規制された AWS ランディングゾーンの OU 構造: 製薬業界の例

AWS 規範ガイダンス

AWS 規範ガイダンス: 規制された AWS ランディングゾーンの OU 構造: 製薬業界の例

Table of Contents

規制された AWS ランディングゾーンの OU 構造: 製薬業界の例

Katja Mueller、Petar Forai、Keval Sheth、Amazon Web Services (AWS)

2023 年 3 月 (ドキュメント履歴)

AWS には、医療を含む特定の業界をサポートする Landing Zone Accelerator 設定がいくつか用意されています。Landing Zone Accelerator for healthcare は、 AWS ベストプラクティスと複数のグローバルコンプライアンスフレームワークに沿ったマルチアカウント環境の管理とガバナンスを容易に AWS Control Tower するために、 と組み合わせて使用されます。ガバナンスのオーケストレーションの重要な側面の 1 つは、組織単位 (OUs) を使用して AWS アカウント グループ化し、それらを 1 つの単位として管理できるようにすることです。

このガイドでは、会社のクラウド成熟度の向上に合わせて既存の OU 構造を再設計するためのベストプラクティスと考慮事項について説明します。大規模な製薬企業の AWS Control Tower 実装に基づく実用的な例を紹介し、その実装から学んだ教訓について説明します。 AWS ランディングゾーンの設計は 1 回限りの作業ではありません。進化することは可能であり、また可能でなければなりません。この進化は、このガイドで強調されている AWS ベストプラクティスとヒントを適用することで、効果的かつ効率的に達成できます。

概要

当社は多国籍製薬会社と協力し、AWS 上で概念実証 (PoC) アクティビティを実行して、オンプレミスから AWS クラウド にアプリケーションを移行する方法を検討しました。本番ワークロードを含めるための移行ワークフローのスケーリングと高速化を開始すると、目標をサポートするために規制と準拠の AWS Landing Zone が必要であることが明らかになりました。新しい AWS Landing Zone の設計と実装には AWS Control Tower を使用しました。

新しい AWS Landing Zone とその組織において重要な側面は、組織単位 (OU) の構造です。OU は、AWS Organizations を使用して作成された AWS アカウント の論理グループです。OU を使用して AWS アカウント を階層に整理し、管理とガバナンスのコントロールを一貫してより簡単に適用できます。

ポリシーベースのコントロールは、OU と AWS アカウント にアタッチできます。OU 内の子 OU は、これらのコントロールを自動的に継承します。したがって、OU は AWS Organizations でセキュリティとガバナンスを管理する上で重要な役割を果たします。

ポリシーは、AWS アカウント のグループに適用するコントロールを定義する 1 つ以上のステートメントを含む JSON ドキュメントです。AWS Organizations は現在、サービスコントロールポリシー (SCP) とも呼ばれる 4 種類のポリシーをサポートしています。SCP は、異なる AWS アカウント で使用できる AWS のサービス およびアクションを定義します。例えば、SCP を使用して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの起動に特定のインスタンスタイプの使用を要求できます。

ポリシータイプ

SCP ポリシータイプには以下が含まれます。

- 許可リストと拒否リストは、SCP を適用してアカウントで利用できるアクセス許可をフィルタ処理するための補足的な戦略です。
- タグポリシーを使用して、アカウント全体のタグキーおよびタグ値の大文字と小文字の処理方法の設定など、一貫したタグを維持できます。
- バックアップポリシーは、バックアップの時間枠や AWS リージョン 全体のバックアップの宛先ボールトなど、サポートされているリソースタイプのバックアップを設定します。
- AI サービスのオプトアウトポリシーは、AWS 人工知能 (AI) サービスの継続的な改善をグローバルに有効または無効にします。

