AWS セキュリティリファレンスアーキテクチャ (AWS SRA) – コアアーキテクチャ

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS セキュリティリファレンスアーキテクチャ (AWS SRA) – コアアーキテクチャ

Table of Contents

AWS セキュリティリファレンスアーキテクチャ (AWS SRA) – コアアーキテクチャ

グローバルサービスセキュリティチーム、Amazon Web Services (寄稿者)

2025 年 12 月 (ドキュメント履歴)

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

アマゾン ウェブ サービス (AWS) セキュリティリファレンスアーキテクチャ (AWS SRA) は、 AWS セキュリティサービスの完全な補完をマルチアカウント環境にデプロイするための包括的なガイドラインのセットです。セキュリティ AWS サービスを設計、実装、管理し、 AWS 推奨されるプラクティスに合わせるのに役立ちます。レコメンデーションは、 AWS セキュリティサービスを含む 1 ページのアーキテクチャを中心に構築されています。セキュリティ目標の達成にどのように役立つか、 でデプロイおよび管理できる最適な場所 AWS アカウント、他のセキュリティサービスとやり取りする方法などです。この全体的なアーキテクチャガイダンスは、AWS セキュリティドキュメントのウェブサイトにあるような、サービス固有の詳細な推奨事項を補完します。

アーキテクチャとそれに付随する推奨事項は、 AWS エンタープライズ顧客との集合的な経験に基づいています。このドキュメントは、特定の環境 AWS のサービス を保護するために を使用するための包括的なガイダンスのセットであるリファレンスであり、AWS SRA コードリポジトリのソリューションパターンは、このリファレンスに示されている特定のアーキテクチャ向けに設計されています。お客様ごとに異なる要件があります。その結果、 AWS 環境の設計は、ここに示す例とは異なる場合があります。これらの推奨事項は、個々の環境やセキュリティのニーズに合わせて変更および調整する必要があります。 必要に応じて、ドキュメント全体で、頻繁に見られる代替シナリオのオプションを提案します。

AWS SRA は生きている一連のガイダンスであり、新しいサービスや機能のリリース、お客様からのフィードバック、絶えず変化する脅威の状況に基づいて定期的に更新されます。各アップデートには、改訂日と関連する 変更ログ が含まれます。

基盤として 1 ページの図に依存していますが、アーキテクチャは 1 つのブロック図よりも深く、基本とセキュリティ原則の十分に構造化された基盤の上に構築する必要があります。このドキュメントは、ナラティブまたはリファレンスとして 2 通りの使い方ができます。トピックはストーリーと

して整理されているため、最初 (基礎的なセキュリティガイダンス) から最後 (実装可能なコードサンプルの考察) まで読むことができるようになっています。また、ニーズに最も適したセキュリティ原則、サービス、アカウントタイプ、ガイダンス、事例に焦点を当て、ドキュメントをナビゲートすることも可能です。

このドキュメントは、以下のセクションと付録に分かれています。

- AWS SRA ライブラリについて は、SRA AWS の出版物コレクションに含まれる技術ガイダンスとコードの概要を提供します。
- AWS SRA の価値 は、SRA の構築の動機を説明し、セキュリティの向上に役立つ SRA AWS の使用方法を説明し、重要な点を一覧表示します。
- セキュリティ基盤は、 AWS クラウド導入フレームワーク (AWS CAF)、 AWS Well-Architected フレームワーク、責任 AWS 共有モデルを確認し、特に SRA AWS に関連する要素を強調します。
- AWS Organizations、 アカウント、IAM ガードレール は AWS Organizations 、サービスを導入し、基本的なセキュリティ機能とガードレールについて説明し、推奨されるマルチアカウント戦略の概要を説明します。
- AWS セキュリティリファレンスアーキテクチャは、機能 AWS アカウント、および一般的に利用可能なセキュリティサービスと機能を示す単一ページのアーキテクチャ図です。
- AI/ML for security では、さまざまな が人工知能と機械学習 (AI/ML) をバックグラウンドで AWS のサービス 使用して、特定のセキュリティ目標を達成する方法について説明します。これらを設計 AWS のサービス に含めることで、高度なセキュリティ機能を活用できます。
- セキュリティアーキテクチャの構築 – 段階的アプローチは、SRA が提供する AWS リファレンスに基づいて、6 つの反復的なフェーズで独自のセキュリティアーキテクチャを構築する方法に関するガイダンスを提供します。
- AWS SRA ベストプラクティスチェックリストは、ガイド全体で説明されている推奨事項をチェックリストにまとめたもので、このチェックリストに従ってセキュリティアーキテクチャのバージョンを構築できます。
- IAM リソースには、セキュリティアーキテクチャにとって重要な AWS Identity and Access Management (IAM) ガイダンスの概要と一連のポインタが表示されます。
- SRA AWS の例のコードリポジトリは、デベロッパーとエンジニアがこのドキュメントで説明されているガイダンスとアーキテクチャパターンの一部をデプロイするのに役立つ、関連する GitHub リポジトリの概要を提供します。サンプルは、 AWS CloudFormation または HashiCorp の Terraform を使用してデプロイできます。環境 AWS Control Tower と非AWS Control Tower 環境の両方をサポートしています。

付録には、個々の AWS セキュリティ、アイデンティティ、コンプライアンスサービスのリストと、各サービスに関する詳細情報へのリンクが含まれています。ドキュメント履歴 セクションは、このドキュメントのバージョンを追跡するための変更ログが表示されます。また、RSS フィード を購読することで、変更通知を受け取ることができます。

SRA AWS ライブラリについて

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

このガイドは、セキュリティアーキテクチャを 設計および構築するためのアーキテクチャ設計図と技術ガイダンスを提供するライブラリの一部です AWS。このライブラリは、実装コード (AWS SRA コードライブラリ)、検証ツール (SRA Verify)、およびコアアーキテクチャとディープダイブアーキテクチャをカバーする 2 つの補完的なカテゴリのガイドで構成されています。

AWS SRA – コアアーキテクチャ (このガイド)

このガイドは、推奨される AWS セキュリティアーキテクチャの基盤を示しています。これは、業界、アプリケーションタイプ、その他の考慮事項に関係なく、すべての組織に適用される出発点です。この基盤は、 で強力でスケーラブルなアーキテクチャを構築し AWS 、ビジネスの成長に合わせて安全にスケールする強力な AWS マルチアカウントセキュリティベースラインを作成するのに役立ちます。

AWS SRA – ディープダイブアーキテクチャ

AWS SRA – コアアーキテクチャガイドは、特定のセキュリティ機能、アプリケーションタイプ、コンプライアンスまたは規制要件に沿ったアーキテクチャパターンを提供する追加の出版物で補完されています。これらのパターンはコアアーキテクチャを拡張するため、AWS SRA – コアアーキテクチャガイドと組み合わせて使用する必要があります。

以下のガイドでは、特定のセキュリティ機能に合わせたアーキテクチャパターンについて説明します。

- AWS SRA – ID 管理 は、スケーラブルで堅牢、一元化された ID およびアクセス管理ソリューションを実装する方法に関するガイダンスを提供します AWS。
- AWS SRA – 境界セキュリティは、中央アカウントまたは個々のアカウントにエッジセキュリティを実装 AWS のサービス するためのアーキテクチャパターンと について説明します。
- AWS SRA – サイバーフォレンジックでは、組織のフォレンジック機能を開発し、セキュリティインシデント対応 (IR) の準備状況を向上させるための出発点としてフォレンジックアカウントを設定する AWS 方法について説明します。

以下のガイドでは、特定のアプリケーションタイプのアーキテクチャパターンについて説明します。ベースラインセキュリティアーキテクチャを構築した後は、これらに焦点を当てることをお勧めします。

- AWS SRA – AI セキュリティは、生成 AI AWS サービスを使用して生成 AI 機能を組み込むアプリケーションを設計および構築するためのセキュリティアーキテクチャの推奨事項を提供します。
- AWS SRA – IoT は、 IoT アプリケーションを設計および構築するためのセキュリティアーキテクチャの推奨事項を提供します AWS。

さらに、次のガイドでは、特定のコンプライアンスまたは規制フレームワークに沿ったアーキテクチャパターンについて説明します。

- AWS プライバシーリファレンスアーキテクチャ (AWS PRA) は、個人データを処理するアプリケーション用のセキュリティアーキテクチャを提供し、一般データ保護規則 (GDPR)、カリフォルニア消費者プライバシー法 (CCPA)、ブラジル一般データ保護法 (LGPD) などの幅広いプライバシーコンプライアンス要件をサポートする必要があります。 AWS PRA は、プライバシーコントロールの設計と設定に固有の一連のガイドラインを提供します AWS のサービス。

基本AWS アーキテクチャを理解するためのコアアーキテクチャガイドである SRA から開始し、補足ガイドを参照して高度な機能と実装を活用することをお勧めします。このコンテンツセットの詳細については、AWS 「セキュリティリファレンスアーキテクチャ」を参照してください。

> **アーキテクチャ図**
>
> ビジネスニーズに基づいて SRA AWS ライブラリのリファレンスアーキテクチャ図をカスタマイズするには、次の .zip ファイルをダウンロードしてその内容を抽出します。
>
> 図のソースファイルをダウンロードする (Microsoft PowerPoint 形式)

SRA AWS の値

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS には、セキュリティおよびセキュリティ関連のサービスの大規模 (および増加中の) なセットがあります。お客様は、当社のサービスドキュメント、ブログ投稿、チュートリアル、サミット、カンファレンスを通じて入手可能な詳細情報に感謝しています。また、全体像をよりよく理解し、 AWS セキュリティサービスの戦略的視点を得たいとも言っています。顧客と協力して必要なものをより深く理解すると、次の 3 つの優先順位が浮上します。

- お客様は、 AWS セキュリティサービスを包括的にデプロイ、設定、運用する方法の詳細と推奨パターンを求めています。サービスのデプロイと管理を行うアカウントとセキュリティ目標 すべてまたはほとんどのサービスが動作するセキュリティアカウントが 1 つありますか? 場所 (組織単位または AWS アカウント) の選択は、セキュリティ目標にどのように役立ちますか? 顧客が注意すべきトレードオフ (設計上の考慮事項) はどれですか?
- お客様は、多くの AWS セキュリティサービスを論理的に整理するためのさまざまな視点に関心を持っています。これらの代替視点は、各サービス (アイデンティティサービスや口グ記録サービスなど) の主な機能を超えて、お客様がセキュリティアーキテクチャを計画、設計、実装するのに役立ちます。このドキュメントで後述する例では、 AWS 環境の推奨構造に沿った保護レイヤーに基づいてサービスをグループ化します。
- お客様は、セキュリティサービスを最も効果的な方法で統合するためのガイダンスと例を求めています。例えば、自動監査およびモニタリングパイプラインの手間をかけるために、他の サービスとどのように連携し、接続 AWS Config するのが最適ですか? お客様は、各 AWS セキュリティサービスが他のセキュリティサービスにどのように依存またはサポートしているかについてのガイダンスを求めています。

これらはそれぞれ SRA AWS で対処します。リストの最初の優先事項 (モノが進む場所) は、メインアーキテクチャ図と、このドキュメントの付随する議論の焦点です。推奨される AWS Organizations アーキテクチャと、どのサービスがどこに移動するかについてのaccount-by-account説明を提供します。リストの 2 番目の優先度 (セキュリティサービスの完全なセットについて考える方法) を開始するには、AWS 「組織全体にセキュリティサービスを適用する」セクションをお読みください。このセクションでは、 AWS 組織内の要素の構造に従ってセキュリティサービスをグループ化する方法について説明します。さらに、これらの同じアイデアは、Amazon Elastic Compute Cloud (Amazon

EC2) インスタンス、Amazon Virtual Private Cloud (Amazon VPC) ネットワーク、およびより広範なアカウントなど、アカウントの特定のレイヤーに集中するためにセキュリティサービスを運用する方法を強調するアプリケーションアカウントの議論に反映されています。最後に、3 番目の優先度 (サービス統合) はガイダンス全体に反映されます。特に、SRA ライブラリのディープダイブガイドの個々のサービスの説明と SRA AWS コードリポジトリのコードの説明に反映されます。 AWS

SRA AWS の使用方法

クラウド導入ジャーニーのどの段階にあるかに応じて、SRA AWS を使用する方法はさまざまです。SRA アセットから最大のインサイトを得る方法 (アーキテクチャ図、書面によるガイダンス、コードサンプル) AWS のリストを次に示します。

- 独自のセキュリティアーキテクチャのターゲット状態を定義します。

  最初のアカウントセットのセットアップ AWS クラウド 、または確立された AWS 環境の強化を計画している場合でも、SRA AWS はセキュリティアーキテクチャの構築を開始する場所です。アカウント構造とセキュリティサービスの包括的な基盤から始め、特定のテクノロジースタック、スキル、セキュリティ目標、コンプライアンス要件に基づいて調整します。より多くのワークロードを構築して起動することがわかっている場合は、カスタマイズされたバージョンの SRA AWS を取得し、組織のセキュリティリファレンスアーキテクチャの基礎として使用できます。 AWS SRA で説明されているターゲット状態を達成する方法については、「セキュリティアーキテクチャの構築 – 段階的アプローチ」を参照してください。
- すでに実装している設計と機能を確認 (および修正) します。

  セキュリティ設計と実装が既にある場合は、SRA AWS と必要なものを比較するために少し時間をかける価値があります。 AWS SRA は包括的に設計されており、独自のセキュリティを確認するための診断ベースラインを提供します。セキュリティ設計が SRA AWS と一致する場合、 を使用する際にベストプラクティスに従っていることをより確信できます AWS のサービス。セキュリティ設計が AWS SRA のガイダンスと異なる、または一致しない場合でも、これは必ずしも何か間違ったことをしている兆候ではありません。代わりに、この観察結果により、決定プロセスを確認する機会が得られます。 AWS SRA のベストプラクティスから逸脱する正当なビジネスおよびテクノロジー上の理由があります。おそらく、特定のコンプライアンス、規制、または組織のセキュリティ要件には、特定のサービス設定が必要です。または、 を使用する代わりに AWS のサービス、 または構築して管理する AWS Partner Network カスタムアプリケーションの製品の機能設定がある場合があります。このレビュー中に、以前の決定が、適用されなくなった古いテクノロジー、 AWS 機能、またはビジネス上の制約に基づいて行われたことに気付くことがあります。これは、更新を確認して優先順位を付け、エンジニアリングバックログの適切な場所に追加する

良い機会です。 AWS SRA に照らしてセキュリティアーキテクチャを評価する際に検出した内容は、その分析を文書化することが有益です。決定とその根拠の履歴を記録すると、将来の決定に関する情報を提供し、優先順位を付けるのに役立ちます。

- 独自のセキュリティアーキテクチャの実装をブートストラップします。

  AWS SRA Infrastructure as Code (IaC) モジュールは、セキュリティアーキテクチャの構築と実装を迅速かつ確実に開始する方法を提供します。これらのモジュールは、コードリポジトリセクションとパブリック GitHub リポジトリでより深く説明されています。エンジニアは、 AWS SRA ガイダンスのパターンの高品質の例に基づいて構築できるだけでなく、IAM パスワードポリシー、Amazon Simple Storage Service (Amazon S3) ブロックアカウントのパブリックアクセス、Amazon EC2 のデフォルトの Amazon Elastic Block Store (Amazon EBS) 暗号化、 との統合などの推奨セキュリティコントロールを組み込む AWS Control Tower ことで、新しい AWS アカウント がオンボーディングまたは廃止されるときにコントロールを適用または削除できます。

- AWS セキュリティサービスと機能の詳細について説明します。

  AWS SRA のガイダンスと議論には、個々の AWS セキュリティおよびセキュリティ関連のサービスに関する重要な機能や、デプロイと管理に関する考慮事項が含まれています。SRA AWS の機能の 1 つは、 AWS セキュリティサービスの幅と、マルチアカウント環境でどのように連携するかについての概要を提供することです。これにより、他のソースで見つかった各サービスの機能と設定を深く掘り下げることができます。この例の 1 つは、 AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) がさまざまな、 AWS Partner 製品 AWS のサービス、さらには独自のアプリケーションからセキュリティ検出結果を取り込む方法の説明です。

- セキュリティに関する組織のガバナンスと責任について説明します。

  セキュリティアーキテクチャまたは戦略を設計および実装するための重要な要素は、組織内の誰にどのセキュリティ関連の責任があるかを理解することです。例えば、セキュリティ検出結果をどこに集約してモニタリングするかという質問は、どのチームがそのアクティビティを担当するかという質問に関連付けられています。組織全体のすべての検出結果は、専用の Security Tooling アカウントにアクセスする必要がある中央チームによってモニタリングされていますか? または、個々のアプリケーションチーム (またはビジネスユニット) が特定のモニタリングアクティビティを担当しているため、特定のアラートおよびモニタリングツールにアクセスする必要がありますか? 別の例として、組織にすべての暗号化キーを一元的に管理するグループがある場合、(AWS Key Management Service AWS KMS) キーを作成するアクセス許可を持つユーザーと、それらのキーを管理するアカウントに影響します。さまざまなチームや責任など、組織の特性を理解することは、ニーズに合わせて AWS SRA を調整するのに役立ちます。逆に、セキュリティアーキテクチャの議論が、既存の組織の責任について議論し、潜在的な変更を検討するための推進力になることがあります。 は、ワークロードチームがワークロードの機能と要件に基づいてセキュリティ

コントロールを定義する責任がある分散型意思決定プロセス AWS を推奨します。一元化されたセキュリティおよびガバナンスチームの目標は、ワークロード所有者が情報に基づいた意思決定を行い、すべての関係者が設定、検出結果、イベントを可視化できるようにするシステムを構築することです。SRA AWS は、これらの議論を特定して通知するための手段となります。

AWS SRA の主要な実装ガイドライン

ここでは、セキュリティを設計および実装する際に留意すべき SRA AWS の 8 つの重要なポイントを示します。

- AWS Organizations と適切なマルチアカウント戦略は、セキュリティアーキテクチャの必須要素です。ワークロード、チーム、機能を適切に分離することは、職務の分離とdefense-in-depth戦略の基盤となります。このガイドでは、これについては後のセクションで詳しく説明します。
- Defense-in-depthは、組織のセキュリティコントロールを選択するための重要な設計上の考慮事項です。これは、 AWS Organizations 構造のさまざまなレイヤーに適切なセキュリティコントロールを挿入するのに役立ちます。これにより、問題の影響を最小限に抑えることができます。1 つのレイヤーに問題がある場合、他の重要な IT リソースを分離するコントロールがあります。 AWS SRA は、 AWS テクノロジースタックのさまざまなレイヤーでのさまざまな AWS のサービス 機能、およびそれらのサービスを組み合わせて使用することでdefense-in-depthを実現する方法を示しています。この defense-in-depthの概念 AWS については、後のセクションでさらに詳しく説明し、アプリケーションアカウントで設計例を示します。
- 堅牢で回復力のあるクラウドインフラストラクチャを構築するには、複数の AWS のサービス および 機能にまたがるさまざまなセキュリティ構成要素を使用します。特定のニーズに合わせて SRA AWS を調整するときは、 AWS のサービス および 機能の主な機能 (認証、暗号化、モニタリング、アクセス許可ポリシーなど) だけでなく、アーキテクチャの構造にどのように適合するかも考慮してください。このガイドの後のセクションでは、一部のサービスが AWS 組織全体でどのように動作するかについて説明します。他のサービスは 1 つのアカウント内で最適に動作し、一部のサービスは個々のプリンシパルにアクセス許可を付与または拒否するように設計されています。これらの両方の視点を考慮すると、より柔軟で階層化されたセキュリティアプローチを構築できます。
- 可能であれば (後のセクションで説明するように) 、すべてのアカウントにデプロイできる を使用し AWS のサービス (一元管理ではなく配布) 、ワークロードを誤用から保護し、セキュリティイベントの影響を軽減するのに役立つ一貫した共有ガードレールのセットを構築します。 AWS SRA は AWS Security Hub CSPM 、 (集中検出結果のモニタリングとコンプライアンスチェック)Amazon GuardDuty (脅威検出と異常検出) 、 AWS Config (リソースモニタリングと変更検出) 、IAM Access Analyzer (リソースアクセスモニタリング) 、 AWS CloudTrail (環境全体の口

ギングサービス API アクティビティ) 、Amazon Macie (データ分類) を、すべての AWS のサービス にデプロイされる の基本セットとして使用します AWS アカウント。

- ガイドの委任管理セクションで後述するように AWS Organizations、サポートされている の委任管理機能を使用します。これにより、サポートされているサービスの管理者として AWS メンバーアカウントを登録できます。委任管理は、企業内のさまざまなチームが、責任に応じて個別のアカウントを使用して環境 AWS のサービス 全体で管理するための柔軟性を提供します。さらに、委任された管理者を使用すると、 AWS Organizations 管理アカウントへのアクセスを制限し、アクセス許可のオーバーヘッドを管理することができます。
- 組織全体で一元的なモニタリング、管理、ガバナンスを実装します AWS 。マルチアカウント (場合によってはマルチリージョン) 集約 AWS のサービス をサポートする と委任管理機能を使用することで、中央のセキュリティ、ネットワーク、クラウドエンジニアリングチームが適切なセキュリティ設定とデータ収集を広範囲に可視化し、制御できるようになります。さらに、データをワークロードチームに提供して、ソフトウェア開発ライフサイクル (SDLC) の早い段階で効果的なセキュリティ上の意思決定を行う権限を与えることができます。
- AWS Control Tower を使用して、セキュリティリファレンスアーキテクチャのビルドをブートストラップする事前構築済みのセキュリティコントロールの実装により、マルチアカウント AWS 環境を設定および管理します。 は、アイデンティティ管理、アカウントへのフェデレーティッドアクセス、集中ロギング、および追加のアカウントをプロビジョニングするための定義されたワークフローを提供するブループリント AWS Control Tower を提供します。その後、Customizations for AWS Control Tower (CfCT) ソリューションを使用して、SRA コードリポジトリで示されているように、追加のセキュリティコントロール、サービス設定、ガバナンス AWS Control Tower を使用して、 AWS によって管理されるアカウントをベースライン化できます。Account Factory 機能は、承認されたアカウント設定に基づいて設定可能なテンプレートを使用して新しいアカウントを自動的にプロビジョニングし、 AWS 組織内のアカウントを標準化します。ガバナンスを既存の個人に拡張するには、すでに管理されている組織単位 (OU) に登録 AWS アカウント します AWS Control Tower。
- AWS SRA コード例は、Infrastructure as Code (IaC) を使用して SRA AWS ガイド内のパターンの実装を自動化する方法を示しています。パターンをコーディングすることで、IaC を組織内の他のアプリケーションと同様に扱い、コードをデプロイする前にテストを自動化できます。IaC は、ガードレールを複数の (SDLC やリージョン固有など) 環境にデプロイすることで、一貫性と再現性を確保するのにも役立ちます。SRA コード例は、 の有無にかかわらず、 AWS Organizations マルチアカウント環境にデプロイできます AWS Control Tower。を必要とするこのリポジトリのソリューションは、 および Customizations for AWS Control Tower (CfCT) を使用してAWS Control Tower環境にデプロイ AWS CloudFormationされ、テスト AWS Control Tower されています。不要なソリューションは、AWS Organizationsを使用して環境内でテスト AWS Control Tower され

ていますAWS CloudFormation。を使用しない場合は AWS Control Tower、 AWS Organizations ベースのデプロイソリューションを使用できます。

セキュリティ基盤

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS SRA は、 AWS クラウド導入フレームワーク (AWS CAF)、 AWS Well-Architected、 責任 AWS 共有モデルという 3 つの AWS セキュリティ基盤と一致しています。

AWS プロフェッショナルサービスは、企業がクラウド導入を成功させるための迅速な道を設計し、それに従うのに役立つ AWS CAF を作成しました。フレームワークが提供するガイダンスとベストプラクティスは、企業全体および IT ライフサイクル全体でクラウドコンピューティングへの包括的なアプローチを構築するのに役立ちます。CAF は、視点と呼ばれる 6 AWS つの重点分野にガイダンスを整理します。 それぞれの視点は、機能に関連する利害関係者が所有または管理する明確な責任をカバーしています。一般に、ビジネス、人材、ガバナンスの視点はビジネス能力に重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的能力に焦点を当てています。

AWS CAF のセキュリティの視点は、ビジネス全体のコントロールの選択と実装を構築するのに役立ちます。セキュリティの柱に記載されている現在の AWS 推奨事項に従うことで、ビジネス要件と規制要件を満たすことができます。

AWS Well-Architected は、クラウドアーキテクトがアプリケーションとワークロードのための安全で高性能、耐障害性、効率的なインフラストラクチャを構築するのに役立ちます。このフレームワークは、運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、コスト最適化、持続可能性という 6 つの柱に基づいており、顧客とパートナーがアーキテクチャを評価し、時間の経過とともにスケールできる設計を実装するための一貫したアプローチ AWS を提供します。私たちは、well-architected ワークロードを設計することで、ビジネスの成功の可能性が大幅に高まると考えています。

Well-Architected フレームワークのセキュリティの柱では、クラウドテクノロジーを活用して、セキュリティ体制を改善できる方法でデータ、システム、アセットを保護する方法について説明します。これにより、現在の AWS 推奨事項に従うことで、ビジネス要件と規制要件を満たすことができます。Well-Architected フレームワークには、ガバナンス、サーバーレス、AI/ML、ゲームなど、特定のドメインのコンテキストをより詳細に把握できるその他の重点領域があります。これらは AWS Well-Architected レンズと呼ばれます。

セキュリティとコンプライアンスは、 AWS とお客様の間の責任共有です。この共有モデルは、ホストオペレーティングシステムや仮想化レイヤーから、サービスが運用されている施設の物理セキュリ

ティまで、様々なコンポーネントを AWS が運用、管理、およびコントロールするのでお客様の運用上の負担を軽減できます。たとえば、ゲストオペレーティングシステム (更新とセキュリティパッチを含む) 、アプリケーションソフトウェア、サーバー側のデータ暗号化、ネットワークトラフィックルートテーブル、 AWSおよび提供されたセキュリティグループファイアウォールの設定の責任と管理を引き受けます。Amazon S3 や Amazon DynamoDB などの抽象化されたサービスの場合、 はインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を操作し、エンドポイントにアクセスしてデータを保存および取得します。お客様は、データ (暗号化オプションを含む) の管理、アセットの分類、IAM ツールを使用して適切なアクセス許可を適用する責任があります。この共有モデルは、 AWS がクラウドのセキュリティ (で提供されているすべてのサービスを実行するインフラストラクチャの保護 AWS クラウド) を担当し、お客様がクラウドのセキュリティ (選択した AWS クラウド サービスによって決定される) を担当していると言うことで説明されることがよくあります。

これらの基本的なドキュメントで提供されるガイダンスでは、SRA の設計と理解には、セキュリティ機能とセキュリティ設計原則の 2 AWS つの概念セットが特に関連しています。

セキュリティ機能

CAF のセキュリティの観点からは、データとクラウドワークロードの機密性、完全性、可用性を実現するのに役立つ 9 AWS つの機能の概要を示しています。

- セキュリティガバナンスは、組織の AWS 環境全体でセキュリティのロール、責任、ポリシー、プロセス、手順を開発して伝達します。
- セキュリティおよびプライバシープログラムの有効性を監視、評価、管理、改善するためのセキュリティ保証。
- ID とアクセス管理は、ID とアクセス許可を大規模に管理します。
- 潜在的なセキュリティ設定ミス、脅威、または予期しない動作を理解して特定するための脅威検出。
- セキュリティの脆弱性を継続的に特定、分類、修復、軽減するための脆弱性管理。
- ワークロード内のシステムとサービスが保護されていることを検証するためのインフラストラクチャ保護。
- データの可視性と制御、および組織内でのデータのアクセスと使用方法を維持するためのデータ保護。
- ソフトウェア開発プロセス中にセキュリティの脆弱性を検出して対処するのに役立つアプリケーションセキュリティ。

- セキュリティインシデントに効果的に対応することで潜在的な害を軽減するためのインシデント対応。

セキュリティ設計原則

Well-Architected フレームワークのセキュリティの柱は、特定のセキュリティ領域をワークロードのセキュリティを強化するのに役立つ実用的なガイダンスに変換する 7 つの設計原則のセットをキャプチャします。セキュリティ機能が全体的なセキュリティ戦略を構成しているところでは、これらの Well-Architected フレームワークの原則は、実行できることを説明しています。これらはこの SRA AWS に非常に意図的に反映され、以下で構成されます。

- 強力なアイデンティティ基盤を実装する - 最小特権の原則を実装し、 AWS リソースとのやり取りごとに適切な認可で職務の分離を適用します。アイデンティティ管理を一元化し、長期的な静的認証情報への依存を排除することを目指します。
- トレーサビリティを有効にする – 環境に対するアクションと変更をリアルタイムでモニタリング、生成、監査します。ログとメトリクスの収集をシステムと統合して、自動的に調査してアクションを実行します。
- すべてのレイヤーにセキュリティを適用する – 複数のセキュリティコントロールでdefense-in-depthアプローチを適用します。エッジオブネットワーク、仮想プライベートクラウド (VPC)、ロードバランシング、インスタンスおよびコンピューティングサービス、オペレーティングシステム、アプリケーション設定、コードなど、複数のタイプのコントロール (予防コントロールや検出コントロールなど) をすべてのレイヤーに適用します。
- セキュリティのベストプラクティスを自動化する – 自動化されたソフトウェアベースのセキュリティメカニズムにより、より迅速かつ費用対効果の高い方法で安全にスケーリングする能力が向上します。セキュアなアーキテクチャを作成し、バージョン管理テンプレートでコードとして定義および管理されるコントロールを実装します。
- 転送中および保管中のデータを保護する - データを機密レベルに分類し、必要に応じて暗号化、トークン化、アクセス制御などのメカニズムを使用します。
- データから遠ざける – メカニズムとツールを使用して、データに直接アクセスしたり、手動で処理したりする必要性を軽減または排除します。これにより、機密データを扱う際の誤処理や変更、人的ミスのリスクが軽減されます。
- セキュリティイベントに備える – 組織の要件に合ったインシデント管理と調査のポリシーとプロセスを用意して、インシデントに備えます。インシデント対応シミュレーションを実行し、ツールと自動化により、検出、調査、復旧のスピードを上げます。

CAF AWS と AWS Well-Architected フレームワークで AWS SRA を使用する方法

AWS CAF、 AWS Well-Architected Framework、および AWS SRA は、クラウド移行とモダナイゼーションの取り組みをサポートするために連携する補完的なフレームワークです。

- AWS CAF は AWS 、経験とベストプラクティスを活用して、クラウド導入の価値を望ましいビジネス成果に合わせるのに役立ちます。 AWS CAF を使用して、トランスフォーメーションの機会を特定して優先順位付けし、クラウドの準備状況を評価して改善し、トランスフォーメーションロードマップを繰り返し進化させます。
- AWS Well-Architected フレームワークは、ビジネス成果を満たすさまざまなアプリケーションやワークロード向けに、安全で高性能、耐障害性、効率的なインフラストラクチャを構築するための AWS 推奨事項を提供します。
- AWS SRA は、CAF と AWS Well-Architected AWS フレームワークの推奨事項に沿った方法でセキュリティサービスをデプロイして管理する方法を理解する のに役立ちます。

たとえば、 AWS CAF セキュリティの観点からは、ワークフォース ID とその認証を一元管理する方法を評価することをお勧めします AWS。この情報に基づいて、Okta、Active Directory、Ping Identity などの新規または既存の企業 ID プロバイダー (IdP) ソリューションをこの目的で使用する場合があります。 AWS Well-Architected フレームワークのガイダンスに従い、IdP を と統合 AWS IAM アイデンティティセンター することで、従業員に対し、グループのメンバーシップとアクセス許可を同期できるシングルサインオンエクスペリエンスを提供します。 AWS SRA 推奨事項を確認して、 AWS 組織の管理アカウントで IAM Identity Center を有効にし、セキュリティ運用チームが使用するセキュリティツールアカウントを通じて管理します。この例では、CAF AWS が希望するセキュリティ体制に関する最初の決定にどのように役立つかを示し、 AWS Well-Architected フレームワークは、その目標を達成するために利用可能な を評価する方法に関するガイダンスを提供し、SRA AWS AWS のサービス は選択したセキュリティサービスをデプロイして管理する方法についての推奨事項を提供します。

SRA 構成要素 – AWS Organizations、アカウント、ガードレール

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS セキュリティサービス、そのコントロール、インタラクションは、 AWSマルチアカウント戦略と ID およびアクセス管理ガードレールの基盤に最適です。これらのガードレールは、最小特権、職務の分離、プライバシーを実装する機能を設定し、必要なコントロールの種類、各セキュリティサービスが管理される場所、 AWS SRA でデータとアクセス許可を共有する方法に関する決定をサポートします。

AWS アカウント は、リソースのセキュリティ、アクセス、請求の AWS 境界を提供し、リソースの独立性と分離を実現します。「複数のアカウントを使用して環境を整理する」ホワイトペーパーの「複数の を使用する利点 AWS アカウント」セクションで説明されているように、複数の を使用すること AWS アカウント は、セキュリティ要件を満たす上で重要な役割を果たします。 AWS たとえば、企業のレポート構造をミラーリングするのではなく、機能、コンプライアンス要件、または一般的な一連のコントロールに基づいて、組織単位 (OU) 内の別々のアカウントとグループアカウントにワークロードを整理できます。セキュリティとインフラストラクチャを念頭に置いて、ワークロードの拡大に合わせて企業が共通のガードレールを設定できるようにします。このアプローチは、ワークロード間の堅牢な境界と制御を提供します。アカウントレベルの分離は、 と組み合わせて AWS Organizations、本番環境を開発環境やテスト環境から分離したり、Payment Card Industry Data Security Standard (PCI DSS) や Health Insurance Portability and Accountability Act (HIPAA) などの異なる分類のデータを処理するワークロード間の強力な論理境界を提供するために使用されます。1 つのアカウントから AWS ジャーニーを開始することもできますが、 では、ワークロードのサイズと複雑さが大きくなるにつれて、複数のアカウントを設定する AWS ことをお勧めします。

アクセス許可を使用すると、 AWS リソースへのアクセスを指定できます。アクセス許可は、プリンシパル (ユーザー、グループ、ロール) として知られる IAM エンティティに付与されます。デフォルトでは、プリンシパルはアクセス許可なしで始まります。IAM プリンシパルは、アクセス許可を付与 AWS するまで で何も実行できません。また、 AWS 組織全体と同様に広範囲に適用されるガードレールを設定することも、プリンシパル、アクション、リソース、条件を個別に組み合わせてきめ細かく設定することもできます。

セキュリティ AWS Organizations のための の使用

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS Organizations は、 AWS リソースの拡大とスケーリングに合わせて環境を一元管理および管理するのに役立ちます。を使用すると AWS Organizations、プログラムで新しい を作成し AWS アカウント、リソースを割り当て、アカウントをグループ化してワークロードを整理し、ガバナンスのためにアカウントまたはアカウントのグループにポリシーを適用できます。 AWS 組織は を統合し AWS アカウント 、それらを 1 つのユニットとして管理できるようにします。1 つの管理アカウントと、ゼロ以上のメンバーアカウントを含みます。ほとんどのワークロードはメンバーアカウントにありますが、管理アカウントまたは特定の の委任管理者として割り当てられたアカウントに存在する必要がある、一元管理されたプロセスの一部を除きます AWS のサービス。セキュリティチームが AWS 組織に代わってセキュリティニーズを管理するためのツールとアクセスを一元的に提供できます。 AWS 組織内で重要なリソースを共有することで、リソースの重複を減らすことができます。アカウントを AWS 組織単位 (OUs) にグループ化して、ワークロードの要件と目的に基づいて異なる環境を表すことができます。 には、組織内のすべてのメンバーアカウントに追加のセキュリティコントロールを一元的に適用できるいくつかのポリシー AWS Organizations も用意されています。このセクションでは、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)、宣言ポリシーに焦点を当てます。

では AWS Organizations、SCPs と RCPs を使用して、 AWS 組織、OU、またはアカウントレベルでアクセス許可ガードレールを適用できます。SCPsは、管理アカウント (このアカウントでワークロードを実行しない理由の 1 つ) を除き、組織のアカウント内のプリンシパルに適用されるガードレールです。SCP を OU にアタッチすると、SCP はその OUs の子 OU とアカウントによって継承されます。SCP はいかなるアクセス許可も付与しません。代わりに、 AWS 組織、OU、またはアカウントのプリンシパルが使用できるアクセス許可の上限を指定します。実際にアクセス許可を付与するには、アイデンティティベースまたはリソースベースのポリシーを AWS アカウント のプリンシパルまたはリソースにアタッチする必要があります。例えば、SCP がすべての Amazon S3 へのアクセスを拒否した場合、SCP の影響を受けるプリンシパルは、IAM ポリシーを通じて明示的にアクセス権が 付与されていても Amazon S3 にアクセスできません。IAM ポリシーの評価方法、SCPs「ポリシー評価ロジック」を参照してください。

RCPsは、リソースが同じ組織に属しているかどうかに関係なく、組織のアカウント内のリソースに適用されるガードレールです。SCPs と同様に、RCPs管理アカウントのリソースには影響せず、アクセス許可も付与しません。RCP を OU にアタッチすると、RCP は OUs の子 OU とアカウントに

よって継承されます。RCPsは、組織内のリソースで使用可能なアクセス許可の最大数を一元的に制御し、現在 のサブセットをサポートしています AWS のサービス。OUs 用に SCPs を設計する場合は、IAM ポリシーシミュレーターを使用して変更を評価することをお勧めします。また、IAM でサービスの最終アクセス時間データを確認し、 を使用してAWS CloudTrail サービス使用状況を API レベルでログに記録し、SCP の変更による潜在的な影響を理解する必要があります。

SCP と RCP は独立したコントロールです。SCPs または RCPs のみを有効にするか、適用するアクセスコントロールに基づいて両方のポリシータイプを一緒に使用することを選択できます。たとえば、組織のプリンシパルが組織外のリソースにアクセスできないようにするには、SCPs。外部 ID がリソースにアクセスできないように制限または防止する場合は、RCPs を使用してこのコントロールを適用します。RCP と SCP の詳細SCPsSCPs RCPs」を参照してください。 AWS Organizations

AWS Organizations 宣言ポリシーを使用して、組織全体 AWS のサービス の大規模な特定の に必要な設定を一元的に宣言して適用できます。例えば、組織全体の Amazon VPC リソースへのパブリックインターネットアクセスをブロックできます。SCPs や RCPs などの認可ポリシーとは異なり、宣言ポリシーは AWS サービスのコントロールプレーンで適用されます。認可ポリシーは APIs へのアクセスを規制しますが、宣言ポリシーはサービスレベルで直接適用され、永続的なインテントを適用します。 これらのポリシー AWS のサービス は、サービスが新機能や APIs を導入した場合でも、のベースライン設定が常に維持されるようにするのに役立ちます。ベースライン設定は、新しいアカウントが組織に追加された場合や、新しいプリンシパルやリソースが作成された場合でも維持されます。宣言ポリシーは、組織全体、または特定の OUs またはアカウントに適用できます。

すべての AWS アカウント には、デフォルトですべての AWS リソースに対する完全なアクセス許可を持つ単一のルートユーザーがあります。 セキュリティのベストプラクティスとして、ルートユーザーを明示的に必要とするいくつかのタスクを除き、ルートユーザーを使用しないことをお勧めします。複数の AWS アカウント を通じて管理する場合 AWS Organizations、ルートサインインを一元的に無効にし、すべてのメンバーアカウントに代わってルート特権アクションを実行できます。メンバーアカウントのルートアクセスを一元管理した後、ルートユーザーのパスワード、アクセスキー、署名証明書を削除し、メンバーアカウントの多要素認証 (MFA) を非アクティブ化できます。一元管理されたルートアクセスで作成された新しいアカウントには、デフォルトではルートユーザーの認証情報はありません。メンバーアカウントは、ルートユーザーでサインインしたり、ルートユーザーのパスワード復旧を実行したりすることはできません。

AWS Control Tower は、複数のアカウントを設定と管理を簡素化する方法を提供します。組織内のアカウントのセットアップを自動化し AWS 、プロビジョニングを自動化し、コントロール (予防コントロールと検出コントロールを含む) を適用し、可視性のためのダッシュボードを提供します。追加の IAM 管理ポリシーである アクセス許可の境界 は、特定の IAM プリンシパル (ユーザーまたは

ロール) にアタッチされ、アイデンティティベースのポリシーが IAM プリンシパルに付与できるアクセス許可の上限を設定します。

AWS Organizations は、すべてのアカウントAWS のサービスに適用される を設定するのに役立ちます。例えば、CloudTrail を使用して AWS 組織全体で実行されるすべてのアクションの中央ログ記録を設定し、メンバーアカウントによるログ記録の無効化を防ぐことができます。 CloudTrail また、を使用して定義したルールのデータを一元的に集約できるためAWS Config、ワークロードのコンプライアンスを監査し、変更に迅速に対応できます。AWS CloudFormation StackSets を使用して、AWS 組織内のアカウントと OUs 間で CloudFormation スタックを一元管理できるため、セキュリティ要件を満たすために新しいアカウントを自動的にプロビジョニングできます。

のデフォルト設定では、拒否リストとしての SCPs の使用 AWS Organizations がサポートされています。拒否リスト戦略を使用することで、メンバーアカウント管理者は、特定のサービスや一連のアクションを拒否する SCP を作成してアタッチするまで、すべてのサービスとアクションを委譲できます。拒否ステートメントは、 が新しいサービス AWS を追加するときに更新する必要がないため、許可リストよりもメンテナンスが少なくて済みます。拒否ステートメントは通常、文字長が短いため、SCPs の最大サイズ内に留まりやすくなります。`Effect` 要素に `Deny` の値があるステートメントでは、特定のリソースへのアクセスを制限したり、SCP 有効時における条件を定義することもできます。対照的に、SCP の `Allow` ステートメントは、すべてのリソース ("`*`") に適用され、条件による制限を受けることができません。詳細と例については、 AWS Organizations ドキュメントのSCPs」を参照してください。

設計上の考慮事項

- または、SCPs を許可リストとして使用するには、AWS マネージド `FullAWSAccess` SCP を、許可するサービスとアクションのみを明示的に許可する SCP に置き換える必要があります。指定されたアカウントに対してアクセス許可を有効にするには、すべての SCP (ルートからアカウントへの直接パス内の各 OU を経由し、アカウント自体にアタッチする) がそのアクセス許可を許可する必要があります。このモデルは本質的により制限的であり、規制の厳しい機密性の高いワークロードに適している可能性があります。このアプローチでは、 から OU AWS アカウント へのパス内のすべての IAM サービスまたはアクションを明示的に許可する必要があります。
- 理想的には、拒否リストと許可リスト戦略の組み合わせを使用します。許可リストを使用して、 AWS 組織内で使用が許可されている AWS のサービス 承認済み のリストを定義し、この SCP を組織のルートにアタッチします AWS 。開発環境ごとに異なるサービスセットが許可されている場合は、各 OU にそれぞれの SCPs をアタッチします。その後、

拒否リストを使用して、特定の IAM アクションを明示的に拒否することで、エンタープライズガードレールを定義できます。

- RCPs、 のサブセットのリソースに適用されます AWS のサービス。詳細については、 ドキュメントの「RCP AWS のサービス をサポートする のリスト RCPs」を参照してください。 AWS Organizations のデフォルト設定では、拒否リストとしての RCPs の使用 AWS Organizations がサポートされています。組織で RCPs を有効にすると、 という AWS 管理ポリシー`RCPFullAWSAccess`が組織ルート、すべての OU、および組織内のすべてのアカウントに自動的にアタッチされます。このポリシーをデタッチすることはできません。このデフォルトの RCP では、すべてのプリンシパルとアクションのアクセスが RCP 評価を通過できます。つまり、RCPs の作成とアタッチを開始するまで、既存の IAM アクセス許可はすべてそのまま動作し続けます。この AWS 管理ポリシーはアクセスを許可しません。その後、組織内のリソースへのアクセスをブロックする拒否ステートメントのリストとして新しい RCPs を作成できます。

管理アカウント、信頼されたアクセス、および委任された管理者

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

管理アカウント (AWS 組織管理アカウントまたは組織管理アカウントとも呼ばれます) は一意であり、 の他のすべてのアカウントと区別されます AWS Organizations。これは、 AWS 組織を作成するアカウントです。このアカウントから、 AWS 組織 AWS アカウント で を作成し、他の既存のアカウントを AWS 組織に招待し (どちらのタイプもメンバーアカウントと見なされます) 、 AWS 組織からアカウントを削除し、 AWS 組織内のルート、OUs、またはアカウントに IAM ポリシーを適用できます。

管理アカウントは、組織内のすべてのメンバーアカウントに影響を与える SCPs、RCPs、サービスデプロイ (CloudTrail など) を通じてユニバーサルセキュリティガードレールをデプロイします AWS 。管理アカウントのアクセス許可をさらに制限するために、これらのアクセス許可は、可能であればセキュリティアカウントなどの別の適切なアカウントに委任できます。

管理アカウントには、支払いアカウントだけでなく、メンバーアカウントによって発生したすべての料金を支払う責任があります。 AWS 組織の管理アカウントを切り替えることはできません。は、一度に 1 つの AWS 組織のメンバーのみ AWS アカウント にすることができます。

管理アカウントが保持する機能と影響範囲から、このアカウントへのアクセスを制限し、必要なロールにのみアクセス許可を付与することをお勧めします。これを実現するための機能として、信頼されたアクセス と 委任された管理者 の 2 つがあります。信頼されたアクセスを使用して、信頼 AWS のサービス されたサービスと呼ばれる指定した を有効にし、ユーザーに代わって AWS 組織とそのアカウントでタスクを実行できます。 このためには、信頼されたサービスにアクセス許可を付与する必要がありますが、IAM ユーザーまたはロールのアクセス許可に影響はありません。信頼されたアクセスを使用して、信頼されたサービスがユーザーに代わって AWS 組織のアカウントで維持する設定と設定の詳細を指定できます。例えば、SRA の組織管理アカウントセクションでは、CloudTrail AWS サービスに信頼されたアクセス権を付与して、組織内のすべてのアカウントに AWS CloudTrail 組織の証跡を作成する方法について説明します。

一部の は、 の委任管理者機能 AWS のサービス をサポートしています AWS Organizations。この機能を使用すると、互換性のあるサービスは AWS 、組織内の AWSメンバーアカウントを、そのサービス内の AWS 組織のアカウントの管理者として登録できます。この機能を使用すると、企業内のさまざまなチームが、責任に応じて個別のアカウントを使用して環境 AWS のサービス 全体で管理できる柔軟性が得られます。現在委任管理者をサポートしている SRA AWS AWS のセキュリティサービスには、IAM Identity Center、 AWS Config AWS Firewall Manager、Amazon GuardDuty、IAM Access Analyzer、Amazon Macie、 AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM)、Amazon Detective、 AWS Audit Manager、Amazon Inspector、および が含まれます AWS Systems Manager。ベストプラクティスとして、委任管理者機能の使用が SRA AWS で強調されており、セキュリティ関連サービスの管理を Security Tooling アカウントに委任しています。

専用アカウント構造

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS アカウント は、リソース AWS のセキュリティ、アクセス、請求の境界を提供し、リソースの独立性と分離を実現します。デフォルトでは、アカウント間のアクセスは許可されていません。

OU とアカウント構造を設計するときは、セキュリティとインフラストラクチャを考慮した上でスタートします。これらの特定の機能のために、インフラストラクチャとセキュリティ OU に分かれて、一連の基礎的なOUを作成することをお勧めします。これらの OU およびアカウントレコメンデーションは、 AWS Organizations およびマルチアカウント構造設計に関するより広範で包括的なガイドラインのサブセットをキャプチャします。推奨事項の完全なセットについては、 ドキュメン

トの AWS「複数のアカウントを使用した AWS 環境の整理」とブログ記事「 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 SRA は、以下のアカウントを使用して、効果的なセキュリティオペレーションを実現しますAWS。これらの専用アカウントは、職務の分離を確実にし、アプリケーションやデータの機密性に応じて異なるガバナンスとアクセスポリシーをサポートし、セキュリティイベントの影響を軽減するのに役立ちます。続く議論では、本番用 (製品) アカウントとそれに関連するワークロードに焦点を当てます。ソフトウェア開発ライフサイクル (SDLC) アカウント (しばしば dev および テスト アカウントと呼ばれる) は、成果物をステージングにあげることを目的としており、本番用アカウントとは異なるセキュリティポリシーセットで運用することが可能です。

アカウント	OU	セキュリティロール
管理	—	すべての アカウントと アカウントの一元的なガバナンス AWS リージョン と管理。組織のルート AWS をホスト AWS アカウント する 。
セキュリティツール	セキュリティ	幅広く適用可能なセキュリティサービス (GuardDuty、Security Hub CSPM、Audit Manager、Detective、Amazon Inspector など AWS Config) の運用、セキュリティアラート AWS アカウントと対応のモニタリングと自動化 AWS アカウント に専念しています。(セキュリティ OU のアカウントの AWS Control Towerデフォルト名は監査アカウントです) 。
ログアーカイブ	セキュリティ	すべての と AWS アカウントのすべてのログ記録とバックアップの取り込みとアーカイブ専用です AWS リージョン AWS アカウント。これは、イ

		ミュータブルストレージとして設計する必要があります。
Network	インフラストラクチャ	アプリケーションとより広範なインターネット間のゲートウェイ。Network アカウントは、個々のアプリケーションワークロード、セキュリティ、およびその他のインフラストラクチャから広範なネットワークサービス、構成、およびオペレーションを分離します。
共有サービス	インフラストラクチャ	このアカウントは、複数のアプリケーションやチームが成果をあげるために利用するサービスをサポートしています。例としては、Identity Center ディレクトリサービス (Active Directory)、メッセージングサービス、メタデータサービスなどがあります。
アプリケーション	ワークロード	AWS アカウント AWS 組織のアプリケーションをホストし、ワークロードを実行する 。(これらはワークロードアカウントと呼ばれることもあります) 。アプリケーションアカウントは、チームにマッピングされるのではなく、ソフトウェアサービスを分離するために作成する必要があります。これにより、デプロイされたアプリケーションは、組織の変化に強くなります。

AWS SRA AWS の組織とアカウント構造

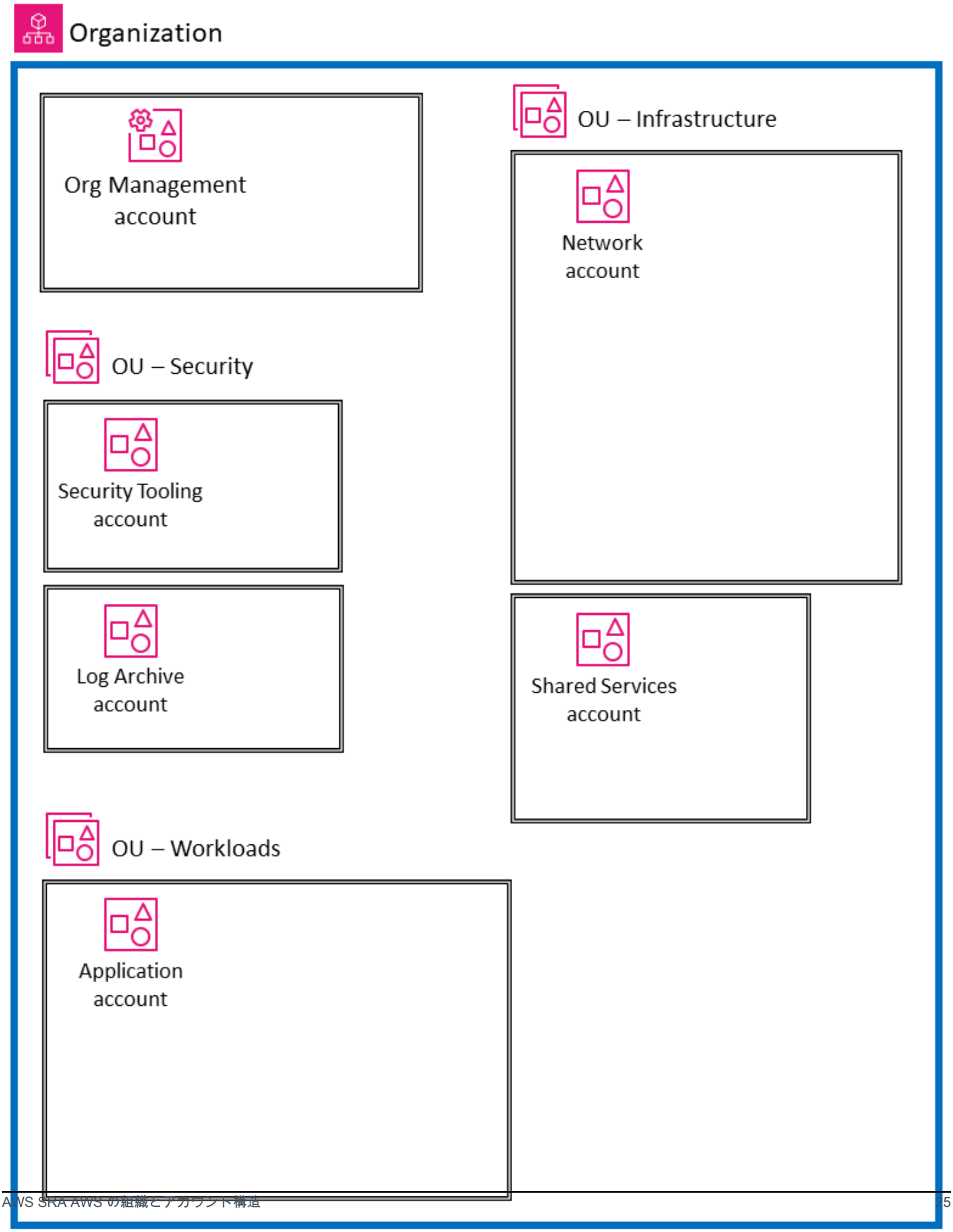
簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は、特定のサービスを表示せずに AWS SRA の高レベルの構造を示しています。この図表は、前のセクションで説明した専用アカウント構造を反映しており、ここではアーキテクチャの主要コンポーネントを中心に議論を進めるために、この図を掲載しています。

