사용 설명서

Amazon Elastic VMware Service

Amazon Elastic VMware Service: 사용 설명서

Table of Contents

Amazon Elastic VMware Service란 무엇입니까?

Amazon Elastic VMware Service(Amazon EVS)를 사용하여 (VPC) 내의 EC2 베어 메탈 인스턴스에 VMware Cloud Foundation Amazon Virtual Private Cloud (VCF) 환경을 직접 배포하고 실행할 수 있습니다.

주제

Amazon EVS의 기능

다음은 Amazon EVS의 주요 기능입니다.

로 마이그레이션 간소화 및 가속화 AWS

클라우드에서 VMware Cloud Foundation(VCF)의 구독 이동성 및 자동 배포를 통해 마이그레이션 마찰을 제거하고 운영 일관성을 보장합니다. IP 주소를 변경하거나, 직원을 재교육하거나, 운영 런북을 다시 작성할 필요 없이 온프레미스 네트워크를 확장하고 워크로드를 마이그레이션합니다.

클라우드에서 VMware 아키텍처 제어 유지

VMware 아키텍처를 완벽하게 제어하고 추가 기능 및 타사 솔루션을 포함하여 애플리케이션의 고유한 요구 사항을 충족하는 가상화 스택을 최적화합니다.

관리형 경험을 위한 AWS 파트너 자체 관리 또는 활용

선택과 유연성을 활용하여 자체 관리하거나 AWS 파트너의 전문 지식을 활용하여에서 VCF 환경을 관리하고 운영 AWS 하여 인재, 시간 및 비용 전반에서 비즈니스 목표를 달성할 수 있습니다.

운영 중단으로부터 비즈니스 확장 및 보호

VMware 기반 워크로드를 마이그레이션하고 운영하기 위해 가장 안전하고 확장 가능하며 복원력이 뛰어난 클라우드에서 확장성을 개선합니다.

AWS 혁신을 수용하여 애플리케이션 및 인프라 혁신

AWS네이티브 서비스인 Amazon EVS는 200개 이상의 서비스(관리형 데이터베이스, 분석, 서버리스 및 컨테이너, 생성형 AI 포함)를 통해 VMware 환경 확장 및 확장을 간소화하여 비즈니스를 혁신합니다.

Amazon EVS 시작하기

첫 번째 Amazon EVS 환경을 생성하려면 섹션을 참조하세요시작하기. 일반적으로 Amazon EVS를 시작하려면 다음 단계를 완료해야 합니다.

1. 사전 조건을 완료합니다. 자세한 내용은 Amazon Elastic VMware Service 설정 단원을 참조하십시오.
2. Amazon EVS 환경을 생성합니다. 환경 생성 중에 Amazon EVS는 지정한 CIDR 범위를 사용하여 필요한 VLAN 서브넷을 생성하고 호스트를 환경에 추가합니다.
3. VCF를 사용자 지정합니다. 필요에 따라 vSphere 사용자 인터페이스에서 환경을 구성합니다. 여기에는 로그인, 정책, 모니터링 설정 등이 포함될 수 있습니다.
4. 연결 및 마이그레이션. 환경을 온프레미스 데이터 센터에 연결하고 VCF 워크로드를 Amazon EVS로 마이그레이션합니다.

Amazon EVS 액세스

다음 인터페이스를 사용하여 Amazon EVS 배포를 정의하고 구성할 수 있습니다.

- Amazon EVS 콘솔 - Amazon EVS 환경을 생성하기 위한 웹 인터페이스를 제공합니다.
- AWS CLI - 광범위한 AWS 서비스 및에 대한 명령을 제공하며 Windows, macOS 및 Linux에서 지원됩니다. 자세한 내용은 AWS Command Line Interface 단원을 참조하십시오.
- AWS CloudFormation -와 같은 각 리소스 유형에 대한 사양을 제공합니다`AWS::EVS::Environment`. 리소스 사양을 사용하여 템플릿을 생성하면 CloudFormation에서 리소스를 프로비저닝하고 구성합니다.

Amazon EVS의 개념 및 구성 요소

이 섹션에서는 몇 가지 주요 Amazon EVS 개념 및 구성 요소에 대해 설명합니다.

Amazon EVS 환경

Amazon EVS 환경은 vSphere 호스트, vSAN, NSX 및 SDDC Manager와 같은 VMware Cloud Foundation(VCF) 리소스를 위한 논리적 컨테이너입니다. 환경에는 VCF 소프트웨어 스택의 관리, 모니터링 및 인스턴스화를 위한 구성 요소를 호스팅하는 vSphere 클러스터가 있는 통합 VCF 도메인이 포함됩니다. 각 환경은 SDDC Manager 어플라이언스에 직접 매핑됩니다. 자세한 내용은 the section called “아키텍처” 단원을 참조하십시오.

