第 1 世代 Outposts ラックのユーザーガイド

# AWS Outposts

# AWS Outposts: 第 1 世代 Outposts ラックのユーザーガイド

# Table of Contents

# とは AWS Outposts

AWS Outposts は、 AWS インフラストラクチャ、サービス、APIs、ツールをお客様の施設に拡張するフルマネージドサービスです。 AWS マネージドインフラストラクチャへのローカルアクセスを提供することで、 AWS Outposts では、AWS リージョンと同じプログラミングインターフェイスを使用してオンプレミスでアプリケーションを構築および実行できます。同時に、ローカルのコンピューティングおよびストレージリソースを使用して、レイテンシーを短縮し、ローカルのデータ処理ニーズに対応できます。

Outpost は、お客様のサイトにデプロイされた AWS コンピューティングおよびストレージ容量のプールです。 は、この容量を AWS リージョンの一部として AWS 運用、モニタリング、管理します。Outpost にサブネットを作成し、EC2 インスタンス、EBS ボリューム、ECS クラスター、RDS インスタンスなどの AWS リソースを作成するときに指定できます。Outpost サブネットのインスタンスは、すべて同じ VPC 内のプライベート IP アドレスを使用して、 AWS リージョン内の他のインスタンスと通信します。

> **Note**
>
> 同じ VPC 内にある他の Outpost やローカルゾーンには、Outpost を接続できません。

詳細については、AWS Outposts 製品ページを参照してください。

## 主要なコンセプト

これらは の主要な概念です AWS Outposts。

- Outpost サイト – AWS が Outpost をインストールするカスタマー管理の物理的な建物。サイトは、Outpost の施設、ネットワーク、および電力の要件を満たさなければなりません。
- Outpost の容量 - Outpost で利用可能なコンピューティングおよびストレージリソース。 AWS Outposts コンソールから Outpost の容量を表示および管理できます。 は、Outposts レベルで定義できるセルフサービスの容量管理 AWS Outposts をサポートし、Outposts 内のすべてのアセットを再設定したり、特に個々のアセットに対して再設定したりできます。Outpost アセットは、Outposts ラック内の単一のサーバーでも、Outposts サーバーでもかまいません。
- Outpost 機器 – AWS Outposts サービスへのアクセスを提供する物理ハードウェア。ハードウェアには、 が所有および管理するラック、サーバー、スイッチ、ケーブルが含まれます AWS。

- Outposts ラック - 産業標準の 42U ラックである Outpost のフォームファクタ Outposts ラックには、ラックマウント可能なサーバー、スイッチ、ネットワークパッチパネル、電源シェルフ、およびブランクパネルが含まれています。
- Outposts ACE ラック - 集約、コア、エッジ (ACE) ラックは、複数ラックの Outpost のデプロイにおけるネットワーク集約ポイントとして機能します。ACE ラックによって、論理 Outposts 内の複数の Outpost コンピューティングラックとオンプレミスネットワーク間を接続することにより、物理ネットワークポートと論理インターフェイスの要件数を削減します。

  コンピューティングラックが 4 架以上ある場合は、ACE ラックを設置する必要があります。コンピューティングラックが 4 架未満であっても、今後 4 架以上のラックに拡張する予定がある場合は、早期に ACE ラックを設置することをお勧めします。

  ACE ラックの詳細については、「ACE AWS Outposts ラックを使用したラックデプロイのスケーリング」を参照してください。
- Outposts サーバー — 産業標準の 1U または 2U サーバーの Outpost フォームファクターです。標準の EIA-310D 19 インチ適合の 4 ポストラックに取り付けることができます。Outposts サーバーは、スペースが限られているか、キャパシティ要件が小さいサイトに対して、ローカルなコンピュートおよびネットワークサービスを提供します。
- Outpost 所有者 – AWS Outposts 注文を行うアカウントのアカウント所有者。が顧客と AWS やり取りした後、所有者は追加の連絡先を含めることができます。 AWS は連絡先と通信して、注文、インストール予約、ハードウェアのメンテナンスと交換を明確にします。連絡先情報が変更された場合は、AWS サポート センターに連絡してください。
- サービスリンク – Outpost とそれに関連する AWS リージョン間の通信を可能にするネットワークルート。各Outpostは、アベイラビリティーゾーンとそれに関連付けられたリージョンの拡張です。
- ローカルゲートウェイ (LGW) - Outposts ラックとオンプレミスネットワークとの間の通信が可能になる論理的な相互接続仮想ルーター。
- ローカルネットワークインターフェイス - Outposts サーバーからオンプレミスネットワークへの通信を可能にするネットワークインターフェイス。

# AWS Outposts の リソース

以下のリソースを Outpost 上で作成して、オンプレミスのデータやアプリケーションに近い場所で実行する必要がある低レイテンシーワークロードをサポートできます。

## コンピューティング

| リソースタイプ | ラック | サーバー |
| --- | --- | --- |
| Amazon EC2 インスタンス |  はい |  はい |
| Amazon ECS クラスター |  はい |  はい |
| Amazon EKS ノード |  はい |  いいえ |

## データベースおよび分析

| リソースタイプ | ラック | サーバー |
| --- | --- | --- |
| Amazon ElastiCache ノード (Redis クラスター、Memcached クラスター) |  はい |  いいえ |
| Amazon EMR クラスター |  はい |  いいえ |
| Amazon RDS DB インスタンス |  はい |  いいえ |

## ネットワーク

| リソースタイプ | ラック | サーバー |
| --- | --- | --- |
| App Mesh Envoy プロキシ | はい | はい |
| アプリケーション ロード バランサー | はい | いいえ |
| Amazon VPC サブネット | はい | はい |
| Amazon Route 53 | はい | いいえ |

## Storage

| リソースタイプ | ラック | サーバー |
| --- | --- | --- |
| Amazon EBS ボリューム | はい | いいえ |
| Amazon S3 バケット | はい | いいえ |

その他 AWS のサービス

| サービス | ラック | サーバー |
| --- | --- | --- |
| AWS IoT Greengrass |  はい |  はい |

# AWS のサービス でサポート AWS リージョン

AWS Outposts は、Outpost が動作する AWS リージョン AWS のサービス に基づいて をサポートします。サポートされているサービスを確認するには、それぞれの地理的エリアで リージョンを表示します。

エリア

- 北米
- アフリカ
- アジアパシフィック
- 欧州
- 中東
- 南米

## 北米

次の表は、北米リージョン AWS のサービス での AWS Outposts のサポートを示しています。

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMF | Ama Elas he | Clou re 移行 | Elas Disa Rec | Appl on Load Bala | Direc Conn | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 米国東部 (バージニア北部) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | あり |
| 米国東部 (オハイオ) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | あり |
| 米国西部 (北カリフォル | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | あり |

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMR | Ama Elas he | Clou re 移行 | Elas Disa Rec | Appl on Load Bala | Dire Con | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ニア) | | | | | | | | | | | | | | | | |
| 米国西部 (オレゴン) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | あり |
| カナダ (中部) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |

## アフリカ

次の表は、アフリカリージョン AWS のサービス での AWS Outposts のサポートを示しています。

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Po QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMR | Ama Elas he | Clou re 移行 | Elas Disa Reco | Appl on Load Bala | Direc Conn | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| アフリカ (ケープタウン) | はい | はい | はい | はい | はい | はい | あり | なし | はい | はい | はい | はい | はい | はい | はい | はい |

## アジアパシフィック

次の表は、アジアパシフィックリージョン AWS のサービス での AWS Outposts のサポートを示しています。

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Po QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMR | Ama Elas he | Clou re 移行 | Elas Disa Reco | Appl on Load Bala | Direc Conn | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| アジアパシ | はい | はい | はい | あり | なし | はい | あり | なし | はい | あり | なし | はい | はい | はい | はい | はい |

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMF | Ama Elas he | Clou re 移行 | Elas Disa Rec | Appl on Load Bala | Dire Con | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| フィク (ジャカルタ) | | | | | | | | | | | | | | | | |
| アジアパシフィク (ムンバイ) | はい | はい | はい | はい | はい | はい | あり | なし | はい | はい | はい | はい | はい | はい | はい | あり |
| アジアパシフィク (大阪) | はい | はい | はい | あり | なし | はい | あり | なし | はい | はい | はい | はい | はい | はい | はい | はい |

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMR | Ama Elas he | Clou re 移行 | Elas Disa Reco | Appl on Load Bala | Dire Conn | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| アジアパシフィック (ソウル) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |
| アジアパシフィック (シンガポール) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMF | Ama Elas he | Clou re 移行 | Elas Disa Rec | Appl on Load Bala | Dire Con | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| アジアパシフィック (シドニー) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |
| アジアパシフィック (東京) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |

## 欧州

次の表は、欧州リージョン AWS のサービス での AWS Outposts のサポートを示しています。

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMF | Ama Elas he | Clou re 移行 | Elas Disa Rec | Appl on Load Bala | Direc Conr | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 欧州 (フランクフルト) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | あり |
| 欧州 (アイルランド) | はい | はい | はい | はい | はい | はい | あり | なし | はい | はい | はい | はい | はい | はい | はい | はい |
| 欧州 (ロンドン) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |
| 欧州 (ミ | はい | はい | はい | はい | はい | はい | あり | なし | はい | はい | はい | はい | はい | はい | はい | はい |

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMR | Ama Elas he | Clou re 移行 | Elas Disa Rec | Appl on Load Bala | Dire Con | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ラノ) | | | | | | | | | | | | | | | | |
| 欧州 (パリ) | はい | はい | はい | はい | はい | はい | あり | なし | はい | はい | はい | はい | はい | はい | はい | はい |
| 欧州 (ストックホルム) | はい | はい | はい | はい | はい | はい | あり | なし | はい | はい | はい | はい | はい | はい | はい | はい |

## 中東

次の表は、中東リージョン AWS のサービス での AWS Outposts のサポートを示しています。

| AWS リージョン | Ama EC2 | Ama EBS | Ama EBS スナップショット | Ama S3 | Ama RDS SQL、Pc QL | Ama ECS | Ama EKS | Ama EKS LC | Ama EMF | Ama Elas he | Clou re 移行 | Elas Disa Rec | Appl on Load Bala | Direc Conr | Ama VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| イスラエル (テルアビブ) | はい | はい | はい | はい | はい | はい | あり | なし | はい | あり | なし | あり | なし | はい | はい | はい |
| 中東 (バーレーン) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |
| 中東 (アラブ首長国連邦) | はい | あり | なし | なし | なし | はい | あり | なし | はい | あり | なし | あり | なし | はい | はい | はい |

## 南米

次の表は、南米リージョン AWS のサービス での AWS Outposts のサポートを示しています。

| AWS リージョン | Amazon EC2 | Amazon EBS | Amazon EBS スナップショット | Amazon S3 | Amazon RDS SQL、PostgreSQL | Amazon ECS | Amazon EKS | Amazon EKS LC | Amazon EMR | Amazon ElastiCache | Cloud 移行 | Elastic Disaster Recovery | Application Load Balancer | Direct Connect | Amazon VPC | ローカルゲートウェイ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 南米 (サンパウロ) | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい | はい |

# AWS Outposts サポートされているリージョンの Amazon RDS

Amazon RDS on AWS Outposts は、以下から入手できます AWS リージョン。

- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (東京)
- アジアパシフィック (ソウル)
- アジアパシフィック (大阪)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- カナダ (中部)
- 欧州 (フランクフルト)

- 欧州 (ストックホルム)
- 欧州 (ミラノ)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- イスラエル (テルアビブ)
- 中東 (アラブ首長国連邦)
- 中東 (バーレーン)
- 南米 (サンパウロ)
- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)

# 料金

料金は、注文の詳細に基づいています。注文の際には、Amazon EC2 のインスタンスタイプとストレージオプションの組み合わせによる、さまざまな Outpost 構成から選択できます。契約期間と支払いオプションも選択します。料金には以下のものが含まれます。

- Outposts ラック - 配送、設置、インフラストラクチャのサービスメンテナンス、ソフトウェアのパッチおよびアップグレード、ラックの撤去。
- Outposts サーバー - 配送、インフラストラクチャのサービスメンテナンス、ソフトウェアのパッチおよびアップグレード。サーバー返却時の設置と梱包は、お客様において行う必要があります。

共有リソースと AWS 、リージョンから Outpost へのデータ転送に対して課金されます。また、可用性とセキュリティを維持するために が AWS 実行するデータ転送に対しても課金されます。

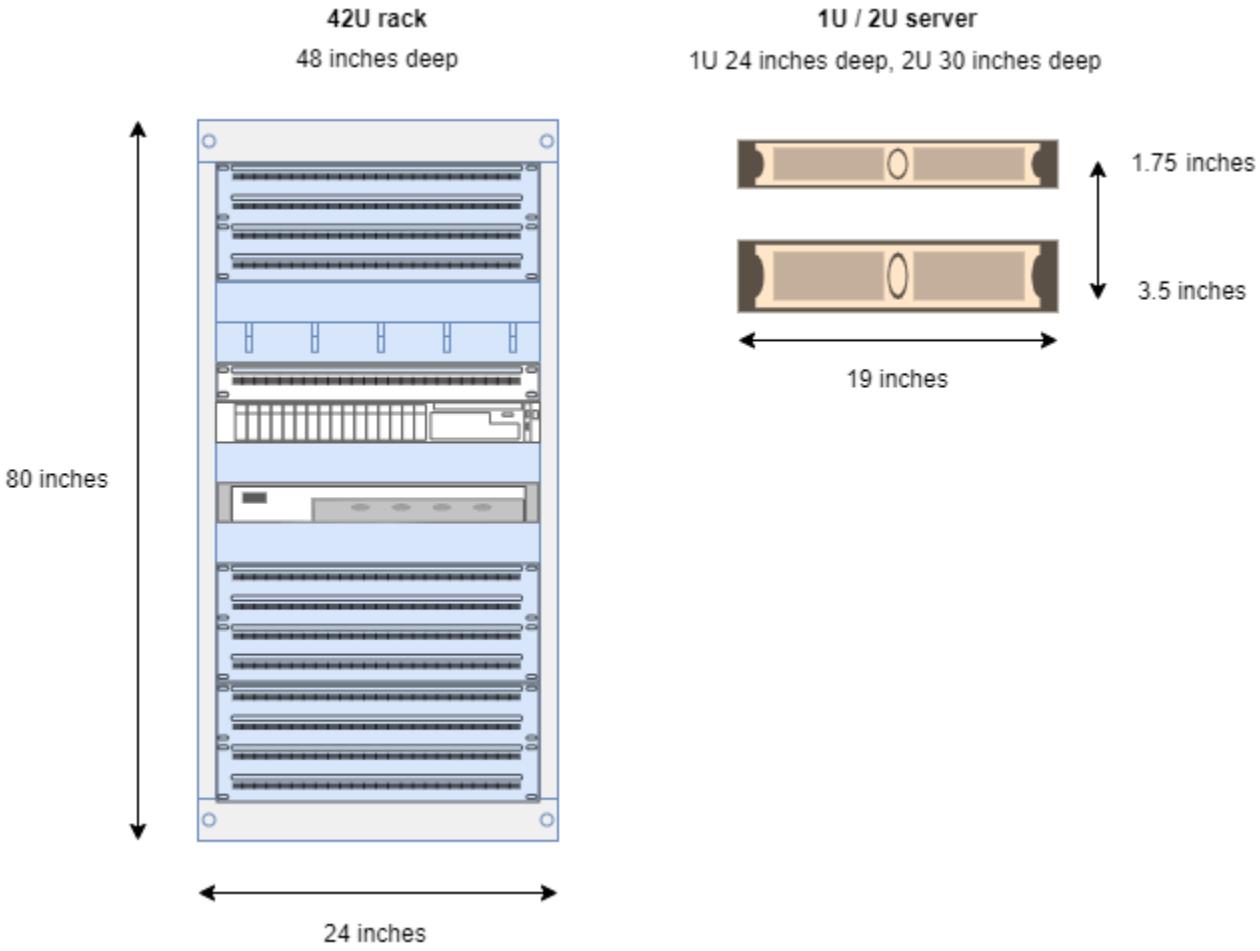
ロケーション、設定、支払いオプションに基づく料金については、以下を参照してください。

- Outposts ラックの料金
- Outposts サーバーの料金

# の AWS Outposts 仕組み

AWS Outposts は、Outpost と AWS リージョン間の安定した接続で動作するように設計されています。リージョンとオンプレミス環境のローカルワークロードとの接続を実現するには、Outpost をオンプレミスネットワークに接続する必要があります。オンプレミスネットワークは、リージョンへのワイドエリアネットワーク (WAN) アクセスを提供する必要があります。また、オンプレミスのワークロードやアプリケーションが存在するローカルネットワークに LAN または WAN でアクセスできるようにする必要があります。

次の図は両方の Outpost フォームファクターを示しています。




内容

- ネットワークコンポーネント
- VPC とサブネット
- ルーティング

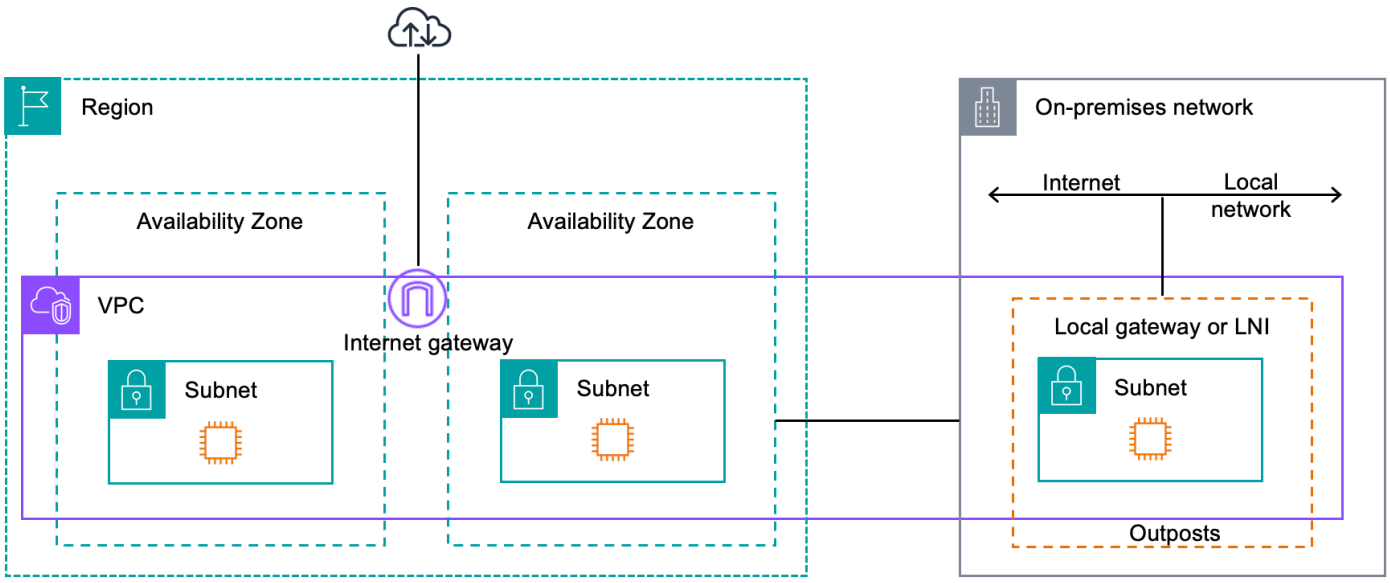
- DNS
- サービスリンク
- ローカルゲートウェイ
- ローカルネットワークインターフェイス

# ネットワークコンポーネント

AWS Outposts は、Amazon VPC を AWS リージョンから Outpost に拡張します。これには、インターネットゲートウェイ、仮想プライベートゲートウェイ、Amazon VPC Transit Gateway、VPC エンドポイントなど、リージョンでアクセスできる VPC コンポーネントが含まれます。Outpost はリージョン内のアベイラビリティーゾーンに設置されており、そのアベイラビリティーゾーンの耐障害性のために使用できる拡張機能です。

次の図は、Outpost のネットワークコンポーネントを示しています。

- AWS リージョン およびオンプレミスネットワーク
- リージョン内に複数のサブネットを持つ VPC
- オンプレミスネットワーク内の Outpost
- Outpost と提供されるローカルネットワーク間の接続：
  - Outposts ラックの場合: ローカルゲートウェイ
  - Outposts サーバーの場合: ローカルネットワークインターフェイス (LNI)



# VPC とサブネット

Virtual Private Cloud (VPC) は、その AWS リージョン内のすべてのアベイラビリティーゾーンにまたがります。Outpost 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 Outpost に拡張できます。Outpost サブネットを VPC に追加するには、サブネットを作成するときに Outpost の Amazon リソースネーム (ARN) を指定します。

Outposts は複数のサブネットをサポートします。Outpost で EC2 インスタンスを起動するときに EC2 インスタンスサブネットを指定できます。Outpost は AWS コンピューティングとストレージ容量のプールであるため、インスタンスがデプロイされる基盤となるハードウェアを指定することはできません。

各 Outpost は 1 つ以上の Outpost サブネットを持つ複数の VPC をサポートできます。VPC クォータの詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC のクォータ」を参照してください。

Outpost サブネットは、Outpost を作成した VPC の VPC CIDR 範囲から作成します。Outpost のアドレス範囲は、Outpost サブネットにある EC2 インスタンスなどのリソースに使用できます。

# ルーティング

デフォルトでは、すべての Outpost サブネットは VPC からメインルートテーブルを継承します。カスタムルート テーブルを作成し、Outpost サブネットに関連付けることができます。

Outpost サブネットのルートテーブルは、アベイラビリティゾーンのサブネットのルートテーブルと同様に機能します。IP アドレス、インターネットゲートウェイ、ローカルゲートウェイ、仮想プライベートゲートウェイ、ピアリング接続を宛先として指定できます。例えば、各 Outpost サブネットは、継承されたメインルートテーブルまたはカスタムテーブルを介して VPC ローカルルートを継承します。つまり、VPC CIDR に宛先がある Outpost サブネットを含む VPC 内のすべてのトラフィックは VPC でルーティングされたままになります。

Outpost サブネットのルートテーブルには、以下の宛先を含めることができます。

- VPC CIDR 範囲 – インストール時にこれ AWS を定義します。これはローカルルートであり、同じ VPC 内の Outpost インスタンス間のトラフィックを含むすべての VPC ルーティングに適用されます。
- AWS リージョンの送信先 – これには、Amazon Simple Storage Service (Amazon S3)、Amazon DynamoDB ゲートウェイエンドポイント、 AWS Transit Gateway、仮想プライベートゲートウェイ、インターネットゲートウェイ、VPC ピアリングのプレフィックスリストが含まれます。

同じ Outpost にある複数の VPC とピアリング接続している場合、VPC 間のトラフィックは Outpost に残り、リージョンに戻るサービスリンクは使用されません。

- ローカルゲートウェイを使用した Outpost 間の VPC 内通信 – ダイレクト VPC ルーティングを使用して、異なる Outpost にわたる同じ VPC 内のサブネット間の通信をローカルゲートウェイで確立できます。詳細については、以下を参照してください。
  - ダイレクト VPC ルーティング
  - AWS Outposts ローカルゲートウェイへのルーティング

## DNS

VPC に接続されたネットワーク インターフェイスの場合、Outposts サブネット内の EC2 インスタンスは Amazon Route 53 DNS サービスを使用してドメイン名を IP アドレスに解決できます。Route 53 は、Outpost で実行されているインスタンスのドメイン登録、DNS ルーティング、ヘルスチェックなどの DNS 機能をサポートしています。特定のドメインへのトラフィックのルーティングでは、パブリックおよびプライベートの両方のホスト型アベイラビリティゾーンがサポートされています。Route 53 リゾルバーは AWS リージョンでホストされます。したがって、これらの DNS 機能を使用するには、Outpost から AWS リージョンへのサービスリンク接続が稼働している必要があります。

Outpost と AWS リージョン間のパスレイテンシーによっては、Route 53 で DNS 解決時間が長くなる場合があります。このような場合、オンプレミス環境でローカルにインストールされた DNS サーバーを使用できます。独自の DNS サーバーを使用するには、オンプレミス DNS サーバー用の DHCP オプションセットを作成し、VPC に関連付ける必要があります。また、これらの DNS サーバーに IP 接続があることを確認する必要があります。また、アクセスしやすくするためにローカルゲートウェイのルーティングテーブルにルートを追加する必要がある場合もありますが、これはローカルゲートウェイを備えた Outposts ラックのみのオプションです。DHCP オプションセットには VPC スコープがあるため、VPC の Outpost サブネットとアベイラビリティー ゾーン サブネットのインスタンスはどちらも、指定された DNS サーバーを DNS 名ソリューションに使用しようとします。

Outpost から送信される DNS クエリのクエリロギングはサポートされていません。

## サービスリンク

サービスリンクは、Outpost から選択した AWS リージョンまたは Outposts ホームリージョンへの接続です。サービスリンクは暗号化された VPN 接続セットで、Outpost が選択したホームリージョ

ンと通信する際に必ず使用されます。仮想 LAN (VLAN) を使用してサービスリンク上のトラフィックをセグメント化します。サービスリンク VLAN により、Outpost と AWS リージョン間の通信が可能になり、Outpost と AWS リージョン間の VPC 内トラフィックの両方を管理できます。

サービスリンクは Outpost のプロビジョニング時に作成されます。サーバーフォームファクターをお持ちの場合は、接続を作成してください。ラックがある場合、 はサービスリンク AWS を作成します。詳細については、以下を参照してください。

- AWS Outposts への接続 AWS リージョン
- 「高可用性の設計とアーキテクチャに関する考慮事項」ホワイトペーパーの「アプリケーション/ワークロードのルーティングAWS Outposts  AWS 」

# ローカルゲートウェイ

Outposts ラックには、オンプレミスネットワークへの接続を提供するローカルゲートウェイが含まれています。Outposts ラックをお持ちの場合は、宛先がオンプレミスネットワークであるローカルゲートウェイをターゲットとして含めることができます。ローカルゲートウェイは Outposts ラックでのみ動作し、Outposts ラックに関連付けられた VPC とサブネットルートテーブルでのみ使用できます。詳細については、以下を参照してください。

- Outposts ラックのローカルゲートウェイ
- 「高可用性の設計とアーキテクチャに関する考慮事項」ホワイトペーパーの「アプリケーション/ワークロードのルーティングAWS Outposts  AWS 」

# ローカルネットワークインターフェイス

Outposts サーバーには、オンプレミスのネットワークへの接続を提供するローカルネットワークインターフェイスが含まれています。ローカルネットワークインターフェイスは、Outpost サブネット上で実行されている Outposts サーバーでのみ使用できます。Outposts ラックまたは AWS リージョンの EC2 インスタンスからローカルネットワークインターフェイスを使用することはできません。ローカル ネットワーク インターフェイスは、オンプレミスのロケーションのみを対象としています。詳細については、「Outposts サーバー用AWS Outposts ユーザーガイド」の「ローカルネットワークインターフェイス」を参照してください。

# Outposts ラックのサイト要件

Outpost サイトは、Outpost が動作する物理的な場所です。サイトは選択された国と地域でのみ利用可能です。詳細については、「AWS Outposts ラックに関するよくある質問」を参照してください。質問「Outposts ラックはどの国と地域で利用できますか？」を参照してください。

このページでは、Outposts ラックの要件について説明します。集約、コア、エッジ (ACE) ラックを設置する場合は、サイトについても Outpost ACE ラックのサイト要件 に記載されている要件を満たしている必要があります。

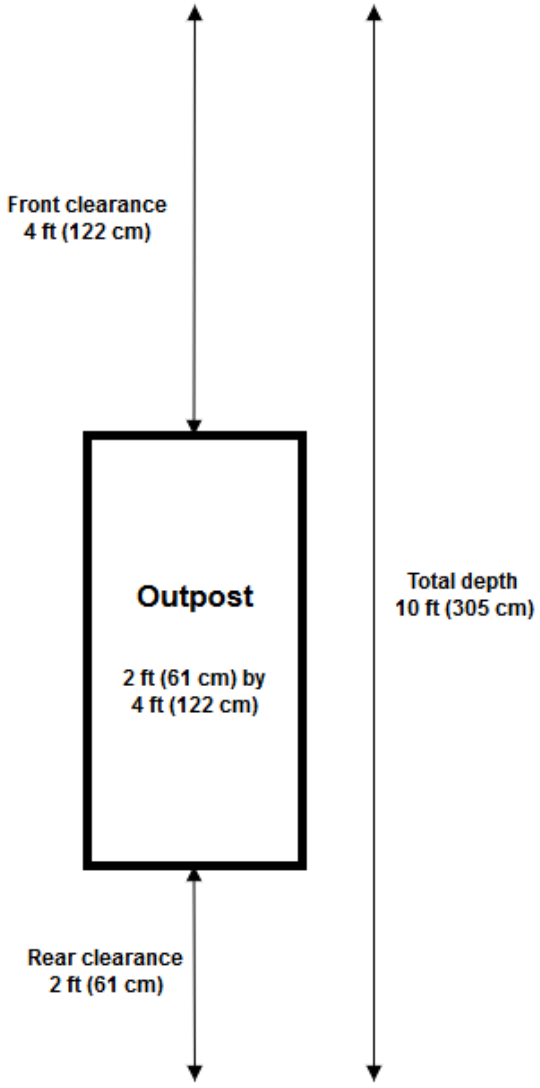
Outposts サービスの要件については、「Outposts サーバーのAWS Outposts ユーザーガイド」の「Outposts サービスのサイト要件」を参照してください。

## 施設

これらはラックの設備要件です。

- 温度と湿度 — 周囲温度は 41　°F (5 °C) から 95 °F (35 °C) の間でなければなりません。相対湿度は8%から80%の間で、結露がない状態でなければなりません。
- エアフロー — ラックは冷気を前面通路から吸い込み、温風を背面通路に排出します。ラックの位置には、少なくとも kVA 立方フィート/分 (CFM) の 145.8 倍のエアフローが供給されている必要があります。
- 積み込みドック — 積み込みドックには、高さ 94 インチ (239 cm)、幅 54 インチ (138 cm)、奥行 51 インチ (130 cm) のラッククレートを収容できる必要があります。
- 重量サポート — 重量は構成によって異なります。注文概要で指定されている構成の重量は、ラックポイントロードで確認できます。ラックを設置する場所とその場所までの経路は、指定された重量に耐えられる必要があります。これには、経路上のすべての貨物用エレベーターと標準エレベーターが含まれます。
- スペースのゆとり — ラックの高さは 80 インチ (203 cm)、幅 24 インチ (61 cm)、奥行きは 48 インチ (122 cm) です。出入口、廊下、曲がり角、スロープ、エレベーターには十分な隙間が必要です。最終的な設置場所には、Outpost を置くための幅 24 インチ (61 cm)、奥行 48 インチ (122 cm) に加えて、さらに前方に 48 インチ (122 cm)、後方に 24 インチ (61 cm) の隙間を設ける必要があります。Outpost に必要な最小面積は、幅 24 インチ (61 cm)、奥行き 10 フィート (305 cm) です。

  次の図は、Outpost に必要な最小面積の合計を示しています (周辺のゆとりを含む)。




- 耐震ブレーシング – 規制またはコードで必要とされる範囲で、ラックが施設内にある間は、ラックに適切な耐震アンカーとブレーシングをインストールして維持します。 は、すべての Outposts ラックで最大 2.0G の耐震アクティビティを保護するフロアブラケット AWS を提供します。
- ボンディングポイント – 電気技師が設置中にラックをボンディングできるように、ラック位置にボンディングワイヤ/ポイントを提供することをお勧めします。これは、 AWS認定技術者によって検証されます。
- 施設アクセス – Outpost へのアクセス、サービス、または削除の能力 AWS に悪影響を及ぼすような方法で施設を変更することはありません。
- 標高 - ラックが設置されている部屋の標高は 10,005 フィート（3,050メートル）以下でなければなりません。

# ネットワーク

これらはラックのネットワーク要件です。

- 1 Gbps、10 Gbps、40 Gbps、または 100 Gbps の速度のアップリンクを提供します。

  サービスリンク接続の推奨帯域幅については、「推奨帯域幅」を参照してください。
- ルーセントコネクタ (LC) 付きのシングルモードファイバー (SMF)、マルチモードファイバ (MMF)、または LC 付き MMF OM4 のいずれかを用意してください。
- 1 台または 2 台のアップストリームデバイスを用意してください。 スイッチでもルーターでもかまいません。高可用性を実現するために 2 つのデバイスの使用をおすすめします。

## ネットワーク準備チェックリスト

Outpost の設定に関する情報を収集するときは、このチェックリストを使用してください。これには、LAN、WAN、Outpost とローカルトラフィックの送信先、および AWS リージョンの送信先間のデバイスが含まれます。

アップリンク速度、ポート、ファイバー

アップリンク速度とポート

Outpost には、ローカルネットワークに接続する 2 つの Outpost ネットワークデバイスがあります。各デバイスがサポートできるアップリンクの数は、帯域幅のニーズとルーターがサポートできるものによって異なります。詳細については、「物理的な接続」を参照してください。

次のリストは、アップリンク速度に基づいて、各 Outpost ネットワークデバイスでサポートされるアップリンクポートの数を示します。

1 Gbps

1、2、4、6、または 8 のアップリンク

10 Gbps

1、2、4、8、12、または 16 のアップリンク

40 Gbps または 100 Gbps

1、2、または 4 のアップリンク

ファイバー

AWS Outposts には Lucent Connectors (LC) を使用したファイバーが必要です。

次の表に、サポートされている光学標準と、対応する必要なファイバータイプを示します。光標準がマルチファイバープッシュオン (DDoS) コネクタを使用している場合は、4 x LC コネクタが Outpost にアタッチされて 1 つのリンクを確立する 4 x LC Type-B ブレークアウトケーブルへの DDoS が必要です。

| アップリンク速度 | 光学標準 | ファイバータイプ |
|---|---|---|
| 1 Gbps | — 1000Base-LX | SMF (LC) |
| 1 Gbps | – 1000Base-SX | MMF (LC) |
| 10 Gbps | – 10GBASE-IR<br>– 10GBASE-LR | SMF (LC) |
| 10 Gbps | – 10GBASE-SR | MMF (LC) |
| 40 Gbps | — 40GBASE-IR4 (LR4L)<br>– 40GBASE-LR4 | SMF (LC) |
| 40 Gbps | – 40GBASE-ESR4<br>– 40GBASE-SR4 | MMF (DDoS から 4 x LC Type-B ブレークアウト ) |
| 100 Gbps | — 100GBASE-CWDM4<br>– 100GBASE-LR4 | SMF (LC) |
| 100 Gbps | — 100G PSM4 MSA | SMF (DDoS から 4 x LC Type-B ブレークアウト ) |
| 100 Gbps | – 100GBASE-SR4 | MMF (DDoS から 4 x LC Type-B ブレークアウト ) |

Outpost リンクアグリゲーションと VLAN

Outpost とネットワーク間にはリンクアグリゲーション制御プロトコル (LACP) が必要です。LACP ではダイナミック LAG を使用する必要があります。

各 Outpost ネットワークデバイスには次の VLAN が必要です。詳細については、「仮想 LAN」を参照してください。

| Outpost ネットワークデバイス | サービスリンク VLAN | ローカルゲートウェイ VLAN |
|---|---|---|
| #1 | 有効な値: 1 ~ 4094 | 有効な値: 1 ~ 4094 |
| #2 | 有効な値: 1 ~ 4094 | 有効な値: 1 ~ 4094 |

Outpost ネットワークデバイスごとに、サービスリンクとローカルゲートウェイに同じ VLAN を使用するか、異なる VLAN を使用するかを選択できます。ただし、各 Outpost ネットワークデバイスには、他の Outpost ネットワークデバイスとは異なる VLAN を設定することをお勧めします。詳細については、「Link aggregation」および「Virtual LANs」を参照してください。

また、冗長レイヤー 2 接続もおすすめです。LACP はリンクアグリゲーションに使用され、高可用性には使用されません。Outpost ネットワークデバイス間の LACP はサポートされていません。

Outpost ネットワークデバイスの IP 接続

2 つの Outpost ネットワークデバイスにはそれぞれ、サービスリンクとローカルゲートウェイ VLAN の CIDR と IP アドレスが必要です。CIDR が /30 または /31 のネットワークデバイスごとに専用サブネットを割り当てることをお勧めします。サブネットから、Outpost が使用するサブネットと IP アドレスを指定します。詳細については、「ネットワークレイヤー接続」を参照してください。

| Outpost ネットワークデバイス | サービスリンクの要件 | ローカルゲートウェイの要件 |
|---|---|---|
| #1 | — サービスリンク CIDR (/30 または /31)<br>— サービスリンク IP アドレス | — ローカルゲートウェイ CIDR (/30 または /31)<br>— ローカルゲートウェイ IP アドレス |

| Outpost ネットワークデバイス | サービスリンクの要件 | ローカルゲートウェイの要件 |
| --- | --- | --- |
| #2 | — サービスリンク CIDR (/30 または /31)<br><br>— サービスリンク IP アドレス | — ローカルゲートウェイ CIDR (/30 または /31)<br><br>— ローカルゲートウェイ IP アドレス |

サービスリンクの最大送信単位 (MTU)

ネットワークは、Outpost と親 AWS リージョンのサービスリンクエンドポイントの間で 1500 バイトの MTU をサポートする必要があります。サービスリンクの詳細については、「AWS Outposts AWS リージョンへの接続」を参照してください。