- 図表に表示されているすべてのアカウントは、1 つの AWS 組織に属しています。
- 図の左上には、 AWS 組織の作成に使用される組織管理アカウントがあります。
- 組織管理アカウントの下には、セキュリティ OU があり、セキュリティツール用とログアーカイブ用の 2 つのアカウントがあります。
- 右側には、ネットワークアカウントと共有サービスアカウントを持つインフラストラクチャ OU があります。
- 図表の下部には、ワークロード OU があり、エンタープライズアプリケーションを格納するアプリケーションアカウントに関連付けられています。

このガイダンスでは、すべてのアカウントが 1 つの で動作する本番稼働用 (製品) アカウントと見なされます AWS リージョン。ほとんどの AWS のサービス (グローバルサービスを除く) はリージョン別にスコープされています。つまり、サービスのコントロールプレーンとデータプレーンは、それぞれに独立して存在します AWS リージョン。このため、ランド AWS スケープ全体を確実にカバーするには、 AWS リージョン 使用する予定のすべての にこのアーキテクチャをレプリケートする必要があります。特定の にワークロードがない場合は AWS リージョン、SCPs を使用するか、ログ記録とモニタリングメカニズムを使用してリージョンを無効にする必要があります。Security Hub CSPM を使用して、検出結果とセキュリティスコアを複数の集約リージョンから 1 つの集約リージョン AWS リージョン に集約し、一元的に可視化できます。

大規模なアカウントセットで AWS 組織をホストする場合、アカウントの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が有益です。 AWS Control Tower では、 AWS マルチアカウント環境を簡単にセットアップして管理できます。GitHub リポジトリの AWS SRA コードサンプルは、Customizations for AWS Control Tower (CfCT) ソリューションを使用して SRA AWS 推奨構造をデプロイする方法を示しています。

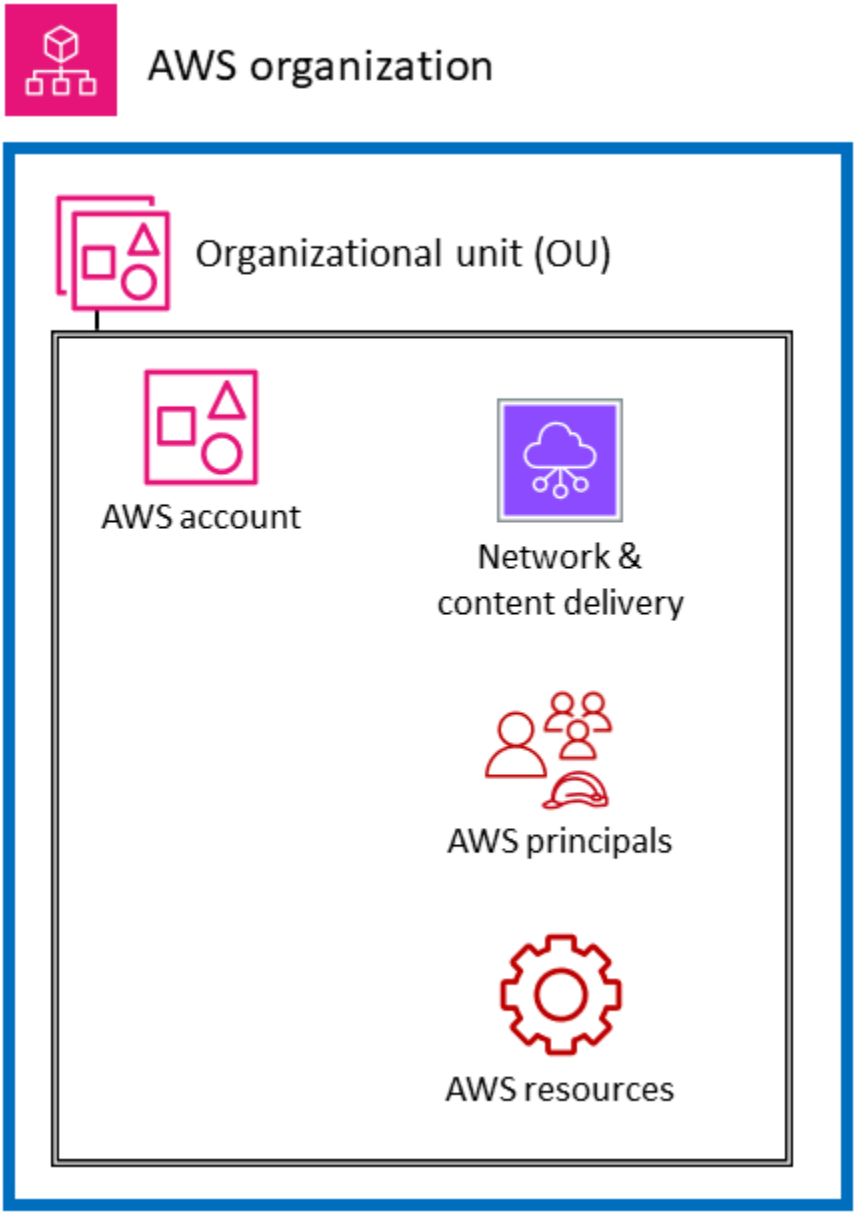

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

AWS 組織全体にセキュリティサービスを適用する

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

前のセクションで説明したように、お客様はセキュリティサービス全体 AWS について考え、戦略的に整理するための追加の方法を探しています。現在の最も一般的な組織的アプローチは、各サービスの動作に応じて、セキュリティサービスをプライマリ機能別にグループ化することです。CAF のセキュリティの観点からは、ID とアクセスの管理、インフラストラクチャの保護、データ保護、脅威の検出など、9 AWS つの機能を示しています。これらの機能 AWS のサービス と組み合わせることは、各領域で実装を決定する実用的な方法です。例えば、ID とアクセスの管理を検討する場合、IAM と IAM アイデンティティセンターは考慮すべきサービスです。脅威検出アプローチを設計するときは、GuardDuty を最初に検討してください。

この機能ビューの補完として、クロスカット構造ビューでセキュリティを表示することもできます。つまり、「アイデンティティ、論理アクセス、または脅威検出メカニズムを制御および保護するためにどの を使用する AWS のサービス べきか？」と尋ねるだけでなく、 AWS 「組織全体にどの を適用 AWS のサービス すべきか？」と尋ねることもできます。アプリケーションの中核にある Amazon EC2 インスタンスを保護するために導入する必要がある防御レイヤーは何ですか？」 このビューでは、 AWS のサービス および の機能を AWS 環境内のレイヤーにマッピングします。一部のサービスと機能は、 AWS 組織全体にコントロールを実装するのに最適です。例えば、Amazon S3 バケットへのパブリックアクセスをブロックすることは、このレイヤーにおける特定のコントロールです。これは、個々のアカウント設定の一部ではなく、ルート組織で行うことをお勧めします。他のサービスや機能は、 内の個々のリソースを保護するのに最適です AWS アカウント。プライベート TLS 証明書を必要とするアカウント内での下位認証機関 (CA) の実装は、このカテゴリの例です。もう 1 つの同様に重要なグループ化は、 AWS インフラストラクチャの仮想ネットワークレイヤーに影響を与えるサービスで構成されます。次の図は、一般的な AWS 環境の 6 つのレイヤーを示しています。 AWS 組織、組織単位 (OU)、アカウント、ネットワークインフラストラクチャ、プリンシパル、リソースです。



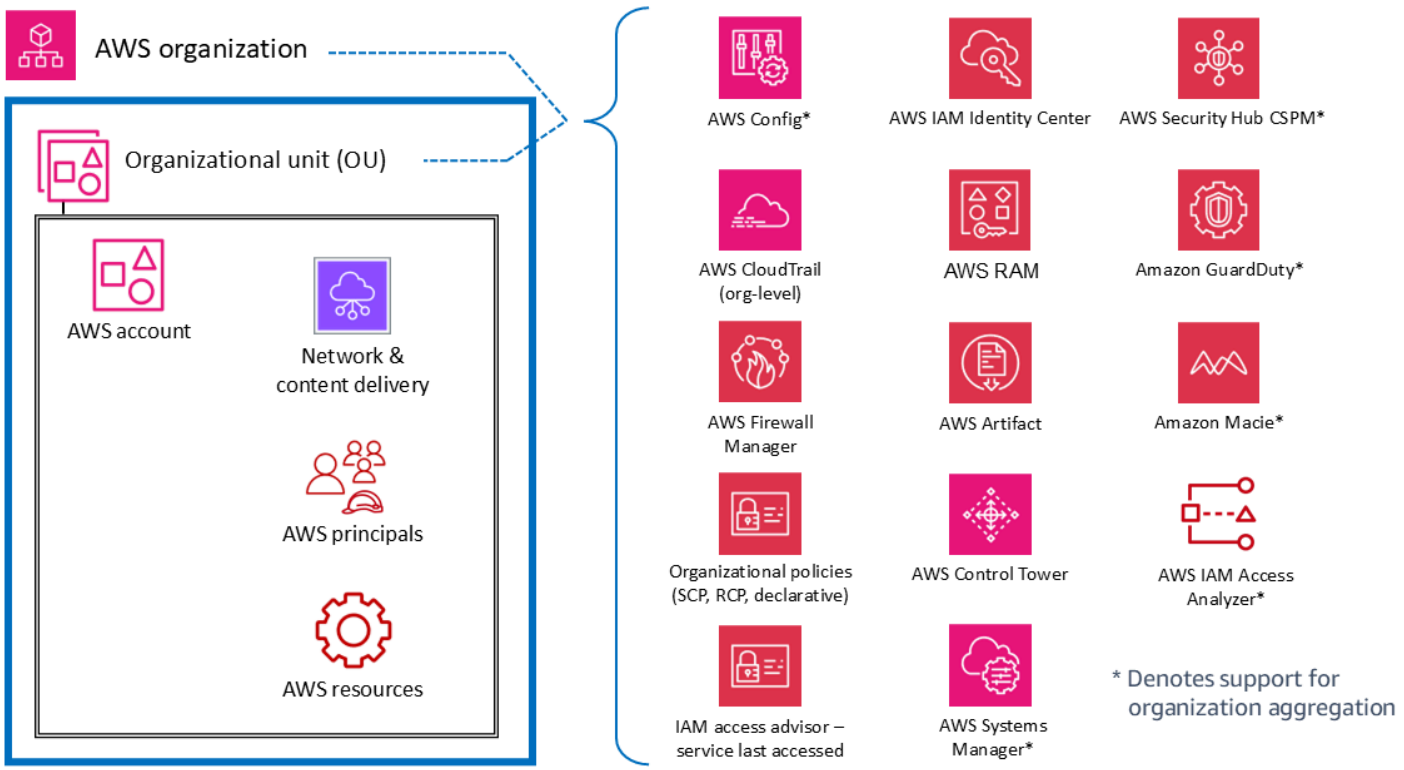
各レイヤーのコントロールや保護など、この構造コンテキストにおけるサービスを理解することで、AWS 環境全体でdefense-in-depth戦略を計画および実装できます。この視点では、トップダウン (たとえば、 AWS 「組織全体でセキュリティコントロールを実装するためにどのサービスを使用していますか？」) とボトムアップ (たとえば、「この EC2 インスタンスでコントロールを管理するのはどのサービスですか？」) の両方の質問に答えることができます。このセクションでは、 AWS 環境の要素について説明し、関連するセキュリティサービスと機能を特定します。もちろん、一部の AWS のサービス には幅広い機能セットがあり、複数のセキュリティ目標をサポートしています。これらのサービスは、 AWS 環境の複数の要素をサポートする場合があります。

わかりやすくするために、一部のサービスが記述された目的にどのように適合するかについて簡単に説明します。次のセクションでは、各 内の個々のサービスについて詳しく説明します AWS アカウント。

組織全体または複数のアカウント

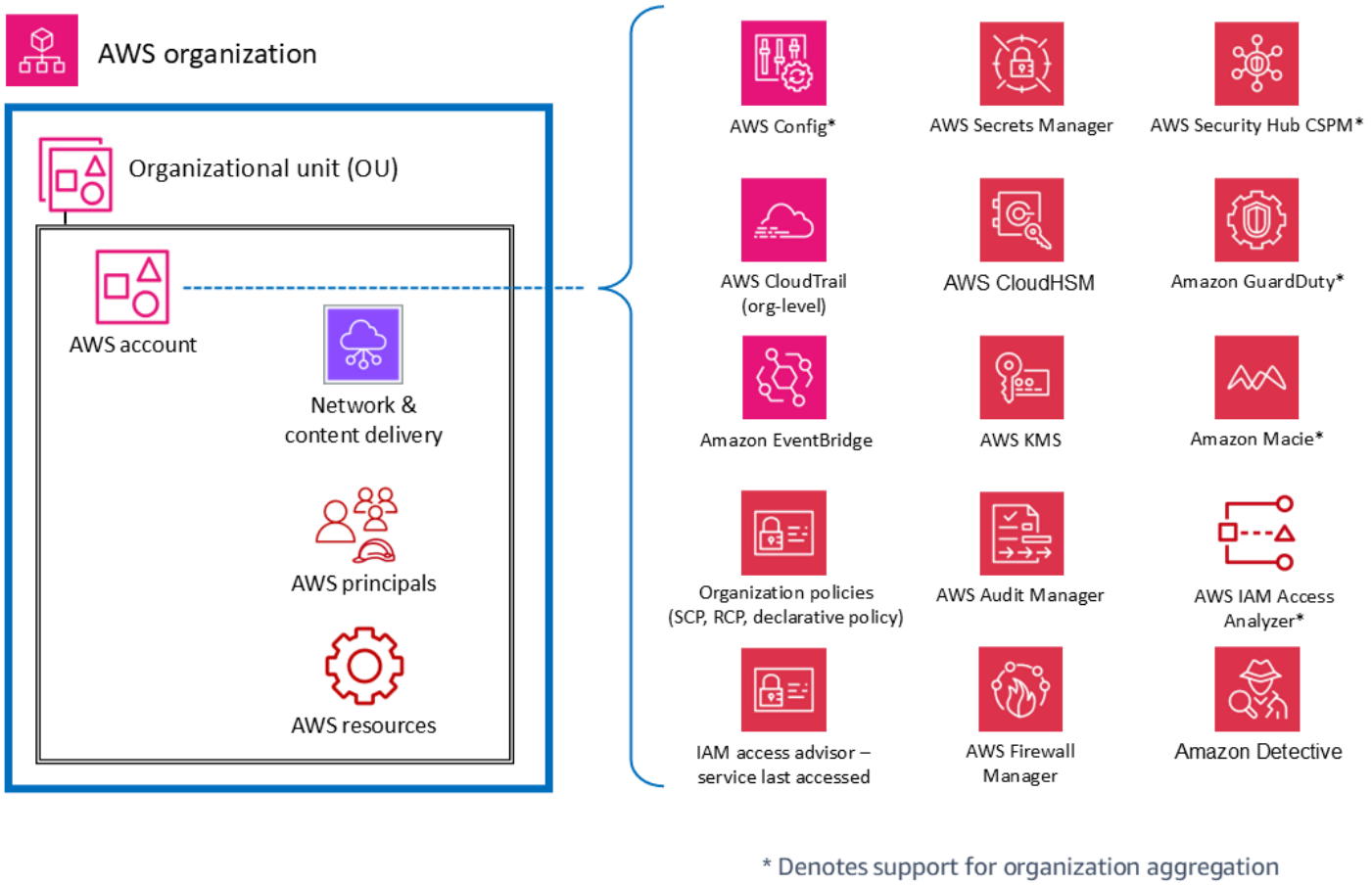
トップレベルには、 AWS 組織内の 複数のアカウント (組織全体または特定の OUs を含む) にガバナンスと制御機能またはガードレールを適用するように設計された AWS のサービス および 機能があります。サービスコントロールポリシー (SCPs) とリソースコントロールポリシー (RCPs) は、予防的で AWS 組織全体のガードレールを提供する IAM 機能の好例です。 は、 のベースライン設定を大規模 AWS のサービス に一元的に定義して適用する宣言ポリシー AWS Organizations も提供します。もう 1 つの例は CloudTrail です。CloudTrail は、その組織内のすべての のすべてのイベントを記録する組織の証跡を通じてモニタリングを提供します。 AWS アカウント AWS この包括的な証跡は、各アカウントで作成される可能性のある個々の証跡とは異なるものです。3 番目の例は AWS Firewall Manager、 AWS 組織内のすべてのアカウントで複数のリソースを設定、適用、管理するために使用できる です。 AWS WAF ルール、 AWS WAF Classic ルール、 AWS Shield Advanced 保護、Amazon Virtual Private Cloud (Amazon VPC) セキュリティグループ、 AWS Network Firewall ポリシー、DNS Firewall Amazon Route 53 Resolver ポリシーです。

次の図でアスタリスク (*) が付いているサービスは、組織全体とアカウントに焦点を当てた 2 つのスコープで動作します。これらのサービスは、個々のアカウント内のセキュリティを基本的にモニタリングまたは制御するのに役立ちます。ただし、一元化された可視性と管理のために、複数のアカウントから組織全体のアカウントに結果を集約する機能もサポートしています。わかりやすくするために、OU 全体 AWS アカウント、または AWS 組織全体に適用される SCPs を検討してください。対照的に、GuardDuty は、アカウントレベル (個々の検出結果が生成される場所) と、検出結果を集計して表示および管理できる AWS 組織レベル (委任管理者機能を使用) の両方で設定および管理できます。



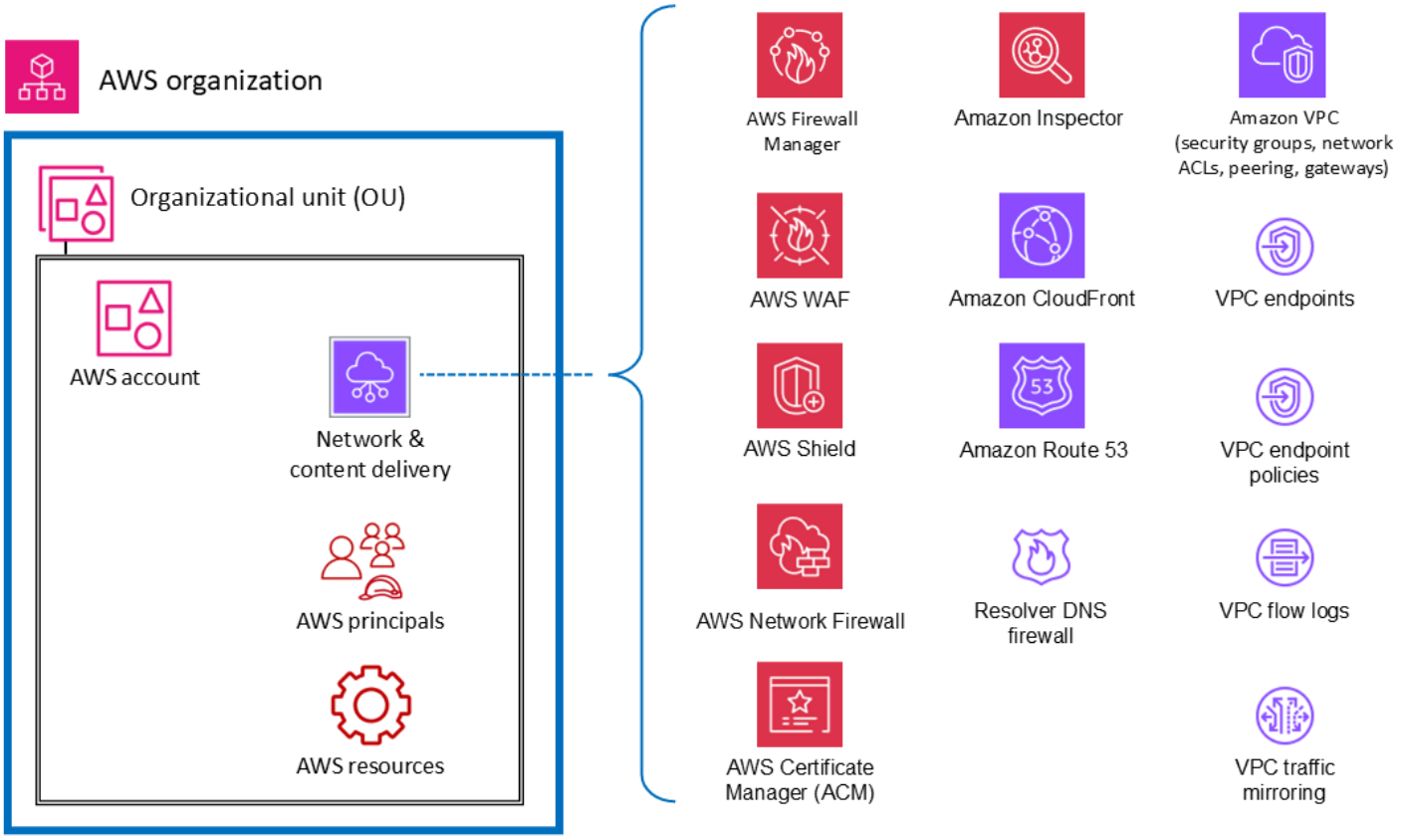
AWS アカウント

OUs 内には、 内の複数のタイプの要素を保護するのに役立つサービスがあります AWS アカウント。例えば、 AWS Secrets Manager は通常、特定のアカウントから管理され、 AWS のサービス そのアカウントのリソース (データベース認証情報や認証情報など) 、アプリケーション、および を保護します。IAM Access Analyzer は、指定されたリソースが 外のプリンシパルからアクセス可能な場合に検出結果を生成するように設定できます AWS アカウント。前のセクションで説明したように、これらの サービスの多くは 内で設定および管理できるため AWS Organizations、複数のアカウントで管理できます。これらのサービスは、図でアスタリスク (*) でマークされています。また、複数のアカウントの結果を集約し、1 つのアカウントに配信することが容易になります。これにより、個々のアプリケーションチームはワークロード固有のセキュリティニーズを管理する柔軟性と可視性を得ると同時に、一元化されたセキュリティチームのガバナンスと可視性を実現できます。GuardDuty はこのようなサービスの例です。GuardDuty は、1 つのアカウントに関連付けられたリソースとアクティビティをモニタリングし、複数のメンバーアカウント (AWS 組織内のすべてのアカウントなど) からの GuardDuty の検出結果を委任された管理者アカウントから収集、表示、管理できます。



仮想ネットワーク、コンピューティング、コンテンツ配信

ネットワークアクセスはセキュリティにとって非常に重要であり、コンピューティングインフラストラクチャは多くの AWS ワークロードの基本的なコンポーネントであるため、これらのリソース専用の AWS 多くのセキュリティサービスと機能があります。例えば、Amazon Inspector は、 AWS ワークロードの脆弱性を継続的にスキャンする脆弱性管理サービスです。これらのスキャンには、環境内の Amazon EC2 インスタンスへのネットワークパスが許可されていることを示すネットワーク到達可能性チェックが含まれます。Amazon VPC では、 AWS リソースを起動できる仮想ネットワークを定義できます。この仮想ネットワークは、従来のネットワークによく似ており、さまざまな機能と利点が含まれています。VPC エンドポイントを使用すると、インターネットへのパスを必要と AWS PrivateLink せずに、サポートされている AWS のサービス および を搭載したエンドポイントサービスに VPC をプライベートに接続できます。次の図は、ネットワーク、コンピューティング、コンテンツ配信インフラストラクチャに焦点を当てたセキュリティサービスを示しています。



プリンシパルとリソース

AWS プリンシパルと AWS リソース (IAM ポリシーとともに) は、アイデンティティとアクセス管理の基本要素です AWS。の認証されたプリンシパル AWS は、アクションを実行し、 AWS リソースにアクセスできます。プリンシパルは、 AWS アカウント ルートユーザーおよび IAM ユーザーとして認証することも、ロールを引き受けることで認証することもできます。

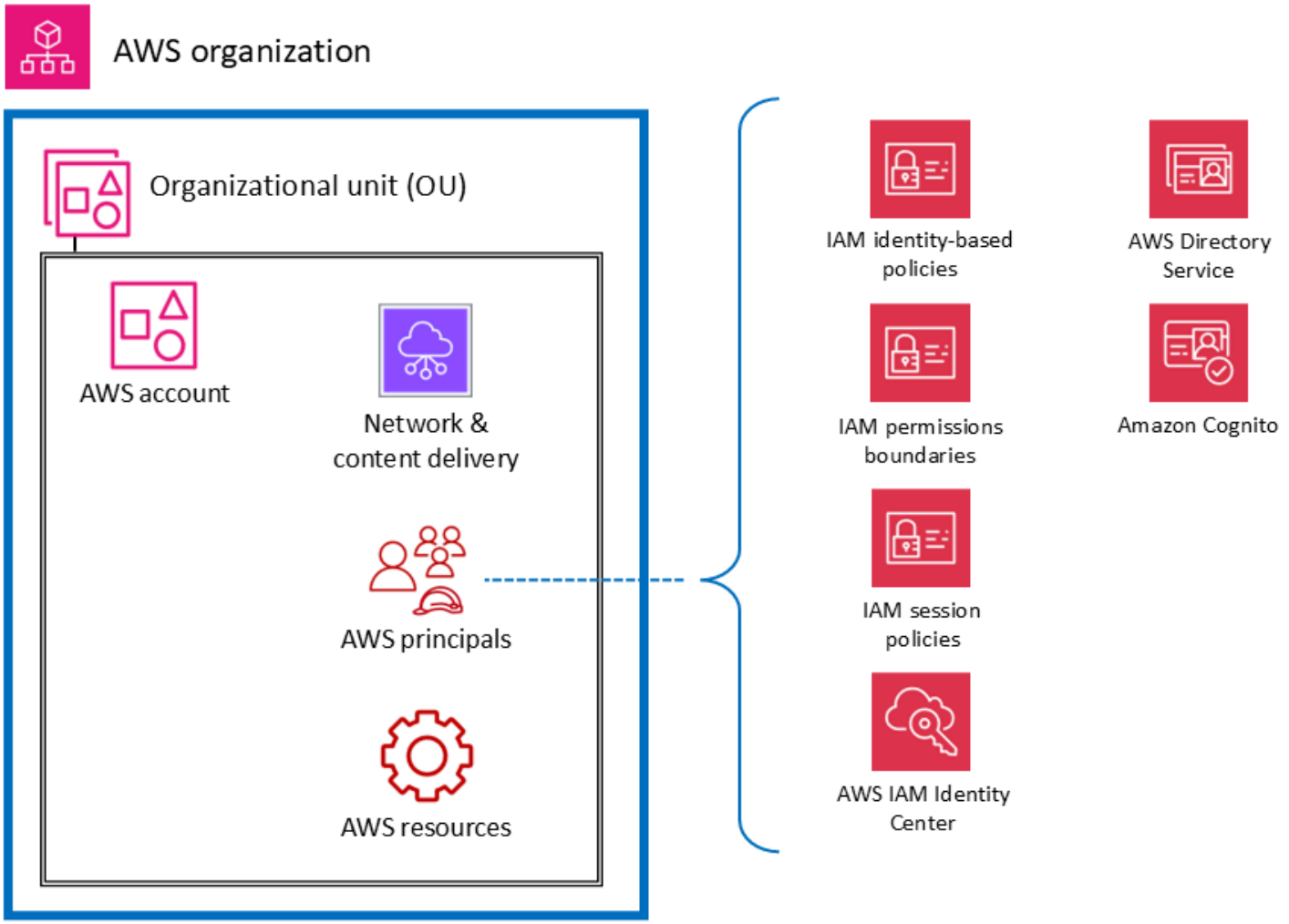
> **Note**
>
> AWS ルートユーザーアカウントに関連付けられた永続 API キーを作成しないでください。ルートユーザーアカウントへのアクセスは、ルートユーザーを必要とするタスクのみに制限し、厳格な例外と承認プロセスを通じてのみ制限する必要があります。アカウントのルートユーザーを保護するためのベストプラクティスについては、IAM ドキュメントを参照してください。

AWS リソースは、 AWS のサービス 操作できる 内に存在するオブジェクトです。例としては、EC2 インスタンス、 CloudFormation スタック、Amazon Simple Notification Service (Amazon SNS) ト

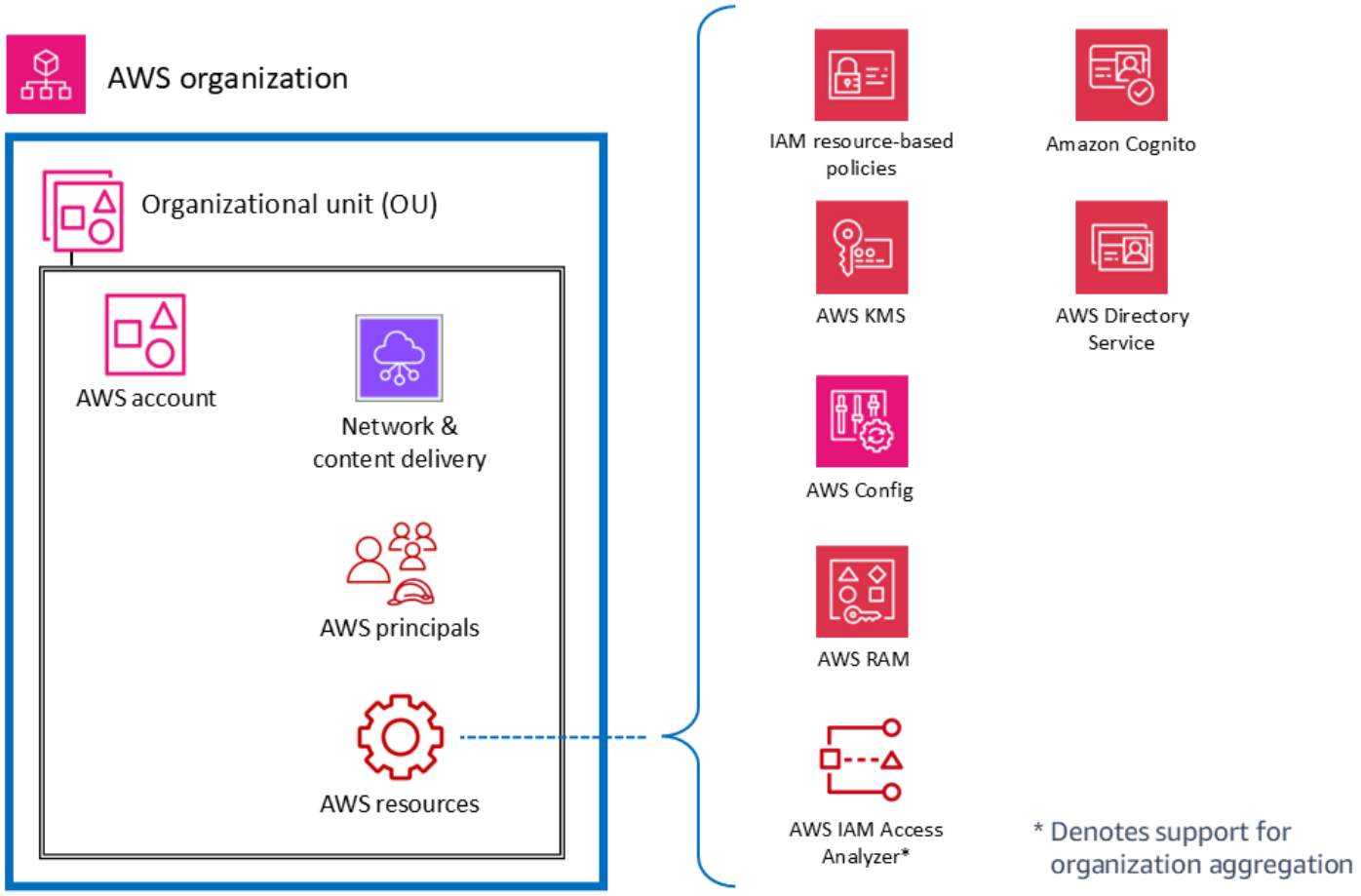
ピック、S3 バケットなどがあります。IAM ポリシーは、IAM プリンシパル (ユーザー、グループ、またはロール) または AWS リソースに関連付けられているときにアクセス許可を定義するオブジェクトです。ID ベースのポリシー は、プリンシパル (ロール、ユーザー、ユーザーのグループ) にアタッチして、プリンシパルが実行できるアクション、リソース、および条件を制御するポリシードキュメントです。リソースベースのポリシー は、S3 バケットなどのリソースにアタッチするポリシードキュメントです。これらのポリシーは、指定されたプリンシパルに、そのリソースに対して特定のアクションを実行し、そのアクセス許可の条件を定義するアクセス許可を付与します。リソースベースのポリシーはインラインポリシーです。IAM リソース のセクションでは、IAM ポリシーの種類とその使用方法について詳しく説明します。

この説明を簡単にするために、アカウントプリンシパルで運用するか、アカウントプリンシパルに適用することを主な目的とする IAM プリンシパル AWS のセキュリティサービスと機能を一覧表示します。IAM アクセス許可ポリシーの柔軟性と幅広い効果を認識しながら、そのシンプルさを維持します。ポリシー内の 1 つのステートメントは、複数のタイプの AWS エンティティに影響を与える可能性があります。たとえば、IAM アイデンティティベースのポリシーは IAM プリンシパルに関連付けられ、そのプリンシパルのアクセス許可 (許可、拒否) を定義しますが、ポリシーは指定されたアクション、リソース、および条件のアクセス許可も暗黙的に定義します。このようにして、アイデンティティベースのポリシーは、リソースのアクセス許可を定義する上で重要な要素になる可能性があります。

次の図は、プリンシパル AWS のセキュリティサービスと機能 AWS を示しています。アイデンティティベースのポリシーは、IAM ユーザー、グループ、ロールにアタッチされます。これらのポリシーを使用すると、そのアイデンティティが実行できる内容 (そのアクセス許可) を指定できます。IAM セッションポリシーは、ユーザーがロールを引き受けるときにセッションで渡す インラインアクセス許可ポリシー です。ポリシーを自分で渡すことも、ID がフェ デレーションされる AWSときにポリシーを挿入するように ID ブローカーを設定することもできます。これにより、複数のユーザーが同じロールを引き受けても一意のセッションアクセス許可を持つことができるため、管理者は作成する必要があるロールの数を減らすことができます。IAM Identity Center サービスは AWS Organizations および AWS API オペレーションと統合されており、 AWS アカウント で SSO アクセスとユーザーアクセス許可を管理するのに役立ちます AWS Organizations。



次の図表は、アカウントリソースに対するサービスと機能を示してます。リソースベースのポリシーをリソースにアタッチします。たとえば、リソースベースのポリシーを S3 バケット、Amazon Simple Queue Service (Amazon SQS) キュー、VPC エンドポイント、 AWS KMS 暗号化キーにアタッチできます。リソースベースのポリシーを使用して、リソースにアクセスできるユーザーとそのリソースに対して実行できるアクションを指定できます。S3 バケットポリシー、 AWS KMS キーポリシー、VPC エンドポイントポリシーは、リソースベースのポリシーのタイプです。IAM Access Analyzer は、外部エンティティと共有されている組織およびアカウント (S3 バケットや IAM ロールなど) 内のリソースを識別するのに役立ちます。これにより、セキュリティリスクであるリソースとデータへの意図しないアクセスを特定できます。 AWS Config は、 でサポートされている AWS リソースの設定を評価、監査、評価できるようにします AWS アカウント。 は AWS リソース設定 AWS Config を継続的にモニタリングおよび記録し、記録された設定を目的の設定と照合して自動的に評価します。


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

AWS セキュリティリファレンスアーキテクチャ

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は SRA AWS を示しています。このアーキテクチャ図は、すべての AWS セキュリティ関連サービスをまとめたものです。これは、単一ページに収まるシンプルな 3 層の Web アーキテクチャを中心に構築されています。このような作業負荷では、ウェブ層どのユーザーが接続して操作するかアプリケーション層である。これはアプリケーションの実際のビジネスロジックを処理する。ユーザーからの入力を受け取り、何らかの計算を行い、出力を生成する。アプリケーション層は、データ層。このアーキテクチャは意図的にモジュール化されており、多くの最新のウェブアプリケーションに高レベルの抽象化を提供します。

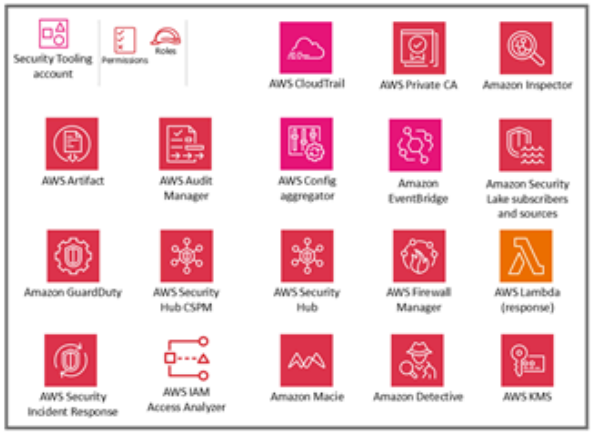
アーキテクチャ図

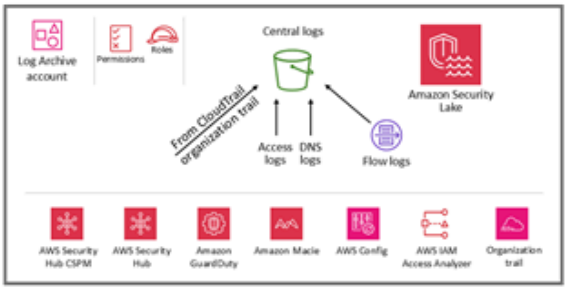
ビジネスニーズに基づいてこのガイドのリファレンスアーキテクチャ図をカスタマイズするには、次の .zip ファイルをダウンロードし、その内容を抽出します。

図のソースファイルをダウンロードする (Microsoft PowerPoint 形式)

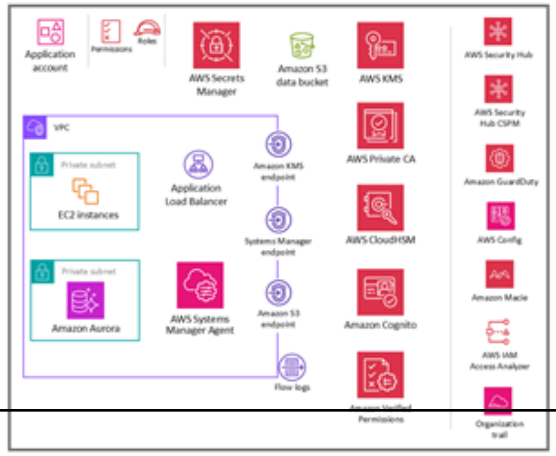
Organization

OU – Security

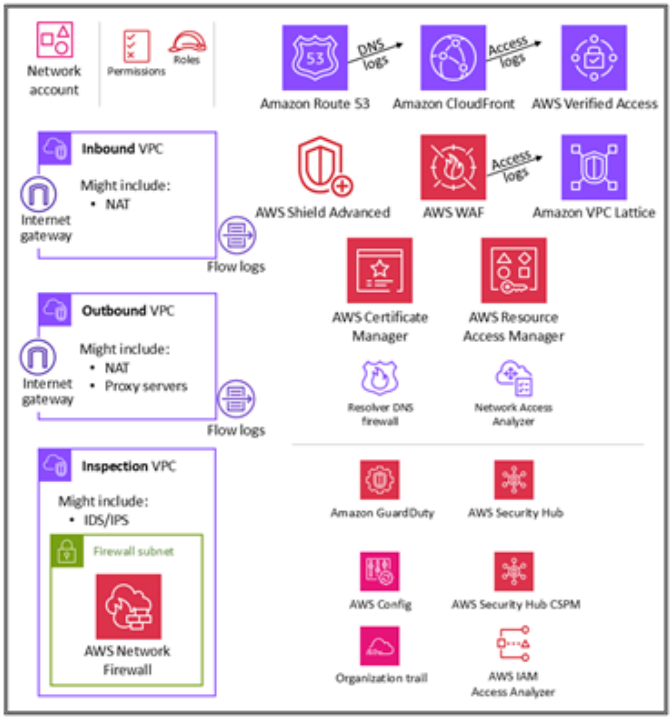


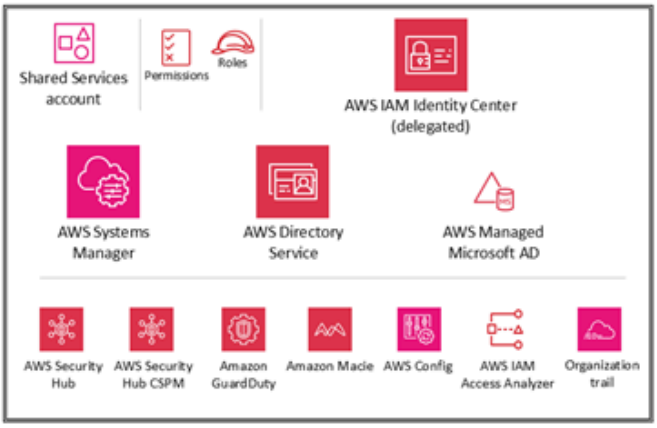


OU – Workloads



OU – Infrastructure





このリファレンスアーキテクチャでは、実際のウェブアプリケーションとデータ階層は、それぞれ Amazon EC2 インスタンスと Amazon Aurora データベースを介して、できるだけ単純に意図的に表されます。ほとんどのアーキテクチャ図は、Web、アプリケーション、およびデータ層に焦点を当てて深く掘り下げています。読みやすくするために、セキュリティコントロールを省略することがよくあります。この図は、可能な限りセキュリティを示すことを強調し、アプリケーション層とデータ層を必要なだけシンプルにして、セキュリティ機能を意味のあるものにします。

AWS SRA には、公開時に利用可能なすべての AWS セキュリティ関連サービスが含まれています。(ドキュメント履歴を参照) 。ただし、固有の脅威にさらされているワークロードや環境によっては、すべてのセキュリティサービスをデプロイする必要はありません。当社の目標は、これらのサービスがどのようにアーキテクチャ的に連携するかなど、さまざまなオプションに関するリファレンスを提供することです。これにより、ビジネスはリスクに基づいてインフラストラクチャ、ワークロード、セキュリティのニーズに最も適した意思決定を行うことができます。

以下のセクションでは、各 OU とアカウントについて説明し、その目的とそれに関連する個々の AWS セキュリティサービスを理解します。各要素 (通常は AWS のサービス) について、このドキュメントは次の情報を提供します。

- SRA AWS の 要素とそのセキュリティ目的の概要。個々のサービスに関する詳細な説明と技術情報については、付録を参照してください。
- サービスを最も効果的に有効化および管理するための推奨配置。これは、各アカウントおよび OU の個々のアーキテクチャ図に取り込まれます。
- 構成、管理、およびデータ共有は、他のセキュリティサービスへのリンクです。このサービスは、他のセキュリティサービスにどのように依存しているか、またはサポートしていますか。
- 設計上の考慮事項 まず、このドキュメントでは、セキュリティに重要な影響を与えるオプションの機能または設定について説明します。第 2 に、チームの経験に、通常は代替要件または制約の結果として行うレコメンデーションの一般的なバリエーションが含まれている場合、このドキュメントではそれらのオプションについて説明します。

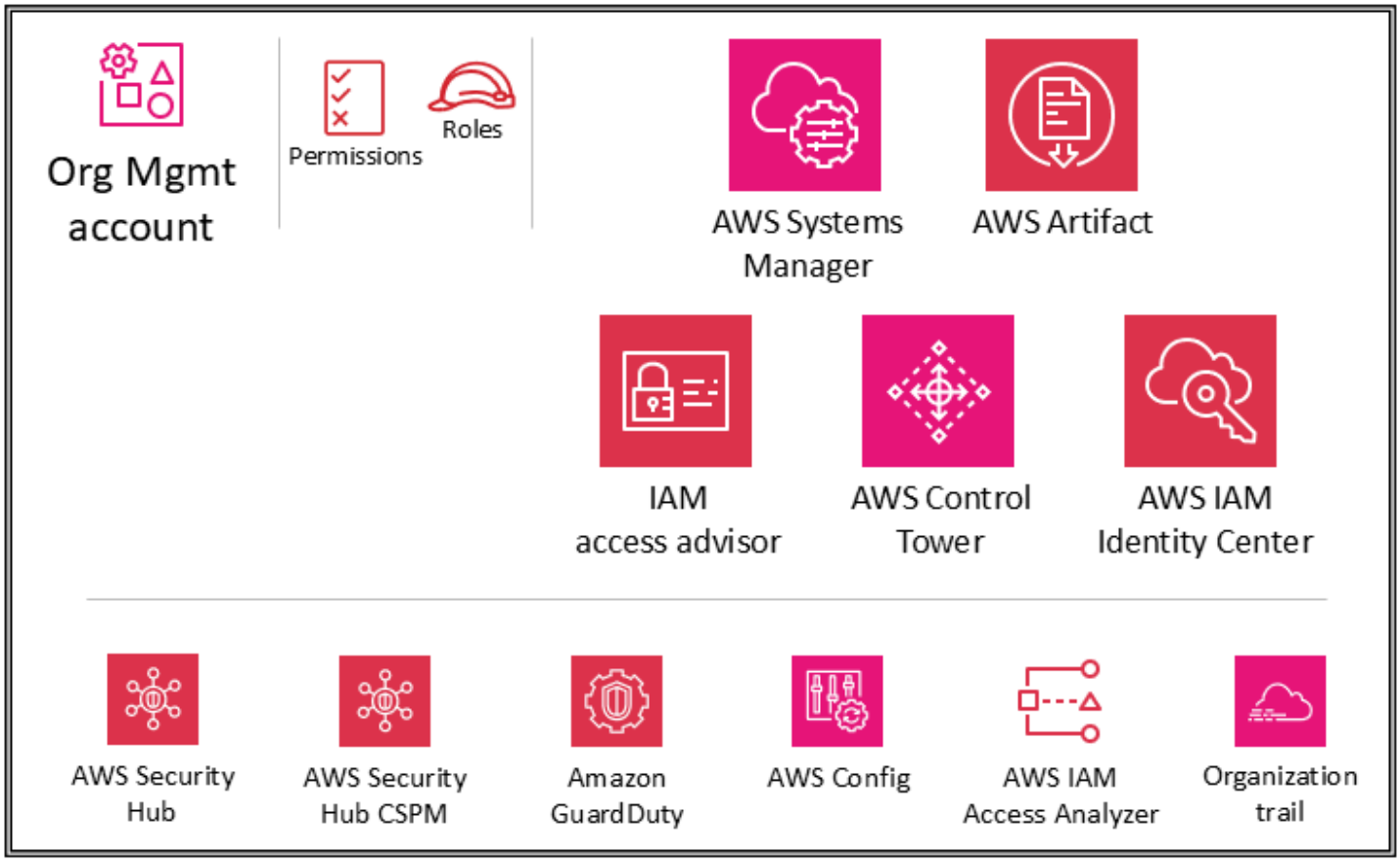
OU とアカウント

- 組織管理アカウント
- セキュリティ OU - Security Tooling アカウント
- セキュリティ OU — ログアーカイブアカウント
- インフラストラクチャ OU — ネットワークアカウント
- インフラストラクチャ OU - 共有サービスアカウント
- ワークロード OU — アプリケーションアカウント

組織管理アカウント

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は、組織管理アカウントで設定されている AWS セキュリティサービスを示しています。



このガイドの前半の「セキュリティ AWS Organizations のための の使用」セクションと「管理アカウント」、「信頼されたアクセス」、および「委任された管理者」セクションでは、組織管理アカウントの目的とセキュリティ目標を詳しく説明しました。組織管理アカウントのセキュリティのベストプラクティスに従います。これには、ビジネスによって管理される E メールアドレスの使用、正しい管理およびセキュリティ連絡先情報の維持 (アカウントの所有者に連絡する必要がある場合に AWS アカウントに電話番号をアタッチするなど) 、すべてのユーザーの多要素認証 (MFA) の有効化、組織管理アカウントにアクセスできるユーザーを定期的に確認することが含まれます。組織管理アカウントにデプロイされたサービスは、適切なロール、信頼ポリシー、およびその他のアクセス許可で構成して、それらのサービスの管理者 (組織管理アカウントでサービスにアクセスする必要があるユーザー) が他のサービスにも不適切にアクセスできないようにします。

サービスコントロールポリシー

を使用すると AWS Organizations、複数のポリシーを一元管理できます AWS アカウント。たとえば、組織のメンバー AWS アカウント である複数の に サービスコントロールポリシー (SCPs) を適用できます。SCPsを使用すると、組織のメンバーの IAM プリンシパル (IAM ユーザーやロールなど) が実行できる API と実行できない AWS のサービス APIs を定義できます AWS アカウント。SCPs は、組織の作成時に AWS アカウント 使用した である組織管理アカウントから作成および適用されます。SCPs「Using AWS Organizations for security」セクションを参照してください。

AWS Control Tower を使用して AWS 組織を管理する場合、一連の SCPs を予防ガードレールとしてデプロイします (必須、強く推奨、または選択的に分類) 。これらのガードレールは、組織全体のセキュリティコントロールを適用することで、リソースを管理するのに役立ちます。これらの SCPs、 の値が Managed-by-control-tower である aws-control-tower タグを自動的に使用します。managed-by-control-tower

> **設計上の考慮事項**
>
> SCPs、組織内のメンバーアカウントのみに影響します AWS 。これらは組織管理アカウントから適用されますが、そのアカウントのユーザーまたはロールには影響しません。SCP 評価ロジックの仕組みと推奨される構造の例については、 AWS ブログ記事「サービスコントロールポリシーの使用方法 AWS Organizations」を参照してください。

リソースコントロールポリシー

リソースコントロールポリシー (RCPsは、組織内のリソースに対して使用可能なアクセス許可の最大数を一元的に制御します。RCP は、アクセス許可ガードレールを定義するか、アイデンティティが組織内のリソースに対して実行できるアクションに制限を設定します。RCPs を使用して、リソースにアクセスできるユーザーを制限し、組織のメンバー でリソースにアクセスする方法に関する要件を適用できます AWS アカウント。RCP は個々のアカウント、OU、または組織のルートに直接アタッチできます。RCPs 「RCP 評価」を参照してください。 AWS Organizations RCPs「Using AWS Organizations for security」セクションを参照してください。

AWS Control Tower を使用して AWS 組織を管理する場合、一連の RCPs を予防ガードレールとしてデプロイします (必須、強く推奨、または選択的に分類) 。これらのガードレールは、組織全体のセキュリティコントロールを適用することで、リソースを管理するのに役立ちます。これらの SCPs、 の値を持つ`aws-control-tower`タグを自動的に使用します`managed-by-control-tower`。

設計上の考慮事項

- RCP は、組織内のメンバーアカウントのリソースのみに影響します。管理アカウントのリソースには影響しません。これは、RCP が委任管理者として指定されたメンバーアカウントに適用されることも意味します。
- RCPs、 のサブセットのリソースに適用されます AWS のサービス。詳細については、ドキュメント の「RCP AWS のサービス をサポートする のリスト RCPs」を参照してください。 AWS Organizations および AWS Lambda 関数 を使用して AWS Config ルール 、RCPs で現在サポートされていないリソースに対するセキュリティコントロールの適用をモニタリングおよび自動化できます。

宣言ポリシー

宣言ポリシーは、組織全体 AWS のサービス の大規模な特定の に必要な設定を一元的に宣言して適用するのに役立つ AWS Organizations 管理ポリシーの一種です。宣言ポリシーは現在、 Amazon EC2、 Amazon VPC、 Amazon EBS サービスをサポートしています。使用可能なサービス属性には、インスタンスメタデータサービスバージョン 2 (IMDSv2) の強制、EC2 シリアルコンソールを使用したトラブルシューティング、 Amazon マシンイメージ (AMI) 設定の許可、Amazon EBS スナップショット、Amazon EC2 AMIs、Amazon VPC リソースへのパブリックアクセスのブロックなどがあります。サポートされている最新のサービスと属性については、 AWS Organizations ドキュメントの「宣言ポリシー」を参照してください。

