ユーザーガイド

AWS Control Tower

AWS Control Tower: ユーザーガイド

Table of Contents

AWS Control Tower とは

AWS Control Tower は、規範的なベストプラクティスに従って、 AWS マルチアカウント環境を簡単に設定および管理する方法を提供します。 AWSControl Tower は、 AWS Organizations、 AWS Service Catalog、 など、他のいくつかの AWS サービスの機能をオーケストレーションし AWS IAM Identity Center、1 時間以内にランディングゾーンを構築します。リソースは、ユーザーに代わって設定および管理されます。

AWS Control Tower オーケストレーションは、 の機能を拡張します AWS Organizations。組織とアカウントがベストプラクティスと異なるドリフトから守るために、AWSControl Tower はコントロール (ガードレールとも呼ばれます) を適用します。例えば、コントロールを使用して、セキュリティログと必要なクロスアカウントアクセス許可が作成され、変更されないようにすることができます。

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

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

つまり、AWSControl Tower は、何千もの企業と協力して確立されたベストプラクティスに基づいて、安全で準拠したマルチアカウント AWS 環境をセットアップして管理するための最も簡単な方法を提供します。AWS Control Tower の操作と AWS 、マルチアカウント戦略で概説されているベストプラクティスの詳細については、「」を参照してくださいAWS マルチアカウント戦略: ベストプラクティスガイダンス。

機能

AWS Control Tower には次の機能があります。

- ランディングゾーン — ランディングゾーンは、セキュリティとコンプライアンスのベストプラクティスに基づく、優れたアーキテクチャ設計の複数アカウントの環境です。これは、コンプライアンス規制の対象となるすべての組織単位 (OUs) 、アカウント、ユーザー、およびその他のリソー

スを保持するエンタープライズ全体のコンテナです。ランディングゾーンは、いずれの規模の企業のニーズに合わせてもスケーリングできます。

- コントロール – コントロール (ガードレールと呼ばれることもあります) は、 AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。これは、わかりやすい形式で表されます。予防コントロール、検出コントロール、プロアクティブコントロールの 3 種類があります。必須、強く推奨、選択的の 3 つのガイダンスカテゴリが適用されます。コントロールの詳細については、「コントロールの仕組み」を参照してください。
- Account Factory – Account Factory は、新しいアカウントのプロビジョニングを事前承認されたアカウント設定で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。 AWSControl Tower には、組織内のアカウントプロビジョニングワークフローを自動化するのに役立つ組み込み Account Factory が用意されています。詳細については、「Account Factory でのアカウントのプロビジョニングと管理」を参照してください。
- ダッシュボード — このダッシュボードでは、中央のクラウド管理者のチームがランディングゾーンを継続的に監視できます。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たアカウント、ポリシーの適用が有効になっているコントロール、ポリシーの非準拠の継続的な検出が有効になっているコントロール、およびアカウントと 別に整理された非準拠リソースを表示しますOUs。

AWS Control Tower が他の AWS サービスとやり取りする方法

AWS Control Tower は AWS Service Catalog AWS IAM Identity Center、 や などの信頼できる AWS サービス上に構築されています AWS Organizations。詳細については、「統合サービス」を参照してください。

AWS Control Tower を他の AWS サービスに組み込むことで、既存のワークロードの移行に役立つソリューションを作成できます AWS。詳細については、AWS「Control Tower を活用する方法」および「ワークロード CloudEndure を に移行する方法 AWS」を参照してください。

構成、ガバナンス、拡張性

- 自動アカウント設定： AWS Control Tower は、プロビジョニングされた製品の上に抽象化として構築された Account Factory (または「自動販売機」) を使用して、アカウントのデプロイと登録を自動化します AWS Service Catalog。Account Factory は AWS アカウントを作成および登録でき、それらのアカウントにコントロールとポリシーを適用するプロセスを自動化します。
- 一元化されたガバナンス： AWS Control Tower は、 の機能を採用することで AWS Organizations、マルチアカウント環境全体で一貫したコンプライアンスとガバナンスを確保するフレームワークをセットアップします。この AWS Organizations サービスは、アカウントの

一元的なガバナンスと管理、アカウントの作成、サービスコントロールポリシー () など AWS Organizations APIs、マルチアカウント環境を管理するための重要な機能を提供しますSCPs。

- 拡張性： AWS Control Tower コンソールだけでなく、 で直接作業することで AWS Organizations、独自の AWS Control Tower 環境を構築または拡張できます。既存の組織を登録し、既存のアカウントを AWS Control Tower に登録すると、変更が AWS Control Tower に反映されます。AWS Control Tower ランディングゾーンを更新して、変更を反映することができます。ワークロードにさらに高度な機能が必要な場合は、AWSControl Tower とともに他の AWS パートナーソリューションを活用できます。

AWS Control Tower を初めてお使いになる方向けの情報

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

AWS Control Tower の仕組み

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

AWS Control Tower ランディングゾーンの構造

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

- ルート – ランディングゾーンOUsに他のすべての を含む親。

- セキュリティ OU - この OU には、ログアーカイブアカウントと監査アカウントが含まれています。これらのアカウントは、共有アカウントとも呼ばれます。ランディングゾーンを起動するときに、これらの共有アカウント用にカスタマイズされた名前を選択できます。また、セキュリティとログ記録のために既存の AWS アカウントを AWS Control Tower に持ち込むオプションもあります。ただし、これらの名前を後で変更することはできません。また、初回起動後にセキュリティとログ記録のために既存のアカウントを追加することはできません。
- サンドボックス OU - サンドボックス OU は、ランディングゾーンを有効にしている場合にランディングゾーンを起動すると作成されます。この およびその他の登録済み には、ユーザーがAWSワークロードを実行するために使用する登録済みアカウントOUsが含まれています。
- IAM Identity Center ディレクトリ – このディレクトリには、IAMIdentity Center ユーザーが格納されます。各 IAM Identity Center ユーザーのアクセス許可の範囲を定義します。
- IAM Identity Center ユーザー – これらは、ユーザーがランディングゾーンで AWS ワークロードを実行するために引き受けることができる ID です。

ランディングゾーンをセットアップした場合に起きること

ランディングゾーンを設定すると、AWSControl Tower はユーザーに代わって管理アカウントで次のアクションを実行します。

- AWS Organizations 組織ルート構造に含まれるOUsセキュリティとサンドボックス (オプション) の 2 つの組織単位 () を作成します。
- セキュリティ OU 内に共有アカウントを 2 つ作成または追加する (ログアーカイブアカウントと監査アカウント)。
- デフォルトの AWS Control Tower 設定を選択した場合、または ID プロバイダーを自己管理できる場合、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、IAMIdentity Center にクラウドネイティブディレクトリを作成します。
- 必須の予防コントロールをすべて適用してポリシーを実施する。
- 必須の検出コントロールをすべて適用して設定違反を検出する。
- 予防コントロールは管理アカウントには適用されません。
- 管理コントロールを除き、ガードレールを組織全体に適用する。

AWS Control Tower ランディングゾーンとアカウント内のリソースを安全に管理する

- ランディングゾーンを作成すると、多数の AWS リソースが作成されます。AWS Control Tower を使用するには、このガイドで説明されている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しないでください。これらのリソースを変更または削除すると、ランディングゾーンの状態が不明になります。詳細については、「AWS Control Tower リソースの作成と変更に関するガイダンス」を参照してください。

- オプションのコントロール (強く推奨されるガイダンスまたは選択的ガイダンスを持つコントロール) を有効にすると、AWSControl Tower はアカウントで管理する AWS リソースを作成します。AWS Control Tower によって作成されたリソースを変更または削除しないでください。これにより、コントロールの状態が不明になる可能性があります。

共有アカウントとは

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

管理アカウントとは

これは、ランディングゾーン専用に作成したアカウントです。このアカウントは、ランディングゾーンでのすべての請求に使用されます。また、アカウントの Account Factory プロビジョニングや、OUsと の管理にも使用されます。

> **Note**
>
> AWS Control Tower 管理アカウントからどのようなタイプの本番ワークロードも実行することはお勧めしません。ワークロードを実行するには、別の AWS Control Tower アカウントを作成します。

詳細については、「管理アカウント」を参照してください。

ログアーカイブアカウントとは

このアカウントは、ランディングゾーン内のすべてのアカウントからのAPIアクティビティとリソース設定のログのリポジトリとして機能します。

詳細については、「ログアーカイブアカウント」を参照してください。

監査アカウントとは

監査アカウントは、セキュリティチームとコンプライアンスチームに対してランディングゾーンのすべてのアカウントへの読み書きアクセスを許可するように設計された制限付きのアカウントです。監

査アカウントからは、Lambda 関数にのみ付与されるロールを使用して、アカウントをレビューするためにプログラムによってアクセスできます。監査アカウントでは、他のアカウントに手動でログインすることはできません。Lambda 関数とロールの詳細については、「別の AWS アカウント からロールを引き受けるように Lambda 関数を設定する」を参照してください。

詳細については、「監査アカウント」を参照してください。

コントロールの仕組み

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

予防コントロールにより、アクションの発生が防止されます。例えば、Amazon S3 バケットのバケットポリシーへの変更を許可しない (以前はログアーカイブへのポリシー変更を許可しない) という選択コントロールは、ログアーカイブ共有アカウント内のIAMポリシー変更をすべて禁止します。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。リソースもログインします AWS Config。

検出コントロールは、特定のイベントが発生したときに検出し、 でアクションをログに記録します CloudTrail。例えば、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の検出という強く推奨されるコントロールは、暗号化されていない Amazon EBSボリュームがランディングゾーンのEC2インスタンスにアタッチされているかどうかを検出します。

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

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

関連トピック

- AWS Control Tower でドリフトを検出して解決する

AWS Control Tower と の連携方法 StackSets

AWS Control Tower は AWS CloudFormation StackSets を使用して、 アカウントのリソースをセットアップします。各スタックセットには、アカウント StackInstances に対応する と、アカウント AWS リージョン ごとに に対応する があります。 AWSControl Tower は、アカウントとリージョンごとに 1 つのスタックセットインスタンスをデプロイします。

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

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

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

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

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

用語

Control AWS Tower ドキュメントに表示されるいくつかの用語の簡単な確認を次に示します。

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

- 組織と の詳細についてはOUs、AWS Organizations 「 の用語と概念」を参照してください。AWS Control Tower を初めて使用する場合は、その用語から始めることをお勧めします。
- AWS Organizations は、ワークロードの拡大とスケーリングに合わせて環境を一元管理するための AWS サービスです AWS。 AWSControl Tower は AWS Organizations 、 を使用してアカウントを作成し、OU レベルで予防コントロールを適用し、一元的な請求を行います。
- AWS Account Factory アカウントは、AWSControl Tower の Account Factory を使用してプロビジョニングされた AWS アカウントです。Account Factory は、アカウントの「自動販売機」と非公式に呼ばれることもあります。
- AWS Control Tower ホームリージョンは、AWSControl Tower ランディングゾーンがデプロイされた AWS リージョンです。ホームリージョンは、ランディングゾーン設定で表示できます。
- AWS Service Catalog では、一般的にデプロイされる IT サービスを一元管理できます。このドキュメントのコンテキストでは、Account Factory は AWS Service Catalog を使用して、カスタマイズされたブループリントからの AWS アカウントを含む新しいアカウントをプロビジョニングします。
- AWS CloudFormation StackSets は、スタックの機能を拡張するリソースの一種です。これにより、1 回のオペレーションと 1 つの CloudFormationテンプレートで複数のアカウントとリージョンにまたがるスタックを作成、更新、または削除できます。
- スタックインスタンスは、リージョン内のターゲットアカウントのスタックへの参照です。
- Astack は、単一のユニットとして管理できる AWS リソースのコレクションです。
- アグリゲータは、組織内の複数のアカウントとリージョンから AWS Config 設定とコンプライアンスデータを収集する AWS Config リソースタイプで、1 つのアカウント内でこのコンプライアンスデータを表示およびクエリできます。
- コンフォーマンスパックは、アカウントとリージョン、または の組織全体に単一のエンティティとしてデプロイできる AWS Config ルールと修復アクションのコレクションです AWS Organizations。コンフォーマンスパックを使用すると、AWSControl Tower 環境をカスタマイズできます。詳細を説明している技術的なブログについては、「関連情報」を参照してください。

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

  アカウントは一度に 1 つの組織のメンバーにしかなることができず、その料金はその組織の管理アカウントに請求されます。メンバーアカウントは、組織のルートコンテナに移動できます。
- AWS アカウント： AWS アカウントは、リソースコンテナおよびリソース分離境界として機能します。 AWS アカウントは、請求と支払いに関連付けることができます。 AWS アカウントは、AWSControl Tower のユーザーアカウント (IAMユーザーアカウントと呼ばれることもあります) とは異なります。Account Factory プロビジョニングプロセスによって作成されたアカウントは AWS accounts です。 AWS アカウントは、アカウント登録または OU 登録プロセスによって AWS Control Tower に追加することもできます。

- コントロール： コントロール (ガードレールとも呼ばれます) は、AWSControl Tower 環境全体に継続的なガバナンスを提供する高レベルのルールです。各コントロールは、1 つのルールを適用します。予防コントロールは で実装されますSCPs。検出コントロールは AWS Config ルールで実装されます。プロアクティブコントロールは AWS CloudFormation フックで実装されます。詳細については、「コントロールの仕組み」を参照してください。
- ランディングゾーン: ランディングゾーンは、デフォルトのアカウント、アカウント構造、ネットワークおよびセキュリティレイアウトなど、推奨される開始点を提供するクラウド環境です。ランディングゾーンから、ソリューションとアプリケーションを利用するワークロードをデプロイできます。
- ネストされた OU: AWS Control Tower のネストされた OU は、別の OU に含まれる OU です。ネストされた OU は、厳密に親を 1 つ持つことができ、各アカウントを厳密に 1 つの OU のメンバーにすることができます。ネストされた階層OUsを作成します。階層内の 1 つの OUs にポリシーをアタッチすると、ポリシーは下に移動し、その下にあるすべての OUsアカウントと アカウントに影響します。AWS Control Tower のネストされた OU 階層の深さは最大 5 レベルです。
- 親 OU: 階層内の現在の OU のすぐ上にある OU。各 OU は、親 OU を 1 つだけ持つことができます。
- 子 OU: 階層内の現在の OU より下にある OU。OU には多数の子 を含めることができますOUs。
- OU 階層： AWS Control Tower では、ネストされた の階層は最大 5 つのレベルを持つOUsことができます。ネストの順序は、レベルと呼ばれます。階層の最上位は、レベル 1 と呼ばれます。
- 最上位の OU: 最上位の OU は、ルート自体ではなく、ルートの直下にある任意の OU です。ルートは、OU とは見なされません。
- 管理対象： 管理対象リージョンは、組織が設定したガバナンスポリシーに従って、AWSControl Tower によって環境で管理および制御されます。これらは、ベストプラクティスと組織ポリシーに準拠するためにモニタリング AWS リージョン されます。AWS Control Tower コントロールを有効にすると、これらのリージョンのリソースは保護されます。
- 管理対象外： 管理対象外ステータスを示すリージョンは、AWSControl Tower によって制御またはモニタリングされません。これらは AWS リージョン 通常、AWSControl Tower が適用するのと同じガバナンスポリシーに準拠していません。これらのリージョンにリソースを作成できますが、それらのリソースは AWS Control Tower コントロールによって保護されません。
- 拒否： 拒否されたリージョンは AWS Control Tower によって特にブロックされます。AWS Control Tower 環境内では、これらの でリソースをプロビジョニングすることはできません AWS リージョン。

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 のサービスおよびランディングゾーン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。例えば、Account Factory でアカウントをプロビジョニングするための Service Catalog と、ランディングゾーンで追跡されているイベントの AWS CloudTrail に対してお支払いいただきます。AWS Control Tower に関する料金表や料金については、「AWS Control Tower の料金」を参照してください。

AWS Control Tower のアカウントからエフェメラルワークロードを実行している場合は、AWS Config に関連するコストが増大する可能性があります。詳細については、「AWS Config 料金表」を参照してください。これらのコストの管理の詳細については、AWS アカウント担当者にお問い合わせください。AWS Config で AWS Control Tower を使用する方法の詳細については、「でリソースの変更をモニタリングする AWS Config」を参照してください。

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

セットアップ

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

にサインアップする AWS

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

他のタスクで必要になるため、 AWS アカウント番号を書き留めておきます。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次のステップを実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/サインアップを開きます。
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、電話キーパッドで検証コードを入力するように求められます。

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

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ に移動してマイアカウントを選択すると、いつでも現在のアカウントアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

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

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

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

管理アクセスを持つユーザーを作成する

1. IAM Identity Center を有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM Identity Center で、ユーザーに管理アクセス権を付与します。

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

管理アクセス権を持つユーザーとしてサインインする

- IAM Identity Center ユーザーでサインインするには、IAMIdentity Center ユーザーの作成時に E メールアドレスにURL送信されたサインインを使用します。

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

追加のユーザーにアクセス権を割り当てる

1. IAM Identity Center で、最小特権のアクセス許可を適用するベストプラクティスに従うアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

> **アカウントのセキュリティ**
>
> AWS Control Tower アカウントのセキュリティを保護するベストプラクティスの設定方法に関する追加のガイダンスは、 AWS Organizations ドキュメントに記載されています。
>
> - 管理アカウントのベストプラクティス
> - メンバーアカウントのベストプラクティス

次のステップ

AWS Control Tower の使用開始方法

AWS Control Tower の使用開始方法

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

現在 AWS のお客様で、AWS Control Tower を初めて使用する場合は、先に進む前に AWS Control Tower ランディングゾーンの計画というセクションを確認することをお勧めします。

トピック

AWS Control Tower クイックスタートガイド

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

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

開始する前に

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

ムリージョンを変更できません。ホームリージョンの選択方法の詳細については、「ランディングゾーンのセットアップに関する管理上のヒント」を参照してください。

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

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

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

クイックスタート手順

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

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

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

前提条件: 管理アカウントの起動前自動チェック

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

- AWS Control Tower を起動するには、 の既存のサービス制限で十分 AWS アカウント である必要があります。詳細については、「AWS Control Tower の制限とクォータ」を参照してください。
- は、次の AWS サービスにサブスクライブ AWS アカウント する必要があります。
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (IAM)
  - AWS Lambda

> **Note**
>
> デフォルトでは、すべてのアカウントがこれらのサービスに登録されています。

AWS IAM Identity Center (IAM Identity Center) のお客様に関する考慮事項

- AWS IAM Identity Center (IAM アイデンティティセンター) が既に設定されている場合、AWS Control Tower ホームリージョンは IAM アイデンティティセンターリージョンと同じである必要があります。
- IAM Identity Center は、組織の管理アカウントにのみインストールできます。
- 選択した ID ソースに基づいて、次の 3 つのオプションが IAM Identity Center ディレクトリに適用されます。

- IAM Identity Center ユーザーストア: SSO for AWS Control Tower が IAM Identity Center でセットアップされている場合、AWS Control Tower は IAM Identity Center ディレクトリにグループを作成し、メンバーアカウント用に選択したユーザーに対してこれらのグループへのアクセスをプロビジョニングします。
- Active Directory: IAM Identity Center for AWS Control Tower が Active Directory でセットアップされている場合、AWS Control Tower は IAM Identity Center ディレクトリを管理しません。新規 AWS アカウントにユーザーやグループを割り当てません。
- 外部 ID プロバイダー: AWS Control Tower for IAM Identity Center が外部 ID プロバイダー (IdP) でセットアップされている場合、AWS Control Tower は IAM Identity Center ディレクトリにグループを作成し、メンバーアカウント用に選択したユーザーに対してこれらのグループへのアクセスをプロビジョニングします。アカウントの作成時に Account Factory の外部 IdP から既存のユーザーを指定できます。AWS Control Tower は、IAM Identity Center と外部 IdP 間で同じ名前のユーザーを同期するときに、その新しく発行されたアカウントへのアクセス許可を指定されたユーザーに付与します。AWS Control Tower のデフォルトグループの名前と一致するように外部 IdP にグループを作成することもできます。これらのグループにユーザーを割り当てると、ユーザーが登録済みのアカウントにアクセスできるようになす。

IAM Identity Center および AWS Control Tower の使用に関する詳細については、「IAM Identity Center アカウントと AWS Control Tower について知っておくべきこと」を参照してください。

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

- では、組織の管理アカウントで信頼されたアクセスを有効にする AWS アカウント ことはできません AWS Config。信頼されたアクセスを無効にする方法については、信頼されたアクセスを有効または無効にする方法に関する AWS Organizations ドキュメントを参照してください。
- AWS Control Tower に登録する予定の既存のアカウントに既存の AWS Config レコーダー、配信チャネル、または集約設定がある場合は、ランディングゾーンの設定後にアカウントの登録を開始する前に、これらの設定を変更または削除する必要があります。この事前チェックは、ランディングゾーンの起動時に AWS Control Tower 管理アカウントには適用されません。詳細については、「既存の AWS Config リソースを持つアカウントを登録する」を参照してください。
- AWS Control Tower のアカウントからエフェメラルワークロードを実行している場合、Config AWS に関連するコストが増加する可能性があります。これらのコストの管理の詳細については、AWS アカウント担当者にお問い合わせください。
- AWS Control Tower にアカウントを登録すると、アカウントは AWS Control Tower 組織の AWS CloudTrail 証跡によって管理されます。アカウントに CloudTrail 追跡の既存のデプロイがある場

合、AWS Control Tower にアカウントを登録する前にアカウントの既存の追跡を削除しない限り、料金が重複して発生する可能性があります。組織レベルの追跡と AWS Control Tower の詳細については、「料金」を参照してください。

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

コンソールから AWS Control Tower の使用を開始する

この入門手順は、AWSControl Tower 管理者を対象としています。AWS Control Tower コンソールを使用してランディングゾーンを設定する準備ができたら、以下の手順に従います。開始から完了まで、所要時間は約 30 分です。この手順は、いくつかの前提条件と 3 つの主なステップを必要とします。

現在 AWS のお客様で Control Tower AWS を初めて使用する場合は、先に進む前に AWS Control Tower ランディングゾーンの計画というセクションを確認することをお勧めします。

トピック

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

ランディングゾーン設定に対する想定

AWS Control Tower ランディングゾーンを設定するプロセスには、複数のステップがあります。AWS Control Tower ランディングゾーンの特定の側面は設定可能です。それ以外の選択肢は、セットアップ後に変更できません。

セットアップ時に設定する主な項目

- セットアップ時に最上位の OU 名を選択できます。また、ランディングゾーンのセットアップ後に OU 名を変更することもできます。デフォルトでは、最上位レベルOUsは Security と Sandbox

という名前です。詳細については、「アーキテクチャが適切に設計された環境をセットアップするためのガイドライン」を参照してください。

- セットアップ中に、デフォルトでログアーカイブと監査と呼ばれる AWS Control Tower が作成する共有アカウント用にカスタマイズされた名前を選択できますが、セットアップ後にこれらの名前を変更することはできません。(これは 1 回限りの選択です)。
- セットアップ時に、必要に応じて AWS Control Tower の既存の AWS アカウントを指定して、監査およびログアーカイブアカウントとして使用できます。既存の AWS アカウントを指定する予定があり、それらのアカウントに既存の AWS Config リソースがある場合は、アカウントを AWS Control Tower に登録する前に既存の AWS Config リソースを削除する必要があります。(これは 1 回限りの選択です)。
- を初めて設定する場合、またはランディングゾーンバージョン 3.0 にアップグレードする場合は、AWSControl Tower が組織の組織レベルの AWS CloudTrail 証跡を設定することを許可するか、AWSControl Tower によって管理される証跡をオプトアウトして独自の CloudTrail 証跡を管理するかを選択できます。ランディングゾーンを更新するたびに、AWSControl Tower によって管理される組織レベルの証跡をオプトインまたはオプトアウトできます。
- オプションで、ランディングゾーンを設定または更新する際、Amazon S3 ログバケットとログアクセスバケットにカスタマイズされた保持ポリシーを設定できます。
- オプションで、AWSControl Tower コンソールからカスタマイズされたメンバーアカウントのプロビジョニングに使用する、以前に定義された設計図を指定できます。使用できるブループリントがない場合は、後でアカウントをカスタマイズできます。「Account Factory Customization を使用してアカウントをカスタマイズする (AFC)」を参照してください。

元に戻すことができない設定の選択

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

ステップ 1: 共有アカウントの E メールアドレスを作成する

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

- 新しい共有アカウントでランディングゾーンをセットアップするには、AWSControl Tower には、にまだ関連付けられていない 2 つの一意の E メールアドレスが必要です AWS アカウント。これ

らの各 E メールアドレスは、AWSControl Tower に関連する特定の作業を行う企業内のさまざまなユーザーを対象とした、共同受信トレイ -- 共有 E メールアカウント -- として機能します。

- AWS Control Tower を初めて設定し、既存のセキュリティアカウントとログアーカイブアカウントを AWS Control Tower に持ち込む場合は、既存の AWS アカウントの現在の E メールアドレスを入力できます。

この E メールアドレスは以下に必要です。

- 監査アカウント – このアカウントは、AWSControl Tower によって提供される監査情報にアクセスする必要があるユーザーのチーム用です。また、環境のプログラムによる監査を実行してコンプライアンス目的の監査に役立つサードパーティー製ツールのアクセスポイントとして、このアカウントを使用することもできます。
- ログアーカイブアカウント – このアカウントは、ランディングゾーンOUsに登録されている 内のすべての登録済みアカウントのすべてのログ情報にアクセスする必要があるユーザーのチーム用です。

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

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

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

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

ステップ 2. ランディングゾーンの設定と起動

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

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

AWS CLI で を使用してランディングゾーンを設定および起動する方法について説明しますを使用して AWS Control Tower の使用を開始する APIs。

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

準備: AWS Control Tower コンソールに移動します。

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

ステップ 2a. AWS リージョンの確認と選択

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

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

管理する追加の AWS リージョンを選択するには

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

特定のリージョンへのアクセスを拒否するには

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

ステップ 2b. 組織単位を設定する (OUs)

これらの のデフォルト名を受け入れるとOUs、セットアップを続行するために実行する必要があるアクションはありません。の名前を変更するにはOUs、フォームフィールドに新しい名前を直接入力します。

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

ステップ 2c。共有アカウント、ログ、および暗号化の設定

セットアッププロセスのこのセクションでは、共有 AWS Control Tower アカウントの名前のデフォルトの選択がパネルに表示されます。これらのアカウントは、ランディングゾーンに不可欠な要素で

す。これらの共有アカウントは移動または削除しないでください。セットアップ時に、監査アカウントとログアーカイブアカウントの名前をカスタマイズできます。または、1 回限りのオプションとして、既存の AWS アカウントを共有アカウントとして指定することもできます。

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

共有アカウントについて

- 管理アカウント – AWS Control Tower 管理アカウントはルートレベルの一部です。管理アカウントは、AWSControl Tower の請求を許可します。また、ランディングゾーンの管理者許可もあります。AWS Control Tower で請求用と管理者権限用に別々のアカウントを作成することはできません。

  管理アカウントに表示される E メールアドレスは、セットアップのこのフェーズでは編集できません。これは確認として表示されます。そのため、複数のアカウントを持っている場合には、正しい管理アカウントを編集していることを確認できます。
- 2 つの共有アカウント - この 2 つのアカウントの名前をカスタマイズできます。またま、自分のアカウントを持ち込んで、新規または既存を問わず、アカウントごとに一意の E メールアドレスを指定することができます。AWS Control Tower で新しい共有アカウントを作成することを選択した場合、E メールアドレスにまだ AWS アカウントが関連付けられていない必要があります。

共有アカウントを設定するには、リクエストされた情報を入力します。

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

オプションでログの保持を設定する

セットアップのこのフェーズでは、ログを AWS Control Tower に保存する Amazon S3 バケットの AWS CloudTrail ログ保持ポリシーを、最大 15 年まで、日単位または年単位でカスタマイズできます。ログの保持をカスタマイズしない場合、デフォルト設定は、標準アカウントのログ記録で 1

年、アクセスログで 10 年です。この機能は、ランディングゾーンの更新またはリセット時にも使用できます。

オプションで自己管理 AWS アカウント アクセス

AWS Control Tower が (IAM) を使用して AWS アカウント AWS Identity and Access Management アクセスを設定するか、 AWS アカウント アクセスを自己管理するかを選択できます。 AWS IAMアイデンティティセンターのユーザー、ロール、アクセス許可は自分で設定してカスタマイズできます。または、IAMアイデンティティセンターを使用して複数のアカウントに直接アカウントフェデレーションまたはフェデレーションを行う外部 IdP などの別の方法を使用できます。この選択は後で変更できます。

デフォルトでは、AWSControl Tower は、「複数のアカウントを使用して AWS 環境を整理する」で定義されているベストプラクティスガイダンスに従って、ランディングゾーンの Identity Center を設定します AWS IAM。ほとんどのお客様はデフォルトを選択します。特定の業界や国、または Identity Center AWS リージョン が AWS IAM利用できない で規制に準拠するために、代替のアクセス方法が必要になる場合があります。

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

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

オプションで AWS CloudTrail 証跡を設定する

ベストプラクティスとして、ロギングを設定することをお勧めします。AWS Control Tower が組織レベルの CloudTrail 証跡をセットアップして管理できるようにする場合は、オプトインを選択します。独自の CloudTrail 証跡またはサードパーティーのログ記録ツールを使用してログ記録を管理する場合は、オプトアウトを選択します。コンソールで要求された場合は、選択を確認します。ランディングゾーンを更新する際、選択を変更したり、組織レベルの証跡をオプトイン/オプトアウトできます。

組織レベルやアカウントレベルの CloudTrail 証跡など、いつでも独自の証跡を設定および管理できます。重複 CloudTrailした証跡を設定すると、 CloudTrail イベントがログに記録されるときに重複コストが発生する可能性があります。

AWS KMS keysの設定 (任意)

暗号化キーを使用してリソースを AWS KMS 暗号化および復号する場合は、チェックボックスをオンにします。既存のキーがある場合は、ドロップダウンメニューに表示される識別子からキーを選択

できます。[Create a key] (キーの作成) を選択して、新しいキーを生成できます。ランディングゾーンを更新するたびに、KMSキーを追加または変更できます。

ランディングゾーンの設定を選択すると、AWSControl Tower はKMSキーを検証するための事前チェックを実行します。キーは、以下の条件を満たす必要があります。

- 有効
- 対称
- マルチリージョンキーではない
- ポリシーに正しい許可が追加されている
- キーが管理アカウントにある

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

KMS キーポリシーを更新する

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

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

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

- **`YOUR-MANAGEMENT-ACCOUNT-ID`** – AWS Control Tower がセットアップされる管理アカウントの ID。
- **`YOUR-HOME-REGION`** – AWS Control Tower の設定時に選択するホームリージョン。
- **`YOUR-KMS-KEY-ID`** – ポリシーで使用されるKMSキー ID。

KMS キーポリシーを更新するには

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

   AWS Config ポリシーステートメント

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

   CloudTrail ポリシーステートメント

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

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

6. [Save changes] (変更の保存) をクリックします。

KMSキーポリシーの例

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

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

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

その他のポリシーの例については、以下のページを参照してください。

- 暗号化権限の付与 (AWS CloudTrail ユーザーガイド)
- AWS Config デベロッパーガイドの「サービスにリンクされたロールS3 バケット配信を使用するときのKMSキーに必要なアクセス許可」)RolesS3。

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

AWS Key Management Service（ AWS KMS) では、マルチリージョンKMSキーと非対称キーを作成できます。ただし、AWSControl Tower はマルチリージョンキーまたは非対称キーをサポートしていません。 AWSControl Tower は、既存のキーの事前チェックを実行します。マルチリージョ

ンキーまたは非対称キーを選択すると、エラーメッセージが表示されることがあります。その場合は、AWSControl Tower リソースで使用する別のキーを生成します。

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

AWS Control Tower の顧客データは、デフォルトで SSE-S3 を使用して保管時に暗号化されることに注意してください。

オプションで、カスタマイズされたメンバーアカウントを設定および作成する

アカウントの作成ワークフローに従ってメンバーアカウントを追加する場合、必要に応じて AWS、Control Tower コンソールからカスタマイズされたメンバーアカウントのプロビジョニングに使用する、以前に定義された設計図を指定できます。使用できるブループリントがない場合は、後でアカウントをカスタマイズできます。「Account Factory Customization を使用してアカウントをカスタマイズする (AFC)」を参照してください。

ステップ 3. ランディングゾーンの確認とセットアップ

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

確定するには

1. コンソールで、 サービスのアクセス許可を確認し、準備ができたら、AWSControl Tower が AWS リソースを管理し、ユーザーに代わってルールを適用するために使用するアクセス許可を理解します。
2. 選択を確定して起動を初期化するには、[Set up landing zone] (ランディングゾーンの設定) を選択します。

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

⚠ SNS サブスクリプションの確認

監査アカウントに指定した E メールアドレスには、AWSControl Tower でサポートされているすべての AWS リージョンからAWS 通知 - サブスクリプション確認 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、AWSControl Tower でサポートされている各 AWS リージョンから各 E メール内のサブスクリプションの確認リンクを選択する必要があります。

を使用して AWS Control Tower の使用を開始する APIs

この入門手順は、AWSControl Tower 管理者を対象としています。この手順は、いくつかの前提条件と 2 つの主なステップを必要とします。

この手順では、AWSControl Tower およびその他の AWS のサービスAPIsから を使用して、ランディングゾーンを設定して起動します。これによりAPIs、AWS CloudFormation コンソールまたはを使用して、プログラムで AWS Control Tower 環境を作成できます AWS CLI。

AWS Control Tower ランディングゾーンを起動する前に、以下の前提条件タスクを実行します。

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

トピック

を使用したランディングゾーン設定の期待値 APIs

AWS Control Tower ランディングゾーンを設定するプロセスには、複数のステップがあります。AWS Control Tower ランディングゾーンの特定の側面は設定可能です。それ以外の選択肢は、セットアップ後に変更できません。

セットアップ時に設定する主な項目

- セットアップ時に基礎となる OU 名を選択できます。また、ランディングゾーンのセットアップ後に OU 名を変更することもできます。デフォルトでは、 Foundational には Security と Sandbox という名前OUsが付けられます。詳細については、「アーキテクチャが適切に設計された環境をセットアップするためのガイドライン」を参照してください。
- セットアップ中に、デフォルトでログアーカイブと監査と呼ばれる AWS Control Tower が作成する共有アカウント用にカスタマイズされた名前を選択できますが、セットアップ後にこれらの名前を変更することはできません。(これは 1 回限りの選択です)。
- のセットアップ時にAPIs、AWSControl Tower が監査およびログアーカイブ AWS アカウントとして使用する既存のアカウントを指定する必要があります。既存の AWS アカウントを指定するには、それらのアカウントに既存の AWS Config リソースがある場合は、アカウントを AWS Control Tower に登録する前に既存の AWS Config リソースを削除または変更する必要があります。(これは 1 回限りの選択です)。
- を初めて設定する場合、またはランディングゾーンバージョン 3.0 にアップグレードする場合は、AWSControl Tower が組織の組織レベルの AWS CloudTrail 証跡を設定することを許可するか、AWSControl Tower によって管理される証跡をオプトアウトして独自の CloudTrail 証跡を管理するかを選択できます。ランディングゾーンを更新するたびに、AWSControl Tower によって管理される組織レベルの証跡をオプトインまたはオプトアウトできます。
- オプションで、ランディングゾーンを設定または更新する際、Amazon S3 ログバケットとログアクセスバケットにカスタマイズされた保持ポリシーを設定できます。

元に戻すことができない設定の選択

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

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

ステップ 1: ランディングゾーンを設定する

AWS Control Tower ランディングゾーンを設定するプロセスには、複数のステップがあります。AWS Control Tower ランディングゾーンの特定の側面は設定可能ですが、セットアップ後に他の選択肢を変更することはできません。ランディングゾーンを起動する前に、これらの重要な考慮事項について確認するには、「ランディングゾーン設定に対する想定 」を参照してください。

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

- 新しい AWS Organizations 組織の作成
- 共有アカウントの E メールアドレスを設定する。
- ランディングゾーン を呼び出すために必要なアクセス許可を持つ IAMロールまたは IAM Identity Center ユーザーを作成しますAPIs。

ステップ 1. ランディングゾーンを含む組織を作成する:

1. を AWS Organizations `CreateOrganization`呼び出しAPI、すべての機能を有効にして基礎 OU を作成します。 AWSControl Tower は最初、これをセキュリティ OU と名付けます。このセキュリティ OU には、2 つの共有アカウントが含まれます。デフォルトでは、ログアーカイブアカウントと監査アカウントです。

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

   AWS Control Tower は、1 つ以上の追加の OUsを設定できます。ランディングゾーンに [Security OU] (セキュリティ OU) の他に少なくとも 1 つの [Additional OU] (追加の OU) をプロビジョニングすることをお勧めします。この追加の OU が開発プロジェクトを対象としている場合は、「AWS AWS Control Tower ランディングゾーンのマルチアカウント戦略」で示すように、サンドボックス OU という名前にすることをお勧めします。

ステップ 2. 必要に応じて共有アカウントをプロビジョニングする:

ランディングゾーンをセットアップするには、AWSControl Tower に 2 つの E メールアドレスが必要です。ランディングゾーンを使用して AWS Control Tower を初めてAPIsセットアップする場合は、既存のセキュリティアカウントとログアーカイブ AWS アカウントを使用する必要があります。既存の の現在の E メールアドレスを使用できます AWS アカウント。これらの各 E メールアドレスは、AWSControl Tower に関連する特定の作業を行う企業内のさまざまなユーザーを対象とした、共同受信トレイ -- 共有 E メールアカウント -- として機能します。

新しいランディングゾーンの設定を開始するには、既存の AWS アカウントがない場合は、 を使用してセキュリティアカウントとログアーカイブ AWS アカウントをプロビジョニングできます AWS Organizations APIs。

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

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

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

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

ステップ 3 必要なサービスロールを作成する

AWS Control Tower がランディングゾーンの設定に必要なAPI呼び出しを実行できるようにする次のIAMサービスロールを作成します。

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

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

IAM ロールを作成するには：

1. すべてのランディングゾーン を呼び出すために必要なアクセス許可を持つ IAMロールを作成しますAPIs。または、IAMIdentity Center ユーザーを作成し、必要なアクセス許可を割り当てることもできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "backup:UpdateGlobalSettings",
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListLandingZoneOperations",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess",
                "organizations:DeregisterDelegatedAdministrator"
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
```

```
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

ステップ 2: ランディングゾーンを起動する

AWS Control Tower では、入力パラメータとしてランディングゾーンバージョンとマニフェストファイルCreateLandingZoneAPIが必要です。マニフェストファイルを使用して、以下の機能を設定できます。

- オプションでログの保持を設定する
- オプションで自己管理 AWS アカウント アクセス
- オプションで AWS CloudTrail 証跡を設定する
- AWS KMS keysの設定 (任意)

マニフェストファイルをコンパイルすると、新しいランディングゾーンを作成する準備が整います。

> **Note**
>
> AWS Control Tower は、 APIsを使用してランディングゾーンを設定および起動するときのリージョン拒否コントロールをサポートしていません。を使用してランディングゾーンを正常に起動したらAPIs、AWSControl Tower コンソールを使用してリージョン拒否コントロールを設定できます。

1. AWS Control Tower CreateLandingZone を呼び出しますAPI。これには、ランディングゾーンのバージョンとマニフェストファイルが入力としてAPI必要です。

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

   LandingZoneManifest.json マニフェストの例：

   ```
   {
   ```

```
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

> **Note**
>
> この例に示すように、 アカウント CentralizedLogging と SecurityRoles アカウントの AccountId は異なる必要があります。

出力:

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

```
}
```

2. を呼び出しGetLandingZoneOperationAPIて、CreateLandingZoneオペレーションのステータスを確認します。は、SUCCEEDED、、FAILEDまたは のステータスGetLandingZoneOperationAPIを返しますIN_PROGRESS。

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

出力:

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

3. ステータスが として返ったらSUCCEEDED、 を呼び出しGetLandingZoneAPIてランディングゾーンの設定を確認できます。

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

出力:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
```

```
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

ランディングゾーンを特定する

を呼び出すListLandingZonesと、アカウントが AWS Control Tower で既にセットアップされているかどうかを判断するのに役立ちます。これにより、ランディングゾーンのホームリージョンに関係なく、任意の商用リージョンで 1 つのランディングゾーン識別子 (ARN) APIが返されます。ランディングゾーンARNsはリージョンごとに一意です。

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

オプトインリージョンの場合、 は、 APIのホームリージョンと同じリージョンAPIで を呼び出すと、ランディングゾーン識別子ListLandingZonesAPIのみを返します。例えば、ランディングゾーンが af-south-1 で設定され、af-south-1 ListLandingZonesで を呼び出すと、 はランディングゾーン識別子APIを返します。 ランディングゾーンが af-south-1 で設定されていて、ap-east-1 ListLandingZonesで を呼び出した場合、 APIはランディングゾーン識別子を返しません。

出力:

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

ランディングゾーンを更新する

新しいランディングゾーンバージョンが使用可能になったとき、またはランディングゾーン設定に他の更新を行うには、 を呼び出しUpdateLandingZoneAPIて、更新されたマニフェストファイルを参照できます。これにより APIが返されます。この はOperationIdentifier、 を呼び出しGetLandingZoneOperationAPIて更新オペレーションのステータスを確認するときに使用できます。

ランディングゾーンを更新するには

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

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

LandingZoneManifest.json：

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

```
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays":2555
            },
            "accessLoggingBucket": {
                "retentionDays": 2555
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

出力:

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

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

アカウントOUs数が 300 未満の登録済み AWS Control Tower の場合、AWSControl Tower コンソールを使用してダッシュボードの OU ページにアクセスし、OU の再登録を選択してその OU のアカウントを更新できます。

ランディングゾーンをリセットしてドリフトを解決する

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

ランディングゾーンがドリフトしているかどうかを確認するには、 GetLandingZone を呼び出しますAPI。これにより、ランディングゾーンのドリフトステータス DRIFTEDまたは APIが返されますIN_SYNC。

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

は、利用可能な最新のランディングゾーンバージョンResetLandingZoneAPIを使用している場合にのみ使用できます。を呼び出しGetLandingZoneAPIて、ランディングゾーンのバージョンを利用可能な最新バージョンと比較できます。必要に応じて、「ランディングゾーンを更新する」を行うことで利用可能な最新バージョンをランディングゾーンで使用できます。これらの例では、バージョン 3.3 を最新バージョンとして使用しています。

1. を呼び出しますGetLandingZoneAPI。が のドリフトステータスをAPI返した場合DRIFTED、ランディングゾーンはドリフト状態になります。
2. を呼び出しResetLandingZoneAPIて、ランディングゾーンを元の設定にリセットします。

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

出力:

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

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

ランディングゾーンを廃止する

ランディングゾーンのすべてのリソースをクリーンアップするプロセスは、ランディングゾーンの廃止と呼ばれます。

> **Important**
>
> この廃止プロセスは、ランディングゾーンの使用を停止する場合にのみ実行することを強くお勧めします。既存のランディングゾーンを廃止した後に再作成することはできません。

AWS Control Tower がデータと既存の を処理する方法に関する重要な情報など、ランディングゾーンの廃止の詳細については AWS Organizations、「」を参照してくださいチュートリアル: AWS Control Tower ランディングゾーンを廃止する。

ランディングゾーンを廃止するには、 `DeleteLandingZone` を呼び出しますAPI。これにより、APIが返されます。これは`OperationIdentifier`、 を呼び出し`GetLandingZoneOperation`APIて削除オペレーションのステータスを確認するときに使用できます。

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

出力:

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

ランディングゾーンオペレーションのステータスを表示する

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

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

ListLandingZoneOperations

ListLandingZoneOperations の入出力の例。

この例は、パラメータなしで API を呼び出す方法を示しています。

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

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

この例は、API を呼び出し、結果の最大数を指定する方法を示しています。

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

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
```

```
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ],
    "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}
```

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

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

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

この例は、フィルターを指定して API を呼び出す方法を示しています。

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

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

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

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

前提条件

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

ステップ 1. 組織と 2 つの必要なアカウントを作成します。

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

ステップ 2. 必要な IAM ロールを作成します。

AWSControlTowerAdmin

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

AWSControlTowerCloudTrailRole

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

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

AWSControlTowerStackSetRole

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

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

AWSControlTowerConfigAggregatorRoleForOrganizations

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

```
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

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

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

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

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

```
}
EOF
```

ステップ 4。最新バージョンでランディングゾーンを作成します。

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

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

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

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

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

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

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

サンプルステータス出力:

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

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

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

ランディングゾーンに関する詳細情報を表示するには

ステップ 1. ランディングゾーンの ARN を特定する

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

出力には、次の出力例に示すように、ランディングゾーンの識別子が含まれます。

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

ステップ 2. 情報を取得する

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

以下は、表示される出力の例です。

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
```

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

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

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

を使用してランディングゾーンを起動する AWS CloudFormation

コンソール AWS CloudFormation または を使用して、ランディングゾーンを設定して起動できます AWS CloudFormation AWS CLI。このセクションでは、 APIs を使用してランディングゾーンを起動する手順と例を示します AWS CloudFormation。

トピック

を使用してランディングゾーンを起動するための前提条件 AWS CloudFormation

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

   詳細な手順については、「ステップ 1: ランディングゾーンを設定する」を参照してください。
2. AWS CloudFormation コンソールまたは を使用して AWS CLI、管理アカウントに次のリソースを作成する AWS CloudFormation テンプレートをデプロイします。
   - ログアーカイブアカウント (「ログ記録」アカウントと呼ばれることもあります)
   - 監査アカウント (「セキュリティ」アカウントと呼ばれることもあります)
   - AWSControlTowerAdmin、AWSControlTowerCloudTrailRole、AWSControlTowerConfigAggregatorRole および AWSControlTowerStackSetRoleサービスロール。

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

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
```

```
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
```

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

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

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

を使用して新しいランディングゾーンを作成する AWS CloudFormation

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

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

```
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
            name:
              Ref: SecurityOuName
          sandbox:
            name:
              Ref: SandboxOuName
```

```
        centralizedLogging:
          accountId:
            Ref: CentralizedLoggingAccountId
          configurations:
            loggingBucket:
              retentionDays:
                Ref: LoggingBucketRetentionPeriod
            accessLoggingBucket:
              retentionDays:
                Ref: AccessLoggingBucketRetentionPeriod
            kmsKeyArn:
              Ref: KMSKey
          enabled: true
        securityRoles:
          accountId:
            Ref: SecurityAccountId
        accessManagement:
          enabled: true
```

を使用して既存のランディングゾーンを管理する AWS CloudFormation

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

ランディングゾーン内のドリフトを検出して解決するには、AWSControl Tower コンソール、、AWS CLIまたは `ResetLandingZone` API を使用できます。

次のステップ

これで、ランディングゾーンがセットアップされ、使用する準備ができました。

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

- 推奨される管理方法については、「ベストプラクティス」を参照してください。
- 特定のロールと許可を持つ IAM Identity Center ユーザーとグループをセットアップできます。推奨事項については、「 グループ、ロール、ポリシーを設定する上での推奨事項 」を参照してください。
- AWS Organizations デプロイから組織とアカウントの登録を開始するには、「既存の組織とアカウントの管理」を参照してください。

- エンドユーザーは、Account Factory を使用してランディングゾーン AWS に独自のアカウントをプロビジョニングできます。詳細については、「アカウントの設定とプロビジョニングのためのアクセス許可」を参照してください。
- AWS Control Tower のコンプライアンス検証 を確保するために、中央クラウド管理者はログアーカイブアカウントのログアーカイブを確認できます。また、指定されたサードパーティー監査人はセキュリティ OU のメンバーである監査 (共有) アカウントの監査情報を確認できます。
- AWS Control Tower の機能の詳細については、「関連情報」を参照してください。
- AWS Control Tower の機能を使用する方法の詳細については、YouTube 動画のキュレーションリストにアクセスしてみてください。
- 場合によっては、最新のバックエンド更新プログラムと最新のコントロールを入手してランディングゾーンを最新の状態に維持するために、ランディングゾーンを更新する必要があります。詳細については、「AWS Control Tower の設定更新管理」を参照してください。
- AWS Control Tower の使用中に問題が発生した場合は、「トラブルシューティング」を参照してください。

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

AWS Control Tower の制限とクォータ

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

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

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

AWS Control Tower の既知の制限事項

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

- AWS Control Tower には全体的な同時実行数の制限があります。通常、一度に実行できるオペレーション数は 1 つです。この制限には次の 2 つの例外があります。
  - オプションのコントロールは、非同期プロセスを通じて同時にアクティブ化および非アクティブ化できます。呼び出し元がコンソールか API に関係なく、一度に合計最大 100 のコントロール関連オペレーションを実行できます。
  - アカウントは、非同期プロセスを通じて Account Factory で同時にプロビジョニング、更新、登録でき、アカウント関連のオペレーションは同時に 5 つまで実行できます。アカウントの管理を解除するには、一度に 1 つのアカウントを実行する必要があります。
- セキュリティ OU の共有アカウントの E メールアドレスは変更できますが、これらの変更を AWS Control Tower コンソールで確認するには、ランディングゾーンを更新する必要があります。
- AWS Control Tower ランディングゾーンの OU には、OU あたり 5 個の SCP という制限が適用されます。
- AWS Control Tower は、ランディングゾーンの組織で、すべての OU 間で分けられたアカウントを最大 10,000 個までサポートします。
- 直接ネストされたアカウントの数が 1000 を超える既存の OU は、AWS Control Tower に登録または再登録することはできません。OU の登録に伴う制限の詳細については、「基盤となる AWS サービスに基づく制限事項」を参照してください。

- AWS Control Tower (CfCT) のカスタマイズは AWS リージョン、一部の依存関係が利用できないため、これらでは使用できません。
  - 欧州 (チューリッヒ) リージョン、eu-central-2
  - 欧州 (スペイン) リージョン、eu-south-2
  - カナダ西部 (カルガリー)
  - AWS アジアパシフィック (マレーシア) リージョン、ap-southeast-5

  CfCT を AWS Control Tower のホームリージョンにデプロイする場合、CfCT を使用してこれらのリージョンにリソースをデプロイおよび管理できますが、これらのリージョンに CfCT を構築することはできません。
- 一部の依存関係は使用できないため AWS リージョン、AWS Control Tower Account Factory for Terraform (AFT) は以下では利用できません。
  - 欧州 (チューリッヒ) リージョン、eu-central-2
  - 欧州 (スペイン) リージョン、eu-south-2
  - カナダ西部 (カルガリー)
  - AWS アジアパシフィック (マレーシア) リージョン、ap-southeast-5
- AWS Control Tower Account Factory for Terraform (AFT) は、次のリージョンの新規の AFT のお客様にデプロイできません。 AWS CodeStar Connections はサードパーティーのバージョン管理システム (VCS) に接続できないためです。
  - アジアパシフィック (香港)、アフリカ (ケープタウン)、中東 (バーレーン)、欧州 (チューリッヒ)、アジアパシフィック (ジャカルタ)、アジアパシフィック (ハイデラバード)、アジアパシフィック (大阪)、アジアパシフィック (メルボルン)、イスラエル (テルアビブ)、欧州 (スペイン)、中東 (アラブ首長国連邦)
- 以下のリージョンは IAM アイデンティティセンターをサポートしていません。
  - AWS アジアパシフィック (マレーシア) リージョン、ap-southeast-5

  IAM Identity Center の詳細 AWS リージョン とサポートについては、AWS 「 Identity and Access Management ユーザーガイド」の「リージョンとエンドポイント」を参照してください。
- 以下のリージョンは AWS Service Catalog をサポートしていません。
  - カナダ西部 (カルガリー)、ca-west-1
  - AWS アジアパシフィック (マレーシア) リージョン、ap-southeast-5

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

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

クォータ引き上げをリクエストする

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

Service Quotas コンソールから次のクォータを表示できます

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

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

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

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

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

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

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

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

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

コントロールの制限事項

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

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

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

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

リージョン別の制限事項

AWS Control Tower の一部のコントロールは、AWS Control Tower が利用可能な特定の AWS リージョン で動作しません。これらのリージョンは、必要な基盤となる機能をサポートしていないためです。したがって、そのコントロールをデプロイしても、AWS Control Tower で管理しているすべてのリージョンで動作しない可能性があります。この制限は、Security Hub サービスマネージドスタンダード: AWS Control Tower における特定の検出コントロール、特定のプロアクティブコントロール、および特定のコントロールに影響します。リージョン別の利用可能性の詳細については、「Security Hub controls」を参照してください。リージョン別のサービスリストのドキュメントと Security Hub controls referenceドキュメント も参照してください。

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

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

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

使用可能なコントロールとリージョンを確認する

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

また、「AWS Control Tower Controls Reference Guide」で AWS Control Tower コントロールとサポートされているリージョンのリファレンス表「Control availability by Region」も参照してください。

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

次の表は、特定の でサポートされていない特定のプロアクティブコントロールを示しています AWS リージョン。

コントロール識別子	デプロイできないリージョン
`CT.DAX.PR.2`	ap-southeast-5、ca-west-1、us-west-1
`CT.REDSHIFT.PR.5`	ap-south-2、ap-southeast-3、ap-southeast-4、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1

次の表は、特定の AWS リージョンでサポートされていない AWS Control Tower 検出コントロールを示しています。

コントロール識別子	デプロイできないリージョン
`API_GW_CACHE_ENABLED_AND_ENCRYPTED`	ap-southeast-5、ca-west-1
`APPSYNC_ASSOCIATED_WITH_WAF`	af-south-1、ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1

コントロール識別子	デプロイできないリージョン
AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED	ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1
AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN	ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1
AUTOSCALING_CAPACITY_REBALANCING	ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、il-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1、ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-1、eu-south-2、il-central-1、me-central-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ap-southeast-5、ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EC2_VOLUME_INUSE_CHECK	ap-southeast-5、ca-west-1
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ap-southeast-5、ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1

コントロール識別子	デプロイできないリージョン
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	af-south-1、ap-northeast-3、ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-1、eu-south-2、il-central-1、me-central-1
AWS-GR_ENCRYPTED_VOLUMES	af-south-1、ap-northeast-3、eu-south-1、il-central-1
AWS-GR_IAM_USER_MFA_ENABLED	ap-south-2、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	ap-south-2、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3、ap-south-2、ap-southeast-3、ap-southeast-5、ca-west-1、eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2、eu-south-2
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	af-south-1、ap-southeast-4、eu-central-2、eu-south-1、eu-south-2、il-central-1
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2、eu-south-2
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2、ap-southeast-3、ap-southeast-5、ca-west-1、eu-south-2
AWS-GR_RESTRICTED_SSH	af-south-1、eu-south-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	ap-southeast-5、ca-west-1、il-central-1、me-central-1

コントロール識別子	デプロイできないリージョン
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	eu-central-2、eu-south-2、il-central-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	af-south-1、ap-northeast-3、ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-1、eu-south-2、il-central-1、me-central-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	ap-southeast-5、ca-west-1、il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK	ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1
BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED	ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1
BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK	ap-south-2、ap-southeast-3、ap-southeast-4、ap-southeast-5、ca-west-1、eu-central-2、eu-south-2、il-central-1、me-central-1

基盤となる AWS サービスに基づく制限事項

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

一般的なガイドライン

原則として、OU の登録時にサポートされるアカウントの数は、その OU に対して管理されるリージョンの数と有効なコントロールの数が増えるにつれて減少すると予想されます。これらの一般的なガイドラインは、15 個のオプションコントロールが有効になっていることを前提としています。OU

で有効になっているコントロールの数がそれより多くても少なくても、登録時の OU あたりのアカウント数の上限は異なります。

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

エラーが発生した場合

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

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

AWS CloudFormation スタックセットの制限

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

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

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

AWS Config 制限事項

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

アカウントとオプトインリージョンに関する初回の制限事項

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

AWS Control Tower 機能の地域的な違い

AWS Control Tower は他の AWS サービスの動作を調整するため AWS リージョン、 全体で AWS Control Tower の動作には特定の違いがあります。以下に例を示します。

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

AWS Control Tower 環境の動作を最適に判断するには、ホームリージョンを確認します。次に、以下の項目を評価します。詳細については、AWS「 Control Tower の制限とクォータ」を参照してください。

- 希望するホームリージョンで AWS Service Catalog 利用できますか？
- 必要なコントロールを使用できるか？「Control limitations」を参照してください。
- IAM Identity Center は目的のホームリージョンで利用できますか？

コントロールのデプロイ可能なリージョン

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

AWS Control Tower によって管理される OU でコントロールをアクティブ化すると、コントロールの有効領域は、AWSControl Tower 管理対象リージョンとコントロールのデプロイ可能なリージョンの共通部分になります。

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

AWS Control Tower でワークロードを運用するコントロールとリージョン間の関係をモニタリングして、 AWS リソースの保護にギャップが生じないようにすることが重要です。

保護されたリージョンを確認する方法

- AWS Control Tower コンソールでは、有効なコントロールとリージョンを「有効なコントロール」セクションで表示できます。
- を呼び出すと`GetEnabledControl`API、 targetRegionsパラメータには、コントロールを効果的にデプロイできるリージョンのみが表示され、デプロイできないリージョンは表示されません。

AWS Control Tower Controls リファレンスガイド

AWS Control Tower のコントロールに関する詳細情報は、AWS「 Control Tower Controls Reference Guide」に移動しました。

AWS Control Tower 管理者向けのベストプラクティス

このトピックは、主に管理アカウントの管理者を対象としています。

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

アクセスについてユーザーに説明する

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

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

リソースアクセスについて説明する

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

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

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

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

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

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

予防コントロールについて説明する

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

AWS 開発者など一部のユーザーは、エンジニアリングソリューションを作成できるように、使用するアカウントや OUs に適用される予防コントロールについて知っておく必要がある場合があります。次の手順では、組織の情報管理ポリシーに従って、適切なユーザーにこの情報を提供する方法に関するガイダンスを示します。

> **Note**
>
> この手順では、ランディングゾーン内に少なくとも 1 つの子 OU と少なくとも 1 人の AWS IAM Identity Center ユーザーを既に作成していることを前提としています。

知っておく必要があるユーザーに予防コントロールを示すには

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

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

AWS Control Tower ランディングゾーンの計画

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

> **Note**
>
> 組織ごとに 1 つのランディングゾーンをセットアップできます。

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

AWS Control Tower をセットアップする方法

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

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

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

機能の比較

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

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

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

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

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

既存の組織での AWS Control Tower の起動

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

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

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

AWS Control Tower を既存の組織に追加した場合の影響

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

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

機能の概要

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

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

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

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

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

新しい組織での AWS Control Tower の起動

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

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

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

AWS Control Tower のお客様は、最良の結果を得るために AWS 環境とアカウントを設定する方法についてのガイダンスを頻繁に求めます。AWS は、AWS Control Tower ランディングゾーンを含む AWS リソースを最大限に活用できるように、マルチアカウント戦略と呼ばれる統合されたレコメンデーションのセットを作成しました。

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

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

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

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

AWS マルチアカウント戦略: ベストプラクティスガイダンス

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

AWS アカウントの定義

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

> **Note**
>
> AWS アカウントは、フェデレーションまたは AWS Identity and Access Management (IAM) によって設定されるユーザーアカウントとは異なります。

AWS アカウントの詳細

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

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

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

アーキテクチャが適切に設計された環境の定義

AWS は、Well-Architected 環境をランディングゾーンで始まる環境として定義します。

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

ランディングゾーンの定義

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

アーキテクチャが適切に設計された環境をセットアップするためのガイドライン

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

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

複数の AWS アカウントの使用

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

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

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

複数の組織単位の使用

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

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

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

ランディングゾーンでの OU 向けに適切に計画された構造の使用

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

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

レコメンデーション

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

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

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

自動的にセットアップされるものを除く推奨される OU

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

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

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

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

- ワークロード OU - ワークロードを実行するアカウントが含まれます。

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

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

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

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

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

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

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

基礎 OU 列では、次の 2 つの OU が基本構造に追加されています。

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

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

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

ルートについて

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

ランディングゾーンのセットアップに関する管理上のヒント

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

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

- 起動時に、AWS Control Tower でサポートされているすべてのリージョンで、 AWS Security Token Service (STS) エンドポイントを管理アカウントでアクティブ化する必要があります。この操作を行わないと、設定プロセスの途中で起動が失敗する可能性があります。
- AWS Control Tower では、有効になっているコントロールのみのタグ付けがサポートされます。詳細については、「AWS Control Tower が、有効になっているコントロールのタグ付けをサポート」を参照してください。
- AWS Control Tower が管理するすべてのアカウントで、多要素認証 (MFA) を有効にすることをお勧めします。

VPC に関する考慮事項

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

グループ、ロール、ポリシーを設定する上での推奨事項

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

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

推奨される制限事項

管理者が AWS Control Tower アクションのみを管理できるようにする IAM ロールまたはポリシーを設定することで、組織への管理アクセスの範囲を制限できます。推奨されるアプローチは、IAM ポリシー `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

を使用することです。AWSControlTowerServiceRolePolicy ロールを有効にすると、管理者は AWS Control Tower のみを管理できます。各アカウントには、予防コントロールを管理する AWS Organizations ための への適切なアクセス、検出コントロールを管理する AWS Configための SCPs、および へのアクセスを必ず含めてください。

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

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

AWS Control Tower リソースの作成と変更に関するガイダンス

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

一般的なガイダンス

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

  特に、次のことに注意してください。

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

ウントを AWS Control Tower に登録したり、直接の親 OU を登録したりすることができなくなります。

- SCPs または AWS Security Token Service () AWS リージョン を介した の使用を許可しないでくださいAWS STS。禁止した場合、AWS Control Tower が未定義の状態になります。でリージョンを禁止すると AWS STS、それらのリージョンでは認証が利用できなくなるため、機能は失敗します。代わりに、コントロールに示すように、AWS Control Tower のリージョン拒否機能、ランディングゾーンレベルで機能するリクエスト AWS された に基づいて へのアクセスを拒否 AWS リージョンする、または OU に適用されたコントロールリージョン拒否機能に依存して、リージョンへのアクセスを制限します。
- SCP AWS Organizations `FullAWSAccess`は適用する必要があり、他の SCPs とマージしないでください。この SCP への変更はドリフトとして報告されません。ただし、特定のリソースへのアクセスが拒否された場合、一部の変更が AWS Control Tower の機能に予期しない影響を与える可能性があります。例えば、SCP がデタッチまたは変更された場合、アカウントは AWS Config レコーダーへのアクセスを失うか、CloudTrail ログにギャップが生まれます。
- API を使用して AWS Organizations `DisableAWSServiceAccess`、ランディングゾーンを設定した組織への AWS Control Tower サービスアクセスをオフにしないでください。オフにした場合、 AWS Organizationsからのメッセージサポートがないと、特定の AWS Control Tower ドリフト検出機能が正しく動作しなくなる可能性があります。これらのドリフト検出機能により、AWS Control Tower は組織内の組織単位、アカウント、統制のコンプライアンスステータスを正確に報告できます。詳細については、 API_DisableAWSServiceAccessAWS Organizations API リファレンスの「」を参照してください。
- 通常、AWS Control Tower は一度に 1 つのアクションを実行します。1 つのアクションを完了してから、別のアクションを開始する必要があります。例えば、コントロールを有効にするプロセスが進行中にアカウントをプロビジョニングしようとすると、アカウントのプロビジョニングは失敗します。

  例外:

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

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

アカウントと OU に関するヒント

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

ルートユーザーとしてサインインする場合

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

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

- アカウント名、ルートユーザーのパスワード、E メールアドレスなど、特定のアカウント設定を変更する。詳細については、「AWS Control Tower または を使用して Account Factory アカウントを更新および移動する AWS Service Catalog」を参照してください。
- を閉じます AWS アカウント。

- ルートユーザーログイン認証情報を必要とするアクションの詳細については、「AWS Account Management リファレンスガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

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

ルートユーザーとしてサインインするには

1. AWS サインインページを開きます。

   アクセス AWS アカウント が必要な の E メールアドレスがない場合は、AWS Control Tower から取得できます。管理アカウントのコンソールを開き、[Accounts] (アカウント) を選択し、E メールアドレスを探します。
2. アクセス AWS アカウント が必要な の E メールアドレスを入力し、Next を選択します。
3. [Forgot password?] (パスワードを忘れた場合) を選択して、パスワードリセット手順をルートユーザーの E メールアドレスに送信します。
4. ルートユーザーのメールボックスからパスワードリセットの E メールメッセージを開き、指示に従ってパスワードをリセットします。
5. AWS サインインページを開き、リセットしたパスワードでサインインします。

AWS Organizations ガイダンス

AWS Control Tower は と密接に関連付けられています AWS Organizations。 AWS 環境を保護するためにどのように連携するのが最適かに関する具体的なガイダンスをいくつか示します。

- AWS Control Tower 管理アカウントとメンバーアカウントのセキュリティを保護するためのベストプラクティスに関するガイダンスは、 AWS Organizations ドキュメントに記載されています。
  - 管理アカウントのベストプラクティス
  - メンバーアカウントのベストプラクティス
- AWS Organizations を使用して、AWS Control Tower に登録されている OU にアタッチされたサービスコントロールポリシー (SCPs) を更新しないでください。これを行うと、コントロールが不明な状態になり、AWS Control Tower でランディングゾーンのリセットや OU の再登録を行う

必要が生じます。代わりに、AWS Control Tower が作成した SCP を編集するのではなく、新しい SCP を作成して OU にアタッチできます。

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

IAM Identity Center のガイダンス

AWS Control Tower では、 AWS Identity and Access Management (IAM) を使用して へのアクセスを規制することをお勧めします AWS アカウント。ただし、AWS Control Tower に IAM Identity Center

をセットアップさせるか、ビジネス要件を最も効果的に満たす方法で IAM Identity Center を自分でセットアップするか、またはアカウントアクセスに別の方法を選択するかを選ぶことができます。

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

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

オプションの選択

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

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

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

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

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

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

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

Account Factory ガイダンス

Account Factory を使用して AWS Control Tower で新しいアカウントをプロビジョニングする際に、問題が発生する可能性があります。これらの問題のトラブルシューティング方法については、「AWS Control Tower ユーザーガイド」で「トラブルシューティング」の「新しいアカウントのプロビジョニングに失敗する」セクションを参照してください。

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

Account Factory で新しいアカウントをプロビジョニングするとき、またはアカウント登録機能 AWS Control Tower を使用するときに、IAM ユーザーまたは IAM Identity Center ユーザーとして認証されている場合は、ユーザーが AWS Service Catalog ポートフォリオにアクセスできることを確認します。アクセスできない場合は、Service Catalog からのエラーメッセージが表示されることが

あります。詳細については、「AWS Control Tower ユーザーガイド」で「トラブルシューティングセクション」の「起動パスが見つからないというエラー」を参照してください。

> **Note**
>
> 一度にプロビジョニングできるアカウントは最大 5 個です。

SNS トピックのサブスクリプションに関するガイダンス

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

- `aws-controltower-AllConfigNotifications` SNS トピックは、コンプライアンス通知や Amazon CloudWatch イベント通知など AWS Config、 によって発行されたすべてのイベントを受信します。例えば、このトピックでは、コントロール違反が発生したかどうかを示します。また、他のタイプのイベントに関する情報も提供します (このトピックが構成されたときに公開する内容については、「AWS Config」を参照してください。)
- `aws-controltower-BaselineCloudTrail` 追跡のデータイベントは、`aws-controltower-AllConfigNotifications` SNS トピックにも公開されるように設定されています。
- 詳細なコンプライアンス通知を受け取るには、`aws-controltower-AllConfigNotifications` SNS トピックをサブスクライブすることをお勧めします。このトピックでは、すべての子アカウントからのコンプライアンス通知を集約します。
- ドリフト通知やその他の通知、コンプライアンス通知を受信して、全体的な通知を少なくするには、`aws-controltower-AggregateSecurityNotifications` SNS トピックをサブスクライブすることをお勧めします。
- AWS Control Tower Account Factory for Terraform (AFT) のエラーに関する通知を受け取るには、AFT リポジトリの aft_failure_notifications という SNS トピックにサブスクライブできます。以下に例を示します。

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

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

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

KMS キーのガイダンス

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

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

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

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

ランディングゾーン更新のベストプラクティス

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

> **Note**
>
> 最新バージョンのランディングゾーンに更新するのがベストプラクティスです。

このセクションで説明するベストプラクティスの概要

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

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

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

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

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

組織レベルの CloudTrail 証跡の選択に関する考慮事項

- 3.0 以降にアップグレードすると、AWS Control Tower は最初に作成したアカウントレベルの証跡を 24 時間後に削除します。

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

組織レベルの証跡の利点

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

テスト環境を検討する

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

AI ベースのサービスと AWS Control Tower

AWS上の AI ベースのサービスによるデータの保存をオプトアウトするためのサービスコントロールポリシー (SCP) を作成できます。これらの SCP ポリシーは、Amazon Rekognition や Amazon

CodeWhisperer などの AI ベースのサービスが、他の AI ベースの AWS サービスを改善するためにデータを保存して使用できないことを指定します。

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

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

AWS Control Tower の設定更新管理

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

> **Note**
>
> AWS Control Tower コンソールには、ランディングゾーンを更新する必要があるタイミングが表示されます。更新するオプションが表示されていない場合、ランディングゾーンは既に最新です。

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

バージョン	リリース日	説明
3.3	12-12-2023	ランディングゾーンバージョン 3.3
3.2	6-09-2023	ランディングゾーンバージョン 3.2
3.1	2-09-2023	ランディングゾーンバージョン 3.1
3.0	7-26-2022	ランディングゾーンバージョン 3.0
2.9	4-22-2022	ランディングゾーンバージョン 2.9
2.8	2-10-2022	ランディングゾーンバージョン 2.8

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

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

更新の利点

- 管理対象リージョンを変更できる
- ログの保持ポリシーを変更することができる
- リージョン拒否コントロールを追加または削除できる
- 暗号化キーを適用 AWS KMSできます。
- 組織レベルの CloudTrail 証跡を有効または無効にできます。
- ランディングゾーンのドリフトを解決できる

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

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

ランディングゾーンを更新するときに、未使用の AWS アイデンティティセンター (以前は と呼ばれていました AWS SSO) マッピングをクリアする機会があります。詳細については、「フィールドノート: AWS Control Tower のアップグレード中に未使用のIAMアイデンティティセンターマッピングを自動的にクリアする」を参照してください。

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

ランディングゾーンの更新について

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

- ランディングゾーンの更新: ほとんどの場合、この種類の更新は、[Landing zone settings] (ランディングゾーン設定) ページで [Update] (更新) を選択して実行します。特定の種類のドリフトを解決するには、ランディングゾーンの更新が必要になる場合があります。必要に応じて [リセット] を選択できます。
- 1 つ以上の個々のアカウントの更新: 関連する情報が変更された場合、または特定の種類のドリフトが発生した場合は、アカウントを更新する必要があります。アカウントが更新を必要とする場合、アカウントのステータスは [Accounts] (アカウント) ページで [Update available] (更新プログラムが利用できます) と表示されます。

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

- 完全な更新: 完全な更新には、ランディングゾーンの更新が含まれ、その後に登録済み OU に登録されているすべてのアカウントの更新が続きます。2.9、3.0 などの AWS Control Tower の新しいリリースでは、完全な更新が必要です。

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

ランディングゾーンを更新する

AWS Control Tower ランディングゾーンを更新する最も簡単な方法は、ランディングゾーン設定ページを使用することです。このページには、AWSControl Tower ダッシュボードの左側のナビゲーションでランディングゾーン設定を選択してアクセスできます。

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

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

標準的な更新手順

次の手順では、 コンソールから AWS Control Tower を完全に更新する手順について説明します。個々のアカウントを更新するには、「コンソールでアカウントを更新する」を参照してください。

OU ごとに任意の数のアカウントを使用してランディングゾーンを更新するには

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

> **オプションで [Re-register OU] (OU の再登録) を使用してアカウントを更新する**
>
> アカウントOUs数が 300 未満の登録済み AWS Control Tower の場合、ダッシュボードの OU ページに移動し、OU の再登録を選択してその OU のアカウントを更新できます。

ランディングゾーンバージョンを選択する

AWS Control Tower ランディングゾーンバージョン 3.1 以降を実行している場合は、ランディングゾーン設定で Update または Reset オペレーションを実行するときに、現在のバージョンのままにするか、新しいバージョンにアップグレードするかを選択できます。ほとんどの場合、ドリフトを修復するのに最適な方法はリセットオペレーションです。

Control Tower コンソールで、または AWS Control AWS Tower を使用して、ランディングゾーンのバージョンを選択できますAPIs。

> **Note**
>
> 中間バージョンをスキップするランディングゾーンバージョンをデプロイすることを選択した場合、例えば 3.1 から 3.3 に移動すると、AWSControl Tower は更新オペレーションの一部として中間バージョンを自動的にデプロイします。
> 会話の中では、新しいバージョンに移行することを、単なる更新ではなくアップグレードと呼ぶことがよくあります。この 2 つの概念は異なります。新しいバージョンにアップグレー

ドしなくても、例えば管理するリージョンを変更することで、ランディングゾーン設定を更新できるためです。コンソールで [更新] ボタンを選択すると、現在のランディングゾーンバージョンとデプロイするランディングゾーンバージョンに基づいて、インプレース更新またはアップグレードオペレーションが実行されます。

ランディングゾーンバージョンの選択 – コンソールでの手順

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

アカウントの更新、ランディングゾーンバージョン、およびベースライン

AWS Control Tower ランディングゾーンは、一連のベースライン設定に対応する AWS リソースです。ベースラインとランディングゾーンバージョンのマッピングはありません one-to-one。OU ベースラインとランディングゾーンバージョンの互換性を示す表を参照できます。

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

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

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

ランディングゾーンのスキーマ

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

AWS Control Tower ランディングゾーンのバージョン 3.0 以降のスキーマは、互換性のあるバージョンの選択に役立つように、このリファレンスセクションで公開されています。

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

ランディングゾーン 3.1 のスキーマ

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

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

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

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

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

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

ランディングゾーン 3.2 のスキーマ

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

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

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

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

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

```
                "maxLength": 120,
                "minLength": 1,
                "pattern": "^[\\s\\S]*$",
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "OrganizationStructure": {
        "type": "object",
        "required": [
            "security"
        ],
        "properties": {
            "sandbox": {
                "$ref": "#/definitions/OrganizationalUnit"
            },
            "security": {
                "$ref": "#/definitions/OrganizationalUnit"
            }
        },
        "additionalProperties": false
    },
    "S3BucketConfiguration": {
        "type": "object",
        "properties": {
            "retentionDays": {
                "type": "number",
                "minimum": 1,
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "SecurityRoles": {
        "type": "object",
        "required": [
            "accountId"
        ],
        "properties": {
            "accountId": {
                "type": "string",
                "maxLength": 12,
                "minLength": 12,
```

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

ランディングゾーン 3.3 のスキーマ

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

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

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

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

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

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

リセットと再登録でドリフトを解決する

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

AWS Control Tower ではドリフト検出が自動的に行われます。の自動スキャンは、ドリフトを解決するために変更や設定の更新が必要なリソースを特定するSCPsのに役立ちます。

さまざまなタイプのドリフトを修復するには、コンソールのランディングゾーン設定ページでリセットを選択します。また、コンソールで OU を再登録することを選択することで、一部のタイプのドリフトを解決できます。コントロールの場合、 を呼び出すことでプログラムでドリフトを解決できますResetEnabledControlAPI。ドリフトの種類とその解決方法の詳細については、「ガバナンスドリフトのタイプ」と「AWS Control Tower でドリフトを検出して解決する」を参照してください。

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

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

- 最新のランディングゾーンバージョンを使用している場合、リセットを選択してから確認を選択すると、ドリフトしたランディングゾーンリソースは保存された AWS Control Tower 設定にリセットされます。ランディングゾーンバージョンは変わりません。
- 最新バージョンでない場合は、[更新] を選択する必要があります。ランディングゾーンは最新のランディングゾーンバージョンにアップグレードされます。このプロセスの一環としてドリフトが解決されます。

自動化によるアカウントのプロビジョニングと更新

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

- AWS Control Tower Account Factory for Terraform () を使用して、アカウントをプロビジョニングおよびカスタマイズできますAFT。詳細については、「AWS Control Tower Account Factory for Terraform の概要 (AFT) 」を参照してください。
- Customizations for AWS Control Tower (CfCT) を使用してアカウントを更新できます。詳細については、「 AWS Control Tower のカスタマイズ (CfCT) の概要 」を参照してください。
- スクリプトの自動化: APIアプローチを使用する場合は、Service Catalog のAPIフレームワークとを使用してアカウントを更新 AWS CLI し、バッチプロセスでアカウントを更新できます。アカウントごとに Service Catalog `UpdateProvisionedProduct`APIの を呼び出します。この を使用して、アカウントを 1 つずつ更新するスクリプトを作成できますAPI。このアプローチの詳細については、ガバナンス用のリージョンを追加するときに、ブログ記事「新しい AWS リージョンでガードレールを有効にする」を参照してください。

  一度に 5 つまでアカウントを更新できます。少なくとも 1 つのアカウントの更新を無事に完了してから、次のアカウントの更新を開始してください。したがって、アカウントが多くある場合

は、処理に時間がかかることはありますが、複雑ではありません。この方法の詳細については、「チュートリアル: Service Catalog による AWS Control Tower でのアカウントプロビジョニングの自動化 APIs」を参照してください。

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

スクリプトによる自動化のさらなるステップは、AWSControl Tower `UpdateLandingZone`ライフサイクルイベントの成功ステータスを確認することです。これは、動画で説明されているように個々のアカウントの更新を開始するためのトリガーとして使用します。ライフサイクルイベントは一連のアクティビティの完了を示すため、このイベントが発生するとランディングゾーンの更新が完了したことを意味します。アカウントの更新を開始する前に、ランディングゾーンの更新が完了している必要があります。ライフサイクルイベントの操作の詳細については、「ライフサイクルイベント」を参照してください。

以下も参照してください。

- AWS CloudShell を使用して を操作する AWS Control Tower.
- AWS Control Tower でタスクを自動化する .

AWS Control Tower でタスクを自動化する

多くのお客様は、アカウントのプロビジョニング、コントロールの割り当て、監査な
ど、AWSControl Tower でのタスクの自動化を好みます。これらの自動アクションは、次のコールを使って設定できます。

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

追加情報とリンク このページには、AWSControl Tower でのタスクの自動化に役立つ優れた技術ブログ投稿へのリンクが含まれています。以下のセクションでは、タスクの自動化に役立つこの AWS Control Tower ユーザーガイドの領域へのリンクを提供します。

コントロールタスクの自動化

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

AWS Control Tower でコントロールオペレーションを実行する方法の詳細についてはAPIs、ブログ記事AWS「Control Tower リリース API、組織単位への事前定義されたコントロール」を参照してください。

ランディングゾーンタスクの自動化

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

OU 登録の自動化

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

アカウントの自動解約

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

アカウントのプロビジョニングと更新の自動化

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

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

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

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

スクリプトによるアカウントの更新も参照してください。

プログラムによるアカウントの監査

プログラムによるアカウントの監査の詳細については、AWS「Control Tower 監査アカウントのプログラムによるロールと信頼関係」を参照してください。

その他のタスクの自動化

自動リクエスト方式を使用して特定の AWS Control Tower サービスクォータを引き上げる方法については、「サービス制限の引き上げを自動化」の動画をご覧ください。

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

セキュリティに関連する特定の自動化タスクに役立つ GitHub 2 つのオープンソースサンプルが で利用できます。

- aws-control-tower-org-setup-sample というサンプルは、セキュリティ関連サービスの委任管理者として Audit アカウントを設定する方法を示しています。
- というサンプルは、新しいアカウントをプロビジョニングおよび設定するときに Step Functions を使用してセキュリティのベストプラクティスを自動化する方法aws-control-tower-accountsetup-using-step-functionsを示しています。このサンプルには、組織で共有された AWS Service Catalog ポートフォリオにプリンシパルを追加したり、組織全体の Identity Center AWS IAMグループを新しいアカウントに自動的に関連付けたりすることが含まれます。また、すべてのリージョンVPCでデフォルトを削除する方法も示します。

AWS セキュリティリファレンスアーキテクチャには、AWSControl Tower に関連するタスクを自動化するためのコード例が含まれています。詳細については、AWS 「 規範的ガイダンス」ページおよび関連する GitHub リポジトリを参照してください。

での作業を容易にする AWS サービスで AWS Control Tower を使用する方法については AWS CloudShell、AWS CloudShell 「」および AWS CLI AWS CLI「」を参照してください。

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

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

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

から を起動 AWS CloudShellAWS Management Consoleすると、コンソールへのサインインに使用した AWS 認証情報が新しいシェルセッションで使用できます。 AWS Control Tower およびその他の AWS サービスとやり取りするときは、設定認証情報の入力をスキップできます。また、シェルのコンピューティング環境にプリインストールされている AWS CLI バージョン 2 を使用します。事前認証済みです AWS CloudShell。

のIAMアクセス許可を取得する AWS CloudShell

AWS Identity and Access Management は、管理者がアクセス許可をIAMユーザーおよび IAM Identity Center ユーザーに付与してアクセスできるようにするアクセス管理リソースを提供します AWS CloudShell。

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

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

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

> **Note**
>
> IAM ID には、 を呼び出すアクセス許可を付与するポリシーも必要です AWS Control Tower。詳細については、「 AWS Control Tower コンソールを使用するために必要なアクセス許可」を参照してください。

起動 AWS CloudShell

から AWS Management Console、ナビゲーションバーで使用できる次のオプション CloudShell を選択して を起動できます。

- CloudShell アイコンを選択します。
- 検索ボックスに「cloudshell」と入力し始め、オプションを選択します CloudShell。

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

AWS Control Tower を介して を操作する AWS CloudShell

AWS CloudShell から を起動すると AWS Management Console、コマンドラインインターフェイス AWS Control Tower からすぐに とのやり取りを開始できます。 AWS CLI コマンドは で標準的に動作します CloudShell。

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

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

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

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

   例: AWS Config ステータスを確認する

   表示コマンド:

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`
   - `aws configservice describe-configuration-recorders`
   - 通常の応答は `"name": "default"` のようになります。
2. AWS Control Tower ランディングゾーンを設定する前に削除する必要がある既存の AWS Config レコーダーまたは配信チャネルがある場合は、入力できるコマンドをいくつか次に示します。

   例: 既存の AWS Config リソースを管理する

削除コマンド:

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

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

詳細については、 AWS Config ドキュメントを参照してください。

- 設定レコーダーの管理 (AWS CLI)
- 配信チャネルの管理

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

   例: 信頼されたサービスのアクセスを有効化または無効化する

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

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

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

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

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

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

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

> **Note**
>
> バケットの命名規則に従わない場合 (例えば、小文字のみを使用) 、次のエラーが表示されます。 CreateBucket オペレーションを呼び出すときにエラーが発生した (InvalidBucketName) 。指定されたバケットは無効です。

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

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

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

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

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

で AWS Control Tower リソースを作成する AWS CloudFormation

AWS Control Tower は と統合されています。これは AWS CloudFormation、 AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセッ

トアップを支援するサービスです。AWS::ControlTower::EnabledControl controls. AWS CloudFormation provisions など、必要なすべての AWS リソースを記述するテンプレートを作成します。

を使用すると AWS CloudFormation、テンプレートを再利用して AWS Control Tower リソースを一貫して繰り返しセットアップできます。リソースを 1 回記述し、複数の AWS アカウント および リージョンで同じリソースを何度もプロビジョニングします。

AWS Control Tower および AWS CloudFormation テンプレート

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

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

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

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

の詳細 AWS CloudFormation

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

- AWS CloudFormation

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

AWS Control Tower ランディングゾーンをカスタマイズする

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

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

AWS Control Tower コンソールからカスタマイズする

ランディングゾーンにこれらのカスタマイズを行うには、AWSControl Tower コンソールで指定された手順に従います。

セットアップ時にカスタマイズした名前を選択する

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

> **ヒント**
>
> で OU の名前を変更 AWS Organizations しても、Account Factory の対応するプロビジョニング済み製品は更新されないことに注意してください。プロビジョニング済み製品を自動的に更新するには (ドリフトを避けるには) 、OU の作成、削除、再登録など、AWSControl Tower を介して OU オペレーションを実行する必要があります。

AWS リージョンの選択

- ガバナンスの対象となる特定の AWS リージョンを選択することで、ランディングゾーンをカスタマイズできます。AWS Control Tower コンソールのステップに従います。

- ランディングゾーンを更新するときに、ガバナンスの AWS リージョンを選択または選択解除できます。
- リージョン拒否コントロールを有効または無効に設定し、管理対象外 AWS リージョンのほとんどの AWS サービスへのユーザーアクセスを制御できます。

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

オプションのコントロールを追加してカスタマイズする

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

AWS CloudTrail 証跡をカスタマイズする

- ランディングゾーンをバージョン 3.0 以降に更新する場合、AWSControl Tower が管理する組織レベルの CloudTrail 証跡をオプトインまたはオプトアウトできます。この選択は、ランディングゾーンを更新するたびに変更できます。 AWSControl Tower は、管理アカウントに組織レベルの証跡を作成し、その証跡は、選択したステータスに基づいてアクティブまたは非アクティブになります。ランディングゾーン 3.0 はアカウントレベルの CloudTrail 証跡をサポートしていませんが、これらが必要な場合は、独自の証跡を設定および管理できます。証跡が重複すると、追加料金が発生する場合があります。

コンソールでカスタマイズされたメンバーアカウントを作成する

- Control Tower コンソールから、カスタマイズした AWS Control Tower AWS メンバーアカウントを作成し、既存のメンバーアカウントを更新してカスタマイズを追加できます。詳細については、

「Account Factory Customization を使用してアカウントをカスタマイズする (AFC)」を参照してください。

AWS Control Tower コンソール外でのカスタマイズの自動化

一部のカスタマイズは AWS Control Tower コンソールでは利用できませんが、他の方法で実装できます。以下に例を示します。

- Account Factory for Terraform (AFT) を使用すると、プロビジョニング中に、 GitOpsスタイルのワークフローでアカウントをカスタマイズできます。

  AFT は、 AFTリポジトリで利用可能な Terraform モジュールでデプロイされます。
- AWS テンプレート AWS CloudFormation とサービスコントロールポリシー () に基づいて構築された機能のパッケージである Customizations for AWS Control Tower (CfCT) を使用して、Control Tower ランディングゾーンをカスタマイズできますSCPs。 CfCT カスタムテンプレートとポリシーは、組織内の個々のアカウントと組織単位 (OUs) にデプロイできます。

  CfCT のソースコードはGitHub リポジトリにあります。
- Landing Zone Accelerator (LZA) をオンにして、 AWS Control Tower ランディングゾーンをカスタマイズできます AWS。このLZAソリューションは、 AWS ベストプラクティスに合致し、複数のグローバルコンプライアンスフレームワークに準拠するように設計されています。AWS Control Tower を基本的なランディングゾーンとしてデプロイし、LZA必要に応じて でランディングゾーン機能を強化することをお勧めします。詳細については、AWS「Control Tower とランディングゾーンアクセラレーター」を参照してください。

AWS Control Tower とランディングゾーンアクセラレーター

このセクションでは、AWSControl Tower と Landing Zone Accelerator (LZA) ソリューションを一緒に使用する利点について説明します。

Landing Zone Accelerator (LZA) をオンにして、 AWS Control Tower ランディングゾーンをカスタマイズできます AWS 。

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

LZA は、安全なワークロードのホスティングに適したクラウド環境を自動的にセットアップします。このソリューションは、運用とガバナンスの一貫性を維持するために AWS リージョン、すべての にデプロイできます。このLZAソリューションは、 AWS ベストプラクティスに合致し、複数のグローバルコンプライアンスフレームワークに準拠するように設計されています。

AWS Control Tower を基本的なランディングゾーンとしてデプロイし、LZA必要に応じて でランディングゾーンの機能を強化することをお勧めします。LZA と AWS Control Tower の組み合わせは、マルチアカウント環境の管理と管理に役立つ包括的なノーコードソリューションを提供します。これは、規制の厳しいワークロードと複雑なコンプライアンス要件をサポートするように構築されています。AWS Control Tower と Landing Zone Accelerator を組み合わせることで、セキュリティ、コンプライアンス、運用機能などのプラットフォームの準備状況を確立できます。

のソースコードLZAはGitHub リポジトリで使用できます。

LZA と AWS Control Tower を組み合わせる方法の詳細については、「 LZA実装ガイド」を参照してください。

AWS Control Tower のカスタマイズ (CfCT) の利点

Control Tower のカスタマイズ (CfCT) と呼ばれる機能のパッケージは、AWSControl AWS Tower コンソールで作成できるよりも広範なカスタマイズをランディングゾーンに作成するのに役立ちます。CfCT これは、 GitOpsスタイルの自動化されたプロセスを提供します。ビジネス要件を満たすようにランディングゾーンを作り直すことができます。

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

> **Note**
>
> Account Factory や とは異なりAFT、CfCT は特に新しいアカウントを作成することを目的としたものではなく、指定したリソースをデプロイしてランディングゾーンOUsでアカウントと をカスタマイズすることを目的としています。

利点

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

その他の CfCT の例

- 「Customizations for AWS Control Tower (CfCT)」によるネットワーキングのユースケースの例は、「Service Catalog と AWS Control Tower のカスタマイズDNSと整合性のあるデプロイ」という AWS アーキテクチャブログ記事に記載されています。
- CfCT と Amazon に関連する GuardDuty特定の例は、 `aws-samples`リポジトリの GitHub で利用できます。
- CfCT に関するその他のコード例は、`aws-samples` リポジトリの AWS セキュリティリファレンスアーキテクチャの一部として入手できます。これらの例の多くで、サンプルの `manifest.yaml` ファイルが `customizations_for_aws_control_tower` という名前のディレクトリに含まれています。

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

AWS Control Tower のカスタマイズ (CfCT) の概要

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

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

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

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

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

Customizations for AWS Control Tower (CfCT) の最新の更新と変更については、 GitHub リポジトリの CHANGELOG.md ファイルを参照してください。

アーキテクチャの概要

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

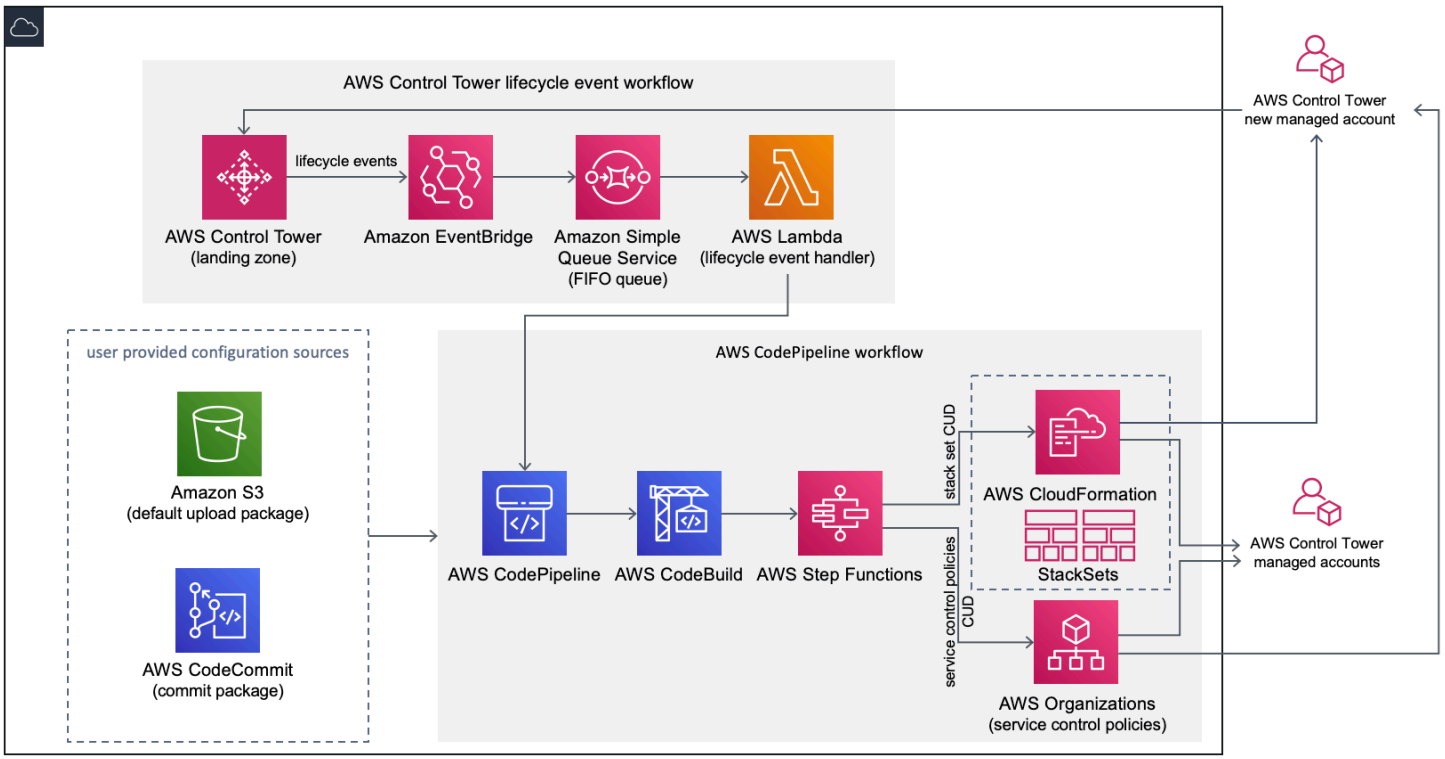

図 1: AWS Control Tower アーキテクチャのカスタマイズ

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

> **メモ**
>
> CfCT はAWS、Control Tower ランディングゾーンがデプロイされる場所であるため、Control Tower ホームリージョンと AWS Control Tower AWS 管理アカウントにデプロイする必要があります。AWS Control Tower ランディングゾーンの設定については、「」を参照してください入門。

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

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

CfCT は次の 2 つのワークフローをデプロイします。

- AWS CodePipeline ワークフロー
- および AWS Control Tower ライフサイクルイベントワークフロー。

AWS CodePipeline ワークフロー

AWS CodePipeline ワークフローは AWS CodePipeline、組織SCPs内の と の管理AWS Step Functionsを調整する 、 AWS CodeBuildプロジェクト AWS CloudFormation StackSets 、 を設定します。

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

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

各ステージで、コードパイプラインはスタックセットとSCPステップ関数を呼び出します。これにより、カスタムスタックセットと SCPs がターゲットの個々のアカウント、または組織単位全体にデプロイされます。

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

AWS Control Tower ライフサイクルイベントワークフロー

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

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

コスト

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

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

コンポーネントサービス

以下の AWS サービスは、Customizations for AWS Control Tower (CfCT) のコンポーネントです。

AWS CodeCommit

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

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

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

> **Note**
>
> をまだ使用していない場合 CodeCommit、唯一のオプションは、設定パッケージのストレージロケーションとして Amazon S3 バケットを設定することです。CfCT を初めてデプロイする場合は CodeCommit 、 は使用できません。

AWS CodePipeline

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

AWS Key Management Service

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

AWS Lambda

CfCT は、 AWS Lambda 関数を使用して、AWSControl Tower ライフサイクルイベントの初期インストールおよびデプロイ中 AWS CloudFormation StackSets 、または AWS Organizations SCPs 中にインストールコンポーネントを呼び出します。

Amazon Simple Notification Service

CfCT は、ワークフロー中にパイプラインの承認などの通知を Amazon Simple Notification Service (Amazon SNS) トピックに発行することがあります。Amazon SNS は、パイプライン承認通知の受信を選択した場合にのみ起動されます。

Amazon Simple Storage Service

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

例: Amazon S3 バケット名

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

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

ファイル名の先頭にアンダースコアがあることに注意してください。

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

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

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

Amazon Simple Queue Service

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

AWS Step Functions

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

AWS Systems Manager パラメータストア

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

デプロイに関する考慮事項

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

デプロイの準備

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

設定ソースを選択します。

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

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

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

> **圧縮の必要性の有無**
>
> デフォルトの S3 バケットを使用する場合は、設定パッケージが `.zip` ファイルとして利用できることを確認します。 AWS CodeCommit リポジトリを使用する場合は、必ず、ファイルを圧縮せずに設定パッケージをリポジトリに配置してください。で設定パッケージを作成して保存する方法については AWS CodeCommit、「」を参照してくださいCfCT カスタマイズガイド。

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

パイプライン設定の承認パラメータの選択

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

手動承認を有効にすると、設定パイプラインは AWS Control Tower ファイルマニフェストとテンプレートに対して行われたカスタマイズを検証し、手動承認が付与されるまでプロセスを一時停止します。承認後、デプロイは必要に応じて残りのパイプラインステージを実行し、Customizations for AWS Control Tower (CfCT) 機能を実装します。

手動承認パラメータを使用して、パイプラインで実行しようとする最初の試行を拒否することで、AWSControl Tower 設定のカスタマイズの実行を維持できます。このパラメータを使用すると、

実装前の最終制御として、AWSControl Tower の設定変更のカスタマイズを手動で検証することもできます。

AWS Control Tower のカスタマイズを更新するには

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

テンプレートおよびソースコード

AWS Control Tower のカスタマイズ (CfCT) は、 AWS CloudFormation テンプレートの起動後に管理アカウントにデプロイされます。テンプレートは からダウンロードし GitHub 、 から起動できますAWS CloudFormation。

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

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

> **Note**
>
> テンプレートは特定の要件に基づいてカスタマイズできます。

ソースコードリポジトリ

GitHub リポジトリにアクセスして、CfCT のテンプレートとスクリプトをダウンロードし、ランディングゾーンのカスタマイズを他のユーザーと共有できます。

自動デプロイ

自動デプロイを開始する前に、「考慮事項」を確認してください。このセクションの step-by-step手順に従って、ソリューションを構成し、AWSControl Tower 管理アカウントにデプロイします。

デプロイ時間: 約 15 分

前提条件

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

デプロイ手順

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

ステップ 1. スタックを起動する

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

ステップ 2. カスタムパッケージを作成する

- カスタム設定パッケージを作成します。

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

ステップ 1. スタックを起動する

このセクションの AWS CloudFormation テンプレートは、アカウントに AWS Control Tower のカスタマイズ (CfCT) をデプロイします。

> **メモ**
>
> CfCT の実行中に使用される AWS サービスのコストは、お客様の負担となります。詳細については、コストを参照してください。

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

   > **Note**
   >
   > CfCT は、ホームリージョンである AWS Control Tower ランディングゾーンをデプロイしたのと同じリージョンとアカウントで起動する必要があります。

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

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

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

AWS CodeCommit セットアップ		
パラメータ	デフォルト	説明
CodeCommit ブランチ名	`main`	カスタマイズパッケージが格納される Git ブランチ。このパラメータを使用するには、CodePipeline ソースパラメータを に設定する必要がありますAWS CodeCommit 。
AWS CloudFormation StackSets 設定		
パラメータ	デフォルト	説明
[Region Concurrency Type] (リージョンの同時実行タイプ)	`PARALLEL`	リージョンでのデプロイ StackSetsオペレーションの同時実行タイプを選択します。この設定は、ワークフローの作成、更新、削除に適用されます。その他の許容値は `SEQUENTIAL` です。
[Max Concurrent Percentage] (最大コンカレントパーセンテージ)	`100`	このオペレーションを一度に実行するアカウントの最大の割合。許容される最大値は 100 です。詳細については、「スタックセットオペレーションのオプション」を参照してください。

