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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

Amazon Elastic VMware Service (Amazon EVS) を使用して、VMware 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入門。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 - などの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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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。環境には、VPC ソフトウェアスタックを管理、モニタリング、インスタンス化するためのコンポーネントをホストする vSphere クラスターを持つ統合 VCF ドメインが含まれています。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 ESXi ホストです。

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 ESXi 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。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。

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

VMkernel 管理 VLAN サブネットをホストする

ホスト VMkernel 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 ESXi 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 ESXi ホスト間のオーバーレイ通信に使用されます。

VM 管理 VLAN サブネット

VM 管理 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残りの VPC およびユーザーが設定した他の外部ネットワークに接続するために使用します。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 AWS 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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

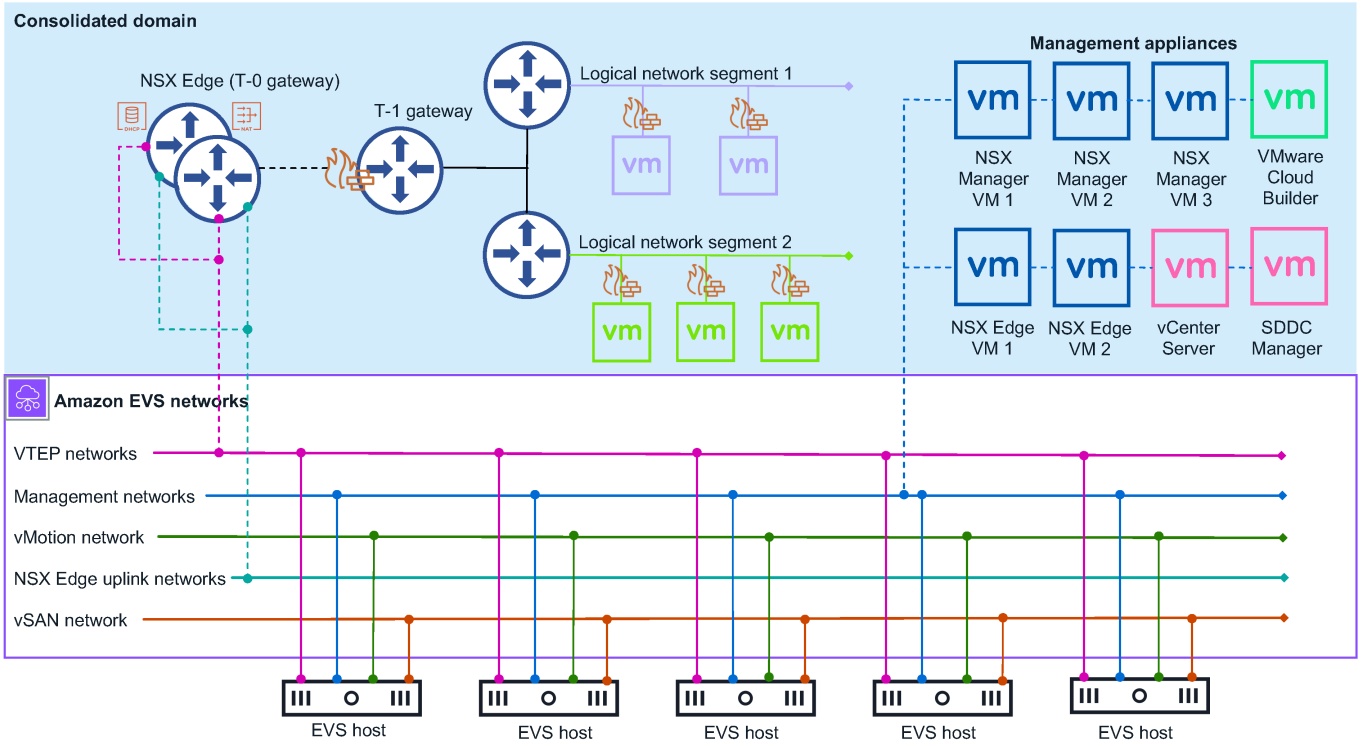
Amazon EVS は、VMware Cloud Foundation (VCF) 統合アーキテクチャモデルを実装しています。このモデルでは、VPC 管理コンポーネントとお客様のワークロードは統合ドメインで一緒に実行されます。Amazon EVS 環境は、管理ワークロードとお客様のワークロードを分離する vSphere リソースプールを備えた単一の vCenter Server から管理されます。 vSphere