のベースライン設定を適用するには、 コンソール AWS Organizations と AWS Control Tower コンソールでいくつかの選択 AWS のサービス を行うか、 few AWS Command Line Interface (AWS CLI) コマンドと AWS SDK コマンドを使用します。宣言型ポリシーは、サービスのコントロールプレーンで適用されます。つまり、サービスが新機能や APIs を導入した場合、新しいアカウントが組織に追加された場合、または新しいプリンシパルやリソースが作成された場合でも、 のベースライン設定 AWS のサービス が常に維持されます。宣言ポリシーは、組織全体、または特定の OUs またはアカウントに適用できます。 有効なポリシー は、組織ルートと OUs から継承される一連のルールと、アカウントに直接アタッチされるポリシーです。 宣言ポリシーが デタッチされると、属性の状態は宣言ポリシーがアタッチされる前にその状態に戻ります。

宣言ポリシーを使用して、カスタムエラーメッセージを作成できます。たとえば、宣言ポリシーが原因で API オペレーションが失敗した場合、エラーメッセージを設定したり、内部 Wiki へのリンクや失敗を説明するメッセージへのリンクなどのカスタム URL を提供したりできます。これにより、ユーザーは問題を自分でトラブルシューティングできるように、より多くの情報を得ることができま

す。を使用して、宣言ポリシーの作成、宣言ポリシーの更新、宣言ポリシーの削除のプロセスを監査することもできます AWS CloudTrail。

宣言ポリシーはアカウントステータスレポートを提供します。これにより、 対象範囲内のアカウントの宣言ポリシーでサポートされているすべての属性の現在のステータスを確認できます。レポートスコープに含めるアカウントと OUs を選択するか、ルートを選択して組織全体を選択できます。このレポートは、属性の現在の状態が アカウント間で統一 されている (値を使用 `numberOfMatchedAccounts`) か、アカウント間で 一貫性がない (値を使用 `numberOfUnmatchedAccounts`) か AWS リージョン を指定して内訳を提供することで、準備状況を評価するのに役立ちます。

> **設計上の考慮事項**
>
> 宣言ポリシーを使用してサービス属性を設定すると、ポリシーが複数の APIs に影響を与える可能性があります。非準拠のアクションはすべて失敗します。アカウント管理者は、個々のアカウントレベルでサービス属性の値を変更することはできません。

一元化されたルートアクセス

のすべてのメンバーアカウント AWS Organizations には独自のルートユーザーがあります。これは、そのメンバーアカウントのすべての AWS のサービス およびリソースへの完全なアクセス権を持つ ID です。IAM は、すべてのメンバーアカウントのルートアクセスを管理するための一元化されたルートアクセス管理を提供します。これにより、メンバールートユーザーの使用が防止され、大規模な復旧が可能になります。一元化されたルートアクセス機能には、ルート認証情報管理 と ルートセッションの 2 つの重要な機能があります。

- ルート認証情報管理機能は、一元管理を可能にし、すべての管理アカウントでルートユーザーを保護するのに役立ちます。この機能には、長期的なルート認証情報の削除、メンバーアカウントによるルート認証情報の復旧の防止、デフォルトでルート認証情報を使用しない新しいメンバーアカウントのプロビジョニングが含まれます。また、コンプライアンスを示す簡単な方法も提供します。ルートユーザー管理が一元化されると、ルートユーザーのパスワード、アクセスキー、署名証明書を削除し、すべてのメンバーアカウントから多要素認証 (MFA) を非アクティブ化できます。
- ルートセッション機能を使用すると、組織管理アカウントまたは委任管理者アカウントのメンバーアカウントで短期認証情報を使用して、特権ルートユーザーアクションを実行できます。この機能は、最小特権の原則に従って、特定のアクションを対象とする短期ルートアクセスを有効にするのに役立ちます。

一元化されたルート認証情報管理を行うには、組織管理アカウントまたは委任された管理者アカウントから、組織レベルでルート認証情報管理とルートセッション機能を有効にする必要があります。SRA AWS のベストプラクティスに従って、この機能を Security Tooling アカウントに委任します。一元化されたルートユーザーアクセスの設定と使用の詳細については、 AWS セキュリティブログ記事「 を使用するお客様のルートアクセスを一元管理する AWS Organizations」を参照してください。

IAM アイデンティティセンター

AWS IAM アイデンティティセンター は、すべての 、プリンシパル AWS アカウント、クラウドワークロードへの SSO アクセスを一元管理するのに役立つ ID フェデレーションサービスです。IAM Identity Center は、一般的に使用されるサードパーティーの Software as a Service (SaaS) アプリケーションへのアクセスとアクセス許可の管理にも役立ちます。ID プロバイダーは、SAML 2.0 を使用して IAM アイデンティティセンターと統合します。一括プロビジョニングとjust-in-timeプロビジョニングは、クロスドメイン ID 管理システム (SCIM) を使用して実行できます。IAM Identity Center は、 を使用して、ID プロバイダーとしてオンプレミスまたは AWSマネージド Microsoft Active Directory (AD) ドメインと統合することもできます AWS Directory Service。IAM Identity Center には、エンドユーザーが割り当てられた AWS アカウント IAM Identity Center、ロール、クラウドアプリケーション、カスタムアプリケーションを 1 か所で検索してアクセスできるユーザーポータルが含まれています。

IAM Identity Center は、デフォルトで とネイティブに統合 AWS Organizations され、組織管理アカウントで実行されます。ただし、最小特権を行使し、管理アカウントへのアクセスを厳密に制御するために、IAM Identity Center の管理を特定のメンバーアカウントに委任できます。 AWS SRA では、共有サービスアカウントは IAM Identity Center の委任管理者アカウントです。IAM Identity Center の委任管理を有効にする前に、以下の考慮事項を確認してください。委任の詳細については、「共有サービスアカウント」セクションを参照してください。委任を有効にした後でも、IAM Identity Center は組織管理アカウントで実行して、組織管理アカウントでプロビジョニングされたアクセス許可セットの管理など、特定の IAM Identity Center 関連のタスクを実行する必要があります。

IAM Identity Center コンソール内では、アカウントはカプセル化 OU によって表示されます。これにより、 をすばやく検出し AWS アカウント、一般的なアクセス許可のセットを適用し、一元的な場所からのアクセスを管理できます。

IAM Identity Center には、特定のユーザー情報を保存する必要がある ID ストアが含まれています。ただし、IAM Identity Center がワークフォース情報の信頼できるソースである必要はありません。エンタープライズにすでに信頼できるソースがある場合、IAM Identity Center は次のタイプの ID プロバイダー (IdPsをサポートしています。

- IAM Identity Center アイデンティティストア – 次の 2 つのオプションが利用できない場合は、このオプションを選択します。ユーザーが作成され、グループの割り当てが行われ、アクセス許可が ID ストアに割り当てられます。信頼できるソースが IAM Identity Center の外部にある場合でも、プリンシパル属性のコピーは ID ストアに保存されます。
- Microsoft Active Directory (AD) – のディレクトリ AWS Directory Service for Microsoft Active Directory または Active Directory のセルフマネージドディレクトリのいずれかでユーザーの管理を継続する場合は、このオプションを選択します。
- 外部 ID プロバイダー – 外部のサードパーティーの SAML ベースの IdP でユーザーを管理する場合は、このオプションを選択します。

エンタープライズ内で既に導入されている既存の IdP を使用できます。これにより、アクセスの作成、管理、および取り消しを 1 箇所で行うことができるため、複数のアプリケーションおよびサービス間のアクセス管理を簡単に行うことができます。たとえば、誰かがチームを離れた場合、1 つの場所からすべてのアプリケーションとサービス (を含む AWS アカウント) へのアクセスを取り消すことができます。これにより、複数の認証情報の必要性が軽減され、人事 (HR) プロセスと統合する機会が得られます。

> **設計上の考慮事項**
>
> そのオプションがエンタープライズで利用可能な場合は、外部 IdP を使用します。IdP がクロスドメインアイデンティティ管理 (SCIM) のシステムをサポートしている場合は、IAM アイデンティティセンターの SCIM 機能を活用して、ユーザー、グループ、アクセス許可のプロビジョニング (同期) を自動化します。これにより、新規採用者、別のチームに移行する従業員、および退職する従業員の社内ワークフローと連携した AWS アクセスが可能になります。いつでも、1 つのディレクトリまたは 1 つの SAML 2.0 ID プロバイダーのみを IAM アイデンティティセンターに接続できます。ただし、別の ID プロバイダーに切り替えることはできます。

IAM アクセスアドバイザー

IAM アクセスアドバイザーは、 AWS アカウント および OUs のサービスの最終アクセス時間情報の形式でトレーサビリティデータを提供します。この検出制御を使用して、最小特権戦略 に貢献します。IAM プリンシパルの場合、許可された情報と許可されたアクション AWS のサービス 情報の 2 種類の最終アクセス情報を表示できます。情報には、試行が行われた日時が含まれます。

組織管理アカウント内の IAM アクセスを使用すると、組織管理アカウント、OU、メンバーアカウント、または AWS IAM ポリシーのサービスの最終アクセス時間データを表示できます。この情報は、管理アカウント内の IAM コンソールで利用でき、 の IAM アクセスアドバイザー APIs AWS CLI またはプログラムクライアントを使用してプログラムで取得することもできます。この情報は、組織またはアカウント内のどのプリンシパルが最後にサービスにアクセスしようとしたかを示しています。最終アクセスの情報は、実際のサービス利用状況を把握できるため (シナリオ例 を参照)、実際に利用されているサービスのみに IAM アクセス許可を消去することが可能です。

AWS Systems Manager

高速セットアップと Explorer は、 の機能でありAWS Systems Manager、組織管理アカウントからのサポート AWS Organizations と運用の両方を行います。

クイックセットアップ は、Systems Manager の自動化機能です。これにより、組織管理アカウントは、Systems Manager が AWS 組織内のアカウント間でユーザーに代わってやり取りするための設定を簡単に定義できます。 AWS 組織全体でクイックセットアップを有効にするか、特定の OU を選択することができます。高速セットアップでは、 AWS Systems Manager エージェント (SSM エージェント) が EC2 インスタンスで隔週更新を実行するようにスケジュールし、それらのインスタンスの毎日のスキャンを設定して、欠落しているパッチを特定できます。

Explorer は、 AWS リソースに関する情報をレポートするカスタマイズ可能なオペレーションダッシュボードです。Explorer は、 AWS アカウントおよび全体のオペレーションデータの集約ビューを表示します AWS リージョン。これには、EC2 インスタンスに関するデータやパッチコンプライアンスの詳細が含まれます 内で統合セットアップ (Systems Manager OpsCenter も含む) を完了すると AWS Organizations、OU または AWS 組織全体のデータを Explorer に集約できます。Systems Manager は、Explorer に表示する前に、データを AWS 組織管理アカウントに集約します。

このガイドの後半の「ワークロード OU」セクションでは、アプリケーションアカウントの EC2 インスタンスでの SSM エージェントの使用について説明します。

AWS Control Tower

AWS Control Tower 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 環境をセットアップして管理するための簡単な方法を提供します。 は、 を使用してランディングゾーン AWS Control Tower を作成し AWS Organizations、継続的なアカウント管理とガバナンス、実装のベストプラクティスを提供します。 AWS Control Tower を使用して、アカウントが組織ポリシーに準拠していることを確認しながら、いくつかのステップで新しいアカウントをプロビジョニングできます。既存のアカウントを新しい AWS Control Tower 環境に追加することもできます。

AWS Control Tower には、広範で柔軟な一連の機能があります。主な機能はAWS のサービス、 や IAM Identity Center など AWS Organizations AWS Service Catalog、他のいくつかの の機能を調整してランディングゾーンを構築する機能です。例えば、 はデフォルトで AWS CloudFormation を使用してベースラインを確立し、 AWS Organizations サービスコントロールポリシー (SCPs) AWS Control Tower を使用して設定変更を防止し、 AWS Config ルール ルールを使用して非準拠を継続的に検出します。 は、マルチアカウント AWS 環境を AWS Well Architected セキュリティ基盤の設計原則とすばやく一致させるのに役立つ設計図 AWS Control Tower を採用しています。ガバナンス機能の中で、 AWS Control Tower には、選択したポリシーに準拠しないリソースのデプロイを防ぐガードレールが用意されています。

を使用して SRA AWS ガイダンスの実装を開始できます AWS Control Tower。たとえば、 は推奨されるマルチアカウントアーキテクチャを使用して AWS 組織 AWS Control Tower を確立します。ID 管理の提供、アカウントへのフェデレーティッドアクセスの提供、ログ記録の一元化、クロスアカウントセキュリティ監査の確立、新しいアカウントのプロビジョニングワークフローの定義、ネットワーク設定によるアカウントベースラインの実装を行うための設計図を提供します。

AWS SRA では、 AWS Control Tower は組織管理アカウント内にあります。 はこのアカウント AWS Control Tower を使用して AWS 組織を自動的にセットアップし、そのアカウントを管理アカウントとして指定するためです。このアカウントは、 AWS 組織全体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、OUs の管理、ガードレールの管理にも使用されます。既存の AWS 組織 AWS Control Tower で を起動する場合は、既存の管理アカウントを使用できます。 AWS Control Tower はそのアカウントを指定された管理アカウントとして使用します。

> **設計上の考慮事項**
>
> アカウント全体でコントロールと設定の追加のベースラインを作成する場合は、 AWS Control Tower (CfCT) のカスタマイズを使用できます。CfCT では、 CloudFormation テンプレートと SCPs を使用して AWS Control Tower ランディングゾーンをカスタマイズできます。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 OUs にデプロイできます。CfCT は AWS Control Tower ライフサイクルイベントと統合して、リソースデプロイがランディングゾーンと同期していることを確認します。

AWS Artifact

AWS Artifact は、 AWS セキュリティおよびコンプライアンスレポートへのオンデマンドアクセスと、一部のオンライン契約を提供します。で利用可能なレポート AWS Artifact には、System and Organization Controls (SOC) レポート、Payment Card Industry (PCI) レポート、および AWS セキュ

リティコントロールの実装と運用の有効性を検証する地域やコンプライアンス分野の認定機関からの証明書が含まれます。 AWS Artifact は、セキュリティコントロール環境への透明性を強化 AWS して のデューデリジェンスを実行するのに役立ちます。また、新しいレポートにすぐにアクセスできる AWS のセキュリティとコンプライアンスを継続的にモニタリングすることもできます。

AWS Artifact 契約を使用すると、個々のアカウントと組織の一部であるアカウントの事業提携契約 (BAA) などの契約のステータス AWS を確認、承諾、追跡できます AWS Organizations。

AWS セキュリティコントロールの証拠として、 AWS 監査アーティファクトを監査人または規制当局に提供できます。また、監査 AWS アーティファクトの一部が提供する責任ガイダンスを使用して、クラウドアーキテクチャを設計することもできます。このガイダンスは、システムの特定のユースケースをサポートするために導入できる追加のセキュリティコントロールを決定するのに役立ちます。

AWS Artifact は組織管理アカウントでホストされ、契約を確認、受諾、管理できる一元的な場所を提供します AWS。これは、管理アカウントで承諾された契約がメンバーアカウントに流れるためです。

> **設計上の考慮事項**
>
> 組織管理アカウント内のユーザーは、 の契約機能のみを使用するように制限 AWS Artifact する必要があります。職務分離を実装するために、 AWS Artifact は Security Tooling アカウントでもホストされます。このアカウントでは、監査アーティファクトにアクセスするためのアクセス許可をコンプライアンス関係者と外部監査人に委任できます。きめ細かな IAM アクセス許可ポリシーを定義することで、この分離を実装できます。例については、 AWS ドキュメントの「IAM ポリシーの例」を参照してください。

分散型および一元化されたセキュリティサービスガードレール

AWS SRA では、 AWS Security Hub、 AWS Security Hub CSPM、Amazon GuardDuty、 AWS Config、IAM Access Analyzer、 AWS CloudTrail 組織の証跡、および多くの場合 Amazon Macie は、アカウント間で適切な委任ガードレールのセットでデプロイされ、 AWS 組織全体で一元的なモニタリング、管理、ガバナンスを提供します。このサービスのグループは、SRA AWS で表されるすべてのタイプのアカウントにあります。これらは の一部 AWS のサービス であり、アカウントのオンボーディングおよびベースライン作成プロセスの一環としてプロビジョニングする必要があります。GitHub コードリポジトリは、 AWS 組織管理アカウントを含むアカウント全体のセキュリティに焦点を当てたサービスの実装 AWS 例を提供します。

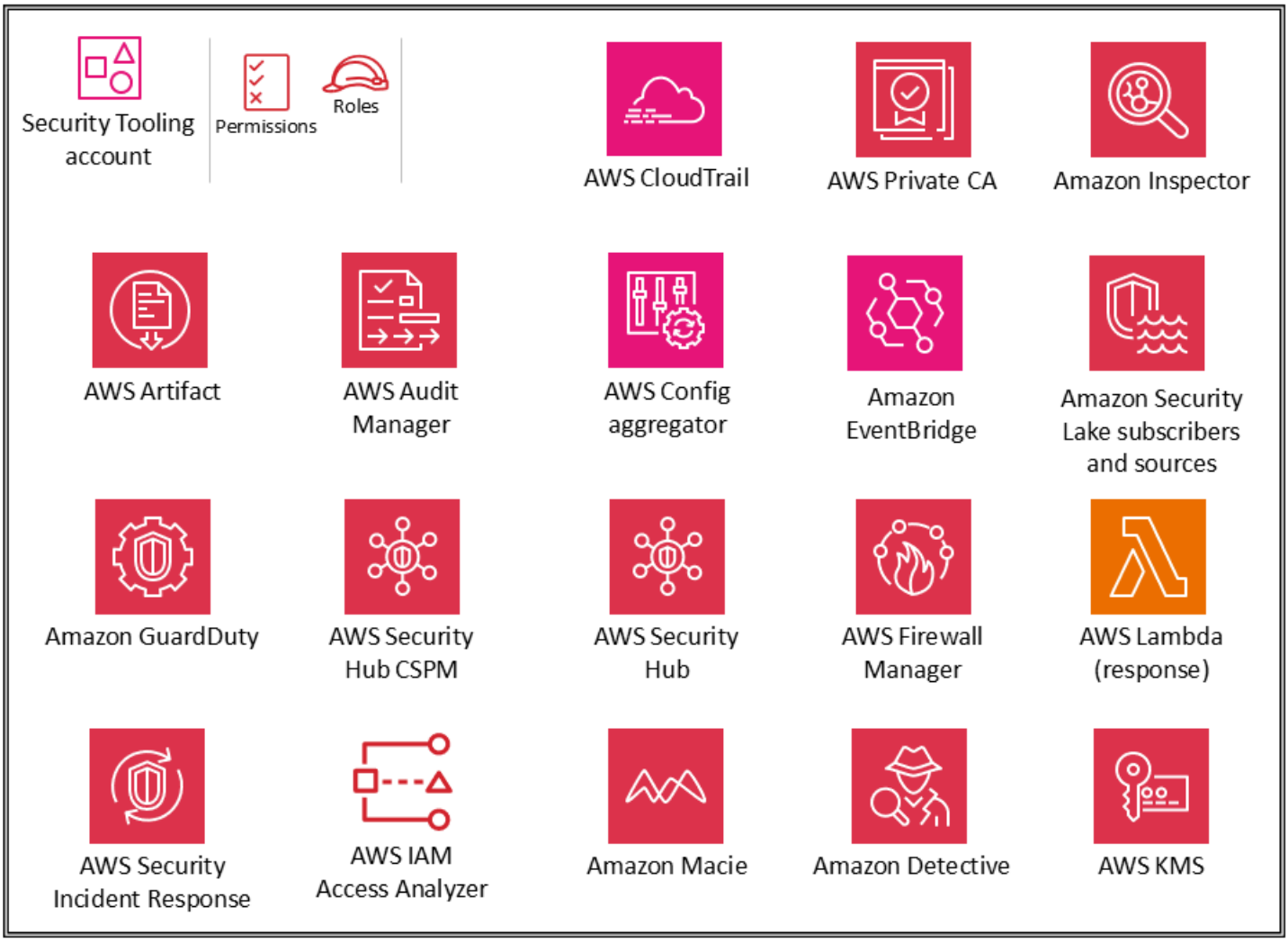
これらのサービスに加えて、 AWS SRA には Amazon Detective と の 2 つのセキュリティに焦点を当てたサービスが含まれており AWS Audit Manager、 の統合と委任された管理者機能をサポートしています AWS Organizations。ただし、アカウントベースライン作成の推奨サービスには含まれていません。これらのサービスは、以下のシナリオで最適に使用されています。

- デジタルフォレンジックおよび IT 監査機能を実行する専任のチームまたはリソースグループがある。Detective はセキュリティアナリストチームが最適に活用でき、Audit Manager は内部監査またはコンプライアンスチームに役立ちます。
- プロジェクトの AWS Security Hub CSPM 開始時に AWS Config、Amazon GuardDuty AWS Security Hubや などのツールのコアセットに重点を置き、追加の機能を提供する サービスを使用してこれらを構築したいと考えています。

セキュリティ OU - Security Tooling アカウント

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は、 AWS Security Tooling アカウントで設定されているセキュリティサービスを示しています。



Security Tooling アカウントは、セキュリティサービスの運用、 のモニタリング AWS アカウント、セキュリティアラートとレスポンスの自動化に専念しています。セキュリティの目的は以下の通りです。

- セキュリティガードレール、モニタリング、および対応へのアクセスを管理するための制御されたアクセスを専用アカウントに提供します。
- セキュリティオペレーションデータをモニタリングし、トレーサビリティを維持するために、適切な一元化されたセキュリティインフラストラクチャを維持します。検出、調査、対応は、セキュリティライフサイクルの重要な部分であり、品質プロセス、法的義務またはコンプライアンス義務をサポートし、脅威の特定と対応の取り組みに使用することができます。
- 暗号化キーやセキュリティグループ設定などの適切なセキュリティ設定とオペレーションを別のレイヤーで管理することで、defense-in-depthの組織戦略をさらにサポートします。セキュリティオペレーターが作業するアカウントです。 AWS 組織全体の情報を表示するための読み取り専用/監

査ロールが一般的ですが、書き込み/変更ロールの数は制限され、厳密に制御、モニタリング、ログ記録されます。

設計上の考慮事項

- AWS Control Tower は、デフォルトでセキュリティ OU の下のアカウントを監査アカウントとして指定します。アカウントの名前は、 AWS Control Tower セットアップ中に変更できます。
- セキュリティツールアカウントを複数持つのが適切かもしれません。例えば、セキュリティイベントのモニタリングと対応は、多くの場合、専用のチームに割り当てられています。ネットワークセキュリティは、クラウドインフラストラクチャやネットワークチームと協力して、独自のアカウントとロールを保証する場合があります。このような分割は、一元化されたセキュリティエンクレーブを分離するという目的を保持し、職務の分離、最小特権、およびチーム割り当ての単純化の可能性をさらに強調するものです。を使用している場合 AWS Control Tower、セキュリティ OU AWS アカウント での追加の作成が制限されます。

セキュリティサービスの委任管理者

Security Tooling アカウントは、 全体で管理者/メンバー構造で管理されるセキュリティサービスの管理者アカウントとして機能します AWS アカウント。前述のように、これは AWS Organizations 委任管理者機能を通じて処理されます。現在委任管理者をサポートしている AWS SRA 内のサービスには、ルートアクセスの IAM 一元管理 AWS Config、 AWS Firewall Manager、Amazon GuardDuty、IAM Access Analyzer、Amazon Macie、 AWS Security Hub、 AWS Security Hub CSPM Amazon Detective、 AWS Audit Manager Amazon Inspector AWS CloudTrail、および が含まれます AWS Systems Manager。セキュリティチームがこれらのサービスのセキュリティ機能を管理し、セキュリティ固有のイベントや検出結果をモニタリングします。

AWS IAM アイデンティティセンター は、メンバーアカウントへの委任管理をサポートします。AWS SRA は、共有サービスアカウントの IAM アイデンティティセンターセクションで後述するように、IAM アイデンティティセンターの委任管理者アカウントとして共有サービスアカウントを使用します。

一元化されたルートアクセス

Security Tooling アカウント は、ルートアクセス機能の IAM 集中管理のための委任管理者アカウントです。 この機能は、メンバーアカウントで認証情報管理と特権ルートアクションを有効にすることで、組織レベルで有効にする必要があります。委任された管理者は、メンバーアカウントに代わって特権ルートアクションを実行できるようにするには、明示的に`sts:AssumeRoot`アクセス許可を付与されている必要があります。このアクセス許可は、組織管理アカウントまたは委任管理者アカウントでメンバーアカウントの特権ルートアクションが有効になっている場合にのみ使用できます。このアクセス許可により、ユーザーは Security Tooling アカウントから一元的にメンバーアカウントで特権ルートユーザータスクを実行できます。特権セッションを起動したら、誤って設定された S3 バケットポリシーの削除、誤って設定された SQS キューポリシーの削除、メンバーアカウントのルートユーザー認証情報の削除、メンバーアカウントのルートユーザー認証情報の再有効化を行うことができます。これらのアクションは、 コンソール、 AWS Command Line Interface (AWS CLI)、または APIs を使用して実行できます。

AWS CloudTrail

AWS CloudTrail は、 でのアクティビティのガバナンス、コンプライアンス、監査をサポートするサービスです AWS アカウント。CloudTrail を使用すると、 AWS インフラストラクチャ全体のアクションに関連するアカウントアクティビティをログに記録し、継続的にモニタリングし、保持できます。CloudTrail は と統合されており AWS Organizations、その統合を使用して、組織内のすべての AWS アカウントのすべてのイベントをログに記録する単一の証跡を作成できます。これは、組織の証跡と呼ばれます。組織の証跡を作成および管理できるのは、組織の管理アカウント内または委任管理者アカウントのみです。組織の証跡を作成すると、指定した名前の証跡が AWS 、組織 AWS アカウント に属するすべての に作成されます。証跡は、 AWS 組織内の管理アカウントを含むすべてのアカウントのアクティビティをログに記録し、ログを 1 つの S3 バケットに保存します。この S3 バケットは機密性が高いため、このガイドの後半にある中央ログストアセクションとして Amazon S3 で説明されているベストプラクティスに従って保護する必要があります。 AWS 組織内のすべてのアカウントは、証跡のリストに組織の証跡を表示できます。ただし、メンバーにはこの証跡への表示のみのアクセス権 AWS アカウント があります。デフォルトでは、CloudTrail コンソールで組織の証跡を作成すると、証跡はマルチリージョン証跡になります。その他のセキュリティのベストプラクティスについては、CloudTrail ドキュメントを参照してください。

AWS SRA では、セキュリティツールアカウントは CloudTrail を管理するための委任管理者アカウントです。組織の証跡ログを保存する対応する S3 バケットは、ログアーカイブアカウントに作成されます。これは、CloudTrail ログ権限の管理と使用を分離するためです。S3 バケットを作成または更新して組織の証跡のログファイルを保存する方法については、CloudTrail ドキュメントを参照してください。セキュリティのベストプラクティスとして、組織の証跡の条件キーを S3 バケットのリソー

スポリシー (および KMS キーや SNS トピックなどの他のリソース) に追加 `aws:SourceArn` します。これにより、S3 バケットは特定の証跡に関連付けられているデータのみを受け入れるようになります。証跡は、ログファイルの整合性検証用のログファイル検証で設定されます。ログファイルとダイジェストファイルは、SSE-KMS を使用して暗号化されます。組織の証跡は CloudWatch Logs のロググループとも統合され、長期保持のためにイベントを送信します。

> **Note**
>
> 組織の証跡は、管理アカウントと委任管理者アカウントの両方から作成および管理できます。ただし、ベストプラクティスとして、管理アカウントへのアクセスを制限し、利用可能な場合は委任管理者機能を使用する必要があります。

> **設計上の考慮事項**
>
> - CloudTrail は、多くの場合、大量のアクティビティであるため、デフォルトではデータイベントを記録しません。ただし、S3 バケット、Lambda 関数、CloudTrail レイクに AWS 送信される外部からのログイベント、SNS トピックなど、特定の重要な AWS リソースのデータイベントをキャプチャする必要があります。これを行うには、個々のリソースの ARNs を指定して、特定のリソースからのデータイベントを含めるように組織の証跡を設定します。
> - メンバーアカウントが独自のアカウントの CloudTrail ログファイルにアクセスする必要がある場合は、中央の S3 バケットから組織の CloudTrail ログファイル[を選択的に共有]できます。ただし、メンバーアカウントがアカウントの CloudTrail ログにローカル Amazon CloudWatch ロググループを必要とする場合、またはログ管理イベントとデータイベント (読み取り専用、書き込み専用、管理イベント、データイベント) を組織の証跡とは異なる方法で設定する場合は、適切なコントロールを使用してローカル証跡を作成できます。ローカルアカウント固有の証跡には[追加料金]が発生します。

AWS Security Hub CSPM

[AWS Security Hub クラウドセキュリティ体制管理] (AWS Security Hub CSPM) は、以前は と呼ばれていましたが AWS Security Hub、 のセキュリティ体制を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスに照らして環境をチェックするのに役立ちます。Security Hub CSPM は、 AWS 統合サービス、サポートされているサードパーティー製品、および使用する可能性のあるその他のカスタムセキュリティ製品全体からセキュリティデータを収集します。セキュリティの傾

向を継続的にモニタリング・分析し、特に優先度の高いセキュリティ問題を特定するのに役立ちます。取り込まれたソースに加えて、Security Hub CSPM は独自の検出結果を生成します。これは、1 つ以上のセキュリティ標準にマッピングされるセキュリティコントロールによって表されます。これらの標準には、 AWS Foundational Security Best Practices (FSBP)、Center for Internet Security (CIS) AWS Foundations Benchmark v1.20 and v1.4.0、米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5、Payment Card Industry Data Security Standard (PCI DSS)、およびサービスマネージド標準が含まれます。現在のセキュリティ標準のリストと特定のセキュリティコントロールの詳細については、Security Hub CSPM ドキュメントの「Security Hub CSPM の標準リファレンス」を参照してください。

Security Hub CSPM は と統合 AWS Organizations され、 AWS 組織内のすべての既存アカウントと将来のアカウントにおけるセキュリティ体制の管理を簡素化します。委任管理者アカウント (この場合は Security Tooling) の Security Hub CSPM 中央設定機能を使用して、複数のリージョンにわたる組織アカウントと組織単位 (OUs) で Security Hub CSPM サービス、セキュリティ標準、およびセキュリティコントロールを設定する方法を指定できます。 これらの設定は、 ホームリージョンと呼ばれる 1 つのプライマリリージョンから数ステップで設定できます。中央設定を使用しない場合は、アカウントとリージョンごとに Security Hub CSPM を個別に設定する必要があります。委任管理者は、アカウントと OUs を自己管理型として指定できます。この場合、メンバーは各リージョンで個別に設定するか、 一元管理型として指定し、委任管理者はリージョン間でメンバーアカウントまたは OU を設定できます。組織内のすべてのアカウントと OU を、一元管理型、すべてセルフマネージド型、または両方の組み合わせとして指定できます。これにより、一貫した設定の適用が簡素化され、OU とアカウントごとに変更する柔軟性が提供されます。

Security Hub CSPM 委任管理者アカウントは、すべてのメンバーアカウントの結果の表示、インサイトの表示、詳細の制御を行うこともできます。さらに、委任管理者アカウント内で集約リージョンを指定して、アカウントとリンクされたリージョン間で検出結果を一元化することもできます。検出結果は、アグリゲータリージョンと他のすべてのリージョンの間で継続的かつ双方向に同期されます。

Security Hub CSPM は、複数の との統合をサポートしています AWS のサービス。Amazon GuardDuty、 AWS Config、Amazon Macie、IAM Access Analyzer、 AWS Firewall Manager Amazon Inspector、 Amazon Route 53 Resolver DNS Firewall、および AWS Systems Manager Patch Manager は、検出結果を Security Hub CSPM にフィードできます。Security Hub CSPM は、AWS Security Finding Format (ASFF) と呼ばれる標準形式を使用して検出結果を処理します。Security Hub CSPM は、統合された製品間で検出結果を関連付けて、最も重要な検出結果を優先します。Security Hub CSPM の検出結果のメタデータを強化して、セキュリティの検出結果のコンテキスト化、優先順位付け、およびアクションの実行を強化できます。このエンリッチメントにより、Security Hub CSPM に取り込まれるすべての検出結果に、リソースタグ、新しい AWS アプリ

ケーションタグ、およびアカウント名情報が追加されます。これにより、自動化ルールの検出結果の微調整、検出結果とインサイトの検索またはフィルタリング、アプリケーション別のセキュリティ体制のステータスの評価を行うことができます。さらに、自動化ルールを使用して検出結果を自動的に更新できます。Security Hub CSPM が検出結果を取り込むと、検出結果の抑制、重要度の変更、検出結果へのメモの追加など、さまざまなルールアクションを適用できます。これらのルールアクションは、結果が関連付けられているリソース ID やアカウント IDs、そのタイトルなど、結果が指定された基準と一致する場合に有効になります。自動化ルールを使用して、ASFF の選択結果フィールドを更新できます。ルールは、新しい検出結果と更新された検出結果の両方に適用されます。

セキュリティイベントの調査中に、Security Hub CSPM から Amazon Detective に移動して GuardDuty の検出結果を調査できます。Security Hub CSPM では、統合をスムーズにするために、Detective (存在する場合) などのサービスの委任管理者アカウントを調整することをお勧めします。たとえば、Detective と Security Hub CSPM の間で管理者アカウントを調整しない場合、検出結果から Detective に移動することはできません。包括的なリストについては、Security Hub CSPM ドキュメントの「Security Hub CSPM と AWS のサービス の統合の概要」を参照してください。

Amazon VPC の Network Access Analyzer 機能で Security Hub CSPM を使用すると、 AWS ネットワーク設定のコンプライアンスを継続的にモニタリングできます。これにより、不要なネットワークアクセスをブロックし、重要なリソースの外部アクセスを防ぐことができます。アーキテクチャと実装の詳細については、ブログ記事 AWS 「Amazon VPC Network Access Analyzer と を使用したネットワークコンプライアンスの継続的な検証 AWS Security Hub CSPM」を参照してください。

Security Hub CSPM は、モニタリング機能に加えて、Amazon EventBridge との統合をサポートし、特定の検出結果の修復を自動化します。結果を受け取ったときに実行するカスタムアクションを定義できます。たとえば、チケット発行システムや自動修復システムに検出結果を送信するなどのカスタムアクションを設定できます。その他の議論と例については、 AWS ブログ記事「 による自動応答と修復 AWS Security Hub CSPM」および「Security Hub CSPM 自動応答と修復の AWS ソリューションをデプロイする方法」を参照してください。

Security Hub CSPM は、サービスにリンクされた AWS Config ルール を使用して、コントロールのセキュリティチェックのほとんどを実行します。これらのコントロールをサポートするには、Security Hub CSPM AWS Config が有効になっている各アカウントで、管理者 (または委任管理者) アカウントとメンバーアカウントを含むすべてのアカウントで を有効にする必要があります。
AWS リージョン

設計上の考慮事項

- PCI-DSS などのコンプライアンス標準が Security Hub CSPM にすでに存在する場合、フルマネージド型の Security Hub CSPM サービスが最も簡単に運用できます。ただし、セキュリティ、運用、コスト最適化チェックなど、独自のコンプライアンスまたはセキュリティ標準をアセンブルする場合、 AWS Config コンフォーマンスパックは簡素化されたカスタマイズプロセスを提供します。(AWS Config および コンフォーマンスパックの詳細については、AWS Config「」セクションを参照してください)。
- Security Hub CSPM の一般的なユースケースは次のとおりです。
  - アプリケーション所有者がリソースのセキュリティとコンプライアンス体制 AWS を可視化するダッシュボードとして
  - セキュリティオペレーション、インシデント対応担当者、脅威ハンターが使用するセキュリティ検出結果の一元的なビューとして、 AWS アカウント および リージョン全体の AWS セキュリティおよびコンプライアンスの検出結果をトリアージしてアクションを実行します。
  - セキュリティとコンプライアンスの検出結果を AWS アカウント および リージョン間で集約し、一元化されたセキュリティ情報とイベント管理 (SIEM) またはその他のセキュリティオーケストレーションシステムにルーティングするには

  セットアップ方法など、これらのユースケースに関する追加のガイダンスについては、ブログ記事「3 つの定期的な Security Hub CSPM の使用パターンとデプロイ方法」を参照してください。

実装例

AWS SRA コードライブラリは、Security Hub CSPM のサンプル実装を提供します。これには、サービスの自動有効化、メンバーアカウントへの委任管理 (セキュリティツール)、AWS 組織内のすべての既存アカウントと将来のアカウントに対して Security Hub CSPM を有効にするための設定が含まれます。

AWS Security Hub

AWS Security Hub は、重要なセキュリティ脅威を優先し、大規模な対応を支援する統合クラウドセキュリティソリューションです。Security Hub は、体制管理 (AWS Security Hub CSPM)、脆弱性

管理 (Amazon Inspector)、機密データ (Amazon Macie)、脅威検出 (Amazon GuardDuty) など、複数のソースからのセキュリティシグナルを自動的に関連付けて強化することで、セキュリティ問題をほぼリアルタイムで検出します。これにより、セキュリティチームは自動分析とコンテキストに応じたインサイトを通じて、クラウド環境でアクティブなリスクに優先順位を付けることができます。Security Hub は、攻撃者が公開結果に関連するリソースにアクセスするために悪用できる潜在的な攻撃経路を視覚的に表現します。これにより、複雑なセキュリティシグナルが実用的なインサイトに変換されるため、セキュリティについて情報に基づいた意思決定を迅速に行うことができます。

Security Hub は戦略的に再設計され、関連するセキュリティサービス構成要素がセキュリティ上の成果を達成できるように簡素化されました。脅威マトリックスのセキュリティ検出結果をさまざまなセキュリティシグナルにほぼリアルタイムで関連付けることで、最も重要なリスクに優先順位を付けることができます。検出結果は、 AWS リソースに関連する露出を検出するために相関しています。露出は、セキュリティコントロール、設定ミス、またはアクティブな脅威によって悪用される可能性のあるその他の領域のより広範な弱点を表します。例えば、インターネットから到達可能であり、悪用の可能性の高いソフトウェアの脆弱性がある EC2 インスタンスが公開される可能性があります。

Security Hub と Security Hub CSPM は補完的なサービスです。Security Hub CSPM は、セキュリティ体制を包括的に把握し、セキュリティ業界標準とベストプラクティスに照らしてクラウド環境を評価するのに役立ちます。 Security Hub は、重要なセキュリティ問題の優先順位付けと対応に役立つ統一されたエクスペリエンスを提供します。Security Hub CSPM の検出結果は Security Hub に自動的にルーティングされ、Amazon Inspector などの他のセキュリティサービスの検出結果との相関に基づいて露出レポートを生成します。これにより、環境内の最も重大なリスクを特定できます。

Security Hub は、 AWS 環境内のリソースの概要をタイプ別および関連する検出結果別にも提供します。露出状況と攻撃シーケンスに応じてリソースに優先順位をつけて表示します。リソースタイプを選択すると、そのリソースタイプに関連付けられているすべてのリソースを確認できます。

最適なエクスペリエンスを得るには、Security Hub と Security Hub CSPM を有効にするとともに、Amazon GuardDuty、Amazon Inspector、Amazon Macie などの他のセキュリティサービスを有効にすることをお勧めします。Security Hub Coverage の検出結果を使用して、これらのサービスと機能が組織のすべてのメンバーアカウントで均一に有効になっているかどうかを可視化できます。

AWS SRA では、Security Tooling アカウントは Security Hub、Security Hub CSPM、およびその他の AWS セキュリティサービスの委任管理者として機能します。Security Tooling アカウント内で、メンバーアカウントに関連付けられているすべてのリソースを表示できます。リンクされた AWS リージョン からホーム内のすべてのリソースを表示することもできます AWS リージョン。

実装ノート

Security Hub を有効にするには、以前に Security Hub CSPM を有効にしたことがあるかどうかを考慮した手順を含む 3 つのステップが必要です。Security Hub は とネイティブに統合されているため AWS Organizations、設定と実装のプロセスが簡素化され、すべての検出結果が一元化されて 1 つの場所に集約されます。SRA のベストプラクティスに従って、Security Tooling AWS アカウントを委任管理者アカウントとして使用して、Security Hub を管理および設定します。 ???Security Hub の設定を使用して、将来のリージョンとアカウントを含むすべてのリージョン、OUs、アカウントを自動的に有効にします。また、複数の の検出結果、リソース、傾向を 1 つのホームリージョン AWS リージョン に集約するようにクロスリージョン集約を設定する必要があります。設定中に、Jira Cloud や ServiceNow などのネイティブ統合を有効にすることもできます。

設計上の考慮事項

- Security Hub の検出結果は、Open Cybersecurity Schema Framework (OCSF) でフォーマットされています。Security Hub は OCSF で検出結果を生成し、Security Hub CSPM などから OCSF で検出結果を受け取ります AWS のサービス。これらの OCSF の検出結果は、Amazon EventBridge 経由で自動化のために送信することも、中央ログ集約アカウントに保存してセキュリティログの分析と保持を実行することもできます。
- AWS 組織管理アカウントは、Security Hub の委任管理者として自身を指定することはできません。これは、Security Tooling AWS アカウントを委任管理者として指定する SRA のベストプラクティスと一致しています。また、次の点にも注意してください。
  - Security Hub CSPM の指定された管理者アカウントは、Security Hub の指定された管理者に自動的になります。
  - Security Hub を使用して委任管理を削除すると、Security Hub CSPM の委任管理も削除されます。同様に、Security Hub CSPM を使用して委任管理を削除すると、Security Hub の委任管理も削除されます。
- Security Hub には、仕様に基づいて結果を自動的に変更してアクションを実行する機能が含まれており、Security Hub は次のタイプのオートメーションをサポートしています。
  - 自動化ルール。定義された基準に基づいて、検出結果を自動的に更新し、検出結果を抑制し、検出結果をほぼリアルタイムでチケット発行ツールに送信します。
  - 自動応答と修復。特定の検出結果とインサイトに対して実行する自動アクションを定義するカスタム EventBridge ルールを作成します。

- Security Hub は、ポリシーを通じてすべてのメンバーアカウントとリージョンに Amazon Inspector を設定し、デプロイを通じて GuardDuty と Security Hub CSPM を設定できます。ポリシーは、アカウントとリージョンの AWS Organizations ポリシー を生成します。デプロイ は、選択したアカウントとリージョンでセキュリティ機能を有効にする 1 回限りのアクションです。デプロイは、新しく有効化されたアカウントには適用されません。別の方法として、GuardDuty および Security Hub CSPM で新しいメンバーアカウントの機能を自動的に有効にすることもできます。

Amazon GuardDuty

Amazon GuardDuty は、悪意のあるアクティビティや不正な動作を継続的にモニタリングして AWS アカウント および ワークロードを保護する脅威検出サービスです。モニタリングと監査の目的では常に適切なログをキャプチャして保存する必要がありますが、GuardDuty は AWS CloudTrail、、Amazon VPC フローログ、および DNS AWS ログから直接独立したデータストリームをプルします。Amazon S3 バケットポリシーを管理したり、ログの収集と保存方法を変更したりする必要はありません。GuardDuty のアクセス許可は、GuardDuty を無効にすることでいつでも取り消すことができるサービスリンクされたロールとして管理されます。これにより、複雑な設定なしでサービスを簡単に利用できるようになり、IAM アクセス許可の変更や S3 バケットポリシーの変更がサービスの運用に影響を与えるリスクを排除します。

GuardDuty は、基本的なデータソースの提供に加えて、セキュリティ上の検出結果を特定するためのオプション機能を提供します。これには、EKS Protection、RDS Protection、S3 Protection、Malware Protection、Lambda Protection が含まれます。新しいディテクターの場合、これらのオプション機能は、手動で有効にする必要がある EKS Protection を除き、デフォルトで有効になっています。

- GuardDuty S3 Protection を使用すると、GuardDuty はデフォルトの CloudTrail 管理イベントに加えてCloudTrail の Amazon S3 データイベントをモニタリングします。データイベントをモニタリングすることで、GuardDuty は S3 バケット内のデータに対する潜在的なセキュリティリスクについて、オブジェクトレベルの API オペレーションをモニタリングできます。
- GuardDuty Malware Protection は、アタッチされた Amazon EC2 インスタンスまたはコンテナワークロードでマルウェアの存在を検出します。GuardDuty は、新しくアップロードされたオブジェクトまたは既存のオブジェクトの新しいバージョンをスキャンして、S3 バケット内の潜在的なマルウェアも検出します。

- GuardDuty RDS Protection は、データベースのパフォーマンスに影響を与えることなく、Amazon Aurora データベースへのアクセスアクティビティをプロファイリングおよびモニタリングするように設計されています。
- GuardDuty EKS Protection には、EKS 監査ログモニタリングと EKS ランタイムモニタリングが含まれます。EKS 監査ログモニタリングを使用すると、GuardDuty は Amazon EKS クラスターからの Kubernetes 監査ログをモニタリングし、悪意のあるアクティビティや疑わしいアクティビティがないか分析します。EKS Runtime Monitoring は、GuardDuty セキュリティエージェント (Amazon EKS アドオン) を使用して、個々の Amazon EKS ワークロードをランタイムで可視化します。GuardDuty セキュリティエージェントは、侵害されている可能性のある Amazon EKS クラスター内の特定のコンテナを識別するのに役立ちます。また、個々のコンテナから基盤となる Amazon EC2 ホストまたはより広範な AWS 環境に権限をエスカレートしようとする試みを検出することもできます。

GuardDuty は、拡張脅威検出と呼ばれる機能も提供します。この機能は、データソース、複数のタイプの AWS リソース、および 内の時間にまたがるマルチステージ攻撃を自動的に検出します AWS アカウント。GuardDuty は、シグナルと呼ばれるこれらのイベントを関連付けて、自身を AWS 環境に対する潜在的な脅威として示すシナリオを特定し、攻撃シーケンスの検出結果を生成します。これには、 AWS 認証情報の誤用に関連する侵害や、 でのデータ侵害の試みに関連する脅威シナリオが含まれます AWS アカウント。 GuardDuty は、すべての攻撃シーケンスの検出タイプを 重大と見なします。この機能はデフォルトで有効になっており、追加コストは発生しません。

AWS SRA では、GuardDuty は を通じてすべてのアカウントで有効になっており AWS Organizations、すべての検出結果は GuardDuty 委任管理者アカウント (この場合は Security Tooling アカウント) の適切なセキュリティチームによって表示および実行可能です。GuardDuty のアクティブな検出結果はログアーカイブアカウントの中央 S3 バケットにエクスポートされるため、検出結果は 90 日間を超えて保持できます。検出結果は委任管理者アカウントからエクスポートされ、同じリージョン内の関連付けられたメンバーアカウントからのすべての検出結果も含まれます。S3 バケット内の検出結果は、 AWS KMS カスタマーマネージドキーで暗号化されます。S3 バケットポリシーと KMS キーポリシーは、GuardDuty のみがリソースを使用できるように設定されています。

AWS Security Hub CSPM を有効にすると、GuardDuty の検出結果は Security Hub CSPM と Security Hub に自動的に流れます。Amazon Detective が有効な場合、GuardDuty の結果は Detective ログの取り込み処理に含まれます。GuardDuty と Detective は、クロスサービスユーザーワークフローをサポートしています。GuardDuty は、選択した結果から、その結果を調査するための厳選されたビジュアライゼーションセットを含む Detective ページにリダイレクトするリンクをコンソールから提供します。例えば、GuardDuty を Amazon EventBridge と統合して、新しい GuardDuty の

検出結果への応答の自動化など、GuardDuty のベストプラクティスを自動化することもできます。GuardDuty

> 実装例
>
> AWS SRA コードライブラリは、GuardDuty のサンプル実装を提供します。これには、暗号化された S3 バケット設定、委任管理、および AWS 組織内のすべての既存および将来のアカウントに対する GuardDuty 有効化が含まれます。

AWS Config

AWS Config は、 でサポートされている AWS リソースの設定を評価、監査、評価できるサービスです AWS アカウント。 は AWS リソース設定 AWS Config を継続的にモニタリングおよび記録し、記録された設定を目的の設定と照合して自動的に評価します。また、 AWS Config を他の サービスと統合して、自動監査およびモニタリングパイプラインの負担を軽減することもできます。たとえば、は 内の個々のシークレットの変更をモニタリング AWS Config できます AWS Secrets Manager。

を使用して AWS リソースの設定を評価できますAWS Config ルール。 は、マネージドルールと呼ばれるカスタマイズ可能な事前定義されたルールのライブラリ AWS Config を提供するか、独自のカスタムルールを記述できます。プロアクティブモード (リソースがデプロイされる前) または検出モード (リソースがデプロイされた後) AWS Config ルール で実行できます。リソースは、設定変更時、定期的、あるいはその両方で評価できます。

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は、 AWS Config マネージドルールまたはカスタムルールと修復アクションのリストを含む YAML テンプレートを作成することによって作成されます。 AWS 環境の評価を開始するには、サンプルコンフォーマンスパックテンプレートのいずれかを使用します。

AWS Config は と統合 AWS Security Hub CSPM して、 AWS Config マネージドルールとカスタムルールの評価結果を結果として Security Hub CSPM に送信します。

AWS Config ルール は と組み合わせて使用 AWS Systems Manager して、非準拠のリソースを効果的に修復できます。Systems Manager Explorer を使用して AWS アカウント 全体のルールの AWS Config コンプライアンスステータスを収集し AWS リージョン 、 Systems Manager Automation ドキュメント (ランブック) を使用して非準拠 AWS Config ルールを解決します。実装の詳細については、ブログ記事「Remediate noncompliant AWS Config rules with AWS Systems Manager Automation runbooks」を参照してください。

AWS Config アグリゲータは、 の複数のアカウント、リージョン、および組織にわたって設定およびコンプライアンスデータを収集します AWS Organizations。アグリゲータダッシュボードには、集約されたリソースの設定データが表示されます。インベントリとコンプライアンスダッシュボードは、組織全体 AWS リージョン、組織全体 AWS アカウント、または組織内の AWS AWS リソース設定とコンプライアンスステータスに関する重要かつ最新の情報を提供します。これにより、 AWS Config 高度なクエリを記述することなく、 AWS リソースインベントリを視覚化して評価できます。リソース別のコンプライアンスの概要、非準拠リソースを持つ上位 10 のアカウント、タイプ別の EC2 インスタンスの実行と停止の比較、ボリュームのタイプとサイズ別の EBS ボリュームなど、重要なインサイトを得ることができます。

AWS Control Tower を使用して AWS 組織を管理する場合、一連の AWS Config ルールが検出ガードレールとしてデプロイされます (必須、強く推奨、または選択的に分類されます) 。これらのガードレールは、リソースを管理し、 AWS 組織内のアカウント全体のコンプライアンスをモニタリングするのに役立ちます。これらの AWS Config ルールは、 の値を持つ`aws-control-tower`タグを自動的に使用します`managed-by-control-tower`。

AWS Config は、 AWS 保護するリソース AWS リージョン を含む組織内のメンバーアカウントごとに有効にする必要があります。 AWS 組織内のすべてのアカウントで AWS Config ルールを一元管理 (作成、更新、削除など) できます。 AWS Config 委任管理者アカウントから、すべてのアカウントに共通の AWS Config ルールセットをデプロイし、 AWS Config ルールを作成すべきではないアカウントを指定できます。 AWS Config 委任管理者アカウントは、すべてのメンバーアカウントからリソース設定とコンプライアンスデータを集約して、単一のビューを提供することもできます。Security Hub CSPM が有効で APIs 、少なくとも 1 つの AWS Config マネージドルールまたはカスタム AWS Config ルールが存在する場合 AWS Security Hub CSPM、 AWS AWS Config は検出結果を送信するようにネイティブに統合されています。

AWS SRA では、 AWS Config 委任管理者アカウントは Security Tooling アカウントです。 AWS Config 配信チャネルは、ログアーカイブアカウントの一元化された S3 バケットにリソース設定スナップショットを配信するように設定されています。Log Archive アカウントは中央ログリポジトリストアであるため、リソース設定の保存に使用されます。

設計上の考慮事項

- AWS Config は、設定とコンプライアンスの変更の通知を Amazon EventBridge にストリーミングします。つまり、EventBridge のネイティブフィルタリング機能を使用して AWS Config イベントをフィルタリングし、特定のタイプの通知を特定のターゲットにルーティングできます。例えば、特定のルールやリソースタイプのコンプライアンス通知を特定の電子メールアドレスに送信したり、設定変更通知を外部 IT サービス管理 (ITSM)

