を使用してハイブリッドクラウドアーキテクチャを構築するためのベストプラクティス AWS のサービス

AWS 規範ガイダンス

AWS 規範ガイダンス: を使用してハイブリッドクラウドアーキテクチャを構築するためのベストプラクティス AWS のサービス

Table of Contents

を使用してハイブリッドクラウドアーキテクチャを構築するためのベストプラクティス AWS のサービス

アマゾン ウェブ サービス (寄稿者)

2025 年 6 月 (ドキュメント履歴)

多くの企業や組織は、テクノロジー戦略の重要な側面としてクラウドコンピューティングを採用しています。通常、ワークロードを に移行 AWS クラウド して、俊敏性、コスト削減、パフォーマンス、可用性、耐障害性、スケーラビリティを向上させます。ほとんどのアプリケーションは簡単に移行できますが、一部のアプリケーションはオンプレミス環境の低レイテンシーとローカルデータ処理を活用するため、データ転送コストが高くなるのを避けるため、または規制コンプライアンスのためにオンプレミスのままにする必要があります。さらに、アプリケーションのサブセットをクラウドに移動する前に、再設計またはモダナイズする必要がある場合があります。これにより、多くの組織がハイブリッドクラウドアーキテクチャを探してオンプレミスとクラウドの運用を統合し、幅広いユースケースをサポートできます。このハイブリッドアプローチは、オンプレミスコンピューティングとクラウドベースのコンピューティングの両方の利点を提供し、エッジコンピューティングのシナリオに特に役立ちます。

を使用してハイブリッドクラウドを構築する場合は AWS、ハイブリッドクラウド戦略と技術戦略を決定することをお勧めします。

- ハイブリッドクラウド戦略は、ビジネス目標をサポートするためにクラウドとオンプレミスのリソースの消費を管理するガイドラインを提供します。このガイダンスでは、クラウドへの継続的な移行のサポート、災害時のビジネス継続性の確保、低レイテンシーのアプリケーションをサポートするためにクラウドインフラストラクチャをオンプレミス環境に拡張する、国際的なプレゼンスを拡大するなど、ハイブリッドクラウドを構築するための一般的なユースケースについて説明しますAWS。この戦略を定義すると、ハイブリッドクラウドを構築するためのビジネス目標を特定して定義し、ハイブリッドクラウドでのワークロード配置のガイドラインが提供されます。
- ハイブリッドクラウドの技術戦略は、ハイブリッドクラウドアーキテクチャの指針となる教義を特定し、実装フレームワークを定義します。このガイダンスでは、計画されたハイブリッドクラウド実装の原則を定義するのに役立つ、一貫してデプロイおよび管理されるハイブリッドクラウドアーキテクチャの一般的な要件の概要を説明します。これらの要件には、クラウドインフラストラクチャ全体のリソースのプロビジョニングと管理のための標準化されたインターフェイスが含まれます。

このガイドでは、ソリューションアーキテクトとオペレーターがハイブリッドクラウドを実装するための構成要素、ベストプラクティス、 AWS ハイブリッドクラウドとリージョン内サービスを特定するのに役立つ運用と管理のフレームワークについて説明します AWS。

多くの組織は、このガイドで説明されているソリューションを使用して、 が提供するスケール、俊敏性、イノベーション、グローバルフットプリントを活用するハイブリッドクラウド環境を正常にデプロイしています AWS クラウド。 (ケーススタディを参照) AWS ハイブリッドクラウドサービスは、クラウドからオンプレミス、エッジまで一貫した AWS エクスペリエンスを提供します。 AWS Outposts や などのサービスは、エンドユーザーデバイスまたは既存のオンプレミスデータセンターとワークロードサーバー間の低レイテンシーが必要な場合に、コンピューティング、ストレージ、データベースなどの選択を大規模な人口や業界の中心 AWS のサービス の近く AWS Local Zones に配置します。

このガイドの内容

概要

このガイドでは、ハイブリッドクラウドの AWS 推奨事項を、ネットワーク、セキュリティ、耐障害性、キャパシティプランニング、インフラストラクチャ管理の 5 つの柱に分類します。準備状況を改善し、 AWS Outposts や などの AWS ハイブリッドエッジサービスを使用して移行戦略を策定するためのガイドラインを提供します AWS Local Zones。このガイドに従ってプロセスを開発する際に、 AWS ハイブリッドクラウドスペシャリスト AWS Partner がサポートできるように、 AWS アカウント チームまたは と協力することを強くお勧めします。

> **Note**
>
> AWS Outposts と Local Zones は同様の問題に対処しますが、ユースケースと利用可能なサービスや機能を確認して、ニーズに最適な の提供を決定することをお勧めします。詳細については、 AWS ブログ記事を参照AWS Local Zones し AWS Outposts、エッジワークロードに適したテクノロジーを選択してください。

ハイブリッドクラウドワークショップ

AWS ハイブリッドクラウド対象領域エキスパート (SME) の支援により、ハイブリッドクラウドワークショップを実行して、このガイドで説明されている 5 つの柱に関連する会社の成熟度レベルを評価できます。

このワークショップでは、ネットワーク、セキュリティ、コンプライアンス、DevOps、仮想化、ビジネスユニットなど、組織内の内部領域に焦点を当てます。このガイドのハイブリッドクラウド導入プロセスセクションのステップに従って、組織の要件を満たすハイブリッドクラウドアーキテクチャを設計し、実装の詳細を定義するのに役立ちます。

PoCs

特定の要件がある場合は、概念実証 (PoCs) を使用して、ローカルゾーンおよびそれらの要件 AWS Outposts に照らして機能を検証できます。

AWS は PoCs を使用して、Outpost または Local Zone に移行するワークロードをテストし、ワークロードがテストアーキテクチャで機能するかどうかを判断します。テストのためにローカルゾーンにアクセスするには、ローカルゾーンドキュメントの指示に従ってください。でワークロードをテストするには AWS Outposts、チームまたは AWS アカウント と協力して AWS Outposts テストラボ

AWS Partner にアクセスし、ソリューションアーキテクトから AWS ガイダンスを受け取ります。すべてのシナリオで、PoC の開発では、以下を含むテストドキュメントを生成する必要があります。

- AWS のサービス Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Block Store (Amazon EBS)、Amazon Virtual Private Cloud (Amazon VPC)、Amazon Elastic Kubernetes Service (Amazon EKS) などの を使用する
- 使用するインスタンスのサイズと数 (例: `m5.xlarge`または `c5.2xlarge`)
- テストアーキテクチャ図
- テストの成功基準
- 実行する各テストの詳細と目的

柱

次のセクションでは、このガイドで説明するアーキテクチャを使用するための前提条件と制限について説明します。以降のセクションでは、ハイブリッドクラウドワークショップで作成したレコメンデーションドキュメントに実装に必要な設計の詳細が反映されるように、各柱の詳細について説明します。

- エッジでのネットワーキング
- エッジのセキュリティ
- エッジの耐障害性
- エッジでのキャパシティプランニング
- エッジインフラストラクチャ管理

前提条件と制限

このガイドに従う前に、 AWS アカウント チームまたは と協力して、 および Local Zones でエッジアーキテクチャを実装するための前提条件 AWS Outposts と制限 AWS Partner を確認してください。

前提条件

AWS Outposts

- 既存のデータセンターは、施設、ネットワーク、電力AWS Outposts の要件を満たす必要があります。 AWS Outposts は、5～15 kVA の冗長電源入力、1 分あたりの立方フィート (CFM) の kVA の 145.8 倍、および 41° F (5° C) ～ 95° F (35° C) の環境温度を持つデータセンター環境で動作するように設計されています。
- AWS Outposts ラックに関するFAQsを参照して、サービス AWS Outposts がお住まいの国で利用可能であることを確認します。質問を参照: Outposts ラックを利用できる国と地域を教えてください。
- 組織に 4 つ以上のAWS Outposts ラックが必要な場合は、データセンターがアグリゲーション、コア、エッジ (ACE) ラックの要件を満たしている必要があります。
- への接続には、インターネットまたは 500 Mbps 以上の AWS Direct Connect リンク (1 Gbps 以上が適しています) を提供し、維持する必要があります。また、ユースケースで必要な場合は、適切なバックアップ接続が必要です。 AWS OutpostsAWS リージョンから リージョン AWS Outposts への往復時間レイテンシーは、最大 175 ミリ秒である必要があります。
- Enterprise AWS Support または AWS Enterprise On-Ramp の有効な契約が必要です。

AWS Local Zones

- AWS Local Zone は、データセンターまたはユーザーの近くで利用できる必要があります。AWS Local Zones 「 の場所」を参照してください。
- オンプレミスインフラストラクチャから Local Zone へのネットワーク接続があることを確認します。
  - オプション 1: データセンター AWS Direct Connect からローカルゾーンに最も近いAWS Direct Connect プレゼンスポイント (PoP) へのリンク。詳細については、「 Local Zones ドキュメント」の「Direct Connect」を参照してください。

- オプション 2: オンプレミス仮想プライベートネットワーク (VPN) アプライアンスに加えてインターネットリンク、およびローカルゾーンの Amazon EC2 でソフトウェアベースの VPN アプライアンスを起動するために必要なライセンス。詳細については、Local Zones ドキュメントの「VPN 接続」を参照してください。

その他の接続オプションについては、ローカルゾーンのドキュメントを参照してください。

制限

AWS Outposts

- AWS Outposts マルチ AZ 配置での Amazon Relational Database Service (Amazon RDS) には、顧客所有の IP (CoIP) アドレスプールが必要です。詳細については、「Amazon RDS のカスタマー所有 IP アドレス AWS Outposts」を参照してください。
- のマルチ AZ AWS Outposts は、Amazon RDS でサポートされているすべてのバージョンの MySQL および PostgreSQL で使用できます AWS Outposts。詳細については、「Amazon RDS 特徴の AWS Outposts サポートに関する Amazon RDS」を参照してください。の AWS Outposts Amazon RDS は、SQL Server、Amazon RDS for MySQL、Amazon RDS for PostgreSQL データベースをサポートしています。 MySQL PostgreSQL
- AWS Outposts は、 から切断されたときに動作するように設計されていません AWS リージョン。詳細については、ホワイトペーパー「高可用性の設計とアーキテクチャに関する考慮事項」の「障害モードに関する考え方 AWS 」セクションを参照してください。 AWS Outposts
- の Amazon Simple Storage Service (Amazon S3) AWS Outposts にはいくつかの制限があります。これらは、Amazon S3 on Outposts ユーザーガイド」の「Amazon S3 on Outposts と Amazon S3 の違い」セクションで説明されています。 Amazon S3
- の Application Load Balancer は、相互 TLS (mTLS) セッションまたはスティッキーセッションをサポート AWS Outposts していません。
- ACE ラックは完全には囲まれておらず、前面または背面のドアは含まれていません。
- インスタンスキャパシティツールは、新しい注文にのみ適用されます。

AWS Local Zones

- ローカルゾーンには AWS Site-to-Site VPN エンドポイントがありません。代わりに、Amazon EC2 でソフトウェアベースの VPN を使用します。

- ローカルゾーンは をサポートしていません AWS Transit Gateway。代わりに、 AWS Direct Connect プライベート仮想インターフェイス (VIF) を使用してローカルゾーンに接続します。
- すべてのローカルゾーンが Amazon RDS、Amazon FSx、Amazon EMR、Amazon ElastiCache、NAT ゲートウェイなどのサービスをサポートしているわけではありません。詳細については、「AWS Local Zones の機能」を参照してください。
- ローカルゾーンの Application Load Balancer は、mTLS セッションまたはスティッキーセッションをサポートしていません。

ハイブリッドクラウドの導入プロセス

以下のセクションでは、 AWS ハイブリッドクラウドの各柱のアーキテクチャと設計の詳細について説明します。

- エッジでのネットワーキング
- エッジのセキュリティ
- エッジの耐障害性
- エッジでのキャパシティプランニング
- エッジインフラストラクチャ管理

エッジでのネットワーキング

AWS Outposts や Local Zones などの AWS エッジインフラストラクチャを使用するソリューションを設計する場合は、ネットワーク設計を慎重に検討する必要があります。ネットワークは、これらのエッジロケーションにデプロイされているワークロードに到達するための接続の基盤を形成し、低レイテンシーを確保するために不可欠です。このセクションでは、ハイブリッドエッジ接続のさまざまな側面の概要を説明します。

VPC アーキテクチャ

Virtual Private Cloud (VPC) は、そのすべてのアベイラビリティーゾーンにまたがります AWS リージョン。 AWS コンソールまたは AWS Command Line Interface （ AWS CLI) を使用して Outpost または Local Zone サブネットを追加することで、リージョン内の任意の VPC を Outposts または Local Zones にシームレスに拡張できます。次の例は、 AWS Outposts および Local Zones で を使用してサブネットを作成する方法を示しています AWS CLI。

- AWS Outposts: Outpost サブネットを VPC に追加するには、Outpost の Amazon リソースネーム (ARN) を指定します。

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

詳細については、AWS Outposts のドキュメントを参照してください。

- ローカルゾーン: ローカルゾーンサブネットを VPC に追加するには、アベイラビリティーゾーンで使用するのと同じ手順に従いますが、ローカルゾーン ID (<local-zone-name>次の例では) を指定します。

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

詳細については、「 Local Zones ドキュメント」を参照してください。

次の図は、Outpost サブネットとローカルゾーンサブネットを含む AWS アーキテクチャを示しています。

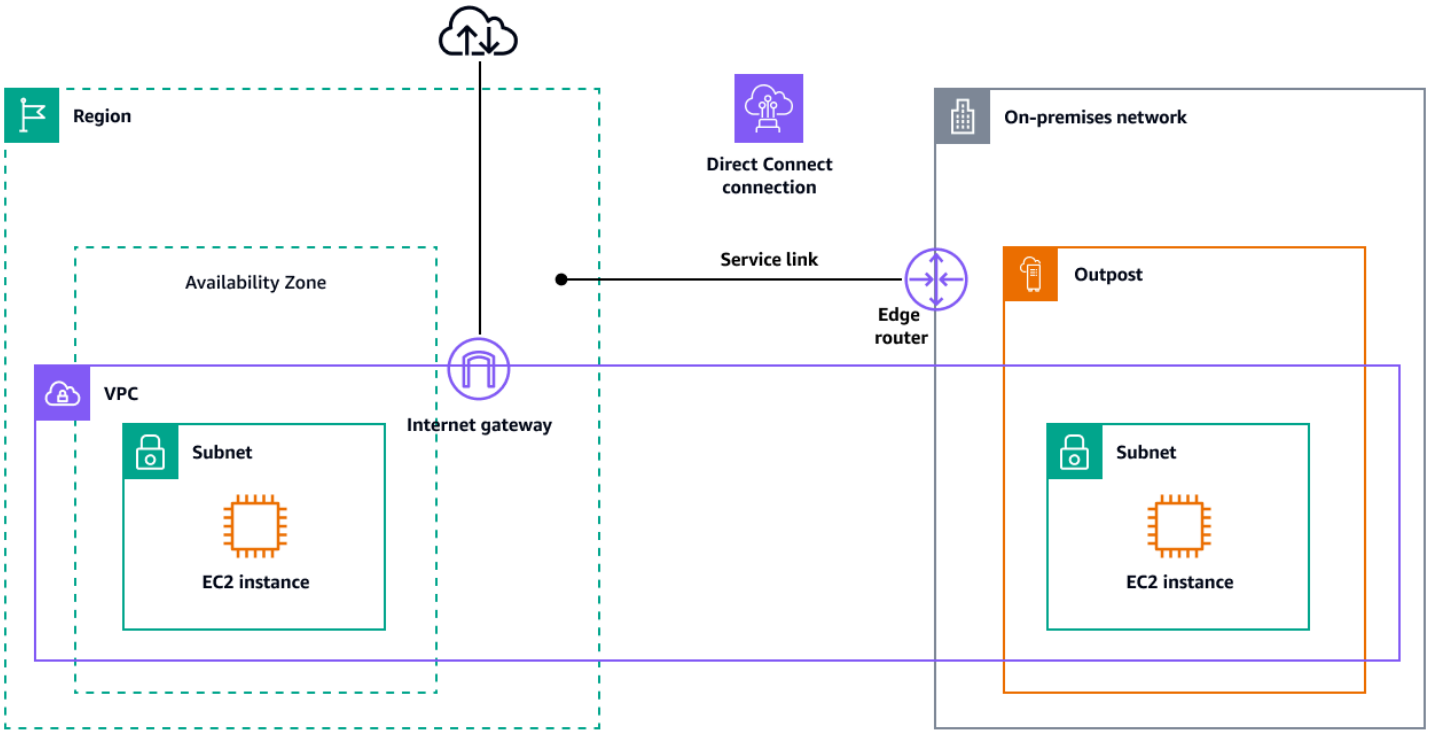
Edge からリージョンへのトラフィック

Local Zones や などのサービスを使用してハイブリッドアーキテクチャを設計する場合は AWS Outposts、エッジインフラストラクチャと 間の制御フローとデータトラフィックフローの両方を検討してください AWS リージョン。エッジインフラストラクチャのタイプによっては、お客様の責任が異なる場合があります。一部のインフラストラクチャでは、親リージョンへの接続を管理する必要があり、 AWS グローバルインフラストラクチャを介してこれを処理するインフラストラクチャもあ

