ユーザーガイド

Amazon Elastic VMware サービス

Amazon Elastic VMware サービス: ユーザーガイド

Table of Contents

Amazon Elastic VMware Service とは

Amazon Elastic VMware Service (Amazon EVS) を使用して、VMware Cloud Foundation (VCF) 環境を Amazon Virtual Private Cloud (VPC) 内の EC2 ベアメタルインスタンスに直接デプロイして実行できます。

トピック

Amazon EVS の機能

Amazon EVS の主な機能は次のとおりです。

への移行を簡素化して高速化する AWS

移行の摩擦を排除し、サブスクリプションの移植性とクラウドへの VMware Cloud Foundation (VCF) の自動デプロイによる運用上の一貫性を確保します。IP アドレスを変更したり、スタッフを再トレーニングしたり、運用ランブックを書き換えたりすることなく、オンプレミスネットワークを拡張し、ワークロードを移行できます。

クラウドで VMware アーキテクチャの制御を維持する

VMware アーキテクチャを完全に制御し、アドオンやサードパーティーソリューションなど、アプリケーションの固有の需要を満たす仮想化スタックを最適化します。

マネージドエクスペリエンスのために AWS パートナーを自己管理または活用する

自己管理の選択と柔軟性を引き出すか、 AWS パートナーの専門知識を活用して で VCF 環境を管理および運用 AWS し、人材、時間、コストにわたるビジネス目標を達成します。

ビジネスのスケールと中断からの保護

VMware ベースのワークロードを移行して運用するために、最も安全でスケーラブルで回復力の高いクラウドでスケーラビリティを強化します。

AWS イノベーションを取り入れてアプリケーションとインフラストラクチャを変革する

AWSネイティブサービスである Amazon EVS は、200 以上のサービス (マネージドデータベース、分析、サーバーレスとコンテナ、生成 AI を含む) を使用して VMware 環境の拡張と拡張を簡素化し、ビジネスを変革します。

Amazon EVS の使用を開始する

最初の Amazon EVS 環境を作成するには、「」を参照してください開始方法。一般的に、Amazon EVS の使用を開始するには、次のステップを完了する必要があります。

1. 前提条件を満たす。詳細については、「Amazon Elastic VMware Service のセットアップ」を参照してください。
2. Amazon EVS 環境を作成します。環境の作成中に、Amazon EVS は指定した CIDR 範囲を使用して必要な VLAN サブネットを作成し、ホストを環境に追加します。
3. VCF をカスタマイズします。必要に応じて、vSphere ユーザーインターフェイスで環境を設定します。これには、ログイン、ポリシー、モニタリングの設定などが含まれます。
4. 接続して移行します。環境をオンプレミスデータセンターに接続し、VPC ワークロードを Amazon EVS に移行します。

Amazon EVS へのアクセス

次のインターフェイスを使用して、Amazon EVS デプロイを定義および設定できます。

- Amazon EVS コンソール - Amazon EVS 環境を作成するためのウェブインターフェイスを提供します。
- AWS CLI - Windows、macOS、Linux で AWS のサービス サポートされている および の幅広いセットのコマンドを提供します。詳細については、「AWS Command Line Interface」を参照してください。
- AWS CloudFormation - など、各リソースタイプの仕様を提供しますAWS::EVS::Environment。リソース仕様を使用してテンプレートを作成すると、CloudFormation がリソースのプロビジョニングと設定を行います。

Amazon EVS の概念とコンポーネント

このセクションでは、Amazon EVS の主要な概念とコンポーネントについて説明します。

Amazon EVS 環境

Amazon EVS 環境は、vSphere ホスト、vSAN、NSX、SDDC Manager などの VMware Cloud Foundation (VCF) リソース用の論理コンテナです。環境では、VCF ソフトウェアスタックの管理、モニタリング、インスタンス化のためのコンポーネントをホストする vSphere クラスターが統合 VCF ドメインに含まれています。各環境は SDDC Manager アプライアンスに直接マッピングされます。詳細については、「the section called “アーキテクチャ”」を参照してください。

Amazon EVS ホスト

Amazon EVS ホストは、 Amazon EC2 ベアメタルインスタンスで実行される VMware ESX ホストです。Amazon EVS ホストは、管理仮想マシンとワークロード仮想マシンを保存する vSAN データストアにローカル NVMe インスタンスストアボリュームを使用します。

> **Warning**
>
> インスタンスストアボリュームはエフェメラルです。これらのボリュームに保存されているデータは、基盤となる EC2 インスタンスが停止または終了しても保持されません。VCF 内で廃止せずに Amazon EVS が使用する Amazon EC2 インスタンスを停止または終了すると、データが失われる可能性があります。
> ホストのメンテナンスの詳細については、「」を参照してくださいthe section called “ホストのメンテナンス”。

サービスアクセスサブネット

サービスアクセスサブネットは、Amazon EVS が VCF デプロイにアクセスできるようにする標準 VPC サブネットです。Amazon EVS 環境の作成時に、サービスアクセスに使用する Amazon EVS の VPC とサブネットを指定します。

Amazon EVS 環境を作成すると、Amazon EVS は VCF アプライアンスと ESX ホストへの管理接続を容易にするために、Elastic Network Interface をサービスアクセスサブネットにプロビジョニングします。この接続は、Amazon EVS が VCF デプロイをデプロイ、管理、モニタリングできるようにするために必要です。

Amazon EVS VLAN サブネット

Amazon EVS VLAN サブネットは、Amazon EVS によって管理される Amazon VPC サブネットです。VLAN サブネットは、Amazon EVS ホスト用の VPC 接続と、VMware NSX、VMware HCX、VMware vCenter Server などの VCF アプライアンスを提供します。各 VLAN サブネットには VLAN タグがあり、VLAN ネットワークトラフィックを論理的にセグメント化できます。

Amazon EVS は、Amazon EVS 環境の作成時にサービスが使用するすべての VLAN サブネットを作成します。VLAN サブネットが使用する CIDR ブロック入力を指定します。VLAN サブネット CIDR ブロックが、将来のスケーリングのニーズを考慮して、設定されるホストの数に応じて適切にサイズ設定されていることを確認する必要があります。CIDR ブロックの最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。CIDR ブロックは、VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。

作成時に、VPC サブネットは VPC のメインルートテーブルに暗黙的に関連付けられます。デプロイ後、VLAN サブネットをカスタムルートテーブルに明示的に関連付けることができます。詳細については、「the section called “Amazon EVS ネットワークに関する考慮事項”」を参照してください。

> **Important**
>
> Amazon EVS VLAN サブネットは Amazon EVS 環境の作成時にのみ作成でき、環境の作成後に変更することはできません。環境を作成する前に、VLAN サブネット CIDR ブロックのサイズが適切であることを確認する必要があります。環境のデプロイ後に VLAN サブネットを追加することはできません。

> **Important**
>
> EC2 セキュリティグループルールは、VLAN サブネットにアタッチされている Amazon EVS Elastic Network Interface には適用されません。VLAN サブネットとの間のトラフィックを制御するには、ネットワークアクセスコントロールリストを使用する必要があります。

ホスト管理 VLAN サブネット

ホスト管理 VLAN サブネットは、管理トラフィックをユーザートラフィックから分離し、ホストのリモート管理を可能にします。EVS ホスト管理 vmkernel ネットワークインターフェイスはこのサブネットに接続します。

vMotion VLAN サブネット

vMotion VLAN サブネットは、VMware vMotion トラフィックを論理的にセグメント化し、vMotion プロセス中にホスト間で仮想マシンを移動するために使用されます。

vSAN VLAN サブネット

vSAN VLAN サブネットは、VMware vSAN によって使用され、vSAN のストレージオペレーションに関連するトラフィックを他のネットワークトラフィックから分離します。

VTEP VLAN サブネット

VTEP VLAN サブネットは、VMware NSX 仮想トンネルエンドポイント (VTEP) を使用して、Amazon EVS ESX ホストのオーバーレイネットワークトラフィックをカプセル化およびカプセル化解除します。

Edge VTEP VLAN サブネット

Edge VTEP VLAN サブネットは、NSX Edge アプライアンスのオーバーレイトラフィック専用の特殊な VTEP VLAN サブネットです。この VLAN は、NSX エッジと ESX ホスト間のオーバーレイ通信に使用されます。

Management VM VLAN サブネット

Management VM VLAN サブネットは、NSX Manager、vCenter Server、SDDC Manager などの仮想アプライアンスの管理に使用されます。

HCX アップリンク VLAN サブネット

HCX アップリンク VLAN サブネットは、HCX Interconnect (HCX-IX) アプライアンスと HCX Network Extension (HCX-NE) アプライアンス間の通信に使用され、HCX サービスメッシュアップリンクの作成を可能にします。

NSX アップリンク VLAN サブネット

NSX アップリンク VLAN サブネットは、NSX オーバーレイネットワークを VPC の残りの部分や、設定した他の外部ネットワークに接続するために使用されます。NSX アップリンク VLAN サブネットは、NSX Edge ノードアップリンクで設定されます。

拡張 VLAN サブネット

拡張 VLAN サブネットを使用して、NSX フェデレーションなど、追加の VCF 対応関数を有効にできます。Amazon EVS は、環境の作成時に 2 つの拡張 VLAN サブネットを作成します。

VMware NSX

VMware NSX は、ネットワーク仮想化を可能にする Software-Defined Networking (SDN) プラットフォームです。Amazon EVS は、VMware NSX を使用して、VMware Cloud Foundation (VCF) アプライアンスとワークロードが実行されるオーバーレイネットワークを作成および管理します。Amazon EVS は、NSX オーバーレイネットワークとともにアクティブ/スタンバイ NSX Edge ノードのペアをデプロイします。Amazon EVS は、デプロイの一環として、ユーザーに代わってすべての NSX ルーティングとアップリンクを自動的に設定します。一般的な NSX の概念の詳細については、VMware NSX インストールガイドの「主要な概念」を参照してください。

VMware Hybrid Cloud Extension (HCX)

VMware Hybrid Cloud Extension (VMware HCX) は、アプリケーションの移行を簡素化し、ワークロードを再調整し、データセンターとクラウド間のディザスタリカバリを最適化するために設計されたアプリケーションモビリティプラットフォームです。HCX を使用して、VMware ベースのワークロードを Amazon EVS に移行できます。

VMware HCX の接続を設定するには、関連付けられたトランジットゲートウェイ Direct Connect を使用するか、トランジットゲートウェイへの AWS Site-to-Site VPN アタッチメントを使用します。詳細については、「移行」を参照してください。

Amazon EVS アーキテクチャ

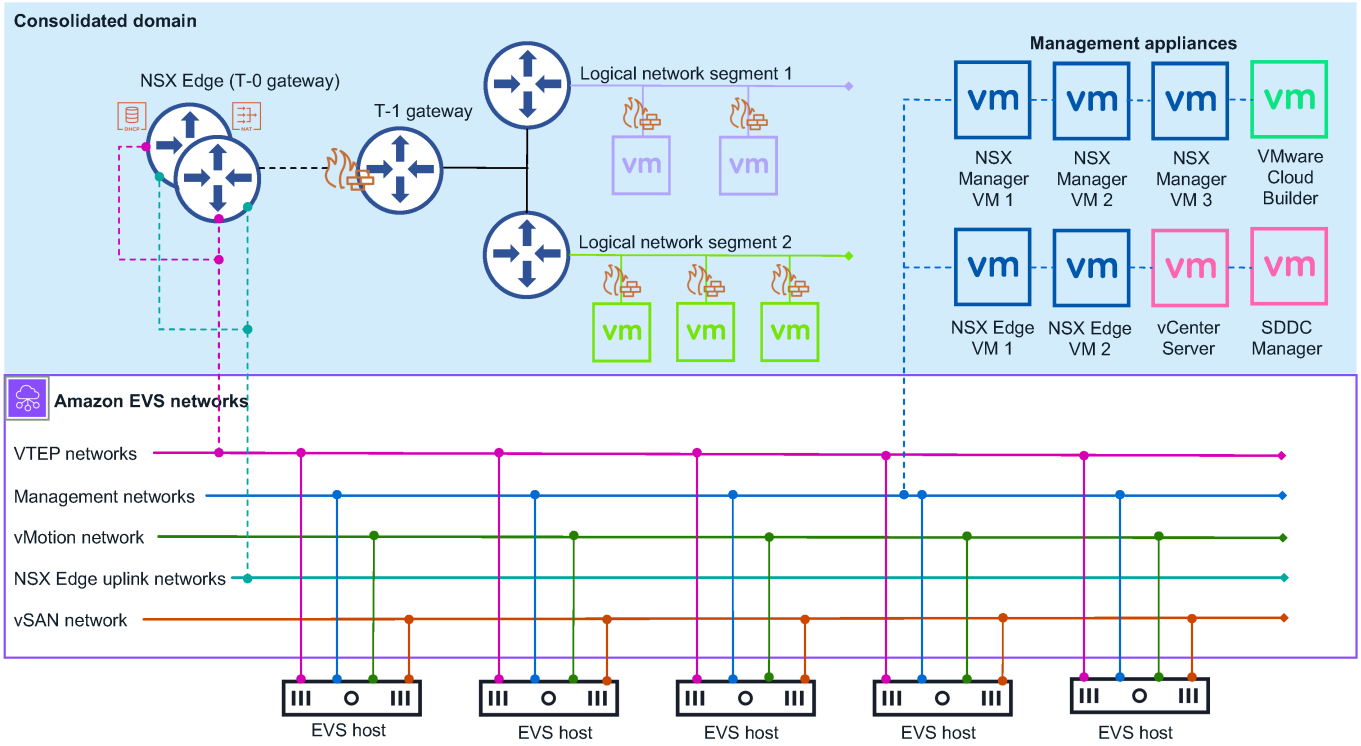
Amazon EVS は、VMware Cloud Foundation (VCF) 統合アーキテクチャモデルを実装しています。このモデルでは、VPC 管理コンポーネントとお客様のワークロードが統合ドメインで一緒に実行されます。Amazon EVS 環境は、管理ワークロードとお客様のワークロードを分離する vSphere リソースプールを備えた単一の vCenter Server から管理されます。 vSphere

Amazon EVS がデプロイする統合ドメインには、次の VCF 管理コンポーネントが含まれています。

- ESX ホスト
- vCenter Server インスタンス
- SDDC マネージャー

- vSAN データストア
- 3 ノード NSX Manager クラスター
- vSphere クラスター
- NSX Edge クラスター

次の図は、Amazon EVS 環境にデプロイされた Amazon EVS アーキテクチャの例と、環境内のコンポーネントの接続方法を示しています。この図では、統合されたドメインアーキテクチャを持つ Amazon EVS 環境は青色にシェーディングされています。基盤となる Amazon EVS ネットワークトポロジは、紫色の実線内に示されています。



ネットワークトポロジ

Amazon EVS 環境には、2 つの異なる管理ネットワークレイヤーがあります。

Amazon VPC

環境の作成中に VPC に作成された Amazon VPC と Amazon EVS VLAN サブネットは、VPC デプロイのアンダーレイネットワークを形成します。このインフラストラクチャは、NSX オーバーレイネットワーク、ホスト管理、vMotion、および VSAN の接続を提供します。Amazon VPC Route Server は、アンダーレイネットワークとオーバーレイネットワーク間の動的ルーティング

を有効にします。詳細については、「the section called “概念とコンポーネント”」を参照してください。

> **Note**
>
> Amazon EVS VLAN サブネットは、VPC アンダーレイ通信を容易にするために使用されます。お客様のワークロードを実行しているゲスト仮想マシンは、NSX オーバーレイネットワークにデプロイする必要があります。Amazon EVS VLAN サブネットアンダーレイネットワークへのゲスト仮想マシンのデプロイはサポートされていません。

VMware NSX オーバーレイネットワーク

Amazon EVS は、デプロイの一部としてユーザーに代わって NSX オーバーレイネットワークを設定します。Amazon EVS 環境内のさまざまなワークロードまたはアプリケーション間でネットワークを分離できるように、追加の NSX オーバーレイネットワークを設定できます。詳細については、VMware Cloud Foundation 製品ドキュメントの「Overlay Design for VMware Cloud Foundation」を参照してください。

> **Note**
>
> Amazon EVS は、2 つの NSX Edge ノードを持つアクティブ/スタンバイ NSX Edge クラスターに対して 1 つの階層 0 ゲートウェイのみをサポートします。この階層 0 ゲートウェイは、Amazon EVS で使用するように設定したすべてのオーバーレイネットワークに接続してアドバタイズします。

2 つのネットワークレイヤーは、2 つの NSX Edge ノードを持つアクティブ/スタンバイ NSX Edge クラスターによって接続されます。NSX Edge ノードにより、VPC を介した VLANs内の仮想マシン間の通信、インターネット接続、またはトランジットゲートウェイでの Direct Connect or AWS Site-to-Site VPN を使用したプライベート接続が可能になります。

Amazon EVS ネットワークに関する考慮事項

管理ネットワークには、次のネットワークリソース設定が必要です。これらの入力は、Amazon EVS 環境の作成時に指定します。詳細については、「the section called “概念とコンポーネント”」を参照してください。

- Amazon VPC。VPC IPv4 CIDR ブロックのサイズが、環境の作成時に Amazon EVS がプロビジョニングする必要な VPC サブネットと Amazon EVS VLAN サブネットに合わせて適切に設定されていることを確認します。詳細については、「the section called “Amazon EVS VLAN サブネット”」を参照してください。

> **Note**
>
> Amazon EVS は現在 IPv6 をサポートしていません。

- VPC のサービスアクセスサブネット。Amazon EVS はこのサブネットを使用して、SDDC Manager アプライアンスへの永続的な接続を維持します。詳細については、「the section called “サービスアクセスサブネット”」を参照してください。

> **Note**
>
> Amazon EVS は、現時点ではシングル AZ 配置のみをサポートしています。Amazon EVS が使用するすべての VPC サブネットは、サービスが利用可能なリージョンの単一のアベイラビリティーゾーンに存在する必要があります。

> **Note**
>
> すべての VPC サブネットには、組織のネットワーク要件に従って設定された、関連付けられたルートテーブルが必要です。

- ホスト IP アドレスを解決するように設定された VPC の DHCP オプション内のプライマリ DNS サーバー IP アドレスとセカンダリ DNS サーバー IP アドレス。また、Amazon EVS では、デプロイ内の各 VCF 管理アプライアンスと Amazon EVS ホストの A レコードを含む DNS フォワードルックアップゾーンと PTR レコードを含むリバースルックアップゾーンを作成する必要があります。詳細については、「the section called “DNS サーバーを設定する”」を参照してください。
- Amazon EVS VLAN サブネット CIDR は、環境の作成中に Amazon EVS がプロビジョニングする VLAN サブネットごとにブロックします。CIDR ブロックの最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。CIDR ブロックは重複していない必要があります。
- Amazon VPC Route Server の伝播が有効になっている Route Server インスタンス。
- サービスアクセスサブネット内の 2 つの Route Server エンドポイント。

- Amazon EVS が Route Server エンドポイントとプロビジョニングする NSX Edge ノードをピアリングする 2 つの Route Server ピア。

Tier-0 ゲートウェイ

階層 0 ゲートウェイは、論理ネットワークと物理ネットワーク間のすべての南北トラフィックを処理し、NSX オーバーレイネットワーク上に作成されます。この tier-0 ゲートウェイは、Amazon EVS デプロイの一部として作成されます。

> **Note**
>
> Amazon EVS は、2 つの NSX Edge ノードを持つアクティブ/スタンバイ NSX Edge クラスターに対して 1 つの階層 0 ゲートウェイのみをサポートします。

Tier-1 ゲートウェイ

階層 1 ゲートウェイは、環境内のルーティングされたネットワークセグメント間の東西トラフィックを処理し、NSX オーバーレイネットワーク上に作成されます。階層 1 ゲートウェイには、セグメントへのダウンリンク接続と階層 0 ゲートウェイへのアップリンク接続があります。必要に応じて、追加の Tier-1 ゲートウェイを作成して設定できます。

NSX Edge クラスター

Amazon EVS は NSX Manager インターフェイスを使用して、アクティブ/スタンバイモードで実行される 2 つの NSX Edge ノードを持つ NSX Edge クラスターをデプロイします。この NSX Edge クラスターは、Tier-0 および Tier-1 ゲートウェイが実行されるプラットフォームと、IPsec VPN 接続とその BGP ルーティングマシンを提供します。

Amazon EVS リソース

Amazon EVS は、環境の作成時に次の AWS リソースをプロビジョニングします。これらのリソースは、Amazon EVS がアクセスすることを許可する VPC に表示され、作成後に AWS マネジメントコンソール および AWS CLI に表示されます。

> **Important**
>
> Amazon EVS コンソールおよび API の外部でこれらのリソースを変更すると、Amazon EVS 環境の可用性と安定性に影響する可能性があります。

- VCF アプライアンスとホストへの接続を可能にする Amazon EVS Elastic Network Interface。
- Amazon EC2 ベアメタルインスタンスで実行される Amazon EVS ESX ホスト。詳細については、「the section called “Amazon EVS ホスト”」を参照してください。

> **Important**
>
> Amazon EVS 環境には、4 つ以上のホストと 16 以下のホストが必要です。Amazon EVS は 4 ~ 16 ホストの環境のみをサポートします。

- VPC を VCF アプライアンスに接続する Amazon EVS VLAN サブネット。詳細については、「the section called “Amazon EVS VLAN サブネット”」を参照してください。

Amazon Elastic VMware Service のセットアップ

Amazon EVS を使用するには、他の AWS サービスを設定し、VMware Cloud Foundation (VCF) の要件を満たすように環境を設定する必要があります。デプロイの前提条件の概要チェックリストについては、「」を参照してくださいthe section called “デプロイチェックリスト”。

トピック

- にサインアップする AWS
- IAM ユーザーの作成
- Amazon EVS アクセス許可を IAM ユーザーに委任する IAM ロールを作成する
- AWS Business、 AWS Enterprise On-Ramp、または AWS Enterprise Support プランにサインアップする
- クォータをチェックする
- VPC CIDR サイズの計画
- サブネットを使用して VPC を作成する
- VPC メインルートテーブルを設定する
- VPC の DHCP オプションセットを設定する
- VPC Route Server インフラストラクチャの作成と設定
- オンプレミス接続用のトランジットゲートウェイを作成する
- Amazon EC2 キャパシティ予約を作成する
- のセットアップ AWS CLI
- Amazon EC2 キーペアを作成する
- VMware Cloud Foundation (VCF) 用の環境を準備する
- VCF ライセンスキーを取得する
- VMware HCX の前提条件
- Amazon EVS デプロイの前提条件チェックリスト

にサインアップする AWS

がない場合は AWS アカウント、次の手順を実行して作成します。

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

IAM ユーザーの作成

1. ルートユーザーを選択し、アカウントの E メールアドレスを入力して、 AWS アカウント所有者として IAM コンソールにサインインします。次のページでパスワードを入力します。

   > **Note**
   >
   > 以下の IAM の Administrator ユーザーの使用に関するベストプラクティスに従って、ルートユーザーの認証情報は安全な場所に保管しておくことを強くお勧めします。ルートユーザーとしてのサインインは、いくつかのアカウントとサービスの管理タスクの実行にのみ使用してください。

2. ナビゲーションペインで、ユーザーを選択し、ユーザーの作成を選択します。
3. [ユーザー名] に「Administrator」と入力します。
4. AWS マネジメントコンソールアクセスの横にあるチェックボックスをオンにします。[Custom password (カスタムパスワード)] を選択し、その後テキストボックスに新しいパスワードを入力します。
5. (オプション) デフォルトでは、 AWS は初回サインイン時に新しいパスワードを作成する必要があります。[User must create a new password at next sign-in] (ユーザーは次回のサインイン時に新しいパスワードを作成する必要がある) の隣にあるチェックボックスのチェックを外して、新しいユーザーがサインインしてからパスワードをリセットできるようにできます。
6. [Next: Permissions] (次のステップ: 許可) を選択します。
7. [Set permissions] (許可の設定) で、Add user to group (ユーザーをグループに追加) を選択します。
8. [Create group] (グループの作成) を選択します。
9. [Create group] (グループの作成) ダイアログボックスで、Group name (グループ名) に「Administrators」と入力します。
10. フィルターポリシーを選択し、 AWS マネージド -job 関数を選択してテーブルコンテンツをフィルタリングします。
11. ポリシーリストで、[AdministratorAccess] のチェックボックスをオンにします。その後、[Create group] (グループの作成) を選択します。

> **Note**
>
> アクセスAdministratorAccess許可を使用して Billing and Cost Management コンソールにアクセスする前に、IAM ユーザーとロールの AWS Billing へのアクセスを有効にする必要があります。これを行うには、請求コンソールへのアクセス権の委任に関するチュートリアルのステップ 1 の手順に従ってください。

12.グループのリストに戻り、新しいグループのチェックボックスをオンにします。必要に応じて [Refresh] (更新) を選択し、リスト内のグループを表示します。

13.[Next: Tags] (次へ: タグ) を選択します。

14.(オプション) タグをキーバリューペアとしてアタッチして、メタデータをユーザーに追加します。IAM でのタグの使用の詳細については、IAM ユーザーガイドの「IAM リソースのタグ付け」を参照してください。

15.[Next: Review] (次のステップ: 確認) を選択して、新しいユーザーに追加されるグループメンバーシップのリストを表示します。続行する準備ができたら、[Create user] (ユーザーの作成) を選択します。

これと同じプロセスを使用して、より多くのグループとユーザーを作成し、ユーザーに AWS アカウントリソースへのアクセスを許可できます。ユーザーアクセス許可を特定の AWS リソースに制限するポリシーの使用については、「アクセス管理」と「ポリシーの例」を参照してください。

Amazon EVS アクセス許可を IAM ユーザーに委任する IAM ロールを作成する

ロールを使用して、 AWS リソースへのアクセスを委任できます。IAM ロールを使用すると、信頼するアカウントと他の AWS 信頼されたアカウントとの間に信頼関係を確立できます。信頼するアカウントはアクセスするリソースを所有し、信頼されたアカウントにはリソースへのアクセスを必要とするユーザーが含まれます。

信頼関係を作成すると、信頼されたアカウントの IAM ユーザーまたはアプリケーションは AWS Security Token Service (AWS STS) AssumeRole API オペレーションを使用できます。このオペレーションは、アカウントの AWS リソースへのアクセスを可能にする一時的なセキュリティ認証情報を提供します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「IAM ユーザーにアクセス許可を委任するロールを作成する」を参照してください。

Amazon EVS オペレーションへのアクセスを許可するアクセス許可ポリシーを持つ IAM ロールを作成するには、次の手順に従います。

> **Note**
>
> Amazon EVS では、インスタンスプロファイルを使用して IAM ロールを EC2 インスタンスに渡すことはサポートされていません。

Example

IAM console

1. IAM コンソールに移動します。
2. 左側のメニューで、ポリシーを選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. ポリシーエディタで、Amazon EVS オペレーションを有効にするアクセス許可ポリシーを作成します。ポリシーの例については「the section called “Amazon EVS 環境の作成と管理”」を参照してください。使用可能なすべての Amazon EVS アクション、リソース、および条件キーを表示するには、「サービス認可リファレンス」の「アクション」を参照してください。
5. [次へ] を選択します。
6. ポリシー名に、このポリシーを識別するためのわかりやすいポリシー名を入力します。
7. このポリシーで定義されているアクセス許可を確認します。
8. (オプション) このリソースの識別、整理、検索に役立つタグを追加します。
9. [Create policy] (ポリシーの作成) を選択します。
10. 左側のメニューで、ロールを選択します。
11. [ロールの作成] を選択してください。
12. 信頼されたエンティティタイプで、 を選択します AWS アカウント。
13. で、Amazon AWS アカウント EVS アクションを実行するアカウントを指定し、次へを選択します。
14. アクセス許可の追加ページで、以前に作成したアクセス許可ポリシーを選択し、次へを選択します。
15. ロール名 に、このロールを識別するわかりやすい名前を入力します。
16. 信頼ポリシーを確認し、正しい AWS アカウント がプリンシパルとしてリストされていることを確認します。

17(オプション) このリソースの識別、整理、検索に役立つタグを追加します。

18[ロールの作成] を選択してください。

AWS CLI

1. 次の内容を信頼ポリシー JSON ファイルにコピーします。プリンシパル ARN の場合、サンプル AWS アカウント ID とservice-user名前を独自の AWS アカウント ID と IAM ユーザー名に置き換えます。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/service-user"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. ロールを作成します。を信頼ポリシーファイル名evs-environment-role-trust-policy.jsonに置き換えます。

```
aws iam create-role \
  --role-name myAmazonEVSEnvironmentRole \
  --assume-role-policy-document file://"evs-environment-role-trust-policy.json"
```

3. Amazon EVS オペレーションを有効にし、ポリシーをロールにアタッチするアクセス許可ポリシーを作成します。myAmazonEVSEnvironmentRole を ロール名前で置き換えます。ポリシーの例については「the section called “Amazon EVS 環境の作成と管理”」を参照してください。使用可能なすべての Amazon EVS アクション、リソース、および条件キーを表示するには、「サービス認可リファレンス」の「アクション」を参照してください。

