成し、セキュリティグループの一部である関連付けられた Amazon EC2 インスタンスを追加すると、は 2 つの CIs AWS Config を生成します。

直接的な関係と間接的な関係の詳細については、[「リソースに関する直接的な関係と間接的な関係とは何ですか?」](#)を参照してください。

[リソース関係のリストは、](#) AWS Config ドキュメントで確認できます。

登録済みアカウントの AWS Config レコーダーデータを表示する

AWS Config は CloudWatch と統合されているため、ダッシュボードで AWS Config CIs を表示できます。詳細については、「[AWS Config が Amazon CloudWatch のメトリクスをサポート](#)」というタイトルのブログ投稿を参照してください。

プログラムで AWS Config データを表示するには、CLI AWS を使用するか、他の AWS ツールを使用できます。

特定のリソースの AWS Config レコーダーデータをクエリする

AWS CLI を使用して、リソースの最新の変更のリストを取得できます。

リソース履歴コマンド:

- aws configservice get-resource-config-history --resource-type *RESOURCE-TYPE* --resource-id *RESOURCE-ID* --region *REGION*

詳細については、[get-config-history の API ドキュメント](#)を参照してください。

Quick で AWS Config データを視覚化する

組織全体 AWS Config で によって記録されたリソースを視覚化およびクエリできます。詳細については、「[Config Resource Compliance Dashboard](#)」と「[Visualizing AWS Config data using Amazon Athena and Quick](#)」を参照してください。

AWS Control Tower AWS Config でのトラブルシューティング

このセクションでは、AWS Control Tower AWS Config で を使用する際に発生する可能性のあるいくつかの問題について説明します。

高 AWS Config コスト

ワークフローにリソースを頻繁に作成、更新、または削除するプロセスが含まれている場合、またはリソースを大量に処理する場合、そのワークフローによって多数の CI が生成されることが考えられます。非本番アカウントでこれらのプロセスを実行する場合、アカウントの登録解除を検討してください。そのアカウントの AWS Config レコーダーを手動で非アクティブ化する必要がある場合があります。

Note

アカウントを登録解除すると、AWS Control Tower は、そのアカウントのリソースに対して検出コントロールを適用したり、AWS Config アクティビティなどのアカウントイベントを記録したりすることはできません。

アカウントの管理解除について詳細は、[登録済みアカウントの管理を解除する](#)を参照してください。AWS Config レコーダーを非アクティブ化する方法については、「[設定レコーダーの管理](#)」を参照してください。

同じリソースが複数回記録されている

そのリソースが[グローバルリソース](#)かどうかをチェックします。バージョン 3.0 より前の AWS Control Tower ランディングゾーンでは、AWS Config が動作しているリージョンごとに特定のグローバルリソースを 1 回記録 AWS Config できます。たとえば、AWS Config が 8 つのリージョンで有効になっている場合、各ロールは 8 回記録されます。

以下のリソースは、AWS Config が動作しているリージョンごとに 1 回記録されます。

- AWS::IAM::Group

- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User

他のグローバルリソースは 1 回のみ記録されます。1 回記録されたリソースの例を次に示します。

- AWS::Route53::HostedZone
- AWS::Route53::HealthCheck
- AWS::ECR::PublicRepository
- AWS::GlobalAccelerator::Listener
- AWS::GlobalAccelerator::EndpointGroup
- AWS::GlobalAccelerator::Accelerator

AWS Config はリソースを記録しませんでした

特定のリソースは、他のリソースと依存関係があります。これらの関係は、直接的または間接的です。非推奨の間接的な関係のリストについては、[FAQ AWS Config](#)を参照してください。

AWS Control Tower でのライフサイクルイベント

AWS Control Tower がログに記録するイベントの一部がライフサイクルイベントです。ライフサイクルイベントの目的は、リソースの状態を変更する特定の AWS Control Tower アクションの完了を記録することです。ライフサイクルイベントは、組織単位 (OU) またはアカウントに関連するランディングゾーン、ベースライン、コントロールなど、AWS Control Tower が作成または管理するリソースに適用されます。

AWS Control Tower のライフサイクルイベントの特徴

- イベントログは、ライフサイクルイベントごとに生成元の Control Tower アクションが正常に完了したか失敗したかを示します。
- AWS CloudTrail は、各ライフサイクルイベントを非 API AWS サービスイベントとして自動的に記録します。詳細については、[AWS CloudTrail ユーザーガイド](#)を参照してください。
- 各ライフサイクルイベントは、Amazon EventBridge サービスと Amazon CloudWatch Events サービスにも配信されます。注: EventBridge でライフサイクルイベントを受信するには、ログ記録を有効にしたアクティブな AWS CloudTrail 証跡が必要です。経由で配信される AWS サービスイ

イベントの詳細については AWS CloudTrail、「Amazon EventBridge ユーザーガイド」の「[AWS CloudTrail 経由で配信される AWS サービスイベント](#)」を参照してください。

AWS Control Tower のライフサイクルイベントには、主に次の 2 つの利点があります。

- ライフサイクルイベントは AWS Control Tower アクションの完了を記録するため、ライフサイクルイベントの状態に基づいて、オートメーションワークフローの次のステップをトリガーできる Amazon EventBridge ルールや Amazon CloudWatch Events ルールを作成できます。
- ログの詳細を参照することで、管理者や監査人は組織内の特定のタイプのアクティビティを確認できます。

ライフサイクルイベントの仕組み

AWS Control Tower は、そのアクションを実行するために複数のサービスに依存します。したがって、各ライフサイクルイベントは、一連のアクションが完了した後にのみ記録されます。例えば、OU のコントロールを有効にすると、AWS Control Tower はリクエストを実行する一連のサブステップを起動します。この一連のサブステップ全体の最終結果が、ライフサイクルイベントの状態としてログに記録されます。

- 基となるサブステップのすべてが正常に完了すると、ライフサイクルイベントの状態は [Succeeded] (成功) として記録されます。
- 基となるサブステップのいずれかが正常に完了しなかった場合、ライフサイクルイベントの状態は [Failed] (失敗) として記録されます。

各ライフサイクルイベントのログには、AWS Control Tower アクションの開始日時を示すタイムスタンプと、ライフサイクルイベントが成功または失敗として完了した日時を示す別のタイムスタンプが含まれます。

Control Tower でのライフサイクルイベントの表示

ライフサイクルイベントは、AWS Control Tower ダッシュボードの [Activities] (アクティビティ) ページに表示されます。

- [Activities] (アクティビティ) ページに移動するには、左側のナビゲーションペインから [Activities] (アクティビティ) を選択します。
- 特定のイベントの詳細を表示するには、イベントを選択し、右上にある [View details] (詳細を表示) ボタンを選択します。

AWS Control Tower ライフサイクルイベントをワークフローに統合する方法の詳細については、こちらのブログ記事「[Using lifecycle events to track AWS Control Tower actions and trigger automated workflows](#)」(ライフサイクルイベントを使用して AWS Control Tower アクションを追跡し、自動化されたワークフローをトリガーする)を参照してください。

CreateManagedAccount および UpdateManagedAccount ライフサイクルイベントの予想される動作

AWS Control Tower でアカウントを作成するか、アカウントを登録すると、これら 2 つのアクションは同じ内部 API を呼び出します。プロセス中にエラーが発生する場合、通常、エラーはアカウントが作成された後に完全にプロビジョニングされていない場合に発生します。エラーの後にアカウントを作成し直すと、またはプロビジョニングされた製品を更新しようとする、AWS Control Tower はアカウントが既に存在しているものと認識します。

アカウントが存在するため、AWS Control Tower は再試行リクエストの終了時に CreateManagedAccount ライフサイクルイベントではなく UpdateManagedAccount ライフサイクルイベントを記録します。エラーが原因で、別の CreateManagedAccount イベントが表示されると予想されるかもしれませんが、UpdateManagedAccount ライフサイクルイベントが期待される望ましい動作です。

自動化されたメソッドを使用して AWS Control Tower にアカウントを作成または登録する場合は、Lambda 関数をプログラムして UpdateManagedAccount ライフサイクルイベントに加えて CreateManagedAccount ライフサイクルイベントも検索します。

ライフサイクルイベント名

各ライフサイクルイベントには、生成元の AWS Control Tower アクション (AWS CloudTrail にも記録される) に対応する名前が付けられます。例えば、AWS Control Tower CreateManagedAccount CloudTrail イベントによって発生したライフサイクルイベントには、CreateManagedAccount と名前を付けます。

次の一覧に示す名前は、それぞれが JSON 形式でログに記録された詳細の例にリンクされています。これらの例で示す追加の詳細は、Amazon CloudWatch イベントログから取得したものです。

JSON はコメントをサポートしていませんが、例には説明の目的でいくつかのコメントを追加しています。コメントは先頭に「//」を付けて、例の右側に表示しています。

これらの例では、一部のアカウント名と組織名が隠されています。accountId は常に 12 桁の数字であり、例では「xxxxxxxxxxxx」に置き換えられています。organizationalUnitID は、文字と数字の一意の文字列です。例では、その形式を保持しています。

- [CreateManagedAccount](#): このログには、Account Factory を使用して新しいアカウントを作成およびプロビジョニングするためのすべてのアクションを AWS Control Tower が正常に完了したかどうか記録されます。
- [UpdateManagedAccount](#): このログには、Account Factory を使用して以前に作成したアカウントに関連付けられているプロビジョニング済み製品を更新するためのすべてのアクションを AWS Control Tower が正常に完了したかどうか記録されます。
- [EnableGuardrail](#): ログには、AWS Control Tower が OU でコントロールを有効にするためのすべてのアクションを正常に完了したかどうか記録されます。
- [DisableGuardrail](#): ログには、AWS Control Tower が OU のコントロールを無効にするすべてのアクションを正常に完了したかどうか記録されます。
- [SetupLandingZone](#): このログには、ランディングゾーンを設定するためのすべてのアクションを AWS Control Tower が正常に完了したかどうか記録されます。
- [UpdateLandingZone](#): このログには、既存のランディングゾーンを更新するためのすべてのアクションを AWS Control Tower が正常に完了したかどうか記録されます。
- [RegisterOrganizationalUnit](#): このログには、OU に対してガバナンス機能を有効にするためのすべてのアクションを AWS Control Tower が正常に完了したかどうか記録されます。
- [DeregisterOrganizationalUnit](#): このログには、OU に対してガバナンス機能を無効にするためのすべてのアクションを AWS Control Tower が正常に完了したかどうか記録されます。
- [PrecheckOrganizationalUnit](#): この ログには、AWS Control Tower がガバナンスの拡張操作の正常な完了を妨げるリソースを検出したかどうか記録されます。
- [EnableBaseline](#): ログには、AWS Control Tower が OU のターゲットメンバーアカウントで新しいベースラインを有効にするためのすべてのアクションを正常に完了したかどうか記録されます。有効化オペレーションは、EnableBaseline API またはコンソールを使用して開始できます。
- [ResetEnabledBaseline](#): ログには、AWS Control Tower が OU のターゲットメンバーアカウントで有効な既存のベースラインをリセットするためのすべてのアクションを正常に完了したかどうか記録されます。リセットオペレーションは、ResetEnabledBaseline API またはコンソールを使用して開始できます。
- [UpdateEnabledBaseline](#): ログには、AWS Control Tower が OU のターゲットメンバーアカウントで有効な既存のベースラインを更新するためのすべてのアクションを正常に完了したかどうか記録されます。更新オペレーションは、UpdateEnabledBaseline API またはコンソールを使用して開始できます。
- [DisableBaseline](#): ログには、AWS Control Tower が OU のターゲットメンバーアカウントで有効な既存のベースラインを無効化するためのすべてのアクションを正常に完了したかどうか記録

されます。無効化オペレーションは、DisableBaseline API またはコンソールを使用して開始できます。

以下のセクションでは、AWS Control Tower ライフサイクルイベントのリストと、ライフサイクルイベントのタイプごとにログに記録される詳細の例を示します。

CreateManagedAccount

このライフサイクルイベントは、AWS Control Tower が Account Factory を使用して新しいアカウントを正常に作成およびプロビジョニングしたかどうかを記録します。このイベントは、AWS Control Tower CreateManagedAccount CloudTrail イベントに対応します。ライフサイクルイベントログには、新しく作成されたアカウントの `accountName` と `accountId`、アカウントの配置先である OU の `organizationalUnitName` と `organizationalUnitId` が含まれます。

```
{
  "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": "00000000-0000-0000-1111-123456789012",
    "readOnly": false,
```

```

    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "createManagedAccountStatus": {
        "organizationalUnit":{
          "organizationalUnitName":"Custom",
          "organizationalUnitId":"ou-XXXX-13zc8b3h"

        },
        "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

このライフサイクルイベントは、AWS Control Tower が Account Factory を使用して以前に作成したアカウントに関連付けられているプロビジョニング済み製品を正常に更新したかどうかを記録します。このイベントは、AWS Control Tower UpdateManagedAccount CloudTrail イベントに対応します。ライフサイクルイベントログには、関連するアカウントの `accountName` と `accountId`、更新されたアカウントの配置先である OU の `organizationalUnitName` と `organizationalUnitId` が含まれます。

```

{
  "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": "XXXXXXXXXX",
      "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": "00000000-0000-0000-1111-123456789012",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "updateManagedAccountStatus": {
        "organizationalUnit": {
          "organizationalUnitName": "Custom",
          "organizationalUnitId": "ou-XXXX-l3zc8b3h"
        },
        "account": {
          "accountName": "LifeCycle1",
          "accountId": "XXXXXXXXXXXXXX"
        },
        "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

このライフサイクルイベントは、AWS Control Tower が管理している OU のコントロールを AWS Control Tower が正常に有効化したかどうかを記録します。このイベントは、AWS Control Tower EnableGuardrail CloudTrail イベントに対応します。ライフサイクルイベントログには、コントロールの `guardrailId` と `guardrailBehavior`、コントロールを有効にした OU の `organizationalUnitName` と `organizationalUnitId` が含まれます。

```
{
```



```

    "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": "00000000-0000-0000-1111-123456789012",
        "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

このライフサイクルイベントは、AWS Control Tower が管理している OU のコントロールを AWS Control Tower が正常に無効化したかどうかを記録します。このイベントは、AWS Control Tower DisableGuardrail CloudTrail イベントに対応します。ライフサイクルイベントログには、コントロールの guardrailId と guardrailBehavior、コントロールを無効にした OU の organizationalUnitName と organizationalUnitId が含まれます。

```

{
  "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": "00000000-0000-0000-1111-123456789012",
    "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

このライフサイクルイベントは、AWS Control Tower がランディングゾーンを正常に設定したかどうかを記録します。このイベントは、AWS Control Tower SetupLandingZone CloudTrail イベントに対応します。ライフサイクルイベントログには、AWS Control Tower が管理アカウントから作成した組織の ID である `rootOrganizationalId` が含まれます。ログエントリには、AWS Control Tower がランディングゾーンの設定時に作成した、各 OU の `organizationalUnitName` と `organizationalUnitId`、各アカウントの `accountName` と `accountId` が含まれます。

```

{
  "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

このライフサイクルイベントは、AWS Control Tower が既存のランディングゾーンを正常に更新したかどうかを記録します。このイベントは、AWS Control Tower UpdateLandingZone CloudTrail イベントに対応します。ライフサイクルイベントログには、AWS Control Tower が管理する (更新された) 組織の ID である `rootOrganizationalId` が含まれます。ログエントリには、AWS Control Tower が最初のランディングゾーンの設定時に作成した各 OU の `organizationalUnitName` と `organizationalUnitId`、各アカウントの `accountName` と `accountId` が含まれます。

```

{
  "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": "XXXXXXXXXXXX"
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
        }
    }
}

```

```
}  
}
```

RegisterOrganizationalUnit

このライフサイクルイベントは、AWS Control Tower がそのガバナンス機能を OU に対して正常に有効化したかどうかを記録します。このイベントは、AWS Control Tower RegisterOrganizationalUnit CloudTrail イベントに対応します。ライフサイクルイベントログには、AWS Control Tower がそのガバナンス機能を有効にした OU の `organizationalUnitName` と `organizationalUnitId` が含まれます。

```
{  
  "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": "00000000-0000-0000-1111-123456789012",  
    "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

このライフサイクルイベントは、AWS Control Tower がそのガバナンス機能を OU に対して正常に無効化したかどうかを記録します。このイベントは、AWS Control Tower DeregisterOrganizationalUnit CloudTrail イベントに対応します。ライフサイクルイベントログには、AWS Control Tower がそのガバナンス機能を無効にした OU `organizationalUnitName` と `organizationalUnitId` が含まれます。

```

{
    "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": "00000000-0000-0000-1111-123456789012",
    }
}

```



```

    "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

このライフサイクルイベントは、AWS Control Tower が OU に対して正常に事前チェックを実行したかどうかを記録します。このイベントは、AWS Control Tower PrecheckOrganizationalUnit CloudTrail イベントに対応します。ライフサイクルイベントログには、OU 登録プロセス中に AWS Control Tower が事前チェックを実行した各リソースの Id、Name、および failedPrechecks の値のフィールドが含まれます。

イベントログには、accountName、accountId、および failedPrechecks フィールドを含む、事前チェックが実行されたネストされたアカウントに関する情報も含まれます。

failedPrechecks の値が空の場合、そのリソースのすべての事前チェックが正常に終了したことを意味します。

- このイベントは、事前チェックに失敗した場合にのみ発生します。
- 空の OU を登録している場合、このイベントは発生しません。

イベントの例:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
          "SCP_CONFLICT"
        ]
      }
    },
    "accounts": [
      {
        "accountName": "Child Account 1",
        "accountId": "XXXXXXXXXXXX",
        "failedPrechecks": [
          "FAILED_TO_ASSUME_ROLE"
        ]
      },
      {
        "accountName": "Child Account 2",
        "accountId": "XXXXXXXXXXXX",
        "failedPrechecks": [
          "FAILED_TO_ASSUME_ROLE"
        ]
      },
      {
        "accountName": "Management Account",
```

```

        "accountId": "XXXXXXXXXXXX",
        "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
        ],
    },
    {
        "accountName": "Child Account 3",
        "accountId": "XXXXXXXXXXXX",
        "failedPrechecks": []
    },
    ...
],
"state": "FAILED",
"message": "AWS Control Tower failed to register an organizational unit due to
pre-check failures. Go to the OU details page to download a list of failed pre-checks
for the OU and accounts within.",
"requestedTimestamp": "2021-09-20T22:44:02+0000",
"completedTimestamp": "2021-09-20T22:45:43+0000"
}
},
"eventCategory": "Management"
}

```

EnableBaseline

このライフサイクルイベントには、AWS Control Tower が OU のターゲットメンバーアカウントでベースラインを正常に有効化したかどうか記録されます。このイベントは、AWS Control Tower RegisterOrganizationalUnit または EnableBaseline CloudTrail イベントに対応します。ライフサイクルイベントログには、有効化されたベースラインとそのバージョン、ベースラインが有効化された targetIdentifier、親 OU で有効化されたベースラインの parentIdentifier、および SUCCEEDED または FAILED ステータスを示す statusSummary と、オペレーションの追加パラメータとタイムスタンプが含まれます。

```

{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T17:14:57Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableBaseline",

```

```

    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "366911a2-4fa6-4e4a-ac2b-280f627e0027",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
      "enableBaselineStatus": {
        "enabledBaselineDetails": {
          "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
          "parentIdentifier": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
          "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-ern76xmzvf/XXXXXXXXXXXX",
          "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/XXXXXXXXXXXXXXXXXXXX",
          "baselineVersion": "4.0",
          "statusSummary": {
            "lastOperationIdentifier": "37f5eb68-e5b9-4c70-ae76-4ca15f6b16de",
            "status": "SUCCEEDED"
          },
          "parameters": [
            {
              "key": "IdentityCenterEnabledBaselineArn",
              "value": {
                "untyped": {
                  "object": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX"
                }
              }
            }
          ],
          "requestedTimestamp": "2025-02-10T17:07:09+0000",
          "completedTimestamp": "2025-02-10T17:14:57+0000"
        }
      },
      "eventCategory": "Management"
    }
  }
}

```

ResetEnabledBaseline

このライフサイクルイベントには、AWS Control Tower が OU のターゲットメンバーアカウントで有効な既存ベースラインを正常にリセットしたかが記録されます。このイベントは、AWS Control Tower RegisterOrganizationalUnit または ResetEnabledBaseline CloudTrail イベントに対応します。ライフサイクルイベントログには、有効化されたベースラインとそのバージョン、ベースラインが有効化された targetIdentifier、親 OU で有効化されたベースラインの parentIdentifier、および SUCCEEDED または FAILED ステータスを示す statusSummary と、オペレーションの追加パラメータとタイムスタンプが含まれます。

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2025-02-10T21:17:55Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "ResetEnabledBaseline",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "c01a32e1-13ab-4b46-8f1b-00699ef6f989",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "resetEnabledBaselineStatus": {
      "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "parentIdentifier": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-0uh2kplf6d/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/XXXXXXXXXXXXXXXXXXXX",
        "baselineVersion": "1.0",
        "statusSummary": {
```

```

        "lastOperationIdentifier": "3e364c89-89fa-42b8-9776-9f7cc47ba1fa",
        "status": "SUCCEEDED"
    },
    "parameters": []
},
"requestedTimestamp": "2025-02-10T21:14:24Z",
"completedTimestamp": "2025-02-10T21:17:54+0000"
}
},
"eventCategory": "Management"
}

```

UpdateEnabledBaseline

このライフサイクルイベントには、AWS Control Tower が OU のターゲットメンバーアカウントで有効な既存ベースラインを正常に更新したかどうか記録されます。このイベントは、AWS Control Tower RegisterOrganizationalUnit または UpdateEnabledBaseline CloudTrail イベントに対応します。ライフサイクルイベントログには、有効化されたベースラインとそのバージョン、ベースラインが有効化された targetIdentifier、親 OU で有効化されたベースラインの parentIdentifier、および SUCCEEDED または FAILED ステータスを示す statusSummary と、オペレーションの追加パラメータとタイムスタンプが含まれます。

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2025-02-10T19:45:28Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "UpdateEnabledBaseline",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "514f2aff-1a99-4912-bda1-0d4d6662c96e",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {

```

```

    "updateEnabledBaselineStatus": {
      "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "parentIdentifier": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-ern76xmzvf/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/XXXXXXXXXXXXXXXXXXXX",
        "baselineVersion": "4.0",
        "statusSummary": {
          "lastOperationIdentifier": "ba3de28f-83fb-4c9a-8a8c-a4e15fac2c41",
          "status": "SUCCEEDED"
        },
        "parameters": [
          {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": {
              "untyped": {
                "object": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX"
              }
            }
          }
        ],
        "requestedTimestamp": "2025-02-10T19:39:35+0000",
        "completedTimestamp": "2025-02-10T19:45:28+0000"
      },
      "eventCategory": "Management"
    }
  }

```

DisableBaseline

このライフサイクルイベントには、AWS Control Tower が OU のターゲットメンバーアカウントで有効な既存ベースラインを正常に無効化したかどうか記録されます。このイベントは、AWS Control Tower DisableBaseline CloudTrail イベントに対応します。ライフサイクルイベントログには、有効化されたベースラインとそのバージョン、ベースラインが有効化された targetIdentifier、親 OU で有効化されたベースラインの parentIdentifier、および SUCCEEDED または FAILED ステータスを示す statusSummary と、オペレーションの追加パラメータとタイムスタンプが含まれます。

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2025-03-14T00:50:58Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "DisableBaseline",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "704794c4-a32e-4960-8386-c7efaa5a22a1",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "disableBaselineStatus": {
      "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "parentIdentifier": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-0uh2kplf6d/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/XXXXXXXXXXXXXXXXXXXX",
        "baselineVersion": "1.0",
        "statusSummary": {
          "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
          "status": "SUCCEEDED"
        },
        "parameters": []
      },
      "baselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",
        "parentIdentifier": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXXXXXX",

```



```

        "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
        "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXX",
        "baselineVersion": "1.0",
        "statusSummary": {
            "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
            "status": "SUCCEEDED"
        },
        "parameters": []
    },
    "requestedTimestamp": "2025-03-14T00:49:13Z",
    "completedTimestamp": "2025-03-14T00:50:58+0000"
}
},
"eventCategory": "Management"
}

```

でのAWSユーザー通知の使用AWS Control Tower

[AWSユーザー通知](#)を使用すると、AWS Control Towerイベントの通知を受ける配信チャネルを設定できます。指定したルールにイベントが一致した場合に通知を受信します。イベントの通知は、Eメール、[チャットアプリケーション内の Amazon Q Developer](#) のチャット通知、[AWSコンソールモバイルアプリ](#)のプッシュ通知などの複数のチャネルで受け取ることができます。「コンソール通知センター」で通知を確認することもできます。

AWSユーザー通知は集約をサポートしているため、特定のイベント中に受け取る通知の数を減らすことができます。通知は、コンソール通知センターで表示することもできます。

EventBridge の代わりにAWSユーザー通知を通じて通知をサブスクライブする利点は次のとおりです。

- わかりやすいユーザーインターフェイス (UI)。
- グローバルナビゲーションバーのベル/通知エリアで、AWSコンソールとの統合。
- Eメール通知がネイティブにサポートされているため、Amazon SNS の設定が不要。
- 特に、AWSユーザー通知を除くモバイルプッシュ通知のサポートです。

例えば、Security Hub CSPM の重大度が重大で重要度が高い場合、受信する通知のタイプは 1 つです。その通知サブスクリプションを設定するための JSON のコードスニペットは次のようになります。

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

イベントのフィルタリング

- AWSユーザー通知コンソールで使えるフィルターを使用して、サービスと名前でイベントをフィルタリングできます。
- JSON コードから独自の EventBridge フィルターを作成すると、特定のプロパティでイベントをフィルタリングできます。

AWS Control Towerイベントの例

の一般的なイベントの例を次に示しますAWS Control Tower。

- EventBridge イベント。
- AWSユーザー通知を使用して EventBridge イベント (このイベントなど) をサブスクライブできます。

```
{
  "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
        }
    }
}

```

AWS Backup と AWS Control Tower

AWS Backup は、AWS リソースを自動的にバックアップするための計画を作成できるサービスです。AWS Control Tower リソースのバックアップを設定するには、次の 4 つの主なステップに従う必要があります。

1. ランディングゾーン AWS Backup で を有効にします。これは、AWS Control Tower コンソールの [ランディングゾーンの設定] ページで行えます。有効にすると AWS Backup、リソースは複数のアカウントで作成されます。詳細については、「[用に作成されたリソース AWS Backup](#)」を参照してください。
2. AWS Backup コンソールで AWS Control Tower のバックアップにオプトインします。詳細については、「AWS Backup デベロッパーガイド」の「[サポートされるサービスの操作](#)」を参照してください。
3. 含める個々の OUs AWS Backup で を有効にします。このタスクは、ランディングゾーンレベルで AWS Backup を有効にした後、コンソールの [OU の詳細] ページで実行できます。OU AWS Backup で を有効にすると、その OU のアカウントはローカル AWS Backup ポールトを受け取ります。
4. 選択したリソースにタグ付けをし、バックアップに含めます。タグは、そのリソースのバックアップの頻度を示します。バックアッププランは、各リソースのリソースタグで指定されたスケジュールに従います。

詳細については、「[AWS Backup デベロッパーガイド](#)」を参照してください。AWS Control Tower で AWS Backup を設定する場合、料金は発生しません。コストが発生します AWS Backup。料金については、「[AWS Backup の料金](#)」を参照してください。

AWS Control Tower が AWS Control Tower ランディングゾーンで作成する AWS Backup リソースの詳細については、「」を参照してください。 [用に作成されたリソース AWS Backup](#)

Note

AWS Control Tower は、AWS Control Tower サービスで有効にすることなく、AWS Backup サービスを通じて AWS Control Tower リソースのバックアッププランを直接設定することはサポートしていません。

前提条件

AWS Control Tower リソース AWS Backup 用に を設定する前に、既存の AWS Organizations 組織が必要です。AWS Control Tower ランディングゾーンを既に設定している場合は、既存の組織として機能します。

AWS Control Tower に登録されていない他の 2 つの AWS アカウントを割り当てるか、作成する必要があります。これらのアカウントは、中央バックアップアカウントとバックアップ管理者アカウントになります。これらのアカウントにそれぞれ名前を付けます。

また、特に AWS Backup 用のマルチリージョン AWS Key Management Service (KMS) キーを選択または作成する必要があります。

前提条件の定義

- 中央バックアップアカウント - 中央バックアップアカウントは、AWS Control Tower バックアップポールドとバックアップを保存します。このポールドは、このアカウント内の AWS Control Tower AWS リージョン が管理するすべての に作成されます。クロスアカウントコピーは、アカウントが漏洩し、データの復元が必要な場合のために、このアカウントに保存されます。
- バックアップ管理者アカウント - バックアップ管理者アカウントは、AWS Control Tower の AWS Backup サービスの委任管理者アカウントです。Backup Audit Manager (BAM) レポートプランが保存されます。このアカウントは、復元ジョブやコピージョブなど、すべてのバックアップモニタリングデータを集約します。データは Amazon S3 バケットに保存されます。詳細については、「[AWS Backup デベロッパーガイド](#)」の「[AWS Backup コンソールを使用したレポートプランの作成](#)」を参照してください。
- マルチリージョン AWS KMS キーのポリシー要件

AWS KMS キーにはキーポリシーが必要です。組織の管理アカウントに関連付けられたアクセス許可を持つプリンシパル (ユーザーとロール) へのアクセスを制限する、次のようなキーポリシーを検討してください。

JSON

```
{
  "Version": "2012-10-17",
  "Id": "KMS key policy",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
```

```

        "Principal": {
            "AWS": "arn:aws:iam::111122223333:root"
        },
        "Action": "kms:*",
        "Resource": "*"
    },
    {
        "Sid": "Allow use of the KMS key for organization",
        "Effect": "Allow",
        "Principal": {
            "AWS": "*"
        },
        "Action": [
            "kms:Decrypt",
            "kms:DescribeKey",
            "kms:GenerateDataKey*",
            "kms:Encrypt",
            "kms:ReEncrypt*",
            "kms:GetKeyPolicy",
            "kms:CreateGrant",
            "kms:ListGrants",
            "kms:RevokeGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "ORGANIZATION-ID"
            }
        }
    }
]
}

```

このポリシー例では、組織のすべてのアカウントに暗号化されたバックアップデータへのアクセスを許可します。[AWS グローバル条件キー](#)と[AWS KMS 条件キー](#)を使用し、バックアップへのアクセスを必要とするプリンシパルに応じてアクセス許可を絞り込みます。

Note

マルチリージョン AWS KMS キーは、AWS Control Tower で管理する AWS リージョン 予定のすべてのリージョンにレプリケートする必要があります。

バックアップの有効化

ランディングゾーンの設定時、またはランディングゾーンの更新時に、AWS Control Tower に登録されているアカウントのリソースのバックアップを有効化できます。

[前提条件](#) として、以下のアイテムを指定する必要があります。

- AWS Backup 管理者アカウント AWS アカウント として機能する。
- AWS Backup 中央バックアップアカウント AWS アカウント として機能する。
- クロスアカウントバックアップ用に管理するマルチリージョン AWS KMS キー

バックアップを有効化する方法

有効化プロセスには主に 2 つの部分があります。まず、ランディングゾーンのバックアップを有効化し、それから、バックアップを必要とする登録済み OU ごとにバックアップを有効化します。

最初の部分: ランディングゾーンのバックアップを設定する

コンソール: [ランディングゾーン設定] ページの AWS Control Tower コンソールでランディングゾーンのバックアップを設定できます。このオプションは、最初のランディングゾーンの設定オペレーション中に表示され、ランディングゾーンの更新を使用し、後で保持できます。

API: AWS Control Tower ランディングゾーンが既にある場合は [UpdateLandingZone](#) API を呼び出し、AWS Control Tower を初めて設定する場合は [CreateLandingZone](#) API を呼び出すことで、AWS Control Tower API でバックアップを有効化できます。(ヒント: その後、[EnableBaseline](#) API を呼び出して、必要な OU ごとにバックアップを確立します。)

AWS Control Tower コンソールの外部

ランディングゾーンのバックアップの有効化には、AWS Control Tower コンソール以外のステップが含まれます。リソースを確認するには、AWS Backup コンソールに移動する必要があります。

オプトインリソースタイプを確認するか、追加のリソースタイプにオプトインするには

1. で AWS Backup コンソールを開きます <https://console.aws.amazon.com/backup>。
2. ナビゲーションペインで [設定] を選択します。
3. [サービスのオプトイン] ページで、[リソースを設定] を選択します。

4. トグルスイッチを使用して、含めるサービスを有効または無効にします AWS Backup。AWS Control Tower 環境の一部であるかどうかに関わらず、RDS、EC2、DDB など、バックアップするリソースが選択されていることを確認してください。

詳細については、「[による サービスの管理にオプトイン AWS Backup](#)する」を参照してください。

新しいリソースタイプに関する考慮事項

AWS Backup を使用して AWS サービスのリソースのデータ保護を管理する前に、前の手順を実行し、そのサービスの AWS Backup をオプトインする必要があります。また、AWS Backup サービスが今後追加のサービスとそのリソースタイプのサポートを追加するため、AWS Control Tower でそのリソースタイプをバックアップ AWS Backup する前に、この手順を繰り返し、追加のリソースタイプごとにオプトインする必要があります。サポートされていないリソースタイプをタグ付けすると、バックアップが失敗する可能性があります。

ランディングゾーンのバックアップを有効化すると、AWS Control Tower は、中央バックアップアカウントとバックアップ管理者アカウントとして指定した 2 つのアカウントをそれぞれ確立します。AWS Control Tower は、これらのアカウントおよび他のアカウントに[リソース](#)を作成します。

Important

AWS Control Tower 監査アカウントとログアーカイブアカウントのバックアップを有効化するには、EnableBaseline API を呼び出してセキュリティ OU のバックアップを設定する必要があります。そのようにすることをお勧めします。

推奨されるプランと保持期間は次のとおりです。

- 時間単位のバックアップ = ローカルポールドは 2 週間の保持、中央バックアップポールドはコピーなし
- 日単位のバックアップ = ローカルポールドは 2 週間の保持、中央バックアップポールドは 1 か月の保持
- 週単位のバックアップ = ローカルポールドは 1 か月の保持、中央バックアップポールドは 3 か月の保持

- 月単位のバックアップ = ローカルポールドは 3 か月の保持、中央バックアップポールドは 3 か月の保持

バックアッププランの作成方法については、「[AWS Backup コンソールを使用したレポートプランの作成](#)」を参照してください。

次のパート: OU でバックアップを有効化する

ランディングゾーン設定 AWS Backup で を有効にしたら、追加のステップを実行して、バックアップする特定の OUs でバックアップを有効にする必要があります。ランディングゾーン AWS Backup に対して を有効にしている場合、コンソールの OU の詳細ページにセクションが表示され、OU のバックアップを有効にするを選択できます。ランディングゾーンレベルでバックアップを有効化していない場合、OU の詳細ページにこのセクションは表示されません。

OU で BackupBaseline を有効化するには、その OU で既に AWSControlTowerBaseline が有効になっている必要があります。各 OU の登録済みアカウントでは、AWSControlTowerBaseline が有効化されています。

選択したアカウントと OU で、AWS Control Tower は追加のリソースを設定します。

- ローカルバックアップポールド

AWS Control Tower は、アカウントにローカルバックアップポールドを作成し、4 種類のバックアッププランをポールドにアタッチします。AWS Control Tower で作成されたバックアッププランには、プレフィックスがタグ付けられます。

```
BackupPlanTags:
  aws-control-tower: 'managed-by-control-tower'
```

- バックアッププランには、時間単位、日単位、週単位、月単位の 4 種類があります。

各プランは、タグベースのリソース割り当てに関連付けられます。例えば、aws-control-tower-backuphourly : true でタグ付けされたリソースは、時間単位のバックアッププランで保護されます。

- アカウントのローカルバックアップロール

AWS Control Tower は、バックアップに使用される IAM ロールを作成します。ロールには 4 つの特定のアクセス許可が必要です。

```
"backup:UpdateGlobalSettings","organizations:RegisterDelegatedAdministrator","organizations:E
```

ロールには、のサービスプリンシパルとの信頼関係があります AWS Backup。ロールの名前は aws-controltower-backup-role、次の管理アクセス許可がアタッチされています。

- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForS3Backup](#)
- [AWSBackupServiceRolePolicyForS3Restore](#)

バックアップ用のリソースをタグ付けする

AWS Control Tower でバックアップを設定するプロセスの一環として、バックアッププランに含めるリソースをタグ付けします。タグはバックアップの頻度を指定します。これらは可能性のあるタグです。

- aws-control-tower-backuphourly : true
- aws-control-tower-backupdaily: true
- aws-control-tower-backupweekly: true
- aws-control-tower-backupmonthly: true

考慮事項

- AWS Backup が OU でアクティブな場合、AWS Control Tower コンソールの OU の詳細ページの Status フィールドに Enabled の値が表示されます。[ステータス] フィールドの値には、[有効になっていません]、[進行中]、[失敗] などがあります。ステータスが Failed の場合は、OU の再登録を選択して AWS Backup 設定を OU に再適用します。
- OU で AWS Backup を有効にしている場合、その OU に含まれる Account Factory を通じてプロビジョニングされた新しいアカウント AWS Backup。

バックアップを無効にする

ランディングゾーンの設定中、またはランディングゾーンの更新時に、AWS Control Tower に登録されているアカウントのリソースのバックアップを無効にできます。

バックアップを無効にするには、主に 2 つのステップが必要です。まず、バックアップが有効になっている各 OU の AWS Backup ベースラインをオフにしてから、ランディングゾーンのバックアップをオフにします。

最初のステップ: OU のバックアップを無効にする

AWS Backup が有効になっている場合は、ランディングゾーン AWS Backup をオフにする前に、すべての OUs から AWS Backup ベースラインを無効にする必要があります。

OU の AWS Backup ベースラインを無効にするには、DisableBaseline API を呼び出します。ネストされた OU はこのステータスを継承するため、AWS Backup ベースラインも無効化されます。

コマンドの例:

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

AWS Backup ベースラインを無効にすると、AWS Control Tower は次のリソースをクリーンアップします。

- に関連するすべてのスタックセット AWS Backup
- に関連するすべてのコントロール AWS Backup

Note

ローカルボールの保持ポリシーは Retain に設定されているため、スタックセットが削除されてもローカルボールは保持されます。データが保持されます。

次のステップ: ランディングゾーン AWS Backup の をオフにする

OU へのバックアップを無効にして前提条件を満たした後、AWS Control Tower コンソールからバックアップを無効にするには、[ランディングゾーン設定] ページに移動します。[バックアップを無効化する] を選択します。

オフにすると AWS Backup、AWS Control Tower は次のリソースを変更します。

- に関連するすべてのスタックセットを削除します。AWS Backup
- セキュリティ OU AWS Backup の に関連するすべてのコントロールを非アクティブ化します

- AWS Backup 管理のための委任管理者アカウントの登録を解除します
- 管理者アカウントと中央バックアップアカウントから AWS Control Tower ガバナンス (CloudTrail AWS Config など) AWS Backup を削除します
- AWS Control Tower AWS Backup は、データを含むボールドと Amazon S3 バケットリソースを保持します

バックアップを無効化すると、新しいバックアップは作成されませんが、既存のバックアップは削除されません。

移動したアカウントでバックアップを有効化する

AWS Backup が有効になっている AWS Control Tower OU にアカウントを移動し、そのアカウントが AWS Control Tower に登録されていない場合、バックアッププランはアカウントに自動的に適用されません。

コンソール: AWS Control Tower コンソールから個々のアカウント AWS Backup に対して を有効にするには、アカウントの詳細ページでアカウントの更新を選択するか、OU の詳細ページで OU の再登録を選択して複数のアカウントを同時に更新できます。

API: API からバックアップベースラインが有効になっている OU にアカウントを移動する場合、その OU で `ResetEnabledBaseline` API を呼び出し、OU の `EnabledBaseline` リソースをターゲットとして指定して、OU からの継承によってアカウントのバックアップをトリガーできます。

コマンドの例:

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier
arn:aws:controltower:REGION:NAMESPACE:enabledbaseline/X0SD0RW8HDB5ZNWEE --region us-
east-1
```

