



Outposts サーバー用ユーザーガイド

AWS Outposts



AWS Outposts: Outposts サーバー用ユーザーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS Outposts	1
主要なコンセプト	1
AWS Outposts の リソース	2
料金	5
の AWS Outposts 仕組み	6
ネットワークコンポーネント	6
VPC とサブネット	7
ルーティング	8
DNS	8
サービスリンク	9
ローカルネットワークインターフェイス	9
サイト要件	10
施設	10
ネットワーク	11
サービスリンクファイアウォール	12
サービスリンクの最大送信単位 (MTU)	13
サービスリンクの推奨帯域幅	13
電源	13
電力サポート	13
消費電力	14
電力ケーブル	14
電源の冗長性	14
注文の履行	14
はじめに	16
Outpost を作成して 容量を注文する	16
ステップ 1: サイトを作成する	17
ステップ 2: Outpost を作成する	17
ステップ 3: 注文を確定する	18
ステップ 4: インスタンスキャパシティを変更する	19
次のステップ	21
インスタンスの起動	22
ステップ 1: サブネットの作成	22
ステップ 2: Outpost 上でインスタンスを起動	23
ステップ 3: 接続の構成	25

ステップ 4: 接続をテストする	25
サービスリンク	28
接続	28
最大送信単位 (MTU) 要件	29
帯域幅のレコメンデーション	13
冗長インターネット接続	30
更新とサービスリンク	30
ファイアウォールとサービスリンク	30
ネットワークのトラブルシューティング	32
初期評価	32
ステップ 1. 物理接続を確認する	33
ステップ 2. への Outposts サーバー接続をテストする AWS	33
ステップ 3. 接続を再確立する	34
サーバーを返却する	36
ステップ 1: サーバーを返却する準備をする	36
ステップ 2: 戻りラベルを印刷する	37
ステップ 3: サーバーを梱包する	38
ステップ 4: 宅配業者を通じてサーバーを返却する	38
ローカルネットワークインターフェイス	41
ローカルネットワークインターフェイスの基本	43
パフォーマンス	44
セキュリティグループ	45
モニタリング	45
MAC アドレス	45
ローカルネットワークインターフェイスの追加	45
ローカルネットワークインターフェイスの表示	46
オペレーティングシステムの設定	47
ローカル接続	47
ネットワーク上のサーバートポロジー	47
サーバーの物理的な接続	48
サーバーのサービスリンクトラフィック	49
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	49
サーバー IP アドレスの割り当て	51
サーバーの登録	51
キャパシティ管理	52
容量の表示	52

インスタンス容量の変更	19
考慮事項	53
キャパシティタスクの問題のトラブルシューティング	56
注文 <i>oo-xxxxxx</i> が Outpost ID <i>op-xxxxx</i> に関連付けられていません	57
キャパシティプランには、サポートされていないインスタンスタイプが含まれます。	57
Outpost ID <i>op-xxxxx</i> を持つ Outpost がない	58
Outpost <i>op-XXXX</i> のアクティブ CapacityTask <i>cap-XXXX</i> が既に見つかりました	58
Outpost <i>op-XXXX</i> のアセット <i>XXXX</i> に Active CapacityTask <i>cap-XXXX</i> が既に見つかりました	59
AssetId= <i>XXXX</i> は Outpost= <i>op-XXXX</i> には無効です	60
共有 リソース	62
共有可能な Outpost リソース	63
Outposts リソースを共有するための前提条件	64
関連サービス	64
アベイラビリティーゾーン間での共有	64
Outpost リソースの共有	65
共有 Outpost リソースの共有解除	66
共有 Outpost リソースの特定	67
共有 Outpost リソースの権限	67
所有者のアクセス許可	67
コンシューマーのアクセス許可	67
請求と使用量測定	68
制限	68
サードパーティーのブロックストレージ	69
外部ブロックデータボリューム	69
外部ブロックブートボリューム	70
セキュリティ	72
データ保護	72
保管中の暗号化	73
転送中の暗号化	73
データの削除	73
ID とアクセス管理	73
AWS Outposts と IAM の連携方法	74
ポリシーの例	78
サービスリンクロール	81
AWS マネージドポリシー	84

インフラストラクチャセキュリティ	86
耐障害性	86
コンプライアンス検証	87
モニタリング	88
CloudWatch メトリクス	89
メトリクス	89
メトリクスのディメンション	96
Outposts サーバーの CloudWatch メトリクスを表示する	96
CloudTrail を使用して API 呼び出しをログに記録する	97
AWS Outposts CloudTrail の管理イベント	99
AWS Outposts イベントの例	99
メンテナンス	101
連絡先の情報を更新する	101
ハードウェアメンテナンス	101
ファームウェアの更新	102
電力とネットワークのイベント	102
電力イベント	102
ネットワーク接続イベント	103
リソース	104
サーバーデータを暗号化して細断する	105
期末オプション	106
サブスクリプションを更新する	106
サーバーを返す	107
ステップ 1: サーバーを返却する準備をする	36
ステップ 2: サーバーを廃止する	108
ステップ 3: 返送用配送ラベルを取得する	37
ステップ 4: サーバーをパックする	38
ステップ 5: 配送業者を通じてサーバーを返却する	38
サブスクリプションの変換	112
クォータ	113
AWS Outposts および他の サービスのクォータ	113
ドキュメント履歴	114

とは AWS Outposts

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

Outpost は、お客様のサイトにデプロイされた AWS コンピューティングおよびストレージ容量のプールです。は、この容量を AWS リージョンの一部として AWS 運用、モニタリング、管理します。Outpost にサブネットを作成し、EC2 インスタンス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 を接続できません。

詳細については、[AWS Outposts 製品ページ](#)を参照してください。

主要なコンセプト

これらは の主要な概念です AWS Outposts。

- Outpost サイト – AWS が Outpost をインストールするカスタマー管理の物理的な建物。サイトは、Outpost の施設、ネットワーク、および電力の要件を満たさなければなりません。
- Outpost の容量 - Outpost で利用可能なコンピューティングおよびストレージリソース。 AWS Outposts コンソールから Outpost の容量を表示および管理できます。は、Outposts レベルで定義できるセルフサービスの容量管理 AWS Outposts をサポートし、Outposts 内のすべてのアセットを再設定したり、特に個々のアセットに対して再設定したりできます。Outpost アセットは、Outposts ラックまたは Outposts サーバー内の単一のサーバーにすることができます。
- 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、およびブランクパネルが含まれています。
- Outposts サーバー — 産業標準の 1U または 2U サーバーの Outpost フォームファクターです。標準の EIA-310D 19 インチ適合の 4 ポストラックに取り付けることができます。Outposts サーバーは、スペースが限られているか、キャパシティ要件が小さいサイトに対して、ローカルなコンピュートおよびネットワークサービスを提供します。
- Outpost 所有者 – AWS Outposts 注文を行うアカウントのアカウント所有者。が顧客と AWS やり取りした後、所有者は追加の連絡先を含めることができます。AWS は連絡先と通信して、注文、インストール予約、ハードウェアのメンテナンスと交換を明確にします。連絡先情報が変更された場合は、[AWS サポートセンター](#)に連絡してください。
- サービスリンク – Outpost と関連付けられた 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、アベイラビリティゾーンとそれに関連付けられたリージョンの拡張です。
- ローカルゲートウェイ (LGW) - Outposts ラックとオンプレミスネットワークとの間の通信が可能になる論理的な相互接続仮想ルーター。
- ローカルネットワークインターフェイス - Outposts サーバーからオンプレミスネットワークへの通信を可能にするネットワークインターフェイス。

AWS Outposts の リソース

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

コンピューティング

リソースタイプ	ラック	サーバー
Amazon EC2 インスタンス	 は い	 は い

リソースタイプ	ラック	サーバー
Amazon ECS クラスター		
Amazon EKS ノード		

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)		
Amazon EMR クラスター		
Amazon RDS DB インスタンス		

ネットワーク

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

[Storage (ストレージ)]

リソースタイプ	ラック	サーバー
<u>Amazon EBS ボリューム</u>	い	いいえ
<u>Amazon S3 バケット</u>	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

料金

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

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

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

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

- [Outposts ラックの料金](#)
- [Outposts サーバーの料金](#)

の AWS Outposts 仕組み

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

次の図は両方の Outpost フォームファクターを示しています。

内容

- [ネットワークコンポーネント](#)
- [VPC とサブネット](#)
- [ルーティング](#)
- [DNS](#)
- [サービスリンク](#)
- [ローカルネットワークインターフェイス](#)