Amazon EVS 호스트

Amazon EVS 호스트는 Amazon EC2 베어 메탈 인스턴스에서 실행되는 VMware ESX 호스트입니다. Amazon EVS 호스트는 관리 및 워크로드 가상 머신을 저장하는 vSAN 데이터 스토어용 로컬 NVMe 인스턴스 스토어 볼륨을 사용합니다.

> **Warning**
>
> 인스턴스 스토어 볼륨은 임시 볼륨입니다. 기본 EC2 인스턴스가 중지되거나 종료된 경우 이러한 볼륨에 저장된 데이터는 지속되지 않습니다. VCF 내에서 서비스 해제 없이 Amazon EVS에서 사용하는 Amazon EC2 인스턴스를 중지하거나 종료하면 데이터가 손실될 수 있습니다. 호스트 유지 관리에 대한 자세한 내용은 섹션을 참조하세요the section called “호스트 유지 관리”.

서비스 액세스 서브넷

서비스 액세스 서브넷은 Amazon EVS가 VCF 배포에 액세스할 수 있도록 허용하는 표준 VPC 서브넷입니다. Amazon EVS 환경을 생성하는 동안 서비스 액세스에 사용할 Amazon EVS의 VPC 및 서브넷을 지정합니다.

Amazon EVS 환경을 생성하면 Amazon EVS는 서비스 액세스 서브넷에 탄력적 네트워크 인터페이스를 프로비저닝하여 VCF 어플라이언스 및 ESX 호스트에 대한 관리 연결을 용이하게 합니다. Amazon EVS가 VCF 배포를 배포, 관리 및 모니터링하려면이 연결이 필요합니다.

Amazon EVS VLAN 서브넷

Amazon EVS VLAN 서브넷은 Amazon EVS에서 관리하는 Amazon VPC 서브넷입니다. VLAN 서브넷은 Amazon EVS 호스트와 VMware NSX, VMware HCX, VMware vCenter Server와 같은 VCF 어플라이언스에 VPC 연결을 제공합니다. 각 VLAN 서브넷에는 VLAN 네트워크 트래픽을 논리적으로 분할할 수 있는 VLAN 태그가 있습니다.

Amazon EVS는 Amazon EVS 환경이 생성될 때 서비스가 사용하는 모든 VLAN 서브넷을 생성합니다. VLAN 서브넷이 사용하는 CIDR 블록 입력을 제공합니다. 향후 조정 요구 사항을 고려하여 구성할 호스트 수에 따라 VLAN 서브넷 CIDR 블록의 크기가 적절한지 확인해야 합니다. CIDR 블록의 최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. CIDR 블록은 VPC와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.

생성 시 VLAN 서브넷은 VPC의 기본 라우팅 테이블에 암시적으로 연결됩니다. 배포 후 VLAN 서브넷을 사용자 지정 라우팅 테이블과 명시적으로 연결할 수 있습니다. 자세한 내용은 the section called “Amazon EVS 네트워킹 고려 사항” 단원을 참조하십시오.

Important

Amazon EVS VLAN 서브넷은 Amazon EVS 환경 생성 중에만 생성할 수 있으며 환경이 생성된 후에는 수정할 수 없습니다. 환경을 생성하기 전에 VLAN 서브넷 CIDR 블록의 크기가 적절한지 확인해야 합니다. 환경이 배포된 후에는 VLAN 서브넷을 추가할 수 없습니다.

Important

EC2 보안 그룹 규칙은 VLAN 서브넷에 연결된 Amazon EVS 탄력적 네트워크 인터페이스에는 적용되지 않습니다. VLAN 서브넷과 주고받는 트래픽을 제어하려면 네트워크 액세스 제어 목록을 사용해야 합니다.

호스트 관리 VLAN 서브넷

호스트 관리 VLAN 서브넷은 관리 트래픽을 사용자 트래픽과 분리하고 호스트의 원격 관리를 허용합니다. EVS 호스트 관리 vmkernel 네트워크 인터페이스는이 서브넷에 연결됩니다.

vMotion VLAN 서브넷

vMotion VLAN 서브넷은 VMware vMotion 트래픽을 논리적으로 분할하며 vMotion 프로세스 중에 호스트 간에 가상 머신을 이동하는 데 사용됩니다.

vSAN VLAN 서브넷

vSAN VLAN 서브넷은 VMware vSAN에서 vSAN의 스토리지 작업과 관련된 트래픽을 다른 네트워크 트래픽과 분리하는 데 사용됩니다.

VTEP VLAN 서브넷

VTEP VLAN 서브넷은 VMware NSX 가상 터널 엔드포인트(VTEP)를 사용하여 Amazon EVS ESX 호스트에 대한 오버레이 네트워크 트래픽을 캡슐화하고 캡슐화 해제합니다.

엣지 VTEP VLAN 서브넷

Edge VTEP VLAN 서브넷은 NSX Edge 어플라이언스 오버레이 트래픽 전용 특수 VTEP VLAN 서브넷입니다. 이 VLAN은 NSX 엣지와 ESX 호스트 간의 오버레이 통신에 사용됩니다.