または構成管理データベース (CMDB) ツールにルーティングしたりすることができます。詳細については、AWS Config ベストプラクティス のブログ投稿を参照してください。

- AWS Config プロアクティブルール評価の使用に加えて、リソース設定のコンプライアンスをプロアクティブにチェックするpolicy-as-code評価ツールAWS CloudFormation Guardである を使用できます。 AWS CloudFormation Guard コマンドラインインターフェイス (CLI) には、ポリシーをコードとして表現するために使用できる宣言型のドメイン固有の言語 (DSL) が用意されています。さらに、 AWS CLI コマンドを使用して、CloudFormation 変更セット、JSON ベースの Terraform 設定ファイル、Kubernetes 設定などの JSON 形式または YAML 形式の構造化データを検証できます。評価は、作成プロセスの一部として AWS CloudFormation Guard CLI を使用してローカルで実行することも、デプロイパイプライン内で実行することもできます。AWS Cloud Development Kit (AWS CDK) アプリケーションがある場合は、cdk-nag を使用してベストプラクティスをプロアクティブにチェックできます。

実装例

AWS SRA コードライブラリは、 AWS 組織内のすべての AWS Config AWS アカウント およびリージョンにコンフォーマンスパックをデプロイするサンプル実装を提供します。AWS Config アグリゲータモジュールは、組織管理アカウント内のメンバーアカウント (セキュリティツール) AWS Config に管理を委任し、組織内のすべての AWS 既存アカウントと将来のアカウントに対して委任管理者アカウント内で AWS Config アグリゲータを設定することで、アグリゲータを設定するのに役立ちます。AWS Config Control Tower 管理アカウントモジュールを使用して、組織管理アカウント AWS Config 内で を有効にできます。 では有効になっていません AWS Control Tower。

Amazon Security Lake

Amazon Security Lake は、フルマネージド型のセキュリティデータレイクサービスです。Security Lake を使用して、 AWS 環境、Software as a Service (SaaS) プロバイダー、オンプレミス、およびサードパーティーソースのセキュリティデータを自動的に一元化できます。Security Lake は、セキュリティデータに対する分析ツールの使用を簡素化する正規化されたデータソースを構築するため、組織全体のセキュリティ体制をより完全に理解できます。データレイクは、Amazon Simple Storage Service (Amazon S3) バケットに支えられており、データの所有権はお客様が保持します。Security Lake は AWS のサービス、 AWS CloudTrail Amazon VPC、Amazon

Route 53、Amazon S3、Amazon EKS 監査ログ AWS Lambda、 AWS Security Hub CSPM 検出結果、ログなどの AWS WAF ログを自動的に収集します。

AWS SRA では、Security Lake の委任管理者アカウントとして Log Archive アカウントを使用することをお勧めします。委任管理者アカウントの設定の詳細については、「Security OU – Log Archive account」セクションの「Amazon Security Lake」を参照してください。 Security Lake データにアクセスする、またはカスタム抽出、変換、ロード (ETL) 関数を使用して Security Lake バケットに 非ネイティブ ログを書き込む機能を必要とするセキュリティチームは、Security Tooling アカウント内で動作する必要があります。

Security Lake は、さまざまなクラウドプロバイダーからのログ、サードパーティーソリューションからのログ、またはその他のカスタムログを収集できます。Security Tooling アカウントを使用して ETL 関数を実行し、ログを Open Cybersecurity Schema Framework (OCSF) 形式に変換し、Apache Parquet 形式でファイルを出力することをお勧めします。Security Lake は、Security Tooling アカウントと、Lambda 関数またはクローラによってバックアップされたカスタムソースに対して、Security Lake の S3 AWS Glue バケットにデータを書き込むための適切なアクセス許可を持つクロスアカウントロールを作成します。

Security Lake 管理者は、Security Tooling アカウントを使用し、Security Lake がサブスクライバーとして収集するログへのアクセスを必要とするセキュリティチームを設定する必要があります。 Security Lake は、2 種類のサブスクライバーアクセスをサポートしています。

- データアクセス – サブスクライバーは Security Lake の Amazon S3 オブジェクトに直接アクセスできます。Security Lake は、インフラストラクチャとアクセス許可を管理します。Security Tooling アカウントを Security Lake データアクセスサブスクライバーとして設定すると、アカウントは Amazon Simple Queue Service (Amazon SQS) を介して Security Lake バケット内の新しいオブジェクトについて通知され、Security Lake はそれらの新しいオブジェクトにアクセスするためのアクセス許可を作成します。
- クエリアクセス – サブスクライバーは、Amazon Athena などのサービスを使用して、S3 バケット内の AWS Lake Formation テーブルからソースデータをクエリできます。クロスアカウントアクセスは、Lake Formation を使用してクエリアクセス用に自動的に設定されます。Security Tooling アカウントを Security Lake クエリアクセスサブスクライバーとして設定すると、そのアカウントには Security Lake アカウントのログへの読み取り専用アクセスが付与されます。このサブスクライバータイプを使用すると、Athena と AWS Glue テーブルは Security Lake Log Archive アカウントから AWS Resource Access Manager 、() を通じて Security Tooling アカウントと共有されます AWS RAM。この機能を有効にするには、 クロスアカウントデータ共有設定を バージョン 3 に更新する必要があります。

サブスクライバーの作成の詳細については、Security Lake ドキュメントの「サブスクライバー管理」を参照してください。

カスタムソースを取り込むためのベストプラクティスについては、Security Lake ドキュメントの「カスタムソースからデータを収集する」を参照してください。

Amazon Quick Sight、Amazon OpenSearch Service、Amazon SageMaker を使用して、Security Lake に保存するセキュリティデータに対する分析を設定できます。

> 設計上の考慮事項
>
> アプリケーションチームがビジネス要件を満たすために Security Lake データへのクエリアクセスを必要とする場合、Security Lake 管理者はそのアプリケーションアカウントをサブスクライバー として設定する必要があります。

Amazon Macie

Amazon Macie は、フルマネージド型のデータセキュリティおよびデータプライバシーサービスであり、機械学習とパターンマッチングを使用して機密データを検出し、保護します AWS。ワークロードが処理しているデータのタイプと分類を特定して、適切なコントロールが確実に適用されるようにする必要があります。Macie を使用して、機密データの検出とレポートを自動化するには、機密データの自動検出を実行する方法と、機密データ検出ジョブを作成して実行する方法の 2 つの方法があります。機密データの自動検出により、Macie は S3 バケットインベントリを毎日評価し、サンプリング手法を使用してバケットから代表的な S3 オブジェクトを識別して選択します。その後、Macie は選択したオブジェクトを取得して分析し、機密データがないか検査します。機密データ検出ジョブは、より深く、よりターゲットを絞った分析を提供します。このオプションでは、分析する S3 バケット、サンプリング深度、S3 オブジェクトのプロパティから派生するカスタム基準など、分析の幅と深さを定義します。Macie がバケットのセキュリティまたはプライバシーに関する潜在的な問題を検出すると、ユーザー用に ポリシーの調査結果を作成します。自動データ検出は、すべての新規 Macie のお客様に対してデフォルトで有効になっており、既存の Macie のお客様はワンクリックで有効にできます。

Macie は、 を通じてすべてのアカウントで有効になっています AWS Organizations。委任された管理者アカウント (この場合は Security Tooling アカウント) で適切なアクセス許可を持つプリンシパルは、どのアカウントでも Macie を有効にしたり停止にしたり、メンバーアカウントが所有するバケットに対して機密データ検出ジョブを作成したり、すべてのメンバーアカウントのすべてのポリシー結果を表示したりすることができます。機密データの結果は、機密結果ジョブを作成したアカウ

ントでのみ表示できます。詳細については、Macie ドキュメントの「組織としての複数の Macie アカウントの管理」を参照してください。

Macie の検出結果は、レビューと分析 AWS Security Hub CSPM のために に流れます。また、Macie は Amazon EventBridge と統合して、アラート、セキュリティ情報およびイベント管理 (SIEM) システムへのフィード、自動修復などの結果への自動応答を促進します。

設計上の考慮事項

- S3 オブジェクトが管理する AWS Key Management Service (AWS KMS) キーで暗号化されている場合は、Macie のサービスにリンクされたロールをキーユーザーとしてその KMS キーに追加して、Macie がデータをスキャンできるようにします。
- Macie は Amazon S3 内のオブジェクトのスキャンに最適化されています。その結果、Amazon S3 に (永続的または一時的に) 配置できる Macie がサポートするオブジェクトタイプ は、機密データをスキャンできます。つまり、Amazon Relational Database Service (Amazon RDS) または Amazon Aurora データベースの定期的なスナップショットエクスポート、エクスポートされた Amazon DynamoDB テーブル、またはネイティブまたはサードパーティーアプリケーションから抽出されたテキストファイルなど、他のソースからのデータを Amazon S3 に移動して Macie で評価することができます。

実装例

AWS SRA コードライブラリは、Amazon Macie のサンプル実装を提供します。これには、メンバーアカウントに管理を委任し、 AWS 組織内のすべての既存および将来のアカウントの委任された管理者アカウント内で Macie を設定することが含まれます。Macie は、 のカスタマーマネージドキーで暗号化された中央 S3 バケットに結果を送信するようにも設定されています AWS KMS。

IAM Access Analyzer

AWS クラウド 導入ジャーニーを加速し、イノベーションを続けるには、きめ細かなアクセス (アクセス許可) を厳密に制御し、アクセスの拡散を防ぎ、アクセス許可を効果的に使用することが重要です。過剰で未使用のアクセスは、セキュリティ上の課題となり、企業が最小特権の原則を強制することが困難になります。この原則は、セキュリティ要件と運用要件およびアプリケーション開発要件のバランスを取るために IAM アクセス許可を継続的に適切なサイズにすることを含む、重要なセ

キュリティアーキテクチャの柱です。この取り組みには、中央セキュリティチーム、Cloud Center of Excellence (CCoE) チーム、分散開発チームなど、複数の利害関係者のペルソナが含まれます。

AWS Identity and Access Management Access Analyzer には、エンタープライズセキュリティ標準を満たすために未使用のアクセスを削除することで、きめ細かなアクセス許可を効率的に設定し、意図したアクセス許可を検証し、アクセス許可を絞り込むためのツールが用意されています。これにより、ダッシュボードと を通じて AWS 、リソースへの外部および内部アクセスと未使用のアクセスの検出結果を 可視化できますAWS Security Hub CSPM。さらに、イベントベースのカスタム通知および修復ワークフローの Amazon EventBridge をサポートしています。

IAM Access Analyzer の外部アクセスアナライザーの検出結果は、 Amazon S3 バケットや IAM ロールなど、外部エンティティと共有されている AWS 組織やアカウント内のリソースを識別するのに役立ちます。選択した AWS 組織またはアカウントは、信頼ゾーンと呼ばれます。アナライザーは 自動推論 を使用して、信頼ゾーン内の サポートされているすべてのリソース を分析し、信頼ゾーン外からリソースにアクセスできるプリンシパルの結果を生成します。これらの検出結果は、外部エンティティと共有されているリソースを特定し、リソース許可をデプロイする前に、ポリシーがリソースへのパブリックアクセスとクロスアカウントアクセスにどのように影響するかをプレビューするのに役立ちます。これは追加料金なしで利用できます。

同様に、IAM Access Analyzer の内部アクセスアナライザーの検出機能は、 AWS 組織内のリソースと、組織またはアカウント内のプリンシパルと共有されているアカウントを識別するのに役立ちます。この分析は、組織内の意図したプリンシパルのみが指定されたリソースにアクセスできるようにすることで、最小特権の原則をサポートします。これは有料機能であり、検査するリソースの明示的な設定が必要です。この機能は、設計上、内部的にもロックダウンする必要がある特定の機密リソースを慎重にモニタリングするために使用します。

IAM Access Analyzer の検出結果は、組織やアカウントで AWS 付与された未使用のアクセスを特定するのにも役立ちます。

- 未使用の IAM ロール – 指定された使用期間内にアクセスアクティビティがないロール。
- 未使用の IAM ユーザー、認証情報、アクセスキー – IAM ユーザーに属する認証情報で、 AWS のサービス および リソースへのアクセスに使用されます。
- 未使用の IAM ポリシーとアクセス許可 – 指定された使用期間内にロールによって使用されなかったサービスレベルおよびアクションレベルのアクセス許可。IAM Access Analyzer は、ロールにアタッチされたアイデンティティベースのポリシーを使用して、それらのロールがアクセスできるサービスとアクションを決定します。アナライザーは、すべてのサービスレベルのアクセス許可に対する未使用のアクセス許可のレビューを提供します。

IAM Access Analyzer から生成された検出結果を使用して、組織のポリシーとセキュリティ標準に基づいて、意図しないアクセスや未使用のアクセスを可視化し、修復できます。修復後、これらの検出結果は次にアナライザーが実行されるときに 解決 済みとしてマークされます。検出結果が意図的なものである場合は、IAM Access Analyzer で アーカイブ済み としてマークし、セキュリティリスクが大きい他の検出結果に優先順位を付けることができます。さらに、 アーカイブルールを設定して、特定の検出結果を自動的にアーカイブできます。例えば、定期的にアクセスを許可する特定の Amazon S3 バケットに関する検出結果を自動的にアーカイブするためのアーカイブルールを作成できます。

ビルダーは、IAM Access Analyzer を使用して、開発およびデプロイ (CI/CD) プロセスの早い段階で自動化された IAM ポリシーチェック を実行し、企業のセキュリティ標準に準拠できます。IAM Access Analyzer のカスタムポリシーチェックとポリシーレビューを と統合 AWS CloudFormation して、開発チームの CI/CD パイプラインの一部としてポリシーレビューを自動化できます。これには、以下が含まれます。

- IAM ポリシーの検証 – IAM Access Analyzer は、IAM ポリシーの文法と AWS ベストプラクティスに照らしてポリシーを検証します。セキュリティ警告、エラー、一般的な警告、ポリシーの提案など、ポリシー検証チェックの結果を表示できます。現在、100 を超える ポリシー検証チェック が利用可能で、 AWS Command Line Interface (AWS CLI) と APIs を使用して自動化できます。
- IAM カスタムポリシーチェック – IAM Access Analyzer カスタムポリシーチェックは、指定されたセキュリティ標準に照らしてポリシーを検証します。カスタムポリシーチェックでは、自動推論を使用して、企業のセキュリティ基準を満たすためのより高いレベルの保証を提供します。カスタムポリシーチェックのタイプは次のとおりです。
  - 参照ポリシーと照合する: ポリシーを編集するときに、ポリシーの既存のバージョンなどの参照ポリシーと比較し、更新が新しいアクセスを許可するかどうかを確認できます。CheckNoNewAccess API は、2 つのポリシー (更新されたポリシーと参照ポリシー) を比較して、更新されたポリシーが参照ポリシーに新しいアクセスを導入するかどうかを判断し、合格または不合格のレスポンスを返します。
  - IAM アクションのリストと照合する： CheckAccessNotGranted API を使用して、ポリシーがセキュリティ標準で定義されている重要なアクションのリストへのアクセスを許可しないようにできます。この API は、ポリシーと最大 100 個の IAM アクションのリストを取得して、ポリシーが少なくとも 1 つのアクションを許可するかどうかをチェックし、合格または不合格のレスポンスを返します。

セキュリティチームやその他の IAM ポリシー作成者は、IAM Access Analyzer を使用して、IAM ポリシーの文法とセキュリティ標準に準拠したポリシーを作成できます。適切なサイズのポリシーを手

動で作成すると、エラーが発生しやすく、時間がかかる場合があります。 IAM Access Analyzer ポリシー生成 機能は、プリンシパルのアクセスアクティビティに基づく IAM ポリシーの作成に役立ちます。IAM Access Analyzer は、サポートされているサービスの AWS CloudTrail ログを確認し、指定された日付範囲でプリンシパルによって使用されたアクセス許可を含むポリシーテンプレートを生成します。その後、このテンプレートを使用して、必要なアクセス許可のみを付与するきめ細かなアクセス許可を持つポリシーを作成できます。

- アクセスアクティビティに基づいてポリシーを生成するには、アカウントで CloudTrail 証跡が有効になっている必要があります。
- IAM Access Analyzer は、生成されたポリシーで Amazon S3 データイベントなどのデータイベントのアクションレベルのアクティビティを識別しません。
- `iam:PassRole` アクションは CloudTrail によって追跡されず、生成されたポリシーに含まれません。

IAM Access Analyzer は、 の委任管理者機能を通じて Security Tooling アカウントにデプロイされます AWS Organizations。委任された管理者には、 AWS 組織を信頼ゾーンとして持つアナライザーを作成および管理するためのアクセス許可があります。

設計上の考慮事項

アカウントスコープの結果 (アカウントが信頼境界として機能する場所) を取得するには、各メンバーアカウントにアカウントスコープのアナライザーを作成します。これは、アカウントパイプラインの一部として実行できます。アカウントスコープの検出結果は、メンバーアカウントレベルで Security Hub CSPM に流れます。そこから、Security Hub CSPM 委任管理者アカウント (Security Tooling) に流れます。

実装例

- AWS SRA コードライブラリは、IAM Access Analyzer のサンプル実装を提供します。委任管理者アカウント内で組織レベルのアナライザーを設定し、各アカウント内でアカウントレベルのアナライザーを設定する方法を示します。
- カスタムポリシーチェックをビルダーワークフロー に統合する方法については、 AWS ブログ記事「IAM Access Analyzer カスタムポリシーチェックの紹介」を参照してください。

AWS Firewall Manager

AWS Firewall Manager は、複数のアカウントとリソースにわたる、 AWS WAF、Amazon VPC セキュリティグループ AWS Shield Advanced、および Amazon Route 53 Resolver DNS Firewall の管理およびメンテナンスタスクを簡素化することで AWS Network Firewall、ネットワークを保護するのに役立ちます。Firewall Manager では、 AWS WAF ファイアウォールルール、Shield Advanced 保護、Amazon VPC セキュリティグループ、Network Firewall ファイアウォール、DNS Firewall ルールグループの関連付けを 1 回だけセットアップします。ルールと保護が既存のアカウントとリソースに (追加する新しいリソースにも) 自動的に適用されます。

Firewall Manager は、少数の特定のアカウントやリソースではなく AWS 組織全体を保護する場合や、保護する新しいリソースを頻繁に追加する場合に特に便利です。Firewall Manager は、セキュリティポリシーを使用して、デプロイする必要がある関連するルール、保護、アクション、および含めるか除外するアカウントとリソース (タグで示される) を含む、一連の設定を定義できます。細分化された柔軟な設定を作成しながら、多数のアカウントと VPC に制御をスケールアウトさせることが可能です。これらのポリシーは、新しいアカウントとリソースが作成された場合でも、設定したルールを自動的かつ一貫して適用します。Firewall Manager は を通じてすべてのアカウントで有効になり AWS Organizations、設定と管理は Firewall Manager の委任管理者アカウント (この場合は Security Tooling アカウント) の適切なセキュリティチームによって実行されます。

保護するリソース AWS リージョン を含む各 AWS Config に対して を有効にする必要があります。すべてのリソース AWS Config に対して を有効にしない場合は、使用する Firewall Manager ポリシーのタイプに関連付けられているリソースに対して有効にする必要があります。 AWS Security Hub CSPM と Firewall Manager の両方を使用すると、Firewall Manager は自動的に検出結果を Security Hub CSPM に送信します。Firewall Manager は、コンプライアンス違反のリソースと検出した攻撃の検出結果を作成し、その検出結果を Security Hub CSPM に送信します。Firewall Manager ポリシーを設定すると AWS WAF、すべての対象アカウントのウェブアクセスコントロールリスト (ウェブ ACLs) のログ記録を一元的に有効にし、ログを 1 つのアカウントで一元管理できます。

Firewall Manager では、組織のファイアウォールリソースを管理できる管理者を 1 人または複数持つことができます。複数の管理者を割り当てる場合、制限的な管理範囲条件を適用して、各管理者が管理できるリソース (アカウント、OUs、リージョン、ポリシータイプ) を定義できます。これにより、組織内のさまざまな管理者に役割を割り当てる上での柔軟性が提供され、最小権限の原則を維持しやすくなります。SRA は、Security Tooling AWS アカウントに委任された完全な管理スコープを持つ 1 人の管理者を使用します。

設計上の考慮事項

AWS 組織内の個々のメンバーアカウントのアカウントマネージャーは、特定のニーズに合わせて Firewall Manager マネージドサービスで追加のコントロール (AWS WAF ルールや Amazon VPC セキュリティグループなど) を設定できます。

実装例

AWS SRA コードライブラリは、Firewall Manager のサンプル実装を提供します。委任管理 (Security Tooling) を示し、最大許容セキュリティグループをデプロイし、セキュリティグループポリシーを設定し、複数の AWS WAF ポリシーを設定します。

Amazon EventBridge

Amazon EventBridge は、アプリケーションをさまざまなイベントソースのデータに簡単に接続できるようにするサーバーレスイベントバスサービスです。セキュリティオートメーションによく使用されます。お客様は、データの送信先を判断するためのルーティングルールを設定して、すべてのデータソースにリアルタイムで反応するアプリケーションアーキテクチャを構築できます。各アカウントでデフォルトのイベントバスを使用するだけでなく、カスタムアプリケーションからイベントを受信するためにカスタムイベントバスを作成することができます。Security Tooling アカウントで、 AWS 組織内の他のアカウントからセキュリティ固有のイベントを受信できるイベントバスを作成できます。たとえば、、 AWS Config ルール Amazon GuardDuty、および EventBridge をリンクすることで、セキュリティデータのルーティング、アラートの生成、問題解決のためのアクションの管理のための柔軟 AWS Security Hub CSPM で自動化されたパイプラインを作成します。

設計上の考慮事項

- EventBridge は、さまざまなターゲットにイベントをルーティングできます。セキュリティアクションを自動化するための重要なパターンの 1 つは、特定のイベントを個々の AWS Lambda レスポンダーに接続し、適切なアクションを実行することです。例えば、特定の状況では、EventBridge を使用して、バケットポリシーを修正し、公開許可を削除する Lambda レスポンダーに公開 S3 バケットの結果をルーティングしたい場合があります。これらのレスポンダーは、調査プレイブックとランブックに統合して、対応アクティビティを調整できます。

- セキュリティ運用チームが成功するためのベストプラクティスは、セキュリティイベントと結果事項のフローを、チケッティングシステム、バグ/イシューシステム、またはその他のセキュリティ情報およびイベント管理 (SIEM) システムなどの通知およびワークフローシステムに統合することです。これにより、電子メールおよび静的レポートからワークフローを取り除き、イベントや結果をルーティング、エスカレーション、管理することが可能になります。EventBridge の柔軟なルーティング機能は、この統合を可能にする強力なイネーブラーです。

Amazon Detective

Amazon Detective は、セキュリティアナリストのセキュリティ検出結果や疑わしいアクティビティの根本原因を簡単に分析、調査、迅速に特定できるようにすることで、応答性の高いセキュリティコントロール戦略をサポートします。Detective は、ログイン試行、API コール、ネットワークトラフィックなどの時間ベースのイベントを AWS CloudTrail ログや Amazon VPC フローログから自動的に抽出します。Detective は、CloudTrail ログと Amazon VPC フローログの独立したストリームを使用して、これらのイベントを消費します。Detective を使用して、最大 1 年間の履歴イベントデータにアクセスできます。Detective は、機械学習とビジュアライゼーションにより、リソースの動作とリソース間のインタラクションを時系列で統合したインタラクティブなビューを作成します。これは ビヘイビアグラフ と呼ばれます。ビヘイビアグラフを詳しく確認して、失敗したログオン試行や疑わしい API コールなどのさまざまなアクションを調べることができます。

Detective は Amazon Security Lake と統合され、セキュリティアナリストが Security Lake に保存されているログをクエリおよび取得できるようにします。この統合を使用して、Detective でセキュリティ調査を実行しながら、Security Lake に保存されている CloudTrail ログと Amazon VPC フローログから追加情報を取得できます。

Detective は、Amazon GuardDuty GuardDuty によって検出された検出結果も取り込みます。アカウントで Detective を有効にすると、そのアカウントがビヘイビアグラフの管理者アカウントになります。Detective を有効にする前に、アカウントが GuardDuty に登録されてから 48 時間以上が経過していることを確認してください。この要件を満たしていない場合、DetectiveDetective を有効にすることはできません。

Detective のその他のオプションのデータソースには、Amazon EKS 監査ログと が含まれます AWS Security Hub CSPM。Amazon EKS 監査ログデータソースは、Amazon EKS クラスター、Kubernetes ポッド、コンテナイメージ、Kubernetes サブジェクトのエンティティタイプに関して提供される情報を強化します。Security Hub データソースはAWS セキュリティ検出結果の一部であり、製品間の検出結果を Security Hub に関連付け、Detective に取り込みます。

Detective は、単一のセキュリティ侵害イベントに関連する複数の検出結果を検出結果グループに自動的にグループ化します。脅威アクターは通常、時間やリソースにまたがる複数のセキュリティ検出結果につながる一連のアクションを実行します。したがって、検出結果グループは、複数のエンティティと検出結果を含む調査の開始点である必要があります。また、Detective は、検出結果グループを自動的に分析する生成 AI を使用して検出結果グループの概要を提供し、セキュリティ調査の 迅速化に役立つ自然言語でのインサイトを提供します。

Detective は と統合されます AWS Organizations。組織管理アカウントは、メンバーアカウントを Detective 管理者アカウントとして委任します。SRA では、これは Security Tooling AWS アカウントです。Detective 管理者アカウントは、組織内のすべての現在のメンバーアカウントを Detective メンバーアカウントとして自動的に有効にし、 AWS 組織に追加された新しいメンバーアカウントを追加することもできます。Detective 管理者アカウントは、現在 AWS 組織には存在しないが、同じリージョン内にあるメンバーアカウントを招待して、プライマリアカウントの動作グラフにデータを提供することもできます。メンバーアカウントが招待を承諾して有効になると、Detective は、メンバーアカウントのデータを取り込み、その動作グラフに抽出し始めます。

> **設計上の考慮事項**
>
> GuardDuty および AWS Security Hub CSPM コンソールから Detective の検出結果プロファイルに移動できます。これらのリンクは、調査プロセスを合理化するのに役立ちます。アカウントは、Detective とピボット元のサービス (GuardDuty または Security Hub CSPM) の両方の管理アカウントである必要があります。サービスのプライマリアカウントが同じであれば、統合リンクはシームレスに機能します。

AWS Audit Manager

AWS Audit Manager は、 AWS 使用状況を継続的に監査し、監査の管理方法と規制や業界標準への準拠を簡素化するのに役立ちます。これにより、証拠を手動で収集、レビュー、管理することから、証拠収集を自動化するソリューションに移行し、監査証拠のソースを追跡する簡単な方法を提供し、チームワークのコラボレーションを可能にし、証拠のセキュリティと整合性を管理するのに役立ちます。監査の時期において、Audit Manager は、コントロールのステークホルダーのレビューを管理するのに役立ちます。

Audit Manager を使用すると、Center for Internet Security (CIS) ベンチマーク、CIS AWS Foundations Benchmark、System and Organization Controls 2 (SOC 2)、Payment Card Industry Data Security Standard (PCI DSS) などの構築済みのフレームワークに対して監査を行うことができ

ます。また、内部監査の特定の要件に基づいて、標準コントロールまたはカスタムコントロールを使用して独自のフレームワークを作成することもできます。

Audit Manager は 4 種類の証拠を収集します。自動化される証拠には、 AWS Config と からのコンプライアンスチェックの証拠 AWS Security Hub CSPM、 からの管理イベントの証拠 AWS CloudTrail、 AWS service-to-service API コールの設定の証拠の 3 種類があります。自動化できない証拠については、Audit Manager では手動証拠をアップロードできます。

デフォルトでは、Audit Manager のデータは AWS マネージドキーを使用して暗号化されます。AWS SRA は暗号化にカスタマーマネージドキーを使用して、論理アクセスをより細かく制御します。また、Audit Manager が評価レポートを発行 AWS リージョン する で S3 バケットを設定する必要があります。このバケットはカスタマーマネージドキーで暗号化し、Audit Manager のみがレポートを発行できるようにバケットポリシーを設定する必要があります。

> **Note**
>
> Audit Manager は、特定のコンプライアンス標準および規制への準拠の検証に関連する証拠の収集を支援します。ただし、コンプライアンスは評価されません。したがって、Audit Manager を通じて収集された証拠には、監査に必要な運用プロセスの詳細が含まれていない可能性があります。Audit Manager は、法律顧問やコンプライアンスの専門家に代わるものではありません。評価対象のコンプライアンスフレームワーク (複数可) の認定を受けているサードパーティーの評価機関のサービスを利用することをお勧めします。

Audit Manager の評価は、 AWS 組織内の複数のアカウントで実行できます。Audit Manager は証拠を収集し、 の委任管理者アカウントに統合します AWS Organizations。この監査機能は、主にコンプライアンスチームと内部監査チームによって使用され、 への読み取りアクセスのみが必要です AWS アカウント。

> **設計上の考慮事項**
>
> - Audit Manager は AWS Security Hub CSPM、、、 などの他の AWS セキュリティサービスを補完 AWS Config して AWS Security Hub、リスク管理フレームワークの実装を支援します。Audit Manager は独立したリスク保証機能を提供しますが、Security Hub CSPM AWS Config はリスクの監視に役立ち、コンフォーマンスパックはリスクの管理に役立ちます。 内部監査機関 (IIA) によって開発された 3 行モデル に精通している監査プロフェッショナルは、この の組み合わせが 3 つの防衛線をカバーする AWS のサービス のに役立つ

ことに注意してください。詳細については、 AWS クラウド 「 オペレーションと移行」ブログの「2 部構成のブログシリーズ」を参照してください。

- Audit Manager が Security Hub CSPM の証拠を収集するには、両方のサービスの委任管理者アカウントが同じである必要があります AWS アカウント。このため、SRA AWS では、Security Tooling アカウントが Audit Manager の委任管理者になります。

AWS Artifact

AWS Artifact は Security Tooling アカウント内でホストされ、コンプライアンスアーティファクト管理機能を AWS 組織管理アカウントから分離します。絶対に必要な場合を除き、デプロイに AWS 組織管理アカウントを使用しないことをお勧めします。代わりに、メンバーアカウントにデプロイを渡します。監査アーティファクト管理はメンバーアカウントから実行でき、 関数はセキュリティおよびコンプライアンスチームと密接に連携するため、Security Tooling アカウントは管理者アカウントとして指定されます AWS Artifact。 AWS Artifact レポートを使用して、 AWS ISO 認定、Payment Card Industry (PCI)、System and Organization Controls (SOC) レポートなどの AWS セキュリティおよびコンプライアンスドキュメントをダウンロードできます。

AWS Artifact は、委任管理機能をサポートしていません。代わりに、この機能を監査チームとコンプライアンスチームに関連する Security Tooling アカウントの IAM ロールのみに制限して、必要に応じてそれらのレポートをダウンロード、レビュー、外部監査人に提供できます。さらに、IAM ポリシーを通じて特定の IAM ロールが特定の AWS Artifact レポートのみにアクセスできるように制限することもできます。IAM ポリシーのサンプルについては、 AWS Artifact ドキュメントを参照してください。

設計上の考慮事項

監査チームとコンプライアンスチーム AWS アカウント 専用の を持つことを選択した場合、Security Tooling アカウントとは別のセキュリティ監査アカウント AWS Artifact でホストできます。 AWS Artifact レポートは、組織が文書化されたプロセスに従っているか、特定の要件を満たしていることを示す証拠を提供します。監査アーティファクトは、システム開発ライフサイクル全体で収集およびアーカイブされ、内部または外部の監査と評価の証拠として使用できます。

AWS KMS

AWS Key Management Service (AWS KMS) は、暗号化キーを作成および管理し、アプリケーションのさまざまな AWS のサービス および での使用を制御するのに役立ちます。 AWS KMS は、ハードウェアセキュリティモジュールを使用して暗号化キーを保護する安全で回復力のあるサービスです。キーのストレージ、ローテーション、アクセス制御など、キーマテリアルに関する業界標準のライフサイクルプロセスに従います。 AWS KMS は、暗号化キーと署名キーを使用してデータを保護するのに役立ち、AWS Encryption SDK によるサーバー側の暗号化とクライアント側の暗号化の両方に使用できます。保護と柔軟性のために、 はカスタマーマネージドキー、マネージドキー、 AWS 所有キーの AWS 3 種類のキー AWS KMS をサポートしています。カスタマーマネージドキーは、 AWS アカウント ユーザーが作成、所有、管理する の AWS KMS キーです。 AWS マネージドキーは、ユーザーに代わって と AWS のサービス 統合された によって作成、管理、使用される AWS KMS アカウントのキーです AWS KMS。 AWS 所有キーは、 が複数の で使用できるように AWS のサービス 所有、管理する AWS KMS キーのコレクションです AWS アカウント。 AWS KMS キーの使用の詳細については、 AWS KMS ドキュメントとAWS KMS 暗号化の詳細を参照してください。

1 つのデプロイオプションは、 AWS KMS キーと IAM ポリシーの組み合わせを使用して、アプリケーションリソースによってアプリケーションアカウントのキーを使用する機能を委任しながら、キー管理の責任を 1 つのアカウントに一元化することです。このアプローチは安全かつ簡単に管理できますが、スロットリング制限、アカウントサービス制限、セキュリティチームが運用上のキー管理タスクに溜まっているため AWS KMS 、ハードルが発生する可能性があります。もう 1 つのデプロイオプションは、複数のアカウントへの配置 AWS KMS を許可する分散モデルを用意し、特定のアカウントのインフラストラクチャとワークロードを担当するユーザーに独自のキーの管理を許可することです。このモデルにより、ワークロードチームは暗号化キーの使用に対する制御性、柔軟性、俊敏性が向上します。また、API の制限を回避し、影響の範囲を 1 AWS アカウント つのみに制限し、レポート、監査、その他のコンプライアンス関連のタスクを簡素化するのに役立ちます。分散モデルでは、分散キーが同じ方法で管理され、確立されたベストプラクティスとポリシーに従ってキーの使用 AWS KMS が監査されるように、ガードレールをデプロイして適用することが重要です。詳細については、ホワイトペーパーAWS Key Management Service 「ベストプラクティス」を参照してください。 AWS SRA では、キーが使用されるアカウント内にローカルに存在する分散 AWS KMS キー管理モデルを推奨しています。すべての暗号化関数で 1 つのアカウントで 1 つのキー を使用しないことをお勧めします。キーは、関数とデータ保護の要件に基づいて作成し、最小特権の原則を適用できます。場合によっては、暗号化アクセス許可は復号アクセス許可とは別に保持され、管理者はライフサイクル関数を管理しますが、管理するキーを使用してデータを暗号化または復号することはできません。

Security Tooling アカウント AWS KMS では、組織が管理する AWS CloudTrail AWS 組織の証跡など、一元化されたセキュリティサービスの暗号化を管理するために使用されます。

AWS Private CA

AWS Private Certificate Authority (AWS Private CA) は、EC2 インスタンス、コンテナ、IoT デバイス、オンプレミスリソースのプライベートエンドエンティティ TLS 証明書のライフサイクルを安全に管理するのに役立つマネージドプライベート CA サービスです。これにより、実行中のアプリケーションへの暗号化された TLS 通信が可能になります。を使用すると AWS Private CA、独自の CA 階層 (ルート CA、下位 CAs、エンドエンティティ証明書) を作成し、証明書を発行して内部ユーザー、コンピュータ、アプリケーション、サービス、サーバー、その他のデバイスを認証し、コンピュータコードに署名できます。プライベート CA によって発行された証明書は、インターネットではなく AWS 組織内でのみ信頼されます。

パブリックキーインフラストラクチャ (PKI) またはセキュリティチームは、すべての PKI インフラストラクチャの管理を担当できます。これには、プライベート CA の管理と作成が含まれます。ただし、ワークロードチームが証明書要件をセルフサービスできるようにするプロビジョニングが必要です。 AWS SRA は、ルート CA が Security Tooling アカウント内でホストされている一元的な CA 階層を示しています。これにより、ルート CA は PKI 全体の基盤であるため、セキュリティチームは厳格なセキュリティコントロールを適用できます。ただし、プライベート CA からのプライベート証明書の作成は、 AWS Resource Access Manager (AWS RAM) を使用して CA をアプリケーションアカウントと共有することで、アプリケーション開発チームに委任されます。 は、クロスアカウント共有に必要なアクセス許可 AWS RAM を管理します。これにより、すべてのアカウントでプライベート CA が不要になり、よりコスト効率の高いデプロイ方法が提供されます。ワークフローと実装の詳細については、ブログ記事「 AWS RAM を使用して AWS Private CA クロスアカウントを共有する方法」を参照してください。

> **Note**
>
> AWS Certificate Manager (ACM) は、 で使用するパブリック TLS 証明書のプロビジョニング、管理、デプロイにも役立ちます AWS のサービス。この機能をサポートするには、ACM がパブリック証明書 AWS アカウント を使用する に存在する必要があります。これは、このガイドの「アプリケーションアカウント」セクションで後ほど説明します。

> **設計上の考慮事項**
>
> - を使用すると AWS Private CA、最大 5 つのレベルで認証機関の階層を作成できます。また、それぞれ独自のルートを持つ複数の階層を作成することもできます。 AWS Private CA 階層は、組織の PKI 設計に従う必要があります。ただし、CA 階層を増やすと、証明書

パス内の証明書の数が増え、その結果、エンドエンティティ証明書の検証時間が長くなることに注意してください。明確に定義された CA 階層には、各 CA に適したきめ細かなセキュリティコントロール、下位 CA を別のアプリケーションに委任することによる管理タスクの分割、取り消し可能な信頼が制限された CA の使用、異なる有効期間を定義する機能、パス制限を適用する機能などの利点があります。理想的には、ルート CA と下位 CAs は別々の にあります AWS アカウント。を使用して CA 階層を計画する方法の詳細については AWS Private CA、 AWS Private CA ドキュメントとブログ記事「自動車および製造のエンタープライズスケール AWS Private CA 階層を保護する方法」を参照してください。

- AWS Private CA は既存の CA 階層と統合できます。これにより、ACM の自動化およびネイティブ AWS 統合機能を、現在使用している既存の信頼のルートと組み合わせて使用できます。オンプレミスの親 CA によって AWS Private CA バックアップされた下位 CA をに作成できます。実装の詳細については、 AWS Private CA ドキュメントの「外部親 CA によって署名された下位 CA 証明書のインストール」を参照してください。

Amazon Inspector

Amazon Inspector は、Amazon EC2 インスタンス、Amazon Elastic Container Registry (Amazon ECR) のコンテナイメージ、 AWS Lambda 関数、およびソースコードマネージャー内のコードリポジトリを自動的に検出してスキャンし、ソフトウェアの既知の脆弱性と意図しないネットワークへの露出を検出する自動脆弱性管理サービスです。

Amazon Inspector は、リソースを変更するたびにリソースを自動的にスキャンすることで、リソースのライフサイクル全体を通じて環境を継続的に評価します。リソースの再スキャンを開始するイベントには、EC2 インスタンスへの新しいパッケージのインストール、パッチのインストール、リソースに影響を与える新しい一般的な脆弱性と露出 (CVE) レポートの公開が含まれます。Amazon Inspector は、EC2 インスタンスのオペレーティングシステムの Center of Internet Security (CIS) Benchmark 評価をサポートしています。

Amazon Inspector は、コンテナイメージ評価のために Jenkins や TeamCity などの開発者ツールと統合されています。継続的インテグレーションおよび継続的デリバリー (CI/CD) ツール内のソフトウェアの脆弱性についてコンテナイメージを評価し、ソフトウェア開発ライフサイクルの早い時点にセキュリティをプッシュできます。評価結果は CI/CD ツールのダッシュボードで利用できるため、ブロックされたビルドやコンテナレジストリへのイメージプッシュなどの重要なセキュリティ問題に応じて自動アクションを実行できます。がアクティブな場合は AWS アカウント、CI/CD ツールマーケットプレイスから Amazon Inspector プラグインをインストールし、Amazon Inspector サービスをアクティブ化することなく Amazon Inspector スキャンをビルドパイプラインに追加できます。この

機能は、オンプレミス AWS、ハイブリッドクラウドなど、どこでもホストされる CI/CD ツールで動作するため、すべての開発パイプラインで 1 つのソリューションを一貫して使用できます。Amazon Inspector を有効にすると、すべての EC2 インスタンス、Amazon ECR および CI/CD ツールのコンテナイメージ、Lambda 関数を大規模に自動的に検出し、既知の脆弱性を継続的にモニタリングします。

Amazon Inspector のネットワーク到達可能性の検出結果は、インターネットゲートウェイ、VPC ピアリング接続、仮想ゲートウェイを介した仮想プライベートネットワーク (VPNs) などの VPC エッジとの間の EC2 インスタンスのアクセシビリティを評価します。これらのルールは、 AWS ネットワークのモニタリングを自動化し、管理ミスのセキュリティグループ、アクセスコントロールリスト (ACLs)、インターネットゲートウェイなどを通じて EC2 インスタンスへのネットワークアクセスが誤って設定される可能性のある場所を特定するのに役立ちます。さらなる詳細については、Amazon Inspector documentation を参照してください。

Amazon Inspector が脆弱性またはオープンネットワークパスを特定すると、調査できる検出結果が生成されます。検出結果には、リスクスコア、影響を受けるリソース、修復推奨事項など、脆弱性に関する包括的な詳細が含まれます。リスクスコアは環境に合わせて特別に調整され、up-to-date CVE 情報をネットワークアクセシビリティやエクスプロイト可能性情報などの時間的および環境的要因と関連付けて、コンテキストに応じた検出結果を提供することで計算されます。

Amazon Inspector Code Security は、ファーストパーティアプリケーションソースコード、サードパーティーアプリケーションの依存関係、Infrastructure as Code (IaC) の脆弱性をスキャンします。Code Security をアクティブ化 すると、スキャンする頻度、スキャンタイプ、リポジトリを決定するためのスキャン設定を作成してコードリポジトリに適用できます。 Code Security は、 静的アプリケーションセキュリティテスト (SAST)、ソフトウェアコンポジション分析 (SCA)、IaC スキャンをサポートしています。頻度を設定するには、オンデマンド、コード変更時、または定期的にスキャンを定義できます。コードスキャンでは、コードスニペットをキャプチャして検出された脆弱性をハイライトします。コードスニペットは KMS キーで暗号化されて保存されます。組織の委任管理者は、メンバーアカウントに属するコードスニペットを表示できません。ソースコードマネージャー (SCMs) を Code Security と統合すると、Amazon Inspector コンソールにすべてのコードリポジトリがプロジェクトとして一覧表示されます。Code Security は、各リポジトリのデフォルトブランチのみをモニタリングします。Amazon Inspector は、開発者が作業する場所で特定のコード修正の推奨事項を直接提供することで、セキュリティ修復を合理化します。SCM との双方向統合では、重要な検出結果と高い検出結果に対するプルリクエスト (PRs) とマージリクエスト (MRs) 内のコメントとして修正を自動的に提案し、ワークフローを中断することなく対処すべき最も重要な脆弱性をデベロッパーに警告します。

脆弱性をスキャンするには、 AWS Systems Manager エージェント (SSMAgent) を使用して EC2 インスタンスを で AWS Systems Manager 管理する必要があります。 Amazon ECR または Lambda 関数の EC2 インスタンスのネットワーク到達可能性やコンテナイメージの脆弱性スキャンにエージェントは必要ありません。

Amazon Inspector は と統合 AWS Organizations されており、委任管理をサポートしています。SRA AWS では、Security Tooling アカウントが Amazon Inspector の委任管理者アカウントになります。Amazon Inspector の委任管理者アカウントは、 AWS 組織のメンバーの検出結果データと特定の設定を管理できます。これには、すべてのメンバーアカウントの集計結果の詳細の表示、メンバーアカウントのスキャンの有効化または無効化、 AWS 組織内のスキャンされたリソースの確認が含まれます。

設計上の考慮事項

- Amazon Inspector は、両方のサービスが有効になっている場合、 AWS Security Hub CSPM および Security Hub と自動的に統合されます。この統合を使用して、Amazon Inspector から Security Hub CSPM にすべての検出結果を送信し、セキュリティ体制の分析にそれらの検出結果を含めることができます。
- Amazon Inspector は、検出結果、リソースカバレッジの変更、個々のリソースの初期スキャンのイベントを Amazon EventBridge に自動的にエクスポートし、オプションで Amazon Simple Storage Service (Amazon S3) バケットに自動的にエクスポートします。アクティブな検出結果を S3 バケットにエクスポートするには、Amazon Inspector が検出結果を暗号化するために使用できる AWS KMS キーと、Amazon Inspector がオブジェクトをアップロードできるようにするアクセス許可を持つ S3 バケットが必要です。EventBridge 統合により、既存のセキュリティおよびコンプライアンスワークフローの一環として、検出結果をほぼリアルタイムでモニタリングおよび処理できます。EventBridge イベントは、元のメンバーアカウントに加えて、Amazon Inspector の委任管理者アカウントに発行されます。
- Amazon Inspector Code Security と GitHub SaaS、GitHub Enterprise Cloud、GitHub Enterprise Server の統合には、パブリックインターネットアクセスが必要です。

実装例

AWS SRA コードライブラリは、Amazon Inspector のサンプル実装を提供します。委任管理 (セキュリティツール) を示し、組織内のすべての AWS 既存アカウントと将来のアカウントに Amazon Inspector を設定します。

AWS Security Incident Response

AWS Security Incident Response は、 AWS 環境のセキュリティインシデントの準備と対応に役立つサービスです。検出結果をトリアージし、 はセキュリティイベントをエスカレートします。と は、即時対応が必要なケースを管理します。 さらに、 これにより、顧客インシデント対応チーム (CIRT) にアクセスできます AWS 。 は、影響を受けるリソースを調査します。 AWS Security Incident Response は、 ドキュメント (SSM ドキュメント) を通じて AWS Systems Manager 自動応答および修復機能も提供します。 セキュリティチームが対応できるように、 から復旧します。 セキュリティインシデントをより効率的に。 AWS Security Incident Response は Amazon GuardDuty および と統合 AWS Security Hub CSPMして、セキュリティ検出結果を受け取り、自動応答を調整します。

AWS SRA では、 AWS Security Incident Response は委任管理者アカウントとして Security Tooling アカウントにデプロイされます。Security Tooling アカウントは、セキュリティサービスを運用し、セキュリティアラートとレスポンスを自動化するアカウントの目的と一致するため、選択されます。Security Tooling アカウントは、Security Hub CSPM と GuardDuty の委任管理者アカウントとしても機能します。これにより、ワークフロー管理を簡素化 AWS Security Incident Responseできます。 AWS Security Incident Response は と連携するように設定されているため AWS Organizations、Security Tooling アカウントから組織のアカウント全体のインシデント対応を管理できます。

AWS Security Incident Response は、インシデント対応ライフサイクルの次のフェーズを実装するのに役立ちます。

- 準備: 封じ込めアクションの対応計画と SSM ドキュメントを作成して維持します。
- 検出と分析: セキュリティの検出結果を自動的に分析し、インシデントの重大度を判断します。
- 検出と分析: サービスがサポートするケースを開き、 AWS CIRT に連絡してサポートを依頼します。CIRT は、アクティブなセキュリティイベント中にサポートを提供する個人のグループです。
- 封じ込めと根絶: SSM ドキュメントを通じて自動封じ込めアクションを実行します。

- インシデント後アクティビティ: インシデントの詳細を文書化し、インシデント後分析を実行します。

AWS Security Incident Response を使用してセルフマネージドケースを作成することもできます。AWS Security Incident Response は、アカウントまたはリソースに影響を与える可能性のある何かを認識したり、対処したりする必要がある場合に、アウトバウンド通知またはケースを作成できます。この機能は、サブスクリプションの一部としてプロアクティブレスポンスとアラートのトリアージワークフローを有効にする場合にのみ使用できます。

設計上の考慮事項

- 実装するときは AWS Security Incident Response、自動応答アクションを本番環境で有効にする前に、慎重に確認してテストしてください。自動化はインシデント対応を高速化できますが、自動アクションの設定が適切でない場合、正当なワークロードに影響を与える可能性があります。
- で SSM ドキュメントを使用して AWS Security Incident Response 、一般的なインシデントタイプのサービスの組み込みベストプラクティスを維持しながら、組織固有の封じ込め手順を実装することを検討してください。
- VPC AWS Security Incident Response で を使用する場合は、Systems Manager やその他の統合サービス用に適切な VPC エンドポイントが設定されており、プライベートサブネットで封じ込めアクションが有効になっていることを確認してください。

すべての 内に共通のセキュリティサービスをデプロイする AWS アカウント

このリファレンスの前半のAWS 「組織全体にセキュリティサービスを適用する」セクションでは、を保護するセキュリティサービスが強調表示され AWS アカウント、これらの サービスの多くは 内で設定および管理できることに注意してください AWS Organizations。これらのサービスの一部はすべてのアカウントにデプロイする必要があり、SRA AWS に表示されます。これにより、一貫したガードレールの設定が有効になり、 AWS 組織全体の集中的なモニタリング、管理、ガバナンスが可能になります。

Security Hub CSPM、GuardDuty AWS Config、IAM Access Analyzer、および CloudTrail 組織の証跡は、すべてのアカウントに表示されます。最初の 3 つは、「管理アカウント、信頼されたアクセ

ス、委任された管理者」セクションで前述した委任管理者機能をサポートしています。CloudTrail は現在、別のアグリゲーションメカニズムを使用しています。

AWS SRA GitHub コードリポジトリは、 AWS 組織管理アカウントを含むすべてのアカウントで Security Hub CSPM、GuardDuty AWS Config AWS Firewall Manager、および CloudTrail 組織の証跡を有効にするサンプル実装を提供します。

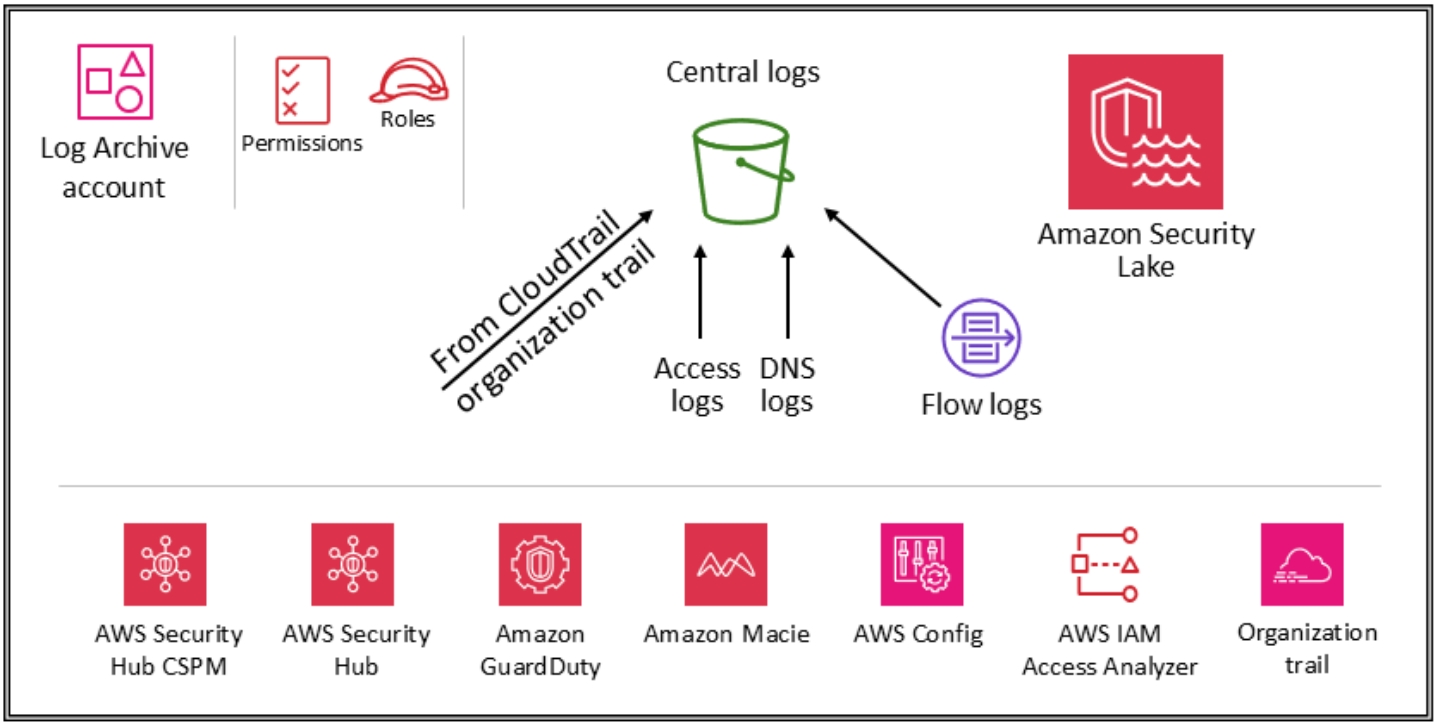
設計上の考慮事項

- 特定のアカウント設定では、追加のセキュリティサービスが必要になる場合があります。例えば、S3 バケットを管理するアカウント (アプリケーションアカウントとログアーカイブアカウント) には Amazon Macie も含め、これらの一般的なセキュリティサービスで CloudTrail S3 データイベントのログ記録を有効にすることを検討する必要があります。(Macie は、一元化された設定とモニタリングによる委任管理をサポートします。) もう 1 つの例は Amazon Inspector です。これは、EC2 インスタンスまたは Amazon ECR イメージをホストするアカウントにのみ適用されます。
- このセクションで前述したサービスに加えて、 AWS SRA には、 AWS Organizations 統合と委任された管理者機能をサポートする Amazon Detective と の AWS Audit Manager 2 つのセキュリティに焦点を当てたサービスが含まれています。ただし、これらのサービスは以下のシナリオで最適に使用されていることがわかっているため、アカウントベースラインの推奨サービスには含まれていません。
  - これらの機能を実行する専用のチームまたはリソースグループがあります。Detective はセキュリティアナリストチームが最適に活用でき、Audit Manager は内部監査またはコンプライアンスチームに役立ちます。
  - プロジェクトの開始時に GuardDuty や Security Hub CSPM などのツールのコアセットに重点を置き、追加の機能を提供するサービスを使用してこれらを構築したいと考えています。