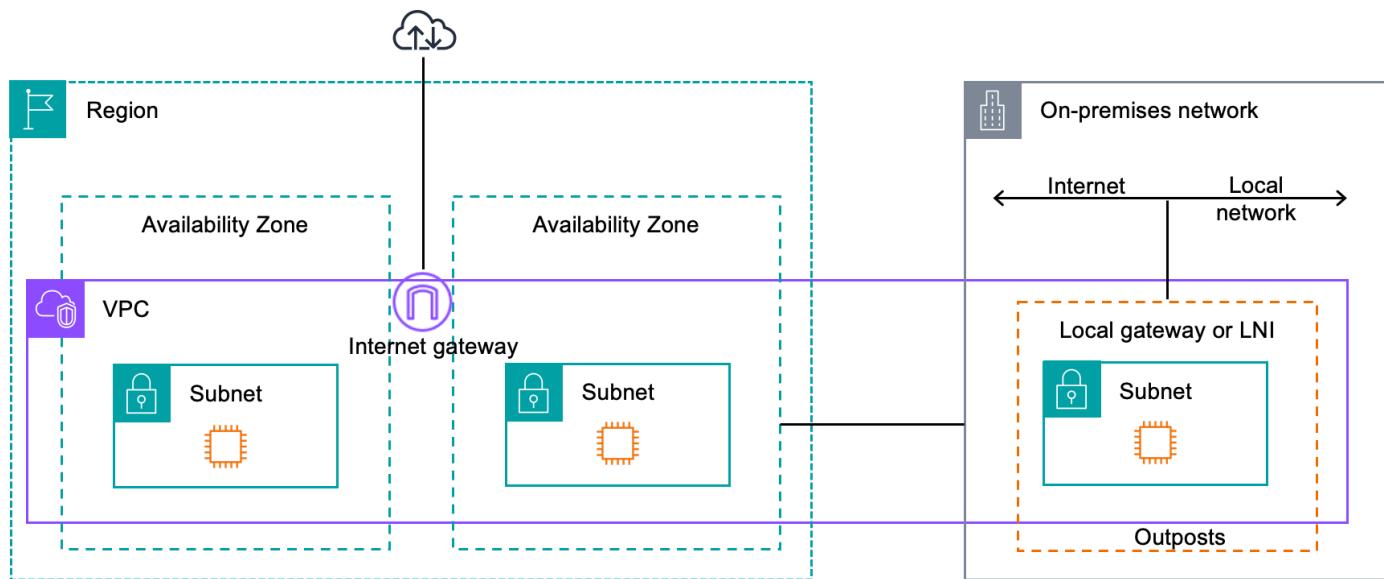
ネットワークコンポーネント

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

次の図は、Outpost のネットワークコンポーネントを示しています。

- AWS リージョン およびオンプレミスネットワーク
- リージョン内に複数のサブネットを持つ VPC
- オンプレミスネットワーク内の Outpost
- Outpost と提供されるローカルネットワーク間の接続 :

- Outposts ラックの場合: ローカルゲートウェイ
- Outposts サーバーの場合: ローカルネットワークインターフェイス (LNI)



VPC とサブネット

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

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

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

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

ルーティング

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

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

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

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

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

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 Outposts ラックのみのオプションです。DHCP オプションセットには VPC スコープがあるため、VPC の Outpost サブネットとアベイラビリティーゾーン サブネットのインスタンスはどちらも、指定された DNS サーバーを DNS 名ソリューションに使用しようとします。

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

サービスリンク

サービスリンクは、Outpost から選択した AWS リージョンまたは Outposts ホームリージョンへの接続です。サービスリンクは暗号化された VPN 接続セットで、Outpost が選択したホームリージョンと通信する際に必ず使用されます。仮想 LAN (VLAN) を使用してサービスリンク上のトラフィックをセグメント化します。サービスリンク VLAN により、Outpost と AWS リージョン間の通信が可能になり、Outpost と AWS リージョン間の VPC 内トラフィックの両方を管理できます。

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

- 「高可用性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/ワークフローのルーティング AWS Outposts AWS」](#)

ローカルネットワークインターフェイス

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

内容

- [施設](#)
- [ネットワーク](#)
- [電源](#)
- [注文の履行](#)

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 リソースの重み要件を確認するには、<https://console.aws.amazon.com/outposts/> の AWS Outposts コンソールでカタログを選択します。

- 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。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。AWS では、サーバーを取り付けるためのレールキットをご用意しています。
 - 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 サーバーを垂直にマウントすることはサポートされません。
 - Outposts 1U サーバーは Outposts 2U サーバーと同じ幅ですが、高さが半分で奥行きが小さいです。

サーバーをラックに設置しない場合でも、サイトの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、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。

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	DNS サーバー
UDP	443, 1024-65535	サービスリンク IP	443	Outposts サービスリンクのエンドポイント
TCP	1024-65535	サービスリンク IP	443	Outposts 登録エンドポイント

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 AWS リージョンのサービスリンクエンドポイントの間で 1500 バイトの MTU をサポートする必要があります。サービスリンクの詳細については、「サーバーの AWS Outposts ユーザーガイド」の「[AWS Outposts connectivity to AWS Regions](#)」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には、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 ミリ秒のラウンドトリップレイテンシーの冗長接続 AWS 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 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 AWS Outposts ユーザーガイド」の「[Service link traffic for servers](#)」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、ワークロードの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。

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、<https://console.aws.amazon.com/outposts/> の AWS Outposts コンソールでカタログを参照を選択します。

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

注文を満たすために、AWS は、レールマウントや必要な電源ケーブルやネットワークケーブルなどの Outposts サーバー機器を、指定した住所に配送します。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 AWS Outposts ユーザーガイド」の「[Service link traffic for servers](#)」を参照してください。

Outposts サーバーの Amazon EC2 キャパシティが AWS アカウントから利用可能であることを確認したら、設置は完了です。

Outposts サーバーの使用開始

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

タスク

- [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、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。
- Outposts サイトの作成、Outpost の作成、注文 AWS アカウントに使用するを決定します。このアカウントに関連付けられている E メールをモニタリングして、からの情報を確認します AWS。

タスク

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

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、はサイトに ID を 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. にサインインします AWS。
2. <https://console.aws.amazon.com/outposts/> で AWS Outposts コンソールを開きます。
3. 親を選択するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
4. ナビゲーションペインで、[サイト] を選択します。
5. [サイトの作成] を選択します。
6. [サポートされているハードウェアタイプ] で、[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 アベイラビリティゾーンを決定します。

Outpost を作成するには

1. ナビゲーションペインで、[Outpost] を選択してください。

2. [Outpost の作成] を選択します。
3. [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 サーバーの注文を確定してください。

Important

送信した後は注文を編集できなくなるため、送信する前にすべての詳細を注意深く確認してください。注文を変更する必要がある場合は、[AWS サポートセンター](#)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、期間中は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. [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. [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: インスタンスキャパシティを変更する

新規の各 Outpost 注文のキャパシティは、デフォルトのキャパシティ設定で設定されています。デフォルトの設定を変換して、ビジネスニーズに合わせたさまざまなインスタンスを作成できます。これを行うには、キャパシティタスクを作成し、インスタンスのサイズと数量を指定して、キャパシティタス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 レベルで定義します。
- インスタンスは、ベストプラクティスに基づいて自動的に配置されます。

インスタンスキャパシティを変更するには

1. [AWS Outposts コンソール](#)の 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を作成] を選択します。
3. [使用開始] ページで [注文] をクリックします。
4. キャパシティを変更するには、コンソールのステップを使用するか、JSON ファイルをアップロードします。

Console steps

1. [新しい Outpost のキャパシティ構成を変更] を選択します。
2. [次へ] を選択します。
3. [インスタンスキャパシティを設定] ページで、各インスタンスタイプには、事前に選択された最大数を含む 1 つのインスタンスサイズが表示されます。インスタンスサイズを追加するには、[インスタンスサイズを追加] を選択します。
4. インスタンスの数量を指定し、そのインスタンスサイズに表示されるキャパシティを書き留めます。
5. 各インスタンスタイプのセクションの最後に、キャパシティが超過しているか不足しているかを通知するメッセージが表示されます。インスタンスサイズまたは数量レベルで調整して、使用できる合計キャパシティを最適化します。
6. 特定のインスタンスサイズのインスタンス数を最適化 AWS Outposts するようにリクエストすることもできます。そのためには、次の操作を行います。
 - a. [インスタンスサイズ] を選択します。
 - b. 関連するインスタンスタイプのセクションの最後で、[オートバランス] を選択します。
7. インスタンスタイプごとに、少なくとも 1 つのインスタンスサイズに対してインスタンス数量が指定されていることを確認します。
8. [次へ] を選択します。
9. [確認して作成] ページで、リクエストする更新を確認します。
10. 「Create. AWS Outposts creates a capacity task」を選択します。
11. [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

 Note

AWS Outposts は、キャパシティタスクの実行を有効にするために、1 つ以上の実行中のインスタンスを停止するよう要求することがあります。これらのインスタンスを停止すると、AWS Outposts はタスクを実行します。

Upload JSON file

1. [キャパシティ構成をアップロード] を選択します。
2. [次へ] を選択します。

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

Example

JSON ファイルの例:

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

- [キャパシティ構成計画] セクションの JSON ファイルの内容を確認します。
- [次へ] を選択します。
- [確認して作成] ページで、リクエストする更新を確認します。
- 「Create. AWS Outposts creates a capacity task」を選択します。
- [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

Note

AWS Outposts は、キャパシティタスクの実行を有効にするために、1つ以上の実行中のインスタンスを停止するよう要求することがあります。これらのインスタンスを停止すると、AWS Outposts はタスクを実行します。

次のステップ

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

注文を満たすために、AWS は配信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、「[Server installation guide](#)」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。キャパシティ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。

