AWS Control Tower

ユーザーガイド

AWS Control Tower: ユーザーガイド

Table of Contents

AWS Control Tower とは? 1
機能 1
関連サービス 1
料金 1
AWS Control Tower を初めてお使いになる方向けの情報 2
仕組み 2
共有アカウントは何ですか 2
ガードレールの仕組み 7
AWS リージョンと AWS Control Tower の連携の仕組み 8
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 8
AWS Control Tower と VPC 8
..... 8
VPC および AWS Control Tower の CIDR とピア接続 9
AWS Control Tower での VPC ピア接続のオプション 9
VPC と CIDR に関する注意事項 9
セットアップ 11
AWS にサインアップ 11
IAM ユーザーを作成する 11
MFA のセットアップ 13
次のステップ 13
開始方法 14
AWS Control Tower を使用するためのガイダンス 14
マスターアカウントの起動前チェック 15
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 15
ステップ 2: ランディングゾーンをセットアップする 16
次のステップ 16
ガードレール 18
考慮事項 18
オプションのガードレール 19
ガードレールの詳細 19
ガードレールの有効化 19
ガードレールリファレンス 20
必須のガードレール 20
強く推奨されるガードレール 31
選択的ガードレール 40
統合サービス 44
AWS CloudFormation 44
CloudTrail 44
CloudWatch 44
AWS Config 45
IAM 45
AWS Lambda 45
AWS Organizations 45
考慮事項 46
Amazon S3 46
AWS Service Catalog 46
AWS SSO 46
AWS Control Tower 用の AWS SSO グループ 47
Amazon SNS 50
Step Functions 50
Account Factory 51
AWS Service Catalog を介したアカウントの設定とプロビジョニング 51
Account Factory アカウントの更新 52
Amazon VPC 設定で Account Factory を設定する 53

メンバーアカウントの管理解除 54
Account Factory で作成したアカウントの解約 55
Account Factory の考慮事項 55
ドリフト 57
移動されたメンバーアカウント 57
解決策 58
追加されたメンバーアカウント 58
解決 58
削除されたメンバーアカウント 58
解決 59
計画外のマネージド SCP の更新 59
解決 59
管理された OU にアタッチされた SCP 59
解決 59
管理された OU からデタッチされた SCP 60
解決 60
メンバーアカウントにアタッチされた SCP 60
解決 60
管理された OU の削除 60
解決 61
セキュリティ 62
データ保護 62
保管時の暗号化 63
転送中の暗号化 63
コンテンツへのアクセスの制限 63
Identity and Access Management 63
認証 64
アクセスコントロール 65
アクセス管理の概要 65
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 68
ロギングとモニタリング 70
モニタリング 70
AWS CloudTrail を使用した AWS Control Tower アクションのログ記録 71
コンプライアンス検証 73
弾力 74
インフラストラクチャセキュリティ 74
設定更新管理 74
ランディングゾーンの更新 74
ドリフトの解決 75
制限 76
統合サービスの制限 76
チュートリアル 77
ウォークスルー: AWS Control Tower マネージドリソースのクリーンアップ 77
SCP の削除 77
StackSets およびスタックの削除 78
ログアーカイブアカウントでの Amazon S3 バケットの削除 79
Account Factory のクリーンアップ 79
ロールおよびポリシーのクリーンアップ 80
AWS Control Tower クリーンアップのヘルプ 81
チュートリアル: VPC を使用せずに AWS Control Tower を設定する 81
AWS Control Tower マスターアカウント VPC の削除 81
VPC なしのアカウントを AWS Control Tower で作成する 82
トラブルシューティング 84
ランディングゾーンの起動の失敗 84
AWS Control Tower 外部で E メールアドレスを変更しないでください。 84
アカウントの組織単位を AWS Control Tower 外に移行しない 84
ドキュメント履歴 85

AWS の用語集 86

AWS Control Tower とは?

AWS Control Tower では、数千の企業との連携で確立されたベストプラクティスに基づいて、安全性と適合性を備えた、複数アカウントの AWS 環境を設定および管理する最も簡単な方法が利用できます。AWS Control Tower を使用すると、分散したチームのエンドユーザーが、新しい AWS アカウントチームをすばやくプロビジョニングできます。中央のクラウド管理者には、すべてのアカウントが、一元的に確立された、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が通知されます。

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 – Landing Zone 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 AWS 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。
- ガードレール – ガードレールは、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。これは、わかりやすい形式で表されます。ガードレールには、予防的と発見的の 2 種類があります。この 2 種類のガードレールには、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。ガードレールの詳細については、「ガードレールの仕組み (p. 7)」を参照してください。
- Account Factory – An 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 では、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 が利用できます。詳細については、「Account Factory (p. 51)」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 Landing Zone 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ガードレール、ポリシーの非準拠の継続的検出に対応するガードレール、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。

関連サービス

AWS Control Tower は、AWS Service Catalog、AWS シングルサインオン、AWS Organizations など、信用と信頼性のある AWS のサービス上に構築されています。詳細については、「統合サービス (p. 44)」を参照してください。

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 のサービスおよび Landing Zone で利用するサービスの料金のみをお支払いいただきます。たとえば、Account Factory でアカウントをプロビジョニングするための AWS Service Catalog の料金、および Landing Zone で追跡されているイベントの AWS CloudTrail に対してお支払いいただきます。AWS Control Tower に関連した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 を初めてお使いになる方向けの情報

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. 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 (p. 14)」を参照してください。
2. ドリフトの検出と防止の詳細については、「AWS Control Tower でのドリフトの検出および解決 (p. 57)」を参照してください。
3. セキュリティの詳細については、「AWS Control Tower でのセキュリティ (p. 62)」を参照してください。
4. Landing Zone 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 (p. 74)」を参照してください。

AWS Control Tower の仕組み

次に、AWS Control Tower 仕組みについて大まかに説明します。Landing Zone は、すべての AWS リソースに対する優れた設計の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 アカウントでコンプライアンス規制を適用できます。

共有アカウントは何ですか

AWS Control Tower では、3 つの共有アカウント (マスターアカウント、ログアーカイブアカウント、および監査アカウント) があります。これらは、Account Factory にプロビジョニングされません。

Landing Zone を作成すると、多くの 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、Landing Zone の状態が不明になります。

> **Important**
>
> 強く推奨されるガイダンスでガードレールを有効にすると、アカウント内で AWS Control Tower マネージド AWS リソースが作成されます。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、ガードレールの状態が不明になる可能性があります。詳細については、「ガードレールリファレンス (p. 20)」を参照してください。

マスターアカウントとは何ですか

これは、Landing Zone 専用に作成したアカウントです。このアカウントは、Landing Zone 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 とガードレールの管理だけでなく、Account Factory プロビジョニングとアカウントに使用することもできます。

Landing Zone をセットアップすると、マスターアカウント内で以下の 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 Organizations	アカウント	audit log archive
AWS Organizations	OU	Core Custom

AWS サービス	リソースタイプ	リソース名
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
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL 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
AWS Service Catalog	製品	AWS Control Tower Account Factory
AWS CloudTrail	証跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs
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 サービス	リソースタイプ	リソース名
AWS シングルサインオン	ディレクトリグループ	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS シングルサインオン	アクセス権限セット	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

ログアーカイブアカウントとは何ですか

このアカウントは、Landing Zone 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のリポジトリとして使用されます。

Landing Zone をセットアップすると、ログアーカイブアカウント内で以下の 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-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-

AWS サービス	リソースタイプ	リソース名
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
AWS Config	AWS Config ルール	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIB AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIE
AWS CloudTrail	証跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder
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-*

監査アカウントとは何ですか

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 Landing Zone 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。

Landing Zone をセットアップすると、監査アカウント内で以下の 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-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED- StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-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_PROHIB AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIB
AWS CloudTrail	証跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs

AWS サービス	リソースタイプ	リソース名
		/aws/lambda/aws-controltower-NotificationForwarder
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-SecurityAdministratorRole aws-controltower-SecurityReadOnlyRole 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

ガードレールの仕組み

ガードレールは、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。各ガードレールは 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。コンプライアンスのニーズは進化します。これに応じて、有効になっている選択的ガードレールまたは強く推奨されるガードレールを AWS Control Tower コンソールからいつでも変更できます。必須ガードレールは常に適用され、変更することはできません。

予防的ガードレールにより、アクションの発生が防止されます。たとえば、[Disallow policy changes to log archive (ログアーカイブのポリシー変更を禁止する)] ガードレールにより、ログアーカイブ共有アカウント内で IAM ポリシーの変更が防止されます。禁止されたアクションを実行しようとすると、拒否され、CloudTrail に記録されます。また、リソースも AWS Config に記録されます。

発見的ガードレールにより、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。たとえば、[Enable encryption for EBS volumes attached to EC2 instances (EC2 インスタンスにアタッチされた EBS ボリュームの暗号化を有効にする)] により、暗号化されていな

い Amazon EBS ボリュームが Landing Zone の EC2 インスタンスにアタッチされているかどうかが検出されます。

関連トピック

- AWS Control Tower のガードレール (p. 18)
- AWS Control Tower でのドリフトの検出および解決 (p. 57)

AWS リージョンと AWS Control Tower の連携の仕組み

現在、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)
- 欧州 (アイルランド)

Landing Zone 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 AWS 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。

現在、すべての予防的ガードレールはグローバルに使用できます。ただし、発見的ガードレールは 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。

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

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。AWS Organizations は、アカウントを作成する際に、このアカウント内にロールを作成します。このロールに対して AWS Control Tower は API にパラメータを渡すことで名前を付けます。名前は `AWSControlTowerExecution` となります。

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` ロールを引き受けます。AWS Control Tower は、このロールを使用してアカウントのベースライニングを行い、必須ガードレール (および他の有効なガードレール) 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は、設計図とガードレールを設定するプロセスです。ベースライニングのプロセスでは、設計図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 と VPC

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。

AWS Control Tower と VPC に関する重要な事実を以下に示します。

- 各 AWS Control Tower アカウントには 1 つの VPC が許可されます。
- 各 VPC には 3 つのアベイラビリティーゾーンがあります。デフォルトでは、アベイラビリティーゾーンごとに 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あります。したがって、デフォルトでは、VPC ごとに 9 つのサブネットがあります。
- VPC 内の 9 つのサブネットのそれぞれに、同じサイズの一意の範囲が割り当てられます。
- IP アドレスは重複しないため、VPC 内の 9 つのサブネットは無制限に相互間で通信できます。

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。

VPC 内のサブネットの数は設定可能です。VPC のサブネット設定を変更する詳しい方法については、「Account Factory トピック」を参照してください。

VPC および AWS Control Tower の CIDR とピア接続

VPC の CIDR 範囲を選択すると、AWS Control Tower は キャリアグレード NAT (CGN) を適用し、Account Factory は RFC 1918 仕様に従って IP アドレス範囲を検証します。また、Account Factory は `10.0.0.0/16`、`172.16.0.0/16`、`192.168.0.0/16` の IP 範囲を許可します。指定した範囲がそ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。

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、マスターアカウントと、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。この実装では、VPC から AWS Control Tower OU 内の他の VPC へのピア接続は許可されません。

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。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ず、VPC と VPC 間のピア接続は許可されません。

デフォルトの CIDR 範囲は `172.31.0.0/16` です。

AWS Control Tower での VPC ピア接続のオプション

AWS Control Tower は、ピア接続の代わりに、AWS Control Tower VPC 間 の VPC ピア接続の推奨ソリューションとして、AWS PrivateLink を介した VPC エンドポイントサービスを提供しています。パケットは、ある VPC 内の特定の IP アドレスから、別の VPC 内の別の特定の IP アドレスに直接送信できます。

ただし、別のオプションを使用できます。AWS Control Tower 内では、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。たとえば、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。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。

VPC と CIDR に関する注意事項

一部のネットワーク管理者は、アカウントの CIDR 設定を変更することなく、2 つの異なる VPC 間 (つまり、2 つの異なるアカウント間) で 2 つのサブネットをピア接続できることに気付くことがあります。VPC 内の 9 つのサブネットは重複しないため、たとえば [VPC1、サブネット 1] から [VPC2、サブネット 2]へ

ピア接続することは技術的には可能です。ただし、このアプローチは、VPC 内でサブネット範囲がどのように割り当てられているかの実装の詳細に左右されます。このピア接続方法はいつでも失敗する可能性があるため、お勧めしません。

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。

セットアップ

AWS Control Tower を初めて使用する場合は、事前に以下のタスクをすべて実行してください。

1. AWS にサインアップ (p. 11)
2. IAM ユーザーを作成する (p. 11)

これらのタスクでは、AWS アカウントと IAM ユーザーをそのアカウントの管理者権限で作成します。特に AWS Control Tower の追加セットアップタスクの詳細については、「AWS Control Tower の使用開始 (p. 14)」を参照してください。

AWS にサインアップ

アマゾン ウェブ サービス (AWS) にサインアップすると、AWS アカウントが AWS 内のすべてのサービス (AWS Control Tower など) に自動的にサインアップされます。既に AWS アカウントをお持ちの場合は次のタスクに進んでください。AWS アカウントをお持ちでない場合は、次に説明する手順にしたがってアカウントを作成してください。

AWS アカウントを作成するには

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、通話呼び出しを受け取り、電話のキーパッドを用いて確認コードを入力することが求められます。

次のタスクで AWS アカウント番号が必要となるので、メモしておいてください。

IAM ユーザーを作成する

AWS のサービス (AWS Control Tower など) では、サービスにアクセスする際に認証情報を提供する必要があります。それにより、サービスのリソースにアクセスする権限があるかどうかをサービスが判定します。AWS では、リクエストを実行するために AWS アカウントの AWS ルートユーザー認証情報を使用しないことをお勧めしています。代わりに、AWS Identity and Access Management (IAM) ユーザーを作成し、そのユーザーにフルアクセスを許可します。これらのユーザーを管理者と呼びます。

ご使用のアカウントの AWS アカウントルートユーザー認証情報ではなく、管理者の認証情報を使用して、AWS を操作し、ユーザーの作成やアクセス許可の付与などのタスクを実行できます。詳細については、「ルートアカウント認証情報とIAM ユーザーの認証情報」(AWS 全般のリファレンス) および「IAM のベストプラクティス」(IAM ユーザーガイド) を参照してください。

AWS にサインアップしても、ご自分の IAM ユーザーをまだ作成していない場合は、IAM 管理コンソールを使用して作成できます。

自分用の管理者ユーザーを作成し、そのユーザーを管理者グループに追加するには (コンソール)

1. AWS アカウント E メールアドレスとパスワードを使用して https://console.aws.amazon.com/iam/ で AWS アカウントのルートユーザー として IAM コンソールにサインインします。

Note

以下の**Administrator**IAMユーザーの使用に関するベストプラクティスに従い、ルートユーザー認証情報を安全な場所に保管しておくことを強くお勧めします。ルートユーザーとしてサインインして、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。

