ラックのユーザーガイド

AWS Outposts

AWS 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、ツールをお客様のオンプレミス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 は、レイテンシーを短縮し、ローカルデータ処理のニーズに対応するために、ローカルコンピューティングとストレージリソースを使用しながら、 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して実行できるようにします。

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 内で、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 を接続することができません。

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。Outpost の容量は、 AWS Outposts コンソールで表示および管理できます。
- 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、電力シェルフ、およびブランクパネルが含まれています。

- Outposts ACE ラック – Aggregation、Core、Edge (ACE) ラックは、マルチラック Outpost デプロイのネットワーク集約ポイントとして機能します。ACE ラックは、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の接続を提供することで、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の数を減らします。

  コンピューティングラックが 5 台以上ある場合は、ACE ラックをインストールする必要があります。コンピュートラックが 5 台未満で、将来 5 台以上に拡張する予定がある場合は、できるだけ早く 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。Outpost サーバーは、スペースが限られているか、容量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。
- 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) — Outpost ラックとオンプレミスネットワーク間の通信を可能にする論理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 — Outpost 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

リソースタイプ	ラック	サーバー
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 (ストレージ)]

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
Amazon SageMaker Edge Manager	 はい	 はい

料金

さまざまな Outpost 構成から選択できます。それぞれが EC2 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を提供しています。ラック構成の価格には、取り付け、取り外し、およびメンテナンスが含まれています。サーバーの場合、装置の取り付けとメンテナンスが必要です。

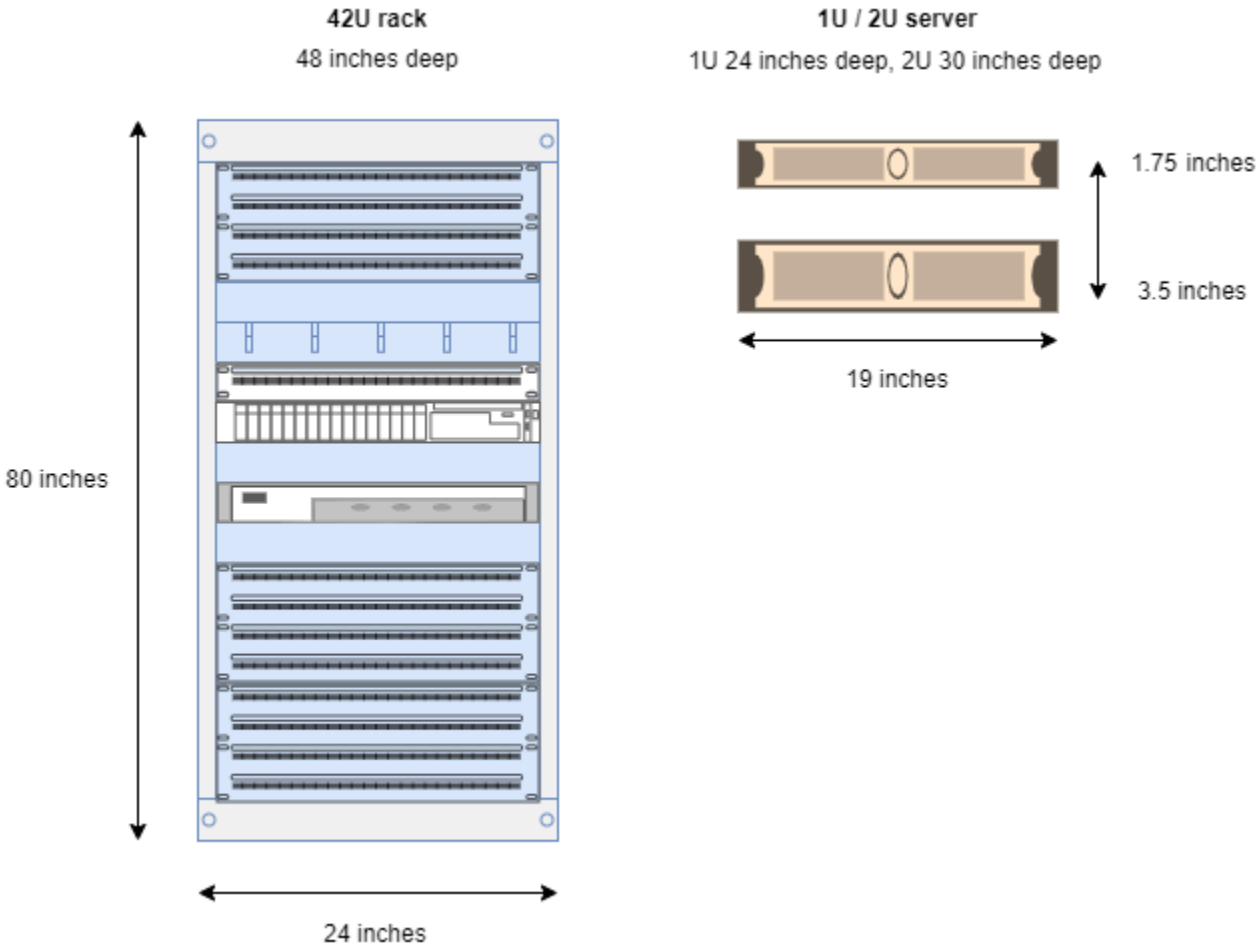
3 年間の契約期間の構成を購入し、全額一括、一部前払い、および前払いなしの3つの支払いオプションから選択できます。一部前払いオプションまたは前払いなしオプションを選択した場合、月単位料金が適用されます。前払い料金は、Outpost がインストールされ、コンピューティング容量とストレージ容量が使用可能になってから 24 時間後に適用されます。詳細については、以下を参照してください。

- AWS Outposts ラック料金
- AWS Outposts サーバーの料金

AWS Outposts の仕組み

AWS Outposts は、Outpost と AWS リージョン間の一定かつ一貫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、リージョンとインターネット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

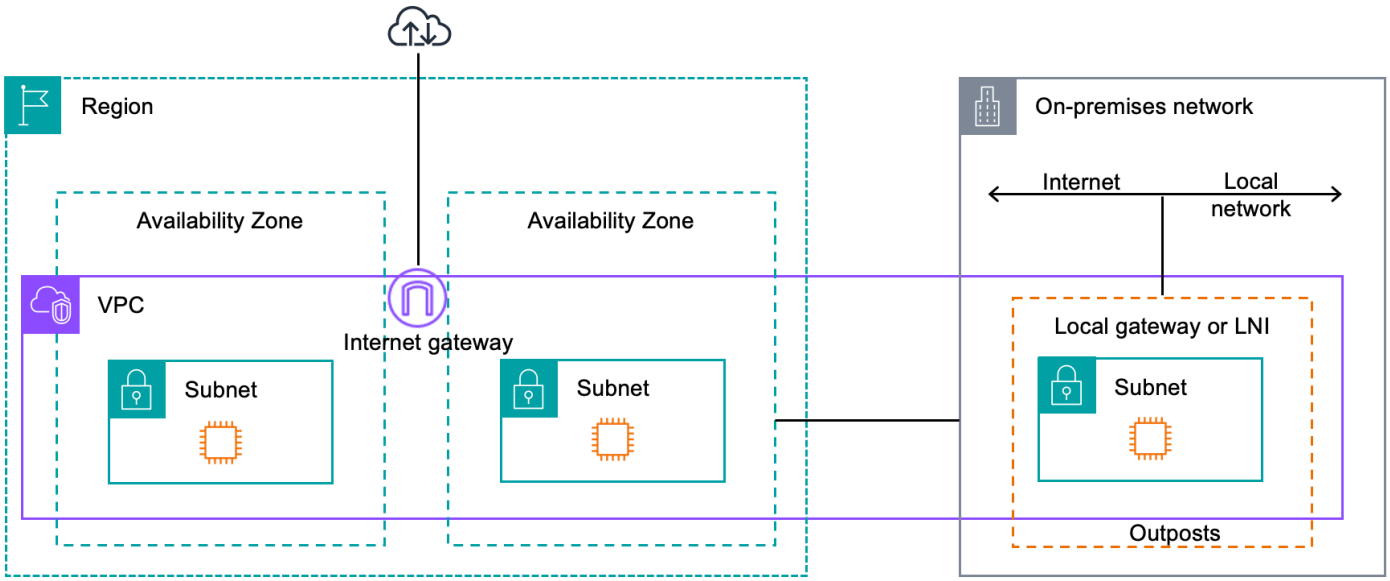
- DNS
- サービスリンク
- ローカルゲートウェイ
- ローカルネットワークインターフェイス

ネットワークコンポーネント

AWS Outposts は、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、 AWS リージョンでアクセス可能な VPC コンポーネントを使用して、Amazon VPC を リージョンから Outpost に拡張します。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
- ローカル ゲートウェイ (ラック) またはローカルネットワークインターフェイス (サーバー) によって提供される Outpost とローカルネットワーク間の接続



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っています。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 s、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 機能が機能するためには、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 Outpost 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 AWS 。

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。

- への Outpost 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

Outpost 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。Outpost 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 Outpost ラックでのみ動作し、Outpost 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。

- 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

Outpost 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。Outpost 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ています。集約、コア、エッジ (ACE) ラックをインストールする場合、サイトは 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 ACE ラックのサイト要件。

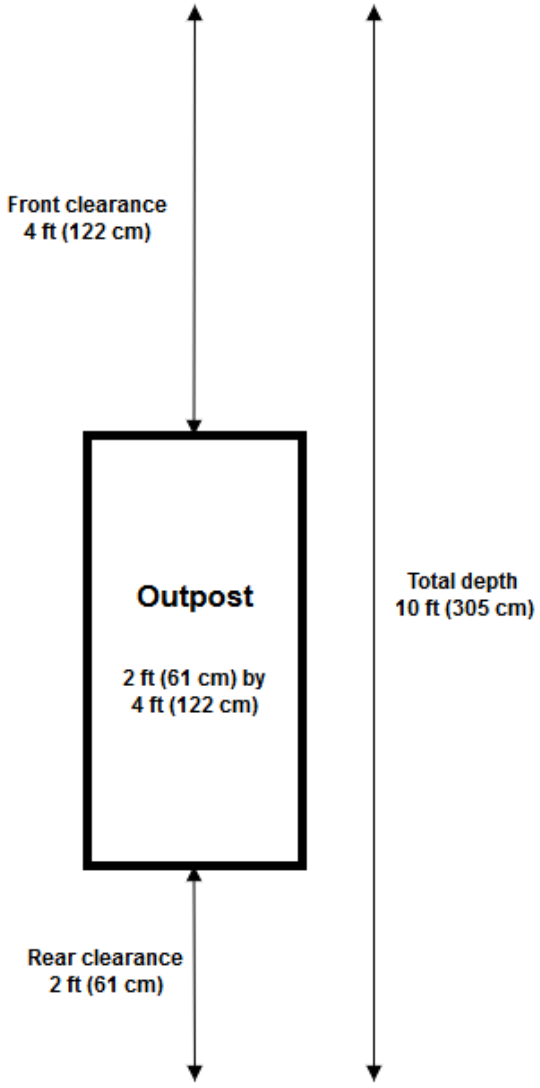
Outposts サービスの要件については、「Outposts サーバーのAWS Outposts ユーザーガイド」の「Outposts サービスのサイト要件」を参照してください。

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)。



- 耐震支柱 – 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支柱を設置して維持します。 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 – AWS認定技術者が設置中にラックをボンディングできるように、ラックの位置をボンディングワイヤ/ポイントとして指定することをお勧めします。
- 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 に悪影響を与える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 リージョン内の送信先の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

以下のファイバー型がサポートされています。

- ルーセントコネクタ (LC) 付きシングルモードファイバー (SMF)
- LC 搭載のマルチモードファイバー (MMF) または MMF OM4

アップリンク速度と選択したファイバーの種類に応じて、次の光学規格がサポートされます。

アップリンク速度	ファイバータイプ	光学標準
1 Gbps	SMF	— 1000Base-LX
1 Gbps	MMF	– 1000Base-SX
10 Gbps	SMF	– 10GBASE-IR – 10GBASE-LR
10 Gbps	MMF	– 10GBASE-SR
40 Gbps	SMF	— 40GBASE-IR4 (LR4L) – 40GBASE-LR4
4 x 10 Gbps ブレークアウトアプリケーション	MMF	– 40GBASE-ESR4 – 40GBASE-SR4
100 Gbps	SMF	— 100G PSM4 MSA — 100GBASE-CWDM4 – 100GBASE-LR4
4 x 25 Gbps ブレークアウトアプリケーション	MMF	– 100GBASE-SR4

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、「リンク集約と仮想 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) — 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) — 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) — 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) — 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間の 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 OutpostsAWS 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。 – 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。 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

AWS 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。

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

Outpost	ローカルゲートウェイ BGP の要件
	イベート ASN 範囲 (64512 ~ 65534 または 4200000000 ~ 4294967294) から。 — 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。 – 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。 – 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 リソースの電力消費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

要件	の仕様
	3 フェーズ ： • 208 ~ 250 VAC (デルタ) 、50 ~ 60 Hz • 346 ~ 480 VAC (Wye)、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): D カーブまたは K カーブサーキットブレーカーを備えた 30 A、32 A、または 50 A。 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。 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 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 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 **Note** 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)
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	2 x L6-30P または IEC309、1 つは S1 に、1 つは S2 にドロップ	2 x AH530P7W, AH532P6W または CS8365C1 つは S1 に、もう 1 つは S2 にドロップ	L6-30P または IEC309 を 1 つ、S1 に 1 つドロップ	1 x AH530P7W, AH532P6W または CS8365C ; S1 に 1 ドロップ
10 kVA	4 x L6-30P または IEC309、2 つは S1 に、2 つは S2 にドロップ		L6-30P または IEC309 を 2 つ、S1 に 2 つドロップ	
15 kVA	6 x L6-30P または IEC309。3 つは S1 に、3 つは S2 にドロップ		L6-30P または IEC309 を 3 つ、S1 に 3 つドロップ	

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。
- お客様である 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、 への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 はユーザー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、予定された日時に到着します。ラックを特定の位置に配置します。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得る必要があります。お客様は、コンプライアンスと変更の安全性を検証するドキュメント AWS を に提供することに同意します。 AWS は、Outpost の電気設備または施設の電気系統、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。

Outposts ACE ラックのサイト要件

> **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、マルチラック Outpost デプロイの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 5 台以上ある場合は、ACE ラックをインストールする必要があります。コンピュートラックが 5 台未満で、将来 5 台以上に拡張する予定がある場合は、できるだけ早く ACE ラックを設置することをお勧めします。

ACE ラックをインストールするには、 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Outposts ラックのサイト要件。

施設

これらは ACE ラックの施設要件です。

- 電源 — すべてのラックには 10kVA 単相 (AA+BB、IEC60309 または L6-30P ホイップコネクタタイプ) が付属しています。
- 重量サポート – ラック重量は 705 ポンド、320 kg です。
- 間隔/サイズディメンション – ラックの高さは 80 インチ、203 cm です。

> **Note**
>
> ACE ラックは完全には囲まれておらず、前面ドアや背面ドアは含まれていません。

ネットワーク

これらは ACE ラックのネットワーク要件です。ACE ラックが 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 Outpost ラックを接続する方法については、「」を参照してくださいACE ラック接続。

- 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 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 つのネットワークデバイスがあり、1 つの Outposts ラックの場合のように 2 つではありません。
  - 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 の速度でアップリンクを提供します。サービスリンク接続の帯域幅に関する推奨事項については、「」を参照してくださいサービスリンクの推奨帯域幅。

  > **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 — Lucent コネクタ (LC) を備えたシングルモードファイバー (SMF)、または Lucent コネクタ (LC) を備えたマルチモードファイバー (MMF) を提供します。サポートされているファイバータイプと光学規格の完全なリストについては、「」を参照してくださいアップリンク速度、ポート、ファイバー。
- アップストリームデバイス — スイッチまたはルーターのアップストリームデバイスを 2 つまたは 4 つ提供します。
- サービス VLAN とローカルゲートウェイ VLAN – 4 つの 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 を指定する必要があります。サービス VLANs とローカルゲートウェイ VLAN の 2 つの異なる VLAN のみを提供するか、サービス VLANs と LGW VLAN の両方について各 ACE ネットワークデバイスに異なる VLAN を持つか、合計 8 つの異なる VLANsかを選択できます。リンク集約グループ (LAGsリンクアグリゲーション「」および「」を参照してください仮想 LAN。

- サービスリンクとローカルゲートウェイ VLANs の CIDR と IP アドレス — /30 または /31 CIDR を使用して、各 ACE ネットワークデバイスに専用サブネットを割り当てることをお勧めします。または、サービスおよびローカルゲートウェイ VLAN ごとに 1 つの /29 サブネットを割り当てることもできます。いずれの場合も、使用する ACE ネットワークデバイスの 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 とローカルゲートウェイ VLAN のカスタマーおよび Outpost BGP 自律システム番号 (ASN) – Outpost は、各 ACE ラックデバイスとローカルネットワークデバイスの間に、サービスリンク VLAN を介したサービスリンク接続用の外部 BGP (eBGP) ピアリングセッションを確立します。さらに、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て、ローカルネットワークからローカルゲートウェイに接続します。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各コンピューティングラックには、サービスリンクインフラストラクチャサブネット (/26 である必要があります) が必要です。