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 の AWS リージョン内の任意の VPC に Outpost サブネットを追加できます。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で有効にする必要があります。AWS CLIから [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ています。

```
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要件を満たすのに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てください。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。

- 単一の EBS スナップショットのみを持つ Amazon EBS-backed AMI を使用する必要があります。複数の EBS 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。
- 互換性のあるサードパーティーストレージにバックアップされたブロックデータまたはブートボリュームを使用するには、Outposts の EC2 インスタンスで使用するようにこれらのボリュームをプロビジョニングして設定する必要があります。詳細については、「[サードパーティのブロックストレージ](#)」を参照してください。
- 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 サブネットをお客様のために選択し、Outposts のラックでサポートされているインスタンスタイプのみを表示します。
5. Outposts ラックでサポートされているインスタンスタイプを選択してください。グレーアウトされたインスタンスは使用できないことに注意してください。
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になります。または、後で追加するには、「[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。
7. (オプション) [サードパーティのデータボリューム](#)を追加できます。
 - a. ストレージの設定を展開します。外部ストレージボリュームの横にある編集を選択します。

- b. Storage Network Protocol で、iSCSI を選択します。
 - c. イニシエーター IQN を入力し、外部ストレージ配列のターゲット IP アドレス、ポート、IQN を追加します。
8. ウィザードを完了して、Outpost サブネット内でインスタンスを起動してください。詳細については、「Amazon EC2 ユーザーガイド」の「[EC2 インスタンスの起動](#)」を参照してください。

ステップ 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。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内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 アドレスに対して ping コマンドを実行します。