サービスリンクボーダーゲートウェイプロトコル

Outpost は、サービスリンク VLAN を介したサービスリンク接続のために、各 Outpost ネットワークデバイスとローカルネットワークデバイスとの間に外部 BGP (eBGP) ピアリングセッションを確立します。詳細については、「サービスリンク (BGP 接続)」を参照してください。

| Outpost | サービスリンク BGP の要件 |
| --- | --- |
| お客様の Outpost | — Outpost BGP AS 番号 (ASN)。2 バイト (16 ビット) または 4 バイト (32 ビット)。プライベート ASN 範囲 (64512 ~ 65534 または 4200000000 ~ 4294967294) から。<br><br>– インフラストラクチャ CIDR (/26 が必要、2 つの連続する /27 としてアドバタイズされます)。 |

| ローカルネットワークデバイス | サービスリンク BGP の要件 |
| --- | --- |
| #1 | — サービスリンクBGP ピア IP アドレス。 |

| ローカルネットワークデバイス | サービスリンク BGP の要件 |
| --- | --- |
| | サービスリンク BGP ピア ASN。2 バイト (16 ビット) または 4 バイト (32 ビット)。 |
| #2 | — サービスリンクBGP ピア IP アドレス。<br><br>サービスリンク BGP ピア ASN。2 バイト (16 ビット) または 4 バイト (32 ビット)。 |

サービスリンクファイアウォール

UDP と TCP 443 は、ファイアウォールにステートフルにリストされている必要があります。

| プロトコル | ソースポート | 送信元アドレス | 発信先ポート | 送信先アドレス |
| --- | --- | --- | --- | --- |
| UDP | 443 | Outpost サービスリンク /26 | 443 | Outpost リージョンのパブリックルート |
| TCP | 1025-65535 | Outpost サービスリンク /26 | 443 | Outpost リージョンのパブリックルート |

Direct Connect 接続またはパブリックインターネット接続を使用して、Outpost を AWS リージョンに接続し直すことができます。Outpost サービスリンク接続では、ファイアウォールまたはエッジルーターで NAT または PAT を使用できます。サービスリンクの確立は常に Outpost から開始されます。

MTU や 175 ミリ秒のレイテンシーなどのサービスリンク要件の詳細については、「サービスリンクを介した接続」を参照してください。

ローカルゲートウェイボーダーゲートウェイプロトコル

Outpost は、ローカルネットワークからローカルゲートウェイへの接続のために、各 Outpost ネットワークデバイスからローカルネットワークデバイスへの eBGP ピアリングセッションを確立します。詳細については、「ローカルゲートウェイの BGP 接続」を参照してください。

| Outpost | ローカルゲートウェイ BGP の要件 |
| --- | --- |
| お客様の Outpost | — Outpost BGP AS 番号 (ASN)。2 バイト (16 ビット) または 4 バイト (32 ビット)。プライベート ASN 範囲 (64512 ~ 65534 または 4200000000 ~ 4294967294) から。<br><br>— 広告に使用する CoIP CIDR (パブリックまたはプライベート、最小 /26)。 |

| ローカルネットワークデバイス | ローカルゲートウェイ BGP の要件 |
| --- | --- |
| #1 | — ローカルゲートウェイ BGP ピア IP アドレス。<br><br>– ローカルゲートウェイ BGP ピア ASN。 2 バイト (16 ビット) または 4 バイト (32 ビット)。 |
| #2 | — ローカルゲートウェイ BGP ピア IP アドレス。<br><br>– ローカルゲートウェイ BGP ピア ASN。 2 バイト (16 ビット) または 4 バイト (32 ビット)。 |

# 電源

Outposts 電源シェルフは 5 kVA、10 kVA、または 15 kVA の 3 つの電源構成をサポートしています。電源シェルフの構成は、Outpost キャパシティの合計消費電力によって異なります。たとえば、Outpost リソースの最大消費電力が 9.7 kVA の場合、10 kVA の電力構成を提供する必要があります。つまり、L6-30P または IEC309 を 4 本使用し、2 本を S1 に、冗長単相電源用に 2 本を S2 に接続します。3 つの電源構成を次の 2 つ目の表で説明します。

さまざまな Outpost リソースの消費電力要件を確認するには、https://console.aws.amazon.com/outposts/ の AWS Outposts コンソールでカタログを参照を選択します。

| 要件 | の仕様 |
| --- | --- |
| AC ライン電圧 | 単相 208 ~ 277 VAC (50 または 60 Hz)<br><br>三相:<br><br>• 208 ~ 250 VAC (デルタ接続)、50 ~ 60 Hz<br>• 346 ~ 480 VAC (スター接続)、50 ~ 60 Hz |
| 消費電力 | 5 kVA (4 kW)、10 kVA (9 kW)、または 15 kVA (13 kW) |
| AC 保護 (アップストリーム電源ブレーカー) | 1N 入力 (非冗長) と 2N 入力 (冗長) の両方: 30 A、32 A、または 50 A (D カーブまたは K カーブの回路ブレーカー付き)。<br><br>2N 入力 (冗長) のみ: C カーブ、D カーブ、または K カーブのサーキットブレーカー。<br><br>B カーブ以下はサポートされていません。 |
| AC インレットタイプ (レセプタクル) | 単相 3XL6-30P、P+P+E、30A または 3xiEC60309 P+N+E、IP67、32A プラグ<br><br>三相、ワイ 1XIEC60309、3P+N+E、IP67、クロックポジション 7、30A プラグまたは 1xiEC60309、 3P+N+E、IP67、クロックポジション 6、32A プラグ<br><br>三相、デルタ 1xNEMA ツイストロック Hubbell CS8365C、3P+E、センターグラウンド、50A プラグ<br><br>**Note**<br>ベストプラクティスは、IP67 プラグと IP67 レセプタクルを組み合わせることです。それが不可能な場合は、IP67 プラグは IP44 レセプタクルと接続します。プラグとソケットを組み合わせた場合の定格は、下位定格 (IP44) になります。 |
| ホイップの長さ | 10.25 フィート (3 メートル) |

| 要件 | の仕様 |
| --- | --- |
| Whip - ラックケーブル入力 | ラックの上または下から |

電源シェルフには S1 と S2 の 2 つの入力があり、次のように設定できます。

| | 冗長、単相 | 冗長、三相 | 単相 | 三相 |
| --- | --- | --- | --- | --- |
| 5 kVA | L6-30P または IEC309 を 2 本使用。1 本を S1 に、もう 1 本を S2 に接続 | AH530P7W、AH532P6W、または CS8365C を 2 本使用。1 本を S1 に、もう 1 本を S2 に接続 | 提供されていません | AH530P7W、AH532P6W、または CS8365C のいずれか 1 本を S1 に接続 |
| 10 kVA | L6-30P または IEC309 を 4 本使用。2 本を S1 に、2 本を S2 に接続 | | L6-30P または IEC309 を 2 本使用。2 本を S1 に接続 | |
| 15 kVA | L6-30P または IEC309 を 6 本使用。3 本を S1 に、3 本を S2 に接続 | | L6-30P または IEC309 を 3 本使用。3 本を S1 に接続 | |

前述のように AWS が提供する AC ホイップに代替電源プラグを取り付ける必要がある場合は、次の点を考慮してください。

- 新しいプラグタイプに合わせるための AC ホイップの改造は、認定電気技師に依頼してください。
- 設置は、該当する国、地域の安全要件をすべて満たし、必要に応じて電気安全の検査を受ける必要があります。
- お客様は、AC ホイッププラグの変更を AWS 担当者に通知する必要があります。リクエストに応じて、変更に関する情報を提供します AWS。また、管轄権を有する当局が発行した安全検査記録もすべて含めてください。これは、 AWS 従業員に機器の作業を行わせる前に、設置の安全性を検証するための要件です。

# 注文の履行

注文を満たすために、 AWS はお客様と一緒に日付と時刻をスケジュールします。インストール前に確認または提供するアイテムのチェックリストも届きます。

AWS インストールチームは、スケジュールされた日時に到着します。ラックを指定された位置に配置します。ラックへの電気接続と設置は、お客様および電気技師が行います。

電気設備およびそれらの設備への変更は、適用されるすべての法律、規範、およびベストプラクティスに従って、認定電気技師が行うようにする必要があります。Outpost ハードウェアまたは電気設備に変更を加える前に、 AWS から書面による承認を取得する必要があります。お客様は、コンプライアンスと変更の安全性を検証する AWS ドキュメントを に提供することに同意します。 AWS は、Outpost の電気設備や施設の電気配線、または変更によって生じるリスクについて責任を負いません。Outposts ハードウェアにその他の変更を加えてはいけません。

チームは、お客様が提供するアップリンクを介して Outposts ラックのネットワーク接続を確立し、ラックの容量を構成します。

Outposts ラックの Amazon EC2 および Amazon EBS の容量が AWS アカウントから利用できることを確認すれば、インストールは完了です。

# Outpost ACE ラックのサイト要件

> **Note**
>
> ACE ラックが必要な場合にのみ適用されます。

集約、コア、エッジ (ACE) ラックは、複数ラックの Outpost のデプロイにおけるネットワーク集約ポイントとして機能します。コンピューティングラックが 4 架以上ある場合は、ACE ラックを設置する必要があります。コンピューティングラックが 4 架未満であっても、今後 4 架以上のラックに拡張する予定がある場合は、ACE ラックを設置することをお勧めします。

ACE ラックを設置するには、Outposts ラックのサイト要件 に記載されている要件に加えて、このセクションの要件を満たす必要があります。

> **Note**
>
> ACE ラックは完全には囲まれておらず、フロントドアやリアドアは含まれていません。

## 施設

以下は、ACE ラックの設備要件です。

- 電源 - すべての ACE ラックには 10 kVA 単相 (AA+BB、IEC60309 または L6-30P ホイップコネクタタイプ) の電源が付属しています。
- 重量サポート - ACE ラックの重量は 320 kg (705 lbs) です。
- スペースのゆとり/サイズ - ACE ラックの高さは 203 cm (80 インチ)、幅 61 cm (24 インチ)、奥行きは 107 cm (42 インチ) です。

  ACE ラックにケーブル管理アームがある場合、ラックの幅は 91.5 cm (36 インチ) です。

## ネットワーク

以下は、ACE ラックのネットワーク要件です。ACE ラックと Outposts ネットワークデバイス、オンプレミスネットワークデバイス、および Outposts ラックとの接続方法については、「ACE ラック接続」を参照してください。

- ラックネットワーク要件 - 以下の変更を除き、ネットワーク準備チェックリスト および Outposts ラックのローカルネットワーク接続 セクションに記載されている要件を満たしていることを確認します。
  - ACE ラックには、アップストリームデバイスに接続する 4 台のネットワークデバイスがあり、Outposts ラック 1 架につき 2 台であるのとは異なります。
  - ACE ラックは 1 Gbps アップリンクをサポートしていません。
- アップリンク速度 - 10 Gbps、40 Gbps、または 100 Gbps の速度のアップリンクを利用できます。サービスリンク接続の推奨帯域幅については、「サービスリンクの推奨帯域幅」を参照してください。

> **Important**
>
> ACE ラックは 1 Gbps アップリンクをサポートしていません。

- ファイバー - ルーセントコネクタ (LC) を使用したシングルモードファイバー (SMF)、またはルーセントコネクタ (LC) を使用したマルチモードファイバー (MMF) を使用できます。サポートされているファイバーの種類と光学規格の全リストについては、「アップリンク速度、ポート、ファイバー」を参照してください。
- アップストリームデバイス - 2 台または 4 台のアップストリームデバイスを用意してください。スイッチでもルーターでもかまいません。
- サービス VLAN とローカルゲートウェイ VLAN - 4 台の ACE ネットワークデバイスごとに、サービス VLAN と異なるローカルゲートウェイ VLAN を用意する必要があります。サービス VLAN とローカルゲートウェイ VLAN の 2 つの異なる VLAN のみを用意するか、サービス VLAN と LGW VLAN の両方で各 ACE ネットワークデバイスに異なる VLAN を設けて、合計 8 つの異なる VLAN を用意するかを選択できます。リンク集約グループ (LAG) と VLAN の使用方法の詳細については、「リンクアグリゲーション」および「仮想 LAN」を参照してください。
- サービスリンクとローカルゲートウェイ VLAN の CIDR と IP アドレス - /30 または /31 の CIDR を持つ ACE ネットワークデバイスごとに専用サブネットを割り当てることをお勧めします。代わりに、各サービス VLAN およびローカルゲートウェイ VLAN に 1 つの /29 サブネットを割り当てることもできます。どちらの場合も、ACE ネットワークデバイスが使用する IP アドレスを指定する必要があります。詳細については、「ネットワークレイヤー接続」を参照してください。
- サービスリンク VLAN およびローカルゲートウェイ VLAN の顧客および Outpost の BGP AS 番号 (ASN) - Outpost は、サービスリンク VLAN を介したサービスリンク接続用に、各 ACE ラックデバイスとローカルネットワークデバイス間の外部 BGP (eBGP) ピアリングセッションを確立します。また、ローカルネットワークからローカルゲートウェイへの接続のために、各 ACE ネットワークデバイスからローカルネットワークデバイスへの eBGP ピアリングセッションを確立しま

す。詳細については、「サービスリンク (BGP 接続)」および「ローカルゲートウェイの BGP 接続」を参照してください。

> **Important**
>
> サービスリンクインフラストラクチャサブネット - Outposts のインストールに含まれるコンピューティングラックごとに、サービスリンクインフラストラクチャサブネット (/26 であること) が必要です。

## 電源

以下、ACE ラックの電源要件です。

| 要件 | の仕様 |
| --- | --- |
| AC ライン電圧 | 単相 200～240 VAC (50 または 60 Hz) |
| 消費電力 | 10 kVA 単相 (AA+BB) |
| AC 保護 (アップストリーム電源ブレーカー) | 2N 入力 (冗長) のみ: C カーブ、D カーブ、または K カーブのサーキットブレーカー。<br><br>B カーブ以下はサポートされていません。 |
| AC インレットタイプ (レセプタクル) | IEC60309 または L6-30P ホイップコネクタタイプ。 |

# Outposts ラックの使用開始

まず、Outposts ラックを注文します。Outpost 機器の設置が完了したら、Amazon EC2 インスタンスを起動し、オンプレミスネットワークへの接続を設定します。

タスク

- Outposts ラックの注文を作成する
- Outposts ラックでインスタンスを起動します。
- の Amazon EC2 を最適化する AWS Outposts

# Outposts ラックの注文を作成する

の使用を開始するには AWS Outposts、Outpost を作成し、Outpost 容量を注文する必要があります。

前提条件

- Outposts ラックの利用可能な構成を確認してください。
- Outpost サイトは Outpost 機器の物理的な場所です。容量を注文する前に、お使いのサイトが要件を満たしていることを確認してください。詳細については、「Outposts ラックのサイト要件」を参照してください。
- AWS エンタープライズサポートプランまたは AWS エンタープライズオンランプサポートプランが必要です。
- Outposts サイトの作成、Outpost の作成、注文 AWS アカウント に使用する を決定します。このアカウントに関連付けられている E メールをモニタリングして、 からの情報を確認します AWS。

タスク

- ステップ 1: サイトを作成する
- ステップ 2: Outpost を作成する
- ステップ 3: 注文を確定する
- ステップ 4: インスタンスキャパシティを変更する
- 次の手順

# ステップ 1: サイトを作成する

サイトを作成し、営業住所を指定します。運用アドレスは、Outposts ラックの物理的な場所です。

前提条件

- 営業住所を決定してください。

サイトを作成するには

1. にサインインします AWS。
2. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
3. 親を選択するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
4. ナビゲーションペインで、[サイト] を選択します。
5. [サイトの作成] を選択します。
6. [サポートされているハードウェアタイプ] で、[ラックとサーバー] を選択します。
7. サイトの名前、説明、および営業住所を入力します。
8. [サイト詳細] では、サイトに関する要求された情報を入力します。
   - 最大重量 - このサイトがサポートできる最大のラック重量 (ポンド)。
   - 消費電力 - ラックについてのハードウェア設置位置で利用可能な消費電力 (kVA)。
   - 電源オプション - ハードウェアに供給できる電力オプション。
   - 電源コネクタ - AWS がハードウェアへの接続に供給することになっている電力コネクタ。
   - 電力の引込み - 給電がラックの上からか下からかを示します。
   - アップリンク速度 - ラックがリージョンへの接続でサポートすることになっているアップリンク速度 (Gbps)。
   - アップリンクの数 - ラックをネットワークに接続するのに使用する各 Outpost ネットワーキングデバイスのアップリンクの数。
   - ファイバーのタイプ - ラックをネットワークに接続するのに使用するファイバーのタイプ。
   - 光学規格 - ラックをネットワークに接続するのに使用する光学規格のタイプ。
9. (オプション) サイトノートには、 がサイトについて知る AWS のに役立つその他の情報を入力します。
10. 施設の要件を読み、[施設の要件を読みました] を選択します。

11. [サイトを作成] を選択します。

## ステップ 2: Outpost を作成する

ラックの Outpost を作成します。以降、注文を行う際に、この Outpost を指定できます。

前提条件

- サイトに関連付ける AWS アベイラビリティーゾーンを決定します。

Outpost を作成するには

1. ナビゲーションペインで、[Outpost] を選択してください。
2. [Outpost の作成] を選択します。
3. [ラック] を選択します。
4. Outpost の名前と説明を入力します。
5. Outpost のアベイラビリティーゾーンを選択します。
6. (オプション) プライベートな接続を構成するには、[プライベート接続を使用] を選択します。Outpost と同じ およびアベイラビリティーゾーン内の VPC AWS アカウント とサブネットを選択します。詳細については、「the section called “前提条件”」を参照してください。

   > **Note**
   >
   > Outpost のプライベート接続を削除する必要がある場合は、AWS サポート センターに連絡する必要があります。

7. [サイト ID] には、自身のサイトを選択します。
8. [Outpost の作成] を選択します。

> **Note**
>
> 注文完了後、Outpost の AZ アンカーまたは物理的な場所を変更することはできません。

# ステップ 3: 注文を確定する

必要な Outposts ラックの注文を確定してください。

> **Important**
>
> 送信した後は注文を編集できなくなるため、送信する前にすべての詳細を注意深く確認してください。注文を変更する必要がある場合は、 AWS アカウントマネージャーにお問い合わせください。

前提条件

- 注文の支払い方法を決定してください。全額前払い、一部前払い、前払いなしで支払うことができます。全額を前払いしないことを選択した場合は、契約期間にわたって月額料金が発生します。

  価格設定には、配送、インストール、インフラストラクチャサービス保守、、およびソフトウェアパッチとアップグレードが含まれます。
- 配送先住所がサイトに指定した営業住所と異なるかどうかを確認してください。

注文するには

1. ナビゲーションペインから、注文を選択します。
2. [発注する] を選択します。
3. [サポートされているハードウェアタイプ] で、[ラック] を選択します。
4. 設定で、必要な各リソースの数量を指定します。使用可能な設定が容量のニーズを満たすことができない場合は、 AWS サポート センターに連絡してカスタム容量設定をリクエストしてください。
5. ストレージ:
   - Amazon EBS ストレージ階層を選択します。
   - (オプション) Amazon S3 ストレージ階層を選択します。
6. [次へ] を選択します。
7. [既存の Outpost を使用] を選択し、Outpost を選択します。
8. [次へ] を選択します。
9. 運用サイトの担当者の名前と番号を入力します。

10. 配送先住所を指定します。新しい住所を指定するか、サイトの営業住所を選択することができます。営業住所を選択した場合は、その後サイトの営業住所を変更しても既存の注文に反映されないことに注意してください。既存の注文の配送先の名前や住所を変更する必要がある場合は、AWS アカウントマネージャーにお問い合わせください。
11. サイトの詳細については、各フィールドにサイト情報を指定します。
12. 施設の要件を確認します。
13. 選択 施設の要件を読みました。
14. [次へ] を選択します。
15. 契約期間と支払いオプションを選択します。
16. [次へ] を選択します。
17. [確認と注文] ページで、情報が正しいことを確認し、必要に応じて編集します。送信した後は注文を編集できなくなります。
18. [発注する] を選択します。

## ステップ 4: インスタンスキャパシティを変更する

Outpost は、 AWS リージョンのアベイラビリティーゾーンのプライベート拡張機能として、サイトに AWS コンピューティングとストレージ容量のプールを提供します。Outpost で使用できるコンピューティングとストレージの容量は限られており、 がサイトに AWS インストールするラックのサイズと数によって決まるため、初期ワークロードの実行、将来の成長への対応、サーバーの障害とメンテナンスイベントを軽減するための追加の容量に必要な AWS Outposts 容量に対する Amazon EC2、Amazon EBS、Amazon S3 の量を決定できます。

新規の各 Outpost 注文のキャパシティは、デフォルトのキャパシティ設定で設定されています。デフォルトの設定を変換して、ビジネスニーズに合わせたさまざまなインスタンスを作成できます。これを行うには、キャパシティタスを作成し、インスタンスのサイズと数量を指定して、キャパシティタスを実行して変更を実装します。

> **Note**
>
> - Outposts の注文後にインスタンスサイズの数量を変更できます。
> - インスタンスのサイズと数量は、Outpost レベルで定義します。
> - インスタンスは、ベストプラクティスに基づいて自動的に配置されます。

インスタンスキャパシティを変更するには

1. [AWS Outposts ] コンソールの の左側のナビゲーションペインから、[キャパシティタスク] を選択します。
2. [キャパシティタスク] ページで、[キャパシティタスクを作成] を選択します。
3. [使用開始] ページで [注文] をクリックします。
4. キャパシティを変更するには、コンソールのステップを使用するか、JSON ファイルをアップロードします。

Console steps

1. Outpost 容量設定の変更を選択します。
2. [次へ] を選択します。
3. [インスタンスキャパシティを設定] ページで、各インスタンスタイプには、事前に選択された最大数を含む 1 つのインスタンスサイズが表示されます。インスタンスサイズを追加するには、[インスタンスサイズを追加] を選択します。
4. インスタンスの数量を指定し、そのインスタンスサイズに表示されるキャパシティを書き留めます。
5. 各インスタンスタイプのセクションの最後に、キャパシティが超過しているか不足しているかを通知するメッセージが表示されます。インスタンスサイズまたは数量レベルで調整して、使用できる合計キャパシティを最適化します。
6. 特定のインスタンスサイズのインスタンス数を最適化 AWS Outposts するようにリクエストすることもできます。そのためには、次の操作を行います。

   a. [インスタンスサイズ] を選択します。

   b. 関連するインスタンスタイプのセクションの最後で、[オートバランス] を選択します。
7. インスタンスタイプごとに、少なくとも 1 つのインスタンスサイズに対してインスタンス数量が指定されていることを確認します。
8. [次へ] を選択します。
9. [確認して作成] ページで、リクエストする更新を確認します。
10. Create. AWS Outposts creates キャパシティタスクを選択します。
11. [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

> **Note**
>
> - AWS Outposts は、キャパシティタスクの実行を有効にするために、1 つ以上の実行中のインスタンスを停止するよう要求することがあります。これらのインスタンスを停止すると、 AWS Outposts はタスクを実行します。
> - 注文完了後にキャパシティを変更する必要がある場合は、AWS サポート センターに連絡して変更してください。

Upload a JSON file

1. [キャパシティ構成をアップロード] を選択します。
2. [次へ] を選択します。
3. [キャパシティ構成計画をアップロード] ページで、インスタンスタイプ、サイズ、数量を指定する JSON ファイルをアップロードします。

   Example

   JSON ファイルの例:

```
{
    "InstancePools": [
        {
            "InstanceType": "c5.24xlarge",
            "Count": 1
        },
        {
            "InstanceType": "m5.24xlarge",
            "Count": 2
        }
    ]
}
```

4. [キャパシティ構成計画] セクションの JSON ファイルの内容を確認します。
5. [次へ] を選択します。
6. [確認して作成] ページで、リクエストする更新を確認します。
7. 「Create. AWS Outposts creates a capacity task」を選択します。

8. [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

> **Note**
>
> - AWS Outposts は、キャパシティタスクの実行を有効にするために、1 つ以上の実行中のインスタンスを停止するよう要求することがあります。これらのインスタンスを停止すると、 AWS Outposts はタスクを実行します。
> - 注文完了後にキャパシティを変更する必要がある場合は、AWS サポート センターに連絡して変更してください。
> - 問題のトラブルシューティングについては、「容量タスクの問題のトラブルシューティング」を参照してください。

## 次の手順

コンソールを使用して注文のステータスを表示できます AWS Outposts 。注文の初期ステータスは [注文を受け取りました] です。注文についてご質問がある場合は、AWS サポート センターにお問い合わせください。

注文を満たすために、 AWS はお客様と一緒に日付と時刻をスケジュールします。

インストール前に確認または提供するアイテムのチェックリストも届きます。 AWS インストールチームは、スケジュールされた日時に到着します。チームがラックを指定された位置まで運び、電気技師はラックに電力を供給できます。チームは、お客様が提供するアップリンクを介してラックのネットワーク接続を確立し、ラックの容量を構成します。Outpost の Amazon EC2 および Amazon EBS 容量が AWS アカウントから使用可能であることを確認すると、インストールは完了です。

# Outposts ラックでインスタンスを起動します。

Outpost がインストールされ、計算およびストレージの容量が使用可能になったら、リソースを作成することで開始できます。Outpostサブネットを使用して、Outpost上で Amazon EC2 インスタンスを起動し、Amazon EBS ボリュームを作成してください。Outpost で Amazon EBS ボリュームのスナップショットを作成することもできます。詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS local snapshots on AWS Outposts」を参照してください。

前提条件

Outpost は、自分のサイトにインストールする必要があります。詳細については、「Outposts ラックの注文を作成する」を参照してください。

タスク

- ステップ 1: VPC を作成する
- ステップ 2: サブネットとカスタムルートテーブルを作成する
- ステップ 3: ローカルゲートウェイ接続を構成する
- ステップ 4: オンプレミスネットワークを設定する
- ステップ 5: Outpost 上でインスタンスを起動
- ステップ 6: 接続をテストする

## ステップ 1: VPC を作成する

AWS リージョン内の任意の VPC を Outpost に拡張できます。既に使用可能な VPC がある場合は、この手順をスキップしてください。

Outpost の VPC を作成するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. Outposts ラックと同じリージョンを選択します。
3. ナビゲーションペインで [VPC]、[VPC を作成] の順に選択します。
4. [VPC のみ] を選択します。
5. (オプション) [名前タグ] に VPC の名前を入力します。
6. [IPv4 CIDR ブロック]では、[IPv4 CIDR 手動入力] を選択し、[IPv4 CIDR] テキストボックスに VPC の IPv4 アドレス範囲を入力します。

   > **Note**
   >
   > ダイレクト VPC ルーティングを使用する必要がある場合は、オンプレミスネットワークで使用する IP 範囲と重複しない CIDR 範囲を指定します。

7. [IPv6 CIDR ブロック] は、[IPv6 CIDR ブロックなし] のままにしておきます。
8. [テナンシー] では、[デフォルト] を選択します。
9. (オプション) VPC にタグを追加するには、[タグを追加] を選択し、キーとタグ値を入力します。

10. [Create VPC ( VPC の作成 ) ] を選択します。

## ステップ 2: サブネットとカスタムルートテーブルを作成する

Outpost サブネットを作成して、Outpost のホームとなる AWS リージョン内の任意の VPC に追加できます。これを実行すると、VPC は Outpost に含まれます。詳細については、「ネットワークコンポーネント」を参照してください。

> **Note**
>
> 別の によって共有されている Outpost サブネットでインスタンスを起動する場合は AWS アカウント、ステップ 5: Outpost でインスタンスを起動するに進みます。

### 2a: Outpost サブネットを作成する

Outpost サブネットを作成するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで [Outposts] を選択します。
3. Outpost を選択し、[アクション]、[サブネットの作成] の順に選択します。Amazon VPC コンソールでサブネットを作成するようにリダイレクトされます。Outpost はお客様のために選択し、Outpost がホストされているアベイラビリティゾーンを選択します。
4. [VPC] を選択します。
5. [サブネット設定] で、サブネットに名前を付け (オプション)、サブネットの IP アドレス範囲を指定します。
6. [サブネットの作成] を選択します。
7. (オプション) Outpost サブネットを識別しやすくするには、[サブネット] ページの [Outpost ID] 列を有効にします。列を有効にするには、[設定] アイコンを選択して、[Outpost ID] を選択し、[確認] を選択します。

### 2b: カスタムルートテーブルを作成する

ローカルゲートウェイへのルートを持つカスタムルートテーブルを作成する手順は以下の通りです。アベイラビリティーゾーンのサブネットと同じルートテーブルを使用することはできません。

カスタムルートテーブルを作成するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、[ルートテーブル] を選択します。
3. [ルートテーブルの作成] を選択します。
4. (オプション) [Name] (名前) には、ルートテーブルの名前を入力します。
5. [VPC] で、ユーザーの VPC を選択します。
6. (オプション) タグを追加するには、[Add new tag] (新しいタグを追加) を選択し、タグキーとタグ値を入力します。
7. [ルートテーブルの作成] を選択します。

2c: Outpost サブネットとカスタムルートテーブルを関連付ける

ルートテーブルのルートを特定のサブネットに適用するには、ルートテーブルをサブネットに関連付ける必要があります。ルートテーブルは複数のサブネットに関連付けることができます。ただし、サブネットは一度に 1 つのルートテーブルにのみ関連付けることができます。どのテーブルにも明示的に関連付けられていないサブネットは、デフォルトでメインルートテーブルに暗示的に関連付けられています。

Outpost サブネットとカスタムルートテーブルを関連付けるには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインから、[ルートテーブル] を選択します。
3. [Subnet Associations] (サブネットの関連付け) タブで、 [Edit subnet associations] (サブネットの関連付けの編集) を選択します。
4. ルートテーブルに関連付けるサブネットのチェックボックスをオンにします。
5. [Save associations] (関連付けを保存する) を選択します。

## ステップ 3: ローカルゲートウェイ接続を構成する

ローカルゲートウェイ (LGW) 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 の詳細については、「ローカルゲートウェイ」を参照してください。

Outposts サブネット内のインスタンスとローカルネットワーク間の接続を提供するには、以下のタスクを完了する必要があります。

3a. カスタムローカルゲートウェイルートテーブルを作成する

ローカルゲートウェイのカスタムルートテーブルを作成する手順は以下のとおりです。

カスタムローカルゲートウェイルートテーブルを作成するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
3. ナビゲーションペインで、[ローカルゲートウェイのルートテーブル] をクリックします。
4. [ローカルゲートウェイルートテーブルの作成] を選択します。
5. (オプション) [Name] (名前) には、ルートテーブルの名前を入力します。
6. [ローカルゲートウェイ] では、ローカルゲートウェイを選択します。
7. [モード] では、オンプレミスネットワークとの通信モードを選択します。
   - インスタンスのプライベート IP アドレスを使用するには、[ダイレクト VPC ルーティング] を選択します。
   - 顧客所有の IP アドレスプール使用するには、[CoIP] を選択します。詳細については、CoIP プールの作成」を参照してください。
8. (オプション) タグを追加するには[新しいタグを追加] を選択し、タグキーとタグ値を入力してください。
9. [ローカルゲートウェイルートテーブルの作成] を選択します。

3b: VPC をカスタムルートテーブルに関連付ける

VPC をローカルゲートウェイのルートテーブルに関連付ける手順は以下のとおりです。デフォルトでは関連付けられていません。

VPC とローカルゲートウェイルートテーブルを関連付けるには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
3. ナビゲーションペインで、[ローカルゲートウェイのルートテーブル] をクリックします。
4. ルートテーブルを選択し、[アクション]、[VPC の関連付け] を選択します。
5. [VPC ID] には、ローカルゲートウェイルートテーブルに関連付ける VPC を選択します。

6. (オプション) タグを追加するには[新しいタグを追加] を選択し、タグキーとタグ値を入力してください。
7. [Associate VPC] を選択します。

### 3c: Outpost サブネットルートテーブルにルートエントリを追加する

Outpost サブネットルートテーブルにルートエントリを追加して、Outpost サブネットとローカルゲートウェイ間のトラフィックを有効にします。

VPC 内の Outpost サブネットにはローカルゲートウェイルートテーブルに関連付けられており、ルートテーブルの Outpost ローカルゲートウェイ ID の追加のターゲットタイプを含めることができます。送信先アドレス 172.16.100.0/24 のトラフィックをローカルゲートウェイ経由で顧客のネットワークにルーティングする場合を考えます。これを行うには、Outpost サブネットルートテーブルを編集し、送信先ネットワークとローカルゲートウェイをターゲットとする次のルートを追加します。

| ルーティング先 | ターゲット |
| --- | --- |
| 172.16.100.0/24 | `lgw-id` |

ローカルゲートウェイをターゲットとするルートエントリをサブネットルートテーブルに追加するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、[ルートテーブル] を選択し、2b: カスタムルートテーブルを作成するに作成したルートテーブルを選択します。
3. [アクション]、[ルートを編集] の順に選択します。
4. ルートを追加するには、[ルートの追加] を選択します。
5. [送信先] には、顧客ネットワークへの送信先 CIDR ブロックを入力します。
6. [ターゲット] で、[Outpost ローカルゲートウェイ ID] を選択します。
7. [Save changes] (変更の保存) をクリックします。

### 3d: カスタムルートテーブルを VIF グループに関連付けてローカルゲートウェイルーティングドメインを作成する

VIF グループは仮想インターフェイス (VIF) を論理的にグループ化したものです。ローカルゲートウェイルートテーブルを VIF グループに関連付けて、ローカルゲートウェイルーティングドメインを作成します。

カスタムルートテーブルを VIF グループに関連付けるには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
3. ナビゲーションペインで、ネットワーキングを選択し、次に LGW ルーティングドメインを選択します。
4. LGW ルーティングドメインの作成 を選択します。
5. ローカルゲートウェイルーティングドメインの名前を入力します。
6. ローカルゲートウェイ、ローカルゲートウェイ VIF グループ、ローカルゲートウェイルートテーブルを選択します。
7. LGW ルーティングドメインの作成 を選択します。

### 3e: ルートテーブルにルートエントリを追加する

ローカルゲートウェイルートテーブルを編集して、VIF グループをターゲット、オンプレミスサブネット CIDR 範囲 (または 0.0.0.0/0) を送信先とする静的ルートを追加します。

| ルーティング先 | ターゲット |
| --- | --- |
| 172.16.100.0/24 | `VIF-Group-ID` |

LGW ルートテーブルにルートエントリを追加するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで、[ローカルゲートウェイのルートテーブル] をクリックします。
3. ローカルゲートウェイのルートテーブルを選択してから、[アクション]、[ルートを編集] の順に選択します。
4. [Add Rule] (ルートの追加) を選択します。

5. [送信先] に、送信先 CIDR ブロック、単一の IP アドレス、またはプレフィックスリストの ID を入力します。
6. [ターゲット] で、ローカルゲートウェイの ID を選択します。
7. [ルーター保存] を選択してください。

3f: (オプション) 顧客所有の IP アドレスをインスタンスに割り当てる。

3a. カスタムローカルゲートウェイルートテーブルを作成する で顧客所有の IP (CoIP) アドレスプールを使用するように Outposts を設定した場合、CoIP アドレスプールから Elastic IP アドレスを割り当て、その Elastic IP アドレスをインスタンスに関連付ける必要があります。詳細については、「カスタマー所有 IP アドレス」を参照してください。

ダイレクト VPC ルーティング (DVR) を使用するように Outposts を設定した場合は、このステップをスキップします。

顧客所有の共有 IP アドレス プール

顧客所有の共有 IP アドレス プールを使用する場合は、構成を開始する前にプールを共有する必要があります。顧客所有の IPv4 アドレスを共有する方法については、「the section called “Outpost リソースの共有”」を参照してください。

## ステップ 4: オンプレミスネットワークを設定する

Outpost は、各 Outpost ネットワーキングデバイス (OND) から顧客のローカルネットワークデバイス (CND) への外部 BGP ピアリングを確立し、オンプレミスネットワークから Outposts へのトラフィックの送受信を行います。

詳細については、「Local gateway BGP connectivity」を参照してください。

オンプレミスネットワークから Outpost にトラフィックを送受信するには、以下を確認します。

- 顧客のネットワークデバイスでは、ローカルゲートウェイ VLAN の BGP セッションは、ネットワークデバイスではアクティブ状態になります。
- オンプレミスから Outposts に移行するトラフィックについては、Outposts から BGP アドバタイズを CND で受信していることを確認してください。これらの BGP アドバタイズには、オンプレミスネットワークがオンプレミスから Outpost にトラフィックをルーティングするために使用する必要があるルートが含まれています。そのため、Outposts とオンプレミスリソースの間でネットワークが適切なルーティングであることを確認してください。

- Outposts からオンプレミスネットワークへのトラフィックについては、CNDs がオンプレミスネットワークサブネットの BGP ルートアドバタイズを Outposts (または 0.0.0.0/0) に送信していることを確認します。代わりに、デフォルトのルート (0.0.0.0/0 など) を Outposts にアドバタイズすることもできます。CND によってアドバタイズされるオンプレミスサブネットは、3e: ルートテーブルにルートエントリを追加する で設定した CIDR 範囲と同じか、範囲に含まれる必要があります。

例: ダイレクト VPC モードでの BGP アドバタイズ

ダイレクト VPC モードで構成された Outpost があり、2 台の Outpost ラックネットワークデバイスがローカルゲートウェイ VLAN で 2 つの顧客のローカルネットワークデバイスに接続されているというシナリオを考えます。以下が設定されています。

- CIDR ブロック 10.0.0.0/16 を持つ VPC。
- CIDR ブロック 10.0.3.0/24 の VPC 内の Outpost サブネット。
- CIDR ブロック 172.16.100.0/24 のオンプレミスネットワーク内のサブネット
- Outposts は Outpost サブネットの (例: 10.0.3.0/24) 上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通信します。

このシナリオでは、アドバタイズされたルートは次のとおりです。

- ローカルゲートウェイから顧客のデバイスへは 10.0.3.0/24 です。
- 顧客のデバイスから Outpost ローカルゲートウェイへは 172.16.100.0/24 です。

その結果、ローカルゲートウェイは、送信先ネットワーク 172.16.100.0/24 の送信トラフィックを顧客のデバイスに送信します。ネットワーク内の送信先ホストにトラフィックを配信するために、ネットワークのルーティング設定が正しいことを確認します。

