Outposts サーバーのユーザーガイド

AWS Outposts

AWS Outposts: Outposts サーバーのユーザーガイド

Table of Contents

とは AWS Outposts

AWS Outposts は、 AWS インフラストラクチャ、サービス、APIs、ツールをお客様のオンプレミスに拡張するフルマネージドサービスです。 AWS マネージドインフラストラクチャへのローカルアクセスを提供することで、 AWS Outposts は、レイテンシーを短縮し、ローカルデータ処理のニーズに応じて、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 サブネットのインスタンスは、プライベート IP アドレス AWS を使用してリージョン内の他のインスタンスと通信します。すべて同じ 内にありますVPC。

> **Note**
>
> Outpost を同じ 内の別の Outpost またはローカルゾーンに接続することはできませんVPC。

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、電源シェルフ、空白パネルが含まれます。

- Outposts サーバー – 業界標準の 1U または 2U サーバーである Outpost フォームファクター。標準の EIA-310D 19 準拠の 4 ポストラックにインストールできます。Outposts サーバーは、スペースが制限されたり、容量要件が小さいサイトにローカルコンピューティング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 とそれに関連付けられた AWS リージョン間の通信を可能にするネットワークルート。各Outpostは、アベイラビリティーゾーンとそれに関連付けられたリージョンの拡張です。
- ローカルゲートウェイ (LGW) — Outposts ラックとオンプレミスネットワーク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 — Outposts サーバーとオンプレミスネットワークからの通信を可能にするネットワークインターフェイス。

AWS Outposts の リソース

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

コンピューティング

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

い

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	いえ
Amazon EMRクラスター	はい	いえ
Amazon RDS DB インスタンス	はい	いえ

ネットワーク

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

リソースタイプ	ラック	サーバー
Amazon Route 53	はい	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	いえ
Amazon S3 バケット	はい	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

インスタンスEC2タイプとストレージオプションの組み合わせを提供するさまざまな Outpost 設定から選択できます。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。

1 年または 3 年の期間の設定を購入し、全額前払い 、一部前払い 、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。一部前払いまたは前払いなしオプションを選択した場合、月額料金が適用されます。前払い料金は、Outposts ラックがアクティブ化されてから 24 時間後、つまり Outposts ラックの容量がインスタンスの起動に使用できるようになったときに適用されます。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LANまたはアプリケーションが存在するローカルネットワークに または WAN アクセスを提供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。

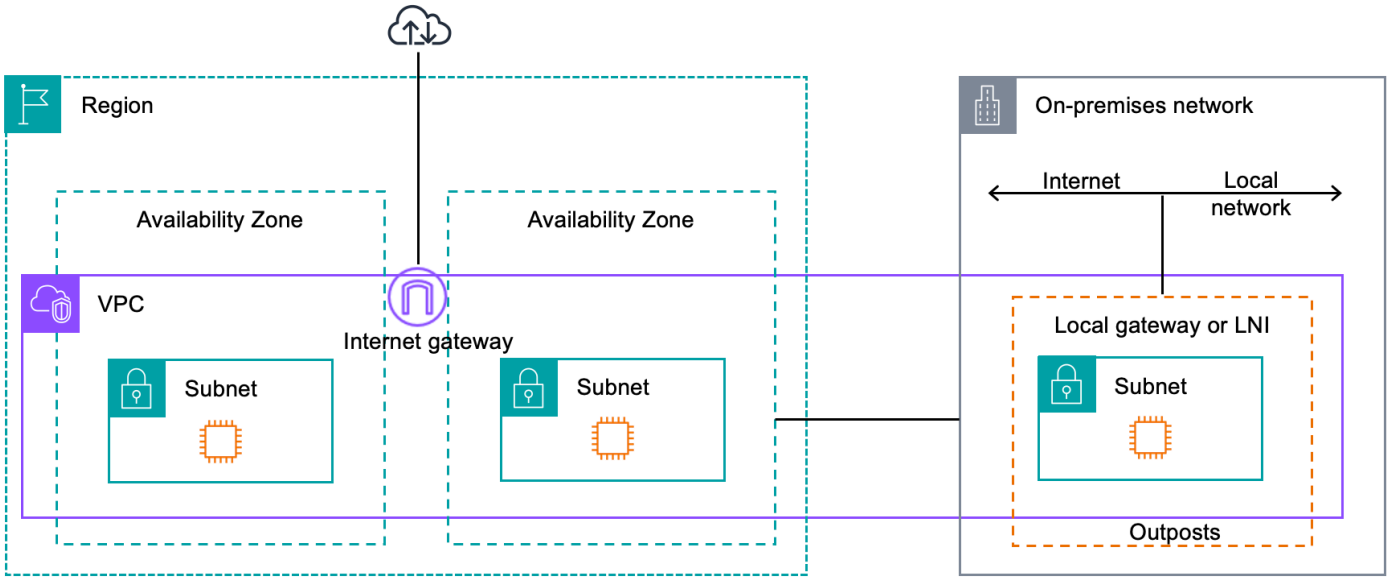
内容

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 を リージョンVPC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
- リージョンに複数のサブネットVPCがある
- 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



VPCs およびサブネット

仮想プライベートクラウド (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VPC内の任意のを Outpost に拡張できます。Outpost サブネットを に追加するにはVPC、サブネットの作成時に 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VPCsことができる複数の をサポートできます。クォータの詳細については、「Amazon VPC VPCユーザーガイド」の「Amazon Quotas」を参照してください。 VPC

Outpost サブネットは、Outpost をVPC作成した VPCCIDRの範囲から作成します。Outpost サブネットに存在するEC2インスタンスなどのリソースには、Outpost アドレス範囲を使用できます。

ルーティング

デフォルトでは、すべての Outpost サブネットが からメインルートテーブルを継承しますVPC。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、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、各 Outpost サブネットがVPCローカルルートを継承します。つまりVPC、 内の送信先を持つ Outpost サブネットを含む、 内のすべてのトラフィックは、 でルーティングされたVPCCIDRままになりますVPC。

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 range – 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 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VPC。
- 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 VPCs上の複数の とのピアリング接続がある場合、 間のトラフィックは Outpost に VPCs残り、リージョンに戻るサービスリンクを使用しません。

