サーバー用ユーザーガイド

AWS Outposts

AWS Outposts: サーバー用ユーザーガイド

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 インスタンスやサブネットなどの AWS リソースを作成するときに指定できます。Outpost サブネット内のインスタンスは、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。これらはすべて同じ VPC 内にあります。

> **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。

- 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
Amazon ECS クラスター	はい	はい

リソースタイプ	ラック	サーバー
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

リソースタイプ	ラック	サーバー
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。

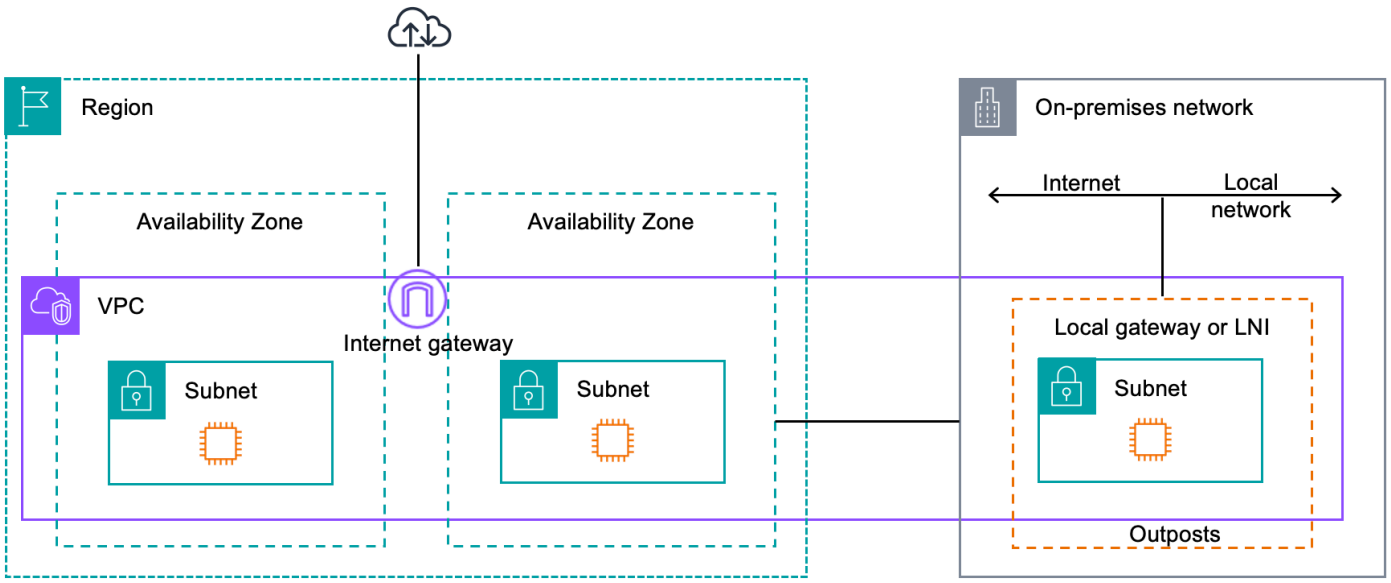
内容

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。

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、「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

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 サーバーに関する FAQ」を参照してください。「Outposts サーバーはどの国と地域で利用できますか?」という質問を参照してください。

このページでは Outposts サーバーの要件について説明しています。Outpost ラックの要件については、「Outpost ラックのAWS Outposts ユーザーガイド」の「Outposts ラックのサイト要件」を参照してください。

施設

これらはサーバーに関する施設の要件です。

> **Note**
>
> 仕様は通常の動作条件におけるサーバーに対するものです。例えば、初期設置時には音響が大きく聞こえ、設置完了後は定格音響出力で動作する場合があります。

- 温度 - 周囲の温度は 41 ~ 95°F (5 ~ 35°C) の範囲内でなければなりません。

  この範囲外の温度では、サーバーはシャットダウンし、温度が再び範囲内に戻ると再起動します。
- 湿度 - 相対湿度は 8 ~ 80% で、結露がない状態でなければなりません。
- 空気品質 - 空気は MERV8 (またはそれ以上) のフィルターにかける必要があります。
- エアフロー - サーバーの位置は、適切なエアフローのクリアランスを確保するために、サーバーの前方および後方の壁との間に最小 6 インチ (15 cm) の隙間を確保する必要があります。
- 重量 — 1U サーバーの重量は 26 ポンドで、2U サーバーの重量は 36 ポンドです。サーバーを設置する場所がサーバーの重量を支えられることを確認してください。

  さまざまな Outposts リソースの重量要件を確認するには、 AWS Outposts コンソールの https://console.aws.amazon.com/outposts/ で [カタログを参照] を選択します。
- レールキットの適合性 - 配送パッケージに含まれるレールキットは、EIA-310-D に適合した 19 インチラックの標準の L 字形マウントブラケットに適合しています。

> **Important**
>
> レールキットは、次の図に示されている U 字型マウントブラケットには適合していません。

- ラックの配置 - 深さが少なくとも 36 インチ (914 mm) の標準 19 インチ EIA-310D ラックの使用をお勧めします。
  - Outposts 2Uサーバーには、高さ3.5インチ (88.9mm)、幅17.5インチ (447 mm)、奥行き30インチ (762 mm) のスペースが必要です。
  - Outposts 1U サーバーには、高さ1.75インチ (44.45 mm)、幅17.5インチ (447 mm)、奥行き24インチ (610 mm) のスペースが必要です。

    > **Note**
    >
    > - サーバーを垂直に取り付けることはサポートされていません。 AWS Outposts
    > - Outposts 1Uサーバーの幅はOutposts 2Uサーバーと同じですが、高さは半分で、奥行きは小さくなっています

  AWS サーバーをラックマウントするためのレールキットが付属しています。詳細については、「ステップ 3: ラックマウント」を参照してください。

  サーバーをラックに設置しない場合でも、このセクションに記載されている他の要件を満たす必要があります。
- 保守性 - Outposts サーバーは正面通路での保守が可能です。
- 音響 — 定格が温度 80°F (27°C) で 78 dBA 以下の音響出力で、GR-63 CORE NEBS に適合しています。
- 耐震支柱 - 規制や規則で義務付けられている範囲で、施設内にある間は適切な耐震固定具および支柱をサーバーに取り付け、維持することになります。
- 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。
- 清掃 — 認定された静電気防止洗浄剤を含む湿らせた布で表面を拭いてください。

ネットワーク

各 Outposts サーバには、。ポートには、以下に詳細が記載されている独自の速度とコネクタの要件があります。

ポートラベル	[Speed] (スピード)	上流のネットワーキングデバイスのコネクタ	トラフィック
ポート 3	10Gbe	SFP+	サービスリンクトラフィックおよび LNI リンクトラフィックの両方 - QSFP+ ブレークアウトケーブル (10 フィート/3 m) によりトラフィックがセグメント化されます。詳細については、「QSFP ネットワークの構成」を参照してください。

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	1024-65535	サービスリンク IP	53	DHCP 提供の DNS サーバー
UDP	443、1024-65535	サービスリンク IP	443	Outposts サービスリンクエンドポイント

[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
TCP	1024-65535	サービスリンク IP	443	Outposts 登録エンドポイント

AWS Direct Connect 接続または公共のインターネット接続を使用して、アウトポストを地域に接続し直すことができます。 AWS Outposts 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。

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 をサポートしている必要があります。 AWS 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。

サービスリンクの推奨帯域幅

AWS 最適な操作性と耐障害性を実現するために、リージョンへのサービスリンク接続には 500 Mbps 以上の冗長接続を使用することを推奨します。 AWS 各 Outpost サーバーの最大使用率は 500 Mbps です。接続速度を上げるには、複数の Outpost サーバーを使用してください。たとえば、AWS Outposts サーバーが 3 台ある場合、最大接続速度は 1.5 Gbps (1,500 Mbps) に増加します。詳細については、「サーバーのサービスリンクトラフィック」を参照してください。

AWS Outposts サービスリンクの帯域幅要件は、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によって異なります。 AWS Outposts サーバーは AMI をキャッシュしないことに注意してください。AMI はインスタンスが起動するたびにリージョンからダウンロードされます。

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推奨を受け取るには、 AWS 営業担当者または APN パートナーにお問い合わせください。

サービスリンクには DHCP 応答が必要です。

サービスリンクでは、ネットワーク設定を行うために IPv4 DHCP 応答が必要です。

サービスリンクの最大レイテンシー

サービスリンクは、サーバーおよびそのアベイラビリティーゾーンからの最大ネットワークレイテンシーを 250 ミリ秒までサポートできます。

電源

これらは Outposts サーバーの電力要件です。

要件

- 電力サポート
- 消費電力
- 電力ケーブル
- 電源の冗長性

電力サポート

サーバーの定格は最大 1600 W、90 ~ 264 VaC、47/63 Hz AC 電源です。

消費電力

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

電力ケーブル

サーバーは IEC C14-C13 電源ケーブルが同梱で出荷されています。

サーバーからラックへの電力ケーブル接続

付属の IEC C14-C13 電力ケーブルを使用して、サーバーをラックに接続します。

サーバーから壁のコンセントへの電力ケーブル接続

サーバーを標準の壁コンセントに接続するには、C14 差込対応のアダプターまたは国固有の電源コードのいずれかを使用する必要があります。

サーバーの設置にかかる時間を節約するために、ご利用の地域に適したアダプターまたは電源コードを用意してください。

- 米国では、IEC C13 to NEMA 5-15P 電源コードが必要です。
- ヨーロッパの一部では、IEC C13 to CEE 7/7 電源コードが必要な場合があります。
- インドでは、IEC C13 to IS1293 電源コードが必要です。

電源の冗長性

サーバーには複数の電源接続があり、電源冗長動作を実現するケーブルが同梱されています。電源の冗長化をお勧めしますが、冗長性は必須ではありません。

サーバーには無停電電源装置 (UPS) が備わっていません。

注文の履行

注文を処理するために AWS 、レールマウント、必要な電源ケーブル、ネットワークケーブルを含む Outposts sサーバー機器を、指定された住所に発送します。サーバーが発送される箱の寸法は次のとおりです。

- 2U サーバーの箱:
  - 長さ:44 インチ/11.8 センチメートル
  - 高さ: 26.5 インチ/67.3 cm
  - 幅: 17 インチ/43.2 cm
- 1U サーバーの箱:
  - 長さ: 34.5 インチ/87.6 cm
  - 高さ: 24 インチ/61 cm
  - 幅: 9 インチ/22.9 cm

お客様のチームまたはサードパーティーのプロバイダーが機器を取り付ける必要があります。詳細については、「Outpost サーバーのインストール」を参照してください。

Outposts サーバーの Amazon EC2 AWS キャパシティが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。

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 サーバーのインストール
- Outpost サーバー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 を所有する AWS アカウントでログインします。サイトと Outpost を作成します。そして、必要な Outposts サーバーの注文を行います。

前提条件

- Outposts サーバーで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 」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。営業住所は、Outposts サーバーを設置して動作させる場所です。サイトを作成すると、 は ID をサイトに AWS Outposts 割り当てます。Outpost を作成するときは、このサイトを指定する必要があります。

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、[サーバーのみ] 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. (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。
9. [サイトを作成] を選択します。

ステップ 2: Outpost を作成する

各サーバーで Outpost を作成します。Outpost は単一のサーバーにのみ関連付けることができます。注文を行う際に、この Outpost を指定できます。

前提条件

- サイトに関連付ける AWS アベイラビリティーゾーンを決定します。

Outpost を作成するには

1. ナビゲーションペインで、[Outpost] を選択します。

2. [Outpost の作成] を選択します。
3. [サーバー] 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. [サイト ID] には、自身のサイトを選択します。
7. [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 サーバーを注文します。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。部分前払いまたは前払いなしの支払いオプションを選択した場合は、3 年間にわたって月額料金を支払うことになります。

  価格設定には、配送、設置、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運用アドレス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、[サーバー] 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。
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

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、最大数量が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、容量が過剰か不足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。キャパシティタスク 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。

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。キャパシティタスク 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。

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、 AWS サポートにお問い合わせください。

注文を満たすために、 AWS は配送日をスケジュールします。

物理的な設置やネットワーク構成を含むすべての設置作業はお客様の責任となります。これらの作業は、サードパーティーと契約して代行してもらうことができます。インストールを自分で行う場合でも、サードパーティーに依頼する場合でも、インストールには、新しいデバイスの ID を確認するのに Outpost を含む AWS アカウント に IAM 認証情報が必要です。このアクセスを提供および管理するのはお客様の責任です。詳細については、「the section called “Outpost サーバーのインストール”」を参照してください。

お客様の Outpost 用の Amazon EC2 キャパシティが、 AWS アカウントからご利用いただけるようになったらインストールは完了です。容量が利用可能になると、Outpost サーバーで Amazon EC2 インスタンスを起動できます。詳細については、「the section called “インスタンスの起動”」を参照してください。

Outpost サーバーのインストール

Outpost サーバーを注文する場合、自分で行うかサードパーティーに依頼するかにかかわらず、インストールはお客様の責任となります。インストール者には、新しいデバイスの ID を確認するための特定の権限が必要です。詳細については、「権限を付与する」を参照してください。

前提条件

お使いのサイトに Outpostサーバーフォームファクタが必要です。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。

> **Note**
>
> インストールプロセス前およびインストールプロセス中に、インストール AWS Outposts サーバーのトレーニングビデオを表示することをお勧めします。トレーニングにアクセスするには、AWS Skill Builderにサインインするか、アカウントを作成する必要があります。

タスク

- ステップ 1: のアクセス許可を付与する
- ステップ 2: 検査する

- ステップ 3: ラックマウント
- ステップ 4: 電源を入れる
- ステップ 5: ネットワークを接続する
- ステップ 6: サーバーを承認する
- Outpost 構成ツールのコマンド リファレンス

ステップ 1: のアクセス許可を付与する

新しいデバイスの ID を検証するには、Outpost を含む AWS アカウント の IAM 認証情報が必要です。AWSOutpostsAuthorizeServerPolicy ポリシーは、Outpost サーバーのインストールに必要な権限を付与します。詳細については、「the section called “ID およびアクセス管理”」を参照してください。

考慮事項

- にアクセスできないサードパーティーを使用している場合は AWS アカウント、一時的なアクセスを提供する必要があります。
- AWS Outposts では、一時的な認証情報の使用がサポートされています。最大 36 時間有効な一時認証情報を設定することができます。サーバーのインストールのすべての手順を行うのに十分な時間をインストール者に与えてください。詳細については、「the section called “一時認証情報”」を参照してください。

ステップ 2: 検査する

Outposts 機器の検査を完了するために、配送パッケージの損傷を確認し、配送パッケージを開梱し、Nitro Security Key (NSK) を見つけるべきです。サーバーの検査については、以下の情報を考慮してください。

- 出荷パッケージには、箱の一番大きな 2 つの側面に衝撃センサーがあります。
- 出荷パッケージの内側の羽蓋には、サーバーの開梱方法と NSK の場所に関する指示が記載されています。
- NSK は暗号化モジュールです。検査を完了するために、NSK を見つけます。NSK を後のステップでサーバーにアタッチします。

出荷パッケージを確認する

出荷パッケージを検査するには

- 出荷パッケージを開封する前に、両方の衝撃センサーを確認し、それらが作動したかどうかを記録します。衝撃センサーが作動していた場合、ユニットが損傷している可能性があります。サーバーやアクセサリにさらなる損傷がないか時間をかけて注意しながらインストールを進めてください。システムの一部が明らかに損傷している場合、またはインストールが期待どおりに進まない場合は、 AWS サポートに連絡して Outposts サーバーの交換に関するガイダンスを依頼してください。

センサーの中央にあるバーが赤色の場合、センサーは作動しています。

配送パッケージを開梱します

出荷パッケージを開梱するには

- パッケージを開いて、次のものが入っていることを確認します。
  - [サーバー]

- Nitro Security Key (暗号化モジュール) - 赤の「NSK」というマークが付いたパッケージ。詳細については、出荷パッケージから NSK を見つけるための次の手順を参照してください
- ラック取り付けキット (内部レール 2 個、外部レール 2 個、ネジ)
- インストールパンフレット
- アクセサリキット
  - C13/14 電源ケーブルのペア - 10 フィート (3m)
  - QSFP ブレークアウト ケーブル - 10 フィート (3m)
  - USB ケーブル、micro-USB - USB-C へ-10 フィート (3m)
  - ブラシガード

NSK を探す

NSK は、サーバーのアクセサリが入った「A」というラベルが貼られた箱の中にあります。

> **Important**
>
> インストール中は NSK を使用してサーバー上のデータを破壊しないでください。

NSK はサーバーをアクティブ化するために必要です。NSK は、サーバーを返送する際にサーバー上のデータを破壊するのにも使用されます。このインストールステップでは、NSK 本体の指示はデータを破壊するためのものであるため無視してください。