ります。このセクションでは、ローカルゾーンと におけるコントロールプレーンとデータプレーンの接続への影響について説明します AWS Outposts。

AWS Outposts コントロールプレーン

AWS Outposts は、サービスリンクと呼ばれるネットワーク構造を提供します。サービスリンクは、AWS Outposts と、選択したリージョン AWS リージョン または親リージョン (ホームリージョンとも呼ばれます) との間の必要な接続です。これにより、Outpost の管理と Outpost と 間のトラフィックの交換が可能になります AWS リージョン。サービスリンクは、暗号化された VPN 接続のセットを使用してホームリージョンと通信します。インターネットリンクまたは AWS Direct Connect パブリック仮想インターフェイス (パブリック VIF) AWS リージョン 、または AWS Direct Connect プライベート仮想インターフェイス (プライベート VIF) を介して、 AWS Outposts と 間の接続を提供する必要があります。最適なエクスペリエンスと回復性を実現するために、 AWS では、 へのサービスリンク接続に少なくとも 500 Mbps (1 Gbps が適しています) の冗長接続を使用することをお勧めします AWS リージョン。500 Mbps 以上のサービスリンク接続により、Amazon EC2 インスタンスの起動、Amazon EBS ボリュームのアタッチ、Amazon EKS、Amazon EMR、Amazon CloudWatch メトリクス AWS のサービス などのアクセスが可能になります。ネットワークは、Outpost と親のサービスリンクエンドポイント間の最大送信単位 (MTU) である 1,500 バイトをサポートする必要があります AWS リージョン。詳細については、Outposts ドキュメントのAWS Outposts 「 への接続 AWS リージョン」を参照してください。



AWS Direct Connect とパブリックインターネットを使用するサービスリンクの回復力のあるアーキテクチャの作成については、 AWS ホワイトペーパー「高可用性設計とアーキテクチャに関する考慮事項」の「アンカー接続」セクションを参照してください。 AWS Outposts

AWS Outposts データプレーン

AWS Outposts と の間のデータプレーン AWS リージョン は、コントロールプレーンで使用されるのと同じサービスリンクアーキテクチャでサポートされています。 AWS Outposts と の間のデータプレーンサービスリンクの帯域幅は、交換する必要があるデータ量と相関 AWS リージョン する必要があります。データ依存度が高いほど、リンク帯域幅は大きくなります。

帯域幅の要件は、次の特性によって異なります。

- AWS Outposts ラック数と容量の設定
- AMI サイズ、アプリケーションの伸縮性、バースト速度のニーズなどのワークロード特性
- リージョンへの VPC トラフィック

の EC2 インスタンス AWS Outposts と の AWS リージョン EC2 インスタンス間のトラフィックの MTU は 1,300 バイトです。リージョンと の間に相互依存関係があるアーキテクチャを提案する前に、 AWS ハイブリッドクラウドスペシャリストとこれらの要件について話し合うことをお勧めします AWS Outposts。

Local Zones データプレーン

Local Zones と の間のデータプレーン AWS リージョン は、 グローバルインフラストラクチャを通じてサポートされています AWS 。データプレーンは、VPC を介して からローカルゾーン AWS リージョン に拡張されます。ローカルゾーンは、 への高帯域幅の安全な接続も提供し AWS リージョン、同じ APIs とツールセットを通じて、リージョン全体のサービスにシームレスに接続できます。

次の表は、接続オプションと関連する MTUsを示しています。

から	送信先	MTU
リージョンの Amazon EC2	ローカルゾーンの Amazon EC2	1,300 バイト
AWS Direct Connect	ローカルゾーン	1,468 バイト

から	送信先	MTU
インターネットゲートウェイ	ローカルゾーン	1,500 バイト
ローカルゾーンの Amazon EC2	ローカルゾーンの Amazon EC2	9,001 バイト

ローカルゾーンは、 AWS グローバルインフラストラクチャを使用して接続します AWS リージョン。インフラストラクチャは によって完全に管理されるため AWS、この接続を設定する必要はありません。リージョンとローカルゾーンの間に相互依存関係があるアーキテクチャを設計する前に、ローカルゾーンの要件と考慮事項について AWS ハイブリッドクラウドスペシャリストと話し合うことをお勧めします。

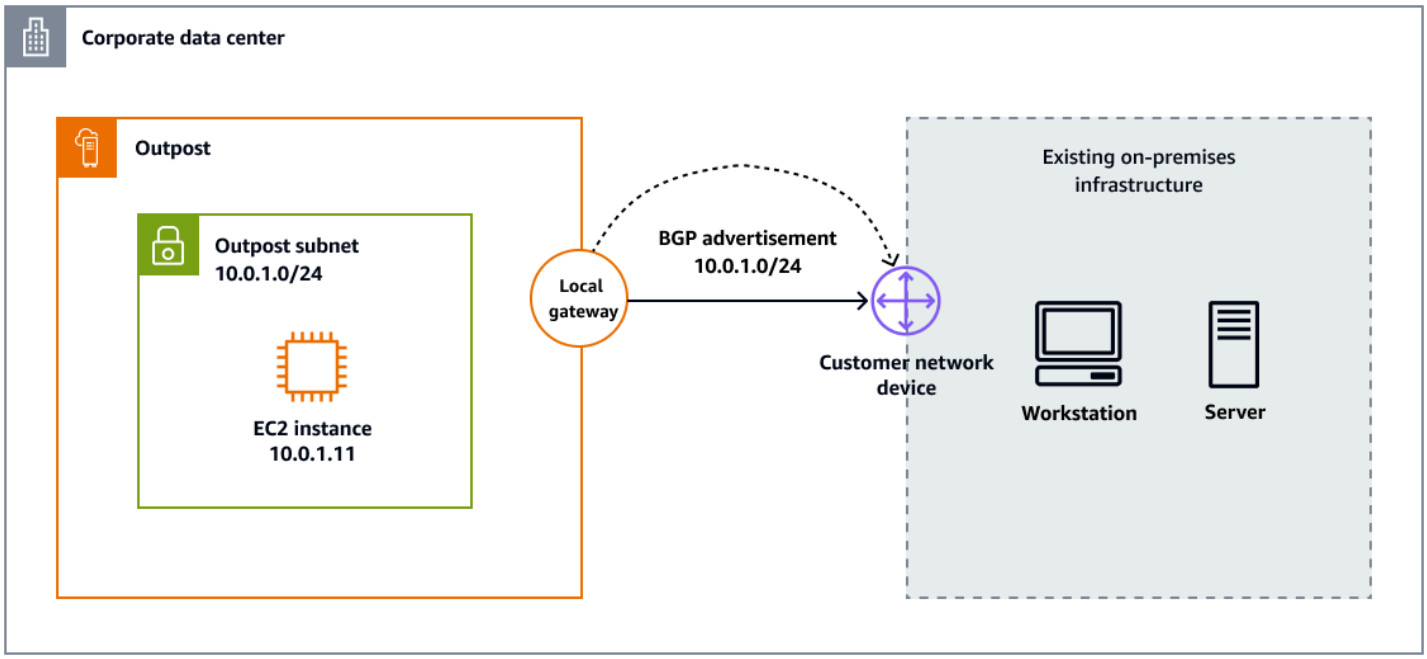
Edge からオンプレミスへのトラフィック

AWS ハイブリッドクラウドサービスは、低レイテンシー、ローカルデータ処理、データレジデンシーコンプライアンスを必要とするユースケースに対応するように設計されています。このデータにアクセスするためのネットワークアーキテクチャは重要であり、ワークロードが AWS Outposts または Local Zones で実行されているかどうかによって異なります。ローカル接続には、以下のセクションで説明するように、明確に定義されたスコープも必要です。

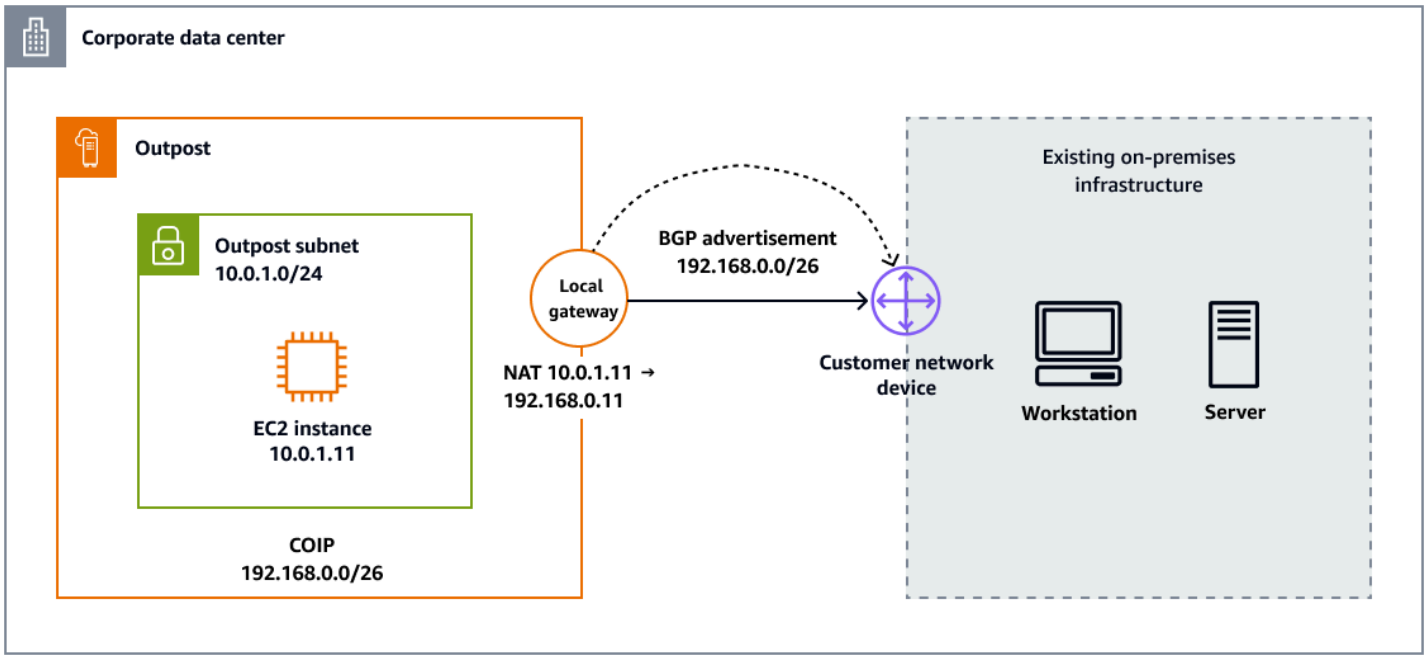
AWS Outposts ローカルゲートウェイ

ローカルゲートウェイ (LGW) は、 AWS Outposts アーキテクチャのコアコンポーネントです。ローカルゲートウェイは、Outpost サブネットとオンプレミスネットワーク間の接続を可能にします。LGW の主な役割は、Outpost からローカルオンプレミスネットワークへの接続を提供することです。また、直接 VPC ルーティングまたは顧客所有の IP アドレスを介して、オンプレミスネットワーク経由でインターネットに接続することもできます。

- ダイレクト VPC ルーティングは、VPC 内のインスタンスのプライベート IP アドレスを使用して、オンプレミスネットワークとの通信を容易にします。これらのアドレスは、ボーダーゲートウェイプロトコル (BGP) を使用してオンプレミスネットワークにアドバタイズされます。BGP へのアドバタイズは Outpost ラックのサブネットに属するプライベート IP アドレスのみを対象としています。このタイプのルーティングは、 のデフォルトモードです AWS Outposts。このモードでは、ローカルゲートウェイはインスタンスに対して NAT を実行せず、EC2 インスタンスに Elastic IP アドレスを割り当てる必要はありません。次の図は、直接 VPC ルーティングを使用する AWS Outposts ローカルゲートウェイを示しています。



- 顧客所有の IP アドレスを使用すると、CIDR 範囲やその他のネットワークトポロジの重複をサポートする、顧客所有の IP (CoIP) アドレスプールと呼ばれるアドレス範囲を指定できます。CoIP を選択するときは、アドレスプールを作成し、ローカルゲートウェイルートテーブルに割り当て、これらのアドレスを BGP 経由でネットワークにアドバタイズする必要があります。CoIP アドレスは、オンプレミスネットワーク内のリソースへのローカル接続または外部接続を提供します。これらの IP アドレスを EC2 インスタンスなどの Outpost のリソースに割り当てるには、CoIP から新しい Elastic IP アドレスを割り当ててから、リソースに割り当てます。次の図は、CoIP モードを使用する AWS Outposts ローカルゲートウェイを示しています。



からローカルネットワーク AWS Outposts へのローカル接続には、BGP ルーティングプロトコルの有効化や BGP ピア間のアドバタイズプレフィックスなど、いくつかのパラメータ設定が必要です。Outpost とローカルゲートウェイの間でサポートできる MTU は 1,500 バイトです。詳細については、 AWS ハイブリッドクラウドスペシャリストに問い合わせるか、AWS Outposts ドキュメントを参照してください。

ローカルゾーンとインターネット

低レイテンシーまたはローカルデータレジデンシーを必要とする業界 (ゲーム、ライブストリーミング、金融サービス、政府など) は、ローカルゾーンを使用してアプリケーションをデプロイし、インターネット経由でエンドユーザーに提供できます。ローカルゾーンのデプロイ中に、ローカルゾーンで使用するパブリック IP アドレスを割り当てる必要があります。Elastic IP アドレスを割り当てるときは、IP アドレスがアドバタイズされる場所を指定できます。この場所はネットワーク境界グループと呼ばれます。ネットワーク境界グループは、 がパブリック IP アドレスを AWS アドバタイズするアベイラビリティーゾーン、ローカルゾーン、または AWS Wavelength ゾーンのコレクションです。これにより、 AWS ネットワークとこれらのゾーンのリソースにアクセスするユーザーとの間のレイテンシーや物理的な距離を最小限に抑えることができます。ローカルゾーンのすべてのネットワーク境界グループを確認するには、ローカルゾーンドキュメントの「利用可能なローカルゾーン」を参照してください。

ローカルゾーンで Amazon EC2 がホストするワークロードをインターネットに公開するには、EC2 インスタンスを起動するときにパブリック IP の自動割り当てオプションを有効にします。Application Load Balancer を使用する場合は、インターネット向けとして定義して、ローカル

ゾーンに割り当てられたパブリック IP アドレスを、ローカルゾーンに関連付けられた境界ネットワークで伝播できます。さらに、Elastic IP アドレスを使用すると、起動後にこれらのリソースの 1 つを EC2 インスタンスに関連付けることができます。ローカルゾーンでインターネットゲートウェイを介してトラフィックを送信する場合、リージョンで使用されるのと同じインスタンス帯域幅仕様が適用されます。ローカルゾーンのネットワークトラフィックは、低レイテンシーコンピューティングへのアクセスを可能にするために、ローカルゾーンの親リージョンを経由せずにインターネットまたはポイントオブプレゼンス (PoPs) に直接送信されます。

ローカルゾーンには、インターネット経由で次の接続オプションが用意されています。

- パブリックアクセス: インターネットゲートウェイを介して Elastic IP アドレスを使用して、ワークロードまたは仮想アプライアンスをインターネットに接続します。
- アウトバウンドインターネットアクセス: ネットワークアドレス変換 (NAT) インスタンスまたは関連付けられた Elastic IP アドレスを持つ仮想アプライアンスを介して、インターネットに直接公開されることなく、リソースがパブリックエンドポイントに到達できるようにします。
- VPN 接続: 関連付けられた Elastic IP アドレスを持つ仮想アプライアンスを介して Internet Protocol Security (IPsec) VPN を使用してプライベート接続を確立します。

詳細については、Local Zones ドキュメントの「Local Zones の接続オプション」を参照してください。

ローカルゾーンと AWS Direct Connect

ローカルゾーンは もサポートしているため AWS Direct Connect、トラフィックをプライベートネットワーク接続経由でルーティングできます。詳細については、「 Local Zones ドキュメント」の「Direct Connect in Local Zones」を参照してください。

