AWS Well-Architected フレームワーク

金融サービス業界レンズ

金融サービス業界レンズ: AWS Well-Architected フレームワーク

Table of Contents

金融サービス業界レンズ - AWS Well-Architected フレームワーク

公開日:: 2020 年 6 月 (改訂履歴)

要約

このドキュメントでは、AWS Well-Architected フレームワークの金融サービス業界レンズについて説明します。このドキュメントでは、一般的な設計原則と、Well-Architected フレームワークの 5 つの柱に関する特定のベストプラクティスとガイダンスについて説明しています。

はじめに

金融サービス業界には、世界中の国々に不可欠なサービスを提供する金融サービス会社、独立系ソフトウェアベンダー (ISV)、市場ユーティリティ、およびインフラストラクチャが含まれます。このシステムは、商品、サービス、および金融資産の支払いのための主要なメカニズムを提供し、貯蓄者と借受人を仲介し (貯蓄が投資に回るようにし)、リスクに備え、分散させます。

AWS Well-Architected フレームワークの目的は、AWS でシステムを構築する際の選択肢の#所と短所をお客様が理解できるように支援することです。フレームワークを使用することによって、信頼性が高く、セキュアかつ効率的で、コスト効率に優れたシステムをクラウド内で設計し、運用するためのアーキテクチャ上のベストプラクティスを学びます。このフレームワークは、アーキテクチャをベストプラクティスに照らし合わせて一貫的に測定し、改善すべき領域を特定する手段を提供します。システムを適切に設計することによって、安全性、信頼性、そしてビジネスの成功の可能性が大いに高まると当社は確信しています。

この「レンズ」では、監督当局により課される規制およびコンプライアンスの要件を遵守するためのものを含め、定義したリスクと制御の目標に沿って、回復力、セキュリティ、および運用パフォーマンスを促進する金融サービス業界 (FSI) のワークロードを設計、デプロイ、設計する方法に焦点を当てます。

すべてのお客様は、AWS Well-Architected フレームワークのホワイトペーパーで概説されているベストプラクティスと質問から始める必要があります。本ドキュメントでは、金融サービス機関向けの追加のベストプラクティスを提供します。

金融サービス業界レンズは、当社が世界中の金融機関と協力した経験に基づいて、金融機関の要件に対応することを目的とした、セキュリティ、データプライバシー、および回復力のベストプラクティスを提示するものです。テクノロジーチームが自信を持って AWS を使用してアプリケーションを構築およびデプロイするために実装できるように、ガードレールに関するガイダンスを提供します。このレンズは、AWS 環境に透明性と監査可能性を組み込むためのガイダンスを提供します。これは、環境への新しいサービスの採用を促進するのに役立つ統制に関する提案を提供します。

本ドキュメントは、最高技術責任者 (CTO)、設計者、デベロッパー、エンジニア、運用チームメンバーなどの技術担当者向けであるとともに、リスク、コンプライアンス、および監査部門に所属する個人向けでもあります。

一般的な設計の原則

Well-Architected フレームワークは、クラウドにおける金融サービスワークロードの適切な設計を可能にする 4 つの一般的な設計の原則を提供します。

1. 文書化された運用計画—クラウド運用モデルを定義するには、内部の消費者や利害関係者と協力して、共通の目標と戦略的方向性を設定する必要があります。多くの組織は、リスク管理の有効性を向上させるために「3 つのディフェンスライン」モデルを採用しています。
   - 第 1 のディフェンスラインでは、運用管理者が日常的にリスクおよび管理手順を実行する責任を負います。
   - 第 2 のディフェンスラインでは、さまざまなリスク管理およびコンプライアンス機能を確立して、第 1 のディフェンスラインの統制の構築および/またはモニタリングをサポートします。
   - 第 3 のディフェンスラインとして、内部監査人は、組織における最高レベルの独立性および客観性に基づいて、統治機関と上級経営陣に包括的な保証を提供します。

   規制対象となるクラウド採用のための効果的な運用モデルを開発するには、3 つのディフェンスラインにわたって明確な役割と責任を確立することが不可欠です。
2. 自動化されたインフラストラクチャとアプリケーションのデプロイ—自動化により、クラウド環境全体でセキュリティ、コンプライアンス、およびガバナンスのアクティビティを迅速に実行および革新し、スケールできます。自動化されたインフラストラクチャとアプリケーションのデプロイに投資する金融サービス機関は、デプロイ速度を加速し、セキュリティとガバナンスのベストプラクティスをより簡単にソフトウェア開発ライフサイクルに組み込むことができます。
3. セキュリティバイデザイン—金融サービス機関は、セキュリティの観点から事前にテストされたアーキテクチャを実装するために、セキュリティバイデザイン (SbD) アプローチを検討する必要があります。SbD は、AWS で実行されているアプリケーションの制御目標、セキュリティベースライン、セキュリティ設定、および監査機能の実装に役立ちます。標準化され、自動化され、規範的で反復可能な設計テンプレートは、一般的なユースケースのデプロイを加速するだけでなく、複数のワークロードにわたるセキュリティ標準を満たす (および監査のエビデンスに関する要件を満たしやすくする) のに役立ちます。例えば、顧客データを保護し、許可されていない第三者によるデータ開示や秘密情報の改ざんのリスクを軽減するために、金融機関は暗号化を採用し、暗号化キーへのアクセスを慎重に管理する必要があります。SbD を使用することにより、保存中、転送中、および必要に応じて、デフォルトでアプリケーションレベルでデータの暗号化を有効化できます。
4. 自動化されたガバナンス—人間がランブックやチェックリストを操作すると、遅延や誤った結果が生じることがよくあります。自動化されたガバナンスは、大規模なアプリケーションのデプロ

イのための迅速で確実なガバナンスチェックを提供します。大規模なガバナンスは通常、次の事項をカバーします。

- アカウント管理—何百ものユーザーとビジネスユニットがクラウドベースのリソースをリクエストしている場合、アカウントプロビジョニングを自動化し、優れたセキュリティを維持します。
- 予算とコストの管理—多くのアカウント、ワークロード、およびユーザーをまたいで予算を適用およびモニタリングします。
- セキュリティとコンプライアンスの自動化—セキュリティ、リスク、およびコンプライアンスを大規模に管理して、組織がビジネス目標に向かって事業を推進しながらコンプライアンスを維持できるようにします。

シナリオ

以下では、AWS での金融サービスワークロードの設計とアーキテクチャに影響する一般的なシナリオをご紹介します。各シナリオには、設計に対する一般的な推進要因と、リファレンスアーキテクチャが含まれています。

トピック

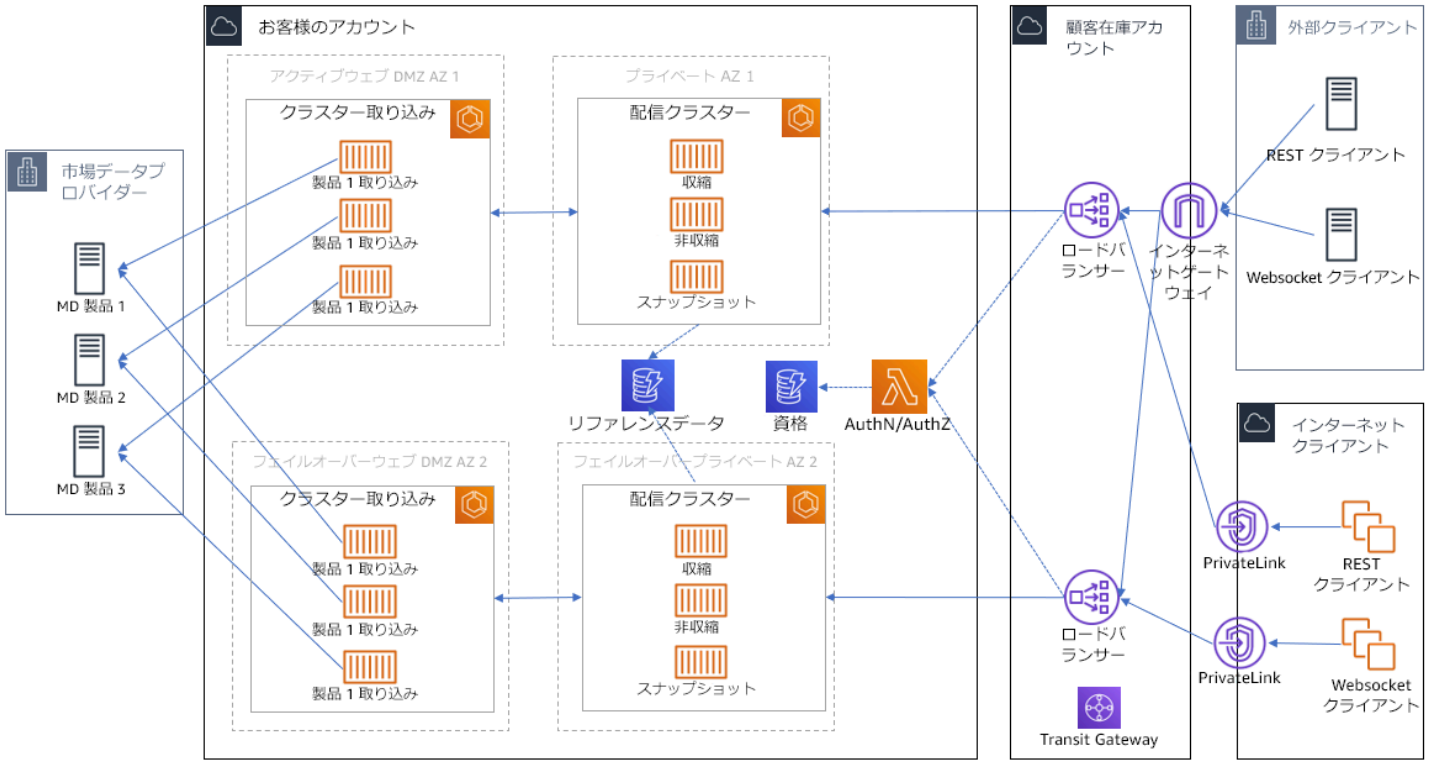
金融データ

クラウドで実行されているワークロードの財務データへアクセスすることは、金融サービス機関の運用にとって不可欠な要素です。こうしたデータセットの例としては、リアルタイムおよび過去の市場データ、消費者動向などの代替データ、洞察のために分析できる購入判断などがあります。

こうしたユースケースをサポートする財務データのアーキテクチャは、以下のような特徴を共有しています。

- ユーザーの資格やデータの再配布に関して厳しい要件があります。
- 市場データの使用方法 (たとえば、取引に関する判断と取引後の分析) に応じて変化する低レイテンシー要件があり、秒単位からサブミリ秒単位まで変化する可能性があります。
- 市場データプロバイダーおよび取引所との間で信頼できるネットワーク接続を使用しています。

リファレンスアーキテクチャ



ゥ 1: 企業内の市場データ配信プラットフォームのリファレンスアーキテクチャ

規制レポート

すべての金融機関は、規制レポートのために大量の情報を扱っており、欧州連合 (EU) の金融商品指令 II (MiFID II) や米国証券取引委員会 (SEC) の規則 613 (統合監査証跡) などの新しい規制には規制レポート要件が含まれています。静的なレガシーインフラストラクチャや非効率的なレポートプロセスは、レポートのコストを上昇させ、顧客が規制の変更に迅速に対応できなくなる可能性があります。AWS にレポートデータレイクを構築し、豊富なサービスセットを活用すれば、規制レポートを複雑化させる多くの課題 (切断されたサイロや分散 ETL プロセスに存在するデータなど) に対処できます。お客様がレポートデータを一貫性のあるデータセットに統合すると、そのデータを使用した高度な分析や機械学習を通じて追加の洞察を得ることができます。

こうしたユースケースをサポートする財務サービスデータレイクのアーキテクチャは、以下のような特徴を共有しています。

- データの品質、整合性、系統を取り込みパイプラインと処理パイプラインに実装します。
- データは保存時と転送中の両方で暗号化する必要があります。
- 規制要件 (EU 一般データ保護規則など) に適合するために、個人を特定できる情報 (PII) をマスクまたはトークン化します。

- きめ細かいアクセス制御と資格を備えたデータカタログを使用しています。

リファレンスアーキテクチャ

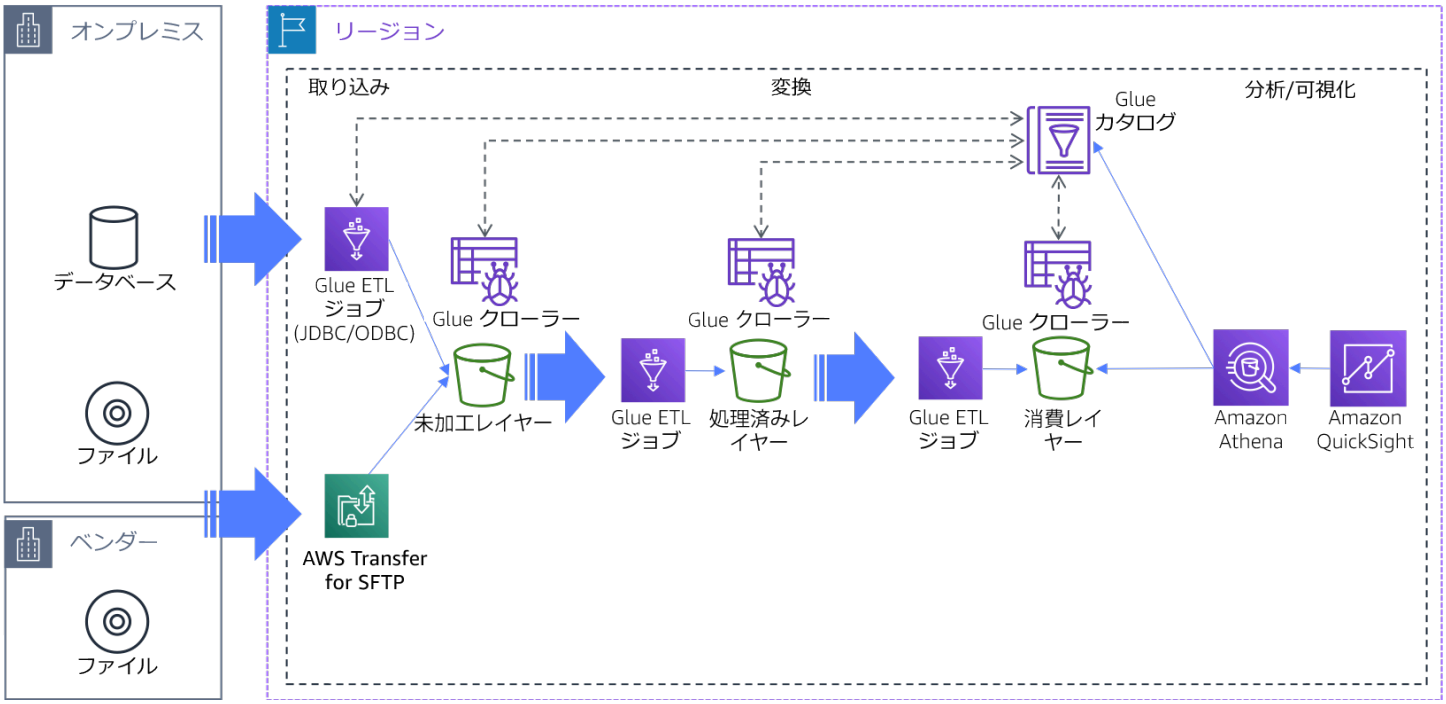


図 2: 金融サービス業界のデータレイクのリファレンスアーキテクチャ

人工知能と機械学習

金融機関は長年にわたり、人工知能と機械学習 (AI/ML) テクノロジーを試してきましたが、社内のデータサイエンスの専門知識が不足しており、大規模なデータセットの操作経験が不十分なため、こうしたテクノロジーの日常業務への統合は速やかには進んでいません。AWS は、あらゆる組織が AI/ML に簡単にアクセスできるようにする一連のツールを提供しています。金融機関は、こうしたツールを使用して、チャットボットを介した顧客とのやり取りを強化し、監視を改善し、非構造化データから取引のアイデアを収集し、提供する製品をカスタマイズしています。

こうしたユースケースをサポートする金融サービス AI/ML のアーキテクチャは、以下のような特徴を共有しています。

- コードやモデルアーティファクトを保護するための安全なアーキテクチャとなっています。
- 事前定義されたセキュリティ構成を備えたモデル開発およびトレーニング環境向けのセルフサービス機能があります。

- モデルのデプロイには、変更管理システムと統合された CI/CD パイプラインを使用しています。
- 開発、トレーニング、デプロイにわたるモデル開発ライフサイクル全体のエンドツーエンドのエビデンスの取得を自動化しています。