AWS CloudFormation StackSets 設定		
パラメータ	デフォルト	説明
[Failure Tolerance Percentage] (フォールトトラレーションパーセンテージ)	10	AWS CloudFormation がリージョンでのオペレーションを停止するまでに、そのスタックオペレーションが失敗する可能性のある、リージョンあたりのアカウントの割合。許容される最小値は 0 で、最大値は 100 です。詳細については、「スタックセットオペレーションのオプション」を参照してください。

6. [Next] (次へ) を選択します。
7. [スタックオプションの設定] ページで、[次へ] を選択します。
8. [確認] ページで、設定を確認して確定します。テンプレートが (IAM) リソースを作成する AWS Identity and Access Management ことを確認するチェックボックスを必ずオンにします。
9. [スタックの作成] を選択してスタックをデプロイします。

   スタックのステータスは、 AWS CloudFormation コンソールの Status 列で確認できます。約 15 分後に CREATE_COMPLETE のステータスが表示されます。

ステップ 2. カスタムパッケージを作成する

起動されたスタックでは、含まれている設定パッケージをカスタマイズすることで、AWSControl Tower ランディングゾーンとサービスコントロールポリシー (SCPs) にカスタマイズを追加できます。カスタムパッケージを作成する詳細な手順については、「CfCT カスタマイズガイド」を参照してください。

> **注意**
>
> パイプラインは、カスタム設定パッケージをアップロードしないと実行されません。

スタックを更新する

以前に Customizations for AWS Control Tower (CfCT) をデプロイした場合は、手順に従って CfCT フレームワークの最新バージョンの AWS CloudFormation スタックを更新します。

> **Important**
>
> 次の手順を完了する前に、 から Amazon Simple Storage Service (Amazon S3) バケットに最新のテンプレート GitHubをアップロードする必要があります。Amazon S3 Amazon S3 の使用を開始する方法については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 の開始方法」を参照してください。

1. AWS CloudFormation コンソール にサインインします。
2. AWS Control Tower の既存のカスタマイズ (CfCT) CloudFormation スタックを選択し、更新を選択します。
3. [前提条件 – テンプレートの準備] で、[既存テンプレートを置き換える] を選択します。
4. [テンプレートの指定] ページで、以下を実行します。
   a. [テンプレートソース] で、[既存テンプレートを置き換える] を選択します。
   b. Amazon S3 でURL、 から Amazon S3 GitGub にアップロードしたテンプレートURLのテンプレートを入力し、次へを選択します。
   c. テンプレートURLが正しいことを確認します。[次へ] を選択し、もう一度 [次へ] を選択します。
5. [Parameters] (パラメータ) で、テンプレートのパラメータを確認し、必要に応じて変更します。パラメータの詳細については、「ステップ 1。 スタックを起動する」を参照してください。
6. [Next] (次へ) を選択します。
7. [スタックオプションの設定] ページで、[次へ] を選択します。
8. [確認] ページで、設定を確認して確定します。テンプレートが (IAM) リソースを作成する AWS Identity and Access Management 可能性があることを確認するチェックボックスをオンにしてください。
9. [変更セットの表示] を選択して、変更を確認します。
10. [スタックの更新] を選択してスタックをデプロイします。

    スタックのステータスは、 AWS CloudFormation コンソールの Status 列で確認できます。約 15 分後に UPDATE_COMPLETE のステータスが表示されます。

スタックセットの削除

マニフェストファイルでスタックセットの削除を有効にしている場合は、スタックセットを削除できます。デフォルトでは、enable_stack_set_deletion パラメータが false に設定されています。この設定では、リソースが CfCT マニフェストファイルから削除されていると、関連するスタックセットを削除するアクションは実行されません。

マニフェストファイルで enable_stack_set_deletion の値を true に変更すると、マニフェストファイルから関連するリソースを削除したときに、CfCT はスタックセットとそのすべてのリソースを削除します。

この機能は、マニフェストファイルの v2 でサポートされています。

> **Important**
>
> 最初に の値を に設定するとenable_stack_set_deletiontrue、次に CfCT を呼び出すときに、キータグ CustomControlTower-が関連付けられているプレフィックス で始まりKey:AWS_Solutions, Value: CustomControlTowerStackSet、マニフェストファイルで宣言されていないALLリソースは削除対象としてステージングされます。

このパラメータを manifest.yaml ファイルで設定する方法の例を次に示します。

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2

  - name: demo_resource_2
```

```
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - eu-north-1
```

Simple Storage Service (Amazon S3) を設定ソースとしてセットアップする

AWS Control Tower のカスタマイズを設定すると、 `_custom-control-tower-configuration.zip` ファイルと呼ばれる初期設定ファイルが、 という名前の Amazon Simple Storage Service (Amazon S3) バケットに保存されます`custom-control-tower-configuration-`*`account-ID`*`-`*`region`*。

> **メモ**
>
> このファイルをダウンロードして変更する場合は、変更を圧縮し、`custom-control-tower-configuration.zip` という名前を付けて新しいファイルとして保存してから、同じ Simple Storage Service (Amazon S3) バケットにアップロードします。
> Simple Storage Service (Amazon S3) バケットは、パイプラインのデフォルトのソースです。デフォルト設定が指定されている場合、ファイル名にアンダースコアプレフィックスを含まない設定 zip ファイルを S3 バケットにアップロードすると、パイプラインが自動的に開始されます。

zip ファイルは、 AWS Key Management Service （ SSE) を使用したサーバー側の暗号化 (AWS KMS ）、およびKMSキーの使用拒否によって保護されます。zip ファイルにアクセスするには、KMSキーポリシーを更新して、アクセスを許可するロール (複数可) を指定する必要があります。ロールは、管理者ロール、ユーザー、またはその両方とすることができます。次の手順に従ってください。

1. AWS Key Management Service コンソールに移動します。

2. カスタマーマネージドキーで、 を選択しますCustomControlTowerKMSKey。
3. [Key policy] (キーポリシー) タブを選択します。次に、[Edit] (編集) を選択します。
4. [Edit key policy] (キーポリシーの編集) ページで、コード内の [Allow Use of the key] (キーの使用を許可) セクションを開き、次のいずれかのアクセス許可を追加します。
   - 管理者ロールを追加する場合:

     ```
     arn:aws:iam::<account-ID>:role/<administrator-role>
     ```
   - ユーザーを追加する場合:

     ```
     arn:aws:iam::<account-ID>:user/<username>
     ```
5. [Save Changes] (変更を保存) をクリックします。
6. Simple Storage Service (Amazon S3) コンソールに移動し、設定 zip ファイルが含まれている S3 バケットを探して、[download] (ダウンロード) を選択します。
7. マニフェストファイルとテンプレートファイルに対して必要な設定変更を行います。マニフェストファイルとテンプレートファイルのカスタマイズについては、「the section called “CfCT カスタマイズガイド”」を参照してください。
8. 変更をアップロード:
   a. 変更された設定ファイルを圧縮し、ファイルに `custom-control-tower-configuration.zip` という名前を付けます。
   b. AWS KMS master-key: で を使用して Amazon S3 にファイルをアップロードしますCustomControlTowerKMSKey。 SSE

設定ソース GitHub として を設定する

このセクションでは、 をソース GitHub として AWS Control Tower のカスタマイズ (CfCT) をデプロイする方法について説明します。このプロセスには主に 3 つのステップがあります。

- GitHub リポジトリを準備する
- GitHub コード接続を作成する
- AWS CloudFormation スタックをデプロイする

GitHub リポジトリを準備する

GitHub アカウント内にリポジトリを作成します。テンプレートで使用されるデフォルト名は `custom-control-tower-configuration` です。ターゲットリポジトリをプライベートにすることを検討してください。カスタマイズは、CfCT リポジトリのデプロイフォルダにある `manifest.yaml` というファイルに定義します。

CfCT カスタマイズガイド」では、カスタマイズを設定するための `manifest.yaml` の作成に関する詳細なガイダンスを提供します。

GitHub 接続を作成する

Github のデベロッパーツール --Connections インスタンスから、次のステップを実行します。

1. 接続の作成を選択し、プロバイダー GitHub として を選択します。
2. GitHub アプリ接続の作成を選択し、接続名フィールドに GitHub CfCT または任意の名前を入力します。
3. Connect to GitHub を選択し、Install a new app を選択します。
4. リポジトリの GitHub ユーザーまたは組織を選択する
5. リポジトリアクセスで、リポジトリのみを選択し、前に作成したリポジトリを選択して、作業を保存します。
6. コード接続に注意してくださいARN。 AWS CloudFormation スタックをデプロイするときに必要になります。

AWS CloudFormation スタックをデプロイする

- リポジトリから `custom-control-tower-initiation.template` ファイルをダウンロードします。
- `custom-control-tower-initiation.template` ファイルを使用して新しい AWS CloudFormation スタックを作成します。
- AWS CodePipeline ソース で、 GitHub （ コード接続経由 ） を選択します。
- GitHub セットアップで、以下のフィールドを指定します。
  - ARN コード接続の には、コード接続を指定します。 ARN
  - GitHub ユーザーまたは組織の場合は、リポジトリを作成した GitHub ユーザーまたは組織の名前を入力します。

- GitHub リポジトリ名にリポジトリ名を入力します (デフォルトは `custom-control-tower-configuration`) 。
- GitHub ブランチ名には、ブランチ名を入力します (デフォルトは `main`) 。

運用メトリクスの収集

AWS Control Tower のカスタマイズ (CfCT) には、匿名の運用メトリクスを AWS に送信するオプションが含まれています。AWS ではこのデータを使用して、お客様が CfCT をどのように使用しているか、および関連するサービスや製品を把握します。データ収集が有効になっていると、次の情報が AWS に送信されます。

- ソリューション ID: AWS ソリューション識別子
- 一意の ID (UUID): デプロイごとにランダムに生成された一意の識別子
- タイムスタンプ: データ収集タイムスタンプ
- ステートマシンの実行回数: このステートマシンが実行された回数を増分カウントします。
- マニフェストのバージョン: 設定で使用されるマニフェストバージョン

> **Note**
>
> AWS は収集したデータを所有します。データ収集には、AWS プライバシーポリシーが適用されます。

匿名の運用メトリクスを AWS に送信しないようにするには、次のいずれかのタスクを実行します。

- AWS CloudFormation テンプレートマッピングセクションを次のように更新します。

  from

```
AnonymousData:
     SendAnonymousData:
        Data: Yes
```

  ~

```
AnonymousData:
```

```
    SendAnonymousData:
       Data: No
```

- CfCT をデプロイしたら、パラメータストアコンソールで **/org/primary/metrics_flag** SSM パラメータキーを見つけ、値を **No** に更新します。

CfCT カスタマイズガイド

AWS Control Tower のカスタマイズ (CfCT) ガイドは、AWS Control Tower 環境を会社または顧客向けにカスタマイズおよび拡張することを希望する管理者、DevOps プロフェッショナル、独立系ソフトウェアベンダー、IT インフラストラクチャアーキテクト、システムインテグレーターを対象としています。このガイドでは、CfCT カスタマイズパッケージを使用して AWS Control Tower 環境をカスタマイズおよび拡張する際に役立つ情報を提供します。

> **Note**
>
> (CfCT) をデプロイして設定するには、設定パッケージをデプロイして処理する必要があります AWS CodePipeline。以下のセクションではこのプロセスを詳しく説明します。

コードパイプラインの概要

設定パッケージには、Amazon Simple Storage Service (Amazon S3) と が必要です AWS CodePipeline。設定パッケージには、次の項目が含まれています。

- マニフェストファイル
- 付随するテンプレートのセット
- AWS Control Tower 環境のカスタマイズを記述および実装するためのその他の JSON ファイル

デフォルトでは、`_custom-control-tower-configuration.zip` 設定パッケージは、次の命名規則に従って Simple Storage Service (Amazon S3) バケットにロードされます。

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

> **Note**
>
> デフォルトでは、CfCT はパイプラインソースを格納するために Amazon S3 バケットを作成します。ほとんどのお客様は、このデフォルトのままで構いません。既存の AWS

CodeCommit リポジトリがある場合は、ソースの場所を AWS CodeCommit リポジトリに変更できます。詳細については、「AWS CodePipeline ユーザーガイド」の「CodePipeline でパイプラインを編集する」を参照してください。

マニフェストファイルは、ランディングゾーンをカスタマイズするためにデプロイできる AWS リソースについて記述するテキストファイルです。CodePipeline は次のタスクを実行します。

- マニフェストファイル、それに付随するテンプレートのセット、およびその他の JSON ファイルを抽出する
- マニフェストとテンプレートの検証を実行する
- マニフェストファイル内のセクションを呼び出して特定の パイプラインステージを実行する。

マニフェストファイルをカスタマイズし、設定パッケージのファイル名からアンダースコア (_) を削除して設定パッケージを更新すると、 AWS CodePipelineが自動的に開始されます。

アンダースコアを覚えておく

設定パッケージのサンプルファイル名はアンダースコア (_) で始まるため、 AWS CodePipeline は自動的に開始されません。設定パッケージのカスタマイズが完了したら、AWS CodePipelineでデプロイをトリガーするため、アンダースコア (_) を付けずにファイル `custom-control-tower-configuration.zip` をアップロードします。

AWS CodePipeline ステージ

CfCT パイプラインでは、AWS Control Tower 環境を実装および更新するために複数の AWS CodePipeline ステージが必要です。

1. ソースステージ

   ソースステージは最初のステージです。カスタマイズされた設定パッケージによって、このパイプラインステージが開始されます。のソース AWS CodePipeline は、設定パッケージをホストできる Amazon S3 バケットまたは AWS CodeCommit リポジトリのいずれかです。

2. ビルドステージ

   ビルドステージでは、設定パッケージの内容を検証 AWS CodeBuild する必要があります。これらのチェックには、 および を使用して、パッケージに含まれる、またはリモートでホストされる

すべての AWS CloudFormation テンプレートとともに、manifest.yamlファイルの構文 AWS CloudFormation validate-templateとスキーマのテストが含まれますcfn_nag。マニフェストファイルと AWS CloudFormation テンプレートがテストに合格すると、パイプラインは次のステージに進みます。テストに不合格だった場合は、CodeBuild ログを確認して問題を特定し、必要に応じて設定ソースファイルを編集できます。

3. 手動承認ステージ (オプション)

   手動承認ステージはオプションです。このステージを有効にすると、設定パイプラインをさらに制御できます。承認が得られるまで、デプロイ中のパイプラインは一時停止します。手動承認をオプトインするには、スタックを起動したときに、[Pipeline Approval Stage] (パイプライン承認ステージ) パラメータを [Yes] (はい) に変更します。

4. ポリシーステージ

   ポリシーステージは、サービスコントロールポリシー (SCP) またはリソースコントロールポリシー (RCP) ステートマシンを呼び出して、SCPsまたは RCP を作成する AWS Organizations APIs を呼び出します。 RCPs

5. AWS CloudFormation リソースステージ

   AWS CloudFormation リソースステージは、スタックセットステートマシンを呼び出して、マニフェストファイルで指定したアカウントまたは組織単位 (OUs) のリストで指定されたリソースをデプロイします。ステートマシンは、マニフェストファイルで指定された順序で AWS CloudFormation リソースを作成します。リソースの依存関係を指定するには、マニフェストファイルでリソースが指定されている順序を調整します。マニフェストファイル内のリソースの順序は、依存関係を指定する唯一の方法です。

カスタム設定の定義

マニフェストファイル、付随するテンプレートのセット、およびその他の JSON ファイルを使用して、カスタム AWS Control Tower 設定を定義します。これらのファイルをフォルダ構造にパッケージ化し、次のコード例に示すように、Simple Storage Service (Amazon S3) バケット内に .zip ファイルとして配置します。

カスタム設定フォルダ構造

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
```

```
    - template files for AWS CloudFormation Resources (*.template)
```

前の例は、カスタム設定フォルダの構造を示しています。フォルダ構造は、ソースストレージの場所として Amazon S3 または AWS CodeCommit リポジトリを選択しても変わりません。Simple Storage Service (Amazon S3) をソースストレージとして選択した場合は、すべてのフォルダとファイルを `custom-control-tower-configuration.zip` ファイルをアップロードし、`.zip` ファイルのみを指定された Simple Storage Service (Amazon S3) バケットにアップロードします。

> **Note**
>
> を使用している場合は AWS CodeCommit、ファイルを圧縮せずにリポジトリに配置します。

マニフェストファイル

`manifest.yaml` ファイルは、 AWS リソースを説明するテキストファイルです。次の例は、マニフェストファイルの構造を示しています。

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

resources:
  #set of CloudFormation resources, SCP policies, or RCP policies
...
```

前のコード例で示したように、マニフェストファイルの最初の 2 行は、region と version キーワードの値を指定します。これらのキーワードの定義は次のとおりです。

region — AWS Control Tower のデフォルトリージョンのテキスト文字列。この値は、有効な AWS リージョン名 (`us-east-1`、、 `eu-west-1`など) である必要がありますap-southeast-1。AWS Control Tower のホームリージョンは、リソース固有のリージョンが指定されていない限り、カスタム AWS Control Tower リソース (AWS CloudFormation StackSets など) を作成するときのデフォルトです。

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

version — マニフェストスキーマのバージョン番号。サポートされている最新バージョンは 2021-03-15 です。

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

> **Note**
>
> 最新バージョンの使用をお勧めします。マニフェストプロパティを最新バージョンに更新するには、「マニフェストのバージョンのアップグレード」を参照してください。

前の例で示した次のキーワードは、resource キーワードです。マニフェストファイルの [resources] (リソース) セクションは高度に構造化されています。これには、CfCT パイプラインによって自動的にデプロイされる AWS リソースの詳細なリストが含まれています。次のセクションで、リソースとその使用可能なパラメータについて説明します。

マニフェストファイルの [resource] (リソース) セクション

このトピックでは、マニフェストファイルの [リソース] セクションについて説明します。このセクションでは、カスタマイズに必要なリソースを定義します。マニフェストファイルのこのセクションは、キーワード resources から始まり、ファイルの末尾まで続きます。

マニフェストファイルのリソースセクションでは、コードパイプラインを介して CfCT が自動的にデプロイする StackSets、または AWS Organizations SCPs と RCPs を指定します AWS CloudFormation 。OU、アカウント、およびリージョンを一覧表示してスタックインスタンスをデプロイできます。

スタックインスタンスは OU レベルではなくアカウントレベルでデプロイされます。SCPsと RCPs は OU レベルでデプロイされます。詳細については、「独自のカスタマイズを構築する」を参照してください。

次のサンプルテンプレートには、マニフェストファイルの [リソース] セクションで利用可能なエントリが説明されています。

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
```

```
        - OuName1
        - OuName2
    deploy_method: scp | stack_set | rcp
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions: #list of strings
    - [String]
```

このトピックの残りの部分では、前のコード例で示したキーワードの詳しい定義について説明します。

name — AWS CloudFormation StackSets に関連付けられた名前。指定する文字列は、スタックセットに対してよりわかりやすい名前を割り当てます。

- タイプ: 文字列
- 必須: はい
- 有効な値: a ~ z、A ~ Z、0 ~ 9、アンダースコア (_)。その他の文字は、自動的にアンダースコア (_) に置き換えられます。

説明: リソースの説明。

- タイプ: 文字列
- 必須: いいえ

resource_file – このファイルは、マニフェストファイル、 AWS CloudFormation リソース、SCPs、または RCPs を作成するための JSON の AWS CloudFormation テンプレートまたは AWS Organizations サービスコントロールポリシーを指す Amazon S3 URI または URL への相対の場所として指定できます。

- 型: 文字列
- 必須: はい

1. 次の例で示している `resource_file` は、設定パッケージ内のリソースファイルへの相対的な場所として指定されます。

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

2. 次の例は、Amazon S3 URI として指定されているリソースファイルを示しています。

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

3. 次の例は、Simple Storage Service (Amazon S3) HTTPS URL として指定されているリソースファイルを示しています。

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

> **Note**
>
> Simple Storage Service (Amazon S3) URL を指定する場合は、バケットポリシーで、CfCT のデプロイ元となる AWS Control Tower 管理アカウントの読み取りアクセスが許可されていることを確認します。Simple Storage Service (Amazon S3) HTTPS URL を指定する場合は、パスがドット表記を使用していることを確認します。例えば、S3.us-west-1 と指定します。CfCT は、S3 とリージョンの間にダッシュを含むエンドポイントをサポートしていません (S3-us-west-2 など)。

4. 次の例は、リソースを保存する Simple Storage Service (Amazon S3) バケットポリシーと ARN を示しています。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
```

```
}
```

例に示す *AccountId* 変数を、CfCT をデプロイする管理アカウントのアカウント AWS ID に置き換えます。その他の例については、「Amazon Simple Storage Service ユーザーガイド」の「バケットポリシーの例」を参照してください。

parameters — AWS CloudFormation パラメータの名前と値を指定します。

- タイプ: MapList
- 必須: いいえ

[parameters] (パラメータ) セクションには、キー/値パラメータのペアが含まれます。次の疑似テンプレートは、[parameters] (パラメータ) セクションの概要を示します。

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

- parameter_key — パラメータに関連付けられたキー。
  - タイプ: 文字列
  - 必須: はい (パラメータプロパティの下)
  - 有効な値: a ~ z、A ~ Z、0 ~ 9
- parameter_value - パラメータに関連付けられた入力値。
  - タイプ: 文字列
  - 必須: はい (パラメータプロパティの下)

deploy_method — アカウントにリソースをデプロイするためのデプロイ方法。現在、deploy_method は、 AWS CloudFormation StackSets を介したリソースデプロイ`stack_set`のオプション、SCPs をデプロイする場合は `scp` オプション、RCPs をデプロイする場合は `rcp`オプションを使用してリソースをデプロイできます。

- 型: 文字列
- 有効な値: `stack_set` | `scp` | `rcp`
- 必須: はい

deployment_targets – CfCT が AWS CloudFormation リソースをデプロイするアカウントまたは組織単位 (OUs) のリスト。アカウントまたは organization_units として指定されます。

> **Note**
>
> SCP または RCP をデプロイする場合、ターゲットはアカウントではなく OU である必要があります。

- タイプ: このリソースが特定のアカウントリストにデプロイされることを示す文字列 `account name` または `account number`、あるいはこのリソースが指定された OU リストにデプロイされることを示す `OU names` のリスト。
- 必須: accounts または organizational_units のうち少なくとも 1 つ
  - accounts:

    タイプ: このリソースが特定のアカウントリストにデプロイされることを示す文字列 `account name` または `account number` のリスト。
  - organizational_units:

    タイプ: このリソースが特定の OU リストにデプロイされることを示す文字列 `OU names` のリスト。アカウントを含まない OU を指定し、accounts プロパティを追加していない場合、CfCT はスタックセットのみを作成します。

    > **Note**
    >
    > 組織の管理アカウント ID が許可されている値ではありません。CfCT は、組織の管理アカウントへのスタックインスタンスのデプロイをサポートしていません。

export_outps — SSM パラメータキーを表す名前/値のペアのリスト。これらの SSM パラメータキーを使用すると、テンプレート出力を SSM パラメータストアに格納できます。出力は、先にマニフェストファイルで定義済みの他のリソースから参照されることになります。

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

- タイプ: name および value キーペアのリスト。name には SSM パラメータストアキーの name 文字列が含まれ、value にはパラメータの value 文字列が含まれています。
- 有効な値: 任意の文字列、または *CfnOutput-Logical-ID* がテンプレート出力変数に対応する $[output_*CfnOutput-Logical-ID*] 変数。 AWS CloudFormation テンプレートの出力セクションの詳細については、「 AWS CloudFormation ユーザーガイド」の「出力」を参照してください。
- 必須: いいえ

例えば、次のコードスニペットは、/org/member/audit/vpc_id という名前の SSM パラメータキーにテンプレート VPCID の出力変数を保存します。

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> export_outps キー名には、output 以外の値を含めることができます。例えば、name が /org/environment-name の場合、value は production とすることができます。

regions – CfCT が AWS CloudFormation スタックインスタンスをデプロイするリージョンのリスト。

- タイプ： AWS 商用リージョン名のリスト。このリソースが指定されたリージョンリストにデプロイされることを示します。このキーワードがマニフェストファイルに存在しない場合、リソースはホームリージョンにのみデプロイされます。
- 必須: いいえ

ルート OU

マニフェスト V2 バージョン (2021-03-15) では、CfCT は organizational_units の組織単位 (OU) の値としてのルートをサポートしています。

- scp または のデプロイ方法を選択した場合rcp、 の下にルートを追加するとorganizational_units、AWS Control Tower はルートのすべての OUs にポリシーを適用します。stack_set のデプロイ方法を選択した場合、organizational_units でルートを追加す

ると、CfCT は、管理アカウントを除き、AWS Control Tower に登録されているルートの下にあるすべてのアカウントにスタックセットをデプロイします。

- AWS Control Tower のベストプラクティスに従って、管理アカウントはメンバーアカウントの管理と請求のみを目的としています。AWS Control Tower 管理アカウントで本番ワークロードを実行しないでください。

  ベストプラクティスのガイダンスに従って、AWS Control Tower のデプロイでは、管理アカウントはルート OU の下に置かれています。これにより、フルアクセス権を付与しながら、管理アカウントが追加のリソースを実行しないようにします。この理由のため、AWSControlTowerExecution ロールは管理アカウントにデプロイされません。
- 管理アカウントについては、次のベストプラクティスに従うことをお勧めします。特定のユースケースで、管理アカウントにスタックセットをデプロイする必要がある場合は、accounts をデプロイターゲットとして含め、管理アカウントを指定します。それ以外の場合は、accounts をデプロイターゲットとして含めないでください。必要な IAM ロールなど、不足しているリソースを管理アカウントで作成する必要があります。

管理アカウントにスタックセットをデプロイするには、`accounts` をデプロイターゲットとして含め、管理アカウントを指定します。それ以外の場合は、accounts をデプロイターゲットとして含めないでください。

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> ルート OU 機能は、V2 バージョンのマニフェストファイル (2021-03-15) でのみサポートされます。`organizational_units` の OU として [Root] (ルート) を追加する場合、他の OU は追加しないでください。

ネストされた OU

CfCT では、1 つ以上のネストされた OU をマニフェスト V2 バージョン (2021-03-15) の `organizational_units` キーワードでリストすることができます。

OU 間の区切り文字としてコロンを使用した、ネストされた OU の完全なパス (ルートを除く) が必要です。デプロイ方法 `scp`または の場合`rcp`、AWS Control Tower は SCPs または RCPs をネストされた OU パスの最後の OU にデプロイします。デプロイ方法 `stack_set` では、AWS Control Tower は、ネストされた OU パスの最後の OU のすべてのアカウントに、スタックセットをデプロイします。

例えば、パス `OUName1:OUName2:OUName3` について考えてみましょう。パス内の最後の OU は `OUName3` です。CfCT はSCPsまたは RCPsを にデプロイ`OUName3`し`OUName3`、スタックセットをの直下のすべてのアカウントにデプロイします。

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> ネストされた OU 機能は、V2 バージョンのマニフェストファイル (2021-03-15) でのみサポートされます。

独自のカスタマイズを構築する

独自のカスタマイズを構築するには、サービスコントロールポリシー (SCPs)、リソースコントロールポリシー (RCPs)、および AWS CloudFormation リソースを追加または更新して`manifest.yaml`、 ファイルを変更します。デプロイする必要があるリソースについては、アカウントと OU を追加または削除できます。パッケージフォルダ内のテンプレートを追加または変更

したり、独自のフォルダを作成したり、テンプレートまたは manifest.yaml ファイル内のフォルダを参照したりできます。

このセクションでは、独自のカスタマイズを構築する際の 2 つの主要部分について説明します。

- サービスコントロールポリシー用に独自の設定パッケージをセットアップする方法
- AWS CloudFormation スタックセット用に独自の設定パッケージを設定する方法

SCPsまたは RCPs の設定パッケージを設定する

このセクションでは、サービスコントロールポリシー (SCPs) またはリソースコントロールポリシー (RCPs) の設定パッケージを作成する方法について説明します。このプロセスの 2 つの主要部分は、(1) マニフェストファイルの準備、(2) フォルダ構造の準備です。

ステップ 1: manifest.yaml ファイルを編集する

サンプル manifest.yaml ファイルを出発点として使用します。必要な設定をすべて入力します。resource_file および deployment_targets の詳細を追加します。

次のスニペットは、デフォルトマニフェストファイルを示しています。

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

resources: []
```

region の値は、デプロイ時に自動的に追加されます。これは CfCT をデプロイしたリージョンと一致する必要があります。このリージョンは AWS Control Tower リージョンと同じものにする必要があります。

Amazon S3 バケットに保存されている zip パッケージの example-configurationフォルダにカスタム SCP または RCP を追加するには、 example-manifest.yaml ファイルを開いて編集を開始します。

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
```

```
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

次のスニペットは、カスタマイズされたマニフェストファイルの例を示しています。1 回の変更で複数のポリシーを追加できます。

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

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

ステップ 2: フォルダ構造を作成する

リソースファイルに Simple Storage Service (Amazon S3) URL を使用していて、キーと値のペアの parameters を使用している場合、このステップを省略できます。

マニフェストファイルは JSON ファイルを参照するため、マニフェストをサポートするには SCP ポリシーまたは RCP ポリシーを JSON 形式で含める必要があります。マニフェストファイルに指定されたパス情報とファイルパスが一致していることを確認します。

- ポリシー JSON ファイルには、OUs にデプロイする SCPs または RCPs が含まれています。

次のスニペットは、サンプルマニフェストファイルのフォルダ構造を示しています。

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

以下のスニペットは、block-s3-public.json ポリシーファイルの一例です。

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

AWS CloudFormation StackSets の設定パッケージを設定する

このセクションでは、 AWS CloudFormation StackSets の設定パッケージを設定する方法について説明します。このプロセスの 2 つの主要部分は、(1) マニフェストファイルの準備、(2) フォルダ構造の更新です。

ステップ 1: 既存のマニフェストファイルを編集する

以前に編集したマニフェストファイルに新しい AWS CloudFormation StackSets 情報を追加します。

確認のためだけに、次のスニペットには、SCPs または RCPs の設定パッケージをセットアップするために前に示したものと同じカスタマイズされたマニフェストファイルが含まれています。このファイルをさらに編集して、リソースの詳細を含めることができるようになりました。

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

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
```

```
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

次のスニペットは、resources の詳細を含む編集済みのサンプルマニフェストファイルを示します。resources の順序は、resources の依存関係を作成するための実行順序を決定します。次のサンプルマニフェストファイルをビジネス要件に応じて編集できます。

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
```

```
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

次の例は、マニフェストファイルに複数の AWS CloudFormation リソースを追加できることを示しています。

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

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

ステップ 2: フォルダ構造を更新する

フォルダ構造を更新するときに、マニフェストファイルにあるすべてのサポート AWS CloudFormation テンプレートファイルと SCP または RCP ポリシーファイルを含めることができます。ファイルパスがマニフェストファイルで指定したものと一致していることを確認します。

- テンプレートファイルには、OUs とアカウントにデプロイされる AWS リソースが含まれています。
- policy ファイルには、テンプレートファイルで使用される入力パラメータが含まれます。

次の例は、ステップ 1 で作成したサンプルマニフェストファイルのフォルダ構造を示しています。

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

「alfred」ヘルパーと AWS CloudFormation パラメータファイル

CfCT には、 AWS CloudFormation テンプレートで定義されている SSM パラメータストアキーの値を取得するための alfred ヘルパーと呼ばれるメカニズムが用意されています。alfred ヘルパーを使用すると、 AWS CloudFormation テンプレートを更新せずに SSM パラメータストアに保存されている値を使用できます。詳細については、「 ユーザーガイド」の AWS CloudFormation 「 テンプレートとは」を参照してください。 AWS CloudFormation

> **Important**
>
> alfred ヘルパーには 2 つの制限があります。パラメータは、AWS Control Tower 管理アカウントのホームリージョンでのみ使用できます。ベストプラクティスとして、スタックインスタンスごとに変わらない値を使用することを検討してください。「alfred」ヘルパーがパラメーターを取得すると、変数をエクスポートするスタックセットからランダムなスタックインスタンスを選択します。

例

2 つの AWS CloudFormation スタックセットがあるとします。スタックセット 1 には 1 つのスタックインスタンスがあり、1 つのリージョンの 1 つのアカウントにデプロイされます。アベイ

ラビリティーゾーンに Amazon VPC とサブネットが作成されます。VPC ID と subnet ID をパラメータ値としてスタックセット 2 に渡す必要があります。VPC ID と subnet ID をスタックセット 2 に渡す前に、AWS:::SSM::Parameter を使用して VPC ID と subnet ID をスタックセット 1 に保存する必要があります。詳細については、AWS CloudFormation ユーザーガイドの AWS:::SSM::Parameterを参照してください。

AWS CloudFormation スタックセット 1:

次のスニペットでは、alfred ヘルパーは、パラメータストアから VPC ID と subnet ID の値を取得し、それらの値を StackSet ステートマシンに入力として渡すことができます。

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

AWS CloudFormation スタックセット 2:

スニペットには、 AWS CloudFormation スタック 2 manifest.yaml ファイルで指定されたパラメータが表示されます。

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation スタックセット 2.1:

このスニペットは、ユーザーが CommaDelimitedList 型のパラメータをサポートする alfred_ssm プロパティを一覧表示できることを示しています。詳細については、AWS CloudFormation ユーザーガイドの Parameters を参照してください。

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

カスタマイズパッケージの JSON スキーマ

CfCT のカスタマイズパッケージの JSON スキーマは、GitHub のソースコードリポジトリにあります。このスキーマはほとんどの開発ツールで使用でき、独自の manifest.yaml ファイルを構築する際のエラーを減らすのに役立ちます。

マニフェストのバージョンのアップグレード

AWS Control Tower のカスタマイズ (CfCT) の最新バージョンについては、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。

Warning

AWS Control Tower のカスタマイズ (CfCT) のバージョン 2.2.0 では、関連する AWS サービス API に合わせてマニフェストスキーマ (バージョン 2021-03-15) が導入されました。APIs マニフェストスキーマを使用すると、1 つの manifest.yaml ファイルが、分離された DevOps ワークフローを通じてサポートされているリソース (AWS CloudFormation テンプレート、SCPs、RCPs) を管理できます。
マニフェストスキーマのバージョン 2020-01-01 を、バージョン 2021-03-15 以降に更新することを強くお勧めします。
CfCT は、引き続き manifest.yaml ファイルのバージョン 2021-03-15 および 2020-01-01 をサポートします。既存の設定を変更する必要はありません。ただし、バージョン 2020-01-01 はサポート終了になります。バージョン 2020-01-01 に更新プログラムを提供し

たり、拡張機能を追加したりすることはありません。ルート OU およびネストされた OU 機能は、バージョン 2020-01-01 ではサポートされていません。

マニフェストバージョン 2021-03-15 で廃止されたプロパティ:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

必須のアップグレードステップ

マニフェストのスキーマバージョンを 2021-03-15 にアップグレードするときに、ファイルを更新するために必要な変更は次のとおりです。次のセクションでは、移行時の必須の推奨および推奨される変更について概説します。

組織ポリシー

1. 新しいプロパティリソースの organization_policies で SCPs または RCPs を移動します。
2. policy_file プロパティを新しいプロパティ resource_file に変更します。
3. apply_to_accounts_in_ou を新しいプロパティ deployment_targets に変更します。OU リストは、サブプロパティ [organizational_units] で定義する必要があります。accounts サブプロパティは、組織ポリシーではサポートされていません。
4. 値 scp または rcp を持つ新しいプロパティ deploy_method を追加します。

AWS CloudFormation リソース

1. CloudFormation リソースを新しいプロパティ resources の下にある cloudformation_resources に移動します。
2. template_file プロパティを新しいプロパティ resource_file に変更します。
3. deploy_to_ou を新しいプロパティ deployment_targets に変更します。OU リストは、サブプロパティ [organizational_units] で定義する必要があります。

4. deploy_to_accounts を新しいプロパティ deployment_targets に変更します。アカウントリストは、サブプロパティ accounts で定義する必要があります。
5. ssm_parameters プロパティを新しいプロパティ export_outputs に変更します。

強く推奨されるアップグレードステップ

AWS CloudFormation パラメータ

1. parameter_file プロパティを新しいプロパティ parameters に変更します。
2. parameter_file プロパティの値にあるファイルパスを削除します。
3. 既存のパラメータ JSON ファイルのパラメータキーとパラメータ値を、parameters プロパティの新しいフォーマットにコピーします。この操作により、マニフェストファイルでこれらの値を管理することができます。

> **Note**
>
> parameter_file プロパティはマニフェストバージョン 2021-03-15 でサポートされています。

AWS Control Tower でのネットワーク

AWS Control Tower は、 を介したネットワークの基本サポートを提供しますVPCs。

AWS Control Tower のデフォルト設定または機能がニーズを満たVPCさない場合は、他の AWS サービスを使用して を設定できますVPC。VPCs および AWS Control Tower の操作方法の詳細については、「スケーラブルで安全なマルチVPC AWS ネットワークインフラストラクチャの構築」を参照してください。

関連トピック

- 既存の を持つアカウントを登録するときの AWS Control Tower の仕組みについてはVPCs、「」を参照してください で既存のアカウントを登録する VPCs。
- Account Factory では、AWSControl Tower を含むアカウントをプロビジョニングすることもVPC、 なしでアカウントをプロビジョニングすることもできますVPC。なしで AWS Control Tower を削除する方法、VPCまたは AWS Control Tower アカウントを設定する方法についてはVPC、「」を参照してください チュートリアル: なしで AWS Control Tower を設定する VPC。
- のアカウント設定を変更する方法についてはVPCs、アカウントの更新に関する Account Factory ドキュメントを参照してください。
- AWS Control Tower VPCsでのネットワークと の操作の詳細については、このユーザーガイドの関連情報ページのネットワークに関するセクションを参照してください。

VPCs AWS Control Tower の および AWS リージョン

アカウント作成の標準的な部分として、 は、AWSControl Tower で管理していないリージョンであっても、すべてのリージョンVPCで AWSデフォルト AWS を作成します。このデフォルトVPCは、プロビジョニングされたアカウント用に AWS Control Tower VPCが作成する とは異なりますが、非管理リージョンVPCの AWS デフォルトにはIAMユーザーがアクセスできる場合があります。

管理者は、リージョン拒否コントロールを有効にして、エンドユーザーが AWS Control Tower でサポートされているが管理対象リージョン外のリージョンVPCの に接続するアクセス許可を持たないようにできます。リージョン拒否コントロールを設定するには、[Landing zone settings] (ランディングゾーン設定) ページに移動し、[Modify settings] (設定を変更する) を選択します。

リージョン拒否コントロールは、管理対象外のほとんどの サービスへのAPI呼び出しをブロックします AWS リージョン。詳細については、「リクエスト AWS された に基づいて へのアクセスを拒否する」を参照してください AWS リージョン。

> **Note**
>
> リージョン拒否コントロールは、IAMユーザーが AWS Control Tower がサポートされていないリージョンVPCの AWS デフォルトに接続できないようにするものではありません。

オプションで、管理対象外のリージョンVPCsの AWS デフォルトを削除できます。リージョンVPCのデフォルトを一覧表示するには、次の例のようなCLIコマンドを使用できます。

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

AWS Control Tower と の概要 VPCs

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

- Account Factory でアカウントをプロビジョニングするときに AWS Control Tower によってVPC作成される は、 AWS デフォルトの とは異なりますVPC。
- AWS Control Tower がサポートされている AWS リージョンに新しいアカウントを設定すると、AWSControl Tower は自動的にデフォルトを削除し AWS VPC、AWSControl Tower によってVPC設定された新しい を設定します。
- 各 AWS Control Tower アカウントには、AWSControl Tower VPC によって作成されたアカウントが許可されます。アカウントは、アカウント制限内で追加の AWS VPCs を持つことができます。
- すべての AWS Control Tower VPCには、米国西部 (北カリフォルニア) リージョンを除くすべてのリージョンに 3 つのアベイラビリティーゾーンとus-west-1、 に 2 つのアベイラビリティーゾーンがありますus-west-1。デフォルトでは、各アベイラビリティーゾーンに 1 つのパブリックサブネットと 2 つのプライベートサブネットが割り当てられます。したがって、米国西部 (北カリフォルニア) を除くリージョンでは、各 AWS Control Tower にはデフォルトで 9 つのサブネットVPCが含まれ、3 つのアベイラビリティーゾーンに分割されます。米国西部 (北カリフォルニア) では、6 つのサブネットが 2 つのアベイラビリティーゾーンで分割されます。
- AWS Control Tower 内の各サブネットには、同じサイズの一意の範囲VPCが割り当てられます。
- 内のサブネットの数VPCは設定可能です。VPC サブネット設定を変更する方法の詳細については、Account Factory トピックを参照してください。
- IP アドレスは重複しないため、AWSControl Tower 内の 6 つまたは 9 つのサブネットは無制限に相互に通信VPCできます。

を使用する場合VPCs、AWSControl Tower はリージョンレベルで区別しません。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 サブネットは任意のリージョンに存在できます。

Notes (メモ)

> **VPC コストの管理**
>
> 新しいアカウントのプロビジョニング時にパブリックサブネットが有効になるように Account Factory VPC設定を設定すると、Account Factory はNATゲートウェイを作成する VPCように を設定します。Amazon による使用量に対して課金されますVPC。

> **VPC および コントロール設定**
>
> VPC インターネットアクセス設定を有効にして Account Factory アカウントをプロビジョニングすると、その Account Factory 設定は、お客様が管理する Amazon VPCインスタンスのインターネットアクセスの禁止コントロールを上書きします。新しくプロビジョニングされたアカウントのインターネットアクセスを有効にしないようにするには、Account Factory で設定を変更する必要があります。詳細については、「チュートリアル: なしで AWS Control Tower を設定するVPC」を参照してください。

CIDR および AWS Control Tower の VPCおよび ピアリング

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、AWSControl Tower 組織の全体的なCIDR範囲を選択するユーザーです。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。

CIDR の範囲を選択するとVPC、AWSControl Tower は 1918 RFC 年の仕様に従って IP アドレスの範囲を検証します。Account Factory では、以下の/16範囲で最大 のCIDRブロックを使用できます。

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10` (インターネットプロバイダーがこの範囲の使用を許可している場合のみ)

/16 区切り記号を使用すると、最大 65,536 個の IP アドレスを指定できます。

以下の範囲から有効な IP アドレスを割り当てることができます。

- `10.0.x.x to 10.255.x.x`
- `172.16.x.x – 172.31.x.x`
- `192.168.0.0 – 192.168.255.255` (IPs`192.168`範囲外なし)

指定した範囲がこれらの範囲外の場合、AWSControl Tower はエラーメッセージを表示します。

デフォルトのCIDR範囲は です`172.31.0.0/16`。

AWS Control Tower は、選択したCIDR範囲VPCを使用して を作成すると、組織単位 (OU) 内で作成するすべてのアカウントについて、すべての VPC に同じCIDR範囲を割り当てます。IP アドレスのデフォルトの重複により、この実装では最初は OU VPCs内の AWS Control Tower 間のピア接続が許可されません。

サブネット

各 内でVPC、AWSControl Tower は指定されたCIDR範囲を 9 つのサブネットに均等に分割します (米国西部 (北カリフォルニア) では 6 つのサブネットを除く)。VPC 重複するサブネットはありません。したがって、それらはすべて 内で相互に通信できますVPC。

つまり、デフォルトでVPCは、 内のサブネット通信は制限されません。必要に応じて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、許可されたトラフィックフローを定義するルールを使用してアクセスコントロールリストを設定することです。特定のインスタンス間のトラフィックを制御するには、セキュリティグループを使用します。AWS Control Tower でセキュリティグループとファイアウォールを設定する方法の詳細については、「チュートリアル: AWS Firewall Manager を使用して AWS Control Tower でセキュリティグループを設定する」を参照してください。

ピア接続

AWS Control Tower は、複数の 間の通信のピア接続を制限 VPC-to-VPCしませんVPCs。ただし、デフォルトでは、すべての AWS Control Tower VPCsのデフォルトCIDR範囲は同じです。ピアリングをサポートするには、IP アドレスが重複しないように Account Factory の設定でCIDR範囲を変更できます。

Account Factory の設定でCIDR範囲を変更すると、AWSControl Tower によって (Account Factory を使用して) 後で作成されるすべての新しいアカウントに新しいCIDR範囲が割り当てられます。古い

アカウントは更新されません。例えば、アカウントを作成し、CIDR範囲を変更して新しいアカウントを作成し、これら 2 つのアカウントVPCsに割り当てられた をピアリング接続できます。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。

必要なロールと許可

AWS Control Tower は、 IAM ロールを使用して リソースへのアクセスを管理します。

ロールの一般情報については、「User groups, roles, and permission sets」を参照してください。

アクセス許可について

- AWS Control Tower のIAMグループとそのアクセス許可の詳細については、IAMAWS「Control Tower の Identity Center グループ」を参照してください。
- アカウントのプロビジョニングに必要なアクセス許可の詳細については、「Permissions required for accounts」を参照してください。
- AWS Control Tower に必要なコンソールのアクセス許可については、AWS「Control Tower コンソールを使用するために必要なアクセス許可」を参照してください。

ロールについて

- プログラムによるアクセス用に設計されたアクセス許可を含むロールの作成方法については、「ロールの作成とアクセス許可の割り当て」、およびAWS「Control Tower 監査アカウントのプログラムによるロールと信頼関係」を参照してください。
- AWS Control Tower がアカウントの管理に使用するその他のロールについては、AWS「Control Tower で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」およびAWS「Control Tower での 管理ポリシー」を参照してください。
- AWS Control Tower と AWS Config ロールの詳細については、AWS「Control Tower ConfigRecorderRole」を参照してください。
- AWS Control Tower がアカウントの AWS Config 情報を集約するために使用するロールの詳細については、「How AWS Control Tower aggregates AWS Config rules in unmanaged OUs and accounts」を参照してください。
- ロールとアクセス許可を割り当てるときにリソースを保護する方法については、「ロールの信頼関係のオプション条件」、「オプションで AWS KMS キーを設定する」、「サービス間のなりすましの防止」を参照してください。
- IAM ロールを使用した AWS Control Tower の自動アカウントプロビジョニングの詳細については、IAM「ロールを使用した自動アカウントプロビジョニング」を参照してください。
- トピックを保護するポリシーを表示するには、 AWS Config SNS「トピック AWS Config SNSポリシー」を参照してください。

AWS Control Tower がロールと連携してアカウントを作成および管理する方法

一般的に、 ロールはアイデンティティとアクセス管理 (IAM) の一部です AWS。の IAMおよび ロールに関する一般的な情報については AWS、AWS IAM「 ユーザーガイド」の「 IAMロール」トピックを参照してください。

ロールとアカウントの作成

AWS Control Tower は、 `CreateAccount`APIの を呼び出してお客様のアカウントを作成します AWS Organizations。がこのアカウント AWS Organizations を作成すると、そのアカウント内にロールが作成されます。このロールは、 にパラメータを渡すことで AWS Control Tower が名前を付けますAPI。ロールの名前は `AWSControlTowerExecution` です。

AWS Control Tower は、Account Factory によって作成されたすべてのアカウントの`AWSControlTowerExecution`ロールを引き継ぎます。このロールを使用すると、AWSControl Tower はアカウントをベースライン化し、必須 (およびその他の有効な) コントロールを適用します。これにより、他のロールが作成されます。これらのロールは、次に AWS Configなどの他のサービスによって使用されます。

> **Note**
>
> アカウントのベースライニングとは、そのリソースを設定することです (Account Factory テンプレートを含む)。これはブループリントまたはコントロールと呼ばれることもあります。ベースライン作成プロセスでは、テンプレートのデプロイの一環として、アカウントの集中ロギングとセキュリティ監査ロールも設定されます。 AWSControl Tower のベースラインは、すべての登録済みアカウントに適用するロールに含まれています。

アカウントとリソースの詳細については、「AWS Control Tower AWS アカウント の について」を参照してください。

ロール AWSControlTowerExecution の説明

`AWSControlTowerExecution` ロールは、登録されたすべてのアカウントに存在する必要があります。これにより、AWSControl Tower は個々のアカウントを管理し、それらの情報を監査アカウントとログアーカイブアカウントにレポートできます。

AWSControlTowerExecution ロールは、次のように、いくつかの方法でアカウントに追加できます。

- Security OU のアカウント (コアアカウントとも呼ばれます) の場合、AWSControl Tower は Control AWS Tower の初回セットアップ時にロールを作成します。
- AWS Control Tower コンソールで作成された Account Factory アカウントの場合、AWSControl Tower はアカウントの作成時にこのロールを作成します。
- 1 つのアカウント登録の場合、ロールを手動で作成し、そのアカウントを AWS Control Tower に登録するようお客様に依頼します。
- ガバナンスを OU に拡張する場合、AWSControl Tower は StackSet-AWSControlTowerExecutionRole を使用して、その OU 内のすべてのアカウントにロールを作成します。

AWSControlTowerExecution ロールの目的:

- AWSControlTowerExecution では、スクリプトと Lambda 関数を使用して、アカウントを自動的に作成および登録できます。
- AWSControlTowerExecution では、各アカウントのすべてのログがロギングアカウントに送信されるよう、組織のロギングを設定できます。
- AWSControlTowerExecution では、個々のアカウントを AWS Control Tower に登録できます。最初に、そのアカウントに AWSControlTowerExecution ロールを追加する必要があります。ロールの追加手順については、「必要なIAMロールを既存の に手動で追加 AWS アカウントして登録する」を参照してください。

AWSControlTowerExecution ロールと の連携方法OUs :

このAWSControlTowerExecutionロールにより、選択した AWS Control Tower コントロールが、組織内の各 OU 内の個々のアカウントと、AWSControl Tower で作成するすべての新しいアカウントに自動的に適用されます。結果として、以下のようになります。

- AWS Control Tower コントロールによって具体化される監査機能と ログ記録機能に基づいて、コンプライアンスレポートとセキュリティレポートをより簡単に提供できます。
- セキュリティチームとコンプライアンスチームは、すべての要件が満たされていること、組織ドリフトが発生していないことを確認できます。

ドリフトの詳細については、AWS「Control Tower でドリフトを検出して解決する」を参照してください。

つまり、AWSControlTowerExecution ロールとその関連ポリシーを使って、組織全体のセキュリティとコンプライアンスを柔軟に管理できるということです。したがって、セキュリティまたはプロトコルの違反が発生する可能性が低くなります。

ロールの信頼関係のオプションの条件

ロールの信頼ポリシーに条件を課して、AWSControl Tower の特定のロールとやり取りするアカウントとリソースを制限できます。AWSControlTowerAdmin ロールは幅広いアクセスを許可するため、このロールへのアクセスを制限することを強くお勧めします。

攻撃者がリソースにアクセスできないようにするには、AWSControl Tower の信頼ポリシーを手動で編集して、ポリシーステートメントに少なくとも 1 つの aws:SourceArnまたは aws:SourceAccount条件を追加します。セキュリティのベストプラクティスとして、aws:SourceArn 条件を追加することを強くお勧めします。これは aws:SourceAccount より具体的であり、特定のアカウントと特定のリソースへのアクセスを制限するためです。

リソースARNの全体がわからない場合、または複数のリソースを指定する場合は、 の不明な部分にワイルドカード (*) で aws:SourceArn条件を使用できますARN。例えば、arn:aws:controltower:*:123456789012:* は、リージョンを指定しない場合に機能します。

次の例は、IAMロール信頼ポリシーで aws:SourceArnIAM条件を使用する方法を示しています。AWS Control Tower サービスプリンシパルがロールを操作するため、AWSControlTowerAdminロールの信頼関係に 条件を追加します。

この例に示すように、ソースは次の形式ARNです。
arn:aws:controltower:*${HOME_REGION}*:*${CUSTOMER_AWSACCOUNT_id}*:*

文字列 ${HOME_REGION} および ${CUSTOMER_AWSACCOUNT_id} を、自身のホームリージョンと呼び出しアカウントのアカウント ID で置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

この例では、 としてARN指定されたソースarn:aws:controltower:us-west-2:012345678901:*が、 sts:AssumeRoleアクションの実行をARN許可されている唯一のです。つまり、 us-west-2リージョン012345678901でアカウント ID にサインインできるユーザーのみが、 として指定された AWS Control Tower サービスのこの特定のロールと信頼関係を必要とするアクションを実行できますcontroltower.amazonaws.com。

次の例は、ロールの信頼ポリシーに適用される aws:SourceAccount 条件と aws:SourceArn 条件を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
```

