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

Amazon Web Services (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、多くの組織は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

前提条件と制限事項

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 で工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。
- AWS Outposts への接続 AWS リージョンには、インターネットまたは 500 Mbps (1 Gbps 以上が適しています) 以上の AWS Direct Connect リンクが提供され、維持されている必要があります。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。からリージョン AWS Outposts へのラウンドトリップタイムレイテンシーは、最大 175 ミリ秒である必要があります。
- AWS エンタープライズサポートまたはAWS 統合オペレーションプランの有効な契約が必要です。

AWS Local Zones

- AWS ローカルゾーンは、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 Direct Connect からローカルゾーンに最も近い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。

制限事項

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。Amazon RDS on AWS Outposts 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 と Amazon S3 の違い」で説明されています。 Amazon S3 on Outposts ユーザーガイドの セクション。
- 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。
- インスタンス容量ツールは、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、 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 のフィーチャー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 アーキテクチャについて

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。

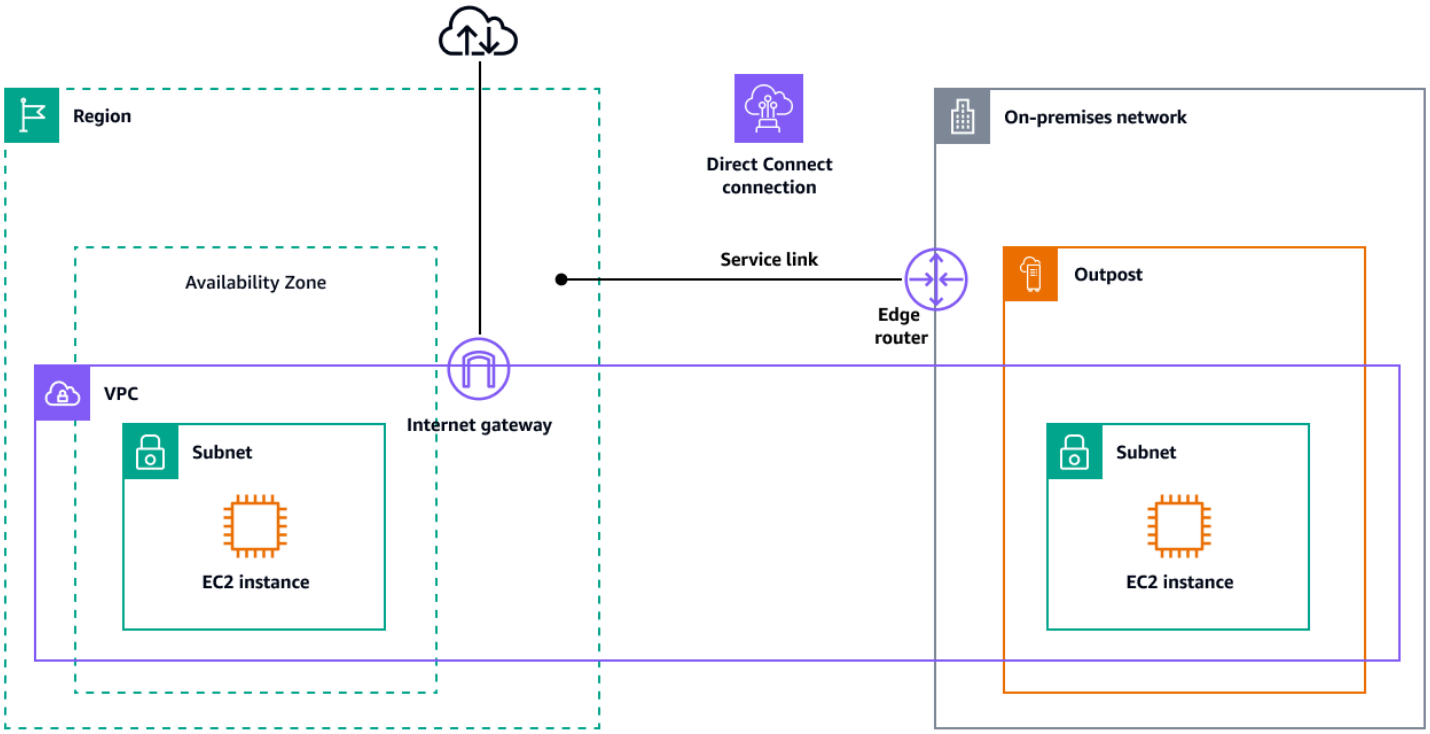
Edge からリージョンへのトラフィック

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ますが、 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 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 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。



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。データ依存が大きいほど、リンク帯域幅は大きくなります。

帯域幅の要件は、以下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。Local Zones 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、すべてのリージョン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
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。