관리 VM VLAN 서브넷

Management VM VLAN 서브넷은 NSX Manager, vCenter Server 및 SDDC Manager를 포함한 가상 어플라이언스를 관리하는 데 사용됩니다.

HCX 업링크 VLAN 서브넷

HCX 업링크 VLAN 서브넷은 HCX 상호 연결(HCX-IX)과 HCX 네트워크 확장(HCX-NE) 어플라이언스 간의 통신에 사용되며 HCX 서비스 메시 업링크를 생성할 수 있습니다.

NSX 업링크 VLAN 서브넷

NSX 업링크 VLAN 서브넷은 NSX 오버레이 네트워크를 나머지 VPC 및 구성한 기타 외부 네트워크에 연결하는 데 사용됩니다. NSX 업링크 VLAN 서브넷은 NSX 엣지 노드 업링크에 구성됩니다.

확장 VLAN 서브넷

확장 VLAN 서브넷을 사용하여 NSX 페더레이션과 같은 추가 VCF 지원 함수를 활성화할 수 있습니다. Amazon EVS는 환경 생성 중에 두 개의 확장 VLAN 서브넷을 생성합니다.

VMware NSX

VMware NSX는 네트워크 가상화를 지원하는 소프트웨어 정의 네트워킹(SDN) 플랫폼입니다. Amazon EVS는 VMware NSX를 사용하여 VMware Cloud Foundation(VCF) 어플라이언스 및 워크로드가 실행되는 오버레이 네트워크를 생성하고 관리합니다. Amazon EVS는 NSX 오버레이 네트워크와 함께 Active/Standby NSX Edge 노드 쌍을 배포합니다. Amazon EVS는 배포의 일부로 사용자를 대신하여 모든 NSX 라우팅 및 업링크를 자동으로 구성합니다. 일반적인 NSX 개념에 대한 자세한 내용은 VMware NSX 설치 안내서의 주요 개념을 참조하세요.

VMware Hybrid Cloud Extension(HCX)

VMware Hybrid Cloud Extension(VMware HCX)은 애플리케이션 마이그레이션을 간소화하고, 워크로드를 리밸런싱하고, 데이터 센터 및 클라우드 전반에서 재해 복구를 최적화하도록 설계된 애플리케이션 모빌리티 플랫폼입니다. HCX를 사용하여 VMware 기반 워크로드를 Amazon EVS로 마이그레이션할 수 있습니다.

연결된 전송 게이트웨이와 Direct Connect 함께를 사용하거나 전송 게이트웨이에 AWS Site-to-Site VPN 연결을 사용하여 VMware HCX에 대한 연결을 구성할 수 있습니다. 자세한 내용은 마이그레이션 단원을 참조하십시오.