```
    }
  ]
}
```

この例は、aws:SourceAccount 条件ステートメントが追加された、aws:SourceArn 条件ステートメントを示しています。詳細については、「クロスサービス偽装の防止」を参照してください。

AWS Control Tower のアクセス許可ポリシーの一般的な情報については、「」を参照してくださいリソースへのアクセスの管理。

推奨事項:

AWS Control Tower が作成するロールに条件を追加することをお勧めします。これらのロールは他の AWSサービスによって直接引き受けられるためです。詳細については、このセクションで前述した AWSControlTowerAdminの例を参照してください。 AWS Config レコーダーロールの場合は、aws:SourceArn条件を追加し、Config レコーダーを許可されたソース ARNとして指定することをお勧めしますARN。

などのロールAWSControlTowerExecutionや、すべてのマネージドアカウントの AWS Control Tower Audit アカウントが引き受けることができるその他のプログラムロールについては、これらのロールの信頼ポリシーに aws:PrincipalOrgID条件を追加することをお勧めします。これにより、リソースにアクセスするプリンシパルが正しい AWS 組織のアカウントに属していることを検証します。aws:SourceArn 条件ステートメントは期待どおりに機能しないため、追加しないでください。

> **Note**
>
> ドリフトの場合、特定の状況下で AWS Control Tower ロールがリセットされる可能性があります。ロールをカスタマイズしている場合は、ロールを定期的に再確認することをお勧めします。

AWS Control Tower がアンマネージド型アカウントOUsとアカウントで AWS Config ルールを集約する方法

AWS Control Tower 管理アカウントは、外部 AWS Config ルールの検出に役立つ組織レベルのアグリゲータを作成します。これにより、AWSControl Tower は管理対象外のアカウントにアクセスする必要がなくなります。AWS Control Tower コンソールには、特定のアカウントに対して外部で作成

された AWS Config ルールの数が表示されます。これらの外部ルールの詳細は、[アカウントの詳細] ページの [外部の Config ルールのコンプライアンス] タブで確認できます。

アグリゲータを作成するために、AWSControl Tower は組織を記述し、その下にあるアカウントを一覧表示するために必要なアクセス許可を持つロールを追加します。AWSControlTowerConfigAggregatorRoleForOrganizations ロールには、AWSConfigRoleForOrganizations マネージドポリシーと、config.amazonaws.com との信頼関係が必要です。

ロールにアタッチされたIAMポリシー (JSON アーティファクト) は次のとおりです。

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

AWSControlTowerConfigAggregatorRoleForOrganizations の信頼関係は次のとおりです。

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

管理アカウントにこの機能をデプロイするには、 AWS Config アグリゲータの作成時にAWSControlTowerAdminロールAWSControlTowerServiceRolePolicyによって使用される管理ポリシー に次のアクセス許可が追加されます。

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

新しいリソース、AWSControlTowerConfigAggregatorRoleForOrganizations および aws-controltower-ConfigAggregatorForOrganizations が作成されました。

準備ができたら、アカウントを個別に登録するか、OU を登録してグループとしてアカウントを登録することができます。アカウントを登録すると、 でルールを作成すると AWS Config、AWSControl Tower は新しいルールを検出します。アグリゲータは外部ルールの数を表示し、アカウントの各外部ルールの詳細を表示できる AWS Config コンソールへのリンクを提供します。コンソールと AWS Control Tower コンソールの情報 AWS Config を使用して、アカウントに対して適切なコントロールが有効になっているかどうかを確認します。

AWS Control Tower 監査アカウントのプログラムによるロールと信頼関係

監査アカウントにサインインし、他のアカウントをプログラムで確認するロールを引き受けることができます。監査アカウントでは、他のアカウントに手動でログインすることはできません。

監査アカウントは、 AWS Lambda 関数にのみ付与される一部のロールを使用して、他のアカウントへのプログラムによるアクセスを許可します。セキュリティ上の理由から、これらのロールには他のロールとの信頼関係があります。つまり、ロールを利用できる条件が厳密に定義されていることを意味します。

AWS Control Tower スタックは、監査アカウントにこれらのプログラムのみのクロスアカウントIAMロールStackSet-AWSControlTowerBP-BASELINE-ROLESを作成します。

- aws-controltower-AdministratorExecutionRole
- aws-controltower-ReadOnlyExecutionRole

AWS Control Tower スタックは、監査アカウントにこれらのプログラムのみのクロスアカウントIAMロールStackSet-AWSControlTowerSecurityResourcesを作成します。

- aws-controltower-AuditAdministratorRole
- aws-controltower-AuditReadOnlyRole

ReadOnlyExecutionRole: このロールは、監査アカウントが、組織全体の Amazon S3 バケット内のオブジェクトを読み取ることを許可する点に注意してください (メタデータアクセスのみを許可する SecurityAudit ポリシーとは対照的です)。

aws-controltower-AdministratorExecutionRole：

- 管理者権限があります
- コンソールから引き受けることはできません
- 監査アカウントのロール (aws-controltower-AuditAdministratorRole) でのみ引き受けることができます

次のアーティファクトは、aws-controltower-AdministratorExecutionRole の信頼関係を示しています。プレースホルダー番号 012345678901 は、監査アカウントの Audit_acct_ID 番号に置き換えられます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-AuditAdministratorRole：

- AWS Lambda サービスのみが引き受けることができます
- 文字列 log で始まる名前を持つ Simple Storage Service (Amazon S3) オブジェクトに対して読み取り (Get) 操作および書き込み (Put) 操作を実行する許可があります

アタッチされるポリシー:

1. AWSLambdaExecute AWS 管理ポリシー

2. AssumeRole-aws-controltower-AuditAdministratorRole – インラインポリシー – AWS Control Tower によって作成され、アーティファクトは次のようになります。

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

次のアーティファクトは、aws-controltower-AuditAdministratorRole の信頼関係を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-ReadOnlyExecutionRole：

- コンソールから引き受けることはできません
- 監査アカウントの別のロール (AuditReadOnlyRole) でのみ引き受けることができます

次のアーティファクトは、aws-controltower-ReadOnlyExecutionRole の信頼関係を示しています。プレースホルダー番号 012345678901 は、監査アカウントの Audit_acct_ID 番号に置き換えられます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-AuditReadOnlyRole：

- AWS Lambda サービスのみが引き受けることができます

- 文字列 log で始まる名前を持つ Simple Storage Service (Amazon S3) オブジェクトに対して読み取り (Get) 操作および書き込み (Put) 操作を実行する許可があります

アタッチされるポリシー:

1. AWSLambdaExecute AWS 管理ポリシー

2. AssumeRole-aws-controltower-AuditReadOnlyRole – インラインポリシー – AWS Control Tower によって作成され、アーティファクトは次のようになります。

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

次のアーティファクトは、aws-controltower-AuditAdministratorRole の信頼関係を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

IAM ロールを使用した自動アカウントプロビジョニング

Account Factory アカウントをより自動化された方法で設定するには、AWSControl Tower 管理アカウントに Lambda 関数を作成します。これにより、メンバーアカウントのAWSControlTowerExecutionロールが引き受けられます。次に、管理アカウントが、ロールを使用して、各メンバーアカウントで必要な設定手順を実行します。

ただし、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アイデンティティには AWSServiceCatalogEndUserFullAccess に加え、次の IAM アクセス許可ポリシーが必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
```

```
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

アクセス許可 `sso:GetPeregrineStatus`、`sso:ProvisionApplicationInstanceForAWSAccount`、`sso:Provis` および `sso:ProvisionSAMLProvide`は、AWSControl Tower Account Factory が Identity Center と AWS IAMやり取りするために必要です。

AWS Control Tower のリソース

- AWS Control Tower のリソース所有権に関する一般情報については、「AWS Control Tower リソースへのアクセス許可の管理の概要」を参照してください。
- AWS Control Tower が共有アカウントに作成するリソースの詳細については、「共有アカウントについて」を参照してください。
- AWS Control Tower が Account Factory を通じてアカウントをプロビジョニングするときに作成するリソースの詳細については、「Account Factory のリソースに関する考慮事項」を参照してください。
- AWS Control Tower で定義されている AWS リソースタイプの詳細を表示し、AWS Control Tower APIs「AWS Control Tower リソースタイプのリファレンス」を参照してください。 AWS CloudFormation

AWS リージョンと AWS Control Tower の連携方法

現在、AWSControl Tower は次の AWS リージョンでサポートされています。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (オレゴン)
- カナダ (中部)
- アジアパシフィック (シドニー)
- アジアパシフィック (シンガポール)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ストックホルム)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (東京)
- 欧州 (パリ)
- 南米 (サンパウロ)
- 米国西部 (北カリフォルニア)
- アジアパシフィック (香港)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (大阪)
- 欧州 (ミラノ)
- アフリカ (ケープタウン)
- 中東 (バーレーン)
- イスラエル (テルアビブ)
- 中東 (UAE)
- 欧州 (スペイン)
- アジアパシフィック (ハイデラバード)
- 欧州 (チューリッヒ)

- アジアパシフィック (メルボルン)
- カナダ西部 (カルガリー)
- マレーシア (クアラルンプール)

ホームリージョンについて

ランディングゾーンを作成すると、 AWS マネジメントコンソールへのアクセスに使用しているリージョンが AWS Control Tower のホーム AWS リージョンになります。作成プロセス中に、一部のリソースがホームリージョンにプロビジョニングされます。OUs や AWS アカウントなどの他のリソースはグローバルです。

いったん選択したホームリージョンは変更できません。

コントロールとリージョン

現在、予防コントロールはすべてグローバルに使用できます。ただし、検出コントロールとプロアクティブコントロールは、AWSControl Tower がサポートされているリージョンでのみ機能します。新しいリージョンで AWS Control Tower をアクティブ化する際のコントロールの動作の詳細については、「」を参照してくださいAWS Control Tower リージョンを設定する。

AWS Control Tower リージョンを設定する

このセクションでは、AWSControl Tower ランディングゾーンを新しい AWS リージョンに拡張したり、ランディングゾーン設定からリージョンを削除したりする場合に想定される動作について説明します。通常、このアクションは AWS Control Tower コンソールの更新機能を使用して実行されます。

> **Note**
>
> AWS Control Tower ランディングゾーンを、ワークロードの実行を必要としないリージョンに AWS 拡張しないことをお勧めします。リージョンからオプトアウトしても、そのリージョンにリソースをデプロイすることはできませんが、それらのリソースは AWS Control Tower ガバナンスの外部に残ります。

新しいリージョンの設定中に、AWSControl Tower はランディングゾーンを更新します。つまり、ランディングゾーンのベースラインを設定します。

- 新たに選択されたすべてのリージョンでアクティブに動作します。

- 選択解除されたリージョンのリソースの管理を停止します。

AWS Control Tower によって管理される組織単位 (OUs) 内の個々のアカウントは、このランディングゾーン更新プロセスの一環として更新されません。したがって、 を再登録してアカウントを更新する必要がありますOUs。

AWS Control Tower リージョンを設定するときは、次の推奨事項と制限事項に注意してください。

- AWS リソースまたはワークロードをホストする予定のリージョンを選択します。
- リージョンからオプトアウトしても、そのリージョンにリソースをデプロイすることはできませんが、それらのリソースは AWS Control Tower ガバナンスの外部に残ります。

ランディングゾーンを新しいリージョンに設定すると、AWSControl Tower の検出コントロールは次のルールに従います。

- 既存のものに変更はありません。既存の OUsリージョンの既存の アカウントでは、検出および予防のコントロール動作は変更されません。
- 更新されていない既存のOUs包含アカウントには、新しい検出コントロールを適用できません。AWS Control Tower ランディングゾーンを新しい リージョン (ランディングゾーンを更新) に設定したら、それらの OUsとアカウントで新しい検出コントロールを有効にするOUs前に、既存の の既存のアカウントを更新する必要があります。
- 既存の検出コントロールは、アカウントを更新するとすぐに新しく設定したリージョンで機能し始めます。AWS Control Tower ランディングゾーンを更新して新しいリージョンを設定し、アカウントを更新すると、OU で既に有効になっている検出コントロールは、新しく設定されたリージョンでそのアカウントでの作業を開始します。

AWS Control Tower リージョンを設定する

1. で AWS Control Tower コンソールにサインインする https://console.aws.amazon.com/controltower
2. 左ペインのナビゲーションメニューで、[Landing zone settings] (ランディングゾーン設定) を選択します。
3. [Landing zone settings] (ランディングゾーン設定) ページの [Details] (詳細) セクションで、右上の [Modify settings] (設定を変更する) ボタンを選択します。ランディングゾーン更新ワークフローに移動します。新しいリージョンを管理したり、リージョンを管理対象から除外したりするには、最新のランディングゾーンバージョンに更新する必要があるためです。

4. ガバナンスの追加 AWS リージョンで、管理するリージョンを検索します (または、管理を停止します) 。[State] (状態) 列に、現在管理対象となっているリージョンと管理対象になっていないリージョンが表示されます。
5. 追加で管理対象とする各リージョンのチェックボックスをオンにします。管理対象から除外する各リージョンのチェックボックスをオフにします。

> **Note**
>
> リージョンを管理しないことを選択した場合でも、そのリージョンにリソースをデプロイすることはできますが、それらのリソースは AWS Control Tower ガバナンスの外部に残ります。

6. 残りのワークフローを完了し、[Update landing zone] (ランディングゾーンの更新) を選択します。
7. ランディングゾーンのセットアップが完了したら、 を再登録OUsして新しいリージョンのアカウントを更新します。詳細については、「AWS Control Tower OUsとアカウントを更新するタイミング」を参照してください。

新しいリージョンを設定した後に個々のアカウントをプロビジョニングまたは更新する別の方法は、Service Catalog のAPIフレームワークと AWS CLIを使用してバッチプロセスでアカウントを更新することです。詳細については、「自動化によるアカウントのプロビジョニングと更新」を参照してください。

リージョンを設定する際は混合ガバナンスを避ける

AWS Control Tower ガバナンスを新しい に拡張した後、およびリージョンから AWS Control Tower ガバナンスを削除した後 AWS リージョン、OU 内のすべてのアカウントを更新することが重要です。

混合ガバナンスは、OU を管理するコントロールが OU 内の各アカウントを管理するコントロールと完全に一致しない場合に発生する可能性のある望ましくない状況です。AWS Control Tower がガバナンスを新しい に拡張した後、またはガバナンスを削除した後にアカウントが更新されない場合 AWS リージョン、混合ガバナンスが OU で発生します。

このような状況では、OU 内の特定のアカウントが、OU 内の他のアカウントと比較されたり、ランディングゾーンの全体的なガバナンス体制と比較されたりすると、リージョンごとに異なるコントロールが適用されることがあります。

ガバナンスが混在している OU では、新しいアカウントをプロビジョニングすると、その新しいアカウントには、ランディングゾーンと同じ (更新された) リージョンと OU のガバナンス体制が適用されます。ただし、まだ更新されていない既存のアカウントには、更新されたリージョンガバナンス体制は適用されません。

一般的に、混合ガバナンスは AWS Control Tower コンソールで矛盾または不正確なステータスインジケータを作成する可能性があります。例えば、混合ガバナンスでは、オプトインリージョンは、まだ更新されていないアカウントの登録済み にOUs管理対象外ステータスで表示されます。

> **Note**
>
> AWS Control Tower では、混合ガバナンスの状態の間はコントロールを有効にできません。

混合ガバナンスにおけるコントロールの動作

- 混合ガバナンス中、AWSControl Tower は、OU の一部のアカウントが更新されていないため、OU が既に管理対象と表示しているリージョンで、 AWS Config ルールに基づくコントロール (検出コントロール) を一貫してデプロイすることはできません。FAILED_TO_ENABLE エラーメッセージが表示されることがあります。
- 混合ガバナンス中に、OU 内のアカウントがまだ更新されていないときにランディングゾーンのガバナンスをオプトインリージョンに拡張すると、OU でのEnableControlAPIオペレーションは検出コントロールとプロアクティブコントロールで失敗します。OU 内の更新されていないメンバーアカウントはまだそれらのリージョンにオプトインされていないため、FAILED_TO_ENABLE エラーメッセージが表示されます。
- 混合ガバナンス中、Security Hub サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールは、ランディングゾーン設定と更新されていないアカウントが一致していないリージョンでは、コンプライアンスを正確に報告できません。
- 混合ガバナンスでは、 SCPベースのコントロール (予防コントロール) の動作は変わりません。これは、すべての管理対象リージョンの OU 内のすべてのアカウントに均一に適用されます。

> **Note**
>
> 混合ガバナンスはドリフトとは異なりますし、ドリフトとして報告されません。

混合ガバナンスを修復するには

- コンソールの [組織] ページに [更新可能] ステータスが表示されている OU 内のアカウントごとに [アカウントの更新] を選択します。
- Organizations ページで OU の再登録 を選択します。これにより、OU 内のすべてのアカウントが 1000 OUs未満の に対して自動的に更新されます。

AWS オプトインリージョンをアクティブ化する際の注意事項

ほとんどの AWS リージョン は に対してデフォルトでアクティブですが AWS アカウント、特定のリージョンは手動で選択した場合にのみアクティブになります。このドキュメントでは、これらのリージョンをオプトインリージョンと呼んでいます。これとは対照的に、 が作成されるとすぐに、デフォルトでアクティブなリージョン AWS アカウント は商用リージョン、または単にリージョンと呼ばれます。

オプトインという用語には歴史的な根拠があります。2019 年 3 月 20 日以降に導入された AWS リージョン はすべてオプトインリージョンとみなされます。オプトインリージョンは、オプトインリージョンでアクティブなアカウントを介したIAMデータの共有に関して、商用リージョンよりもセキュリティ要件が高くなります。IAM サービスを通じて管理されるすべてのデータは、ユーザー、グループ、ロール、ポリシー、ID プロバイダー、関連するデータ (X.509 署名証明書やコンテキスト固有の認証情報など) 、パスワードポリシーやアカウントエイリアスなどのアカウントレベルの設定を含む ID データと見なされます。

オプトインリージョンは、ランディングゾーン設定時に選択することで自動的にアクティブ化できます。ランディングゾーンは、選択したすべてのリージョンで有効になります。

AWS Control Tower のホームリージョンとしてオプトインリージョンを選択する場合は、まず「 AWS マネジメントコンソールにサインインしたときにリージョンを有効にする」の手順に従ってアクティブ化します。オプトインリージョンから既存のログアーカイブアカウントと監査アカウントを取得するには、まずそのリージョンを手動でアクティブ化します。

AWS オプトインリージョンには、AWSControl Tower が利用可能な複数のリージョンが含まれます。

- アジアパシフィック (香港) リージョン、ap-east-1
- アジアパシフィック (ジャカルタ) リージョン、ap-southeast-3
- 欧州 (ミラノ) リージョン、eu-south-1
- アフリカ (ケープタウン) リージョン、af-south-1

- 中東 (バーレーン) リージョン、me-south-1
- イスラエル (テルアビブ)、il-central-1
- 中東 (UAE) リージョン、me-central-1
- 欧州 (スペイン) リージョン、eu-south-2
- アジアパシフィック (ハイデラバード) リージョン、ap-south-2
- 欧州 (チューリッヒ) リージョン、eu-central-2
- アジアパシフィック (メルボルン) リージョン、ap-southeast-4
- カナダ西部 (カルガリー) リージョン、ca-west-1

AWS Control Tower には、オプトインリージョンと商用リージョンで動作が異なるコントロールがいくつかあります。詳細については、「コントロールの制限事項」を参照してください。オプトインリージョンにワークロードをデプロイする際に留意すべき点をいくつか紹介します。

> **管理かアクティブ化か？**
>
> リージョンの管理は、AWSコントロールをリージョンに適用できるように Control Tower コンソールから選択できるアクションであることに注意してください。オプトインリージョンをアクティブ化または非アクティブ化することは、 AWS コンソールで選択できるもう 1 つのアクションです。これにより、リージョンがアカウントで開かれ、そのリージョンにリソースとワークロードをデプロイできるようになります。

動作に関する注意事項

- オプトインリージョンを管理する場合は、ワークロードの障害につながる可能性があるため、管理されたオプトインリージョンを非アクティブ化 (オプトアウト) しないことをお勧めします。AWSControl Tower では、AWSControl Tower コンソール内から管理対象リージョンを非アクティブ化することはできませんが、 AWS 請求コンソールや などの AWS Control Tower 外のソースから管理対象リージョンを非アクティブ化しないでください AWS SDK。
- AWS Control Tower がガバナンスをオプトインリージョンに拡張すると、すべてのメンバーアカウントのリージョンに対してアクティブ化 (オプトイン) されます。ガバナンスからリージョンを削除しても、AWSControl Tower はメンバーアカウントのリージョンを非アクティブ化 (オプトアウト) しません。
- リージョンの選択解除中に、 AWS 請求コンソールや などの AWS Control Tower 外のソースからアカウントに対してそのリージョンが手動で非アクティブ化された場合、AWSControl Tower はオ

プトインリージョンからのリソースの削除をスキップします AWS SDK。非アクティブ化したリージョンからはリソースを削除することをお勧めします。そうしないと、それらのリソースに対して予想外の請求が発生する可能性があります。

- ランディングゾーンが廃止されると、AWSControl Tower はオプトインリージョンを含むすべての管理対象リージョンのリソースをクリーンアップします。ただし、AWSControl Tower はオプトインリージョンを非アクティブ化しません。廃止後の追加手順として、オプトインリージョンを非アクティブ化できます。
- ホームリージョンがオプトインリージョンで、既存のアカウントをログアーカイブアカウントと監査アカウントとして登録する場合、オプトインリージョンをランディングゾーンのホームリージョンとして選択する前に、オプトインリージョンを手動でアクティブ化する必要があります。リージョンを有効にするを参照
- AWS Control Tower がオプトインリージョンをホームリージョンとして設定されており、他のリージョンの AWS コンソールから AWS Control Tower サービスにアクセスしても、コンソールによって自動的にホームリージョンにリダイレクトされることはありません。
- 基盤となる APIには容量制限があり、リージョン、アカウント、サービス負荷の数によっては、レイテンシーが数分から数時間に増加する可能性があります。ベストプラクティスとして、ワークロードを実行する AWS リージョン にのみオプトインし、一度に 1 つのリージョンをオプトインします。

管理とアカウントに関する重要な制限

- オプトインリージョンを含む AWS Control Tower が利用可能な 16 以上の商用リージョンが管理されている場合、OU の登録時に組織単位 (OU) あたりのアカウント数の上限が削減されます。詳細については、「基盤となる AWS サービスに基づく制限事項」を参照してください。

リージョン拒否コントロールの設定

AWS Control Tower には 2 つのリージョン拒否コントロールがあります。1 つのコントロール GRREGIONDENY を有効にすると、ランディングゾーン全体に適用されます。別のコントロールはCTMULTISERVICEPV1、アクティブ化すると、OUs指定した特定の に適用できます。詳細については、「リクエストされた AWS に基づいて へのアクセスを拒否する AWS リージョン」および「OU に適用されたリージョン拒否コントロール」を参照してください。

ランディングゾーンのリージョン拒否コントロールに関する考慮事項

リージョン拒否コントロールである GRREGIONDENY は独特のコントロールです。特定の OU ではなく、ランディングゾーン全体に適用されるためです。リージョン拒否コントロールを設定するには、[Landing zone settings] (ランディングゾーン設定) ページに移動し、[Modify settings] (設定を変更する) を選択します。

- この設定は後で変更できます。
- 有効にすると、このコントロールは登録されているすべての に適用されますOUs。
- このコントロールを個々の に設定することはできませんOUs。

> **Note**
>
> リージョン拒否コントロールを有効にする前に、適用するリージョンに既存のリソースがないことを確認してください。コントロールを適用すると、以後そのリージョン内のリソースにアクセスできなくなるためです。このコントロールが有効になっている間は、拒否したリージョンにリソースをデプロイできません。

コントロールを有効にすると、階層OUs内のすべての登録済み最上位レベルに適用され、チェーン内のOUs下位に継承されます。コントロールを削除すると、すべての登録済み で削除されOUs、AWSControl Tower のすべての非管理リージョンは管理対象外ステータスのままになり、AWSControl Tower の可用性の外部にあるリージョンにリソースをデプロイできます。

> **例外**
>
> ホームリージョンへのアクセスを拒否することはできません。IAM や などの特定のグローバル AWS サービスは AWS Organizations、リージョン拒否コントロールから除外されます。詳細については、「Deny access to AWS based on the requested AWS リージョン」を参照してください。

- フルコントロール名: リクエスト AWS されたリージョン AWS に基づいて へのアクセスを拒否する
- コントロールの説明: 指定されたリージョンの外部にあるグローバルサービスおよびリージョンサービスでは、リストされていない操作へのアクセスを禁止します。
- これは、予防ガイダンスによる選択的コントロールです。

リージョン拒否コントロール のテンプレートを表示するにはSCP、AWS「Control Tower Control リファレンス」の「リクエストされた に基づいて へのアクセス AWS を拒否する AWS リージョン」を参照してください。AWS Control Tower SCPは for と似SCP AWS Organizationsていますが、同一ではありません。

リージョンサービスページでリージョンサービスエンドポイントを設定できます。

OU レベルでのリージョン拒否コントロールに関する考慮事項

OU レベルのリージョン拒否コントロールに関する主な考慮事項は、ランディングゾーンのリージョン拒否コントロールも有効になっている場合に、それがランディングゾーンのリージョン拒否コントロールとどのように相互作用するかを判断することです。詳細については、「Region deny control applied to the OU」を参照してください。

また、「Configure the Region deny control」を確認することもできます。

AWS Control Tower でのアカウントのプロビジョニングと管理

この章では、AWSControl Tower ランディングゾーンでメンバーアカウントをプロビジョニングおよび管理するための概要と手順について説明します。

また、既存の AWS アカウントを AWS Control Tower に登録するための概要と手順も含まれています。

AWS Control Tower のアカウントの詳細については、「」を参照してくださいAWS Control Tower AWS アカウント の について。AWS Control Tower に複数のアカウントを登録する方法については、「」を参照してくださいAWS Control Tower に既存の組織単位を登録する。

> **Note**
>
> プロビジョニング、更新、登録など、最大 5 つのアカウント関連のオペレーションを同時に実行できます。

プロビジョニングの方法

AWS Control Tower には、メンバーアカウントを作成および更新するためのいくつかの方法が用意されています。一部の方法は主にコンソールベースで、一部の方法は主に自動化されています。

概要

メンバーアカウントを作成するための標準的な方法は、Account Factory を使用することです。Account Factory は、Service Catalog に含まれるコンソールベースの製品です。ランディングゾーンがドリフト状態でない場合は、アカウントの作成をコンソールから新しいアカウントを追加する方法として使用し、アカウントを登録して既存の AWS アカウントを AWS Control Tower に登録できます。

Account Factory を使用すると、AWSControl Tower のデフォルト設定に依存することで、基本的なアカウントをプロビジョニングできます。また、特殊なユースケースの要件を満たすカスタマイズされたアカウントをプロビジョニングすることもできます。

Account Factory Customization (AFC) は、AWSControl Tower コンソールからカスタマイズされたアカウントをプロビジョニングする方法であり、アカウントのカスタマイズとデプロイを自動化しま

す。1 回限りのセットアップのためのいくつかのステップを実行すると、コンソールベースの自動プロビジョニングを使用できるようになり、スクリプトの作成やパイプラインの設定は不要となります。詳細については、「Account Factory Customization を使用してアカウントをカスタマイズする (AFC) 」を参照してください。

コンソールベースの方法:

- 基本アカウントまたはカスタマイズされたアカウントについては AWS Service Catalog、 の一部である Account Factory コンソールから。詳細と手順については、「Account Factory でのアカウントのプロビジョニングと管理」を参照してください。
- ランディングゾーンがドリフト状態でない場合は、AWSControl Tower 内のアカウント登録機能を使用します。「既存のアカウントを登録する」を参照してください。
- AWS Control Tower コンソールでは、Account Factory を使用して、最大 5 つのアカウントを同時に作成、更新、または登録できます。

自動化された方法:

- Lambda コード: AWS Control Tower ランディングゾーンの管理アカウントから、Lambda コードと適切なIAMロールを使用します。「 IAMロールによる自動アカウントプロビジョニング」を参照してください。
- Terraform: AWS Control Tower Account Factory for Terraform (AFT) から。Account Factory と GitOps モデルに依存して、アカウントのプロビジョニングと更新を自動化できます。「 AWS Control Tower Account Factory for Terraform (AFT) によるアカウントのプロビジョニング 」を参照してください。
- AWS Control Tower コンソールでの Account Factory のカスタマイズ : セットアップ手順の後、カスタマイズしたアカウントを今後プロビジョニングする際に、追加の設定やパイプラインのメンテナンスは必要ありません。アカウントは、ブループリントと呼ばれる AWS Service Catalog 製品によってプロビジョニングされます。設計図では、 AWS CloudFormation テンプレートまたは Terraform テンプレートを使用できます。

> **Note**
>
> AWS CloudFormation ブループリントは、複数のリージョンにリソースをデプロイできます。Terraform ブループリントでは、1 つのリージョンにのみリソースをデプロイできます。デフォルトでは、それはホームリージョンです。

AWS Control Tower がアカウントを作成するとどうなるか

AWS Control Tower の新しいアカウントは、AWSControl Tower、、および 間のやり取りによって作成 AWS Organizationsおよびプロビジョニングされます AWS Service Catalog。AWS Control Tower コンソール AWS アカウント を使用して既存の を登録する手順については、「」を参照してください既存のアカウントを登録する。

アカウント作成の舞台裏

1. AWS Control Tower Account Factory ページから、コンソールから直接、または Service Catalog `ProvisionProduct` を呼び出して AWS Service Catalog 、リクエストを開始しますAPI。
2. AWS Service Catalog は AWS Control Tower を呼び出します。
3. AWS Control Tower はワークフローを開始し、最初のステップとして `CreateAccount` を AWS Organizations 呼び出しますAPI。
4. がアカウント AWS Organizations を作成すると、AWSControl Tower はブループリントとコントロールを適用してプロビジョニングプロセスを完了します。
5. Service Catalog は Control Tower AWS のポーリングを継続し、プロビジョニングプロセスの完了をチェックします。
6. AWS Control Tower のワークフローが完了すると、Service Catalog はアカウントの状態を確定し、結果をユーザー (リクエスタ) に通知します。

アカウントに必要なアクセス許可

アカウントのプロビジョニングと更新の各方法に必要なアクセス許可については、それぞれのセクションで説明します。適切なユーザーグループの許可があれば、組織内のすべてのアカウントに対して標準化されたベースラインとネットワーク設定を指定できます。

> **Note**
>
> アカウントをプロビジョニングする場合、アカウントのリクエスタには必ず `CreateAccount` および `DescribeCreateAccountStatus` アクセス許可が必要です。このアクセス許可セットは Admin ロールの一部であり、リクエスタが Admin ロールを引き受けると自動的に付与されます。アカウントをプロビジョニングするアクセス許可を委任する場合、これらのアクセス許可をアカウントリクエスタに直接追加する必要がある場合があります。

Account Factory で AWS Control Tower コンソールからアカウントを作成する場合、`AWSServiceCatalogEndUserFullAccess`ポリシーが有効になっている IAM ユーザーと AWS Control Tower コンソールを使用するアクセス許可を使用してアカウントにサインインする必要があります。ルートユーザーとしてサインインすることはできません。

AWS Control Tower に必要なアクセス許可の一般的な情報については、「」を参照してくださいAWS Control Tower でアイデンティティベースのポリシー (IAM ポリシー) を使用する。AWS Control Tower のロールとアカウントの詳細については、「ロールとアカウント」を参照してください。

> **アカウントのセキュリティ**
>
> AWS Control Tower 管理アカウントとメンバーアカウントのセキュリティを保護するためのベストプラクティスに関するガイダンスは、 AWS Organizations ドキュメントに記載されています。
>
> - 管理アカウントのベストプラクティス
> - メンバーアカウントのベストプラクティス

AWS Control Tower AWS アカウント の について

AWS アカウント は、所有するすべてのリソースのコンテナです。これらのリソースには、アカウントによって受け入れられる AWS Identity and Access Management （ IAM) ID が含まれます。これにより、そのアカウントにアクセスできるユーザーを決定します。 ID IAM には、ユーザー、グループ、ロールなどが含まれます。AWS Control Tower での IAM、ユーザー、ロール、ポリシーの操作の詳細については、AWS「Control Tower での Identity and Access Management」を参照してください。

リソースとアカウントの作成時間

AWS Control Tower がアカウントを作成または登録すると、Account Factory テンプレートの形式のリソースやランディングゾーン内の他のリソースなど、アカウントの必要最小限のリソース設定がデプロイされます。これらのリソースには、IAMロール、 AWS CloudTrail 証跡、Service Catalog プロビジョニング済み製品、IAMIdentity Center ユーザーなどがあります。 AWSControl Tower は、新しいアカウントがメンバーアカウントになる予定の組織単位 (OU) のリソースを、コントロール設定で必要とされるとおりにデプロイします。

AWS Control Tower は、ユーザーに代わってこれらのリソースのデプロイを調整します。デプロイを完了するにはリソースごとに数分かかる場合があるため、アカウントを作成または登録する前に作業の合計時間を考慮してください。アカウントのリソースの管理の詳細については、「AWS Control Tower リソースの作成と変更に関するガイダンス」を参照してください。

既存のセキュリティアカウントまたはログアカウントを使用する際の考慮事項

をセキュリティアカウントまたはログ記録アカウント AWS アカウント として受け入れる前に、AWSControl Tower は Control Tower AWS の要件と競合するリソースがないかアカウントをチェックします。例えば、AWSControl Tower が必要とするのと同じ名前のログバケットがあるとします。また、AWSControl Tower は、アカウントがリソースをプロビジョニングできることを検証します。たとえば、 AWS Security Token Service （ AWS STS) が有効になっていること、アカウントが停止されていないこと、AWSControl Tower がアカウント内でリソースをプロビジョニングするアクセス許可を持っていることを確認します。

AWS Control Tower は、指定したログ記録アカウントとセキュリティアカウントの既存のリソースを削除しません。ただし、 AWS リージョン 拒否機能を有効にすると、リージョン拒否コントロールは拒否されたリージョンのリソースへのアクセスを禁止します。

アカウントの表示

組織ページには、AWSControl Tower の OU または登録ステータスに関係なく、組織内のすべてのOUsおよびアカウントが一覧表示されます。各アカウントが登録の前提条件を満たしている場合は、メンバーアカウントを個別に、または OU グループごとに AWS Control Tower に表示して登録できます。

[Organization] (組織) ページで特定のアカウントを表示するには、右上のドロップダウンメニューから [Accounts only] (アカウントのみ) を選択し、テーブルから目的のアカウントの名前を選択します。テーブルから親 OU の名前を選択して、その OU の [Details] (詳細) ページで、その OU 内のすべてのアカウントのリストを表示することもできます。

[組織] ページと [アカウントの詳細] ページで、アカウントの [状態] を表示できます。これは、次のいずれかです。

- 未登録 – アカウントは親 OU のメンバーですが、AWSControl Tower によって完全に管理されていません。親 OU が登録されている場合、アカウントはその登録済みの親 OU に設定された予防コントロールによって管理されますが、OU の検出コントロールはこのアカウントに適用されません。親 OU が未登録の場合は、どのコントロールもこのアカウントに適用されません。

- 登録中 – アカウントは AWS Control Tower によってガバナンスに移行されています。親 OU のコントロール設定に適合するようにアカウントが調整されます。このプロセスには、アカウントリソースごとに数分かかる場合があります。
- [Enrolled] (登録済み) - アカウントは、その親 OU 用に設定されたコントロールによって管理されています。AWS Control Tower によって完全に管理されます。
- 登録に失敗しました — アカウントを AWS Control Tower に登録できませんでした。詳細については、「登録の失敗の一般的な原因」を参照してください。
- Update available (更新が利用可能) – アカウントには利用可能な更新があります。この状態のアカウントは登録済みですが、環境に加えられた最近の変更を反映するには、アカウントを更新する必要があります。単一のアカウントを更新するには、アカウントの詳細ページに移動し、[Update account] (アカウントの更新) を選択します。

  1 つの OU の下にこの状態のアカウントが複数ある場合は、OU を再登録することを選択し、これらのアカウントをまとめて更新できます。

共有アカウントで作成されたリソース

このセクションでは、ランディングゾーンを設定するときに AWS Control Tower が共有アカウントで作成するリソースを示します。

メンバーアカウントリソースの詳細については、「Account Factory のリソースに関する考慮事項」を参照してください。

管理アカウントのリソース

ランディングゾーンを設定すると、管理アカウント内に次の AWS リソースが作成されます。

AWS のサービス	リソースタイプ	リソース名
AWS Organizations	アカウント	audit log archive
AWS Organizations	OUs	Security Sandbox

AWS のサービス	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 AWSControlTowerBP-BASELINE-CONFIG-MASTER（バージョン 2.6 以降）

AWS のサービス	リソースタイプ	リソース名
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL (3.0 以降ではデプロイされません)
		AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later)
		AWSControlTowerBP-BASELINE-CLOUDWATCH
		AWSControlTowerBP-BASELINE-CONFIG
		AWSControlTowerBP-BASELINE-ROLES
		AWSControlTowerBP-BASELINE-SERVICE-ROLES
		AWSControlTowerBP-SECURITY-TOPICS
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED
		AWSControlTowerLoggingResources

AWS のサービス	リソースタイプ	リソース名
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	製品	AWS Control Tower Account Factory
AWS Config	アグリゲータ	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	追跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch ログ	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 のサービス	リソースタイプ	リソース名
AWS IAM Identity Center	ディレクトリグループ	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	許可セット	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

> **Note**
>
> はランディングゾーンバージョン AWS CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL3.0` 以降ではデプロイされません。ただし、ランディングゾーンを更新するまでは、ランディングゾーンの以前のバージョンに引き続き存在します。

ログアーカイブアカウントのリソース

ランディングゾーンを設定すると、ログアーカイブアカウント内に次の AWS リソースが作成されます。

AWS のサービス	リソースタイプ	リソース名
AWS CloudFormation	スタック	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

AWS のサービス	リソースタイプ	リソース名
		StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
AWS Config	AWS Config ルール	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	追跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch ログ	/aws/lambda/aws-controltower-NotificationForwarder

AWS のサービス	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	ポリシー	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	トピック	aws-controltower-SecurityNotifications
AWS Lambda	アプリケーション	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	関数	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	バケット	aws-controltower-logs-* aws-controltower-s3-access-logs-*

アカウントリソースを監査する

ランディングゾーンを設定すると、監査アカウント内に次の AWS リソースが作成されます。

AWS のサービス	リソースタイプ	リソース名
AWS CloudFormation	スタック	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED- StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES-

AWS のサービス	リソースタイプ	リソース名
		StackSet-AWSControlTowerSecurityResources-*
AWS Config	アグリゲータ	aws-controltower-GuardrailsComplianceAggregator
AWS Config	AWS Config ルール	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	追跡	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch ログ	/aws/lambda/aws-controltower-NotificationForwarder

AWS のサービス	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution
AWS Identity and Access Management	ポリシー	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	トピック	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications
AWS Lambda	関数	aws-controltower-NotificationForwarder

共有アカウントについて

AWS Control Tower には、管理アカウント、監査アカウント、ログアーカイブアカウントの 3 つの特別な AWS アカウント が関連付けられています。これらのアカウントは通常、共有アカウントと呼ばれ、場合によってはコアアカウントと呼ばれることもあります。

- ランディングゾーンのセットアップ時に、監査アカウントとログアーカイブアカウントの名前をカスタマイズすることを選択できます。アカウント名の変更については、「外部で AWS Control Tower リソース名を変更する」を参照してください。
- 最初のランディングゾーンのセットアッププロセス中に、既存の を AWS Control Tower のセキュリティアカウントまたはログ記録アカウント AWS アカウント として指定することもできます。このオプションを使用すると、AWSControl Tower で新しい共有アカウントを作成する必要がなくなります。(これは 1 回限りの選択です)。

共有アカウントおよび関連リソースの詳細については、「共有アカウントで作成されたリソース」を参照してください。

管理アカウント

これにより AWS Control Tower が AWS アカウント 起動します。デフォルトでは、このアカウントのルートユーザーと、このアカウントのIAMユーザーまたはIAM管理者ユーザーは、ランディングゾーン内のすべてのリソースにフルアクセスできます。

> **Note**
>
> ベストプラクティスとして、このアカウントのルートユーザーまたは管理者ユーザーとしてサインインするのではなく、AWSControl Tower コンソールで管理機能を実行するときは、IAM管理者権限を持つ IAM Identity Center ユーザーとしてサインインすることをお勧めします。

管理アカウントで使用できるロールとリソースの詳細については、「共有アカウントで作成されたリソース」を参照してください。

ログアーカイブアカウント

ログアーカイブ共有アカウントは、ランディングゾーンの作成時に自動的にセットアップされます。

このアカウントには、ランディングゾーン内の他のすべてのアカウントのすべての AWS CloudTrail および AWS Config ログファイルのコピーを保存するための中央 Amazon S3 バケットが含まれています。ベストプラクティスとして、ログアーカイブアカウントへのアクセスを制限することをお勧めします。コンプライアンスと調査を担当し、それに関連するセキュリティツールまたは監査ツールを使用するチームに制限します。このアカウントは、自動セキュリティ監査や AWS Config ルール、Lambda 関数などのカスタム をホストして修復アクションを実行するために使用できます。

> **Amazon S3 バケットポリシー**
>
> AWS Control Tower ランディングゾーンバージョン 3.3 以降では、アカウントは Audit バケットへの書き込みアクセス許可の `aws:SourceOrgID`条件を満たす必要があります。この条件により、 は組織内のアカウントに代わって CloudTrail のみ S3 バケットにログを書き込むことができます。これにより、組織外の CloudTrail ログが AWS Control Tower S3 バケットに書き込まれなくなります。詳細については、「AWS Control Tower ランディングゾーンバージョン 3.3」を参照してください。

ログアーカイブアカウントで使用可能なロールとリソースの詳細については、「ログアーカイブアカウントのリソース」を参照してください。

> **Note**
>
> これらのログは変更できません。アカウントアクティビティに関連する監査とコンプライアンス調査の目的で、すべてのログが保存されます。

監査アカウント

この共有アカウントは、ランディングゾーンの作成時に自動的にセットアップされます。

監査アカウントは、セキュリティとコンプライアンスのチームに制限することをお勧めします。チームは、ランディングゾーン内のすべてのアカウントに対して監査人 (読み取り専用) と管理者 (フルアクセス) というアカウント横断的なロールを持ちます。このようなロールは、セキュリティとコンプライアンスのチームが次の目的で使用するためのものです。

- カスタム AWS Config ルールの Lambda 関数のホスティングなどの AWS メカニズムを使用して監査を実行します。
- 修復アクションなど、自動化されたセキュリティ操作を実行します。

監査アカウントは、Amazon Simple Notification Service (Amazon SNS) サービスを通じて通知も受け取ります。次の 3 つのカテゴリの通知を受け取ることができます。

- すべての設定イベント – このトピックでは、ランディングゾーン内のすべてのアカウントからのすべての CloudTrail および AWS Config 通知を集計します。
- セキュリティ通知の集約 – このトピックでは、特定の CloudWatch イベント、 AWS Config ルール コンプライアンスステータス変更イベント、および GuardDuty 検出結果からのすべてのセキュリティ通知を集約します。
- ドリフト通知 – このトピックでは、ランディングゾーン内のすべてのアカウント、ユーザー、、OUsおよび SCPs で検出されたすべてのドリフト警告を集計します。ドリフトの詳細については、「AWS Control Tower でドリフトを検出して解決する」を参照してください。

メンバーアカウント内でトリガーされる監査通知は、ローカル Amazon SNSトピックにアラートを送信することもできます。この機能により、アカウント管理者は個々のメンバーアカウントに固有の監査通知をサブスクライブできます。そのため、管理者は個々のアカウントに影響する問題を解決しながら、一元管理された監査アカウントにすべてのアカウント通知を集約できます。詳細については、「Amazon Simple Notification Service デベロッパーガイド」を参照してください。

監査アカウントで使用できるロールとリソースの詳細については、「アカウントリソースを監査する」を参照してください。

プログラムによる監査の詳細については、AWS「Control Tower 監査アカウントのプログラムによるロールと信頼関係」を参照してください。

> **Important**
>
> 監査アカウント用に指定した E メールアドレスは、AWSControl Tower で AWS リージョン サポートされているすべての からAWS 通知 - サブスクリプション確認 E メールを受信します。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、AWSControl Tower で AWS リージョン サポートされている各 E メールから、各 E メール内のサブスクリプションの確認リンクを選択する必要があります。

メンバーアカウントについて

メンバーアカウントは、ユーザーが AWS ワークロードを実行するアカウントです。これらのメンバーアカウントは、Account Factory、Service Catalog コンソールの管理者権限を持つ IAM Identity Center ユーザー、または自動化された方法で作成できます。これらのメンバーアカウントは、作成

時に AWS Control Tower コンソールで作成された、または Control Tower に登録された OU AWS に存在します。詳細については、次の関連トピックを参照してください。

- Account Factory でのアカウントのプロビジョニングと管理
- AWS Control Tower でタスクを自動化する
- AWS Organizations ユーザーガイドの「AWS Organizations の用語と概念」

また、「 AWS Control Tower Account Factory for Terraform (AFT) によるアカウントのプロビジョニング 」も参照してください。

> **アカウントとコントロール**
>
> メンバーアカウントは AWS Control Tower に登録することも、登録を解除することもできます。コントロールは、登録済みアカウントと未登録アカウントで異なる方法で適用され、継承OUsに基づいてネストされたアカウントに適用される場合があります。

AWS Control Tower が割り当てるメンバーアカウントリソースの詳細については、「」を参照してくださいAccount Factory のリソースに関する考慮事項。

既存の を登録する AWS アカウント

AWS Control Tower ガバナンスを、既に Control Tower によって管理されている組織単位 (OU) AWS に登録 AWS アカウント するときに既存の個人に拡張できます。Control Tower AWS OU と同じ AWS Organizations 組織OUsに属する未登録の に適格なアカウントが存在する。

> **Note**
>
> ランディングゾーンの初期セットアップ時を除き、既存のアカウントを監査アカウントまたはログアーカイブアカウントとして登録することはできません。

信頼されたアクセスを最初にセットアップする

既存の AWS アカウント を AWS Control Tower に登録する前に、AWSControl Tower がアカウントを管理または管理するアクセス許可を付与する必要があります。具体的に AWS CloudFormation は、AWSControl Tower には、 がスタックを選択した組織のアカウントに自動的にデプロ

イできるように、 AWS Organizations ユーザーに代わって AWS CloudFormation と の間に信頼されたアクセスを確立するためのアクセス許可が必要です。この信頼されたアクセスでは、AWSControlTowerExecution ロールは、各アカウントを管理するために必要なアクティビティを実行します。そのため、登録する前にこのロールを各アカウントに追加する必要があります。

信頼されたアクセスが有効になっている場合、 は 1 回のオペレーション AWS リージョン で複数のアカウントおよび のスタックを作成、更新、または削除 AWS CloudFormation できます。AWSControl Tower は、この信頼機能を利用して、既存のアカウントを登録済みの組織単位に移動する前にロールとアクセス許可を適用し、ガバナンス下に置くことができます。

信頼されたアクセスと AWS CloudFormation StackSets、「」を参照してください。 AWS CloudFormationStackSets および AWS Organizations。

アカウント登録中の処理

登録プロセス中に、AWSControl Tower は次のアクションを実行します。

- アカウントのベースラインを作成します。これには、以下のスタックセットのデプロイが含まれます。
  - AWSControlTowerBP-BASELINE-CLOUDTRAIL
  - AWSControlTowerBP-BASELINE-CLOUDWATCH
  - AWSControlTowerBP-BASELINE-CONFIG
  - AWSControlTowerBP-BASELINE-ROLES
  - AWSControlTowerBP-BASELINE-SERVICE-ROLES
  - AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES
  - AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1

  これらのスタックセットのテンプレートで既存のポリシーとの競合がないことを確認することをお勧めします。
- AWS IAM Identity Center または を通じてアカウントを識別します AWS Organizations。
- 指定した OU にアカウントを配置します。セキュリティ体制が一貫しているように、現在の OU SCPsに適用されるすべての を必ず適用してください。
- 選択した OU 全体SCPsに適用される を使用して、必須コントロールをアカウントに適用します。
- アカウント内のすべてのリソースを記録するように有効化 AWS Config して設定します。
- AWS Control Tower の検出コントロールをアカウントに適用する AWS Config ルールを追加します。

アカウントと組織レベルの CloudTrail 証跡

OU 内のすべてのメンバーアカウントは、登録されているかどうかにかかわらず、OU の AWS CloudTrail 証跡によって管理されます。

- AWS Control Tower にアカウントを登録すると、アカウントは新しい組織の AWS CloudTrail 証跡によって管理されます。証 CloudTrail 跡の既存のデプロイがある場合、AWSControl Tower に登録する前にアカウントの既存の証跡を削除しない限り、料金が重複することがあります。
- AWS Organizations コンソールなどを使用してアカウントを登録済み OU に移動し、そのアカウントを AWS Control Tower に登録しない場合は、アカウントの残りのアカウントレベルの証跡を削除できます。証 CloudTrail 跡の既存のデプロイがある場合、重複 CloudTrail 料金が発生します。

ランディングゾーンを更新して組織レベルの証跡をオプトアウトすることを選択した場合、またはランディングゾーンがバージョン 3.0 より古い場合、組織レベルの CloudTrail証跡はアカウントには適用されません。

で既存のアカウントを登録する VPCs

AWS Control Tower は、Account Factory で新しいアカウントをプロビジョニングするときと、既存のアカウントを登録するときの処理VPCsが異なります。

- 新しいアカウントを作成すると、AWSControl Tower は自動的に AWS デフォルトを削除VPCし、そのアカウントの新しい VPC を作成します。
- 既存のアカウントを登録しても、AWSControl Tower はそのVPCアカウントの新しい を作成しません。
- 既存のアカウントを登録しても、AWSControl Tower はアカウントVPCに関連付けられた既存のアカウントVPCまたは AWS デフォルトを削除しません。

Tip

Account Factory を設定することで、新しいアカウントのデフォルトの動作を変更できるため、AWSControl Tower の組織内のアカウントに対してVPCデフォルトで は設定されませ

ん。詳細については、「を使用せずに AWS Control Tower でアカウントを作成する VPC」を参照してください。

登録の前提条件

AWS Control Tower AWS アカウント に既存の を登録する前に、以下の前提条件が必要です。

1. 既存の を登録するには AWS アカウント、登録するアカウントにAWSControlTowerExecutionロールが存在する必要があります。詳細と手順については、「アカウントを登録する」で参照できます。
2. AWSControlTowerExecution ロールに加えて、登録する既存の AWS アカウント には、以下のアクセス許可と信頼関係が必要です。それ以外の場合、登録は失敗します。

   ロールのアクセス許可: AdministratorAccess (AWS 管理ポリシー)

   ロールの信頼関係:

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

3. アカウントには AWS Config 設定レコーダーや配信チャネルを含めないことをお勧めします。アカウントを登録する前に、 AWS CLI を使用してこれらを削除または変更できます。それ以外の場合は、既存の AWS Config リソースを持つアカウントを登録して、既存のリソースを変更する方法の手順を確認してください。
4. 登録するアカウントは、AWSControl Tower 管理アカウントと同じ AWS Organizations 組織に存在する必要があります。存在するアカウントは、AWS既に Control Tower に登録されている OU の AWS Control Tower 管理アカウントと同じ組織にのみ登録できます。

登録に関するその他の前提条件を確認するには、AWS「Control Tower の開始方法」を参照してください。

> **Note**
>
> アカウントを AWS Control Tower に登録すると、そのアカウントは AWS Control Tower 組織の証跡によって AWS CloudTrail 管理されます。証跡の CloudTrail既存のデプロイがある場合、AWSControl Tower に登録する前にアカウントの既存の証跡を削除しない限り、料金が重複することがあります。

既存のアカウントを登録する

アカウント登録機能は、AWSControl Tower コンソールで既存の を登録 AWS アカウント して AWS Control Tower によって管理されるようにできます。詳細については、「既存の を登録する AWS アカウント」を参照してください。

[Enroll account] (アカウントの登録) 機能は、ランディングゾーンがドリフト状態でないときに使用できます。コンソールでこの機能を表示するには:

- AWS Control Tower の Organization ページに移動します。
- 登録するアカウントの名前を見つけます。見つけるには、アカウント名は、右上にあるドロップダウンメニューから [Accounts only] (アカウントのみ) を選択し、フィルターされたテーブルで探してください。
- アカウントを登録する手順 セクションで示されているように、個々のアカウントを登録する手順に従います。

> **Note**
>
> 既存の E メールアドレスを登録するときは AWS アカウント、必ず既存の E メールアドレスを確認してください。それ以外の場合は、新しいアカウントが作成されます。

特定のエラーが表示された場合、ページを更新してもう一度試す必要があります。ランディングゾーンがドリフト状態にある場合は、[Enroll account] (アカウントの登録) 機能を正常に使用できないことがあります。ランディングゾーンのドリフトが解決されるまで、Account Factory を使用して新しいアカウントをプロビジョニングする必要があります。

AWS Control Tower コンソールからアカウントを登録する場合、AWSServiceCatalogEndUserFullAccessポリシーが有効になっているユーザーとともにAWS、Control Tower コンソールを使用する管理者アクセス許可を持つアカウントにサインインする必要があります。ルートユーザーとしてサインインすることはできません。

登録したアカウントは、他のアカウントを更新する場合と同様に、 AWS Service Catalog および AWS Control Tower Account Factory によって更新される場合があります。更新手順については、「AWS Control Tower または を使用して Account Factory アカウントを更新および移動する AWS Service Catalog」セクションを参照してください。

アカウントを登録する手順

既存のアカウントにアクセスAdministratorAccess許可 (ポリシー) を設定したら、次のステップに従ってアカウントを登録します。

AWS Control Tower に個々のアカウントを登録するには

- AWS Control Tower Organization ページに移動します。
- [Organization] (組織) ページで、登録できるアカウントでは、セクション上部の [Actions] ドロップダウンメニューから [Enroll] を選択できます。これらのアカウントには、[Account details] (アカウントの詳細) ページでも [Enroll account] (アカウントの登録) ボタンが表示されます。
- [Enroll account] (アカウントの登録) を選択した場合、[Enroll account] (アカウントの登録) ページが表示され、AWSControlTowerExecution ロールをアカウントに追加するよう促されます。手順については、「必要なIAMロールを既存の に手動で追加 AWS アカウント して登録する」を参照してください。
- 次に、ドロップダウンの一覧から登録された OU を選択します。アカウントが既に登録済みの OU にある場合、このリストには OU が表示されます。
- [[Enroll account (アカウントの登録)] を選択します。
- AWSControlTowerExecution ロールを追加するためのモーダルリマインダーが表示されるので、アクションを確認します。
- [Enroll] (登録する) を選択します。
- AWS Control Tower は登録プロセスを開始し、アカウントの詳細ページに戻ります。

登録の失敗の一般的な原因

- 既存のアカウントを登録するには、登録するアカウントに AWSControlTowerExecution ロールが存在する必要があります。

- IAM プリンシパルには、アカウントのプロビジョニングに必要なアクセス許可がない場合があります。
- AWS Security Token Service （ AWS STS) は、ホームリージョンの または AWS Control Tower AWS アカウント でサポートされている任意のリージョンで無効になっています。
- AWS Service Catalogの Account Factory ポートフォリオに追加する必要があるアカウントにサインインしている場合があります。アカウントを AWS Control Tower で作成または登録するには、Account Factory にアクセスする前にアカウントを追加する必要があります。適切なユーザーまたはロールが Account Factory ポートフォリオに追加されていない場合、アカウントを追加しようとするとエラーが発生します。 AWS Service Catalog ポートフォリオへのアクセスを許可する方法については、「ユーザーへのアクセスの許可」を参照してください。
- root としてサインインしている可能性があります。
- 登録しようとしているアカウントに、残っている AWS Config 設定がある可能性があります。特に、アカウントに設定レコーダーや配信チャネルを持たないようにできます。これらは、アカウントを登録する AWS CLI 前に、 を通じて削除または変更する必要があります。詳細については、既存の AWS Config リソースを持つアカウントを登録するおよびAWS Control Tower を介して を操作する AWS CloudShellを参照してください。
- アカウントが別の AWS Control Tower OU を含む管理アカウントを持つ別の OU に属している場合は、別の OU に参加する前に現在の OU のアカウントを終了する必要があります。元の OU で既存のリソースを削除する必要があります。それ以外の場合、登録は失敗します。
- 送信先 OU で、そのアカウントに必要なすべてのリソースを作成SCPsできない場合、アカウントのプロビジョニングと登録は失敗します。例えば、送信先 OU SCPの は、特定のタグなしでリソースの作成をブロックする場合があります。この場合、AWSControl Tower はリソースのタグ付けをサポートしていないため、アカウントのプロビジョニングまたは登録は失敗します。サポートについては、アカウント担当者または サポートにお問い合わせください。

新しいアカウントの作成時または既存のアカウントの登録時に AWS Control Tower がロールと連携する方法の詳細については、「ロールとアカウント」を参照してください。

> **Tip**
>
> 既存の が登録の前提条件 AWS アカウント を満たしていることが確認できない場合は、登録 OU をセットアップし、その OU にアカウントを登録できます。登録が成功したら、アカウントを目的の OU に移動できます。登録が失敗した場合、他のアカウントや OUsは失敗の影響を受けません。

既存のアカウントとその設定が AWS Control Tower と互換性があることが不明な場合は、次のセクションで推奨されるベストプラクティスに従うことができます。

推奨: アカウントの登録に 2 段階のアプローチを設定する

- まず、コン AWS Config フォーマンスパックを使用して、一部の AWS Control Tower コントロールがアカウントに与える影響を評価します。AWS Control Tower への登録がアカウントに与える影響を判断するには、「コンフォーマンスパックを使用して AWS Control Tower AWS Config ガバナンスを拡張する」を参照してください。
- 次に、アカウントを登録できます。コンプライアンスの結果が満足のいくものであれば、予期しない結果を招くことなくアカウントを登録できるため、移行パスが簡単になります。
- 評価が完了したら、AWSControl Tower ランディングゾーンを設定する場合は、評価用に作成された AWS Config 配信チャネルと設定レコーダーを削除する必要がある場合があります。その後、AWSControl Tower を正常にセットアップできます。

> **Note**
>
> コンフォーマンスパックは、アカウントが AWS Control Tower OUsに登録されているが、ワークロードは AWS Control Tower がサポートしていない AWS リージョン内で実行される状況でも機能します。コンフォーマンスパックを使用して、AWSControl Tower がデプロイされていないリージョンに存在するアカウントのリソースを管理できます。

アカウントが前提条件を満たしていない場合

前提条件として、AWSControl Tower ガバナンスに登録できるアカウントは、同じ組織全体の一部である必要があることに注意してください。アカウント登録のこの前提条件を満たすには、以下の準備手順に従って、アカウントを AWS Control Tower と同じ組織に移動できます。

AWS Control Tower と同じ組織にアカウントを持ち込むための準備手順

1. 既存の組織からアカウントを削除します このアプローチを使用する場合は、別の支払い方法を指定する必要があります。
2. AWS Control Tower 組織にアカウントを招待します。詳細については、「 ユーザーガイド」の「組織に参加する AWS アカウントを招待する」を参照してください。 AWS Organizations

3. 招待を受け入れます アカウントは組織のルートに表示されます。このステップでは、アカウントを AWS Control Tower と同じ組織に移動します。 と は、一括請求を確立SCPsして統合します。

> **Tip**
>
> アカウントが古い組織から削除される前に、新しい組織への招待を送信できます。招待は、アカウントが既存の組織から正式に削除されるのを待機します。

残りの前提条件を満たすステップ:

1. 必要な `AWSControlTowerExecution` ロールを作成します。
2. デフォルトの をクリアしますVPC。（ この部分はオプションです。 AWS Control Tower は既存のデフォルト を変更しません ）VPC。
3. または を使用して、既存の AWS Config 設定レコーダーまたは配信チャネルを削除 AWS CLI または変更します AWS CloudShell。詳細については、「リソースステータスのコマンド例 AWS Config CLI 」および「既存の AWS Config リソースを持つアカウントを登録する」を参照してください。

これらの準備手順を完了したら、アカウントを AWS Control Tower に登録できます。詳細については、「アカウントを登録する手順」を参照してください。このステップでは、アカウントを完全な AWS Control Tower ガバナンスに移行します。

アカウントのプロビジョニングを解除して、アカウントを登録しスタックを維持できるようにするための任意のステップ

1. 適用された AWS CloudFormation スタックを保持するには、スタックセットからスタックインスタンスを削除し、インスタンスのスタックを保持するを選択します。
2. AWS Service Catalog Account Factory でアカウントプロビジョニング済み製品を削除します。（ このステップでは、プロビジョニングされた製品のみを AWS Control Tower から削除します。 アカウントは削除されません。 ）
3. 必要に応じて、組織に属していないアカウントに必要な請求の詳細を使用してアカウントを設定します。次に、組織からアカウントを削除します（ これを行うと、アカウントは AWS Organizations クォータの合計に対してカウントされません ）。

4. リソースが残っている場合はアカウントをクリーンアップし、「アカウントを登録解除する」のアカウント閉鎖のステップに従って、アカウントを閉鎖します。
5. コントロールが定義された [Suspended] (停止状態) の OU がある場合、ステップ 1 を実行する代わりに、その OU にアカウントを移動できます。

リソースステータスのコマンド例 AWS Config CLI

設定レコーダーと配信チャネルのステータスを判断するために使用できるコマンドの例 AWS Config CLIを次に示します。

表示コマンド:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

通常の応答は `"name": "default"` のようになります。

削除コマンド:

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

必要なIAMロールを既存の に手動で追加 AWS アカウント して登録する

AWS Control Tower ランディングゾーンをすでに設定している場合は、組織のアカウントを AWS Control Tower に登録されている OU に登録できます。ランディングゾーンを設定していない場合は、「開始方法、ステップ 2」のAWS「Control Tower ユーザーガイド」で説明されているステップに従ってください。 https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html#step-twoランディングゾーンの準備ができたら、次のステップを実行して、既存のアカウントを AWS Control Tower によって手動でガバナンスします。

この章で前述した 登録の前提条件 を必ず確認してください。

AWS Control Tower にアカウントを登録する前に、そのアカウントを管理するアクセス許可を AWS Control Tower に付与する必要があります。これを行うには、次のステップに示すように、アカウントへのフルアクセス権を持つロールを追加します。これらのステップは、登録するアカウントごとに実行する必要があります。

アカウントごとに次の手順を実行します。

ステップ 1: 登録するアカウントが現在含まれている組織の管理アカウントに、管理者アクセス権を使ってサインインします。

例えば、 からこのアカウントを作成し AWS Organizations 、クロスアカウントIAMロールを使用してサインインする場合、以下のステップを実行できます。

1. 組織の管理アカウントにサインインします。
2. AWS Organizations に移動します。
3. [Accounts] (アカウント) で、登録するアカウントを選択し、アカウント ID をコピーします。
4. 上部のナビゲーションバーのアカウントドロップダウンメニューを開き、[Switch Role] (ロールの切り替え) を選択します。
5. [Switch Role] (ロールの切り替え) フォームで、次のフィールドに入力します。
   - [Account] (アカウント) に、コピーしたアカウント ID を入力します。
   - ロール に、このアカウントへのクロスアカウントアクセスを有効にするIAMロールの名前を入力します。このロールの名前は、アカウントの作成時に定義されています。アカウントの作成時にロール名を指定していない場合は、デフォルトのロール名、`OrganizationAccountAccessRole` を入力します。
6. [Switch Role] (ロールの切り替え) を選択します。
7. これで、子アカウント AWS Management Console として にサインインします。
8. 完了したら、次の手順を実行するために子アカウントにとどまります。
9. 管理アカウント ID は次のステップで入力する必要があるため、メモしておきます。

ステップ 2: アカウントを管理するアクセス許可を AWS Control Tower に付与します。

1. IAM に移動します。
2. [Roles] (ロール) に移動します。
3. [ロールの作成] を選択します。
4. ロールの対象となるサービスの選択を求められたら、[カスタム信頼ポリシー] を選択します。

5. ここに示すコード例をコピーして、ポリシードキュメントに貼り付けます。文字列 *Management Account ID* を、管理アカウントの実際の管理アカウント ID に置き換えます。貼り付けるポリシーは次のとおりです。

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

6. ポリシーをアタッチするように求められたら、 を選択しますAdministratorAccess。
7. [Next:Tags] (次へ: タグ) を選択します。
8. [Add tags] (タグを追加する) というタイトルのオプションの画面が表示されることがあります。[Next:Review] (次へ: レビュー) を選択して、この画面をスキップします。
9. [Review] (確認) 画面の [Role name] (ロール名) フィールドに、`AWSControlTowerExecution` と入力します。
10. [Description] (説明) ボックスに、登録のためのフルアカウントアクセスを許可などの短い説明を入力します。
11. [ロールの作成] を選択します。

ステップ 3: 登録された OU に移動してアカウントを登録し、登録を確認します。

ロールを作成して必要なアクセス許可を設定したら、次のステップに従ってアカウントを登録し、登録を確認します。

1. Admin として再度サインインし、AWSControl Tower に移動します。
2. アカウントを登録します。

   - AWS Control Tower の Organization ページでアカウントを選択し、右上の Actions ドロップダウンメニューから Enroll を選択します。

- アカウントを登録する手順 ページで示されているように、個々のアカウントを登録する手順に従います。

3. 登録を確認します。

- AWS Control Tower から、左側のナビゲーションで Organization を選択します。
- 最近登録したアカウントを探します。初期状態では、[Enrolling] (登録中) のステータスが表示されます。
- 状態が [Enrolled] (登録済み) に変わったら、移動は成功です。

このプロセスを続行するには、AWSControl Tower に登録する組織内の各アカウントにサインインします。各アカウントについて、前提条件のステップと登録のステップを繰り返します。

AWS Organizations アカウントの自動登録

ブログ記事「既存のAWS アカウントを AWS Control Tower に登録する」で説明されている登録方法を使用して、プログラムによるプロセスでアカウント AWS Organizations を AWS Control Tower に登録できます。

次のYAMLテンプレートは、プログラムで登録できるように、アカウントで必要なロールを作成するのに役立ちます。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
```

```
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

既存の AWS Config リソースを持つアカウントを登録する

このトピックでは、 step-by-step既存の AWS Config リソースを持つアカウントを登録する方法のアプローチを示します。既存のリソースを確認する方法の例については、「リソースステータスのコマンド例 AWS Config CLI 」を参照してください。

> **Note**
>
> 既存の AWS アカウントを監査およびログアーカイブアカウントとして AWS Control Tower に持ち込む予定で、それらのアカウントに既存の AWS Config リソースがある場合は、この目的でこれらのアカウントを AWS Control Tower に登録する前に、既存の AWS Config リソースを完全に削除する必要があります。監査アカウントやログアーカイブアカウントにする予定がないアカウントについては、既存の Config リソースを変更できます。

AWS Config リソースの例

アカウントにすでに用意されている可能性のある AWS Config リソースのタイプを次に示します。これらのリソースは、アカウントを AWS Control Tower に登録できるように変更する必要がある場合があります。

- AWS Config レコーダー
- AWS Config 配信チャネル
- AWS Config 集約認可

引き受け

- AWS Control Tower ランディングゾーンをデプロイしました
- アカウントが AWS Control Tower にまだ登録されていません。

- アカウントには、管理アカウントによって管理される AWS Control Tower リージョンの少なくとも 1 つに、少なくとも 1 つの既存の AWS Config リソースがあります。
- アカウントは AWS Control Tower 管理アカウントではありません。
- アカウントでガバナンスドリフトが発生していないこと。

既存の AWS Config リソースにアカウントを登録する自動アプローチを説明するブログについては、「既存の AWS Config リソースにアカウントを登録する自動化」を参照してくださいAWS。次の「ステップ 1: チケットを使用してカスタマーサポートに連絡し、アカウントを AWS Control Tower 許可リストに追加する」の説明に従って、登録するすべてのアカウントに対して単一のサポートチケットを送信できます。

制限

- アカウントは、AWSControl Tower ワークフローを使用してガバナンスを拡張することによってのみ登録できます。
- リソースが変更され、アカウントにドリフトが作成された場合、AWSControl Tower はリソースを更新しません。
- AWS Config AWS Control Tower によって管理されていないリージョンの リソースは変更されません。

> **Note**
>
> 既存の Config リソースを持つアカウントを、許可リストに追加せずに登録しようとすると、登録は失敗します。その後、同じアカウントを許可リストに追加しようとすると、AWSControl Tower はアカウントが正しくプロビジョニングされていることを検証できません。許可リストをリクエストしてから登録する前に、AWSControl Tower からアカウントのプロビジョニングを解除する必要があります。アカウントを別の AWS Control Tower OU にのみ移動すると、ガバナンスドリフトが発生し、アカウントが許可リストに追加されなくなります。

このプロセスには主に次の 5 つのステップがあります。

1. AWS Control Tower 許可リストにアカウントを追加します。
2. アカウントに新しいIAMロールを作成します。
3. 既存の AWS Config リソースを変更します。

4. リソースが存在しない AWS リージョンに AWS Config リソースを作成します。
5. AWS Control Tower にアカウントを登録します。

先に進む前に、このプロセスに関する次の期待事項を考慮してください。

- AWS Control Tower はこのアカウントに AWS Config リソースを作成しません。
- 登録後、AWSControl Tower コントロールは、新しいIAMロールを含め、作成した AWS Config リソースを自動的に保護します。
- 登録後に AWS Config リソースに変更があった場合は、アカウントを再登録する前に、それらのリソースを AWS Control Tower の設定に合わせて更新する必要があります。

ステップ 1: チケットを使用してカスタマーサポートに連絡し、アカウントを AWS Control Tower 許可リストに追加する

チケットの件名には次の文章を使用してください。

既存の AWS Config リソースを持つアカウントを AWS Control Tower に登録する

チケットの本文に以下の詳細を記載してください。

- 管理アカウント番号
- 既存の AWS Config リソースを持つメンバーアカウントのアカウント番号
- AWS Control Tower のセットアップ用に選択したホームリージョン

> **Note**
>
> アカウントを許可リストに追加するのに必要な時間は 2 営業日です。

ステップ 2: メンバーアカウントに新しいIAMロールを作成する

1. メンバーアカウントの AWS CloudFormation コンソールを開きます。
2. 次のテンプレートを使用して新しいスタックを作成します。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
```

```
Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. スタックの名前を として指定します。 CustomerCreatedConfigRecorderRoleForControlTower
4. スタックを作成します。

> **Note**
>
> SCPs 作成する は、 `aws-controltower-ConfigRecorderRole*`ロールを除外する必要があります。 AWS Config ルールによる評価の実行を制限するアクセス許可は変更しないでください。
> 以下のガイドラインに従って、 SCPs が Config を呼び出すブロックAccessDeniedExceptionがある場合`aws-controltower-ConfigRecorderRole*`にを受信しないようにします。

ステップ 3: 既存のリソースがある AWS リージョンを特定する

アカウント内の管理対象リージョン (AWS Control Tower 管理対象) ごとに、前述の既存の AWS Config リソースサンプルタイプが少なくとも 1 つあるリージョンを特定してメモします。

ステップ 4: AWS Config リソースがない AWS リージョンを特定する

アカウント内の管理対象リージョン (AWS Control Tower 管理対象) ごとに、前述の例タイプの AWS Config リソースがないリージョンを特定してメモします。

ステップ 5: AWS リージョンごとの既存のリソースを変更する

このステップでは、AWSControl Tower のセットアップに関する次の情報が必要です。

- LOGGING_ACCOUNT - ロギングアカウント ID
- AUDIT_ACCOUNT - 監査アカウント ID
- IAM_ROLE_ARN - ステップ 1 でARN作成したIAMロール
- ORGANIZATION_ID - 管理アカウントの組織 ID
- MEMBER_ACCOUNT_NUMBER - 変更対象のメンバーアカウント
- HOME_REGION - AWS Control Tower セットアップのホームリージョン。

次のセクション 5a ~ 5c の指示に従って、既存のリソースを変更します。

ステップ 5a. AWS Config recorder リソース

AWS リージョンごとに存在できる AWS Config レコーダーは 1 つだけです。それが存在する場合は、次のように設定を変更します。ホームリージョンでは項目 GLOBAL_RESOURCE_RECORDING を true に置き換えます。 AWS Config レコーダーが存在する他のリージョンでは、項目を false に置き換えます。

- 名前： DON'T CHANGE
- ロールARN： IAM_ROLE_ARN
  - RecordingGroup:
  - AllSupported： true
  - IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
  - ResourceTypes： 空

この変更は、次のコマンドを使用して AWS CLIから行うことができます。文字列を既存の AWS Config レコーダー名RECORDER_NAMEに置き換えます。

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

ステップ 5b。 AWS Config 配信チャネルリソースを変更する

リージョンごとに存在できる AWS Config 配信チャネルは 1 つだけです。2 つ以上存在する場合は、次のように設定を変更します。

- 名前： DON'T CHANGE
- ConfigSnapshotDeliveryProperties： TwentyFour_時間
- S3BucketName： AWS Control Tower ログ記録アカウントのログ記録バケット名

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix: *ORGANIZATION_ID*
- SnsTopicARN: 監査アカウントのSNSトピックARN。次の形式になります。

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

この変更は、次のコマンドを使用して AWS CLIから行うことができます。文字列を既存の AWS Config レコーダー名*DELIVERY_CHANNEL_NAME*に置き換えます。

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

ステップ 5c。 AWS Config 集約認可リソースの変更

リージョンごとに複数の集約認可が存在する場合があります。 AWSControl Tower には、監査アカウントを認可されたアカウントとして指定し、AWSControl Tower のホームリージョンを認可された

リージョンとして持つ集約認可が必要です。存在しない場合、次の設定を使用して新しく作成します。

- AuthorizedAccountId: 監査アカウント ID
- AuthorizedAwsRegion： AWS Control Tower セットアップのホームリージョン

この変更は、次のコマンドを使用して AWS CLIから行うことができます。

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

ステップ 6: AWS Control Tower によって管理されるリージョンに、存在しないリソースを作成する

次の例GLOBAL_RESOURCE_RECORDINGに示すように、ホームリージョンで IncludeGlobalResourcesTypesパラメータの値が になるように AWS CloudFormation テンプレートを変更します。また、このセクションで指定している、テンプレートの必須フィールドを更新します。

ホームリージョンでは項目 GLOBAL_RESOURCE_RECORDING を true に置き換えます。 AWS Config レコーダーが存在する他のリージョンでは、項目を false に置き換えます。

1. 管理アカウントの AWS CloudFormation コンソールに移動します。
2. という名前 StackSet の新しい を作成しますCustomerCreatedConfigResourcesForControlTower。
3. 次のテンプレートをコピーして更新します。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
```

```
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

必須フィールドを使用してテンプレートを更新します。

a. S3BucketName フィールドで、 *LOGGING_ACCOUNT_ID*と を置き換えます。 *HOME_REGION*

b. S3KeyPrefix フィールドで、 *ORGANIZATION_ID*

c. SnsTopicARN フィールドで、 *AUDIT_ACCOUNT*

d. AuthorizedAccountId フィールドで、 *AUDIT_ACCOUNT*

e. AuthorizedAwsRegion フィールドで、 *HOME_REGION*

4. AWS CloudFormation コンソールでのデプロイ中に、メンバーアカウント番号を追加します。
5. ステップ 4 で特定した AWS リージョンを追加します。
6. スタックセットをデプロイします。

ステップ 7: Control Tower に OU AWS を登録する

AWS Control Tower ダッシュボードで、OU を登録します。

> **Note**
>
> アカウントの登録ワークフローは、このタスクでは成功しません。[Register OU] (OU の登録) または [Re-register OU] (OU の再登録) を選択する必要があります。

Account Factory でのアカウントのプロビジョニングと管理

この章では、Account Factory を使用して AWS Control Tower ランディングゾーンに新しいメンバーアカウントをプロビジョニングする概要と手順について説明します。

アカウントの設定とプロビジョニングのためのアクセス許可

AWS Control Tower Account Factory を使用すると、 のクラウド管理者とユーザーがランディングゾーンにアカウント AWS IAM Identity Center 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 IAM Identity Center ユーザーは、 `AWSAccountFactory`グループまたは 管理グループに属している必要があります。

> **Note**
>
> 組織全体で許可を持つアカウントを使用する場合と同様に、管理アカウントから作業するときは注意が必要です。

AWS Control Tower 管理アカウントには、`AWSControlTowerExecution`ロールとの信頼関係があります。これにより、一部の自動アカウント設定を含む、管理アカウントからのアカウント設定が可能になります。`AWSControlTowerExecution` ロールの詳細については、「Roles and accounts」を参照してください。

> **Note**
>
> 既存の AWS アカウント を AWS Control Tower に登録するには、そのアカウントで`AWSControlTowerExecution`ロールが有効になっている必要があります。既存のアカウントを登録する方法の詳細については、「既存の を登録する AWS アカウント」を参照してください。

権限の詳細については、「アカウントに必要なアクセス許可」を参照してください。

AWS Service Catalog Account Factory でアカウントをプロビジョニングする

次の手順では、 を介して IAM Identity Center でアカウントをユーザーとして作成およびプロビジョニングする方法について説明します AWS Service Catalog。この手順は、アドバンストアカウントプ

ロビジョニングまたはマニュアルアカウントプロビジョニングとも呼ばれます。必要に応じて、 または AWS Control Tower Account Factory for Terraform () を使用して、プログラムでアカウントを AWS CLIプロビジョニングできますAFT。以前にカスタムブループリントを設定したことがある場合は、カスタマイズされたアカウントをコンソールでプロビジョニングできる場合があります。カスタマイズの詳細については、「Account Factory Customization を使用してアカウントをカスタマイズする (AFC)」を参照してください。

Account Factory でユーザーとしてアカウントをプロビジョニングするには

1. ユーザーポータル からサインインしますURL。
2. [Your applications] (お申込み内容) から、[AWS Account] (アカウント) を選択します。
3. アカウントのリストで、管理アカウントのアカウント ID を選択します。この ID には、[(Management)] ((管理)) などのラベルが付いている場合もあります。
4. からAWSServiceCatalogEndUserAccess、 マネジメントコンソールを選択します。これにより、このアカウントの AWS Management Console このユーザーの が開きます。
5. AWS Control Tower リージョンであるアカウントのプロビジョニング AWS リージョン に正しい を選択していることを確認します。
6. [Service Catalog] を検索して選択し、Service Catalog コンソールを開きます。
7. ナビゲーションペインで、[Products] (製品) を選択します。
8. AWS Control Tower Account Factory を選択し、製品の起動ボタンを選択します。この選択により、新しいアカウントをプロビジョニングするウィザードが開始されます。
9. 情報を入力し、以下の点に注意してください。

   - は、新しい E メールアドレス、または既存の IAM Identity Center ユーザーに関連付けられた E メールアドレスSSOUserEmailにすることができます。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。
   - は、 にまだ関連付けられていない E メールアドレスAccountEmailである必要がありますAWS アカウント。で新しい E メールアドレスを使用した場合はSSOUserEmail、ここでその E メールアドレスを使用できます。

10. 通知を定義TagOptionsしたり有効にしたりしないでください。有効にしないと、アカウントのプロビジョニングに失敗する可能性があります。完了したら、[Launch product] (製品の起動) を選択します。
11. アカウント設定を確認し、[Launch] (起動) を選択します。アカウントのプロビジョニングに失敗するため、リソースプランを作成しないでください。

12. これで、アカウントのプロビジョニングが開始されます。この処理には数分かかることがあります。ページをリフレッシュして、表示されたステータス情報を更新できます。

> **Note**
>
> 一度にプロビジョニングできるアカウントは最大 5 個です。

Account Factory アカウントの管理に関する考慮事項

Account Factory を使用して作成およびプロビジョニングしたアカウントは、更新、登録解除、および閉鎖できます。転用したいアカウントのユーザーパラメータを更新することで、アカウントを再利用できます。アカウントの組織単位 (OU) を変更することもできます。

> **Note**
>
> Account Factory が供給するアカウントに関連付けられているプロビジョニング済み製品を更新するときに、新しいユーザーの E メールアドレスを指定すると AWS IAM Identity Center、AWSControl Tower は IAM Identity Center に新しいユーザーを作成します。以前に作成したアカウントは削除されません。Identity Center から以前の IAM Identity IAM Center ユーザーの E メールアドレスを削除する方法については、「ユーザーの無効化」を参照してください。

AWS Control Tower または を使用して Account Factory アカウントを更新および移動する AWS Service Catalog

登録済みアカウントを更新する最も簡単な方法は、AWSControl Tower コンソールを使用することです。個々のアカウントの更新は、移動したメンバーアカウント のようなドリフトを解決するのに役立ちます。ランディングゾーンの完全な更新の一部として、アカウントの更新も必要です。

ある組織単位 (OU) から別の OU にアカウントを移動する場合、新しい OU によって適用されるコントロールが以前の OU のコントロールとは異なる場合があることに注意してください。新しい OU のコントロールがアカウントのポリシー要件を満たしている必要があります。

アカウントが 間で移動されるときの動作を制御する
OUs

間でアカウントを移動するとOUs、送信先 OU のコントロールが に適用されます。

アカウント。ただし、以前の OU のアカウントに適用されていたコントロールは削除されません。コントロールの正確な動作は、以前の OU と宛先 OU でアクティブなコントロールの実装に固有です。

- AWS Config ルールで実装されたコントロールの場合： 以前の OU のコントロールは削除されません。このようなコントロールは手動で削除する必要があります。
- で実装されたコントロールの場合SCPs： 以前の OU の SCPベースのコントロールは、削除されました。送信先 OU の SCPベースのコントロールは、このアカウントで有効になります。
- AWS CloudFormation フックを使用して実装されたコントロールの場合: この動作は、新しい OU のコントロールのステータスによって異なります。
  - 宛先 OU でフックベースのコントロールが有効になっていない場合: 古いコントロールは、手動で削除しない限り、移動したアカウントに対して有効なままとなります。
  - 宛先 OU でフックのコントロールが有効になっている場合: 古いコントロールは削除され、宛先 OU のコントロールがアカウントに適用されます。

コンソールでアカウントを更新する

AWS Control Tower コンソールでアカウントを更新するには

1. AWS Control Tower にサインインしたら、組織ページに移動します。
2. OUs および アカウントのリストで、更新するアカウントの名前を選択します。更新可能なアカウントには、[Update available] (更新可能) のステータスが表示されます。
3. 次に、選択したアカウントのページの [Account details] (アカウントの詳細) が表示されます。
4. 右上の [Update account] (アカウントの更新) を選択します。

プロビジョニング済み製品の更新

次の手順では、Service Catalog を使用して、アカウントのプロビジョニング済み製品を更新することにより、Account Factory のアカウントを更新したり、新しい OU に移動したりする方法を示します。

Account Factory アカウントを更新したり、Service Catalog からその OU を変更したりするには

1. AWS マネジメントコンソールにサインインし、 で AWS Service Catalog コンソールを開きますhttps://console.aws.amazon.com/servicecatalog/。

> **Note**
>
> 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 (`AWSAccountFactory`または `AWSServiceCatalogAdmins`グループの IAM Identity Center ユーザーなど) としてサインインする必要があります。

2. ナビゲーションペインで [Provisioning] (プロビジョニング) を選択し、次に [Provisioned products] (プロビジョニング済み製品) を選択します。
3. 一覧表示されているメンバーアカウントごとに以下のステップを実行して、すべてのメンバーアカウントを更新します。

   a. メンバーアカウントを選択します。そのアカウントの [Provisioned product details] (プロビジョニングされた製品の詳細) ページが表示されます。

   b. [Provisioned product details] (プロビジョニングされた製品の詳細) ページで、[Events] (イベント) タブを選択します。

   c. 以下のパラメータを書き留めます。

      - SSOUserEmail (プロビジョニング済み製品の詳細で利用可能)
      - AccountEmail (プロビジョニング済み製品の詳細で利用可能)
      - SSOUserFirstName (IAMIdentity Center で利用可能)
      - SSOUSerLastName (IAMIdentity Center で利用可能)
      - AccountName (IAMIdentity Center で利用可能)

   d. [Actions] (アクション) で、[Update] (更新) を選択します。

   e. 更新する製品の [Version] (バージョン) の横にあるボタンを選択して、[Next] (次へ) を選択します。

   f. 前に説明したパラメータ値を入力します。

      - 既存の OU を保持する場合は、 でManagedOrganizationalUnit、アカウントがすでに存在していた OU を選択します。
      - アカウントを新しい OU に移行する場合は、 で、アカウントの新しい OU ManagedOrganizationalUnitを選択します。

      中央のクラウド管理者は、この情報を Control Tower AWS コンソールの「組織」ページで確認できます。

g. [Next (次へ)] を選択します。

h. 変更内容を確認し、[Update] (更新) を選択します。このプロセスには、アカウントごとに数分かかることがあります。

登録済みアカウントの E メールアドレスの変更

AWS Control Tower で登録済みメンバーアカウントの E メールアドレスを変更するには、このセクションの手順に従います。

> **Note**
>
> 以下の手順では、管理アカウント、ログアーカイブアカウント、または監査アカウントの E メールアドレスを変更することはできません。詳細については、「 AWS アカウントに関連付けられている E メールアドレスを変更する方法」または「 サポート」にお問い合わせください AWS 。

AWS Control Tower が作成するアカウントの E メールアドレスを変更するには

1. アカウントのルートユーザーパスワードを回復します。「紛失または忘れた AWS パスワードを復元するにはどうすればよいですか？」という記事の手順に従います。
2. ルートユーザーパスワードでアカウントにサインインします。
3. E メールアドレスを他のメールアドレスと同じように変更し AWS アカウント、変更が反映されるまで待ちます AWS Organizations。E メールアドレスの変更による更新が完了するまで、遅延が発生する可能性があります。
4. アカウントに以前にあった E メールアドレスを使用して、Service Catalog でプロビジョニング済み製品を更新します。プロビジョニング済み製品を更新するプロセスには、新しい E メールアドレスのプロビジョニング済み製品への関連付けが含まれます。これにより、E メールアドレスの変更が AWS Control Tower で有効になります。今後プロビジョニングされる製品の更新には、新しい E メールアドレスを使用します。

AWS Organizationsで作成したメンバーアカウントのパスワードまたは E メールアドレスを変更するには、「AWS Organizations ユーザーガイド」の「ルートユーザーとしてのメンバーアカウントへのアクセス」を参照してください。

または、ルートユーザーとしてログインせずに、 AWS Organizations コンソールから Account Factory または他のメンバーアカウントの E メールアドレスを更新することもできます。詳細については、「AWS Organizations User Guide」の「Updating the root user email address for a member account with AWS Organizations」を参照してください。

登録済みアカウントの名前を変更する

このセクションの手順に従って、登録された AWS Control Tower アカウントの名前を変更します。

> **Note**
>
> AWS 管理者アカウントの名前を変更するには、管理者権限があり、アカウントのルートユーザーとしてログインしている必要があります。

AWS Control Tower によって作成されたアカウントの名前を変更するには

1. アカウントの root パスワードを回復します。この記事「紛失または忘れた AWS パスワードを復元するにはどうすればよいですか？」で説明されているステップに従います。
2. root パスワードでアカウントにサインインします。
3. AWS Billing コンソールで、アカウント設定ページに移動します。
4. その他の AWS アカウントの場合と同様に、[Account settings] (アカウント設定) で名前を変更します。
5. AWS Control Tower は、名前の変更を反映するように自動的に更新します。この更新は、 AWS Service Catalogのプロビジョニング済み製品には反映されません。

Amazon Virtual Private Cloud の設定を使用して Account Factory を構成する

Account Factory により、組織内のアカウントに対して、事前承認済みのベースラインと設定オプションを作成できます。 AWS Service Catalogを通じて新しいアカウントを設定し、プロビジョニングできます。

Account Factory ページには、組織単位 (OUs) とその許可リストのステータスのリストが表示されます。デフォルトでは、すべての OUsが許可リストに含まれます。つまり、アカウントは許可リストの下にプロビジョニングできます。アカウントプロビジョニングOUsの特定の を無効にすることができます AWS Service Catalog。

エンドユーザーが新しいアカウントをプロビジョニングするときに使用できる Amazon VPC設定オプションを表示できます。

Account Factory で Amazon VPC設定を構成するには

1. 中央クラウド管理者として、管理アカウントの管理者アクセス許可を使用して 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 アカウントに対して確立するVPC設定オプションを選択し、設定をフィールドに入力します。

- Amazon でパブリックサブネットを作成するには、無効または有効を選択しますVPC。デフォルトでは、インターネットにアクセス可能なサブネットは許可されません。

  > **Note**
  >
  > 新しいアカウントのプロビジョニング時にパブリックサブネットを有効にするように Account Factory VPC設定を設定すると、Account Factory はNATゲートウェイを作成するVPCように Amazon を設定します。Amazon によって使用量に対して課金されますVPC。詳細については、「VPC 料金表」を参照してください。

- リストから Amazon のプライベートサブネットの最大数VPCを選択します。デフォルトでは、[1] が選択されています。許可されるプライベートサブネットの最大数は、アベイラビリティーゾーンごとに 2 です。
- アカウントを作成するための IP アドレスの範囲を入力しますVPCs。値は、クラスレスドメイン間ルーティング (CIDR) ブロックの形式である必要があります (たとえば、デフォルトは)`172.31.0.0/16`。このCIDRブロックは、Account Factory VPCがアカウント用に作成する のサブネット IP アドレスの全体的な範囲を提供します。内ではVPC、サブネットは指定した範囲から自動的に割り当てられ、サイズは等しくなります。デフォルトでは、 内のサブネットは重複VPC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 VPCs のサブネット IP アドレス範囲は重複する可能性があります。

- アカウントがプロビジョニングされたVPCときに を作成する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 で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VPC。デフォルト値および推奨値は 3 です。
- [Save] を選択します。

これらの設定オプションを設定して、 を含まない新しいアカウントを作成できますVPC。詳しくは「チュートリアル」を参照してください。

アカウントを登録解除する

Account Factory でアカウントを作成したか、 を登録し AWS アカウント、そのアカウントを Control Tower によってランディングゾーンで管理する必要がなくなった場合は、AWSControl Tower AWS コンソールからアカウントを登録解除できます。

AWS Control Tower アカウントを登録解除すると、設計図を含め、AWSControl Tower によってプロビジョニングされたすべてのリソースが削除されます。アカウントは AWS Control Tower OU からルートエリアに移動されます。アカウントは登録された OU の一部ではなくなり、AWSControl Tower の対象外になりますSCPs。アカウントは、 AWS Organizationsから解約できます。

アカウントの登録解除は、プロビジョニング済み製品を終了することで、`AWSAccountFactory`グループ内の IAM Identity Center ユーザーが Service Catalog コンソールで実行することもできます。IAM Identity Center のユーザーまたはグループの詳細については、「ユーザーとアクセスの管理 AWS IAM Identity Center」を参照してください。Service Catalog でメンバーアカウントを登録解除する手順を以下に説明します。

登録済みアカウントを登録解除するには

1. ウェブブラウザで Service Catalog コンソール (https://console.aws.amazon.com/servicecatalog) を開きます。
2. 左のナビゲーションペインで [Provisioned products list] (プロビジョニング済み製品リスト) を選択します。
3. プロビジョニングされたアカウントのリストから、AWSControl Tower で管理しなくなったアカウントの名前を選択します。
4. [Provisioned product details] (プロビジョニングされた製品の詳細) ページの [Actions] (アクション) メニューから、[Terminate] (終了) を選択します。
5. 表示されるダイアログボックスで [Terminate] (終了) を選択します。

> **Important**
>
> terminate (終了) という単語は Service Catalog に固有のものです。Service Catalog Account Factory でアカウントを終了しても、アカウントは解約されません。このアクションにより、アカウントの OU およびランディングゾーンからアカウントが削除されます。

6. アカウントが登録解除されると、ステータスが [未登録] に変わります。
7. このアカウントが不要になった場合は、解約します。 AWS アカウントの閉鎖の詳細については、「 AWS Billing ユーザーガイド」の「アカウントの閉鎖」を参照してください。

カスタマイズされたアカウントを登録解除すると、AWSControl Tower はブループリントがデプロイしたリソースと、AWSControl Tower がアカウント内で作成したその他のリソースを削除します。アカウントを登録解除した後、 AWS Organizationsからアカウントを解約できます。

> **Note**
>
> 登録解除されたアカウントは解約も削除もされていません。アカウントが登録されていない場合でも、Account Factory でアカウントを作成したときに選択した IAM Identity Center ユーザーは、そのアカウントへの管理アクセス権を保持します。このユーザーに管理アクセスを許可しない場合は、Account Factory でアカウントを更新し、アカウントの IAM Identity Center ユーザーの E メールアドレスを変更して、 IAM Identity Center でこの設定を変更する必要があります。詳細については、「AWS Control Tower または を使用して Account Factory アカウントを更新および移動する AWS Service Catalog」を参照してください。

動画チュートリアル

この動画 (3:25) では、AWSControl Tower からアカウントを削除し、そのアカウントへのルートアクセスを取得して、最後に を閉鎖する方法について説明します AWS アカウント。を使用してアカウントを AWS Organizations API閉鎖することもできます。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

AWS Control Tower でアカウントを閉鎖するビデオチュートリアル。

AWS Control Tower の一般的なタスクを説明する AWS YouTube ビデオのリストを表示できます。

Account Factory で作成されたアカウントを解約する

Account Factory で作成されたアカウントは です AWS アカウント。 AWS アカウントの解約の詳細については、「AWS Account Management Reference Guide」の「Closing an account」を参照してください。

> **Note**
>
> の閉鎖 AWS アカウント は、AWSControl Tower からアカウントを登録解除するのと同じではありません。これらは個別のアクションです。アカウントを解約する前に、アカウントを登録解除する必要があります。

を使用して AWS Control Tower メンバーアカウントを閉鎖する AWS Organizations

ルート認証情報を使用して各メンバーアカウントに個別にサインインする必要なく、組織の管理アカウントから AWS Control Tower メンバーアカウントを閉鎖できます AWS Organizations。ただし、この方法で管理アカウントを解約することはできません。

を呼び出すとき AWS Organizations CloseAccount API、または AWS Organizations コンソールでアカウントを閉鎖すると、メンバーアカウントは AWS アカウント 90 日間分離されます。アカウントは、AWSControl Tower と に停止ステータスを表示します AWS Organizations。その 90 日間にアカウントを使用しようとすると、AWSControl Tower はエラーメッセージを表示します。

90 日が経過する前に、メンバーアカウントを復元できます AWS アカウント。90 日が過ぎると、アカウントのレコードは削除されます。

ベストプラクティスとして、メンバーアカウントを解約する前に、そのアカウントを登録解除することをお勧めします。メンバーアカウントを最初に管理解除せずに閉鎖すると、AWSControl Tower はアカウントのステータスを一時停止として表示しますが、登録済みとして表示します。その結果、その 90 日間にアカウントの OU を再登録しようとすると、AWSControl Tower はエラーメッセージを生成します。停止中のアカウントは、基本的に、事前チェックに失敗した再登録アクションをブロックします。OU からアカウントを削除すると、OU を再登録できますが、アカウントの支払い方法がないとエラーが発生する AWS 可能性があります。この制約を回避するには、別の OU を作成し、この OU にアカウントを移動してから再登録を試みます。この OU の名前は、Suspended OU とすることをお勧めします。

> **Note**
>
> アカウントを解約する前に登録を解除しない場合は、その 90 日が AWS Service Catalog 経過した後に、 でアカウントのプロビジョニング済み製品を削除する必要があります。

詳細については、 に関する AWS Organizations ドキュメントを参照してください。 CloseAccount API.

Account Factory のリソースに関する考慮事項

アカウントが Account Factory でプロビジョニングされると、アカウント内に次の AWS リソースが作成されます。

AWS サービス	リソースタイプ	リソース名
AWS CloudFormation	スタック	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	追跡	aws-controltower-BaselineCloudTrail

AWS サービス	リソースタイプ	リソース名
Amazon CloudWatch	CloudWatch イベントルール	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch ログ	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

AWS サービス	リソースタイプ	リソース名
Amazon EventBridge	ルール	AWSControlTowerManagedRule
Amazon EventBridge	ルール	aws-controltower-ConfigComplianceChangeEventRule

Account Factory Customization を使用してアカウントをカスタマイズする (AFC)

AWS Control Tower では、Control Tower コンソールからリソースをプロビジョニング AWS アカウント するときに、新規および既存の AWS をカスタマイズできます。Account Factory のカスタマイズを設定すると、AWSControl Tower は今後のプロビジョニングのためにこのプロセスを自動化するため、パイプラインを維持する必要はありません。カスタマイズされたアカウントは、リソースがプロビジョニングされるとすぐに使用できます。

カスタマイズされたアカウントは、Account Factory、 AWS CloudFormation テンプレート、または Terraform を使用してプロビジョニングされます。カスタマイズされたアカウントのブループリントとして機能するテンプレートは、ユーザーが定義します。ブループリントでは、アカウントのプロビジョニング時に必要な特定のリソースと設定が記述されています。 AWS パートナーによって構築および管理される事前定義された設計図も利用できます。パートナーが管理するブループリントの詳細については、「AWS Service Catalog 入門ライブラリ」を参照してください。

> **Note**
>
> AWS Control Tower には、Control Tower の AWS CloudFormation リソースをモニタリングするプロアクティブAWSコントロールが含まれています。オプションで、これらのコントロールをランディングゾーンでアクティブ化できます。プロアクティブコントロールを適用すると、アカウントにデプロイするリソースが組織のポリシーと手順に準拠しているかどうかがチェックされます。プロアクティブコントロールの詳細については、「Proactive controls」を参照してください。

アカウントのブループリントは に保存されます。このため AWS アカウント、ハブアカウントと呼ばれます。ブループリントは Service Catalog 製品の形式で保存されます。他の Service Catalog 製

品と区別するために、この製品をブループリントと呼びます。Service Catalog 製品の作成方法の詳細については、「AWS Service Catalog 管理者ガイド」の「製品の作成」を参照してください。

既存のアカウントにブループリントを適用

AWS Control Tower コンソールのアカウントの更新ステップに従って、カスタマイズされたブループリントを既存のアカウントに適用することもできます。詳細については、「コンソールでアカウントを更新する」を参照してください。

> [開始する前に]
>
> AWS Control Tower Account Factory でカスタマイズされたアカウントの作成を開始する前に、AWSControl Tower ランディングゾーン環境をデプロイし、新しく作成されたアカウントが配置される Control Tower に登録された組織単位 (OU) AWS が必要です。

の操作の詳細についてはAFC、AWS「Control Tower の Account Factory Customization を使用してアカウントのカスタマイズを自動化する」を参照してください。

カスタマイズの準備

- ハブアカウントとして機能する新しいアカウントを作成することも、既存のアカウントを使用することもできます AWS アカウント。AWS Control Tower 管理アカウントをブループリントハブアカウントとして使用しないことを強くお勧めします。
- AWS Control Tower AWS アカウント に登録してカスタマイズする場合は、まず AWS Control Tower に登録する他のアカウントと同様に、それらのアカウントにAWSControlTowerExecutionロールを追加する必要があります。
- Marketplace サブスクリプション要件があるパートナーブループリントを使用する場合は、パートナーブループリントを Account Factory カスタマイズブループリントとしてデプロイする前に、AWSControl Tower 管理アカウントからこれらを設定する必要があります。

トピック

- カスタマイズのための設定
- ブループリントからカスタマイズされたアカウントを作成する
- アカウントを登録およびカスタマイズする
- AWS Control Tower アカウントにブループリントを追加する
- ブループリントを更新する

- アカウントからブループリントを削除する
- パートナーのブループリント
- Account Factory のカスタマイズに関する考慮事項 (AFC)
- ブループリントエラーが発生した場合
- に基づくAFC設計図のポリシードキュメントのカスタマイズ CloudFormation
- Terraform ベースの Service Catalog 製品の作成に必要な追加のアクセス許可

カスタマイズのための設定

次のセクションでは、カスタマイズプロセスのために Account Factory を設定する手順について説明します。これらの手順を開始する前に、ハブアカウントを委任管理者として設定することをお勧めします。

概要

- ステップ 1. 必要なロールを作成します。ブループリントとも呼ばれる Service Catalog 製品が保存されている (ハブ) アカウントへのアクセス許可を AWS Control Tower に付与する IAMロールを作成します。
- ステップ 2. AWS Service Catalog 製品を作成します。カスタムアカウントのベースライン化に必要な AWS Service Catalog 製品 (「ブループリント製品」とも呼ばれます) を作成します。
- ステップ 3 カスタムブループリントを確認します。作成した AWS Service Catalog 製品 (ブループリント) を検査します。
- ステップ 4。ブループリントを呼び出して、カスタマイズされたアカウントを作成します。アカウントの作成時に、AWSControl Tower コンソールの Account Factory の適切なフィールドに、設計図の製品情報とロール情報を入力します。

ステップ 1. 必要なロールを作成する

アカウントのカスタマイズを開始する前に、AWSControl Tower とハブアカウント間の信頼関係を含むロールを設定する必要があります。引き受けると、ロールは AWS Control Tower にハブアカウントを管理するためのアクセスを許可します。ロールには という名前を付ける必要がありますAWSControlTowerBlueprintAccess。

AWS Control Tower は、このロールを引き受けて、ユーザーに代わってポートフォリオリソースを作成し AWS Service Catalog、設計図を Service Catalog 製品としてこのポートフォリオに追加し、アカウントプロビジョニング中にこのポートフォリオと設計図をメンバーアカウントと共有します。

以下のセクションの説明に従って、AWSControlTowerBlueprintAccess ロールを作成します。

IAM コンソールに移動して、必要なロールを設定します。

登録済みの AWS Control Tower アカウントでロールを設定するには

1. AWS Control Tower 管理アカウントのプリンシパルとしてフェデレーションまたはサインインします。
2. 管理アカウントのフェデレーティッドプリンシパルから、ブループリントハブアカウントとして機能するように選択した登録済み AWS Control Tower アカウントのAWSControlTowerExecutionロールを引き受けるか、ロールを切り替えます。
3. 登録された AWS Control Tower アカウントのAWSControlTowerExecutionロールから、適切なアクセス許可と信頼関係を持つAWSControlTowerBlueprintAccessロールを作成します。

Note

AWS ベストプラクティスのガイダンスに準拠するには、AWSControlTowerExecutionロールの作成直後にAWSControlTowerBlueprintAccessロールからサインアウトすることが重要です。リソースへの意図しない変更を防ぐため、AWSControlTowerExecutionロールは AWS Control Tower でのみ使用することを目的としています。

ブループリントハブアカウントが AWS Control Tower に登録されていない場合、AWSControlTowerExecutionロールはアカウントに存在しないため、ロールの設定を続行する前にAWSControlTowerBlueprintAccessロールを引き受ける必要はありません。

未登録のメンバーアカウントでロールを設定するには

1. 推奨されている方法で、ハブアカウントとして指定したいアカウントにプリンシパルとしてフェデレートまたはサインインします。
2. アカウントにプリンシパルとしてログインしたら、適切な権限と信頼関係を持つ AWSControlTowerBlueprintAccess ロールを作成します。

AWSControlTowerBlueprintAccess ロールは、次の 2 つのプリンシパルに信頼を付与するように設定する必要があります。

- AWS Control Tower 管理アカウントで Control Tower AWS を実行するプリンシパル (ユーザー) 。
- AWS Control Tower 管理アカウントAWSControlTowerAdminで という名前のロール。

次に信頼ポリシーの例を示します。これは、ロールに含める必要があるポリシーと似ています。このポリシーは、最小特権アクセスの付与のベストプラクティスを示しています。独自のポリシーを作成するときは、 という用語を AWS Control Tower 管理アカウントの実際のアカウント ID *YourManagementAccountId*に置き換え、 *YourControlTowerUserRole*という用語を管理アカウントのIAMロールの識別子に置き換えます。

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

必要なアクセス許可ポリシー

AWS Control Tower では、 という名前の管理ポリシーをAWSControlTowerBlueprintAccessロールにアタッチAWSServiceCatalogAdminFullAccessする必要があります。このポリシーは、AWSControl Tower がポートフォリオと AWS Service Catalog 製品リソースを管理できるようにするときに AWS Service Catalog が探すアクセス許可を提供します。IAM コンソールでロールを作成するときに、このポリシーをアタッチできます。

追加のアクセス許可が必要な場合があります

- ブループリントを Amazon S3 に保存する場合、AWSControl Tower にはAWSControlTowerBlueprintAccessロールのAmazonS3ReadOnlyAccessアクセス許可ポリシーも必要です。
- デフォルトの管理者IAMポリシーを使用しない場合、 AWS Service Catalog Terraform タイプの製品では、AFCカスタムポリシーにいくつかのアクセス許可を追加する必要があります。Terraform テンプレートで定義するリソースを作成するために必要なアクセス許可に加えて、これらが必要です。

ステップ 2. AWS Service Catalog 製品を作成する

AWS Service Catalog 製品を作成するには、「 AWS Service Catalog 管理者ガイド」の「製品の作成」の手順に従います。 AWS Service Catalog 製品を作成するときに、アカウントのブループリントをテンプレートとして追加します。

Important

Terraform のライセンス HashiCorpが更新され、Terraform Open Source 製品とプロビジョニング済み製品のサポートが External という新しい製品タイプ AWS Service Catalog に変更されました。既存のアカウントのブループリントを External 製品タイプに更新する方法など AFC、この変更が に与える影響の詳細については、「外部製品タイプへの移行」を参照してください。

ブループリントを作成する手順の概要

- アカウントのブループリントとなる AWS CloudFormation テンプレートまたは Terraform tar.gz 設定ファイルを作成またはダウンロードします。いくつかのテンプレートの例については、このセクションの後半に示します。
- Account Factory ブループリント AWS アカウント を保存する にサインインします (ハブアカウントと呼ばれることもあります) 。
- AWS Service Catalog コンソールに移動します。次に、[Product list] (製品リスト) を選択し、[Upload new product] (新しい製品をアップロード) を選択します。
- [Product details] (製品詳細) ペインに、名前や説明など、ブループリント製品の詳細を入力します。

- [Use a template file] (テンプレートファイルの使用)、[Choose file] (ファイルの選択) の順に選択します。ブループリントとして使用するために作成またはダウンロードしたテンプレートや設定ファイルを選択または貼り付けます。
- コンソールページの下部にある [Create product] (製品を作成する) を選択します。

テンプレートは、 AWS Service Catalog リファレンスアーキテクチャリポジトリ AWS CloudFormation からダウンロードできます。そのリポジトリの例は、リソースのバックアッププランを設定するのに役立ちます。

以下は、Best Pets という架空の会社向けのテンプレートの例です。これは、ペットのデータベースへの接続を設定するのに役立ちます。

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
 Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs16.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
```

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

  ConnectionString:
    Type: Custom::ConnectionStringGenerator
    Properties:
      ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

  PetDatabaseConnectionString:
    DependsOn: ConnectionString
    # For example purposes we're using SSM parameter store.
    # In your template, use secure alternatives to store
    # sensitive values such as connection strings.
    Type: AWS::SSM::Parameter
    Properties:
      Name: pet-database-connection-string
      Description: Connection information for the BestPets pet database
      Type: String
      Value: !GetAtt ConnectionString.Value
```

ステップ 3. カスタムブループリントを確認する

ブループリントは AWS Service Catalog コンソールで表示できます。詳細については、「Service Catalog 管理者ガイド」の「製品の管理」を参照してください。

ステップ 4. ブループリントを呼び出して、カスタマイズされたアカウントを作成する

AWS Control Tower コンソールでアカウントの作成ワークフローに従うと、オプションの セクションが表示され、アカウントのカスタマイズに使用するブループリントに関する情報を入力できます。

> **Note**
>
> AWS Control Tower コンソールにその情報を入力してカスタマイズされたアカウントのプロビジョニングを開始する前に、カスタマイズハブアカウントを設定し、少なくとも 1 つのブループリント (Service Catalog 製品) を追加する必要があります。

AWS Control Tower コンソールでカスタマイズされたアカウントを作成または更新します。

1. ブループリントを含んでいるアカウントのアカウント ID を入力します。
2. そのアカウントから、既存の Service Catalog 製品 (既存のブループリント) を選択します。
3. 複数のバージョンのブループリント (Service Catalog 製品) がある場合は、適切なバージョンを選択します。
4. (オプション) プロセスのこの時点で、ブループリントプロビジョニングポリシーを追加または変更できます。ブループリントプロビジョニングポリシーは で記述JSONされ、 IAMロールにアタッチされるため、ブループリントテンプレートで指定されたリソースをプロビジョニングできます。 AWSControl Tower は、Service Catalog が AWS CloudFormation スタックセットを使用してリソースをデプロイできるように、メンバーアカウントにこのロールを作成します。ロールの名前は `AWSControlTower-BlueprintExecution-bp-xxxx` です。デフォルトでは、`AdministratorAccess` ポリシーがここに適用されます。
5. この設計図に基づいて、アカウントをデプロイする AWS リージョン または リージョンを選択します。
6. 設計図にパラメータが含まれている場合は、パラメータの値を AWS Control Tower ワークフローの追加フィールドに入力できます。追加の値には、 GitHub リポジトリ名、 GitHub ブランチ、Amazon ECSクラスター名、リポジトリ所有者の GitHub ID などがあります。
7. ハブアカウントまたはブループリントの準備がまだ整っていない場合は、アカウントの更新プロセスに従って後からアカウントをカスタマイズできます。

詳細については、ブループリントからカスタマイズされたアカウントを作成するを参照してください。

ブループリントからカスタマイズされたアカウントを作成する

カスタムブループリントを作成したら、AWSControl Tower Account Factory でカスタムアカウントの作成を開始できます。

新しい AWS アカウントを作成する場合、次の手順に従ってカスタムブループリントをデプロイします。

1. の AWS Control Tower に移動します AWS Management Console。
2. [Account Factory] と [Create account] (アカウントの作成) を選択します。
3. アカウント名や E メールアドレスなどのアカウントの詳細を入力します。
4. E メールアドレスとユーザー名を使用して IAM Identity Center の詳細を設定します。

5. アカウントが追加される登録済みの OU を選択します。
6. [Account Factory Customization] セクションを展開します。
7. Service Catalog 製品が含まれているブループリントハブアカウントのアカウント ID を入力し、[Validate] (検証) を選択します。ブループリントハブアカウントの詳細については、「Account Factory Customization を使用してアカウントをカスタマイズする (AFC)」を参照してください。
8. Service Catalog 製品リスト (すべてのカスタムブループリント、パートナーブループリント) から、すべてのブループリントが含まれているドロップダウンメニューを選択します。ブループリントと対応するバージョンを選択してデプロイします。
9. ブループリントにパラメータが含まれている場合は、これらのフィールドが表示されて入力できます。事前にデフォルト値が入力されています。
10. 最後に、ブループリントをデプロイする場所を [Home Region] (ホームリージョン) または [All governed Regions] (すべての管理対象リージョン) から選択します。Route 53 や などのグローバルリソースはIAM、単一のリージョンにのみデプロイする必要がある場合があります。Amazon EC2インスタンスや Amazon S3 バケットなどのリージョンリソースは、すべての管理対象リージョンにデプロイできます。
11. すべてのフィールドに入力したら、[Create account] (アカウントの作成) を選択します。

> **Note**
>
> Terraform で作成されたブループリントは 1 つのリージョンにのみデプロイでき、複数のリージョンにはデプロイできません。

アカウントプロビジョニングの進捗状況は、[Organization] (組織) ページで確認できます。アカウントのプロビジョニングが完了すると、ブループリントで指定されたリソースはすでにそのアカウント内にデプロイされています。アカウントとブループリントの詳細を表示するには、[Account details] (アカウント詳細) ページに移動します。

アカウントを登録およびカスタマイズする

AWS Control Tower コンソールでアカウントを登録およびカスタマイズするには。

1. AWS Control Tower コンソールに移動し、左側のナビゲーションから Organization を選択します。

2. 使用可能なアカウントのリストが表示されます。カスタムブループリントを使用して登録するアカウントを特定します。そのアカウントの [State] (状態) 列に、[Not enrolled] (未登録) ステータスのアカウントが反映されています。
3. アカウントの左側にあるラジオボタンを選択し、画面右上の [Actions] (アクション) ドロップダウンメニューを選択します。ここで、[Enroll] (登録) オプションを選択します。
4. アクセス設定セクションにアカウントの IAM Identity Center 情報を入力します。
5. アカウントがメンバーとなる登録済みの OU を選択します。
6. アカウント作成手順の 7 ~ 12 と同じ手順を使用して、[Account Factory Customization] (Account Factory のカスタマイズ) セクションを完了します。詳細については、「 で Account Factory アカウントをプロビジョニングする AWS Service Catalog」を参照してください。

アカウントの進捗状況は、[Organization] (組織) ページで確認できます。アカウントの登録が完了すると、ブループリントで指定されたリソースはすでにそのアカウント内にデプロイされています。

AWS Control Tower アカウントにブループリントを追加する

既存の AWS Control Tower メンバーアカウントにブループリントを追加するには、AWSControl Tower コンソールのアカウントの更新ワークフローに従い、アカウントに追加する新しいブループリントを選択します。詳細については、AWS「Control Tower または で Account Factory アカウントを更新して移動する AWS Service Catalog」を参照してください。

> **Note**
>
> アカウントに新しいブループリントを追加すると、既存のブループリントは上書きされます。

> **Note**
>
> AWS Control Tower アカウントごとに 1 つのブループリントをデプロイできます。

ブループリントを更新する

以下の手順では、カスタムブループリントの更新方法とデプロイ方法について説明します。

カスタムブループリントを更新するには

1. AWS CloudFormation テンプレートまたは Terraform tar.gz ファイル (ブループリント) を新しい設定で更新します。
2. 更新したブループリントを新しいバージョンとして AWS Service Catalogに保存します。

更新したブループリントをデプロイするには

1. AWS Control Tower コンソールの Organization ページに移動します。
2. [Organization] (組織) ページをブループリント名とバージョンでフィルタリングします。
3. アカウントの更新プロセスに従い、アカウントに最新バージョンのブループリントをデプロイします。

ブループリントの更新に失敗した場合

AWS Control Tower は、プロビジョニングされた製品が AVAILABLE状態にあるときにブループリントの更新を許可します。プロビジョニングされた製品が TAINTED 状態である場合、更新は失敗します。次の回避策を推奨します。

1. AWS Service Catalog コンソールで、TAINTEDプロビジョニング済み製品を手動で更新して、状態を に変更しますAVAILABLE。詳細については、「プロビジョニングされた製品の更新」を参照してください。
2. 次に、AWSControl Tower のアカウント更新プロセスに従って、ブループリントのデプロイエラーを修正します。

この手動ステップを推奨する理由は、次のとおりです。ブループリントを削除すると、メンバーアカウントのリソースが削除される可能性があります。リソースの削除は、既存のワークロードに影響する場合があります。このため、特に実稼働ワークロードを実行している場合には、ブループリントを更新する別の方法 (元のブループリントを削除して置換する) ではなく、この方法をお勧めします。

アカウントからブループリントを削除する

アカウントからブループリントを削除するには、アカウントの更新ワークフローに従ってブループリントを削除し、そのアカウントを AWS Control Tower のデフォルト設定に戻します。

コンソールでアカウントの更新ワークフローを開始すると、アカウントの詳細がすべて入力されます。カスタマイズの詳細は入力されません。これらのAFC詳細を空白のままにすると、AWSControl

Tower はアカウントからブループリントを削除します。このとき、アクションが開始される前に、警告メッセージが表示されます。

> **Note**
>
> AWS Control Tower は、アカウントの作成またはアカウントの更新プロセス中にブループリントを選択した場合のみ、ブループリントをアカウントに追加します。

パートナーのブループリント

AWS Control Tower Account Factory Customization (AFC) は、 AWS パートナーによって構築および管理される事前定義されたカスタマイズブループリントへのアクセスを提供します。このようなパートナーブループリントは、特定のユースケースに合わせてアカウントをカスタマイズするのに役立ちます。各パートナーのブループリントは、特定のパートナーからの製品提供と連携するように事前に設定してカスタマイズされたアカウントの作成に役立ちます。

AWS Control Tower パートナーのブループリントの完全なリストを表示するには、コンソールの Service Catalog 入門ライブラリに移動します。AWS Control Tower ブループリントのソースタイプを検索します。

Account Factory のカスタマイズに関する考慮事項 (AFC)

- AFC は、単一の AWS Service Catalog ブループリント製品を使用したカスタマイズのみをサポートします。
- AWS Service Catalog ブループリント製品は、AWSハブアカウントと Control Tower ランディングゾーンのホームリージョンと同じリージョンに作成する必要があります。
- `AWSControlTowerBlueprintAccess` IAM ロールは、適切な名前、アクセス許可、および信頼ポリシーで作成する必要があります。
- AWS Control Tower は、設計図の 2 つのデプロイオプションをサポートしています。ホームリージョンにのみデプロイするか、AWSControl Tower によって管理されるすべてのリージョンにデプロイします。リージョンの選択はできません。
- メンバーアカウントのブループリントを更新すると、ブループリントハブアカウント ID と AWS Service Catalog ブループリント製品を変更することはできません。
- AWS Control Tower は、既存のブループリントの削除と、単一のブループリント更新オペレーションでの新しいブループリントの追加をサポートしていません。ブループリントを削除してから、別の操作で新しいブループリントを追加できます。

- AWS Control Tower は、カスタマイズされたアカウントを作成または登録しているか、カスタマイズされていないアカウントを作成または登録しているかに基づいて動作を変更します。カスタマイズされたアカウントをブループリントで作成または登録していない場合、AWSControl Tower は Control Tower 管理アカウントに Account Factory でプロビジョニングされた製品を (Service Catalog を介して) AWS 作成します。ブループリントを使用してアカウントを作成または登録するときにカスタマイズを指定している場合、AWSControl Tower は Control Tower 管理アカウントに Account Factory AWS でプロビジョニングされた製品を作成しません。

ブループリントエラーが発生した場合

ブループリントの適用中のエラー

AWS Control Tower に登録する新しいアカウントまたは既存のアカウントのいずれかにブループリントを適用するプロセス中にエラーが発生した場合、復旧手順は同じです。アカウントは存在しますが、カスタマイズされておらず、AWSControl Tower に登録されていません。続行するには、手順に従ってアカウントを AWS Control Tower に登録し、登録時にブループリントを追加します。

`AWSControlTowerBlueprintAccess` ロール作成中のエラーと回避策

AWS Control Tower アカウントから`AWSControlTowerBlueprintAccess`ロールを作成するときは、`AWSControlTowerExecution`ロールを使用してプリンシパルとしてサインインする必要があります。他の としてサインインしている場合、次のアーティファクトに示すようにSCP、`CreateRole` オペレーションは によって防止されます。

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
                        "arn:aws:iam::*:role/stacksets-exec-*"
                    ]
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
```

```
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-controltower-*",
                "arn:aws:iam::*:role/*AWSControlTower*",
                "arn:aws:iam::*:role/stacksets-exec-*"
            ],
            "Effect": "Deny",
            "Sid": "GRIAMROLEPOLICY"
        }
```

以下の回避策を使用できます。

- (最も推奨)AWSControlTowerExecution ロールを継承して、AWSControlTowerBlueprintAccess ロールを作成します。この回避策を選択した場合、リソースの意図しない変更を防ぐために、ロールの作成後すぐに AWSControlTowerExecution ロールからサインアウトしてください。
- AWS Control Tower に登録されていないため、この の対象ではないアカウントにサインインしますSCP。
- これを一時的に編集SCPして、 オペレーションを許可します。
- (強くお勧めしません) AWS Control Tower 管理アカウントをハブアカウントとして使用すると、の対象にはなりませんSCP。

に基づくAFC設計図のポリシードキュメントのカスタマイズ CloudFormation

Account Factory を通じてブループリントを有効にすると、AWSControl Tower は StackSet ユーザーに代わって を作成する AWS CloudFormation ように に指示します。 では、 でスタックを作成 AWS CloudFormation するために、マネージドアカウントへのアクセス AWS CloudFormation が必要です StackSet。には、 AWSControlTowerExecutionロールを通じてマネージドアカウントの管理者権限が AWS CloudFormation 既にありますが、このロールは によって引き受けることはできません AWS CloudFormation。

設計図の有効化の一環として、AWSControl Tower はメンバーアカウントにロールを作成します。このロールは、 が StackSet 管理タスクを完了するために引き受ける AWS CloudFormation 場合があ

ります。Account Factory を使用してカスタマイズ済みブループリントを有効にする最も簡単な方法は、allow-all ポリシーを使用することです。このようなポリシーはすべてのブループリントテンプレートと互換性があるためです。

ただし、ベストプラクティスでは、ターゲットアカウントの AWS CloudFormation のアクセス許可を制限する必要があることを提案しています。Control AWS Tower が作成するロールに適用して AWS CloudFormation 使用するためにカスタマイズされたポリシーを指定できます。例えば、設計図で何か重要なSSMパラメータを作成する場合は、次のポリシーを指定できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
}
```

`AllowCloudFormationActionsOnStacks` ステートメントはすべてのAFCカスタムポリシーに必要です。このロール AWS CloudFormation を使用してスタックインスタンスを作成するため、スタックで AWS CloudFormation アクションを実行するアクセス許可が必要です。`AllowSsmParameterActions` セクションは、有効になっているテンプレートに固有です。

権限に関する問題の解決

制限付きポリシーを使用してブループリントを有効にするとき、ブループリントを有効にする権限が不足していることがあります。このような問題を解決するには、ポリシードキュメントを改訂し、修正されたポリシーを使用するようにメンバーアカウントのブループリント設定を更新します。ポ

リシーが設計図を有効にするのに十分であることを確認するには、 AWS CloudFormation アクセス許可が付与されていること、およびそのロールを使用してスタックを直接作成できることを確認します。

Terraform ベースの Service Catalog 製品の作成に必要な追加のアクセス許可

の Terraform 設定ファイルを使用して AWS Service Catalog External 製品を作成する場合AFC、AWS Service Catalog では、テンプレートで定義されたリソースの作成に必要なアクセス許可に加えて、AFCカスタムIAMポリシーに特定のアクセス許可を追加する必要があります。デフォルトのフル Admin ポリシーを選択した場合は、これらの追加のアクセス許可を追加する必要はありません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

で External 製品タイプを使用して Terraform 製品を作成する方法の詳細については AWS Service Catalog、「Service Catalog 管理者ガイド」の「ステップ 5: 起動ロールを作成する」を参照してください。

AWS Control Tower Account Factory for Terraform (AFT) によるアカウントのプロビジョニング

AWS Control Tower Account Factory for Terraform (AFT) は、AWS Control Tower でのアカウントプロビジョニングとアカウント更新のプロセスを自動化する GitOps モデルを採用します。

> **Note**
>
> AFT は、AWS Control Tower のワークフローパフォーマンスに影響しません。Account Factory または AFT によってアカウントをプロビジョニングした場合、同じバックエンドワークフローが発生します。

AFT では、AFT ワークフローを呼び出す入力を含むアカウントリクエスト Terraform ファイルを作成します。AFT のワークフローは、AFT のアカウントプロビジョニングフレームワークとアカウントカスタマイズステップを実行します。

前提条件

AFT の使用を開始するときは、以下を作成します。

- AWS Control Tower で、AFT 環境の OU、次に AFT 管理アカウントを作成します。アカウント ID を書き留めておき、後で Terraform モジュールで AFT をデプロイするときに、`main.tf`ファイルに入力できるようにします。このアカウント ID は、AWS Control Tower Control の詳細ページで確認できます。詳細については、「Terraform のドキュメント」を参照してください。
- 完全にデプロイされた AFT 環境の `git` 1 つ以上のリポジトリ。詳細については、「Post-deployment steps for AFT」を参照してください。

- 完全にデプロイされた AFT 環境。詳細については、「AWS Control Tower Account Factory for Terraform (AFT) の概要」および「Deploy AWS Control Tower Account Factory for Terraform (AFT)」を参照してください。Terraform のドキュメントも参照してください。

> **Tip**
>
> AFT 管理アカウントは、アカウントの作成を使用して AWS Control Tower コンソールから作成できます。詳細については、「プロビジョニング方法」を参照してください。
> また、オプションで、アカウントテンプレートフォルダを作成して、aft-account-customizations リポジトリで追加のアカウントを定義することもできます。

AFT にデプロイの制限 AWS リージョン がある場所については、AWS Control Tower の制限とクォータ「」および「」を参照してくださいコントロールの制限事項。

Terraform ドキュメントには、AWS Control Tower Account Factory for Terraform (AFT) をセットアップする方法の概要が記載されています。

AFT による新しいアカウントのプロビジョニング

このセクションでは、AFT と AFT 管理アカウントが既に設定されており、追加のアカウントをプロビジョニングしていることを前提としています。

AFT で新しいアカウントをプロビジョニングするには、アカウントリクエストの Terraform ファイルを作成します。このファイルには、aft-account-request リポジトリ内のパラメータの入力が含まれています。アカウントリクエストの Terraform ファイルを作成したら、`git push` を実行してアカウントリクエストの処理を開始します。このコマンドは、 で `ct-aft-account-request`オペレーションを呼び出します。このオペレーションは AWS CodePipeline、アカウントのプロビジョニングが完了した後に AFT 管理アカウントで作成されます。詳細については、「AFT アカウントプロビジョニングパイプライン」を参照してください。

アカウントリクエスト Terraform ファイルのパラメータ

アカウントリクエストの Terraform ファイルには、次のパラメータを含める必要があります。アカウントリクエストの Terraform ファイルの例は GitHub で確認できます。

- `module name` の値は、 AWS アカウント リクエストごとに一意である必要があります。
- `module source` の値は、AFT が提供するアカウントリクエスト Terraform モジュールへのパスです。

- `control_tower_parameters` の値は、AWS Control Tower アカウントの作成に必要な入力をキャプチャします。値には次の入力フィールドが含まれます。
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> `control_tower_parameters` に対して入力した内容は、アカウントのプロビジョニング中に変更することはできません。
> aft-account-request リポジトリの `ManagedOrganizationalUnit` の指定にサポートされている形式には、 `OUName` および `OUName (OU-ID)` があります。

- `account_tags` は、ビジネス基準 AWS アカウント に従ってタグ付けできるユーザー定義のキーと値をキャプチャします。詳細については、 AWS Organizations ユーザーガイドの AWS Organizations リソースへのタグ付けを参照してください。
- `change_management_parameters` の値には、アカウントリクエストが作成された理由やアカウントリクエストを開始したユーザーなどの追加情報が含まれます。値には次の入力フィールドが含まれます。
  - `change_reason`
  - `change_requested_by`
- `custom_fields` は、/aft/account-request/custom-fields/ で発行されたアカウントに SSM パラメータとしてデプロイするキーと値を持つ追加メタデータをキャプチャします。アカウントのカスタマイズ中にこのメタデータを参照すると、適切なコントロールをデプロイできます。例えば、規制コンプライアンスの対象となるアカウントは、追加の をデプロイする場合があります AWS Config ルール。`custom_fields` で収集したメタデータは、アカウントのプロビジョニングおよび更新中に追加の処理を引き起こす可能性があります。アカウントリクエストからカスタムフィールドを削除すると、そのカスタムフィールドは発行されたアカウントの SSM パラメータストアから削除されます。

- (オプション) account_customizations_name は、aft-account-customizations リポジトリ内のアカウントテンプレートフォルダをキャプチャします。詳細については、「アカウントのカスタマイズ」を参照してください。

複数のアカウントリクエストの送信

AFT はアカウントリクエストを 1 つずつ処理しますが、AFT パイプラインには複数のアカウントリクエストを送信できます。AFT パイプラインに複数のアカウントリクエストを送信すると、AFT はアカウントリクエストを先入れ先出しの順序でキューに入れ、処理します。

> **Note**
>
> AFT がプロビジョニングするアカウントごとに 1 つのアカウントリクエスト Terraform ファイルを作成することも、1 つの Terraform ファイルに複数のリクエストをカスケードすることもできます。

既存のアカウントの更新

以前に送信されたアカウントリクエストを更新するして git push を実行することで、AFT がプロビジョニングしたアカウントを更新できます。このコマンドは、アカウントプロビジョニングワークフローを起動し、アカウント更新リクエストを処理できます。ManagedOrganizationalUnit の入力を更新できます。これは control_tower_parameters に必要な値の一部です。

ManagedOrganizationalUnit は、すべての control_tower_parameters の中で唯一の更新可能なパラメータです。ただし、custom_fields など、アカウントリクエストの Terraform ファイルに含まれるその他のパラメータは更新できます。詳細については、「AFT による新しいアカウントのプロビジョニング」を参照してください。

> **Note**
>
> control_tower_parameters に対して入力した内容は、アカウントのプロビジョニング中に変更することはできません。
> aft-account-request リポジトリの ManagedOrganizationalUnit の指定にサポートされている形式には、 OUName および OUName (OU-ID) があります。

AFT がプロビジョニングしていないアカウントを更新する

AFT の外部で作成された AWS Control Tower アカウントを更新するには、aft-account-request リポジトリにアカウントを指定します。

> **Note**
>
> すべてのアカウントの詳細が正しく、AWS Control Tower 組織およびそれぞれの AWS Service Catalog プロビジョニング済み製品と一致していることを確認します。

AFT AWS アカウント で既存の を更新するための前提条件

- は AWS Control Tower に登録 AWS アカウント する必要があります。
- は AWS Control Tower 組織の一部 AWS アカウント である必要があります。

AWS Control Tower Account Factory for Terraform (AFT) のデプロイ

このセクションは、既存の環境で Account Factory for Terraform (AFT) を設定する AWS Control Tower 環境の管理者を対象としています。ここでは、新しい専用の AFT 管理アカウントを使用して、Account Factory for Terraform (AFT) 環境を設定する方法について説明します。

> **Note**
>
> Terraform モジュールは AFT をデプロイします。このモジュールは GitHub の AFT リポジトリで入手可能で、AFT リポジトリ全体がモジュールと見なされます。
> AFT リポジトリのクローンを作成する代わりに、GitHub の AFT モジュールを参照することをお勧めします。これにより、モジュールが利用可能になったときにその更新を管理して使用することができます。

AWS Control Tower Account Factory for Terraform (AFT) 機能の最新リリースの詳細については、この GitHub リポジトリのリリースファイルを参照してください。

デプロイの前提条件

AFT 環境を設定して起動する前に、次のリソースを使用できる必要があります。

- AWS Control Tower ランディングゾーンのホームリージョン。詳細については、「AWS Control Tower で AWS リージョン を使用する方法」を参照してください。
- AWS Control Tower ランディングゾーン。詳細については、「AWS Control Tower のランディングゾーンを計画する」を参照してください。
- AFT 管理アカウント。AWS Control Tower でプロビジョニングすることも、他の方法でプロビジョニングして AWS Control Tower に登録することもできます。
- Terraform のバージョンとディストリビューション。詳細については、「Terraform と AFT のバージョン」を参照してください。
- コードやその他のファイルへの変更を追跡および管理するための VCS プロバイダー。デフォルトでは、AFT は を使用します AWS CodeCommit。詳細については、「 AWS CodeCommit ユーザーガイド」の「 とは AWS CodeCommit」を参照してください。

  AFT を初めてデプロイする場合に、既存の CodeCommit リポジトリがないときは、GitHub や BitBucket などの外部 VCS プロバイダーを選択する必要があります。詳細については、「Alternatives for version control of source code in AFT」を参照してください。
- AFT をインストールする Terraform モジュールを実行できるランタイム環境。
- AFT 機能のオプション。詳細については、「機能オプションを有効にする」を参照してください。

AWS Control Tower Account Factory for Terraform を設定して起動する

以下の手順は、Terraform のワークフローに精通していることを前提としています。また、AFT のデプロイの詳細については、 AWS Workshop Studio ウェブサイトの「AFT の概要」ラボを参照してください。

ステップ 1: AWS Control Tower ランディングゾーンを起動する

「AWS Control Tower の開始方法」のステップを完了します。ここで、AWS Control Tower 管理アカウントを作成し、AWS Control Tower ランディングゾーンを設定します。

> **Note**
>
> AdministratorAccess 認証情報を持つ AWS Control Tower 管理アカウントのロールを必ず作成してください。詳細については次を参照してください:
>
> - 「AWS Identity and Access Management IAM ユーザーガイド」の「IAM ID (ユーザー、ユーザーグループ、ロール)」

- 「AWS マネージドポリシーリファレンスガイド」の「AdministratorAccess」

ステップ 2: AFT 用の新しい組織単位を作成する (強く推奨)

AWS Control Tower ランディングゾーン に別の OU を作成することをお勧めします。この OU は、AFT 管理アカウントをプロビジョニングする場所です。AWS Control Tower 管理アカウントから新しい OU と AFT 管理アカウントを作成します。詳細については、「新しい OU を作成する」を参照してください。

ステップ 3: AFT 管理アカウントをプロビジョニングする

AFT では、AFT 管理オペレーション専用の AWS アカウントをプロビジョニングする必要があります。AWS Control Tower ランディングゾーンに関連付けられている AWS Control Tower 管理アカウントにサインインしたら、AFT 管理アカウントを作成します。AWS Control Tower コンソールから AFT 管理アカウントをプロビジョニングするには、組織ページでアカウントの作成を選択するか、その他の方法を選択します。詳細については、AWS Service Catalog 「Account Factory でアカウントをプロビジョニング」を参照してください。

> **Note**
>
> AFT 用に別の OU を作成した場合は、AFT 管理アカウントを作成するときに必ずこの OU を選択してください。

AFT 管理アカウントを完全にプロビジョニングするには、最大 30 分かかる場合があります。

ステップ 4: Terraform 環境がデプロイに使用可能であることを検証する

このステップは、Terraform の使用経験があり、Terraform を実行するための手順を適切に行っていることを前提としています。詳細については、HashiCorp Developer ウェブサイトの「Command: init」を参照してください。

> **Note**
>
> AFT は Terraform バージョン `1.6.0` 以降をサポートしています。

ステップ 5: Account Factory for Terraform モジュールを呼び出して AFT をデプロイする

AdministratorAccess 認証情報を持つ AWS Control Tower 管理アカウント用に作成したロールで、AFT モジュールを呼び出します。AWS Control Tower は、AWS Control Tower 管理アカウントを通じて、AWS Control Tower Account Factory リクエストをオーケストレーションするために必要なすべてのインフラストラクチャを確立する Terraform モジュールをプロビジョニングします。

GitHub の AFT リポジトリで AFT モジュールを表示できます。GitHub リポジトリ全体が AFT モジュールと見なされます。AFT モジュールの実行と AFT のデプロイに必要な入力については、README ファイルを参照してください。または、Terraform レジストリで AFT モジュールを表示することもできます。

AFT モジュールには、AWS Control Tower が中央 AFT 管理アカウントの仮想プライベートクラウド (VPC) 内にアカウントリソースをプロビジョニングするかどうかを指定する `aft_enable_vpc`パラメータが含まれています。デフォルトでは、パラメータは `true` に設定されています。このパラメータを `false` に設定すると、AWS Control Tower は VPC やプライベートネットワークリソース (NAT ゲートウェイや VPC エンドポイントなど) を使用せずに AFT をデプロイします。`aft_enable_vpc` を無効にすると、一部の使用パターンで AFT の運用コストを削減できる場合があります。

> **Note**
>
> `aft_enable_vpc` パラメータを再度有効にする (値を `false` から `true` に切り替える) には、`terraform apply` コマンドを 2 回連続して実行する必要があります。

環境で Terraform を管理するために確立されたパイプラインを持っている場合は、この AFT モジュールを既存のワークフローに統合できます。それ以外の場合は、必要な認証情報で認証された環境から AFT モジュールを実行します。

タイムアウトするとデプロイが失敗します。(AWS Security Token Service STS) 認証情報を使用して、完全なデプロイに十分なタイムアウトを確保することをお勧めします。 AWS STS 認証情報の最小タイムアウトは 60 分です。詳細については、「AWS Identity and Access Management ユーザーガイド」の「IAM の一時的な認証情報」を参照してください。

> **Note**
>
> AFT が Terraform モジュールを使用してデプロイを完了するまで最大 30 分かかる場合があります。

ステップ 6: Terraform 状態ファイルを管理する

AFT をデプロイすると、Terraform 状態ファイルが生成されます。このアーティファクトは、Terraform が作成したリソースの状態を記述します。AFT バージョンを更新する予定がある場合は、必ず Terraform 状態ファイルを保存するか、Amazon S3 と DynamoDB を使用して Terraform バックエンドをセットアップします。AFT モジュールはバックエンドの Terraform 状態を管理しません。

> **Note**
>
> Terraform 状態ファイルを保護するのはユーザーの責任です。一部の入力変数には、プライベートの ssh キーまたは Terraform トークンなどの機密値が含まれる場合があります。デプロイ方法によって、これらの値は Terraform 状態ファイルにプレーンテキストとして表示されることがあります。詳細については、HashiCorp ウェブサイトの「Sensitive data in State」を参照してください。

デプロイ後のステップ

AFT インフラストラクチャのデプロイが完了したら、次の追加ステップに従って設定プロセスを完了し、アカウントをプロビジョニングする準備を整えます。

ステップ 1: 目的の VCS プロバイダーとの CodeConnection を完了する

サードパーティーの VCS プロバイダーを選択した場合、AFT によって CodeConnection が確立されるので、その CodeConnection を確認します。希望する VCS を使用して AFT を設定する方法については、「でのソースコードのバージョン管理の代替方法 AFT」を参照してください。

AWS CodeStar 接続を確立する最初のステップは、AFT によって行われます。接続を確認する必要があります。

ステップ 2: 各リポジトリを設定する

AFT では、次の 4 つのリポジトリを管理する必要があります。

1. アカウントリクエスト — このリポジトリは、アカウントリクエストの配置または更新を処理します。使用可能な例。AFT アカウントリクエストの詳細については、「AFT による新しいアカウントのプロビジョニング」を参照してください。
2. AFT アカウントプロビジョニングのカスタマイズ — このリポジトリは、グローバルカスタマイズステージを開始する前に、AFT で作成され、管理されるすべてのアカウントに適用されるカスタ

マイズを管理します。使用可能な例。AFT アカウントプロビジョニングのカスタマイズを作成するには、「AFT アカウントプロビジョニングのカスタマイズステートマシンを作成する」を参照してください。

3. グローバルカスタマイズ — このリポジトリは、AFT で作成され、管理されるすべてのアカウントに適用されるカスタマイズを管理します。使用可能な例。AFT グローバルカスタマイズを作成するには、「グローバルカスタマイズの適用」を参照してください。
4. アカウントのカスタマイズ — このリポジトリは、AFT で作成され、管理される特定のアカウントにのみ適用されるカスタマイズを管理します。使用可能な例。AFT アカウントのカスタマイズを作成するには、「アカウントカスタマイズの適用」を参照してください。

AFT は、これらの各リポジトリが特定のディレクトリ構造に従うことを期待しています。リポジトリの入力に使用されるテンプレート、およびそれらのテンプレートの設定方法については、AFT GitHub リポジトリの Account Factory for Terraform モジュールで入手できます。

AWS Control Tower Account Factory for Terraform の概要 (AFT)

Account Factory for Terraform (AFT) は、AWSControl Tower でのアカウントのプロビジョニングとカスタマイズに役立つ Terraform パイプラインを設定します。 AFTは、AWSControl Tower でアカウントを管理できると同時に、Terraform ベースのアカウントプロビジョニングの利点を提供します。

AFT では、アカウントリクエスト Terraform ファイルを作成して、アカウントプロビジョニングのAFTワークフローをトリガーする入力を取得します。アカウントプロビジョニングステージが完了すると、 はアカウントカスタマイズステージが始まる前に一連のステップAFTを自動的に実行します。詳細については、AFT「 アカウントプロビジョニングパイプライン」を参照してください。

AFT は、Terraform Cloud、Terraform Enterprise、および Terraform Community Edition をサポートしています。AFT を使用すると、入力ファイルとシンプルな`git push`コマンドを使用してアカウントの作成を開始し、新規または既存のアカウントをカスタマイズできます。アカウントの作成には、組織の標準的なセキュリティ手順とコンプライアンスガイドラインを満たすのに役立つ AWS Control Tower ガバナンスの利点とアカウントカスタマイズがすべて含まれています。

AFT は、アカウントカスタマイズリクエストのトレースをサポートします。アカウントカスタマイズリクエストを送信するたびに、 はAFTカスタマイズ AWS Step Functions ステートマシンを通過する一意のトレーストークンAFTを生成します。このステートマシンは、トークンを実行の一部としてログに記録します。その後、Amazon CloudWatch Logs Insights クエリを使用してタイムスタンプ範囲を検索し、リクエストトークンを取得できます。その結果、トークンに付随するペイロードが表示されるため、AFTワークフロー全体でアカウントのカスタマイズリクエストを追跡できます。CloudWatch ログと Step Functions の詳細については、以下を参照してください。

- 「Amazon CloudWatch Logs ユーザーガイド」の「Amazon CloudWatch Logs とは」
- 「AWS Step Functions デベロッパーガイド」の「AWS Step Functionsの概要」

AFT はコンポーネントサービス、他の AWS サービスの機能を として組み合わせ、Terraform Infrastructure as Code (IaC) をデプロイするパイプラインを使用してフレームワークを構築します。AFTを使用すると、次のことが可能になります。

- GitOps モデルでアカウントのプロビジョニングリクエストと更新リクエストを送信する
- アカウントのメタデータと監査履歴を保存する
- アカウントレベルのタグを適用する
- すべてのアカウント、一連のアカウント、または個々のアカウントにカスタマイズを追加する
- 機能オプションの有効化

AFT は、管理アカウントと呼ばれる別のAFTアカウントを作成し、AFT機能をデプロイします。を設定する前にAFT、既存の AWS Control Tower ランディングゾーンが必要です。AFT 管理アカウントは Control Tower AWS 管理アカウントと同じではありません。

AFT に柔軟性を提供

- プラットフォームの柔軟性： は、Community Edition、Cloud、Enterprise の初回デプロイと継続的な運用のために Terraform ディストリビューションAFTをサポートします。
- バージョン管理システムの柔軟性： は AWS CodeCommit、 および を介した代替バージョン管理ソースAFTをサポートします AWS CodeConnections。

AFT の機能オプションを提供

ベストプラクティスに基づいて、いくつかの機能オプションを有効にできます。

- データイベントを ログ記録 CloudTrail するための組織レベルの作成
- VPC アカウントの AWS デフォルトを削除する
- プロビジョニングされたアカウントを AWS エンタープライズサポートプランに登録する

> **Note**
>
> AFT パイプラインは、アカウントがアプリケーションを実行するために必要な Amazon EC2インスタンスなどの リソースのデプロイでの使用を目的としていません。これ

は、AWSControl Tower アカウントの自動プロビジョニングとカスタマイズのみを目的としています。

動画チュートリアル

このビデオ (7:33) では、AWSControl Tower Account Factory for Terraform を使用してアカウントをデプロイする方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

AWS Control Tower での自動アカウントプロビジョニングのビデオチュートリアル。

AFT アーキテクチャ

オペレーションの順序

AFT 管理アカウントでAFTオペレーションを実行します。完全なアカウントプロビジョニングワークフローの場合、図表の左から右に示されているステージの順序は次のとおりです。

1. アカウントリクエストが作成され、パイプラインに送信されます。一度に複数のアカウントリクエストを作成して送信できます。Account Factory はリクエストを first-in-first-out順番に処理します。詳細については、「複数のアカウントリクエストを送信する」を参照してください。
2. 各アカウントがプロビジョニングされます。このステージは AWS Control Tower 管理アカウントで実行されます。
3. グローバルカスタマイズは、発行された各アカウントごとに作成されたパイプラインで実行されます。
4. 最初のアカウントプロビジョニングリクエストでカスタマイズが指定されている場合、カスタマイズは対象アカウントでのみ実行されます。アカウントが既にプロビジョニングされている場合は、そのアカウントのパイプラインでさらにカスタマイズを手動で開始する必要があります。

AWS Control Tower Account Factory for Terraform – アカウントプロビジョニングワークフロー

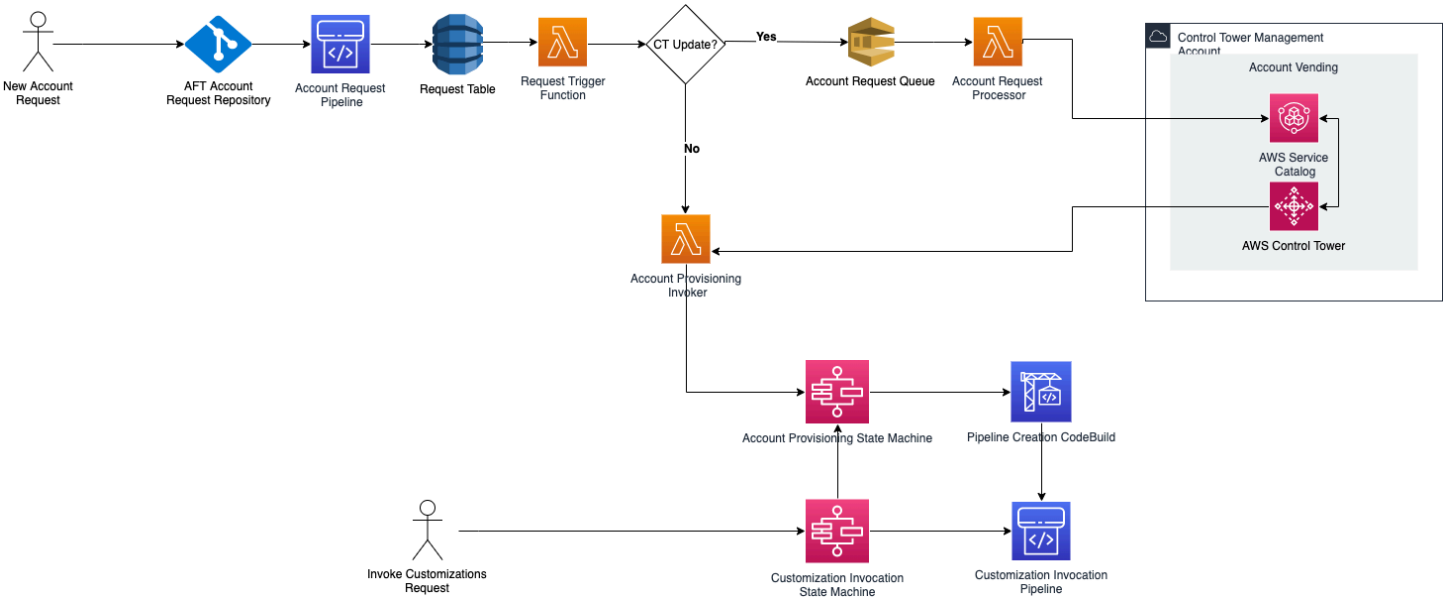

図 1: AWS Control Tower Account Factory for Terraform

コスト

には追加料金はかかりませんAFT。によってデプロイされたリソースAFT、 によって有効化された AWS サービスAFT、およびAFT環境にデプロイしたリソースに対してのみ料金が発生します。

AFT デフォルト設定には、データ保護とセキュリティを強化するための AWS PrivateLink エンドポイントの割り当て、および のサポートに必要なNATゲートウェイが含まれます AWS CodeBuild。このインフラストラクチャの料金の詳細については、Gateway のAWS PrivateLink 料金と Amazon の料金を参照してください。 VPC NAT これらのコストの管理の詳細については、 AWS アカウント担当者にお問い合わせください。これらのデフォルト設定は で変更できますAFT。

Terraform および AFTバージョン

Account Factory for Terraform (AFT) は Terraform バージョン `1.6.0` 以降をサポートしています。次の例に示すように、AFTデプロイプロセスの入力パラメータとして Terraform バージョンを指定する必要があります。