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。

- ESXi 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 ノードを使用すると、VPC 経由で 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 AWS 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、「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する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 サーバーの IP アドレスとセカンダリ DNS サーバーの 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 サーバーの設定”」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 エンドポイントで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、環境の作成中に次の 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 Management Console 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 ESXi 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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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。

トピック

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. [Root user (ルートユーザー)] を選択し、AWS アカウントのメールアドレスを入力して、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. [User name (ユーザー名)] に「`Administrator`」と入力します。
4. [AWS Management Console access (AWS マネジメントコンソールへのアクセス)] 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 は新しいユーザーの初回のサインイン時に新しいパスワードの作成を要求します。必要に応じて [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)] のチェックボックスをオフにして、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. [Filter policies (フィルタポリシー)] を選択し、[AWS managed -job function (AWS 管理ジョブ機能)] を選択して、表の内容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。次に、[Create group (グループの作成)] を選択します。

> **Note**
>
> AdministratorAccess アクセス許可を使用して AWS の請求およびコスト管理コンソールにアクセスするには、IAM ユーザーと IAM ロールの請求情報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。

このプロセスを繰り返して新しいグループとユーザーを作成して、AWS アカウントのリソースへのアクセス許可をユーザーに付与できます。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、「 ユーザーガイド」の「IAM ユーザーに権限を委任するロールを作成する」を参照してください。 AWS Identity and Access Management

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意味のある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. Trusted 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 Amazon EVS 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できるように、 AWS Business、 AWS Enterprise On-Ramp、または AWS Enterprise Support プランに登録する必要があります。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、「the section called “Service Quotas”」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 サイズの計画と VPC コンポーネントの設定

Amazon EVS 環境の作成を有効にするには、サブネットと十分な IP アドレス空間を含む VPC を Amazon EVS に提供して、VPC アプライアンスに接続する VLAN サブネットを作成する必要があります。VPC 作成要件の詳細については、「」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”。

メインルートテーブル

Amazon EVS サブネットは、作成時に 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。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 VPC のメインルートテーブルを設定する必要があります。Amazon EVS のメインルートテーブル設定の詳細については、「」を参照してくださいthe section called “VPC メインルートテーブルを設定する”。

DHCP オプションセット

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 アドレスの解決に使用されるドメインネームシステム (DNS) サーバー。
- SDDC での時刻同期の問題を回避するために使用される Network Time Protocol (NTP) サーバー。

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 サーバーの IP アドレスとセカンダリ DNS サーバーの IP アドレス。
- 「」で説明されているように、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the section called “Amazon EVS 環境を作成する”。
- 「」で説明されているように、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the section called “Amazon EVS 環境を作成する”。

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。

DNS および NTP サーバー設定で Amazon EVS がサポートするオプションの詳細については、「」を参照してください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”。

VPC Route Server インフラストラクチャを作成する

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。Amazon EVS 用に Route Server を設定する方法については、「」を参照してください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”。

オンプレミス接続用のトランジットガトウェイを作成する

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は、関連付けられたトランジットゲートウェイ AWS 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設定できます。詳細については、「the section called “ (オプション) オンプレミスネットワーク接続を設定する”」を参照してください。

Amazon EC2 キャパシティ予約を作成する

Amazon EVS は、Amazon EVS 環境で ESXi ホストを表す Amazon EC2 ESXi.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によるコンピューティングキャパシティの予約」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 5.2.1 の要件にも精通する必要があります。詳細については、「VPC 5.2.1 リリースノート」を参照してください。

> **Note**
>
> Amazon EVS は、現時点では VCF バージョン 5.2.1.x のみをサポートしています。

VCF ライセンスキーの取得

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

> **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**
>
> 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 を使用してこれらのキーを管理する場合は、それらのキーが 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。

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。

Amazon Elastic VMware Service の開始方法

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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) 内のホストを使用して 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。また、VPC 5.2.1 の要件にも精通する必要があります。詳細については、「VPC 5.2.1 リリースノート」を参照してください。

> **Important**
>
> Amazon EVS は、現時点では VCF バージョン 5.2.1.x のみをサポートしています。

トピック

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。

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、「」を参照してくださいエンドポイントとクォータ。

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。
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。