レスポンスの例:

```
{
  "operationIdentifier": "0bbdb587-c849-4152-95c6-7afa7664ee71"
}
```

AWS Control Tower のバックアップドリフト

ドリフトは AWS Control Tower AWS Backup の設定では報告されません。AWS Control Tower のドリフトの詳細については、「[AWS Control Tower のドリフトを検出し、解決する](#)」を参照してください。

AWS Backup プランを削除または変更すると、プランがドリフト状態になる可能性があります。次に回避すべきいくつかの変更を示します。

- バックアップ管理者アカウントをセキュリティ OU から移動しないでください。
- 中央バックアップアカウントをセキュリティ OU から移動しないでください。
- バックアップ管理者アカウントを組織から削除しないでください。
- 中央バックアップアカウントを組織から削除しないでください。
- セキュリティ OU に適用される AWS Backup SCP をデタッチ、アタッチ、または更新しないでください。
- 他の OUs に適用される AWS Backup SCP をデタッチ、アタッチ、または更新しないでください。
- AWS Backup のバックアップ管理者アカウントのアクセス許可を削除しないでください。
- クロスアカウントバックアップ設定を更新して、クロスアカウントバックアップを無効にしないでください。クロスアカウントバックアップの詳細については、「AWS Backup API リファレンス」の「[UpdateGlobalSettings](#)」を参照してください。
- AWS KMS キーを削除しないでください。
- 設定後に AWS KMS キーポリシーを変更しないでください。
- サービスの信頼されたアクセスを無効にしないでください AWS Backup。

Note

ドリフトは、AWS Control Tower の AWS Backup リソースを保護する SCP ベースのコントロールのステータスに関して報告されます。

用に作成されたリソース AWS Backup

このページの表は、を有効にしたときに AWS Control Tower アカウントで作成されたリソースを示しています AWS Backup。

次の表は、ランディングゾーン組織 AWS Backup に対して を有効にするときに AWS Control Tower が AWS Control Tower Central Backup アカウントで作成するリソースを示しています。

説明	中央バックアップアカウントのリソース
どの OU にアカウントが含まれていますか？	セキュリティ OU
リソースを作成したアクション	ランディングゾーンの作成または更新
どのようなリソースが作成されますか？	中央バックアップポールドット —aws-controltower-central-backupvault-*
どのリージョンが含まれていますか？	すべての管理対象リージョン
これらのリソースに関連するコントロールは何ですか？	CT.BACKUP.PV.3

次の表は、ランディングゾーン組織 AWS Backup に対して を有効にするときに AWS Control Tower が AWS Control Tower Backup Administrator アカウントで作成するリソースを示しています。

説明	Backup 管理者アカウントのリソース: これは の委任管理者アカウントです AWS Backup
どの OU にアカウントが含まれていますか？	セキュリティ OU
リソースを作成したアクション	ランディングゾーンの作成または更新
どのようなリソースが作成されますか？	Backup Audit Manager (BAM) - aws_controltower_copy_report - aws_controltower_backup_report - aws_controltower_restore_report BAM ログを保存するための Amazon S3 バケット —aws-controltower-backup-reports- <i>{accountId}</i> -*

説明	Backup 管理者アカウントのリソース: これは の委任管理者アカウントです AWS Backup Amazon S3 アクセスログ記録バケット —aws- controltower-backup-reports-log- <i>{accountId}</i> -*
どのリージョンが含まれていますか？	ホームリージョン
これらのリソースに関連するコントロールは何ですか？	- CT.BACKUP.PV.2 - CT.S3.PV.1 - CT.S3.PV.1

次の表は、セキュリティ OU AWS Backup に対して を有効にすると、AWS Control Tower 監査アカウントと AWS Control Tower Log Archive アカウントで AWS Control Tower が作成するリソースを示しています。

説明	監査アカウントとログアーカイブアカウントのリソース
どの OU にアカウントが含まれていますか？	セキュリティ OU
リソースを作成したアクション	の有効化 BackupBaseline
どのようなリソースが作成されますか？	- ローカルバックアップボールド —aws-controltower-local-backupvault-* - ローカルバックアップロール -aws-controltower-BackupRole 4 つのローカルバックアッププラン (時間単位、週単位、月単位、日単位) - aws-controltower-hourly-backup-plan - aws-controltower-daily-backup-plan

説明	監査アカウントとログアーカイブアカウントのリソース
	- aws-controltower-weekly-backup-plan - aws-controltower-monthly-backup-plan - IAM ロール —aws-controltower-BackupRole
どのリージョンが含まれていますか？	すべての管理対象リージョン
これらのリソースに関連するコントロールは何ですか？	- CT.BACKUP.PV.3 - CT.IAM.PV.1 - CT.BACKUP.PV.3 - CT.BACKUP.PV.1

 Note

BackupBaseline をセキュリティ OU に適用すると、監査アカウントとログアーカイブアカウントだけでなく、その OU 内のすべてのメンバーアカウントが AWS Backup リソースを受け取ります。

次の表は、ターゲット OU で を有効にしたときに AWS Control Tower が AWS Control Tower OU メンバーアカウント AWS Backup で作成するリソースを示しています。

説明	他の OUs のメンバーアカウントのリソース
どの OU にアカウントが含まれていますか？	セキュリティ OU 以外の OU
リソースを作成したアクション	の有効化 BackupBaseline
どのようなリソースが作成されますか？	ローカルバックアップボールド —aws-controltower-local-backupvault-*

説明	他の OUs のメンバーアカウントのリソース
	- ローカルバックアップロール -aws-controltower-BackupRole 4 つのローカルバックアッププラン (時間単位、週単位、月単位、日単位) - aws-controltower-hourly-backup-plan - aws-controltower-daily-backup-plan - aws-controltower-weekly-backup-plan - aws-controltower-monthly-backup-plan - IAM ロール —aws-controltower-BackupRole
どのリージョンが含まれていますか？	すべての管理対象リージョン
これらのリソースに関連するコントロールは何ですか？	- CT.BACKUP.PV.3 - CT.IAM.PV.1 - CT.BACKUP.PV.3 - CT.BACKUP.PV.1

AWS バックアップのコントロール

AWS Control Tower ランディングゾーン AWS Backup で を有効にすると、環境内でいくつかの予防コントロールがアクティブ化されます。これらのコントロールは、AWS Control Tower を操作する AWS Backup ために必要なリソースを保護します。ランディングゾーンで が有効になっていない場合 AWS Backup 、これらのコントロールを有効にすることはできません。

コントロールの詳細については、「[AWS Backupのコントロール](#)」を参照してください。

AWS Control Tower のランディングゾーンを廃止する

AWS Control Tower では、ランディングゾーンと呼ばれる安全なマルチアカウント AWS 環境を設定および管理できます。AWS Control Tower が配置したすべてのリソースをクリーンアップするプロセスは、ランディングゾーンの廃止と呼ばれます。

AWS Control Tower を使用しなくなった場合は、自動廃止ツールによって AWS Control Tower によって割り当てられたリソースがクリーンアップされます。自動廃止プロセスを開始するには、[Landing Zone Settings] (ランディングゾーンの設定) ページで [decommission] (廃止) タブを選択し、[Decommission landing zone] (ランディングゾーンの廃止) を選択します。

廃止処理中に実行するアクションの一覧に関しては、「[廃止プロセスの概要](#)」を参照してください。

Warning

すべての AWS Control Tower リソースを手動で削除することは、廃止とは異なります。この場合、新しいランディングゾーンを設定することはできません。

データおよび既存の AWS Organizations は、次の方法で廃止プロセスによって変更されません。

- データは削除されず、AWS Control Tower によって作成されたランディングゾーンの一部のみが削除されます。
- 廃止プロセスの完了後は、Simple Storage Service (Amazon S3) バケットや Amazon CloudWatch Logs ロググループなどの一部のリソースアーティファクトが残ります。これらのリソースは、別のランディングゾーンを設定する前に、手動で削除する必要があります。これにより、特定のリソースの保守に伴い派生する可能性があるコストを回避できます。
- 自動廃止を使用して、部分的にセットアップされたランディングゾーンを削除することはできません。ランディングゾーンのセットアッププロセスが失敗した場合、自動廃止を有効にするには、障害状態を解決してセットアップを完了する必要があります。または、リソースを個別に手動で削除する必要があります。

ランディングゾーンの廃止は、重大な影響を引き起こす処理であり、元に戻すことはできません。AWS Control Tower によって実行される廃止アクション、および廃止後に残るアーティファクトについては、次のセクションで説明します。

⚠ Important

この廃止プロセスは、ランディングゾーンの使用を停止する場合にのみ実行することを強くお勧めします。既存のランディングゾーンを廃止した後に再作成することはできません。

廃止プロセスの概要

ランディングゾーンの廃止をリクエストすると、AWS Control Tower は次のアクションを実行します。

- ランディングゾーンで有効になっている各検出コントロールを無効にします。AWS Control Tower は、コントロールをサポートする CloudFormation リソースを削除します。
- サービスコントロールポリシー (SCPs) を削除して、各予防コントロールを無効にします AWS Organizations。ポリシーが空欄の場合 (AWS Control Tower が管理するすべての SPC の削除後に空欄になる)、AWS Control Tower は、ポリシーを完全にデタッチし、削除します。
- CloudFormation StackSets としてデプロイされたすべてのブループrintを削除します。
- CloudFormation スタックとしてデプロイされたすべてのリージョンのすべてのブループrintを削除します。
- プロビジョニングされたアカウントごとに、AWS Control Tower は、廃止プロセス中に以下のアクションを実行します。
 - 各 Account Factory アカウントのレコードを削除します。
 - AWS Control Tower が作成した IAM ロールを削除し、アカウントへの AWS Control Tower アクセス許可を取り消し (追加のポリシーが追加されていない限り)、標準の OrganizationsFullAccessRole IAM ロールを再作成します。
 - アカウントのレコードを から削除します AWS Service Catalog。
 - Account Factory 製品およびポートフォリオを AWS Service Catalog から削除します。
- 共有 (監査およびログアーカイブ) アカウントのブループrintを削除します。
- AWS Control Tower が作成した IAM ロールを削除して、共有アカウントから AWS Control Tower アクセス許可を取り消し (追加のポリシーが追加されていない限り)、OrganizationsFullAccessRole IAM ロールを再作成します。
- 共有アカウントに関連するレコードを削除します。
- ユーザー作成の OU に関連するレコードを削除します。
- ホームリージョンを識別する内部レコードを削除します。

Note

廃止後、VPC が空でない場合は、Account Factory VPC ブループリント (BP_ACCOUNT_FACTORY_VPC) を削除して、ルートと NAT ゲートウェイをクリーンアップすることもできます。

ランディングゾーンの廃止方法

コンソールから AWS Control Tower のランディングゾーンを廃止するには、ここで示す手順に従います。

Note

廃止する前に、登録済みアカウントの管理を解除することをお勧めします。

1. AWS Control Tower コンソールの [Landing Zone Settings] (ランディングゾーンの設定) ページに移動します。
2. [Decommission your landing zone] (ランディングゾーンを廃止します) セクションにある [Decommission your landing zone] (ランディングゾーンを廃止します) を選択します。
3. 実行しようとしているアクションと必要な確認プロセスについて説明するダイアログが表示されます。廃止の意思を確認するには、すべてのボックスを選択し、要求どおりに確認を入力する必要があります。

Important

廃止プロセスは元に戻せません。

4. ランディングゾーン廃止の意思を確認すると、廃止処理中に AWS Control Tower ホームページにリダイレクトされます。この処理には最長で 2 時間かかります。
5. 廃止処理が成功した場合は、AWS Control Tower コンソールから新しいランディングゾーンを設定する前に、残ったリソースを手動で削除する必要があります。これらの残ったリソースには、特定の Amazon S3 バケット、組織、CloudWatch Logs ロググループが含まれます。

Note

これらのアクションは、請求およびコンプライアンス作業に重大な影響を及ぼす可能性があります。例えば、これらのリソースの削除に失敗すると、予期しない請求が発生する可能性があります。

リソースを手動で削除する方法の詳細については、「[AWS Control Tower リソースの削除について](#)」を参照してください。

- 新しい AWS リージョンに新しいランディングゾーンを設定する場合は、この追加ステップに従います。CLI を開いて、次のコマンドを入力します。

```
aws organizations disable-aws-service-access --service-principal  
controltower.amazonaws.com
```

API を使用してランディングゾーンを廃止する

ランディングゾーンのすべてのリソースをクリーンアップするプロセスは、ランディングゾーンの廃止と呼ばれます。

Important

この廃止プロセスは、ランディングゾーンの使用を停止する場合にのみ実行することを強くお勧めします。既存のランディングゾーンを廃止した後に再作成することはできません。

AWS Control Tower がデータと既存のを処理する方法に関する重要な情報など、ランディングゾーンの廃止の詳細については AWS Organizations、「」を参照してください[AWS Control Tower のランディングゾーンを廃止する](#)。

ランディングゾーンを廃止するには、DeleteLandingZone API を呼び出します。この API は OperationIdentifier を返します。これを使用して GetLandingZoneOperation API を呼び出し、削除オペレーションのステータスを確認できます。

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

出力:

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

廃止後に必要な手動クリーンアップタスク

このセクションでは、最初の廃止のステップ後に実行する必要がある手動クリーンアップタスクを一覧表示します。

- landing zone を廃止した後に新しいランディングゾーンを作成する場合、ロギングアーカイブアカウントと監査アカウントに異なる E メールアドレスを指定する必要があります。そうでない場合、既存のロギングアーカイブアカウントまたは監査アカウントを持ち込むための手順に従ってください。
- aws-controltower/CloudTrailLogs という CloudWatch Logs ロググループは、別のランディングゾーンを設定する前に手動で削除する必要があります。
- ログ用に予約された 2 つの Amazon S3 バケットは、手動で削除するか、名前を変更する必要があります。
- 既存の [Security] (セキュリティ) 組織と [Sandbox] (サンドボックス) 組織は、手動で削除するか、名前を変更する必要があります。

Note

AWS Control Tower の [Security OU] (セキュリティ OU) 組織を削除する前に、まずロギングアカウントと監査アカウントを削除する必要がありますが、管理アカウントは削除する必要はありません。これらのアカウントを削除するには、監査アカウントとロギングアカウントに [ルートユーザーとしてサインインする場合](#) (ルートユーザーとしてログイン) し、個別に削除する必要があります。

- AWS Control Tower の AWS IAM アイデンティティセンター (IAM Identity Center) 設定を手動で削除することもできますが、既存の IAM Identity Center 設定に進むことができます。
- AWS Control Tower によって作成された VPC を削除し、関連する AWS CloudFormation スタックセットも削除することもできます。

- 新しい AWS リージョンで新しいランディングゾーンを設定する前に、以下の追加ステップに従う必要があります。
- CLI を開いて、次のコマンドを入力します。

```
aws organizations disable-aws-service-access --service-principal  
controltower.amazonaws.com
```

- 残っているマネージドルール (AWSControlTowerManagedRule) を、すべての管理対象リージョンで共有アカウントおよびメンバーアカウントから削除します。AWSControlTowerManagedRule は Amazon EventBridge ルールです。

廃止処理中に削除されないリソース

ランディングゾーンを廃止しても、AWS Control Tower セットアッププロセスは完全には元に戻りません。一部のリソースは残るため、手動で削除しなければならない場合があります。

AWS Organizations

既存の AWS Organizations 組織を持たないお客様の場合、AWS Control Tower は 1 つ以上の組織単位 (OUs。指定されたセキュリティ OU と、オプションで作成されたサンドボックス OU。ランディングゾーンを廃止すると、組織の階層は次のように保持されます。

- AWS Control Tower コンソールから作成した組織単位 (OU) は削除されません。
- セキュリティ OU とサンドボックス OU は削除されません。
- 組織は から削除されません AWS Organizations。
- AWS Organizations (共有、プロビジョニング、または管理) のアカウントは移動または削除されません。

AWS IAM アイデンティティセンター (SSO)

既存の IAM Identity Center ディレクトリを持たないお客様の場合、AWS Control Tower により、IAM Identity Center が設定され、初期ディレクトリが構成されます。ランディングゾーンを廃止しても、AWS Control Tower は、IAM Identity Center に対して変更を行いません。必要であれば、管理アカウントに保管されている IAM Identity Center 情報は手動で削除できます。特に、これらの領域に廃止による変更はありません。

- Account Factory で作成されたユーザーは削除されません。

- AWS Control Tower のセットアップによって作成されたグループは削除されません。
- AWS Control Tower によって作成された許可セットは削除されません。
- AWS アカウントと IAM Identity Center アクセス許可セット間の関連付けは削除されません。
- IAM Identity Center のディレクトリは変更されません。
- AWS Control Tower のこれらの IAM Identity Center ポリシーは削除されません。
 - `AWSControlTowerAdminPolicy`
 - `AWSControlTowerCloudTrailRolePolicy`
 - `AWSControlTowerStackSetRolePolicy`

ロール

セットアップ中、AWS Control Tower はユーザーに代わって特定のロールを作成するか (コンソールを使用する場合)、それらのロールを作成するようユーザーに求めます (API を使用してランディングゾーンをセットアップする場合)。ランディングゾーンを廃止しても、次のロールは削除されません。

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

Note

メンバーアカウントの `AWSControlTowerExecution` ロールは、AWS Control Tower がユーザーに代わってロールを作成したか、手動でロールを作成したかにかかわらず、ランディングゾーンが削除されると削除されます。ただし、このロールに追加のポリシーをアタッチした場合、またはこのロールにアタッチされたポリシーを変更した場合、AWS Control Tower はランディングゾーンの削除中にこのロールを削除できない場合があります。このような場合、ランディングゾーンの削除は成功しますが、ロールはメンバーアカウントに保持されます。

Amazon S3 バケット

セットアップ中、AWS Control Tower は AWS CloudTrail のログアーカイブアカウントと AWS Config 統合の設定中央アグリゲータアカウントにバケットを作成します。AWS Control Tower は、これらの各アカウントのログ記録とアクセスのログ記録用のバケットを作成します。ランディングゾーンを廃止しても、次のリソースは削除されません。

- ログアーカイブアカウントの S3 バケットのログ記録とアクセスログ記録は削除されません。
- 設定中央アグリゲータアカウントのログ記録とログ記録アクセス S3 バケットは削除されません。
- これらの各アカウントのログ記録およびログ記録アクセスバケットの内容は削除されません。

サービス統合アカウント

AWS Control Tower では、各サービス統合設定に中央アカウントが必要です。このアカウントは、ランディングゾーンのバージョンに基づいて AWS Control Tower のセットアップ中に作成される場合と作成されない場合があります。ランディングゾーンを廃止した場合:

- AWS Control Tower のセットアップ中に作成されたサービス統合アカウントは閉じられません。
- IAM OrganizationAccountAccessRole ロールは、標準 AWS Organizations 設定に合わせて再作成されます。
- AWSControlTowerExecution ロールが削除されます。

プロビジョニングされたアカウント

AWS Control Tower のお客様は、Account Factory を使用して新しい AWS アカウントを作成できます。ランディングゾーンを廃止した場合:

- Account Factory で作成したプロビジョニングされたアカウントは閉鎖されません。
- のプロビジョニング済み製品は削除 AWS Service Catalog されません。それらを終了してクリーンアップすると、それらのアカウントは [Root OU] (ルート OU) に移動されます。
- AWS Control Tower によって作成された VPC は削除されず、関連する AWS CloudFormation スタックセット (BP_ACCOUNT_FACTORY_VPC) も削除されません。
- IAM OrganizationAccountAccessRole ロールは、標準 AWS Organizations 設定に合わせて再作成されます。
- AWSControlTowerExecution ロールが削除されます。

CloudWatch Logs ロググループ

- aws-controltower/CloudTrailLogs という CloudWatch Logs ロググループが、AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER という名前のブループリントの一部として作成されます。このロググループは削除されません。代わりに、ブループリントが削除され、リソースは保持されます。

Note

ランディングゾーン 3.0 以降のお客様は、個々の登録済みアカウントの CloudTrail ログと CloudTrail ログのロールを削除する必要はありません。これらは、組織レベルの証跡用に管理アカウントでのみ作成されるためです。

ランディングゾーンバージョン 3.2 以降、AWS Control Tower は AWSControlTowerManagedRule という Amazon EventBridge ルールを作成します。このルールは、すべての管理対象リージョンで、メンバーアカウントごとに作成されます。ルールは廃止時に自動的に削除されないため、新しいリージョンでランディングゾーンを設定する前に、すべての管理対象リージョンのサービス統合アカウントとメンバーアカウントからルールを手動で削除する必要があります。

AWS Control Tower リソースを削除する方法の手順については、「[AWS Control Tower リソースを削除する](#)」を参照してください。

AWS Control Tower リソースを削除する

このドキュメントでは、定期的なメンテナンスおよび管理タスクの一環として、AWS Control Tower リソースを削除する方法の手順を示します。この章で説明する手順は、必要に応じて個々のリソースまたはいくつかのリソースを削除することのみを目的としています。これは、ランディングゾーンの廃止とは異なります。

以下の 2 種類のタスクでリソースの削除が必要になることがあります。

- ランディングゾーンを通常の状況で管理するときにリソースを削除する場合。
- 自動廃止処理後に残っているリソースをクリーンアップする場合。

⚠ Warning

リソースを手動で削除すると、新しいランディングゾーンを設定できなくなります。これは、廃止とは異なります。AWS Control Tower のランディングゾーンを廃止する場合は、この章で説明されているアクションを実行する前に、「[AWS Control Tower のランディングゾーンを廃止する](#)」の指示に従ってください。この章の手順は、自動廃止が完了した後に残っているリソースをクリーンアップするのに役立ちます。すべてのランディングゾーンリソースを手動で削除しても、その削除はランディングゾーンの廃止とは異なり、予期しない料金が発生する可能性があります。

AWS Control Tower からアカウントを削除する必要がある場合は、次のセクションを参照してアカウントを閉鎖してください。

- [アカウントの管理を解除する](#)
- [Account Factory で作成されたアカウントを解約する](#)

削除ではなく廃止が必要か

AWS Control Tower を企業で使用しなくなった場合、または組織のリソースに大幅な再デプロイが必要な場合は、ランディングゾーンを最初にセットアップしたときに作成されたリソースを廃止することができます。

- 廃止プロセスの完了後は、Simple Storage Service (Amazon S3) バケットや Amazon CloudWatch Logs ロググループなどの一部のリソースアーティファクトが残ります。
- 別のランディングゾーンを設定する前に、アカウントの残りのリソースを手動でクリーンアップし、予期しない請求が発生する可能性を回避する必要があります。詳細については、「[廃止処理中に削除されないリソース](#)」を参照してください。

⚠ Warning

廃止プロセスは、ランディングゾーンの使用を停止する場合にのみ実行することを強くお勧めします。このプロセスは元に戻せません。

AWS Control Tower リソースの削除について

この章の個々の手順では、AWS Control Tower リソースを手動で削除する方法を示します。これらの手順は、ランディングゾーンから特定のリソースを削除する必要があるときに実行できます。

これらの手順を実行する前に、特に明記されていない限り、ランディングゾーンのホームリージョンの AWS マネジメントコンソール にサインインし、ランディングゾーンを含む管理アカウントの管理者権限を持つ IAM ユーザーまたは IAM Identity Center のユーザーとしてサインインする必要があります。

Warning

これらは、AWS Control Tower 設定にガバナンスドリフトを発生させる可能性がある破壊的なアクションです。元に戻すことはできません。

トピック

- [SCP の削除](#)
- [StackSets およびスタックの削除](#)
- [ログアーカイブアカウントでの Simple Storage Service \(Amazon S3\) バケットの削除](#)
- [Account Factory ポートフォリオおよび製品を削除する](#)
- [AWS Control Tower のロールとポリシーを削除する](#)
- [AWS Control Tower リソースのヘルプ](#)

SCP の削除

AWS Control Tower では、コントロールのサービスコントロールポリシー (SCP) が使用されます。この手順では、AWS Control Tower に明示的に関連付けられている SCP を削除する方法を示します。

AWS Organizations SCPsを削除するには

1. Organizations コンソール (<https://console.aws.amazon.com/organizations/>) を開きます。
2. [Policies] (ポリシー) タブを開き、プレフィックス [aws-guardrails-] のサービスコントロールポリシー (SCP) を見つけ、SCP ごとに以下を実行します。
 - a. 関連付けられた OU から SCP をデタッチします。

- b. SCP を削除します。

StackSets およびスタックの削除

AWS Control Tower は StackSets と スタックを使用して、ランディングゾーンのコントロール AWS Config ルールに関連する をデプロイします。次の手順では、これらの特定のリソースを削除する方法を示します。

Stack CloudFormation StackSets を削除するには

1. <https://console.aws.amazon.com/cloudformation> で CloudFormation コンソールを開きます。
2. 左のナビゲーションメニューから [StackSets] を選択します。
3. プレフィックス AWSControlTower の StackSet ごとに、次の操作を実行します。1 つの StackSet に複数のアカウントがある場合、これには多少時間がかかることがあります。
 - a. ダッシュボード内のテーブルから特定の StackSet を選択します。その StackSet のプロパティページが開きます。
 - b. ページの下部にある スタックテーブルで、テーブル内のすべての AWS アカウントのアカウント IDs を記録します。すべてのアカウントのリストをコピーします。
 - c. [Actions] (アクション) から [Delete stacks from StackSet] (StackSet からスタックを削除) を選択します。
 - d. [Set deployment options] (デプロイオプションの設定) で、[Deployment locations] (デプロイ先) から [Deploy stacks in accounts] (スタックをアカウントにデプロイ) を選択します。
 - e. テキストフィールドに、ステップ 3.b で記録した AWS アカウント IDs をカンマで区切って入力します。例: **123456789012**、**098765431098**、など。
 - f. [Specify regions] (リージョンの指定) で、[Add all] (すべて追加) を選択し、ページにある他のすべてのパラメータはデフォルト設定のままにして、[Next] (次へ) を選択します。
 - g. [Review] (確認) ページで、選択内容を確認し、[Delete stacks] (スタックの削除) を選択します。
 - h. [StackSet properties] (StackSet のプロパティ) ページで、他の StackSets に再度この手順を開始できます。
4. このプロセスは、別の [StackSets properties] (StackSet のプロパティ) ページの [Stacks] (スタック) テーブルのレコードが空になると完了します。
5. [Stacks] (スタック) テーブルのレコードが空になったら、[Delete StackSet] (StackSet の削除) を選択します。

CloudFormation スタックを削除するには

1. <https://console.aws.amazon.com/cloudformation> で CloudFormation コンソールを開きます。
2. [Stacks] (スタック) ダッシュボードから [AWSControlTower] というプレフィックスが付いたすべてのスタックを検索します。
3. テーブル内の各スタックについて、次の操作を行います。
 - a. スタックの名前の横にあるチェックボックスを選択します。
 - b. [Actions] (アクション) メニューから [Delete Stack] (スタックの削除) を選択します。
 - c. 開いたダイアログボックスで、情報が正確であることを確認し、[Yes, Delete] (はい、削除します) を選択します。

ログアーカイブアカウントでの Simple Storage Service (Amazon S3) バケットの削除

次の手順では、[AWSControlTowerExecution] グループの IAM Identity Center ユーザーとしてログアーカイブアカウントにサインインし、ログアーカイブアカウントの Simple Storage Service (Amazon S3) バケットを削除する方法について説明します。

適切なアクセス許可でログアーカイブアカウントにサインインするには

1. Organizations コンソール (<https://console.aws.amazon.com/organizations/>) を開きます。
2. [Accounts] (アカウント) タブから [Log archive] (ログアーカイブ) アカウントを見つけます。
3. 開いた右側のペインで、ログアーカイブアカウント番号を記録します。
4. ナビゲーションバーから アカウント名を選択し、アカウントメニューを開きます。
5. [Switch Role] (ロールの切り替え) を選択します。
6. 開いたページで、[Account] (アカウント) でログアーカイブアカウントのアカウント番号を指定します。
7. [Role] (ロール) に [AWSControlTowerExecution] と入力します。
8. [Display Name] (表示名) にテキストを入力します。
9. お気に入りの [Color] (色) を選択します。
10. [Switch Role] (ロールの切り替え) を選択します。

Simple Storage Service (Amazon S3) バケットを削除するには

1. <https://console.aws.amazon.com/s3/> で Simple Storage Service (Amazon S3) コンソールを開きます。
2. [aws-controltower] を含むバケット名を検索します。
3. テーブル内の各バケットについて、次の操作を行います。
 - a. テーブル内のバケットのチェックボックスをオンにします。
 - b. [Delete] (削除) を選択します。
 - c. 開いたダイアログボックスで、情報が正確であることを確認し、確定するためのバケット名を入力し、[Confirm] (確認) を選択します。

Account Factory ポートフォリオおよび製品を削除する

次の手順では、AWSServiceCatalogAdmins グループの IAM Identity Center ユーザーとしてサインインし、Account Factory ポートフォリオおよび製品をクリーンアップする方法を示します。

適切なアクセス許可で管理アカウントにサインインするには

1. directory-id.awsapps.com/start の URL でユーザーポータルにアクセスします
2. [AWS アカウント] から [管理] アカウントを見つけます。
3. AWSServiceCatalogAdminFullAccess から、 マネジメントコンソールを選択して、このロール AWS マネジメントコンソール として にサインインします。

Account Factory をクリーンアップするには

1. Service Catalog コンソール (<https://console.amazonaws.cn/servicecatalog/>) を開きます。
2. 左のナビゲーションメニューから [Portfolios list] (ポートフォリオリスト) を選択します。
3. [Local Portfolios] (ローカルポートフォリオ) テーブルで、[AWS Control Tower Account Factory Portfolio] という名前のポートフォリオを検索します。
4. そのポートフォリオの名前を選択し、詳細ページに移動します。
5. ページの [Constraints] (制約) セクションを展開し、製品名 [AWS Control Tower Account Factory] のある制約のラジオボタンを選択します。
6. [REMOVE CONSTRAINTS] (制約の削除) を選択します。

7. 開いたダイアログボックスで、情報が正確であることを確認し、[CONTINUE] (続行) を選択します。
8. ページの [Products] (製品) セクションから製品名 [AWS Control Tower Account Factory] のラジオボタンを選択します。
9. [REMOVE PRODUCT] (製品の削除) を選択します。
10. 開いたダイアログボックスで、情報が正確であることを確認し、[CONTINUE] (続行) を選択します。
11. [Users, Groups, and Roles] (ユーザー、グループ、およびロール) セクションを展開し、このテーブルのすべてのレコードのチェックボックスをオンにします。
12. [REMOVE USERS, GROUP OR ROLE] (ユーザー、グループ、またはロールを削除) を選択します。
13. 開いたダイアログボックスで、情報が正確であることを確認し、[CONTINUE] (続行) を選択します。
14. 左のナビゲーションメニューから [Portfolios list] (ポートフォリオリスト) を選択します。
15. [Local Portfolios] (ローカルポートフォリオ) テーブルで、[AWS Control Tower Account Factory Portfolio] という名前のポートフォリオを検索します。
16. そのポートフォリオのラジオボタンを選択し、[DELETE PORTFOLIO] (ポートフォリオの削除) を選択します。
17. 開いたダイアログボックスで、情報が正確であることを確認し、[CONTINUE] (続行) を選択します。
18. 左のナビゲーションメニューから [Product list] (製品リスト) を選択します。
19. [Admin products] (管理者製品) ページで、[AWS Control Tower Account Factory] という名前の製品を検索します。
20. 製品を選択して、[Admin product details] (Admin 製品の詳細) ページを開きます。
21. [Actions] (アクション) から [Delete product] (製品の削除) を選択します。
22. 開いたダイアログボックスで、情報が正確であることを確認し、[CONTINUE] (続行) を選択します。

AWS Control Tower のロールとポリシーを削除する

これらの手順では、ランディングゾーンの設定時または以降に AWS Control Tower で作成したロールやポリシーをクリーンアップする方法を示します。

IAM Identity Center AWSServiceCatalogEndUserAccess ロールを削除するには

1. <https://console.aws.amazon.com/singlesignon/> で AWS IAM アイデンティティセンター コンソールを開きます。
2. AWS リージョンをホームリージョンに変更します。ホームリージョンは、AWS Control Tower を最初にセットアップしたリージョンです。
3. 左のナビゲーションメニューから [AWS アカウント] を選択します。
4. 管理アカウントのリンクを選択します。
5. [Permission sets] (許可セット) のドロップダウンを選択し、[AWSServiceCatalogEndUserAccess]、[Remove] (削除) の順に選択します。
6. 左側のパネルから [AWS アカウント] を選択します。
7. [Permission sets] (許可セット) タブを開きます。
8. [AWSServiceCatalogEndUserAccess] を選択して、削除します。

IAM ロールを削除するには

1. IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. 左のナビゲーションメニューから [Roles] (ロール) を選択します。
3. テーブルから [AWSControlTower] という名前のロールを検索します。
4. テーブル内の各ロールについて、次の操作を行います。
 - a. ロールのチェックボックスをオンにします。
 - b. [Delete role] (ロールの削除) を選択します。
 - c. 開いたダイアログボックスで、情報が正確であることを確認し、[Yes, delete] (はい、削除します) を選択します。

IAM ポリシーを削除するには

1. IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. 左のナビゲーションメニューから [Policies] (ポリシー) を選択します。
3. テーブルから [AWSControlTower] という名前のポリシーを検索します。
4. テーブル内の各ポリシーについて、次の操作を行います。
 - a. ポリシーのチェックボックスをオンにします。

- b. ドロップダウンメニューから [Policy actions] (ポリシーアクション) と [Delete] (削除) を選択します。
- c. 開いたダイアログボックスで、情報が正確であることを確認し、[Delete] (削除) を選択します。

AWS Control Tower リソースのヘルプ

AWS Control Tower リソースの削除時に解決できない問題が発生した場合は、[AWS サポート](#)までお問い合わせください。

ランディングゾーン廃止後のセットアップ

ランディングゾーン廃止後は、手動クリーンアップが完了するまでセットアップを再実行できません。また、これらの残ったリソースを手動でクリーンアップしないと、予期しない請求が発生する可能性があります。次の点に注意してください。

- AWS Control Tower 管理アカウントは AWS Control Tower のルート OU の一部です。これらの IAM ロールと IAM ポリシーが管理アカウントから削除されていることを確認します。
 - ロール:
 - `AWSControlTowerAdmin`
 - `AWSControlTowerCloudTrailRole`
 - `AWSControlTowerStackSetRole`
 - ポリシー:
 - `AWSControlTowerAdminPolicy`
 - `AWSControlTowerCloudTrailRolePolicy`
 - `AWSControlTowerStackSetRolePolicy`
- ランディングゾーンを再度設定する前に、AWS Control Tower の既存 IAM Identity Center の設定を削除または更新することもできますが、削除は必須ではありません。
- AWS Control Tower によって作成された VPC を削除することもできます。
- ログ記録アカウントまたは監査アカウントに指定された E メールアドレスが既存の AWS アカウントに関連付けられている場合、セットアップは失敗します。AWS アカウントを閉鎖すること

も、別の E メールアドレスを使用してランディングゾーンを再度セットアップすることもできます。または、これらの既存の共有アカウントを再利用して、独自のロギングアカウントと監査アカウントを持ち込む機能を使用することもできます。詳細については、「[既存のセキュリティアカウントまたはログアカウントを使用する際の考慮事項](#)」を参照してください。

- ロギングアカウントに次の予約名の Amazon S3 バケットが既に存在する場合、セットアップは失敗します。
 - `aws-controltower-logs-{accountId}-{region}` (ロギングバケットに使用)。
 - `aws-controltower-s3-access-logs-{accountId}-{region}` (ロギングアクセスバケットに使用)。

これらのバケットの名前を変更または削除するか、ロギングアカウントに別のアカウントを使用する必要があります。

- CloudWatch Logs の管理アカウントに `aws-controltower/CloudTrailLogs` というロググループが既に存在する場合、セットアップは失敗します。ロググループの名前を変更するか、ロググループを削除する必要があります。

新しい `で` を設定する前に AWS リージョン

新しい AWS リージョンに新しいランディングゾーンを設定する場合は、以下の追加ステップに従います。

- CLI を開いて、次のコマンドを入力します。

```
aws organizations disable-aws-service-access --service-principal
controltower.amazonaws.com
```

- 残っているマネージドルール (`AWSControlTowerManagedRule`) を、すべての管理対象リージョンで共有アカウントおよびメンバーアカウントから削除します。

Note

セキュリティまたはサンドボックスという名前のトップレベルの OU がある組織では、新しいランディングゾーンをセットアップできません。ランディングゾーンを再度セットアップするには、これらの OU の名前変更または削除を行う必要があります。

チュートリアル

この章では、AWS Control Tower の使用に役立つチュートリアルの手順が含まれています。

トピック

- [チュートリアル: ALZ から AWS Control Tower に移行する](#)
- [チュートリアル: VPC を使用せずに AWS Control Tower を設定する](#)
- [AWS Control Tower リソースを削除する](#)
- [チュートリアル: を使用して AWS Control Tower でセキュリティグループを設定する AWS Firewall Manager](#)
- [AWS Control Tower のランディングゾーンを廃止する](#)

チュートリアル: ALZ から AWS Control Tower に移行する

多くのAWSお客様は、[AWS Landing Zone ソリューション \(ALZ\)](#) を採用して、安全で準拠したマルチアカウントAWS環境をセットアップしています。ランディングゾーンの管理負担を軽減するために、AWSは AWS Control Tower というマネージドサービスを作成しました。