2. ナビゲーションペインで [Users]、[Add user] の順に選択します。
3. [ユーザー名] に「**Administrator**」と入力します。
4. [AWS マネジメントコンソール access (アクセス)] の横にあるチェックボックスをオンにします。[Custom password (カスタムパスワード)] を選択し、その後テキストボックスに新しいパスワードを入力します。
5. (オプション) AWS では、デフォルトで、新しいユーザーに対して初回のサインイン時に新しいパスワードを作成することが必要です。必要に応じて [User must create a new password at next sign-in (ユーザーは次回のサインイン時に新しいパスワードを作成する必要がある)] のチェックボックスをオフにして、新しいユーザーがサインインしてからパスワードをリセットできるようにできます。
6. [Next: Permissions (次へ: アクセス許可)] を選択します。
7. [Set permissions (アクセス許可の設定)] で、[Add user to group (ユーザーをグループに追加)] を選択します。
8. [Create group] を選択します。
9. [グループの作成] ダイアログボックスで、[グループ名] に「**Administrators**」と入力します。
10. [Filter policies (フィルタポリシー)] を選択し、その後 [AWS managed -job function (AWS 管理ジョブの機能] を選択してテーブルのコンテンツをフィルタリングします。
11. ポリシーリストで、[AdministratorAccess] のチェックボックスをオンにします。次に、[Create group] を選択します。

    Note

    `AdministratorAccess` アクセス許可を使用して、AWS Billing and Cost Management コンソールを使用する前に、IAM ユーザーおよびロールの請求へのアクセスをアクティブ化する必要があります。これを行うには、請求コンソールへのアクセスの委任に関するチュートリアルのステップ 1 の手順に従ってください。
12. グループのリストに戻り、新しいグループのチェックボックスをオンにします。必要に応じて [Refresh] を選択し、リスト内のグループを表示します。
13. [次へ: タグ] を選択します。
14. (オプション) タグをキー - 値のペアとしてアタッチして、メタデータをユーザーに追加します。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「IAM エンティティのタグ付け」を参照してください。
15. [Next: Review] を選択して、新しいユーザーに追加するグループメンバーシップのリストを表示します。続行する準備ができたら、[Create user] を選択します。

この同じプロセスを繰り返して新しいグループとユーザーを作成し、AWS アカウントのリソースへのアクセス権をユーザーに付与できます。ポリシーを使用して特定の AWS リソースに対するユーザーのアクセス許可を制限する方法については、「アクセス管理」と「ポリシーの例」を参照してください。

この新しい IAM ユーザーとしてサインインするには、まず AWS マネジメントコンソールからサインアウトします。その後、以下の URL を使用します。このとき、your_aws_account_id はハイフンを除いた AWS アカウント番号です (たとえば AWS アカウント番号が `1234-5678-9012` であれば、AWS アカウント ID は `123456789012` です)。

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

作成した IAM ユーザー名とパスワードを入力します。サインインすると、ナビゲーションバーに「your_user_name@your_aws_account_id」と表示されます。

サインページの URL に AWS アカウント ID を含めない場合は、アカウントのエイリアスを作成します。これを行うには、IAM ダッシュボードから [アカウントエイリアスを作成する] を選択し、エイリアス (会社名など) を入力します。アカウントエイリアスを作成した後、サインインするには、次の URL を使用します。

```
https://your_account_alias.signin.aws.amazon.com/console/
```

アカウントの IAM ユーザーのサインインリンクを確認するには、IAM コンソールを開き、ダッシュボードの [AWS アカウントエイリアス] の下を確認します。

MFA のセットアップ

AWS Control Tower の性質上、マスターアカウントには多要素認証 (MFA) を有効にすることを強くお勧めします。詳細については、IAM ユーザーガイド の「AWS アカウントの root ユーザーに対して MFA を有効にする」を参照してください。

次のステップ

AWS Control Tower の使用開始 (p. 14)

AWS Control Tower の使用開始

これは、集中型クラウド管理者向けの AWS Control Tower の使用開始手順です。Landing Zone をセットアップする準備ができたら、次の手順を使用し ます。開始から完了まで、所要時間は約 1 時間です。この手順には、2 つのステップがあります。

AWS Control Tower を使用するためのガイダンス

AWS Control Tower を使用する際の推奨事項は次のとおりです。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。

通常の問い合わせ/機能要望

- マスターアカウントまたは共有アカウントで、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。
- コア組織単位 (OU) の共有アカウント内に作成された AWS Identity and Access Management (IAM) の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。
- AWS Control Tower によって作成されたリソースの詳細については、「共有アカウントは何ですか (p. 2)」を参照してください。

AWS Organizations ガイダンス

- AWS Organizations を使用して、AWS Control Tower によって AWS Control Tower 管理 OU にアタッチされている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。この操作を行うと、ガードレールが不明な状態になり、影響を受けたガードレールの再有効化が必要になります。
- 組織 を使用して、AWS Control Tower によって作成された組織内でアカウントを作成、招待、または移動すると、それらの外部アカウントは AWS Control Tower によって管理されなくなり、[アカウント] テーブルには表示されません。
- 組織 を使用して、AWS Control Tower によって作成された組織内で OU を作成または移動すると、それらの外部 OU は AWS Control Tower によって管理されなくなり、[組織単位] テーブルには表示されません。
- 組織 を使用して、AWS Control Tower によって作成された OU の名前変更または削除を行う場合、この OU は元の名前で AWS Control Tower に引き続き表示されます。Account Factory を使用してこの OU に新しいアカウントをプロビジョニングすることはできません。

AWS シングルサインオン ガイダンス

- AWS シングルサインオン のディレクトリを Active Directory に再設定する場合は、AWS SSO で事前設定されたすべてのユーザーおよびグループが削除されます。

Account Factory ガイダンス

- Account Factory を使用して新しいアカウントを AWS Service Catalog にプロビジョニングする場合、`TagOptions` を定義したり、通知を有効にしたり、プロビジョニング済み製品プランを作成したりしないでください。それらの操作を行うと、新しいアカウントをプロビジョニングできない場合があります。

マスターアカウントの起動前チェック

AWS Control Tower は、お客様のアカウントで Landing Zone を設定するための処理を実行する前に、一連の起動前チェックを実行します。これらの起動チェックにより、マスターアカウントで Landing Zone を設定するための変更の準備ができます。Landing Zone を設定する前に実行するチェックは以下のとおりです。

- AWS アカウントの既存のサービス制限は、AWS Control Tower が起動するのに十分であることが必要です。詳細については、「制限 (p. 76)」を参照してください。
- AWS アカウントは既存の AWS Organizations OU のメンバーにすることはできません (すべての機能を有効にした状態で、あるいは一括請求 (コンソリデーティッドビリング) 用にそのアカウントがセットアップされているかどうかに関係なく)。
- AWS アカウントは、次の AWS サービスに登録されている必要があります。
  - Amazon Simple Storage Service (Amazon S3)
  - 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はこれらのサービスに登録されています。
- AWS アカウントに、すでに設定された AWS Config アグリゲータを含めることはできません。
- AWS アカウントに、すでに設定された AWS シングルサインオン (AWS SSO) を含めることはできません。

Landing Zone をセットアップすると、ユーザーに代わって AWS Control Tower がマスターアカウントで次のアクションを実行します。

- 3 つの 組織 組織ユニット (OU) (ルート、コア、およびカスタム) を作成する。
- 2 つの共有アカウント (ログアーカイブアカウントと監査アカウント) を作成する。
- 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、AWS SSO でクラウドネイティブなディレクトリを作成する。
- 17 個の予防的ガードレールを適用して、ポリシーを適用する。
- 3 個の発見的ガードレールを適用して、設定違反を検出する。

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

このガイドでは、新しい AWS アカウントで Landing Zone を設定していることを前提とします。アカウントと IAM 管理者の作成については、「セットアップ (p. 11)」を参照してください。

Landing Zone をセットアップするには、AWS Control Tower に、AWS アカウント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。これらの E メールアドレスはそれぞれ、共同受信箱、

つまり、AWS Control Tower に関連する特定の作業を行う企業のさまざまなユーザーの共有 E メールアカウントであることが必要です。E メールアドレスは以下のとおりです。

- 監査アカウント – これは、AWS Control Towerにより利用可能になった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 – これは、Landing Zone の管理された OU 内で管理されたすべての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。

ステップ 2: ランディングゾーンをセットアップする

AWS Control Tower には、API またはプログラムによるアクセスがありません。Landing Zone をセットアップするには、次の手順を実行します。

Landing Zone をセットアップするには

1. ウェブブラウザを開いて、https://console.aws.amazon.com/controltower の AWS Control Tower コンソールに移動します。
2. [Set up Landing Zone (Landing Zone のセットアップ)] を選択します。
3. ログアーカイブアカウントおよび監査アカウントの E メールアドレスを指定します。これらは、AWS アカウントにまだ関連付けられていない E メールアドレスであることが必要です。
4. [Service permissions (サービスのアクセス許可)] を確認し、準備が整ったら、[I understand the permissions AWS Control Tower will use to administer AWS resources and enforce rules on my behalf (お客様に代わって AWS リソースを管理してルールを適用するためのアクセス許可が AWS Control Tower に付与されることを了承する)] を選択します。
5. [Launch your AWS Control Tower (AWS Control Tower を起動する)] を選択します。

これにより、Landing Zone をセットアップするプロセスが開始されます。完了するまでに約 1 時間かかる場合があります。設定中に、コアアカウントが作成され、root およびコア OU が作成され、AWS リソースが作成、変更、または削除されます。

> **Important**
>
> 監査アカウントに指定した E メールアドレスには、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 Notification - Subscription Confirmation (AWS 通知 - サブスクリプション確認)] E メールが送信されます。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 リージョンからの各 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。

次のステップ

これで、Landing Zone がセットアップされ、使用する準備ができました。

AWS Control Tower をセットアップすると、ユーザーに代わって Landing Zone がマスターアカウントで次のアクションを実行します。

- 2 つの組織ユニット (OU) (コアとカスタム) を作成する。
- コア OU 内に 2 つのアカウント (ログアーカイブアカウントとセキュリティ監査アカウント) を作成する。

- 事前設定されたグループ、アクセス権限セット、およびシングルサインオンアクセスを使用して、AWS SSO でクラウドネイティブなディレクトリを作成する。
- 10 個の予防的ガードレールを適用して、ポリシーを適用する。
- 2 つの発見的ガードレールを適用して、設定違反を検出する。
- エンドユーザーが Landing Zone 内に新しい AWS アカウントをプロビジョニングできるように AWS Service Catalog で Account Factory 製品を作成する。

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。

- エンドユーザーは、Account Factory を使用して独自の AWS アカウントを Landing Zone にプロビジョニングできます。詳細については、「AWS Service Catalog を介したアカウントの設定とプロビジョニング (p. 51)」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、最新のガードレールを入手して Landing Zone を最新の状態に維持するために、ランディングゾーンの更新が必要な場合があります。詳細については、「AWS Control Tower での設定更新管理 (p. 74)」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 (p. 84)」を参照してください。

AWS Control Tower のガードレール

ガードレールは、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。これは、わかりやすい形式で表されます。ユーザーが Landing Zone において AWS アカウントで作業を実行すると、ユーザーはガードレールの対象となります。

各ガードレールの動作は防止または検出のいずれかです。

- 予防 – 予防的ガードレールにより、アカウントのコンプライアンスが維持されるようになります。予防的ガードレールの動作のステータスは、適用または無効です。予防的ガードレールは、サービスコントロールポリシーおよび AWS Lambda 関数を使用してポリシー違反を防止します。予防的ガードレールは、すべての AWS リージョンでサポートされています。
- 検出 – 発見的ガードレールにより、アカウント内のリソースのコンプライアンス違反が検出されます。検出の動作のステータスは、クリアまたは違反です。発見的ガードレールでは、ポリシー違反が検出され、ダッシュボードを使用してアラートが提供されます。発見的ガードレールは、AWS Control Tower でサポートされている AWS リージョンでのみ適用されます。

AWS Control Tower には、必須ガードレール、強く推奨されるガードレール、および選択的ガードレールが用意されています。新しい Landing Zone を作成すると、すべての必須ガードレールがデフォルトで適用されます。強く推奨されるガードレールと選択的ガードレールは有効になりません。

ガードレールを使用すると、ポリシーの目的を表すことができます。AWS Control Tower では、予防制御または検出制御を実装して、AWS アカウント全体におけるリソースのコンプライアンスを管理および監視します。たとえば、[Disallow public read access to S3 buckets (S3 バケットへのパブリック読み取りアクセスを禁止する)] を有効にして、OU 下のすべてのアカウントに対してすべての S3 バケットへのパブリック読み取りアクセスを拒否します。組織単位でガードレールを有効にすると、そのガードレールが OU 下のすべての子アカウントに適用されます。

ガードレールの実装:

- 予防的ガードレールは、AWS Organizations の一部であるサービスコントロールポリシー (SCP) を使用して実装されます。
- 発見的ガードレールは、AWS Config ルールと AWS Lambda 関数を使用して実装されます。

考慮事項

ガードレールを使用する際、以下の点を考慮してください。

- Landing Zone を作成した後、Landing Zone 内のすべてのリソースはガードレールの対象となります。
- AWS Control Tower を使用して作成された OU には、ガードレールが適用されます。Landing Zone の外部で作成された OU にはガードレールを適用できないため、AWS Control Tower コンソールに OU は表示されません。
- Account Factory を使用して作成されたアカウントは、 親 OU のガードレールを継承します。Landing Zone の外部で作成されたアカウントは、親 OU のガードレールを継承せず、AWS Control Tower コンソールに表示されません。
- マスターアカウントの root ユーザーおよび IAM 管理者は、通常はガードレールで拒否される作業を実行できます。これは意図的なものです。これは、マスターアカウントが使用できない状態になるのを防ぎます。このような場合は、マスターアカウント内で実行されるすべてのアクションが引き続きログアーカイブログのログで追跡されます。このログにより、説明責任と監査ログが有効になります。

オプションのガードレール

ガードレールに適用されるガイダンスには、必須、強く推奨される、選択的の 3 種類があります。必須のガードレールは常に強制されます。強く推奨されるガードレールは、適切に設計されたマルチアカウント環境のベストプラクティスに基づいています。選択的ガードレールを使用すると、AWS エンタープライズ環境で一般的に制限されているアクションを追跡またはロックダウンできます。

強く推奨されるガードレールと選択的ガードレールはオプションです。つまり、どのガードレールを有効にするかを選択することで、Landing Zone のエンフォースメントレベルをカスタマイズできます。オプションのガードレールはデフォルトでは有効になっていません。詳細については、以下のガードレールリファレンスを参照してください。

- 強く推奨されるガードレール (p. 31)
- 選択的ガードレール (p. 40)