```
ping 10.0.3.128
```

以下は出力の例です。

```
Pinging 10.0.3.128

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

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

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

Outpost インスタンスからローカル ネットワークへの接続をテストする

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

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

```
ping 172.16.0.130
```

以下は出力の例です。

```
Pinging 172.16.0.130
```

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

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

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

AWS リージョンと Outpost 間の接続をテストする

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

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

インスタンスの実行後、次の操作を実行します。

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

```
ping 10.0.1.5
```

以下は出力の例です。

```
Pinging 10.0.1.5
```

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

```
Ping statistics for 10.0.1.5
```

```
Packets: Sent = 3, Received = 3, Lost = 0 (0% lost)
```

```
Approximate round trip time in milliseconds
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

AWS Outposts AWS リージョンへの接続

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

Note

Outposts サーバーを AWS リージョンまたは AWS Outposts ホーム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](#)
- [更新とサービスリンク](#)
- [ファイアウォールとサービスリンク](#)
- [Outposts サーバーネットワークのトラブルシューティング](#)

サービスリンク経由の接続

AWS Outposts プロビジョニング中、または Outposts サーバーを選択した AWS リージョンまたはホームリージョンに接続するサービスリンク接続 AWS を作成します。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 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。

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。のパブリック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」](#)を参照してください。

サービスリンクが確立されると、Outpost は稼働中であり、によって管理されます 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。

次の点に注意してください。

- ネットワークは、Outpost と親 AWS リージョンのサービスリンクエンドポイントの間で 1500 バイトの MTU をサポートする必要があります。
- Outposts のインスタンスからリージョンのインスタンスに移動するトラフィックの MTU は 1300 バイトで、パケットオーバーヘッドのために必要な MTU である 1500 バイトよりも低くなります。

サービスリンクの推奨帯域幅

最適なエクスペリエンスと回復性を実現するには、AWS リージョンへのサービスリンク接続に 500 Mbps 以上、最大 175 ミリ秒のラウンドトリップレイテンシーの冗長接続 AWS 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 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、「[Service link traffic for servers](#)」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、ワークロードの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。

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

冗長インターネット接続

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

パブリックインターネットへの接続が必要な場合は、既存のオンプレミスワーカードと同様に、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。

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 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、異なるアベイラビリティーボーンに属する 2 つの Outposts にアクティブ/アクティブ設計でアプリケーションをデプロイすることを推奨しています。詳細については、「[AWS Outposts の高可用性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やパケット損失が発生すると、リージョン内でホストされるリソースへの VPC 接続に依存するワーカ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作業に対してアプリケーションが[耐障害性](#)を持つようにすることにより、アプリケーションへの影響を回避できます。

ファイアウォールとサービスリンク

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

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

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

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

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

プロトコル	ソースポート	送信元アドレス	発信先ポート	送信先アドレス
UDP	1024-65535	サービスリンク IP	53	DNS サーバー
UDP	443, 1024-65535	サービスリンク IP	443	AWS Outposts Service Link 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

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

プロトコル	ソースポート	送信元アドレス	発信先ポート	送信先アドレス
UDP	1024-65535	サービスリンク IP	53	DNS サーバー

プロトコル	ソースポート	送信元アドレス	発信先ポート	送信先アドレス
UDP	443, 1024-65535	サービスリンク IP	443	AWS Outposts Service Link エンドポイント
TCP	1025-65535	サービスリンク IP	443	AWS Outposts Service Link エンドポイント
UDP	53	DNS サーバー	1025-65535	サービスリンク IP
UDP	443	AWS Outposts Service Link エンドポート	443, 1024-65535	サービスリンク IP
TCP	443	AWS Outposts Service Link エンドポート	1025-65535	サービスリンク IP

 Note

Outposts 内のインスタンスは、サービスリンクを使用して別の Outpost 内のインスタンスと通信することはできません。ローカルゲートウェイまたはローカルネットワークインターフェイスを介したルーティングを活用して Outposts 間の通信を行います。

Outposts サーバーネットワークのトラブルシューティング

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

初期評価

Amazon CloudWatch メトリクスを使用してサービスリンクのステータスを確認します。

1. 名前空間で ConnectedStatus メトリクスを AWS Outposts モニタリングします。
2. 平均値が 1 未満の場合、サービスリンクに障害があることを確認します。
3. サービスリンクに障害が発生した場合は、以下のセクションのステップを実行して接続を解決し、再確立します。

ステップ 1. 物理接続を確認する

1. 提供された QSFP ブレークアウトケーブルを使用していることを確認します。問題が解決しない場合は、可能であれば別の QSFP ブレークアウトケーブルでテストします。
2. Outposts サーバーの QSFP ブレークアウトケーブルがしっかりと固定されていることを確認します。
3. ケーブル 1 (LNI) がスイッチにしっかりと固定されていることを確認します。
4. ケーブル 2 (サービスリンク) がスイッチにしっかりと固定されていることを確認します。
5. リンクライトのチェックなど、一般的なスイッチの正常性チェックを完了します。

ステップ 2. への Outposts サーバー接続をテストする AWS

Outposts サーバーへのシリアル接続を作成し、次のテストを実行します。

1. リンクをテストします。
 - a. 成功したら、次のテストに進みます。
 - b. 失敗した場合、ネットワーク設定の確認。
2. DNS 解決をテストします。
 - a. 成功したら、次のテストに進みます。
 - b. 失敗した場合、ファイアウォールルールを確認する。
3. AWS リージョンへのアクセスをテストします。
 - a. 成功したら、接続の再確立に進みます。
 - b. 失敗した場合、MTU の検証。

ネットワーク設定の確認

スイッチが次の仕様を満たしていることを確認します。

- 基本設定 — サービスリンクポートは、ゲートウェイと AWS エンドポイントへのルートを持つ VLAN へのタグなしアクセスポートである必要があります。
- リンク速度 — スイッチポートのリンク速度を 10 Gb に設定し、自動ネゴシエーションをオフにする必要があります。

MTU の検証

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

ファイアウォールルールを確認する

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	DNS サーバー
UDP	443, 1024-65535	サービスリンク IP	443	AWS Outposts Service Link 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

ステップ 3. 接続を再確立する

前のチェックに合格してもサービスリンクが残っている場合 DOWN (CloudWatch でConnectedStatus が 1 未満) 、「[Outpost 設定ツールを使用して Outposts サーバーを承認する](#)」の手順に従って接続を再確立します。

Note

サービスリンクがダウンしたままの場合は、[AWS サポートセンター](#)でケースを作成します。

Outposts サーバーの返却

Note

配送中に破損したサーバーを受け取った場合は、サーバー AWS Outposts インストールガイドの [「ステップ 2: Outposts サーバー機器の検査」](#) を参照してください。

使用中で置き換えるサーバー、またはサブスクリプションが終了したサーバーを返すには、このセクションを確認してください。

がサーバーに不具合 AWS Outposts を検出した場合、から通知され、新しいサーバーを送信する代替プロセスが開始され、コンソールから AWS Outposts 戻りラベルが提供されます。Outposts サーバーを返送しても、配送料金は発生しません。ただし、破損したサーバーを返却すると、コストが発生する可能性があります。

返却を開始するには、以下のステップを完了します。

タスク

- [ステップ 1: サーバーを返却する準備をする](#)
- [ステップ 2: 戻りラベルを印刷する](#)
- [ステップ 3: サーバーを梱包する](#)
- [ステップ 4: 宅配業者を通じてサーバーを返却する](#)

ステップ 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 [disassociate-resource-share](#) コマンド AWS CLI を実行します。

共有可能な Outpost リソースの一覧については、「[共有可能な Outpost リソース](#)」を参照してください。

2. 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 のサブネットに関するアクティブなインスタンスを終了してください。インスタンスを終了するには、「Amazon EC2 ユーザーガイド」の「[インスタンスの終了](#)」のステップに従ってください。
5. Nitro セキュリティキー (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します。NSK を破棄するには、[Cryptographically shred server data](#) の手順に従います。

ステップ 2: 戻りラベルを印刷する

⚠ Important

AWS が提供する戻りラベルのみを使用する必要があります。これは、返すサーバーに関するアセット ID などの特定の情報が含まれているためです。独自のリターンラベルを作成しないでください。

リターンラベルを取得するには：

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 [注文] を選択します。
3. 返すサーバーの順序を選択します。
4. 注文の詳細ページの注文ステータスセクションで、返品ラベルの印刷を選択します。

ⓘ Note

現在のサブスクリプションが終了する前に Outposts サーバーを返却しても、この Outpost に関する未払いの料金は終了しません。

ステップ 3: サーバーを梱包する

サーバーをパックするには、が提供するボックスとパッケージマテリアルを使用します AWS。

1. サーバーを次のいずれかの箱に梱包します。

- サーバーが元々入っていた箱と梱包材。
- 交換用サーバーが入っていた箱と梱包材。

または、[AWS サポートセンター](#) に連絡して箱をリクエストしてください。

2. AWS 提供された戻りラベルをボックスの外側に貼り付けます。

 Important

リターンラベルのアセット ID が、返すサーバーのアセット ID と一致することを確認します。

アセット ID は、サーバー前面の引き出しタブにあります。例: 1203779889 または 9305589922

3. 箱を確実に密封します。

ステップ 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 が提供する戻りラベルには、サーバーを返す正しいアドレスが含まれています。

次の表は発送元の国での連絡先を示しています。

国	連絡先
アルゼンチン	AWS サポートセンター 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。
バーレーン	
ブラジル	<ul style="list-style-type: none">• AWS 提供された返送ラベルに記載されている追跡番号
ブルネイ	

国	連絡先
カナダ	<ul style="list-style-type: none">・ 宅配業者にサーバーを集荷してもらいたい日時
チリ	<ul style="list-style-type: none">・ 問い合わせ名
コロンビア	<ul style="list-style-type: none">・ 電話番号
香港	<ul style="list-style-type: none">・ E メールアドレス
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	
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	

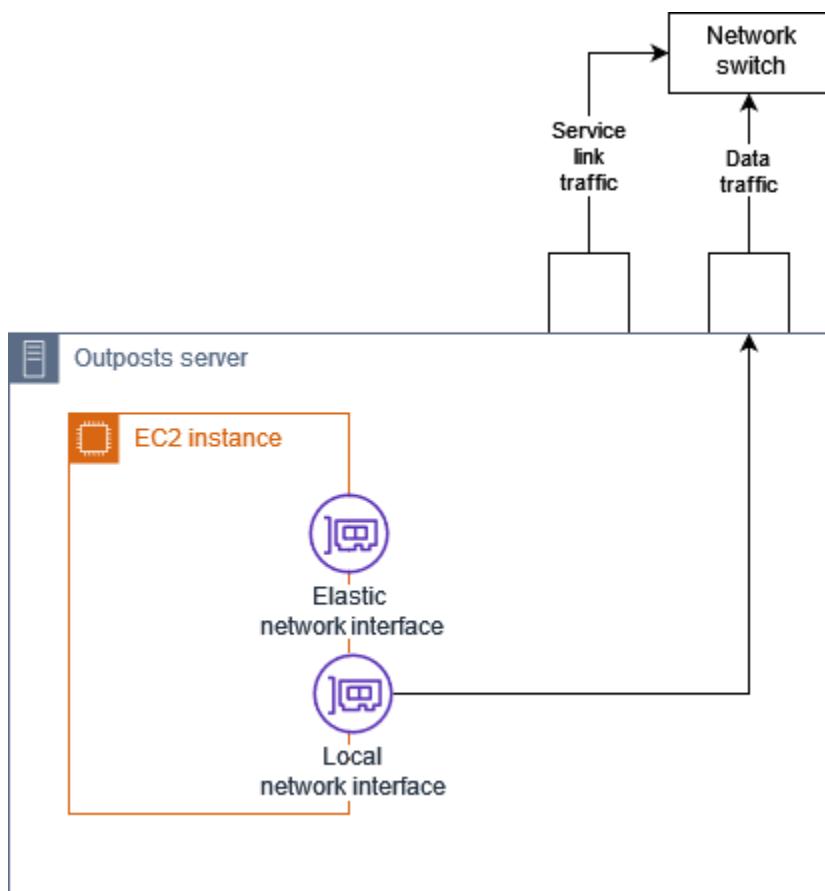
国	連絡先
ベトナム	
メキシコ	AWS は DB Schenker に連絡し、お客様の口頭からの集荷をリクエストします。DB Schenker は、集荷日時をスケジュールするためにお客様に連絡します。
アメリカ合衆国	<p>UPS に問い合わせてください。</p> <p>サーバーは以下の方法で返却できます。</p> <ul style="list-style-type: none">お客様のサイトでの UPS の定期集荷でサーバーを返却する。UPS の営業所にサーバーを持ち込む。希望の日時で集荷をスケジュールする。送料無料の AWS が提供する返送ラベルから追跡番号を入力します。
他のすべての国	<p>DHL に問い合わせてください。</p> <p>サーバーは以下の方法で返却できます。</p> <ul style="list-style-type: none">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。送料無料の AWS 返送ラベルから DHL Waybill 番号を入力します。 <p>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。</p>

Outposts サーバー用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、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。たとえば、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では、Outposts 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のクォータ](#)」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、Outposts 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ローカルネットワークインターフェイスは、使用可能な 10 GbE の物理的帯域幅の一部を提供します。以下の表は、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ています。

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 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、エラスティックネットワークインターフェイスの場合と同様に、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 EC2 ユーザーガイド」の「[EC2 インスタンスでの ENA 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。

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 サブネットの 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。た

とえば、create AWS CLI[create-network-interface](#) と [attach-network-interface](#) のコマンドを使用します。

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、「[Launch an instance on the Outpost](#)」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. Amazon EC2 コンソールの <https://console.aws.amazon.com/ec2/> を開いてください。
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] をクリックしてください。
 - 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] をクリックしてください。
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] の順にクリックしてください。
 - c. インスタンスを選択します。
 - d. [アタッチ] を選択してください。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。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。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、ゲストオペレーティングシステム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。

Outposts 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、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の要件を理解してください。詳細については、「[Outposts サーバー用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](#)
- [サーバーの物理的な接続](#)
- [サーバーのサービスリンクトラフィック](#)
- [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](#)
- [サーバー IP アドレスの割り当て](#)
- [サーバーの登録](#)

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。

次の表では、Outposts 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 Outposts 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 Outposts 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。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インターフェイス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

Outpost が AWS リージョン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 が使用可能である必要があります。この接続では、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

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付けしません。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 `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 Linux 2 [ユーザーガイド](#)」の「[ec2-net-utils for AL2 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

インスタンス上の AWS Outposts サーバーのサービスリンクとローカルネットワークインターフェイスにパブリック IP アドレスを割り当てる必要はありません。サービスリンクでは、IP アドレスを手動で割り当てるか、動的ホスト制御プロトコル (DHCP) を使用できます。サービスリンク接続を設定するには、AWS Outposts サーバーインストールガイドの「[接続の設定とテスト](#)」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を設定するには、「」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

Outposts 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、サーバー自身を登録します。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。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 VPC 経由のプライベート接続をサポートしていません。

のキャパシティ管理 AWS Outposts

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

トピック

- [AWS Outposts 容量の表示](#)
- [AWS Outposts インスタンス容量の変更](#)
- [キャパシティタスクの問題のトラブルシューティング](#)

AWS Outposts 容量の表示

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

コンソールを使用して Outpost の容量設定を表示するには

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

AWS Outposts インスタンス容量の変更

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

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

考慮事項

インスタンス容量を変更する前に、次の点を考慮してください。

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

- インスタンスファミリー内で複数のインスタンスサイズを持つアセットを設定するときは、自動分散を使用して、ドロップレットを過剰または過小プロビジョニングしようとしていることを確認します。オーバープロビジョニングはサポートされていないため、キャパシティタスクが失敗します。
- 相互に排他的な AssetIDs のセットに適用される限り、複数のキャパシティタスクを並行して実行できます。たとえば、異なる AssetIDs に対して複数のアセットレベルのキャパシティタスクを同時に作成できます。ただし、実行中の Outpost レベルのタスクがある場合、別の Outpost またはアセットレベルのタスクを同時に作成することはできません。同様に、実行中のアセットレベルのタスクがある場合、同じAssetID に Outpost レベルのタスクまたはアセットレベルのタスクを同時に作成することはできません。

コンソールを使用して Outpost の容量設定を変更するには

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

 Note

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

Console steps

- インスタンスピューまたはラックビューを選択します。
- 1つのアセットで Outpost 容量設定の変更または変更を選択します。
- 現在の選択と異なる場合は、Outpost またはアセットを選択します。

4. このキャパシティタスクをすぐに実行するか、48 時間以上定期的に実行するかを選択します。
5. [次へ] を選択します。
6. [インスタンスキャパシティを設定] ページで、各インスタンスタイプには、事前に選択された最大数を含む 1 つのインスタンスサイズが表示されます。インスタンスサイズを追加するには、[インスタンスサイズを追加] を選択します。
7. インスタンスの数量を指定し、そのインスタンスサイズに表示されるキャパシティを書き留めます。
8. 各インスタンスタイプのセクションの最後に、キャパシティが超過しているか不足しているかを通知するメッセージが表示されます。インスタンスサイズまたは数量レベルで調整して、使用できる合計キャパシティを最適化します。
9. 特定のインスタンスサイズのインスタンス数を最適化 AWS Outposts するようにリクエストすることもできます。そのためには、次の操作を行います。
 - a. [インスタンスサイズ] を選択します。
 - b. 関連するインスタンスタイプのセクションの最後で、[オートバランス] を選択します。
10. インスタンスタイプごとに、少なくとも 1 つのインスタンスサイズに対してインスタンス数量が指定されていることを確認します。
11. 必要に応じて、インスタンスを選択してそのままにします。
12. [次へ] を選択します。
13. [確認して作成] ページで、リクエストする更新を確認します。
14. Create AWS Outposts creates キャパシティタスクを選択します。
15. [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

Upload a JSON file

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

Example

JSON ファイルの例:

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

4. [キャパシティ構成計画] セクションの JSON ファイルの内容を確認します。
5. [次へ] を選択します。
6. [確認して作成] ページで、リクエストする更新を確認します。
7. Create AWS Outposts creates キャパシティタスクを選択します。
8. [キャパシティタスク] ページで、タスクのステータスをモニタリングします。

キャパシティタスクの問題のトラブルシューティング

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

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

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

この問題を解決するには。

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

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

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

この問題を解決するには、コンソールまたは CLI を使用します。

コンソールを使用する

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

CLI を使用する

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

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

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

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

この問題を解決するには。

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

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

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

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

コンソールを使用する

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

CLI を使用する

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

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

この問題は、AWS Outposts コンソールまたは API を使用してアセットで [StartCapacityTask](#) を実行し、アセットに対して既に実行中のキャパシティタスクがある場合に発生します。キャパシティタスクのステータスが REQUESTED、、、または のいずれかである場合 IN_PROGRESS_WAITING_FOR_EVACUATION、キャパシティタスクは実行中と見なされます CANCELLATION_IN_PROGRESS。

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

コンソールを使用する

1. にサインインします AWS。
2. <https://console.aws.amazon.com/outposts/> で AWS Outposts コンソールを開きます。
3. ナビゲーションペインから、キャパシティタスクを選択します。

4. OutpostId に対して実行中のキャパシティタスクがなく、AssetId に対して実行中のアセットレベルのキャパシティタスクがないことを確認します。
5. 実行中のキャパシティタスクがある場合は、タスクが終了するのを待つか、必要に応じてキャンセルします。
6. 実行中のキャパシティタスクがない場合は、リクエストを再試行してキャパシティタスクを作成します。

CLI を使用する

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

AssetId=XXXX は Outpost=op-XXXX には無効です

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

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

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

コンソールを使用する

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

- a. アセットが分離されている場合、キャパシティタスクが実行されていることが原因である可能性があります。キャパシティタスクパネルに移動し、OutpostId と AssetId に対して実行中の Outpost タスクまたはAssetIdレベルのタスクがあるかどうかを確認できます。存在する場合は、タスクが終了し、アセットが再び利用可能になるまで待ちます。
 - b. 分離されたアセットに対して実行中のキャパシティタスクがない場合、アセットが劣化する可能性があります。
5. アセットが存在し、有効な状態であることを確認したら、リクエストを再試行してキャパシティタスクを作成します。

CLI を使用する

1. [ListAssets](#) コマンドを使用して、OutpostId に関連付けられたアセットを検索します。
2. リクエストされた AssetId が Outpost に関連付けられており、その状態が であることを確認しますACTIVE。
 - a. アセットの状態が ACTIVE でない場合、キャパシティタスクが実行されていることが原因である可能性があります。 [ListCapacityTasks](#) コマンドを使用して、OutpostId と AssetId に対して Outpost またはアセットレベルのタスクが実行されているかどうかを確認します。 AssetId 存在する場合は、タスクが終了し、アセットが再び ACTIVE になるまで待ちます。
 - b. 分離されたアセットに対して実行中のキャパシティタスクがない場合、アセットが劣化する可能性があります。
3. アセットが存在し、有効な状態であることを確認したら、リクエストを再試行してキャパシティタスクを作成します。

AWS Outposts リソースを共有する

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

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

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

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

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

内容

- ・ [共有可能な Outpost リソース](#)
- ・ [Outposts リソースを共有するための前提条件](#)
- ・ [関連サービス](#)
- ・ [アベイラビリティーゾーン間での共有](#)
- ・ [Outpost リソースの共有](#)
- ・ [共有 Outpost リソースの共有解除](#)

- ・ [共有 Outpost リソースの特定](#)
- ・ [共有 Outpost リソースの権限](#)
- ・ [請求と使用量測定](#)
- ・ [制限](#)

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。

Outposts サーバーリソースについては、[「共有 AWS Outposts リソースの使用」](#) を参照してください。

これらは Outposts サーバーで利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。
 - ・ 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している必要があります。自身が共有を受けている Outpost リソースを共有することはできません。
- Outpost リソースを共有するには、組織内のアカウントと共有する必要があります。

関連サービス

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

詳細については AWS RAM、 [AWS RAM ユーザーガイド](#)を参照してください。

アベイラビリティーゾーン間での共有

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

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

アカウントのアベイラビリティーゾーンの IDs を表示するには

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

Note

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

Outpost リソースの共有

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

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

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

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

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

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

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

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

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

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

[create-resource-share](#) コマンドを使用します。

共有 Outpost リソースの共有解除

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

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

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

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

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

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

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

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

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

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

[disassociate-resource-share](#) コマンドを使用します。

共有 Outpost リソースの特定

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

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

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

を使用して共有 Outpost リソースを識別するには AWS CLI

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

共有 Outpost リソースの権限

所有者のアクセス許可

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

コンシューマーのアクセス許可

コンシューマーは、各自のアカウントで作成した Outposts にリソースを作成する場合と同じように、共有された Outposts にリソースを作成できます。コンシューマーは、Outposts 上に作成された

自身が共有しているリソースの管理に責任を負います。コンシューマーは、他のコンシューマーまたは Outpost 所有者が所有するリソースを表示または変更することはできません。また、自己が共有している Outpost を変更することはできません。

請求と使用量測定

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

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

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

制限

AWS Outposts 共有の使用には、次の制限が適用されます。

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

サーバー上のサードパーティーブロックストレージ

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

考慮事項

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

Note

外部ストレージ配列に保存されているブロックボリュームには、Outposts の EC2 インスタンスに起動されるオペレーティングシステムが含まれています。外部ストレージ配列にバックアップされた AMI の起動はサポートされていません。AMI を起動するには、Outposts サーバーのインスタンストレージが使用されます。

外部ブロックデータボリューム

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

主要なステップ

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

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

外部ロックブートボリューム

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

iSCSI SAN ブート

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

iSCSI または NVMe-over-TCP LocalBoot

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

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

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

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

のセキュリティ AWS Outposts

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

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

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

のセキュリティとコンプライアンスの詳細については AWS Outposts、[AWS Outposts サーバーに関するよくある質問](#)」を参照してください。

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

内容

- ・ [でのデータ保護 AWS Outposts](#)
- ・ [AWS Outposts の Identity and Access Management \(IAM\)](#)
- ・ [のインフラストラクチャセキュリティ AWS Outposts](#)
- ・ [の耐障害性 AWS Outposts](#)
- ・ [のコンプライアンス検証 AWS Outposts](#)

でのデータ保護 AWS Outposts

責任 AWS [共有モデル](#)、でのデータ保護に適用されます AWS Outposts。このモデルで説明されているように、 AWS はすべてのを実行するグローバルインフラストラクチャを保護する責任がありま

す AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。このコンテンツには、AWS のサービス 使用する のセキュリティ設定および管理タスクが含まれます。

データ保護の目的で、AWS アカウント 認証情報を保護し、AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。

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

保管中の暗号化

では AWS Outposts、すべてのデータは保管時に暗号化されます。キーマテリアルは、リムーバブル デバイスである Nitro Security Key (NSK) に保存される外部キーにラップされます。NSK は Outposts 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ップ (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。

AWS Outposts の Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御するのに役立つ AWS サービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Outposts リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAMは追加料金なしでご利用いただけます。

内容

- [AWS Outposts と IAM の連携方法](#)
- [AWS Outposts ポリシーの例](#)
- [のサービスにリンクされたロール AWS Outposts](#)
- [AWS Outposts の マネージドポリシー](#)

AWS Outposts と IAM の連携方法

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

IAM の特徴量	AWS Outposts のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
プリンシパルアクセス権限	あり
サービスロール	いいえ
サービスリンクロール	あり

AWS Outposts のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

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

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

AWS Outposts のアイデンティティベースのポリシーの例

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

AWS Outposts のポリシーアクション

ポリシーアクションのサポート: あり

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

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

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

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

outposts

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

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