電源

これらは 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。 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。

の使用を開始する AWS Outposts

開始するためには、アウトポストを注文します。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にアクセスします。

タスク

- Outpost を作成して Outpost 容量を注文する
- Outpost ラックでインスタンスを起動する

Outpost を作成して Outpost 容量を注文する

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。
- Outpost AWS アカウント を所有する を決定します。このアカウントを使用して、Outposts サイトを作成し、Outpost を作成し、注文してください。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: インスタンス容量を変更する
- 次のステップ

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. Outpost を所有 AWS アカウント する AWS を使用して にサインインします。
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 のに役立つ可能性のある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。次に、注文時にこの Outpost を指定します。

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] を選択します。
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。
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。

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。ご注文後、 AWS Outposts 担当者よりご連絡させていただきます。

> **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。すべての前払いを選択しない場合は、3 年間にわたって毎月の料金を支払うことになります。

  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で、[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. キャパシティを増やすには、構成を選択します。使用可能な設定が二ーズを満たさない場合は、AWS に連絡してカスタム容量設定をリクエストできます。
5. [次へ] をクリックします。
6. [既存の Outpost を使用] を選択し、Outpost を選択します。
7. [次へ] をクリックします。
8. 契約期間と支払いオプションを選択します。
9. 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。
10. [次へ] をクリックします。
11. [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。
12. [発注する] を選択します。

ステップ 4: インスタンス容量を変更する

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として、お客様のサイトに AWS コンピューティング性能とストレージ容量のプールを提供します。Outpost で使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、 がサイトにインストールする AWS

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、サーバー障害や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、および Amazon S3 の容量を決定できます。

新しい Outpost 注文の容量は、デフォルトの容量設定で設定されます。デフォルト設定を変換して、ビジネスニーズに合わせて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、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。

> **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 レベルで定義されます。
> - 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。

インスタンス容量を変更するには

1. AWS Outposts コンソールのAWS Outposts 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の作成」を選択します。
3. 開始方法ページで、順序を選択します。
4. 容量を変更するには、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. 新しい Outpost 容量設定の変更 を選択します。
2. [次へ] をクリックします。
3. インスタンス容量の設定 ページで、各インスタンスタイプに 1 つのインスタンスサイズが表示され、最大数は事前に選択されています。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. インスタンス数を指定し、そのインスタンスサイズに表示される容量を書き留めます。
5. 各インスタンスタイプのセクションの最後に、容量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を表示します。インスタンスサイズまたは数量レベルで調整して、使用可能な合計容量を最適化します。

6. 特定のインスタンスサイズに合わせて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にある自動調整を選択します。

7. インスタンスタイプごとに、インスタンス数が少なくとも 1 つのインスタンスサイズに指定されていることを確認します。
8. [次へ] をクリックします。
9. 確認と作成ページで、リクエストしている更新を確認します。
10. 「Create」を選択します。容量タスク AWS Outposts を作成します。
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、実行中のインスタンスを 1 つ以上停止するように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。
> - 注文の完了後に容量を変更する必要がある場合は、 AWS Support に連絡して変更を行ってください。

Upload JSON file

1. キャパシティ設定のアップロード を選択します。
2. [次へ] をクリックします。
3. 容量設定プランの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:

```
{
    "RequestedInstancePools": [
        {
            "InstanceType": "c5.24xlarge",
            "Count": 1
```

```
        },
        {
            "InstanceType": "m5.24xlarge",
            "Count": 2
        }
    ]
}
```

4. 容量設定プランセクションの JSON ファイルの内容を確認します。
5. [次へ] をクリックします。
6. 確認と作成ページで、リクエストしている更新を確認します。
7. 「Create」を選択します。容量タスク AWS Outposts を作成します。
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、実行中のインスタンスを 1 つ以上停止するように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。
> - 注文の完了後に容量を変更する必要がある場合は、 AWS Support に連絡して変更を行ってください。

次のステップ

AWS Outposts 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。注文の初期ステータスは [注文を受け取りました] です。 AWS 3 営業日以内に担当者から連絡があります。注文のステータスが [注文を処理中です] に変わると、メールで確認の通知が届きます。 AWS 担当者から連絡があり、が AWS 必要とする追加情報を取得できます。

注文についてご質問がある場合は、 にお問い合わせください AWS Support。

注文を満たすために、 AWS はユーザー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、予定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 と Amazon EBS の容量が AWS アカウントから利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。

Outpost ラックでインスタンスを起動する

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。Linux に適用される詳細については、「Amazon EC2 ユーザーガイド」の「 でのローカル Amazon EBS スナップショット AWS Outposts」を参照してください。 Amazon EC2 Windows に適用される詳細については、「Amazon EC2 ユーザーガイド」の「 でのローカル Amazon EBS スナップショット AWS Outposts」を参照してください。 Amazon EC2

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、「Outpost を作成して Outpost 容量を注文する」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設定する
- 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 でインスタンスを起動する
- 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。使用できる VPC が既にある場合は、このステップをスキップします。

Outpost の VPC を作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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 VPCs の作成 を選択します。

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、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 で、IPv6 CIDR ブロック なし を選択します。
8. テナンシー で、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 が属する AWS リージョン内の任意の VPC に追加できます。これを行うと、VPC には Outpost が含まれます。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、「」に進みますステップ 5: Outpost でインスタンスを起動する。

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、オプションでサブネットに名前を付け、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、サブネットページで 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、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 (https://console.aws.amazon.com/vpc/) を開きます。
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 (https://console.aws.amazon.com/vpc/) を開きます。
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設定する

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有効にします。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、次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

コンソールを使用して AWS Outposts 、ローカルゲートウェイ (LGW) 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 LGW 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、LGW 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。
   - 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。

8. (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。
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 LGW ルートテーブルに関連付ける

VPCs を LGW ルートテーブルに関連付ける必要があります。デフォルトでは関連付けられていません。

VPC を LGW ルートテーブルに関連付けるには、次の手順に従います。

オプションとして、関連付けにタグを付けて、識別しやすくしたり、組織のニーズに応じて分類したりできます。

AWS Outposts console

VPC をカスタム LGW ルートテーブルに関連付けるには

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) タグを追加または削除します。

タグを追加するには、[新しいタグの追加] を選択して、次の操作を実行します。

- [キー] にはキー名を入力します。
- [値] にキー値を入力します。

タグを削除するには、タグのキーと値の右側にある [削除] を選択します。

7. [Associate VPC] を選択します。

AWS CLI

VPC をカスタム LGW ルートテーブルに関連付けるには

create-local-gateway-route-table-vpc-association コマンドを使用します。

例

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

出力

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

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 LGW 間のトラフィックを有効にします。

Outpost LGW ルートテーブルに関連付けられている VPC 内の Outpost サブネットには、ルートテーブルの Outpost Local Gateway ID の追加ターゲットタイプを設定できます。送信先アドレスが

172.16.100.0/24 のトラフィックを LGW 経由でカスタマーネットワークにルーティングする場合を考えてみましょう。これを行うには、Outpost サブネットルートテーブルを編集し、宛先ネットワークと LGW () のターゲットに次のルートを追加しますlgw-xxxx。

デスティネーション	ターゲット
172.16.100.0/24	lgw-id

Outpost サブネットルートテーブルのターゲット**lgw-id**として を持つルートエントリを追加するには：

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、ルートテーブル を選択し、 で作成したルートテーブルを選択しますステップ 2b: カスタムルートテーブルを作成する。
3. アクション を選択し、ルート を編集します。
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、カスタマー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. [変更の保存] をクリックします。

3d: カスタム LGW ルートテーブルを LGW VIF グループに関連付ける

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ます。

カスタム LGW ルートテーブルを LGW 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 [VIF グループ関連付け] タブを選択し、[VIF グループ関連付けの編集] を選択します。
6. VIF グループ設定 で、VIF グループ を関連付け、VIF グループを選択します。
7. [変更の保存] をクリックします。

3e: LGW 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とし、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。

デスティネーション	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ルートテーブルを選択し、アクション、ルートの編集 を選択します。
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. [ルートの保存] を選択します。

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

カスタマー所有の IP (CoIP) アドレスプールを使用する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ように で Outposts を設定した場合は、CoIP アドレスプールから Elastic IP アドレスを割り当て、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。CoIP の詳細については、「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 (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。

Amazon VPC console

インスタンスに CoIP アドレスを割り当てるには

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] を選択します。
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

インスタンスに CoIP アドレスを割り当てるには

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
```

以下は出力例です。

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

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、「AWS RAM ユーザーガイド」の「AWS 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 ネットワークデバイス (OND) からカスタマー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て、オンプレミスネットワークから Outposts へのトラフィックを送受信します。詳細については、「ローカルゲートウェイ BGP 接続」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、以下を確認してください。

- カスタマー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から ACTIVE 状態になります。

- オンプレミスから Outposts に向かうトラフィックについては、CND で Outposts からの BGP アドバタイズを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。したがって、ネットワークが Outposts とオンプレミスリソースの間で適切なルーティングをしていることを確認します。
- Outposts からオンプレミスネットワークに向かうトラフィックの場合、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。別の方法として、デフォルトルート (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。CNDs によってアドバタイズされるオンプレミスサブネットには、で設定した CIDR 範囲と同じか、含まれている CIDR 範囲が必要です3e: LGW ルートテーブルにルートエントリを追加する。

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 モードで設定された Outpost があり、2 つの Outposts 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 によって 2 つのカスタマー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 を持つ VPC 内の Outpost サブネット。
- CIDR ブロック 172.16.100.0/24 を持つオンプレミスネットワークのサブネット
- Outposts は、Outpost サブネット上のインスタンスのプライベート IP アドレス、例えば 10.0.3.0/24 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、 によってアドバタイズされるルートは次のとおりです。

- カスタマーデバイスへのローカルゲートウェイは 10.0.3.0/24 です。
- Outpost ローカルゲートウェイへのカスタマーデバイスは 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 のアウトバウンドトラフィックをカスタマー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の正しいルーティング設定がネットワークにあることを確認します。

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チェックするために必要な特定の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 「 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」を参照してください。

例: CoIP モードでの BGP アドバタイズ

ローカルゲートウェイ VLAN によって 2 つの Outposts ラックネットワークデバイスが 2 つのカスタマーローカルネットワークデバイスに接続されている Outpost があ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 を持つオンプレミスネットワークのサブネット
- 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、ルートは次の方法でアドバタイズされます。

- カスタマーデバイスへのローカルゲートウェイは 10.1.0.0/26 です。
- Outpost ローカルゲートウェイへのカスタマーデバイスは 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 のアウトバウンドトラフィックをカスタマー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の適切なルーティング設定がネットワークにあることを確認します。

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チェックするために必要な特定の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 「 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」を参照してください。

ステップ 5: Outpost でインスタンスを起動する

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

- 配置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。
- 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。グレー表示されているインスタンスは Outpost で使用できないことに注意してください。
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. 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」の以下のトピックを参照してください。

   - Linux – 新しいインスタンス起動ウィザードを使用してインスタンスを起動する
   - Windows – 新しいインスタンス起動ウィザードを使用してインスタンスを起動する

> **Note**
>
> Amazon EBS ボリュームを作成する場合は、gp2 ボリュームタイプを使用する必要があります。そうしないと、ウィザードは失敗します。

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 ping コマンドを実行します。

```
ping 10.0.3.128
```

以下は出力例です。

```
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 インスタンスへの接続の詳細については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスに接続する」を参照してください。 Amazon EC2 Windows インスタンスへの接続の詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。 Amazon EC2

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。Linux インスタンスへの接続の詳細については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスに接続する」を参照してください。 Amazon EC2 Windows インスタンスへの接続の詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。 Amazon EC2