ステップ 3: ラックマウント

このステップを完了するには、サーバーに内部レールを取り付け、ラックに外部レールを取り付け、その後サーバーをラックに取り付ける必要があります。これらのステップを完了するには、プラスドライバーが必要です。

ラックマウントの代替品

サーバーをラックに取り付ける必要はありません。ラックにサーバーを取り付けない場合、以下の情報を考慮してください。

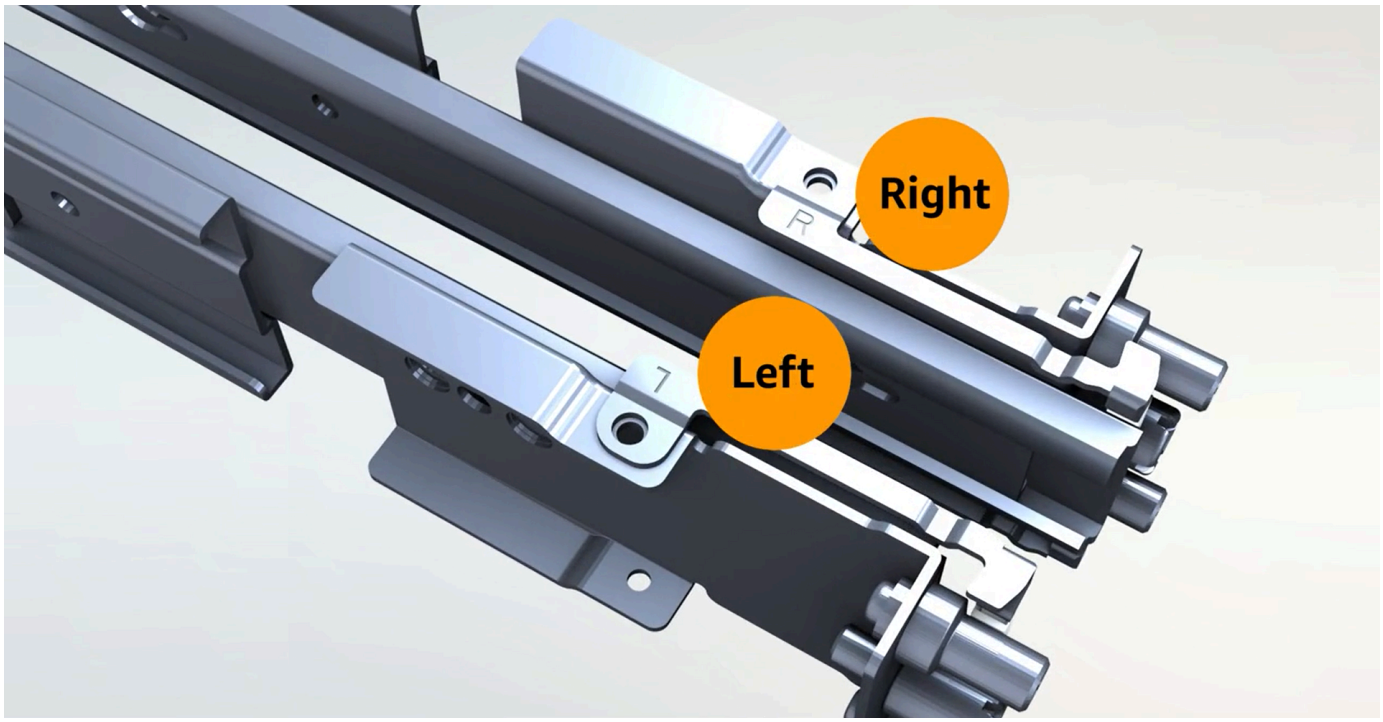
- サーバーと前後の壁の間には、熱い空気が循環できるように最低 6 インチ (15 センチメートル) の隙間を確保してください。
- サーバーは、湿気や落下物などの機械的危険のない安定した面に置きます。

- サーバーに付属のネットワーク ケーブルを使用するには、サーバーを上流のネットワーク デバイスから 3 m (10 フィート) 以内に配置する必要があります。
- 地元の指針に従って、地震補強およびボンディングを行ってください。

側面と端を識別する

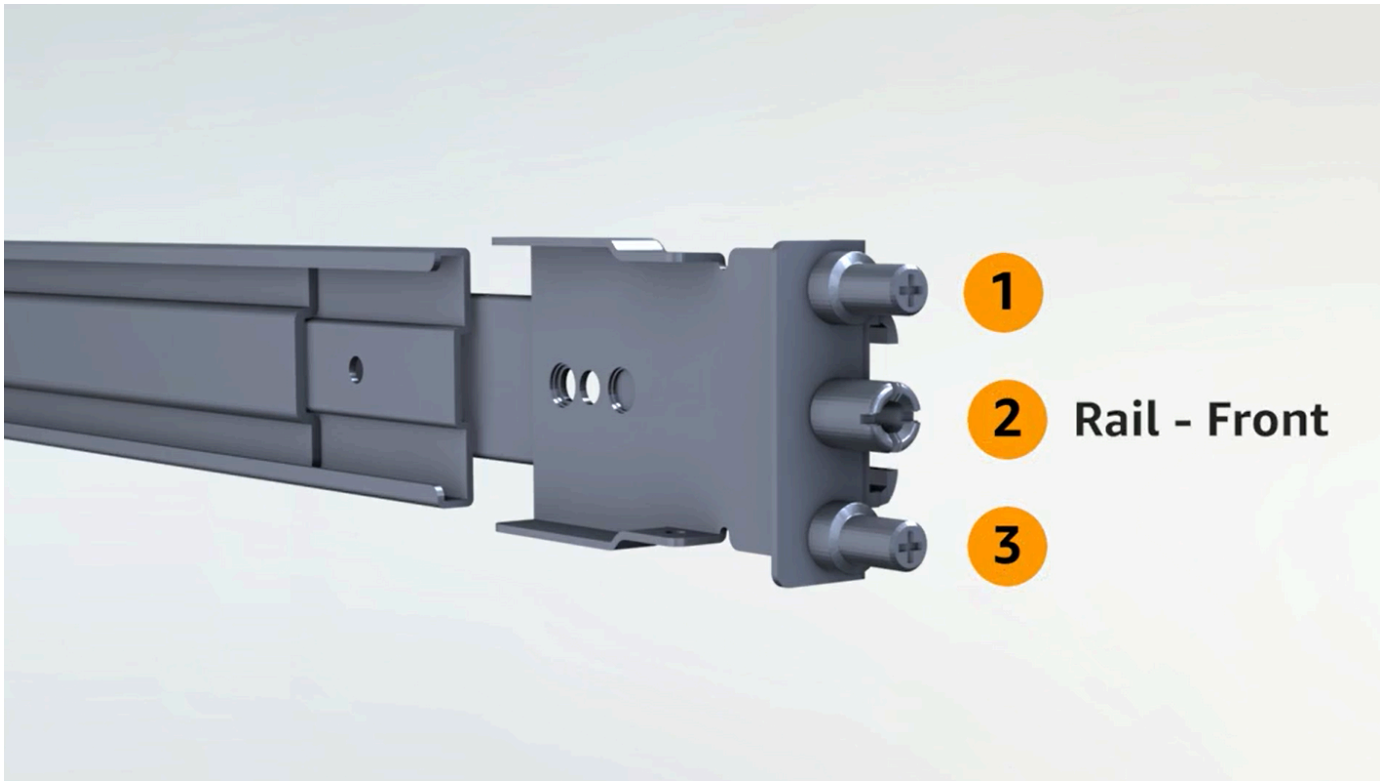
左と右、前と後ろを識別するには

1. サーバーと一緒に届いたラックのレールの箱を見つけ、開けます。
2. レールの刻印を見て左右を判断してください。これらのマーキングにより、各レールがサーバーのどちら側に接続されるかが決まります。

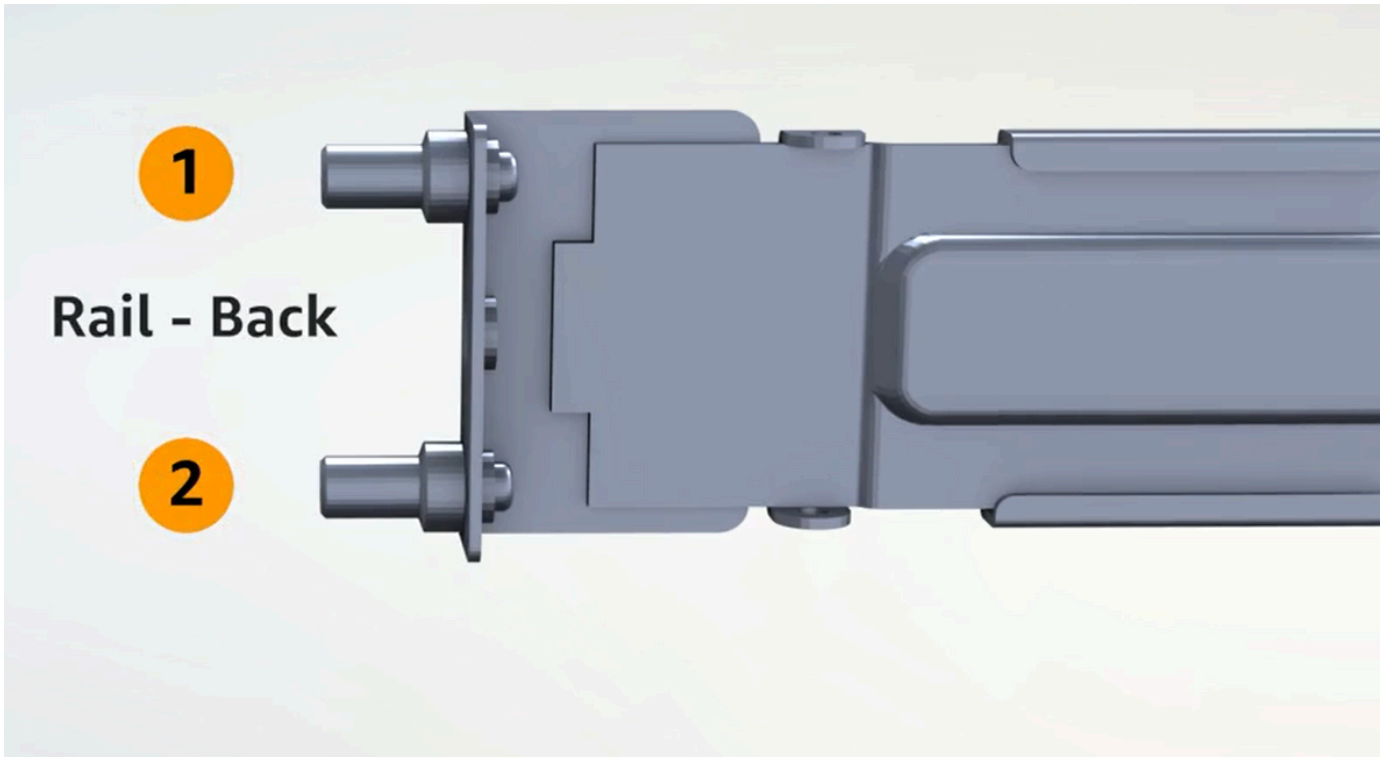


3. レールの両端の柱を見て、どちらが前でどちらが後ろかを判断します。

   フロントエンドには 3 つのポストがあります。



バックエンドには 2 つのポストがあります。



インナーレールを取り付ける

内側レールをサーバーに取り付けるには

1. 両レールともインナーレールをアウターレールから外します。レールは 4 つあるはずです。
2. 右内側レールを本体右側面に取り付け、ネジで固定します。サーバーに対してレールの向きが正しいことを確認してください。レールの前部をサーバーの正面に向けます。
3. 左内側レールを本体左側面に取り付け、ネジで固定します。

外側レールを取り付ける

外側レールをラックに取り付けるには

1. ラックに向かって右側の R とマークされたレールを使用します。まずレールの背面をラックに取り付けてから、レールを延長してラックの前面に接続します。

   > **Tip**
   >
   > レールの向きに注意してください。必要に応じて、付属のピンアダプターを使用してください。

2. 左側の左側のレールでも同じ手順を繰り返します。

サーバーをマウントする

サーバーをラックに取り付けるには

- 前の手順でラックに取り付けた外側レールにサーバーをスライドさせ、付属の 2 本のネジでサーバーの前面を固定します。

  > **Tip**
  >
  > 2 人でサーバーをラックにスライドさせます。

ステップ 4: 電源を入れる

電源投入を完了するには、NSK を接続し、サーバーを電源に接続し、サーバーの電源が入っていることを確認します。サーバーへの電力供給については、次の情報を考慮してください。

- サーバーは 1 つの電源で機能しますが、冗長性のために 2 つの電源を使用する AWS ことをお勧めします。
- ネットワーク ケーブルを接続する前に、電源ケーブルを接続します。
- C13 アウトレット/C14 インレット電源ケーブルのペアを使用して、サーバーをラック上の電源に接続します。C14 インレット電源ケーブルを使用してサーバーをラック上の電源に接続していない場合は、電源に接続する C14 インレット用のアダプターを用意する必要があります。

NSK を取り付ける

動作中にサーバー上のデータを復号化できるように、NSK をサーバーに接続する必要があります。

Important

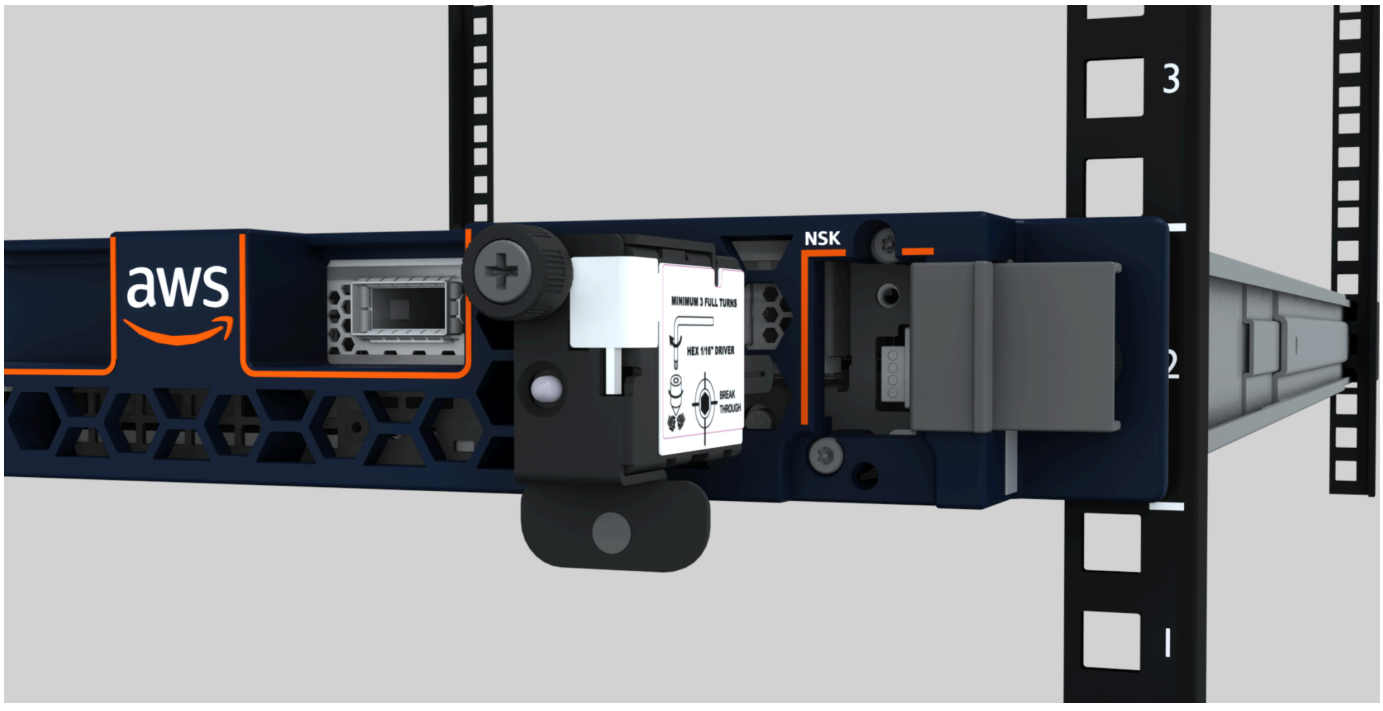
- NSK の側面には NSK の破壊方法が記載されています。この時点では、それらの指示には従わないでください。これらの手順は、サーバーを AWSに返送する前にサーバー上のデータを暗号化してシュレッドする場合にのみ実行してください。
- 複数のサーバーを同時にインストールする場合は、NSK を混同しないようにしてください。NSK は、同梱されているサーバーに接続する必要があります。別の NSK を使用すると、サーバーは起動しません。