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEVSEnvironmentPolicy \
  --role-name myAmazonEVSEnvironmentRole
```

AWS Business、 AWS Enterprise On-Ramp、または AWS Enterprise Support プランにサインアップする

Amazon EVS では、お客様が AWS Business、 AWS Enterprise On-Ramp、または AWS Enterprise Support プランに登録して、テクニカルサポートとアーキテクチャガイダンスに継続的にアクセスする必要があります。 AWS Business Support は、Amazon EVS の要件を満たす最小 AWS サポート階層です。ビジネスクリティカルなワークロードがある場合は、 AWS Enterprise On-Ramp プランまたは AWS Enterprise Support プランに登録することをお勧めします。詳細については、AWS 「サポートプランの比較」を参照してください。

> **Important**
>
> AWS Business、 AWS Enterprise On-Ramp、または AWS Enterprise Support プランにサインアップしないと、Amazon EVS 環境の作成は失敗します。

クォータをチェックする

Amazon EVS 環境の作成を有効にするには、アカウントに最低限必要なアカウントレベルのクォータがあることを確認します。詳細については、「サービスクォータ」を参照してください。

> **Important**
>
> EVS 環境クォータあたりのホスト数が 4 以上の場合、Amazon EVS 環境の作成は失敗します。

VPC CIDR サイズの計画

Amazon EVS 環境を作成するときは、VPC CIDR ブロックを指定する必要があります。環境の作成後に VPC CIDR ブロックを変更することはできません。また、環境のデプロイ中に Amazon EVS が作成する必要な EVS サブネットとホストに対応するのに十分なスペースを確保する必要があります。そのため、デプロイ前に Amazon EVS の要件と将来のスケーリングのニーズを考慮して、CIDR ブロックサイズを慎重に計画することが重要です。Amazon EVS には、必要な EVS サブネットとホストに十分なスペースを確保するために、最小サイズが /22 ネットマスクの VPC CIDR ブロックが必要です。詳細については、「the section called “Amazon EVS ネットワークに関する考慮事項”」を参照してください。

> **Important**
>
> VPC サブネットと Amazon EVS が VCF アプライアンス用に作成する VLAN サブネットの両方に十分な IP アドレス空間があることを確認します。VPC CIDR ブロックは、必要な EVS サブネットとホストに十分なスペースを確保するために、最小サイズが /22 ネットマスクである必要があります。

> **Note**
>
> Amazon EVS は現在 IPv6 をサポートしていません。

サブネットを使用して VPC を作成する

Amazon EVS は、指定した VPC に環境をデプロイします。この VPC には、Amazon EVS サービスアクセス () のサブネットが含まれている必要がありますthe section called “サービスアクセスサブネット”。Amazon EVS のサブネットを使用して VPC を作成する手順については、「」を参照してくださいthe section called “サブネットとルートテーブルを使用して VPC を作成する”。

VPC メインルートテーブルを設定する

Amazon EVS VLAN サブネットは、VPC メインルートテーブルに暗黙的に関連付けられます。環境のデプロイを成功させるために DNS やオンプレミスシステムなどの依存サービスへの接続を有効にするには、これらのシステムへのトラフィックを許可するようにメインルートテーブルを設定する必要があります。詳細については、「the section called “Amazon EVS VLAN サブネットを VPC ルートテーブルに明示的に関連付ける”」を参照してください。

> **Important**
>
> Amazon EVS は、Amazon EVS 環境の作成後にのみカスタムルートテーブルの使用をサポートします。Amazon EVS 環境の作成中にカスタムルートテーブルを使用しないでください。接続に問題がある可能性があります。

ゲートウェイルートの要件

接続要件に基づいて、これらのゲートウェイタイプのルートを設定します。

- NAT ゲートウェイ (NGW)
  - アウトバウンドのみのインターネットアクセスのオプション。
  - インターネットゲートウェイにアクセスできるパブリックサブネットに存在する必要があります。
  - プライベートサブネットと EVS VLAN サブネットから NAT ゲートウェイにルートを追加します。
  - 詳細については、「Amazon VPC ユーザーガイド」の「NAT ゲートウェイの使用」を参照してください。
- トランジットゲートウェイ (TGW)
  - AWS Direct Connect と AWS Site-to-Site VPN の両方を介したオンプレミス接続に必要です。
  - オンプレミスネットワーク範囲のルートを追加します。
  - BGP を使用している場合は、ルート伝達を設定します。
  - 詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC トランジットゲートウェイ」を参照してください。

ベストプラクティス

- すべてのルートテーブル設定を文書化します。
- 一貫した命名規則を使用します。
- ルートテーブルを定期的に監査します。
- 変更後に接続をテストします。
- ルートテーブル設定をバックアップします。
- ルートのヘルスと伝播をモニタリングします。

ルートテーブルの操作の詳細については、「Amazon VPC ユーザーガイド」の「ルートテーブルの設定」を参照してください。

VPC の DHCP オプションセットを設定する

> **Important**
>
> これらの Amazon EVS 要件を満たしていない場合、環境のデプロイは失敗します。

- DHCP オプションセットにプライマリ DNS サーバーの IP アドレスとセカンダリ DNS サーバーの IP アドレスを含めます。
- デプロイに各 VCF 管理アプライアンスと Amazon EVS ホストの A レコードを含む DNS フォワードルックアップゾーンを含めます。
- デプロイ内の各 VCF 管理アプライアンスと Amazon EVS ホストの PTR レコードに DNS リバースルックアップゾーンを含めます。
- VPC のメインルートテーブルを設定して、DNS サーバーへのルートが存在することを確認します。
- ドメイン名登録が有効で有効期限が切れていないこと、および重複するホスト名や IP アドレスが存在しないことを確認します。
- Amazon EVS が以下と通信できるように、セキュリティグループとネットワークアクセスコントロールリスト (ACLs) を設定します。
  - TCP/UDP ポート 53 経由の DNS サーバー。
  - HTTPS および SSH 経由で管理 VLAN サブネットをホストします。
  - HTTPS および SSH 経由の管理 VLAN サブネット。

詳細については、「the section called “VPC DHCP オプションセットを使用して DNS サーバーと NTP サーバーを設定する”」を参照してください。

VPC Route Server インフラストラクチャの作成と設定

Amazon EVS は Amazon VPC Route Server を使用して、VPC アンダーレイネットワークへの BGP ベースの動的ルーティングを有効にします。サービスアクセスサブネット内の少なくとも 2 つのルートサーバーエンドポイントにルートを共有するルートサーバーを指定する必要があります。ルートサーバーピアに設定したピア ASN は一致している必要があり、ピア IP アドレスは一意である必要があります。

Important

VPC Route Server 設定の次の Amazon EVS 要件を満たしていない場合、環境のデプロイは失敗します。

- サービスアクセスサブネットには、少なくとも 2 つのルートサーバーエンドポイントを設定する必要があります。

- Tier-0 ゲートウェイのボーダーゲートウェイプロトコル (BGP) を設定する場合、VPC Route Server ピア ASN 値は NSX Edge ピア ASN 値と一致する必要があります。
- 2 つのルートサーバーピアを作成するときは、エンドポイントごとに NSX アップリンク VLAN の一意の IP アドレスを使用する必要があります。これらの 2 つの IP アドレスは、Amazon EVS 環境のデプロイ中に NSX エッジに割り当てられます。
- Route Server の伝播を有効にするときは、伝播されるすべてのルートテーブルに少なくとも 1 つの明示的なサブネットの関連付けがあることを確認する必要があります。伝播されたルートテーブルに明示的なサブネットの関連付けがない場合、BGP ルートアドバタイズは失敗します。

> **Note**
>
> Route Server ピアのライブネス検出の場合、Amazon EVS はデフォルトの BGP キープアライブメカニズムのみをサポートします。Amazon EVS は、マルチホップ双方向転送検出 (BFD) をサポートしていません。

前提条件

開始するには、以下が必要です。

- ルートサーバーの VPC サブネット。
- VPC Route Server リソースを管理するための IAM アクセス許可。
- ルートサーバーの BGP ASN 値 (Amazon 側の ASN)。この値は 1 ~ 4294967295 の範囲で指定する必要があります。
- NSX Tier-0 ゲートウェイとルートサーバーをピアリングするピア ASN。ルートサーバーと NSX Tier-0 ゲートウェイに入力されたピア ASN 値は一致する必要があります。NSX Edge アプライアンスのデフォルトの ASN は 65000 です。

Steps

VPC Route Server をセットアップする手順については、Route Server の開始方法チュートリアルを参照してください。

> **Note**
>
> NAT ゲートウェイまたはトランジットゲートウェイを使用している場合は、VPC ルートテーブル (複数可) に NSX ルートを伝達するようにルートサーバーが正しく設定されていることを確認します。

> **Note**
>
> ルートサーバーインスタンスの永続ルートを有効にし、永続期間を 1～5 分にすることをお勧めします。有効にすると、すべての BGP セッションが終了しても、ルートはルートサーバーのルーティングデータベースに保持されます。

> **Note**
>
> BGP 接続ステータスは、Amazon EVS 環境がデプロイされて動作するまでダウンします。

オンプレミス接続用のトランジットゲートウェイを作成する

関連付けられたトランジットゲートウェイ Direct Connect を使用するか、トランジットゲートウェイへの AWS Site-to-Site VPN アタッチメントを使用して、オンプレミスデータセンターの AWS インフラストラクチャへの接続を設定できます。詳細については、「the section called “オンプレミスネットワーク接続を設定する (オプション)”」を参照してください。

Amazon EC2 キャパシティ予約を作成する

Amazon EVS は、Amazon EVS 環境で ESX ホストを表す Amazon EC2 i4i.metal インスタンスを起動します。必要なときに十分な i4i.metal インスタンス容量を確保できるように、Amazon EC2 キャパシティ予約をリクエストすることをお勧めします。キャパシティ予約はいつでも作成でき、開始時期を選択できます。キャパシティ予約の即時使用をリクエストすることも、将来の日付のキャパシティ予約をリクエストすることもできます。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」のEC2 オンデマンドキャパシティ予約でコンピューティングキャパシティを予約する」を参照してください。

のセットアップ AWS CLI

AWS CLI は、Amazon EVS を含む AWS のサービスを操作するためのコマンドラインツールです。また、ローカルマシンから Amazon EVS 仮想化環境やその他の AWS リソースにアクセスするための IAM ユーザーまたはロールを認証するために使用されます。コマンドラインから AWS リソースをプロビジョニングするには、コマンドラインで使用する AWS アクセスキー ID とシークレットキーを取得する必要があります。次に、これらの認証情報を AWS CLIで設定する必要があります。詳細については、「 バージョン 2 用ユーザーガイド AWS CLI」の「 のセットアップ AWS Command Line Interface 」を参照してください。

Amazon EC2 キーペアを作成する

Amazon EVS は、環境の作成時に指定した Amazon EC2 キーペアを使用してホストに接続します。キーペアを作成するには、「 Amazon Elastic Compute Cloud ユーザーガイド」のAmazon EC2 「インスタンスのキーペアを作成する」の手順に従います。

VMware Cloud Foundation (VCF) 用の環境を準備する

Amazon EVS 環境をデプロイする前に、環境が VMware Cloud Foundation (VCF) インフラストラクチャ要件を満たしている必要があります。VCF の詳細な前提条件については、VMware Cloud Foundation 製品ドキュメントの「計画と準備ワークブック」を参照してください。

また、VPC 5.2.x の要件にも精通する必要があります。関連するリリース情報については、VPC 5.2.x リリースノートを参照してください。

> **Note**
>
> Amazon EVS が提供する VCF バージョンの詳細については、「」を参照してくださいthe section called “VCF バージョンと EC2 インスタンス”。

VCF ライセンスキーを取得する

Amazon EVS を使用するには、VPC ソリューションキーと vSAN ライセンスキーを提供する必要があります。VCF ソリューションキーには、少なくとも 256 コアが必要です。vSAN ライセンスキーには、少なくとも 110 TiB の vSAN 容量が必要です。VCF ライセンスの詳細については、VMware Cloud Foundation 管理ガイドの「VMware Cloud Foundation でのライセンスキーの管理」を参照してください。 VMware

Important

SDDC Manager ユーザーインターフェイスを使用して、VPC ソリューションと vSAN ライセンスキーを管理します。Amazon EVS では、サービスが正しく機能するためには、有効な VCF ソリューションと vSAN ライセンスキーを SDDC Manager に維持する必要があります。

Note

VCF ライセンスは、ライセンスコンプライアンスのためにすべての AWS リージョンで Amazon EVS で利用できます。Amazon EVS はライセンスキーを検証しません。ライセンスキーを検証するには、Broadcom サポートにアクセスしてください。

VMware HCX の前提条件

VMware HCX を使用して、既存の VMware ベースのワークロードを Amazon EVS に移行できます。Amazon EVS で VMware HCX を使用する前に、次の前提条件タスクが完了していることを確認してください。

Note

デフォルトでは、VMware HCX は EVS 環境にインストールされません。

- Amazon EVS で VMware HCX を使用する前に、最小限のネットワークアンダーレイ要件を満たす必要があります。詳細については、VMware HCX ユーザーガイドの「ネットワークアンダーレイの最小要件」を参照してください。
- VMware NSX が環境にインストールおよび設定されていることを確認します。詳細については、VMware NSX インストールガイドを参照してください。
- VMware HCX がアクティブ化され、環境にインストールされていることを確認します。VMware HCX のアクティブ化とインストールの詳細については、VMware HCX 入門ガイドのVMware HCX の開始方法」を参照してください。
- HCX インターネット接続が必要な場合は、次の前提条件タスクを完了する必要があります。
  - Amazon が提供する連続したパブリック IPv4 CIDR ブロックネットマスク長の IPAM クォータが /28 以上であることを確認します。

> **Important**
>
> HCX インターネット接続の場合、Amazon EVS はネットマスク長が /28 以上のパブリック IPAM プールから IPv4 CIDR ブロックを使用する必要があります。ネットマスク長が /28 未満の CIDR ブロックを使用すると、HCX 接続の問題が発生します。IPAM クォータの増加の詳細については、「IPAM のクォータ」を参照してください。

- 最小ネットマスク長が /28 の CIDR を持つ IPAM とパブリック IPv4 IPAM プールを作成します。
- HCX Manager および HCX Interconnect (HCX-IX) アプライアンスの IPAM プールから少なくとも 2 つの Elastic IP アドレス (EIPs) を割り当てます。デプロイする必要がある HCX ネットワークアプライアンスごとに追加の Elastic IP アドレスを割り当てます。
- パブリック IPv4 CIDR ブロックを追加の CIDR として VPC に追加します。

HCX のセットアップの詳細については、the section called “HCX 接続オプションを選択する”「」および「」を参照してくださいthe section called “HCX 接続オプション”。

Amazon EVS デプロイの前提条件チェックリスト

このセクションでは、Amazon EVS 環境のデプロイを成功させるために完了する必要がある前提条件のリストを示します。

VCF ライセンスキー情報

コンポーネント	説明	最小要件	値の例 (複数可)
サイト ID	Broadcom サポートポータルにアクセスするために Broadcom が提供するサイト ID。	EVS 環境作成リクエストで、Broadcom からのサイト ID を指定する必要があります。	01234567
VCF ソリューションキー	vSphere、NSX、SDDC Manager、vCenter Server など、VPC スタック全体の機能を	EVS 環境作成リクエストで有効なアクティブな VCF ソリューションキーを指定する必要があり	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

コンポーネント	説明	最小要件	値の例 (複数可)
	ロック解除する単一の VCF ライセンスキー。	ます。既存の EVS 環境でキーを既に使用することはできません。	
vSAN ライセンスキー	vSAN ライセンスキーを使用すると、vSAN ソフトウェアを VCF 環境内でアクティブ化して使用できます。	EVS 環境作成リクエストで有効なアクティブな vSAN ライセンスキーを指定する必要があります。既存の EVS 環境でキーを既に使用することはできません。	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS アカウントとリージョンの情報

コンポーネント	説明	最小要件	値の例 (複数可)
AWS アカウント ID 番号	AWS アカウントを使用すると、 AWS リソースを作成および管理し、 AWS サービスにアクセスできます。	AWS アカウントにアクセスできる必要があります。	999999999999
AWS リージョン	がアベイラビリティーゾーンと呼ばれる複数の独立したデータセンター AWS を維持する物理的な地理的エリア。	Amazon EVS がデプロイする AWS リージョンを指定する必要があります。Amazon EVS が現在利用可能なリージョンのリストについては、「 AWS 全般リファレンスガイド」の「Amazon Elastic	米国西部 (オレゴン)

コンポーネント	説明	最小要件	値の例 (複数可)
		VMware Service エンドポイントとクォータ」を参照してください。	

AWS オンプレミスデータセンター接続用の Transit Gateway

コンポーネント	説明	最小要件	値の例 (複数可)
Transit Gateway ID	トランジットゲートウェイは、VPC とオンプレミスネットワーク間を流れるトラフィックのリージョン仮想ルーターとして機能します。	Amazon EVS 環境をオンプレミスネットワークに接続するには、トランジットゲートウェイを使用する必要があります。	tgw-0262a0e521EXAMPLE
接続方法	オンプレミスネットワークを Amazon EVS 環境に接続するには、 AWS Direct Connect または AWS Site-to-Site VPN でトランジットゲートウェイを使用する必要があります。	AWS Direct Connect、 AWS Site-to-Site VPN、またはその両方の組み合わせを使用するかどうかを決定します。Direct Connect での Site-to-Site VPN の使用の詳細については、AWS 「Direct Connect での Private IP AWS Site-to-Site VPN」を参照してください。	AWS Direct Connect を使用した AWS Site-to-Site VPN

Amazon EVS 環境用の VPC

コンポーネント	説明	最小要件	値の例 (複数可)
VPC ID	VPC は、独自のデータセンターで運用する従来のネットワークによく似た仮想ネットワークです。	環境のデプロイには、任意の Amazon VPC を使用できます。	vpc-0abcdef1234567890
VPC CIDR ブロック	Amazon VPC では、CIDR ブロックは VPC 内で使用可能な IP アドレスの範囲を定義します。	最小サイズが /22 ネットマスクの RFC 1918 CIDR ブロック。VPC CIDR ブロックは、VPC にデプロイされるすべての EVS サブネットとホストに対応するように適切なサイズにする必要があります。この CIDR ブロックは、環境全体で一意である必要があります。	10.1.0.0/20

EVS 環境の VPC サブネット

コンポーネント	説明	最小要件	値の例 (複数可)
サービスアクセスサブネット ID	サービスアクセスサブネットは、Amazon EVS サービスアクセスを有効にする標準の VPC サブネットです。詳細については、「the section called “サービスアク	サブネットが VPC 内で適切なサイズであれば、任意の VPC サブネットを使用できます。ネットマスクが /24 の VPC サブネット CIDR ブロッ	subnet-abcdef1234567890e

コンポーネント	説明	最小要件	値の例 (複数可)
	セスサブネット”」を参照してください。	クを指定することをお勧めします。	
サービスアクセスサブネット CIDR	VPC サブネット CIDR ブロックは、IP アドレスの範囲であり、CIDR 表記を使用して定義され、VPC 内の特定のサブネットに割り当てられます。	サービスアクセスサブネットは、VPC にデプロイされる他の EVS サブネットとホストにも対応できるように適切なサイズにする必要があります。ネットマスクが /24 の VPC サブネット CIDR ブロックを指定することをお勧めします。	10.1.0.0/24
AWS リージョン内のアベイラビリティーゾーン ID	AWS リージョン内の個別の場所。他の AZs の障害から分離されるように設計されており、1 つ以上のデータセンターで構成されています。	サブネットの作成時に VPC サブネットがデプロイするアベイラビリティーゾーンを指定できます。詳細については、「Amazon VPC ユーザーガイド」の「サブネットを作成する」を参照してください。	us-west-2a

EVS 環境の EVS VLAN サブネット

コンポーネント	説明	最小要件	値の例 (複数可)
ホスト管理 VLAN CIDR	ホスト管理 VLAN サブネットの CIDR ブロック。詳細につい	最小サイズは /28 ネットマスク、最大サイズは /24 ネットマス	10.1.1.0/24

コンポーネント	説明	最小要件	値の例 (複数可)
	ては、「the section called “ホスト管理 VLAN サブネット”」を参照してください。	クである必要があります。VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。	
vMotion VLAN CIDR	vMotion VLAN サブネットの CIDR ブロック。詳細については、「the section called “vMotion VLAN サブネット”」を参照してください。	ホスト管理 VLAN と同じサイズである必要があります。	10.1.2.0/24
vSAN VLAN CIDR	vSAN VLAN サブネットの CIDR ブロック。詳細については、「the section called “vSAN VLAN サブネット”」を参照してください。	ホスト管理 VLAN と同じサイズである必要があります。	10.1.3.0/24
VTEP VLAN CIDR	VTEP VLAN サブネットの CIDR ブロック。詳細については、「the section called “VTEP VLAN サブネット”」を参照してください。	ホスト管理 VLAN と同じサイズである必要があります。	10.1.4.0/24

コンポーネント	説明	最小要件	値の例 (複数可)
Edge VTEP VLAN CIDR	エッジ VTEP VLAN サブネットの CIDR ブロック。詳細については、「the section called “Edge VTEP VLAN サブネット”」を参照してください。	最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。	10.1.5.0/24
管理 VM VLAN CIDR	Management VM VLAN サブネットの CIDR ブロック。詳細については、「the section called “Management VM VLAN サブネット”」を参照してください。	最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。	10.1.6.0/24
HCX アップリンク VLAN CIDR	HCX アップリンク VLAN サブネットの CIDR ブロック。詳細については、「the section called “HCX アップリンク VLAN サブネット”」を参照してください。	最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。	10.1.7.0/24

コンポーネント	説明	最小要件	値の例 (複数可)
NSX アップリンク VLAN CIDR	NSX アップリンク VLAN サブネットの CIDR ブロック。詳細については、「the section called “NSX アップリンク VLAN サブネット”」を参照してください。	最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。	10.1.8.0/24
拡張 VLAN 1 CIDR	拡張 VLAN サブネットの CIDR ブロック。詳細については、「the section called “拡張 VLAN サブネット”」を参照してください。	最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。	10.1.9.0/24
拡張 VLAN 2 CIDR	拡張 VLAN サブネットの CIDR ブロック。詳細については、「the section called “拡張 VLAN サブネット”」を参照してください。	最小サイズは /28 ネットマスク、最大サイズは /24 ネットマスクである必要があります。VPC に関連付けられている既存の CIDR ブロックと重複してはいけません。	10.1.10.0/24

DNS および NTP インフラストラクチャ

コンポーネント	説明	最小要件	値の例 (複数可)
プライマリ DNS サーバーの IP アドレス	ドメインのすべての DNS レコードの信頼できるソースとして使用されるメインド	使用可能なホスト範囲内で、有効で未使用の IPv4 アドレスを使用できます。	10.1.1.10

コンポーネント	説明	最小要件	値の例 (複数可)
	メインネームシステム (DNS) サーバー。		
セカンダリ DNS サーバーの IP アドレス	ドメインの DNS レコードのバックアップ DNS サーバー。	使用可能なホスト範囲内で、有効で未使用の IPv4 アドレスを使用できます。	10.1.5.25
NTP サーバーの IP アドレス	ネットワークタイムプロトコル (NTP) サーバーは、NTP 標準を使用してネットワーク内のクロックを同期するデバイスまたはアプリケーションです。	デフォルトの Amazon Time Sync Service は、ローカル `169.254.169.123` IP アドレス、または別の NTP サーバー IP アドレスで使用できます。	169.254.169.123 (Amazon Time Sync Service)
VCF デプロイ用の FQDN	完全修飾ドメイン名 (FQDN) は、ネットワーク上のデバイスの絶対名です。FQDN はホスト名とドメイン名で構成されます。	FQDN に含めることができるのは、英数字、マイナス記号 (-)、およびラベル間の区切り文字として使用されるピリオドのみです。有効で有効期限が切れていない一意の FQDN である必要があります。	evs.local

VPC DHCP オプションセット

コンポーネント	説明	最小要件	値の例 (複数可)
DHCP オプションセット ID	DHCP オプションセットは、EC2 インスタンスなど、VPC 内のリソースが仮想	最低 2 つの DNS サーバーを含める必要があります。Route 53 またはカスタム DNS	dopt-0a1b2c3d

コンポーネント	説明	最小要件	値の例 (複数可)
	ネットワーク経由で通信するために使用するネットワーク設定のグループです。	サーバーを使用できます。また、DNS ドメイン名と NTP サーバーを含める必要があります。	

EC2 キーペア

コンポーネント	説明	最小要件	値の例 (複数可)
EC2 キーペア名	EC2 キーペアは、Amazon EC2 インスタンスに安全に接続するために使用される一連のセキュリティ認証情報です。	キーペア名は一意である必要があります。	`my-ec2-key-pair`

VPC ルートテーブル

コンポーネント	説明	最小要件	値の例 (複数可)
メインルートテーブル ID	Amazon VPC では、メインルートテーブルは VPC で自動的に作成されるデフォルトのルートテーブルであり、別のルートテーブルに明示的に関連付けられていない VPC サブネットのトラフィックを管理します。EVS VLAN サブネットは、Amazon EVS が作成する	環境のデプロイを成功させるには、DNS やオンプレミスシステムなどの依存サービスへの接続を有効にするように設定する必要があります。	rtb-0123456789abcdef0

コンポーネント	説明	最小要件	値の例 (複数可)
	ときに VPC のメインルートテーブルに暗黙的に関連付けられます。		

ネットワークアクセスコントロールリスト (ACL)

コンポーネント	説明	最小要件	値の例 (複数可)
ネットワーク ACL ID	ネットワークアクセスコントロールリスト (ACL) は、サブネットレベルでインバウンドトラフィックまたはアウトバウンドトラフィックを許可または拒否します。	Amazon EVS が以下と通信できるようにする必要があります。 • TCP/UDP ポート 53 経由の DNS サーバー。 • HTTPS および SSH 経由で管理 VLAN サブネットをホストします。 • HTTPS および SSH 経由の管理 VM VLAN サブネット。	acl-0f62c640e793a38a3

VCF コンポーネントの DNS レコード

コンポーネント	説明	最小要件	IP アドレスの例	ホスト名の例
ESX ホスト 1	ESX ホスト 1 の A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、各 EVS デプロ	10.1.0.10	esxi01

コンポーネント	説明	最小要件	IP アドレスの例	ホスト名の例
		イの各 ESX ホスト用に作成された PTR レコードを含むリバースルックアップゾーンが必要です。		
ESX ホスト 2	ESX ホスト 2 の A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、各 EVS デプロイの各 ESX ホスト用に作成された PTR レコードを含むリバースルックアップゾーンが必要です。	10.1.0.11	esxi02
ESX ホスト 3	ESX ホスト 3 の A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、各 EVS デプロイの各 ESX ホスト用に作成された PTR レコードを含むリバースルックアップゾーンが必要です。	10.1.0.12	esxi03

コンポーネント	説明	最小要件	IP アドレスの例	ホスト名の例
ESX ホスト 4	ESX ホスト 4 の A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、各 EVS デプロイの各 ESX ホスト用に作成された PTR レコードを含むリバースルックアップゾーンが必要です。	10.1.0.13	esxi04
vCenter Server アプライアンス	vCenter Server アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを含むリバースルックアップゾーンが必要です。	10.1.5.10	vc01

コンポーネント	説明	最小要件	IP アドレスの例	ホスト名の例
NSX Manager クラスター	NSX Manager クラスターの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを含むリバースルックアップゾーンが必要です。	10.1.5.11	nsx
SDDC Manager アプライアンス	SDDC Manager アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを含むリバースルックアップゾーンが必要です。	10.1.5.12	sddcm01

コンポーネント	説明	最小要件	IP アドレスの例	ホスト名の例
Cloud Builder アプライアンス	Cloud Builder アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを含む DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを含むリバースルックアップゾーンが必要です。	10.1.5.13	cb01
NSX Edge 1 アプライアンス	NSX Edge 1 アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを持つ DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを持つリバースルックアップゾーンが必要です。	10.1.5.14	edge01

コンポーネント	説明	最小要件	IP アドレスの例	ホスト名の例
NSX Edge 2 アプライアンス	NSX Edge 2 アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを持つ DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを持つリバースルックアップゾーンが必要です。	10.1.5.15	edge02
NSX Manager 1 アプライアンス	NSX Manager 1 アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを持つ DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを持つリバースルックアップゾーンが必要です。	10.1.5.16	nsx01

コンポーネント	説明	最小要件	IP アドレスの例	ホスト名の例
NSX Manager 2 アプライアンス	NSX Manager 2 アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを持つ DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを持つリバースルックアップゾーンが必要です。	10.1.5.17	nsx02
NSX Manager 3 アプライアンス	NSX Manager 3 アプライアンスの A レコードと PTR レコードで定義されている IP アドレスとホスト名。	Amazon EVS には、A レコードを持つ DNS フォワードルックアップゾーンと、EVS デプロイごとに VCF 管理アプライアンスごとに作成された PTR レコードを持つリバースルックアップゾーンが必要です。	10.1.5.18	nsx03

VPC Route Server インフラストラクチャ

コンポーネント	説明	最小要件	値の例 (複数可)
サーバー ID をルーティングする	Amazon EVS は Amazon VPC Route Server を使用して、VPC アンダーレイネットワークへの BGP ベースの動的ルーティングを有効にします。	サービスアクセスサブネット内の少なくとも 2 つのルートサーバーエンドポイントにルートを共有するルートサーバーを指定する必要があります。ルートサーバーで設定されたピア ASN と NSX Edge ピアは一致する必要があり、ピア IP アドレスは一意である必要があります。	rs-0a1b2c3d4e5f67890
ルートサーバーの関連付け	ルートサーバーと VPC 間の接続。	ルートサーバーは VPC に関連付ける必要があります。	{ "RouteServerAssociation": { "RouteServerId": "rs-0a1b2c3d4e5f67890", "VpcId": "vpc-1", "State": "associating" } }
VPC Route Server 側の BGP ASN (Amazon 側の ASN)	Amazon 側の ASN は、VPC ルートサーバーと NSX Edge ピア間の BGP セッション AWS の側面を表し	この値は一意でなければならず、範囲は 1-4294967295 です。AWS 64512 ~ 65534 (16 ビット ASN) ま	65001

コンポーネント	説明	最小要件	値の例 (複数可)
	ます。この BGP ASN は、ルートサーバーの作成時に指定します。詳細については、「Amazon VPC ユーザーガイド」の「ルートサーバーの作成」を参照してください。	たは 4200000000 ~ 4294967294 (32 ビット ASN) のプライベート ASN を使用することをお勧めします。	
ルートサーバーエンドポイント 1 ID	ルートサーバーエンドポイントは、ルートサーバーと BGP ピア間の BGP (ボーダーゲートウェイプロトコル) 接続を容易にするサブネット内の AWSマネージドコンポーネントです。	ルートサーバーエンドポイントをサービスアクセスサブネットにデプロイする必要があります。	rse-0123456789abcdef0
ルートサーバーピア 1 ID	ルートサーバーピアは、ルートサーバーエンドポイントと AWS (NSX Edge) にデプロイされたデバイス間の BGP ピアリングセッションです。	ルートサーバーピアで指定されたピア ASN 値は、NSX Edge Tier-0 ゲートウェイに使用されるピア ASN 値と一致する必要があります。	rsp-0123456789abcdef0

コンポーネント	説明	最小要件	値の例 (複数可)
ルートサーバーピア 1 IP アドレス (EVS NSX Edge 1 側)	ルートサーバーピアの IP アドレス (`PeerAddress`)。	NSX アップリンク VLAN から一意の未使用の IP アドレスを使用する必要があります。Amazon EVS は、デプロイの一部としてこの IP アドレスを NSX Edge 1 に適用し、ルートサーバーエンドポイントピアとピア接続します。	10.1.7.10
ルートサーバーピア 1 エンドポイント ENI アドレス	ルートサーバーピア () のエンドポイント ENI IP アドレス`EndpointEniAddress` 。	ピア作成時にルートサーバーによって自動的に生成されます。	10.1.7.11
ルートサーバーエンドポイント 2 ID	ルートサーバーエンドポイントは、ルートサーバーと BGP ピア間の BGP (ボーダーゲートウェイプロトコル) 接続を容易にするサブネット内の AWSマネージドコンポーネントです。	ルートサーバーエンドポイントをサービスアクセスサブネットにデプロイする必要があります。	rse-fedcba9876543210f

コンポーネント	説明	最小要件	値の例 (複数可)
ルートサーバーピア 2 ID (EVS NSX Edge 2 側)	ルートサーバーピアは、ルートサーバーエンドポイントと AWS (NSX Edge) にデプロイされたデバイス間の BGP ピアリングセッションです。	ルートサーバーピアで指定されたピア ASN 値は、NSX Edge Tier-0 ゲートウェイに使用されるピア ASN 値と一致する必要があります。	rsp-fedcba9876543210f
ルートサーバーピア 2 IP アドレス	ルートサーバーピアの IP アドレス (`PeerAddress`)。	NSX アップリンク VLAN の一意の IP アドレスを使用する必要があります。Amazon EVS は、デプロイの一部としてこの IP アドレスを NSX Edge 2 に適用し、ルートサーバーエンドポイントピアとピア接続します。	10.1.7.200
ルートサーバーピア 2 エンドポイント ENI アドレス	ルートサーバーピア () のエンドポイント ENI IP アドレス`EndpointEniAddress` 。	ピア作成時にルートサーバーによって自動的に生成されます。	10.1.7.201

コンポーネント	説明	最小要件	値の例 (複数可)

ルートサーバーの伝播	ルートサーバーの伝播は、指定したルートテーブルの FIB にルートをインストールします。	サービスアクセスサブネットに関連付けられたルートテーブルを指定する必要があります。Amazon EVS は、現時点では IPv4 ネットワークのみをサポートしています。	<pre>{
			"RouteServerEndpoint": {
			"RouteServerId": "rs-1",
			"RouteServerEndpointId": "rse-1",
			"VpcId": "vpc-1",
			"SubnetId": "subnet-1",
			"State": "pending"
			}
			}</pre>

NSX ピア側の BGP ASN	接続の NSX 側の BGP ASN。	NSX デフォルト ASN 65000 の使用を提案する	65000

HCX インターネットアクセスリソース (オプション)

コンポーネント	説明	最小要件	値の例 (複数可)
IPAM ID	HCX インターネットアクセスの IP アドレスを管理するために使用される Amazon VPC IP Address Manager (IPAM)。	パブリック IPv4 アドレスを提供するように設定する必要があります。HCX インターネットアクセス設定にのみ必要です。	ipam-0123456789abcdef0
IPAM プール ID	HCX コンポーネントのアドレスを提供する Amazon 所有のパ	パブリック IPv4 プールとして設定する必要があります。HCX インターネットアク	ipam-pool-0123456789abcdef0

コンポーネント	説明	最小要件	値の例 (複数可)
	ブリック IPv4 IPAM プール。	セス設定にのみ必要です。	
HCX パブリック VLAN CIDR ブロック	HCX パブリック VLAN サブネットの IPAM プールから割り当てられたセカンダリパブリック IPv4 CIDR ブロック。	/28 ネットマスクが必要で、Amazon 所有の IPAM パブリックプールから割り当てる必要があります。HCX インターネットアクセス設定にのみ必要です。	18.97.137.0/28
Elastic IP アドレス	HCX コンポーネントの IPAM プールから割り当てられた順次 Elastic IP アドレス。	HCX Manager、HCX Interconnect Appliance (HCX-IX)、HCX Network Extension (HCX-NE) の同じ IPAM プールから最低 3 つの EIPs。HCX インターネットアクセス設定にのみ必要です。	eipalloc-0123456789abcdef0、eipalloc-0123456789abcdef1、eipalloc-0123456789abcdef2

Amazon Elastic VMware Service の開始方法

このガイドを使用して、Amazon Elastic VMware Service (Amazon EVS) の使用を開始します。独自の Amazon Virtual Private Cloud (VPC) 内にホストを持つ Amazon EVS 環境を作成する方法について説明します。

完了すると、VMware vSphere ベースのワークロードを に移行するために使用できる Amazon EVS 環境が作成されます AWS クラウド。

Important

このトピックでは、できるだけ簡単かつ迅速に開始するために、VPC を作成する手順と、DNS サーバー設定と Amazon EVS 環境作成の最小要件について説明します。これらのリソースを作成する前に、要件を満たす IP アドレス空間と DNS レコードのセットアップを計画することをお勧めします。VCF 5.2.x の要件にも精通する必要があります。関連するリリース情報については、VPC 5.2.x リリースノートを参照してください。

Important

Amazon EVS が提供する VCF バージョンの詳細については、「」を参照してくださいthe section called “VCF バージョンと EC2 インスタンス”。

トピック

- VCF 認証情報を取得して VCF 管理アプライアンスにアクセスする
- クリーンアップ
- 次の手順

前提条件

開始する前に、Amazon EVS の前提条件タスクを完了する必要があります。詳細については、「Amazon Elastic VMware Service のセットアップ」を参照してください。

サブネットとルートテーブルを使用して VPC を作成する

> **Note**
>
> VPC、サブネット、Amazon EVS 環境はすべて同じアカウントで作成する必要があります。Amazon EVS は、VPC サブネットまたは Amazon EVS 環境のクロスアカウント共有をサポートしていません。

Example

Amazon VPC console

1. Amazon VPC コンソール を開きます。
2. VPC ダッシュボードで、[Create VPC (VPC を作成する)] を選択します。
3. [Resources to create] (作成するリソース) で、[VPC and more] (VPC など) を選択します。
4. [名前タグの自動生成] を選択したままにすると VPC リソース用の名前タグが作成され、オフにすると VPC リソース用の独自の名前タグが作成されます。
5. IPv4 CIDR ブロックの場合は、IPv4 CIDR ブロックを入力します。VPC には IPv4 CIDR ブロックが必要です。Amazon EVS サブネットに対応する適切なサイズの VPC を作成してください。詳細については、「the section called “Amazon EVS ネットワークに関する考慮事項”」を参照してください。

   > **Note**
   >
   > Amazon EVS は現在 IPv6 をサポートしていません。

6. テナンシーを のままにしますDefault。このオプションを選択すると、この VPC で起動される EC2 インスタンスは、インスタンスの起動時に指定されたテナンシー属性を使用します。Amazon EVS は、ユーザーに代わってベアメタル EC2 インスタンスを起動します。
7. [Number of Availability Zones (AZs)] (アベイラビリティゾーンの数 (AZ)) には、[1] を選択します。

> **Note**
>
> Amazon EVS は、現時点ではシングル AZ 配置のみをサポートしています。

8. AZs をカスタマイズ を展開し、サブネットの AZ を選択します。

> **Note**
>
> Amazon EVS がサポートされている AWS リージョンにデプロイする必要があります。Amazon EVS リージョンの可用性の詳細については、「 AWS 全般リファレンスガイド」の「Amazon Elastic VMware Service エンドポイントとクォータ」を参照してください。

9. (オプション) インターネット接続が必要な場合は、パブリックサブネットの数で 1 を選択します。
10. プライベートサブネットの数 で、1 を選択します。このプライベートサブネットは、環境の作成ステップ中に Amazon EVS に提供したサービスアクセスサブネットとして使用されます。詳細については、「the section called “サービスアクセスサブネット”」を参照してください。
11. サブネットの IP アドレス範囲を選択するには、[サブネット CIDR ブロックをカスタマイズ] を展開します。

> **Note**
>
> Amazon EVS VLAN サブネットも、この VPC CIDR スペースから作成する必要があります。サービスが必要とする VLAN サブネットに十分なスペースを VPC CIDR ブロックに残してください。詳細については、the section called “Amazon EVS ネットワークに関する考慮事項”を参照してください。

12. (オプション) IPv4 経由のインターネットアクセスをリソースに付与するには、NAT ゲートウェイで「In 1 AZ」を選択します。NAT ゲートウェイにはコストが発生することに注意してください。詳細については、「NAT ゲートウェイの料金」を参照してください。

> **Note**
>
> Amazon EVS では、アウトバウンドインターネット接続を有効にするために NAT ゲートウェイを使用する必要があります。

13[VPC エンドポイント] には、[なし] を選択します。

> **Note**
>
> Amazon EVS は Amazon S3 、現時点では のゲートウェイ VPC エンドポイントをサポートしていません。 Amazon S3 接続を有効にするには、 AWS PrivateLink を使用してインターフェイス VPC エンドポイントを設定する必要があります Amazon S3。詳細については、「Amazon Simple Storage Service ユーザーガイド」のAWS PrivateLink 「 の Amazon S3 」を参照してください。

14DNS オプションの場合は、デフォルトを選択したままにします。Amazon EVS では、VPC にすべての VCF コンポーネントの DNS 解決機能が必要です。

15(オプション) VPC にタグを追加するには、[追加のタグ] を展開して、[新しいタグを追加] を選択し、タグキーとタグ値を入力します。

16[Create VPC (VPC の作成)] を選択します。

> **Note**
>
> VPC の作成中に、 はメインルートテーブル Amazon VPC を自動的に作成し、デフォルトでサブネットを暗黙的に関連付けます。

AWS CLI

1. ターミナルセッションを開きます。
2. 1 つのアベイラビリティーゾーンにプライベートサブネットとオプションのパブリックサブネットを持つ VPC を作成します。