ローカルゾーンとトランジットゲートウェイ

AWS Transit Gateway は、ローカルゾーンサブネットへの直接 VPC アタッチメントをサポートしていません。ただし、同じ VPC の親アベイラビリティーゾーンサブネットに Transit Gateway アタッチメントを作成することで、ローカルゾーンワークロードに接続できます。この設定により、複数の VPCsとローカルゾーンワークロード間の相互接続が可能になります。詳細については、Local Zones ドキュメントの「Local Zones 間のトランジットゲートウェイ接続」を参照してください。

ローカルゾーンと VPC ピアリング

新しいサブネットを作成してローカルゾーンに割り当てることで、親リージョンからローカルゾーンに任意の VPC を拡張できます。VPC ピアリングは、ローカルゾーンに拡張された VPCs 間で確立

できます。ピア接続された VPCs が同じローカルゾーンにある場合、トラフィックはローカルゾーン内にとどまり、親リージョンを通じてヘアピンされることはありません。

エッジのセキュリティ

では AWS クラウド、セキュリティが最優先事項です。組織がクラウドのスケーラビリティと柔軟性を採用するにつれて、 はセキュリティ、アイデンティティ、コンプライアンスを主要なビジネス要素として採用する AWS のに役立ちます。 は、セキュリティをコアインフラストラクチャ AWS に統合し、独自のクラウドセキュリティ要件を満たすのに役立つサービスを提供します。アーキテクチャの範囲を に拡張すると AWS クラウド、Local Zones や Outposts などのインフラストラクチャを に統合する利点があります AWS リージョン。この統合により AWS 、 はコアセキュリティサービスの選択されたグループをエッジに拡張できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。AWS 責任共有モデルは、クラウドのセキュリティとクラウドのセキュリティを区別します。

- クラウドのセキュリティ – AWS は、 AWS のサービス で実行されるインフラストラクチャを保護する責任を担います AWS クラウド。 AWS また、 は、お客様が安全に使用できるサービスも提供します。サードパーティーの監査者は、AWS コンプライアンスプログラムの一環として、 AWS セキュリティの有効性を定期的にテストおよび検証します。
- クラウド内のセキュリティ – お客様の責任は、使用する によって決まり AWS のサービス ます。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

データ保護

責任 AWS 共有モデルは、 AWS Outposts および でのデータ保護に適用されます AWS Local Zones。このモデルで説明されているように、 AWS は AWS クラウド (クラウドのセキュリティ) を実行するグローバルインフラストラクチャを保護する責任があります。このインフラストラクチャ (クラウドのセキュリティ) でホストされているコンテンツの制御を維持するのはお客様の責任です。このコンテンツには、 AWS のサービス 使用する のセキュリティ設定および管理タスクが含まれます。

データ保護の目的で、 AWS Identity and Access Management (IAM) または を使用して AWS アカウント 認証情報を保護し、個々のユーザーを設定することをお勧めしますAWS IAM Identity Center。これにより、各ユーザーに各自の職務を果たすために必要なアクセス許可のみが付与されます。

保管中の暗号化

EBS ボリュームでの暗号化

では AWS Outposts、すべてのデータは保管時に暗号化されます。キーマテリアルは、外部キーである Nitro Security Key (NSK) でラップされ、リムーバブルデバイスに保存されます。NSK は、Outpost ラック上のデータを復号化するために必要です。EBS ボリュームとスナップショットに Amazon EBS 暗号化を使用できます。Amazon EBS 暗号化ではAWS Key Management Service 、(AWS KMS) と KMS キーを使用します。

Local Zones の場合、アカウントで暗号化が有効になっていない限り、 すべての EBS ボリュームはすべての Local Zones でデフォルトで暗号化されます。ただし、AWS Local Zones よくある質問に記載されているリスト (「Local Zones での EBS ボリュームのデフォルトの暗号化動作は何ですか？」を参照) を除きます。

Amazon S3 on Outposts での暗号化

デフォルトでは、Amazon S3 on Outposts に保存されるすべてのデータは、Amazon S3 マネージド暗号化キーによるサーバー側の暗号化 (SSE-S3) を使用して暗号化されます。オプションで、ユーザーが用意した暗号化キーによるサーバー側の暗号化 (SSE-C) を使用できます。SSE-C を使用するには、オブジェクト API リクエストの一部として暗号化キーを指定します。サーバー側の暗号化では、オブジェクトのメタデータではなく、オブジェクトデータのみが暗号化されます。

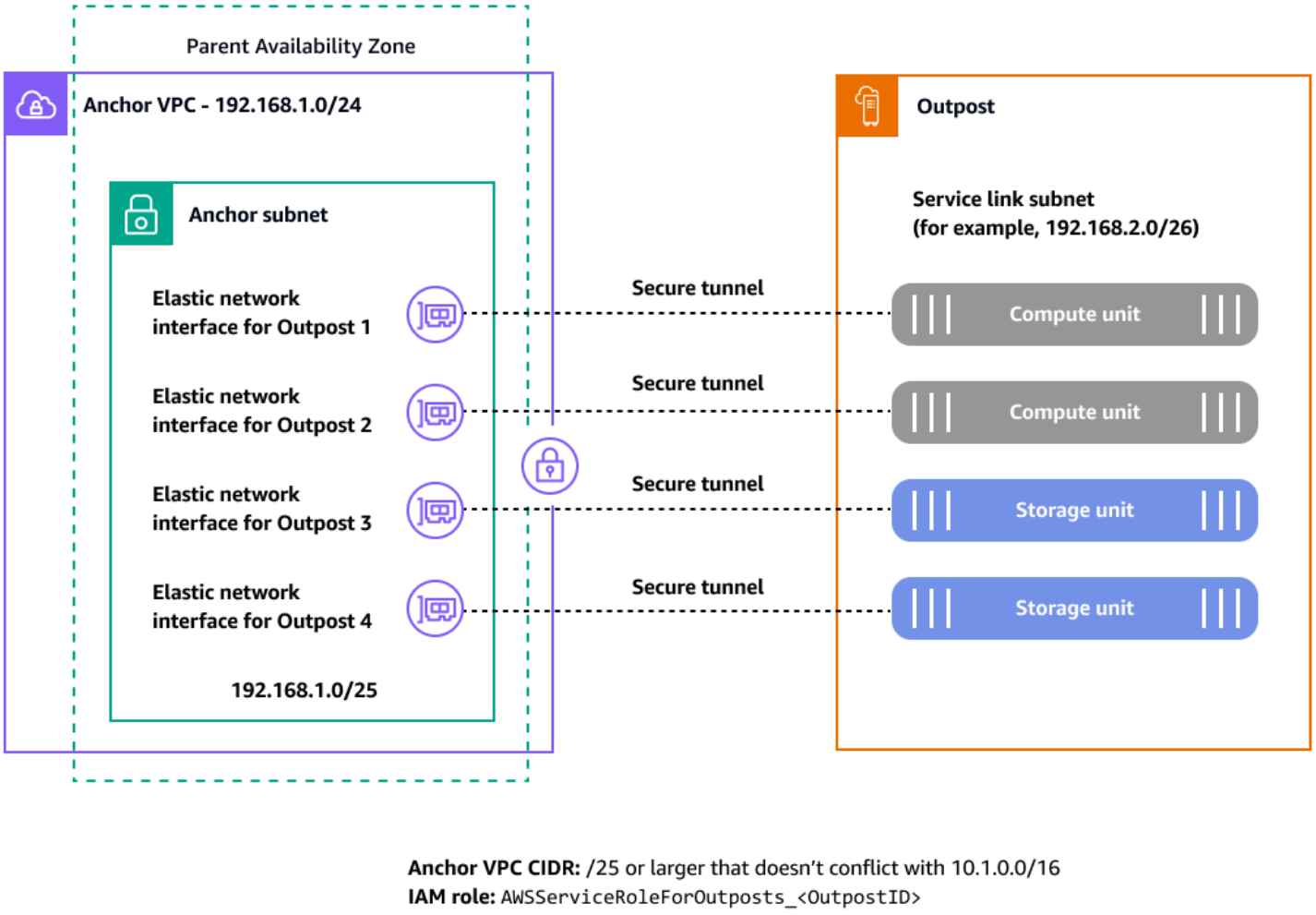
> **Note**
>
> Amazon S3 on Outposts は、KMS キーによるサーバー側の暗号化 (SSE-KMS) をサポートしていません。

転送中の暗号化

の場合 AWS Outposts、サービスリンクは Outposts サーバーと選択した AWS リージョン （ またはホームリージョン) との間の必要な接続であり、Outpost の管理と との間のトラフィックの交換を可能にします AWS リージョン。サービスリンクは、 AWS マネージド VPN を使用してホームリージョンと通信します。内の各ホストは、コントロールプレーントラフィックと VPC トラフィックを分割するための一連の VPN トンネル AWS Outposts を作成します。のサービスリンク接続 (インターネットまたは AWS Direct Connect) に応じて AWS Outposts、これらのトンネルでは、サービスリンクの上にオーバーレイを作成するためにファイアウォールポートを開く必要があります。とサービスリンクのセキュリティに関する詳細な技術情報については、 AWS Outposts ドキュメント

の AWS Outposts 「サービスリンクを介した接続」と「インフラストラクチャセキュリティ AWS Outposts」を参照してください。

AWS Outposts サービスリンクは、次の図に示すように AWS リージョン、親へのコントロールプレーンとデータプレーンの接続を確立する暗号化されたトンネルを作成します。



各 AWS Outposts ホスト (コンピューティングとストレージ) は、親リージョンと通信するために、よく知られている TCP ポートと UDP ポートを介してこれらの暗号化されたトンネルを必要とします。次の表は、UDP プロトコルと TCP プロトコルの送信元ポートと送信先ポートとアドレスを示しています。

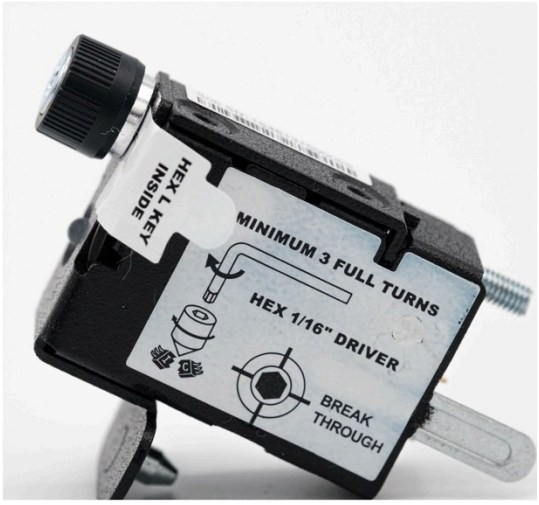
[プロトコル]	ソースポート	送信元アドレス	送信先ポート	送信先アドレス
UDP	443	AWS Outposts サービスリンク /26	443	AWS Outposts リージョンのパブリックルート

[プロトコル]	ソースポート	送信元アドレス	送信先ポート	送信先アドレス
				またはアンカー VPC CIDR
TCP	1025-65535	AWS Outposts サービスリンク /26	443	AWS Outposts リージョンのパブリックルートまたはアンカー VPC CIDR

ローカルゾーンは、Amazon の冗長かつ高帯域幅のグローバルプライベートバックボーンを介して親リージョンにも接続されます。この接続により、ローカルゾーンで実行されているアプリケーションに、他の への高速、セキュア、シームレスなアクセスが可能になります AWS のサービス。ローカルゾーンが AWS グローバルインフラストラクチャの一部である限り、 AWS グローバルネットワークを通過するすべてのデータは、 AWS 保護された施設を離れる前に物理レイヤーで自動的に暗号化されます。オンプレミスロケーションと AWS Direct Connect PoPs 間で転送中のデータを暗号化してローカルゾーンにアクセスする特定の要件がある場合は、オンプレミスルーターまたはスイッチと AWS Direct Connect エンドポイントの間で MAC セキュリティ (MACsec) を有効にできます。詳細については、 AWS ブログ記事AWS Direct Connect 「接続への MACsec セキュリティの追加」を参照してください。

データの削除

で EC2 インスタンスを停止または終了すると AWS Outposts、そのインスタンスに割り当てられたメモリは、新しいインスタンスに割り当てられる前にハイパーバイザーによってスクラブ (ゼロに設定) され、ストレージのすべてのブロックがリセットされます。Outpost ハードウェアからデータを削除するには、特殊なハードウェアを使用します。NSK は、次の写真に示されている小さなデバイスで、Outpost 内のすべてのコンピューティングまたはストレージユニットの前面にアタッチされます。これは、データセンターやコロケーションサイトからデータが公開されないようにするメカニズムを提供するように設計されています。Outpost デバイスのデータは、デバイスの暗号化に使用されるキーマテリアルをラップし、ラップされたマテリアルを NSK に保存することで保護されます。Outpost ホストを返すときは、NSK を破壊するチップの小さなネジを回して NSK を破壊し、物理的にチップを破壊します。NSK を破棄すると、Outpost のデータを暗号化的にシュレッダーにかけます。



Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Outposts リソースの使用を許可する (アクセス許可を付与する) かを制御します。をお持ちの場合は AWS アカウント、追加料金なしで IAM を使用できます。

次の表に、 で使用できる IAM 機能を示します AWS Outposts。

IAM の機能	AWS Outposts のサポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	はい*
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	あり
アクセスコントロールリスト (ACL)	なし
属性ベースのアクセスコントロール (ABAC) (ポリシーのタグ)	あり
一時的な認証情報	はい

IAM の機能	AWS Outposts のサポート
プリンシパル権限	はい
サービスロール	いいえ
サービスリンクロール	あり

* Amazon S3 on Outposts は、IAM アイデンティティベースのポリシーに加えて、バケットポリシーとアクセスポイントポリシーの両方をサポートしています。これらは、Amazon S3 on Outposts リソースにアタッチされたリソースベースのポリシーです。

これらの機能が でサポートされる方法の詳細については AWS Outposts、 AWS Outposts ユーザーガイドを参照してください。

インフラストラクチャセキュリティ

インフラストラクチャ保護は、情報セキュリティプログラムの重要な部分です。これにより、ワークロードシステムとサービスは、意図しない不正アクセスや潜在的な脆弱性から保護されます。たとえば、信頼境界 (ネットワークとアカウントの境界など) 、システムセキュリティの設定とメンテナンス (強化、最小化、パッチ適用など) 、オペレーティングシステムの認証と認可 (ユーザー、キー、アクセスレベルなど) 、その他の適切なポリシー適用ポイント (ウェブアプリケーションファイアウォールや API ゲートウェイなど) を定義します。

AWS は、以下のセクションで説明するように、インフラストラクチャ保護に対するさまざまなアプローチを提供します。

ネットワークの保護

ユーザーはワークフォースまたは顧客の一部であり、どこにでも配置できます。このため、ネットワークにアクセスできるすべてのユーザーを信頼することはできません。すべてのレイヤーにセキュリティを適用する原則に従う場合は、ゼロトラストアプローチを採用します。ゼロトラストセキュリティモデルでは、アプリケーションコンポーネントまたはマイクロサービスは個別と見なされ、コンポーネントまたはマイクロサービスは他のコンポーネントまたはマイクロサービスを信頼しません。ゼロトラストセキュリティを実現するには、次の推奨事項に従ってください。

- ネットワークレイヤーを作成します。レイヤードネットワークは、類似したネットワークコンポーネントを論理的にグループ化するのに役立ちます。また、不正なネットワークアクセスの影響の潜在的な範囲を縮小します。

- トラフィックレイヤーを制御します。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両方にdefense-in-depthアプローチで複数のコントロールを適用します。これには、セキュリティグループ (ステートフル検査ファイアウォール) 、ネットワーク ACLs、サブネット、ルートテーブルの使用が含まれます。
- 検査と保護を実装します。各レイヤーでトラフィックを検査し、フィルタリングします。Network Access Analyzer を使用して、VPC 設定で意図しないアクセスの可能性を調べることができます。ネットワークアクセス要件を指定し、それらを満たしていない潜在的なネットワークパスを特定できます。

コンピューティングリソースの保護

コンピューティングリソースには、EC2 インスタンス、コンテナ、 AWS Lambda 関数、データベースサービス、IoT デバイスなどが含まれます。コンピューティングリソースタイプごとに異なるセキュリティアプローチが必要です。ただし、これらのリソースは、多層防御、脆弱性管理、攻撃対象領域の削減、設定と運用の自動化、遠くでのアクションの実行など、考慮すべき一般的な戦略を共有します。

主要なサービスのコンピューティングリソースを保護するための一般的なガイダンスを次に示します。

- 脆弱性管理プログラムを作成して維持します。EC2 インスタンス、Amazon Elastic Container Service (Amazon ECS) コンテナ、Amazon Elastic Kubernetes Service (Amazon EKS) ワークロードなどのリソースを定期的にスキャンしてパッチを適用します。
- コンピューティング保護を自動化します。脆弱性管理、攻撃対象領域の削減、リソースの管理など、保護コンピューティングメカニズムを自動化します。この自動化により、ワークロードの他の側面を保護するために使用できる時間が解放され、人為的ミスのリスクが軽減されます。
- アタックサーフェスを減らします。オペレーティングシステムを強化し、使用するコンポーネント、ライブラリ、外部で使用可能なサービスを最小限に抑えることで、意図しないアクセスへの露出を減らします。