```
terraform_version = "1.6.0"
```

Terraform ディストリビューション

AFT は 3 つの Terraform ディストリビューションをサポートしています。

- Terraform Community Edition
- Terraform Cloud
- Terraform Enterprise

これらのディストリビューションについては、以降のセクションで説明します。AFT ブートストラッププロセス中に、選択した Terraform ディストリビューションを入力パラメータとして指定します。AFT デプロイと入力パラメータの詳細については、AWS Control Tower Account Factory for Terraform (AFT) のデプロイ「」を参照してください。

Terraform Cloud または Terraform Enterprise ディストリビューションを選択した場合、 に指定するAPIトークンはユーザートークンまたはチームAPIトークンterraform_token である必要があります。組織トークンは、必要なすべての でサポートされているわけではありませんAPIs。セキュリティ上の理由から、次の例に示すように、Terraform 変数を割り当てることで、このトークンの値をバージョン管理システム (VCS) にチェックインしないようにする必要があります。

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

Terraform Community Edition

ディストリビューションとして Terraform Community Edition を選択すると、 はAFT管理アカウントで Terraform バックエンドAFTを管理します。 はterraform-cli、指定された Terraform バージョンの AFTをダウンロードして、AFTデプロイフェーズとAFTパイプラインフェーズで実行します。結果の Terraform 状態設定は、次の形式の名前で Simple Storage Service (Amazon S3) バケットに格納されます。

```
aft-backend-[account_id]-primary-region
```

AFT は、災害対策 AWS リージョンの目的で、別の に Terraform 状態設定をレプリケートする Amazon S3 バケットも作成します。名前は次の形式で指定します。

```
aft-backend-[account_id]-secondary-region
```

これらの Terraform 状態の Amazon S3 バケットの削除関数には、多要素認証 (MFA) を有効にすることをお勧めします。 Amazon S3 Terraform Community Edition の詳細については、Terraform のドキュメントを参照してください。

ディストリビューションOSSとして Terraform を選択するには、次の入力パラメータを指定します。

```
terraform_distribution = "oss"
```

Terraform Cloud

ディストリビューションとして Terraform Cloud を選択すると、 は Terraform Cloud 組織に以下のコンポーネントのワークスペースAFTを作成し、 主導APIのワークフローを開始します。

- アカウントリクエスト
- AFT がAFTプロビジョニングするアカウントのカスタマイズ
- がAFTプロビジョニングするアカウントのアカウントカスタマイズ
- がAFTプロビジョニングするアカウントのグローバルカスタマイズ

Terraform Cloud が、結果の Terraform の状態設定を管理します。

ディストリビューションとして Terraform Cloud を選択するときは、次の入力パラメータを指定します。

- `terraform_distribution = "tfc"`
- `terraform_token` – このパラメータには Terraform Cloud トークンの値が含まれています。 は を機密としてAFTマークし、その値をAFT管理アカウントのSSMパラメータストアに安全な文字列として保存します。会社のセキュリティポリシーとコンプライアンスガイドラインに従って、Terraform トークンの値を定期的にローテーションすることをお勧めします。Terraform トークンは、ユーザーまたはチームレベルのAPIトークンである必要があります。組織トークンはサポートされていません。
- `terraform_org_name` — このパラメータには、Terraform Cloud 組織の名前が含まれます。

> **Note**
>
> 単一の Terraform Cloud 組織での複数のAFTデプロイはサポートされていません。

Terraform Cloud の設定方法の詳細については、Terraform のドキュメントを参照してください。

Terraform Enterprise

ディストリビューションとして Terraform Enterprise を選択すると、 は Terraform Enterprise 組織に次のコンポーネントのワークスペースAFTを作成し、結果として生じる Terraform 実行の 駆動API型ワークフローをトリガーします。

- アカウントリクエスト
- AFT によってプロビジョニングされたアカウントのアカウントプロビジョニングのカスタマイズ AFT
- によってプロビジョニングされたアカウントのアカウントカスタマイズ AFT
- によってプロビジョニングされたアカウントのグローバルカスタマイズ AFT

結果の Terraform の状態設定は Terraform Enterprise セットアップによって管理されます。

ディストリビューションとして Terraform Enterprise を選択するには、次の入力パラメータを指定します。

- `terraform_distribution = "tfe"`
- `terraform_token` – このパラメータには、Terraform Enterprise トークンの値が含まれています。 はその値を機密としてAFTマークし、AFT管理アカウントのSSMパラメータストアに安全な文字列として保存します。会社のセキュリティポリシーとコンプライアンスガイドラインに従って、Terraform トークンの値を定期的にローテーションすることをお勧めします。
- `terraform_org_name` — このパラメータには、Terraform Enterprise 組織の名前が含まれます。
- `terraform_api_endpoint` – このパラメータには、Terraform Enterprise 環境URLの が含まれます。このパラメータの値は、次の形式であることが必要です。

```
https://{fqdn}/api/v2/
```

Terraform Enterprise の設定方法の詳細については、Terraform のドキュメントを参照してください。

AFT バージョンを確認する

デプロイされたAFTバージョンを確認するには、Parameter Store キーを AWS SSMクエリします。

```
/aft/config/aft/version
```

レジストリメソッドを使用すると、バージョンをピン留めできます。

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

AFT リポジトリAFTのバージョンに関する詳細情報を表示できます。

AFT バージョンを更新する

デプロイしたAFTバージョンは、mainリポジトリブランチからプルすることで更新できます。

```
terraform get -update
```

プルが完了したら、Terraform プランを再実行するか、適用を実行して最新の変更でAFTインフラストラクチャを更新できます。

機能オプションの有効化

AFT は、ベストプラクティスに基づいて機能オプションを提供します。AFT デプロイ中に、機能フラグを使用してこれらの機能をオプトインできます。AFT 入力設定パラメータの詳細についてはAFT による新しいアカウントのプロビジョニング、「」を参照してください。

デフォルトでは、これらの機能は有効になっていません。環境でそれぞれの機能を明示的に有効にする必要があります。

トピック

- AWS CloudTrail データイベント
- AWS エンタープライズサポートプラン
- AWS デフォルトを削除する VPC

AWS CloudTrail データイベント

有効にすると、 AWS CloudTrail データイベントオプションによってこれらの機能が設定されます。

- の AWS Control Tower 管理アカウントに Organization Trail を作成します。 CloudTrail

- Simple Storage Service (Amazon S3) および Lambda データイベントのログ記録をオンにします。
- 暗号化を使用して、すべての CloudTrail データイベントを暗号化し、AWSControl Tower Log Archive `aws-aft-logs-*` アカウントの S3 バケットにエクスポートします。 AWS KMS
- [Log file validation] (ログファイルの検証) 設定をオンにします。

このオプションを有効にするには、AFTデプロイ入力設定で次の機能フラグを True に設定します。

```
aft_feature_cloudtrail_data_events
```

前提条件

この機能オプションを有効にする前に、 の信頼されたアクセス AWS CloudTrail が組織で有効になっていることを確認してください。

の信頼されたアクセスのステータスを確認するには CloudTrail ：

1. AWS Organizations コンソールに移動します。
2. サービス > CloudTrail を選択します。
3. 次に、必要に応じて、右上の [Enable trusted access] (信頼されたアクセスを有効にする) を選択します。

AWS CloudTrail コンソールを使用するように指示する警告メッセージが表示される場合がありますが、この場合は警告を無視してください。信頼されたアクセスを許可した後、 はこの機能オプションを有効にする一環として証跡AFTを作成します。信頼されたアクセスが有効になっていない場合、がデータイベントの証跡を作成AFTしようとすると、エラーメッセージが表示されます。

> **Note**
>
> この設定は組織レベルで機能します。この設定を有効にすると AWS Organizations、 で管理されているかどうかにかかわらず、 のすべてのアカウントに影響AFTします。有効化時の AWS Control Tower Log Archive アカウントのすべてのバケットは、Amazon S3 データイベントから除外されます。詳細については、 AWS CloudTrail 「 ユーザーガイド」を参照してください CloudTrail。

AWS エンタープライズサポートプラン

このオプションを有効にすると、AFTパイプラインは によってプロビジョニングされたアカウントの AWS エンタープライズサポートプランを有効にしますAFT。

AWS アカウントには、デフォルトで AWS 基本サポートプランが有効になっています。 AFTは、 がAFTプロビジョニングするアカウントに対して、エンタープライズサポートレベルへの自動登録を提供します。プロビジョニングプロセスにより、 アカウントのサポートチケットが開き、 AWS エンタープライズサポートプランへの追加がリクエストされます。

エンタープライズサポートオプションを有効にするには、AFTデプロイ入力設定で次の機能フラグを True に設定します。

```
aft_feature_enterprise_support=false
```

サポートプランの詳細については、 AWS 「サポートプランの比較」を参照してください。 AWS

> **Note**
>
> この機能を使用するには、支払いアカウントを Enterprise Support プランに登録する必要があります。

AWS デフォルトを削除する VPC

このオプションを有効にすると、 は、管理アカウントとすべての の AWS デフォルトをすべてAFT削除します。これらの VPCsに AWS Control Tower リソースをデプロイしていない場合 AWS リージョンでも、すべて削除されます AWS リージョン。

AFT は、AFTプロビジョニングする AWS Control Tower アカウント、または を介して AWS Control Tower に登録する既存の AWS アカウントの AWS デフォルトVPCsを自動的に削除しませんAFT。

デフォルトでは AWS リージョン、新しい AWS アカウントは各 に VPC がセットアップされた状態で作成されます。エンタープライズではVPCs、 を作成するための標準プラクティスがある場合があります。そのため、特にAFT管理アカウントでは、 AWS デフォルトを削除VPCし、有効にしないようにする必要があります。

このオプションを有効にするには、AFTデプロイ入力設定で次の機能フラグを True に設定します。

```
aft_feature_delete_default_vpcs_enabled
```

デフォルトの の詳細については、「デフォルトVPCサブネットとデフォルトサブネット」を参照してくださいVPCs。

AWS Control Tower Account Factory for Terraform のリソースに関する考慮事項

AWS Control Tower Account Factory for Terraform を使用してランディングゾーンを設定すると、AWS アカウント内に複数のタイプの AWS リソースが作成されます。

リソースの検索

- タグを使用して、リソースの最新のリストを検索できますAFT。検索のキーと値のペアは次のとおりです。

```
Key: managed_by | Value: AFT
```

- タグをサポートしないコンポーネントサービスの場合は、リソース名で `aft` を検索してリソースを特定できます。

最初に作成されたリソースのテーブル (アカウント別)

AWS Control Tower Account Factory for Terraform 管理アカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*
AWS Identity and Access Management	ポリシー	aws-ct-aft-*
CodeCommit	リポジトリ	aws-ct-aft-*
CodeBuild	ビルドプロジェクト	aws-ct-aft-*
コードパイプライン	パイプライン	*-baseline-*

AWS service	リソースタイプ	リソース名
Simple Storage Service (Amazon S3)	バケット	*-aws-ct-aft-* aws-ct-aft-*
Lambda	関数	aws-ct-aft-*
Lambda	レイヤー	aws-ct-aft-common-layer
DynamoDB	テーブル	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	ステートマシン	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	トピック	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	イベントバス	aws-ct-aft-events-from-ct-management
Amazon EventBridge	イベントルール	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor

AWS service	リソースタイプ	リソース名
Key Management Service (KMS)	カスタマーマネージドキー	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	パラメータストア	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	キュー	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	ロググループ	/aws/*/aws-ct-aft-* aws-ct-aft-*
AWS サポートセンター (オプション)	サポートプラン	Enterprise

AWS AWS Control Tower Account Factory for Terraform を通じてプロビジョニングされた アカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecution
AWS サポートセンター (オプション)	サポートプラン	Enterprise

AWS Control Tower 管理アカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecutionRole AWSAFTExecution

AWS service	リソースタイプ	リソース名
		aws-ct-aft-controltower-events-rule
AWS Systems Manager	パラメータストア	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations（オプション）	サービスコントロールポリシー	aws-ct-aft-protect-resources
CloudTrail（オプション）	追跡	aws-ct-aft-BaselineCloudTrail
AWS Support Center (オプション)	サポートプラン	Enterprise

AWS Control Tower ログアーカイブアカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role
Key Management Service (KMS）	カスタマーマネージドキー	*-aws-ct-aft-kms-gd-findings
Simple Storage Service (Amazon S3)	バケット	*-aws-ct-aft-logs* aws-ct-aft-s3-access-logs*
AWS サポートセンター (オプション）	サポートプラン	Enterprise

AWS Control Tower 監査アカウント

AWS service	リソースタイプ	リソース名
AWS Identity and Access Management	ロール	AWSAFTExecutionRole AWSAFTExecution
AWS サポートセンター (オプション)	サポートプラン	Enterprise

必要なロール

一般的に、ロールとポリシーは、 のアイデンティティとアクセス管理 (IAM) の一部です AWS。詳細については、AWS IAM「 ユーザーガイド」を参照してください。

AFT は、AFTパイプラインのオペレーションをサポートするために、AFT管理アカウントと AWS Control Tower 管理アカウントに複数のIAMロールとポリシーを作成します。これらのロールは、最小特権アクセスモデルに基づいて作成されます。このモデルは、各ロールおよびポリシーで最小限必要なアクションとリソースのセットに対する許可を制限します。これらのロールとポリシーには、識別 `managed_by:AFT`用の AWS として タグ`key:value`ペアが割り当てられます。

これらのIAMロールに加えて、 は 3 つの重要なロールAFTを作成します。

- `AWSAFTAdmin` ロール
- `AWSAFTExecution` ロール
- `AWSAFTService` ロール

これらのロールについては、以降のセクションで説明します。

ロール AWSAFTAdmin の説明

をデプロイするとAFT、`AWSAFTAdmin`ロールがAFT管理アカウントに作成されます。このロールにより、AFTパイプラインは AWS Control Tower とAFTプロビジョニングされたアカウントで`AWSAFTExecution`ロールを引き受けることができるため、アカウントのプロビジョニングとカスタマイズに関連するアクションを実行できます。

`AWSAFTAdmin` ロールにアタッチされたインラインポリシー (JSON アーティファクト) は次のとおりです。

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

次のJSONアーティファクトは、AWSAFTAdminロールの信頼関係を示しています。プレースホルダー番号012345678901は、AFT管理アカウント ID 番号に置き換えられます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

ロール AWSAFTExecution の説明

をデプロイするとAFT、AWSAFTExecutionロールはAFT管理アカウントと AWS Control Tower 管理アカウントに作成されます。後で、AFTパイプラインはアカウントAFTプロビジョニング段階でプロビジョニングされた各AFTアカウントにAWSAFTExecutionロールを作成します。

AFT は、最初にAWSControlTowerExecutionロールを使用して、指定されたアカウントにAWSAFTExecutionロールを作成します。このAWSAFTExecutionロールにより、AFTパイプラインはAFT、フレームワークのプロビジョニングとプロビジョニングのカスタマイズの段階で実行されるステップを、AFTプロビジョニングされたアカウントと共有アカウントに対して実行できます。

> **個別のロールは範囲を制限するのに役立つ**
>
> ベストプラクティスとして、カスタマイズ権限は、リソースの初期デプロイ時に許可されるアクセス許可とは別にしておきます。AWSAFTService ロールはアカウントのプロビジョニングを目的としており、AWSAFTExecution ロールは、アカウントのカスタマイズを目的としていることを忘れないようにしてください。この分離により、パイプラインの各フェーズで許可されるアクセス許可の範囲が制限されます。この区別は、AWSControl Tower 共有アカウントをカスタマイズする場合に特に重要です。共有アカウントには、請求の詳細やユーザー情報などの機密情報が含まれている可能性があるためです。

AWSAFTExecution ロールのアクセス許可: AdministratorAccess – AWS管理ポリシー

次のJSONアーティファクトは、AWSAFTExecutionロールにアタッチされたIAMポリシー (信頼関係) を示しています。プレースホルダー番号012345678901は、AFT管理アカウント ID 番号に置き換えられます。

AWSAFTExecution の信頼ポリシー

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

ロール AWSAFTService の説明

AWSAFTService ロールは、共有アカウントや管理アカウントを含む、登録および管理されているすべてのアカウントにAFTリソースをデプロイします。リソースは、以前は、AWSAFTExecution ロールによってのみデプロイされていました。

AWSAFTService ロールは、プロビジョニング段階でリソースをデプロイするためにサービスインフラストラクチャで使用することを目的としており、AWSAFTExecution ロールは、カスタマイズ

のデプロイにのみ使用するためのものです。この方法でロールを引き受けると、各ステージでより詳細なアクセス制御を維持できます。

AWSAFTService ロールのアクセス許可: AdministratorAccess – AWS管理ポリシー

次のJSONアーティファクトは、AWSAFTServiceロールにアタッチされたIAMポリシー (信頼関係) を示しています。プレースホルダー番号012345678901は、AFT管理アカウント ID 番号に置き換えられます。

AWSAFTService の信頼ポリシー

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

コンポーネントサービス

をデプロイするとAFT、コンポーネントはこれらの各 AWS サービスから AWS 環境に追加されます。

- AWS Control Tower – AFTは、AWSControl Tower 管理アカウントの AWS Control Tower Account Factory を使用してアカウントをプロビジョニングします。
- Amazon DynamoDB – AFT は、アカウントリクエスト、アカウント更新の監査履歴、アカウントメタデータ、および AWS Control Tower ライフサイクルイベントを保存するAFT管理アカウントに Amazon DynamoDB テーブルを作成します。AFTまた、 は DynamoDB Lambda トリガーを作成して、AFTアカウントプロビジョニングワークフローの開始などのダウンストリームプロセスを開始します。
- Amazon Simple Storage Service – AFTは、管理アカウントと AWS Control Tower ログアーカイブアカウントに Amazon Simple Storage Service (S3) バケットAFTを作成します。これは、AFTパイプラインが必要とする AWS サービスによって生成されたログを保存します。AFTまた、 は、プラ

イマリとセカンダリに Terraform バックエンド S3 バケットを作成し AWS リージョン、AFTパイプラインワークフロー中に生成された Terraform 状態を保存します。

- Amazon Simple Notification Service – はAFT、管理アカウントに Amazon Simple Notification Service (SNS) トピックAFTを作成します。このトピックは、AFTアカウントリクエストの処理後に成功通知と失敗通知を保存します。任意のプロトコルを使用して、これらのメッセージを受信できます。
- Amazon Simple Queuing Service – AFT管理アカウントに Amazon Simple Queuing Service (Amazon SQS) FIFOキューAFTを作成します。キューでは、複数のアカウントリクエストを並行して送信できますが、一度に 1 つのリクエストを AWS Control Tower Account Factory に送信してシーケンシャル処理を行います。
- AWS CodeBuild - はAFT管理アカウントにAWS CodeBuild ビルドプロジェクトAFTを作成し、さまざまなビルドステージでAFTソースコードの Terraform プランを初期化、コンパイル、テスト、適用します。
- AWS CodePipeline – はAFT管理アカウントにAWS CodePipeline パイプラインAFTを作成し、AFTソースコード用に選択したサポートされているAWS CodeStar 接続プロバイダーと統合し、 AWS でビルドジョブをトリガーします CodeBuild。
- AWS Lambda – AFTは管理アカウントに AWS Lambda 関数とレイヤーAFTを作成し、アカウントのリクエスト、AFTアカウントのプロビジョニング、およびアカウントのカスタマイズプロセス中にステップを実行します。
- AWS Systems Manager パラメータストア – AFT管理アカウントに AWS Systems Manager パラメータストアAFTを設定し、AFTパイプラインプロセスに必要な設定パラメータを保存します。
- Amazon CloudWatch – はAFT、管理アカウントに Amazon CloudWatch ロググループAFTを作成し、AFTパイプラインで使用されるAWSサービスによって生成されたログを保存します。CloudWatch ログの保持期間は に設定されます`Never Expire`。
- Amazon VPC – は Amazon Virtual Private Cloud (VPC) AFTを作成し、セキュリティを強化するために、AFT管理アカウントのサービスとリソースを別のネットワーク環境に分離します。
- AWS KMS – は、AFT管理アカウントと AWS Control Tower ログアーカイブアカウントの AWS Key Management Service (KMS) AFTを使用します。 は、Terraform の状態、DynamoDB テーブルに保存されたデータ、およびSNSトピックを暗号化するためのキーAFTを作成します。これらのログとアーティファクトは、AWSリソースとサービスが によってデプロイされたときに生成されますAFT。 によって作成された KMSキーAFTは、デフォルトで毎年のローテーションが有効になっています。
- AWS Identity and Access Management (IAM) – 推奨される最小特権モデルAFTに従います。Identity AWS and Access Management (IAM) のロールとポリシーは、AFT管理アカウン

ト、AWSControl Tower アカウント、およびAFTプロビジョニングされたアカウントに、AFTパイプラインワークフロー中に必要なアクションを実行するために必要に応じて作成されます。

- AWS Step Functions – は、AFT管理アカウントに AWS Step Functions ステートマシンAFTを作成します。これらのステートマシンは、AFTアカウントプロビジョニングフレームワークとカスタマイズのプロセスとステップをオーケストレーションおよび自動化します。
- Amazon EventBridge – は、 AFTと AWS Control Tower 管理アカウントに Amazon EventBridge イベントバスAFTを作成し、AFT管理アカウントの DynamoDB テーブルに AWS Control Tower ライフサイクルイベントを長期間キャプチャして保存します。 はAFT、管理アカウントと AWS Control Tower 管理アカウントに Amazon CloudWatch イベントルールAFTを作成し、AFTパイプラインワークフローの実行中に複数のステップをトリガーします。
- AWS CloudTrail （ オプション ） – この機能を有効にすると、 は、Amazon S3 バケットと AWS Lambda 関数のデータイベントをログ記録するための AWS CloudTrail 組織の証跡を AWS Control Tower 管理アカウントにAFT作成します。 は、これらのログを AWS Control Tower ログアーカイブアカウントの中央 S3 バケットAFTに送信します。
- AWS サポート (オプション ） – この機能を有効にすると、 によってプロビジョニングされたアカウントの AWS エンタープライズサポートプランAFTが有効になりますAFT。デフォルトでは、AWS アカウントは AWS 基本サポートプランを有効にして作成されます。

AFT アカウントプロビジョニングパイプライン

パイプラインのアカウントプロビジョニングステージが完了すると、AFTフレームワークは続行されます。これにより、一連のステップが自動的に実行され、アカウントのカスタマイズステージが開始される前に、新しくプロビジョニングされたアカウントに詳細が設定されるようになります。

AFT パイプラインが実行する次のステップは次のとおりです。

1. アカウントリクエストの入力を検証します。
2. プロビジョニングされたアカウント (アカウント ID など) に関する情報を取得します。
3. アカウントメタデータを管理AFTアカウントの DynamoDB テーブルに保存します。
4. 新しくプロビジョニングされたアカウントにAWSAFTExecutionIAMロールを作成します。 は、このロールをAFT引き受けてアカウントカスタマイズステージを実行します。これは、このロールが Account Factory ポートフォリオへのアクセスを許可するためです。
5. アカウントリクエスト入力パラメータの一部として指定したアカウントタグを適用します。
6. AFT デプロイ時に選択したAFT機能オプションを適用します。

7. 指定したAFTアカウントプロビジョニングのカスタマイズを適用します。次のセクションでは、gitリポジトリ内の AWS Step Functions ステートマシンを使用してこれらのカスタマイズを設定する方法について詳しく説明します。このステージは、アカウントプロビジョニングフレームワークステージと呼ばれることもあります。これはコアプロビジョニングプロセスの一部ですが、アカウントプロビジョニングワークフローの一部としてカスタマイズされた統合を提供するフレームワークをあらかじめ設定してから、次のステージで追加のカスタマイズをアカウントに追加します。
8. プロビジョニングされたアカウントごとに、 AWS CodePipeline AFT管理アカウントに が作成され、 (次のグローバル) アカウントのカスタマイズステージを実行するために実行されます。
9. プロビジョニングされた (およびターゲットの) アカウントごとに、アカウントカスタマイズパイプラインを呼び出します。
10. 成功または失敗の通知を SNSトピックに送信します。そこからメッセージを取得できます。

ステートマシンを使用したアカウントプロビジョニングフレームワークのカスタマイズの設定

アカウントをプロビジョニングする前に、Terraform 以外のカスタム統合を設定すると、これらのカスタマイズはAFTアカウントプロビジョニングワークフローに含まれます。たとえば、 によって作成されたすべてのアカウントAFTがセキュリティ標準などの組織の標準とポリシーに準拠していることを確認するために、特定のカスタマイズが必要になる場合があります。これらの標準は、追加のカスタマイズの前にアカウントに追加される場合があります。これらのアカウントプロビジョニングフレームワークのカスタマイズは、グローバルアカウントのカスタマイズステージが次に開始される前に、プロビジョニングされたすべてのアカウントに実装されます。

> **Note**
>
> このセクションで説明するAFT機能は、AWSStep Functions の機能を理解している上級ユーザーを対象としています。代替として、アカウントのカスタマイズステージでグローバルヘルパーを操作することをお勧めします。

AFT アカウントプロビジョニングフレームワークは、ユーザーが定義した AWS Step Functions ステートマシンを呼び出して、カスタマイズを実装します。ステートマシンの統合の詳細については、AWSStep Functions のドキュメントを参照してください。

一般的な統合を次に示します。

- AWS 選択した言語での Lambda 関数
- AWS ECS Docker コンテナを使用した または AWS Fargate タスク
- AWS AWSまたはオンプレミスでホストされているカスタムワーカーを使用した Step Functions アクティビティ
- Amazon SNSまたは SQS統合

AWS Step Functions ステートマシンが定義されていない場合、ステージは no-op で合格します。AFT アカウントプロビジョニングのカスタマイズステートマシンを作成するには、「」の手順に従いますAFT アカウントプロビジョニングのカスタマイズステートマシンを作成する。カスタマイズを追加する前に、前提条件を満たしていることを確認してください。

これらのタイプの統合は AWS Control Tower の一部ではなく、AFTアカウントカスタマイズのグローバル事前API段階で追加することはできません。代わりに、AFTパイプラインでは、これらのカスタマイズをプロビジョニングプロセスの一部として設定でき、プロビジョニングワークフローで実行されます。以下のセクションで説明するように、AFTアカウントプロビジョニングステージを開始する前に、ステートマシンを事前に作成して、これらのカスタマイズを実装する必要があります。

ステートマシンを作成するための前提条件

- 完全にデプロイされた AFT。AFT デプロイの詳細については、AWS Control Tower Account Factory for Terraform (AFT) のデプロイ「」を参照してください。
- AFT アカウントのプロビジョニングをカスタマイズするために、 環境にgitリポジトリを設定します。詳細については、「デプロイ後のステップ」を参照してください。

AFT アカウントプロビジョニングのカスタマイズステートマシンを作成する

ステップ 1: ステートマシンの定義を変更する

例の `customizations.asl.json` ステートマシンの定義を変更します。この例は、デプロイ後のステップでAFTアカウントプロビジョニングのカスタマイズを保存するために設定したgitリポジトリで使用できます。ステートマシンの定義の詳細については、AWS「Step Functions デベロッパーガイド」を参照してください。

ステップ 2: 対応する Terraform 構成を含める

カスタム統合のためのステートマシンの定義を使用して、`.tf` 拡張子を持つ Terraform ファイルを同じ `git` リポジトリに含めます。例えば、ステートマシンのタスク定義で Lambda 関数を呼び出す

場合は、lambda.tf ファイルを同じディレクトリに保存します。カスタム設定に必要なIAMロールとアクセス許可を必ず含めてください。

適切な入力を指定すると、AFTパイプラインは自動的にステートマシンを呼び出し、AFTアカウントプロビジョニングフレームワークステージの一部としてカスタマイズをデプロイします。

AFT アカウントプロビジョニングフレームワークとカスタマイズを再開するには

AFT は、AFTパイプラインを通じて発行されたすべてのアカウントに対して、アカウントプロビジョニングフレームワークとカスタマイズステップを実行します。アカウントプロビジョニングのカスタマイズを再開するには、次の 2 つの方法のいずれかを使用できます。

1. アカウントリクエストリポジトリの既存のアカウントに変更を加えます。
2. で新しいアカウントをプロビジョニングしますAFT。

アカウントのカスタマイズ

AFT は、プロビジョニングされたアカウントに標準またはカスタマイズされた設定をデプロイできます。AFT 管理アカウントでは、 AFTはアカウントごとに 1 つのパイプラインを提供します。このパイプラインを使用すると、すべてのアカウント、一組のアカウント、または個々のアカウントにカスタマイズを実装できます。Python スクリプト、bash スクリプト、Terraform 設定を実行することも、アカウントカスタマイズステージAWSCLIの一部として を操作することもできます。

概要

選択したgitリポジトリでカスタマイズを指定すると、グローバルカスタマイズを保存する場所またはアカウントカスタマイズを保存する場所のいずれかで、AFTパイプラインによってアカウントカスタマイズステージが自動的に完了します。アカウントを遡及的にカスタマイズするには、「カスタマイズの再呼び出し」を参照してください。

グローバルカスタマイズ (オプション)

によってプロビジョニングされるすべてのアカウントに特定のカスタマイズを適用することを選択できますAFT。例えば、特定のIAMロールを作成したり、すべてのアカウントにカスタムコントロールをデプロイしたりする必要がある場合、AFTパイプラインのグローバルカスタマイズステージで自動的に実行できます。

アカウントカスタマイズ (オプション)

個々のアカウントまたは一連のアカウントを、他のAFTプロビジョニングされたアカウントとは異なる方法でカスタマイズするには、AFTパイプラインのアカウントカスタマイズ部分を活用して、アカウント固有の設定を実装できます。例えば、特定のアカウントでのみ、インターネットゲートウェイへのアクセスが必要になる場合があります。

カスタマイズの前提条件

アカウントのカスタマイズを開始する前に、次の前提条件が満たされていることを確認してください。

- 完全にデプロイされた AFT。デプロイ方法については、「AWS Control Tower Account Factory for Terraform を設定して起動する」を参照してください。
- 環境内のグローバルカスタマイズおよびアカウントカスタマイズ用の `git` リポジトリに必要な情報が事前入力されていること。詳細については、「デプロイ後のステップ」の「ステップ 3: (必須) 各リポジトリを設定する」を参照してください。

グローバルカスタマイズの適用

グローバルカスタマイズを適用するには、選択したリポジトリに特定のフォルダ構造をプッシュする必要があります。

- カスタム設定が Python プログラムまたはスクリプトの形式である場合は、それらをリポジトリ内の [api_helpers/python] フォルダに配置します。
- カスタム設定が Bash スクリプトの形式である場合は、それらをリポジトリ内の [api_helpers] フォルダに配置します。
- カスタム設定が Terraform の形式である場合は、それらをリポジトリ内の [terraform] フォルダに配置します。
- カスタム設定の作成の詳細については、グローバルカスタマイズREADMEファイルを参照してください。

> **Note**
>
> グローバルカスタマイズは、AFTパイプラインのAFTアカウントプロビジョニングフレームワークステージの後に自動的に適用されます。

アカウントカスタマイズの適用

選択したリポジトリに特定のフォルダ構造をプッシュすると、アカウントカスタマイズを適用できます。アカウントのカスタマイズは、AFTパイプラインとグローバルカスタマイズステージの後に自動的に適用されます。アカウントカスタマイズリポジトリに、さまざまなアカウントカスタマイズを含む複数のフォルダーを作成することもできます。必要なアカウントカスタマイズの実装ごとに、以下のステップを使用します。

アカウントカスタマイズを適用するには

1. ステップ 1: アカウントカスタマイズ用のフォルダを作成する

   選択したリポジトリで、 AFTが提供するACCOUNT_TEMPLATEフォルダを新しいフォルダにコピーします。新しいフォルダの名前は、アカウントリクエストで指定した `account_customizations_name` と一致する必要があります。

2. 特定のアカウントカスタマイズフォルダの設定を追加する

   設定の形式に基づいて、アカウントカスタマイズフォルダーに設定を追加できます。

   - カスタム設定が Python プログラムまたはスクリプトの形式である場合は、リポジトリ内の ***[account_customizations_name]***/api_helpers/python フォルダに配置します。
   - カスタム設定が Bash スクリプトの形式である場合は、リポジトリ内の ***[account_customizations_name]***/api_helpers フォルダに配置します。
   - カスタム設定が Terraform の形式である場合は、リポジトリ内の ***[account_customizations_name]***/terraform フォルダに配置します。

   カスタム設定の作成の詳細については、アカウントカスタマイズREADMEファイルを参照してください。

3. アカウントリクエストファイルの特定の **account_customizations_name** パラメータを参照する

   AFT アカウントリクエストファイルには、入力パラメータ が含まれていますaccount_customizations_name。このパラメータの値として、アカウントカスタマイズの名前を入力します。

> **Note**
>
> 環境内のアカウントに対して複数のアカウントリクエストを送信できます。異なるまたは類似のアカウントカスタマイズを適用する場合は、アカウントリクエストの `account_customizations_name` 入力パラメータを使用してアカウントのカスタマイズを指定します。詳細については、「複数のアカウントリクエストを送信する」を参照してください。

カスタマイズの再呼び出し

AFT は、AFTパイプラインでカスタマイズを再呼び出す方法を提供します。この方法は、新しいカスタマイズステップを追加した場合や、既存のカスタマイズを変更する場合に便利です。再呼び出すと、 はカスタマイズパイプラインAFTを開始し、AFTプロビジョニングされたアカウントに変更を加えます。再呼び出しを使用すると、個々のアカウント、すべてのアカウント、OU event-source-basedに応じたアカウント、またはタグに応じて選択されたアカウントにカスタマイズを適用できます。

AFTプロビジョニングされたアカウントのカスタマイズを再呼び出すには、次の 3 つのステップに従います。

ステップ 1: グローバルカスタマイズまたはアカウントカスタマイズの **`git`** リポジトリに変更をプッシュする

必要に応じてグローバルカスタマイズおよびアカウントカスタマイズを更新し、変更を `git` リポジトリに再度プッシュします。この時点では何も起こりません。次の 2 つのステップで説明するように、イベントソースによってカスタマイズパイプラインを呼び出す必要があります。

ステップ 2: カスタマイズを再呼び出すための AWS Step Function の実行を開始する

AFT は、AFT管理アカウント`aft-invoke-customizations`で という AWS Step Function を提供します。この関数の目的は、AFTプロビジョニングされたアカウントのカスタマイズパイプラインを再呼び出すことです。

Step Function に入力を渡すために作成できるイベントスキーマ (JSON 形式) `aft-invoke-customizations` AWS の例を次に示します。

```
{
```

```
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],

  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

このイベントスキーマの例に示すように、再呼び出しプロセスに対して含めたり除外したりするアカウントを選択できます。組織単位 (OU)、アカウントタグ、およびアカウント ID でフィルタリングできます。フィルターを適用せず、ステートメント を含めた場合`"type":"all"`、AFTプロビジョニングされたすべてのアカウントのカスタマイズが再呼び出されます。

> **Note**
>
> AWS Control Tower Account Factory for Terraform (AFT) のバージョンが 1.6.5 以降の場合は、ネストされた を構文 OUsでターゲットにすることができます`OU Name (ou-id-1234)`。詳細については、 の次のトピックを参照してくださいGitHub。

イベントパラメータを入力すると、Step Functions が実行され、対応するカスタマイズが呼び出されます。 は、一度に最大 5 つのカスタマイズを呼び出すAFTことができます。Step Functions は、イベント条件に一致するすべてのアカウントが完了するまで待機してループします。

ステップ 3: AWS Step Function 出力をモニタリングし、AWS CodePipeline 実行中を監視する

- 結果の Step Function 出力には、Step Function 入力イベントソースIDsに一致するアカウントが含まれます。
- デベロッパーツールAWS CodePipeline の に移動し、アカウント ID に対応するカスタマイズパイプラインを表示します。

AFT アカウントカスタマイズリクエストトレースを使用したトラブルシューティング

ターゲットアカウントとカスタマイズリクエスト を含むログを出力する AWS Lambda アカウントカスタマイズワークフローIDs。 AFT では、ターゲットアカウントまたはカスタマイズリクエスト ID CloudWatch でカスタマイズリクエストに関連するログをフィルタリングするために使用できる CloudWatch Logs Insights クエリを提供することで、Amazon CloudWatch Logs を使用してカスタマイズリクエストをトレースおよびトラブルシューティングできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「Amazon Logs を使用したログデータの分析 CloudWatch 」を参照してください。

で CloudWatch Logs Insights を使用するには AFT

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. ナビゲーションペインで、[ログ]、[ログのインサイト] の順に選択します。
3. [クエリ] を選択します。
4. [サンプルクエリ] で [Account Factory for Terraform] を選択し、次のクエリのいずれかを選択します。

    - アカウント ID 別のカスタマイズログ

> **Note**
>
> をターゲットアカウント ID *"YOUR-ACCOUNT-ID"*に置き換えてください。

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
customization_request_id/
```

- カスタマイズリクエスト ID 別のカスタマイズログ

> **Note**
>
> をカスタマイズリクエスト ID *"YOUR-CUSTOMIZATION-REQUEST-ID"*に置き換えてください。カスタマイズリクエスト ID は、AFTアカウントプロビジョニングフレームワーク AWS Step Functions ステートマシンの出力にあります。AFT アカウントプロビジョニングフレームワークの詳細については、AFT「アカウントプロビジョニングパイプライン」を参照してください。

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
```

5. クエリを選択したら、必ず時間間隔を選択し、[クエリの実行] を選択します。

でのソースコードのバージョン管理の代替方法 AFT

AFT は、ソースコードバージョン管理システム (VCS) AWS CodeCommit に を使用し、ビジネス要件または既存のアーキテクチャCodeConnectionsを満たす他の を許可します。

AFT 初めてデプロイする場合で、既存の CodeCommitリポジトリがない場合は、AFTデプロイの前提条件の一部として外部VCSプロバイダーを指定する必要があります。詳細については、「」の「ソースコードのバージョン管理の代替AFT方法」を参照してください。

AFT は、次のソースコード制御の代替方法をサポートしています。

- GitHub
- GitHub エンタープライズサーバー
- BitBucket
- GitLab
- GitLab セルフマネージド

> **Note**
>
> AWS CodeCommit として を指定した場合VCS、追加のステップは必要ありません。 は、必要なgitリポジトリをデフォルト名で環境内にAFT作成します。ただし、組織の標準に準拠するために CodeCommit、必要に応じて のデフォルトのリポジトリ名を上書きできます。

で代替ソースコードバージョン管理システム (カスタム VCS) を設定する AFT

AFT デプロイ用の代替ソースコードバージョン管理システムを設定するには、次の手順に従います。

ステップ 1: サポートされているサードパーティーのバージョン管理システム () で**git**リポジトリを作成しますVCS。

を使用していない場合は AWS CodeCommit、以下の項目について、 AFTがサポートするサードパーティーVCSプロバイダー環境でgitリポジトリを作成する必要があります。

- AFT アカウントリクエスト。サンプルコードがあります。AFT アカウントリクエストの詳細については、「」を参照してくださいAFT による新しいアカウントのプロビジョニング。
- AFT アカウントのプロビジョニングのカスタマイズ。サンプルコードがあります。AFT アカウントプロビジョニングのカスタマイズの詳細については、「」を参照してくださいAFT アカウントプロビジョニングのカスタマイズステートマシンを作成する。
- AFT グローバルカスタマイズ。サンプルコードがあります。AFT グローバルカスタマイズの詳細については、「」を参照してくださいアカウントのカスタマイズ。

- AFT アカウントのカスタマイズ。サンプルコードがあります。AFT アカウントのカスタマイズの詳細については、「」を参照してくださいアカウントのカスタマイズ。

ステップ 2: AFTデプロイに必要なVCS設定パラメータを指定する

AFT デプロイの一部としてVCSプロバイダーを設定するには、次の入力パラメータが必要です。

- vcs_provider: を使用していない場合は AWS CodeCommit、ユースケースに基づいて、VCSプロバイダーを "bitbucket"、"gitlab"、、"github""githubenterprise"または として指定します。
- github_enterprise_url: GitHub Enterprise のお客様のみ、 を指定します GitHub URL。
- account_request_repo_name: AWS CodeCommit ユーザーの場合、この値は に設定されますaft-account-request。がAFTサポートするサードパーティーVCSプロバイダー環境では、この入力値を実際のリポジトリ名で更新します。Github BitBucket、 GitHub Enterprise GitLab、セルフ GitLabマネージドの場合、リポジトリ名は の形式である必要があります[Org]/[Repo]。
- account_customizations_repo_name: AWS CodeCommit ユーザーの場合、この値は に設定されますaft-account-customizations。がAFTサポートするサードパーティーVCSプロバイダー環境では、この入力値をリポジトリ名で更新します。Github BitBucket、 GitHub Enterprise GitLab、GitLab セルフマネージドの場合、リポジトリ名は の形式である必要があります[Org]/[Repo]。
- account_provisioning_customizations_repo_name: AWS CodeCommit ユーザーの場合、この値は aft-account-provisioning-customizations に設定されます。がAFTサポートするサードパーティーVCSプロバイダー環境では、この入力値をリポジトリ名で更新します。Github BitBucket、 GitHub Enterprise GitLab、セルフ GitLabマネージドの場合、リポジトリ名は の形式である必要があります[Org]/[Repo]。
- global_customizations_repo_name: AWS CodeCommit ユーザーの場合、この値は に設定されますaft-global-customizations。がAFTサポートするサードパーティーVCSプロバイダー環境では、この入力値をリポジトリ名で更新します。Github BitBucket、 GitHub Enterprise GitLab、GitLab セルフマネージドの場合、リポジトリ名は の形式である必要があります[Org]/[Repo]。
- account_request_repo_branch: ブランチはデフォルトで main ですが、この値はオーバーライドできます。

デフォルトでは、 は各gitリポジトリの main ブランチからAFTソースを作成します。ブランチ名の値は、追加の入力パラメータでオーバーライドできます。入力パラメータの詳細については、AFTTerraform モジュールの README ファイルを参照してください。

> **既存の AWS CodeCommit お客様向け**
>
> の新しい名前で CodeCommit リポジトリを作成する場合はAFT、これらの入力パラメータの値を更新することでリポジトリ名を更新できます。

ステップ 3: サードパーティーVCSプロバイダー AWS CodeStar の接続を完了する

デプロイを実行すると、 AFTは必要な AWS CodeCommit リポジトリを作成するか、選択したサードパーティーVCSプロバイダーの AWS CodeStar 接続を作成します。後者の場合は、AFT管理アカウントのコンソールに手動でサインインして、保留中 AWS CodeStar の接続を完了する必要があります。 AWS CodeStar 接続の完了に関する詳細な手順については、 ドキュメントを参照してください AWS CodeStar。

データ保護

責任AWS 共有モデルは、 でのデータ保護に適用されますAFT。データ保護のため、セキュリティについては、次のベストプラクティスをお勧めします。

- AWS Control Tower が提供するデータ保護ガイドラインに従ってください。詳細については、「AWS Control Tower のデータ保護」を参照してください。
- AFT デプロイ時に生成された Terraform 状態設定を保持します。詳細については、「AWS Control Tower Account Factory for Terraform (AFT) のデプロイ」を参照してください。
- 組織のセキュリティポリシーの指示に従って、機密性の高い認証情報を定期的にローテーションします。シークレットの例としては、Terraform トークン、`git` トークンなどがあります。

保管時の暗号化

AFT は、保管時に AWS Key Management Service キーで暗号化される Amazon S3 バケット、Amazon SNSトピック、Amazon SQSキュー、および Amazon DynamoDB データベースを作成します。 によって作成された KMS キーAFTは、デフォルトで毎年のローテーションが有効になっています。Terraform の Terraform Cloud または Terraform Enterprise ディストリビューションを選択した場合、 には、機密性の高い Terraform トークン値を保存するための AWS Systems Manager SecureString パラメータAFTが含まれます。

AFT は、 で説明コンポーネントサービスされている AWS サービスを使用します。デフォルトでは、保管時に暗号化されます。詳細については、 の各コンポーネント AWS サービスの AWS ドキュメントを参照しAFT、各サービスが従うデータ保護プラクティスについて学びます。

転送時の暗号化

AFT は、デフォルトで転送中に暗号化を使用する で説明コンポーネントサービスされている AWS サービスに依存します。詳細については、 の各コンポーネント AWS サービスの AWS ドキュメントを参照しAFT、各サービスが従うデータ保護プラクティスについて学びます。

Terraform Cloud または Terraform Enterprise ディストリビューションAPIの場合、 は Terraform 組織にアクセスするためのHTTPSエンドポイントをAFT呼び出します。 AWS CodeStar 接続でサポートされているサードパーティーVCSプロバイダーを選択した場合、 はVCSプロバイダー組織APIにアクセスするためにHTTPSエンドポイントをAFT呼び出します。

からアカウントを削除する AFT

このトピックでは、AFTパイプラインがアカウントのデプロイと更新を停止するようにAFT、 からアカウントを削除する方法について説明します。

> **Important**
>
> AFT パイプラインからアカウントを削除すると元に戻せず、状態が失われる可能性があります。

リタイアしたアプリケーションのアカウントを閉鎖したり、侵害されたアカウントを分離したり、ある組織から別の組織へアカウントを移動したりAFTする場合は、 からアカウントを削除できます。

> **Note**
>
> からアカウントを削除するAFTと、AWSControl Tower アカウントまたは を削除する場合とは異なります AWS アカウント。からアカウントを削除してもAFT、AWSControl Tower は引き続きアカウントを管理します。AWS Control Tower アカウントまたは を削除するには AWS アカウント、以下を参照してください。
>
> - AWS Control Tower ユーザーガイドの「アカウントの管理を解除する」。
> - 「AWS Billing ユーザーガイド」の「アカウントの解約」

AFT パイプラインからアカウントを削除するには

次の手順では、 からアカウントを削除する方法について説明しますAFT。

1. アカウントリクエストを保存する **git** リポジトリからアカウントを削除する

   アカウントリクエストを保存するgitリポジトリで、 から削除するアカウントのアカウントリクエストを から削除しますAFT。

   アカウントリクエストリポジトリからアカウントリクエストを削除すると、 はカスタマイズパイプラインとアカウントメタデータAFTを削除します。詳細については、 AFTの 1.8.0 リリースノートを参照してください GitHub。

2. Terraform ワークスペースを削除する (Terraform Cloud および Terraform Enterprise のお客様のみ)

   から削除するアカウントのグローバルカスタマイズとアカウントカスタマイズワークスペースを削除しますAFT。

3. Amazon S3 バックエンドから Terraform の状態を削除する

   AFT 管理アカウントで、 から削除するアカウントの Amazon S3 バケット内の関連するフォルダをすべて削除しますAFT。

   > **Tip**
   >
   > 次の例では、 を管理AFTアカウント ID 番号*012345678901*に置き換えます。

   例: Terraform OSS

   Terraform を選択するとOSS、 `aft-backend-`*`012345678901`*`-primary-region`および `aft-backend-`*`012345678901`*`-secondary-region` Amazon S3 バケットにアカウントごとに 3 つのフォルダがあります。これらのフォルダは、カスタマイズパイプラインの状態、アカウントのカスタマイズ状態、およびグローバルカスタマイズ状態に関連しています

   例: テラフォームクラウドまたはテラフォームエンタープライズ

   Terraform Cloud または Terraform Enterprise を選択した場合、`aft-backend-`*`012345678901`*`-primary-region` および `aft-backend-`*`012345678901`*`-secondary-region` Amazon S3 バケットには、アカウントごとにフォルダがあります。これらのフォルダは、カスタマイズパイプラインの状態に関連しています。

運用メトリクス

デフォルトでは、Account Factory for Terraform (AFT) は匿名の運用メトリクスを に送信します AWS。このデータは、ソリューションの品質と機能を向上させるAFTために、お客様が をどのように使用しているかを理解するために使用されます。AFT デプロイ中にパラメータを変更することで、データ収集をオプトアウトできます。収集を有効にすると、次のデータが に送信されます AWS。

- 解決策： AFT固有の識別子
- バージョン： のバージョン AFT
- Universally Unique Identifier (UUID): ランダムに生成された各AFTデプロイの一意の識別子
- タイムスタンプ: データ収集タイムスタンプ
- データ： お客様が実行したAFT設定とアクション

AWS は収集されたデータを所有します。データ収集には、AWS プライバシーポリシーが適用されます。

> **Note**
>
> 1.6.0 AFTより前のバージョンの では、使用状況メトリクスはレポートされません AWS。

レポートメトリクスをオプトアウトするには:

- 次の例に示すように、Terraform 入力設定ファイル`false`で の入力値を `aft_metrics_reporting`に設定し、 を再デプロイしますAFT。明示的に設定しない場合、この値は、デフォルトで `true` に設定されます。

例をコピーする場合は、x の部分の文字列を実際の ID とリージョン値で置き換えてください。

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
```

```
    audit_account_id             = "xxxxxxxxxxx"
    aft_management_account_id    = "xxxxxxxxxxx"
    ct_home_region               = "xx-xxxx-x"
    tf_backend_secondary_region = "xx-xxxx-x"

    # Optional Vars
    aft_metrics_reporting = false    # to opt out, set this value to false
    }
```

Account Factory for Terraform (AFT)

このセクションは、Account Factory for Terraform (AFT) 使用時に直面する可能性のある一般的な問題をトラブルシューティングするのに役立ちます。

トピック

- 一般的な問題
- アカウントのプロビジョニング/登録に関連する問題
- カスタマイズの呼び出しに関する問題
- アカウントカスタマイズのワークフローに関連する問題

一般的な問題

- AWS リソースクォータの超過

  ロググループが AWS リソースクォータを超えたことを示している場合は、 AWS サポートにお問い合わせください。Account Factory は AWS CodeBuild、、 AWS Organizations、 を含むリソースクォータ AWS のサービス で を使用します AWS Systems Manager。詳細については次を参照してください:

  - 「CodeBuild ユーザーガイド」の「AWS CodeBuildとは」。
  - Organizations ユーザーガイドの「 とは AWS Organizations」。
  - Systems Manager ユーザーガイドの「 AWS Systems Managerとは」。
- Account Factory バージョンが古い

  問題が発生した際、それがバグであることを確かめるには、Account Factory が最新バージョンであることを確認します。詳細については、「Updating the Account Factory version」(Account Factory バージョンの更新)を参照してください。
- Account Factory ソースコードにローカルな変更が加えられている

Account Factory は、オープンソースプロジェクトです。AWS Control Tower は Account Factory コアコードをサポートしています。Account Factory コアコードにローカルな変更を加える場合、AWS Control Tower は Account Factory デプロイをベストエフォートベースでのみサポートします。

- Account Factory ロールのアクセス許可が不十分

  Account Factory では、IAM ロールとポリシーを作成して、発行されたアカウントのデプロイとカスタマイズを管理します。このようなロールまたはポリシーを変更すると、Account Factory パイプラインで特定のアクションを実行できなくなる可能性があります。詳細については、「Required roles」(必要なロール) を参照してください。
- アカウントリポジトリに情報が正しく入力されていない

  アカウントをプロビジョニングする前に、必ず「デプロイ後の手順」に従ってください。
- 手動による OU の変更後、ドリフトが検出されなくなる

> **Note**
>
> ドリフト検出は、AWS Control Tower で自動的に行われます。ドリフトの解決の詳細については、「Detect and resolve drift in AWS Control Tower」(AWS Control Tower でドリフトを検出して解決する) を参照してください。

組織単位 (OU) が手動で変更されると、ドリフトが検出されなくなります。これは、イベント駆動型の Account Factory が持つ性質によるものです。アカウントリクエストが送信されるとき、Terraform によって管理されるリソースは Amazon DynamoDB アイテムであり、直接のアカウントではありません。アイテムが変更されると、リクエストはキューに入れられ、AWS Control Tower によって (アカウントの詳細を管理するサービス) を通じて処理されます。OU を手動で変更すると、アカウントリクエストが変更されないため、ドリフトは検出されません。

アカウントのプロビジョニング/登録に関連する問題

- アカウントリクエスト (メールアドレス/名前) がすでに存在する

  この問題は通常、プロビジョニング中または `ConditionalCheckFailedException` 発生時に、Service Catalog 製品の障害を引き起こします。

  この問題の詳細情報は、次のいずれかを実行することで確認できます。

  - Terraform または CloudWatch Logs ロググループを確認する。
  - Amazon SNS トピックに発行されたエラー `aft-failure-notifications` を確認する。
- 不正な形式のアカウントリクエスト

  アカウントリクエストが期待されるスキーマに従っていることを確認します。例については、GitHub の terraform-aws-control_tower_account_factory を参照してください。
- AWS Organizations リソースクォータの超過

  アカウントリクエストが AWS Organizations リソースクォータを超えていないことを確認してください。詳細については、AWS「組織のクォータ」を参照してください。

カスタマイズの呼び出しに関する問題

- ターゲットアカウントが Account Factory にオンボードされていない

  カスタマイズリクエストに含まれるすべてのアカウントが Account Factory にオンボードされていることを確認します。詳細については、「Update an existing account」(既存のアカウントの更新)を参照してください。
- カスタマイズリクエストのターゲットとなるアカウントが DynamoDB テーブル **`aft-request-metadata`** には存在するが、アカウントリクエストリポジトリに存在しない

  次のいずれかを実行して、問題のあるアカウントを除外するようにカスタマイズ呼び出しリクエストを書式設定します。
  - DynamoDB テーブル `aft-request-metadata` で、アカウントリクエストリポジトリに存在しないアカウントを参照するエントリを削除する。
  - 「all」をターゲットとして使用しない。
  - アカウントが属する OU をターゲットにしない。
  - アカウントを直接ターゲットにしない。
- Terraform Cloud に使用されたトークンが誤っている

  正しいトークンを設定していることを確認します。Terraform Cloud はチームベースのトークンのみをサポートし、組織ベースのトークンをサポートしていません。
- アカウントカスタマイズパイプラインが作成される前にアカウントを作成できなかった。アカウントをカスタマイズできない

アカウントリクエストリポジトリのアカウント仕様を変更します。アカウントのタグ値を変更するなどの変更を加えると、パイプラインが存在しない場合でも、Account Factory はパイプラインの作成を試みるパスをたどります。

アカウントカスタマイズのワークフローに関連する問題

アカウントカスタマイズのワークフローに関連する問題が発生した場合は、AFT のバージョンが 1.8.0 以上であることを確認し、DynamoDB リクエストテーブルからアカウント関連のメタデータのインスタンスをすべて削除してください。

AFT バージョン 1.8.0 の詳細については、GitHub の「リリース 1.8.0」を参照してください。

AFT のバージョンを確認および更新する方法については、以下を参照してください。

- AFT バージョンを確認する
- AFT バージョンを更新する

Amazon CloudWatch Logs Insights クエリを使用して、ターゲットアカウントとカスタマイズリクエスト ID を含むログをフィルタリングすることで、カスタマイズリクエストの追跡とトラブルシューティングを行うこともできます。詳細については、「AFT アカウントカスタマイズリクエストの追跡によるトラブルシューティング」を参照してください。

AWS Control Tower でドリフトを検出して解決する

ドリフトの特定と解決は、AWSControl Tower 管理アカウント管理者の通常のオペレーションタスクです。ドリフトを解決することで、ガバナンス要件のコンプライアンスを確保できます。

ランディングゾーンを作成すると、ランディングゾーンとすべての組織単位 (OUs) 、アカウント、リソースは、選択したコントロールによって適用されるガバナンスルールに準拠します。ユーザーおよび組織のメンバーがランディングゾーンを使用する際、コンプライアンスステータスが変更されることがあります。一部の変更は偶発的になされますが、時間的制約のある操作上のイベントに対応するために意図的になされる場合もあります。

ドリフト検出は、ドリフトを解決するために変更や設定更新が必要になるリソースを識別するのに役立ちます。

ドリフトの検出

AWS Control Tower はドリフトを自動的に検出します。ドリフトを検出するには、`AWSControlTowerAdmin`ロールに管理アカウントへの永続的なアクセスが必要です。これにより、AWSControl Tower は読み取り専用のAPI呼び出しを行うことができます AWS Organizations。これらのAPI呼び出しは AWS CloudTrail イベントとして表示されます。

ドリフトは、監査アカウントに集約された Amazon Simple Notification Service (Amazon SNS) 通知に表示されます。各メンバーアカウントの通知は、ローカル Amazon SNSトピックと Lambda 関数にアラートを送信します。

AWS Security Hub サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールの場合、ドリフトは AWS Control Tower コンソールのアカウントとアカウントの詳細ページ、および Amazon SNS通知によって表示されます。

メンバーアカウント管理者は、特定のアカウントのSNSドリフト通知をサブスクライブできます (ベストプラクティスとして、サブスクライブする必要があります) 。例えば、 `aws-controltower-AggregateSecurityNotifications`SNSトピックはドリフト通知を提供します。AWS Control Tower コンソールは、ドリフトが発生したときに管理アカウント管理者に通知します。ドリフトの検出と通知に関するSNSトピックの詳細については、「ドリフトの防止と通知」を参照してください。

ドリフト通知の重複除外

同じタイプのドリフトが同じリソースセットで複数回発生する場合、AWSControl Tower はドリフトの最初のインスタンスに対してのみ SNS通知を送信します。AWS Control Tower は、このドリフトのインスタンスが修正されたことを検出した場合、それらの同じリソースに対してドリフトが再発生した場合にのみ、別の通知を送信します。

例: アカウントドリフトとSCPドリフトは、次の方法で処理されます。

- 同じマネージド をSCP複数回変更すると、初めて変更したときに通知が送信されます。
- マネージド を変更しSCP、ドリフトを修正してから再度変更すると、2 つの通知を受け取ります。
- アカウントを同じ送信元と送信先の間でOUs複数回移動する場合、最初にドリフトを修復せずに、アカウントがそれらの間でOUs複数回移動した場合でも、1 つの通知が送信されます。

アカウントドリフトのタイプ

- アカウントの移動 OUs
- アカウントが組織から削除

> **Note**
>
> アカウントを 1 つの OU から別の OU に移動しても、以前の OU のコントロールは削除されません。移動先 OU で新しいフックベースのコントロールを有効にすると、古いフックベースのコントロールがアカウントから削除され、新しいコントロールに置き換わります。SCPs および AWS Config ルールで実装されたコントロールは、アカウントが を変更したときに常に手動で削除する必要がありますOUs。

ポリシードリフトのタイプ

- SCP 更新済み
- SCP OU にアタッチされている
- SCP OU からデタッチされた
- SCP アカウントにアタッチされている

詳細については、「Types of Governance Drift」を参照してください。

ドリフトの解決

検出は自動ですが、ドリフトを解決するステップは、 コンソールを使用して手動で行うか、ResetEnabledControl を呼び出してコントロールに対して実行する必要がありますAPI。

- [Landing zone settings] (ランディングゾーン設定) ページでは、さまざまなタイプのドリフトを解決できます。これらのタイプのドリフトを解決するには、[バージョン] セクションの [リセット] ボタンを選択します。
- OU のアカウント数が 1000 未満の場合、組織ページまたは OU の詳細ページで OU の再登録 を選択することで、Account Factory SCP でプロビジョニングされたアカウントのドリフトを解決できます。
- 個々のアカウントを更新することで、移動したメンバーアカウント などのアカウントドリフトを解決できる場合があります。詳細については、「コンソールでアカウントを更新する」を参照してください。
- コントロールの場合、 を呼び出すことで、多くのタイプのドリフトを解決できますResetEnabledControlAPI。

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

- 最新のランディングゾーンバージョンを使用している場合、リセットを選択してから確認を選択すると、ドリフトしたランディングゾーンリソースは保存された AWS Control Tower 設定にリセットされます。ランディングゾーンバージョンは変わりません。
- 最新バージョンでない場合は、[更新] を選択する必要があります。ランディングゾーンは最新のランディングゾーンバージョンにアップグレードされます。このプロセスの一環としてドリフトが解決されます。

ドリフトとSCPスキャンに関する考慮事項

AWS Control Tower は、SCPs毎日マネージド をスキャンして、対応するコントロールが正しく適用され、ドリフトしていないことを確認します。を取得SCPsしてチェックを実行するために、AWSControl Tower AWS Organizations は管理アカウントのロールを使用して、ユーザーに代わって を呼び出します。

AWS Control Tower スキャンでドリフトが検出されると、通知が送信されます。 AWSControl Tower はドリフト問題ごとに 1 つの通知のみを送信するため、ランディングゾーンが既にドリフト状態になっている場合、新しいドリフト項目が見つからない限り、追加の通知は送信されません。

AWS Organizations は、各 を呼び出すAPIsことができる頻度を制限します。この制限は 1 秒あたりのトランザクション (TPS) で表され、TPS制限、スロットリングレート、またはAPIリクエストレートと呼ばれます。AWS Control Tower が を呼び出しSCPsて を監査する場合 AWS Organizations、AWSControl Tower が行うAPI呼び出しはTPS制限にカウントされます。これは、AWSControl Tower が管理アカウントを使用して呼び出しを行うためです。

まれに、サードパーティーのソリューションや作成したカスタムスクリプトを通じて同じ APIsを繰り返し呼び出すと、この制限に達することがあります。例えば、ユーザーと AWS Control Tower が同時に (1 秒以内に) 同じ AWS Organizations APIs を呼び出し、TPS制限に達すると、それ以降の呼び出しはスロットリングされます。つまり、これらのコールは `Rate exceeded` のようなエラーを返します。

API リクエストレートを超えた場合

- AWS Control Tower が制限に達してスロットリングされた場合、監査の実行を一時停止し、後で再開します。
- ワークロードが制限に達してスロットリングされた場合、その結果は、ワークロードの構成方法に応じて、わずかな遅延からワークロードの致命的なエラーにまで及ぶ可能性があります。このエッジケースには注意が必要です。

日次SCPスキャンは、 で構成されます。

1. 最近アクティブになった を取得しますOUs。
2. 登録された OU ごとに、OU にアタッチされている AWS Control Tower によってSCPs管理されるすべての を取得します。マネージドSCPsには、 で始まる識別子がありますaws-guardrails。
3. OU で有効になっている予防コントロールごとに、コントロールのポリシーステートメントが OU のマネージド に存在することを確認しますSCPs。

OU には、1 つ以上のマネージド がありますSCPs。

すぐに解決すべきドリフトのタイプ

ほとんどのタイプのドリフトは、管理者が解決できます。AWS Control Tower ランディングゾーンに必要な組織単位の削除など、いくつかのタイプのドリフトをすぐに解決する必要があります。回避すべき重要なドリフトの例を以下に示します。

- セキュリティ OU を削除しない： AWS Control Tower によって設定されたランディングゾーン中に、元々 Security と名付けられた組織単位は削除しないでください。削除すると、ランディングゾーンをすぐにリセットするように指示するエラーメッセージが表示されます。リセットが完了するまで、AWSControl Tower で他のアクションを実行することはできません。
- 必要なロールを削除しない： AWS Control Tower は、コンソールにログインしてロールのドリフトがないか、特定の AWS Identity and Access Management （ IAM) ロールをチェックします。 IAM これらのロールが見つからないかアクセス可能でない場合は、ランディングゾーンをリセットするように指示するエラーページが表示されます。これらのロールは、`AWSControlTowerAdmin` `AWSControlTowerCloudTrailRole` `AWSControlTowerStackSetRole` です。

  これらのユーザーロールの詳細については、「AWS Control Tower コンソールを使用するために必要なアクセス許可」を参照してください。
- すべての追加 を削除しないでくださいOUs： AWS Control Tower によって設定されたランディングゾーン中にサンドボックスという名前の組織単位を削除した場合、ランディングゾーンはドリフト状態になりますが、AWS引き続き Control Tower を使用できます。AWS Control Tower を動作させるには少なくとも 1 つの追加の OU が必要ですが、サンドボックス OU である必要はありません。
- 共有アカウントを削除しない: セキュリティ OU からログ記録アカウントを削除するなどOUs、基礎 から共有アカウントを削除すると、ランディングゾーンはドリフト状態になります。AWS Control Tower コンソールを引き続き使用する前に、ランディングゾーンをリセットする必要があります。

リソースへの修復可能な変更

以下は、解決可能なドリフトを作成するものの、許可される AWS Control Tower リソースへの変更のリストです。これらの許可されたオペレーションの結果は AWS Control Tower コンソールで表示できますが、更新が必要になる場合があります。

結果のドリフトを解決する方法の詳細については、AWS「Control Tower の外部でのリソースの管理」を参照してください。

AWS Control Tower コンソール以外で許可される変更

- 登録済み OU の名前変更。
- セキュリティ OU の名前変更。
- 基礎 以外の のメンバーアカウントの名前を変更しますOUs。
- セキュリティ OU で AWS Control Tower 共有アカウントの名前を変更します。
- 基礎以外の OU の削除。
- 基礎以外の OU からの登録済みアカウントの削除。
- セキュリティ OU での共有アカウントのメールアドレスの変更。
- 登録された OU 内のメンバーアカウントのメールアドレスの変更。

> **Note**
>
> 間でのアカウントの移動OUsはドリフトと見なされ、解決する必要があります。

ドリフトと新しいアカウントのプロビジョニング

ランディングゾーンがドリフト状態の場合、AWSControl Tower のアカウント登録機能は機能しません。その場合は、AWSService Catalog を使用して新しいアカウントをプロビジョニングする必要があります。手順については、AWS Service Catalog Account Factory でアカウントをプロビジョニングする を参照してください。

特に、ポートフォリオの名前変更など、Service Catalog を使用してアカウントに特定の変更を加えた場合、[Enroll account] (アカウントの登録) 機能は動作しません。

ガバナンスドリフトのタイプ

ガバナンスドリフトは、組織ドリフトとも呼ばれ、OUs、SCPs、およびメンバーアカウントが変更または更新されたときに発生します。AWS Control Tower で検出できるガバナンスドリフトのタイプは次のとおりです。

- 移動したメンバーアカウント
- 削除されたメンバーアカウント

- マネージド の計画外の更新 SCP
- SCP メンバーアカウントにアタッチされている
- SCP マネージド OU にアタッチされている
- SCP マネージド OU からデタッチされた

別のタイプのドリフトはランディングゾーンドリフトで、これは管理アカウントを通じて見られます。ランディングゾーンドリフトは、IAMロールドリフト、または基礎アカウントOUsと共有アカウントに特に影響を与える任意のタイプの組織ドリフトで構成されます。

- 削除された基礎 OU
- 信頼されたアクセスの無効化

ランディングゾーンドリフトの特殊なケースは、ロールドリフトで、必要なロールが利用できない場合に検出されます。このようなドリフトが発生すると、コンソールに警告ページと、ロールを復元する方法に関するいくつかの指示が表示されます。ロールドリフトが解決されるまで、ランディングゾーンは利用できません。ドリフトの詳細については、すぐに解決すべきドリフトのタイプ というセクションの「必要なロールを削除しない」を参照してください。

AWS Control Tower は、リソースコントロールポリシー () で実装されたコントロールと、サービスマネージドスタンダード: Control Tower の一部であるコントロールに関するコントロールドリフトを報告します。RCPs AWS Security Hub AWS

- Security Hub コントロールドリフト
- コントロールポリシーのドリフト

AWS Control Tower は、IAMIdentity Center など CloudTrail CloudWatch、管理アカウントと連携する他のサービスに関するドリフトを探しません AWS CloudFormation AWS Config。これらのアカウントは必須の予防コントロールによって保護されているため、子アカウントではドリフト検出は使用できません。

移動したメンバーアカウント

このタイプのドリフトは、OU ではなくアカウントで発生します。このタイプのドリフトは、AWSControl Tower メンバーアカウント、監査アカウント、またはログアーカイブアカウントが、登録された AWS Control Tower OU から他の OU に移動されたときに発生する可能性があります。このタイプのドリフトが検出された場合の Amazon SNS通知の例を次に示します。

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 1000 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

解決策

最大 1000 のアカウントを持つ OU の、Account Factory でプロビジョニングされたアカウントでこのタイプのドリフトが発生した場合は、次の方法で解決できます。

- AWS Control Tower コンソールの Organization ページに移動し、アカウントを選択し、右上の Update account を選択します (個々のアカウントの最短オプション)。
- AWS Control Tower コンソールの Organization ページに移動し、アカウントを含む OU の再登録 (複数のアカウントの最短オプション) を選択します。詳細については、「AWS Control Tower に既存の組織単位を登録する」を参照してください。
- Account Factory でプロビジョニングされた製品を更新する。詳細については、「AWS Control Tower または を使用して Account Factory アカウントを更新および移動する AWS Service Catalog」を参照してください。

  > **Note**
  >
  > 更新する個々のアカウントが複数ある場合は、スクリプト 自動化によるアカウントのプロビジョニングと更新 を使用して更新を行う方法も参照してください。

- 1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合、ドリフトの解決は、次の段落で説明するように、移動されたアカウントのタイプによって異なる場合があります。詳細については、「ランディングゾーンを更新する」を参照してください。

- Account Factory でプロビジョニングされたアカウントが移動された場合 — アカウントが 1000 未満の OU では、Account Factory でプロビジョニングされた製品を更新するか、OU を再登録するか、ランディングゾーンを更新することで、アカウントドリフトを解決できます。

  1,000 を超えるアカウントを持つ OU では、再登録 OU は更新を実行しないため、AWSControl Tower コンソールまたはプロビジョニング済み製品を使用して、移動した各アカウントを更新してドリフトを解決する必要があります。詳細については、「AWS Control Tower または を使用して Account Factory アカウントを更新および移動する AWS Service Catalog」を参照してください。
- 共有アカウントが移動された場合 — ランディングゾーンを更新することで、監査またはログアーカイブアカウントの移動によるドリフトを解決できます。詳細については、「ランディングゾーンを更新する」を参照してください。

> ⚠ 廃止されたフィールド名
>
> ガイドラインに準拠ManagementAccountIDするため、フィールド名MasterAccountIDはに変更されました AWS 。古い名前は廃止されました。2022 年以降、廃止されたフィールド名を含むスクリプトは機能しなくなりました。

削除されたメンバーアカウント

このタイプのドリフトは、登録された AWS Control Tower 組織単位からメンバーアカウントが削除されたときに発生する可能性があります。次の例は、このタイプのドリフトが検出されたときのAmazon SNS通知を示しています。

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
```

```
}
```

解決方法

- このタイプのドリフトがメンバーアカウントで発生した場合は、AWSControl Tower コンソールまたは 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。例えば、Account Factory の更新ウィザードから、別の登録された OU にアカウントを追加できます。詳細については、「AWS Control Tower または を使用して Account Factory アカウントを更新および移動する AWS Service Catalog」を参照してください。
- 共有アカウントが基礎 OU から削除された場合、ランディングゾーンをリセットしてドリフトを解決する必要があります。このドリフトが解決されるまで、AWSControl Tower コンソールを使用することはできません。
- アカウントと のドリフトの解決の詳細についてはOUs、「」を参照してくださいAWS Control Tower の外部でリソースを管理する場合。

> **Note**
>
> Service Catalog では、Account Factory でプロビジョニングされた製品のうちアカウントを表すものは、アカウントを削除するために更新されません。代わりに、プロビジョニングされた製品は TAINTED として表示され、エラー状態になります。クリーンアップするには、Service Catalog に移動し、プロビジョニングされた製品を選択してから、[Terminate] (終了) を選択します。

マネージド の計画外の更新 SCP

このタイプのドリフトは、コントロールSCPの がコンソールで AWS Organizations 更新されたとき、または AWS CLI または のいずれかを使用してプログラムで更新されたときに発生する可能性がありますAWSSDKs。このタイプのドリフトが検出された場合の Amazon SNS通知の例を次に示します。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
```

```
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

解決方法

最大 1000 アカウントの OU でこのタイプのドリフトが発生した場合は、次の方法で解決できます。

- AWS Control Tower コンソールの Organization ページに移動して、OU を再登録します (最短オプション)。詳細については、「AWS Control Tower に既存の組織単位を登録する」を参照してください。
- ランディングゾーンを更新する (時間のかかるオプション)。詳細については、「ランディングゾーンを更新する」を参照してください。

1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合は、ランディングゾーンを更新して解決してください。詳細については、「ランディングゾーンを更新する」を参照してください。

SCP マネージド OU にアタッチされている

このタイプのドリフトは、コントロールSCPの が他の OU にアタッチされている場合に発生する可能性があります。この発生は、AWSControl Tower コンソールの外部OUsから を操作する場合に特に一般的です。このタイプのドリフトが検出された場合の Amazon SNS通知の例を次に示します。

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

```
  "PolicyId" : "p-tEXAMPLE"
}
```

解決方法

最大 1000 アカウントの OU でこのタイプのドリフトが発生した場合は、次の方法で解決できます。

- AWS Control Tower コンソールの Organization ページに移動して OU を再登録します (最短オプション) 。詳細については、「AWS Control Tower に既存の組織単位を登録する」を参照してください。
- ランディングゾーンを更新する (時間のかかるオプション)。詳細については、「ランディングゾーンを更新する」を参照してください。

1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合は、ランディングゾーンを更新して解決してください。詳細については、「ランディングゾーンを更新する」を参照してください。

SCP マネージド OU からデタッチされた

このタイプのドリフトは、コントロールSCPの が AWS Control Tower によって管理されている 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。この発生は、AWSControl Tower コンソールの外部から作業する場合に特に一般的です。このタイプのドリフトが検出された場合の Amazon SNS通知の例を次に示します。

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

解決方法

最大 1000 アカウントの OU でこのタイプのドリフトが発生した場合は、次の方法で解決できます。

- AWS Control Tower コンソールで OU に移動して OU を再登録する (最も速いオプション) 。詳細については、「AWS Control Tower に既存の組織単位を登録する」を参照してください。
- ランディングゾーンを更新する (時間のかかるオプション)。ドリフトが必須コントロールに影響を与えている場合、更新プロセスは新しいサービスコントロールポリシー (SCP) を作成し、それを OU にアタッチしてドリフトを解決します。ランディングゾーンを更新する方法については、「ランディングゾーンを更新する」を参照してください。

1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合は、ランディングゾーンを更新して解決してください。ドリフトが必須コントロールに影響を与えている場合、更新プロセスは新しいサービスコントロールポリシー (SCP) を作成し、それを OU にアタッチしてドリフトを解決します。ランディングゾーンを更新する方法については、「ランディングゾーンを更新する」を参照してください。

SCP メンバーアカウントにアタッチされている

このタイプのドリフトは、コントロールSCPの が Organizations コンソールのアカウントにアタッチされている場合に発生する可能性があります。ガードレールとそのガードレールは、AWSControl Tower コンソールを介して で有効にできます OUs (したがって、OU のすべての登録済みアカウントに適用SCPsできます) 。このタイプのドリフトが検出された場合の Amazon SNS通知の例を次に示します。

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

解決方法

このタイプのドリフトは、OU ではなくアカウントで発生します。

セキュリティ OU などの基礎 OU のアカウントでこのタイプのドリフトが発生した場合の解決策は、ランディングゾーンを更新することです。詳細については、「ランディングゾーンを更新する」を参照してください。

最大 1000 アカウントを持つ、基礎以外の OU でこのタイプのドリフトが発生した場合は、次のように解決できます。

- Account Factory アカウントSCPから AWS Control Tower をデタッチします。
- AWS Control Tower コンソールで OU に移動して OU を再登録する (最も速いオプション) 。詳細については、「AWS Control Tower に既存の組織単位を登録する」を参照してください。

1000 を超えるアカウントを持つ OU でこのタイプのドリフトが発生した場合は、アカウントの Account Factory 設定を更新することで解決を試みることができます。正常には解決できない場合があります。詳細については、「ランディングゾーンを更新する」を参照してください。

削除された基礎 OU

このタイプのドリフトはOUs、セキュリティ OU などの AWS Control Tower Foundational にのみ適用されます。これは、基礎 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。OU の移動は削除して別の場所に追加するのと同じであるため、このタイプのドリフトを作成しないと基礎を移動OUsできません。ランディングゾーンを更新してドリフトを解決すると、AWSControl Tower は元の場所の基本的な OU を置き換えます。次の例は、このタイプのドリフトが検出されたときに受信できる Amazon SNS通知を示しています。

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

解決方法

このドリフトは Foundational に対してOUsのみ発生するため、解決策はランディングゾーンを更新することです。他のタイプの が削除されOUsると、AWSControl Tower は自動的に更新されます。

アカウントと のドリフトの解決の詳細についてはOUs、「」を参照してくださいAWS Control Tower の外部でリソースを管理する場合。

Security Hub コントロールドリフト

このタイプのドリフトは、AWS Security Hub サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールがドリフトの状態をレポートした場合に発生します。 AWS Security Hub サービス自体は、これらのコントロールのドリフト状態を報告しません。代わりに、サービスは検出結果を AWS Control Tower に送信します。

Security Hub コントロールドリフトは、AWSControl Tower が Security Hub からステータス更新を 24 時間以上受け取っていない場合にも検出できます。これらの検出結果が期待どおりに受信されない場合、AWSControl Tower はコントロールがドリフトしていることを確認します。次の例は、このタイプのドリフトが検出されたときに受信できる Amazon SNS通知を示しています。

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "SH.XXXXXXX.1",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>".
"Region" : "us-east-1"
}
```

解決方法

アカウントOUsが 1000 未満の の場合、推奨される解決方法は、ドリフトされたコントロールResetEnabledControlAPIの を呼び出すことです。コンソールでは、OU の再登録を選択できます。これにより、コントロールが元の状態にリセットされます。または、どの OU でも、コンソールまたは AWS Control Tower を使用してコントロールを削除して再度有効にできます。これによりAPIs、コントロールもリセットされます。

アカウントと のドリフトの解決の詳細についてはOUs、「」を参照してくださいAWS Control Tower の外部でリソースを管理する場合。

コントロールポリシーのドリフト

このタイプのドリフトは、リソースコントロールポリシー (RCPs) または宣言ポリシーで実装されたコントロールがドリフトの状態をレポートした場合に発生します。これは の状態を返します。CONTROL_INEFFECTIVEこれは AWS Control Tower コンソールとドリフトメッセージで表示できます。このタイプのドリフトのドリフトメッセージには、影響を受けるコントロールEnabledControlIdentifierの も含まれます。

このタイプのドリフトは、 SCPベースのコントロールでは報告されません。

次の例は、このタイプのドリフトが検出されたときに受信できる Amazon SNS通知を示しています。

```
{
    "Message": "AWS Control Tower detects that a policy it owns was updated
 unexpectedly. This mismatch indicates that configuration changes were made outside of
 AWS Control Tower.",
    "MasterAccountId": "123456789XXX",
    "ManagementAccountId": "123456789XXX",
    "OrganizationId": "o-123EXAMPLE",
    "DriftType": "CONTROL_INEFFECTIVE",
    "RemediationStep": "To remediate the issue, Reset the DRIFTED enabled control if
 permitted or Re-register the OU. If the problem persists, contact AWS support.",
    "TargetIdentifier": "arn:aws:::organizations/o-123456/ou-1234-4567",
    "ControlId": "CT.XXXXXXX.PV.1",
    "ControlName": "EBS snapshots should not be publicly restorable",
    "ApiControlIdentifier": "arn:aws:controlcatalog:::control/<UNIQUE_ID>",
    "EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>"
}
```

解決方法

AWS Control Tower で有効になっているコントロール、宣言型ポリシーコントロール、Security Hub コントロールに対するRCPコントロールポリシーのドリフトの最も簡単な解決策は、`ResetEnabledControl` を呼び出すことですAPI。

アカウントOUsが 1,000 未満の の場合、コンソールまたは からの別の解決策APIは、OU を再登録することです。これにより、コントロールが元の状態にリセットされます。

個々の OU の場合、コンソールまたは AWS Control Tower を使用してコントロールを削除および再有効化できます。これによりAPIs、コントロールもリセットされます。

アカウントと のドリフトの解決の詳細についてはOUs、「」を参照してくださいAWS Control Tower の外部でリソースを管理する場合。

信頼されたアクセスの無効化

このタイプのドリフトは、AWSControl Tower ランディングゾーンに適用されます。これは、AWSControl Tower ランディングゾーンを設定 AWS Organizations した後に、 で AWS Control Tower への信頼されたアクセスを無効にした場合に発生します。

信頼されたアクセスが無効になっている場合、AWSControl Tower は から変更イベントを受信しなくなります AWS Organizations。 AWSControl Tower は、これらの変更イベントを使用して同期を維持します AWS Organizations。その結果、AWSControl Tower はアカウント および の組織的な変更を見逃す可能性がありますOUs。そのため、ランディングゾーンを更新するたびに、各 OU を再登録することが重要です。

例: Amazon SNS通知

このタイプのドリフトが発生したときに受信する Amazon SNS通知の例を次に示します。

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
```

```
}
```

解決方法

AWS Control Tower コンソールでこのタイプのドリフトが発生すると、AWSControl Tower から通知されます。解決策は、AWSControl Tower ランディングゾーンをリセットすることです。詳細については、「ドリフトの解決」を参照してください。

AWS Control Tower の外部でリソースを管理する場合

AWS Control Tower は、ユーザーに代わってアカウント、組織単位、その他のリソースを設定しますが、ユーザーはこれらのリソースの所有者です。これらのリソースは、AWSControl Tower 内またはその外部で変更できます。AWS Control Tower の外部でリソースを変更する最も一般的な場所は、 AWS Organizations コンソールです。このトピックでは、AWSControl Tower の外部で変更を行うときに、AWSControl Tower リソースの変更を調整する方法について説明します。

AWS Control Tower コンソールの外部でリソースの名前変更、削除、および移動を行うと、コンソールの同期が停止します。変更の多くは自動的に調整されます。AWS Control Tower コンソールに表示される情報を更新するには、特定の変更でランディングゾーンへのリセットが必要です。

一般的に、AWSControl Tower コンソールの外部で AWS Control Tower リソースに加えた変更は、ランディングゾーンに解決可能なドリフトの状態を作成します。これらの変更の詳細については、「リソースへの修復可能な変更」を参照してください。

ランディングゾーンのリセットが必要なタスク

- セキュリティ OU の削除 (特殊なケースであるため、不用意に行わないでください)
- セキュリティ OU からの共有アカウントの削除 (非推奨)
- セキュリティ OU SCPに関連付けられた を更新、アタッチ、またはデタッチします。

AWS Control Tower によって自動的に更新される変更

- 登録済みアカウントの E メールアドレスの変更
- 登録済みアカウントの名前変更
- 新しい最上位の組織単位 (OU) の作成
- 登録済み OU の名前変更
- 登録済み OU の削除 (更新が必要なセキュリティ OU は除きます)

- 登録済みアカウントの削除 (セキュリティ OU の共有アカウントは除きます)

> **Note**
>
> AWS Service Catalog は AWS Control Tower とは異なる方法で変更を処理します。変更を調整すると、ガバナンス体制に変更が生じる AWS Service Catalog 場合があります。プロビジョニング済み製品の更新の詳細については、 AWS Service Catalog ドキュメントの「プロビジョニング済み製品の更新」を参照してください。

AWS Control Tower 外のリソースを参照する

AWS Control Tower の外部で新しい アカウントOUsと アカウントを作成する場合、それらは表示されていても AWS Control Tower によって管理されません。

OU の作成

AWS Control Tower の外部で作成された組織単位 (OUs) は未登録と呼ばれます。これらは Organization ページに表示されますが、AWSControl Tower コントロールによって管理されません。

アカウントの作成

AWS Control Tower の外部で作成されたアカウントは、未登録と呼ばれます。AWS Control Tower に登録されている OU に属する登録済みアカウントと登録されていないアカウントは、組織ページに表示されます。登録済み OU に属していないアカウントは、 AWS Organizations コンソールを使用して招待できます。この参加の招待では、アカウントを AWS Control Tower に登録したり、AWSControl Tower ガバナンスをアカウントに拡張したりしません。アカウントを登録してガバナンスを拡張するには、AWSControl Tower の組織ページまたはアカウント詳細ページに移動し、アカウントの登録を選択します。

AWS Control Tower リソース名を外部で変更する

AWS Control Tower コンソールの外部で組織単位 (OUs) とアカウントの名前を変更でき、それらの変更を反映するためにコンソールが自動的に更新されます。

OU の名前変更

では AWS Organizations、 または コンソールを使用して AWS Organizations API OU の名前を変更できます。AWS Control Tower の外部で OU 名を変更すると、AWSControl Tower コンソールに名

前の変更が自動的に反映されます。ただし、 を使用してアカウントをプロビジョニングする場合は AWS Service Catalog、 AWS Control Tower が と整合性を保つようにランディングゾーンをリセットする必要があります AWS Organizations。リセットワークフローは、基礎 および追加 のサービス間の一貫性を保証しますOUs。このタイプのドリフトは、[ランディングゾーン設定] ページから解決できます。「AWS Control Tower でドリフトを検出して解決する」の「ドリフトの解決」を参照してください。

AWS Control Tower は、AWSControl Tower ダッシュボードの OUs Organization ページに の名前を表示します。ランディングゾーンのリセットオペレーションが正常に完了したことを確認できます。

登録済みアカウントの名前変更

各 AWS アカウントには、 AWS Billing and Cost Management コンソールでアカウントのルートユーザーが変更できる表示名があります。AWS Control Tower に登録されているアカウントの名前を変更すると、名前の変更は自動的に AWS Control Tower に反映されます。アカウント名の変更の詳細については、AWS 「 Billing User Guide」の「Managing an AWS account」を参照してください。

セキュリティ OU の削除

このタイプのドリフトは特殊なケースです。セキュリティ OU を削除すると、ランディングゾーンのリセットを求めるエラーメッセージページが表示されます。AWS Control Tower で他のアクションを実行する前に、ランディングゾーンをリセットする必要があります。

- AWS Control Tower コンソールでアクションを実行することはできず、 AWS Service Catalog リセットが完了するまで で新しいアカウントを作成することはできません。
- [ランディングゾーン設定] ページを開いても、そのページに [リセット] ボタンは表示されません。

この場合、ランディングゾーンのリセットプロセスによって新しいセキュリティ OU が作成され、2 つの共有アカウントが新しいセキュリティ OU に移動されます。 AWSControl Tower は、ログアーカイブアカウントと監査アカウントをドリフト済みとしてマークします。どちらのアカウントでも同じプロセスでドリフトが解決されます。

[Security] (セキュリティ) OU を削除する必要があると判断した場合は、次の点に留意してください。

[Security] (セキュリティ) OU を削除する前に、その OU にアカウントが含まれていないことを確認する必要があります。具体的には、OU からログアーカイブアカウントと監査アカウントを削除する必要があります。これらのアカウントを別の OU に移動することをお勧めします。

> **Note**
>
> セキュリティ OU を削除するアクションは不用意に実行しないでください。ログが一時的に停止されている場合、一部のコントロールが適用されない可能性があるため、このアクションによりコンプライアンスの問題が発生することがあります。

ドリフトに関する一般的な情報については、「AWS Control Tower でドリフトを検出して解決する」の「ドリフトの解決」を参照してください。

セキュリティ OU からのアカウントの削除

組織から共有アカウントを削除したり、[Security] (セキュリティ) OU から共有アカウントを移動したりすることはお勧めしません。誤って共有アカウントを削除した場合は、このセクションの修復ステップに従ってアカウントを復元できます。

- AWS Control Tower コンソール内から: 修復プロセスを開始するには、半手動修復ステップに従います。AWS Control Tower コンソールへのアクセスに使用するユーザーまたはロールに、 を実行するアクセス許可があることを確認しますorganizations:InviteAccountToOrganization。このようなアクセス許可がない場合は、手動修復ステップに従います。このステップでは、AWSControl Tower コンソールと AWS Organizations コンソールの両方を使用します。
- AWS Organizations コンソールから開始： この修復プロセスは、少し長く、完全に手動の手順です。手動修復手順に従うと、 AWS Organizations コンソールと AWS Control Tower コンソールが切り替わります。で作業するときは AWS Organizations、 AWSOrganizationsFullAccess管理ポリシーまたは同等のポリシーを持つユーザーまたはロールが必要です。AWS Control Tower コンソールで作業する場合、 AWSControlTowerServiceRolePolicy管理ポリシーまたは同等のポリシーを持つユーザーまたはロール、およびすべての AWS Control Tower アクション (controltower:*) を実行するアクセス許可が必要です。
- 修復ステップでアカウントが復元されない場合は、 AWS サポートにお問い合わせください。

共有アカウントを削除した結果 AWS Organizations：

- アカウントは、サービスコントロールポリシー () による AWS Control Tower の必須コントロールによって保護されなくなりましたSCPs。結果： アカウントで AWS Control Tower によって作成されたリソースは、変更または削除される場合があります。

- アカウントは AWS Organizations 管理アカウントの下に存在しなくなりました。結果： AWS Organizations 管理アカウントの管理者は、アカウントの支出を可視化できなくなりました。
- アカウントが によってモニタリングされることは保証されなくなりました AWS Config。結果： AWS Organizations 管理アカウントの管理者は、リソースの変更を検出できない場合があります。
- アカウントが組織内に存在しなくなります。結果： AWS Control Tower の更新とリセットは失敗します。

AWS Control Tower コンソールを使用して共有アカウントを復元するには (半手動手順)

1. https://console.aws.amazon.com/controltower で AWS Control Tower コンソールにサインインします。ユーザーIAM、IAMIdentity Center のユーザー、または を実行するアクセス許可を持つロールとしてサインインする必要がありますorganizations:InviteAccountToOrganization。このような許可がない場合は、このトピックで後述する手動修復ステップを使用してください。
2. [Landing zone drift detected] (ランディングゾーンのドリフトが検出されました) ページで、[Re-Invite] (再招待) を選択して、共有アカウントを組織に再招待することで共有アカウントの削除を修復します。自動的に生成された E メールが、アカウントの E メールアドレスに送信されます。
3. 招待を承諾して、共有アカウントを組織に戻します。次のいずれかを行います。
   - 削除された共有アカウントにサインインし、https://console.aws.amazon.com/organizations/home#/invites に移動します。
   - アカウントを再招待したときに送信された E メールメッセージにアクセスできる場合は、削除したアカウントにサインインし、メッセージ内のリンクをクリックして、アカウントの招待に直接移動します。
   - 削除された共有アカウントが別の組織にない場合は、アカウントにサインインし、 AWS Organizations コンソールを開いて招待に移動します。
4. 管理アカウントに再度サインインするか、AWSControl Tower コンソールがすでに開いている場合は再ロードします。[Landing zone drift] (ランディングゾーンドリフト) ページが表示されます。[リセット] を選択してランディングゾーンを修復します。
5. リセットプロセスが完了するまで待ちます。

修復が成功すると、共有アカウントが通常の状態およびコンプライアンスで表示されます。

修復ステップでアカウントが復元されない場合は、 AWS サポートにお問い合わせください。

AWS Control Tower と AWS Organizations コンソールを使用して共有アカウントを復元するには (手動修復)

1. で AWS Organizations コンソールにサインインしますhttps://console.aws.amazon.com/organizations/。AWSOrganizationsFullAccess 管理ポリシーまたは同等のポリシーを使用して、 IAM ユーザー、IAMIdentity Center のユーザー、またはロールとしてサインインする必要があります。
2. 共有アカウントを組織に招待し直します。アカウントを招待する要件、前提条件、手順については AWS Organizations、「 ユーザーガイド」の「組織への AWS アカウントの招待」を参照してください。 AWS Organizations
3. 削除された共有アカウントにサインインし、https://console.aws.amazon.com/organizations/home#/invites に移動して招待を受け入れます。
4. 管理アカウントにもう一度サインインします。。
5. AWSControlTowerServiceRolePolicy 管理ポリシーまたは同等のポリシーを持つユーザーまたはロールとして AWS Control Tower コンソールにサインインし、すべての AWS Control Tower アクション (コントローラー:*) を実行するアクセス許可を付与します。
6. [ランディングゾーンのドリフト] ページが表示されます。ここには、ランディングゾーンをリセットするオプションがあります。[リセット] を選択してランディングゾーンを修復します。
7. リセットプロセスが完了するまで待ちます。

修復が成功すると、共有アカウントが通常の状態およびコンプライアンスで表示されます。

修復ステップでアカウントが復元されない場合は、 AWS サポートにお問い合わせください。

自動的に更新される外部変更

アカウントの E メールアドレスに加えた変更は、AWSControl Tower によって自動的に更新されますが、Account Factory によって自動的に更新されることはありません。

管理対象アカウントの E メールアドレスの変更

AWS Control Tower は、コンソールエクスペリエンスの必要に応じて E メールアドレスを取得して表示します。したがって、共有およびその他のアカウントの E メールアドレスは、変更後に Control Tower AWS で一貫して更新および表示されます。

> **Note**
>
> では AWS Service Catalog、プロビジョニング済み製品の作成時にコンソールで指定されたパラメータが Account Factory に表示されます。ただし、元のアカウントの E メールアドレスは変更されても、自動的には更新されません。これは、アカウントがプロビジョニングされた製品に概念的に含まれているためです。プロビジョニングされた製品とは異なります。この値を更新するには、プロビジョニングされた製品を更新する必要があります。これにより、ガバナンス体制が変更される可能性があります。

外部 AWS Config ルールの適用

AWS Control Tower は、AWSControl Tower コンソールの外部でアクティブ化された AWS Config ルールを含め、AWSControl Tower に登録された組織単位にデプロイされたすべてのルールのコンプライアンスステータスを表示します。

AWS Control Tower の外部での AWS Control Tower リソースの削除

AWS Control Tower で OUsおよび アカウントを削除でき、更新を表示するためにそれ以上のアクションを実行する必要はありません。Account Factory は、OU を削除したときには自動的に更新されますが、アカウントを削除したときには更新されません。

登録済み OU の削除 (セキュリティ OU は除きます)

内では AWS Organizations、 APIまたは コンソールを使用して、空の組織単位 (OUs) を削除できます。アカウントOUsを含む は削除できません。

AWS OU が削除され AWS Organizations ると、Control Tower は から通知を受け取ります。Account Factory の OU リストを更新して、登録された のリストの整合性OUsを維持します。

> **Note**
>
> では AWS Service Catalog、Account Factory が更新され、アカウントをプロビジョニング OUsできる のリストから削除された OU が削除されます。

OU からの登録済みアカウントの削除

登録済みのアカウントを削除すると、AWSControl Tower は通知を受信して更新し、情報の整合性を維持します。

> **Note**
>
> では AWS Service Catalog、管理対象アカウントを表す Account Factory プロビジョニング済み製品は、アカウントを削除するために更新されません。代わりに、プロビジョニングされた製品は `TAINTED` として表示され、エラー状態になります。クリーンアップするには、AWS Service Catalogに移動し、プロビジョニングされた製品を選択してから、[Terminate] (削除) を選択します。

AWS Control Tower で組織とアカウントを管理する

AWS Control Tower で作成するすべての組織単位 (OUs) とアカウントは、Control Tower AWS によって自動的に管理されます。また、AWSControl Tower の外部で作成された既存の アカウント OUsと アカウントがある場合は、AWSそれらを Control Tower ガバナンスに取り込むことができます。

既存の アカウント AWS Organizations と AWS アカウントの場合、ほとんどのお客様は、アカウントを含む組織単位 (OU) 全体を登録することで、アカウントのグループを登録することを好みます。アカウントを個別に登録することもできます。個々のアカウント登録の詳細については、「既存のを登録する AWS アカウント」を参照してください。

用語

- 既存の組織を AWS Control Tower に持ち込む場合、組織を登録するか、ガバナンスを組織に拡張します。
- AWS Control Tower に AWS アカウントを持ち込むと、アカウントの登録と呼ばれます。

OUsおよび アカウントを表示する

AWS Control Tower Organization ページで、AWSControl Tower に登録OUsされている や登録されていない など AWS Organizations、 OUs 内のすべての を表示できます。ネストされた を階層OUsの一部として表示できます。右上のドロップダウンから [Organizational units only] (組織単位のみ) を選択すると、[Organization] (組織) ページで組織単位を表示できます。

組織ページには、AWSControl Tower の OU または登録ステータスに関係なく、組織内のすべてのアカウントが一覧表示されます。右上のドロップダウンから [Organization only] (アカウントのみ) を選択すると、[Organization] (組織) ページでアカウントを表示できます。アカウントが登録の前提条件を満たしている場合は、 内でアカウントを個別に表示、更新OUs、登録できます。

フィルタリングを選択しない場合、組織ページにはアカウントと が階層OUsに表示されます。これは、すべての AWS Control Tower リソースをモニタリングし、アクションを実行するための中心的な場所です。[Organization] (組織) ページの詳細については、動画チュートリアルをご覧ください。

動画チュートリアル

このビデオ (4:01) では、AWSControl Tower の Organization ページを操作する方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

AWS Control Tower での組織ページの使用に関するビデオチュートリアル。

トピック

- AWS Control Tower に既存の組織単位を登録する
- 既存の を登録する AWS アカウント

ガバナンスを既存の組織に拡張する

「開始方法、ステップ 2」のAWS「Control Tower ユーザーガイド」で説明されているようにランディングゾーン (LZ) を設定することで、既存の組織に AWS Control Tower ガバナンスを追加できます。 https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html#step-two

既存の組織で AWS Control Tower ランディングゾーンをセットアップする場合に予想されることは次のとおりです。

- AWS Organizations 組織ごとに 1 つのランディングゾーンを設定できます。
- AWS Control Tower は、既存の AWS Organizations 組織の管理アカウントを管理アカウントとして使用します。新しい管理アカウントは不要です。
- AWS Control Tower は、登録された OU に監査アカウントとログ記録アカウントの 2 つの新しいアカウントを設定します。
- 組織のサービスの制限により、これら 2 つの追加のアカウントの作成が許可されている必要があります。
- ランディングゾーンを起動するか、OU を登録すると、その OU に登録されているすべてのアカウントに AWS Control Tower コントロールが自動的に適用されます。
- AWS Control Tower によって管理される OU に追加の既存の AWS アカウントを登録して、それらのアカウントにコントロールを適用できます。
- AWS Control Tower OUsでさらに を追加し、既存の を登録できますOUs。

登録と登録のその他の前提条件を確認するには、AWS「Control Tower の開始方法」を参照してください。

AWS Control Tower ランディングゾーンが設定されていないAWS組織OUsで Control Tower AWS コントロールが に適用されない方法の詳細については、以下を参照してください。

- AWS Control Tower Account Factory の外部で作成された新しいアカウントは、登録された OU のコントロールによってバインドされません。
- AWS Control Tower に登録OUsされていない で作成された新しいアカウントは、特にそれらのアカウントを AWS Control Tower に登録しない限り、コントロールによって制限されません。アカウントの登録の詳細については、「既存の を登録する AWS アカウント」を参照してください。
- 追加の既存の組織、既存のアカウント、および AWS Control Tower の外部で新規OUsまたは作成するアカウントは、OU を個別に登録するか、アカウントを登録しない限り、AWSControl Towerコントロールによって制限されません。