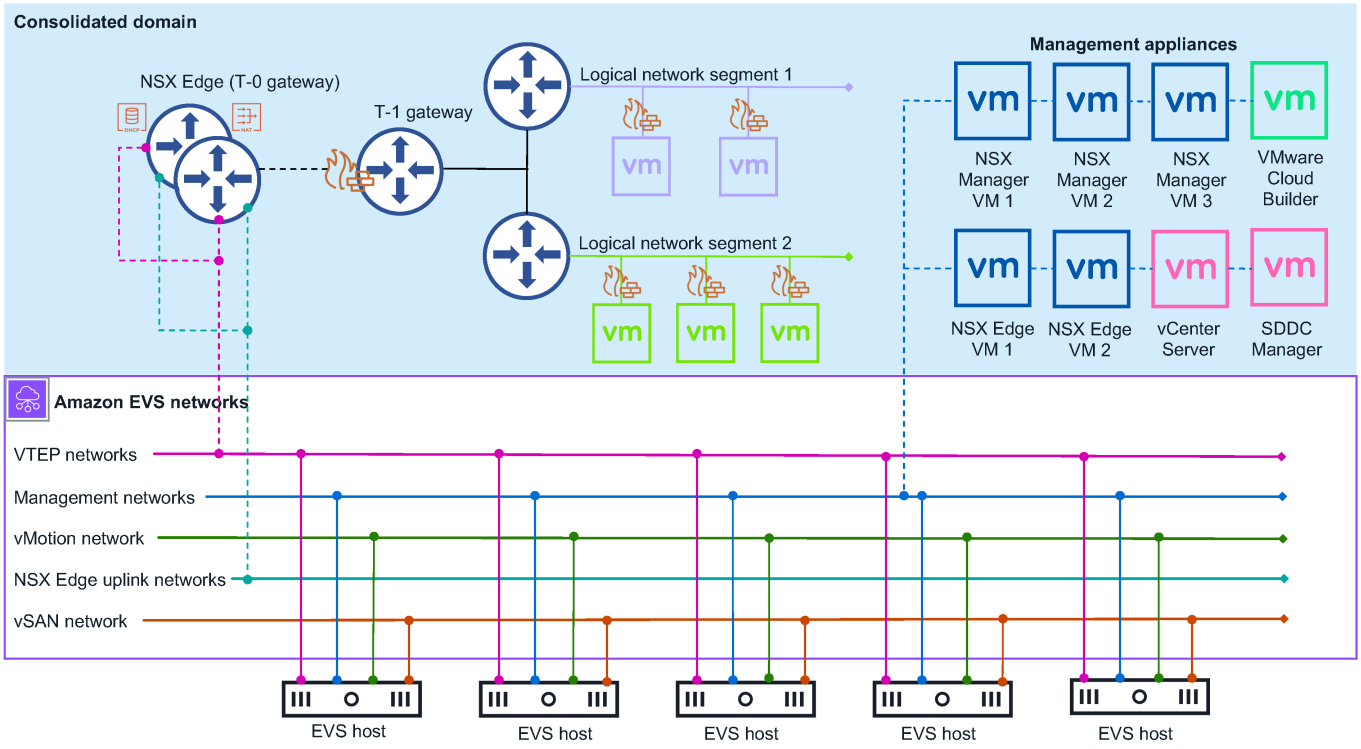
Amazon EVS 아키텍처

Amazon EVS는 VMware Cloud Foundation(VCF) 통합 아키텍처 모델을 구현합니다. 이 모델에서 VCF 관리 구성 요소와 고객 워크로드는 통합 도메인에서 함께 실행됩니다. Amazon EVS 환경은 관리 워크로드와 고객 워크로드를 격리하는 vSphere 리소스 풀이 있는 단일 vCenter Server에서 관리됩니다.

Amazon EVS가 배포하는 통합 도메인에는 다음과 같은 VCF 관리 구성 요소가 포함되어 있습니다.

- ESX 호스트
- vCenter Server 인스턴스
- SDDC 관리자
- vSAN 데이터 스토어
- 3노드 NSX Manager 클러스터
- vSphere 클러스터
- NSX Edge 클러스터

다음 다이어그램은 Amazon EVS 환경에 배포된 예제 Amazon EVS 아키텍처와 환경의 구성 요소가 연결되는 방법을 보여줍니다. 다이어그램에서 통합 도메인 아키텍처가 있는 Amazon EVS 환경은 파란색으로 음영 처리됩니다. 기본 Amazon EVS 네트워크 토폴로지는 보라색 실선으로 표시됩니다.



네트워크 토폴로지

Amazon EVS 환경에는 두 개의 개별 관리 네트워크 계층이 있습니다.

Amazon VPC

환경 생성 중에 VPC에 생성된 Amazon VPC 및 Amazon EVS VLAN 서브넷은 VCF 배포를 위한 언더레이 네트워크를 형성합니다. 이 인프라는 NSX 오버레이 네트워크, 호스트 관리, vMotion 및 VSAN에 대한 연결을 제공합니다. Amazon VPC Route Server는 언더레이 네트워크와 오버레이 네트워크 간의 동적 라우팅을 활성화합니다. 자세한 내용은 the section called “개념 및 구성 요소” 단원을 참조하십시오.

> **Note**
>
> Amazon EVS VLAN 서브넷은 VCF 언더레이 통신을 용이하게 하는 데에만 사용됩니다. 고객 워크로드를 실행하는 게스트 가상 머신은 NSX 오버레이 네트워크에 배포해야 합니다. Amazon EVS VLAN 서브넷 언더레이 네트워크에 게스트 가상 머신을 배포하는 것은 지원되지 않습니다.

VMware NSX 오버레이 네트워크

Amazon EVS는 배포의 일부로 사용자를 대신하여 NSX 오버레이 네트워크를 구성합니다. Amazon EVS 환경 내의 다양한 워크로드 또는 애플리케이션 간에 네트워크 격리를 달성하도록 추가 NSX 오버레이 네트워크를 구성할 수 있습니다. 자세한 내용은 VMware Cloud Foundation 제품 설명서의 Overlay Design for VMware Cloud Foundation을 참조하세요.

> **Note**
>
> Amazon EVS는 두 개의 NSX Edge 노드가 있는 Active/Standby NSX Edge 클러스터에 대해 하나의 티어-0 게이트웨이만 지원합니다. 이 tier-0 게이트웨이는 Amazon EVS와 함께 사용하도록 구성한 모든 오버레이 네트워크에 연결하고 알립니다.

두 네트워크 계층은 두 개의 NSX Edge 노드가 있는 Active/Standby NSX Edge 클러스터에 의해 연결됩니다. NSX Edge 노드는 VLANs의 가상 머신 간 VPC를 통한 통신과 인터넷 연결, 전송 게이트웨이와 함께 Direct Connect or AWS Site-to-Site VPN을 사용한 프라이빗 연결을 지원합니다.