リファレンスアーキテクチャ

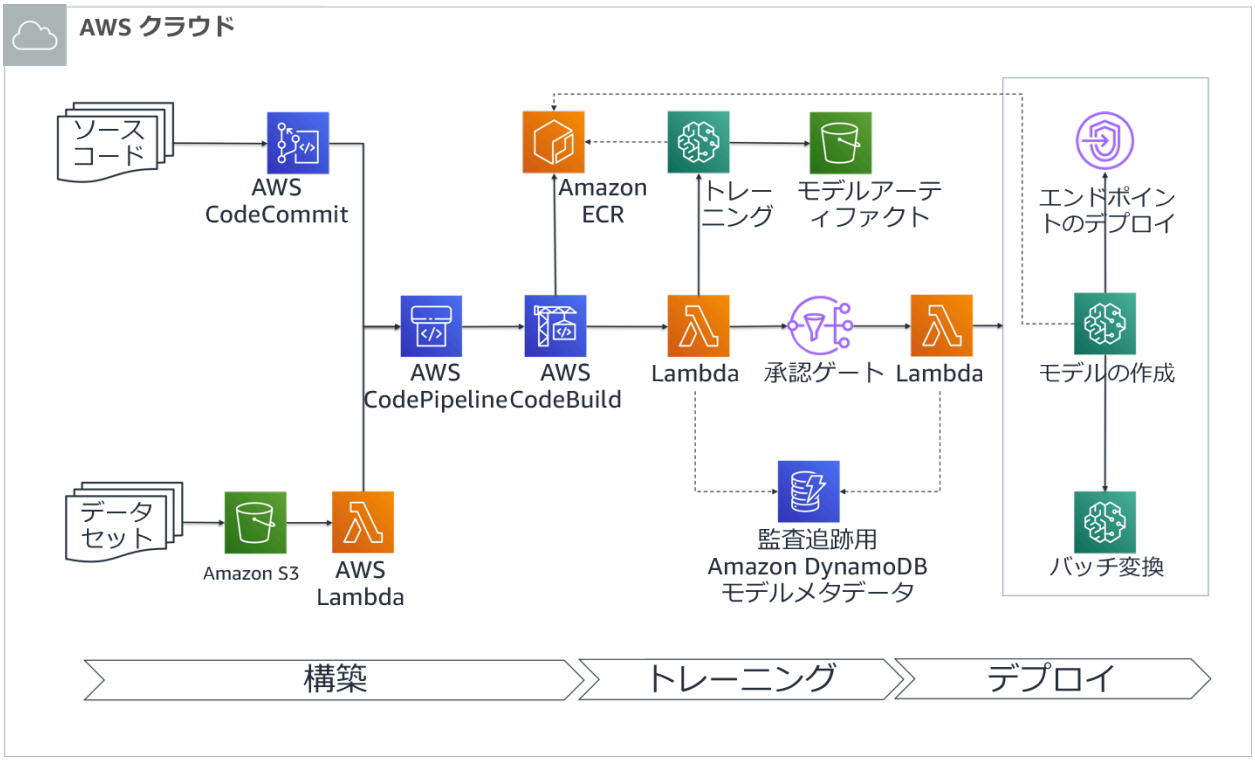


図 3: AI/ML パイプラインのリファレンスアーキテクチャ

グリッドコンピューティング

金融シミュレーションは、リスクを理解して管理し、資本ポジションを完全に把握し、what-if テストを実施し、情報に基づいた投資と価格決定を行うために、あらゆる種類の金融機関の運用に不可欠です。こうしたシミュレーションを実行するために、金融機関はコンピューティングリソースのクラスター (グリッド) を活用しています。ただし、さまざまな種類の関連データの急増、より高いレベルのストレステストの実行を求める規制要件、新しい定量的取引戦略とより複雑な製品のバックテストの複雑さなど、さまざまな要因によって計算がより困難になる可能性があります。グリッドコンピューティングのニーズに対応するために、金融機関は AWS を使用して、処理を高速化し、総コストを削減し、アクセシビリティを向上させています。

こうしたユースケースをサポートする金融サービスのハイパフォーマンスコンピューティング (HPC) アーキテクチャは、以下のような特徴を共有しています。

- さまざまなコンピューティングタイプ (CPU、GPU、FPGA) を混在させ、組み合わせることができます。
- スポットインスタンスを活用して、グリッドコストを大幅に削減しています。
- Amazon Simple Storage Service (S3)、Amazon Elastic File System (EFS) または Amazon FSx を永続的ストレージに活用します。

リファレンスアーキテクチャ

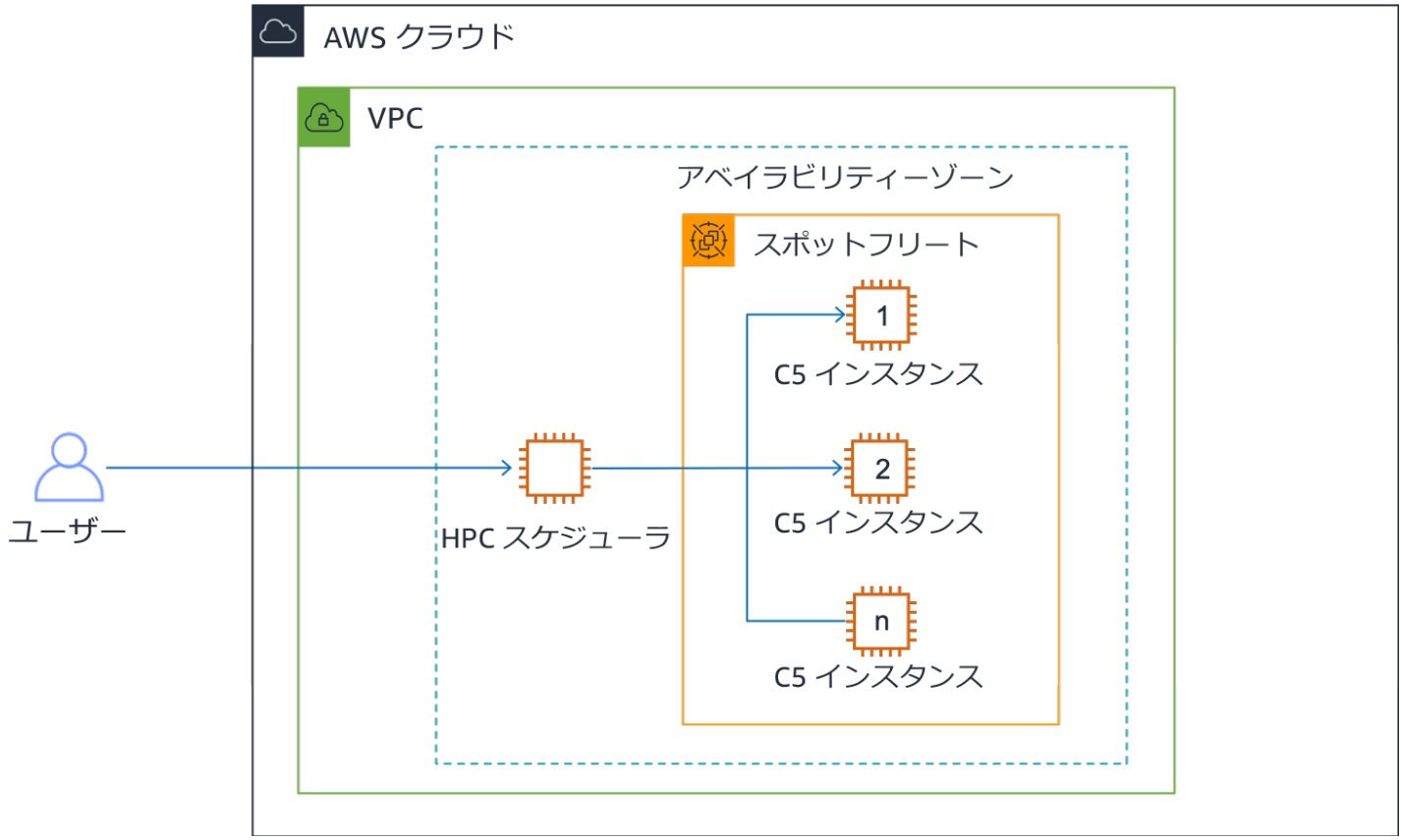


図 4: スポットインスタンスを使用した HPC グリッドのリファレンスアーキテクチャ

オープンバンキング

オープンバンキングでは、銀行はアプリケーションプログラミングインターフェイス (API) を使用して、顧客データをサードパーティのデベロッパーやサービスプロバイダーと安全に共有し、勘定系プラットフォームの機能への自動化された安全なアクセスを可能にします。銀行は、新しい規制や顧客の要求に応えて、オープンバンキングプラットフォームを構築しています。オープン API を構築している銀行は、スケーラビリティ、費用対効果、および大量の新しいデータの分析用に AWS が提供するサービスが優れているため AWS を選択します。

こうしたユースケースをサポートするオープンバンキングアーキテクチャは、以下のような特徴を共有しています。

- OAuth 2.0 認証標準を使用しています。
- API 主導のインフラストラクチャと伸縮自在でスケーラブルな環境を備えています。
- 顧客アカウントデータへの即時またはほぼ即時のアクセスを提供しています。
- 改ざん防止の口ギングおよび監査機能を備えています。

リファレンスアーキテクチャ

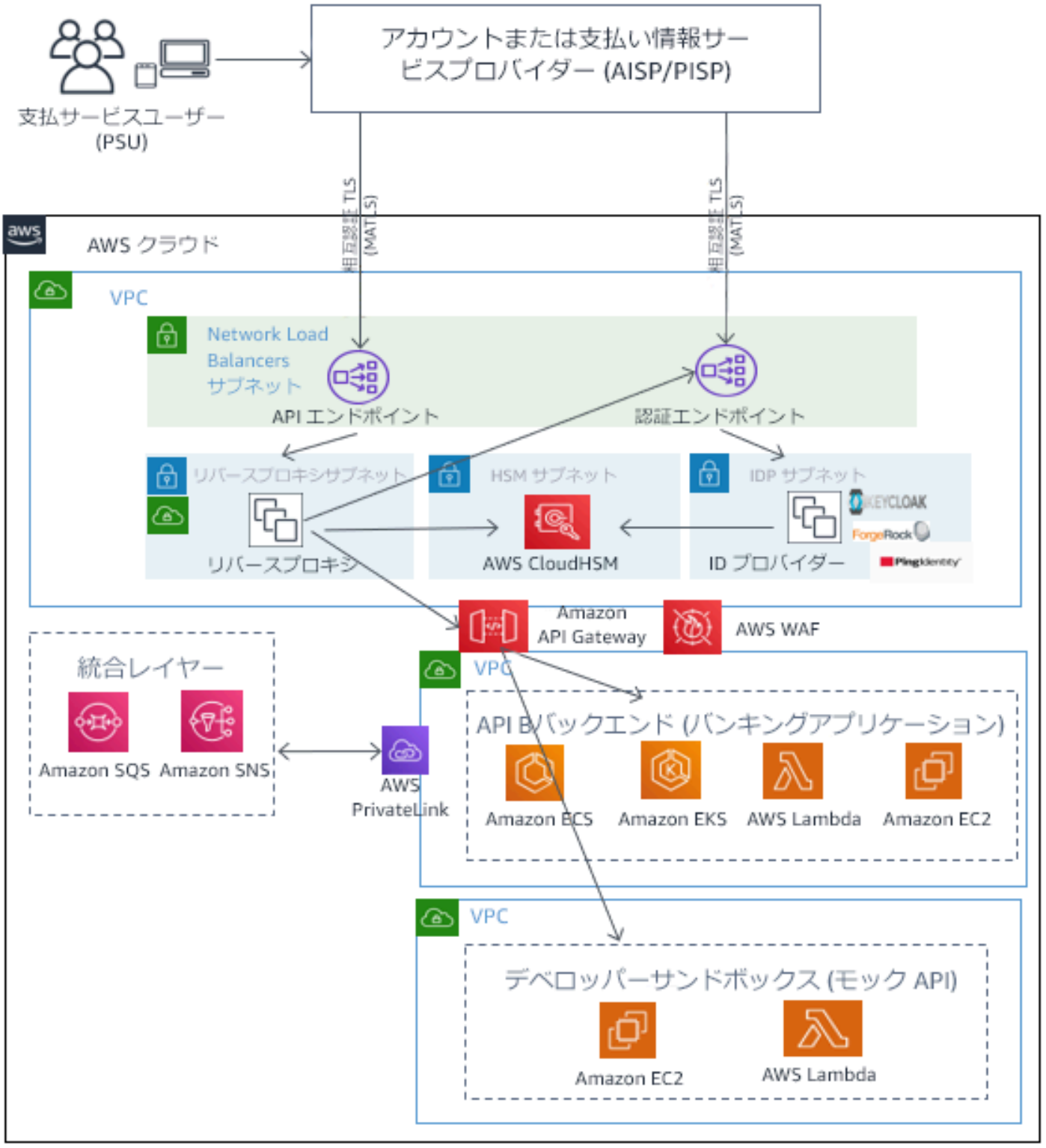


図 5: オープンバンキングのリファレンスアーキテクチャ

ユーザーエンゲージメント

金融機関は、モバイルアプリケーション、ウェブポータル、コールセンターエージェントとチャットボット、アドバイザー/ブローカーなど、独自の顧客対応チャネルにますます投資しており、すべてが全体的な顧客体験を向上させています。

こうしたユースケースをサポートする金融サービスユーザーエンゲージメントのアーキテクチャは、以下のような特徴を共有しています。

- 公的および私的ソースから大量のリアルタイムデータを取り込んで使用します。
- データ分類に基づいて、さまざまなデータ保護の考慮事項が必要です。
- イベント駆動型アーキテクチャを採用して、オンデマンドのスケーラビリティと従量課金モデルを活用しています。
- リアルタイムおよびアーカイブのデータフローを含んでいます。

リファレンスアーキテクチャ

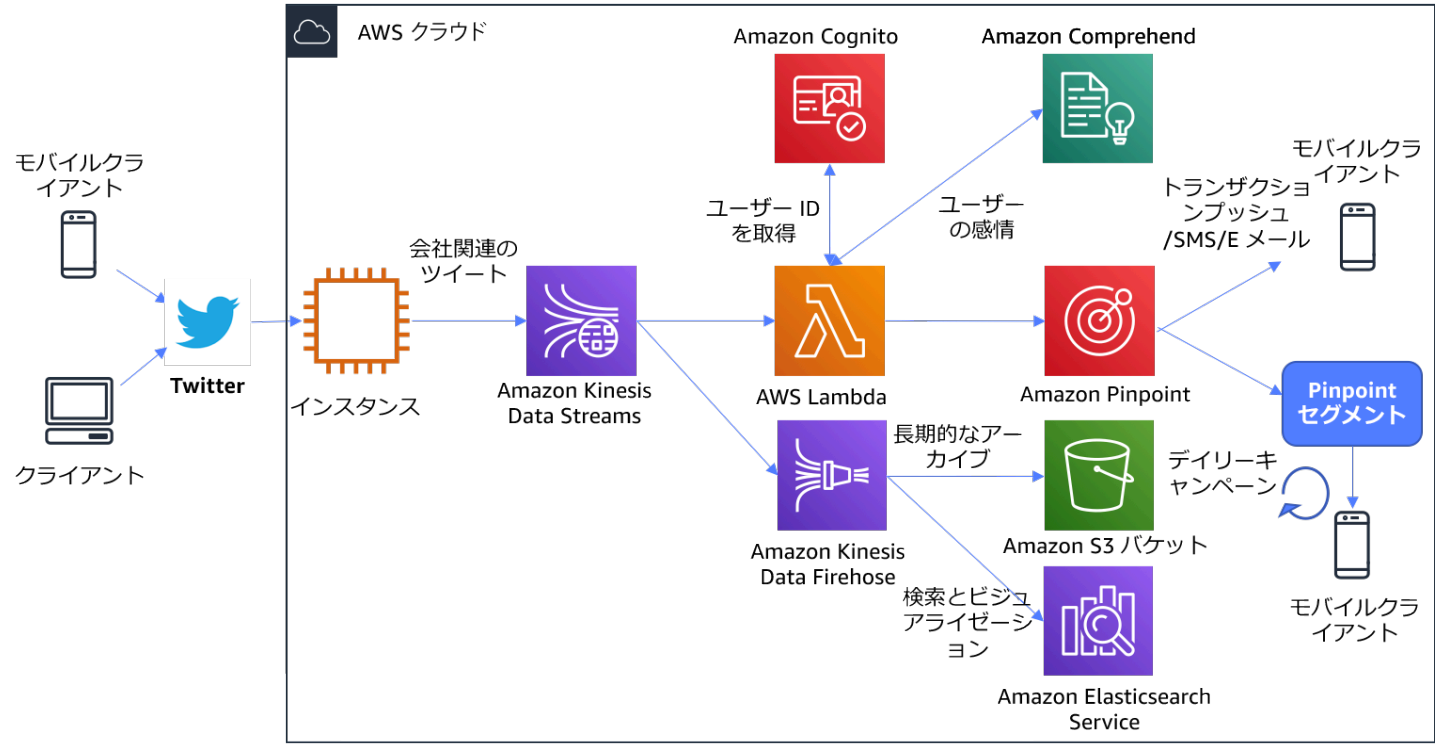


図 6: 社会的心理に基づくリアルタイムユーザーエンゲージメントのリファレンスアーキテクチャ

Well-Architected フレームワークの柱

トピック

運用上の優秀性の柱

運用上の優秀性の柱には、ビジネス価値を提供し、サポートプロセスと手順を継続的に改善していくために、システムを実行してモニタリングする能力が含まれています。

金融機関は、人、プロセス、および運用モデルに関連する予防策や機能など、運用上の優秀性に焦点を当てる必要があります。この領域に焦点を当てることで、金融機関は問題が発生した場合に迅速に対応して回復することができます。

トピック

- イベント後の運用レビューを実施

リスク部門全体における役割と責任の定義

FSIOPS1: クラウドのリスクとコンプライアンスの役割を定義しましたか?