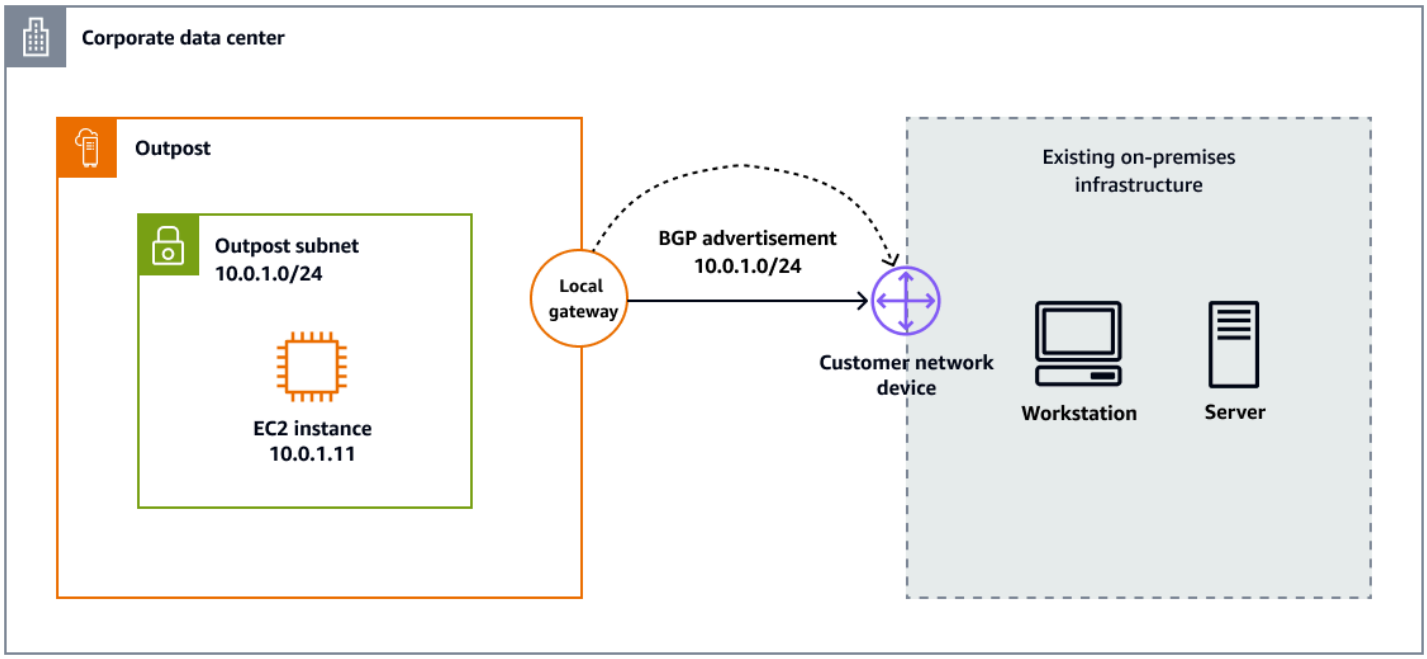
Edge からオンプレミスへのトラフィック

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。

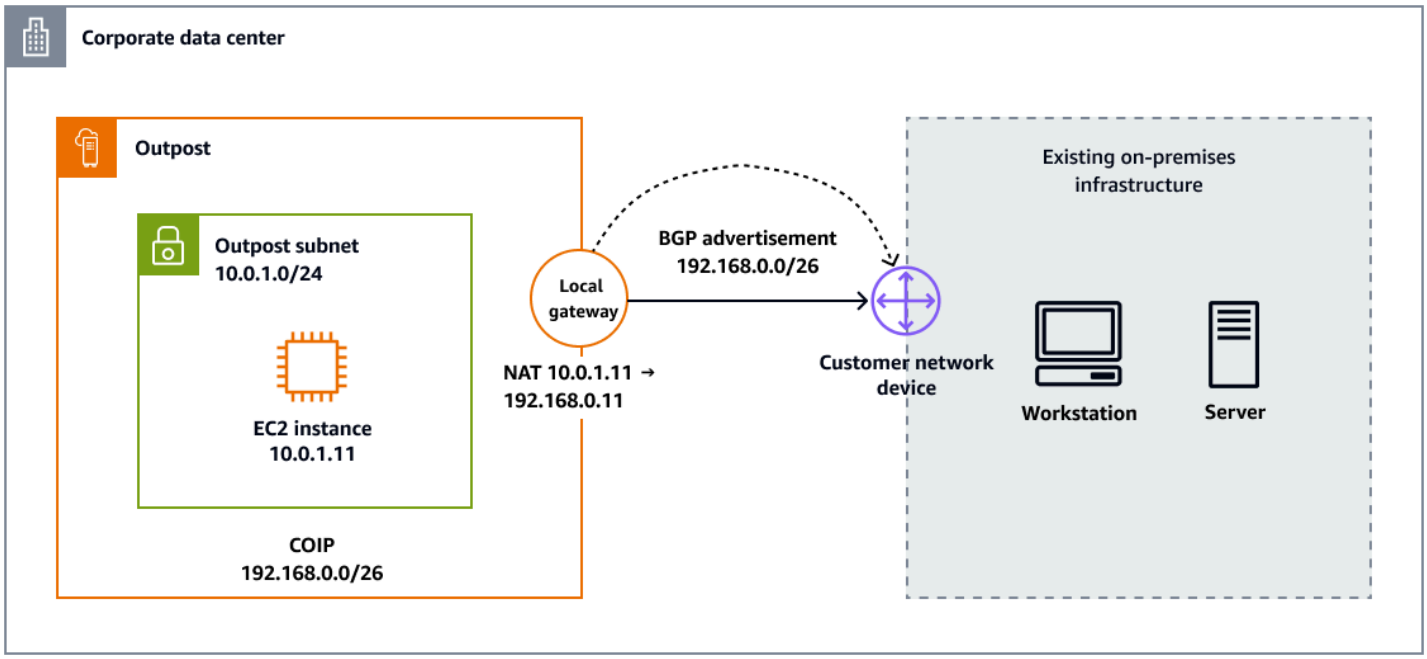
AWS Outposts ローカルゲートウェイ

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、Local Zones 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に、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 Direct Connect

ローカルゾーンは もサポートしているため 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、親リージョンをヘアピンしません。

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、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 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。 は、お客様が安全に使用できるサービス AWS 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 アイデンティティセンター。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。Outpost ラックのデータを復号するには、NSK が必要です。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。

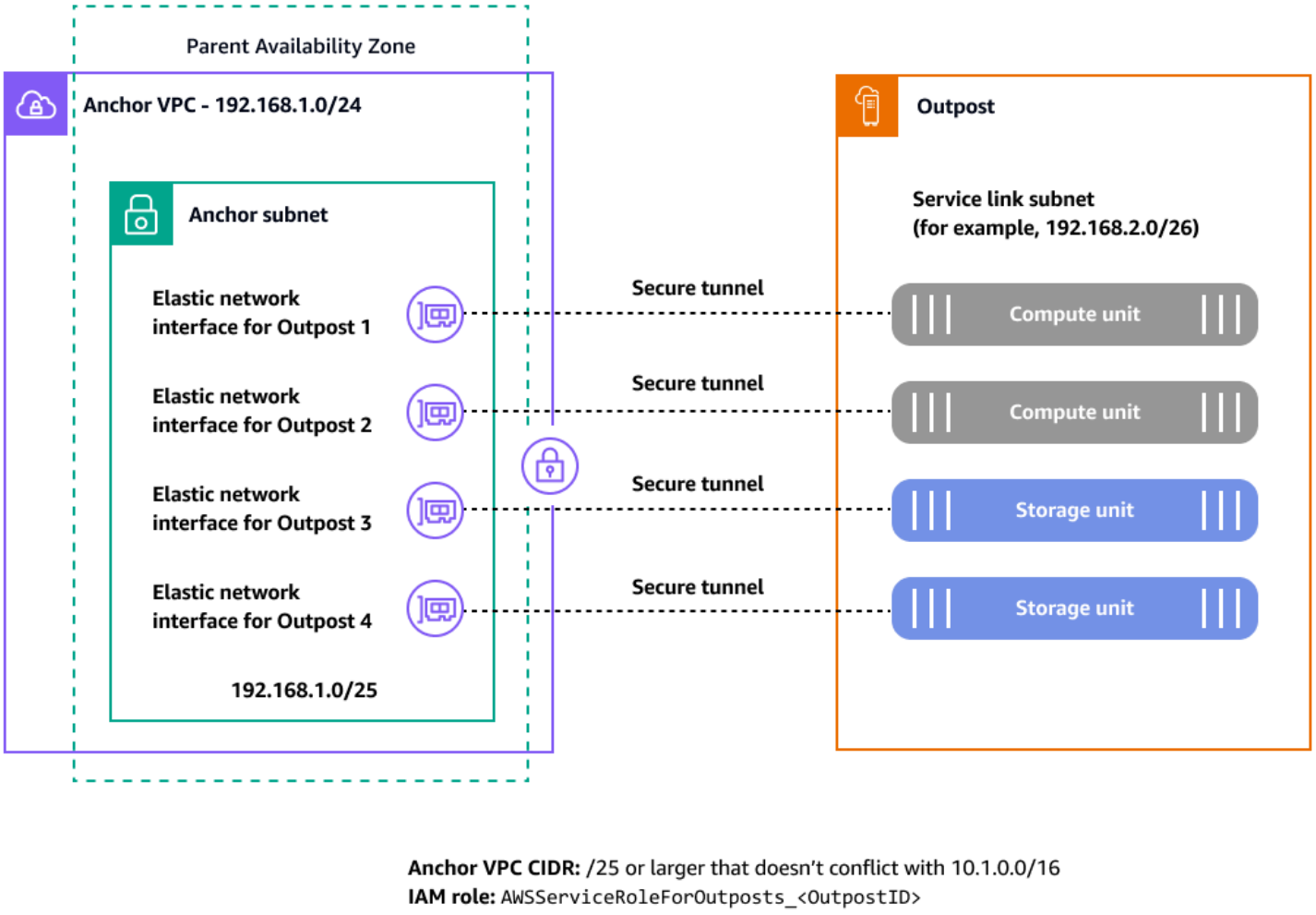
> **Note**
>
> Amazon S3 on Outposts は、KMS キーによるサーバー側の暗号化 (SSE-KMS) をサポートしていません。