```
aws ec2 create-vpc \
  --cidr-block 10.0.0.0/16 \
  --instance-tenancy default \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=evs-vpc}]'
```

```
---
. Store the VPC ID for use in subsequent commands.
+
[source,bash]
```

VPC_ID=$(aws ec2 describe-vpcs \ --filters Name=tag:Name,Values=evs-vpc \ --query 'Vpcs[0]。VpcId' \ --output text) ---

3. DNS ホスト名と DNS サポートを有効にします。

```
aws ec2 modify-vpc-attribute \
  --vpc-id $VPC_ID \
  --enable-dns-hostnames
aws ec2 modify-vpc-attribute \
  --vpc-id $VPC_ID \
  --enable-dns-support
```

4. VPC にプライベートサブネットを作成します。

```
aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-west-2a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=evs-private-
subnet}]'
```

5. 後続のコマンドで使用するプライベートサブネット ID を保存します。

```
PRIVATE_SUBNET_ID=$(aws ec2 describe-subnets \
  --filters Name=tag:Name,Values=evs-private-subnet \
  --query 'Subnets[0].SubnetId' \
  --output text)
```

6. (オプション) インターネット接続が必要な場合は、パブリックサブネットを作成します。

```
aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-west-2a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=evs-public-
subnet}]'
```

7. (オプション) 後続のコマンドで使用するパブリックサブネット ID を保存します。

```
PUBLIC_SUBNET_ID=$(aws ec2 describe-subnets \
  --filters Name=tag:Name,Values=evs-public-subnet \
  --query 'Subnets[0].SubnetId' \
  --output text)
```

8. (オプション) パブリックサブネットが作成されている場合は、インターネットゲートウェイを作成してアタッチします。

```
aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=evs-
igw}]'

IGW_ID=$(aws ec2 describe-internet-gateways \
  --filters Name=tag:Name,Values=evs-igw \
  --query 'InternetGateways[0].InternetGatewayId' \
  --output text)

aws ec2 attach-internet-gateway \
  --vpc-id $VPC_ID \
  --internet-gateway-id $IGW_ID
```

9. (オプション) インターネット接続が必要な場合は、NAT ゲートウェイを作成します。

```
aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-nat-
eip}]'

EIP_ID=$(aws ec2 describe-addresses \
  --filters Name=tag:Name,Values=evs-nat-eip \
  --query 'Addresses[0].AllocationId' \
  --output text)

aws ec2 create-nat-gateway \
  --subnet-id $PUBLIC_SUBNET_ID \
  --allocation-id $EIP_ID \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=evs-nat}]'
```

10必要なルートテーブルを作成して設定します。

```
aws ec2 create-route-table \
  --vpc-id $VPC_ID \
```

```
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=evs-
private-rt}]'

PRIVATE_RT_ID=$(aws ec2 describe-route-tables \
  --filters Name=tag:Name,Values=evs-private-rt \
  --query 'RouteTables[0].RouteTableId' \
  --output text)

aws ec2 create-route-table \
  --vpc-id $VPC_ID \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=evs-public-
rt}]'

PUBLIC_RT_ID=$(aws ec2 describe-route-tables \
  --filters Name=tag:Name,Values=evs-public-rt \
  --query 'RouteTables[0].RouteTableId' \
  --output text)
```

11必要なルートをルートテーブルに追加します。

```
aws ec2 create-route \
  --route-table-id $PUBLIC_RT_ID \
  --destination-cidr-block 0.0.0.0/0 \
  --gateway-id $IGW_ID

aws ec2 create-route \
  --route-table-id $PRIVATE_RT_ID \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id $NAT_GW_ID
```

12ルートテーブルをサブネットに関連付けます。

```
aws ec2 associate-route-table \
  --route-table-id $PRIVATE_RT_ID \
  --subnet-id $PRIVATE_SUBNET_ID

aws ec2 associate-route-table \
  --route-table-id $PUBLIC_RT_ID \
  --subnet-id $PUBLIC_SUBNET_ID
```

> **Note**
>
> VPC の作成中に、 はメインルートテーブル Amazon VPC を自動的に作成し、デフォルトでサブネットを暗黙的に関連付けます。

HCX 接続オプションを選択する

Amazon EVS 環境の接続オプションを 1 つ選択します。

- プライベート接続: HCX の高性能ネットワークパスを提供し、信頼性と一貫性を最適化します。外部ネットワーク接続には AWS Direct Connect または Site-to-Site VPN を使用する必要があります。
- インターネット接続: パブリックインターネットを使用して、設定が簡単な柔軟な移行パスを確立します。VPC IP Address Manager (IPAM) と Elastic IP アドレスを使用する必要があります。

詳細な分析については、「」を参照してくださいthe section called “HCX 接続オプション”。

オプションを選択します。

- オプション A: プライベート接続のみ → に進みますthe section called “VPC メインルートテーブルを設定する”。
- オプション B: インターネット接続 → に進みますthe section called “HCX インターネット接続のセットアップ”。

HCX インターネット接続のセットアップ

> **Note**
>
> HCX プライベート接続を選択した場合は、このセクションをスキップして に進みますthe section called “VPC メインルートテーブルを設定する”。

Amazon EVS の HCX インターネット接続を有効にするには、以下を実行する必要があります。

- Amazon が提供する連続したパブリック IPv4 CIDR ブロックネットマスク長の VPC IP Address Manager (IPAM) クォータが /28 以上であることを確認します。

> **Important**
>
> Amazon が提供する連続したパブリック IPv4 CIDR ブロックをネットマスク長 /28 未満で使用すると、HCX 接続の問題が発生します。IPAM クォータの増加の詳細については、「IPAM のクォータ」を参照してください。

- 最小ネットマスク長が /28 の CIDR を持つ IPAM とパブリック IPv4 IPAM プールを作成します。
- HCX Manager および HCX Interconnect (HCX-IX) アプライアンスの IPAM プールから少なくとも 2 つの Elastic IP アドレス (EIPs) を割り当てます。デプロイする必要がある HCX ネットワークアプライアンスごとに追加の Elastic IP アドレスを割り当てます。
- パブリック IPv4 CIDR ブロックを追加の CIDR として VPC に追加します。

環境作成後の HCX インターネット接続の管理の詳細については、「」を参照してくださいthe section called “HCX パブリック接続”。

IPAM を作成する

IPAM を作成するには、次の手順に従います。

> **Note**
>
> IPAM 無料利用枠を使用して、Amazon EVS で使用する IPAM リソースを作成できます。IPAM 自体は無料利用枠で無料ですが、NAT ゲートウェイや無料利用枠の制限を超えるパブリック IPv4 アドレスなど、IPAM と組み合わせて使用される他の AWS サービスのコストはお客様の負担となります。IPAM 料金の詳細については、Amazon VPC 料金表ページを参照してください。

> **Note**
>
> Amazon EVS は、現時点ではプライベート IPv6 グローバルユニキャストアドレス (GUA) CIDRs をサポートしていません。

パブリック IPv4 IPAM プールを作成する

パブリック IPv4 プールを作成するには、次の手順に従います。

IPAM console

1. IPAM コンソールを開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. パブリックスコープを選択します。スコープの詳細については、「IPAM の仕組み」を参照してください。
4. [プールを作成] を選択します。
5. (オプション) プールの [名前タグ] とプールの [説明] を追加します。
6. [アドレスファミリー] には [IPv4] を選択します。
7. [リソース計画] で、[範囲内のIP 空間計画] は選択したままにしておきます。
8. [Locale] (ロケール) で、プールのロケールを選択します。ロケールは、この IPAM プールを割り当てに使用できる AWS リージョンです。選択したロケールは、VPC がデプロイされている AWS リージョンと一致する必要があります。
9. [Service] (サービス) で、[EC2 (EIP/VPC)] を選択します。これにより、このプールから Amazon EC2 サービス (Elastic IP アドレス) に割り当てられた CIDRs がアドバタイズされます。
10. [パブリック IP ソース] で、[Amazon 所有] を選択します。
11. プロビジョニングする CIDRs、Amazon 所有のパブリック CIDR の追加を選択します。
12. Netmask で CIDR ネットマスクの長さを選択します。/28 は必要な最小ネットマスク長です。
13. [プールを作成] を選択します。

AWS CLI

1. ターミナルセッションを開きます。
2. IPAM からパブリックスコープ ID を取得します。

```
SCOPE_ID=$(aws ec2 describe-ipam-scopes \
  --filters Name=ipam-scope-type,Values=public \
  --query 'IpamScopes[0].IpamScopeId' \
  --output text)
```

3. パブリックスコープに IPAM プールを作成します。

```
aws ec2 create-ipam-pool \
  --ipam-scope-id $SCOPE_ID \
  --address-family ipv4 \
```

```
  --no-auto-import \
  --locale us-east-2 \
  --description "Public IPv4 pool for HCX" \
  --tag-specifications 'ResourceType=ipam-pool,Tags=[{Key=Name,Value=evs-hcx-
public-pool}]' \
  --public-ip-source amazon \
  --aws-service ec2
```

4. 後続のコマンドで使用するプール ID を保存します。

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)
```

5. 最小ネットマスク長が /28 の CIDR ブロックをプールからプロビジョニングします。

```
aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id $POOL_ID \
  --netmask-length 28
```

IPAM プールから Elastic IP アドレスを割り当てる

HCX Service Mesh アプライアンスの IPAM プールから Elastic IP アドレス (EIPs) を割り当てるには、次の手順に従います。

Amazon VPC console

1. Amazon VPC コンソール を開きます。
2. ナビゲーションペインで [Elastic IP] を選択します。
3. [Elastic IP アドレスの割り当て] を選択してください。
4. IPv4 IPAM プールを使用して割り当てるを選択します。
5. 以前に設定した Amazon 所有のパブリック IPv4 プールを選択します。
6. IPAM メソッドの割り当てで、IPAM プール内のアドレスを手動で入力を選択します。

> **Important**
>
> 最初の 2 つの EIPsまたはパブリック IPAM CIDR ブロックからの最後の EIP を VLAN サブネットに関連付けることはできません。これらの EIPsは、ネットワーク、デフォ

ルトゲートウェイ、ブロードキャストアドレスとして予約されています。これらの EIPs を VLAN サブネットに関連付けると、Amazon EVS は検証エラーをスローします。

> **Important**
>
> Amazon EVS が予約する EIPs が割り当てられないように、IPAM プール内にアドレスを手動で入力します。IPAM に EIP の選択を許可すると、IPAM は Amazon EVS が予約する EIP を割り当て、VLAN サブネットへの EIP の関連付け中に障害が発生する可能性があります。

7. IPAM プールから割り当てる EIP を指定します。
8. [割り当て] を選択してください。
9. このプロセスを繰り返して、必要な残りの EIPsを割り当てます。HCX Manager および HCX Interconnect (HCX-IX) アプライアンスには、IPAM プールから少なくとも 2 つの EIPs を割り当てる必要があります。デプロイする必要がある HCX ネットワークアプライアンスごとに追加の EIP を割り当てます。

AWS CLI

1. ターミナルセッションを開きます。
2. 前に作成した IPAM プール ID を取得します。

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)
```

3. IPAM プールから Elastic IP アドレスを割り当てます。HCX Manager および HCX Interconnect (HCX-IX) アプライアンスには、IPAM プールから少なくとも 2 つの EIPs を割り当てる必要があります。デプロイする必要がある HCX ネットワークアプライアンスごとに追加の EIP を割り当てます。

> **Important**
>
> パブリック IPAM CIDR ブロックの最初の 2 つの EIPs または最後の EIP を VLAN サブネットに関連付けることはできません。これらの EIPsは、ネットワーク、デフォルトゲートウェイ、ブロードキャストアドレスとして予約されています。これらの EIPs を VLAN サブネットに関連付けると、Amazon EVS は検証エラーをスローします。

> **Important**
>
> Amazon EVS が予約する EIPs が割り当てられないように、IPAM プール内にアドレスを手動で入力します。IPAM に EIP の選択を許可すると、IPAM は Amazon EVS が予約する EIP を割り当て、VLAN サブネットへの EIP の関連付け中に障害が発生する可能性があります。

```
aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-
manager-eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.3

aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-ix-
eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.4

aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-ne-
eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.5
```

IPAM プールから HCX インターネット接続用の VPC にパブリック IPv4 CIDR ブロックを追加する

HCX インターネット接続を有効にするには、IPAM プールから VPC にパブリック IPv4 CIDR ブロックを追加 CIDR として追加する必要があります。Amazon EVS は、この CIDR ブロックを使用して VMware HCX をネットワークに接続します。CIDR ブロックを VPC に追加するには、次の手順に従います。

> **Important**
>
> VPC に追加する IPv4 CIDR ブロックを手動で入力する必要があります。Amazon EVS は、現時点では IPAM 割り当て CIDR ブロックの使用をサポートしていません。IPAM 割り当て CIDR ブロックを使用すると、EIP 関連付けが失敗する可能性があります。

Amazon VPC console

1. Amazon VPC コンソール を開きます。
2. ナビゲーションペインで、[Your VPCs (お使いの VPC)] を選択します。
3. 以前に作成した VPC を選択し、アクション、CIDRs の編集を選択します。
4. 新しい IPV4 CIDR の追加 を選択します。
5. IPV4 CIDR 手動入力を選択します。
6. 以前に作成したパブリック IPAM プールから CIDR ブロックを指定します。

AWS CLI

1. ターミナルセッションを開きます。
2. IPAM プール ID とプロビジョニングされた CIDR ブロックを取得します。

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)

CIDR_BLOCK=$(aws ec2 get-ipam-pool-cidrs \
  --ipam-pool-id $POOL_ID \
  --query 'IpamPoolCidrs[0].Cidr' \
  --output text)
```

3. CIDR ブロックを VPC に追加します。

```
aws ec2 associate-vpc-cidr-block \
  --vpc-id $VPC_ID \
  --cidr-block $CIDR_BLOCK
```

VPC メインルートテーブルを設定する

Amazon EVS VLAN サブネットは、VPC メインルートテーブルに暗黙的に関連付けられます。環境のデプロイを成功させるために DNS やオンプレミスシステムなどの依存サービスへの接続を有効にするには、これらのシステムへのトラフィックを許可するようにメインルートテーブルを設定する必要があります。メインルートテーブルには、VPC の CIDR のルートが含まれている必要があります。メインルートテーブルの使用は、最初の Amazon EVS 環境のデプロイにのみ必要です。環境のデプロイ後、カスタムルートテーブルを使用するように環境を設定できます。詳細については、「the section called “カスタムルートテーブルを設定する”」を参照してください。

環境のデプロイ後、各 Amazon EVS VLAN サブネットを VPC 内のルートテーブルに明示的に関連付ける必要があります。VLAN サブネットが VPC ルートテーブルに明示的に関連付けられていない場合、NSX 接続は失敗します。環境デプロイ後にサブネットをカスタムルートテーブルに明示的に関連付けることを強くお勧めします。詳細については、「the section called “VPC メインルートテーブルを設定する”」を参照してください。

> **Important**
>
> Amazon EVS は、Amazon EVS 環境の作成後にのみカスタムルートテーブルの使用をサポートします。Amazon EVS 環境の作成中にカスタムルートテーブルを使用しないでください。接続に問題がある可能性があります。

VPC DHCP オプションセットを使用して DNS サーバーと NTP サーバーを設定する

> **Important**
>
> これらの Amazon EVS 要件を満たしていない場合、環境のデプロイは失敗します。
>
> - DHCP オプションセットにプライマリ DNS サーバーの IP アドレスとセカンダリ DNS サーバーの IP アドレスを含めます。

- デプロイに各 VCF 管理アプライアンスと Amazon EVS ホストの A レコードを含む DNS フォワードルックアップゾーンを含めます。
- デプロイに各 VCF 管理アプライアンスと Amazon EVS ホストの PTR レコードを含む DNS リバースルックアップゾーンを含めます。
- VPC のメインルートテーブルを設定して、DNS サーバーへのルートが存在することを確認します。
- ドメイン名登録が有効で有効期限が切れていないこと、および重複するホスト名や IP アドレスが存在しないことを確認します。
- Amazon EVS が以下と通信できるように、セキュリティグループとネットワークアクセスコントロールリスト (ACLs) を設定します。
  - TCP/UDP ポート 53 経由の DNS サーバー。
  - HTTPS および SSH 経由で管理 VLAN サブネットをホストします。
  - HTTPS および SSH 経由の管理 VLAN サブネット。

Amazon EVS は VPC の DHCP オプションセットを使用して以下を取得します。

- ホスト IP アドレス解決用のドメインネームシステム (DNS) サーバー。
- DNS 解決のドメイン名。
- 時刻同期用の Network Time Protocol (NTP) サーバー。

DHCP オプションセットは、 Amazon VPC コンソールまたは を使用して作成できます AWS CLI。詳細については、「 Amazon VPC ユーザーガイド」の「DHCP オプションセットの作成」を参照してください。

DNS サーバーを設定する

DNS 設定により、Amazon EVS 環境でホスト名解決が有効になります。Amazon EVS 環境を正常にデプロイするには、VPC の DHCP オプションセットに次の DNS 設定が必要です。

- DHCP オプションセットのプライマリ DNS サーバー IP アドレスとセカンダリ DNS サーバー IP アドレス。
- デプロイ内の各 VCF 管理アプライアンスと Amazon EVS ホストの A レコードを含む DNS フォワードルックアップゾーン。

- デプロイ内の各 VCF 管理アプライアンスと Amazon EVS ホストの PTR レコードを含むリバースルックアップゾーン。NTP 設定では、デフォルトの Amazon NTP アドレス `169.254.169.123`または別の IPv4 アドレスを使用できます。

DHCP オプションセットで DNS サーバーを設定する方法の詳細については、「DHCP オプションセットの作成」を参照してください。

オンプレミス接続用に DNS を設定する

オンプレミス接続の場合は、インバウンドリゾルバーで Route 53 プライベートホストゾーンを使用することをお勧めします。この設定によりハイブリッド DNS 解決が有効になり、VPC 内の内部 DNS に Route 53 を使用して、既存のオンプレミス DNS インフラストラクチャと統合できます。これにより、VPC 内のリソースは、複雑な設定を必要とせずに、オンプレミスネットワークでホストされているドメイン名を解決できます。必要に応じて、Route 53 アウトバウンドリゾルバーで独自の DNS サーバーを使用することもできます。設定する手順については、Amazon Route 53 デベロッパーガイドの「プライベートホストゾーンの作成」および「VPC へのインバウンド DNS クエリの転送」を参照してください。

> **Note**
>
> DHCP オプションセットで Route 53 とカスタムドメインネームシステム (DNS) サーバーの両方を使用すると、予期しない動作が発生する可能性があります。

> **Note**
>
> のプライベートホストゾーンで定義されたカスタム DNS ドメイン名を使用する場合 Route 53、またはインターフェイス VPC エンドポイント (AWS PrivateLink) でプライベート DNS を使用する場合は、 属性`enableDnsHostnames`と `enableDnsSupport` 属性の両方を に設定する必要がありま`true`す。詳細については、「VPC の DNS 属性」を参照してください。

DNS 到達可能性の問題のトラブルシューティング

Amazon EVS では、DNS レコードに到達するために、VPC の DHCP オプションセット内の SDDC Manager サーバーと DNS サーバーへの永続的な接続が必要です。SDDC Manager への永続的な接

続が使用できなくなった場合、Amazon EVS は環境ステータスを検証できなくなり、環境へのアクセスが失われる可能性があります。この問題のトラブルシューティング手順については、「」を参照してくださいthe section called “到達可能性チェックに失敗しました”。

NTP サーバーの設定

NTP サーバーは、ネットワークに時間を提供します。Amazon EC2 インスタンスでの一貫性のある正確な時間参照は、多くの VCF 環境タスクとプロセスにとって不可欠です。時刻の同期は、次の場合に不可欠です。

- システムのログ記録と監査
- セキュリティオペレーション
- 分散システム管理
- トラブルシューティング

VPC の DHCP オプションセットには、最大 4 つの NTP サーバーの IPv4 アドレスを入力できます。Amazon Time Sync Service は、IPv4 アドレス で指定できます`169.254.169.123`。デフォルトでは、Amazon EVS がデプロイする Amazon EC2 インスタンスは、IPv4 アドレス の Amazon Time Sync Service を使用します`169.254.169.123`。

NTP サーバーの詳細については、「RFC 2123」を参照してください。Amazon Time Sync Service の詳細については、VMware Cloud Foundation ドキュメントのEC2 インスタンスの精度クロックと時刻の同期」および「VMware Cloud Foundation Hosts での NTP の設定」を参照してください。VMware

NTP 設定を構成するには

1. NTP ソースを選択します。
   - Amazon Time Sync Service (推奨)
   - カスタム NTP サーバー
2. DHCP オプションセットに NTP サーバーを追加します。詳細については、「Amazon VPC ユーザーガイド」の「DHCP オプションセットの作成」を参照してください。
3. 時刻の同期を確認します。DHCP オプションセット設定の詳細については、「」を参照してくださいthe section called “VPC の DHCP オプションセットを設定する”。

オンプレミスネットワーク接続を設定する (オプション)

関連付けられたトランジットゲートウェイ Direct Connect を使用するか、トランジットゲートウェイへの AWS Site-to-Site VPN アタッチメントを使用して、オンプレミスデータセンターの AWS インフラストラクチャへの接続を設定できます。

オンプレミスシステムへの接続を有効にして環境のデプロイを成功させるには、これらのシステムへのトラフィックを許可するように VPC のメインルートテーブルを設定する必要があります。詳細については、「the section called “VPC メインルートテーブルを設定する”」を参照してください。

Amazon EVS 環境を作成したら、Amazon EVS 環境内で作成された VPC CIDRs を使用してトランジットゲートウェイルートテーブルを更新する必要があります。詳細については、「the section called “オンプレミス接続用のトランジットゲートウェイルートテーブルと Direct Connect プレフィックスを設定する (オプション)”」を参照してください。

Direct Connect 接続の設定の詳細については、Direct Connect 「ゲートウェイとトランジットゲートウェイの関連付け」を参照してください。Transit Gateway で AWS Site-to-Site VPN を使用する方法の詳細については、 AWS Transit Gateway ユーザーガイド Amazon VPC のAWSAmazon VPC「Transit Gateway の Site-to-Site VPN アタッチメント」を参照してください。

> **Note**
>
> Amazon EVS は、 AWS Direct Connect プライベート仮想インターフェイス (VIF)、またはアンダーレイ VPC に直接終了する AWS Site-to-Site VPN 接続を介した接続をサポートしていません。

エンドポイントとピアを使用して VPC Route Server インスタンスをセットアップする

Amazon EVS は Amazon VPC Route Server を使用して、VPC アンダーレイネットワークへの BGP ベースの動的ルーティングを有効にします。サービスアクセスサブネット内の少なくとも 2 つのルートサーバーエンドポイントにルートを共有するルートサーバーを指定する必要があります。ルートサーバーピアに設定したピア ASN は一致している必要があり、ピア IP アドレスは一意である必要があります。

HCX インターネット接続用に Route Server を設定する場合は、この手順の最初のステップで作成したサービスアクセスサブネットとパブリックサブネットの両方に対して Route Server の伝播を設定する必要があります。

Important

VPC Route Server 設定の次の Amazon EVS 要件を満たしていない場合、環境のデプロイは失敗します。

- サービスアクセスサブネットには、少なくとも 2 つのルートサーバーエンドポイントを設定する必要があります。
- Tier-0 ゲートウェイのボーダーゲートウェイプロトコル (BGP) を設定する場合、VPC Route Server ピア ASN 値は NSX Edge ピア ASN 値と一致する必要があります。
- 2 つのルートサーバーピアを作成するときは、エンドポイントごとに NSX アップリンク VLAN の一意の IP アドレスを使用する必要があります。これらの 2 つの IP アドレスは、Amazon EVS 環境のデプロイ中に NSX エッジに割り当てられます。
- Route Server の伝播を有効にするときは、伝播されるすべてのルートテーブルに少なくとも 1 つの明示的なサブネットの関連付けがあることを確認する必要があります。伝播されたルートテーブルに明示的なサブネットの関連付けがない場合、BGP ルートアドバタイズは失敗します。

VPC Route Server のセットアップの詳細については、「Route Server の開始方法チュートリアル」を参照してください。

Important

Route Server の伝播を有効にするときは、伝播されるすべてのルートテーブルに少なくとも 1 つの明示的なサブネットの関連付けがあることを確認します。ルートテーブルに明示的なサブネットの関連付けがある場合、BGP ルートアドバタイズは失敗します。

Note

Route Server ピアのライブネス検出の場合、Amazon EVS はデフォルトの BGP キープアライブメカニズムのみをサポートします。Amazon EVS は、マルチホップ双方向転送検出 (BFD) をサポートしていません。

> **Note**
>
> ルートサーバーインスタンスの永続ルートを 1～5 分で有効にすることをお勧めします。有効にすると、すべての BGP セッションが終了しても、ルートはルートサーバーのルーティングデータベースに保持されます。詳細については、「 Amazon VPC ユーザーガイド」の「ルートサーバーの作成」を参照してください。

> **Note**
>
> NAT ゲートウェイまたはトランジットゲートウェイを使用している場合は、VPC ルートテーブル (複数可) に NSX ルートを伝達するようにルートサーバーが正しく設定されていることを確認します。

トラブルシューティング

問題が発生した場合:

- 各ルートテーブルに明示的なサブネットの関連付けがあることを確認します。
- ルートサーバーと NSX Tier-0 ゲートウェイに入力されたピア ASN 値が一致することを確認します。
- Route Server エンドポイントの IP アドレスが一意であることを確認します。
- ルートテーブルのルート伝播ステータスを確認します。
- VPC Route Server ピアログ記録を使用して、BGP セッションの状態をモニタリングし、接続の問題をトラブルシューティングします。詳細については、「Amazon VPC ユーザーガイド」の「Route server peer logging」を参照してください。

Amazon EVS VLAN サブネットトラフィックを制御するネットワーク ACL を作成する

Amazon EVS は、ネットワークアクセスコントロールリスト (ACL) を使用して、Amazon EVS VLAN サブネットとの間のトラフィックを制御します。VPC のデフォルトのネットワーク ACL を使用するか、セキュリティグループのルールに似たルールを使用して VPC のカスタムネットワーク ACL を作成し、VPC にセキュリティレイヤーを追加できます。詳細については、「Amazon VPC ユーザーガイド」の「VPC のネットワーク ACL を作成する」を参照してください。

HCX インターネット接続を設定する場合は、設定したネットワーク ACL ルールで HCX コンポーネントの必要なインバウンド接続とアウトバウンド接続が許可されていることを確認してください。HCX ポート要件の詳細については、VMware HCX ユーザーガイドを参照してください。

Important

インターネット経由で接続している場合、Elastic IP アドレスを VLAN に関連付けると、その VLAN サブネット上のすべてのリソースに直接インターネットアクセスできます。セキュリティ要件に応じてアクセスを制限するように、適切なネットワークアクセスコントロールリストが設定されていることを確認します。

Important

EC2 セキュリティグループは、Amazon EVS VLAN サブネットにアタッチされている Elastic Network Interface では機能しません。Amazon EVS VLAN サブネットとの間のトラフィックを制御するには、ネットワークアクセスコントロールリストを使用する必要があります。

Amazon EVS 環境を作成する

Important

このトピックでは、できるだけ簡単かつ迅速に開始するために、デフォルト設定で Amazon EVS 環境を作成する手順について説明します。環境を作成する前に、すべての設定に精通し、要件を満たす設定で環境をデプロイすることをお勧めします。環境は、最初の環境の作成時にのみ設定できます。環境は、作成後に変更することはできません。考えられるすべての Amazon EVS 環境設定の概要については、「Amazon EVS API リファレンスガイド」を参照してください。

Note

環境 ID は、VPC ライセンスコンプライアンスのニーズに応じて、すべての AWS リージョンで Amazon EVS で使用できます。

> **Note**
>
> Amazon EVS 環境は、VPC および VPC サブネットと同じリージョンとアベイラビリティーゾーンにデプロイする必要があります。

ホストと VLAN サブネットを使用して Amazon EVS 環境を作成するには、このステップを実行します。

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。

   > **Note**
   >
   > コンソールの右上に表示される AWS リージョンが、環境を作成する AWS リージョンであることを確認します。そうでない場合は、 AWS リージョン名の横にあるドロップダウンを選択し、使用する AWS リージョンを選択します。

2. ナビゲーションペインで [Environment (環境)] を選択します。
3. [Create environment (環境の作成)] を選択します。
4. Amazon EVS 要件の検証ページで、サービス要件が満たされていることを確認します。詳細については、「Amazon Elastic VMware Service のセットアップ」を参照してください。
   a. (オプション) Name に環境名を入力します。
   b. 環境バージョンで、VPC バージョンを選択します。Amazon EVS が提供する VCF バージョンの詳細については、「」を参照してくださいthe section called “VCF バージョンと EC2 インスタンス”。
   c. サイト ID には、Broadcom サイト ID を入力します。
   d. VCF ソリューションキーには、VPC ソリューションキー (VMware vSphere 8 Enterprise Plus for VCF) を入力します。このライセンスキーは、既存の環境では使用できません。

      > **Note**
      >
      > VCF ソリューションキーには、少なくとも 256 コアが必要です。

> **Note**
>
> VCF ライセンスは、ライセンスコンプライアンスのためにすべての AWS リージョンで Amazon EVS で利用できます。Amazon EVS はライセンスキーを検証しません。ライセンスキーを検証するには、Broadcom サポートにアクセスしてください。

> **Note**
>
> Amazon EVS では、サービスが正しく機能するためには、SDDC Manager で有効な VCF ソリューションキーを維持する必要があります。デプロイ後に vSphere Client を使用して VCF ソリューションキーを管理する場合は、キーが SDDC Manager ユーザーインターフェイスのライセンス画面にも表示されることを確認する必要があります。

e. vSAN ライセンスキーの場合は、vSAN ライセンスキーを入力します。このライセンスキーは、既存の環境では使用できません。

> **Note**
>
> vSAN ライセンスキーには、少なくとも 110 TiB の vSAN 容量が必要です。

> **Note**
>
> VCF ライセンスは、ライセンスコンプライアンスのためにすべての AWS リージョンで Amazon EVS で利用できます。Amazon EVS はライセンスキーを検証しません。ライセンスキーを検証するには、Broadcom サポートにアクセスしてください。

> **Note**
>
> Amazon EVS では、SDDC Manager forchooose で有効な vSAN ライセンスキーを維持し、適切に機能するようにサービスを選択する必要があります。デプロイ後に

vSphere Client を使用して vSAN ライセンスキーを管理する場合は、キーが SDDC Manager ユーザーインターフェイスのライセンス画面にも表示されることを確認する必要があります。

f. VCF ライセンス条項については、チェックボックスをオンにして、Amazon EVS 環境内のすべての物理プロセッサコアをカバーするために必要な数の VCF ソフトウェアライセンスを購入し、引き続き維持することを確認します。Amazon EVS の VCF ソフトウェアに関する情報は、ライセンスコンプライアンスを確認するために Broadcom と共有されます。

g. [次へ] を選択します。

5. ホストの詳細を指定ページで、以下のステップを 4 回実行して、4 つのホストを環境に追加します。Amazon EVS 環境では、初期デプロイに 4 つのホストが必要です。

a. ホストの詳細の追加 を選択します。

b. DNS ホスト名には、ホストのホスト名を入力します。

c. インスタンスタイプで、EC2 インスタンスタイプを選択します。

d. ESX ホストバージョンの場合、環境の作成中に、選択した VCF バージョンのデフォルトの ESX バージョンが使用されます。詳細については「the section called “VCF バージョンと EC2 インスタンス”」を参照してください。

Important

Amazon EVS がデプロイする EC2 インスタンスを停止または終了しないでください。このアクションにより、データが失われます。

Note

Amazon EVS は、現時点では i4i.metal EC2 インスタンスのみをサポートしています。

e. SSH キーペアの場合は、ホストへの SSH アクセス用の SSH キーペアを選択します。

f. ホストの追加 を選択します。

6. ネットワークと接続の設定ページで、次の操作を行います。

a. HCX 接続要件については、HCX をプライベート接続で使用するか、インターネット経由で使用するかを選択します。

b. VPC の場合は、以前に作成した VPC を選択します。

c. (HCX インターネット接続のみ) HCX ネットワーク ACL の場合は、HCX VLAN が関連付けられるネットワーク ACL を選択します。

> **Important**
>
> HCX VLAN 専用のカスタムネットワーク ACL を作成することを強くお勧めします。詳細については、「the section called “ネットワーク ACL を設定する”」を参照してください。

d. サービスアクセスサブネットで、VPC の作成時に作成されたプライベートサブネットを選択します。

e. セキュリティグループ - オプション では、Amazon EVS コントロールプレーンと VPC 間の通信を制御するセキュリティグループを最大 2 つ選択できます。セキュリティグループが選択されていない場合、Amazon EVS はデフォルトのセキュリティグループを使用します。