上記の「一般的な設計の原則」のセクションで説明したように、金融機関は通常、リスク管理の有効性を向上させるために 3 つのディフェンスラインモデルを採用しています。2 つ目と 3 つ目のディフェンスラインには、クラウドを使用したビジネスサービス (1 つ目のディフェンスラインが所有および管理するサービス) の提供に伴うリスクを理解するために必要な適切なスキルとトレーニングが必要です。クラウド運用モデルの有効性と監査可能性を確保するには、3 つの各ディフェンスライン内およびディフェンスライン全体の両方で明確な役割と責任を確立する必要があります。これらの役割と責任は、ガバナンスモデルが引き続き効率的かつ効果的であることを保証するために、定期的に再評価する必要があります。

リスク管理および内部監査部門と連携して、クラウドリスク管理の承認プロセスを実装する

クラウドへの移行など、テクノロジーの大幅な変更には、潜在的なリスクの新たな評価と、統制環境が特定されたリスクを軽減できるだけでなく、その有効性を証明できることの検証が必要です。リスクおよび内部監査部門との連携は、クラウドの使用量が増加したときに、要求されるガバナンスに関する義務が確実に遵守されるようにするのに役立ちます。この連携には、クラウド環境を保護および運用するために実装された統制、テクノロジー、およびプロセスに関して、第 1 のディフェンスラインによる、第 2 および第 3 のディフェンスラインに対するトレーニングと教育を含める必要があります。このプロセスには、新しいコントロールに対する定期的なレビューの実施を含めることができるため、第 1 のディフェンスラインでは必要に応じて実装内容を進化させることができるので、新しい脅威に関するベストプラクティスを迅速かつ安全に採用できます。

適切なリスク選好を採用するためのプロセスを実装する

障害はいつでも発生する可能性があります。企業内の適切なリスク機関 (たとえば、取締役会、最高リスク責任者、ビジネスリスク責任者など) は、ビジネスプロセス (およびそのプロセスをサポートする基礎となるワークロード) の重要性を評価し、企業がそのプロセスに求める可用性のレベルを指定する必要があります。この判断では、そのプロセスが中断した場合に、企業、顧客、金融インフラストラクチャに与える潜在的な影響、ならびに高可用性モードでのワークロードの運用コストとビジ

ネスの俊敏性およびイノベーションの比較を考慮する必要があります。これらのリスク選好から遡って考えることで、ビジネスサービスを優先的にサポートするクラウドワークロードの運用上の優先順位と回復力の設計における選択を判断できます。明確なリスク選好を設定することで、効果的なリスク管理とガバナンスが可能になります。

責任共有モデルと、それがクラウドで実行するサービスやワークロードにどのように適用されるかを理解していることを確認してください。

FSIOPS2: 運用リスクを評価完了しましたか?

クラウドの使用に関連して、AWS 責任共有モデルがコントロール環境に与える影響を理解する必要があります。たとえば、特定のコントロールは AWS の責任である場合がありますが、特定のコントロールは依然として金融サービス機関の責任です。AWS の責任共有モデルを確認し、使用される AWS の各サービスやコントロール環境に応じて AWS の責任とお客様の責任とを対応付けます。AWS の責任であるコントロールについては、AWS Artifact を使用して AWS 監査レポートにアクセスし、AWS セキュリティコントロールの実装と運用の有効性を確認することができます。

エンタープライズクラウドのリスク計画を立案

クラウドサービスのビジネス消費者と、この消費を形成する内部の関係者との間の相互作用をマッピングすることが、優れたアプローチです。さらに、リスクやコントロールの考慮事項、3 つのディフェンスライン機能の統合、戦略的目標の達成に努める一方で、クラウドでビジネスを運用および保護するために必要なリソースとトレーニングを確保することなども含めることが重要です。この統合は、運用モデルをリスクベースで評価することで実現でき、意思決定プロセスと権限をレビューしてクラウドに適していることを確認することで特に効果的になります。要件がコントロールに変換されるとき、コントロールの強度 (特定されたリスクが軽減されることを保証するため)、およびコントロールの設計とパフォーマンスを証明する能力 (内部リスク管理と監査機能による独立した評価を容易にするため) に注意を払う必要があります。コントロールの設計に焦点を合わせることで、主要なコントロール要件を最初から設計に組み込むことができます。

ワークロードに適用可能なコンプライアンスおよび規制要件を確認するプロセスを実装

FSIOPS3: 規制上のニーズに対して特定のワークロードを評価しましたか?

金融サービス機関は、クラウドの使用に適用されるすべての規制およびコンプライアンスの義務を認識し、そうした義務を果たすために適切な措置を講じていることを確認する必要があります。戦略の一環として、コンプライアンスを担当する関連する内部の関係者と連携して、移行計画とコントロールのフレームワークを見直し、クラウドの使用に適用される法的要件や規制要件を含めてコンプライアンス要件を特定します。特定の技術要件を満たすようにワークロードを設計することは、コンプライアンスの 1 つの側面にすぎない可能性があるため、総合的な規制およびコンプライアンスのレビューを必ず実施してください。このプロセスには、初期設計と計画の両方、ならびに本番稼働前の準備活動が含まれている必要があります。

コンプライアンスおよび規制上の義務に対する継続的な変更を監視するプロセスも存在していることを確認してください。AWS コンプライアンスセンターは、クラウドの使用に影響を与える可能性のあるいくつかの主要なクラウド関連の規制要件の詳細を知るために使用できるリソースの 1 つです。

クラウドの変更管理プロセスを実装

FSIOPS4: クラウドでワークロードを運用する能力をどのように評価しますか?

クラウド IT 変更管理プロセスは、ポリシー、監査、およびリスクコントロールを遵守しながら、本番稼働環境へのリスクを最小限に抑えるために、IT システムへの変更を容易にします。特に金融サービス機関では、ゲート付きの変更管理プロセスで、外部の変更諮問委員会によるレビューが必要になることが多く、判断に数日から数週間かかることも珍しくありません。構成管理、コードとしてのインフラストラクチャ、自動化されたテストと検証、継続的インテグレーションとデリバリーを活用すれば、CI/CD パイプラインツールに緊密に統合された軽量の承認プロセスを実装できます。

自動化を活用して不良な変更を検出して拒否することにより、手動の承認手順の大部分をより高い信頼性で完全に自動化することができます。外部審査が必要となる金融サービスなどの規制の厳しい業界でも、たとえ当初は手動での手順であっても、審査を全体的なパイプラインと統合する必要があります。すべてのテスト、検証、承認、拒否は、パイプラインデプロイの一部として文書化する必要があります。そうすることで、監査人は、テストと検証が実行された環境や、各変更を誰が (いつ) 承認したかなど、適用されたすべての変更を完全に記録することができます。

金融サービス機関は、クラウド機能をレイヤーで開発し、Amazon ゴールデンマシンイメージ (AMI)、CloudFormation テンプレート、サービスカタログ製品などの承認済み再利用可能なアーティファクトを各レイヤーで生成する必要があります。基本レイヤーのアーティファクトは、変更コントロールプロセスを経て、企業ガイドラインに準拠していることを確認する必要があります。このガイ

ドラインは、組織の他のメンバーがビルディングブロックとして再利用できます。組織が認定されたアーティファクトに基づいて高レベルのアプリケーションを構築すると、変更コントロールプロセスが促進されるので、高レベルのアーティファクトに焦点を当てるだけで済み、リスクを最小限に抑えてコンプライアンスを確保しながら、変更を大幅に高速化できます。時間が経過すると、組織は、手動による介入を必要とする変更をわずかに残しながら、ほとんどの変更を自動化された方法で管理できるようになります。

優れた変更管理プロセスは、リスクとビジネス価値のバランスを取りながら、ビジネス価値を提供できます。これは、生産性を最大化し、プロセスのすべての参加者の無駄な労力やコストを最小化できる方法で行う必要があります。クラウドの自動化、統合、デプロイのツールを使用すると、企業は小さな変更を頻繁に行うことで、リスクを軽減し、ビジネス価値をより速い速度で提供できます。その他のベストプラクティスについては、クラウドでの変更管理に関するホワイトペーパーで確認してください。

コードとしてのインフラストラクチャの実装

コードとしてのクラウドとインフラストラクチャの利点は、プログラム的および自動的に環境全体を構築し、分離できるという能力です。回復力を念頭に置いて設計されている場合、AWS CloudFormationテンプレートまたは AWS Systems Manager 自動化を使用すれば、リカバリ環境を数分で実装できます。自動化は、高可用性と迅速な復旧を維持するために不可欠です。

AWS は、回復力の目標を達成するための幅広い種類の自動化ツールを提供しています。AWS Systems Manager は、災害時のアプリケーションのリカバリ中に使用される完全なランブックを自動化するのに役立ちます。イベントの検出時に自動的に実行されるように、一連の操作を順位付けできます。Systems Manager 自動化ドキュメントを使用すると、これらのランブックをコードと同様に管理できます。それらをバージョン管理し、すべてのリリースと共に更新することができます。これにより、復旧計画をリリースされたコードおよびインフラストラクチャの更新と同期させることができます。

設定ドリフトの回避

プライマリサイトとセカンダリサイト間をドリフトすると、災害発生時の復旧に失敗する可能性があります。金融サービス機関は、AWS CloudTrail と AWS Config を使用してアプリケーションインフラストラクチャへの変更を監視する必要があります。これらのサービスにより、AWS Management Console、AWS SDK、コマンドラインツール、およびその他の AWS のサービスを通じて行われたアクションを含め、AWS アカウント内のアクティビティをモニタリングする機能が提供されます。検出されると、Amazon CloudWatch Events 統合を使用してワークフローを定義し、事後対応アクションを自動化できます。

インフラストラクチャ、アプリケーション、運用上の手順にわたってコードベースの管理の手法を実装することによって、環境へのエラーの発生を制限し、平均修復時間 (MTTR) を短縮するために必要な高度なバージョン管理、テスト、検証、ならびに人的エラーおよび設定ドリフトの軽減が可能になります。

クラウドでの拡張モニタリングの使用

FSIOPS5: オペレーションの正常性をどのように把握しますか?

重要な機能をサポートするワークロードが高可用性を保つには、障害を検出してそれらから迅速に復旧する機能が必要です。運用モデルに組み込むことができるクラウド内のメトリクスを定義、収集、分析することで、ワークロードの運用状態を把握できます。これらのメトリクスは、コード、ワークロード、ユーザーアクティビティによって生成され、実際のパフォーマンスデータを視覚化および調査するために使用できる一元化された照会可能なシステムに収集する必要があります。これは、アプリケーションログ、Amazon CloudWatch、システムログを単独で見るだけでは明確にならないことが多い問題を診断するために重要です。

クラウドプロバイダーのイベントを監視

金融機関は、AWS でワークロードに影響を与える可能性のあるイベントが発生したときにアラートと修復のガイダンスを提供する AWS Health Dashboard を使用する必要があります。ダッシュボードには、関連する情報が適切なタイミングで表示されるため、進行中のイベントを管理するのに役立ちます。また、積極的な通知は、スケジュールされたアクティビティを計画するのに役立ちます。AWS Health Dashboard では、ご使用中のアプリケーションで使用されている AWS リソースの状態に変化があった場合にアラートがトリガーされます。イベントが可視化され問題をすばやく診断して解決するためのガイダンスが表示されます。AWS Health API にアクセスできるエンタープライズサポートおよびビジネスサポートのお客様は、この API を使用して、AWS Health Dashboard から情報を一元化された監視システムに統合し、一貫性のある包括的なアラートメカニズムを定義することができます。

ロールアウト前にシナリオをテスト、モデル化、シミュレーション

FSIOPS6: 継続的改善モデルを開発しましたか?

適切なコントロールによってリスクに対処したかどうかを判断するためのベストプラクティスの 1 つは、クラウドコントロールフレームワークと運用手順に対して実際にシナリオを実行することです。リスクおよびコントロールプログラムを確立し金融機関は、継続的に運用プロセスを評価および最適化する必要があります。AWS にデプロイされたワークロードの定期的な「ゲームデー (本番環境での実行)」は、チームのマッスルメモリーを構築し、すべての運用手順がリカバリの目標をサポートするのに効果的であることを検証するのに役立ちます。リスク選好度をテストし、厳しいが現実的なシナリオを含めるように、ゲームデーを設計することをお勧めします。

イベント後の運用レビューを実施

イベント後の運用レビューは、インシデントの発生後に実施する必要があります。トラブルシューティングと修復手順を実行した後、フォローアップドキュメントとアクションを割り当てる必要があります。イベント後に適切なレビューを実施すると、脅威アクターの成功を可能にした各問題に対処する実践的なアクションのリストが得られます。こうしたアクションによって、イベントの影響を最小限に抑え、将来同様のイベントが発生することを防止、検出、対処する方法を広範な企業に周知する必要があります。重要なイベントであれば、根本原因を把握し、将来的に予防措置を講じることができるように、エラーの修正 (COE) ドキュメントを作成する必要があります。予防措置の実施は、今後の運用会議で測定する必要があります。

セキュリティの柱

セキュリティの柱とは、リスクの評価とその軽減戦略を通してビジネス価値を提供しながら、情報、システム、資産を保護する能力のことを指します。

顧客、カウンターパーティ、規制当局は、金融機関が強力なサイバーセキュリティ体制を維持することを期待しています。AWS とお客様の間での責任共有モデルを考えると、AWS が担当する側面と、お客様が担当する側面を把握することにさらに注意を向ける必要があります。

トピック

- アイデンティティ管理とアクセス管理
- インフラストラクチャの保護
- データ保護
- 主要な AWS のサービス

アイデンティティ管理とアクセス管理

FSISEC1: AWS IAM ロールが最小権限の原則に準拠していることをどのように確認しますか?

FSISEC2: 管理者アカウントなどの昇格された資格情報の使用をどのように監視し、特権の昇格を防ぎますか?