```
"outposts:action2"
```

```
]
```

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

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

AWS Outposts のポリシーリソース

ポリシーリソースのサポート: あり

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

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

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

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

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

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

AWS Outposts のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

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

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

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

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

AWS Outposts での ABAC

ABAC (ポリシー内のタグ) のサポート: あり

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

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

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

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

AWS Outposts での一時的な認証情報の使用

一時的な認証情報のサポート: あり

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

AWS Outposts のクロスサービスプリンシパルアクセス許可

転送アクセスセッション (FAS) のサポート: あり

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

AWS Outposts のサービスにリンクされたロール

サービスリンクロールのサポート: あり

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

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

AWS Outposts ポリシーの例

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

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

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

内容

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

ポリシーに関するベストプラクティス

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

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行 – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらはで使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の [AWS マネージドポリシー](#) または [ジョブ機能のAWS マネージドポリシー](#) を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の [IAM でのポリシーとアクセス許可](#) を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションがなどの特定のを通じて使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の [IAM JSON ポリシー要素:条件](#) を参照してください。
- IAM アクセスアナライザーを使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザーは、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の [IAM Access Analyzer でポリシーを検証する](#) を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーション

が呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドの [MFA を使用した安全な API アクセス](#) を参照してください。

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

例: リソースレベルのアクセス許可の使用

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

JSON

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

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

JSON

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