DNS

に接続されているネットワークインターフェイスの場合VPC、Outposts サブネットのEC2インスタンスは Amazon Route 53 DNS Service を使用してドメイン名を IP アドレスに解決できます。Route 53 は、Outpost で実行されているインスタンスのドメイン登録、DNSルーティング、ヘルスチェックなどのDNS機能をサポートしています。特定のドメインへのトラフィックのルーティングでは、パブリックおよびプライベートの両方のホスト型アベイラビリティゾーンがサポートされています。Route 53 リゾルバーは AWS リージョンでホストされます。したがって、これらのDNS機能を機能させるには、Outpost から AWS リージョンに戻る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。このような場合は、オンプレミス環境に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サーバーのDHCPオプションセットを作成し、 に関連付ける必要がありますVPC。また、これらのDNSサーバーへの IP 接続があることを確認する必要があります。また、到達可能性のためにローカルゲートウェイルーティングテーブルにルートを追加する必要がある場合もありますが、これはローカルゲートウェイを備えた Outposts ラックのオプションにすぎません。DHCP オプションセットにはVPCス

コープがあるため、Outpost サブネットと のアベイラビリティーゾーンサブネットの両方のインスタンスVPCは、DNS名前解決に指定されたDNSサーバーを使用しようとします。

クエリログは、Outpost から送信されるDNSクエリで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 ホームリージョンに戻る接続です。サービスリンクは、Outpost が選択したホームリージョンと通信するたびに使用される暗号化されたVPN接続のセットです。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を使用すると、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 間のトラフィックVPC内の両方が可能になります。

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

- 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

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

Outposts サーバーのサイト要件

Outpost サイトは、Outpost が動作する物理的な場所です。サイトは選択された国と地域でのみ利用可能です。詳細については、「 AWS Outposts サーバーFAQs」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。Outposts ラックの要件については、「Outposts ラックのユーザーガイド」の「Outposts ラックのサイト要件AWS Outposts 」を参照してください。

内容

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。
- 空気の品質 – 空気は MERV8 (またはそれ以上) フィルターを使用してフィルタリングする必要があります。
- 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、 の AWS Outposts コンソールでカタログを参照を選択しますhttps://console.aws.amazon.com/outposts/。
- Rail-Kit の互換性 – 配送パッケージに含まれているレールキットは、EIA-310-D 準拠の 19 インチラックの標準 L 字型マウントブラケットと互換性があります。次の図に示すように、レールキットは U 字型のマウントブラケットと互換性がありません。
- ラックの配置 — 深さが 36 インチ (914 mm) EIA以上の標準の 19 インチ -310D ラックを使用することをお勧めします。 AWS には、サーバーをラックに取り付けるためのレールキットが用意されています。
  - Outposts 2U サーバーには、高さ 3.5 インチ (88.9 mm)、幅 17.5 インチ (447 mm)、奥行き 30 インチ (762 mm) の寸法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) の寸法のスペースが必要です。
  - AWS Outposts サーバーを垂直方向にマウントすることはサポートされていません。
  - Outposts 1U サーバーは Outposts 2U サーバーと同じ幅ですが、高さの半分で深さの半分です。

  サーバーをラックに配置しない場合でも、他のサイト要件を満たしている必要があります。
- 保守性 - Outposts サーバーは正面通路での保守が可能です。
- アコースティクス – 80 ° F (27 ° C) の温度で 78 dBA 未満の音力と評価され、GR-63 CORENEBS に準拠しています。
- 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 サーバーには、冗長でない つの物理アップリンクポートが含まれています。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+	サービスと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) はトラフィックをセグメント化します。

サービスリンクファイアウォール

UDP および 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 が提供する 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
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 接続またはパブリックインターネット接続を使用して、Outpost を AWS リージョンに接続し直すことができます。Outposts サービスリンク接続の場合、ファイアウォールNATまたはエッジルーターPATで または 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 AWS リージョンのサービスリンクエンドポイントMTU間の 1500 バイトをサポートする必要があります。サービスリンクの詳細については、「サーバー用AWS Outposts ユーザーガイド」の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

最適なエクスペリエンスと耐障害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、最大 175 ms のラウンドトリップレイテンシーの冗長接続を使用する必要があります。各 Outposts 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 Outposts サーバーを使用します。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、「 サーバーのユーザーガイド」の「サーバーのサービスリンクトラフィックAWS Outposts 」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 をキャッシュしないことに注意してくださいAMIs。AMIs は、インスタンスの起動ごとに 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。

サービスリンクにはDHCPレスポンスが必要です

サービスリンクには、ネットワーク設定を構成するためのIPv4DHCPレスポンスが必要です。

サービスリンクの最大レイテンシー

サービスリンクは、サーバーとそのアベイラビリティーゾーンから最大 175 ミリ秒のネットワークレイテンシーをサポートできます。

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

電力ケーブル

サーバーには C14-C13 IEC 電源ケーブルが付属しています。

サーバーからラックへの電力ケーブル接続

付属の IECC14-C13 電源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、IECC13 ~ 5-15P NEMA の電源コードが必要です。
- 欧州の一部では、C13 から IEC 7/7 CEE までの電源コードが必要になる場合があります。
- インドでは、IS1293電源コードに IEC C13 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 () は含まれていませんUPS。

注文の履行

注文を満たすために、 AWS は、レールマウントや必要な電力ケーブル、ネットワークケーブルなどの Outposts サーバー機器をご指定の住所に配送します。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 / 111.8 cm
  - 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、「 サーバーのユーザーガイド」の「サーバーのサービスリンクトラフィックAWS Outposts 」を参照してください。

Outposts サーバーの Amazon EC2容量が から使用可能であることを確認すると、インストールは完了です AWS アカウント。

Outposts サーバーの使用を開始する

Outposts サーバーを注文して開始します。Outpost 機器をインストールしたら、Amazon EC2インスタンスを起動し、オンプレミスネットワークへの接続を設定します。

タスク

- Outpost を作成して Outpost 容量を注文する
- Outposts 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 サーバーのサイト要件」を参照してください。
- AWS エンタープライズサポートプランまたは AWS エンタープライズオンランプサポートプランが必要です。
- Outpost AWS アカウント を所有する を決定します。このアカウントを使用して、Outposts サイトを作成し、Outpost を作成し、注文してください。このアカウントに関連付けられている E メールをモニタリングして、 からの情報を確認します AWS。

タスク

- ステップ 1: サイトを作成する
- ステップ 2: Outpost を作成する
- ステップ 3: 注文を確定する
- ステップ 4: インスタンス容量を変更する
- 次のステップ

ステップ 1: サイトを作成する

サイトを作成し、営業住所を指定します。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、 によってサイトに ID が AWS Outposts 割り当てられます。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. で AWS Outposts コンソールを開きますhttps://console.aws.amazon.com/outposts/。
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。

> **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、 にお問い合わせください AWS Support。

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。一部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、期間中の月額料金が発生します。