最小権限の原則に基づいて機能的 IAM ロールを設計します。最小限のポリシーセットを持ち、適用可能なアクション、リソース、条件でスコープダウンされたロールを作成します。たとえば、組織内のすべてのデータサイエンティスト向けにロールを作成し、特定のバケット/キーへの読み取り専用アクセスを使用して AWS のデータ分析サービスのみにアクセスできるように制限することができます。

また、AWS IAM ロールを使用して AWS アカウント間でアクセスを委任することにより、1つの AWS アカウントのリソースを別の AWS アカウントのユーザーと共有することもできます。あるアカウントのユーザーが別のアカウントのリソースにアクセスできるようにするには、そのアカウントにアクセスできるユーザーと、そのアカウントに切り替えるユーザーに付与するアクセス許可を定義するロールを作成します。最小権限の原則に沿って、ロールのアクセス許可を、そのロールが機能を実行するために必要なものだけに制限できます。

IAM ポリシーの確認 IAM ポリシーは強力で精巧であるため、各ポリシーによって付与されるアクセス許可を調べて理解することが重要です。詳細については、IAM ポリシーの確認に関するヒントをお読みください。

サービスの最終アクセス時間データを使用してアクセス許可を確認

サービスの最終アクセス時間データを使用して、IAM ロールを定期的に確認します。IAM エンティティ (ユーザーまたはロール) が最後にサービスにアクセスを試みたときのレポートを表示できます。次に、その情報を使用してポリシーを調整し、使用中のサービスのみへのアクセスを許可することができます。IAM のリソースの種類ごとにレポートを生成できます。詳細については、サービスの最終アクセス時間データの表示プロセスのドキュメントをお読みください。

ロールの確認を実行し、未使用のロールを削除 IAM ロールを定期的に確認し、使用されていないロールを削除します。ロールを削除する前に、サービスの最終アクセス時間データレポートを表示して、最近のサービスレベルのアクティビティを確認してください。

特権昇格を緩和 特権昇格とは、悪意のある攻撃者がステルス権限を使用してアクセス許可のレベルを上げ、セキュリティを危険にさらすことです。特権昇格は、管理者以外またはフルアクセス以外のアクセス許可を多数悪用した結果として発生する可能性があります。たとえば、IAM:CreatePolicyVersion です。このアクセス許可により、管理者権限を持たないユーザーが、IAM:SetDefaultPolicyVersion アクセス許可にアクセスしなくても、新しいカスタム権限を作成して、それをポリシーのデフォルトバージョンとして設定することができてしまいます。このようなシナリオを回避するには、次のアクセス許可に注意してください。

- IAM:AddUserToGroup
- IAM:AttachRolePolicy
- IAM:AttachUserPolicy
- IAM:CreateAccessKey
- IAM:CreateLoginProfile
- IAM:CreatePolicyVersion
- IAM:CreateRole
- IAM:CreateUser
- IAM:DeleteRole
- IAM:DeleteRolePermissionsBoundary
- IAM:DeleteRolePolicy
- IAM:DeleteUserPermissionsBoundary
- IAM:DeleteUserPolicy
- IAM:DetachRolePolicy
- IAM:PassRole
- IAM:PutRolePermissionsBoundary
- IAM:PutRolePolicy
- IAM:PutUserPermissionsBoundary
- IAM:SetDefaultPolicyVersion
- IAM:UpdateAssumeRolePolicy
- IAM:UpdateLoginProfile
- IAM:UpdateLoginProfile IAM:CreatePolicyVersion
- IAM:UpdateRole
- IAM:UpdateRoleDescription

- AWS STS:AssumeRole

特権の昇格を防ぐために、アカウント内のユーザー (IAM 管理者または委任された管理者を除く) が管理 IAM アクションを使用できないようにするには、サービスコントロールポリシー (SCP) を使用する必要があります。アクセス許可管理を信頼できる従業員に安全に委任する場合は、IAM アクセス許可境界機能を使用できます。IAM アクセス許可境界により、特権の昇格を防ぎながら、IAM アクセス許可管理を安全に委任できます。たとえば、デベロッパーは、IAM 管理者によって定義された特定のアクセス許可境界を超えることなく、AWS Lambda 関数と Amazon EC2 インスタンスの IAM ロールを安全に作成できます。実際のアクセス許可境界の例については、アクセス許可境界ラウンドのドキュメントを参照してください。

AWS アカウントのアクティビティを監視

次のガイドラインを使用して、AWS アカウントのアクティビティを監視します。

- 各アカウントで AWS CloudTrail をオンにして、サポートされている各リージョンで使用します。
- アクセスが非常に制限された一元化されたログアカウントにAWS CloudTrail ログを保存します。
- CloudTrail ログファイルを定期的に調べます。また、AWS CloudTrail イベント、VPC フローログ、DNS ログを継続的に分析することで脅威を検出するサービスである GuardDuty を使用することもできます。
- Amazon S3 バケットのロギングを有効にして、各バケットに対して行われたリクエストを監視します。
- アカウントが不正に使用されたと考えられる場合は、発行された一時的な認証情報に注意してください。認識できない一時的な認証情報が発行された場合は、それらのアクセス許可を無効にします。

FSISEC3: IAM ロール設計の一環として、役割分担にどのように対応しますか?

セキュリティに関連する役割分担には、2 つの主要な目的があります。最初の目的は、利益相反、乱用、エラーの防止です。2 番目の目的は、セキュリティ違反、情報の盗難、セキュリティコントロールの回避などのコントロール失敗を検出することです。

インフラストラクチャとアプリケーションのデプロイを強力に自動化することで、人間によるアクセスの必要性を減らすことはできますが、それでも個人が主要な機能を完了する必要がある状況も依

然としてあります。役割を分担することは、リスクを軽減するのに役立ちます。増し加えられた特権を持つユーザーの場合、システム管理アクティビティを分散して、1 人の管理者が自分のアクティビティを秘匿したり、システム全体をコントロールしたりできないようにすることが重要です。重要なタスクに対して承認レベルの追加、アクティビティの独立したレビューが必要です。

職務ポリシーを使用してロールを作成

AWS 管理の職務ポリシーは、最小権限の原則が有効であることを保証するために、組織全体のロールを作成するための出発点として使用できます。AWS は、組織内の共通の職務セットに対して、デフォルトで 10 の職務ベースのポリシーを提供しています。

AWS Config を使用して、履歴 IAM 構成と経時変化を表示

AWS Config を使用して、AWS Config の記録中の任意の時点で IAM ユーザー、グループ、ロールに割り当てられた IAM ポリシーを表示します。この情報は、特定の時点でユーザーが有していたアクセス許可を判別するのに役立ちます。たとえば、ユーザー John Doe が 2015 年 1 月 1 日に Amazon VPC 設定を変更するアクセス許可を持っていたかどうかを確認できます。

IAM の構成変更のアラートを設定し、監査を実行

IAM の構成変更を通知するアラートを設定することにより、間接参照のレベルを追加できます。これは、特権が昇格したユーザーによるアクティビティを監視するのに役立ちます。AWS CloudTrail、Amazon CloudWatch、Amazon SNS の組み合わせを使用して追加された間接参照を設定できます。詳細については、IAM の構成が変更されたときにアラートを受信する方法に関するブログ投稿を参照してください。

FSISEC4: すべての人のアクセスが必ずフェデレーションを使用することをどのように保証しますか?

金融機関では、内部および外部のリスクチームと監査チームが、ユーザーアクセス管理とユーザーアクションの監査可能性を精査しています。フェデレーションにより、組織は、ユーザーライフサイクル、パスワード、Multi-Factor Authentication (MFA) 管理などの既存の機能を活用して、アプリケーションと AWS Management Console のシングルサインオンを拡張できます。

デベロッパーの CLI および API 環境にフェデレーションアクセスを使用

フェデレーションアクセスを設定する際は、AWS Management Console および CLI または AWS API へのアクセスを含めることが重要です。CLI および API へのアクセス用に SAML フェデレー

ションを設定する方法の詳細とサンプルスクリプトについては、SAML 2.0 および AD FS を使用してフェデレーション API および CLI アクセスを実装する方法についてのブログ投稿を参照してください。同様のスクリプトは、サードパーティの IdP ベンダーからも入手できます。

IAM ユーザーの作成に関する予防的および発見的コントロールの実装

人によるアクセス用にフェデレーションを設定し、EC2 インスタンスプロファイルをアプリケーションアクセスに使用すると、さらに AWS で作成する必要がある ID または IAM ユーザーはごくわずかです。Break Glass プロセスの管理者 ID がごく少数である場合があります (たとえば、フェデレーション構成または ID プロバイダーに問題がある場合)。また、IAM ロールとの統合をサポートしていないサードパーティアプリケーションのユーザーがごく少数である場合もあります。新しい IAM ユーザーまたはグループを作成する際は、AWS Config による発見的コントロールを実装する必要があります。

IAM ユーザーの認証情報を使用する際は、発見的コントロールを実装

フェデレーションされていない IAM プリンシパルによって実行される API アクションには、発見的コントロールを実装する必要があります。IAM ロールを活用する完全にフェデレーションされた環境では、IAM ユーザーを使用するのは Break Glass 手順など、稀な場合のみにする必要があります。IAM ユーザーによるすべてのアクションを監視し、警告する必要があります。

FSISEC5: すべてのサードパーティアプリケーションがベストプラクティスを使用して AWS API にアクセスしていることをどのように確認しますか?

セキュリティのベストプラクティスとして、組織の AWS API リソースへのアクセスを委任する場合は、サードパーティアプリケーションに IAM ロールとフェデレーションを使用します。

ロールを通じてアクセス許可を付与する

ロールは、ロールセッションの一時的なセキュリティ認証情報を提供します。サードパーティアプリケーションは、AWS アカウントで作成したロールを引き受けることで、AWS リソースにアクセスできます。ロールの権限ポリシーを定義する場合は、IAM 権限を指定する必要があります。このポリシーは、実行できるアクションとアクセスできるリソースを定義します。

IAM ロールは、IAM ユーザー、サードパーティアプリケーション、または EC2 などの AWS のサービスなどの承認されたエンティティによって引き継がれることを意図しています。IAM ロールを EC2 インスタンスに関連付けて、AWS アクセスキーの管理とデプロイを簡素化することができます。EC2 インスタンスは、そのインスタンスで実行されているサードパーティアプリケーションに

一時的なセキュリティ認証情報を提供できます。そして、サードパーティアプリケーションは、それらの認証情報を使用して AWS リソースに API リクエストを行うことができます。

サードパーティに割り当てられた IAM 権限をローテーションして確認する

サードパーティアプリケーションはフェデレーションを使用する必要があります。フェデレーションがサポートされていない場合、IAM 認証情報を定期的にローテーションし、定義された目的が不要になった後や、ユーザーが危険にさらされている疑いがある場合は削除する必要があります。

特定の IAM ユーザーをローテーションまたは削除する必要がある期間を定義する際に考慮するべき事項としては、データの機密性、会社のセキュリティ体制、コーポレートガバナンスとコンプライアンスの要件、および侵害された IAM ユーザーが金融システムに引き起こす可能性がある損害のリスクが含まれますが、これらに限定されるわけではありません。

インフラストラクチャの保護

FSISEC6: SDLC 環境 (開発、テスト、本稼働) 間の分離をどのように保証しますか?

ソフトウェア開発ライフサイクル (SDLC) 環境間でリソースの分離を維持することで、本稼働環境での不正行為や事故の可能性を減らすことができます。これは、クレジットカード業界のデータセキュリティ基準 (PCI DSS) の対象となる金融機関を含め、すべての金融機関にとって重要なガイダンスです。

マルチアカウント戦略を持つ

別個の VPC にデプロイすることで環境を分離することができますが、別個の AWS アカウントにデプロイすると、最高レベルの分離を実現できます。AWS は、複雑さを処理するためのマルチアカウント戦略に関するパターンを提供します。お客様は、SDLC のステージに基づいて個別のアカウントを作成し、このマルチアカウント戦略を通じてセキュリティおよびインフラストラクチャポリシーを適用することを選択できます。この戦略は、設計による AWS のセキュリティ (SbD) の原則に基づいています。この原則は、AWS アカウントの設計を形式化し、セキュリティコントロールを自動化し、監査を効率化するセキュリティ保証アプローチです。詳細については、AWS マルチアカウント戦略の動画を参照してください。

IAM の分離を実装

さまざまな SDLC 環境専用にさまざまなアカウントを持つことで、IAM での特権の管理を自然に分離できます。AWS Organizations は、アカウント階層の管理を容易にします。サービスコントロール

ポリシー (SCP) を定義して、ユーザーがこれらのアカウント内で実行できるアクションを制限します。たとえば、本番環境で CloudTrail 口ギングへの変更を防止したり、VPC でインターネットゲートウェイが設定されないようにしたり、AWS Config 追跡の変更を防止したりできます。

ネットワークの分離を実施

IAM の分離に加えて、本番環境と非本番環境の間でリソースを明確に分離します。異なるアカウントを使用することで、AWS で可能な限り最高の分離形式を構築できます。ただし、特に口ギングやセキュリティサービスなどの共有サービスにアクセスする場合は、アカウントを超えてリソースにアクセスできる必要がある場合があります。VPC ピアリングは、追加のゲートウェイや VPN 接続を必要とせずに、2 つの VPC (同じアカウントまたは異なるアカウント) にあるリソースを接続し、ピアリングされたすべてのネットワークを相互に認識できるようにします。これには、2 つの VPC 間で完全なネットワーク信頼が必要であり、ユースケースに応じてより適切な代替手段が存在します。他の VPC にある少数のサービスにアクセスすることだけが目的である場合は、AWS PrivateLink を使用します。AWS PrivateLink は、VPN なしで内部ネットワークを介した接続を提供し、ネットワークの露出を制限します。サービス発行者は、これらのエンドポイントを使用できる IAM の原則を指定し、許可されるアクションを指定する IAM リソースポリシーをアタッチする必要もあります。より広範な VPC をまたぐアクセスが必要な場合は、AWS Transit Gateway を使用して分離とプライベート接続を確立することも可能です。

FSISEC7: 可能な限りトラフィックをプライベートに保つにはどうすればよいですか?

金融機関は、アプリケーションをクラウドにデプロイする際に、Virtual Private Cloud (VPC) を活用して、組織のニーズに合わせてパブリッククラウドの分離されたプライベート部分を全体から取り除くことができます。最もセキュリティに敏感なお客様は、可能な限りトラフィックがプライベートであり、AWS インフラストラクチャを離れないことを要求しています。

VPC エンドポイントを使用してトラフィックをプライベートに保つ

VPC エンドポイントを使用して、必ずトラフィックが AWS インフラストラクチャ内で行われるようにします。VPC エンドポイントは、VPC 内のリソースとサポートされている AWS のサービスの間でのプライベート接続を許可します。VPC エンドポイントを使用すると、データをプライベートに保つことができ、トラフィックがインターネット経由でルーティングされないため、レイテンシーが低くなります。

リソースポリシーを使用して、VPC エンドポイントを介したアクセスのみを許可

エンドポイントを作成する際に、エンドポイントを使用して AWS リソースへのアクセスをコントロールするポリシーをアタッチできます。たとえば、Amazon API Gateway エンドポイントにエンドポイントポリシーをアタッチすることによって、特定の API へのアクセスを制限します。リソースベースのポリシーに加えて、指定された AWS リソースがエンドポイントを介してのみアクセスされるようにすることもできます。たとえば、エンドポイントを介してのみ S3 バケットへのアクセスを許可するには、トラフィックが VPC から来ていない場合に、リソースへの拒否アクションを含むバケットポリシーを使用します。この条件を指定するには、VPC ID を持つ AWS:sourceVpce 条件を使用します。こうすることで、バケットへのアクセスが強制的にプライベートになり、インターネットを経由せずにエンドポイントのみを通過します。

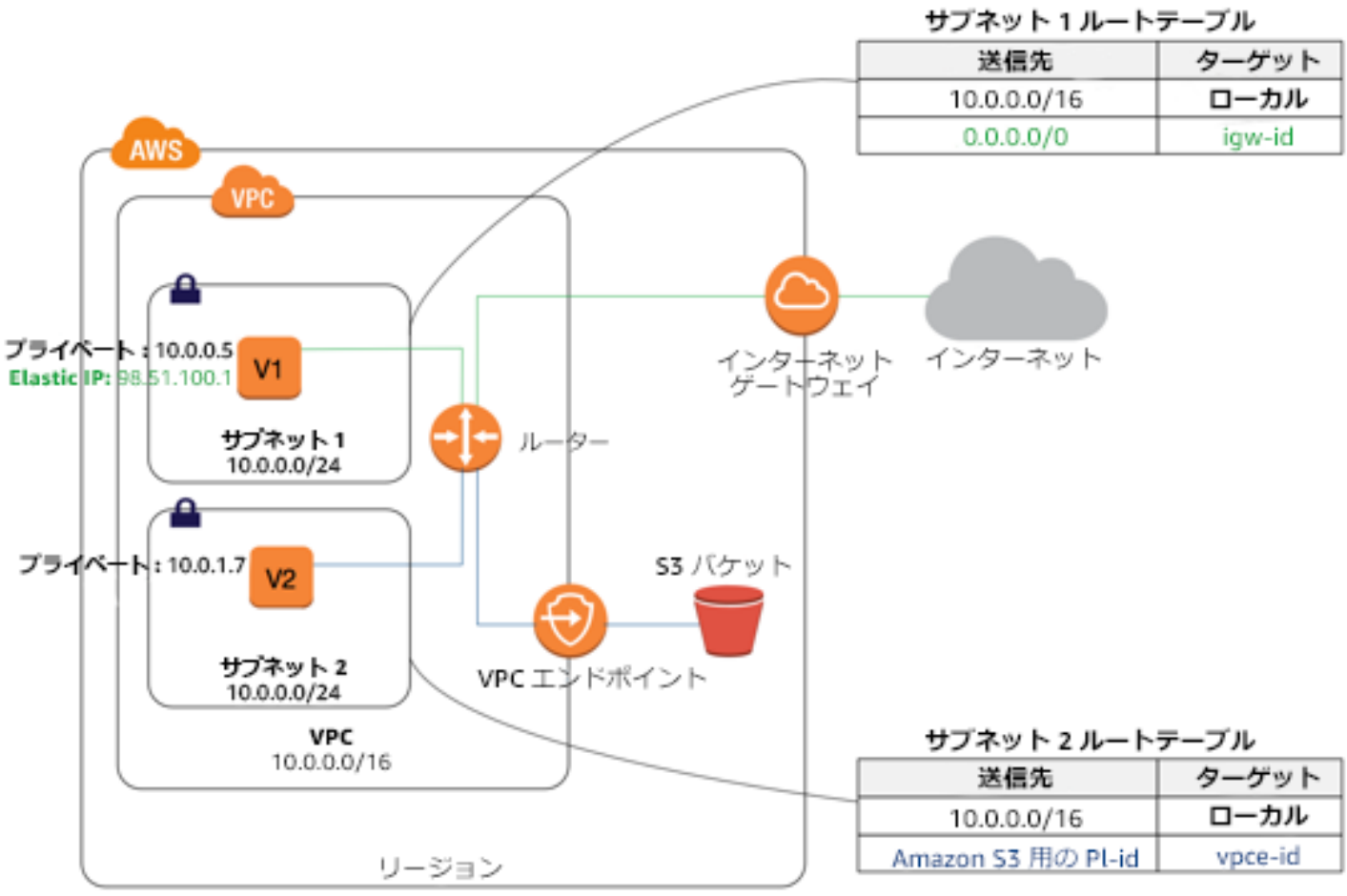


図 7: サブネット 2 のインスタンスは、ゲートウェイエンドポイントを介してのみ Amazon S3 にアクセスできる

制限的セキュリティグループを使用して、プライベートサブネット内のデータベースを保護

金融サービスの顧客がファイアウォールの背後に設定したものと同様に、データベース、ストレージシステム、ボリュームをプライベートサブネットにロックダウンします (データセンターにパブリッ

クアクセスはありません)。データベースへのアクセスは、ネットワークセキュリティグループを使用する特定のポートでデータベースを使用しているアプリケーションレイヤーに制限する必要があります。

FSISEC8: ネットワークに、悪意のあるトラフィックがないかをどのように検査していますか?