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 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。

次の図に示すように AWS リージョン、 AWS Outposts サービスリンクは、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。

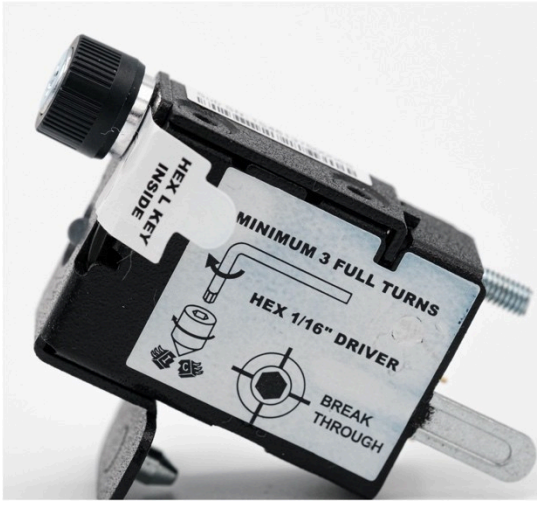
[プロトコル]	ソースポート	送信元アドレス	送信先ポート	送信先アドレス
UDP	443	AWS Outposts サービスリンク /26	443	AWS Outposts リージョンのパブリックルート

[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 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 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 でデータを暗号化的にシュレッダーします。



ID とアクセス管理

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のポリシー	あり
リソースベースのポリシー	はい*
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
アクセスコントロールリスト (ACL)	いいえ
属性ベースのアクセスコントロール (ABAC) (ポリシーのタグ)	はい
一時的な認証情報	あり

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

* 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の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、同様の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による潜在的な影響範囲も縮小されます。

- 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、設定とオペレーションの自動化、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。

キー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、外部で消費される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、リージョンか

らのインターネット消費を、外部の Git リポジトリへのパッチ適用、更新、アクセス AWS、および同様のシナリオにのみ使用できる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では 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。

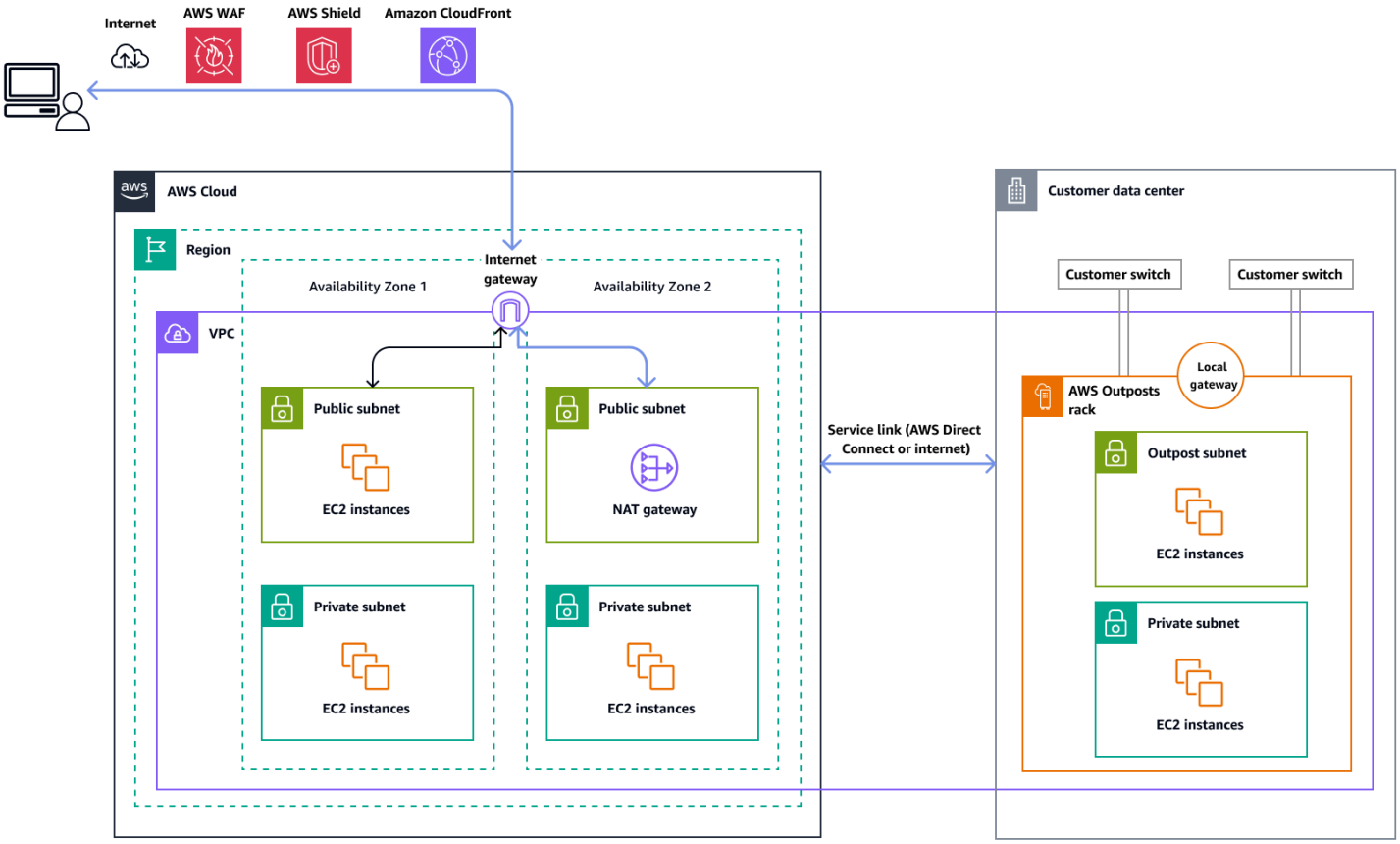
Local Zones は、ネットワーク境界グループと呼ばれるネットワーク構造を採用します AWS リージョン。この境界グループは、これらの一意のグループのパブリック IP アドレスを AWS アドバタイズします。ネットワーク境界グループは、アベイラビリティーゾーン、ローカルゾーン、または Wavelength Zones で構成されます。ネットワーク境界グループで使用するパブリック IP アドレスのプールを明示的に割り当てることができます。ネットワーク境界グループを使用して、Elastic IP アドレスをグループから提供できるようにすることで、インターネットゲートウェイをローカルゾーンに拡張できます。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 AWS Local Zones で説明されているように、Local Zone で検査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。