ポリシー継承の動作: 特定の OU にポリシーをアタッチすると、その OU または子 OU の直下にあるアカウントがポリシーを継承します。特定のアカウントにポリシーをアタッチすると、ポリシーはそのアカウントにのみ影響します。例外ポリシーを導入することで、継承されたポリシーを上書きできます。継承により、明示的にアクセス許可を拒否しない限り、すべてのアクセス許可がルート (OU) からその OU と子 OU のすべての AWS アカウント に流れていくことを明示的に許可します。アクセス許可を拒否するには、追加のポリシーを作成し、適切な OU または AWS アカウント にアタッチします。ポリシーの継承と例外の詳細については、AWS Organizations ドキュメントを参照してください。

AWS Control Tower は、OU 構造を使用して独自の検出コントロールと予防コントロール (ガードレールとも呼ばれます) のセットも提供します。AWS Control Tower 予防コントロールは、AWS Organizations の SCP を使用してアクションを防止します。検出コントロールは、AWS Config を使用して、コントロールに対する設定ドリフトを報告します。これらのコントロールの詳細については、AWS Control Tower ドキュメントを参照してください。

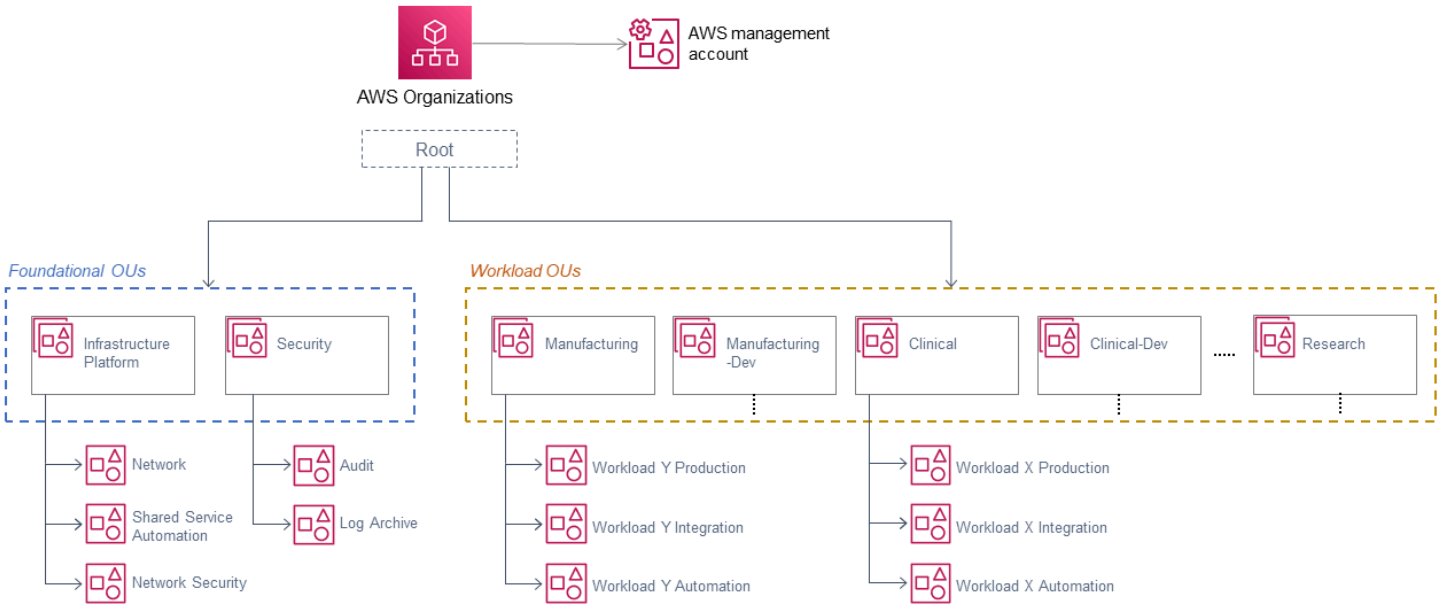
AWS Security Hub CSPM を有効にして、セキュリティのベストプラクティスチェックを自動化し、セキュリティアラートを 1 つの場所と形式に集約し、すべての AWS アカウント 全体のセキュリティ体制を把握することもできます。