予想されるトラフィックと予期しないトラフィックのネットワークトラフィックを監視して、不規則性を特定し、システムのセキュリティに関する重要な洞察を得ます。たとえば、パフォーマンスの低いネットワークは、そのネットワークが攻撃を受けていることを示している可能性があり、予期しない外部システムへの不規則な接続の試みは、内部ホストが侵害されていることを示している可能性があります。

インスタンストラフィックを監視

Amazon EC2 インスタンスは、Amazon CloudWatch を使用してネットワークの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の集約を自動的に追跡します。カスタムメトリックを使用し、ログファイルを CloudWatch にプッシュして、保存、集計、レポート、アラート通知を行います。EC2 インスタンスごとに予想されるネットワーク動作のプロファイルを作成し、逸脱が検出されたときはアラームをトリガーします。たとえば、CloudWatch Logs に送信されたシステムまたはウェブのログは、ログイン失敗の回数またはウェブリクエストの待ち時間に基づいてアラームをトリガーする可能性があります。同様に、TCP 接続または未処理の接続要求数を CloudWatch に保存し、SYN フラッド攻撃などのセキュリティ脅威を検出するために使用することができます。

異常なトラフィックパターンがないか VPC フローログを監視

VPC フローログをセキュリティツールとして使用して、インスタンスに到達するトラフィックのモニタリング、ネットワークトラフィックのプロファイリング、および異常なトラフィック動作の検出を行うことができます。VPC フローログを使用して、異常で予期しない拒否されたアウトバウンド接続リクエストを監視します。これは、EC2 インスタンスの設定ミスまたは侵害を示している可能性があります。CloudWatch アラートは、VPC フローログで基本的なネットワークアラートを提供します。また、VPC フローログデータに基づいて広範なレポート、視覚化、アラート機能を提供するサードパーティのログ管理システムが複数あります。GuardDuty は、AWS CloudTrail イベント、Amazon VPC フローログ、DNS ログを分析することにより、アカウントを継続的に監視できる脅威検出サービスです。また、既知の悪意のある IP アドレス、異常検出、機械学習などの統合された脅威インテリジェンスを使用して、脅威をより正確に識別します。

フローログはすべての IP トラフィックをキャプチャするわけではなく、いくつかの制限があります。詳細については、VPC フローログのドキュメントを参照してください。

VPC トラフィックミラーリングの使用

VPC トラフィックミラーリングを使用して、Amazon 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し、コンテンツ検査、脅威モニタリング、トラブルシューティングなどのユースケースのために、そのトラフィックをセキュリティおよびモニタリングのアプライアンスに転送します。これらのセキュリティおよびモニタリングのアプライアンスは、User Datagram Protocol (UDP) リスナーを備えた Network Load Balancer (NLB) の背後にあるインスタンスのフリートにデプロイできます。Amazon VPC トラフィックミラーリングは、トラフィックフィルタリングとパケット切り捨てをサポートしているため、監視したいトラフィックを抽出できます。また、EC2 インスタンスにパケット転送エージェントをインストールして実行する必要があるという課題にも対処します。パケットは Elastic Network Interface レベルでキャプチャされますが、ユーザースペースから改ざんされることはないため、セキュリティ体制が向上します。

人為的なアクセスがない、イミュータブルなインフラストラクチャを使用

FSISEC9: コンピューティングリソースへのアクセスをどのように保護していますか?

監査とコンプライアンスのニーズをより適切に満たすために、人為的なアクセスがない、イミュータブルなインフラストラクチャのプラクティスを採用します。インフラストラクチャのバージョン管理が可能になり、障害の処理は日常的かつ継続的なビジネス手法になります。

緊急時にのみインタラクティブアクセスを許可 EC2 インスタンスへのインタラクティブアクセスを厳密にコントロールおよび監視します。インタラクティブアクセスは、通常、緊急時のみの Break-glass シナリオに限定する必要があります。

これらの事前設定された緊急ユーザーアカウントをテストおよび確認します。これらのアカウントは通常、非常に高い特権があり、読み取り専用に制限される可能性があります。Break-glass 手順の期間とパスワードの期間を制限します。アカウントの誤用をコントロールおよび削減する目的で、アカウントが利用可能になる前に、受け入れ可能な形式の認証を要求者が提供し、記録することを要求する手順を備えたチケットシステムを用意し、特定の緊急タスクを完了するのは事前承認された担当者だけにします 。Break-glass アカウントと配布手順は、実装の一部として文書化およびテストし、必要なときにタイムリーにアクセスできるように注意深く管理する必要があります。後の監査とレビューに備えて、緊急アクセスを監視するために、特別な監査証跡を設ける必要があります。

Systems Manager Session Manager を使用して、Amazon EC2 インスタンス、オンプレミスインスタンス、仮想マシン (VM) にインタラクティブなワンクリックのブラウザベースのシェルを提供する必要があります。Session Manager を使用することで、インバウンドポートを開いたり、要塞ホストを維持したり、SSH キーを管理したりする必要なしに、安全で監査可能なインスタンス管理が可能となります。

FSISEC10: コンピューティングリソースをどのように構成および強化していますか?

コンピューティングリソースの攻撃対象領域を減らすには、コンピューティングリソースを強化する必要があります。必要なセキュリティツールが常に存在することを確認し、その後、リソースのデプロイとライフサイクルをコントロールして、リソースが常に準拠していることを確認します。

ゴールデン AMI を構築して配布 自動化されたファクトリを使用して、標準に準拠している AMI を構築し、必要なポリシーの遵守をテストし、既知の脆弱性を調査して、使用するために組織全体に配布します。EC2 Image Builder を使用して、Amazon EC2 およびオンプレミスで使用する Linux または Windows Server のイメージを作成、保守、検証、共有、デプロイします。

不可欠なものだけをデプロイ ゴールデン AMI は、必須のソフトウェアのみを実行し、不要なプロセス、ライブラリ、ツールをすべて排除するように強化する必要があります (たとえば、SSH アクセスの無効化)。この最小限の基本オペレーティングシステムのインストールに加えて、ウイルス対策およびエンドポイント保護エージェント、ファイルの整合性、侵入検知エージェントなどの追加の保護ソフトウェアを階層化させることができます。

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、自動化されたセキュリティ評価サービスである Amazon Inspectorを使用して、標準および既知の脆弱性への準拠について新しい AMI をテストしますAmazon Inspector ルールはセキュリティスペシャリストによって定期的に更新されるため、既存の AMI も定期的に再テストして、新たに見つかった脆弱性の影響を受けないようにする必要があります。また、EC2 Image Builder は独自のテストを実行して、機能、互換性、セキュリティコンプライアンスについてイメージを検証することもできます。

承認済みゴールデン AMI のみを許可 承認済み AMI は、組織および AWS Organizations や Service Catalog などのツールに配布できます。サービスコントロールポリシー (SCP) を使用してコントロールを適用し、承認されたバージョンのゴールデン AMI を使用してのみ新しいコンピューティングリソースを開始できるようにすることができます。

コンプライアンスのために構成の変更を監視 AWS Config ルールを使用して、ポリシーへの準拠を監視できます。たとえば、古い AMI が廃止されたり、新しい脆弱性が見つかった場合に、準拠していない古いリソースを自動的に強調表示します。

パッチ管理に AMI パイプラインを使用 AMI パイプラインを使用して、ゴールデン AMI の新しいバージョンでパッチをロールアウトできます。この戦略は、コードのベストプラクティスとしてインフラストラクチャと連携し、コンピューティングリソースの安全で監査可能な証跡を提供します。

基盤となるコンピューティングリソースを保護

FSISEC11: コンテナリソースをどのように構成および強化していますか?

コンテナのセキュリティは、それが実行されている基盤となるホストのセキュリティと同じ程度であり、そのホストが危険にさらされると、そのホストで実行されているすべてのコンテナも危険にさらされます。このために、コンテナを使用する場合、またはコンテナホストのセキュリティを担当する AWS Fargate などのマネージドサービスを使用する場合は、コンピューティングリソースの強化に関するすべてのアドバイスに従う必要があります。コンテナーホストと関連するオーケストレーションソフトウェアを使用している場合は、Docker Bench Security や公開されているコンテナセキュリティのガイドラインなどのツールを使用してインフラストラクチャを強化します。

プライベートコンテナリポジトリを使用

プライベートコンテナリポジトリを使用。Amazon Elastic Container Registry などのプライベートコンテナリポジトリを使用して、コンテナイメージをダウンロードして保存します。プライベートリポジトリを使用すると、一元化されたリポジトリとコンテナツールとの統合による利点を維持しながら、リポジトリへのアクセスをコントロールできます。

最小限のイミュータブルなコンテナイメージを作成

要件を満たすために必要な最小限の依存関係のセットを含む、軽量で安全なイメージから始めます。コンテナの操作に必要のない追加のソフトウェアをインストールしないでください。予期しない機能や脆弱性が発生する可能性があります。コンテナイメージは、実行時に変更されることを意図していません。イメージへの変更が必要な場合は、以下に説明するように、適切に実装されたコンテナビルドパイプラインを介して変更してください。

コンテナのビルドとデプロイのパイプラインを使用

コンテナーのビルドとデプロイメントのパイプラインを使用して、コンテナイメージをビルドし、テスト (ユニットテストや統合テストなど)、コード品質チェック、脆弱性スキャンなどの段階を定義します。イメージがすべての段階を通過した場合は、イメージにタグを付けて署名し、コンテナーリポジトリにアップロードして、環境へのデプロイを開始します。

コンテナイメージをスキャンして脆弱性を確認

CI/CD パイプラインの一部としてコンテナイメージをスキャンし、脆弱性を検出して、デプロイメントに含まれるのを防止します。コンテナスキャンツールを使うと、既知の脆弱性に対するイメージコンテンツのチェック、セキュリティに敏感な構成の構成の分析、独自の追加要件のセットなど、多くの潜在的な問題を検出できます。デプロイの後、コンテナのランタイムスキャンを使用して、リソースの継続的な整合性を確保し、誤った構成やデータ漏洩を防ぐ必要があります。

FSISEC12: 新たな脅威にどのように対処しますか?

セキュリティを重視している企業では、DevSecOps を使用して脅威の特定と修復のレベルを引き上げています。このアプローチにより、アプリケーション開発が加速され、脅威が早期に特定され、確実にソフトウェア開発ライフサイクルの各ステップでセキュリティテストが実行されます。

CVE の修復を自動化

一般的な脆弱性についてサーバーをスキャンすることは、長年にわたるベストプラクティスです。ただし、クラウドでは、お客様は運用環境やアプリケーションの評価を自動化するだけでなく、既知および新たなセキュリティの脆弱性を自動的に修正することもできます。たとえば、Amazon Inspector サービスを使用して本番環境のサーバーを自動的にスキャンし、セキュリティに関する検出結果を Amazon Simple Notification Service (SNS) トピックに公開できます。次に、これらの通知によってトリガーされる AWS Lambda 関数を作成して検出結果を調べ、問題のタイプに基づいて適切な修復を実装します。

すべてのコードデプロイで静的分析を実行

DevSecOps 戦略の一環として、パイプライン内で予防的および発見的なセキュリティコントロールを統合することにより、アプリケーションデプロイのセキュリティを確保できます。静的コード分析の主要な利点の 1 つは、AWS リソースをプロビジョニングする前にセキュリティの脆弱性について把握できることです。これにより、コストとリスクを低減できます。

定期的に侵入テストを実施

AWS 環境内でセキュリティインシデントをシミュレートすることで、セキュリティ体制をよりよく把握できます。金融サービス業界のお客様は、新しいアプリケーションが起動を開始したとき、または最初にクラウドに移行したときに、ほとんどの場合、ウェブアプリケーションへの侵入テストを実行します。一部のお客様では、毎年定期的に侵入テストを実施する場合もあります。大幅なアーキテクチャの変更を伴うすべてのメジャーリリースの後には、侵入テストを必ず実行してください。メジャーリリースでは、以前は存在しなかった脆弱性が導入される可能性があります。

WebApplication ファイアウォールをデプロイ

WebApplication は、HTTP での通信に一連のルールを適用する HTTP アプリケーション用のアプリケーションファイアウォールです。OWASP、ボット、または新たな一般的な脆弱性と露出 (CVE) などのアプリケーションの脆弱性から保護するマネージドルールセットを AWS Marketplace から購入できます。すべてのマネージドルールは、AWS Marketplace セキュリティセラーによって自動的に更新されます。

データ保護

FSISEC13: どのようにデータを分類していますか?

金融サービス機関は、データ分類を使用して、機密データまたは重要なデータを適切なレベルの保護で保護する判断を下します。データがオンプレミスシステムまたはクラウドのどちらで処理や保存されているかに関係なく、データ分類は、組織に対するリスクに基づいて、データの機密性、整合性、可用性に対する適切なコントロールレベルを決定するための開始点です。データを分類し、クラウド環境内で適切なコントロール (暗号化など) を実装するのはお客様の責任です。AWS がインフラストラクチャや提供するサービス内に実装するセキュリティコントロールは、最も機密性の高いデータ要件を満たすために使用できます。

データ分類に基づいて AWS のサービスにタグを付ける

データ分類のベストプラクティスは、組織、法律、コンプライアンス基準を満たす、明確に定義されたデータ分類の階層と要件から始まります。

データ分類フレームワークに基づいて AWS リソースでタグを使用して、データガバナンスプログラムへのコンプライアンスを実装します。このコンテキストでのタグ付けは、データの暗号化、保持、アーカイブの有効化と検証などの自動化に使用できます。

分類に基づいてアクセスを制限

これらのリソースタグと IAM ポリシーを AWS KMS や CloudHSM とともに使用して、データ分類に基づいて保護を実施する独自のポリシーを定義および実装します。たとえば、非常に重要で機密性の高いデータを含むまたは処理する S3 バケットまたは EC2 インスタンスがある場合は、 `#### DataClassification=CRITICAL #######` そこに存在するデータを自動的に、AWS KMS で暗号化します。適切なサービスのみが機密コンテンツにアクセスできるようにするには、キーポリシーを使用してそれらの KMS 暗号化キーへのアクセスレベルを定義します。

機密データの自動検出を活用

機密性の高いものとして分類されるデータには多くの種類のデータがありますが、中でも個人識別情報 (PII) は長い間規制当局の注目を集めてきました。AWS は、組織によるデータ分類スキームの実装と自動化を促進できるいくつかのサービスと機能を提供しています。 Amazon Macie は、クラウドに保存されている機密データやビジネスクリティカルなデータのインベントリと分類に役立ちます。Amazon Macie は、個人識別情報 (PII) や知的財産などの機密データを認識し、このデータがどのようにアクセスまたは移動されているかを可視化するダッシュボードとアラートを提供します。

分類に基づいてデータの使用状況を監視/監査

Amazon Macie は、 CloudWatch Events を使用して、セキュリティ情報とイベント管理 (SIEM) システムおよびマネージドセキュリティサービスプロバイダー (MSSP) ソリューションと統合することにより、データ保護ワークフローを自動化できます。この統合により、アラート処理、コンプライアンスルールセットの作成と変更、Amazon S3 のコンテンツのレポートと構成、CloudTrail によるユーザー認証とアクセスパターンの検出などのセキュリティとコンプライアンスのユースケースを解決できます。Amazon Macie は、アクセスコントロールリストのリセットやパスワードリセットポリシーのトリガーなど、自動修復アクションを簡単に定義およびカスタマイズする機能も提供します。

その他のベストプラクティスについては、AWS データ分類のホワイトペーパーを参照してください。

FSISEC14: クラウド環境でデータ損失をどのように防止していますか?