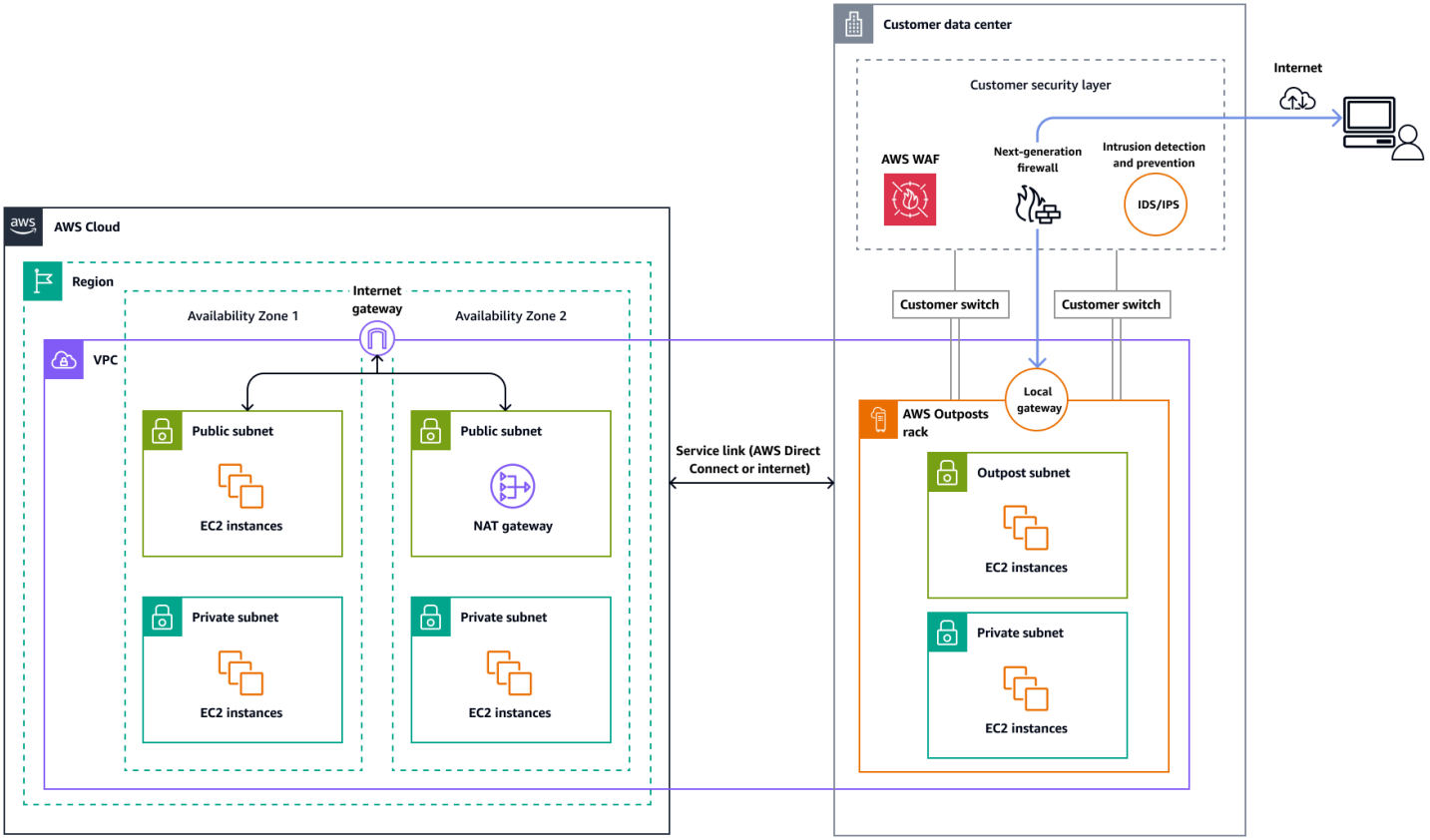
次の図は、 AWS Outposts インスタンス内のワークロードと親を通過するインターネット間のトラフィックを示しています AWS リージョン。



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 Identity Center (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 環境で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、 の一元管理を行うには AWS Outposts、どのアカウント AWS Outposts リソースを共有するかを一元管理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

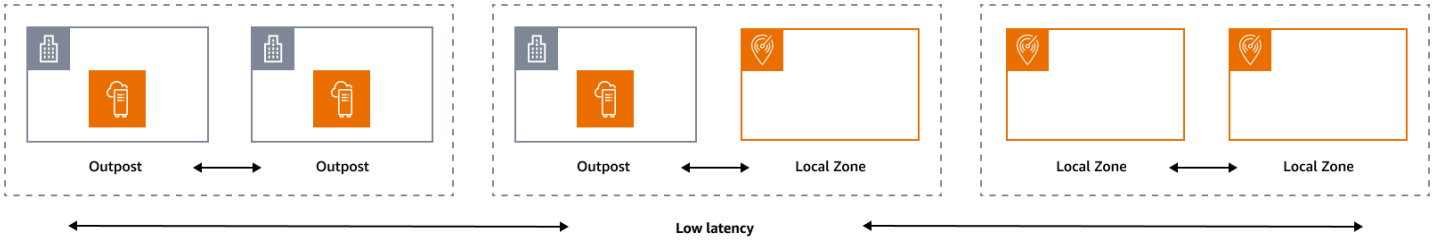
マルチアカウント環境で Outposts リソースを共有するためのベストプラクティスに従うには、次の AWS ブログ記事を参照してください。

- 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。それにもかかわらず、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、ローカルゾーン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。この選択により、Outposts デプロイのコントロールプレーンが選択した AWS インフラストラクチャに固定されます。

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
```

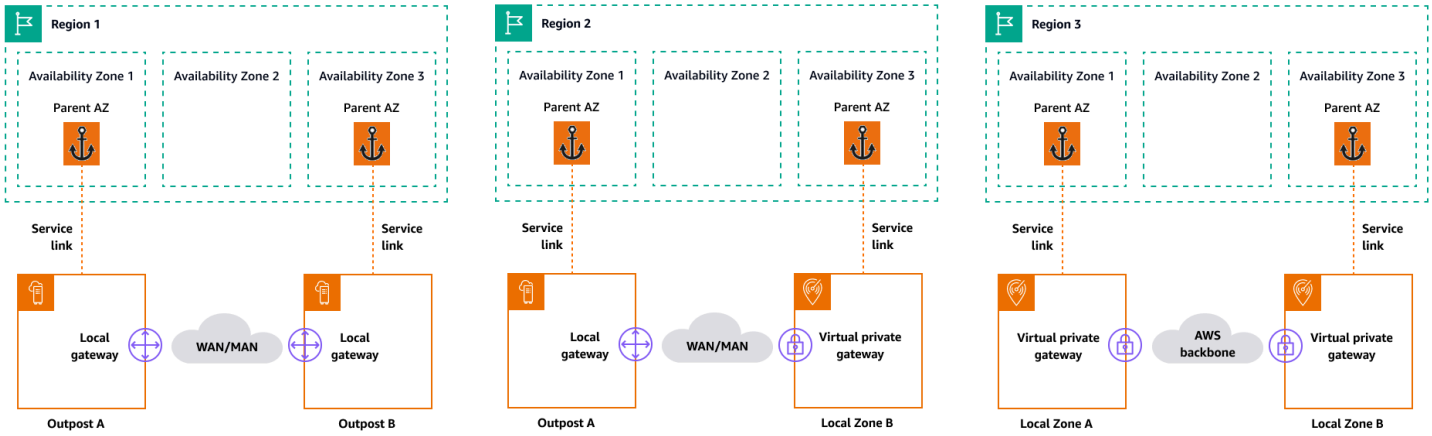
前のコマンドの出力:

```
{     "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ク、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