ガードレールのガイダンスは、予防的であるか発見的であるかに関係ありません。

ガードレールの詳細

コンソールのガードレール詳細ページで、各ガードレールに関する以下の詳細が表示されます。

- 名前 – ガードレールの名前。
- 説明 – ガードレールの説明。
- ガイダンス – ガイダンスは、必須、強く推奨される、または選択的のいずれかです。
- [カテゴリ] – カテゴリは、監査ログ、モニタリング、データセキュリティ、ネットワーク、IAM、Control Tower 設定のいずれかです。
- [Behavior (動作)] – ガードレールの動作は予防的または発見的のいずれかに設定されます。
- [コンプライアンス状況] – ガードレールのコンプライアンス状況は、クリア、準拠、適用、不明、違反のいずれかです。

ガードレール詳細ページでは、ガードレールアーティファクトを確認することもできます。ガードレールは、1 つ以上のアーティファクトによって実装されます。これらのアーティファクトには、AWS CloudFormation テンプレート、設定ドリフトを作成できるのアカウントレベルの設定変更またはアクティビティを回避するためのサービスコントロールポリシー 、およびアカウントレベルのポリシー違反を検出するための AWS Config ルール を含めることができます。

ガードレールの有効化

ほとんどのカードレールは OU の設定に従って自動的に有効になりますが、一部のガードレールは OU で手動で有効にする場合があります。次の手順では、OU でガードレールを有効にするためのステップについて説明します。

> Important
>
> 強く推奨されるガイダンスでガードレールを有効にすると、アカウント内で AWS Control Tower マネージド AWS リソースが作成されます。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、ガードレールの状態が不明になる可能性があります。

OU でガードレールを有効にするには

1. ウェブブラウザを使用して、https://console.aws.amazon.com/controltower の 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、[Guardrails (ガードレール)] を選択します。
3. 有効にするガードレール (たとえば、 [Guardrail: Enable encryption for EBS volumes attached to EC2 instances (ガードレール: EC2インスタンスにアタッチされたEBSボリュームの暗号化を有効にする)]) を選択します。これにより、ガードレールの詳細ページが開きます。
4. 有効になっている組織ユニットから、[Enable guardrail on OU (OU でガードレールを有効にする)]を選択します。
5. 新しいページが表示され、OU の名前が一覧表示されます。このガードレールを有効にする OU を選択します。
6. [Enable guardrail on OU (OU でガードレールを有効にする)] を選択します。
7. これで、ガードレールが有効になりました。変更が完了するまでに数分かかることがあります。完了すると、選択した OU でこのガードレールが有効になっていることがわかります。

ガードレールリファレンス

次のセクションには、AWS Control Tower で利用可能な各ガードレールのリファレンスが含まれています。各ガードレールリファレンスには、Landing Zone の OU で特定のガードレールを有効にする場合の詳細、アーティファクト、追加情報、考慮事項が含まれています。

トピック

- 必須のガードレール (p. 20)
- 強く推奨されるガードレール (p. 31)
- 選択的ガードレール (p. 40)

必須のガードレール

Landing Zone を設定すると、必須のガードレールがデフォルトで有効になっており、無効にすることはできません。以下に、AWS Control Tower で使用できる各必須ガードレールのリファレンスを示します。

Enable Encryption at Rest for Log Archive (ログアーカイブの保管時に暗号化を有効にする)

このガードレールにより、ログアーカイブアカウントでの Amazon S3 バケットの補間時に暗号化が有効になります。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはコア OU で有効になっています。

このガードレールのアーティファクトは、次のサービスコントロールポリシー (SCP) です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRAUDITBUCKETENCRYPTIONENABLED",
            "Effect": "Deny",
            "Action": [
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
```

```
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Enable Access Logging for Log Archive (ログアーカイブのアクセスログを有効にする)

このガードレールにより、ログアーカイブ共有アカウントのアクセスログが有効になります。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはコア OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRAUDITBUCKETLOGGINGENABLED",
            "Effect": "Deny",
            "Action": [
                "s3:PutBucketLogging"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Disallow Policy Changes to Log Archive (ログアーカイブのポリシー変更を禁止する)

このガードレールにより、ログアーカイブ共有アカウントでポリシー変更の発生が禁止されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはコア OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRAUDITBUCKETPOLICYCHANGESPROHIBITED",
            "Effect": "Deny",
            "Action": [
                "s3:PutBucketPolicy"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
```

```
        }
    ]
}
```

Disallow Public Read Access to Log Archive (ログアーカイブへのパブリック読み取りアクセスを禁止する)

このガードレールにより、ログアーカイブ共有アカウントで Amazon S3 バケットへのパブリック読み取りアクセスが有効になっているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、必須のガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールはコア OU で有効になっています。

このガードレールのアーティファクトは、次の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check that your S3 buckets do not allow public
 access
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForS3PublicRead:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks that your S3 buckets do not allow public read access. If an S3
 bucket policy or bucket ACL allows public read access, the bucket is noncompliant.
      Source:
        Owner: AWS
        SourceIdentifier: S3_BUCKET_PUBLIC_READ_PROHIBITED
      Scope:
        ComplianceResourceTypes:
          - AWS::S3::Bucket
```

Disallow Public Write Access to Log Archive (ログアーカイブへのパブリック書き込みアクセスを禁止する)

このガードレールにより、ログアーカイブ共有アカウントで Amazon S3 バケットへのパブリック書き込みアクセスが有効になっているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、必須のガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールはコア OU で有効になっています。

このガードレールのアーティファクトは、次の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check that your S3 buckets do not allow public
 access
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForS3PublicWrite:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks that your S3 buckets do not allow public write access. If an S3
 bucket policy or bucket ACL allows public write access, the bucket is noncompliant.
```

```
      Source:
        Owner: AWS
        SourceIdentifier: S3_BUCKET_PUBLIC_WRITE_PROHIBITED
      Scope:
        ComplianceResourceTypes:
          - AWS::S3::Bucket
```

Set a Retention Policy for Log Archive (ログアーカイブの保持ポリシーを設定する)

このガードレールにより、365 日間のログアーカイブ共有アカウントのログで保持ポリシーが設定されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはコア OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRAUDITBUCKETRETENTIONPOLICY",
            "Effect": "Deny",
            "Action": [
                "s3:PutLifecycleConfiguration"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Disallow Configuration Changes to CloudTrail (CloudTrail の設定変更を禁止する)

このガードレールにより、Landing Zone で CloudTrail の設定変更が回避されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRCLOUDTRAILENABLED",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:DeleteTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
```

```
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Integrate CloudTrail Events with CloudWatch Logs (CloudTrail イベントと CloudWatch ログを統合する)

このガードレールにより、CloudTrail イベントを CloudWatch Logs ログファイルに送信してアクティビティデータのリアルタイム分析が実行されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRCLOUDTRAILENABLED",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:DeleteTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Enable CloudTrail in All Available Regions (利用可能なすべてのリージョンで CloudTrail を有効にする)

このガードレールにより、利用可能なすべての AWS リージョンで CloudTrail が有効になります。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRCLOUDTRAILENABLED",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:DeleteTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
```

```
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Enable Integrity Validation for CloudTrail Log File (CloudTrail ログファイルの整合性の検証を有効にする)

このガードレールにより、すべてのアカウントおよび OU で CloudTrail ログファイルの整合性の検証が有効になります。それにより、CloudTrail ログファイルを使用してアカウントアクティビティログの整合性が確保され、CloudTrail が Amazon S3 に書き込む各ログのハッシュが含まれるデジタル署名されたダイジェストファイルが作成されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、以下の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRCLOUDTRAILENABLED",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:DeleteTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Disallow Changes to CloudWatch Set Up by AWS Control Tower (AWS Control Tower によって設定された CloudWatch の変更を禁止する)

このガードレールにより、Landing Zone のセットアップ時に AWS Control Tower によって設定された CloudWatch の変更が禁止されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRCLOUDWATCHEVENTPOLICY",
```

```
      "Effect": "Deny",
      "Action": [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DisableRule",
        "events:DeleteRule"
      ],
      "Resource": [
        "arn:aws:events:*:*:rule/aws-controltower-*"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSControlTowerExecution"
        }
      }
    }
  ]
}
```

Disallow Changes to AWS Config Aggregation Set Up by AWS Control Tower (AWS Control Tower によって設定された AWS Config の集計の変更を禁止する)

このガードレールにより、Landing Zone のセットアップ時に設定とコンプライアンスデータを収集するために AWS Control Tower によって行われた AWS Config の集計設定の変更が禁止されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRCONFIGRULETAGSPOLICY",
      "Effect": "Deny",
      "Action": [
        "config:TagResource",
        "config:UntagResource"
      ],
      "Resource": ["*"],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSControlTowerExecution"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "aws-control-tower"
        }
      }
    }
  ]
}
```

Disallow Configuration Changes to AWS Config (AWS Config の設定変更を禁止する)

このガードレールにより、AWS Config の設定変更が禁止されます。これにより、AWS Config の設定変更を許可することで、AWS Config レコードのリソース設定が一貫性のある形で確保されます。これは、必

須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、次の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRCONFIGENABLED",
            "Effect": "Deny",
            "Action": [
                "config:DeleteConfigurationRecorder",
                "config:DeleteDeliveryChannel",
                "config:DeleteRetentionConfiguration",
                "config:PutConfigurationRecorder",
                "config:PutDeliveryChannel",
                "config:PutRetentionConfiguration",
                "config:StopConfigurationRecorder"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
}
```

Enable AWS Config in All Available Regions (利用可能なすべてのリージョンで AWS Config を有効にする)

このガードレールにより、利用可能なすべての AWS リージョンで AWS Config が有効になります。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、以下の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRCONFIGENABLED",
            "Effect": "Deny",
            "Action": [
                "config:DeleteConfigurationRecorder",
                "config:DeleteDeliveryChannel",
                "config:DeleteRetentionConfiguration",
                "config:PutConfigurationRecorder",
                "config:PutDeliveryChannel",
                "config:PutRetentionConfiguration",
                "config:StopConfigurationRecorder"
            ],
            "Resource": ["*"],
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
                }
            }
        }
    ]
```

```
}
```

Disallow Changes to AWS Config ルール Set Up by AWS Control Tower (AWS Control Tower によって設定された AWS Config ルール の変更を禁止する)

このガードレールにより、Landing Zone のセットアップ時に AWS Control Tower よって実装された AWS Config ルール の変更が禁止されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、以下の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRCONFIGRULEPOLICY",
      "Effect": "Deny",
      "Action": [
        "config:PutConfigRule",
        "config:DeleteConfigRule",
        "config:DeleteEvaluationResults",
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource": ["*"],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSControlTowerExecution"
        },
        "StringEquals": {
          "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
        }
      }
    }
  ]
}
```

Disallow Changes to IAM Roles Set Up by AWS Control Tower (AWS Control Tower によって設定された IAM ルールの変更を禁止する)

このガードレールにより、Landing Zone のセットアップ時に AWS Control Tower によって作成された IAM ルールの変更が禁止されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、以下の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRIAMROLEPOLICY",
      "Effect": "Deny",
      "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*"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
        }
      }
    }
  ]
}
```

Disallow Changes to Lambda Functions Set Up by AWS Control Tower (AWS Control Tower によって設定された Lambda 関数の変更を禁止する)

このガードレールにより、AWS Control Tower によって設定された Lambda 関数の変更が禁止されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、以下の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRLAMBDAFUNCTIONPOLICY",
      "Effect": "Deny",
      "Action": [
        "lambda:AddPermission",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:PutFunctionConcurrency",
        "lambda:RemovePermission",
        "lambda:UpdateEventSourceMapping",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": [
        "arn:aws:lambda:*:*:function:aws-controltower-*"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
        }
      }
    }
  ]
```

```
}
```

Disallow Changes to Amazon SNS Set Up by AWS Control Tower (AWS Control Tower によって設定された Amazon SNS の変更を禁止する)

このガードレールにより、AWS Control Tower によって設定された Amazon SNS の変更が禁止されます。それにより、Landing Zone の Amazon SNS 通知設定の整合性が保護されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、以下の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRSNSTOPICPOLICY",
      "Effect": "Deny",
      "Action": [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:RemovePermission",
        "sns:SetTopicAttributes"
      ],
      "Resource": [
        "arn:aws:sns:*:*:aws-controltower-*"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
        }
      }
    }
  ]
}
```

Disallow Changes to Amazon SNS Subscriptions Set Up by AWS Control Tower (AWS Control Tower によって設定された Amazon SNS サブスクリプションの変更を禁止する)

このガードレールにより、AWS Control Tower によって設定された Amazon SNS サブスクリプションの変更が禁止されます。それにより、Landing Zone の Amazon SNS サブスクリプション設定の整合性が保護されます。これは、必須のガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールはすべての OU で有効になっています。

このガードレールのアーティファクトは、以下の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRSNSSUBSCRIPTIONPOLICY",
      "Effect": "Deny",
      "Action": [
        "sns:Subscribe",
```

```
        "sns:Unsubscribe"
      ],
      "Resource": [
        "arn:aws:sns:*:*:aws-controltower-SecurityNotifications"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/AWSControlTowerExecution"
        }
      }
    }
  ]
}
```

強く推奨されるガードレール

強く推奨されるガードレールは、適切に設計されたマルチアカウント環境のベストプラクティスに基づいています。これらのガードレールはデフォルトで無効になっており、無効のままでもかまいません。以下に、AWS Control Tower で使用できる強く推奨されるガードレールそれぞれのリファレンスを示します。

Disallow Creation of Access Keys for the Root User (root ユーザーのアクセスキーの作成を禁止する)

root ユーザーのアクセスキーの作成を禁止することで、AWS アカウントを保護します。代わりに、AWS アカウントの操作のためのアクセス許可を制限した IAM ユーザーのアクセスキーを作成することをお勧めします。これは、強く推奨されるガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSERACCESSKEYS",
            "Effect": "Deny",
            "Action": "iam:CreateAccessKey",
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

root ユーザーとしてのアクションを禁止する

AWS アカウントを保護するには、root ユーザー認証情報 (アカウントのすべてのリソースへの無制限のアクセスを許可するアカウント所有者の認証情報) を使用したアカウントアクセスを禁止します。代わりに、AWS アカウントとの日常的なやり取り用に AWS IAM (Identity and Access Management) ユーザーを作成することをお勧めします。これは、強く推奨されるガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRRESTRICTROOTUSER",
      "Effect": "Deny",
      "Action": "*",
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

Enable Encryption 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 ボリュームの暗号化を有効にする)