BGP セッションの状態とそれらのセッション内のアドバタイズされたルートを確認するために必要な具体的なコマンドと設定については、ネットワークベンダーのドキュメントを参照してください。

トラブルシューティングについては、「AWS Outposts rack network troubleshooting checklist」を参照してください。

例: CoIP モードでの BGP アドバタイズ

2 台の Outpost ラックネットワークデバイスが 1 台の Outpost で、ローカルゲートウェイ VLAN によって 2 台の顧客のローカルネットワークデバイスに接続されているシナリオを考えてみましょう。以下が設定されています。

- CIDR ブロック 10.0.0.0/16 を持つ VPC。
- CIDR ブロック 10.0.3.0/24 の VPC 内のサブネット。
- カスタマー所有 IP プール (10.1.0.0/26)。
- 10.0.3.112 を 10.1.0.2 に関連付ける Elastic IP アドレス関連付け。
- CIDR ブロック 172.16.100.0/24 のオンプレミスネットワーク内のサブネット
- Outpost とオンプレミスネットワーク間の通信では、CoIP Elastic IP を使用して Outpost 内のインスタンスをアドレス指定しますが、VPC CIDR 範囲は使用されません。

このシナリオでは、アドバタイズされたルートは次のとおりです。

- ローカルゲートウェイから顧客のデバイスへは 10.1.0.0/26 です。
- 顧客のデバイスから Outpost ローカルゲートウェイへは 172.16.100.0/24 です。

その結果、ローカルゲートウェイは、送信先ネットワーク 172.16.100.0/24 の送信トラフィックを顧客のデバイスに送信します。ネットワーク内の送信先ホストにトラフィックを配信するために、ネットワークのルーティング設定が正しいことを確認します。

BGP セッションの状態とそれらのセッション内のアドバタイズされたルートを確認するために必要な具体的なコマンドと設定については、ネットワークベンダーのドキュメントを参照してください。

トラブルシューティングについては、「AWS Outposts rack network troubleshooting checklist」を参照してください。

トラブルシューティングについては、「AWS Outposts rack network troubleshooting checklist」を参照してください。

## ステップ 5: Outpost 上でインスタンスを起動

作成した Outpost サブネットまたは共有されている Outpost サブネット内で EC2 インスタンスを起動できます セキュリティグループは、アベイラビリティーゾーンサブネットのインスタンスと同

様に、Outpost サブネットのインスタンスのインバウンドトラフィックとアウトバウンド VPC トラフィックを制御します。Outpost サブネットの EC2 インスタンスに接続するには、アベイラビリティーゾーンサブネットのインスタンスの場合と同様に、インスタンスの起動時にキーペアを指定できます。

### 考慮事項

- 互換性のあるサードパーティーストレージにバックアップされたブロックデータまたはブートボリュームを使用するには、Outposts の EC2 インスタンスで使用するようにこれらのボリュームをプロビジョニングして設定する必要があります。詳細については、「サードパーティーのブロックストレージ」を参照してください。
- プレイスメントグループを作成して、Amazon EC2 が相互依存するインスタンスのグループを Outposts ハードウェアに配置する方法に影響を与えることができます。ワークロードのニーズを満たす配置グループ戦略を選択できます。
- Amazon EBS ボリュームを追加する場合は、gp2 ボリュームタイプを使用する必要があります。
- Outpost が顧客所有の IP (CoIP) アドレス プールを使用するように構成されている場合は、起動するすべてのインスタンスに顧客所有の IP アドレスを割り当てる必要があります。

### Outpost サブネットでインスタンスを起動する

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで [Outposts] を選択します。
3. Outpost を選択し、[アクション、詳細の表示] を選択します。
4. [Outpost の概要] ページで [インスタンスを起動] を選択します。Amazon EC2 コンソールのインスタンス起動ウィザードにリダイレクトされます。Outpost サブネットをお客様のために選択し、Outposts ラックでサポートされているインスタンスタイプのみを表示します。
5. Outposts ラックでサポートされているインスタンスタイプを選択します。グレー表示されたインスタンスは使用できないので注意してください。
6. (オプション) インスタンスをプレイスメントグループで起動するには、[詳細設定] を展開し、[プレイスメントグループ] までスクロールしてください。既存のプレイスメントグループを選択するか、新しいプレイスメントグループを作成できます。
7. (オプション) サードパーティーのデータボリュームを追加できます。
    a. ストレージの設定 を展開します。外部ストレージボリュームの横にある編集 を選択します。

b. Storage Network Protocol で、iSCSI を選択します。

c. イニシエーター IQN を入力し、外部ストレージ配列のターゲット IP アドレス、ポート、IQN を追加します。

8. ウィザードを完了して、Outpost サブネット内でインスタンスを起動してください。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスの起動」を参照してください。

## ステップ 6: 接続をテストする

適切な使用例を使用して接続をテストできます。

ローカルネットワークから Outpost への接続テスト

ローカルネットワーク内のコンピュータから、Outpost インスタンスのプライベート IP アドレスに対して ping コマンドを実行します。

```
ping 10.0.3.128
```

以下は出力の例です。

```
Pinging 10.0.3.128

Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Outpost インスタンスからローカル ネットワークへの接続をテストする

OS に応じて、[ssh] または [rdp] を使用して Outpost インスタンスのプライベート IP アドレスに接続します。Linux インスタンスに接続する方法については、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスに接続する」を参照してください。

インスタンスが実行されたら、ローカルネットワーク内のコンピューターの IP アドレスに対して ping コマンドを実行します。以下の例では、IP アドレスは 172.16.0.130 です。

```
ping 172.16.0.130
```

以下は出力の例です。

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

AWS リージョンと Outpost 間の接続をテストする

AWS リージョンのサブネットでインスタンスを起動します。例えば、run-instances コマンドを使用します。

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

インスタンスの実行後、次の操作を実行します。

1. AWS リージョン内のインスタンスのプライベート IP アドレスを取得します。この情報は、Amazon EC2 コンソールのインスタンスの詳細ページで確認できます。
2. OS に応じて、ssh または rdp を使用して Outpost インスタンスのプライベート IP アドレスへ接続します。
3. Outpost インスタンスから ping コマンドを実行し、 AWS リージョン内のインスタンスの IP アドレスを指定します。

   ```
   ping 10.0.1.5
   ```

   以下は出力の例です。

```
Pinging 10.0.1.5

Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.1.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

顧客所有の IP アドレスの接続例

ローカル ネットワークから Outpost への接続を確立します。

ローカル ネットワーク内のコンピューターから、Outpost インスタンスの顧客所有の IP ping アドレスに対して 1 コマンドを実行します。

```
ping 172.16.0.128
```

以下は出力の例です。

```
Pinging 172.16.0.128

Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Outpost インスタンスからローカル ネットワークへの接続をテストする

OS に応じて、[ssh] または [rdp] を使用して Outpost インスタンスのプライベート IP アドレスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスに接続する」を参照してください。

Outpost インスタンスが実行されたら、ローカルネットワーク内のコンピューターの IP アドレスに対して ping コマンドを実行します。

```
ping 172.16.0.130
```

以下は出力の例です。

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

AWS リージョンと Outpost 間の接続をテストする

AWS リージョンのサブネットでインスタンスを起動します。例えば、run-instances コマンドを使用します。

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

インスタンスの実行後、次の操作を実行します。

1. AWS リージョンインスタンスのプライベート IP アドレス、たとえば 10.0.0.5 を取得します。この情報は、Amazon EC2 コンソールのインスタンスの詳細ページで確認できます。
2. OS に応じて、[ssh] または [rdp] を使用して Outpost インスタンスのプライベート IP アドレスに接続します。
3. Outpost インスタンスから AWS リージョンインスタンスの IP アドレスに ping コマンドを実行します。

```
ping 10.0.0.5
```

以下は出力の例です。

```
Pinging 10.0.0.5

Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.0.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

# の Amazon EC2 を最適化する AWS Outposts

とは対照的に AWS リージョン、Outpost 上の Amazon Elastic Compute Cloud (Amazon EC2) 容量は有限です。注文したコンピューティング能力の総量によって制限されます。このトピックでは、Amazon EC2 の容量を AWS Outpostsで最大限に活用するのに役立つベストプラクティスと最適化戦略を提供します。

内容

- Outposts の専有ホスト
- インスタンスのリカバリを設定する
- Outpost の配置グループ

## Outposts の専有ホスト

Amazon EC2 Dedicated Host は、EC2 インスタンス容量を利用したお客様専用の物理サーバーです。Outpost ではすでに専用のハードウェアが提供されていますが、専有ホストを使用すると、単一のホストに対してソケットごと、コアごと、または VM ごとのライセンス制限のある既存のソフトウェア ライセンスを使用できます。詳細については、「Amazon EC2 ユーザーガイド」の「AWS Outpostsの専有ホスト」を参照してください。

ライセンス以外にも、Outpost の所有者は専有ホストを使用して、次の 2 つの方法で Outpost デプロイ内のサーバーを最適化できます。

- サーバーの容量レイアウトを変更する
- インスタンスの配置をハードウェアレベルで制御する

### サーバーの容量レイアウトを変更する

Dedicated Hosts では、Outpost デプロイ内のサーバーのレイアウトを、 に連絡せずに変更することができます サポート。Outpost の容量を購入するときは、各サーバーが提供する EC2 容量レイアウトを指定します。各サーバーは、インスタンス タイプの単一ファミリーをサポートします。レイアウトでは、単一のインスタンス タイプまたは複数のインスタンス タイプを提供できます。専有ホストを使用すると、最初のレイアウトで選択したものをすべて変更できます。容量全体に対して 1 つのインスタンス タイプをサポートするようにホストを割り当てる場合、そのホストからは 1 つのインスタンス タイプのみを起動できます。次の図は、均一なレイアウトの m5.24xlarge サーバーを示しています。

複数のインスタンス タイプに同じ容量を割り当てることができます。複数のインスタンス タイプをサポートするようにホストを割り当てると、明示的な容量レイアウトを必要としない異種レイアウトが得られます。次の図は、容量最大での異種混合レイアウトの m5.24xlarge サーバーを示しています。

詳細については、「Amazon EC2 ユーザーガイド」の「専有ホストを割り当てる」を参照してください。

### インスタンスの配置をハードウェアレベルで制御する

専有ホストを使用すると、ハードウェアレベルでインスタンスの配置を制御できます。専有ホストの自動配置を使用して、起動するインスタンスについて、特定のホストで起動されるようにするか、設定が合致する任意の利用可能なホストで起動されるようにするかを管理します。ホストアフィニティを使用して、インスタンスと専有ホストの間の関係を確立します。Outposts ラックをお持ちの場合は、これらの専有ホスト機能を使用して、関連するハードウェア障害の影響を最小限に抑えることができます。インスタンスリカバリの詳細については、「Amazon EC2 ユーザーガイド」の「専有ホストの自動配置とホストアフィニティ」を参照してください。

Dedicated Hosts は を使用して共有できます AWS Resource Access Manager。専有ホストを共有すると、Outpost デプロイ内のホストを AWS アカウント全体に分散できます。詳細については、「共有 リソース」を参照してください。

## インスタンスのリカバリを設定する

ハードウェア障害により異常な状態になった Outpost 上のインスタンスは、正常なホストに移行する必要があります。自動リカバリを設定して、インスタンスのステータスチェックに基づいてこの移行を自動的に実行できます。詳細については、「インスタンスの耐障害性」を参照してください。

## Outpost の配置グループ

AWS Outposts はプレイスメントグループをサポートします。配置グループを使用して、基盤となるハードウェア上で起動する相互依存インスタンスのグループを Amazon EC2 が配置する方法に影響を与えます。さまざまな戦略 (クラスター、パーティション、またはスプレッド) を使用して、さまざまなワークロードのニーズを満たすことができます。シングルラック Outpost がある場合は、分散戦略を使用して、ラックではなくホスト全体にインスタンスを配置できます。

### スプレッドプレイスメントグループ

スプレッドプレイスメントグループを使用して、単一のインスタンスを異なるハードウェアに分散します。スプレッドプレイスメントグループでインスタンスを起動すると、インスタンスが同じ機器を共有するときに発生し得る同時障害のリスクが軽減されます。プレイスメントグループは、ラックまたはホスト全体でインスタンスを分散できます。ホストレベルのスプレッドプレイスメントグループは、 でのみ使用できます AWS Outposts。

#### ラックスプレッドレベルのプレイスメントグループ

ラック スプレッド レベル配置グループは、Outpost デプロイメント内のラックと同じ数のインスタンスを保持できます。次の図は、ラック スプレッド レベル配置グループで 3 つのインスタンスを実行している 3 ラック Outpost デプロイメントを示しています。

#### ホストスプレッドレベルのプレイスメントグループ

ホスト スプレッド レベル配置グループは、Outpost デプロイメント内のホストと同じ数のインスタンスを保持できます。次の図は、ホスト スプレッド レベル配置グループで 3 つのインスタンスを実行しているシングル ラック Outpost デプロイメントを示しています。

## パーティションプレイスメントグループ

パーティションプレイスメントグループを使用して、複数のインスタンスをパーティションのあるラックに分散します。各パーティションは複数のインスタンスを保持できます 自動分散を使用して、インスタンスをパーティションに配布したり、インスタンスをターゲットパーティションに展開することができます。次の図は、自動分散を使用したパーティションプレイスメントグループを示しています。

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もできます。次の図は、ターゲットを絞った分散を使用したパーティションプレイスメントグループを示しています。

プレイスメントグループでの作業の詳細については、「Amazon EC2 ユーザーガイド」の「プレイスメントグループ」および「AWS Outpostsのプレイスメントグループ」を参照してください。

AWS Outposts 高可用性の詳細については、AWS Outposts 「高可用性の設計とアーキテクチャに関する考慮事項」を参照してください。

# AWS Outposts AWS リージョンへの接続

AWS Outposts は、サービスリンク接続を介したワイドエリアネットワーク (WAN) 接続をサポートします。

内容



## サービスリンク経由の接続

サービスリンクは、Outposts と AWS リージョン (またはホームリージョン) 間で必要な接続です。これにより、Outposts の管理と AWS 、リージョンとの間のトラフィックの交換が可能になります。サービスリンクは、暗号化された一連の VPN 接続を活用して、ホームリージョンと通信します。

サービスリンク接続が確立されると、Outpost は稼働し、 によって管理されます AWS。サービスリンクによって、以下のトラフィックを円滑化します。

- Outpost と関連付けられた VPC 間のカスタマー VPC トラフィック。
- リソース管理、リソースのモニタリング、ファームウェアとソフトウェアの更新など、Outpost 管理トラフィック。

### サービスリンクの最大送信単位 (MTU) 要件

ネットワーク接続の最大送信単位 (MTU) とは接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。

次の点に注意してください。

- ネットワークは、Outpost と親 AWS リージョンのサービスリンクエンドポイントの間で 1500 バイトの MTU をサポートする必要があります。

- Outposts のインスタンスからリージョンのインスタンスに移動するトラフィックの MTU は 1300 バイトで、パケットオーバーヘッドのために必要な MTU である 1500 バイトよりも低くなります。

## サービスリンクの推奨帯域幅

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、コンピューティングラックごとに少なくとも 500 Mbps の冗長接続を使用し、 AWS リージョンへのサービスリンク接続には最大 175 ミリ秒のラウンドトリップレイテンシーを使用する必要があります。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。サービスリンク接続の最小 500 Mbps と最大往復時間の要件により、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、CloudWatch メトリクスなどの AWS サービスへのアクセスを最適なパフォーマンスで行うことができます。

Outposts サービスのリンク帯域幅要件は、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、リージョンへの Amazon VPC トラフィックなどのワークロード特性

AWS 販売担当者または APN パートナーと相談して、地域内で利用可能なホームリージョンオプションを評価し、ワークロードのサービスリンク帯域幅とレイテンシー要件に関するカスタムレコメンデーションを求めることを強くお勧めします。

## 冗長インターネット接続

Outpost から AWS リージョンへの接続を構築するときは、可用性と回復性を高めるために複数の接続を作成することをお勧めします。詳細については、「Direct Connect の回復性に関する推奨事項」を参照してください。

パブリックインターネットへの接続が必要な場合は、既存のオンプレミスワークロードと同様に、冗長インターネット接続とさまざまなインターネットプロバイダーを使用できます。

## サービスリンクを設定する

次の手順では、サービスリンクのセットアッププロセスについて説明します。

1. Outposts とホーム AWS リージョン間の接続オプションを選択します。パブリック接続またはプライベート接続のいずれかを選択できます。

2. Outposts ラックを注文すると、 は VLAN、IP、BGP、インフラストラクチャサブネット IP を収集するためにお客様に AWS 連絡します。 IPs 詳細については、「ローカルネットワーク接続」を参照してください。
3. インストール時に、 は指定した情報に基づいて Outpost のサービスリンク AWS を設定します。
4. ルーターなどのローカルネットワークデバイスは、BGP 接続を介して各 Outpost ネットワークデバイスに接続するように設定します。サービスリンク VLAN、IP、BGP 接続の詳細については、「ネットワーク」を参照してください。
5. Outposts が AWS リージョンまたはホームリージョンにアクセスできるように、ファイアウォールなどのネットワークデバイスを設定します。 は、サービスリンクインフラストラクチャサブネット IPs AWS Outposts を使用して VPN 接続を設定し、コントロールとデータトラフィックをリージョンと交換します。サービスリンクの確立は常に Outpost から開始されます。

> **Note**
>
> 注文完了後、サービスリンクの設定や接続タイプを変更することはできません。

## サービスリンクのパブリック接続オプション

Outposts とホーム AWS リージョン間のトラフィックのパブリック接続を使用してサービスリンクを設定できます。パブリックインターネットまたは Direct Connect パブリック VIFs を使用できます。

ファイアウォールで AWS リージョンパブリック IPs のみを (0.0.0.0/0 ではなく) 許可リストに登録する場合は、ファイアウォールルールが現在の IP アドレス範囲とup-to-dateであることを確認する必要があります。詳細については、「Amazon VPC ユーザーガイド」の「AWS IP アドレスの範囲」を参照してください。

次の図は、Outposts と AWS リージョン間のサービスリンクパブリック接続を確立するための両方のオプションを示しています。

### オプション 1. インターネット経由のパブリック接続

このオプションでは、 AWS Outposts サービスリンクインフラストラクチャサブネット IPsが、リージョン AWS またはホームリージョンのパブリック IP 範囲にアクセスできる必要があります。ファ

イアウォールなどのネットワークデバイスでは、 AWS リージョンのパブリック IPs または 0.0.0.0/0 を許可リストに登録する必要があります。

### オプション 2. パブリック VIFs を介した Direct Connect パブリック接続

このオプションでは、 AWS Outposts サービスリンクインフラストラクチャサブネット IPsが DX サービス経由でリージョン AWS またはホームリージョンのパブリック IP 範囲にアクセスできる必要があります。ファイアウォールなどのネットワークデバイスでは、 AWS リージョンのパブリック IPs または 0.0.0.0/0 を許可リストに登録する必要があります。

## サービスリンクのプライベート接続オプション

Outposts とホーム AWS リージョン間のトラフィックのプライベート接続を使用してサービスリンクを設定できます。 Direct Connect プライベート VIF またはトランジット VIFs を使用できます。

AWS Outposts コンソールで Outpost を作成するときに、プライベート接続オプションを選択します。手順については、「Outpost の作成」を参照してください。

プライベート接続オプションを選択すると、指定した VPC とサブネットを使用して、Outpost のインストール後にサービスリンク VPN 接続が確立されます。これにより、VPC を介したプライベート接続が可能になり、パブリックインターネットへの露出が最小限に抑えられます。

次の図は、Outposts と AWS リージョン間のサービスリンク VPN プライベート接続を確立するための両方のオプションを示しています。

### 前提条件

Outpost にプライベート接続を設定するには、次の前提条件を満たす必要があります。

- ユーザーまたはロールがサービスにリンクされたロールをプライベート接続で作成できるようにするには、IAM エンティティ (ユーザーまたはロール) のアクセス許可を設定する必要があります。IAM エンティティには、以下のアクションにアクセスする権限が必要です。
  - `iam:CreateServiceLinkedRolearn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*` での
  - `iam:PutRolePolicyarn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*` での
  - `ec2:DescribeVpcs`

- `ec2:DescribeSubnets`

詳細については、AWS Identity and Access ManagementAWS Outposts「」を参照してください。

- Outpost と同じ AWS アカウントとアベイラビリティーゾーンで、10.1.0.0/16 と競合しないサブネット /25 以上との Outpost プライベート接続のみを目的として VPC を作成します。たとえば、10.3.0.0/16 を使用できます。

> **Important**
>
> Outposts への接続が維持されるため、この VPC を削除しないでください。

- セキュリティコントロールポリシー (SCP) を使用して、この VPC が削除されないように保護します。

  次のサンプル SCP は、以下を削除できないようにします。

  - サブネットにタグ付けされた Outposts Anchor サブネット
  - VPC タグ付き Outposts Anchor VPC
  - タグ付けされたルートテーブル Outposts Anchor ルートテーブル
  - Transit Gateway タグ付き Outposts Transit Gateway
  - Virtual Private Gateway タグ付き Outposts Virtual Private Gateway
  - トランジットゲートウェイルートテーブルタグ Outposts Transit Gateway ルートテーブル
  - Outposts Anchor ENI タグを持つ ENI
- UDP 443 のインバウンドおよびアウトバウンド方向のトラフィックを許可するようにサブネットセキュリティグループを設定します。
- サブネット CIDR をオンプレミスネットワークにアドバタイズします。これを行う AWS Direct Connect には、 を使用します。詳細については、「Direct Connect ユーザーガイド」の「Direct Connect 仮想インターフェイス」と「Direct Connect ゲートウェイの操作」を参照してください。

> **Note**
>
> Outpost が保留中ステータスのときにプライベート接続オプションを選択するには、コンソールから AWS Outposts Outposts を選択し、Outposts を選択します。アクションを選択し、プライベート接続を追加を選択し、表示される手順に従います。

Outpost のプライベート接続オプションを選択すると、 は アカウントにサービスにリンクされたロール AWS Outposts を自動的に作成し、ユーザーに代わって次のタスクを完了できるようにします。

- 指定したサブネットと VPC にネットワークインターフェイスを作成し、ネットワークインターフェイスのセキュリティグループを作成します。
- アカウント内の AWS Outposts サービスリンクエンドポイントインスタンスにネットワークインターフェイスをアタッチするアクセス許可をサービスに付与します。
- アカウントからサービス リンク エンドポイント インスタンスにネットワーク インターフェイスを接続します。

> **Important**
>
> Outpost をインストールしたら、Outpost からサブネット内のプライベート IP への接続を確認します。

## オプション 1. プライベート VIFs を介した Direct Connect プライベート接続

AWS Direct Connect 接続、プライベート仮想インターフェイス、仮想プライベートゲートウェイを作成して、オンプレミスの Outpost が VPC にアクセスできるようにします。

詳細については、 Direct Connect ユーザーガイドの以下のセクションを参照してください。

- 専用接続とホスト接続
- プライベート仮想インターフェイスを作成する
- 仮想プライベートゲートウェイの関連付け

AWS Direct Connect 接続が VPC とは異なる AWS アカウントにある場合は、Direct Connect 「 ユーザーガイド」の「アカウント間の仮想プライベートゲートウェイの関連付け」を参照してください。

## オプション 2. トランジット VIFs を介した Direct Connect プライベート接続

AWS Direct Connect 接続、トランジット仮想インターフェイス、トランジットゲートウェイを作成して、オンプレミスの Outpost が VPC にアクセスできるようにします。

詳細については、 Direct Connect ユーザーガイドの以下のセクションを参照してください。

- 専用接続とホスト接続
- Direct Connect ゲートウェイへのトランジット仮想インターフェイスを作成する
- トランジットゲートウェイの関連付け

# ファイアウォールとサービスリンク

このセクションでは、ファイアウォール設定とサービスリンク接続について説明します。

次の図では、設定は Amazon VPC を AWS リージョンから Outpost に拡張します。 Direct Connect パブリック仮想インターフェイスは、サービスリンク接続です。次のトラフィックがサービスリンクと Direct Connect 接続を通過します。

- サービスリンク経由の Outpost への管理トラフィック
- Outpost と関連するすべての VPC 間のトラフィック

インターネット接続にステートフルファイアウォールを使用してパブリックインターネットからサービスリンク VLAN への接続を制限している場合、インターネットから開始されるすべてのインバウンド接続をブロックできます。これは、サービスリンク VPN は Outpost からリージョンにのみ開始され、リージョンから Outpost には開始されないためです。

UDP と TCP 対応の両方のステートフルファイアウォールを使用してサービスリンク VLAN に関する接続を制限する場合は、すべてのインバウンド接続を拒否できます。ファイアウォールがステートフルに動作している場合、Outposts サービスリンクからの許可されたアウトバウンド接続は、明示的なルール設定なしで返信トラフィックを自動的に に戻すことを許可する必要があります。Outpost サービスリンクから開始されたアウトバウンド接続のみを許可として設定する必要があります。

| プロトコル | ソースポート | 送信元アドレス | 発信先ポート | 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ネットワーク |
| 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ネットワーク |

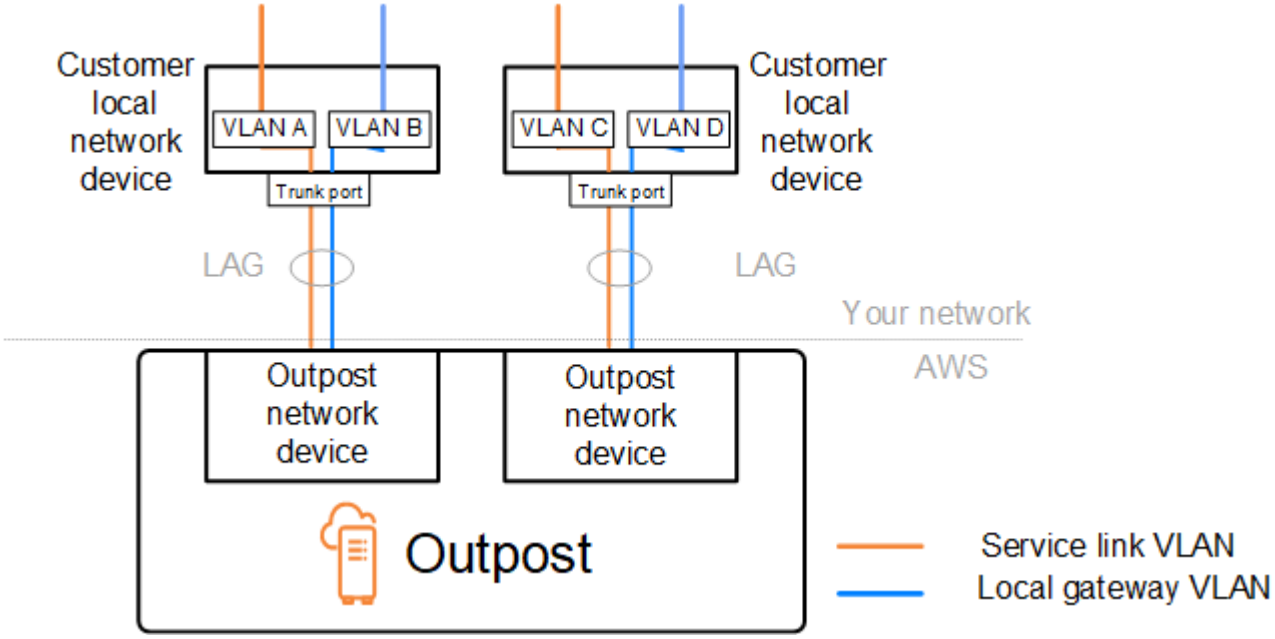
非ステートフルファイアウォールを使用してサービスリンク VLAN に関する接続を制限する場合は、Outposts サービスリンクからリージョンのパブリックネットワークへの AWS Outposts アウトバウンド接続を許可する必要があります。また、サービスリンク VLAN への Outposts リージョンのパブリックネットワークからの での返信トラフィックを明示的に許可する必要があります。接続は常に Outposts サービスリンクからアウトバウンドで開始されますが、応答トラフィックはサービスリンク VLAN に戻す必要があります。

| プロトコル | ソースポート | 送信元アドレス | 発信先ポート | 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ネットワーク |
| 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ネットワーク |
| UDP | 443 | AWS Outposts リージョンのパブリックネットワーク | 443 | AWS Outposts サービスリンク /26 |
| TCP | 443 | AWS Outposts リージョンのパブリックネットワーク | 1025-65535 | AWS Outposts サービスリンク /26 |

> **Note**
>
> Outposts 内のインスタンスは、サービスリンクを使用して別の Outpost 内のインスタンスと通信することはできません。ローカルゲートウェイまたはローカルネットワークインターフェイスを介したルーティングを活用して Outposts 間の通信を行います。
> AWS Outposts ラックは、ローカルゲートウェイコンポーネントを含む冗長な電源およびネットワーク機器でも設計されています。詳細については、「レジリエンス AWS Outposts」を参照してください。

# Outposts ラックネットワークのトラブルシューティングチェックリスト

このチェックリストは、ステータスが DOWN のサービス リンクのトラブルシューティングに役立ちます。




## Outpost ネットワーク デバイスとの接続

Outpost ネットワーク デバイスに接続されている顧客のローカル ネットワーク デバイスの BGP ピアリング ステータスを確認します。BGP ピアリングのステータスが DOWN の場合は、次の手順に従います。

1. 顧客のデバイスから Outpost ネットワーク デバイス上のリモート ピア IP アドレスに ping を実行します。ピア IP アドレスは、デバイスの BGP 設定で確認できます。ネットワーク準備チェックリスト インストール時に提供される を参照することもできます。
2. ping が失敗した場合は、物理接続をチェックし、接続ステータスが UP であることを確認します。
   a. お客様のローカルネットワーク機器の LACP 状態を確認します。
   b. デバイスのインターフェイスのステータスを確認します。ステータスが の場合 UP は、手順 3 に進みます。
   c. お客様のローカル ネットワーク デバイスをチェックし、光モジュールが動作していることを確認します。
   d. 障害のあるファイバーを交換し、ライト (Tx/Rx) が許容範囲内にあることを確認します。
3. ping が成功した場合は、顧客のローカル ネットワーク デバイスをチェックし、次の BGP 構成が正しいことを確認します。
   a. ローカル自律システム番号 (顧客 ASN) が正しく構成されていることを確認します。
   b. リモート自律システム番号 (Outpost ASN) が正しく構成されていることを確認します。
   c. インターフェイスの IP アドレスとリモート ピアの IP アドレスが正しく構成されていることを確認します。
   d. 広告および受信したルートが正しいことを確認します。
4. BGP セッションがアクティブ状態と接続状態の間でフラッピングしている場合は、TCP ポート 179 およびその他の関連する一時ポートが顧客のローカル ネットワーク デバイスでブロックされていないことを確認してください。
5. さらにトラブルシューティングが必要な場合は、顧客のローカル ネットワーク デバイスで次の点を確認してください。
   a. BGP および TCP のデバッグ ログ
   b. BGP ログ
   c. パケットキャプチャ
6. 問題が解決しない場合は、Outpost に接続されているルーターから Outpost ネットワーク デバイスのピア IP アドレスに対して MTR/traceroute/パケット キャプチャを実行します。エンタープライズ AWS サポートプランを使用して、テスト結果を サポートと共有します。

BGP ピアリング ステータスが顧客のローカル ネットワーク デバイスと UP Outpost ネットワーク デバイスの間であるにもかかわらず、サービス リンクがまだ である場合は DOWN、顧客のローカル ネットワーク デバイス上の次のデバイスを確認することで、さらにトラブルシューティングを行う

ことができます。サービス リンク接続のプロビジョニング方法に応じて、次のチェックリストのいずれかを使用してください。

- に接続されたエッジルーター Direct Connect — サービスリンク接続に使用されているパブリック仮想インターフェイス。詳細については、「Direct Connect リージョンへの AWS パブリック仮想インターフェイス接続」を参照してください。
- に接続されたエッジルーター Direct Connect – サービスリンク接続に使用されているプライベート仮想インターフェイス。詳細については、「Direct Connect リージョンへの AWS プライベート仮想インターフェイス接続」を参照してください。
- インターネット サービス プロバイダー (ISP) に接続されたエッジ ルーター - サービス リンク接続に使用されるパブリック インターネット。詳細については、「リージョンへの ISP パブリック インターネット接続 AWS」を参照してください。

## Direct Connect リージョンへの AWS パブリック仮想インターフェイス接続

次のチェックリストを使用して、パブリック仮想インターフェイスがサービスリンク接続に使用されている Direct Connect ときに に接続されたエッジルーターのトラブルシューティングを行います。

1. Outpost ネットワーク デバイスに直接接続しているデバイスが、BGP 経由でサービス リンク IP アドレス範囲を受信していることを確認します。
   a. デバイスから BGP 経由で受信されているルートを確認します。
   b. サービス リンクの Virtual Routing and Forwarding インスタンス (VRF) のルート テーブルを確認します。IP アドレス範囲を使用していることが表示されます。
2. リージョンの接続を確認するには、サービス リンク VRF のルート テーブルを確認します。これには、 AWS パブリック IP アドレス範囲またはデフォルトルートを含める必要があります。
3. サービスリンク VRF で AWS パブリック IP アドレス範囲を受信していない場合は、次の項目を確認してください。
   a. エッジルーターまたは から Direct Connect リンクステータスを確認します AWS マネジメントコンソール。
   b. 物理リンクが の場合は UP、エッジ ルータから BGP ピアリングのステータスを確認します。
   c. BGP ピアリングステータスが の場合DOWN、ピア AWS IP アドレスに ping を送信し、エッジルーターの BGP 設定を確認します。詳細については、Direct Connect 「 ユーザーガイド」の「トラブルシューティング Direct Connect」と「 AWS コンソールで仮想インターフェイスの BGP ステータスがダウンしている」を参照してください。「どうすればよいですか?」。

d. BGP が確立されていて、VRF にデフォルトルートまたは AWS パブリック IP アドレス範囲が表示されない場合は、エンタープライズ AWS サポートプランを使用して サポートにお問い合わせください。

4. オンプレミスのファイアウォールを使用している場合は、次の項目を確認してください。

   a. サービス リンク接続に必要なポートがネットワーク ファイアウォールで許可されていることを確認します。ポート 443 での traceroute またはその他のネットワーク トラブルシューティング ツールを使用して、ファイアウォールとネットワーク デバイスを介した接続を確認します。次のポートは、サービス リンク接続用のファイアウォール ポリシーで設定する必要があります。

      - TCP プロトコル - 送信元ポート: TCP 1025-65535、宛先ポート: 443。
      - UDP プロトコル — 送信元ポート: TCP 1025-65535、宛先ポート: 443。

   b. ファイアウォールがステートフルである場合は、アウトバウンドルールが Outpost のサービスリンク IP アドレス範囲を AWS パブリック IP アドレス範囲に許可していることを確認します。詳細については、「AWS Outposts AWS リージョンへの接続」を参照してください。

   c. ファイアウォールがステートフルでない場合は、インバウンドフローも許可してください ( AWS パブリック IP アドレス範囲からサービスリンク IP アドレス範囲まで ) 。

   d. ファイアウォールで仮想ルーターを構成している場合は、Outpost と AWS リージョン間のトラフィックに対して適切なルーティングが構成されていることを確認してください。

5. Outpost のサービス リンク IP アドレス範囲を独自のパブリック IP アドレスに変換するようにオンプレミス ネットワークで NAT を構成している場合は、次の項目を確認してください。

   a. NAT デバイスが過負荷になっておらず、新しいセッションに割り当てる空きポートがあることを確認します。

   b. NAT デバイスがアドレス変換を実行するように正しく構成されていることを確認します。

6. 問題が解決しない場合は、エッジルーターから Direct Connect ピア IP アドレスへの MTR/traceroute/パケットキャプチャを実行します。エンタープライズ AWS サポートプランを使用して、テスト結果を サポートと共有します。

## Direct Connect リージョンへの AWS プライベート仮想インターフェイス接続

以下のチェックリストを使用して、プライベート仮想インターフェイスがサービスリンク接続に使用されている Direct Connect ときに に接続されたエッジルーターのトラブルシューティングを行います。

1. Outposts ラックと AWS リージョン間の接続でプライベート接続機能を使用している場合 AWS Outposts は、次の項目を確認してください。

   a. エッジルーターからリモートピアリング AWS IP アドレスを Ping し、BGP ピアリングのステータスを確認します。

   b. サービスリンクエンドポイント VPC とオンプレミスにインストールされている Outpost 間の Direct Connect プライベート仮想インターフェイスを介した BGP ピアリングが であることを確認しますUP。詳細については、Direct Connect 「 ユーザーガイド」の「トラブルシューティング Direct Connect」を参照してください。 AWS コンソールで仮想インターフェイス BGP ステータスがダウンしています。「どうすればよいですか?」および「Direct Connect 経由の BGP 接続の問題をトラブルシューティングするにはどうすればよいですか?」

   c. Direct Connect プライベート仮想インターフェイスは、選択した Direct Connect ロケーションのエッジルーターへのプライベート接続であり、BGP を使用してルートを交換します。プライベート仮想プライベートクラウド (VPC) CIDR 範囲は、この BGP セッションを通じてエッジルーターにアドバタイズされます。同様に、Outpost サービス リンクの IP アドレス範囲は、エッジ ルーターから BGP 経由でリージョンにアドバタイズされます。

   d. VPC 内のサービス リンク プライベート エンドポイントに関連付けられたネットワーク ACL が関連するトラフィックを許可していることを確認します。詳細については、「ネットワーク準備チェックリスト」を参照してください。

   e. オンプレミスのファイアウォールがある場合は、VPC または VPC CIDR にあるサービス リンクの IP アドレス範囲と Outpost サービス エンドポイント (ネットワーク インターフェイスの IP アドレス) を許可するアウトバウンド ルールがファイアウォールにあることを確認してください。TCP 1025-65535 および UDP 443 ポートがブロックされていないことを確認してください。詳細については、AWS Outposts 「プライベート接続の紹介」を参照してください。

   f. ファイアウォールがステートフルでない場合は、VPC 内の Outpost サービス エンドポイントから Outpost への受信トラフィックを許可するルールとポリシーがファイアウォールにあることを確認してください。