NSK を取り付けるには

1. サーバーの前面右側にある NSK コンパートメントを開きます。

   次の図は、2U サーバーに接続された NSK を示しています。

次の図は、1U サーバーに接続された NSK を示しています。

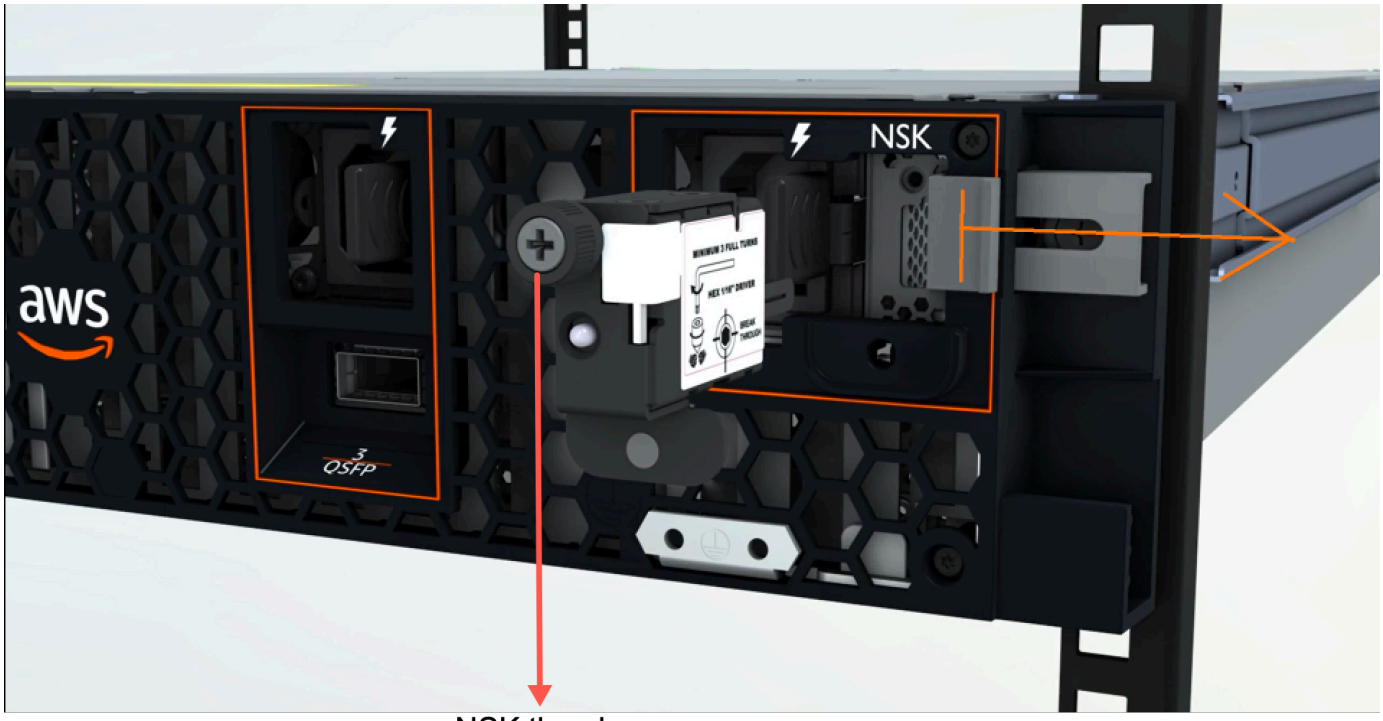


2. NSK のシリアル番号 (SN) が、サーバーの NSK コンパートメントのベゼル引き出しタブの SN と一致していることを確認します。

   次の図は、NSK とベゼルの引き出しタブの SN 番号を示しています。

3. NSK をスロットに差し込みます。
4. 親指ねじまたはドライバーを使用して手で締め込み、締め付けるまで (0.7 Nm / 0.52 lb-ft) 締め込んでください。電動工具は使用しないでください。NSK を過度なトルクで損傷する可能性があります。

   次の図は、蝶ねじの位置を示しています。



NSK thumbscrew

次の図は、NSK をサーバーに取り付ける際に使用できるドライバーの種類を示しています。

電源を入れる

サーバーを電源に接続するには

1. サーバーに付属していた C13/C14 電源ケーブルのペアを見つけてください。

2. 両方のケーブルの C14 端子を電源に接続してください。
3. 両方のケーブルの C13 端子をサーバーの前面のポートに接続してください。

サーバーの電源を確認する

サーバーに電源があることを確認するには

1. サーバーが稼働している音が聞こえるかを確認してください。

> **Tip**
>
> サーバーが自己プロビジョニングを完了すると、騒音レベルが低下します。

2. LED 電源ライトが電源ポートの上に点灯しているか確認してください。

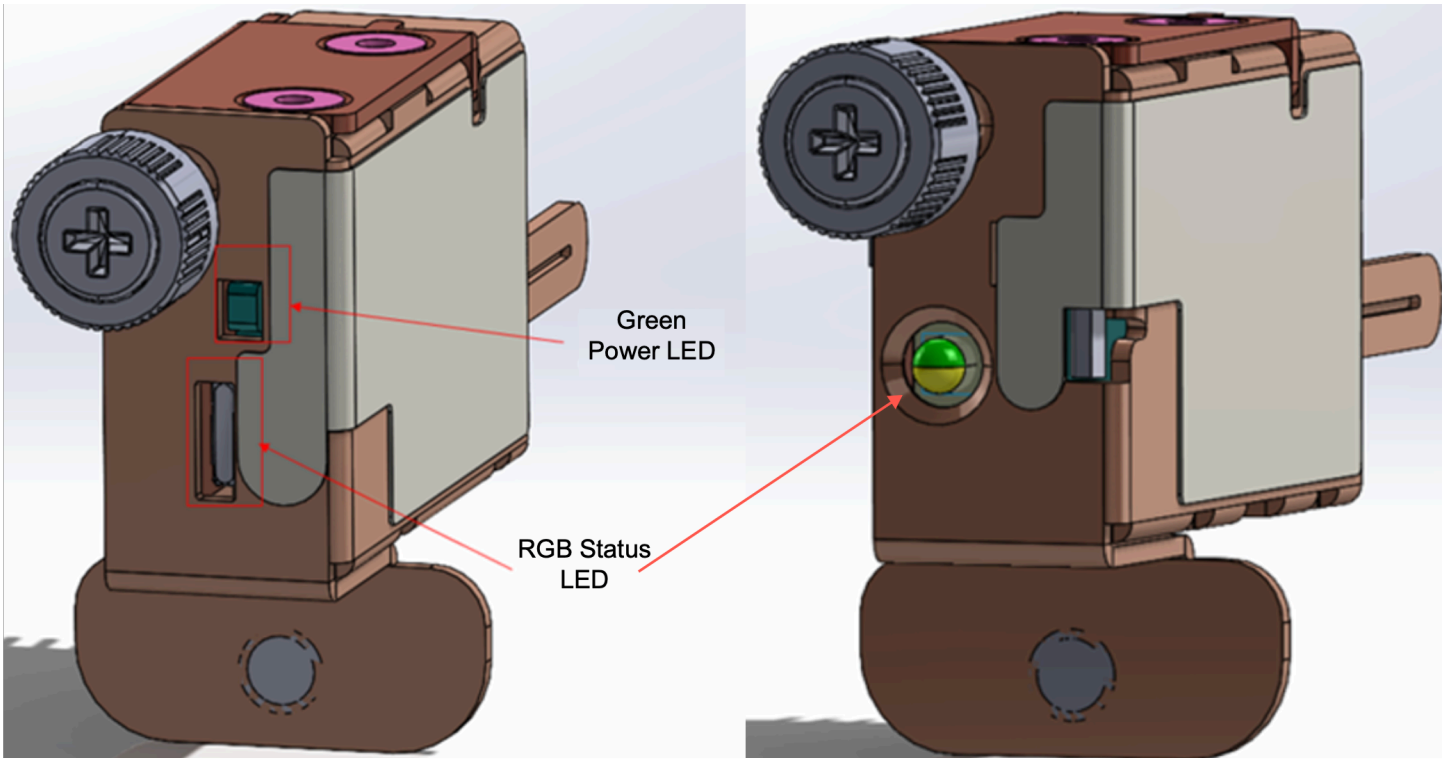
   次の図は、2U サーバーの LED 電源ライトを示しています。

   次の図は、1U サーバーの LED 電源ライトを示しています。

Atlas 3.0 の電源 LED を確認します。NSK

AWS Outposts は、Atlas 2.0 と Atlas 3.0 の 2 つのバージョンの NSK をサポートしています。どちらの NSK バージョンにも RGB ステータス LED があります。さらに、Atlas 3.0 には緑色の電源 LED があります。このステップは、Atlas 3.0 NSK 専用です。

次の画像は、Atlas 2.0 および Atlas 3.0 NSKs 上の LEDs の位置を示しています。



Atlas 3.0 Atlas 2.0

Atlas 2.0 NSK を使用している場合は、次のステップに進みます。このバージョンの NSK には RGB ステータス LED のみがあり、Outpost サーバーがプロビジョニングされてアクティブ化された後に確認する必要があるステップ 5: ネットワークを接続するためです。

Atlas 3.0 NSK を使用している場合は、緑色の電源 LED を確認します。

- 緑色のライトがオンになっている場合、NSK はホストに正しく接続されており、電源があります。次のステップに進むことができます。
- 緑色のライトがオフの場合、NSK はホストに正しく接続されていないか、電源がありません。にお問い合わせください AWS Support。

ステップ 5: ネットワークを接続する

ネットワークのセットアップを完了するために、サーバーを上流のネットワーキングデバイスにネットワークケーブルで接続します。

ネットワークへの接続については、以下の情報を考慮してください。

- サーバーには、サービスリンクトラフィックとローカルネットワークインターフェイス (LNI) リンクトラフィックの 2 種類のトラフィックに対する接続が必要です。以下のセクションの指示は、

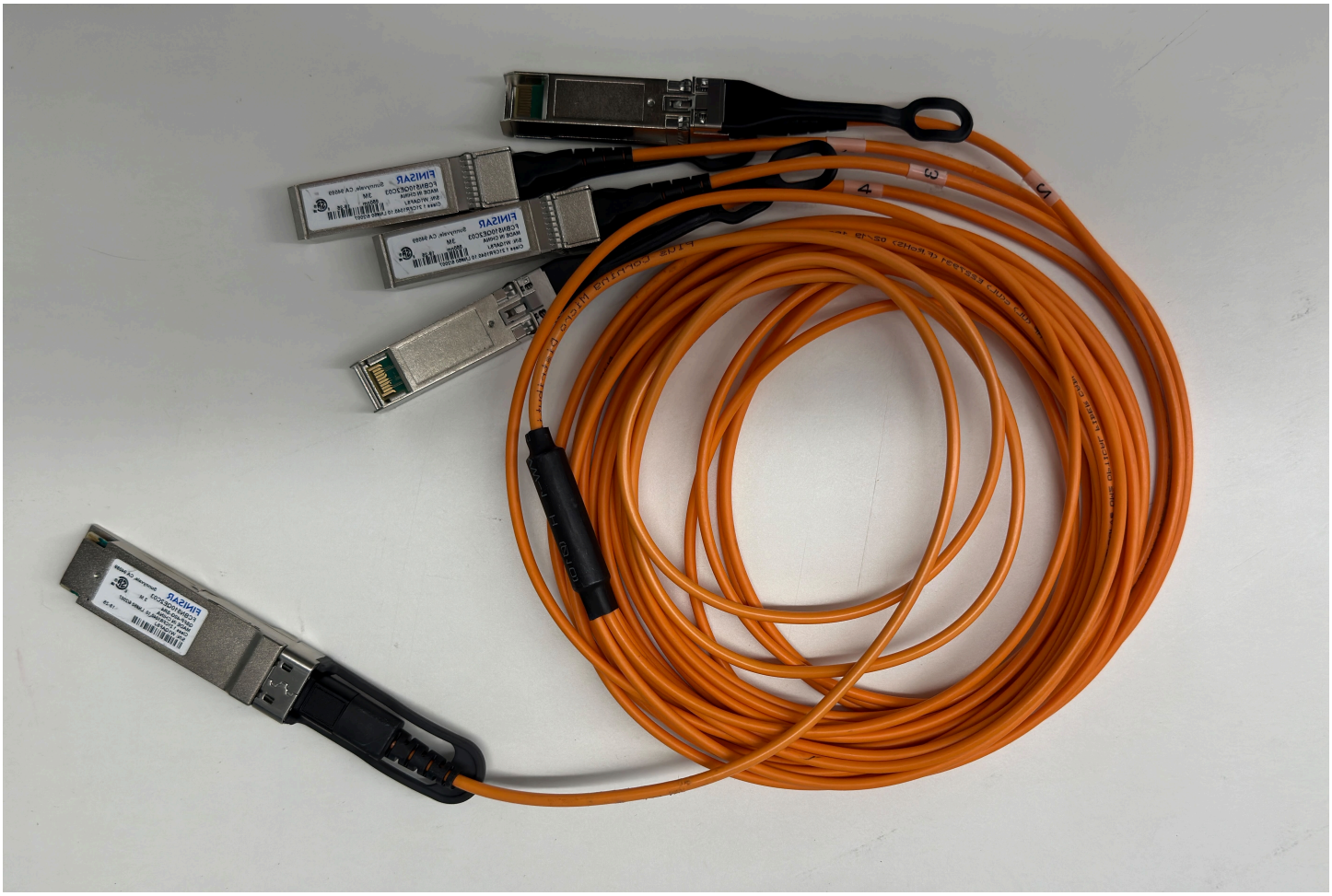
トラフィックをセグメント化するためにサーバー上でどのポートを使用するかを説明しています。お使いの上流のネットワーキングデバイス上で、各タイプのトラフィックを担当するべきポートを決定するために、IT グループと相談してください。

- サーバーが上流のネットワーキングデバイスに接続され、IP アドレスが割り当てられていることを確認してください。詳細については、「サーバー IP アドレスの割り当て」を参照してください。
- AWS Outposts サーバーの光接続は 10 Gbit のみをサポートし、ポート速度の自動ネゴシエーションはサポートしていません。ホストポートがポート速度を 10 Gbit から 25 Gbit までの範囲でネゴシエーションしようとする場合、問題が発生する可能性があります。そのような場合、以下の手順をお勧めします：
  - スイッチポートのポート速度を 10 Gbit に設定してください。
  - スイッチのベンダーと協力して、静的な構成をサポートするようにしてください。