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 アドレスを取得します。例: 10.0.0.5。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
```

AWS OutpostsAWS 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広域ネットワーク (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 と選択した AWS リージョン (またはホームリージョン) との間の必要な接続であり、Outposts の管理と AWS リージョンとの間のトラフィックの交換を可能にします。サービスリンクは、暗号化された VPN 接続のセットを活用して、ホームリージョンと通信します。

サービスリンク接続を設定するには、Outpost のプロビジョニング中にローカルネットワークデバイスとの物理、仮想 LAN (VLAN)、およびネットワークレイヤー接続サービスリンクを設定 AWS する必要があります。詳細については、「ラックのローカルネットワーク接続」および「Outposts ラックのサイト要件」を参照してください。

AWS リージョンへのワイドエリアネットワーク (WAN) 接続の場合、 AWS Outposts は AWS リージョンのパブリック接続を介してサービスリンク VPN 接続を確立できます。そのためには、Outposts が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。パブリック IP 範囲は、パブリックインターネットまたは AWS Direct Connect パブリック仮想インターフェイスを経由できます。現在の IP アドレス範囲については、「Amazon VPC ユーザーガイド」の「AWS IP アドレス範囲」を参照してください。 この接続を有効にするには、サービスリンクネットワークレイヤーパスで特定のルートまたはデフォルトルート (0.0.0.0/0) を設定します。詳細については、「サービスリンク BGP 接続」および「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」を参照してください。

または、Outpost のプライベート接続オプションを選択することもできます。詳細については、「VPC を使用したサービスリンクのプライベート接続」を参照してください。

サービスリンク接続が確立されると、Outpost は によって運用され、管理されます AWS。サービスリンクは以下のトラフィックに使用されます。

- Outpost と関連付けられた VPC 間のカスタマー VPCsトラフィック。

- リソース管理、リソースモニタリング、ファームウェア、ソフトウェア更新などの Outposts 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。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間の 1500 バイトの MTU をサポートする必要があります。サービスリンクを介した Outpost のインスタンスと AWS リージョンのインスタンス間の必要な MTU については、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最大送信単位 (MTU)Amazon EC2」を参照してください。

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、 では、 AWS リージョンへのサービスリンク接続に 500 Mbps (1 Gbps 以上が適しています) の冗長接続を使用する AWS ことをお勧めします。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。最低 500 Mbps のサービスリンク接続により、Amazon EC2 インスタンスの起動、Amazon EBS ボリュームのアタッチ、Amazon EKS、Amazon EMR、メトリクス CloudWatchなどの AWS のサービスへのアクセスが可能になります。

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

ニーズに必要なサービスリンク帯域幅に関するカスタムレコメンデーションを受け取るには、 AWS 販売担当者または APN パートナーにお問い合わせください。

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、設定によって Amazon VPC が AWS リージョンから Outpost に拡張されています。AWS 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 AWS 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。

ファイアウォールを使用してサービスリンク VLAN からの接続を制限すると、すべてのインバウンド接続をブロックできます。次の表に従って、 AWS リージョンから Outpost へのアウトバウンド接続を許可する必要があります。ファイアウォールがステートフルであれば、許可されている Outpost からのアウトバウンド接続、つまり Outpost から開始された接続は、インバウンドに戻ることも許可される必要があります。

[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ルート
TCP	1025-65535	AWS Outposts サービスリンク /26	443	AWS Outposts リージョンのパブリックルート

> **Note**
>
> Outpost 内のインスタンスは、サービスリンクを使用して別の Outposts 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、「 の耐障害性 AWS Outposts」を参照してください。

VPC を使用したサービスリンクのプライベート接続

Outpost を作成する際に、コンソールでプライベート接続オプションを選択できます。これを行うと、指定した VPC とサブネットを使用して Outpost をインストールした後に、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。

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、「の Identity and Access Management (IAM) AWS Outposts」および「AWS Outpostsのサービスにリンクされたロールの使用」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、10.2.0.0/16 を使用することができます。
- 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。接続が VPC AWS Direct Connect とは異なる AWS アカウントにある場合は、「 ユーザーガイド」の「アカウント間で仮想プライベートゲートウェイを関連付ける」を参照してください。 AWS Direct Connect
- 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、 を使用できます。詳細については、「AWS Direct Connect ユーザーガイド」の「AWS Direct Connect 仮想インターフェイス」と「AWS Direct Connect ゲートウェイの操作」を参照してください。

AWS Outposts コンソールで Outpost を作成する際に、プライベート接続オプションを選択できます。手順については、「Outpost を作成して Outpost 容量を注文する」を参照してください。

> **Note**
>
> Outpost のステータスが保留中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 Outposts を選択し、Outpost 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、 によって自動的にサービスにリンクされたロールがアカウントに AWS Outposts 作成され、ユーザーに代わって次のタスクを完了できるようになります。

- 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。

サービスにリンクされたロールの詳細については、「AWS Outpostsのサービスにリンクされたロールの使用」を参照してください。

> **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。

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場合は、可用性と耐障害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、「AWS 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。

Outposts とサイト

の Outposts とサイトを管理します AWS Outposts。

Outposts とサイトにタグを付けて、識別しやすくしたり、組織のニーズに応じて分類したりできます。タグ付けの詳細については、「 AWS 全般のリファレンス ガイド」の「 AWS リソースのタグ付け」を参照してください。

トピック

- Outposts の管理
- Outpost サイトを管理する

Outposts の管理

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ます。このセクションを使用して、Outposts 作成と管理 (名前の変更、詳細やタグの追加や表示など) を行います。

Outpost 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 [Outposts] を選択します。
4. [Outpost の作成] を選択します。
5. この Outpost のハードウェアタイプを選択します。
6. Outpost の名前と説明を入力します。
7. Outpost のアベイラビリティーゾーンを選択します。
8. (オプション) プライベート接続オプションを選択します。VPC とサブネット で、Outpost と同じ AWS アカウントとアベイラビリティーゾーンの VPC とサブネットを選択します。

   > **Note**
   >
   > Outpost のプライベート接続を元に戻す必要がある場合は、 AWS エンタープライズサポートに連絡する必要があります。

9. [サイト ID] から、次のいずれかを実行します。

- 既存のサイトを選択するには、そのサイトを選択します。
- 新しいサイトを作成するには、[サイトの作成] を選択し、[次へ] をクリックして、新しいウィンドウにサイトに関する情報を入力します。

  サイトを作成したら、このウィンドウに戻ってサイトを選択します。新しいサイトを表示するには、サイトリストを更新する必要がある場合があります。データを更新するには、更新アイコン () をクリックします。

  詳細については、「the section called “サイト”」を参照してください。

10. [Outpost の作成] を選択します。

> **Tip**
>
> 新しい Outpost にキャパシティを追加するには、注文する必要があります。

以下の手順で Outpost の名前と説明を編集します。

Outpost の名前と説明を編集するには

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 [Outposts] を選択します。
4. Outpost を選択し、[アクション]、[Outpost の編集] の順に選択します。
5. 名前と説明を変更する

   [名前] には、名前を入力します。

   [説明] に説明を入力します。
6. [変更の保存] をクリックします。

Outpost の詳細を表示するには、次のステップを実行します。

Outpost の詳細を表示するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 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 [Outposts] を選択します。
4. Outpost を選択し、[アクション、詳細の表示] を選択します。

を使用して AWS CLI Outpost の詳細を表示することもできます。

を使用して Outpost の詳細を表示するには AWS CLI

- get-outpost AWS CLI コマンドを使用します。

以下の手順で Outpost のタグを管理します。

Outpost のタグを管理するには

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 [Outposts] を選択します。
4. Outpost を選択し、[アクション]、[タグの管理] の順に選択します。
5. タグを追加または削除します。

   タグを追加するには、[新しいタグの追加] を選択して、次の操作を実行します。

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

   タグを削除するには、タグのキーと値の右側にある [削除] を選択します。
6. [変更の保存] をクリックします。

Outpost サイトを管理する

AWS が Outpost をインストールするカスタマーマネージドの物理的な建物。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。詳細については、「Outposts ラックの要件」を参照してください。

Outpost サイトを作成するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 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、[サイト] を選択します。
4. [サイトを作成] を選択します。
5. サイトでサポートされているハードウェアタイプを選択します。
6. サイトの名前、説明、および営業住所を入力します。サイトでラックをサポートすることを選択した場合は、以下の情報を入力します。

   - 最大重量 — このサイトがサポートできる最大ラック重量を指定します。
   - 消費電力 — ラックのハードウェア配置位置で利用可能な消費電力を kVA 単位で指定します。
   - 電源オプション — ハードウェアに提供できる電源オプションを指定します。
   - 電源コネクタ – ハードウェアへの接続用に が提供する AWS 予定の電源コネクタを指定します。
   - 給電ドロップ – 給電がラックの上か下かを指定します。
   - 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必要があるアップリンク速度を指定します。
   - アップリンクの数 – ラックをネットワークに接続するために使用される Outpost ネットワークデバイスごとにアップリンクの数を指定します。
   - ファイバータイプ – Outpost をネットワークに接続するために使用されるファイバーのタイプを指定します。
   - 光規格 — Outpost をネットワークに接続するために使用される光規格のタイプを指定します。
   - メモ — サイトに関するメモを指定します。
7. 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。
8. [サイトを作成] を選択します。

Outpost サイトを編集するには、次の手順に従います。

サイトを編集するには

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、[サイト] を選択します。
4. サイトを選択し、[アクション]、[サイトの編集] の順に選択します。
5. 名前、説明、営業住所、サイトの詳細を変更できます。

   営業住所を変更した場合、その変更は既存の注文に反映されないので、ご注意ください。
6. [変更の保存] をクリックします。

以下の手順で Outpost サイトの詳細を表示します。

サイトの詳細を表示するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 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、[サイト] を選択します。
4. サイトを選択し、[アクション]、[詳細の表示] の順に選択します。

以下の手順で Outpost サイトのタグを管理します。

サイトのタグを管理するには

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、[サイト] を選択します。
4. サイトを選択し、[アクション]、[タグの管理] の順に選択します。
5. タグを追加または削除します。

   タグを追加するには、[新しいタグの追加] を選択して、次の操作を実行します。

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

   タグを削除するには、タグのキーと値の右側にある [削除] を選択します。
6. [変更の保存] をクリックします。

ローカルゲートウェイ

ローカルゲートウェイは Outposts アーキテクチャのコアコンポーネントです。ローカルゲートウェイは、Outpost サブネットとオンプレミスネットワーク間の接続を可能にします。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 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 OutpostsAWS 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

各 Outpost 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、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ルートテーブルの作成に使用します。詳細については、「the section called “ローカルゲートウェイルートテーブル”」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) – 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 グループの関連付け – 作成した 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。詳細については、「the section called “VIF グループの関連付け”」を参照してください。
- VPC 関連付け — VPC およびローカルゲートウェイルートテーブルとの VPC 関連付けの作成に使用します。Outpost にあるサブネットに関連付けられた VPC ルートテーブルは、ローカルゲート

ウェイをルートターゲットとして使用できます。詳細については、「the section called “VPC の関連付け”」を参照してください。

が Outpost ラックを AWS プロビジョニングすると、いくつか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 グループとローカルゲートウェイルートテーブルの関連付け

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 “ローカルゲートウェイルートテーブル”」を参照してください。

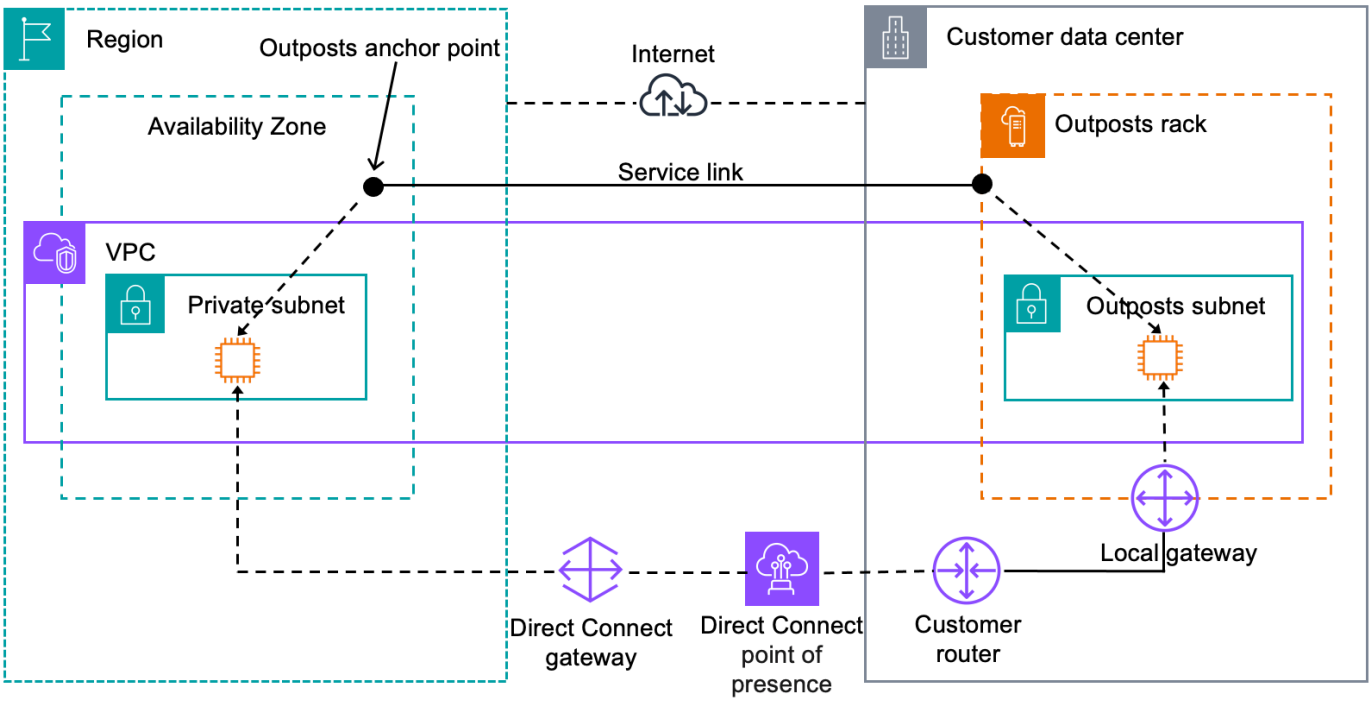
ローカルゲートウェイ経由の接続

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 経由で 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 AWS 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 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ルートを含めることができます。ローカルゲートウェイは、低遅延ルーティングのために、このトラフィックをオンプレミスネットワークにルーティングします。

デフォルトでは、Outposts は Outpost 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。これは AWS Outposts用ダイレクト VPC ルーティング (またはダイレクト VPC ルーティング) として知られています。ただし、カスタマー所有 IP アドレスプール (CoIP) のアドレス範囲を指定し、ネットワーク上のインスタンスにそれらのアドレスを使用してオンプレミスネットワークと通信させることができます。ダイレクト VPC ルーティングと CoIP は相互に排他的なオプションであり、ルーティングの仕組みは選択によって異なります。

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 Outpost ラックのサブネットに属するプライベート IP アドレスのみを対象としています。このタイプのルーティングは 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と呼ばれる) では、それらのプライベート IP アドレスにオンプレミスネットワークからアクセスすることはできません。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
- 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

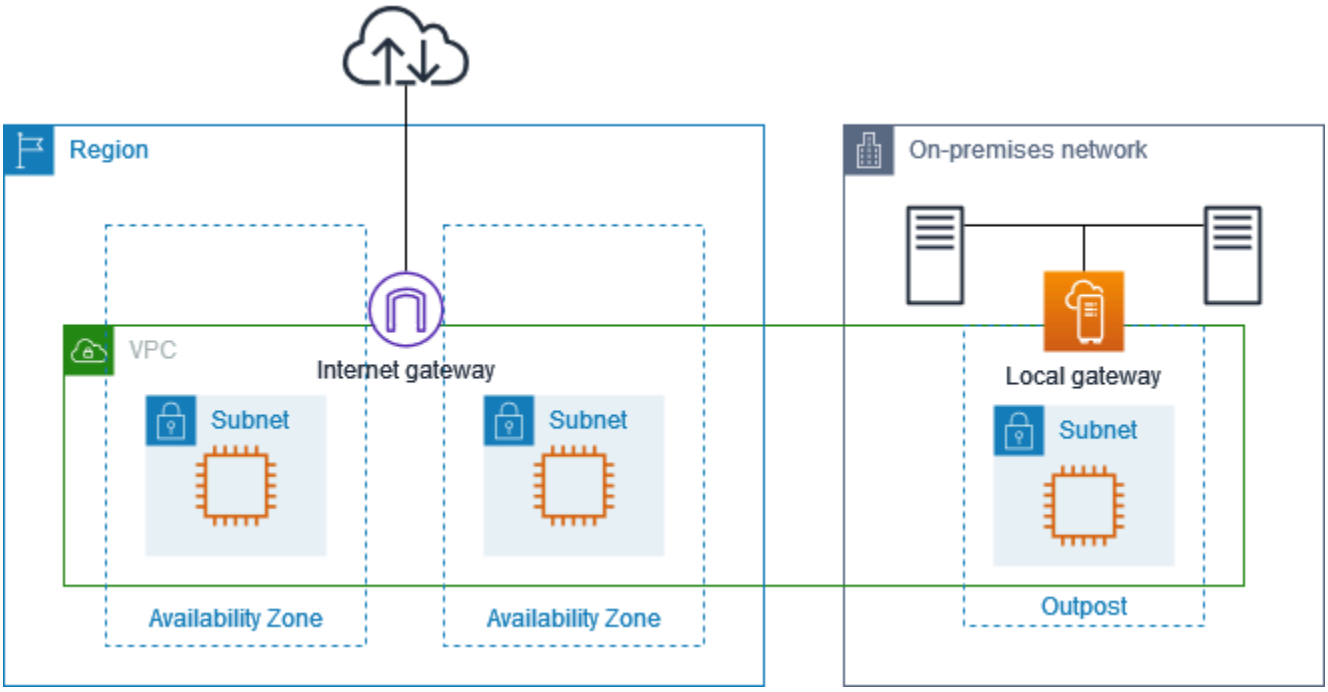
Outpost サブネットのインスタンスは、VPC にアタッチされたインターネットゲートウェイを介してインターネットにアクセスできます。

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。
- 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。

デスティネーション	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。

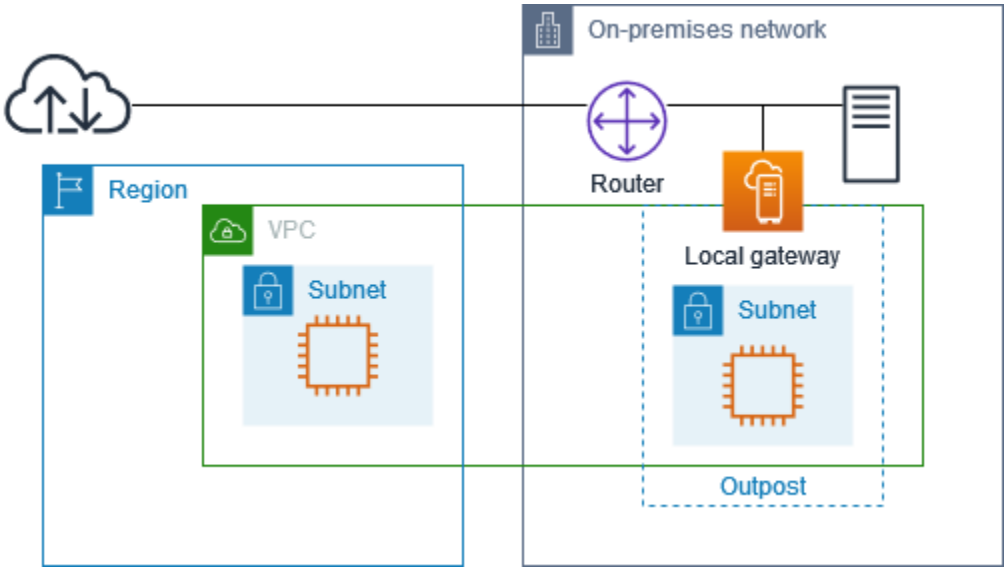
以下の設定を考慮します。

- 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。

デスティネーション	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。	

デスティネーション	ターゲット	コメント	
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、「the section called “3f: (オプション) インスタンスに顧客所有の IP アドレスを割り当てる”」を参照してください。

カスタマー所有 IP アドレスプールには以下の要件が適用されます。

- ネットワーク内でアドレスをルーティングできる必要があります。
- CIDR ブロックは /26 以上でなければなりません。

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。

オプションで、 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。詳しくは、AWS RAM ユーザーガイドの「AWS リソースを共有する」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

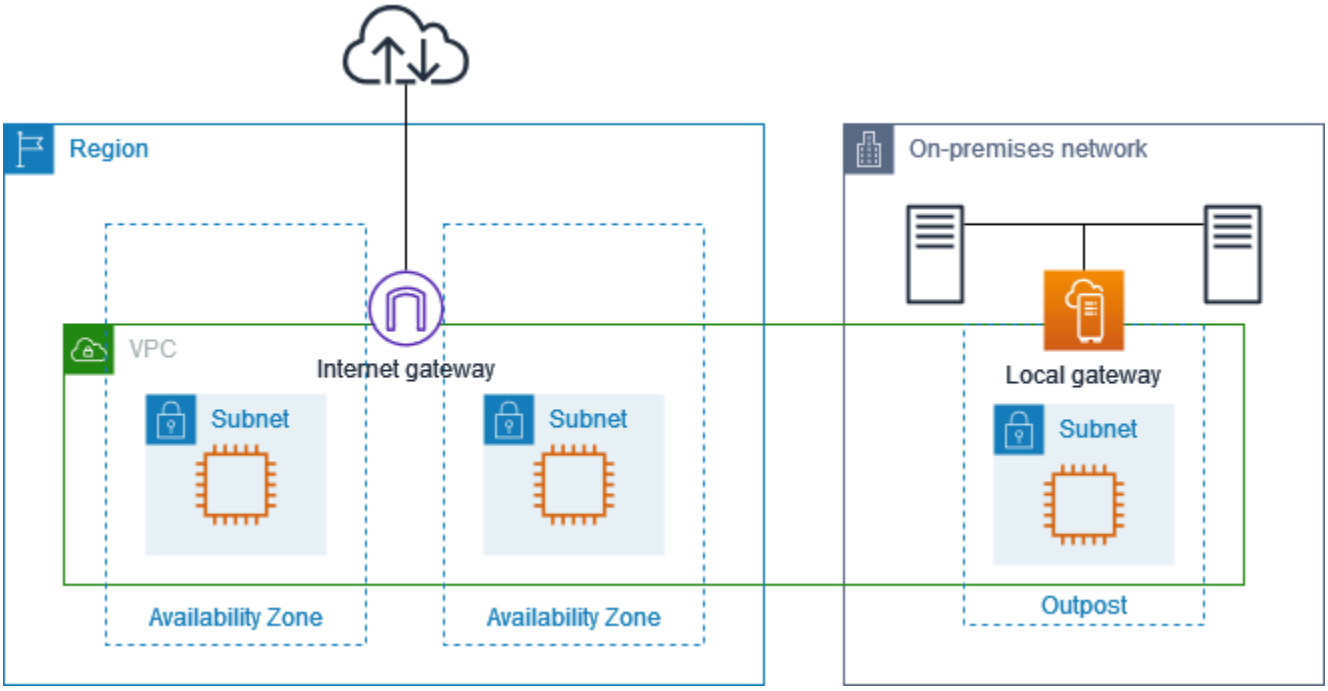
例: VPC 経由のインターネット接続

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。

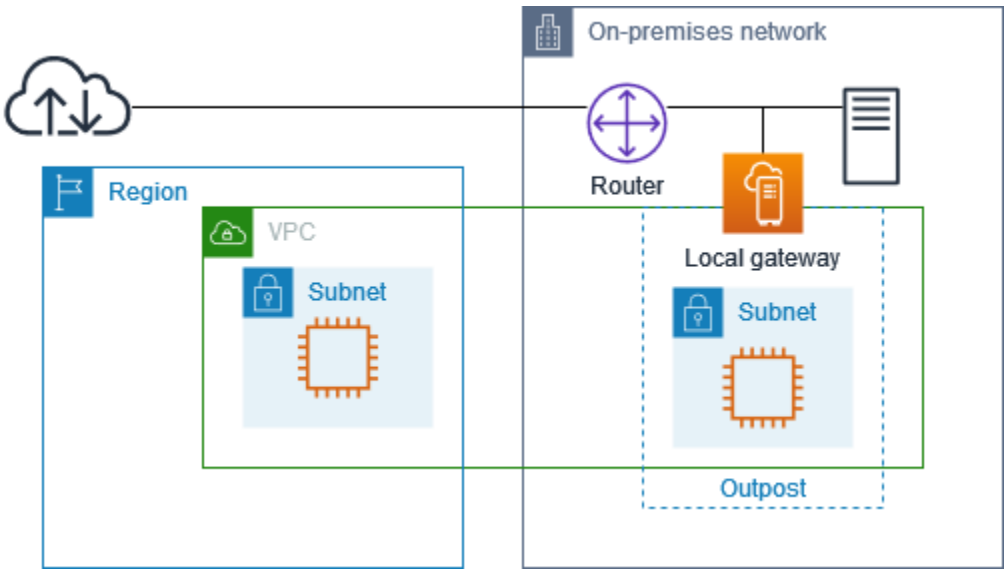
デスティネーション	ターゲット	コメント
VPC CIDR	ローカル	VPC 内のサブネット間の接続を提供します。
0.0.0.0	*internet-gateway-id*	パブリックインターネット宛てのトラフィックをインターネットゲートウェイに送信します。
############ CIDR	*local-gateway-id*	オンプレミスネットワーク宛てのトラフィックを、ローカルゲートウェイに送信します。

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。

デスティネーション	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。

ローカルゲートウェイルートテーブルを操作する

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ルートテーブルに関する以下の情報を考慮してください。

- VIF グループとローカルゲートウェイルートテーブルには関係 one-to-oneが必要です。
- 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ており、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。
- 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。
- ローカルゲートウェイルートテーブルには、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 (ダイレクト VPC ルーティング) と通信するモードと、カスタマー所有

IP アドレスプール (CoIP) を使用するモードがあります。ダイレクト VPC ルーティングと CoIP は相互に排他的なオプションであり、ルーティングの仕組みは選択によって異なります。詳細については、「???」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。

タスク

- ローカルゲートウェイのルートテーブルの詳細を表示する
- カスタムローカルゲートウェイルートテーブルの作成
- ローカルゲートウェイのルートテーブルルートの管理
- ローカルゲートウェイルートテーブルのタグの管理
- 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
- CoIP プールの管理
- VIF グループの関連付け
- VPC の関連付け

ローカルゲートウェイのルートテーブルの詳細を表示する

AWS CLIコンソールまたはを使用して、ローカルゲートウェイルートテーブルの詳細を表示できます。

AWS Outposts console

ローカルゲートウェイのルートテーブルの詳細を表示するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 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を選択し、[アクション、詳細の表示] の順に選択します。

AWS CLI

ローカルゲートウェイのルートテーブルの詳細を表示するには

describe-local-gateway-route-tables AWS CLI コマンドを使用します。

例