さらに、 AWS のサービス 使用する ごとに、サービスドキュメントで特定のセキュリティ推奨事項を確認してください。

インターネットアクセス

AWS Outposts と Local Zones の両方が、ワークロードがインターネットとの間でアクセスできるようにするアーキテクチャパターンを提供します。これらのパターンを使用する場合は、外部の Git

リポジトリへのパッチ適用、更新、アクセスなどに使用する場合のみ AWS、リージョンからのインターネット消費を有効なオプションと見なしてください。このアーキテクチャパターンでは、一元化されたインバウンド検査と一元化されたインターネット出力の概念が適用されます。これらのアクセスパターンは AWS Transit Gateway、、NAT ゲートウェイ、ネットワークファイアウォール、およびその他のコンポーネントを使用しますが AWS リージョン、リージョンとエッジ間のデータパスを介して AWS Outposts または Local Zones に接続されます。

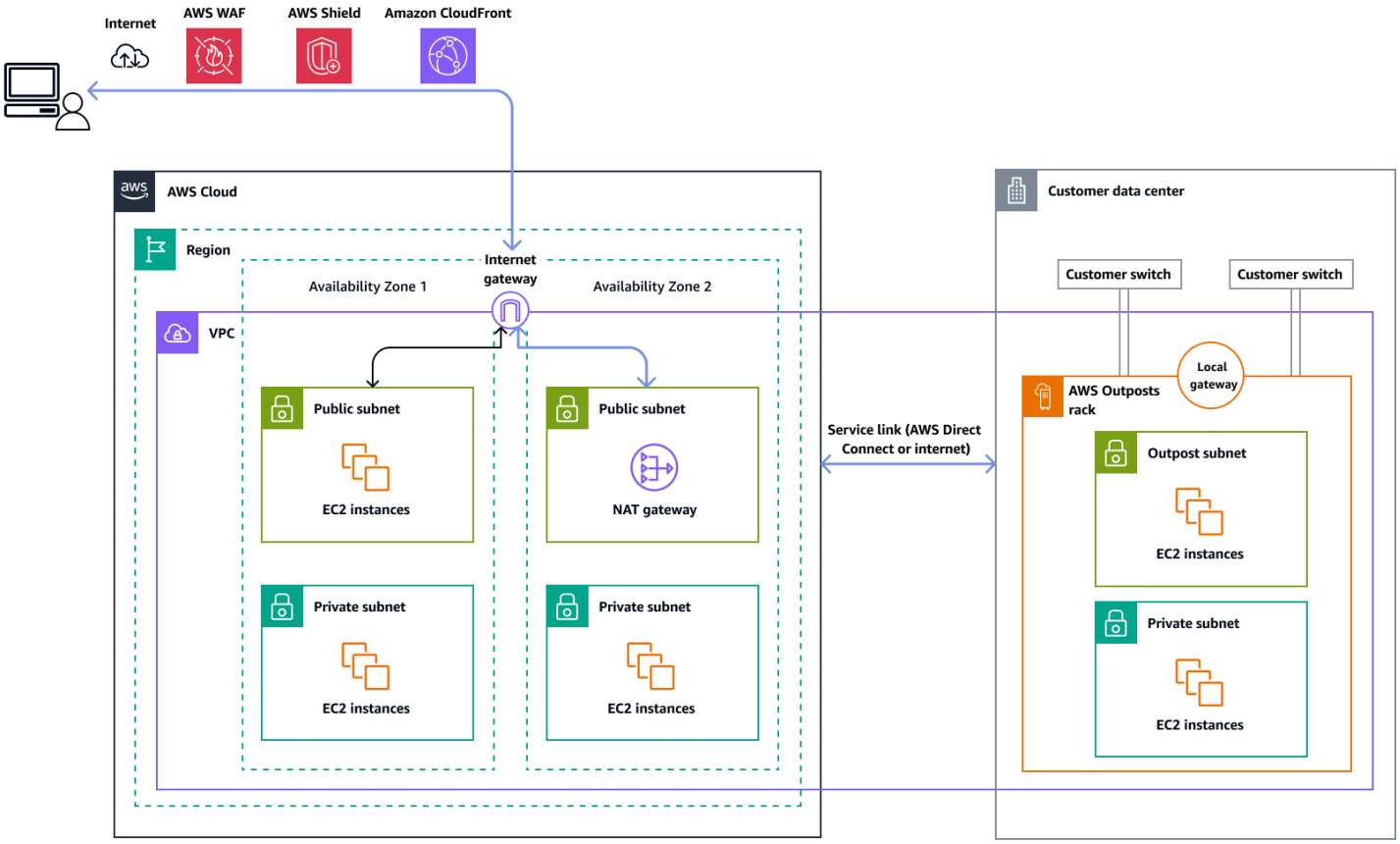
Local Zones は、ネットワーク境界グループと呼ばれるネットワーク構造を採用します AWS リージョン。この境界グループは、これらの一意のグループのパブリック IP アドレスを AWS アドバタイズします。ネットワーク境界グループは、アベイラビリティーゾーン、ローカルゾーン、または Wavelength Zone で構成されます。ネットワーク境界グループで使用するパブリック IP アドレスのプールを明示的に割り当てることができます。ネットワーク境界グループを使用して、Elastic IP アドレスをグループから提供できるようにすることで、インターネットゲートウェイをローカルゾーンに拡張できます。このオプションでは、ローカルゾーンで利用可能なコアサービスを補完するために、他のコンポーネントをデプロイする必要があります。これらのコンポーネントは ISVs から取得され、 AWS ブログ記事 Hybrid inspection architectures with で説明されているように、Local Zone で検査 AWS Local Zonesレイヤーを構築するのに役立ちます。

で AWS Outposts、ローカルゲートウェイ (LGW) を使用してネットワークからインターネットにアクセスする場合は、 AWS Outposts サブネットに関連付けられているカスタムルートテーブルを変更する必要があります。ルートテーブルには、次のホップとして LGW を使用するデフォルトのルートエントリ (0.0.0.0/0) が必要です。お客様は、ファイアウォールや侵入防止システム、侵入検知システム (IPS/IDS) などの境界防御など、残りのセキュリティコントロールをローカルネットワークに実装する責任があります。これは、ユーザーとクラウドプロバイダーのセキュリティ職務を分割する責任共有モデルと一致しています。

親を介したインターネットアクセス AWS リージョン

このオプションでは、Outpost のワークロードは、サービスリンクと親のインターネットゲートウェイを介してインターネットにアクセスします AWS リージョン。インターネットへのアウトバウンドトラフィックは、VPC でインスタンス化された NAT ゲートウェイを介してルーティングできます。イングレストラフィックとエグレストラフィックのセキュリティを強化するには、 で AWS WAF AWS Shieldや Amazon CloudFront などの AWS セキュリティサービスを使用できます AWS リージョン。

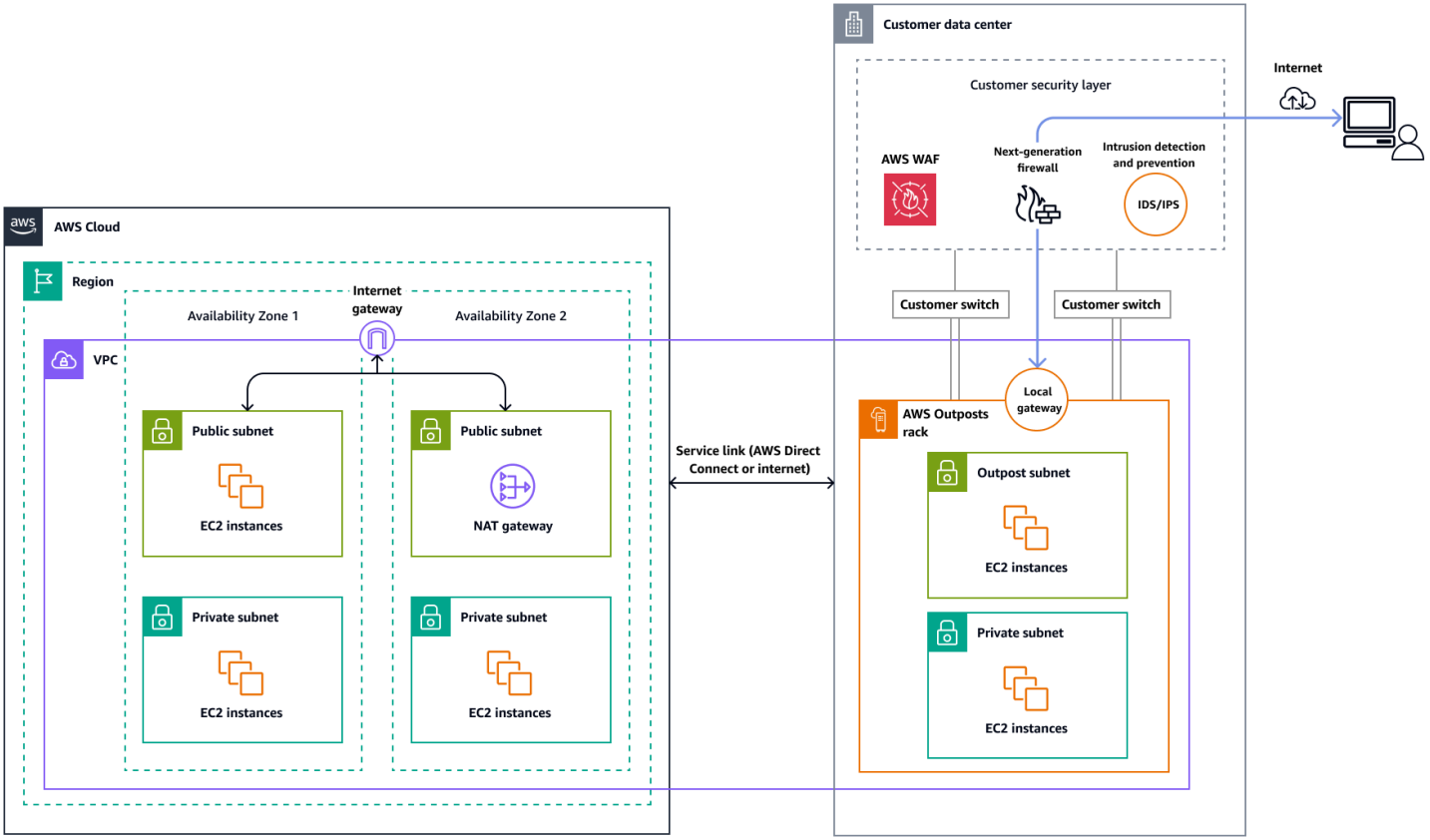
次の図は、 AWS Outposts インスタンス内のワークロードと親を通過するインターネット間のトラフィックを示しています AWS リージョン。



ローカルデータセンターのネットワーク経由のインターネットアクセス

このオプションでは、Outpost のワークロードはローカルデータセンターを介してインターネットにアクセスします。インターネットにアクセスするワークロードトラフィックは、ローカルインターネットのプレゼンスポイントを通過し、ローカルに出力されます。この場合、ローカルデータセンターのネットワークセキュリティインフラストラクチャがワークロードトラフィックの保護を担当します AWS Outposts 。

次の図は、 AWS Outposts サブネット内のワークロードと、データセンターを通過するインターネット間のトラフィックを示しています。



インフラストラクチャガバナンス

ワークロードが AWS リージョン、ローカルゾーン、または Outpost にデプロイされているかどうかにかかわらず、 インフラストラクチャガバナンス AWS Control Tower に を使用できます。 は、規範的なベストプラクティスに従って、 AWS マルチアカウント環境を設定および管理するための簡単な方法 AWS Control Tower を提供します。 は AWS Organizations、 や IAM アイデンティティセンター (すべての統合サービスを参照) など AWS のサービス、他のいくつかの の機能 AWS Control Tower を調整し AWS Service Catalogて、1 時間以内にランディングゾーンを構築します。リソースは、ユーザーに代わって設定および管理されます。

AWS Control Tower は、リージョン、ローカルゾーン (低レイテンシーの拡張機能) 、Outposts (オンプレミスインフラストラクチャ) など、すべての AWS 環境にわたって統一されたガバナンスを提供します。これにより、ハイブリッドクラウドアーキテクチャ全体で一貫したセキュリティとコンプライアンスを確保できます。詳細については、AWS Control Tower のドキュメントを参照してください。

ガードレールなどの AWS Control Tower および 機能は、政府や金融サービス機関 (FSIs) などの規制対象業界のデータレジデンシー要件に準拠するように設定できます。エッジでデータレジデンシーのガードレールをデプロイする方法については、以下を参照してください。

- ランディングゾーンコントロール AWS Local Zones を使用して のデータレジデンシーを管理するためのベストプラクティス (AWS ブログ記事)
- AWS Outposts ラックとランディングゾーンのガードレールを使用したデータレジデンシーの設計 (AWS ブログ記事)
- Hybrid Cloud Services レンズによるデータレジデンシー (AWS Well-Architected Framework ドキュメント)

Outposts リソースの共有

Outpost はデータセンターまたはコロケーションスペースに存在する有限のインフラストラクチャであるため、 を一元管理するには AWS Outposts、どのアカウント AWS Outposts リソースを共有するかを一元的に制御する必要があります。

Outpost 共有を使用すると、Outpost 所有者は Outpost サイトやサブネットを含む Outpost と Outpost リソースを、同じ組織内の他の AWS アカウント と共有できます AWS Organizations。Outpost 所有者は、Outpost リソースを一元的に作成および管理し、 AWS 組織 AWS アカウント 内の複数の 間でリソースを共有できます。これにより、他のコンシューマーは Outpost サイトを使用したり、VPC を設定したり、共有 Outpost 上でインスタンスを起動して実行したりできるようになります。

の共有可能なリソース AWS Outposts は次のとおりです。

- 割り当てられた専用ホスト
- キャパシティ予約
- お客様所有の IP (CoIP) アドレスプール
- ローカルゲートウェイルートテーブル
- Outposts
- Amazon S3 on Outposts
- サイト
- サブネット

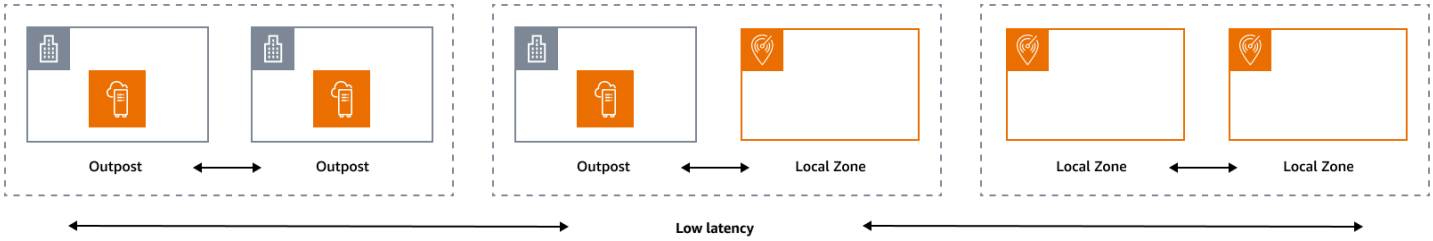
マルチアカウント環境で Outposts リソースを共有するためのベストプラクティスに従うには、次の AWS ブログ記事を参照してください。

- AWS Outposts マルチアカウント AWS 環境での共有: パート 1

- AWS Outposts マルチアカウント AWS 環境での共有: パート 2

エッジの耐障害性

信頼性の柱には、ワークロードが意図した機能を正しく一貫して実行する能力が含まれます。これには、ライフサイクルを通じてワークロードを運用およびテストする機能が含まれます。この点で、エッジで回復力のあるアーキテクチャを設計するときは、まずそのアーキテクチャのデプロイに使用するインフラストラクチャを考慮する必要があります。次の図に示すように、 AWS Local Zones と を使用して実装できる組み合わせは、Outpost AWS Outpostsから Outpost、Outpost から Local Zone、Local Zone から Local Zone の 3 つです。 AWS エッジサービスと従来のオンプレミスインフラストラクチャや を組み合わせるなど、回復力のあるアーキテクチャには他にも可能性がありますが AWS リージョン、このガイドではハイブリッドクラウドサービスの設計に適用されるこれら 3 つの組み合わせに焦点を当てています。