2. オンプレミスネットワークに 100 を超えるネットワークがある場合は、BGP セッション経由でデフォルトのルートをプライベート仮想インターフェイス AWS の にアドバタイズできます。デフォルトルートを広告したくない場合は、広告する経路数が 100 未満になるように経路を集約してください。

3. 問題が解決しない場合は、エッジルーターから Direct Connect ピア IP アドレスへの MTR/traceroute/パケットキャプチャを実行します。エンタープライズ AWS サポートプランを使用して、テスト結果を サポートと共有します。

# リージョンへの ISP パブリック インターネット接続 AWS

サービス リンク接続にパブリック インターネットを使用する場合、ISP 経由で接続されている エッジ ルーターのトラブルシューティングを行うには、次のチェックリストを使用してください。

- インターネット リンクが確立されていることを確認します。
- ISP 経由で接続された エッジ デバイスからパブリック サーバーにアクセスできることを確認します。

ISP リンク経由でインターネットまたはパブリック サーバーにアクセスできない場合は、次の手順を実行します。

1. ISP ルーターとの BGP ピアリング状態が確立されているか確認してください。
   a. BGP がフラッピングしていないことを確認します。
   b. BGP が ISP から必要なルートを受信してアドバタイズしていることを確認します。
2. スタティック ルート設定の場合は、エッジ デバイス上でデフォルト ルートが適切に設定されていることを確認してください。
3. 別の ISP 接続を使用してインターネットに接続できるかどうかを確認します。
4. 問題が解決しない場合は、エッジ ルーターで MTR/traceroute/パケット キャプチャを実行します。さらにトラブルシューティングを行うために、結果を ISP のテクニカル サポート チームと共有してください。

ISP リンクを通じてインターネットとパブリック サーバーにアクセスできる場合は、次の手順を実行します。

1. Outpost ホーム リージョン内のパブリックにアクセス可能な EC2 インスタンスまたはロード バランサーのいずれかがエッジ デバイスからアクセス可能かどうかを確認します。ping または telnet を使用して接続を確認し、traceroute を使用してネットワーク パスを確認できます。
2. VRF を使用してネットワーク内のトラフィックを分離する場合は、サービス リンク VRF に、ISP (インターネット) と VRF の間でトラフィックを送受信するルートまたはポリシーがあることを確認してください。次のチェックポイントを参照してください。
   a. ISP に接続するエッジ ルーター。エッジ ルータの ISP VRF ルート テーブルを調べて、サービス リンクの IP アドレス範囲が存在することを確認します。
   b. Outpost に接続する顧客のローカル ネットワーク デバイス。VRF の設定をチェックし、サービス リンク VRF と ISP VRF の間の接続に必要なルーティングとポリシーが適切に設定されて

いることを確認します。通常、デフォルト ルートは、インターネットへのトラフィックのために ISP VRF からサービス リンク VRF に送信されます。

c. Outpost に接続されているルーターでソースベースのルーティングを構成した場合は、構成が正しいことを確認してください。

3. Outpost サービスリンク IP アドレス範囲からパブリック IP AWS アドレス範囲へのアウトバウンド接続 (TCP 1025-65535 および UDP 443 ポート) を許可するようにオンプレミスファイアウォールが設定されていることを確認します。ファイアウォールがステートフルでない場合は、Outpost への受信接続も構成されていることを確認してください。
4. Outpost のサービス リンク IP アドレス範囲をパブリック IP アドレスに変換するために、オンプレミス ネットワークで NAT が構成されていることを確認します。また、以下の項目についても確認してください。

   a. NAT デバイスは過負荷になっておらず、新しいセッションに割り当てるための空きポートがあります。

   b. NAT デバイスはアドレス変換を実行するように正しく構成されています。

問題が解決しない場合は、MTR/traceroute/パケット キャプチャを実行します。

- オンプレミス ネットワークでパケットがドロップまたはブロックされていることが結果で示された場合は、ネットワークまたは技術チームに追加のガイダンスを確認してください。
- 結果から、パケットが ISP のネットワークでドロップまたはブロックされていることが示された場合は、ISP のテクニカルサポートチームに連絡してください。
- 結果に問題が表示されない場合は、すべてのテスト (MTR、telnet、Traceroute、パケットキャプチャ、BGP ログなど) から結果を収集し、エンタープライズサポートプランを使用して AWS サポートにお問い合わせください。

## Outposts は 2 つのファイアウォールデバイスの内側にあります。

Outpost を同期したファイアウォールの高可用性ペアまたは 2 つのスタンドアロンのファイアウォールの内側に置くと、サービスリンクの非対称ルーティングが発生する可能性があります。つまり、インバウンドトラフィックはファイアウォール 1 を通過し、アウトバウンドトラフィックはファイアウォール 2 を通過することになります。特に以前に正しく機能していた場合、以下のチェックリストを使用して、サービスリンクの非対称ルーティングの可能性を見極めます。

- ファイアウォールを介したサービスリンクの非対称ルーティングにつながる可能性がある企業ネットワークのルーティング設定で、最近行われた変更や継続中のメンテナンスがあるかどうかを確認します。
  - ファイアウォールのトラフィックグラフを使用して、サービスリンクの問題の開始と一致するトラフィックパターンの変化を確認します。
  - ファイアウォールに部分的な障害や、ファイアウォールが相互に接続テーブルを同期しなくなった可能性のある、スプリットブレインが発生したファイアウォールペアのケースがないかを確認してください。
  - 企業ネットワークで、サービスリンクの問題発生と一致するリンクダウンやルーティングの変更 (OSPF/ISIS/EIGRP のメトリクス変更、BGP ルートマップの変更) がないかを確認してください。
- ホームリージョンへのサービスリンクにパブリックインターネット接続を使用している場合、サービスプロバイダーのメンテナンスにより、ファイアウォールを介したサービスリンクの非対称ルーティングが発生する可能性があります。
  - トラフィックグラフで、ISP へのリンクのトラフィックパターンに、サービスリンクの問題発生と一致する変化がないかを確認します。
- サービスリンク Direct Connect の接続を使用している場合、 AWS 計画されたメンテナンスによってサービスリンクの非対称ルーティングがトリガーされる可能性があります。
  - Direct Connect サービスで計画されたメンテナンスの通知を確認します (複数可 ) 。
  - 冗長 Direct Connect サービスがある場合は、メンテナンス条件下で、考えられる各ネットワークパスに対する Outposts サービスリンクのルーティングを事前にテストできます。これにより、いずれかの Direct Connect サービスが中断された場合に、サービスリンクの非対称ルーティングにつながるかどうかをテストできます。エンドツーエンドのネットワーク接続の Direct Connect 部分の耐障害性は、 Direct Connect Resiliency Toolkit でテストできます。詳細については、「Testing Direct Connect Resiliency with Resiliency Toolkit – Failover Testing」を参照してください。

上記のチェックリストをすべて確認し、サービスリンクの非対称ルーティングが根本原因である可能性が高いと特定した後は、さらにいくつかの対応策があります。

- 企業ネットワークの変更を元に戻すか、プロバイダーが計画したメンテナンスが完了するまで待機して、対称ルーティングを復元します。
- ファイアウォールのいずれか一方または両方にログインし、コマンドラインからすべてのフローのフロー状態の情報をすべてクリアします (ファイアウォールベンダーがサポートしている場合)。

- 一方のファイアウォールを介して BGP アナウンスを一時的にフィルタリングするか、もう一方のファイアウォールのインターフェイスをシャットダウンして、もう一方のファイアウォールを介して対称ルーティングを強制的に行います。
- 各ファイアウォールを再起動して、ファイアウォールのメモリ内のサービスリンクトラフィックのフロー状態追跡における破損の可能性を排除します。
- ファイアウォールベンダーと協力して、ポート 443 宛ての UDP 接続の UDP フロー状態の追跡を検証するか緩和します。

# Outposts ラックのローカルゲートウェイ

ローカルゲートウェイは Outposts ラックの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。オンプレミスインフラストラクチャがインターネットアクセスを提供する場合、Outposts ラックで実行されているワークロードは、ローカルゲートウェイを利用してリージョンのサービスまたはリージョンのワークロードと通信することもできます。この接続は、パブリック接続 (インターネット) または Direct Connectを使用して実現できます。詳細については、「AWS Outposts AWS リージョンへの接続」を参照してください。

内容



## ローカルゲートウェイの基本

AWS は、インストールプロセスの一環として、Outposts ラックごとにローカルゲートウェイを作成します。Outposts ラックは 1 つのローカルゲートウェイをサポートします。ローカルゲートウェイは、Outposts ラックに関連付けられた AWS アカウント によって所有されます。

> **Note**
>
> ローカルゲートウェイを通過するトラフィックのインスタンス帯域幅の制限を理解するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスのネットワーク帯域幅」を参照してください。

ローカルゲートウェイは、以下のコンポーネントを含みます。

- ルートテーブル - ローカルゲートウェイの所有者のみがローカルゲートウェイルートテーブルを作成できます。詳細については、「the section called “ルートテーブル”」を参照してください。

- CoIP プール — (オプション) 所有している IP アドレス範囲を使用して、オンプレミスネットワークと VPC 内のインスタンス間の通信を容易にできます。詳細については、「the section called “顧客所有の IP アドレス”」を参照してください。
- 仮想インターフェイス (VIFs) – ローカルゲートウェイ VIFs (仮想インターフェイス) は、Outposts ラックの論理インターフェイスコンポーネントであり、Outposts ネットワークデバイスとオンプレミスネットワークデバイス間の VLAN、IP、BGP 接続をローカルゲートウェイ接続用にセットアップします。 は LAG ごとに 1 つの VIF AWS を作成し、両方の VIFsを VIF グループに追加します。ローカルゲートウェイのルートテーブルには、ローカルネットワーク接続用の 2 つの VIF へのデフォルトルートが必要です。詳細については、「ローカルネットワーク接続」を参照してください。
- VIF グループ – 作成する VIFs を VIF グループ AWS に追加します。VIF グループは VIF を論理的にグループ化したものです。
- ローカルゲートウェイルートテーブルと VPC の関連付け – ローカルゲートウェイルートテーブルと VPC の関連付けを使用すると、VPCsをローカルゲートウェイルートテーブルに接続できます。この関連付けにより、Outposts サブネットルートテーブル内のローカルゲートウェイをターゲットとするルートを追加できます。これにより、ローカルゲートウェイを介して Outposts サブネットリソースとオンプレミスネットワーク間の通信が可能になります。
- ローカルゲートウェイルーティングドメイン – ローカルゲートウェイルーティングドメインは、ローカルゲートウェイルートテーブルとローカルゲートウェイ VIF グループの関連付けです。この関連付けを使用すると、ローカルゲートウェイルートテーブル内のローカルゲートウェイ VIF グループをターゲットとするルートを追加できます。これにより、選択した VIF グループを介して Outposts サブネットリソースとオンプレミスネットワーク間の通信が可能になります。

が Outposts ラックを AWS プロビジョニングすると、一部のコンポーネントが作成され、お客様は他のコンポーネントを作成する責任があります。

AWS 責任

- ハードウェアの引き渡し
- ローカルゲートウェイの作成
- 仮想インターフェイス (VIF) と VIF グループの作成

あなたの責任

- ローカルゲートウェイルートテーブルの作成
- VPC とローカルゲートウェイルートテーブルの関連付け

- VIF グループをローカルゲートウェイルートテーブルに関連付けて、ローカルゲートウェイルーティングドメインを作成します。

# ローカルゲートウェイルーティング

Outpost サブネット内のインスタンスは、以下のオプションのいずれかを使用して、ローカルゲートウェイ経由でオンプレミスネットワークと通信できます。

- プライベート IP アドレス — ローカルゲートウェイは、Outpost サブネット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。これがデフォルトです。
- カスタマー所有 IP アドレス — ローカルゲートウェイは、Outpost サブネット内のインスタンスに割り当てたカスタマー所有 IP アドレスのネットワークアドレス変換 (NAT) を実行します。このオプションでは、CIDR 範囲やその他のネットワークトポロジーの重複がサポートされます。

詳細については、「the section called “ルートテーブル”」を参照してください。

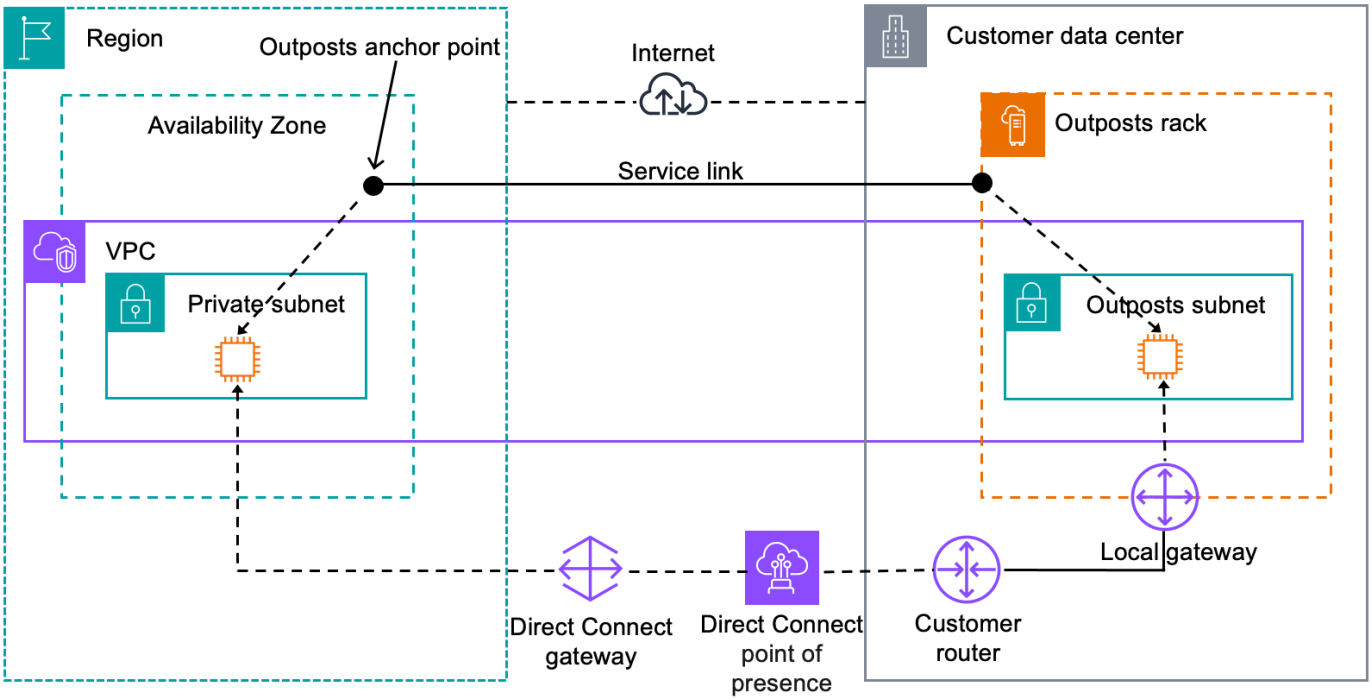
# ローカルゲートウェイ経由の接続

ローカルゲートウェイの主な役割は、Outpost からローカルの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。オンプレミスネットワークを介してインターネットに接続することもできます。例については、「the section called “ダイレクト VPC ルーティング”」および「the section called “顧客所有の IP アドレス”」を参照してください。

ローカルゲートウェイは、 AWS リージョンに戻るデータプレーンパスを提供することもできます。ローカルゲートウェイのデータプレーンパスは、Outpost からローカルゲートウェイを経由して、プライベートローカルゲートウェイ LAN セグメントに到達します。その後、プライベートパスをたどってリージョンの AWS サービスエンドポイントに戻ります。使用するデータプレーンパスにかかわらず、コントロールプレーンパスは常にサービスリンク接続を使用することに注意してください。

オンプレミスの Outposts インフラストラクチャを リージョン AWS のサービス の にプライベートに接続できます Direct Connect。詳細については、「AWS Outposts プライベート接続」を参照してください。

次の画像は、ローカルゲートウェイを介した接続を示しています。




# ローカルゲートウェイルートテーブル

ラックのインストールの一環として、 はローカルゲートウェイ AWS を作成し、VIFs と VIF グループを設定します。ローカルゲートウェイは、Outpost に関連付けられた AWS アカウントによって所有されます。ローカルゲートウェイルートテーブルを作成します。ローカルゲートウェイルートテーブルには、VIF グループと VPC との関連付けが必要です。VIF グループと VPC の関連付けを作成および管理します。ローカルゲートウェイの所有者のみが、ローカルゲートウェイルートテーブルを変更できます。

Outpost サブネットルートテーブルには、オンプレミスネットワークへの接続を提供するために、ローカルゲートウェイ VIF グループへのルートを含めることができます。

ローカルゲートウェイルートテーブルには、Outposts サブネット内のインスタンスがオンプレミスネットワークと通信する方法を決定するモードがあります。デフォルトのオプションは、インスタンスのプライベート IP アドレスを使用するダイレクト VPC ルーティングです。もう 1 つのオプションは、指定した顧客所有 IP アドレスプール (CoIP) のアドレスを使用します。ダイレクト VPC ルーティングと CoIP は、ルーティングの動きを制御する相互に排他的なオプションです。Outpost に最適なオプションを決定するには、「Outposts ラックで CoIP とダイレクト VPC AWS のルーティングモードを選択する方法」を参照してください。

を使用して、ローカルゲートウェイルートテーブルを他の AWS アカウントまたは組織単位と共有できます AWS Resource Access Manager。詳細については、「共有 AWS Outposts リソースの使用」を参照してください。

内容



## ダイレクト VPC ルーティング

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、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 Outposts 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 Outposts のデフォルトモードです。このモードでは、ローカルゲートウェイはインスタンスの NAT を実行しないため、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。ダイレクト VPC ルーティングモードの代わりに独自のアドレススペースを使用するオプションがあります。詳細については、「顧客所有の IP アドレス」を参照してください。

ダイレクト VPC ルーティングモードは、CIDR 範囲の重複をサポートしていません。

ダイレクト VPC ルーティングは、インスタンスネットワークインターフェースでのみサポートされます。がユーザーに代わって AWS 作成するネットワークインターフェイス (リクエスタマネージドネットワークインターフェイス) では、それらのプライベート IP アドレスはオンプレミスネットワークから到達できません。例えば、オンプレミスネットワークから VPC エンドポイントに直接アクセスすることはできません。

以下の例は、ダイレクト VPC のルーティングを示しています。

例

## 例: VPC 経由のインターネット接続

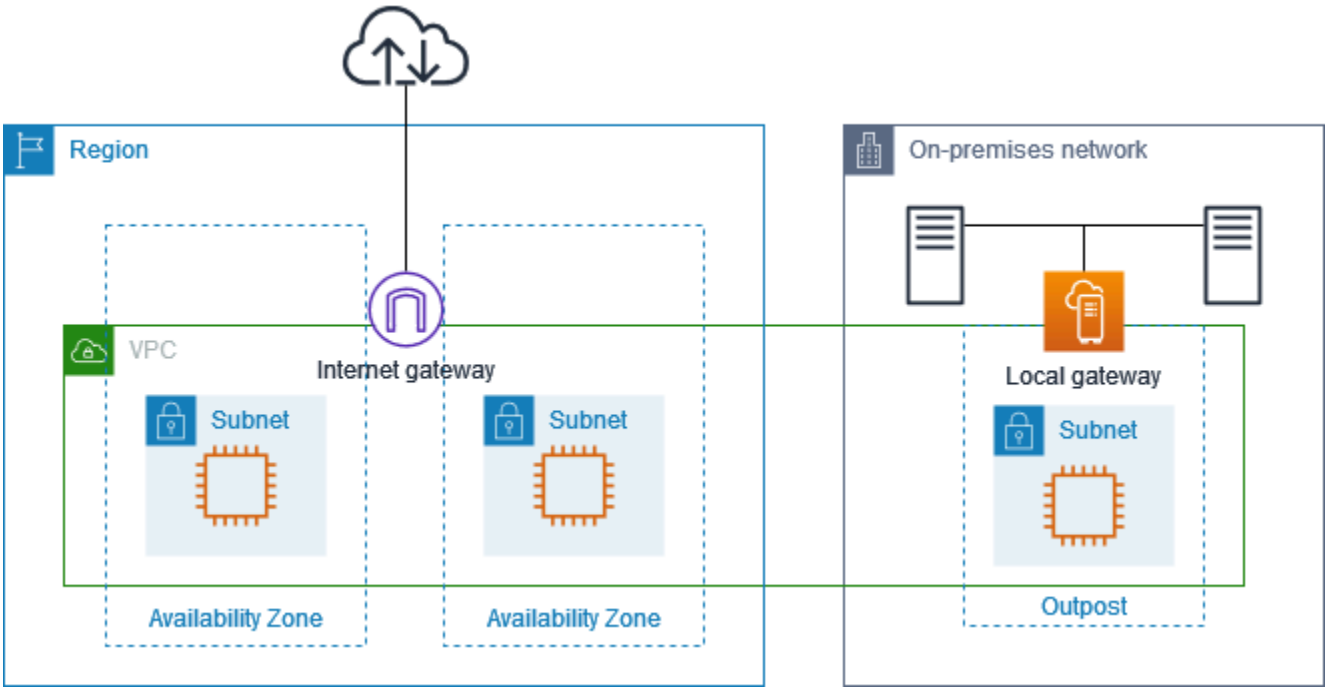
Outpost サブネットのインスタンスは、VPC にアタッチされたインターネットゲートウェイを介してインターネットにアクセスできます。

以下の設定を考慮します。

- 親 VPC は 2 つのアベイラビリティーゾーンにまたがり、各アベイラビリティーゾーンにサブネットがあります。
- Outpost には 1 つのサブネットがあります。
- 各サブネットには EC2 インスタンスがあります。
- ローカルゲートウェイは BGP アドバタイズを使用して Outpost サブネットのプライベート IP アドレスをオンプレミスネットワークにアドバタイズします。

> **Note**
>
> BGP アドバタイズは、ローカルゲートウェイを宛先とするルートがある Outpost 上のサブネットでのみサポートされます。その他のサブネットは BGP を通じてアドバタイズされません。

以下の図では、Outpost サブネット内のインスタンスからのトラフィックは VPC のインターネットゲートウェイを使用してインターネットにアクセスできます。



親リージョンを経由してインターネット接続を実現するには、Outpost サブネットのルートテーブルに以下のルートが必要です。

| ルーティング先 | ターゲット | コメント |
| --- | --- | --- |
| *VPC CIDR* | ローカル | VPC 内のサブネット間の接続を提供します。 |
| 0.0.0.0 | *internet-gateway-id* | インターネット宛てのトラフィックをインターネットゲートウェイに送信します。 |
| *############ CIDR* | *local-gateway-id* | オンプレミスネットワーク宛てのトラフィックを、ローカルゲートウェイに送信します。 |

## 例: オンプレミスネットワーク経由のインターネット接続

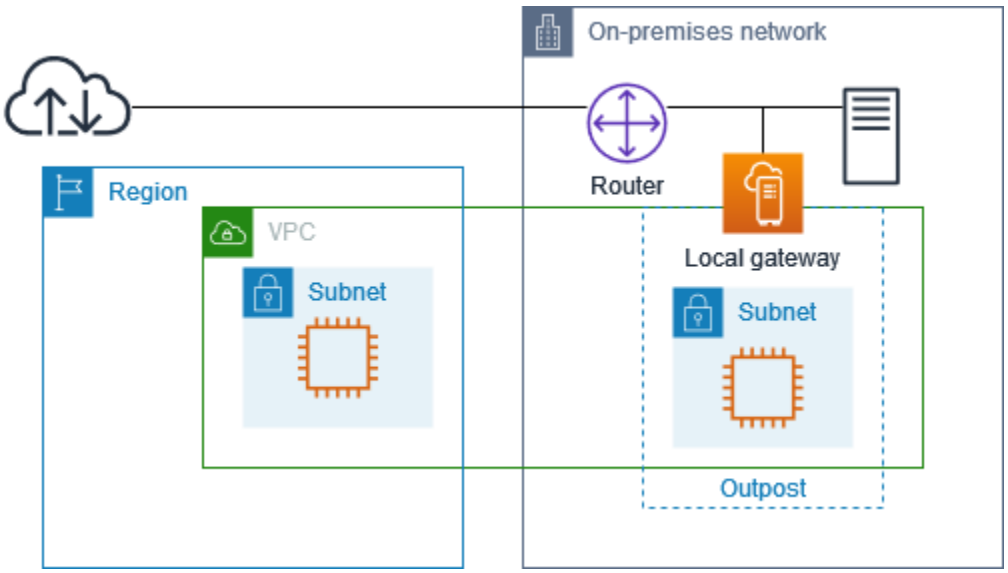
Outpost サブネット内のインスタンスは、オンプレミスネットワークを介してインターネットにアクセスできます。Outpost サブネットのインスタンスには、パブリック IP アドレスや Elastic IP アドレスは必要ありません。

以下の設定を考慮します。

- Outpost サブネットには EC2 インスタンスがあります。
- オンプレミスネットワークのルーターは、ネットワークアドレス変換 (NAT) を実行します。
- ローカルゲートウェイは BGP アドバタイズを使用して Outpost サブネットのプライベート IP アドレスをオンプレミスネットワークにアドバタイズします。

> **Note**
>
> BGP アドバタイズは、ローカルゲートウェイを宛先とするルートがある Outpost 上のサブネットでのみサポートされます。その他のサブネットは BGP を通じてアドバタイズされません。

以下の図では、Outpost サブネット内のインスタンスからのトラフィックは、ローカルゲートウェイを使用してインターネットまたはオンプレミスネットワークにアクセスできます。オンプレミスネットワークからのトラフィックは、ローカルゲートウェイを使用して Outpost サブネットのインスタンスにアクセスします。




オンプレミスネットワークを介してインターネット接続を実現するには、Outpost サブネットのルートテーブルに以下のルートが必要です。

| ルーティング先 | ターゲット | コメント |
| --- | --- | --- |
| *VPC CIDR* | ローカル | VPC 内のサブネット間の接続を提供します。 |
| 0.0.0.0/0 | *local-gateway-id* | インターネット宛てのトラフィックをローカルゲートウェイに送信します。 |

インターネットへのアウトバウンドアクセス

Outpost サブネットのインスタンスから開始されたインターネット宛てのトラフィックは、0.0.0.0/0 のルートを使用して、トラフィックをローカルゲートウェイにルーティングします。ローカルゲートウェイは、そのトラフィックをルーターに送信します。ルーターは NAT を使用して、プライベート IP アドレスをルーターのパブリック IP アドレスに変換し、トラフィックを宛先に送信します。

オンプレミスネットワークへのアウトバウンドアクセス

Outpost サブネット内のインスタンスから開始されたオンプレミスネットワークの宛てのトラフィックは、0.0.0.0/0 のルートを使用してローカルゲートウェイにトラフィックをルーティングします。ローカルゲートウェイは、オンプレミス ネットワーク内の宛先にトラフィックを送信します。

オンプレミスネットワークからのインバウンドアクセス

オンプレミスネットワークから Outpost サブネットにあるインスタンス宛てのトラフィックは、インスタンスのプライベート IP アドレスを使用します。トラフィックがローカルゲートウェイに到達すると、ローカルゲートウェイは VPC 内の宛先にトラフィックを送信します。

## 顧客所有の IP アドレス

デフォルトでは、ローカルゲートウェイは 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。ただし、カスタマー所有 IP アドレスプール (CoIP) と呼ばれるアドレス範囲を指定して、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こともできます。

CoIP を選択した場合は、アドレスプールを作成して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 経由でカスタマーネットワークにアドバタイズする必要があります。ローカルゲートウェイルートテーブルに関連付けられているカスタマー所有 IP アドレスは、伝達されたルートとしてルートテーブルに表示されます。

顧客所有の IP 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または外部接続を提供します。これらの IP アドレスは、カスタマー所有 IP プールから新しい Elastic IP アドレスを割り当て、それをリソースに割り当てることによって、EC2 インスタンスなどの Outpost 上のリソースに割り当てることができます。詳細については、「CoIP プール」を参照してください。

> **Note**
>
> 顧客所有の IP アドレスプールの場合、ネットワーク内のアドレスをルーティングできる必要があります。

カスタマー所有 IP アドレスプールから Elastic IP アドレスを割り当てる場合、そのカスタマー所有 IP アドレスプールの IP アドレスは引き続き所有することになります。必要に応じて、社内ネットワークまたは WAN にそれらをアドバタイズする責任があります。

必要に応じて、 を使用して、顧客所有のプールを組織 AWS アカウント 内の複数の と共有できます AWS Resource Access Manager。プールを共有すると、参加者はカスタマー所有 IP アドレスプールから Elastic IP アドレスを割り当て、それを Outpost の EC2 インスタンスに割り当てることができます。詳細については、「共有 リソース」を参照してください。

例

- 例: VPC 経由のインターネット接続

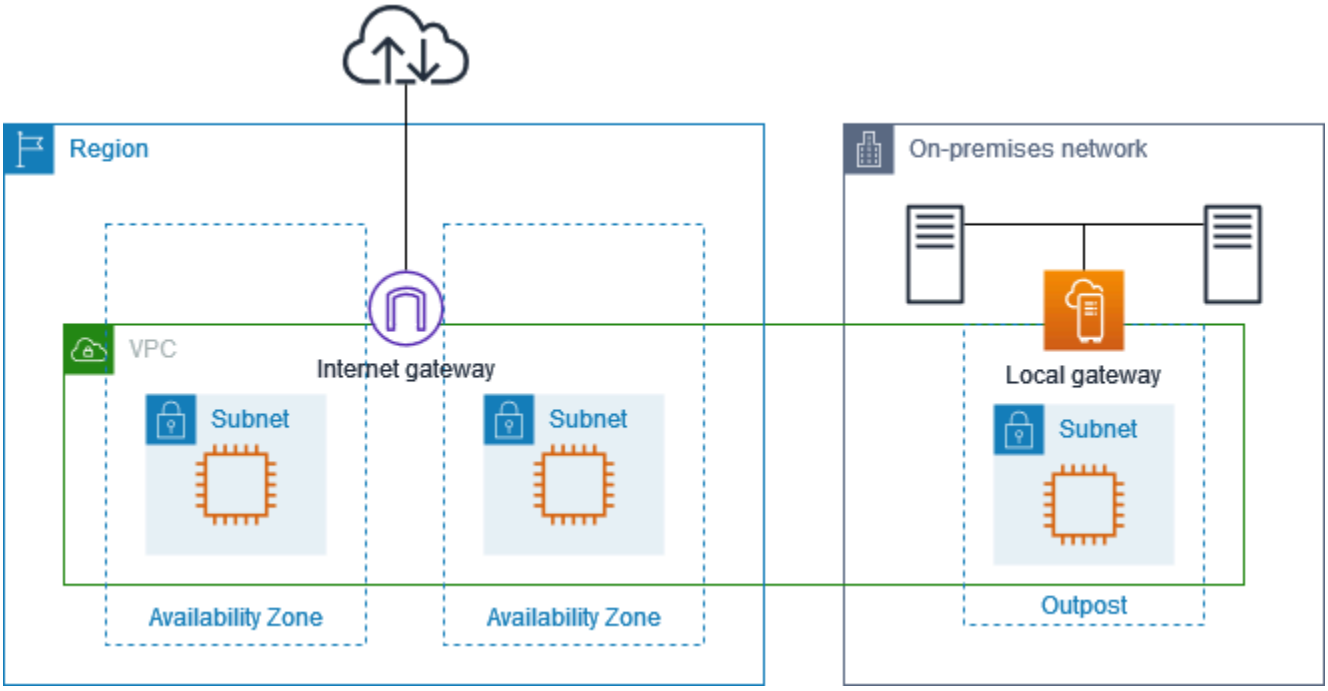
- 例: オンプレミスネットワーク経由のインターネット接続

## 例: VPC 経由のインターネット接続

Outpost サブネットのインスタンスは、VPC にアタッチされた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できます。

以下の設定を考慮します。

- 親 VPC は 2 つのアベイラビリティーゾーンにまたがり、各アベイラビリティーゾーンにサブネットがあります。
- Outpost には 1 つのサブネットがあります。
- 各サブネットには EC2 インスタンスがあります。
- カスタマー所有 IP アドレスプールがあります。
- Outpost サブネット内のインスタンスには、カスタマー所有 IP アドレスプールの Elastic IP アドレスが割り当てられています。
- ローカルゲートウェイは BGP アドバタイズを使用して、カスタマー所有 IP アドレスプールをオンプレミスネットワークにアドバタイズします。




リージョンを介してインターネット接続を実現するには、Outpost サブネットのルートテーブルに以下のルートが必要です。

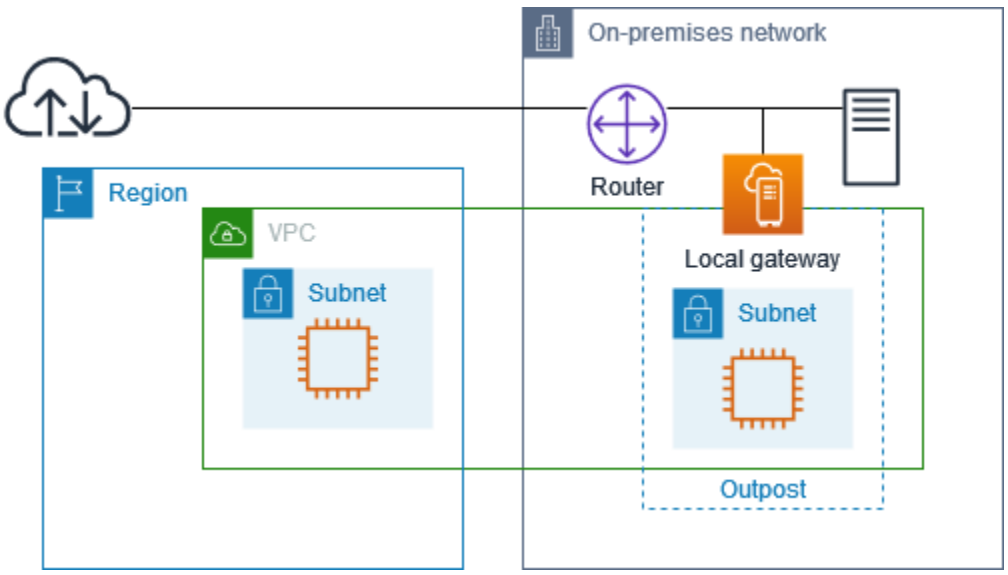
| ルーティング先 | ターゲット | コメント |
| --- | --- | --- |
| *VPC CIDR* | ローカル | VPC 内のサブネット間の接続を提供します。 |
| 0.0.0.0 | *internet-gateway-id* | パブリックインターネット宛てのトラフィックをインターネットゲートウェイに送信します。 |
| *############ CIDR* | *local-gateway-id* | オンプレミスネットワーク宛てのトラフィックを、ローカルゲートウェイに送信します。 |

## 例: オンプレミスネットワーク経由のインターネット接続

Outpost サブネット内のインスタンスは、オンプレミスネットワークを介してインターネットにアクセスできます。

以下の設定を考慮します。

- Outpost サブネットには EC2 インスタンスがあります。
- カスタマー所有 IP アドレスプールがあります。
- ローカルゲートウェイは BGP アドバタイズを使用して、カスタマー所有 IP アドレスプールをオンプレミスネットワークにアドバタイズします。
- 10.0.3.112 を 10.1.0.2 にマッピングする Elastic IP アドレス関連付け。
- カスタマーのオンプレミスネットワーク内のルーターは NAT を実行します。



ローカルゲートウェイ経由でインターネット接続を実現するには、Outpost サブネットのルートテーブルに次のルートが必要です。

| ルーティング先 | ターゲット | コメント |
| --- | --- | --- |
| *VPC CIDR* | ローカル | VPC 内のサブネット間の接続を提供します。 |
| 0.0.0.0/0 | *local-gateway-id* | インターネット宛てのトラフィックをローカルゲートウェイに送信します。 |

インターネットへのアウトバウンドアクセス

Outpost サブネットの EC2 インスタンスから開始されたインターネット宛てのトラフィックは、0.0.0.0/0 のルートを使用して、トラフィックをローカルゲートウェイにルーティングします。ローカルゲートウェイは、インスタンスのプライベート IP アドレスをカスタマー所有 IP アドレスにマッピングし、トラフィックをルーターに送信します。ルーターは NAT を使用して、カスタマー所有 IP アドレスをルーターのパブリック IP アドレスに変換し、トラフィックを宛先に送信します。

オンプレミスネットワークへのアウトバウンドアクセス

Outpost サブネット内の EC2 インスタンスから開始されたオンプレミスネットワーク宛てのトラフィックは、0.0.0.0/0 のルートを使用してローカルゲートウェイにトラフィックをルーティングします。ローカルゲートウェイは EC2 インスタンスの IP アドレスをカスタマー所有 IP アドレス (Elastic IP アドレス) に変換し、トラフィックを宛先に送信します。

オンプレミスネットワークからのインバウンドアクセス

Outpost サブネットにあるオンプレミスネットワークからインスタンス宛てのトラフィックは、カスタマー所有のインスタンスの IP アドレス (Elastic IP アドレス) を使用します。トラフィックがローカルゲートウェイに到達すると、ローカルゲートウェイはカスタマー所有 IP アドレス (Elastic IP アドレス) をインスタンス IP アドレスにマッピングし、トラフィックを VPC 内の宛先に送信します。さらに、ローカルゲートウェイルートテーブルは、Elastic Network Interface をターゲットとするすべてのルートを評価します。宛先アドレスがいずれかの静的ルートの宛先 CIDR と一致する場合、トラフィックはその Elastic Network Interface に送信されます。トラフィックが Elastic Network Interface への静的ルートをたどる場合、宛先アドレスは保存され、ネットワークインターフェイスのプライベート IP アドレスに変換されません。