  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. [Next (次へ)] を選択します。

6. [既存の Outpost を使用] を選択し、Outpost を選択します。
7. [Next (次へ)] を選択します。
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. [Next (次へ)] を選択します。
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. [Next (次へ)] を選択します。
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、容量が超過しているか不足しているかを通知するメッセージを表示します。インスタンスサイズまたは数量レベルで調整して、使用可能な合計容量を最適化します。
6. 特定のインスタンスサイズに合わせてインスタンス数を最適化 AWS Outposts するようにリクエストすることもできます。そのためには、次の操作を行います。
   a. インスタンスサイズを選択します。
   b. 関連するインスタンスタイプのセクションの最後にある自動調整を選択します。
7. インスタンスタイプごとに、インスタンス数が少なくとも 1 つのインスタンスサイズに指定されていることを確認します。
8. [Next (次へ)] を選択します。
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. [Next (次へ)] を選択します。

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. [Next (次へ)] を選択します。
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。注文についてご質問がある場合は、 にお問い合わせください AWS Support。

注文を満たすために、 AWS は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。インストールを行う場合もサードパーティーとの契約を行う場合も、インストールには、新しいデバイスの ID を検証するために Outpost AWS アカウント を含む の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、サーバーインストールガイド を参照してください。

Outpost の Amazon EC2容量が から使用可能になると、インストールは完了です AWS アカウント。容量が利用可能になったら、Outposts 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。

Outposts 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VPC内の任意の に追加できます。これを行うと、 は Outpost VPCにもまたがります。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、 にスキップしますステップ 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. で AWS Outposts コンソールを開きますhttps://console.aws.amazon.com/outposts/。
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ます。
5. [Create] (作成) を選択します。
6. サブネットを作成したら、ローカルネットワークインターフェイスのサブネットを有効にする必要があります。 AWS CLIで modify-subnet-attribute コマンドを使用します。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。次の例では、値 1 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します。

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

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、または自分と共有されている Outpost サブネットで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 サブネット内の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内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備えたインスタンスサイズを選択します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスストアボリューム」および「Instance Store-Backed AMI を作成する」を参照してください。

- Amazon EBS-backed は 1 つのEBSスナップショットAMIでのみ使用する必要があります。AMIs 複数のEBSスナップショットを持つ 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. で AWS Outposts コンソールを開きますhttps://console.aws.amazon.com/outposts/。
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 サブネットのローカルネットワークインターフェイス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です。または、後で追加するには、「」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の追加。
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 ユーザーガイド」のEC2「インスタンスの起動」を参照してください。 EC2

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、「ローカルネットワークインターフェイスの追加」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、これを行うには を使用しますDHCP。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。EC2 インスタンスへの接続の詳細については、「Amazon ユーザーガイド」のEC2「インスタンスに接続する」を参照してください。 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、インスタンスの詳細ページの Amazon EC2コンソールで確認できます。
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**
> Outposts 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、Outpost が選択したホームリージョンと通信するたびに使用される暗号化されたVPN接続のセットです。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 間のトラフィックVPC内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介してリージョンVPNへの AWS サービスリンクを作成できます。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 内の特定のルートVLAN、または 0.0.0.0/0 のデフォルトルートを介して行うことができます。 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VPCs、カスタマーデータプレーントラフィックを含む、関連する の間のトラフィック。

サービスリンクの最大送信単位 (MTU) 要件

ネットワーク接続の最大送信単位 (MTU) は、接続を介して渡すことができる最大許容パケットのサイズをバイト単位で表したものです。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MTU間の 1500 バイト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MTUの間で必要な については、「Amazon 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)」を参照してください。 EC2

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耐障害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、最大 175 ms のラウンドトリップレイテンシーの冗長接続を使用する必要があります。各 Outposts 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 Outposts サーバーを使用します。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 をキャッシュしないことに注意してくださいAMIs。AMIs は、インスタンスの起動ごとに 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 が AWS リージョンVPC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 と関連付けられた の間のトラフィック VPCs

インターネット接続で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 への接続を制限している場合はVLAN、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、サービスリンクが Outpost からリージョンにのみVPN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 からの接続を制限する場合VLAN、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 が提供する 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 のインスタンスは、サービスリンクを使用して別の Outposts 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、Outposts 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 リージョン間のトラフィッ

クVPC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/アクティブ設計で異なるアベイラビリティーゾーンに親親された 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時間の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VPCへの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 Outposts 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 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、新しいサーバーを送信する交換プロセスを開始し、コンソールから配送ラベルを提供します AWS Outposts 。開始するには、次のステップを実行します。

タスク

- ステップ 1: サーバーを返却できるように準備する
- ステップ 2: 返送用配送ラベルを取得する
- ステップ 3: サーバーをパックする
- ステップ 4: 配送業者を通じてサーバーを返却する

サーバーが契約期間の終了に達したためにサーバーを返す場合、または別の理由でサーバーを返すには、 AWS Support センターにお問い合わせください。

ステップ 1: サーバーを返却できるように準備する

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。
   - AWS CLI を使用して 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 インスタンスのEC2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。

ステップ 2: 返送用配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. で AWS Outposts コンソールを開きますhttps://console.aws.amazon.com/outposts/。
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。

ステップ 3: サーバーをパックする

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。

ステップ 4: 配送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	にお問い合わせくださいUPS。 サーバーは以下の方法で返却できます。 • サイトの定期UPS集荷中にサーバーを返却します。 • UPS ロケーション でサーバーをドロップオフします。 • 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。