セキュリティ OU — ログアーカイブアカウント

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は、ログアーカイブアカウントで設定されている AWS セキュリティサービスを示しています。



ログアーカイブアカウントは、セキュリティ関連のすべてのログとバックアップの取り込みとアーカイブ専用です。一元化されたログを使用すると、Amazon S3 オブジェクトアクセス、ID による不正なアクティビティ、IAM ポリシーの変更、および機密リソースで実行されるその他の重要なアクティビティをモニタリング、監査、およびアラートを実行できます。セキュリティの目的はシンプルです。これは不変のストレージであり、制御、自動化、モニタリングされたメカニズムによってのみ、イミュータブルに保存、アクセスされ、耐久性のために構築されている必要があります (適切なレプリケーションおよびアーカイブプロセスの使用などによる) 。ログとログ管理プロセスの整合性と可用性を保護するために、コントロールを詳細に実装できます。アクセスに使用する最小特権ロールの割り当てや、制御された AWS KMS キーによるログの暗号化などの予防的コントロールに加えて、 などの検出コントロールを使用して、予期しない変更がないかこのアクセス許可のコレクション AWS Config をモニタリング (および警告して修正) します。

> **設計上の考慮事項**
>
> インフラストラクチャ、オペレーション、およびワークロードチームが使用するオペレーションログデータは、多くの場合、セキュリティ、監査、コンプライアンスチームが使用するログデータと重複します。オペレーションログデータを ログアーカイブアカウントに統合することをお勧めします。特定のセキュリティおよびガバナンス要件に基づいて、このアカウントに保存されたオペレーションログデータをフィルタリングする必要がある場合があり

ます。また、ログアーカイブアカウントのオペレーションログデータにアクセスできるユーザーを指定する必要がある場合もあります。

ログの種類

AWS SRA に表示されるプライマリログには、 AWS CloudTrail (組織証跡) 、Amazon VPC フローログ、Amazon CloudFront および からのアクセスログ AWS WAF、Amazon Route 53 からの DNS ログが含まれます。これらのログは、ユーザー、ロール、またはネットワークエンティティ (IP アドレスなどで識別) によって実行 (AWS のサービスまたは試行) されたアクションの監査を提供します。他のログタイプ (アプリケーションログやデータベースログなど) もキャプチャ、アーカイブすることができます。ログソースおよびログのベストプラクティスの詳細については、各サービスのセキュリティドキュメント を参照してください。

中央ログストアとしての Amazon S3

多くの AWS のサービス ログ情報は、デフォルトでも排他的にも Amazon S3 に記録されます。AWS CloudTrail、Amazon VPC フローログ、Elastic Load Balancing、Amazon GuardDuty、および AWS WAF は AWS Config、Amazon S3 で情報をログに記録するサービスの例です。つまり、ログの整合性は S3 オブジェクトの整合性を通じて達成され、ログの機密性は S3 オブジェクトのアクセスコントロールを通じて達成され、ログの可用性は S3 オブジェクトロック、S3 オブジェクトバージョン、S3 ライフサイクルルールを通じて達成されます。専用アカウントにある専用の一元化された S3 バケットに情報をログ記録することで、これらのログをわずか数個のバケットで管理し、厳格なセキュリティコントロール、アクセス、職務の分離を適用できます。

AWS SRA では、Amazon S3 に保存されているプライマリログは CloudTrail から取得されるため、このセクションではこれらのオブジェクトを保護する方法について説明します。このガイダンスは、独自のアプリケーションまたは他のアプリケーションによって作成された他の S3 オブジェクトにも適用されます AWS のサービス。これらのパターンは、Amazon S3 に高い整合性、強力なアクセスコントロール、自動保持または破棄を必要とするデータがあるたびに適用します。

S3 バケットにアップロードされたすべての新しいオブジェクト (CloudTrail ログを含む) は、Amazon S3 S3-managed暗号化キー (SSE-S3) による Amazon サーバー側の暗号化を使用してデフォルトで暗号化されます。これにより、保管中のデータを保護することができますが、アクセスコントロールは IAM ポリシーによってのみ制御されます。追加のマネージドセキュリティレイヤーを提供するには、すべてのセキュリティ S3 バケットで管理する AWS KMS キー (SSE-KMS) でサーバー側の暗号化を使用できます。これにより、第 2 レベルのアクセスコントロールが追加されます。ログファイルを読み取るには、ユーザーは Amazon S3 S3 読み取りアクセス許可と、関連付

けられたキーポリシーによる復号化を許可する IAM ポリシーまたはロールの両方を持っている必要があります。

2 つのオプションは、Amazon S3 に保存されている CloudTrail ログオブジェクトの整合性を保護または検証するのに役立ちます。CloudTrail は、CloudTrail がログファイルを配信した後にログファイルが変更または削除されたかどうかを判断するためのログファイルの整合性検証を提供します。CloudTrail もう 1 つのオプションは S3 オブジェクトロックです。

S3 バケット自体を保護するだけでなく、ログ記録サービス (CloudTrail など) とログアーカイブアカウントの最小特権の原則に従うことができます。例えば、 AWS マネージド IAM ポリシーによって付与されたアクセス許可を持つユーザーは`AWSCloudTrail_FullAccess`、その中で最も機密性が高く重要な監査機能を無効化または再設定できます AWS アカウント。この IAM ポリシーの適用は、できるだけ少ない人数に制限してください。

AWS Config や IAM Access Analyzer によって提供されるような検出コントロールを使用して、この広範な予防コントロールの集合をモニタリング (および警告して修正) して、予期しない変更がないか調べます。

S3 バケットのセキュリティのベストプラクティスの詳細については、Amazon S3 ドキュメント、オンライン技術トーク、ブログ記事Amazon S3 でデータを保護するためのセキュリティのベストプラクティスのトップ 10」を参照してください。

> 実装例
>
> AWS SRA コードライブラリは、Amazon S3 ブロックアカウントのパブリックアクセスのサンプル実装を提供します。このモジュールは、 AWS 組織内のすべての既存および将来のアカウントの Amazon S3 パブリックアクセスをブロックします。

Amazon Security Lake

AWS SRA では、Amazon Security Lake の委任管理者アカウントとして Log Archive アカウントを使用することをお勧めします。これを行うと、Security Lake は、他の SRA が推奨するセキュリティログと同じアカウントの専用 S3 バケットでサポートされているログを収集します。

ログの可用性とログ管理プロセスを保護するために、Security Lake の S3 バケットには、Security Lake サービス、またはソースまたはサブスクライバーの Security Lake によって管理される IAM ロールのみがアクセスする必要があります。アクセス用の最小特権ロールの割り当て、制御された AWS KMS キーによるログの暗号化などの予防コントロールの使用に加えて、 などの検出コント

ロールを使用して、このアクセス許可のコレクション AWS Config を予期しない変更がないかモニタリング (およびアラートと修正) します。

Security Lake 管理者は、 AWS 組織全体でログ収集を有効にできます。これらのログは、ログアーカイブアカウントのリージョン S3 バケットに保存されます。さらに、ログを一元化し、ストレージと分析を容易にするために、Security Lake 管理者は、すべてのリージョンの S3 バケットからのログが統合および保存される 1 つ以上のロールアップリージョンを選択できます。サポートされている からのログ AWS のサービス は、Open Cybersecurity Schema Framework (OCSF) と呼ばれる標準化されたオープンソーススキーマに自動的に変換され、Security Lake S3 バケットの Apache Parquet 形式で保存されます。OCSF サポートにより、Security Lake は およびその他のエンタープライズセキュリティソースのセキュリティデータを効率的に正規化 AWS して統合し、セキュリティ関連情報の統合され信頼性の高いリポジトリを作成します。

Security Lake は、Amazon S3 および AWS CloudTrail の管理イベントと CloudTrail データイベントに関連付けられたログを収集できます AWS Lambda。Security Lake で CloudTrail 管理イベントを収集するには、CloudTrail 管理イベントの読み取りと書き込みを収集する CloudTrail マルチリージョン組織の証跡が少なくとも 1 つ必要です。 トレイルのロギングが有効になっている必要があります。マルチリージョン証跡は、複数のリージョンから単一の の単一の S3 バケットにログファイルを配信します AWS アカウント。リージョンが異なる国にある 場合は、データエクスポート要件を検討して、マルチリージョン証跡を有効にできるかどうかを判断します。

AWS Security Hub CSPM は Security Lake でサポートされているネイティブデータソースであるため、Security Hub CSPM の検出結果を Security Lake に追加する必要があります。Security Hub CSPM は、さまざまな AWS のサービス およびサードパーティーの統合から検出結果を生成します。これらの検出結果は、コンプライアンス体制の概要と、 AWS および AWS Partner ソリューションのセキュリティ推奨事項に従っているかどうかを把握するのに役立ちます。

ログやイベントから可視性と実用的なインサイトを得るには、Amazon Athena、Amazon OpenSearch Service、Amazon Quick、サードパーティーソリューションなどのツールを使用してデータをクエリできます。Security Lake ログデータへのアクセスを必要とするユーザーは、ログアーカイブアカウントに直接アクセスしないでください。Security Tooling アカウントからのみデータにアクセスする必要があります。または、OpenSearch Service AWS アカウント 、Quick、またはセキュリティ情報およびイベント管理 (SIEM) ツールなどのサードパーティーツールなどの分析ツールを提供する他の場所やオンプレミスの場所を使用することもできます。データへのアクセスを提供するには、管理者はログアーカイブアカウントで Security Lake サブスクライバーを設定し、データへのアクセスを必要とするアカウントをクエリアクセスサブスクライバーとして設定する必要があります。詳細については、このガイドの Security OU – Security Tooling アカウントセクションの「Amazon Security Lake」を参照してください。

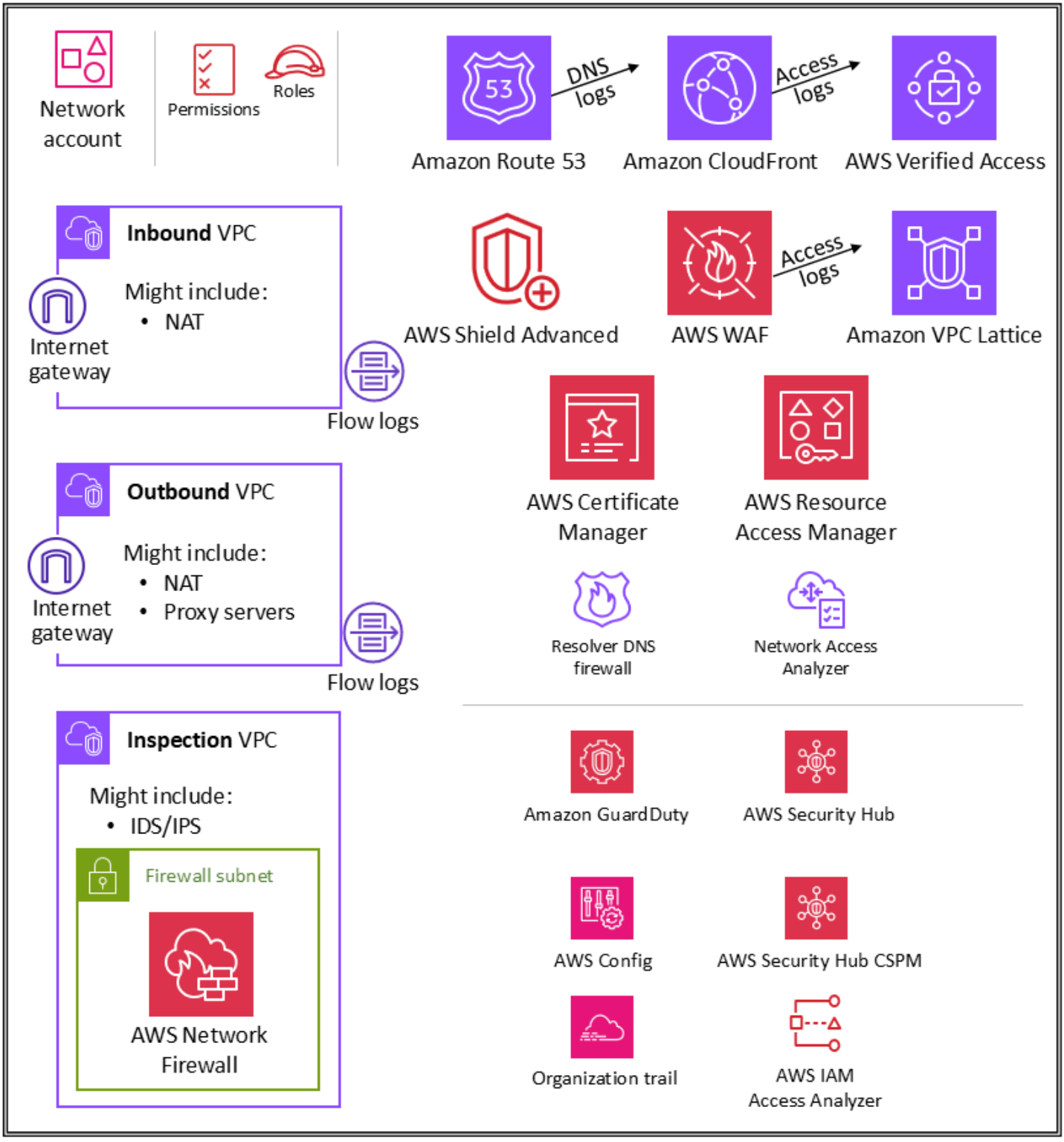
Security Lake には、サービスへの管理者アクセスの管理に役立つ AWS マネージドポリシーが用意されています。詳細については、Security Lake ユーザーガイドを参照してください。ベストプラクティスとして、開発パイプラインを通じて Security Lake の設定を制限し、 AWS コンソールまたは AWS Command Line Interface () を通じて設定の変更を防ぐことをお勧めしますAWS CLI。さらに、Security Lake を管理するために必要なアクセス許可のみを提供するように、厳格な IAM ポリシーとサービスコントロールポリシー (SCPs) を設定する必要があります。これらの S3 バケットへの直接アクセスを検出するように通知を設定できます。

> **設計上の考慮事項**
>
> Security Lake で CloudTrail 管理イベントを有効にすると、Security Lake の料金が発生します。Security Lake での CloudTrail 管理イベントのコレクションには、CloudTrail 管理イベントの読み取りと書き込みを収集する CloudTrail マルチリージョン組織の証跡が必要です。この最初の証跡は無料で利用できます。CloudTrail 管理イベントは通常、CloudTrail イベント全体のごく一部 (約 5%) を占めます。これは、 を使用するか、ログアーカイブアカウントに一元化された CloudTrail ログ AWS Control Tower があるお客様に適用されます。

インフラストラクチャ OU — ネットワークアカウント

簡単なアンケートに回答して、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は、ネットワークアカウントで設定されている AWS セキュリティサービスを示しています。



Network アカウントは、アプリケーションとより広範なインターネット間のゲートウェイを管理しています。その双方向インターフェイスを保護することが重要です。Network アカウントは、個々のアプリケーションワークロード、セキュリティ、およびその他のインフラストラクチャからネットワー

クサービス、構成、およびオペレーションを分離します。この配置は、接続性、権限、およびデータフローを制限するだけでなく、これらのアカウントで運用する必要があるチームの職務分離と最小権限もサポートします。ネットワークフローを個別のインバウンドとアウトバウンドの仮想プライベートクラウド (VPC) に分割することで、機密性の高いインフラストラクチャとトラフィックを不用意なアクセスから保護できます。インバウンドネットワークは一般的に高いリスクと考えられ、適切なルーティング、モニタリング、および潜在的な問題の軽減が必要です。これらのインフラストラクチャアカウントは、Org Management アカウントとインフラストラクチャ OU から権限ガードレールを継承します。ネットワーキング (およびセキュリティ) チームは、このアカウントのインフラストラクチャの大部分を管理します。

ネットワークアーキテクチャ

ネットワーク設計と詳細はこのドキュメントの範囲外ですが、さまざまなアカウント間のネットワーク接続には、VPC ピアリングと AWS PrivateLinkの 3 つのオプションをお勧めします AWS Transit Gateway。これらの中から選択する際の重要な考慮事項は、運用規範、予算、および特定の帯域幅のニーズです。

- VPC ピアリング — 2 つの VPC を接続する最も簡単な方法は、VPC ピアリングを使用することです。接続することで、VPC 間の完全な双方向接続が可能になります。別々のアカウントにあり、ピア接続 AWS リージョン もできる VPCs。スケールでは、数十から数百の VPC がある場合、それらをピアリングと相互接続すると、数百から数千のピアリング接続のメッシュとなり、管理やスケールが困難になる可能性があります。VPC ピアリングは、ある VPC のリソースが別の VPC のリソースと通信する必要があり、両方の VPC の環境が制御およびセキュリティで保護され、接続する VPC の数が 10 未満の場合 (各接続の個別の管理を可能にする) に最適です。
- AWS PrivateLink – PrivateLink はVPCs、サービス、アプリケーション間のプライベート接続を提供します。VPC で独自のアプリケーションを作成し、PrivateLink を使用するサービス (エンドポイントサービスといいます) として設定できます。他の AWS プリンシパルは、サービスのタイプに応じて、インターフェイス VPC エンドポイントまたは Gateway Load Balancer エンドポイントを使用して、VPC からエンドポイントサービスへの接続を作成できます。PrivateLink を使用する場合、サービストラフィックは一般にルーティング可能なネットワークを通過しません。クライアント・サーバーの設定で、1 つまたは複数のコンシューマー VPC に、サービスプロバイダー VPC 内の特定のサービスまたはインスタンスのセットに一方的にアクセスさせたい場合、PrivateLink を使用します。また、2 つの VPC 内のクライアントとサーバに IP アドレスが重複している場合、PrivateLink はクライアント VPC 内の 伸縮自在のネットワークインターフェイスを使用しており、サービスプロバイダーと IP の競合が発生しないため、このオプションも適しています。

- AWS Transit Gateway – Transit Gateway は、hub-and-spoke設計を提供します。 は、高可用性とスケーラビリティ AWS を管理します。 VPCs トランジットゲートウェイはリージョンのリソースであり、同じ 内の何千もの VPCs を接続できます AWS リージョン。ハイブリッド接続 (VPN と AWS Direct Connect 接続) を単一のトランジットゲートウェイにアタッチできるため、 AWS 組織のルーティング設定全体を 1 か所に統合して制御できます。Transit gateway は、複数の VPC ピアリング接続を大規模に作成および管理する際の複雑さを解決します。これは、ほとんどのネットワークアーキテクチャではデフォルトですが、コスト、帯域幅、レイテンシーに関する特定のニーズでは、VPC ピアリングがより適切かもしれません。

インバウンド (受信) VPC

インバウンド VPC は、アプリケーション外から開始されたネットワーク接続を受け入れ、検査し、ルーティングすることを目的としています。アプリケーションの特性にもよりますが、この VPC ではネットワークアドレス変換 (NAT) が行われることが期待できます。この VPC からのフローログはキャプチャされ、Log Archive アカウントに保存されます。

アウトバウンド (送信) VPC

アウトバウンド VPC は、アプリケーション内から開始されたネットワーク接続を処理することを目的としています。アプリケーションの詳細によっては、トラフィック NAT、 AWS のサービス固有の VPC エンドポイント、およびこの VPC 内の外部 API エンドポイントのホスティングが表示されることが予想されます。この VPC からのフローログはキャプチャされ、Log Archive アカウントに保存されます。

インスペクション VPC

専用検査 VPC は、VPCs (同一または異なる AWS リージョン)、インターネット、オンプレミスネットワーク間の検査を管理するための簡素化された一元的なアプローチを提供します。 AWS SRA の場合、VPCs 間のすべてのトラフィックが検査 VPC を通過し、検査 VPC を他のワークロードに使用しないようにします。

AWS Network Firewall

AWS Network Firewall は、VPC 用の高可用性のマネージドネットワークファイアウォールサービスです。これにより、ステートフルインスペクション、侵入防止と検出、ウェブフィルタリングを簡単にデプロイおよび管理して、仮想ネットワークを保護できます AWS。Network Firewall を使用して TLS セッションを復号し、インバウンドトラフィックとアウトバウンドトラフィックを検査できま

す。Network Firewall の設定の詳細については、VPC のブログ記事AWS Network Firewall 「 — New Managed Firewall Service」を参照してください。

VPC では、アベイラビリティーゾーンごとにファイアウォールを使用します。アベイラビリティーゾーンごとに、トラフィックをフィルタリングするファイアウォールエンドポイントをホストするサブネットを選択します。アベイラビリティーゾーンのファイアウォールエンドポイントは、ゾーンが存在するサブネットを除くゾーン内のすべてのサブネットを保護できます。ユースケースとデプロイメントモデルに応じて、ファイアウォールサブネットはパブリックまたはプライベートのいずれかになります。ファイアウォールは、トラフィックフローに対して完全に透過的であり、NAT を実行しません。送信元と送信先のアドレスが保持されます。このリファレンスアーキテクチャでは、ファイアウォールエンドポイントはインスペクション VPC でホストされています。インバウンド VPC からとアウトバウンド VPC へのすべてのトラフィックは、検査のためにこのファイアウォールサブネットを介してルーティングされます。

Network Firewall はAmazon CloudWatch メトリクスを通じてファイアウォールアクティビティをリアルタイムで表示し、Amazon Simple Storage Service (Amazon S3)、CloudWatch、Amazon Data Firehose にログを送信することで、ネットワークトラフィックの可視性を向上させます。Network Firewall は、AWS Partners の技術を含む、お客様の既存のセキュリティアプローチと相互運用が可能です。既存の Suricata ルールセットをインポートすることもでき、ルールセットは内部で作成されたものや、サードパーティのベンダーまたはオープンソースプラットフォームから外部調達されているものである場合があります。

AWS SRA では、Network Firewall はネットワークアカウント内で使用されます。これは、サービスのネットワーク制御に焦点を当てた機能がアカウントのインテントと一致するためです。

設計上の考慮事項

- AWS Firewall Manager は Network Firewall をサポートしているため、組織全体で Network Firewall ルールを一元的に設定してデプロイできます。(詳細については、 AWS ドキュメントの「Firewall Manager での AWS Network Firewall ポリシーの使用」を参照してください。) Firewall Manager を構成すると、指定したアカウントと VPC に一連のルールを持つファイアウォールが自動的に作成されます。また、パブリックサブネットを含むすべてのアベイラビリティーゾーンの専用サブネットにエンドポイントをデプロイします。同時に、集中的に構成された一連のルールに変更があった場合、デプロイされた Network Firewall ファイヤウォールの下流で自動的に更新されます。
- Network Firewall には、複数のデプロイモデル が用意されています。適切なモデルは、ユースケースと要件によって異なります。次に例を示します。
  - Network Firewall を個々の VPC にデプロイする配信型デプロイモデル。

- 中央集中型デプロイモデルで、そこでは Network Firewall が東西 (VPC 間) または南北 (インターネット送信および受信、オンプレミス) のトラフィック用に集中型 VPC にデプロイされます。
- Network Firewall を東西と南北のトラフィックのサブセット用に中央集中型 VPC にデプロイした複合型デプロイモデル。

- ベストプラクティスとして、Network Firewall サブネットを使用して他のサービスをデプロイしないでください。これは、Network Firewall がファイアウォールサブネット内の送信元または発信先からのトラフィックを検査できないためです。

Network Access Analyzer

Network Access Analyzer は Amazon VPC の機能で、リソースへの意図しないネットワークアクセスを特定します。Network Access Analyzer を使用すると、ネットワークのセグメンテーションを検証し、インターネットからアクセスできるリソースや信頼できる IP アドレス範囲からのみアクセスできるリソースを特定し、すべてのネットワークパスで適切なネットワーク制御が行われていることを検証できます。

Network Access Analyzer は、自動推論アルゴリズムを使用して、パケットがネットワーク内のリソース間で実行できる AWS ネットワークパスを分析し、定義された Network Access Scope に一致するパスの検出結果を生成します。Network Access Analyzer はネットワーク構成の静的な分析を行います。つまり、この分析の一環としてネットワーク内でパケットが送信されることはありません。

Amazon Inspector Network Reachability ルールが、関連する機能を提供します。これらのルールによって生成された結果は Application アカウントで使用されます。Network Access Analyzer と Network Reachability はどちらもAWS 、実証済みのセキュリティイニシアチブの最新テクノロジーを使用し、このテクノロジーをさまざまな重点分野に適用します。Network Reachability パッケージは、特に EC2 インスタンスとそのインターネットアクセシビリティに重点を置いています。

ネットワークアカウントは、 AWS 環境に出入りするトラフィックを制御する重要なネットワークインフラストラクチャを定義します。このトラフィックは厳重に監視する必要があります。 AWS SRA では、Network Access Analyzer はネットワークアカウント内で使用され、意図しないネットワークアクセスの識別、インターネットゲートウェイを介したインターネットアクセス可能なリソースの識別、ネットワークファイアウォールや NAT ゲートウェイなどの適切なネットワークコントロールがリソースとインターネットゲートウェイ間のすべてのネットワークパスに存在することを確認します。

設計上の考慮事項

Network Access Analyzer は Amazon VPC の機能であり、VPC AWS アカウント を持つ任意の で使用できます。ネットワーク管理者は、厳密にスコープされたクロスアカウント IAM ロールを取得して、承認されたネットワークパスが各ロール内に強制されていることを検証できます AWS アカウント。

AWS RAM

AWS Resource Access Manager (AWS RAM) を使用すると、1 つの で作成した AWS リソースを他の AWS アカウント と安全に共有できます AWS アカウント。AWS RAM は、リソースの共有を管理し、アカウント間でこのエクスペリエンスを標準化するための一元的な場所を提供します。これにより、管理上および請求上の分離を活用しながらリソースの管理を容易に行うことで、マルチアカウント戦略によってもたらされる影響抑制のメリットの範囲が狭まります。アカウントが によって管理されている場合 AWS Organizations、 AWS RAM は組織内のすべてのアカウント、または 1 つ以上の指定された組織単位 (OUs。アカウントが組織の一部であるかどうかにかかわらず、アカウント ID AWS アカウント ごとに特定の と共有することもできます。サポートされているリソースタイプの一部 は、指定した IAM ロールおよびユーザーと共有もできます。

AWS RAM では、VPC サブネットや Route 53 ルールなど、IAM リソースベースのポリシーをサポートしていないリソースを共有できます。さらに、リソースの所有者は AWS RAM、共有した個々のリソースにアクセスできるプリンシパルを確認できます。IAM プリンシパルは、共有されているリソースのリストを直接取得できます。これは、IAM リソースポリシーによって共有されているリソースとは関係ありません。 AWS RAM を使用して AWS 組織外のリソースを共有する場合、招待プロセスが開始されます。受信者は、リソースへのアクセスを許可する前に招待を受け入れる必要があります。これにより、追加のチェックと残高が提供されます。

AWS RAM は、共有リソースがデプロイされているアカウントで、リソース所有者によって呼び出され、管理されます。SRA AWS に AWS RAM 示されている の一般的なユースケースの 1 つは、ネットワーク管理者が VPC サブネットとトランジットゲートウェイ AWS を組織全体と共有することです。これにより、 AWS アカウント とネットワーク管理機能を切り離すことができ、職務の分離に役立ちます。VPC 共有の詳細については、 AWS ブログ記事「VPC 共有: 複数のアカウントと VPC 管理に対する新しいアプローチ」およびAWS 「ネットワークインフラストラクチャ」ホワイトペーパーを参照してください。

設計上の考慮事項

AWS RAM サービスは AWS SRA のネットワークアカウント内にのみデプロイされますが、通常は複数のアカウントにデプロイされます。たとえば、データレイク管理を単一のデータレイクアカウントに一元化し、 AWS Lake Formation データカタログリソース (データベースとテーブル) を AWS 組織内の他のアカウントと共有できます。詳細については、「 AWS Lake Formation ドキュメント」および AWS 「 ブログ記事」を参照してください AWS アカウントAWS Lake Formation。さらに、セキュリティ管理者は、 AWS RAM を使用して AWS Private Certificate Authority 階層を構築するときにベストプラクティスに従うことができます。CAsは、CA 階層にアクセスせずに証明書を発行できる外部のサードパーティーと共有できます。これにより、発信元の組織は第三者のアクセスを制限したり取り消したりすることができます。

AWS Verified Access

AWS Verified Access は、VPN なしで企業のアプリケーションとリソースへの安全なアクセスを提供します。これにより、セキュリティ体制が強化され、事前定義された要件に照らして各アクセスリクエストをリアルタイムで評価することで、ゼロトラストアクセスを適用できます。ID データ および デバイスポスチャ に基づく条件を使用して、アプリケーションごとに固有のアクセスポリシーを定義できます。Verified Access は、ブラウザベースのアプリケーションなどの HTTP(S) アプリケーション、および Git リポジトリ、データベース、EC2 インスタンスのグループなどのアプリケーションの TCP、SSH、RDP プロトコルを介した非 HTTP(S) アプリケーションへの安全なアクセスを提供します。これらは、コマンドラインターミナルを使用するか、デスクトップアプリケーションからアクセスできます。また、Verified Access は、管理者がアクセスポリシーを効率的に設定して監視できるようにすることで、セキュリティ運用を簡素化します。これにより、ポリシーの更新、セキュリティや接続に関するインシデントへの対応、コンプライアンス基準の監査のための時間が確保されます。Verified Access は、SQL インジェクションやクロスサイトスクリプティング (XSS) などの一般的な脅威を除外 AWS WAF するのに役立つ との統合もサポートしています。Verified Access は とシームレスに統合されているため AWS IAM アイデンティティセンター、ユーザーは SAML ベースのサードパーティー ID プロバイダー (IdPs で認証できます。OpenID Connect (OIDC) と互換性のあるカスタム IdP ソリューションをすでに使用している場合、Verified Access は IdP に直接接続してユーザーを認証することもできます。Verified Access はすべてのアクセス試行を口グに記録するため、セキュリティインシデントや監査請求に迅速に対応できます。Verified Access は、Amazon Simple Storage Service (Amazon S3)、Amazon CloudWatch Logs、Amazon Data Firehose へのこれらのログの配信をサポートしています。

Verified Access は、社内用とインターネット向けの 2 つの一般的な企業アプリケーションパターンをサポートします。Verified Access は、Application Load Balancer またはエラスティックネットワークインターフェースを使用してアプリケーションと統合します。Application Load Balancer を使用している場合、Verified Access には内部ロードバランサーが必要です。Verified Access は AWS WAF インスタンスレベルで をサポートしているため、Application Load Balancer と統合されている既存のアプリケーションは AWS WAF 、ロードバランサーから Verified Access インスタンスにポリシーを移動できます。企業アプリケーションは Verified Access エンドポイントとして表されます。各エンドポイントは Verified Access グループに関連付けられ、グループのアクセスポリシーを継承します。Verified Access グループは、Verified Access エンドポイントとグループレベルの Verified Access ポリシーの集合です。グループはポリシー管理を簡素化し、IT 管理者がベースライン基準を設定できるようにします。アプリケーション所有者は、アプリケーションの機密性に応じて、さらに詳細なポリシーを定義できます。

AWS SRA では、Verified Access はネットワークアカウント内でホストされます。中央の IT チームが、一元管理された構成を設定します。例えば、ID プロバイダー (Okta など) とデバイストラストプロバイダー (Jamf など) などの信頼プロバイダーを接続し、グループを作成し、グループレベルのポリシーを決定する場合があります。これらの設定は、 を使用して数十、数百、または数千のワークロードアカウントと共有できます AWS RAM。これにより、アプリケーションチームは、他のチームのオーバーヘッドなしでアプリケーションを管理する基盤となるエンドポイントを管理できます。 は、さまざまなワークロードアカウントでホストされている企業アプリケーションに Verified Access を活用するスケーラブルな方法 AWS RAM を提供します。

> **設計上の考慮事項**
>
> ポリシー管理を簡素化するために、同様のセキュリティ要件を持つアプリケーションのエンドポイントをグループ化し、そのグループをアプリケーションアカウントと共有できます。グループ内のすべてのアプリケーションはグループポリシーを共有します。エッジケースのためにグループ内のアプリケーションが特定のポリシーを必要とする場合は、そのアプリケーションにアプリケーションレベルのポリシーを適用できます。

Amazon VPC Lattice

Amazon VPC Lattice は、service-to-service通信を接続、モニタリング、保護するアプリケーションネットワークサービスです。マイクロサービスと呼ばれるサービスは、特定のタスクを配信するソフトウェアの独立したデプロイ可能なユニットです。VPC Lattice は、基盤となるネットワーク接続、フロントエンドロードバランサー、またはサイドカープロキシを管理する AWS アカウント ことなく、VPCs 間のサービス間のネットワーク接続とアプリケーションレイヤールーティングを自動的に

管理します。パスやヘッダーなどのリクエスト特性に基づいてアプリケーションレベルのルーティングを行う、フルマネージド型のアプリケーションレイヤープロキシを提供します。VPC Lattice は VPC インフラストラクチャに組み込まれているため、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Kubernetes Service (Amazon EKS)、 などの幅広いコンピューティングタイプにわたって一貫したアプローチを提供します AWS Lambda。VPC Lattice は、ブルー/グリーンおよび canary スタイルのデプロイメント用の加重ルーティングもサポートしています。VPC Lattice を使用して、サービスの検出と接続を自動的に実装する論理境界を持つサービスネットワークを作成できます。VPC Lattice は IAM と統合され、service-to-service認証と認可を行います。

VPC Lattice は と統合 AWS RAM され、サービスとサービスネットワークの共有を可能にします。AWS SRA は、開発者またはサービス所有者がアプリケーションアカウントに VPC Lattice サービスを作成する分散アーキテクチャを示しています。サービスオーナーは、リスナー、ルーティングルール、ターゲットグループを認証ポリシーとともに定義します。次に、サービスを他のアカウントと共有し、そのサービスを VPC Lattice サービスネットワークに関連付けます。これらのネットワークは、ネットワーク管理者が Network アカウントで作成し、Application アカウントと共有します。ネットワーク管理者は、サービスのネットワークレベルの認証ポリシーと監視を設定します。管理者は VPC と VPC Lattice サービスを 1 つ以上のサービスネットワークに関連付けます。この分散アーキテクチャの詳細なチュートリアルについては、 AWS ブログ記事「Amazon VPC Lattice を使用してアプリケーションに安全なマルチアカウントマルチ VPC 接続を構築する」を参照してください。

設計上の考慮事項

- 組織のサービスまたはサービスネットワークの可視性の運用モデルに応じて、ネットワーク管理者はサービスネットワークを共有し、サービスと VPCs をこれらのサービスネットワークに関連付けるためのコントロールをサービス所有者に付与できます。また、サービスオーナーはサービスを共有し、ネットワーク管理者はサービスをサービスネットワークに関連付けることができます。
- クライアントは、同じサービスネットワークに関連付けられている VPC 内にある場合に限り、サービスネットワークに関連付けられたサービスにリクエストを送信できます。VPC ピアリング接続またはトランジットゲートウェイを通過するクライアントトラフィックは拒否されます。

エッジセキュリティ

エッジセキュリティには通常、安全なコンテンツ配信、ネットワーク層とアプリケーション層の保護、分散型サービス拒否 (DDoS) の緩和という 3 種類の保護が必要です。データ、動画、アプリ

ケーション、API などのコンテンツは、エンドポイント間の通信を暗号化する TLS 推奨バージョンを使用して、迅速かつ安全に配信する必要があります。コンテンツには、署名付き URL、署名付き Cookie、トークン認証によるアクセス制限も必要です。アプリケーションレベルのセキュリティは、ボットトラフィックを制御し、SQL インジェクションやクロスサイトスクリプティング (XSS) などの一般的な攻撃パターンをブロックし、Web トラフィックを可視化するように設計する必要があります。エッジでは、DDoS 対策がミッションクリティカルな事業運営やサービスの継続的な可用性を確保する重要な防御層を提供します。アプリケーションと API を SYN フラッド、UDP フラッド、またはその他のリフレクション攻撃から保護し、基本的なネットワーク層攻撃を阻止するためのインライン緩和を備えている必要があります。

AWS は、コアクラウドから AWS ネットワークのエッジまで、安全な環境を提供するのに役立ついくつかのサービスを提供します。Amazon CloudFront、 AWS Certificate Manager (ACM) AWS Shield AWS WAF、および Amazon Route 53 は連携して、柔軟でレイヤー化されたセキュリティ境界を作成します。CloudFront では、コンテンツ、APIs、またはアプリケーションは、TLSv1.3 を使用してビューワークライアントと CloudFront 間の通信を暗号化して保護することで、HTTPS 経由で配信できます。ACM を使用してカスタム SSL 証明書を作成し、CloudFront ディストリビューションに無料でデプロイできます。ACM は証明書の更新を自動的に処理します。Shield は、 で実行されるアプリケーションを保護するのに役立つマネージド DDoS 保護サービスです AWS。アプリケーションのダウンタイムとレイテンシーを最小限に抑える動的検出と自動インライン緩和を提供します。特定の条件 (IP アドレス、HTTP ヘッダーと本文、またはカスタム URIs)、一般的なウェブ攻撃、および広範なボットに基づいてウェブトラフィックをフィルタリングするルール AWS WAF を作成します。Amazon Route 53 は、高可用性でスケーラブルな DNS Web サービスです。Route 53 は、ユーザーリクエストを、 AWS またはオンプレミスで実行されるインターネットアプリケーションに接続します。 AWS SRA は、ネットワークアカウント内でホストされている AWS Transit Gatewayを使用して一元化されたネットワーク進入アーキテクチャを採用しているため、エッジセキュリティインフラストラクチャもこのアカウントに集中されます。

Amazon CloudFront

Amazon CloudFront は、一般的なネットワーク層とトランスポート DDoS 攻撃に対する固有の保護を提供する安全なコンテンツ配信ネットワーク (CDN) です。TLS 証明書を使用してコンテンツ、API、またはアプリケーションを配信でき、高度な TLS 機能が自動的に有効になります。 AWS Certificate Manager (ACM) を使用してカスタム TLS 証明書を作成し、ACM セクションで後述するように、ビューワーと CloudFront 間の HTTPS 通信を適用できます。 ???CloudFront とカスタムオリジン間の通信に、転送中のエンドツーエンドの暗号化を実装するようにも要求できます。このシナリオでは、TLS 証明書をオリジンサーバーにインストールする必要があります。オリジンが エラスティックロードバランサーの場合、ACM によって生成された証明書、またはサードパーティの認証機関 (CA) によって検証されて ACM にインポートされた証明書を使用できます。S3 バケット

ウェブサイトエンドポイントが CloudFront のオリジンとして機能する場合、Amazon S3 はウェブサイトエンドポイントの HTTPS をサポートしていないため、オリジンで HTTPS を使用するように CloudFront を設定することはできません。(ただし、閲覧者と CloudFront の間で HTTPS を要求することはできます)。HTTPS 証明書のインストールをサポートする他のすべてのオリジンでは、信頼できるサードパーティ CA によって署名された証明書を使用する必要があります。

CloudFront は、コンテンツへのアクセスを保護および制限するための複数のオプションを提供します。例えば、署名付き URL と署名付き Cookie を使用して、Amazon S3 オリジンへのアクセスを制限できます。詳細については、CloudFront ドキュメントの「安全なアクセスの設定」および「コンテンツへのアクセスの制限」を参照してください。

AWS SRA は、 を使用して実装される一元化されたネットワークパターンと一致するため、ネットワークアカウントの一元化された CloudFront ディストリビューションを示しています AWS Transit Gateway。Network アカウントで CloudFront ディストリビューションをデプロイして管理することで、集中管理のメリットが得られます。すべての CloudFront ディストリビューションを 1 か所で管理できるため、すべてのアカウントのアクセス制御、設定の構成、使用状況の監視が容易になります。さらに、ACM 証明書、DNS レコード、CloudFront ロギングを 1 つの集中アカウントから管理できます。

CloudFront セキュリティダッシュボードは、CloudFront ディストリビューションで直接 AWS WAF 可視性とコントロールを提供します。アプリケーションの主要なセキュリティ傾向、許可およびブロックされたトラフィック、ボットアクティビティを可視化できます。ビジュアルログアナライザーや組み込みブロッキングコントロールなどの調査ツールを使用して、ログをクエリしたりセキュリティルールを記述したりすることなく、トラフィックパターンを分離し、トラフィックをブロックできます。

設計上の考慮事項

- または、CloudFront を Application アカウントのアプリケーションの一部としてデプロイすることもできます。このシナリオでは、アプリケーションチームが CloudFront ディストリビューションのデプロイ方法などの決定を下し、適切なキャッシュポリシーを決定し、CloudFront ディストリビューションのガバナンス、監査、監視を担当します。CloudFront ディストリビューションを複数のアカウントに分散させることで、サービスクォータを増やすことができます。もう 1 つの利点として、CloudFront の固有の自動オリジンアクセスアイデンティティ (OAI) およびオリジンアクセスコントロール (OAC) 設定を使用して、Amazon S3 オリジンへのアクセスを制限できます。
- CloudFront などの CDN を介してウェブコンテンツを配信する場合、ビューワーが CDN をバイパスして、オリジンコンテンツに直接アクセスすることを防ぐ必要があります。

このオリジンアクセス制限を実現するには、CloudFront と を使用してカスタムヘッダー AWS WAF を追加し、カスタムオリジンにリクエストを転送する前にヘッダーを検証できます。このソリューションの詳細な説明については、 AWS セキュリティブログ記事「AWS WAF および を使用して Amazon CloudFront オリジンセキュリティを強化する方法 AWS Secrets Manager」を参照してください。別の方法は、Application Load Balancer に関連付けられているセキュリティグループ内の CloudFront プレフィックスリストのみを制限することです。これにより、CloudFront ディストリビューションのみがロードバランサーにアクセスできるようになります。

AWS WAF

AWS WAF は、アプリケーションの可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のある一般的な脆弱性やボットなどのウェブエクスプロイトからウェブアプリケーションを保護するのに役立つウェブアプリケーションファイアウォールです。Amazon CloudFront ディストリビューション、Amazon API Gateway REST API、Application Load Balancer、 AWS AppSync GraphQL API、Amazon Cognito ユーザープール、および AWS App Runner サービスと統合できます。

AWS WAF は、一連のリソースを保護するためにウェブアクセスコントロールリスト (ACLs) を使用します。 AWS ウェブ ACL は、検査基準を定義する一連のルールであり、ウェブリクエストが基準を満たした場合に実行する (ブロック、許可、カウント、またはボット制御を実行する) 関連アクションです。 は、一般的なアプリケーションの脆弱性に対する保護を提供する一連のマネージドルール AWS WAF を提供します。これらのルールは、 AWS および AWS パートナーによってキュレートおよび管理されます。 は、カスタムルールを作成するための強力なルール言語 AWS WAF も提供します。カスタムルールを使用して、特定のニーズに合った検査基準を記述できます。例としては、IP 制限、地理的制約、特定のアプリケーションの動作により適したカスタマイズされたマネージドルールなどがあります。

AWS WAF は、共通ボットとターゲットボット、およびアカウント乗っ取り保護 (ATP) のためのインテリジェントな階層管理ルールのセットを提供します。ボットコントロールと ATP ルールグループを使用すると、サブスクリプション料金とトラフィック検査料金がかかります。従って、最初にトラフィックを監視してから、何を使用するかを決定することをお勧めします。コンソールで AWS WAF 無料で利用できるボット管理ダッシュボードとアカウント乗っ取りダッシュボードを使用して、これらのアクティビティをモニタリングし、インテリジェント階層 AWS WAF ルールグループが必要かどうかを判断できます。

AWS SRA では、 AWS WAF はネットワークアカウントの CloudFront と統合されています。この設定では、 AWS WAF ルール処理は VPC 内ではなくエッジロケーションで行われます。これにより、コンテンツをリクエストしたエンドユーザーの近くで悪意のあるトラフィックをフィルタリングできるようになり、悪意のあるトラフィックがコアネットワークに侵入するのを防ぐことができます。

S3 バケットへのクロスアカウントアクセスを設定することで、 AWS WAF ログアーカイブアカウントの S3 バケットに完全なログを送信できます。詳細については、このトピックの AWS re:Post 記事を参照してください。

設計上の考慮事項

- ネットワークアカウントに一 AWS WAF 元的にデプロイする代わりに、 AWS WAF アプリケーションアカウントにデプロイすることで、いくつかのユースケースを満たすことができます。例えば、CloudFront ディストリビューションをアプリケーションアカウントにデプロイする場合や、公開されている Application Load Balancer がある場合、またはウェブアプリケーションの前に API Gateway を使用している場合に、このオプションを選択できます。 AWS WAF 各アプリケーションアカウントにデプロイする場合は、 を使用して、一元化された AWS WAF Security Tooling アカウントからこれらのアカウントのルール AWS Firewall Manager を管理します。
- CloudFront レイヤーに一般的な AWS WAF ルールを追加し、Application Load Balancer や API ゲートウェイなどのリージョンリソースにアプリケーション固有の AWS WAF ルールを追加することもできます。

AWS Shield

AWS Shield は、 AWSで実行されるアプリケーションを保護するマネージド DDoS 保護サービスです。Shield には、Shield Standard と Shield Advanced の 2 つの階層があります。Shield Standard は、最も一般的なインフラストラクチャ (レイヤー 3 および 4) イベントに対する保護をすべての AWS お客様に追加料金なしで提供します。Shield Advanced は、保護された Amazon EC2、Elastic Load Balancing (Elastic Load Balancing)、CloudFront AWS Global Accelerator、Route 53 ホストゾーンでアプリケーションをターゲットとする不正なイベントに対して、より高度な自動緩和を提供します。可視性の高いウェブサイトを所有している場合、または頻繁に DDoS 攻撃を受けやすい場合は、Shield Advanced が提供する追加機能を検討できます。

Shield Advanced 自動アプリケーションレイヤー DDoS 緩和機能を使用して、保護された CloudFront ディストリビューション、Elastic Load Balancing (Elastic Load Balancing) ロードバラン

サー (アプリケーション、ネットワーク、クラシック) 、Amazon Route 53 ホストゾーン、Amazon EC2 Elastic IP アドレス、および AWS Global Accelerator 標準アクセラレーターに対するアプリケーションレイヤー (レイヤー 7) 攻撃を自動的に軽減するように Shield Advanced を設定できます。この機能を有効にすると、Shield Advanced は DDoS 攻撃を軽減するためのカスタム AWS WAF ルールを自動的に生成します。Shield Advanced では、AWS Shield レスポンスチーム (SRT) にもアクセスできます。アクティブな DDoS 攻撃中は、いつでも SRT に連絡して、アプリケーションのカスタム緩和策を作成および管理できます。SRT が保護対象リソースをプロアクティブに監視し、DDoS 攻撃時に連絡を受信する必要がある場合は、プロアクティブエンゲージメント機能 を有効にすることを検討してください。

設計上の考慮事項

- CloudFront、Application Load Balancer、Network Load Balancer など、アプリケーションアカウントのインターネット向けリソースが前面にあるワークロードがある場合は、アプリケーションアカウントで Shield Advanced を設定し、それらのリソースを Shield Protection に追加します。を使用して、これらのオプション AWS Firewall Manager を大規模に設定できます。
- Application Load Balancer の前に CloudFront ディストリビューションなど、データフローに複数のリソースがある場合は、保護されたリソースとしてエントリポイントリソースのみを使用します。これにより、2 つのリソースに対して Shield Data Transfer Out (DTO) 料金を 2 回支払う必要がなくなります。
- Shield Advanced は、Amazon CloudWatch でモニタリングできるメトリクスをレコードします。(詳細については、 AWS ドキュメントのAmazon CloudWatch によるモニタリング」を参照してください。) DDoS イベントが検出されたときに、セキュリティセンターが SNS 通知を受信するように CloudWatch アラームを設定します。DDoS イベントが疑われる場合は、AWS エンタープライズサポートチームに連絡してサポートチケットを提出し、最優先事項を割り当てます。イベントを処理する際のエンタープライズサポートチームには、Shield Response Team (SRT) が含まれます。さらに、 AWS Shield エンゲージメント Lambda 関数を事前設定してサポートチケットを作成し、SRT チームに E メールを送信できます。

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) を使用すると、 および内部接続リソースで使用するパブリック TLS 証明書とプライベート TLS 証明書をプロビジョニング、管理 AWS のサービス 、デプロイで

きます。ACM を使用すると、証明書を迅速にリクエストしたり、Elastic Load Balancing ロードバランサー、CloudFront ディストリビューション、Amazon API Gateway の APIs などの ACM 統合 AWS リソースにデプロイしたり、ACM が証明書の更新を処理したりできます。ACM パブリック証明書をリクエストする場合、キーペアや証明書署名リクエスト (CSR) を生成したり、CSR を認証局 (CA) に送信したり、証明書を受信したときにアップロードしてインストールしたりする必要はありません。ACM には、サードパーティ CA が発行した TLS 証明書をインポートして ACM 統合サービスにデプロイするオプションもあります。ACM を使用して証明書を管理する場合、証明書のプライベートキーは強力な暗号化とキー管理のベストプラクティスを使用して安全に保護され、保存されます。ACM では、パブリック証明書のプロビジョニングに追加料金は発生せず、ACM が更新プロセスを管理します。

ACM は Network アカウントでパブリック TLS 証明書を生成するために使用され、次に CloudFront ディストリビューションはこの証明書を使用してビューワーと CloudFront 間の HTTPS 接続を確立します。詳細については、「CloudFront ドキュメント」を参照してください。

> **設計上の考慮事項**
>
> 外部向け証明書の場合、ACM は証明書をプロビジョニングするリソースと同じアカウントに存在する必要があります。アカウント間で証明書を共有することはできません。

Amazon Route 53

Amazon Route 53 は、高可用性でスケーラブルな DNS ウェブサービスです。Route 53 を使用すると、ドメイン登録、DNS ルーティング、ヘルスチェックの 3 つの主要な機能を実行できます。

Route 53 を DNS サービスとして使用して、ドメイン名を EC2 インスタンス、S3 バケット、CloudFront ディストリビューション、その他の AWS リソースにマッピングできます。DNS AWS サーバーの分散性により、エンドユーザーがアプリケーションに一貫してルーティングされます。Route 53 トラフィックフローやルーティング制御などの機能は、信頼性の向上に役立ちます。プライマリアプリケーションのエンドポイントが使用できなくなった場合は、ユーザーを別の場所に再ルーティングするようにフェールオーバーを設定できます。Route 53 Resolver は、 AWS Direct Connect または AWS マネージド VPN 経由で VPC およびオンプレミスネットワークに再帰的な DNS を提供します。

Route 53 で IAM サービスを使用すると、DNS データを更新できるユーザーをきめ細かく制御できます。DNS Security Extensions (DNSSEC) 署名を有効にして、DNS 応答が Route 53 から送信されていて、改ざんされていないことを DNS リゾルバーが検証できるようにします。

Route 53 Resolver DNS Firewall は、VPC からのアウトバウンド DNS リクエストを保護できます。これらのリクエストは、ドメイン名の解決用に Route 53 Resolver を経由します。DNS Firewall による保護の主な用途は、データの DNS 漏洩を防ぐことです。DNS Firewall を使用すると、アプリケーションでクエリできるドメインを監視および管理できます。不正であるとわかっているドメインへのアクセスを拒否し、他のすべてのクエリの通過を許可できます。また、確実に信頼できるドメインを除くすべてのドメインへのアクセスを拒否することもできます。DNS ファイアウォールは、VPC エンドポイント名など、プライベートのホストゾーン (共有またはローカル) 内のリソースに対する解決リクエストをブロックする場合にも使用できます。また、パブリックまたはプライベートの EC2 インスタンス名のリクエストをブロックすることもできます。