OU 設計: フェーズ 1

この例では、多国籍製薬企業の場合、 の組織と OUs の初期設計は、セットアップに関する AWS 推奨事項に AWS Organizations 厳密に従っていました AWS Control Tower。例については、ブログ記事「Best Practices for Organizational Units with AWS Organizations」で説明されている「Best Practices for Organizational Units, including the Security OU, the Platform Infrastructure OU, and company-specific OUs」で説明 OUs されているように、「Landing Zone Accelerator on AWS for healthcare. AWS Control Tower initially provisioned a simple OU structure with common foundational OUs」を参照してください。

アーキテクチャの設計

初期 OU アーキテクチャを次の図に示します。



セキュリティ OU

セキュリティ OU は、セキュリティ機能 AWS アカウント に関連する広範なグループをまとめ、2 つのアカウント (監査とログアーカイブ) を使用してセキュリティ運用データを保存し、環境への一元的なログ記録と監査アクセスを行います。Amazon GuardDuty や などの AWS コアセキュリティサービスは、監査アカウント AWS Security Hub CSPM にあります。

インフラストラクチャプラットフォーム OU

インフラストラクチャ基盤 AWS アカウント を提供するインフラストラクチャプラットフォーム OU グループ。この OU 内に最初にデプロイされたのは、中央ネットワークコンポーネント (ゲートウェイ、ファイアウォール、中央ネットワークハブ、および同様のサービス) AWS アカウント の です。

追加の OU

その他の会社固有の OU (臨床 OU など) は、低レベルの階層内の基礎となる OU を強化します。ワークロードは、マルチアカウント構造と、それらの OU 内の個別の環境を使用して実装されます。

この初期設計は、いくつかの考慮事項に基づいて作成されました。

- ネストされた OUs でその時点で使用できず AWS Control Tower 、広範なカスタマイズが必要でした。
- クラウド用に指定された初期ワークロードは、臨床試験や製造装置の分析 (機能ビュー) など、会社の特定の側面に焦点を当てていました。
- 同社は、5 つのワークロード環境 (開発、検証、統合、トレーニング、本番稼働) を区別しています。同社は、本番ワークロードに必要な AWS コントロールによる厳格なガバナンスなしでアプリケーションを開発するためのプレイグラウンドを必要としていました。この目的のために、製造開発 OU のような開発 OU が割り当てられました。
- ワークロードの自動化は各アプリケーションのエコシステムの一部であり、分離は必要ありませんでした。
- インフラストラクチャ認定 (IQ) と GxP コンプライアンスプロセスでは、OU レベルで AWS コントロールを区別する必要がありませんでした。

OU 設計: フェーズ 2

この例に登場する製薬企業は、認証済みの本稼働ワークロードを既存の OU にデプロイすることで、新たなクラウド成熟フェーズへの移行を加速させました。これにより、初期設計のレビューが開始され、規制された AWS ランディングゾーンに移行するワークロードが増えるにつれて、フェーズ 1 の構造に課題がありました。