QSFP ネットワークの構成

QSFP ブレークアウトケーブルを使用する場合、ブレークアウトを使用してトラフィックをセグメント化します。

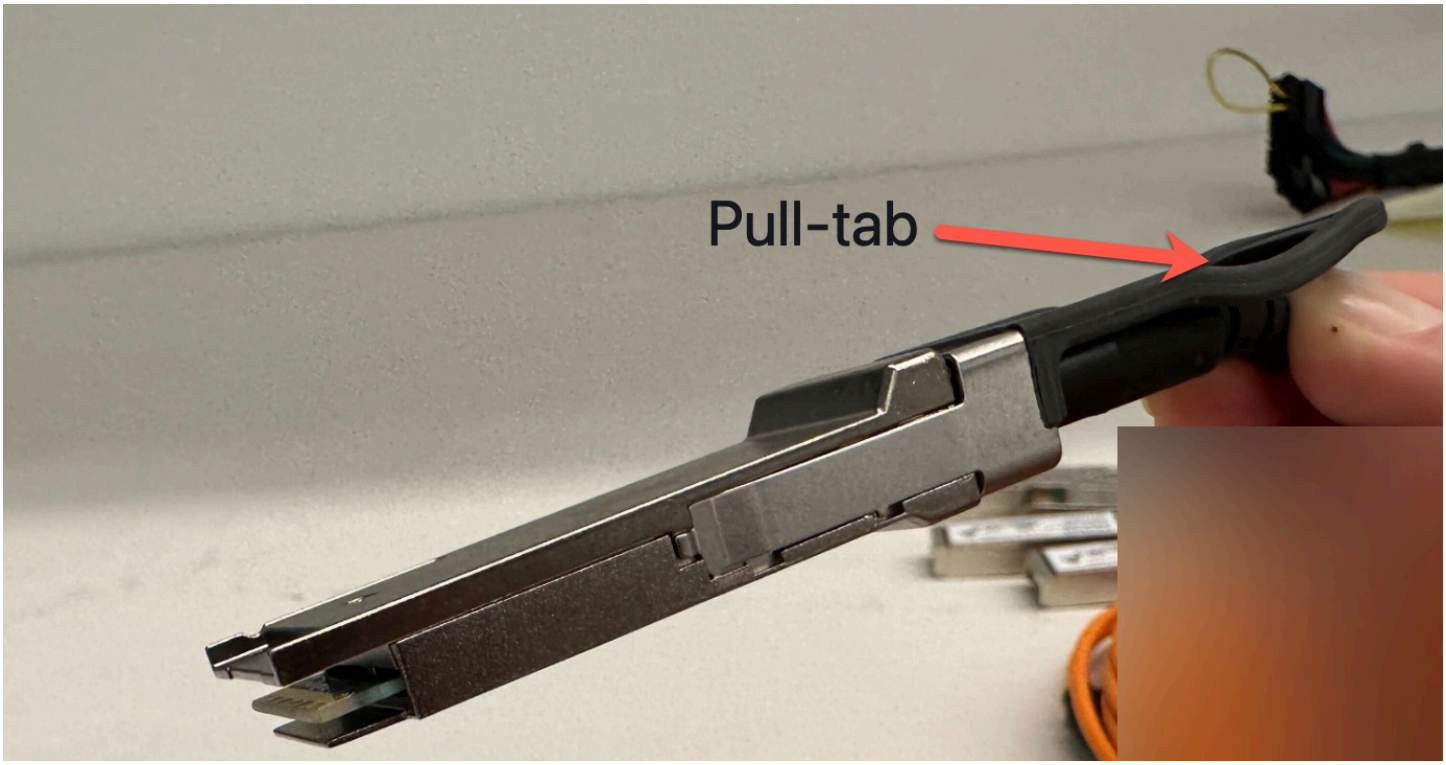
次の図は、QSFP ブレークアウトケーブルを示しています。



> **Note**
>
> AWS Outposts サーバーには、QSFP ポートの横に物理 RJ45 ポートがあります。ただし、この RJ45 ポートはお客様による使用では有効になっていません。RJ45 1GbE 接続が必要な場合は、付属の QSFP ケーブルを使用して 10GBASE-X SFP+ を 1GbE RJ45 メディアコンバータに接続します。

QSFP ケーブルの一方の端には単一のコネクタがあります。このエンドをサーバーに接続します。

次の図は、1 つのコネクタがあるケーブルの端を示しています。



QSFP ケーブルのもう一方の端には、1 から 4 までラベル付けされた 4 本のブレークアウトケーブルがあります。LNI リンク トラフィックには 1 というラベルの付いたケーブルを使用し、サービス リンク トラフィックには 2 というラベルの付いたケーブルを使用します。

次の図は、4 本のブレークアウトケーブルがあるケーブルの端を示しています。

QSFP ブレークアウトケーブルでサーバーをネットワークに接続するには

1. サーバーに付属の QSFP ブレークアウト ケーブルを見つけます。
2. QSFP ブレークアウト ケーブルの片端をサーバーの QSFP ポートに接続します。

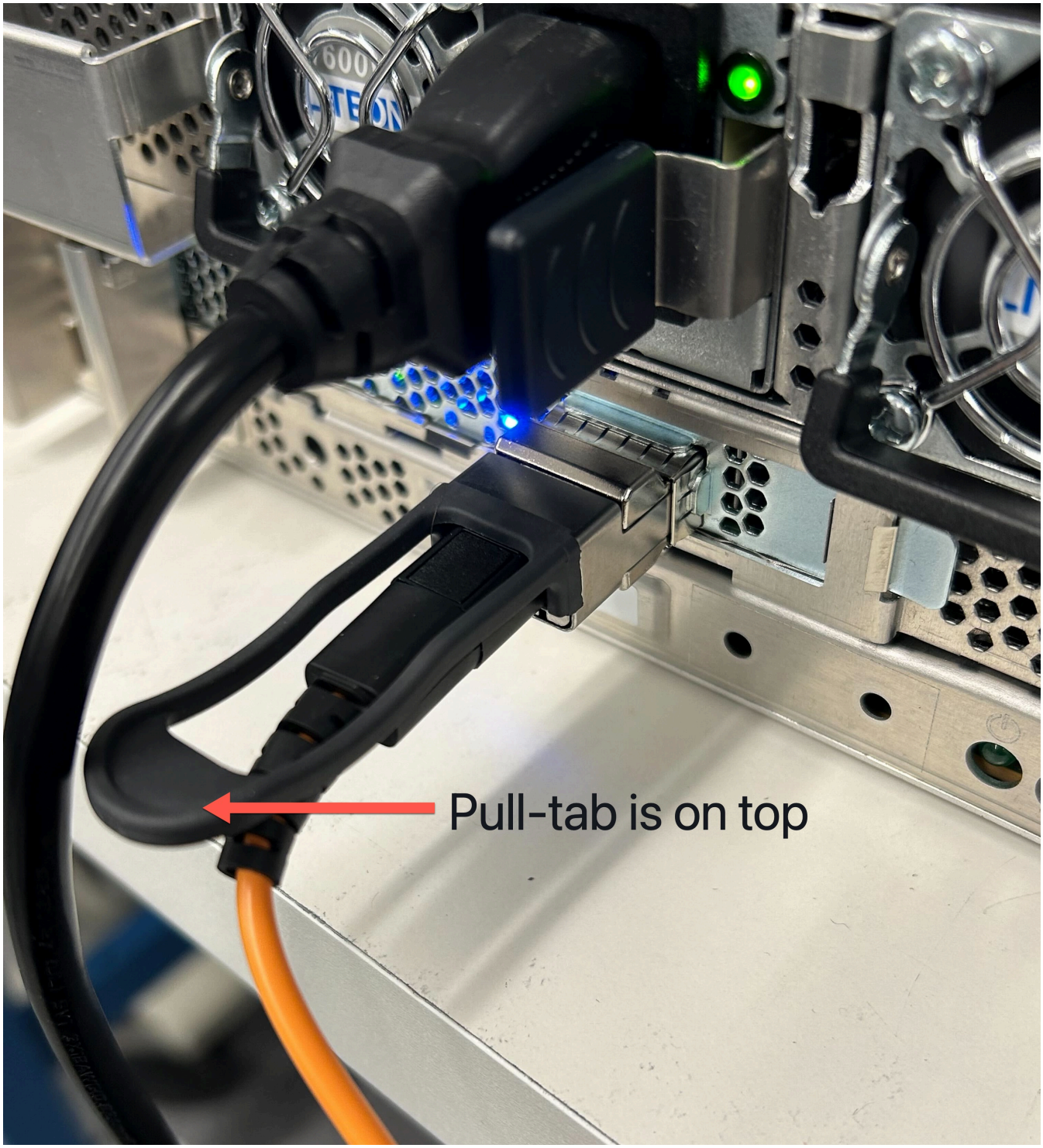
    1. QSFP ポートを見つけます。

        次の画像は、2U サーバー上の QSFP ポートの位置を示しています。

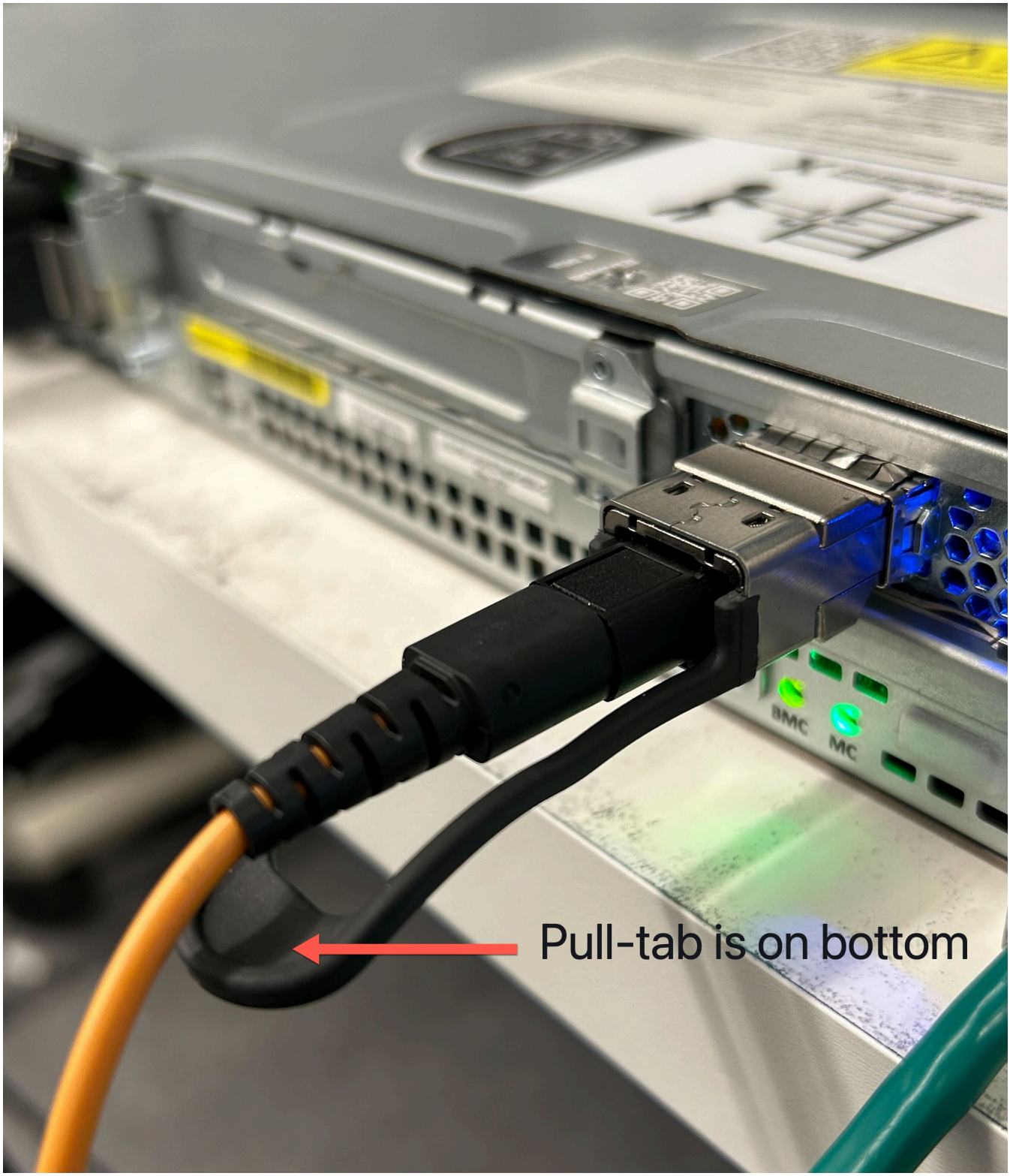
次の画像は、1U サーバー上の QSFP ポートの位置を示しています。

2. プルタブを正しい向きにして QSFP を差し込みます。

   2U サーバの場合は、次の図のようにプルタブを上にして QSFP を接続します。



1U サーバの場合は、次の図に示すように、QSFP を下部のプルタブで接続します。



3. ケーブルを差し込むときに、カチッという音がすることを確認してください。これは、ケーブルが正しく接続されていることを示します。

3. QSFP ケーブルのブレークアウト 1 と 2 を上流のネットワーク デバイスに接続します。

> **Important**
>
> Outpost サーバーが機能するには、次の両方のケーブルが必要です。
>
> - LNI リンク トラフィックには 1 というラベルの付いたケーブルを使用します。
> - サービスリンクトラフィックには 2 というラベルの付いたケーブルを使用してください。

ステップ 6: サーバーを承認する

サーバーを認証するには、USB ケーブルでノート PC をサーバーに接続し、コマンドベースのシリアルプロトコルを使用して接続をテストし、サーバーを認証する必要があります。これらのステップを完了するには、IAM 認証情報に加えて、USB ケーブル、ノート PC、および PuTTY や screen などのシリアルターミナルソフトウェアが必要です。

また、USB On The Go (OTG) に対応した USB-C コネクタまたは micro-USB コネクタを搭載した Android スマートフォンまたはタブレットをお使いの場合は、Outposts Server Activator アプリを使用してサーバー認証プロセスを段階的に実行できます。Google Play からアプリをダウンロードできます。

サーバーの認証については、以下の情報を考慮してください。

- サーバーを認証するには、ユーザーまたはサーバーをインストールする関係者が、Outpost AWS アカウント を含む に IAM 認証情報が必要です。詳細については、「the section called “ステップ 1: のアクセス許可を付与する”」を参照してください。
- 接続をテストするのに IAM 認証情報で認証する必要はありません。
- export コマンドを使用して IAM 認証情報を環境変数として設定する前に、接続をテストすることを検討してください。
- アカウントを保護するために、Outpost Configuration Tool は IAM 認証情報を保存しません。
- ノート PC をサーバーに接続するには、常に USB ケーブルをまずラップトップに差し込み、次にサーバーに差し込みます。

タスク

- ノート PC をサーバーに接続する
- サーバーにシリアル接続を作成してください。

- 接続をテストする
- サーバーを認証する
- NSK LEDsを確認する

ノート PC をサーバーに接続する

USB ケーブルをまずノート PC に接続し、次にサーバーに接続します。サーバーには、ノート PC で利用可能な仮想シリアルポートを作成する USB チップが備わっています。この仮想シリアルポートを使用して、シリアルターミナルエミュレーションソフトウェアを使ってサーバーに接続することができます。この仮想シリアルポートは、Outpost Configuration Tool のコマンドを実行するためにのみ使用できます。

ノート PC をサーバーに接続するには

USB ケーブルをまずノート PC に接続し、次にサーバーに接続します。

> **Note**
>
> USB チップには、仮想シリアルポートを作成するためのドライバが必要です。必要なドライバがまだインストールされていない場合、オペレーティングシステムは自動的にそれらをインストールするはずです。ドライバをダウンロードしてインストールするには、FTDI の「インストールガイド」 を参照してください。

サーバーにシリアル接続を作成してください。

このセクションには、一般的なシリアルターミナルプログラムの使用方法に関する手順が含まれていますが、これらのプログラムを使用する必要はありません。接続速度が 115200 ボーの好みのシリアルターミナルプログラムを使用してください。

例

- Windows におけるシリアル接続
- Mac のシリアル接続

Windows におけるシリアル接続

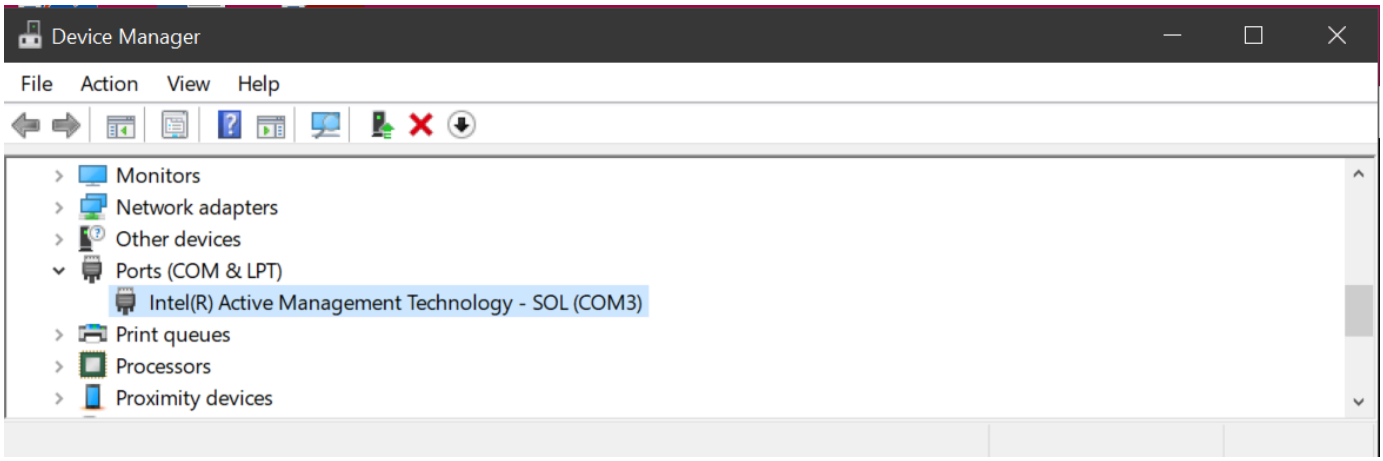
次の手順は Windows 上の PuTTY 用です。PuTTY は無料ですが、ダウンロードする必要があるかもしれません。