このガードレールにより、Landing Zone の 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が検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは OU で有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check for encryption of all storage volumes
 attached to compute
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForEncryptedVolumes:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether EBS volumes that are in an attached state are encrypted.
      Source:
        Owner: AWS
        SourceIdentifier: ENCRYPTED_VOLUMES
      Scope:
        ComplianceResourceTypes:
          - AWS::EC2::Volume
```

Disallow Internet Connection Through RDP (RDP を介したインターネット接続を禁止する)

このガードレールにより、Remote Desktop Protocol (RDP) などのサービスを介したインターネット接続が Amazon EC2 インスタンスに対して有効になっているかどうかが検出されます。このガードレールによ

り、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether security groups that are in use
 disallow unrestricted incoming TCP traffic to the specified ports.
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
  blockedPort1:
    Type: String
    Default: '20'
    Description: Blocked TCP port number.
  blockedPort2:
    Type: String
    Default: '21'
    Description: Blocked TCP port number.
  blockedPort3:
    Type: String
    Default: '3389'
    Description: Blocked TCP port number.
  blockedPort4:
    Type: String
    Default: '3306'
    Description: Blocked TCP port number.
  blockedPort5:
    Type: String
    Default: '4333'
    Description: Blocked TCP port number.
Conditions:
  blockedPort1:
    Fn::Not:
    - Fn::Equals:
      - ''
      - Ref: blockedPort1
  blockedPort2:
    Fn::Not:
    - Fn::Equals:
      - ''
      - Ref: blockedPort2
  blockedPort3:
    Fn::Not:
    - Fn::Equals:
      - ''
      - Ref: blockedPort3
  blockedPort4:
    Fn::Not:
    - Fn::Equals:
      - ''
      - Ref: blockedPort4
  blockedPort5:
    Fn::Not:
    - Fn::Equals:
      - ''
      - Ref: blockedPort5
Resources:
  CheckForRestrictedCommonPortsPolicy:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether security groups that are in use disallow unrestricted
 incoming TCP traffic to the specified ports.
```

```
      InputParameters:
        blockedPort1:
          Fn::If:
          - blockedPort1
          - Ref: blockedPort1
          - Ref: AWS::NoValue
        blockedPort2:
          Fn::If:
          - blockedPort2
          - Ref: blockedPort2
          - Ref: AWS::NoValue
        blockedPort3:
          Fn::If:
          - blockedPort3
          - Ref: blockedPort3
          - Ref: AWS::NoValue
        blockedPort4:
          Fn::If:
          - blockedPort4
          - Ref: blockedPort4
          - Ref: AWS::NoValue
        blockedPort5:
          Fn::If:
          - blockedPort5
          - Ref: blockedPort5
          - Ref: AWS::NoValue
      Scope:
        ComplianceResourceTypes:
        - AWS::EC2::SecurityGroup
      Source:
        Owner: AWS
        SourceIdentifier: RESTRICTED_INCOMING_TRAFFIC
```

Disallow Internet Connection Through SSH (SSH を介したインターネット接続を禁止する)

このガードレールにより、Secure Shell (SSH) プロトコルなどのリモートサービスを介したインターネット接続が許可されているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether security groups that are in use
 disallow SSH
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForRestrictedSshPolicy:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether security groups that are in use disallow unrestricted
 incoming SSH traffic.
      Scope:
        ComplianceResourceTypes:
        - AWS::EC2::SecurityGroup
      Source:
        Owner: AWS
```

```
        SourceIdentifier: INCOMING_SSH_DISABLED
```

Enable MFA for the Root User (root ユーザーに対して MFA を有効にする)

このガードレールにより、マスターアカウントの root ユーザーに対して多要素認証 (MFA) が有効になっているかどうかが検出されます。MFA では、ユーザー名とパスワードに加えて認証コードが使用されるため、セキュリティ的に弱い認証から生じる脆弱性のリスクが軽減されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to require MFA for root access to accounts
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
  MaximumExecutionFrequency:
    Type: String
    Default: 24hours
    Description: The frequency that you want AWS Config to run evaluations for the rule.
    AllowedValues:
    - 1hour
    - 3hours
    - 6hours
    - 12hours
    - 24hours
Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours
Resources:
  CheckForRootMfa:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether the root user of your AWS account requires multi-factor
 authentication for console sign-in.
      Source:
        Owner: AWS
        SourceIdentifier: ROOT_ACCOUNT_MFA_ENABLED
      MaximumExecutionFrequency:
        !FindInMap
          - Settings
          - FrequencyMap
          - !Ref MaximumExecutionFrequency
```

Disallow Public Read Access to Amazon S3 Buckets (Amazon S3 バケットへのパブリック読み取りアクセスを禁止する)

このガードレールにより、Amazon S3 バケットへのパブリック読み取りアクセスが許可されているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check that your S3 buckets do not allow public
 access
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForS3PublicRead:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks that your S3 buckets do not allow public read access. If an S3
 bucket policy or bucket ACL allows public read access, the bucket is noncompliant.
      Source:
        Owner: AWS
        SourceIdentifier: S3_BUCKET_PUBLIC_READ_PROHIBITED
      Scope:
        ComplianceResourceTypes:
          - AWS::S3::Bucket
```

Disallow Public Write Access to Amazon S3 Buckets (Amazon S3 バケットへのパブリック書き込みアクセスを禁止する)

このガードレールにより、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が検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check that your S3 buckets do not allow public
 access
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForS3PublicWrite:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks that your S3 buckets do not allow public write access. If an S3
 bucket policy or bucket ACL allows public write access, the bucket is noncompliant.
      Source:
        Owner: AWS
        SourceIdentifier: S3_BUCKET_PUBLIC_WRITE_PROHIBITED
      Scope:
        ComplianceResourceTypes:
          - AWS::S3::Bucket
```

Disallow Amazon EBS Volumes That Are Unattached to An Amazon EC2 Instance (Amazon EC2 インスタンスにアタッチされていない Amazon EBS ボリュームを禁止する)

Amazon EBS ボリュームが Amazon EC2 インスタンスから独立して存続するかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether EBS volumes are attached to EC2
 instances
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
  deleteOnTermination:
    Type: 'String'
    Default: 'None'
    Description: 'Check for Delete on termination'
Conditions:
  deleteOnTermination:
    Fn::Not:
    - Fn::Equals:
      - 'None'
      - Ref: deleteOnTermination
Resources:
  CheckForEc2VolumesInUse:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether EBS volumes are attached to EC2 instances
      InputParameters:
        deleteOnTermination:
          Fn::If:
            - deleteOnTermination
            - Ref: deleteOnTermination
            - Ref: AWS::NoValue
      Source:
        Owner: AWS
        SourceIdentifier: EC2_VOLUME_INUSE_CHECK
      Scope:
        ComplianceResourceTypes:
          - AWS::EC2::Volume
```

Disallow Amazon EC2Instance Types That Are Not Amazon EBS-Optimized (Amazon EBS 最適化以外のタイプの Amazon EC2 インスタンスを禁止する)

パフォーマンスが最適化された Amazon EBS ボリュームなしで Amazon EC2 インスタンスが起動されるかどうかが検出されます。Amazon EBS 最適化ボリュームにより、Amazon EBS I/O と、インスタンスからの他のトラフィックとの間で、競合が最小限に抑えられます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
```

```
Description: Configure AWS Config rules to check whether EBS optimization is enabled for
 your EC2 instances that can be EBS-optimized
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForEbsOptimizedInstance:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether EBS optimization is enabled for your EC2 instances that
 can be EBS-optimized
      Source:
        Owner: AWS
        SourceIdentifier: EBS_OPTIMIZED_INSTANCE
      Scope:
        ComplianceResourceTypes:
          - AWS::EC2::Instance
```

Disallow Public Access to Amazon RDS Database Instances (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を禁止する)

Amazon RDS データベースインスタンスでパブリックアクセスが有効になっているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether Amazon RDS instances are not
 publicly accessible.
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForRdsPublicAccess:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether the Amazon Relational Database Service (RDS) instances
 are not publicly accessible. The rule is non-compliant if the publiclyAccessible field is
 true in the instance configuration item.
      Source:
        Owner: AWS
        SourceIdentifier: RDS_INSTANCE_PUBLIC_ACCESS_CHECK
      Scope:
        ComplianceResourceTypes:
          - AWS::RDS::DBInstance
```

Disallow Public Access to Amazon RDS Database Snapshots (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を禁止する)

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が検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨され

るガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Checks if Amazon Relational Database Service (Amazon RDS) snapshots are
 public.
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForRdsStorageEncryption:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks if Amazon Relational Database Service (Amazon RDS) snapshots are
 public. The rule is non-compliant if any existing and new Amazon RDS snapshots are public.
      Source:
        Owner: AWS
        SourceIdentifier: RDS_SNAPSHOTS_PUBLIC_PROHIBITED
      Scope:
        ComplianceResourceTypes:
          - AWS::RDS::DBSnapshot
```

Disallow Amazon RDS Database Instances That Are Not Storage Encrypted (ストレージが暗号化されていない Amazon RDS データベースインスタンスを禁止する)

Amazon RDS データベースインスタンスが、自動バックアップ、リードレプリカ、スナップショットと共に、保管時に暗号化されていないかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether storage encryption is enabled for
 your RDS DB instances
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForRdsStorageEncryption:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether storage encryption is enabled for your RDS DB instances.
      Source:
        Owner: AWS
        SourceIdentifier: RDS_STORAGE_ENCRYPTED
      Scope:
        ComplianceResourceTypes:
          - AWS::RDS::DBInstance
```

選択的ガードレール

選択的ガードレールを使用すると、AWS エンタープライズ環境で一般的に制限されているアクションが実行されようとした場合、その試みをロックダウンまたは追跡できます。これらのガードレールはデフォルトで無効になっており、無効のままでもかまいません。以下に、AWS Control Tower で使用できる各選択的ガードレールのリファレンスを示します。

Disallow Cross-Region Replication for Amazon S3 Bucket (Amazon S3 バケットのクロスリージョンレプリケーションを禁止する)

バケット間でオブジェクトを他の AWS リージョンに自動的に非同期コピーすることを無効にすることで、Amazon S3 データの場所を 1 つの AWS リージョンに制限します。これは、選択的ガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTS3CROSSREGIONREPLICATION",
            "Effect": "Deny",
            "Action": [
                "s3:PutReplicationConfiguration"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Disallow Delete Actions on Amazon S3 Buckets Without MFA (MFA なしの Amazon S3 バケットの削除アクションを禁止する)

削除アクションに MFA を必須とすることで、Amazon S3 バケットを保護します。MFA では、ユーザー名とパスワードのほかに追加の認証コードが使用されます。これは、選択的ガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の SCP です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTS3DELETEWITHOUTMFA",
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObject",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
```

```
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": [
                        "false"
                    ]
                }
            }
        }
    ]
}
```

Disallow Access to IAM Users Without MFA (MFA なしの IAM ユーザーへのアクセスを禁止する)

アカウントのすべての IAM ユーザーに MFA を必須とすることで、アカウントを保護します。MFA では、ユーザー名とパスワードのほかに追加の認証コードが使用されます。このガードレールにより、MFA が有効になっているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、選択的ガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether the IAM users have MFA enabled
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
  MaximumExecutionFrequency:
    Type: String
    Default: 1hour
    Description: The frequency that you want AWS Config to run evaluations for the rule.
    AllowedValues:
    - 1hour
    - 3hours
    - 6hours
    - 12hours
    - 24hours
Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours
Resources:
  CheckForIAMUserMFA:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether the AWS Identity and Access Management users have multi-
factor authentication (MFA) enabled. The rule is COMPLIANT if MFA is enabled.
      Source:
        Owner: AWS
        SourceIdentifier: IAM_USER_MFA_ENABLED
      MaximumExecutionFrequency:
        !FindInMap
          - Settings
          - FrequencyMap
          - !Ref MaximumExecutionFrequency
```

Disallow Console Access to IAM Users Without MFA (MFA なしの IAM ユーザーへのコンソールアクセスを禁止する)

コンソールのすべての IAM ユーザーに MFA を必須とすることで、アカウントを保護します。MFA では、ユーザー名とパスワードのほかに追加の認証コードが使用されます。このガードレールにより、MFA が有効になっているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、選択的ガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether MFA is enabled for all AWS IAM
 users that use a console password.
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
  MaximumExecutionFrequency:
    Type: String
    Default: 1hour
    Description: The frequency that you want AWS Config to run evaluations for the rule.
    AllowedValues:
    - 1hour
    - 3hours
    - 6hours
    - 12hours
    - 24hours
Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours
Resources:
  CheckForIAMUserConsoleMFA:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether AWS Multi-Factor Authentication (MFA) is enabled for all
 AWS Identity and Access Management (IAM) users that use a console password. The rule is
 COMPLIANT if MFA is enabled.
      Source:
        Owner: AWS
        SourceIdentifier: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
      MaximumExecutionFrequency:
        !FindInMap
          - Settings
          - FrequencyMap
          - !Ref MaximumExecutionFrequency
```

Disallow Amazon S3 Buckets That Are Not Versioning Enabled (バージョニングが有効になっていない Amazon S3 バケットを禁止する)

Amazon S3 バケットでバージョニングに有効になっていないかどうかが検出されます。バージョニングにより、誤って削除または上書きしたオブジェクトを復旧できます。このガードレールにより、アカウント