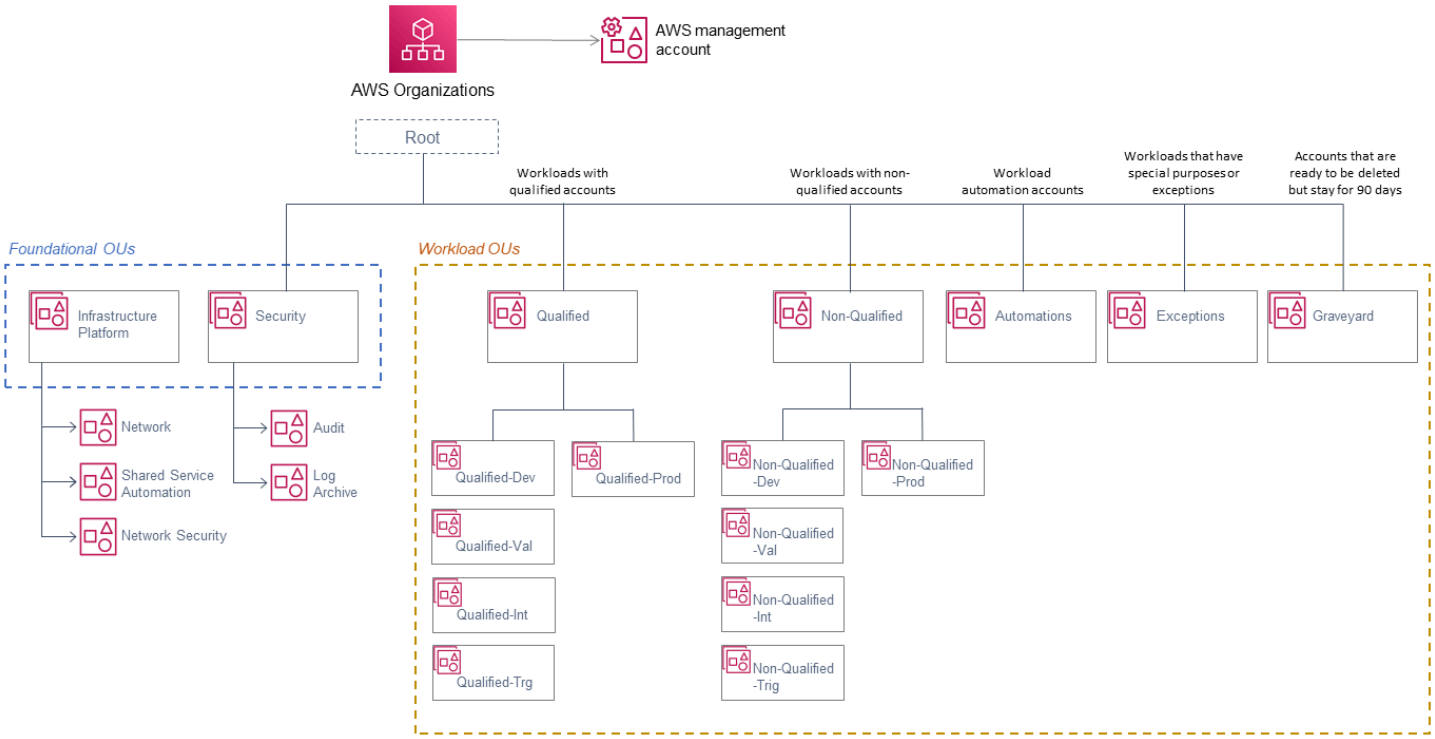
以下の新しい要件とインサイトが重要になりました。

- 同社ではデータ共有モデルのワークロードを実装していたため、臨床や製造といった個別の OU に割り当てることができないようアプリケーションに多目的性を持たせました。
- 認定 (特に継続的な認定) が、多くのワークロードの重要な側面となりました。セキュリティのベストプラクティスをより簡単に遵守できるよう、これらのワークロードを運用プロセスに統合する必要がありました。適格なワークロードには、フェーズ 1 で OU レベルで設定された、より厳格な AWS コントロールが必要でした。
- ネストされた OU 機能が で利用可能になりました AWS Control Tower。
- スキルの向上と経験により、ワークロードに関連する特定のポリシーについて、よりよく理解できるようになりました。
- 会社は、責任のアラインメントに基づく運用モデルを定義し、これに合意しました。
- ワークロードのセグメンテーションと構造のブループリントが成熟し、ワークロードの移行に導入されました。

その結果、フェーズ 2 およびその新しい構造へと移行された AWS アカウント では新しい設計が実装されました。この新しい構造には、以下のセクションに記載された OU が含まれます。

アーキテクチャの設計

次の図は、フェーズ 2 の OU アーキテクチャを示しています。



セキュリティ OU

セキュリティ OU には、セキュリティ機能に広く AWS アカウント 関連し、2 つのアカウント (監査とログアーカイブ) を使用して、環境への中央ログ記録と監査アクセスのためのセキュリティ運用データを保存します。Amazon GuardDuty などの AWS コアセキュリティサービスは、監査アカウント AWS Security Hub CSPM にあります。この OU は元の設計から変更されません。