AWS Control Tower を既存の OUsおよびアカウントに適用する方法の詳細については、「」を参照してくださいAWS Control Tower に既存の組織単位を登録する。

既存の組織で AWS Control Tower ランディングゾーンを設定するプロセスの概要については、次のセクションの動画を参照してください。

> **Note**
>
> セットアップ中、AWSControl Tower は一般的な問題を避けるために事前チェックを実行します。ただし、現在 AWS ランディングゾーンソリューションを使用している場合は AWS Organizations、組織で AWS Control Tower を有効にして Control Tower が現在のランディングゾーンのデプロイを妨げる可能性があるかどうかを判断する前に、 AWS ソリューションアーキテクトAWSに確認してください。また、ランディングゾーン間でのアカウントの移動については、「アカウントが前提条件を満たしていない場合」を参照してください。

動画: 既存の AWS Organizationsでランディングゾーンを有効にする

このビデオ (7:48) では、既存の AWS Organizations 構造で AWS Control Tower ランディングゾーンを設定および有効にする方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

既存の組織の AWS Control Tower を有効にする

IAM Identity Center と既存の組織に関する考慮事項

- AWS IAM Identity Center （ IAM Identity Center) が既に設定されている場合、AWSControl Towerホームリージョンは IAM Identity Center リージョンと同じである必要があります。

- AWS Control Tower は既存の設定を削除しません。
- IAM Identity Center が既に有効になっており、IAMIdentity Center Directory を使用している場合、AWSControl Tower はアクセス許可セット、グループなどのリソースを追加し、通常どおり続行します。
- 別のディレクトリ (外部、AD、マネージド AD) が設定されている場合、AWSControl Tower は既存の設定を変更しません。詳細については、AWS IAM Identity Center (IAM Identity Center) のお客様に関する考慮事項を参照してください。

他の AWS サービスへのアクセス

組織を AWS Control Tower ガバナンスに導入した後も、 コンソールと を使用して AWS Organizations AWS Organizations 、 を通じて利用可能な AWS サービスにアクセスできますAPIs。詳細については、「関連する AWS のサービス」を参照してください。

AWS Control Tower OUsにネストされている

この章では、AWSControl Tower OUsでネストされた を使用する際に注意すべき期待と考慮事項を示します。ほとんどの場合、ネストされた の操作OUsは、フラットな OU 構造の操作と同じです。登録および再登録機能は、この章で説明されている変更された動作を除きOUs、ネストされたで動作します。

動画チュートリアル

このビデオ (4:46) では、AWSControl Tower でネストされた OU デプロイを管理する方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

AWS Control Tower OUsでネストを管理するビデオチュートリアル。

ネストされた OUsとランディングゾーンのベストプラクティスに関するガイダンスについては、ブログ記事「ネストされた で AWS Control Tower ランディングゾーンを整理するOUs」を参照してください。

フラットな OU 構造からネストされた OU 構造への拡張

フラットな OU 構造で AWS Control Tower ランディングゾーンを作成した場合は、ネストされた OU 構造に拡張できます。

このプロセスには主に次の 4 つのステップがあります。

1. AWS Control Tower で目的のネストされた OU 構造を作成します。
2. AWS Organizations コンソールに移動し、一括移動機能を使用して、アカウントをソース OU (フラット) から宛先 OU (ネスト) に移動します。その方法は次のとおりです。
   a. アカウントの移動元となる OU に移動します。
   b. OU 内のすべてのアカウントを選択します。
   c. [Move] (移動) を選択します。

   > **Note**
   >
   > AWS Control Tower には移動機能がないため、このステップは AWS Organizations コンソールの で実行する必要があります。

3. AWS Control Tower のネストされた OU に移動し、登録または再登録します。ネストされた OU 内のすべてのアカウントが登録されます。
   - AWS Control Tower で OU を作成した場合は、OU を再登録します。
   - で OU を作成した場合は AWS Organizations、OU を初めて登録します。
4. アカウントを移動して登録したら、コンソールまたは AWS Control Tower AWS Organizations コンソールから空の最上位 OU を削除します。

ネストされた OU の登録の事前チェック

ネストされたアカウントOUsとそのメンバーアカウントの正常な登録をサポートするために、AWSControl Tower は一連の事前チェックを実行します。これと同じ事前チェックが、最上位の OU またはネストされた OU を登録するときにも実行されます。詳細については、「Common causes of failure during registration or re-registration」を参照してください。

- すべての事前チェックに合格すると、AWSControl Tower は自動的に OU の登録を開始します。
- 事前チェックが失敗した場合、AWSControl Tower は登録プロセスを停止し、OU を登録する前に修正する必要がある項目のリストを提供します。

ネストされた OUsロールと ロール

AWS Control Tower は`AWSControlTowerExecution`、ターゲット OU の下のアカウントと、ターゲット OU OUs の下のネストされたすべてのアカウントのアカウントに、ロールをデプロ

イします。これは、ターゲット OU のみを登録する意図がある場合も同様です。管理アカウント [Administrator] (管理者) のすべてのユーザーに、AWSControlTowerExecution ロールを持つアカウントに対する許可が付与されます。ロールを使用して、AWS通常 Control Tower コントロールで許可されないアクションを実行できます。

このロールは、登録する予定がない未登録のアカウントから削除できます。このロールを削除すると、ロールをアカウントに復元しない限り、アカウントを AWS Control Tower に登録したりOUs、直接の親 を登録したりすることはできません。アカウントからAWSControlTowerExecutionロールを削除するには、そのAWSControlTowerExecutionロールでサインインする必要があります。これは、AWSControl Tower によって管理されるロールを他のIAMプリンシパルが削除できないためです。

ロールのアクセスを制限する方法については、「Optional conditions for your role trust relationships」を参照してください。

ネストされた アカウントと アカウントの登録OUs時および再登録時に何が起こるか

ネストされた OU を登録または再登録すると、AWSControl Tower はターゲット OU のすべての未登録アカウントを登録し、すべての登録済みアカウントを更新します。以下のような処理が発生すると想定されています。

AWS Control Tower は以下のタスクを実行します。

- この OU で登録されていないすべてのアカウントと、ネストされた で登録されていないすべてのアカウントにAWSControlTowerExecutionロールを追加しますOUs。
- 未登録のメンバーアカウントを登録します。
- 登録済みのメンバーアカウントを再登録します。
- 新しく登録されたメンバーアカウントの IAM Identity Center ログインを作成します。
- 既存の登録済みのメンバーアカウントを更新して、ランディングゾーンへの変更を反映します。
- この OU とそのメンバーアカウント用に設定されているコントロールを更新します。

ネストされた OU を登録する際の考慮事項

- コア OU (セキュリティ OU) の下に OU を登録することはできません。
- ネストされた は個別に登録OUsする必要があります。
- 親 OU が登録されていない限り、OU を登録することはできません。

- ツリー内のOUs上位のすべての がしばらく正常に登録されていない限り (削除されている可能性があります) 、OU を登録することはできません。
- 上位にあるドリフトされた OU の下に OU を登録することはできますが、そのアクションによってドリフトが修復されることはありません。

ネストされた OU の制限

- OUs は、ルートの下に最大 5 レベルの深さでネストできます。
- ターゲット OU OUsの下にネストされている は、個別に登録または再登録する必要があります。
- ターゲット OU が階層のレベル 2 以下である場合、つまり最上位 OU でない場合、より高い で有効になっている予防コントロールOUsは、この OU とそのOUs下位すべてに自動的に適用されます。
- OU 登録の失敗は、階層ツリーの上位に伝播されません。ネストされた の状態に関する詳細は、OUs親の OU の詳細ページで確認できます。
- OU 登録の失敗は、階層ツリーの下位に伝播されません。
- AWS Control Tower は、新規または既存のアカウントのVPC設定を変更しません。

ネストされた OUsとコンプライアンス

AWS Control Tower コンソールから、組織ページで非準拠の アカウントOUsと アカウントを表示できるため、コンプライアンスをより大規模に把握できます。

ネストされた アカウントOUsと アカウントのコンプライアンスに関する考慮事項

- OU のコンプライアンスは、その下にネストされた OUs のコンプライアンスに基づいて決定されません。
- コントロールのコンプライアンスステータスは、ネストされた を含め、コントロールが有効になっているすべての OUsに対して計算されますOUs。AWS OUs 「 および アカウントの Control Tower コンプライアンスステータス」を参照してください。
- OU は、OU 階層内のどこに配置されているかにかかわらず、非準拠のアカウントがある場合にのみ非準拠として表示されます。
- ネストされた OU が非準拠の場合、その親 OU は自動的に非準拠とは見なされません。
- OU の詳細ページまたはアカウントの詳細ページで、 OUsまたは アカウントが非準拠ステータスを表示している可能性がある非準拠リソースのリストを表示できます。

ネストOUsおよびドリフト

状況によっては、ドリフトによってネストされた の登録が妨げられることがありますOUs。

ドリフトとネストの期待値 OUs

- ドリフトした親OUsを使用して でコントロールを有効にできますが、直接ドリフトすることはできませんOUs。
- ドリフトされた OU の下で検出コントロールを有効にすることができます。ただし、最上位のドリフトされた OU でない場合に限られます。
- 必須コントロールは最上位OUsでのみ有効になります。ネストされた OU を登録するときには、必須コントロールはスキップされます。
- 1 つの必須コントロールは AWS Config リソースを保護するため、ネストされた を登録するには、そのコントロールがドリフトしていない状態である必要がありますOUs。ドリフトしている場合、AWSControl Tower はネストされた の登録をブロックしますOUs。
- 最上位の OU がドリフトしている場合、 AWS Config リソースを保護するコントロールはドリフトしている可能性があります。この場合、AWSControl Tower は、検出コントロールの適用を含め、 AWS Config リソースの作成または更新を必要とするアクションをブロックします。

ネストされた OUsおよび コントロール

登録済みの OU でコントロールを有効にした場合、予防コントロールと検出コントロールでは動作が異なります。ネストされた の場合OUs、プロアクティブコントロールは検出コントロールと同様に動作します。

予防コントロール

- ネストされた には予防コントロールが適用されますOUs。
- 必須の予防コントロールは、OU とそのネストされた のすべてのアカウントに適用されますOUs。
- 予防的コントロールOUsは、すべてのアカウントに影響し、ターゲット OUs OU の下にネストされます。それらのアカウントと が登録されていない場合でも影響を受けます。

検出コントロールとプロアクティブコントロール

- ネストされた OUs は、検出コントロールまたはプロアクティブコントロールを自動的に継承しません。これらは個別に有効にする必要があります。

- 検出コントロールとプロアクティブコントロールは、ランディングゾーンの運用リージョンに登録されているアカウントにのみデプロイされます。

コントロールの状態と継承を有効化

[OU details] (OU 詳細) ページでは、継承されたコントロールを OU ごとに表示できます。

> **Tip**
>
> OU のSCPクォータ内に収まるように、コントロールの継承を活用できます。例えば、ネストされた OU に対してコントロールを直接有効にする代わりに、OU 階層の最上位の OU で有効にすることができます。

ステータスの継承

- ステータスが [Inherited] (継承済み) の場合、コントロールが継承によってのみ有効になり、OU に直接適用されていないことを示します。
- 有効ステータスは、他の の状態に関係なく、この OU にコントロールが適用されることを意味しますOUs。
- Failed ステータスは、他の の状態に関係なく、この OU にコントロールが適用されないことを意味しますOUs。

> **Note**
>
> ステータスが [Inherited] (継承済み) の場合、コントロールがツリー内の上位の OU に適用されたことと、この OU に適用されるものの直接には追加されなかったことを示します。

> **ランディングゾーンが現在のバージョンでない場合**
>
> [Enabled controls] (有効なコントロール) 表内の各行は、1 つの個別の OU にある 1 つの有効なコントロールを表します。

ネストされた OUsとルート

ルートは OU ではなく、登録や再登録ができません。ルートにアカウントを直接作成することもできません。ルートが非準拠になったり、登録済みやドリフトなどのライフサイクル状態になったりすることはありません。

ただし、ルートはすべてのアカウントと の最上位コンテナですOUs。ネストされた のコンテキストではOUs、他のすべての がネストされるノードOUsです。

AWS Control Tower に既存の組織単位を登録する

複数の既存の AWS アカウントを AWS Control Tower に取り込む効率的な方法は、AWSControl Tower によるガバナンスを組織単位 (OU) 全体に拡張することです。

AWS Organizationsとそのアカウントで作成された既存の OU に対する AWS Control Tower ガバナンスを有効にするには、OU を AWS Control Tower ランディングゾーンに登録します。最大 1000 OUs個のアカウントを含む を登録できます。OU に 1000 を超えるアカウントが含まれている場合、AWSControl Tower に登録することはできません。

OU を登録すると、そのメンバーアカウントが AWS Control Tower ランディングゾーンに登録されます。メンバーアカウントは、OU に適用されるコントロールによって管理されます。

> **Note**
>
> AWS Control Tower ランディングゾーンをまだお持ちでない場合は、まず AWS Control Tower によって作成された新しい組織または既存の AWS Organizations 組織でランディングゾーンを設定します。ランディングゾーンのセットアップ方法の詳細については、「AWS Control Tower の使用開始方法」を参照してください。

OU の登録によるアカウントの処理

AWS Control Tower には、 が組織内のアカウントにスタックを自動的にデプロイできるように、AWS Organizations ユーザーに代わって AWS CloudFormation と の間に信頼 AWS CloudFormation されたアクセスを確立するためのアクセス許可が必要です。

- ステータスが [Not enrolled] (未登録) であるすべてのアカウントに `AWSControlTowerExecution` ロールが追加されます。
- OU を登録すると、デフォルトでは OU に対して必須のコントロールが有効になります。

OU 登録後の一部のアカウントの登録

OU を正常に登録できても、一部のアカウントが未登録のままになることがあります。その場合、未登録のアカウントは登録の前提条件の一部を満たしていません。[Register OU] (OU の登録) プロセスの一環としてアカウントの登録が失敗した場合は、アカウントページのアカウントステータスに [Enrollment failed] (登録に失敗しました) と表示されます。OU ページでは、アカウントフィールドに [4 of 5] (4/5) といったアカウント情報が表示されることもあります。

例えば、[4 of 5] と表示されている場合は、[Register OU] (OU の登録) プロセスを実行したところ、OU に全部で 5 個あるアカウントのうち 4 個は正常に登録されたものの、1 個が失敗したということになります。アカウントを登録するには、アカウントが登録の前提条件を満たしていることを確認した後で [Re-Register OU] (OU を再登録) を選択します。

IAM OU を登録するための ユーザー前提条件

アクセスAdmin許可がすでにある場合でも、Register OU オペレーションを実行するときは、 AWS Identity and Access Management （ IAM) ID (ユーザーまたはロール) または IAM Identity Center ユーザー ID を適切な Account Factory ポートフォリオに含める必要があります。そうしないと、登録時にプロビジョニング済み製品の作成が失敗します。AWS Control Tower が OU の登録時にIAMユーザーまたは IAM Identity Center のユーザー ID の認証情報に依存しているため、障害が発生します。

関連するポートフォリオは、AWSControl Tower AWS Account Factory Portfolio と呼ばれる Control Tower によって作成されたポートフォリオです。Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio を選択して、これに移動します。次に、グループ、ロール、ユーザーというタブを選択して、 IAMまたは IAM Identity Center の ID を表示します。アクセス権を付与する方法の詳細については、「AWS Service Catalogのドキュメント」を参照してください。

既存の OU の登録

AWS Control Tower コンソールの Organization ページで、AWSControl Tower に登録OUsされているアカウントOUsや登録されていないアカウントなど、階層内のすべての組織の およびアカウントを表示できます。

一般に、未登録の OUsは で作成され AWS Organizations、他のランディングゾーンによって管理されません。最大 1000 OUs個のアカウントを含む既存の を登録できます。OU に 1000 を超えるアカウントが含まれている場合、AWSControl Tower に登録することはできません。

既存の OU を登録するには

1. https://console.aws.amazon.com/controltower で AWS Control Tower コンソールにサインインします。

2. 左ペインのナビゲーションメニューで、[Organization] (組織) を選択します。
3. [Organization] (組織) ページで、登録する OU の横にあるラジオボタンを選択し、右上の [Actions] (アクション) ドロップダウンメニューから [Register organizational unit] (組織単位の登録) を選択します。または、OU の名前を選択すると、その OU の [OU details] (OU の詳細) ページが表示されます。
4. [OU details] (OU の詳細) ページで、右上の [Actions] (アクション) ドロップダウンメニューから [Register OU] (OU の登録) を選択できます。

登録プロセスでは、管理対象を OU に拡大するのに少なくとも 10 分かかり、アカウントを追加するたびに最大 2 分かかります。

既存の OU を登録した場合の結果

既存の OU を登録すると、`AWSControlTowerExecution`ロールにより AWS Control Tower はガバナンスを個々のアカウントに拡張できます。ガードレールが適用され、アカウントアクティビティに関する情報が監査および口グ記録のアカウントに報告されます。

他には以下のような結果があります。

- `AWSControlTowerExecution` は、AWSControl Tower 監査アカウントによる監査を許可します。
- `AWSControlTowerExecution` では、各アカウントのすべてのログがログ記録アカウントに送信されるように組織の口グ記録を設定できます。
- `AWSControlTowerExecution` は、選択した AWS Control Tower コントロールが、 のすべての個々のアカウントとOUs、AWSControl Tower で作成するすべての新しいアカウントに自動的に適用されるようにします。

登録された OU の場合、AWSControl Tower コントロールによって具体化される監査機能と口グ記録機能に基づいて、コンプライアンスレポートとセキュリティレポートを提供できます。セキュリティチームとコンプライアンスチームは、すべての要件が満たされていること、組織ドリフトが発生していないことを確認できます。ドリフトの詳細については、「AWS Control Tower でドリフトを検出して解決する」を参照してください。

> **Note**
>
> AWS Control Tower に OUsとそのアカウントが表示されると、1 つの異常な状況が発生する可能性があります。登録済み OU にアカウントを作成した後、登録済みのアカウントを

別の未登録の OU に移動すると (特に AWS Organizations を使用してアカウントを移動すると)、OU の詳細ページに「1/0」アカウントという結果が表示されることがあります。また、その未登録の OU に別の未登録のアカウントを作成した可能性もあります。未登録のアカウントがある場合、コンソールではその OU に対して「1/1」などと表示されます。単一の (新規作成の) アカウントが登録されているように見えますが、実際には登録されていません。新しいアカウントを登録する必要があります。

新しい OU の作成

AWS Control Tower で OU またはネストされた OU を作成する方法は次のとおりです。

AWS Control Tower で新しい OU を作成するには

1. [Organization] (組織) ページに移動します。
2. 右上の [Create resources] (リソースの作成) ドロップダウンメニューから [Create organizational unit] (組織単位の作成) を選択します。
3. [OU name] (OU 名) フィールドに名前を指定します。
4. 親 OU ドロップダウンには、登録された の階層が表示されますOUs。作成している新しい OU の親 OU を選択します。
5. [追加] を選択します。

> **Tip**
>
> ネストされた OU をより少ない手順で追加するには、[Organization] (組織) ページのテーブルに表示される親 OU の名前を選択し、親 OU の [OU] ページを表示します。次に、右上にある [Actions] (アクション) ドロップダウンメニューから [Add an OU] (OU の追加) を選択します。新しい OU が、選択した OU の下にネストされた OU として自動的に作成されます。

> **Note**
>
> ランディングゾーンが最新でない場合は、ドロップダウンメニューに階層ではなくフラットリストが表示されます。ランディングゾーンにネストされた が含まれている場合でも OUs、L5 OU の下に新しい OU を作成できないため、ドロップダウンに L5 OU の は表示さ

れません。AWS Control Tower OUsにネストされた の詳細については、「」を参照してくださいAWS Control Tower OUsにネストされている。

登録時または再登録時に発生する障害のよくある原因

通常、OU を登録または再登録すると、その OU 内のすべてのアカウントが AWS Control Tower に登録されます。ただし、OU 全体が正常に登録されても、一部のアカウントが登録に失敗する場合があります。このような場合は、そのアカウントに関連する事前チェックの失敗を解決して、そのアカウントまたは OU を再登録する必要があります。

OU またはそのメンバーアカウントの登録 (または再登録) が失敗した場合、AWSControl Tower は影響を受けるメンバーアカウントのエラーメッセージを返します。エラーメッセージは [OU の詳細] ページで確認できます。このページでは、事前チェックとアカウントのエラーメッセージが表にまとめられています。[OU を登録] オペレーションが失敗した場合、表には OU に属するすべてのアカウントのエラーメッセージがすべて表示されます。必要に応じて、[アカウントの詳細] ページで各アカウントのエラーメッセージを確認することもできます。

オプションで、どの事前チェックに合格しなかったかを示す詳細なレポートを含むファイルをオフライン分析用にダウンロードできます。登録領域の右上に表示される [Download] (ダウンロード) ボタンを選択すると、ダウンロードを完了できます。

このセクションでは、事前チェックが失敗した場合に発生する可能性がある エラーの種類とその エラーの修正方法について説明します。

ランディングゾーンのエラー

- ランディングゾーンの準備ができていない

  現在のランディングゾーンをリセットするか、最新バージョンに更新してください。

OU エラー

- の最大数を超えています SCPs

  OU あたりのサービスコントロールポリシー (SCPs) の制限を超えているか、別のクォータに達した可能性があります。OU SCPsあたり 5 の制限は、AWSControl Tower ランディングゾーンOUs のすべての に適用されます。クォータで許可されている数SCPsを超える場合は、 を削除または組み合わせる必要がありますSCPs。

- 競合 SCPs

  既存の が OU またはアカウントに適用され、AWSControl Tower がアカウントを登録できなくなるSCPs場合があります。AWS Control Tower が機能しなくなる可能性のあるポリシーSCPsに適用されている を確認します。階層のOUs上位からSCPs継承された を必ず確認してください。

- スタックセットのクォータを超えている

  スタックセットのクォータを超えている可能性があります。クォータの許容数を超えるインスタンスがある場合は、スタックインスタンスをいくつか削除する必要があります。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation のクォータ」を参照してください。

- アカウントの上限を超えている

  AWS Control Tower は、登録時に各 OU を 1000 アカウントに制限します。

アカウントエラー

- アカウントで事前チェックが禁止されている

  OU SCP上の既存の は、AWSControl Tower が OU メンバーアカウントで事前チェックを実行できないようにします。この事前チェックの失敗を解決するには、OU SCPから を更新または削除します。

- E メールアドレスのエラー

  アカウントに指定した E メールアドレスが命名基準に準拠していません。許可される文字を正規表現 (regex) で指定するは、`[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+` を使用します。

- 設定レコーダーまたは配信チャネルが有効

  アカウントには、既存の AWS Config 設定レコーダーまたは配信チャネルがある場合があります。これらは、アカウントを登録する前に、AWSControl Tower 管理アカウントがリソースを管理しているすべての AWS リージョン AWS CLI の を通じて削除または変更する必要があります。

- STS 無効

  AWS Security Token Service （ AWS STS) はアカウントで無効にすることができます。 AWS STS エンドポイントは、AWSControl Tower でサポートされているすべてのリージョンのアカウントでアクティブ化する必要があります。

- IAM Identity Center の競合

AWS Control Tower ホームリージョンは、 AWS IAM Identity Center （ IAM Identity Center) リージョンとは異なります。IAM Identity Center が既に設定されている場合、AWSControl Tower ホームリージョンは IAM Identity Center リージョンと同じである必要があります。

- 競合するSNSトピック

  アカウントには、AWSControl Tower が使用する必要がある Amazon Simple Notification Service (Amazon SNS) トピック名があります。 AWSControl Tower は、特定の名前でリソース (SNSトピックなど) を作成します。これらの名前が既に取得されている場合、AWSControl Tower のセットアップは失敗します。この状況は、以前に AWS Control Tower に登録したアカウントを再利用している場合に発生する可能性があります。

- 一時停止中のアカウントが検出される

  このアカウントは停止しています。AWS Control Tower に登録することはできません。アカウントをこの OU から削除してから再試行してください。

- IAM ポートフォリオにない ユーザー

  OU を登録する前に、Service Catalog ポートフォリオに AWS Identity and Access Management （ IAM) ユーザーを追加します。このエラーは、管理アカウントにのみ関係します。

- アカウントが前提条件を満たしていない

  アカウントがアカウント登録の前提条件を満たしていません。例えば、AWSControl Tower への登録に必要なロールとアクセス許可がアカウントにない可能性があります。ロールを追加する手順については、「必要なIAMロールを既存の に手動で追加 AWS アカウント して登録する」を参照してください。

Control AWS Tower に登録すると、すべての AWS アカウントで AWS CloudTrail が自動的に有効になります。登録前のアカウントで CloudTrail が有効になっている場合、登録プロセス CloudTrail を開始する前に を非アクティブ化しない限り、二重請求が発生する可能性があります。

組織の更新

組織単位 (OU) を更新したり、OU 内の複数のアカウントを更新したりするための最も簡単な方法は、OU を再登録することです。

AWS Control Tower OUsとアカウントを更新するタイミング

ランディングゾーン更新を実行するときは、登録済みのアカウントを更新して、そのアカウントに新しいコントロールを適用する必要があります。

- [Re-Register] (再登録) オプションを使用して、OU の下にあるすべてのアカウントを更新できます。
- ランディングゾーンに複数の OU が登録されている場合は、すべての を再登録OUsしてすべてのアカウントを更新します。
- 1 つのアカウントを更新するには、AWSControl Tower コンソールから を更新するか、 でプロビジョニング済み製品の更新オプションを選択します AWS Service Catalog。「コンソールでアカウントを更新する」を参照してください。

同じ OU 内の複数のアカウントの更新

すべてのアカウントと を更新する必要がある場合は、AWSControl Tower 組織内の OU ごとにこれらの手順を繰り返しますOUs。

1 つの操作で 1 つの OU 内の複数のアカウントを更新するには

1. https://console.aws.amazon.com/controltower で AWS Control Tower コンソールにサインインします。
2. 左ペインのナビゲーションメニューで、[Organization] (組織) を選択します。
3. [Organization] (組織) ページで、OU を選択して [OU details] (OU の詳細ページ) を表示します。
4. 右上の [Actions] (アクション) で、[Re-Register OU] (OU を再登録) を選択します。

または、[更新プログラムが利用できます] のステータスが表示されているアカウントを必要な数だけ選択して、[アカウントの更新] を選択することもできます。

再登録中の処理

OU を再登録すると、次のような処理が行われます。

- State フィールドには、アカウントが現在 AWS Control Tower に登録されている (登録済み) 、アカウントが登録されていない (未登録) 、または以前に登録に失敗した (登録失敗) かどうかが表示されます。

- OU を再登録すると、ステータスが [Not enrolled] (未登録) または [Enrollment failed] (登録に失敗しました) であるすべてのアカウントに `AWSControlTowerExecution` ロールが追加されます。
- AWS Control Tower は、これらの新しい登録済みアカウントのシングルサインオン (IAM Identity Center) ログインを作成します。
- 登録されたアカウントは AWS Control Tower に再登録されます。
- OU に適用される予防コントロールのドリフトは修正されます。これは、 SCPs がデフォルトの定義に戻されるためです。
- 最新のランディングゾーンの変更を反映するように、すべてのアカウントが更新されます。

詳細については、「既存の を登録する AWS アカウント」を参照してください。

> **Tip**
>
> OU を再登録するとき、またはランディングゾーンのバージョンと複数のメンバーアカウントを更新するときに、StackSet-AWSControlTowerExecutionRole というエラーメッセージが表示されます。AWSControlTowerExecution IAM ロール StackSet は登録済みのすべてのメンバーアカウントにすでに存在するため、管理アカウントのこの操作は失敗する可能性があります。このエラーメッセージは想定される動作であり、無視してもかまいません。

1 つのアカウントを更新するには

個々の Control Tower アカウントは、AWSControl Tower コンソールまたは Service Catalog AWS コンソールで更新できます。

AWS Control Tower コンソールで単一のアカウントを更新するには、「」を参照してくださいコンソールでアカウントを更新する。

で 1 つのアカウントを更新するには AWS Service Catalog

1. AWS Service Catalogに移動します。
2. 左ペインのナビゲーションメニューで、[Provisioned products] (プロビジョニングされた製品) を選択します。
3. [Provisioned products] (プロビジョニングされた製品) ページで、更新するプロビジョニングされた製品の横にあるラジオボタンを選択します。
4. 右上の [Actions] (アクション) ドロップダウンから [Update] (更新) を選択して更新します。

での更新の詳細については AWS Service Catalog、「Service Catalog 管理者ガイド」のプロビジョニング済み製品の更新「」および「製品の更新」を参照してください。

統合サービス

AWS Control Tower は、適切に設計された環境のセットアップを支援するために、他の AWS サービス上に構築されたサービスです。この章では、基盤となるサービスの設定情報や AWS Control Tower でのそれらの動作など、これらのサービスの概要を説明します。

アーキテクチャが適切に設計された環境の評価方法の詳細については、「AWS Well-Architected Tool」を確認してください。「管理とガバナンスクラウド環境ガイド」も参照してください。

トピック

- AWS 使用可能なバックアップオプション
- を使用して環境をデプロイする AWS CloudFormation
- でイベントをモニタリングする CloudTrail
- で リソースとサービスをモニタリングする CloudWatch
- を使用したリソース設定の管理 AWS Config
- IAM によるエンティティのアクセス許可の管理
- AWS Key Management Service
- Lambda によるサーバーレスコンピューティング関数の実行
- によるアカウントの管理 AWS Organizations
- Simple Storage Service (Amazon S3) によるオブジェクトの保存
- Security Hub を使用した環境のモニタリング
- によるアカウントのプロビジョニング AWS Service Catalog
- Amazon Simple Notification Service によるアラートの追跡
- を使用して分散アプリケーションを構築する AWS Step Functions

AWS 使用可能なバックアップオプション

AWS Backup では、AWSControl Tower ランディングゾーンのバックアッププランを作成できます。ランディングゾーンにデータのバックアップと復旧ワークフローを直接組み込むことができます。バックアッププランには、保持日数、バックアップ頻度、バックアップが発生する時間枠などの事前定義されたルールが含まれています。詳細については、AWS 「Backup and AWS Control Tower」を参照してください。

を使用して環境をデプロイする AWS CloudFormation

AWS CloudFormation を使用すると、 AWS インフラストラクチャのデプロイを予測どおりに繰り返し作成およびプロビジョニングできます。これにより、基盤となる AWS インフラストラクチャの作成と設定を気にすることなく、 AWS 製品を活用して、信頼性とスケーラビリティに優れた費用対効果の高い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、リソースのコレクションを 1 つのユニット (スタック) としてまとめて作成および削除できます。詳細については、「AWS CloudFormation ユーザーガイド」を参照してください。

AWS Control Tower は AWS CloudFormation 、スタックセットを使用してアカウントにコントロールを適用します。 AWS CloudFormation と AWS Control Tower の連携の詳細については、「」を参照してください で AWS Control Tower リソースを作成する AWS CloudFormation。

でイベントをモニタリングする CloudTrail

AWS Control Tower は、一元化された口グ記録と監査を有効にする AWS CloudTrail ように を設定します。を使用すると CloudTrail、管理アカウントはメンバーアカウントの管理アクションとライフサイクルイベントを確認できます。

CloudTrail は、 アカウントの AWS API呼び出し履歴を保持することで、クラウド内の AWS 環境をモニタリングするのに役立ちます。例えば、 がサポートするサービスを呼び出し AWS APIsたユーザーとアカウント CloudTrail、呼び出し元の IP アドレス、呼び出しが発生した時間を特定できます。を使用して CloudTrail をアプリケーションに統合しAPI、組織の証跡作成を自動化し、証跡のステータスをチェックして、管理者が CloudTrail ログ記録をオン/オフにする方法を制御できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

で リソースとサービスをモニタリングする CloudWatch

Amazon CloudWatch は、数分以内に使用を開始できる、信頼性が高く、スケーラブルで柔軟な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。

Amazon と AWS Control Tower CloudWatch の連携の詳細については、「モニタリング」を参照してください。

を使用したリソース設定の管理 AWS Config

AWS Config は、 AWS アカウントに関連付けられたリソースの詳細ビューを提供します。これには、リソースの設定方法、相互の関係、時間の経過とともに設定と関係がどのように変化したかが含まれます。詳細については、「AWS Config デベロッパーガイド」を参照してください。

AWS Config AWS Control Tower によってプロビジョニングされた リソースには、 `aws-control-tower` と の値が自動的にタグ付けされます`managed-by-control-tower`。

AWS Control Tower で がリソースを AWS Config モニタリングおよび記録する方法、およびリソースの請求方法の詳細については、「」を参照してくださいでリソースの変更をモニタリングする AWS Config。

AWS Control Tower は AWS Config ルール を使用して検出コントロールを実装します。詳細については、AWS「Control Tower のコントロールについて」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、他の AWS サービスへのアクセスを制御するための AWS サービスです。を使用するとIAM、ユーザー、アクセスキーなどのセキュリティ認証情報、およびアクセス許可を一元管理して、ユーザーとアプリケーションにアクセス権を付与する AWS リソースを指定できます。

ランディングゾーンを設定するときに、ID プロバイダーIAMとして を選択すると、 用に AWS IAM Identity Center 複数のグループを自動的に作成できます。これらのグループには、IAM から事前定義された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。エンドユーザーは、 IAMを使用して、メンバーアカウント内のIAMユーザーやその他のエンティティのアクセス許可の範囲を定義することもできます。

AWS Identity and Access Management （ IAM) は、 AWS アカウントとビジネスアプリケーションへのアクセスを管理する方法を簡素化します。AWS Control Tower のすべてのアカウントで、IAMIdentity Center へのアクセスとユーザーアクセス許可を AWS 制御できます。

詳細については、「AWS IAM Identity Center ユーザーガイド」を参照してください。

をサポート AWS リージョン していない を拠点としている場合はIAM、別の ID プロバイダーを導入して、独自のユーザーとグループを手動でセットアップして維持できます。

AWS Key Management Service

AWS Key Management Service （ AWS KMS) では、データを保護するキーを作成および管理できます。 AWSControl Tower では、オプションで暗号化キーを使用してデータを AWS KMS 暗号化できます。詳細については AWS KMS、「 AWS KMSデベロッパーガイド」を参照してください。

AWS Control Tower で AWS KMS キーを設定する方法については、「オプションで AWS KMS キーを設定する」を参照してください。

Lambda によるサーバーレスコンピューティング関数の実行

を使用すると AWS Lambda、サーバーのプロビジョニングや管理を行わずにコードを実行できます。余分な管理オーバーヘッドが発生することなく、多くのタイプのアプリケーションやバックエンドサービスのコードを実行できます。コードをアップロードすると、Lambda が高い可用性でコードを実行および拡張できます。他の AWS のサービスから自動的にトリガーするようにコードをセットアップすることも、ウェブやモバイルアプリケーションから直接コードを呼び出すこともできます。

例えば、AWSControl Tower 監査アカウントの特定のロールをプログラムで引き受けることができるため、Lambda を使用して他のアカウントを確認できます。また、AWSControl Tower ライフサイクルイベントを使用して Lambda 関数をトリガーすることもできます。

によるアカウントの管理 AWS Organizations

AWS Organizations は、作成して一元管理する組織に複数の AWS アカウントを統合することができるアカウント管理サービスです。Organizations では、メンバーアカウントを作成して、既存のアカウントを組織に招待できます。それらのアカウントをグループ分けしたり、ポリシーに基づいて管理したりできます。詳細については、「AWS Organizations ユーザーガイド」を参照してください。

AWS Control Tower では、Organizations は請求の一元管理、アクセス、コンプライアンス、セキュリティの制御、メンバー AWS アカウント間でのリソースの共有に役立ちます。アカウントは、組織単位 () と呼ばれる論理グループにグループ化されますOUs。Organizations の詳細については、「AWS Organizations ユーザーガイド」を参照してください。

AWS Control Tower は次の を使用しますOUs。

- ルート – ランディングゾーンOUs内のすべてのアカウントと他のすべてのアカウントの親コンテナ。

- Security - この OU には、ログアーカイブアカウント、監査アカウント、および所有されているリソースが含まれます。
- Sandbox - この OU は、ランディングゾーンをセットアップすると作成されます。ランディングゾーンOUsの と他の子には、メンバーアカウントが含まれます。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**
>
> ランディングゾーンOUsには、組織単位ページの AWS Control Tower コンソールから追加できます。

考慮事項

OUs AWS Control Tower を介して作成された には、コントロールを適用できます。Control Tower の外部でOUs作成された AWS には、デフォルトではコントロールを適用できません。ただし、このような を登録することはできますOUs。OU を登録したら、その OU とそのアカウントにコントロールを適用できます。OU の登録については、「既存の組織単位を AWS Control Tower に登録する」を参照してください。

Simple Storage Service (Amazon S3) によるオブジェクトの保存

Amazon Simple Storage Service (Amazon S3) は、インターネット用のストレージです。Simple Storage Service (Amazon S3) を使用すると、いつでもウェブ上の任意の場所から任意の量のデータを保存および取得できます。 AWS Management Consoleのシンプルかつ直感的なウェブインターフェイスを使用して、これらのタスクを実行できます。詳細については、「Amazon Simple Storage Service ユーザーガイド」を参照してください。

ランディングゾーンのセットアップ時に、ランディングゾーン内にあるすべてのアカウントのすべてのログを含めるための Simple Storage Service (Amazon S3) バケットがログアーカイブアカウントに作成されます。

Security Hub を使用した環境のモニタリング

AWS Control Tower は AWS 、サービスマネージドスタンダード: AWS Control Tower と呼ばれる Security Hub 標準によって Security Hub と統合されています。詳細については、「Security Hub standard」を参照してください。

によるアカウントのプロビジョニング AWS Service Catalog

AWS Service Catalog を使用すると、IT 管理者は承認された製品のポートフォリオを作成、管理、配布し、エンドユーザーはパーソナライズされたポータルで必要な製品にアクセスできます。一般的な製品には、 AWS リソースを使用してデプロイされるサーバー、データベース、ウェブサイト、またはアプリケーションが含まれます。

特定の製品にアクセスできるユーザーを制御できます。これにより、組織のビジネス標準へのコンプライアンスを実現したり、製品のライフサイクルを管理したり、ユーザーが確実に製品を見つけて起動したりできるようにすることが可能です。詳細については、「Service Catalog 管理者ガイド」を参照してください。

AWS Control Tower では、中央のクラウド管理者とエンドユーザーは、「カスタムブループリント」と呼ばれる AWS Service Catalog 製品を使用して、ランディングゾーンにカスタムアカウントをプロビジョニングできます。詳細については、「Step2. AWS Service Catalog 製品を作成します。

AWS Control Tower は Service Catalog を利用してAPIs、アカウントのプロビジョニングと更新をさらに自動化することもできます。詳細については、「 AWS Service Catalog デベロッパーガイド」を参照してください。

AWS Service Catalog External 製品タイプへの移行

AWS Service Catalog は、Terraform Open Source 製品とプロビジョニング済み製品のサポートを External という新しい製品タイプに変更しました。この移行の詳細については、「AWS Service Catalog 管理者ガイド」の「既存の Terraform オープンソース製品およびプロビジョニングされた製品から External 製品タイプへの更新」を参照してください。

この変更は、AWSControl Tower Account Factory のカスタマイズで作成または登録した既存のアカウントに影響します。これらのアカウントを External 製品タイプに移行するには、 AWS Service Catalog と AWS Control Tower の両方を変更する必要があります。

新しい External 製品タイプに移行するには

1. の既存の Terraform リファレンスエンジンをアップグレード AWS Service Catalog して、External 製品タイプと Terraform Open Source 製品タイプの両方のサポートを含めます。Terraform リファレンスエンジンを更新する手順については、 AWS Service Catalog GitHub リポジトリを参照してください。

2. で AWS Service Catalog、新しい External 製品タイプを使用して、既存の Terraform Open Source 製品 (ブループリント) を複製します。既存の Terraform Open Source ブループリントを削除しないでください。
3. AWS Control Tower で、Terraform Open Source ブループリントを使用して各アカウントを更新し、新しい External ブループリントを使用します。

   a. ブループリントを更新するには、まず Terraform オープンソースブループリントを完全に削除する必要があります。詳細については、「アカウントからブループリントを削除する」を参照してください。

   b. 新しい External ブループリントを同じアカウントに追加します。詳細については、「設計図を AWS Control Tower アカウントに追加する」を参照してください。
4. Terraform Open Source ブループリントを使用するすべてのアカウントが External ブループリントに更新されたら、Terraform Open Source を製品タイプとして使用するすべての製品に戻って AWS Service Catalog 終了します。
5. 今後、AWSControl Tower Account Factory のカスタマイズを使用して作成または登録されたすべてのアカウントは、 AWS CloudFormationまたは External 製品タイプを使用して設計図を参照する必要があります。

   External 製品タイプを使用して作成された設計図の場合、AWSControl Tower は Terraform テンプレートと Terraform リファレンスエンジンを使用するアカウントのカスタマイズのみをサポートします。詳細については、「カスタマイズのための設定」を参照してください。

> **Note**
>
> AWS Control Tower は、新しいアカウントの作成時に製品タイプとして Terraform Open Source をサポートしていません。これらの変更の詳細については、AWS Service Catalog 管理者ガイドの「既存の Terraform Open Source 製品とプロビジョニング済み製品の External 製品タイプへの更新」を参照してください。 AWS Service Catalog は、必要に応じてこの製品タイプの移行を通じてお客様をサポートします。アカウント担当者を通じて支援をリクエストしてください。

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、デバイスがクラウドから通知を即座に送受信できるようにするウェブサービスです。詳細については、「Amazon Simple Notification Service デベロッパーガイド」を参照してください。

AWS Control Tower は Amazon SNSを使用して、管理アカウントと監査アカウントの E メールアドレスにプログラムによるアラートを送信します。これらのアラートは、ランディングゾーン内でのドリフトの防止に役立ちます。詳細については、「AWS Control Tower でドリフトを検出して解決する」を参照してください。

また、Amazon Simple Notification Service を使用してコンプライアンス通知を送信します AWS Config。

> **Tip**
>
> AWS Control Tower コントロールコンプライアンス通知 (監査アカウント内) を受信する最善の方法の 1 つは、 をサブスクライブすることですAggregateConfigurationNotifications。コンプライアンスの検査に役立つサービスです。これにより、コンプライアンスから外れるルールに関する AWS Config 実際のデータが得られます。 は、OU 内のアカウントのリスト AWS Config を自動的に維持します。E メールまたは がSNS許可する任意のタイプのサブスクリプション を使用して、手動でサブスクライブする必要があります。ステートメント `arn:aws:sns:homeregion:account:aws-controltower-AggregateSecurityNotifications` により、監査アカウントにつながります。

を使用して分散アプリケーションを構築する AWS Step Functions

AWS Step Functions を使用すると、分散アプリケーションのコンポーネントをビジュアルワークフローの一連のステップとして簡単に調整できます。ステートマシンをすばやく構築および実行し、アプリケーションのステップを信頼性が高くスケーラブルな方法で実行できます。詳細については、「AWS Step Functions デベロッパーガイド」を参照してください。

AWS Control Tower での Identity and Access Management

Account Factory でのアカウントのプロビジョニングや AWS Control Tower コンソールでの新しい組織単位 (OUs) の作成など、ランディングゾーンでオペレーションを実行するには、 AWS Identity and Access Management （ IAM) または のいずれかで、承認された AWS ユーザーであることを認証 AWS IAM Identity Center する必要があります。例えば、AWSControl Tower コンソールを使用している場合は、管理者から提供された認証情報を指定して ID を AWS 認証します。

ID を認証すると、 は、特定のオペレーションとリソースのセットに対する一連の定義されたアクセス許可 AWS を使用して、 へのアクセスIAMを制御します。アカウント管理者である場合、IAM を使用して、アカウントに関連付けられたリソースへの他の IAM ユーザーのアクセスを制御できます。

トピック

- 認証
- アクセスコントロール
- Identity Center と AWS Control Tower の使用 AWS IAM
- AWS Control Tower リソースへのアクセス許可の管理の概要
- クロスサービス偽装の防止
- AWS Control Tower でアイデンティティベースのポリシー (IAM ポリシー) を使用する

認証

には、次のいずれかのタイプの ID AWS としてアクセスできます。

- AWS アカウントのルートユーザー – AWS アカウントを初めて作成するときは、アカウント内のすべての AWS サービスとリソースへの完全なアクセス権を持つ ID から始めます。このアイデンティティは、 AWS アカウントのルートユーザーと呼ばれます。アカウントの作成に使用した E メールアドレスとパスワードでサインインすると、このアイデンティティにアクセスできます。日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことを強くお勧めします。代わりに、最初の IAM Identity Center ユーザー (推奨) または ユーザー (ほとんどのユースケースではベストプラクティスではない) を作成する場合にのみ、ルートIAMユーザーを使用するというベストプラクティスに従ってください。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。詳細については、「ルートユーザーとしてサインインする場合」を参照してください。

- IAM ユーザー – IAMユーザーは、特定のカスタマイズされたアクセス許可を持つ AWS アカウント内のアイデンティティです。ユーザーIAM認証情報を使用して、 マネジメントコンソール、 AWS ディスカッションフォーラム、 AWS サポートセンターなどの AWS 安全な AWS ウェブページにサインインできます。 AWS のベストプラクティスでは、長期的な認証情報を持つ ユーザーを作成するとセキュリティ上のリスクが高くなるため、 IAM ユーザーではなく IAM Identity Center IAM ユーザーを作成することをお勧めします。

  特定の目的で IAM ユーザーを作成する必要がある場合は、サインイン認証情報に加えて、IAM ユーザーごとにアクセスキーを生成できます。これらのキーは、プログラムで AWS サービスを呼び出すときに、複数の のいずれかまたは コマンドラインインターフェイス () AWS SDKsを使用して使用できますCLI。SDK および CLIツールは、 アクセスキーを使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。AWSControl Tower は、署名バージョン 4 をサポートしています。これは、インバウンドAPIリクエストを認証するためのプロトコルです。リクエストの認証の詳細については、「 AWS 全般のリファレンス」の「署名バージョン 4 の署名プロセス」を参照してください。

- IAM ロール – IAMロールは、特定のアクセス許可を持つアカウントで作成できる IAM ID です。IAM ロールは、 AWS アイデンティティであるという点で IAM ユーザーと似ており、アイデンティティが でできることとできないことを決定するアクセス許可ポリシーがあります AWS。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッションの一時的なセキュリティ認証情報が提供されます。一時的な認証情報を持つ IAM ロールは、以下の状況で役立ちます。

  - フェデレーティッドユーザーアクセス – IAM ユーザーを作成する代わりに、 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 ID プロバイダーの既存の ID を使用できます。これらはフェデレーティッドユーザーと呼ばれます。 は、ID プロバイダーを介してアクセスがリクエストされると、フェデレーティッドユーザーにロールを AWS 割り当てます。フェデレー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 サービスアクセス – サービスロールは、サービスがユーザーに代わってアカウントでアクションを実行するために引き受ける IAMロールです。一部の AWS サービス環境を設定するときは、サービスが引き受けるロールを定義する必要があります。このサービスロールには、サービスが必要な AWS リソースにアクセスするために必要なすべてのアクセス許可が含まれている必要があります。サービスロールはサービスによって異なりますが、多くのサービスロールでは、そのサービスの文書化された要件を満たしている限り、許可を選択することができます。サービスロールは、お客様のアカウント内のみでアクセスを提供します。他のアカウント

のサービスへのアクセス権を付与するためにサービスロールを使用することはできません。IAM内部からロールを作成、修正、削除できます。例えば、Amazon Redshift がユーザーに代わってSimple Storage Service (Amazon S3) バケットにアクセスし、そのバケットのデータを Amazon Redshift クラスターにロードすることを許可するロールを作成できます。詳細については、「IAMユーザーガイド」の「 AWS サービスにアクセス許可を委任するロールの作成」を参照してください。

- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、Amazon EC2インスタンスで実行され、 または AWS API リクエストを行う AWS CLIアプリケーションの一時的な認証情報を管理できます。これは、Amazon EC2インスタンス内にアクセスキーを保存するよりも望ましいです。 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できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、Amazon EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 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。 IAM

- IAM Identity Center ユーザー IAM Identity Center ユーザーポータルへの認証は、IAMIdentity Center に接続したディレクトリによって制御されます。ただし、ユーザーポータル内からエンドユーザーが利用できる AWS アカウントの承認は、次の 2 つの要因によって決まります。
  - IAM Identity Center コンソールで AWS それらの AWS アカウントへのアクセス権が割り当てられているユーザー。詳細については、「AWS IAM Identity Center 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。
  - AWS IAM Identity Center コンソールでエンドユーザーに付与されたアクセス許可のレベルは、それらの AWS アカウントへの適切なアクセスを許可するものです。詳細については、「AWS IAM Identity Center ユーザーガイド」の「許可セット」を参照してください。

アクセスコントロール

ランディングゾーンで AWS Control Tower リソースまたは他の AWS リソースを作成、更新、削除、または一覧表示するには、 オペレーションを実行するためのアクセス許可と、対応するリソースにアクセスするためのアクセス許可が必要です。また、プログラムでオペレーションを実行するには、有効なアクセスキーが必要です。

以下のセクションでは、AWSControl Tower のアクセス許可を管理する方法について説明します。

トピック

- AWS Control Tower リソースへのアクセス許可の管理の概要

- AWS Control Tower でアイデンティティベースのポリシー (IAM ポリシー) を使用する

Identity Center と AWS Control Tower の使用 AWS IAM

AWS Control Tower では、IAMIdentity Center により、中央のクラウド管理者とエンドユーザーが複数の AWS アカウントとビジネスアプリケーションへのアクセスを管理できます。デフォルトでは、アイデンティティとアクセスコントロールを自己管理するオプションを選択しない限り、AWSControl Tower はこのサービスを使用して Account Factory で作成されたアカウントへのアクセスを設定および管理します。

ID プロバイダーの選択については、「IAM Identity Center のガイダンス」を参照してください。

AWS Control Tower で IAM Identity Center のユーザーとアクセス許可を設定する方法に関する簡単なチュートリアルについては、この動画 (6:23) をご覧ください。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

AWS Control Tower での Identity Center のセットアップ AWS IAMに関するビデオチュートリアル。

IAM Identity Center を使用した AWS Control Tower の設定について

AWS Control Tower を最初にセットアップすると、ルートユーザーと正しいアクセス許可を持つIAMユーザーのみが IAM Identity Center ユーザーを追加できます。ただし、エンドユーザーがAWSAccountFactoryグループに追加されると、Account Factory ウィザードから新しい IAM Identity Center ユーザーを作成できます。詳細については、「Account Factory でのアカウントのプロビジョニングと管理」を参照してください。

推奨されるデフォルトを選択すると、AWSControl Tower はユーザー ID とシングルサインオンの管理に役立つ事前設定されたディレクトリでランディングゾーンを設定し、ユーザーがアカウント間でフェデレーションアクセスできるようにします。ランディングゾーンのセットアップ時に、このデフォルトディレクトリはユーザーグループと許可セットを含むように作成されます。

> **Note**
>
> IAM Identity Center の委任管理者機能を使用して、組織 AWS IAM Identity Center 内の の管理を管理アカウント以外のアカウントに委任できます。この機能を使用する場合、メンバーシップを管理するアクセス権を持つ管理者は、管理アカウントに割り当てられたグループも管理できることに注意してください。詳細については、このブログ記事「Getting started with AWS SSO delegated administration」を参照してください。

ユーザーグループ、ロール、アクセス許可セット

ユーザーグループは、共有アカウント内で定義された特殊なロールを管理します。ロールは、一緒に属する許可のセットを確立します。グループのすべてのメンバーは、グループに関連付けられた許可セットやロールを継承します。メンバーアカウントのエンドユーザー用に新しいグループを作成して、グループが実行する特定のタスクに必要なロールのみをカスタムに割り当てることができます。

使用可能なアクセス許可セットは、読み取り専用アクセス、AWSControl Tower 管理アクセス、Service Catalog アクセスなど、さまざまなユーザーアクセス許可要件に対応しています。これらのアクセス許可セットにより、エンドユーザーはエンタープライズのガイドラインに従って、ランディングゾーンに自分の AWS アカウントをすばやくプロビジョニングできます。

ユーザー、グループ、および許可の割り当てを計画するためのヒントについては、「グループ、ロール、ポリシーを設定する上での推奨事項」を参照してください。

AWS Control Tower のコンテキストでこのサービスを使用する方法の詳細については、 AWS IAM Identity Center ユーザーガイドの以下のトピックを参照してください。

- ユーザーを追加するには、「ユーザーを追加する」を参照してください。
- グループにユーザーを追加するには、「グループにユーザーを追加する」を参照してください。
- ユーザーのプロパティを編集するには、「ユーザーのプロパティの編集」を参照してください。
- グループを追加するには、「グループの追加」を参照してください。

> **Warning**
>
> AWS Control Tower は、ホームリージョンに IAM Identity Center ディレクトリを設定します。別のリージョンでランディングゾーンをセットアップし、IAMIdentity Center コンソールに移動する場合は、リージョンをホームリージョンに変更する必要があります。ホームリージョンの IAM Identity Center 設定を削除しないでください。

IAM Identity Center アカウントと AWS Control Tower について知っておくべきこと

AWS Control Tower で IAM Identity Center ユーザーアカウントを使用する際に知っておくべきいくつかの良い点を以下に示します。

- Identity Center AWS IAMユーザーアカウントが無効になっている場合、Account Factory で新しいアカウントをプロビジョニングしようとすると、エラーメッセージが表示されます。IAM Identity Center コンソールで IAM Identity Center ユーザーを再度有効にできます。
- Account Factory によって発行されたアカウントに関連付けられたプロビジョニング済み製品を更新するときに新しい IAM Identity Center ユーザーの E メールアドレスを指定すると、AWSControl Tower は新しい IAM Identity Center ユーザーアカウントを作成します。以前に作成したユーザーアカウントは削除されません。以前の IAM Identity Center ユーザーの E メールアドレスを AWS IAM Identity Center から削除する場合は、「ユーザーの無効化」を参照してください。
- AWS IAM Identity Center は Azure Active Directory と統合されており、既存の Azure Active Directory を AWS Control Tower に接続できます。
- AWS Control Tower の動作が IAM Identity Center およびさまざまな ID ソースと AWS どのように相互作用するかの詳細については、Identity Center ドキュメントの「ID ソースの変更に関する考慮事項」を参照してください。 AWS IAM

IAM AWS Control Tower の Identity Center グループ

AWS Control Tower には、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の事前設定済みグループが用意されています。ユーザーを追加し、IAMIdentity Center でこれらのグループに直接割り当てることができます。これにより、アカウント内では許可セットがグループのユーザーに一致します。グループの設定に関する最新のガイダンスとベストプラクティスについては、IAM「 Identity Center ユーザーガイド」の「ベストプラクティス」を参照してください。

ランディングゾーンをセットアップすると、以下のグループが作成されます。

AWSAccountFactory

アカウント	許可セット	説明
管理アカウント	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	許可セット	説明
管理アカウント	AWSServiceCatalogAdminFullAccess	このグループは、Account Factory で管理者権限を変更するためにこのアカウントでのみ使用されます。このグループのユーザーは、AWSAccountFactoryグループ内にない限り、新しいアカウントをプロビジョニングできません。

AWSControlTowerAdmins

アカウント	許可セット	説明
管理アカウント	AWSAdministratorAccess	このアカウントのこのグループのユーザーは、AWSControl Tower コンソールにアクセスできる唯一のユーザーです。
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 Organizations へのフルアクセスが与えられます。

AWSSecurityAuditPowerUsers

アカウント	許可セット	説明
管理アカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行でき、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。
ログアーカイブアカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行でき、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。
監査アカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行でき、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。
メンバーアカウント	AWSPowerUserAccess	ユーザーはアプリケーション開発タスクを実行でき、AWS アプリケーション開発をサポートするリソースとサービスを作成および設定できます。

AWSSecurityAuditors

アカウント	許可セット	説明
管理アカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスと

アカウント	許可セット	説明
		リソースへの読み取り専用アクセス権を持ちます。
ログアーカイブアカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースへの読み取り専用アクセス権を持ちます。
監査アカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースへの読み取り専用アクセス権を持ちます。
メンバーアカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースへの読み取り専用アクセス権を持ちます。

AWSLogArchiveAdmins

アカウント	許可セット	説明
ログアーカイブアカウント	AWSAdministratorAccess	ユーザーは、このアカウントで管理者アクセスが与えられます。

AWSLogArchiveViewers

アカウント	許可セット	説明
ログアーカイブアカウント	AWSReadOnlyAccess	ユーザーは、このアカウントのすべての AWS サービスとリソースへの読み取り専用アクセス権を持ちます。

AWSAuditAccountAdmins

アカウント	許可セット	説明
監査アカウント	AWSAdministratorAccess	ユーザーは、このアカウントで管理者アクセスが与えられます。

AWS Control Tower リソースへのアクセス許可の管理の概要

すべての AWS リソースは によって所有され AWS アカウント、リソースを作成またはアクセスするためのアクセス許可はアクセス許可ポリシーによって管理されます。アカウント管理者は、IAM ID (ユーザー、グループ、ロール) にアクセス許可ポリシーをアタッチできます。一部のサービス (など AWS Lambda) では、 リソースへのアクセス許可ポリシーのアタッチもサポートされています。

> **Note**
>
> アカウント管理者 (または管理者) は、管理者権限を持つユーザーです。詳細については、「IAMユーザーガイド」のIAM「ベストプラクティス」を参照してください。

ユーザーまたはロールに権限を付与する責任を負う場合は、権限を必要とするユーザーとロール、各ユーザーとロールが権限を必要とするリソース、およびそれらのリソースを操作するために許可する必要のある特定のアクションを把握して追跡する必要があります。

トピック

- AWS Control Tower のリソースとオペレーション
- リソース所有権について
- リソースへのアクセスの管理
- ポリシー要素を指定: アクション、効果、プリンシパル
- ポリシーの条件の指定

AWS Control Tower のリソースとオペレーション

AWS Control Tower では、プライマリリソースはランディングゾーンです。 AWSControl Tower は、ガードレールとも呼ばれる追加のリソースタイプであるコントロールもサポートしています。

ただし、AWSControl Tower では、既存のランディングゾーンのコンテキストでのみコントロールを管理できます。コントロールはサブリソースと呼ぶことができます。

のリソースとサブリソース AWS には、次の例に示すように、一意の Amazon リソースネーム (ARNs) が関連付けられています。

AWS Control Tower には、AWSControl Tower リソースを操作するための一連のAPIオペレーションが用意されています。使用可能なオペレーションのリストについては、AWS「 Control Tower APIリファレンス」のAWS「Control Tower」を参照してください。

AWS Control Tower の AWS CloudFormation リソースの詳細については、「 ユーザーガイド AWS CloudFormation」を参照してください。

リソース所有権について

AWS アカウントは、リソースを作成したユーザーに関係なく、アカウントで作成されたリソースを所有します。具体的には、リソース所有者は、リソース作成リクエストを認証するプリンシパルエンティティ (AWS アカウント ルートユーザー、IAMIdentity Center ユーザー、 IAM ユーザー、または IAMロール) の AWS アカウントです。次の例は、この仕組みを示しています。

- AWS アカウントのアカウントルートユーザー認証情報を使用してランディングゾーン AWS を設定する場合、 AWS アカウントはリソースの所有者です。
- AWS アカウントに IAM ユーザーを作成し、そのユーザーにランディングゾーンを設定するアクセス許可を付与する場合、そのユーザーは、アカウントが前提条件を満たしている限り、ランディングゾーンを設定できます。ただし、ユーザーが属する AWS アカウントはランディングゾーンリソースを所有しています。
- ランディングゾーンをセットアップするアクセス許可を持つ AWS アカウントに IAMロールを作成すると、ロールを引き受けることのできるいずれのユーザーもランディングゾーンを設定できます。ロールが属する AWS アカウントは、ランディングゾーンリソースを所有します。

リソースへのアクセスの管理

アクセス権限ポリシー では、誰が何にアクセスできるかを記述します。以下のセクションで、アクセス許可ポリシーを作成するために使用可能なオプションについて説明します。

> **Note**
>
> このセクションでは、AWSControl Tower のコンテキストIAMでの の使用について説明します。これは、IAM サービスに関する詳細情報を取得できません。詳細な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 ポリシーの構文と説明については、「 IAMユーザーガイド」のAWS IAM「 ポリシーリファレンス」を参照してください。

IAM アイデンティティにアタッチされたポリシーは、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。リソースに添付されたポリシーは、リソースベースのポリシーと呼ばれます。

> **Note**
>
> AWS Control Tower は、アイデンティティベースのポリシー (IAM ポリシー) のみをサポートしています。

トピック

- アイデンティティベースのポリシーについて (IAM ポリシー)
- ロールを作成して、アクセス許可を割り当てる
- リソースベースのポリシー

アイデンティティベースのポリシーについて (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。例えば、次のオペレーションを実行できます。

- アカウントのユーザーまたはグループにアクセス許可ポリシーをアタッチする – ランディングゾーンの設定などの AWS Control Tower リソースを作成するアクセス許可をユーザーに付与するには、ユーザーが属するユーザーまたはグループにアクセス許可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) – 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。例えば、ある AWS アカウント (アカウント A) の管理者は、別のアカウント (AWS アカウント B) にクロスアカウントアクセス許可を付与するロールを作成したり、別の AWS サービスにアクセス許可を付与するロールを作成したりできます。
  1. アカウント A の管理者は、 IAMロールを作成し、アカウント A のリソースを管理するアクセス許可を付与するアクセス許可ポリシーをロールにアタッチします。
  2. アカウント A の管理者は、ロールに信頼ポリシーをアタッチします。ポリシーは、ロールを引き受けることのできるプリンシパルとしてアカウント B を識別します。

3. プリンシパルとして、アカウント B の管理者は、アカウント B のすべてのユーザーにそのロールを引き受ける権限を与えることができます。このロールを引き受けることで、アカウント B のユーザーはアカウント A のリソースを作成したり、アクセスしたりできます。
4. AWS サービスにロールを引き受ける機能 (アクセス許可) を付与するには、信頼ポリシーで指定するプリンシパルを AWS サービスにすることができます。

ロールを作成して、アクセス許可を割り当てる

ロールとアクセス許可により、AWSControl Tower および リソースへのプログラムによるアクセスを含む他の AWS サービスで、 リソースにアクセスできます。

アクセス権限を付与するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM Identity Center：

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- ID プロバイダーIAMを介して で管理されるユーザー：

  ID フェデレーションのロールを作成します。IAM 「 ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) のロールを作成する」の手順に従います。
- IAM ユーザー：
  - ユーザーが担当できるロールを作成します。「 IAMユーザーガイド」の「 IAMユーザーのロールを作成する」の手順に従います。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。「 IAMユーザーガイド」の「ユーザーへのアクセス許可の追加 (コンソール) 」の手順に従います。

を使用してアクセス許可IAMを委任する方法の詳細については、「 IAMユーザーガイド」の「アクセス管理」を参照してください。

> **Note**
>
> AWS Control Tower ランディングゾーンを設定するときは、 AdministratorAccess管理ポリシーを持つユーザーまたはロールが必要です (arn:aws:iam::aws:policy/AdministratorAccess) 。

のロールを作成するには AWS のサービス（ IAM コンソール ）

1. にサインイン AWS Management Console し、 で IAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールの作成] の順に選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
4. [サービスまたはユースケース] でサービスを選択し、次にユースケースを選択します。ユースケースは、サービスに必要な信頼ポリシーを含める定義になります。
5. [Next (次へ)] を選択します。
6. [アクセス許可ポリシー] では、オプションは選択したユースケースによって異なります。
   - サービスがロールのアクセス許可を定義している場合、アクセス許可ポリシーを選択することはできません。
   - 制限されたアクセス許可ポリシーのセットから選択します。
   - すべてのアクセス許可ポリシーから選択します。
   - アクセス許可ポリシーを選択するのではなく、ロールの作成後にポリシーを作成し、そのポリシーをロールにアタッチします。
7. (オプション) アクセス許可の境界を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。
   a. [アクセス許可の境界の設定] セクションを開き、[アクセス許可の境界を使用してロールのアクセス許可の上限を設定する] を選択します。

      IAM には、アカウントの AWS 管理ポリシーとカスタマー管理ポリシーのリストが含まれています。
   b. アクセス許可の境界として使用するポリシーを選択します。
8. [Next (次へ)] を選択します。
9. [ロール名] では、オプションはサービスによって異なります。
   - サービスでロール名が定義されている場合、ロール名を編集することはできません。
   - サービスでロール名のプレフィックスが定義されている場合、オプションのサフィックスを入力できます。
   - サービスでロール名が定義されていない場合、ロールに名前を付けることができます。

> **Important**
>
> ロールに名前を付けるときは、次のことに注意してください。
>
> - ロール名は 内で一意である必要があり AWS アカウント、大文字と小文字を区別することはできません。
>
> 例えば、**PRODROLE** と **prodrole** の両方の名前でロールを作成することはできません。ロール名がポリシーまたは の一部として使用される場合ARN、ロール名では大文字と小文字が区別されますが、サインインプロセス中など、コンソールでロール名が顧客に表示される場合、ロール名では大文字と小文字が区別されません。
> - 他のエンティティがロールを参照する可能性があるため、ロールを作成した後にロール名を編集することはできません。

10. (オプション) [説明] にロールの説明を入力します。
11. (オプション) ロールのユースケースとアクセス許可を編集するには、[ステップ 1: 信頼された エンティティを選択] または [ステップ 2: アクセス権限を追加] のセクションで [編集] を選択します。
12. (オプション) ロールの識別、整理、検索を簡単にするには、キーと値のペアとしてタグを追加します。でのタグの使用の詳細についてはIAM、「 IAMユーザーガイド」の「 AWS Identity and Access Management リソースのタグ」を参照してください。
13. ロールを確認したら、[ロールを作成] を選択します。

JSON ポリシーエディタを使用してポリシーを作成するには

1. にサインイン AWS Management Console し、 で IAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

   初めて [ポリシー] を選択する場合には、[管理ポリシーにようこそ] ページが表示されます。[今すぐ始める] を選択します。
3. ページの上部で、[ポリシーを作成] を選択します。
4. ポリシーエディタセクションで、JSONオプションを選択します。
5. JSON ポリシードキュメントを入力または貼り付けます。IAM ポリシー言語の詳細については、「 IAMJSONポリシーリファレンス」を参照してください。

6. ポリシーの検証中に生成されたセキュリティ警告、エラー、または一般警告をすべて解決してから、[次へ] を選択します。

> **Note**
>
> ビジュアルオプションとJSONエディタオプションはいつでも切り替えることができます。ただし、ビジュアルエディタで変更を加えるか、次へ を選択すると、 IAMはビジュアルエディタに合わせて最適化するようにポリシーを再構築することがあります。詳細については、「 IAMユーザーガイド」の「ポリシーの再構築」を参照してください。

7. (オプション) でポリシーを作成または編集するときに AWS Management Console、 テンプレートで使用できる JSONまたは YAMLポリシー AWS CloudFormation テンプレートを生成できます。

   これを行うには、ポリシーエディタでアクションを選択し、テンプレートの生成 CloudFormationを選択します。詳細については AWS CloudFormation、「 AWS CloudFormation ユーザーガイド」の「 AWS Identity and Access Management リソースタイプのリファレンス」を参照してください。

8. ポリシーにアクセス権限を追加し終えたら、[次へ] を選択します。

9. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。

10. (オプション) タグをキー - 値のペアとしてアタッチして、メタデータをポリシーに追加します。でのタグの使用の詳細についてはIAM、「 IAMユーザーガイド」の「 AWS Identity and Access Management リソースのタグ」を参照してください。

11. [Create Policy (ポリシーを作成)] をクリックして、新しいポリシーを保存します。

ビジュアルエディタを使用してポリシーを作成するには

1. にサインイン AWS Management Console し、 で IAMコンソールを開きますhttps://console.aws.amazon.com/iam/。

2. 左側のナビゲーションペインで、[ポリシー] を選択します。

   初めて [ポリシー] を選択する場合には、[管理ポリシーにようこそ] ページが表示されます。[Get Started] (今すぐ始める) を選択します。

3. [Create policy] を選択します。

4. [ポリシーエディタ] セクションで、[サービスを選択] セクションを見つけて、 AWS のサービスを選択します。上部の検索ボックスを使用して、サービスのリストの結果を制限することができます。ビジュアルエディタのアクセス許可ブロック内で選択できるサービスは 1 つだけです。複数のサービスにアクセス許可を付与するには、[さらにアクセス許可を追加する] を選択して、複数のアクセス許可ブロックを追加します。
5. [許可されるアクション] で、ポリシーに追加するアクションを選択します。アクションは次の方法で選択できます。

   - すべてのアクションのチェックボックスをオンにします。
   - [アクションを追加] を選択して、特定のアクションの名前を入力します。ワイルドカード文字 (*) を使用すると、複数のアクションを指定できます。
   - [アクセスレベル] グループの 1 つを選択して、アクセスレベルのすべてのアクション ([読み取り]、[書き込み]、または [リスト] など) を選択します。
   - それぞれの [アクセスレベル] グループを展開して、個々のアクションを選択します。

   デフォルトでは、作成しているポリシーが選択するアクションを許可します。その代わりに選択したアクションを拒否するには、[Switch to deny permissions (アクセス許可の拒否に切り替え)] を選択します。IAM はデフォルトでは拒否されるため、ユーザーが必要とするアクションとリソースのみに対するアクセス許可を付与することを、セキュリティのベストプラクティスとしてお勧めします。別のJSONステートメントまたはポリシーで個別に許可されているアクセス許可を上書きする場合にのみ、アクセス許可を拒否するステートメントを作成します。これにより、アクセス許可のトラブルシューティングがより困難になる可能性があるため、拒否ステートメントの数は最小限に制限することをお勧めします。
6. [リソース] では、前のステップで選択したサービスとアクションが特定のリソースの選択をサポートしていない場合は、すべてのリソースが許可され、このセクションを編集することはできません。

   リソースレベルのアクセス許可をサポートする 1 つ以上のアクションを選択した場合、ビジュアルエディタでそれらのリソースが一覧表示されます。[リソース] を展開して、ポリシーのリソースを指定できます。

   リソースは次の方法で指定できます。

   - 追加 ARNs を選択して、Amazon リソースネーム () でリソースを指定しますARN。ビジュアルARN工ディタまたはリストARNsを手動で使用できます。ARN 構文の詳細については、「 IAMユーザーガイド」の「Amazon リソースネーム (ARNs) 」を参照してください。

ポリシーの Resource要素ARNsで を使用する方法については、IAM「 ユーザーガイド」のIAMJSON「ポリシー要素: リソース」を参照してください。

- リソースの横にある [このアカウント内のすべて] を選択して、そのタイプのすべてのリソースにアクセス許可を付与します。
- [すべて] を選択し、そのサービスのすべてのリソースを選択します。

7. (オプション) [リクエスト条件 - オプション] を選択して、作成するポリシーに条件を追加します。条件は、JSONポリシーステートメントの効果を制限します。例えば、特定の時間範囲内でそのユーザーのリクエストが発生した場合にのみ、ユーザーがリソースに対してアクションを実行できるように指定できます。一般的に使用される条件を使用して、多要素認証 (MFA) デバイスを使用してユーザーを認証する必要があるかどうかを制限することもできます。または、リクエストの発行元を特定範囲内の IP アドレスに限定できます。ポリシー条件で使用できるすべてのコンテキストキーのリストについては、「サービス認可リファレンス」のAWS 「 サービスのアクション、リソース、および条件キー」を参照してください。

   条件は次の方法で選択できます。

   - 一般的に使用される条件を選択するには、チェックボックスを使用します。
   - 他の条件を指定するには、[別の条件を追加] を選択します。条件の [条件キー]、[修飾子]、[演算子] を選択し、[値] に入力します。複数の値を追加するには、[追加] を選択します。値は、論理 OR 演算子によって接続されていると見なすことができます。完了したら、[条件を追加] を選択します。

   複数の条件を追加するには、[別の条件を追加] を選択します。必要に応じて操作を繰り返します。各条件は、この 1 つのビジュアルエディタのアクセス許可ブロックにのみ適用されます。アクセス許可ブロックが一致すると見なされるためには、すべての条件が満たされている必要があります。つまり、論理 AND 演算子によって接続される条件を考慮します。

   条件要素の詳細については、「 IAMユーザーガイド」のIAMJSON「ポリシー要素: 条件」を参照してください。

8. さらにアクセス許可ブロックを追加するには、[さらにアクセス許可を追加] を選択します。各ブロックに対して、ステップ 2 から 5 を繰り返します。

> **Note**
>
> ビジュアルオプションとJSONエディタオプションはいつでも切り替えることができます。ただし、ビジュアルエディタで変更を加えるか、次へ を選択すると、 IAMはポリ

シーを再構成してビジュアルエディタ用に最適化する場合があります。詳細については、「 IAMユーザーガイド」の「ポリシーの再構築」を参照してください。

9. （オプション) でポリシーを作成または編集するときに AWS Management Console、 テンプレートで使用できる JSONまたは YAMLポリシー AWS CloudFormation テンプレートを生成できます。

   これを行うには、ポリシーエディタでアクションを選択し、テンプレートの生成 CloudFormationを選択します。詳細については AWS CloudFormation、「 AWS CloudFormation ユーザーガイド」の「 AWS Identity and Access Management リソースタイプのリファレンス」を参照してください。
10. ポリシーにアクセス権限を追加し終えたら、[次へ] を選択します。
11. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認し、意図したアクセス許可を付与したことを確認します。
12. (オプション) タグをキー - 値のペアとしてアタッチして、メタデータをポリシーに追加します。でのタグの使用の詳細についてはIAM、「 IAMユーザーガイド」の「 AWS Identity and Access Management リソースのタグ」を参照してください。
13. [Create Policy (ポリシーを作成)] をクリックして、新しいポリシーを保存します。

プログラム的なアクセス権を付与するには

ユーザーが の AWS 外部で を操作する場合は、プログラムによるアクセスが必要です AWS Management Console。プログラムによるアクセスを許可する方法は、 がアクセスするユーザーのタイプによって異なります AWS。

ユーザーにプログラマチックアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ （ IAMIdentity Center で管理されるユーザー ）	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または へのプログラムによるリクエストに署名します AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line

プログラマチックアクセス権を必要とするユーザー	目的	方法
		Interface ユーザーガイド」の「 を使用する AWS CLI ための の設定 AWS IAM Identity Center」を参照してください。 • AWS SDKs、ツール、および については AWS APIs、AWS SDKs「 およびツールリファレンスガイド」のIAM「 Identity Center 認証」を参照してください。
IAM	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または へのプログラムによるリクエストに署名します AWS APIs。	「 ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。 IAM

プログラマチックアクセス権を必要とするユーザー	目的	方法
IAM	(非推奨) 長期認証情報を使用して、、AWS SDKs AWS CLI、または AWS APIs へのプログラムによるリクエストに署名します。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」のIAM「ユーザー認証情報を使用した認証」を参照してください。 • および ツールについては AWS SDKs、「 AWS SDKs およびツールリファレンスガイド」の「長期認証情報を使用した認証」を参照してください。 • については AWS APIs、「 IAMユーザーガイド」のIAM「 ユーザーのアクセスキーの管理」を参照してください。

攻撃者からの保護

他の AWS サービスプリンシパルにアクセス許可を付与するときに攻撃者から保護する方法の詳細については、「ロールの信頼関係のオプション条件」を参照してください。ポリシーに特定の条件を追加することで、混乱した代理攻撃と呼ばれる特定のタイプの攻撃を防ぐことができます。これは、クロスサービス偽装など、エンティティが、より特権のあるエンティティにアクションを実行させる場合に発生します。ポリシー条件に関する一般的な情報については、「ポリシーの条件の指定」も参照してください。

AWS Control Tower でのアイデンティティベースのポリシーの使用の詳細については、「」を参照してくださいAWS Control Tower でアイデンティティベースのポリシー (IAM ポリシー) を使用する。ユーザー、グループ、ロール、アクセス許可の詳細については、 IAM ユーザーガイドの「アイデンティティ (ユーザー、グループ、ロール)」を参照してください。

リソースベースのポリシー

Amazon S3 などの他のサービスでは、リソースベースの許可ポリシーもサポートされています。例えば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス権限を管理できます。AWSControl 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。

ポリシー要素を指定: アクション、効果、プリンシパル

AWS Control Tower コンソールまたはランディングゾーン を使用して、ランディングゾーンAPIsを設定および管理できます。ランディングゾーンを設定するには、IAMポリシーで定義されている管理アクセス許可を持つ IAM ユーザーである必要があります。

ポリシーで識別できる最も基本的な要素は次の通りです。

- リソース – ポリシーでは、Amazon リソースネーム (ARN) を使用して、ポリシーが適用されるリソースを識別します。詳細については、「AWS Control Tower のリソースとオペレーション」を参照してください。
- アクション – アクションキーワードを使用して、許可または拒否するリソース操作を特定します。実行できるアクションのタイプについては、AWS「Control Tower で定義されるアクション」を参照してください。
- 効果 – ユーザーが特定のアクションを要求する際の効果を指定します。許可または拒否のいずれかになります。リソースへのアクセスを明示的に付与 (許可) していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- 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) では、ポリシーがアタッチされているユーザーが暗黙的なプリンシパルです。リソースベースのポリシーでは、許可 (リソースベースのポリシーにのみ適用) を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。AWSControl 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。例えば、特定の日付の後にのみ適用されるポリシーが必要になる場合がありま

す。ポリシー言語での条件の指定の詳細については、「 IAMユーザーガイド」の「条件」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。AWS Control Tower に固有の条件キーはありません。ただし、必要に応じて使用できる AWS全体の条件キーがあります。 AWS全体のキーの完全なリストについては、「 IAMユーザーガイド」の「条件に使用可能なキー」を参照してください。

クロスサービス偽装の防止

では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。あるサービスが別のサービスを呼び出すとき、あるサービスが別のサービスを操作し、それ以外では許可されていない方法で、お客様のリソースに影響を及ぼす許可を使用した場合、クロスサービス偽装が発生します。この攻撃を防ぐために、 は、正当なアクセス許可を持つサービスのみがアカウント内のリソースにアクセスできるように、データを保護するのに役立つツール AWS を提供します。

Control Tower がリソースにアクセスするために別のサービスに付与するアクセス許可を制限するには、ポリシーの `aws:SourceArn`および AWS `aws:SourceAccount`条件を使用することをお勧めします。

- クロスサービスのアクセスにリソースを 1 つだけ関連付けたい場合は、`aws:SourceArn` を使用します。
- クロスサービスが使用できるように、アカウント内の任意のリソースを関連付けたい場合は、`aws:SourceAccount` を使用します。
- `aws:SourceArn` 値に Amazon S3 バケットARNの などのアカウント ID が含まれていない場合は、両方の条件を使用してアクセス許可を制限する必要があります。
- 両方の条件を使用する場合、および `aws:SourceArn` の値にアカウント ID が含まれている場合は、`aws:SourceAccount` の値と、`aws:SourceArn` の値のアカウントは、同じポリシーステートメントで使用するとき、同じアカウント ID を示している必要があります。

詳細な説明と例については、「https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html」を参照してください。

AWS Control Tower でアイデンティティベースのポリシー (IAM ポリシー) を使用する

このトピックでは、アカウント管理者がどのようにして IAM アイデンティティ (ユーザー、グループ、ロール) に許可ポリシーをアタッチし、それによって AWS Control Tower リソースでのオペレーションを実行する許可を付与する方法を示す、アイデンティティベースのポリシーの例を示します。

> **Important**
>
> 初めに、AWS Control Tower リソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要トピックをお読みになることをお勧めします。詳細については、「AWS Control Tower リソースへのアクセス許可の管理の概要」を参照してください。

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

AWS Control Tower は、ランディングゾーンを設定するときに、3 つのロールを自動的に作成します。コンソールアクセスを許可するには、3 つのロールすべてが必要です。AWS Control Tower では、アクションおよびリソースの最小セットへのアクセスを制限するためのベストプラクティスとして、アクセス許可が 3 つのロールに分割されます。

3 つの必須ロール

- AWS Control Tower 管理者ロール
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

これらのロールのロール信頼ポリシーへのアクセスを制限することをお勧めします。詳細については、「Optional conditions for your role trust relationships」を参照してください。

AWS Control Tower 管理者ロール

このロールは、ランディングゾーンの維持にきわめて重要なインフラストラクチャへのアクセス権を持つ AWS Control Tower を提供します。`AWS ControlTowerAdmin` ロールには、アタッチされたマネージドポリシーと、IAM ロールのロール信頼ポリシーが必要です。ロール信頼ポリシーは、リソースベースのポリシーで、どのプリンシパルがロールを引き受けることができるかを指定します。

このロールの信頼ポリシーのサンプルスニペットを次に示します。

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

AWS CLI からこのロールを作成し、 という名前のファイルに入れるにはtrust.json、CLI コマンドの例を次に示します。

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

このロールには 2 つの IAM ポリシーが必要です。

1. インラインポリシー。次に例を示します。

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

2. 次に示すマネージドポリシー。これは AWS ControlTowerServiceRolePolicy です。

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicy は、CloudFormation スタックセットとスタックインスタンス、 AWS CloudTrail ログファイル、AWS Control Tower の設定アグリゲータ、AWS Control Tower によって管理される AWS Organizations アカウントと組織単位 (OUs) などの AWS AWS Control Tower リソースを作成および管理するためのアクセス許可を定義する AWSマネージドポリシーです。

この管理ポリシーの更新は、表 AWS Control Tower のマネージドポリシー にまとめられています。

詳細については、『AWS マネージドポリシーリファレンスガイド』の「AWSControlTowerServiceRolePolicy」を参照してください。

ロール信頼ポリシー:

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

インラインポリシーは AWSControlTowerAdminPolicy です。

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

AWS ControlTowerStackSetRole

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"
        }
    ]
}
```

信頼ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control Tower は、ベストプラクティスとして CloudTrail を有効にし、CloudTrail にこのロールを提供します。CloudTrail は CloudTrail ログを作成し公開するために、このロールを引き受けます。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"
        }
    ]
}
```

信頼ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess ロールの要件

AWS Control Tower では、同じ組織内の指定されたブループリントハブアカウントに AWSControlTowerBlueprintAccess ロールを作成する必要があります。

ロール名

ロールタイプは、AWSControlTowerBlueprintAccess である必要があります。

ロール信頼ポリシー

ロールは、以下のプリンシパルを信頼するように設定する必要があります。

- 管理アカウントで AWS Control Tower を使用するプリンシパル。
- 管理アカウントの AWSControlTowerAdmin ロール。

以下の例は、最小特権の信頼ポリシーを示しています。独自のポリシーを作成する場合は、*YourManagementAccountId* を AWS Control Tower 管理アカウントの実際のアカウント ID で置き換え、*YourControlTowerUserRole* を管理アカウントの IAM ロールの識別子で置き換えます。

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

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

ロールのアクセス許可

管理ポリシーの AWSServiceCatalogAdminFullAccess をロールにアタッチする必要があります。

AWSServiceRoleForAWSControlTower

このロールは、ランディングゾーンの維持に不可欠な操作 (ドリフトしたリソースの通知など) のために、Log Archive アカウント、監査アカウント、およびメンバーアカウントへのアクセス権を AWS Control Tower に 付与します。

AWSServiceRoleForAWSControlTower ロールには、アタッチされたマネージドポリシーと、IAM ロールのロール信頼ポリシーが必要です。

このロールのマネージドポリシー: AWSControlTowerAccountServiceRolePolicy

ロール信頼ポリシー:

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

AWSControlTowerAccountServiceRolePolicy

この AWS管理ポリシーにより、AWS Control Tower は自動アカウント設定と一元化されたガバナンスを提供する AWS サービスをユーザーに代わって呼び出すことができます。

このポリシーには、Security Hub サービスマネージドスタンダード: (AWS Control Tower の一部である Security Hub コントロールによって管理されるリソースついの AWS Security Hub 検出結果の転送を AWS Control Tower が実装するための最低限のアクセス許可が含まれており、顧客アカウントの管理機能を制限する変更を防止します。これはバックグラウンド AWS Security Hub ドリフト検出プロセスの一部であり、お客様が直接開始することはありません。

このポリシーでは、Security Hub コントロール専用の Amazon EventBridge ルールを各メンバーアカウントに作成するアクセス許可が与えられます。これらのルールには、正確な EventPattern を指定する必要があります。また、ルールはサービスプリンシパルが管理するルールにのみ適用されます。

サービスプリンシパル: `controltower.amazonaws.com`

詳細については、「 AWS マネージドポリシーリファレンスガイドAWSControlTowerAccountServiceRolePolicy」の「」を参照してください。

この管理ポリシーの更新は、表 AWS Control Tower のマネージドポリシー にまとめられています。

AWS Control Tower のマネージドポリシー

AWS は、 によって作成および管理されるスタンドアロン IAM ポリシーを提供することで、多くの一般的なユースケースに対処します AWS。マネージドポリシーは、一般的ユースケースに必要な許

可を付与することで、どの許可が必要なのかをユーザーが調査する必要をなくすることができます。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

変更	説明	日付
AWS ControlTowerServiceRolePolicy - 既存ポリシーへの更新	AWS Control Tower は、AWS Control Tower が で AWS CloudFormation サービス APIs `ActivateType` 、、`DeactivateType` および を呼び出すことを許可する新しいアクセス許可を追加`SetTypeConfiguration` しましたAWS::ControlTower types。 この変更により、お客様はプライベート AWS CloudFormation フックタイプのデプロイなしでプロアクティブコントロールをプロビジョニングできます。	2024 年 12 月 10 日
AWSControlTowerAccountServiceRolePolicy - 新しいポリシー	AWS Control Tower には、サービスにリンクされた新しいロールが追加されました。これにより、AWS Control Tower はイベントルールを作成および管理し、それらのルールに基づいて Security Hub に関連するコントロールのドリフト検出を管理できます。 この変更は、ドリフトしたリソースが Security Hub サービスマネージドスタンダード:	2023 年 5 月 22 日

変更	説明	日付
	AWS Control Tower の一部である Security Hub コントロールに関連している場合に、お客様がコンソールでリソースを確認するために必要です。	
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower は、ランディングゾーンの顧客アカウント (管理アカウント、ログアーカイブアカウント、監査アカウント、OU メンバーアカウント) がオプトイン AWS リージョン を利用できるように、AWS Control Tower が AWS アカウント管理サービスにより実装された `EnableRegion` 、`ListRegions` 、および`GetRegionOptStatus` API を呼び出すための新しい権限を追加されました。 この変更は、お客様が AWS Control Tower によるリージョン管理をオプトインリージョンに拡張するために必要です。	2023 年 4 月 6 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower では、AWS Control Tower がブループリント (ハブ) アカウントで AWSControlTowerBlueprintAccess ロールを引き受けることができる新しいアクセス許可が追加されました。ブループリント (ハブ) アカウントは、組織内の専用アカウントであり、1 つ以上の Service Catalog 製品に保存されている事前定義済みのブループリントを含みます。AWS Control Tower は、Service Catalog ポートフォリオの作成、リクエストされたブループリント製品の追加、およびアカウントプロビジョニング時にリクエストされたメンバーアカウントへのポートフォリオの共有という 3 つのタスクを実行するために AWSControlTowerBlueprintAccess ロールを引き受けます。 この変更は、お客様が AWS Control Tower Account Factory を通じてカスタマイズされたアカウントをプロビジョニングするために必要です。	2022 年 10 月 28 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存ポリシーへの更新	AWS Control Tower では、ランディングゾーンバージョン 3.0 以降、お客様が組織レベルの AWS CloudTrail 証跡を設定できるようにする新しいアクセス許可が追加されました。 組織ベースの CloudTrail 機能を使用するには、お客様が CloudTrail サービスに対して信頼されたアクセスを有効にする必要があります。また、IAM ユーザーまたはロールが、管理アカウントで組織レベルの追跡を作成するアクセス許可を持っていることが必要です。	2022 年 6 月 20 日

変更	説明	日付
AWS ControlTowerServiceRolePolicy – 既存のポリシーを更新します	AWS Control Tower では、お客様が KMS キー暗号化を使用できるようにする新しいアクセス許可が追加されました。 KMS 機能を使用すると、お客様独自の KMS キーを提供して AWS CloudTrail ログを暗号化できます。また、お客様は、ランディングゾーンの更新または修復中に KMS キーを変更することもできます。KMS キーを更新する場合、 AWS CloudFormation には AWS CloudTrail `PutEventSelector` API を呼び出すアクセス許可が必要です。ポリシーの変更は、AWS ControlTowerAdmin ロールが API を呼び出せるようにすることです AWS CloudTrail `PutEventSelector` 。	2021 年 7 月 28 日
AWS Control Tower は変更の追跡を開始しました	AWS Control Tower が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 5 月 27 日

AWS Control Tower のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。 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メリットを得られます。

セキュリティは、 AWS とお客様の間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 は、お客様が安全に使用できるサービスも提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。AWS Control Tower に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内のAWS のサービス」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、AWS Control Tower を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するよう AWS Control Tower を設定する方法について説明します。また、AWS Control Tower リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

AWS Control Tower のデータ保護

責任 AWS 共有モデル、AWS Control Tower でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。

この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して AWS Control Tower AWS CLIまたは他の AWS のサービス を操作する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

> **Note**
>
> を使用したユーザーアクティビティのログ記録 AWS CloudTrail は、ランディングゾーンを設定すると AWS Control Tower で自動的に処理されます。

データ保護の詳細については、AWS セキュリティブログ のブログ投稿「AWS の責任共有モデルと GDPR」を参照してください。AWS Control Tower には、ランディングゾーンに存在するコンテンツを保護するために使用できる次のオプションがあります。

トピック

- 保管時の暗号化

- 転送時の暗号化
- コンテンツへのアクセスの制限

保管時の暗号化

AWS Control Tower では、ランディングゾーンを支援するために Simple Storage Service (Amazon S3) マネージドキー (SSE-S3) を使用して保管時に暗号化される Simple Storage Service (Amazon S3) バケットおよび Amazon DynamoDB データベースを使用します。デフォルトでは、この暗号化はランディングゾーンのセットアップ時に設定されます。必要に応じて、KMS 暗号化キーでリソースを暗号化するようにランディングゾーンを構成できます。また、ランディングゾーンでそれをサポートするサービス用に使用するサービスに対して保管時の暗号化を確立することもできます。詳細については、そのサービスのオンラインドキュメントでセキュリティに関する章を参照してください。

転送時の暗号化

AWS Control Tower では、ランディングゾーンを支援するために転送中の暗号化に Transport Layer Security (TLS) とクライアント側の暗号化を使用します。さらに、AWS Control Tower へのアクセスには、HTTPS エンドポイント経由でのみアクセスできるコンソールを使用する必要があります。デフォルトでは、この暗号化はランディングゾーンのセットアップ時に設定されます。

コンテンツへのアクセスの制限

ベストプラクティスとして、適切なユーザーのサブセットへのアクセスを制限する必要があります。AWS Control Tower でこれを行うには、集中型クラウド管理者とエンドユーザーが適切な IAM アクセス許可を持ち、IAM Identity Center ユーザーの場合は、適切なグループに存在している必要があります。

- IAM エンティティのロールとポリシーの詳細については、「IAM ユーザーガイド」を参照してください。
- ランディングゾーンのセットアップ時に作成された IAM Identity Center グループの詳細については、「IAM AWS Control Tower の Identity Center グループ」を参照してください。

AWS Control Tower のコンプライアンス検証

AWS Control Tower は、組織がコントロールおよびベストプラクティスでコンプライアンスのニーズを満たすのに役立つ優れた設計のサービスです。さらに、サードパーティーの監査者

が、複数の AWS コンプライアンスプログラムの一部としてランディングゾーンで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。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、AWS「コンプライアンスプログラムによる対象範囲内のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 AWS Artifact ユーザーガイド」の AWS「アーティファクトでのレポートのダウンロード」を参照してください。

AWS Control Tower を使用する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、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイする手順を示します AWS。
- アマゾン ウェブ サービスでの HIPAA セキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や場所に適用される場合があります。
- AWS Config – この AWS サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。
- AWS Security Hub – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

AWS Control Tower の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。

AWS リージョンは、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。これらは、低レイテンシー、高スループット、および高度に冗長なネットワークによって接続されます。複数のアベイラビリティーゾーンがあることで、アベイラビリティーゾーン間で自動的

にフェイルオーバーして中断することなく動作するアプリケーションとデータベースを設計して運用できます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS Control Tower が利用可能な AWS リージョン のリストについては、「」を参照してくださいAWS リージョンと AWS Control Tower の連携方法。

ホームリージョンは、ランディングゾーンが設定された AWS リージョンとして定義されます。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

AWS Control Tower のインフラストラクチャセキュリティ

AWS Control Tower は、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。

が AWS 公開した API コールを使用して、 ネットワーク経由でランディングゾーン内の AWS サービスとリソースにアクセスします。Transport Layer Security (TLS) 1.2 が必要であり、Transport Layer Security (TLS) 1.3 以降が推奨されています。また、一時的ディフィー・ヘルマン Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、テンポラリセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Control Tower ランディングゾーンワークロードのネットワークインフラストラクチャセキュリティを強化するようにセキュリティグループを設定できます。詳細については、「チュートリアル: を使用して AWS Control Tower でセキュリティグループを設定する AWS Firewall Manager」を参照してください。

AWS Control Tower でのログ記録とモニタリング

モニタリングを使用すると、潜在的なインシデントに対して計画を立て、対応することができます。モニタリングアクティビティの結果が、ログファイルに保存されます。したがって、ログ記録とモニタリングは密接に関連する概念であり、AWSControl Tower の優れた設計性の重要な部分です。

ランディングゾーンをセットアップすると作成される共有アカウントの 1 つが、ログアーカイブアカウントです。これは、すべての共有アカウントとメンバーアカウントのログを含む、すべてのログを一元的に収集することに特化しています。ログファイルは Amazon S3 バケットに保存されます。これらのログファイルを参照することで、管理者と監査人は発生したアクションとイベントを確認できます。

ベストプラクティスとして、マルチポイント障害が発生した場合に簡単にデバッグできるように、AWS セットアップのすべての部分からモニタリングデータをログに収集することをお勧めします。AWS には、ランディングゾーンのリソースとアクティビティをモニタリングするためのツールがいくつか用意されています。

例えば、コントロールのステータスは常にモニタリングされます。Control Tower コンソールで、または AWS Control AWS Tower を使用してプログラムでステータスを確認できますAPIs。Account Factory でプロビジョニングしたアカウントの正常性とステータスも常にモニタリングされます。

ログに記録されたアクションを [アクティビティ] ページから表示する

AWS Control Tower コンソールのアクティビティページには、AWSControl Tower 管理アカウントのアクションの概要が表示されます。AWS Control Tower のアクティビティページに移動するには、左側のナビゲーションからアクティビティを選択します。

アクティビティページに表示されるアクティビティは、AWSControl Tower の AWS CloudTrail イベントログで報告されるアクティビティと同じですが、テーブル形式で表示されます。特定のアクティビティの詳細を表示するには、表からアクティビティを選択し、[View details] (詳細の表示) を選択します。

メンバーアカウントのアクションとイベントは、ログアーカイブファイルで表示できます。

以下のセクションでは、AWSControl Tower でのモニタリングとログ記録について詳しく説明します。

トピック

- を使用した AWS Control Tower アクションの ログ記録 AWS CloudTrail
- AWS Control Tower のライフサイクルイベント
- での AWS ユーザー通知の使用 AWS Control Tower

AWS Control Tower でのログ記録について

AWS Control Tower は、 および との統合を通じてアクション AWS CloudTrail とイベントのログ記録を自動的に実行し AWS Config、記録します CloudWatch。AWS Control Tower 管理アカウントからのアクションや組織のメンバーアカウントからのアクションなど、すべてのアクションがログに記録されます。管理アカウントのアクションとイベントは、コンソールの [Activities] (アクティビティ) ページに表示されます。メンバーアカウントのアクションとイベントは、ログアーカイブファイルで表示できます。

組織レベルの証跡

AWS Control Tower は、ランディングゾーンを設定するときに新しい CloudTrail 証跡を設定します。これは組織レベルの証跡で、組織内の管理アカウントとすべてのメンバーアカウントの全イベントがログされます。この機能は、各メンバーアカウントで証跡を作成する管理アカウントアクセス許可を付与するのに信頼されたアクセスに依存します。

AWS Control Tower と CloudTrail 組織の証跡の詳細については、「組織の証跡の作成」を参照してください。

> **Note**
>
> ランディングゾーンバージョン 3.0 より前の AWS Control Tower リリースでは、AWSControl Tower は各アカウントにメンバーアカウントの証跡を作成しました。リリース 3.0 に更新すると、証 CloudTrail 跡は組織の証跡になります。証跡間を移動する際のベストプラクティスについては、「 CloudTrail ユーザーガイド」の「証跡変更のベストプラクティス」を参照してください。

アカウントを AWS Control Tower に登録すると、そのアカウントは AWS Control Tower 組織の AWS CloudTrail 証跡によって管理されます。そのアカウントに既存の CloudTrail 証跡のデプロイがある場合、AWSControl Tower に登録する前にアカウントの既存の証跡を削除しない限り、料金が重複することがあります。

> **Note**
>
> ランディングゾーンバージョン 3.0 に更新すると、AWSControl Tower はユーザーに代わって登録済みアカウントのアカウントレベルの証跡 (AWSControl Tower が作成した証跡) を削除します。既存のアカウントレベルのログファイルは、Amazon S3 バケットに保存されます。

監査アカウントの Amazon S3 バケットポリシー

AWS Control Tower では、リクエストが組織または組織単位 (OU) から発信された場合にのみ、 AWS サービスはリソースにアクセスできます。書き込みアクセス許可のためには、`aws:SourceOrgID` 条件を満たす必要があります。

`aws:SourceOrgID` 条件キーを使用して、Amazon S3 バケットポリシーの条件要素で [組織 ID] の値を設定できます。この条件により、 は組織内のアカウントに代わって CloudTrail のみ S3 バケットにログを書き込むことができます。これにより、組織外の CloudTrail ログが AWS Control Tower S3 バケットに書き込まれなくなります。

このポリシーは、既存のワークロードの機能には影響しません。このポリシーを以下の例に示します。

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
```

```
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForConfig
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - Fn::Join:
                  - ""
                  -
                    - !Sub "arn:${AWS::Partition}:s3:::"
                    - !Ref "S3AuditBucket"
                    - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
          - Sid: AWSBucketDeliveryForOrganizationTrail
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
```