PuTTY をダウンロードしてください。

PuTTY のダウンロードページから、PuTTY をダウンロードしてインストールします。

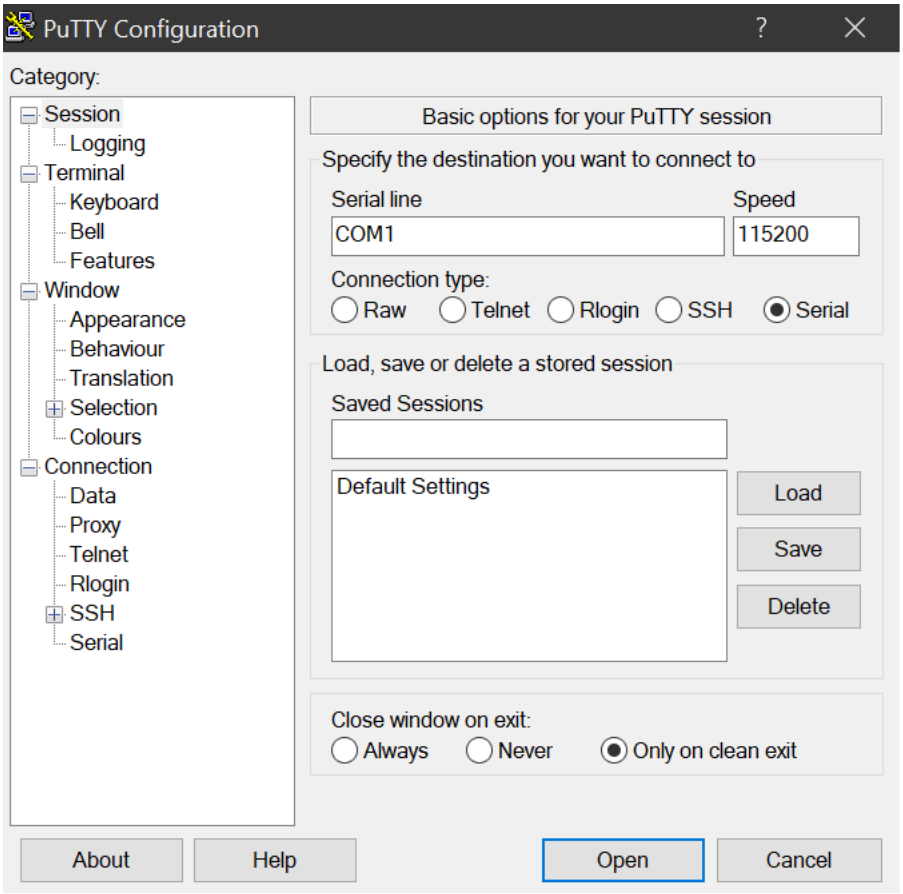
PuTTY を使用して Windows にシリアルターミナルを作成するには

1. まず USB ケーブルを Windows ノート PC に接続し、次にサーバーに接続します。
2. デスクトップから [スタート] を右クリックし、[デバイスマネージャ] を選択します。
3. [デバイスマネージャー] で、[ポート (COM と LPT)] を展開して USB シリアル接続の COM ポートを指定します。[USB シリアルポート (COM #)] という名前のノードが表示されます。COM ポートの値は、お使いのハードウェアに依存します。



4. PuTTY の [セッション] で、[接続タイプ] に [シリアル] を選択し、次の情報を入力します。
   - [シリアルライン] に、デバイスマネージャの COM # ポートを入力します。
   - [速度] に、115200 を入力します。

   次の図は、[PuTTY 設定] ページの例を示しています。



5. 開く をクリックします。

   空のコンソール ウィンドウが表示されます。次のいずれかが表示されるまで、1〜2 分かかることがあります :

   - `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
   - `Outpost>` プロンプト。

Mac のシリアル接続

次の手順は screen macOS での手順です。screen オペレーティング システムに含まれています。

次を使用して macOS でシリアル ターミナルを作成するには screen

1. USB ケーブルをまず Mac ノートPCに差し込み、次にサーバーに接続します。
2. ターミナルで、/dev を *usb* でフィルターして一覧表示し、仮想シリアルポートを探します。

```
ls -ltr /dev/*usb*
```

シリアルデバイスは tty として表示されます。例えば、前の list コマンドからの次の出力例を考えてみましょう。

```
ls -ltr /dev/*usb*
crw-rw-rw-  1 root  wheel   21,   3 Feb  8 15:48 /dev/cu.usbserial-EXAMPLE1
crw-rw-rw-  1 root  wheel   21,   2 Feb  9 08:56 /dev/tty.usbserial-EXAMPLE1
```

3. ターミナルで、シリアル接続のシリアルデバイスとボーレートに screen を使用してシリアル接続を設定します。次のコマンドで、*EXAMPLE1* をノート PC の値に置き換えます。

```
screen /dev/tty.usbserial-EXAMPLE1 115200
```

空のコンソール ウィンドウが表示されます。次のいずれかが表示されるまで、1〜2 分かかることがあります：

- `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
- `Outpost>` プロンプト。

接続をテストする

このセクションでは、Outpost 構成ツールを使用して、接続をテストする方法について説明します。接続をテストするために IAM 認証情報は必要ありません。 AWS リージョンにアクセスするには、接続で DNS を解決できる必要があります。

1. リンクをテストし、接続に関する情報を収集する
2. DNS リゾルバのテスト
3. へのアクセスをテストする AWS リージョン

リンクをテストするには

1. まず USB ケーブルをノート PC に差し込み、次にサーバーに差し込みます。

2. PuTTY や screen などのシリアルターミナルプログラムを使用して、サーバーに接続します。詳細については、「the section called “サーバーにシリアル接続を作成してください。”」を参照してください。
3. Enter を押して Outpost Configuration Tool のコマンドプロンプトにアクセスします。

```
Outpost>
```

> **Note**
>
> 電源を入れた後、サーバーのシャーシ内側の左側で赤い光が点灯し続け、Outpost Configuration Tool に接続できない場合は、続行するのにサーバーの電源を切ってドレインする必要がある場合があります。サーバーをドレインするには、すべてのネットワークケーブルと電源ケーブルを切断し、5 分待ってから電源を入れて再びネットワークに接続してください。

4. describe-links を使用して、サーバーのネットワークリンクに関する情報を取得します。Outpost サーバーは、1 つのサービスリンクと 1 つのローカルネットワークインターフェイス (LNI) リンクを持っている必要があります。

```
Outpost>describe-links
---
service_link_connected: True
local_link_connected: False
links:
-
  name: local_link
  connected: False
  mac: 00:00:00:00:00:00
-
  name: service_link
  connected: True
  mac: 0A:DC:FE:D7:8E:1F
checksum: 0x46FDC542
```

いずれかのリンクで `connected: False` を取得した場合は、ハードウェア上のネットワーク接続のトラブルシューティングを行ってください。

5. describe-ip を使用して、サービスリンクの IP 割り当てステータスと設定を返します。

```
Outpost>describe-ip
```

```
---
links:
-
  name: service_link
  configured: True
  ip: 192.168.0.0
  netmask: 255.255.0.0
  gateway: 192.168.1.1
  dns: [ "192.168.1.1" ]
  ntp: [ ]
checksum: 0x8411B47C
```

NTP の値は、DHCP オプションセットではオプションであるため、欠落している可能性があります。他に欠落している値はありません。

DNS をテストするには

1. まず USB ケーブルをノート PC に差し込み、次にサーバーに差し込みます。
2. PuTTY や screen などのシリアルターミナルプログラムを使用して、サーバーに接続します。詳細については、「the section called “サーバーにシリアル接続を作成してください。”」を参照してください。
3. Enter を押して Outpost Configuration Tool のコマンドプロンプトにアクセスします。

```
Outpost>
```

> **Note**
>
> 電源を入れた後、サーバーのシャーシ内側の左側で赤い光が点灯し続け、Outpost Configuration Tool に接続できない場合は、続行するのにサーバーの電源を切ってドレインする必要がある場合があります。サーバーをドレインするには、すべてのネットワークケーブルと電源ケーブルを切断し、5 分待ってから電源を入れて再びネットワークに接続してください。

4. export を使用して、Outpost サーバーの親リージョンを AWS_DEFAULT_REGION の値として入力します。

```
AWS_DEFAULT_REGION=#####
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: 0xB2A945RE
```

- 等号 (=) の前後にスペースを入れないでください。
- 環境変数は保存されません。Outpost Configuration Tool を実行する AWS リージョン たびにエクスポートする必要があります。
- サーバーのインストールをサードパーティーに依頼する場合、そのサードパーティーに親リージョンを提供する必要があります。

5. describe-resolve を使用して、Outpost サーバーが DNS リゾルバーに到達し、リージョン内の Outpost 構成エンドポイントの IP アドレスを解決できるかどうかを判断します。IP 構成を含むリンクが少なくとも 1 つ必要です。

```
Outpost>describe-resolve
---
dns_responding: True
dns_resolving: True
dns: [ "198.xx.xxx.xx", "198.xx.xxx.xx" ]
query: outposts.us-west-2.amazonaws.com
records: [ "18.xxx.xx.xxx", "44.xxx.xxx.xxx", "44.xxx.xxx.xxx" ]
checksum: 0xB6A961CE
```

へのアクセスをテストするには AWS リージョン

1. まず USB ケーブルをノート PC に差し込み、次にサーバーに差し込みます。
2. PuTTY や screen などのシリアルターミナルプログラムを使用して、サーバーに接続します。詳細については、「the section called “サーバーにシリアル接続を作成してください。”」を参照してください。
3. Enter を押して Outpost Configuration Tool のコマンドプロンプトにアクセスします。

```
Outpost>
```

> **Note**
>
> 電源を入れた後、サーバーのシャーシ内側の左側で赤い光が点灯し続け、Outpost Configuration Tool に接続できない場合は、続行するのにサーバーの電源を切ってドレインする必要がある場合があります。サーバーをドレインするには、すべてのネットワークケーブルと電源ケーブルを切断し、5 分待ってから電源を入れて再びネットワークに接続してください。

4. export を使用して、Outpost サーバーの親リージョンを AWS_DEFAULT_REGION の値として入力します。

   AWS_DEFAULT_REGION=*#####*

   ```
   Outpost>export AWS_DEFAULT_REGION=us-west-2

   result: OK
   checksum: 0xB2A945RE
   ```

   - 等号 (=) の前後にスペースを入れないでください。
   - 環境変数は保存されません。Outpost Configuration Tool を実行する AWS リージョン たびにエクスポートする必要があります。
   - サーバーのインストールをサードパーティーに依頼する場合、そのサードパーティーに親リージョンを提供する必要があります。

5. describe-reachability を使用して、Outpost サーバーがリージョン内の Outpost 構成エンドポイントに到達できるかどうかを判断します。機能する DNS 設定が必要です。これは、describe-resolve を使用して確認できます。

   ```
   Outpost>describe-reachability
   ---
   is_reachable: True
   src_ip: 10.0.0.0
   dst_ip: 54.xx.x.xx
   dst_port: xxx
   checksum: 0xCB506615
   ```

   - is_reachable テストの結果を示しています。
   - src_ip はサーバーの IP アドレスです。

- dst_ip は、リージョンの Outpost 構成エンドポイントの IP アドレスです。
- dst_port はサーバーが dst_ip への接続に使用したポートです。

サーバーを認証する

このセクションでは、Outpost Configuration Tool および Outpost を含む AWS アカウントからの IAM 認証情報を使用してサーバーを認可する方法について説明しています。

サーバーを認証するには

1. まず USB ケーブルをノート PC に差し込み、次にサーバーに差し込みます。
2. PuTTY や screen などのシリアルターミナルプログラムを使用して、サーバーに接続します。詳細については、「the section called “サーバーにシリアル接続を作成してください。”」を参照してください。
3. Enter を押して Outpost Configuration Tool のコマンドプロンプトにアクセスします。

```
Outpost>
```

> **Note**
>
> 電源を入れた後、サーバーのシャーシ内側の左側で赤い光が点灯し続け、Outpost Configuration Tool に接続できない場合は、続行するのにサーバーの電源を切ってドレインする必要がある場合があります。サーバーをドレインするには、すべてのネットワークケーブルと電源ケーブルを切断し、5 分待ってから電源を入れて再びネットワークに接続してください。

4. export を使用して IAM 認証情報を Outpost 構成ツールに入力します。サードパーティーを利用してサーバーをインストールする場合、IAM 認証情報をそのサードパーティーに提供する必要があります。

   認証するには、次の 4 つの変数を エクスポートする必要があります。変数は一度に 1 つずつエクスポートします。等号 (=) の前後にスペースを入れないでください。

   - AWS_ACCESS_KEY_ID=*access-key-id*
   - AWS_SECRET_ACCESS_KEY=*secret-access-key*
   - AWS_SESSION_TOKEN=*session-token*

- コマンドを使用して AWS CLI `GetSessionToken` を取得しますAWS_SESSION_TOKEN。詳細については、「AWS CLI コマンドリファレンス」の「get-session-toke」を参照してください。

  > **Note**
  >
  > を取得するには、IAM ロールに がアAWSOutpostsAuthorizeServerPolicyタッチされている必要がありますAWS_SESSION_TOKEN。

- をインストールするには AWS CLI、AWS CLI Verrsion 2 ユーザーガイドの「AWS CLI の最新バージョンのインストールまたは更新」を参照してください。

- AWS_DEFAULT_REGION=*#####*

  AWS_DEFAULT_REGION の値には Outpost サーバーの親リージョンを使用します。サーバーのインストールを第三者に依頼している場合、親リージョンをその第三者に提供する必要があります。

以下の例の出力は、成功したエクスポートを示しています。

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
```

```
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

5. start-connection を使用して、リージョンへのセキュアな接続を作成してください。

   次の例の出力は、接続が正常に開始されたことを示しています。

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connection-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

6. 5 分ほど待ってください。
7. get-connection を使用して、リージョンへの接続が確立されているかどうかを確認してください。

   以下の例の出力は、成功した接続を示しています。

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
```

```
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

keys_exchanged および connection_established を変更して True になった後、Outpost サーバーは自動的にプロビジョニングされ、最新のソフトウェアと構成に更新されます。

> **Note**
>
> プロビジョニングのプロセスについては、次の点に注意してください。
>
> - アクティベーションが完了した後、Outpost サーバーが使用可能になるまでに最大で 10 時間かかることがあります。
> - このプロセス中、Outpost サーバーの電源とネットワークを接続し、安定させておく必要があります。
> - このプロセス中にサービスリンクが変動することは正常です。
> - exchange_active が True の場合、接続はまだ確立中です。5 分後に再試行してください。
> - keys_exchanged または connection_established が False で、exchange_active が True の場合は、接続はまだ確立中です。5 分後に再試行してください。
> - 1 時間経過しても keys_exchanged または connection_established が False の場合は、AWS Support センターに連絡してください。
> - メッセージprimary_status: No such asset id found.が表示されたら、以下を確認します。
>   - 正しいリージョンを指定しました。
>   - Outpost サーバーの注文に使用したアカウントと同じアカウントを使用しています。

リージョンが正しく、Outpost サーバーの注文に使用したアカウントと同じアカウントを使用している場合は、 AWS Support センターにお問い合わせください。

- Outpost の属性 `LifeCycleStatus` 属性が `Provisioning` から `Active` に移行します。その後、Outpostサーバーがプロビジョニングおよびアクティベートされたことを知らせるメールが届きます。
- Outposts サーバーがアクティベートされた後は、Outposts サーバーを再認可する必要はありません。