インフラストラクチャの考慮事項

サービス設計の中核となる原則の 1 つは AWS、基盤となる物理インフラストラクチャの単一障害点を回避することです。この原則により、 AWS ソフトウェアとシステムは複数のアベイラビリティーゾーンを使用し、1 つのゾーンの障害に対して回復力があります。エッジで、 は Local Zones と Outposts に基づくインフラストラクチャ AWS を提供します。したがって、インフラストラクチャ設計のレジリエンスを確保する上で重要な要素は、アプリケーションのリソースがデプロイされる場所を定義することです。

ローカルゾーン

ローカルゾーンは、サブネットや EC2 インスタンスなどのゾーン AWS リソースの配置場所として選択できるため AWS リージョン、 内のアベイラビリティーゾーンと同様に動作します。ただし、現在 AWS リージョン 存在しない ではなく AWS リージョン、大規模な人口、産業、IT センターの近くにあります。これにもかかわらず、ローカルゾーンのローカルワークロードと で実行されているワークロード間の高帯域幅の安全な接続は維持されます AWS リージョン。したがって、低レイテンシーの要件では、Local Zones を使用してワークロードをユーザーの近くにデプロイする必要があります。

Outposts

AWS Outposts は、 AWS インフラストラクチャ、 AWS のサービス、APIs、ツールをデータセンターに拡張するフルマネージドサービスです。で使用されているのと同じハードウェアインフラストラクチャ AWS クラウド がデータセンターにインストールされます。その後、Outposts は最も近いに接続されます AWS リージョン。Outposts を使用して、低レイテンシーまたはローカルデータ処理要件を持つワークロードをサポートできます。

親アベイラビリティーゾーン

各ローカルゾーンまたは Outpost には、親リージョン (ホームリージョンとも呼ばれます) があります。親リージョンは、 AWS エッジインフラストラクチャ (Outpost または Local Zone) のコントロールプレーンがアンカーされている場所です。Local Zones の場合、親リージョンは Local Zone の基本的なアーキテクチャコンポーネントであり、お客様が変更することはできません。 は AWS クラウド をオンプレミス環境に AWS Outposts 拡張するため、注文プロセス中に特定のリージョンとアベイラビリティーゾーンを選択する必要があります。この選択は、Outposts デプロイのコントロールプレーンを選択した AWS インフラストラクチャに固定します。

エッジで高可用性アーキテクチャを開発する場合、VPC をそれらの間で拡張できるように、Outposts や Local Zones などのこれらのインフラストラクチャの親リージョンが同じである必要があります。この拡張 VPC は、これらの高可用性アーキテクチャを作成するための基盤です。回復力の高いアーキテクチャを定義する場合は、サービスがアンカーされる (またはアンカーされる) リージョンの親リージョンとアベイラビリティーゾーンを検証する必要があります。次の図に示すように、2 つの Outposts 間に高可用性ソリューションをデプロイする場合は、2 つの異なるアベイラビリティーゾーンを選択して Outposts を固定する必要があります。これにより、コントロールプレーンの観点からマルチ AZ アーキテクチャが可能になります。1 つ以上のローカルゾーンを含む高可用性ソリューションをデプロイする場合は、まずインフラストラクチャがアンカーされている親アベイラビリティーゾーンを検証する必要があります。そのためには、次の AWS CLI コマンドを使用します。

```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

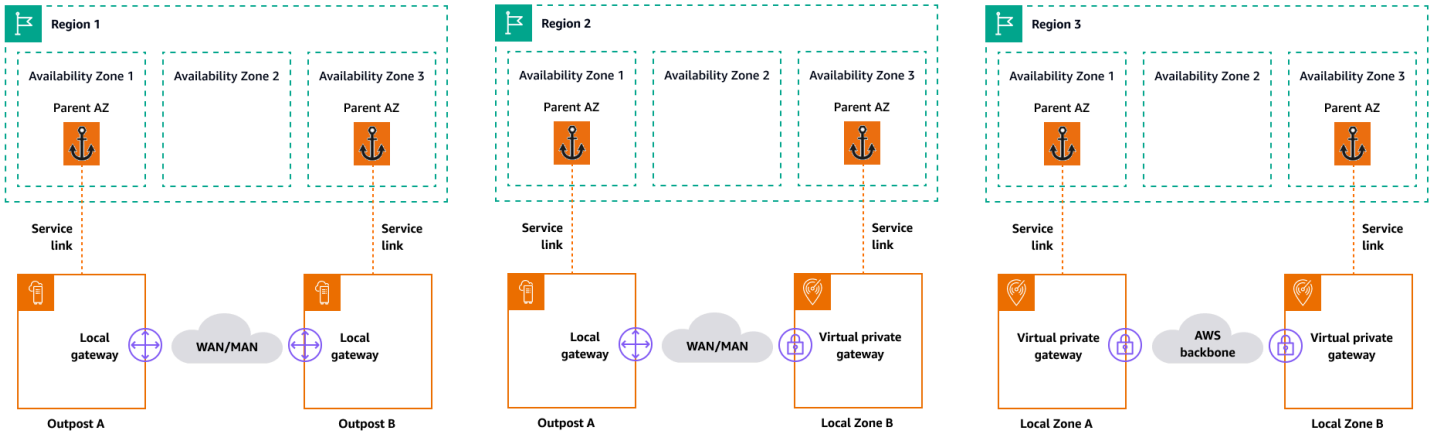
前のコマンドの出力：

```
{     "AvailabilityZones": [
          {
             "State": "available",
             "OptInStatus": "opted-in",
             "Messages": [],
```