```
aws ec2 describe-local-gateway-route-tables --region us-west-2
```

出力

```
{
    "LocalGatewayRouteTables": [
        {
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7deEXAMPLE",
            "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
            "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-0dc11b66edEXAMPLE",
            "State": "available",
            "Tags": []
        }
    ]
}
```

> **Note**
>
> 表示しているデフォルトのローカルゲートウェイルートテーブルが CoIP モードを使用している場合、ローカルゲートウェイルートテーブルは、各 VIF へのデフォルトルートと、プール CoIP プール内の関連するカスタマー所有IPアドレスへの伝達ルートで構成されます。

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。
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のルートテーブルルートの管理

Outpost 上のローカルゲートウェイルート テーブルと Elastic Network Interface 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Elastic Network Interface 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 Elastic Network Interface 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] の状態になります。

ローカルゲートウェイには、以下の要件と制約事項が適用されます。

- ターゲットの Elastic Network Interface 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 Elastic Network Interface ルートは 100 個を超えてはなりません。
- 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 ENI 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 ENI 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。
- VPCE エンドポイントやインターフェースなどのマネージドインターフェースには、ローカルゲートウェイを経由してオンプレミスからアクセスすることはできません。これらには Outpost 内のインスタンスからのみアクセスできます。

以下のNAT 考慮事項に注意してください。

- ローカルゲートウェイは、Elastic Network Interface 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 Elastic Network Interface 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基本」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。

AWS Outposts console

ローカルゲートウェイルートテーブルのルートを編集するには

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のルートテーブルを選択してから [アクション、ルートの編集] を選択します。
5. ルートを追加するには、[ルートの追加] を選択します。[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. 既存のルートを変更するには、[送信先] で、宛先 CIDR ブロックまたは 1 つの IP アドレスを置き換えます。[ターゲット] で、ターゲットを選択します。
7. [ルートの保存] を選択します。

AWS CLI

ローカルゲートウェイルートテーブルのルートを作成するには

- create-local-gateway-route AWS CLI コマンドを使用します。

例

```
aws ec2 create-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-03e612f0a1EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

出力

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
```

```
        "NetworkInterfaceId": "eni-03e612f0a1EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

ローカルゲートウェイルートテーブルのルートを変更するには

ターゲットの Elastic Network Interface は既存のルートで変更できます。変更操作を使用するには、指定した宛先 CIDR ブロックを持つルートがルートテーブルにすでに存在している必要があります。

- modify-local-gateway-route AWS CLI コマンドを使用します。

例

```
aws ec2 modify-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-12a345b6c7EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

出力

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-12a345b6c7EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

ローカルゲートウェイルートテーブルのタグの管理

ローカルゲートウェイルート テーブルにタグを付けると、組織のニーズに応じてルートテーブルを識別したり、分類したりすることができます。

ローカルゲートウェイルートテーブルのタグを管理するには

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を選択してから [アクション、タグの管理] を選択します。
5. タグを追加または削除します。

   タグを追加するには、[新しいタグの追加] を選択して、次の操作を実行します。

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

   タグを削除するには、タグのキーと値の右側にある [削除] を選択します。
6. [変更の保存] をクリックします。

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 にいることを確認します AWS リージョン。

   リージョンを変更するには、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が VIF グループに関連付けられているかどうかを確認します。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の編集 を選択します。
   d. VIF グループの関連付けチェックボックスをオフにします。
   e. [変更の保存] をクリックします。
5. ローカルゲートウェイルートテーブルの削除 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 プールの管理

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。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には、「ローカルゲートウェイルートテーブルモードの切り替え」を参照してください。

以下の手順に従って CoIP プールを作成します。

CoIP プールを作成するには

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. [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 ブロックを追加または削除します

   [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。

   [CIDR ブロックを削除] CIDR ブロックの右側にある [削除] を選択します。
9. [CoIP プールの作成] を選択します。

CoIP プールを編集するには、以下の手順に従います。

CoIP プールを編集するには

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. [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、次に CoIP プールを選択します。
6. [アクション、CoIP プールの編集] を選択します。
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 ブロックを追加または削除します

   [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。

   [CIDR ブロックを削除] CIDR ブロックの右側にある [削除] を選択します。
9. [変更の保存] をクリックします。

次の手順に従って、タグを管理したり、CoIP プールにネームタグを追加したりします。

CoIP プールのタグを管理するには

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. [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、次に CoIP プールを選択します。
6. [アクション、タグの管理] を選択します。
7. タグを追加または削除します。

   タグを追加するには、[新しいタグの追加] を選択して、次の操作を実行します。

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

   タグを削除するには、タグのキーと値の右側にある [削除] を選択します。
8. [変更の保存] をクリックします。

次の手順に従って、CoIP プールを削除します。

CoIP プールを削除するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 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、次に CoIP プールを選択します。
6. [アクション、CoIP プールの削除] を選択します。
7. 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。

VIF グループの関連付け

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。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は変更できます。VIF グループとローカルゲートウェイルートテーブルの関連付けを解除すると、ルートテーブルからすべてのルートが削除され、ネットワークトラフィックが中断されます。

VIF グループの関連付けを変更するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 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 [VIF グループ関連付け] タブを選択し、[VIF グループ関連付けの編集] を選択します。
6. [VIF グループの設定] には、次のいずれかのアクションを実行します。
   - 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るには、[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。
   - VIF グループとローカルゲートウェイルートテーブルの関連付けを解除するには、[VIF グループの関連付け] をクリアします。

   > **Important**
   >
   > VIF グループとローカルゲートウェイルートテーブルの関連付けを解除すると、すべてのルートが自動的に削除され、ネットワークトラフィックが中断されます。
7. [変更の保存] をクリックします。

VPC の関連付け

VPC をローカルゲートウェイルートテーブルに関連付ける必要があります。デフォルトでは関連付けられていません。

VPC の関連付けを作成する

VPC をローカルゲートウェイルートテーブルに関連付けるには、次の手順を実行します。

オプションとして、関連付けにタグを付けて、識別しやすくしたり、組織のニーズに応じて分類したりできます。

AWS Outposts console

VPC 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) タグを追加または削除します。

   タグを追加するには、[新しいタグの追加] を選択して、次の操作を実行します。

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

   タグを削除するには、タグのキーと値の右側にある [削除] を選択します。
7. [Associate VPC] を選択します。

AWS CLI

VPC を関連付けるには

create-local-gateway-route-table-vpc-association コマンドを使用します。

例

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

出力

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

VPC の関連付けを削除する

VPC とローカルゲートウェイルートテーブルの関連付けを解除するには、次の手順を実行します。

AWS Outposts console

VPC の関連付けを解除するには

1. https://console.aws.amazon.com/outposts/ で AWS Outposts コンソールを開きます。
2. 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てから、[アクション]、[詳細を表示] の順に選択します。
5. [VPC の関連付け] で、関連付けを解除する VPC を選択し、[関連付け解除] を選択します。
6. [Disassociate] (関連付け解除) を選択します。

AWS CLI

VPC の関連付けを解除するには

delete-local-route-route-table-vpc-association コマンドを使用します。

例

```
aws ec2 delete-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

出力

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

ラックのローカルネットワーク接続

Outpost 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 のレイヤー 3 point-to-point 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

Outpost 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。

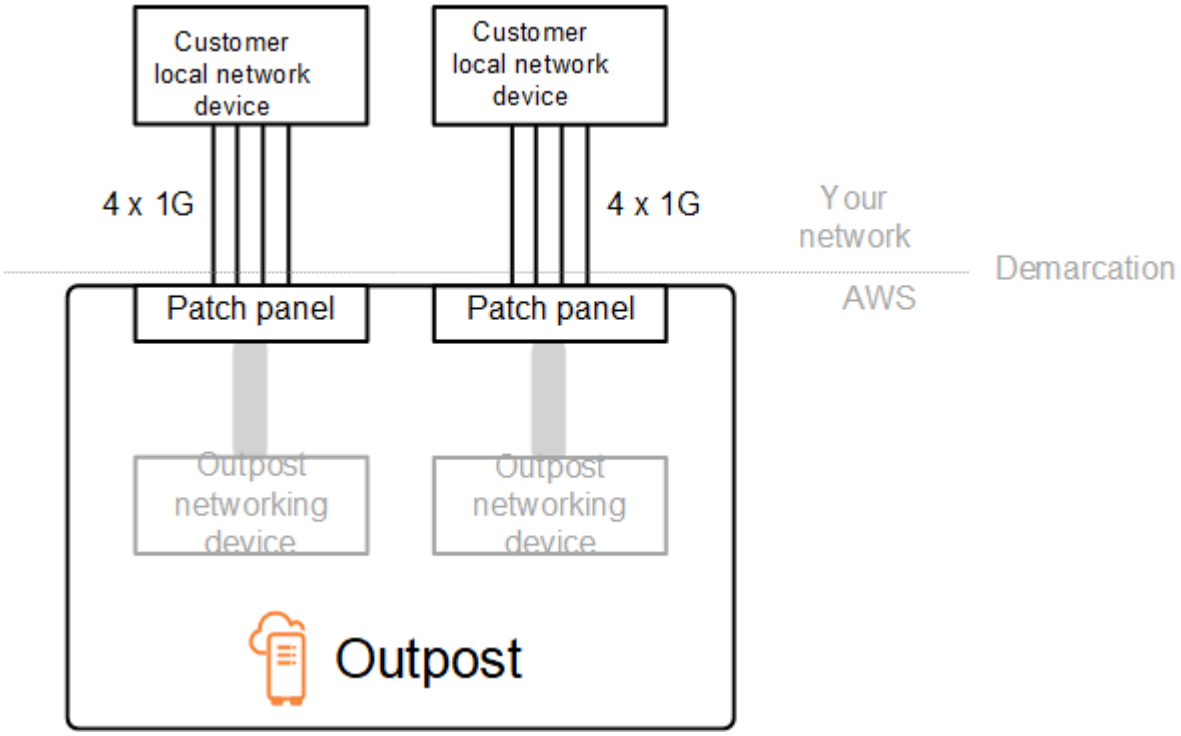
Outpost には、これらの Outpost ネットワークデバイスとローカルネットワークデバイスとの間に最低 2 つの物理リンクが必要です。Outpost は Outpost ネットワークデバイスごとに以下のアップリンク速度とアップリンク数をサポートします。

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。

Outpost ラックは、Lucent コネクタ (LC) を備え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 を備えた MMF OM4 をサポートできます。 は、ラックの位置で提供するファイバーと互換性のある光学系 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