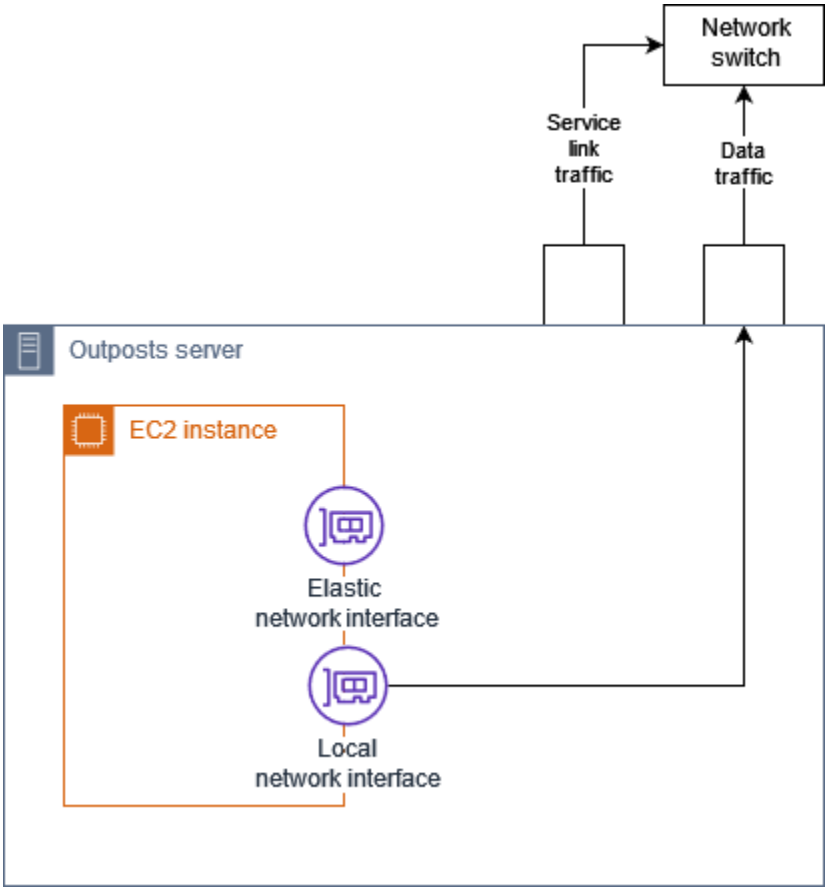
国	問い合わせ
他のすべての国	にお問い合わせくださいDHL。 サーバーは以下の方法で返却できます。 • DHL ロケーション でサーバーをドロップオフします。 • 希望の日時で集荷をスケジュールする。送料無料用に、 AWSが提供する配送ラベルからDHL配送状番号を入力します。 `Courier pickup can't be scheduled for an import shipment` というエラーが表示された場合は、通常は選択した集荷国が返品発送ラベルに記載された集荷国と一致していないことを意味します。発送元の国を選択して、もう一度試してください。

Outposts サーバーのローカルネットワークインターフェイス

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、Elastic Network Interface 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 サブネット内の EC2インスタンスを設定できます。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 に接続しますVPC。次の図は、Elastic Network Interface とローカルネットワークインターフェイスの両方を持つ 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実行されるため、 DHCPの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VPC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 サブネット内の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を追加する
- Outposts 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は、Outposts サーバーにVPCレイヤー 3 フローの可視性を提供しません。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、 および DHCP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 ユーザーガイド」の「ネットワークインターフェイスのクォータ」を参照してください。 VPC
- 各EC2インスタンスは、1 つのローカルネットワークインターフェイスを持つことができます。
- 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使用して複数のEC2インスタンスをホストできます。

> **Note**
>
> EC2 同じサーバー内の インスタンスは、Outposts サーバー外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、Outposts サーバーの 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、不敬モードや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ローカルネットワークインターフェイスは、物理 10 GbE の利用可能な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.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 のセキュリティグループを使用しませんVPC。セキュリティグループは、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。ローカルネットワークインターフェイスが にアタッチされていませんVPC。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。詳細については、「Amazon ユーザーガイド」のEC2「インスタンスENAの設定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。 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、そのアドレスにローカルで管理されるMAC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、インターフェイスを削除するまで同じ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 サブネット内の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を追加する

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、 AWS CLIcreate-network-interfaceと のコマンドを使用しますattach-network-interface。

インスタンスの起動後にローカルネットワークインターフェイスを追加するには、次の手順に従います。インスタンスの起動時に追加する方法については、Outpost の「インスタンスを起動する」を参照してください。

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を追加するには

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. 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。
3. 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ローカルネットワークインターフェイスに適用されないため、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。
4. 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 サブネットのローカルネットワークインターフェイスの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です。

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中の状態にある間、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 Elastic Network Interface 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 からのローカルネットワークインターフェイスのプライベートIPv4アドレスが表示されますCIDR。このアドレスはローカルネットワークインターフェイスの IP アドレスではなく、使用できません。ただし、このアドレスはサブネット から割り当てられるためCIDR、サ

ブネットのサイズ設定で考慮する必要があります。ゲストオペレーティングシステム内のローカルネットワークインターフェイスの IP アドレスは、静的に、またはDHCPサーバーを介して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。マルチホームネットワーク設定をサポートするように、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設定してください。

Outposts サーバーのローカルネットワーク接続

このトピックでは、Outposts 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ーの要件について説明します。詳細については、「Outposts サーバーのローカルネットワークインターフェイス」を参照してください。

内容

ネットワーク上のサーバートポロジー

Outposts 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。

次の表は、Outposts サーバーのトラフィックタイプとラベルを示しています。

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 の管理と AWS リージョンと Outpost 間のトラフィックVPC内の両方が可能になります。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、カスタムVPNまたは Outpost VPNsからリージョンへのものです。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リンクトラフィック — このトラフィックにより、からローカルネットワークインターフェイスLANを介したローカルVPC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 Outposts サーバーには、冗長でない つの物理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、Outposts サーバーのポート 3 にアタッチ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。Outposts 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、ローカルネットワーク1インターフェイスリンクトラフィックには 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

スイッチのサービスリンクポートを、ゲートウェイと次のリージョンエンドポイントへのルートVLANを持つ へのタグなしアクセスポートとして設定します。

- サービスリンクエンドポイント
- Outposts 登録エンドポイント

Outpost が AWS リージョン内の登録エンドポイントを検出するには、サービスリンク接続にパブリックDNSにアクセスできる必要があります。接続には、Outposts サーバーと登録エンドポイントの間にNATデバイスを含めることができます。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 サーバーでは、 AWS リージョンへの最小アップリンク速度 20 Mbps が必要です。

ローカルネットワークインターフェイスリンクとサービスリンクの使用率によっては、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ローカルネットワークインターフェイスリンクポートを、ローカルネットワークVLAN上の への標準アクセスポートとして設定します。複数の がある場合は

VLAN、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。複数のMACアドレスを想定するようにアップストリームネットワークデバイスのポートを設定します。サーバー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には、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があります。

> **Note**
>
> AWS Outposts サーバーはVLANトラフィックにタグを付けません。ローカルネットワークインターフェイス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を付けることを確認する必要があります。

次の例は、Amazon Linux 2023 でローカルネットワークインターフェイスのVLANタグ付けを設定する方法を示しています。別の Linux ディストリビューションを使用している場合は、VLANタグ付けの設定に関する 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 および Amazon Linux 2 でローカルネットワークインターフェイスの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。

   - ローカルネットワークインターフェイスのインターフェイス名は です。 `ens6`
   - VLAN ID は 59
   - VLAN デバイスに割り当てられた名前は です。 `ens6.59`