VPC メインルートテーブルを設定する

Amazon EVS サブネットは、作成時に 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。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。サブネットルートテーブルの管理の詳細については、 Amazon VPC 「 ユーザーガイド」の「サブネットルートテーブルの管理」を参照してください。

Amazon EVS 環境がデプロイされたら、明示的なルートテーブルの関連付けを設定して、カスタムルートテーブルを介した接続を有効にできます。詳細については、「 Amazon VPC ユーザーガイド」の「メインルートテーブルの置き換え」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

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 アドレスの解決に使用されるドメインネームシステム (DNS) サーバー。
- SDDC での時刻同期の問題を回避するために使用される 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。

環境のデプロイを成功させるために DNS 接続を有効にするには、まず DNS 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。

DNS サーバーの設定

最大 4 つのドメインネームシステム (DNS) サーバーの IPv4 アドレスを入力できます。DNS サーバープロバイダー Route 53 として を使用するか、独自のカスタム DNS サーバーを提供できます。既存のドメインの DNS サービスとして Route 53 を設定する方法の詳細については、Route 53を使用中のドメインの DNS サービスにする」を参照してください。

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

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 サーバーの IP アドレスとセカンダリ DNS サーバーの IP アドレス。
- 「」で説明されているように、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the section called “Amazon EVS 環境を作成する”。
- 「」で説明されているように、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the section called “Amazon EVS 環境を作成する”。

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。

> **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。

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。最大 4 つの Network Time Protocol (NTP) サーバーの IPv4 アドレスを入力できます。DHCP オプションセットで NTP 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。

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

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、「Amazon EC2 ユーザーガイド」の「インスタンスの時刻の設定」を参照してください。

(オプション) オンプレミスネットワーク接続を設定する

関連付けられたトランジットゲートウェイ AWS 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。 AWS Site-to-Site VPN は、インターネット経由でトランジットゲートウェイへの IPsec VPN 接続を作成します。 は、プライベート専用接続経由でトランジットゲートウェイへの IPsec VPN 接続 AWS Direct Connect を作成します。Amazon EVS 環境を作成したら、いずれかのオプションを使用して、オンプレミスのデータセンターファイアウォールを VMware NSX 環境に接続できます。

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 “ (オプション) 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”」を参照してください。

AWS Direct Connect 接続の設定の詳細については、AWS 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で設定されたピア ASN 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。

> **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。

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。

> **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は、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、NSX ルートを VPC ルートテーブル (複数可) に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。

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、すべての設定を理解し、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。

   > **Note**
   >
   > Amazon EVS コンソールからトリガーされた Amazon EVS オペレーションは CloudTrail イベントを生成しません。

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、次の操作を行います。
   a. AWS サポート要件とサービスクォータ要件が満たされていることを確認します。Amazon EVS サポート要件の詳細については、「」を参照してくださいthe section called “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 のクォータ要件の詳細については、「」を参照してくださいthe section called “Service Quotas”。
   b. (オプション) Name に環境名を入力します。

c. 環境バージョンで、VPC バージョンを選択します。Amazon EVS は現在、バージョン 5.2.1.x のみをサポートしています。

d. サイト ID には、Broadcom サイト ID を入力します。

e. VCF ソリューションキーには、VPC ソリューションキーを入力します。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**
>
> 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。

f. 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、サービスが正しく機能するためには、SDDC Manager で有効な vSAN ライセンス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 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。

g. 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。

h. [次へ] を選択します。

5. ホストの詳細の指定ページで、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。

> **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。

d. 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。

e. 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. VPC の場合は、以前に作成した VPC を選択します。

b. 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。

c. 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。

d. 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。

> **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。

e. 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。

> **Note**
>
> 指定した VLAN CIDR ブロックが VPC 内で適切にサイズ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 ネットワークに関する考慮事項”」を参照してください。

f. 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、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。

g. [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 アップグレードは SDDC Manager の外部で実行する必要があります。

> **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。Amazon EVS サポート要件の詳細については、「」を参照してくださいthe section called “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 のクォータ要件の詳細については、「」を参照してくださいthe section called “Service Quotas”。

> **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 アップグレードは SDDC Manager の外部で実行する必要があります。