ALZ では、追加機能は予定されていません。長期サポートのみです。したがって、ALZ から AWS Control Tower サービスに移行することをお勧めします。この章でリンクされているブログでは、その移行に関するさまざまな考慮事項について説明し、ALZ から AWS Control Tower への正常な移行を計画する方法について説明します。

ブログ: [AWSランディングゾーンソリューションを AWS Control Tower に移行する](#)

AWS規範ガイダンスでは、ALZ から AWS Control Tower への移行手順など、より広範なドキュメントを提供しています。基本的に、いくつかの前提条件に基づいて、ALZ を実行している既存の組織で AWS Control Tower ガバナンスを有効にします。詳細については、[AWS「ランディングゾーンから AWS Control Tower への移行」](#)を参照してください。

チュートリアル: VPC を使用せずに AWS Control Tower を設定する

このトピックでは、VPC を使用せずに AWS Control Tower アカウントを設定する方法について説明します。

ワークロードに VPC が必要ない場合は、次の操作を実行できます。

- AWS Control Tower 仮想プライベートクラウド (VPC) を削除できます。この VPC は、ランディングゾーンの設定時に作成されます。
- VPC が関連付けられていない新しい AWS Control Tower アカウントが作成されるように、Account Factory 設定を変更できます。

Important

VPC インターネットアクセス設定を有効にして Account Factory アカウントをプロビジョニングすると、その Account Factory 設定によってコントロール「[顧客が管理する Amazon VPC インスタンスのインターネットアクセスを許可しない](#)」が上書きされます。新しくプロビジョニングされたアカウントのインターネットアクセスを有効にしないようにするには、Account Factory で設定を変更する必要があります。

AWS Control Tower VPC を削除する

AWS Control Tower 以外では、すべての AWS お客様にデフォルトの VPC があり、<https://console.aws.amazon.com/vpc/> の Amazon Virtual Private Cloud (Amazon VPC) コンソールで表示できます。デフォルトの VPC は、その名前の末尾に必ず単語 (default) が含まれているため判別できます。

AWS Control Tower ランディングゾーンを設定すると、AWS Control Tower は AWS デフォルトの VPC を削除し、新しい AWS Control Tower のデフォルト VPC を作成します。新しい VPC は、AWS Control Tower 管理アカウントに関連付けられます。このトピックでは、この新しい VPC を Control Tower VPC と呼びます。

Amazon VPC コンソールで AWS Control Tower VPC を表示すると、その名前の末尾に単語 (default) は表示されません。複数の VPC がある場合は、割り当てられた CIDR 範囲を使用して、該当する AWS Control Tower VPC を特定する必要があります。

AWS Control Tower VPC は削除できますが、後で AWS Control Tower で VPC が必要になった場合は、自分で作成する必要があります。

AWS Control Tower VPC を削除するには

1. Amazon VPC コンソールの <https://console.aws.amazon.com/vpc/> を開いてください。

2. **VPC** を検索するか、Service Catalog のオプションから [VPC] を選択します。[VPC Dashboard] (VPC ダッシュボード) が表示されます。
3. 左側のメニューから、[Your VPCs] (お使いの VPC) を選択します。すべての自分の VPC が一覧表示されます。
4. AWS Control Tower VPC をその CIDR 範囲で特定します。
5. VPC を削除するには、[Actions] (アクション)、[Delete VPC] (VPC の削除) の順に選択します。

AWS (デフォルト) VPC は、AWS Control Tower 管理アカウントのすべてのリージョンに既に存在します。セキュリティのベストプラクティスに従うために、AWS Control Tower VPC を削除する場合は、管理アカウントに関連付けられた AWS デフォルトの VPC をすべての AWS リージョンから削除することをお勧めします。したがって、管理アカウントをセキュリティで保護するには、各リージョンからデフォルトの VPC を削除し、AWS Control Tower ホームリージョンの Control Tower によって作成された VPC も削除します。

オプションでアカウントの VPC リソースをクリーンアップする

オプションで、既存のアカウント `aws-controltower-VPC` から AWS Control Tower VPC リソースをクリーンアップするには、VPC に既存のリソースやリソース依存関係がないことを確認した後 `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`、AWS CloudFormation StackSet からスタックインスタンスを削除できます。

AWS Control Tower で VPC なしのアカウントを作成する

エンドユーザーのワークロードに VPC が不要である場合は、この方法を使用して、VPC が自動作成されないユーザーアカウントを設定できます。

AWS Control Tower ダッシュボードから、ネットワーク設定を表示および編集できます。関連付けられた VPC なしで AWS Control Tower アカウントが作成されるように設定を変更すると、設定を再度変更するまでは、すべての新しいアカウントが VPC なしで作成されます。

VPC なしのアカウントを作成するように Account Factory を設定するには

1. ウェブブラウザを開き、AWS Control Tower コンソール (<https://console.aws.amazon.com/controltower>) に移動します。
2. 左側のメニューから、[Account Factory] を選択します。
3. [Account Factory] ページに [Network Configuration] (ネットワーク設定) セクションが表示されます。

4. 後で復元する場合のために、現在の設定を書き留めておきます。
5. [Network Configuration] (ネットワーク設定) セクションで [Edit] (編集) ボタンを選択します。
6. [Edit account factory network configuration] (Account Factory ネットワーク設定の編集) ページで、[VPC Configuration options for new accounts] (新規アカウント用の VPC 設定オプション) セクションに移動します。

[Option 1] (オプション 1) または [Option 2] (オプション 2)、あるいはその両方に従って、アカウントのプロビジョニング時に AWS Control Tower が VPC を作成しないようにします。

a. オプション 1 — サブネットの削除

- [Internet-accessible subnet] (インターネットアクセス可能なサブネット) のトグルスイッチをオフにします。
- [Maximum number of private subnets] (プライベートサブネットの最大数) の値を 0 に設定します。

b. オプション 2 – AWS リージョンの削除

- [Regions for VPC creation] (VPC 作成のリージョン) 列のすべてのチェックボックスをオフにします。

7. [保存] を選択します。

起こり得るエラー

AWS Control Tower VPC を削除したり、VPC なしのアカウントを作成するように Account Factory を再設定したりするときは、以下のエラーが起こる場合があるため注意してください。

- 既存の管理アカウントには、AWS Control Tower VPC の依存関係やリソースが含まれている場合があります。これにより、削除エラーが発生する可能性があります。
- VPC なしで新しいアカウントを起動するように設定するときにデフォルトの CIDR を残したままにすると、リクエストは失敗し、CIDR が無効であるというエラーが発生します。

チュートリアル: を使用して AWS Control Tower でセキュリティグループを設定する AWS Firewall Manager

この動画では、AWS Firewall Manager サービスを使用して AWS Control Tower のネットワークセキュリティを強化する方法を示します。セキュリティグループを設定するためのセキュリティ管理者

アカウントを指定できます。セキュリティポリシーを設定してセキュリティルールを AWS Control Tower 組織に適用する方法、およびポリシーを自動的に適用して非準拠のリソースを修復する方法を確認できます。組織内の各アカウントおよびリソース (Amazon EC2 インスタンスなど) に適用されているセキュリティグループを確認できます。

独自のファイアウォールポリシーを作成することも、信頼できるベンダーのルールをサブスクライブすることもできます。

AWS Firewall Manager でセキュリティグループを設定する

この動画 (所要時間: 8 分 2 秒) では、AWS Control Tower のリソースとワークロードのネットワークインフラストラクチャセキュリティを強化する方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[AWS Control Tower のファイアウォール設定の動画チュートリアル。](#)

詳細については、[AWS WAF のセットアップ方法に関するドキュメント](#)を参照してください。

トラブルシューティング

AWS Control Tower の使用中に問題が発生した場合は、次の情報を使用して、当社のベストプラクティスに従って解決できます。発生した問題が次の情報の範囲外である場合、または解決を試みた後にも持続する場合は、[AWS Support](#) にお問い合わせください。

トピック

- [ランディングゾーンの起動の失敗](#)
- [ランディングゾーンの更新が KMS エラーで失敗した](#)
- [ランディングゾーンを更新できない](#)
- [ランディングゾーンが最新ではないエラー](#)
- [新しいアカウントのプロビジョニングに失敗する](#)
- [既存のアカウントを登録できない](#)
- [Account Factory アカウントを更新できない](#)
- [が言及する失敗エラー AWS Config](#)
- [起動パスが見つからないというエラー](#)
- [許可不足のエラーを受け取った](#)
- [検出コントロールがアカウントで有効になっていない](#)
- [AWS Organizations API によって返されるレート超過エラー](#)
- [ある AWS Control Tower ランディングゾーンから別の AWS Control Tower ランディングゾーンに Account Factory アカウントを直接移動できない](#)
- [AWS サポート](#)

ランディングゾーンの起動の失敗

ランディングゾーンの起動の失敗の一般的な原因:

- 確認メールメッセージへの応答の欠如。
- CloudFormation StackSet の失敗。

確認メールメッセージ: 管理アカウントが作成後 1 時間未満である場合、追加のアカウントを作成すると、問題が発生することがあります。

実行するアクション

この問題が発生した場合は、E メールを確認してください。確認メールが着信し、応答を待機していることがあります。または、1 時間待ってから、もう一度試すことをお勧めします。問題が解決しない場合は、[AWS Support](#) までお問い合わせください。

StackSets の失敗: ランディングゾーンの起動失敗のもう 1 つの考えられる原因は、CloudFormation StackSet の失敗です。AWS Control Tower が管理するすべてのリージョンの管理アカウントで AWS セキュリティトークンサービス (STS) AWS リージョンを有効にする必要があります。そうしないと、スタックセットの起動が失敗します。

実行するアクション

AWS Control Tower を起動する前に、必要なすべての AWS Security Token Service [\(STS\) エンドポイントリージョン](#) を必ず有効にしてください。

失敗したスタックセットを修正して設定を再試行するには

1. 適切な AWS リージョンで CloudFormation コンソールに移動します。
2. AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER という名前の失敗したスタックをクリーンアップします。
3. スタックの削除が完了するまで待ちます。
4. AWS Control Tower ページに戻ります。
5. もう一度、[ランディングゾーンの設定] を選択します。

AWS Control Tower がサポートする AWS リージョン のリストを表示するには、「」を参照してください [AWS リージョンと AWS Control Tower の連携方法](#)。

ランディングゾーンの更新が KMS エラーで失敗した

ランディングゾーンの更新失敗の最も一般的な原因は、無効な AWS KMS キーポリシーです。

無効な KMS キーポリシーの一般的な原因:

- ポリシーのタイプミス。
- 必要なポリシーステートメントの追加を忘れた。
- AWS パーティションが正しくありません。
- ポリシーのアカウント番号が正しくない。

- サンプルポリシーのプレースホルダーの削除を忘れた。

実行するアクション

ポリシーを確認して、これらのエラーを確認します。

AWS KMS キーポリシーの詳細については、[「KMS キーの設定」](#) および [「バックアップの前提条件」](#) を参照してください。

ランディングゾーンを更新できない

更新が失敗しても、AWS Control Tower は以前のランディングゾーンバージョンにロールバックしません。ランディングゾーンが不確定な状態になる場合があります。その場合は、AWS サポートにお問い合わせください。

ランディングゾーンの更新は、いくつかの理由で失敗することがあります。

- 前提条件が満たされていない
- AWS Config リソースが特定のアカウントに存在する
- 閉鎖されたアカウントが存在する

前提条件が満たされていない

ランディングゾーンの更新時には、ランディングゾーンの設定時と同じ前提条件を満たす必要があります。更新の前に、[起動前チェック](#)を確認してください。

AWS Config リソースがセキュリティ OU アカウントに存在する

監査アーカイブアカウントとログアーカイブアカウントに AWS Config リソースを追加しないでください。ランディングゾーンの更新プロセスは、これらのリソースが存在する状態では完了できません。これらの制限は、アカウントを登録したり、ランディングゾーンを初めて設定したりする場合の制限と似ています。詳細については、[「既存の AWS Config リソースを持つアカウントの登録」](#) を参照してください。

閉鎖されたアカウントが存在する

アカウントが [Closed] (閉鎖) または [Suspended] (一時停止) 状態の場合は、ランディングゾーンを更新しようとする問題が発生する可能性があります。ランディングゾーンの更新を実行する前に、クローズされたすべてのアカウントのプロビジョニング済み製品を削除する必要があります。

AWS Service Catalog プロビジョニングされた製品ページには、次のようなエラーメッセージが表示されることがあります。

`AWSControlTowerExecution` role can't be assumed on the account.

一般的な原因: プロビジョニング済み製品を削除せずにアカウントを一時停止しました。

実行するアクション: このエラーが表示された場合は、次の 2 つのオプションがあります。

1. AWS サポートに連絡してアカウントを再開し、プロビジョニング済み製品を削除してから、アカウントを再度閉鎖します。
2. アカウント閉鎖のために孤立した StackSets からリソースを削除します。(このオプションは、削除しない [Current] (最新) 状態のインスタンスが StackSets にある場合にのみ使用できます。)

StackSets からリソースを削除するには、閉鎖したアカウントごとにこれを行います。

- AWS Control Tower の各 StackSets にアクセスし、閉鎖したアカウントのすべてのリージョンから StackInstances を削除します。
- 重要: [Retain Stack] (スタックの保持) オプションを選択すると、StackSet はスタックインスタンスのみを削除します。StackSet は閉鎖したアカウントからロールを引き受けることができないため、AWSControlTowerExecution ロールを引き受けようとした場合は失敗し、エラーメッセージが表示されます。

ランディングゾーンが最新ではないエラー

ランディングゾーンを最近更新していない場合は、AWS Control Tower へのアクセスを回復しようとしたときにエラーが発生することがあります。以下のようなエラーメッセージが表示されることがあります。

Unable to access Control Tower

アカウントは長い間非アクティブになっています。非アクティブのため、AWS Control Tower にアクセスするにはランディングゾーンを更新する必要があります。

ただし、ランディングゾーンの更新が失敗する可能性があります。

実行する手順

組織の管理アカウントにサインインし、ルートユーザーとしてサインインします。IAM ユーザーまたは AWS Identity Center のユーザーは AWS Control Tower 管理者権限を持

ち、AWSControlTowerAdmins グループに属している必要があります。その場合は、更新を再試行してください。

新しいアカウントのプロビジョニングに失敗する

この問題が発生した場合は、以下の一般的な原因を確認します。

アカウントのプロビジョニングフォームに入力した際に、次を行った可能性があります。

- tagOptions を指定した
- SNS 通知を有効化した
- プロビジョニング済み製品の通知を有効化した

これらのオプションを指定せずに、アカウントのプロビジョニングを再試行してください。詳細については、「[Account Factory を使用して Service Catalog コンソールでアカウントをプロビジョニングする](#)」を参照してください。

その他の一般的な失敗の原因:

- プロビジョニングされた製品プランを作成した場合 (リソースの変更を表示するため)、アカウントのプロビジョニングが無期限に [In progress] (進行中) 状態のままになることがあります。
- AWS Control Tower の他の設定変更が進行中に Account Factory で新しいアカウントを作成しようとすると、作成は失敗します。例えば、OU にコントロールを追加するプロセスの進行中にアカウントをプロビジョニングしようとする、Account Factory にエラーメッセージが表示されます。

AWS Control Tower で前のアクションのステータスを確認するには

- AWS [CloudFormation] > [StackSets] に移動します。
- AWS Control Tower と関連する各スタックセットをチェックします (プレフィックス: 「AWSControlTower」)。
- まだ実行中の CloudFormation StackSets オペレーションを探します。

アカウントのプロビジョニングに 1 時間以上かかる場合は、プロビジョニングプロセスを終了し、もう一度試してください。

既存のアカウントを登録できない

既存の AWS アカウントを登録しようとしたときに登録が失敗した場合、2 回目に試行すると、スタックセットが存在することを示すエラーメッセージが表示されることがあります。続行するには、プロビジョニングされた製品を Account Factory から削除する必要があります。

最初の登録が失敗した原因が、アカウントに `AWSControlTowerExecution` ロールを作成し忘れていたことである場合は、表示されるエラーメッセージで、ロールを作成するように指示されます。ただし、ロールを作成しようとすると、AWS Control Tower がロールを作成できなかったという別のエラーメッセージが表示されることがあります。このエラーは、プロセスが部分的に完了しているために発生します。

この場合、既存のアカウントの登録に進む前に、2 つの回復手順を実行する必要があります。まず、AWS Service Catalog コンソールを使用して Account Factory でプロビジョニングされた製品を終了する必要があります。次に、AWS Organizations コンソールを使用して、OU からアカウントを手動で移動し、ルートに戻す必要があります。その後、アカウントに `AWSControlTowerExecution` ロールを作成し、[Enroll account] (アカウントの登録) フォームに再度入力します。

登録に失敗するもう 1 つの原因として、アカウントに既存の AWS Config リソースがあることが考えられます。この場合、[既存の AWS Config リソースを変更する方法については、「既存のリソースがあるアカウントを登録する」](#)を参照してください。

Account Factory アカウントを更新できない

アカウントの状態が一貫していない場合、Account Factory または から正常に更新することはできません AWS Service Catalog。

ケース 1: 以下のようなエラーメッセージが表示されることがあります。

AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.

一般的な原因: AWS Control Tower は、初期プロビジョニング中に常に AWS デフォルトの VPC を削除します。アカウントに AWS デフォルトの VPC を設定するには、アカウントの作成後に VPC を追加する必要があります。AWS Control Tower には、AWS のデフォルト VPC に代わる独自のデフォルト VPC があります。ただし、チュートリアルで示されているように Account Factory を設定しない限り、AWS Control Tower によって VPC はまったくプロビジョニングされません。この場合、アカウントに VPC はありません。AWS デフォルトの VPC を使用する場合は、その VPC を再追加する必要があります。

ただし、AWS Control Tower は AWS デフォルトの VPC をサポートしていません。その種の VPC をデプロイすると、アカウントは Tainted 状態になります。その状態にある場合、アカウントを更新することはできません AWS Service Catalog。

実行するアクション: 追加したデフォルト VPC を削除する必要があります。これによりアカウントを更新できるようになります。

 Note

Tainted 状態になると、未更新のアカウントは属する先の OU でコントロールを有効にできないという問題が発生する場合があります。

ケース 2: 以下のようなエラーメッセージが表示されることがあります。

AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.

一般的な原因: アカウントを登録済みの OU から別の OU に移動しようとしたが、古い AWS Config ルールは残ります。アカウントが不整合な状態になっています。

実行するアクション:

アカウントの移動が意図されていた場合:

- Service Catalog のアカウントを終了します。
- もう一度アカウントを登録してください。
- コンテキスト/影響: デプロイされた AWS Config ルールが、送信先 OU によって指定された設定と一致しません。
- AWS Config ルールが以前の OU から残り、意図しない支出が発生する可能性があります。
- リソース名の競合により、アカウントを再登録または更新しようとすると失敗します。

アカウントの移動が意図されていなかった場合:

- アカウントを元の OU に戻します。
- Service Catalog からアカウントを更新します。
- 起動パラメータに、アカウントの元の OU を入力します。

- コンテキスト/インパクト: アカウントが元の OU に戻らない場合、アカウントの状態は新しい OU によって指示されたコントロールと一致しません。
- アカウントの更新は、以前の OU に関連付けられた AWS Config ルールが削除されないため、有効な修復ではありません。

が言及する失敗エラー AWS Config

AWS Control Tower でサポートされている AWS リージョンで AWS Config が有効になっている場合、事前チェックが失敗したため、エラーメッセージが表示されることがあります。メッセージは、の基本的な動作が原因で、問題を適切に説明していないように見える場合があります AWS Config。

次のいずれかに類似したエラーメッセージが表示される場合があります。

- `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`
.

一般的な原因: AWS アカウントで AWS Config サービスを有効にすると、デフォルトの名前で設定レコーダーと配信チャネルが作成されます。コンソールで AWS Config サービスを無効にすると、設定レコーダーや配信チャネルは削除されません。これらは CLI を使用して削除するか、AWS Control Tower で使用できるように変更する必要があります。AWS Control Tower でサポートされているいずれかのリージョンで AWS Config サービスが有効になっている場合、このエラーが発生する可能性があります。

アカウントに既存の AWS Config リソースがある場合、[既存の AWS Config リソースを変更する方法](#)については、「[既存のリソースを持つアカウントを登録する](#)」を参照してください。

実行するアクション: サポートされているすべてのリージョンで、設定レコーダーと配信チャネルを削除します。AWS Config を無効にするだけでは不十分です。設定レコーダーと配信チャネルは CLI を使用して削除する必要があります。CLI から設定レコーダーと配信チャネルを削除した後、もう一度 AWS Control Tower の起動とアカウントの登録を試すことができます。

プロビジョニング済み製品をデプロイしようとしている場合は、再試行する前にプロビジョニング済み製品を削除する必要があります。そうしないと、以下のようなエラーメッセージが表示されることがあります。

- An error occurred (**InvalidParametersException**) when calling the **ProvisionProduct** operation: A stack named *Stackname* already exists.

メッセージでは、*Stackname* がスタック名を指定します。

設定レコーダーと配信チャネルのステータスを判断するために使用できる AWS Config CLI コマンドの例を次に示します。

表示コマンド:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- The normal response is something like "name": "default"

削除コマンド:

- `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`

詳細については、AWS Config ドキュメントを参照してください。

- [設定レコーダーの管理 \(AWS CLI\)](#)
- [配信チャネルの管理](#)

起動パスが見つからないというエラー

新しいアカウントを作成しようとする、次のようなエラーメッセージが表示されることがあります。

```
No launch paths found for resource: prod-dpqqfywxxx
```

このエラーメッセージは AWS Service Catalog、AWS Control Tower でのアカウントのプロビジョニングに役立つ統合サービスである によって生成されます。

一般的な原因:

- ルートとしてログインしている可能性があります。AWS Control Tower では、ルートユーザーとしてログインしている場合のアカウントの作成はサポートされていません。
- IAM Identity Center ユーザーが適切なアクセス許可グループに追加されていません。場合によっては、AWSAccountFactory (エンドユーザーアクセス用) または AWSServiceCatalogAdmins (管理者アクセス用) のいずれかのアクセス許可グループに IAM Identity Center ユーザーを追加する必要があります。
- IAM ユーザーとして認証されている場合は、正しいアクセス許可を持つように [AWS Service Catalog ポートフォリオに追加](#) する必要があります。
- この問題は、正しい権限を持っているが、AWS Control Tower ドリフトが検出され、ドリフトの修復が必要な場合にも発生します。ほとんどの種類のドリフトを修復するには、[ランディングゾーン設定] ページで [リセット] を選択します。

許可不足のエラーを受け取った

特定の AWS Organizations で特定の作業を実行するために必要な許可がアカウントにない可能性があります。次の種類のエラーが発生した場合は、IAM や IAM Identity Center の許可など、すべての許可領域をチェックして、それらの場所から許可が拒否されていないことを確認します。

```
You have insufficient permissions to perform AWS Organizations API actions.
```

試行するアクションが作業に必要で、関連する制限が見つからない場合は、システム管理者または [AWS Support](#) にお問い合わせください。

検出コントロールがアカウントで有効になっていない

最近 AWS Control Tower のデプロイを新しい AWS リージョンに拡張した場合、新しく適用された検出コントロールは、AWS Control Tower によって管理される OUs 内の個々のアカウントが更新されるまで、どのリージョンで作成した新しいアカウントにも有効になりません。既存のアカウントにある既存の検出コントロールはまだ有効です。

アカウントを更新する前に検出コントロールを有効にしようとすると、次のようなエラーメッセージが表示されることがあります。

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

実行するアクション: アカウントの更新。

AWS Control Tower コンソールからアカウントを更新するには、「[AWS Control Tower の OU とアカウントを更新する場合](#)」を参照してください。

複数の個々のアカウントをプログラムで更新するには、AWS Service Catalog および CLI AWS APIs を使用して更新を自動化できます。更新プロセスにアプローチする方法の詳細については、こちらの「[動画チュートリアル](#)」を参照してください。動画で説明されている ProvisionProduct API の代わりに UpdateProvisionedProduct API を使用できます。

それでもアカウントで検出コントロールが有効にならない場合は、[AWS Support](#) にお問い合わせください。

AWS Organizations API によって返されるレート超過エラー

考えられる原因

AWS Control Tower が毎日のスキャンを実行して SCP がドリフトしているかどうかを確認している間、ワークロードが実行されていました。

従うべき手順

API スロットリングまたは rate exceeded エラーが発生した場合は、次の手順を試してください。

- ワークロードを別のタイミングで実行します。(AWS Control Tower が監査スキャンを実行するタイミングを確認するには、リージョン別の AWS Control Tower SCP 不変スキャンのスケジュールを参照してください。)
- HTTP 経由で API APIs を直接呼び出す場合: AWS SDK を使用すると、失敗したアクションが自動的に再試行されます。
- [Service Quotas](#) と AWS Support を通じて制限の引き上げをリクエストします。

Elastic Beanstalk での API スロットリングのトラブルシューティング手順の例については、<https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/> を参照してください。

ある AWS Control Tower ランディングゾーンから別の AWS Control Tower ランディングゾーンに Account Factory アカウントを直接移動できない

Warning

このプラクティスは、対象となるアカウント登録の前提条件を満たしていません。なぜなら、対象となるアカウントは同じ AWS 組織全体に属していなければならない、各組織にはランディングゾーンが 1 つしかない可能性があるためです。このアクションを実行しようとして、複数のエラーメッセージが表示された場合には、次の情報が参考になる可能性があります。

Account Factory を使用してプロビジョニングしたアカウントを、別の管理アカウントの下にある AWS Control Tower が管理する別のランディングゾーンに移動するには、すべての IAM ロールとそのアカウントに関連付けられているスタックを元の OU から削除する必要があります。これらのリソースを、アカウントがデプロイされているすべてのリージョンから削除します。

Note

リソースを削除する最善の方法は、元の OU でアカウントのプロビジョニングを解除してから、リソースを移動させることです。

リソースを削除しないと、新しい OU への登録は失敗します。1 つ以上のエラーメッセージが表示されることがあり、アカウントがデプロイされたすべてのリージョンから残りのロールとスタックが削除されるまで、同様のエラーメッセージが表示され続けます。

エラーメッセージが表示されるたびに、新しい OU からアカウントを削除し、エラーメッセージの対象となる古いリソースを削除してから、アカウントを新しい OU に戻す必要があります。削除と削除のこのプロセスは、残りのすべてのリソース、アカウントがデプロイされたすべてのリージョンについて、10 回または 20 回繰り返す必要があります。このようなエラーが繰り返し発生するのは、IAM ロールの削除を防止する SCP を使用して OU にアカウントがプロビジョニングされたためです。再試行する前に、アカウントのリソースをすべて削除することで、回復プロセスを短縮できます。

以下の例は、削除されていないロールとスタックが残っている場合に表示される可能性のある失敗に関するメッセージの種類を示しています。ほとんどの場合、古いリソースが残っている限り、アカウントを登録しようとするたびに、これらのメッセージのいずれかが表示されます。

この例では、リソース ID 文字列の値が変更されています。これらの値は、表示されるエラーメッセージでは同じにはなりません。次の例に示すようなメッセージが表示されます。

- 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.

または、次のようなスタックセットの失敗に関するエラーメッセージが表示されることがあります。

```
"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.
```

残りのリソースをすべて最初の OU から削除すると、アカウントを新しい OU に招待したり、プロビジョニングしたり、登録したりできるようになります。

AWS サポート

既存のメンバーアカウントを別のサポートプランに移動する場合は、ルートアカウントの認証情報を使用して各アカウントにサインインし、[プランを比較](#)して、希望するサポートレベルを設定できます。

サポートプランを変更するときは、MFA とアカウントのセキュリティの連絡先を更新することをお勧めします。

ベースラインのタイプ

AWS Control Tower のベースラインは、ターゲットに適用できるリソースと特定の設定のグループです。最も一般的なベースラインターゲットは、組織単位 (OU) です。例えば、ターゲットとして選択した OU でベースラインを有効にして、その OU を AWS Control Tower に登録できます。

ランディングゾーンの設定中に、一部のベースラインが共有アカウントで自動的に有効になる場合があります。ランディングゾーンの設定と構成に基づいて、特定のベースラインを有効にして更新できます。AWS Control Tower は、ベースラインで指定された方法でリソースを作成してターゲットにデプロイします。

ターゲットでベースラインを有効にすると、ベースラインは リソースと呼ばれる AWS EnabledBaseline リソースとして表されます。

AWS Control Tower には、一般的なベースラインタイプが 2 つあります。

- OU で有効にできるベースライン。
- ランディングゾーンのセットアップ中に共有アカウントで有効にできるベースライン。

OU レベルで適用されるベースラインタイプ

Note

EnableBaseline API で直接有効にできるのは、OU レベルで適用されるベースラインのみです。

- 名前: AWSControlTowerBaseline

説明: このベースラインは、コンプライアンスモニタリング、監査、セキュリティモニタリング、およびオプションでアクセス管理に必要な、ターゲット OU 内のメンバーアカウントのリソースとコントロールを設定します。このベースラインは、AWS Control Tower に OU を登録すると有効になります。

前提条件: AWS Control Tower ランディングゾーンで AWS Config 統合を有効にする必要があります。

考慮事項: このベースラインは、ランディングゾーンのリージョン拒否コントロールの設定を保持します。つまり、リージョンがランディングゾーンレベルで許可されていない場合、EnableBaseline API を呼び出して OU を登録する際に、そのリージョンはその OU に対して許可されません。

 Note

OU レベルのリージョン拒否コントロールは、ランディングゾーンのリージョン拒否コントロールが許可しないリージョンを許可することはできません。

詳細については、AWS Organizations ドキュメントの「How [SCPs work with deny](#)」を参照してください。

推奨事項: ターゲット OU がワークロードを実行している可能性のあるリージョンを確認し、その結果をランディングゾーンのリージョン拒否コントロールに対してチェックしてから、OU の EnableBaseline API を呼び出すことをお勧めします。そうしないと、特定のリージョンのリソースにアクセスできなくなる可能性があります。

- 名前: ConfigBaseline

説明: このベースラインは、Detective Controls の有効化に必要なターゲット OU 内のメンバーアカウントの AWS Config 関連リソースを設定します。セットアップされたリソースは、AWSControlTowerBaseline のリソースのサブセットです。

前提条件: AWS Control Tower ランディングゾーンで AWS Config 統合を有効にする必要があります。

考慮事項: このベースラインは、ランディングゾーンリージョン拒否コントロールの設定を保持しません。リージョン拒否コントロールは、ConfigBaseline の有効化の一部として有効になります。

制限: AWSControlTowerBaseline と ConfigBaseline を同じ OU で有効にすることはできません。OU では、そのうちの 1 つだけが許可されます。

- 名前: BackupBaseline

説明: このベースラインは、ターゲット OU 内のメンバーアカウントのリソースとコントロールを設定します。これらは、との統合 AWS Backup によってデータのバックアップが自動化され AWS のサービス、バックアップポリシー管理が一元化されるようにするために必要です。

前提条件:

- AWS Backup 統合は、AWS Control Tower ランディングゾーンで有効にする必要があります。
- AWS Config 統合は、AWS Control Tower ランディングゾーンで有効にする必要があります。
- AWSControlTowerBaseline ターゲット OU で を有効にする必要があります。

考慮事項: ターゲット OU で BackupBaseline を有効化する前に、ターゲット OU で AWSControlTowerBaseline が有効になっていることを確認してください。つまり、ターゲット OU は AWS Control Tower で登録されている必要があります。

- AWS Control Tower ランディングゾーンの作成プロセス AWS Backup 中にアクティブ化するか、ランディングゾーンの更新プロセス中にアクティブ化するかを選択できます。
- BackupBaseline は、ランディングゾーンバージョン 3.1 以降と互換性があります。
- BackupBaseline は管理アカウントには適用されません。

ランディングゾーンのセットアップ中に共有アカウントに適用できるベースラインタイプ

AWS Control Tower は、ランディングゾーンのセットアップと更新プロセスの一環として、共有アカウントの特定のベースラインを有効にします。ランディングゾーンの設定を変更すると、ランディングゾーンのベースラインが変更される場合があります。例えば、IAM アイデンティティセンターをオプトインした場合、AWS Control Tower はランディングゾーンで最新バージョンの IdentityCenterBaseline ベースラインを有効にすることができます。

ListEnabledBaselines API コールを使用すると、ランディングゾーンで有効になっているベースラインを表示できます。

Note

Landing Zone バージョン 4.0 以降、AuditBaseline は CentralSecurityRolesBaseline と の 2 つの異なるベースラインに置き換えられます CentralConfigBaseline。

- 名前: CentralConfigBaseline

説明: AWS Config を使用して、組織内のコンプライアンスのモニタリングと監査のための中央リソースを設定します。

- 名前: CentralSecurityRolesBaseline

説明: 組織内のセキュリティモニタリング用の中央リソースを設定します。

- 名前: AuditBaseline

説明: 組織内のアカウントのセキュリティとコンプライアンスをモニタリングするためのリソースを設定します。

- 名前: LogArchiveBaseline

説明: 組織内のアカウントからの API アクティビティとリソース設定のログ用に中央リポジトリを設定します。

- 名前: IdentityCenterBaseline

説明: IAM アイデンティティセンターの共有リソースを設定します。これにより、AWSControlTowerBaseline がアカウントのアイデンティティセンターアクセスを設定する準備が整います。

考慮事項: このベースラインが機能するのは、ランディングゾーンの初期設定時に ID プロバイダーとして IAM アイデンティティセンターを選択した場合、または後でランディングゾーン設定を変更して、IAM アイデンティティセンターをランディングゾーンに対して有効にした場合のみです。別の ID プロバイダーを使用している場合、このベースラインを有効にするためのアクセス権限はありません。

- 名前: BackupCentralVaultBaseline

説明: 組織内の中央 AWS Backup ボールトを設定します。

- 名前: BackupAdminBaseline

説明: 委任管理者と AWS Backup Audit Manager を設定します。

アカウントの一部登録

ベースラインの操作中に、アカウントが一部登録済みという状態になる場合があります。

この状態は、ResetEnabledBaseline API を呼び出して OU を再登録する場合に発生する可能性があります。AWS Control Tower は、ターゲット OU のアカウントに必須リソースのみを適用する

ためです。親 OU のオプションリソース (コントロール) がないアカウントは、一部登録済みとマークされます。

未登録のアカウントを登録済みの OU に移動した後、その OU に対して `ResetEnabledBaseline` API を呼び出してそのアカウントを登録すると、AWS Control Tower は `AWSControlTowerBaseline` に関連付けられたリソースを新しく登録されたアカウントに適用します。ただし、この OU で有効になっているオプションコントロールは、アカウントに適用されません。アカウントは一部登録済み状態のままです。

アカウントを完全に登録するには、コンソールで [再登録] または [アカウントの更新] を選択します。コンソールからこれらのオペレーションを選択すると、AWS Control Tower は、その OU に対してアクティブ化されるオプションコントロールも含めて、その OU のすべてのリソースを新しく登録されたアカウントに適用します。

AWS Control Tower コンソールとベースラインの API でのオペレーションの相違点

OU のガバナンスステータスを変更する場合、AWS Control Tower コンソールは、ベースラインの API を使用してガバナンスを変更する場合と比べて、より多くのオペレーションを自動的に実行します。

相違点

- 登録とプロビジョニング済み製品

コンソールを介して OU を登録すると、AWS Control Tower は各アカウントの登録の一環として、OU のメンバーアカウント用に Service Catalog 製品を作成します。EnableBaseline API と `AWSControlTowerBaseline` を使用して OU を登録すると、AWS Control Tower は OU のメンバーアカウント用にプロビジョニング済み製品を作成しません。

- OU の登録解除

OU の登録を解除するときは、まずすべてのメンバーアカウントとネストされた OU を削除する必要があります。その後、OU に適用されているすべてのコントロールを AWS Control Tower が削除します。

- コンソールから OU の [削除] を選択すると、AWS Control Tower は登録解除に進み、組織から OU を削除します。

- 一方、DisableBaseline API を呼び出して OU から AWSControlTowerBaseline を削除することで OU を登録解除しても、AWS Control Tower は組織から OU を削除せず、OU は未登録のまま組織内に残ります。

有効なベースラインとメンバーアカウント

OU でベースラインを有効にすると、その設定は OU のメンバーアカウントによって継承されます。継承の事実により、アカウントを参照するときに子で有効なベースラインと呼びます。OU に適用されるベースラインは、親で有効なベースラインと呼ばれます。親で有効なベースラインは、子で有効なベースラインの設定を制御します。これは、OU で有効になっている制御が OU 内のすべてのアカウントに適用されるのに似ています。

アカウントのベースラインのステータスを表示する

AWS Control Tower では、ベースラインを使用してアカウントを直接ターゲットにすることはできません。ただし、継承された子で有効なベースラインを使用して、各メンバーアカウントの有効化とドリフトのステータスを追跡できます。アカウントのステータスを表示するには、includeChildren 機能フラグを使用して [ListEnabledBaselines](#) API を呼び出します。

アカウントのベースラインを無効にする

AWS Control Tower では、親が有効なベースラインにリンクされた子が有効なベースラインを無効にすることはできません。子が有効なベースラインは、継承がドリフトし、親が有効なベースラインにリンクされなくなった場合に無効にできます。

ベースラインとバージョニングのデフォルト

AWS Control Tower のランディングゾーンが既に設定されている場合に、ランディングゾーンのベースラインの有効化を選択すると、AWS Control Tower はランディングゾーンのバージョンと互換性のある最新バージョンのベースラインを有効にします。まだ AWS Control Tower に登録されていない OU に対してベースラインの有効化を選択すると、AWS Control Tower は互換性のある最新バージョンのベースラインをその OU に自動的に提供します。

OU ベースラインとランディングゾーンバージョンの互換性

AWS Control Tower ベースラインを使用すると、ビジネスニーズに応じて、ランディングゾーンレベルではなく、OU レベルでガバナンス標準を設定できます。OU を AWS Control Tower に登録するのに役立つ AWSControlTowerBaseline というベースラインがあります。

Note

ベースラインとは、ランディングゾーン内に安定したガバナンス環境を確立するために連携するコントロールとリソースのグループです。

AWS Control Tower で EnableBaseline API を呼び出して OU でベースラインを有効にする際には、現在の AWS Control Tower ランディングゾーンバージョンと互換性のあるベースラインバージョンを指定する必要があります。ベースラインを指定すると、OU 内のすべてのメンバーアカウントが OU に指定されたベースラインに従います。つまり、新しいアカウントは更新されたベースラインでプロビジョニングされ、既存のメンバーアカウントは新しいベースラインに従って管理されるようになります。

既存の OU とアカウントのベースラインを選択しない場合は、デフォルトで、ランディングゾーンバージョンによってガバナンス体制全体が決まります。ただし、ランディングゾーンに登録された各 OU にはベースラインバージョンが割り当てられています。これは、現在のランディングゾーンバージョンと互換性のある最新のベースラインです。したがって、特にベースラインを割り当てなくても、OU と登録済みのメンバーアカウントにはそれぞれベースラインが関連付けられています。