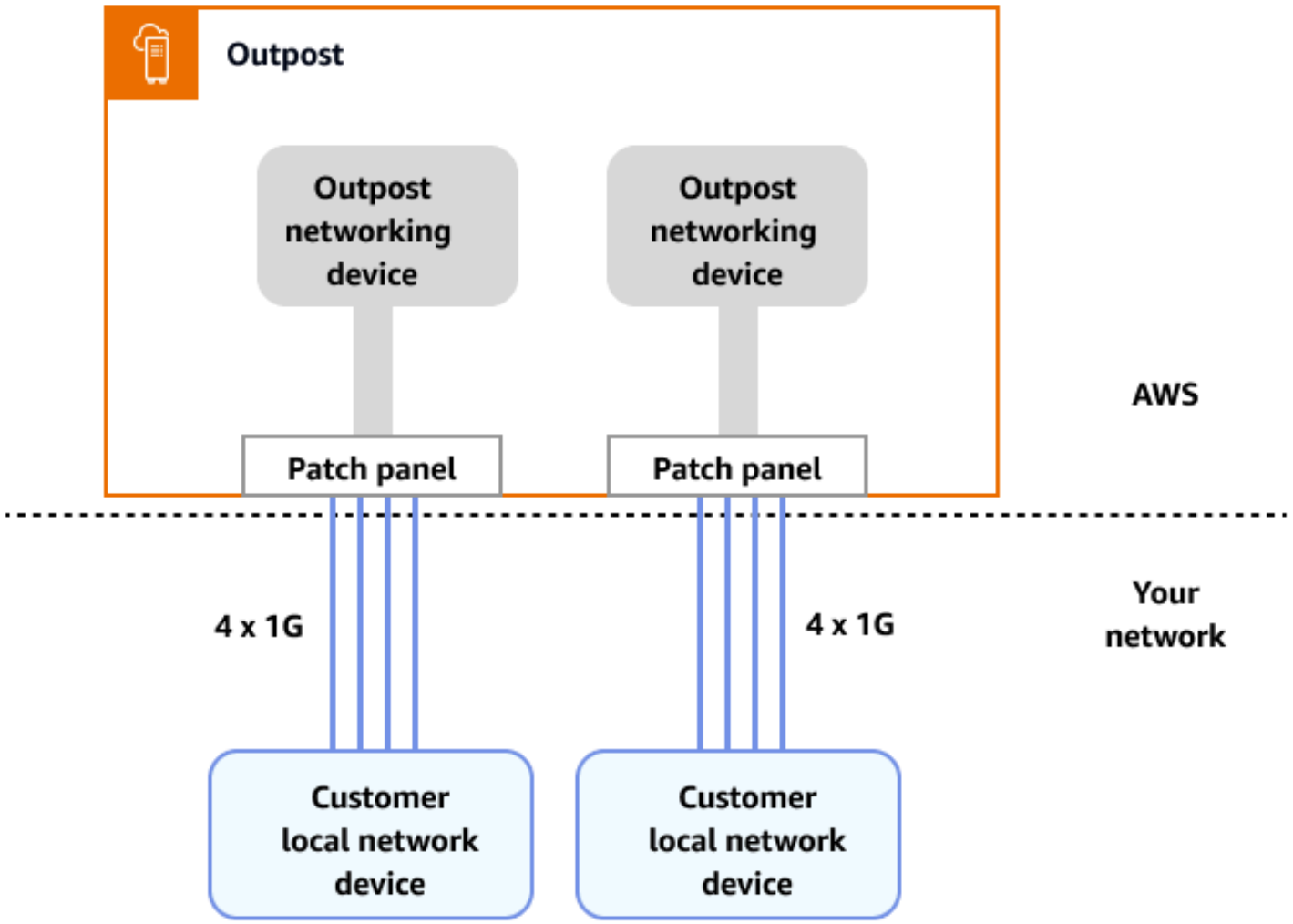
ローカルゾーンは、Amazon S3 や Amazon RDS などの任意のリージョンサービスをシームレスに使用できるようにする複数の冗長で安全な高速リンクを使用して親リージョンに接続されます。お

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 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 Direct Connect、該当する耐障害性アーキテクチャは AWS リージョン、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、 Direct Connect PoP が 1 つしかないため、 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 Direct Connect ロケーション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 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キング

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。

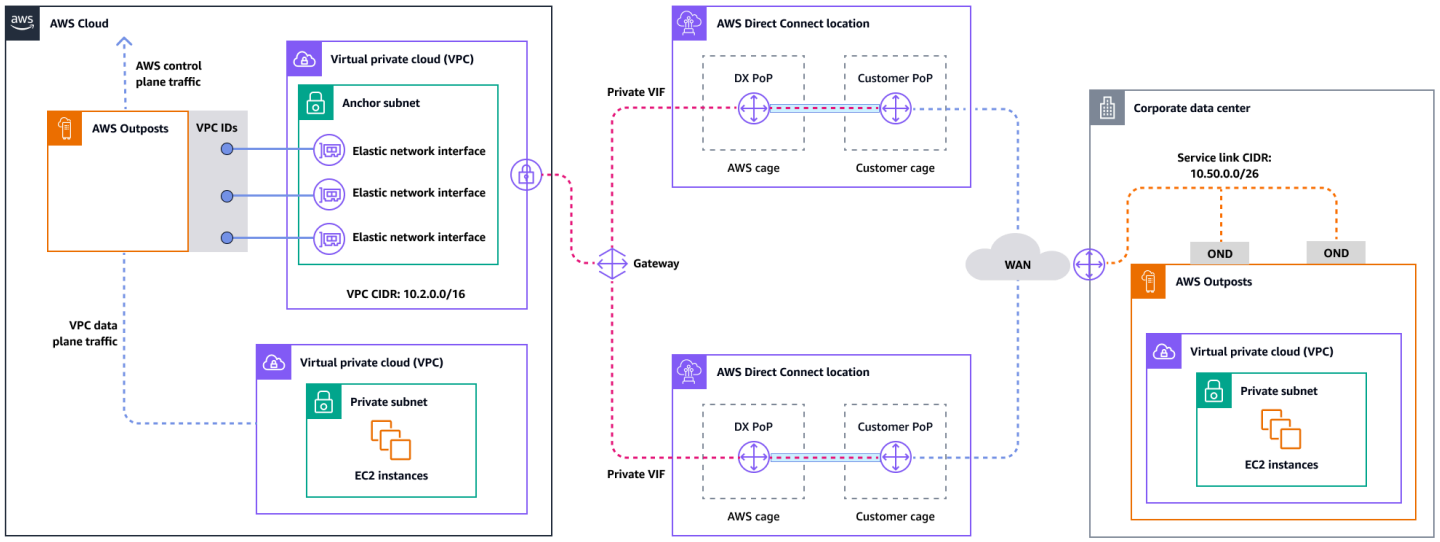
アップリンク速度	アップリンク数
1 Gbps	1、2、4、6 または 8
10 Gbps	1、2、4、8、12 または 16
40 または 100 Gbps	1、2 または 4