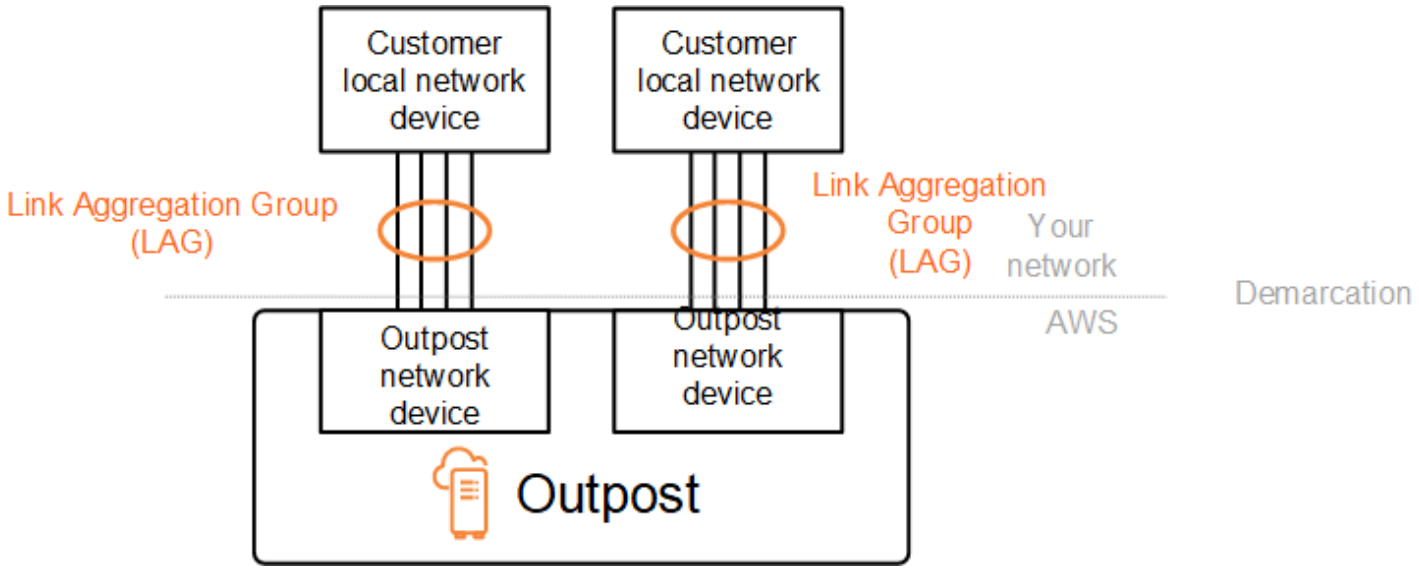
AWS Outposts は、リンク集約制御プロトコル (LACP) を使用して、各 Outpost ネットワークデバイスから各ローカルネットワークデバイスへの 1 つのリンク集約グループ (LAG) 接続を 2 つ確立します。各 Outpost ネットワークデバイスからのリンクは 1 つのイーサネット LAG に集約され、1 つのネットワーク接続を表します。これらの LAG は標準の高速タイマで LACP を使用します。低速タイマを使用するように LAG を設定することはできません。

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

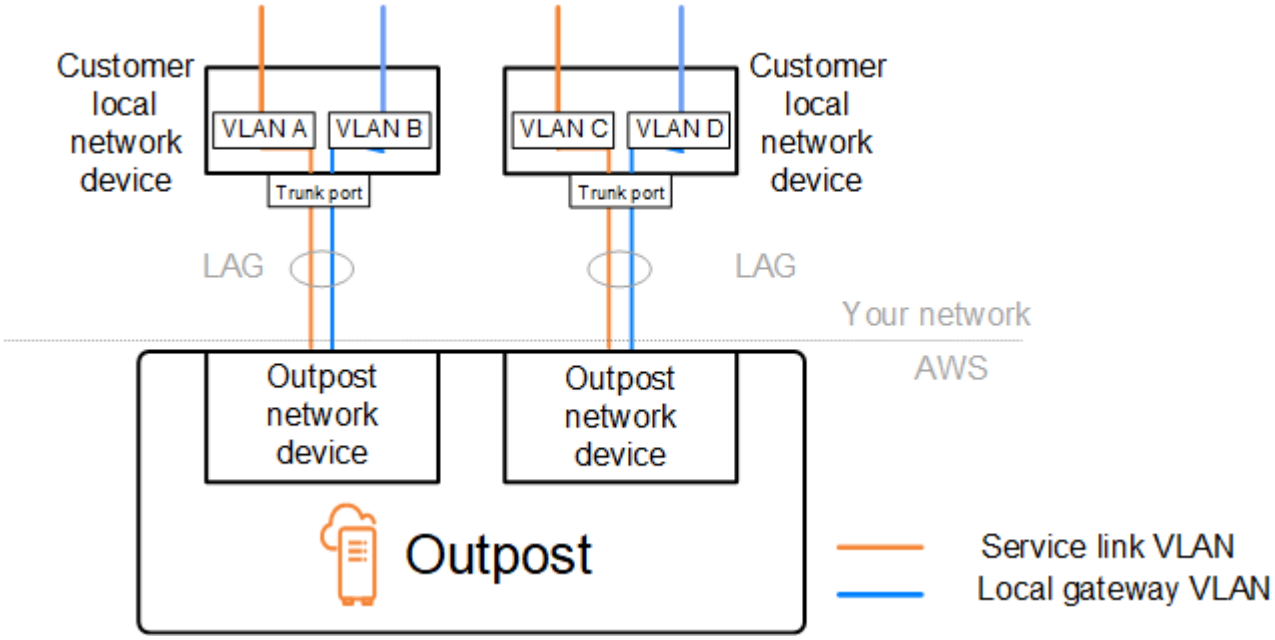
Outpost ネットワークデバイスとローカルネットワークデバイス間の各 LAG は IEEE 802.1q イーサネットトランクとして設定する必要があります。これにより、複数の VLAN を使用してデータパス間のネットワークを分離できます。

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の次の VLANs 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 リージョンへの接続 AWS」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 を活用して、インスタンスにオンプレミスネットワークへの接続を提供します。これには、ネットワークを介したインターネットアクセスが含まれる場合があります。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。

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あります。 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、その行の 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

ネットワークレイヤーの接続を確立するため、各 Outpost ネットワークデバイスは、各 VLAN の IP アドレスを含む仮想インターフェイス (VIFsで設定されます。これらの VIFs、 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 point-to-point 接続を表すには、/30 または /31 CIDR を持つ専用サブネットを使用します。
- ローカルネットワークデバイス間で VLANsをブリッジしないでください。

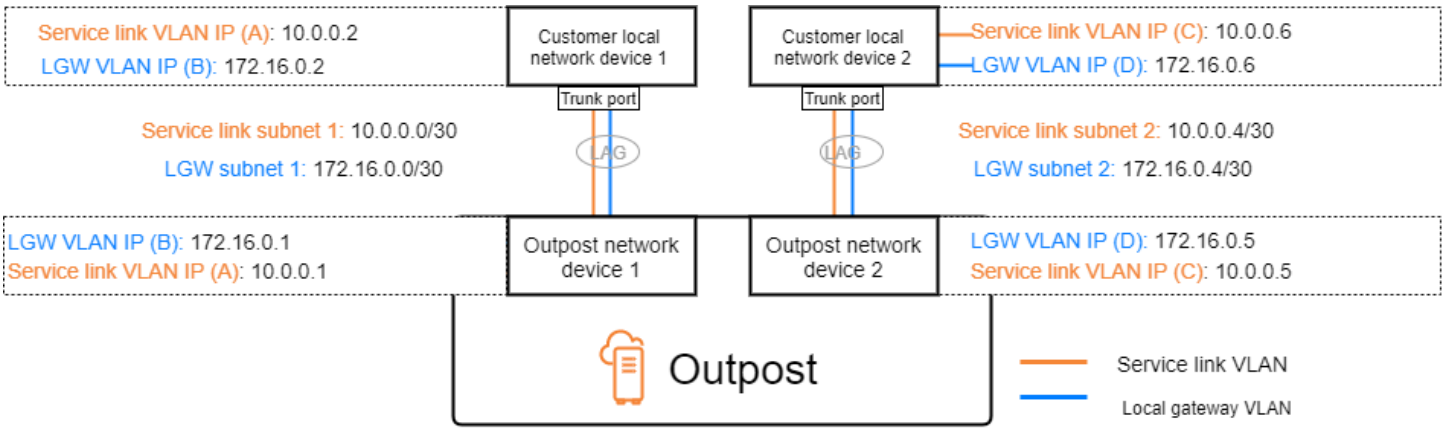
ネットワークレイヤーの接続には、次の 2 つのパスを確立する必要があります。

- サービスリンクパス - このパスを確立するには、ネットワークデバイス上の AWS Outposts 各サービスリンク VLAN に /30 または /31 の範囲の VLAN サブネットと IP アドレスを指定します。このパスには、サービスリンク仮想インターフェイス (VIFs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、サービスリンク接続を行います。詳細については、「 AWS Outposts リージョンへの接続 AWS」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、ネットワークデバイス上の AWS Outposts ローカルゲートウェイ VLAN の IP アドレスを指定します。ローカルゲートウェイ VIFs は、このパスで使用され、ローカルリソース接続のために 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。

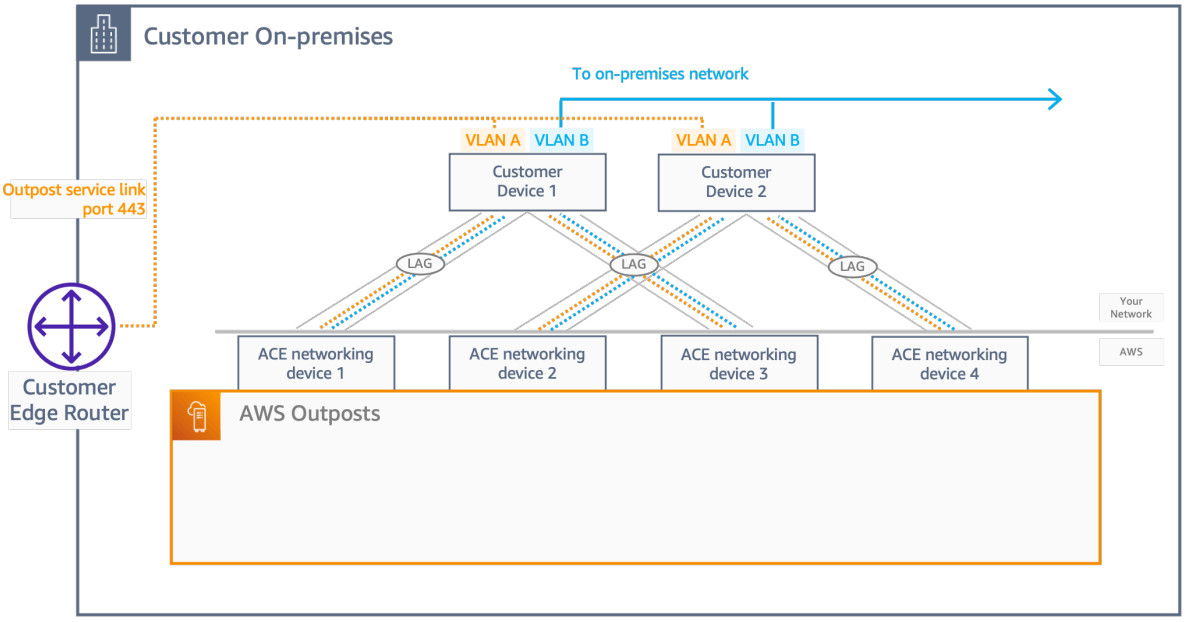
集約、コア、エッジ (ACE) ラックは、マルチラック Outpost デプロイのネットワーク集約ポイントとして機能します。コンピュートラックが 5 台以上ある場合は、ACE ラックを使用する必要があります。コンピュートラックが 5 台未満で、今後 5 台以上に拡張する予定がある場合は、できるだけ早く ACE ラックを設置することをお勧めします。

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の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、これらは Outpost ラックへの接続を提供する ACE ラックに接続されます。このトポロジでは、 AWS 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を所有します。

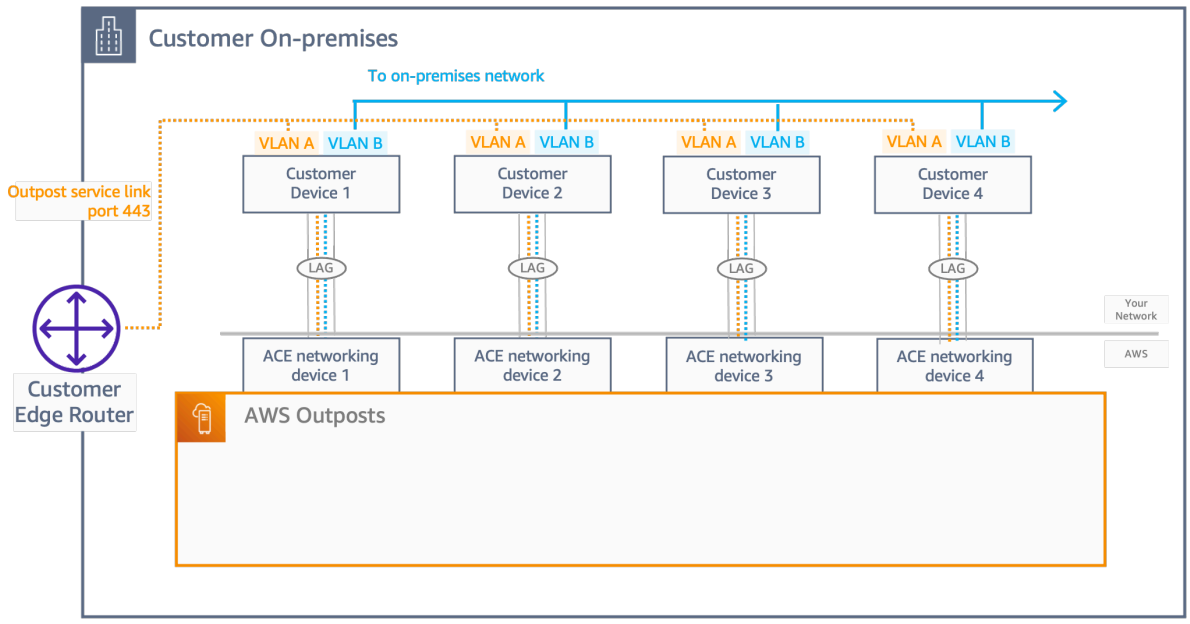
ACE ラックには 4 つのネットワークデバイスが含まれており、お客様のオンプレミスネットワーク内の 2 つのアップストリームカスタマーデバイス、または 4 つのアップストリームカスタマーデバイスに接続して回復性を最大限に高めることができます。

次の図は、2 つのネットワークトポロジを示しています。

次の図は、2 つのアップストリームカスタマーデバイスに接続された ACE ラックの 4 つの ACE ネットワークデバイスを示しています。



次の図は、4 つのアップストリームカスタマーデバイスに接続された ACE ラックの 4 つの ACE ネットワークデバイスを示しています。



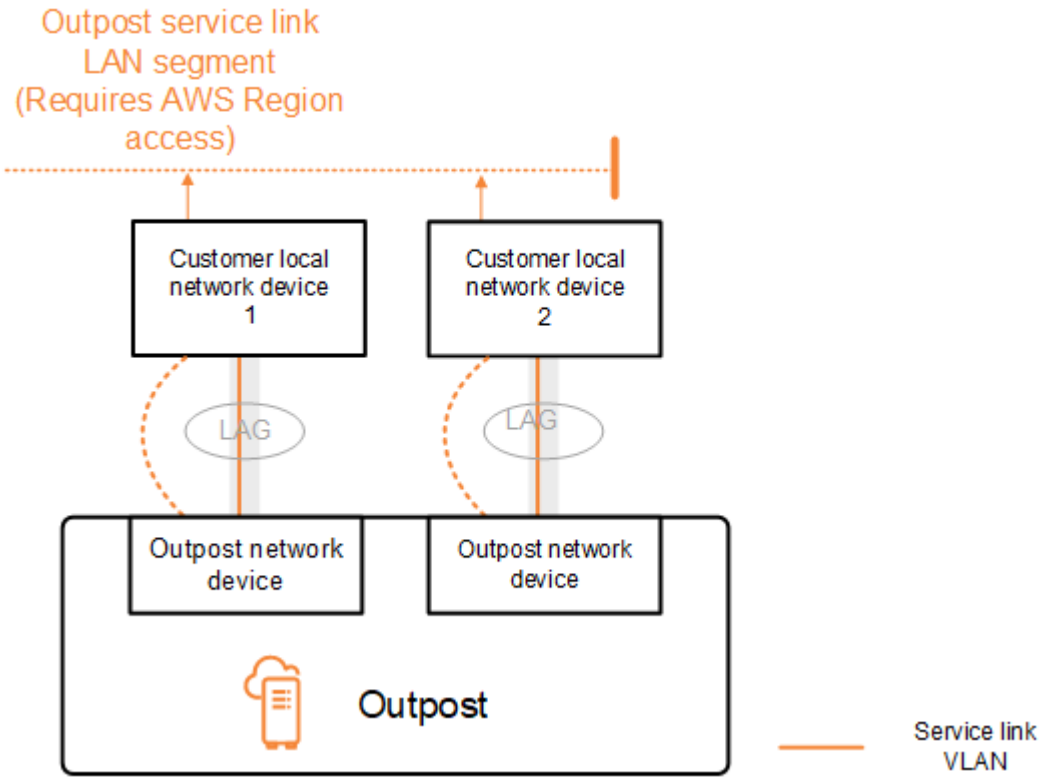
サービスリンク (BGP 接続)