> **Note**
>
> 選択したセキュリティグループが DNS サーバーと Amazon EVS VLAN サブネットへの接続を提供していることを確認します。

f. 管理接続で、Amazon EVS VLAN サブネットに使用する CIDR ブロックを入力します。HCX アップリンク VLAN CIDR ブロックの場合、パブリック HCX VLAN を設定する場合は、ネットマスクの長さが正確に /28 の CIDR ブロックを指定する必要があります。パブリック HCX VLAN に他の CIDR ブロックサイズが指定されている場合、Amazon EVS は検証エラーをスローします。プライベート HCX VLAN およびその他のすべての VLANs CIDR ブロックの場合、使用できる最小ネットマスク長は /28 で、最大長は /24 です。

> **Important**
>
> Amazon EVS VLAN サブネットは Amazon EVS 環境の作成時にのみ作成でき、環境の作成後に変更することはできません。環境を作成する前に、VLAN サブネット CIDR ブロックのサイズが適切であることを確認する必要があります。環境のデプロイ後に VLAN サブネットを追加することはできません。詳細については、「the section called “Amazon EVS ネットワークに関する考慮事項”」を参照してください。

g. 拡張 VLANs で、NSX フェデレーションの有効化など、Amazon EVS 内の VCF 機能を拡張するために使用できる追加の Amazon EVS VLAN サブネットの CIDR ブロックを入力します。

h. ワークロード/VCF 接続で、NSX アップリンク VLAN の CIDR ブロックを入力し、NSX アップリンク経由で Route Server エンドポイントにピアリングする 2 つの VPC Route Server ピア IDs を選択します。

> **Note**
>
> Amazon EVS には、EVS デプロイ前に 2 つの Route Server エンドポイントと 2 つの Route Server ピアに関連付けられている VPC Route Server インスタンスが必要です。この設定により、NSX アップリンクを介した BGP ベースの動的ルーティングが有効になります。詳細については、「the section called “エンドポイントとピアを使用して VPC Route Server インスタンスをセットアップする”」を参照してください。

i. [Next] (次へ) を選択します。

7. 「管理 DNS ホスト名の指定」ページで、次の操作を行います。

a. 管理アプライアンスの DNS ホスト名に、仮想マシンが VCF 管理アプライアンスをホストするための DNS ホスト名を入力します。Route 53 を DNS プロバイダーとして使用する場合は、DNS レコードを含むホストゾーンも選択します。

b. 認証情報で、Secrets Manager の AWS マネージド KMS キーを使用するか、指定したカスタマーマネージド KMS キーを使用するかを選択します。このキーは、SDDC Manager、NSX Manager、vCenter アプライアンスを使用するために必要な VCF 認証情報を暗号化するために使用されます。

> **Note**
>
> カスタマーマネージド KMS キーには使用コストがかかります。詳細については、AWS KMS の料金ページを参照してください。

c. [次へ] を選択します。

8. (オプション) タグの追加ページで、この環境に割り当てるタグを追加し、次へを選択します。

> **Note**
>
> この環境の一部として作成されたホストには、 タグ が付けられますDoNotDelete-EVS-<environmentid>-<hostname>。

> **Note**
>
> Amazon EVS 環境に関連付けられているタグは、EC2 インスタンスなどの基盤となる AWS リソースには伝播されません。基盤となる AWS リソースにタグを作成するには、それぞれのサービスコンソールまたは を使用します AWS CLI。

9. 確認と作成ページで、設定を確認し、環境の作成を選択します。

> **Important**
>
> 環境のデプロイ中、Amazon EVS は EVS VLAN サブネットを作成し、それをメインルートテーブルに暗黙的に関連付けます。デプロイが完了したら、NSX 接続の目的で Amazon EVS VLAN サブネットをルートテーブルに明示的に関連付ける必要があります。詳細については、「the section called “Amazon EVS VLAN サブネットを VPC ルートテーブルに明示的に関連付ける”」を参照してください。

> **Note**
>
> Amazon EVS は、VMware Cloud Foundation の最新のバンドルバージョンをデプロイします。このバンドルバージョンには、非同期パッチと呼ばれる個々の製品更新が含まれていない場合があります。このデプロイが完了したら、Broadcom の非同期パッチツール (AP ツール) または SDDC Manager の製品内 LCM オートメーションを使用して、個々の製品を確認して更新することを強くお勧めします。NSX のアップグレードは SDDC Manager の外部で行う必要があります。

> **Note**
>
> 環境の作成には数時間かかる場合があります。

AWS CLI

1. ターミナルセッションを開きます。
2. Amazon EVS 環境を作成します。以下は、サンプル`aws evs create-environment`リクエストです。

> **Important**
>
> `aws evs create-environment` コマンドを実行する前に、Amazon EVS のすべての前提条件が満たされていることを確認します。前提条件が満たされていない場合、環境のデプロイは失敗します。詳細については、「Amazon Elastic VMware Service のセットアップ」を参照してください。

> **Important**
>
> 環境のデプロイ中、Amazon EVS は EVS VLAN サブネットを作成し、それをメインルートテーブルに暗黙的に関連付けます。デプロイが完了したら、NSX 接続の目的で Amazon EVS VLAN サブネットをルートテーブルに明示的に関連付ける必要があります。詳細については、「the section called “Amazon EVS VLAN サブネットを VPC ルートテーブルに明示的に関連付ける”」を参照してください。

> **Note**
>
> Amazon EVS は、VMware Cloud Foundation の最新のバンドルバージョンをデプロイします。このバンドルバージョンには、非同期パッチと呼ばれる個々の製品更新が含まれていない場合があります。このデプロイが完了したら、Broadcom の非同期パッチツール (AP ツール) または SDDC Manager の製品内 LCM オートメーションを使用して、個々の製品を確認して更新することを強くお勧めします。NSX のアップグレードは SDDC Manager の外部で行う必要があります。

> **Note**
>
> 環境のデプロイには数時間かかる場合があります。

- には`--vpc-id`、/22 の最小 IPv4 CIDR 範囲で以前に作成した VPC を指定します。
- には`--service-access-subnet-id`、VPC の作成時に作成されたプライベートサブネットの一意の ID を指定します。
- については`--vcf-version`、Amazon EVS が提供する VCF バージョンthe section called "VCF バージョンと EC2 インスタンス"については、「」を参照してください。
- では`--terms-accepted`、Amazon EVS 環境内のすべての物理プロセッサコアをカバーするために必要な数の VCF ソフトウェアライセンスを購入し、引き続き維持することを確認します。Amazon EVS の VCF ソフトウェアに関する情報は、ライセンスコンプライアンスを確認するために Broadcom と共有されます。
- には`--license-info`、VPC ソリューションキー (VMware vSphere 8 Enterprise Plus for VCF) と vSAN ライセンスキーを入力します。

> **Note**
>
> VCF ソリューションキーには、少なくとも 256 コアが必要です。vSAN ライセンスキーには、少なくとも 110 TiB の vSAN 容量が必要です。

> **Note**
>
> Amazon EVS では、サービスが正しく機能するためには、有効な VCF ソリューションキーと vSAN ライセンスキーを SDDC Manager に維持する必要があります。デプロイ後に vSphere Client を使用してこれらのライセンスキーを管理する場合は、SDDC Manager ユーザーインターフェイスのライセンス画面にも表示されることを確認する必要があります。

> **Note**
>
> VCF ソリューションキーと vSAN ライセンスキーは、既存の Amazon EVS 環境では使用できません。

- には、Amazon EVS がユーザーに代わって作成する Amazon EVS VLAN サブネットの CIDR 範囲`--initial-vlans`を指定します。これらの VLANsは VCF 管理アプライアンスをデプロイするために使用されます。パブリック HCX VLAN を設定する場合は、ネット

マスクの長さが正確に /28 の CIDR ブロックを指定する必要があります。パブリック HCX VLAN に他の CIDR ブロックサイズが指定されている場合、Amazon EVS は検証エラーをスローします。プライベート HCX VLAN およびその他のすべての VLANs CIDR ブロックの場合、使用できる最小ネットマスク長は /28 で、最大長は /24 です。

- `hcxNetworkAclId` HCX インターネット接続を設定する場合、 が使用されます。パブリック HCX VLAN のカスタムネットワーク ACL を指定します。

> **Important**
>
> HCX VLAN 専用のカスタムネットワーク ACL を作成することを強くお勧めします。詳細については、「the section called “ネットワーク ACL を設定する”」を参照してください。

> **Important**
>
> Amazon EVS VLAN サブネットは Amazon EVS 環境の作成時にのみ作成でき、環境の作成後に変更することはできません。環境を作成する前に、VLAN サブネット CIDR ブロックのサイズが適切であることを確認する必要があります。環境のデプロイ後に VLAN サブネットを追加することはできません。詳細については、「the section called “Amazon EVS ネットワークに関する考慮事項”」を参照してください。

- には`--hosts`、Amazon EVS が環境デプロイに必要とするホストのホストの詳細を指定します。各ホストに DNS ホスト名、EC2 SSH キー名、EC2 インスタンスタイプを含めます。専用ホスト ID はオプションです。

> **Important**
>
> Amazon EVS がデプロイする EC2 インスタンスを停止または終了しないでください。このアクションにより、データが失われます。

> **Note**
>
> Amazon EVS は、現時点では i4i.metal EC2 インスタンスのみをサポートしています。

- には`--connectivity-info`、前のステップで作成した 2 つの VPC Route Server ピア IDs を指定します。

> **Note**
>
> Amazon EVS では、EVS デプロイ前に 2 つの Route Server エンドポイントと 2 つの Route Server ピアに関連付けられている VPC Route Server インスタンスが必要です。この設定により、NSX アップリンクを介した BGP ベースの動的ルーティングが有効になります。詳細については、「the section called “エンドポイントとピアを使用して VPC Route Server インスタンスをセットアップする”」を参照してください。

- には`--vcf-hostnames`、仮想マシンが VCF 管理アプライアンスをホストするための DNS ホスト名を入力します。
- には`--site-id`、一意の Broadcom サイト ID を入力します。この ID により、Broadcom ポータルへのアクセスが許可されます。ID は、ソフトウェア契約の終了時または契約更新時に Broadcom から提供されます。
- (オプション) には`--region`、環境をデプロイするリージョンを入力します。リージョンが指定されていない場合は、デフォルトのリージョンが使用されます。

```
aws evs create-environment \
--environment-name testEnv \
--vpc-id vpc-1234567890abcdef0 \
--service-access-subnet-id subnet-01234a1b2cde1234f \
--vcf-version VCF-5.2.2 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"isHcxPublic\": true,
```

```
      \"hcxNetworkAclId\": \"nacl-abcd1234\",
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07879acf49EXAMPLE\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07878bde50EXAMPLE\"
```

```
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07877eio51EXAMPLE\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07863ghi52EXAMPLE\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

レスポンスの例を次に示します。

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATING",
        "stateDetails": "The environment is being initialized, this operation
 may take some time to complete.",
        "createdAt": "2025-04-13T12:03:39.718000+00:00",
        "modifiedAt": "2025-04-13T12:03:39.718000+00:00",
```

```
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-1234567890abcdef0",
        "serviceAccessSubnetId": "subnet-01234a1b2cde1234f",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-1234567890abcdef0",
                "rsp-abcdef01234567890"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        }
    }
}
```

Amazon EVS 環境の作成を検証する

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションペインで [Environments (環境)] を選択します。

3. 環境を選択します。
4. 詳細タブを選択します。
5. 環境ステータスが合格で、環境ステータスが作成済みであることを確認します。これにより、環境を使用する準備ができたことがわかります。

> **Note**
>
> 環境の作成には数時間かかる場合があります。環境の状態がまだ作成中である場合は、ページを更新します。

AWS CLI

1. ターミナルセッションを開きます。
2. 環境の環境 ID とリソースを含むリージョン名を使用して、次のコマンドを実行します。が の場合、環境を使用する準備environmentStateが整いますCREATED。

> **Note**
>
> 環境の作成には数時間かかる場合があります。environmentState がまだ と表示されている場合はCREATING、 コマンドを再度実行して出力を更新します。

```
aws evs get-environment  --environment-id env-abcde12345
```

レスポンスの例を次に示します。

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATED",
        "createdAt": "2025-04-13T13:39:49.546000+00:00",
        "modifiedAt": "2025-04-13T13:40:39.355000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-0c6def5b7b61c9f41",
        "serviceAccessSubnetId": "subnet-06a3c3b74d36b7d5e",
```

```
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

Amazon EVS VLAN サブネットを VPC ルートテーブルに明示的に関連付ける

各 Amazon EVS VLAN サブネットを VPC 内のルートテーブルに明示的に関連付けます。このルートテーブルは、 AWS リソースが Amazon EVS で実行されている NSX ネットワークセグメント上の仮想マシンと通信できるようにするために使用されます。パブリック HCX VLAN を作成した場合は、パブリック HCX VLAN サブネットをインターネットゲートウェイにルーティングする VPC 内のパブリックルートテーブルに明示的に関連付けてください。

Example

Amazon VPC console

1. VPC コンソールに移動します。
2. ナビゲーションペインで、[Route tables] (ルートテーブル) を選択します。
3. Amazon EVS VLAN サブネットに関連付けるルートテーブルを選択します。
4. [サブネットの関連付け] タブを選択します。
5. 明示的なサブネットの関連付けで、サブネットの関連付けの編集を選択します。
6. すべての Amazon EVS VLAN サブネットを選択します。
7. [Save associations] (関連付けを保存する) を選択します。

AWS CLI

1. ターミナルセッションを開きます。
2. Amazon EVS VLAN サブネット IDsを特定します。

```
aws ec2 describe-subnets
```

3. Amazon EVS VLAN サブネットを VPC のルートテーブルに関連付けます。

```
aws ec2 associate-route-table \
--route-table-id rtb-0123456789abcdef0 \
--subnet-id subnet-01234a1b2cde1234f
```

EIPsを HCX パブリック VLAN サブネットに関連付ける (HCX インターネット接続用)

IPAM プールから HCX インターネット接続用の HCX パブリック VLAN に Elastic IP アドレス (EIPs) を関連付けるには、次の手順に従います。HCX Manager および HCX Interconnect (HCX-IX) アプライアンスには、少なくとも 2 つの EIPs を関連付ける必要があります。デプロイする必要がある HCX ネットワークアプライアンスごとに追加の EIP を関連付けます。HCX パブリック VLAN に関連付けられた IPAM プールから最大 13 EIPs を持つことができます。

Important

IPAM プールから少なくとも 2 つの EIPs を HCX パブリック VLAN サブネットに関連付けない場合、HCX パブリックインターネット接続は失敗します。

Note

Amazon EVS は、現時点では EIPs HCX VLAN の関連付けのみをサポートしています。

Note

パブリック IPAM CIDR ブロックの最初の 2 つの EIPs または最後の EIP を VLAN サブネットに関連付けることはできません。これらの EIPsは、ネットワーク、デフォルトゲートウェイ、ブロードキャストアドレスとして予約されています。これらの EIPs を VLAN サブネットに関連付けると、Amazon EVS は検証エラーをスローします。

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションメニューで、環境を選択します。
3. 環境を選択します。
4. ネットワークと接続タブで、HCX パブリック VLAN を選択します。
5. EIP を VLAN に関連付けるを選択します。
6. HCX パブリック VLAN に関連付ける Elastic IP アドレス (複数可) を選択します。
7. EIPs関連付けを選択します。
8. EIP の関連付けをチェックして、EIPsが HCX パブリック VLAN に関連付けられていることを確認します。

AWS CLI

1. Elastic IP アドレスを VLAN に関連付けるには、 `associate-eip-to-vlan` コマンド例を使用します。

- `environment-id` - Amazon EVS 環境の ID。
- `vlan-name` - Elastic IP アドレスに関連付ける VLAN の名前。
- `allocation-id` - Elastic IP アドレスの割り当て ID。

```
aws evs associate-eip-to-vlan \
  --environment-id "env-605uove256" \
  --vlan-name "hcx" \
  --allocation-id "eipalloc-0429268f30c4a34f7"
```

コマンドは、新しい EIP 関連付けなど、VLAN に関する詳細を返します。

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [
            {
                "associationId": "eipassoc-09e966faad7ecc58a",
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

`eipAssociations` 配列には、以下を含む新しい関連付けが表示されます。

- `associationId` - この EIP 関連付けの一意の ID。関連付けの解除に使用されます。
- `allocationId` - 関連付けられた Elastic IP アドレスの割り当て ID。
- `ipAddress` - VLAN に割り当てられた IP アドレス。

2. ステップを繰り返して、追加の EIPs。

オンプレミス接続用のトランジットゲートウェイルートテーブルと Direct Connect プレフィックスを設定する (オプション)

トランジットゲートウェイで Direct Connect or AWS Site-to-Site VPN を使用してオンプレミスネットワーク接続を設定する場合は、Amazon EVS 環境内で作成された VPC CIDRs を使用してトランジットゲートウェイルートテーブルを更新する必要があります。詳細については、「Amazon VPC Transit Gateways の Transit Gateway ルートテーブル」を参照してください。

AWS Direct Connect を使用している場合は、VPC から更新されたルートを送受信するために Direct Connect プレフィックスも更新する必要がある場合があります。詳細については、AWS 「Direct Connect ゲートウェイのプレフィックスインタラクションを許可する」を参照してください。

VCF 認証情報を取得して VCF 管理アプライアンスにアクセスする

Amazon EVS は AWS Secrets Manager を使用して、アカウントにマネージドシークレットを作成、暗号化、保存します。これらのシークレットには、vCenter Server、NSX、SDDC Manager などの VCF 管理アプライアンスをインストールしてアクセスするために必要な VCF 認証情報と、ESX ルートパスワードが含まれています。シークレットの取得の詳細については、AWS 「 Secrets Manager ユーザーガイド」の「Secrets Manager からシー AWS クレットを取得する」を参照してください。

> **Note**
>
> Amazon EVS では、シークレットのマネージドローテーションは提供されません。シークレットの有効期間が長くならないように、設定されたローテーション期間に定期的にシークレットをローテーションすることをお勧めします。

AWS Secrets Manager から VCF 認証情報を取得したら、それを使用して VCF 管理アプライアンスにログインできます。詳細については、VMware 製品ドキュメントの「SDDC Manager ユーザーインターフェイスにログインする」およびvSphere クライアントを使用および設定する方法」を参照してください。

EC2 シリアルコンソールを設定する (オプション)

デフォルトでは、Amazon EVS は新しくデプロイされた Amazon EVS ホストで ESX シェルを有効にします。この設定により、ECAmazon EC22 インスタンスのシリアルポートにアクセスできま

す。このポートを使用して、起動、ネットワーク設定、その他の問題のトラブルシューティングを行うことができます。シリアルコンソールではインスタンスにネットワーク機能を持たせる必要はありません。シリアルコンソールでは、キーボードとモニターがインスタンスのシリアルポートに直接アタッチされているかのように、実行中の EC2 インスタンスにコマンドを入力できます。

EC2 シリアルコンソールには、EC2 コンソールまたは を使用してアクセスできます AWS CLI。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの EC2 シリアルコンソール」を参照してください。 Amazon EC2

> **Note**
>
> EC2 シリアルコンソールは、ダイレクトコンソールユーザーインターフェイス (DCUI) にアクセスして ESX ホストとローカルでやり取りする Amazon EVS がサポートする唯一のメカニズムです。

> **Note**
>
> Amazon EVS は、デフォルトでリモート SSH を無効にします。SSH がリモート ESX シェルにアクセスできるようにする方法の詳細については、VMware vSphere 製品ドキュメントの「Remote ESX Shell Access with SSH」を参照してください。

EC2 シリアルコンソールに接続する

EC2 シリアルコンソールに接続し、選択したツールを使用してトラブルシューティングを行うには、特定の前提条件タスクを完了する必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 シリアルコンソールの前提条件」および「EC2 シリアルコンソールに接続する」を参照してください。 Amazon EC2

> **Note**
>
> EC2 シリアルコンソールに接続するには、EC2 インスタンスの状態が である必要がありますrunning。インスタンスが pending、、stopping、stopped、または terminated状態にある場合shutting-down、シリアルコンソールに接続することはできません。インスタンスの状態変更の詳細については、Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスの状態変更」を参照してください。 Amazon EC2

EC2 シリアルコンソールへのアクセスを設定する

EC2 シリアルコンソールへのアクセスを設定するには、ユーザーまたは管理者がアカウントレベルでシリアルコンソールアクセスを許可し、ユーザーにアクセス権を付与するように IAM ポリシーを設定する必要があります。Linux インスタンスの場合、ユーザーがトラブルシューティングにシリアルコンソールを使用できるように、すべてのインスタンスでパスワードベースのユーザーを設定する必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 シリアルコンソールへのアクセスを設定する」を参照してください。 Amazon EC2

クリーンアップ

作成された AWS リソースを削除するには、次の手順に従います。

Amazon EVS ホストと環境を削除する

Amazon EVS ホストと環境を削除するには、次の手順に従います。このアクションは、Amazon EVS 環境で実行される VMware VCF インストールを削除します。

> **Note**
>
> Amazon EVS 環境を削除するには、まず環境内のすべてのホストを削除する必要があります。環境に関連付けられているホストがある場合、環境を削除することはできません。

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションペインで、環境を選択します。
3. 削除するホストを含む環境を選択します。
4. ホストタブを選択します。
5. ホストを選択し、ホストタブで削除を選択します。環境内のホストごとにこのステップを繰り返します。
6. Environments ページの上部で、Delete を選択し、Delete environment を選択します。

> **Note**
>
> 環境を削除すると、Amazon EVS が作成した Amazon EVS VLAN サブネットと AWS Secrets Manager シークレットも削除されます。作成した AWS リソースは削除されません。これらのリソースには引き続きコストが発生する可能性があります。

7. 不要になった Amazon EC2 キャパシティ予約がある場合は、キャンセルしたことを確認してください。詳細については、Amazon EC2 ユーザーガイドの「キャパシティ予約のキャンセル」を参照してください。

AWS CLI

1. ターミナルセッションを開きます。
2. 削除するホストを含む環境を特定します。

```
aws evs list-environments
```

レスポンスの例を次に示します。

```
{
    "environmentSummaries": [
        {
            "environmentId": "env-abcde12345",
            "environmentName": "testEnv",
            "vcfVersion": "VCF-5.2.2",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T14:42:41.430000+00:00",
            "modifiedAt": "2025-04-13T14:43:33.412000+00:00",
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345"
        },
        {
            "environmentId": "env-edcba54321",
            "environmentName": "testEnv2",
            "vcfVersion": "VCF-5.2.2",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T13:39:49.546000+00:00",
            "modifiedAt": "2025-04-13T13:52:13.342000+00:00",
```

```
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
edcba54321"
        }
    ]
}
```

3. 環境からホストを削除します。以下はサンプルaws evs delete-environment-hostリクエストです。

> **Note**
>
> 環境を削除できるようにするには、まず環境に含まれるすべてのホストを削除する必要があります。

```
aws evs delete-environment-host \
--environment-id env-abcde12345 \
--host esx01
```

4. 前の手順を繰り返して、環境内の残りのホストを削除します。
5. 環境を削除します。

```
aws evs delete-environment --environment-id env-abcde12345
```

> **Note**
>
> 環境を削除すると、Amazon EVS が作成した Amazon EVS VLAN サブネットと AWS Secrets Manager シークレットも削除されます。作成した他の AWS リソースは削除されません。これらのリソースには引き続きコストが発生する可能性があります。

6. 不要になった Amazon EC2 キャパシティ予約がある場合は、キャンセルしたことを確認してください。詳細については、Amazon EC2 ユーザーガイドの「キャパシティ予約のキャンセル」を参照してください。

IPAM リソースの削除 (HCX インターネット接続の場合)

HCX インターネット接続を設定している場合は、以下の手順に従って IPAM リソースを削除します。

1. パブリック IPAM プールから EIP 割り当てを解放します。詳細については、「VPC IP Address Manager ユーザーガイド」の「Release an allocation」を参照してください。
2. IPAM プールからパブリック IPv4 CIDR のプロビジョニングを解除します。詳細については、VPC IP Address Manager ユーザーガイドのCIDRs のプロビジョニングを解除する」を参照してください。
3. パブリック IPAM プールを削除します。詳細については、「VPC IP Address Manager ユーザーガイド」の「プールの削除」を参照してください。
4. IPAM を削除します。詳細については、「VPC IP Address Manager ユーザーガイド」の「IPAM の削除」を参照してください。

VPC Route Server コンポーネントを削除する

作成した Amazon VPC Route Server コンポーネントを削除する手順については、「Amazon VPC ユーザーガイド」の「Route Server のクリーンアップ」を参照してください。

ネットワークアクセスコントロールリスト (ACL) を削除する

ネットワークアクセスコントロールリストを削除する手順については、「Amazon VPC ユーザーガイド」の「VPC のネットワーク ACL を削除する」を参照してください。

サブネットルートテーブルの関連付け解除と削除

サブネットルートテーブルの関連付けを解除および削除する手順については、「Amazon VPC ユーザーガイド」の「サブネットルートテーブル」を参照してください。

サブネットを削除する

サービスアクセスサブネットを含む VPC サブネットを削除します。VPC サブネットを削除する手順については、「Amazon VPC ユーザーガイド」の「サブネットの削除」を参照してください。

> **Note**
>
> DNS に Route 53 を使用している場合は、サービスアクセスサブネットを削除する前に、インバウンドエンドポイントを削除します。それ以外の場合、サービスアクセスサブネットを削除することはできません。

> **Note**
>
> Amazon EVS は、環境が削除されると、ユーザーに代わって VLAN サブネットを削除します。Amazon EVS VLAN サブネットは、環境が削除された場合にのみ削除できます。

VPC を削除する

VPC を削除する手順については、「Amazon VPC ユーザーガイド」の「VPC を削除する」を参照してください。

次の手順

VMware Hybrid Cloud Extension (VMware HCX) を使用してワークロードを Amazon EVS VMware に移行します。詳細については、「移行」を参照してください。

VMware HCX を使用してワークロードを Amazon EVS に移行する

Amazon EVS がデプロイされたら、プライベートまたはパブリックのインターネット接続で VMware HCX をデプロイして、ワークロードの Amazon EVS への移行を容易にできます。詳細については、VMware HCX ユーザーガイドの「VMware HCX の開始方法」を参照してください。

> **Important**
>
> HCX インターネットベースの移行は、通常、以下には推奨されません。
>
> - ネットワークのジッターやレイテンシーの影響を受けやすいアプリケーション。
> - タイムクリティカルな vMotion オペレーション。
> - 厳格なパフォーマンス要件を持つ大規模な移行。
>
> このようなシナリオでは、HCX プライベート接続を使用することをお勧めします。プライベート専用接続は、インターネットベースの接続よりも信頼性の高いパフォーマンスを提供します。

HCX 接続オプション

AWS Direct Connect または Site-to-Site VPN 接続とのプライベート接続、またはパブリック接続を使用して、ワークロードを Amazon EVS に移行できます。

状況や接続オプションによっては、HCX とのパブリック接続またはプライベート接続を使用することをお勧めします。例えば、一部のサイトでは、プライベート接続でパフォーマンスの一貫性は向上しますが、VPN 暗号化やリンク速度の制限によりスループットが低下する場合があります。同様に、高スループットのパブリックインターネット接続では、パフォーマンスに大きな違いが生じる可能性があります。Amazon EVS では、最適な接続オプションを選択できます。

次の表は、HCX プライベート接続とパブリック接続の違いを比較したものです。

プライベート接続	パブリック接続
概要:	概要:
VPC 内のプライベート接続のみを使用します。必要に応じて、外部ネットワーク接続用のトランジットゲートウェイで AWS Direct Connect または Site-to-Site VPN を使用できます。	Elastic IP アドレスとのパブリックインターネット接続を使用して、専用のプライベート接続なしで移行を可能にします。
に最適	に最適
• 時間的制約のある vMotion オペレーション。 • 大規模な移行。 • レイテンシー/ジッターの影響を受けやすいアプリケーション。 • 大量のデータ転送。 • 既存の AWS Direct Connect/AWS Site-to-Site VPN を持つ組織。	• AWS Direct Connect/AWS Site-to-Site VPN のない場所。 • コスト重視のプロジェクト。
主な利点	主な利点
• 一貫した低レイテンシーの接続。 • 専用帯域幅の割り当て。 • より信頼性の高いネットワークパフォーマンス。 • デフォルトの HCX 暗号化は、プライベート環境で無効にしてパフォーマンスを最適化できます。 • パブリック IP 管理は必要ありません。	• プライベート接続よりも高速なセットアップ。 • 小規模な移行のための費用対効果。
主な考慮事項	主な考慮事項
• より複雑な初期設定。 • インフラストラクチャの前払いコストが高い。	• より可変なネットワークパフォーマンス。 • 帯域幅の制限があります。 • プライベート接続よりも高いレイテンシー。

プライベート接続	パブリック接続
• 実装タイムラインが長くなります。 • どの HCX コンポーネントにも直接インターネット接続はありません。	• 各コンポーネントには、パブリック IPAM プールから割り当てられた専用の Elastic IP アドレスが必要です。 • EIP 関連付けにより、HCX コンポーネントごとに直接インターネット接続が可能になります。

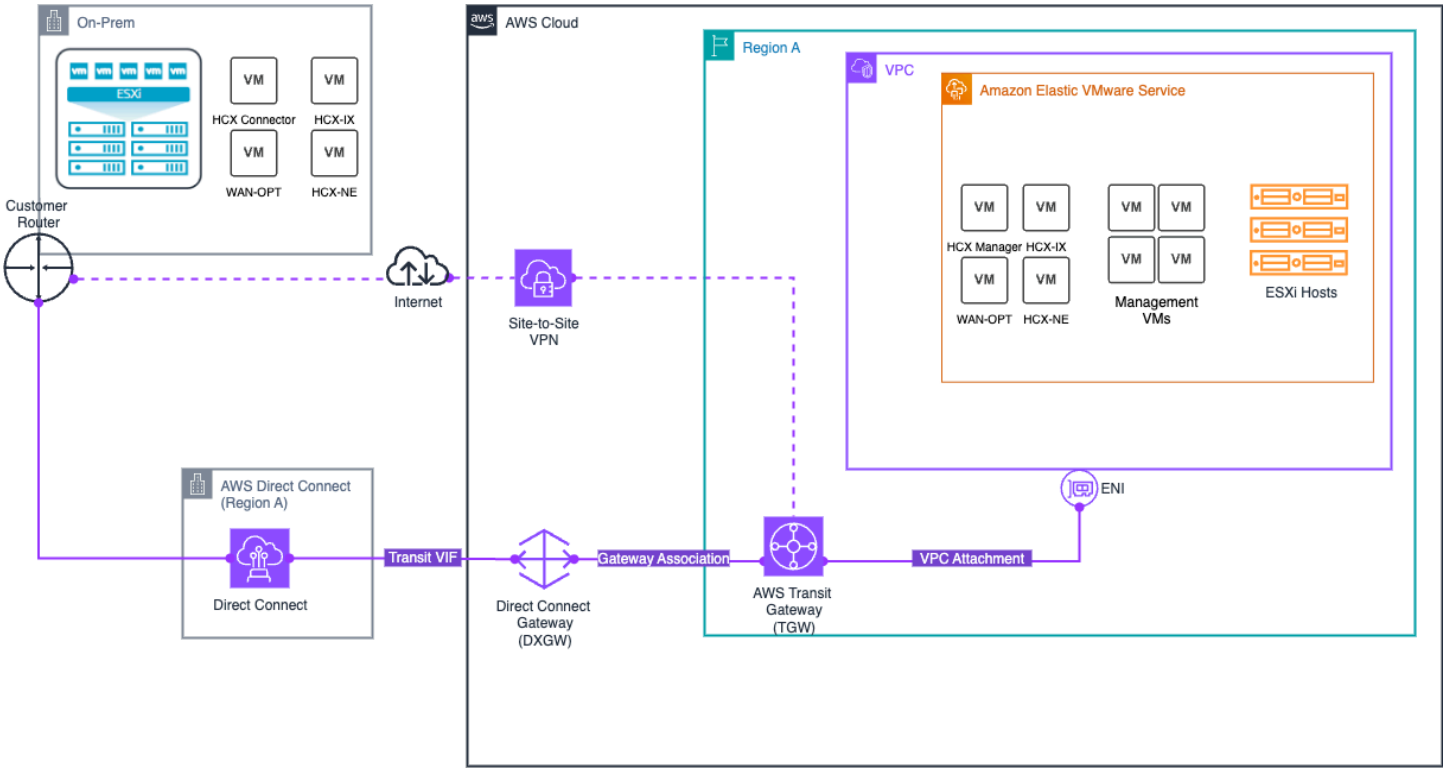
HCX プライベート接続アーキテクチャ

HCX プライベート接続ソリューションには、いくつかのコンポーネントが統合されています。

- Amazon EVS ネットワークコンポーネント
  - プライベート HCX VLAN を含む安全な通信には、プライベート VLAN サブネットのみを使用します。
  - トラフィック制御ACLs をサポートします。
  - プライベート VPC ルートサーバーを介したルートの動的 BGP 伝播をサポートします。
- AWS オンプレミス接続のマネージドネットワークトランジットオプション
  - AWS Direct Connect + AWS Transit Gateway を使用すると、プライベート専用接続を介してオンプレミスネットワークを Amazon EVS に接続できます。詳細については、AWS 「Direct Connect + AWS Transit Gateway」を参照してください。
  - AWS Site-to-Site VPN + AWS Transit Gateway には、インターネット経由でリモートネットワークとトランジットゲートウェイの間に IPsec VPN 接続を作成するオプションがあります。詳細については、AWS 「Transit Gateway + AWS Site-to-Site VPN」を参照してください。

> **Note**
>
> Amazon EVS は、 AWS Direct Connect プライベート仮想インターフェイス (VIF)、またはアンダーレイ VPC に直接終了する AWS Site-to-Site VPN 接続を介した接続をサポートしていません。

次の図は、HCX プライベート接続アーキテクチャを示しています。トランジットゲートウェイで AWS Direct Connect と Site-to-Site VPN を使用して、プライベート専用接続を介した安全なワークロード移行を可能にする方法を示しています。