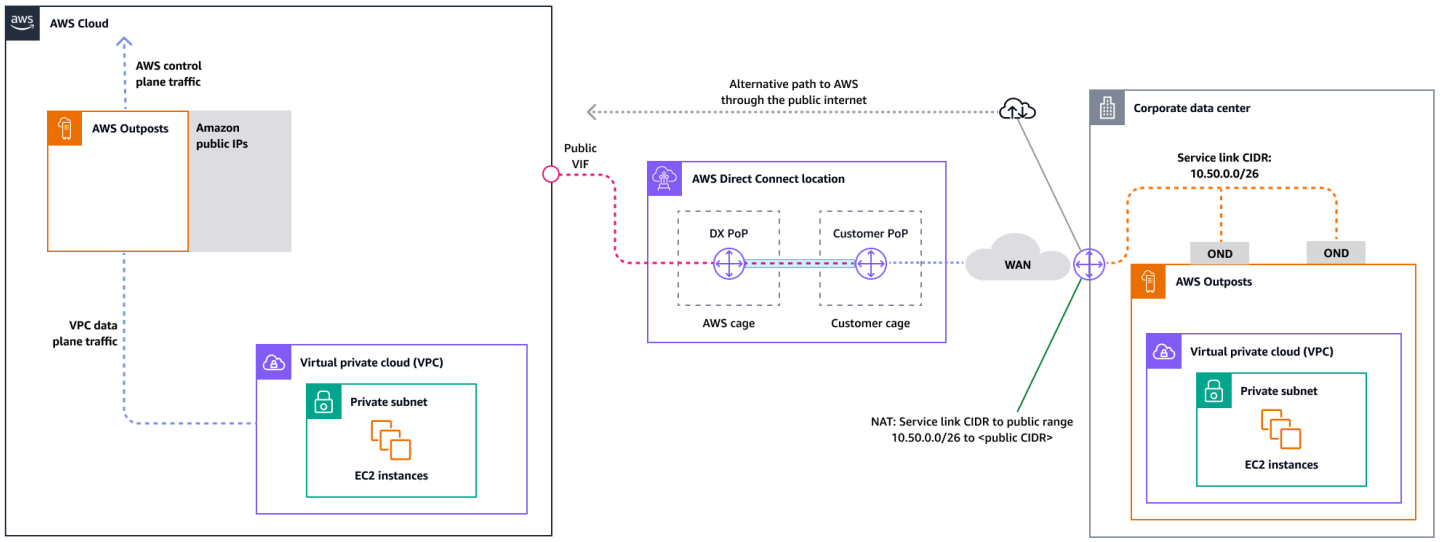
この接続の詳細については、 AWS Outposts ドキュメントの「Outposts ラックのローカルネットワーク接続」を参照してください。

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、 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。



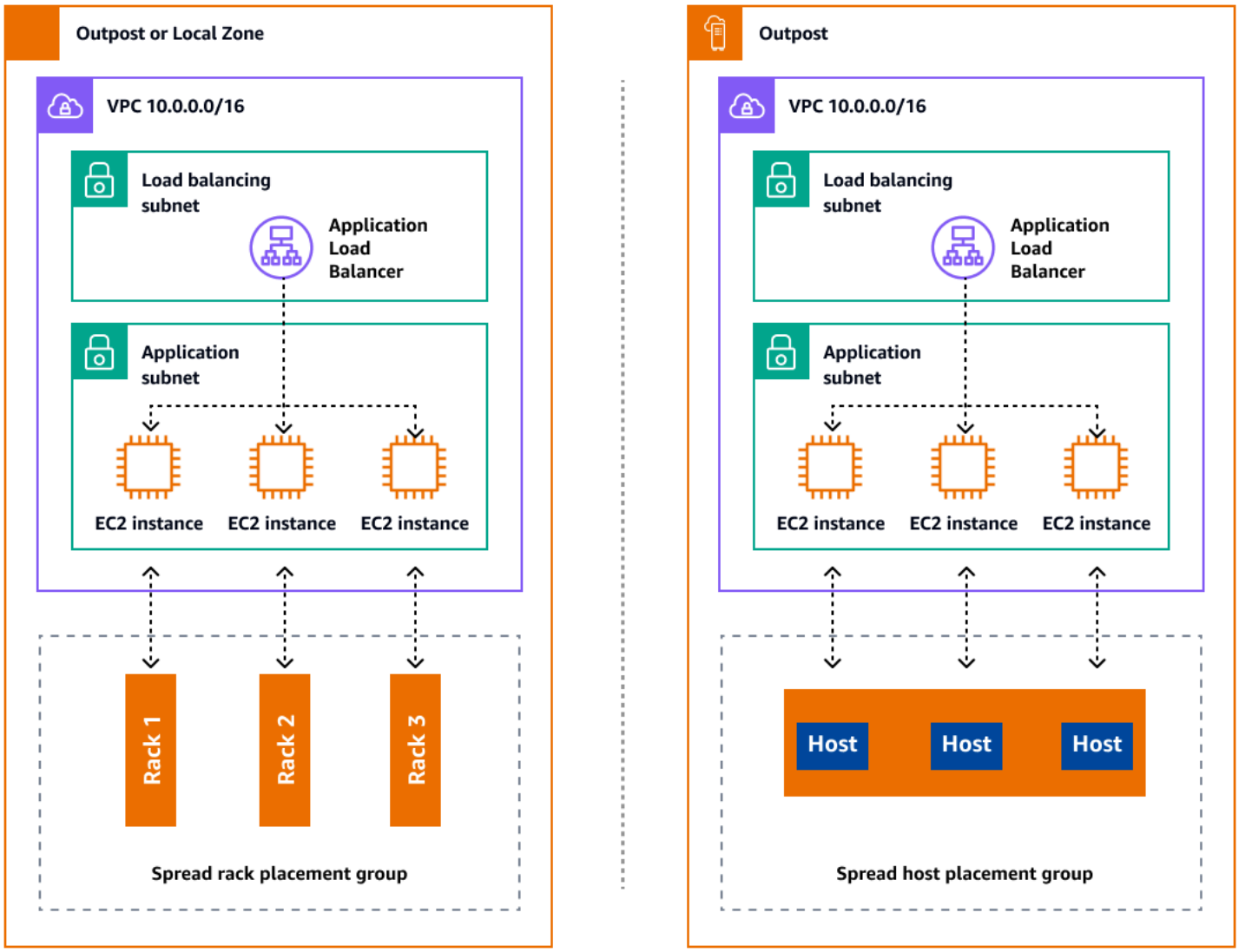
ACE ラックを使用した Outposts ラックデプロイのスケーリング

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) 。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での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場合があります。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