AWS は、効果的なデータ保護戦略の実装に役立つ幅広いツールとサービスを提供しています。不正アクセスを防止する IAM、キー管理サービス (KMS)、暗号化を管理する CloudHSM、データアクセスアクティビティを監視する CloudTrail、リアルタイムで修復アクションを実行する Lambda 関数、機械学習を使用してアクセスパターンを監視する Amazon Macie などがあります。

完全修飾ドメイン名 (FQDN) の送受信フィルターを使用

ドメイン名は多くの異なる IP アドレスに変換されることが多く、それぞれの送信ポイントでセキュリティグループを維持することが困難な場合があるため、IP によるポリシーの指定は実用的でない場合があります。予想されるドメイン名のリストでアウトバウンドトラフィックをフィルタリングすることは、VPC からの送信トラフィックを保護するための効率的な方法です。これらのサービスのホスト名は通常、デプロイ時に認識されており、アプリケーションがアクセスする必要のあるホストのリストは広範囲ではなく、滅多に変更されないからです。

ドメイン名のリストでトラフィックをフィルタリングすることで、企業はルールの保守とデプロイを一元化できます。サードパーティのソリューションを使用して、可用性が高く安全な FQDN 送信フィルタリングサービスを実装します。

ネットワーク境界のセキュリティに VPC エンドポイントと VPC エンドポイントポリシーを使用

VPC エンドポイントを使用すると、パブリック IP アドレスを必要とせずに、サポートされているリージョンのサービスに VPC をプライベートに接続することができます。エンドポイントを作成する際に、エンドポイントポリシーをアタッチすることもできます。このポリシーは、接続しているサービスへのアクセスをコントロールします。VPC エンドポイントポリシーは、エンドポイントポリシーで AWS:PrincipalAccount、AWS:PrincipalOrgId、AWS:PrincipalOrgPaths などの条件を使用することにより、企業以外の認証情報での AWS のサービスへのアクセスを防ぐことができます。こうした条件により、AWS リージョンのサービスに接続するために VPC 内で企業の認証情報のみが使用されることを保証できます。また、エンドポイントポリシーを使用して、エンドポイントを介して、特定の Amazon S3 バケットなど、特定の AWS リソースへのアクセスを制限できます。

Amazon S3 へのパブリックアクセスの拒否を強制

データ分類のベストプラクティスを使用して、公開データと非公開データを識別します。Amazon S3 に保存されている非公開データは、公開アクセスが拒否されていることを確認してください。各バケットまたはアカウントレベルで Amazon S3 パブリックアクセスのブロック設定を使用して、既存および新しく作成されたリソースがバケットポリシーまたは ACL をブロックしてパブリックアクセスを許可しないようにすることができます。また、SCP を定義して、ユーザーがこの設定を変更できないようにすることも可能です。AWS Config および Lambda を使用して、S3 バケットがパブリックにアクセス可能かどうかを検出および修正します。

暗号化を適用

転送中と保存中の両方での暗号化は、理由に関係なく、データのセキュリティを確保するためのベストプラクティスです。ほとんどの AWS のサービスで暗号化を有効にするには、デプロイ時に暗号化を選択するだけです。AWS Config を使用して、ポリシーに適合しないデプロイが行われたときにアラートを出します。

デフォルトで Amazon S3 を暗号化

意図せずに暗号化されていないデータを保存しないようにするには、保存データの暗号化をデフォルトで有効にする必要がありますこれは、特に Amazon S3 を使用したオブジェクトベースのストレージに関係があります。S3 バケットにデフォルトの暗号化を設定して、そのバケットに保存されるすべてのオブジェクトの暗号化をデフォルトでオンにします (暗号化がオンになった時点でバケットにすでに保存されているオブジェクトは暗号化されないままであることに注意してください)。FSISEC15 で説明されているように、CMK ベースの暗号化を使用します。

異常なトラフィックパターンがないか VPC フローログを監視

VPC フローログを使用して、異常や予期しないアウトバウンド接続リクエストを監視します。これは、データの不正な漏洩を示している可能性があります。Amazon GuardDuty は、VPCフローログ、AWS CloudTrail イベントログ、DNS ログを分析して、AWS 環境内の予期しない潜在的に悪意のあるアクティビティを特定します。たとえば、GuardDuty は、既知のコマンドアンドコントロールサーバーと通信している侵害された EC2 インスタンスを検出することができます。

Amazon S3 で暗号化の使用を監査

S3 バケットのデフォルトの暗号化動作を設定することに加えて、自動監視レポートを通じて暗号化ステータスの定期的な監査を実行することが重要です。S3 インベントリレポートには、オブジェクトとそのメタデータのリストに暗号化ステータスが含まれています。これは、バケットまたはプレフィックスについて毎日または毎週提供されるスケジュールに基づくレポートです。S3 インベントリに暗号化ステータスを追加すると、コンプライアンス監査やその他の目的でオブジェクトがどのように暗号化されているかを確認できます。

S3 インベントリレポートは、オブジェクトのメタデータが許可されていない第三者に開示されるのを防ぐための追加の保護手段として暗号化できます (たとえば、ファイルの名前は機密情報である可能性があります)。

カスタマーマスターキーでエンベロープ暗号化を使用

FSISEC15: 暗号化キーをどのように管理していますか?

AWS KMS ソリューションは、カスタマーマスターキー (CMK) によるエンベロープ暗号化戦略を使用しています。エンベロープ暗号化は、平文データをデータキーで暗号化し、次にデータキーを別のキーで暗号化する方法です。CMK を使用して、AWS KMS の外部で使用するデータキーを生成、暗号化、復号化して、データを暗号化します。CMKs は AWS KMS で作成され、AWS KMS が暗号化されないままになることはありません。

AWS KMS は、カスタマー管理の CMK、AWS 管理の CMK、AWS 所有の CMK の 3 種類の CMK をサポートします (詳細については、 https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys を参照してください)。多くの金融サービス機関のお客様にとって、カスタマー管理の CMK は、お客様のアプリケーションまたは AWS のサービスのいずれかからキーを使用するためのアクセス許可をコントロールできるため、推奨されるオプションになります。カスタマー管理の CMK は、キーの生成や保管にさらなる柔軟性も提供します。さらに、キーの使用またはポリシーの変更はすべて、監査目的でAWS CloudTrail に記録されます。

暗号化キーのローテーション

暗号化のベストプラクティスは、暗号化キーの広範な再利用を推奨しません。セキュリティのベストプラクティスは、既存の CMK の自動キーローテーションを有効にすることです。カスタマー管理の CMK の自動キーローテーションを有効にすると、AWS KMS は CMK の新しい暗号化素材を毎年生成します。また、AWS KMS は CMK の古い暗号化素材も保存して、暗号化したデータの復号化に使用できるようにします。

自動キーローテーションは、すでに CMK で暗号化されているデータには影響しません。既存の CMK データキーを変更したり、その CMK によって保護されているデータを再暗号化したりすることはなく、侵害されたデータキーの影響を軽減することもありません。この場合、データは新しいデータキーで再暗号化する必要があります。

暗号化ログを監視

暗号化キーの使用と管理アクティビティのログを監視することは、金融サービス業界で重要な機能です。また、AWS KMS は AWS CloudTrail と連携して暗号化キーの使用ログを提供し、監査、規制、コンプライアンスのニーズを満たすのにも役立ちます。

キーの削除を監視

キーの破棄は、キー管理者のみが実行できます。すべての破壊要求が安全ウィンドウ内で確認されていることを確認してください (キーをすぐに破棄することはできません。使用できないように無効にされますが、削除されるのはウィンドウの満了時になります)。

FSISEC16: アプリケーションの認証情報 (たとえば、データベース接続文字列やログイン情報) をどのように保護していますか?

「金融における IT リスク: ヒューマンエラーの危険性」と呼ばれる最近の Netwrix 調査によると、データ損失インシデントの 78% は通常のユーザーによって引き起こされていることが確認されました。安全でないパスワードとパスワード共有が、上位 2 つのセキュリティ上の脅威として特定されました。

アプリケーション認証情報の保護 アプリケーション認証情報 (データベース認証情報、パスワード、トークン、API キー) は、顧客データへの直接または間接的なアクセスを許可します。たとえば、データベースでアプリケーションを認証するために、認証情報とパスワードをどこかに保存することが必要になる場合があります。適切なメカニズムでアプリケーション認証情報を保護することで、企業のセキュリティポリシーに準拠し、安全に保つ必要のある機密の財務データへの偶発的または悪意のある使用や不正アクセスのリスクを軽減できます。

アプリケーション認証情報を安全に保存

1 台のマシンと 1 つのアプリケーションでローカルに作業しているなら、データベースの認証情報、パスワード、API キーなどのアプリケーションシークレットの管理は簡単です。多くの分散型マイクロサービスに成長して拡張するにつれて、シークレットを安全に保存、配布、ローテーション、消費することは困難な作業になります。以前は、お客様がシークレット管理のためだけに追加のインフラストラクチャをプロビジョニングおよび保守する必要がありました。これにより、コストが発生し、システムに不要な複雑さが生じる可能性がありました。

AWS Secrets Manager を使用して、認証情報を自動的に更新およびローテーションします。シークレットは、選択した AWS Key Management Service (KMS) キーで暗号化されます。管理者は、個々のロールまたはユーザーの詳細な IAM ポリシーを使用して、これらのシークレットへのアクセスを明示的に許可することができます。

シークレットがコード (平文または暗号化されたコード) に含まれている場合にアラートを送信

アプリケーションのクライアント側で認証情報をハードコーディングしないでください。そうすることで、実装メカニズムによってコードがオープンソースになった場合でも、認証情報が危険にさらされることはありません。

一般的な方法は、コード内のシークレットを暗号化して、ソースコントロールや他のデベロッパーにその値を公開しないようにします。ただし、これらのシークレットを復号化するには、サーバーが別のキーを管理する必要があります。この「シークレットの復号化」キーは、安全に保存してアクセスする必要があります。このアプローチを徐々に廃止して、外部の暗号的に安全な Secrets Manager にシークレットを保存することをお勧めします。

構成データを大規模に安全に保管

AWS Systems Manager を使用して、構成データを管理するための集中ストアとします。パラメータストアを使用すると、シークレットと構成データをコードから分離できます。構成は、選択した KMS キーを使用して暗号化でき、詳細な IAM ポリシーを使用してこれらのパラメーターへのアクセスを明示的に許可することができます。

最小権限の原則の下でアプリケーションプロセスを実行

攻撃者は、OS で昇格された特権 (スーパーユーザー) で実行されているアプリケーションを利用して、アプリケーションサーバーでデータをマイニングしたり、アプリケーションの欠陥を発見したりできるツールセットを実行できます。スーパーユーザー権限でプロセスを実行する権限を持つ正当なユーザーでさえ、隠しキーロガーやその他のマルウェアを使用してアプリケーションを危険にさらす可能性があります。アプリケーションをデプロイして実行するときは、必ず、アクセスする必要のあるリソースをコントロールするための詳細な権限を定義してください。たとえば、アプリケーションは必要なファイルとフォルダにのみアクセスできる必要があります。可能な場合は、Linux 用のカーネルセキュリティモジュール (Secure Enhanced Linux、AppArmor など) のオペレーティングシステム機能を有効にします。同様に、セキュリティの監視/スキャンなどの特定の目的で必要とされない限り、コンテナを特権コンテナとして実行しないでください。Amazon ECS の Linux 機能や、Amazon EKS のポッドセキュリティポリシーなどの機能を使用して、実行時に最小権限の原則を適用します。

特権プロセスと非特権プロセスを分離

アプリケーションが特定の操作を実行するために昇格された特権を必要とする場合があります。こうした状況では、特権プロセスを非特権プロセスから分離し、それらを別々のプロセスとして実行する

必要があります。次に、それぞれのプロセスまたはサービスは、最小権限の原則に従って、異なるセキュリティプリンシパルの下で実行されるように構成できます。

FSISEC17: シークレットへのアクセスと使用をどのように監査しますか?

機密性の高い金融サービスアプリケーションおよび財務報告チェーンに関連するデータに対して、ロールごとにアクセスコントロールを完全に文書化する必要があります。

認証情報を監視および監査して、シークレットの使用状況とシークレットへの変更がログに記録されていることを確認します。こうすることで、予期しない使用や変更を調査し、不要な変更をロールバックすることができます。AWS Secrets Manager を使用して、シークレットを保存します。AWS Secrets Manager は、現在、組織のシークレットと組織内で発生するアクティビティを監視する他の AWS サービス (CloudWatch および CloudTrail) をサポートしています。

シークレットアクセスを監査 AWS Secrets Manager は AWS CloudTrail と統合します。CloudTrail によって収集された情報を使用すると、Secrets Manager に対して各リクエストがいつ行われたか、リクエストが行われた IP アドレス、誰がリクエストを行ったか、追加の詳細を判別するのに役立ちます。

シークレットの使用を監視 Secrets Manager は CloudWatch Events と連携して、シークレットで管理操作が発生したときにアラートをトリガーします。たとえば、シークレットが削除されたとき、またはシークレットがローテーションされたときに、管理者に警告することができます。CloudWatch Events ルールを構成して、これらの操作を監視し、生成されたイベントを管理者が定義したターゲット(Amazon SNS トピックや、後で確認できるように操作の詳細をログに記録する、イベントによってトリガーされる簡単な AWS Lambda 関数) に送信します。

削除が予定されているシークレットのバージョンを監視 AWS CloudTrail, Amazon CloudWatch Logs と Amazon Simple Notification Service (Amazon SNS) の組み合わせを使用して、削除が保留されているバージョンのシークレットへのアクセスの試みを通知するアラームを作成します。このようなアラームで通知を受け取った場合は、シークレットの削除をキャンセルして、本当に削除する必要があるかどうかを判断するための時間を確保してください。調査の結果、本当はまだ必要であるため、シークレットが復元されることになるかもしれません。または、代わりに使用する必要がある新しいシークレットの詳細によるユーザーの更新が必要になることがあります。

FSISEC18: ログの整合性とセキュリティをどのように保護していますか?

ログの監査可能性とログが改竄されないことの保証は、金融サービスが運用管理の有効性とコンプライアンスを実証するために重要です。監査証跡またはログは、コンプライアンス違反のインシデントを特定する上で重要です。このセクションでは、ログの継続的な整合性を確保するのに役立つサービスやベストプラクティスについて説明します。これらのベストプラクティスは、ログを含むデータの保持、インデックス作成、アクセス可能性に関する規制要件にも対応している場合があります。

CloudTrail のログファイルの整合性の検証を有効にする

CloudTrail のログファイルの整合性検証を有効にすることで、ログファイルが CloudTrail の配信後に変更、削除されたか、または変更されていないかを判断できます。CloudTrail は、過去 1 時間に配信された各ファイルのハッシュを含む個別のダイジェストファイルを 1 時間ごとに作成し、パブリックキーとプライベートキーのペアでダイジェストファイルに署名します。

AWS Config を使用

AWS Config を有効にして、リソース構成の変更を追跡し、リソース構成に関する質問に回答し、特定の時点または一定期間にわたってコンプライアンスを実証し、トラブルシューティングを行い、セキュリティ分析を実行します。構成変更通知を処理するときは、ワーカーで AWS Lambda または Amazon Simple Queue Service (SQS) を活用して、変更通知やアラートを処理、フィルタリング、統合します。

Amazon S3 Object Lock を使用

指定された S3 バケットにログを安全に配信し、S3 オブジェクトロック機能を使用してログの不変性を確保できます。S3 オブジェクトロックは、顧客が定義した保持期間中にオブジェクトバージョンの削除をブロックする Amazon S3 の機能であるため、データ保護の追加レイヤーとして保持ポリシーを適用できます。オブジェクトが上書きされないように保護する S3 バージョン管理と組み合わせることで、S3 オブジェクトロック保護が適用されている限り、オブジェクトが不変のままであることを保証できます。オブジェクトに「RetainUntil」日付または「LegalHold」を割り当てることで、S3 オブジェクトロック保護を適用できます。PUT リクエスト内で保持設定を適用することもできますし、作成後に既存のオブジェクトに適用することもできます。

FSISEC19: ランサムウェアからどのように保護していますか?