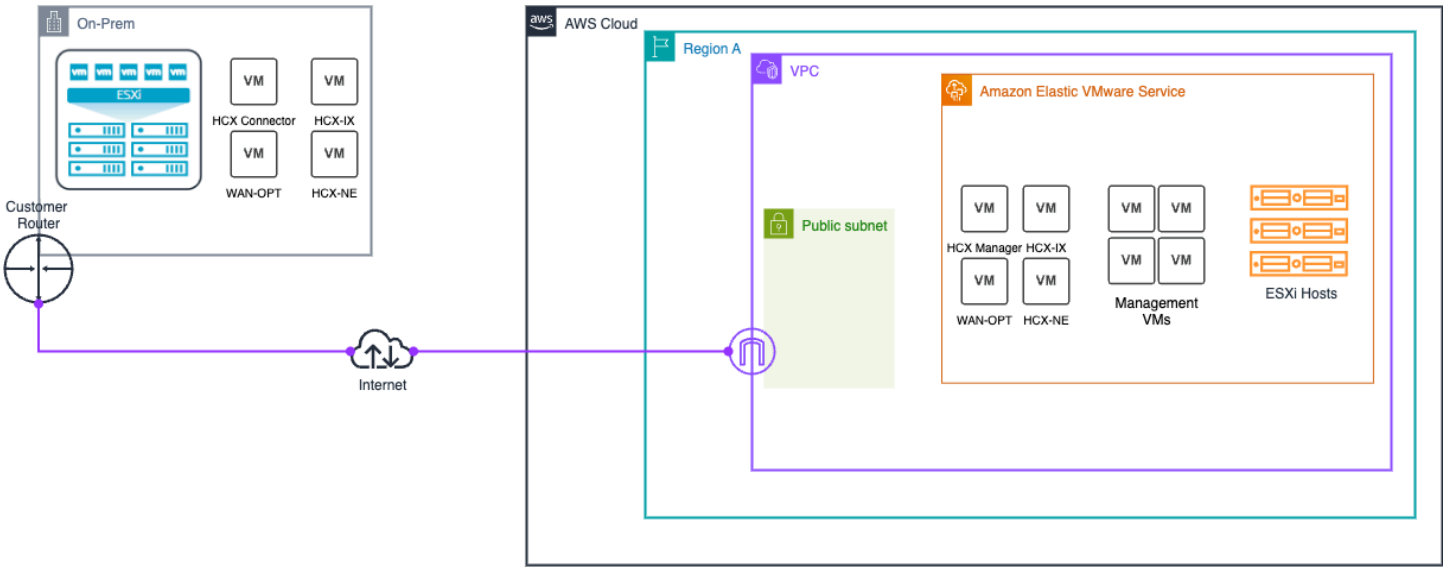
HCX インターネット接続アーキテクチャ

HCX インターネット接続ソリューションは、複数のコンポーネントが連携して動作します。

- Amazon EVS ネットワークコンポーネント
  - 分離されたパブリック HCX VLAN サブネットを使用して、Amazon EVS とオンプレミス HCX アプライアンス間のインターネット接続を有効にします。
  - トラフィック制御ACLs をサポートします。
  - パブリック VPC ルートサーバーを介したルートの動的 BGP 伝播をサポートします。
- IPAM とパブリック IP 管理
  - Amazon VPC IP Address Manager (IPAM) は、Amazon 所有のパブリック IPAM プールからのパブリック IPv4 アドレス割り当てを管理します。
  - セカンダリ VPC CIDR ブロック (/28) は IPAM プールから割り当てられ、メイン VPC CIDR とは別の独立したパブリックサブネットが作成されます。

詳細については、「the section called “HCX パブリック接続”」を参照してください。

次の図は、HCX インターネット接続アーキテクチャを示しています。



HCX 移行のセットアップ

このチュートリアルでは、ワークロードを Amazon EVS に移行するように VMware HCX を設定する方法について説明します。

前提条件

Amazon EVS で VMware HCX を使用する前に、HCX の前提条件が満たされていることを確認してください。詳細については、「the section called “VMware HCX の前提条件”」を参照してください。

> **Important**
>
> Amazon EVS には、HCX パブリックインターネット接続に関する固有の要件があります。HCX パブリック接続が必要な場合は、次の要件を満たす必要があります。
>
> - 最小ネットマスク長が /28 の CIDR を持つ IPAM とパブリック IPv4 IPAM プールを作成します。
> - HCX Manager および HCX Interconnect (HCX-IX) アプライアンスの IPAM プールから少なくとも 2 つの Elastic IP アドレス (EIPs) を割り当てます。デプロイする必要がある HCX ネットワークアプライアンスごとに追加の Elastic IP アドレスを割り当てます。
> - パブリック IPv4 CIDR ブロックを追加の CIDR として VPC に追加します。

詳細については、「the section called “HCX インターネット接続のセットアップ”」を参照してください。

HCX VLAN サブネットのステータスを確認する

VLAN は、標準の Amazon EVS デプロイの一部として HCX 用に作成されます。HCX VLAN サブネットが正しく設定されていることを確認するには、次の手順に従います。

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションペインで [Environments (環境)] を選択します。
3. Amazon EVS 環境を選択します。
4. ネットワークと接続タブを選択します。
5. VLANs で HCX VLAN を識別し、状態が作成され、パブリックが true であることを確認します。

AWS CLI

1. 環境の環境 ID とリソースを含むリージョン名を使用して、次のコマンドを実行します。

```
aws evs list-environment-vlans  --region <region-name> --environment-id env-
abcde12345
```

2. レスポンス出力で、 が functionNameの VLAN を特定しhcx、 vlanStateが CREATEDであり、 isPublic が に設定されていることを確認しますtrue。レスポンスの例を次に示します。

```
{
    "environmentVlans": [{
            "vlanId": 50,
            "cidr": "10.10.4.0/24",
            "availabilityZone": "us-east-2b",
            "functionName": "vTep",
```

```
            "subnetId": "subnet-0ce640ac79e7f4dbc",
            "createdAt": "2025-09-09T12:09:37.526000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.596000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [],
            "isPublic": false
        },
        {
            "vlanId": 80,
            "cidr": "18.97.141.240/28",
            "availabilityZone": "us-east-2b",
            "functionName": "hcx",
            "subnetId": "subnet-0f080c94782cc74b4",
            "createdAt": "2025-09-09T12:09:37.675000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.359000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [{
                    "assocationId": "eipassoc-0be981accbbdf443a",
                    "allocationId": "eipalloc-0cef80396f4a0cc24",
                    "ipAddress": "18.97.141.245"
                },
                {
                    "assocationId": "eipassoc-0d5572f66b7952e9d",
                    "allocationId": "eipalloc-003fc9807d35d1ad3",
                    "ipAddress": "18.97.141.244"
                }
            ],
            "isPublic": true
        }
    ]
}
```


HCX VLAN サブネットがネットワーク ACL に関連付けられていることを確認します。

HCX VLAN サブネットがネットワーク ACL に関連付けられていることを確認するには、次の手順に従います。ネットワーク ACL の関連付けの詳細については、「」を参照してくださいthe section called “Amazon EVS VLAN サブネットトラフィックを制御するネットワーク ACL を作成する”。

> **Important**
>
> インターネット経由で接続している場合、Elastic IP アドレスを VLAN に関連付けると、その VLAN 上のすべてのリソースに直接インターネットアクセスできます。セキュリティ要件に応じてアクセスを制限するように、適切なネットワークアクセスコントロールリストが設定されていることを確認します。

> **Important**
>
> EC2 セキュリティグループは、Amazon EVS VLAN サブネットにアタッチされている Elastic Network Interface では機能しません。Amazon EVS VLAN サブネットとの間のトラフィックを制御するには、ネットワークアクセスコントロールリスト (ACL) を使用する必要があります。

Example

Amazon VPC console

1. Amazon VPC コンソールに移動します。
2. ナビゲーションペインの [Network ACLs] を選択します。
3. VLAN サブネットが関連付けられているネットワーク ACL を選択します。
4. [サブネットの関連付け] タブを選択します。
5. HCX VLAN サブネットが関連するサブネットにリストされていることを確認します。

AWS CLI

1. `Values` フィルターの HCX VLAN サブネット ID を使用して、次のコマンドを実行します。

```
aws ec2 describe-network-acls --filters "Name=subnet-id,Values=subnet-
abcdefg9876543210"
```

2. レスポンスで正しいネットワーク ACL が返されることを確認します。

EVS VLAN サブネットがルートテーブルに明示的に関連付けられていることを確認する

Amazon EVS では、すべての EVS VLAN サブネットを VPC 内のルートテーブルに明示的に関連付ける必要があります。HCX インターネット接続の場合、HCX パブリック VLAN サブネットは、インターネットゲートウェイにルーティングする VPC 内のパブリックルートテーブルに明示的に関連付ける必要があります。明示的なルートテーブルの関連付けを確認するには、次の手順に従います。

Example

Amazon VPC console

1. VPC コンソールに移動します。
2. ナビゲーションペインで、[Route tables] (ルートテーブル) を選択します。
3. EVS VLAN サブネットを明示的に関連付けるルートテーブルを選択します。
4. [サブネットの関連付け] タブを選択します。
5. 明示的なサブネットの関連付けで、すべての EVS VLAN サブネットがリストされていることを確認します。VLAN サブネットがここにリストされていない場合、VLAN サブネットはメインルートテーブルに暗黙的に関連付けられます。Amazon EVS が正しく機能するには、すべての VLAN サブネットをルートテーブルに明示的に関連付ける必要があります。HCX パブリック VLAN サブネットには、インターネットゲートウェイをターゲットとするパブリックルートテーブルが関連付けられている必要があります。この問題に対処するには、サブネットの関連付けを編集を選択し、欠落している VLAN サブネット (複数可) を追加します。

AWS CLI

1. ターミナルセッションを開きます。
2. 次のコマンド例を実行して、ルートテーブルの関連付けなど、すべての EVS VLAN サブネットに関する詳細を取得します。VLAN サブネットがここにリストされていない場合、VLAN サブネットはメインルートテーブルに暗黙的に関連付けられます。Amazon EVS が正しく機能するには、すべての VLAN サブネットをルートテーブルに明示的に関連付ける必要があります。HCX パブリック VLAN サブネットには、インターネットゲートウェイをターゲットとするパブリックルートテーブルが関連付けられている必要があります。

```
aws ec2 describe-subnets
```

3. EVS VLAN サブネットを VPC のルートテーブルに明示的に関連付けます。以下はコマンドの例です。

```
aws ec2 associate-route-table \
--route-table-id rtb-0123456789abcdef0 \
--subnet-id subnet-01234a1b2cde1234f
```

(HCX インターネット接続の場合) EIPsが HCX VLAN サブネットに関連付けられていることを確認します。

デプロイする HCX ネットワークアプライアンスごとに、HCX パブリック VLAN サブネットに関連付けられた IPAM プールからの EIP が必要です。HCX Manager および HCX Interconnect (HCX-IX) アプライアンスの HCX パブリック VLAN サブネットには、少なくとも 2 つの EIPs を関連付ける必要があります。以下の手順に従って、必要な EIP 関連付けが存在することを確認します。

> **Important**
>
> IPAM プールから少なくとも 2 つの EIPs を HCX パブリック VLAN サブネットに関連付けると、HCX パブリックインターネット接続は失敗します。

> **Note**
>
> パブリック IPAM CIDR ブロックの最初の 2 つの EIPs または最後の EIP を VLAN サブネットに関連付けることはできません。これらの EIPsは、ネットワーク、デフォルトゲートウェイ、ブロードキャストアドレスとして予約されています。これらの EIPs を VLAN サブネットに関連付けると、Amazon EVS は検証エラーをスローします。

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションメニューで、環境を選択します。
3. 環境を選択します。
4. ネットワークと接続タブで、HCX パブリック VLAN を選択します。

5. EIP の関連付けタブをチェックして、EIPsが HCX パブリック VLAN に関連付けられていることを確認します。

AWS CLI

1. HCX VLAN サブネットに関連付けられている EIPs を確認するには、 `list-environment-vlans` コマンドを使用します。では`environment-id`、HCX VLAN を含む EVS 環境の一意の ID を使用します。

```
aws evs list-environment-vlans \
  --environment-id "env-605uove256" \
```

コマンドは、EIP の関連付けなど、VLANs に関する詳細を返します。


```
{
  "environmentVlans": [
    {
      "vlanId": 80,
      "cidr": "18.97.137.0/28",
      "availabilityZone": "us-east-2c",
      "functionName": "hcx",
      "subnetId": "subnet-02f9a4ee9e1208cfc",
      "createdAt": "2025-08-26T22:15:00.200000+00:00",
      "modifiedAt": "2025-08-26T22:20:28.155000+00:00",
      "vlanState": "CREATED",
      "stateDetails": "VLAN successfully created",
      "eipAssociations": [
        {
          "associationId": "eipassoc-09876543210abcdef",
          "allocationId": "eipalloc-0123456789abcdef0",
          "ipAddress": "18.97.137.3"
        },
        {
          "associationId": "eipassoc-12345678901abcdef",
          "allocationId": "eipalloc-1234567890abcdef1",
          "ipAddress": "18.97.137.4"
        },
        {
          "associationId": "eipassoc-23456789012abcdef",
          "allocationId": "eipalloc-2345678901abcdef2",
          "ipAddress": "18.97.137.5"
```

```
        }
      ],
      "isPublic": true,
      "networkAclId": "acl-0123456789abcdef0"
    },
    ...
  ]
}
```

`eipAssociations` 配列には、以下を含む EIP の関連付けが表示されます。

- `associationId` - この EIP 関連付けの一意の ID。
- `allocationId` - 関連付けられた Elastic IP アドレスの割り当て ID。
- `ipAddress` - VLAN に割り当てられた IP アドレス。

HCX パブリックアップリンク VLAN ID を使用して分散ポートグループを作成する

vSphere Client インターフェイスに移動し、「分散ポートグループを追加する」の手順に従って、分散ポートグループを vSphere 分散スイッチに追加します。

vSphere Client インターフェイス内でフェイルバックを設定するときは、uplink1 がアクティブなアップリンクであり、uplink2 がアクティブ/スタンバイフェイルオーバーを有効にするスタンバイアップリンクであることを確認します。vSphere Client インターフェイスの VLAN 設定で、以前に特定した HCX VLAN ID を入力します。

(オプション) HCX WAN 最適化を設定する

> **Note**
>
> WAN 最適化機能は HCX 4.11.3 では使用できなくなりました。詳細については、HCX 4.11.3 リリースノートを参照してください。

HCX WAN Optimization Service (HCX-WO) は、データ削減や WAN パスコンディショニングなどの WAN 最適化手法を適用することで、プライベートラインやインターネットパスのパフォーマンス特性を向上させます。HCX WAN 最適化サービスは、移行に 10Gbit パスを専念できないデプロイに推奨されます。10Gbit では、WAN 最適化を使用した低レイテンシーのデプロイでは、移行パフォーマ

ンスが向上しない場合があります。詳細については、VMware HCX デプロイに関する考慮事項とベストプラクティス」を参照してください。

HCX WAN 最適化サービスは、HCX WAN Interconnect Service Appliance (HCX-IX) と組み合わせてデプロイされます。HCX-IX は、エンタープライズ環境と Amazon EVS 環境間のデータレプリケーションを担当します。

Amazon EVS で HCX WAN 最適化サービスを使用するには、HCX VLAN サブネットで分散ポートグループを使用する必要があります。前のステップで作成した分散ポートグループを使用します。

(オプション) HCX モビリティ最適化ネットワーキングを有効にする

HCX Mobility Optimized Networking (MON) は、HCX Network Extension Service の機能です。MON 対応のネットワーク拡張機能は、Amazon EVS 環境内で選択的ルーティングを有効にすることで、移行された仮想マシンのトラフィックフローを向上させます。MON を使用すると、レイヤー 2 ネットワークを拡張するときにワークロードトラフィックを Amazon EVS に移行するための最適なパスを設定し、ソースゲートウェイを通過する長いラウンドトリップネットワークパスを回避できます。この機能は、すべての Amazon EVS デプロイで使用できます。詳細については、VMware HCX ユーザーガイドの「モビリティ最適化ネットワーキングの設定」を参照してください。

Important

HCX MON を有効にする前に、HCX Network Extension の以下の制限とサポートされていない設定を確認してください。
Network Extension の制限と制限
モビリティ最適化ネットワーキングトポロジーの制限と制限

Important

HCX MON を有効にする前に、NSX インターフェイスで送信先ネットワーク CIDR のルート再分散が設定されていることを確認してください。詳細については、VMware NSX ドキュメントの「Configure BGP and Route Redistribution」を参照してください。

HCX 接続の検証

VMware HCX には、接続のテストに使用できる診断ツールが組み込まれています。詳細については、VMware HCX ユーザーガイドの「VMware HCX のトラブルシューティング」を参照してください。 VMware

HCX パブリックインターネット接続を設定する

Elastic IP アドレスを VLAN に関連付けることで、HCX パブリック VLAN のパブリックインターネットアクセスを設定できます。これにより、移行オペレーションにインターネットアクセスを必要とする VMware HCX アプライアンスとワークロードの直接インターネット接続が可能になります。

関連トピック

このトピックでは、HCX パブリック VLAN のインターネットアクセスの管理について説明します。完全な実装の場合:

1. の前提条件を完了しますAmazon Elastic VMware Service のセットアップ。
2. で初期設定を設定します開始方法。
3. インターネットアクセスを設定します (このトピック) 。

HCX VLAN インターネットアクセスについて

VMware HCX アプライアンスのインターネットアクセスを設定して、インターネット経由でワークロードを Amazon EVS に HCX 移行できます。

このアプローチ:

- 専用プライベート接続を必要とせずに仮想マシンの移行を有効にします。
- 柔軟でコスト効率の高い移行ソリューションを提供します。

> **Important**
>
> HCX インターネットベースの移行は、通常、以下には推奨されません。
>
> - ネットワークのジッターやレイテンシーの影響を受けやすいアプリケーション。
> - タイムクリティカルな vMotion オペレーション。

- 厳格なパフォーマンス要件を持つ大規模な移行。

これらのシナリオでは、HCX プライベート接続を使用することをお勧めします。プライベート専用接続は、インターネットベースの接続よりも信頼性の高いパフォーマンスを提供します。

インターネット接続の概要

以下の考慮事項を確認してください。

HCX ネットワーク要件と DNAT

HCX には、パブリックインターネットアクセスの設定方法に影響する特定のネットワーク制約があります。

HCX は送信先ネットワークアドレス変換 (DNAT) をサポートしていません。代わりに、HCX では、アップリンクネットワークがデフォルトのゲートウェイ IP アドレスでルーティング可能である必要があります。

Amazon EVS VLAN サブネットには、他の VPC サブネットと同様にデフォルトのゲートウェイ IP アドレスが含まれています。ただし、RFC1918 アドレス範囲外の CIDR ブロックを使用している場合でも、これらのサブネットは常にプライベートサブネットです。

HCX インターネット接続の有効化

DNAT なしでインターネット接続を有効にするために、Amazon EVS は特定の CIDR 設定アプローチを使用します。

- インターネットルーティング可能な CIDR 要件: Amazon EVS には、HCX VLAN サブネット CIDR に一致するインターネットルーティング可能な CIDR が必要です。
- IPAM 割り当て: Amazon EVS は、インターネットルーティング可能な CIDR として、最小ネットマスク長 /28 のパブリック IPAM 割り当て CIDR を使用します。
- VPC 設定: パブリック IPAM 割り当て CIDR をセカンダリ VPC CIDR として VPC に手動で追加する必要があります。
- VLAN サブネットのデプロイ: IPAM と VPC を設定したら、Amazon EVS のデプロイ中に HCX VLAN サブネットでパブリック IPAM 割り当て CIDR を使用できます。

- Elastic IP 設定: Amazon EVS には次の設定が必要です。
  - Elastic IPs を割り当てる: IPs に割り当てられた CIDR から Elastic IP を割り当てます。HCX Manager および HCX Interconnect (HCX-IX) アプライアンスの IPAM プールから少なくとも 2 つの Elastic IP アドレス (EIPs) を割り当てる必要があります。デプロイする必要がある HCX ネットワークアプライアンスごとに追加の Elastic IP アドレスを割り当てます。
  - VLAN に関連付ける: HCX アプライアンスで使用する各 Elastic IP を HCX VLAN サブネットに関連付けます。この関連付けには、Amazon EVS コンソールまたは AWS CLI を使用します。
  - ゲートウェイアドレスの設定: CIDR から最初に使用できるアドレスは、HCX アプライアンスで設定したゲートウェイアドレスになります。
  - トラフィックルーティング: 関連付けられた各 Elastic IP のトラフィックは、同じ IP アドレスを持つ送信先 HCX アプライアンスに直接ルーティングされ、DNAT は使用されません。

Amazon EVS 環境デプロイのインターネット接続で HCX を設定する手順については、Amazon Elastic VMware Service のセットアップ「」および「」を参照してください開始方法。

オペレーションに関する考慮事項

- HCX パブリック VLAN CIDR ブロックのネットマスク長は /28 である必要があります。
- EIPsは、Amazon EVS コンソールまたは を使用してデプロイした後、HCX パブリック VLAN に関連付けることも、HCX パブリック VLAN から関連付けを解除することもできますが AWS CLI、同じ IPAM プールから取得する必要があります。
- 各 EIP 関連付けには、独自の一意の関連付け ID があります。
- /28 HCX パブリック VLAN に関連付けられたパブリック IPAM プールから最大 13 個の EIPs を持つことができます。パブリック IPAM 割り当て CIDR ブロックの最初の 2 つの EIPs または最後の EIP を HCX パブリック VLAN サブネットに関連付けることはできません。これらの EIPsは、ネットワーク、デフォルトゲートウェイ、ブロードキャストアドレスとして予約されています。これらの EIPs を VLAN に関連付けると、Amazon EVS は検証エラーをスローします。

セキュリティに関する考慮事項

- ネットワークアクセスコントロールリスト (ACLs) は、HCX パブリック VLAN サブネットを通過するトラフィックにも適用されます。
- セキュリティグループルールは、HCX パブリック VLAN サブネット上のトラフィックには適用されません。トラフィック制御ACLs を使用します。

> **Important**
>
> インターネット経由で接続している場合、Elastic IP アドレスを VLAN に関連付けると、その VLAN 上のすべてのリソースに直接インターネットアクセスできます。セキュリティ要件に応じてアクセスを制限するように、適切なネットワークアクセスコントロールリストが設定されていることを確認します。

VLANs の Elastic IP アドレスの管理

Amazon EVS コンソールまたは を使用して、Elastic IP アドレスと HCX パブリック VLAN の関連付けと関連付け解除を行うことができます AWS CLI。

> **Note**
>
> Amazon EVS は、現時点では Elastic IP アドレスと HCX パブリック VLAN の関連付けと関連付け解除のみをサポートしています。

Elastic IP アドレスを VLAN に関連付ける

前提条件

以下があることを確認します。

- Elastic IP アドレスは、Amazon 所有のパブリック IPAM プールから割り当てられます。
- Amazon EVS 環境はすでに作成されています。

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションメニューで、環境を選択します。
3. 環境を選択します。
4. ネットワークと接続タブで、HCX パブリック VLAN を選択します。

> **Note**
>
> Amazon EVS は、現時点では EIPs HCX VLAN の関連付けのみをサポートしています。

5. EIP を VLAN に関連付けるを選択します。
6. HCX パブリック VLAN に関連付ける Elastic IP アドレス (複数可) を選択します。
7. EIPs関連付けを選択します。HCX パブリック VLAN には、最大 13 EIPs を関連付けることができます。

> **Note**
>
> パブリック IPAM CIDR ブロックの最初の 2 つの EIPs を VLAN サブネットに関連付けることはできません。これらの EIPsは、ネットワークおよびデフォルトのゲートウェイアドレスとして予約されています。

8. EIP の関連付けをチェックして、EIPsが HCX パブリック VLAN に関連付けられていることを確認します。

AWS CLI

1. Elastic IP アドレスを VLAN に関連付けるには、 `associate-eip-to-vlan` コマンド例を使用します。
   - `environment-id` - Amazon EVS 環境の ID。
   - `vlan-name` - である必要がありますhcx。Amazon EVS は、現時点では HCX VLAN との EIP 関連付けのみをサポートしています。
   - `allocation-id` - Elastic IP アドレスの割り当て ID。

   ```
   aws evs associate-eip-to-vlan \
     --environment-id "env-605uove256" \
     --vlan-name "hcx" \
     --allocation-id "eipalloc-0429268f30c4a34f7"
   ```

   コマンドは、新しい EIP 関連付けなど、VLAN に関する詳細を返します。

   ```
   {
   ```

```
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [
            {
                "associationId": "eipassoc-09e966faad7ecc58a",
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```


`eipAssociations` 配列には、以下を含む新しい関連付けが表示されます。

- `associationId` - この EIP 関連付けの一意の ID。関連付け解除に使用されます。
- `allocationId` - 関連付けられた Elastic IP アドレスの割り当て ID。
- `ipAddress` - VLAN に割り当てられた IP アドレス。

2. ステップを繰り返して、追加の EIPs。HCX パブリック VLAN には、最大 13 EIPs を関連付けることができます。

VLAN から Elastic IP アドレスの関連付けを解除する

前提条件

以下があることを確認します。

- Amazon EVS 環境はすでに作成されています。
- EIP は Amazon EVS 環境に関連付けられています。

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションメニューで、環境を選択します。
3. 環境を選択します。
4. ネットワークと接続タブで、HCX パブリック VLAN を選択します。
5. VLAN から EIP の関連付けを解除を選択します。
6. HCX パブリック VLAN との関連付けを解除する Elastic IP アドレス (複数可) を選択します。

> **Important**
>
> EIPs関連付けを解除すると、パブリック VLAN サブネットを使用するアプライアンスのインターネット接続が失われる可能性があります。

7. EIPs。
8. EIP の関連付けをチェックして、EIPsが HCX パブリック VLAN から関連付け解除されていることを確認します。

AWS CLI

VLAN から Elastic IP アドレスの関連付けを解除するには、 `disassociate-eip-from-vlan` コマンド例を使用します。

- `environment-id` - Amazon EVS 環境の ID。
- `vlan-name` - である必要がありますhcx。Amazon EVS は、現時点では HCX VLAN との EIP 関連付けのみをサポートしています。
- `association-id` - 削除する EIP 関連付けの関連付け ID。

> **Important**
>
> EIPs関連付けを解除すると、パブリック VLAN サブネットを使用するアプライアンスのインターネット接続が失われる可能性があります。

```
aws evs disassociate-eip-from-vlan \
  --environment-id "env-605uove256" \
  --vlan-name "hcx" \
  --association-id "eipassoc-09e966faad7ecc58a"
```

コマンドは、EIP 関連付けが削除された VLAN に関する詳細を返します。


```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:48:49.846000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```


空の`eipAssociations`配列は、Elastic IP アドレスと VLAN の関連付けが正常に解除されたことを確認します。

インターネットベースの移行のための HCX WAN 最適化について

> **Note**
>
> WAN 最適化機能は HCX 4.11.3 では使用できなくなりました。詳細については、HCX 4.11.3 リリースノートを参照してください。

インターネット経由で移行を実行する場合、HCX WAN Optimization (HCX-WO) は移行パフォーマンスを向上させることができます。このサービスは、HCX Interconnect Appliance (HCX-IX) と連携して以下のことを行います。

- データ削減手法を適用して、帯域幅の使用量を最小限に抑えます。
- WAN パスコンディショニングを実装してネットワークパフォーマンスを最適化します。
- 高レイテンシーのインターネット接続による移行速度の向上。
- インターネットベースの移行の信頼性を向上させます。

HCX WAN 最適化は、インターネットベースの移行で特に役立ちます。

- ネットワークレイテンシーは、プライベート接続オプションよりも高い場合があります。
- 使用可能な帯域幅は制限または可変である場合があります。
- インターネットトラフィックパターンにより、ネットワークの状態が変動することがあります。

インターネット接続の設定後に HCX WAN 最適化を設定する詳細な手順については、「」を参照してくださいthe section called “(オプション) HCX WAN 最適化を設定する”。

> **Note**
>
> WAN 最適化はインターネットベースの移行パフォーマンスを大幅に向上させることができますが、専用の 10Gbit で低レイテンシーの接続を使用する環境では、追加の利点が得られない場合があります。この機能を有効にするかどうかを決定するときは、ネットワークの特性を考慮してください。

Amazon EVS 環境の管理

この章には、環境の管理に役立つ以下のトピックが含まれています。

- the section called “VCF サブスクリプション” - VCF サブスクリプションが Amazon EVS とどのように連携するか、および VCF サブスクリプション管理に関するお客様の責任について説明します。
- the section called “VCF バージョンと EC2 インスタンス” - サポートされている VCF および ESX バージョンと、Amazon EVS でバージョンの可用性を確認する方法について説明します。
- the section called “ライフサイクル管理” - 基盤となるインフラストラクチャ管理、VPC アップグレード管理、ESX ホストライフサイクル管理など、Amazon EVS 環境内のライフサイクル管理の責任について説明します。
- the section called “環境メンテナンス” - ネットワーク設定、ESX ホストのメンテナンス、環境ステータスの確認、VPC 認証情報のシークレットローテーションスケジュールの管理など、Amazon EVS 環境の一般的なメンテナンスタスクを実行する方法について説明します。
- the section called “ホストの作成” - 環境がデプロイされた後に Amazon EVS ホストを作成し、そのホストをクラスターに追加する方法について説明します。
- the section called “ホストの削除” - Amazon EVS ホストを削除し、クラスターから削除する方法について説明します。

VCF サブスクリプション

> **Note**
>
> Amazon EVS は、永続的な vSphere ライセンスをサポートしていません。Amazon EVS を使用するには、有効でアクティブな VMware Cloud Foundation サブスクリプションが必要です。

Amazon EVS は、VMware Cloud Foundation (VCF) サブスクリプションと AWS 、(BYOS) に持ち込むライセンス移植資格を使用します。Amazon EVS 環境を正常にデプロイするには、環境作成リクエストで有効な VCF ソリューションキーと vSAN ライセンスキーを指定する必要があります。vSphere ライセンスキーは VCF のソリューションキーとして機能します。各 VCF ライセンスキーは、1 つの Amazon EVS 環境にのみ使用できます。別の環境で既に使用されている VCF ライセンスキーを使用しようとすると、環境の作成は失敗します。

VCF ソリューションキーには、Amazon EVS が環境の作成時にデプロイする 4 つの初期 EC2 i4i.metal ホストに適切なコア容量を提供するために、少なくとも 256 コアが必要です。各 i4i.metal ホストには 64 コアが必要です。vSAN ライセンスキーには、少なくとも 110 TiB の vSAN 容量が必要です。サイズが小さいライセンスキーを使用しようとすると、環境の作成は失敗します。

> **Note**
>
> VCF サブスクリプションは、ライセンスコンプライアンスのためにすべての AWS リージョンで Amazon EVS で利用できます。Amazon EVS はライセンスキーを検証しません。ライセンスキーを検証するには、Broadcom サポートにアクセスしてください。

> **Note**
>
> Amazon EVS の VCF ソフトウェアに関する情報は、ライセンスコンプライアンスを確認するために Broadcom と共有されます。

サブスクリプションの管理

VCF サブスクリプションの管理はお客様の責任となります。VCF サブスクリプションは SDDC Manager で管理する必要があります。SDDC Manager からライセンスキーを削除するか、使用中のライセンスキーに置き換えると、環境ステータスチェックが失敗し、Amazon EVS 環境にホストを追加できなくなります。環境ステータスチェックの詳細については、the section called “環境ステータスのモニタリング”「」および「」を参照してくださいthe section called “失敗した環境ステータスチェックのトラブルシューティング”。VCF ライセンスキーの詳細については、VMware Cloud Foundation ドキュメントの「VMware Cloud Foundation でのライセンスキーの管理」を参照してください。 VMware

> **Important**
>
> SDDC Manager ユーザーインターフェイスを使用して、VPC ソリューションと vSAN ライセンスキーを管理します。Amazon EVS では、サービスが正しく機能するためには、有効な VCF ソリューションと vSAN ライセンスキーを SDDC Manager に維持する必要があります。vSphere Client を使用してホストと vSAN クラスターにキーを割り当てる必要がありますが、これらのキーが SDDC Manager ユーザーインターフェイスのライセンス画面にも表示されることを確認する必要があります。

VCF ライセンスキーの追加

Broadcom サポートポータルでは、追加の VCF ライセンスキーを購入したり、既に大きなキーがある場合はライセンスキーを分割したり、複数のライセンスキーをマージしたりできます。これにより、最初のデプロイ後に環境に追加したホストをライセンスしたり、追加の環境をライセンスしたりできます。購入したライセンスキーが vCenter Sever および SDDC Manager インベントリに追加されていることを確認します。ホストを追加する場合は、ライセンスが vSphere の適切なホストに割り当てられ、適切なコアと vSAN ストレージ容量があることを確認してください。Amazon EVS は、ライセンスのないホストをサポートしていません。詳細については、VMware ドキュメントの vSphere クライアントの「アセットのライセンス設定の設定」を参照してください。

ライセンスキーの評価期間が終了する前に、有効期限が切れていない新しいライセンスキーを vCenter Server に割り当てる必要があります。Amazon EVS 環境を正常にセットアップするには、アクティブなライセンスキーが必要です。期限切れのライセンスキーが指定されている場合、環境はデプロイに失敗します。VCF ライセンスキーの作成の詳細については、VMware ドキュメントの「新しいライセンスの作成」を参照してください。追加されたライセンスキーに問題がある場合は、「」を参照してくださいthe section called “キーカバレッジチェックに失敗しました”。

VCF ライセンスキーの削除

環境内のホストを削除した後、SDDC Manager インベントリから VCF ライセンスキーを削除して、コア容量と vSAN 容量を減らすことができます。vSphere で使用する製品のライセンスモデルに準拠し続けるには、割り当てられていないライセンスキーをすべてインベントリから削除する必要があります。Broadcom サポートポータルでライセンスキーを分割、マージ、またはアップグレードした場合は、古いライセンスキーを削除する必要があります。詳細については、VMware ドキュメントの「ライセンスの削除」を参照してください。

Amazon EVS が提供する VCF バージョンと EC2 インスタンスタイプ

Amazon EVS は、VMware Cloud Foundation (VCF)、ESX、EC2 インスタンスタイプの複数のバージョンを提供しており、環境の作成時およびホストの作成時に選択できます。