OU レベルのベースライン AWSControlTowerBaseline について、ベースラインと AWS Control Tower ランディングゾーンバージョンの互換性を次の表に示します。

ベースラインバージョン	ランディングゾーンバージョン	含まれるグループプリント	以前のベースラインからの変更		
1.0	2.0 ~ 2.7	BP_BASELINE_CLOUDTRAIL、BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLE、BP_BASELINE_SERVICE、BP_BASELINE_SERVERICE_ROLES	なし		

ベースラインバージョン	ランディングゾーンバージョン	含まれるブループリント	以前のベースラインからの変更		
		、IAM リソース			
2.0	2.8 ~ 2.9	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLE、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM リソース	SLR を使用するための AWS Config サービスにリンクされたロール (SLR) と新しい Config ブループリントを追加		
3.0	3.0 ~ 3.1	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLE、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM リソース	新しい AWS Config ブループリント。グローバルリソースをホームリージョンでのみ記録するように変更。CloudTrail ブループリントを削除		

ベースラインバージョン	ランディングゾーンバージョン	含まれるブループリント	以前のベースラインからの変更		
4.0	3.2 ~ 3.3	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_LINKED_ROLE、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM リソース	新しい SLR ブループリント		

ベースラインバージョン	ランディングゾーンバージョン	含まれるブループリント	以前のベースラインからの変更		
5.0	4.0	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_LINKED_ROLE、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM リソース	AWS Config Aggregation on Authorization (複数可) を削除しました。LandingZone AWS Config バージョン 4.0 では、組織内のすべてのメンバーアカウントにアクセスできる AWS Organizations Config Aggregator を採用しているため、各メンバーアカウントからの AWS Config Aggregation Authorization は必要ありません。		

ランディングゾーンのセットアップ時にアカウントに作成された特定のリソースの詳細については、「[Resources created in the shared accounts](#)」を参照してください。

ランディングゾーンを、新しい AWSControlTowerBaseline ベースラインバージョンをサポートするバージョンに更新したときに、新しいランディングゾーンバージョンが既存のベースラインバージョンと互換性がある場合は、OU の状態が [更新が利用できます] に変わります。

- ランディングゾーンが 2.x から 3.x に更新される場合を除き、OU のベースラインをすぐに更新しなくても、アカウントファクトリやその他の機能を引き続き使用できます。
- この OU に登録された新しいアカウントは、(コンソールで [ガバナンスを拡張] 機能を使用するか、UpdateEnabledBaseline API を使用して) ベースラインバージョンが更新されるまで、既存のベースラインバージョンに基づいてリソースを受け取ります。
- ベースラインバージョンを更新すると、その OU 内のすべてのアカウントが新しいベースラインバージョンに基づいてリソースを受け取ります。

Note

AWS Control Tower ランディングゾーンをバージョン 2.X からバージョン 3.X に更新する場合、アカウントレベルから組織レベルの AWS CloudTrail 証跡への変更により、OUs のベースラインバージョンも更新する必要があります。コンソールで、OU のステータスが [更新は必須です] と表示されます。

ベースラインに関する考慮事項

- OU でベースラインの更新が必要な場合は、新しいアカウントをプロビジョニングしたり、既存のアカウントをその OU に登録したりすることはできません。
- ランディングゾーンの更新後、OU のベースラインも更新する場合は、OU を再登録するか、OU のベースラインバージョンをプログラムで更新する必要があります。
- ランディングゾーンとベースラインを組み合わせた場合の利点がすべて得られるように、ご使用のランディングゾーンバージョンと互換性のある最も高いバージョンのベースラインに更新することをお勧めします。例えば、ランディングゾーンバージョン 3.3 に更新した場合、ベースライン 3.0 を引き続き使用できますが、ベースライン 4.0 への更新も行わないと、ランディングゾーンバージョン 3.3 の利点をすべて得ることはできません。
- ベースラインの更新はロールバックできません。
- ベースラインの有効化は、一度に 1 つの OU を対象とします。したがって、ネストされた OU は、親 OU が更新されても自動的に更新されません。ネストされた OU を更新する前に、親 OU を更新することをお勧めします。

- UpdateEnabledBaseline API を呼び出すか、コンソールから OU を再登録した場合、OU はベースラインの更新前に有効になっていたすべてのコントロールを保持します。
- ランディングゾーンバージョンと互換性のあるベースラインバージョンが複数あるときに、管理対象外の OU でベースラインを有効にする場合は、最新のベースラインバージョンを使用する必要があります。

例: API のみを使用して AWS Control Tower OU を登録する

この例によるチュートリアルは、付随的なドキュメントです。説明、注意事項、および詳細については、「[ベースラインのタイプ](#)」を参照してください。

前提条件

登録する OU として、AWS Control Tower に登録されていない既存の OU が必要です。または、更新の目的で再登録する、登録済みの OU が必要です。

OU の登録

1. IdentityCenterBaseline がランディングゾーンに対して有効になっているかどうかを確認します。有効になっている場合は、アイデンティティセンターの有効なベースラインの識別子を取得します。

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. ターゲット OU の ARN を取得します。

```
aws organizations describe-organizational-unit --organizational-unit-id  
<Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. AWSControlTowerBaseline ベースラインの ARN を取得します。

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].[arn]'
```

4. ターゲット OU に AWSControlTowerBaseline ベースラインを作成します。

アイデンティティセンターベースラインが有効になっている場合:

```
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>" } ]'
```

アイデンティティセンターベースラインが有効になっていない場合は、次のように `parameters` フラグを省略します。

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
--baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

OU の再登録

ランディングゾーン設定の更新を行うか、ランディングゾーンバージョンを更新した後は、OU を再登録して最新の変更を加える必要があります。以下の手順に従って、関連付けられた `EnabledBaseline` リソースおよび関連する `EnabledControl` リソースをリセットして、OU をプログラムで再登録します。

Important

OU でオプションのコントロールが有効になっている場合は、ベースラインをリセットした後、有効なオプションコントロールごとに [ResetEnabledControl](#) API を呼び出す必要があります。このステップにより、オプションのコントロールが最新のランディングゾーン設定と整合性が保たれます。このステップをスキップすると、OU のオプションコントロールに最新のランディングゾーンの変更が反映されない場合があります。オプションのコントロールが有効になっていない場合、このステップは必要ありません。

1. 再登録するターゲット OU の ARN を取得します。

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. ターゲット OU の `EnabledBaseline` リソースの ARN を取得します。

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier=='<OUARN>'].[arn]'
```

3. 有効なベースラインをリセットします。

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

4. OU でオプションのコントロールが有効になっている場合は、OU に対して有効なコントロールを一覧表示し、それぞれをリセットして、最新のランディングゾーン設定との整合性を維持します。

ターゲット OU で有効なコントロールを一覧表示します。

```
aws controltower list-enabled-controls --target-identifier <OU ARN>
```

有効なオプションコントロールが返されるたびに、以下を呼び出してリセットします。

```
aws controltower reset-enabled-control --enabled-control-
identifier <EnabledControlArn>
```

詳細については、AWS Control Tower API リファレンスの[ResetEnabledControl](#)」を参照してください。

ベースライン API の使用例

このセクションでは、AWS Control Tower ベースライン API の入出力パラメータの例を示します。

DisableBaseline

この API オペレーションの詳細については、「[DisableBaseline](#)」を参照してください。

DisableBaseline の入力:

```
{
  "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

DisableBaseline の出力:

```
{
  "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

DisableBaseline CLI の例:

```
aws controltower disable-baseline \
  --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
  --region us-west-2
```

EnableBaseline

この API オペレーションの詳細については、「[EnableBaseline](#)」を参照してください。

EnableBaseline の入力:

```
{
  "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
  "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjq1",
  "baselineVersion": "3.0",
  "parameters": [
    {
      "key": "IdentityCenterEnabledBaselineArn",
      "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTISI4W07MZ"
    }
  ]
}
```

EnableBaseline の出力 (新しいリソースを返す):

```
{
  "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
  "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TN0HRD7ES5VV"
}
```

EnableBaseline CLI の例:

この例では、AWS Control Tower AWSによって管理される IAM Identity Center アクセスにオプトインされたランディングゾーンを持つAWS Organizations組織のベースラインを有効にする方法を示します。アイデンティティセンターの EnabledBaseline 識別子を取得するには、ListEnabledBaselines API を呼び出し、アイデンティティセンターベースライン: (arn:aws:controltower:*Region*::baseline/LN25R72TTG6IGPTQ)でフィルタリングします。

```
aws controltower list-enabled-baselines \
  --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
  --region us-west-2
```

レスポンスには EnabledBaseline の詳細が表示されます。この中に識別子が示されています。

```
{
  "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

レスポンスの ARN 値を書き留め、この値をパラメータとして渡してデフォルトのベースラインを有効にします。

```
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-po90-1k87jh65 \  
--parameters  
'[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \  
--region us-west-2
```

ランディングゾーンが IAM アイデンティティセンターの AWS Control Tower 管理からオプトアウトされている組織に対しては、パラメータなしでベースラインを有効にします。

```
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-po90-1k87jh65 \  
--region us-west-2
```

GetBaseline

この API オペレーションの詳細については、「[GetBaseline](#)」を参照してください。

GetBaseline の入力:

```
{  
  "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"  
}
```

GetBaseline の出力:

```
{  
  "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 の例:

```
aws controltower get-baseline \  

```

```
--baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \  
--region us-west-2
```

GetBaselineOperation

この API オペレーションの詳細については、「[GetBaselineOperation](#)」を参照してください。

GetBaselineOperation の入力:

```
{  
  "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"  
}
```

GetBaselineOperation の出力:

```
{  
  "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 の例:

```
aws controltower get-baseline-operation \  
  --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \  
  --region us-west-2
```

GetEnabledBaseline

この API オペレーションの詳細については、「[GetEnabledBaseline](#)」を参照してください。

GetEnabledBaseline の入力:

```
{
```



```
"enabledBaselineIdentifier": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/XAHCR4CJTISI4W07MZ"
}
```

GetEnabledBaseline の出力:

```
{
  "enabledBaselineDetails": {
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/XAHCR4CJTISI4W07MZ",
    "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/XAHCR4CJTISI4W07MZ"
      }
    ]
  }
}
```

GetEnabledBaseline CLI の例:

```
aws controltower get-enabled-baseline \
  --enabled-baseline-identifier arn:aws:controltower:us-west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EYC \
  --region us-west-2
```

ListBaselines

この API オペレーションの詳細については、「[ListBaselines](#)」を参照してください。

ListBaselines の入力 (オプションの入力を使用):

```
{
  "nextToken": "AbCd1234",
  "maxResults": "4"
}
```

ListBaselines の出力:

```
{
  "baselines": [
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/4T4HA1KM010S6311",
      "name": "AuditBaseline",
      "description": "Sets up resources to monitor security and compliance of accounts in your organization."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/J8HX46AHS5MIKQPD",
      "name": "LogArchiveBaseline",
      "description": "Sets up a central repository for logs of API activities and resource configurations from accounts in your organization."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/LN25R72TTG6IGPTQ",
      "name": "IdentityCenterBaseline",
      "description": "Sets up shared resources for AWS Identity Center, which prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2",
      "name": "AWSControlTowerBaseline",
      "description": "Sets up resources and mandatory controls for member accounts within the target OU, required for AWS Control Tower governance."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/3WPD0NA6TJ9A0MU2",
      "name": "BackupCentralVaultBaseline",
      "description": "Sets up central AWS Backup vault in your organization."
    },
    {
      "arn": "arn:aws:controltower:us-east-1::baseline/H6C5JFCJJ3CPU3J5",
      "name": "BackupManagerBaseline",
      "description": "Sets up delegated admin and AWS Backup Audit Manager."
    }
  ]
}
```

```
{
  "arn": "arn:aws:controltower:us-east-1::baseline/AP09ATVPBKFRRLK",
  "name": "BackupBaseline",
  "description": "Sets up local Backup vault and attach Backup policy."
}
]
```

ListBaselines CLI の例:

```
aws controltower list-baselines \
  --region us-west-2
```

ListEnabledBaselines

ListEnabledBaselines API には、OU のメンバーであるアカウントに適用されるベースラインを表示できるオプションのパラメータがあります。以下の例は、アカウントのベースラインを表示するために使用できる CLI コマンドの一部を示しています。AWS Control Tower は、OU で有効になっているこれらのベースラインを参照しますが、OU に適用されるベースラインからガバナンス設定を取得するため、子で有効なベースラインとして OU 内の各アカウントに適用します。

この API オペレーションの詳細については、「[ListEnabledBaselines](#)」を参照してください。

子で有効なベースラインを表示する ListEnabledBaselines 入力。

```
aws controltower list-enabled-baselines --include-children
```

子で有効なベースラインを表示する ListEnabledBaselines 出力。

```
{
  "enabledBaselines": [
    {
      "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/X02UQ1PC6BB5085S5",
      "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/AP09ATVPBKFRRLK",
      "baselineVersion": "1.0",
      "statusSummary": {
        "lastOperationIdentifier": "07d6d2b8-e357-4f96-ba00-98ea88143445",
        "status": "SUCCEEDED"
      }
    },
  ],
}
```

```

        "targetIdentifier": "arn:aws:organizations::666355521292:ou/o-vaex10vaey/
ou-k86y-ld9k8vpu"
      },
      {
        "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XAFPKQQX0JB50ZWQH",
        "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
AP09ATVPBKFRRLK",
        "baselineVersion": "1.0",
        "parentIdentifier": "arn:aws:controltower:us-
east-1:666355521292:enabledbaseline/X0IZ4G08CWB50ZWON",
        "statusSummary": {
          "lastOperationIdentifier": "3508793e-48c8-4895-965b-3dc6abd52b6b",
          "status": "SUCCEEDED"
        },
        "targetIdentifier": "arn:aws:organizations::666355521292:account/o-
vaex10vaey/183295447314"
      }
    ]
  ]

```

Note

前の例では、`parentIdentifier` フィールドには、この子で有効なベースラインの親 OU の有効なベースラインを示します。

特定のターゲット (OU またはアカウント) に適用されているすべてのベースラインを表示します。

```

aws controltower list-enabled-baselines \
  --filter '{
    "targetIdentifiers": ["TARGET_ARN"]
  }

```

特定のベースラインを持つすべての OU を表示します。

```

aws controltower list-enabled-baselines \
  --filter '{
    "baselineIdentifiers": ["BASELINE_ARN"]
  }'

```

特定のベースラインを持つすべての OU とアカウントを表示します。

```
aws controltower list-enabled-baselines \
  --filter '{
    "baselineIdentifiers": ["BASELINE_ARN"]
  }' \
  --include-children
```

ベースライン B が有効になっている OU のすべてのアカウントを表示します。

```
### First fetch the enabled baseline record for Baseline B on the OU
aws controltower list-enabled-baselines \
  --filter '{
    "targetIdentifiers": ["OU_TARGET_ARN"],
    "baselineIdentifiers": ["BASELINE_ARN_FOR_BASELINE_B"]
  }'

### Call ListEnabled baseline to fetch all accounts that have their parent as the
enabled baseline record on the OU
aws controltower list-enabled-baselines \
  --filter '{
    "parentIdentifiers": ["ENABLED_BASELINE_ARN_FOR_OU"]
  }' \
  --include-children
```

子で有効なベースラインの詳細

- GetEnabledBaseline API を使用して、特定の子で有効なベースラインに関する詳細情報を表示できます。
- GetBaselineOperation API を使用して、子で有効なベースラインで実行されたオペレーションを表示できます。
- 子で有効なベースラインでは、EnableBaseline、UpdateEnabledBaseline、ResetEnabledBaseline、DisableBaselineなどの書き込み API を直接呼び出すことはできません。
- 子で有効なベースラインリソースは、AWS Control Tower サービス、親 OU で実行されるオペレーション、または Account Factory によってのみ変更できます。

フィルターの使用例:

ListEnabledBaselines の入力 (フィルターなし):

```
{
  "nextToken": "bde7-XX0c6fXXXXXX",
  "maxResults": 5
}
```

ListEnabledBaselines の入力 (baselineIdentifiers フィルターのみ):

```
{
  "filter": {
    "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
  },
  "nextToken": "bde7-XX0c6fXXXXXX",
  "maxResults": 5
}
```

ListEnabledBaselines の入力 (targetIdentifiers フィルターのみ):

```
{
  "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 の入力 (baselineIdentifiers および targetIdentifiers フィルター):

```
{
  "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 の出力:

```
{
  "enabledBaselines": [
    {
      "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCRC4CJTSI4W07MZ",
      "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
      "baselineVersion": "3.0",
      "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjq1",
      "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"
}
```

1 種類のフィルター (baselineIdentifiers フィルター) を使用した CLI の例:

```
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
```

複数のフィルター (baselineIdentifiers および targetIdentifiers フィルター) を使用した CLI の例:

```
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

この API オペレーションの詳細については、「[ResetEnabledBaseline](#)」を参照してください。

ResetEnabledbaseline の入力:

```
{
  "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

ResetEnabledBaseline の出力:

```
{
  "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

ResetEnabledBaseline CLI の例:

```
aws controltower reset-enabled-baseline \
  --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EYC \
  --region us-west-2
```

UpdateEnabledBaseline

この API オペレーションの詳細については、「[UpdateEnabledBaseline](#)」を参照してください。

UpdateEnabledBaseline の入力:

```
{
```



```
{
  "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/
XAHCR4CJTISI4W07MZ"
    }
  ]
}
```

UpdateEnabledBaseline の出力:

```
{
  "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

UpdateEnabledBaseline CLI の例:

```
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
```

追加情報とリンク

このトピックには、関連するブログ記事、技術ドキュメント、関連情報へのリンクが含まれています。AWS Control Tower を使用する場合にお役立てください。ソースは、AWS Control Tower の機能と追加の拡張機能に関する一般的なユースケースとベストプラクティスを網羅しています。

チュートリアルとラボ

- [AWS Control Tower ラボ](#) - これらのラボでは、AWS Control Tower に関してよく使用されるタスクの大まかな概要を示します。
- ユースケースは念頭にあってもどこから始めるべきかわからない場合は、AWS Control Tower ダッシュボードで [Get personalized guidance] (パーソナライズされたガイダンスを取得する) を選択してください。
- この [AWS クラウド運用 YouTube プレイリスト](#) にアクセスして AWS Control Tower を検索し、AWS Control Tower の機能の使用方法について詳しく説明する動画をご覧ください。

ネットワーク

でネットワークの繰り返し可能なパターンと管理可能なパターンを設定します AWS。お客様によく使用される設計、オートメーション、およびアプライアンスの詳細について確認します。

- [AWS クイックスタート VPC アーキテクチャ](#) - このクイックスタートガイドは、AWS クラウドインフラストラクチャの AWS ベストプラクティスに基づくネットワーク基盤を提供します。AWS サービスやその他のリソースを起動できるパブリックサブネットとプライベートサブネットを持つ AWS Virtual Private Network 環境を構築します。
- [AWS Service Catalog を使用した AWS Control Tower のセルフサービス VPC](#) - このブログ記事では、Account Factory をセットアップして、カスタマイズした VPC でアカウントをプロビジョニングできるようにする方法について説明しています。
- [AWS Control Tower での Serverless Transit Network Orchestrator \(STNO\) の実装](#) - このブログ記事では、アカウント間でのネットワーク接続アクセスを自動化する方法について説明しています。このブログは、AWS Control Tower 管理者または AWS 環境内のネットワークを管理する担当者を対象としています。

セキュリティ、アイデンティティ、ログ記録

セキュリティ体制を拡張し、外部または既存のアイデンティティプロバイダーと統合して、ログ記録システムを一元管理します。

セキュリティ

- [AWS Control Tower ライフサイクルイベントによる AWS Security Hub CSPM アラートの自動化](#) – このブログ記事では、既存アカウントと新規アカウントの AWS Control Tower マルチアカウント環境で Security Hub CSPM の有効化と設定を自動化する方法について説明します。
- [有効化 AWS Identity and Access Management](#) – このブログ記事では、IAM Access Analyzer の検出結果を有効にして一元化することで、組織のセキュリティの可視性を高める方法について説明します。
- [AWS Systems Manager Parameter Store](#) は、設定データ管理とシークレット管理のための安全な階層型ストレージを提供します。これにより、安全な場所で設定情報を共有して、AWS Systems Manager と AWS CloudFormation で設定情報を使用できるようになります。例えば、適合パックをデプロイするリージョンのリストを保存できます。

アイデンティティ

- [Azure AD ユーザー ID をシングルサインオン用の AWS アカウントとアプリケーションにリンクする](#) – このブログ記事では、IAM Identity Center と AWS Control Tower で Azure AD を使用方法について説明します。
- [で Okta ユーザーの AWS へのアクセスを一元管理する AWS IAM アイデンティティセンター](#) – このブログ記事では、IAM Identity Center と AWS Control Tower で Okta を使用方法について説明します。

ログ記録

- [AWS 一元的なログ記録ソリューション](#) – このソリューションの投稿では、組織が複数のアカウント AWS とリージョン AWS でログを収集、分析、表示できるようにする一元的なログ記録ソリューションについて説明しています。
- AWS Config リソースの表示については、[「Config Resource Compliance Dashboard」](#)を参照してください。

リソースのデプロイとワークロードの管理

リソースとワークロードをデプロイして管理します。

- [入門ライブラリ統合](#) - このブログ記事では、使用できる入門ポートフォリオについて説明しています。
- [AWS Control Tower への Cloud Custodian の継続的なデプロイ](#)

既存の組織とアカウントの操作

既存の AWS 組織とアカウントを使用します。

- [アカウントの登録](#) - このユーザーガイドトピックでは、AWS Control Tower に既存の AWS アカウントを登録する方法について説明します。
- [AWS Control Tower でアカウントを使用する](#) - このブログ記事では、AWS Control Tower を既存の AWS 組織にデプロイする方法について説明します。
- [AWS Config 適合パックを使用した AWS Control Tower 管理の拡大](#) - このブログ記事では、既存のアカウントと組織を AWS Control Tower の管理対象にする際に役立つ AWS Config 適合パックをデプロイする方法について説明しています。
- [AWS Control Tower でガードレール違反を検出して軽減する方法](#) - このブログ記事では、コントロールのコンプライアンス違反について E メールで通知できるように、コントロールを追加する方法と SNS 通知をサブスクライブする方法について説明しています。

オートメーションと統合

AWS Control Tower でアカウント作成を自動化し、ライフサイクルイベントを統合します。

- [ライフサイクルイベント](#) - このブログ記事では、AWS Control Tower でライフサイクルイベントを使用する方法について説明しています。
- [アカウント作成の自動化](#) - このブログ記事では、AWS Control Tower で自動アカウント作成をセットアップする方法について説明しています。
- [Amazon VPC フローログのオートメーション](#) - このブログ記事では、マルチアカウント環境で Amazon VPC フローログのオートメーションおよび一元管理を行う方法について説明しています。

- [AWS Control Tower ライフサイクルイベントを使用した VPC タグ付けの自動化](#) - このブログ記事では、AWS Control Tower のライフサイクルイベントを使用して、VPC 用にリソースをタグ付けする作業を自動化する方法について説明しています。
- [自動アカウント管理](#) - このブログ記事では、AWS Control Tower 環境のセットアップ後にアカウント管理タスクを自動化する方法について説明しています。

ワークロードの移行

AWS Control Tower で他の AWS サービスを使用して、ワークロードの移行を支援します。

- [CloudEndure の移行](#) - このブログ記事では、CloudEndure およびその他の AWS サービスと AWS Control Tower を組み合わせてワークロードの移行を支援する方法について説明します。

AWS の関連サービス

AWS Control Tower は、AWS Organizations のオーケストレーションレイヤーとして機能します。これにより、AWS Organizations コンソールと API を使用して、AWS Control Tower で動作する 20 以上の他の AWS のサービスにアクセスできます。このような他のサービスに、AWS Control Tower コンソールから直接アクセスすることはできません。

- AWS Organizations によって AWS Control Tower で利用できるようになるサービスの詳細なリストについては、「[AWS services that you can use with AWS Organizations](#)」(AWS Organizations で使用できる AWS のサービス) を参照してください。
- これらの関連する AWS のサービスでマルチアカウント機能を有効にするには、信頼されたアクセスを有効にする必要があります。詳細については、「[Using AWS Organizations with other AWS services](#)」(他の AWS のサービスでの AWS Organizations の使用) を参照してください。

Note

AWS IAM Identity Center、AWS CloudTrail は AWS Control Tower でセットアップされ AWS Config、完全に統合されていることに注意してください。これらのサービスのために信頼されたアクセスや委任管理設定を変更する必要はありません。

- で利用できる AWS サービスの中には AWS Organizations、AWS Systems Manager や AWS Firewall Manager など、委任管理を使用できるものがあります。詳細については、「[Configuring a Delegated Administrator](#)」(委任管理の設定) および「[Enabling a delegated administrator account](#)

[for Firewall Manager](#)」 (Firewall Manager 用の委任管理者アカウントの有効化) を参照してください。「[Set up security groups with AWS Firewall Manager](#)」 (AWS Firewall Manager を使用したセキュリティグループのセットアップ) という動画もご覧ください。

AWS Marketplace ソリューション

ソリューションについては、「」を参照してください AWS Marketplace。

- [AWS Control Tower Marketplace](#) – AWS Control Tower には、サードパーティーソフトウェアの統合に役立つ幅広いソリューション AWS Marketplace が用意されています。これらのソリューションは、アイデンティティ管理、マルチアカウント環境のセキュリティ、ネットワークの一元管理、運用インテリジェンス、セキュリティ情報およびイベント管理 (SIEM) など、インフラストラクチャと運用の主要なユースケースを解決する場合に役立ちます。

AWS Control Tower リリースノート

以下のセクションで、サービスの開始以降の AWS Control Tower リリースの詳細を示します。一部のリリースでは、AWS Control Tower ランディングゾーンの更新が必要であり、他のリリースは自動的にサービスに組み込まれます。

機能およびリリースは、公式に発表された日付を基準として新しい順 (最新が最初) に記載されています。

トピック

- [2026 年 1 月 ~ 現在](#)
- [2025 年 1 月 ~ 2025 年 12 月](#)
- [2024 年 1 月 ~ 12 月](#)
- [2023 年 1 月 ~ 12 月](#)
- [2022 年 1 月 ~ 12 月](#)
- [2021 年 1 月 ~ 12 月](#)
- [2020 年 1 月 ~ 12 月](#)
- [2019 年 6 月 ~ 12 月](#)

2026 年 1 月 ~ 現在

2026 年 1 月以降、AWS Control Tower は次の更新をリリースしました。

- [欧州の主権クラウドで利用可能な AWS Control Tower](#)

欧州の主権クラウドで利用可能な AWS Control Tower

2026 年 1 月 13 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が欧州の主権クラウドで利用可能になりました。European Sovereign Cloud の AWS Control Tower の詳細については、[「European Sovereign Cloud の AWS Control Tower ユーザーガイド」](#)を参照してください。

2025 年 1 月 ~ 2025 年 12 月

2025 年 1 月以降、AWS Control Tower は次の更新をリリースしました。

- [AWS Control Tower ランディングゾーンバージョン 4.0](#)
- [AWS Control Tower が Control Catalog に 279 個の AWS Config コントロールを追加](#)
- [AWS Control Tower が、アジアパシフィック \(ニュージーランド\) リージョンで利用可能に](#)
- [AWS Control Tower が自動アカウント登録をサポート](#)
- [AWS Control Tower が Python バージョンを更新](#)
- [AWS Control Tower が IPv6 アドレスをサポート](#)
- [AWS Control Tower がドリフトを低減](#)

[Account Factory for Terraform バージョン 1.15.0 が利用可能に](#)

- [Nitro インスタンスタイプでコントロールを更新](#)
- [AWS Control Tower がアジアパシフィック \(台北\) リージョンで利用可能に](#)
- [AWS Control Tower が PrivateLink をサポート](#)
- [追加の業界フレームワークのサポート、メタデータの更新](#)
- [サービスにリンクされた AWS Config コントロール](#)
- [有効なコントロールコンソールビューによる一元的な可視性](#)
- [the section called “Account Factory for Terraform \(AFT\) がデプロイ時に新しい設定をサポート”](#)
- [AWS Control Tower がベースライン API のアカウントレベルのレポートを導入](#)
- [the section called “AWS アジアパシフィック \(タイ\) およびメキシコ \(中部\) リージョンで利用可能な AWS Control Tower”](#)
- [利用可能な追加の AWS Config コントロール](#)
- [OU のアクションの登録解除と削除](#)
- [the section called “Control Catalog が IPv6 アドレスをサポート”](#)

AWS Control Tower ランディングゾーンバージョン 4.0

2025 年 11 月 17 日

(AWS Control Tower ランディングゾーンをバージョン 4.0 に更新する必要があります。詳細については、「」を参照してください[ランディングゾーンを更新する](#))。

AWS Control Tower ランディングゾーン 4.0 は、柔軟な Controls-Only エクスペリエンスを導入する主要な更新プログラムであり、お客様は AWS マルチアカウント環境の実装と管理方法をカスタマイズできます。このリリースでは、AWS Control Tower が AWS サービスと統合し、組織リソースを管理する方法が大幅に変更されました。主な変更点については、「」を参照してください[Landing Zone v4.0 移行ガイド](#)。

主な変更点と機能

- オプションのサービス統合 - ランディングゾーン 4.0 では、環境で有効にするサービス統合を選択できます。統合を無効にすると、マネージドアカウントとサービス統合中央アカウントで、その統合に固有の AWS Control Tower デプロイ済みリソースがクリーンアップされます。サービス統合を選択的に有効または無効にできるようになりました。

- AWS Config
- AWS CloudTrail
- セキュリティロール
- AWS Backup

重要: AWS Config 統合を無効にする場合は、セキュリティロール、IAM アイデンティティセンター、AWS Backup 統合も無効にする必要があります。

- 共有リソースを使用する代わりに専有リソース - ランディングゾーン 4.0 がキーサービス専用のリソースを作成できるようになりました。この分離により、リソースの分離が改善され、サービス固有のリソースをより詳細に制御できます。

- AWS Config の個別の S3 バケット
- AWS CloudTrail 用に S3 バケットを分離する
- 各サービスの個々の SNS トピック

- Flexible Organization Structure - ランディングゾーン 4.0 は、以前の組織構造要件を削除します。

- セキュリティ OU を使用する必要がなくなった
- 独自の組織構造を定義できます
- 唯一の要件は、すべてのハブアカウントが同じ OU に存在する必要があることです。

- 専用コントロールエクスペリエンス - 以下を含む最小限のランディングゾーン設定を作成できるようになりました。

- AWS Organizations の基本的な統合

- AWSControlTowerBaseline ベースラインを有効にせずにコントロールを有効にする機能
- ニーズに基づいたカスタムガバナンス設定
- AWS Config の変更 - Landing Zone 4.0 では、AWS Config 統合の実装にいくつかの改善が導入されています。
 - 検出コントロール専用の新しい Config スポークベースライン
 - Config ハブアカウントのサービスにリンクされた Config アグリゲータ (SLCA)
 - 従来の組織とアカウントアグリゲータの置き換え
- オプションのマニフェスト:
 - マニフェストフィールドがオプションになり、次のことができるようになりました。
 - サービス統合なしでランディングゾーンを作成する
 - 初期設定の柔軟性の向上
 - カスタマイズされたデプロイオプション

AWS Control Tower が Control Catalog に 279 個の AWS Config コントロールを追加

2025 年 11 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower には、AWS Config コントロールカタログの一部として追加の 279 個のコントロールが含まれるようになりました。コントロールは、AWS Control Tower コンソールと APIs を使用して表示できます。

特定のコントロールは、他のコントロールと関係があります。これらの関係は、AWS Control Tower コンソールと APIs。関係タイプには、補完的、相互排他的、代替が含まれます。

AWS Control Tower が、アジアパシフィック (ニュージーランド) リージョンで利用可能に

2025 年 10 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が、アジアパシフィック (ニュージーランド) リージョンで利用可能になりました。

AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン別のサービス表](#)」を参照してください。

AWS Control Tower が自動アカウント登録をサポート

2025 年 10 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower ランディングゾーンバージョン 3.1 以降を運用しているお客様は、AWS Control Tower で OU にアカウントを自動登録できるようになりました。アカウントの自動登録をオプトインすると、AWS Control Tower は、OU の有効なベースラインリソースとコントロールを新しい OU に移動するときにアカウントに適用します。前の OU のコントロールとベースラインは削除されます。ほとんどの場合、このアクションによってドリフトは作成されません。

自動登録を有効にするには: AWS Control Tower コンソールのランディングゾーンの [設定] ページでアカウントの自動登録を選択するか、RemediationType パラメータの値を継承ドリフトに設定して AWS Control Tower CreateLandingZone または UpdateLandingZone API を呼び出します。

自動登録を適用するには: 設定ページでこのオプションを選択した後、AWS Organizations コンソール、API、AWS Organizations MoveAccount または AWS Control Tower コンソールを使用してアカウントを移動できます。

自動登録を使用してアカウントの登録を解除するには: 登録されている OU の外部にアカウントを移動すると、AWS Control Tower はデプロイされたすべてのベースラインとコントロールを自動的に削除します。

自動登録の詳細については、「[オプションでアカウントの自動登録を設定する](#)」を参照してください。

このリリースには、管理ポリシーと新しい管理ポリシーの更新も含まれています。[AWS ControlTowerServiceRolePolicy](#) を更新し、新しい [AWS ControlTowerIdentityCenterManagementPolicy](#) を追加しました。

AWS Control Tower CreateLandingZone と UpdateLandingZone API を更新して、Inheritance Drift という名前の新しい RemediationType を追加しました。

AWS Control Tower が Python バージョンを更新

2025 年 9 月 3 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

Python のバージョン 3.9 は非推奨です。AWS Control Tower は、AWS Control Tower 環境で Python のバージョンを更新しました。アクションは必要なく、この更新は既存のワークロードに影響しません。

AWS Control Tower がドリフトを低減

2025 年 8 月 20 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、サービスコントロールポリシードリフトの機能を更新しました。このリリースでは、2 種類のガバナンスドリフトが AWS Control Tower によって直接処理され、環境でドリフトが発生しなくなりました。

2 種類のガバナンスドリフトが削除

- マネージド OU にアタッチされた SCP - このタイプのドリフトは、コントロールの SCP が他の OU にアタッチされたときに発生しました。AWS Control Tower コンソールの外部から OU を更新したときに発生するのが特に一般的です。
- メンバーアカウントにアタッチされた SCP - このタイプのドリフトは、コントロールの SCP が AWS Control Tower コンソールの外部からアカウントにアタッチされたときによく発生します。

ドリフトの詳細については、「[Detect and resolve drift in AWS Control Tower](#)」(AWS Control Tower でドリフトを検出して解決する)を参照してください。

AWS Control Tower が IPv6 アドレスをサポート

2025 年 8 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower API は、新しいデュアルスタックエンドポイントを通じてインターネットプロトコルバージョン 6 (IPv6) アドレスをサポートするようになりました。IPv4 をサポートする既存のエンドポイントは、下位互換性のために引き続き利用可能です。新しいデュアルスタックドメインは、[インターネットから](#)、または [AWS PrivateLink](#) を使用した [Amazon 仮想プライベートクラウド \(VPC\) 内から](#) 使用できます。

Account Factory for Terraform バージョン 1.15.0 が利用可能に

2025 年 7 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower Account Factory for Terraform (AFT) のバージョン 1.15.0 が利用可能になりました。詳細については、「[AFT GitHub リポジトリ](#)」を参照してください。

Nitro インスタンスタイプでコントロールを更新

2025 年 7 月 24 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、Amazon EC2 インスタンスタイプを実施する Control Catalog (以前は Control Library と呼ばれていました) の 8 つのプロアクティブコントロールを更新しました。この更新により、いくつかの新しい Nitro インスタンスタイプをインスタンス化し、非推奨の u-series インスタンスタイプを削除できます。

更新されたコントロール

- [CT.AUTOSCALING.PR.10](#)
- [CT.AUTOSCALING.PR.11](#)
- [CT.EC2.PR.15](#)
- [CT.EC2.PR.16](#)
- [CT.EC2.PR.17](#)
- [CT.EC2.PR.18](#)
- [CT.EC2.PR.19](#)
- [CT.EC2.PR.20](#)

新しいインスタンスタイプが利用可能に

- c8gd
- c8gn
- i7i
- m8gd
- p6-b200
- r8gd

削除されたインスタンスタイプ

- u-12tb1
- u-18tb1
- u-24tb1
- u-9tb1

更新されたコントロールは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能なリージョンのリストについては、「[AWS リージョンの表](#)」を参照してください。

AWS Control Tower がアジアパシフィック (台北) リージョンで利用可能に

2025 年 7 月 23 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower がアジアパシフィック (台北) リージョンで利用可能になりました。

AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン別のサービス表](#)」を参照してください。

AWS Control Tower が PrivateLink をサポート

2025 年 6 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が [AWS PrivateLink](#) をサポートするようになりました。パブリックインターネットを経由することなく、Amazon Virtual Private Cloud (VPC) 内から AWS Control Tower および Control Catalog APIs を呼び出すことができます。AWS PrivateLink は、仮想プライベートクラウド (VPCs)、サポートされているサービスとリソース、オンプレミスネットワーク間のプライベート接続を提供します。AWS Control Tower AWS PrivateLink のサポートは、AWS Control Tower が利用可能なすべての AWS リージョン で利用できます。

追加の業界フレームワークのサポート、メタデータの更新

2025 年 6 月 12 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

このリリースで、AWS Control Tower が 10 の業界フレームワークのサポートを含むように拡張されました。フレームワークのリストについては、「[サポートされるフレームワーク](#)」を参照してください。

例えば、初めに AWS Control Tower コンソールの [Control Catalog] ページに移動し、PCI-DSS-v4.0 などのフレームワークを検索して、そのフレームワークに関連するすべてのコントロールを表示できます。または、新しい [ListControlMappings](#) API を呼び出して、プログラムを使用してコントロールとフレームワークを調べることができます。

コントロールに関連するメタデータ定義は、これらの追加の業界フレームワークのサポートを向上させるために変更されています。メタデータの変更は、有効化のコントロールを評価する方法に影響を与える可能性があります。例えば、NIST、PCI、CIS メタデータの値が変更されることがあります。コンソールの [コントロールの詳細] ページで、有効なコントロールのマッピングを確認することをお勧めします。

コンソールと API で、3 つの新しいメタデータフィールドが導入されました。まとめると、これらのフィールドは、コントロールを分類して有効化する方法を理解するのに役立つ階層を記述します。フィールドは、ドメイン、目的、[一般的なコントロール](#)です。利用可能な幅広い業界フレームワークに合わせて[コントロールの目的](#)を再定義しました。この階層の詳細については、「[オントロジーの該当](#)」を参照してください。