   ```
   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タグ付けの変更を永続化するには、次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 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。 EC2
- 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

Outposts サーバーにパブリック 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 ネットワークでデバイスを設定する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。Outposts サーバーでは、次の DHCP2 つの方法を使用できます。

- 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、Outposts サーバーは DHCPを使用してローカルネットワーク。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。Outposts 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。

ローカルネットワークインターフェイスリンクの場合は、 DHCPを使用して、ローカルネットワークにアタッチするインスタンスを設定します。詳細については、「」を参照してくださいthe section called “オペレーティングシステムの設定”。

> **Note**
>
> Outposts サーバーには安定した IP アドレスを使用していることを確認してください。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

Outposts サーバーがローカルネットワーク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、自身を登録します。登録にはパブリック が必要ですDNS。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。Outposts 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。Outposts サーバーは、 を介したプライベート接続をサポートしていませんVPC。

AWS Outposts リソースを共有する

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

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、コンシューマーが共有しているキャパシティー予約で起動するインスタンスを変更することはできません。

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

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

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

内容

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

- 専有ホストの割り当て — このリソースにアクセスできるコンシューマーは、以下のことができます。
  - Dedicated Host 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。
  - を使用して、 AWS Outposts APIOutpost 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 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。 VPC

Outposts リソースを共有するための前提条件

- Outpost リソースを の組織または組織単位と共有するには AWS Organizations、 との共有を有効にする必要があります AWS Organizations。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、アカウント内でそのリソースを所有している必要があります AWS 。共有されている Outpost リソースを共有することはできません。
- Outpost リソースを共有するには、組織内のアカウントと共有する必要があります。

関連サービス

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

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

アベイラビリティーゾーン間での共有

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

アカウントに関連する Outpost リソースの場所を特定するには、アベイラビリティーゾーン ID (AZ ID) を使用する必要があります。AZ ID は、すべての AWS アカウントでアベイラビリティーゾーンの一意で一貫性のある識別子です。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です。

アカウントのIDsアベイラビリティーゾーンの AZ を表示するには

1. https://console.aws.amazon.com/ram で AWS RAM コンソールを開きます。
2. 現在のリージョンIDsの AZ は、画面の右側にある AZ ID パネルに表示されます。

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

Outpost リソースの共有

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

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

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

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

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

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

AWS RAM コンソールにリダイレクトされ、次の手順を使用して Outpost の共有が完了します。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、所有している Outpost またはローカルゲートウェイルートテーブルを共有するには

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

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

create-resource-share コマンドを使用します。

共有 Outpost リソースの共有解除

共有 Outpost の共有が解除されると、コンシューマーは AWS Outposts コンソールで Outpost を表示できなくなります。Outpost で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 コンソールまたは を使用して Outpost の詳細とインスタンスタイプを表示したりすることはできません AWS CLI。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に新しい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VPCs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。これは、 AWS RAM コンソールまたは を使用して実行できます AWS CLI。

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

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

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

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

共有 Outpost リソースの特定

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

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

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

を使用して共有 Outpost リソースを識別するには AWS CLI

list-outposts コマンドと describe-local-gateway-route-tables コマンドを使用します。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 Outposts で作成するリソースを表示、変更、削除できます。

コンシューマーのアクセス許可

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

請求と使用量測定

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

ローカルゲートウェイルートテーブルの共有に追加料金はかかりません。共有サブネットの場合、VPC所有者は 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レベルのリソースに対して課金されます。

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

制限事項

AWS Outposts 共有の使用には、次の制限が適用されます。

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

のセキュリティ AWS Outposts

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

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS は AWS にあります。 AWS また、 では、安全に使用できるサービスも提供しています。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 サーバー FAQ」を参照してください。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Outposts。ここでは、セキュリティとコンプライアンスの目標を満たす方法を説明します。また、リソースのモニタリングや保護に役立つ他の AWS 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 () 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IAM。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FAQ」を参照してください。欧州におけるデータ保護の詳細については、AWS 「 セキュリティブログ」のAWS 「責任共有モデル」とGDPRブログ記事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に保存されている外部キーである Nitro セキュリティキー () にラップされますNSK。NSK は、Outposts サーバー 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 インスタンス終了すると、そのインスタンスに割り当てられたメモリは、ハイパーバイザーによってスクラブ (ゼロに設定) され、その後、新しい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 追加料金なしで を使用できます。

内容

AWS Outposts と の連携方法 IAM

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

IAM AWS Outposts で使用できる機能

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	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	あり
ACLs	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	いいえ
サービスリンクロール	あり

AWS Outposts のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」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、許可または拒否されたアクションとリソース、およびアクションが許可または拒否され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、「 ユーザーガイド」の「 IAMJSONポリシー要素のリファレンスIAM」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: なし

リソースベースのポリシーは、リソースにアタッチする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の例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。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コントロールできます。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、リソースベースのポリシーで、アカウント全体または別のアカウントのIAMエンティティをプリンシパルとして指定できます。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さらに付与する必要はありません。詳細については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」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のサポート: あり

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

JSON ポリシーの `Action`要素は、ポリシーで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を記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数の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

ポリシーリソースのサポート: あり

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

Policy `Resource`JSON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、リソースレベルの許可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 AWS API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。1 つのステートメントで複数のリソースを指定するには、 をカンマARNsで区切ります。

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

AWS Outposts リソースタイプとその のリストを確認するにはARNs、「サービス認証リファレンス」の「 で定義されるリソースタイプ AWS Outposts」を参照してください。各リソースARNの を指定できるアクションについては、「 で定義されるアクション AWS Outposts」を参照してください。

AWS Outposts のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

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

Condition 要素 (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 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では 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ユーザー名でタグ付けされている場合にのみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」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、「 ユーザーガイド」のAWS 「 グローバル条件コンテキストキーIAM」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。

ACLs AWS Outposts の

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

ABAC AWS Outposts を使用する

サポート ABAC (ポリシー内のタグ): はい

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。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、の最初のステップですABAC。次に、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する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

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

の詳細についてはABAC、「 IAMユーザーガイド」の「 とはABAC」を参照してください。のセットアップ手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用するIAM」を参照してください。

AWS Outposts での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の 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、 ユーザーガイドのAWS のサービス 「 と連携する IAM IAM 」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、会社のシングルサインオン (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。ロールの切り替えの詳細については、「 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 を使用して手動で作成できます AWS API。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、「」の「一時的なセキュリティ認証情報IAM」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

転送アクセスセッションをサポート (FAS): 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 へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。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: なし

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

AWS Outposts のサービスにリンクされたロール

サービスリンクロールのサポート: あり

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

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

AWS Outposts ポリシーの例

デフォルトでは、ユーザーとロールには 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 を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

各リソースタイプの 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 OutpostsARNs」を参照してください。

内容

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

ポリシー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、「 ユーザーガイド」の「 AWS 管理ポリシーAWS 」または「 ジョブ機能の 管理ポリシーIAM」を参照してください。
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの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、アクションと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 を使用して送信する必要があることを指定できますSSL。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、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」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、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されてい

ます。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。

- 多要素認証を要求する (MFA) – 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MFAするために をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、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「 で保護されたAPIアクセスの設定」を参照してください。

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「 のセキュリティのベストプラクティスIAMIAM」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"
    }
  ]
}
```