のステータスは変更されません。これは、選択的ガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check whether versioning is enabled for your S3
 buckets.
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForS3VersioningEnabled:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether versioning is enabled for your S3 buckets.
      Source:
        Owner: AWS
        SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
      Scope:
        ComplianceResourceTypes:
          - AWS::S3::Bucket
```

統合サービス

AWS Control Tower は、他の AWS サービスの上に構築された、優れたアーキテクチャのサービスです。この章では、以下のサービスとそれが AWS Control Tower でどのように機能するかを含め、これらのサービスの概要を説明します。

トピック

- AWS CloudFormation による環境のスクリプト化 (p. 44)
- CloudTrail によるイベントのモニタリング (p. 44)
- CloudWatch によるリソースとサービスのモニタリング (p. 44)
- AWS Config によるリソース設定の管理 (p. 45)
- IAM によるエンティティのアクセス許可の管理 (p. 45)
- Lambda によるサーバーレスコンピューティング関数の実行 (p. 45)
- AWS Organizations によるアカウントの管理 (p. 45)
- Amazon S3 によるオブジェクトの保存 (p. 46)
- AWS Service Catalog によるアカウントのプロビジョニング (p. 46)
- AWS シングルサインオン によるユーザーとアカウントの管理 (p. 46)
- Amazon Simple Notification Service によるアラートの追跡 (p. 50)
- AWS Step Functions による分散アプリケーションの構築 (p. 50)

AWS CloudFormation による環境のスクリプト化

AWS CloudFormation は、計画に従い、再現性の高い方法で、AWS インフラストラクチャデプロイを作成し、プロビジョニングします。これにより、基盤となる AWS インフラストラクチャの作成や設定を行うことなく、AWS 製品を活用して、信頼性が高く、非常にスケーラブルで、コスト効率に優れたアプリケーションをクラウドで構築できます。AWS CloudFormation では、テンプレートファイルを使用して、リソースの集合を 1 つの単位 (スタック) として作成および削除することができます。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 では、アカウントでガードレールを適用する AWS CloudFormation StackSets が使用されます。

CloudTrail によるイベントのモニタリング

AWS CloudTrail を使用すると、アカウントの AWS API コールの履歴を取得して、クラウド内の AWS デプロイをモニタリングできます。CloudTrail に対応するサービスの AWS API を呼び出したユーザーやアカウント、呼び出し元であるソース 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、組織用の証跡作成を自動化したり、証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 User Guide」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、数分で使用を開始できる、信頼性、拡張性、および柔軟性あるモニタリングソリューションを提供します。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 Config によるリソース設定の管理

AWS Config では、設定内容、相互の関連、時間の経過と共に設定と関係がどのように変化するかなど、&AWS; アカウントに関連付けられたリソースの詳細が提供されます。詳細については、「AWS Config Developer Guide」を参照してください。

AWS Control Tower では、いくつかのガードレールで AWS Config ルール を使用します。詳細については、「AWS Control Tower のガードレール (p. 18)」を参照してください。

IAM によるエンティティのアクセス許可の管理

AWS Identity and Access Management IAM は、AWS のサービスへのアクセスをセキュアに制御するためのウェブサービスです。IAM を使用すると、ユーザー、セキュリティ認証情報 (アクセスキーなど)、およびユーザーとアプリケーションがアクセスできる AWS リソースを制御するアクセス許可を集中管理できます。

Landing Zone の設定時に、多数のグループが AWS SSO に作成されます。これらのグループには、IAM から事前定義されたアクセス権限ポリシーであるアクセス権限セットがあります。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アクセス権限の範囲を定義できます。

Lambda によるサーバーレスコンピューティング関数の実行

AWS Lambda を使用すると、サーバーをプロビジョニングまたは管理しなくてもコードを実行できます。実質的にどのようなタイプのアプリケーションやバックエンドサービスでも、管理なしでコードを実行できます。コードをアップロードするだけで、コードの実行とスケールに必要な処理はすべて Lambda により自動的に実行され、高い可用性が維持されます。コードは、他の AWS サービスから自動的にトリガーするよう設定することも、ウェブやモバイルアプリケーションから直接呼び出すよう設定することもできます。

AWS Organizations によるアカウントの管理

AWS Organizations は、お客様が作成して一元管理する組織に複数の AWS アカウントを統合できるようにするアカウント管理サービスです。組織 では、メンバーアカウントを作成して、既存アカウントを組織に招待できます。複数のアカウントをグループに分けることや、ポリシーに基づいて管理することが可能です。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、組織 により請求の一元管理や、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ができます。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。組織 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 では、以下の OU が使用されます。

- ルート – すべてのアカウントおよび Landing Zone にあるその他のすべての OU の親コンテナです。
- コア – 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。

- カスタム OU – この OU は、Landing Zone の設定時に作成され ます。カスタム OU と Landing Zone 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

  [組織単位] ページの AWS Control Tower コンソールにより Landing Zone にさらに OU を追加できます。

考慮事項

AWS Control Tower から作成された OU には、適用されるガードレールを設定できます。AWS Control Tower 外部で作成された OU には設定できず、AWS Control Tower に表示されません。

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。Amazon S3 を使用すると、データの大きさにかかわらず、ウェブ上のどんな場所からでもいつでも保存、取得することができます。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することができます。詳細については、「Amazon Simple Storage Service コンソールユーザーガイド」を参照してください。

Landing Zone の設定時に、Landing Zone 内にあるすべてのアカウントのすべての口グを含めるための 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。

AWS Service Catalog によるアカウントのプロビジョニング

AWS Service Catalog では、IT 管理者が承認された製品のポートフォリオを作成および管理し、そのポートフォリオをエンドユーザーに配布できます。エンドユーザーは、パーソナライズされたポータルから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、アプリケーションなどがあります。特定の製品にアクセスできるユーザーを制御して、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、ユーザーが確信を持って製品を見つけ、起動できるようにすることができます。詳細については、「AWS Service Catalog Administrator Guide」を参照してください。

AWS Control Tower では、AWS Service Catalog の製品である、Account Factory を使用して中央のクラウド管理者とエンドユーザーが Landing Zone で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、「Account Factory (p. 51)」を参照してください。

AWS シングルサインオン によるユーザーとアカウントの管理

AWS シングルサインオン は、AWS アカウントおよびビジネスアプリケーションへの SSO アクセスの管理をシンプルにするクラウドベースのサービスです。AWS Organizations では、すべての AWS アカウントの SSO アクセスとユーザーアクセス権限を管理できます。また、一般的なビジネスアプリケーションや、Security Assertion Markup Language (SAML) 2.0 をサポートするカスタムアプリケーションに対するアクセスを管理することもできます。さらに、AWS SSO には、エンドユーザーが自分に割り当てられている AWS アカウント、ビジネスアプリケーション、カスタムアプリケーションを一元的に検索できる

ユーザーポータルが含まれます。詳細については、「AWS シングルサインオン ユーザーガイド」を参照してください。

AWS Control Tower では、AWS シングルサインオン により中央のクラウド管理者とエンドユーザーの両方が、複数の AWS アカウントやビジネスアプリケーションへの SSO アクセスを管理できます。AWS Control Tower では、このサービスを AWS Service Catalog で作成されるアカウントへのユーザーアクセスの作成と管理に使用します。

> Note
>
> 初めて AWS Control Tower を設定するとき、ルートユーザーと正しいアクセス許可を持つ IAM ユーザーのみ、AWS SSO 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 SSO ユーザーを作成できます。詳細については、「Account Factory (p. 51)」を参照してください。

Landing Zone は、ユーザー ID とシングルサインオンを管理して、ユーザーにアカウント間でフェデレーティッドアクセスを提供するために、ディレクトリで設定されます。Landing Zone を設定すると、デフォルトのディレクトリが設定されています。このディレクトリは、あらかじめ設定されたユーザーグループとアクセス権限セットで設定されています。

このグループは、共有アカウント内で特殊化されたロールを簡単に管理できるように設計されています。メンバーアカウントでエンドユーザーに新しいグループを作成することができます。使用できるアクセス権限セットは、読み取り専用アクセス権限、AWS Control Tower 管理者アクセス、AWS Service Catalog アクセスなど、異なるユーザー権限の幅広いユースケースをカバーします。エンドユーザーは、これらのアクセス権限セットを使用して、Landing Zone で独自の 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 のコンテキストでのこのサービスの詳しい使用方法については、AWS シングルサインオン 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 を使用する場合、AWS SSO は 米国東部 (バージニア北部) ディレクトリにあります。Landing Zone を別のリージョンに設定してから、AWS SSO コンソールに移動する場合、リージョンを 米国東部 (バージニア北部) に変更する必要があります。米国東部 (バージニア北部) で AWS SSO 設定を削除しないでください。

AWS Control Tower 用の AWS SSO 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整理するために事前設定されたグループが利用できます。ユーザーを追加して、AWS SSO で直接これらのグループに割り当てられます。これにより、アカウント内でアクセス権限セットをグループにいるユーザーに一致させます。Landing Zone の設定時に作成されるグループは次のとおりです。

AWSAccountFactory

アカウント	アクセス権限セット	説明
マスターアカウント	AWSServiceCatalogEndUserAccess	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	アクセス権限セット	説明
マスターアカウント	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	アクセス権限セット	説明
マスターアカウント	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。
メンバーアカウント	AWSOrganizationsFullAccess	ユーザーはこのアカウントで 組織 へのフルアクセスが与えられます。

AWSSecurityAuditPowerUsers

アカウント	アクセス権限セット	説明
マスターアカウント	AWSPowerUserAccess	ユーザーは、アプリケーション開発タスクを実行し、AWS 対応アプリケーションの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することができます。
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 対応アプリケーションの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することができます。
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 対応アプリケーションの開発をサポートするリソースとサービス

アカウント	アクセス権限セット	説明
		を作成および設定することができます。
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 対応アプリケーションの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することができます。

AWSSecurityAuditors

アカウント	アクセス権限セット	説明
マスターアカウント	AWSReadOnlyAccess	ユーザーには、このアカウントのすべての AWS のサービスとリソースに読み取り専用アクセスがあります。
ログアーカイブアカウント	AWSReadOnlyAccess	ユーザーには、このアカウントのすべての AWS のサービスとリソースに読み取り専用アクセスがあります。
監査アカウント	AWSReadOnlyAccess	ユーザーには、このアカウントのすべての AWS のサービスとリソースに読み取り専用アクセスがあります。
メンバーアカウント	AWSReadOnlyAccess	ユーザーには、このアカウントのすべての AWS のサービスとリソースに読み取り専用アクセスがあります。

AWSLogArchiveAdmins

アカウント	アクセス権限セット	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	アクセス権限セット	説明
ログアーカイブアカウント	AWSReadOnlyAccess	ユーザーには、このアカウントのすべての AWS のサービスとリソースに読み取り専用アクセスがあります。

AWSAuditAccountAdmins

アカウント	アクセス権限セット	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。

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すぐに通知を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 開発者ガイド」を参照してください。

AWS Control Tower では、Amazon SNS を使用して、マスターアカウントにプログラムによるアラートを送信して、アカウントの E メールアドレスを監査します。これらのアラートは、Landing Zone 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 でのドリフトの検出および解決 (p. 57)」を参照してください。

AWS Step Functions による分散アプリケーションの構築

AWS Step Functions により、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編成できます。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 開発者ガイド」を参照してください。

Account Factory

この章では、AWS Service Catalog コンソールをベースにした、Landing Zone で使用する新しいアカウントをプロビジョニングするために使用する製品である、Account Factory の概要と手順を説明します。

AWS Service Catalog を介したアカウントの設定とプロビジョニング

Account Factory を使用すると、中央のクラウド管理者と AWS シングルサインオン エンドユーザーが Landing Zone でアカウントをプロビジョニングできます。デフォルトでは、アカウントをプロビジョニングする AWS SSO ユーザーは AWSAccountFactory グループに属している必要があります。ただし、プログラム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 ID には `AWSServiceCatalogEndUserFullAccess` に加え、次の IAM アクセス許可ポリシーが必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS SSO と AWS Control Tower の使用の詳細については、「AWS シングルサインオン によるユーザーとアカウントの管理 (p. 46)」を参照してください。次の手順では、AWS SSO エンドユーザーとして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。

Account Factory でエンド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 にサインインします。
2. [Your applications] から、[AWS Account] を選択します。
3. アカウントのリストで、マスターアカウントのアカウント ID を選択します。これには [(Master)] のラベルもあります。
4. [AWSServiceCatalogEndUserAccess] から [Management console] を選択します。これにより、このアカウントのこのユーザーの AWS マネジメントコンソール が開きます。
5. [Service Catalog] を検索して選択し、AWS Service Catalog コンソールを開きます。
6. ナビゲーションペインで、[Products list] を選択します。
7. [AWS Control Tower Account Factory] からドロップダウンメニューを選択して、[Launch product] を選択します。これにより、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します。
8. 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 AWS SSO 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 メールアドレスであることが必要です。[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。
9. 完了したら、ウィザードの [Review (確認)] ページが表示されるまで [NEXT (次へ)] を選択します。[TagOptions] を定義しないでください。また、[Notifications] 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。
10. アカウント設定を確認し、[LAUNCH] を選択します。リソースプランを作成しないでください。この操作を行うと、アカウントのプロビジョニングに失敗します。
11. これで、アカウントのプロビジョニングが開始されました。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。

プロビジョニングしたアカウントは閉鎖することも、管理対象外のアカウントに変更することもできます。または、アカウントの E メールアドレスとユーザーパラメータを更新することで、他のワークロードや他のユーザーにアカウントを転用できます。更新手順に従って、アカウントの組織単位を変更できます。アカウントの管理解除について詳細は、「メンバーアカウントの管理解除 (p. 54)」を参照してください。

Account Factory アカウントの更新

次の手順では、Account Factory アカウントを更新または移行する方法について説明します。

> **Important**
>
> アカウントの OU を移行するには、他のすべての更新を行う場合と同様に、この手順を使用します。

Account Factory アカウントを更新するには

1. AWS マネジメントコンソールにサインインし、AWS シングルサインオン コンソール (https://console.aws.amazon.com/singlesignon/) を開きます。

Note

AWS Service Catalog で新しい製品をプロビジョニングするアクセス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。たとえば、AWSAccountFactory グループか AWSServiceCatalogAdmins グループにいる AWS SSO ユーザーです。

2. [Provision new account (新しいアカウントをプロビジョニングする)] を選択して AWS Service Catalog コンソールと Account Factory 製品を開きます。
3. 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。
4. 一覧表示されているアカウントごとに以下の手順を実行して、すべてのメンバーアカウントを更新します。

   a. アカウントのドロップダウンメニューから [プロビジョニングされた製品の詳細] を選択します。
   b. 以下のパラメータを書き留めます。

      - SSOUserEmail
      - AccountEmail
      - SSOUserFirstName
      - SSOUSerLastName
      - AccountName

   c. [アクション] で、[更新] を選択します。
   d. 更新する製品の [バージョン] の隣にあるボタンを選択して、[次へ] を選択します。
   e. 前に説明したパラメータ値を入力します。[ManagedOrganizationlUnit] で、既存のアカウントの OU を選択するか、新しい OU に移行するには、該当するアカウントで新しい OU を選択します。中央のクラウド管理者は、AWS Control Tower コンソールの [Accounts] でこの情報を見つけることができます。
   f. [次へ] を選択します。
   g. 変更内容を確認し、[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。

Amazon Virtual Private Cloud 設定で Account Factory を設定する

Account Factory により、組織内のアカウントに対して、承認済みのベースラインと構成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 ページで、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。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。AWS Service Catalog を介して、アカウントの特定の OU のプロビジョニングを無効にできます。

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、マスター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。
3. 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、これらの設定をフィールドに入力します。

- Amazon VPC でのパブリックサブネットの作成を無効にする場合は [disabled] を、有効にする場合は [enabled] を選択します。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。
- 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 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ー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] を選択します。

メンバーアカウントの管理解除

Landing Zone で今後 AWS Control Tower による管理を希望しないアカウントを Account Factory に作成した場合、アカウントの管理を解除できます。これは、AWSAccountFactory グループまたは AWSServiceCatalogAdmins グループにいる AWS SSO ユーザーにより、AWS Service Catalog コンソールで実行できます。AWS SSO ユーザーまたはグループの詳細については、「AWS シングルサインオンによるユーザーとアカウントの管理 (p. 46)」を参照してください。メンバーアカウントの管理を解除する手順を以下に説明します。

メンバーアカウントの管理を停止するには

1. ウェブブラウザで AWS 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から [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. [プロビジョニングされた製品の詳細] ページの [アクション] メニューから、[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] を選択します。

   Important

   terminate (終了) という単語は AWS Service Catalog に固有のものです。AWS Service Catalog で Account Factory 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 Landing Zone からアカウントが削除されます。
6. [Deregistering Managed Account] メッセージが表示されます。
7. 表示されたアカウントのステータスを更新するには、ページをリフレッシュします。アカウントが管理対象外になると、ステータスが [terminated] に変わります。
8. 終了したアカウントが不要になった場合は、閉鎖します。AWS アカウントの閉鎖の詳細については、AWS Billing and Cost Management 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。

Note

管理対象外の (終了した) アカウントは閉鎖または削除されません。アカウントが管理対象外になっても、Account Factory でアカウントを作成する際に選択した AWS SSO 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AWS SSO ユーザー E メールアドレスを変更して、AWS SSO のこの設定を変更する必要があります。詳細については、「Account Factory アカウントの更新 (p. 52)」を参照してください。

Account Factory で作成したアカウントの解約

Account Factory で作成されたアカウントは AWS アカウントです。AWS アカウントの解約について詳細は、『AWS Billing and Cost Management 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。

Account Factory の考慮事項

Account Factory を介して AWS Control Tower で作成されたアカウントは、親 OU のガードレールを継承します。AWS Control Tower の外部で作成されたアカウントはこれらのガードレールを継承しません。これらのアカウントは AWS Control Tower に表示されることもありません。

アカウントが Account Factory でプロビジョニングされる場合、以下の AWS リソースがアカウント内で作成されます。

AWS サービス	リソースタイプ	リソース名
AWS CloudFormation	スタック	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	証跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	ロール	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole

AWS サービス	リソースタイプ	リソース名
		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

強く推奨されるガイダンスでガードレールを有効にすると、アカウント内で AWS Control Tower マネージド AWS リソースが作成されます。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、ガードレールの状態が不明になる可能性があります。詳細については、「ガードレールリファレンス (p. 20)」を参照してください。

AWS Control Tower でのドリフトの検出および解決

Landing Zone を作成するとき、Landing Zone とすべての OU、アカウント、リソースは、選択したガードレールにより適用されるすべてのガバナンスルールに準拠します。管理者およびユーザーが Landing Zone を使用するとき、このコンプライアンス状況に変更が発生する可能性があります。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。

変更の理由にかかわらず、変更に伴ってコンプライアンスのストーリーが複雑になる可能性があります。変更や設定の更新が必要なリソースを識別するドリフト検出を使用して、ドリフトを解決できます。ドリフトの解決は、ガバナンス規制への準拠に役立ちます。これは、マスターアカウント管理者の通常のオペレーションタスクです。

現在、ドリフトは AWS Control Tower によって自動的に検出されます。これは、監査アカウントに集約される Amazon SNS 通知に表示されます。検出は自動的に行われますが、ドリフトを解決するステップは手動です。これらのステップは、コンソールから実行する必要があります。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。これにより、メンバーアカウントの管理者は、特定のアカウントのドリフト通知をサブスクライブできます。

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。

トピック

- 移動されたメンバーアカウント (p. 57)
- 追加されたメンバーアカウント (p. 58)
- 削除されたメンバーアカウント (p. 58)
- 計画外のマネージド SCP の更新 (p. 59)
- 管理された OU にアタッチされた SCP (p. 59)
- 管理された OU からデタッチされた SCP (p. 60)
- メンバーアカウントにアタッチされた SCP (p. 60)
- 管理された OU の削除 (p. 60)

移動されたメンバーアカウント

このようなドリフトは、管理されたアカウント、監査アカウント、またはログアーカイブアカウントが、ある OU から別の OU に移動されたときに発生する可能性があります。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
{
  "Message" : "AWS Control Tower has detected that your managed account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Custom (ou-0123-
eEXAMPLE)' to 'Core (ou-3210-1EXAMPLE)'. For more information, including steps to resolve
 this issue, see 'https://docs.aws.amazon.com/console/controltower/move-account'",
  "MasterAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "AccountMovedBetweenOrganizationalUnits",
  "RemediationStep" : "Update Account Factory Provisioned Product",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
```

```
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

解決策

このようなドリフトが発生した場合は、以下の方法で解決できます。

- Account Factory でプロビジョニングされたアカウント – Account Factory でアカウントを更新することで、ドリフトを解決できます。詳細については、「Account Factory アカウントの更新 (p. 52)」を参照してください。
- 共有アカウント – Landing Zone 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の更新 (p. 74)」を参照してください。

追加されたメンバーアカウント

このようなドリフトは、管理されたアカウントが管理された OU に追加された場合に発生する可能性があります。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
"{
  ""Message"" : ""AWS Control Tower has detected that the managed account 'account-
email@amazon.com (012345678909)' has been added to organization o-123EXAMPLE. For more
 information, including steps to resolve this issue, see 'https://docs.aws.amazon.com/
console/controltower/add-account'"",
  ""MasterAccountId"" : ""012345678912"",
  ""OrganizationId"" : ""o-123EXAMPLE"",
  ""DriftType"" : ""AccountAddedToOrganization"",
  ""RemediationStep"" : ""Update Account Factory Provisioned Product"",
  ""AccountId"" : ""012345678909""
}"
```