- これらのメタデータの変更は AWS Control Tower コンソールに反映され、コンソールのエクスペリエンスは AWS Control Tower と AWS Config コンソール全体で一貫しています。
- AWS Control Tower コンソールでコントロール情報を表示するには、IAM ポリシーに `controlcatalog` のアクセス許可を追加する必要があります。詳細については、「[Permissions required to use the AWS Control Tower console](#)」(AWS Control Tower コンソールを使用するために必要なアクセス許可) を参照してください。
- 各コントロールに、コントロールが管理するリソースタイプを示す `GovernedResources` という新しいフィールドが追加されました。場合によっては、このフィールドにリソースのサービスプレフィックスが表示され、他のインスタンスでは空白になることがあります。詳細については、「[GetControl](#)」および「[ListControls](#)」を参照してください。

このリリースでは、他の用語との整合性のため、コントロールライブラリという名前を Control Catalog に変更しました。

サービスにリンクされた AWS Config コントロール

2025 年 6 月 12 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、サービスにリンクされた AWS Config ルールとしてデプロイされる AWS Control Tower 検出コントロールのサポートを発表しました。

このリリースでは、AWS Control Tower がサービスにリンクされた Config ルールを登録済みアカウントに直接デプロイし、以前のデプロイ方法を AWS CloudFormation スタックセットに置き換えるようになりました。この変更により、デプロイの速度が大幅に向上します。また、これらのサービスにリンクされた Config ルールは、CloudFormation スタックセットまたは Config ルールの手動変更によって発生する可能性のある意図しない設定ドリフトを防ぐため、リソースの一貫したガバナンスを確保するのに役立ちます。

今後、AWS Config ルールによって実装されるすべての AWS Control Tower コントロールは、AWS Config APIs を直接呼び出すこのメカニズムでデプロイされます。

Important

サービスにリンクされた Config ルールを採用する前に、AWS Control Tower の外部の Config ルールに行った修復などの既存のカスタマイズを確認してください。これらのカスタマイズは移行中に削除されます。AWS Config APIs サービスにリンクされた AWS Config ルールの修正設定の追加をサポートしていません。
「[PutRemediationConfigurations](#)」を参照してください。

詳細と必要なアクション

- ランディングゾーンを更新またはリセットすると、AWS Control Tower はセキュリティ OU を管理する必須コントロールを更新します。アップグレードを完了するには、AWS Config ルールで実装されている各検出コントロールをリセットするか、OU を再登録する必要があります。
- このアップグレードの全範囲は、AWS Control Tower ランディングゾーンのバージョンが 3.2 以降の場合に適用されます。この更新を適用すると、既存の AWS Config ルールが新しいデプロイ方法とともにサービスマネージド Config ルールに変更されます。
- ランディングゾーンがバージョン 3.1 以下の場合、新しい Config ルールは新しいメソッドでデプロイされ、スタックセットではデプロイされなくなります。既存の Config ルールは、サービスマネージド Config ルールに更新されません。標準タイプのままになります。
- サービスにリンクされた設定ルールは、以下の形式のようなリソース ARN で識別できます。

```
arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*
```


サービスにリンクされた AWS Config ルールによって実装されたコントロールの意図した機能は変更されていません。AWS Control Tower の検出サービスにリンクされた Config ルールは、ポリシー違反など、アカウント内の非準拠リソースを識別し、ダッシュボードを介してアラートを提供できます。一貫性を維持し、設定ドリフトを防ぎ、全体的なユーザーエクスペリエンスを簡略化するために、これらのルールは AWS Control Tower を介してのみ変更できるようになりました。

このリリースの一環として、サービスにリンクされたロール (SLR) のポリシーに 4 つの新しいアクセス許可が追加されました。これにより[AWSServiceRoleForAWSControlTower](#)、登録されたアカウントのサービスにリンクされた AWS Config ルールを有効または無効にできます。

```
config:DescribeConfigRules
config:TagResource
config:PutConfigRule
config>DeleteConfigRule
```

有効なコントロールコンソールビューによる一元的な可視性

2025 年 5 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、有効なすべてのコントロールを 1 つの一元化されたビューに表示する新しいページをコンソールに追加しました。以前は、コントロールはそのアカウントまたは有効化された OU でのみ表示できました。統合ビューを使用すると、コントロールガバナンスのギャップを簡単に大規模に特定できます。

[有効なコントロール] ページで、予防、検出、またはプロアクティブの動作に従ってコントロールをフィルタリングできます。SCP などのコントロール実装に従ってフィルタリングすることもできます。コントロールごとに、このコントロールが有効になっている OU の数を確認できます。

[有効なコントロール] ページを表示するには、AWS Control Tower コンソールの [コントロール] セクションに移動します。

Account Factory for Terraform (AFT) がデプロイ時に新しい設定をサポート

2025 年 5 月 13 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower アカウントカスタマイズフレームワークである Account Factory for Terraform (AFT) は、デプロイ時に 3 つの追加のオプション設定をサポートするようになりました。AFT をカスタム仮想プライベートクラウド (VPC) にデプロイし、AFT デプロイの Terraform プロジェクト名を指定し、AFT が作成するリソースにタグ付けすることができます。

詳細については、「[AWS Control Tower Account Factory for Terraform \(AFT\) のデプロイ](#)」を参照してください。

AWS Control Tower がベースライン API のアカウントレベルのレポートを導入

2025 年 5 月 12 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

ベースライン API を呼び出すことで、管理対象アカウントのドリフトとアカウント登録ステータスをプログラムで表示できるようになりました。この機能を使用すると、アカウントと OU のベースライン設定がいつドリフトするか、または同期しなくなるかを特定できます。プログラムでドリフトステータスを表示するには、有効なベースラインに [ListEnabledBaselines](#) API を呼び出します。ListEnabledBaselines API を使用して個々のアカウントのステータスをプログラムで表示するには、includeChildren フラグを使用します。これらのステータスでフィルタリングし、注意が必要なアカウントと OU のみを表示できます。

[AWS ControlTowerBaseline](#) は、ガバナンスに必要なベストプラクティスの設定、コントロール、リソースを設定します。組織単位 (OU) でこのベースラインを有効化すると、OU 内のメンバーアカウントは自動的に AWS Control Tower に登録されます。AWS Control Tower ベースライン APIs には CloudFormation サポートが含まれており、Infrastructure as Code (IaC) を使用して OUs とアカウントを管理するオートメーションを構築できます。

これらの API の詳細については、「AWS Control Tower ユーザーガイド」の「[Baselines](#)」を確認してください。ドリフトとアカウント登録ステータスのベースライン APIs と新しく起動されたレポート機能は、AWS Control Tower が利用可能なすべての AWS リージョンで使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS アジアパシフィック (タイ) およびメキシコ (中部) リージョンで利用可能な AWS Control Tower

2025 年 5 月 9 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が次の AWS リージョンで利用可能になりました。

- アジアパシフィック (タイ)
- メキシコ (中部)

AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン別のサービス表](#)」を参照してください。

利用可能な追加の AWS Config コントロール

2025 年 4 月 11 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、セキュリティ、コスト、耐久性、オペレーションなど、さまざまなユースケースで 223 のマネージド AWS Config ルールを追加でサポートするようになりました。この起動により、AWS Control Tower を使用して、マルチアカウント環境を管理するために必要な AWS Config ルールを検索して検出し、AWS Control Tower から直接コントロールを有効にして管理できるようになりました。

AWS Control Tower コンソールから開始するには、Control Catalog に移動し、実装フィルター AWS Configを使用してコントロールを検索します。AWS Control Tower コンソールから直接コントロールを有効化できます。

詳細については、「[AWS Control Tower で利用可能な統合 AWS Config コントロール](#)」を参照してください。

このリリースにより、ListControls および GetControl API が更新され、CreateTime、Severity 度、Implementationの 3 つの新しいフィールドがサポートされるようになりました。これらは Control Catalog でコントロールを検索するときに使用できます。例えば、前回の評価後に作成された重要度の高い AWS Config ルールをプログラムで検索できるようになりました。

AWS Control Tower が利用可能なすべての AWS リージョン で新しい AWS Config ルールを検索できます。ルールをデプロイするには、そのルール AWS リージョン でサポートされている のリストを参照して、有効にできる場所を確認します。

OU のアクションの登録解除と削除

2025 年 4 月 8 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、OU の登録を解除し、OU を削除する別のコンソールアクションをサポートするようになりました。OU を削除する前に、登録を解除する必要があります。登録を解除することによって、AWS Control Tower から OU を削除できます。

詳細については、「[OU を削除する](#)」を参照してください。

Control Catalog が IPv6 アドレスをサポート

2025 年 4 月 2 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower Control Catalog API は、新しいデュアルスタックエンドポイントを通じてインターネットプロトコルバージョン 6 (IPv6) アドレスをサポートするようになりました。IPv4 をサポートする既存の Control Catalog エンドポイントは、下位互換性のために引き続き利用可能です。新しいデュアルスタックドメインは、[インターネットから](#)、または [AWS PrivateLink](#) を使用した [Amazon 仮想プライベートクラウド \(VPC\)](#) 内から使用できます。

2024 年 1 月 ~ 12 月

2024 年、AWS Control Tower は次の更新をリリースしました。

- [AWS Control Tower CfCT が GitHub と RCP をサポート](#)
- [AWS Control Tower に宣言型ポリシーを使用した予防コントロールを追加](#)
- [AWS Control Tower に規範バックアッププランオプションを追加](#)
- [AWS Control Tower は AWS Config コントロールを統合します](#)
- [AWS Control Tower でフック管理を改善し、プロアクティブコントロールリージョンを追加](#)
- [AWS Control Tower がマネージドリソースコントロールポリシーを起動](#)
- [AWS Control Tower によるコントロールポリシードリフトの報告](#)
- [新しい ResetEnabledControl API](#)
- [コントロールカタログの GetControl API の更新](#)
- [AWS Control Tower AFT が GitLab をサポート](#)

- [AWS アジアパシフィック \(マレーシア\) リージョンで AWS Control Tower が利用可能に](#)
- [AWS Control Tower が OU あたり最大 1000 アカウントをサポート](#)
- [AWS Control Tower でランディングゾーンバージョンの選択が可能に](#)
- [記述的なコントロール API が利用可能になり、リージョンとコントロールへのアクセスが拡大](#)
- [AWS Control Tower がオプトインリージョンで AFT と CfCT をサポート](#)
- [AWS Control Tower に ListLandingZoneOperations API を追加](#)
- [AWS Control Tower が最大 100 の同時コントロールオペレーションをサポート](#)
- [AWS Control Tower が AWS カナダ西部 \(カルガリー\) で利用可能に](#)
- [AWS Control Tower がセルフサービスのクォータ調整をサポート](#)
- [AWS Control Tower の「Controls Reference Guide」をリリース](#)
- [AWS Control Tower で 2 つのプロアクティブコントロールを更新し、名前を変更](#)
- [非推奨のコントロールが使用不可に](#)
- [AWS Control Tower が CloudFormation の EnabledControl リソースのタグ付けをサポート](#)
- [AWS Control Tower がベースラインを使用した OU 登録と設定用の API をサポート](#)

AWS Control Tower CfCT が GitHub と RCP をサポート

2024 年 12 月 9 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、サードパーティーのバージョン管理システム (VCS) のオプションとして GitHub™ をサポートし、AWS Control Tower のカスタマイズ (CFCT) の設定ソースをサポートするようになりました。詳細については、「[GitHub を設定ソースとしてセットアップする](#)」を参照してください。

AWS Control Tower は、AWS Control Tower のカスタマイズ (CFCT) のリソースコントロールポリシー (RCP) をサポートするようになりました。詳細については、「[CfCT カスタマイズガイド](#)」を参照してください。

AWS Control Tower に宣言型ポリシーを使用した予防コントロールを追加

2024 年 12 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、宣言ポリシーによって実装される予防コントロールをサポートするようになりました。宣言型ポリシーは、サービスレベルで直接適用されます。このアプローチにより、サービスによって新機能や API が導入された場合でも、指定された設定が適用されます。詳細については、「[宣言型ポリシーを使用して実装されるコントロール](#)」を参照してください。

AWS Control Tower に規範バックアッププランオプションを追加

2024 年 11 月 25 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、データのバックアップと復旧ワークフローをランディングゾーンに直接組み込める規範的な AWS Backup プランをサポートするようになりました。バックアッププランには、保持日数、バックアップの頻度、バックアップが発生する時間枠などの事前定義済みのルールが含まれます。これらのルールは、管理対象メンバーアカウント全体で AWS リソースをバックアップする方法を定義します。ランディングゾーンにバックアッププランを適用すると、AWS Control Tower は、プランがすべてのメンバーアカウントで一貫しており、AWS Backup からのベストプラクティスの推奨事項と一致していることを確認します。

詳細については、「[AWS Backup と AWS Control Tower](#)」を参照してください。

AWS Control Tower は AWS Config コントロールを統合します

2024 年 11 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は選択した AWS Config コントロールを統合しているため、AWS Control Tower で表示および管理できます。

詳細については、「[AWS Control Tower で使用可能な、統合された AWS Config コントロール](#)」を参照してください。

AWS Control Tower でフック管理を改善し、プロアクティブコントロールリージョンを追加

2024 年 11 月 20 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

このリリースでは、AWS Control Tower による制限なしに、CloudFormation フックの全容量を利用できます。また、プロアクティブコントロールは、カナダ西部 (カルガリー) リージョンとアジアパシフィック (マレーシア) リージョンでも利用可能です。

以前は、AWS Control Tower のみを変更できるように、環境内のすべての CloudFormation フックを CT.CLOUDFORMATION.PR.1 コントロールで保護する必要がありました。このリリースでは、AWS Control Tower サービスで以前必要だった制限なしに、CloudFormation フックをデプロイし、これらのフックを変更できます。

現在、プロアクティブコントロールをデプロイしている場合は、この改善されたフック機能に移行できます。OU のすべてのプロアクティブコントロールをリセットするには、その OU でアクティブな 1 つのプロアクティブコントロールをリセットします。リセットは、ResetEnabledControl API を呼び出すか、コンソールからコントロールを更新し、リセット機能を使用して実行できます。プロアクティブコントロールにこのリセットタスクを完了すると、AWS Control Tower は OU のすべてのプロアクティブコントロールフックを新しい機能に移行します。プロアクティブコントロールをデプロイする OU ごとにこのプロセスを繰り返します。

プロアクティブコントロールをリセットした後、別の目的でコントロールを有効化していない限り、AWS Control Tower OU の CT.CLOUDFORMATION.PR.1 コントロールを削除します。CT.CLOUDFORMATION.PR.1 コントロールをオフにしない場合、他の CloudFormation フックを作成および変更することはできません。

詳細については、「[プロアクティブコントロールのフックを更新する](#)」を参照してください。

AWS Control Tower がマネージドリソースコントロールポリシーを起動

2024 年 11 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、リソースコントロールポリシー (RCP) で実装された新しいタイプの予防コントロールを提供します。これらのコントロールは、AWS Control Tower 環境全体でデータ境界を確立し、意図しないアクセスからリソースを保護するのに役立ちます。

例えば、Amazon S3、Amazon SQS AWS Security Token Service AWS Key Management Service、および AWS Secrets Manager サービスの RCP ベースのコントロールを有効にできます。RCP ベースのコントロールは、個々のバケットポリシーに付与されたアクセス許可に関係なく、「組織の Amazon S3 リソースが組織に属する IAM プリンシパルまたは AWS サービスによってのみアクセス可能であることを要求」などの要件を適用できます。

新しい RCP ベースのコントロールと特定の既存の SCP ベースの予防コントロールを設定して、プリンシパルとリソースの AWS IAM 免除を指定できます。プリンシパルまたはリソースをコントロールによって管理しない場合、免除を設定できます。

AWS Control Tower で予防コントロール、プロアクティブコントロール、検出コントロールを組み合わせることで、マルチアカウント AWS 環境が [AWS](#)、[Foundational Security Best Practices 標準](#)などのベストプラクティスに従って安全で管理されているかどうかをモニタリングできます。

これらの新しい RCP ベースの予防コントロールは、AWS Control Tower AWS リージョン が利用可能な で利用できます。AWS Control Tower が利用可能な AWS リージョン の完全なリストについては、表を参照してください [AWS リージョン](#)。

AWS Control Tower によるコントロールポリシードリフトの報告

2024 年 11 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、リソースコントロールポリシー (RCPs) で実装されたコントロール、および Security Hub CSPM サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールについて、コントロールポリシーのドリフトを報告するようになりました。このタイプのドリフトは、新しい `ResetEnabledControl` API を通じて修正できます。詳細については、「[Types of governance drift](#)」を参照してください。

新しい `ResetEnabledControl` API

2024 年 11 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、コントロールドリフトをプログラムで管理するのに役立つ新しい API を発表しました。コントロールドリフトを修復し、意図した設定にコントロールをリセットできます。`ResetEnabledControl` API は、強く推奨されるコントロールや選択的コントロールを含め、オプションの AWS Control Tower コントロールを操作します。

コントロールの例外

- サービスコントロールポリシーで実装されているコントロールは、この API ではリセットできません。詳細については、「[ResetEnabledControl](#)」を参照してください。
- 必須コントロールは AWS Control Tower リソースを保護するため、リセットできません。

- ランディングゾーンのリージョン拒否コントロールは、コンソールからリセットする必要があります。

コントロールドリフトは、AWS Control Tower コントロールが AWS Organizations コンソールなどから AWS Control Tower の外部で変更されたときに発生します。ドリフトを解決することで、ガバナンス要件のコンプライアンスを確保できます。

コントロールカタログの **GetControl** API の更新

2024 年 11 月 8 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、すべてのコントロールの Implementation タイプと設定可能な特定のコントロール Parameters の 2 つの新しいフィールドを含む、更新された GetControl API をサポートするようになりました。

GetControl API は AWS Control Tower の controlcatalog 名前空間の一部です。

詳細については、「Control Catalog API リファレンス」の「[GetControl API](#)」を参照してください。

このリリースには、AWS Control Tower コンソールに表示される関連した変更が含まれています。

- 既存のコントロールはすべて AWS Security Hub CSPM Implementation、パラメータ値を AWS Config ルールからに変更します AWS Security Hub CSPM。対応するコンソールのヘルプパネルが、この変更を反映するように修正されています。
- 既存のフックコントロールはすべて Implementation、パラメータ値を CloudFormation ガードルールから CloudFormation フックに変更します。対応するコンソールのヘルプパネルが、この変更を反映するように修正されています。

AWS Control Tower AFT が GitLab をサポート

2024 年 10 月 23 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、Account Factory for Terraform (AFT) のサードパーティーバージョン管理システム (VCS) と設定ソースのオプションとして、GitLab™ と GitLab セルフマネージドをサポートするようになりました。

AWS アジアパシフィック (マレーシア) リージョンで AWS Control Tower が利用可能に

2024 年 10 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が AWS のアジアパシフィック (マレーシア) リージョンで利用可能になりました。

AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン別のサービス表](#)」を参照してください。

AWS Control Tower が OU あたり最大 1000 アカountをサポート

2024 年 8 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、組織単位 (OU) あたりの最大許容アカウント数が 300 から 1000 に引き上げられました。これで、OU 構造を変更することなく、一度に最大 1000 AWS アカount を AWS Control Tower ガバナンスに登録できます。OU の登録プロセスと再登録プロセスも効率化されたため、AWS Control Tower ベースラインリソースをアカウントにデプロイする際の所要時間が大幅に短縮されます。

利用可能な CloudFormation スタックセットの数に制限があるため、一部のアカウントの制限が引き続き適用されます。具体的には、OU に登録できるアカウントの最大数は、管理下に置いているリージョンの数によって変わることがあります。詳細については、[AWS Control Tower ユーザーガイドの基盤となる AWS サービスに基づく制限](#)を参照してください。AWS Control Tower を使用できる AWS リージョン の完全なリストについては、「[AWS リージョン 別のサービス表](#)」を参照してください。

AWS Control Tower でランディングゾーンバージョンの選択が可能に

2024 年 8 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower ランディングゾーンバージョン 3.1 以降を実行している場合は、現在のバージョンのままでランディングゾーンを更新または修復することも、選択したバージョンにアップグ

レードすることもできます。これまで、ランディングゾーンを更新または修復するには、最新のランディングゾーンバージョンにアップグレードする必要がありました。

ランディングゾーンバージョンを選択することで、環境に加えられる可能性のある変更を評価しながら、バージョンのアップグレードをより柔軟に計画できます。ドリフトを修復してコンプライアンスを維持するか、ランディングゾーン設定を更新するか、最新のランディングゾーンバージョンにアップグレードするかを選択する必要はありません。ランディングゾーンバージョン 3.1 以降を実行している場合は、ランディングゾーン設定を更新またはリセットするときに、現在のバージョンを維持するか、新しいバージョンにアップグレードするかを選択できます。

記述的なコントロール API が利用可能になり、リージョンとコントロールへのアクセスが拡大

2024 年 8 月 6 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、利用可能なコントロールの詳細情報をプログラムで確認するのに役立つ新しい API オペレーションが 2 つ追加されました。この機能により、自動化を使用したコントロールのデプロイが容易になります。

- [GetControl](#) API は、ターゲット識別子、コントロール情報の概要、ターゲットリージョンのリスト、ドリフトステータスなど、有効なコントロールの詳細を返します。
- [ListControls](#) API は、AWS Control Tower のコントロールライブラリで使用可能なすべてのコントロールのページ分割されたリストを返します。

これらの API には、[AWS Control Catalog 名前空間](#)を介してアクセスします。AWS Control Catalog は AWS Control Tower の一部であり、AWS Control Tower だけでなく、他の AWS のサービスの管理に役立つコントロールが含まれています。この拡張カタログは、複数の AWS サービスのコントロールを統合するため、セキュリティ、コスト、耐久性、オペレーションなどの一般的なユースケースに従って AWS コントロールを表示できます。詳細については、「[Control Catalog API Reference](#)」を参照してください。

リージョンの可用性の拡大

このリリース以降、AWS Control Tower ガバナンスを、(既に) 有効になっているコントロールの一部が利用できない AWS リージョン に拡張できます。また、管理対象リージョンの一部でコントロールがサポートされていない場合でも、より多くのリージョンで特定のコントロールを有効にできるようになりました。

これまで、AWS Control Tower では、有効なコントロールと管理対象リージョンのすべてで一貫性が維持されていなければ、ガバナンスをリージョンに拡張したり、コントロールを有効にしたりすることはできませんでした。このリリースでは、すべての有効なコントロールとすべての管理対象リージョンに対して設定が正しいことをより柔軟に責任を持って確認できます。[AWS Control Tower コントロール APIs](#) と [コントロールカタログ APIs](#) は、有効なコントロールで保護されている AWS リージョンと、追加のコントロールをデプロイできるリージョンに関する情報を取得するのに役立ちます。リージョンとコントロールの情報は、AWS Control Tower コンソールでも確認できます。

AWS Control Tower がオプトインリージョンで AFT と CfCT をサポート

2024 年 7 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

現在、AWS Control Tower カスタマイズフレームワーク Account Factory for Terraform (AFT) と Customizations for AWS Control Tower (CfCT) は、AWS リージョンアジアパシフィック (ハイデラバード、ジャカルタ、大阪)、イスラエル (テルアビブ)、中東 (アラブ首長国連邦) の 5 つの追加で利用できます。

Account Factory for Terraform (AFT) は、AWS Control Tower でアカウントのプロビジョニングとカスタマイズに役立つ Terraform パイプラインを設定します。AWS Control Tower (CfCT) のカスタマイズは、CloudFormation テンプレートとサービスコントロールポリシー (SCPs) を使用して AWS Control Tower ランディングゾーンとアカウントをカスタマイズするのに役立ちます。

詳細については、「AWS Control Tower User Guide」の Account Factory for Terraform と AWS Control Tower のカスタマイズのページを参照してください。AFT の GitHub ページと CfCT の GitHub ページでリリースノートを確認することもできます。AFT と CfCT は、一部の例外を除き、すべての AWS リージョンでサポートされています。詳細については、「[Region limitations](#)」を参照してください。

AWS Control Tower に ListLandingZoneOperations API を追加

2024 年 6 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、ランディングゾーンに最近適用されたオペレーションと現在進行中のオペレーションのリストを取得できる API が追加されました。この API は、最大で 90 日分のランディングゾーンオペレーションとその識別子の履歴を返すことができます。使用例については、「[View the status of your landing zone operations](#)」を参照してください。

ListLandingZoneOperations API の詳細については、「AWS Control Tower API Reference」の「[ListLandingZoneOperations](#)」を参照してください。

AWS Control Tower が最大 100 の同時コントロールオペレーションをサポート

2024 年 5 月 20 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が同時実行性の高い複数のコントロールオペレーションをサポートするようになりました。コンソールから、または API を使用して、複数の組織単位 (OU) にわたって最大 100 の AWS Control Tower コントロールオペレーションを同時に送信できます。最大 10 のオペレーションを同時に実行でき、追加のオペレーションはキューに入れられます。このようにして、反復的な制御操作の運用上の負担をかけずに AWS アカウント、複数の にまたがってより標準化された設定をセットアップできます。

進行中のコントロールオペレーションとキューに入れられたコントロールオペレーションのステータスをモニタリングするには、AWS Control Tower コンソールの新しい [最近の業務] ページに移動するか、新しい [ListControlOperations](#) API を呼び出します。

AWS Control Tower ライブラリには 500 を超えるコントロールが含まれており、さまざまなコントロールの目標、フレームワーク、サービスに対応しています。[保管中のデータを暗号化] などの特定のコントロールの目標については、1 つのコントロールオペレーションで複数のコントロールを有効にして、目標を達成できます。この機能により、開発スピードの向上、ベストプラクティスコントロールの導入の迅速化、運用の複雑さの軽減が可能になります。

AWS Control Tower が AWS カナダ西部 (カルガリー) で利用可能に

2024 年 5 月 3 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

本日より、カナダ西部 (カルガリー) リージョンで AWS Control Tower をアクティブ化できます。既に AWS Control Tower をデプロイしている場合に、ガバナンス機能をこのリージョンに拡張するには、AWS Control Tower [ランディングゾーン API](#) を使用します。または、コンソールから AWS Control Tower ダッシュボードの [設定] ページに移動し、リージョンを選択して、ランディングゾーンを更新します。

カナダ西部 (カルガリー) リージョンは AWS Service Catalog をサポートしていません。このため、AWS Control Tower の一部の機能が異なります。機能の変更点として最も顕著なのは、Account

Factory が利用できないことです。ホームリージョンとしてカナダ西部 (カルガリー) を選択した場合、アカウントの更新、アカウントのオートメーションの設定、および Service Catalog が関係するその他のプロセスが他のリージョンと異なります。

アカウントのプロビジョニング

カナダ西部 (カルガリー) リージョンで新しいアカウントを作成してプロビジョニングする場合は、AWS Control Tower の外部でアカウントを作成し、登録済みの OU に登録することをお勧めします。詳細については、「[Enroll an existing account](#)」と「[Steps to enroll an account](#)」を参照してください。

Service Catalog API は、カナダ西部 (カルガリー) リージョンでは利用できません。「[Automate account provisioning in AWS Control Tower by Service Catalog APIs](#)」に示されているスクリプトの例は機能しません。

Account Factory Customizations (AFC)、Account Factory for Terraform (AFT)、および AWS Control Tower のカスタマイズ (CfCT) は、AWS Control Tower の基盤となる他の依存関係がないため、カナダ西部 (カルガリー) では利用できません。ガバナンスをカナダ西部 (カルガリー) リージョンに拡張する場合、Service Catalog がホームリージョンで利用できる限り、AWS Control Tower がサポートするすべてのリージョンで AFC ブループリントを引き続き管理できます。

コントロール

AWS Security Hub CSPM サービスマネージドスタンダード: AWS Control Tower のプロアクティブコントロールとコントロールは、カナダ西部 (カルガリー) リージョンでは利用できません。予防コントロール CT.CLOUDFORMATION.PR.1 は、フックベースのプロアクティブコントロールのアクティブ化にのみ必要であるため、カナダ西部 (カルガリー) では利用できません。に基づく特定の検出コントロール AWS Config は使用できません。詳細については、「[コントロールの制限事項](#)」を参照してください。

ID プロバイダー

IAM アイデンティティセンターは、カナダ西部 (カルガリー) では利用できません。推奨されるベストプラクティスは、IAM アイデンティティセンターが利用可能なリージョンでランディングゾーンをセットアップすることです。または、カナダ西部 (カルガリー) で外部 ID プロバイダーを使用する場合、アカウントのアクセス設定を自己管理することもできます。

カナダ西部 (カルガリー) リージョンで Service Catalog を使用できない場合でも、AWS Control Tower でサポートされている他のリージョンには影響しません。これらの違いは、ホームリージョンがカナダ西部 (カルガリー) である場合にのみ適用されます。

AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン別のサービス表](#)」を参照してください。

AWS Control Tower がセルフサービスのクォータ調整をサポート

2024 年 4 月 25 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が Service Quotas コンソールを通じてセルフサービスのクォータ調整をサポートするようになりました。詳細については、「[クォータ引き上げをリクエストする](#)」を参照してください。

AWS Control Tower の「Controls Reference Guide」をリリース

2024 年 4 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower の「Controls Reference Guide」がリリースされました。これは、AWS Control Tower 環境に固有のコントロールに関する詳細情報が記載された新しいドキュメントです。これまで、この資料は「AWS Control Tower User Guide」に含まれていました。「Controls Reference Guide」では、コントロールについて拡張形式で説明しています。詳細については、「[AWS Control Tower Controls Reference Guide](#)」を参照してください。

AWS Control Tower で 2 つのプロアクティブコントロールを更新し、名前を変更

2024 年 3 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、Amazon OpenSearch Service の更新に合わせて 2 つのプロアクティブコントロールの名前が変更されました。

- [\[CT.OPENSEARCH.PR.8\] TLSv1.2 を使用するには Elasticsearch Service ドメインが必要です](#)
- [\[CT.OPENSEARCH.PR.16\] TLSv1.2 を使用するには Amazon OpenSearch Service ドメインが必要です](#)

Amazon OpenSearch Service の最近のリリースに合わせて、この 2 つのコントロールのコントロール名とアーティファクトを更新しました。Amazon OpenSearch Service では、ドメインエンドポ

イントのセキュリティ用のトランスポートセキュリティオプションとして [Transport Layer Security \(TLS\) バージョン 1.3](#) がサポートされるようになっていきます。

これらのコントロールでの TLSv1.3 のサポートを追加するために、コントロールのアーティファクトと名前を更新して、コントロールの意図を反映させました。サービストメインの最小 TLS バージョンが評価されるようになりました。ご使用の環境でこの更新を行うには、コントロールを [無効] にしてから [有効] にして、最新のアーティファクトをデプロイする必要があります。

この変更の影響を受けるその他のプロアクティブコントロールはありません。これらのコントロールを確認して、コントロールの目標が確実に達成されるようにすることをお勧めします。

ご質問やご不明な点がある場合は、[AWS サポート](#)にお問い合わせください。

非推奨のコントロールが使用不可に

2024 年 3 月 12 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower でいくつかのコントロールが廃止されました。これらのコントロールは使用できなくなりました。

- 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 が での **EnabledControl** リソースのタグ付けをサポート CloudFormation

2024 年 2 月 22 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

この AWS Control Tower リリースでは、EnabledControl リソースの動作を更新することで、設定可能なコントロールとの連携を強化するとともに、AWS Control Tower 環境をオートメーションによって管理する機能を向上させています。このリリースでは、CloudFormation テンプレートを使用して設定可能な EnabledControl リソースにタグを追加できます。これまで、タグを追加できたのは AWS Control Tower コンソールと API を使用する場合のみでした。

AWS Control Tower の GetEnabledControl、EnableControl、ListTagsForResource API オペレーションは、EnabledControl リソースの機能を利用しているため、このリリースで更新されます。

詳細については、「[Tagging EnabledControl resources in AWS Control Tower](#)」と「CloudFormation User Guide」の「[EnabledControl](#)」を参照してください。

AWS Control Tower がベースラインを使用した OU 登録と設定用の API をサポート

2024 年 2 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

これらの API は、EnableBaseline の呼び出しを使用したプログラムによる OU 登録をサポートします。OU でベースラインを有効にすると、OU 内のメンバーアカウントが AWS Control Tower ガバナンスに登録されます。特定の注意事項が適用される場合があります。例えば、AWS Control Tower コンソールを介して OU を登録すると、オプションのコントロールと必須のコントロールが有効になります。API を呼び出す際には、オプションのコントロールが有効になるように追加のステップを実行する必要が生じる場合があります。

AWS Control Tower ベースラインとは、OU とメンバーアカウントの AWS Control Tower ガバナンスのベストプラクティスを具体化したものです。たとえば、OU でベースラインを有効にすると、OU 内のメンバーアカウントは、AWS CloudTrail、IAM Identity Center AWS Config、必要な IAM AWS ロールなど、定義されたリソースグループを受け取ります。

特定のベースラインは、特定の AWS Control Tower ランディングゾーンバージョンと互換性があります。ランディングゾーン設定を変更する際、AWS Control Tower は互換性のある最新のベースラインをランディングゾーンに適用できます。詳細については、「[OU ベースラインとランディングゾーンバージョンの互換性](#)」を参照してください。

このリリースには、基本的な[ベースラインのタイプ](#)が 4 つ含まれています

- AWSControlTowerBaseline

- AuditBaseline
- LogArchiveBaseline
- IdentityCenterBaseline

新しい API と定義済みのベースラインを使用すると、OU を登録して、OU のプロビジョニングワークフローを自動化できます。API では、既に AWS Control Tower のガバナンス下にある OU の管理も行えるため、ランディングゾーンの更新後に OU を再登録できます。APIs には CloudFormation EnabledBaseline リソースのサポートが含まれており、Infrastructure as Code (IaC) を使用して OUs を管理できます。

ベースライン API

- EnableBaseline、UpdateEnabledBaseline、DisableBaseline: OU のベースラインに対してアクションを実行します。
- GetEnabledBaseline、ListEnabledBaselines: 有効なベースラインの設定を検出します。
- GetBaselineOperation: 特定のベースラインオペレーションのステータスを表示します。
- ResetEnabledBaseline: ベースラインが有効になっている OU のリソースドリフト (ネストされた OU と必須コントロールのドリフトを含む) を修正します。ランディングゾーンレベルのリージョン拒否コントロールのドリフトも修正します。
- GetBaseline、ListBaselines: AWS Control Tower ベースラインの内容を検出します。

これらの API の詳細については、「AWS Control Tower User Guide」の「[Baselines](#)」と「[API Reference](#)」を参照してください。新しい APIs は、GovCloud (米国) リージョンを除き、AWS Control Tower が利用可能な AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、AWS リージョン 表を参照してください。

2023 年 1 月 ~ 12 月

2023 年、AWS Control Tower は次の更新をリリースしました。

- [新しい AWS Service Catalog 外部製品タイプへの移行 \(フェーズ 3\)](#)
- [AWS Control Tower ランディングゾーンバージョン 3.3](#)
- [新しい AWS Service Catalog 外部製品タイプへの移行 \(フェーズ 2\)](#)
- [AWS Control Tower がデジタル主権を支援するコントロールを発表](#)
- [AWS Control Tower ランディングゾーン API](#)

- [AWS Control Tower コントロールのタグ付け API](#)
- [AWS アジアパシフィック \(メルボルン\) で利用可能な AWS Control Tower](#)
- [新しい AWS Service Catalog 外部製品タイプへの移行 \(フェーズ 1\)](#)
- [AWS Control Tower で新しいコントロール API が追加されました](#)
- [AWS Control Tower で新しいコントロールが追加されました](#)
- [AWS Control Tower で信頼されるアクセスドリフトを検出する](#)
- [AWS Control Tower が 4 つの追加で利用可能に AWS リージョン](#)
- [AWS イスラエル \(テルアビブ\) で AWS Control Tower が利用可能に](#)
- [AWS Control Tower に 28 個の新しいプロアクティブコントロールを追加](#)
- [AWS Control Tower で 2 つのコントロールが廃止されます](#)
- [AWS Control Tower ランディングゾーンバージョン 3.2](#)
- [AWS Control Tower に IAM Identity Center の email-to-ID マッピングが追加されました](#)
- [AWS Control Tower が AWS Security Hub CSPM コントロールを追加](#)
- [AWS Control Tower が AWS Security Hub CSPM コントロールのメタデータを発行する](#)
- [AWS Control Tower に Terraform 用の Account Factory Customization \(AFC\) を追加](#)
- [AWS Control Tower にセルフマネージド IAM アイデンティティセンターを追加](#)
- [AWS Control Tower に 混合ガバナンスの注意事項を追加](#)
- [AWS Control Tower に新しいプロアクティブコントロールを追加](#)
- [AWS Control Tower で Amazon EC2 コントロールを更新する](#)
- [AWS Control Tower が 7 つの追加で利用可能に AWS リージョン](#)
- [AWS Control Tower Account Factory Customization \(AFC\) とリクエストトレースが一般利用可能](#)
- [AWS Control Tower ランディングゾーンバージョン 3.1](#)
- [AWS Control Tower プロアクティブコントロールが一般利用可能](#)

新しい AWS Service Catalog 外部製品タイプへの移行 (フェーズ 3)

2023 年 12 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、新規作成時に製品タイプ (ブループリント) として Terraform Open Source をサポートしなくなりました AWS アカウント。アカウントブループリントの更新の詳細と手順については、[AWS Service Catalog 「外部製品タイプへの移行」](#)を参照してください。

External 製品タイプを使用するようにアカウントブループリントを更新しない場合、Terraform オープンソースブループリントを使用してプロビジョニングしたアカウントの更新または終了のみが可能です。

AWS Control Tower ランディングゾーンバージョン 3.3

2023 年 12 月 14 日

(AWS Control Tower ランディングゾーンをバージョン 3.3 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください)。

AWS Control Tower 監査アカウントの S3 バケットポリシーの更新

AWS Control Tower がアカウントにデプロイする Amazon S3 監査バケットポリシーが変更されました。これにより、すべての書き込みアクセス許可のためには `aws:SourceOrgID` 条件を満たす必要があります。このリリースでは、リクエストが組織または組織単位 (OU) から送信された場合にのみ、AWS サービスはリソースにアクセスできます。

`aws:SourceOrgID` 条件キーを使用して、S3 バケットポリシーの条件要素で [組織 ID] の値を設定できます。この条件によってのみ、CloudTrail は組織内のアカウントに代わってお客様の S3 バケットへログを書き込めるようになり、組織外の CloudTrail ログによるお客様の AWS Control Tower S3 バケットへの書き込みを防ぎます。

この変更は、既存のワークロードの機能に影響を与えることなく、潜在的なセキュリティ上の脆弱性を修正するために行われました。更新されたポリシーを表示する方法については、「[監査アカウントの Amazon S3 バケットポリシー](#)」を参照してください。

新しい条件キーの詳細については、IAM ドキュメントと「リソースにアクセスする AWS サービスにスケーラブルなコントロールを使用する」というタイトルの IAM ブログ記事を参照してください。