インフラストラクチャプラットフォーム OU

インフラストラクチャプラットフォーム OU には、ラン AWS ディングゾーン全体のネットワークや共有オートメーションなどの基盤インフラストラクチャアカウントが含まれています。この OU は元の設計から変更されません。

認定 OU

認定 OU には、厳格な変更管理、認定、検証などの認定インフラストラクチャを必要とするワークロードが含まれています。

非認定 OU

非認定 OU には、GxP 要件がないか、ビジネスクリティカルではないワークロードが含まれています。

オートメーション OU

オートメーション OU には、インフラストラクチャ管理のための継続的インテグレーションや継続的デリバリー (CI/CD) パイプラインなど、ワークロードの自動化に対応する共有リソースが含まれています。要件に応じて、オートメーションは環境間で分割することも、単一の AWS アカウントでホストすることもできます。

例外 OU

例外 OU には、特別な処理を必要とするワークロードが含まれており、それ以外のワークロードはポリシーによって阻止されます。例えば、広くアクセス可能で読み取り可能な Amazon Simple Storage Service (Amazon S3) バケットは例外 OU に該当します。

グレイブヤード OU

Graveyard OU には、削除されるワークロード AWS アカウント の が含まれます。これらのアカウントのポリシーは、アカウントの有効期限が切れるか削除されるまで、効果的でシンプルな管理アクセスのために削除する必要があります。

OU の移行と検証

この例の多国籍製薬会社では、クラウドプラットフォームエンジニアリングチームと変更管理チームが移行計画とスケジュールについて合意しました。AWS アカウント は、計画の一環としてビジネスへの影響と重要度に応じてレビューされ、ランク付けされました。

新しい OU 構造は、新しいポリシーのステージングと段階的な移行を可能にするために、既存の OU 構造と並行してデプロイされました。子 OU を含む新しい空の OU を作成し、それらの子 OU に AWS Organizations ポリシーと AWS Control Tower コントロールを割り当てました。

AWS Organizations ポリシーは、新しい構造に目的のポリシーを適用して手動で移行されました。AWS Organizations ポリシー検証には手動のスポットチェックを使用し、AWS Control Tower コントロール検証には自動化メカニズムを使用しました。これらのチェックが成功した場合にのみ、AWS アカウント は新しい OU に移動されました。

アカウント移行は半自動化され、ずらされたアプローチまたはバッチ化されたアプローチに従いました。最初の移行では、重要度が低いと判断された AWS アカウント を対象とし、移行の実行ごとに 5 つの AWS アカウント のバッチを使用しました。移行バッチは 10 アカウントを超えませんでした。アカウントが移行されると、レビュー担当者とテスターは AWS Control Tower コンソールを使用して、これらのアカウントが正しい OU に移動されたことを検証し、AWS CloudTrail ログでエラーがないかモニタリングしました レビュー担当者は、テイント状態または不明状態のドリフトまたはアカウントについて、AWS Service Catalog および AWS Control Tower コンソールもチェックしました。

アカウントの OU 配置を変更しても、リソースの接続やアクセシビリティには影響しませんでした。本番用アプリケーションの停止は報告されませんでした。

学んだ教訓とベストプラクティス

- OU 構造設計は 1 回限りの作業ではありません。企業がクラウドの導入を増やし、追加のワークロードを AWS ランディングゾーンに移行するにつれて、その OU 設計 (および暗黙的にそのポリシーの概念) も自然に進化します。
- OU をフォルダと間違えないでください。OU はポリシーの対象と考えてください。OU とその階層は AWS アカウント の構造化要素を提供し、常にポリシーのコンテナとして扱う必要があります。同じポリシーセットを必要とするすべての AWS アカウント を同じ OU に配置することをお勧めします。このガイドラインは、ネストされた OU (OU 内の OU) にも適用されます。