提供されている VCF バージョン、ESX バージョン、および EC2 インスタンスタイプのチェック

AWS コンソールには、Amazon EVS が提供する VCF バージョンのリストが環境作成ウィザードに表示されます。使用可能な ESX バージョンは、既存の環境へのホストの追加中にインスタンスタイ

プを選択すると表示されます。CLI を使用して VCF バージョン、ESX バージョン、EC2 インスタンスタイプを表示することもできます。

Example

Amazon EVS console

1. Amazon EVS コンソールに移動します。
2. ナビゲーションメニューで、環境を選択します。
3. 次のいずれかを行います。

   VCF バージョンを確認するには:

   a. 環境の作成 を選択します。

   b. Amazon EVS の検証要件で、VPC バージョンを選択して、ステータスが使用可能か制限されているかを確認します。

   ESX バージョンを確認するには:

   a. 既存の環境を選択します。

   b. [Create host] (ホストの作成) を選択します。

   c. インスタンスタイプを選択すると、使用可能な ESX バージョンが表示されます。

AWS CLI

次のコマンドを実行して、VPC および ESX バージョンに関する情報を取得します。

```
aws evs get-versions --region <region-name>
```

レスポンスの例:

```
{
   "instanceTypeEsxVersions": [
      {
         "esxVersions": [ "ESXi-8.0U3b-24280767","ESXi-8.0U3g-24859861" ],
         "instanceType": "i4i.metal"
      }
   ],
   "vcfVersions": [
      {
```

```
            "vcfVersion": "VCF-5.2.1",
            "status": "RESTRICTED",
            "defaultEsxVersion": "ESXi-8.0U3b-24280767",
            "instanceTypes": ["i4i.metal"]
      },
      {
            "vcfVersion": "VCF-5.2.2",
            "status": "AVAILABLE",
            "defaultEsxVersion": "ESXi-8.0U3g-24859861",
            "instanceTypes": ["i4i.metal"]
      }
   ]
}
```

> **Note**
>
> 必要なバージョンに が表示されRESTRICTED、特定のニーズがある場合は、そのバージョンへのアクセス方法の詳細については、the section called “制限付き VCF バージョンへのアクセスのリクエスト”「」を参照してください。

Amazon EVS の現在の VCF バージョン

Amazon EVS は現在、環境作成用に次の VCF バージョンを提供しています。

VCF バージョン	デフォルトの ESX バージョン	ステータス	EC2 インスタンスタイプ
VCF-5.2.2	ESXi-8.0U3g-24859861	利用可能	i4i.metal
VCF-5.2.1	ESXi-8.0U3b-24280767	制限付き	i4i.metal

> **Note**
>
> 新しい Amazon EVS 環境を作成するときは、VPC バージョンを指定する必要があります。

ESX バージョンに関する考慮事項

各 VCF バージョンには、Broadcom VCF 部品表 (BOM) に基づくデフォルトの ESX バージョンがあります。新しい環境を作成するときに、特定の ESX バージョンを選択することはできません。選択した VCF バージョンのデフォルトの ESX バージョンが自動的に適用されます。

ただし、ホストを環境に追加するときは、選択したインスタンスタイプに使用可能な ESX バージョンを選択できます。指定しない場合、Amazon EVS は環境の VCF バージョンに関連付けられたデフォルトの ESX バージョンを使用します。

ホストが追加されると、その ESX バージョンは vCenter Lifecycle Manager を使用してのみアップグレードできます。

> **Note**
>
> Amazon EVS は、Broadcom によってリリースされた VCF および ESX のすべてのバージョンを提供するわけではありません。ソフトウェアの相互運用性については、「Broadcom Interoperability Matrix」を参照してください。 AWS EC2 インスタンスとのハードウェアの完全な互換性については、Broadcom 互換性ガイドを参照してください。

制限付き VCF バージョンへのアクセスのリクエスト

`RESTRICTED` ステータスが の VCF バージョンにアクセスする必要がある場合は、以下の情報を AWS サポートにお問い合わせください。

- AWS アカウント ID
- AWS リージョン
- 必要な特定の VCF バージョン
- ユースケースとビジネス上の根拠 (セキュリティ/コンプライアンス、互換性/依存関係など)

AWS サポートはリクエストを確認し、追加情報を承認またはリクエストします。承認後、 AWS コンソールまたは `get-versions` API レスポンス`AVAILABLE`でバージョンステータスが に変わります。

Amazon EVS 環境ライフサイクル管理

このページでは、Amazon EVS 環境におけるライフサイクル管理の責任について説明します。

Amazon EVS の主な利点は、クラウド内の VMware アーキテクチャを完全に制御できることです。VMware Cloud Foundation (VCF) ソフトウェアスタックを最適化して、アプリケーションの固有の需要に対応できます。Amazon EVS はセルフマネージドサービスであるため、ESX、vSphere、vSAN、NSX、SDDC Manager など、Amazon EVS 環境で使用される VMware ソフトウェアのライフサイクル管理とメンテナンスはお客様の責任となります。また、Amazon EVS ホストに統合するデータ保護ソリューションなど、サードパーティーの統合を維持する責任もあります。

VPC ルートテーブル、セキュリティグループと AWS ネットワークアクセスコントロールリスト (ACL) ルール、VPC ルートサーバー設定、インターネットゲートウェイ、NAT ゲートウェイ、トランジットゲートウェイ (オンプレミス接続用) など、Amazon EVS が使用する基盤となるネットワークコンポーネントの設定は、お客様の責任となります。

AWS は、指定したネットワーク設定を使用して Amazon EVS 環境をデプロイする責任があります。環境デプロイには以下が含まれます。

- Amazon EVS 環境のネットワーク設定のブートストラップ。
- 指定した VPC Route Server インスタンスで南北ルーティングを有効にします。
- 必要な EVS VLAN サブネット、Elastic Network Interface、4 つの初期 ESX ホストをデプロイします。
- Tier-0 ゲートウェイと Tier-1 ゲートウェイを使用した NSX オーバーレイネットワークの設定。
- アクティブ/スタンバイモードで 2 つの NSX Edge ノードを持つ NSX Edge クラスターをデプロイします。
- 初期 vSAN クラスターを作成して設定し、データストアをマウントします。

ネットワークセグメント、分散ファイアウォールルール、ロードバランサーなど、VMware NSX の設定はお客様の責任となります。また、VMware HCX 設定や追加の NSX Tier-1 ゲートウェイなど、EVS 環境のデプロイ後に Amazon EVS で実装する統合ソリューションの設定についても責任を負います。

AWS とお客様の責任の詳細については、AWS 「 責任共有モデル」を参照してください。

> **Note**
>
> Tier-0 ゲートウェイと Tier-1 ゲートウェイは、Amazon EVS 環境デプロイの一部として作成および設定されます。Amazon EVS は、現時点では 1 つの Tier-0 ゲートウェイのみをサポー

トしています。これらの論理ルーターまたは NSX エッジノード VMs を変更すると、接続に影響する可能性があるため、避けてください。

VMware ソフトウェアの更新

> **Warning**
>
> Amazon EVS 環境のデプロイ後に ESX バージョンを更新した場合、コミッションホストステップの VCF ホストの検証中に SDDC マネージャーが失敗することがあります。この問題のトラブルシューティング手順については、「」を参照してくださいthe section called “SDDC Manager がホストコミッショニング中に VCF ホストの検証に失敗する”。

Amazon EVS が提供する VCF バージョンの詳細については、「」を参照してくださいthe section called “VCF バージョンと EC2 インスタンス”。AWS 責任共有モデルでは、ESX、vCenter Server、vSAN、NSX、SDDC Manager、その他の統合ソリューションを含む VCF ソフトウェアに EVS 環境でパッチ、更新、アップグレードを適用する責任があります。デプロイ後、Amazon EVS によってデプロイされた VCF ソフトウェアバージョンを確認し、必要に応じて更新することをお勧めします。VCF の更新は、Broadcom サポートポータルから取得できます。また、更新とパッチの定期的なメンテナンススケジュールを確立して遵守することをお勧めします。

> **Note**
>
> Amazon EVS は、現時点では VMware Cloud Foundation 9 をサポートしていません。

> **Note**
>
> Amazon EVS は、Broadcom によってリリースされた VCF および ESX のすべてのバージョンを提供するわけではありません。ソフトウェアの相互運用性については、「Broadcom Interoperability Matrix」を参照してください。 AWS EC2 インスタンスとのハードウェアの完全な互換性については、Broadcom 互換性ガイドを参照してください。

特定のパッチ、更新、またはアップグレードは、環境で実行されているワークロードに影響を与える可能性があります。VCF ソフトウェアにパッチを適用、更新、またはアップグレードする前

に、VPC ライフサイクル管理ガイドを確認して、これらの変更が環境にどのように影響するかを理解しておくことをお勧めします。また、本番環境にデプロイする前に、ステージング環境で変更をテストすることをお勧めします。VCF 5.2.x リリースノートを確認して、最新の VCF 5.2.x の更新を理解できます。

ESX ホストのライフサイクルとメンテナンス

お客様は、ホストの状態のモニタリングやホストの問題の修復など、Amazon EVS 環境内の ESX ホストライフサイクルの管理とメンテナンスを担当します。詳細については、「the section called “環境メンテナンス”」を参照してください。

AWS は、基盤となる i4i.metal EC2 インスタンスでスケジュールされたメンテナンスを実行し、インフラストラクチャの信頼性、可用性、パフォーマンスを確保します。詳細については、「the section called “EC2 インスタンスのスケジュール AWS されたメンテナンスについて”」を参照してください。

環境でのメンテナンスの実行

このセクションでは、Amazon EVS 環境で一般的なメンテナンスタスクを実行する方法について説明します。

トピック

- 環境のステータスとリソースをモニタリングする
- AMI メンテナンス
- Amazon EVS ホストのメンテナンス
- Amazon EVS サブネットのカスタムルートテーブルを設定する
- Amazon EVS VLAN サブネットトラフィックを制御するようにネットワークアクセスコントロールリストを設定する
- シークレット管理ライフサイクル

環境のステータスとリソースをモニタリングする

Amazon EVS コンソールまたは を使用して、Amazon EVS 環境と基盤となる AWS リソースのさまざまな側面をモニタリングできます AWS CLI。

> **Note**
>
> VMware Cloud Foundation (VCF) コンポーネントは SDDC Manager でモニタリングされます。Amazon EVS コンソールまたは を使用して VCF コンポーネントをモニタリングすることはできません AWS CLI。SDDC Manager を使用して VMware Cloud Foundation (VCF) コンポーネントをモニタリングする方法については、「SDDC Manager の開始方法」を参照してください。

環境のステータスとリソースを表示する

環境ステータスは、環境で注意が必要な問題が発生しているかどうかを判断するのに役立ちます。以下の手順に従って、環境のステータスを確認し、基盤となるリソースを表示します。

Example

Amazon EVS console

1. Amazon EVS コンソールを開きます。
2. ナビゲーションペインで [Environments (環境)] を選択します。
3. 環境 ID を選択して、環境の詳細ページを開きます。
4. 詳細 で、環境ステータスを表示します。

   環境が正常であれば、ステータスは合格と表示されます。問題がある場合、ステータスは「失敗」と表示されます。ステータスが Failed の場合、4 つの環境ステータスチェックの結果を示すポップオーバーを表示できます。

   - キーの再利用 - VCF ライセンスキーが有効かどうかを示すために合格または不合格を表示します。
   - ホスト数 - ホスト接続のステータスを示すために不明、合格、または失敗を示します。
   - キーカバレッジ - VCF ライセンスキーがすべてのホストをカバーしているかどうかを示す合格または不合格を表示します。
   - 到達可能性 - SDDC Manager の到達可能性を示すために合格または不合格を示します。

   環境ステータスチェックの失敗のトラブルシューティングについては、「」を参照してくださいトラブルシューティング。

   環境内のリソースを表示するには

次のいずれかのタブを選択します。

- ホスト - 環境内のホストを表示します。
- ネットワークと接続 - 環境に関連付けられた VPC、EVS サブネット、VPC Route Server リソースを表示します。
- 管理アプライアンス - 環境内の VCF 管理アプライアンスを DNS ホスト名と関連認証情報とともに表示します。
- タグ - 環境に関連付けられているタグを表示します。

AWS CLI

を使用して AWS CLI 、環境のステータスとリソースを確認できます。

すべての環境とそのステータスを一覧表示するには

```
aws evs list-environments
```

> **Tip**
>
> --query パラメータを使用して出力をフィルタリングします。例えば、次のようになります。

```
aws evs list-environments --query 'Environments[*].[EnvironmentId,Status]'
```

環境ホストを一覧表示するには

```
aws evs list-environment-hosts \
    --environment-id environment-id
```

環境 VLANs一覧表示するには

```
aws evs list-environment-vlans \
    --environment-id environment-id
```

API オペレーションの詳細については、Amazon EVS API リファレンスガイドの以下を参照してください。

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

AMI メンテナンス

Amazon EVS は、カスタム EVS Amazon マシンイメージ (AMI) を使用して ESX ホストをデプロイします。AMI には、Amazon EC2 で ESX を実行するために必要なパッケージを含むカスタムベンダーアドオンが含まれています。

互換性のないクラスターイメージによるホストの追加失敗のトラブルシューティング

環境にホストを追加すると、ホストには利用可能な最新バージョンの EVS カスタムベンダーアドオンがあります。環境が古いアドオンバージョンのホストを使用している場合、新しいホストの追加は失敗し、新しいホストがクラスターイメージと互換性がないというエラーが発生します。この問題を修正する詳細な手順については、「」を参照してくださいthe section called “互換性のないクラスターイメージによるホスト障害の追加”。

Amazon EVS ホストのメンテナンス

Amazon EVS はセルフマネージドサービスであるため、ホスト上で実行される VMware Cloud Foundation (VCF) ソフトウェアのメンテナンス、ホストの状態のモニタリング、ホストの障害発生時のホスト交換を含むホストの問題の修復はお客様の責任となります。VMware Cloud Foundation (VCF) での ESX ホストの管理の詳細については、VMware Cloud Foundation ドキュメントの「ホスト管理」を参照してください。

基盤となる EC2 インスタンスの正常性の確認

Amazon EC2 は稼働中のすべての EC2 インスタンスに対して自動チェックを実行して、ハードウェアおよびソフトウェアの問題を特定します。これらのステータスチェックの結果は、EC2 コンソールで表示することも、検出可能な特定の問題を特定 AWS CLI することもできます。詳細については、Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスのステータスチェックを表示する」および AWS CLI 「 コマンドラインリファレンス」のdescribe-instance-status」を参照してください。 Amazon EC2

特定のインスタンスでステータスチェックが失敗した場合に警告する CloudWatch アラームを作成できます。詳細については、Amazon EC2 ユーザーガイド」の「ステータスチェックに失敗した

Amazon EC2 インスタンスの CloudWatch アラームを作成する」を参照してください。 Amazon EC2

EC2 インスタンスのスケジュール AWS されたメンテナンスについて

AWS は、基盤となる EC2 インスタンスでスケジュールされたメンテナンスを実行し、信頼性、可用性、パフォーマンスを確保します。EC2 ベアメタルインスタンスは、他の EC2 インスタンスと同じタイプのスケジュールされたイベントの対象となります。 AWS は、基盤となるハードウェアの問題やスケジュールされたメンテナンスが原因で、インスタンスを再起動、停止、廃止するようにイベントをスケジュールできます。これらのイベントは頻繁には発生しません。詳細については、Amazon EC2 ユーザーガイド」の「スケジュールされたイベントのタイプ」を参照してください。

> **Note**
>
> スケジュールされた再起動イベントの前に、ホストを vSphere Client のメンテナンスモードにする必要があります。

スケジュールされたイベントの影響を受けるインスタンスがある場合、 は、 に関連付けられている E メールアドレスを使用して事前に E メールで AWS 通知します AWS アカウント。 は、Amazon EventBridge を使用してモニタリングおよび管理できる AWS Health イベント AWS も送信します。EventBridge 詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EventBridge による AWS Health でのイベントのモニタリング」および「Amazon EC2 インスタンスのスケジュールされたイベント」を参照してください。 Amazon EC2 Amazon EC2

いつでもイベントを再スケジュールして、都合のよい特定の日時でイベントが発生するようにすることができます。イベントはイベント期限日まで再スケジュールできます。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスのスケジュールされたイベントを再スケジュールする」を参照してください。 Amazon EC2

EC2 オンデマンドキャパシティ予約の使用

EC2 オンデマンドキャパシティ予約を使用して、メンテナンス期間中にクラスターに十分なキャパシティを確保できます。特定のアベイラビリティーゾーンの容量は、任意の期間予約できます。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 オンデマンドキャパシティ予約でコンピューティングキャパシティを予約する」を参照してください。 Amazon EC2

キャパシティ予約を作成する手順については、Amazon EC2 ユーザーガイド」の「キャパシティ予約の作成」を参照してください。

> **Note**
>
> EC2 オンデマンドキャパシティ予約または EC2 専有ホストを使用する場合は、ミッションクリティカルなワークロード用に予備のホストを保持することをお勧めします。キャパシティ予約では、特定のアベイラビリティーゾーン内の特定の量の EC2 インスタンスキャパシティーにアクセスできますが、予備のホストを使用すると、ミッションクリティカルなワークロードにとって重要な冗長性をさらに強化できます。Dedicated Hosts の場合、予備のホストがあれば、プライマリホストにメンテナンスが必要な場合や問題が発生した場合でも、ミッションクリティカルなワークロードの環境を維持できます。

AWS スケジュールされた イベント**system-maintenance**と **instance-retirement**イベントの準備

AWS は、ネットワークメンテナンスと電力メンテナンスの 2 種類のsystem-maintenanceイベントをスケジュールします。

- ネットワークメンテナンス中は短い期間、予定されたインスタンスのネットワーク接続が切断されます。メンテナンスが終了すると、インスタンスとの通常のネットワーク接続が回復します。
- 電源のメンテナンス中は短い期間、予定されたインスタンスはオフラインになり、その後再起動されます。EC2 ベアメタルインスタンスで再起動を実行すると、インスタンスストアボリュームデータは保持されません。

AWS EC2 インスタンスをホストする基盤となるハードウェアの劣化が検出されると、 は EC2 instance-retirementイベントをスケジュールします。

system-maintenance および instance-retirementイベントを修正するには、メンテナンスイベントが発生する前に、Amazon EVS コンソールまたは AWS CLI SDDC Manager を使用して、障害が発生したホストを新しいホストに置き換えます。メンテナンスイベントが発生するのを待っていて EC2 インスタンスの再起動が必要な場合は、インスタンスストアボリュームに保存されている vSAN データが失われます。詳細なステップについては、「the section called “Amazon EVS ホストを置き換える”」を参照してください。

> **Important**
>
> EC2 コンソールは、停止、開始、終了など、Amazon EVS ホストの状態を管理するために使用しないでください。Amazon EVS がデプロイする EC2 インスタンスを起動、停止、または終了しようとしないでください。このアクションにより、vSAN データが失われます。

Amazon EVS ホストを置き換える

Amazon EVS ホストを置き換えるには、次の手順に従います。

> **Warning**
>
> Amazon EVS ホストは、カスタムベンダーアドオンを使用して重要なホスト機能を提供します。環境にホストを追加すると、Amazon EVS カスタムアドオンの最新バージョンが提供されます。環境が古いアドオンバージョンのホストを使用している場合、vSphere クラスターにホストを追加すると、クラスターイメージの修復が失敗します。この問題のトラブルシューティング手順については、「」を参照してくださいthe section called “互換性のないクラスターイメージによるホストの追加失敗のトラブルシューティング”。

> **Warning**
>
> デプロイ後に ESX バージョンを更新した場合、コミッションホストステップの VCF ホストの検証中に SDDC マネージャーが失敗することがあります。この問題のトラブルシューティング手順については、「」を参照してくださいthe section called “SDDC Manager がホストコミッショニング中に VCF ホストの検証に失敗する”。

> **Note**
>
> ホストが正常に作成されるように、EVS 環境クォータあたりの Amazon EVS ホスト数が正しく設定されていることを確認します。このクォータ値が単一の Amazon EVS 環境内でプロビジョニングしようとしているホストの数より少ない場合、ホストの作成は失敗します。ホストの交換が必要なメンテナンスオペレーションについては、クォータの引き上げをリクエストする必要がある場合があります。詳細については、「サービスクォータ」を参照してください。

Example

Amazon EVS console and SDDC Managuer UI

1. Amazon EVS コンソールに移動します。
2. ナビゲーションペインで、環境を選択します。
3. 置き換えるホストを含む環境を選択します。
4. ホストタブを選択します。
5. [Create host] (ホストの作成) を選択します。
6. ホストの詳細を指定し、ホストの作成を選択します。
7. 完了を確認するには、ホストの状態が「作成済み」に変更されていることを確認します。
8. AWS Secrets Manager から ESX ルートパスワードの認証情報を取得します。シークレットの取得の詳細については、AWS 「 Secrets Manager ユーザーガイド」の「Secrets Manager からシー AWS クレットを取得する」を参照してください。
9. SDDC Manager に移動します。
10. 前のステップで取得した ESX ルート認証情報を使用して、SDDC Manager で新しいホストをコミッショニングします。詳細については、VMware Cloud Foundation ドキュメントの「コミッションホスト」を参照してください。
11. 新しいホストをクラスターに追加します。詳細については、vSphere ドキュメントの「クイックスタートワークフローを使用して ESX ホストを vSphere クラスターに追加する方法」を参照してください。 vSphere
12. SDDC Manager から削除する SDDC Manager の古いホストを廃止します。詳細については、VMware Cloud Foundation ドキュメントの「Decommission Hosts」を参照してください。
13. Amazon EVS コンソールに戻ります。
14. Hosts タブで、失敗したホストを選択し、Delete > Delete host を選択します。

AWS CLI and SDDC Manager UI

1. 新しいターミナルセッションを開きます。
2. 新しいホストを作成します。リファレンスについては、以下のコマンド例を参照してください。

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
```

```
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
        "instanceType": "i4i.metal" \
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. AWS Secrets Manager から ESX ルートパスワードの認証情報を取得します。シークレットの取得の詳細については、AWS 「 Secrets Manager ユーザーガイド」の「Secrets Manager からシー AWS クレットを取得する」を参照してください。
4. SDDC Manager に移動します。
5. 前のステップで取得した ESX ルート認証情報を使用して、SDDC Manager で新しいホストをコミッショニングします。詳細については、VMware Cloud Foundation ドキュメントの「Commission Hosts」を参照してください。
6. 障害のあるホストを含むクラスターに新しいホストを追加します。
7. SDDC Manager で障害のあるホストを廃止します。詳細については、VMware Cloud Foundation ドキュメントの「Decommission Hosts」を参照してください。
8. ターミナルに戻ります。
9. 失敗したホストを削除します。リファレンスについては、以下のコマンド例を参照してください。

```
aws evs delete-environment-host --environment-id "env-abcde12345" --host-name
 "esxi-host-05"
```

トラブルシューティング

トラブルシューティングのガイダンスについては、「トラブルシューティング」を参照してください。トラブルシューティングガイダンスを確認しても問題が解決しない場合は、 AWS サポートにお問い合わせください。

Amazon EVS サブネットのカスタムルートテーブルを設定する

Amazon EVS は、Amazon EVS 環境の作成後にのみカスタムルートテーブルの使用をサポートします。環境の作成を成功させるには、DNS やオンプレミスシステムなどの依存サービスへのトラフィックを許可するようにメインルートテーブルを設定する必要があります。これは、Amazon EVS VLAN サブネットが環境のデプロイ中に VPC のメインルートテーブルに暗黙的に関連付けられているためです。

環境がデプロイされたら、各 Amazon EVS VLAN サブネットを VPC 内のルートテーブルに明示的に関連付ける必要があります。VLAN サブネットが VPC ルートテーブルに明示的に関連付けられていない場合、NSX 接続は失敗します。サブネットをカスタムルートテーブルに明示的に関連付けることを強くお勧めします。カスタムルートテーブルを使用すると、VPC 内のネットワークトラフィックルーティングをより詳細に制御できるため、特定のサブネットまたはゲートウェイのルーティングルールをカスタマイズできます。カスタムルートテーブルの作成の詳細については、「Amazon VPC ユーザーガイド」の「VPC のルートテーブルを作成する」を参照してください。

Amazon EVS VLAN サブネットトラフィックを制御するようにネットワークアクセスコントロールリストを設定する

ネットワークアクセスコントロールリスト (ACL) は、サブネットレベルで特定のインバウンドまたはアウトバウンドのトラフィックを許可または拒否します。ネットワーク ACLs、Amazon EVS VLAN サブネット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できます。詳細については、「Amazon VPC ユーザーガイド」の「VPC のネットワーク ACL を作成する」を参照してください。

> **Important**
>
> EC2 セキュリティグループは、Amazon EVS VLAN サブネットにアタッチされている Elastic Network Interface では機能しません。Amazon EVS VLAN サブネットとの間のトラフィックを制御するには、ネットワークアクセスコントロールリストを使用する必要があります。

> **Warning**
>
> Amazon EVS は VCF デプロイにアクセスする必要があります。Amazon EVS が以下と通信できるようにするには、セキュリティグループとネットワークアクセスコントロールリスト (ACLs) を設定する必要があります。
>
> - TCP/UDP ポート 53 経由の DNS サーバー。
> - HTTPS および SSH 経由で管理 VLAN サブネットをホストします。
> - HTTPS および SSH 経由の管理 VM VLAN サブネット。

セキュリティグループとネットワーク ACLsしない場合、Amazon EVS 環境のデプロイは失敗し、既存の環境のコンプライアンスステータスが低下する可能性があります。

シークレット管理ライフサイクル

Amazon EVS は AWS Secrets Manager を使用して、最初の環境デプロイ時にアカウントにシークレットを作成、暗号化、保存します。これらのシークレットには、vCenter Server、NSX、SDDC Manager などの VCF 管理アプライアンスをインストールしてアクセスするために必要な VCF 認証情報と、ESX ホストルートパスワードが含まれています。Amazon EVS は、EVS 環境が削除されると、ユーザーに代わってマネージドシークレットも削除します。

シークレットのローテーションを含むシークレットライフサイクルの管理は、お客様の責任となります。Amazon EVS では、シークレットのマネージドローテーションは提供されません。シークレットが長期間存続しないように、セットローテーションウィンドウでシークレットを定期的にローテーションすることをお勧めします。詳細については、 AWS Secrets Manager ユーザーガイドの「ローテーションスケジュール」を参照してください。

Amazon EVS ホストを作成する

Amazon EVS 環境がデプロイされたら、ホストを追加して容量とワークロードの耐障害性を高めることができます。Amazon EVS は、環境ごとに 4 ~ 16 個のホストをサポートします。このアクションは、Amazon EVS 環境がデプロイされた後にのみ使用できます。

> **Note**
>
> SDDC Manager ユーザーインターフェイス内でホストを割り当ててコミッショニングする必要があります。

Amazon EVS ホストを作成するには

Amazon EVS ホストを作成するには、次の手順に従います。

> **Warning**
>
> Amazon EVS ホストは、カスタムベンダーアドオンを使用して重要なホスト機能を提供します。環境にホストを追加すると、Amazon EVS カスタムアドオンの最新バージョンが提

供されます。環境が古いアドオンバージョンのホストを使用している場合、vSphere クラスターにホストを追加すると、クラスターイメージの修復が失敗します。この問題のトラブルシューティング手順については、「」を参照してくださいthe section called “互換性のないクラスターイメージによるホストの追加失敗のトラブルシューティング”。

Warning

Amazon EVS 環境のデプロイ後に ESX バージョンを更新した場合、コミッションホストステップの VCF ホストの検証中に SDDC マネージャーが失敗することがあります。この問題のトラブルシューティング手順については、「」を参照してくださいthe section called “SDDC Manager がホストコミッショニング中に VCF ホストの検証に失敗する”。

Note

ホストが正常に作成されるように、EVS 環境クォータあたりの Amazon EVS ホスト数が正しく設定されていることを確認します。このクォータ値が単一の Amazon EVS 環境内でプロビジョニングしようとしているホストの数より少ない場合、ホストの作成は失敗します。クォータを引き上げるには、クォータの引き上げをリクエストできます。詳細については、「サービスクォータ」を参照してください。

Note

環境にホストを追加するときに ESX バージョンを指定しない場合、Amazon EVS は環境の VCF バージョンに関連付けられたデフォルトの ESX バージョンを自動的に使用します。詳細については「the section called “VCF バージョンと EC2 インスタンス”」を参照してください。

Important

ESX ホストを追加するときは、ターゲット vSphere クラスターに一致する ESX バージョンを選択します。同じバージョンが使用できない場合は、古いバージョンをデプロイし、vSphere Lifecycle Manager を使用してアップグレードします。詳細については、「the section called “SDDC Manager がホストコミッショニング中に VCF ホストの検証に失敗す

る”」を参照してください。アップグレードにはホストの再起動が必要で、ホストのコミッショニングにかかる時間が長くなる場合があります。
vSphere クラスターイメージ ESX バージョンより新しい ESX バージョンを持つホストはダウングレードできません。ホストを削除し、正しい ESX バージョンで再作成する必要があります。

Example

Amazon EVS console and SDDC Managuer UI

1. Amazon EVS コンソールに移動します。
2. ナビゲーションペインで、環境を選択します。
3. ホストを作成する環境を選択します。
4. ホストタブを選択します。
5. [Create host] (ホストの作成) を選択します。
6. ホストの詳細を指定し、ホストの作成を選択します。
7. 完了を確認するには、ホストの状態が「作成済み」に変更されていることを確認します。
8. SDDC Manager に移動します。
9. SDDC Manager で新しいホストをコミッショニングします。詳細については、VMware Cloud Foundation ドキュメントの「Commission Hosts」を参照してください。
10. SDDC Manager を使用して、新しいホストをクラスターに追加します。詳細については、vSphere ドキュメントの「クイックスタートワークフローを使用して ESX ホストを vSphere クラスターに追加する方法」を参照してください。 vSphere

AWS CLI and SDDC Manager UI

1. 新しいターミナルセッションを開きます。
2. 新しいホストを作成します。リファレンスについては、以下のコマンド例を参照してください。

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
```

```
        "instanceType": "i4i.metal",\
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. SDDC Manager に移動します。
4. SDDC Manager で新しいホストをコミッショニングします。詳細については、VMware Cloud Foundation ドキュメントの「Commission Hosts」を参照してください。
5. SDDC Manager を使用して、新しいホストをクラスターに追加します。詳細については、vSphere ドキュメントの「クイックスタートワークフローを使用して ESX ホストを vSphere クラスターに追加する方法」を参照してください。 vSphere

Amazon EVS ホストを削除する

ホストが不要になったら、Amazon EVS ホストを環境から削除できます。Amazon EVS では、環境に最低 4 つのホストが必要です。Amazon EVS は、ホストが 4 つ未満の環境をサポートしていません。

> **Warning**
>
> 廃止せずにホストを削除すると、vCenter と SDDC Manager に古いデータが残り、クリーンアップに追加の作業が必要になる場合があります。Amazon EVS コンソールまたは API でホストを削除する前に、ホストが廃止されていることを確認します。

> **Warning**
>
> Amazon EVS ホストを削除するには、常に Amazon EVS コンソールまたは API を使用します。EC2 コンソールからホストを削除すると、環境が一貫性のない状態になる可能性があります。

Amazon EVS ホストを削除するには

Amazon EVS ホストを削除するには、次の手順に従います。

Example

SDDC Managuer UI and Amazon EVS console

1. SDDC Manager に移動します。
2. SDDC Manager からクラスターを削除します。
3. SDDC Manager でホストを廃止します。詳細については、VMware Cloud Foundation ドキュメントの「Decommission Hosts」を参照してください。
4. Amazon EVS コンソールに移動します。
5. ナビゲーションペインで、環境を選択します。
6. 削除するホストを含む環境を選択します。
7. ホストタブを選択します。
8. ホストの削除を選択します。
9. ホストを選択し、ホストタブで削除を選択します。削除するホストごとにこのステップを繰り返します。

SDDC Manager UI and AWS CLI

1. SDDC Manager に移動します。
2. SDDC Manager からクラスターを削除します。
3. SDDC Manager でホストを廃止します。詳細については、VMware Cloud Foundation ドキュメントの「Decommission Hosts」を参照してください。
4. 新しいターミナルセッションを開きます。
5. ホストを削除します。リファレンスについては、以下のコマンド例を参照してください。

```
aws evs delete-environment-host \
--environment-id env-abcdefghij \
--host-name my-evs-host.example.com
```

Amazon Elastic VMware Service のセキュリティ

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

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

- クラウドのセキュリティ – AWS は、 AWS のサービス で実行されるインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査人は、AWS コンプライアンスプログラム の一環として、セキュリティの有効性を定期的にテストおよび検証します。Amazon Elastic VMware Service (Amazon EVS) に適用されるコンプライアンスプログラムの詳細については、AWS のサービス「コンプライアンスプログラムによる対象範囲内」を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する によって決まり AWS のサービス 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。

このドキュメントは、Amazon EVS を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。セキュリティとコンプライアンスの目的を達成するように Amazon EVS を設定する方法を示します。また、Amazon EVS リソースのモニタリングと保護 AWS のサービス に役立つ他の の使用方法についても説明します。

内容

Amazon EVS でのデータ保護

AWS 責任共有モデルは、Amazon Elastic VMware Service でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての AWS クラウド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。お客様は、VMware Cloud Foundation (VCF) コンポーネントなど、このインフラストラクチャでホストされているコンテンツの制御を維持する責任があります。また、 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についても責任を負い

ます。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、 セキュリティAWS ブログの 責任共有モデルと GDPR ブログ記事を参照してください。 AWS

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 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 AWS Identity and Access Management。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。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。証 CloudTrail 跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 「証跡の使用」を参照してください。

> **Note**
>
> Amazon EVS は、VPC 環境内のアクティビティなど、非AWS コンポーネントのユーザーアクティビティを記録しません。これらのアクティビティは、vSphere や NSX Manager などのさまざまな VMware コンソールに記録されます。一元化された VCF ログ記録が必要な場合は、VMware Aria Operations や VMware Tanzu Observability などの VCF モニタリングソリューションを設定して、この結果を実現できます。詳細については、VPC ドキュメントのVMware Cloud Foundation with VMware Tanzu」およびVMware Cloud Foundation モードの VMware Aria Suite Lifecyle」を参照してください。

- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- などの高度なマネージドセキュリティサービスを使用して Amazon Macie、 に保存されている機密データの検出と保護を支援します Amazon S3。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

顧客の E メールアドレスなどの機密性の高い識別情報をタグや名前フィールドなどの自由形式のテキストフィールドに入力しないことを強くお勧めします。これは、コンソール、API、または SDK AWS のサービス を使用して Amazon EVS AWS CLIまたは他の を使用する場合も同様です。 AWS

SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

保管中の暗号化

Amazon EVS は、インスタンスストアボリュームに保存されているデータに対してデフォルトで透過的な AES-256 暗号化を使用する i4i.metal EC2 インスタンスをデプロイします。 AES-256 Amazon EVS は、現時点では EBS ブートボリューム暗号化をサポートしていません。

Amazon EBS ブートボリューム

Amazon EVS i4i.metal インスタンスは Amazon EBS ブートボリュームを使用します。ブートボリュームには、オペレーティングシステムと、EC2 インスタンスの起動と実行に必要なその他のファイルが含まれています。ブートボリュームは暗号化されません。Amazon EVS は、現時点ではブートボリューム暗号化をサポートしていません。ブートボリュームには、仮想マシンからのユーザーデータは含まれません。

インスタンスストアボリューム

Amazon EVS i4i.metal EC2 インスタンスには、インスタンスのハードウェアの一部であるローカル NVMe SSD ストレージが付属しています。Amazon EVS は、NVMe インスタンスストアボリュームを vSAN データストアのディスクとして使用します。vSAN データストアは、Amazon EVS 環境をデプロイした後、管理仮想マシンとワークロード仮想マシンを保持します。

NVMe インスタンスストアボリューム内のデータは、インスタンスのハードウェアモジュールに実装されている XTS-AES-256 暗号を使用して暗号化されます。ローカルにアタッチされた NVMe ストレージデバイスに書き込まれるデータの暗号化に使用されるキーは、顧客ごと、およびボリュームごとです。詳細については、「Amazon EC2 ユーザーガイド」の「保管中の暗号化」を参照してください。

Amazon EVS 環境をデプロイした後、vSAN data-at-rest時のデータの暗号化を有効にできます。VMs このきめ細かな制御は、一部の VMsが暗号化を必要とするのに対し、そうでない VM や VM 内の特定のディスクやファイルを暗号化する必要がある場合に役立ちます。詳細については、VMware vSAN ドキュメントの「vSAN Data-At-Rest Encryption の仕組み」を参照してください。

転送中の暗号化

Amazon EVS は、デフォルトでは転送中のトラフィックを暗号化しません。Amazon EVS を通過する転送中のデータを暗号化するには、Transport Layer Security (TLS) などのプロトコルでアプリ

ケーションレイヤー暗号化を使用できます。EC2 インスタンストラフィックの暗号化の詳細については、Amazon EC2 ユーザーガイド」の「転送中の暗号化」を参照してください。

> **Note**
>
> Nitro ネットワーク暗号化は、Amazon EVS がデプロイする EC2 インスタンスには適用されません。Amazon EVS は、ホスト間トラフィックの転送中の暗号化をサポートしていません。

オンプレミス接続の転送時の暗号化オプション

オンプレミスデータセンターと Amazon EVS 間のトラフィックを暗号化するには、 AWS Direct Connect と AWS Site-To-Site VPN を AWS Transit Gateway と組み合わせて使用できます。この組み合わせにより、IPsec で暗号化されたプライベート接続が提供されます。これにより、ネットワークコストが削減され、帯域幅のスループットが向上し、インターネットベースの VPN 接続よりも一貫性のあるネットワーク体験が提供されます。詳細については、AWS 「Direct Connect を使用したプライベート IP AWS Site-to-Site VPN」を参照してください。

> **Note**
>
> Amazon EVS は、 AWS Direct Connect プライベート仮想インターフェイス (VIF) を介した接続、またはアンダーレイ VPC に直接終了する AWS Site-to-Site VPN 接続を介した接続をサポートしていません。Amazon EVS は、NSX Edge Tier-0 または Tier-1 ゲートウェイでの IPSec VPN 終了をサポートしています。詳細については、VMware NSX ドキュメントの「NSX IPSec VPN サービスの追加」を参照してください。

MAC Security (MACsec) は IEEE 標準の 1 つです。データの機密性、データの整合性、およびデータオリジンの信頼性を定義しています。MACsec をサポートする AWS Direct Connect 接続を使用して、企業のデータセンターから AWS Direct Connect ロケーションにデータを暗号化できます。詳細については、AWS 「 Direct Connect ユーザーガイド」の「Direct Connect での MAC セキュリティ」を参照してください。 AWS

VMware ネットワークデータの転送中の暗号化

Amazon EVS 環境がデプロイされたら、VMware VCF レイヤーで転送中のデータの暗号化を適用する複数のオプションがあります。

- VMware vDefend Distributed Firewall - きめ細かなネットワークセグメンテーションを実装し、仮想マシン間で TLS/SSL 暗号化を適用できます。詳細については、VMware VCF ドキュメントの「ユーザーインターフェイスを使用して分散ファイアウォールのセキュリティ設定を構成する」を参照してください。
- vSAN data-in-transit暗号化 - vSAN クラスター内のホスト間のすべてのデータとメタデータを暗号化するために使用できます。詳細については、VMware vSAN ドキュメントの「vSAN Data-In-Transit Encryption」を参照してください。
- 暗号化された vSphere vMotion - vSphere vMotion で転送されるデータの機密性、完全性、信頼性を保護します。詳細については、vSphere ドキュメントの「暗号化された vSphere vMotion とは」を参照してください。 vSphere

キーとシークレットの管理

Amazon EVS 環境のデプロイ中、Amazon EVS は AWS Secrets Manager を使用して、VMware VCF 管理アプライアンスのインストールとアクセスに必要な VCF 認証情報と ESX ルートパスワードを含むシークレットを作成、暗号化、保存します。Amazon EVS は、EVS 環境が削除されると、ユーザーに代わってマネージドシークレットも削除します。詳細については、「 Secrets Manager ユーザーガイド」の「Secrets Manager シークレットの内容 AWS 」を参照してください。

Secrets Manager は AWS KMS 、キーとデータキーによるエンベロープ暗号化を使用して、各シークレット値を保護します。Secrets Manager のデフォルトの AWS マネージドキーは、特に指定がない限り使用されます。または、環境の作成時にカスタマーマネージドキーを指定して、シークレットを暗号化することもできます。詳細については、「 Secrets Manager ユーザーガイド」の AWS「Secrets Manager でのシークレットの暗号化と復号」を参照してください。 AWS

> **Note**
>
> カスタマーマネージドキーには追加料金がかかります。デフォルトの AWS マネージドキーは無料で提供されます。詳細については、 AWS Secrets Manager ユーザーガイドの「 料金表」を参照してください。

Amazon EVS は、デプロイ後に AWS Secrets Manager と VCF ソフトウェアの間で認証情報を同期しません。VCF パスワードの有効期限が切れたり、VPC ソフトウェアにアクセスできなくなったりしないように、Amazon EVS 環境に関連付けられたシークレットが SDDC Manager の認証情報と同期されていることを確認する責任があります。

Amazon EVS はユーザーに代わってシークレットを更新しません。環境に関連付けられたシークレットをローテーションする責任があります。環境が作成されたらすぐにシークレットを更新し、定期的にシークレットを更新するためのローテーションスケジュールを実装することを強くお勧めします。 AWS Secrets Manager シークレットのローテーションの詳細については、Secrets Manager ユーザーガイドの「Lambda 関数によるローテーション」を参照してください。 AWS VCF パスワード管理の詳細については、VMware Cloud Foundation ドキュメントの「パスワード管理」を参照してください。

Important

Amazon EVS は、デプロイ後に AWS Secrets Manager と VCF ソフトウェアの間で認証情報を同期しません。デプロイ後に AWS Secrets Manager を使用する場合は、VPC パスワードの有効期限の問題を回避するために、 AWS Secrets Manager と SDDC Manager の間の認証情報を同期させる必要があります。SDDC Manager の認証情報が最新でない場合、VPC ソフトウェアにアクセスできなくなる可能性があります。

Note

Amazon EVS はシークレットのマネージドローテーションを提供しません。

Note

AWS Secrets Manager シークレットローテーションに Lambda 関数を使用するにはコストがかかります。詳細については、 AWS Secrets Manager ユーザーガイドの「料金表」を参照してください。

ネットワーク間のトラフィックのプライバシー

Amazon EVS は、お客様が用意した VPC を使用して、Amazon EVS 環境内のリソース間の境界を作成し、リソース、オンプレミスネットワーク、インターネット間のトラフィックを制御します。Amazon VPC セキュリティの詳細については、「 Amazon VPC ユーザーガイド」の「 でインターネットネットワークトラフィックのプライバシー Amazon VPCを確保する」を参照してください。

デフォルトでは、Amazon EVS は環境の作成時に直接インターネットアクセスを拒否するプライベート VLAN サブネットを作成します。VPC に別のセキュリティレイヤーを追加するには、イン

ターネット接続をさらに制限するルールを使用して、VPC のカスタムネットワークアクセスコントロールリストを作成できます。詳細については、「Amazon VPC ユーザーガイド」の「VPC のネットワーク ACL を作成する」を参照してください。

> **Important**
>
> EC2 セキュリティグループは、Amazon EVS VLAN サブネットにアタッチされている Elastic Network Interface では機能しません。Amazon EVS VLAN サブネットとの間のトラフィックを制御するには、ネットワークアクセスコントロールリストを使用する必要があります。

NSX 管理者の場合は、ネットワークトラフィックを保護するために次の NSX 機能を設定できます。

- VMware vDefend Gateway Firewall - ネットワーク境界を保護し、外部の脅威 (南北トラフィック) から保護します。詳細については、VMware NSX ドキュメントの「ゲートウェイファイアウォールポリシーとルールを追加する」を参照してください。
- VMware vDefend Distributed Firewall - 内部ネットワーク内 (東西トラフィック) から発生する攻撃から保護します。詳細については、VMware NSX ドキュメントの「分散ファイアウォールの追加」を参照してください。

Amazon Elastic VMware Service の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS resources へのアクセスを安全に制御 AWS のサービス するのに役立つ です。 IAM 管理者は、誰を認証 (サインイン) し、誰に Amazon Elastic VMware Service (Amazon EVS) リソースの使用を許可する (アクセス許可を付与 AWS のサービス する) かを制御します。 IAM は、追加料金なしで使用できる です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon EVS と の連携方法 IAM
- Amazon EVS アイデンティティベースのポリシーの例

- Amazon EVS ID とアクセスのトラブルシューティング
- AWS Amazon EVS の マネージドポリシー
- Amazon EVS のサービスにリンクされたロールの使用

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、Amazon EVS で行う作業によって異なります。

サービスユーザー – Amazon EVS サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの Amazon EVS 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。

Amazon EVS の機能にアクセスできない場合は、「」を参照してくださいthe section called “Amazon EVS ID とアクセスのトラブルシューティング”。

サービス管理者 - 社内の Amazon EVS リソースを担当している場合は、通常、Amazon EVS へのフルアクセスがあります。サービスユーザーがどの Amazon EVS 機能とリソースにアクセスするかを決めるのは管理者の仕事です。その後、 IAM 管理者にリクエストを送信して、サービスユーザーのアクセス許可を変更する必要があります。このページの情報を確認して、 の基本概念を理解します IAM。会社が Amazon EVS IAM で を使用する方法の詳細については、「」を参照してくださいthe section called “Amazon EVS と の連携方法 IAM”。

IAM 管理者 - IAM 管理者は、Amazon EVS へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。で使用できる Amazon EVS 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 IAM、「」を参照してくださいthe section called “Amazon EVS アイデンティティベースのポリシーの例”。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。 AWS アカウントのルートユーザー、、または IAM ロールを引き受けることで IAM ユーザー、認証 (にサインイン AWS) される必要があります。

ID ソースを通じて提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM アイデンティティセンター (IAM アイデンティティセンター) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例

です。フェデレーティッド ID としてサインインすると、管理者は以前に IAM ロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS マネジメントコンソール または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「サインインユーザーガイド」の「 へのサインイン方法 AWS アカウント」を参照してください。 AWS

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストに署名する方法の詳細については、 AWS 「 全般のリファレンス」の「署名バージョン 4 の署名プロセス」を参照してください。

使用する認証方法を問わず、追加のセキュリティ情報の提供を要求される場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「IAM アイデンティティセンター (シングルサインオンの後継) ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「 での多要素認証 (MFA) の使用 AWS」を参照してください。 AWS AWS

AWS アカウントのルートユーザー

を初めて作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの完全なアクセス権を持つ単一のサインインアイデンティティから始めます。この ID は AWS アカウントのルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、ルートユーザーのみが実行できるタスク実行に使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「 アカウント管理リファレンスガイド」の「ルートユーザーの認証情報を必要とするタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを介して提供さ

れた認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、IAM Identity Center (シングルサインオンの後継) ユーザーガイドの「IAM Identity Center とは」を参照してください。 AWS AWS

IAM ユーザー および グループ

IAM ユーザー は、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を持つ IAM ユーザー ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、 で長期的な認証情報を必要とする特定のユースケースがある場合は IAM ユーザー、アクセスキーをローテーション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「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、 のコレクションを指定する ID です IAM ユーザー。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が簡単になります。たとえば、IAMAdmins という名前のグループがあり、そのグループに IAM リソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、IAM ユーザーガイドの IAM ユーザー 「 (ロールではなく) を作成するタイミング」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは に似ていますが IAM ユーザー、特定のユーザーに関連付けられていません。 IAM ロールを切り替える AWS マネジメントコンソール ことで、 で ロールを一時的に引き受けることができます。ロールを引き受けるには、 AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールの使用方法の詳細については、IAM ユーザーガイドの IAM「ロールの使用」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーテッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーテッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。ID が認証後にアクセスできるものをコントロールするために、IAM アイデンティティセンター は権限セットを IAMのロールに関連付けます。アクセス許可セットの詳細については、 AWS 「IAM アイデンティティセンター (AWS シングルサインオンの後継) ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー アクセス許可 – は、 IAM ロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受け IAM ユーザー ることができます。
- クロスアカウントアクセス – IAM ロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) が自分のアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、IAM ユーザーガイドの IAM 「ロールとリソースベースのポリシーの違い」を参照してください。
- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。たとえば、サービスで呼び出しを行うと、そのサービスが でアプリケーションを実行 Amazon EC2 したり、オブジェクトを保存したりするのが一般的です Amazon S3。サービスは、呼び出し元のプリンシパルの許可、サービスロール、サービスリンクロールを使用してこれを行う場合があります。
  - プリンシパルアクセス許可 – IAM ユーザー または ロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。ポリシーによって、プリンシパルに許可が付与されます。一部のサービスを使用する際に、アクションを実行することで、別サービスの別アクションがトリガーされることがあります。この場合、両方のアクションを実行するためのアクセス許可が必要です。
  - サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAM ロールです。 IAM 管理者は、内部からサービスロールを作成、変更、削除できます IAM。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカ

ウント 、サービスによって所有されます。 IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- で Amazon EC2 実行されているアプリケーション – IAM ロールを使用して、 Amazon EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、 Amazon EC2 インスタンス内にアクセスキーを保存するよりも優先されます。 AWS ロールを Amazon EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、 Amazon EC2 インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、IAM ユーザーガイドの「 IAM ロールを使用して Amazon EC2 インスタンスで実行されているアプリケーションにアクセス許可を付与する」を参照してください。

IAM ロールを使用するかどうかについては、IAM ユーザーガイドの (ユーザーではなく) IAM ロールを作成するタイミングを参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

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。

すべての IAM エンティティ (ユーザーまたはロール) は、アクセス許可なしで始まります。デフォルトでは、ユーザーは何もできず、自分のパスワードを変更することすらできません。何かを実行する許可をユーザーに付与するには、管理者がユーザーに許可ポリシーをアタッチする必要があります。また、管理者は、必要な許可があるグループにユーザーを追加できます。管理者がグループに許可を付与すると、そのグループ内のすべてのユーザーにこれらの許可が付与されます。

IAM ポリシーは、オペレーションの実行に使用するメソッドに関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリ

シーを持つユーザーは、 AWS マネジメントコンソール、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

ID ベースのポリシーは、、 IAM ユーザーロール、グループなどの ID にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM 「ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれます。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、IAM ユーザーガイドのマネージドポリシーとインラインポリシーの比較を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、 Amazon S3 バケットなどのリソースにアタッチする JSON ポリシードキュメントです。サービス管理者は、これらのポリシーを使用して、特定のプリンシパル (アカウントメンバー、ユーザー、またはロール) がそのリソースに対して実行する条件およびアクションを定義することができます。リソースベースのポリシーはインラインポリシーです。マネージド型のリソースベースのポリシーはありません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、ロール) がリソースにアクセスする許可を持つかについて管理するポリシーのタイプです。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式を使用しません。 Amazon S3、 AWS WAF、 Amazon VPC は ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーが IAM エンティティ (IAM ユーザー またはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として許可される範囲は、エンティティのアイデンティティベースのポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM 「エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の をグループ化して一元管理するためのサービス AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各アカウントのルートユーザーを含む、メンバー AWS アカウントのエンティティのアクセス許可を制限します。Organizations と SCPsSCPs の仕組み」を参照してください。 AWS
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果として得られるセッションの許可は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分です。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

Amazon EVS と の連携方法 IAM

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

IAM 機能	Amazon EVS のサポート
the section called “Amazon EVS のアイデンティティベースのポリシー”	はい
the section called “Amazon EVS 内のリソースベースのポリシー”	なし
the section called “Amazon EVS のポリシーアクション”	はい
the section called “Amazon EVS のポリシーリソース”	部分的
the section called “Amazon EVS のポリシー条件キー”	はい
the section called “Amazon EVS のアクセスコントロールリスト (ACLs)”	なし
the section called “Amazon EVS を使用した属性ベースのアクセスコントロール (ABAC)”	はい
the section called “Amazon EVS での一時的な認証情報の使用”	はい
the section called “Amazon EVS の転送アクセスセッション”	あり
the section called “Amazon EVS のサービスロール”	なし
the section called “Amazon EVS のサービスにリンクされたロール”	はい

Amazon EVS およびその他の の AWS のサービス 仕組みの概要については IAM、IAM ユーザーガイドの「 AWS のサービス の仕組み IAM」を参照してください。

Amazon EVS のアイデンティティベースのポリシー

ID 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、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルはアタッチされているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用するすべての要素については、IAM ユーザーガイドのIAM 「JSON ポリシー要素リファレンス」を参照してください。

Amazon EVS のアイデンティティベースのポリシーの例

Amazon EVS 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the section called “Amazon EVS アイデンティティベースのポリシーの例”。

Amazon EVS 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチ

することで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

Amazon EVS のポリシーアクション

アクションをサポート はい

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。

IAM アイデンティティベースのポリシーの `Action`要素は、ポリシーによって許可または拒否される特定のアクションを記述します。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。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。

Amazon EVS のポリシーアクションは、アクションの前にプレフィックス を使用しますevs:。例えば、Amazon EVS `CreateEnvironment` API オペレーションを使用して環境を作成するアクセス許可を付与するには、ポリシーに `evs:CreateEnvironment`アクションを含めます。ポリシーステートメントには`Action` または `NotAction` 要素を含める必要があります。Amazon EVS は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一のステートメントに複数のアクションを指定するには次のようにコンマで区切ります。

```
"Action": [
      "evs:action1",
      "evs: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": "evs:List*"
```

Amazon EVS 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「Amazon EVS で定義されるアクション」を参照してください。

Amazon EVS のポリシーリソース

ポリシーリソースのサポート: 一部

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。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これはリソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの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表示するワイルドカード (*) を使用します。

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

Amazon EVS リソースタイプとその ARNs「Amazon Elastic VMware Service で定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、「Amazon Elastic VMware Service で定義されるアクション」を参照してください。

一部の Amazon EVS API アクションは、複数のリソースをサポートしています。たとえば、ListEnvironments API アクションを呼び出すときに複数の環境を参照できます。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": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

例えば、Amazon EVS 環境リソースには次の ARN があります。

```
arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentId}
```

ステートメントmy-environment-2で環境my-environment-1と を指定するには、次の ARNs の例を使用します。

```
"Resource": [
        "arn:aws:evs:us-east-1:123456789012:environment/my-environment-1",
        "arn:aws:evs:us-east-1:123456789012:environment/my-environment-2"
```

特定のアカウントに属するすべての環境を指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:evs:us-east-1:123456789012:environment/*"
```

Amazon EVS 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 (またはConditionブロック) を使用すると、ステートメントが有効になる条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、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。

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

条件を指定する際にプレースホルダー変数も使用できます。たとえば、リソースにその IAM ユーザー 名前がタグ付けされている場合にのみ、リソースへのアクセス IAM ユーザー 許可を付与できます。詳細については、IAM ユーザーガイドのIAM 「ポリシー要素: 変数とタグ」を参照してください。

Amazon EVS は独自の条件キーのセットを定義し、いくつかのグローバル条件キーの使用もサポートしています。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。

すべての Amazon EC2 アクションは、 aws:RequestedRegion および ec2:Region条件キーをサポートします。詳細については、「例: 特定のリージョンへのアクセスの制限」を参照してください。

Amazon EVS 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「Amazon EVS の条件キー」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、「Amazon EVS で定義されるアクション」を参照してください。

Amazon EVS のアクセスコントロールリスト (ACLs)

ACL のサポート: なし

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

Amazon EVS を使用した属性ベースのアクセスコントロール (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、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初のステップです。次に、プリンシパルのタグが、アクセスを試行するリソースのタグと一致したときにオペレーションを許可するよう、ABAC ポリシーを設計します。

ABAC は、急成長する環境や、ポリシー管理が煩雑になる状況で役に立ちます。

Amazon EVS リソースにタグをアタッチすることも、Amazon EVS へのリクエストでタグを渡すこともできます。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。条件キーでタグを使用できるアクションの詳細については、「サービス認可リファレンス」の「Amazon EVS で定義されるアクション」を参照してください。

Amazon EVS での一時的な認証情報の使用

一時的な認証情報のサポート: あり

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

ユーザー名とパスワード以外の AWS マネジメントコンソール 方法で にサインインする場合は、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して アクセスできます AWS。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 の一時的セキュリティ認証情報」を参照してください。

Amazon EVS の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Amazon EVS のサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成するを参照してください。

Amazon EVS 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。

Amazon EVS 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the section called “サービスにリンクされたロールの使用”。

Amazon EVS アイデンティティベースのポリシーの例

デフォルトでは、 IAM ユーザー および ロールには Amazon EVS リソースを作成または変更するアクセス許可はありません。また、 AWS マネジメントコンソール、 AWS CLI、または AWS API を使

用してタスクを実行することはできません。 IAM 管理者は、必要な指定されたリソースに対して特定の API オペレーションを実行するアクセス許可をユーザーとロールに付与する IAM ポリシーを作成する必要があります。管理者は、これらのアクセス許可を必要とする IAM ユーザー または グループにこれらのポリシーをアタッチする必要があります。

これらのサンプル 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「JSON エディタを使用したポリシーの作成」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- Amazon EVS コンソールの使用
- 自分の権限の表示をユーザーに許可する
- Amazon EVS 環境の作成と管理
- Amazon EVS 環境、ホスト、および VLANs の取得と一覧表示

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

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

リクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイドのIAM「JSON ポリシー要素: 条件」を参照してください。

- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的なアクセス許可を確保する – ポリシーがポリシー IAM 言語 (JSON) と IAM ベストプラクティスに準拠するように、新規および既存のポリシー IAM Access Analyzer を検証します。 は、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項 IAM Access Analyzer を提供します。詳細については、「IAM ユーザーガイド」のIAM Access Analyzer「ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – アカウントに 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、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

Amazon EVS コンソールの使用

Amazon EVS コンソールにアクセスするには、IAM プリンシパルに最小限のアクセス許可のセットが必要です。これらのアクセス許可により、プリンシパルは 内の Amazon EVS リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限されたアイデンティティベースのポリシーを作成すると、そのポリシーをアタッチしたプリンシパルに対してはコンソールが意図したとおりに機能しません。

IAM プリンシパルが引き続き Amazon EVS コンソールを使用できるようにするには、 などの独自の一意の名前でポリシーを作成しますAmazonEVSAdminPolicy。ポリシーをプリンシパルにアタッチします。詳細については、IAM ユーザーガイド」の「ユーザーへの許可の追加」を参照してください。

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

```
        {
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行する API オペレーションと一致するアクションのみへのアクセスを許可します。

自分の権限の表示をユーザーに許可する

この例では、 がユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示 IAM ユーザー できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
```

```
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon EVS 環境の作成と管理

このポリシーの例には、Amazon EVS 環境を作成および削除し、環境の作成後にホストを追加または削除するために必要なアクセス許可が含まれています。

を AWS リージョン 、環境 AWS リージョン を作成する に置き換えることができます。
アカウントに AWSServiceRoleForAmazonEVS ロールがすでにある場合、ポリシーから iam:CreateServiceLinkedRole アクションを削除できます。アカウントで Amazon EVS 環境を作成したことがある場合は、削除しない限り、これらのアクセス許可を持つロールが既に存在します。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeHosts",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeRouteServers",
                "ec2:DescribeRouteServerEndpoints",
                "ec2:DescribeRouteServerPeers",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "support:DescribeServices",
                "support:DescribeSupportLevel",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListServiceQuotas"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ModifyNetworkInterfaceStatement",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "ModifyNetworkInterfaceStatementForSubnetAssociation",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
```

```
            "Sid": "CreateNetworkInterfaceWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceAdditionalResources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "TagOnCreateEC2Resources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "StringEquals": {
```

```
                    "ec2:CreateAction": [
                        "CreateNetworkInterface",
                        "RunInstances",
                        "CreateSubnet",
                        "CreateVolume"
                    ]
                },
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "DetachNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
```

```
        {
            "Sid": "RunInstancesWithTagResource",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithoutTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:image/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:placement-group/*"
            ]
        },
        {
            "Sid": "TerminateInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
```

```
            "Sid": "CreateSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithoutTagForExistingVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "DeleteSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSubnet"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDeletion",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
```

```
             "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDetachment",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RouteServerAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:GetRouteServerAssociations"
            ],
            "Resource": "arn:aws:ec2:*:*:route-server/*"

        },
        {
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "SecretsManagerCreateWithTag",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerTagging",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true",
                    "aws:ResourceTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerOps",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DeleteSecret",
                "secretsmanager:GetSecretValue",
```

```
                "secretsmanager:UpdateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "SecretsManagerRandomPassword",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EVSPermissions",
            "Effect": "Allow",
            "Action": [
                "evs:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyAccessInConsole",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        },

        {
            "Sid": "KMSKeyAliasAccess",
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Amazon EVS 環境、ホスト、および VLANs の取得と一覧表示

このポリシーの例には、管理者が us-east-2 の特定のアカウント内のすべての Amazon EVS 環境、ホスト、および VLANs を取得して一覧表示するために必要な最小限のアクセス許可が含まれています AWS リージョン。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "evs:Get*",
        "evs:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon EVS ID とアクセスのトラブルシューティング

以下の情報は、Amazon EVS および の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます IAM。

トピック

- AccessDeniedException
- 自分の 以外のユーザーに Amazon EVS リソース AWS アカウント へのアクセスを許可したい

AccessDeniedException

AWS API オペレーションを呼び出すAccessDeniedExceptionときに を受け取った場合、使用している IAM プリンシパル認証情報には、その呼び出しを行うために必要なアクセス許可がありません。

```
An error occurred (AccessDeniedException) when calling the CreateEnvironment operation:
User: arn:aws:iam::111122223333:user/user_name is not authorized to perform:
```

```
evs:CreateEnvironment on resource: arn:aws:evs:region:111122223333:environment/my-env
```

前のメッセージ例では、ユーザーには Amazon EVS `CreateEnvironment` API オペレーションを呼び出すアクセス許可がありません。IAM プリンシパルに Amazon EVS 管理者アクセス許可を付与するには、「」を参照してくださいthe section called “Amazon EVS アイデンティティベースのポリシーの例”。

IAM の詳細については、IAM ユーザーガイドの「ポリシーを使用して AWS リソースへのアクセスを制御する」を参照してください。

自分の 以外のユーザーに Amazon EVS リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Amazon EVS がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいthe section called “Amazon EVS と の連携方法 IAM”。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の IAM ユーザー の へのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにロールとリソースベースのポリシーを使用する方法の違いについては、IAM ユーザーガイドの IAM 「ロールとリソースベースのポリシーの違い」を参照してください。

AWS Amazon EVS の マネージドポリシー

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

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

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

AWS マネージドポリシー: AmazonEVSServiceRolePolicy

IAM エンティティに AmazonEVSServiceRolePolicy をアタッチすることはできません。このポリシーは、Amazon EVS 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、「the section called “サービスにリンクされたロールの使用”」を参照してください。アクセスiam:CreateServiceLinkedRole許可を持つ IAM プリンシパルを使用して環境を作成すると、AWSServiceRoleforAmazonEVSサービスにリンクされたロールが自動的に作成され、このポリシーがアタッチされます。

このポリシーは、AWSServiceRoleForAmazonEVSサービスにリンクされたロールが AWS のサービス ユーザーに代わって を呼び出すことを許可します。

アクセス許可の詳細

このポリシーには、Amazon EVS が以下のタスクを完了できるようにする以下のアクセス許可が含まれています。

- ec2 - サブネットや VPC などの VPCs。VPC サブネット内の Amazon EVS と VMware Virtual Cloud Foundation (VCF) SDDC Manager アプライアンス間の永続的な接続を確立するために使用される Elastic Network Interface を作成、変更、タグ付け、削除します。この接続は、Amazon EVS が VCF デプロイをデプロイ、管理、モニタリングするために必要です。
- ec2 - EVS ホスト削除リクエストを行うときに Amazon EVS が作成する EC2 インスタンスを削除します。EC2 インスタンス属性を記述および変更して、EVS ホストの削除をサポートするために

必要に応じてデフォルトの EC2 インスタンスの終了と停止の保護を無効にすることができるようにします。

- ec2 - Cloud Builder のインストールとクリーンアップの EBS ボリュームを管理します。環境の作成中、Cloud Builder は Amazon EVS にデプロイされたホストの 1 つにインストールされ、VPC 設定の変更を実行します。完了すると、Amazon EVS は、保存されている EC2 ボリュームをデタッチして削除することで Cloud Builder を削除します。
- ec2 - 環境の削除をリクエストする場合は、ユーザーに代わって EVS VLAN サブネットを削除します。
- secretsmanager - 環境の作成中に Amazon EVS が作成して AWS Secrets Manager に保存する VCF パスワードを削除します。Amazon EVS は、環境の作成に失敗した場合、または環境の削除をリクエストした場合に、サービスがアカウントで作成するすべてのシークレットを削除します。シー AWS クレット ARN を指定して vCenter コネクタを設定するときに、Secrets Manager から vCenter 認証情報を取得します。アクセス許可は、Amazon EVS vCenter アクセス用に明示的にタグ付けされたシークレットにのみ Amazon EVS がアクセスEvsAccess=trueするように、リソースタグ条件でスコープされます。
- kms - Secrets Manager に保存されている vCenter 認証情報が KMS キーで暗号化されている場合、シークレットを復号し、KMS キーを記述します。アクセス許可は、Amazon EVS が vCenter アクセス用に明示的にタグ付けされた KMS キーにのみアクセスEvsAccess=trueするように、リソースタグ条件でスコープされます。
- cloudwatch - クォータを持つ Amazon EVS リソース CloudWatch の AWS 使用状況メトリクスを に発行します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーの詳細については、 AWS 「 マネージドポリシーリファレンスガイド」のAmazonEVSServiceRolePolicy」を参照してください。

AWS マネージドポリシーへの Amazon EVS 更新

このサービスがこれらの変更の追跡を開始してからの Amazon EVS 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。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

変更	説明	日付
AmazonEVSServiceRolePolicy — ポリシーが更新されました	Amazon EVS は、サービスが AWS Secrets Manager から vCenter 認証情報を取得し、	2026 年 3 月 23 日

変更	説明	日付
	KMS キーで暗号化されたシークレットを復号できるようにポリシーを更新しました。詳細については the section called “AWS マネージドポリシー: AmazonEVSServiceRolePolicy”を参照してください。	
AmazonEVSServiceRolePolicy — ポリシーが更新されました	Amazon EVS は、EC2 インスタンス管理、EBS ボリュームオペレーション、AWS Secrets Manager 統合などの包括的なリソース管理機能を追加するためにポリシーを更新しました。詳細については the section called “AWS マネージドポリシー: AmazonEVSServiceRolePolicy”を参照してください。	2025 年 8 月 14 日
AmazonEVSServiceRolePolicy — ポリシーが更新されました	Amazon EVS は、サービスが EVS VLAN サブネットを削除し、Amazon EVS 使用状況メトリクスを公開できるようにポリシーを更新しました CloudWatch。詳細については the section called “AWS マネージドポリシー: AmazonEVSServiceRolePolicy”を参照してください。	2025 年 7 月 14 日

変更	説明	日付
AmazonEVSServiceRolePolicy — 新しいポリシーが追加されました	Amazon EVS は、サービスが顧客アカウントの VPC サブネットに接続できるようにする新しいポリシーを追加しました。この接続はサービス機能に必要です。詳細については the section called “AWS マネージドポリシー: AmazonEVSServiceRolePolicy”を参照してください。	2025/06/09
Amazon EVS が変更の追跡を開始	Amazon EVS は、 AWS 管理ポリシーの変更の追跡を開始しました。	2025/06/09

Amazon EVS のサービスにリンクされたロールの使用

Amazon Elastic VMware Service 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、Amazon EVS に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは Amazon EVS によって事前定義されており、サービスが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が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、Amazon EVS の設定が簡単になります。Amazon EVS は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、Amazon EVS のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、最初に関連リソースを削除する必要があります。これにより、Amazon EVS リソースへのアクセス許可が誤って削除されないため、Amazon EVS リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連動するAWS サービス」を参照し、[Service-linked roles] (サービスにリンクされたロール) の列内で [Yes] (はい)