SNS AWS Config トピックのポリシーの更新

AWS Config SNS のポリシーに新しい `aws:SourceOrgID` 条件キーを追加しました。更新されたポリシー `topic.To` を表示します。[AWS Config 「SNS トピックポリシー」](#) を参照してください。

ランディングゾーンのリージョン拒否コントロールの更新

- `discovery-marketplace:` を削除しました。このアクションは `aws-marketplace:*` 除外の対象となります。
- 「`quicksight:DescribeAccountSubscription`」を追加

CloudFormation テンプレートの更新

AWS KMS 暗号化が使用されていない場合に ガドリフトを表示しないようにBASELINE-CLOUDTRAIL-MASTER、という名前のスタックの CloudFormation テンプレートを更新しました。

新しい AWS Service Catalog 外部製品タイプへの移行 (フェーズ 2)

2023 年 12 月 7 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

HashiCorp が Terraform ライセンスを更新しました。その結果、Terraform Open Source 製品とプロビジョニング済み製品のサポートが External という新しい製品タイプ AWS Service Catalog に変更されました。

アカウント内の既存のワークロードと AWS リソースの中断を回避するには、2023 年 12 月 14 日までに[AWS Service Catalog 「外部製品タイプへの移行」の「AWS Control Tower の移行手順」](#)に従ってください。

AWS Control Tower がデジタル主権を支援するコントロールを発表

2023 年 11 月 27 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、デジタル主権要件を満たすのに役立つ 65 の新しい AWS マネージドコントロールを発表しました。このリリースでは、これらのコントロールを AWS Control Tower コンソールの新しいデジタル主権グループで確認できます。これらのコントロールを利用することで、データレジデンシー、きめ細かなアクセス制限、暗号化、レジリエンシー機能に関するアクションを防止したり、リソースの変更を検出したりできます。これらのコントロールは、要件に対して大規模かつ簡単に対応できるように設計されています。デジタル主権コントロールの詳細については、「[Controls that enhance digital sovereignty protection](#)」を参照してください。

たとえば、AWS AppSync API キャッシュで転送中の暗号化を有効にしたり、Network Firewall を複数のアベイラビリティゾーンにデプロイしたりする必要があるなど、AWS 暗号化と回復戦略を適用するのに役立つコントロールを有効にすることができます。また、AWS Control Tower のリージョン拒否コントロールをカスタマイズして、独自のビジネスニーズに最適なリージョン別の制限を適用することもできます。

このリリースでは、AWS Control Tower のリージョン拒否機能が大幅に強化されています。パラメータ化された新しいリージョン拒否コントロールを OU レベルで適用して、ガバナンスの細分性

を高めながら、ランディングゾーンレベルでの追加のリージョンガバナンスを維持できます。このカスタマイズ可能なリージョン拒否コントロールにより、独自のビジネスニーズに最適なリージョン別の制限を適用できます。新しい設定可能なリージョン拒否コントロールの詳細については、「[Region deny control applied to the OU](#)」を参照してください。

リージョン拒否の新しい強化ツールとして、このリリースには新しい API、`UpdateEnabledControl` が含まれています。これにより、有効にしたコントロールをデフォルト設定にリセットできます。この API は、ドリフトを迅速に解決する必要がある場合や、コントロールがドリフト状態でないことをプログラムで確認する必要がある場合に特に役立ちます。新しい API の詳細については、「[AWS Control Tower API リファレンス](#)」を参照してください。

新しいプロアクティブコントロール

- CT.APIGATEWAY.PR.6: Amazon API Gateway REST ドメインでは TLS プロトコルの最小バージョン TLSv1.2 を指定するセキュリティポリシーを使用する必要があります
- CT.APPSYNC.PR.2: AWS AppSync GraphQL API をプライベート可視性で設定する必要があります
- CT.APPSYNC.PR.3: AWS AppSync GraphQL API が API キーで認証されていない必要があります
- CT.APPSYNC.PR.4: AWS AppSync GraphQL API キャッシュで転送中の暗号化を有効にする必要があります。
- CT.APPSYNC.PR.5: AWS AppSync GraphQL API キャッシュで保管時の暗号化を有効にする必要があります。
- CT.AUTOSCALING.PR.9: Amazon EC2 Auto Scaling 起動設定を使用して設定した Amazon EBS ボリュームでは、保管中のデータを暗号化する必要があります
- CT.AUTOSCALING.PR.10: 起動テンプレートを上書きするときに、Amazon EC2 Auto Scaling グループが AWS Nitro インスタンスタイプのみを使用する必要があります
- CT.AUTOSCALING.PR.11: 起動テンプレートを上書きするときに、インスタンス間のネットワークトラフィックの暗号化をサポートする AWS Nitro インスタンスタイプのみを Amazon EC2 Auto Scaling グループに追加する必要があります
- CT.DAX.PR.3: DynamoDB Accelerator クラスターでは Transport Layer Security (TLS) を使用して転送中のデータを暗号化する必要があります
- CT.DMS.PR.2: AWS Database Migration Service (DMS) エンドポイントがソースエンドポイントとターゲットエンドポイントの接続を暗号化する必要があります
- CT.EC2.PR.15: Amazon EC2 インスタンスは、`AWS::EC2::LaunchTemplate` リソースタイプから作成する場合、AWS Nitro インスタンスタイプを使用する必要があります

- CT.EC2.PR.16: Amazon EC2 インスタンスは、AWS::EC2::Instance リソースタイプを使用して作成した場合、AWS Nitro インスタンスタイプを使用する必要があります
- CT.EC2.PR.17: Amazon EC2 専用ホストでは AWS Nitro インスタンスタイプを使用する必要があります
- CT.EC2.PR.18: Amazon EC2 フリートは、これらの起動テンプレートのみを AWS Nitro インスタンスタイプで上書きする必要があります
- CT.EC2.PR.19: Amazon EC2 インスタンスは、AWS::EC2::Instance リソースタイプを使用して作成した場合、インスタンス間の転送中の暗号化をサポートする Nitro インスタンスタイプを使用する必要があります
- CT.EC2.PR.20: Amazon EC2 フリートは、インスタンス間の転送中の暗号化をサポートする AWS Nitro インスタンスタイプを持つ起動テンプレートのみを上書きする必要があります。
- CT.ELASTICACHE.PR.8: 新しい Redis バージョンの Amazon ElastiCache レプリケーショングループでは RBAC 認証をアクティブにする必要があります
- CT.MQ.PR.1: Amazon MQ ActiveMQ ブローカーでは、高可用性を確保するためにアクティブ/スタンバイデプロイモードを使用する必要があります
- CT.MQ.PR.2: Amazon MQ Rabbit MQ ブローカーでは、高可用性を確保するためにマルチ AZ クラスターモードを使用する必要があります
- CT.MSK.PR.1: Amazon Managed Streaming for Apache Kafka (MSK) クラスターでは、クラスターブローカーノード間の転送中の暗号化を適用する必要があります
- CT.MSK.PR.2: Amazon Managed Streaming for Apache Kafka (MSK) クラスターでは、PublicAccess を無効に設定する必要があります
- CT.NETWORK-FIREWALL.PR.5: AWS Network Firewall ファイアウォールを複数のアベイラビリティゾーンにデプロイする必要があります
- CT.RDS.PR.26: Amazon RDS DB Proxy は Transport Layer Security (TLS) 接続を要求する必要があります
- CT.RDS.PR.27: Amazon RDS DB クラスターパラメータグループは、サポートしているエンジンタイプのために Transport Layer Security (TLS) 接続を要求する必要があります
- CT.RDS.PR.28: Amazon RDS DB パラメータグループは、サポートしているエンジンタイプのために Transport Layer Security (TLS) 接続を要求する必要があります
- CT.RDS.PR.29: Amazon RDS クラスターは、「PubliclyAccessible」プロパティを使用してパブリックでアクセスできないように設定する必要があります
- CT.RDS.PR.30: Amazon RDS データベースインスタンスでは、サポートしているエンジンタイプのために指定した KMS キーを使用するように保管中の暗号化を設定する必要があります

- CT.S3.PR.12: Amazon S3 のアクセスポイントでは、パブリックアクセスブロック (BPA) 設定のすべてのオプションを true に設定する必要があります

新しい予防コントロール

- CT.APPSYNC.PV.1 AWS AppSync GraphQL API がプライベート可視性で設定されている必要があります
- CT.EC2.PV.1 Amazon EBS スナップショットは、暗号化した EC2 ボリュームから作成する必要があります
- CT.EC2.PV.2 アタッチした Amazon EBS ボリュームは、保管中のデータを暗号化するように設定する必要があります
- CT.EC2.PV.3 Amazon EBS スナップショットはパブリックに復元できないようにする必要があります
- CT.EC2.PV.4 Amazon EBS direct API が呼び出されないようにする必要があります
- CT.EC2.PV.5 Amazon EC2 VM のインポートとエクスポートの使用を禁止します
- CT.EC2.PV.6 廃止された Amazon EC2 RequestSpotFleet および RequestSpotInstances API アクションの使用を禁止します
- CT.KMS.PV.1 AWS サービスへの AWS KMS 許可の作成を制限するステートメントを AWS KMS キーポリシーに要求する
- CT.KMS.PV.2 暗号化に使用される RSA キーマテリアルを持つ AWS KMS 非対称キーのキー長が 2048 ビットでない必要があります
- CT.KMS.PV.3 バイパスポリシーのロックアウト安全チェックを有効にして AWS KMS キーを設定する必要があります
- CT.KMS.PV.4 AWS KMS カスタマーマネージドキー (CMK) が AWS CloudHSM から発信されるキーマテリアルで設定されている必要があります
- CT.KMS.PV.5 AWS KMS カスタマーマネージドキー (CMK) がインポートされたキーマテリアルで設定されている必要があります
- CT.KMS.PV.6 AWS KMS カスタマーマネージドキー (CMK) は、外部キーストア (XKS) から発信されるキーマテリアルで設定する必要があります。
- CT.LAMBDA.PV.1 AWS Lambda 関数 URL に AWS IAM ベースの認証の使用を要求する
- CT.LAMBDA.PV.2 AWS Lambda 関数 URL は、内のプリンシパルのみがアクセスできるように設定する必要があります。AWS アカウント

AWS Control Tower ランディングゾーン API

2023 年 11 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、プログラムを使用してランディングゾーンを管理できる API が提供されるようになりました。これらの API を使用すると、ランディングゾーンを作成、更新、リセットしたり、ランディングゾーンの設定とオペレーションに関する情報を取得したりできます。詳細については、「[ランディングゾーン API の例](#)」を参照してください。

ランディングゾーン APIs は、GovCloud (米国) AWS リージョン リージョンを除く、AWS Control Tower が利用可能なすべてので使用できます。AWS Control Tower が利用可能な AWS リージョンのリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower コントロールのタグ付け API

2023 年 11 月 10 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、プログラムを使用して有効なコントロールにタグ付けする API が提供されるようになりました。これらの API を使用すると、有効なコントロールのタグを追加、削除、一覧表示できます。詳細については、「[AWS Control Tower リソースのタグ付け](#)」を参照してください。

コントロールタグ付け APIs は、GovCloud (米国) リージョンを除く、AWS Control Tower AWS リージョン が利用可能なすべてので使用できます。AWS Control Tower が利用可能な AWS リージョンのリストについては、[AWS リージョン 表](#)を参照してください。

AWS アジアパシフィック (メルボルン) で利用可能な AWS Control Tower

2023 年 11 月 3 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower がアジアパシフィック (メルボルン) で利用可能です。AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン の表](#)」を参照してください。

新しい AWS Service Catalog 外部製品タイプへの移行 (フェーズ 1)

2023 年 10 月 31 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

HashiCorp が Terraform ライセンスを更新しました。その結果、Terraform Open Source 製品とプロビジョニング済み製品のサポートが External という新しい製品タイプ AWS Service Catalog に変更されました。

アカウント内の既存のワークロードと AWS リソースの中断を回避するには、2023 年 12 月 14 日までに[AWS Service Catalog 「外部製品タイプへの移行」](#)の「AWS Control Tower の移行手順」に従ってください。

AWS Control Tower で新しいコントロール API が追加されました

2023 年 10 月 27 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、有効なコントロールを更新できる新しい API、UpdateEnabledControl が提供されるようになりました。この API は、ドリフトを迅速に解決する必要がある場合や、コントロールがドリフト状態でないことをプログラムで確認する必要がある場合に特に役立ちます。新しい API の詳細については、「[AWS Control Tower API リファレンス](#)」を参照してください。

UpdateEnabledControl API は、GovCloud (米国) リージョンを除く、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、「[AWS リージョン の表](#)」を参照してください。

AWS Control Tower で新しいコントロールが追加されました

2023 年 10 月 20 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、AWS Control Tower コントロールライブラリに 22 個の新しいコントロールが追加されました。これらのコントロールは、AWS リソースのベストプラクティスを適用するのに役立ちます。新しいコントロールの詳細については、「[Control のカテゴリ](#)」を参照してください。

新しいコントロールは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower で信頼されるアクセスドリフトを検出する

2023 年 10 月 13 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、信頼されるアクセス設定のドリフトを検出して報告するようになりました。信頼できるアクセス設定により、AWS Control Tower はユーザーに代わって他の AWS サービスとやり取りできます。これらの設定が AWS Control Tower の外部で変更された場合、AWS Control Tower はドリフトを検出し、AWS Control Tower コンソールで報告します。信頼されるアクセスのドリフトに関する詳細については、「[ガバナンスドリフトのタイプ](#)」を参照してください。

信頼できるアクセスドリフト検出は、AWS Control Tower が利用可能なすべての AWS リージョンで使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower が 4 つの追加で利用可能に AWS リージョン

2023 年 9 月 29 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、アジアパシフィック (ハイデラバード) AWS リージョン、アジアパシフィック (ジャカルタ)、欧州 (スペイン)、欧州 (チューリッヒ) の 4 つの追加で利用できます。AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン の表](#)」を参照してください。

AWS イスラエル (テルアビブ) で AWS Control Tower が利用可能に

2023 年 8 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower がイスラエル (テルアビブ) で利用可能です。AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン の表](#)」を参照してください。

AWS Control Tower に 28 個の新しいプロアクティブコントロールを追加

2023 年 7 月 27 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、AWS Control Tower コントロールライブラリに 28 個の新しいプロアクティブコントロールが追加されました。これらのコントロールは、AWS リソースのベストプラクティス

を適用するのに役立ちます。新しいコントロールの詳細については、「[Control のカテゴリ](#)」を参照してください。

新しいコントロールは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower で 2 つのコントロールが廃止されます

2023 年 7 月 27 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、CT.CLOUDFORMATION.PR.2 と CT.CLOUDFORMATION.PR.3 の 2 つのコントロールが廃止されました。これらのコントロールは、AWS Control Tower のコントロールライブラリで利用できなくなりました。廃止されたコントロールの詳細については、「[Control のカテゴリ](#)」を参照してください。

廃止されたコントロールは、どの でも使用できなくなりました AWS リージョン。

AWS Control Tower ランディングゾーンバージョン 3.2

2023 年 6 月 16 日

(AWS Control Tower ランディングゾーンをバージョン 3.2 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください)。

AWS Control Tower ランディングゾーンバージョン 3.2 では、AWS Security Hub CSPM サービス マネージドスタンダード: AWS Control Tower の一部であるコントロールが一般公開されています。この標準に含まれるコントロールのドリフトステータスを AWS Control Tower コンソールで表示する機能が導入されました。

このアップデートには、AWSServiceRoleForAWSControlTower と呼ばれる新しいサービスにリンクされたロール (SLR) が含まれています。このロールは、各メンバーアカウントに AWSControlTowerManagedRule と呼ばれる EventBridge マネージドルールを作成することで AWS Control Tower を支援します。このマネージドルールは、AWS Control Tower を使用してから AWS Security Hub CSPM 検出イベントを収集し、コントロールドリフトを判断できます。

このルールは、AWS Control Tower によって作成される最初のマネージドルールです。ルールはスタックによってデプロイされるのではなく、EventBridge API から直接デプロイされます。ルールは EventBridge コンソールで確認することも、EventBridge API を使用して表示することもできま

す。managed-by フィールドに入力すると、AWS Control Tower のサービスプリンシパルが表示されます。

以前は、AWS Control Tower は AWSControlTowerExecution ロールを前提として、メンバーアカウントで操作を実行していました。この新しいロールとルールは、マルチアカウント AWS 環境でオペレーションを実行するときに最小特権を許可するというベストプラクティスの原則により適しています。新しいロールでは、メンバーアカウントでのマネージドルールの作成、マネージドルールの管理、SNS によるセキュリティ通知の公開、ドリフトの検証など、具体的に許可する範囲を絞ったアクセス許可が提供されます。詳細については、「[AWSServiceRoleForAWSControlTower](#)」を参照してください。

ランディングゾーン 3.2 のアップデートには、管理アカウントに新しい StackSet リソース、BP_BASELINE_SERVICE_LINKED_ROLE も含まれています。これは、サービスにリンクされたロールを最初にデプロイします。

Security Hub CSPM コントロールドリフト (ランディングゾーン 3.2 以降) を報告すると、AWS Control Tower は Security Hub CSPM から毎日のステータス更新を受け取ります。コントロールはすべての管理対象リージョンでアクティブですが、AWS Control Tower は AWS Security Hub CSPM 検出イベントを AWS Control Tower ホームリージョンにのみ送信します。詳細については、「[Security Hub control drift reporting](#)」を参照してください。

リージョン拒否コントロールの更新

このランディングゾーンバージョンには、リージョン拒否コントロールの更新も含まれています。

追加されたグローバルサービスと API

- AWS Billing and Cost Management (billing:*)
- AWS CloudTrail (cloudtrail:LookupEvents) は、メンバーアカウントのグローバルイベントを可視化します。
- AWS 一括請求 (consolidatedbilling:*)
- AWS マネジメントコンソールモバイルアプリケーション (consoleapp:*)
- AWS 無料利用枠 (freetier:*)
- AWS Invoicing (invoicing:*)
- AWS IQ (iq:*)
- AWS ユーザー通知 (notifications:*)
- AWS ユーザー通知の連絡先 (notifications-contacts:*)

- Amazon Payments (payments:*)
- AWS 税設定 (tax:*)

削除されたグローバルサービスと API

- 有効なアクションではないため、s3:GetAccountPublic は削除されました。
- 有効なアクションではないため、s3:PutAccountPublic は削除されました。

AWS Control Tower に IAM Identity Center の email-to-ID マッピングが追加されました

2023 年 7 月 13 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で IAM Identity Center の email-to-ID マッピングがサポートされるようになりました。この機能を使用すると、E メールアドレスを IAM Identity Center ユーザー ID にマッピングし、AWS Control Tower 環境へのユーザーアクセスを簡単に管理できます。email-to-ID マッピングの詳細については、「[IAM Identity Center との統合](#)」を参照してください。

Email-to-ID マッピングは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン表](#)を参照してください。

AWS Control Tower が AWS Security Hub CSPM コントロールを追加

2023 年 6 月 29 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower の AWS Security Hub CSPM コントロールライブラリにコントロールを追加しました。これらのコントロールは、AWS リソースのベストプラクティスを適用するのに役立ちます。新しいコントロールの詳細については、「[Control のカテゴリ](#)」を参照してください。

新しいコントロールは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン表](#)を参照してください。

AWS Control Tower が AWS Security Hub CSPM コントロールのメタデータを発行する

2023 年 6 月 22 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が AWS Security Hub CSPM コントロールのメタデータを発行するようになりました。このメタデータには、コントロール ID、コントロールタイトル、コントロールの説明など、コントロールに関する情報が含まれます。メタデータの詳細については、「[コントロールのメタデータ](#)」を参照してください。

コントロールメタデータは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower に Terraform 用の Account Factory Customization (AFC) を追加

2023 年 6 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に Terraform 用の Account Factory Customization (AFC) が追加されました。この機能を使用すると、Terraform を使用して AWS Control Tower アカウントをカスタマイズできます。AFC for Terraform の詳細については、「[Account Factory for Terraform のカスタマイズ](#)」を参照してください。

AFC for Terraform は、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower にセルフマネージド IAM アイデンティティセンターを追加

2023 年 6 月 8 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower でセルフマネージド IAM アイデンティティセンターがサポートされるようになりました。この機能を使用すると、AWS Control Tower で独自の ID プロバイダーを使用できます。

セルフマネージド IAM Identity Center の詳細については、「[IAM Identity Center](#)」を参照してください。

セルフマネージド IAM アイデンティティセンターは、AWS Control Tower が利用可能なすべての AWS リージョン で利用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower に 混合ガバナンスの注意事項を追加

2023 年 6 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、混合ガバナンスに関する注意事項が追加されました。このノートでは、AWS Control Tower が他の AWS サービスと連携してリソースの AWS ガバナンスを提供する方法について説明します。混合ガバナンスの詳細については、「[混合ガバナンス](#)」を参照してください。

混合ガバナンスノートは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower に新しいプロアクティブコントロールを追加

2023 年 5 月 25 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、AWS Control Tower コントロールライブラリに新しいプロアクティブコントロールが追加されました。これらのコントロールは、AWS リソースのベストプラクティスを適用するのに役立ちます。新しいコントロールの詳細については、「[Control のカテゴリ](#)」を参照してください。

新しいコントロールは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower で Amazon EC2 コントロールを更新する

2023 年 5 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、AWS Control Tower コントロールライブラリの Amazon EC2 コントロールが更新されました。これらの更新により、AWS Control Tower 環境のセキュリティと信頼性が向上します。更新されたコントロールの詳細については、「[Control のカテゴリ](#)」を参照してください。

更新されたコントロールは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower が 7 つの追加で利用可能に AWS リージョン

2023 年 5 月 11 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は AWS リージョン、アジアパシフィック (大阪)、カナダ (中部)、欧州 (ミラノ)、欧州 (ストックホルム)、中東 (バーレーン)、中東 (アラブ首長国連邦)、南米 (サンパウロ) の 7 つの追加で利用できます。AWS Control Tower を使用できるリージョンの全リストについては、「[AWS リージョン の表](#)」を参照してください。

AWS Control Tower Account Factory Customization (AFC) とリクエストトレースが一般利用可能

2023 年 4 月 27 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower Account Factory Customization (AFC) とリクエストトレースが一般利用可能になりました。AFC では AWS Control Tower アカウントをカスタマイズでき、リクエストトレースにより AWS Control Tower リクエストのステータスを追跡できます。AFC とリクエストトレースの詳細については、「[Account Factory のカスタマイズ](#)」と「[リクエストのトレース](#)」を参照してください。

AFC とリクエストのトレースは、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

AWS Control Tower ランディングゾーンバージョン 3.1

2023 年 2 月 9 日

(AWS Control Tower のランディングゾーンをバージョン 3.1 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください)

AWS Control Tower ランディングゾーンバージョン 3.1 には、次の更新が含まれています。

- 今回のリリースでは、AWS Control Tower はアクセスログバケット (アクセスログが Log Archive アカウントに保存される Amazon S3 バケット) の不要なアクセスログを無効化し、S3 バケットのサーバーアクセスログを引き続き有効にします。このリリースには、サポート Plans やなどのグローバルサービスに追加のアクションを許可するリージョン拒否コントロールの更新も含まれています AWS Artifact。
- AWS Control Tower アクセスログバケットのサーバーアクセスログ記録を無効にすると、Security Hub CSPM は Log Archive アカウントのアクセスログバケットの結果を作成します。AWS Security Hub CSPM ルールにより、[\[S3.9\] S3 バケットサーバーのアクセスログ記録を有効にする必要があります](#)。Security Hub CSPM に合わせて、このルールの Security Hub CSPM の説明に記載されているように、この特定の検出結果を抑制することをお勧めします。追加情報については、「[非表示の結果に関する情報](#)」を参照してください。
- Log Archive アカウントの (通常の) ログバケットのアクセスログは、バージョン 3.1 でも変更されていません。ベストプラクティスに従い、そのバケットのアクセスイベントは、アクセスログバケットにログエントリとして記録されます。アクセスログの詳細については、Amazon S3 ドキュメントの「[サーバーアクセスログを使用したリクエストのログ記録](#)」を参照してください。
- リージョン拒否コントロールを更新しました。この更新により、より多くのグローバルサービスによるアクションが可能になります。この SCP の詳細については、「[リクエストされた AWS に基づいて へのアクセスを拒否する AWS リージョン](#)」および「[データレジデンシー保護を強化するコントロール](#)」を参照してください。

追加されたグローバルサービス:

- AWS アカウント管理 (account:*)
- AWS アクティブ化 (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 Resource Explorer (resource-explorer-2:*)
- Amazon S3
(s3:CreateMultiRegionAccessPoint、s3:GetBucketPolicyStatus、s3:PutMultiRegionA
- AWS Savings Plans (savingsplans:*)
- IAM Identity Center (sso:*)
- AWS Support App (supportapp:*)
- サポート プラン (supportplans:*)
- AWS 持続可能性 (sustainability:*)
- AWS Resource Groups Tagging API (tag:GetResources)
- AWS Marketplace Vendor Insights (vendor-insights:ListEntitledSecurityProfiles)

AWS Control Tower プロアクティブコントロールが一般利用可能

2023 年 4 月 13 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower プロアクティブコントロールが一般利用可能になりました。プロアクティブコントロールは、AWS リソースのベストプラクティスを適用するのに役立ちます。プロアクティブコントロールの詳細については、「[Proactive controls](#)」を参照してください。

プロアクティブコントロールは、AWS Control Tower が利用可能なすべての AWS リージョンで使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、[AWS リージョン 表](#)を参照してください。

2022 年 1 月 ~ 12 月

2022 年、AWS Control Tower は次の更新をリリースしました。

- [同時アカウント操作](#)
- [Account Factory Customization \(AFC\)](#)
- [包括的なコントロールは AWS リソースのプロビジョニングと管理に役立ちます](#)
- [すべての AWS Config ルールでコンプライアンスステータスを表示可能](#)

- [コントロールと新しい CloudFormation リソース用の API](#)
- [CfCT がスタックセットの削除をサポート](#)
- [カスタマイズされたログの保持](#)
- [ロールドリフト修復可能](#)
- [AWS Control Tower ランディングゾーンバージョン 3.0](#)
- [OU とアカウントのビューが組み合わされた組織ページ](#)
- [簡略化されたアカウントの作成と登録](#)
- [AFT は、AWS Control Tower の共有アカウントの自動カスタマイズをサポートします](#)
- [すべてのオプションのコントロールの同時操作](#)
- [既存のセキュリティアカウントとログアカウント](#)
- [AWS Control Tower ランディングゾーンバージョン 2.9](#)
- [AWS Control Tower ランディングゾーンバージョン 2.8](#)

同時アカウント操作

2022 年 12 月 16 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、Account Factory の同時実行アクションがサポートされるようになりました。一度に最大 5 つのアカウントを作成、更新、または登録できるようになります。最大 5 つのアクションを連続して送信し、各リクエストの完了状況を確認できます。その間、アカウントの作成はバックグラウンドで完了します。たとえば、別のアカウントを更新したり、組織単位 (OU) 全体を再登録したりする前に、各プロセスが完了するのを待つ必要がなくなります。

Account Factory Customization (AFC)

2022 年 11 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

Account Factory Customization を使用すると、AWS Control Tower コンソール内から新しいアカウントと既存のアカウントをカスタマイズできます。これらの新しいカスタマイズ機能により、特殊な Service Catalog 製品に含まれる CloudFormation テンプレートであるアカウントブループリントを柔

軟に定義できます。ブループリントにより、完全にカスタマイズされたリソースと構成がプロビジョニングされます。また、特定のユースケースに合わせてアカウントをカスタマイズするのに役立つ、AWS パートナーによって作成および管理される定義済みのブループリントを使用することもできます。

これまで、AWS Control Tower の Account Factory では、コンソールでのアカウントのカスタマイズをサポートしていませんでした。Account Factory の今回の更新により、アカウント要件を事前に定義して、明確に定義されたワークフローの一部として実装できます。ブループリントを適用して、新しいアカウントを作成し、他の AWS アカウントを AWS Control Tower に登録し、既存の AWS Control Tower アカウントを更新できます。

Account Factory でアカウントをプロビジョニング、登録、または更新するとき、デプロイするブループリントを選択します。ブループリントで指定されているリソースは、アカウントでプロビジョニングされます。アカウントの作成が完了すると、すべてのカスタム構成をすぐに使用できます。

アカウントのカスタマイズを開始するには、Service Catalog 製品で目的のユースケースに合わせてリソースを定義します。入 AWS 門ライブラリからパートナー管理のソリューションを選択することもできます。詳細については、「[Account Factory Customization \(AFC\) を使用したアカウントのカスタマイズ](#)」を参照してください。

包括的なコントロールは AWS リソースのプロビジョニングと管理に役立ちます

2022 年 11 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、CloudFormation フックを通じて実装された新しいオプションのプロアクティブコントロールを含む包括的なコントロール管理をサポートするようになりました。これらのコントロールは、リソースをデプロイする前にリソースをチェックして、新しいリソースが環境内で有効になっているコントロールに準拠しているかどうかを判断するため、プロアクティブと呼ばれます。

130 を超える新しいプロアクティブコントロールは、AWS Control Tower 環境の特定のポリシー目標を達成し、業界標準のコンプライアンスフレームワークの要件を満たすとともに、他の 20 を超える AWS サービスで AWS Control Tower のやり取りを管理するのに役立ちます。

AWS Control Tower コントロールライブラリは、関連する AWS サービスとリソースに従ってこれらのコントロールを分類します。詳細については、「[Proactive controls](#)」を参照してください。

このリリースでは、AWS Control Tower は AWS 、 Foundational Security Best Practices (FSBP) 標準をサポートする新しい Security Hub CSPM Service-Managed Standard: AWS Control Tower AWS Security Hub CSPMによっても統合されています。コンソールで AWS Control Tower コントロールとともに 160 を超える Security Hub CSPM コントロールを表示でき、AWS Control Tower 環境の Security Hub CSPM セキュリティスコアを取得できます。詳細については、「[Security Hub controls](#)」を参照してください。

すべての AWS Config ルールでコンプライアンスステータスを表示可能

2022 年 11 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower に登録された組織単位にデプロイされたすべての AWS Config ルールのコンプライアンスステータスを表示するようになりました。AWS Control Tower コンソールの外に移動しなくても、登録済みまたは未登録の AWS Control Tower のアカウントに影響するすべての AWS Config ルールのコンプライアンスステータスを表示できます。お客様は、検出コントロールと呼ばれる Config ルールを AWS Control Tower で設定するか、AWS Config サービスを通じて直接設定するかを選択できます。によってデプロイされたルール AWS Config と、AWS Control Tower によってデプロイされたルールが表示されます。

以前は、AWS Config サービスを通じてデプロイされた AWS Config ルールは AWS Control Tower コンソールに表示されていませんでした。お客様は、非準拠 AWS Config ルールを特定するために AWS Config サービスに移動する必要がありました。これで、AWS Control Tower コンソール内で非準拠 AWS Config ルールを特定できます。すべての設定ルールのコンプライアンスステータスを確認するには、AWS Control Tower コンソールの [Account details] (アカウントの詳細) のページに移動します。AWS Control Tower によって管理されるコントロールと AWS Control Tower の外部でデプロイされた設定ルールのコンプライアンスステータスを示すリストが表示されます。

コントロールと新しい CloudFormation リソース用の API

2022 年 9 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、一連の API コールによるコントロール (ガードレールとも呼ばれる) の、プログラムによる管理をサポートするようになりました。新しい CloudFormation リソースは、コントロールの API 機能をサポートしています。詳細については、「[AWS Control Tower でのタスクの自動化](#)」および「[を使用して AWS Control Tower リソースを作成する AWS CloudFormation](#)」を参照してください。

これらの API により、AWS Control Tower ライブラリでコントロールの有効化、無効化、およびアプリケーションステータスの表示を行うことができます。APIs のサポートが含まれているため CloudFormation、Infrastructure as code (IaC) として AWS リソースを管理できます。AWS Control Tower は、組織単位 (OU) 全体と OU 内のすべての AWS アカウントに関するポリシーの意図を表すオプションの予防コントロールと検出コントロールを提供します。これらのルールは、新しいアカウントを作成したり、既存のアカウントを変更したりしても、有効に存続します。

このリリースに含まれる API

- **EnableControl** — この API コールはコントロールをアクティブにします。非同期オペレーションを開始して、指定した組織単位とその組織単位内のアカウントの AWS リソースを作成します。
- **DisableControl** — この API コールは、コントロールをオフにします。非同期オペレーションを開始して、指定した組織単位とその組織単位内のアカウントの AWS リソースを削除します。
- **GetControlOperation** — 特定の EnableControl オペレーションまたは DisableControl オペレーションのステータスを返します。
- **ListEnabledControls** — 指定した組織単位とその組織単位内のアカウントで、AWS Control Tower によって有効化されたコントロールを一覧表示します。

オプションコントロールのコントロール名のリストを表示するには、「AWS Control Tower Controls Reference Guide」の「[Resource identifiers for APIs and controls](#)」を参照してください。

CfCT がスタックセットの削除をサポート

2022 年 8 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower のカスタマイズ (CfCT) は、manifest.yaml ファイルのパラメータを設定することで、スタックセットの削除をサポートするようになりました。詳細については、「[スタックセットの削除](#)」を参照してください。

Important

最初に enable_stack_set_deletion の値を true に設定すると、次回 CfCT を呼び出したときに、プレフィックス CustomControlTower- で始まるすべてのリソースのうち、キータグ Key:AWS_Solutions, Value: CustomControlTowerStackSet が関連付けられているリソースと、マニフェストファイルに宣言されていないリソースは、削除対象としてステージングされます。

カスタマイズされたログの保持

2022 年 8 月 15 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。)

AWS Control Tower は、AWS Control Tower CloudTrail ログを保存する Amazon S3 バケットの保持ポリシーをカスタマイズする機能を提供するようになりました。日単位または年単位で最大 15 年まで保存するという Amazon S3 ログ保持ポリシーをカスタマイズできます。

ログの保持をカスタマイズしない場合、デフォルト設定は、標準アカウントのログ記録で 1 年、アクセスログで 10 年です。

この機能は、ランディングゾーンを更新または修復する際は AWS Control Tower を介して既存のお客様が、AWS Control Tower のセットアップを通じて新規のお客様が利用できます。

ロールドリフト修復可能

2022 年 8 月 11 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、ロールドリフトの修復がサポートされるようになりました。ランディングゾーンを完全に修復しなくても、必要なロールを復元できます。このタイプのドリフト修復が必要な場合、コンソールのエラーページにロールを復元する手順が示され、ランディングゾーンが再び使用可能になります。

AWS Control Tower ランディングゾーンバージョン 3.0

2022 年 7 月 29 日

(AWS Control Tower のランディングゾーンをバージョン 3.0 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください)

AWS Control Tower ランディングゾーンバージョン 3.0 には、次の更新が含まれています。

- 組織レベルの AWS CloudTrail 証跡を選択するか、AWS Control Tower によって管理される CloudTrail 証跡をオプトアウトするオプション。
- AWS CloudTrail がアカウント内のアクティビティをログに記録するかどうかを判断する 2 つの新しい検出コントロール。

- ホームリージョンのみのグローバルリソース AWS Config に関する情報を集約するオプション。
- リージョン拒否コントロールの更新。
- 管理ポリシー AWSControlTowerServiceRolePolicy の更新。
- 各登録アカウントで、IAM ロール `aws-controltower-CloudWatchLogsRole` と CloudWatch ロググループ `aws-controltower/CloudTrailLogs` を作成しなくなりました。以前は、アカウント証跡用に各アカウントでこれらを作成していました。組織証跡では、管理アカウントに 1 つだけ作成します。

次のセクションでは、各能力タイプの詳細を示します。

AWS Control Tower の組織レベルの CloudTrail 証跡

ランディングゾーンバージョン 3.0 では、AWS Control Tower が組織レベルの AWS CloudTrail 証跡をサポートするようになりました。

AWS Control Tower ランディングゾーンをバージョン 3.0 に更新する場合、ログ記録設定として組織レベルの AWS CloudTrail 証跡を選択するか、AWS Control Tower によって管理される CloudTrail 証跡をオプトアウトするかを選択できます。バージョン 3.0 に更新すると、AWS Control Tower は 24 時間の待機期間後に登録済みアカウントの既存のアカウントレベルの証跡を削除します。AWS Control Tower は、未登録アカウントのアカウントレベルの証跡は削除しません。万ーランディングゾーンの更新が正常に行われず、AWS Control Tower が組織レベルの証跡を既に作成した後で障害が発生した場合、更新オペレーションを正常に完了できるようになるまで、組織レベルの証跡とアカウントレベルの証跡に対して請求が二重に発生する可能性があります。

ランディングゾーン 3.0 以降、AWS Control Tower は が AWS 管理するアカウントレベルの証跡をサポートしなくなりました。代わりに、AWS Control Tower は、お客様の選択に応じて、アクティブまたは非アクティブの組織レベルの証跡を作成します。

Note

バージョン 3.0 以降に更新後、AWS Control Tower によって管理されるアカウントレベルの CloudTrail 証跡作成を続行するオプションはありません。

ログは保存されている既存の Amazon S3 バケットに残っているため、集約されたアカウントログからログデータが失われることはありません。証跡のみが削除され、既存のログは削除されません。組織レベルの証跡を追加するオプションを選択すると、AWS Control Tower は Amazon S3 バケッ

ト内の新しいフォルダへの新しいパスを開き、その場所にログ情報を送信し続けます。AWS Control Tower によって管理される証跡をオプトアウトすることを選択した場合、既存のログは変更されずにバケットに残ります。

ログストレージのパス命名規則

- アカウント証跡ログは、次の形式のパスで保存されます。/org id/AWSLogs/...
- アカウント証跡ログは、次の形式のパスで保存されます。/org id/AWSLogs/org id/...

AWS Control Tower が組織レベルの CloudTrail 証跡用に作成するパスは、手動で作成する組織レベルの証跡のデフォルトパス (以下の形式) とは異なります。

- /AWSLogs/org id/...