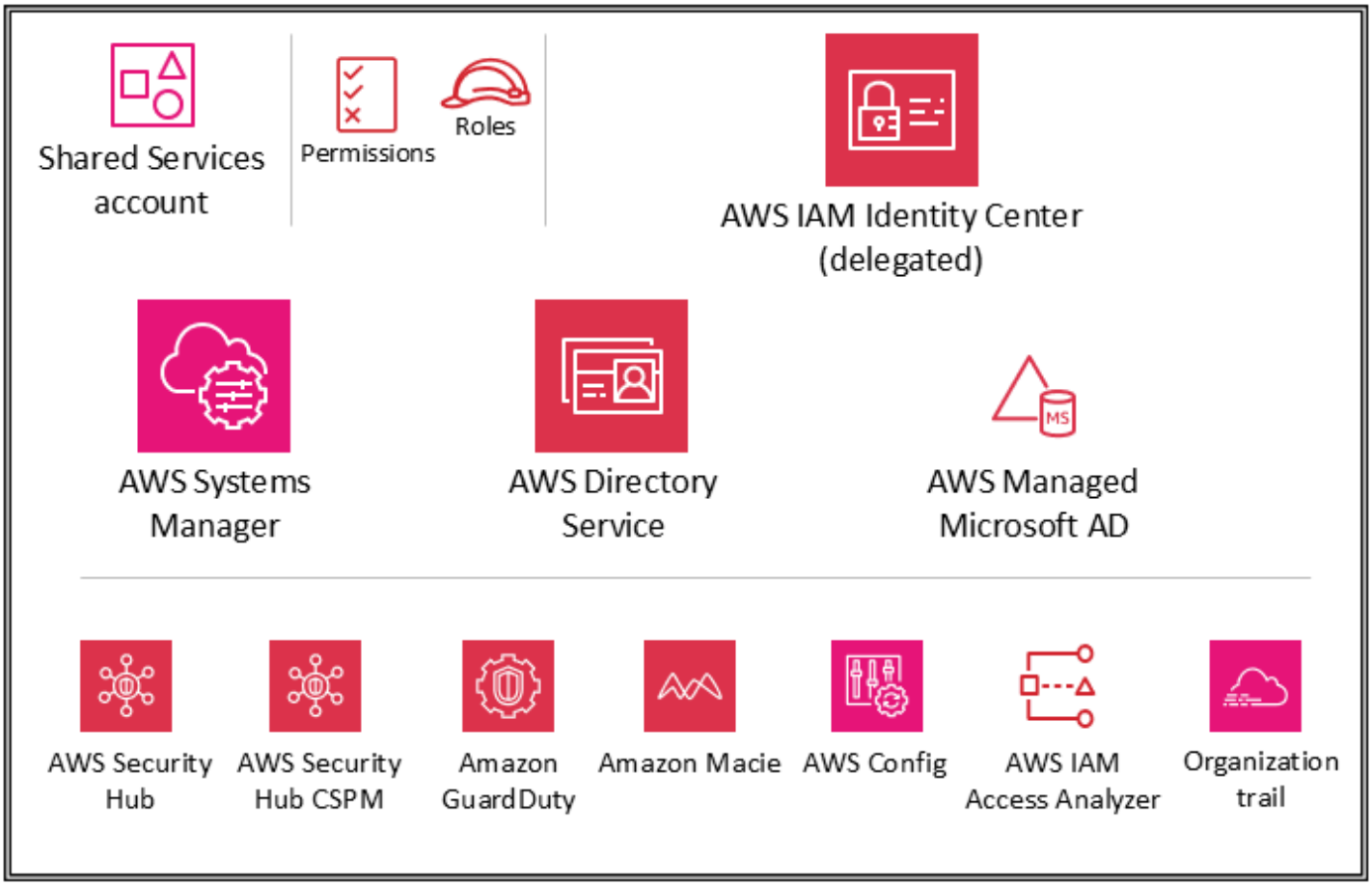
Route 53 リゾルバーは、すべての VPC の一部としてデフォルトで作成されます。 AWS SRA では、Route 53 は主に DNS ファイアウォール機能のためにネットワークアカウントで使用されます。

> **設計上の考慮事項**
>
> DNS Firewall と AWS Network Firewall はどちらもドメイン名フィルタリングを提供しますが、トラフィックのタイプは異なります。DNS Firewall と Network Firewall を一緒に使用して、2 つの異なるネットワークパスでアプリケーションレイヤートラフィックのドメインベースのフィルタリングを設定できます。
>
> - DNS Firewall は、VPC 内のアプリケーションから Route 53 Resolver を通過するアウトバウンド DNS クエリのフィルタリングを行います。また、ブロックしたドメイン名にクエリのカスタムレスポンスを送信するように DNS Firewall を設定できます。
> - Network Firewall は、ネットワーク層とアプリケーション層の両方のトラフィックに対してフィルタリングを行いますが、Route 53 Resolver によって実行されるクエリに対する可視性はありません。

インフラストラクチャ OU - 共有サービスアカウント

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は、共有サービスアカウントで設定されている AWS セキュリティサービスを示しています。



共有サービスアカウントは、インフラストラクチャ OU の一部であり、その目的は、複数のアプリケーションやチームが成果を達成するために使用するサービスをサポートすることです。例えば、ディレクトリサービス (Active Directory)、メッセージングサービス、メタデータサービスがこのカテゴリに含まれます。 AWS SRA は、セキュリティコントロールをサポートする共有サービスに焦点を当てています。ネットワークアカウントもインフラストラクチャ OU の一部ですが、職務の分離をサポートするために、共有サービスアカウントから削除されています。これらのサービスを管理するチームには、ネットワークアカウントへのアクセス許可やアクセス許可は必要ありません。

AWS Systems Manager

AWS Systems Manager (組織管理アカウントとアプリケーションアカウントにも含まれる) は、AWS リソースの可視性と制御を可能にする機能のコレクションを提供します。これらの機能の 1 つである Systems Manager Explorer は、 AWS リソースに関する情報をレポートするカスタマイズ可能なオペレーションダッシュボードです。 AWS Organizations および Systems Manager Explorer を使用して、 AWS 組織内のすべてのアカウント間でオペレーションデータを同期できます。Systems Manager は、 AWS Organizationsの委任管理者機能により、共有サービスアカウントにデプロイされます。

Systems Manager は、マネージドインスタンスをスキャンし、検出されたポリシー違反を報告する (または是正措置を講じる) ことで、セキュリティとコンプライアンスを維持するのに役立ちます。Systems Manager を個々のメンバー AWS アカウント (アプリケーションアカウントなど) の適切なデプロイと組み合わせることで、インスタンスインベントリデータ収集を調整し、パッチ適用やセキュリティ更新などの自動化を一元化できます。

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directoryは、ディレクトリ対応のワークロードと AWS リソースでマネージド Active Directory を使用 AWS Managed Microsoft ADできるようにします AWS。 AWS Managed Microsoft AD を使用してAmazon EC2 for Windows Server、Amazon EC2 for Linux、Amazon RDS for SQL Server インスタンスをドメインに結合し、Amazon WorkSpaces などのAWS エンドユーザーコンピューティング (EUC) サービスを Active Directory ユーザーおよびグループとともに使用できます。

AWS Managed Microsoft AD は、既存の Active Directory を に拡張 AWS し、既存のオンプレミスユーザー認証情報を使用してクラウドリソースにアクセスするのに役立ちます。オンプレミスのユーザー、グループ、アプリケーション、システムを、オンプレミスの高可用性 Active Directory の実行と維持の複雑さなしに管理することもできます。既存のコンピュータ、ラップトップ、プリンターを AWS Managed Microsoft AD ドメインに結合できます。

AWS Managed Microsoft AD は Microsoft Active Directory 上に構築されており、既存の Active Directory からクラウドにデータを同期またはレプリケートする必要はありません。グループポリシーオブジェクト (GPOs)、ドメイン信頼、きめ細かなパスワードポリシー、グループマネージドサービスアカウント (gMSAs)、スキーマ拡張、Kerberos ベースのシングルサインオンなど、使い慣れた Active Directory 管理ツールと機能を使用できます。Active Directory セキュリティグループを使用して管理タスクを委任し、アクセスを許可することもできます。

マルチリージョンレプリケーションを使用すると、1 つの AWS Managed Microsoft AD ディレクトリを複数のディレクトリにデプロイして使用できます AWS リージョン。これにより、Microsoft Windows および Linux ワークロードをグローバルにデプロイして管理し、より簡単でコスト効率の高いものにすることができます。自動マルチリージョンレプリケーション機能を使用すると、アプリケーションが最適なパフォーマンスを得るためにローカルディレクトリを使用している間、耐障害性が向上します。

AWS Managed Microsoft AD は、クライアントロールとサーバーロールの両方で、LDAPS とも呼ばれる SSL/TLS 経由の Lightweight Directory Access Protocol (LDAP) をサポートします。サーバーとして機能する場合、 AWS Managed Microsoft AD はポート 636 (SSL) および 389 (TLS) 経由の LDAPS をサポートします。 AWSベースの Active Directory Certificate Services (AD CS) 認証局 (CA)

から AWS Managed Microsoft AD ドメインコントローラーに証明書をインストールすることで、サーバー側の LDAPS 通信を有効にします。クライアントとして機能すると、 はポート 636 (SSL) 経由の LDAPS AWS Managed Microsoft AD をサポートします。サーバー証明書発行者から に CA 証明書を登録し、 ディレクトリで LDAPS を有効にすることで AWS、クライアント側の LDAPS 通信を有効にできます。

AWS SRA Directory Service では、共有サービスアカウント内で使用され、複数の AWS メンバーアカウントにわたる Microsoft 対応ワークロードにドメインサービスを提供します。

> **設計上の考慮事項**
>
> IAM Identity Center を使用して ID ソース AWS Managed Microsoft AD として を選択することで、オンプレミスの Active Directory ユーザーに既存の Active Directory 認証情報を使用して および AWS マネジメントコンソール AWS Command Line Interface (AWS CLI) にサインインするためのアクセス権を付与できます。これにより、ユーザーはサインイン時に割り当てられたロールの 1 つを引き受け、ロールに定義されたアクセス許可に従ってリソースにアクセスしてアクションを実行できます。別のオプションは、 AWS Managed Microsoft AD を使用して、ユーザーが IAM ロールを引き受けられるようにすることです。

IAM アイデンティティセンター

AWS SRA は、 でサポートされている委任管理者機能 AWS IAM アイデンティティセンター を使用して、IAM アイデンティティセンターの管理の大部分を共有サービスアカウントに委任します。これにより、組織管理アカウントへのアクセスを必要とするユーザーの数を制限できます。組織管理アカウント内でプロビジョニングされたアクセス許可セットの管理など、特定のタスクを実行するには、組織管理アカウントで IAM Identity Center を有効にする必要があります。

IAM Identity Center の委任管理者として共有サービスアカウントを使用する主な理由は、Active Directory の場所です。Active Directory を IAM アイデンティティセンターの ID ソースとして使用する場合は、IAM アイデンティティセンターの委任管理者アカウントとして指定したメンバーアカウント内のディレクトリを見つける必要があります。 AWS SRA では、共有サービスアカウントがホストするため AWS Managed Microsoft AD、そのアカウントは IAM Identity Center の委任管理者になります。

IAM Identity Center は、一度に 1 つのメンバーアカウントを委任管理者として登録することをサポートしています。メンバーアカウントを登録できるのは、管理アカウントの認証情報を使用してサインインする場合のみです。委任を有効にするには、IAM Identity Center ドキュメントに記載されている

前提条件を考慮する必要があります。委任管理者アカウントは、ほとんどの IAM アイデンティティセンター管理タスクを実行できますが、いくつかの制限があります。これらの制限については、IAM アイデンティティセンターのドキュメントに記載されています。IAM Identity Center の委任管理者アカウントへのアクセスは、厳密に制御する必要があります。

設計上の考慮事項

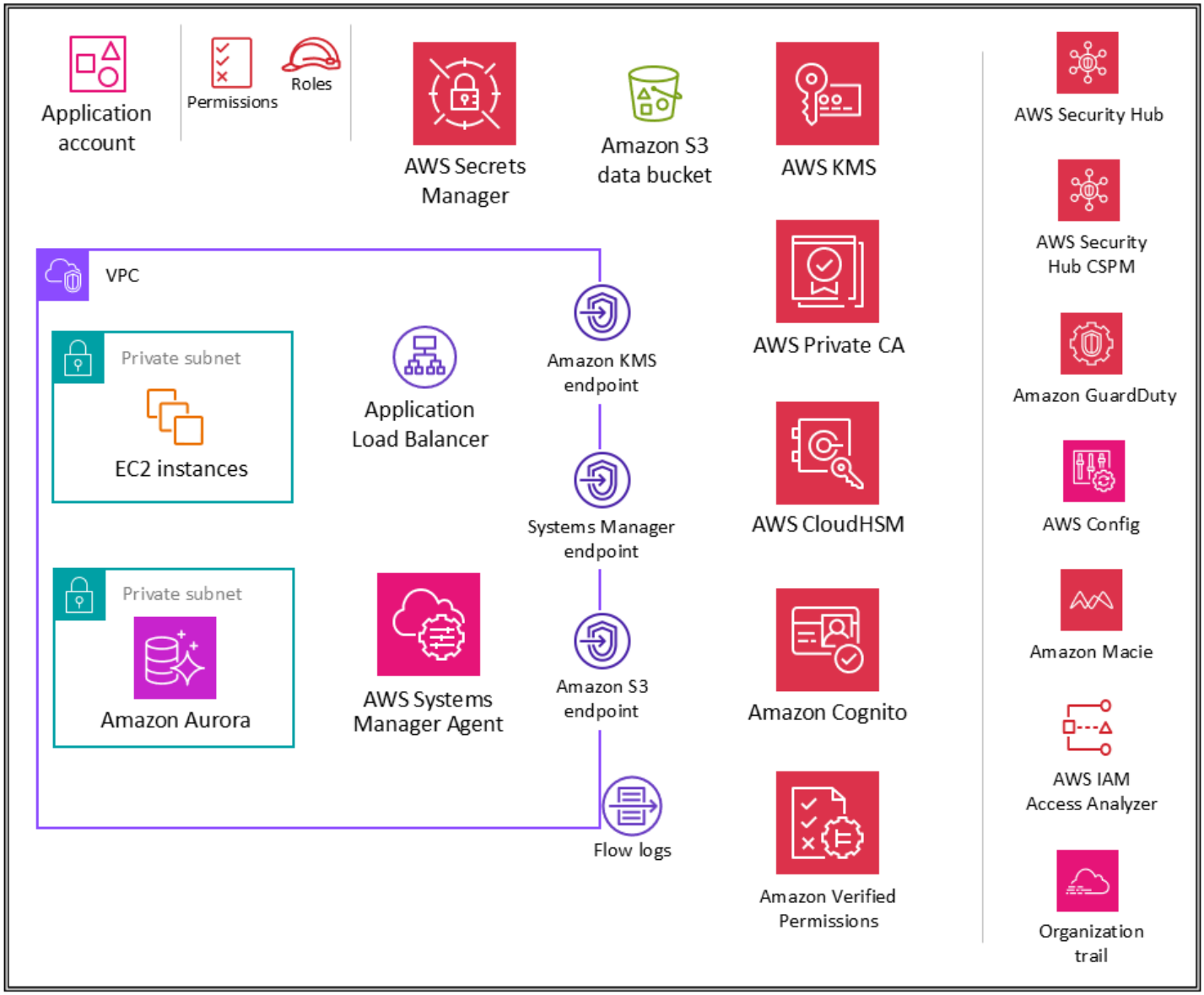
- IAM アイデンティティセンターの ID ソースを他のソースから Active Directory に変更する場合、または Active Directory から他のソースに変更する場合、ディレクトリは IAM アイデンティティセンターの委任された管理者メンバーアカウントにある (所有されている) 必要があります。存在しない場合は、管理アカウントにある必要があります。
- 別のアカウントの専用 VPC AWS Managed Microsoft AD 内で をホストし、 AWS Resource Access Manager (AWS RAM) を使用して、この他のアカウントのサブネットを委任管理者アカウントと共有できます。これにより、 AWS Managed Microsoft AD インスタンスは委任管理者アカウントで制御されますが、ネットワークの観点からは、別のアカウントの VPC にデプロイされているかのように動作します。これは、複数の AWS Managed Microsoft AD インスタンスがあり、ワークロードが実行されている場所にローカルにデプロイし、1 つのアカウントで一元管理する場合に役立ちます。
- 定期的な ID およびアクセス管理アクティビティを実行する専用の ID チームがある場合、または ID 管理機能を他の共有サービス機能から分離するための厳格なセキュリティ要件がある場合は、ID 管理 AWS アカウント 専用の をホストできます。このシナリオでは、このアカウントを IAM Identity Center の委任管理者として指定し、 AWS Managed Microsoft AD ディレクトリもホストします。単一の共有サービスアカウント内できめ細かな IAM アクセス許可を使用することで、ID 管理ワークロードと他の共有サービスワークロードの間で同じレベルの論理分離を実現できます。
- IAM アイデンティティセンターは現在、マルチリージョンをサポートしていません。(別のリージョンで IAM アイデンティティセンターを有効にするには、まず現在の IAM アイデンティティセンター設定を削除する必要があります) 。さらに、異なるアカウントセットに対する異なる ID ソースの使用をサポートしておらず、組織の異なる部分 (複数の委任された管理者) または異なる管理者グループに権限管理を委任することもできません。これらの機能のいずれかが必要な場合は、IAM フェデレーションを使用して の外部の ID プロバイダー (IdP) 内のユーザー ID を管理し AWS 、これらの外部ユーザー ID にアカウント内の AWS リソースを使用するアクセス許可を付与できます。IAM は、OpenID Connect (OIDC) または SAML 2.0 と互換性のある IdPs をサポートしています。ベストプラクティスとして、Active Directory Federation Service (AD FS)、Okta、Azure Active Directory (Azure AD)、Ping Identity などのサードパーティー ID プロバイダーと SAML 2.0

フェデレーションを使用して、ユーザーが にログインしたり AWS API オペレーションを呼び出し AWS マネジメントコンソール たりするためのシングルサインオン機能を提供します。IAM フェデレーションと ID プロバイダーの詳細については、IAM ドキュメントの「SAML 2.0 ベースのフェデレーションについて」を参照してください。

ワークロード OU — アプリケーションアカウント

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

次の図は、アプリケーションアカウント (およびアプリケーション自体) で設定されている AWS セキュリティサービスを示しています。



Application アカウントは、エンタープライズアプリケーションを実行および維持するためのプライマリインフラストラクチャとサービスをホストします。アプリケーションアカウントとワークロード OU は、いくつかの主要なセキュリティ目標を果たします。まず、アプリケーションごとに個別のアカウントを作成して、ワークロード間の境界と制御を提供し、役割、許可、データ、および暗号化キーが発生する問題を回避します。アプリケーションチームに、他のユーザーに影響を与えることなく、独自のインフラストラクチャを管理する幅広い権限を付与できる個別のアカウントコンテナを提供したいと考えています。次に、セキュリティ運用チームがセキュリティデータを監視および収集するメカニズムを提供して、保護のレイヤーを追加します。セキュリティチームによって設定およびモニタリングされるアカウントセキュリティサービス (Amazon GuardDuty、 AWS Config AWS Security Hub CSPM、Amazon EventBridge、IAM Access Analyzer) の組織の証跡とローカルデプロイを採用します。最後に、企業が一元的に制御を設定できるようにします。アプリケーションアカウ

ントは、適切なサービス権限、制約、およびガードレールを継承する Workloads OU のメンバーにして、より広範なセキュリティ構造に合わせます。

> **設計上の考慮事項**
>
> 組織内には、複数のビジネスアプリケーションが存在する可能性があります。ワークロード OU は、本番環境と非本番環境の両方を含む、ビジネス固有のワークロードのほとんどを格納することを目的としています。これらのワークロードは、商用の既製品 (COTS) アプリケーションと、社内で独自に開発したカスタムアプリケーションやデータサービスを組み合わせることができます。開発環境とともにさまざまなビジネスアプリケーションを整理するためのパターンはほとんどありません。1 つのパターンは、本番環境、ステージング環境、テスト環境、開発環境など、開発環境に基づいて複数の子 OUs を持ち、異なるアプリケーションに関連する OU AWS アカウント の下に個別の子を使用することです。 OUs もう 1 つの一般的なパターンは、アプリケーションごとに個別の子 OUs を設定し、個々の開発環境に個別の子を使用すること AWS アカウント です。正確な OU とアカウント構造は、アプリケーション設計とそれらのアプリケーションを管理するチームによって異なります。これらのコントロールは OU に SCPs として実装する方が簡単なため、環境固有でもアプリケーション固有でも、適用するセキュリティコントロールを検討してください。 OUs ワークロード指向の OUs整理に関するその他の考慮事項については、 AWS ホワイトペーパーの「アプリケーション OUs」セクションを参照してください。複数のアカウントを使用して AWS 環境を整理する。

アプリケーション VPC

アプリケーションアカウントの Virtual Private Cloud (VPC) には、インバウンドアクセス (モデリングするシンプルなウェブサービス用) とアウトバウンドアクセス (アプリケーションのニーズまたは AWS のサービス ニーズ用) の両方が必要です。デフォルトでは、VPC 内のリソースは相互にルーティング可能です。2 つのプライベートサブネットがあります。1 つは EC2 インスタンス (アプリケーションレイヤー) をホストし、もう 1 つは Amazon Aurora (データベースレイヤー) をホストします。アプリケーション層やデータベース層など、異なる層間のネットワークセグメンテーションは、インスタンスレベルでトラフィックを制限する VPC セキュリティグループを介して行われます。復元力のために、ワークロードは複数のアベイラビリティーゾーンにまたがり、ゾーンごとに 2 つのサブネットを使用します。

設計上の考慮事項

Traffic Mirroring を使用して、EC2 インスタンスの Elastic Network Interface からネットワークトラフィックをコピーできます。その後、コンテンツ検査、脅威モニタリング、またはトラブルシューティングのために、トラフィックを帯域外セキュリティアプライアンスおよびモニタリングアプライアンスに送信できます。たとえば、VPC から出るトラフィック、またはソースが VPC 外にあるトラフィックを監視できます。この場合、VPC 内を通過するトラフィックを除くすべてのトラフィックをミラーリングし、単一のモニタリングアプライアンスに送信します。Amazon VPC フローログはミラーリングされたトラフィックをキャプチャしません。通常、パケットヘッダーからの情報のみをキャプチャします。トラフィックミラーリングを使用すると、ペイロードを含む実際のトラフィックコンテンツを分析できるため、ネットワークトラフィックに関するより深い洞察が得られます。トラフィックミラーリングは、機密性の高いワークロードの一部として動作している可能性がある、または問題が発生した場合に詳細な診断が必要と予想される EC2 インスタンスの elastic network interface に対してのみ有効にします。

VPC エンドポイント

VPC endpoints は、スケーラビリティと信頼性だけでなく、セキュリティ制御の別のレイヤーを提供します。これらを使用して、アプリケーション VPC を他の に接続します AWS のサービス。(アプリケーションアカウントでは、SRA AWS は AWS KMS AWS Systems Managerと Amazon S3 の VPC エンドポイントを使用します)。エンドポイントは仮想デバイスです。これらは水平にスケールされ、冗長で、可用性の高い VPC コンポーネントです。これにより、ネットワークトラフィックに可用性リスクや帯域幅の制約を課すことなく、VPC 内のインスタンスとサービス間の通信が可能になります。VPC エンドポイントを使用して、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を必要と AWS PrivateLink せずに、サポートされている AWS のサービス および を搭載した VPC エンドポイントサービスに VPC をプライベートに接続できます。VPC 内のインスタンスは、他の と通信するためにパブリック IP アドレスを必要としません AWS のサービス。VPC と他の VPC 間のトラフィック AWS のサービス は、Amazon ネットワークを離れません。

VPC エンドポイントを使用するもう 1 つの利点は、エンドポイントポリシーの設定を有効にすることです。VPC エンドポイントポリシーは、エンドポイントの作成時または変更時にエンドポイントに加える IAM リソースポリシーです。エンドポイントの作成時に IAM ポリシーをアタッチしない場合、 はサービスへのフルアクセスを許可するデフォルトの IAM ポリシーをア AWS タッチします。エンドポイントポリシーは、IAM ユーザーポリシーやサービス固有のポリシー (S3 バケットポ

リシーなど) を上書き、または置き換えません。これは、エンドポイントから指定されたサービスへのアクセスを制御するための別個の IAM ポリシーです。このようにして、どの AWS プリンシパルがリソースまたはサービスと通信できるかを別の制御レイヤーに追加します。

Amazon EC2

アプリケーションを構成する Amazon EC2 インスタンスは、インスタンスメタデータサービス (IMDSv2) のバージョン 2 を使用します。IMDSv2 は、IDMS にアクセスを試みるために使われた、ウェブサイトアプリケーションファイアウォール、オープンリバースプロキシ、サーバーサイドリクエストフォージェリ (SSRF) の脆弱性、オープンレイヤー 3 ファイアウォール、および NAT という 4 種類の脆弱性に対する保護を追加します。さらなる詳細については、ブログ投稿 Add defense in depth against open firewalls, reverse proxies, and SSRF vulnerabilities with enhancements to the EC2 Instance Metadata Service を参照してください。

(アカウント境界のサブセットとして) 個別の VPCs を使用して、ワークロードセグメント別にインフラストラクチャを分離します。サブネットを使用すると、単一の VPC 内で多階層ウェブアプリケーションの各階層 (ウェブサーバー、アプリケーションサーバーおよびデータベースサーバーなど) を隔離できます。インターネットからの直接アクセスを認めるべきでないインスタンスには、プライベートサブネットを使用します。インターネットゲートウェイを使用せずにプライベートサブネットから Amazon EC2 API を呼び出すには、 を使用します AWS PrivateLink。セキュリティグループを使用してインスタンスへのアクセスを制限します。VPC フローログを使用して、インスタンスに到達するトラフィックをモニタリングします。の一機能である Session Manager を使用して AWS Systems Manager、インバウンド SSH ポートを開いて SSH キーを管理する代わりに、インスタンスにリモートでアクセスします。オペレーティングシステムとデータには、個別の Amazon Elastic Block Store (Amazon EBS) ボリュームを使用します。作成した新しい EBS ボリュームとスナップショットコピーの暗号化を強制するように を設定できます AWS アカウント。

> 実装例
>
> AWS SRA コードライブラリは、Amazon EC2 でのデフォルトの Amazon EBS 暗号化の実装例を提供します。 AWS 組織内の各 AWS アカウント AWS リージョンおよび 内でアカウントレベルのデフォルトの Amazon EBS 暗号化を有効にする方法を示します。

AWS Nitro Enclaves

AWS Nitro Enclaves は、Amazon EC2 インスタンスから enclaves と呼ばれる独立した実行環境を作成できる Amazon EC2 機能です。Enclaves は、分離された、強化された、制約の厳しい仮想マシン

です。単一の親 EC2 インスタンスの CPU とメモリは、分離されたエンクレーブに分割されます。各エンクレーブは独立したカーネルを実行します。エンクレーブは、親インスタンスとの安全なローカルソケット接続のみを提供します。永続的ストレージ、対話型アクセス、外部ネットワークはありません。ユーザーはエンクレーブに SSH 接続できず、エンクレーブ内のデータとアプリケーションには、親インスタンスのプロセス、アプリケーション、またはユーザー (ルートまたは管理者) がアクセスできません。EC2 インスタンス内で、個人を特定できる情報 (PII)、医療、財務、知的財産のデータなど、最も機密性の高いデータを保護できます。Nitro Enclaves を使用すると、外部サービスとの統合を心配することなく、アプリケーションに集中できます。Nitro Enclaves には、承認されたコードのみが実行されていることを確認するためのソフトウェアの暗号化認証と、エンクレーブのみが機密マテリアルにアクセスできる AWS KMS ように との統合が含まれています。これにより、最も機密性の高いデータ処理アプリケーションの攻撃対象領域を減らすことができます。Nitro Enclaves の使用には追加料金はかかりません。

暗号化認証は、エンクレーブのアイデンティティを証明するために使用されるプロセスです。認証プロセスは Nitro Hypervisor を通じて行われます。これにより、エンクレーブの署名付き認証ドキュメントが生成され、そのアイデンティティが別のサードパーティーまたはサービスに証明されます。認証ドキュメントには、エンクレーブのパブリックキー、エンクレーブイメージとアプリケーションのハッシュなど、エンクレーブのキーの詳細が含まれています。

Nitro Enclaves 用の AWS Certificate Manager (ACM) を使用すると、Nitro Enclaves で EC2 インスタンスで実行されているウェブアプリケーションとウェブサーバーでパブリックおよびプライベート SSL/TLS 証明書を使用できます。SSL/TLS 証明書は、ネットワーク通信を保護し、インターネット経由でウェブサイトのアイデンティティを確立し、プライベートネットワーク上のリソースを確立するために使用されます。ACM for Nitro Enclaves は、SSL/TLS 証明書の購入、アップロード、更新の時間がかかり、エラーが発生しやすい手動プロセスを削除します。ACM for Nitro Enclaves は、安全なプライベートキーを作成し、証明書とそのプライベートキーをエンクレーブに配布し、証明書の更新を管理します。ACM for Nitro Enclaves では、証明書のプライベートキーはエンクレーブ内で分離されたままになるため、インスタンスとそのユーザーがアクセスできなくなります。詳細については、AWS Certificate Manager Nitro Enclaves ドキュメントの「 for Nitro Enclaves」を参照してください。

アプリケーション ロード バランサー

アプリケーションロードバランサーは、受信アプリケーショントラフィックを複数のアベイラビリティーゾーンの EC2 インスタンスなどの複数のターゲットに分散します。 AWS SRA では、ロードバランサーのターゲットグループはアプリケーション EC2 インスタンスです。 AWS SRA は HTTPS リスナーを使用して、通信チャネルが暗号化されていることを確認します。Application Load

Balancer はサーバー証明書を使用してフロントエンド接続を終了し、ターゲットにリクエストを送信する前に、クライアントからのリクエストを復号化します。

AWS Certificate Manager (ACM) は Application Load Balancer とネイティブに統合され、SRA AWS は ACM を使用して必要な X.509 (TLS サーバー) パブリック証明書を生成および管理します。Application Load Balancer セキュリティポリシーを通して、フロントエンド接続に TLS 1.2 と強力な暗号を適用できます。詳細については、「Elastic Load Balancing ドキュメント」を参照してください。

設計上の考慮事項

- Application Load Balancer でプライベート TLS 証明書を必要とする厳密に内部アプリケーションなどの一般的なシナリオでは、このアカウント内の ACM を使用してプライベート証明書を生成できます AWS Private CA。 AWS SRA では、ACM ルートプライベート CA は Security Tooling アカウントでホストされ、Security Tooling アカウントセクションで前述したように、 AWS 組織全体、またはエンドエンティティ証明書の発行 AWS アカウント に固有の と共有できます。
- パブリック証明書の場合、ACM を使用してこれらの証明書を生成し、自動ローテーションを含めて管理できます。または、SSL/TLS ツールを使用して証明書署名リクエスト (CSR) を作成し、認証機関 (CA) によって署名された CSR を取得して証明書を生成し、証明書を ACM にインポートするか、証明書を IAM にアップロードして Application Load Balancer で使用することもできます。証明書をACMにインポートする場合は、証明書の有効期限を監視し、有効期限が切れる前に更新する必要があります。
- 追加の防御レイヤーについては、Application Load Balancer を保護するための AWS WAF ポリシーをデプロイできます。エッジポリシー、アプリケーションポリシー、さらにはプライベートまたは内部ポリシー強制レイヤーさえあれば、通信要求の可視性が高まり、統一されたポリシー強制が提供されます。詳細については、ブログ記事「Deploying defense in deep using AWS マネージドルール for AWS WAF」を参照してください。

AWS Private CA

AWS Private Certificate Authority (AWS Private CA) は、Application Load Balancer で使用するプライベート証明書を生成するために Application アカウントで使用されます。Application Load Balancer が TLS 経由で安全なコンテンツを提供する一般的なシナリオです。これには、Application Load Balancer に TLS 証明書をインストールする必要があります。厳密に内部のアプリケーションの場合、プライベート TLS 証明書は安全なチャネルを提供できます。

AWS SRA では、 AWS Private CA は Security Tooling アカウントでホストされ、 を使用してアプリケーションアカウントに共有されます AWS RAM。これにより、アプリケーションアカウントのデベロッパーは、共有プライベート CA から証明書をリクエストできます。組織全体または組織全体で CAs を共有する AWS アカウント と、すべての で重複CAs を作成および管理する際のコストと複雑さが軽減されます AWS アカウント。ACM を使用して共有 CA からプライベート証明書を発行すると、証明書はリクエスト元のアカウントでローカルに生成され、ACM は完全なライフサイクル管理と更新を提供します。

Amazon Inspector

AWS SRA は Amazon Inspector を使用して、Amazon Elastic Container Registry (Amazon ECR) に存在する EC2 インスタンスとコンテナイメージを自動的に検出してスキャンし、ソフトウェアの脆弱性や意図しないネットワークへの露出 がないか確認します。

Amazon Inspector は、このアカウントの EC2 インスタンスに脆弱性管理サービスを提供するため、アプリケーションアカウントに配置されます。さらに、Amazon Inspector は EC2 インスタンスとの間の不要なネットワークパスをレポートします。

メンバーアカウントの Amazon Inspector は、委任管理者アカウントによって一元管理されます。SRA では、Security Tooling AWS アカウントは委任管理者アカウントです。委任管理者アカウントは、組織のメンバーの検出結果データと特定の設定を管理できます。これには、すべてのメンバーアカウントの集計結果の詳細の表示、メンバーアカウントのスキャンの有効化または無効化、AWS 組織内のスキャンされたリソースの確認が含まれます。

> 設計上の考慮事項
>
> の一機能である Patch Manager を使用してオンデマンドパッチ適用をトリガーし AWS Systems Manager、Amazon Inspector のゼロデイまたはその他の重大なセキュリティ脆弱性を修復できます。Patch Manager を使用すると、通常のパッチ適用スケジュールを待つことなく、これらの脆弱性にパッチを適用できます。修復は、Systems Manager Automation ランブックを使用して実行されます。詳細については、2 部構成のブログシリーズAmazon Inspector と AWS を使用して の脆弱性管理と修復を自動化 AWS Systems Managerする」を参照してください。

AWS Systems Manager

AWS Systems Manager は、 AWS のサービス 複数の からの運用データを表示 AWS のサービスし、 AWS リソース全体の運用タスクを自動化するために使用できる です。自動承認ワークフロー

とランブックを使用すると、人為的ミスを減らし、 AWS リソースのメンテナンスとデプロイタスクを簡素化できます。

これらの一般的な自動化機能に加えて、Systems Manager は、予防、detective な、および応答性の高いセキュリティ機能を多数サポートしています。AWS Systems Manager エージェント (SSM エージェント) は、EC2 インスタンス、オンプレミスサーバー、または仮想マシン (VM) にインストールして設定できる Amazon ソフトウェアです。SSM Agent により、Systems Manager がこれらのリソースを更新、管理、および設定できるようにします。Systems Manager は、これらのマネージドインスタンスをスキャンし、パッチ、設定、カスタムポリシーで検出された違反を報告する (または是正措置を講じる) ことで、セキュリティとコンプライアンスを維持するのに役立ちます。

SRA は、Systems Manager AWS の一機能である Session Manager を使用して、インタラクティブなブラウザベースのシェルと CLI エクスペリエンスを提供します。 https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.htmlこれにより、インバウンドポートを開いたり、baston ホストを維持したり、SSH キーを管理したりすることなく、安全で監査可能なインスタンス管理が提供されます。 AWS SRA は、Systems Manager の一機能である Patch Manager を使用して、オペレーティングシステムとアプリケーションの両方の EC2 インスタンスにパッチを適用します。

また、SRA は Systems Manager AWS の一機能である Automation を使用して、Amazon EC2 インスタンスやその他の AWS リソースの一般的なメンテナンスおよびデプロイタスクを簡素化します。オートメーションは、1 つ以上のノードの状態を変更 (承認されたオートメーションを使用) したり、スケジュールに従ってノードの状態を管理するなどの一般的な IT タスクを簡略化できます。Systems Manager には、タグを使用したインスタンスの大規模なグループのターゲットに役立つ機能や定義する制限に応じた変更を行うために役立つ速度制御といった機能が含まれます。Automation は、golden Amazon マシンイメージ (AMI) の作成や到達不可能な EC2 インスタンスの復元などの複雑なタスクを簡素化する、ワンクリックAutomation を提供します。さらに、IAM ロールに特定の関数を実行するための特定のランブックへのアクセスを許可することで、運用セキュリティを強化できます。これらのロールに直接アクセス許可を付与する必要はありません。たとえば、IAM ロールにパッチ更新後に特定の EC2 インスタンスを再起動するアクセス許可を付与したいが、そのロールに直接アクセス許可を付与しない場合は、代わりに Automation ランブックを作成し、そのロールにランブックのみを実行するアクセス許可を付与できます。

設計上の考慮事項

- Systems Manager の正常な機能は、EC2 インスタンスメタデータに左右されます。Systems Manager は、インスタンスメタデータサービスのバージョン 1 またはバー

ジョン 2（IMDSv1 および IMDSv2）を使用してインスタンスメタデータにアクセスできます。

- SSM エージェントは、Amazon EC2 メッセージ AWS のサービス 、Systems Manager、Amazon S3 などのさまざまな および リソースと通信する必要があります。この通信を実現するには、サブネットにアウトバウンドインターネット接続または適切な VPC エンドポイントのプロビジョニングが必要です。 AWS SRA は、SSM Agent の VPC エンドポイントを使用して、さまざまな へのプライベートネットワークパスを確立します AWS のサービス。
- オートメーションを使用すると、組織内でベストプラクティスを共有できます。ランブックでリソース管理のベストプラクティスを作成し、 AWS リージョン および グループ間でランブックを共有できます。ランブックパラメータの許容値を制限することもできます。これらのユースケースでは、セキュリティツールや共有サービスなどの中央アカウントで自動化ランブックを作成し、 AWS 組織の他の部分と共有する必要がある場合があります。一般的なユースケースには、パッチ適用とセキュリティ更新を一元的に実装し、VPC 設定または S3 バケットポリシーのドリフトを修正し、EC2 インスタンスを大規模に管理する機能が含まれます。実装の詳細については、Systems Manager のドキュメントを参照してください。

Amazon Aurora

AWS SRA では、Amazon Aurora と Amazon S3 が論理データ層を構成します。Aurora はフルマネージド型のリレーショナルデータベースエンジンで、MySQL および PostgreSQL と互換性があります。EC2 インスタンスで実行されているアプリケーションは、必要に応じて Aurora および Amazon S3 と通信します。Aurora は DB サブネットグループ内のデータベースクラスターで構成されます。

設計上の考慮事項

多くのデータベースサービスと同様に、Aurora のセキュリティは 3 つのレベルで管理されます。AuroraDB クラスターおよび DB インスタンス上でAmazon Relational Database Service（Amazon RDS）管理アクションを実行できるユーザーを制御するには、IAMを使用します VPC 内の Aurora DB クラスタのクラスタエンドポイントと DB インスタンスのポートへの接続を開くことができるデバイスと EC2 インスタンスを制御するには、VPC セキュリティグループを使用します。Aurora DB クラスターのログインとアクセス権限を認証するには、MySQL または PostgreSQL のスタンドアロン DB インスタンスと同じ方法を使用するか、Aurora MySQL 互換エディションの IAM データベース認証を使用します。この後者

のアプローチでは、IAM ロールと認証トークンを使用して、Aurora MySQL 互換 DB クラスターに対して認証を行います。

Amazon S3

Amazon S3 は、業界をリードするスケーラビリティ、データ可用性、セキュリティ、パフォーマンスを提供するオブジェクトストレージサービスです。これは、 上に構築された多くのアプリケーションのデータバックボーンであり AWS、機密データを保護するために適切なアクセス許可とセキュリティコントロールが不可欠です。Amazon S3 の推奨されるセキュリティのベストプラクティスについては、documentation、 online tech talks、および blog posts 中のより深いダイブインを参照します。最も重要なベストプラクティスは、S3 バケットへの過度に許容されるアクセス (特にパブリックアクセス) をブロックすることです。

AWS KMS

AWS SRA は、キー管理に推奨されるディストリビューションモデルを示しています。ここで、 は暗号化されるリソース AWS アカウント と同じ 内に AWS KMS key 存在します。このため、 AWS KMS は Security Tooling アカウントに含まれるだけでなく、アプリケーションアカウントで使用されます。アプリケーションアカウントでは、アプリケーションリソースに固有のキーを管理する AWS KMS ために使用されます。キーポリシーを使用して、ローカルアプリケーションロールにキー使用権限を付与し、キー管理者への管理およびモニタリング権限を制限することで、職務の分離を実装できます。

設計上の考慮事項

分散モデルでは、 AWS KMS キー管理責任はアプリケーションチームにあります。ただし、中央セキュリティチームは、次のような重要な暗号化イベントのガバナンスとモニタリングを担当できます。

- KMS キーにインポートされたキーマテリアルの有効期限が近づいています。
- KMS キーのキーマテリアルが自動的にローテーションされました。
- AKMS キーが削除されました。
- 復号の失敗率が高い。

AWS CloudHSM

AWS CloudHSM は、 でマネージドハードウェアセキュリティモジュール (HSMs) を提供します AWS クラウド。これにより、アクセスを制御する FIPS 140-2 レベル 3 検証HSMs を使用して AWS 、 で独自の暗号化キーを生成して使用できます。を使用して AWS CloudHSM 、ウェブサーバーの SSL/TLS 処理をオフロードできます。これにより、Webサーバーの負担が軽減され、 AWS CloudHSM中のWebサーバーのプライベートキーが保存されるためセキュリティが強化されます。同様に、ネットワークアカウントの AWS CloudHSM インバウンド VPC に から HSM をデプロイしてプライベートキーを保存し、発行認証機関として機能する必要がある場合は証明書リクエストに署名できます。

> **設計上の考慮事項**
>
> FIPS 140-2 レベル 3 のハード要件がある場合は、ネイティブ KMS キーストアを使用するのではなく、 AWS CloudHSM クラスターをカスタムキーストアとして使用する AWS KMS ように を設定することもできます。これにより、KMS キーを保護する HSMs を担当しながら、データを暗号化 AWS のサービス する AWS KMS と の統合からメリットを得られます。これにより、管理下にあるシングルテナント HSM と、 AWS KMSの使いやすさと統合が組み合わされます。インフラストラクチャを管理する AWS CloudHSM には、パブリックキーインフラストラクチャ (PKI) を採用し、HSMs の管理経験のあるチームが必要です。

AWS Secrets Manager

AWS Secrets Manager は、必要とする認証情報(secrets) を保護し、アプリケーションサービス、および IT リソースへアクセスするのに役立ちます。このサービスを使用すると、データベース認証情報、API キー、その他のシークレットをライフサイクルを通じて効率的にローテーション、管理、取得できます。コード内のハードコードされた認証情報 を Secrets Manager への API コールに置き換えて、シークレットをプログラムで取得できます。これは、シークレットがコード内に存在しなくなったため、コードを調べる人によってシークレットが侵害されないようにするのに役立ちます。さらに、Secrets Manager は、環境 (開発、本番前、本番) 間でアプリケーションを移動するのに役立ちます。コードを変更する代わりに、適切に名前が付けられ、参照されているシークレットが環境で使用可能であることを確認することができます。これにより、さまざまな環境でアプリケーションコードの一貫性と再利用性が促進されますが、コードのテスト後に必要な変更や人間による操作が少なくなります。

Secrets Manager を用いて、きめ細かい IAM ポリシーとリソースベースのポリシーを使用して、シークレットへのアクセスを管理できます。 AWS KMSを使用して、管理する暗号化キーを用いて

シークレットを暗号化することで、シークレットを保護できます。Secrets Manager は、一元化された監査のための AWS ログ記録およびモニタリングサービスとも統合されます。

Secrets Manager は、 AWS KMS keys および データキーによるエンベロープ暗号化を使用して、各シークレット値を保護します。シークレットを作成するときは、 AWS アカウント および リージョンで任意の対称カスタマーマネージドキーを選択するか、Secrets Manager の AWS マネージドキーを使用できます。

ベストプラクティスとして、シークレットをモニタリングして変更を記録できます。これにより、予期しない使用や変更を調査できます。不要な変更はロールバックできます。Secrets Manager は現在、組織とアクティビティをモニタリング AWS のサービス できる 2 つの AWS CloudTrail と をサポートしています AWS Config。CloudTrail は、Secrets Manager コンソールからの呼び出しや Secrets Manager API へのコード呼び出しを含む、Secrets Manager のすべての API コールをイベントとしてキャプチャします。さらに、CloudTrail は、 にセキュリティやコンプライアンスに影響する可能性がある、 AWS アカウント または運用上の問題のトラブルシューティングに役立つ可能性がある、その他の関連 (非 API) イベントをキャプチャします。これには、特定のシークレットローテーションイベントやシークレットバージョンの削除が含まれます。 は、Secrets Manager のシークレットへの変更を追跡およびモニタリングすることで、検出コントロールを提供 AWS Config できます。これらの変更には、シークレットの説明、ローテーション設定、タグ、および KMS 暗号化キーやシークレットローテーションに使用される AWS Lambda 関数などの他の AWS ソースとの関係が含まれます。設定とコンプライアンスの変更の通知を受信する Amazon EventBridge を設定して AWS Config、通知または修復アクションのために特定のシークレットイベントをルーティングすることもできます。

AWS SRA では、Secrets Manager はアプリケーションアカウントに配置され、ローカルアプリケーションのユースケースをサポートし、使用状況に近いシークレットを管理します。ここでは、インスタンスプロファイルがアプリケーションアカウントの EC2 インスタンスにアタッチされます。次に、Secrets Manager で個別のシークレットを設定して、そのインスタンスプロファイルがシークレットを取得できるようにします。たとえば、適切な Active Directory または LDAP ドメインに参加し、Aurora データベースにアクセスできるようにします。Secrets Manager は Amazon RDS と統合され、Amazon RDS DB インスタンスまたはマルチ AZ DB クラスターを作成、変更、または復元するときにユーザー認証情報を管理します。これにより、キーの作成とローテーションを管理し、コード内のハードコードされた認証情報を Secrets Manager へのプログラムによる API コールに置き換えることができます。

設計上の考慮事項

一般に、シークレットが使用される場所に最も近いアカウントで Secrets Manager を設定および管理します。このアプローチは、ユースケースに関するローカルな知識を活用し、アプリケーション開発チームにスピードと柔軟性を提供します。追加の制御レイヤーが適切である可能性のある厳密に制御された情報については、Secrets Manager が Security Tooling アカウントのシークレットを一元管理できます。

Amazon Cognito

Amazon Cognito を使用すると、ユーザーのサインアップ、サインイン、アクセスコントロールをウェブおよびモバイルアプリに迅速かつ効率的に追加できます。Amazon Cognito は数百万のユーザーにスケールし、Apple、Facebook、Google、Amazon などのソーシャル ID プロバイダー、および SAML 2.0 と OpenID Connect を介したエンタープライズ ID プロバイダーとのサインインをサポートします。Amazon Cognito の 2 つの主なコンポーネントは、ユーザープールと ID プールです。ユーザープールは、アプリケーションユーザーにサインアップとサインインのオプションを提供するユーザーディレクトリです。ID プールを使用すると、ユーザーに他の へのアクセスを許可できます AWS のサービス。ID プールとユーザープールは別々に使用することも、一緒に使用することもできます。一般的な使用シナリオについては、Amazon Cognito ドキュメントを参照してください。

Amazon Cognito は、ユーザーのサインアップとサインインのための組み込みのカスタマイズ可能な UI を提供します。Amazon Cognito 用の Android、iOS、JavaScript SDKs を使用して、アプリにユーザーのサインアップページとサインインページを追加できます。Amazon Cognito Sync は、アプリケーション関連のユーザーデータのデバイス間同期を可能にする AWS のサービス および クライアントライブラリです。

Amazon Cognito は、保管中のデータと転送中のデータの多要素認証と暗号化をサポートしています。Amazon Cognito ユーザープールは、アプリケーション内のユーザーアカウントへのアクセスを保護するのに役立つ高度なセキュリティ機能を提供します。これらの高度なセキュリティ機能は、リスクベースの適応認証を提供し、侵害された認証情報の使用から保護します。

設計上の考慮事項

- AWS Lambda 関数を作成し、Lambda トリガーを使用して、ユーザーのサインアップ、確認、サインイン (認証) などのユーザープールオペレーション中にその関数をトリガーできます。認証チャレンジの追加、ユーザーの移行、検証メッセージのカスタマイズを行うこ

とができます。一般的なオペレーションとユーザーフローについては、Amazon Cognito ドキュメントを参照してください。Amazon Cognito は Lambda 関数を同期的に呼び出します。

- Amazon Cognito ユーザープールを使用して、小さなマルチテナントアプリケーションを保護できます。マルチテナント設計の一般的なユースケースは、アプリケーションの複数のバージョンのテストをサポートするためにワークロードを実行することです。マルチテナント設計は異なるデータセットを持つ単一のアプリケーションのテストにも役立ち、これはクラスターリソースを最大限に活用することを可能にします。ただし、テナントの数と予想されるボリュームが関連する Amazon Cognito サービスクォータと一致していることを確認してください。これらのクォータは、アプリケーション内のすべてのテナント間で共有されます。

Amazon Verified Permissions

Amazon Verified Permissions は、構築するアプリケーションのスケーラブルなアクセス許可管理およびきめ細かな認可サービスです。開発者と管理者は、専用でセキュリティファーストのオープンソースポリシー言語である Cedar をロールと属性とともに使用して、よりきめ細かなコンテキスト対応のポリシーベースのアクセスコントロールを定義できます。開発者は、認可を外部化し、ポリシーの管理と管理を一元化することで、より安全なアプリケーションを迅速に構築できます。Verified Permissions には、スキーマ定義、ポリシーステートメントの文法、数百万のアクセス許可にまたがる自動推論が含まれているため、デフォルトの拒否と最小特権の原則を適用できます。このサービスには、認可の決定と作成者ポリシーのテストに役立つ評価シミュレーターツールも含まれています。これらの機能により、ゼロトラストオブジェクトをサポートするために、詳細できめ細かな認可モデルのデプロイが容易になります。Verified Permissions は、ポリシーストア内のアクセス許可を一元化し、開発者がこれらのアクセス許可を使用してアプリケーション内のユーザーアクションを承認するのに役立ちます。

API を使用してアプリケーションからサービスに接続し、ユーザーアクセスリクエストを承認できます。認可リクエストごとに、サービスは関連するポリシーを取得し、それらのポリシーを評価して、ユーザー、ロール、グループメンバーシップ、属性などのコンテキスト入力に基づいて、ユーザーがリソースに対してアクションを実行することを許可されているかどうかを判断します。Verified Permissions を設定して接続し、ポリシー管理および認可ログを送信できます AWS CloudTrail。ID ストアとして Amazon Cognito を使用する場合は、Verified Permissions と統合し、Amazon Cognito がアプリケーションの認可決定で返す ID トークンとアクセストークンを使用できます。Verified Permissions に Amazon Cognito トークンを提供します。これは、トークンに含まれる属性を使用してプリンシパルを表し、プリンシパルのエンタイトルメントを識別します。この統合の詳細について

は、ブログ AWS 記事「Simplifying fine-grained authorization with Amazon Verified Permissions and Amazon Cognito」を参照してください。

Verified Permissions は、ポリシーベースのアクセスコントロール (PBAC) を定義するのに役立ちます。PBAC は、ポリシーとして表現されるアクセス許可を使用して、アプリケーション内のどのリソースにアクセスできるかを決定するアクセスコントロールモデルです。PBAC は、ロールベースのアクセスコントロール (RBAC) と属性ベースのアクセスコントロール (ABAC) を統合し、より強力で柔軟なアクセスコントロールモデルを実現します。PBAC の詳細と、Verified Permissions を使用して認可モデルを設計する方法については、 AWS ブログ記事「Amazon Verified Permissions を使用したアプリケーション開発におけるポリシーベースのアクセスコントロール」を参照してください。

AWS SRA では、Verified Permissions はアプリケーションアカウントにあり、Amazon Cognito との統合を通じてアプリケーションのアクセス許可管理をサポートします。

多層防御

アプリケーションアカウントは、 AWS を有効にするレイヤード防御プリンシパルを説明する機会を提供します。SRA で表されるシンプルなサンプルアプリケーションの中核をなす EC2 AWS インスタンスのセキュリティを考えてみましょう。多層防御で AWS のサービス 連携する方法を確認できます。このアプローチは、このガイドの前半の「組織全体に AWS セキュリティサービスを適用する」セクションで説明されているように、セキュリティサービスの構造図と一致しています AWS。