と表記されたサービスを確認してください。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

Amazon EVS のサービスにリンクされたロールのアクセス許可

Amazon EVS は、 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AWSServiceRoleForAmazonEVS。このロールにより、Amazon EVS はアカウントの環境を管理できます。アタッチされたポリシーにより、ロールは次のリソースを管理できます。EVS Elastic Network Interface、EVS VLAN サブネット、EVS ホスト、VPCs、CloudWatch メトリクス。

AWSServiceRoleForAmazonEVS サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- evs.amazonaws.com

ロールのアクセス許可ポリシーにより、Amazon EVS 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。

- AmazonEVSServiceRolePolicy

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。

Amazon EVS のサービスにリンクされたロールの作成

サービスリンク役割を手動で作成する必要はありません。、 CLI AWS マネジメントコンソール、または AWS API AWS で環境を作成すると、Amazon EVS によってサービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。環境を作成すると、Amazon EVS によってサービスにリンクされたロールが再度作成されます。

Amazon EVS のサービスにリンクされたロールの編集

Amazon EVS では、AWSServiceRoleForAmazonEVS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の作成後は、さまざまなエンティティがロールを参照す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 を使用してロールの説明を

編集することはできます。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編集」を参照してください。

Amazon EVS のサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンク役割をクリーンアップする必要があります。

サービスリンク役割のクリーンアップ

IAM を使用してサービスにリンクされた役割を削除するには最初に、その役割で使用されているリソースをすべて削除する必要があります。ホストを使用して Amazon EVS 環境を削除する手順については、「」を参照してくださいthe section called “Amazon EVS ホストと環境を削除する”。

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

サービスにリンクされたロールを手動で削除する

IAM コンソール、CLI、または AWS API AWS を使用して、`AWSServiceRoleForAmazonEVS`サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

Amazon EVS 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

Amazon EVS 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、「 AWS 全般のリファレンスガイド」の「Amazon Elastic VMware Service エンドポイントとクォータ」を参照してください。

Amazon EVS の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。複数の物理的に分離および分離されたアベイラビリティーゾーン AWS リー

ジョン は、低レイテンシー、高スループット、高度に冗長なネットワークを介して接続されます。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェールオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、フォールトトレランス、および拡張性が優れています。

Amazon EVS 環境は、単一の AWS アベイラビリティーゾーンで使用できます。Amazon EVS シングル AZ インフラストラクチャの高可用性を確保するために、Amazon EVS には次の機能があります。

> **Note**
>
> Amazon EVS は、現時点ではシングル AZ 配置のみをサポートしています。

- Amazon EVS では、Elastic Disaster Recovery AWS を使用してデータのバックアップとリカバリを自動化できます。
- Amazon EVS は、VPC 要件ごとに 2 つの NSX Edge ノードを持つアクティブ/スタンバイ NSX Edge クラスターをデプロイします。NSX Edge ノードは、高可用性を確保し、まれに NSX Edge ノードに障害が発生した場合に迅速なフェイルオーバーを可能にするために、異なるホストで実行されます。
- Amazon EVS は、VPC が必要とする 4 つの ESX ホストの最小限の環境をデプロイします。デプロイ後にホストを追加できます。これは、適切な vSAN クォーラムを確保し、メンテナンスオペレーションやホスト障害発生時の可用性を維持するための VMware 設計要件です。詳細については、VMware Cloud Foundation ドキュメントのvSphere Cluster Design for VMware Cloud Foundation」を参照してください。
- Amazon EVS は、EC2 ホストの EC2 パーティションプレイスメントグループまたはクラスタープレイスメントグループの使用をサポートしています。パーティションプレイスメントグループは EC2 インスタンスを論理パーティションに分散し、1 つのパーティション内のインスタンスのグループが異なるパーティション内のインスタンスのグループと基盤となるハードウェアを共有しないようにします。この戦略は、大規模な分散ワークロードで相関するハードウェア障害の可能性を減らすのに役立ちます。クラスタープレイスメントグループを使用して EC2 インスタンスを同じ物理ラックに配置し、遅延を軽減します。詳細については、「 Amazon EC2 ユーザーガイド」の「パーティションプレイスメントグループ」を参照してください。

AWS 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。

VMware コンポーネントの耐障害性

Amazon EVS のお客様は、仮想マシン (VMs) の高可用性とワークロードの耐障害性を確保するために、Amazon EVS で実行されている VMware コンポーネントを設定する責任があります。

Amazon EVS は、次の VMware Cloud Foundation (VCF) の耐障害性機能をサポートしています。

- vSphere レプリケーション - ディザスタリカバリとワークロード移行の目的で、VMs のホストベースの非同期レプリケーションを提供します。詳細については、VMware vSphere レプリケーションドキュメントの「vSphere レプリケーションの仕組み」を参照してください。 vSphere
- vSAN データ保護 - vSAN クラスターにローカルに保存されているネイティブスナップショットを使用して、ランサムウェア攻撃の運用上の障害から VMs をすばやく復旧できます。詳細については、vSAN ドキュメントの「vSAN データ保護の使用」を参照してください。
- vSphere HA - ホストに障害が発生した場合に VMs の自動フェイルオーバーを提供します。詳細については、VPC ドキュメントのvCenter Server for VMware Cloud Foundation の高可用性設計」を参照してください。
- vSphere フォールトトレランス (FT) - フェイルオーバー状況が発生した場合に、同じで継続的に置き換えることができる別の VMs を作成して維持することで、ミッションクリティカルな VM の継続的な可用性を提供します。詳細については、vSphere ドキュメントの「How Fault Tolerance Works」を参照してください。
- vSAN Failure to Tolerate (FTT) - VM がアクセス不能になる前に耐えることができるホスト障害の数を決定する vSAN 設定。これにより、vSAN クラスター内の仮想マシンの冗長性と耐障害性のレベルが定義されます。詳細については、vSAN ドキュメントの「vSAN クラスターの障害ドメインで追加の障害を許容する」を参照してください。

他の AWS サービスでの Amazon EVS の使用

Amazon EVS は他の と統合 AWS のサービス され、追加のソリューションを提供します。このトピックでは、Amazon EVS が機能を追加するために使用するサービスの一部を示します。

トピック

- AWS CloudFormation を使用して Amazon EVS リソースを作成する
- Amazon FSx for NetApp ONTAP を使用して高性能ワークロードを実行する

AWS CloudFormation を使用して Amazon EVS リソースを作成する

Amazon EVS は AWS CloudFormation と統合されています。CloudFormation は、 AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップを支援するサービスです。必要なすべての AWS リソース、例えば Amazon EVS 環境を記述するテンプレートを作成すると、 AWS CloudFormation がそれらのリソースのプロビジョニングと設定を処理します。

AWS CloudFormation を使用すると、テンプレートを再利用して Amazon EVS リソースを一貫して繰り返しセットアップできます。リソースを一度記述するだけで、複数の AWS アカウント およびリージョンで同じリソースを何度もプロビジョニングできます。

Amazon EVS および AWS CloudFormation テンプレート

Amazon EVS および関連サービスのリソースをプロビジョニングして設定するには、AWS CloudFormation テンプレートを理解する必要があります。テンプレートは、JSON や YAML でフォーマットされたテキストファイルです。これらのテンプレートは、 AWS CloudFormation スタックでプロビジョニングするリソースを記述します。JSON または YAML に慣れていない場合は、 AWS CloudFormation デザイナー を使用して AWS CloudFormation テンプレートの使用を開始できます。詳細については、AWS CloudFormation ユーザーガイド」の「CloudFormation デザイナーとは」を参照してください。 AWS CloudFormation

Amazon EVS は、 AWS CloudFormation での環境の作成をサポートしています。環境の JSON テンプレートと YAML テンプレートの例を含む詳細については、 AWS CloudFormation ユーザーガイドの「Amazon EVS リソースタイプのリファレンス」を参照してください。

AWS CloudFormation の詳細

AWS CloudFormation の詳細については、次のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

Amazon FSx for NetApp ONTAP を使用して高性能ワークロードを実行する

Amazon FSx for NetApp ONTAP は、クラウドでフルマネージド型の ONTAP ファイルシステムを起動して実行できるストレージサービスです。ONTAP は、NetApp のファイルシステムテクノロジーであり、幅広く採用されているデータアクセス機能とデータ管理機能を提供します。FSx for ONTAP は、フルマネージド AWS サービスの俊敏性、スケーラビリティ、シンプルさを備えたオンプレミス NetApp ファイルシステムの機能、パフォーマンス、APIs を提供します。詳細については、「FSx for ONTAP ユーザーガイド」を参照してください。

Amazon EVS は、NFS/iSCSI データストアおよび Amazon EVS で実行されている VMware 仮想マシンのゲスト接続ストレージとしての Amazon FSx for NetApp ONTAP の使用をサポートしています。

FSx for NetApp ONTAP を NFS データストアとして設定する

次の手順では、FSx コンソールと Amazon EVS で実行される VMware vSphere クライアントインターフェイスを使用して、FSx for NetApp ONTAP を Amazon EVS の NFS データストアとして設定するために必要な最小限のステップについて詳しく説明します。

前提条件

Amazon FSx for NetApp ONTAP で Amazon EVS を使用する前に、次の前提条件タスクが完了していることを確認してください。

- Amazon EVS 環境は、Virtual Private Cloud (VPC) にデプロイされます。詳細については、「開始方法」を参照してください。
- Amazon EVS で実行されている vSphere クライアントにアクセスできます。

- ユーザーまたはストレージ管理者は、VPC で FSx for ONTAP ファイルシステムを作成および管理するために必要なアクセス許可を持っている必要があります。詳細については、「Amazon FSx for NetApp ONTAP の Identity and Access Management」を参照してください。

IAM プリンシパルには、VPC で FSx for ONTAP ファイルシステムを作成および管理するための適切なアクセス許可があります。詳細については、「the section called “Amazon EVS 環境の作成と管理”」を参照してください。

FSx for NetApp ONTAP ファイルシステムを作成する

1. Amazon FSx コンソールに移動します。
2. ファイルシステムを作成する を選択します。
3. Amazon FSx for NetApp ONTAP を選択します。
4. [次へ] を選択します。
5. Standard create を選択します。
6. デプロイタイプで、シングル AZ デプロイオプションを選択します。

> **Note**
>
> Amazon EVS は、現時点ではシングル AZ 配置のみをサポートしています。

7. SSD ストレージ容量には、1024 GiB を指定します。
8. スループット容量 で、スループット容量を指定する を選択します。シングル AZ 1 の場合は 512 MB/秒以上、シングル AZ 2 の場合は 768 MB/秒以上を選択します。
9. Amazon EVS VLAN サブネットに接続している Amazon EVS VPC を選択します。
10. Amazon EVS ホスト VMkernel 管理 VLAN サブネットへのすべての必要な FSx for ONTAP NFS トラフィックを許可するセキュリティグループを選択します。
11. ファイルシステムがデプロイされる Amazon EVS サービスアクセスサブネットを選択します。詳細については、「the section called “サービスアクセスサブネット”」を参照してください。
12. ジャンクションパスには、 などの意味のある名前を指定`/vol1`して、vSphere でこのボリュームを識別します。
13. デフォルトのボリューム設定で、ストレージ効率を有効に設定します。
14. 残りの設定をデフォルト値のままにして、次へを選択します。
15. ファイルシステムの属性を確認し、ファイルシステムの作成を選択します。

ストレージ仮想マシンの NFS DNS 名を取得する

1. Amazon FSx コンソールに移動します。
2. 左側のメニューで、ファイルシステムを選択します。
3. 新しく作成したファイルシステムを選択します。
4. Storage virtual machines タブを選択します。
5. ストレージ仮想マシンを選択します。
6. エンドポイントタブを選択します。
7. VMware Vsphere で後で使用するために、ネットワークファイルシステム (NFS) DNS 名をコピーします。

FSx for ONTAP ボリュームを使用して vSphere に NFS データストアを作成する

vSphere 環境で NFS データストアを作成する」の手順に従って、VMware vSphere の外部ストレージとして Amazon FSx for NetApp ONTAP を設定します。vSphere クライアントインターフェイスのサーバー設定では、前のステップでコピーしたストレージ仮想マシン (SVM) NFS DNS 名を使用します。

FSx for NetApp ONTAP FSx を iSCSI データストアとして設定する

次の手順では、FSx コンソールと Amazon EVS で実行される VMware vSphere クライアントインターフェイスを使用して、FSx for NetApp ONTAP を Amazon EVS の iSCSI データストアとして設定するために必要な最小限のステップについて詳しく説明します。

前提条件

Amazon FSx for NetApp ONTAP で Amazon EVS を使用する前に、次の前提条件タスクが完了していることを確認してください。

- Amazon EVS 環境は、Virtual Private Cloud (VPC) にデプロイされます。詳細については、「開始方法」を参照してください。
- Amazon EVS で実行されている vSphere クライアントにアクセスできます。
- ユーザーまたはストレージ管理者は、VPC で FSx for ONTAP ファイルシステムを作成および管理するために必要なアクセス許可を持っている必要があります。詳細については、「Amazon FSx for NetApp ONTAP の Identity and Access Management」を参照してください。

FSx for NetApp ONTAP ファイルシステムを作成する

1. Amazon FSx コンソールに移動します。
2. ファイルシステムを作成する を選択します。
3. Amazon FSx for NetApp ONTAP を選択します。
4. [次へ] を選択します。
5. Standard create を選択します。
6. デプロイタイプで、シングル AZ デプロイオプションを選択します。

> **Note**
>
> Amazon EVS は、現時点ではシングル AZ 配置のみをサポートしています。

7. SSD ストレージ容量には、1024 GiB を指定します。
8. スループット容量 で、スループット容量を指定する を選択します。シングル AZ 1 の場合は 512 MB/秒以上、シングル AZ 2 の場合は 768 MB/秒以上を選択します。
9. Amazon EVS VLAN サブネットに接続している Amazon EVS VPC を選択します。
10. Amazon EVS ホスト VMkernel 管理 VLAN サブネットへの ONTAP iSCSI トラフィックに必要なすべての FSx を許可するセキュリティグループを選択します。
11. ファイルシステムがデプロイされる Amazon EVS サービスアクセスサブネットを選択します。詳細については、「the section called “サービスアクセスサブネット”」を参照してください。
12. デフォルトのボリューム設定内で、ストレージ効率を有効に設定します。
13. 残りの設定をデフォルト値のままにして、次へを選択します。
14. ファイルシステムの属性を確認し、ファイルシステムの作成を選択します。

ESX ホストストレージ用の vSphere でソフトウェア iSCSI アダプターを設定する

ESX ホストごとに、ソフトウェア iSCSI アダプターを設定して、ESX ホストがそれを使用して iSCSI ストレージにアクセスできるようにする必要があります。vSphere で ESX ホスト用のソフトウェア iSCSI アダプターを設定する手順については、VMware vSphere 製品ドキュメントの「ソフトウェア iSCSI アダプターの追加または削除」を参照してください。

ソフトウェア iSCSI アダプターを設定したら、iSCSI アダプターに関連付けられた iSCSI 修飾名 (IQN) をコピーします。これらの値は後で使用されます。

iSCSI LUN を作成する

FSx for ONTAP を使用すると、iSCSI アクセス専用の論理ユニット番号 (LUNs) を作成し、ESX ホストに共有ブロックストレージを提供できます。NetApp ONTAP CLI を使用して LUN を作成します。

以下はサンプルコマンドです。

> **Note**
>
> LUN サイズをボリュームサイズの 90% に設定することをお勧めします。

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

詳細については、FSx for ONTAP ユーザーガイド」の「iSCSI LUN の作成」を参照してください。

イニシエータグループを設定して iSCSI LUN にマッピングする

iSCSI LUN を作成したので、プロセスの次のステップは、イニシエータグループ (igroup) を作成してボリュームをクラスターに接続し、LUN をイニシエータグループにマッピングすることです。NetApp ONTAP CLI を使用して、これらのアクションを実行します。

1. イニシエータグループを設定します。

   以下はサンプルコマンドです。には`--initiator`、前のステップでコピーした iSCSI アダプター IQNs を使用します。

   ```
   igroup create <svm_name> \
   -igroup <initiator_group_name> \
   -protocol iscsi \
   -ostype vmware \
   -initiator <esxi_iqn_1>,<esxi_iqn_2>,<esxi_iqn_3>,<esxi_iqn_4>
   ```

2. `igroup` が存在することを確認します。

   ```
   lun igroup show
   ```

3. LUN をイニシエータグループにマッピングします。以下はサンプルコマンドです。

```
lun mapping create -vserver <svm_name> \
-path /vol/<vol_name>/<lun_name> \
-igroup <initiator_group_name> \
-lun-id <scsi_lun_number_for this_datastore>
```

4. `lun show -path` コマンドを使用して、LUN が作成、オンライン、マッピングされていることを確認します。

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

詳細については、「FSx for ONTAP ユーザーガイド」の「Linux 用 iSCSI FSx のプロビジョニング」または「Windows 用 iSCSI のプロビジョニング」を参照してください。

vSphere で iSCSI LUN の動的検出を設定する

ESX ホストが iSCSI LUN を表示できるようにするには、vSphere クライアントインターフェイスでホストごとに動的検出を設定する必要があります。iSCSI サーバーフィールドに、前のステップでコピーした (NFS) DNS 名を入力します。詳細については、VMware vSphere 製品ドキュメントの「Configure Dynamic or Static Discovery for iSCSI and iSER on ESX Host」を参照してください。

iSCSI LUN を使用して VMware vSphere に VMFS Datastore を作成する

仮想マシンファイルシステム (VMFS) データストアは、VMware 仮想マシンのリポジトリとして機能します。vSphere VMFS データストアを作成する」の手順に従って、以前に設定した iSCSI LUN を使用して VMware vSphere に VMFS データストアを設定します。

トラブルシューティング

この章では、Amazon EVS 環境の作成または管理中に発生する一般的な問題について詳しく説明します。

失敗した環境ステータスチェックのトラブルシューティング

Amazon EVS は環境を自動的にチェックして問題を特定します。環境のステータスを表示して、特定の検出可能な問題を識別できます。

環境ステータスチェック情報を確認する

Amazon EVS コンソールを使用して障害のある環境を調査するには

1. Amazon EVS コンソールを開きます。
2. ナビゲーションペインで、環境を選択し、環境を選択します。
3. 詳細タブを選択すると、環境の概要が表示されます。
4. 環境のステータスを確認します。このフィールドにカーソルを合わせると、環境ステータスチェックごとに個別の結果を含むポップオーバーが展開されます。

到達可能性チェックに失敗しました

到達可能性チェックでは、Amazon EVS が SDDC Manager に永続的に接続されていることを確認します。Amazon EVS が環境にアクセスできない場合、このチェックは失敗します。

このチェックに失敗すると、Amazon EVS は SDDC Manager にアクセスして環境ステータスを検証したり、ホストを環境に追加したりできなくなります。到達可能性の障害により、ライセンスキーの再利用とキーカバレッジのチェックも失敗し、ホスト数のチェックで [不明] レスポンスが返されます。

到達可能性を確保するには、以下を確認してください。

- 証明書が有効で、有効期限が切れていないことを確認します。SDDC Manager ユーザーインターフェイスまたは vSphere クライアントを使用して VCF 環境内の証明書を管理できます。デプロイ後は、VMware Cloud Foundation 管理ドメインのすべての証明書を置き換えることをお勧めします。詳細については、VMware Cloud Foundation ドキュメントの「Managing Certificates in VMware Cloud Foundation」を参照してください。

- サービスアクセスサブネットから DNS サーバーにアクセスできること、DNS レコードが有効であること、重複するホスト名や IP アドレスが存在しないことを確認します。
- 独自のファイアウォールルールを作成する場合は、以下のガイドラインに従ってください。
  - DNS サーバーへの TCP/UDP アクセスを許可する。
  - ホスト管理 VLAN サブネットへの HTTPS/SSH アクセスを許可する。
  - 管理 VM VLAN サブネットへの HTTPS/SSH アクセスを許可する。

このガイダンスに従っても問題を解決できない場合は、 AWS サポートに連絡してサポートを受けることをお勧めします。

ホスト数チェックに失敗しました

このチェックでは、環境のホストが 4 つ以上あることを確認します。これは VCF 5.2.x の要件です。

このチェックに失敗した場合は、環境がこの最小要件を満たすようにホストを追加する必要があります。Amazon EVS は 4 ~ 16 個のホストがある環境のみをサポートします。

キー再利用チェックに失敗しました

このチェックでは、別の Amazon EVS 環境で VCF ライセンスキーが使用されていないことを確認します。VCF ライセンスは 1 つの Amazon EVS 環境でのみ使用できます。このチェックは、別の環境で既に使用されている環境作成リクエストで VCF ライセンスキーを指定すると失敗します。

このチェックが失敗すると、Amazon EVS 環境を作成できなかったというエラーレスポンスが返されます。この問題を解決するには、SDDC Manager でライセンス設定を確認し、使用されている既存のライセンスを未使用のライセンスに置き換えます。

> **Important**
>
> SDDC Manager ユーザーインターフェイスを使用して、VPC ソリューションと vSAN ライセンスキーを管理します。Amazon EVS では、サービスが正しく機能するためには、有効な VCF ソリューションと vSAN ライセンスキーを SDDC Manager に維持する必要があります。vSphere Client を使用してホストと vSAN クラスターにキーを割り当てる必要がありますが、これらのキーが SDDC Manager ユーザーインターフェイスのライセンス画面にも表示されることを確認する必要があります。

キーカバレッジチェックに失敗しました

このチェックでは、vCenter Server に割り当てられた VCF ライセンスキーが、デプロイされたすべてのホストに十分な vCPU コアと vSAN ストレージ容量 (TiB) を割り当てていることを確認します。

このチェックが失敗すると、Amazon EVS 環境を作成できなかったというエラーレスポンスが返されます。キーカバレッジの障害は、次の問題のいずれかを示している可能性があります。

- VCF ライセンスが vCenter Server に正しく割り当てられていません。評価期間が終了するか、現在割り当てられているライセンスの有効期限が切れる前に、vCenter Server にライセンスを割り当てる必要があります。これが問題である場合は、SDDC Manager でライセンスの割り当てを確認してください。
- 現在の VCF ライセンスは、vCPU コアおよび vSAN ストレージ容量のニーズをカバーしていません。VCF ソリューションキーには、少なくとも 256 コアが必要です。vSAN ライセンスキーには、少なくとも 110 TiB の vSAN 容量が必要です。これが問題である場合は、使用ニーズが満たされるまで SDDC Manager で vSAN ライセンスを追加してください。

上記のアクションで問題が解決しない場合は、 AWS サポートにお問い合わせください。

> **Important**
>
> SDDC Manager ユーザーインターフェイスを使用して、VPC ソリューションと vSAN ライセンスキーを管理します。Amazon EVS では、サービスが正しく機能するためには、有効な VCF ソリューションと vSAN ライセンスキーを SDDC Manager に維持する必要があります。vSphere Client を使用してホストと vSAN クラスターにキーを割り当てる必要がありますが、これらのキーが SDDC Manager ユーザーインターフェイスのライセンス画面にも表示されることを確認する必要があります。

このホストの vSphere HA エージェントは分離アドレスに到達できませんでした

vCenter ユーザーインターフェイスで ESX ホストを選択すると、「このホストの vSphere HA エージェントは分離アドレス <IPv6 アドレス> に到達できませんでした」というメッセージが表示されます。

このエラーメッセージは、ホスト上の vSphere HA エージェントが、vSphere HA がハートビートチェックに使用するデフォルトの IPv6 分離アドレスに到達できないことを示します。エラーメッセージは問題を示すものではなく、現時点では Amazon EVS が IPv6 をサポートしていないためにのみ発生します。Amazon EVS の IPV6 サポートがないため、vSphere HA のコア機能には影響しません。

ESX ホストクラスターの vSAN アップグレードの事前チェックが失敗する

SDDC Manager を使用して ESX ホストクラスターをアップグレードしようとすると、vSAN ディスク関連の事前チェックが失敗することがあります。これは、Amazon EVS が vSAN Express Storage Architecture (ESA) を使用し、アップグレードの事前チェックが vSAN ESA に適用されないためです。詳細については、このトピックに関する Broadcom ナレッジベースの記事を参照してください。

互換性のないクラスターイメージによるホスト障害の追加

[Problem] (問題)

環境にホストを追加すると、ホストには利用可能な最新バージョンの EVS カスタムベンダーアドオンがあります。環境が古いアドオンバージョンのホストを使用している場合、新しいホストの追加は失敗し、新しいホストがクラスターイメージと互換性がないというエラーが発生します。この問題を解決するには、vSphere Lifecyle Manager を使用して、新しく追加されたホストから利用可能な最新のアドオンバージョンを抽出する必要があります。

解決策

以下の手順に従ってください。

1. VMware vCenter Server のホストとクラスターのインベントリに移動します。
2. 一時的に空のクラスターを作成して、新しく追加されたホストからアドオンを抽出します。
3. 基本 で、vCenter インベントリ内の既存のホストからイメージをインポートを選択し、クラスターを作成します。他のすべての設定はデフォルトのままにします。
4. この一時クラスターが抽出されたイメージで作成されたら、一時クラスターを削除できます。アドオンが vSphere Lifecycle Manager デポで使用できるようになりました。
5. 環境クラスターに移動し、更新タブを選択します。

6. クラスターイメージを編集し、アドオンバージョンを新しく抽出されたバージョンに変更します。
7. [保存] を選択します。
8. SDDC Manager で、失敗したホストの追加タスクを再試行します。これにより、クラスターホストが修復され、すべてのホストが最新のアドオンバージョンに更新されます。クラスターイメージの修復には、ホストの再起動が必要です。

SDDC Manager がホストコミッショニング中に VCF ホストの検証に失敗する

[Problem] (問題)

Amazon EVS 環境のデプロイ後に ESX バージョンを更新した場合、コミッションホストステップの VCF ホストの検証中に SDDC マネージャーが失敗することがあります。この問題を解決するには、vSphere Lifecyle Manager を使用して、新しく追加されたホストで ESX をアップグレードする必要があります。

解決策

以下の手順に従ってください。

> **Important**
>
> これらのステップでは、SDDC Manager の外部でホストを vCenter に一時的に追加する必要があります。ESX アップグレード以外のオペレーションに vSphere Lifecyle Manager を使用すると、ホストが使用できなくなる可能性があり、新しい Amazon EVS ホストを削除して作成する必要があります。

1. VMware vCenter Server のホストとクラスターのインベントリに移動します。
2. ホストを仮想データセンターに一時的に追加し、 がイメージを使用してホストを管理するように選択します。ホストは、ESX アップグレードが完了した後のステップで削除されます。詳細については、vSphere ドキュメントの「vSphere データセンターまたはフォルダにホストを追加する方法」を参照してください。 vSphere
3. ホストが vSphere に追加されたら、ホストの ESX バージョンをアップグレードします。これは、ホストの更新タブで実行できます。クラスターの ESX バージョンと一致するようにホストイメージを編集します。

4. アップグレードが完了したら、vCenter インベントリからホストを削除します。詳細については、vSphere ドキュメントの「vCenter Server インスタンスから ESX ホストを削除する方法」を参照してください。
5. SDDC マネージャーでホストをコミッショニングします。詳細については、VMware Cloud Foundation ドキュメントの「Commission Hosts」を参照してください。
6. ホストがコミッショニングされたら、SDDC Manager を使用してホストをクラスターに追加します。

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

Amazon EVS は、Amazon EVS の IAM ユーザー、IAM ロール、または AWS サービスによって実行されたアクションを記録するサービスである AWS CloudTrail と統合されています。CloudTrail は、Amazon EVS のすべての AWS API コールをイベント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、Amazon EVS コンソールからの呼び出しと、Amazon EVS API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Amazon EVS に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail に関する詳細は、「AWS CloudTrail ユーザーガイド」を参照してください。

> **Note**
>
> Amazon EVS は、VPC 環境内のアクティビティなど、非AWS コンポーネントのユーザーアクティビティを記録しません。これらのアクティビティは、vSphere や NSX Manager などのさまざまな VMware コンソールに記録されます。
> 一元化された VCF ログ記録が必要な場合は、VMware Cloud Foundation Operations などの VCF モニタリングソリューションを設定して、この結果を実現できます。

CloudTrail の Amazon EVS 情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。Amazon EVS でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、CloudTrail イベント履歴でのイベントの表示を参照してください。

Amazon EVS のイベントなど、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。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。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベント

データをさらに分析して処理するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- CloudTrail がサポートされているサービスと統合
- 「CloudTrail の Amazon SNS 通知の設定」
- CloudTrail ログファイルの複数のリージョンからの受け取り
- 複数のアカウントから CloudTrail ログファイルを受け取る

すべての Amazon EVS アクションは CloudTrail によってログに記録され、Amazon EVS API リファレンスに記載されています。例えば、`CreateEnvironment`、`GetEnvironment`、`DeleteEnvironment` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、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。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用し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 サービスによって行われたかどうか。

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

Amazon EVS ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、公開 API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

Amazon EVS サービスクォータ

Amazon EVS は Service Quotas と統合されています。 AWS のサービス Service Quotas は、クォータを一元的に表示および管理するために使用できる です。詳細は、Service Quotas ユーザーガイドの「Service Quotas とは」を参照してください。

Service Quotas 統合を使用すると、 AWS マネジメントコンソール または AWS CLI を使用して Amazon EVS クォータの値を検索し、調整可能なクォータのクォータ引き上げをリクエストできます。詳細については、「Service Quotas ユーザーガイド」の「クォータの引き上げのリクエスト」および AWS CLI 「 コマンドリファレンス」のrequest-service-quota-increase」を参照してください。 Service Quotas

Amazon EVS サービスクォータの詳細については、 AWS 全般のリファレンスガイドの「Amazon EVS クォータ」を参照してください。

Important

EC2 実行オンデマンド標準インスタンスのクォータに、Amazon EVS で使用するすべての EC2 インスタンスに必要な vCPU の数が反映されていることを確認します。各 i4i.metal インスタンスは 128 個の vCPU を使用します。EC2 サービスクォータの引き上げについては、「Amazon EC2 ユーザーガイド」の「引き上げのリクエスト」を参照してください。

Note

Amazon EVS 環境に EC2 専有ホストを使用する予定の場合は、EC2 専有 i4i ホストのクォータに、目的のリージョンに使用する専有ホストの数が反映されていることを確認します。EC2 サービスクォータの引き上げについては、「Amazon EC2 ユーザーガイド」の「引き上げのリクエスト」を参照してください。

Note

HCX インターネット接続を設定する場合、Amazon が提供する連続したパブリック IPv4 CIDR ブロックネットマスクの長さの IPAM クォータは /28 以上である必要があります。詳細については、「IPAM のクォータ」を参照してください。

> **Note**
>
> Amazon CloudWatch は、クォータ (環境とホスト) を持つ Amazon EVS リソースの AWS 使用状況メトリクスを収集します。詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch 使用状況メトリクス」を参照してください。

で Amazon EVS サービスクォータを表示する AWS マネジメントコンソール

1. Service Quotas コンソールを開きます。
2. 左側のナビゲーションペインで、 AWS サービスを選択します。
3. AWS サービスリストから、Amazon Elastic VMware Service を検索して選択します。
4. [クォータの表示] をクリックします。

   サービスクォータリストでは、サービスクォータ名、適用された値 (使用可能な場合) 、 AWS デフォルトのクォータ、およびクォータ値が調整可能かどうかを確認できます。
5. 説明など、Service Quotas に関する追加情報を表示するには、クォータ名を選択します。
6. (オプション) クォータの引き上げをリクエストするには、引き上げるクォータを選択し、アカウントレベルで引き上げをリクエストを選択し、必要な情報を入力または選択し、リクエストを選択します。

を使用してサービスクォータをさらに操作するには AWS マネジメントコンソール、Service Quotas ユーザーガイド」を参照してください。クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。

CLI で Amazon EVS AWS サービスクォータを表示する

次のコマンドを実行して、Amazon EVS クォータを表示します。

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
    --output table
```

> **Note**
>
> 返されるクォータは、現在の AWS リージョンでこのアカウントで作成できる Amazon EVS 環境またはホストの数です。

AWS CLI を使用してサービスクォータをさらに操作するには、 AWS 「 CLI コマンドリファレンス」の「service-quotas」を参照してください。クォータの引き上げをリクエストするには、 AWS CLI コマンドリファレンスの request-service-quota-increase コマンドを参照してください。

Amazon Elastic VMware Service ユーザーガイドのドキュメント履歴

次の表に、Amazon Elastic VMware Service のドキュメントリリースを示します。

変更	説明	日付
AmazonEVSServiceRolePolicy の更新	Amazon EVS は、マネージドポリシーを更新AmazonEVSServiceRolePolicy して、サービスが AWS Secrets Manager から vCenter 認証情報を取得し、カスタマーマネージド KMS キーで暗号化されたシークレットを復号できるようにしました。	2026 年 3 月 23 日
AmazonEVSServiceRolePolicy の更新	Amazon EVS は、EC2 インスタンス管理、EBS ボリュームオペレーション、AWS Secrets Manager 統合などの包括的なリソース管理機能を追加AmazonEVSServiceRolePolicy するために、マネージドポリシーを更新しました。詳細については、「Amazon EVS updates to AWS managed policies」を参照してください。	2025 年 8 月 14 日
AmazonEVSServiceRolePolicy の更新	AWS マネージドポリシー AmazonEVSServiceRolePolicy を更新しました。	2025 年 8 月 4 日

AWS アカウントクォータあたりの環境数をリリース	Amazon EVS がリリースした AWS アカウントクォータあたりの環境数。 AWS アカウントあたりの環境数は、特定のアカウントとリージョンで作成できる Amazon EVS 環境の最大数を表します。	2025 年 7 月 8 日
Amazon EVS が欧州 (アイルランド) リージョンでリリースされました	Amazon EVS が欧州 (アイルランド) リージョンでリリースされました。	2025 年 6 月 18 日
AmazonEVSServiceRolePolicy をリリース	AWS マネージドポリシー AmazonEVSServiceRolePolicy がリリースされました。	2025 年 6 月 9 日
ユーザーガイドの初回リリース	Amazon Elastic VMware Service ユーザーガイドがリリースされました。 Amazon EVS ユーザーガイドでは、Amazon EVS のすべての概念について説明し、コンソールとコマンドラインインターフェイスの両方でさまざまな機能を使用する手順について説明します。	2025 年 6 月 9 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。