CloudTrail のパス命名の詳細については、「[CloudTrail ログファイルの検索](#)」を参照してください。

Tip

独自のアカウントレベルの証跡を作成して管理する場合は、AWS Control Tower のランディングゾーンバージョン 3.0 への更新を完了する前に新しい証跡を作成して、すぐにログ記録を開始することをお勧めします。

新しいアカウントレベルまたは組織レベルの CloudTrail 証跡を随時作成し、自分で管理することを選択できます。AWS Control Tower によって管理される組織レベルの CloudTrail 証跡を選択するオプションは、バージョン 3.0 以降へのランディングゾーン更新中に利用できます。ランディングゾーンを更新するたびに、組織レベルの証跡をオプトイン/オプトアウトできます。

ログがサードパーティサービスによって管理されている場合は、必ずそのサービスに新しいパス名を提供してください。

Note

バージョン 3.0 以降のランディングゾーンでは、アカウントレベルの AWS CloudTrail 証跡は AWS Control Tower ではサポートされていません。アカウントレベルの証跡は随時作成して維持するか、AWS Control Tower によって管理される組織レベルの証跡情報にオプトインすることができます。

ホームリージョンのみに AWS Config リソースを記録する

ランディングゾーンバージョン 3.0 では、AWS Control Tower で AWS Config のベースライン設定が更新され、ホームリージョンのみにグローバルリソースが記録されるようになります。バージョン 3.0 にアップデートした後、グローバルリソースのリソース記録がホームリージョンでのみ有効化されます。

この設定はベストプラクティスであるとみなされています。グローバルリソースの作成 AWS Config、変更、または削除時に作成される設定項目の数を減らすことで、AWS Security Hub CSPM とが推奨し、コスト削減を実現します。以前は、グローバルリソースがお客様または AWS サービスにより作成、更新、または削除されるたびに、設定項目が管理対象の各リージョンの各項目に対して作成されていました。

AWS CloudTrail ログのための 2 つの新しい検出コントロール

組織レベルの AWS CloudTrail 証跡の変更の一環として、AWS Control Tower は CloudTrail が有効になっているかどうかを確認する 2 つの新しい検出コントロールを導入しています。最初のコントロールには必須ガイダンスがあり、3.0 以降のセットアップまたはランディングゾーン更新中にセキュリティ OU で有効になります。2 番目のコントロールは強く推奨されるガイダンスがあり、必須のコントロール保護が既に実装されているセキュリティ OU 以外の任意の OU にオプションで適用されます。

必須コントロール: [セキュリティ組織単位の共有アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する](#)

強く推奨されるコントロール: [アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する](#)

新しいコントロールの詳細については、「[The AWS Control Tower controls library](#)」を参照してください。

リージョン拒否コントロールの更新

リージョン拒否コントロールの NotAction リストを更新して、以下にリストされているいくつかの追加サービスによるアクションを含めました。

```
"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",
```

動画チュートリアル

このビデオ (3:07) では、既存の AWS Control Tower ランディングゾーンをバージョン 3 に更新する方法について説明しています。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[既存の AWS Control Tower のランディングゾーンをランディングゾーン 3 に更新するビデオウォークスルー。](#)

OU とアカウントのビューが組み合わされた組織ページ

2022 年 7 月 18 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower の新しい [組織] ページには、すべての組織単位 (OU) とアカウントの階層的な (ツリー) ビューが表示されます。ここでは、以前の [OU] ページと [Accounts] ページに表示されていた情報が表示されます。

新しいページでは、親 OU と、そのネストされた OU およびアカウントとの関係を確認することができ、リソースのグループに対してアクションを実行できます。ページビューを構成できます。例えば、階層ビューを展開することや折りたたむことに加えて、ビューをフィルターしてアカウントまたは OU のみを表示すること、登録済みアカウントと登録済みの OU のみを表示すること、関連リソースのグループを表示することができます。組織全体が適切に更新されていることを簡単に確認できます。

簡略化されたアカウントの作成と登録

2022 年 6 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、アカウントの作成と登録のワークフローが簡略化されました。Service Catalog コンソールに移動せずに、新しいアカウントを作成したり、既存のアカウントを単一のワークフローに登録したりできます。詳細については、「[AWS Control Tower コンソールから既存のアカウントを登録する](#)」を参照してください。

AFT は、AWS Control Tower の共有アカウントの自動カスタマイズをサポートします

2022 年 5 月 27 日

(AWS Control Tower ランディングゾーンの更新は不要です)

Account Factory for Terraform (AFT) では、AWS Control Tower で管理されているアカウント (管理アカウント、監査アカウント、ログアーカイブアカウントなど) を登録済みアカウントとともに、プログラムでカスタマイズおよび更新できるようになりました。アカウントのカスタマイズと更新の管理を一元化するとともに、アカウント設定のセキュリティを保護できます (この作業を実行するロールの適用範囲はユーザーが決めます)。

既存の AWSAFTExecution ロールが、すべてのアカウントにカスタマイズをデプロイするようになりました。IAM の許可をセットアップするには、ビジネス要件とセキュリティ要件に応じて、AWSAFTExecution ロールのアクセス権を制限する境界を使用できます。また、そのロールに承認されたカスタマイズの許可を、信頼されたユーザーにプログラムで委任することもできます。ベストプラクティスとして、必要なカスタマイズをデプロイする必要があるユーザーだけに許可を制限することをお勧めします。

AFT は、新しい AWSAFTService ロールを作成して、共有アカウントと管理アカウントを含むすべてのマネージドアカウントに AFT リソースをデプロイするようになりました。リソースは、以前は、AWSAFTExecution ロールによってデプロイされていました。

AWS Control Tower の共有アカウントと管理アカウントは Account Factory を通じてプロビジョニングされないため、対応するプロビジョニング済み製品はありません AWS Service Catalog。したがって、Service Catalog では共有アカウントと管理アカウントを更新できません。

すべてのオプションのコントロールの同時操作

2022 年 5 月 18 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower は、予防コントロールと検出コントロールの同時操作をサポートするようになりました。

この新しい機能により、すべてのオプションのコントロールを同時に適用または削除できるため、これらのコントロールの使いやすさとパフォーマンスが向上します。個々のコントロールの操作が完了するまで待たずに、複数のオプションのコントロールを有効にできます。同時操作が制限されるのは、AWS Control Tower がランディングゾーンのセットアップ中であるか、新しい組織にガバナンスを拡張中である場合だけです。

予防コントロールでサポートされる機能は以下のとおりです。

- 同じ OU に対して複数の異なる予防コントロールを適用または削除する。
- 複数の異なる予防コントロールを複数の異なる OU に対して同時に適用または削除します。
- 同じ予防コントロールを複数の異なる OU に対して同時に適用または削除します。
- 任意の数の予防コントロールと検出コントロールを同時に適用または削除できます。

AWS Control Tower のすべてのリリース済みバージョンで、これらのコントロールの同時実行の機能強化を体験できます。

予防コントロールは、ネストされた OU に適用すると、ターゲット OU の下にネストされたすべてのアカウントと OU に影響します。これらのアカウントや OU が AWS Control Tower に登録されていない場合でも影響を受けます。予防コントロールは、の一部であるサービスコントロールポリシー (SCPs) を使用して実装されます AWS Organizations。検出コントロールは AWS Config ルールを使用して実装されます。ガードレールは、新しいアカウントを作成したり、既存のアカウントを変更したりしても有効に存続します。AWS Control Tower は、各アカウントが有効なポリシーにどのように準拠しているかを示すサマリーレポートを提供します。使用可能なコントロールの完全なリストについては、「[The AWS Control Tower controls library](#)」を参照してください。

既存のセキュリティアカウントとログアカウント

2022 年 5 月 16 日

(初期セットアップ時に使用可能)

AWS Control Tower では、最初のランディングゾーンのセットアッププロセス中に、既存の AWS アカウントを AWS Control Tower セキュリティアカウントまたはログ記録アカウントとして指定できるようになりました。このオプションを使用すると、AWS Control Tower は新しい共有アカウントを作成する必要がなくなります。セキュリティアカウント (デフォルトでは、監査アカウントと呼ばれます) は、セキュリティチームとコンプライアンスチームに対してランディングゾーンのすべてのアカウントへのアクセスを許可する制限付きアカウントです。ログアカウント (デフォルトでは、ログアーカイブアカウントと呼ばれます) は、リポジトリとして機能します。このアカウントには、ラ

ランディングゾーンのすべてのアカウントからの API アクティビティとリソース設定のログが保存されます。

既存のセキュリティアカウントとログアカウントを使用することで、AWS Control Tower のガバナンスを既存の組織に拡張したり、別のランディングゾーンから AWS Control Tower に移動したりすることが容易になります。既存のアカウントを使用するオプションは、ランディングゾーンの最初のセットアップ時に表示されます。これには、セットアッププロセス中のチェックも含まれ、デプロイが正常に完了したことが確認されます。AWS Control Tower は、既存のアカウントに必要なロールとコントロールを実装します。これらのアカウントにある既存のリソースやデータは削除またはマージされません。

制限: 既存の AWS アカウントを監査およびログアーカイブアカウントとして AWS Control Tower に持ち込む予定で、それらのアカウントに既存の AWS Config リソースがある場合は、AWS Control Tower にアカウントを登録する前に既存の AWS Config リソースを削除する必要があります。

AWS Control Tower ランディングゾーンバージョン 2.9

2020 年 4 月 22 日

(AWS Control Tower のランディングゾーンをバージョン 2.9 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください)

AWS Control Tower のランディングゾーンバージョン 2.9 は、Python バージョン 3.9 ランタイムを使用するように通知フォワーダー Lambda を更新します。この更新プログラムは、2022 年 7 月に予定されている Python バージョン 3.6 の非推奨化に対処します。最新情報については、[Python の非推奨化に関するページ](#)を参照してください。

AWS Control Tower ランディングゾーンバージョン 2.8

2022 年 2 月 10 日

(AWS Control Tower のランディングゾーンをバージョン 2.8 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。)

AWS Control Tower ランディングゾーンバージョン 2.8 は、「[AWS の基本的なセキュリティのベストプラクティス](#)」の最新の更新に合わせて機能が追加されています。

このリリースでは:

- 既存の S3 アクセスログバケットへのアクセスを追跡するために、ログアーカイブアカウントのアクセスログバケットに対してアクセスログが設定されました。

- ライフサイクルポリシーのサポートが追加されました。既存の S3 アクセスログバケットのアクセスログは、デフォルトの保持期間の 10 年に設定されます。
- さらに、このリリースでは、AWS Control Tower が更新され、すべてのマネージドアカウント (管理アカウントを除く) で提供される AWS サービスリンクロール (SLR) が使用されるため AWS Config、AWS Config ベストプラクティスに合わせて Config ルールを設定および管理できます。アップグレードを行わないお客様は、引き続き既存のロールを使用することになります。
- このリリースでは、AWS Config データを暗号化するための AWS Control Tower KMS 設定プロセスを合理化し、CloudTrail の関連するステータスメッセージングを改善しました。
- このリリースには、リージョン拒否コントロールの更新が含まれており、us-west-2 で route53-application-recovery 機能を使用できるようになりました。
- 更新: 2022 年 2 月 15 日に、AWS Lambda 関数のデッドレターキューを削除しました。

その他の詳細:

- ランディングゾーンを廃止しても、AWS Control Tower は、AWS Config サービスにリンクされたロールを削除しません。
- Account Factory アカウントのプロビジョニングを解除しても、AWS Control Tower は、AWS Config サービスにリンクされたロールを削除しません。

ランディングゾーンを 2.8 に更新するには、[Landing zone settings] (ランディングゾーンの設定) ページに移動し、2.8 バージョンを選択して、[Update] (更新) を選択します。ランディングゾーンを更新したら、「[AWS Control Tower での設定更新管理](#)」に示すように、AWS Control Tower によって管理されているすべてのアカウントを更新する必要があります。

2021 年 1 月 ~ 12 月

2021 年、AWS Control Tower は次の更新をリリースしました。

- [リージョン拒否機能](#)
- [データ所在地機能](#)
- [AWS Control Tower で、Terraform アカウントのプロビジョニングとカスタマイズが導入されました](#)
- [新しいライフサイクルイベントが利用可能に](#)
- [AWS Control Tower でネストされた OU が有効になりました](#)
- [検出コントロールの同時実行性](#)

- [2 つの新しいリージョンが利用可能に](#)
- [リージョンの選択解除](#)
- [AWS Control Tower が AWS キー管理システムと連携する](#)
- [コントロールの名前が変更され、機能は変更されません](#)
- [AWS Control Tower は SCP を毎日スキャンしてドリフトをチェックするようになりました](#)
- [OU とアカウントのカスタマイズされた名前](#)
- [AWS Control Tower ランディングゾーンバージョン 2.7](#)
- [3 つの新しい AWS リージョンが利用可能に](#)
- [選択したリージョンのみを管理](#)
- [AWS Control Tower がガバナンスを AWS 組織内の既存の OUs に拡張](#)
- [AWS Control Tower でアカウントの一括更新が可能になりました](#)

リージョン拒否機能

2021 年 11 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower はリージョン拒否機能を提供するようになりました。これにより、AWS Control Tower 環境に登録されたアカウントの AWS サービスとオペレーションへのアクセスを制限できます。リージョン拒否機能は、AWS Control Tower の既存のリージョン選択およびリージョン選択解除機能を補完します。これらの機能を組み合わせて、追加のリージョンへの拡大に伴うコストのバランスをとり、コンプライアンスや規制上の懸念に対処するのに役立ちます。

たとえば、ドイツの AWS お客様は、フランクフルトリージョン以外のリージョン AWS のサービスへのアクセスを拒否できます。制限付きリージョンは、AWS Control Tower の設定プロセス中に、または [Landing zone settings] (ランディングゾーンの設定) ページで選択することができます。リージョン拒否機能は、AWS Control Tower ランディングゾーンのバージョンを更新するときに使用できます。一部の AWS サービスはリージョン拒否機能から除外されます。詳細については、「[Configure the Region deny control](#)」を参照してください。

データ所在地機能

2021 年 11 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、AWS サービスにアップロードする顧客データが、指定した AWS リージョンにのみ配置されるように、専用のコントロールが提供されるようになりました。顧客データが保存および処理される AWS リージョンを選択できます。AWS Control Tower が利用可能な AWS リージョンの完全なリストについては、[AWS 「リージョンテーブル」](#)を参照してください。

きめ細かく制御するには、[Disallow Amazon Virtual Private Network (VPN) connections] (Amazon Virtual Private Network (VPN) 接続を許可しない) や [Disallow internet access for an Amazon VPC instance] (Amazon VPC インスタンスのインターネットアクセスを許可しない) などの追加のコントロールを適用できます。AWS Control Tower コンソールでコントロールのコンプライアンスステータスを表示できます。使用可能なコントロールの完全なリストについては、「[The AWS Control Tower controls library](#)」を参照してください。

AWS Control Tower で、Terraform アカountのプロビジョニングとカスタマイズが導入されました

2021 年 11 月 29 日

(AWS Control Tower ランディングゾーンのオプションの更新)

AWS Control Tower Account Factory for Terraform (AFT) により、AWS Control Tower を通じて、Terraform を使用し、カスタマイズされたアカウントをプロビジョニングおよび更新できるようになりました。

AFT は、単一の Terraform Infrastructure as Code (IaC) パイプラインを提供し、AWS Control Tower が管理するアカウントをプロビジョニングします。プロビジョニング中のカスタマイズは、アカウントをエンドユーザーに提供する前に、ビジネスポリシーとセキュリティポリシーを満たすのに役立ちます。

AFT 自動アカウント作成パイプラインは、アカウントのプロビジョニングが完了するまで監視し、引き続き、必要なカスタマイズでアカウントを強化する追加の Terraform モジュールをトリガーします。カスタマイズプロセスの追加部分として、独自のカスタム Terraform モジュールをインストールするようにパイプラインを設定できます。また、一般的なカスタマイズ AWS のために が提供する任意の AFT 機能オプションを追加することもできます。

AWS Control Tower Account Factory for Terraform の使用を開始するには、「AWS Control Tower ユーザーガイド」の「[AWS Control Tower Account Factory for Terraform \(AFT\) のデプロイ](#)」に記載されているステップに従い、Terraform インスタンスの AFT をダウンロードします。AFT は、Terraform Cloud、Terraform Enterprise、および Terraform Open Source のディストリビューションをサポートしています。

新しいライフサイクルイベントが利用可能に

2021 年 11 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

PrecheckOrganizationalUnit イベントは、ネストされた OU のリソースを含め、[Extend governance] (ガバナンスを拡張) タスクが成功しないようリソースがブロックしているかどうかを記録します。詳細については、「[PrecheckOrganizationalUnit](#)」を参照してください。

AWS Control Tower でネストされた OU が有効になりました

2021 年 11 月 16 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、ランディングゾーンの一部として、ネストされた OU を含めることができるようになりました。

AWS Control Tower は、ネストされた組織単位 (OU、Organizational Unit) のサポートを提供して、アカウントを複数の階層レベルに編成し、予防コントロールを階層的に実施できるようにします。深さに関係なく、ネストされた OU を含む OU を登録し、親 OU の下に OU を作成して登録し、登録された OU でコントロールを有効にすることができます。この機能をサポートするために、管理されているアカウントと OU の数がコンソールに表示されます。

ネストされた OUs を使用すると、AWS Control Tower OUs を AWS マルチアカウント戦略に合わせることができ、親 OUs レベルでコントロールを適用することで、複数の OU でコントロールを有効にするために必要な時間を短縮できます。

主な考慮事項

1. AWS Control Tower に既存のマルチレベル OU を登録するときは、OU を 1 つずつ登録します。最上位の OU から開始し、ツリーの下の方へと進めます。詳細については、「[フラットな OU 構造からネストされた OU 構造への拡張](#)」を参照してください。
2. 登録された OU の直下のアカウントは自動的に登録されます。ツリーの下の方にあるアカウントは、直接の親 OU を登録することで登録できます。
3. 予防コントロール (SCP) は自動的に階層の下の方に継承されます。親に適用された SCP は、すべてのネストされた OU に継承されます。
4. 検出コントロール (AWS Config ルール) は自動的に継承されません。
5. 検出コントロールのコンプライアンスは、各 OU によって報告されます。

6. OU の SCP ドリフトは、その下にあるすべてのアカウントと OU に影響します。
7. セキュリティ OU (コア OU) の下に新しいネストされた OU を作成することはできません。

検出コントロールの同時実行性

2021 年 11 月 5 日

(AWS Control Tower ランディングゾーンのオプションの更新)

AWS Control Tower 検出コントロールは、検出コントロールの同時オペレーションをサポートするようになり、使いやすさとパフォーマンスが向上しました。個々のコントロールオペレーションが完了するのを待たずに、複数の検出コントロールを有効にできます。

サポートされている機能:

- 同じ OU で異なる検出コントロールを有効にします (例えば、[Detect Whether MFA for the Root User is Enabled] (ルートユーザーに対して MFA が有効になっているかどうかを検出する) と [Detect Whether Public Write Access to Amazon S3 Buckets is Allowed] (Simple Storage Service (Amazon S3) バケットへのパブリック書き込みアクセスが許可されているかどうかを検出する))。
- 異なる OU で異なる検出コントロールを同時に有効にします。
- ガードレールのエラーメッセージングが改善され、サポートされているコントロールの同時実行オペレーションに関する追加のガイダンスが提供されるようになりました。

このリリースではサポートされない機能:

- 同じ検出コントロールを複数の OU で同時に有効にすることはサポートされていません。
- 予防的コントロールの同時実行はサポートされていません。

AWS Control Tower のすべてのバージョンで、検出コントロールの同時実行性の改善を体験できます。現在バージョン 2.7 を使用していないお客様は、最新バージョンで利用できるリージョンの選択や選択解除などの機能を利用できるように、ランディングゾーンの更新を実行することをお勧めします。

2 つの新しいリージョンが利用可能に

2021 年 7 月 29 日

(AWS Control Tower ランディングゾーンは更新が必要です。)

AWS Control Tower が、南米 (サンパウロ)、欧州 (パリ) の 2 つの追加 AWS リージョンで利用可能になりました。この更新により、AWS Control Tower の可用性が 15 の AWS リージョンに拡張されます。

AWS Control Tower を初めて使用する場合も、サポートされている任意のリージョンですぐに起動できます。起動時に、AWS Control Tower でマルチアカウント環境を構築および管理するリージョンを選択できます。

AWS Control Tower 環境が既にある、サポートされている 1 つ以上のリージョンの AWS Control Tower ガバナンス機能を拡張または削除する場合は、AWS Control Tower ダッシュボードの [Landing Zone Settings] (ランディングゾーンの設定) ページに移動し、[Regions] (リージョン) を選択します。ランディングゾーンを更新したら、[AWS Control Tower によって管理されているすべてのアカウントを更新する](#)必要があります。

リージョンの選択解除

2021 年 7 月 29 日

(AWS Control Tower ランディングゾーンのオプションの更新)

AWS Control Tower リージョンの選択解除により、AWS Control Tower リソースの地理的フットプリントを管理する機能が強化されます。AWS Control Tower の管理を望まないリージョンの選択を解除できます。この機能により、追加のリージョンへの拡大に伴うコストのバランスをとりながら、コンプライアンスや規制に関する懸念に対処できます。

リージョンの選択解除は、AWS Control Tower ランディングゾーンのバージョンを更新するときに使用できます。

Account Factory を使用して新しいアカウントを作成するか、既存のメンバーアカウントを登録する場合、または [Extend Governance] (ガバナンスを拡張) を選択して既存の組織単位にアカウントを登録する場合、AWS Control Tower は、アカウントの選択したリージョンにガバナンス機能 (一元化されたロギング、モニタリング、コントロールなど) をデプロイします。リージョンの選択を解除し、そのリージョンから AWS Control Tower ガバナンスを削除することを選択すると、そのガバナンス機能は削除されますが、ユーザーがそれらのリージョンに AWS リソースまたはワークロードをデプロイする能力は妨げられません。

AWS Control Tower が AWS キー管理システムと連携する

2021 年 7 月 28 日

(AWS Control Tower のランディングゾーンのオプションの更新)

AWS Control Tower には、AWS Key Management Service (AWS KMS) キーを使用するオプションがあります。キーは、AWS Control Tower がデプロイするサービス、および関連する Amazon S3 データを保護するために、ユーザーによって提供および管理されます。AWS KMS 暗号化は AWS CloudTrail AWS Config、AWS Control Tower がデフォルトで使用する SSE-S3 暗号化よりも強化されたレベルの暗号化です。

AWS KMS サポートを AWS Control Tower に統合することは、機密性の高いログファイルにセキュリティレイヤーを追加することを推奨する AWS Foundational Security Best Practices と一致しています。保管時の暗号化には AWS KMS マネージドキー (SSE-KMS) を使用する必要があります。AWS KMS 暗号化のサポートは、新しいランディングゾーンを設定するとき、または既存の AWS Control Tower ランディングゾーンを更新するときに使用できます。

この機能を設定するには、ランディングゾーンの初期設定時に [KMS Key Configuration] (KMS キー設定) を選択します。既存の KMS キーを選択するか、KMS AWS コンソールに誘導するボタンを選択して新しいキーを作成できます。また、デフォルトの暗号化から SSE-KMS、または別の SSE-KMS キーに変更できる柔軟性があります。

既存の AWS Control Tower ランディングゾーンでは、更新を実行して AWS KMS キーの使用を開始できます。

コントロールの名前が変更され、機能は変更されません

2021 年 7 月 26 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower は、コントロールのポリシー意図をよりよく反映するように、特定のコントロールの名前と説明を改訂しています。改訂された名前と説明は、コントロールがアカウントのポリシーを具現化する方法をより直感的に理解するのに役立ちます。例えば、検出コントロール自体が特定のアクションを停止せず、ポリシー違反を検出し、ダッシュボードを介してアラートを提供するため、検出コントロールの名前の一部を「許可しない」から「検出」に変更しました。

コントロールの機能、ガイダンス、および実装は変更ありません。コントロールの名前と説明のみ改訂されています。

AWS Control Tower は SCP を毎日スキャンしてドリフトをチェックするようになりました

2021 年 5 月 11 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower は、管理対象の SCP を毎日自動スキャンして、対応するコントロールが正しく適用され、ドリフトが発生していないことを確認するようになりました。スキャンでドリフトが検出されると、通知が届きます。AWS Control Tower は、ドリフトの問題ごとに通知を 1 つだけ送信するため、ランディングゾーンが既にドリフト状態にある場合、新しいドリフトアイテムが見つからない限り、追加の通知が送信されることはありません。

OU とアカウントのカスタマイズされた名前

2021 年 4 月 16 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、ランディングゾーンの名前付けをカスタマイズできるようになりました。AWS Control Tower が組織単位 (OU、Organizational Unit) およびコアアカウントに推奨する名前を保持するか、ランディングゾーン初期設定プロセス中にこれらの名前を変更することができます。

AWS Control Tower が OU およびコアアカウントに提供するデフォルトの名前は、AWS マルチアカウントのベストプラクティスのガイダンスに合致しています。ただし、会社で特定の命名ポリシーがある場合、あるいは同じ推奨名を持つ既存の OU またはアカウントが既に存在する場合は、この新しい OU およびアカウント命名機能によって、これらの制約に柔軟に対応できます。

設定時のこのワークフローの変更とは別に、以前はコア OU と呼ばれていた OU はセキュリティ OU と呼ばれ、以前はカスタム OU と呼ばれていた OU はサンドボックス OU と呼ばれるようになりました。命名に関する全体的な AWS ベストプラクティスのガイダンスとの連携を改善するために、この変更を加えました。

新しいお客様には、これらの新しい OU 名が表示されます。既存のお客様には、これらの OU の元の名前が引き続き表示されます。ドキュメントを新しい名前に更新している間、OU の命名に不一致が生じることがあります。

AWS マネジメントコンソールから AWS Control Tower の使用を開始するには、AWS Control Tower コンソールに移動し、右上の「ランディングゾーンのセットアップ」を選択します。詳細については、「AWS Control Tower ランディングゾーンの計画」を参照してください。

AWS Control Tower ランディングゾーンバージョン 2.7

2021 年 4 月 8 日

(AWS Control Tower のランディングゾーンをバージョン 2.7 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。)

AWS Control Tower バージョン 2.7 では、AWS Control Tower のリソースにのみポリシーを実装する 4 つの新しい必須予防的ログアーカイブコントロールが導入されました。AWS Control Tower の外にあるリソースのポリシーを設定するため、4 つの既存のログアーカイブコントロールのガイダンスを必須から選択的に調整しました。このコントロールの変更と拡張により、AWS Control Tower 内のリソースのログアーカイブガバナンスと AWS Control Tower 外のリソースのガバナンスを分離できます。

4 つの変更されたコントロールを新しい必須コントロールと組み合わせて使用して、より広範な AWS ログアーカイブのセットにガバナンスを提供できます。既存の AWS Control Tower 環境では、環境の一貫性を保つため、これらの 4 つの変更されたコントロールが自動的に有効になります。ただし、これらの選択的コントロールは無効にできるようになりました。新しい AWS Control Tower 環境では、すべての選択的コントロールを有効にする必要があります。既存の環境では、AWS Control Tower によってデプロイされていない Amazon S3 バケットに暗号化を追加する前に、以前は必須のコントロールを無効にする必要があります。

新しい必須コントロール:

- Disallow Changes to Encryption Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットの暗号化設定の変更を許可しない)
- Disallow Changes to Logging Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットのログ設定の変更を許可しない)
- Disallow Changes to Bucket Policy for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットのバケットポリシーの変更を許可しない)
- Disallow Changes to Lifecycle Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットのライフサイクル設定の変更を許可しない)

必須から選択的に変更されたガイダンス:

- Disallow Changes to Encryption Configuration for all Amazon S3 Buckets (すべての Simple Storage Service (Amazon S3) バケットの暗号化設定の変更を許可しない) [Previously: Enable Encryption at Rest for Log Archive (以前: ログアーカイブの保管時に暗号化を有効にする)]

- Disallow Changes to Logging Configuration for all Amazon S3 Buckets (すべての Simple Storage Service (Amazon S3) バケットのログ設定の変更を許可しない) [Previously: Enable Access Logging for Log Archive (以前: ログアーカイブのアクセスログを有効にする)]
- Disallow Changes to Bucket Policy for all Amazon S3 Buckets (すべての Amazon S3 バケットのバケットポリシーの変更を不許可にする) [Previously: Disallow Policy Changes to Log Archive (以前: ログアーカイブのポリシー変更を禁止する)]
- Disallow Changes to Lifecycle Configuration for all Amazon S3 Buckets (すべての Simple Storage Service (Amazon S3) バケットのライフサイクル設定の変更を許可しない) [Previously: Set a Retention Policy for Log Archive (以前: ログアーカイブの保持ポリシーを設定する)]

AWS Control Tower バージョン 2.7 には、2.7 にアップグレードした後に以前のバージョンとの互換性がなくなる可能性がある AWS Control Tower ランディングゾーンのブループリントに対する変更が含まれています。

- 特に、AWS Control Tower バージョン 2.7 では、AWS Control Tower によってデプロイされた S3 バケットで自動的に BlockPublicAccess が有効になります。ワークロードでアカウント全体のアクセスが必要な場合は、このデフォルトをオフにすることができます。BlockPublicAccess を有効にした場合の動作については、「[Amazon S3 ストレージへのパブリックアクセスのブロック](#)」を参照してください。
- AWS Control Tower バージョン 2.7 には HTTPS の要件が含まれています。AWS Control Tower によってデプロイされた S3 バケットに送信されるすべてのリクエストは、Secure Sockets Layer (SSL) を使用する必要があります。HTTPS リクエストのみ渡すことができます。HTTP (SSL なし) をエンドポイントとして使用してリクエストを送信すると、この変更によってアクセス拒否エラーが発生し、ワークフローが中断する可能性があります。ランディングゾーンを 2.7 に更新した後で、この変更を元に戻すことはできません。

HTTP の代わりに TLS を使用するようにリクエストを変更することをお勧めします。

3 つの新しい AWS リージョンが利用可能に

2021 年 4 月 8 日

(AWS Control Tower ランディングゾーンは更新が必要です。)

AWS Control Tower は、アジアパシフィック (東京) AWS リージョン、アジアパシフィック (ソウル) リージョン、アジアパシフィック (ムンバイ) リージョンの 3 つの追加リージョンで利用できます。

これらのリージョンにガバナンスを拡大するには、ランディングゾーンをバージョン 2.7 に更新する必要があります。

バージョン 2.7 への更新を実行しても、ランディングゾーンがこれらのリージョンに自動的に展開されることはありません。含まれるようにするには、リージョン表でそれらを表示して選択する必要があります。

選択したリージョンのみを管理

2021 年 2 月 19 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower リージョンを選択すると、AWS Control Tower リソースの地理的フットプリントをより適切に管理できます。コンプライアンス、規制、コストなどの理由で AWS リソースまたはワークロードをホストするリージョンの数を拡張するために、管理する追加のリージョンを選択できるようになりました。

リージョン選択は、新しいランディングゾーンを設定するか、AWS Control Tower ランディングゾーンのバージョンを更新するときに利用できます。Account Factory を使用して新しいアカウントを作成するか、既存のメンバーアカウントを登録する場合、または [Extend Governance] (ガバナンスを拡張) を使用して既存の組織単位にアカウントを登録する場合、AWS Control Tower は、アカウントの選択したリージョンにガバナンス機能 (一元化されたロギング、モニタリング、コントロール) をデプロイします。リージョンの選択の詳細については、「[AWS Control Tower リージョンの設定](#)」を参照してください。

AWS Control Tower がガバナンスを AWS 組織内の既存の OUs に拡張

2021 年 1 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower コンソール内から既存の組織単位 (OU、Organizational Unit) (AWS Control Tower にはない OU) にガバナンスを拡張します。この機能を使用すると、最上位の OU と含まれるアカウントを AWS Control Tower ガバナンス下に置くことができます。OU 全体へのガバナンスの拡張については、「[AWS Control Tower への既存の組織単位の登録](#)」を参照してください。

OU を登録すると、AWS Control Tower は一連のチェックを実行して、ガバナンスの拡張と OU 内のアカウントの登録が正常に行われていることを確認します。OU の初期登録に関連する一般的な問題の詳細については、「[登録時または再登録時に発生する障害のよくある原因](#)」を参照してください。

また、AWS Control Tower [製品ウェブページ](#)にアクセスしたり、YouTube にアクセスして [AWS Organizations向け AWS Control Tower の開始方法](#)に関する動画を視聴することもできます。

AWS Control Tower でアカウントの一括更新が可能になりました

2021 年 1 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

一括更新機能により、最大 300 個のアカウントを含む登録済みの AWS Organizations 組織単位 (OU、Organizational Unit) のすべてのアカウントを、AWS Control Tower ダッシュボードから、1 回のクリックで更新できるようになりました。これは、AWS Control Tower ランディングゾーンを更新し、現行のランディングゾーンのバージョンに合うように登録済みアカウントも更新する必要がある場合に特に便利です。

また、この機能は、AWS Control Tower ランディングゾーンを更新して新しいリージョンに拡張する場合や、OU を再登録して OU のすべてのアカウントに最新のコントロールが適用されるようにする場合に、アカウントを最新状態に保つのに役立ちます。アカウントの一括更新により、アカウントを 1 つずつ更新したり、外部スクリプトを使用して複数のアカウントに対して更新を実行したりする必要がなくなります。

ランディングゾーンの更新の詳細については、「[ランディングゾーンを更新する](#)」を参照してください。

OU の登録または再登録の詳細については、「[AWS Control Tower への既存の組織単位の登録](#)」を参照してください。

2020 年 1 月 ~ 12 月

2020 年、AWS Control Tower は次の更新をリリースしました。

- [AWS Control Tower コンソールが外部 Config AWS ルールにリンクされるようになりました](#)
- [AWS Control Tower が追加のリージョンで利用可能になりました](#)
- [ガードレールの更新](#)
- [AWS Control Tower コンソールに OU とアカウントの詳細が表示されます](#)
- [AWS Control Tower を使用して 新しいマルチアカウント AWS 環境をセットアップする AWS Organizations](#)

- [AWS Control Tower ソリューションのカスタマイズ](#)
- [AWS Control Tower バージョン 2.3 の一般提供](#)
- [AWS Control Tower でのシングルステップのアカウントプロビジョニング](#)
- [AWS Control Tower の廃止ツール](#)
- [AWS Control Tower のライフサイクルイベント通知](#)

AWS Control Tower コンソールが外部 Config AWS ルールにリンクされるようになりました

2020 年 12 月 29 日

(AWS Control Tower のランディングゾーンをバージョン 2.6 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。)

AWS Control Tower に、外部 AWS Config ルールの検出を支援する組織レベルのアグリゲータが追加されました。これにより、AWS Control Tower コンソールで可視性が得られ、AWS Control Tower によって作成された Config AWS ルールに加えて、外部で作成された AWS Config ルールの存在を確認できます。アグリゲータを使用すると、AWS Control Tower は外部ルールを検出し、AWS Control Tower AWS がアンマネージドアカウントにアクセスすることなく、Config コンソールへのリンクを提供できます。

この機能により、アカウントに適用される検出コントロールの統合ビューが作成され、コンプライアンスを追跡し、アカウントに追加のコントロールが必要かどうかを判断できるようになりました。詳細については、「[AWS Control Tower がアンマネージド OU とアカウントで AWS Config ルールを集約する方法 OUs](#)」を参照してください。

AWS Control Tower が追加のリージョンで利用可能になりました

2020 年 11 月 18 日

(AWS Control Tower のランディングゾーンをバージョン 2.5 に更新する必要があります。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。)

AWS Control Tower が 5 つの追加 AWS リージョンで利用可能になりました。

- アジアパシフィック (シンガポール) リージョン
- 欧州 (フランクフルト) リージョン

- 欧州 (ロンドン) リージョン
- 欧州 (ストックホルム) リージョン
- カナダ (中部) リージョン

これらの 5 AWS リージョンの追加は、AWS Control Tower のバージョン 2.5 で導入された唯一の変更です。

AWS Control Tower は、米国東部 (バージニア北部) リージョン、米国東部 (オハイオ) リージョン、米国西部 (オレゴン) リージョン、欧州 (アイルランド) リージョン、アジアパシフィック (シドニー) リージョンでも利用できます。このリリースにより、AWS Control Tower が 10 AWS リージョンで利用可能になりました。

このランディングゾーンの更新には、リストされているすべてのリージョンが含まれており、元に戻すことはできません。ランディングゾーンをバージョン 2.5 に更新したら、AWS Control Tower に登録されているすべてのアカウントを手動で更新して、サポートされている 10 の AWS リージョンで管理する必要があります。詳細については、「[AWS Control Tower リージョンの設定](#)」を参照してください。

ガードレールの更新

2020 年 10 月 8 日

(AWS Control Tower ランディングゾーンの更新は不要です)

必須コントロール AWS-GR_IAM_ROLE_CHANGE_PROHIBITED の更新バージョンがリリースされました。

AWS Control Tower に自動的に登録されるアカウントは AWSControlTowerExecution ロールを有効にする必要があるため、コントロールのこの変更が必要になります。コントロールの以前のバージョンでは、このロールは作成されません。

詳細については、「[AWS Control Tower AWS によって設定された IAM ロールの変更の禁止](#)」および [CloudFormation](#) 「AWS Control Tower コントロールリファレンスガイド」の「」を参照してください。

AWS Control Tower コンソールに OU とアカウントの詳細が表示されます

2020 年 7 月 22 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower に登録されていない組織およびアカウントを、登録されている組織およびアカウントと共に表示できます。

AWS Control Tower コンソールでは、AWS アカウントと組織単位 (OUs) の詳細を表示できます。[Accounts] (アカウント) ページには、AWS Control Tower での OU や登録のステータスに関係なく、組織内のすべてのアカウントが一覧表示されるようになりました。すべてのテーブルで検索、並べ替え、フィルタリングを実行できるようになりました。

AWS Control Tower を使用して 新しいマルチアカウント AWS 環境をセットアップする AWS Organizations

2020 年 4 月 22 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Organizations のお客様は、AWS Control Tower を使用して、新しく作成された組織単位 (OUs) とアカウントを管理できるようになりました。

- 既存の AWS Organizations お客様は、既存の管理アカウントに新しい組織単位 (OUs) 用の新しいランディングゾーンを設定できるようになりました。AWS Control Tower で新しい OU を作成し、AWS Control Tower ガバナンスを使用して OU に新しいアカウントを作成できます。
- AWS Organizations のお客様は、アカウント登録プロセスまたはスクリプトを使用して、既存のアカウントを登録できます。

AWS Control Tower は、他の サービスを使用するオーケストレーション AWS サービスを提供します。これは、複数のアカウントを持つ組織や、新規または既存のマルチアカウント AWS 環境を設定し、大規模に管理するための最も簡単な方法を探しているチーム向けに設計されています。AWS Control Tower によって管理されている組織では、クラウド管理者は、組織内のアカウントが確立されたポリシーに準拠していることを知っています。ビルダーは、コンプライアンスについて過度に心配することなく、新しい AWS アカウントを迅速にプロビジョニングできるため、メリットがあります。

ランディングゾーンの設定の詳細については、「[AWS Control Tower ランディングゾーンの計画](#)」を参照してください。また、AWS Control Tower [製品ウェブページ](#)にアクセスしたり、YouTube にアクセスして [AWS Organizations向け AWS Control Tower の開始方法](#)に関する動画を視聴することもできます。

この変更に加えて、AWS Control Tower のクイックアカウントプロビジョニング機能の名前がアカウントの登録に変更されました。既存の AWS アカウントの登録と新しいアカウントの作成を許可できるようになりました。詳細については、「[AWS Control Tower コンソールから既存のアカウントを登録する](#)」を参照してください。

AWS Control Tower ソリューションのカスタマイズ

2020 年 3 月 17 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower には、カスタムテンプレートおよびポリシーを AWS Control Tower ランディングゾーンに簡単に適用できる新しいリファレンス実装が追加されました。