のサービスにリンクされたロール AWS Outposts

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

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

サービスリンクロールは、関連する リソースを削除した後でしか削除できません。これにより、AWS Outposts リソース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。

のサービスにリンクされたロールのアクセス許可 AWS Outposts

AWS Outposts は、AWSServiceRoleForOutposts_ 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。***OutpostID*** — Outposts がユーザーに代わってプライベート接続用の AWS リソースにアクセスできるようにします。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*** ポリシーでは 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: `all AWS resources that match the following Condition:` 上で `ec2:CreateTags`

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

IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、または削除できるようにするには、アクセス許可を設定する必要があります。詳細について

は、「 ユーザーガイド」の「サービスにリンクされたロールのアクセス許可IAM」を参照してください。

のサービスにリンクされたロールを作成する AWS Outposts

サービスリンクロールを手動で作成する必要はありません。で Outpost のプライベート接続を設定すると AWS 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。

のサービスにリンクされたロールを編集する AWS Outposts

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

のサービスにリンクされたロールを削除する AWS Outposts

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

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

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

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_ が使用する AWS Outposts リソースを削除するには***OutpostID***

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。

を使用してサービスにリンクされたロールを手動で削除するには IAM

詳細については、「 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IAM」を参照してください。

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

AWS Outposts は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、FAQs「 for Outposts ラックと Outposts サーバー」を参照してください。

AWSAWS Outposts の マネージドポリシー

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

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース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。 AWS のサービス は、新しい AWS が起動されたとき、または既存のサービスで新しいAPI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、「 ユーザーガイド」の「 AWS 管理ポリシーIAM」を参照してください。

AWS マネージドポリシー： AWSOutpostsServiceRolePolicy

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

AWS 管理ポリシー： AWSOutpostsPrivateConnectivityPolicy

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

AWS 管理ポリシー： AWSOutpostsAuthorizeServerPolicy

このポリシーを使用して、オンプレミスネットワークで Outposts サーバーハードウェアを承認するために必要なアクセス許可を付与します。

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": "*"
    }
  ]
}
```

AWSAWS 管理ポリシーに対する Outposts の更新

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

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内の Outposts 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 は、 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呼び出しを使用して、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) 。1TLS.2 が必要で、1.3 TLS をお勧めします。
- (Ephemeral Diffie-HellmanPFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を備えた暗号スイート。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。

さらに、 リクエストは、 IAMプリンシパルに関連付けられたアクセスキー ID と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 のインフラストラクチャセキュリティEC2」を参照してください。

VPC Flow Logs は、 AWS リージョンの場合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正常性をモニタリングし、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呼び出しへの応答、Outpost のモニタリング、Outpost の更新などのコントロールプレーンオペレーションをサポートします。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。 では、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HIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – 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**
>
> すべての AWS のサービス がHIPAA対象となるわけではありません。詳細については、HIPAA「対象サービスリファレンス」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) など) 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把握できます 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DSS、 PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- 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。

Outposts サーバーのモニタリング

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 サーバー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 Outposts メトリクス」を参照してください。

CloudTrail ログ

を使用して AWS CloudTrail 、 に対して行われた呼び出しに関する詳細情報をキャプチャします AWS APIs。これらの呼び出しはログ ファイルとして Amazon S3 に保存できます。これらの CloudTrail ログを使用して、呼び出しが行われた日時、呼び出し元の送信元 IP アドレス、呼び出し元、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。また、Amazon EC2や Amazon などの Outpost 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EBS。詳細については、「を使用したAPI通話のログ記録 CloudTrail」を参照してください。

VPC フローログ

VPC フローログを使用して、Outpost との間で送受信されるトラフィック、および Outpost 内で送受信されるトラフィックに関する詳細情報をキャプチャします。詳細については、「Amazon VPCユーザーガイドVPC」の「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、Outposts サーバーから out-of-band 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 VPC トラフィックミラーリングガイド」を参照してください。

AWS Health Dashboard

には、 AWS リソースの正常性の変化によって開始される情報と通知 AWS Health Dashboard が表示されます。情報は 2 つの方法で表示されます。ダッシュボードには、最近のイベントおよび予定されているイベントがカテゴリ別に分類されて表示されます。詳細なイベントログには、過

去 90 日間のすべてのイベントが表示されます。たとえば、サービスリンク上の接続の問題によりイベントが開始され、ダッシュボードとイベントログに表示され、イベントログに 90 日間残ります。 AWS Health サービスの一部である はセットアップを AWS Health Dashboard 必要とせず、アカウントで認証されたすべてのユーザーが表示できます。詳細については、「Getting started with the AWS Health Dashboard」を参照してください。

CloudWatch Outposts メトリクス

AWS Outposts は、Outposts CloudWatch のデータポイントを Amazon に発行します。 CloudWatch では、こ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ます。メトリクスは監視対象の変数、データポイントは時間の経過と共に変わる変数の値と考えることができます。たとえば、指定した期間にわたって Outpost で利用可能なインスタンスの容量を監視できます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。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1、 は 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設定の変更、インターネット接続の問題などがあります。`ConnectedStatus` 問題が発生した場合は、オンプレミスネットワーク内から AWS リージョンへの接続を確認し、問題が解決しない場合は Support に連絡 AWS 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 ユーザーガイド CloudWatch 」を参照してください。

内容

メトリクス

`AWS/Outposts` 名前空間には、次の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1より小さい場合、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`

起動など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`、および`OutpostId`

`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`、および`OutpostId`

`UsedInstanceType_Count`

Amazon Relational Database Service (Amazon) 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、現在使用されているインスタンスタイプの数。 RDS Application Load Balancer 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`、および`OutpostId`

`AvailableInstanceType_Count`

使用可能なインスタンスタイプ。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`

キャパシティ予約 を使用して予約されたコンピューティングキャパシティーで起動できるインスタンスの数。このメトリクスには Amazon EC2リザーブドインスタンス は含まれません。

単位: 個

最大解像度:5 分

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

`UsedReservedInstances`

キャパシティ予約 を使用して予約されたコンピューティングキャパシティで実行されているインスタンスの数。このメトリクスには Amazon EC2リザーブドインスタンス は含まれません。

単位: 個

最大解像度:5 分

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

`TotalReservedInstances`

キャパシティ予約 を使用して予約されたコンピューティングキャパシティによって提供される、実行中で起動可能なインスタンスの合計数。このメトリクスには Amazon EC2リザーブドインスタンス は含まれません。

単位: 個

最大解像度:5 分

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

メトリクスディメンション

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 () の仮想インターフェイスグループの IDVIF。

Outposts サーバーの CloudWatch メトリクスを表示する

CloudWatch コンソールを使用して、Outposts サーバーの 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. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. ナビゲーションペインで Metrics (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、検索フィールドに名称を入力します。

を使用してメトリクスを表示するには AWS CLI

使用可能なメトリクスを表示するには、次の list-metrics コマンドを使用します。

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

を使用してメトリクスの統計を取得するには AWS CLI

次のget-metric-statisticsコマンドを使用して、指定されたメトリクスと 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
```