ランサムウェアは、被害者のファイルを暗号化するマルウェアの一種です。次に、攻撃者は、支払い時にデータへのアクセスを復元するとして、被害者に身代金を要求します。マルウェアは、E メー

ルの添付ファイル、ウェブサイトからのダウンロード、より大規模で高度なデータ侵害の一部など、さまざまな経路で侵入する可能性があります。ただし、足場が確立されると、マルウェアは目に見えるデータの暗号化を開始できます。ランサムウェアに対する効果的な戦略には、予防と回復という 2 つの部分があります。

コンピューティングリソースを保護して、マルウェアの侵入を防ぐ

コンピューティングリソースを保護して、マルウェアのインストールに悪用される可能性のある脆弱性に対してパッチが適用されていることを確認します。コンピューティングリソースに自動的にパッチを適用し、コンプライアンスを監視できるようにする多数のベストプラクティスが、FSISEC9、FSISEC10、FSISEC11、FSISEC12 で説明されています。

攻撃者がデータストアにアクセスするのを防ぐ

最小権限の原則に基づいてデータへのアクセスを絞り込むことは、攻撃の被害範囲を防止および限定するのに役立ちます。効果的なデータ分類スキームは、FSISEC14 で説明されているように、そのスキームに基づく施行や監視とともに、攻撃者がデータにアクセスして暗号化するのを防ぐのに役立ちます。

侵害されたシステムがネットワークの奥深くまで到達できないため、ネットワークの分離や隔離は効果的な保護です。FSISEC7 では、限られた数のホストからプライベートネットワーク経由でデータストアにアクセスできるようにするためのいくつかのベストプラクティスについて説明しています。

トピック

- データアクセスの失敗を監視して攻撃を検出
- 頻繁なバックアップを使用して攻撃から回復

データアクセスの失敗を監視して攻撃を検出

データアクセスログ (S3 アクセスログなど) を SIEM モニターに統合し、アクセスの繰り返し失敗を警告する必要があります。攻撃の兆候である可能性があるからです。異常な CPU 使用率の急上昇は、攻撃者がデータを再暗号化していることを示している可能性もあります。データの暗号化は CPU に負荷がかかるからです。

頻繁なバックアップを使用して攻撃から回復

ランサムウェアはすぐに認識されるため、短期間のアンチランサムウェアバックアップをバックアップサイクルに組み込みます。AWS を使用すると、データストアのスナップショットを簡単に取得で

きるため、頻繁にバックアップし、数日間だけ保管してコストを限定してください。FSISEC19 では、バックアップの整合性を確保および保護するためのいくつかの戦略について説明しています。

主要な AWS のサービス

- アイデンティティ管理とアクセス管理
  - AWS Directory Service: Amazon EC2 for Microsoft Windows Server や Amazon RDS for SQL Server、カスタム .NET アプリケーション、AWS Enterprise などの Active Directory に依存するワークロードを Microsoft Active Directory と統合します。
  - AWS Identity and Access Management (IAM): AWS へのユーザーのアクセスと使用をコントールします。ユーザーおよびグループの作成および管理、アクセスの付与または拒否を行います。強力な承認と認証を実施します。
  - AWS Organizations: 複数の AWS アカウントに適用される作成とポリシーを一元管理します。

- 発見的コントロール
  - AWS CloudTrail: AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にします。AWS インフラストラクチャ全体で、API 呼び出しに関連するイベントのログ記録、継続的なモニタリング、および保持を行います。
  - AWS Config: セキュリティとガバナンスを実現するため、リソースのインベントリ、設定履歴、および設定変更通知を促進します。
  - Amazon CloudWatch: AWS で実行されている AWS クラウドリソースとアプリケーションを監視し、メトリクスを収集および追跡し、ログファイルを収集および監視し、アラームを設定し、AWS リソースへの変更に自動的に対応します。

- データ保護
  - AWS CloudHSM (クラウドハードウェアセキュリティモデル): 専用ハードウェアセキュリティモジュールアプライアンスを使用して、データセキュリティに対する企業コンプライアンス要件、契約上のコンプライアンス要件、および法令遵守の要件を満たします。
  - AWS Key Management Service (KMS): データの暗号化に使用する暗号化キーを作成および管理します。

- インフラストラクチャセキュリティ
  - Amazon EC2 Systems Manager: インベントリの自動管理、OS パッチの適用、安全なシステムイメージの作成、および安全なオペレーティングシステムの構成を支援します。

- AWS Certificate Manager: Secure Sockets Layer/Transport Layer Security (SSL/TLS) 証明書のプロビジョニング、管理、およびデプロイを行います。
- AWS Shield: 選択した AWS のサービスを構成してソリューションを構築するか、DDoS 専用のマネージドサービスを採用することで、DDoS 攻撃を阻止します。
- AWS Web Application Firewall (AWS WAF): 可用性、セキュリティ、およびリソースに影響を与える可能性のある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ます。
- Amazon Inspector: 自動化されたセキュリティ評価を採用し、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ます。
- Amazon Virtual Private Cloud (VPC): ユーザー定義の仮想ネットワーク内で AWS リソースを起動できる AWS の論理的に隔離されたセクションをプロビジョニングします。

- インシデント対応
  - 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エンリッチ化、既知の正常な設定への復元といった、環境の変化に応じて自動的にアクションを実行するルールを作成することを可能にします。
  - GuardDuty: AWS のアカウントとワークロードにおける悪意のある動作や不正な動作を継続的にモニタリングする脅威検出を提供します。GuardDuty は、CloudTrail イベント、VPC フローログ、DNS ログなど、複数の AWS データソースにわたる数百億のイベントを分析し、Amazon CloudWatch Events と AWS Lambda を活用して脅威に対応する方法を簡単に自動化できます。
  - Amazon Detective: セキュリティの検出結果を調査し、根本原因を特定するプロセスを簡素化します。Amazon Detective は、VPC フローログ、AWS CloudTrail ログ、Amazon GuardDuty の検出結果などの複数のデータソースからの何兆ものイベントを分析し、リソース、ユーザー、および時間の経過に伴うそれらの間での相互作用の統一されたインタラクティブなビューを提供するグラフモデルを自動的に作成します。
  - AWS Lambda: サーバーレスコンピューティングサービスを使用して、インシデントに対するプログラムされた自動応答をスケーリングします。

信頼性の柱

信頼性の柱には、インフラストラクチャまたはサービスの障害からの復旧、必要に応じた動的なコンピューティングリソースの獲得、設定ミスや一時的なネットワークの問題などによる障害の軽減などのシステムの能力が含まれます。

金融機関のテクノロジーシステムは複雑で、相互に、また非金融組織とも密接に関連しています。支払い処理、取引と決済、市場データ、保管管理および使用権限管理、ならびに金融メッセージングは、多くの業界が適切に機能するために依拠するアプリケーションの種類の例です。規制当局は、バーゼル銀行監督委員会、連邦準備制度理事会、イングランド銀行などの機関を通じて、金融機関の回復力に引き続き焦点を当てています。

このセクションでは、金融機関が AWS のサービスで使用し、従来のオンプレミス IT と比較して、高度に伸縮自在で、可用性が高く、回復力があり、スケーラブルなソリューションを低コストで構築できる詳細なベストプラクティスを提示します。こうしたベストプラクティスについて説明するために、サービスの可用性という概念を、目標復旧時間 (RTO) および目標復旧時点 (RPO) と同じ意味で使用します。サービスの可用性の概念とその回復目標との関係の概要は、「Well-Architected 信頼性の柱」に記載されています。

金融機関は AWS のサービスを活用して、アプリケーションが提供する必要のあるレベルの回復力と可用性を提供できます。AWS グローバルインフラストラクチャは、リージョンとアベイラビリティーゾーン (AZ) を中心に構築されています。AWS のサービスは、その範囲と可用性が異なります。一部のサービスは単一の AZ (Amazon EC2, Amazon EBS) でのみ利用可能ですが、別のサービスはリージョン内の複数のアベイラビリティーゾーン (Amazon S3) にまたがっており、さらに高いレベルの可用性を実現するクロスリージョンレプリケーション機能を提供するサービスもあります。CloudFront や Route 53 などの一部の AWS のサービスは、リージョン外のエッジネットワークにデプロイされています。AWS インフラストラクチャの可用性と範囲のより包括的な背景については、「金融サービスの回復力のあるアプリケーション」ホワイトペーパーを参照してください。

トピック

回復力のための設計

AWS は、クラウドでさまざまなレベルの回復力を提供するために活用できる機能を提供します。AWS でのアプリケーションの実装、構成、運用は、お客様の責任です。金融機関は、クラウド上で回復力のあるアプリケーションを構築する際に、以下の次元を使用する必要があります。

- 回復力要件の計画
- 回復アーキテクチャ
- モニタリング
- 開発とデプロイメント
- データバックアップと保持

回復力要件の計画

FSIREL1: ワークロードの回復力要件をどのように決定しますか?

トピック

- ビジネスの重要度を使用して回復目標を推進
- 詳細なアプリケーションの回復力要件を適用
- ピーク負荷を決定する際に市場のボラティリティの過去の例を使用

ビジネスの重要度を使用して回復目標を推進

回復力の要件を決定するための鍵は、ワークロードがサポートする機能の重要度を確立することです。金融機関は、回復力に関する規制要件を検討し、そうした要件を念頭に置いてアプリケーションを設計する必要があります。金融機関は、金融サービス機関が外部のエンドユーザーまたは参加者に提供するサービスを含む重要な機能を最大限に精査します。サービスの中断により、消費者または市場参加者に許容できない損害が発生し、市場の完全性が損なわれ、保険契約者の保護、安全性、健全性、または財政的安定が脅かされるからです。

重要なビジネスサービスに課せられる回復力の要件は、こうした重要性に比例する必要があります。これは、金融機関によって設定されるリスク選好に反映され、回復目標 (RTO、RPO) および可用性メトリクスを通知します。金融機関は、回復力がリスクを規定の範囲内に保つようにアプリケーションを設計し、可用性を監視して継続的に維持する必要があります。また、金融機関はコントロールと回復機能の信頼性をテストして、リスクが発生した場合に規定の範囲内でリスクを取り戻し、中断があっても継続的に運用できることを確認する必要があります。

詳細なアプリケーションの回復力要件を適用

アプリケーションの可用性を、初めにアプリケーション全体の単一ターゲットとして考えてしまうケースがよくあります。しかし詳しく分析してみれば、アプリケーションやサービスは、特定の側面によって求められる可用性がさまざまであることに気付くこともしばしばです。たとえば、システムによっては、既存データを取得するよりも、新しいデータを受信して保存する機能を優先させる場合があります。また、システムの構成や環境を変更するオペレーションよりも、リアルタイムオペレーションを優先させるシステムもあります。Well-Architected 信頼性の柱のホワイトペーパーでは、単一のアプリケーションを構成要素に分解し、それぞれの可用性要件を評価する方法のいくつかについて概説しています。分解のメリットは、システム全体を最も厳格な要件に合わせて設計するのではなく、特定のニーズに応じた可用性に労力をかけることができることです。

コストは重要な要素であり、高レベルの可用性を設計することは非常にコストがかかる可能性があります。最も重要な部分を他の部分から分離することで、効果的なコストのトレードオフを行うことができ、重要な機能を提供しながらパフォーマンスの低下に対応できる機能を提供できます。

ピーク負荷を決定する際に市場のボラティリティの過去の例を使用

金融サービスのワークロードでは、決済や清算などのサービスをトレーダーに直接提供しないものでも、市場のボラティリティが「ロングテール」でピーク需要要件を生み出します。極端なイベントのピークボリュームは、正規分布をモデル化する場合に予想されるよりもはるかに大きいため、通常の p95 および p99 メトリクスではピーク負荷を推定するには不十分です。ワークロードが市場のボラティリティに依存しているかどうかを判断し、過去のピークに基づいて負荷テストのシナリオを調整します。金融サービスのワークロードでは、一般的に需要が劇的に増加する可能性があります。需要の増加に対するスケーリング応答は、需要の変化に対応できる必要があります。たとえば、自動スケーリングはキャパシティを追加するのに数分かかる場合があり、需要が急激に変化するワークロードでは、自動スケーリングが対応できる能力を超える場合があります。過負荷の期間中に障害が発生する可能性があることを念頭に置いて、回復力の要件を決定する必要があります。

回復アーキテクチャ

FSIREL2: 貴社のアーキテクチャは回復力のために設計されていますか?

AWS のサービスがワークロードの可用性にどのように影響するかを把握することは、アーキテクチャの回復力を決定する上で重要なステップです。

トピック

- ベストプラクティスを使用して回復力のあるティア 1 アプリケーションを構築
- 予想されるネットワークトラフィックのベースラインを確立

ベストプラクティスを使用して回復力のあるティア 1 アプリケーションを構築

規制当局や金融機関によってティア 1 として指定されたワークロードは、データの損失がほとんどなく、短いダウンタイムで回復できることを実証する必要があるため、より詳細な調査の対象となります。そうした目標を達成するには、回復力のあるアプリケーションの設計パターンに加えて、自動化された運用、一貫性があるデプロイ、予防的な応答による予知保全を活用する必要があります。こうした戦略は、「金融サービスに対応した AWS」のホワイトペーパーのレジリエントアプリケーションで説明されています。

FSIREL3: 貴社のネットワークは回復力の要件をサポートしていますか?

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドのプライベートで隔離されたセクションをプロビジョニングできます。ここでは、お客様が定義する仮想ネットワークで AWS リソースを起動できます。ただし、回復力のあるワークロードがネットワーク障害、接続の喪失、ネットワークトラフィックの予期しない増加、または DOS 攻撃にどのように反応するかに影響を与える可能性のある機能がいくつかあります。ネットワーク設計は、回復力の目標を達成するためのワークロードのキャパシティを支えます。「Well-Architected 信頼性の柱」のホワイトペーパーでは、ネットワーキングの設計における基本的なベストプラクティスについて概説しています。

予想されるネットワークトラフィックのベースラインを確立

高い、または予期しないネットワークトラフィックの状態を把握するには、ユーザーとシステム間の予想されるデータフローのメトリクスのベースラインを確立する必要があります。このベースラインは、ワークロードが DOS 攻撃を受けているか、予期しない負荷がかかっている場合に、運用上の応答をトリガーする必要があります。AWS は、DOS 攻撃に対する保護を提供できる多くのサービスを提供しています。AWS Shield および AWS Shield Advanced は、Amazon CloudFront、ELB、EC2 リソースで実行されているウェブアプリケーションに統合ウェブアプリケーションファイアウォール (AWS WAF) を提供します。VPC セキュリティグループやネットワークアクセスコントロールリスト (ACL) などの AWS 仮想ネットワーク機能も、ネットワーク攻撃に対する保護で効果的です。

モニタリング

FSIREL4: リソースをどのように監視しますか?

アプリケーションの高可用性には、障害を検出して迅速に回復する機能が必要です。アプリケーションは、障害を検出するために関連するテレメトリを送信するように構成する必要があります。これにより、運用プロセスがこれらのイベントをキャプチャして対応できるようになります。

トピック

- 監視で一括管理を行う
- イベントがない場合のアラート
- 負荷テストを通じてメトリクスを特定し、アラートを検証
- ランブックと RCA を確認し、新しいアラームを特定して、修復を自動化
- サービス指向アーキテクチャーに分散トレースツールを使用

監視で一括管理を行う

AWS クラウドサービスは堅牢なモニタリングを提供しますが、データを整理して、問題をできるだけ早くエスカレーションする必要があります。適切なプロセスが配置されていないと、問題の先行指標を見逃す可能性があります。組織全体で一括管理とクラウド監視標準を標準化することで、情報サイロを回避し、監視データの分析を簡素化できます。AWS、システムメトリクス、アプリケーションログのモニタリングを組み合わせることで、アナリストはシグナルを相互参照し、依存するシステム間で情報をログに記録できます。多くの場合、問題は呼び出しシステムで表面化し、IT プロフェッショナルは、エラーが発生した対象システムではなく、呼び出しシステムでログの解析に時間を費やします。

イベントがない場合のアラート

監視データがない場合は、根本的な問題を示している可能性があります。レポート間隔の欠落を警告するコントロールを実装します。データの欠落を違反として扱い、警告を発します。

負荷テストを通じてメトリクスを特定し、アラートを検証

スケーリングと回復力を検証するには、定期的にワークロードの負荷テストを実行する必要があります。こうした負荷テスト中のキャパシティの制約と顧客による停止に相関する主要なメトリクス (需

要に合わせて自動スケーリングするコンポーネントと、リレーショナルデータベースなど自動スケーリングしないリソースの両方) を特定します。監視するアラートとダッシュボードを作成します。

アプリケーションテストの一部として、自動アラートの検証と修正を含めます。負荷が低い環境で負荷テストを実行し、アラートのトリガーを特定して、自動修復の有効性を確認します。ワークロードの平均検出時間 (MTTD) を最小限に抑えることができれば、回復メカニズムが応答する時間が長くなり、アプリケーションの可用性が向上します。

ランブックと RCA を確認し、新しいアラームを特定して、修復を自動化

定期的に、運用ランブックとインシデントプレイブックを確認して、一般的に発生する手動プロセスを特定します。こうした定常的な活動をトリガーするアラートを作成し、プレイブックのステップを実行する自動化を実装します。最も効果的な修復を提供するには、こうした問題について詳細な根本原因分析を実行することが不可欠です。

サービス指向アーキテクチャーに分散トレースツールを使用

システムがマイクロサービスアーキテクチャの実装と相互依存するようになると、パフォーマンスのボトルネックを特定するという課題が増えます。複数のシステム間でテレメトリを追跡および提供する AWS X-Ray などのアプリケーションパフォーマンス監視ツールを使用します。AWS X-Ray は、サーバーレス、コンテナ、オンプレミスのワークロードをサポートする統合ツールであり、トランザクションが複数のサービスにまたがるときに追跡および実行のデータを提供します。

AWS Backup および保持

FSIREL5: クラウド内のデータをどのようにバックアップしていますか?

FSIREL6: バックアップをどのように保持していますか?