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

- では`--vpc-id`、IPv4 CIDR の最小範囲が /22 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。
- の場合`--vcf-version`、Amazon EVS は現在 VCF 5.2.1.x のみをサポートしています。
- 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`--license-info`、VPC ソリューションキーと 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 に保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のデプロイに使用されます。

> **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。

- 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。

> **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 には、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 は、Broadcom ポータルへのアクセスを許可し、Broadcom によってソフトウェア契約または契約更新の終了時に提供されます。
- (オプション) に--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-5.2.1 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"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\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    }
  ]" \
--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-5.2.1",
        "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、環境は使用できる状態`environmentState`になります`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-5.2.1",
        "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。

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. Amazon EVS VLAN サブネットをすべて選択します。
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
```

(オプション) 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

トランジットゲートウェイで AWS 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。

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。

> **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。

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、「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 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。シークレットが長期間存続しないように、シークレットを定期的にセットローテーションウィンドウで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

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 ESXi シェルを有効にします。この設定により、ECAmazon EC2EC2 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、Direct Console User Interface (DCUI) にアクセスして ESXi ホストとローカルでやり取りする唯一の Amazon EVS 対応メカニズムです。

> **Note**
>
> Amazon EVS は、デフォルトでリモート SSH を無効にします。SSH によるリモート ESXi シェルへのアクセスを有効にする方法の詳細については、VMware vSphere 製品ドキュメントの「SSH によるリモート ESXi シェルアクセス」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、、、、または terminated状態にある場合stoppingstoppedshutting-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

SDDC UI and Amazon EVS console

1. SDDC Manager ユーザーインターフェイスに移動します。
2. vSphere クラスターからホストを削除します。これにより、SDDC ドメインからホストの割り当てが解除されます。クラスター内のホストごとにこのステップを繰り返します。詳細については、VPC 製品ドキュメントの「ワークロードドメインの vSphere クラスターからホストを削除する」を参照してください。
3. 割り当てられていないホストを廃止します。詳細については、VPC 製品ドキュメントの「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。

   > **Note**
   >
   > Amazon EVS コンソールからトリガーされた Amazon EVS オペレーションは CloudTrail イベントを生成しません。

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。
9. 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。

10.不要になった Amazon EC2 キャパシティ予約がある場合は、キャンセルしている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。

SDDC UI and 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-5.2.1",
            "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-5.2.1",
            "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. SDDC Manager ユーザーインターフェイスに移動します。
4. vSphere クラスターからホストを削除します。これにより、SDDC ドメインからホストの割り当てが解除されます。クラスター内のホストごとにこのステップを繰り返します。詳細については、VPC 製品ドキュメントの「ワークロードドメインの vSphere クラスターからホストを削除する」を参照してください。
5. 割り当てられていないホストを廃止します。詳細については、VPC 製品ドキュメントの「Decommission Hosts」を参照してください。
6. 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
```

7. 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。
8. 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。

9. 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。

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。

Elastic Network Interface を削除する

Elastic Network Interface を削除する手順については、Amazon EC2 ユーザーガイド」の「Delete a network interface」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**
>
> 環境が削除されると、Amazon EVS は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。

次のステップ

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 Hybrid Cloud Extension (VMware HCX) を使用してワークロードを Amazon EVS に移行する

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

Amazon EVS 環境を作成したら、VMware Hybrid Cloud Extension (VMware HCX) を使用して、既存の VMware ベースのワークロードを Amazon Elastic VMware Service (Amazon EVS)VMware に移行できます。VMware HCX 移行の詳細については、VMware HCX ユーザーガイドの「VMware HCX 移行タイプ」を参照してください。 VMware

次のチュートリアルでは、VMware HCX を使用して VMware ワークロードを Amazon EVS に移行する方法について説明します。

VMware HCX を使用して、関連付けられたトランジットゲートウェイ AWS Direct Connect で を使用するか、 AWS Site-to-Site VPN アタッチメントを使用して、プライベート接続経由でワークロードをトランジットゲートウェイに移行できます。

> **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。

AWS Direct Connect 接続の設定の詳細については、AWS Direct Connect 「 ユーザーガイド」の「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。 AWS Direct Connect 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。

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、Amazon EVS 環境が作成され、トランジットゲートウェイまたはトランジットゲートウェイ AWS Direct Connect