を使用した通話のログ AWS Outposts API記録 AWS CloudTrail

AWS Outposts は、ユーザー AWS CloudTrail、ロール、または service. CloudTrail captures が をイベント AWS Outposts としてAPI呼び出すアクションを記録する AWS サービスである と統合されています。キャプチャされた呼び出しには、 AWS Outposts コンソールからの呼び出しと、 API オペレーションへのコード呼び出しが含まれます AWS Outposts 。で収集された情報を使用して CloudTrail、 に対して行われたリクエスト AWS Outposts、リクエスト元の IP アドレス、リクエスト日時などの詳細を確認できます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

CloudTrail AWS アカウントを作成すると、 はアカウントでアクティブになり、 CloudTrail イベント履歴 に自動的にアクセスできます。 CloudTrail イベント履歴は、 に記録された過去 90 日間の管理イベントの表示可能、検索可能、ダウンロード可能、およびイミュータブルなレコードを提供します AWS リージョン。詳細については、「 ユーザーガイド」の CloudTrail 「イベント履歴の使用AWS CloudTrail 」を参照してください。イベント履歴を表示するための料金はかかりません CloudTrail。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。を使用して作成された証跡はすべてマルチリージョン AWS Management Console です。 AWS CLIを使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント AWS リージョン 内のすべての でアクティビティをキャプチャするため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョンに記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウントの証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成 CloudTrail することで、 から Amazon S3 バケットに継続的な管理イベントのコピーを 1 つ無料で配信できますが、Amazon S3 ストレージ料金が発生します。 CloudTrail 料金の詳細については、「 の料金AWS CloudTrail」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

CloudTrail Lake では、イベントに対して SQLベースのクエリを実行できます。 CloudTrail Lake は、既存のイベントを行ベースのJSON形式で Apache ORC 形式に変換します。ORC は、データの高速取得に最適化された列指向ストレージ形式です。イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。 CloudTrail Lake の詳細については、「 ユーザーガイド」の AWS CloudTrail 「Lake の使用AWS CloudTrail 」を参照してください。

CloudTrail Lake イベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。 CloudTrail 料金の詳細については、「 の料金AWS CloudTrail」を参照してください。

AWS Outposts の管理イベント CloudTrail

管理イベントは、 のリソースで実行される管理オペレーションに関する情報を提供します AWS アカウント。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。デフォルトでは、 は管理イベント CloudTrail を記録します。

AWS Outposts は、すべての Outposts AWS コントロールプレーンオペレーションを管理イベントとしてログに記録します。 AWS Outposts が に記録する Outposts AWS コントロールプレーンオペレーションのリストについては CloudTrail、「Outposts AWS APIリファレンス」を参照してください。

AWS Outposts イベントの例

次の例は、 `SetSiteAddress`オペレーションを示す CloudTrail イベントを示しています。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
```

```
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Outposts サーバーのメンテナンス

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、Outposts サーバーのパフォーマンス、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、インスタンスストアボリュームの長期データを、オンプレミスネットワーク内の Amazon S3 バケット、ネットワークストレージデバイスなどの永続的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、サーバーのプロビジョニングプロセス中、または Outposts サーバー で実行されている Amazon EC2インスタンスをホストしている間に、ハードウェアの回復不可能な問題 AWS を検出した場合、影響を受けたインスタンスのリタイアが予定されていることを Outpost 所有者とインスタンスの所有者の両方に通知します。詳細については、「Amazon ユーザーガイド」の「インスタンスの廃止」を参照してください。 EC2

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。「Outposts 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。

電力およびネットワーク イベントのベスト プラクティス

AWS Outposts お客様向けのAWS サービス条件に記載されているように、Outposts 機器を設置する施設は、Outposts 機器のインストール、メンテナンス、使用をサポートするために、電力とネットワークの最小要件を満たしている必要があります。Outposts 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。

- DNSベースまたはオフラックの負荷分散の変更を使用して、制御された方法でサービスとアプリケーションを Outposts 機器から移動します。
- 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。
- メンテナンス中に電源 (off-on-off-on) を繰り返し切り替えないようにしてください。
- 予期せぬ事態に対処するために、メンテナンス期間内に余分な時間を確保してください。
- 通常必要とされるよりも広いメンテナンス時間枠を伝えることで、ユーザーや顧客の期待に応えます。

ネットワーク接続イベント

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

Outposts サーバー上の Amazon EC2インスタンス、LNIネットワーク、およびインスタンスストレージボリュームは引き続き正常に動作し、ローカルネットワークおよび を介してローカルにアクセスできますLNI。同様に、Amazon ECSワーカーノードなどの AWS サービスリソースは引き続きローカルで実行されます。ただし、API可用性は低下します。例えば、実行、開始、停止、終了が機能しないAPIs場合があります。インスタンスのメトリクスとログは数時間ローカルにキャッシュされ続け、接続が戻ると AWS リージョンにプッシュされます。ただし、数時間以上切断すると、メトリクスとログが失われる可能性があります。