  一元共有機能とクロスワークロードデータ共有機能 (エンタープライズデータプラットフォームで頻繁に見られる) を必要とする AWS 環境は、事業部門 (LOB) 関数分類に基づいていない OU 構造でより簡単に対応できます。例えば、製造アプリケーションの本番環境は、AWS Organizations のポリシーの観点から見れば、臨床試験分析アプリケーションの本番環境と変わりません。
- 継承を尊重して使用します。特定の OU にポリシーをアタッチすると、その OU の直下または子 OU の下にある AWS アカウント がポリシーを継承します。特定の AWS アカウント にポリシーをアタッチすると、ポリシーはその AWS アカウント にのみ影響します。

  ある OU 構造から別の OU 構造への移行作業は、OU または AWS アカウント レベルで設定されている既存のポリシーの範囲によって異なります。もう 1 つの重要な要因は、既存の OU 階層でポリシー継承がどの程度使用されたか、また継承が壊れたかどうかです。移行の複雑さは、不規則な継承パスや逸脱した継承パスの実装に伴って増大します。例えば、ポリシーを個々の AWS アカウント レベルで適用する場合や、頻繁にポリシー例外 (継承が中断される) を行う場合、それらのポリシーを新しい構造に移行するには、かなりの労力がかかります。このように複雑度が高い場合は、移行計画中にポリシーの継承を確認して再設計することに時間をかけることをお勧めします。
- AWS Organizations ポリシーと AWS Control Tower コントロールの両方に対処します。OU 構造は AWS Control Tower と AWS Organizations の間で共有されます。AWS Control Tower は独自の検出コントロールと予防コントロールのセットを提供します。これらのコントロールは AWS アカウント または OU レベルで適用されます。AWS Organizations は OU レベルでポリシーをオーケストレートします。OU 移行では、コンプライアンスの重みが増すため、まず AWS Organizations ポリシーを移行することをお勧めします。2 番目の移行ステップでは、新しい OU 構造に AWS Control Tower コントロールを適用することをお勧めします。
- AWS アカウント の更新には時間がかかります。AWS Control Tower を使用して、既存の AWS アカウント を新しい OU 構造に個別に再登録する必要があります。これには時間がかかります。アカウントが多数ある場合は、自動化によってこの作業を合理化し、AWS アカウント の OU 配置を制御および自動化することをお勧めします。次の 2 つのシナリオの例を示します。

- 小規模な移行の手動変更: 移行リードは、各 AWS アカウント を古い OU から AWS マネジメントコンソール の新しい OU に再割り当てします。この再割り当てがすべての AWS アカウント で完了すると、移行リードは AWS アカウント ごとに個別に、またはすべての OU に対して AWS Control Tower を開きます。AWS Control Tower に AWS アカウント を再登録するには、アカウント内で使用されている AWS リージョン の数に応じて、AWS アカウント ごとに 10 ~ 15 分かかります。AWS Control Tower では、この種の同時操作を最大 5 つ並行して実行できます。
- カスタム変更の自動化: 自動化により、作業を簡素化し省くことができます。例えば、作成から移行、終了に至るまで、AWS アカウント ライフサイクルの管理を自動化できます。AWS Control Tower アカウントファクトリーを使用して、AWS アカウント の OU 割り当てを変更し、再登録プロセスを実行できます。この自動化は、数百の AWS アカウント という大規模な移行をサポートします。

リソース

- AWS Organizations ユーザーガイド (AWS ドキュメント)
- AWS Organizations の用語と概念 (AWS ドキュメント)
- サービスコントロールポリシー (SCP) (AWS ドキュメント)
- AWS Organizations API リファレンス (AWS ドキュメント)
- AWS Control Tower ユーザーガイド (AWS ドキュメント)
- Landing Zone Accelerator for Healthcare のご紹介 (AWS のブログ記事)
- Managing the multi-account environment using AWS Organizations and AWS Control Tower (AWS のブログ記事)
- AWS Organizations での組織単位のベストプラクティス (AWS のブログ記事)
- AWS Security Reference Architecture (AWS SRA) (AWS 規範ガイダンス)
- Establishing Your Cloud Foundation AWS (AWS のホワイトペーパー)
- Organizing Your AWS Environment Using Multiple Accounts (AWS のホワイトペーパー)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
初版発行	—	2023 年 3 月 28 日

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。