```
            "RegionName": "us-east-1",
            "ZoneName": "us-east-1-mia-1a",
            "ZoneId": "use1-mia1-az1",
            "GroupName": "us-east-1-mia-1",
            "NetworkBorderGroup": "us-east-1-mia-1",
            "ZoneType": "local-zone",
            "ParentZoneName": "us-east-1d",
            "ParentZoneId": "use1-az2"
        }
    ]
}
```

この例では、Miami Local Zone (us-east-1d-mia-1a1) はus-east-1d-az2 アベイラビリティーゾーンに固定されています。したがって、エッジで回復力のあるアーキテクチャを作成する必要がある場合は、セカンダリインフラストラクチャ (Outposts またはローカルゾーン) が 以外のアベイラビリティーゾーンに固定されていることを確認する必要がありますus-east-1d-az2。たとえば、us-east-1d-az1は有効です。

次の図は、可用性の高いエッジインフラストラクチャの例を示しています。



ネットワークに関する考慮事項

このセクションでは、エッジでのネットワーキング、主にエッジインフラストラクチャにアクセスするための接続に関する最初の考慮事項について説明します。サービスリンクの回復力のあるネットワークを提供する有効なアーキテクチャを確認します。

ローカルゾーンの耐障害性ネットワーク

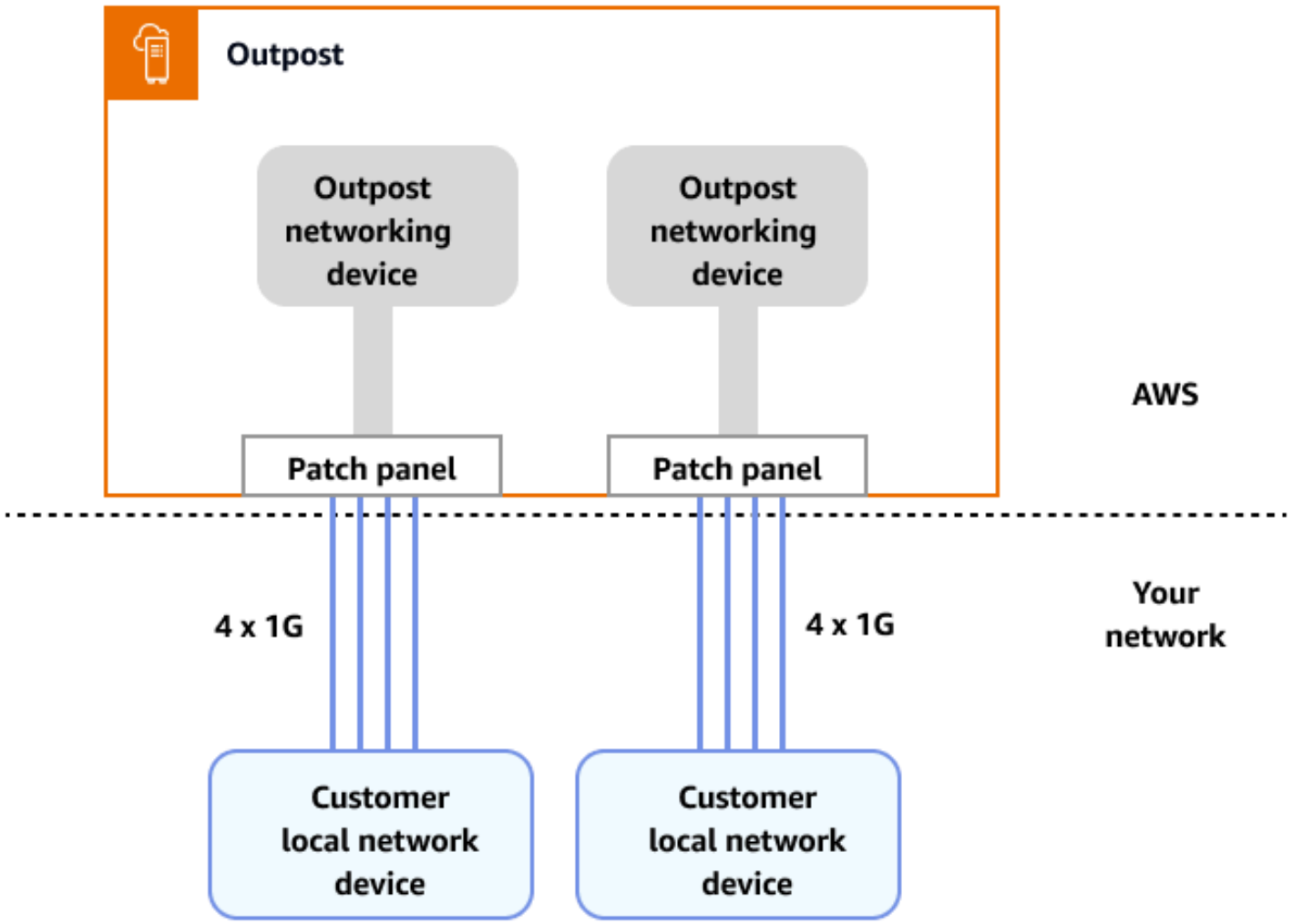
ローカルゾーンは、Amazon S3 や Amazon RDS などの任意のリージョンサービスをシームレスに使用できるようにする、複数の冗長で安全な高速リンクを使用して親リージョンに接続されます。お

客様は、オンプレミス環境またはユーザーからローカルゾーンへの接続を提供する責任があります。選択した接続アーキテクチャ (VPN や など AWS Direct Connect) に関係なく、メインリンクで障害が発生した場合にアプリケーションのパフォーマンスに影響を与えないように、ネットワークリンクを介して達成する必要があるレイテンシーは同等である必要があります。を使用している場合 AWS Direct Connect、該当する耐障害性アーキテクチャは AWS リージョン、AWS Direct Connect 耐障害性に関する推奨事項に記載されている へのアクセスアーキテクチャと同じです。ただし、主に国際ローカルゾーンに適用されるシナリオがあります。Local Zone が有効になっている国では、 AWS Direct Connect PoP が 1 つしかないため、 AWS Direct Connect レジリエンスに推奨されるアーキテクチャを作成することはできません。単一の AWS Direct Connect 場所にのみアクセスできる場合、または単一の接続を超える回復力が必要な場合は、 AWS ブログ記事「オンプレミスから への高可用性接続の有効化 AWS Local Zones」で説明されているように AWS Direct Connect、Amazon EC2 で VPN アプライアンスを作成できます。

Outposts の耐障害性ネットワーク

ローカルゾーンとは対照的に、Outposts には、ローカルネットワークから Outposts にデプロイされたワークロードにアクセスするための冗長接続があります。この冗長性は、2 つの Outposts ネットワークデバイス (ONDs。各 OND には、ローカルネットワークへの 1 Gbps、10 Gbps、40 Gbps、または 100 Gbps で少なくとも 2 つのファイバー接続が必要です。これらの接続は、スケーラブルなリンクの追加を可能にするために、リンク集約グループ (LAG) として設定する必要があります。

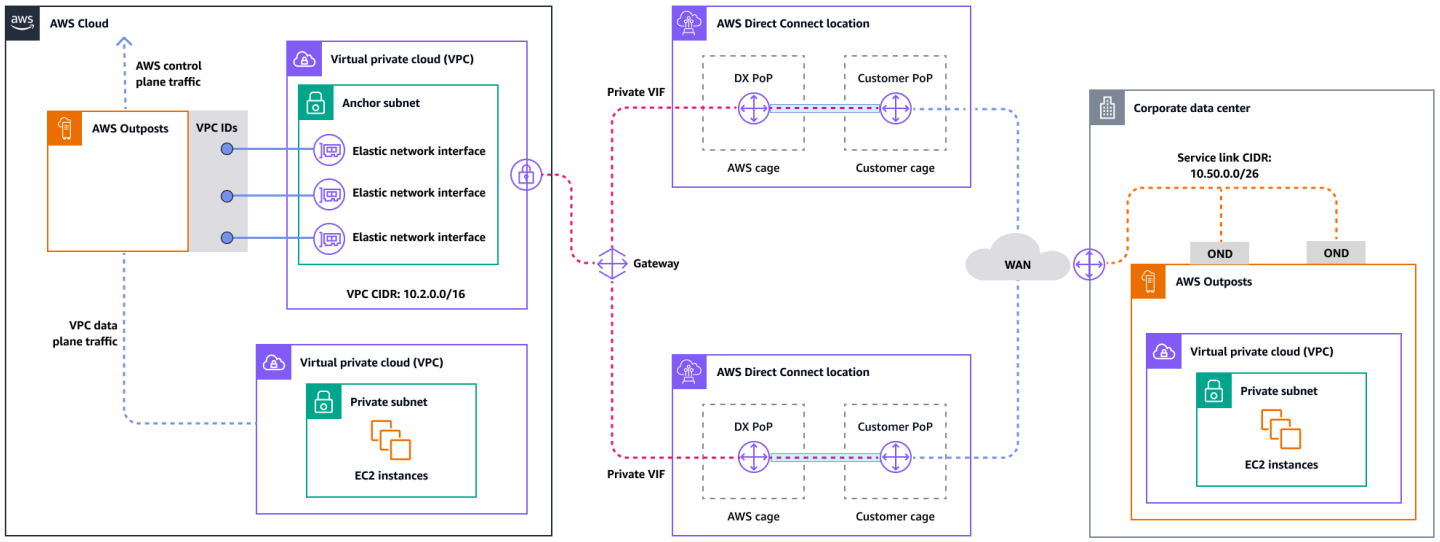
アップリンク速度	アップリンク数
1 Gbps	1、2、4、6 または 8
10 Gbps	1、2、4、8、12 または 16
40 または 100 Gbps	1、2 または 4



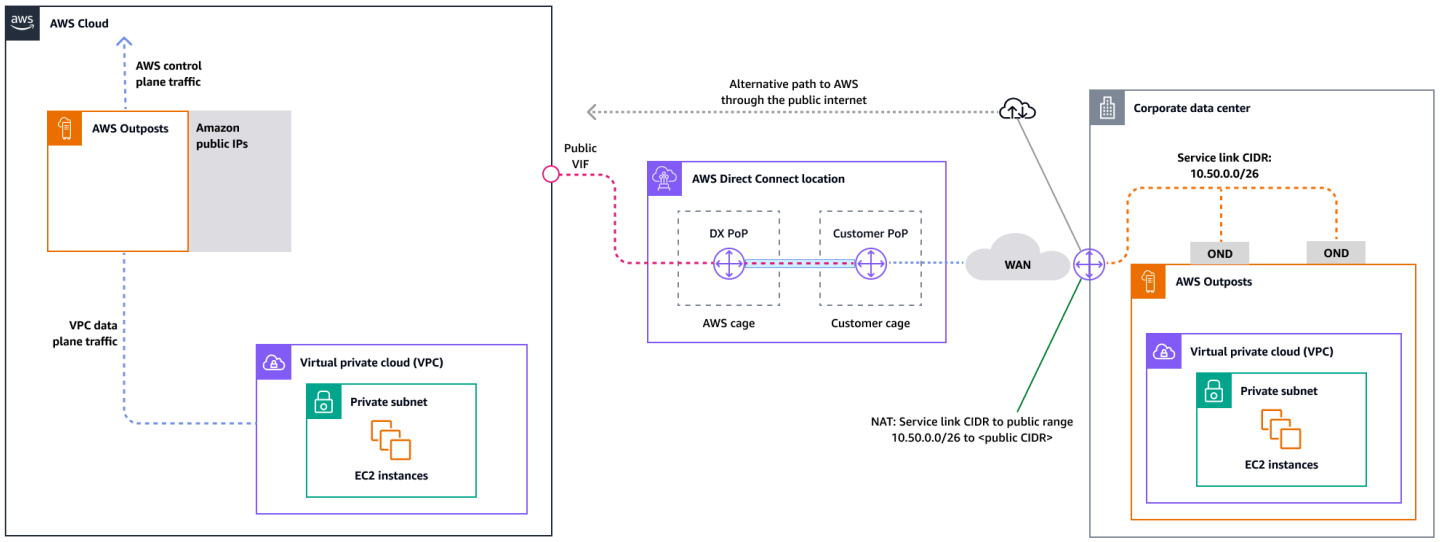
この接続の詳細については、 AWS Outposts ドキュメントの「Outposts ラックのローカルネットワーク接続」を参照してください。

最適なエクスペリエンスと回復性を実現するために、 へのサービスリンク接続には、少なくとも 500 Mbps (1 Gbps が適しています) の冗長接続を使用する AWSことをお勧めします AWS リージョン。サービスリンクには、 AWS Direct Connect または インターネット接続を使用できます。この最小値により、EC2 インスタンスの起動、EBS ボリュームのアタッチ、Amazon EKS AWS のサービス、Amazon EMR、CloudWatch メトリクスなどのアクセスが可能になります。

次の図は、高可用性プライベート接続のこのアーキテクチャを示しています。



次の図は、高可用性パブリック接続のこのアーキテクチャを示しています。



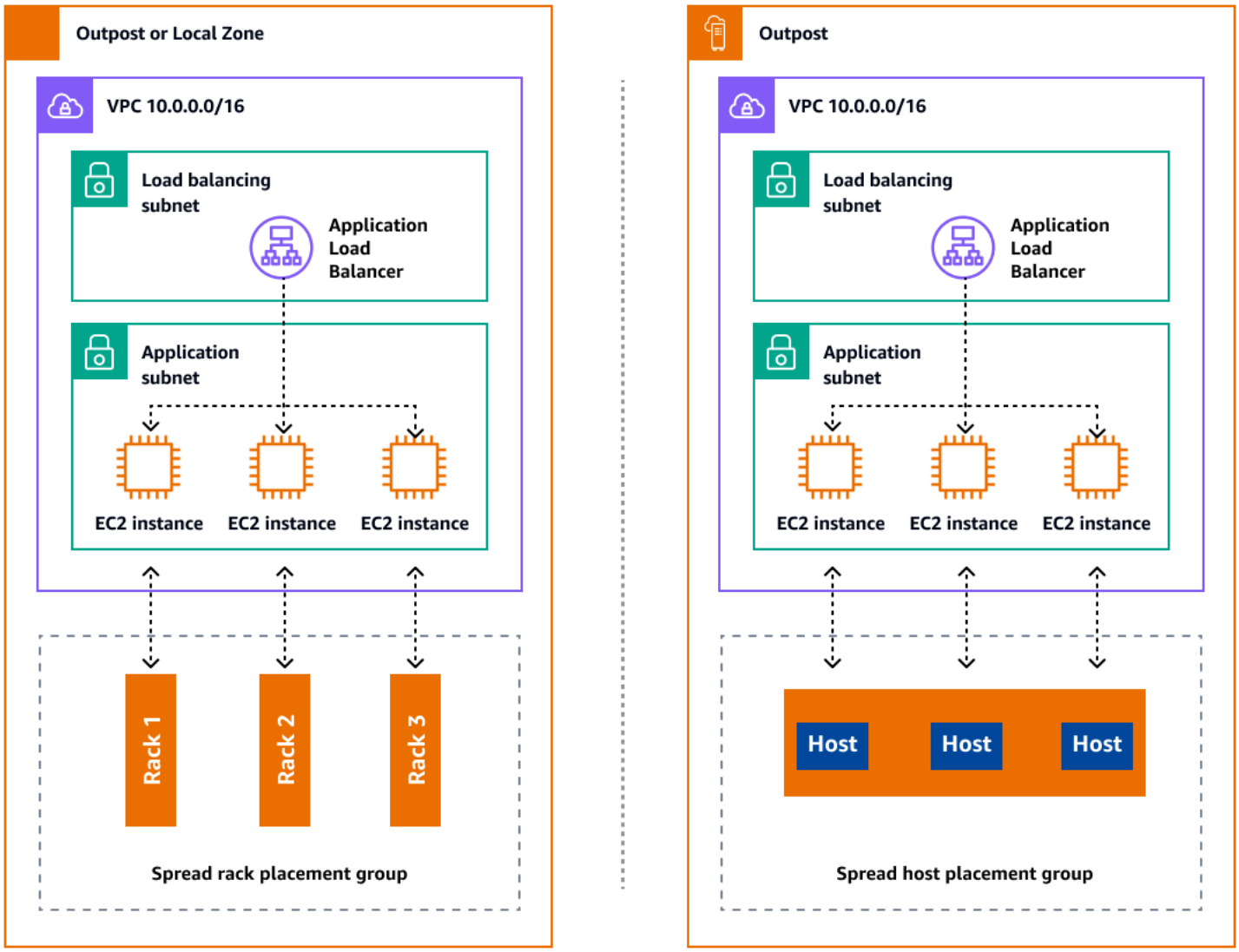
ACE ラックを使用した Outposts ラックデプロイのスケーリング

集約、コア、エッジ (ACE) ラックは、 AWS Outposts マルチラックデプロイの重要な集約ポイントとして機能し、主に 3 ラックを超えるインストールや将来の拡張を計画する場合に推奨されます。各 ACE ラックには、10 Gbps、40 Gbps、および 100 Gbps 接続をサポートする 4 つのルーターがあります (100 Gbps が最適です) 。各ラックは、冗長性を最大化するために最大 4 つのアップストリームカスタマーデバイスに接続できます。ACE ラックは最大 10 kVA の電力を消費し、重さは最大 705 ポンドです。主な利点には、物理ネットワーク要件の軽減、ファイバーケーブルアップリンクの軽減、VLAN 仮想インターフェイスの削減などがあります。 は、VPN トンネルを介してテレメトリデータを通じてこれらのラック AWS を監視し、インストール中にお客様と密接に連携して、適切な電源の可用性、ネットワーク設定、最適な配置を確保します。ACE ラックアーキテクチャは、

デプロイのスケールに応じて価値を高め、大規模なインストールにおける複雑さと物理ポート要件を軽減しながら、接続を効果的に簡素化します。 詳細については、 AWS ブログ記事「Scaling AWS Outposts rack deployments with ACE Rack」を参照してください。

Outposts とローカルゾーン間でインスタンスを分散する

Outposts と Local Zones には、有限数のコンピューティングサーバーがあります。アプリケーションが複数の関連インスタンスをデプロイする場合、これらのインスタンスは、異なる設定がない限り、同じサーバーまたは同じラック内のサーバーにデプロイされる可能性があります。デフォルトのオプションに加えて、サーバー間でインスタンスを分散して、同じインフラストラクチャで関連するインスタンスを実行するリスクを軽減できます。パーティションプレイスメントグループを使用して、複数のラックにインスタンスを分散することもできます。これはスプレッドラック分散モデルと呼ばれます。自動ディストリビューションを使用して、グループ内のパーティション間でインスタンスを分散するか、選択したターゲットパーティションにインスタンスをデプロイします。インスタンスをターゲットパーティションにデプロイすることで、ラック間で他のリソースを分散しながら、選択したリソースを同じラックにデプロイできます。Outposts には、ホストレベルでワークロードを分散できるスプレッドホストと呼ばれる別のオプションもあります。次の図は、スプレッドラックとスプレッドホストの分散オプションを示しています。



の Amazon RDS マルチ AZ AWS Outposts

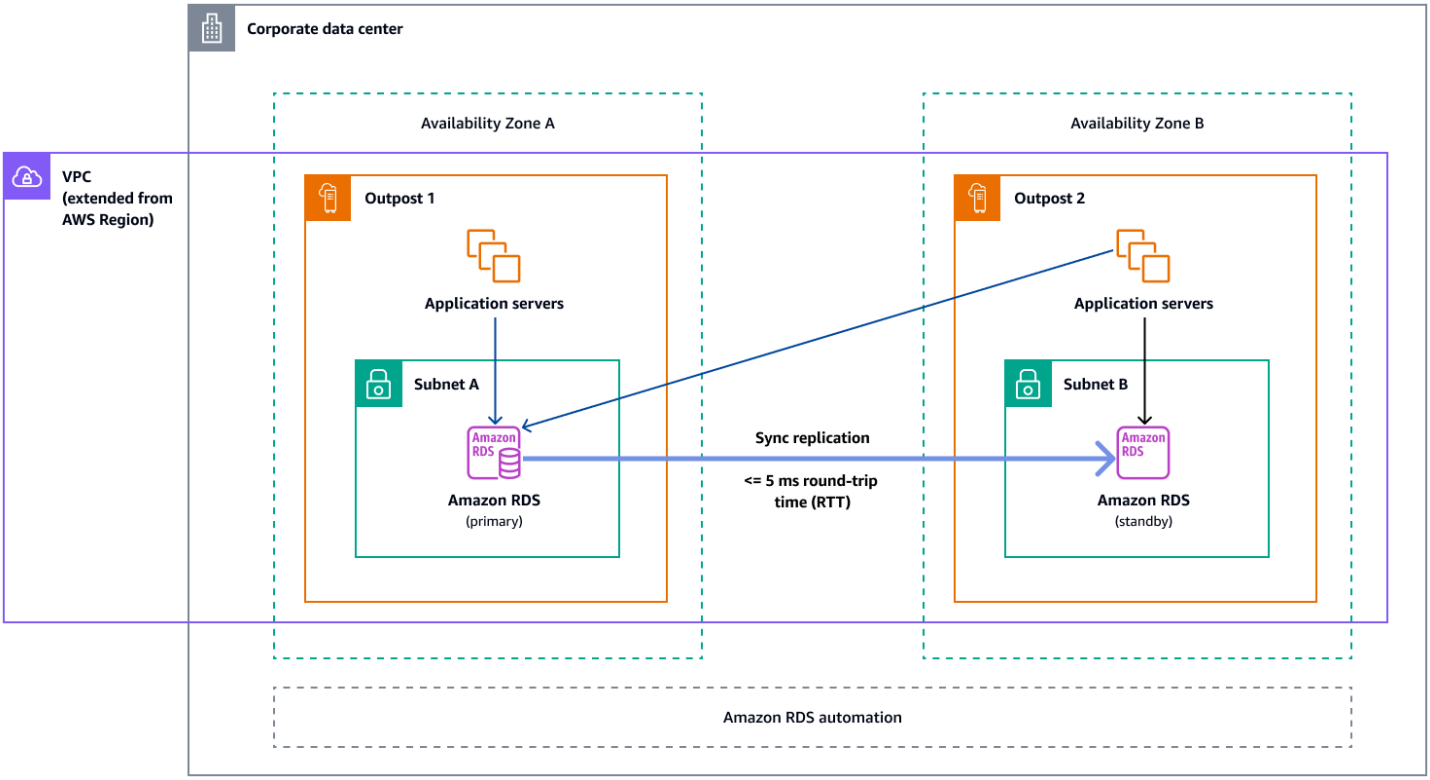
Outposts でマルチ AZ インスタンスデプロイを使用すると、Amazon RDS は 2 つの Outposts に 2 つのデータベースインスタンスを作成します。各 Outpost は独自の物理インフラストラクチャ上で動作し、高可用性のためにリージョン内の異なるアベイラビリティーゾーンに接続します。2 つの Outposts がカスタマー管理のローカル接続を介して接続されている場合、Amazon RDS はプライマリデータベースインスタンスとスタンバイデータベースインスタンス間の同期レプリケーションを管理します。ソフトウェアまたはインフラストラクチャに障害が発生した場合、Amazon RDS はスタンバイインスタンスをプライマリロールに自動的に昇格させ、新しいプライマリインスタンスを指すように DNS レコードを更新します。マルチ AZ 配置の場合、Amazon RDS はプライマリ DB インスタンスを 1 つの Outpost に作成し、別の Outpost 上にあるスタンバイ DB インスタンスにデータを

同期的にレプリケートします。Outposts でのマルチ AZ 配置は、 でのマルチ AZ 配置のように動作しますが AWS リージョン、以下の違いがあります。

- 2 つ以上の Outposts 間のローカル接続が必要です。
- 顧客所有の IP (CoIP) アドレスプールが必要です。詳細については、Amazon RDS ドキュメントの「Amazon RDS のカスタマー所有 IP アドレス AWS Outposts」を参照してください。
- レプリケーションは、ローカルネットワークで実行されます。

マルチ AZ 配置は、Amazon RDS on Outposts でサポートされているすべてのバージョンの MySQL および PostgreSQL で使用できます。ローカルバックアップは、マルチ AZ 配置ではサポートされていません。

次の図は、Amazon RDS on Outposts マルチ AZ 設定のアーキテクチャを示しています。



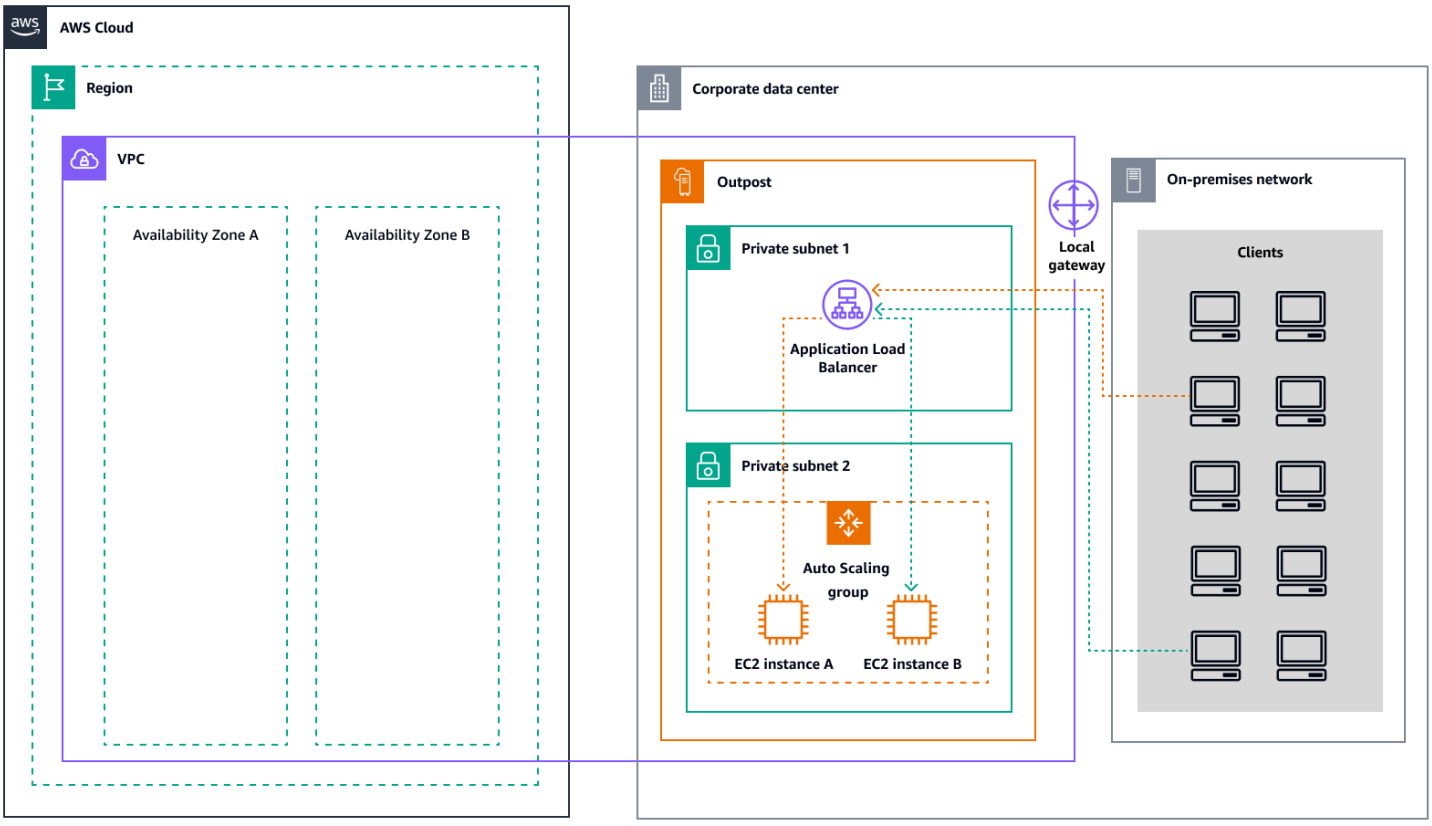
フェイルオーバーメカニズム

ロードバランシングと自動スケーリング

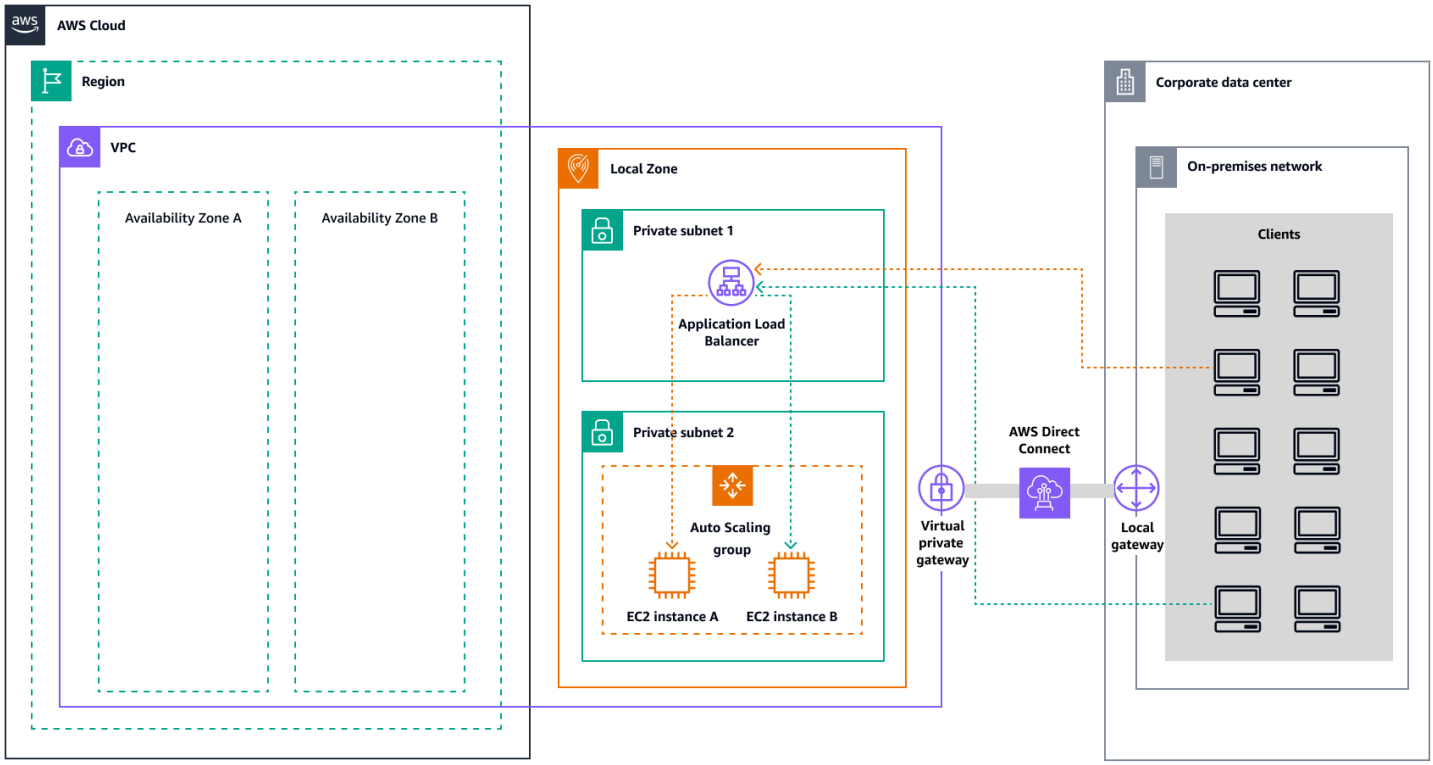
Elastic Load Balancing (ELB) は、実行中のすべての EC2 インスタンスに受信アプリケーショントラフィックを自動的に分散します。ELB は、1 つのインスタンスが過負荷にならないようにトラ

フィックを最適にルーティングすることで、受信リクエストを管理するのに役立ちます。Amazon EC2 Auto Scaling グループで ELB を使用するには、ロードバランサーを Auto Scaling グループにアタッチします。これにより、グループがロードバランサーに登録されます。ロードバランサーは、グループへのすべての受信ウェブトラフィックの単一の連絡先として機能します。Auto Scaling グループで ELB を使用する場合、個々の EC2 インスタンスをロードバランサーに登録する必要はありません。Auto Scaling グループによって起動されたインスタンスは、自動的にロードバランサーのメンバーとなります。同様に、Auto Scaling グループによって終了したインスタンスは、ロードバランサーから自動的に登録解除されます。Auto Scaling グループにロードバランサーをアタッチした後、ELB メトリクス (ターゲットあたりの Application Load Balancer リクエスト数など) を使用して、需要の変動に応じてグループ内のインスタンス数をスケールするようにグループを設定できます。必要に応じて、Auto Scaling グループに ELB ヘルスチェックを追加して、Amazon EC2 Auto Scaling がこれらのヘルスチェックに基づいて異常なインスタンスを識別して置き換えることができます。ターゲットグループの正常なホスト数が許容数を下回った場合に通知する Amazon CloudWatch アラームを作成することもできます。

次の図は、Application Load Balancer が の Amazon EC2 でワークロードを管理する方法を示しています AWS Outposts。



次の図は、ローカルゾーンでの Amazon EC2 の同様のアーキテクチャを示しています。



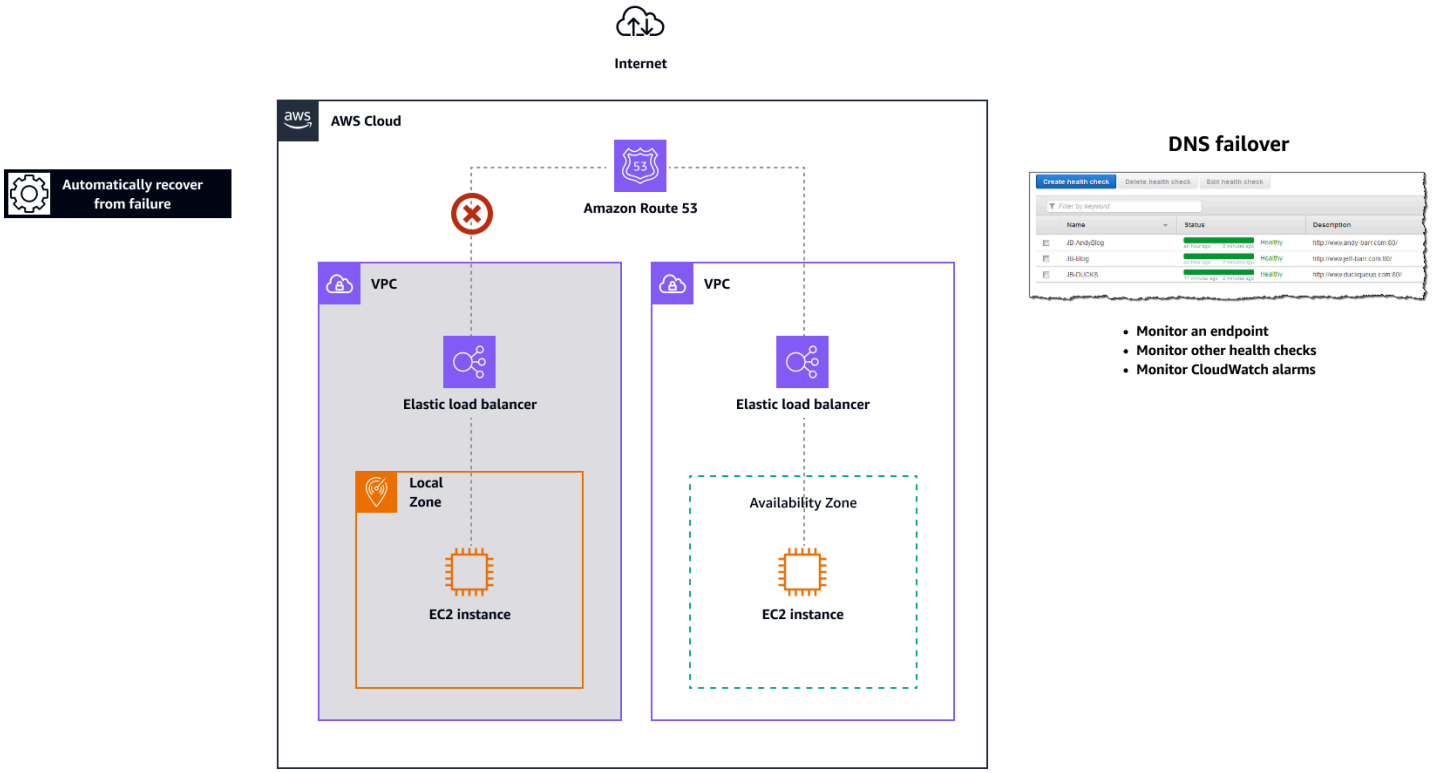
> **Note**
>
> Application Load Balancer は、 AWS Outposts と Local Zones の両方で使用できます。ただし、 で Application Load Balancer を使用するには AWS Outposts、ロードバランサーに必要なスケーラビリティを提供するために Amazon EC2 容量のサイズを設定する必要があります。でのロードバランサーのサイズ設定の詳細については AWS Outposts、 AWS ブログ記事「Configuring an Application Load Balancer on AWS Outposts」を参照してください。

Amazon Route 53 for DNS フェイルオーバー

複数の HTTP サーバーやメールサーバーなど、同じ機能を実行する複数のリソースがある場合、Amazon Route 53 を設定してリソースの正常性をチェックし、正常なリソースのみを使用して DNS クエリに応答できます。たとえば、ウェブサイト `example.com`が 2 つのサーバーでホストされていると仮定します。1 つのサーバーはローカルゾーンにあり、もう 1 つのサーバーは Outpost にあります。これらのサーバーの状態をチェックし、現在正常なサーバーのみ`example.com`を使用して の DNS クエリに応答するように Route 53 を設定できます。エイリアスレコードを使用して ELB ロードバランサーなどの選択した AWS リソースにトラフィックをルーティングする場合は、リソースの正常性を評価し、正常なリソースにのみトラフィックをルーティングするように Route 53 を設

定できます。リソースのヘルスを評価するようにエイリアスレコードを設定する場合、そのリソースのヘルスチェックを作成する必要はありません。

次の図は、Route 53 フェイルオーバーメカニズムを示しています。



注意

- プライベートホストゾーンでフェイルオーバーレコードを作成する場合は、CloudWatch メトリクスを作成し、アラームを メトリクスに関連付けてから、アラームのデータストリームに基づくヘルスチェックを作成できます。
- Application Load Balancer AWS Outposts を使用して でアプリケーションをパブリックにアクセスできるようにするには、パブリック IPs からロードバランサーの完全修飾ドメイン名 (FQDN) への宛先ネットワークアドレス変換 (DNAT) を有効にするネットワーク設定をセットアップし、公開されたパブリック IP を指すヘルスチェックを使用して Route 53 フェイルオーバールールを作成します。この組み合わせにより、Outposts がホストするアプリケーションへの信頼性の高いパブリックアクセスが保証されます。

Amazon Route 53 Resolver の AWS Outposts

Amazon Route 53 Resolver は Outposts ラックで使用できます。オンプレミスのサービスとアプリケーションに、Outposts から直接ローカル DNS 解決を提供します。ローカル Route 53 Resolver エンドポイントは、Outposts とオンプレミス DNS サーバー間の DNS 解決も有効にします。Route 53 Resolver on Outposts は、オンプレミスアプリケーションの可用性とパフォーマンスの向上に役立ちます。

Outposts の一般的なユースケースの 1 つは、工場設備、高頻度取引アプリケーション、医療診断システムなど、オンプレミスシステムへの低レイテンシーアクセスを必要とするアプリケーションをデプロイすることです。

Outposts でローカル Route 53 Resolver を使用するようにオプトインすると、親への接続が失われた場合でも、アプリケーションとサービスは引き続きローカル DNS 解決の恩恵を受け、他のサービスを検出 AWS リージョン できます。ローカルリゾルバーは、クエリ結果が Outposts からローカルにキャッシュおよび提供されるため、DNS 解決のレイテンシーを減らすのにも役立ちます。これにより、親への不要なラウンドトリップがなくなります AWS リージョン。プライベート DNS を使用する Outposts VPCs 内のアプリケーションのすべての DNS 解決はローカルで提供されます。https://docs.aws.amazon.com/managedservices/latest/userguide/set-dns.html

ローカルリゾルバーを有効にするだけでなく、この起動によりローカルリゾルバーエンドポイントも有効になります。Route 53 Resolver アウトバウンドエンドポイントを使用すると、Route 53 Resolver は DNS クエリを管理対象の DNS リゾルバーに転送できます。例えば、オンプレミスネットワーク上などです。対照的に、Route 53 Resolver インバウンドエンドポイントは、VPC の外部から受信した DNS クエリを、Outposts で実行されているリゾルバーに転送します。これにより、プライベート Outposts VPC にデプロイされたサービスの DNS クエリを、その VPC の外部から送信できます。インバウンドエンドポイントとアウトバウンドエンドポイントの詳細については、Route 53 ドキュメントの「VPC とネットワーク間の VPCs」を参照してください。

エッジでのキャパシティプランニング

キャパシティプランニングフェーズでは、アーキテクチャをデプロイするための vCPU、メモリ、ストレージ要件を収集します。AWS Well-Architected フレームワークのコスト最適化の柱では、適切なサイズ設定は計画から始まる継続的なプロセスです。ツールを使用して AWS 、 内のリソース消費に基づいて最適化を定義できます AWS。

ローカルゾーンでのエッジキャパシティプランニングは、 と同じです AWS リージョン。一部のインスタンスタイプは のタイプとは異なる可能性があるため、インスタンスが各ローカルゾーンで使用可能であることを確認する必要があります AWS リージョン。Outposts の場合、ワークロードの

要件に基づいて容量を計画する必要があります。Outposts はホストごとに固定数のインスタンスでスロットされ、必要に応じて再スロットできます。ワークロードに予備の容量が必要な場合は、容量のニーズを計画するときにそれを考慮してください。

Outposts でのキャパシティプランニング

AWS Outposts キャパシティプランニングには、リージョン別の適切なサイズ設定のための特定の入力と、アプリケーションの可用性、パフォーマンス、成長に影響するエッジ固有の要因が必要です。詳細なガイダンスについては、ホワイトペーパー「高可用性設計とアーキテクチャに関する考慮事項」の AWS 「キャパシティプランニング」を参照してください。 AWS Outposts

ローカルゾーンのキャパシティプランニング

ローカルゾーンは、地理的にユーザーに近い の拡張機能 AWS リージョン です。Local Zone で作成されたリソースは、ローカルユーザーに非常に低レイテンシーの通信を提供できます。でローカルゾーンを有効にするには AWS アカウント、 AWS ドキュメントの「 の開始方法 AWS Local Zones」を参照してください。各ローカルゾーンには、EC2 インスタンスのファミリーで使用できる異なるスロッティングがあります。各ローカルゾーンで使用できるインスタンスを使用する前に検証します。使用可能な EC2 インスタンスを確認するには、次の AWS CLI コマンドを実行します。

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

正常な出力:

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
      },
      ...
  ]
```

```
}
```