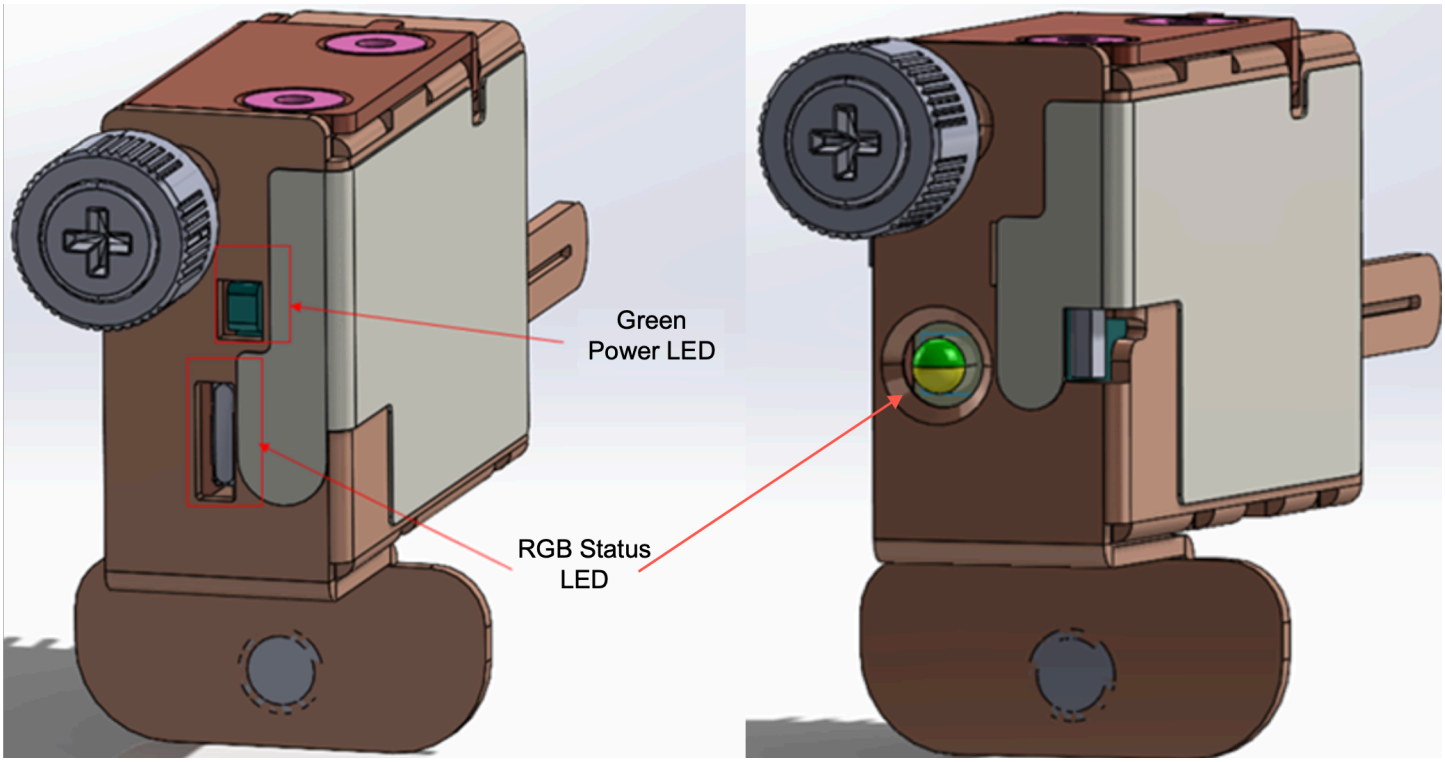
8. 接続が成功したら、ノート PC をサーバーから切断できます。

NSK LEDsを確認する

プロビジョニングプロセスが完了したら、NSK LEDsを確認します。

AWS Outposts は、Atlas 2.0 と Atlas 3.0 の 2 つのバージョンの NSK をサポートしています。どちらの NSK バージョンにも RGB ステータス LED があります。さらに、Atlas 3.0 には緑色の電源 LED があります。

次の図は、Atlas 2.0 および Atlas 3.0 の LEDs の位置を示しています。



Atlas 3.0 Atlas 2.0

NSK のステータス LED と電源 LEDs を確認するには

1. RGB ステータス LED の色を確認します。色が緑色の場合、NSK は正常です。色が緑色でない場合は、 にお問い合わせください AWS Support。
2. Atlas 3.0 NSK を使用している場合は、緑色の電源 LED を確認します。緑色のライトがオンになっている場合、NSK はホストに正しく接続されており、電源があります。緑色のライトがオンになっていない場合は、 にお問い合わせください AWS Support。

Outpost 構成ツールのコマンド リファレンス

Outpost 構成ツールには次のコマンドが用意されています

コマンド

- [Export] (エクスポート)
- Echo
- リンクの説明
- IP の説明
- 決意の説明
- 到達可能性の説明
- 接続を開始する
- GET 接続

[Export] (エクスポート)

export

export を使用して、IAM 認証情報を環境変数として設定します。

構文

```
Outpost>export variable=value
```

export は変数代入文を取ります。

これは、次の形式を使用する必要があります: *variable*=*value*

認証するには、次の 4 つの変数をエクスポートする必要があります。変数は一度に 1 つずつエクスポートします。等号 (=) の前後にスペースを入れないでください。

- AWS_ACCESS_KEY_ID=*access-key-id*
- AWS_SECRET_ACCESS_KEY=*secret-access-key*
- AWS_SESSION_TOKEN=*session-token*
- AWS_DEFAULT_REGION=*#####*

  AWS_DEFAULT_REGION の値には Outpost サーバーの親リージョンを使用します。

Example : 認証情報のインポート成功

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

Echo

echo

echo を使用して、exportコマンドで変数に設定した値を表示するのに使用します。

構文

```
Outpost>echo $variable-name
```

variable-name は、以下のいずれかにすることができます。

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example : 成功

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

variable name: AWS_DEFAULT_REGION
variable value: us-west-2
checksum: example-checksum
```

Example : export コマンドで変数値が設定されていないため失敗

```
Outpost> echo $AWS_ACCESS_KEY_ID
```

```
error_type: execution_error
error_attributes:
  AWS_ACCESS_KEY_ID: no value set
error_message: No value set for AWS_ACCESS_KEY_ID using export.
checksum: example-checksum
```

Example : 変数名が無効なため失敗しました

```
Oupost>echo $foo

error_type: invalid_argument
error_attributes:
  foo: invalid variable name
error_message: Variables can only be AWS credentials.
checksum: example-checksum
```

Example : 構文の問題による失敗

```
Outpost>echo AWS_SECRET_ACCESS_KEY

error_type: invalid_argument
error_attributes:
  AWS_SECRET_ACCESS_KEY: not a variable
error_message: Expecting $ before variable name.
checksum: example-checksum
```

リンクの説明

describe-links

describe-links を使用して、サーバーのネットワークリンクに関する情報を取得します。Outpost サーバーは、1 つのサービスリンクと 1 つのローカルネットワークインターフェイス (LNI) リンクを持っている必要があります。

構文

```
Outpost>describe-links
```

describe-links は引数を取りません。

IP の説明

describe-ip

describe-ip は、接続されている各リンクの IP 割り当てステータスと構成を返します。

構文

```
Outpost>describe-ip
```

describe-ip は引数を取りません。

決意の説明

describe-resolve

describe-resolve を使用して、Outpost サーバーが DNS リゾルバーに到達し、リージョン内の Outpost 構成エンドポイントの IP アドレスを解決できるかどうかを判断します。IP 構成を含むリンクが少なくとも 1 つ必要です。

構文

```
Outpost>describe-resolve
```

describe-resolve は引数を取りません。

到達可能性の説明

describe-reachability

describe-reachability を使用して、Outpost サーバーがリージョン内の Outpost 構成エンドポイントに到達できるかどうかを判断します。機能する DNS 設定が必要です。これは、describe-resolve を使用して確認できます。

構文

```
Outpost>describe-reachability
```

describe-reachability は引数を取りません。

接続を開始する

start-connection

start-connection は、リージョン内の Outpost サービスとの接続を開始するのに使用します。このコマンドは、export でロードした環境変数から Signature Version 4 (SigV4) 認証情報を取得します。接続は非同期で実行され、即座に return されます。接続ステータスを確認するには、get-connection を使用します。

構文

```
Outpost>start-connection [0|1]
```

start-connection は別の接続を開始するのに、接続インデックスを引数に取ります (オプション)。有効な値は `0` と `1` のみです。

Example : 接続が開始されました

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connecdtion-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

GET 接続

get-connection

get-connection を使用して接続の状態を返します。

構文

```
Outpost>get-connection [0|1]
```

get-connection 1 は、オプションの接続インデックスを取得して、別の接続のステータスを返します。有効な値は `0` と `1` のみです。

Example : 接続成功

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

[Note:] (メモ:)

- exchange_active が True の場合、接続はまだ確立中です。5 分後に再試行してください。
- keys_exchanged または connection_established が False で、exchange_active が True の場合は、接続はまだ確立中です。5 分後に再試行してください。

1 時間経過しても問題が解決しない場合は、AWS Support センターに連絡してください。

Outpost サーバー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。例えば、Amazon EC2 インスタンスを起動できます。

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: サブネットの作成
- ステップ 2: Outpost 上でインスタンスを起動
- ステップ 3: 接続の構成
- ステップ 4: 接続をテストする

ステップ 1: サブネットの作成

Outpost サブネットは、Outpost の 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 は Outpost にも広がります。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 2: Outpost 上でインスタンスを起動。

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、サブネットの IP アドレス範囲を指定してください。
5. [作成] を選択します。
6. サブネットを作成したら、そのサブネットをローカルネットワークインターフェイスに有効にしてください。

ステップ 2: Outpost 上でインスタンスを起動

作成した Outpost サブネットまたは共有されている Outpost サブネット内で EC2 インスタンスを起動できます セキュリティグループは、アベイラビリティーゾーンサブネットのインスタンスと同様に、Outpost サブネットのインスタンスのインバウンドトラフィックとアウトバウンド VPC トラフィックを制御します。Outpost サブネットの EC2 インスタンスに接続するには、アベイラビリティーゾーンサブネットのインスタンスの場合と同様に、インスタンスの起動時にキーペアを指定できます。

考慮事項

- Outposts サーバー上のインスタンスには、インスタンスストアボリュームが含まれますが、EBS ボリュームは含まれません。アプリケーションのニーズに合わせて十分なインスタンスストレージを持つインスタンスサイズを選択します。詳細については、「Amazon EC2 Linux インスタンス用ユーザーガイド」の「インスタンスストアボリューム」を参照してください。
- 単一のスナップショットのみを持つ AMI を指定する必要があります。複数のスナップショットを持つ AMI はサポートされていません。
- インスタンスストアボリューム上のデータは、インスタンスの再起動後も保持されますが、インスタンスの終了後は保持されません。インスタンスの寿命を超えてインスタンスストアボリュームの長期データを保持するには、データを Amazon S3 バケットやオンプレミスネットワークのネットワークストレージデバイスなどの永続ストレージにバックアップしてください。
- Outpost サブネット内のインスタンスをオンプレミス ネットワークに接続するには、次の手順で説明するように、ローカル ネットワーク インターフェイスを追加する必要があります。

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 サーバー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 サーバー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。
6. (オプション) ローカルネットワークインターフェイスを今すぐ追加するか、インスタンスを作成した後に追加できます。今すぐ追加するには、[詳細なネットワーク構成] を展開し、[ネットワークインターフェイスを追加] を選択してください。Outpost サブネットを選択してくださ

い。これにより、デバイスインデックス1を使用してインスタンスのためにネットワークインターフェイスが作成されます。Outpost サブネットの LNI デバイスインデックスとして 1 を指定した場合、このネットワークインターフェイスはインスタンスのローカルネットワークインターフェイスになります。

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

ステップ 3: 接続の構成

インスタンスの起動時にローカル ネットワーク インターフェイスをインスタンスに追加しなかった場合は、ここで追加する必要があります。詳細については、「起動後に LNI を追加」 を参照してください。

ローカル ネットワークの IP アドレスを使用して、インスタンスのローカル ネットワーク インターフェイスを構成する必要があります。通常、これは DHCP を使用して行います。詳細については、インスタンスのオペレーティングシステムに関するドキュメントを参照してください。追加のネットワークインターフェイスとセカンダリ IP アドレスの設定に関する情報が記載されています。

ステップ 4: 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 インスタンスのローカルネットワークインターフェイス 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 インスタンスへの接続」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
   ```

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。

> **Note**
>
> Outpost サーバーを自分のリージョンまたは AWS Outposts ホーム AWS リージョンに接続するサービスリンク接続にプライベート接続を使用することはできません。

内容

サービスリンク経由の接続

AWS Outposts プロビジョニング中に、Outpost を選択したリージョンまたは AWS Outposts ホーム AWS リージョンに接続するサービスリンク接続をユーザーまたは が AWS 作成します。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 の管理と AWS リージョンと Outpost 間の VPC 内トラフィックの両方が可能になります。

Outpost はパブリックリージョン接続を通じて AWS リージョンに戻るサービスリンク VPN を作成することができます。そのためには、Outpost はパブリックインターネットまたはパブリック仮想インターフェイスを介して、 AWS リージョンの AWS Direct Connect パブリック IP 範囲に接続する必要があります。この接続は、サービスリンク VLAN 内の特定のルート経由でも、0.0.0.0/0 のデフォルトルート経由でも可能です。 AWSのパブリックレンジの詳細については、「AWS IP アドレス範囲」を参照してください。

サービスリンクが確立されると、Outpost は によって稼働および管理されます 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。

- 内部コントロールプレーントラフィック、内部リソース監視、ファームウェアとソフトウェアの更新など、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 (顧客データプレーントラフィックを含む)。

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、 AWS では、リージョンへの AWS サービスリンク接続に 500 Mbps 以上の冗長接続を使用することをお勧めします。各 Outpost サーバーの最大使用率は 500 Mbps です。接続速度を上げるには、複数の Outpost サーバーを使用してください。たとえば、 AWS Outposts サーバーが 3 台ある場合、最大接続速度は 1.5 Gbps (1,500 Mbps) に増加します。詳細については、「サーバーのサービスリンクトラフィック」を参照してください。

AWS Outposts サービスリンクの帯域幅要件は、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によって異なります。 AWS Outposts サーバーは AMIsキャッシュしないことに注意してください。AMI はインスタンスが起動するたびにリージョンからダウンロードされます。

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	1024-65535	サービスリンク IP	53	DHCP 提供の DNS サーバー
UDP	443、1024-65535	サービスリンク IP	443	AWS Outposts サービスリンクエンドポイント
TCP	1024-65535	サービスリンク IP	443	AWS Outposts 登録エンドポイント

> **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。

更新とサービスリンク

AWS は、Outpost サーバーとその親 AWS リージョン間の安全なネットワーク接続を維持します。サービスリンクと呼ばれるこのネットワーク接続は、Outpost と AWS リージョン間の VPC 内トラフィックを提供することで、Outpost を管理する上で不可欠です。AWS Well-Architected のベスト

プラクティスでは、アクティブ/アクティブ設計の異なるアベイラビリティーゾーンに親親化された 2 つの Outposts にアプリケーションをデプロイすることをお勧めします。詳細については、AWS Outposts「高可用性の設計とアーキテクチャに関する考慮事項」を参照してください。

サービスリンクは、運用品質とパフォーマンスを維持するために定期的に更新されます。メンテナンス中、このネットワークで短いレイテンシーとパケット損失が発生し、リージョンでホストされているリソースへの VPC 接続に依存するワークロードに影響を与える可能性があります。ただし、ローカルネットワークインターフェイス (LNI) を通過するトラフィックは影響を受けません。AWS Well-Architected のベストプラクティスに従い、単一の Outpost サーバーに影響する障害やメンテナンスアクティビティにアプリケーションが回復できるようにすることで、アプリケーションへの影響を回避できます。

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ています。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、「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。

AWS Outposts サーバーを返す

がサーバーに欠陥 AWS Outposts を検出した場合、通知し、交換プロセスを開始して新しいサーバーを送信し、 コンソールから配送ラベルを渡します AWS Outposts 。

契約期間の終了やその他の理由でサーバーを返却したい場合は、AWS Support Center にご連絡ください。

トピック

以下の手順では、サーバーを AWSに返却する方法について説明しています。

1. サーバーを返却する準備をする

サーバーを返却する準備をするには、リソースの共有を解除し、データをバックアップし、ローカルネットワークインターフェイスを削除し、アクティブなインスタンスを終了します。

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. AWS Outposts サーバーで実行されている Amazon EC2 インスタンスのインスタンスストレージに保存されているデータのバックアップを作成します。
3. サーバーで実行されていたインスタンスに関連付けられているローカルネットワークインターフェイスを削除します。

4. 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

2. 返却用の発送ラベルを取得する

> **Important**
>
> AWS が提供する配送ラベルのみを使用する必要があります。独自の発送ラベルを作成しないでください。

返品の理由に基づいて発送ラベルを取得します。

Shipping label for a server that is being replaced

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 [注文] を選択します。
3. [交換注文の概要] で、[返品ラベルを印刷する] を選択し、返却するサーバーの構成 ID を選択します。

Shipping label for a server that is not being replaced

1. AWS Support センター に問い合わせます。
2. 返却するサーバーの発送ラベルをリクエストします。

3. サーバーを梱包

サーバーを梱包するには、サーバーが元々入っていた箱と梱包材を使用してください。交換サーバーが入っていた箱も使用できます。または、AWS Support センター に連絡して箱をリクエストしてください。サーバーを梱包したら、 から AWS 提供された配送ラベルを貼り付けます。

4. 宅配業者を通じてサーバーを返却する

お使いの国の指定された宅配業者を利用してサーバーを返却する必要があります。サーバーを宅配業者に持ち込むことも、宅配業者がサーバーを集荷する希望の日時をスケジュールすることもできます。 AWS が提供する配送ラベルには、サーバーを返送するための正しい住所が含まれています。