AWS Control Tower のカスタマイズを使用すると、CloudFormation テンプレートを使用して、組織内の既存アカウントと新規アカウントに新しいリソースをデプロイできます。また、これらのアカウントには、AWS Control Tower によって既に提供されているサービスコントロールポリシー (SCP、Service Control Policies) に加えて、カスタム SCP を適用することもできます。AWS Control Tower パイプラインのカスタマイズは、リソースのデプロイとランディングゾーンの同期が保たれるように、AWS Control Tower のライフサイクルイベントおよび通知 (「[AWS Control Tower でのライフサイクルイベント](#)」) と統合されます。

この AWS Control Tower ソリューションアーキテクチャのデプロイドキュメントは、[AWS Solutions ウェブページ](#)から入手できます。

AWS Control Tower バージョン 2.3 の一般提供

2020 年 3 月 5 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。)

AWS Control Tower が、米国東部 (オハイオ)、米国東部 (バージニア北部)、米国西部 (オレゴン)、欧州 (アイルランド) AWS の各リージョンに加えて、アジアパシフィック (シドニー) リージョンで利用可能になりました。アジアパシフィック (シドニー) リージョンの追加は、AWS Control Tower のバージョン 2.3 で導入された唯一の変更点です。

これまで AWS Control Tower を使用していなかった場合は、サポートされている任意のリージョンで今すぐ AWS Control Tower を起動できます。既に AWS Control Tower を使用していて、アカウン

トのアジアパシフィック (シドニー) リージョンにガバナンス機能を拡張する場合は、AWS Control Tower ダッシュボードの [Settings] (設定) ページに移動します。そこから、ランディングゾーンを最新リリースに更新します。そして、アカウントを個別に更新します。

Note

ランディングゾーンを更新しても、アカウントは自動的に更新されません。アカウントが数個以上ある場合は、必要な更新を行うのに時間がかかることがあります。そのため、ワークロードの実行を必要としないリージョンに AWS Control Tower ランディングゾーンを拡張することは避けてください。

新しいリージョンへのデプロイの結果としての検出コントロールの予想される動作の詳細については、「[Configure your AWS Control Tower Regions](#)」を参照してください。

AWS Control Tower でのシングルステップのアカウントプロビジョニング

2020 年 3 月 2 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower コンソールを使用したシングルステップのアカウントプロビジョニングをサポートするようになりました。この機能を使用すると、AWS Control Tower コンソール内から新しいアカウントをプロビジョニングできます。

簡略化された形式を使用するには、AWS Control Tower コンソールの [Account Factory] に移動し、[Quick account provisioning] (クイックアカウントプロビジョニング) を選択します。AWS Control Tower は、プロビジョニングされたアカウントとそのアカウントに作成された Single Sign-On (IAM Identity Center) ユーザーに同じ E メールアドレスを割り当てます。これら 2 つの E メールアドレスを異なるものにすることが必要な場合は、Service Catalog を通じてアカウントをプロビジョニングする必要があります。

他のアカウントの更新と同様に、Service Catalog および AWS Control Tower Account Factory を使用して、クイックアカウントプロビジョニングで作成したアカウントを更新します。

Note

2020 年 4 月、クイックアカウントプロビジョニング機能の名前がアカウントの登録に変更されました。2022 年 6 月、AWS Control Tower コンソールでアカウントを作成および更

新する機能は、AWS アカウントを登録する機能とは分離されました。詳細については、「[AWS Control Tower コンソールから既存のアカウントを登録する](#)」を参照してください。

AWS Control Tower の廃止ツール

2020 年 2 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower によって割り当てられたリソースのクリーンアップを支援する自動廃止ツールをサポートするようになりました。AWS Control Tower を企業で使用しなくなった場合、または組織のリソースに大幅な再デプロイが必要な場合は、ランディングゾーンを最初にセットアップしたときに作成されたリソースをクリーンアップすることができます。

ほぼ自動化されたプロセスを使用してランディングゾーンを廃止するには、AWS サポート に連絡して、必要な追加ステップについてサポートを受けてください。廃止の詳細については、「[AWS Control Tower のランディングゾーンを廃止する](#)」を参照してください。

AWS Control Tower のライフサイクルイベント通知

2020 年 1 月 22 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、ライフサイクルイベント通知が利用可能になりました。[ライフサイクルイベント](#)は、AWS Control Tower で作成および管理する組織単位 (OU)、アカウント、コントロールなどのリソースの状態を変更できる AWS Control Tower アクションの完了をマークします。ライフサイクルイベントは、AWS CloudTrail イベントとして記録され、Amazon EventBridge にイベントとして配信されます。

AWS Control Tower は、サービスを使用して実行できる次のアクションの完了時にライフサイクルイベントを記録します: ランディングゾーンの作成または更新、OU の作成または削除、OU でのコントロールの有効化または無効化、Account Factory を使用した新規アカウントの作成または別の OU へのアカウントの移動。

AWS Control Tower は、複数の AWS サービスを使用して、ベストプラクティスのマルチアカウント AWS 環境を構築および管理します。AWS Control Tower アクションが完了するまで数分かかることがあります。CloudTrail ログでライフサイクルイベントを追跡して、元の AWS Control Tower アクションが正常に完了したかどうかを確認できます。EventBridge ルールを作成して、CloudTrail がラ

ライフサイクルイベントを記録したときに通知したり、オートメーションワークフローで次のステップを自動的にトリガーしたりすることができます。

2019 年 6 月 ~ 12 月

2019 年 6 月 24 日から 12 月 31 日までに、AWS Control Tower は次の更新をリリースしました。

- [AWS Control Tower バージョン 2.2 の一般提供](#)
- [AWS Control Tower の新しい選択的コントロール](#)
- [AWS Control Tower の新しい検出コントロール](#)
- [AWS Control Tower は、管理アカウントとは異なるドメインを持つ共有アカウントの E メールアドレスを受け付けます](#)
- [AWS Control Tower バージョン 2.1 の一般提供](#)

AWS Control Tower バージョン 2.2 の一般提供

2019 年 11 月 13 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「[ランディングゾーンを更新する](#)」を参照してください。)

AWS Control Tower バージョン 2.2 では、アカウントのドリフトを防止する 3 つの新しい予防コントロールが用意されています。

- [AWS Control Tower によって設定された Amazon CloudWatch Logs ロググループへの変更を許可しない](#)
- [AWS Control Tower によって作成された AWS Config 集約認可の削除を禁止する](#)
- [ログアーカイブの削除を許可しない](#)

コントロールは、AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。AWS Control Tower ランディングゾーンを作成するとき、ランディングゾーンとすべての組織単位 (OU、Organizational Unit)、アカウント、リソースは、選択したコントロールによって適用されるガバナンスルールに準拠します。ユーザーおよび組織のメンバーがランディングゾーンを使用する際、コンプライアンスステータスが (偶発的または意図的に) 変更されることがあります。ドリフト検出は、ドリフトを解決するために変更や設定更新が必要になるリソースを識別するのに役立ちます。詳細については、「[AWS Control Tower でドリフトを検出および解決する](#)」を参照してください。

AWS Control Tower の新しい選択的コントロール

2019 年 9 月 5 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower には、次の 4 つの新しい選択的コントロールが含まれるようになりました。

- [MFA を使用しない Amazon S3 バケットでの削除アクションを許可しない](#)
- [Amazon S3 バケットのレプリケーション設定の変更を許可しない](#)
- [ルートユーザーとしてのアクションを許可しない](#)
- [ルートユーザーのアクセスキーの作成を許可しない](#)

コントロールは、AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。ガードレールを使用すると、ポリシーの意図を表現できます。詳細については、「[About controls in AWS Control Tower](#)」を参照してください。

AWS Control Tower の新しい検出コントロール

2019 年 8 月 25 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower には、次の 8 つの新しい検出コントロールが含まれるようになりました。

- [Amazon S3 バケットのバージョニングが有効になっているかどうかを検出する](#)
- [AWS コンソールの IAM ユーザーに対して MFA が有効になっているかどうかを検出する](#)
- [IAM ユーザーに対して MFA が有効になっているかどうかを検出する](#)
- [Amazon EC2 インスタンスに対して Amazon EBS 最適化が有効になっているかどうかを検出する](#)
- [Amazon EBS ボリュームが Amazon EC2 インスタンスにアタッチされているかどうかを検出する](#)
- [Amazon RDS データベースインスタンスへのパブリックアクセスが有効になっているかどうかを検出する](#)
- [Amazon RDS データベーススナップショットへのパブリックアクセスが有効になっているかどうかを検出する](#)
- [Amazon RDS データベースインスタンスに対してストレージ暗号化が有効になっているかどうかを検出する](#)

コントロールは、AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。検出コントロールは、ポリシー違反など、アカウント内のリソースの非準拠を検出し、ダッシュボードを通じてアラートを提供します。詳細については、「[About controls in AWS Control Tower](#)」を参照してください。

AWS Control Tower は、管理アカウントとは異なるドメインを持つ共有アカウントの E メールアドレスを受け付けます

2019 年 8 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、ドメインが管理アカウントの E メールアドレスと異なる共有アカウント (ログアーカイブと監査メンバー) および子アカウント (Account Factory を使用して提供) の E メールアドレスを送信できるようになりました。この機能は、新しいランディングゾーンを作成する場合、および新しい子アカウントをプロビジョニングする場合にのみ使用できます。

AWS Control Tower バージョン 2.1 の一般提供

2019 年 6 月 24 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「[Update Your Landing Zone](#)」を参照してください。)

AWS Control Tower は、本番稼働用に一般提供され、サポートされるようになりました。AWS Control Tower は、複数のアカウントを持つ組織と、新しいマルチアカウント AWS 環境を設定し、大規模に管理するための最も簡単な方法を探しているチームを対象としています。AWS Control Tower を使用すると、組織のアカウントが確立されたポリシーに確実に準拠するようにすることができます。分散チームのエンドユーザーは、新しい AWS アカウントを迅速にプロビジョニングできます。

AWS Control Tower を使用すると、を使用した[マルチアカウント構造](#)の設定、を使用したユーザー ID とフェデレーティッドアクセスの管理 AWS Organizations、Service Catalog によるアカウントプロビジョニングの有効化 AWS IAM アイデンティティセンター、AWS CloudTrail とを使用した一元的なログアーカイブの作成などのベストプラクティスを採用する[ランディングゾーンを設定できます](#) AWS Config。

継続的なガバナンスのために、セキュリティ、運用、コンプライアンスに関する明確に定義されたルールである事前構成済みのコントロールを有効にできます。ガードレールは、ポリシーに準拠し

ないリソースのデプロイを防止し、デプロイされたリソースの不適合を継続的に監視するのに役立ちます。AWS Control Tower ダッシュボードは、プロビジョニングされたアカウント、有効なコントロール、アカウントのコンプライアンスステータスなど、AWS 環境を一元的に可視化します。

AWS Control Tower コンソールで 1 回クリックするだけで、新しいマルチアカウント環境を設定できます。AWS Control Tower を使用するのに追加料金や前払いの義務はありません。ランディングゾーンの設定と選択したコントロールの実装を有効にした AWS サービスに対してのみ料金が発生します。

ドキュメント履歴

- ドキュメントの最終更新日: 2025 年 12 月 30 日

次の表は、「AWS Control Tower ユーザーガイド」に対する重要な変更点の一覧です。ドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
マネージドポリシーの更新	AWS ControlTowerAccountServiceRolePolicy を更新しました。	2025 年 12 月 30 日
AWS Control Tower ランディングゾーンバージョン 4.0 と専用コントロール環境	AWS Control Tower ランディングゾーンバージョン 4.0 が、オプションのサービス統合と専用のコントロール環境で利用可能になりました	2025 年 11 月 17 日
AWS Control Tower には追加の 279 個の AWS Config コントロールが含まれています	Control Catalog を更新し、追加の 279 AWS Config コントロールを追加しました。	2025 年 11 月 14 日
マネージドポリシーの更新	AWS ControlTowerAccountServiceRolePolicy を更新しました。	2025 年 11 月 10 日
マネージドポリシーの更新	AWS ControlTowerServiceRolePolicy を更新して、ランディングゾーン 4.0 のオプション AWS CloudTrail 統合をサポートしました。Amazon CloudWatch Logs リソースパターンが <code>aws-controltower/CloudTrailLogs:*</code> に変更 <code>aws-controltower/CloudTrail</code>	2025 年 11 月 5 日

Logs*: * され、一意のサフィックスを持つロググループを管理できるようになりました。この下位互換性の更新により、お客様は、名前の競合を避けるために、ロググループを毎回一意のサフィックスで再作成して、AWS CloudTrail 統合を複数回有効または無効にできます。

[新しいマネージドポリシー](#)

[AWS ControlTowerCloudTrailRolePolicy](#) 管理ポリシーのドキュメントを追加しました。この管理ポリシーは、AWS ControlTowerCloudTrailRole が以前に使用していたインラインポリシーを置き換え、お客様の介入なしにポリシー AWS を更新できるようにします。

2025 年 11 月 5 日

[AWS Control Tower が、アジアパシフィック \(ニューージーランド\) リージョンで利用可能に](#)

AWS Control Tower は、ニューージーランドのオークランドリージョンで利用可能です。

2025 年 10 月 28 日

[AWS Control Tower が自動アカウント登録をサポート](#)

アカウントの自動登録と OU 間の移動。

2025 年 10 月 15 日

[マネージドポリシーの更新、新しいマネージドポリシー](#)

[AWS ControlTowerServiceRolePolicy](#) を更新し、新しい [AWS ControlTowerIdentityCenterManagementPolicy](#) を追加しました。

2025 年 10 月 14 日

[AWS Control Tower が Python バージョンを更新](#)

AWS Control Tower 環境で更新された Python バージョン

2025 年 9 月 3 日

AWS Control Tower が IPv6 をサポート	AWS Control Tower で IPv6 エンドポイントのサポートが追加されました。	2025 年 8 月 18 日
Account Factory for Terraform バージョン 1.15.0	AFT バージョン 1.15.0 が利用可能です。	2025 年 7 月 28 日
Nitro インスタンスタイプでコントロールを更新	8 つのプロアクティブコントロールを更新し、新しいインスタンスタイプを追加しました。	2025 年 7 月 24 日
AWS Control Tower がアジアパシフィック (台北) で利用可能に	AWS Control Tower がアジアパシフィック (台北) のサポートを追加しました。	2025 年 7 月 23 日
AWS Control Tower がサポートする AWS PrivateLink	AWS Control Tower で AWS PrivateLink のサポートが追加されました。	2025 年 6 月 30 日
サービスにリンクされた AWS Config コントロール	AWS Control Tower は、サービスにリンクされた AWS Config コントロールをデプロイします。	2025 年 6 月 12 日
拡張メタデータ。追加のコントロール、新しいフレームワーク	AWS Control Tower は、から追加の統合コントロールを導入し AWS Config、Control Catalog 内のすべてのコントロールのメタデータを強化し、より多くの業界フレームワークをサポートします。	2025 年 6 月 12 日
有効なコントロールビュー	AWS Control Tower は、有効なコントロールの包括的なコンソールビューを導入しています。	2025 年 5 月 21 日

AFT が新しい設定をサポート	AWS Control Tower AFT は、デプロイ時に 3 つの追加オプション設定をサポートしています。	2025 年 5 月 13 日
拡張ベースライン	AWS Control Tower がベースラインドリフトを報告するようになりました。	2025 年 5 月 12 日
AWS Control Tower が AWS アジアパシフィック (タイ) およびメキシコ (中部) リージョンで利用可能に	アジアパシフィック (タイ) とメキシコ (中部) の リージョンが利用可能です。	2025 年 5 月 9 日
AWS Control Tower が 233 個の AWS Config コントロールを追加	新しい Config コントロール、メタデータテーブルの刷新、リージョンテーブル、グローバル識別子ページを追加しました。	2025 年 4 月 11 日
AWS Control Tower がサービスにリンクされたロールを更新	AWSControlTowerAccountServiceRolePolicy に更新します。	2024 年 12 月 10 日
AWS Control Tower CfCT が GitHub をサポート	サードパーティー設定ソースの新しいオプション。	2024 年 12 月 9 日
宣言型ポリシーを使用した AWS Control Tower 予防コントロール	新しいタイプのポリシーは、新しいタイプの予防コントロールを実装します。	2024 年 12 月 1 日
AWS Control Tower と AWS Backup の統合	AWS Control Tower リソースをバックアップするプランを設定できます。	2024 年 11 月 25 日
AWS Control Tower は AWS Config コントロールを統合します	AWS Control Tower は、選択した AWS Config コントロールを統合します。	2024 年 11 月 21 日

AWS Control Tower のフック管理が向上	AWS Control Tower がプロアクティブコントロールのフックを管理するようになりました。	2024 年 11 月 20 日
コントロールポリシードリフトの報告	AWS Control Tower は、新しいタイプのドリフトを報告します。	2024 年 11 月 15 日
AWS Control Tower がマネージドリソースコントロールポリシーを起動	RCP で実装された新しいタイプの予防コントロール。	2024 年 11 月 15 日
AWS Control Tower が ResetEnabledControl API を追加	コントロールドリフトを管理する新しい API。	2024 年 11 月 14 日
GetControl API を更新	GetControl の 2 つの新しいコントロールフィールド。	2024 年 11 月 8 日
AWS Control Tower AFT が GitLab をサポート	サードパーティー設定ソースの新しいオプション。	2024 年 10 月 23 日
AWS アジアパシフィック (マレーシア) リージョンで AWS Control Tower が利用可能に	新しいリージョンであるマレーシア (クアラルンプール) が利用可能になりました。	2024 年 10 月 21 日
AWS Control Tower が OU あたり最大 1000 アカウントをサポート	OU あたりのアカウント数の制限が引き上げられました。	2024 年 8 月 30 日
AWS Control Tower でランディングゾーンバージョンの選択が可能に	3.1 以降を実行している場合は、最新バージョンに移行せずにランディングゾーンを更新または修復できます。	2024 年 8 月 15 日

GetControl および ListControls API オペレーションが利用可能に	2 つの新しい Control Catalog オペレーションは、コントロールの詳細情報を確認するのに役立ちます。	2024 年 8 月 6 日
AWS Control Tower がオプトインリージョンで AFT と CfCT をサポート	AFT と CfCT は追加で利用できます AWS リージョン。	2024 年 7 月 18 日
AWS Control Tower に ListLandingZoneOperations API を追加	ランディングゾーンの最近のオペレーションを取得できる新しい API。	2024 年 6 月 26 日
AWS Control Tower が最大 100 の同時コントロールオペレーションをサポート	同時コントロールオペレーションのクォータが 100 に引き上げられました。	2024 年 5 月 20 日
AWS カルガリー西部 (カナダ) リージョンで AWS Control Tower が利用可能に	AWS Control Tower がカナダ西部 (カルガリー) リージョンで利用可能になりました。	2024 年 5 月 3 日
AWS Control Tower がセルフサービスのクォータ調整をサポート	AWS Control Tower は、コンソールの AWS Service Quotas と統合されています。	2024 年 4 月 25 日
コントロールのドキュメントを新しいガイドに移動	AWS Control Tower の「Controls Reference Guide」が発行されました。	2024 年 4 月 21 日
でのEnabledControl リソースのタグ付け CloudFormation	AWS Control Tower は、CloudFormation テンプレートを使用した EnabledControl リソースへのタグの追加をサポートします。	2024 年 2 月 22 日

ベースライン API が利用可能に	AWS Control Tower が OU をプログラムによって登録するための新しい API をリリースしました。	2024 年 2 月 14 日
AWS Control Tower ランディングゾーンバージョン 3.3	AWS Control Tower ランディングゾーンバージョン 3.3 が利用可能になりました。	2023 年 12 月 14 日
AWS Control Tower がデジタル主権を支援するコントロールを発表	AWS Control Tower は、お客様のデジタル主権の要件を支援する一連のコントロールをリリースしました。	2023 年 11 月 27 日
AWS Control Tower がランディングゾーン API をサポート	AWS Control Tower は、新しい API を使用したランディングゾーンの設定と起動をサポートします。	2023 年 11 月 26 日
AWS Control Tower が、有効になっているコントロールのタグ付けをサポート	AWS Control Tower では、コンソールから、および新しい API により、有効になっているコントロールのタグ付けがサポートされます。	2023 年 11 月 10 日
アジアパシフィック (メルボルン) で AWS Control Tower が利用可能に AWS リージョン	アジアパシフィック (メルボルン) リージョンで利用可能。	2023 年 11 月 3 日
新しいコントロール API が利用可能に	AWS Control Tower が新しいコントロール API をリリースしました。	2023 年 10 月 14 日
AWS Control Tower が新しいコントロールをリリース	AWS Control Tower が新しいプロアクティブコントロールと検出コントロールをリリースしました。	2023 年 10 月 5 日

<u>AWS Control Tower が信頼できるアクセスの無効化に伴うドリフトを報告</u>	お客様が AWS Organizations で AWS Control Tower への信頼できるアクセスをオフにした際にドリフトが発生すると、AWS Control Tower から通知されます。	2023 年 9 月 21 日
<u>AWS Control Tower が 4 つの追加で利用可能に AWS リージョン</u>	アジアパシフィック (ハイデラバード)、欧州 (スペインおよびチューリッヒ)、中東 (アラブ首長国連邦) で利用可能です。	2023 年 9 月 13 日
<u>AWS Control Tower がテルアビブリージョンで利用可能に</u>	AWS Control Tower が、テルアビブリージョン (il-central-1) で利用可能になりました。	2023 年 8 月 28 日
<u>AWS Control Tower が 28 個の新しいプロアクティブコントロールをリリース</u>	AWS Control Tower が 28 個の新しいプロアクティブコントロールをリリースしました。	2023 年 7 月 24 日
<u>AWS Control Tower で 2 つのコントロールが廃止されます</u>	AWS Control Tower は、2023 年 8 月 18 日にコントロールライブラリから 2 つのコントロールを削除しました。	2023 年 7 月 18 日
<u>AWS Control Tower ランディングゾーン 3.2 が利用可能に</u>	AWS Control Tower ランディングゾーンバージョン 3.2 が利用可能になりました。	2023 年 6 月 16 日
<u>AWS Control Tower は、ID に基づいてアカウントを処理します</u>	AWS Control Tower は、AWS アカウントの E メールアドレスではなく、アカウント ID を追跡します。	2023 年 6 月 14 日

[追加の Security Hub CSPM 検出コントロールが利用可能に](#)

AWS Control Tower は、Security Hub CSPM Service-Managed Standard: AWS Control Tower のコントロールライブラリに 10 個の新しいコントロールを追加します。

2023 年 6 月 12 日

[AWS Control Tower はコントロールメタデータテーブルを公開します](#)

AWS Control Tower では、公開されたドキュメントの一部としてコントロールメタデータのテーブルが提供されるようになりました。

2023 年 6 月 7 日

[Account Factory のカスタマイズに対する Terraform サポート](#)

AFC の Terraform オープンソースブループリントの単一リージョンサポート。

2023 年 6 月 6 日

[AWS ランディングゾーンで利用可能な IAM 自己管理](#)

AWS Control Tower では、お客様がランディングゾーンの ID プロバイダーを選択できるようになりました。

2023 年 6 月 6 日

[新しいロールが追加されました](#)

AWS Control Tower に、サービスにリンクされた新しいロール `AWSServiceRoleForAWSControlTower` と、関連するポリシー `AWSServiceRoleForAWSControlTower` が追加されました。

2023 年 6 月 1 日

[混合ガバナンスの更新](#)

混合ガバナンスについてお客様にアドバイスするための更新

2023 年 6 月 1 日

[追加のプロアクティブコントロールが利用可能になりました](#)

新しいプロアクティブコントロールは、マルチアカウント環境を管理し、特定のコントロール目標を達成するのに役立ちます。

2023 年 5 月 19 日

[リージョンがさらに 7 つ利用可能になりました](#)

AWS Control Tower が AWS リージョン、北カリフォルニア (サンフランシスコ)、アジアパシフィック (香港、ジャカルタ、大阪)、欧州 (ミラノ)、中東 (バーレーン)、アフリカ (ケープタウン) の 7 つの追加で利用可能になりました。

2023 年 4 月 19 日

[マネージドポリシーへの変更](#)

AWSControlTowerServiceRolePolicy を変更しました。EnableRegion ListRegions GetRegion OptStatus APIs AWS

2023 年 4 月 6 日

[アカウントカスタマイズリクエストのトレースが一般利用可能に](#)

AWS Control Tower では、Account Factory for Terraform (AFT) のワークフローを使用して、アカウントのカスタマイズリクエストを追跡できるようになりました

2023 年 2 月 16 日

[IAM ベストプラクティスの更新](#)

IAM ベストプラクティスの推奨事項に合わせてガイドを更新しました。詳細については、「[IAM でのセキュリティのベストプラクティス](#)」を参照してください。

2023 年 2 月 15 日

AWS Control Tower ランディングゾーンバージョン 3.1 が利用可能に	AWS Control Tower ランディングゾーンバージョン 3.1 が利用可能になりました。	2023 年 2 月 9 日
プロアクティブコントロールの一般公開	プロアクティブコントロールはプレビュー版から一般公開に変わりました。	2023 年 1 月 24 日
同時アカウント操作	AWS Control Tower で、最大 5 つの Account Factory の同時実行アクションがサポートされるようになりました。一度に最大 5 つのアカウントを作成、更新、または登録できるようになります。	2022 年 12 月 16 日
プロアクティブコントロールによるリソースのプロビジョニングのサポート	AWS Control Tower は、CloudFormation フックを介して実装されたプロアクティブコントロールをサポートするようになりました。	2022 年 11 月 28 日
Account Factory Customization が利用可能に	AWS Control Tower で、ブループリントと呼ばれるカスタマイズ可能なアカウントテンプレートを使用するアカウントのプロビジョニングが AWS Control Tower コンソールから直接実行できるようになりました。	2022 年 11 月 28 日
すべての AWS Config ルールでコンプライアンスステータスを表示可能	AWS Control Tower は、AWS Control Tower に登録された組織単位にデプロイされたすべての AWS Config ルールのコンプライアンスステータスを表示するようになりました。	2022 年 11 月 18 日

マネージドポリシーへの変更	Account Factory Customization に必要な AWSControlTowerBlueprintAccess ロールを AWS Control Tower が引き継ぐことができるように、AWSControlTowerServiceRolePolicy が変更されました。	2022 年 10 月 28 日
コントロールAPIs、CloudFormation リソース	AWS Control Tower は、一連の API コールと新しい CloudFormation リソースによるコントロールのアクティブ化と非アクティブ化をサポートするようになりました。	2022 年 9 月 1 日
CfCT がスタックセットの削除をサポート	CfCT は、マニフェストファイルにパラメータを設定することにより、スタックセットの削除をサポートします。	2022 年 8 月 26 日
カスタマイズされたログの保持	AWS Control Tower CloudTrail ログを日単位または年単位で最大 15 年まで保存するという Amazon S3 バケットの保持ポリシーをカスタマイズできます。	2022 年 8 月 15 日
ロールドリフト修理可能	AWS Control Tower は、ランディングゾーンを完全に修理しない状態のロールドリフトの修理をサポートします。	2022 年 8 月 11 日

[バージョン 3.0 が利用可能](#)

AWS Control Tower ランディングゾーンバージョン 3.0 は、アカウントベースの AWS CloudTrail 証跡から組織ベースの証跡に変更され、管理ポリシーを更新して組織レベルの証跡を有効にします。これにより、ホームリージョンでのみ AWS Config 情報を集約できます。バージョン 3.0 には、リージョン拒否コントロールと 2 つの新しい検出コントロールも含まれています。

2022 年 7 月 29 日

[OU とアカウントのビューが 組み合わされた組織ページ](#)

AWS Control Tower の新しい [Organization] (組織) ページには、すべての組織単位 (OU) とアカウントの階層的なビューが表示されます。

2022 年 7 月 18 日

[マネージドポリシーへの変更](#)

AWSControlTowerServiceRolePolicy を変更し、お客様が組織レベルの AWS CloudTrail 証跡を使用して AWS CloudTrail ログを集約できるようにしました。

2022 年 6 月 20 日

[メンバーアカウントの登録と更新が容易に](#)

AWS Control Tower では、ランディングゾーン内から、メンバーアカウントを個別に登録および更新することができるようになりました。各アカウントには更新がいつ利用可能かが表示されます。Account Factory の [Create] (作成) アカウントワークフローから [Enroll account] (アカウントの登録) ボタンを分離しました。

2022 年 5 月 31 日

[AFT は共有アカウントのカスタマイズをサポートしています](#)

AWS Control Tower Account Factory for Terraform は、AWS Control Tower の管理アカウント、ログアーカイブ、監査アカウントのカスタマイズをサポートするようになりました。

2022 年 5 月 27 日

[すべてのオプションのコントロールの同時操作](#)

AWS Control Tower では、オプションの予防ガードレールと検出コントロールを同時に適用または削除できるようになりました。

2022 年 5 月 18 日

[既存のセキュリティアカウントとログアカウント](#)

AWS Control Tower は、ランディングゾーンのセットアップ中に新しいアカウントを作成するのではなく、既存のセキュリティアカウントとログアカウントを持ち込む機能をサポートするようになりました。

2022 年 5 月 16 日

[バージョン 2.9 が利用可能に](#)

AWS Control Tower のランディングゾーンバージョン 2.9 は、Python バージョン 3.9 ランタイムを使用するように通知フォワーダー Lambda を更新します。

2022 年 4 月 22 日

[AWS ベストプラクティス、バージョン 2.8 のサポートを更新](#)

AWS Control Tower ランディングゾーンバージョン 2.8 では、ワークロードと AWS アカウントが AWS ベストプラクティスと一致していることを確認するためのサポートが追加されています。

2022 年 2 月 10 日

[リージョン拒否コントロール](#)

AWS Control Tower に、コンプライアンスと規制の問題に対処するために、AWS リージョンへのアクセスを制限するのに役立つコントロールが追加されました。

2021 年 11 月 30 日

[データレジデンシーコントロール](#)

AWS Control Tower で、きめ細かな制御によるデータの所在場所管理に役立つコントロールがサポートされるようになりました。

2021 年 11 月 30 日

[AWS Control Tower Account Factory for Terraform](#)

AWS Control Tower では、自動化されたアカウントのプロビジョニングと更新のために Terraform がサポートされるようになりました。

2021 年 11 月 29 日

新しいライフサイクルイベントが利用可能に	PrecheckOrganizationalUnit イベントは、ネストされた OU のリソースを含め、[Extend governance] (ガバナンスを拡張) タスクが成功しないようリソースがブロックしているかどうかを記録します。	2021 年 11 月 18 日
ネストされた OU が利用可能に	AWS Control Tower では、ランディングゾーンにネストされた OU 構造を含めることができるようになりました。	2021 年 11 月 16 日
検出コントロールの同時実行性	AWS Control Tower の検出コントロールで、同時有効化および無効化操作がサポートされるようになりました。	2021 年 11 月 5 日
2 つの新しいリージョンが利用可能に	AWS Control Tower が欧州 (パリ) AWS リージョンと南米 (サンパウロ) リージョンの 2 つの新しいリージョンで利用可能になりました。	2021 年 7 月 29 日
リージョンの選択解除	AWS Control Tower を通じて管理しなくなった AWS リージョンの選択を解除できます。	2021 年 7 月 29 日
KMS キーが利用可能に	必要に応じて、管理する KMS キーを作成または選択して、データとリソースを暗号化できます。	2021 年 7 月 28 日

マネージドポリシーへの変更	お客様が AWS CloudTrail ログに独自の KMS 暗号化キーを使用できるように、AWSControlTowerServiceRolePolicy を変更しました。	2021 年 7 月 28 日
コントロールの名前を変更、機能は変更なし	コントロールのポリシーの意図をより適切に反映するように、一部のコントロールの名前と説明が更新されました。機能に変更はありません。	2021 年 7 月 26 日
マネージド SCP の自動スキャン	AWS Control Tower は、マネージド SCP を毎日自動スキャンしてドリフトをチェックします。	2021 年 5 月 11 日
OU とアカウントのカスタマイズされた名前	AWS Control Tower では、ランディングゾーンのセットアッププロセス中に、重要な OU とアカウントに対して、ドリフトを生成せずに、カスタマイズした名前を指定できます。	2021 年 4 月 16 日
ランディングゾーンの廃止がセルフサービスに	AWS Control Tower では、AWS Support に連絡することなく、ランディングゾーンを廃止できるようになりました。廃止は半自動プロセスであり、元に戻すことはできません。すべての AWS Control Tower リソースを手動で削除することとは異なります。	2021 年 4 月 9 日

3 つの追加リージョン

AWS Control Tower が、アジアパシフィック (東京) AWS リージョン、アジアパシフィック (ソウル) リージョン、アジアパシフィック (ムンバイ) リージョンの 3 つの追加リージョンで利用可能になりました。

2021 年 4 月 8 日

新しいログアーカイブコントロール、ランディングゾーンバージョン 2.7 が利用可能に

4 つの新しいログアーカイブコントロールは、AWS Control Tower の外部リソースのガバナンスとは別に、AWS Control Tower リソースに対するログアーカイブのガバナンスを提供します。既存の 4 つのコントロールに関するガイダンスが、必須から選択式に変更されました。AWS Control Tower のランディングゾーンバージョン 2.7 には HTTPS の要件が含まれており、更新後に元に戻すことはできません。

2021 年 4 月 8 日

[リージョンの選択](#)

AWS Control Tower リージョンを選択すると、AWS Control Tower リソースの地理的フットプリントをより適切に管理できます。コンプライアンス、規制、コスト、その他の理由から、AWS リソースまたはワークロードをホストするリージョンの数を増やすために、管理するリージョンを追加で選択できるようになりました。

2021 年 2 月 19 日

[OU を登録し、AWS Control Tower ですべてのアカウントを一度に管理する](#)

AWS Control Tower では、OU を登録する機能が追加されています。この方法により、複数のアカウントを同時にガバナンスの対象とすることができます。

2021 年 1 月 28 日

[登録された OU での複数のアカウントの更新](#)

AWS Control Tower ダッシュボードから、最大 300 個のアカウントを含む登録済み AWS Organizations 組織単位 (OU) 内のすべてのアカウントをワンクリックで更新できるようになりました。複数アカウントの更新機能は一括更新とも呼ばれ、一度に 1 つのアカウントを更新したり、外部スクリプトを使用して複数のアカウントに対して更新を実行したりする必要がなくなります。

2021 年 1 月 28 日

[管理対象外の OU とアカウントを集約するための新しいロール](#)

新しいロールは外部 AWS Config ルールの検出に役立つため、AWS Control Tower はアンマネージドアカウントにアクセスする必要はありません。

2020 年 12 月 29 日

[AWS Control Tower は、より多くの AWS リージョンで利用できます。](#)

AWS Control Tower は、アジアパシフィック (シンガポール) リージョン、欧州 (フランクフルト) リージョン、欧州 (ロンドン) リージョン、欧州 (ストックホルム) リージョン、カナダ (中部) リージョンでデプロイできるようになりました。このリリースにより、AWS Control Tower が 10 AWS リージョンで利用可能になりました。このランディングゾーンの更新には、リストされているすべてのリージョンが含まれており、元に戻すことはできません。ランディングゾーンをバージョン 2.5 に更新したら、AWS Control Tower に登録されているすべてのアカウントを手動で更新して、サポートされている 10 の AWS リージョンで管理する必要があります。

2020 年 11 月 18 日

[コントロールの更新](#)

必須コントロール AWS-GR_IA M_ROLE_CHANGE_PROHIBITED の更新バージョンがリリースされました。更新されたコントロールでは、アカウントの自動登録が簡単になりました。

[AWS Control Tower の関連情報ページが利用可能に](#)

関連情報ページでは、AWS Control Tower のランディングゾーンを設定した後に役立つ一般的なタスクを簡単に探すことができます。

[AWS Control Tower コンソールに OU とアカウントの詳細が表示される](#)

AWS Control Tower コンソールでは、AWS アカウントと組織単位 (OUs) の詳細を表示できます。[Accounts] (アカウント) ページに、OU や AWS Control Tower の登録ステータスに関係なく、組織内のすべてのアカウントが一覧表示されるようになりました。すべてのテーブルで検索、並べ替え、フィルタリングを実行できるようになりました。

[AWS Control Tower により、 既存の組織でランディング ゾーンをセットアップ可能に](#)

既存の組織で AWS Control Tower のランディングゾーンを起動して、組織をガバナンスに組み込むことができるようになりました。AWS Control Tower のクイックアカウントプロビジョニング機能の名前が Enroll account に変更され、既存の AWS アカウントの登録と新しいアカウントの作成が可能になりました。

2020 年 4 月 16 日

[AWS Control Tower がアジア パシフィックで利用可能に](#)

AWS Control Tower がアジアパシフィック (シドニー) AWS リージョンでデプロイできるようになりました。このリリースでは、提供アカウントを手動で更新する必要があります。更新は、アジアパシフィック (シドニー) でワークロードを実行する場合にのみ行います。

2020 年 3 月 3 日

[AWS Control Tower のラン ディングゾーンの廃止が可能 に](#)

AWS サポートは、組織を保持するほぼ自動化されたプロセスを通じてランディングゾーンを完全に廃止するのに役立ちますが、手動でのクリーンアップが必要です。

2020 年 2 月 27 日

[クイックアカウントプロ
ビジョニングが AWS Control
Tower で利用可能に](#)

クイックアカウントプロ
ビジョニングでは、[Enroll
account] (アカウントの登録)
機能を使用して、ランディ
ングゾーンが最新の状態にな
ったときに新しいメンバーア
カウントをさらに簡単に起動
できるようになりました。

2020 年 2 月 20 日

[ライフサイクルイベントが
AWS Control Tower で追跡対
象に](#)

ライフサイクルイベントは、
一部のワークフローのオー
トメーションを容易にする
ため、特定の AWS Control
Tower イベントに関する詳細
を提供します。

2019 年 12 月 12 日

[AWS Control Tower で設定
ページとアクティビティペ
ージが利用可能に](#)

設定ページとアクティビティ
ページを使用すると、ラン
ディングゾーンの更新や、ロ
グに記録されたイベントの表
示が容易になります。

2019 年 11 月 30 日

[AWS Control Tower で追加の
予防コントロールが利用可能
に](#)

AWS Control Tower の予防コ
ントロールは、組織およびリ
ソースと、環境との整合性を
維持します。

2019 年 9 月 6 日

[AWS Control Tower で追加の
検出コントロールが利用可能
に](#)

AWS Control Tower の検出コ
ントロールは、組織の状態と
リソースに関する情報を提供
します。

2019 年 8 月 27 日

[AWS Control Tower が一般公
開](#)

AWS Control Tower は、マル
チアカウント AWS 環境を大
規模にセットアップおよび
管理する最も簡単な方法を提
供するサービスです。

2019 年 6 月 24 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「[AWS 用語集](#)」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。