- 最も内側のレイヤーは EC2 インスタンスです。前述のように、EC2 インスタンスには、デフォルトで、またはオプションとして多くのネイティブセキュリティ機能が含まれています。例としては、IMDSv2、Nitro システム、Amazon EBS ストレージ暗号化などがあります。
- 2 番目の保護レイヤーは、EC2 インスタンスで実行されているオペレーティングシステムとソフトウェアに焦点を当てています。Amazon Inspector や などのサービスAWS Systems Managerを使用すると、これらの設定をモニタリング、報告、修正できます。Amazon Inspector はソフトウェアに脆弱性がないか監視し、Systems Manager はマネージドインスタンスのパッチと設定ステータスをスキャンし、指定した修正アクションを報告して実行することで、セキュリティとコンプライアンスを維持するのに役立ちます。
- インスタンス、およびこれらのインスタンスで実行されているソフトウェアは、 AWS ネットワークインフラストラクチャに配置されます。Amazon VPC のセキュリティ機能を使用することに加えて、SRA AWS は VPC エンドポイントを使用して VPC とサポートされている 間のプライベート接続を提供し AWS のサービス、ネットワーク境界にアクセスポリシーを配置するメカニズムも提供します。
- EC2 インスタンス、ソフトウェア、ネットワーク、IAM ロールとリソースのアクティビティと設定は AWS Security Hub CSPM、Amazon AWS アカウント GuardDuty AWS Security Hub、、

AWS Config IAM Access Analyzer AWS CloudTrail、Amazon Macie などの重点サービスによってさらにモニタリングされます。 Amazon GuardDuty

- 最後に、アプリケーションアカウント以外にも、 はどのリソースを他のアカウントと共有するか AWS RAM を制御し、IAM サービスコントロールポリシーは AWS 組織全体で一貫したアクセス許可を適用するのに役立ちます。

セキュリティのための AI/ML

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

人工知能と機械学習 (AI/ML) はビジネスを変革しています。AI/ML は 20 年以上にわたって Amazon の焦点であり、セキュリティサービスなど AWS、お客様が で使用する機能の多くが AI/ML によって駆動されています。これにより、セキュリティチームやアプリケーション開発チームに AI/ML に関する専門知識を必要と AWS せずに、 を安全に構築できるため、組み込みの差別化された価値が生まれます。

AI は、マシンとシステムがインテリジェンスと予測機能を取得できるようにする高度なテクノロジーです。AI システムは、消費またはトレーニングされるデータを通じて過去の経験から学習します。ML は AI の最も重要な側面の 1 つです。ML は、コンピュータが明示的にプログラムされることなくデータから学習する機能です。従来のプログラミングでは、プログラマーはプログラムがコンピュータまたはマシンでどのように機能するかを定義するルールを記述します。ML では、モデルはデータからルールを学習します。ML モデルは、データの隠れたパターンを検出したり、トレーニング中に使用されなかった新しいデータを正確に予測したりできます。複数の AWS のサービス が AI/ML を使用して巨大なデータセットから学習し、セキュリティ推論を行います。

- Amazon Macie は、ML とパターンマッチングを使用して機密データを検出し、保護するのに役立つデータセキュリティサービスです。Macie は、名前、住所、クレジットカード番号などの財務情報などの個人を特定できる情報 (PII) を含む、大規模で増加している機密データタイプのリストを自動的に検出します。また、Amazon Simple Storage Service (Amazon S3) に保存されているデータを常に可視化できます。Macie は、さまざまなタイプのデータセットでトレーニングされた自然言語処理 (NLP) モデルと ML モデルを使用して、既存のデータを理解し、ビジネス価値を割り当ててビジネスクリティカルなデータを優先します。その後、Macie は機密データの検出結果を生成します。
- Amazon GuardDuty は、ML、異常検出、統合された脅威インテリジェンスを使用して悪意のあるアクティビティと不正な動作を継続的にモニタリングし AWS アカウント、ユーザー、ユーザー、データベース、ストレージを保護する脅威検出サービスです。GuardDuty には、悪意のある可能性のあるユーザーアクティビティを内部の異常な操作動作と区別するのに非常に効果的な ML 手法が組み込まれています AWS アカウント。この機能は、アカウント内の API 呼び出しを継続的にモデル化し、確率予測を組み込むことで、非常に疑わしいユーザーの動作をより正確に分離して警告します。このアプローチは、検出、初期アクセス、永続性、特権エスカレーション、防御回

避、認証情報アクセス、影響、データ流出など、既知の脅威戦術に関連する悪意のあるアクティビティを特定するのに役立ちます。GuardDuty が機械学習を使用する方法の詳細については、AWS re:Inforce 2023 breakout sessionDeveloping new findings using machine learning in Amazon GuardDuty (TDR310) を参照してください。

検証可能なセキュリティ

AWS は、数学的ロジックを使用してインフラストラクチャに関する重要な質問に答え、データを公開する可能性がある設定ミスを検出する自動推論ツールを開発します。この機能は、クラウドとクラウドのセキュリティでより高い保証を提供するため、provable security と呼ばれます。実証可能なセキュリティでは、自動推論を使用します。これは、コンピュータシステムに論理的推論を適用する AI の特定の分野です。例えば、自動推論ツールはポリシーとネットワークアーキテクチャ設定を分析し、脆弱なデータを公開する可能性がある意図しない設定がないことを証明することができます。このアプローチは、クラウドの重要なセキュリティ特性に対して可能な限り最高レベルの保証を提供します。詳細については、 AWS ウェブサイトの「Provable Security Resources」を参照してください。以下の AWS のサービス および 機能は、現在、アプリケーションに対して実証可能なセキュリティを実現するために自動推論を使用しています。

- Amazon Verified Permissions は、構築するアプリケーション用のスケーラブルなアクセス許可管理およびきめ細かな認可サービスです。Verified Permissions は、自動推論テストと差分テストを使用して構築されたアクセスコントロール用のオープンソース言語である Cedar を使用します。Cedar は、どのユーザーがどのリソースにアクセスできるかを説明するポリシーとしてアクセス許可を定義するための言語です。また、これらのポリシーを評価するための仕様でもあります。Cedar ポリシーを使用して、アプリケーションの各ユーザーが実行できる操作とアクセスできるリソースを制御します。Cedar ポリシーは、ユーザーがリソースを操作できるかどうかを決定する許可禁止ステートメントです。ポリシーはリソースに関連付けられており、リソースに複数のポリシーをアタッチできます。禁止ポリシーは許可ポリシーを上書きします。アプリケーションのユーザーがリソースに対してアクションを実行しようとすると、アプリケーションは Cedar ポリシーエンジンに認可リクエストを行います。Cedar は該当するポリシーを評価し、 `ALLOW`または `DENY`の決定を返します。Cedar は、任意のタイプのプリンシパルとリソースの認可ルールをサポートし、ロールベースおよび属性ベースのアクセスコントロールを可能にし、ポリシーの最適化とセキュリティモデルの検証に役立つ自動推論ツールによる分析をサポートします。
- AWS Identity and Access Management Access Analyzer は、アクセス許可の管理を合理化するのに役立ちます。この機能を使用すると、未使用のアクセスを削除して、きめ細かなアクセス許可の設定、意図したアクセス許可の検証、アクセス許可の絞り込みを行うことができます。IAM Access Analyzer は、ログにキャプチャされたアクセスアクティビティに基づいてきめ細かなポリ

シーを生成します。また、ポリシーの作成と検証に役立つ 100 を超えるポリシーチェックも提供します。IAM Access Analyzer は、実証可能なセキュリティを使用してアクセスパスを分析し、リソースへのパブリックアクセスとクロスアカウントアクセスの包括的な検出結果を提供します。このツールは Zelkova 上に構築されており、IAM ポリシーを同等の論理ステートメントに変換し、問題に対して汎用および特殊な論理ソルバー (充足可能性モジュロ理論) のスイートを実行します。IAM Access Analyzer は、ポリシーが許可する動作のクラスの特徴を明確にするクエリを使用して Zelkova を繰り返しポリシーに適用します。アナライザーは、外部エンティティが信頼ゾーン内のリソースにアクセスしたかどうかを判断するためにアクセスログを調べません。リソースベースのポリシーが、外部エンティティによってリソースにアクセスされなかった場合でも、リソースへのアクセスを許可すると、検出結果が生成されます。満足度モジュロ理論の詳細については、「Handbook of Satisfiability」の「Satisfiability Modulo Theories」を参照してください。*

- Amazon S3 パブリックアクセスブロックは、バケットやオブジェクトへのパブリックアクセスにつながる可能性のある設定ミスをブロックできる Amazon S3 の機能です。アクセスポイント、バケット、アカウント、および AWS 組織 (アカウントの既存バケットと新規バケットの両方に影響) に対して Amazon S3 パブリックアクセスのブロックを有効にできます。パブリックアクセスは、アクセスコントロールリスト (ACL)、バケットポリシー、またはその両方からバケットおよびオブジェクトに付与されます。特定のポリシーまたは ACL がパブリックと見なされるかどうかの判断は、Zelkova 自動推論システムを使用して行われます。Amazon S3 は Zelkova を使用して各バケットポリシーをチェックし、権限のないユーザーがバケットを読み書きできるかどうかを警告します。バケットにパブリックとしてフラグが付けられている場合、一部のパブリックリクエストはバケットへのアクセスが許可されます。バケットにパブリックではないフラグが付けられている場合、すべてのパブリックリクエストは拒否されます。Zelkova は IAM ポリシーを正確に数学的に表現しているため、このような判断を行うことができます。ポリシーごとに数式を作成し、その数式に関する定理を証明します。

- Amazon VPC Network Access Analyzer は、リソースへの潜在的なネットワークパスを理解し、意図しないネットワークアクセスの可能性を特定するのに役立つ Amazon VPC の機能です。Network Access Analyzer は、ネットワークセグメンテーションの検証、インターネットアクセシビリティの特定、信頼できるネットワークパスとネットワークアクセスの検証に役立ちます。この機能は、自動推論アルゴリズムを使用して、パケットがネットワーク内のリソース間で実行できる AWS ネットワークパスを分析します。次に、アウトバウンドトラフィックパターンとインバウンドトラフィックパターンを定義するネットワークアクセススコープに一致するパスの検出結果を生成します。Network Access Analyzer はネットワーク構成の静的な分析を行います。つまり、この分析の一環としてネットワーク内でパケットが送信されることはありません。

- Amazon VPC Reachability Analyzer は、 AWS ネットワーク内の接続をデバッグ、理解、視覚化できる Amazon VPC の機能です。Reachability Analyzer は、仮想プライベートクラウド (VPC) 内のソースリソースと送信先リソース間の接続テストを実行できるようにする設定分析ツールです。送

信先に到達すると、Reachability Analyzer は送信元と送信先間の仮想ネットワークパスのhop-by-hopの詳細を生成します。送信先に到達できない場合、Reachability Analyzer はブロッキングコンポーネントを識別します。Reachability Analyzer は自動推論を使用して、送信元と送信先の間にネットワーク設定のモデルを構築することで、実行可能なパスを特定します。次に、設定に基づいて到達可能性をチェックします。パケットを送信したり、データプレーンを分析したりすることはありません。

[*] Biere、A. M. Heule、H. van Maaren、T. Walsh。2009 年。満足度ハンドブック。IOS Press、NLD。

セキュリティアーキテクチャの構築 – 段階的なアプローチ

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS SRA が推奨するマルチアカウントセキュリティアーキテクチャは、設計プロセスの早い段階でセキュリティを挿入するのに役立つベースラインアーキテクチャです。各組織のクラウドジャーニーは一意です。クラウドセキュリティアーキテクチャを正常に 進化させるには、希望するターゲット状態を構想し、現在のクラウドの準備状況を理解し、ギャップを埋めるためのアジャイルアプローチを採用する必要があります。 AWS SRA は、セキュリティアーキテクチャの参照ターゲット状態を提供します。段階的に変換することで、広範囲の予測を行う必要性を最小限に抑えながら、価値をすばやく実証できます。

AWS クラウド導入フレームワーク (AWS CAF) では、 ビジョン化、調整、起動、スケーリングの 4 つの反復的および増分的なクラウド変換フェーズを推奨しています。起動フェーズに入り、本番稼働環境でパイロットイニシアチブを提供することに重点を置く際には、最もビジネスクリティカルなワークロードを自信を持って移行して運用するための技術的な能力を確保するために、スケールフェーズの基盤として強力なセキュリティアーキテクチャを構築することに集中する必要があります。この段階的なアプローチは、スタートアップ企業、事業を拡大したい中小企業、または新しいビジネスユニットを買収したり、合併や買収を行っている企業に適用されます。 AWS SRA は、そのセキュリティベースラインアーキテクチャを実現するのに役立ちます。これにより、 で拡張する組織全体にセキュリティコントロールを均一に適用できます AWS Organizations。ベースラインアーキテクチャは、複数の AWS アカウント および サービスで構成されます。計画と実装は、より小さなマイルストーンを繰り返してベースラインセキュリティアーキテクチャを設定するというより大きな目標を達成できるように、複数フェーズのプロセスである必要があります。このセクションでは、構造化されたアプローチに基づくクラウドジャーニーの一般的なフェーズについて説明します。これらのフェーズは、 AWS Well-Architected フレームワークのセキュリティ設計原則と一致しています。

フェーズ 1: OU とアカウント構造を構築する

強力なセキュリティ基盤の前提条件は、適切に設計された AWS 組織とアカウント構造です。このガイドの「SRA 構成要素」セクションで前述したように、複数の を使用することで、さまざまなビジネス機能とセキュリティ機能を設計的に分離 AWS アカウント できます。これは最初は不要な作業のように見えるかもしれませんが、迅速かつ安全にスケーリングするための投資です。このセクションでは、 AWS Organizations を使用して複数の を管理する方法と AWS アカウント、信頼されたア

クセスと委任された管理者機能を使用してこれらの複数のアカウント AWS のサービス 間で一元管理する方法についても説明します。

このガイドで前述したAWS Control Towerように を使用して、ランディングゾーンをオーケストレーションできます。現在 1 つの を使用している場合は AWS アカウント、「複数のアカウントへの移行 AWS アカウント」ガイドを参照して、できるだけ早く複数のアカウントに移行してください。例えば、スタートアップ企業が現在 1 つの製品で製品のアイデアとプロトタイプを作成している場合は AWS アカウント、製品を市場に投入する前にマルチアカウント戦略を採用することを検討する必要があります。同様に、小規模、中規模、エンタープライズの組織は、最初の本番ワークロードを計画したらすぐにマルチアカウント戦略の構築を開始する必要があります。基盤 OUs と から開始し AWS アカウント、ワークロード関連の OUs とアカウントを追加します。

SRA で AWS 提供されているもの以外の AWS アカウント および OU 構造の推奨事項については、ブログ記事「中小企業向けのマルチアカウント戦略」を参照してください。OU とアカウント構造を確定するときは、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)、宣言ポリシーを使用して適用する組織全体のセキュリティコントロールを検討してください。

設計上の考慮事項

OU とアカウント構造を設計するときは、会社のレポート構造をレプリケートしないでください。OUs は、ワークロード関数と、ワークロードに適用される一般的な一連のセキュリティコントロールに基づいている必要があります。アカウント構造全体を最初から設計しないでください。基本的な OUs に焦点を当て、必要に応じてワークロード OUs を追加します。 OUs 間でアカウントを移動して、設計の初期段階で代替アプローチを試すことができます。ただし、OU とアカウントパスに基づく SCPs、RCPs、宣言ポリシー、IAM 条件によっては、論理アクセス許可の管理に多少のオーバーヘッドが発生する可能性があります。

実装例

AWS SRA コードライブラリは、アカウント代替連絡先のサンプル実装を提供します。このソリューションは、組織内のすべてのアカウントの請求、オペレーション、およびセキュリティの代替連絡先 を設定します。

フェーズ 2: 強力な ID 基盤を実装する

複数の を作成するとすぐに AWS アカウント、それらのアカウント内の AWS リソースへのアクセス権をチームに付与する必要があります。ID 管理には、ワークフォース ID とアクセス管理、カスタマー ID とアクセス管理 (CIAM) の 2 つの一般的なカテゴリがあります。ワークフォース IAM は、従業員と自動化されたワークロードがジョブを実行する AWS ために にログインする必要がある組織向けです。CIAM は、組織のアプリケーションへのアクセスを提供するユーザーを認証する方法を組織が必要とする場合に使用されます。チームがアプリケーションを構築して移行できるように、まずワークフォース IAM 戦略が必要です。人間またはマシンユーザーにアクセスを提供するには、常に IAM ユーザーではなく IAM ロールを使用する必要があります。組織管理アカウントと共有サービスアカウント AWS IAM アイデンティティセンター 内で AWS を使用して、 へのシングルサインオン (SSO) アクセスを一元管理する方法に関する SRA ガイダンスに従ってください AWS アカウント。このガイダンスでは、IAM Identity Center を使用できないときに IAM フェデレーションを使用するための設計上の考慮事項も示しています。

IAM ロールを使用して AWS リソースへのユーザーアクセスを提供する場合は、このガイドの「セキュリティツールと組織管理」セクションで説明されているように、IAM Access Analyzer と IAM アクセスアドバイザーを使用する必要があります。 ???これらのサービスは、最小特権の達成に役立ちます。これは、適切なセキュリティ体制の構築に役立つ重要な予防コントロールです。

> **設計上の考慮事項**
>
> 最小特権を実現するには、ID と適切な機能に必要なアクセス許可との関係を定期的に確認および理解するプロセスを設計します。学習したら、これらのアクセス許可を微調整し、最小限のアクセス許可に徐々に減らします。スケーラビリティについては、中央のセキュリティチームとアプリケーションチームの間で責任を共有する必要があります。 リソースベースのポリシー、 アクセス許可の境界、 属性ベースのアクセスコントロール、 セッションポリシー などの機能を使用して、アプリケーション所有者がきめ細かなアクセスコントロールを定義できるようにします。

> **実装例**
>
> AWS SRA コードライブラリには、このフェーズに適用される 2 つのサンプル実装が用意されています。
>
> - IAM パスワードポリシーは、一般的なコンプライアンス標準に合わせてユーザーのアカウントパスワードポリシーを設定します。

- Access Analyzer は、委任管理者アカウント内の組織レベルのアナライザーと、各アカウント内のアカウントレベルのアナライザーを設定します。

フェーズ 3: トレーサビリティを維持する

ユーザーが にアクセスして構築を開始する AWS と、誰が何を、いつ、どこで行っているかを知ることができます。また、潜在的なセキュリティ設定ミス、脅威、予期しない動作を可視化することもできます。セキュリティ脅威をよりよく理解することで、適切なセキュリティコントロールに優先順位を付けることができます。アクティビティをモニタリング AWS するには、 を使用してログアーカイブアカウント内にログをAWS CloudTrail一元化することで、組織の証跡を設定するための AWS SRA の推奨事項に従います。セキュリティイベントのモニタリングには、「 Security Tooling アカウント」セクションで説明されているように、、 AWS Security Hub CSPM Amazon GuardDuty AWS Config、および Amazon Security Lake を使用します。

設計上の考慮事項

新しい の使用を開始するときは AWS のサービス、サービスの サービス固有のログ を有効にし、中央ログリポジトリの一部として保存します。

実装例

AWS SRA コードライブラリには、このフェーズに適用される以下のサンプル実装が用意されています。

- Organization CloudTrail は組織の証跡を作成し、 によって設定された CloudTrail の重複を減らすためにデータイベント (Amazon S3 や など AWS Lambda) を設定するデフォルトを設定します AWS Control Tower。このソリューションには、管理イベントを設定するためのオプションが用意されています。
- AWS Config Control Tower 管理アカウント は、管理アカウント AWS Config で がリソースのコンプライアンスをモニタリングできるようにします。
- Conformance Pack Organization Rules は、組織内のアカウントと指定されたリージョンにコンフォーマンスパックをデプロイします。
- AWS Config アグリゲータ は、監査アカウント以外のメンバーアカウントに管理を委任することで、アグリゲータをデプロイします。

- Security Hub CSPM Organization は、組織内のアカウントと管理対象リージョンの委任管理者アカウント内で Security Hub CSPM を設定します。
- GuardDuty Organization は、組織内のアカウントの委任管理者アカウント内で GuardDuty を設定します。

フェーズ 4: すべてのレイヤーにセキュリティを適用する

この時点で、次のものが必要です。

- に適したセキュリティコントロール AWS アカウント。
- SCPs、RCPs、宣言型ポリシー、最小特権 IAM ロールとポリシーを通じて定義された予防コントロールを持つ明確に定義されたアカウントと OU 構造。
- を使用して AWS アクティビティをログに記録し AWS CloudTrail、 AWS Security Hub CSPM、、Amazon GuardDuty、および を使用してセキュリティイベントを検出 AWS Config し、Amazon Security Lake を使用してセキュリティのために専用のデータレイクで高度な分析を実行する機能。

このフェーズでは、「組織全体にセキュリティサービスを適用する」セクションで説明されているように、 AWS 組織の他のレイヤーにセキュリティを適用する計画を立てます。 AWS ネットワークアカウントセクションで説明されているように AWS WAF AWS Shield、 AWS Certificate Manager (ACM) AWS Firewall Manager、Amazon CloudFront AWS Network Firewall、Amazon Route 53、Amazon VPC などのサービスを使用して、 ネットワークレイヤーのセキュリティコントロールを構築できます。テクノロジースタックを下に移動するときは、ワークロードまたはアプリケーションスタックに固有のセキュリティコントロールを適用します。アプリケーションアカウント セクションで説明されているように、VPC エンドポイント、Amazon Inspector AWS Systems Manager AWS Secrets Manager、および Amazon Cognito を使用します。

設計上の考慮事項

多層防御 (DiD) セキュリティコントロールを設計するときは、スケーリング要因を検討してください。中央セキュリティチームには、環境内のすべてのアプリケーションの動作に関する帯域幅や完全な理解はありません。アプリケーションチームに、アプリケーションに適したセキュリティコントロールを特定して設計する責任と説明責任を持たせます。中央セキュリティチームは、アプリケーションチームを可能にするための適切なツールと相談の提供に集中する必要があります。が AWS セキュリティへのよりシフトレフトなアプローチを採用

するために使用するスケーリングメカニズムを理解するには、ブログ記事「セキュリティ所有権を分散するメカニズムである Security Guardians プログラム AWS の構築方法」を参照してください。

実装例

AWS SRA コードライブラリには、このフェーズに適用される以下のサンプル実装が用意されています。

- EC2 Default EBS Encryption は、提供された AWS KMS key 内のデフォルトを使用するように Amazon EC2 のデフォルトの Amazon EBS 暗号化を設定します AWS リージョン。
- S3 ブロックアカウントパブリックアクセス は、組織内のアカウントに対して Amazon S3 のアカウントレベルのブロックパブリックアクセス (BPA) 設定を構成します。
- Firewall Manager は、組織内のアカウントのセキュリティグループポリシーと AWS WAF ポリシーを設定する方法を示します。
- Inspector Organization は、組織内のアカウントと管理対象リージョンの委任管理者アカウント内で Amazon Inspector を設定します。

フェーズ 5: 転送中および保管中のデータを保護する

ビジネスデータと顧客データは、保護する必要がある貴重なアセットです。 AWS は、移動中および保管中のデータを保護するためのさまざまなセキュリティサービスと機能を提供します。 ネットワークアカウント セクションで説明されているように AWS Certificate Manager、 で Amazon CloudFront を使用して、インターネット経由で収集された転送中のデータを保護します。内部ネットワーク内で転送中のデータについては、「アプリケーションアカウント」セクションで説明されているように、 で Application Load Balancer を使用します。 AWS KMS と は、保管中のデータを保護するための暗号化キー管理を提供する AWS CloudHSM のに役立ちます。 AWS Private Certificate Authority ???

フェーズ 6: セキュリティイベントに備える

IT 環境を運用すると、セキュリティイベントが発生します。これは、セキュリティポリシー違反の可能性やセキュリティコントロールの失敗を示す、IT 環境の日常業務における変更です。セキュリティイベントをできるだけ早く認識するには、適切なトレーサビリティが不可欠です。セキュリティ

イベントがエスカレートする前に適切なアクションを実行できるように、このようなセキュリティイベントの優先順位付けと対応を準備することも同様に重要です。準備は、セキュリティイベントを迅速にトリアージして、潜在的な影響を理解するのに役立ちます。

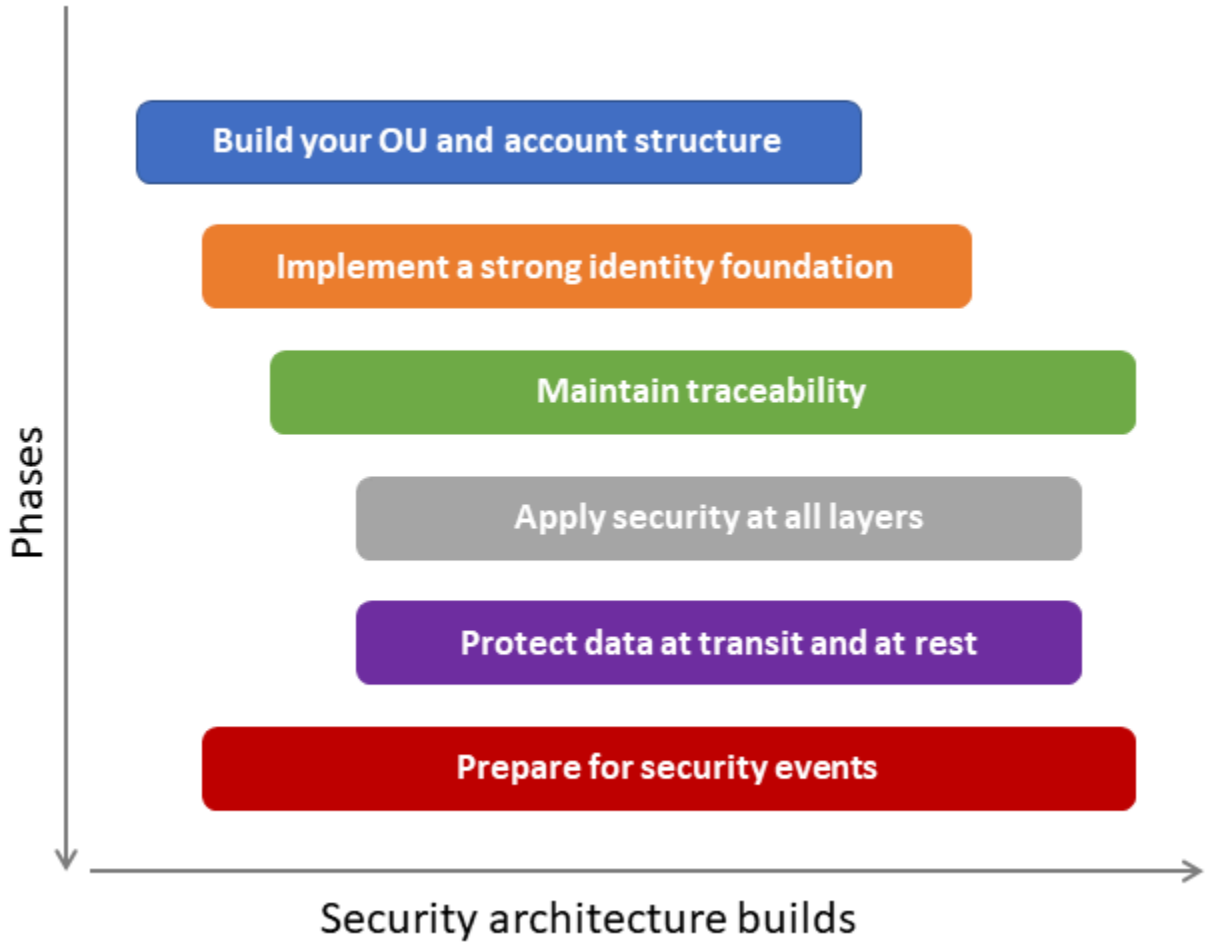
AWS SRA は、 Security Tooling アカウント の設計と すべての 内での一般的なセキュリティサービスのデプロイを通じて AWS アカウント、 組織全体のセキュリティイベント AWS を検出する機能を提供します。Security Tooling アカウント内の Amazon Detective は、セキュリティイベントの優先順位付けと根本原因の特定に役立ちます。セキュリティ調査中、関連するログを確認して、インシデントの全範囲とタイムラインを記録し、理解できる必要があります。特定の目的のアクションが発生した場合にアラートを生成するには、ログも必要です。 AWS SRA では、すべてのセキュリティログと運用ログのイミュータブルストレージとして、中央 のログアーカイブアカウント を推奨しています。 CloudWatch Logs Insights を使用して CloudWatch ロググループに保存されているデータをクエリし、Amazon Athena と Amazon OpenSearch Service を使用して Amazon S3 に保存されているデータを CloudWatch クエリできます。Amazon Security Lake を使用して、 AWS 環境、Software as a Service (SaaS) プロバイダー、オンプレミス、その他のクラウドプロバイダーのセキュリティデータを自動的に一元化します。SRA で説明されているように、Security Tooling AWS アカウントまたは専用アカウントのサブスクライバーを設定して、調査のためにそれらのログをクエリします。

AWS Security Incident Response は、セキュリティインシデント対応、調査、修復を自動化するのに役立ちます。セキュリティイベントに迅速かつ一貫して対応できるように、構築済みのプレイブックとワークフローが用意されています。プロアクティブレスポンス機能を有効にすると、Security Incident Response は Security Hub CSPM および GuardDuty と統合され、セキュリティ検出結果が検出されるとレスポンスワークフローが自動的にトリガーされます。このサービスは、 AWS 組織全体のインシデント対応プロセスを標準化および自動化するのに役立ちます。追加のサポートが必要な場合は、サービスサポートケースを開いて、カスタマーインシデント対応チーム (CIRT) AWS に連絡できます。

設計上の考慮事項

- クラウドジャーニーの最初からセキュリティイベントを検出して対応するための準備を開始する必要があります。限られたリソースをより有効に活用するには、データとビジネス重要度を AWS リソースに割り当てます。これにより、セキュリティイベントを検出したときに、関連するリソースの重要度に基づいてトリアージと対応を優先できます。
- このセクションで説明するように、クラウドセキュリティアーキテクチャを構築するためのフェーズは、本質的に順次です。ただし、次のフェーズを開始する前に、1 つのフェーズが完全に完了するのを待つ必要はありません。反復アプローチを採用することをお勧め

します。反復アプローチでは、複数のフェーズに並行して作業を開始し、クラウドセキュリティ体制を進化させるたびに各フェーズを進化させます。さまざまなフェーズを進めるにつれて、設計は進化します。次の図に示す推奨シーケンスを特定のニーズに合わせて調整することを検討してください。



実装例

AWS SRA コードライブラリは、 Detective Organization のサンプル実装を提供します。 これにより、管理をアカウント (監査やセキュリティツールなど) に委任して Amazon Detective を自動的に有効にし、既存および将来の AWS Organizations アカウント用に Detective を設定します。

AWS SRA ベストプラクティスチェックリスト

簡単なアンケートに回答して、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

このセクションでは、このガイドで詳しく説明されている AWS SRA のベストプラクティスをチェックリストにまとめています。このチェックリストに従って、セキュリティアーキテクチャのバージョンを構築できます AWS。このリストは、ガイドを確認する代替としてではなく、参照点として使用してください。チェックリストは 別にグループ化されています AWS のサービス。 AWS SRA ベストプラクティスチェックリストに照らして既存の AWS 環境をプログラムで検証する場合は、SRA Verify を使用できます。

SRA Verify は、複数の AWS アカウント およびリージョンにわたる SRA AWS に対する組織の整合性を評価するのに役立つセキュリティ評価ツールです。 AWS SRA ガイダンスに照らして実装を検証する自動チェックを提供することで、SRA AWS レコメンデーションに直接マッピングされます。このツールは、セキュリティサービスがリファレンスアーキテクチャに従って適切に設定されていることを確認するのに役立ちます。詳細な検出結果と実用的な修復手順を提供し、 AWS 環境がセキュリティのベストプラクティスに従っていることを確認します。SRA Verify は、組織監査 (セキュリティツール) アカウント AWS CodeBuild で で実行されるように設計されています。ローカルで実行することも、SRA Verify ライブラリを使用して拡張することもできます。

> **Note**
>
> SRA Verify には複数のサービスのチェックが含まれていますが、SRA AWS のすべての考慮事項のチェックが含まれているとは限りません。詳細については、AWS SRA ライブラリのガイドを参照してください。

AWS Organizations

- AWS Organizations はすべての機能で有効になっています。
- サービスコントロールポリシー (SCPs) は、IAM プリンシパルのアクセスコントロールガイドラインを定義するために使用されます。
- リソースコントロールポリシー (RCPs) は、 AWS リソースのアクセスコントロールガイドラインを定義するために使用されます。

- 宣言ポリシーは、組織全体 AWS のサービス で特定の に必要な設定を一元的に宣言して適用するために使用されます。
- 基盤サービスを提供するメンバーアカウントをグループ化するために、3 つの基盤 OUs (セキュリティ、インフラストラクチャ、ワークロード) が作成されます。
- Security Tooling アカウントは Security OU の下に作成されます。このアカウントでは、 AWS セキュリティサービスやその他のサードパーティーのセキュリティツールを一元管理できます。
- ログアーカイブアカウントは、セキュリティ OU の下に作成されます。このアカウントは、 AWS のサービス およびアプリケーションログの厳密に制御された中央ログリポジトリを提供します。
- ネットワークアカウントは、インフラストラクチャ OU の下に作成されます。このアカウントは、アプリケーションとより広範なインターネット間のゲートウェイを管理します。ネットワークサービス、設定、オペレーションを個々のアプリケーションワークロード、セキュリティ、その他のインフラストラクチャから分離します。
- 共有サービスアカウントは、インフラストラクチャ OU の下に作成されます。このアカウントは、複数のアプリケーションやチームが成果をあげるために利用するサービスをサポートしています。
- アプリケーションアカウントはワークロード OU の下に作成されます。このアカウントは、エンタープライズアプリケーションを実行および維持するためのプライマリインフラストラクチャとサービスをホストします。このガイドは表現を提供しますが、実際には、アプリケーション、開発環境、その他のセキュリティ上の考慮事項によって分離された複数の OUs とメンバーアカウントがあります。
- すべてのメンバーアカウントの請求、オペレーション、セキュリティに関する代替連絡先情報が設定されます。

AWS CloudTrail

- 組織の証跡は、管理アカウントと組織内のすべてのメンバーアカウント AWS で CloudTrail 管理イベントを配信できるように設定されています。
- 組織の証跡は、マルチリージョン証跡として設定されます。
- 組織の証跡は、グローバルリソースからイベントをキャプチャするように設定されています。
- 特定のデータイベントをキャプチャするための追加の証跡は、機密 AWS リソースアクティビティをモニタリングするために必要に応じて設定されます。
- Security Tooling アカウントは、組織の証跡の委任管理者として設定されます。
- 組織の証跡は、すべての新しいメンバーアカウントで自動的に有効になるように設定されています。

- 組織の証跡は、ログアーカイブアカウントでホストされている一元化された S3 バケットにログを発行するように設定されています。
- 組織の証跡では、ログファイルの整合性を検証するためにログファイルの検証が有効になっています。
- 組織の証跡は、ログの保持のために CloudWatch Logs と統合されています。
- 組織の証跡は、カスタマーマネージドキーを使用して暗号化されます。
- Log Archive アカウントのログリポジトリに使用される中央 S3 バケットは、カスタマーマネージドキーで暗号化されます。
- Log Archive アカウントのログリポジトリに使用される中央 S3 バケットは、イミュータビリティのために S3 オブジェクトロックで設定されています。
- バージョニングは、ログアーカイブアカウントのログリポジトリに使用される中央 S3 バケットに対して有効になります。
- Log Archive アカウントのログリポジトリに使用される中央 S3 バケットには、リソースポリシーが定義されており、リソース Amazon リソースネーム (ARN) を通じて組織の証跡によってのみオブジェクトのアップロードを制限します。

AWS Security Hub CSPM

- Security Hub CSPM は、すべてのメンバーアカウントと管理アカウントで有効になっています。
- AWS Config は、Security Hub CSPM の前提条件として、すべてのメンバーアカウントで有効になっています。
- Security Tooling アカウントは、Security Hub CSPM の委任管理者として設定されます。
- Amazon GuardDuty と Amazon Detective には、スムーズなサービス統合のために Security Hub CSPM と同じ委任管理者アカウントがあります。
- 中央設定は、複数の と にわたって Security Hub CSPM を設定 AWS アカウント および管理するために使用します AWS リージョン。
- すべての OU アカウントとメンバーアカウントは、Security Hub CSPM の委任管理者によって一元管理として指定されます。
- Security Hub CSPM は、すべての新しいメンバーアカウントで自動的に有効になります。
- Security Hub CSPM は、新しい標準の設定に対して自動的に有効になります。
- すべてのリージョンからの Security Hub CSPM の検出結果は、単一のホームリージョンに集約されます。

- すべてのメンバーアカウントからの Security Hub CSPM の検出結果は、Security Tooling アカウント内で集計されます。
- Security Hub CSPM AWS の Foundational Best Practices (FSBP) 標準は、すべてのメンバーアカウントで有効になっています。
- Security Hub CSPM の CIS AWS Foundation Benchmark 標準は、すべてのメンバーアカウントで有効になっています。
- 必要に応じて、他の Security Hub CSPM 標準が有効になっています。
- Security Hub CSPM 自動化ルールは、検出結果をリソースコンテキストで強化するために使用されます。
- Security Hub CSPM 自動応答および修復機能は、特定の検出結果に対して自動アクションを実行するカスタム EventBridge ルールを作成するために使用されます。

AWS Config

- AWS Config レコーダーは、すべてのメンバーアカウントと管理アカウントで有効になっています。
- AWS Config レコーダーはすべてのリージョンで有効になっています。
- AWS Config 配信チャネル S3 バケットは、ログアーカイブアカウントに一元化されます。
- AWS Config 委任管理者アカウントは Security Tooling アカウントに設定されます。
- AWS Config には組織アグリゲータが設定されています。アグリゲータにはすべてのリージョンが含まれます。
- AWS Config コンフォーマンスパックは、委任管理者アカウントからすべてのメンバーアカウントに均一にデプロイされます。
- AWS Config ルールの検出結果は、Security Hub CSPM に自動的に送信されます。

Amazon GuardDuty

- GuardDuty ディテクターは、すべてのメンバーアカウントと管理アカウントで有効になっています。
- GuardDuty ディテクターはすべてのリージョンで有効になっています。
- GuardDuty ディテクターは、すべての新しいメンバーアカウントで自動的に有効になります。
- GuardDuty 委任管理は Security Tooling アカウントに設定されます。

- CloudTrail 管理イベント、VPC フローログ、Route 53 Resolver DNS クエリログなどの GuardDuty 基盤データソースが有効になっています。
- GuardDuty S3 Protection が有効になっています。
- GuardDuty Malware Protection for EBS ボリュームが有効になっています。
- GuardDuty Malware Protection for S3 が有効になっています。
- GuardDuty RDS Protection が有効になっています。
- GuardDuty Lambda Protection が有効になっています。
- GuardDuty EKS Protection が有効になっています。
- GuardDuty EKS Runtime Monitoring が有効になっています。
- GuardDuty 拡張脅威検出が有効になっています。
- GuardDuty の検出結果は、ログアーカイブアカウントの中央 S3 バケットにエクスポートされ、保持されます。

IAM

- IAM ユーザーは使用されません。
- メンバーアカウントのルートアクセスの一元管理が適用されます。
- 管理アカウントの一元化された特権ルートユーザータスクは、委任された管理者から適用されます。
- 一元化されたルートアクセス管理は、Security Tooling アカウントに委任されます。
- すべてのメンバーアカウントのルート認証情報が削除されます。
- すべてのメンバーパスワードポリシーと管理 AWS アカウント パスワードポリシーは、組織のセキュリティ標準に従って設定されます。
- IAM アクセスアドバイザーは、IAM グループ、ユーザー、ロール、ポリシーの最後に使用された情報を確認するために使用されます。
- アクセス許可の境界は、IAM ロールに対して可能な最大アクセス許可を制限するために使用されます。

IAM Access Analyzer

- IAM Access Analyzer は、すべてのメンバーアカウントと管理アカウントで有効になっています。
- IAM Access Analyzer の委任管理者は Security Tooling アカウントに設定されます。

- IAM Access Analyzer の外部アクセスアナライザーは、すべてのリージョンで組織の信頼ゾーンで設定されます。
- IAM Access Analyzer の外部アクセスアナライザーは、すべてのリージョンのアカウント信頼ゾーンで設定されます。
- IAM Access Analyzer の内部アクセスアナライザーは、すべてのリージョンで組織の信頼ゾーンで設定されます。
- IAM Access Analyzer の内部アクセスアナライザーは、すべてのリージョンのアカウント信頼ゾーンで設定されます。
- 現在のアカウントの IAM Access Analyzer 未使用のアクセスアナライザーが作成されます。
- 現在の組織の IAM Access Analyzer 未使用のアクセスアナライザーが作成されます。

Amazon Detective

- Detective はすべてのメンバーアカウントで有効になっています。
- Detective は、すべての新しいメンバーアカウントで自動的に有効になります。
- Detective はすべてのリージョンで有効になっています。
- Detective の委任管理者は Security Tooling アカウントに設定されます。
- Detective、GuardDuty、および Security Hub CSPM の委任管理者は、同じ Security Tooling アカウントに設定されます。
- Detective は、未加工ログの保存と分析のために Security Lake と統合されています。
- Detective は、検出結果を取り込むために GuardDuty と統合されています。
- Detective は分析のために Amazon EKS 監査ログを取り込んでいます。
- Detective は、分析のために Security Hub CSPM ログを取り込んでいます。

AWS Firewall Manager

- Firewall Manager セキュリティポリシーが設定されています。
- Firewall Manager の委任管理者は、Security Tooling アカウントに設定されます。
- AWS Config は前提条件として有効になっています。
- 複数の Firewall Manager 管理者は、OU、アカウント、リージョンごとに制限されたスコープで設定されます。
- Firewall Manager AWS WAF セキュリティポリシーが定義されています。

- Firewall Manager の AWS WAF 集中ログ記録ポリシーが定義されています。
- Firewall Manager Shield Advanced セキュリティポリシーが定義されています。
- Firewall Manager セキュリティグループセキュリティポリシーが定義されています。

Amazon Inspector

- Amazon Inspector は、すべてのメンバーアカウントで有効になっています。
- Amazon Inspector は、新しいメンバーアカウントに対して自動的に有効になります。
- Amazon Inspector の委任管理者は Security Tooling アカウントに設定されます。
- Amazon Inspector EC2 脆弱性スキャンが有効になっています。
- Amazon Inspector ECR イメージ脆弱性スキャンが有効になっています。
- Amazon Inspector Lambda 関数とレイヤーの脆弱性スキャンが有効になっています。
- Amazon Inspector Lambda コードスキャンが有効になっています。
- Amazon Inspector コードセキュリティスキャンが有効になっています。

Amazon Macie

- Macie は、該当するメンバーアカウントに対して有効になっています。
- Macie は、該当する新しいメンバーアカウントに対して自動的に有効になります。
- Macie 委任管理者は Security Tooling アカウントに設定されます。
- Macie の検出結果は、ログアーカイブアカウントの中央 S3 バケットにエクスポートされます。
- Macie の検出結果を保存する S3 バケットは、カスタマーマネージドキーで暗号化されます。
- Macie ポリシーと分類ポリシーは Security Hub CSPM に発行されます。

Amazon Security Lake

- Security Lake 組織設定が有効になっています。
- Security Lake の委任管理者は Security Tooling アカウントに設定されます。
- Security Lake 組織設定は、新しいメンバーアカウントに対して有効になっています。
- Security Tooling アカウントは、ログの分析を実行するためのデータアクセスサブスクライバーとして設定されます。

- Security Tooling アカウントは、ログの分析を実行するためのデータクエリサブスクライバーとして設定されます。
- CloudTrail 管理ログソースは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- VPC フローログソースは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- Route 53 ログソースは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- S3 ログソースの CloudTrail データイベントは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- Lambda 実行ログソースは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- Amazon EKS 監査ログソースは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- Security Hub の検出結果ログソースは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- AWS WAF ログソースは、すべてまたは指定されたアクティブなメンバーアカウントで Security Lake に対して有効になっています。
- 委任管理者アカウントの Security Lake SQS キューは、カスタマーマネージドキーで暗号化されます。
- 委任管理者アカウントの Security Lake SQS デッドレターキューは、カスタマーマネージドキーで暗号化されます。
- Security Lake S3 バケットは、カスタマーマネージドキーで暗号化されます。
- Security Lake S3 バケットには、Security Lake による直接アクセスのみを制限するリソースポリシーがあります。

AWS WAF

- すべての CloudFront ディストリビューションが関連付けられています AWS WAF。
- すべての Amazon API Gateway REST APIsが関連付けられています AWS WAF。
- すべての Application Load Balancer が関連付けられています AWS WAF。
- すべての AWS AppSync GraphQL APIsが関連付けられています AWS WAF。
- すべての Amazon Cognito ユーザープールが関連付けられています AWS WAF。

- すべての AWS App Runner サービスが関連付けられています AWS WAF。
- すべての AWS Verified Access インスタンスが関連付けられています AWS WAF。
- すべての AWS Amplify アプリケーションが関連付けられています AWS WAF。
- AWS WAF ログ記録が有効になっています。
- AWS WAF ログは、ログアーカイブアカウントの S3 バケットに一元化されます。

AWS Shield Advanced

- Shield Advanced サブスクリプションが有効になり、パブリックリソースを持つすべてのアプリケーションアカウントに対して自動更新に設定されます。
- Shield Advanced は、すべての CloudFront ディストリビューションに対して設定されます。
- Shield Advanced は、すべての Application Load Balancer に対して設定されます。
- Shield Advanced は、すべての Network Load Balancer に対して設定されます。
- Shield Advanced は、すべての Route 53 ホストゾーンに対して設定されます。
- Shield Advanced は、すべての Elastic IP アドレスに対して設定されます。
- Shield Advanced は、すべての Global Accelerator に対して設定されます。
- CloudWatch アラームは、Shield Advanced で保護されている CloudFront リソースと Route 53 リソースに対して設定されます。
- Shield Response Team (SRT) アクセスが設定されています。
- Shield Advanced プロアクティブエンゲージメントが有効になっています。
- Shield Advanced プロアクティブエンゲージメントコンタクトが設定されています。
- Shield Advanced で保護されたリソースには、カスタム AWS WAF ルールが設定されています。
- Shield Advanced で保護されたリソースでは、アプリケーションレイヤー DDoS 自動緩和が有効になっています。

AWS セキュリティインシデント対応

- AWS セキュリティインシデント対応は組織全体 AWS で有効になっています。
- AWS Security Incident Response の委任管理者は Security Tooling アカウントに設定されます。
- プロアクティブレスポンスとアラートのトリアージワークフローが有効になっています。
- AWS Customer Incident Response Team (CIRT) の封じ込めアクションが承認されます。

AWS Audit Manager

- Audit Manager は、すべてのメンバーアカウントで有効になっています。
- Audit Manager は、新しいメンバーアカウントに対して自動的に有効になります。
- Audit Manager の委任管理者は、Security Tooling アカウントに設定されます。
- AWS Config は、Audit Manager の前提条件として有効になっています。
- カスタマーマネージドキーは、Audit Manager に保存されているデータに使用されます。
- デフォルトの評価レポートの送信先が設定されています。

IAM リソース

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS Identity and Access Management (IAM) は従来のアーキテクチャ図に含まれるサービスではありませんが、 AWS 組織のあらゆる側面、 AWS アカウント、および に影響します AWS のサービス。IAM エンティティを作成し、最初にアクセス許可を付与 AWS のサービス しない限り、 をデプロイすることはできません。IAM の完全な説明は、このドキュメントの範囲外ですが、このセクションでは、ベストプラクティスの推奨事項と追加のリソースへのポインタの重要な概要を提供します。

- IAM のベストプラクティスについては、「 AWS ドキュメント」の「IAM のセキュリティのベストプラクティス」、 AWS 「 セキュリティブログ」の「IAM 記事」、およびAWS 「re:Invent プレゼンテーション」を参照してください。
- AWS Well-Architected セキュリティの柱は、アクセス許可管理プロセスの主要なステップの概要を示しています。アクセス許可ガードレールの定義、最小特権アクセスの付与、パブリックアクセスとクロスアカウントアクセスの分析、リソースの安全な共有、アクセス許可の継続的な削減、緊急アクセスプロセスの確立です。
- 次の表とそれに付随するメモは、使用可能な IAM アクセス権限ポリシーの種類と、セキュリティアーキテクチャでのそれらの使用方法に関する推奨ガイダンスの概要を示しています。詳細については、次を参照してください。AWS re:Invent 2020のビデオで IAMポリシーの適切な組み合わせを選択について 参照してください。

ユースケースまたはポリシー	[Effect] (効果)	による管理	目的	に関連	影響	にデプロイ
サービスコントロールポリシー (SCP)	Restrict	プラットフォームチームやセキュリティチームなど	ガードレール、ガバナンス	組織、OU、アカウント	Organization、OU、および アカウントのすべてのプリンシパル	組織管理アカウント [2]

		の中央チーム [1]				
リソースコントロールポリシー (RCPs)	Restrict	プラットフォームチームやセキュリティチームなどの中央チーム [1]	ガードレール、ガバナンス	組織、OU、アカウント	メンバーアカウントのリソース [12]	組織管理アカウント [2]
ベースラインアカウントの自動化ポリシー (アカウントを運用するためにプラットフォームが使用する IAM ロール)	許可と制限	プラットフォーム、セキュリティ、IAM チームなどの中央チーム [1]	(ベースライン) 非ワークロード自動化ロールのアクセス許可 [3]	単一アカウント [4]	メンバーアカウント内のオートメーションで使用されるプリンシパル	メンバーアカウント
ベースラインヒューマンポリシー (作業を実行するためのアクセス許可をユーザーに付与する IAM ロール)	許可と制限	プラットフォーム、セキュリティ、IAM チームなどの中央チーム [1]	ヒューマンロールのアクセス許可 [5]	単一アカウント [4]	フェデレーティッドプリンシパル [5] と IAM ユーザー [6]	メンバーアカウント

アクセス許可の境界 (権限のある開発者が別のプリンシパルに割り当てることができるアクセス許可の最大数)	Restrict	プラットフォーム、セキュリティ、IAM チームなどの中央チーム [1]	アプリケーションロールのガードレール (適用する必要があります)	単一アカウント [4]	このアカウントのアプリケーションまたはワークロードの個々のロール [7]	メンバーアカウント
アプリケーションのマシンロールポリシー (開発者がデプロイしたインフラストラクチャにアタッチされたロール)	許可と制限	デベロッパーに委任 [8]	アプリケーションまたはワークロードのアクセス許可 [9]	単一のアカウント	このアカウントのプリンシパル	メンバーアカウント
リソースポリシー	許可と制限	開発者に委任 [8,10]	リソースへのアクセス許可	単一のアカウント	アカウントのプリンシパル [11]	メンバーアカウント
中央ルートユーザー管理	許可と制限	プラットフォーム、セキュリティ、IAM チームなどの中央チーム [1]	メンバーアカウントのルートユーザーを大規模に一元管理する	組織	メンバーアカウントのすべてのルートユーザー	組織管理アカウント、委任管理者アカウント

テーブルからのメモ:

1. 企業には、これらの独立したコントロールの責任と相互のポリシーを分担する集中型チーム (クラウドプラットフォーム、セキュリティオペレーション、アイデンティティおよびアクセス管理チームなど) が多数あります。表の例はプレースホルダです。お客様の企業にとって最も効果的な職務の分離を決定する必要があります。
2. SCPs を使用するには、 内のすべての機能を有効にする必要があります AWS Organizations。
3. パイプラインのアクセス許可、デプロイツール、モニタリングツール (AWS Lambda や など AWS Config ルール)、その他のアクセス許可など、自動化を有効にするには、一般的に共通のベースラインロールとポリシーが必要です。この設定は、通常、アカウントのプロビジョニング時に提供されます。
4. これらは 1 つのアカウントのリソース (ロールやポリシーなど) に関連していますが、AWS CloudFormation StackSets を使用して複数のアカウントにレプリケートまたはデプロイできます。
5. 中央チームによってすべてのメンバーアカウントに展開される (多くの場合、アカウントのプロビジョニング中)、基本的な人間の役割とポリシーのコアセットを定義します。例としては、プラットフォームチームの開発者、IAM チーム、セキュリティ監査チームなどがあります。
6. 可能であれば、(ローカルの IAM ユーザーの代わりに) ID フェデレーションを使用します。
7. 権限の境界は、委任された管理者によって使用されます。この IAM ポリシーでは、アクセス許可の上限を定義し、その他のポリシー (リソースに対するすべてのアクションを許可する "*:*" ポリシー) をオーバーライドします。ロール (ワークロードパフォーマンスロールなど) を作成し、ポリシーをアタッチするための条件として、ベースラインのヒューマンポリシーでアクセス許可の境界が必要です。SCP などの追加設定では、権限境界の添付が強制されます。
8. これは、十分なガードレール (SCP や権限境界など) がデプロイされていることを前提としています。
9. これらのオプションポリシーは、アカウントのプロビジョニング中またはアプリケーション開発プロセスの一部として配信できます。これらのポリシーを作成してアタッチするアクセス許可は、アプリケーション開発者自身のアクセス許可によって管理されます。
10. ローカルアカウントのアクセス許可に加えて、一元化されたチーム (クラウドプラットフォームチームやセキュリティオペレーションチームなど) は、多くの場合、一部のリソースベースのポリシーを管理し、アカウントを運用するためのクロスアカウントアクセスを有効にします (ログ記録用の S3 バケットへのアクセスを提供するなど) 。
11. リソースベースの IAM ポリシーは、任意のアカウントの任意のプリンシパルを参照して、そのリソースへのアクセスを許可または拒否できます。また、匿名プリンシパルを参照してパブリックアクセスを有効にすることもできます。