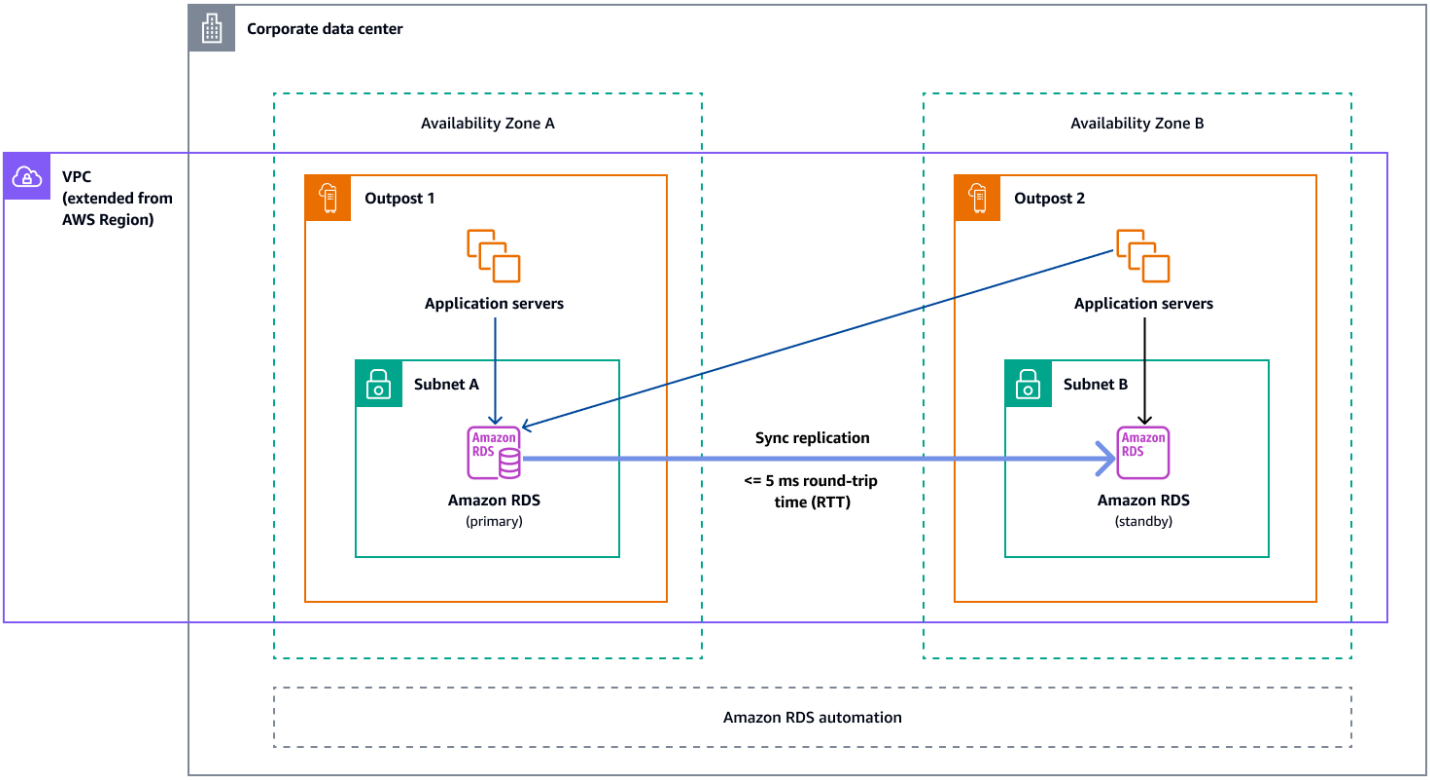
Outposts でマルチ AZ インスタンスデプロイを使用すると、Amazon RDS は 2 つの Outposts に 2 つのデータベースインスタンスを作成します。各 Outpost は独自の物理インフラストラクチャで実行され、高可用性のためにリージョン内の異なるアベイラビリティーゾーンに接続します。2 つの Outposts がカスタマー管理のローカル接続を介して接続されている場合、Amazon RDS はプライマリデータベースインスタンスとスタンバイデータベースインスタンス間の同期レプリケーションを管理します。ソフトウェアまたはインフラストラクチャに障害が発生した場合、Amazon RDS は自動的にスタンバイインスタンスをプライマリロールに昇格させ、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。