```



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 を定義します。特に定義されている場合を除き、のみがそのロールを引き受け AWS Outposts ることができます。定義された許可には信頼ポリシーと許可ポリシーが含まれ、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

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

のサービスにリンクされたロールのアクセス許可 AWS Outposts

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

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

- outposts.amazonaws.com

サービスにリンクされたロールポリシー

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

- [AWSOutpostsServiceRolePolicy](#)
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

AWSOutpostsServiceRolePolicy

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

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

- アクション: すべての AWS リソースec2:DescribeNetworkInterfacesで
- アクション: すべての AWS リソースec2:DescribeSecurityGroupsで
- アクション: すべての AWS リソースec2>CreateSecurityGroupで
- アクション: すべての AWS リソースec2>CreateNetworkInterfaceで

AWSOutpostsPrivateConnectivityPolicy_OutpostID

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

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

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

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

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

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

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

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

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

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

のサービスにリンクされたロールを作成する AWS Outposts

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

のサービスにリンクされたロールを編集する AWS Outposts

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

のサービスにリンクされたロールを削除する AWS Outposts

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

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

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

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

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

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

サービスリンクロールを IAM で手動削除するには

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

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

AWS Outposts は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートしています。 詳細については、[Outposts FAQs](#)を参照してください。

AWS Outposts の マネージドポリシー

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

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

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

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

AWS マネージドポリシー: AWSOutpostsServiceRolePolicy

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

AWS 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 Outposts 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。

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。

JSON

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

AWS AWS 管理ポリシーに対する Outposts の更新

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

変更	説明	日付
AWSOutpostsAuthorizeServerPolicy — 新しいポリシー	AWS Outposts は、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 、管理ポリシーの変更の追跡を開始しました。	2019 年 12 月 3 日

のインフラストラクチャセキュリティ AWS Outposts

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

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

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

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

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

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マトリクスに対して N+1 のインスタンスをサポートします。推奨されるのは、AWS 基盤となるホストに問題が発生した場合にリカバリーとフェイルオーバーを可能にするため、ミッションクリティカルなアプリケーションに十分な追加容量を割り当てることです。Amazon CloudWatch の容量可用性メトリクスを使用して、アプリケーションの健康状態を監視し、アラームを設定できます。CloudWatch アクションを作成して自動リカバリオプションを構成し、Outposts の容量利用状況を時間とともにモニターすることができます。

Outpost を作成するときは、AWS リージョンからアベイラビリティゾーンを選択します。このアベイラビリティゾーンは、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であるかどうかを確認するには、「コンプライアンス[AWS のサービス プログラムによる対象範囲内のコンプライアンス](#)」を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS 「コンプライアンスプログラム」](#)を参照してください。

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

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

Outposts サーバーをモニタリングする

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

CloudWatch メトリクス

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

CloudTrail ログ

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

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

VPC フローログ

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

トラフィックのミラーリング

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

AWS Health Dashboard

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

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

Outposts サーバーの CloudWatch メトリクス

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

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

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

内容

- [メトリクス](#)
- [メトリクスのディメンション](#)
- [Outposts サーバーの CloudWatch メトリクスを表示する](#)

メトリクス

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

内容

- [インスタンスマトリクス](#)
- [Outposts メトリクス](#)

インスタンスマトリクス

Amazon EC2 インスタンスでは、次のメトリクスを使用できます。

メトリクス	ディメンション	説明
InstanceFamilyCapacityAvailability	InstanceFamily および OutpostId	<p>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。</p> <p>単位: パーセント</p> <p>最大解像度:5 分</p> <p>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。</p>
InstanceFamilyCapacityUtilization	Account、InstanceFamily および OutpostId	<p>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。</p> <p>単位: パーセント</p> <p>最大解像度:5 分</p> <p>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。</p>
InstanceTypeCapacityAvailability	InstanceType および OutpostId	利用可能なインスタンス容量の割合。このメトリクスに

メトリクス	ディメンション	説明
		<p>は、Outpost 上で構成された専有ホストの容量は含まれません。</p> <p>単位: パーセント</p> <p>最大解像度:5 分</p> <p>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。</p>
InstanceTypeCapacityUtilization	Account、InstanceType 、および OutpostId	<p>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。</p> <p>単位: パーセント</p> <p>最大解像度:5 分</p> <p>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。</p>

メトリクス	ディメンション	説明
UsedInstanceType_Count	Account、InstanceType、およびOutpostId	<p>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。</p> <p>単位: 個</p> <p>最大解像度:5 分</p>

メトリクス	ディメンション	説明
AvailableInstanceType_Count	InstanceType および OutpostId	<p>使用可能なインスタンスタイプ。このメトリクスには AvailableReservedInstances の数が含まれます。</p> <p>予約可能なインスタンスの数を確認するには、AvailableReservedInstances の数から AvailableInstanceType_Count の数を引きます。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Number of instances that you can reserve $= \text{AvailableInstanceType_Count} - \text{AvailableReservedInstances}$ </div> <p>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。</p> <p>単位: 個</p> <p>最大解像度:5 分</p>

メトリクス	ディメンション	説明
AvailableReservedInstances	InstanceType および OutpostId	<p><u>キャパシティ予約</u>を使用して予約したコンピューティングキャパシティで起動できるインスタンスの数。</p> <p>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。</p> <p>このメトリクスには、予約可能なインスタンスの数は含まれません。予約可能なインスタンスを確認するには、Available ReservedInstances の数から AvailableInstanceType_Count の数を引きます。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Number of instances that you can reserve $= \text{AvailableInstanceType_Count} - \text{AvailableReservedInstances}$ </div> <p>単位: 個</p> <p>最大解像度:5 分</p>

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

Outposts メトリクス

Outposts では、次のメトリクスを使用できます。

メトリクス	ディメンション	説明
ConnectedStatus	OutpostId	<p>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。</p> <p>単位: 個</p>

メトリクス	ディメンション	説明
		最大解像度:1 分 統計: 最も有用な統計は Average です。
CapacityExceptions	InstanceType および OutpostId	起動などの容量不足エラーの数。 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。

メトリクスのディメンション

Outpost のメトリクスをフィルタするには、次のディメンションを使用できます。

ディメンション	説明
Account	容量を使用しているアカウントまたはサービス。
InstanceFamily	インスタンスファミリー。
InstanceType	インスタンスタイプ。
OutpostId	Outpost の ID。

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. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。

2. ナビゲーションペインで [Metrics (メトリクス)] を選択してください。
3. [Outposts] 名前空間を選択します。
4. (オプション) すべてのディメンションでメトリクスを表示するには、検索フィールドに名称を入力します。

を使用してメトリクスを表示するには AWS CLI

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

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

を使用してメトリクスの統計を取得するには AWS CLI

次の [get-metric-statistics](#) コマンドを使用して、指定されたメトリクスとディメンションの統計情報を取得します。CloudWatch は、ディメンションの一意の組み合わせをそれぞれ別のメトリクスとして扱います。特に発行されていないディメンションの組み合わせを使用した統計を取得することはできません。メトリクス作成時に使用した同じディメンションを指定する必要があります。

```
aws cloudwatch get-metric-statistics \  
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \  
--statistics Average --period 3600 \  
--dimensions Name=OutpostId,Value=op-01234567890abcdef \  
Name=InstanceType,Value=c5.xlarge \  
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

を使用した AWS Outposts API コールのログ記録 AWS CloudTrail

AWS Outposts は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスであると統合されています。CloudTrail は、 の API コールをイベント AWS Outposts としてキャプチャします。キャプチャされた呼び出しには、 AWS Outposts コンソールからの呼び出しと AWS Outposts API オペレーションへのコード呼び出しが含まれます。CloudTrail によって収集された情報を使用して、リクエストの実行元の IP アドレス AWS Outposts、リクエストの実行日時などの詳細を確認できます。

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

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。

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

CloudTrail は AWS、アカウントの作成時にアカウントでアクティブになり、CloudTrail イベント履歴に自動的にアクセスできます。CloudTrail の [イベント履歴] では、AWS リージョンで過去 90 日間に記録された管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「[CloudTrail イベント履歴の使用](#)」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

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

CloudTrail 証跡

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

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「[AWS CloudTrail の料金](#)」を参照してください。Amazon S3 の料金に関する詳細については、「[Amazon S3 の料金](#)」を参照してください。

CloudTrail Lake イベントデータストア

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

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

AWS Outposts CloudTrail の管理イベント

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

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

AWS Outposts イベントの例

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