Amazon EVS 네트워킹 고려 사항

관리 네트워크에는 다음과 같은 네트워킹 리소스 구성이 필요합니다. Amazon EVS 환경을 생성하는 동안 이러한 입력을 제공합니다. 자세한 내용은 the section called “개념 및 구성 요소” 단원을 참조하십시오.

- Amazon VPC. 환경 생성 중에 Amazon EVS가 프로비저닝하는 필수 VPC 서브넷 및 Amazon EVS VLAN 서브넷을 수용할 수 있도록 VPC IPv4 CIDR 블록의 크기가 적절한지 확인합니다. 자세한 내용은 the section called “Amazon EVS VLAN 서브넷” 단원을 참조하십시오.

  > **Note**
  >
  > Amazon EVS는 현재 IPv6를 지원하지 않습니다.

- VPC의 서비스 액세스 서브넷입니다. Amazon EVS는이 서브넷을 사용하여 SDDC Manager 어플라이언스에 대한 지속적인 연결을 유지합니다. 자세한 내용은 the section called “서비스 액세스 서브넷” 단원을 참조하십시오.

> **Note**
>
> Amazon EVS는 현재 단일 AZ 배포만 지원합니다. Amazon EVS가 사용하는 모든 VPC 서브넷은 서비스를 사용할 수 있는 리전의 단일 가용 영역에 있어야 합니다.

> **Note**
>
> 모든 VPC 서브넷에는 조직의 네트워킹 요구 사항에 따라 구성된 연결된 라우팅 테이블이 필요합니다.

- 호스트 IP 주소를 확인하도록 설정된 VPC의 DHCP 옵션에 있는 기본 DNS 서버 IP 주소 및 보조 DNS 서버 IP 주소입니다. 또한 Amazon EVS에서는 배포의 각 VCF 관리 어플라이언스 및 Amazon EVS 호스트에 대해 A 레코드가 있는 DNS 순방향 조회 영역과 PTR 레코드가 있는 역방향 조회 영역을 생성해야 합니다. 자세한 내용은 the section called “DNS 서버 구성” 단원을 참조하십시오.
- 환경 생성 중에 Amazon EVS가 프로비저닝하는 각 VLAN 서브넷에 대한 Amazon EVS VLAN 서브넷 CIDR 블록입니다. CIDR 블록의 최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. CIDR 블록은 겹치지 않아야 합니다.
- Amazon VPC Route Server 전파가 활성화된 Route Server 인스턴스입니다.
- 서비스 액세스 서브넷의 Route Server 엔드포인트 2개.
- Amazon EVS가 Route Server 엔드포인트로 프로비저닝하는 NSX Edge 노드를 피어링하는 두 개의 Route Server 피어입니다.

Tier-0 게이트웨이

tier-0 게이트웨이는 논리적 네트워크와 물리적 네트워크 간의 모든 남북 트래픽을 처리하고 NSX 오버레이 네트워크에서 생성됩니다. 이 tier-0 게이트웨이는 Amazon EVS 배포의 일부로 생성됩니다.

> **Note**
>
> Amazon EVS는 두 개의 NSX Edge 노드가 있는 Active/Standby NSX Edge 클러스터에 대해 하나의 티어-0 게이트웨이만 지원합니다.

Tier-1 게이트웨이

tier-1 게이트웨이는 환경 내에서 라우팅된 네트워크 세그먼트 간의 동서 트래픽을 처리하고 NSX 오버레이 네트워크에 생성됩니다. 티어-1 게이트웨이에는 세그먼트에 대한 다운링크 연결과 티어-0 게이트웨이에 대한 업링크 연결이 있습니다. 필요한 경우 추가 Tier-1 게이트웨이를 생성하고 구성할 수 있습니다.

NSX Edge 클러스터

Amazon EVS는 NSX 관리자 인터페이스를 사용하여 활성/대기 모드에서 실행되는 두 개의 NSX Edge 노드가 있는 NSX Edge 클러스터를 배포합니다. 이 NSX Edge 클러스터는 IPsec VPN 연결 및 BGP 라우팅 기계와 함께 Tier-0 및 Tier-1 게이트웨이가 실행되는 플랫폼을 제공합니다.

Amazon EVS 리소스

Amazon EVS는 환경 생성 중에 다음 AWS 리소스를 프로비저닝합니다. 이러한 리소스는 Amazon EVS가 액세스할 수 있도록 허용하는 VPC에 표시되며, 생성된 AWS Management Console 후 및 AWS CLI 에 표시됩니다.

> **Important**
>
> Amazon EVS 콘솔 및 API 외부에서 이러한 리소스를 수정하면 Amazon EVS 환경의 가용성과 안정성에 영향을 미칠 수 있습니다.