解決

このようなドリフトが発生した場合は、Account Factory でアカウントを更新することで解決できます。詳細については、「Account Factory アカウントの更新 (p. 52)」を参照してください。

削除されたメンバーアカウント

このようなドリフトは、管理されたアカウントが管理された OU から削除された場合に発生する可能性があります。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
"{
  ""Message"" : ""AWS Control Tower has detected that the managed 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'"",
  ""MasterAccountId"" : ""012345678912"",
  ""OrganizationId"" : ""o-123EXAMPLE"",
  ""DriftType"" : ""AccountRemovedFromOrganization"",
  ""RemediationStep"" : ""Add account to Organization and update Account Factory
 provisioned product"",
  ""AccountId"" : ""012345678909""
}"
```

解決

このような変動が発生した場合は、Account Factory でアカウントを更新して Account Factory 更新ウィザードからそのアカウントを管理された OU に追加することで解決できます。詳細については、「Account Factory アカウントの更新 (p. 52)」を参照してください。

計画外のマネージド SCP の更新

このようなドリフトは、AWS CLI または AWS SDK の 1 つを使用して 組織 コンソールまたはプログラムでガードレールの SCP が更新されたときに発生する可能性があります。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
"{
  ""Message"" : ""AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the managed organizational unit 'Core
 (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'"",
  ""MasterAccountId"" : ""012345678912"",
  ""OrganizationId"" : ""o-123EXAMPLE"",
  ""DriftType"" : ""ServiceControlPolicyUpdated"",
  ""RemediationStep"" : ""Update Control Tower Setup"",
  ""OrganizationalUnitId"" : ""ou-0123-1EXAMPLE"",
  ""PolicyId"" : ""p-tEXAMPLE""
}"
```

解決

このようなドリフトが発生した場合は、Landing Zone を更新することで解決できます。詳細については、「ランディングゾーンの更新 (p. 74)」を参照してください。

管理された OU にアタッチされた SCP

このようなドリフトは、SCP が AWS Control Tower コンソール外部の OU にアタッチされた場合に発生する可能性があります。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
"{
  ""Message"" : ""AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the managed organizational unit
 'Custom (ou-0123-1EXAMPLE)'. For more information, including steps to resolve this issue,
 see 'https://docs.aws.amazon.com/console/controltower/scp-detached-ou'"",
  ""MasterAccountId"" : ""012345678912"",
  ""OrganizationId"" : ""o-123EXAMPLE"",
  ""DriftType"" : ""ServiceControlPolicyAttachedToOrganizationalUnit"",
  ""RemediationStep"" : ""Update Control Tower Setup"",
  ""OrganizationalUnitId"" : ""ou-0123-1EXAMPLE"",
  ""PolicyId"" : ""p-tEXAMPLE""
}"
```

解決

このようなドリフトが発生した場合は、Landing Zone を更新することで解決できます。詳細については、「ランディングゾーンの更新 (p. 74)」を参照してください。

管理された OU からデタッチされた SCP

このようなドリフトは、SCP が AWS Control Tower コンソール外部の OU からデタッチされた場合に発生する可能性があります。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
"{
  ""Message"" : ""AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the managed organizational
 unit 'Custom (ou-0123-1EXAMPLE)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached'"",
  ""MasterAccountId"" : ""012345678912"",
  ""OrganizationId"" : ""o-123EXAMPLE"",
  ""DriftType"" : ""ServiceControlPolicyDetachedFromOrganizationalUnit"",
  ""RemediationStep"" : ""Update Control Tower Setup"",
  ""OrganizationalUnitId"" : ""ou-0123-1EXAMPLE"",
  ""PolicyId"" : ""p-tEXAMPLE""
}"
```

解決

このようなドリフトが発生した場合は、Landing Zone を更新することで解決できます。詳細については、「ランディングゾーンの更新 (p. 74)」を参照してください。

メンバーアカウントにアタッチされた SCP

このようなドリフトは、SCP が 組織 コンソールのアカウントにアタッチされた場合に発生する可能性があります。ガードレールとその SCP は、AWS Control Tower コンソールを使用して OU と OU のすべてのメンバーアカウントで有効にすることができます。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
"{
  ""Message"" : ""AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the managed account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'"",
  ""MasterAccountId"" : ""012345678912"",
  ""OrganizationId"" : ""o-123EXAMPLE"",
  ""DriftType"" : ""ServiceControlPolicyAttachedToAccount"",
  ""RemediationStep"" : ""Update Control Tower Setup"",
  ""AccountId"" : ""012345678909"",
  ""PolicyId"" : ""p-tEXAMPLE""
}"
```

解決

このようなドリフトが発生した場合は、Landing Zone を更新することで解決できます。詳細については、「ランディングゾーンの更新 (p. 74)」を参照してください。

管理された OU の削除

このようなドリフトは、管理された OU が AWS Control Tower コンソールの外部で削除された場合に発生する可能性があります。以下に、このタイプのドリフトが検出されたときの Amazon SNS 通知の例を示します。