で AWS Site-to-Site VPN を使用してオンプレミスネットワークに接続されていることを確認します。Amazon EVS 環境を作成する手順については、「」を参照してください入門。VMware HCX の前提条件の詳細については、「」を参照してくださいthe section called “VMware HCX の前提条件”。

HCX VLAN サブネットのステータスを確認する

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、状態が作成されていることを確認します。
6. 後で使用するために HCX `vlan` ID をコピーします。

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
```

レスポンスの例を次に示します。

```
{
 "environmentVlans": [
        {
            "vlan": 80,
            "cidr": "10.10.7.0/24",
            "availabilityZone": "us-east-2c",
            "functionName": "hcx",
            "createdAt": "2025-04-13T13:39:58.845000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.067000+00:00",
            "vlanState": "CREATED",
            "stateDetails": ""
```

```
        },
        {
            "vlan": 20,
            "cidr": "10.10.1.0/24",
            "availabilityZone": "us-east-2c",
            "functionName": "vmManagement",
            "createdAt": "2025-04-13T13:39:58.456000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.524000+00:00",
            "vlanState": "CREATED",
            "stateDetails": ""
        }
 ]
}
```

2. `functionName` が の VLAN を特定し`hcx`、 `vlanState`が であることを確認しますCREATED。
3. 後で使用するために HCX `vlan` ID をコピーします。

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”。

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。

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

HCX WAN Optimization Service (HCX-WAN-OPT) 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-WAN-IX) と組み合わせてデプロイされます。HCX-WAN-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、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できるため、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お読みください。
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

Amazon Elastic VMware Service のセキュリティ

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

で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 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。
- クラウド内のセキュリティ — 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、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Amazon Elastic VMware Service 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 Elastic VMware Service を設定する方法を示します。また、Amazon Elastic VMware Service 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 Elastic VMware Service の Identity and Access Management

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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 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

対象者

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

サービスユーザー – Amazon Elastic VMware Service 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 Elastic VMware Service 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。

サービス管理者 - 社内の Amazon Elastic VMware Service リソースを担当している場合は、通常、Amazon Elastic VMware Service 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 Elastic VMware Service の機能や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 Elastic VMware Service 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 Elastic VMware Service と の連携方法 IAM”。

IAM 管理者 - IAM 管理者は、Amazon Elastic VMware Service 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 Elastic VMware Service 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、「Amazon Elastic VMware Service アイデンティティベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

認証は、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 ソースを介し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 Identity Center （ IAM Identity Center) 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。

ユーザーの種類に応じて、 AWS Management Console 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、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 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、自分でリクエストに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、「AWS IAM アイデンティティセンター (AWS Single Sign-On) 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 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。このアイデンティティは root ユーザーと呼ばれ、AWS アカウントの作成に使用したメールアドレスとパスワードでのサインインによりアクセスされます。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。

フェデレーティ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 Identity Center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、AWS IAM Identity Center (AWS Single Sign-On 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 Single Sign-On

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容易になります。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 Management Console 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 – フェデレーティッド 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。フェデレーティッド 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 Identity Center (AWS Single Sign-On 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推奨されます。 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、 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 ロールを使用する方法については、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 Management Console、、 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ています。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ています。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 AWS アカウントルートユーザーを含めてメンバーアカウントのエンティティに対するアクセス許可を制限します。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの SCP の仕組みを参照してください。
- 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ティッドユーザーの一時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権限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 Elastic VMware Service と の連携方法 IAM

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