- VCF 어플라이언스 및 호스트에 연결할 수 있는 Amazon EVS 탄력적 네트워크 인터페이스입니다.
- Amazon EC2 베어 메탈 인스턴스에서 실행되는 Amazon EVS ESX 호스트입니다. 자세한 내용은 the section called “Amazon EVS 호스트” 단원을 참조하십시오.

  > **Important**
  >
  > Amazon EVS 환경에는 최소 4개의 호스트와 최대 16개의 호스트가 있어야 합니다. Amazon EVS는 호스트가 4~16개인 환경만 지원합니다.

- VPC를 VCF 어플라이언스에 연결하는 Amazon EVS VLAN 서브넷입니다. 자세한 내용은 the section called “Amazon EVS VLAN 서브넷” 단원을 참조하십시오.

Amazon Elastic VMware Service 설정

Amazon EVS를 사용하려면 다른 AWS 서비스를 구성하고 VMware Cloud Foundation(VCF) 요구 사항을 충족하도록 환경을 설정해야 합니다. 배포 사전 조건에 대한 요약 체크리스트는 섹션을 참조하세요the section called “배포 체크리스트”.

주제

에 가입 AWS

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

IAM 사용자를 생성합니다.

1. 루트 사용자를 선택하고 계정 AWS 이메일 주소를 입력하여 계정 소유자로 IAM 콘솔에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   > **Note**
   >
   > `Administrator` IAM 사용자를 사용하는 아래 모범 사례를 준수하고, 루트 사용자 자격 증명을 안전하게 보관해 두는 것이 좋습니다. 몇 가지 계정 및 서비스 관리 태스크를 수행하려면 반드시 루트 사용자로 로그인해야 합니다.

2. 탐색 창에서 사용자를 선택한 다음 사용자 생성을 선택합니다.
3. 사용자 이름에 `Administrator`를 입력합니다.
4. AWS Management Console 액세스 옆의 확인란을 선택합니다. 그런 다음 사용자 지정 암호를 선택하고 텍스트 상자에 새 암호를 입력합니다.
5. (선택 사항) 기본적으로 에서는 처음 로그인할 때 새 사용자가 새 암호를 생성해야 AWS 합니다. 사용자가 다음에 로그인할 때 새 암호를 생성해야 합니다(User must create a new password at next sign-in) 옆에 있는 확인란의 선택을 취소하면 새 사용자가 로그인한 후 암호를 재설정할 수 있습니다.
6. 다음: 권한을 선택합니다.
7. 권한 설정 아래에서 그룹에 사용자 추가를 선택합니다.
8. 그룹 생성을 선택합니다.
9. 그룹 생성 대화 상자의 그룹 이름에 `Administrators`를 입력합니다.
10. 정책 필터링을 선택한 다음 AWS 관리형 -작업 함수를 선택하여 테이블 내용을 필터링합니다.
11. 정책 목록에서 AdministratorAccess 확인란을 선택합니다. 그런 다음 그룹 생성을 선택합니다.

    > **Note**
    >
    > Billing and Cost Management 콘솔에 액세스할 수 있는 `AdministratorAccess` 권한을 사용하려면 AWS 먼저 결제에 대한 IAM 사용자 및 역할 액세스를 활성화해야 합니다. 이를 위해 결제 콘솔에 액세스를 위임하기 위한 자습서 1단계의 지침을 따르십시오.

12. 그룹 목록으로 돌아가 새 그룹의 확인란을 선택합니다. 목록에서 그룹을 확인하기 위해 필요한 경우 새로 고침을 선택합니다.
13. 다음: 태그를 선택합니다.

14. (선택 사항) 태그를 키 값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서 태그 사용에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티 태깅을 참조하십시오.
15. 다음: 검토를 선택하여 새 사용자에 추가될 그룹 멤버십의 목록을 확인합니다. 계속 진행할 준비가 되었으면 사용자 생성을 선택합니다.

이 동일한 프로세스를 사용하여 더 많은 그룹과 사용자를 생성하고 사용자에게 AWS 계정 리소스에 대한 액세스 권한을 부여할 수 있습니다. 사용자 권한을 특정 AWS 리소스로 제한하는 정책을 사용하는 방법에 대한 자세한 내용은 액세스 관리 및 정책 예제를 참조하세요.

IAM 사용자에게 Amazon EVS 권한을 위임하는 IAM 역할 생성

역할을 사용하여 AWS 리소스에 대한 액세스를 위임할 수 있습니다. IAM 역할을 사용하면 신뢰할 수 있는 계정과 다른 신뢰할 수 AWS 있는 계정 간에 신뢰 관계를 설정할 수 있습니다. 신뢰할 수 있는 계정은 액세스할 리소스를 소유하며, 신뢰할 수 있는 계정에는 리소스에 액세스해야 하는 사용자가 포함됩니다.