## カスタムルートテーブル

ローカルゲートウェイ用のカスタムルートテーブルを作成できます。ローカルゲートウェイルートテーブルには、VIF グループと VPC との関連付けが必要です。手順の詳細については、「ローカルゲートウェイ接続を構成する」を参照してください。

# ローカルゲートウェイのルートテーブルルート

Outpost 上のローカルゲートウェイルートテーブルとネットワークインターフェイスへの受信ルートを作成できます。既存のローカルゲートウェイのインバウンドルートを変更して、ターゲットのネットワークインターフェイスを変更することもできます。

ルートが [アクティブ] 状態になるのは、そのターゲットのネットワークインターフェイスが実行中のインスタンスにアタッチされている場合のみです。インスタンスが停止したり、インターフェイスがデタッチされたりすると、ルートステータスは [アクティブ] から [ブラックホール] に変更されます。

内容



## 要件と制限

次の要件と制限事項が適用されます。

- ターゲットのネットワークインターフェイスは、Outpost のサブネットに属し、その Outpost のインスタンスにアタッチされている必要があります。ローカルゲートウェイルートは、別の Outpost または親 AWS リージョンにある Amazon EC2 インスタンスをターゲットにすることはできません。
- サブネットは、ローカルゲートウェイルートテーブルに関連付けられた VPC に属している必要があります。
- 同じルートテーブル内のネットワークインターフェイスルートは 100 個以下にしてください。
- AWS は最も具体的なルートを優先し、ルートが一致する場合は、伝播されたルートよりも静的ルートを優先します。

- インターフェイス VPC エンドポイントはサポートされていません。
- BGP アドバタイズは、ルートテーブルにローカルゲートウェイをターゲットとするルートがある Outpost のサブネットのみを対象としています。サブネットのルートテーブルにローカルゲートウェイをターゲットとするルートがない場合、そのサブネットは BGP でアドバタイズされません。
- Outpost インスタンスにアタッチされているネットワークインターフェイスだけが、その Outpost のローカルゲートウェイを介して通信できます。Outpost サブネットに属しているが、リージョン内のインスタンスに接続されているネットワークインターフェイスは、その Outpost のローカルゲートウェイを介して通信できません。
- VPC エンドポイント用に作成されたものなどのリクエスタ管理インターフェイスは、ローカルゲートウェイ経由では、オンプレミスネットワークからアクセスできません。これらには Outpost サブネット内のインスタンスからのみアクセスできます。

以下の NAT 考慮事項が適用されます。

- ローカルゲートウェイは、ネットワークインターフェイスルートと一致するトラフィックに対して NAT を実行しません。代わりに、宛先 IP アドレスは保持されます。
- ターゲットのネットワークインターフェイスの送信元/送信先チェックを無効にします。詳細については、「Amazon EC2 ユーザーガイド」の「ネットワークインターフェイスの概念」を参照してください。
- 宛先 CIDR からのトラフィックがネットワークインターフェイスで受け入れられるように OS を設定します。

## カスタムローカルゲートウェイルートテーブルの作成

AWS Outposts コンソールを使用してローカルゲートウェイ用のカスタムルートテーブルを作成できます。

コンソールを使用してカスタムローカルゲートウェイルートテーブルを作成するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
3. ナビゲーションペインで、[ローカルゲートウェイのルートテーブル] をクリックします。
4. [ローカルゲートウェイルートテーブルの作成] を選択します。
5. (オプション) [名前] には、ローカルゲートウェイルートテーブルの名前を入力します。

6. [ローカルゲートウェイ] では、ローカルゲートウェイを選択します。
7. (オプション) [VIF グループの関連付け] を選択し、[VIF グループ] を選択します。

   ローカルゲートウェイルートテーブルを編集して、VIF グループをターゲットとする静的ルートを追加します。
8. [モード] では、オンプレミスネットワークとの通信モードを選択します。

   - インスタンスのプライベート IP アドレスを使用するには、[ダイレクト VPC ルーティング] を選択します。
   - カスタマー所有 IP アドレスを使用するには [CoIP] を選択します。
     - (オプション) CoIP プールと追加の CIDR ブロックを追加または削除する

       [CoIP プールの追加] [新しいプールの追加] を選択して、以下を実行します。
       - [名前] には、CoIP ポリシーの名前を入力します。
       - [CIDR] には、カスタマー所有 IP アドレスの CIDR ブロックを入力します。
     - [CIDR ブロックを追加] [新しい CIDR を追加] を選択し、カスタマー所有 IP アドレスの範囲を入力します。
     - [CoIP プールまたは追加の CIDR ブロックを削除] CIDR ブロックの右または CoIP プールの下にある [削除]を選択します。

       最大 10 個の CoIP プールと 100 個の CIDR ブロックを指定できます。
9. (オプション) タグを追加または削除します。

   [タグの追加] [新しいタグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。
10. [ローカルゲートウェイルートテーブルの作成] を選択します。

# ローカルゲートウェイルートテーブルのモードを切り替えるか、ローカルゲートウェイルートテーブルを削除します

モードを切り替えるには、ローカルゲートウェイルートテーブルを削除し、改めて作成する必要があります。ローカルゲートウェイルートテーブルを削除すると、ネットワークトラフィックが中断されます。

モードを切り替えたり、ローカルゲートウェイルートテーブルを削除するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 正しい AWS リージョンを使用していることを確認します。

   リージョンを変更するには、ページの右上にあるリージョンセレクターを使用します。
3. ナビゲーションペインで、[ローカルゲートウェイのルートテーブル] をクリックします。
4. VIF グループが関連付けられているローカルゲートウェイルートテーブルを検証します。関連付けられている場合は、ローカルゲートウェイルートテーブルと VIF グループ間の関連付けを削除する必要があります。

   a. ローカルゲートウェイルートテーブルの ID を選択します。

   b. [VIF グループの関連付け] タブを選択します。

   c. 1 つ以上の VIF グループがローカルゲートウェイルートテーブルに関連付けられている場合は、[VIF グループの関連付けを編集] を選択します。

   d. [VIF グループを関連付ける] チェックボックスをオフにします。

   e. [Save changes] (変更の保存) をクリックします。
5. [ローカルゲートウェイのルートテーブルを削除] を選択します。
6. 確認ダイアログボックスで、**delete** と入力し、[削除] を選択します。
7. (オプション) 新しいモードでローカルゲートウェイルートテーブルを作成します。

   a. ナビゲーションペインで、[ローカルゲートウェイのルートテーブル] をクリックします。

   b. [ローカルゲートウェイルートテーブルの作成] を選択します。

   c. 新しいモードを使用して、ローカルゲートウェイルートテーブルを設定します。詳細については、「カスタムローカルゲートウェイルートテーブルを作成する」を参照してください。

# CoIP プールを作成する

IP アドレス範囲を指定して、オンプレミス ネットワークと VPC 内のインスタンス間の通信を簡単にすることができます。詳細については、「カスタマー所有 IP アドレス」を参照してください。

カスタマー所有 IP プールは、CoIP モードのローカルゲートウェイルートテーブルで使用できます。

以下の手順に従って CoIP プールを作成します。

Console

コンソールを使用して CoIP プールを作成する

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
3. ナビゲーションペインで、[ローカルゲートウェイのルートテーブル] をクリックします。
4. [ルートテーブル] を選択します。
5. 詳細ペインの [CoIP プール] タブを選択し、[CoIP プールの作成] を選択します。
6. (オプション) [名前] には、使用する CoIP プールの名前を入力します。
7. [新しい CIDR を追加] を選択し、カスタマー所有 IP アドレスの範囲を入力します。
8. (オプション) CIDR ブロックを追加するには、[新しい CIDR を追加] を選択し、顧客所有 IP アドレスの範囲を入力します。
9. [CoIP プールの作成] を選択します。

AWS CLI

を使用して CoIP プールを作成するには AWS CLI

1. create-coip-pool コマンドを使用して、指定されたローカルゲートウェイルートテーブルの CoIP アドレスのプールを作成します。

```
aws ec2 create-coip-pool --local-gateway-route-table-id lgw-rtb-
abcdefg1234567890
```

以下は出力の例です。

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

2. create-coip-cidr コマンドを使用して、指定された CoIP プールに CoIP アドレスの範囲を作成します。

```
aws ec2 create-coip-cidr --cidr 15.0.0.0/24 --coip-pool-id ipv4pool-
coip-1234567890abcdefg
```

以下は出力の例です。

```
{
    "CoipCidr": {
        "Cidr": "15.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

CoIP プールを作成したら、次の手順を使用してインスタンスにアドレスを割り当てます。

Console

コンソールを使用して、CoIP アドレスをインスタンスに割り当てるには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Elastic IP] を選択します。
3. [Elastic IP アドレスの割り当て] を選択します。
4. [ネットワーク境界グループ] で、IP アドレスがアドバタイズされる場所を選択します。
5. [パブリック IPv4 アドレスプール] で、[カスタマー所有 IPv4 アドレスプール] を選択します。
6. [カスタマー所有の IPv4 アドレスプール] では、構成したプールを選択します。

7. [割り当て] を選択してください。
8. Elastic IP アドレスを選択してから、[アクション]、[Elastic IP アドレスの関連付け] の順に選択します。
9. [インスタンス] からインスタンスを選択し、次に [アソシエイト] を選択します。

AWS CLI

を使用して CoIP アドレスをインスタンスに割り当てるには AWS CLI

1. describe-coip-pools コマンドを使用して、顧客所有のアドレスプールに関する情報を取得してください。

```
aws ec2 describe-coip-pools
```

以下は出力の例です。

```
{
    "CoipPools": [
        {
            "PoolId": "ipv4pool-coip-0abcdef0123456789",
            "PoolCidrs":  [
                "192.168.0.0/16"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-0abcdef0123456789"
        }
    ]
}
```

2. [アドレスの割り当て] コマンドを使用して、Elastic IP アドレスを割り当てます。前のステップで返されたプール ID を使用します。

```
aws ec2 allocate-address--address 192.0.2.128 --customer-owned-ipv4-
pool ipv4pool-coip-0abcdef0123456789
```

以下は出力の例です。

```
{
    "CustomerOwnedIp": "192.0.2.128",
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
```

```
    "CustomerOwnedIpv4Pool": "ipv4pool-coip-0abcdef0123456789",
}
```

3. 次のように、アドレスの関連付け コマンドを使用して、Elastic IP アドレスを Outpost インスタンスに関連付けます。前の手順で返された割り当て ID を使用します。

```
aws ec2 associate-address --allocation-id eipalloc-02463d08ceEXAMPLE --network-
interface-id eni-1a2b3c4d
```

以下は出力の例です。