12RCPs、 のサブセットのリソースに適用されます AWS のサービス。詳細については、 ドキュメントの「RCP AWS のサービス をサポートする のリスト RCPs」を参照してください。 AWS Organizations

IAM アイデンティティが明確に定義された一連のタスクに必要なアクセス許可のみを持つようにすることは、悪意のあるまたは意図しないアクセス権限の悪用のリスクを軽減するために重要です。最小限の特権を認めるモデル を確立し、維持するには、超過特権を継続的に更新、評価、軽減するための意図的な計画が必要です。ここでは、そのプランに関するその他のレコメンデーションを示します。

- 組織のガバナンスモデルと確立されたリスク選好度を使用して、特定のガードレールとアクセス許可の境界を確立します。
- 継続的な反復プロセスを通じて最小特権を実装します。この演習を行うのは 1 回限りではありません。
- SCP を使用して、実用的なリスクを軽減します。これらは、狭義のターゲットコントロールではなく、幅広いガードレールを目的としています。
- アクセス権限の境界を使用して、より安全な方法で IAM 管理を委任します。
  - 委任された管理者が、作成したロールとユーザーに適切な IAM 境界ポリシーをアタッチしていることを確認します。
- 詳細な防御アプローチとして (アイデンティティベースのポリシーと組み合わせて)、リソースベースの IAM ポリシーを使用して、リソースへの広範なアクセスを拒否します。
- IAM アクセスアドバイザー、 AWS CloudTrail、IAM Access Analyzer、および関連するツールを使用して、付与された使用状況とアクセス許可の履歴を定期的に分析します。明らかなオーバーパーミッションをすぐに修正します。
- アスタリスクをワイルドカードとして使用し、すべてのリソースを示す代わりに、幅広いアクションを特定のリソースに適用します。
- リクエストに基づいて IAM ポリシーの例外を迅速に識別、確認、承認するメカニズムを実装します。

SRA AWS のコードリポジトリの例

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

AWS SRA でガイダンスの構築と実装を開始できるように、https://github.com/aws-samples/aws-security-reference-architecture-examples の Infrastructure as Code (IaC) リポジトリにこのガイドが付属しています。このリポジトリには、デベロッパーとエンジニアがこのドキュメントで説明されているガイダンスとアーキテクチャパターンの一部をデプロイするのに役立つコードが含まれています。このコードは、 AWS プロフェッショナルサービスコンサルタントのお客様との直接の経験に基づいています。テンプレートは本質的に一般的なものであり、完全なソリューションを提供するのではなく、実装パターンを説明することが目的です。 AWS のサービス 設定とリソースのデプロイは、意図的に非常に制限されています。環境やセキュリティのニーズに合わせて、これらのソリューションを変更して調整する必要がある場合があります。

AWS SRA コードリポジトリは、 AWS CloudFormation と Terraform の両方のデプロイオプションを含むコードサンプルを提供します。ソリューションパターンは 2 つの環境をサポートします。1 つは を必要とし AWS Control Tower 、もう 1 つは AWS Organizations なしで使用します AWS Control Tower。このリポジトリで を必要とするソリューションは、 および Customizations for AWS Control Tower (CfCT) を使用してAWS Control Tower環境内でデプロイ AWS CloudFormationおよびテスト AWS Control Tower されています。不要なソリューションは、 AWS Organizationsを使用して環境内でテスト AWS Control Tower されています AWS CloudFormation。CfCT ソリューションは、 AWS お客様がベストプラクティスに基づいて安全なマルチアカウント AWS 環境を迅速にセットアップするのに役立ちます。アカウントとリソースの作成を通じて初期セキュリティベースラインを実装しながら、安全でスケーラブルなワークロードを実行する環境のセットアップを自動化することで、時間を節約できます。また、 は、マルチアカウントアーキテクチャ、アイデンティティとアクセスの管理、ガバナンス、データセキュリティ、ネットワーク設計、ログ記録を開始するためのベースライン環境 AWS Control Tower も提供します。 AWS SRA リポジトリのソリューションは、このドキュメントで説明されているパターンを実装するための追加のセキュリティ設定を提供します。

AWS SRA リポジトリ内のソリューションの概要を次に示します。各ソリューションには、詳細を含む `README.md` ファイルが含まれています。

- CloudTrail Organization ソリューションは、組織管理アカウント内に組織の証跡を作成し、監査やセキュリティツールアカウントなどのメンバーアカウントに管理を委任します。この証跡

は、Security Tooling アカウントで作成されたカスタマーマネージドキーで暗号化され、ログアーカイブアカウントの S3 バケットにログを配信します。必要に応じて、Amazon S3 および AWS Lambda 関数でデータイベントを有効にすることができます。組織の証跡は、メンバーアカウントが設定を変更できないようにしながら、 AWS 組織 AWS アカウント 内のすべての のイベントをログに記録します。

- GuardDuty Organization ソリューションは、Security Tooling アカウントに管理を委任することで、Amazon GuardDuty を有効にします。すべての既存および将来の AWS 組織アカウントについて、Security Tooling アカウント内で GuardDuty を設定します。GuardDuty の結果も KMS キーで暗号化され、ログアーカイブアカウントの S3 バケットに送信されます。
- Security Hub CSPM Organization ソリューションは、Security Tooling アカウントに管理を委任することで、Security Hub CSPM を設定します。すべての既存および将来の AWS 組織アカウントの Security Tooling アカウント内で Security Hub CSPM を設定します。このソリューションでは、すべてのアカウントとリージョンで有効なセキュリティ標準を同期し、Security Tooling アカウント内でリージョンアグリゲータを設定するためのパラメータも提供します。Security Tooling アカウント内の Security Hub CSPM を一元化すると、セキュリティ標準のコンプライアンスと、 AWS のサービス とサードパーティー AWS Partner の統合の結果をクロスアカウントで確認できます。
- Inspector ソリューションは、組織内のすべての AWS アカウントと管理対象リージョンの委任管理者 (セキュリティツール) アカウント内で Amazon Inspector を設定します。
- Firewall Manager ソリューションは、Security Tooling アカウントに管理を委任し、 AWS Firewall Manager セキュリティグループポリシーと複数の AWS WAF ポリシーを使用して Firewall Manager を設定することで、セキュリティポリシーを設定します。セキュリティグループポリシーには、ソリューションによってデプロイされる VPC (既存またはソリューションによって作成された) 内の最大許容セキュリティグループが必要です。
- Macie Organization ソリューションでは、管理を Security Tooling アカウントに委任することで Amazon Macie を有効にします。すべての既存および将来の AWS 組織アカウントについて、Security Tooling アカウント内で Macie を設定します。Macie は、KMS キーで暗号化された中央の S3 バケットにディスカバリ結果を送信するようにさらに構成されています。
- AWS Config:
  - Config Aggregator ソリューションは、Security Tooling AWS Config アカウントに管理を委任してアグリゲータを設定します。次に、このソリューションは、 AWS 組織内のすべての既存アカウントと将来のアカウントに対して Security Tooling AWS Config アカウント内にアグリゲータを設定します。
  - Conformance Pack Organization Rules ソリューションは、Security Tooling アカウントに管理を委任 AWS Config ルール してデプロイします。次に、組織内のすべての既存および将来のアカウントの委任管理者アカウント内に AWS 組織コンフォーマンスパックを作成します。このソ

リューションは、暗号化とキー管理の運用上のベストプラクティスコンフォーマンスパックのサンプルテンプレートをデプロイするように設定されています。

  - AWS Config Control Tower 管理アカウントソリューションは、 AWS Control Tower 管理アカウント AWS Config で を有効にし、それに応じて Security Tooling AWS Config アカウント内のアグリゲータを更新します。このソリューションでは、 AWS Control Tower CloudFormation テンプレートを使用して をリファレンス AWS Config として有効にし、 AWS 組織内の他のアカウントとの整合性を確保します。

- IAM:
  - Access Analyzer ソリューションは、Security Tooling アカウントに管理を委任することで、IAM Access Analyzer を有効にします。次に、組織内のすべての既存および将来のアカウントについて、Security Tooling アカウント内で AWS 組織レベルの IAM Access Analyzer を設定します。このソリューションは、アカウントレベルのアクセス許可の分析をサポートするために、IAM Access Analyzer をすべてのメンバーアカウントとリージョンにデプロイします。
  - IAM パスワードポリシーソリューションは、 AWS アカウント AWS 組織内のすべてのアカウント内のパスワードポリシーを更新します。このソリューションには、業界のコンプライアンス標準に合わせてパスワードポリシーを設定するためのパラメータが用意されています。
- EC2 デフォルト EBS 暗号化ソリューションは、各 AWS アカウント および組織 AWS リージョン内の AWS アカウントレベルのデフォルトの Amazon EBS 暗号化を有効にします。これにより、作成した新しい EBS ボリュームとスナップショットの暗号化が強制されます。例えば、Amazon EBS は、インスタンスの起動時に作成される EBS ボリュームと、暗号化されていないスナップショットからコピーするスナップショットを暗号化します。
- S3 ブロックアカウントパブリックアクセスソリューションは、 AWS 組織 AWS アカウント 内の各 内で Amazon S3 アカウントレベルの設定を有効にします。Amazon S3 のパブリックアクセスブロック機能は、Amazon S3 のリソースへのパブリックアクセスの管理に役立つ、アクセスポイント、バケット、アカウントの設定を提供します。デフォルトでは、新しいバケット、アクセスポイント、およびオブジェクトはパブリックアクセスを許可しません。ただし、ユーザーはバケットポリシー、アクセスポイントポリシー、またはオブジェクトのアクセス許可を変更することで、パブリックアクセスを許可できます。Amazon S3 パブリックアクセスブロック設定は、これらのポリシーとアクセス許可を上書きして、これらのリソースへのパブリックアクセスを制限できるようにします。
- Detective Organization ソリューションは、管理を アカウント (監査またはセキュリティツールアカウントなど) に委任し、既存および将来のすべての AWS Organizations アカウントに対して Detective を設定することで、Amazon Detective の有効化を自動化します。
- Shield Advanced ソリューションは、 のデプロイを自動化 AWS Shield Advanced して、 上のアプリケーションに拡張 DDoS 保護を提供します AWS。

- AMI Bakery Organization ソリューションは、標準の強化された Amazon マシンイメージ (AMI) イメージの構築と管理のプロセスを自動化するのに役立ちます。これにより、 AWS インスタンス間の一貫性とセキュリティが確保され、デプロイとメンテナンスのタスクが簡素化されます。
- Patch Manager ソリューションは、複数の にわたるパッチ管理を効率化するのに役立ちます AWS アカウント。このソリューションを使用して、すべてのマネージドインスタンスで AWS Systems Manager エージェント (SSM エージェント) を更新し、Windows および Linux のタグ付けされたインスタンスで重要かつ重要なセキュリティパッチとバグ修正をスキャンしてインストールできます。このソリューションは、新しい の作成を検出 AWS アカウント し、それらのアカウントにソリューションを自動的にデプロイするように、デフォルトのホスト管理設定も設定します。

寄稿者

プライマリ作成者:

- Avik Mukherjee、 AWS Senior Security SA

寄稿者:

- Jason Hurst、 AWS CIRT シニアセキュリティ調査担当者
- Abhishek Panday、 AWS Principal Product Manager – Tech
- Itay Meller、 AWS シニアスペシャリスト SA
- Jonathan VanKim、 AWS Principal Security SA
- Josh Du Lac、 AWS エンタープライズセキュリティストラテジスト
- James Thompson、 AWS シニアソリューションアーキテクト
- Jeremy Girven、 AWS スペシャリスト SA
- Rodney Underkoffler、 AWS スペシャリストシニア SA
- Farhan Farooq、 AWS シニアソリューションアーキテクト
- Prashob Krishnan、 AWS テクニカルアカウントマネージャー
- Meg Peddada、 AWS シニアセキュリティコンサルタント
- Ashwin Phadke、 AWS シニアソリューションアーキテクト
- Sowjanya Rajavaram、 AWS Senior Security SA
- Tomek Jakubowski、 AWS シニアコンサルタント
- Arun Thomas、 AWS シニアソリューションアーキテクト
- Ross Warren、 AWS 製品ソリューションアーキテクト
- Scott Conklin、 AWS シニアコンサルタント
- Ilya Epshteyn、アイデンティティソリューション担当 AWS シニアマネージャー
- Michael Haken、 AWS プリンシパル技術者
- Mehial Mendrin、 AWS シニアコンサルタント
- Christopher Evensen、 AWS シニアテクニカルアカウントマネージャー

確認:

- Eric Rose、 AWS Principal Security SA
- Manoj Kumar、 AWS 配信コンサルタント

テクニカルライティング:

- Handan Selamoglu、 AWS シニアテクニカルライター

付録: AWS セキュリティ、アイデンティティ、コンプライアンスサービス

簡単な調査を行い、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA) の未来に影響を与えます。

入門または復習については、「 AWS ウェブサイト」の「セキュリティ、アイデンティティ、コンプライアンス AWS」で、クラウド内のワークロードとアプリケーションを保護する AWS のサービス のに役立つ のリストを参照してください。これらのサービスは、データ保護、ID とアクセスの管理、ネットワークとアプリケーションの保護、脅威の検出と継続的なモニタリング、コンプライアンスとデータプライバシーの 5 つのカテゴリに分類されます。

データ保護 – データ、アカウント、ワークロードを不正アクセスから保護するのに役立つサービス AWS を提供します。

- Amazon Macie: 機械学習によるセキュリティ機能で、機密データの検出、分類、保護を行います。
- AWS KMS – データの暗号化に使用されるキーを作成して制御します。
- AWS CloudHSM– でハードウェアセキュリティモジュール (HSMs) を管理します AWS クラウド。
- AWS Certificate Manager – で使用する SSL/TLS 証明書をプロビジョニング、管理、デプロイします AWS のサービス。
- AWS Secrets Manager – ライフサイクルを通じて、データベース認証情報、API キー、その他のシークレットをローテーション、管理、取得します。

Identity & Access Management – AWS ID サービスを使用すると、ID、リソース、アクセス許可を大規模に安全に管理できます。

- IAM – AWS のサービス および リソースへのアクセスを安全に制御します。
- IAM Identity Center – 複数の AWS アカウント およびビジネスアプリケーションへの SSO アクセスを一元管理します。
- Amazon Cognito: Web およびモバイルアプリケーションに、ユーザーサインアップ、サインイン、アクセス制御を追加します。
- AWS Directory Service – でマネージド Microsoft Active Directory を使用します AWS クラウド。

- AWS RAM – AWS リソースを簡単かつ安全に共有します。
- AWS Organizations – 複数の にポリシーベースの管理を実装します AWS アカウント。
- Amazon Verified Permissions – カスタムアプリケーションのスケーラブルできめ細かなアクセス許可と認可を管理します。

ネットワークとアプリケーションの保護 – これらのサービスのカテゴリを使用すると、組織全体のネットワークコントロールポイントにきめ細かなセキュリティポリシーを適用できます。 AWS のサービス は、トラフィックを検査およびフィルタリングして、ホストレベル、ネットワークレベル、およびアプリケーションレベルの境界での不正なリソースアクセスを防ぐのに役立ちます。

- AWS Shield – マネージド DDoS 保護 AWS を使用して、 で実行されるウェブアプリケーションを保護します。
- AWS WAF – 一般的なウェブエクスプロイトからウェブアプリケーション を保護し、可用性とセキュリティを確保します。
- AWS Firewall Manager – AWS アカウント および アプリケーション間の AWS WAF ルールを一元的に設定および管理します。
- AWS Systems Manager – OS パッチの適用、安全なシステムイメージの作成、安全なオペレーティングシステムの設定を行うように Amazon EC2 とオンプレミスシステムを設定および管理します。
- Amazon VPC – 論理的に隔離された セクションをプロビジョニングし、定義した仮想ネットワークで AWS リソースを起動 AWS できるようにします。
- AWS Network Firewall – VPCs に不可欠なネットワーク保護をデプロイします。
- Amazon Route 53 DNS Firewall – VPCs からのアウトバウンド DNS リクエストを保護します。
- AWS Verified Access – 仮想プライベートネットワーク (VPNs) を必要とせずに、アプリケーションへの安全なアクセスを提供します。
- Amazon VPC Lattice – service-to-service接続、セキュリティ、モニタリングを簡素化します。

脅威検出と継続的なモニタリング – AWS モニタリングおよび検出サービスは、 AWS 環境内の潜在的なセキュリティインシデントを特定するのに役立つガイダンスを提供します。

- AWS Security Hub CSPM：セキュリティアラートを表示および管理し、一元的な場所からコンプライアンスチェックを自動化します。
- AWS Security Hub – セキュリティの検出結果を関連付けて強化し、アカウントと 全体で重大なセキュリティ問題を優先します AWS リージョン。

- Amazon GuardDuty – インテリジェントな脅威検出と継続的なモニタリングにより AWS アカウント 、 および ワークロードを保護します。
- Amazon Inspector： AWSにデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるためのセキュリティ評価を自動化します。
- AWS Config – AWS リソースの設定を記録して評価し、コンプライアンス監査、リソース変更の追跡、セキュリティ分析を有効にします。
- AWS Config ルール: リソースの分離、追加データによるイベントの強化、既知の正常な状態への構成の復元など、環境内の変更に応じて自動的にアクションを実行するルールを作成します。
- AWS Security Incident Response – 構築済みのプレイブックとワークフローを使用して、セキュリティインシデント対応、調査、修復を自動化します。
- AWS CloudTrail – ユーザーアクティビティと API 使用状況を追跡して、 のガバナンス、運用、リスク監査を可能にします AWS アカウント。
- Amazon Detective：セキュリティデータを分析して視覚化し、潜在的なセキュリティ問題の根本原因を迅速に把握できます。
- AWS Lambda: サーバのプロビジョニングや管理を行わずにコードを実行し、インシデントに対するプログラム化された自動応答を拡張できます。

コンプライアンスとデータプライバシー – ビジネス AWS が従う AWS ベストプラクティスと業界標準に基づいて自動化されたコンプライアンスチェックを使用して、コンプライアンスステータスを包括的に把握し、環境を継続的にモニタリングします。

- AWS Artifact – 無料のセルフサービスポータルを使用して、 AWS セキュリティおよびコンプライアンスレポートへのオンデマンドアクセスを取得し、オンライン契約を選択します。
- AWS Audit Manager – AWS 使用状況を継続的に監査し、リスクと規制や業界標準への準拠を評価する方法を簡素化します。

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
コンテンツの再構築と更新	• Security Hub と AWS Nitro Enclaves のガイダンスを追加しました。 • AWS SRA を再構築してコアアーキテクチャに焦点を当て、詳細なセクションをアイデンティティ管理、境界セキュリティ、サイバーフォレンジック、生成 AI、IoT の個別のガイドに移動しました。 • AWS CloudTrail、、Amazon Detective AWS Config、、Amazon GuardDuty AWS Firewall Manager、IAM Access Analyzer、Amazon Security Lake AWS Shield Advanced、および の追加の詳細を含むように既存のガイダンスを更新しました AWS Audit Manager。	2025 年 12 月 22 日
主な更新	• 新しい IAM 集中ルートユーザーアクセス管理、リソースコントロールポリシー (RCPs)、宣言ポリシーに関する情報を追加しました。	2025 年 8 月 29 日

- Security Hub CSPM の新しい Security Hub CSPM への参照を更新しました。
- Amazon GuardDuty と Security Hub CSPM の新しいサービス機能を追加しました。
- AWS Security Incident Response サービスガイダンスを追加しました。
- IAM ディープダイブガイダンスを更新し、machine-to-machine ID 管理用の VPC Lattice を追加しました。
- 新しい詳細なガイダンス「SRA for IoT」を追加しました。

追加と明確化	• Security Tooling アカウントセクションで、ガイダンスを更新しました AWS KMS 。 • 「顧客 ID 管理」セクションで、API Gateway の認可に関する情報を展開しました。 • Generative AI セクションを更新し、OU とアカウント設計の設計上の考慮事項を追加しました。 • AWS SRA コードリポジトリセクションに、新しいパッチ管理ソリューションに関する情報を追加しました。	2024 年 9 月 12 日

主な更新	• 詳細なアーキテクチャガイダンスとして、Amazon Bedrock を使用した生成 AI と ID 管理の 2 つのセクションを追加しました。 • AWS Identity and Access Management Access Analyzer、Amazon Detective、Amazon Inspector、AWS Artifact、AWS Config、Amazon Security Lake、AWS Security Hub CSPM、Amazon CloudFront の各セクションを新しいサービス機能で更新しました。 • AWS SRA コードリポジトリセクションを更新し、新しい Terraform デプロイオプションと AWS Shield Advanced および AMI Bakery ソリューションを追加しました。	2024 年 6 月 7 日

主な更新	• ネットワークアカウントとアプリケーションアカウントのセクションを更新し、Amazon Verified Permissions AWS Verified Access、および Amazon VPC Lattice のアーキテクチャガイダンスを追加しました。 • セキュリティ機能に基づく詳細なアーキテクチャガイダンスを追加しました。 • AI/ML AWS のサービス を使用してセキュリティ上の成果を向上させる方法に関する新しいガイダンスを追加しました。 • セキュリティアーキテクチャを段階的に計画する方法に関するガイダンスを追加しました。	2023 年 11 月 4 日
Security Lake の追加	Security Tooling アカウントと Log Archive アカウントセクションを更新し、Amazon Security Lake に関連する設計ガイダンスを追加しました。	2023 年 9 月 22 日

マイナーな更新	• 新機能 AWS のサービスとベストプラクティスを反映するように既存のガイダンスを更新しました。 • AWS CloudTrail、 AWS IAM アイデンティティセンター、エッジセキュリティのアーキテクチャガイダンスを更新しました。	2023 年 5 月 10 日
アンケート	組織での SRA AWS の使用方法をよりよく理解するための簡単なアンケートを追加しました。	2022 年 12 月 14 日
リファレンスアーキテクチャ図のソースファイル	AWS セキュリティリファレンスアーキテクチャセクションで、編集可能な PowerPoint 形式でこのガイドのアーキテクチャ図を提供するダウンロードファイルを追加しました。	2022 年 11 月 17 日
セキュリティ基盤の更新セクション	セキュリティ基盤セクションで、 Well-Architected フレームワークの柱とセキュリティ設計原則に関する情報を更新しました。	2022 年 9 月 27 日

主な追加と更新	• SRA AWS の使用方法と主要な実装ガイドラインに関する情報を追加しました。 • AWS Artifact、Amazon Inspector、Amazon Route 53、 AWS Control Tower AWS Audit Manager、 AWS RAM Amazon Directory Service Amazon Cognito、Network Access Analyzer AWS のサービス などの追加のアーキテクチャガイダンスを追加しました。 • 新機能 AWS のサービス とベストプラクティスを反映するように既存のガイダンスを更新しました。	2022 年 7 月 25 日
二	初版発行	2021 年 6 月 23 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範ガイダンスが提供する戦略、ガイド、パターンで一般的に使用される用語です。エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

数字

7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行する。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例： Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。
- 廃止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセス制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

アクティブ/アクティブ移行

(双方向レプリケーションツールまたは二重書き込み操作を使用して) ソースデータベースとターゲットデータベースを同期させ、移行中に両方のデータベースが接続アプリケーションからのトランザクションを処理するデータベース移行方法。この方法では、1 回限りのカットオーバーの必要がなく、管理された小規模なバッチで移行できます。アクティブ/パッシブ移行よりも柔軟な方法ですが、さらに多くの作業が必要となります。

アクティブ/パッシブ移行

ソースデータベースとターゲットデータベースを同期させながら、データがターゲットデータベースにレプリケートされている間、接続しているアプリケーションからのトランザクションをソースデータベースのみで処理するデータベース移行方法。移行中、ターゲットデータベースはトランザクションを受け付けません。

集計関数

複数行に処理を行い、グループ全体を対象に単一の戻り値を計算する SQL 関数。集計関数の例としては、SUM や MAX などがあります。

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

データセット内の個人情報を完全に削除するプロセス。匿名化は個人のプライバシー保護に役立ちます。匿名化されたデータは、もはや個人データとは見なされません。

アンチパターン

繰り返し起こる問題に対して頻繁に用いられる解決策で、その解決策が逆効果であったり、効果がなかったり、代替案よりも効果が低かったりするもの。

アプリケーション制御

マルウェアからシステムを保護するために、承認されたアプリケーションのみを使用できるようにするセキュリティアプローチ。

アプリケーションポートフォリオ

アプリケーションの構築と維持にかかるコスト、およびそのビジネス価値を含む、組織が使用する各アプリケーションに関する詳細情報の集まり。この情報は、ポートフォリオの検出と分析プロセス の重要な要素であり、移行、モダナイズ、最適化するアプリケーションを特定し、優先順位を付けるのに役立ちます。

人工知能 (AI)

コンピューティングテクノロジーを使用し、学習、問題の解決、パターンの認識など、通常は人間に関連づけられる認知機能の実行に特化したコンピュータサイエンスの分野。詳細については、「人工知能 (AI) とは何ですか?」をご覧ください。

AI オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。 AWS 移行戦略での AIOps の使用方法については、オペレーション統合ガイド を参照してください。

非対称暗号化

暗号化用のパブリックキーと復号用のプライベートキーから成る 1 組のキーを使用した、暗号化のアルゴリズム。パブリックキーは復号には使用されないため共有しても問題ありませんが、プライベートキーの利用は厳しく制限する必要があります。

原子性、一貫性、分離性、耐久性 (ACID)

エラー、停電、その他の問題が発生した場合でも、データベースのデータ有効性と運用上の信頼性を保証する一連のソフトウェアプロパティ。

属性ベースのアクセス制御 (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、 AWS Identity and Access Management (IAM) ドキュメントの「 の ABAC AWS」を参照してください。

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン (AZ)

他のアベイラビリティーゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティーゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るための、 のガイドラインとベストプラクティスのフレームワークです。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスをまとめています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、クラウド導入を成功させるための組織の準備に役立つ人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、AWS CAF ウェブサイトと AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool (AWS SCT) に含まれています。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他同様のアクションを調べることができます。詳細については、Detective ドキュメントの「動作グラフのデータ」を参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 1 つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

ブルー/グリーンデプロイ

それぞれが独立しているが、同一の環境を 2 つ作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンを別の環境 (グリーン) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

ボット

インターネット経由で自動タスクを実行し、人間のアクティビティややり取りをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボットと呼ばれる他のボットの中には、個人や組織を混乱させたり、損害を与えたりすることを意図したものもあります。

ボットネット

マルウェアに感染しており、ボットハーダーまたはボットオペレーターと呼ばれる単一の当事者によって制御されているボットのネットワーク。ボットネットは、ボットとその影響力を拡大する仕組みとして、非常によく知られています。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発した

り、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチの概要」(GitHub ドキュメント) を参照してください。

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようにします。詳細については、 AWS Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータを参照してください。

ブラウンフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウンフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、AWSでのコンテナ化されたマイクロサービスの実行ホワイトペーパーの「ビジネス機能を中心に組織化」セクションを参照してください。

ビジネス継続性計画 (BCP)

大規模移行など、中断を伴うイベントが運用に与える潜在的な影響に対処し、ビジネスを迅速に再開できるようにする計画。

C

CAF

「AWS クラウド導入フレームワーク」を参照してください

カナリアデプロイ

エンドユーザーへのバージョンリリースを、時間をかけて段階的に行うこと。確信が持てたら新規バージョンをデプロイして、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「変更データキャプチャ」を参照してください。

変更データキャプチャ (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストすること。AWS Fault Injection Service (AWS FIS) を使用して、 AWS ワークロードにストレスを与え、その応答を評価する実験を実行できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、ローカルでデータを暗号化します。

Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、 AWS クラウド エンタープライズ戦略ブログの CCoE 投稿を参照してください。

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的に、エッジコンピューティングに接続されています。

クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、「クラウド運用モデルの構築」を参照してください。

導入のクラウドステージ

組織が、 AWS クラウドへの移行時に通常実行する 4 つの段階。

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、運用モデルの確立など)
- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。移行戦略との関連性については、 AWS「移行準備ガイド」を参照してください。

CMDB

「構成管理データベース (CMDB)」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、GitHub や Bitbucket Cloud があります。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオといった、ビジュアル形式の情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI では、CV 用の画像処理アルゴリズムを利用できます。

設定ドリフト

ワークロードにおいて、設定が想定した状態から変化すること。これによって、ワークロードが非準拠になる可能性がありますが、この状態は、徐々に生じ、意図的なものではありません。

構成管理データベース (CMDB)

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイすることも、組織全体にデプロイすることもできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 AWS Well-Architected フレームワークのセキュリティの柱のコンポーネントです。詳細については、「データ分類」を参照してください。

データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

非一元的で分散型のデータ所有権を持つとともに、一元的な管理およびガバナンスを行えるアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

データ境界

AWS 環境内の一連の予防ガードレール。信頼された ID のみが、期待されるネットワークから信頼されたリソースにアクセスできるようにします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには、一般的に、大量の履歴データが含まれており、多くの場合、それらはクエリや分析に使用されます。

データベース定義言語 (DDL)

データベース内のテーブルやオブジェクトの構造を作成または変更するためのステートメントまたはコマンド。

データベース操作言語 (DML)

データベース内の情報を変更 (挿入、更新、削除) するためのステートメントまたはコマンド。

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせます。ディープアンサンブルを使用して、より正確な予測を取得したり、予測の不確実性を推定したりできます。

深層学習

人工ニューラルネットワークの複数層を使用して、入力データと対象のターゲット変数の間のマッピングを識別する機械学習サブフィールド。

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を に採用するときは AWS、リソースの保護に役立つように、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加します。たとえば、多層防御アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、 AWS

Organizations ドキュメントの「AWS Organizationsで使用できるサービス」を参照してください。

トラブルシューティング

アプリケーション、新機能、コードの修正をターゲットの環境で利用できるようにするプロセス。デプロイでは、コードベースに変更を施した後、アプリケーションの環境でそのコードベースを構築して実行します。

開発環境

「環境」を参照してください。

検出管理

イベントが発生したときに、検出、ログ記録、警告を行うように設計されたセキュリティコントロール。これらのコントロールは副次的な防衛手段であり、実行中の予防的コントロールをすり抜けたセキュリティイベントをユーザーに警告します。詳細については、「 AWSでのセキュリティコントロールの実装」の「検出的コントロール」を参照してください。

開発バリューストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニュファクチャリング・プラクティスのために設計されたバリューストリームマッピング・プロセスを拡張したものです。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

ディメンションテーブル

スタースキーマにおいて、ファクトテーブルの定量データに関するデータ属性が含まれる小さいテーブル。ディメンションテーブルの属性は、通常、テキストフィールド、またはテキストのように扱える個別の数値で示されます。これらの属性は、一般的に、クエリの制約、フィルタリング、結果セットのラベル付けに使用されます。

ディザスタ

ワークロードまたはシステムが、導入されている主要な場所でのビジネス目標の達成を妨げるイベント。これらのイベントは、自然災害、技術的障害、または意図しない設定ミスやマルウェア攻撃などの人間の行動の結果である場合があります。

ディザスタリカバリ (DR)

ディザスタによるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software (ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み) で紹介されています (ボストン: Addison-Wesley Professional、2003)。strangler fig パターンでドメイン駆動型設計を使用する方法の詳細については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差を追跡します。たとえば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 を使用して AWS Control Tower 、ガバナンス要件への準拠に影響するランディングゾーンの変更を検出したりできます。

DVSM

「開発バリューストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。クラウドコンピューティングと比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を改善できます。

電子データ交換 (EDI)

組織間で行う、ビジネスドキュメントの自動交換。詳細については、「電子データ交換とは」を参照してください。

暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティング処理。

暗号化キー

暗号化アルゴリズムが生成した、ランダム化されたビットからなる暗号文字列。キーの長さは決まっておらず、各キーは予測できないように、一意になるように設計されています。

エンディアン

コンピュータメモリにバイトが格納される順序。ビッグエンディアンシステムでは、最上位バイトが最初に格納されます。リトルエンディアンシステムでは、最下位バイトが最初に格納されます。

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

エンタープライズの主要なビジネスプロセス (会計、MES、プロジェクト管理など) を自動化および管理するシステム。

エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、 AWS Key Management Service (AWS KMS) ドキュメントの「エンベロープ暗号化」を参照してください。

環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが使用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。例えば、 AWS CAF セキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。 AWS 移行戦略のエピックの詳細については、プログラム実装ガイドを参照してください。

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、統計の概要を計算し、データの可視化を作成することによって実行されます。

F

ファクトテーブル

スタースキーマの中央にあるテーブル。ビジネスオペレーションに関する定量的データが保存されます。一般的に、ファクトテーブルは、2 種類の列で構成されます。1 つは測定値が含まれる列、もう 1 つはディメンションテーブルへの外部キーが含まれる列です。

フェイルファスト

開発ライフサイクルを短縮するために、頻繁かつ段階的にテストを行う哲学であり、アジャイルアプローチでは、この考え方がきわめて重要です。

障害分離境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を高めるのに役立つアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界。詳細については、「AWS 障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

数ショットプロンプト

LLM に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例 (ショット) からモデルが学習する「インコンテキスト学

習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要なタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセス制御」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

変更データのキャプチャによる継続的なデータ複製を利用して、段階的なアプローチではなく、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

大規模な深層学習ニューラルネットワークであり、一般化およびラベル付けされていないデータからなる大規模データセットでトレーニングされています。FM により、言語理解、テキストおよび画像生成、自然言語での会話といった、一般的な各種タスクを実行できます。詳細については、「基盤モデルとは何ですか?」を参照してください。

G

生成 AI

AI モデルのサブセット。大量のデータでトレーニングされており、シンプルなテキストプロンプトを使用して、画像、動画、テキスト、オーディオなどの新しいコンテンツやアーティファクトを作成できます。詳細については、「生成 AI とは何ですか?」を参照してください。

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リスト

を使って指定します。詳細については、CloudFront ドキュメントの「コンテンツの地理的ディストリビューションの制限」を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローは古いと見なされている方法であり、トランクベースのワークフローは推奨されている新しい方法です。

ゴールデンイメージ

システムまたはソフトウェアのスナップショットであり、システムまたはソフトウェアの新規インスタンスをデプロイするテンプレートとして使用されます。製造の例で言えば、ゴールデンイメージを使用すると、複数のデバイスにソフトウェアをプロビジョニングして、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名ブラウンフィールド) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは AWS Config、、Amazon GuardDuty AWS Security Hub CSPM、、 AWS Trusted Advisor Amazon Inspector、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。AWS は、スキーマの変換に役立つ AWS SCTを提供します。

高可用性 (HA)

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

ヒストリアンのモダナイゼーション

製造業のニーズによりよく応えるために、オペレーションテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

ホールドアウトデータ

機械学習モデルのトレーニング用データセットから保留される、ラベル付き履歴データの一部。ホールドアウトデータを使用すると、モデル予測をホールドアウトデータと比較して、モデルのパフォーマンスを評価できます。

同種データベースの移行

お客様の出典データベースを、同じデータベースエンジンを共有するターゲットデータベース (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。同種間移行は、通常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性が高いため、通常の DevOps のリリースワークフローからは外れた形で実施されます。

ハイパーケア期間

カットオーバー直後、移行したアプリケーションを移行チームがクラウドで管理、監視して問題に対処する期間。通常、この期間は 1～4 日です。ハイパーケア期間が終了すると、アプリケーションに対する責任は一般的に移行チームからクラウドオペレーションチームに移ります。

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義する 1 つ以上の IAM プリンシパルにアタッチされたポリシー。

アイドル状態のアプリケーション

90 日間の平均的な CPU およびメモリ使用率が 5～20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

IIoT

「インダストリアル IoT」を参照してください。

イミュータブルインフラストラクチャ

既存インフラストラクチャの更新、パッチ適用、変更などを行わずに、本番環境ワークロードに使用する新規インフラストラクチャをデプロイするモデル。本質的に、イミュータブルインフラストラクチャは、ミュータブルインフラストラクチャよりも一貫性、信頼性、予測性に優れています。詳細については、 AWS Well-Architected フレームワークにある「イミュータブルインフラストラクチャを使用してデプロイする」のベストプラクティスを参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

インダストリー 4.0

2016 年に Klaus Schwab 氏が提唱した用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩による、ビジネスプロセスのモダナイズを意味します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

インダストリアル IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「インダストリアル IoT (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、VPC (同一または異なる 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する一元化された VPCs。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

IoT

インターネットまたはローカル通信ネットワークを介して他のデバイスやシステムと通信する、センサーまたはプロセッサが組み込まれた接続済み物理オブジェクトのネットワーク。詳細については、「IoT とは」を参照してください。

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

IoT

「IoT」を参照してください。

IT 情報ライブラリ (ITIL)

IT サービスを提供し、これらのサービスをビジネス要件に合わせるための一連のベストプラクティス。ITIL は ITSM の基盤を提供します。

IT サービス管理 (ITSM)

組織の IT サービスの設計、実装、管理、およびサポートに関連する活動。クラウドオペレーションと ITSM ツールの統合については、オペレーション統合ガイドを参照してください。

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

強制アクセス制御 (MAC) の実装で、ユーザーとデータ自体にそれぞれセキュリティラベル値が明示的に割り当てられます。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロードとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、「安全でスケーラブルなマルチアカウント AWS 環境のセットアップ」を参照してください。

大規模言語モデル (LLM)

大量のデータで事前トレーニングされた深層学習 AI モデル。LLM では、質問への回答、ドキュメントの要約、他言語へのテキスト翻訳、文を完成させるなど、さまざまなタスクを実行できます。詳細については、「大規模言語モデル (LLM) とは何ですか?」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースアクセス制御」を参照してください。

最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、IAM ドキュメントの「最小特権アクセス許可を適用する」を参照してください。

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「機械学習」を参照してください。

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティやプライバシーを侵害するように設計されたソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスを招く可能性があります。マルウェアの例には、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

AWS のサービス はインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、エンドポイントにアクセスしてデータを保存および取得します。マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、抽象化されたサービスとも呼ばれます。

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するソフトウェアシステムであり、工場では、これによって、原材料から製品を完成させます。

MAP

「Migration Acceleration Program」を参照してください。

メカニズム

ツールを作成してその導入を推進し、導入結果を調べて調整を行うための包括的なプロセス。メカニズムとは、運用中にそれ自体を強化し改善するサイクルを意味します。詳細については、AWS 「 Well-Architected フレームワーク」の「メカニズムの構築」を参照してください。

メンバーアカウント

組織の一部である管理アカウント AWS アカウント 以外のすべて AWS Organizations。 アカウントが 組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

発行/サブスクライブのパターンに基づく、軽量のマシンツーマシン (M2M) 通信プロトコルであり、リソースに限りのある IoT デバイスに使用されます。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス

機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、AWS「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量 API を使用して、明確に定義されたインターフェイスを介して通信します。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、「 でのマイクロサービスの実装 AWS」を参照してください。

Migration Acceleration Program (MAP)

組織がクラウドに移行するための強力な運用基盤を構築し、移行の初期コストを相殺するのに役立つコンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。MAP には、組織的な方法でレガシー移行を実行するための移行方法論と、一般的な移行シナリオを自動化および高速化する一連のツールが含まれています。

大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、AWS 移行戦略 の第 3 段階です。

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、運用、ビジネスアナリストおよび所有者、移行エンジニア、デベロッパー、およびスプリントで作業する DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20～50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの移行ファクトリーに関する解説とCloud Migration Factory ガイドを参照してください。

移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例としては、ターゲットサブネット、セキュリティグループ、 AWS アカウントなどがあります。

移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: AWS Application Migration Service を使用して Amazon EC2 への移行をリホストします。

Migration Portfolio Assessment (MPA)

オンラインツール。これによって、 AWS クラウドに移行するビジネスケースの検証に必要な情報を得られます。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、およびウェーブプランニング) を提供します。MPA ツール (ログインが必要) は、すべての AWS コンサルタントと APN パートナーコンサルタントが無料で利用できます。

移行準備状況評価 (MRA)

AWS CAF を使用して、組織のクラウド準備状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、移行準備状況ガイドを参照してください。MRA は、AWS 移行戦略の第一段階です。

移行戦略

ワークロードを AWS クラウドに移行するために使用するアプローチ。詳細については、この用語集の 7 Rs エントリと、「組織を動員して大規模な移行を加速する」を参照してください。

ML

「機械学習」を参照してください。

モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、「AWS クラウドでのアプリケーションのモダナイズ戦略」を参照してください。

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定されたギャップに対処するためのアクションプランが得られます。詳細については、「AWS クラウドでのアプリケーションのモダナイゼーションの準備状況を評価する」を参照してください。

モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1 つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、「モノリスをマイクロサービスに分解する」を参照してください。

MPA

「Migration Portfolio Assessment」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」 または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

ミュータブルなインフラストラクチャ

本番ワークロードに使用する既存のインフラストラクチャを更新および変更するためのモデル。Well-Architected AWS フレームワークでは、一貫性、信頼性、予測可能性を向上させるために、イミュータブルインフラストラクチャの使用をベストプラクティスとして推奨しています。

O

OAC

「オリジンアクセス制御」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

移行プロセス中にソースワークロードを停止させる移行方法。この方法はダウンタイムが長くなるため、通常は重要ではない小規模なワークロードに使用されます。

OI

「オペレーション統合」を参照してください。

Ola

「オペレーショナルレベルアグリーメント」を参照してください。

オンライン移行

ソースワークロードをオフラインにせずにターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

Open Process Communications - Unified Architecture (OPC-UA)

産業オートメーション用のマシンツーマシン (M2M) 通信プロトコル。OPC-UA により、相互運用の際に、データ暗号化、認証、認可の各スキームを標準化できます。

オペレーショナルレベルアグリーメント (OLA)

サービスレベルアグリーメント (SLA) をサポートするために、どの機能的 IT グループが互いに提供することを約束するかを明確にする契約。

運用準備状況レビュー (ORR)

質問と関連するベストプラクティスのチェックリスト。インシデントや起こり得る障害を理解、評価、防止したり、その範囲を縮小したりする際に役立ちます。詳細については、 AWS Well-Architected フレームワークの「Operational Readiness Reviews (ORR)」を参照してください。

運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携させるハードウェアおよびソフトウェアシステム。製造分野では、Industry 4.0 への変革を進める上で、OT と情報技術 (IT) システムの統合に焦点が当てられています。

オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、オペレーション統合ガイドを参照してください。

組織の証跡

組織 AWS アカウント 内のすべての のすべてのイベント AWS CloudTrail を ログに記録する によって作成された証跡 AWS Organizations。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、CloudTrail ドキュメントの「組織の証跡の作成」を参照してください。

組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードにより、このフレームワークは人材アクセラレーションと呼ばれます。詳細については、OCM ガイドを参照してください。

オリジンアクセス制御 (OAC)

Amazon Simple Storage Service (Amazon S3) コンテンツを保護するための、CloudFront のアクセス制限の強化オプション。OAC は AWS リージョン、すべての S3 バケット、 AWS KMS (SSE-KMS) によるサーバー側の暗号化、S3 バケットへの動的 PUT および DELETEリクエストをサポートします。

オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介してのみアクセスできます。OAC も併せて参照してください。OAC では、より詳細な、強化されたアクセス制御が可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されたネットワーク接続を処理する VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリンシパルにアタッチされる IAM 管理ポリシー。詳細については、IAM ドキュメントのアクセス許可の境界を参照してください。

個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。PII の例には、氏名、住所、連絡先情報などがあります。

PII

「個人を特定できる情報」を参照してください。

プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

PLC

「プログラマブルロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

次の操作を可能にするオブジェクト: アクセス許可を定義する (ID ベースのポリシーを参照)。アクセス条件を指定する (リソースベースのポリシーを参照)。 AWS Organizations の組織における全アカウントにアクセス許可の上限を定義する (サービスコントロールポリシーを参照)。

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。

ポートフォリオ評価

移行を計画するために、アプリケーションポートフォリオの検出、分析、優先順位付けを行うプロセス。詳細については、「移行の準備状況の評価」を参照してください。

述語

`true` または `false` を返すためのクエリ条件。一般的に、`WHERE` 句に記述されます。

述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、クエリのパフォーマンスが向上します。

予防的コントロール

イベントの発生を防ぐように設計されたセキュリティコントロール。このコントロールは、ネットワークへの不正アクセスや好ましくない変更を防ぐ最前線の防御です。詳細については、「AWSでのセキュリティコントロールの実装」の「予防的コントロール」を参照してください。

プリンシパル

アクションを実行し AWS 、リソースにアクセスできる のエンティティ。このエンティティは通常、、IAM AWS アカウントロール、または ユーザーのルートユーザーです。詳細については、IAM ドキュメントの「ロールに関する用語と概念」にあるプリンシパルを参照してください。

プライバシーバイデザイン

開発プロセス全体を通してプライバシーが考慮されているシステムエンジニアリングのアプローチ。

プライベートホストゾーン

1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 がどのように応答するかに関する情報を保持するコンテナ。詳細については、Route 53 ドキュメントの「プライベートホストゾーンの使用」を参照してください。

プロアクティブコントロール

非準拠リソースのデプロイ防止を目的としたセキュリティコントロール。このコントロールにより、プロビジョニング前にリソースをスキャンします。コントロールに準拠していないリソースは、プロビジョニングされません。詳細については、 AWS Control Tower ドキュメントの「コントロールリファレンスガイド」および「 セキュリティコントロールの実装」の「プロアクティブコントロール」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

製品の設計、開発、発売から、成長、成熟、衰退、廃棄に至る、製品のライフサイクル全体を通してデータとプロセスを管理すること。

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

製造分野で使用される、信頼性と適応性に優れたコンピュータであり、これによって、マシンをモニタリングするとともに、製造プロセスを自動化します。

プロンプトチェイニング

1 つの LLM プロンプトによる出力を次のプロンプトの入力に使用して、より良いレスポンスを生成します。この手法を使用すると、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改良または拡張したりできます。これによって、モデルのレスポンスの精度と関連性が向上し、粒度の高いパーソナライズされた結果を得られます。

仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

発行/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。これにより、スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの MES の場合、マイクロサービスは、他のマイクロサービスがサブスクライブ可能なチャネルにイベントメッセージを発行できます。このシステムでは、発行サービスの変更なしに、新規マイクロサービスを追加できます。

Q

クエリプラン

手順などの一連のステップであり、SQL リレーショナルデータベースシステムのデータにアクセスするために使用されます。

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RAG

「検索拡張生成」を参照してください。

ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

RASCI マトリックス

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RCAC

「行と列のアクセス制御」を参照してください。

リードレプリカ

読み取り専用に使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の から分離され、独立しています。詳細については、「アカウントが使用できる AWS リージョン を指定する」を参照してください。

リグレッション

数値を予測する機械学習手法。例えば、「この家はどれくらいの値段で売れるでしょうか?」という問題を解決するために、機械学習モデルは、線形回帰モデルを使用して、この家に関する既知の事実 (平方フィートなど) に基づいて家の販売価格を予測できます。

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

リプラットフォーム

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または中断から回復するアプリケーションの機能。 AWS クラウドでの回復力を計画する際には、一般的に、高可用性とディザスタリカバリが考慮されます。詳細については、「AWS クラウド の耐障害性」を参照してください。

リソースベースのポリシー

Amazon S3 バケット、エンドポイント、暗号化キーなどのリソースにアタッチされたポリシー。このタイプのポリシーは、アクセスが許可されているプリンシパル、サポートされているアクション、その他の満たすべき条件を指定します。

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R) 、説明責任 (A) 、協議 (C) 、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートが含まれる場合は RASCI マトリックスと呼ばれ、含まれない場合は RACI マトリックスと呼ばれます。

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、「 AWSでのセキュリティコントロールの実装」の「レスポンシブコントロール」を参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

検索拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」を参照してください。

ローテーション

定期的にシークレット情報を更新して、攻撃者が認証情報にアクセスするのをより困難にするプロセス。

行と列のアクセス制御 (RCAC)

アクセスルールが定義された、基本的で柔軟な SQL 表現の使用。RCAC は行権限と列マスクで構成されています。

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

特定のタスクを実行するために必要な手動または自動化された一連の手順。これらは通常、エラー率の高い反復操作や手順を合理化するために構築されています。

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能を使用すると、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、 AWS マネジメントコンソール にログインしたり AWS 、API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントの「SAML 2.0 ベースのフェデレーションについて」を参照してください。

SCADA

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存するパスワードやユーザー認証情報などの AWS Secrets Manager機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値には、バイナリ、1 つの文字列、複数の文字列を指定できます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの概要」を参照してください。

セキュリティバイデザイン

開発プロセス全体を通してセキュリティが考慮されているシステムエンジニアリングのアプローチ。

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、主に 4 つの種類があります。4 つとは、予防、検出、レスポンシブ、プロアクティブです。

セキュリティ強化

アタックサーフェスを狭めて攻撃への耐性を高めるプロセス。このプロセスには、不要になったリソースの削除、最小特権を付与するセキュリティのベストプラクティスの実装、設定ファイル内の不要な機能の無効化、といったアクションが含まれています。

Security Information and Event Management (SIEM) システム

セキュリティ情報管理 (SIM) とセキュリティイベント管理 (SEM) のシステムを組み合わせたツールとサービス。SIEM システムは、サーバー、ネットワーク、デバイス、その他ソースからデータを収集、モニタリング、分析して、脅威やセキュリティ違反を検出し、アラートを発信します。

セキュリティレスポンスの自動化

セキュリティイベントへの自動レスポンスまたは自動修復を目的として、事前定義およびプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先にあるデータの、それ AWS のサービス を受け取る による暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。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」を参照してください。

サービスエンドポイント

のエントリポイントの URL AWS のサービス。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、「AWS 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

サービスレベルインジケータによって測定され、サービスの状態を表すターゲットメトリクス。

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、お客様はクラウドのセキュリティを担当します。詳細については、「責任共有モデル」を参照してください。

SIEM

「Security Information and Event Management システム」を参照してください。

単一障害点 (SPOF)

特定のアプリケーションを構成する単一の重要なコンポーネントで発生し、システム稼働に支障をきたす可能性のある障害。

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、「AWS クラウドでのアプリケーションをモダナイズするための段階的アプローチ」を参照してください。

SPOF

「単一障害点」を参照してください。

スタースキーマ

データベースの編成構造を意味し、1 つの大きいファクトテーブルにトランザクションデータまたは測定データが保存され、1 つ以上の小さいディメンションテーブルにデータ属性が保存されます。この構造は、データウェアハウスやビジネスインテリジェンスを用途とするように設計されています。

strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として Martin Fowler により提唱されました。このパターンの適用方法の例については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

サブネット

VPC 内の IP アドレスの範囲。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

監視制御とデータ取得 (SCADA)

製造分野において、ハードウェアとソフトウェアを使用して物理アセットと本番運用をモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーとのやり取りをシミュレートして、起こり得る問題を検出したり、パフォーマンスをモニタリングしたりすることで、システムをテストします。Amazon CloudWatch Synthetics を使用すると、こうしたテストを作成できます。

システムプロンプト

コンテキスト、指示、ガイドラインなどを提示して、LLM に動作を指示する手法。システムプロンプトは、コンテキストを設定して、ユーザーとやり取りするルールを確立するのに有用です。

T

タグ

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。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。詳細については、「AWS リソースのタグ付け」を参照してください。

ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要のある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパターンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。詳細については、 AWS Transit Gateway ドキュメントの「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「 を他の AWS のサービス AWS Organizations で使用する AWS Organizations 」を参照してください。

チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

ツーピザチーム

2 枚のピザを分け合えることができるくらい小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。

未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

上位環境

「環境」を参照してください。

V

バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングできる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「VPC ピア機能とは」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

ウィンドウ関数

現在のレコードに何らかの形で関連している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといったタスクの処理に役立ちます。

ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

データを 1 回のみ書き込むことで、データの削除や変更を防ぐストレージモデル。承認済みユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャは、イミュータブルと見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

ゼロショットプロンプト

LLM にタスク実行の手順は提示するが、実行のガイドとして役立つ例 (ショット) は提示しない方法。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「数ショットプロンプト」も参照してください。

ゾンビアプリケーション

平均 CPU およびメモリ使用率が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

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。