トピック

- データバックアップと保持の要件を理解
- バックアップ戦略の一環としてログをバックアップ
- ランサムウェア対策のバックアップをバックアップ戦略に組み込む
- バックアップのライフサイクルポリシーを作成

- WORM ストレージに S3 オブジェクトロックを使用

データバックアップと保持の要件を理解

ワークロードの回復力の要件を決定する重要なタスクは、データのバックアップと保持のニーズを特定することです。金融機関では、システム内のデータのバックアップと保持に関する標準があり、規制要件によって通知される場合があります。金融サービス業界のお客様は、ご使用の環境で実行されているワークロードに適用される要件を理解する必要があります。

バックアップ戦略の一環としてログをバックアップ

アプリケーションデータやデータベースのバックアップに加えて、システムログのバックアップも規制要件に該当する場合があります。CloudTrail、CloudWatch Logs、アプリケーション、システムログをログバックアップ計画に含めます。AWS では、AWS のサービスのバックアップのために Amazon S3、Amazon S3 Glacier、EBS スナップショット、RDS スナップショットを使用し、AWS へのオンプレミスバックアップのために AWS Storage Gateway を使用します。AWS Backup サービスは、バックアップを管理するためのタグベースのポリシーを作成することにより、AWS 環境全体でバックアップの管理を一元化します。

ランサムウェア対策のバックアップをバックアップ戦略に組み込む

通常のバックアップサイクルに加えて、短期間のランサムウェア対策バックアップをバックアップサイクルに組み込む必要があります。ランサムウェアはすぐに認識されるため、こうした追加のバックアップは 1〜2 日だけ保持します。これにより、追加のストレージコストが制限されます。ランサムウェア攻撃から保護するためのバックアップサイクルと保存期間を定義します。データのリージョンでのコピーで十分ですが、これらのバックアップへのアクセスは厳しく制限する必要があります (バックアップもソースと同様に暗号化する必要があります)。ランサムウェア攻撃の防止に関する詳細については、FSISEC19 を参照してください。

バックアップのライフサイクルポリシーを作成

規制要件に基づいて、AWS でデータを保持およびパージするライフサイクルポリシーを作成します。Amazon S3 のデータに関しては、S3 ライフサイクルポリシーにより、最も適切なストレージ階層へのデータの移行を自動化できます。AWS Backup は、タグベースのポリシーを通じて、環境全体でデータの保持を管理できます。

WORM ストレージに S3 オブジェクトロックを使用

金融機関は、S3 オブジェクトロックモードで、「write-once-read-many」 (WORM) モデルを使用してデータを保存できます。オブジェクトに適用される Amazon S3 オブジェクトロックモードは、

ユーザーがそのオブジェクトを変更できないようにします。どのオブジェクトに S3 オブジェクトロックがあるかを追跡するには、オブジェクトのステータスを含む S3 インベントリレポートを参照してください。Amazon S3 オブジェクトロックは、WORM ストレージを必要とする規制要件を満たすのに役立ちます。また、オブジェクトの変更や削除に対する保護の別のレイヤーを追加するだけの場合にも役立ちます。Amazon S3 オブジェクトロックは、SEC 17a-4、CFTC、FINRA 規制の対象となる環境での使用について Cohasset Associates によって評価されています。Amazon S3 オブジェクトロックがこれらの規制にどのように関連しているかについての詳細は、Cohasset Associates Compliance Assessment for Amazon S3 のホワイトペーパーを参照してください。

主要な AWS のサービス

- 回復力のあるアーキテクチャ
  - Amazon S3: Amazon S3 オブジェクトストレージを活用して、AWS 上のデータの耐久性と回復力を提供します。リージョンで利用可能であり (アベイラビリティーゾーン全体に影響を与えるイベントに対して回復力があります)、地理的な分離のためにリージョン間のレプリケーションもサポートします。
  - EC2 Auto Scaling: アプリケーションの可用性を維持し、定義した条件に従って EC2 インスタンスを自動的に追加または削除します。EC2 Auto Scaling の動的および予測スケーリング機能を使用して、変化する需要に対応し、予測需要に基づいて適切な数の EC2 インスタンスをスケジュールして、より高速にスケーリングすることもできます。
  - Amazon Route 53: Route 53 の可用性を利用して、レイテンシー、近接性、アプリケーションのヘルスチェックに基づいてトラフィックを転送し、さまざまな低レイテンシー、フォールトトレラントなアーキテクチャを実現します。
  - AWS Direct Connect: DX を使用して、専用のプライベートで一貫性のある接続を介してデータセンターを AWS に接続します。
  - Amazon Virtual Private Cloud (VPC): AWS リソースを起動できる AWS の論理的に分離されたセクションをプロビジョニングします。
  - Amazon CloudFront: 世界中の CloudFront のエッジロケーションにコンテンツをキャッシュし、必要な場合にのみオリジンからコンテンツをフェッチすることで、オリジンのワークロードを減らすことができます。CloudFront にネイティブなオリジンフェイルオーバー機能を使用して、プライマリオリジンが利用できない場合にバックアップオリジンからコンテンツを自動的に提供できます。
  - Amazon RDS マルチ AZ: RDS マルチ AZ デプロイメントを使用して、本稼働データベースワークロードの可用性を強化します。RDS は、物理的に異なる独立したインフラストラクチャで実行される別の AZ のセカンダリにプライマリインスタンスを同期的にレプリケートします。イン

フラストラクチャに障害が発生した場合、RDS は自動的にスタンバイにフェイルオーバーするため、データベース操作を再開できます。

- Amazon DynamoDB: Amazon DynamoDB は、シームレスなスケーラビリティを備えた、高速で予測可能なパフォーマンスを提供する、完全マネージド型 NoSQL データベースサービスです。DynamoDB は、テーブルのデータとトラフィックをスループットとストレージの要件を処理するのに十分な数のサーバーに自動的に分散し、すべてのデータを保存し、AWS リージョンの複数のアベイラビリティーゾーンに自動的にレプリケートします。
- AWS Shield および AWS Shield Advanced: AWS Shield は、AWS で実行されているアプリケーションの分散型サービス拒否 (DDoS) 攻撃に対する保護を提供するマネージドサービスです。 AWS Shield Advanced は、Amazon EC2、Elastic Load Balancing (ELB)、Amazon CloudFront、AWS Global Accelerator、 Route 53 で実行されているアプリケーションに対して、より高度で大規模な攻撃に対する追加の保護を提供します。
- AWS Lambda: AWS Lambda は、サーバーをプロビジョニングまたは管理することなくコードを実行できます。AWS Lambda は、レプリケーションと冗長性を使用して、サービス自体とサービスが動作するLambda 機能の両方に高可用性を提供するように設計されています。どちらにもメンテナンスウィンドウやスケジュールされたダウンタイムはありません。

- モニタリング
  - CloudWatch: Amazon CloudWatch は、AWS クラウドのリソースと AWS で実行されるアプリケーションについての主要なモニタリングサービスです。
  - VPC フローログ: VPC フローログは、VPC のネットワークインターフェイス間を行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。VPC フローログは、CloudWatch を介して監視できます。

- AWS Backup および保持
  - Amazon S3 Glacier: Amazon Simple Storage Service Glacier は、使用頻度の低いデータ、つまり「コールドデータ」用に最適化された非常に低コストのストレージサービスです。
  - EBS スナップショット、および RDS スナップショット: RDS と EBS の両方のスナップショットにより、それらに保存されているデータのポイントインタイムリカバリが可能になります。どちらのスナップショットも、自動的にまたはスケジュールされた時間に実行するように構成できます。
  - AWS Backup: AWS クラウドおよびオンプレミスの AWS のサービス全体でアプリケーションデータを簡単かつ費用効果の高い方法でバックアップできる一元化されたバックアップサービスです。ストレージボリューム、データベース、ファイルシステムは、バックアップする AWS リ

ソースの構成と監査、バックアップスケジュールの自動化、保持ポリシーの設定、最近のすべてのバックアップと復元のアクティビティの監視を行うことができる中心的な場所にバックアップされます。

パフォーマンス効率の柱

パフォーマンス効率の柱では、コンピューティングリソースを効率的に使ってシステム要件を満たし、需要が変化し技術が進化するのに合わせて効率性を維持することに重点を置きます。

規制当局は、金融サービス機関がワークロードの運用パフォーマンス目標を定義し、そうした目標の達成に役立つポリシーを実装することを期待しています。目標は、運用パフォーマンスの定性的および定量的測定の両方を定義し、ワークロードが満たそうとしているパフォーマンス基準を明示的に示す必要があります。このセクションでは、これらの要件を満たすためにコンピューティングリソースを効率的に使用するための戦略と、需要の変化やテクノロジーの進化に合わせてその効率を維持する方法に焦点を当てます。

目標とサービスレベルの目標を定義したら、ワークロードが期待を満たしているかどうかを定期的に監視および評価する必要があります。ワークロードのパフォーマンスは定期的に報告する必要があります。運用目標も定期的に見直され、新しいテクノロジーとビジネス開発が組み込まれることが期待されています。

FSIPERF1: どのように最良パフォーマンスのアーキテクチャを選択するのですか?

ワークロードのパフォーマンス目標は、ワークロードの重要度によって異なります。市場データフィード、取引実行、決済、清算システムなどの重要なシステムでは、より厳しいパフォーマンス要件が予想されますが、すべてのクラウドワークロードはパフォーマンス要件を定義することで恩恵を受けることができます。

内部および外部のリスクを利用して、パフォーマンス要件を決定

多くの場合、外部の規制および内部のリスク要件は、パフォーマンス要件の検討を開始するのに適した場所です。一部のシステムについては、規制当局が潜在的なストレステストを含む業界全体のガイダンスを発表しています。 ただし、別の規制当局は、金融機関が自ら設定した運用の回復力とパフォーマンス目標を達成する能力を備えていることを要求しています。

負荷の増加率とスケールアウト間隔を考慮に入れる

システムに対するピーク負荷の上限、ならびにピーク負荷に到達するまでに必要な時間を特定します。負荷テストは、トラフィックの増加率を見落とし、スケールアップが速すぎたり遅すぎたりするテストとなることがよくあります。負荷テストの立ち上げが速すぎると、システムが需要を満たすのに十分な速さでキャパシティを追加できない可能性があり、パフォーマンスが低下し、エラーが発生します。負荷テストは、定期的に、またシステムのメジャーリリースごとに実行する必要があります。

FSIPERF2: コンプライアンス要件をどのように評価しますか?

モニタリングすることで、期待されるパフォーマンスからの逸脱を確実に把握できるようにします。

アプリケーション性能のモニタリング (APM) を使用

APM を使用すると、組織はアプリケーションのパフォーマンスが定義された要件を確実に満たすようにする機能を持てます。AWS は、パフォーマンス要件を満たすために必要なクラウドサービスを監視して適切なサイズにする機能を提供します。たとえば、各ユーザーリクエストのレイテンシーとエラー率、すべてのダウンストリーム依存関係、または主要な操作の成功と失敗を監視してアラームを設定することができます。このレベルの監視では、運用チームが保存、分析、視覚化するのが困難な大量のデータが生成されます。チームは、スキルとプロセスを更新し、この新しい洞察の忠実度を最大限に活用するために、頻繁なトレーニングを必要とします。

負荷テスト中の一貫性と障害回復を確認

高負荷である期間中のデータの整合性と回復を確認する必要があります。ワークロードの RTO と RPO が最大負荷の下でも有効であることを保証することで、アーキテクチャと運用の回復力のギャップを明らかにすることができます。

負荷テストに依存関係を含める

金融機関は、重要なビジネスサービスを継続的に提供するために必要なリソースをマッピングする必要があります。こうしたリソースとしては、サードパーティのサービスプロバイダーを含めて、要員、プロセス、テクノロジー、設備、および情報などがあります。このマッピングにより、運用上の依存関係、脆弱性、脅威を特定できます。パフォーマンステストの一部としてワークロードの依存関係 (金融メッセージングプロバイダーなど) を組み込むことで、ワークロードの全体的な回復力を実証できます。

コスト最適化の柱

コスト最適化の柱は、サービスやリソースを最も効果的に活用したシステムを最小限のコストで設計する方法に焦点を当てます。従来のオンプレミスソリューションでは、コストを最適化するためのハードルにぶつかる可能性があります。これは将来のキャパシティーやビジネスニーズを予測すると同時に、複雑な調達プロセスを進める必要があるためです。この柱のプラクティスを採用することで、以下を実現できるアーキテクチャを構築できるようになります。

- 使用量とコストの変動を需要の変動と一致させる。
- 適切なタイプのサービスとリソースを使用して、コストを最小化する。
- コストを分析、属性付け、予測する。
- コストを徐々に削減する。

コスト最適化とは、システムを全ライフサイクルにわたり向上・改善する継続的プロセスです。コストが最適化されたシステムは、すべてのリソースをフル活用して、最小コストで成果を上げ、機能上の要件を満たします。

プロアクティブおよびリアクティブなコスト最適化

Well-Architected フレームワーク内の他の柱と同様に、トレードオフがあります。たとえば、市場投入に要する期間と、コストのどちらを優先すべきでしょうか。場合によっては、市場に迅速に参入したり、期限を守るために、速度の最適化が必要になります。お客様は、最もコストが最適なデプロイのベンチマークに時間を費やすのではなく、「万#の場合」の備えを過度に重視してしまうことがよくあります。これにより、リソースが過剰にプロビジョニングされ、結果として十分に活用されなくなる可能性があります。ただし、これは、オンプレミス環境からクラウドに「リフト & シフト」してから最適化を図る必要がある場合は、必要な選択である場合があります。

どの選択肢を選んでも、金融サービス業界のお客様は、クラウドの経済的メリットをより簡単に実現するために、コスト最適化戦略に投資する必要があります。Well-Architected コスト最適化の柱のホワイトペーパーでは、環境での初期および継続的なコスト最適化のデプロイの手法とベストプラクティスについて説明しています。

まとめ

Well-Architected フレームワークの金融サービス業界レンズの目標は、AWS で信頼性が高く、安全で、効率的で、費用効果の高い規制対象の金融サービスワークロードを設計および運用するためのアーキテクチャのベストプラクティスを提供することです。運用上の優秀性では、AWS で実行されているワークロードが重要な金融サービスビジネスのサービスをサポートできるように、人、プロセス、および運用モデルがどのように調整される必要があるかに関するベストプラクティスの概要を説明します。金融サービスワークロードのアーキテクチャには、セキュリティとエビデンスに基づくコンプライアンス設計パターンを組み込む必要があります。金融サービスを提供するお客様は、ビジネスの回復力と業績目標を達成するために、クラウドでの障害と回復を継続的にモニタリング、測定、およびテストする必要もあります。AWS リソースの消費とモニタリングに関するガバナンスモデルの規模を適切化し、確立することで、コスト削減を大幅に削減した上で、これらの目標を達成できます。

このフレームワークは、AWS でアプリを移行および構築するすべての金融サービスを提供するお客様のセキュリティ、回復力、および運用効率を向上させることができるとともに、規制およびコンプライアンスの義務の遵守にも役立ちます。

寄稿者

本ドキュメントの寄稿者は次のとおりです。

- Arjun Chakraborty、プリンシパルソリューションアーキテクト、AWS 金融サービス
- Ilya Epshteyn、プリンシパルソリューションアーキテクト、AWS 金融サービス
- Misha Goussev、プリンシパルソリューションアーキテクト、AWS 金融サービス
- Som Chatterjee、シニアテクニカルプログラムマネージャー、AWS コマースプラットフォーム
- James Craig、シニアプリンシパルソリューションアーキテクト、AWS 金融サービス
- Anjana Kandalam、マネージャー、ソリューションアーキテクチャ、AWS
- Roberto Silva、シニアソリューションアーキテクト、AWS
- Chris Redmond、シニアコンサルタント、ガバナンス、リスクおよびコンプライアンス部門、AWS プロフェッショナルサービス
- Pawan Agnihotri、シニアマネージャー、ソリューションアーキテクチャ、AWS グローバルファイナンス
- Rahul Prabhakar、グローバル FSI リーダー、AWS セキュリティアシュアランス
- Jaswinder Hayre、シニアマネージャー、ソリューションアーキテクチャ – セキュリティ、AWS
- Jennifer Code、プリンシパルテクニカルプログラムマネージャー、AWS 金融サービス
- Igor Kleyman、FSI 業界スペシャリスト, AWS セキュリティアシュアランス
- John McDonald、ガバナンス、リスク、およびコンプライアンス部門長 – アメリカ州、AWS 金融サービス
- John Kain、銀行および資本市場事業開発部門長

改訂履歴

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードをサブスクライブしてください。

変更	説明	日付
マイナーな更新	FSISEC および FSIREL の質問番号を更新しました。正確性を高めるため、テキストに軽微な更新を加えました。	June 3, 2020
初版発行	金融サービス業界レンズが初めて公開されました。	May 19, 2020

注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。本ドキュメントは、(a) 情報提供のみを目的としており、(b) AWS の現行製品と慣行ついて説明していますが、予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本ドキュメントは、AWS とお客様の間で締結される一切の契約の一部ではなく、その内容を修正することもありません。