```
        Condition:
          StringEquals:
        aws:SourceOrgID: !Ref OrganizationId
```

この条件キーの詳細については、 IAMドキュメントとIAMブログ記事「リソースにアクセスするAWS サービスにスケーラブルなコントロールを使用する」を参照してください。

統合されたモニタリング用ツール

モニタリングは、AWSControl Tower およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。 は、AWSControl Tower を監視したり、問題が発生したときに報告したり、必要に応じて自動アクションを実行したりするために、以下のモニタリングツール AWS を提供します。

- Amazon CloudWatch は、 AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、 で Amazon EC2インスタンスのCPU使用状況やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。
- Amazon CloudWatch Events は、 AWS リソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。 CloudWatch Events は、特定のイベントを監視し、これらのイベントが発生したときに他の AWS サービスで自動アクションをトリガーするルールを記述できるため、自動イベント駆動型コンピューティングを有効にします。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 を使用すると、Amazon EC2インスタンスやその他のソースからログファイルをモニタリング、保存 CloudTrail、アクセスできます。 CloudWatch Logs はログファイル内の情報をモニタリングし、特定のしきい値に達したときに通知できます。高い耐久性を備えたストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われたAPI呼び出しおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元の IP アドレス、呼び出しの発生日時を特定できます。

ヒント: Logs と CloudWatch Logs Insights CloudWatch を使用して、アカウントの CloudTrail アクティビティを表示およびクエリできます。このアクティビティには、AWSControl Tower ライフサイ

クルイベントが含まれます。 CloudWatch ログの機能を使用すると、通常使用できるクエリよりも詳細で正確なクエリを実行できます CloudTrail。

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

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

AWS Control Tower は、ユーザー AWS CloudTrail、ロール、または AWS Control Tower の 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ある と統合されています。 は AWS、Control Tower のアクションをイベントとして CloudTrail キャプチャします。証跡を作成する場合は、AWSControl Tower の CloudTrail イベントなど、Amazon S3 バケットへの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。によって収集された情報を使用して CloudTrail、AWSControl Tower に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

設定と有効化の方法などの詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

AWS の Control Tower 情報 CloudTrail

CloudTrail AWS アカウントを作成すると、 はアカウントで有効になります。AWS Control Tower でサポートされているイベントアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴の他の AWS サービスイベントとともにイベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

> **Note**
>
> ランディングゾーンバージョン 3.0 より前の AWS Control Tower リリースでは、AWSControl Tower はメンバーアカウントの証跡を作成しました。リリース 3.0 に更新すると、 CloudTrail 証跡は組織の証跡に更新されます。証跡間を移動する際のベストプラクティスについては、「 CloudTrail ユーザーガイド」の「組織証跡の作成」を参照してください。

推奨: 証跡の作成

AWS Control Tower のイベントなど、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、 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、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析してそれに基づく対応を行うように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- 証跡の作成を準備する
- コストの管理 CloudTrail
- CloudTrail サポートされているサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからのログファイルの受信 CloudTrail

AWS Control Tower は、次のアクションをイベントとして CloudTrail ログファイルに記録します。

パブリック APIs

- AWS Control Tower のパブリックの完全なリストAPIsとそれぞれの詳細については、AWS「Control Tower APIリファレンス」を参照してください。これらのパブリックへの呼び出しAPIsは、 によってログに記録されます AWS CloudTrail。

その他 APIs

- `SetupLandingZone`
- `UpdateAccountFactoryConfig`
- `ManageOrganizationalUnit`
- `CreateManagedAccount`
- `GetLandingZoneStatus`
- `GetHomeRegion`
- `ListManagedAccounts`

- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが root または AWS Identity and Access Management （ IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。
- リクエストがアクセス拒否として拒否されたか、正常に処理されたか。

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

例: AWS Control Tower ログファイルエントリ

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ようにする設定です。 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。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエスト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、SetupLandingZoneAWSControl Tower イベントの一般的なログファイルエントリの構造 CloudTrail を示すログエントリを示しています。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
```

```
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```


でリソースの変更をモニタリングする AWS Config

AWS Control Tower は、すべての登録済みアカウント AWS Config で を有効にし、検出コントロールによるコンプライアンスのモニタリング、リソースの変更の記録、ログアーカイブアカウントへのリソース変更ログの配信を可能にします。

ランディングゾーンのバージョンが 3.0 より前の場合: 登録済みアカウントの場合、 は、アカウントが動作するすべてのリージョンのリソースに対するすべての変更を AWS Config ログに記録します。各変更は、リソース識別子、リージョン、各変更が記録された日付、および変更が既知のリソースまたは新しく検出されたリソースに関連するかどうかなどの情報を含む構成項目 (CI) としてモデル化されます。

ランディングゾーンのバージョンが 3.0 以降の場合: AWS Control Tower は、IAMユーザー、グループ、ロール、カスタマー管理ポリシーなどのグローバルリソースの記録をホームリージョンのみに制限します。グローバルリソースの変更のコピーは、すべてのリージョンに保存されるわけではありません。このリソース記録の制限は、 AWS Config ベストプラクティスに準拠しています。グローバルリソースの完全なリストは、 AWS Config ドキュメントで入手できます。

- 詳細については AWS Config、「 AWS Config の仕組み」を参照してください。
- がサポート AWS Config できるリソースのリストについては、「サポートされているリソースタイプ」を参照してください。
- AWS Control Tower 環境でリソース追跡をカスタマイズする方法については、ブログ記事「Customize AWS Config resource tracking in AWS Control Tower」を参照してください。

AWS Control Tower は、すべての登録済みアカウントで AWS Config 配信チャネルを設定します。この配信チャネルを通じて、 AWS Config によってログアーカイブアカウントに記録されたすべての変更がログに記録され、Amazon Simple Storage Service バケットのフォルダに保存されます。

AWS Control Tower で AWS Config コストを管理する

このセクションでは、 が AWS Control Tower アカウントのリソースの変更 AWS Config を記録し、請求する方法について説明します。この情報は、AWSControl Tower を利用するときに AWS Config、関連するコストを管理する方法を理解するのに役立ちます。 AWSControl Tower には追加コストはかかりません。

> **Note**
>
> ランディングゾーンのバージョンが 3.0 以降の場合: AWS Control Tower は、IAMユーザー、グループ、ロール、カスタマー管理ポリシーなどのグローバルリソース AWS Config の記録をホームリージョンのみに制限します。したがって、このセクションの情報の一部がランディングゾーンに適用されない場合があります。

AWS Config は、アカウントが動作する各リージョンの各リソースに対する各変更を、設定項目 (CI) として記録するように設計されています。 は、生成する設定項目ごとに AWS Config 請求します。

AWS Config の動作

AWS Config は、各リージョンのリソースを個別に記録します。IAM ロールなどの一部のグローバルリソースは、リージョンごとに 1 回記録されます。たとえば、5 つのリージョンで運用されている登録済みアカウントに新しいIAMロールを作成すると、 はリージョンごとに 1 つずつCIs、5 つの AWS Config を生成します。Route 53 ホストゾーンなどの他のグローバルリソースは、すべてのリージョンで 1 回だけ記録されます。たとえば、登録済みアカウントで新しい Route 53 ホストゾーンを作成すると、そのアカウントに選択されているリージョンの数に関係なく、 AWS Config が CI を 1 回生成します。これらのタイプのリソースを区別するのに役立つリストについては、「同じリソースが複数回記録されている」を参照してください。

> **Note**
>
> AWS Control Tower が と連携する場合 AWS Config、リージョンは AWS Control Tower によって管理されるか、管理されていない AWS Config 可能性があり、アカウントがそのリージョンで動作している場合は変更が記録されます。

AWS Config が リソース内の 2 種類の関係を検出する

AWS Config は、リソース間の直接関係と間接関係を区別します。リソースが別のリソースの Describe API呼び出しで返された場合、それらのリソースは直接的な関係として記録されます。別のリソースとの直接的な関係でリソースを変更しても、 AWS Config は両方のリソースに対して CI を作成しません。

例えば、Amazon EC2インスタンスを作成し、 でネットワークインターフェイスを作成APIする必要がある場合、 では、Amazon EC2インスタンスがネットワークインターフェイスと直接関係があること AWS Config を考慮します。その結果、 は 1 つの CI のみ AWS Config を生成します。

AWS Config は、間接的な関係であるリソース関係に個別の変更を記録します。例えば、セキュリティグループCIsを作成し、セキュリティグループの一部である関連付けられた Amazon EC2インスタンスを追加すると、 は 2 AWS Config を生成します。

直接的な関係と間接的な関係の詳細については、「リソースに関する直接的な関係と間接的な関係とは何ですか?」を参照してください。

リソース関係のリストは、 AWS Config ドキュメントに記載されています。

登録済みアカウントの AWS Config レコーダーデータを表示する

AWS Config は と統合 CloudWatch されているため、ダッシュボードで を表示できます AWS Config CIs。詳細については、ブログ記事AWS Config 「Supports Amazon CloudWatch metrics」を参照してください。

プログラムで AWS Config データを表示するには、 を使用するか AWS CLI、他の AWS ツールを使用できます。

特定のリソースの AWS Config レコーダーデータをクエリする

を使用して AWS CLI、リソースの最新の変更のリストを取得できます。

リソース履歴コマンド:

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

詳細については、 のAPIドキュメントget-config-historyを参照してください。

Amazon で AWS Config データを視覚化する QuickSight

組織全体で によって記録されたリソース AWS Config を視覚化してクエリできます。詳細については、Amazon Athena と Amazon を使用した AWS Config データの視覚化 QuickSight」を参照してください。

AWS Control Tower AWS Config でのトラブルシューティング

このセクションでは、AWSControl Tower AWS Config で を使用するときに発生する可能性のあるいくつかの問題について説明します。

高 AWS Config コスト

ワークフローにリソースを頻繁に作成、更新、削除するプロセスが含まれている場合、または大量のリソースを処理する場合、そのワークフローは多数の を生成する可能性がありますCIs。非本番アカウントでこれらのプロセスを実行する場合、アカウントの登録解除を検討してください。そのアカウントの AWS Config レコーダーを手動で非アクティブ化する必要がある場合があります。

> **Note**
>
> アカウントを登録解除すると、AWSControl Tower は、そのアカウントのリソースに対して検出コントロールを適用したり、 AWS Config アクティビティなどのアカウントイベントをログに記録したりすることはできません。

アカウントの管理解除について詳細は、登録済みアカウントの管理を解除するを参照してください。AWS Config レコーダーを非アクティブ化する方法については、「設定レコーダーの管理」を参照してください。

同じリソースが複数回記録されている

そのリソースがグローバルリソースかどうかをチェックします。バージョン 3.0 より前の AWS Control Tower ランディングゾーンでは、 AWS Config が動作しているリージョンごとに特定のグローバルリソースを 1 回記録 AWS Config できます。たとえば、 AWS Config が 8 つのリージョンで有効になっている場合、各ロールは 8 回記録されます。

以下のリソースは、 AWS Config が動作しているリージョンごとに 1 回記録されます。

- `AWS::IAM::Group`

- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User

他のグローバルリソースは 1 回のみ記録されます。1 回記録されたリソースの例を次に示します。

- AWS::Route53::HostedZone
- AWS::Route53::HealthCheck
- AWS::ECR::PublicRepository
- AWS::GlobalAccelerator::Listener
- AWS::GlobalAccelerator::EndpointGroup
- AWS::GlobalAccelerator::Accelerator

AWS Config はリソースを記録しませんでした

特定のリソースは、他のリソースと依存関係があります。これらの関係は、直接的または間接的です。非推奨の間接的な関係のリストは、 AWS Config FAQにあります。

AWS Control Tower のライフサイクルイベント

AWS Control Tower によってログに記録されるイベントには、ライフサイクルイベントがあります。ライフサイクルイベントの目的は、リソースの状態を変更する特定の AWS Control Tower アクションの完了をマークすることです。ライフサイクルイベントは、組織単位 (OUs) 、アカウント、コントロールなど、AWSControl Tower が作成または管理するリソースに適用されます。

AWS Control Tower ライフサイクルイベントの特徴

- イベントログは、ライフサイクルイベントごとに生成元の Control Tower アクションが正常に完了したか失敗したかを示します。
- AWS CloudTrail は、各ライフサイクルイベントを非API AWS サービスイベントとして自動的に記録します。詳細については、「 CloudTrail ユーザーガイド AWS 」を参照してください。
- 各ライフサイクルイベントは、Amazon EventBridge および Amazon CloudWatch Events サービスにも配信されます。

AWS Control Tower のライフサイクルイベントには、主に 2 つの利点があります。

- ライフサイクルイベントは AWS Control Tower アクションの完了を登録するため、ライフサイクルイベントの状態に基づいて、自動化ワークフローの次のステップをトリガーできる Amazon EventBridge ルールまたは Amazon CloudWatch Events ルールを作成できます。
- ログの詳細を参照することで、管理者や監査人は組織内の特定のタイプのアクティビティを確認できます。

ライフサイクルイベントの仕組み

AWS Control Tower は、複数のサービスに依存してアクションを実装します。したがって、各ライフサイクルイベントは、一連のアクションが完了した後にのみ記録されます。たとえば、OU でコントロールを有効にすると、AWSControl Tower はリクエストを実装する一連のサブステップを起動します。この一連のサブステップ全体の最終結果が、ライフサイクルイベントの状態としてログに記録されます。

- 基となるサブステップのすべてが正常に完了すると、ライフサイクルイベントの状態は [Succeeded] (成功) として記録されます。
- 基となるサブステップのいずれかが正常に完了しなかった場合、ライフサイクルイベントの状態は [Failed] (失敗) として記録されます。

各ライフサイクルイベントには、AWSControl Tower アクションが開始された日時を示すログに記録されたタイムスタンプと、ライフサイクルイベントが完了した日時を示す別のタイムスタンプが含まれ、成功または失敗を示します。

Control Tower でのライフサイクルイベントの表示

Control AWS Tower ダッシュボードのアクティビティページからライフサイクルイベントを表示できます。

- [Activities] (アクティビティ) ページに移動するには、左側のナビゲーションペインから [Activities] (アクティビティ) を選択します。
- 特定のイベントの詳細を表示するには、イベントを選択し、右上にある [View details] (詳細を表示) ボタンを選択します。

AWS Control Tower ライフサイクルイベントをワークフローに統合する方法の詳細については、このブログ記事「ライフサイクルイベントを使用して AWS Control Tower アクションを追跡し、自動ワークフローをトリガーする」を参照してください。

CreateManagedAccount および UpdateManagedAccount ライフサイクルイベントの予想される動作

Control Tower でアカウントを作成または登録すると、これらの 2 AWS つのアクションは同じ内部を呼び出しますAPI。プロセス中にエラーが発生する場合、通常、エラーはアカウントが作成された後に完全にプロビジョニングされていない場合に発生します。エラー後にアカウントの作成を再試行する場合、またはプロビジョニング済み製品を更新しようとすると、AWSControl Tower はアカウントがすでに存在することを確認します。

アカウントが存在するため、AWSControl Tower は再試行リクエストの最後にUpdateManagedAccountライフサイクルイベントではなくCreateManagedAccountライフサイクルイベントを記録します。エラーが原因で、別の CreateManagedAccount イベントが表示されると予想されるかもしれませんが、UpdateManagedAccount ライフサイクルイベントが期待される望ましい動作です。

自動メソッドを使用してアカウントを作成または AWS Control Tower に登録する場合は、UpdateManagedAccountライフサイクルイベントだけでなく、CreateManagedAccountライフサイクルイベントも検索するように Lambda 関数をプログラムします。

ライフサイクルイベント名

各ライフサイクルイベントは、発信元 AWS Control Tower アクションに対応するように名前が付けられます。このアクションも によって記録されますAWS CloudTrail。したがって、例えば、AWSControl Tower イベントによって発生したライフサイクルCreateManagedAccount CloudTrail イベントには という名前が付けられますCreateManagedAccount。

次の一覧に示す名前は、それぞれが JSON 形式でログに記録された詳細の例にリンクされています。これらの例に示されている追加の詳細は、Amazon CloudWatch イベントログから取得されます。

JSON はコメントをサポートしていませんが、例には説明の目的でいくつかのコメントを追加しています。コメントは先頭に「//」を付けて、例の右側に表示しています。

これらの例では、一部のアカウント名と組織名が隠されています。accountId は常に 12 桁の数字であり、例では「xxxxxxxxxxx」に置き換えられています。organizationalUnitID は、文字と数字の一意の文字列です。例では、その形式を保持しています。

- CreateManagedAccount: ログには、Account Factory を使用して新しいアカウントを作成およびプロビジョニングするすべてのアクションを AWS Control Tower が正常に完了したかどうかが記録されます。
- UpdateManagedAccount: ログには、以前に Account Factory を使用して作成したアカウントに関連付けられているプロビジョニング済み製品を更新するすべてのアクションを AWS Control Tower が正常に完了したかどうかが記録されます。
- EnableGuardrail: ログには、AWSControl Tower によって作成された OU でコントロールを有効にするためのすべてのアクションを AWS Control Tower が正常に完了したかどうかが記録されます。
- DisableGuardrail: Control Tower がAWS、Control Tower によって作成された OU のコントロールを無効にするすべてのアクションを正常に完了したかどうかを記録しますAWS。
- SetupLandingZone: AWS Control Tower がランディングゾーンをセットアップするためのすべてのアクションを正常に完了したかどうかがログに記録されます。
- UpdateLandingZone: AWS Control Tower が既存のランディングゾーンを更新するためのすべてのアクションを正常に完了したかどうかがログに記録されます。
- RegisterOrganizationalUnit: AWS Control Tower が OU でガバナンス機能を有効にするためのすべてのアクションを正常に完了したかどうかがログに記録されます。
- DeregisterOrganizationalUnit: AWS Control Tower が OU のガバナンス機能を無効にするすべてのアクションを正常に完了したかどうかがログに記録されます。
- PrecheckOrganizationalUnit: ログには、ガバナンスの拡張オペレーションが正常に完了するのを妨げるリソースが AWS Control Tower によって検出されたかどうかが記録されます。

以下のセクションでは、AWSControl Tower ライフサイクルイベントのリストと、ライフサイクルイベントのタイプごとにログに記録される詳細の例を示します。

CreateManagedAccount

このライフサイクルイベントは、AWSControl Tower が Account Factory を使用して新しいアカウントを正常に作成およびプロビジョニングしたかどうかを記録します。このイベントは Control Tower AWS `CreateManagedAccount` CloudTrail イベントに対応します。ライフサイクルイベントログには、新しく作成されたアカウントの `accountName` と `accountId`、アカウントの配置先である OU の `organizationalUnitName` と `organizationalUnitId` が含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
```

```
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

UpdateManagedAccount

このライフサイクルイベントは、以前に Account Factory を使用して作成されたアカウントに関連付けられたプロビジョニング済み製品を AWS Control Tower が正常に更新したかどうかを記録します。このイベントは Control Tower AWS UpdateManagedAccount CloudTrailイベントに対応します。ライフサイクルイベントログには、関連するアカウントの accountName と accountId、更新されたアカウントの配置先である OU の organizationalUnitName と organizationalUnitId が含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
```

```
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

EnableGuardrail

このライフサイクルイベントは、AWSControl Tower が管理している OU で AWS Control Tower が正常にコントロールを有効にしたかどうかを記録します。このイベントは Control Tower AWS EnableGuardrail CloudTrail イベントに対応します。ライフサイクルイベントログには、コントロールの guardrailId と guardrailBehavior、コントロールを有効にした OU の organizationalUnitName と organizationalUnitId が含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                    // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                             // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
```

```
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
        }
    }
}
```

DisableGuardrail

このライフサイクルイベントは、AWSControl Tower が管理している OU のコントロールを AWS Control Tower が正常に無効にしたかどうかを記録します。このイベントは Control Tower AWS DisableGuardrail CloudTrail イベントに対応します。ライフサイクルイベントログには、コントロールの guardrailId と guardrailBehavior、コントロールを無効にした OU の organizationalUnitName と organizationalUnitId が含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
```

```
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
               }
            }
        }
    }
```

SetupLandingZone

このライフサイクルイベントは、AWSControl Tower がランディングゾーンを正常にセットアップしたかどうかを記録します。このイベントは Control Tower AWS SetupLandingZone CloudTrail イベントに対応します。ライフサイクルイベントログにはrootOrganizationalId、AWSControl Tower が管理アカウントから作成する組織の ID である が含まれます。ログエントリには、AWSControl Tower がランディングゾーンを設定するときに作成される、各organizationalUnitIdの organizationalUnitNameと 、およびaccountId各アカウントのOUsaccountNameと も含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management-account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "SetupLandingZone",
        "awsRegion": "us-east-1",                                // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                        // This value is
 generated by CloudTrail.
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
```

```
            "setupLandingZoneStatus": {
                "state": "SUCCEEDED",                                  // Status of entire
 lifecycle operation.
                "message": "AWS Control Tower successfully set up a new landing zone.",

                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                              // Use a list.
                  {
                    "organizationalUnitName": "Security",              // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",            // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                  },
                ],
               "accounts": [                                           // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

UpdateLandingZone

このライフサイクルイベントは、AWSControl Tower が既存のランディングゾーンを正常に更新したかどうかを記録します。このイベントは Control Tower AWS UpdateLandingZone CloudTrail イベントに対応します。ライフサイクルイベントログには`rootOrganizationalId`、AWSControl Tower によって管理される (更新された) 組織の ID である が含まれます。ログエントリに

は、AWSControl Tower organizationalUnitIdが最初にランディングゾーンをセットアップしたときに以前に作成された各 accountIdの organizationalUnitNameと 、および各アカウントのOUsaccountNameと も含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateLandingZone",
        "awsRegion": "us-east-1",                                // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                        // This value is
 generated by CloudTrail.

        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateLandingZoneStatus": {
                "state": "SUCCEEDED",                            // Status of entire
 operation.
                "message": "AWS Control Tower successfully updated a landing zone.",
```

```
                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                          // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",            // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                  },
                ],
               "accounts": [                                        // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

RegisterOrganizationalUnit

このライフサイクルイベントは、AWSControl Tower が OU でガバナンス機能を有効にしたかどうかを記録します。このイベントは Control Tower AWS `RegisterOrganizationalUnit` CloudTrail イベントに対応します。ライフサイクルイベントログには、AWSControl Tower がガバナンスを引き受けた OU `organizationalUnitId`の `organizationalUnitName`と が含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
```

```
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

このライフサイクルイベントは、AWSControl Tower が OU のガバナンス機能を正常に無効にしたかどうかを記録します。このイベントは Control Tower AWS `DeregisterOrganizationalUnit` CloudTrail イベントに対応します。ライフサイクルイベントログには、AWSControl Tower がガバナ

ンス機能を無効にした OU organizationalUnitIdの organizationalUnitNameと が含まれます。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully deregistered an
 organizational unit, and enabled mandatory guardrails on the new organizational
 unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                   // Foundational
 OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"          // Foundational
 OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
```

```
            }
        }
    }
```

PrecheckOrganizationalUnit

このライフサイクルイベントは、AWSControl Tower が OU で事前チェックを正常に実行したかどうかを記録します。このイベントは Control Tower AWS PrecheckOrganizationalUnit CloudTrail イベントに対応します。ライフサイクルイベントログにはId、OU 登録プロセス中に AWS Control Tower が事前チェックを実行した各リソースの 、、Nameおよび failedPrechecks値のフィールドが含まれます。

イベントログには、accountName、accountId、および failedPrechecks フィールドを含む、事前チェックが実行されたネストされたアカウントに関する情報も含まれます。

failedPrechecks の値が空の場合、そのリソースのすべての事前チェックが正常に終了したことを意味します。

- このイベントは、事前チェックに失敗した場合にのみ発生します。
- 空の OU を登録している場合、このイベントは発生しません。

イベントの例:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
```

```
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
pre-check failures. Go to the OU details page to download a list of failed pre-checks
for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
```

```
  },
  "eventCategory": "Management"
}
```

での AWS ユーザー通知の使用 AWS Control Tower

AWS ユーザー通知を使用すると、 AWS Control Tower イベントの通知を受ける配信チャネルを設定できます。指定したルールにイベントが一致した場合に通知を受信します。イベントの通知は、Eメール、チャットアプリケーションでの Amazon Q Developer のチャット通知、AWS コンソールモバイルアプリケーションのプッシュ通知など、複数のチャネルで受け取ることができます。「コンソール通知センター」で通知を確認することもできます。

AWS ユーザー通知は集約をサポートしているため、特定のイベント中に受け取る通知の数を減らすことができます。通知は、コンソール通知センターで表示することもできます。

の代わりに AWS ユーザー通知を通じて通知をサブスクライブする利点 EventBridge は次のとおりです。

- わかりやすいユーザーインターフェイス (UI)。
- グローバルナビゲーションバーのベル/通知エリアにある AWS コンソールとの統合。
- E メール通知をネイティブにサポートしているため、Amazon をセットアップする必要はありませんSNS。
- 最も重要なのは、 AWS ユーザー通知専用のモバイルプッシュ通知のサポートです。

例えば、Security Hub が緊急かつ重大度が高い結果を出した場合に、ある種類の通知を受け取りたいとします。通知サブスクリプションを設定JSONするための のコードスニペットは次のようになります。

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
```

```
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

イベントのフィルタリング

- AWS ユーザー通知コンソールで使用できるフィルターを使用して、サービスと名前でイベントをフィルタリングできます。
- JSON コードから独自のフィルターを作成する場合は、特定のプロパティでイベントを EventBridge フィルタリングできます。

AWS Control Tower イベントの例

の一般的なイベントの例を次に示します AWS Control Tower。

- これは EventBridge イベントです。
- AWS ユーザー通知を使用して EventBridge イベント (このイベントなど) をサブスクライブできます。

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
```

```
        "eventName": "<event name>", // one of the 9 event names in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

AWS Backup と AWS Control Tower

AWS Backup は、 AWS リソースを自動的にバックアップするための計画を作成できるサービスです。AWS Control Tower リソースのバックアップを設定するには、次の 4 つの主要なステップに従う必要があります。

1. ランディングゾーン AWS Backup で を有効にします。これは、AWS Control Tower コンソールのランディングゾーン設定ページで実行できます。有効にすると AWS Backup、リソースは複数の アカウントに作成されます。詳細については、「用に作成されたリソース AWS Backup」を参照してください。
2. AWS Backup コンソールで AWS Control Tower のバックアップにオプトインします。詳細については、「 デベロッパーガイド」の「サポートされている のサービスの使用」を参照してください。 AWS Backup
3. 含める個々の OUs AWS Backup で を有効にします。このタスクは、ランディングゾーンレベルで を有効に AWS Backup した後、 コンソールの OU の詳細ページで実行できます。OU AWS Backup で を有効にすると、その OU のアカウントはローカル AWS Backup ボールトを受け取ります。
4. 選択したリソースにタグを付けてバックアップに含めます。タグは、そのリソースのバックアップの頻度を示します。バックアッププランは、各リソースのリソースタグで指定されたスケジュールに従います。

詳細については、「 AWS Backup デベロッパーガイド」を参照してください。AWS Control Tower で AWS バックアップを設定する場合、コストは発生しません。コストが発生します AWS Backup。料金については、「AWS Backup の料金」を参照してください。

AWS Control Tower が AWS Control Tower ランディングゾーンで作成する AWS Backup リソースの詳細については、「」を参照してください。 用に作成されたリソース AWS Backup

> **Note**
>
> AWS Control Tower は、AWS Control Tower AWS Backup サービスで有効にすることなく、サービスを通じて AWS Control Tower リソースのバックアッププランを直接設定することはできません。

前提条件

AWS Control Tower リソース AWS Backup 用に を設定する前に、既存の AWS Organizations 組織が必要です。AWS Control Tower ランディングゾーンを既に設定している場合は、既存の組織として機能します。

AWS Control Tower に登録されていない他の 2 つの AWS アカウントを割り当てるか、作成する必要があります。これらのアカウントは、中央バックアップアカウントおよびバックアップ管理者アカウントになります。これらのアカウントにそれらの名前を付けます。

また、特に AWS Backup 用のマルチリージョン AWS Key Management Service (KMS) キーを選択または作成する必要があります。

前提条件の定義

- 中央バックアップアカウント - 中央バックアップアカウントは、AWS Control Tower バックアップボールトとバックアップを保存します。このボールトは、このアカウント内の AWS Control Tower AWS リージョン が管理するすべての に作成されます。クロスアカウントコピーは、アカウントが侵害され、データの復元が必要な場合に備えて、このアカウントに保存されます。
- バックアップ管理者アカウント - バックアップ管理者アカウントは、AWS Control Tower の AWS Backup サービスの委任管理者アカウントです。Backup Audit Manager (BAM) レポートプランが保存されます。このアカウントは、復元ジョブやコピージョブなど、すべてのバックアップモニタリングデータを集約します。データは Amazon S3 バケットに保存されます。詳細については、「AWS Backup デベロッパーガイド」の「 AWS Backup コンソールを使用したレポートプランの作成」を参照してください。
- マルチリージョン AWS KMS キーのポリシー要件

  AWS KMS キーにはキーポリシーが必要です。組織の管理アカウントに関連付けられたルート IAM アクセス許可を持つプリンシパル (ユーザーとロール) へのアクセスを制限する、次のようなキーポリシーを検討してください。

```
{
    "Version": "2012-10-17",
    "Id": "KMS key policy",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::MANAGEMENT-ACCOUNT-ID:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the KMS key for organization",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:Encrypt",
                "kms:ReEncrypt*",
                "kms:GetKeyPolicy",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "ORGANIZATION-ID"
                }
            }
        }
    ]
}
```

> **Note**
>
> マルチリージョン AWS KMS キーは、AWS Control Tower で管理する AWS リージョン すべての に対してレプリケートする必要があります。

バックアップを有効にする

ランディングゾーンのセットアップ中またはランディングゾーンの更新時に、AWS Control Tower に登録されているアカウントのリソースのバックアップを有効にできます。

として前提条件、次の項目を指定する必要があります。

- AWS Backup 管理者アカウント AWS アカウント として機能する 。
- AWS Backup 中央バックアップアカウント AWS アカウント として機能する 。
- クロスアカウントバックアップ用に管理するマルチリージョン AWS KMS キー

バックアップを有効にする方法

有効化プロセスには 2 つの主な部分があります。まずランディングゾーンのバックアップを有効にし、次にバックアップを必要とする登録済み OU ごとにバックアップを有効にします。

第 1 部: ランディングゾーンのバックアップを設定する

コンソール： ランディングゾーン設定ページの AWS Control Tower コンソールでランディングゾーンのバックアップを設定できます。このオプションは、最初のランディングゾーンセットアップオペレーション中に表示され、ランディングゾーンの更新で後で再確認できます。

API: AWS Control Tower ランディングゾーンがすでにあるUpdateLandingZone場合は APIs を呼び出し、AWS Control Tower を初めて設定する場合は CreateLandingZone API を呼び出してバックアップを有効にできます。（ヒント: その後、 EnableBaseline API を呼び出して、必要な各 OU のバックアップを確立します）。

AWS Control Tower コンソール外

ランディングゾーンのバックアップの有効化には、AWS Control Tower コンソールの外部にあるステップが含まれます。リソースを確認するには、 AWS Backup コンソールに移動する必要があります。

オプトインリソースタイプを確認するか、追加のリソースタイプにオプトインするには

1. で AWS Backup コンソールを開きますhttps://console.aws.amazon.com/backup。
2. ナビゲーションペインで [設定] を選択します。
3. [サービスのオプトイン] ページで、[リソースを設定] を選択します。
4. トグルスイッチを使用して、含めるサービスを有効または無効にします AWS Backup。RDS、EC2、DDB など、バックアップするリソースが、AWS Control Tower 環境の一部であるかどうかにかかわらず選択されていることを確認します。

詳細については、「 による サービスの管理にオプトイン AWS Backupする」を参照してください。

> **新しいリソースタイプの考慮事項**
>
> AWS Backup を使用して AWS サービスのリソースのデータ保護を管理する前に、前の手順を実行し、 AWS Backup そのサービスの にオプトインする必要があります。また、AWS Backup サービスが今後追加の サービスとそのリソースタイプのサポートを追加するため、AWS Control Tower でそのリソースタイプをバックアップ AWS Backup する前に、この手順を繰り返し、追加のリソースタイプごとに でオプトインする必要があります。サポートされていないリソースタイプにタグを付けると、バックアップが失敗する可能性があります。

ランディングゾーンのバックアップをアクティブ化すると、AWS Control Tower は、中央バックアップアカウントとバックアップ管理者アカウントとして指定した 2 つのアカウントをそれぞれ確立します。AWS Control Tower は、これらのアカウントと他のアカウントにリソースを作成します。

> **Important**
>
> AWS Control Tower 監査アカウントとログアーカイブアカウントのバックアップを有効にするには、 `EnableBaseline` API を呼び出してセキュリティ OU のバックアップを設定する必要があります。そのようにすることをお勧めします。

計画と保持の推奨銀行は次のとおりです。

- 時間単位のバックアップ = ローカルボールトで 2 週間の保持期間、中央バックアップボールトではコピーなし
- 日次バックアップ = ローカルボールトでの 2 週間の保持、中央バックアップボールトでの 1 か月の保持
- 週次バックアップ = ローカルボールトでの 1 か月の保持、中央ボールトでの 3 か月の保持
- 毎月のバックアップ = ローカルボールトでの 3 か月の保持、中央バックアップボールトでの 3 か月の保持

バックアッププランの作成方法については、「AWS Backup コンソールを使用したレポートプランの作成」を参照してください。

次のパート: OUs でバックアップを有効にする

ランディングゾーン設定 AWS Backup で を有効にしたら、追加のステップを実行して、バックアップする特定の OUs でバックアップを有効にする必要があります。ランディングゾーン AWS Backup で を有効にしている場合は、コンソールの OU の詳細ページにセクションが表示され、OU のバックアップを有効にするを選択できます。ランディングゾーンレベルでバックアップが有効になっていない場合、このセクションは OU の詳細ページに表示されません。

OU BackupBaselineで を有効にするには、その OU で がすでにAWSControlTowerBaseline有効になっている必要があります。各 OU に登録されたアカウントでは、AWSControlTowerBaselineが有効になっています。

選択したアカウントと OUs、AWS Control Tower は追加のリソースを設定します。

- ローカルバックアップボールト

  AWS Control Tower は、 アカウントにローカルバックアップボールトを作成し、4 つのバックアッププランのタイプをボールトにアタッチします。AWS Control Tower で作成されたバックアッププランには、プレフィックスが付けられます。

  ```
  BackupPlanTags:
          aws-control-tower: 'managed-by-control-tower'
  ```

- バックアッププランには、時間単位、日単位、週単位、月単位の 4 種類があります。

  各プランは、タグベースのリソース割り当てに関連付けられます。例えば、aws-controltower-backuphourly でタグ付けされたすべてのリソース: true は時間単位のバックアッププランで保護されます。

- アカウントのローカルバックアップロール

  AWS Control Tower は、バックアップに使用される IAM ロールを作成します。ロールには 4 つの特定のアクセス許可が必要です。

  ```
  "backup:UpdateGlobalSettings","organizations:RegisterDelegatedAdministrator","organizations:E
  ```

  ロールには、 のサービスプリンシパルとの信頼関係があります AWS Backup 。ロールの名前はでaws-controltower-backup-role、次の管理アクセス許可がアタッチされています。

  - AWSBackupServiceRolePolicyForBackup
  - AWSBackupServiceRolePolicyForRestores

- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore

バックアップ用のリソースのタグ付け

AWS Control Tower でバックアップを設定するプロセスの一環として、バックアッププランに含めるリソースにタグを付けます。タグはバックアップの頻度を指定します。これらは可能なタグです。

- `aws-controltower-backuphourly : true`
- `aws-controltower-backupdaily: true`
- `aws-controltower-backupweekly: true`
- `aws-controltower-backupmonthly: true`

考慮事項

- AWS Backup が OU でアクティブになると、AWS Control Tower コンソールの OU の詳細ページのステータスフィールドに Enabled の値が表示されます。Status フィールドの他の可能な値には、Not enabled、In progress、Failed などがあります。失敗のステータスが表示された場合は、OU の再登録を選択して AWS Backup 設定を OU に再適用します。
- OU で AWS Backup を有効にしている場合、OU に含まれる Account Factory を通じてプロビジョニングされた新しいアカウント AWS Backup。

バックアップをオフにする

ランディングゾーンのセットアップ中またはランディングゾーンの更新時に、AWS Control Tower に登録されているアカウントのリソースのバックアップをオフにできます。

バックアップを無効にするには、主に 2 つのステップが必要です。まず、バックアップが有効になっている各 OU の AWS Backup ベースラインをオフにしてから、ランディングゾーンのバックアップをオフにします。

最初のステップ: OUs でバックアップを無効にする

が有効になっている場合 AWS Backup は、 AWS Backup ランディングゾーンをオフにする前に、すべての OUs から AWS Backup ベースラインを無効にする必要があります。

OU の AWS Backup ベースラインを無効にするには、 DisableBaseline API を呼び出します。ネストされた OUs はこのステータスを継承するため、AWS Backup ベースラインベースラインも無効になります。

コマンドの例:

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

AWS Backup ベースラインを無効にすると、AWS Control Tower は次のリソースをクリーンアップします。

- に関連するすべてのスタックセット AWS Backup
- に関連するすべてのコントロール AWS Backup

> **Note**
>
> ローカルボールトの保持ポリシーは に設定されているため、スタックセットが削除されてもローカルボールトは保持されますRetain。データは保持されます。

次のステップ: ランディングゾーン AWS Backup の をオフにする

OUs へのバックアップをオフにして前提条件を満たしたら、AWS Control Tower コンソールからバックアップをオフにするには、ランディングゾーン設定ページに移動します。バックアップを無効にする を選択します。

オフにすると AWS Backup、AWS Control Tower は次のリソースを変更します。

- に関連するすべてのスタックセットを削除します。 AWS Backup
- セキュリティ OU AWS Backup の に関連するすべてのコントロールを無効にします
- 管理のために AWS Backup 委任管理者アカウントを登録解除します
- 管理者アカウントと中央バックアップアカウントから AWS Control Tower ガバナンス (CloudTrail AWS Configなど) AWS Backup を削除します。
- AWS Control Tower AWS Backup は、データを含むボールトと Amazon S3 バケットリソースを保持します。

バックアップを無効にすると、新しいバックアップは作成されませんが、既存のバックアップは削除されません。

移動したアカウントでバックアップを有効にする

AWS Backup が有効になっている AWS Control Tower OU にアカウントを移動し、そのアカウントが AWS Control Tower に登録されていない場合、バックアッププランは自動的にアカウントに適用されません。

コンソール： AWS Control Tower コンソールから個々のアカウント AWS Backup に対して を有効にするには、アカウントの詳細ページでアカウントの更新を選択するか、OU の詳細ページで OU を再登録して複数のアカウントを同時に更新できます。

API: API から、バックアップベースラインが有効になっている OU にアカウントを移動する場合、その OU で `ResetEnabledBaseline` API を呼び出し、OU の`EnabledBaseline`リソースをターゲットとして指定して、OU からの継承によってアカウントのバックアップをトリガーできます。

コマンドの例:

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier
 arn:aws:controltower:REGION:NAMESPACE:enabledbaseline/XOSDORW8HDB5ZNWEE --region us-
east-1
```

レスポンスの例:

```
{
        "operationIdentifier": "0bbdb587-c849-4152-95c6-7afa7664ee71"
}
```

AWS Control Tower でのバックアップドリフト

ドリフトは AWS Control Tower AWS Backup の設定では報告されません。AWS Control Tower でのドリフトの詳細については、「AWS Control Tower でのドリフトの検出と解決」を参照してください。

AWS Backup プランを削除または変更すると、プランがドリフト状態になる可能性があります。回避すべき変更をいくつか示します。

- Backup 管理者アカウントをセキュリティ OU から移動しないでください。

- セキュリティ OU から中央バックアップアカウントを移動しないでください。
- Backup 管理者アカウントを組織から削除しないでください。
- 組織から中央バックアップアカウントを削除しないでください。
- セキュリティ OU に適用される AWS Backup SCP をデタッチ、アタッチ、または更新しないでください。
- 他の OUs に適用されている AWS Backup SCP をデタッチ、アタッチ、または更新しないでください。
- Backup 管理者アカウントの アクセス許可を削除しないでください AWS Backup。
- クロスアカウントバックアップ設定を更新して、クロスアカウントバックアップをオフにしないでください。クロスアカウントバックアップの詳細については、 AWS Backup API リファレンス`UpdateGlobalSettings`の「」を参照してください。
- AWS KMS キーを削除しないでください。
- 設定後に AWS KMS キーポリシーを変更しないでください。
- サービスの信頼されたアクセスを無効にしないでください AWS Backup。

> **Note**
>
> ドリフトは、AWS Control Tower の AWS Backup リソースを保護する SCP ベースのコントロールのステータスに関して報告されます。

用に作成されたリソース AWS Backup

このページの表は、有効にしたときに AWS Control Tower アカウントで作成されたリソースを示しています AWS Backup。

次の表は、ランディングゾーン組織 AWS Backup に対して を有効にしたときに AWS Control Tower が AWS Control Tower Central Backup アカウントで作成するリソースを示しています。

説明	中央バックアップアカウントのリソース
どの OU にアカウントが含まれていますか？	セキュリティ OU
リソースを作成したアクション	ランディングゾーンの作成または更新

説明	中央バックアップアカウントのリソース
どのようなリソースが作成されますか？	中央バックアップボールト —aws-controltower-central-backupvault-*
どのリージョンが含まれていますか？	すべての管理対象リージョン
これらのリソースに関連するコントロール	CT.BACKUP.PV.3

次の表は、ランディングゾーン組織 AWS Backup に対して を有効にするときに AWS Control Tower が AWS Control Tower Backup 管理者アカウントで作成するリソースを示しています。

説明	Backup 管理者アカウントのリソース: これは の委任管理者アカウントです。 AWS Backup
どの OU にアカウントが含まれていますか？	セキュリティ OU
リソースを作成したアクション	ランディングゾーンの作成または更新
どのようなリソースが作成されますか？	Backup Audit Manager (BAM) • aws_controltower_copy_report • aws_controltower_backup_report • aws_controltower_restore_report BAM ログを保存するための Amazon S3 バケット —aws-controltower-backup-reports- *{accountId}* -* Amazon S3 アクセスログ記録バケット -aws-controltower-backup-reports-log- *{accountId}* -*
どのリージョンが含まれていますか？	ホームリージョン
これらのリソースに関連するコントロールは何ですか？	• CT.BACKUP.PV.2

説明	Backup 管理者アカウントのリソース: これは の委任管理者アカウントです。 AWS Backup
	• CT.S3.PV.1 • CT.S3.PV.1

次の表は、Security OU AWS AWS Backup に対して を有効にしたときに AWS Control Tower 監査アカウントと AWS Control Tower Log Archive アカウントで Control Tower が作成するリソースを示しています。

説明	監査アカウントとログアーカイブアカウントのリソース
どの OU にアカウントが含まれていますか？	セキュリティ OU
リソースを作成したアクション	の有効化 BackupBaseline

どのようなリソースが作成されますか？	• ローカルバックアップボールト —aws-controltower-local-backupvault-*
	• ローカルバックアップロール -aws-controltower-BackupRole
	• 4 つのローカルバックアッププラン (時間単位、週単位、月単位、日単位)
	  • aws-controltower-hourly-backup-plan
	  • aws-controltower-daily-backup-plan
	  • aws-controltower-weekly-backup-plan
	  • aws-controltower-monthly-backup-plan
	• IAM ロール -aws-controltower-backup-role

説明	監査アカウントとログアーカイブアカウントのリソース
どのリージョンが含まれていますか？	すべての管理対象リージョン
これらのリソースに関連するコントロール	• CT.BACKUP.PV.3 • CT.IAM.PV.1 • CT.BACKUP.PV.3 • CT.BACKUP.PV.1

> **Note**
>
> BackupBaseline をセキュリティ OU に適用すると、監査アカウントとログアーカイブアカウントだけでなく、その OU 内のすべてのメンバーアカウントが AWS Backup リソースを受け取ります。

次の表は、ターゲット OU で を有効にするときに AWS Control Tower が AWS Control Tower OU メンバーアカウント AWS Backup で作成するリソースを示しています。

説明	他の のメンバーアカウントのリソース OUs
どの OU にアカウントが含まれていますか？	セキュリティ OU 以外の OU
リソースを作成したアクション	の有効化 BackupBaseline
どのようなリソースが作成されますか？	• ローカルバックアップボールト —aws-controltower-local-backupvault-* • ローカルバックアップロール -aws-controltower-BackupRole • 4 つのローカルバックアッププラン (時間単位、週単位、月単位、日単位) • aws-controltower-hourly-backup-plan

説明	他の のメンバーアカウントのリソース OUs
	• aws-controltower-daily-backup-plan • aws-controltower-weekly-backup-plan • aws-controltower-monthly-backup-plan • IAM ロール -aws-controltower-backup-role
どのリージョンが含まれていますか？	すべての管理対象リージョン
これらのリソースに関連するコントロールは何ですか？	• CT.BACKUP.PV.3 • CT.IAM.PV.1 • CT.BACKUP.PV.3 • CT.BACKUP.PV.1

AWS バックアップのコントロール

AWS Control Tower ランディングゾーン AWS Backup で を有効にすると、一部の予防コントロールが環境でアクティブ化されます。これらのコントロールは、AWS Control Tower を操作する AWS Backup ために必要なリソースを保護します。ランディングゾーンで が有効になっていない場合 AWS Backup 、これらのコントロールを有効にすることはできません。

詳細については、「 のコントロール」を参照してください AWS Backup。

チュートリアル

この章には、AWSControl Tower の使用に役立つチュートリアルの手順が含まれています。

トピック

チュートリアル: から AWS Control Tower ALZに移動する

多くの AWS お客様は、AWSランディングゾーンソリューション (ALZ) を採用して、安全で準拠したマルチアカウント AWS 環境をセットアップしています。ランディングゾーンを管理する負担を軽減するために、 は Control Tower というAWSマネージドサービス AWS を作成しました。

には追加の機能は予定されていませんALZ。長期サポートのみとなります。したがって、 から AWS Control Tower サービスに移行することをお勧めしますALZ。この章でリンクされているブログでは、その移行に関するさまざまな考慮事項について説明し、 から AWS Control Tower ALZへの移行を成功させる計画を立てる方法について説明します。

ブログ: AWS ランディングゾーンソリューションを AWS Control Tower に移行する

AWS 規範ガイダンスでは、 から ALZ AWS Control Tower への移行手順など、より広範なドキュメントを提供しています。基本的に、いくつかの前提条件に基づいてALZ、 を実行している既存の組織で AWS Control Tower ガバナンスを有効にします。詳細については、AWS 「ランディングゾーンから AWS Control Tower への移行」を参照してください。

チュートリアル: Service Catalog による AWS Control Tower でのアカウントプロビジョニングの自動化 APIs

AWS Control Tower は、 など、他のいくつかの AWS サービスと統合されています AWS Service Catalog。を使用してAPIs、AWSControl Tower でメンバーアカウントを作成およびプロビジョニングできます。

このビデオでは、 を呼び出して、自動バッチ方式でアカウントをプロビジョニングする方法を示します AWS Service Catalog APIs。プロビジョニングでは、 AWS コマンドラインインターフェイス (CLI) `ProvisionProduct`APIから を呼び出し、セットアップする各アカウントのパラメータを含むJSONファイルを指定します。この動画では、AWS Cloud9 開発環境をインストールして使用し、この作業を実行する方法を説明します。 AWS Cloud9 の代わりに AWS Cloudshell を使用する場合、CLIコマンドは同じになります。

> **Note**
>
> また、各アカウントの `UpdateProvisionedProduct`APIの を呼び出すことで、アカウントの更新を自動化 AWS Service Catalog するためにこのアプローチを適応させることもできます。アカウントを更新するスクリプトを 1 つずつ作成できます。

まったく異なる自動化方法として、Terraform に精通している場合は、AWSControl Tower Account Factory for Terraform (AFT) を使用してアカウントをプロビジョニングできます。

オートメーションの管理ロールのサンプル

次に示すのは、管理アカウントでオートメーションの管理ロールを設定するために使用できるサンプルテンプレートです。このロールは、ターゲットアカウントの管理者アクセスを使用してオートメーションを実行できるように、管理アカウントで設定します。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
```

```
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

オートメーションの実行ロールのサンプル

次に示すのは、オートメーションの実行ロールを設定するために使用できるサンプルテンプレートです。このロールは、ターゲットアカウントで設定します。

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400
```

```
Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

これらのロールを設定したら、 AWS Service Catalog APIsを呼び出して自動タスクを実行します。CLI コマンドはビデオで示されています。

Service Catalog のプロビジョニング入力の例 API

を使用して AWS Control Tower アカウントをプロビジョニング`ProvisionProduct`APIする場合に Service Catalog に渡すことができる入力の例APIを次に示します。

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
      key: "AccountName",
      value: "ABC"
    },
```

```
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

詳細については、APIService Catalog のリファレンスを参照してください。

> **Note**
>
> ManagedOrganizationalUnit の値の入力文字列の形式が OU_NAME から OU_NAME (OU_ID) に変更されていることに注意してください。続く動画では、この変更については言及していません。

動画チュートリアル

このビデオ (6:58) では、AWSControl Tower でのアカウントのデプロイを自動化する方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

AWS Control Tower での自動アカウントプロビジョニングのビデオチュートリアル。

チュートリアル: なしで AWS Control Tower を設定する VPC

このトピックでは、 なしで AWS Control Tower アカウントを設定する方法について説明します VPC。

ワークロードに が必要ない場合はVPC、次の操作を実行できます。

- AWS Control Tower 仮想プライベートクラウド () を削除できますVPC。これはVPC、ランディングゾーンをセットアップしたときに作成されました。
- Account Factory 設定を変更して、関連付けられた なしで新しい AWS Control Tower アカウントを作成することができますVPC。

> **Important**
>
> VPC インターネットアクセス設定を有効にして Account Factory アカウントをプロビジョニングすると、その Account Factory 設定は、お客様が管理する Amazon VPCインスタンスのインターネットアクセスの禁止コントロールを上書きします。新しくプロビジョニングされたアカウントのインターネットアクセスを有効にしないようにするには、Account Factory で設定を変更する必要があります。

AWS Control Tower を削除する VPC

AWS Control Tower の外部では、すべての AWS お客様にデフォルトの がありVPC、 の Amazon Virtual Private Cloud (Amazon VPC) コンソールで表示できますhttps://console.aws.amazon.com/vpc/。デフォルトの は認識されます。名前の末尾には常に単語 (デフォルト) が含まれているVPCためです。

AWS Control Tower ランディングゾーンを設定すると、AWSControl Tower は AWS デフォルトを削除VPCし、新しい AWS Control Tower のデフォルト を作成しますVPC。新しい VPCは Control Tower AWS 管理アカウントに関連付けられています。このトピックでは、新しい を Control Tower VPCVPCと呼びます。

Amazon VPCコンソールVPCで AWS Control Tower を表示すると、名前の末尾に単語 (デフォルト) は表示されません。複数の がある場合はVPC、割り当てられたCIDR範囲を使用して正しい AWS Control Tower を識別する必要がありますVPC。

AWS Control Tower は削除できますがVPC、後で AWS Control Tower VPCで が必要な場合は、自分で作成する必要があります。

AWS Control Tower を削除するには VPC

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. Service Catalog オプションを検索**VPC**またはVPC選択します。ダッシュボードが表示されますVPC。
3. 左側のメニューから、 VPCsを選択します。その後、すべての のリストが表示されますVPCs。
4. AWS Control Tower をCIDR範囲VPC別に識別します。
5. を削除するにはVPC、アクション を選択し、 の削除 VPCを選択します。

Control Tower 管理アカウントのすべてのリージョンに AWS （ デフォルト ） AWS がVPC既に存在します。セキュリティのベストプラクティスに従うには、AWSControl Tower を削除する場合はVPC、管理アカウントVPCに関連付けられた AWS デフォルトをすべての AWS リージョンから削除することをお勧めします。したがって、管理アカウントをセキュリティで保護するには、各リージョンVPCからデフォルト を削除するとともに、Control Tower ホームリージョンで Control Tower によってVPC作成された AWS を削除します。

を使用せずに AWS Control Tower でアカウントを作成する VPC

エンドユーザーワークロードに が必要ない場合はVPCs、この方法を使用して、 によって自動的にVPCs作成されていないエンド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。に関連付けられた 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VPC、設定を再度変更VPCするまで、すべての新しいアカウントが なしで作成されます。

Account Factory を設定して なしでアカウントを作成するには VPCs

1. ウェブブラウザを開き、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) セクションで [Edit] (編集) ボタンを選択します。
6. 「アカウントファクトリネットワーク設定の編集」ページで、VPC「新しいアカウントの設定オプション」セクションに移動します。

   オプション 1 またはオプション 2、またはその両方に従って、アカウントのプロビジョニングVPC時に AWS Control Tower が を作成しないようにすることができます。

a. オプション 1 — サブネットの削除

- [Internet-accessible subnet] (インターネットアクセス可能なサブネット) のトグルスイッチをオフにします。
- [Maximum number of private subnets] (プライベートサブネットの最大数) の値を 0 に設定します。

b. オプション 2 – AWS リージョンの削除

- VPC 作成列のリージョン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 を削除するVPCか、Account Factory を再設定して なしでアカウントを作成するときに発生する可能性があるこれらのエラーに注意してくださいVPCs。

- 既存の管理アカウントに AWS Control Tower の依存関係またはリソースが含まれている可能性がありVPC、削除失敗エラーが発生する可能性があります。
- なしで新しいアカウントを起動するように を設定するときにデフォルトCIDRのままにするとVPC、リクエストCIDRは失敗し、 が無効であるというエラーが表示されます。

チュートリアル: を使用して AWS Control Tower でセキュリティグループを設定する AWS Firewall Manager

この動画では、 AWS Firewall Manager サービスを使用して AWS Control Tower のネットワークセキュリティを強化する方法を示します。セキュリティグループを設定するためのセキュリティ管理者アカウントを指定できます。AWS Control Tower 組織のセキュリティポリシーを設定してセキュリティルールを適用する方法と、ポリシーを自動的に適用して非準拠のリソースを修復する方法について説明します。組織内のアカウントとリソース (Amazon EC2インスタンスなど) ごとに有効なセキュリティグループを表示できます。

独自のファイアウォールポリシーを作成することも、信頼できるベンダーのルールをサブスクライブすることもできます。

AWS Firewall Manager でセキュリティグループを設定する

このビデオ (8:02) では、AWSControl Tower のリソースとワークロードに対してネットワークインフラストラクチャのセキュリティを強化する方法について説明します。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

AWS Control Tower でのファイアウォール設定のビデオチュートリアル。

詳細については、 のセットアップ方法に関するドキュメント AWS WAFを参照してください。

チュートリアル: AWS Control Tower ランディングゾーンを廃止する

AWS Control Tower では、ランディングゾーンと呼ばれる安全なマルチアカウント AWS 環境を設定および管理できます。AWS Control Tower によって割り当てられたすべてのリソースをクリーンアップするプロセスは、ランディングゾーンの廃止と呼ばれます。

AWS Control Tower が不要になった場合、自動廃止ツールは AWS Control Tower によって割り当てられたリソースをクリーンアップします。自動廃止プロセスを開始するには、[Landing Zone Settings] (ランディングゾーンの設定) ページで [decommission] (廃止) タブを選択し、[Decommission landing zone] (ランディングゾーンの廃止) を選択します。

廃止処理中に実行するアクションの一覧に関しては、「廃止プロセスの概要」を参照してください。

> **Warning**
>
> すべての AWS Control Tower リソースを手動で削除することは、廃止とは異なります。この場合、新しいランディングゾーンを設定することはできません。

データおよび既存の AWS Organizations は、次の方法で廃止プロセスによって変更されません。

- AWS Control Tower はデータを削除せず、作成したランディングゾーンの一部のみを削除します。
- 廃止プロセスが完了すると、Amazon S3 バケットや Amazon CloudWatch Logs ロググループなど、いくつかのリソースアーティファクトが残ります。これらのリソースは、別のランディングゾーンを設定する前に、手動で削除する必要があります。これにより、特定のリソースの保守に伴い派生する可能性があるコストを回避できます。

- 自動廃止を使用して、部分的にセットアップされたランディングゾーンを削除することはできません。ランディングゾーンのセットアッププロセスが失敗した場合、自動廃止を有効にするには、障害状態を解決してセットアップを完了する必要があります。または、リソースを個別に手動で削除する必要があります。

ランディングゾーンの廃止は、重大な影響を引き起こす処理であり、元に戻すことはできません。AWS Control Tower が実行する廃止アクションと廃止後に残っているアーティファクトについては、以下のセクションで説明します。

> **Important**
>
> この廃止プロセスは、ランディングゾーンの使用を停止する場合にのみ実行することを強くお勧めします。既存のランディングゾーンを廃止した後に再作成することはできません。

廃止プロセスの概要

ランディングゾーンの廃止をリクエストすると、AWSControl Tower は次のアクションを実行します。

- ランディングゾーンで有効になっている各検出コントロールを無効にします。 AWSControl Tower は、コントロールをサポートする AWS CloudFormation リソースを削除します。
- サービスコントロールポリシー (SCPs) を削除することで、各予防コントロールを無効にします AWS Organizations。ポリシーが空の場合 (AWSControl Tower がSCPs管理するすべての を削除した後) 、AWSControl Tower はポリシーを完全にデタッチして削除します。
- としてデプロイされたすべてのブループリントを削除します AWS CloudFormation StackSets。
- すべてのリージョンで CloudFormation スタックとしてデプロイされたすべてのブループリントを削除します。
- プロビジョニングされたアカウントごとに、AWSControl Tower は廃止プロセス中に次のアクションを実行します。
  - 各 Account Factory アカウントのレコードを削除します。
  - AWS Control Tower が作成したIAMロールを削除して、アカウントに対する AWS Control Tower のアクセス許可を取り消し (追加のポリシーが追加されていない限り) 、標準`OrganizationsFullAccessRole`IAMロールを再作成します。
  - アカウントのレコードを から削除します AWS Service Catalog。
  - Account Factory 製品およびポートフォリオを AWS Service Catalogから削除します。

- 共有 (監査およびログアーカイブ) アカウントのブループリントを削除します。
- AWS Control Tower が作成したIAMロールを削除して、共有アカウントから AWS Control Tower のアクセス許可を取り消し (追加のポリシーが追加されていない限り)、`OrganizationsFullAccessRole`IAMロールを再作成します。
- 共有アカウントに関連するレコードを削除します。
- お客様が作成した に関連するレコードを削除しますOUs。
- ホームリージョンを識別する内部レコードを削除します。

> **Note**
>
> が空VPCでない場合は、廃止後に Account Factory VPCブループリント (`BP_ACCOUNT_FACTORY_VPC`) を削除してルートとNATゲートウェイをクリーンアップできます。

廃止処理中に削除されないリソース

ランディングゾーンを廃止しても、AWSControl Tower のセットアッププロセスが完全に逆になるわけではありません。一部のリソースは残るため、手動で削除しなければならない場合があります。

AWS Organizations

既存の AWS Organizations 組織を持たないお客様の場合、AWSControl Tower は Security と Sandbox という名前の 2 つの組織単位 (OUs) で組織をセットアップします。ランディングゾーンを廃止すると、組織の階層は次のように保持されます。

- AWS Control Tower コンソールから作成した組織単位 (OUs) は削除されません。
- セキュリティとサンドボックスOUsは削除されません。
- 組織は から削除されません AWS Organizations。
- AWS Organizations (共有、プロビジョニング、管理) のアカウントは移動または削除されません。

AWS IAM Identity Center (SSO)

既存の IAM Identity Center ディレクトリがないお客様の場合、AWSControl Tower は IAM Identity Center を設定し、初期ディレクトリを設定します。ランディングゾーンを廃止しても、AWSControl

Tower は IAM Identity Center を変更しません。必要に応じて、管理アカウントに保存されている IAM Identity Center 情報を手動で削除できます。特に、これらの領域に廃止による変更はありません。

- Account Factory で作成されたユーザーは削除されません。
- AWS Control Tower のセットアップによって作成されたグループは削除されません。
- AWS Control Tower によって作成されたアクセス許可セットは削除されません。
- AWS アカウントと IAM Identity Center アクセス許可セット間の関連付けは削除されません。
- IAM Identity Center ディレクトリは変更されません。

ロール

コンソールを使用する場合、AWSControl Tower はセットアップ時に特定のロールを作成します。または、 を使用してランディングゾーンを設定する場合は、これらのロールを作成するように求められますAPIs。ランディングゾーンを廃止しても、次のロールは削除されません。

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

Amazon S3 バケット

セットアップ中、AWSControl Tower はログ記録用とログアクセス用のバケットをログ記録アカウントに作成します。ランディングゾーンを廃止しても、次のリソースは削除されません。

- ロギングアカウント内のロギングおよびロギングアクセス S3 バケットは削除されません。
- ロギングおよびロギングアクセスバケットの内容は削除されません。

共有アカウント

AWS Control Tower のセットアップ中に、2 つの共有アカウント (監査とログアーカイブ) がセキュリティ OU に作成されます。ランディングゾーンを廃止した場合:

- AWS Control Tower のセットアップ中に作成された共有アカウントは閉鎖されません。

- `OrganizationAccountAccessRole` IAM ロールは、標準 AWS Organizations 設定に合わせて再作成されます。
- `AWSControlTowerExecution` ロールが削除されます。

プロビジョニングされたアカウント

AWS Control Tower のお客様は、Account Factory を使用して新しいAWSアカウントを作成できます。ランディングゾーンを廃止した場合:

- Account Factory で作成したプロビジョニングされたアカウントは閉鎖されません。
- のプロビジョニング済み製品は削除 AWS Service Catalog されません。それらを終了してクリーンアップすると、それらのアカウントは [Root OU] (ルート OU) に移動されます。
- AWS Control Tower VPCが作成した は削除されず、関連する AWS CloudFormation スタックセット (BP_ACCOUNT_FACTORY_VPC) も削除されません。
- `OrganizationAccountAccessRole` IAM ロールは、標準 AWS Organizations 設定に合わせて再作成されます。
- `AWSControlTowerExecution` ロールが削除されます。

CloudWatch ログロググループ

CloudWatch Logs ロググループ は`aws-controltower/CloudTrailLogs`、 という名前のブループリントの一部として作成されます`AWSControlTowerBP-BASELINE-CLOUDTRAIL-MANAGEMENT`。このロググループは削除されません。代わりに、ブループリントが削除され、リソースは保持されます。

- このロググループは、別のランディングゾーンを設定する前に手動で削除する必要があります。

> **Note**
>
> ランディングゾーン 3.0 以降のお客様は、個々の登録アカウントの CloudTrail ログと CloudTrail ログロールを削除する必要はありません。これらは組織レベルの証跡の管理アカウントでのみ作成されるためです。
> ランディングゾーンバージョン 3.2 以降、AWSControl Tower は という Amazon EventBridge ルールを作成します`AWSControlTowerManagedRule`。このルールは、すべての管理対象リージョンで、メンバーアカウントごとに作成されます。ルールは廃止時に自動的に削除されないため、すべての管理対象リージョンで共有アカウントおよびメンバーアカ

ウントから手動で削除してから、新しいリージョンでランディングゾーンを設定する必要があります。

AWS Control Tower リソースを削除する手順については、「」を参照してくださいAWS Control Tower リソースの管理。

AWS Control Tower リソースの管理

このドキュメントでは、定期的なメンテナンスおよび管理タスクの一環として Control Tower AWS リソースを個別に削除する方法について説明します。この章で説明する手順は、必要に応じて個々のリソースまたはいくつかのリソースを削除することのみを目的としています。これは、ランディングゾーンの廃止とは異なります。

以下の 2 種類のタスクでリソースの削除が必要になることがあります。

- ランディングゾーンを通常の状況で管理するときにリソースを削除する場合。
- 自動廃止処理後に残っているリソースをクリーンアップする場合。

Warning

リソースを手動で削除すると、新しいランディングゾーンを設定できなくなります。これは、廃止とは異なります。AWS Control Tower ランディングゾーンを廃止する場合は、この章で説明されているアクションを実行チュートリアル: AWS Control Tower ランディングゾーンを廃止するする前に、「」の指示に従ってください。この章の手順は、自動廃止が完了した後に残っているリソースをクリーンアップするのに役立ちます。すべてのランディングゾーンリソースを手動で削除しても、その削除はランディングゾーンの廃止とは異なり、予期しない料金が発生する可能性があります。

AWS Control Tower からアカウントを削除する必要がある場合は、以下のセクションを参照してアカウントを閉鎖します。

- アカウントの管理を解除する
- Account Factory で作成されたアカウントを解約する

削除ではなく廃止が必要か

エンタープライズに AWS Control Tower を使用する予定がなくなった場合、または組織リソースの大規模な再デプロイが必要な場合は、ランディングゾーンを最初にセットアップしたときに作成されたリソースを廃止できます。

- 廃止プロセスが完了すると、Amazon S3 バケットや Amazon CloudWatch Logs ロググループなど、いくつかのリソースアーティファクトが残ります。
- 別のランディングゾーンを設定する前に、アカウントの残りのリソースを手動でクリーンアップし、予期しない請求が発生する可能性を回避する必要があります。詳細については、「廃止処理中に削除されないリソース」を参照してください。

> **Warning**
>
> 廃止プロセスは、ランディングゾーンの使用を停止する場合にのみ実行することを強くお勧めします。このプロセスは元に戻せません。

AWS Control Tower リソースの削除について

この章の個々の手順では、AWSControl Tower リソースを手動で削除する方法について説明します。これらの手順は、ランディングゾーンから特定のリソースを削除する必要があるときに実行できます。

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

> **Warning**
>
> これらは、AWSControl Tower のセットアップにガバナンスのドリフトを引き起こす可能性のある破壊的なアクションです。元に戻すことはできません。

トピック

- SCPs を削除する
- StackSets および スタックの削除

- ログアーカイブアカウントでの Simple Storage Service (Amazon S3) バケットの削除
- Account Factory ポートフォリオおよび製品を削除する
- AWS Control Tower のロールとポリシーを削除する
- AWS Control Tower リソースのヘルプ

SCPs を削除する

AWS Control Tower は、コントロールにサービスコントロールポリシー (SCPs) を使用します。この手順では、AWSControl Tower にSCPs特に関連する を削除する方法について説明します。

削除するには AWS Organizations SCPs

1. で Organizations コンソールを開きます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- を持つサービスコントロールポリシー (SCPs) を見つけ、 ごとに次の操作を行いますSCP。
   a. 関連付けられた OU SCPから をデタッチします。
   b. SCP を削除します。

StackSets および スタックの削除

AWS Control Tower は、 StackSets および スタックを使用して、ランディングゾーンのコントロール AWS Config ルール に関連する をデプロイします。次の手順では、これらの特定のリソースを削除する方法を示します。

削除するには AWS CloudFormation StackSets

1. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。
2. 左側のナビゲーションメニューから、 を選択しますStackSets。
3. プレフィックスが StackSet の ごとにAWSControlTower、次の操作を行います。に多数のアカウントがある場合 StackSet、これには時間がかかることがあります。
   a. ダッシュボードのテーブル StackSet から特定の を選択します。そのプロパティページが開きます StackSet。
   b. ページの下部にある スタック テーブルで、テーブル内のすべての AWS アカウントのIDsアカウントのレコードを作成します。すべてのアカウントのリストをコピーします。

c. アクションから、 からスタックの削除を選択します StackSet。

d. [Set deployment options] (デプロイオプションの設定) で、[Deployment locations] (デプロイ先) から [Deploy stacks in accounts] (スタックをアカウントにデプロイ) を選択します。

e. テキストフィールドに、ステップ 3.b で記録IDsした AWS アカウントをカンマで区切って入力します。たとえば、*123456789012098765431098* などです。

f. [Specify regions] (リージョンの指定) で、[Add all] (すべて追加) を選択し、ページにある他のすべてのパラメータはデフォルト設定のままにして、[Next] (次へ) を選択します。

g. [Review] (確認) ページで、選択内容を確認し、[Delete stacks] (スタックの削除) を選択します。

h. StackSet プロパティページで、この手順を別のページ用に再度開始できます StackSets。

4. さまざまなStackSets プロパティページの スタックテーブルのレコードが空になると、このプロセスは完了です。

5. スタックテーブルのレコードが空になったら、削除 StackSet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、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AWSControlTower。

3. テーブル内の各スタックについて、次の操作を行います。

   a. スタックの名前の横にあるチェックボックスを選択します。

   b. [Actions] (アクション) メニューから [Delete Stack] (スタックの削除) を選択します。

   c. 開いたダイアログボックスで、情報が正確であることを確認し、[Yes, Delete] (はい、削除します) を選択します。

ログアーカイブアカウントでの Simple Storage Service (Amazon S3) バケットの削除

次の手順では、 AWSControlTowerExecutionグループの IAM Identity Center ユーザーとしてログアーカイブアカウントにサインインし、ログアーカイブアカウントの Amazon S3 バケットを削除する方法について説明します。

適切なアクセス許可でログアーカイブアカウントにサインインするには

1. で Organizations コンソールを開きますhttps://console.aws.amazon.com/organizations/。
2. [Accounts] (アカウント) タブから [Log archive] (ログアーカイブ) アカウントを見つけます。
3. 開いた右側のペインで、ログアーカイブアカウント番号を記録します。
4. ナビゲーションバーから アカウント名を選択し、アカウントメニューを開きます。
5. [Switch Role] (ロールの切り替え) を選択します。
6. 開いたページで、[Account] (アカウント) でログアーカイブアカウントのアカウント番号を指定します。
7. ロールには、 と入力しますAWSControlTowerExecution。
8. [Display Name] (表示名) にテキストを入力します。
9. お気に入りの [Color] (色) を選択します。
10. [Switch Role] (ロールの切り替え) を選択します。

Simple Storage Service (Amazon S3) バケットを削除するには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [aws-controltower] を含むバケット名を検索します。
3. テーブル内の各バケットについて、次の操作を行います。
    a. テーブル内のバケットのチェックボックスをオンにします。
    b. [Delete] (削除) を選択します。
    c. 開いたダイアログボックスで、情報が正確であることを確認し、確定するためのバケット名を入力し、[Confirm] (確認) を選択します。

Account Factory ポートフォリオおよび製品を削除する

次の手順では、 AWSServiceCatalogAdminsグループの IAM Identity Center ユーザーとしてサインインし、Account Factory ポートフォリオと製品をクリーンアップする方法を説明します。

適切なアクセス許可で管理アカウントにサインインするには

1. .awsapps.com/start URLでユーザーポータルに移動します*directory-id*。
2. [AWS Account] (AWS アカウント) から [Management] (管理) アカウントを見つけます。

3. からAWSServiceCatalogAdminFullAccess、 マネジメントコンソールを選択して、このロール AWS Management Console として にサインインします。

Account Factory をクリーンアップするには

1. で Service Catalog コンソールを開きますhttps://console.aws.amazon.com/servicecatalog/。
2. 左のナビゲーションメニューから [Portfolios list] (ポートフォリオリスト) を選択します。
3. [Local Portfolios] (ローカルポートフォリオ) テーブルで、[AWS Control Tower Account Factory Portfolio] という名前のポートフォリオを検索します。
4. そのポートフォリオの名前を選択し、詳細ページに移動します。
5. ページの [Constraints] (制約) セクションを展開し、製品名 [AWS Control Tower Account Factory] のある制約のラジオボタンを選択します。
6. [REMOVE CONSTRAINTS] を選択します。
7. ダイアログボックスが開き、情報が正しいことを確認し、 を選択しますCONTINUE。
8. ページの [Products] (製品) セクションから製品名 [AWS Control Tower Account Factory] のラジオボタンを選択します。
9. [REMOVE PRODUCT] を選択します。
10. ダイアログボックスが開き、情報が正しいことを確認し、 を選択しますCONTINUE。
11. [Users, Groups, and Roles] (ユーザー、グループ、およびロール) セクションを展開し、このテーブルのすべてのレコードのチェックボックスをオンにします。
12. REMOVE USERS、GROUPまたは ROLEを選択します。
13. ダイアログボックスが開き、情報が正しいことを確認し、 を選択しますCONTINUE。
14. 左のナビゲーションメニューから [Portfolios list] (ポートフォリオリスト) を選択します。
15. [Local Portfolios] (ローカルポートフォリオ) テーブルで、[AWS Control Tower Account Factory Portfolio] という名前のポートフォリオを検索します。
16. そのポートフォリオのラジオボタンを選択し、 DELETE PORTFOLIOを選択します。
17. ダイアログボックスが開き、情報が正しいことを確認し、 を選択しますCONTINUE。
18. 左のナビゲーションメニューから [Product list] (製品リスト) を選択します。
19. [Admin products] (管理者製品) ページで、[AWS Control Tower Account Factory] という名前の製品を検索します。
20. 製品を選択して、[Admin product details] (Admin 製品の詳細) ページを開きます。
21. [Actions] (アクション) から [Delete product] (製品の削除) を選択します。

22. ダイアログボックスが開き、情報が正しいことを確認し、 を選択しますCONTINUE。

AWS Control Tower のロールとポリシーを削除する

これらの手順では、ランディングゾーンのセットアップ時、または後で AWS Control Tower が作成したロールとポリシーをクリーンアップする方法について説明します。

IAM Identity Center AWSServiceCatalogEndUserAccess ロールを削除するには

1. で AWS IAM Identity Center コンソールを開きますhttps://console.aws.amazon.com/singlesignon/。
2. AWS リージョンを、最初に AWS Control Tower をセットアップしたリージョンであるホームリージョンに変更します。
3. 左のナビゲーションメニューから [AWS accounts] (AWS アカウント) を選択します。
4. 管理アカウントのリンクを選択します。
5. アクセス許可セットのドロップダウンを選択し、 を選択してAWSServiceCatalogEndUserAccess、削除を選択します。
6. 左側のパネルから [AWS accounts] (AWS アカウント) を選択します。
7. [Permission sets] (許可セット) タブを開きます。
8. これを選択して削除AWSServiceCatalogEndUserAccessします。

IAM ロールを削除するには

1. https://console.aws.amazon.com/iam/ で 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 [Roles] (ロール) を選択します。
3. テーブルから、 という名前のロールを検索しますAWSControlTower。
4. テーブル内の各ロールについて、次の操作を行います。
   a. ロールのチェックボックスをオンにします。
   b. [Delete role] (ロールの削除) を選択します。
   c. 開いたダイアログボックスで、情報が正確であることを確認し、[Yes, delete] (はい、削除します) を選択します。

IAM ポリシーを削除するには

1. https://console.aws.amazon.com/iam/ で 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 [Policies] (ポリシー) を選択します。
3. テーブルから、 という名前のポリシーを検索しますAWSControlTower。
4. テーブル内の各ポリシーについて、次の操作を行います。

   a. ポリシーのチェックボックスをオンにします。
   b. ドロップダウンメニューから [Policy actions] (ポリシーアクション) と [Delete] (削除) を選択します。
   c. 開いたダイアログボックスで、情報が正確であることを確認し、[Delete] (削除) を選択します。

AWS Control Tower リソースのヘルプ

AWS Control Tower リソースを削除するとき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。

ランディングゾーンの廃止方法

AWS Control Tower ランディングゾーンを廃止するには、ここに記載されている手順に従います。

> **Note**
>
> 廃止する前に、登録済みアカウントの管理を解除することをお勧めします。

1. AWS Control Tower コンソールのランディングゾーン設定ページに移動します。
2. [Decommission your landing zone] (ランディングゾーンを廃止します) セクションにある [Decommission your landing zone] (ランディングゾーンを廃止します) を選択します。
3. 実行しようとしているアクションと必要な確認プロセスについて説明するダイアログが表示されます。廃止の意思を確認するには、すべてのボックスを選択し、要求どおりに確認を入力する必要があります。

> **Important**
>
> 廃止プロセスは元に戻せません。

4. ランディングゾーンを廃止する意図を確認すると、廃止の進行中に AWS Control Tower のホームページにリダイレクトされます。この処理には最長で 2 時間かかります。
5. 廃止が成功したら、AWSControl Tower コンソールから新しいランディングゾーンを設定する前に、残りのリソースを手動で削除する必要があります。これらの残りのリソースには、特定の Amazon S3 バケット、組織、 CloudWatch ログロググループが含まれます。

   > **Note**
   >
   > これらのアクションは、請求およびコンプライアンス作業に重大な影響を及ぼす可能性があります。例えば、これらのリソースの削除に失敗すると、予期しない請求が発生する可能性があります。

   リソースを手動で削除する方法の詳細については、「AWS Control Tower リソースの削除について」を参照してください。
6. 新しい AWS リージョンに新しいランディングゾーンを設定する場合は、この追加ステップに従います。を使用して次のコマンドを入力しますCLI。

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

廃止後に必要な手動クリーンアップタスク

- landing zone を廃止した後に新しいランディングゾーンを作成する場合、ロギングアーカイブアカウントと監査アカウントに異なる E メールアドレスを指定する必要があります。そうでない場合、既存のロギングアーカイブアカウントまたは監査アカウントを持ち込むための手順に従ってください。
- CloudWatch Logs ロググループ は`aws-controltower/CloudTrailLogs`、別のランディングゾーンを設定する前に手動で削除する必要があります。
- ログ用に予約された 2 つの Amazon S3 バケットは、手動で削除するか、名前を変更する必要があります。
- 既存の [Security] (セキュリティ) 組織と [Sandbox] (サンドボックス) 組織は、手動で削除するか、名前を変更する必要があります。

> **Note**
>
> AWS Control Tower Security OU 組織を削除する前に、まずログ記録アカウントと監査アカウントを削除する必要がありますが、管理アカウントを削除することはできません。これらのアカウントを削除するには、監査アカウントとロギングアカウントに ルートユーザーとしてサインインする場合 (ルートユーザーとしてログイン) し、個別に削除する必要があります

- AWS Control Tower の AWS IAM Identity Center （ IAM Identity Center) 設定を手動で削除することもできますが、既存の IAM Identity Center 設定に進むことができます。
- AWS Control Tower によってVPC作成された を削除し、関連するAWS CloudFormation スタックセットを削除することもできます。
- 新しい AWS リージョンに新しいランディングゾーンを設定する前に、以下の追加ステップに従う必要があります。
  - を使用して次のコマンドを入力しますCLI。

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

  - すべての管理対象リージョンの共有アカウントとメンバーアカウントAWSControlTowerManagedRuleから、 という残りのマネージドルールを削除します。AWSControlTowerManagedRuleは Amazon EventBridge ルールです。

ランディングゾーン廃止後のセットアップ

ランディングゾーン廃止後は、手動クリーンアップが完了するまでセットアップを再実行できません。また、これらの残ったリソースを手動でクリーンアップしないと、予期しない請求が発生する可能性があります。次の点に注意してください。

- AWS Control Tower 管理アカウントは、AWSControl Tower ルート OU の一部です。これらのIAMロールとIAMポリシーが管理アカウントから削除されていることを確認してください。
  - ロール:
    - AWSControlTowerAdmin
    - AWSControlTowerCloudTrailRole

    - AWSControlTowerStackSetRole
  - ポリシー:
    - AWSControlTowerAdminPolicy
    - AWSControlTowerCloudTrailRolePolicy
    - AWSControlTowerStackSetRolePolicy
- ランディングゾーンを再度起動する前に、AWSControl Tower の既存の IAM Identity Center 設定を削除または更新できますが、削除する必要はありません。
- AWS Control Tower によってVPC作成された を削除することもできます。
- ログ記録アカウントまたは監査アカウントに指定された E メールアドレスが既存の AWS アカウントに関連付けられている場合、セットアップは失敗します。 AWS アカウントを閉鎖することも、別の E メールアドレスを使用してランディングゾーンを再度セットアップすることもできます。または、これらの既存の共有アカウントを再利用して、独自のロギングアカウントと監査アカウントを持ち込む機能を使用することもできます。詳細については、「既存のセキュリティアカウントまたはログアカウントを使用する際の考慮事項」を参照してください。
- ロギングアカウントに次の予約名の Amazon S3 バケットが既に存在する場合、セットアップは失敗します。
  - aws-controltower-logs-*{accountId}*-*{region}* (ロギングバケットに使用)。
  - aws-controltower-s3-access-logs-*{accountId}*-*{region}* (ロギングアクセスバケットに使用)。

  これらのバケットの名前を変更または削除するか、ロギングアカウントに別のアカウントを使用する必要があります。
- 管理アカウントに CloudWatch Logs に既存のロググループ がある場合aws-controltower/CloudTrailLogs、セットアップは失敗します。ロググループの名前を変更するか、ロググループを削除する必要があります。

新しい で を設定する前に AWS リージョン

新しい AWS リージョンに新しいランディングゾーンを設定する場合は、以下の追加ステップに従います。

- を使用して次のコマンドを入力しますCLI。

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- 残っているマネージドルール (AWSControlTowerManagedRule) を、すべての管理対象リージョンで共有アカウントおよびメンバーアカウントから削除します。

> **Note**
>
> Security または Sandbox OUsという名前の最上位レベルの組織では、新しいランディングゾーンを設定できません。ランディングゾーンを再度設定OUsするには、これらの名前を変更または削除する必要があります。

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、以下の情報を使用してベストプラクティスに従って解決できます。発生した問題が次の情報の範囲外である場合、または解決を試みた後にも持続する場合は、AWS Support にお問い合わせください。

ランディングゾーンの起動の失敗

ランディングゾーンの起動の失敗の一般的な原因:

- 確認メールメッセージへの応答の欠如。
- AWS CloudFormation StackSet 失敗。

確認メールメッセージ: 管理アカウントが作成後 1 時間未満である場合、追加のアカウントを作成すると、問題が発生することがあります。

実行するアクション

この問題が発生した場合は、E メールを確認してください。確認メールが着信し、応答を待機していることがあります。または、1 時間待ってから、もう一度試すことをお勧めします。問題が解決しない場合は、AWS Support までお問い合わせください。

失敗 StackSets: ランディングゾーンの起動に失敗するもう 1 つの原因は AWS CloudFormation StackSet 失敗です。 AWS Security Token Service (STS) リージョンは、AWSControl Tower が管理するすべての AWS リージョンの管理アカウントで有効にする必要があります。有効にしないと、スタックセットは起動できません。

実行するアクション

AWS Control Tower を起動する前に、必要なすべての AWS Security Token Service (STS) エンドポイントリージョンを必ず有効にしてください。

AWS Control Tower がサポート AWS リージョン する のリストを表示するには、「」を参照してくださいAWS リージョンと AWS Control Tower の連携方法。

ランディングゾーンが最新ではないエラー

ランディングゾーンを最近更新していない場合は、AWSControl Tower へのアクセスを回復しようとするとエラーが表示されることがあります。以下のようなエラーメッセージが表示されることがあります。

```
Unable to access Control Tower
```

アカウントは長い間非アクティブになっています。非アクティブのため、 AWS Control Tower にアクセスするにはランディングゾーンを更新する必要があります。

ただし、ランディングゾーンの更新が失敗する可能性があります。

実行する手順

組織の管理アカウントにサインインし、ルートユーザーとしてサインインします。IAM Identity Center のIAMユーザーまたはユーザーは、AWSControl Tower 管理者権限を持ち、AWSControlTowerAdminsグループの一部である必要があります。その場合は、更新を再試行してください。

新しいアカウントのプロビジョニングに失敗する

この問題が発生した場合は、以下の一般的な原因を確認します。

アカウントのプロビジョニングフォームに入力した際に、次を行った可能性があります。

- 指定された tagOptions、
- 有効なSNS通知、
- プロビジョニング済み製品の通知を有効化した

これらのオプションを指定せずに、アカウントのプロビジョニングを再試行してください。詳細については、「AWS Service Catalog Account Factory でアカウントをプロビジョニングする 」を参照してください。

その他の一般的な失敗の原因:

- プロビジョニングされた製品プランを作成した場合 (リソースの変更を表示するため)、アカウントのプロビジョニングが無期限に [In progress] (進行中) 状態のままになることがあります。

- Account Factory での新しいアカウントの作成は、他の AWS Control Tower 設定の変更の進行中に失敗します。例えば、OU にコントロールを追加するプロセスの進行中にアカウントをプロビジョニングしようとすると、Account Factory にエラーメッセージが表示されます。

AWS Control Tower で以前のアクションのステータスを確認するには

- > AWS CloudFormation StackSetsに移動する
- AWS Control Tower に関連する各スタックセットを確認する (プレフィックス : AWSControlTower「」)
- まだ実行中の AWS CloudFormation StackSets オペレーションを探します。

アカウントのプロビジョニングに 1 時間以上かかる場合は、プロビジョニングプロセスを終了し、もう一度試してください。

既存のアカウントを登録できない

既存の AWS アカウントを 1 回登録しようとして、その登録が失敗した場合、2 回目に試行すると、スタックセットが存在することを示すエラーメッセージが表示されることがあります。続行するには、プロビジョニングされた製品を Account Factory から削除する必要があります。

最初の登録が失敗した原因が、アカウントに `AWSControlTowerExecution` ロールを作成し忘れていたことである場合は、表示されるエラーメッセージで、ロールを作成するように指示されます。ただし、ロールを作成しようとすると、AWSControl Tower がロールを作成できなかったことを示す別のエラーメッセージが表示される可能性があります。このエラーは、プロセスが部分的に完了しているために発生します。

この場合、既存のアカウントの登録に進む前に、2 つの回復手順を実行する必要があります。まず、AWS Service Catalog コンソールから Account Factory でプロビジョニングされた製品を終了する必要があります。次に、 AWS Organizations コンソールを使用して、OU からアカウントを手動で移動し、ルートに戻す必要があります。その後、アカウントに `AWSControlTowerExecution` ロールを作成し、[Enroll account] (アカウントの登録) フォームに再度入力します。

登録に失敗するもう 1 つの原因として、アカウントに既存の AWS Config リソースがあることが考えられます。その場合、既存の AWS Config リソースを変更する方法については、「既存のリソースを持つアカウントの登録」を参照してください。

Account Factory アカウントを更新できない

アカウントが不整合な状態にある場合、Account Factory または から正常に更新することはできません AWS Service Catalog。

ケース 1: 以下のようなエラーメッセージが表示されることがあります。

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

一般的な原因： AWS Control Tower は、初期プロビジョニングVPC中に常に AWS デフォルトを削除します。VPC アカウントに AWS デフォルトを設定するには、アカウントの作成後にデフォルトを追加する必要があります。 AWSControl Tower には、チュートリアルで示すように Account Factory を設定しない限りVPC、デフォルトの を置き換えVPC AWS る独自のデフォルトがあります。これにより、AWSControl Tower は をVPCまったくプロビジョニングしません。その後、アカウントには がありませんVPC。デフォルトVPCを使用する場合は、その AWS デフォルトを再度追加する必要があります。

ただし、AWSControl Tower は AWS デフォルトの をサポートしていませんVPC。その種の VPC をデプロイすると、アカウントは `Tainted` 状態になります。その状態にある場合、アカウントを更新することはできません AWS Service Catalog。

実行するアクション： 追加VPCしたデフォルトを削除する必要があります。削除すると、アカウントを更新できます。

> **Note**
>
> `Tainted` 状態になると、未更新のアカウントは属する先の OU でコントロールを有効にできないという問題が発生する場合があります。

ケース 2: 以下のようなエラーメッセージが表示されることがあります。

```
AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.
```

一般的な原因： アカウントを登録済みの OU から別の OU に移動しようとしましたが、古い AWS Config ルールは残ります。アカウントが不整合な状態になっています。

実行するアクション:

アカウントの移動が意図されていた場合:

- Service Catalog のアカウントを終了します。
- もう一度アカウントを登録してください。
- コンテキスト/影響： デプロイされた AWS Config ルールが、送信先 OU によって指定された設定と一致しません。
- AWS Config ルールが以前の OU から残り、意図しない支出が発生する可能性があります。
- リソース名の競合により、アカウントを再登録または更新しようとすると失敗します。

アカウントの移動が意図されていなかった場合:

- アカウントを元の OU に戻します。
- Service Catalog からアカウントを更新します。
- 起動パラメータに、アカウントの元の OU を入力します。
- コンテキスト/インパクト: アカウントが元の OU に戻らない場合、アカウントの状態は新しい OU によって指示されたコントロールと一致しません。
- アカウントの更新は、以前の OU に関連付けられた AWS Config ルールが削除されないため、有効な修復ではありません。

ランディングゾーンを更新できない

AWS 更新が失敗した場合、Control Tower は以前のランディングゾーンバージョンにロールバックしません。ランディングゾーンが不確定な状態になる場合があります。その場合は、 AWS サポートにお問い合わせください。

ランディングゾーンの更新は、いくつかの理由で失敗することがあります。

- 前提条件が満たされていない
- AWS Config リソースが特定のアカウントに存在する
- 閉鎖されたアカウントが存在する

前提条件が満たされていない

ランディングゾーンの更新時には、ランディングゾーンの設定時と同じ前提条件を満たす必要があります。更新の前に、起動前チェックを確認してください。

AWS Config リソースがセキュリティ OU アカウントに存在する

監査およびログアーカイブアカウントに AWS Config リソースを追加しないでください。ランディングゾーンの更新プロセスは、これらのリソースが存在する状態では完了できません。これらの制限は、アカウントを登録したり、ランディングゾーンを初めて設定したりする場合の制限と似ています。詳細については、「既存の AWS Config リソースを持つアカウントの登録」を参照してください。

閉鎖されたアカウントが存在する

アカウントが [Closed] (閉鎖) または [Suspended] (一時停止) 状態の場合は、ランディングゾーンを更新しようとすると問題が発生する可能性があります。ランディングゾーンの更新を実行する前に、クローズされたすべてのアカウントのプロビジョニング済み製品を削除する必要があります。

AWS Service Catalog プロビジョニング済み製品ページに、次のようなエラーメッセージが表示されることがあります。

```
AWSControlTowerExecution role can't be assumed on the account.
```

一般的な原因: プロビジョニング済み製品を削除せずにアカウントを一時停止しました。

実行するアクション: このエラーが表示された場合は、次の 2 つのオプションがあります。

1. AWS サポートに連絡してアカウントを再度開き、プロビジョニング済み製品を削除してから、アカウントを再度閉鎖します。
2. アカウント閉鎖のために孤立 StackSets した からリソースを削除します。 (このオプションは、StackSets に削除しない現在の状態のインスタンスがある場合にのみ使用できます。)

からリソースを削除するには StackSets、閉鎖されたアカウントごとにこれを行います。

- 各 AWS Control Tower に移動 StackSets し、閉鎖されたアカウントの をすべてのリージョン StackInstances から削除します。
- IMPORTANT： スタックを保持 オプションを選択すると、 はスタックインスタンスのみ StackSet を削除します。 StackSet は閉鎖されたアカウントからロールを引き受けることができないため、`AWSControlTowerExecution`ロールを引き受けようとすると失敗し、受信したエラーメッセージが表示されます。

が言及する失敗エラー AWS Config

AWS Control Tower でサポートされている AWS リージョンで AWS Config が有効になっている場合は、事前チェックが失敗したため、エラーメッセージが表示されることがあります。メッセージは、根本的な動作が原因で問題を適切に説明していないように見える場合があります AWS Config。

次のいずれかに類似したエラーメッセージが表示される場合があります。

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

一般的な原因： AWS アカウントで AWS Config サービスを有効にすると、デフォルトの名前で設定レコーダーと配信チャネルが作成されます。コンソールから AWS Config サービスを無効にすると、設定レコーダーや配信チャネルは削除されません。を使用して削除するかCLI、AWSControl Tower 用に変更する必要があります。AWS Control Tower でサポートされているいずれかのリージョンで AWS Config サービスが有効になっている場合、このエラーが発生する可能性があります。

アカウントに既存の AWS Config リソースがある場合は、「既存の AWS Config リソースを持つアカウントを登録する」を参照して、既存のリソースを変更する方法の手順を確認してください。

実行するアクション: サポートされているすべてのリージョンで、設定レコーダーと配信チャネルを削除します。 AWS Config を無効にするだけでは不十分です。設定レコーダーと配信チャネルは を使用して削除する必要がありますCLI。設定レコーダーと配信チャネルを から削除したら CLI、AWSControl Tower の起動とアカウントの登録を再試行できます。

プロビジョニング済み製品をデプロイしようとしている場合は、再試行する前にプロビジョニング済み製品を削除する必要があります。そうしないと、以下のようなエラーメッセージが表示されることがあります。

- `An error occurred` **`(InvalidParametersException)`** `when calling the` **`ProvisionProduct`** `operation: A stack named` *`Stackname`* `already exists.`

メッセージでは、*Stackname* がスタック名を指定します。

設定レコーダーと配信チャネルのステータスを判断するために使用できるコマンドの例 AWS Config CLIを次に示します。

表示コマンド:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

削除コマンド:

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

詳細については、 AWS Config ドキュメントを参照してください。

- 設定レコーダーの管理 (AWS CLI)
- 配信チャネルの管理

起動パスが見つからないというエラー

新しいアカウントを作成しようとすると、次のようなエラーメッセージが表示されることがあります。

```
No launch paths found for resource: prod-dpqqfywxxxx
```

このエラーメッセージは AWS Service Catalog、AWSControl Tower でのアカウントのプロビジョニングに役立つ統合サービスである によって生成されます。

一般的な原因:

- root としてログインしている可能性があります。 AWSControl Tower は、ルートユーザーとしてログインしている場合のアカウントの作成をサポートしていません。
- IAM Identity Center ユーザーが適切なアクセス許可グループに追加されていません。IAM Identity Center ユーザーを (エンドユーザーアクセスの場合) または AWSAccountFactory (管理者アクセスAWSServiceCatalogAdminsの場合) のいずれかのアクセス許可グループに追加する必要がある場合があります。
- IAM ユーザーとして認証されている場合は、正しいアクセス許可を持つようにAWS Service Catalog ポートフォリオに追加する必要があります。
- この問題は、正しいアクセス許可を持っていても AWS Control Tower ドリフトが検出され、ドリフト修復が必要な場合にも発生します。ほとんどの種類のドリフトを修復するには、[ランディングゾーン設定] ページで [リセット] を選択します。

許可不足のエラーを受け取った

特定の AWS Organizationsで特定の作業を実行するために必要な許可がアカウントにない可能性があります。次のタイプのエラーが発生した場合は、 IAMや IAM Identity Center のアクセス許可など、すべてのアクセス許可領域をチェックして、アクセス許可がそれらの場所から拒否されていないことを確認します。

```
You have insufficient permissions to perform AWS Organizations API actions.
```

試行するアクションが作業に必要で、関連する制限が見つからない場合は、システム管理者または AWS Support にお問い合わせください。

検出コントロールがアカウントで有効になっていない

最近 AWS Control Tower のデプロイを新しい AWS リージョンに拡張した場合、新しく適用された検出コントロールは、AWSControl Tower によってOUs管理される 内の個々のアカウントが更新されるまで、どのリージョンで作成した新しいアカウントにも有効になりません。既存のアカウントにある既存の検出コントロールはまだ有効です。

アカウントを更新する前に検出コントロールを有効にしようとすると、次のようなエラーメッセージが表示されることがあります。

```
AWS Control Tower can't enable the selected control on this OU. AWS Control
Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child
```

`accounts have dependencies that are missing. Update all child accounts under the OU, then try again.`

実行するアクション: アカウントの更新。

AWS Control Tower コンソールからアカウントを更新するには、「」を参照してくださいAWS Control Tower OUsとアカウントを更新するタイミング。

複数の個々のアカウントをプログラムで更新するには、 APIs から AWS Service Catalog と AWS CLIを使用して更新を自動化できます。更新プロセスにアプローチする方法の詳細については、こちらの「動画チュートリアル」を参照してください。 は、ビデオにUpdateProvisionedProductAPIProvisionProductAPI示されている に置き換えることができます。

それでもアカウントで検出コントロールが有効にならない場合は、AWS Support にお問い合わせください。

によって返されるレート超過エラー AWS Organizations API

考えられる原因

AWS Control Tower が毎日のスキャンを実行して、 SCPsがドリフトしたかどうかを確認する間に、ワークロードが実行されていました。

従うべき手順

API スロットリングまたは`rate exceeded`エラーが発生した場合は、次の手順を試してください。

- ワークロードを別のタイミングで実行します。(AWSControl Tower が監査スキャンを実行するタイミングを確認するには、リージョン別の AWS Control Tower SCP 不変スキャンスケジュールを参照してください。)
- を介して APIsを直接呼び出す場合HTTP: を使用して AWS SDK、失敗したアクションを自動的に再試行します。
- Service Quotas と AWS Support を通じて制限の引き上げをリクエストします。

Elastic Beanstalk API でのスロットリングのトラブルシューティング手順の例については、以下を参照してください。 `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

Account Factory アカウントを 1 つの AWS Control Tower ランディングゾーンから別の AWS Control Tower ランディングゾーンに直接移動できない

> **Warning**
>
> この方法は、対象となるアカウントがAWS組織全体の同じアカウントである必要があり、各組織にはランディングゾーンが 1 つしか存在しないため、対象となるアカウント登録の前提条件を満たしていません。このアクションを実行しようとして、複数のエラーメッセージが表示された場合には、次の情報が参考になる可能性があります。

Account Factory を通じてプロビジョニングしたアカウントを AWS Control Tower が管理する別のランディングゾーンに移動するには、別の管理アカウントで、そのアカウントに関連付けられているすべてのIAMロールとスタックを元の OU から削除する必要があります。これらのリソースを、アカウントがデプロイされているすべてのリージョンから削除します。

> **Note**
>
> リソースを削除する最善の方法は、元の OU でアカウントのプロビジョニングを解除してから、リソースを移動させることです。

リソースを削除しないと、新しい OU への登録は失敗します。1 つ以上のエラーメッセージが表示されることがあり、アカウントがデプロイされたすべてのリージョンから残りのロールとスタックが削除されるまで、同様のエラーメッセージが表示され続けます。

エラーメッセージが表示されるたびに、新しい OU からアカウントを削除し、エラーメッセージの対象となる古いリソースを削除してから、アカウントを新しい OU に戻す必要があります。このプロセス removing-and-deletingは、アカウントがデプロイされたすべてのリージョン、場合によっては 10 回または 20 回、残りのリソースごとに繰り返す必要があります。これらの繰り返しエラーは、アカウントがIAMロールの削除SCPを防止する を使用して OU にプロビジョニングされたために発生します。再試行する前に、アカウントのリソースをすべて削除することで、回復プロセスを短縮できます。

以下の例は、削除されていないロールとスタックが残っている場合に表示される可能性のある失敗に関するメッセージの種類を示しています。ほとんどの場合、古いリソースが残っている限り、アカウントを登録しようとするたびに、これらのメッセージのいずれかが表示されます。

この例では、リソース ID 文字列の値が変更されています。これらの値は、表示されるエラーメッセージでは同じにはなりません。次の例に示すようなメッセージが表示されます。

- AWS Control Tower cannot create the IAM role *aws-controltower-AdministratorExecutionRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ConfigRecorderRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ForwardSnsNotificationRole* because the role already exists. To continue, delete the existing IAM role and try again.