次の表は発送元の国での連絡先を示しています。

国	問い合わせ
アルゼンチン	AWS Support センター に問い合わせます。リクエストで以下の情報を提供してください。 • AWSが提供する配送ラベルに記載されている追跡番号 • 宅配業者にサーバーを集荷してもらいたい日時 • 問い合わせ名 • 電話番号 • E メールアドレス
バーレーン	
ブラジル	
ブルネイ	
カナダ	
チリ	
コロンビア	
香港	
インド	
インドネシア	
日本	
マレーシア	
ナイジェリア	
オマーン	
パナマ	
ペルー	

国	問い合わせ
フィリピン	
セルビア	
シンガポール	
南アフリカ	
韓国	
台湾	
タイ	
アラブ首長国連邦	
ベトナム	
United States of America	UPS に問い合わせてください。 サーバーは以下の方法で返却できます。 • お客様のサイトでの UPS の定期集荷でサーバーを返却する。 • UPS の営業所にサーバーを持ち込む。 • 希望の日時で集荷をスケジュールする。送料無料用に、 AWSが提供する配送ラベルから追跡番号を入力します。

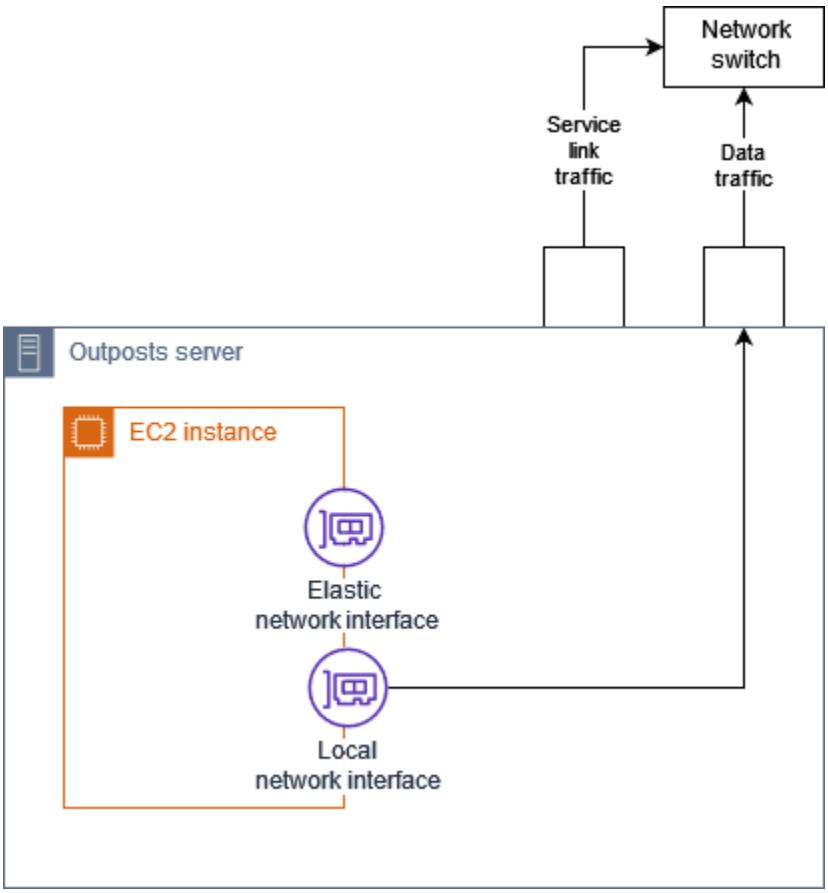
国	問い合わせ
他のすべての国	DHL に問い合わせてください。 サーバーは以下の方法で返却できます。 • DHL の営業所 にサーバーを持ち込む。 • 希望の日時で集荷をスケジュールする。送料無料用に、 AWSが提供する配送ラベルからの配送状番号を入力します。 `Courier pickup cannot be scheduled for an import shipment` というエラーが表示された場合は、通常は選択した集荷国が返品発送ラベルに記載された集荷国と一致していないことを意味します。発送元の国を選択して、もう一度試してください。

ローカルネットワークインターフェイス

AWS Outposts サーバーでは、ローカルネットワークインターフェイス (LNI) は、Outposts サブネット内の Amazon EC2 インスタンスをオンプレミスネットワークに接続する論理ネットワークコンポーネントです。

ローカルネットワークインターフェイスはローカルエリアネットワーク上で直接実行されます。このタイプのローカル接続では、オンプレミス機器と通信するためのルーターやゲートウェイは必要ありません。ローカルネットワークインターフェイスは、ネットワークインターフェイスや エラスティックネットワークインターフェイスに似た名前が付けられています。ローカルネットワークインターフェイスを指すときは常に ローカル を使うことで、この 2 つのインターフェイスを区別しています。

Outpost サブネットでローカルネットワークインターフェイスを有効にした後、エラスティックネットワークインターフェイスに加えてローカルネットワークインターフェイスを含めるように Outpost サブネットの EC2 インスタンスを構成できます。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ネットワークに接続し、ネットワークインターフェイスは VPC に接続します。次の図は、エラスティックネットワークインターフェイスとローカルネットワークインターフェイスの両方を備えた Outposts サーバー上の EC2 インスタンスを示しています。



他のオンプレミス機器の場合と同様に、ローカルネットワークインターフェイスがローカルエリアネットワーク上で通信できるようにオペレーティングシステムを設定する必要があります。ローカルネットワークインターフェイスはローカルエリアネットワーク上で動作するため、VPC の DHCP オプションセットを使用してローカルネットワークインターフェイスを設定することはできません。

エラスティックネットワークインターフェイスは、アベイラビリティーゾーンサブネット内のインスタンスとまったく同じように機能します。例えば、VPC ネットワーク接続を使用して のパブリックリージョンエンドポイントにアクセスしたり AWS のサービス、インターフェイス VPC エンドポイントを使用して を使用して にアクセス AWS のサービス したりできます AWS PrivateLink。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

- ローカルネットワークインターフェイスの基本
- Outposts サーバーのサブネットをローカルネットワークインターフェイス用に有効にする
- ローカルネットワークインターフェイスでの作業
- サーバーのローカルネットワーク接続

ローカルネットワークインターフェイスの基本

ローカルネットワークインターフェイスは、物理レイヤー 2 ネットワークへのアクセスを提供します。VPC は仮想化されたレイヤー 3 ネットワークです。ローカルネットワークインターフェイスは VPC ネットワークコンポーネントをサポートしていません。これらのコンポーネントには、セキュリティグループ、ネットワークアクセスコントロールリスト、仮想化ルーターまたはルートテーブル、およびフローログが含まれます。ローカルネットワークインターフェイスでは、Outpost サーバーは VPC レイヤー 3 フローを可視化できません。インスタンスのホストオペレーティングシステムは、物理ネットワークからのフレームを完全に可視化できます。これらのフレーム内の情報には、標準のファイアウォールロジックを適用できます。ただし、この通信はインスタンス内で行われますが、仮想化されたコンストラクトの範囲外です。

考慮事項

- ローカルネットワークインターフェイスは ARP と DHCP のプロトコルをサポートします。一般的な L2 ブロードキャストメッセージはサポートしていません。
- 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クォータから差し引かれます。詳細については、「Amazon VPC ユーザーガイド」の「ネットワークインターフェイス」を参照してください。
- 各 EC2 インスタンスには、1 つのローカルネットワークインターフェイスを含めることができます。
- ローカルネットワークインターフェイスは、インスタンスのプライマリネットワークインターフェイス (eth0) を使用できません。
- Outposts サーバーは、ローカルネットワークインターフェイスを持つ複数の EC2 インスタンスをホストできます。

> **Note**
>
> 同じサーバー内の EC2 インスタンスは、Outposts サーバーの外部にデータを送信せずに直接通信できます。この通信には、ローカルネットワークインターフェイスまたはエラスティックネットワークインターフェイスを経由するトラフィックが含まれます。

- ローカルネットワークインターフェイスは、Outpost サーバー上の Outposts サブネットで実行されているインスタンスでのみ使用できます。
- ローカルネットワークインターフェイスは、無差別モードや MAC アドレススプーフィングをサポートしていません。

パフォーマンス

各インスタンスサイズの LNI は、使用可能な物理 10 GbE LNI 帯域幅の一部を提供します。次の表に、各インスタンスタイプの LNI ネットワークパフォーマンスを示します。

インスタンスタイプ	ベースライン帯域幅 (Gbps)	バースト帯域幅 (Gbps)
c6id.large	0.15625	2.5
c6id.large	0.15625	2.5
c6id.xlarge	0.3125	2.5
c6id.2xlarge	0.625	2.5
c6id.4xlarge	1.25	2.5
c6id.8xlarge	2.5	2.5
c6id.12xlarge	3.75	3.75
c6id.16xlarge	5	5
c6id.24xlarge	7.5	7.5
c6id.32xlarge	10	10
c6gd.medium	0.15625	4
c6gd.large	0.3125	4
c6gd.xlarge	0.625	4
c6gd.2xlarge	1.25	4
c6gd.4xlarge	2.5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7.5	7.5
c6gd.16xlarge	10	10

セキュリティグループ

設計上、ローカルネットワークインターフェイスは VPC のセキュリティグループを使用しません。セキュリティグループは、インバウンドとアウトバウンドの VPC トラフィック を制御します。ローカルネットワークインターフェイスは VPC にアタッチされていません。ローカルネットワークインターフェイスは、ローカルネットワークにアタッチされています。ローカルネットワークインターフェイス上のインバウンドトラフィックとアウトバウンドトラフィックを制御するには、他のオンプレミス機器と同様に、ファイアウォールまたは同様の方法を使用します。

モニタリング

CloudWatch メトリクスは、Elastic Network Interface の場合と同様に、ローカルネットワークインターフェイスごとに生成されます。Linux インスタンスの詳細については、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスのネットワークパフォーマンスのモニタリング」を参照してください。 Amazon EC2 Windows インスタンスについては、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスのネットワークパフォーマンスのモニタリング」を参照してください。
Amazon EC2

MAC アドレス

AWS は、ローカルネットワークインターフェイスの MAC アドレスを提供します。ローカルネットワークインターフェイスは MAC アドレスにローカル管理アドレス (LAA) を使用します。ローカルネットワークインターフェイスは、インターフェイスが削除されるまで同じ MAC アドレスを使用します。ローカルネットワークインターフェイスを削除したら、ローカル設定から MAC アドレスを削除します。 は、使用されなくなった MAC アドレスを再利用 AWS できます。

Outposts サーバーのサブネットをローカルネットワークインターフェイス用に有効にする

から modify-subnet-attribute コマンド AWS CLI を使用して、ローカルネットワークインターフェイスの Outpost サブネットを有効にします。デバイスインデックスでネットワークインターフェイスの位置を指定する必要があります。有効な Outpost サブネットで起動されるすべてのインスタンスは、このデバイス位置をローカルネットワークインターフェイスに使用します。たとえば、値が1の場合、Outpost サブネット内のインスタンスのセカンダリネットワークインターフェイス (eth1) がローカルネットワークインターフェイスであることを示します。

ローカルネットワークインターフェイスの Outpost サブネットを有効にするには

コマンドプロンプトで、次のコマンドを使用して、ローカルネットワークインターフェイスのデバイスの位置を指定します。

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-1a2b3c4d \
    --enable-lni-at-device-index 1
```

ローカルネットワークインターフェイスでの作業

このセクションでは、ローカルネットワークインターフェイスの操作方法について説明します。

タスク

- ローカルネットワークインターフェイスの追加
- ローカルネットワークインターフェイスの表示
- オペレーティングシステムの設定

ローカルネットワークインターフェイスの追加

起動中または起動後に、Outposts サブネット上の Amazon EC2 インスタンスにローカルネットワークインターフェイス (LNI) を追加できます。そのためには、ローカルネットワークインターフェイスの Outpost サブネットを有効にしたときに指定したデバイスインデックスを使用して、インスタンスにセカンダリネットワークインターフェイスを追加します。

考慮事項

コンソールを使用してセカンダリネットワークインターフェイスを指定すると、デバイスインデックス 1 を使用してネットワークインターフェイスが作成されます。ローカルネットワークインターフェイスの Outpost サブネットを有効にしたときに指定したデバイスインデックスでない場合は、代わりに AWS CLI または AWS SDK を使用して正しいデバイスインデックスを指定できます。例えば、 から次のコマンドを使用します AWS CLI: create-network-interface と attach-network-interface 。

インスタンスの起動時に LNI を追加するには

1. インスタンス起動ウィザードで、ネットワーク設定の横にある「編集」を選択します。
2. 高度なネットワーク設定の拡張。
3. [Add network interface] を選択します。これにより、デバイスインデックス 1 を使用してネットワークインターフェイスが作成されます。Outpost サブネットの LNI デバイスインデックスと

して 1 を指定した場合、このネットワークインターフェイスはインスタンスのローカルネットワークインターフェイスになります。

4. Outpost サブネットを選択し、必要に応じてネットワークインターフェイスの設定を更新します。
5. ウィザードを終了してインスタンスを起動します。

インスタンスの起動後に LNI を追加するには

1. ナビゲーションペインで、[ネットワークとセキュリティ]、[ネットワークインターフェイス] を選択します。
2. ネットワークインターフェイスを作成する
   a. [ネットワークインターフェイスの作成] をクリックします。
   b. インスタンスと同じ Outpost サブネットを選択します。
   c. プライベート IPv4 アドレスが自動割り当てに設定されていることを確認します。
   d. セキュリティグループを選択します。セキュリティグループは LNI には適用されないため、選択したセキュリティグループは関係ありません。
   e. [ネットワークインターフェイスの作成] をクリックします。
3. インスタンスへのネットワークインターフェイスのアタッチ
   a. 新しく作成したネットワークインターフェイスのチェックボックスを選択します。
   b. [アクション]、[アタッチ] の順にクリックします。
   c. インスタンスを選択します。
   d. 添付を選択します。ネットワークインターフェースはデバイスインデックス 1 にアタッチされています。Outpost サブネットの LNI デバイスインデックスとして 1 を指定した場合、このネットワークインターフェースはインスタンスのローカルネットワークインターフェースになります。

ローカルネットワークインターフェイスの表示

インスタンスが実行ステータスにある間は、Amazon EC2 コンソールを使用して、Outpost サブネット内のインスタンスのエラスティックネットワークインターフェイスとローカルネットワークインターフェイスの両方を表示できます。インスタンスを選択し、[ネットワーキング] タブを選択します。

コンソールには、サブネット CIDR の LNI のプライベート IPv4 アドレスが表示されます。このアドレスは LNI の IP アドレスではないため、使用できません。ただし、このアドレスはサブネット CIDR から割り当てられるため、サブネットのサイズ設定にはこのアドレスを考慮する必要があります。LNI の IP アドレスは、ゲスト OS 内で静的に設定するか、DHCP サーバー経由で設定する必要があります。

オペレーティングシステムの設定

ローカルネットワークインターフェイスを有効にすると、Amazon EC2 インスタンスには 2 つのネットワークインターフェイスがあり、そのうちの 1 つはローカルネットワークインターフェイスです。起動する Amazon EC2 インスタンスのオペレーティングシステムを、マルチホームネットワーク設定をサポートするように設定してください。

サーバーのローカルネットワーク接続

このトピックを参照して、Outpost サーバーをホストするためのネットワークケーブルとトポロジの要件を理解してください。詳細については、「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。

内容

ネットワーク上のサーバートポロジー

Outpost サーバーには、ネットワーク機器への 2 つの異なる接続が必要です。接続ごとに異なるケーブルが使用され、異なる種類のトラフィックが伝送されます。複数のケーブルはトラフィッククラスの分離のみを目的としており、冗長性向上のためのものではありません。2 本のケーブルを共通のネットワークに接続する必要はありません。

次の表では、Outpost サーバーのトラフィックタイプとラベルについて説明しています。

トラフィックラベル	説明
2	サービスリンクトラフィック — このトラフィックにより、Outpost と AWS リージョン間の通信が可能になり、Outpost と AWS リージョン間の VPC 内トラフィックの両方を管理できます。サービスリンクトラフィックには、Outpost からリージョンへのサービスリンク接続が含まれます。サービスリンクは、Outpost からリージョンへの 1 つまたは複数のカスタムVPNです。Outpost は、購入時に選択したリージョンのアベイラビリティーゾーンに接続します。
1	ローカルネットワークインターフェイス (LNI) リンクトラフィック — このトラフィックにより、ローカルネットワークインターフェイスを介して VPC からローカル LAN への通信が可能になります。ローカルリンクトラフィックには、Outpost 上で実行され、オンプレミスネットワークと通信するインスタンスが含まれます。ローカルリンクトラフィックには、オンプレミスネットワークを介してインターネットと通信するインスタンスも含まれる場合があります。

サーバーの物理的な接続

各 Outpost サーバーには、冗長でない物理的なアップリンクポートが 含まれています。ポートには、次のような独自の速度とコネクタ要件があります。

- 10GbE — コネクタタイプ: QSFP+

QSFP+ ケーブル

QSFP+ ケーブルには Outpost サーバーのポート 3 に接続するコネクタがあります。QSFP+ ケーブルのもう一方の端には、スイッチに接続する 4 つの SFP+ インターフェイスがあります。スイッチ側の 2 つのインターフェイスには 1 と 2 というラベルが付いています。Outpost サーバーが機能するには、両方のインターフェイスが必要です。サービスリンクトラフィックには 2 インターフェイスを使用し、LNI リンクトラフィックには 1 インターフェイスを使用します。残りのインターフェイスは使用されません。

サーバーのサービスリンクトラフィック

スイッチ上のサービスリンクポートを、ゲートウェイを備えた VLAN へのタグなしアクセスポートとして構成し、次のリージョンエンドポイントへのルートを設定します。

- サービスリンクエンドポイント
- Outposts 登録エンドポイント

サービスリンク接続では、Outpost が AWS リージョン内の登録エンドポイントを検出するために、パブリック DNS が使用可能である必要があります。この接続では、Outpost サーバーと登録エンドポイントの間に NAT デバイスを接続できます。のパブリックアドレス範囲の詳細についてはAWS、「Amazon VPC ユーザーガイド」のAWS 「IP アドレス範囲」および「」のAWS Outposts「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

サーバーを登録するには、以下のネットワークポートを開きます。

- TCP 443
- UDP 443
- UDP 53

アップリンク速度

各 Outposts サーバーには、 AWS リージョンへの最低 20 Mbps のアップリンク速度が必要です。

LNI リンクとサービスリンクの使用状況によっては、より高速なアップリンクが必要になる場合があります。詳細については、「サービスリンクの推奨帯域幅」を参照してください。

ローカルネットワークインターフェイス (LNI) リンクトラフィック

アップストリームネットワークデバイスの LNI リンクポートを、ローカルネットワーク上の VLAN への標準アクセスポートとして設定します。VLAN が複数ある場合は、アップストリームネットワー

クデバイスのすべてのポートをトランクポートとして設定します。アップストリームネットワークデバイスのポートが複数の MAC アドレスに対応するように設定します。サーバー上で起動される各インスタンスは MAC アドレスを使用します。一部のネットワークデバイスは、複数の MAC アドレスを報告するポートをシャットダウンするポートセキュリティ機能を提供します。

> **Note**
>
> AWS Outposts サーバーは VLAN トラフィックにタグを付けません。LNI をトランクとして設定する場合は、OS が VLAN トラフィックにタグ付けされていることを確認する必要があります。

次に、Amazon Linux 2023 で LNI の VLAN タグ付けを設定する方法の例を示します。別の Linux ディストリビューションを使用している場合、「VLAN タグ付けについて Linux ディストリビューション」のドキュメントを参照してください。

例: Amazon Linux 2023 と Amazon Linux 2 での LNI の VLAN タグ付けを設定するには

1. 8021q モジュールがカーネルにロードされていることを確認します。読み込まれていない場合は、`modprobe` コマンドを使用してロードしてください。