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、 point-to-point VLAN に提供された /30 または /31 IP アドレスの間で確立されます。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 AS 番号 (ASN) と、カスタマーのローカルネットワークデバイス用に選択した ASN が使用されます。 AWS は、インストールプロセスの一部として属性を提供します。

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 からリージョンへの接続に使用されます AWS 。

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、ローカルゲートウェイに接続するために、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外部 BGP ピアリングを確立します。外部 BGP セッションを確立するために、ユーザーが割り当てるプライベート AS 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。

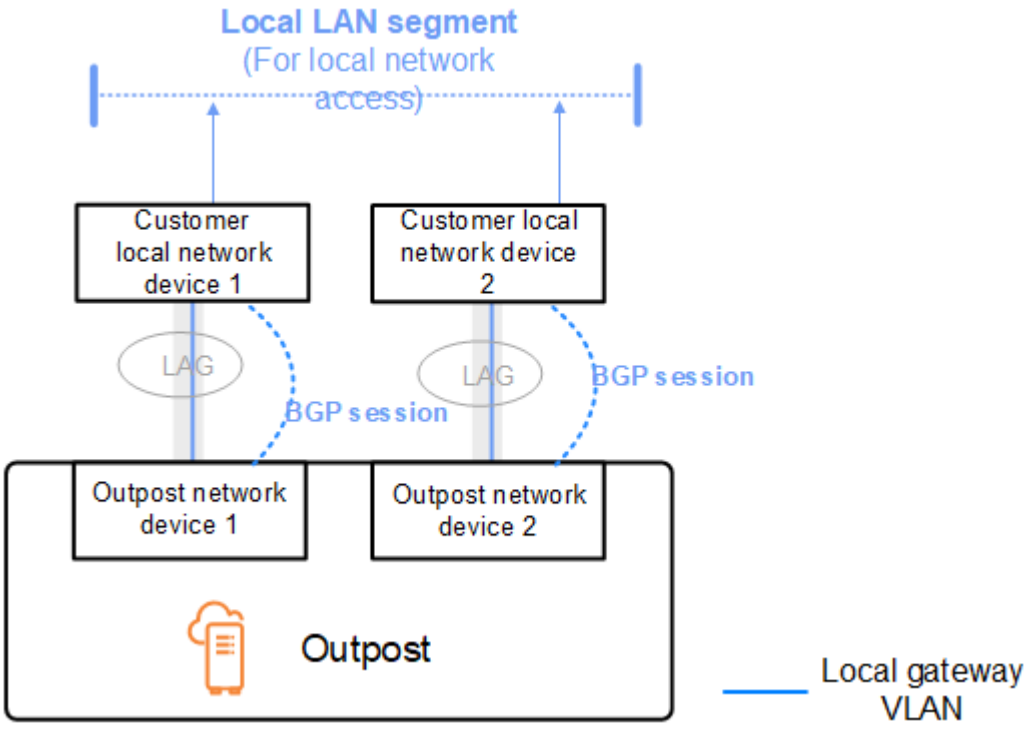
Outpost は、各 Outpost ネットワークデバイスと接続されているカスタマーのローカルネットワークデバイスとの間で、ローカルゲートウェイ VLAN 上で外部 BGP ピアリングセッションを確立します。ピアリングセッションは、ネットワーク接続の設定時に指定した /30 または /31 IPs の間で確立

され、Outpost ネットワークデバイスとお客様のローカルネットワークデバイス間の point-to-point 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、カスタマー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 を提供します。

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。

- AWS 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 アドレスを使用して、オンプレミス ネットワークとの通信を簡単にします。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。

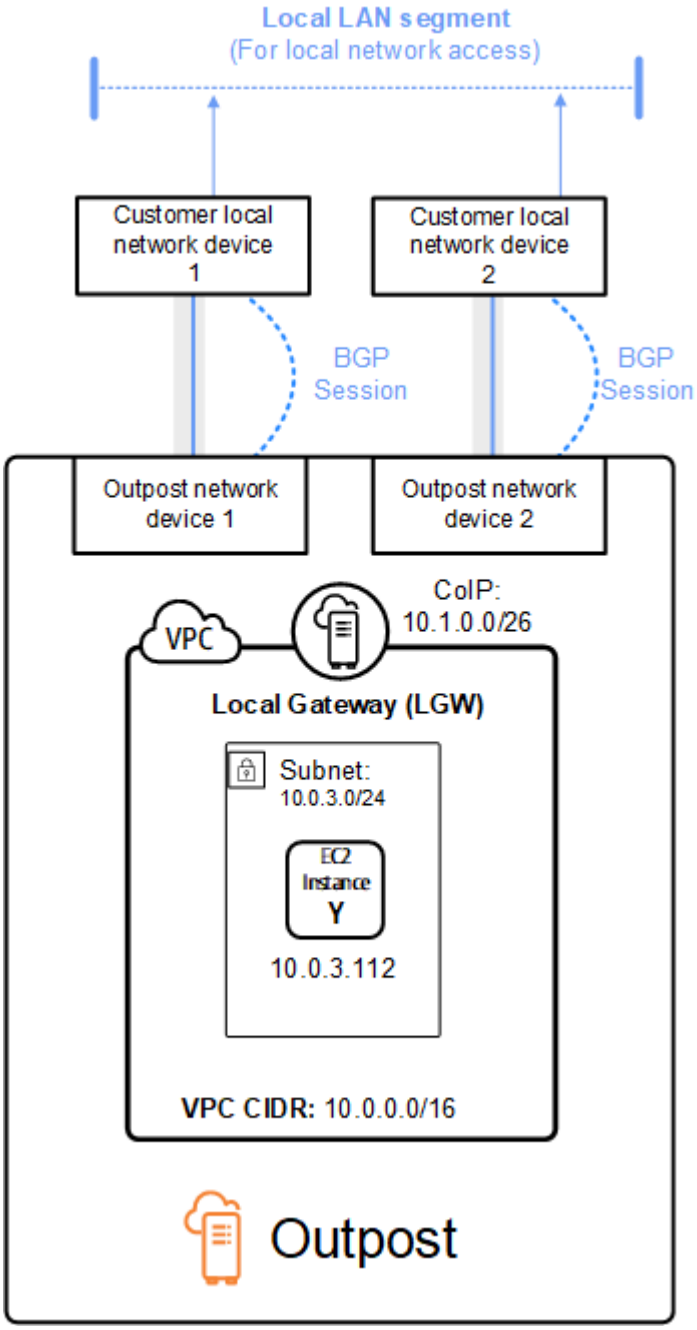
CoIP を選択した場合、 はインストールプロセス中に指定した情報からプール AWS を作成します。このプールから Elastic IP アドレスを作成し、そのアドレスを Outpost 上のリソース (EC2 インスタンスなど) に割り当てることができます。

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

共有 AWS Outposts リソースの使用

Outpost 共有を使用すると、Outpost の所有者は、同じ AWS 組織内の他の AWS アカウントと、Outpost や Outpost リソース (ローカルゲートウェイルートテーブルなど) を共有できます。Outpost の所有者は、Outpost リソースを一元的に作成して管理し、AWS 組織内の複数の AWS アカウント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 キャパシティーの予約 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。

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

目次

- 共有 Outpost リソースの共有解除
- 共有 Outpost リソースの特定
- 共有 Outpost リソースの権限
- 請求と使用量測定
- 制限事項

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 Outpost ラックで利用できるリソースです。サーバーリソースについては、「Outposts サーバー AWS Outposts ユーザーガイド」の「共有 AWS Outposts リソースの使用」を参照してください。

- 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。
- 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する必要があります。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

Outposts リソースの共有は AWS Resource Access Manager (AWS RAM) と統合されます。AWS RAM は、AWS リソースを任意の AWS アカウントと共有したり、AWS Organizations 経由で共有したりするためのサービスです。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。コンシューマーには、個別の AWS アカウント、組織単位または AWS Organizations 内の組織全体が指定できます。

AWS RAM の詳細については、「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。例えば、us-east-1a アカウントのアベイラビリティーゾーン AWS の場所は、別の us-east-1a アカウントのアベイラビリティーゾーン AWS の場所と異なる可能性があります。

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 アカウントで同じアベイラビリティーゾーンを一貫して示すための一意の識別子です。例えば、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を示します。

アカウントのアベイラビリティーゾーンの AZ ID を表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
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。リソース共有とは、AWS RAM アカウント間で自身のリソースを共有するための AWS 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と、既存のリソース共有に追加されます。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。

AWS Organizations の組織の一員であり、組織内での共有が有効になっている場合は、組織内のコンシューマーに AWS RAM コンソールから共有 Outpost リソースへのアクセスを許可できます。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。

自身が所有する Outpost リソースは、 AWS Outposts コンソール、AWS RAM コンソール、または AWS CLI を使用して共有できます。

AWS Outposts コンソールを使用して、自身が所有する Outpost を共有するには

1. AWS Outposts コンソール (https://console.aws.amazon.com/outposts/) 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るので、以下の手順で 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。

AWS CLI 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

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

共有されている Outpost が共有解除されると、コンシューマーはその Outpost を AWS Outposts コンソールに表示できなくなります。Outpost に新しいサブネットを作成したり、Outpost で新しい EBS ボリュームを作成したり、AWS Outposts コンソールや AWS CLI を使用して Outpost の詳細やインスタンスタイプを表示したりすることはできません。コンシューマーが作成した既存のサブネット、ボリューム、またはインスタンスは削除されません。コンシューマーが Outpost で作成した既存のサブネットは、引き続き新しいインスタンスの起動に使用できます。

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 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 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。

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 AWS CLI を使用できます。

AWS RAM コンソールを使用して、自身が所有する共有 Outpost リソースを共有解除するには

「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。

AWS CLI を使用して、自身が所有する共有 Outpost リソースを共有解除するには

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 AWS CLI を使用して、共有 Outpost を特定できます。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 を特定するには

1. AWS Outposts コンソール (https://console.aws.amazon.com/outposts/) 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 を識別します。

AWS CLI を使用して、共有 Outpostを特定するには

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、ユーザー所有の Outpost リソースとあなたと共有されている Outpost リソースを返します。`OwnerId` は、Outpost リソース所有者の AWS アカウント ID 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。AWS Organizations を使用して、コンシューマーが共有 Outpost 上に作成したリソースを表示、変更、および削除できます。

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 所有者が所有するインスタン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 所有者には AWS Direct Connect および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 レベルのリソースの料金が請求されます。

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の料金も請求されます。

制限事項

AWS Outposts 共有の使用には、以下の制限があります。

- AWS Outposts 共有による操作には、共有サブネットの制限が適用されます。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。

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からメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。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 — 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責任 AWS は AWS にあります。 AWS また、 は、安全に使用できるサービスも提供します。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。に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。
- クラウド内のセキュリティ — 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、お客様は、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 「 ラックのよくある質問」を参照してください。

このドキュメントは、 の使用時に責任共有モデルを適用する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 の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。お客様は、このインフラストラクチャでホストされてい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 Identity Center 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のよくある質問」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 Outpost ラック上のデータを復号化するために必要です。

EBS ボリュームとスナップショットに Amazon EBS 暗号化を使用できます。Amazon EBS 暗号化は AWS Key Management Service （ AWS KMS) と KMS キーを使用します。詳細については、Amazon EC2 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。

の Identity and Access Management (IAM) AWS Outposts

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 リソースの使用を承認する (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 機能について学びます。

Outposts で使用できる AWS IAM の機能

IAM 機能	AWS Outposts のサポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	No
ポリシーアクション	Yes
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	No
ABAC (ポリシー内のタグ)	はい
一時的な認証情報	Yes
プリンシパル権限	Yes

IAM 機能	AWS Outposts のサポート
サービスロール	いいえ
サービスリンクロール	はい

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ポリシーをサポートする	Yes

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 権限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 ポリシーの作成」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。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「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 内のリソースベースのポリシー

リソースベースのポリシーのサポート	No

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの

場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

AWS Outposts のポリシーアクション

ポリシーアクションに対するサポート	はい

管理者は AWS JSON 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んなリソースにどんな条件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。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

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権限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、「サービス認証リファレンス」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

ポリシーリソースに対するサポート	はい

管理者は AWS JSON 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どのような条件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。ステートメントには、Resource または NotResource要素を含める必要があります。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。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限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": "*"
```

Outposts API AWS アクションの中には、複数のリソースをサポートするものがあります。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	はい

管理者は AWS JSON 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んなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。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することで、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。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。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 の条件キーのリストを確認するには、「サービス認証リファレンス」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 ACLs

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

AWS Outposts での ABAC

ABAC のサポート (ポリシー内のタグ)	はい

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義するアクセス許可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

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はいです。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 とは?」を参照してください。ABAC をセットアップするステップ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「属性に基づく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	はい

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセ

スすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、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することを推奨しています。詳細については、「IAM の一時的セキュリティ認証情報」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許可

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。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 のサービスロール

サービスロールのサポート	いいえ

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」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	はい

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、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

AWS Outposts の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AWS Outpostsのサービスにリンクされたロールの使用。

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 Outposts AWS 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。また、、 AWS Command Line Interface （ AWS CLI ）AWS Management Console、または AWS API を使用してタスクを実行することはできません。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。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの 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 ポリシーの作成」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、「サービス認証リファレンス」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

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Outposts AWS リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。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を付与するには、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して、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「AWS ジョブ機能の管理ポリシー」を参照してください。

- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。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、最小特権権限とも呼ばれています。IAM を使用して権限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 でのポリシーと権限」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。例えば、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、 などの特定の を介してサービスアクションが使用される場合に 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 AWS CloudFormation。詳細については、IAM ユーザーガイドの [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer 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 Access Analyzer 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 ポリシーの検証」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、セキュリティを強化するために MFA を有効にします。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 保護 API アクセスの設定」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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012: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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
}
```

AWS Outpostsのサービスにリンクされたロールの使用

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一意のタイプの IAM ロールです AWS Outposts。サービスにリンクされたロールは によって事前定義 AWS Outposts されており、ユーザーに代わってサービスから他の AWS の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が含まれています。

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。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティに添付することはできません。

サービスにリンクされたロールを削除するには、まずその関連リソースを削除します。これにより、AWS Outposts リソースにアクセスするためのアクセス許可を誤って削除できないため、リソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、「IAM と連携するAWS のサービス」を参照して、[サービスリンクロール] 列が [はい] のサービスを探してください。[はい] のリンクを選択すると、該当するサービスのサービスリンクロールに関するドキュメントが表示されます。

AWS Outpostsのサービスリンクロールのアクセス許可

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。これにより、Outposts がユーザーに代わってプライベート接続用の AWS リソースにアクセスできるようになります。このサービスにリンクされたロールにより、プライベート接続の構成が可能になり、ネットワークインターフェイスが作成され、サービス リンク エンドポイント インスタンスに接続されます。

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

- `outposts.amazonaws.com`

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 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するサービスにリンクされたロールポリシーです 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: `all AWS resources` 上で `ec2:DescribeNetworkInterfaces`
- アクション: `all AWS resources` 上で `ec2:DescribeSecurityGroups`
- アクション: `all AWS resources` 上で `ec2:CreateSecurityGroup`
- アクション: `all AWS resources` 上で `ec2:CreateNetworkInterface`

AWSOutpostsPrivateConnectivityPolicy_***OutpostID*** ポリシーは AWS Outposts 、 が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るようにします。

- アクション: `all AWS resources that match the following Condition:` 上で `ec2:AuthorizeSecurityGroupIngress`

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

- アクション: `all AWS resources that match the following Condition:` 上で `ec2:AuthorizeSecurityGroupEgress`

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

- アクション: `all AWS resources that match the following Condition:` 上で `ec2:CreateNetworkInterfacePermission`