```
"{
  ""Message"" : ""AWS Control Tower has detected that the managed organizational unit
 'Custom (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'"",
  ""MasterAccountId"" : ""012345678912"",
  ""OrganizationId"" : ""o-123EXAMPLE"",
  ""DriftType"" : ""OrganizationalUnitDeleted"",
  ""RemediationStep"" : ""Delete managed organizational unit in Control Tower"",
  ""OrganizationalUnitId"" : ""ou-0123-1EXAMPLE""
}"
```

解決

このようなドリフトが発生した場合は、集中型クラウドが AWS Control Tower コンソールにサインインして [組織ユニット] のリストから管理された OU を削除する必要があります。

AWS Control Tower でのセキュリティ

クラウドセキュリティは AWS の最優先事項です。AWS のお客様は、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から利点を得られます。

セキュリティは、AWS とお客様の間の共有責任です。共有責任モデルでは、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 は、AWS クラウドで AWS のサービスを実行するインフラストラクチャの保護を担います。また、AWS では安全に使用できるサービスも用意されています。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、サードパーティの監査が定期的にテストおよび検証されています。AWS Control Tower に適用す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 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 – お客様の責任はお客様が使用する AWS の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 を使用する際に共有責任モデルを適用する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ために AWS Control Tower を設定する方法を示します。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 でのデータ保護

AWS Control Tower は、AWS 責任共有モデルに準拠し、データ保護の規制とガイドラインが含まれています。AWS は、すべての AWS サービスを実行するグローバルインフラストラクチャの保護を担います。AWS では、カスタマーコンテンツと個人データを処理するためのセキュリティ設定管理など、このインフラストラクチャでホストされているデータの制御が維持されます。AWS のお客様と APN パートナーは、データコントローラーまたはデータプロセッサの役割を果たし、AWS クラウドに配置する個人データを担当します。

データ保護目的の場合、AWS アカウント認証情報を保護して AWS Identity and Access Management (IAM) で個々のユーザーアカウントをセットアップし、そのユーザーに各自の職務を果たすために必要なアクセス許可のみが付与されるようにすることをお勧めします。また、以下の方法でデータを保護することをお勧めします。

- 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。
- CloudTrail で API とユーザーアクティビティログをセットアップします。これは、Landing Zone のセットアップ時に AWS Control Tower で自動的に処理され ます。
- AWS 暗号化ソリューションを、AWS サービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これにより、Amazon S3 に保存される個人データの検出と保護が支援されます。

顧客のアカウント番号などの機密の識別情報を、[名前] フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、コンソール、API、AWS CLI、または AWS SDK で AWS Control Tower または他の AWS サービスを使用する場合も同様です。AWS Control Tower または他のサービスに

入力したデータはすべて、診断ログの内容として取得される可能性があります。外部サーバーへの URL を指定するときは、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。

データ保護の詳細については、AWS セキュリティブログの「AWS 責任共有モデル」ブログ投稿を参照してください。AWS Control Tower では、Landing Zone に存在するコンテンツを保護する場合に役立つ以下のオプションが用意されています。

トピック

- 保管時の暗号化 (p. 63)
- 転送中の暗号化 (p. 63)
- コンテンツへのアクセスの制限 (p. 63)

保管時の暗号化

AWS Control Tower では、Landing Zone を支援するために AWS マネージド AWS KMS キーを使用して保管時に暗号化される 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 Landing Zone のセットアップ時に設定されます。また、Landing Zone 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のセキュリティの章を参照してください。

転送中の暗号化

AWS Control Tower では、Landing Zone 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 Landing Zone 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、AWS SSO 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。
- Landing Zone のセットアップ時に作成された AWS SSO グループの詳細については、「AWS Control Tower 用の AWS SSO グループ (p. 47)」を参照してください。

AWS Control Tower におけるアイデンティティとアクセスの管理

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ユニット (OU) の作成など、Landing Zoneで操作を実行するには、AWS Identity and Access Management (IAM) または AWS シングルサインオン (AWS SSO) で承認されたAWSユーザーであることを認証する必要があります。たとえば、AWS Control Tower コンソールを使用している場合は、AWS ユーザー名およびパスワードを指定して、自分の ID を認証します。

IDを認証した後、IAM で 特定の一連のオペレーションおよびリソースコントロールに対して定義されたアクセス権限セットを使用して、AWS へのアクセスが制御されます。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制御できます。

トピック

- 認証 (p. 64)
- アクセスコントロール (p. 65)
- AWS Control Tower リソースへのアクセス権限の管理の概要 (p. 65)
- AWS Control Tower のアイデンティティベースのポリシー (IAM ポリシー) の使用 (p. 68)

認証

AWS には、次のタイプのアイデンティティでアクセスできます。

- AWS アカウントのルートユーザー – AWS アカウントを初めて作成する場合は、このアカウントのすべての AWS のサービスとリソースに対して完全なアクセス権限を持つアイデンティティで始めます。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、AWS アカウントの作成に使用したメールアドレスとパスワードでのサインインによりアクセスされます。強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、root ユーザーを使用しないことです。代わりに、最初の IAM ユーザー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。
- IAM ユーザー – IAM ユーザーは、単に特定のカスタムアクセス権限を持つ、AWS アカウント内のアイデンティティです。IAM のユーザー名とパスワードを使用して、AWS 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セキュリティ保護された AWS ウェブページにサインインできます。

  ユーザー名とパスワードに加えて、各ユーザーのアクセスキーを生成することもできます。複数の SDK の 1 つを通してまたは AWS コマンドラインインターフェース (CLI) を使用して、プログラムで AWS サービスにアクセスするときに、これらのキーを使用します。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、リクエストを自分で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 全般的なリファレンスの「署名バージョン 4 署名プロセス」を参照してください。
- IAM ロール – IAM ロールは、特定のアクセス権限を持ち、アカウントで作成できる IAM アイデンティティです。IAM ロールは、AWS でできることとできないことを決定するのが、アクセス権限ポリシーを伴う AWS ID であるという点で IAM ユーザーと似ています。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 ユーザーを作成せずに、AWS Directory Service、エンタープライズユーザーディレクトリ、またはウェブアイデンティティプロバイダーの既存のアイデンティティを使用することもできます。このようなユーザーはフェデレーティッドユーザーと呼ばれます。AWS では、アイデンティティプロバイダーを通じてアクセスがリクエストされたときに、フェデレーティッドユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、IAM ユーザーガイドの「フェデレーティッドユーザーとロール」を参照してください。
  - AWS サービスへのアクセス – サービスロールは、サービスがお客様に代わってお客様の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 のサービス環境を設定するときに、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、サービスが必要とする AWS のリソースにサービスがアクセスするために必要なすべてのアクセス権限を含める必要があります。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、アクセス権限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 内部からロールを作成、修正、削除できます。たとえば、Amazon Redshift がお客様に代わって Amazon S3 バケットにアクセスし、バケットからデータを 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 のサービスにアクセス権限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 – Amazon EC2 インスタンスで実行され、AWS CLI リクエストまたは AWS API を作成しているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用します。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用するには、インスタンスプロファイルを作成してインスタンスにアタッチします。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「IAM ロールを使用して、Amazon EC2 インスタンスで実行されるアプリケーションにアクセス許可を付与する」を参照してください。
- AWS SSO ユーザーポータルに対する AWS SSO ユーザー認証は、AWS SSO に接続したディレクトリによって制御されます。ただし、ユーザーポータルからエンドユーザーが利用できる AWS アカウントに対する権限付与は、以下の 2 つの要因によって決まります。
  - AWS SSO コンソールでそれらの AWS アカウントに対するアクセス権限がだれに割り当てられているか。詳細については、AWS シングルサインオン 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 アカウントへの適切なアクセスを許可するために、AWS SSO コンソールでエンドユーザーにどのレベルのアクセス権限が付与されているか。詳細については、AWS シングルサインオン ユーザーガイドの「アクセス権限セット」を参照してください。

アクセスコントロール

Landing Zone 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、またはリストするには、オペレーションを実行する権限と、対応するリソースにアクセスする権限が必要です。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 のアクセス権限を管理する方法について説明します。

トピック

- AWS Control Tower リソースへのアクセス権限の管理の概要 (p. 65)
- AWS Control Tower のアイデンティティベースのポリシー (IAM ポリシー) の使用 (p. 68)

AWS Control Tower リソースへのアクセス権限の管理の概要

すべての AWS リソースは AWS アカウントによって所有され、となり、リソースの作成またはアクセスは、アクセス権限のポリシーによって管理されます。アカウント管理者は、アクセス許可ポリシーを IAM アイデンティティ (ユーザー、グループ、ロール) にアタッチできます。一部のサービス (AWS Lambda など) では、アクセス許可ポリシーをリソースにアタッチすることもできます。

> 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。

アクセス権限を付与する場合、アクセス権限を取得するユーザー、取得するアクセス権限の対象となるリソース、およびそれらのリソースに対して許可される特定のアクションを決定します。

トピック

- AWS Control Tower リソースおよびオペレーション (p. 66)
- リソース所有権について (p. 66)
- リソースへのアクセスの管理 (p. 66)

- ポリシー要素の指定 : アクション、効果、プリンシパル (p. 67)
- ポリシーでの条件の指定 (p. 68)

AWS Control Tower リソースおよびオペレーション

AWS Control Tower では、プライマリリソースは Landing Zone です。AWS Control Tower では、追加のリソースタイプとして ガードレールもサポートされています。ただし、AWS Control Tower では、ガードレールを既存の Landing Zone のコンテキストでのみ管理できます。ガードレールは サブリソースと呼ばれます。

リソース所有権について

AWS アカウントは、誰がリソースを作成したかにかかわらず、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、リソースの作成リクエストを認証するプリンシパルエンティティ (AWS アカウントルートユーザー、IAM ユーザー、または IAM ロール) の AWS アカウントです。以下の例では、このしくみを示しています。

- AWS アカウントの AWS アカウントのルートユーザー認証情報を使用して Landing Zone をセットアップする場合、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 Landing Zone を設定するためのアクセス許可を付与すると、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 Landing Zone を設定できます。ただし、ユーザーが属する AWS アカウントは Landing Zone リソースを所有しているとします。
- Landing Zone を設定するためのアクセス許可を持つ AWS アカウントに IAM ロールを作成する場合は、ロールを引き受けることのできるいずれのユーザーも Landing Zone を設定できます。ロールが属する AWS アカウントは Landing Zone リソースを所有しています。

リソースへのアクセスの管理

アクセスポリシーでは、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、アクセス権限の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細情報は提供しません。完全な IAM ドキュメントについては、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および説明については、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たポリシーは、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。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) のみがサポートされています。

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) (p. 66)
- リソースベースのポリシー (p. 67)

アイデンティティベースのポリシー (IAM ポリシー)

ポリシーを IAM アイデンティティにアタッチできます。たとえば、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アクセス権限ポリシーをアタッチする – Landing Zone のセットアップなどの AWS Control Tower リソースを作成するアクセス権限を付与するために、ユーザーまたはユーザーが所属するグループにアクセス権限のポリシーをアタッチできます。

- アクセス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アクセス許可を付与する) – 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アクセス許可を付与することができます。たとえば、アカウント A の管理者は、次のように他のまたは AWS にクロスアカウントのアクセス権限を別の AWS アカウント (アカウント B) または AWS サービスに付与するロールを作成することができます。
  1. アカウント A の管理者は、IAM ロールを作成して、アカウント A のリソースに権限を付与するロールに権限ポリシーをアタッチします。
  2. アカウント A の管理者は、アカウント B をそのロールを引き受けるプリンシパルとして識別するロールに、信頼ポリシーをアタッチします。
  3. アカウント B の管理者は、アカウント B のユーザーにロールを引き受ける権限を委任できるようになります。これにより、アカウント B のユーザーにアカウント A のリソースの作成とアクセスが許可されます。AWS サービスのアクセス権限を付与してロールを引き受けさせたい場合は、信頼ポリシー内のプリンシパルも、AWS サービスのプリンシパルとなることができます。

  IAM を使用したアクセス権限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。

次に、ユーザーが AWS アカウントで Landing Zone をセットアップできるポリシー例を示します。

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

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方法の詳細については、「AWS Control Tower のアイデンティティベースのポリシー (IAM ポリシー) の使用 (p. 68)」を参照してください。ユーザー、グループ、ロール、アクセス権限の詳細については、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

Amazon S3 などの他のサービスでは、リソースベースのアクセス権限ポリシーもサポートされています。たとえば、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。

ポリシー要素の指定 : アクション、効果、プリンシパル

現在、AWS Control Tower には API はありません。AWS Control Tower コンソールで Landing Zone をセットアップおよび管理できます。Landing Zone をセットアップするには、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。

以下は、最も基本的なポリシーの要素です。

- リソース – ポリシーで Amazon Resource Name (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 リソースおよびオペレーション (p. 66)」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。
- 効果 – ユーザーが特定のアクションをリクエスト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。

- プリンシパル – アイデンティティベースのポリシー (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、リソースに対するアクセス権限 (リソースベースのポリシーにのみ適用) が付与されるエンティティ (ユーザー、アカウント、サービスなど) を指定します。AWS Control Tower はリソースベースのポリシーをサポートしていません。

IAM ポリシーの構文と説明についての詳細については、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

アクセス権限を付与するとき、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。たとえば、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、AWS 全体の条件キーがあり、必要に応じて使用できます。AWS 全体を対象とするすべてのキーのリストについては、『IAM ユーザーガイド』の「条件に利用可能なキー」を参照してください。

AWS Control Tower のアイデンティティベースのポリシー (IAM ポリシー) の使用

このトピックでは、アカウント管理者が IAM アイデンティティ (ユーザー、グループ、ロール) にアクセス権限ポリシーをアタッチし、それによって AWS Control Tower リソースでオペレーションを実行するアクセス権限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 リソースへのアクセス権限の管理の概要 (p. 65)」を参照してください。

以下に示しているのは、アクセス権限ポリシーの例です。

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

このポリシーには、アカウントのすべてのリソースにおけるすべての AWS アクションの権限を付与する 1 つのステートメントがあります。これは、AWS アカウントの管理者アクセス権のアクセス許可ポリシーです。これは、Landing Zone をセットアップする IAM エンティティに必要なアクセス許可レベルです。

アイデンティティベースのポリシーでアクセス権限を得るプリンシパルを指定していないため、ポリシーでは `Principal` 要素を指定していません。ユーザーにポリシーをアタッチすると、そのユーザーが暗黙のプリンシパルになります。IAM ロールにアクセス権限ポリシーをアタッチすると、ロールの信頼ポリシーで識別されたプリンシパルがアクセス権限を得ることになります。

AWS Control Tower コンソールを使用するために必要なアクセス権限

AWS Control Tower では、Landing Zone をセットアップするために 3 つのロールを作成する必要があります。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。

AWSControlTowerAdmin

このロールは、Landing Zone 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。インラインポリシー:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

AWSControlTowerServiceRolePolicy

AWS 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:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AWSControlTowerCloudTrailRole

AWS Control Tower は、ベストプラクティスとして CloudTrail を有効にし、このロールを CloudTrail に提供します。CloudTrail は CloudTrail ログを作成して公開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:

```
{
    "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"
        }
    ]
}
```

AWS Control Tower のログ記録とモニタリング

モニタリングは、AWS Control Tower の優れたアーキテクチャの性質の重要な部分です。Landing Zone をセットアップするとき、クロスアカウントモニタリングも設定されます。作成される共有アカウントのうち 1 つは、他のすべてのアカウントですべてのログを一元的に専用で収集する、ログアーカイブアカウントです。ガードレールの状態とステータスは常に監視され、AWS Control Tower コンソールで一目で確認できます。これは、Account Factory でプロビジョニングしたアカウントの状態とステータスについても同様です。

マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。AWS では、Landing Zone でリソースとアクティビティをモニタリングするためのいくつかのツールが用意されており、潜在的なインシデントに備え、対応できます。

AWS Control Tower でのアクションとイベントのログ記録は、CloudWatch との統合によって自動的に行われます。

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

- モニタリング (p. 70)
- AWS CloudTrail を使用した AWS Control Tower アクションのログ記録 (p. 71)

モニタリング

モニタリングは、AWS Control Tower および 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。AWS には、AWS Control Tower を監視して異常を検出した場合に報告し、必要に応じて対処するために、次のモニタリングツールが用意されています。

- Amazon CloudWatch は、AWS リソースと、AWS でリアルタイムに実行されるアプリケーションを監視します。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。たとえば、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することができます。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 リソースの変更を示すシステムイベントをほぼリアルタイムのストリームとして提供します。CloudWatch イベント 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、特定のイベントを監視するルールを記述し、これらのイベントが発生したときに AWS の他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 を使用して、Amazon EC2 インスタンス、CloudTrail、その他のソースのログファイルを監視、保存し、それらのファイルにアクセスできます。CloudWatch Logs は、ログファイル内の情報を監視し、特定のしきい値が満たされたときに通知します。また、耐久性の高いストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs User Guide」を参照してください。

- AWS CloudTrail は、AWS アカウントにより、またはそのアカウントに代わって行われた、API 呼び出しおよび関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。AWS 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、および呼び出しの発生日時を特定できます。

詳細については、「AWS CloudTrail を使用した AWS Control Tower アクションのログ記録 (p. 71)」を参照してください。

AWS CloudTrail を使用した AWS Control Tower アクションのログ記録

AWS Control Tower は AWS CloudTrail と統合されています。このサービスは、AWS Control Tower のユーザー、ロール、または AWS サービスによって実行されたアクションを記録するサービスです。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。証跡を作成する場合は、AWS Control Tower のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証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、リクエストの作成元の IP アドレス、リクエストの実行者、リクエストの実行日時などの詳細を調べて、AWS Control Tower に対してどのようなリクエストが行われたかを判断できます。

CloudTrail の詳細 (設定して有効にする方法など) については、『AWS CloudTrail User Guide』を参照してください。

CloudTrail 内の AWS Control Tower 情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。AWS Control Tower でサポートされ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 CloudTrail イベントとして AWS のサービスの他のイベントとともに [Event history (イベント履歴)] に記録されます。最近のイベントは、AWS アカウントで表示、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。

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、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで作成した証跡がすべての AWS リージョンに適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した Amazon S3 バケットにログファイルが配信されます。さらに、より詳細な分析と AWS ログで収集されたデータに基づいた行動のためにその他の CloudTrail サービスを設定できます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- CloudTrail でサポートされるサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- 「複数のリージョンから CloudTrail ログファイルを受け取る」と「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。

- `SetupLandingZone`
- `UpdateAccountFactoryConfig`
- `ManageOrganizationalUnit`
- `CreateManagedAccount`
- `EnableGuardrail`
- `GetLandingZoneStatus`

- `GetHomeRegion`
- `ListManagedAccounts`
- `DescribeManagedAccount`
- `DescribeAccountFactoryConfig`
- `DescribeManagedOrganizationalUnit`
- `ListManagedOrganizationalUnits`
- `ListGuardrailViolations`
- `ListGuardrails`
- `ListEnabledGuardrails`
- `GetGuardrailComplianceStatus`
- `DescribeGuardrail`
- `ListDirectoryGroups`
- `DescribeSingleSignOn`
- `DescribeCoreService`
- `GetAvailableUpdates`

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。この ID 情報は以下のことを確認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) ユーザー認証情報のどちらを使用して送信されたかどうか。
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか.
- リクエストが、別の AWS サービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

例: AWS Control Tower ログファイルエントリ

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できる設定です。CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは任意の送信元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に関する情報が含まれます。CloudTrail イベントはログファイルに特定の順序では表示されません。

次の例は、アクションを開始したユーザーの ID のレコードを含む、CloudTrail `SetupLandingZone` 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 AWS Control Tower 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"
}
```