または、次のようなスタックセットの失敗に関するエラーメッセージが表示されることがあります。

```
"Error\":\"StackSetFailState\",
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

残りのリソースをすべて最初の OU から削除すると、アカウントを新しい OU に招待したり、プロビジョニングしたり、登録したりできるようになります。

AWS サポート

既存のメンバーアカウントを別のサポートプランに移動する場合は、ルートアカウントの認証情報を使用して各アカウントにサインインし、プランを比較して、希望するサポートレベルを設定できます。

サポートプランを変更するときは、 MFAおよび アカウントのセキュリティ連絡先を更新することをお勧めします。

ベースラインのタイプ

AWS Control Tower のベースラインは、ターゲットに適用できるリソースと特定の設定のグループです。最も一般的なベースラインターゲットは、組織単位 (OU) です。例えば、ターゲットとして選択した OU でベースラインを有効にして、その OU を AWS Control Tower に登録できます。

ランディングゾーンの設定時には、共有アカウントまたはランディングゾーン全体をベースラインターゲットとすることができます。ランディングゾーンの設定と構成に基づいて、特定のベースラインを有効にして更新できます。AWS Control Tower は、ベースラインで指定された方法でリソースを作成してターゲットにデプロイします。

ターゲットのベースラインを有効にすると、ベースラインは AWS CloudFormation リソースと呼ばれる `EnabledBaseline`リソースとして表されます。

AWS Control Tower には、次の 2 つの一般的なタイプのベースラインがあります。

- AWS Control Tower に登録されている OU に適用できるベースラインタイプ、またはベースラインを適用して登録する予定の OU に適用できるベースラインタイプ。
- ランディングゾーンまたは共有アカウントに適用できるベースラインタイプは、初期設定時またはランディングゾーンの更新時に適用されます。

OU の登録と更新のために OUs レベルで適用されるベースラインタイプ

- 名前: `AWSControlTowerBaseline`

  説明: AWS Control Tower ガバナンスに必要な、ターゲット OU 内のメンバーアカウントのリソースと必須コントロールを設定します。

  考慮事項: このベースラインは、ランディングゾーンのリージョン拒否コントロールの設定を保持します。つまり、リージョンがランディングゾーンレベルで許可されていない場合、`EnableBaseline` API を呼び出して OU を登録する際に、そのリージョンはその OU に対して許可されません。

> **Note**
>
> OU レベルのリージョン拒否コントロールは、ランディングゾーンのリージョン拒否コントロールが許可しないリージョンを許可することはできません。

詳細については、 AWS Organizations ドキュメントのSCPs」を参照してください。

推奨事項: ターゲット OU がワークロードを実行している可能性のあるリージョンを確認し、その結果をランディングゾーンのリージョン拒否コントロールに対してチェックしてから、OU の EnableBaseline API を呼び出すことをお勧めします。そうしないと、特定のリージョンのリソースにアクセスできなくなる可能性があります。

- 名前: BackupBaseline

  説明: このベースラインは、ターゲット OU 内のメンバーアカウントのリソースとコントロールを設定します。これらは、 との統合 AWS Backup により、 間のデータバックアップを自動化し AWS のサービス、バックアップポリシー管理を一元化するために必要です。

  考慮事項: ターゲット OU BackupBaselineで を有効にする前に、ターゲット OU で AWSControlTowerBaselineが有効になっていることを確認してください。つまり、ターゲット OU を AWS Control Tower に登録する必要があります。

  - AWS Control Tower ランディングゾーンの作成プロセス AWS Backup 中にアクティブ化するか、ランディングゾーンの更新プロセス中にアクティブ化するかを選択できます。
  - BackupBaseline は、ランディングゾーンバージョン 3.1 以降と互換性があります。
  - BackupBaseline は管理アカウントには適用されません。

> **Note**
>
> ランディングゾーンのベースラインの動作は、OU レベルのベースラインの動作と異なります。

ランディングゾーンまたは共有アカウントに適用される可能性のあるベースラインタイプ

AWS Control Tower は、ランディングゾーンの設定と更新のプロセスの一環として、ランディングゾーンレベルで自動的に適用されるベースラインを有効にします。ランディングゾーンの設定を変更すると、ランディングゾーンのベースラインが変更される場合があります。例えば、IAM アイデンティティセンターをオプトインした場合、AWS Control Tower はランディングゾーンで最新バージョンの `IdentityCenterBaseline` ベースラインを有効にすることができます。

`ListEnabledBaselines` API コールを使用すると、ランディングゾーンで有効になっているベースラインを表示できます。

> **Note**
>
> `EnableBaseline` API で直接適用`AWSControlTowerBaseline`できるのは のみです。他のベースラインは自動的に管理されます (`AuditBaseline`、`LogArchiveBaseline`)。を適用すると、 のステータス`IdentityCenterBaseline`が情報として提供されます`AWSControlTowerBaseline`。

- 名前: `AuditBaseline`

  説明: 組織内のアカウントのセキュリティとコンプライアンスをモニタリングするためのリソースを設定します。このベースラインは変更できません。AWS Control Tower によってデプロイされます。
- 名前: `LogArchiveBaseline`

  説明: 組織内のアカウントからの API アクティビティとリソース設定のログ用に中央リポジトリを設定します。このベースラインは変更できません。AWS Control Tower によってデプロイされます。
- 名前: `IdentityCenterBaseline`

  説明: IAM アイデンティティセンターの共有リソースを設定します。これにより、`AWSControlTowerBaseline` がアカウントのアイデンティティセンターアクセスを設定する準備が整います。

  考慮事項: このベースラインが機能するのは、ランディングゾーンの初期設定時に ID プロバイダーとして IAM アイデンティティセンターを選択した場合、または後でランディングゾーン設定

を変更して、IAM アイデンティティセンターをランディングゾーンに対して有効にした場合のみです。別の ID プロバイダーを使用している場合、このベースラインを有効にするためのアクセス権限はありません。

- 名前: `BackupCentralVaultBaseline`

  説明: 組織内の中央 AWS Backup ボールトを設定します。

- 名前: `BackupAdminBaseline`

  説明: 委任管理者と AWS Backup Audit Manager を設定します。

アカウントの一部登録

ベースラインの操作中に、アカウントが一部登録済みという状態になる場合があります。

この状態は、`ResetEnabledBaseline` API を呼び出して OU を再登録する場合に発生する可能性があります。AWS Control Tower は、ターゲット OU のアカウントに必須リソースのみを適用するためです。親 OU のオプションリソース (コントロール) がないアカウントは、一部登録済みとマークされます。

未登録のアカウントを登録済みの OU に移動した後、その OU に対して `ResetEnabledBaseline` API を呼び出してそのアカウントを登録すると、AWS Control Tower は `AWSControlTowerBaseline` に関連付けられたリソースを新しく登録されたアカウントに適用します。ただし、この OU で有効になっているオプションコントロールは、アカウントに適用されません。アカウントは一部登録済み状態のままです。

アカウントを完全に登録するには、コンソールで [再登録] または [アカウントの更新] を選択します。コンソールからこれらのオペレーションを選択すると、AWS Control Tower は、その OU に対してアクティブ化されるオプションコントロールも含めて、その OU のすべてのリソースを新しく登録されたアカウントに適用します。

AWS Control Tower コンソールとベースラインの API でのオペレーションの相違点

OU のガバナンスステータスを変更する場合、AWS Control Tower コンソールは、ベースラインの API を使用してガバナンスを変更する場合と比べて、より多くのオペレーションを自動的に実行します。

相違点

- 登録とプロビジョニング済み製品

  コンソールを介して OU を登録すると、AWS Control Tower は各アカウントの登録の一環として、OU のメンバーアカウント用に Service Catalog 製品を作成します。`EnableBaseline` API と `AWSControlTowerBaseline` を使用して OU を登録すると、AWS Control Tower は OU のメンバーアカウント用にプロビジョニング済み製品を作成しません。

- OU の登録解除

  OU の登録を解除するときは、まずすべてのメンバーアカウントとネストされた OU を削除する必要があります。その後、OU に適用されているすべてのコントロールを AWS Control Tower が削除します。

  - コンソールから OU の [削除] を選択すると、AWS Control Tower は登録解除に進み、組織から OU を削除します。
  - 一方、`DisableBaseline` API を呼び出して OU から `AWSControlTowerBaseline` を削除することで OU を登録解除しても、AWS Control Tower は組織から OU を削除せず、OU は未登録のまま組織内に残ります。

ベースラインとバージョニングのデフォルト

AWS Control Tower のランディングゾーンが既に設定されている場合に、ランディングゾーンのベースラインの有効化を選択すると、AWS Control Tower はランディングゾーンのバージョンと互換性のある最新バージョンのベースラインを有効にします。まだ AWS Control Tower に登録されていない OU に対してベースラインの有効化を選択すると、AWS Control Tower は互換性のある最新バージョンのベースラインをその OU に自動的に提供します。

OU ベースラインとランディングゾーンバージョンの互換性

AWS Control Tower ベースラインを使用すると、ビジネスで必要な場合、ランディングゾーンレベルではなく OU レベルでガバナンス標準を設定できます。と呼ばれるベースライン`AWSControlTowerBaseline`は、 OUsを AWS Control Tower に登録するのに役立ちます。

> **Note**
>
> ベースラインとは、ランディングゾーン内に安定したガバナンス環境を確立するために連携するコントロールとリソースのグループです。

OU でベースラインを有効にする場合、AWSControl Tower `EnableBaseline`APIで を呼び出すことで、現在の AWS Control Tower ランディングゾーンバージョンと互換性のあるベースラインバージョンを指定する必要があります。ベースラインを指定すると、OU 内のすべてのメンバーアカウントが OU に指定されたベースラインに従います。つまり、新しいアカウントは更新されたベースラインでプロビジョニングされ、既存のメンバーアカウントは新しいベースラインに従って管理されるようになります。

既存の アカウントOUsと アカウントのベースラインを選択しない場合、ランディングゾーンのバージョンによって、デフォルトでガバナンス体制全体が決まります。ただし、ランディングゾーンに登録された各 OU にはベースラインバージョンが割り当てられています。これは、現在のランディングゾーンバージョンと互換性のある最新のベースラインです。したがって、特にベースラインを割り当てなくても、OU と登録済みのメンバーアカウントにはそれぞれベースラインが関連付けられています。

OU レベルのベースライン についてはAWSControlTowerBaseline、次の表に、ベースラインと AWS Control Tower ランディングゾーンのバージョンとの互換性を示します。

ベースラインバージョン	ランディングゾーンバージョン	含まれるブループリント	含まれるコントロール	以前のベースラインからの変更	
1.0	2.0 ~ 2.7	BP_BASELINE_CLOUDTRAIL、BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP__、BP_BASELINE	すべての必須コントロール	[なし]	

ベースラインバージョン	ランディングゾーンバージョン	含まれるブループリント	含まれるコントロール	以前のベースラインからの変更	
		SERVICE_ROLES、IAMリソース			
2.0	2.8 ~ 2.9	BP_BASELINE_CLOUDTRAIL、BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINESERVICE_ROLES、ConfigSLR、IAMリソース	すべての必須コントロール	を使用するための AWS Config サービスにリンクされたロール (SLR) と新しい Config ブループリントを追加 SLR	
3.0	3.0 ~ 3.1	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINESERVICE_ROLES、ConfigSLR、IAMリソース	すべての必須コントロール	新しい AWS Config 設計図。グローバルリソースをホームリージョンでのみ記録するように変更。CloudTrail ブループリントの削除	

ベースラインバージョン	ランディングゾーンバージョン	含まれるブループリント	含まれるコントロール	以前のベースラインからの変更	
4.0	3.2 ~ 3.3	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICELINKED_ROLE、BP_BASELINESERVICE_ROLES_、Config SLR、IAMリソース	すべての必須コントロール	新しいSLR設計図	

ランディングゾーンのセットアップ時にアカウントに作成された特定のリソースの詳細については、「Resources created in the shared accounts」を参照してください。

ランディングゾーンを、新しい AWSControlTowerBaseline ベースラインバージョンをサポートするバージョンに更新したときに、新しいランディングゾーンバージョンが既存のベースラインバージョンと互換性がある場合は、OU の状態が [更新が利用できます] に変わります。

- ランディングゾーンが 2.x から 3.x に更新される場合を除き、OU のベースラインをすぐに更新しなくても、アカウントファクトリやその他の機能を引き続き使用できます。
- この OU に登録された新しいアカウントは、ベースラインバージョンが更新されるまで (コンソールでガバナンス機能を拡張するか、 を使用して) 、既存のベースラインバージョンに基づいてリソースを受け取りますUpdateEnabledBaselineAPI。
- ベースラインバージョンを更新すると、その OU 内のすべてのアカウントが新しいベースラインバージョンに基づいてリソースを受け取ります。

> **Note**
>
> AWS Control Tower ランディングゾーンをバージョン 2.X からバージョン 3.X に更新する場合は、アカウントレベルから組織レベルの AWS CloudTrail 証跡への変更によりOUs、 のベースラインバージョンも更新する必要があります。コンソールで、OU のステータスが [更新は必須です] と表示されます。

ベースラインに関する考慮事項

- OU でベースラインの更新が必要な場合は、新しいアカウントをプロビジョニングしたり、既存のアカウントをその OU に登録したりすることはできません。
- ランディングゾーンの更新後、OU のベースラインも更新する場合は、OU を再登録するか、OU のベースラインバージョンをプログラムで更新する必要があります。
- ランディングゾーンとベースラインを組み合わせた場合の利点がすべて得られるように、ご使用のランディングゾーンバージョンと互換性のある最も高いバージョンのベースラインに更新することをお勧めします。例えば、ランディングゾーンバージョン 3.3 に更新した場合、ベースライン 3.0 を引き続き使用できますが、ベースライン 4.0 への更新も行わないと、ランディングゾーンバージョン 3.3 の利点をすべて得ることはできません。
- ベースラインの更新はロールバックできません。
- ベースラインの有効化は、一度に 1 つの OU を対象とします。したがって、親 OU が更新されても、ネストされた は自動的に更新OUsされません。ネストされた を更新する前に、親 OU を更新することをお勧めしますOUs。
- を呼び出すUpdateEnabledBaselineAPIか、コンソールから OU を再登録すると、OU はベースライン更新前に有効だったすべてのコントロールを保持します。
- 複数のベースラインバージョンがランディングゾーンのバージョンと互換性がある場合は、アンマネージド OU でベースラインを有効にする場合は、最新のベースラインバージョンを使用する必要があります。

例: AWS Control Tower OU を APIsのみに登録する

この例によるチュートリアルは、付随的なドキュメントです。説明、注意事項、および詳細については、「ベースラインのタイプ」を参照してください。

前提条件

AWS Control Tower に登録されておらず、登録する既存の OU が必要です。または、更新の目的で再登録する、登録済みの OU が必要です。

OU の登録

1. IdentityCenterBaseline がランディングゾーンに対して有効になっているかどうかを確認します。有効になっている場合は、アイデンティティセンターの有効なベースラインの識別子を取得します。

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. ターゲット OU ARNの を取得します。

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. AWSControlTowerBaseline ベースラインARNの を取得します。

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. ターゲット OU に AWSControlTowerBaseline ベースラインを作成します。

   アイデンティティセンターベースラインが有効になっている場合:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

   アイデンティティセンターベースラインが有効になっていない場合は、次のように *parameters* フラグを省略します。

```

aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

OU の再登録

ランディングゾーンの設定を更新した後、またはランディングゾーンのバージョンを更新した後、再登録OUsして最新の変更を提供する必要があります。関連付けられた EnabledBaseline リソースをリセットすることで、OU をプログラムによって再登録するには、次の手順に従います。

1. 再登録するターゲット OU ARNの を取得します。

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. ターゲット OU ARNのEnabledBaselineリソースの を取得します。

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. 有効なベースラインをリセットします。

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

ベースラインAPIの使用例

このセクションでは、AWSControl Tower ベースライン の入出力パラメータの例を示しますAPIs。

DisableBaseline

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

DisableBaseline の入力:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

DisableBaseline の出力:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
```

```
}
```

DisableBaseline CLI 例：

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

EnableBaseline

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

EnableBaseline の入力:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

EnableBaseline の出力 (新しいリソースを返す):

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}
```

EnableBaseline CLI 例：

この例では、 AWS Control Tower によって管理される Identity Center アクセスに AWS IAM オプトインされたランディングゾーンを持つ AWS Organizations 組織のベースラインを有効にする方法を示します。Identity Center EnabledBaseline識別子を取得するには、 を呼び

出しAPI、Identity Center `ListEnabledBaselines` ベースラインでフィルタリングします。(`arn:aws:controltower:`*`Region`*`::baseline/LN25R72TTG6IGPTQ`)

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

レスポンスには `EnabledBaseline` の詳細が表示されます。この中に識別子が示されています。

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> レスポンスのARN値を書き留めておき、この値をパラメータとして渡し、デフォルトのベースラインを有効にします。

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

ランディングゾーンが IAM Identity Center の AWS Control Tower 管理からオプトアウトされた組織では、 パラメータを指定せずにベースラインを有効にします。

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

GetBaseline

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

GetBaseline の入力:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

GetBaseline の出力:

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

GetBaseline CLI 例 :

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

GetBaselineOperation

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

GetBaselineOperation の入力:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

GetBaselineOperation の出力:

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

GetBaselineOperation CLI 例 :

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

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

GetEnabledBaseline の入力:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

GetEnabledBaseline の出力:

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
```

```
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

GetEnabledBaseline CLI 例：

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

ListBaselines

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

ListBaselines の入力 (オプションの入力を使用):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

ListBaselines の出力:

```
{
    "baselines": [
```

```
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2",
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/3WPD0NA6TJ9AOMU2",
            "name": "BackupCentralVaultBaseline",
            "description": "Sets up central AWS Backup vault in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/H6C5JFCJJ3CPU3J5",
            "name": "BackupManagerBaseline",
            "description": "Sets up delegated admin and AWS Backup Audit Manager."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/APO9ATVPBKFRRGLK",
            "name": "BackupBaseline",
            "description": "Sets up local Backup vault and attach Backup policy."
        }
    ]
}
```

ListBaselines CLI 例：

```
aws controltower list-baselines \
    --region us-west-2
```

ListEnabledBaselines

ListEnabledBaselines API には、OU のメンバーであるアカウントに適用されるベースラインを表示できるオプションのパラメータがあります。次の例は、アカウントのベースラインを表示するために使用できるCLIコマンドを示しています。 AWSControl Tower は、これらのベースラインを参照します。これらのベースラインは OU で有効になっていますが、OU に適用されているベースラインからガバナンス設定を取得するため、子が有効なベースラインとして OU 内の各アカウントに適用されます。

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

ListEnabledBaselines 子が有効なベースラインを表示する入力：

```
aws controltower list-enabled-baselines --include-children
```

ListEnabledBaselines 子が有効なベースラインを表示する出力：

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XO2UQ1PC6BB5085S5",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "statusSummary": {
                "lastOperationIdentifier": "07d6d2b8-e357-4f96-ba00-98ea88143445",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:ou/o-vaex10vaey/
ou-k86y-ld9k8vpu"
        },
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XAFPKQQXOJB50ZWQH",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
```

```
            "parentIdentifier": "arn:aws:controltower:us-
east-1:666355521292:enabledbaseline/XOIZ4G08CWB50ZWON",
            "statusSummary": {
                "lastOperationIdentifier": "3508793e-48c8-4895-965b-3dc6abd52b6b",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:account/o-
vaex10vaey/183295447314"
        }
]
```

> **Note**
>
> 前の例では、 parentIdentifierフィールドには、この子が有効なベースラインの親 OU の有効なベースラインが表示されます。

特定のターゲット (OU またはアカウント) に適用されているすべてのベースラインを表示します。

```
aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["TARGET_ARN"]
    }
```

特定のベースラインOUsを持つすべての を表示します。

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'
```

特定のベースラインを持つすべての OUs およびアカウントを表示します。

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'  \
    --include-children
```

ベースライン B が有効になっている OU 内のすべてのアカウントを表示します。

```
### First fetch the enabled baseline record for Baseline B on the OU
 aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["OU_TARGET_ARN"],
        "baselineIdentifiers": ["BASELINE_ARN_FOR_BASELINE_B"]
    }'

### Call ListEnabled baseline to fetch all accounts that have their parent as the
 enabled baseline record on the OU
aws controltower list-enabled-baselines \
    --filter '{
        "parentIdentifiers": ["ENABLED_BASELINE_ARN_FOR_OU"]
    }' \
    --include-children
```

子が有効なベースラインの詳細

- を使用してGetEnabledBaselineAPI、特定の子が有効なベースラインに関する詳細情報を表示できます。
- を使用してGetBaselineOperationAPI、子が有効なベースラインで実行されたオペレーションを表示できます。
- 子が有効なベースラインDisableBaselineではAPIs、EnableBaseline、UpdateEnabledBaseline、 ResetEnabledBaseline などの書き込み を直接呼び出すことはできません。
- 子が有効なベースラインリソースは、AWSControl Tower サービス、親 OU で実行されるオペレーション、または Account Factory によってのみ変更できます。

フィルターの使用例 :

ListEnabledBaselines の入力 (フィルターなし):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines の入力 (baselineIdentifiers フィルターのみ):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines の入力 (targetIdentifiers フィルターのみ):

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

ListEnabledBaselines の入力 (baselineIdentifiers および targetIdentifiers フィルター):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines の出力:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
```

```
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

CLI 1 種類のフィルター (baselineIdentifiers フィルター): の例

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

CLI 複数のフィルター (baselineIdentifiers および targetIdentifiers フィルター) を使用した の例：

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
```

```
    --region us-west-2
```

ResetEnabledBaseline

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

ResetEnabledbaseline の入力:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

ResetEnabledBaseline の出力:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

ResetEnabledBaseline CLI 例 :

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

UpdateEnabledBaseline

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

UpdateEnabledBaseline の入力:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
```

```
        }
    ]
}
```

UpdateEnabledBaseline の出力:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

UpdateEnabledBaseline CLI 例 :

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

追加情報とリンク

このトピックには、関連するブログ投稿、技術ドキュメント、および AWS Control Tower の使用に役立つ関連情報へのリンクが含まれています。ソースには、AWSControl Tower 機能の一般的なユースケースとベストプラクティス、およびいくつかの追加機能強化が含まれています。

チュートリアルとラボ

- AWS Control Tower ラボ – これらのラボでは、AWSControl Tower に関連する一般的なタスクの概要を説明します。
- AWS Control Tower ダッシュボードで、ユースケースを念頭に置いていてもどこから始めるべきかわからない場合は、パーソナライズされたガイダンスの取得を選択します。
- AWS Control Tower の機能の使用方法について詳しく説明する厳選された YouTube 動画リストをご覧ください。

ネットワーク

でネットワークの繰り返し可能なパターンと管理可能なパターンを設定します AWS。お客様によく使用される設計、オートメーション、およびアプライアンスの詳細について確認します。

- AWS クイックスタートVPCアーキテクチャ — このクイックスタートガイドは、 AWS クラウドインフラストラクチャの AWS ベストプラクティスに基づくネットワーク基盤を提供します。 AWS サービスやその他のリソースを起動できるパブリックサブネットとプライベートサブネットを持つ AWS Virtual Private Network 環境を構築します。
- AWS Service Catalog を使用した AWS Control Tower VPCsのセルフサービス – このブログ記事では、カスタマイズされた でアカウントをプロビジョニングできるように Account Factory を設定する方法について説明しますVPCs。
- AWS Control Tower での Serverless Transit Network Orchestrator (STNO) の実装 – このブログ記事では、アカウント間のネットワーク接続アクセスを自動化する方法を示します。このブログは、AWSControl Tower 管理者、または環境内のネットワークの管理を担当する管理者を対象としています AWS 。

セキュリティ、アイデンティティ、ログ記録

セキュリティ体制を拡張し、外部または既存のアイデンティティプロバイダーと統合して、ログ記録システムを一元管理します。

セキュリティ

- AWS Control Tower ライフサイクルイベントによる AWS Security Hub アラートの自動化 – このブログ記事では、既存および新規のアカウントで AWS Control Tower マルチアカウント環境で Security Hub の有効化と設定を自動化する方法について説明します。
- 有効化 AWS Identity and Access Management — このブログ記事では、IAMAccess Analyzer の検出結果を有効にして一元化することで、組織のセキュリティの可視性を高める方法について説明します。
- AWS Systems Manager パラメータストアは、設定データ管理とシークレット管理のための安全な階層型ストレージを提供します。これを使用して、AWSSystems Manager および で使用する設定情報を安全な場所で共有できますAWS CloudFormation。例えば、適合パックをデプロイするリージョンのリストを保存できます。

アイデンティティ

- Azure AD ユーザー ID をシングルサインオン用の AWS アカウントとアプリケーションにリンクする – このブログ記事では、IAMIdentity Center と AWS Control Tower で Azure AD を使用する方法について説明します。
- で Okta ユーザーの へのアクセスをAWS一元管理する AWS IAM Identity Center – このブログ記事では、IAMIdentity Center と AWS Control Tower で Okta を使用する方法について説明します。

ログ記録

- AWS 集中ロギングソリューション – このソリューションの投稿では、組織が複数のアカウント AWS とリージョン AWS で のログを収集、分析、表示できるようにする集中ロギングソリューションについて説明しています。

リソースのデプロイとワークロードの管理

リソースとワークロードをデプロイして管理します。

- 入門ライブラリ統合 - このブログ記事では、使用できる入門ポートフォリオについて説明しています。
- AWS Control Tower へのクラウドカストディアンの継続的なデプロイ

既存の組織とアカウントの操作

既存の AWS 組織とアカウントを使用します。

- アカウントの登録 – このユーザーガイドトピックでは、既存の AWS アカウントを AWS Control Tower に登録する方法について説明します。
- AWS Control Tower でアカウントを使用する – このブログ記事では、既存の AWS 組織に AWS Control Tower をデプロイする方法について説明します。
- Config コンフォーマンスパックを使用して AWS Control Tower AWS ガバナンスを拡張する – このブログ記事では、コンフォーマンスパックをデプロイ AWS Config して、既存のアカウントと組織を AWS Control Tower によるガバナンスに導入する方法について説明します。
- AWS Control Tower でガードレール違反を検出して軽減する方法 – このブログ記事では、コントロールを追加する方法と、コントロールコンプライアンス違反を E メールで通知できるように SNS通知をサブスクライブする方法について説明します。

オートメーションと統合

アカウントの作成を自動化し、ライフサイクルイベントを AWS Control Tower と統合します。

- ライフサイクルイベント — このブログ記事では、 AWS Control Tower でライフサイクルイベントを使用する方法について説明します。
- アカウント作成の自動化 – このブログ記事では、AWSControl Tower で自動アカウント作成を設定する方法について説明します。
- Amazon VPC フローログの自動化 – このブログ記事では、Amazon VPC Flow Logs を自動化してマルチアカウント環境で一元化する方法について説明します。
- AWS Control Tower ライフサイクルイベントによるVPCタグ付けの自動化 – このブログ記事では、AWSControl Tower のライフサイクルイベントを使用してVPCs、 のリソースタグ付けを自動化する方法について説明します。
- 自動アカウント管理 – このブログ記事では、AWSControl Tower 環境のセットアップ後にアカウント管理タスクを自動化する方法について説明します。

ワークロードの移行

AWS Control Tower で他の AWS サービスを使用して、ワークロードの移行を支援します。

- CloudEndure 移行 – このブログ記事では、 CloudEndure およびその他の AWS サービスを AWS Control Tower と組み合わせてワークロードの移行を支援する方法について説明します。

関連する AWS のサービス

AWS Control Tower は、オーケストレーションレイヤーとして機能します AWS Organizations。したがって、AWSOrganizations コンソールと を使用してAPIs、AWSControl Tower と連携する 20 を超える他のAWSサービスにアクセスできます。これらの追加サービスは、AWSControl Tower コンソールから直接アクセスすることはできません。

- Organizations によって AWS Control Tower で使用できるサービスの完全なリストについては、AWSOrganizationAWSAWSs で使用できるサービスを参照してください。
- これらの関連AWSサービスでマルチアカウント機能を有効にするには、信頼されたアクセスを有効にする必要があります。詳細については、「他の AWSサービスでの AWS Organizations の使用」を参照してください。

> **Note**
>
> Identity Center と AWS CloudTrail は Control Tower AWS でセットアップされ AWS Config、完全に統合されています AWS IAM。これらのサービスのために信頼されたアクセスや委任管理設定を変更する必要はありません。

- Systems AWS Manager や AWS Firewall Manager など、 で利用できる AWS 一部のサービスでは、委任された管理 AWS Organizations を使用できます。詳細については、「Configuring a Delegated Administrator」 (委任管理の設定) および「Enabling a delegated administrator account for Firewall Manager」 (Firewall Manager 用の委任管理者アカウントの有効化) を参照してください。このビデオAWS「Firewall Manager でセキュリティグループを設定する」も参照してください。

AWS Marketplace ソリューション

のソリューションをご覧ください AWS Marketplace。

- AWS Control Tower Marketplace – AWS Control Tower には、サードパーティー製ソフトウェアの統合に役立つ幅広いソリューション AWS Marketplace が用意されています。これらのソリューションは、ID 管理、マルチアカウント環境のセキュリティ、一元化されたネットワーク、運用インテリジェンス、セキュリティ情報とイベント管理 () などの主要なインフラストラクチャと運用のユースケースを解決するのに役立ちますSIEM。

AWS Control Tower リリースノート

以下のセクションでは、AWS Control Tower ランディングゾーンの更新が必要な AWS Control Tower のリリースと、このサービスに自動的に組み込まれているリリースの詳細を示します。

機能およびリリースは、公式に発表された日付を基準として新しい順 (最新が最初) に記載されています。機能またはリリースが文書化されたときの日付と公式に発表されたときの日付の間にタイムラグが生じている可能性があるため、ここで機能またはリリースに対して記載されている日付は、「ドキュメント履歴」の日付と多少異なっている場合があります。

2025 年 1 月 - 現在

2025 年 1 月以降、AWS Control Tower は次の更新をリリースしました。

2024 年 1 月 ~ 12 月

2024 年、AWS Control Tower は次の更新をリリースしました。

- AWS Control Tower CfCT が GitHub と RCPsをサポート
- AWS Control Tower が宣言ポリシーによる予防コントロールを追加
- AWS Control Tower が規範的なバックアッププランオプションを追加
- AWS Control Tower は AWS Config コントロールを統合します

- AWS Control Tower がフック管理を改善し、プロアクティブコントロールリージョンを追加
- AWS Control Tower がマネージドリソースコントロールポリシーを起動
- AWS Control Tower がコントロールポリシードリフトをレポートする
- 新しい `ResetEnabledControl` API
- カタログ更新 `GetControl` API を制御する
- AWS Control Tower AFT が GitLab をサポート
- AWS Control Tower が AWS アジアパシフィック (マレーシア) リージョンで利用可能に
- AWS Control Tower が OU あたり最大 1000 アカウントをサポート
- AWS Control Tower でランディングゾーンバージョンの選択が可能に
- 記述的なコントロール API が利用可能になり、リージョンとコントロールへのアクセスが拡大
- AWS Control Tower がオプトインリージョンで AFT と CfCT をサポート
- AWS Control Tower に `ListLandingZoneOperations` API を追加
- AWS Control Tower が最大 100 の同時コントロールオペレーションをサポート
- AWS Control Tower が AWS のカナダ西部 (カルガリー) で利用可能に
- AWS Control Tower がセルフサービスのクォータ調整をサポート
- AWS Control Tower の「Controls Reference Guide」をリリース
- AWS Control Tower で 2 つのプロアクティブコントロールを更新し、名前を変更
- 非推奨のコントロールが使用不可に
- AWS Control Tower が でのEnabledControlリソースのタグ付けをサポート AWS CloudFormation
- AWS Control Tower がベースラインを使用した OU 登録と設定用の API をサポート

AWS Control Tower CfCT が GitHub と RCPsをサポート

2024 年 12 月 9 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower のカスタマイズ (CFCT) 用のサードパーティーバージョン管理システム (VCS) と設定ソースのオプションとして GitHub™ TMをサポートするようになりました。詳細については、「設定ソース GitHub として を設定する」を参照してください。

AWS Control Tower は、AWS Control Tower (CFCT) のカスタマイズのリソースコントロールポリシー (RCPs) をサポートするようになりました。詳細については、「CfCT カスタマイズガイド」を参照してください。

AWS Control Tower が宣言ポリシーによる予防コントロールを追加

2024 年 12 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、宣言ポリシーによって実装される予防コントロールをサポートするようになりました AWS Organizations。宣言型ポリシーは、サービスレベルで直接適用されます。このアプローチにより、サービスによって新機能や APIs が導入された場合でも、指定された設定が適用されます。詳細については、「宣言ポリシーで実装されるコントロール」を参照してください。

AWS Control Tower が規範的なバックアッププランオプションを追加

2024 年 11 月 25 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、データのバックアップと復旧のワークフローをランディングゾーンに直接組み込める規範的な AWS Backup プランがサポートされるようになりました。バックアッププランには、保持日数、バックアップ頻度、バックアップが発生する時間枠などの事前定義されたルールが含まれています。これらのルールは、管理対象 AWS メンバーアカウント全体でリソースをバックアップする方法を定義します。ランディングゾーンにバックアッププランを適用すると、AWS Control Tower は、プランがすべてのメンバーアカウントで一貫しており、 AWS Backup からのベストプラクティスの推奨事項と一致していることを確認します。

詳細については、AWS 「バックアップと AWS Control Tower」を参照してください。

AWS Control Tower は AWS Config コントロールを統合します

2024 年 11 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、選択した AWS Config コントロールが統合されているため、AWS Control Tower で表示および管理できます。

詳細については、「AWS Control Tower で利用可能な統合 AWS Config コントロール」を参照してください。

AWS Control Tower がフック管理を改善し、プロアクティブコントロールリージョンを追加

2024 年 11 月 20 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

このリリースでは、プロアクティブコントロール用にデプロイされたフックは AWS Control Tower によって管理されます。また、プロアクティブコントロールは、カナダ西部 (カルガリー) リージョンとアジアパシフィック (マレーシア) リージョンで利用できます。

以前は、AWS Control Tower はプロアクティブコントロール機能の AWS CloudFormation フックに依存していました。その結果、デプロイされたフックは保護され、AWS Control Tower のみが変更できるようになりました。このリリースでは、プロアクティブコントロールによってデプロイされたフックは AWS Control Tower サービスによって管理されます。独自のフックを作成できますが、AWS Control Tower のプロアクティブコントロールの利点はそのままです。

現在プロアクティブコントロールをデプロイしている場合は、この改善されたフック機能に移行できます。これを行うには、`ResetEnabledControl`API を呼び出すか、コンソールからリセット機能でコントロールを更新して、各 OU でアクティブなプロアクティブコントロールをリセットします。このタスクを実行すると、AWS Control Tower はプロアクティブコントロールフックを新しい機能に移動し、フックは AWS Control Tower によって直接管理されます。

また、プロアクティブコントロールをリセットした後、他の目的で使用しない場合は、CT.CLOUDFORMATION.PR.1 コントロールを削除できます。このコントロールは、 AWS CloudFormation フックを保護するために必要でした。

AWS Control Tower がマネージドリソースコントロールポリシーを起動

2024 年 11 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、リソースコントロールポリシー (RCPs) で実装された新しいタイプの予防コントロールを提供します。これらのコントロールは、AWS Control Tower 環境全体でデータ境界を確立し、意図しないアクセスからリソースを保護するのに役立ちます。

例えば、Amazon S3、、Amazon SQS AWS Security Token Service AWS Key Management Service、および AWS Secrets Manager サービスの RCP ベースのコントロールを有効にできます。RCP ベースのコントロールは、個々のバケットポリシーに付与されたアクセス許可に関係なく、「組織の Amazon S3 リソースが、組織に属する IAM プリンシパルまたは AWS サービスによってのみアクセス可能であることを要求」などの要件を適用できます。

新しい RCP ベースのコントロールと特定の既存の SCP ベースの予防コントロールを設定して、プリンシパルとリソースの AWS IAM 免除を指定できます。プリンシパルまたはリソースをコントロールによって管理しない場合は、免除を設定できます。

AWS Control Tower で予防コントロール、プロアクティブコントロール、検出コントロールを組み合わせることで、マルチアカウント AWS 環境が AWS Foundational Security Best Practices 標準などのベストプラクティスに従ってセキュアで管理されているかどうかをモニタリングできます。

これらの新しい RCP ベースの予防コントロールは、AWS Control Tower AWS リージョン が利用可能な で使用できます。AWS Control Tower が利用可能な AWS リージョン の完全なリストについては、 AWS リージョン 表を参照してください。

AWS Control Tower がコントロールポリシードリフトをレポートする

2024 年 11 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、リソースコントロールポリシー (RCPs) で実装されたコントロール、および Security Hub サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールについて、コントロールポリシーのドリフトを報告するようになりました。このタイプのドリフトは、新しい `ResetEnabledControl` API を使用して修正できます。詳細については、「Types of governance drift」を参照してください。

新しい **`ResetEnabledControl`** API

2024 年 11 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、コントロールドリフトをプログラムで管理するための新しい API を発表しました。コントロールドリフトを修復し、コントロールを意図した設定にリセットできます。`ResetEnabledControl` API は、強く推奨されるコントロールや選択的コントロールなど、オプションの AWS Control Tower コントロールで動作します。

コントロールの例外

- サービスコントロールポリシー (SCPs) で実装されたコントロールは、この API ではリセットできません。詳細については、「ResetEnabledControl」を参照してください。
- 必須コントロールは AWS Control Tower リソースを保護するため、リセットできません。
- ランディングゾーンのリージョン拒否コントロールは、コンソールからリセットする必要があります。

コントロールドリフトは、 AWS Organizations コンソールなどから AWS Control Tower のコントロールが AWS Control Tower の外部で変更されたときに発生します。ドリフトを解決することで、ガバナンス要件のコンプライアンスを確保できます。

カタログ更新 **GetControl** API を制御する

2024 年 11 月 8 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、すべてのコントロールのタイプと設定可能な特定のコントロールImplementationのタイプという 2 つの新しいフィールドを含む更新された GetControl API Parameters をサポートするようになりました。

GetControl API は AWS Control Tower controlcatalogの名前空間の一部です。

詳細については、「 Control Catalog GetControl API リファレンス」の「 API」を参照してください。

このリリースには、AWS Control Tower コンソールに表示される関連する変更が含まれています。

- 既存のコントロールはすべて AWS Security Hub Implementation、パラメータ値を AWS Config ルールからルールに変更します AWS Security Hub。対応するコンソールのヘルプパネルは、この変更を反映するように変更されています。
- 既存のフックコントロールはすべて、Implementationパラメータ値を AWS CloudFormation ガードルールから AWS CloudFormation フックに変更します。対応するコンソールのヘルプパネルは、この変更を反映するように変更されています。

AWS Control Tower AFT が GitLab をサポート

2024 年 10 月 23 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、Account Factory for Terraform (AFT) のサードパーティーバージョン管理システム (VCS) と設定ソースのオプションとして、GitLabTM™ と GitLab セルフマネージドをサポートするようになりました。

AWS Control Tower が AWS アジアパシフィック (マレーシア) リージョンで利用可能に

2024 年 10 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が AWS のアジアパシフィック (マレーシア) リージョンで利用可能になりました。

AWS Control Tower を使用できるリージョンの全リストについては、「AWS リージョン別のサービス表」を参照してください。

AWS Control Tower が OU あたり最大 1000 アカウントをサポート

2024 年 8 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、組織単位 (OU) あたりの最大許容アカウント数が 300 から 1000 に引き上げられました。これで、OU 構造を変更することなく、一度に最大 1000 AWS アカウント を AWS Control Tower ガバナンスに登録できます。OU の登録プロセスと再登録プロセスも効率化されたため、AWS Control Tower ベースラインリソースをアカウントにデプロイする際の所要時間が大幅に短縮されます。

利用可能な AWS CloudFormation スタックセットの数に制限があるため、一部のアカウントの制限が引き続き適用されます。具体的には、OU に登録できるアカウントの最大数は、管理下に置いているリージョンの数によって変わることがあります。詳細については、AWS Control Tower ユーザーガイドの基盤となる AWS サービスに基づく制限を参照してください。AWS Control Tower を使用できる AWS リージョン の完全なリストについては、「AWS リージョン 別のサービス表」を参照してください。

AWS Control Tower でランディングゾーンバージョンの選択が可能に

2024 年 8 月 15 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower ランディングゾーンバージョン 3.1 以降を実行している場合は、現在のバージョンのままでランディングゾーンを更新または修復することも、選択したバージョンにアップグレードすることもできます。これまで、ランディングゾーンを更新または修復するには、最新のランディングゾーンバージョンにアップグレードする必要がありました。

ランディングゾーンバージョンを選択することで、環境に加えられる可能性のある変更を評価しながら、バージョンのアップグレードをより柔軟に計画できます。ドリフトを修復してコンプライアンスを維持するか、ランディングゾーン設定を更新するか、最新のランディングゾーンバージョンにアップグレードするかを選択する必要はありません。ランディングゾーンバージョン 3.1 以降を実行している場合は、ランディングゾーン設定を更新またはリセットするときに、現在のバージョンを維持するか、新しいバージョンにアップグレードするかを選択できます。

記述的なコントロール API が利用可能になり、リージョンとコントロールへのアクセスが拡大

2024 年 8 月 6 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、利用可能なコントロールの詳細情報をプログラムで確認するのに役立つ新しい API オペレーションが 2 つ追加されました。この機能により、自動化を使用したコントロールのデプロイが容易になります。

- `GetControl` API は、ターゲット識別子、コントロール情報の概要、ターゲットリージョンのリスト、ドリフトステータスなど、有効なコントロールの詳細を返します。
- `ListControls` API は、AWS Control Tower のコントロールライブラリで使用可能なすべてのコントロールのページ分割されたリストを返します。

これらの API には、AWS Control Catalog 名前空間を介してアクセスします。 AWS Control Catalog は AWS Control Tower の一部であり、AWS Control Tower だけでなく、他の AWS のサービスの管理に役立つコントロールが含まれています。この拡張されたカタログは、複数の AWS サービスのコントロールを統合するため、セキュリティ、コスト、耐久性、オペレーションなどの一般的なユースケースに従って AWS コントロールを表示できます。詳細については、「Control Catalog API Reference」を参照してください。

リージョンの可用性の拡大

このリリース以降、AWS Control Tower ガバナンスを、(既に) 有効になっているコントロールの一部が利用できない AWS リージョン に拡張できます。また、管理対象リージョンの一部でコントロールがサポートされていない場合でも、より多くのリージョンで特定のコントロールを有効にできるようになりました。

これまで、AWS Control Tower では、有効なコントロールと管理対象リージョンのすべてで一貫性が維持されていなければ、ガバナンスをリージョンに拡張したり、コントロールを有効にしたりすることはできませんでした。このリリースでは、すべての有効なコントロールとすべての管理対象リージョンに対して設定が正しいことをより柔軟に責任を持って確認できます。AWS Control Tower コントロール APIs とコントロールカタログ APIs は、有効なコントロールで保護されている AWS リージョンと、追加のコントロールをデプロイできるリージョンに関する情報を取得するのに役立ちます。リージョンとコントロールの情報は、AWS Control Tower コンソールでも確認できます。

AWS Control Tower がオプトインリージョンで AFT と CfCT をサポート

2024 年 7 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

現在、AWS Control Tower カスタマイズフレームワーク Account Factory for Terraform (AFT) と Customizations for AWS Control Tower (CfCT) は、 AWS リージョンアジアパシフィック (ハイデラバード、ジャカルタ、大阪) 、イスラエル (テルアビブ) 、中東 (アラブ首長国連邦) の 5 つの追加で利用できます。

Account Factory for Terraform (AFT) は、AWS Control Tower でアカウントのプロビジョニングとカスタマイズに役立つ Terraform パイプラインを設定します。AWS Control Tower (CfCT) のカスタマイズは、 AWS CloudFormation テンプレートとサービスコントロールポリシー (SCPs) を使用して AWS Control Tower ランディングゾーンとアカウントをカスタマイズするのに役立ちます。

詳細については、「AWS Control Tower User Guide」の Account Factory for Terraform と AWS Control Tower のカスタマイズのページを参照してください。AFT の GitHub ページと CfCT の GitHub ページでリリースノートを確認することもできます。AFT と CfCT は、一部の例外を除き、すべての AWS リージョンでサポートされています。詳細については、「Region limitations」を参照してください。

AWS Control Tower に **`ListLandingZoneOperations`** API を追加

2024 年 6 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower に、ランディングゾーンに最近適用されたオペレーションと現在進行中のオペレーションのリストを取得できる API が追加されました。この API は、最大で 90 日分のランディングゾーンオペレーションとその識別子の履歴を返すことができます。使用例については、「View the status of your landing zone operations」を参照してください。

`ListLandingZoneOperations` API の詳細については、「AWS Control Tower API Reference」の「`ListLandingZoneOperations`」を参照してください。

AWS Control Tower が最大 100 の同時コントロールオペレーションをサポート

2024 年 5 月 20 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が同時実行性の高い複数のコントロールオペレーションをサポートするようになりました。コンソールから、または API を使用して、複数の組織単位 (OU) にわたって最大 100 の AWS Control Tower コントロールオペレーションを同時に送信できます。最大 10 のオペレーションを同時に実行でき、追加のオペレーションはキューに入れられます。このようにして、反復的な制御操作による運用上の負担なしに AWS アカウント、複数の にまたがってより標準化された設定をセットアップできます。

進行中のコントロールオペレーションとキューに入れられたコントロールオペレーションのステータスをモニタリングするには、AWS Control Tower コンソールの新しい [最近の業務] ページに移動するか、新しい `ListControlOperations` API を呼び出します。

AWS Control Tower ライブラリには 500 を超えるコントロールが含まれており、さまざまなコントロールの目標、フレームワーク、サービスに対応しています。[保管中のデータを暗号化] などの特定のコントロールの目標については、1 つのコントロールオペレーションで複数のコントロールを有効にして、目標を達成できます。この機能により、開発スピードの向上、ベストプラクティスコントロールの導入の迅速化、運用の複雑さの軽減が可能になります。

AWS Control Tower が AWS のカナダ西部 (カルガリー) で利用可能に

2024 年 5 月 3 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

本日より、カナダ西部 (カルガリー) リージョンで AWS Control Tower をアクティブ化できます。既に AWS Control Tower をデプロイしている場合に、ガバナンス機能をこのリージョンに拡張する

には、AWS Control Tower ランディングゾーン API を使用します。または、コンソールから AWS Control Tower ダッシュボードの [設定] ページに移動し、リージョンを選択して、ランディングゾーンを更新します。

カナダ西部 (カルガリー) リージョンは AWS Service Catalogをサポートしていません。このため、AWS Control Tower の一部の機能が異なります。機能の変更点として最も顕著なのは、Account Factory が利用できないことです。ホームリージョンとしてカナダ西部 (カルガリー) を選択した場合、アカウントの更新、アカウントのオートメーションの設定、および Service Catalog が関係するその他のプロセスが他のリージョンと異なります。

アカウントのプロビジョニング

カナダ西部 (カルガリー) リージョンで新しいアカウントを作成してプロビジョニングする場合は、AWS Control Tower の外部でアカウントを作成し、登録済みの OU に登録することをお勧めします。詳細については、「Enroll an existing account」と「Steps to enroll an account」を参照してください。

Service Catalog API は、カナダ西部 (カルガリー) リージョンでは利用できません。「Automate account provisioning in AWS Control Tower by Service Catalog APIs」に示されているスクリプトの例は機能しません。

Account Factory Customizations (AFC)、Account Factory for Terraform (AFT)、および AWS Control Tower のカスタマイズ (CfCT) は、AWS Control Tower の基盤となる他の依存関係がないため、カナダ西部 (カルガリー) では利用できません。ガバナンスをカナダ西部 (カルガリー) リージョンに拡張する場合、Service Catalog がホームリージョンで利用できる限り、AWS Control Tower がサポートするすべてのリージョンで AFC ブループリントを引き続き管理できます。

コントロール

AWS Security Hub サービスマネージドスタンダード: AWS Control Tower のプロアクティブコントロールとコントロールは、カナダ西部 (カルガリー) リージョンでは利用できません。予防コントロール `CT.CLOUDFORMATION.PR.1` は、フックベースのプロアクティブコントロールのアクティブ化にのみ必要であるため、カナダ西部 (カルガリー) では利用できません。に基づく特定の検出コントロール AWS Config は使用できません。詳細については、「コントロールの制限事項」を参照してください。

ID プロバイダー

IAM アイデンティティセンターは、カナダ西部 (カルガリー) では利用できません。推奨されるベストプラクティスは、IAM アイデンティティセンターが利用可能なリージョンでランディングゾーン

をセットアップすることです。または、カナダ西部 (カルガリー) で外部 ID プロバイダーを使用する場合、アカウントのアクセス設定を自己管理することもできます。

カナダ西部 (カルガリー) リージョンで Service Catalog を使用できない場合でも、AWS Control Tower でサポートされている他のリージョンには影響しません。これらの違いは、ホームリージョンがカナダ西部 (カルガリー) である場合にのみ適用されます。

AWS Control Tower を使用できるリージョンの全リストについては、「AWS リージョン別のサービス表」を参照してください。

AWS Control Tower がセルフサービスのクォータ調整をサポート

2024 年 4 月 25 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が Service Quotas コンソールを通じてセルフサービスのクォータ調整をサポートするようになりました。詳細については、「クォータ引き上げをリクエストする」を参照してください。

AWS Control Tower の「Controls Reference Guide」をリリース

2024 年 4 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower の「Controls Reference Guide」がリリースされました。これは、AWS Control Tower 環境に固有のコントロールに関する詳細情報が記載された新しいドキュメントです。これまで、この資料は「AWS Control Tower User Guide」に含まれていました。「Controls Reference Guide」では、コントロールについて拡張形式で説明しています。詳細については、「AWS Control Tower Controls Reference Guide」を参照してください。

AWS Control Tower で 2 つのプロアクティブコントロールを更新し、名前を変更

2024 年 3 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、Amazon OpenSearch Service の更新に合わせて 2 つのプロアクティブコントロールの名前が変更されました。

- [CT.OPENSEARCH.PR.8] Elasticsearch Service ドメインで TLSv1.2 を使用する必要がある
- [CT.OPENSEARCH.PR.16] Amazon OpenSearch Service ドメインで TLSv1.2 を使用する必要がある

Amazon OpenSearch Service の最近のリリースに合わせて、この 2 つのコントロールのコントロール名とアーティファクトを更新しました。Amazon OpenSearch Service では、ドメインエンドポイントのセキュリティ用のトランスポートセキュリティオプションとして Transport Layer Security (TLS) バージョン 1.3 がサポートされるようになっています。

これらのコントロールでの TLSv1.3 のサポートを追加するために、コントロールのアーティファクトと名前を更新して、コントロールの意図を反映させました。サービスドメインの最小 TLS バージョンが評価されるようになりました。ご使用の環境でこの更新を行うには、コントロールを [無効] にしてから [有効] にして、最新のアーティファクトをデプロイする必要があります。

この変更の影響を受けるその他のプロアクティブコントロールはありません。これらのコントロールを確認して、コントロールの目標が確実に達成されるようにすることをお勧めします。

ご質問やご不明な点がある場合は、AWS サポートにお問い合わせください。

非推奨のコントロールが使用不可に

2024 年 3 月 12 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower でいくつかのコントロールが廃止されました。これらのコントロールは使用できなくなりました。

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower が でのEnabledControlリソースのタグ付けをサポート AWS CloudFormation

2024 年 2 月 22 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

この AWS Control Tower リリースでは、EnabledControl リソースの動作を更新することで、設定可能なコントロールとの連携を強化するとともに、AWS Control Tower 環境をオートメーションによって管理する機能を向上させています。このリリースでは、 AWS CloudFormation テンプレートを使用して設定可能な EnabledControl リソースにタグを追加できます。これまで、タグを追加できたのは AWS Control Tower コンソールと API を使用する場合のみでした。

AWS Control Tower の GetEnabledControl、EnableControl、ListTagsforResource API オペレーションは、EnabledControl リソースの機能を利用しているため、このリリースで更新されます。

詳細については、「Tagging EnabledControl resources in AWS Control Tower」と「AWS CloudFormation User Guide」の「EnabledControl」を参照してください。

AWS Control Tower がベースラインを使用した OU 登録と設定用の API をサポート

2024 年 2 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

これらの API は、EnableBaseline の呼び出しを使用したプログラムによる OU 登録をサポートします。OU でベースラインを有効にすると、OU 内のメンバーアカウントが AWS Control Tower ガバナンスに登録されます。特定の注意事項が適用される場合があります。例えば、AWS Control Tower コンソールを介して OU を登録すると、オプションのコントロールと必須のコントロールが有効になります。API を呼び出す際には、オプションのコントロールが有効になるように追加のステップを実行する必要が生じる場合があります。

AWS Control Tower ベースラインとは、OU とメンバーアカウントの AWS Control Tower ガバナンスのベストプラクティスを具体化したものです。例えば、OU でベースラインを有効にすると、OU 内のメンバーアカウントは、 AWS CloudTrail、IAM アイデンティティセンター AWS Config、必要な AWS IAM ロールなど、定義されたリソースグループを受け取ります。

特定のベースラインは、特定の AWS Control Tower ランディングゾーンバージョンと互換性があります。ランディングゾーン設定を変更する際、AWS Control Tower は互換性のある最新のベースラインをランディングゾーンに適用できます。詳細については、「OU ベースラインとランディングゾーンバージョンの互換性」を参照してください。

このリリースには、基本的なベースラインのタイプが 4 つ含まれています

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

新しい API と定義済みのベースラインを使用すると、OU を登録して、OU のプロビジョニングワークフローを自動化できます。API では、既に AWS Control Tower のガバナンス下にある OU の管理も行えるため、ランディングゾーンの更新後に OU を再登録できます。APIs には リソースのサポート AWS CloudFormation `EnabledBaseline`が含まれており、Infrastructure as Code (IaC) を使用して OUsを管理できます。

ベースライン API

- EnableBaseline、UpdateEnabledBaseline、DisableBaseline: OU のベースラインに対してアクションを実行します。
- GetEnabledBaseline、ListEnabledBaselines: 有効なベースラインの設定を検出します。
- GetBaselineOperation: 特定のベースラインオペレーションのステータスを表示します。
- ResetEnabledBaseline: ベースラインが有効になっている OU のリソースドリフト (ネストされた OU と必須コントロールのドリフトを含む) を修正します。ランディングゾーンレベルのリージョン拒否コントロールのドリフトも修正します。
- GetBaseline、ListBaselines: AWS Control Tower ベースラインの内容を検出します。

これらの API の詳細については、「AWS Control Tower User Guide」の「Baselines」と「API Reference」を参照してください。新しい APIsは、 GovCloud (米国) リージョンを除き、AWS Control Tower が利用可能な AWS リージョン で使用できます。AWS Control Tower が利用可能な AWS リージョン のリストについては、 AWS リージョン 表を参照してください。

2023 年 1 月 ~ 12 月

2023 年、AWS Control Tower は次の更新をリリースしました。

- 新しい AWS Service Catalog External 製品タイプへの移行 (フェーズ 3)
- AWS Control Tower ランディングゾーンバージョン 3.3
- 新しい AWS Service Catalog External 製品タイプへの移行 (フェーズ 2)
- AWS Control Tower がデジタル主権を支援するコントロールを発表
- AWS Control Tower がランディングゾーン API をサポート
- AWS Control Tower が、有効になっているコントロールのタグ付けをサポート
- AWS Control Tower がアジアパシフィック (メルボルン) リージョンで利用可能に
- 新しい AWS Service Catalog External 製品タイプへの移行 (フェーズ 1)
- 新しいコントロール API が利用可能に
- AWS Control Tower が追加のコントロールをリリース
- 新しいドリフトタイプの報告: 信頼できるアクセスの無効化
- 4 つの追加 AWS リージョン
- AWS Control Tower がテルアビブリージョンで利用可能に
- AWS Control Tower が 28 個の新しいプロアクティブコントロールをリリース
- AWS Control Tower で 2 つのコントロールが廃止されます
- AWS Control Tower ランディングゾーンバージョン 3.2
- AWS Control Tower は ID に基づいてアカウントを処理します
- AWS Control Tower コントロールライブラリで使用できるその他の Security Hub 検出コントロール
- AWS Control Tower は、コントロールメタデータテーブルを公開します
- Account Factory のカスタマイズに対する Terraform サポート
- AWS ランディングゾーンで利用可能な IAM アイデンティティセンターの自己管理
- AWS Control Tower は OU の混合ガバナンスに対応
- 追加のプロアクティブコントロールが利用可能に
- Amazon EC2 プロアクティブコントロールの更新
- 7 つの追加 AWS リージョン が利用可能
- Account Factory for Terraform (AFT) アカウントのカスタマイズリクエストの追跡

- AWS Control Tower ランディングゾーンバージョン 3.1
- プロアクティブコントロールの一般公開

新しい AWS Service Catalog External 製品タイプへの移行 (フェーズ 3)

2023 年 12 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、新規作成時に製品タイプ (ブループリント) として Terraform Open Source をサポートしなくなりました AWS アカウント。アカウントブループリントの更新の詳細と手順については、AWS Service Catalog 「外部製品タイプへの移行」を参照してください。

External 製品タイプを使用するようにアカウントブループリントを更新しない場合、Terraform オープンソースブループリントを使用してプロビジョニングしたアカウントの更新または終了のみが可能です。

AWS Control Tower ランディングゾーンバージョン 3.3

2023 年 12 月 14 日

(AWS Control Tower ランディングゾーンをバージョン 3.3 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください)。

AWS Control Tower 監査アカウントの S3 バケットポリシーの更新

AWS Control Tower がアカウントにデプロイする Amazon S3 監査バケットポリシーが変更されました。これにより、すべての書き込みアクセス許可のためには `aws:SourceOrgID` 条件を満たす必要があります。このリリースでは、リクエストが組織または組織単位 (OU) から発信された場合にのみ、 AWS サービスはリソースにアクセスできます。

`aws:SourceOrgID` 条件キーを使用して、S3 バケットポリシーの条件要素で [組織 ID] の値を設定できます。この条件によってのみ、CloudTrail は組織内のアカウントに代わってお客様の S3 バケットへログを書き込めるようになり、組織外の CloudTrail ログによるお客様の AWS Control Tower S3 バケットへの書き込みを防ぎます。

この変更は、既存のワークロードの機能に影響を与えることなく、潜在的なセキュリティ上の脆弱性を修正するために行われました。更新されたポリシーを表示する方法については、「監査アカウントの Amazon S3 バケットポリシー」を参照してください。

新しい条件キーの詳細については、「IAM ドキュメント」と「リソースにアクセスする AWS サービスにスケーラブルなコントロールを使用する」というタイトルの IAM ブログ記事を参照してください。

SNS AWS Config トピックのポリシーの更新

AWS Config SNS topic.To のポリシーに新しいaws:SourceOrgID条件キーを追加しました。更新されたポリシーを表示します。AWS Config 「SNS トピックポリシー」を参照してください。

ランディングゾーンのリージョン拒否コントロールの更新

- discovery-marketplace: を削除しました。このアクションは aws-marketplace:* 除外の対象となります。
- 「quicksight:DescribeAccountSubscription」を追加

AWS CloudFormation テンプレートの更新

AWS KMS 暗号化が使用されていない場合に がドリフトを表示しないようにBASELINE-CLOUDTRAIL-MASTER、 という名前のスタックの AWS CloudFormation テンプレートを更新しました。

新しい AWS Service Catalog External 製品タイプへの移行 (フェーズ 2)

2023 年 12 月 7 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

HashiCorp が Terraform ライセンスを更新しました。その結果、Terraform Open Source 製品とプロビジョニング済み製品のサポートが External という新しい製品タイプ AWS Service Catalog に変更されました。

アカウント内の既存のワークロードと AWS リソースの中断を回避するには、2023 年 12 月 14 日までにAWS Service Catalog 「外部製品タイプへの移行」の AWS Control Tower 移行ステップに従ってください。

AWS Control Tower がデジタル主権を支援するコントロールを発表

2023 年 11 月 27 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、デジタル主権の要件を満たすのに役立つ 65 個の新しい AWSマネージドコントロールを発表しました。このリリースでは、これらのコントロールを AWS Control Tower コンソールの新しいデジタル主権グループで確認できます。これらのコントロールを利用することで、データレジデンシー、きめ細かなアクセス制限、暗号化、レジリエンシー機能に関するアクションを防止したり、リソースの変更を検出したりできます。これらのコントロールは、要件に対して大規模かつ簡単に対応できるように設計されています。デジタル主権コントロールの詳細については、「Controls that enhance digital sovereignty protection」を参照してください。

例えば、転送中の暗号化を有効にする AWS ように AppSync API キャッシュに要求する、複数のアベイラビリティーゾーンにネットワークファイアウォールをデプロイするように要求するなど、暗号化と回復力戦略を適用するのに役立つコントロールを有効にすることができます。 AWS また、AWS Control Tower のリージョン拒否コントロールをカスタマイズして、独自のビジネスニーズに最適なリージョン別の制限を適用することもできます。

このリリースでは、AWS Control Tower のリージョン拒否機能が大幅に強化されています。パラメータ化された新しいリージョン拒否コントロールを OU レベルで適用して、ガバナンスの細分性を高めながら、ランディングゾーンレベルでの追加のリージョンガバナンスを維持できます。このカスタマイズ可能なリージョン拒否コントロールにより、独自のビジネスニーズに最適なリージョン別の制限を適用できます。新しい設定可能なリージョン拒否コントロールの詳細については、「Region deny control applied to the OU」を参照してください。

リージョン拒否の新しい強化ツールとして、このリリースには新しい API、`UpdateEnabledControl` が含まれています。これにより、有効にしたコントロールをデフォルト設定にリセットできます。この API は、ドリフトを迅速に解決する必要がある場合や、コントロールがドリフト状態でないことをプログラムで確認する必要がある場合に特に役立ちます。新しい API の詳細については、「AWS Control Tower API リファレンス」を参照してください。

新しいプロアクティブコントロール

- CT.APIGATEWAY.PR.6: Amazon API Gateway REST ドメインでは TLS プロトコルの最小バージョン TLSv1.2 を指定するセキュリティポリシーを使用する必要があります
- CT.APPSYNC.PR.2: AWS AppSync GraphQL API をプライベート可視性で設定する必要があります
- CT.APPSYNC.PR.3: AWS AppSync GraphQL API が API キーで認証されていないことを要求する
- CT.APPSYNC.PR.4: AWS AppSync GraphQL API キャッシュで転送中の暗号化を有効にする必要があります。
- CT.APPSYNC.PR.5: AWS AppSync GraphQL API キャッシュで保管時の暗号化を有効にする必要があります。

- CT.AUTOSCALING.PR.9: Amazon EC2 Auto Scaling 起動設定を使用して設定した Amazon EBS ボリュームでは、保管中のデータを暗号化する必要があります
- CT.AUTOSCALING.PR.10: 起動テンプレートを上書きするときに、Amazon EC2 Auto Scaling グループが AWS Nitro インスタンスタイプのみを使用するよう要求する
- CT.AUTOSCALING.PR.11: 起動テンプレートを上書きするときに、インスタンス間のネットワークトラフィックの暗号化をサポートする AWS Nitro インスタンスタイプのみを Amazon EC2 Auto Scaling グループに追加する必要があります
- CT.DAX.PR.3: DynamoDB Accelerator クラスターでは Transport Layer Security (TLS) を使用して転送中のデータを暗号化する必要があります
- CT.DMS.PR.2: AWS Database Migration Service (DMS) エンドポイントがソースエンドポイントとターゲットエンドポイントの接続を暗号化する必要がある
- CT.EC2.PR.15: Amazon EC2 インスタンスは、`AWS::EC2::LaunchTemplate` リソースタイプから作成する場合、 AWS Nitro インスタンスタイプを使用する必要があります
- CT.EC2.PR.16: Amazon EC2 インスタンスは、`AWS::EC2::Instance` リソースタイプを使用して作成した場合、 AWS Nitro インスタンスタイプを使用する必要があります
- CT.EC2.PR.17: Amazon EC2 専有ホストでは AWS Nitro インスタンスタイプを使用する必要があります
- CT.EC2.PR.18: Amazon EC2 フリートが AWS Nitro インスタンスタイプの起動テンプレートのみを上書きするように要求する
- CT.EC2.PR.19: Amazon EC2 インスタンスは、`AWS::EC2::Instance` リソースタイプを使用して作成した場合、インスタンス間の転送中の暗号化をサポートする Nitro インスタンスタイプを使用する必要があります
- CT.EC2.PR.20: Amazon EC2 フリートは、インスタンス間の転送中の暗号化をサポートする AWS Nitro インスタンスタイプを持つ起動テンプレートのみを上書きする必要があります
- CT.ELASTICACHE.PR.8: 新しい Redis バージョンの Amazon ElastiCache レプリケーショングループでは RBAC 認証をアクティブにする必要があります
- CT.MQ.PR.1: Amazon MQ ActiveMQ ブローカーでは、高可用性を確保するためにアクティブ/スタンバイデプロイモードを使用する必要があります
- CT.MQ.PR.2: Amazon MQ Rabbit MQ ブローカーでは、高可用性を確保するためにマルチ AZ クラスターモードを使用する必要があります
- CT.MSK.PR.1: Amazon Managed Streaming for Apache Kafka (MSK) クラスターでは、クラスターブローカーノード間の転送中の暗号化を適用する必要があります

- CT.MSK.PR.2: Amazon Managed Streaming for Apache Kafka (MSK) クラスターでは、PublicAccess を無効に設定する必要があります
- CT.NETWORK-FIREWALL.PR.5: Network AWS Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- CT.RDS.PR.26: Amazon RDS DB Proxy は Transport Layer Security (TLS) 接続を要求する必要があります
- CT.RDS.PR.27: Amazon RDS DB クラスターパラメータグループは、サポートしているエンジンタイプのために Transport Layer Security (TLS) 接続を要求する必要があります
- CT.RDS.PR.28: Amazon RDS DB パラメータグループは、サポートしているエンジンタイプのために Transport Layer Security (TLS) 接続を要求する必要があります
- CT.RDS.PR.29: Amazon RDS クラスターは、「PubliclyAccessible」プロパティを使用してパブリックでアクセスできないように設定する必要があります
- CT.RDS.PR.30: Amazon RDS データベースインスタンスでは、サポートしているエンジンタイプのために指定した KMS キーを使用するように保管中の暗号化を設定する必要があります
- CT.S3.PR.12: Amazon S3 のアクセスポイントでは、パブリックアクセスブロック (BPA) 設定のすべてのオプションを true に設定する必要があります

新しい予防コントロール

- CT.APPSYNC.PV.1 AWS AppSync GraphQL API がプライベート可視性で設定されていることを要求する
- CT.EC2.PV.1 Amazon EBS スナップショットは、暗号化した EC2 ボリュームから作成する必要があります
- CT.EC2.PV.2 アタッチした Amazon EBS ボリュームは、保管中のデータを暗号化するように設定する必要があります
- CT.EC2.PV.3 Amazon EBS スナップショットはパブリックに復元できないようにする必要があります
- CT.EC2.PV.4 Amazon EBS direct API が呼び出されないようにする必要があります
- CT.EC2.PV.5 Amazon EC2 VM のインポートとエクスポートの使用を禁止します
- CT.EC2.PV.6 廃止された Amazon EC2 RequestSpotFleet および RequestSpotInstances API アクションの使用を禁止します
- CT.KMS.PV.1 AWS KMS キーポリシーに、 AWS サービスへの AWS KMS 許可の作成を制限するステートメントがあることを要求する

- CT.KMS.PV.2 暗号化に使用される RSA キーマテリアルを持つ AWS KMS 非対称キーのキー長が 2048 ビットでない必要があります
- CT.KMS.PV.3 バイパスポリシーのロックアウト安全チェックを有効にして AWS KMS キーを設定する必要があります。
- CT.KMS.PV.4 AWS KMS カスタマーマネージドキー (CMK) は、 AWS CloudHSM から発信されるキーマテリアルで設定する必要があります
- CT.KMS.PV.5 AWS KMS カスタマーマネージドキー (CMK) がインポートされたキーマテリアルで設定されている必要があります
- CT.KMS.PV.6 AWS KMS カスタマーマネージドキー (CMK) は、外部キーストア (XKS) から発信されるキーマテリアルで設定する必要があります。
- CT.LAMBDA.PV.1 AWS IAM ベースの認証を使用する関数 AWS Lambda URL を要求する
- CT.LAMBDA.PV.2 AWS Lambda 関数 URL は、 内のプリンシパルのみがアクセスできるように設定する必要があります。 AWS アカウント
- CT.MULTISERVICE.PV.1: 組織単位 AWS リージョン にリクエストされた AWS に基づいて へのアクセスを拒否する

デジタル主権ガバナンス体制を強化する新しい委任コントロールは、 AWS Security Hub サービスマネージドスタンダード AWS Control Tower の一部です。

新しい検出コントロール

- SH.ACM.2: ACM が管理する RSA 証明書では、少なくとも 2,048 ビットのキー長を使用する必要があります
- SH.AppSync.5： AWS AppSync GraphQL APIsは API キーで認証しないでください
- SH.CloudTrail.6: CloudTrail ログの保存に使用する S3 バケットは、パブリックアクセス可能でないことを確認します
- SH.DMS.9: DMS エンドポイントでは SSL を使用する必要があります
- SH.DocumentDB.3: Amazon DocumentDB 手動クラスタースナップショットは公開できません
- SH.DynamoDB.3: DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- SH.EC2.23: EC2 Transit Gateway は VPC アタッチメントリクエストを自動的に受け入れないようにする必要があります
- SH.EKS.1: EKS クラスターエンドポイントはパブリックアクセス可能にしない必要があります

- SH.ElastiCache.3: ElastiCache レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- SH.ElastiCache.4: ElastiCache レプリケーショングループでは、保管中の暗号化を有効にする必要があります
- SH.ElastiCache.5: ElastiCache レプリケーショングループでは、転送中の暗号化を有効にする必要があります
- SH.ElastiCache.6: 以前の Redis バージョンの ElastiCache レプリケーショングループでは、Redis AUTH を有効にする必要があります
- SH.EventBridge.3: EventBridge カスタムイベントバスには、リソースベースのポリシーをアタッチする必要があります
- SH.KMS.4： AWS KMS key ローテーションを有効にする必要があります
- SH.Lambda.3: Lambda 関数は VPC 内に存在する必要があります
- SH.MQ.5: ActiveMQ ブローカーは、アクティブ/スタンバイデプロイモードを使用する必要があります
- SH.MQ.6: RabbitMQ ブローカーは、クラスターデプロイモードを使用する必要があります。
- SH.MSK.1: MSK クラスターは、ブローカーノード間で転送中に暗号化する必要があります
- SH.RDS.12: IAM 認証は RDS クラスター用に設定する必要があります
- SH.RDS.15: RDS DB クラスターは、複数のアベイラビリティーゾーンで設定する必要があります
- SH.S3.17: S3 バケットは、 AWS KMS キーを使用して保管中に暗号化する必要があります

AWS Security Hub サービスマネージドスタンダード AWS Control Tower に追加されたコントロールの詳細については、 AWS Security Hub ドキュメントの「サービスマネージドスタンダード: AWS Control Tower に適用されるコントロール」を参照してください。

AWS Security Hub サービスマネージドスタンダード AWS Control Tower の一部である特定のコントロールをサポート AWS リージョン していない のリストについては、「サポートされていないリージョン」を参照してください。

OU レベルでのリージョン拒否用の新しい設定可能なコントロール

CT.MULTISERVICE.PV.1: このコントロールは、AWS Control Tower のランディングゾーン全体ではなく、OU レベルで許可される除外リージョン、IAM プリンシパル、アクションを指定するパラメータを受け入れます。これは予防コントロールであり、サービスコントロールポリシー (SCP) によって実装されます。

詳細については、「Region deny control applied to the OU」を参照してください。

`UpdateEnabledControl` API

この AWS Control Tower リリースでは、コントロール用の次の API サポートを追加しています。

- 更新された `EnableControl` API では、設定可能なコントロールを設定できます。
- 更新された `GetEnabledControl` API では、有効なコントロールに設定されたパラメータが表示されます。
- 新しい `UpdateEnabledControl` API では、有効なコントロールのパラメータを変更できます。

詳細については、AWS Control Tower の「API リファレンス」を参照してください。

AWS Control Tower がランディングゾーン API をサポート

2023 年 11 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、API を使用したランディングゾーンの設定と起動をサポートするようになりました。API を使用して、ランディングゾーンの作成、更新、取得、一覧表示、リセット、および削除を行うことができます。

次の APIs を使用すると、 AWS CloudFormation または を使用してランディングゾーンをプログラムでセットアップおよび管理できます AWS CLI。

AWS Control Tower では、ランディングゾーンに関する以下の API をサポートしています。

- `CreateLandingZone` — この API コールは、ランディングゾーンバージョンとマニフェストファイルを使用してランディングゾーンを作成します。
- `GetLandingZoneOperation` — この API コールは、指定したランディングゾーンオペレーションのステータスを返します。
- `GetLandingZone` — この API コールは、バージョン、マニフェストファイル、ステータスなど、指定したランディングゾーンに関する詳細を返します。
- `UpdateLandingZone` — この API コールは、ランディングゾーンバージョンまたはマニフェストファイルを更新します。
- `ListLandingZone` — この API コールは、管理アカウントのランディングゾーン設定のランディングゾーン識別子 (ARN) を 1 つ返します。

- `ResetLandingZone` — この API コールは、ランディングゾーンを最新の更新で指定されたパラメータにリセットします。これにより、ドリフトを修復できます。ランディングゾーンが更新されていない場合、このコールはランディングゾーンを作成時に指定されたパラメータにリセットします。
- `DeleteLandingZone` — この API コールはランディングゾーンを廃止します。

ランディングゾーン API の使用を開始するには、「を使用して AWS Control Tower の使用を開始する APIs」を参照してください。

AWS Control Tower が、有効になっているコントロールのタグ付けをサポート

2023 年 11 月 10 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、AWS Control Tower コンソールから、または API により、有効になっているコントロールのリソースのタグ付けがサポートされました。有効になっているコントロールのタグを追加、削除、または一覧表示できます。

次の API のリリースにより、AWS Control Tower で有効にするコントロールのタグを設定できます。タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。

AWS Control Tower では、コントロールのタグ付けのために次の API がサポートされます。

- `TagResource` – この API コールは、AWS Control Tower で有効になっているコントロールにタグを追加します。
- `UntagResource` – この API コールは、AWS Control Tower で有効になっているコントロールからタグを削除します。
- `ListTagsForResource` – この API コールは、AWS Control Tower で有効になっているコントロールのタグを返します。

AWS Control Tower コントロール APIsは、AWS Control Tower AWS リージョン が利用可能な で使用できます。AWS Control Tower AWS リージョン が利用可能な の完全なリストについては、AWS「リージョン表」を参照してください。AWS Control Tower API の完全なリストについては、「API リファレンス」を参照してください。

AWS Control Tower がアジアパシフィック (メルボルン) リージョンで利用可能に

2023 年 11 月 3 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower がアジアパシフィック (メルボルン) リージョンで利用可能です。

既に AWS Control Tower を使用していて、アカウントのこのリージョンにガバナンス機能を拡張する場合は、AWS Control Tower ダッシュボードの [設定] ページに移動し、リージョンを選択してから、ランディングゾーンを更新します。ランディングゾーンの更新後、AWS Control Tower が管理するアカウントをすべて更新し、アカウントと OU を新しいリージョンの管理下に置く必要があります。詳細については、「更新について」を参照してください

AWS Control Tower を使用できるリージョンの完全なリストについては、「AWS リージョン の表」を参照してください。

新しい AWS Service Catalog External 製品タイプへの移行 (フェーズ 1)

2023 年 10 月 31 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

HashiCorp が Terraform ライセンスを更新しました。その結果、Terraform Open Source 製品とプロビジョニング済み製品のサポートが External という新しい製品タイプに AWS Service Catalog 更新されました。

AWS Control Tower は、 AWS Service Catalog External 製品タイプに依存する Account Factory のカスタマイズをサポートしていません。アカウント内の既存のワークロードと AWS リソースの中断を回避するには、2023 年 12 月 14 日までに、次の推奨順序で AWS Control Tower の移行手順に従ってください。

1. の既存の Terraform リファレンスエンジンをアップグレード AWS Service Catalog して、外部製品タイプと Terraform オープンソース製品タイプの両方のサポートを含めます。Terraform Reference Engine の更新方法については、AWS Service Catalog GitHub リポジトリを参照してください。
2. に移動 AWS Service Catalog し、既存の Terraform Open Source ブループリントを複製して、新しい External 製品タイプを使用します。既存の Terraform Open Source ブループリントを削除しないでください。

3. 既存の Terraform Open Source ブループリントを引き続き使用して、AWS Control Tower のアカウントを作成または更新します。

新しいコントロール API が利用可能に

2023 年 10 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、AWS Control Tower のコントロールを大規模にデプロイおよび管理するために使用できる追加の API がサポートされるようになりました。AWS Control Tower API の詳細については、「API リファレンス」を参照してください。

AWS Control Tower で新しいコントロール API が追加されました。

- `GetEnabledControl` – API コールは、有効になっているコントロールに関する詳細を提供します。

この API も更新されました。

`ListEnabledControls` – この API コールは、指定した組織単位とその組織単位内のアカウントで、AWS Control Tower によって有効化されたコントロールを一覧表示します。`EnabledControlSummary` オブジェクトの追加情報を返すようになりました。

これらの API を使用すると、いくつかの一般的なオペレーションをプログラムで実行できます。以下に例を示します。

- AWS Control Tower コントロールライブラリから、有効にしたすべてのコントロールのリストを取得します。
- 有効になっているコントロールについては、コントロールがサポートされているリージョン、コントロールの識別子 (ARN)、コントロールのドリフトステータス、およびコントロールのステータス概要に関する情報を取得できます。

AWS Control Tower コントロール APIsは、AWS Control Tower AWS リージョン が利用可能な で使用できます。AWS Control Tower AWS リージョン が利用可能な の完全なリストについては、AWS リージョン表を参照してください。AWS Control Tower API の完全なリストについては、「API リファレンス」を参照してください。

AWS Control Tower が追加のコントロールをリリース

2023 年 10 月 5 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、新しいプロアクティブコントロールと検出コントロールを発表しました。

AWS Control Tower のプロアクティブコントロールは AWS CloudFormation 、フックによって実装されます。フックは、 が非準拠のリソース AWS CloudFormation をプロビジョニングする前に識別してブロックします。プロアクティブコントロールは、AWS Control Tower の既存の予防および検出コントロール機能を補完します。

新しいプロアクティブコントロール

- [CT.ATHENA.PR.1] Amazon Athena ワークグループは Athena クエリ結果を保管中に暗号化する必要があります
- [CT.ATHENA.PR.2] Amazon Athena ワークグループは AWS Key Management Service (KMS) キーを使用して Athena クエリ結果を保管中に暗号化する必要があります
- 〔CT.CLOUDTRAIL.PR.4〕 AWS CloudTrail Lake イベントデータストアで AWS KMS キーを使用した保管時の暗号化を有効にする必要があります
- [CT.DAX.PR.2] Amazon DAX クラスターは少なくとも 3 つのアベイラビリティーゾーンにノードをデプロイする必要があります
- [CT.EC2.PR.14] 保管中のデータを暗号化するには、Amazon EC2 起動テンプレートを使用して Amazon EBS ボリュームを設定する必要があります
- 〔CT.EKS.PR.2〕 Amazon EKS クラスターは、 AWS Key Management Service (KMS) キーを使用したシークレット暗号化で設定する必要があります
- [CT.ELASTICLOADBALANCING.PR.14] Network Load Balancer ではクロスゾーン負荷分散を有効にする必要があります
- [CT.ELASTICLOADBALANCING.PR.15] Elastic Load Balancing v2 ターゲットグループはクロスゾーン負荷分散を明示的に無効にしないようにする必要があります
- [CT.EMR.PR.1] Amazon EMR (EMR) のセキュリティ設定は、Amazon S3 に保管中のデータを暗号化するように構成する必要があります
- 〔CT.EMR.PR.2〕 Amazon EMR (EMR) セキュリティ設定は、Amazon S3 の保管中のデータを AWS KMS キーで暗号化するように設定する必要があります
- 〔CT.EMR.PR.3〕 Amazon EMR (EMR) セキュリティ設定は、 AWS KMS キーを使用した EBS ボリュームのローカルディスク暗号化で設定する必要があります

- [CT.EMR.PR.4] 転送中のデータを暗号化するように Amazon EMR (EMR) のセキュリティ設定を構成する必要があります
- [CT.GLUE.PR.1] AWS Glue ジョブには関連するセキュリティ設定が必要です
- [CT.GLUE.PR.2] AWS Glue セキュリティ設定は、 AWS KMS キーを使用して Amazon S3 ターゲット内のデータを暗号化する必要があります
- 〔CT.KMS.PR.2〕 暗号化に使用される RSA キーマテリアルを持つ AWS KMS 非対称キーの長さが 2048 ビットを超える必要があります
- 〔CT.KMS.PR.3〕 AWS KMS キーポリシーには、 AWS サービスへの AWS KMS 許可の作成を制限するステートメントが必要です
- 〔CT.LAMBDA.PR.4〕 AWS 組織または特定の AWS アカウントへのアクセス許可を付与するには、 AWS Lambda レイヤーのアクセス許可が必要です
- 〔CT.LAMBDA.PR.5〕 IAM ベースの認証を使用するには AWS Lambda 関数 URL AWS が必要です
- 〔CT.LAMBDA.PR.6〕 特定のオリジンへのアクセスを制限するには、 AWS Lambda 関数 URL CORS ポリシーが必要です
- [CT.NEPTUNE.PR.4] Amazon Neptune DB クラスターは、監査ログ用に Amazon CloudWatch ログのエクスポートを有効にする必要があります
- [CT.NEPTUNE.PR.5] Amazon Neptune DB クラスターは、バックアップ保持期間を 7 日間以上に設定する必要があります
- [CT.REDSHIFT.PR.9] Amazon Redshift クラスターのパラメータグループは、転送中のデータの暗号化に Secure Sockets Layer (SSL) を使用するように設定する必要があります

これらの新しいプロアクティブコントロールは、AWS Control Tower AWS リージョン が利用可能な商用 で利用できます。これらのコントロールの詳細については、「Proactive controls」を参照してください。コントロールが利用できる場所の詳細については、「Control limitations」を参照してください。

新しい検出コントロール

Security Hub サービスマネージド標準: AWS Control Tower に新しいコントロールが追加されました。これらのコントロールは、ガバナンス体制の強化に役立ちます。これらのコントロールは、特定の OU で有効にすると、Security Hub サービスマネージド標準: AWS Control Tower の一部として機能します。

- [SH.Athena.1] Athena ワークグループは、保管中に暗号化する必要があります

- [SH.Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [SH.Neptune.2] Neptune DB クラスターは、監査ログを CloudWatch Logs に発行する必要があります
- [SH.Neptune.3] Neptune DB クラススナップショットをパブリックにすることはできません
- [SH.Neptune.4] Neptune DB クラスターでは、削除保護を有効にする必要があります
- [SH.Neptune.5] Neptune DB クラスターでは、自動バックアップを有効にする必要があります
- [SH.Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります
- [SH.Neptune.7] Neptune DB クラスターでは、IAM データベース認証を有効にする必要があります
- [SH.Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [SH.RDS.27] RDS DB クラスターは保管中に暗号化する必要があります

新しい AWS Security Hub 検出コントロールは、AWS Control Tower が利用可能なほとんどの AWS リージョン で使用できます。これらのコントロールの詳細については、「サービスマネージドスタンダード: AWS Control Tower に適用されるコントロール」を参照してください。コントロールが利用できる場所の詳細については、「コントロールの制限事項」を参照してください。

新しいドリフトタイプの報告: 信頼できるアクセスの無効化

2023 年 9 月 21 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower のランディングゾーンをセットアップしたら、 AWS Organizationsで AWS Control Tower への信頼できるアクセスを無効にできます。ただし、これに伴ってドリフトが発生します。

信頼できるアクセスの無効化に伴うドリフトタイプにより、この種のドリフトが発生すると AWS Control Tower から通知が届くため、AWS Control Tower のランディングゾーンを修復できます。詳細については、「Types of governance drift」を参照してください。

4 つの追加 AWS リージョン

2023 年 9 月 13 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が、アジアパシフィック (ハイデラバード)、欧州 (スペインおよびチューリッヒ)、中東 (アラブ首長国連邦) で利用可能になりました。

既に AWS Control Tower を使用していて、アカウントのこのリージョンにガバナンス機能を拡張する場合は、AWS Control Tower ダッシュボードの [設定] ページに移動し、リージョンを選択してから、ランディングゾーンを更新します。ランディングゾーンの更新後、AWS Control Tower が管理するアカウントをすべて更新し、アカウントと OU を新しいリージョンの管理下に置く必要があります。詳細については、「更新について」を参照してください

AWS Control Tower を使用できるリージョンの完全なリストについては、「AWS リージョン の表」を参照してください。

AWS Control Tower がテルアビブリージョンで利用可能に

2023 年 8 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が、イスラエル (テルアビブ) で利用可能になりました。

既に AWS Control Tower を使用していて、アカウントのこのリージョンにガバナンス機能を拡張する場合は、AWS Control Tower ダッシュボードの [設定] ページに移動し、リージョンを選択してから、ランディングゾーンを更新します。ランディングゾーンの更新後、AWS Control Tower が管理するアカウントをすべて更新し、アカウントと OU を新しいリージョンの管理下に置く必要があります。詳細については、「更新について」を参照してください

AWS Control Tower を使用できるリージョンの完全なリストについては、「AWS リージョン の表」を参照してください。

AWS Control Tower が 28 個の新しいプロアクティブコントロールをリリース

2023 年 7 月 24 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、 AWS 環境の管理に役立つ 28 個の新しいプロアクティブコントロールを追加します。

プロアクティブコントロールは、プロビジョニング前に非準拠のリソースをブロックすることで、マルチアカウント AWS 環境全体で AWS Control Tower のガバナンス機能を強化します。これら

のコントロールは、Amazon CloudWatch、Amazon Neptune、Amazon ElastiCache AWS Step Functions、Amazon DocumentDB などの AWS のサービスの管理に役立ちます。新しいコントロールは、ログ記録とモニタリングの確立、保管中のデータの暗号化、耐障害性の向上などの統制目標を達成するのに役立ちます。

新しいコントロールの詳細なリストは次のとおりです。

- [CT.APPSYNC.PR.1] AWS AppSync GraphQL API でログ記録を有効にする必要がある
- [CT.CLOUDWATCH.PR.1] Amazon CloudWatch アラームでアラーム状態に応じたアクションを設定する必要がある
- [CT.CLOUDWATCH.PR.2] Amazon CloudWatch ロググループを少なくとも 1 年間保持する必要がある
- [CT.CLOUDWATCH.PR.3] Amazon CloudWatch ロググループを KMS AWS キーで保管時に暗号化する必要があります
- [CT.CLOUDWATCH.PR.4] Amazon CloudWatch アラームアクションをアクティブにする必要がある
- [CT.DOCUMENTDB.PR.1] Amazon DocumentDB クラスターを保管中に暗号化する必要がある
- [CT.DOCUMENTDB.PR.2] Amazon DocumentDB クラスターで自動バックアップを有効にする必要がある
- [CT.DYNAMODB.PR.2] AWS KMS キーを使用して Amazon DynamoDB テーブルを保管時に暗号化する必要があります
- [CT.EC2.PR.13] Amazon EC2 インスタンスで詳細モニタリングを有効にする必要がある
- [CT.EKS.PR.1] クラスターの Kubernetes API サーバーエンドポイントへのパブリックアクセスを無効にして Amazon EKS クラスターを設定する必要がある
- [CT.ELASTICACHE.PR.1] Amazon ElastiCache for Redis クラスターで自動バックアップをアクティブにする必要がある
- [CT.ELASTICACHE.PR.2] Amazon ElastiCache for Redis クラスターで自動マイナーバージョンアップグレードをアクティブにする必要がある
- [CT.ELASTICACHE.PR.3] Amazon ElastiCache for Redis レプリケーショングループで自動フェイルオーバーを有効にする必要がある
- [CT.ELASTICACHE.PR.4] Amazon ElastiCache レプリケーショングループで保管中の暗号化をアクティブにする必要がある
- [CT.ELASTICACHE.PR.5] Amazon ElastiCache for Redis レプリケーショングループで転送中の暗号化をアクティブにする必要がある

- [CT.ELASTICACHE.PR.6] Amazon ElastiCache キャッシュクラスターでカスタムサブネットグループを使用する必要がある
- [CT.ELASTICACHE.PR.7] 以前の Redis バージョンの Amazon ElastiCache レプリケーショングループに Redis AUTH 認証が必要である
- [CT.ELASTICBEANSTALK.PR.3] AWS Elastic Beanstalk 環境にログ記録設定が必要である
- [CT.LAMBDA.PR.3] カスタマーマネージド Amazon 仮想プライベートクラウド (VPC) に AWS Lambda 関数を含める必要がある
- [CT.NEPTUNE.PR.1] Amazon Neptune DB クラスターには AWS Identity and Access Management (IAM) データベース認証が必要です
- [CT.NEPTUNE.PR.2] Amazon Neptune DB クラスターで削除保護を有効にする必要がある
- [CT.NEPTUNE.PR.3] Amazon Neptune DB クラスターでストレージ暗号化を有効にする必要がある
- [CT.REDSHIFT.PR.8] Amazon Redshift クラスターを暗号化する必要がある
- [CT.S3.PR.9] Amazon S3 バケットで S3 オブジェクトロックを有効にする必要がある
- [CT.S3.PR.10] Amazon S3 バケットでは、 AWS KMS キーを使用してサーバー側の暗号化を設定する必要があります
- [CT.S3.PR.11] Amazon S3 バケットでバージョニングを有効にする必要がある
- [CT.STEPFUNCTIONS.PR.1] AWS Step Functions ステートマシンでログ記録をアクティブにする必要がある
- [CT.STEPFUNCTIONS.PR.2] AWS Step Functions ステートマシンで AWS X-Ray トレースを有効にする必要があります

AWS Control Tower のプロアクティブコントロールは AWS CloudFormation 、フックによって実装されます。フックは、 が非準拠のリソース AWS CloudFormation をプロビジョニングする前に識別してブロックします。プロアクティブコントロールは、AWS Control Tower の既存の予防および検出コントロール機能を補完します。

これらの新しいプロアクティブコントロールは、AWS Control Tower AWS リージョン が利用可能なすべての で使用できます。これらのコントロールの詳細については、「Proactive controls」を参照してください。

AWS Control Tower で 2 つのコントロールが廃止されます

2023 年 7 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower はセキュリティコントロールを定期的に見直し、最新の状態であり、引き続きベストプラクティスと見なされていることを確認します。次の 2 つのコントロールは 2023 年 7 月 18 日に廃止され、2023 年 8 月 18 日にコントロールライブラリから削除されます。どの組織単位でもこれらのコントロールを有効にすることはできなくなりました。削除日より前にこれらのコントロールを無効にすることもできます。

- [SH.S3.4] S3 バケットでは、サーバー側の暗号化を有効にする必要があります
- [CT.S3.PR.7] Amazon S3 バケットにサーバー側の暗号化が設定されている必要があります

廃止の理由

2023 年 1 月現在、Amazon S3 は、暗号化されていない新しいバケットと既存のバケットすべてにデフォルトの暗号化を設定して、これらのバケットにアップロードされる新しいオブジェクトの暗号化の基本レベルとして、S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を適用します。SSE-S3 または AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) が既に設定されている既存のバケットのデフォルトの暗号化設定は変更されていません。

AWS Control Tower ランディングゾーンバージョン 3.2

2023 年 6 月 16 日

(AWS Control Tower ランディングゾーンをバージョン 3.2 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください)。

AWS Control Tower ランディングゾーンバージョン 3.2 では、 AWS Security Hub サービスマネージドスタンダード: AWS Control Tower の一部であるコントロールが一般公開されています。この標準に含まれるコントロールのドリフトステータスを AWS Control Tower コンソールで表示する機能が導入されました。

このアップデートには、AWSServiceRoleForAWSControlTower と呼ばれる新しいサービスにリンクされたロール (SLR) が含まれています。このロールは、各メンバーアカウントに AWSControlTowerManagedRule と呼ばれる EventBridge マネージドルールを作成することで AWS Control Tower を支援します。このマネージドルールは、AWS Control Tower を使用して から AWS Security Hub 検出イベントを収集し、コントロールドリフトを判断できます。

このルールは、AWS Control Tower によって作成される最初のマネージドルールです。ルールはスタックによってデプロイされるのではなく、EventBridge API から直接デプロイされます。ルール

は EventBridge コンソールで確認することも、EventBridge API を使用して表示することもできます。managed-by フィールドに入力すると、AWS Control Tower のサービスプリンシパルが表示されます。

以前は、AWS Control Tower は AWSControlTowerExecution ロールを前提として、メンバーアカウントで操作を実行していました。この新しいロールとルールは、マルチアカウント AWS 環境でオペレーションを実行するときに最小特権を許可するというベストプラクティスの原則により適しています。新しいロールでは、メンバーアカウントでのマネージドルールの作成、マネージドルールの管理、SNS によるセキュリティ通知の公開、ドリフトの検証など、具体的に許可する範囲を絞ったアクセス許可が提供されます。詳細については、「AWSServiceRoleForAWSControlTower」を参照してください。

ランディングゾーン 3.2 のアップデートには、管理アカウントに新しい StackSet リソース、BP_BASELINE_SERVICE_LINKED_ROLE も含まれています。これは、サービスにリンクされたロールを最初にデプロイします。

Security Hub のコントロールドリフト (ランディングゾーン 3.2 以降) を報告すると、AWS Control Tower は Security Hub から日次ステータス更新を受け取ります。コントロールはすべての管理対象リージョンでアクティブですが、AWS Control Tower は AWS Security Hub 検出イベントを AWS Control Tower ホームリージョンにのみ送信します。詳細については、「Security Hub control drift reporting」を参照してください。

リージョン拒否コントロールの更新

このランディングゾーンバージョンには、リージョン拒否コントロールの更新も含まれています。

追加されたグローバルサービスと API

- AWS Billing and Cost Management (billing:*)
- AWS CloudTrail（ cloudtrail:LookupEvents) は、メンバーアカウントのグローバルイベントを可視化します。
- AWS 一括請求 (consolidatedbilling:*)
- AWS マネジメントコンソールモバイルアプリケーション (consoleapp:*)
- AWS 無料利用枠 (freetier:*)
- AWS Invoicing (invoicing:*)
- AWS IQ (iq:*)
- AWS ユーザー通知 (notifications:*)
- AWS ユーザー通知連絡先 (notifications-contacts:*)

- Amazon Payments (`payments:*`)
- AWS 税設定 (`tax:*`)

削除されたグローバルサービスと API

- 有効なアクションではないため、`s3:GetAccountPublic` は削除されました。
- 有効なアクションではないため、`s3:PutAccountPublic` は削除されました。

AWS Control Tower は ID に基づいてアカウントを処理します

2023 年 6 月 14 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、アカウントの E メールアドレスではなく AWS アカウント ID を追跡することで、Account Factory で作成したアカウントを作成および管理できるようになりました。

アカウントをプロビジョニングする場合、アカウントのリクエスタには必ず `CreateAccount` および `DescribeCreateAccountStatus` アクセス許可が必要です。このアクセス許可セットは Admin ロールの一部であり、リクエスタが Admin ロールを引き受けると自動的に付与されます。アカウントをプロビジョニングするアクセス許可を委任する場合、これらのアクセス許可をアカウントリクエスタに直接追加する必要がある場合があります。

AWS Control Tower コントロールライブラリで使用できるその他の Security Hub 検出コントロール

2023 年 6 月 12 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower コントロールライブラリに 10 個の新しい AWS Security Hub 検出コントロールを追加しました。これらの新しいコントロールは、API Gateway、AWS CodeBuild、Amazon Elastic Compute Cloud (EC2)、Amazon Elastic Load Balancer、Amazon Redshift、Amazon SageMaker AI、 などのサービスをターゲットとします AWS WAF。これらの新しいコントロールは、ロギングと監視の確立、ネットワークアクセスの制限、保管中のデータの暗号化などの制御目標を達成することで、ガバナンス体制の強化に役立ちます。

これらのコントロールは、特定の OU で有効にした後、Security Hub サービスマネージドスタンダード: AWS Control Tower の一部として機能します。

- [SH.Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [SH.APIGateway.8] API Gateway ルートは承認タイプを指定する必要があります
- [SH.APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [SH.CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [SH.EC2.25] EC2 起動テンプレートでパブリック IP をネットワークインターフェイスに割り当てないでください
- [SH.ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [SH.Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [SH.SageMaker.2] SageMaker AI ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SH.SageMaker.3] ユーザーには SageMaker AI ノートブックインスタンスへのルートアクセスを許可しないでください
- [SH.WAF.10] WAFV2 ウェブ ACL には、1 つ以上のルールまたはルールグループが必要です

新しい AWS Security Hub 検出コントロールは、AWS Control Tower AWS リージョン が利用可能なすべての で使用できます。これらのコントロールの詳細については、「サービスマネージドスタンダード: AWS Control Tower に適用されるコントロール」を参照してください。

AWS Control Tower は、コントロールメタデータテーブルを公開します

2023 年 6 月 7 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower はで、公開されたドキュメントの一部として、コントロールメタデータの全表が提供されるようになりました。コントロール API を操作するとき、各コントロールの API controlIdentifier を検索できます。これは、各 AWS リージョン に関連付けられた一意の ARN です。表には、各コントロールの対象となるフレームワークと制御目標が含まれています。以前は、この情報はコンソールにのみ表示されていました。

テーブルには、AWS Security Hub サービスマネージドスタンダード: AWS Control Tower の一部である Security Hub コントロールのメタデータも含まれています。詳細については、「Tables of control metadata」を参照してください。

コントロール識別子の簡略リストと使用例については、「Resource identifiers for APIs and controls」を参照してください。

Account Factory のカスタマイズに対する Terraform サポート

2023 年 6 月 6 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、Account Factory のカスタマイズ (AFC) を通じて、Terraform の単一リージョンサポートを提供しています。今回のリリースから、AWS Control Tower と Service Catalog を併用して、Terraform オープンソースで AFC アカウントのブループリントを定義できるようになりました。AWS Control Tower でリソースをプロビジョニングする前に AWS アカウント、新規および既存の をカスタマイズできます。デフォルトでは、この機能により、Terraform を使用して AWS Control Tower のホームリージョンにアカウントをデプロイおよび更新できます。

アカウントブループリントは、 AWS アカウント がプロビジョニングされるときに必要な特定のリソースと設定を記述します。ブループリントをテンプレートとして使用して、複数の を AWS アカウント 大規模に作成できます。

はじめに、GitHub の Terraform リファレンスエンジンを使用します。リファレンスエンジンは、Terraform オープンソースエンジンが Service Catalog と連携するために必要なコードとインフラストラクチャを設定します。この 1 回限りのセットアッププロセスには数分かかります。その後、Terraform でカスタムアカウントの要件を定義し、明確に定義された AWS Control Tower アカウントファクトリワークフローを使用してアカウントをデプロイできます。Terraform の使用を希望するお客様は、AWS Control Tower のアカウントを AFC で大規模にカスタマイズでき、プロビジョニング後に各アカウントにすぐにアクセスできます。

これらのカスタマイズを作成する方法については、Service Catalog ドキュメントの「製品の作成」と「Terraform オープンソース入門」を参照してください。この機能は、AWS Control Tower が利用可能なすべての AWS リージョン で使用できます。

AWS ランディングゾーンで利用可能な IAM アイデンティティセンターの自己管理

2023 年 6 月 6 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、セットアップまたは更新時に設定できる AWS Control Tower ランディングゾーンの ID プロバイダーをオプションで選択できるようになりました。デフォルトでは、ランディングゾーンは、「複数のアカウントを使用した AWS 環境の整理」で定義されているベストプラ

クティスのガイダンスに従って、 AWS IAM Identity Center の使用にオプトインされます。これで、選択肢は次の 3 つになりました。

- デフォルトを受け入れて、AWS Control Tower に AWS IAM Identity Center のセットアップと管理を任せることができます。
- 特定のビジネス要件を反映するために、IAM Identity Center AWS を自己管理することを選択できます。
- 必要な場合は、サードパーティの ID プロバイダーを IAM Identity Center 経由で接続して、自分で管理することもできます。規制環境で特定のプロバイダーを使用する必要がある場合、または IAM Identity Center AWS リージョン が利用できない で運用している場合は、ID AWS プロバイダーのオプションを使用する必要があります。

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

アカウントレベルでの ID プロバイダーの選択はサポートされていません。この機能はランディングゾーン全体にのみ適用されます。AWS Control Tower ID プロバイダーのオプションは、AWS Control Tower AWS リージョン が利用可能なすべての で使用できます。

AWS Control Tower は OU の混合ガバナンスに対応

2023 年 6 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

今回のリリースでは、組織単位 (OU) が混合ガバナンスの状態にある場合、AWS Control Tower はコントロールが OU にデプロイされないようにします。AWS Control Tower がガバナンスを新しいに拡張した後、またはガバナンスを削除した後にアカウントが更新されない場合 AWS リージョン、混合ガバナンスが OU で発生します。このリリースにより、その OU のメンバーアカウントを統一したコンプライアンスに維持できます。詳細については、「リージョンを設定する際は混合ガバナンスを避ける」を参照してください。

追加のプロアクティブコントロールが利用可能に

2023 年 5 月 19 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、マルチアカウント環境を管理し、保管中のデータの暗号化やネットワークアクセスの制限などの特定のコントロール目標の達成を支援するために、28 種類のプロアクティブコントロールが新たに追加されています。プロアクティブコントロールは、プロビジョニング

前にリソースをチェックする AWS CloudFormation フックで実装されます。新しいコントロールは、Amazon OpenSearch Service、Amazon EC2 Auto Scaling、Amazon SageMaker AI、Amazon API Gateway、Amazon Relational Database Service (RDS) などの AWS サービスを管理するのに役立ちます。

プロアクティブコントロールは、AWS Control Tower AWS リージョン が利用可能なすべての商用でサポートされています。

Amazon OpenSearch Service

- [CT.OPENSEARCH.PR.1] 保管中のデータを暗号化するには Elasticsearch ドメインが必要です
- [CT.OPENSEARCH.PR.2] ユーザーが指定した Amazon VPC に Elasticsearch ドメインが作成されている必要があります
- [CT.OPENSEARCH.PR.3] ノード間のデータを暗号化するには Elasticsearch ドメインが必要です
- [CT.OPENSEARCH.PR.4] エラーログを Amazon CloudWatch Logs に送信するには Elasticsearch ドメインが必要です
- [CT.OPENSEARCH.PR.5] 監査ログを Amazon CloudWatch Logs に送信するには Elasticsearch ドメインが必要です
- [CT.OPENSEARCH.PR.6] Elasticsearch ドメインにはゾーン認識および少なくとも 3 つのデータノードが必要です
- [CT.OPENSEARCH.PR.7] Elasticsearch ドメインには少なくとも 3 つの専用マスターノードが必要です
- [CT.OPENSEARCH.PR.8] Elasticsearch Service ドメインで TLSv1.2 を使用する必要がある
- [CT.OPENSEARCH.PR.9] 保管中のデータを暗号化するには Amazon OpenSearch Service ドメインが必要です
- [CT.OPENSEARCH.PR.10] ユーザー指定の Amazon VPC に Amazon OpenSearch Service ドメインが作成されている必要があります
- [CT.OPENSEARCH.PR.11] ノード間で送信されるデータを暗号化するには Amazon OpenSearch Service ドメインが必要です
- [CT.OPENSEARCH.PR.12] エラーログを Amazon CloudWatch Logs に送信するには Amazon OpenSearch Service ドメインが必要です
- [CT.OPENSEARCH.PR.13] 監査ログを Amazon CloudWatch Logs に送信するには Amazon OpenSearch Service ドメインが必要です
- [CT.OPENSEARCH.PR.14] Amazon OpenSearch Service ドメインにはゾーン認識および少なくとも 3 つのデータノードが必要です

- [CT.OPENSEARCH.PR.15] きめ細かなアクセスコントロールを使用するには Amazon OpenSearch Service ドメインが必要です
- [CT.OPENSEARCH.PR.16] Amazon OpenSearch Service ドメインで TLSv1.2 を使用する必要がある

アマゾン EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] Amazon EC2 Auto Scaling グループには複数のアベイラビリティーゾーンが含まれている必要があります
- [CT.AUTOSCALING.PR.2] IMDSv2 用の Amazon EC2 インスタンスを設定するには Amazon EC2 Auto Scaling グループの起動設定が必要です
- [CT.AUTOSCALING.PR.3] Amazon EC2 Auto Scaling の起動設定でメタデータ応答ホップ制限を 1 に設定する必要があります
- [CT.AUTOSCALING.PR.4] ELB ヘルスチェックを有効にするには、Amazon Elastic Load Balancing (ELB) に関連付けられた Amazon EC2 Auto Scaling グループが必要です
- [CT.AUTOSCALING.PR.5] Amazon EC2 Auto Scaling グループの起動設定にパブリック IP アドレスを持つ Amazon EC2 インスタンスが含まれていない必要があります
- [CT.AUTOSCALING.PR.6] Amazon EC2 Auto Scaling グループでは複数のインスタンスタイプを使用する必要があります
- [CT.AUTOSCALING.PR.8] Amazon EC2 Auto Scaling グループに EC2 起動テンプレートを設定する必要があります

Amazon SageMaker AI

- [CT.SAGEMAKER.PR.1] 直接インターネットアクセスを防ぐために Amazon SageMaker AI ノートブックインスタンスが必要です
- [CT.SAGEMAKER.PR.2] Amazon SageMaker AI ノートブックインスタンスをカスタム Amazon VPC 内にデプロイする必要があります
- [CT.SAGEMAKER.PR.3] Amazon SageMaker AI ノートブックインスタンスにはルートアクセスが許可されないようにする必要があります

Amazon API Gateway

- [CT.APIGATEWAY.PR.5] Amazon API Gateway V2 Websocket および HTTP ルートで権限付与タイプが指定されている必要があります

Amazon Relational Database Service (RDS)

- [CT.RDS.PR.25] Amazon RDS データベースクラスターにロギングが設定されている必要があります

詳細については、「Proactive controls」を参照してください。

Amazon EC2 プロアクティブコントロールの更新

2023 年 5 月 2 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、次の 2 つのプロアクティブコントロールが更新されました: CT.EC2.PR.3 および CT.EC2.PR.4。

更新されたCT.EC2.PR.3コントロールの場合、ポート 80 または 443 でない限り、セキュリティグループリソースのプレフィックスリストを参照 AWS CloudFormation するデプロイはデプロイからブロックされます。

更新されたCT.EC2.PR.4コントロールでは、ポートが
3389、20、23、110、143、3306、8080、1433、9200、9300、25、445、135、21、1434、4333、5432、の場合、セキュリティグループリソースのプレフィックスリストを参照する AWS CloudFormation デプロイはブロックされます。

7 つの追加 AWS リージョン が利用可能

2023 年 4 月 19 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower が AWS リージョン、北カリフォルニア (サンフランシスコ) 、アジアパシフィック (香港、ジャカルタ、大阪) 、欧州 (ミラノ) 、中東 (バーレーン) 、アフリカ (ケープタウン) の 7 つの追加で利用可能になりました。AWS Control Tower 用のこれらの追加リージョンは、オプトインリージョンと呼ばれ、デフォルトで有効になっている米国西部 (北カリフォルニア) リージョンを除き、デフォルトではアクティブになっていません。

AWS Control Tower のコントロールの中には、AWS Control Tower が利用できるこれらの追加 AWS リージョン で動作しないものがあります。これは、これらのリージョンが必要な基本機能をサポートしていないためです。詳細については、「コントロールの制限事項」を参照してください。

これらの新しいリージョンのうち、CfCT は、アジアパシフィック (ジャカルタおよび大阪) ではご利用いただけません。他の の可用性 AWS リージョン は変更されません。

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

AFT で必要な vPCE エンドポイントは、中東 (バーレーン) リージョンでは利用できません。このリージョンに AFT を導入するお客様は、パラメータ `aft_vpc_endpoints=false` を指定して導入する必要があります。詳細については、README ファイルのパラメータを参照してください。

Amazon EC2 の制限により、AWS Control Tower VPC には 米国西部 (北カリフォルニア) と `us-west-1` という 2 つのアベイラビリティーゾーンがあります。米国西部 (北カリフォルニア) では、6 つのサブネットが 2 つのアベイラビリティーゾーンで分割されます。詳細については、「AWS Control Tower と の概要 VPCs」を参照してください。

AWS Control Tower は、AWS Control Tower `AWSControlTowerServiceRolePolicy`が AWS アカウント管理サービスによって実装された `EnableRegion`、`ListRegions`、および `GetRegionOptStatus` APIs を呼び出して、ランディングゾーン (管理アカウント、ログアーカイブアカウント、監査アカウント) の共有アカウントと OU メンバーアカウントでこれらの追加 AWS リージョン を使用できるようにする新しいアクセス許可を に追加しました。詳細については、「AWS Control Tower のマネージドポリシー」を参照してください。

Account Factory for Terraform (AFT) アカウントのカスタマイズリクエストの追跡

2023 年 2 月 16 日

AFT はアカウントのカスタマイズリクエストの追跡をサポートしています。アカウントのカスタマイズリクエストを送信するたびに、AFT は AFT カスタマイズ AWS Step Functions ステートマシンを通過する一意のトレーストークンを生成します。このステートマシンは、トークンを実行の一部としてログに記録します。Amazon CloudWatch Logs Insights のクエリを使用して、タイムスタンプの範囲を検索し、リクエストトークンを取得できます。その結果、トークンに関連付けられたペイロードを確認し、AFT ワークフロー全体を通じてアカウントカスタマイズリクエストを追跡することができます。AFT の詳細については、「AWS Control Tower Account Factory for Terraform の概要」を参照してください。CloudWatch Logs と Step Functions の詳細については、以下を参照してください。

- Amazon CloudWatch Logs ユーザーガイドの「Amazon CloudWatch Logs とは」
- AWS Step Functions デベロッパーガイドの「 AWS Step Functionsとは」

AWS Control Tower ランディングゾーンバージョン 3.1

2023 年 2 月 9 日

(AWS Control Tower のランディングゾーンをバージョン 3.1 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください)

AWS Control Tower ランディングゾーンバージョン 3.1 には、次の更新が含まれています。

- 今回のリリースでは、AWS Control Tower はアクセスログバケット (アクセスログが Log Archive アカウントに保存される Amazon S3 バケット) の不要なアクセスログを無効化し、S3 バケットのサーバーアクセスログを引き続き有効にします。このリリースには、 サポート プランや などのグローバルサービスに追加のアクションを許可するリージョン拒否コントロールの更新も含まれています AWS Artifact。
- AWS Control Tower アクセスログバケットのサーバーアクセスログを無効にすると、Security Hub は Log Archive アカウントのアクセスログバケットの結果を作成します。これは、[S3.9] S3 バケットのサーバーアクセスログを有効にする必要があるという AWS Security Hub ルールによるものです。Security Hub に従い、このルールの Security Hub の説明に記載されているように、この特定の結果を非表示にすることをお勧めします。追加情報については、「非表示の結果に関する情報」を参照してください。
- Log Archive アカウントの (通常の) ログバケットのアクセスログは、バージョン 3.1 でも変更されていません。ベストプラクティスに従い、そのバケットのアクセスイベントは、アクセスログバケットにログエントリとして記録されます。アクセスログの詳細については、Amazon S3 ドキュメントの「サーバーアクセスログを使用したリクエストのログ記録」を参照してください。
- リージョン拒否コントロールを更新しました。この更新により、より多くのグローバルサービスによるアクションが可能になります。この SCP の詳細については、「リクエストされた AWS に基づいて へのアクセスを拒否する AWS リージョン」および「データレジデンシー保護を強化するコントロール」を参照してください。

  追加されたグローバルサービス:

  - AWS Account Management (`account:*`)
  - AWS アクティブ化 (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)
  - AWS Compute Optimizer (`compute-optimizer:*`)
  - AWS Data Pipeline (`datapipeline:GetAccountLimits`)

- AWS Device Farm(devicefarm:*)
- AWS Marketplace (discovery-marketplace:*)
- Amazon ECR (ecr-public:*)
- AWS License Manager (license-manager:ListReceivedLicenses)
- AWS Lightsail (lightsail:Get*)
- AWS Resource Explorer (resource-explorer-2:*)
- Amazon S3 (s3:CreateMultiRegionAccessPoint、s3:GetBucketPolicyStatus、s3:PutMultiRegionA
- AWS Savings Plans (savingsplans:*)
- IAM Identity Center (sso:*)
- AWS Support App (supportapp:*)
- サポート プラン (supportplans:*)
- AWS 持続可能性 (sustainability:*)
- AWS Resource Groups Tagging API (tag:GetResources)
- AWS Marketplace Vendor Insights (vendor-insights:ListEntitledSecurityProfiles)

プロアクティブコントロールの一般公開

2023 年 1 月 24 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

以前はプレビュー版として発表されていた、オプションのプロアクティブコントロールが一般公開されました。これらのコントロールは、リソースをデプロイする前にリソースをチェックして、新しいリソースが環境内で有効になっているコントロールに準拠しているかどうかを判断するため、プロアクティブと呼ばれます。詳細については、「包括的なコントロールによる AWS リソースのプロビジョニングと管理のサポート」を参照してください。

2022 年 1 月 ~ 12 月

2022 年、AWS Control Tower は次の更新をリリースしました。

- 同時アカウント操作

- Account Factory Customization (AFC)
- 包括的なコントロールによる AWS リソースのプロビジョニングと管理のサポート
- すべての AWS Config ルールで表示可能なコンプライアンスステータス
- コントロールの API と新しい AWS CloudFormation リソース
- CfCT がスタックセットの削除をサポート
- カスタマイズされたログの保持
- ロールドリフト修復可能
- AWS Control Tower ランディングゾーンバージョン 3.0
- OU とアカウントのビューが組み合わされた組織ページ
- 個々のメンバーアカウントの登録と更新が容易に
- AFT は、AWS Control Tower の共有アカウントの自動カスタマイズをサポートします
- すべてのオプションのコントロールの同時操作
- 既存のセキュリティアカウントとログアカウント
- AWS Control Tower ランディングゾーンバージョン 2.9
- AWS Control Tower ランディングゾーンバージョン 2.8

同時アカウント操作

2022 年 12 月 16 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、Account Factory の同時実行アクションがサポートされるようになりました。一度に最大 5 つのアカウントを作成、更新、または登録できるようになります。最大 5 つのアクションを連続して送信し、各リクエストの完了状況を確認できます。その間、アカウントの作成はバックグラウンドで完了します。たとえば、別のアカウントを更新したり、組織単位 (OU) 全体を再登録したりする前に、各プロセスが完了するのを待つ必要がなくなります。

Account Factory Customization (AFC)

2022 年 11 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

Account Factory Customization を使用すると、AWS Control Tower コンソール内から新しいアカウントと既存のアカウントをカスタマイズできます。これらの新しいカスタマイズ機能により、特殊な

Service Catalog 製品に含まれる AWS CloudFormation テンプレートであるアカウントのブループリントを柔軟に定義できます。ブループリントにより、完全にカスタマイズされたリソースと構成がプロビジョニングされます。また、特定のユースケースに合わせてアカウントをカスタマイズするのに役立つ、 AWS パートナーによって作成および管理される定義済みのブループリントを使用することもできます。

これまで、AWS Control Tower の Account Factory では、コンソールでのアカウントのカスタマイズをサポートしていませんでした。Account Factory の今回の更新により、アカウント要件を事前に定義して、明確に定義されたワークフローの一部として実装できます。ブループリントを適用して、新しいアカウントの作成、AWS Control Tower への他の AWS アカウントの登録、既存の AWS Control Tower アカウントの更新を行うことができます。

Account Factory でアカウントをプロビジョニング、登録、または更新するとき、デプロイするブループリントを選択します。ブループリントで指定されているリソースは、アカウントでプロビジョニングされます。アカウントの作成が完了すると、すべてのカスタム構成をすぐに使用できます。

アカウントのカスタマイズを開始するには、Service Catalog 製品で目的のユースケースに合わせてリソースを定義します。 AWS 入門ライブラリからパートナーマネージドソリューションを選択することもできます。詳細については、「Account Factory Customization を使用してアカウントをカスタマイズする (AFC)」を参照してください。

包括的なコントロールによる AWS リソースのプロビジョニングと管理のサポート

2022 年 11 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、 AWS CloudFormation フックを通じて実装される新しいオプションのプロアクティブコントロールを含む包括的なコントロール管理をサポートするようになりました。これらのコントロールは、リソースをデプロイする前にリソースをチェックして、新しいリソースが環境内で有効になっているコントロールに準拠しているかどうかを判断するため、プロアクティブと呼ばれます。

130 を超える新しいプロアクティブコントロールは、AWS Control Tower 環境の特定のポリシー目標の達成、業界標準のコンプライアンスフレームワークの要件を満たすこと、その他 20 を超える AWS のサービスでの AWS Control Tower のやり取りの管理に役立ちます。

AWS Control Tower コントロールライブラリは、関連する AWS サービスとリソースに従ってこれらのコントロールを分類します。詳細については、「Proactive controls」を参照してください。

このリリースでは、AWS Control Tower は AWS Security Hub、 AWS Foundational Security Best Practices (FSBP) 標準をサポートする新しい Security Hub Service-Managed Standard: AWS Control Tower によって とも統合されています。160 を超える Security Hub コントロールと AWS Control Tower コントロールをコンソールで表示し、AWS Control Tower 環境の Security Hub セキュリティスコアを取得できます。詳細については、「Security Hub controls」を参照してください。

すべての AWS Config ルールで表示可能なコンプライアンスステータス

2022 年 11 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower に登録された組織単位にデプロイされたすべての AWS Config ルールのコンプライアンスステータスを表示するようになりました。AWS Control Tower コンソールの外に移動しなくても、登録済みまたは未登録の AWS Control Tower のアカウントに影響するすべての AWS Config ルールのコンプライアンスステータスを表示できます。お客様は、検出コントロールと呼ばれる Config ルールを AWS Control Tower で設定するか、 AWS Config サービスを通じて直接設定するかを選択できます。によってデプロイされたルール AWS Config と、AWS Control Tower によってデプロイされたルールが表示されます。

以前は、 AWS Config サービスを通じてデプロイされた AWS Config ルールは AWS Control Tower コンソールに表示されませんでした。お客様は、非準拠 AWS Config ルールを特定するために AWS Config サービスに移動する必要がありました。これで、AWS Control Tower コンソール内で非準拠 AWS Config ルールを特定できます。すべての設定ルールのコンプライアンスステータスを確認するには、AWS Control Tower コンソールの [Account details] (アカウントの詳細) のページに移動します。AWS Control Tower によって管理されるコントロールと AWS Control Tower の外部でデプロイされた設定ルールのコンプライアンスステータスを示すリストが表示されます。

コントロールの API と新しい AWS CloudFormation リソース

2022 年 9 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、一連の API コールによるコントロール (ガードレールとも呼ばれる) の、プログラムによる管理をサポートするようになりました。新しい AWS CloudFormation リソースは、コントロールの API 機能をサポートしています。詳細については、「 AWS Control Tower でタスクを自動化する 」および「 で AWS Control Tower リソースを作成する AWS CloudFormation」を参照してください。

これらの API により、AWS Control Tower ライブラリでコントロールの有効化、無効化、およびアプリケーションステータスの表示を行うことができます。APIs には のサポートが含まれているため AWS CloudFormation、Infrastructure infrastructure-as-code (IaC) として AWS リソースを管理できます。AWS Control Tower は、組織単位 (OU) 全体と OU 内のすべての AWS アカウントに関するポリシーの意図を表すオプションの予防コントロールと検出コントロールを提供します。これらのルールは、新しいアカウントを作成したり、既存のアカウントを変更したりしても、有効に存続します。

このリリースに含まれる API

- EnableControl — この API コールはコントロールをアクティブにします。非同期オペレーションを開始して、指定した組織単位とその組織単位内のアカウントの AWS リソースを作成します。
- DisableControl — この API コールは、コントロールをオフにします。非同期オペレーションを開始して、指定した組織単位とその組織単位内のアカウントの AWS リソースを削除します。
- GetControlOperation — 特定の EnableControl オペレーションまたは DisableControl オペレーションのステータスを返します。
- ListEnabledControls — 指定した組織単位とその組織単位内のアカウントで、AWS Control Tower によって有効化されたコントロールを一覧表示します。

オプションコントロールのコントロール名のリストを表示するには、「AWS Control Tower Controls Reference Guide」の「Resource identifiers for APIs and controls」を参照してください。

CfCT がスタックセットの削除をサポート

2022 年 8 月 26 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower のカスタマイズ (CfCT) は、`manifest.yaml` ファイルのパラメータを設定することで、スタックセットの削除をサポートするようになりました。詳細については、「スタックセットの削除」を参照してください。

> **Important**
>
> 最初に `enable_stack_set_deletion` の値を `true` に設定すると、次回 CfCT を呼び出したときに、プレフィックス `CustomControlTower-` で始まるすべてのリソースのうち、キータグ `Key:AWS_Solutions, Value: CustomControlTowerStackSet` が関連付けられているリソースと、マニフェストファイルに宣言されていないリソースは、削除対象としてステージングされます。

カスタマイズされたログの保持

2022 年 8 月 15 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「ランディングゾーンを更新する」を参照してください。)

AWS Control Tower は、AWS Control Tower CloudTrail ログを保存する Amazon S3 バケットの保持ポリシーをカスタマイズする機能を提供するようになりました。日単位または年単位で最大 15 年まで保存するという Amazon S3 ログ保持ポリシーをカスタマイズできます。

ログの保持をカスタマイズしない場合、デフォルト設定は、標準アカウントのログ記録で 1 年、アクセスログで 10 年です。

この機能は、ランディングゾーンを更新または修復する際は AWS Control Tower を介して既存のお客様が、AWS Control Tower のセットアッププロセスを通じて新規のお客様が利用できます。

ロールドリフト修復可能

2022 年 8 月 11 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、ロールドリフトの修復がサポートされるようになりました。ランディングゾーンを完全に修復しなくても、必要なロールを復元できます。このタイプのドリフト修復が必要な場合、コンソールのエラーページにロールを復元する手順が示され、ランディングゾーンが再び使用可能になります。

AWS Control Tower ランディングゾーンバージョン 3.0

2022 年 7 月 29 日

(AWS Control Tower のランディングゾーンをバージョン 3.0 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください)

AWS Control Tower ランディングゾーンバージョン 3.0 には、次の更新が含まれています。

- 組織レベルの AWS CloudTrail 証跡を選択するか、AWS Control Tower によって管理される CloudTrail 証跡をオプトアウトするオプション。
- AWS CloudTrail がアカウントでアクティビティを ログ記録しているかどうかを決定する 2 つの新しい検出コントロール。

- ホームリージョン内のグローバルリソース AWS Config に関する情報のみを集約するオプション。
- リージョン拒否コントロールの更新。
- 管理ポリシー AWSControlTowerServiceRolePolicy の更新。
- 各登録アカウントで、IAM ロール `aws-controltower-CloudWatchLogsRole` と CloudWatch ロググループ `aws-controltower/CloudTrailLogs` を作成しなくなりました。以前は、アカウント証跡用に各アカウントでこれらを作成していました。組織証跡では、管理アカウントに 1 つだけ作成します。

次のセクションでは、各能力タイプの詳細を示します。

AWS Control Tower の組織レベルの CloudTrail 証跡

ランディングゾーンバージョン 3.0 では、AWS Control Tower が組織レベルの AWS CloudTrail 証跡をサポートするようになりました。

AWS Control Tower ランディングゾーンをバージョン 3.0 に更新する場合、ログ記録の設定として組織レベルの AWS CloudTrail 証跡を選択するか、AWS Control Tower によって管理される CloudTrail 証跡をオプトアウトするかを選択できます。バージョン 3.0 に更新すると、AWS Control Tower は 24 時間の待機期間後に登録済みアカウントの既存のアカウントレベルの証跡を削除します。AWS Control Tower は、未登録アカウントのアカウントレベルの証跡は削除しません。万一ランディングゾーンの更新が正常に行われず、AWS Control Tower が組織レベルの証跡を既に作成した後で障害が発生した場合、更新オペレーションを正常に完了できるようになるまで、組織レベルの証跡とアカウントレベルの証跡に対して請求が二重に発生する可能性があります。

ランディングゾーン 3.0 以降、AWS Control Tower は が AWS 管理するアカウントレベルの証跡をサポートしなくなりました。代わりに、AWS Control Tower は、お客様の選択に応じて、アクティブまたは非アクティブの組織レベルの証跡を作成します。

> **Note**
>
> バージョン 3.0 以降に更新後、AWS Control Tower によって管理されるアカウントレベルの CloudTrail 証跡作成を続行するオプションはありません。

ログは保存されている既存の Amazon S3 バケットに残っているため、集約されたアカウントログからログデータが失われることはありません。証跡のみが削除され、既存の口グは削除されません。組織レベルの証跡を追加するオプションを選択すると、AWS Control Tower は Amazon S3 バケッ

ト内の新しいフォルダへの新しいパスを開き、その場所にログ情報を送信し続けます。AWS Control Tower によって管理される証跡をオプトアウトすることを選択した場合、既存のログは変更されずにバケットに残ります。

ログストレージのパス命名規則

- アカウント証跡ログは、次の形式のパスで保存されます。`/org id/AWSLogs/…`
- アカウント証跡ログは、次の形式のパスで保存されます。`/org id/AWSLogs/org id/…`

AWS Control Tower が組織レベルの CloudTrail 証跡用に作成するパスは、手動で作成する組織レベルの証跡のデフォルトパス (以下の形式) とは異なります。

- `/AWSLogs/org id/…`

CloudTrail のパス命名の詳細については、「CloudTrail ログファイルの検索」を参照してください。

> **Tip**
>
> 独自のアカウントレベルの証跡を作成して管理する場合は、AWS Control Tower のランディングゾーンバージョン 3.0 への更新を完了する前に新しい証跡を作成して、すぐにログ記録を開始することをお勧めします。

新しいアカウントレベルまたは組織レベルの CloudTrail 証跡を随時作成し、自分で管理することを選択できます。AWS Control Tower によって管理される組織レベルの CloudTrail 証跡を選択するオプションは、バージョン 3.0 以降へのランディングゾーン更新中に利用できます。ランディングゾーンを更新するたびに、組織レベルの証跡をオプトイン/オプトアウトできます。

ログがサードパーティサービスによって管理されている場合は、必ずそのサービスに新しいパス名を提供してください。

> **Note**
>
> バージョン 3.0 以降のランディングゾーンでは、アカウントレベルの AWS CloudTrail 証跡は AWS Control Tower ではサポートされていません。アカウントレベルの証跡は随時作成して維持するか、AWS Control Tower によって管理される組織レベルの証跡情報にオプトインすることができます。

ホームリージョンでのみ AWS Config リソースを記録する

ランディングゾーンバージョン 3.0 では、AWS Control Tower で AWS Config のベースライン設定が更新され、ホームリージョンのみでグローバルリソースが記録されるようになります。バージョン 3.0 にアップデートした後、グローバルリソースのリソース記録がホームリージョンでのみ有効化されます。

この設定はベストプラクティスであるとみなされています。 AWS Security Hub と が推奨し AWS Config、グローバルリソースの作成、変更、または削除時に作成される設定項目の数を減らすことでコスト削減を実現します。以前は、グローバルリソースがお客様または AWS サービスにより作成、更新、または削除されるたびに、設定項目が管理対象の各リージョンの各項目に対して作成されていました。

AWS CloudTrail ログのための 2 つの新しい検出コントロール

組織レベルの AWS CloudTrail 証跡の変更の一環として、AWS Control Tower は CloudTrail が有効になっているかどうかを確認する 2 つの新しい検出コントロールを導入しています。最初のコントロールには必須ガイダンスがあり、3.0 以降のセットアップまたはランディングゾーン更新中にセキュリティ OU で有効になります。2 番目のコントロールは強く推奨されるガイダンスがあり、必須のコントロール保護が既に実装されているセキュリティ OU 以外の任意の OU にオプションで適用されます。

必須コントロール： セキュリティ組織単位の共有アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する

強く推奨されるコントロール: アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する

新しいコントロールの詳細については、「The AWS Control Tower controls library」を参照してください。

リージョン拒否コントロールの更新

リージョン拒否コントロールの NotAction リストを更新して、以下にリストされているいくつかの追加サービスによるアクションを含めました。