```
{  
    "eventVersion": "1.05",  
    "userIdentity": {  
        "type": "AssumedRole",  
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",  
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",  
        "accountId": "111122223333",  
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",  
        "sessionContext": {  
            "sessionIssuer": {  
                "type": "Role",  
                "principalId": "AKIAIOSFODNN7EXAMPLE",  
                "arn": "arn:aws:iam::111122223333:role/example",  
                "accountId": "111122223333",  
                "userName": "example"  
            },  
            "webIdFederationData": {},  
            "attributes": {  
                "mfaAuthenticated": "false",  
                "creationDate": "2020-08-14T16:28:16Z"  
            }  
        }  
    }  
}
```

```
        }
    },
},
"eventTime": "2020-08-14T16:32:23Z",
"eventSource": "outposts.amazonaws.com",
"eventName": "SetSiteAddress",
"awsRegion": "us-west-2",
"sourceIPAddress": "XXX.XXX.XXX.XXX",
"userAgent": "userAgent",
"requestParameters": {
    "SiteId": "os-123ab4c56789de01f",
    "Address": "***"
},
"responseElements": {
    "Address": "***",
    "SiteId": "os-123ab4c56789de01f"
},
"requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
"eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

Outposts サーバーメンテナンス

責任共有モデルの下で、 AWS は AWS サービスを実行するハードウェアとソフトウェアを担当します。これは AWS Outposts、 AWS リージョンと同様にに適用されます。たとえば、はセキュリティパッチ AWS の管理、ファームウェアの更新、Outpost 機器の保守を行います。 AWS また、は Outposts サーバーのパフォーマンス、ヘルス、メトリクスを監視し、メンテナンスが必要かどうかを判断します。

⚠ Warning

基盤となるディスクドライブに障害が発生した場合、またはインスタンスが終了すると、インスタンストアボリュームのデータは失われます。データ損失を防ぐために、インスタンストアボリュームの長期データをAmazon S3バケットや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ストレージにバックアップすることをお勧めします。

内容

- ・ [連絡先の情報を更新する](#)
- ・ [ハードウェアメンテナンス](#)
- ・ [ファームウェアの更新](#)
- ・ [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](#)
- ・ [サーバーデータを暗号化して細断する](#)

連絡先の情報を更新する

Outpost の所有者が変更された場合は、新しい所有者の名前と連絡先の情報を[AWS サポートセンター](#)までご連絡ください。

ハードウェアメンテナンス

がサーバープロビジョニングプロセス中、または Outposts サーバーで実行されている Amazon EC2 インスタンスをホスト中にハードウェアに回復不可能な問題 AWS を検出した場合、影響を受けるインスタンスのリタイアが予定されていることをインスタンスの所有者に通知します。 詳細については、「Amazon EC2 ユーザーガイド」の「[インスタンスのリタイア](#)」を参照してください。

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 サーバーの設置](#)」の設置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のと同じパッケージ AWS でに梱包します。
- 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。
- サーバーをに返します 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 機器が配置されている施設は、Outposts 機器のインストール、メンテナンス、使用をサポートするために、最小限の[電力とネットワーク](#)要件を満たしている必要があります。Outposts サーバーは、電力供給とネットワーク接続が中断されない場合にのみ正常に動作します。

電力イベント

完全な停電では、AWS Outposts リソースが自動的にサービスに戻らないという固有のリスクがあります。冗長電源およびバックアップ電源ソリューションの導入に加えて、最悪のシナリオの影響を軽減するために、事前に次のことを実行することをお勧めします。

- 制御された方法で DNS ベースまたはラック外のロードバランシングの変更を使用して、サービスとアプリケーションを Outposts の機器から移動させてください。
- コンテナ、インスタンス、データベースを順序立てて停止し、それらを復元する際には逆の順序を使用してください。
- サービスの移動または停止を制御するためのテスト計画。
- 重要なデータと構成をバックアップし、Outpost の外部に保存します。
- 電源のダウンタイムを最小限に抑えます。
- メンテナンス中は電源の切り替え（オフ、オン、オフ、オン）を繰り返さないでください。
- 予期せぬ事態に対処するために、メンテナンス期間内に余分な時間を確保してください。
- 通常必要とされるよりも広いメンテナンス時間枠を伝えることで、ユーザーや顧客の期待に応えます。
- 電源が復旧したら、[AWS サポートセンター](#)でケースを作成して、AWS Outposts および関連サービスが実行されていることの検証をリクエストします。

ネットワーク接続イベント

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

Outposts サーバーの Amazon EC2 インスタンス、LNI ネットワーク、インスタン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と LNI 経由でローカルにアクセスできます。同様に、Amazon ECS ワーカーノードなどの AWS サービスリソースは引き続きローカルで実行されます。ただし、API の可用性は低下します。例えば、実行、開始、停止、終了 API は機能しない場合があります。インスタンスマトリクスとログは最大 7 日間ローカルにキャッシュされ、接続が戻ると AWS リージョンにプッシュされます。7 日以上切断すると、マトリクスとログが失われる可能性があります。

オンラインの電源の問題またはネットワーク接続の喪失が原因でサービスリンクがダウンした場合は Outposts を所有するアカウントに通知 Health Dashboard を送信します。中断が予想される場合でも、ユーザーも もサービスリンクの中止の通知を抑制する AWS ことはできません。詳細については、「AWS Health ユーザーガイド」の「[Health Dashboard の開始方法](#)」を参照してください。

ネットワーク接続に影響を与える計画的なサービスメンテナンスの場合は、次の予防的な手順を実行して、潜在的な問題のあるシナリオの影響を制限してください。

- 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。

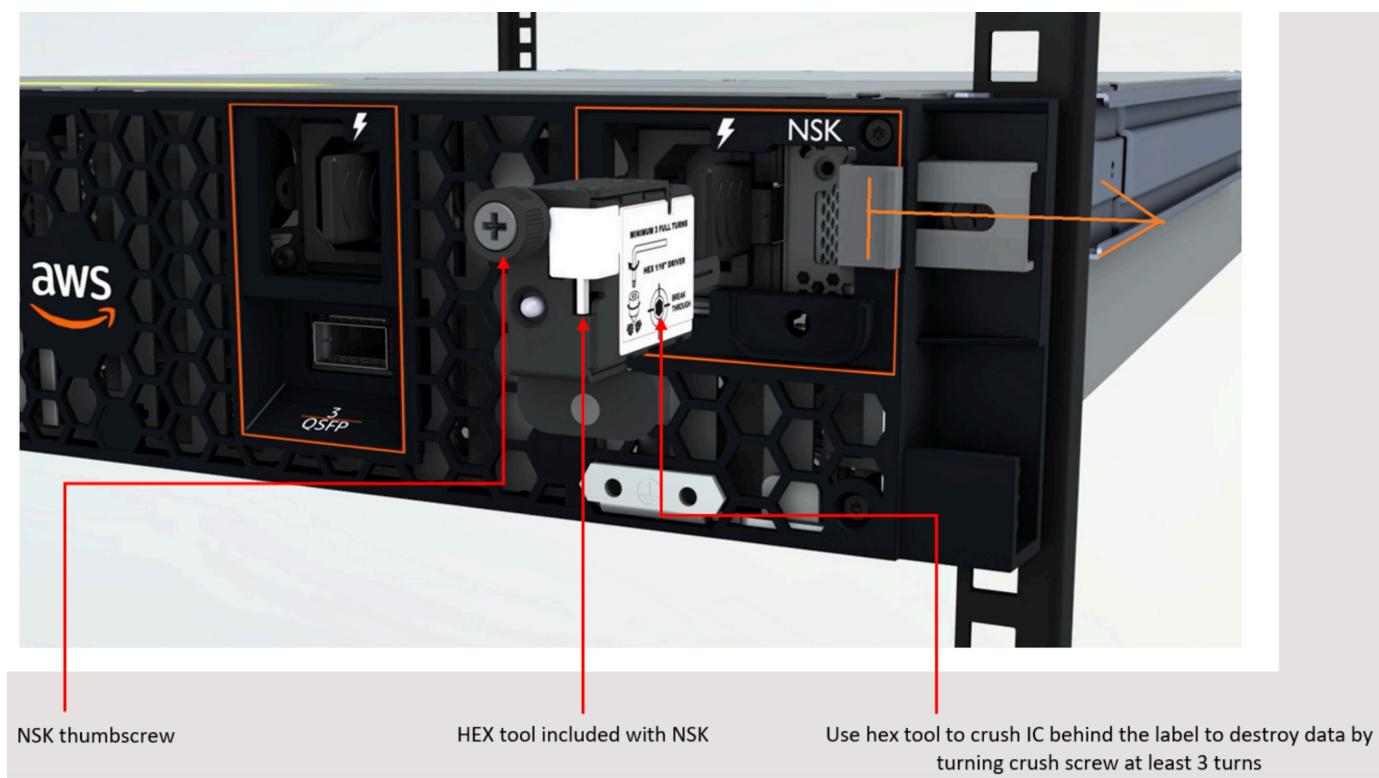
- AWS ブログ [「のモニタリングのベストプラクティス AWS Outposts」](#)では、Outposts固有のオペーパビリティとイベント管理のベストプラクティスについて説明しています。
- AWS ブログ [「Amazon VPCからのネットワーク接続用のデバッグツール」](#)では、AWSSupport-SetupIPMonitoringFromVPCツールについて説明します。本ツールは、お客様が指定したサブネットにAmazon EC2 Monitor Instanceを作成し、対象のIP AWS Systems Manager アドレスを監視するためのドキュメント(SSMドキュ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