エッジインフラストラクチャ管理

AWS は、エンドユーザーやデータセンターに近い AWS インフラストラクチャ、サービス、APIs、ツールを拡張するフルマネージドサービスを提供します。Outposts および Local Zones で利用可能なサービスは、 で利用可能なサービスと同じであるため AWS リージョン、同じ AWS コンソール、AWS CLI、または AWS APIs を使用してこれらのサービスを管理できます。サポートされているサービスについては、AWS Outposts 機能比較表とAWS Local Zones 機能を参照してください。

エッジでのサービスのデプロイ

Local Zones および Outposts で使用可能なサービスは、 AWS コンソール、 AWS CLI、または AWS APIs AWS リージョンを使用して設定するのと同じ方法で設定できます。リージョンデプロイとエッジデプロイの主な違いは、リソースがプロビジョニングされるサブネットです。エッジでのネットワーキングセクションでは、サブネットが Outposts とローカルゾーンにデプロイされる方法について説明します。エッジサブネットを特定したら、エッジサブネット ID をパラメータとして使用して、サービスを Outposts または Local Zones にデプロイします。以下のセクションでは、エッジサービスをデプロイする例を示します。

エッジの Amazon EC2

次の のrun-instances例では、現在のリージョンのエッジサブネットm5.2xlargeに タイプの単一のインスタンスを起動します。Linux では SSH、Windows ではリモートデスクトッププロトコル (RDP) を使用してインスタンスに接続する予定がない場合は、キーペアはオプションです。