신뢰 관계를 생성한 후 신뢰할 수 있는 계정의 IAM 사용자 또는 애플리케이션은 AWS Security Token Service (AWS STS) `AssumeRole` API 작업을 사용할 수 있습니다. 이 작업은 계정의 AWS 리소스에 액세스할 수 있는 임시 보안 자격 증명을 제공합니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 사용자에게 권한을 위임할 역할 생성을 참조하세요.

다음 단계에 따라 Amazon EVS 작업에 대한 액세스를 허용하는 권한 정책을 사용하여 IAM 역할을 생성합니다.

> **Note**
>
> Amazon EVS는 인스턴스 프로파일을 사용하여 EC2 인스턴스에 IAM 역할을 전달하는 것을 지원하지 않습니다.

Example

IAM console

1. IAM 콘솔로 이동합니다.
2. 왼쪽 메뉴에서 정책을 선택합니다.
3. 정책 생성을 선택합니다.

4. 정책 편집기에서 Amazon EVS 작업을 활성화하는 권한 정책을 생성합니다. 정책 예제는 the section called “Amazon EVS 환경 생성 및 관리”을 참조하세요. 사용 가능한 모든 Amazon EVS 작업, 리소스 및 조건 키를 보려면 서비스 승인 참조의 작업을 참조하세요.
5. 다음을 선택합니다.
6. 정책 이름에 의미 있는 정책 이름을 입력하여이 정책을 식별합니다.
7. 이 정책에 정의된 권한을 검토합니다.
8. (선택 사항)이 리소스를 식별, 구성 또는 검색하는 데 도움이 되는 태그를 추가합니다.
9. 정책 생성을 선택합니다.
10. 왼쪽 메뉴에서 역할을 선택합니다.
11. 역할 생성을 선택합니다.
12. 신뢰할 수 있는 엔터티 유형에서를 선택합니다 AWS 계정.
13. 에서 Amazon EVS 작업을 수행할 계정을 AWS 계정 지정하고 다음을 선택합니다.
14. 권한 추가 페이지에서 이전에 생성한 권한 정책을 선택하고 다음을 선택합니다.
15. 역할 이름에 의미 있는 이름을 입력하여이 역할을 식별합니다.
16. 신뢰 정책을 검토하고 올바른 AWS 계정 가 보안 주체로 나열되어 있는지 확인합니다.
17. (선택 사항)이 리소스를 식별, 구성 또는 검색하는 데 도움이 되는 태그를 추가합니다.
18. 역할 생성을 선택합니다.

AWS CLI

1. 다음 내용을 신뢰 정책 JSON 파일에 복사합니다. 보안 주체 ARN의 경우 예제 AWS 계정 ID와 `service-user` 이름을 자신의 AWS 계정 ID와 IAM 사용자 이름으로 바꿉니다.

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

2. 역할을 생성합니다. `evs-environment-role-trust-policy.json`를 신뢰 정책 파일 이름으로 바꿉니다.

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

3. Amazon EVS 작업을 활성화하는 권한 정책을 생성하고 정책을 역할에 연결합니다. `myAmazonEVSEnvironmentRole`을 역할 이름으로 바꿉니다. 정책 예제는 the section called "Amazon EVS 환경 생성 및 관리"을 참조하세요. 사용 가능한 모든 Amazon EVS 작업, 리소스 및 조건 키를 보려면 서비스 승인 참조의 작업을 참조하세요.

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

AWS Business, AWS Enterprise On-Ramp 또는 AWS Enterprise Support 플랜에 가입

Amazon EVS를 사용하려면 고객이 AWS Business, AWS Enterprise On-Ramp 또는 AWS Enterprise Support 플랜에 등록되어 있어야 기술 지원 및 아키텍처 지침에 지속적으로 액세스할 수 있습니다. AWS Business Support는 Amazon EVS 요구 사항을 충족하는 최소 AWS 지원 티어입니다. 비즈니스 크리티컬 워크로드가 있는 경우 AWS Enterprise On-Ramp 또는 AWS Enterprise Support 플랜에 등록하는 것이 좋습니다. 자세한 내용은 AWS 지원 플랜 비교를 참조하세요.

> **Important**
>
> AWS Business, AWS Enterprise On-Ramp 또는 AWS Enterprise Support 플랜에 가입하지 않으면 Amazon EVS 환경 생성이 실패합니다.

할당량 확인

Amazon EVS 환경 생성을 활성화하려면 계정에 필요한 최소 계정 수준 할당량이 있는지 확인합니다. 자세한 내용은 Service Quotas 단원을 참조하십시오.

> **Important**
>
> EVS 환경 할당량 값당 호스트 수가 4 이상이 아닌 경우 Amazon EVS 환경 생성이 실패합니다.