```
{
    "AssociationId": "eipassoc-02463d08ceEXAMPLE",
}
```

# Outposts ラックのローカルネットワーク接続

Outposts ラックをオンプレミスネットワークに接続するには、以下のコンポーネントが必要です。

- Outpost パッチパネルからカスタマーのローカルネットワークデバイスへの物理接続。
- Outpost ネットワークデバイスとローカルネットワークデバイスへの 2 つのリンクアグリゲーショングループ (LAG) 接続を確立するリンクアグリゲーションコントロールプロトコル (LACP)。
- Outpost とカスタマーのローカルネットワークデバイス間の仮想 LAN (VLAN) 接続。
- 各 VLAN のレイヤ 3 ポイントツーポイント接続。
- Outpost とオンプレミスサービスリンク間のルートアドバタイズ用のボーダーゲートウェイプロトコル (BGP)。
- Outpost とオンプレミスのローカルネットワークデバイス間のルートアドバタイズ用の BGP。

内容



## 物理的な接続

Outposts ラックには、ローカルネットワークに接続する 2 つの物理ネットワークデバイスがあります。

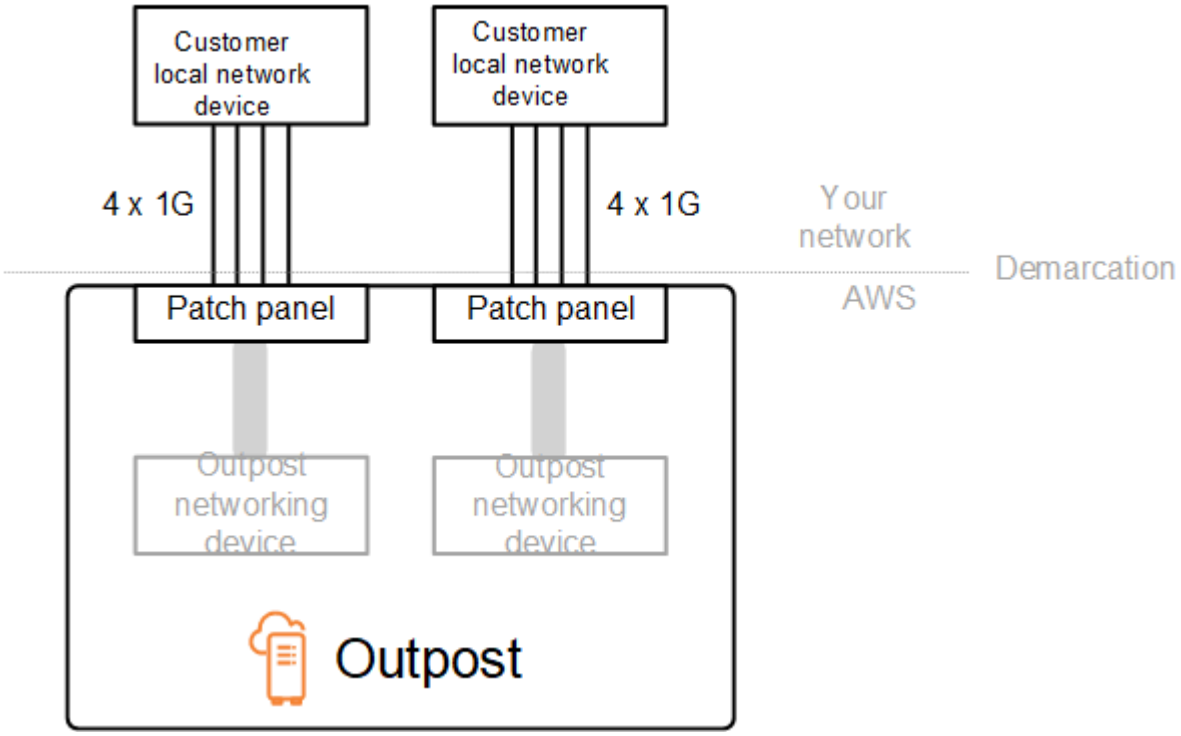
Outpost には、これらの Outpost ネットワークデバイスとローカルネットワークデバイスとの間に最低 2 つの物理リンクが必要です。Outpost は Outpost ネットワークデバイスごとに以下のアップリンク速度とアップリンク数をサポートします。

| 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 Gbps または 100 Gbps | 1、2 または 4 |

アップリンクの速度と数は各 Outpost ネットワークデバイスで左右対称です。アップリンク速度として 100 Gbps を使用する場合は、前方誤り訂正 (FEC CL91) を使用してリンクを設定する必要があります。

Outposts ラックは、Lucent Connector (LC) を使用したシングルモードファイバー (SMF)、マルチモードファイバー (MMF)、または LC を使用した MMF OM4 をサポートできます。 は、ラック位置で提供するファイバーと互換性のあるオプティクス AWS を提供します。

以下の図では、物理的な境界は各 Outpost のファイバーパッチパネルです。Outpost をパッチパネルに接続するのに必要なファイバーケーブルを用意します。



# リンクアグリゲーション

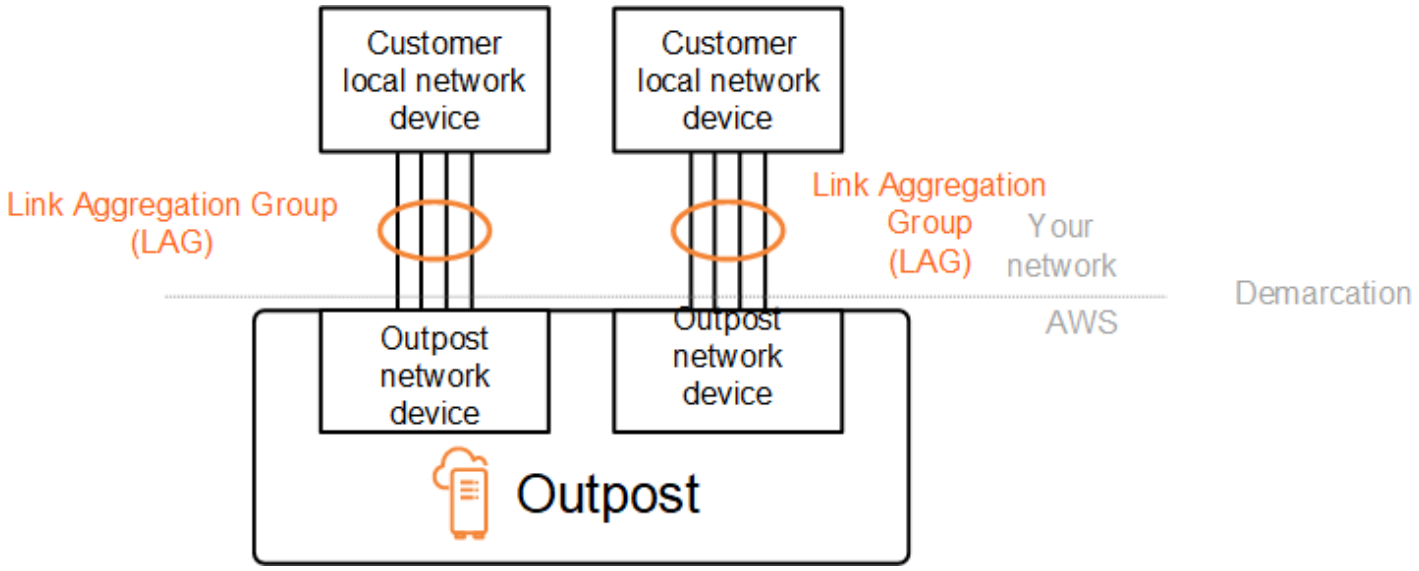
AWS Outposts は、リンク集約制御プロトコル (LACP) を使用して、Outpost ネットワークデバイスとローカルネットワークデバイス間のリンク集約グループ (LAG) 接続を確立します。各 Outpost ネットワークデバイスからのリンクは 1 つのイーサネット LAG に集約され、1 つのネットワーク接続を表します。これらの LAG は標準の高速タイマで LACP を使用します。低速タイマを使用するように LAG を設定することはできません。

サイトで Outpost を設置できるようにするには、ネットワークデバイス上でユーザー側の LAG 接続を設定する必要があります。

論理的には、Outpost のパッチパネルを境界点として無視し、Outpost のネットワークデバイスを使用してください。

ラックが複数あるデプロイでは、Outpost ネットワークデバイスのアグリゲーションレイヤーとローカルネットワークデバイスの間に 4 つの LAG が必要です。

次の図は、各 Outpost ネットワークデバイスとそれに接続されたローカルネットワークデバイス間の 4 つの物理接続を示しています。イーサネット LAG を使用して、Outpost ネットワークデバイスとカスタマーのローカルネットワークデバイスを接続する物理リンクを集約します。




# 仮想 LAN

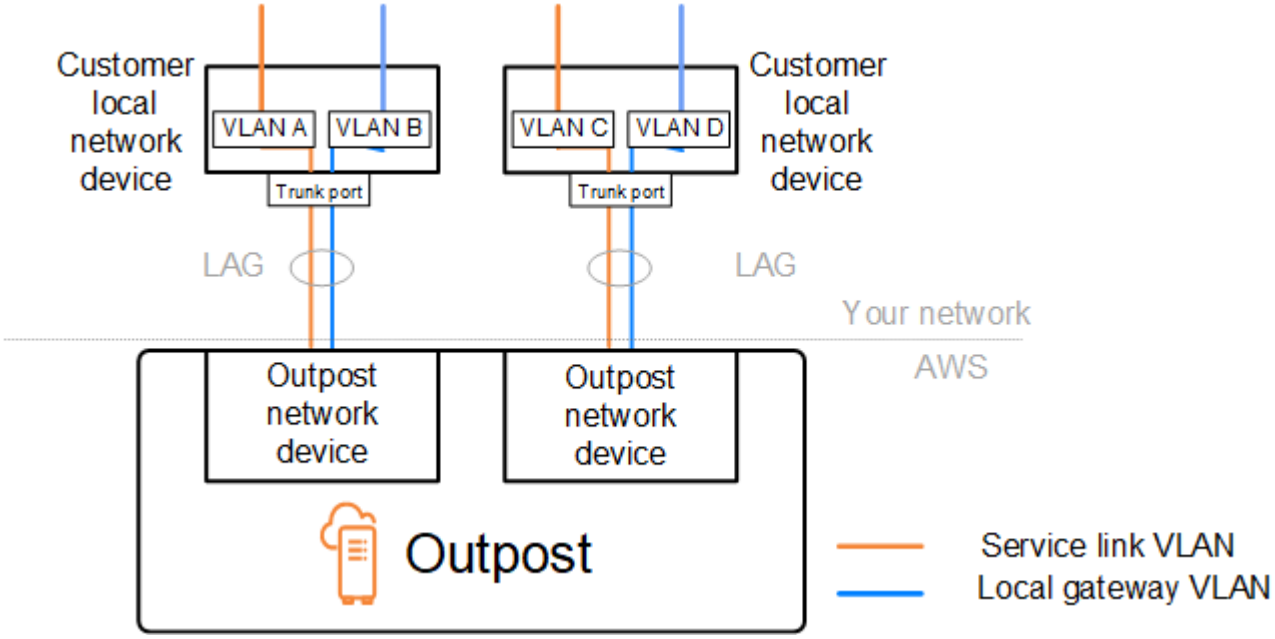
Outpost ネットワークデバイスとローカルネットワークデバイス間の各 LAG は IEEE 802.1q イーサネットトランクとして設定する必要があります。これにより、複数の VLAN を使用してデータパス間のネットワークを分離できます。

各 Outpost には、ローカルネットワークデバイスと通信するため、以下のような VLAN があります。

- サービスリンク VLAN - サービスリンク接続のサービスリンクパスを確立するために、Outpost とローカルネットワークデバイス間の通信を有効にします。詳細については、「AWS Outposts connectivity to AWS Regions」を参照してください。
- ローカルゲートウェイ VLAN - Outpost サブネットとローカルエリアネットワークを接続するローカルゲートウェイパスを確立するために、Outpost とローカルネットワークデバイス間の通信を有効にします。Outpost ローカルゲートウェイは、この VLAN を利用してインスタンスにオンプレミスネットワーク (ネットワーク経由のインターネットアクセスを含む) への接続を提供します。詳細については、「Local gateway」を参照してください。

サービスリンク VLAN とローカルゲートウェイ VLAN は、Outpost とカスタマーのローカルネットワークデバイス間でのみ設定できます。

Outpost は、サービスリンクとローカルゲートウェイのデータパスを 2 つの独立したネットワークに分離するように設計されています。これにより、Outpost で実行されているサービスと通信できるネットワークを選択できます。また、カスタマーのローカルネットワークデバイス上の複数のルートテーブルを使用することで、サービスリンクをローカルゲートウェイネットワークから分離したネットワークにすることもできます(一般に仮想ルーティング/転送インスタンス (VRF) と呼ばれます)。境界線は、Outpost ネットワークデバイスのポートに存在します。 は、接続の AWS 側にあるインフラストラクチャ AWS をすべて管理し、 は、回線の 側にあるインフラストラクチャを管理します。



設置中および運用中に Outpost をオンプレミスネットワークと統合するには、Outpost ネットワークデバイスとカスタマーのローカルネットワークデバイス間で使用する VLAN を割り当てる必要があります。インストール AWS する前に、この情報を に提供する必要があります。詳細については、「the section called “ネットワーク準備チェックリスト”」を参照してください。

# ネットワークレイヤー接続

ネットワーク層での接続を確立するために、各 Outpost ネットワークデバイスには、各 VLAN の IP アドレスを含む仮想インターフェイス (VIF) が設定されています。これらの VIF によって、 AWS Outposts ネットワークデバイスは、ローカルネットワーク機器との IP 接続と BGP セッションを設定できます。

次の構成を推奨します。

- この論理的なポイントツーポイント接続を表すには、CIDR が/30 または /31 である専用サブネットを使用します。
- 顧客のローカルネットワークデバイス間では、VLAN をブリッジしないでください。

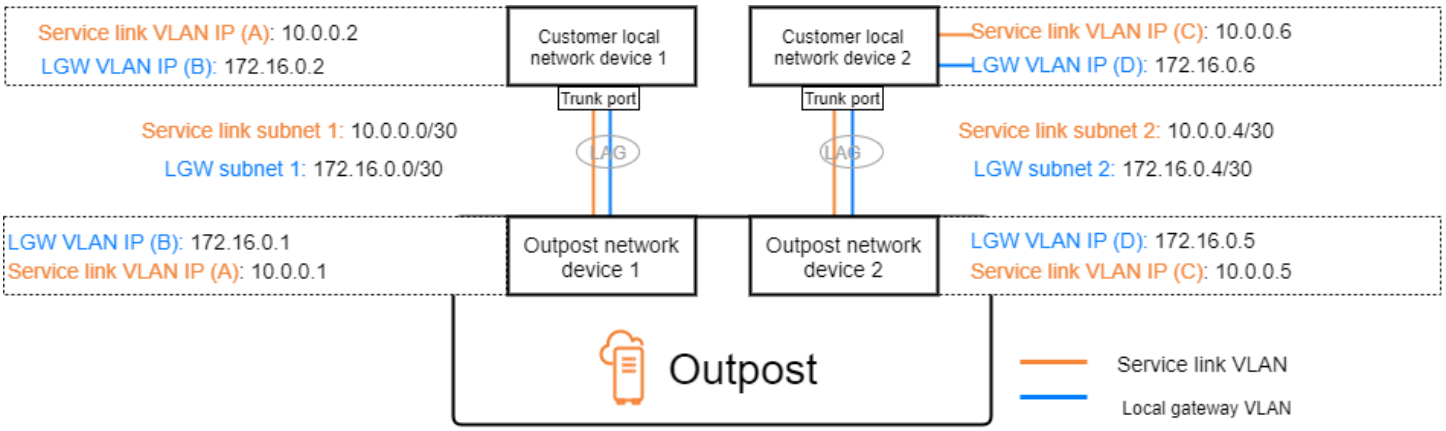
ネットワーク層での接続には、次の 2 つのパスを確立する必要があります。

- サービスリンクパス - このパスを確立するには、/30 または /31 の範囲の VLAN サブネットと、AWS Outposts ネットワークデバイス上のサービスリンク VLAN の IP アドレスを指定します。サービスリンク仮想インターフェイス (VIF) は、このパスで Outpost とローカルネットワークデバイス間の IP 接続と BGP セッションを確立し、サービスリンク接続に使用します。詳細については、「AWS Outposts connectivity to AWS Regions」を参照してください。
- ローカルゲートウェイパス - このパスを確立するには、/30 または /31 の範囲の VLAN サブネットと、 AWS Outposts ネットワークデバイス上のローカルゲートウェイ VLAN の IP アドレスを指定します。このパスでは、ローカルゲートウェイ VIF を使用して、Outpost とローカルネットワークデバイス間の IP 接続と BGP セッションを確立し、ローカルリソース接続を行います。

次の図は、サービスリンクパスとローカルゲートウェイパスの、各 Outpost ネットワークデバイスからカスタマーのローカルネットワークデバイスへの接続を示しています。この例には 4 つの VLAN があります。

- VLAN A は Outpost ネットワークデバイス 1 とカスタマーのローカルネットワークデバイス 1 を接続するサービスリンクパス用です。

- VLAN B は Outpost ネットワークデバイス 1 とカスタマーのローカルネットワークデバイス 1 を接続するローカルゲートウェイパス用です。
- VLAN C は Outpost ネットワークデバイス 2 とカスタマーのローカルネットワークデバイス 2 を接続するサービスリンクパス用です。
- VLAN D は Outpost ネットワークデバイス 2 とカスタマーのローカルネットワークデバイス 2 を接続するローカルゲートウェイパス用です。




次の表は、Outpost ネットワークデバイス 1 とカスタマーのローカルネットワークデバイス 1 を接続するサブネットの値の例を示しています。

| VLAN | サブネット | カスタマーデバイス 1 の IP アドレス | AWS OND 1 IP |
|---|---|---|---|
| A | 10.0.0.0/30 | 10.0.0.2 | 10.0.0.1 |
| B | 172.16.0.0/30 | 172.16.0.2 | 172.16.0.1 |

次の表は、Outpost ネットワークデバイス 2 とカスタマーのローカルネットワークデバイス 2 を接続するサブネットの値の例を示しています。

| VLAN | サブネット | カスタマーデバイス 2 の IP アドレス | AWS OND 2 IP |
|---|---|---|---|
| C | 10.0.0.4/30 | 10.0.0.6 | 10.0.0.5 |
| D | 172.16.0.4/30 | 172.16.0.6 | 172.16.0.5 |

# ACE ラック接続

> **Note**
>
> ACE ラックが必要ない場合は、このセクションをスキップしてください。

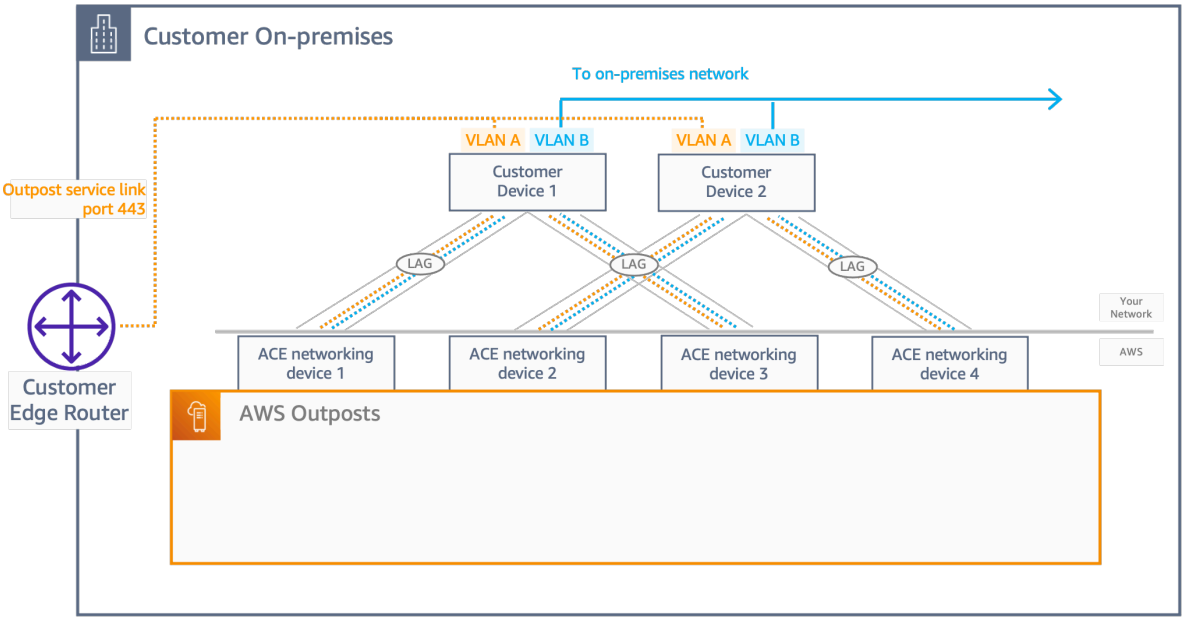
集約、コア、エッジ (ACE) ラックは、複数ラックの Outpost のデプロイにおけるネットワーク集約ポイントとして機能します。コンピューティングラックが 4 架以上ある場合は、ACE ラックを使用する必要があります。コンピューティングラックが 4 架未満であっても、今後 4 架以上のラックに拡張する予定がある場合は、早期に ACE ラックを設置することをお勧めします。

ACE ラックを使用すると、Outposts ネットワークデバイスはオンプレミスネットワークデバイスに直接接続されなくなります。代わりに、これらのデバイスは ACE ラックに接続され、Outposts ラックへの接続を提供します。このトポロジでは、 は Outposts ネットワークデバイスと ACE ネットワークデバイス間の VLAN インターフェイスの割り当てと設定 AWS を所有します。

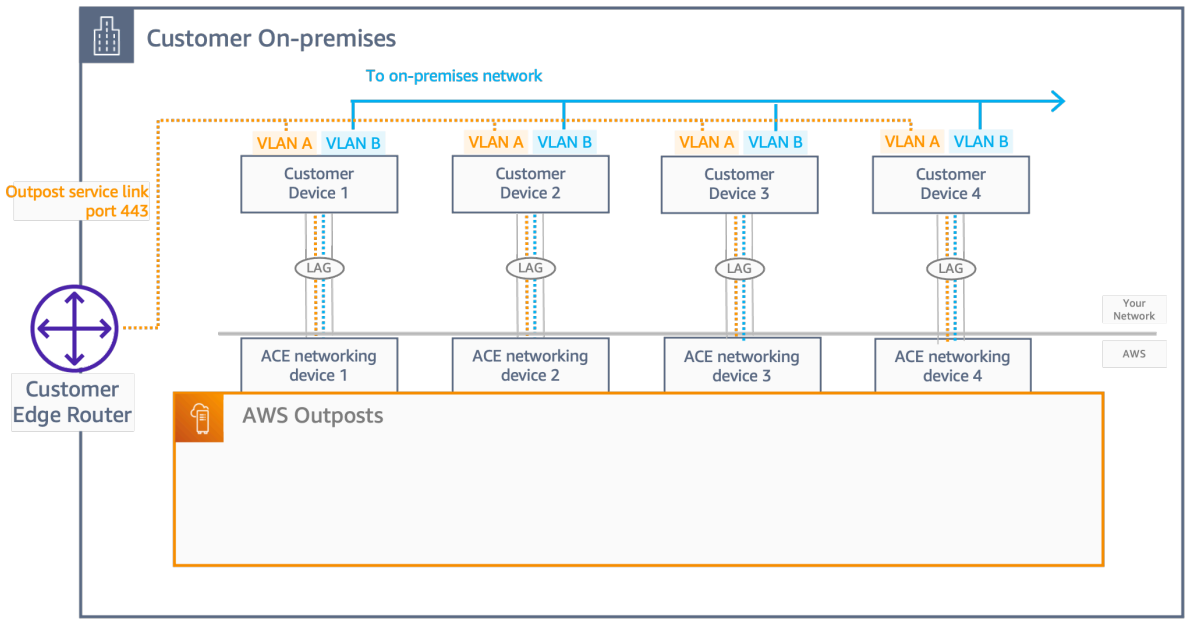
ACE ラックには 4 台のネットワークデバイスが設置されており、顧客のオンプレミスネットワーク内の 2 台のアップストリームの顧客デバイスまたは 4 台のアップストリームの顧客デバイスに接続して、回復性を最大化できます。

次の図は、2 種類のネットワークトポロジを示しています。

次の図は、2 台のアップストリームの顧客デバイスに接続された ACE ラックの 4 台の ACE ネットワークデバイスを示しています。



次の図は、4 台のアップストリームの顧客デバイスに接続された ACE ラックの 4 台の ACE ネットワークデバイスを示しています。



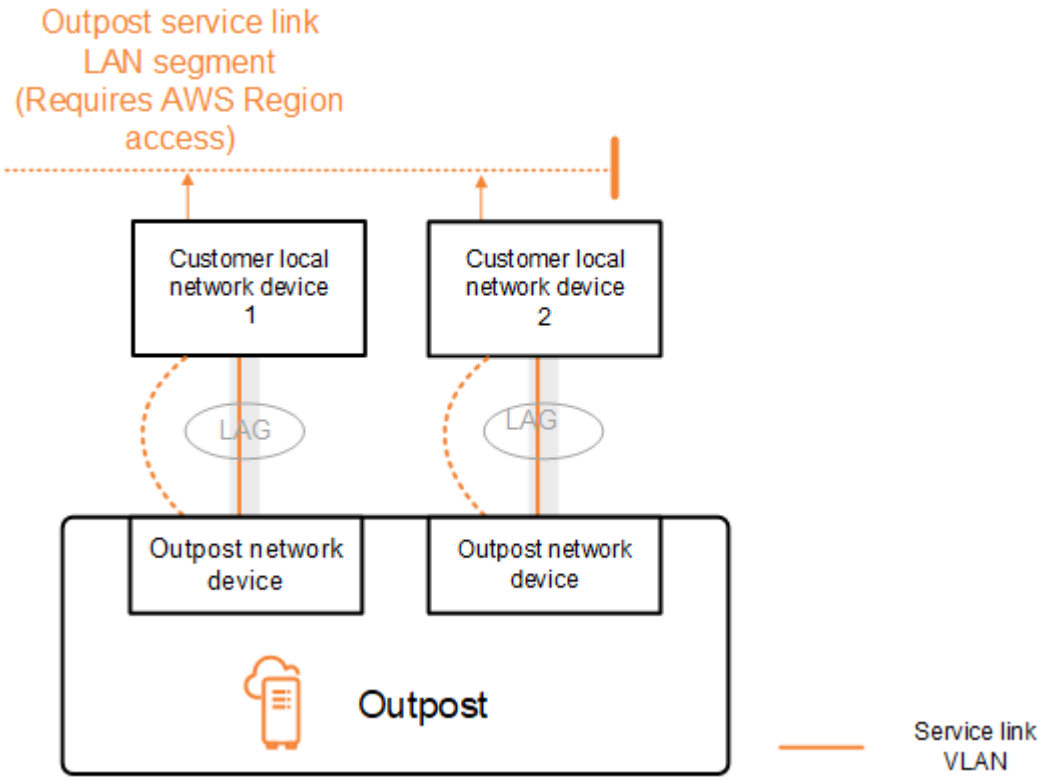

# サービスリンク (BGP 接続)

Outpost は、サービスリンク VLAN を介したサービスリンク接続のために、各 Outpost ネットワークデバイスとカスタマーのローカルネットワークデバイスとの間に外部 BGP ピアリングセッションを確立します。BGP ピアリングセッションは、ポイントツーポイント VLAN に提供された /30 または /31 IP アドレス間で確立されます。各 BGP ピアリングセッションでは、Outpost ネットワークデバイス上のプライベート自律システム番号 (ASN) と、お客様のローカルネットワークデバイス用に選択した ASN を使用します。インストールプロセスの一環として、 は指定した属性 AWS を設定します。

2 台の Outpost ネットワークデバイスが 1 台の Outpost で、サービスリンク VLAN によって 2 台のカスタマーのローカルネットワークデバイスに接続されているシナリオを考えてみましょう。サービスリンクごとに、次のインフラストラクチャとカスタマーのローカルネットワークデバイス BGP ASN 属性を設定します。

- サービスリンク BGP ASN。2 バイト (16 ビット) または 4 バイト (32 ビット)。有効な値は 64512-65535 または 4200000000-4294967294 です。
- インフラストラクチャ CIDR。これはラックあたり CIDR /26 でなければなりません。
- カスタマーのローカルネットワークデバイス 1 のサービスリンク BGP ピア IP アドレス。
- カスタマーのローカルネットワークデバイス 1 のサービスリンク BGP ピア ASN。有効な値は 1 ～ 4294967294 です。

- カスタマーのローカルネットワークデバイス 2 のサービスリンク BGP ピア IP アドレス。
- カスタマーのローカルネットワークデバイス 2 のサービスリンク BGP ピア ASN。有効な値は 1 ~ 4294967294 です。詳細については、「RFC4893」を参照してください。




Outpost は、以下のプロセスを使用してサービスリンク VLAN 上で外部 BGP ピアリングセッションを確立します。

1. 各 Outpost ネットワークデバイスは ASN を使用して、接続されているローカルネットワークデバイスとの BGP ピアリングセッションを確立します。
2. Outpost ネットワークデバイスは、リンクやデバイスの障害に対応するため、/26 の CIDR 範囲を 2 つの /27 の CIDR 範囲としてアドバタイズします。各 OND は、AS パス長 1 の独自の /27 プレフィックスと、AS パス長 4 のその他すべての OND の /27 プレフィックスをバックアップとしてアドバタイズします。
3. サブネットは、Outpost から AWS リージョンへの接続に使用されます。

BGP 属性を変更せずに Outposts から BGP アドバタイズを受信するようにカスタマーのネットワーク機器を設定することをお勧めします。お客様のネットワークは、4 の AS-Path length のルートよりも、1 の AS-Path length の Outposts からのルートを優先する必要があります。

お客様のネットワークは、すべての OND に対して、同じ属性を持つ同じ BGP プレフィックスをアドバタイズする必要があります。デフォルトでは、Outpost ネットワークロードバランスはすべてのアップリンク間でアウトバウンドトラフィックの負荷分散を行います。Outpost 側では、メンテナンスが必要な場合にトラフィックを OND から移行するために、ルーティングポリシーが使用されます。このトラフィックのシフトには、すべての OND で顧客側からの等しい BGP プレフィックスが必要です。お客様のネットワークでメンテナンスが必要な場合は、AS-Path への付加を使用して、特定のアップリンクからのトラフィックを一時的に移行することをお勧めします。

# サービスリンクインフラストラクチャ、サブネットアドバタイズメント、および IP 範囲

サービスリンクインフラストラクチャサブネットのプレインストールプロセスで /26 の CIDR 範囲を指定します。Outpost インフラストラクチャは、この範囲を使用して、サービスリンクを介してリージョンへの接続を確立します。サービスリンクサブネットは Outpost ソースであり、接続を開始します。

Outpost ネットワークデバイスは、リンクやデバイスの障害に対応するため、/26 の CIDR 範囲を 2 つの /27 の CIDR ブロックとしてアドバタイズします。

Outpost のサービスリンク BGP ASN とインフラストラクチャサブネット CIDR (/26) を指定する必要があります。Outpost ネットワークデバイスごとに、ローカルネットワークデバイスの VLAN 上の BGP ピアリング IP アドレスとローカルネットワークデバイスの BGP ASN を提供します。

複数のラックをデプロイしている場合は、ラックごとに /26 サブネットを 1 つ用意する必要があります。

# ローカルゲートウェイの BGP 接続

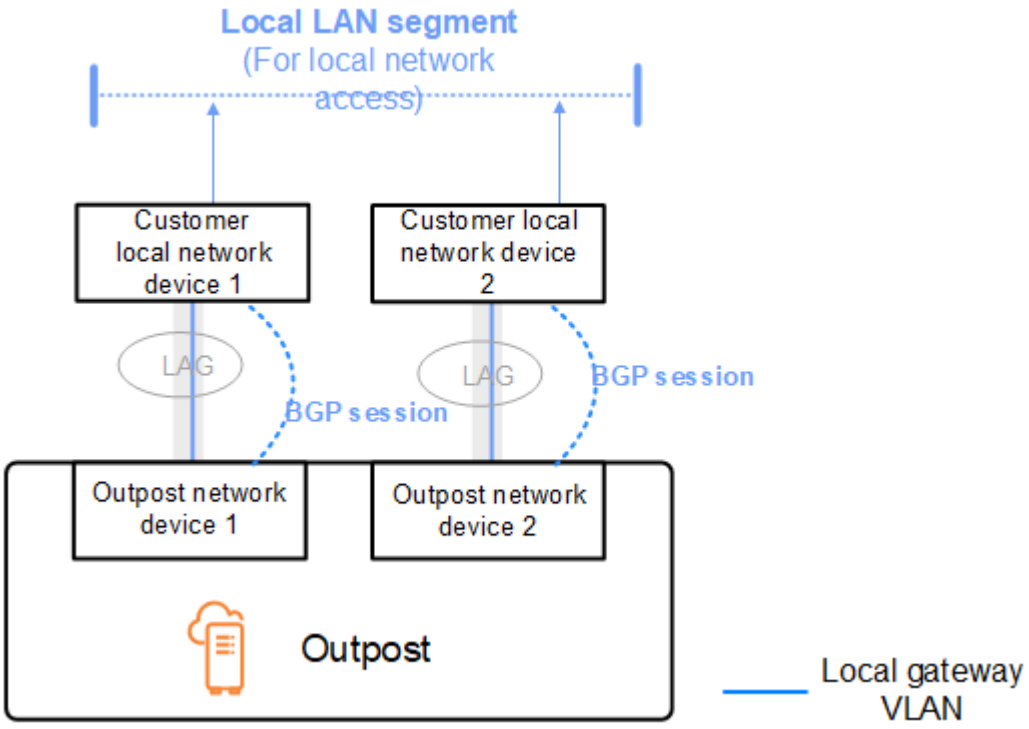
Outpost は、外部 BGP セッションを確立するために割り当てたプライベート自律システム番号 (ASN) を使用します。各 Outpost ネットワークデバイスには、自身のローカルゲートウェイ VLAN を使用してローカルネットワークデバイスとピアリングする外部 BGP が 1 つあります。

Outpost は、各 Outpost ネットワークデバイスと接続されているカスタマーのローカルネットワークデバイスとの間で、ローカルゲートウェイ VLAN 上で外部 BGP ピアリングセッションを確立します。ピアリングセッションは、ネットワーク接続の設定時に指定した /30 または /31 IP アドレス間で確立され、Outpost ネットワークデバイスとカスタマーのローカルネットワークデバイス間のポイントツーポイント接続を使用します。詳細については、「the section called “ネットワークレイヤー接続”」を参照してください。

各 BGP セッションでは、Outpost ネットワークデバイス側でプライベート ASN を使用し、お客様のローカルネットワークデバイス側で選択した ASN を使用します。 は、プリインストールプロセスの一環として属性 AWS を設定します。

2 台の Outpost ネットワークデバイスが 1 台の Outpost で、サービスリンク VLAN によって 2 台のカスタマーのローカルネットワークデバイスに接続されているシナリオを考えてみましょう。サービスリンクごとに、次のローカルゲートウェイとカスタマーローカルネットワークデバイスの BGP ASN 属性を設定します。

- お客様はローカルゲートウェイ BGP ASN を提供します。2 バイト (16 ビット) または 4 バイト (32 ビット ) 。有効な値は 64512-65535 または 4200000000-4294967294 です。
- (オプション) アドバタイズされるカスタマー所有 CIDR (パブリックまたはプライベート、最低 /26) を指定します。
- カスタマーのローカルネットワークデバイス 1 のローカルゲートウェイ BGP ピア IP アドレスを提供します。
- カスタマーローカルネットワークデバイス 1 のローカルゲートウェイ BGP ピア ASN を提供します。有効な値は 1 ~ 4294967294 です。詳細については、「RFC4893」を参照してください。
- カスタマーのローカルネットワークデバイス 2 のローカルゲートウェイ BGP ピア IP アドレスを提供します。
- カスタマーローカルネットワークデバイス 2 のローカルゲートウェイ BGP ピア ASN を提供します。有効な値は 1 ~ 4294967294 です。詳細については、「RFC4893」を参照してください。




お客様のネットワーク機器は、BGP 属性を変更せずに Outpost から BGP アドバタイズを受信し、BGP マルチパス/ロードバランシングを有効にして最適なインバウンドトラフィックフローを可能にすることをお勧めします。AS-Path のプリペンドは、メンテナンスが必要な場合にトラフィックを OND から離れるようにするために、ローカルゲートウェイのプレフィックスに使用されます。お客様のネットワークは、4 の AS-Path length のルートよりも、1 の AS-Path length の Outposts からのルートを優先する必要があります。

お客様のネットワークは、すべての OND に対して、同じ属性を持つ同じ BGP プレフィックスをアドバタイズする必要があります。デフォルトでは、Outpost ネットワークロードバランスはすべてのアップリンク間でアウトバウンドトラフィックの負荷分散を行います。Outpost 側では、メンテナンスが必要な場合にトラフィックを OND から移行するために、ルーティングポリシーが使用されます。このトラフィックのシフトには、すべての OND で顧客側からの等しい BGP プレフィックスが必要です。お客様のネットワークでメンテナンスが必要な場合は、AS-Path への付加を使用して、特定のアップリンクからのトラフィックを一時的に移行することをお勧めします。

# ローカルゲートウェイのカスタマー所有 IP サブネットアドバタイズ

デフォルトでは、ローカルゲートウェイは VPC 内のインスタンスのプライベート IP アドレス (「直接 VPC ルーティング」を参照) 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。ただし、カスタマー所有 IP アドレスプール (CoIP) を提供できます。

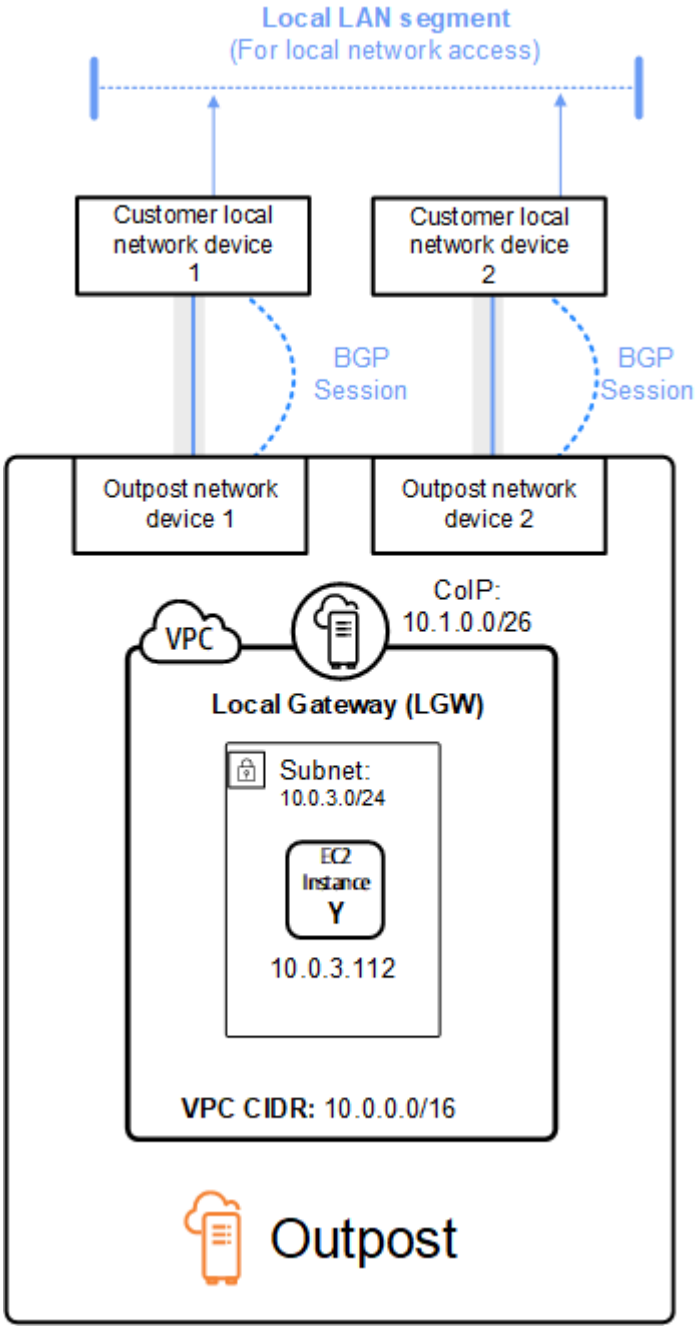
このプールから Elastic IP アドレスを作成し、そのアドレスを Outpost 上のリソース (EC2 インスタンスなど) に割り当てることができます。

ローカルゲートウェイは Elastic IP アドレスをカスタマー所有プール内のアドレスに変換します。ローカルゲートウェイは、変換されたアドレスをオンプレミスネットワークおよび Outpost と通信するその他のネットワークにアドバタイズします。アドレスは、両方のローカルゲートウェイ BGP セッションでローカルネットワークデバイスにアドバタイズされます。

> **Tip**
>
> CoIP を使用していない場合、BGP はルートテーブルにローカルゲートウェイをターゲットとするルートがある Outpost 上のサブネットのプライベート IP アドレスをアドバタイズします。

2 台の Outpost ネットワークデバイスが 1 台の Outpost で、サービスリンク VLAN によって 2 台のカスタマーのローカルネットワークデバイスに接続されているシナリオを考えてみましょう。以下が設定されています。

- CIDR ブロック 10.0.0.0/16 を持つ VPC。
- CIDR ブロック 10.0.3.0/24 の VPC 内のサブネット。
- プライベート IP アドレスが 10.0.3.112 のサブネット内の EC2 インスタンス。
- カスタマー所有 IP プール (10.1.0.0/26)。
- 10.0.3.112 を 10.1.0.2 に関連付ける Elastic IP アドレス関連付け。
- BGP を使用してローカルデバイスを介して 10.1.0.0/26 をオンプレミスネットワークにアドバタイズするローカルゲートウェイ。
- Outpost とオンプレミスネットワーク間の通信では、CoIP Elastic IP を使用して Outpost 内のインスタンスをアドレス指定しますが、VPC CIDR 範囲は使用されません。


Local LAN segment
(For local network access)
Customer local network device 1
Customer local network device 2
BGP Session
BGP Session
Outpost network device 1
Outpost network device 2
CoIP: 10.1.0.0/26
VPC
Local Gateway (LGW)
Subnet: 10.0.3.0/24
EC2 Instance Y
10.0.3.112
VPC CIDR: 10.0.0.0/16
Outpost

# のキャパシティ管理 AWS Outposts

Outpost は、 AWS リージョンのアベイラビリティーゾーンのプライベート拡張として、サイトに AWS コンピューティングとストレージ容量のプールを提供します。Outpost で利用可能なコンピューティングおよびストレージ容量は有限であり、 がサイトに AWS インストールするアセットのサイズと数によって決定されるため、初期ワークロードの実行、将来の成長への対応、サーバーの障害とメンテナンスイベントを軽減するための追加容量の提供に必要な AWS Outposts 容量に対する Amazon EC2、Amazon EBS、Amazon S3 の量を決定できます。

トピック



## AWS Outposts 容量の表示

キャパシティ設定は、インスタンスレベルまたは Outpost レベルで表示できます。

コンソールを使用して Outpost の容量設定を表示するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 左側のナビゲーションペインから、Outposts を選択します。
3. Outpost を選択します。
4. Outpost の詳細ページで、インスタンスビューまたはラックビューを選択します。
   - インスタンスビュー - Outposts で設定されたインスタンスと、サイズとファミリー別のインスタンスのディストリビューションに関する情報を提供します。
   - ラックビュー - 各 Outpost 内の各アセットのインスタンスを視覚化し、インスタンス容量を変更を選択してインスタンス容量を変更することができます。

## AWS Outposts インスタンス容量の変更

新規の各 Outpost 注文のキャパシティは、デフォルトのキャパシティ設定で設定されています。デフォルトの設定を変換して、ビジネスニーズに合わせたさまざまなインスタンスを作成できます。そ

のためには、キャパシティタスクを作成し、Outposts または 1 つのアセットを選択し、インスタンスのサイズと数量を指定し、キャパシティタスクを実行して変更を実装します。

## 考慮事項

インスタンス容量を変更する前に、次の点を考慮してください。

- キャパシティタスクは、Outpost リソースを所有する AWS アカウント (所有者) のみが実行できます。コンシューマーはキャパシティタスクを実行できません。所有者とコンシューマーの詳細については、「リソースの共有 AWS Outposts」を参照してください。
- インスタンスのサイズと数量は、Outpost レベルまたは個々のアセットレベルで定義できます。
- 容量は、可能な設定とベストプラクティスに基づいて、Outpost 内のアセットまたはすべてのアセットにわたって自動的に設定されます。
- キャパシティタスクの実行中に、選択した Outpost に関連付けられたアセットが分離される可能性があります。このため、Outposts で新しいインスタンスを起動する予定がない場合にのみ、キャパシティタスクを作成することをお勧めします。
- キャパシティタスクをすぐに実行するか、次の 48 時間にわたって定期的に試行し続けるかを選択できます。すぐに実行することを選択すると、アセットの分離時間が短くなりますが、タスクを実行するためにインスタンスを停止する必要がある場合、タスクは失敗する可能性があります。定期的に実行することを選択すると、タスクが失敗する前にインスタンスを停止する時間が長くなりますが、アセットはより長く分離される可能性があります。
- 有効な容量設定では、アセットで使用可能なすべての vCPU を使用できない場合があります。この場合、インスタンスタイプセクションの最後に、キャパシティーが不足していることを通知するメッセージが表示されますが、リクエストに応じて設定を適用できます。
- コンソールで Outpost を変更すると、ディスクバッキングされたインスタンスとディスクバnon-disk-backedインスタンスの混在はコンソールで完全にはサポートされていないため、サポートされているすべてのインスタンスが表示されません。可能なすべてのインスタンスにアクセスするには、StartCapacityTask API を使用します。
- Outpost の容量を定義する場合、回避するインスタンスとしてリストされていない限り、すべてのインスタンスファミリーとタイプが再設定に含まれます。
- 既存の Outposts 容量設定を変更できるのは、それぞれのアセットモデルでサポートされているインスタンスファミリーから有効な Amazon EC2 インスタンスサイズを使用するようにのみです。
- Outpost で実行中のインスタンスでキャパシティタスクの実行を停止しない場合は、「インスタンス」セクションでそれぞれのインスタンス ID を選択してそのままにしておきます。オプションで、更新されたキャパシティ設定で必要な量のこのインスタンスサイズを保持してください。こ

れにより、キャパシティタスクの実行中に本稼働ワークロードをサポートするために使用されているインスタンスが保持されます。

- インスタンスファミリー内で複数のインスタンスサイズを持つアセットを設定するときは、自動分散を使用して、ドロップレットを過剰または過小プロビジョニングしようとしていないことを確認します。オーバープロビジョニングはサポートされていないため、キャパシティタスクが失敗します。
- 元の容量設定からインスタンスサイズを保持せずに Outpost でインスタンスファミリーを完全に再設定する場合は、容量タスクを実行する前に Outpost でそのファミリーの実行中のインスタンスを停止する必要があります。インスタンスが別のアカウントによって所有されているか、Outpost で実行されているレイヤードサービスによって使用されている場合は、インスタンス所有者アカウントを使用してインスタンスまたはサービスインスタンスを停止する必要があります。
- 相互に排他的な AssetIDs のセットに適用される限り、複数のキャパシティタスクを並行して実行できます。たとえば、異なる AssetIDs に対して複数のアセットレベルのキャパシティタスクを同時に作成できます。ただし、実行中の Outpost レベルのタスクがある場合、別の Outpost またはアセットレベルのタスクを同時に作成することはできません。同様に、実行中のアセットレベルのタスクがある場合、同じAssetID に Outpost レベルのタスクまたはアセットレベルのタスクを同時に作成することはできません。

コンソールを使用して Outpost の容量設定を変更するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 左側のナビゲーションペインから、キャパシティタスクを選択します。
3. [キャパシティタスク] ページで、[キャパシティタスクを作成] を選択します。
4. 開始方法ページで、設定する順序、Outpost、またはアセットを選択します。
5. 容量を変更するには、変更方法のオプションを指定します。コンソールで手順を指定するか、JSON ファイルをアップロードします。
   - コンソールのステップを使用するようにキャパシティ設定プランを変更する
   - 容量設定プランをアップロードして JSON ファイルをアップロードする

> **Note**
>
> - キャパシティ管理が特定のインスタンスを停止を推奨しないようにするには、停止すべきではないインスタンスを指定します。これらのインスタンスは、停止するインスタンスのリストから除外されます。

Console steps

1. インスタンスビューまたはラックビューを選択します。
2. 1 つのアセットで Outpost 容量設定の変更または変更を選択します。
3. 現在の選択と異なる場合は、Outpost またはアセットを選択します。
4. このキャパシティタスクをすぐに実行するか、48 時間以上定期的に実行するかを選択します。
5. [次へ] を選択します。
6. [インスタンスキャパシティを設定] ページで、各インスタンスタイプには、事前に選択された最大数を含む 1 つのインスタンスサイズが表示されます。インスタンスサイズを追加するには、[インスタンスサイズを追加] を選択します。
7. インスタンスの数量を指定し、そのインスタンスサイズに表示されるキャパシティを書き留めます。
8. 各インスタンスタイプのセクションの最後に、キャパシティが超過しているか不足しているかを通知するメッセージが表示されます。インスタンスサイズまたは数量レベルで調整して、使用できる合計キャパシティを最適化します。
9. 特定のインスタンスサイズのインスタンス数を最適化 AWS Outposts するようにリクエストすることもできます。そのためには、次の操作を行います。

   a. [インスタンスサイズ] を選択します。

   b. 関連するインスタンスタイプのセクションの最後で、[オートバランス] を選択します。
10. インスタンスタイプごとに、少なくとも 1 つのインスタンスサイズに対してインスタンス数量が指定されていることを確認します。
11. 必要に応じて、インスタンスを選択してそのままにします。
12. [次へ] を選択します。
13. [確認して作成] ページで、リクエストする更新を確認します。
14. Create. AWS Outposts creates キャパシティタスクを選択します。

15. [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

Upload a JSON file

1. [キャパシティ構成をアップロード] を選択します。
2. [次へ] を選択します。
3. [キャパシティ構成計画をアップロード] ページで、インスタンスタイプ、サイズ、数量を指定する JSON ファイルをアップロードします。必要に応じて、JSON ファイルで InstancesToExclude パラメータと TaskActionOnBlockingInstances パラメータを指定できます。

   Example

   JSON ファイルの例:

   ```
   {
     "InstancePools": [
       {
         "InstanceType": "c5.24xlarge",
         "Count": 1
       },
       {
         "InstanceType": "m5.24xlarge",
         "Count": 2
       }
     ],
     "InstancesToExclude": {
       "AccountIds": [
         "111122223333"
       ],
       "Instances": [
         "i-1234567890abcdef0"
       ],
       "Services": [
         "ALB"
       ]
     },
     "TaskActionOnBlockingInstances": "WAIT_FOR_EVACUATION"
   }
   ```

4. [キャパシティ構成計画] セクションの JSON ファイルの内容を確認します。

5. [次へ] を選択します。
6. [確認して作成] ページで、リクエストする更新を確認します。
7. Create. AWS Outposts creates キャパシティタスクを選択します。
8. [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

# キャパシティタスクの問題のトラブルシューティング

次の既知の問題を確認して、キャパシティ管理に関連する問題を新しい順序で解決します。問題が表示されない場合は、 にお問い合わせください サポート。

## 注文 *oo-xxxxxx* が Outpost ID *op-xxxxx* に関連付けられていません

この問題は、 AWS CLI または API を使用して を実行し`StartCapacityTask`、リクエストの Outpost ID が Outpost ID の順序と一致しない場合に発生します。

この問題を解決するには。

1. にサインインします AWS。
2. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
3. ナビゲーションペインから、注文を選択します。
4. 注文を選択し、注文ステータスが `PREPARING`、、`IN_PROGRESS`または のいずれかであることを確認します`ACTIVE`。
5. Outpost ID を順番に書き留めます。
6. `StartCapacityTask` API リクエストに正しい Outpost ID を入力します。

## キャパシティプランには、サポートされていないインスタンスタイプが含まれます。

この問題は、 AWS CLI または API を使用してキャパシティタスクを作成または変更し、リクエストにサポートされていないインスタンスタイプが含まれている場合に発生します。

この問題を解決するには、 コンソールまたは CLI を使用します。

コンソールを使用する

1. にサインインします AWS。

2. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
3. ナビゲーションペインから、キャパシティタスクを選択します。
4. キャパシティ設定のアップロードオプションを使用して、同じインスタンスタイプのリストを持つ JSON をアップロードします。
5. コンソールには、サポートされているインスタンスタイプのリストを含むエラーメッセージが表示されます。
6. リクエストを修正して、サポートされていないインスタンスタイプを削除します。
7. 修正された JSON を使用してコンソールでキャパシティタスクを作成または変更するか、この修正されたインスタンスタイプのリストで CLI または API を使用します。

CLI を使用する

1. GetOutpostSupportedInstanceTypes コマンドを使用して、サポートされているインスタンスタイプのリストを表示します。
2. インスタンスタイプの正しいリストを使用して、キャパシティタスクを作成または変更します。

## Outpost ID *op-xxxxx* を持つ Outpost がない

この問題は、 AWS CLI または API を使用して を実行しStartCapacityTask、リクエストに次のいずれかの理由で無効な Outpost ID が含まれている場合に発生します。

- Outpost は別の AWS リージョンにあります。
- この Outpost へのアクセス許可がありません。
- Outpost ID が正しくありません。

この問題を解決するには。

1. `StartCapacityTask` API リクエストで使用した AWS リージョンを書き留めます。
2. `ListOutposts` API アクションを使用して、 AWS リージョンで所有している Outposts のリストを取得します。
3. Outpost ID が一覧表示されているかどうかを確認します。
4. `StartCapacityTask` リクエストに正しい Outpost ID を入力します。
5. Outpost ID が見つからない場合は、 `ListOutposts` API アクションを再度使用して、Outpost が別の AWS リージョンに存在するかどうかを確認します。

# Outpost op-*XXXX* のアクティブ CapacityTask cap-*XXXX* が既に見つかりました

この問題は、 AWS Outposts コンソールまたは API を使用して Outpost で StartCapacityTask を実行し、Outpost のキャパシティタスクがすでに実行されている場合に発生します。キャパシティタスクのステータスが REQUESTED、、、または のいずれかである場合IN_PROGRESSWAITING_FOR_EVACUATION、キャパシティタスクは実行中と見なされますCANCELLATION_IN_PROGRESS。

この問題を解決するには、 AWS Outposts コンソールまたは CLI を使用します。

コンソールを使用する

1. にサインインします AWS。
2. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
3. ナビゲーションペインから、キャパシティタスクを選択します。
4. OutpostId に対して実行中のキャパシティタスクがないことを確認します。
5. OutpostId の実行中のキャパシティタスクがある場合は、タスクが終了するのを待つか、必要に応じてキャンセルします。
6. リクエストされた OutpostId に対して実行中のキャパシティタスクがない場合は、リクエストを再試行してキャパシティタスクを作成します。

CLI を使用する

1. ListCapacityTasks コマンドを使用して、Outpost の実行中のキャパシティタスクを検索します。
2. 実行中のすべてのキャパシティタスクが終了するのを待つか、必要に応じてキャンセルします。
3. リクエストされた OutpostId に対して実行中のキャパシティタスクがない場合は、リクエストを再試行してキャパシティタスクを作成します。

# Outpost op-*XXXX* のアセット *XXXX* に Active CapacityTask cap-XXXX が既に見つかりました

この問題は、 AWS Outposts コンソールまたは API を使用してアセットで StartCapacityTask を実行し、アセットに対して既に実行中のキャパシティタスクがある場合に発生しま

す。キャパシティタスクのステータスが REQUESTED、、、または のいずれかである場合IN_PROGRESSWAITING_FOR_EVACUATION、キャパシティタスクは実行中と見なされますCANCELLATION_IN_PROGRESS。

この問題を解決するには、 AWS Outposts コンソールまたは CLI を使用します。

コンソールを使用する

1. にサインインします AWS。
2. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
3. ナビゲーションペインから、キャパシティタスクを選択します。
4. OutpostId に対して実行中のキャパシティタスクがなく、AssetId に対して実行中のアセットレベルのキャパシティタスクがないことを確認します。
5. 実行中のキャパシティタスクがある場合は、タスクが終了するのを待つか、必要に応じてキャンセルします。
6. 実行中のキャパシティタスクがない場合は、リクエストを再試行してキャパシティタスクを作成します。

CLI を使用する

1. ListCapacityTasks コマンドを使用して、OutpostID と AssetID の実行中のキャパシティタスクを検索します。
2. OutpostId に対して実行中の Outpost レベルのキャパシティタスクがなく、AssetId に対して実行中のアセットレベルのキャパシティタスクがないことを確認します。
3. 実行中のキャパシティタスクがある場合は、タスクが終了するのを待つか、必要に応じてキャンセルします。
4. リクエストを再試行してキャパシティタスクを作成します。

## AssetId=*XXXX* は Outpost=op-*XXXX* には無効です

この問題は、 AWS Outposts コンソールまたは API を使用してアセットで StartCapacityTask を実行し、AssetID が次のいずれかの理由で有効でない場合に発生します。

- アセットは Outpost に関連付けられていません。
- アセットは分離されています。

この問題を解決するには、 AWS Outposts コンソールまたは CLI を使用します。

コンソールを使用する

1. にサインインします AWS。
2. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
3. Outpost の ラックビューを選択します。
4. リクエストされた AssetId が Outpost に関連付けられていること、および隔離されたホストとしてマークされていないことを確認します。

    a. アセットが分離されている場合、キャパシティタスクが実行されていることが原因である可能性があります。キャパシティタスクパネルに移動し、OutpostId と AssetId に対して実行中の Outpost タスクまたはAssetIdレベルのタスクがあるかどうかを確認できます。存在する場合は、タスクが終了し、アセットが再び使用可能になるまで待ちます。

    b. 分離されたアセットに対して実行中のキャパシティタスクがない場合、アセットが劣化する可能性があります。
5. アセットが存在し、有効な状態であることを確認したら、リクエストを再試行してキャパシティタスクを作成します。

CLI を使用する

1. ListAssets コマンドを使用して、OutpostID に関連付けられたアセットを検索します。
2. リクエストされた AssetId が Outpost に関連付けられており、その状態が であることを確認しますACTIVE。

    a. アセットの状態が ACTIVE でない場合、キャパシティタスクが実行されていることが原因である可能性があります。ListCapacityTasks コマンドを使用して、OutpostId と AssetId に対して Outpost またはアセットレベルのタスクが実行されているかどうかを確認します。AssetId 存在する場合は、タスクが終了し、アセットが再びアクティブになるまで待ちます。

    b. 分離されたアセットに対して実行中のキャパシティタスクがない場合、アセットが劣化する可能性があります。
3. アセットが存在し、有効な状態であることを確認したら、リクエストを再試行してキャパシティタスクを作成します。

# AWS Outposts リソースを共有する

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 AWS 組織内の他の AWS アカウントと共有できます。Outpost 所有者は、Outpost リソースを一元的に作成および管理し、 AWS 組織内の複数の AWS アカウント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。

このモデルでは、Outpost リソースを所有する AWS アカウント (所有者) は、同じ組織内の他の AWS アカウント (コンシューマー) とリソースを共有します。コンシューマーは、各自のアカウントで作成した Outposts にリソースを作成する場合と同じように、共有された Outposts にリソースを作成できます。所有者は、Outpost およびそこに作成したリソースの管理に責任を負います。所有者は、いつでも共有アクセスを変更または取り消すことができます。キャパシティ予約を使用するインスタンスを除き、所有者は、コンシューマーが共有の Outposts 上に作成したリソースを表示、変更、および削除できます。所有者は、共有したキャパシティ予約でコンシューマーが起動したインスタンスを変更することはできません。

コンシューマーは、キャパシティ予約を消費するあらゆるリソースを含めた、Outpost 上に作成、共有されるリソースを管理する責任があります。コンシューマーは、他のコンシューマーまたは Outpost 所有者が所有するリソースを表示または変更することはできません。また、共有された Outposts を変更することもできません。

Outpost の所有者は、Outpost のリソースを以下の相手と共有できます。

- の組織内の特定の AWS アカウント AWS Organizations。
- AWS Organizationsの組織内の組織単位
- AWS Organizationsの組織全体。

内容

# 共有可能な Outpost リソース

Outpost の所有者は、このセクションに記載されている Outpost リソースをコンシューマーと共有できます。

これらは Outposts ラックで利用できるリソースです。

- 専有ホストの割り当て — このリソースにアクセスできるコンシューマーは、以下のことができます。
  - 専用ホスト で EC2 インスタンスを起動して実行します。
- キャパシティ予約 — このリソースにアクセスできるコンシューマーは、以下のことができます。
  - 共有されているキャパシティ予約を特定します。
  - キャパシティ予約を使用するインスタンスを起動して管理します。
- カスタマー所有 IP アドレス (CoIP) プール — このリソースにアクセスできるコンシューマーは、次のことができます。
  - カスタマー所有 IP アドレスをインスタンスに割り当てて関連付けます。
- ローカルゲートウェイルートテーブル — このリソースにアクセスできるコンシューマーは、次のことができます。
  - ローカルゲートウェイへの VPC 関連付けを作成して管理します。
  - ローカルゲートウェイルートテーブルと仮想インターフェイスの設定を表示します。
  - ターゲットがローカルゲートウェイである VPC サブネットルートを作成します。
- Outposts — このリソースにアクセスできるコンシューマーは、次のことができます。
  - Outpost にサブネットを作成して管理します。
  - Outpost で EBS ボリュームを作成および管理します。
  - AWS Outposts API を使用して、Outpost に関する情報を表示します。
- Outposts 上の S3 — このリソースにアクセスできるコンシューマーは、次のことができます。
  - Outpost で S3 バケット、アクセスポイント、エンドポイントを作成および管理します。
- サイト — このリソースにアクセスできるコンシューマーは、次のことができます。

  - サイト内で Outpost を作成、管理、制御できます。
- サブネット — このリソースにアクセスできるコンシューマーは、次のことができます。
  - サブネットに関する情報を表示します。
  - サブネットで EC2 インスタンスを起動して実行します。

  Amazon VPC コンソールを使用して Outpost サブネットを共有します。詳細については、「Amazon VPC ユーザーガイド」の「サブネットの共有」を参照してください。

## Outposts リソースを共有するための前提条件

- 組織、または AWS Organizations内の組織単位と Outpost リソースを共有するには、 AWS Organizationsとの共有を有効にする必要があります 詳細については、「AWS RAM ユーザーガイド」の「AWS Organizationsで共有を有効化する」を参照してください。
- Outpost リソースを共有するには、 AWS アカウントでそのリソースを所有している必要があります。自身が共有を受けている Outpost リソースを共有することはできません。
- Outpost リソースを共有するには、組織内のアカウントと共有する必要があります。

## 関連サービス

Outpost リソース共有は AWS Resource Access Manager () と統合されていますAWS RAM。 AWS RAM は、任意の AWS アカウントまたは を通じて AWS リソースを共有できるサービスです AWS Organizations。 AWS RAMを使用した リソース共有。これにより、自身が所有するリソースを共有できます。リソース共有は、共有するリソースと、それらを共有するコンシューマーを指定します。コンシューマーは、個々の AWS アカウント、組織単位、または の組織全体にすることができます AWS Organizations。

詳細については AWS RAM、AWS RAM 「 ユーザーガイド」を参照してください。

## アベイラビリティーゾーン間での共有

リソースがリージョンの複数のアベイラビリティーゾーンに分散されるようにするために、アベイラビリティーゾーンは各 アカウントの名前に個別にマッピングされます。このため、アカウントが異なると、アベイラビリティーゾーンの命名方法が異なる場合があります。たとえば、us-east-1a AWS アカウントのアベイラビリティーゾーンがus-east-1a別の AWS アカウントと同じ場所ではない場合があります。

アカウントに関連する Outpost リソースの場所を特定するには、アベイラビリティーゾーン ID (AZ ID) を使用する必要があります。AZ ID は、すべての AWS アカウントにわたるアベイラビリティーゾーンの一意で一貫した識別子です。たとえば、 `use1-az1`は`us-east-1`リージョンの AZ ID であり、すべての AWS アカウントで同じ場所です。

アカウントのアベイラビリティーゾーンIDs を表示するには

1. AWS RAM コンソールで AWS RAM コンソールに移動します。
2. 現在のリージョンの AZ ID は、画面の右側にある [お客様の AZ ID] パネルに表示されます。

> **Note**
>
> ローカルゲートウェイルートテーブルは Outpost と同じ AZ にあるため、ルートテーブルに AZ ID を指定する必要はありません。

# Outpost リソースの共有

所有者が Outpost をコンシューマと共有すると、コンシューマは自分のアカウントで作成した Outpost にリソースを作成する場合と同じように、その Outpost にリソースを作成できます。共有ローカルゲートウェイルートテーブルにアクセスできるコンシューマーは、VPC 関連付けを作成および管理できます。詳細については、「共有可能な Outpost リソース」を参照してください。

Outpost リソースを共有するには、リソース共有に追加する必要があります。リソース共有は、AWS アカウント間で AWS RAM リソースを共有できる リソースです。リソース共有では、共有対象のリソースと、共有先のコンシューマーを指定します。 AWS Outposts コンソールを使用して Outpost リソースを共有する場合は、既存のリソース共有に追加します。Outposts リソースを新しいリソース共有に追加するには、まず AWS RAM コンソールを使用してリソース共有を作成する必要があります。

の組織に属 AWS Organizations していて、組織内での共有が有効になっている場合は、 AWS RAM コンソールから共有 Outpost リソースへのアクセスを組織内のコンシューマーに許可できます。これに該当しない場合、コンシューマーはリソースへの参加の招待を受け取り、その招待を受け入れた後で、共有 Outposts に対するアクセス許可が付与されます。

AWS Outposts コンソール、 AWS RAM コンソール、または を使用して、所有している Outpost リソースを共有できます AWS CLI。

AWS Outposts コンソールを使用して所有している Outpost を共有するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで [Outposts] を選択します。
3. Outpost を選択し、[アクション]、[詳細の表示] の順に選択します。
4. [Outpost の概要] ページで [リソース共有] を選択します。
5. [リソースの共有の作成] を選択します。

AWS RAM コンソールにリダイレクトされ、次の手順を使用して Outpost の共有を完了します。所有しているローカルゲートウェイルートテーブルを共有するには、以下の手順も実行してください。

AWS RAM コンソールを使用して所有する Outpost またはローカル ゲートウェイルートテーブルを共有するには

「AWS RAM ユーザーガイド 」の「リソース共有の作成」を参照してください。

を使用して、所有している Outpost またはローカルゲートウェイルートテーブルを共有するには AWS CLI

create-resource-share コマンドを使用します。

# 共有 Outpost リソースの共有解除

Outpost とコンシューマーとの共有を解除すると、コンシューマーは以下を実行できなくなります。

- AWS Outposts コンソールで Outpost を表示します。
- Outpost に新規のサブネットを作成する。
- Outpost で新規の Amazon EBS ボリュームを作成および管理する。
- AWS Outposts コンソールまたは を使用して、Outpost の詳細とインスタンスタイプを表示します AWS CLI。

共有期間中にコンシューマーが作成したサブネット、ボリューム、またはインスタンスは削除されず、コンシューマーは引き続き以下を実行できます。

- これらのリソースにアクセスして変更する。
- コンシューマーが作成した既存のサブネットで新規のインスタンスを起動する。

コンシューマーが自分のリソースにアクセスし、Outpost で新規のインスタンスを起動しないようにするには、コンシューマーにリソースを削除するようにリクエストします。

共有ローカルゲートウェイルートテーブルが共有解除されると、コンシューマーはそのテーブルへの新しい VPC の関連付けを作成できなくなります。コンシューマーが作成した既存の VPC の関連付けは、引き続きルートテーブルに関連付けられます。これらの VPC 内のリソースは、引き続きトラフィックをローカルゲートウェイにルーティングできます。関連付けされないようにするは、コンシューマーに VPC の関連付けの削除をリクエストします。

所有する共有 Outposts リソースの共有を解除するには、リソース共有から削除する必要があります。これを行うには、 AWS RAM コンソールまたは を使用します AWS CLI。

AWS RAM コンソールを使用して、所有している共有 Outpost リソースの共有を解除するには

「AWS RAM ユーザーガイド」の「リソース共有の更新」を参照してください。

を使用して、所有している共有 Outpost リソースの共有を解除するには AWS CLI

disassociate-resource-share コマンドを使用します。

# 共有 Outpost リソースの特定

所有者とコンシューマーは、 AWS Outposts コンソールと を使用して共有 Outposts を識別できます AWS CLI。 AWS CLIを使用して共有ローカルゲートウェイルートテーブルを特定できます。

AWS Outposts コンソールを使用して共有 Outpost を識別するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで [Outposts] を選択します。
3. Outpost を選択し、[アクション]、[詳細の表示] の順に選択します。
4. Outpost の概要ページで、所有者 ID を表示して Outpost 所有者の AWS アカウント ID を特定します。

を使用して共有 Outpost リソースを識別するには AWS CLI

list-outposts コマンドと describe-local-gateway-route-tables コマンドを使用してください。これらのコマンドは、所有している Outpost リソースと共有されている Outpost リソースを返します。は、Outpost リソース所有者の AWS アカウント ID `OwnerId`を示します。

# 共有 Outpost リソースの権限

## 所有者のアクセス許可

所有者は、Outpost およびそこに作成したリソースの管理に責任を負います。所有者は、いつでも共有アクセスを変更または取り消すことができます。を使用して、コンシューマーが共有 Outposts で作成するリソース AWS Organizations を表示、変更、削除できます。

## コンシューマーのアクセス許可

コンシューマーは、各自のアカウントで作成した Outposts にリソースを作成する場合と同じように、共有された Outposts にリソースを作成できます。コンシューマーは、Outposts 上に作成された自身が共有しているリソースの管理に責任を負います。コンシューマーは、他のコンシューマーまたは Outpost 所有者が所有するリソースを表示または変更することはできません。また、自己が共有している Outpost を変更することはできません。

# 請求と使用量測定

所有者は、共有する Outpost および Outpost リソースに対して課金されます。また、 AWS リージョンからの Outpost のサービスリンク VPN トラフィックに関連するデータ転送料金も請求されます。

ローカルゲートウェイルートテーブルの共有に追加料金はかかりません。共有サブネットの場合、VPC 所有者は、 Direct Connect や VPN 接続、NAT ゲートウェイ、プライベートリンク接続などの VPC レベルのリソースに対して課金されます。

コンシューマーには、ロードバランサーや Amazon RDS データベースなど、共有 Outposts で作成したアプリケーションリソースの料金が請求されます。コンシューマーには、 AWS リージョンからの有料データ転送に対しても課金されます。

# 制限

AWS Outposts 共有の使用には、次の制限が適用されます。

- 共有サブネットの制限は、 AWS Outposts 共有の使用に適用されます。VPC 共有の制限事項についての詳細は、「Amazon Virtual Private Cloud ユーザーガイド」の「制限事項」を参照してください。
- サービスクォータはアカウントごとに適用されます。

# Outposts ラック上のサードパーティーブロックストレージ

Outposts ラックを使用すると、サードパーティーのストレージ配列に保存されている既存のデータを活用できます。Outposts の EC2 インスタンスの外部ブロックデータボリュームと外部ブロックブートボリュームを指定できます。この統合を使用すると、Dell PowerStore、HPE Alletra Storage MP B10000、NetApp オンプレミスエンタープライズストレージアレイ、Pure Storage FlashArray ストレージシステムなどのサードパーティーベンダーによってバックアップされた外部ブロックデータとブートボリュームを使用できます。

考慮事項

- Outposts ラックと Outposts 2U サーバーで使用できます。Outposts 1U サーバーでは使用できません。
- 第 1 世代 Outposts ラックがサポートされているすべての AWS リージョンで使用できます。
- 追加料金なしで利用できます。
- ストレージ配列の設定とday-to-day管理はお客様の責任となります。また、ストレージ配列で外部ブロックボリュームを作成および管理します。ストレージアレイのハードウェア、ソフトウェア、または接続に問題がある場合は、サードパーティーのストレージベンダーにお問い合わせください。

> **Note**
>
> 外部ストレージ配列に保存されているブロックボリュームには、Outposts の EC2 インスタンスに起動されるオペレーティングシステムが含まれています。外部ストレージ配列にバックアップされた AMI の起動はサポートされていません。AMI を起動するには、Outposts ラックに EBS またはインスタンスストレージが必要です。

## 外部ブロックデータボリューム

互換性のあるサードパーティーストレージシステムにバックアップされたブロックデータボリュームをプロビジョニングして設定したら、起動時にボリュームを EC2 インスタンスにアタッチできます。ストレージ配列でマルチアタッチ用にボリュームを設定すると、ボリュームを複数の EC2 インスタンスにアタッチできます。

主要なステップ

- AWS 技術者は、Outpost サブネットとローカルネットワーク間の接続を確保するためにローカルゲートウェイを設定します。
- 外部ストレージ配列の管理インターフェイスを使用してボリュームを作成します。次に、新しいイニシエーターグループを作成し、ターゲット EC2 インスタンスの iSCSI 修飾名 (IQN) をこのグループに追加して、イニシエータマッピングを設定します。これにより、外部ブロックデータボリュームが EC2 インスタンスに関連付けられます。
- インスタンスを起動するときに、外部データボリュームを追加します。外部ストレージ配列のイニシエーター IQN、ターゲット IP アドレス、ポート、IQN が必要です。詳細については、「Outpost でインスタンスを起動する」を参照してください。

詳細については、「 を使用したサードパーティーのブロックストレージの使用の簡素化 AWS Outposts」を参照してください。

# 外部ブロックブートボリューム

外部ストレージアレイから Outposts で EC2 インスタンスを起動すると、サードパーティーのストレージに依存するオンプレミスワークロードに対して、一元化され、費用対効果が高く、効率的なソリューションが提供されます。以下のオプションから選択できます。

iSCSI SAN ブート

外部ストレージ配列から直接起動します。 AWSが提供する iPXE ヘルパー AMI を使用して、インスタンスをネットワークの場所から起動できるようにします。iPXE を iSCSI と組み合わせると、EC2 インスタンスはリモート iSCSI ターゲット (ストレージ配列) をローカルディスクとして扱います。オペレーティングシステムからのすべての読み取りおよび書き込みオペレーションは、外部ストレージ配列で実行されます。

iSCSI または NVMe-over-TCP LocalBoot

ストレージ配列から取得したブートボリュームのコピーを使用して EC2 インスタンスを起動します。元のソースイメージは変更されません。LocalBoot AMI を使用してヘルパーインスタンスを起動します。このヘルパーインスタンスは、起動ボリュームをストレージ配列から EC2 インスタンスのインスタンスストアにコピーし、iSCSI イニシエータまたは NVMe-over-TCP ホストとして機能します。最後に、EC2 インスタンスはローカルインスタンスストアボリュームを使用して再起動します。

インスタンスストアは一時ストレージであるため、EC2 インスタンスが終了するとブートボリュームは削除されます。したがって、このオプションは、仮想デスクトップインフラストラクチャ (VDI) で使用されるなど、読み取り専用のブートボリュームに適しています。

NVMe-over-TCP LocalBoot を使用して EC2 Windows インスタンスを起動することはできません。これは EC2 Linux インスタンスを使用してのみサポートされます。

詳細については、「 で使用する外部ブートボリュームのデプロイ AWS Outposts」を参照してください。

# のセキュリティ AWS Outposts

のセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルではこれをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。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コンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。が適用されるコンプライアンスプログラムの詳細については AWS Outposts、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

のセキュリティとコンプライアンスの詳細については AWS Outposts、AWS Outposts 「 ラックに関するよくある質問」を参照してください。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Outposts。ここでは、セキュリティとコンプライアンスの目標を満たす方法を説明します。また、リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

内容

# でのデータ保護 AWS Outposts

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Outposts。このモデルで説明されているように、 AWS はすべての 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 AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。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 アカウント 認証情報を保護し、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。

データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿されたAWS 責任共有モデルおよび GDPR ブログを参照してください。

## 保管中の暗号化

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、リムーバブル デバイスである Nitro Security Key (NSK) に保存される外部キーにラップされます。NSK は Outposts 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 暗号化は AWS Key Management Service (AWS KMS) と KMS キーを使用します。詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。

## 転送中の暗号化

AWS は、Outpost とその AWS リージョン間の転送中のデータを暗号化します。詳細については、「サービスリンク経由の接続」を参照してください。

Transport Layer Security (TLS) などの暗号化プロトコルを使用して、ローカルゲートウェイを介してローカルネットワークに送信される転送中の機密データを暗号化できます。

## データの削除

EC2 インスタンスを停止または終了すると、そのインスタンスに割り当てられていたメモリをハイパーバイザーがスクラブ (ゼロに設定) し、そのメモリが新たなインスタンスに割り当てられ、すべてのストレージブロックがリセットされます。

Nitro セキュリティ キーを破棄すると、Outpost 上のデータが暗号的に細断されます。

# AWS Outpostsの Identity and Access Management (IAM)

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するのに役立つ AWS サービスです。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。IAMは追加料金なしでご利用いただけます。

内容



## AWS Outposts と IAM の連携方法

IAM を使用して AWS Outposts へのアクセスを管理する前に、Outposts で使用できる IAM AWS 機能を確認してください。

| IAM の特徴量 | 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 | なし |
| 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 |
| ACL | なし |
| ABAC (ポリシー内のタグ) | あり |
| 一時的な認証情報 | あり |

| IAM の特徴量 | 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 | あり |

## AWS Outposts のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

AWS Outposts のアイデンティティベースのポリシーの例

AWS Outposts のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Outposts ポリシーの例。

## AWS Outposts のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

AWS Outposts アクションのリストを確認するには、「サービス認可リファレンス」の「 で定義されるアクション AWS Outposts」を参照してください。

AWS Outposts のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
outposts
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
    "outposts:action1",
    "outposts:action2"
]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、List という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "outposts:List*"
```