```
        “chatbot:*”,
        "s3:GetAccountPublic",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
```

```
            "s3:GetMultiRegionAccessPoint",
            "s3:GetMultiRegionAccessPointPolicy",
            "s3:GetMultiRegionAccessPointPolicyStatus",
            "s3:ListMultiRegionAccessPoints",
            "s3:GetStorageLensConfiguration",
            “s3:GetStorageLensDashboard",
            “s3:ListStorageLensConfigurations”
            “s3:GetAccountPublicAccessBlock“,,
            “s3:PutAccountPublic",
            “s3:PutAccountPublicAccessBlock“,
```

動画チュートリアル

このビデオ (3:07) では、既存の AWS Control Tower ランディングゾーンをバージョン 3 に更新する方法について説明しています。動画の右下にあるアイコンを選択すると、全画面表示にできます。字幕を利用できます。

[既存の AWS Control Tower のランディングゾーンをランディングゾーン 3 に更新するビデオウォークスルー。]

OU とアカウントのビューが組み合わされた組織ページ

2022 年 7 月 18 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower の新しい [Organization] (組織) ページには、すべての組織単位 (OU) とアカウントの階層的なビューが表示されます。ここでは、以前の [OU] ページと [Accounts] ページに表示されていた情報が表示されます。

新しいページでは、親 OU と、そのネストされた OU およびアカウントとの関係を確認することができ、リソースのグループに対してアクションを実行できます。ページビューを構成できます。例えば、階層ビューを展開することや折りたたむことに加えて、ビューをフィルターしてアカウントまたは OU のみを表示すること、登録済みアカウントと登録済みの OU のみを表示すること、関連リソースのグループを表示することができます。組織全体が適切に更新されていることを簡単に確認できます。

個々のメンバーアカウントの登録と更新が容易に

2022 年 5 月 31 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower は、メンバーアカウントを個別に更新および登録するための改善された機能を提供するようになりました。各アカウントには更新可能な日時が表示されるため、メンバーアカウントに最新の設定が含まれていることをより簡単に確認できます。わずか数ステップの効率的な方法で、ランディングゾーンを更新したり、アカウントドリフトを修正したり、アカウントを登録済み OU に登録したりできます。

アカウントを更新するとき、各更新アクションにアカウントの組織単位 (OU) 全体を含める必要はありません。その結果、個々のアカウントの更新に必要な時間が大幅に短縮されます。

AWS Control Tower コンソールのより充実したヘルプを使用して、AWS Control Tower OU にアカウントを登録できます。AWS Control Tower に登録する既存のアカウントは、アカウントの前提条件を引き続き満たしている必要があり、`AWSControlTowerExecution` ロールを追加する必要があります。次に、任意の登録済みの OU を選択し、[Enroll] (登録) ボタンを選択してその OU にアカウントを登録できます。

Account Factory の [Create] (作成) アカウントのワークフローから [Enroll account] (アカウントの登録) 機能を分離して、これらの類似したプロセスをより区別し、アカウント情報を入力するときの設定エラーを回避できるようにしました。

AFT は、AWS Control Tower の共有アカウントの自動カスタマイズをサポートします

2022 年 5 月 27 日

(AWS Control Tower ランディングゾーンの更新は不要です)

Account Factory for Terraform (AFT) では、AWS Control Tower で管理されているアカウント (管理アカウント、監査アカウント、ログアーカイブアカウントなど) を登録済みアカウントとともに、プログラムでカスタマイズおよび更新できるようになりました。アカウントのカスタマイズと更新の管理を一元化するとともに、アカウント設定のセキュリティを保護できます (この作業を実行するロールの適用範囲はユーザーが決めます)。

既存の AWSAFTExecution ロールが、すべてのアカウントにカスタマイズをデプロイするようになりました。IAM の許可をセットアップするには、ビジネス要件とセキュリティ要件に応じて、AWSAFTExecution ロールのアクセス権を制限する境界を使用できます。また、そのロールに承認されたカスタマイズの許可を、信頼されたユーザーにプログラムで委任することもできます。ベストプラクティスとして、必要なカスタマイズをデプロイする必要があるユーザーだけに許可を制限することをお勧めします。

AFT は、新しい AWSAFTService ロールを作成して、共有アカウントと管理アカウントを含むすべてのマネージドアカウントに AFT リソースをデプロイするようになりました。リソースは、以前は、AWSAFTExecution ロールによってデプロイされていました。

AWS Control Tower の共有アカウントと管理アカウントは Account Factory を通じてプロビジョニングされないため、対応するプロビジョニング済み製品はありません AWS Service Catalog。したがって、Service Catalog では共有アカウントと管理アカウントを更新できません。

すべてのオプションのコントロールの同時操作

2022 年 5 月 18 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower は、予防コントロールと検出コントロールの同時操作をサポートするようになりました。

この新しい機能により、すべてのオプションのコントロールを同時に適用または削除できるため、これらのコントロールの使いやすさとパフォーマンスが向上します。個々のコントロールの操作が完了するまで待たずに、複数のオプションのコントロールを有効にできます。同時操作が制限されるのは、AWS Control Tower がランディングゾーンのセットアップ中であるか、新しい組織にガバナンスを拡張中である場合だけです。

予防コントロールでサポートされる機能は以下のとおりです。

- 同じ OU に対して複数の異なる予防コントロールを適用または削除する。
- 複数の異なる予防コントロールを複数の異なる OU に対して同時に適用または削除します。
- 同じ予防コントロールを複数の異なる OU に対して同時に適用または削除します。
- 任意の数の予防コントロールと検出コントロールを同時に適用または削除できます。

AWS Control Tower のすべてのリリース済みバージョンで、これらのコントロールの同時実行の機能強化を体験できます。

予防コントロールは、ネストされた OU に適用すると、ターゲット OU の下にネストされたすべてのアカウントと OU に影響します。これらのアカウントや OU が AWS Control Tower に登録されていない場合でも影響を受けます。予防コントロールは、その一部であるサービスコントロールポリシー (SCPs) を使用して実装されます AWS Organizations。検出コントロールは AWS Config ルールを使用して実装されます。ガードレールは、新しいアカウントを作成したり、既存のアカウントを変

更したりしても有効に存続します。AWS Control Tower は、各アカウントが有効なポリシーにどのように準拠しているかを示すサマリーレポートを提供します。使用可能なコントロールの完全なリストについては、「The AWS Control Tower controls library」を参照してください。

既存のセキュリティアカウントとログアカウント

2022 年 5 月 16 日

(初期セットアップ時に使用可能)

AWS Control Tower では、最初のランディングゾーンのセットアッププロセス中に、既存の AWS アカウントを AWS Control Tower のセキュリティアカウントまたはログ記録アカウントとして指定できるようになりました。このオプションを使用すると、AWS Control Tower は新しい共有アカウントを作成する必要がなくなります。セキュリティアカウント (デフォルトでは、監査アカウントと呼ばれます) は、セキュリティチームとコンプライアンスチームに対してランディングゾーンのすべてのアカウントへのアクセスを許可する制限付きアカウントです。ログアカウント (デフォルトでは、ログアーカイブアカウントと呼ばれます) は、リポジトリとして機能します。このアカウントには、ランディングゾーンのすべてのアカウントからの API アクティビティとリソース設定のログが保存されます。

既存のセキュリティアカウントとログアカウントを使用することで、AWS Control Tower のガバナンスを既存の組織に拡張したり、別のランディングゾーンから AWS Control Tower に移動したりすることが容易になります。既存のアカウントを使用するオプションは、ランディングゾーンの最初のセットアップ時に表示されます。これには、セットアッププロセス中のチェックも含まれ、デプロイが正常に完了したことが確認されます。AWS Control Tower は、既存のアカウントに必要なロールとコントロールを実装します。これらのアカウントにある既存のリソースやデータは削除またはマージされません。

制限: 既存の AWS アカウントを監査アカウントおよびログアーカイブアカウントとして AWS Control Tower に持ち込む予定で、それらのアカウントに既存の AWS Config リソースがある場合は、AWS Control Tower にアカウントを登録する前に既存の AWS Config リソースを削除する必要があります。

AWS Control Tower ランディングゾーンバージョン 2.9

2020 年 4 月 22 日

(AWS Control Tower のランディングゾーンをバージョン 2.9 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください)

AWS Control Tower のランディングゾーンバージョン 2.9 は、Python バージョン 3.9 ランタイムを使用するように通知フォワーダー Lambda を更新します。この更新プログラムは、2022 年 7 月に予定されている Python バージョン 3.6 の非推奨化に対処します。最新情報については、Python の非推奨化に関するページを参照してください。

AWS Control Tower ランディングゾーンバージョン 2.8

2022 年 2 月 10 日

(AWS Control Tower のランディングゾーンをバージョン 2.8 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください。)

AWS Control Tower ランディングゾーンバージョン 2.8 は、「AWS の基本的なセキュリティのベストプラクティス」の最新の更新に合わせて機能が追加されています。

このリリースでは:

- 既存の S3 アクセスログバケットへのアクセスを追跡するために、ログアーカイブアカウントのアクセスログバケットに対してアクセスログが設定されました。
- ライフサイクルポリシーのサポートが追加されました。既存の S3 アクセスログバケットのアクセスログは、デフォルトの保持期間の 10 年に設定されます。
- さらに、このリリースでは、AWS Control Tower が更新され、すべてのマネージドアカウント (管理アカウントを除く) で が提供する AWS サービスリンクロール (SLR) が使用されるため AWS Config、 AWS Config ベストプラクティスに合わせて Config ルールを設定および管理できます。アップグレードを行わないお客様は、引き続き既存のロールを使用することになります。
- このリリースでは、 AWS Config データを暗号化するための AWS Control Tower KMS 設定プロセスが合理化され、CloudTrail の関連するステータスメッセージングが改善されました。
- このリリースには、リージョン拒否コントロールの更新が含まれており、`us-west-2` で `route53-application-recovery` 機能を使用できるようになりました。
- 更新: 2022 年 2 月 15 日に、 AWS Lambda 関数のデッドレターキューを削除しました。

その他の詳細:

- ランディングゾーンを廃止しても、AWS Control Tower は、 AWS Config サービスにリンクされたロールを削除しません。
- Account Factory アカウントのプロビジョニングを解除しても、AWS Control Tower は、 AWS Config サービスにリンクされたロールを削除しません。

ランディングゾーンを 2.8 に更新するには、[Landing zone settings] (ランディングゾーンの設定) ページに移動し、2.8 バージョンを選択して、[Update] (更新) を選択します。ランディングゾーンを更新したら、「AWS Control Tower の設定更新管理」に示すように、AWS Control Tower によって管理されているすべてのアカウントを更新する必要があります。

2021 年 1 月 ~ 12 月

2021 年、AWS Control Tower は次の更新をリリースしました。

- リージョン拒否機能
- データ所在地機能
- AWS Control Tower で、Terraform アカウントのプロビジョニングとカスタマイズが導入されました
- 新しいライフサイクルイベントが利用可能に
- AWS Control Tower でネストされた OU が有効になりました
- 検出コントロールの同時実行性
- 2 つの新しいリージョンが利用可能に
- リージョンの選択解除
- AWS Control Tower が AWS キー管理システムと連携する
- コントロールの名前が変更され、機能は変更されません
- AWS Control Tower は SCP を毎日スキャンしてドリフトをチェックするようになりました
- OU とアカウントのカスタマイズされた名前
- AWS Control Tower ランディングゾーンバージョン 2.7
- 3 つの新しい AWS リージョンが利用可能に
- 選択したリージョンのみを管理
- AWS Control Tower がガバナンスを AWS 組織内の既存の OUs に拡張
- AWS Control Tower でアカウントの一括更新が可能になりました

リージョン拒否機能

2021 年 11 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、AWS Control Tower 環境の登録済みアカウントの AWS サービスとオペレーションへのアクセスを制限するのに役立つリージョン拒否機能が提供されるようになりました。リージョン拒否機能は、AWS Control Tower の既存のリージョン選択およびリージョン選択解除機能を補完します。これらの機能を組み合わせて、追加のリージョンへの拡大に伴うコストのバランスをとり、コンプライアンスや規制上の懸念に対処するのに役立ちます。

例えば、ドイツの AWS お客様は、フランクフルトリージョン以外のリージョン AWS のサービスへのアクセスを拒否できます。制限付きリージョンは、AWS Control Tower の設定プロセス中に、または [Landing zone settings] (ランディングゾーンの設定) ページで選択することができます。リージョン拒否機能は、AWS Control Tower ランディングゾーンのバージョンを更新するときに使用できます。一部の AWS サービスはリージョン拒否機能から除外されます。詳細については、「Configure the Region deny control」を参照してください。

データ所在地機能

2021 年 11 月 30 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、 AWS サービスにアップロードする顧客データが、指定した AWS リージョンにのみ配置されるように、専用のコントロールが提供されるようになりました。顧客データが保存および処理される AWS リージョンを選択できます。AWS Control Tower が利用可能な AWS リージョンの完全なリストについては、AWS 「リージョン表」を参照してください。

きめ細かく制御するには、[Disallow Amazon Virtual Private Network (VPN) connections] (Amazon Virtual Private Network (VPN) 接続を許可しない) や [Disallow internet access for an Amazon VPC instance] (Amazon VPC インスタンスのインターネットアクセスを許可しない) などの追加のコントロールを適用できます。AWS Control Tower コンソールでコントロールのコンプライアンスステータスを表示できます。使用可能なコントロールの完全なリストについては、「The AWS Control Tower controls library」を参照してください。

AWS Control Tower で、Terraform アカウントのプロビジョニングとカスタマイズが導入されました

2021 年 11 月 29 日

(AWS Control Tower ランディングゾーンのオプションの更新)

AWS Control Tower Account Factory for Terraform (AFT) により、AWS Control Tower を通じて、Terraform を使用し、カスタマイズされたアカウントをプロビジョニングおよび更新できるようになりました。

AFT は、単一の Terraform Infrastructure as Code (IaC) パイプラインを提供し、AWS Control Tower が管理するアカウントをプロビジョニングします。プロビジョニング中のカスタマイズは、アカウントをエンドユーザーに提供する前に、ビジネスポリシーとセキュリティポリシーを満たすのに役立ちます。

AFT 自動アカウント作成パイプラインは、アカウントのプロビジョニングが完了するまで監視し、引き続き、必要なカスタマイズでアカウントを強化する追加の Terraform モジュールをトリガーします。カスタマイズプロセスの追加部分として、独自のカスタム Terraform モジュールをインストールするようにパイプラインを設定したり、一般的なカスタマイズ AWS のために によって提供される AFT 機能オプションを追加したりできます。

AWS Control Tower Account Factory for Terraform の使用を開始するには、「AWS Control Tower ユーザーガイド」の「AWS Control Tower Account Factory for Terraform (AFT) のデプロイ」に記載されているステップに従い、Terraform インスタンスの AFT をダウンロードします。AFT は、Terraform Cloud、Terraform Enterprise、および Terraform Open Source のディストリビューションをサポートしています。

新しいライフサイクルイベントが利用可能に

2021 年 11 月 18 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

`PrecheckOrganizationalUnit` イベントは、ネストされた OU のリソースを含め、[Extend governance] (ガバナンスを拡張) タスクが成功しないようリソースがブロックしているかどうかを記録します。詳細については、「`PrecheckOrganizationalUnit`」を参照してください。

AWS Control Tower でネストされた OU が有効になりました

2021 年 11 月 16 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower では、ランディングゾーンの一部として、ネストされた OU を含めることができるようになりました。

AWS Control Tower は、ネストされた組織単位 (OU、Organizational Unit) のサポートを提供して、アカウントを複数の階層レベルに編成し、予防コントロールを階層的に実施できるようにします。深さに関係なく、ネストされた OU を含む OU を登録し、親 OU の下に OU を作成して登録し、登録された OU でコントロールを有効にすることができます。この機能をサポートするために、管理されているアカウントと OU の数がコンソールに表示されます。

ネストされた OUs を使用すると、AWS Control Tower OUs を AWS マルチアカウント戦略に合わせることができ、親 OUs レベルでコントロールを適用することで、複数の OU でコントロールを有効にするために必要な時間を短縮できます。

主な考慮事項

1. AWS Control Tower に既存のマルチレベル OU を登録するときは、OU を 1 つずつ登録します。最上位の OU から開始し、ツリーの下の方へと進めます。詳細については、「フラットな OU 構造からネストされた OU 構造への拡張」を参照してください。
2. 登録された OU の直下のアカウントは自動的に登録されます。ツリーの下の方にあるアカウントは、直接の親 OU を登録することで登録できます。
3. 予防コントロール (SCP) は自動的に階層の下の方に継承されます。親に適用された SCP は、すべてのネストされた OU に継承されます。
4. 検出コントロール (AWS Config ルール) は自動的に継承されません。
5. 検出コントロールのコンプライアンスは、各 OU によって報告されます。
6. OU の SCP ドリフトは、その下にあるすべてのアカウントと OU に影響します。
7. セキュリティ OU (コア OU) の下に新しいネストされた OU を作成することはできません。

検出コントロールの同時実行性

2021 年 11 月 5 日

(AWS Control Tower ランディングゾーンのオプションの更新)

AWS Control Tower 検出コントロールは、検出コントロールの同時オペレーションをサポートするようになり、使いやすさとパフォーマンスが向上しました。個々のコントロールオペレーションが完了するのを待たずに、複数の検出コントロールを有効にできます。

サポートされている機能:

- 同じ OU で異なる検出コントロールを有効にします (例えば、[Detect Whether MFA for the Root User is Enabled] (ルートユーザーに対して MFA が有効になっているかどうかを検出する) と

[Detect Whether Public Write Access to Amazon S3 Buckets is Allowed] (Simple Storage Service (Amazon S3) バケットへのパブリック書き込みアクセスが許可されているかどうかを検出する))。

- 異なる OU で異なる検出コントロールを同時に有効にします。
- ガードレールのエラーメッセージングが改善され、サポートされているコントロールの同時実行オペレーションに関する追加のガイダンスが提供されるようになりました。

このリリースではサポートされない機能:

- 同じ検出コントロールを複数の OU で同時に有効にすることはサポートされていません。
- 予防的コントロールの同時実行はサポートされていません。

AWS Control Tower のすべてのバージョンで、検出コントロールの同時実行性の改善を体験できます。現在バージョン 2.7 を使用していないお客様は、最新バージョンで利用できるリージョンの選択や選択解除などの機能を利用できるように、ランディングゾーンの更新を実行することをお勧めします。

2 つの新しいリージョンが利用可能に

2021 年 7 月 29 日

(AWS Control Tower ランディングゾーンは更新が必要です。)

AWS Control Tower が、南米 (サンパウロ) と欧州 (パリ) の 2 つの追加 AWS リージョンで利用可能になりました。この更新により、AWS Control Tower の可用性が 15 の AWS リージョンに拡張されます。

AWS Control Tower を初めて使用する場合も、サポートされている任意のリージョンですぐに起動できます。起動時に、AWS Control Tower でマルチアカウント環境を構築および管理するリージョンを選択できます。

AWS Control Tower 環境が既にあり、サポートされている 1 つ以上のリージョンの AWS Control Tower ガバナンス機能を拡張または削除する場合は、AWS Control Tower ダッシュボードの [Landing Zone Settings] (ランディングゾーンの設定) ページに移動し、[Regions] (リージョン) を選択します。ランディングゾーンを更新したら、AWS Control Tower によって管理されているすべてのアカウントを更新する必要があります。

リージョンの選択解除

2021 年 7 月 29 日

(AWS Control Tower ランディングゾーンのオプションの更新)

AWS Control Tower リージョンの選択解除により、AWS Control Tower リソースの地理的フットプリントを管理する機能が強化されます。AWS Control Tower の管理を望まないリージョンの選択を解除できます。この機能により、追加のリージョンへの拡大に伴うコストのバランスをとりながら、コンプライアンスや規制に関する懸念に対処できます。

リージョンの選択解除は、AWS Control Tower ランディングゾーンのバージョンを更新するときに使用できます。

Account Factory を使用して新しいアカウントを作成するか、既存のメンバーアカウントを登録する場合、または [Extend Governance] (ガバナンスを拡張) を選択して既存の組織単位にアカウントを登録する場合、AWS Control Tower は、アカウントの選択したリージョンにガバナンス機能 (一元化された口ギング、モニタリング、コントロールなど) をデプロイします。リージョンの選択を解除し、そのリージョンから AWS Control Tower ガバナンスを削除することを選択すると、そのガバナンス機能は削除されますが、ユーザーがそれらのリージョンに AWS リソースまたはワークロードをデプロイする機能が妨げられることはありません。

AWS Control Tower が AWS キー管理システムと連携する

2021 年 7 月 28 日

(AWS Control Tower のランディングゾーンのオプションの更新)

AWS Control Tower には、 AWS Key Management Service (AWS KMS) キーを使用するオプションがあります。キーは、AWS Control Tower がデプロイするサービスと、関連する Amazon S3 データなどを保護するために、ユーザーによって提供および管理されます。 AWS KMS 暗号化は AWS CloudTrail AWS Config、AWS Control Tower がデフォルトで使用する SSE-S3 暗号化に対する拡張レベルの暗号化です。

AWS KMS サポートの AWS Control Tower への統合は、機密性の高いログファイルにセキュリティレイヤーを追加することを推奨する AWS Foundational Security Best Practices と一致しています。保管時の暗号化には AWS KMS マネージドキー (SSE-KMS) を使用する必要があります。 AWS KMS 暗号化のサポートは、新しいランディングゾーンを設定するとき、または既存の AWS Control Tower ランディングゾーンを更新するときに使用できます。

この機能を設定するには、ランディングゾーンの初期設定時に [KMS Key Configuration] (KMS キー設定) を選択します。既存の KMS キーを選択するか、KMS AWS コンソールに誘導するボタンを選択して新しいキーを作成できます。また、デフォルトの暗号化から SSE-KMS、または別の SSE-KMS キーに変更できる柔軟性があります。

既存の AWS Control Tower ランディングゾーンでは、更新を実行して AWS KMS キーの使用を開始できます。

コントロールの名前が変更され、機能は変更されません

2021 年 7 月 26 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower は、コントロールのポリシー意図をよりよく反映するように、特定のコントロールの名前と説明を改訂しています。改訂された名前と説明は、コントロールがアカウントのポリシーを具現化する方法をより直感的に理解するのに役立ちます。例えば、検出コントロール自体が特定のアクションを停止せず、ポリシー違反を検出し、ダッシュボードを介してアラートを提供するだけであるため、検出コントロールの名前の一部を「許可しない」から「検出」に変更しました。

コントロールの機能、ガイダンス、および実装は変更ありません。コントロールの名前と説明のみ改訂されています。

AWS Control Tower は SCP を毎日スキャンしてドリフトをチェックするようになりました

2021 年 5 月 11 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower は、管理対象の SCP を毎日自動スキャンして、対応するコントロールが正しく適用され、ドリフトが発生していないことを確認するようになりました。スキャンでドリフトが検出されると、通知が届きます。AWS Control Tower は、ドリフトの問題ごとに通知を 1 つだけ送信するため、ランディングゾーンが既にドリフト状態にある場合、新しいドリフトアイテムが見つからない限り、追加の通知が送信されることはありません。

OU とアカウントのカスタマイズされた名前

2021 年 4 月 16 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、ランディングゾーンの名前付けをカスタマイズできるようになりました。AWS Control Tower が組織単位 (OU、Organizational Unit) およびコアアカウントに推奨する名前を保持するか、ランディングゾーン初期設定プロセス中にこれらの名前を変更することができます。

AWS Control Tower が OU およびコアアカウントに提供するデフォルトの名前は、 AWS マルチアカウントのベストプラクティスのガイダンスに合致しています。ただし、会社に特定の命名ポリシーがある場合、あるいは同じ推奨名を持つ既存の OU またはアカウントが既に存在する場合は、この新しい OU およびアカウント命名機能によって、これらの制約に柔軟に対応できます。

設定時のこのワークフローの変更とは別に、以前はコア OU と呼ばれていた OU はセキュリティ OU と呼ばれ、以前はカスタム OU と呼ばれていた OU はサンドボックス OU と呼ばれるようになりました。命名に関する全体的な AWS ベストプラクティスのガイダンスとの連携を改善するために、この変更を加えました。

新しいお客様には、これらの新しい OU 名が表示されます。既存のお客様には、これらの OU の元の名前が引き続き表示されます。ドキュメントを新しい名前に更新している間、OU の命名に不一致が生じることがあります。

AWS マネジメントコンソールから AWS Control Tower の使用を開始するには、AWS Control Tower コンソールに移動し、右上のランディングゾーンの設定を選択します。詳細については、「AWS Control Tower ランディングゾーンの計画」を参照してください。

AWS Control Tower ランディングゾーンバージョン 2.7

2021 年 4 月 8 日

(AWS Control Tower のランディングゾーンをバージョン 2.7 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください。)

AWS Control Tower バージョン 2.7 では、AWS Control Tower のリソースにのみポリシーを実装する 4 つの新しい必須予防的ログアーカイブコントロールが導入されました。AWS Control Tower の外にあるリソースのポリシーを設定するため、4 つの既存のログアーカイブコントロールのガイダンスを必須から選択的に調整しました。このコントロールの変更と拡張により、AWS Control Tower 内のリソースのログアーカイブガバナンスと AWS Control Tower 外のリソースのガバナンスを分離できます。

4 つの変更されたコントロールを新しい必須コントロールと組み合わせて使用して、より広範な AWS ログアーカイブのセットにガバナンスを提供できます。既存の AWS Control Tower 環境では、環境の一貫性を保つため、これらの 4 つの変更されたコントロールが自動的に有効になります。ただし、これらの選択的コントロールは無効にできるようになりました。新しい AWS Control Tower 環境では、すべての選択的コントロールを有効にする必要があります。既存の環境では、AWS Control Tower によってデプロイされていない Amazon S3 バケットに暗号化を追加する前に、以前は必須のコントロールを無効にする必要があります。

新しい必須コントロール:

- Disallow Changes to Encryption Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットの暗号化設定の変更を許可しない)
- Disallow Changes to Logging Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットのログ設定の変更を許可しない)
- Disallow Changes to Bucket Policy for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットのバケットポリシーの変更を許可しない)
- Disallow Changes to Lifecycle Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive (AWS Control Tower がログアーカイブに作成した Simple Storage Service (Amazon S3) バケットのライフサイクル設定の変更を許可しない)

必須から選択的に変更されたガイダンス:

- Disallow Changes to Encryption Configuration for all Amazon S3 Buckets (すべての Simple Storage Service (Amazon S3) バケットの暗号化設定の変更を許可しない) [Previously: Enable Encryption at Rest for Log Archive (以前: ログアーカイブの保管時に暗号化を有効にする)]
- Disallow Changes to Logging Configuration for all Amazon S3 Buckets (すべての Simple Storage Service (Amazon S3) バケットのログ設定の変更を許可しない) [Previously: Enable Access Logging for Log Archive (以前: ログアーカイブのアクセスログを有効にする)]
- Disallow Changes to Bucket Policy for all Amazon S3 Buckets (すべての Amazon S3 バケットのバケットポリシーの変更を不許可にする) [Previously: Disallow Policy Changes to Log Archive (以前: ログアーカイブのポリシー変更を禁止する)]
- Disallow Changes to Lifecycle Configuration for all Amazon S3 Buckets (すべての Simple Storage Service (Amazon S3) バケットのライフサイクル設定の変更を許可しない) [Previously: Set a Retention Policy for Log Archive (以前: ログアーカイブの保持ポリシーを設定する)]

AWS Control Tower バージョン 2.7 には、2.7 にアップグレードした後に以前のバージョンとの互換性がなくなる可能性がある AWS Control Tower ランディングゾーンのブループリントに対する変更が含まれています。

- 特に、AWS Control Tower バージョン 2.7 では、AWS Control Tower によってデプロイされた S3 バケットで自動的に `BlockPublicAccess` が有効になります。ワークロードでアカウント全体の

アクセスが必要な場合は、このデフォルトをオフにすることができます。BlockPublicaccess を有効にした場合の動作については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

- AWS Control Tower バージョン 2.7 には HTTPS の要件が含まれています。AWS Control Tower によってデプロイされた S3 バケットに送信されるすべてのリクエストは、Secure Sockets Layer (SSL) を使用する必要があります。HTTPS リクエストのみ渡すことができます。HTTP (SSL なし) をエンドポイントとして使用してリクエストを送信すると、この変更によってアクセス拒否エラーが発生し、ワークフローが中断する可能性があります。ランディングゾーンを 2.7 に更新した後で、この変更を元に戻すことはできません。

  HTTP の代わりに TLS を使用するようにリクエストを変更することをお勧めします。

3 つの新しい AWS リージョンが利用可能に

2021 年 4 月 8 日

(AWS Control Tower ランディングゾーンは更新が必要です。)

AWS Control Tower は、アジアパシフィック (東京) AWS リージョン、アジアパシフィック (ソウル) リージョン、アジアパシフィック (ムンバイ) リージョンの 3 つの追加リージョンで利用できます。これらのリージョンにガバナンスを拡大するには、ランディングゾーンをバージョン 2.7 に更新する必要があります。

バージョン 2.7 への更新を実行しても、ランディングゾーンがこれらのリージョンに自動的に展開されることはありません。含まれるようにするには、リージョン表でそれらを表示して選択する必要があります。

選択したリージョンのみを管理

2021 年 2 月 19 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower リージョンを選択すると、AWS Control Tower リソースの地理的フットプリントをより適切に管理できます。コンプライアンス、規制、コストなどの理由で AWS リソースまたはワークロードをホストするリージョンの数を拡張するために、管理する追加のリージョンを選択できるようになりました。

リージョン選択は、新しいランディングゾーンを設定するか、AWS Control Tower ランディングゾーンのバージョンを更新するときに利用できます。Account Factory を使用して新しいアカウント

を作成するか、既存のメンバーアカウントを登録する場合、または [Extend Governance] (ガバナンスを拡張) を使用して既存の組織単位にアカウントを登録する場合、AWS Control Tower は、アカウントの選択したリージョンにガバナンス機能 (一元化されたロギング、モニタリング、コントロール) をデプロイします。リージョンの選択の詳細については、「AWS Control Tower リージョンを設定する」を参照してください。

AWS Control Tower がガバナンスを AWS 組織内の既存の OUs に拡張

2021 年 1 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower コンソール内から既存の組織単位 (OU、Organizational Unit) (AWS Control Tower にない OU) にガバナンスを拡張します。この機能を使用すると、最上位の OU と含まれるアカウントを AWS Control Tower ガバナンス下に置くことができます。OU 全体へのガバナンスの拡張については、「AWS Control Tower に既存の組織単位を登録する」を参照してください。

OU を登録すると、AWS Control Tower は一連のチェックを実行して、ガバナンスの拡張と OU 内のアカウントの登録が正常に行われていることを確認します。OU の初期登録に関連する一般的な問題の詳細については、「登録時または再登録時に発生する障害のよくある原因」を参照してください。

また、AWS Control Tower 製品ウェブページにアクセスしたり、YouTube にアクセスして AWS Organizations向け AWS Control Tower の開始方法に関する動画を視聴することもできます。

AWS Control Tower でアカウントの一括更新が可能になりました

2021 年 1 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

一括更新機能により、最大 300 個のアカウントを含む登録済みの AWS Organizations 組織単位 (OU、Organizational Unit) のすべてのアカウントを、AWS Control Tower ダッシュボードから、1 回のクリックで更新できるようになりました。これは、AWS Control Tower ランディングゾーンを更新し、現行のランディングゾーンのバージョンに合うように登録済みアカウントも更新する必要がある場合に特に便利です。

また、この機能は、AWS Control Tower ランディングゾーンを更新して新しいリージョンに拡張する場合や、OU を再登録して OU のすべてのアカウントに最新のコントロールが適用されるようにする場合に、アカウントを最新状態に保つのに役立ちます。アカウントの一括更新により、アカウントを 1 つずつ更新したり、外部スクリプトを使用して複数のアカウントに対して更新を実行したりする必要がなくなります。

ランディングゾーンの更新の詳細については、「ランディングゾーンを更新する」を参照してください。

OU の登録または再登録の詳細については、「AWS Control Tower に既存の組織単位を登録する」を参照してください。

2020 年 1 月 ~ 12 月

2020 年、AWS Control Tower は次の更新をリリースしました。

- AWS Control Tower コンソールが外部 AWS Config ルールにリンクするようになりました
- AWS Control Tower が追加のリージョンで利用可能になりました
- ガードレールの更新
- AWS Control Tower コンソールに OU とアカウントの詳細が表示されます
- AWS Control Tower を使用して で新しいマルチアカウント AWS 環境をセットアップする AWS Organizations
- AWS Control Tower ソリューションのカスタマイズ
- AWS Control Tower バージョン 2.3 の一般提供
- AWS Control Tower でのシングルステップのアカウントプロビジョニング
- AWS Control Tower の廃止ツール
- AWS Control Tower のライフサイクルイベント通知

AWS Control Tower コンソールが外部 AWS Config ルールにリンクするようになりました

2020 年 12 月 29 日

(AWS Control Tower のランディングゾーンをバージョン 2.6 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください。)

AWS Control Tower に、外部 AWS Config ルールの検出を支援する組織レベルのアグリゲータが追加されました。これにより、AWS Control Tower コンソールで可視性が得られ、AWS Control Tower によって作成された Config AWS ルールに加えて、外部で作成された AWS Config ルールの存在を確認できます。アグリゲータを使用すると、AWS Control Tower は外部ルールを検出し、AWS Control Tower AWS がアンマネージドアカウントにアクセスすることなく、Config コンソールへのリンクを提供できます。

この機能により、アカウントに適用される検出コントロールの統合ビューが作成され、コンプライアンスを追跡し、アカウントに追加のコントロールが必要かどうかを判断できるようになりました。詳細については、「AWS Control Tower がアンマネージド OU とアカウントで AWS Config ルールを集約する方法 OUs」を参照してください。

AWS Control Tower が追加のリージョンで利用可能になりました

2020 年 11 月 18 日

(AWS Control Tower のランディングゾーンをバージョン 2.5 に更新する必要があります。詳細については、「ランディングゾーンを更新する」を参照してください。)

AWS Control Tower が 5 つの追加 AWS リージョンで利用可能になりました。

- アジアパシフィック (シンガポール) リージョン
- 欧州 (フランクフルト) リージョン
- 欧州 (ロンドン) リージョン
- 欧州 (ストックホルム) リージョン
- カナダ (中部) リージョン

これらの 5 AWS リージョンの追加は、AWS Control Tower のバージョン 2.5 で導入された唯一の変更です。

AWS Control Tower は、米国東部 (バージニア北部) リージョン、米国東部 (オハイオ) リージョン、米国西部 (オレゴン) リージョン、欧州 (アイルランド) リージョン、アジアパシフィック (シドニー) リージョンでも利用できます。このリリースで、AWS Control Tower が 10 AWS リージョンで利用可能になりました。

このランディングゾーンの更新には、リストされているすべてのリージョンが含まれており、元に戻すことはできません。ランディングゾーンをバージョン 2.5 に更新したら、AWS Control Tower のすべての登録済みアカウントを手動で更新して、サポートされている 10 の AWS リージョンで管理する必要があります。詳細については、AWS Control Tower リージョンを設定する を参照してください。

ガードレールの更新

2020 年 10 月 8 日

(AWS Control Tower ランディングゾーンの更新は不要です)

必須コントロール AWS-GR_IAM_ROLE_CHANGE_PROHIBITED の更新バージョンがリリースされました。

AWS Control Tower に自動的に登録されるアカウントは AWSControlTowerExecution ロールを有効にする必要があるため、コントロールのこの変更が必要になります。コントロールの以前のバージョンでは、このロールは作成されません。

詳細については、AWS Control Tower によって設定された AWS IAM ロールへの変更の禁止および AWS Control Tower Controls リファレンスガイドの AWS CloudFormation「」を参照してください。

AWS Control Tower コンソールに OU とアカウントの詳細が表示されます

2020 年 7 月 22 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower に登録されていない組織およびアカウントを、登録されている組織およびアカウントと共に表示できます。

AWS Control Tower コンソールでは、 AWS アカウントと組織単位 (OUs) の詳細を表示できます。[Accounts] (アカウント) ページには、AWS Control Tower での OU や 登録のステータスに関係なく、組織内のすべてのアカウントが一覧表示されるようになりました。すべてのテーブルで検索、並べ替え、フィルタリングを実行できるようになりました。

AWS Control Tower を使用して で新しいマルチアカウント AWS 環境をセットアップする AWS Organizations

2020 年 4 月 22 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Organizations のお客様は、AWS Control Tower を使用して、新しく作成された組織単位 (OUs) とアカウントを管理できるようになりました。

- 既存の AWS Organizations お客様は、既存の管理アカウントで新しい組織単位 (OUs) の新しいランディングゾーンを設定できるようになりました。AWS Control Tower で新しい OU を作成し、AWS Control Tower ガバナンスを使用して OU に新しいアカウントを作成できます。
- AWS Organizations のお客様は、アカウント登録プロセスまたはスクリプトを使用して、既存のアカウントを登録できます。

AWS Control Tower は、他の サービスを使用するオーケストレーション AWS サービスを提供します。これは、新規または既存のマルチアカウント AWS 環境を設定し、大規模に管理するための最も簡単な方法を探している複数のアカウントとチームを持つ組織向けに設計されています。AWS Control Tower によって管理されている組織では、クラウド管理者は、組織内のアカウントが確立されたポリシーに準拠していることを知っています。ビルダーは、コンプライアンスについて過度に懸念することなく、新しい AWS アカウントを迅速にプロビジョニングできるため、メリットがあります。

ランディングゾーンの設定の詳細については、「AWS Control Tower ランディングゾーンの計画」を参照してください。また、AWS Control Tower 製品ウェブページにアクセスしたり、YouTube にアクセスして AWS Organizations向け AWS Control Tower の開始方法に関する動画を視聴することもできます。

この変更に加えて、AWS Control Tower のクイックアカウントプロビジョニング機能の名前がアカウントの登録に変更されました。既存の AWS アカウントの登録と新しいアカウントの作成が可能になりました。詳細については、「既存のアカウントを登録する」を参照してください。

AWS Control Tower ソリューションのカスタマイズ

2020 年 3 月 17 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower には、カスタムテンプレートおよびポリシーを AWS Control Tower ランディングゾーンに簡単に適用できる新しいリファレンス実装が追加されました。

AWS Control Tower のカスタマイズを使用すると、 AWS CloudFormation テンプレートを使用して、組織内の既存アカウントと新規アカウントに新しいリソースをデプロイできます。また、これらのアカウントには、AWS Control Tower によって既に提供されているサービスコントロールポリシー (SCP、Service Control Policies) に加えて、カスタム SCP を適用することもできます。AWS Control Tower パイプラインのカスタマイズは、リソースのデプロイとランディングゾーンの同期が保たれるように、AWS Control Tower のライフサイクルイベントおよび通知 (「AWS Control Tower のライフサイクルイベント」) と統合されます。

この AWS Control Tower ソリューションアーキテクチャのデプロイドキュメントは、AWS Solutions ウェブページから入手できます。

AWS Control Tower バージョン 2.3 の一般提供

2020 年 3 月 5 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「ランディングゾーンを更新する」を参照してください。)

AWS Control Tower が、米国東部 (オハイオ) 、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、欧州 (アイルランド) AWS の各リージョンに加えて、アジアパシフィック (シドニー) リージョンで利用可能になりました。アジアパシフィック (シドニー) リージョンの追加は、AWS Control Tower のバージョン 2.3 で導入された唯一の変更点です。

これまで AWS Control Tower を使用していなかった場合は、サポートされている任意のリージョンで今すぐ AWS Control Tower を起動できます。既に AWS Control Tower を使用していて、アカウントのアジアパシフィック (シドニー) リージョンにガバナンス機能を拡張する場合は、AWS Control Tower ダッシュボードの [Settings] (設定) ページに移動します。そこから、ランディングゾーンを最新リリースに更新します。そして、アカウントを個別に更新します。

> **Note**
>
> ランディングゾーンを更新しても、アカウントは自動的に更新されません。アカウントが数個以上ある場合は、必要な更新を行うのに時間がかかることがあります。そのため、ワークロードの実行を必要としないリージョンに AWS Control Tower ランディングゾーンを拡張することは避けてください。

新しいリージョンへのデプロイの結果としての検出コントロールの予想される動作の詳細については、「Configure your AWS Control Tower Regions」を参照してください。

AWS Control Tower でのシングルステップのアカウントプロビジョニング

2020 年 3 月 2 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower コンソールを使用したシングルステップのアカウントプロビジョニングをサポートするようになりました。この機能を使用すると、AWS Control Tower コンソール内から新しいアカウントをプロビジョニングできます。

簡略化された形式を使用するには、AWS Control Tower コンソールの [Account Factory] に移動し、[Quick account provisioning] (クイックアカウントプロビジョニング) を選択します。AWS Control Tower は、プロビジョニングされたアカウントとそのアカウントに作成された Single Sign-On (IAM Identity Center) ユーザーに同じ E メールアドレスを割り当てます。これら 2 つの E メール

アドレスを異なるものにする必要がある場合は、Service Catalog を通じてアカウントをプロビジョニングする必要があります。

他のアカウントの更新と同様に、Service Catalog および AWS Control Tower Account Factory を使用して、クイックアカウントプロビジョニングで作成したアカウントを更新します。

> **Note**
>
> 2020 年 4 月、クイックアカウントプロビジョニング機能の名前がアカウントの登録に変更されました。2022 年 6 月、AWS Control Tower コンソールでアカウントを作成および更新する機能は、 AWS アカウントを登録する機能とは分離されました。詳細については、「既存のアカウントを登録する」を参照してください。

AWS Control Tower の廃止ツール

2020 年 2 月 28 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower は、AWS Control Tower によって割り当てられたリソースのクリーンアップを支援する自動廃止ツールをサポートするようになりました。AWS Control Tower を企業で使用しなくなった場合、または組織のリソースに大幅な再デプロイが必要な場合は、ランディングゾーンを最初にセットアップしたときに作成されたリソースをクリーンアップすることができます。

ほぼ自動化されたプロセスを使用してランディングゾーンを廃止するには、 AWS サポート に連絡して、必要な追加のステップについてサポートを受けてください。廃止の詳細については、「チュートリアル: AWS Control Tower ランディングゾーンを廃止する」を参照してください。

AWS Control Tower のライフサイクルイベント通知

2020 年 1 月 22 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、ライフサイクルイベント通知が利用可能になりました。ライフサイクルイベントは、AWS Control Tower で作成および管理する組織単位 (OU)、アカウント、コントロールなどのリソースの状態を変更できる AWS Control Tower アクションの完了をマークします。ライフサイクルイベントは、 AWS CloudTrail イベントとして記録され、Amazon EventBridge にイベントとして配信されます。

AWS Control Tower は、サービスを使用して実行できる次のアクションの完了時にライフサイクルイベントを記録します: ランディングゾーンの作成または更新、OU の作成または削除、OU でのコントロールの有効化または無効化、Account Factory を使用した新規アカウントの作成または別の OU へのアカウントの移動。

AWS Control Tower は、複数の AWS サービスを使用して、ベストプラクティスのマルチアカウント AWS 環境を構築および管理します。AWS Control Tower アクションが完了するまで数分かかることがあります。CloudTrail ログでライフサイクルイベントを追跡して、元の AWS Control Tower アクションが正常に完了したかどうかを確認できます。EventBridge ルールを作成して、CloudTrail がライフサイクルイベントを記録したときに通知したり、オートメーションワークフローで次のステップを自動的にトリガーしたりすることができます。

2019 年 1 月 ~ 12 月

2019 年 1 月 1 日から 12 月 31 日までに、AWS Control Tower は次の更新をリリースしました。

- AWS Control Tower バージョン 2.2 の一般提供
- AWS Control Tower の新しい選択的コントロール
- AWS Control Tower の新しい検出コントロール
- AWS Control Tower は、管理アカウントとは異なるドメインを持つ共有アカウントの E メールアドレスを受け付けます
- AWS Control Tower バージョン 2.1 の一般提供

AWS Control Tower バージョン 2.2 の一般提供

2019 年 11 月 13 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「ランディングゾーンを更新する」を参照してください。)

AWS Control Tower バージョン 2.2 では、アカウントのドリフトを防止する 3 つの新しい予防コントロールが用意されています。

- AWS Control Tower によって設定された Amazon CloudWatch Logs ロググループへの変更を許可しない
- AWS Control Tower によって作成された AWS Config 集約認可の削除を禁止する
- ログアーカイブの削除を許可しない

コントロールは、 AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。AWS Control Tower ランディングゾーンを作成するとき、ランディングゾーンとすべての組織単位 (OU、Organizational Unit)、アカウント、リソースは、選択したコントロールによって適用されるガバナンスルールに準拠します。ユーザーおよび組織のメンバーがランディングゾーンを使用する際、コンプライアンスステータスが (偶発的または意図的に) 変更されることがあります。ドリフト検出は、ドリフトを解決するために変更や設定更新が必要になるリソースを識別するのに役立ちます。詳細については、「AWS Control Tower でドリフトを検出して解決する」を参照してください。

AWS Control Tower の新しい選択的コントロール

2019 年 9 月 5 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower には、次の 4 つの新しい選択的コントロールが含まれるようになりました。

- MFA を使用しない Amazon S3 バケットでの削除アクションを許可しない
- Amazon S3 バケットのレプリケーション設定の変更を許可しない
- ルートユーザーとしてのアクションを許可しない
- ルートユーザーのアクセスキーの作成を許可しない

コントロールは、 AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。ガードレールを使用すると、ポリシーの意図を表現できます。詳細については、「About controls in AWS Control Tower」を参照してください。

AWS Control Tower の新しい検出コントロール

2019 年 8 月 25 日

(AWS Control Tower ランディングゾーンの更新は不要です)

AWS Control Tower には、次の 8 つの新しい検出コントロールが含まれるようになりました。

- Amazon S3 バケットのバージョニングが有効になっているかどうかを検出する
- AWS コンソールの IAM ユーザーに対して MFA が有効になっているかどうかを検出する
- IAM ユーザーに対して MFA が有効になっているかどうかを検出する
- Amazon EC2 インスタンスに対して Amazon EBS 最適化が有効になっているかどうかを検出する

- Amazon EBS ボリュームが Amazon EC2 インスタンスにアタッチされているかどうかを検出する
- Amazon RDS データベースインスタンスへのパブリックアクセスが有効になっているかどうかを検出する
- Amazon RDS データベーススナップショットへのパブリックアクセスが有効になっているかどうかを検出する
- Amazon RDS データベースインスタンスに対してストレージ暗号化が有効になっているかどうかを検出する

コントロールは、 AWS 環境全体に継続的なガバナンスを提供する高レベルのルールです。検出コントロールは、ポリシー違反など、アカウント内のリソースの非準拠を検出し、ダッシュボードを通じてアラートを提供します。詳細については、「About controls in AWS Control Tower」を参照してください。

AWS Control Tower は、管理アカウントとは異なるドメインを持つ共有アカウントの E メールアドレスを受け付けます

2019 年 8 月 1 日

(AWS Control Tower ランディングゾーンに更新は必要ありません。)

AWS Control Tower で、ドメインが管理アカウントの E メールアドレスと異なる共有アカウント (ログアーカイブと監査メンバー) および子アカウント (Account Factory を使用して提供) の E メールアドレスを送信できるようになりました。この機能は、新しいランディングゾーンを作成する場合、および新しい子アカウントをプロビジョニングする場合にのみ使用できます。

AWS Control Tower バージョン 2.1 の一般提供

2019 年 6 月 24 日

(AWS Control Tower ランディングゾーンの更新が必要です。詳細については、「Update Your Landing Zone」を参照してください。)

AWS Control Tower は、本番稼働用に一般提供され、サポートされるようになりました。AWS Control Tower は、複数のアカウントを持つ組織や、新しいマルチアカウント AWS 環境を設定し、大規模に管理するための最も簡単な方法を探しているチームを対象としています。AWS Control Tower を使用すると、組織のアカウントが確立されたポリシーに確実に準拠するようにすることができます。分散チームのエンドユーザーは、新しい AWS アカウントを迅速にプロビジョニングできます。

AWS Control Tower を使用すると、 を使用したマルチアカウント構造の設定 AWS Organizations、を使用したユーザー ID とフェデレーティッドアクセスの管理、Service Catalog によるアカウントプロビジョニングの有効化 AWS IAM Identity Center、 AWS CloudTrail と を使用した集中ログアーカイブの作成などのベストプラクティスを採用するランディングゾーンを設定できます AWS Config。

継続的なガバナンスのために、セキュリティ、運用、コンプライアンスに関する明確に定義されたルールである事前構成済みのコントロールを有効にできます。ガードレールは、ポリシーに準拠しないリソースのデプロイを防止し、デプロイされたリソースの不適合を継続的に監視するのに役立ちます。AWS Control Tower ダッシュボードは、プロビジョニングされたアカウント、有効化されたコントロール、アカウントのコンプライアンスステータスなど、 AWS 環境を一元的に可視化します。

AWS Control Tower コンソールで 1 回クリックするだけで、新しいマルチアカウント環境を設定できます。AWS Control Tower を使用するのに追加料金や前払いの義務はありません。ランディングゾーンの設定と選択したコントロールの実装を有効にした AWS サービスに対してのみ料金が発生します。

ドキュメント履歴

- ドキュメントの最終更新日： 2024 年 12 月 10 日

次の表は、「AWS Control Tower ユーザーガイド」に対する重要な変更点の一覧です。ドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
AWS Control Tower がサービスにリンクされたロールを更新する	の更新`AWSControlTowerAccountServiceRolePolicy` 。	2024 年 12 月 10 日
AWS Control Tower CfCT が GitHub をサポート	サードパーティー設定ソースの新しいオプション。	2024 年 12 月 9 日
宣言ポリシーを使用した AWS Control Tower 予防コントロール	新しいタイプのポリシーは、新しいタイプの予防コントロールを実装します。	2024 年 12 月 1 日
AWS Control Tower と AWS Backup の統合	AWS Control Tower リソースをバックアップするプランを設定できます。	2024 年 11 月 25 日
AWS Control Tower は AWS Config コントロールを統合します	AWS Control Tower は、選択した AWS Config コントロールを統合します。	2024 年 11 月 21 日
AWS Control Tower がフック管理を改善	AWS Control Tower がプロアクティブコントロールのフックを管理するようになりました。	2024 年 11 月 20 日
コントロールポリシードリフトが報告されました	AWS Control Tower は、新しいタイプのドリフトを報告します。	2024 年 11 月 15 日

AWS Control Tower がマネージドリソースコントロールポリシーを起動	RCPs で実装された新しいタイプの予防コントロール。	2024 年 11 月 15 日
AWS Control Tower が ResetEnabledControl API を追加	コントロールドリフトを管理するための新しい API。	2024 年 11 月 14 日
`GetControl` API の更新	の 2 つの新しいコントロールフィールド`GetControl` 。	2024 年 11 月 8 日
AWS Control Tower AFT が GitLab をサポート	サードパーティー設定ソースの新しいオプション。	2024 年 10 月 23 日
AWS Control Tower が AWS アジアパシフィック (マレーシア) リージョンで利用可能に	新しいリージョンであるマレーシア (クアラルンプール) が利用可能になりました。	2024 年 10 月 21 日
AWS Control Tower が OU あたり最大 1000 アカウントをサポート	OU あたりのアカウント数の制限が引き上げられました。	2024 年 8 月 30 日
AWS Control Tower でランディングゾーンバージョンの選択が可能に	3.1 以降を実行している場合は、最新バージョンに移行せずにランディングゾーンを更新または修復できます。	2024 年 8 月 15 日
GetControl および ListControls API オペレーションが利用可能に	2 つの新しい Control Catalog オペレーションは、コントロールの詳細情報を確認するのに役立ちます。	2024 年 8 月 6 日
AWS Control Tower がオプトインリージョンで AFT と CfCT をサポート	AFT と CfCT は追加で利用できます AWS リージョン。	2024 年 7 月 18 日
AWS Control Tower に `ListLandingZoneOperations` API を追加	ランディングゾーンの最近のオペレーションを取得できる新しい API。	2024 年 6 月 26 日

AWS Control Tower が最大 100 の同時コントロールオペレーションをサポート	同時コントロールオペレーションのクォータが 100 に引き上げられました。	2024 年 5 月 20 日
AWS Control Tower が AWS カルガリー西部 (カナダ) リージョンで利用可能に	AWS Control Tower がカナダ西部 (カルガリー) リージョンで利用可能になりました。	2024 年 5 月 3 日
AWS Control Tower がセルフサービスのクォータ調整をサポート	AWS Control Tower は、 コンソールの AWS Service Quotas と統合されています。	2024 年 4 月 25 日
コントロールのドキュメントを新しいガイドに移動	AWS Control Tower の「Controls Reference Guide」が発行されました。	2024 年 4 月 21 日
AWS CloudFormationでの `EnabledControl` リソースのタグ付け	AWS Control Tower は、 AWS CloudFormation テンプレートによる`EnabledControl` リソースへのタグの追加をサポートしています。	2024 年 2 月 22 日
ベースライン API が利用可能に	AWS Control Tower が OU をプログラムによって登録するための新しい API をリリースしました。	2024 年 2 月 14 日
AWS Control Tower ランディングゾーンバージョン 3.3	AWS Control Tower ランディングゾーンバージョン 3.3 が利用可能になりました。	2023 年 12 月 14 日
AWS Control Tower がデジタル主権を支援するコントロールを発表	AWS Control Tower は、お客様のデジタル主権の要件を支援する一連のコントロールをリリースしました。	2023 年 11 月 27 日

AWS Control Tower がランディングゾーン API をサポート	AWS Control Tower は、新しい API を使用したランディングゾーンの設定と起動をサポートします。	2023 年 11 月 26 日
AWS Control Tower が、有効になっているコントロールのタグ付けをサポート	AWS Control Tower では、コンソールから、および新しい API により、有効になっているコントロールのタグ付けがサポートされます。	2023 年 11 月 10 日
AWS Control Tower がアジアパシフィック (メルボルン) で利用可能に AWS リージョン	アジアパシフィック (メルボルン) リージョンで利用可能。	2023 年 11 月 3 日
新しいコントロール API が利用可能に	AWS Control Tower が新しいコントロール API をリリースしました。	2023 年 10 月 14 日
AWS Control Tower が新しいコントロールをリリース	AWS Control Tower が新しいプロアクティブコントロールと検出コントロールをリリースしました。	2023 年 10 月 5 日
AWS Control Tower が信頼できるアクセスの無効化に伴うドリフトを報告	お客様が AWS Organizations で AWS Control Tower への信頼できるアクセスをオフにした際にドリフトが発生すると、AWS Control Tower から通知されます。	2023 年 9 月 21 日
AWS Control Tower が 4 つの追加で利用可能に AWS リージョン	アジアパシフィック (ハイデラバード)、欧州 (スペインおよびチューリッヒ)、中東 (アラブ首長国連邦) で利用可能です。	2023 年 9 月 13 日

AWS Control Tower がテルアビブリージョンで利用可能に	AWS Control Tower が、テルアビブリージョン (il-central-1) で利用可能になりました。	2023 年 8 月 28 日
AWS Control Tower が 28 個の新しいプロアクティブコントロールをリリース	AWS Control Tower が 28 個の新しいプロアクティブコントロールをリリースしました。	2023 年 7 月 24 日
AWS Control Tower で 2 つのコントロールが廃止されます	AWS Control Tower は、2023 年 8 月 18 日にコントロールライブラリから 2 つのコントロールを削除しました。	2023 年 7 月 18 日
AWS Control Tower ランディングゾーン 3.2 が利用可能に	AWS Control Tower ランディングゾーンバージョン 3.2 が利用可能になりました。	2023 年 6 月 16 日
AWS Control Tower は、ID に基づいてアカウントを処理します	AWS Control Tower は、 AWS アカウントの E メールアドレスではなく、アカウント ID を追跡します。	2023 年 6 月 14 日
追加の Security Hub 検出コントロールが利用可能に	AWS Control Tower は、Security Hub サービスマネージドスタンダード: AWS Control Tower 用に 10 個の新しいコントロールをコントロールライブラリに追加します。	2023 年 6 月 12 日
AWS Control Tower はコントロールメタデータテーブルを公開します	AWS Control Tower では、公開されたドキュメントの一部としてコントロールメタデータのテーブルが提供されるようになりました。	2023 年 6 月 7 日

Account Factory のカスタマイズに対する Terraform サポート	AFC の Terraform オープンソースブループリントの単一リージョンサポート。	2023 年 6 月 6 日
AWS ランディングゾーンで利用可能な IAM 自己管理	AWS Control Tower では、お客様がランディングゾーンの ID プロバイダーを選択できるようになりました。	2023 年 6 月 6 日
新しいロールが追加されました	AWS Control Tower に、サービスにリンクされた新しいロール AWSServiceRoleForAWSControlTower と、関連するポリシー AWSServiceRoleForAWSControlTower が追加されました。	2023 年 6 月 1 日
混合ガバナンスの更新	混合ガバナンスについてお客様にアドバイスするための更新	2023 年 6 月 1 日
追加のプロアクティブコントロールが利用可能になりました	新しいプロアクティブコントロールは、マルチアカウント環境を管理し、特定のコントロール目標を達成するのに役立ちます。	2023 年 5 月 19 日
リージョンがさらに 7 つ利用可能になりました	AWS Control Tower が AWS リージョン、北カリフォルニア (サンフランシスコ) 、アジアパシフィック (香港、ジャカルタ、大阪) 、欧州 (ミラノ) 、中東 (バーレーン) 、アフリカ (ケープタウン) の 7 つの追加で利用可能になりました。	2023 年 4 月 19 日

マネージドポリシーへの変更	AWSControlTowerServiceRolePolicy を変更し、AWS Control Tower が AWS アカウント管理サービスによって実装されている `EnableRegion` 、`ListRegions` 、`GetRegionOptStatus` APIs を呼び出せるようにしました。	2023 年 4 月 6 日
アカウントのカスタマイズリクエストの追跡が一般公開されました	AWS Control Tower では、Account Factory for Terraform (AFT) のワークフローを使用して、アカウントのカスタマイズリクエストを追跡できるようになりました	2023 年 2 月 16 日
IAM ベストプラクティスの更新	IAM ベストプラクティスの推奨事項に合わせてガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。	2023 年 2 月 15 日
AWS Control Tower ランディングゾーンバージョン 3.1 が利用可能に	AWS Control Tower ランディングゾーンバージョン 3.1 が利用可能になりました。	2023 年 2 月 9 日
プロアクティブコントロールの一般公開	プロアクティブコントロールはプレビュー版から一般公開に変わりました。	2023 年 1 月 24 日

同時アカウント操作	AWS Control Tower で、最大 5 つの Account Factory の同時実行アクションがサポートされるようになりました。一度に最大 5 つのアカウントを作成、更新、または登録できるようになります。	2022 年 12 月 16 日
プロアクティブコントロールによるリソースのプロビジョニングのサポート	AWS Control Tower は、 AWS CloudFormation フックを介して実装されるプロアクティブコントロールをサポートするようになりました。	2022 年 11 月 28 日
Account Factory Customization が利用可能に	AWS Control Tower で、ブループリントと呼ばれるカスタマイズ可能なアカウントテンプレートを使用するアカウントのプロビジョニングが AWS Control Tower コンソールから直接実行できるようになりました。	2022 年 11 月 28 日
すべての AWS Config ルールで表示可能なコンプライアンスステータス	AWS Control Tower は、AWS Control Tower に登録された組織単位にデプロイされたすべての AWS Config ルールのコンプライアンスステータスを表示するようになりました。	2022 年 11 月 18 日

マネージドポリシーへの変更	Account Factory Customization に必要な `AWSControlTowerBlueprintAccess` ロールを AWS Control Tower が引き継ぐことができるように、AWSControlTowerServiceRolePolicy が変更されました。	2022 年 10 月 28 日
コントロールAPIs、 AWS CloudFormation リソース	AWS Control Tower は、一連の API コールと新しい AWS CloudFormation リソースによるコントロールのアクティブ化と非アクティブ化をサポートするようになりました。	2022 年 9 月 1 日
CfCT がスタックセットの削除をサポート	CfCT は、マニフェストファイルにパラメータを設定することにより、スタックセットの削除をサポートします。	2022 年 8 月 26 日
カスタマイズされたログの保持	AWS Control Tower CloudTrail ログを日単位または年単位で最大 15 年まで保存するという Amazon S3 バケットの保持ポリシーをカスタマイズできます。	2022 年 8 月 15 日
ロールドリフト修理可能	AWS Control Tower は、ランディングゾーンを完全に修理しない状態のロールドリフトの修理をサポートします。	2022 年 8 月 11 日

バージョン 3.0 が利用可能	AWS Control Tower ランディングゾーンバージョン 3.0 は、アカウントベースの AWS CloudTrail 証跡から組織ベースの証跡に変更され、管理ポリシーを更新して組織レベルの証跡を有効にします。これにより、ホームリージョンでのみ AWS Config 情報を集約できます。バージョン 3.0 には、リージョン拒否コントロールと 2 つの新しい検出コントロールも含まれています。	2022 年 7 月 29 日
OU とアカウントのビューが組み合わされた組織ページ	AWS Control Tower の新しい [Organization] (組織) ページには、すべての組織単位 (OU) とアカウントの階層的なビューが表示されます。	2022 年 7 月 18 日
マネージドポリシーへの変更	AWSControlTowerServiceRolePolicy を変更し、お客様が組織レベルの AWS CloudTrail 証跡を作成して AWS CloudTrail ログを集約できるようにしました。	2022 年 6 月 20 日

メンバーアカウントの登録と更新が容易に	AWS Control Tower では、ランディングゾーン内から、メンバーアカウントを個別に登録および更新することができるようになりました。各アカウントには更新がいつ利用可能かが表示されます。Account Factory の [Create] (作成) アカウントワークフローから [Enroll account] (アカウントの登録) ボタンを分離しました。	2022 年 5 月 31 日
AFT は共有アカウントのカスタマイズをサポートしています	AWS Control Tower Account Factory for Terraform は、AWS Control Tower の管理アカウント、ログアーカイブ、監査アカウントのカスタマイズをサポートするようになりました。	2022 年 5 月 27 日
すべてのオプションのコントロールの同時操作	AWS Control Tower では、オプションの予防ガードレールと検出コントロールを同時に適用または削除できるようになりました。	2022 年 5 月 18 日
既存のセキュリティアカウントとログアカウント	AWS Control Tower は、ランディングゾーンのセットアップ中に新しいアカウントを作成するのではなく、既存のセキュリティアカウントとログアカウントを持ち込む機能をサポートするようになりました。	2022 年 5 月 16 日

バージョン 2.9 が利用可能に	AWS Control Tower のランディングゾーンバージョン 2.9 は、Python バージョン 3.9 ランタイムを使用するように通知フォワーダー Lambda を更新します。	2022 年 4 月 22 日
AWS ベストプラクティス、バージョン 2.8 のサポートを更新	AWS Control Tower ランディングゾーンバージョン 2.8 では、ワークロードと AWS アカウントが AWS ベストプラクティスに準拠していることを確認するための追加サポートが提供されます。	2022 年 2 月 10 日
リージョン拒否コントロール	AWS Control Tower には、コンプライアンスや規制上の懸念に対処するために、 AWS リージョンへのアクセスを制限するのに役立つコントロールが含まれるようになりました。	2021 年 11 月 30 日
データレジデンシーコントロール	AWS Control Tower で、きめ細かな制御によるデータの所在場所管理に役立つコントロールがサポートされるようになりました。	2021 年 11 月 30 日
AWS Control Tower Account Factory for Terraform	AWS Control Tower では、自動化されたアカウントのプロビジョニングと更新のために Terraform がサポートされるようになりました。	2021 年 11 月 29 日

新しいライフサイクルイベントが利用可能に	`PrecheckOrganizationalUnit` イベントは、ネストされた OU のリソースを含め、[Extend governance] (ガバナンスを拡張) タスクが成功しないようリソースがブロックしているかどうかを記録します。	2021 年 11 月 18 日
ネストされた OU が利用可能に	AWS Control Tower では、ランディングゾーンにネストされた OU 構造を含めることができるようになりました。	2021 年 11 月 16 日
検出コントロールの同時実行性	AWS Control Tower の検出コントロールで、同時有効化および無効化操作がサポートされるようになりました。	2021 年 11 月 5 日
2 つの新しいリージョンが利用可能に	AWS Control Tower が欧州 (パリ) AWS リージョンと南米 (サンパウロ) リージョンの 2 つの新しいリージョンで利用可能になりました。	2021 年 7 月 29 日
リージョンの選択解除	AWS Control Tower を通じて、管理したくない AWS リージョンの選択を解除できます。	2021 年 7 月 29 日
KMS キーが利用可能に	必要に応じて、管理する KMS キーを作成または選択して、データとリソースを暗号化できます。	2021 年 7 月 28 日

マネージドポリシーへの変更	AWSControlTowerServiceRolePolicy を変更し、お客様が AWS CloudTrail ログに独自の KMS 暗号化キーを使用できるようにしました。	2021 年 7 月 28 日
コントロールの名前を変更、機能は変更なし	コントロールのポリシーの意図をより適切に反映するように、一部のコントロールの名前と説明が更新されました。機能に変更はありません。	2021 年 7 月 26 日
マネージド SCP の自動スキャン	AWS Control Tower は、マネージド SCP を毎日自動スキャンしてドリフトをチェックします。	2021 年 5 月 11 日
OU とアカウントのカスタマイズされた名前	AWS Control Tower では、ランディングゾーンのセットアッププロセス中に、重要な OU とアカウントに対して、ドリフトを生成せずに、カスタマイズした名前を指定できます。	2021 年 4 月 16 日
ランディングゾーンの廃止がセルフサービスに	AWS Control Tower では、AWS Support に連絡することなく、ランディングゾーンを廃止できるようになりました。廃止は半自動プロセスであり、元に戻すことはできません。すべての AWS Control Tower リソースを手動で削除することとは異なります。	2021 年 4 月 9 日

3 つの追加リージョン	AWS Control Tower が、アジアパシフィック (東京) AWS リージョン、アジアパシフィック (ソウル) リージョン、アジアパシフィック (ムンバイ) リージョンの 3 つの追加リージョンで利用可能になりました。	2021 年 4 月 8 日
新しいログアーカイブコントロール、ランディングゾーンバージョン 2.7 が利用可能に	4 つの新しいログアーカイブコントロールは、AWS Control Tower の外部リソースのガバナンスとは別に、AWS Control Tower リソースに対するログアーカイブのガバナンスを提供します。既存の 4 つのコントロールに関するガイダンスが、必須から選択式に変更されました。AWS Control Tower のランディングゾーンバージョン 2.7 には HTTPS の要件が含まれており、更新後に元に戻すことはできません。	2021 年 4 月 8 日

リージョンの選択	AWS Control Tower リージョンを選択すると、AWS Control Tower リソースの地理的フットプリントをより適切に管理できます。コンプライアンス、規制、コスト、その他の理由から、 AWS リソースまたはワークロードをホストするリージョンの数を増やすために、管理するリージョンを追加で選択できるようになりました。	2021 年 2 月 19 日
OU を登録し、AWS Control Tower ですべてのアカウントを一度に管理する	AWS Control Tower では、OU を登録する機能が追加されています。この方法により、複数のアカウントを同時にガバナンスの対象とすることができます。	2021 年 1 月 28 日
登録された OU での複数のアカウントの更新	AWS Control Tower ダッシュボードから、最大 300 のアカウントを含む登録済み AWS Organizations 組織単位 (OU) 内のすべてのアカウントをワンクリックで更新できるようになりました。複数アカウントの更新機能は一括更新とも呼ばれ、一度に 1 つのアカウントを更新したり、外部スクリプトを使用して複数のアカウントに対して更新を実行したりする必要がなくなります。	2021 年 1 月 28 日

管理対象外の OU とアカウントを集約するための新しいロール	新しいロールは外部 AWS Config ルールの検出に役立つため、AWS Control Tower はアンマネージドアカウントにアクセスする必要はありません。	2020 年 12 月 29 日
AWS Control Tower は、より多くの AWS リージョンで利用できます。	AWS Control Tower は、アジアパシフィック (シンガポール) リージョン、欧州 (フランクフルト) リージョン、欧州 (ロンドン) リージョン、欧州 (ストックホルム) リージョン、カナダ (中部) リージョンでデプロイできるようになりました。このリリースで、AWS Control Tower が 10 AWS リージョンで利用可能になりました。このランディングゾーンの更新には、リストされているすべてのリージョンが含まれており、元に戻すことはできません。ランディングゾーンをバージョン 2.5 に更新したら、AWS Control Tower のすべての登録済みアカウントを手動で更新して、サポートされている 10 の AWS リージョンで管理する必要があります。	2020 年 11 月 18 日

コントロールの更新	必須コントロール AWS-GR_IAM_ROLE_CHANGE_PROHIBITED の更新バージョンがリリースされました。更新されたコントロールでは、アカウントの自動登録が簡単になりました。	2020 年 10 月 8 日
AWS Control Tower の関連情報ページが利用可能に	関連情報ページでは、AWS Control Tower のランディングゾーンを設定した後に役立つ一般的なタスクを簡単に探すことができます。	2020 年 9 月 18 日
AWS Control Tower コンソールに OU とアカウントの詳細が表示される	AWS Control Tower コンソールでは、 AWS アカウントと組織単位 (OUs) の詳細を表示できます。[Accounts] (アカウント) ページに、OU や AWS Control Tower の登録ステータスに関係なく、組織内のすべてのアカウントが一覧表示されるようになりました。すべてのテーブルで検索、並べ替え、フィルタリングを実行できるようになりました。	2020 年 7 月 22 日

AWS Control Tower により、既存の組織でランディングゾーンをセットアップ可能に	既存の組織で AWS Control Tower のランディングゾーンを起動して、組織をガバナンスに組み込むことができるようになりました。AWS Control Tower のクイックアカウントプロビジョニング機能の名前が「アカウントの登録」に変更され、既存の AWS アカウントの登録と新しいアカウントの作成が可能になりました。	2020 年 4 月 16 日
AWS Control Tower がアジアパシフィックで利用可能に	AWS Control Tower がアジアパシフィック (シドニー) AWS リージョンでデプロイできるようになりました。このリリースでは、提供アカウントを手動で更新する必要があります。更新は、アジアパシフィック (シドニー) でワークロードを実行する場合にのみ行います。	2020 年 3 月 3 日
AWS Control Tower のランディングゾーンの廃止が可能に	AWS サポートは、組織を維持するほぼ自動化されたプロセスを通じてランディングゾーンを完全に廃止するのに役立ちますが、手動によるクリーンアップが必要です。	2020 年 2 月 27 日

クイックアカウントプロビジョニングが AWS Control Tower で利用可能に	クイックアカウントプロビジョニングでは、[Enroll account] (アカウントの登録) 機能を使用して、ランディングゾーンが最新の状態になったときに新しいメンバーアカウントをさらに簡単に起動できるようになりました。	2020 年 2 月 20 日
ライフサイクルイベントが AWS Control Tower で追跡対象に	ライフサイクルイベントは、一部のワークフローのオートメーションを容易にするため、特定の AWS Control Tower イベントに関する詳細を提供します。	2019 年 12 月 12 日
AWS Control Tower で設定ページとアクティビティページが利用可能に	設定ページとアクティビティページを使用すると、ランディングゾーンの更新や、ログに記録されたイベントの表示が容易になります。	2019 年 11 月 30 日
追加の予防コントロールが AWS Control Tower で使用可能に	AWS Control Tower の予防コントロールは、組織およびリソースと、環境との整合性を維持します。	2019 年 9 月 6 日
追加の検出コントロールが AWS Control Tower で使用可能に	AWS Control Tower の検出コントロールは、組織の状態とリソースに関する情報を提供します。	2019 年 8 月 27 日
AWS Control Tower が一般公開	AWS Control Tower は、マルチアカウント AWS 環境を大規模にセットアップおよび管理する最も簡単な方法を提供するサービスです。	2019 年 6 月 24 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。