IAM を使用して Amazon Elastic VMware Service へのアクセスを管理する前に、Amazon Elastic VMware Service 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 での属性ベースのアクセスコントロール (ABAC)”	はい

IAM 機能	Amazon EVS のサポート
the section called “Amazon EVS での一時的な認証情報の使用”	あり
the section called “Amazon EVS の転送アクセスセッション”	はい
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 Elastic VMware Service とその他の AWS のサービス の連携の概要については IAM、IAM ユーザーガイドの「 AWS のサービス と連携する IAM」を参照してください。

トピック

- Amazon EVS のアイデンティティベースのポリシー
- Amazon EVS のアクセスコントロールリスト (ACLs)
- Amazon EVS での属性ベースのアクセスコントロール (ABAC)
- Amazon EVS での一時的な認証情報の使用
- Amazon EVS の転送アクセスセッション
- Amazon EVS のサービスロール
- Amazon EVS のサービスにリンクされたロール

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 ユーザーグループ、ユーザーのグループ、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 Elastic VMware Service のアイデンティティベースのポリシーの例を確認するには、「Amazon Elastic VMware Service のアイデンティティベースのポリシーの例」を参照してください。

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

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 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 AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 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 AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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 AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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。例えば、リソースにアクセスするためのアクセス IAM ユーザー 許可は、 IAM ユーザー リソースの名前がタグ付けされている場合にのみ付与できます。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 Elastic VMware Service 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 Elastic VMware Service の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 Elastic VMware Service 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 Elastic VMware Service 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 での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。IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにタグをアタッチできます。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 Elastic VMware Service リソースにタグをアタッチすることも、Amazon Elastic VMware Service 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制御するには`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 Management Console 方法で にサインインする場合、一時的な認証情報を使用します。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することができます 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 Elastic VMware Service 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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

デフォルトでは、 IAM ユーザー および ロールには Amazon Elastic VMware Service 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 Management Console、 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 Elastic VMware Service 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 Elastic VMware Service 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を実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可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ときは、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。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、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 AWS 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 Elastic VMware Service コンソールの使用

Amazon Elastic VMware Service 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 Elastic VMware Service 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 Amazon Elastic VMware Service コンソールを引き続き使用できるようにするには、 などの独自の一意の名前の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、 IAM ユーザー 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。アカウントに 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"
            ],
            "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 Elastic VMware Service のアイデンティティとアクセスのトラブルシューティング

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

以下の情報は、Amazon Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースに対するアクセス許可を提供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 マネージド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 マネージド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、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 - お客様の VPC サブネットで 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、モニタリングできるようにするために必要です。

JSON ポリシードキュメントの最新バージョンを表示するには、 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 — 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 年 6 月 9 日
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 年 6 月 9 日

Amazon EVS のサービスにリンクされたロールの使用

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれます。アクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、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、VPCs。

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

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) 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 Management Console、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、「エンドポイントとクォータ」を参照してください。

他の AWS サービスでの Amazon EVS の使用

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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および設定するには、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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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、「入門」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内で、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、Amazon FSx for NetApp ONTAP を VMware vSphere の外部ストレージとして設定します。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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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、「入門」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。