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「 のモニタリングのベストプラクティス AWS Outposts」では、Outposts 固有のオブザーバビリティとイベント管理のベストプラクティスについて説明しています。
- AWS ブログ「Amazon からのネットワーク接続用のデバッグツールVPC」では、AWSSupport-S etupIPMonitoringFromVPC ツールについて説明しています。このツールは、ユーザーが指定したサブネットに Amazon EC2 Monitor インスタンスを作成し、ターゲット IP アドレスをモニタリングする AWS Systems Manager ドキュメント (SSM ドキュメント) です。このドキュメントでは、pingMTR、、TCPトレースルート、トレースパスの診断テストを実行し、結果を Amazon CloudWatch Logs に保存します。その結果は CloudWatch ダッシュボードで視覚化できます (レイテンシー、パケットロスなど) 。Outposts モニタリングの場合、モニターインスタンスは親 AWS リージョンの 1 つのサブネットにあり、プライベート IP (複数可) を使用して 1 つ以上の Outpost インスタンスをモニタリングするように設定する必要があります。これにより、 AWS Outposts と親 AWS リージョン間のパケット損失グラフとレイテンシーが提供されます。
- AWS ブログ「 AWS Outposts を使用するための自動 Amazon CloudWatch ダッシュボードのデプロイ AWS CDK」では、自動ダッシュボードのデプロイに関連する手順について説明しています。
- 質問がある場合、または詳細情報が必要な場合は、「AWS サポートユーザー ガイド」の「サポート ケースの作成」を参照してください。

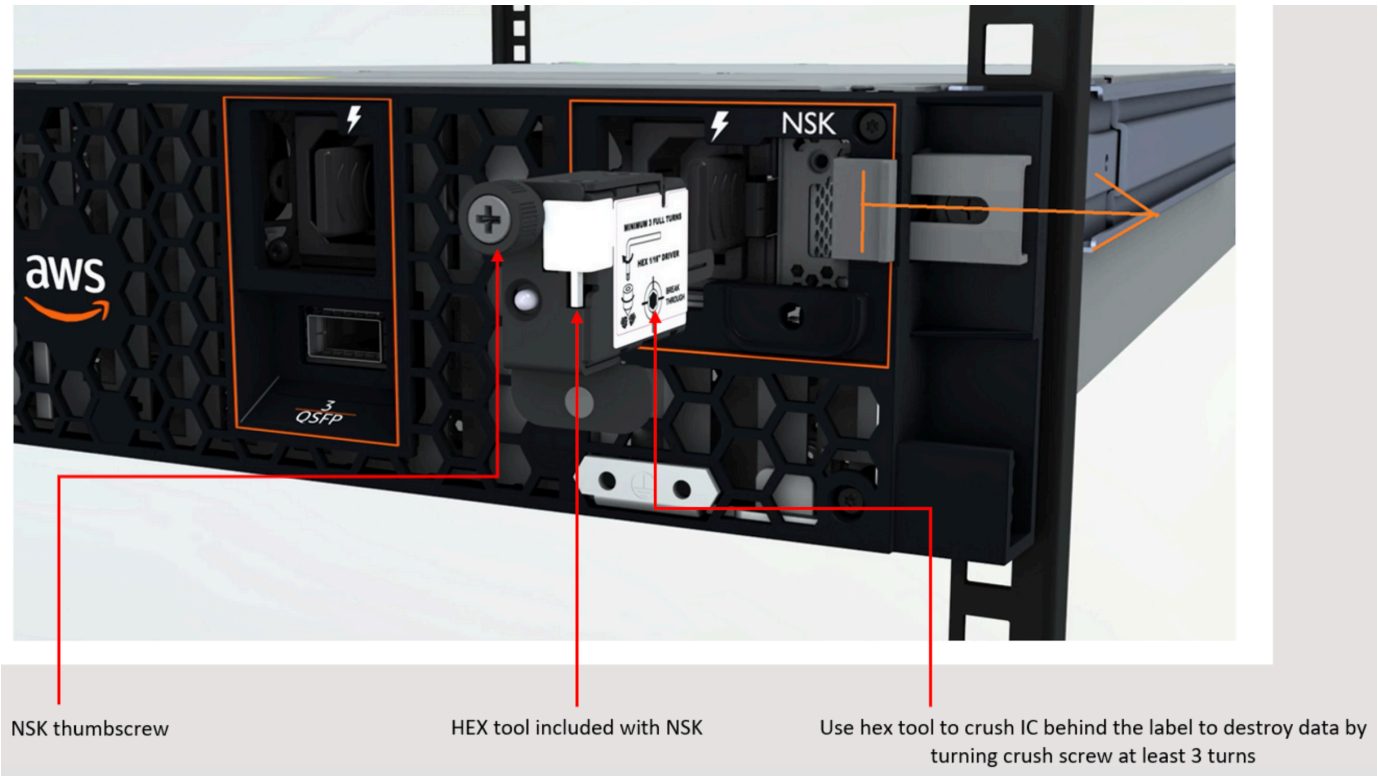
サーバーデータを暗号化して細断する

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、 を破棄NSK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、サーバーNSKから を削除します AWS。
2. サーバーに同梱NSKされている正しい があることを確認します。
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、 が破棄NSKされ、サーバー上のすべてのデータが暗号的に細断されます。



Outposts サーバー end-of-term オプション

AWS Outposts 期間の終了時に、次のオプションのいずれかを選択する必要があります。

- サブスクリプションを更新し、既存の Outposts サーバーを保持します。
- サブスクリプションを終了し、Outposts サーバーを返します。
- month-to-month サブスクリプションに変換し、既存の Outposts サーバーを保持します。

サブスクリプションを更新する

Outposts サーバーの現在のサブスクリプションが終了する少なくとも 30 日前に、次のステップを完了する必要があります。

サブスクリプションを更新して既存の Outposts サーバーを保持するには

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 Outposts 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

Outposts サーバーの現在のサブスクリプションが終了する少なくとも 30 日前に、次の手順を完了する必要があります。 AWS は、完了するまで戻りプロセスを開始できません。

> **Important**
>
> AWS は、サブスクリプションを終了するためのサポートケースを開いた後、返品プロセスを停止できません。

サブスクリプションを終了するには

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NOTの電源を切るか、ネットワークから切断します。

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 Outposts 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。新しい月額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。

Outposts サーバーのドキュメント履歴

次の表は、Outposts サーバー のドキュメントの更新を示しています。

変更	説明	日付
キャパシティ管理	新しい Outposts 注文のデフォルトの容量設定を変更できます。	2024 年 4 月 16 日
AWS Outposts サーバーの End-of-term オプション	AWS Outposts 期間が終了すると、サブスクリプションを更新、終了、または変換できます。	2023 年 8 月 1 日
Outposts サーバー用 AWS Outposts ユーザーガイドを作成	AWS Outposts ユーザーガイドは、ラックとサーバー用に別々のガイドに分かれています。	2022 年 9 月 14 日
でのプレイスメントグループ AWS Outposts	スプレッド戦略を使用する配置グループは、インスタンスを異なるホストに分散させることができます。	2022 年 6 月 30 日
の Dedicated Hosts 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
Outposts サーバーの紹介	新しい AWS Outposts フォームファクターである Outposts 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。