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

- アクション: `ec2:CreateTags` 上で `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}}
```

サービスにリンクされたロールの作成、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、権限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ロールの許可を参照してください。

AWS Outpostsのサービスリンクロールの作成

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 Management Console、 AWS Outposts によってサービスにリンクされたロールが作成されます。

詳細については、「VPC を使用したサービスリンクのプライベート接続」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の編集

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した後は、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

用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

AWS Outpostsのサービスリンクロールの削除

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。

> **Note**
>
> 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、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。

> **Warning**
>
> AWSServiceRoleForOutposts_*OutpostID* を削除する必要があります。次の手順で、Outpost を削除します。

開始する前に、 AWS Resource Access Manager () を使用して Outpost が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*** が使用する 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。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、、または AWS API を使用して AWS CLI、AWSServiceRoleForOutposts_*OutpostID* サービスにリンクされたロールを削除します。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ロールの削除」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をサポートするリージョン

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ます。詳細については、「AWS Outposts エンドポイントとクォータ」を参照してください。

AWS の マネージドポリシー AWS Outposts

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対する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、ロールへの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。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシー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) が更新されます。 は、新しい AWS のサービス が起動されたとき、または既存のサービスで新しい API AWS オペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

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、 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 AWS Outposts 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の使用」を参照してください。

AWS マネージドポリシー： AWSOutpostsPrivateConnectivityPolicy

このポリシーは、 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 AWS Outposts 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の使用」を参照してください。

AWS OutpostsAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS Outposts 以降の 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 Outposts が変更の追跡を開始しました	AWS Outposts が AWS マネージド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 AWS 環境を設計するには、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開した 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 は必須で TLS 1.3 がお勧めです。
- 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。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

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 リージョンで機能するのと同じ方法で機能します。つまり、分析 GuardDuty のために CloudWatch Logs、Amazon S3、または Amazon に発行できます。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 が切断された状態の場合、 CloudWatch や他のサービスからは表示されません。

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、または改ざんしていないことを確認してください。AWS Outposts 機器には、 AWS Outposts AWS 「 サービス条件」への準拠を保証するために改ざんモニタリングが搭載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。Outpost 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 キャパシティーの可用性メトリクスを使用して、アプリケーションの状態をモニタリングし、自動復旧オプションを設定する CloudWatch アクションを作成し、Outposts のキャパシティー使用率を経時的にモニタリングするためにアラームを設定できます。

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にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、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、「 でのレポートのダウンロード AWS Artifact」の」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。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

  > **Note**
  >
  > すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config

- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

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 リージョンを介した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、次に親 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 ゲートウェイを経由できます。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 WAF AWS Shield、Amazon などの AWS セキュリティサービスを AWS リージョン CloudFront で使用できます。

Outposts サブネットのルートテーブル設定については、「ローカルゲートウェイルートテーブル」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アクセスポイントがない。
- 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 リージョンで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します。

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を介した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は、ローカルデータセンターを介してインターネットにアクセスします。インターネットにアクセスするワークロードトラフィックは、ローカルインターネットのプレゼンスポイントを通過し、ローカルに出力されます。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 ワークロードトラフィックを保護する役割を担います。

Outposts サブネットのルートテーブル設定については、「ローカルゲートウェイルートテーブル」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への低レイテンシーアクセスが必要です。
  - Data Transfer Out (DTO) 料金が発生しないようにしたい。
  - 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したい。
- セキュリティレイヤーは、Outposts のワークロードトラフィックを保護する責任があります。
- ダイレクト VPC ルーティング (DVR) を選択した場合は、Outposts CIDRs がオンプレミス CIDRs 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) を介して伝播されている場合、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。または、VPC エンドポイントを選択して目的のサービスに到達することもできます。

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。

Outpost を監視します。

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 のデータポイントに関する統計を、メトリクス と呼ばれる時系列データの順序付けられたセットとして取得します。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、「CloudWatch のメトリクス AWS Outposts」を参照してください。

CloudTrail ログ

AWS CloudTrail を使用して、AWS API に対して実行された呼び出しに関する詳細情報をキャプチャできます。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、呼び出し者、呼び出し日時などの情報を判断できます。

CloudTrail ログには、 の 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、「AWS Outposts 内の情報 CloudTrail」を参照してください。

VPC Flow Logs

VPC フローログを使用して、Outpost との送受信および Outpost 内の送受信のトラフィックに関する詳細情報を取得します。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

トラフィックミラーリングを使用して、Outpost から Outpost のセキュリティアプライアンスとモニタリングアプライアンスに out-of-bandネットワークトラフィックを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、Amazon Virtual Private Cloud の「Traffic Mirroring Guide」を参照してください。

AWS Health Dashboard

AWS Health Dashboard には、AWS リソースのヘルス状態の変化によってトリガーされる情報と通知が表示されます。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。例えば、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 AWS Health Dashboard はセットアップを必要とせず、アカウントで認証されたユーザーが表示できます。詳細については、「Getting started with the AWS Health Dashboard」を参照してください。

CloudWatch の メトリクス AWS Outposts

AWS Outposts は、Outposts. CloudWatch Enables CloudWatch のデータポイントを Amazon に発行し、それらのデータポイントに関する統計を、メトリクス と呼ばれる時系列データの順序付けられたセットとして取得できるようにします。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。例えば、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。例えば、`ConnectedStatus`メトリクスをモニタリングする CloudWatch アラームを作成できます。平均メトリクスが 未満の場合は1、E 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 CloudWatch 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、AWS オンプレミス ネットワーク内からリージョンへの接続を確認し、AWS 問題が解決しない場合はサポートに連絡する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 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 CloudWatch、「Amazon CloudWatch ユーザーガイド」を参照してください。

内容

- Outpost メトリクス
- Outpost メトリック ディメンション
- Outpost の CloudWatch メトリクスを表示する

Outpost メトリクス

`AWS/Outposts` 名前空間には、次のメトリクスが含まれます。

`ConnectedStatus`

Outpost のサービス リンク接続のステータス。平均統計値が より小さい場合 1、接続は障害を受けています。

単位: 個

最大解像度:1 分

統計: 最も有用な統計は `Average` です。

ディメンション: `OutpostId`

`CapacityExceptions`

インスタンス起動時の容量不足エラーの数。

単位: 個

最大解像度:5 分

統計値: 最も有用な統計値は `Maximum` および `Minimum` です。

ディメンション: `InstanceType`および `OutpostId`

`IfTrafficIn`

Outposts 仮想インターフェイス (VIFs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。

単位: ビット/秒

最大解像度:5 分

統計値: 最も有用な統計値は `Max` および `Min` です。

ローカルゲートウェイ VIFs (lgw-vif) のディメンション: `OutpostsId`、`VirtualInterfaceGroupId`、および `VirtualInterfaceId`

サービスリンク VIFs (sl-vif) のディメンション: `OutpostsId`および `VirtualInterfaceId`

`IfTrafficOut`

Outposts 仮想インターフェイス (VIFs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。

単位: ビット/秒

最大解像度:5 分

統計値: 最も有用な統計値は Max および Min です。

ローカルゲートウェイ VIFs (lgw-vif) のディメンション: OutpostsId、VirtualInterfaceGroupId、および VirtualInterfaceId

サービスリンク VIFs (sl-vif) のディメンション: OutpostsIdおよび VirtualInterfaceId

InstanceFamilyCapacityAvailability

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。

単位: パーセント

最大解像度:5 分

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。

ディメンション: InstanceFamilyおよび OutpostId

InstanceFamilyCapacityUtilization

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。

単位: パーセント

最大解像度:5 分

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。

ディメンション: Account、InstanceFamily、OutpostId など

InstanceTypeCapacityAvailability

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。

単位: パーセント

最大解像度:5 分

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。

ディメンション: InstanceTypeおよび OutpostId

InstanceTypeCapacityUtilization

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。

単位: パーセント

最大解像度:5 分

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。

ディメンション: Account、InstanceType、OutpostId など

UsedInstanceType_Count

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。

単位: 個

最大解像度:5 分

ディメンション: Account、InstanceType、OutpostId など

AvailableInstanceType_Count

使用可能なインスタンス数。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。

単位: 個

最大解像度:5 分

ディメンション: InstanceTypeおよび OutpostId

AvailableReservedInstances

Outpost でオンデマンドキャパシティ予約 (ODCR) に使用できるインスタンスの数。このメトリクスは、Amazon EC2 リザーブドインスタンスを測定しません。

単位: 個

最大解像度:5 分

ディメンション: InstanceTypeおよび OutpostId

UsedReservedInstances

Outpost でオンデマンドキャパシティ予約 (ODCR) に使用できるインスタンスの数。このメトリクスは、Amazon EC2 リザーブドインスタンスを測定しません。

単位: 個

最大解像度:5 分

ディメンション: InstanceTypeおよび OutpostId

TotalReservedInstances

Outpost でオンデマンドキャパシティ予約 (ODCR) に使用できるインスタンスの数。このメトリクスは、Amazon EC2 リザーブドインスタンスを測定しません。

単位: 個

最大解像度:5 分

ディメンション: InstanceTypeおよび OutpostId

EBSVolumeTypeCapacityUtilization

使用されている EBS ボリューム タイプの容量の割合。

単位: パーセント

最大解像度:5 分

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。

ディメンション: VolumeTypeおよび OutpostId

EBSVolumeTypeCapacityAvailability

利用可能な EBS ボリューム タイプの容量の割合。

単位: パーセント

最大解像度:5 分

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。

ディメンション: VolumeTypeおよび OutpostId

EBSVolumeTypeCapacityUtilizationGB

EBS ボリューム タイプに使用されているギガバイト数。

単位:ギガバイト

最大解像度:5 分

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。

ディメンション: VolumeTypeおよび OutpostId

EBSVolumeTypeCapacityAvailabilityGB

EBS ボリューム タイプの利用可能な容量のギガバイト数。

単位:ギガバイト

最大解像度:5 分

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。

ディメンション: VolumeTypeおよび OutpostId

Outpost メトリック 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。

ディメンション	説明
VirtualInterfaceId	ローカルゲートウェイまたはサービスリンク仮想インターフェイス (VIF) の ID。
VirtualInterfaceGroupId	ローカルゲートウェイ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。

Outpost の CloudWatch メトリクスを表示する

CloudWatch コンソールを使用して、ロードバランサーの 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. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで メトリクスを選択します。
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、検索ボックスに名称を入力します。

AWS CLI を使ってメトリクスを表示するには

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
```

AWS CLI を使用してメトリクスの統計を取得するには

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 dimension. CloudWatch treats のディメンションの一意の各組み合わせを個別のメトリクスとして取得します。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、 のユーザーAWS CloudTrail、ロール、または AWSのサービスによって実行されたアクションを記録するサービスである と統合されていますAWS Outposts。 は、 のすべての API コールをイベントAWS Outpostsとして CloudTrail キャプチャします。キャプチャされたコールには、AWS Outposts コンソールのコールと、AWS Outposts API オペレーションへのコードのコールが含まれます。証跡を作成する場合は、 の CloudTrail イベントなど、S3 バケットへのイベントの継続的な配信を有効にすることができますAWS Outposts。証跡を設定しない場合でも、コンソールのイベント履歴 で最新の CloudTrail イベントを表示できます。 で収集された情報を使用して CloudTrail、 に対するリクエストAWS Outposts、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

AWS Outposts 内の情報 CloudTrail

CloudTrail AWSアカウントを作成すると、 がアカウントで有効になります。でアクティビティが発生するとAWS Outposts、そのアクティビティは CloudTrail イベント履歴 の他のAWSサービスイベントとともに イベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「イベント履歴 を使用した CloudTrail イベントの表示」を参照してください。

AWSのイベントなど、AWS Outpostsアカウントのイベントの継続的なレコードについては、追跡を作成します。証跡により CloudTrail 、 は親 の S3 バケットにログファイルを配信できますAWS リージョン。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した S3 バケットにログファイルが配信されます。さらに、 CloudTrail ログで収集されたデータをより詳細に分析し、それに基づく対応を行うように他の AWSサービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail サポートされているサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからのログファイルの受信 CloudTrail

すべての AWS Outposts アクションは によってログに記録されます CloudTrail。これらは、AWS Outposts API リファレンスで説明されています。例えば、CreateOutpost、、および ListSitesアクションを呼び出すとGetOutpostInstanceTypes、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。この ID 情報は、リクエストがどのようにして送信されたかを確認するのに役立ちます:

- ルートまたはユーザーの認証情報を使用して行われたか。
- ロールまたはフェデレーティッドユーザーの一時的なセキュリティ認証情報を使用して行われたか。
- 別の AWS のサービスによって行われたか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

AWS Outposts ログファイルエントリについて

証跡は、指定した S3 バケットにイベントをログファイルとして配信できるようにする設定です。CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベント は、任意の送信元からの単一の要求を表します。これには、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 CreateOutpostアクションを示す CloudTrail ログエントリを示しています。

```
{
    "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"
}
```

Outpost のメンテナンス

責任共有モデル、 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に責任を負います。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。例えば、 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 は、Outpost のパフォーマンス、ヘルス、メトリクスもモニタリングし、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

ハードウェアメンテナンス

が Outpost で実行されている Amazon EC2 インスタンスをホストするハードウェアで回復不可能な問題 AWS を検出した場合、影響を受けたインスタンスのリタイアが予定されていることを Outpost の所有者と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 を停止して起動します。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 サイトのマネージャー 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、サイトのマネージャーが AWS チームと話し合ってから最短で 2 営業日以内にスケジュールできます。

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、またはラック要素を置き換え、新しい容量をオンラインにします。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。

AWS Outposts 電力イベントと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 機器を設置する施設は、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、電力とネットワークの最小要件を満たしている必要があります。Outposts ラックは、電源とネットワーク接続が中断されていない場合にのみ正しく動作します。

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。

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復旧します。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。

詳細については、「施設のネットワーク接続がダウンするとどうなりますか?」という質問を参照してください。「AWS Outposts ラックの FAQ」 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により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 AWS 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「AWS 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は、計画的な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工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-SetupIPMonitoringFrom VPC ツールについて説明しています。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。このドキュメントは、ping、MTR、TCP トレースルート、トレースパスの診断テストを実行し、結果を Amazon CloudWatch Logs に保存します。その結果は CloudWatch ダッシュボードで視覚化できます (レイテンシー、パケットロスなど) 。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 を使用するための自動 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ています。
- 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。

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「 の Dedicated Host AWS Outposts」を参照してください。 Amazon EC2 Windows の場合は、「Amazon EC2 ユーザーガイド」の「 の Dedicated Host AWS Outposts」を参照してください。 Amazon EC2

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、 に連絡せずに Outpost デプロイ内のサーバーのレイアウトを変更することができます AWS Support。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「専有ホストの割り当て」または「専有ホストの割り当て」を参照してくださいAmazon EC2。

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。Outpost 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。インスタンス復旧の詳細については、Amazon EC2 ユーザーガイド」の「自動配置とアフィニティを理解する」または「自動配置とアフィニティを理解する」を参照してください。Amazon EC2

を使用して Dedicated Hosts を共有できます 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、「共有リソースの使用」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、「Linux インスタンスの復旧」または「Windows インスタンスの復旧」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。

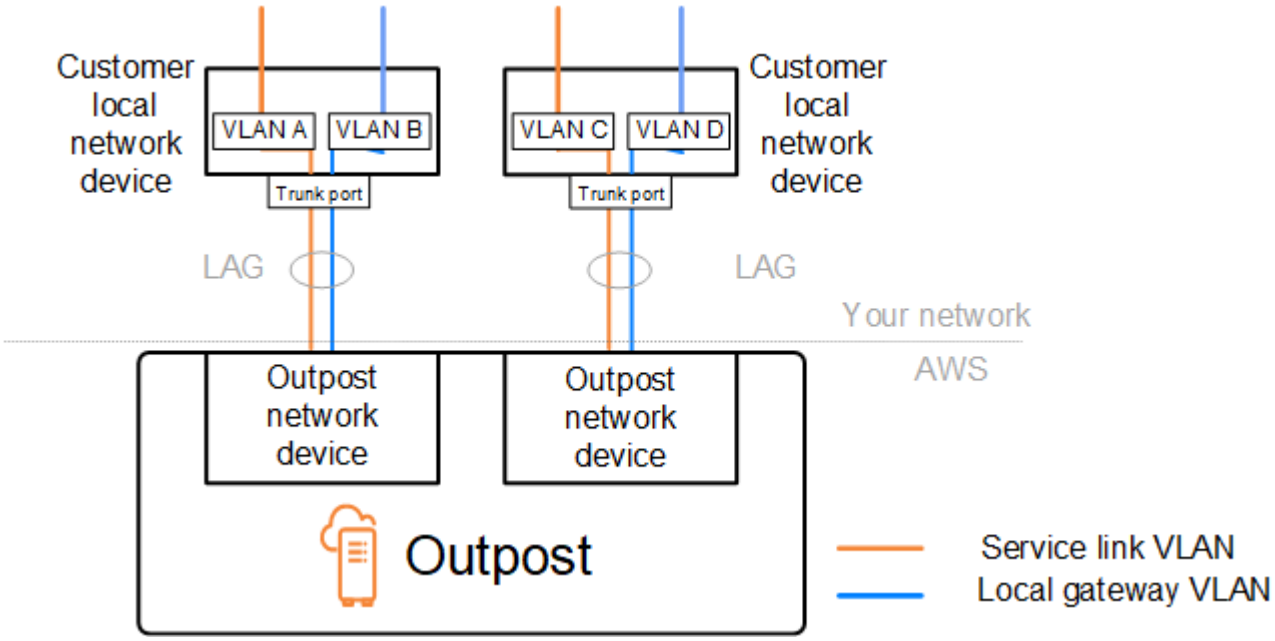
インスタンスをターゲット パーティションにデプロイすることもできます。次の図は、ターゲットを絞った分散を使用したパーティションプレイスメントグループを示しています。

プレイスメントグループの使用の詳細については、Amazon EC2 ユーザーガイド」の「 でのプレイスメントグループとプレイスメントグループ AWS Outposts」を参照してください。Windows については、「Amazon EC2 ユーザーガイド」の「 でのプレイスメントグループとプレイスメントグループ AWS OutpostsAmazon EC2」を参照してください。