AWS Control Tower のコンプライアンス検証

AWS Control Tower は、組織がガードレ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 Landing Zone で使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範囲内の AWS サービスのリストについては、「コンプライアンスプログラムによる AWS 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。

サードパーティの監査レポートをダウンロードするには、AWS Artifact を使用します。詳細については、AWS Artifact ユーザーガイドの「AWS Artifact のレポートのダウンロード」を参照してください。

AWS Control Tower を使用する際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や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティおよびコンプライアンスのクイックスタートガイド – これらのデプロイメントガイドでは、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 AWS にデプロイするための手順を説明します。
- HIPAA のセキュリティとコンプライアンスに関するホワイトペーパーを作成する – 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 コンプライアンスのリソース – このワークブックとガイドのコレクションは、お客様の業界や場所に適用される場合があります。
- AWS Config – この AWS サービスでは、自社プラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。

- AWS Security Hub – この AWS サービスでは、AWS 内のセキュリティ状態を包括的に表示しており、セキュリティ業界の標準および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 の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ーゾーンを中心として構築されます。AWS リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立・隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。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、耐障害性、および拡張性が優れています。

AWS Control Tower は、4 つの AWS リージョン (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)、欧州 (アイルランド)) で利用可能であり、ホームリージョンは、内部で Landing Zone がセットアップされている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: AWS 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の手順で保護されています。

AWS が公開した API 呼び出しを使用し、ネットワーク経由で Landing Zone 内の AWS サービスとリソースにアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、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の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、一時的な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 での設定更新管理

Landing Zone を更新された状態に維持するのは、中央のクラウド管理者のメンバーの責任です。Landing Zone を更新することにより、AWS Control Tower はパッチが適用され、更新された状態で維持されます。さらに、潜在的なコンプライアンスの問題から Landing Zone を保護するために、中央のクラウド管理者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。

ランディングゾーンの更新

以下の手順は、Landing Zone を更新するためのステップについて説明します。

> Note
>
> AWS Control Tower コンソールは、Landing Zone 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、Landing Zone はすでに最新です。

Landing Zone を更新するには

1. ウェブブラウザを開いて、https://us-west-2.console.aws.amazon.com/controltower/home/update の AWS Control Tower コンソールに移動します。
2. ウィザードの情報を確認し、[更新] を選択します。これにより、Landing Zone 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 1 時間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。ナビゲーションペインで、[アカウント] を選択します。
4. [Provision new account (新しいアカウントをプロビジョニングする)] を選択して AWS Service Catalog コンソールと Account Factory 製品を開きます。
5. 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。
6. 一覧表示されているアカウントごとに以下の手順を実行して、すべてのメンバーアカウントを更新します。

   a. アカウントのメニューから [プロビジョニングされた製品の詳細] を選択します。
   b. 以下のパラメータを書き留めます。

      - SSOUserEmail
      - AccountEmail
      - SSOUserFirstName
      - SSOUSerLastName
      - AccountName

   c. [アクション] で、[更新] を選択します。
   d. 更新する製品の [バージョン] の隣にあるラジオボタンを選択して、[次へ] を選択します。
   e. 前に説明したパラメータ値を入力します。[ManagedOrganizationlUnit] には、アカウントがある OU を選択します。この情報は、AWS Control Tower コンソールの [アカウント] の下にあります。
   f. [次へ] を選択します。
   g. 変更内容を確認し、[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。

ドリフトの解決

Landing Zone を作成するとき、Landing Zone とすべての OU、アカウント、リソースは、選択したガードレールにより適用されるすべてのガバナンスルールに準拠します。管理者およびユーザーが Landing Zone を使用するとき、このコンプライアンス状況に変更が発生する可能性があります。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。いずれにしても、変更によりコンプライアンスが複雑になる可能性があります。

変更や設定の更新が必要なリソースを識別するドリフト検出を使用して、ドリフトを解決できます。ドリフトの解決は、ガバナンス規制の遵守に役立ち、マスターアカウント管理者の通常のオペレーションタスクです。詳細については、「AWS Control Tower でのドリフトの検出および解決 (p. 57)」を参照してください。

制限

この章では、AWS Control Tower を使用するときに注意すべき AWS のサービス制限を取り上げます。サービス制限の問題により Landing Zone を設定できない場合は、AWS サポート にお問い合わせください。

統合サービスの制限

AWS のサービスにはそれぞれ異なる制限があります。サービスの制限は、サービスのドキュメントに記載されています。詳細については、以下の関連リンクを参照してください。

- AWS CloudFormation – AWS CloudFormation の制限
- AWS CloudTrail – AWS CloudTrail での制限
- Amazon CloudWatch – CloudWatch の制限
- AWS Config – AWS Config の制限
- AWS Identity and Access Management – IAM エンティティおよびオブジェクトの制限
- AWS Lambda – AWS Lambda の制限
- AWS Organizations – AWS Organizations の制限
- Amazon Simple Storage Service – バケットの制約と制限
- AWS Service Catalog – AWS Service Catalog のデフォルトサービス制限
- AWS シングルサインオン – AWS SSO での制限
- Amazon Simple Notification Service – Amazon Simple Notification Service (Amazon SNS) の制限
- AWS Step Functions – の制限

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

- ウォークスルー: AWS Control Tower マネージドリソースのクリーンアップ (p. 77)
- チュートリアル: VPC を使用せずに AWS Control Tower を設定する (p. 81)

ウォークスルー: AWS Control Tower マネージドリソースのクリーンアップ

Landing Zone を設定したとき、ユーザーに代わって AWS Control Tower により Landing Zone でリソースとサービスがプロビジョニングされました。たとえば、複数のアカウントを持つ AWS Organizations 組織や組織単位 (OU) がプロビジョニングされました。また、AWS CloudFormation スタック、スタックセットおよび AWS Organizations ポリシーを使用して、アカウントにガードレールがデプロイされました。

「使用開始」の手順を完了した後、または企業の AWS Control Tower を評価していない場合は、Landing Zone 設定時に作成したリソースをクリーンアップできます。次の手順では、ライフサイクル目的でこれらのリソースをクリーンアップする方法を示します。

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、Landing Zone のホームリージョンにある AWS マネジメントコンソール にサインインしている必要があり、Landing Zone を含むマスターアカウントの管理者権限を持つ IAM ユーザーとしてサインインしている必要があります。

> Warning
>
> これらは、AWS Control Tower 設定にずれ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。これらの手順は、Landing Zone 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。

トピック

- SCP の削除 (p. 77)
- StackSets およびスタックの削除 (p. 78)
- ログアーカイブアカウントでの Amazon S3 バケットの削除 (p. 79)
- Account Factory のクリーンアップ (p. 79)
- ロールおよびポリシーのクリーンアップ (p. 80)
- AWS Control Tower クリーンアップのヘルプ (p. 81)

SCP の削除

AWS Control Tower では、ガードレ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 SCP を削除するには

1. Open the 組織 console at https://console.aws.amazon.com/organizations/.
2. [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 では、StackSets とスタックを使用して、Landing Zone にあるガードレールに関連する AWS Config ルール をデプロイします。次の手順では、これらのリソースを削除する方法を示します。

AWS CloudFormation StackSets を削除するには

1. https://console.aws.amazon.com/cloudformation で AWS 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. ページの下部の [スタック] テーブルで、テーブル内のすべてのアカウントの AWS アカウント ID 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. [Manage StackSet (StackSet の管理)] を選択して、管理ウィザードを開きます。
   d. [アクションの選択] から [Delete stacks (スタックの削除)] を選択し、[次へ] を選択します。
   e. [Set deployment options (デプロイオプションの設定)] の [Specify accounts (アカウントの指定)] で、[Delete stacks from account (アカウントからスタックを削除する)] を選択します。
   f. テキストフィールドにステップ 3.b で記録した、作成した AWS アカウント ID をコンマで区切って入力します。例: *123456789012*、*098765431098*、など。
   g. [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、[次へ] を選択します。
   h. [確認] ページで、選択内容を確認し、[スタックの削除] を選択します。
   i. [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. [StackSet properties (StackSet のプロパティ)] ページの [スタック] テーブルが空になったとき、プロセスが完了しています。
5. [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。

AWS CloudFormation スタックを削除するには

1. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。
2. [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. [アクション] メニューから、[スタックの削除] を選択します。
   c. 表示され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、[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 Amazon S3 バケットの削除

次の手順では、[AWSControlTowerExecution アーカイブログ] グループで AWS SSO 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、次にログアーカイブアカウントで Amazon S3 バケットを削除する方法を示します。

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. Open the 組織 console at https://console.aws.amazon.com/organizations/.
2. [アカウント] タブから、[ログアーカイブ] アカウントを選択します。
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、[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. [ロール] に [AWSControlTowerExecution] と入力します。
8. [表示名] にテキストを入力します。
9. お気に入りの [色] を選択します。
10. [Switch Role (ロールの切り替え)] を選択します。

Amazon S3 バケットを削除するには

1. https://console.aws.amazon.com/s3/ にある 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] 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、[確認] を選択します。

Account Factory のクリーンアップ

次の手順では、[AWSServiceCatalogAdmins] グループで AWS SSO ユーザーとしてサインインし、Account Factory アカウント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マスター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 [マスター] 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、このロールで AWS マネジメントコンソール にサインインします。

Account Factory をクリーンアップするには

1. https://console.aws.amazon.com/servicecatalog/ で AWS Service Catalog 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 [ポートフォリオリスト] を選択します。
3. [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 [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. [制約の削除] を選択します。
7. 表示され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、[続行] を選択します。
8. ページの [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. [製品の削除] を選択します。
10. 表示され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、[続行] を選択します。
11. [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. 表示され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、[続行] を選択します。
14. 左のナビゲーションメニューから [ポートフォリオリスト] を選択します。
15. [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. 表示され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、[続行] を選択します。
18. 左側のナビゲーションメニューで、[製品リスト] を選択します。
19. [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. [アクション] から、[Delete product] を選択します。
22. 表示され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、[続行] を選択します。

ロールおよびポリシーのクリーンアップ

これらの手順では、Landing Zone の設定時に作成されたロールおよびポリシーをクリーンアップする方法を示します。

AWS SSO AWSServiceCatalogEndUserAccess ロールを削除するには

1. AWS シングルサインオン コンソール (https://console.aws.amazon.com/singlesignon/) を開きます。
2. AWS リージョンを 米国東部 (バージニア北部) に変更します。
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. マスターアカウントのリンクを選択します。
5. [アクセス権限セット] のドロップダウンを選択し、[AWSServiceCatalogEndUserAccess]、[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. [アクセス許可セット] 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. https://console.aws.amazon.com/iam/ にある IAM 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 [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. [ロールの削除] を選択します。
c. 表示され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、[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. https://console.aws.amazon.com/iam/ にある IAM 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 [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 [ポリシーアクション] と [削除] を選択します。
c. 表示され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、[削除] を選択します。

AWS Control Tower クリーンアップのヘルプ

このクリーンアッププロセス中に解決できない問題が発生した場合は、AWS サポートにお問い合わせください。

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 マスターアカウント VPC (Virtual Private Cloud) 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。

AWS Control Tower マスターアカウント VPC の削除

AWS Control Tower 外では、すべての AWS のお客様にデフォルトの VPC があります。これは、Amazon Virtual Private Cloud (Amazon VPC) コンソール (https://console.aws.amazon.com/vpc/) に表示されます。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 のデフォルト VPC を削除し、新しい AWS Control Tower デフォルト VPC を作成します。新しい VPC は AWS Control Tower マスター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 マスターアカウント VPC と呼びます。

AWS Control Tower マスターアカウント VPC を Amazon VPC コンソールで確認する場合は、その名前の末尾に (default) という単語が 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 マスターアカウント VPC を特定する必要があります。

AWS Control Tower マスターアカウント 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 マスターアカウント VPC を削除するには

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。
2. **VPC** を検索するか、 AWS Service Catalog のオプションから [VPC] を選択します。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 (自分の 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 マスターアカウント 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。

VPC なしのアカウントを AWS Control Tower で作成する

エンドユーザーのワークロードに VPC が必要ない場合は、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いて、https://console.aws.amazon.com/controltower の AWS Control Tower コンソールに移動します。
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)] セクションの [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 (新しいアカウントの VPC 設定オプション)] セクションに移動します。

    a. [Internet-accessible subnet (インターネットにアクセスできるサブネット)] のトグルスイッチをオフにします。
    b. [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。
    c. [Address range (CIDR) restriction for account VPCs (アカウント VPC のアドレス範囲 (CIDR) 制限] の値を `10.0.0.0/16` に変更します。
    d. [Regions for VPC creation (VPC を作成するリージョン)] 列のすべてのチェックボックスをオフにします。
7. [Save] を選択します。

起こり得るエラー

AWS Control Tower マスターアカウント 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。

- 既存のマスターアカウントには、 AWS Control Tower マスターアカウント 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。

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 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起動の失敗

マスター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 サポートまでお問い合わせください。

AWS Control Tower 外部で E メールアドレスを変更しないでください。

共有サービスアカウント (マスターアカウント、監査アカウント、ログアーカイブアカウント) の E メールアドレスは変更しないでください。これらのいずれかの E メールアドレスを変更した場合は、AWS サポートにご連絡ください。

Account Factory で作成されたメンバーアカウントの E メールアドレスは変更できますが、Account Factory でアカウントを更新することでのみ変更できます。詳細については、「Account Factory アカウントの更新 (p. 52)」を参照してください。

アカウントの組織単位を AWS Control Tower 外に移行しない

AWS Control Tower 内でアカウントの組織単位を移行するには、Account Factory でアカウントを更新する手順を使用します 。ステップ 4(e) で、現在の組織単位の名前ではなく、アカウントの新しい組織単位の名前を選択します。

詳細については、「Account Factory アカウントの更新 (p. 52)」を参照してください。

ドキュメント履歴

- 前回のドキュメント更新日: 2019 年 9 月 6 日

以下の表は、AWS Control Tower ユーザーガイドの重要な変更点をまとめたものです。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。

update-history-change	update-history-description	update-history-date
追加の予防的ガードレールが AWS Control Tower で使用できるようになりました (p. 85)	AWS Control Tower の予防的ガードレールは、組織およびリソースと、環境との整合性を維持します。	September 6, 2019
追加の発見的ガードレールが AWS Control Tower で使用できるようになりました (p. 85)	AWS Control Tower の発見的ガードレールは、組織の状態とリソースに関する情報を提供します。	August 27, 2019
AWS Control Tower は一般利用可能です。 (p. 85)	AWS Control Tower は、マルチアカウントの 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。	June 24, 2019

AWS の用語集

最新の AWS の用語については、『AWS General Reference』の「AWS の用語集」を参照してください。