ESXi 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

ESXi ホストごとに、ソフトウェア iSCSI アダプターを設定して、ESXi 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 ESXi 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、ESXi 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

ESXi 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 ESXi 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 Datastore 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

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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、環境で自動チェックを実行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特定できます。

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 が環境に到達できない場合、このチェックは失敗します。

このチェックが失敗すると、Amazon EVS は SDDC Manager に到達して環境ステータスを検証できなくなり、ホストを環境に追加できなくなります。また、到達可能性に障害が発生すると、ライセンスキーの再利用とキーカバレッジチェックが失敗し、ホスト数チェックで不明なレスポンスが返されます。

Reachabilty の失敗は、SDDC Manager、ファイアウォール設定、または証明書の欠落に問題がある可能性があることを示します。これらの問題の解決を試みるか、 AWS サポートにお問い合わせください。

ホスト数チェックに失敗しました

このチェックでは、環境のホストが最低 4 つあることを確認します。これは VCF 5.2.1 の要件です。

このチェックが失敗した場合は、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 個のホストを持つ環境のみをサポートします。

キーの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。使用済みライセンスが環境に追加されると、このチェックは失敗します。

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表示されます。この問題に対処するには、SDDC Manager のライセンス設定を確認し、以前に使用した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 VCF コンポーネントの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、SDDC Manager で有効なコンポーネントライセンスキーを維持する必要があります。vSphere Client を使用してコンポーネントライセンスキーを管理する場合は、ライセンスキーチェックの失敗を防ぐために、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。

このチェックに失敗すると、Amazon EVS 環境を作成できなかったか、Amazon EVS ホストを環境に追加できなかったというエラーレスポンスが表示されます。キーカバレッジの失敗は、次のいずれかの問題を示している可能性があります。

- Amazon EVS でサポートされているホスト数を超えました。Amazon EVS は、環境ごとに 4 ~ 16 個のホストをサポートします。この問題が発生した場合は、環境がサポートされているホスト範囲内になるまでホストを削除または追加します。
- VCF ライセンスが vCenter Server に正しく割り当てられていない。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。この問題が発生した場合は、SDDC Manager でライセンスの割り当てを確認します。
- 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。この問題が発生した場合は、使用ニーズが満たされるまで SDDC Manager に vSAN ライセンスを追加します。

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 VCF コンポーネントの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、SDDC Manager で有効なコンポーネントライセンスキーを維持する必要があります。vSphere Client を使用してコンポーネントライセンスキーを管理する場合は、ライセンスキーチェックの失敗を防ぐために、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、ESXi 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 サポートがない場合でも、vSphere HA のコア機能には影響しません。

vSphere HA エラーメッセージを削除するには、vSphere HA を無効にする必要があります。vSphere クライアントで vSphere HA を無効にする手順については、Broadcom の記事VMware High Availability (HA) の無効化と有効化」を参照してください。

ESXi 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 ESXi 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可能性があります。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、このトピックの「Broadcom ナレッジベースの記事」を参照してください。

Amazon Elastic VMware Service エンドポイントとクォータ

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

このサービスのサービスエンドポイントおよび Service Quotas を以下に示します。プログラムで に接続するには AWS のサービス、 エンドポイントを使用します。標準 AWS エンドポイントに加えて、一部の は選択したリージョンで FIPS エンドポイント AWS のサービス を提供します。詳細については、AWS サービスエンドポイントを参照してください。サービスクォータ (制限とも呼ばれます) は、 AWS アカウントのサービスリソースまたはオペレーションの最大数です。詳細については、「AWS サービスクォータ」を参照してください。

サービスエンドポイント

Amazon EVS API は、リージョンエンドポイントとデュアルスタックエンドポイント、および米国リージョンの FIPS エンドポイントを提供します。でデュアルスタックエンドポイントを使用するには AWS CLI、「 SDK およびツールリファレンスガイド」の「デュアルスタックと FIPS エンドポイントの設定」を参照してください。 AWS SDKs

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (バージニア北部)	us-east-1	evs.us-east-1.amazonaws.com evs-fips.us-east-1.amazonaws.com evs.us-east-1.api.aws evs-fips.us-east-1.api.aws	HTTPS
米国東部 (オハイオ)	us-east-2	evs.us-east-2.amazonaws.com evs-fips.us-east-2.amazonaws.com evs.us-east-2.api.aws evs-fips.us-east-2.api.aws	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
米国西部 (オレゴン)	us-west-2	evs.us-west-2.amazonaws.com evs-fips.us-west-2.amazonaws.com evs.us-west-2.api.aws evs-fips.us-west-2.api.aws	HTTPS
アジアパシフィック (東京)	ap-northeast-1	evs.ap-northeast-1.amazonaws.com evs.ap-northeast-1.api.aws	HTTPS
欧州 (フランクフルト)	eu-central-1	evs.eu-central-1.amazonaws.com evs.eu-central-1.api.aws	HTTPS
欧州 (アイルランド)	eu-west-1	evs.eu-west-1.amazonaws.com evs.eu-west-1.api.aws	HTTPS

Service Quotas

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。詳細については、「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 Management Console 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

> **Important**
>
> Amazon EVS 環境の作成を有効にするには、EVS 環境クォータあたりのホスト数が 4 以上である必要があります。デフォルトのクォータは 0 です。このクォータを引き上げるには、Service Quotas コンソールに移動し、クォータの引き上げをリクエストします。

Important

EC2 Running On-Demand Standard Instance 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 vCPUs 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 vCPUs 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「引き上げをリクエストする」を参照してください。

Note

Amazon EVS 環境に EC2 Dedicated Hosts を使用する予定がある場合は、EC2 Dedicated i4i Hosts のクォータに、目的のリージョンに使用する Dedicated Hosts 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「引き上げをリクエストする」を参照してください。

名前	デフォルト	引き上げ可能	説明
EVS 環境あたりのホスト数	0	あり	1 つの Amazon EVS 環境でプロビジョニングできるホストの最大数。
AWS アカウントあたりの環境数	1	あり	このアカウントで現在のリージョンに作成できる EVS 環境の最大数。

Amazon Elastic VMware Service ユーザーガイドのドキュメント履歴

> **Note**
>
> Amazon EVS はパブリックプレビューリリースであり、変更される可能性があります。

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
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 管理ポリシー 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	2025 年 6 月 9 日

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。

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。