高可用性の詳細については、 AWS Outposts 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 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 AWS 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、「AWS 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 AWS 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、「AWS 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。

AWS 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 AWS 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 AWS Direct Connect リンクステータスを確認します AWS Management Console。
   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 を実行し、エッジルーターの BGP 設定を確認します。詳細については、「 AWS Direct Connect ユーザーガイド」の「トラブルシューティング AWS Direct Connect」および「 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ます」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、VRF にデフォルトルートまたは AWS パブリック IP アドレスの範囲が表示されない場合は、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。
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で Outpost のサービスリンク IP アドレス範囲と AWS パブリック IP アドレス範囲が許可されていることを確認します。詳細については、「AWS OutpostsAWS 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 AWS Direct Connect ピア IP アドレスへの MTR/tracerroute/パケットキャプチャを実行します。エンタープライズサポートプランを使用して、テスト結果を AWS サポートと共有します。

AWS 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 AWS 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 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 アドレスに Ping を実行し、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 AWS 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、「 AWS Direct Connect ユーザーガイド」の「トラブルシューティング AWS Direct Connect」、「 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」を参照してください。「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. AWS Direct Connect プライベート仮想インターフェイスは、選択した AWS 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 セッション経由でプライベート仮想インターフェイス AWS の にデフォルトルートを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 AWS Direct Connect ピア IP アドレスへの MTR/tracerroute/パケットキャプチャを実行します。エンタープライズサポートプランを使用して、テスト結果を AWS 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 アドレス AWS 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、tracerroute、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背後にあります

Outpost を同期され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ファイアウォールの背後に配置すると、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 firewall-1 を通過し、アウトバウンドトラフィックは firewall-2 を通過します。以下のチェックリストを使用して、特に以前に正しく機能していた場合、サービスリンクの非対称ルーティングの可能性を特定します。

- 企業ネットワークのルーティング設定に、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った可能性のある最近の変更や継続的なメンテナンスがあった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時と一致するトラフィックパターンの変更を確認します。
  - 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原因となっていた可能性のある分割ブレインファイアウォールペアのシナリオがないか確認してください。
  - サービスリンクの問題の開始に合わせて、企業ネットワークのルーティング (OSPF/ISIS/EIGRP メトリクスの変更、BGP ルートマップの変更) へのリンクダウンまたは最近の変更を確認します。

- 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。
  - ISP へのリンクのトラフィックグラフをチェックして、サービスリンクの問題の開始時と一致するトラフィックパターンへの変更がないか確認します。
- サービスリンク AWS 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。
  - AWS Direct Connect サービスの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 AWS 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での 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、いずれかのサービスを中断すると、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 AWS Direct Connect 。 end-to-end ネットワーク接続の AWS Direct Connect 部分の耐障害性は、Resiliency with AWS Direct Connect Resiliency Toolkit でテストできます。詳細については、AWS Direct Connect 「Resiliency Toolkit による障害耐性のテスト — フェイルオーバーテスト」を参照してください。

前述のチェックリストを実行し、考えられる根本原因としてサービスリンクの非対称ルーティングを特定した後は、他にもいくつかのアクションを実行できます。

- 会社の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。
- 一方または両方のファイアウォールにログインし、コマンドラインからすべてのフローのすべてのフロー状態情報をクリアします (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 の発表を一時的に除外するか、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します。
- 各ファイアウォールを順番に再起動して、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の潜在的な破損を排除します。
- ファイアウォールベンダーに、ポート 443 から送信され、ポート 443 宛ての UDP 接続の UDP フローステートの追跡を確認または緩和してもらいます。

AWS Outposts end-of-term オプション

AWS Outposts 期間の終了時には、次の 3 つのオプションがあります。

- サブスクリプションを更新し、既存の Outpost を維持します。
- サブスクリプションを終了し、Outpost ラックを返却できるように準備してください。
- month-to-month サブスクリプションに変換し、既存の Outpost を保持します。

トピック

サブスクリプションを更新する

サブスクリプションを更新し、既存の Outpost を維持するには

Outpost の期間が終了する 30 日前までに次の手順を完了してください。

1. AWS Support センターコンソールにサインインします。
2. [ケースを作成] を選択します。
3. [Account and billing] (アカウントおよび請求) を選択します。
4. [サービス] で [請求] を選択します。
5. カテゴリでその他の請求に関する質問を選択します。
6. 重要度で重要な質問 を選択します。
7. [Next step: Additional information] (次のステップ:追加情報) を選択します。
8. 追加情報ページの件名に、**`Renew my Outpost subscription`** などの更新リクエストを入力します。
9. 説明には、次の支払いオプションのいずれかを入力します。
    - 前払いなし
    - 一部前払い

- 全前払い

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。

10. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。
11. [Contact us] (お問い合わせ) ページで、希望する言語を選択します。
12. 希望する連絡方法を変更します。
13. ケースの詳細を確認して、[Submit] (送信) を選択します。ケース ID 番号と概要が表示されます。

AWS カスタマーサポートがサブスクリプションの更新プロセスを開始します。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を更新するか Outpost ラックを返すように指定しない場合、自動的に month-to-month サブスクリプションに変換されます。Outpost 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。

サブスクリプションを終了し、ラックを返却できるように準備する

> **Important**
>
> AWS は、次の手順を完了するまで戻りプロセスを開始できません。サポートケースを開いてサブスクリプションを終了した後は、返品プロセスを中止することはできません。

サブスクリプションを終了するには

Outpost の期間が終了する 30 日前までに次の手順を完了してください。

1. AWS Support センターコンソールにサインインします。
2. [ケースを作成] を選択します。
3. [Account and billing] (アカウントおよび請求) を選択します。
4. [サービス] で [請求] を選択します。
5. カテゴリでその他の請求に関する質問を選択します。

6. 重要度で重要な質問 を選択します。
7. [Next step: Additional information] (次のステップ:追加情報) を選択します。
8. 追加情報ページの件名に、**`End my Outpost subscription`** などの明確なリクエストを入力します。
9. 説明には、Outpost の取り出しを希望する日付を入力します。
10. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。
11. [Contact us] (お問い合わせ) ページで、希望する言語を選択します。
12. 希望する連絡方法を変更します。
13. ケースの詳細を確認して、[Submit] (送信) を選択します。ケース ID 番号と概要が表示されます。

AWS カスタマーサポートから連絡があり、取得の調整が行われます。

AWS Outposts ラックを返却できるように準備するには：

> **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、Outpost 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 AWS CLI disassociate-resource-share コマンドを実行します。

   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「インスタンスを終了する」の手順に従います。 Amazon EC2

> **Note**
>
> Application Load Balancer や Amazon Relational Database Service (RDS) など、Outpost で実行されている AWSマネージドサービスの中には、EC2 容量を消費するものがあります。 Amazon Relational Database Service ただし、関連付けられたインスタンスは Amazon EC2 ダッシュボードに表示されません。容量を解放するには、これらのサービスに関連するリソースを終了する必要があります。詳細については、「一部の EC2 インスタンス容量が Outpost にないのはなぜですか？」を参照してください。

3. アカウント内の Amazon EC2 インスタンス instance-capacity-availability の を確認します AWS 。

   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。

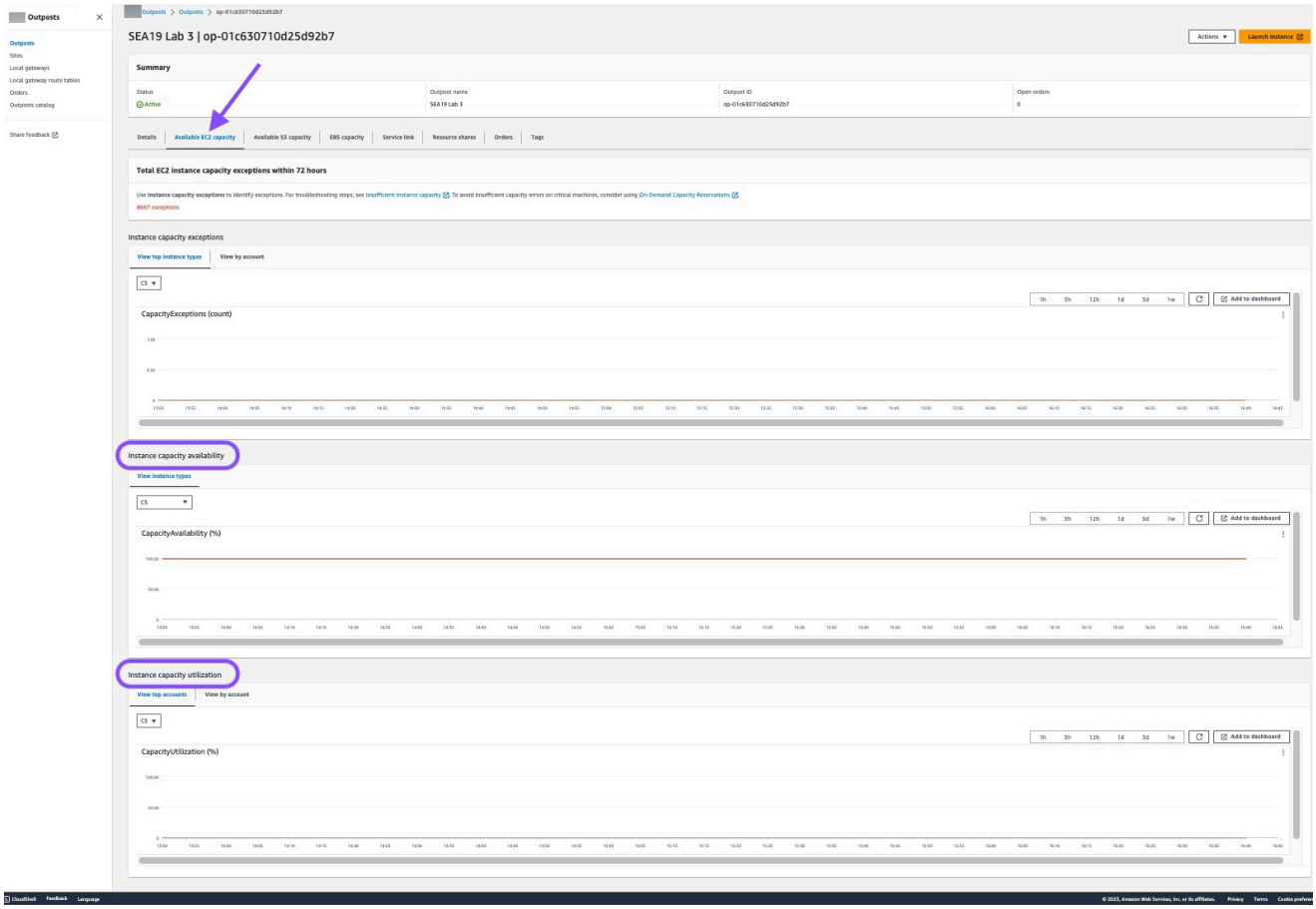
   c. 返す特定の Outpost を選択します。

   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。

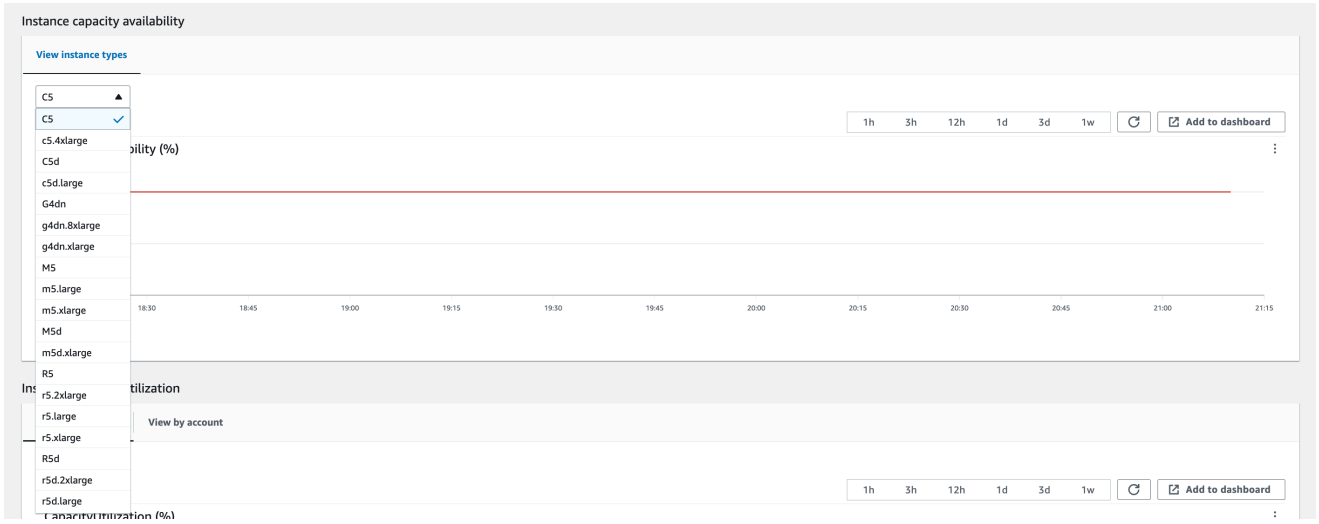
   e. 各インスタンスファミリーのインスタンス容量の可用性が 100% であることを確認します。

   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. Outpost 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 Simple Storage Service ユーザーガイド」の「Outpost 上で Amazon S3 バケットを削除する方法」に従ってください。
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 取り出しチームがユーザーに代わって破棄できます。

month-to-month サブスクリプションに変換する

month-to-month サブスクリプションに変換して既存の Outpost を維持するには、アクションは必要ありません。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。

Outpost 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 のクォータ

AWS アカウント には、AWS のサービス ごとにデフォルトのクォータ (以前は制限と呼ばれていました) があります。特に明記されていない限り、クォータはリージョンごとに存在します。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。

AWS Outposts のクォータを表示するには、[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。

お客様の AWS アカウント アカウントには、AWS Outposts に関連する以下のクォータがあります。

リソース	デフォルト	引き上げ可能	コメント
Outpost サイト	100	はい	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。 AWS アカウントの各リージョンには100 の Outpost サイトを持つことができます。
サイトあたりの Outpost	10	はい	AWS Outposts には、Outpost と呼ばれるハードウェアと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。 各 Outposts サイトには 10 個の Outpost を設置できます。

AWS Outposts およびその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ており、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。

ドキュメント履歴

以下の表は、AWS Outposts ユーザーガイド の重要な変更点をまとめたものです。

変更	説明	日付
キャパシティ管理	新しい Outposts オーダーのデフォルトの容量設定を変更できます。	2024 年 4 月 16 日
AWS Outposts ラックはサービスリンクインターフェースのスループットメトリクスをサポートします。	`IfTrafficIn` とのメトリクスを活用して、Outpost ラックのサービスリンク仮想インターフェイス (VIF) 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量を監視できるようになりました。`IfTrafficOut` Amazon CloudWatch	2023 年 11 月 17 日
ローカルゲートウェイとの VPC 内通信 AWS Outposts	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
E-nd-of-term AWS Outposts ラック用オプション	AWS Outposts 期間の終了時に、サブスクリプションを更新、終了、または変更することができます。	2023 年 8 月 1 日
Outposts Amazon ルート 53 AWS Outposts はラックでもご利用いただけます。	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	2023 年 7 月 20 日

	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。	
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
のダイレクト 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 AWS Outposts ラックのユーザーガイドを作成しました	AWS Outposts ユーザーガイドは、ラック用とサーバー用に別々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
配置グループは以下のとおりです。 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
専用ホスト: 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、管理し、 AWS 組織内の他のアカウントと共有します。	2021 年 10 月 18 日

新しい次元 CloudWatch	CloudWatch AWS Outposts 名前空間のメトリクスの新しいディメンション。	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
その他の指標 CloudWatch	CloudWatch リザーブドインスタンスには追加のメトリックスがあります。	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
CloudWatch その他のメトリックス	EBS CloudWatch ボリュームのメトリクスは他にもあります。	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

共有リソース AWS Outposts	アウトポストの共有により、アウトポストのオーナーは、ローカルゲートウェイルートテーブルを含むアウトOutposts AWS とアウトポストリソースを同じ組織内の他のアカウントと共有できます。 AWS	2020 年 10 月 15 日
その他の指標 CloudWatch	CloudWatch インスタンスタイプ数のメトリクスは他にもあります。	2020 年 9 月 21 日
CloudWatch その他の指標	CloudWatch サービスリンクの接続状況を示す指標が追加されました。	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	AWS Resource Access Manager 顧客所有の IPv4 アドレスを共有する場合に使用します。	2020 年 4 月 20 日
その他の指標 CloudWatch	EBS CloudWatch ボリュームのメトリクスは他にもあります。	2020 年 4 月 4 日
初回リリース	AWS Outpostsこれはの最初のリリースです。	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。