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. サーバーを返送する前に、サーバーから NSK を削除します 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。



Outposts サーバーの契約期間終了オプション

AWS Outposts 期間の終了時に、次のオプションから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 サーバーを維持する。
- Outposts サーバーを返します。
- 月単位のサブスクリプションに切り替えて、既存の Outposts サーバーを維持する。

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 5 営業日前に、次のステップを完了する必要があります。現在のサブスクリプションが終了する少なくとも 5 営業日前にこれらのステップを完了しないと、予期しない料金が発生する可能性があります。

サブスクリプションを更新し、既存の Outposts サーバーを維持するには

1. <https://console.aws.amazon.com/outposts/> で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで、[Outpost] を選択してください。
3. [アクション] を選択します。
4. Outpost の更新を選択します。
5. サブスクリプション期間の長さと支払いオプションを選択します。

料金については、「[AWS Outposts 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。

6. サポートチケットの送信を選択します。

Note

Outposts サーバーの現在のサブスクリプションが終了する前に更新すると、前払い料金がすぐにお支払いされます。

新しいサブスクリプションは、現在のサブスクリプションが終了した翌日に開始されます。

サブスクリプションの更新や Outposts サーバーの返却を指定しない場合、自動的に月単位のサブスクリプションに切り替わります。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。

Outposts サーバーを返す

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には、まず 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 5 営業日前に廃止プロセスを完了する必要があります。完了するまで、AWS は返却プロセスを開始できません。現在のサブスクリプションが終了する少なくとも 5 営業日前に廃止プロセスを完了しないと、廃止の遅延や予期しない料金が発生する可能性があります。

廃止プロセスが完了したら、サーバーを返却する準備をし、配送ラベルを取得し、サーバーを梱包して返送する必要があります AWS。

Outposts サーバーを返送しても、配送料金は発生しません。ただし、破損したサーバーを返却すると、コストが発生する可能性があります。

タスク

- [ステップ 1: サーバーを返却する準備をする](#)
- [ステップ 2: サーバーを廃止する](#)
- [ステップ 3: 返送用配送ラベルを取得する](#)
- [ステップ 4: サーバーをパックする](#)
- [ステップ 5: 配送業者を通じてサーバーを返却する](#)

ステップ 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 [disassociate-resource-share](#) コマンド AWS CLI を実行します。

共有可能な Outpost リソースの一覧については、「[共有可能な Outpost リソース](#)」を参照してください。

2. 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 のサブネットに関するアクティブなインスタンスを終了してください。インスタンスを終了するには、「Amazon EC2 ユーザーガイド」の「[インスタンスの終了](#)」のステップに従ってください。
5. Nitro セキュリティキー (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します。NSK を破棄するには、[Cryptographically shred server data](#) の手順に従います。

ステップ 2: サーバーを廃止する

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 5 営業日前に、次の手順を実行します。

⚠ Important

AWS は、廃止リクエストを送信した後、返却プロセスを停止することはできません。

1. <https://console.aws.amazon.com/outposts/> で AWS Outposts コンソールを開きます。
2. ナビゲーションペインで、[Outpost] を選択してください。
3. [アクション] を選択します。
4. Decommission Outpost を選択し、ワークフローに従ってリソースを削除します。
5. [Submit request (リクエストの送信)] を選択します。

ⓘ Note

現在のサブスクリプションが終了する前に Outposts サーバーを返却しても、この Outpost に関する未払いの料金は終了しません。

ステップ 3: 返送用配送ラベルを取得する

⚠️ Important

AWS 返送するサーバーに関するアセット ID などの特定の情報が含まれているため、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。

配送ラベルを取得するには:

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 [注文] を選択します。
3. 返すサーバーの順序を選択します。
4. 注文の詳細ページの注文ステータスセクションで、返品ラベルの印刷を選択します。

ℹ️ Note

現在のサブスクリプションが終了する前に Outposts サーバーを返却しても、この Outpost に関連する未払いの料金は終了しません。

ステップ 4: サーバーをパックする

サーバーをパックするには、が提供するボックスとパッケージマテリアルを使用します AWS。

1. サーバーを次のいずれかの箱に梱包します。
 - サーバーが元々入っていた箱と梱包材。
 - 交換用サーバーが入っていた箱と梱包材。

または、[AWS サポート センター](#) に連絡して箱をリクエストしてください。

2. AWS 提供された配送ラベルを箱の外側に貼り付けます。

⚠️ Important

配送ラベルのアセット ID が、返送するサーバーのアセット ID と一致することを確認してください。

アセット ID は、サーバー前面の引き出しタブにあります。例: 1203779889 または 9305589922

3. 箱を確実に密封します。

ステップ 5: 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。

Country	連絡先
アルゼンチン	AWS サポートセンター に問い合わせます。リストで以下の情報を提供してください。
バーレーン	<ul style="list-style-type: none">AWS 提供された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
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	

Country	連絡先
日本	
マレーシア	
ナイジェリア	
オマーン	
パナマ	
ペルー	
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	

Country	連絡先
アメリカ合衆国	<p>UPS に問い合わせてください。</p> <p>サーバーは以下の方法で返却できます。</p> <ul style="list-style-type: none"> 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。 AWS 提供の発送ラベルにある追跡番号を入力すると送料が無料になります。
他のすべての国	<p>DHL に問い合わせてください。</p> <p>サーバーは以下の方法で返却できます。</p> <ul style="list-style-type: none"> 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。 AWS 送料無料の配送ラベルから DHL Waybill 番号を入力します。 <p>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。</p>

月単位のサブスクリプションへの変換

月単位のサブスクリプションに切り替えて、既存の Outposts サーバーを維持する場合、アクションを起こす必要はありません。質問がある場合は、請求サポートケースを開いてください。

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。

のクオータ AWS Outposts

にはデフォルトのクオータ AWS アカウント があり、以前は制限と呼ばれていました AWS のサービス。特に明記していない限り、クオータはリージョン固有です。一部のクオータについては引き上げをリクエストできますが、一部のクオータについてはリクエストできません。

のクオータを表示するには AWS Outposts、[Service Quotas コンソール](#)を開きます。ナビゲーションペインで、[AWS のサービス] を選択し、次に [AWS Outposts] を選択します。

クオ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「[クオータ引き上げリクエスト](#)」を参照してください。

AWS アカウント には、 に関する次のクオータがあります AWS Outposts。

リソース	デフォルト値	引き上げ可能	コメント
Outpost サイト	100	可能	Outpost サイトは、Outpost 機器に電力を供給してネットワークに接続する、カスタマー管理の物理的な建物です。 AWS アカウントの各リージョンに 100 の Outposts サイトを設定できます。
サイトあたりの Outpost	10	可能	AWS Outposts には、Outposts と呼ばれるハードウェアおよび仮想リソースが含まれています。このクオータは、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 および他の サービスの クオータ

AWS Outposts は他の サービスのリソースに依存し、それらのサービスには独自のデフォルトクオ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オータは、ネットワークインターフェイスの Amazon VPC クオータから取得されます。

Outposts サーバーのドキュメント履歴

以下の表は、Outposts サーバーのドキュメントに対する更新について説明しています。

変更	説明	日付
<u>AWS Outposts が Dell および HPE ストレージ配列の外部ブロックボリュームをサポート</u>	Dell PowerStore や HPE Alletra Storage MP B10000 などのサードパーティイーベンダーがサポートする外部ブロックデータとブートボリュームを使用できます。	2025 年 9 月 30 日
<u>サブスクリプションを更新し、サーバーを返却する準備をする</u>	サブスクリプションを更新またはサーバーを返すには、現在のサブスクリプションが終了する少なくとも 10 営業日前にプロセスを完了する必要があります。	2025 年 7 月 16 日
<u>サービスリンク接続のトラブルシューティング</u>	Outposts サーバーと AWS リージョン間の接続が停止している場合は、以下の手順に従ってトラブルシューティングと解決を行います。	2025 年 5 月 5 日
<u>静的安定性の更新</u>	ネットワークが中断された場合、インスタンスマトリクスとログは最大 7 日間ローカルにキャッシュされます。以前は、Outposts はわずか数時間ログをキャッシュできました。	2025 年 5 月 1 日
<u>アセットレベルでのキャパシティ管理</u>	アセットレベルで容量設定を変更できます。	2025 年 3 月 31 日

<u>サードパーティーストレージにバックアップされた外部ブロックボリューム</u>	Outpost のインスタンス起動プロセス中に、互換性のあるサードパーティのブロックストレージシステムにバックアップされたブロックデータボリュームをアタッチできるようになりました。	2024 年 12 月 1 日
<u>キャパシティ管理</u>	新しい Outposts の注文のデフォルトのキャパシティ設定を変更できます。	2024 年 4 月 16 日
<u>AWS Outposts サーバーの End-of-term オプション</u>	AWS Outposts 契約期間の終了時に、サブスクリプションを更新、終了、または変換できます。	2023 年 8 月 1 日
<u>Outposts サーバー用 AWS Outposts ユーザーガイドを作成</u>	AWS Outposts ユーザーガイドは、ラックとサーバーの個別のガイドに分かれています。	2022 年 9 月 14 日
<u>でのプレイスメントグループ AWS Outposts</u>	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
<u>Outposts サーバーの紹介</u>	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。