## AWS Outposts のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

一部の AWS Outposts API アクションは、複数のリソースをサポートしています。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [
    "resource1",
    "resource2"
```

```
]
```

AWS Outposts リソースタイプとその ARNs「 で定義されるリソースタイプ AWS Outposts」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「AWS Outposts で定義されるアクション」を参照してください。

## AWS Outposts のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Condition` 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS 「グローバル条件コンテキストキー」を参照してください。

AWS Outposts 条件キーのリストを確認するには、「サービス認可リファレンス」の「 の条件キー AWS Outposts」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS Outposts」を参照してください。

AWS Outposts のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Outposts ポリシーの例。

## AWS Outposts での ABAC

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

### AWS Outposts での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールの使用時に自動的に作成されます。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

### AWS Outposts のクロスサービスプリンシパルアクセス許可

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

### AWS Outposts のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

AWS Outposts サービスにリンクされたロールの作成または管理の詳細については、「」を参照してくださいのサービスにリンクされたロール AWS Outposts。

## AWS Outposts ポリシーの例

デフォルトでは、ユーザーとロールには AWS Outposts リソースを作成または変更するアクセス許可はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など、 AWS Outposts で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」の「 のアクション、リソース、および条件キー AWS Outposts」を参照してください。 ARNs

内容

- ポリシーに関するベストプラクティス
- 例: リソースレベルのアクセス許可の使用

## ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが AWS Outposts リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。

- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

## 例: リソースレベルのアクセス許可の使用

以下の例では、リソースレベルの権限を使用して、指定した Outpost に関する情報を取得する権限を付与しています。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "outposts:GetOutpost",
            "Resource": "arn:aws:outposts:us-east-1:111122223333:outpost/
op-1234567890abcdef0"
        }
    ]
}
```

以下の例では、リソースレベルの権限を使用して、指定されたサイトに関する情報を取得する権限を付与しています。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "outposts:GetSite",
            "Resource": "arn:aws:outposts:us-east-1:111122223333:site/
os-0abcdef1234567890"
        }
    ]
}
```

## のサービスにリンクされたロール AWS Outposts

AWS Outposts は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、 に直接リンクされたサービスロールの一種です AWS Outposts。 は、サービスにリンクされたロール AWS Outposts を定義し、ユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可を含みます。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 の設定 AWS Outposts がより効率的になります。 は、サービスにリンクされたロールのアクセス許可 AWS Outposts を定義し、特に定義されている場合を除き、 のみがその ロールを引き受け AWS Outposts ることができます。定義された許可には信頼ポリシーと許可ポリシーが含まれ、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールは、関連する リソースを削除した後でしか削除できません。これにより、AWS Outposts リソースへのアクセス許可が誤って削除されないため、リソースが保護されます。

### のサービスにリンクされたロールのアクセス許可 AWS Outposts

AWS Outposts は、AWSServiceRoleForOutposts_*OutpostID* という名前のサービスにリンクされたロールを使用します。このロールは、ユーザーに代わってプライベート接続を有効にするネットワークリソースを管理するアクセス許可を Outposts に付与します。このロールにより、Outposts はネットワークインターフェイスの作成と設定、セキュリティグループの管理、サービスリンクエンドポイントインスタンスへのインターフェイスのアタッチを行うこともできます。これらのアクセス許可は、オンプレミスの Outpost と AWS サービス間の安全なプライベート接続を確立して維持し、Outpost デプロイの信頼性の高いオペレーションを確保するために必要です。

AWSServiceRoleForOutposts_*OutpostID* サービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `outposts.amazonaws.com`

### サービスにリンクされたロールポリシー

AWSServiceRoleForOutposts_*OutpostID* サービスにリンクされたロールには、次のポリシーが含まれます。

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

### AWSOutpostsServiceRolePolicy

このAWSOutpostsServiceRolePolicyポリシーは、 によって管理される AWS リソースへのアクセスを有効にします AWS Outposts。

このポリシーにより AWS Outposts 、 は指定されたリソースに対して次のアクションを実行できます。

- アクション: すべての AWS リソースec2:DescribeNetworkInterfacesで
- アクション: すべての AWS リソースec2:DescribeSecurityGroupsで
- アクション: すべての AWS リソースec2:DescribeSubnetsで
- アクション: すべての AWS リソースec2:DescribeVpcEndpointsで
- アクション: 次の AWS リソースec2:CreateNetworkInterfaceで:

```
"arn:*:ec2:*:*:vpc/*",
"arn:*:ec2:*:*:subnet/*",
"arn:*:ec2:*:*:security-group/*"
```

- アクション: 次の条件"arn:*:ec2:*:*:network-interface/*"に一致する AWS リソースec2:CreateNetworkInterface。

```
"ForAnyValue:StringEquals" : { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

- アクション: 次の AWS リソースec2:CreateSecurityGroupで:

```
"arn:*:ec2:*:*:vpc/*"
```

- アクション: 次の条件"arn:*:ec2:*:*:security-group/*"に一致する AWS リソースec2:CreateSecurityGroup。

```
"ForAnyValue:StringEquals": { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

### AWSOutpostsPrivateConnectivityPolicy_OutpostID

このAWSOutpostsPrivateConnectivityPolicy_*OutpostID*ポリシーにより AWS Outposts 、は指定されたリソースに対して次のアクションを実行できます。

- アクション: 次の条件に一致するすべての AWS リソースec2:AuthorizeSecurityGroupIngress。

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- アクション: 次の条件に一致するすべての AWS リソースec2:AuthorizeSecurityGroupEgress。

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- アクション: 次の条件に一致するすべての AWS リソースec2:CreateNetworkInterfacePermission。

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- アクション: 次の条件に一致するすべての AWS リソースec2:CreateTags。

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}},
"StringEquals": {"ec2:CreateAction" : ["CreateSecurityGroup",
 "CreateNetworkInterface"]}
```

- アクション: 次の条件に一致するすべての AWS リソースec2:RevokeSecurityGroupIngress。

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- アクション: 次の条件に一致するすべての AWS リソースec2:RevokeSecurityGroupEgress。

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- アクション: 次の条件に一致するすべての AWS リソースec2:DeleteNetworkInterface。

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- アクション: 次の条件に一致するすべての AWS リソースec2:DeleteSecurityGroup。

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細についてはIAM ユーザーガイド の「サービスにリンクされた役割のアクセス許可」を参照してください。

## のサービスにリンクされたロールを作成する AWS Outposts

サービスリンクロールを手動で作成する必要はありません。で Outpost のプライベート接続を設定すると AWS マネジメントコンソール、 によってサービスにリンクされたロールが自動的に AWS Outposts 作成されます。

詳細については、「サービスリンクのプライベート接続オプション」を参照してください。

## のサービスにリンクされたロールを編集する AWS Outposts

AWS Outposts では、AWSServiceRoleForOutposts_*OutpostID* サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの更新」を参照してください。

## のサービスにリンクされたロールを削除する AWS Outposts

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

リソースを削除しようとしたときに AWS Outposts サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForOutposts_*OutpostID* サービスにリンクされたロールを削除する前に、Outpost を削除する必要があります。

開始する前に、Outpost が AWS Resource Access Manager () を使用して共有されていないことを確認してくださいAWS RAM。詳細については、「共有 Outpost リソースの共有解除」を参照してください。

AWSServiceRoleForOutposts_***OutpostID*** で使用される AWS Outposts リソースを削除するには

Outpost を削除するには、 AWS エンタープライズサポートにお問い合わせください。

サービスリンクロールを IAM で手動削除するには

詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

## AWS Outposts サービスにリンクされたロールでサポートされているリージョン

AWS Outposts は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートしています。詳細については、FAQshttps://aws.amazon.com/outposts/rack/faqs/」を参照してください。

# AWS AWS Outposts の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS 管理ポリシーを更新する可能性が高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

## AWS マネージドポリシー: AWSOutpostsServiceRolePolicy

このポリシーは、 AWS Outposts がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロールにアタッチされます。詳細については、「サービスリンクロール」を参照してください。

## AWS AWS 管理ポリシーに対する Outposts の更新

このサービスがこれらの変更の追跡を開始した以降の AWS Outposts の AWS マネージドポリシーの更新に関する詳細を表示します。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| AWS Identity and Access Management サービスにリンクされたロール AWSServiceRoleForOutposts_*OutpostID* の更新 | AWSServiceRoleForOutposts_*OutpostID* サービスにリンクされたロールのアクセス許可が更新され、 がプライベート接続のネットワークリソース AWS Outposts を管理する方法を絞り込み、サービスリンクエンドポイントインスタンスに必要なネットワークインターフェイスとセキュリティグループのオペレーションをより正確に制御できるようになりました。 | 2025 年 4 月 18 日 |
| AWS Outposts が変更の追跡を開始しました | AWS Outposts は AWS 、管理ポリシーの変更の追跡を開始しました。 | 2019 年 12 月 3 日 |

# のインフラストラクチャセキュリティ AWS Outposts

マネージドサービスである AWS Outposts は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」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のベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で AWS Outposts にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

Outpost で実行されている EC2 インスタンスと EBS ボリュームに提供されるインフラストラクチャセキュリティの詳細については、「Amazon EC2 のインフラストラクチャ セキュリティ」を参照してください。

VPC フローログは、 AWS リージョンと同じように機能します。これは、分析のために CloudWatch Logs、Amazon S3、または Amazon GuardDuty に公開できることを意味します。データはこれらのサービスに公開するためにリージョンに送り返される必要があるため、Outpost が切断状態にあるときは CloudWatch や他のサービスからデータを参照することはできません。

## AWS Outposts 機器の改ざんモニタリング

誰も機器を変更、変更、リバースエンジニア、改ざん AWS Outposts していないことを確認してください。 AWS Outposts 機器には、 AWS サービス条件への準拠を確保するための改ざんモニタリングが装備されている場合があります。

# の耐障害性 AWS Outposts

AWS Outposts は高可用性を実現するように設計されています。Outposts ラックは冗長な電源とネットワーキング機器を備えて設計されています。追加の耐障害性を確保するために、Outpost にはデュアルの電源源と冗長なネットワーク接続を提供することをお勧めします。

高可用性を実現するために、Outposts ラックには追加の組み込みおよび常時アクティブな容量を確保したり、。Outpost の容量構成は、本番環境での運用を想定しており、容量を確保する際には各インスタンスファミリーに対して N+1 のインスタンスをサポートします。推奨されるのは、 AWS 基盤となるホストに問題が発生した場合にリカバリーとフェイルオーバーを可能にするため、ミッションクリティカルなアプリケーションに十分な追加容量を割り当てることです。Amazon CloudWatch の容量可用性メトリクスを使用して、アプリケーションの健康状態を監視し、アラームを設定できます。CloudWatch アクションを作成して自動リカバリオプションを構成し、Outposts の容量利用状況を時間とともにモニターすることができます。

Outpost を作成するときは、 AWS リージョンからアベイラビリティーゾーンを選択します。このアベイラビリティーゾーンは、API コールへの応答、Outpost のモニタリング、および Outpost の更新などのコントロールプレーンの操作をサポートしています。アベイラビリティーゾーンが提供する弾力性を活用するために、それぞれが異なるアベイラビリティーゾーンに接続された複数の Outposts にアプリケーションをデプロイすることができます。これにより、アプリケーションの耐障害性をさらに高め、単一のアベイラビリティーゾーンへの依存を回避できます。リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

インスタンスが異なる Outposts ラックに配置されるようにするために、スプレッド戦略を使用した配置グループを利用できます。これにより、相関した障害を減少させるのに役立ちます。詳細については、「Outpost の配置グループ」を参照してください。

Amazon EC2 Auto Scaling を使用して Outposts でインスタンスを起動し、Application Load Balancer を作成して、インスタンス間でトラフィックを分散させることができます。詳細については、「AWS Outpostsでの Application Load Balancer の設定」を参照してください。

# のコンプライアンス検証 AWS Outposts

AWS のサービス が特定のコンプライアンスプログラムの範囲内であるかどうかを確認するには、「コンプライアンスAWS のサービス プログラムによる対象範囲内のコンプライアンス」を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS 「 セキュリティドキュメント」を参照してください。

# AWS Outposts ワークロードのインターネットアクセス

このセクションでは、 AWS Outposts ワークロードが次の方法でインターネットにアクセスする方法について説明します。

- 親 AWS リージョン経由
- ローカルデータセンターのネットワーク経由

## 親 AWS リージョン経由のインターネットアクセス

このオプションでは、Outposts のワークロードは、サービスリンクを介してインターネットにアクセスし、親 AWS リージョンのインターネットゲートウェイ (IGW) 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通信できます。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、 AWS リージョンで 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。

Outposts サブネットのルートテーブル設定については、「Local gateway route tables」を参照してください。

### 考慮事項

- このオプションは、次の場合に使用します。
  - AWS リージョン内の複数の AWS サービスでインターネットトラフィックを柔軟に保護する必要があります。
  - データセンターやコロケーション施設にインターネットの接続ポイントがない場合。
- このオプションでは、トラフィックは親 AWS リージョンを通過する必要があり、レイテンシーが発生します。
- AWS リージョンのデータ転送料金と同様に、親アベイラビリティーゾーンから Outpost へのデータ転送には料金が発生します。データ転送の詳細については、「Amazon EC2 オンデマンド料金」を参照してください。
- サービスリンク帯域幅の使用率が増加することになります。

次の図は、Outposts インスタンスのワークロードと、親 AWS リージョン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。

# 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、Outposts に存在するワークロードがローカルデータセンターを経由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のトラフィックは、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。ローカルデータセンターのネットワークのセキュリティレイヤーは、Outposts ワークロードのトラフィックを保護する役割があります。

Outposts サブネットのルートテーブル設定については、「Local gateway route tables」を参照してください。

## 考慮事項

- このオプションは、次の場合に使用します。
  - ワークロードには、インターネットサービスに短いレイテンシーでアクセスする必要がある。
  - データ転送 (DTO) 料金が発生しないように検討している。
  - コントロールプレーントラフィックのサービスリンク帯域幅を保持する必要がある。
- セキュリティレイヤーは、Outposts ワークロードのトラフィックを保護する役割があります。
- ダイレクト VPC ルーティング (DVR) を選択した場合は、Outposts CIDR がオンプレミス CIDR と競合しないようにする必要があります。
- デフォルトルート (0/0) がローカルゲートウェイ (LGW) を介して伝播する場合、インスタンスはサービスエンドポイントに到達できない可能性があります。代わりに、VPC エンドポイントを選択すると、目的のサービスに到達できます。

次の図は、Outposts インスタンスのワークロードと、ローカル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。

# Outposts ラックをモニタリングする

AWS Outposts は、モニタリングおよびログ記録機能を提供する以下のサービスと統合されます。

CloudWatch メトリクス

Amazon CloudWatch を使用して、Outposts ラックのデータポイントに関する統計情報を、メトリクスと呼ばれる時系列データの時間順のセットとして取得できます。これらのメトリクスを使用して、システムが正常に実行されていることを確認できます。詳細については、「Outposts ラック CloudWatch メトリクス」を参照してください。

CloudTrail ログ

を使用して AWS CloudTrail 、 AWS APIs。これらの呼び出しはログ ファイルとして Amazon S3 に保存できます。これらの CloudTrail ログを使用して、行われた呼び出し、呼び出し元のソース IP アドレス、呼び出し元、呼び出し時間などを判断できます。

CloudTrail ログには、API アクションの呼び出しに関する情報が含まれています AWS Outposts。これらには、Amazon EC2 や Amazon EBS などの Outpost 上のサービスからの API アクションの呼び出しに関する情報も含まれています。詳細については、「CloudTrail を使用して API 呼び出しを口グに記録する」を参照してください。

VPC フローログ

VPC フローログを使用して、Outpost間、および Outpost 内部で送受信されるトラフィックに関する詳細情報を取得できます。詳細については、「Amazon VPC ユーザーガイド」の「VPC フローログを使用した IP トラフィックのログ記録」を参照してください。

トラフィックのミラーリング

トラフィックのミラーリングを使用して、ネットワークのトラフィックを Outposts ラックから帯域外セキュリティおよびモニタリングアプライアンスにコピーして転送します。ミラーリングされたトラフィックは、コンテンツ検査、脅威の監視、またはトラブルシューティングに使用できます。詳細については、「What is Traffic Mirroring?」を参照してください。

AWS Health Dashboard

には、 AWS リソースの正常性の変化によって開始された情報と通知 Health Dashboard が表示されます。情報は 2 つの方法で表示されます。ダッシュボードには、最近のイベントおよび予定されているイベントがカテゴリ別に分類されて表示されます。詳細なイベントログには、過去 90 日間のすべてのイベントが表示されます。たとえば、サービスリンク上の接続の問題によりイベントが開始され、ダッシュボードとイベントログに表示され、イベントログに 90 日間

残ります。 AWS Health サービスの一部である はセットアップを Health Dashboard 必要とせず、アカウントで認証されたすべてのユーザーが表示できます。詳細については、「AWS Health Dashboardを使い始める」を参照してください。

# Outposts ラック CloudWatch メトリクス

AWS Outposts は、Outposts のデータポイントを Amazon CloudWatch に発行します。CloudWatch では、それらのデータポイントについての統計を、順序付けられた時系列データのセット (メトリクス と呼ばれる) として取得できます。メトリクスは監視対象の変数、データポイントは時間の経過と共に変わる変数の値と考えることができます。たとえば、指定した期間にわたって Outpost で利用可能なインスタンスの容量を監視できます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。たとえば、CloudWatch アラームを作成して ConnectedStatus メトリクスを監視できます。平均メトリクスが1未満の場合、CloudWatch は電子メールアドレスに通知を送信するなどのアクションを開始できます。その後、Outpost の運用に影響を与える可能性があるオンプレミスまたはアップリンクネットワークの問題を調査できます。一般的な問題には、ファイアウォールと NAT ルールに対する最近のオンプレミスネットワーク構成の変更、またはインターネット接続の問題が含まれます。ConnectedStatus 問題が発生した場合は、オンプレミスネットワーク内から AWS リージョンへの接続を確認し、問題が解決しない場合は サポートに問い合わせる AWS ことをお勧めします。

CloudWatch アラームの作成の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch アラームの使用」を参照してください。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

内容



# メトリクス

AWS/Outposts 名前空間には、次のカテゴリのメトリクスが含まれます。

内容

## インスタンスメトリクス

Amazon EC2 インスタンスでは、次のメトリクスを使用できます。

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| InstanceFamilyCapacityAvailability | InstanceFamily および OutpostId | 利用可能なインスタンス容量の割合。このメトリクスには、Outpost 上で構成された専有ホストの容量は含まれません。<br><br>単位: パーセント<br><br>最大解像度:5 分<br><br>統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |
| InstanceFamilyCapacityUtilization | Account、InstanceFamily 、および OutpostId | 使用中のインスタンス容量の割合。このメトリクスには、Outpost 上で構成された専有ホストの容量は含まれません。<br><br>単位: パーセント<br><br>最大解像度:5 分<br><br>統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| InstanceTypeCapacityAvailability | InstanceType および OutpostId | 利用可能なインスタンス容量の割合。このメトリクスには、Outpost 上で構成された専有ホストの容量は含まれません。<br><br>単位: パーセント<br><br>最大解像度:5 分<br><br>統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |
| InstanceTypeCapacityUtilization | Account、InstanceType 、および OutpostId | 使用中のインスタンス容量の割合。このメトリクスには、Outpost 上で構成された専有ホストの容量は含まれません。<br><br>単位: パーセント<br><br>最大解像度:5 分<br><br>統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| UsedInstanceType_Count | Account、InstanceType 、および OutpostId | 現在使用中のインスタンスタイプの数 (Amazon Relational Database Service (Amazon RDS) や Application Load Balancer などのマネージドサービスで使用されるインスタンスタイプを含む)。このメトリクスには、Outpost 上で構成された専有ホストの容量は含まれません。<br><br>単位: 個<br><br>最大解像度:5 分 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| AvailableInstanceType_Count | InstanceType および OutpostId | 使用可能なインスタンスタイプ。このメトリクスには AvailableReservedInstances の数が含まれます。<br><br>予約可能なインスタンスの数を確認するには、AvailableReservedInstances の数から AvailableInstanceType_Count の数を引きます。<br><br>`Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances`<br><br>このメトリクスには、Outpost 上で構成された専有ホストの容量は含まれません。<br><br>単位: 個<br><br>最大解像度:5 分 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| AvailableReservedInstances | InstanceType および OutpostId | キャパシティ予約を使用して予約したコンピューティングキャパシティで起動できるインスタンスの数。<br><br>このメトリクスには、Amazon EC2 リザーブドインスタンスは含まれません。<br><br>このメトリクスには、予約可能なインスタンスの数は含まれません。予約可能なインスタンスを確認するには、AvailableReservedInstances の数から AvailableInstanceType_Count の数を引きます。<br><br>`Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances`<br><br>単位: 個<br><br>最大解像度:5 分 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| UsedReservedInstances | InstanceType および OutpostId | キャパシティ予約を使用して予約したコンピューティングキャパシティで実行中のインスタンスの数。このメトリクスには、Amazon EC2 リザーブドインスタンスは含まれません。<br><br>単位: 個<br><br>最大解像度:5 分 |
| TotalReservedInstances | InstanceType および OutpostId | キャパシティ予約を使用して予約したコンピューティングキャパシティで実行中および起動できるインスタンスの数。このメトリクスには、Amazon EC2 リザーブドインスタンスは含まれません。<br><br>単位: 個<br><br>最大解像度:5 分 |

## Amazon EBS のメトリクス

EBS ボリュームタイプの容量では、次のメトリクスを使用できます。

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| EBSVolumeTypeCapacityUtilization | VolumeType および OutpostId | 使用されている EBS ボリュームタイプの容量の割合。<br><br>単位: パーセント<br><br>最大解像度:5 分 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| | | 統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |
| EBSVolumeTypeCapacityAvailability | VolumeType および OutpostId | 利用可能な EBS ボリュームタイプの容量の割合。<br><br>単位: パーセント<br><br>最大解像度:5 分<br><br>統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |
| EBSVolumeTypeCapacityUtilizationGB | VolumeType および OutpostId | EBS ボリュームタイプに使用されているギガバイト数。<br><br>単位:ギガバイト<br><br>最大解像度:5 分<br><br>統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |
| EBSVolumeTypeCapacityAvailabilityGB | VolumeType および OutpostId | EBS ボリュームタイプの利用可能な容量のギガバイト数。<br><br>単位:ギガバイト<br><br>最大解像度:5 分<br><br>統計: 最も有用な統計は Average および pNN.NN (パーセンタイル) です。 |

# 仮想インターフェイスメトリクス

仮想インターフェイス (VIF) では、次のメトリクスを使用できます。

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| VifBgpSessionState | ローカルゲートウェイ VIFs ディメンション: OutpostsID 、VirtualInterfaceGroupId 、VirtualInterfaceID 。<br><br>サービスリンク VIFsディメンション: OutpostsID 、VirtualInterfaceID 。 | 仮想インターフェイス (VIF) AWS Outposts の とオンプレミスデバイス間のボーダーゲートウェイプロトコル (BGP) セッション状態。<br><br>単位: 値が 1～6 の場合:<br><br>• 1 – アイドル。これは、Outposts ラックが開始イベントを待っている最初の状態です。<br>• 2 – 接続します。Outposts ラックは、TCP 接続が完了するまで待機しています。<br>• 3 – アクティブ。Outposts ラックは TCP 接続を開始しようとしています。<br>• 4 – OpenSent。ルーターは OPEN メッセージを送信し、見返りに OPEN メッセージを待っています。<br>• 5 – OpenConfirm。ルーターは OPEN メッセージを受信し、KEEPALIVE メッセージを待っています。<br>• 6 – 確立済み。BGP 接続は完全に確立されており、Outposts ラックとオンプレミスデバイスはルー |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| | | ティング情報を交換できます。<br><br>最大解像度: 5 分<br><br>統計: 最も有用な統計は Maximum です。 |
| VifConnectionStatus | ローカルゲートウェイ VIFs ディメンション: OutpostsID 、VirtualInterfaceGroupId 、VirtualInterfaceID 。<br><br>サービスリンク VIFsディメンション: OutpostsID 、VirtualInterfaceID 。 | 仮想インターフェイス (VIFs) がトラフィックを転送する準備ができているかどうかを示します。<br><br>単位: 1 または 0 の場合:<br><br>• 1 – Outpost VIF がオンプレミスデバイスに正常に接続され、設定され、トラフィックを転送する準備ができていることを示します。<br>• 0 – Outpost VIF がトラフィックを転送する準備ができていないことを示します。<br><br>最大解像度: 5 分<br><br>統計: 最も有用な統計は Maximum です。 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| IfTrafficIn | ローカルゲートウェイ VIF (lgw-vif) のディメンション: OutpostsId 、VirtualInterfaceGroupId 、および VirtualInterfaceId<br><br>サービスリンク VIF (sl-vif) のディメンション: OutpostsId および VirtualInterfaceId | Outposts 仮想インターフェイス (VIF) が接続されたローカルネットワークデバイスから受信するデータのビットレート。<br><br>単位: ビット/秒<br><br>最大解像度:5 分<br><br>統計値: 最も有用な統計値は Max および Min です。 |
| IfTrafficOut | ローカルゲートウェイ VIF (lgw-vif) のディメンション: OutpostsId 、VirtualInterfaceGroupId 、および VirtualInterfaceId<br><br>サービスリンク VIF (sl-vif) のディメンション: OutpostsId および VirtualInterfaceId | Outposts 仮想インターフェイス (VIF) が接続されたローカルネットワークデバイスに転送するデータのビットレート。<br><br>単位: ビット/秒<br><br>最大解像度:5 分<br><br>統計値: 最も有用な統計値は Max および Min です。 |