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

エッジの Application Load Balancer

次の のcreate-load-balancer例では、内部 Application Load Balancer を作成し、指定されたサブネットのローカルゾーンまたは Outposts を有効にします。

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internal \
```

```
    --subnets <subnet-edge-id>
```

インターネット向け Application Load Balancer を Outpost のサブネットにデプロイするには、次の例に示すように、 `--scheme`オプションで `internet-facing`フラグを設定し、CoIP プール ID を指定します。

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

エッジでの他のサービスのデプロイについては、次のリンクを参照してください。

サービス	AWS Outposts	AWS Local Zones
Amazon EKS	を使用して Amazon EKS をオンプレミスにデプロイする AWS Outposts	で低レイテンシーの EKS クラスターを起動する AWS Local Zones
Amazon ECS	での Amazon ECS AWS Outposts	共有サブネット、ローカルゾーン、および Wavelength Zones の Amazon ECS アプリケーション
Amazon RDS	での Amazon RDS AWS Outposts	ローカルゾーンサブネットを選択する
Amazon S3	Amazon S3 on Outposts の開始方法	利用不可
Amazon ElastiCache	ElastiCache での Outposts の使用	ElastiCache でのローカルゾーンの使用
Amazon EMR	の EMR クラスター AWS Outposts	の EMR クラスター AWS Local Zones
Amazon FSx	利用不可	ローカルゾーンサブネットを選択する

サービス	AWS Outposts	AWS Local Zones
AWS Elastic Disaster Recovery	AWS Elastic Disaster Recovery および の使用 AWS Outposts	利用不可
AWS Application Migration Service	利用不可	ローカルゾーンサブネットをステージングサブネットとして選択する

Outposts 固有の CLI と SDK

AWS Outposts には、サービスオーダーを作成したり、ローカルゲートウェイとローカルネットワーク間のルーティングテーブルを操作したりするためのコマンドと APIs の 2 つのグループがあります。

Outposts の注文プロセス

AWS CLI または Outposts APIs を使用して、Outposts サイトの作成、Outpost の作成、Outposts の注文の作成を行うことができます。 AWS Outposts 注文プロセス中にハイブリッドクラウドスペシャリストと協力して、リソース IDs の適切な選択と実装ニーズに最適な設定を確保することをお勧めします。完全なリソース ID リストについては、AWS Outposts 「 ラックの料金」ページを参照してください。

ローカルゲートウェイ管理

Outposts でのローカルゲートウェイ (LGW) の管理とオペレーションには、このタスクで使用できる AWS CLI および SDK コマンドに関する知識が必要です。 AWS CLI および AWS SDKs を使用して、LGW ルートを作成および変更できます。LGW の管理の詳細については、以下のリソースを参照してください。

- AWS CLI Amazon EC2 用
- の「EC2.ClientAWS SDK for Python (Boto)」
- の「Ec2ClientAWS SDK for Java」

CloudWatch メトリクスおよびログ

Outposts と Local Zones の両方で AWS のサービス 利用可能な の場合、メトリクスとログはリージョンと同じ方法で管理されます。Amazon CloudWatch は、以下のディメンションで Outposts のモニタリング専用のメトリクスを提供します。

ディメンション	説明
`Account`	容量を使用するアカウントまたはサービス
`InstanceFamily`	インスタンスファミリー
`InstanceType`	インスタンスタイプ
`OutpostId`	Outpost の ID
`VolumeType`	EBS ボリュームタイプ
`VirtualInterfaceId`	ローカルゲートウェイまたはサービスリンク仮想インターフェイス (VIF) の ID
`VirtualInterfaceGroupId`	ローカルゲートウェイ VIF の VIF グループの ID

詳細については、Outposts ドキュメントの「Outposts ラックの CloudWatch メトリクス」を参照してください。

リソース

AWS リファレンス

- でのハイブリッドクラウド AWS
- AWS Outposts Outposts ラックのユーザーガイド
- AWS Local Zones ユーザーガイド
- AWS Outposts ファミリー
- AWS Local Zones
- VPC をローカルゾーン、Wavelength Zone、または Outpost に拡張する (Amazon VPC ドキュメント)
- Local Zones の Linux インスタンス (Amazon EC2 ドキュメント)
- Outposts の Linux インスタンス (Amazon EC2 ドキュメント)
- を使用した低レイテンシーアプリケーションのデプロイの開始 AWS Local Zones (チュートリアル)

AWS ブログ投稿

- Amazon EC2 を使用してオンプレミスで AWS インフラストラクチャを実行する
- Amazon EC2 での Amazon EKS を使用した最新のアプリケーションの構築
- Amazon EC2 ラックで CoIP とダイレクト VPC のルーティングモードを選択する方法
- Amazon EC2 のネットワークスイッチの選択
- でのデータのローカルコピーの維持 AWS Local Zones
- Amazon EC2 での Amazon ECS
- Amazon EKS for によるエッジ対応サービスメッシュの管理 AWS Local Zones
- Amazon EC2 でのローカルゲートウェイ進入ルーティングのデプロイ
- でのワークロードのデプロイの自動化 AWS Local Zones
- マルチアカウント AWS 環境での Amazon EC2 の共有: パート 1
- マルチアカウント AWS 環境での Amazon EC2 の共有: パート 2
- AWS Direct Connect および AWS Local Zones 相互運用性パターン
- マルチ AZ 高可用性を使用して Amazon EC2 に Amazon RDS をデプロイする

寄稿者

以下の個人がこのガイドに貢献しました。

オーサリング

- プリンシパルハイブリッドクラウドソリューションアーキテクト、レオナルド・ソラーノ AWS
- Len Gomes、パートナーソリューションアーキテクト、 AWS
- Matt Price、シニアエンタープライズサポートエンジニア、 AWS
- Tom Gadomski、ソリューションアーキテクト、 AWS
- Obed Gutierrez、ソリューションアーキテクト、 AWS
- Dionysios Kakaletris、テクニカルアカウントマネージャー、 AWS
- Vamsi Krishna、プリンシパル Outposts スペシャリスト、 AWS

の確認

- David Filiatrault、デリバリーコンサルタント、 AWS

テクニカルライティング

- Handan Selamoglu、シニアドキュメントマネージャー、 AWS

ドキュメント履歴

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

変更	説明	日付
初版発行	—	2025 年 6 月 10 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範ガイダンスによって提供される戦略、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します。
- 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: オンプレミスの Oracle データベースを の Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 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: カスタマーリレーションシップ管理 (CRM) システムを Salesforce.com に移行します。
- 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: オンプレミスの Oracle データベースを の EC2 インスタンス上の Oracle に移行します AWS クラウド。
- 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。

- 使用停止 — 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コントロール」を参照してください。

抽象化されたサービス

「マネージドサービス」を参照してください。

ACID

アトミック性、一貫性、分離性、耐久性を参照してください。

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。より柔軟ですが、アクティブ/パッシブ移行よりも多くの作業が必要です。

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が同期されるデータベース移行方法。ただし、ソースデータベースのみが、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、接続アプリケーションからのトランザクションを処理します。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

行のグループで動作し、グループの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 などがありま`MAX`す。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

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。

アプリケーションコントロール

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 の需要要素であり、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?」を参照してください。

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

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。 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整理しています。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

個人や組織を混乱させたり、損害を与えたりすることを意図したボット。

BCP

事業継続計画を参照してください。

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Data in a behavior graph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。エンディアン性も参照してください。

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

2 つの異なる同一の環境を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は 1 つの環境 (青) で実行し、新しいアプリケーションバージョンは別の環境 (緑) 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、ボットハーダーまたはボットオペレーターとして知られる 1 人の当事者が管理しているボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

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、 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 AWS 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、ホワイトペーパー AWSでのコンテナ化されたマイクロサービスの実行 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。

Canary デプロイ

エンドユーザーへのバージョンのスローリリースと増分リリース。確信できたら、新しいバージョンをデプロイし、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

「データキャプチャの変更」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します。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 を受信する前のローカルでのデータの暗号化。

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テクノロジー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 に移行するときに通常実行する 4 つのフェーズ AWS クラウド :

- 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

「設定管理データベース」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または が含まれますBitbucket Cloud。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などのビジュアル形式から情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI は CV 用の画像処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定が想定状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

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

一元管理とガバナンスを備えた分散型の分散型データ所有権を提供す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、通常、大量の履歴データが含まれており、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る。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。

ディープラーニング

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。この戦略を採用するときは AWS、 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て、リソースの安全性を確保します。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。

デプロイ

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、Implementing security controls on AWSのDetective controls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

スタースキーマでは、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する

離散数値です。これらの属性は、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一般的に使用されます。

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)

災害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に使用する戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 Disaster Recovery of Workloads on AWS: Recovery in the Cloud」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

「開発値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、応答時間を短縮できます。

電子データ交換 (EDI)

組織間の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プロセス。

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。たとえば、 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

星スキーマの中央テーブル。事業運営に関する量的データを保存します。通常、ファクトテーブルには、メジャーを含む列とディメンションテーブルへの外部キーを含む列の 2 つのタイプの列が含まれます。

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で段階的なテストを使用する哲学。これはアジャイルアプローチの重要な部分です。

障害分離の境界

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

同様のタスクの実行を求める前に、タスクと必要な出力を示す少数の例を LLM に提供します。この手法は、プロンプトに埋め込まれた例 (ショット) からモデルが学習するコンテキスト内学習のアプリケーションです。少数ショットプロンプトは、特定のフォーマット、推論、またはドメインの知識を必要とする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コントロール」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

段階的なアプローチを使用する代わりに、変更データキャプチャによる継続的なデータレプリケーションを使用して、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)

一般化およびラベル付けされていないデータの大規模なデータセットでトレーニングされている大規模な深層学習ニューラルネットワーク。FMs は、言語の理解、テキストと画像の生成、自然言語の会話など、さまざまな一般的なタスクを実行できます。詳細については、「基盤モデルとは」を参照してください。

G

生成 AI

大量のデータでトレーニングされ、シンプルなテキストプロンプトを使用してイメージ、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る AI モデルのサブセット。詳細については、「生成 AI とは」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 ワークフローはレガシーと見なされ、[トランクベースのワークフロー]はモダンで推奨されるアプローチです。

ゴールデンイメージ

そのシステムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、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、、 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。

ハイアベイラビリティ (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に使用されるデータセットから保留される、ラベル付きの履歴データの一部。モデル予測をホールドアウトデータと比較することで、ホールドアウトデータを使用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

「産業用モノのインターネット」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

既存のインフラストラクチャを更新、パッチ適用、または変更する代わりに、本番環境のワークロード用に新しいインフラストラクチャをデプロイするモデル。イミュータブルインフラストラクチャは、本質的に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、予測性が高くなります。詳細については、 AWS 「 Well-Architected フレームワーク」の「イミュータブルインフラストラクチャを使用したデプロイ」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 によって導入された用語で、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ゼーションを指します。

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。

産業分野における 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、「Building an industrial Internet of Things (IIoT) digital transformation strategy」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。

モノのインターネット (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

「モノのインターネット」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)

大量のデータに対して事前トレーニングされた深層学習 AI モデル。LLM は、質問への回答、ドキュメントの要約、テキストの他の言語への翻訳、文の完了など、複数のタスクを実行できます。詳細については、LLMs」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

「ラベルベースのアクセスコントロール」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。エンディアン性も参照してください。

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または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、不正アクセスにつながる可能性があります。マルウェアの例としては、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。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、マネージドサービスの例です。これら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)

原材料を工場の完成製品に変換する生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステム。

MAP

「移行促進プログラム」を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整を行うために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化して改善するサイクルです。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 を除くすべて 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。

メッセージキューイングテレメトリトランスポート (MQTT)

リソースに制約のある IoT デバイス用の、パブリッシュ/サブスクライブパターンに基づく軽量 machine-to-machine (M2M) 通信プロトコル。

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)

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。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 に移行するために使用するアプローチ AWS クラウド。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、「」の「アプリケーションをモダナイズするための戦略 AWS クラウド」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、『』の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」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

「移行ポートフォリオ評価」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。

ミュータブルインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。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

「オリジンアクセスコントロール」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

「 オペレーションの統合」を参照してください。

OLA

「運用レベルの契約」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。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

産業用オートメーション用のmachine-to-machine (M2M) 通信プロトコル。OPC-UA は、データの暗号化、認証、認可スキームとの相互運用性標準を提供します。

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)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問とそれに関連するベストプラクティスのチェックリスト。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するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 変換の主な焦点です。

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。

オリジンアクセスコントロール (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コントロールが可能です。

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

「プログラム可能な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

アクセス許可を定義 (アイデンティティベースのポリシーを参照)、アクセス条件を指定 (リソースベースのポリシーを参照)、または の組織内のすべてのアカウントに対する最大アクセス許可を定義 AWS Organizations （ サービスコントロールポリシーを参照) できるオブジェクト。

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。詳細については、マイクロサービスでのデータ永続性の有効化 を参照してください。

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、「移行準備状況ガイド」を参照してください。

述語

`true` または を返すクエリ条件。一般的に`false`は `WHERE`句にあります。

述語プッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得して処理する必要があるデータの量が減少し、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、Implementing security controls on AWSのPreventative controls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内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じてプライバシーを考慮するシステムエンジニアリングアプローチ。

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

非準拠のリソースのデプロイを防ぐ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、プロビジョニングされる前にリソースをスキャンします。リソースがコントロールに準拠していない場合、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)

設計、開発、発売から成長と成熟まで、製品のデータとプロセスのライフサイクル全体にわたる管理。

本番環境

「環境」を参照してください。

プログラム可能なロジックコントローラー (PLC)

製造では、マシンをモニタリングし、製造プロセスを自動化する、信頼性の高い適応可能なコンピュータです。

プロンプトの連鎖

1 つの LLM プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、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善または拡張したりするために使用されます。これにより、モデルのレスポンスの精度と関連性が向上し、より詳細でパーソナライズされた結果が得られます。

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。

パブリッシュ/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。スケーラビリティと応答性を向上させます。たとえば、マイクロサービスベースの MES では、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できるチャネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

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る手順などの一連のステップ。

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

責任、説明責任、相談、情報 (RACI) を参照してください。

RAG

「取得拡張生成」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

責任、説明責任、相談、情報 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」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。

再設計

「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 とは独立しています。詳細については、AWS リージョン「アカウントで使用できる を指定する」を参照してください。

回帰

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。

プラットフォーム変更

「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

中断に抵抗または回復するアプリケーションの機能。高可用性とディザスタリカバリは、 で回復性を計画する際の一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド「レジリエンス」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。サポートを含めると、そのマトリックスは RASCI マトリックスと呼ばれ、サポートを除外すると 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、Implementing security controls on AWSのResponsive controls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。

取得拡張生成 (RAG)

LLM がレスポンスを生成する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を参照する生成 AI テクノロジー。たとえば、RAG モデルは、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する場合があります。詳細については、「RAG とは」を参照してください。

ローテーション

攻撃者が認証情報にアクセスすることをより困難にするために、シークレットを定期的に更新するプロセス。

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 Management Console 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

「監視コントロールとデータ取得」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 AWS Secrets Managerパスワードやユーザー認証情報などの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。シークレット値は、バイナリ、単一の文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

設計によるセキュリティ

開発プロセス全体でセキュリティを考慮するシステムエンジニアリングアプローチ。

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、予防的、検出的、応答的、プロアクティブの 4 つの主なタイプがあります。

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に自動的に応答または修復するように設計された、事前定義された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。自動応答アクションの例としては、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、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

サービスレベルのインジケータによって測定される、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

セキュリティ情報とイベント管理システムを参照してください。

単一障害点 (SPOF)

システムを中断する可能性のあるアプリケーションの 1 つの重要なコンポーネントの障害。

SLA

「サービスレベルの契約」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、『』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 AWS クラウド」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

1 つの大きなファクトテーブルを使用してトランザクションデータまたは測定データを保存し、1 つ以上の小さなディメンションテーブルを使用してデータ属性を保存するデータベース組織構造。この構造は、データウェアハウスまたはビジネスインテリジェンスの目的で使用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。

監視制御とデータ収集 (SCADA)

製造では、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稼働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潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用して、これらのテストを作成できます。

システムプロンプト

LLM にコンテキスト、指示、またはガイドラインを提供して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、ユーザーとのやり取りのルールを確立するのに役立ちます。

T

tags

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 枚のピザで養う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。詳細については、深層学習システムにおける不確実性の定量化 ガイドを参照してください。

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 ピアリング接続

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する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどの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 「ワークロード認定フレームワーク」を参照してください。

Write Once, Read Many (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。承認されたユーザーは、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

ゼロデイ脆弱性を利用する攻撃、通常はマルウェア。

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 にタスクを実行する手順を提供しますが、タスクのガイドに役立つ例 (ショット) はありません。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。