```
modinfo 8021q
modprobe --first-time 8021q
```

2. VLAN デバイスを作成します。この例では、以下のようになっています。

   - LNI のインターフェイスの名前は `ens6` です
   - VLAN ID は 59 です
   - VLAN デバイスに割り当てられる名前は `ens6.59` です

```
ip link add link ens6 name ens6.59 type vlan id 59
```

3. オプション。IP を手動で割り当てる場合は、このステップを実行してください。この例では、IP 192.168.59.205 を割り当てています。サブネット CIDR は 192.168.59.0/24 です。

```
ip addr add 192.168.59.205/24 brd 192.168.59.255 dev ens6.59
```

4. リンクを有効にします。

```
ip link set dev ens6.59 up
```

OS レベルでネットワークインターフェイスを設定し、VLAN タグの変更を永続化するには、以下のリソースを参照してください。

- Amazon Linux 2 を使用している場合は、「Amazon Amazon EC2 ユーザーガイド」の「Amazon Linux の ec2-net-utils を使用してネットワークインターフェイスを設定する」を参照してください。
- Amazon Linux 2023 を使用している場合は、「Amazon Linux 2023 ユーザーガイド」の「ネットワークサービス」を参照してください。

サーバー IP アドレスの割り当て

Outpost サーバーにはパブリック IP アドレスを割り当てる必要はありません。

動的ホスト制御プロトコル (DHCP) は、IP ネットワーク上のデバイスの設定プロセスを自動化するために使用されるネットワーク管理プロトコルです。Outpost サーバーの場合、DHCP は次の 2 つの方法で使用できます。

- サーバー上のネットワークカード
- インスタンス上のローカルネットワークインターフェイス

サービスリンクの場合、Outpost サーバーは DHCP を使用してローカルネットワークに接続しますが。DHCP は DNS ネームサーバーとデフォルトゲートウェイを返す必要があります。Outpost サーバーは、サービスリンクの静的 IP 割り当てをサポートしていません。

LNI リンクの場合は、DHCP を使用してインスタンスをローカルネットワークに接続するように設定します。詳細については、「the section called “オペレーティングシステムの設定”」を参照してください。

> **Note**
>
> Outpost サーバーには必ず安定した IP アドレスを使用してください。IP アドレスを変更すると、Outpost サブネットのサービスが一時的に中断される可能性があります。

サーバーの登録

Outpost サーバーがローカルネットワーク上で接続を確立すると、サービスリンク接続を使用して Outpost 登録エンドポイントに接続し、サーバー自体を登録します。登録にはパブリック DNS が必要です。サーバーが登録されると、リージョンのサービスリンクエンドポイントへの安全なトンネルが作成されます。Outpost サーバーは TCP ポート 443 を使用して、パブリックインターネットを介したリージョンとの通信を容易にします。現在、 AWS Outposts サーバーは VPC 経由のプライベート接続をサポートしていません。詳細については、「the section called “ステップ 6: サーバーを承認する”」を参照してください。

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 サーバーで利用できるリソースです。ラックリソースについては、「AWS Outposts Outposts ラック用ユーザーガイド」の「共有 AWS Outposts リソースの操作」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。
- 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。
  - AWS Outposts API を使用して Outpost に関する情報を表示します。
- 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 Outposts 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 Outposts 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 コンソールおよび AWS CLI を使用して、共有 Outposts 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 所有者が所有するリソースを表示または変更することはできません。また、自己が共有している Outpost を変更することはできません。

請求と使用量測定

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

ローカルゲートウェイルートテーブルの共有に追加料金はかかりません。共有サブネットの場合、VPC 所有者には 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。 AWS のお客様は、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 — AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS を担います。 AWS また、 は、お客様が安全に使用できるサービスも提供します。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 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 サーバー上のデータを復号化するために必要です。

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。

データの削除

EC2 インスタンスを終了すると、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。詳細については、サーバーデータを暗号化して細断する を参照してください。

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
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。

Outposts AWS 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。この際、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お勧めします。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と AWS、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 へのリクエストリクエスト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 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することがないため、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***

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

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 マネージドポリシー： AWSOutpostsAuthorizeServerPolicy

このポリシーを使用して、オンプレミスネットワーク内で Outpost サーバーハードウェアを承認するために必要な権限を付与します。詳細については、「許可の付与」を参照してください。

このポリシーには、以下のアクセス許可が含まれています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

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
AWSOutpostsAuthorizeServerPolicy - 新しいポリシー	AWS Outposts は、オンプレミスネットワークで Outpost サーバーハードウェアを承認するアクセス許可を付与するポリシーを追加しました。	2023 年 1 月 4 日
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。

の耐障害性 AWS Outposts

高可用性を実現するために、、追加の Outposts サーバーを注文したりできます。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。

Outposts サーバーにはインスタンスストアボリュームが含まれていますが、Amazon EBS ボリュームはサポートされていません。インスタンスストアボリューム上のデータは、インスタンスの再起動後も保持されますが、インスタンスの終了後は保持されません。インスタンスの寿命を超えてインスタンスストアボリュームの長期データを保持するには、データを Amazon S3 バケットやオンプレミスネットワークのネットワークストレージデバイスなどの永続ストレージにバックアップしてください。

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。

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`

`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

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。
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 リージョンの場合と同様に AWS Outposts、 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 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、Outpost の所有者とインスタンスの所有者に、影響を受けるインスタンスのリタイアが予定されていることを通知します。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。

AWS は、インスタンスの廃止日に影響を受けるインスタンスを終了します。インスタンス ストアボリューム上のデータは、インスタンスの終了後は保持されません。したがって、インスタンスの廃止日より前にアクションを起こすことが重要です。まず、長期データを、影響を受ける各インスタンスのインスタンス ストア ボリュームから、Amazon S3 バケットや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ストレージに転送します。

代替サーバーが Outpost サイトに発送されます。次に、以下の操作を実行します。

- 修復できないサーバーからネットワークおよび電力ケーブルを取り外し、必要に応じてラックから取り外します。
- 同じ場所に交換用のサーバーを取り付けます。「Outpost サーバーのインストール」のインストール手順に従ってください。
- 修復不可能なサーバーを、代替サーバーが到着した AWS のと同じパッケージに梱包します。
- コンソールにアタッチされた注文構成の詳細または交換サーバーの注文に利用可能な、事前支払いの返品配送ラベルを使用してください。
- サーバーを に戻します AWS。詳細については、「AWS Outposts サーバーを返却する」を参照してください。

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。

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に関する最小要件を満たしている必要があります。Outposts サーバーは、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

通常、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、ネットワークメンテナンスが完了すると、アップストリームの企業ネットワークデバイスまたはサードパーティーの接続プロバイダーのネットワークで発生する可能性のあるネットワークの中断や問題から自動的に回復します。サービス リンク接続がダウンしている間、Outposts の操作はローカル ネットワーク アクティビティに限定されます。

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。

- ネットワークのメンテナンスを管理している場合は、サービス リンクのダウンタイムの期間を制限します。メンテナンスプロセスに、ネットワークが回復したことを確認するステップを含めます。
- 発表されたメンテナンス期間の終了時にサービス リンクがバックアップされていない場合、ネットワーク メンテナンスを管理できない場合は、発表されたメンテナンス期間に関してサービス リンクのダウンタイムを監視し、計画されたネットワーク メンテナンスの担当者に早めに エスカレーションしてください。

リソース

計画的または計画外の電力イベントやネットワーク イベントの後、Outpost が正常に動作していることを保証できる監視関連リソースをいくつか紹介します。

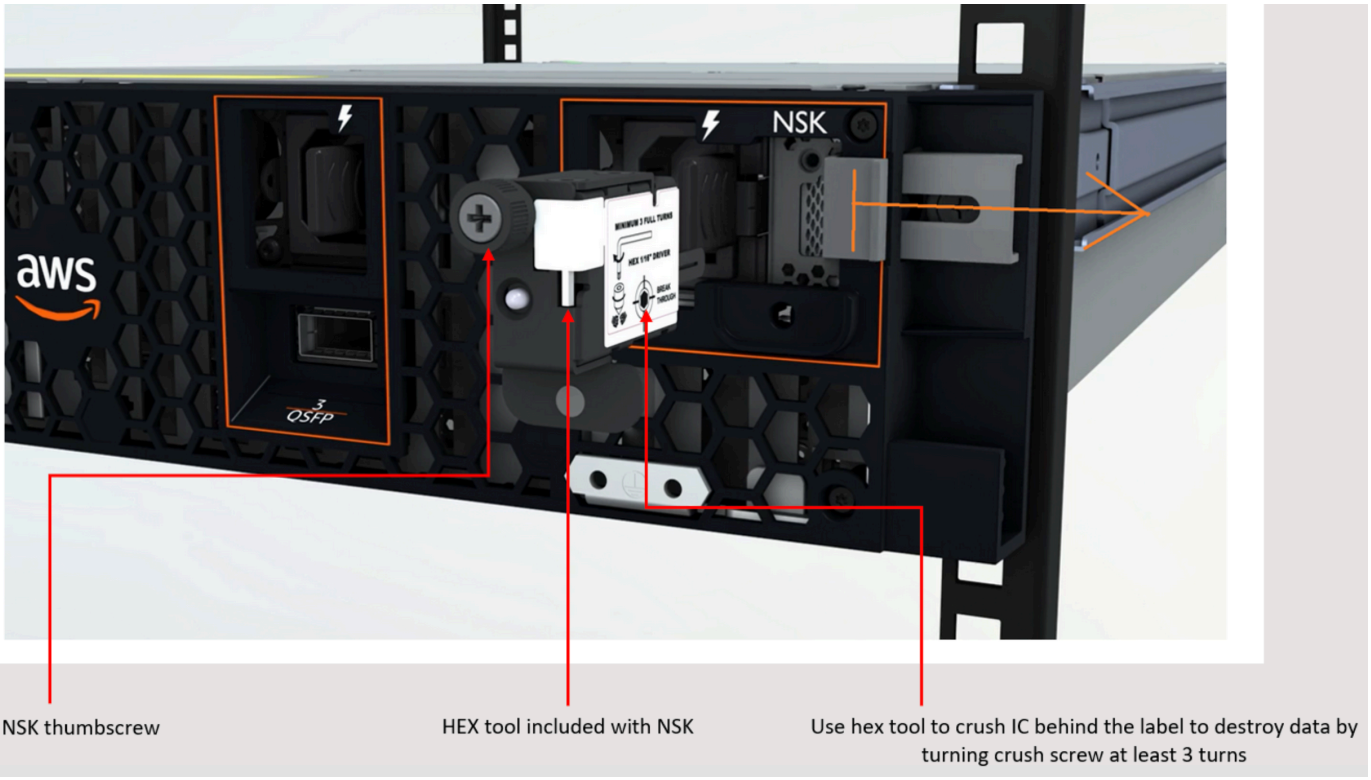
- AWS ブログ「 のベストプラクティスのモニタリング AWS Outposts」では、Outposts に固有のオブザーバビリティとイベント管理のベストプラクティスについて説明しています。
- AWS ブログ「Amazon VPC からのネットワーク接続用のデバッグツール」では、AWSSupport-SetupIPMonitoringFrom VPC ツールについて説明しています。本ツールは、お客様が指定したサブネットに Amazon EC2 Monitor Instance を作成し、対象の IP AWS Systems Manager アドレスを監視するためのドキュメント (SSM ドキュメント)です。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。このログは 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。

サーバーデータを暗号化して細断する

サーバー上のデータを復号化するには、Nitro セキュリティ キー (NSK) が必要です。サーバーを に戻すときは AWS、サーバーを交換するか、サービスを中止するかにかかわらず、NSK を破棄してサーバー上のデータを暗号化的にシュレッダーできます。

サーバー上のデータを暗号化してシュレッドするには

1. サーバーを に返送する前に、NSK をサーバーから削除します AWS。
2. サーバーに同梱されている正しい NSK を使用していることを確認してください。
3. ステッカーの下から小さな六角工具/六角レンチを取り外します。
4. 六角工具を使用して、ステッカーの下にある小さなネジを 3 回転させます。このアクションにより NSK が破壊され、サーバー上のすべてのデータが暗号化されてシュレッドされます。


NSK
aws
QSFP
NSK thumbscrew
HEX tool included with NSK
Use hex tool to crush IC behind the label to destroy data by turning crush screw at least 3 turns

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 サーバーを返却します。
- month-to-month サブスクリプションに変換し、既存の Outpost サーバーを維持します。

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 サーバーを維持するには

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 サーバー料金」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 サーバー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、サーバーを返却する

> **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、サブスクリプションを終了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. 必要に応じて、サーバーに存在するインスタンスとインスタンスデータをバックアップします。
14. サーバーで起動されたインスタンスを終了します。
15. 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。
16. サポートケースで指示されるまで、サーバーの電源を切ったり、ネットワークから切断したりしないでください。

AWS Outposts サーバーを返すには、AWS Outposts 「サーバーを返す」の手順に従います。

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 サーバーを維持するには、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たもの) 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
サーバーの E オプション nd-of-term AWS Outposts	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 AWS Outposts sサーバー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
プレイスメントグループ:オン 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:オン 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
Outpost サーバーの紹介	AWS Outposts 新しいフォームファクターであるOutposts sサーバーを追加しました。	2021 年 11 月 30 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。