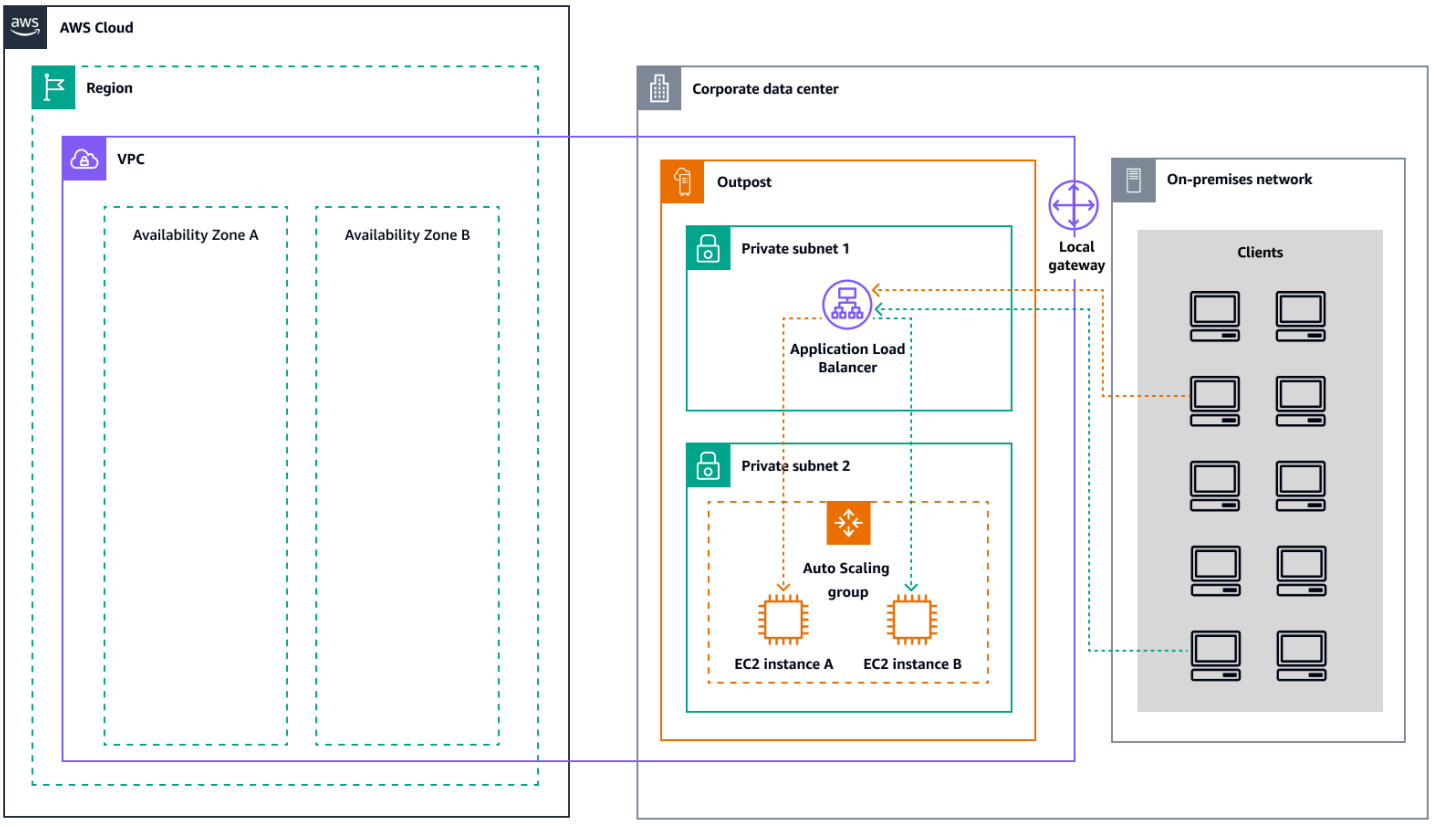
フェイルオーバーメカニズム

ロードバランシングと自動スケーリング

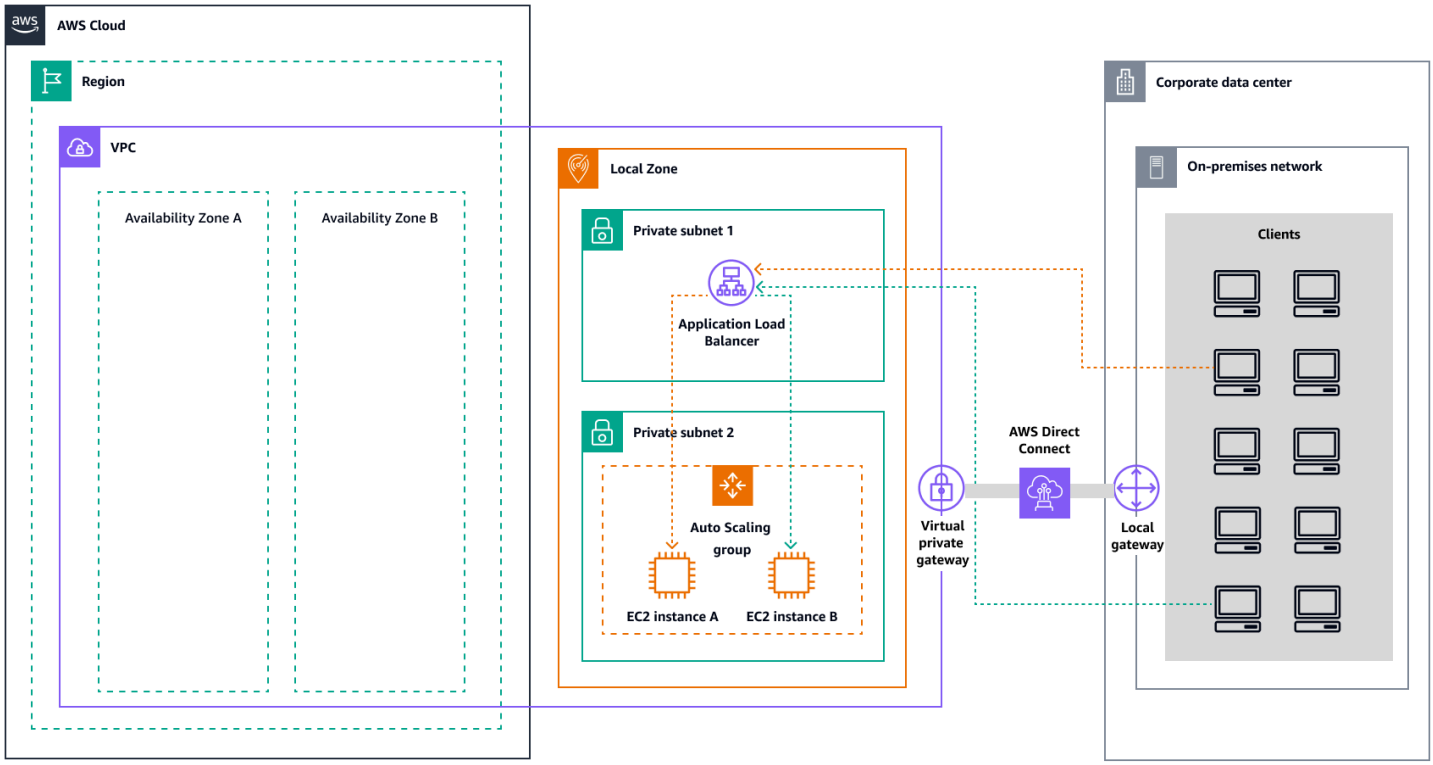
Elastic Load Balancing (ELB) は、実行中のすべての EC2 インスタンスに受信アプリケーショントラフィックを自動的に分散します。ELB は、1 つのインスタンスが過負荷にならないようにトラ

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。



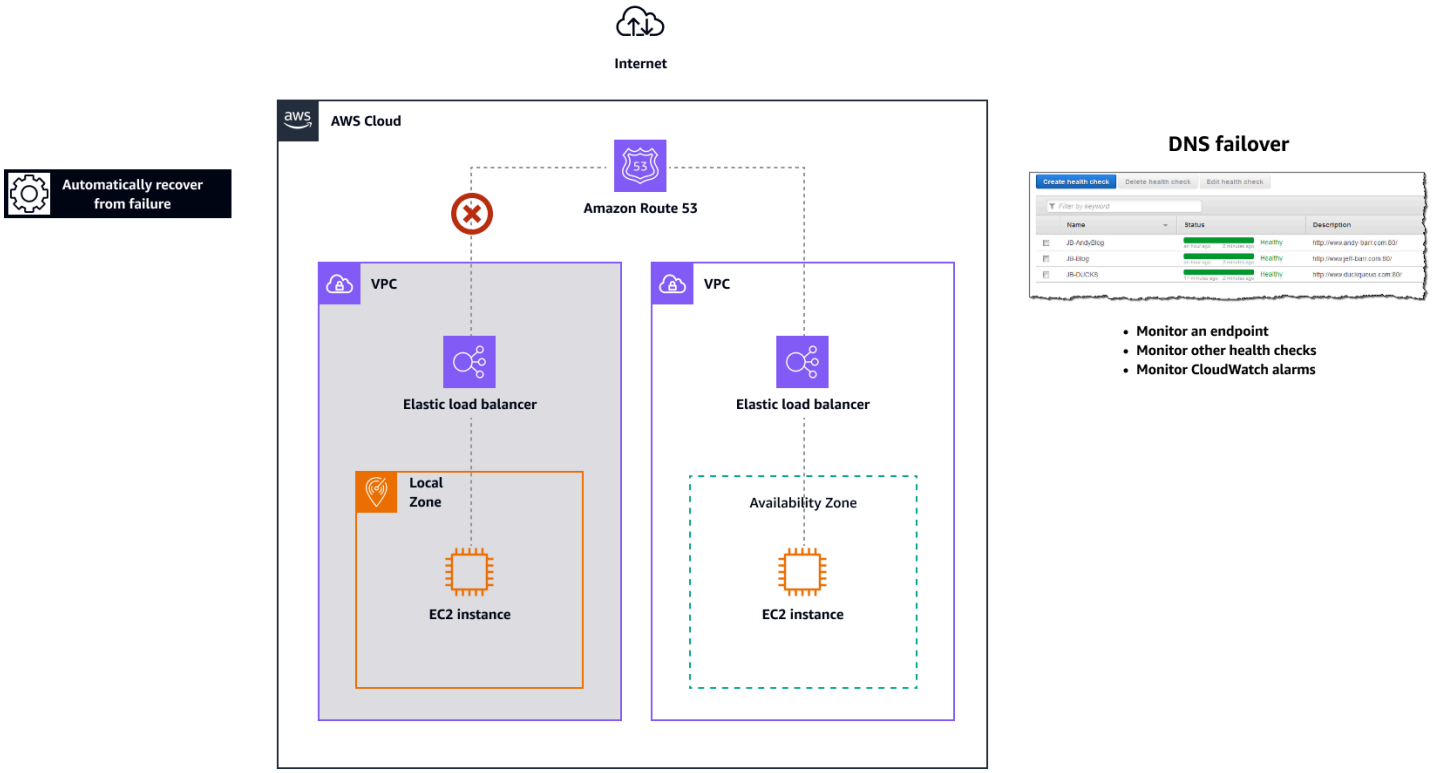
> **Note**
>
> Application Load Balancer は、 AWS Outposts と Local Zones の両方で使用できます。ただし、 で Application Load Balancer を使用するには AWS Outposts、ロードバランサーに必要なスケーラビリティを提供するために Amazon EC2 容量のサイズを設定する必要があります。でのロードバランサーのサイズ設定の詳細については AWS Outposts、 AWS ブログ記事「Configuring an Application Load Balancer on AWS Outposts」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



注意事項

- 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 上の 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、工場機器、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 AWS リージョン 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、オンプレミスネットワークなど、管理する DNS リゾルバーに DNS クエリを転送できます。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 Transform MGN	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

このガイドの寄稿者は次のとおりです。

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

レビューアー

- David Filiatrault、デリバリーコンサルタント、 AWS

テクニカルライター

- 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

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。