## Outposts メトリクス

Outposts では、次のメトリクスを使用できます。

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| ConnectedStatus | OutpostId | Outpost のサービスリンク接続のステータス。平均統計値が1より小さい場合、接続は障害を受けています。 |

| メトリクス | ディメンション | 説明 |
| --- | --- | --- |
| | | 単位: 個<br><br>最大解像度:1 分<br><br>統計: 最も有用な統計は Average です。 |
| CapacityExceptions | InstanceType および OutpostId | 起動などの容量不足エラーの数。<br><br>単位: 個<br><br>最大解像度:5 分<br><br>統計値: 最も有用な統計値は Maximum および Minimum です。 |

## メトリクスのディメンション

Outpost のメトリクスをフィルタするには、次のディメンションを使用できます。

| ディメンション | 説明 |
| --- | --- |
| Account | 容量を使用してい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。 |

| ディメンション | 説明 |
| --- | --- |
| VirtualInterfaceGroupId | ローカルゲートウェイ仮想インターフェイス (VIF) の仮想インターフェイスグループの ID。 |

## Outposts ラックの CloudWatch メトリクスを表示する

CloudWatch コンソールを使用して、Outposts ラックの CloudWatch メトリクスを表示できます。

CloudWatch コンソールを使用してメトリクスを表示するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで [Metrics (メトリクス)] を選択してください。
3. [Outposts] 名前空間を選択します。
4. (オプション) すべてのディメンションでメトリクスを表示するには、検索フィールドに名称を入力します。

を使用してメトリクスを表示するには AWS CLI

使用可能なメトリクスを表示するには、次の list-metrics コマンドを使用します。

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

を使用してメトリクスの統計を取得するには AWS CLI

次の get-metric-statistics コマンドを使用して、指定されたメトリクスとディメンションの統計情報を取得します。CloudWatch は、ディメンションの一意の組み合わせをそれぞれ別のメトリクスとして扱います。特に発行されていないディメンションの組み合わせを使用した統計を取得することはできません。メトリクス作成時に使用した同じディメンションを指定する必要があります。

```
aws cloudwatch get-metric-statistics \
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \
--statistics Average --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef
 Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

# を使用した AWS Outposts API コールのログ記録 AWS CloudTrail

AWS Outposts は、ユーザー AWS CloudTrail、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、 の API コールをイベント AWS Outposts としてキャプチャします。キャプチャされた呼び出しには、 AWS Outposts コンソールからの呼び出しと AWS Outposts API オペレーションへのコード呼び出しが含まれます。CloudTrail によって収集された情報を使用して、リクエストの実行元の IP アドレス AWS Outposts、リクエストの実行日時などの詳細を確認できます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

CloudTrail は AWS 、アカウントの作成時にアカウントでアクティブになり、CloudTrail イベント履歴に自動的にアクセスできます。CloudTrail の [イベント履歴] では、 AWS リージョンで過去 90 日間に記録された管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。を使用して作成された証跡はすべてマルチリージョン AWS マネジメントコンソール です。 AWS CLIを使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント AWS リージョン 内のすべての でアクティビティをキャプチャするため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョンに記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウントの証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、 AWS CloudTrail ユーザーガイドのAWS CloudTrail 「Lake の使用」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

## AWS Outposts CloudTrail の管理イベント

管理イベントは、 のリソースで実行される管理オペレーションに関する情報を提供します AWS アカウント。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

AWS Outposts は、すべての AWS Outposts コントロールプレーンオペレーションを管理イベントとしてログに記録します。 AWS Outposts が CloudTrail に記録する Outposts AWS コントロールプレーンオペレーションのリストについては、AWS 「Outposts API リファレンス」を参照してください。

## AWS Outposts イベントの例

次の例は、`SetSiteAddress` オペレーションを示す CloudTrail イベントを示しています。

```
{
    "eventVersion": "1.05",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

# Outposts ラックメンテナンス

責任共有モデルの下で、 AWS は AWS サービスを実行するハードウェアとソフトウェアを担当します。これは AWS Outposts、 AWS リージョンの場合と同様に、 に適用されます。たとえば、 はセキュリティパッチ AWS の管理、ファームウェアの更新、Outpost 機器の保守を行います。 AWS また、 は Outposts ラックのパフォーマンス、ヘルス、メトリクスを監視し、メンテナンスが必要かどうかを判断します。

> **Warning**
>
> インスタンスストアボリュームのデータは、基盤となるディスクドライブが故障した場合、またはインスタンスが 停止、休止状態、または終了した場合に失われます。データ損失を防ぐために、インスタンスストアボリューム上の長期データを Amazon S3 バケット、Amazon EBSボリューム、またはオンプレミスネットワーク内のネットワークストレージデバイスなどの永続的なストレージにバックアップすることをお勧めします。

内容



## 連絡先の情報を更新する

Outpost の所有者が変更された場合は、新しい所有者の名前と連絡先の情報をAWS サポート センターまでご連絡ください。

## ハードウェアメンテナンス

がサーバープロビジョニングプロセス中、または Outposts ラックで実行されている Amazon EC2 インスタンスをホスト中にハードウェアに回復不可能な問題 AWS を検出した場合、影響を受けるインスタンスのリタイアが予定されていることをインスタンスの所有者に通知します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスのリタイア」を参照してください。

Outpost の所有者とインスタンスの所有者は、共に問題を解決することができます。インスタンスの所有者は、影響を受けるインスタンスを停止してから再起動し、利用可能な容量に移行させることができます。インスタンスの所有者は、自分たちにとって便利なタイミングで影響を受けるインスタンスを停止および再起動できます。それ以外の場合、 はインスタンスの廃止日に影響を受けるインスタンス AWS を停止して開始します。Outpost に追加の容量がない場合、インスタンスは停止した状態のままとなります。Outpost の所有者は、使用済みの容量を解放するか、Outpost に追加の容量をリクエストして移行を完了させることができます。

ハードウェアのメンテナンスが必要な場合は、Outpost 所有者 AWS に連絡して、 AWS インストールチームが訪問する日時を確認します。訪問は、Outpost の所有者が AWS チームと話し合ってから最短で 2 営業日以内に計画できます。

AWS インストールチームが現場に到着すると、異常なホスト、スイッチ、またはラック要素が置き換えられ、新しい容量がオンラインになります。オンサイトでハードウェアの診断や修理を行うことはありません。ホストを交換すると、NIST 準拠の物理セキュリティ キーが削除および破壊され、ハードウェア上に残る可能性のあるデータが効果的にシュレッダー化されます。これにより、データがサイトから流出することがなくなります。Outpost ネットワーク デバイスを交換する場合、デバイスがサイトから削除されたときにネットワーク構成情報がデバイス上に存在する可能性があります。この情報には、ローカル ネットワークへのパス、またはリージョンへ戻るパスを構成するための仮想インターフェイスを確立するために使用される IP アドレスと ASN が含まれる場合があります。

# ファームウェアの更新

通常、Outpost ファームウェアを更新しても、Outpost 上のインスタンスには影響しません。まれに、アップデートをインストールするために Outpost 機器の再起動が必要になる場合があり、その容量で実行されているインスタンスについてインスタンスの廃止通知が届きます。

# ネットワーク機器のメンテナンス

Outpost ネットワーキングデバイス (OND) のメンテナンスは、通常の Outpost の運用やトラフィックに影響を与えずに実施されます。メンテナンスが必要な場合、トラフィックは OND から離れます。AS-Path の前置や、Outpost のアップリンクでのトラフィックパターンの対応する変更など、一時的な BGP 広告の変更が発生する可能性があります。OND ファームウェアの更新中には、BGP のフラッピングが発生する可能性があります。

お客様のネットワーク機器は、BGP 属性を変更せずに Outpost から BGP アドバタイズを受信し、BGP マルチパス/ロードバランシングを有効にして最適なインバウンドトラフィックフローを可

能にすることをお勧めします。AS-Path のプリペンドは、メンテナンスが必要な場合にトラフィックを OND から離れるようにするために、ローカルゲートウェイのプレフィックスに使用されます。お客様のネットワークは、4 の AS-Path length のルートよりも、1 の AS-Path length の Outposts からのルートを優先する必要があります。

お客様のネットワークは、すべての OND に対して、同じ属性を持つ同じ BGP プレフィックスをアドバタイズする必要があります。デフォルトでは、Outpost ネットワークロードバランスはすべてのアップリンク間でアウトバウンドトラフィックの負荷分散を行います。Outpost 側では、メンテナンスが必要な場合にトラフィックを OND から移行するために、ルーティングポリシーが使用されます。このトラフィックのシフトには、すべての OND で顧客側からの等しい BGP プレフィックスが必要です。お客様のネットワークでメンテナンスが必要な場合は、AS-Path への付加を使用して、特定のアップリンクからのトラフィックを一時的に移行することをお勧めします。

# 電力およびネットワーク イベントのベスト プラクティス

AWS Outposts お客様向けのAWS サービス条件に記載されているように、Outposts 機器が配置されている施設は、Outposts 機器のインストール、メンテナンス、使用をサポートするために、最小限の電力とネットワーク要件を満たしている必要があります。Outposts ラックは、電力供給とネットワーク接続が中断されない場合にのみ正常に動作します。

## 電力イベント

完全な停電では、 AWS Outposts リソースが自動的にサービスに戻らないという固有のリスクがあります。冗長電源およびバックアップ電源ソリューションの導入に加えて、最悪のシナリオの影響を軽減するために、事前に次のことを実行することをお勧めします。

- 制御された方法で DNS ベースまたはラック外のロードバランシングの変更を使用して、サービスとアプリケーションを Outposts の機器から移動させてください。
- コンテナ、インスタンス、データベースを順序立てて停止し、それらを復元する際には逆の順序を使用してください。
- サービスの移動または停止を制御するためのテスト計画。
- 重要なデータと構成をバックアップし、Outpost の外部に保存します。
- 電源のダウンタイムを最小限に抑えます。
- メンテナンス中は電源の切り替え (オフ、オン、オフ、オン) を繰り返さないでください。
- 予期せぬ事態に対処するために、メンテナンス期間内に余分な時間を確保してください。
- 通常必要とされるよりも広いメンテナンス時間枠を伝えることで、ユーザーや顧客の期待に応えます。

- 電源が復旧したら、AWS サポート センターでケースを作成して、 AWS Outposts および関連サービスが実行されていることの検証をリクエストします。

## ネットワーク接続イベント

Outpost と AWS リージョンまたは Outposts ホームリージョン間のサービスリンク接続は、通常、ネットワークメンテナンスが完了すると、アップストリームの企業ネットワークデバイスまたはサードパーティーの接続プロバイダーのネットワークで発生する可能性のあるネットワークの中断や問題から自動的に回復します。サービス リンク接続がダウンしている間、Outposts の操作はローカル ネットワーク アクティビティに限定されます。

Outposts の Amazon EC2 インスタンス、ローカルゲートウェイ、および Amazon EBS ボリュームは引き続き正常に動作し、ローカルネットワークを介してローカルにアクセスできます。同様に、Amazon ECS ワーカーノードなどの AWS サービスリソースは引き続きローカルで実行されます。ただし、API の可用性は低下します。例えば、実行、開始、停止、終了 API は機能しない場合があります。インスタンスメトリクスとログは最大 7 日間ローカルにキャッシュされ、接続が戻ると AWS リージョンにプッシュされます。7 日以上切断すると、メトリクスとログが失われる可能性があります。

詳細については、「施設のネットワーク接続が切断されたときはどうなりますか?」という質問を参照してください。「AWS Outposts ラックに関するよくある質問」ページにあります。

オンサイトの電源の問題またはネットワーク接続の喪失が原因でサービスリンクがダウンした場合、は Outposts を所有するアカウントに通知 Health Dashboard を送信します。中断が予想される場合でも、ユーザーも もサービスリンクの中断の通知を抑制する AWS ことはできません。詳細については、「AWS Health ユーザーガイド」の「Health Dashboardの開始方法」を参照してください。

ネットワーク接続に影響を与える計画的なサービス メンテナンスの場合は、次の予防的な手順を実行して、潜在的な問題のあるシナリオの影響を制限してください。

- Outposts ラックがインターネットまたはパブリック Direct Connect を介して親 AWS リージョンに接続する場合、計画されたメンテナンスの前にトレースルートをキャプチャします。動作中の (ネットワーク メンテナンス前) ネットワーク パスと問題のある (ネットワーク メンテナンス後) ネットワーク パスを用意して違いを特定すると、トラブルシューティングに役立ちます。メンテナンス後の問題を AWS または ISP にエスカレーションする場合は、この情報を含めることができます。

  以下の間のトレース ルートをキャプチャします。

  - Outposts の場所のパブリック IP アドレスと、`outposts.region.amazonaws.com` によって返された IP アドレス。*region* を親 AWS リージョンの名前に置き換えます。
  - パブリック インターネット接続と Outposts の場所のパブリック IP アドレスを持つ親リージョン内のインスタンス。
- ネットワークのメンテナンスを管理している場合は、サービス リンクのダウンタイムの期間を制限します。メンテナンスプロセスに、ネットワークが回復したことを確認するステップを含めます。
- 発表されたメンテナンス期間の終了時にサービス リンクがバックアップされていない場合、ネットワーク メンテナンスを管理できない場合は、発表されたメンテナンス期間に関してサービス リンクのダウンタイムを監視し、計画されたネットワーク メンテナンスの担当者に早めにエスカレーションしてください。

## リソース

計画的または計画外の電力イベントやネットワーク イベントの後、Outpost が正常に動作していることを保証できる監視関連リソースをいくつか紹介します。

- AWS ブログ「 のモニタリングのベストプラクティス AWS Outposts」では、Outposts 固有のオブザーバビリティとイベント管理のベストプラクティスについて説明しています。
- AWS ブログ「Amazon VPC からのネットワーク接続用のデバッグツール」では、AWSSupport-SetupIPMonitoringFromVPC ツールについて説明します。本ツールは、お客様が指定したサブネットに Amazon EC2 Monitor Instance を作成し、対象の IP AWS Systems Manager アドレスを監視するためのドキュメント (SSM ドキュメント)です。このドキュメントでは、ping、MTR、TCP トレースルート、トレースパス診断テストを実行し、結果を Amazon CloudWatch Logs に保存し、CloudWatch ダッシュボードで視覚化できます。(例: 遅延、パケット損失)。Outposts モニタリングの場合、モニターインスタンスは親 AWS リージョンの 1 つのサブネットにあり、プライベート IP (複数可) を使用して 1 つ以上の Outpost インスタンスをモニタリングするように設定する必要があります。これにより、 AWS Outposts と親 AWS リージョン間のパケット損失グラフとレイテンシーが提供されます。
- AWS ブログ AWS Outposts を使用した自動 Amazon CloudWatch ダッシュボードのデプロイ AWS CDKでは、自動ダッシュボードのデプロイに関連する手順について説明します。
- 質問がある場合、または詳細情報が必要な場合は、「AWS サポートユーザー ガイド」の「サポート ケースの作成」を参照してください。

# Outposts ラックの契約期間終了オプション

AWS Outposts 期間が終了したら、次のオプションのいずれかを選択する必要があります。

- サブスクリプションを更新し、既存の Outposts ラックを維持する。
- Outposts ラックを返却用に準備します。
- 月単位のサブスクリプションに切り替えて、既存の Outposts ラックを維持する。

## サブスクリプションを更新する

Outposts ラックの現在のサブスクリプションが終了する少なくとも 5 営業日前に、次のステップを完了する必要があります。現在のサブスクリプションが終了する少なくとも 5 営業日前にこれらのステップを完了しないと、予期しない料金が発生する可能性があります。

サブスクリプションを更新して既存の Outposts ラックを保持するには:

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで、[Outpost] を選択してください。
3. [アクション] を選択します。
4. Outpost の更新を選択します。
5. サブスクリプション期間の長さと支払いオプションを選択します。

   料金については、「AWS Outposts ラックの料金」を参照してください。見積もりをリクエストすることもできます。
6. サポートチケットの送信を選択します。

> **Note**
>
> Outposts ラックの現在のサブスクリプションが終了する前に更新すると、前払い料金がすぐに請求されます。

新しいサブスクリプションは、現在のサブスクリプションが終了した翌日に開始されます。

サブスクリプションの更新や Outposts ラックの返却を指定しない場合、自動的に月単位のサブスクリプションに切り替わります。Outposts ラックは、 AWS Outposts 設定に対応する前払いなしオプ

ションの割合で毎月更新されます。新しい月単位サブスクリプションは、現在のサブスクリプションが終了した翌日に開始されます。

# AWS Outposts ラックを返す

Outposts AWS Outposts ラックの現在のサブスクリプションが終了する少なくとも 5 営業日前に、ラックを返却できるように準備し、廃止プロセスを完了する必要があります。完了するまで、 AWS は返却プロセスを開始できません。現在のサブスクリプションが終了する少なくとも 5 営業日前にこれらのステップを完了しないと、廃止の遅延や予期しない料金が発生する可能性があります。

Outposts ラックを返送しても、配送料金は発生しません。ただし、破損したラックを返送すると、コストが発生する可能性があります。

AWS Outposts ラックの返送を準備するには:

> **Important**
>
> スケジュールされた取り出しのために AWS がオンサイトになるまで、Outposts ラックの電源を切らないでください。

1. Outpost のリソースが共有されている場合、これらのリソースの共有を解除する必要があります。

   以下の方法で、共有されている Outpost のリソースの共有を解除できます。

   - AWS RAM コンソールを使用します。詳細については、「AWS RAM ユーザーガイド」の「リソース共有のアップデート」を参照してください。
   - を使用して disassociate-resource-share コマンド AWS CLI を実行します。

   共有可能な Outpost リソースの一覧については、「共有可能な Outpost リソース」を参照してください。
2. Outpost のサブネットに関連するアクティブなインスタンスを終了してください。インスタンスを終了するには、「Amazon EC2 ユーザーガイド」の「インスタンスの終了」のステップに従ってください。

> **Note**
>
> Application Load Balancer や Amazon Relational Database Service (RDS) など、Outpost で実行されている一部の AWSマネージドサービスは、EC2 容量を消費します。ただし、関連するインスタンスは Amazon EC2 ダッシュボードには表示されません。キャパシティを解放するには、これらのサービスに関連付けられたリソースを終了する必要があります。詳細については、「私たちのアウトポストで一部の EC2 インスタンス容量が不足しているのはなぜですか？」を参照してください。

3. AWS アカウント内の Amazon EC2 インスタンスのインスタンスキャパシティアベイラビリティを確認します。

   a. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。

   b. Outposts を選択します。

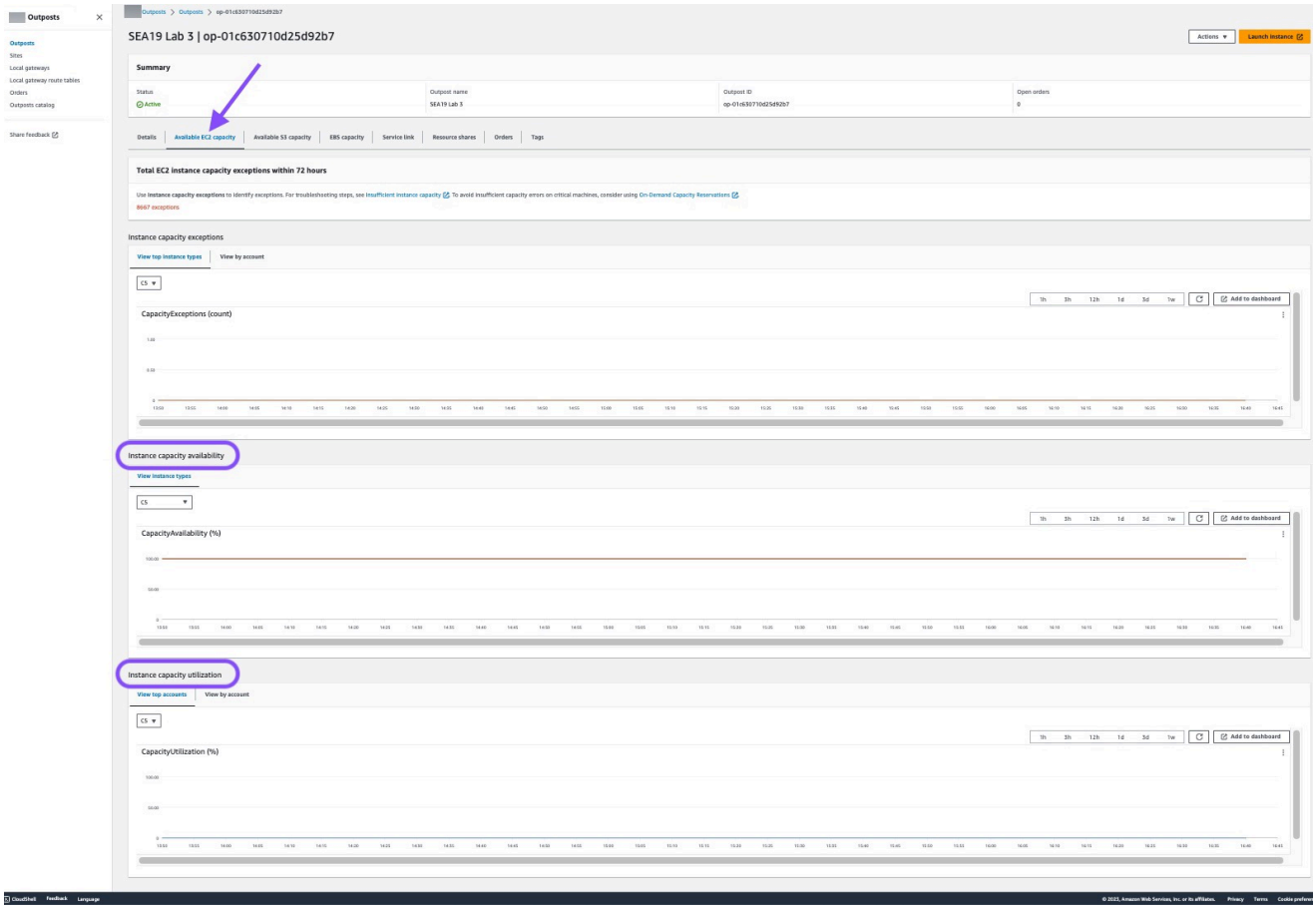
   c. 返す特定の Outpost を選択します。

   d. Outpost のページで、利用可能な EC2 キャパシティタブを選択します。

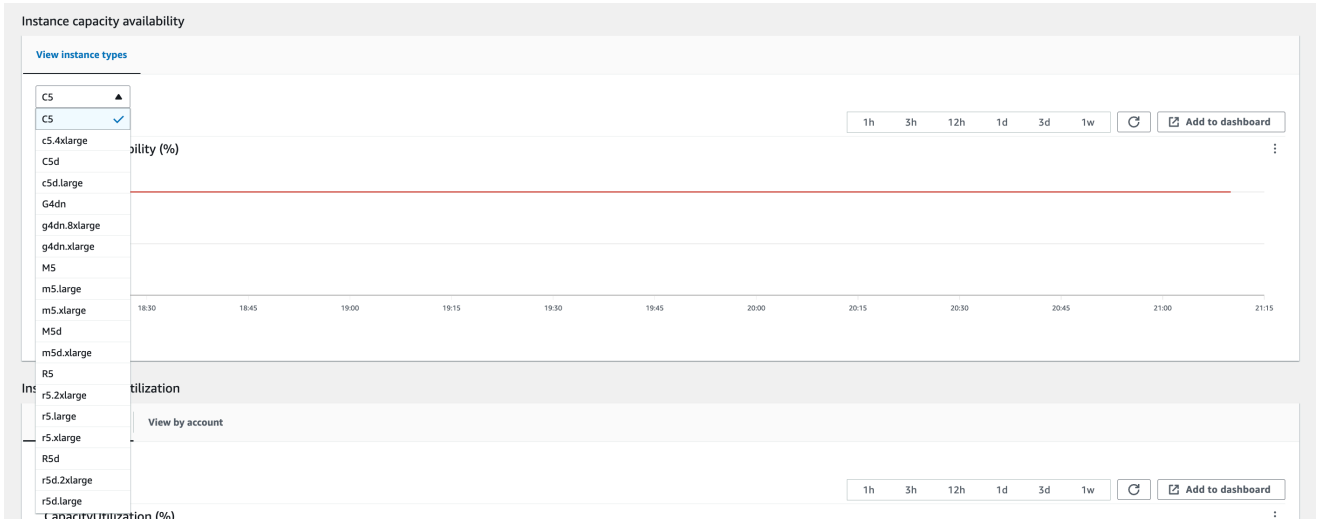
   e. 各インスタンスファミリーのインスタンス容量の可用性が 100% であることを確認します。

   f. 各インスタンスファミリーのインスタンス容量の使用率が 0% であることを確認します。

      以下の画像は、[利用可能な EC2 容量] タブの「インスタンス容量の可用性」と「インスタンス容量の使用率」グラフを示しています。




以下の画像は、インスタンスタイプのリストを示しています。




4. Amazon EC2 インスタンスとサーバーボリュームのバックアップを作成します。バックアップを作成するには、「AWS 規範ガイダンスガイド」の「EBS ボリュームを使用した Amazon EC2 のバックアップとリカバリ」の手順に従ってください。
5. Outpost に関連付けられている Amazon EBS ボリュームを削除します。

a. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
b. ナビゲーションペインの [ボリューム] を選択します。
c. アクションとボリューム削除を選択します。
d. 確認ダイアログボックスで、[削除] を選択します。

6. Amazon S3 を Outposts にインストールしている場合、Outposts にあるローカルスナップショットをすべて削除します。

a. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
b. ナビゲーションペインで、[Snapshots (スナップショット)] を選択します。
c. アウトポスト ARN のスナップショットを選択します。
d. アクションとスナップショット削除を選択します。
e. 確認ダイアログボックスで、[削除] を選択します。

7. Outposts ラックに関連付けられている Amazon S3 バケットをすべて削除します。バケットを削除するには、Amazon S3 on Outposts ユーザーガイド」の「Amazon S3 on Outposts バケットの削除」の手順に従います。 Amazon S3
8. Outpost に関連付けられている VPC アソシエーションとカスタマー所有の IP アドレスプール (CoIP) CIDR をすべて削除します。

AWS 取り出しチームがラックの電源を切ります。電源を切ったら、 AWS Nitro セキュリティキーを破棄するか、 AWS 取得チームがユーザーに代わって破棄できます。

AWS Outposts ラックを返却するには

> **Important**
> AWS は、廃止リクエストを送信した後、返却プロセスを停止することはできません。

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで、[Outpost] を選択してください。
3. [アクション] を選択します。
4. Decommission Outpost を選択し、ワークフローに従ってリソースを削除します。
5. [Submit request (リクエストの送信)] を選択します。

AWS 担当者から連絡があり、廃止プロセスが開始されます。

> **Note**
>
> Outposts ラックの現在のサブスクリプションが終了する前にラックを返却しても、この Outpost に関連する未払いの料金は終了しません。

AWS 取り出しチームがラックの電源を切ります。電源を切ったら、 AWS Nitro セキュリティキーを破棄するか、 AWS 取得チームがユーザーに代わって破棄できます。

## 月単位のサブスクリプションへの変換

月単位のサブスクリプションに切り替えて、既存の Outposts ラックを維持する場合、アクションを起こす必要はありません。質問がある場合は、請求サポートケースを開いてください。

Outposts ラックは、Outposts 設定に対応する前払いなしオプションのレートで毎月更新されます。新しい月単位サブスクリプションは、現在のサブスクリプションが終了した翌日に開始されます。

# のクォータ AWS Outposts

にはデフォルトのクォータ AWS アカウント があり、以前は制限と呼ばれていました AWS のサービス。特に明記していない限り、クォータはリージョン固有です。一部のクォータについては引き上げをリクエストできますが、一部のクォータについてはリクエストできません。

のクォータを表示するには AWS Outposts、Service Quotas コンソールを開きます。ナビゲーションペインで、[AWS のサービス] を選択し、次に [AWS Outposts] を選択します。

クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト を参照してください。

AWS アカウント には、 に関連する次のクォータがあります AWS Outposts。

| リソース | デフォルト値 | 引き上げ可能 | コメント |
|---|---|---|---|
| Outpost サイト | 100 | 可能 | Outpost サイトは、Outpost 機器に電力を供給してネットワークに接続する、カスタマー管理の物理的な建物です。<br><br>AWS アカウントの各リージョンに 100 の Outposts サイトを設定できます。 |
| サイトあたりの Outpost | 10 | 可能 | AWS Outposts には、Outposts と呼ばれるハードウェアおよび仮想リソースが含まれています。このクォータは、Outpost 仮想リソースを制限します。<br><br>各 Outposts サイトには 10 個の Outpost を設置できます。 |

## AWS Outposts および他の サービスのクォータ

AWS Outposts は他の サービスのリソースに依存し、それらのサービスには独自のデフォルトクォータがある場合があります。例えば、ローカルネットワークインターフェイスのクォータは、ネットワークインターフェイスの Amazon VPC クォータから取得されます。

# Outposts ラックのドキュメント履歴

以下の表は、Outposts ラックのドキュメントに対する更新について説明しています。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| AWS Outposts が Dell および HPE ストレージ配列の外部ブロックボリュームをサポート | Dell PowerStore や HPE Alletra Storage MP B10000 などのサードパーティーベンダーがサポートする外部ブロックデータとブートボリュームを使用できます。 | 2025 年 9 月 30 日 |
| VIF 接続ステータスと BGP セッション状態に使用できるメトリクス。 | ConnectionStatus と BGPSessionState AWS Outposts メトリクスを使用して、CloudWatch コンソールで VIF 接続と BGP セッションのステータスをモニタリングできます。 ConnectionStatus BGPSessionState | 2025 年 7 月 31 日 |
| サブスクリプションの更新と返却用のラックの準備 | サブスクリプションを更新したり、ラックを返却したりするには、現在のサブスクリプションが終了する少なくとも 10 営業日前にプロセスを完了する必要があります。 | 2025 年 7 月 16 日 |
| AWS サービスのサポート | AWS Outposts は、Outpost が動作する AWS リージョンに基づいて AWS サービスをサポートします。 | 2025 年 7 月 14 日 |
| 静的安定性の更新 | ネットワークが中断された場合、インスタンスメトリクスとログは最大 7 日間ローカル | 2025 年 5 月 1 日 |

| | | |
|---|---|---|
| | にキャッシュされます。以前は、Outposts はわずか数時間ログをキャッシュできました。 | |
| AWS Identity and Access Management サービスにリンクされたロール AWSServiceRoleForOutposts_*OutpostID* の更新 | AWSServiceRoleForOutposts_*OutpostID* サービスにリンクされたロールのアクセス許可が更新され、 がプライベート接続のネットワークリソース AWS Outposts を管理する方法を絞り込み、サービスリンクエンドポイントインスタンスに必要なネットワークインターフェイスとセキュリティグループのオペレーションをより正確に制御できるようになりました。 | 2025 年 4 月 17 日 |
| アセットレベルでのキャパシティ管理 | アセットレベルで容量設定を変更できます。 | 2025 年 3 月 31 日 |
| Direct Connect トランジット VIF を使用したプライベート接続 | Direct Connect トランジット VIF を使用して Outposts とホーム AWS リージョン間のプライベート接続を有効にするようにサービスリンクを設定できるようになりました。 | 2024 年 12 月 11 日 |
| サードパーティーストレージにバックアップされた外部ブロックボリューム | Outpost のインスタンス起動プロセス中に、互換性のあるサードパーティーのブロックストレージシステムによってバックアップされたブロックデータボリュームをアタッチできるようになりました。 | 2024 年 12 月 1 日 |

| | | |
|---|---|---|
| キャパシティ管理 | インスタンスの容量設定を変更できます。 | 2024 年 11 月 11 日 |
| キャパシティ管理 | 新しい Outposts の注文のデフォルトのキャパシティ設定を変更できます。 | 2024 年 4 月 16 日 |
| AWS Outposts ラックがサービスリンクインターフェイスのスループットメトリクスをサポート | `IfTrafficIn` および `IfTrafficOut` Amazon CloudWatch メトリクスを活用して、Outposts ラックサービスリンク仮想インターフェイス (VIFs) とローカルネットワークデバイス間のスループット使用状況をモニタリングできるようになりました。 | 2023 年 11 月 17 日 |
| ローカルゲートウェイ AWS Outposts との VPC 内通信 | ローカル ゲートウェイを使用して、異なる Outpost 全体で同じ VPC 内のサブネット間の通信を確立できます。 | 2023 年 8 月 30 日 |
| AWS Outposts ラックEnd-of-termオプション | AWS Outposts 契約期間の終了時に、サブスクリプションを更新、終了、または変換できます。 | 2023 年 8 月 1 日 |

| | | |
|---|---|---|
| Amazon Route 53 on Outposts は AWS Outposts ラックで使用できます。 | Outposts の Amazon Route 53 には、 AWS Outpostsから来たすべての DNS クエリをキャッシュするリゾルバーが含まれています。インバウンドおよびアウトバウンドエンドポイントをデプロイするとき、Outpost とオンプレミス DNS リゾルバーの間でハイブリッド接続をセットアップすることもできます。 | 2023 年 7 月 20 日 |
| ローカルゲートウェイのインバウンドルート | Outpost 上に Elastic Network Interface へのローカルゲートウェイ着信ルートを作成および変更できます。 | 2022 年 9 月 15 日 |
| の直接 VPC ルーティングの紹介 AWS Outposts | 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。 | 2022 年 9 月 14 日 |
| Outposts ラック用 AWS Outposts ユーザーガイドを作成 | AWS Outposts ユーザーガイドは、ラックとサーバーの個別のガイドに分かれています。 | 2022 年 9 月 14 日 |
| ローカルゲートウェイルートテーブルの作成と管理 | ローカルゲートウェイのルートテーブルおよび CoIP プールを作成および変更します。VIF グループの関連付けを管理します。 | 2022 年 9 月 14 日 |
| でのプレイスメントグループ AWS Outposts | スプレッド戦略を使用する配置グループは、インスタンスを異なるホストに分散させることができます。 | 2022 年 6 月 30 日 |

| | | |
|---|---|---|
| の専有ホスト AWS Outposts | Outposts 上で専有ホストを使用できるようになりました。 | 2022 年 5 月 31 日 |
| 共有の Outpost サイト | Outpost サイトを作成および管理し、組織内の他の AWS アカウントと共有します。 | 2021 年 10 月 18 日 |
| 新しい CloudWatch のディメンション | AWS Outposts 名前空間内のメトリクスの新しい CloudWatch ディメンション。 | 2021 年 10 月 13 日 |
| S3 バケットを共有する | Outpost 上で S3 バケットを共有および管理します。 | 2021 年 8 月 5 日 |
| 一部のプレイスメントグループのサポート | クラスター、パーティション、スプレッドプレイスメント戦略は、リージョンと同じように使用できます。 | 2021 年 7 月 28 日 |
| 追加の CloudWatch のメトリクス | リザーブドインスタンスに対して追加の CloudWatch メトリクスが利用可能になりました。 | 2021 年 5 月 24 日 |
| ネットワークトラブルシューティングチェックリスト | ネットワークトラブルシューティングチェックリストも用意されています。 | 2021 年 2 月 22 日 |
| 追加の CloudWatch のメトリクス | EBS ボリュームに関する追加の CloudWatch メトリクスが利用可能になりました。 | 2021 年 2 月 2 日 |
| コンソールの注文の更新 | コンソールの注文プロセスが更新されました。 | 2021 年 1 月 14 日 |
| プライベート接続 | AWS Outposts コンソールで Outpost を作成する場合、Outpost のプライベート接続を構成できます。 | 2020 年 12 月 21 日 |

| | | |
|---|---|---|
| ネットワーク準備チェックリスト | Outpost 構成に関する情報を収集する際に、ネットワーク準備チェックリストを使用します。 | 2020 年 10 月 28 日 |
| 共有 AWS Outposts リソース | Outpost 共有を使用すると、Outpost 所有者は、ローカルゲートウェイルートテーブルを含む Outposts と Outpost リソースを、同じ AWS 組織内の他の AWS アカウントと共有できます。 | 2020 年 10 月 15 日 |
| 追加の CloudWatch のメトリクス | インスタンスタイプの数に関する追加の CloudWatch メトリクスが利用可能になりました。 | 2020 年 9 月 21 日 |
| 追加の CloudWatch のメトリクス | サービスリンクの接続状態に関する追加の CloudWatch メトリクスが利用可能になりました。 | 2020 年 9 月 11 日 |
| カスタマー所有 IPv4 アドレス共有のサポート | を使用して AWS Resource Access Manager 、顧客所有の IPv4 アドレスを共有します。 | 2020 年 4 月 20 日 |
| 追加の CloudWatch のメトリクス | EBS ボリュームに関する追加の CloudWatch メトリクスが利用可能になりました。 | 2020 年 4 月 4 日 |
| 初回リリース | これは の初期リリースです AWS Outposts。 | 2019 年 12 月 3 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。