VPC CIDR 크기 계획

Amazon EVS 환경을 생성할 때 VPC CIDR 블록을 지정해야 합니다. 환경이 생성된 후에는 VPC CIDR 블록을 변경할 수 없으며, Amazon EVS가 환경 배포 중에 생성하는 필수 EVS 서브넷 및 호스트를 수용할 수 있도록 충분한 공간을 예약해야 합니다. 따라서 배포 전에 Amazon EVS 요구 사항과 향후 규모 조정 요구 사항을 고려하여 CIDR 블록 크기를 신중하게 계획하는 것이 중요합니다. Amazon EVS에는 필요한 EVS 서브넷 및 호스트에 충분한 공간을 허용하려면 최소 크기가 /22 넷마스크인 VPC CIDR 블록이 필요합니다. 자세한 내용은 the section called “Amazon EVS 네트워킹 고려 사항” 단원을 참조하십시오.

> **Important**
>
> Amazon EVS가 VCF 어플라이언스용으로 생성하는 VPC 서브넷과 VLAN 서브넷 모두에 대해 충분한 IP 주소 공간이 있는지 확인합니다. 필요한 EVS 서브넷 및 호스트에 충분한 공간을 허용하려면 VPC CIDR 블록의 최소 크기가 /22 넷마스크여야 합니다.

> **Note**
>
> Amazon EVS는 현재 IPv6를 지원하지 않습니다.

서브넷이 있는 VPC 생성

Amazon EVS는 사용자가 제공하는 VPC에 환경을 배포합니다. 이 VPC에는 Amazon EVS 서비스 액세스()를 위한 서브넷이 포함되어야 합니다the section called “서비스 액세스 서브넷”. Amazon EVS용 서브넷이 있는 VPC를 생성하는 단계는 섹션을 참조하세요the section called “서브넷 및 라우팅 테이블이 있는 VPC 생성”.

VPC 기본 라우팅 테이블 구성

Amazon EVS VLAN 서브넷은 VPC 기본 라우팅 테이블에 암시적으로 연결됩니다. 성공적인 환경 배포를 위해 DNS 또는 온프레미스 시스템과 같은 종속 서비스에 대한 연결을 활성화하려면 이러한 시스템에 대한 트래픽을 허용하도록 기본 라우팅 테이블을 구성해야 합니다. 자세한 내용은 the section called “Amazon EVS VLAN 서브넷을 VPC 라우팅 테이블에 명시적으로 연결” 단원을 참조하십시오.

> **Important**
>
> Amazon EVS는 Amazon EVS 환경이 생성된 후에만 사용자 지정 라우팅 테이블 사용을 지원합니다. Amazon EVS 환경 생성 중에는 사용자 지정 라우팅 테이블을 사용해서는 안 됩니다. 연결 문제가 발생할 수 있습니다.

게이트웨이 라우팅 요구 사항

연결 요구 사항에 따라 이러한 게이트웨이 유형에 대한 경로를 구성합니다.

- NAT 게이트웨이(NGW)
  - 아웃바운드 전용 인터넷 액세스의 경우 선택 사항입니다.
  - 인터넷 게이트웨이에 액세스할 수 있는 퍼블릭 서브넷에 있어야 합니다.
  - 프라이빗 서브넷 및 EVS VLAN 서브넷의 경로를 NAT 게이트웨이에 추가합니다.
  - 자세한 내용은 Amazon VPC 사용 설명서의 NAT 게이트웨이 작업을 참조하세요.
- 전송 게이트웨이(TGW)
  - AWS Direct Connect 및 AWS Site-to-Site VPN을 통한 온프레미스 연결에 필요합니다.
  - 온프레미스 네트워크 범위에 대한 경로를 추가합니다.
  - BGP를 사용하는 경우 라우팅 전파를 구성합니다.
  - 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC Transit Gateways의 전송 게이트웨이를 참조하세요.

모범 사례

- 모든 라우팅 테이블 구성을 문서화합니다.
- 일관된 이름 지정 규칙을 사용합니다.
- 라우팅 테이블을 정기적으로 감사합니다.

- 변경 후 연결을 테스트합니다.
- 라우팅 테이블 구성을 백업합니다.
- 라우팅 상태 및 전파를 모니터링합니다.

라우팅 테이블 작업에 대한 자세한 내용은 Amazon VPC 사용 설명서의 라우팅 테이블 구성을 참조하세요.

VPC의 DHCP 옵션 세트 구성

Important

이러한 Amazon EVS 요구 사항을 충족하지 않으면 환경 배포가 실패합니다.

- DHCP 옵션 세트에 기본 DNS 서버 IP 주소와 보조 DNS 서버 IP 주소를 포함합니다.
- 배포의 각 VCF 관리 어플라이언스 및 Amazon EVS 호스트에 대한 A 레코드와 함께 DNS 순방향 조회 영역을 포함합니다.
- 배포의 각 VCF 관리 어플라이언스 및 Amazon EVS 호스트에 대한 PTR 레코드와 함께 DNS 역방향 조회 영역을 포함합니다.
- DNS 서버에 대한 경로가 존재하도록 VPC의 기본 라우팅 테이블을 구성합니다.
- 도메인 이름 등록이 유효하며 만료되지 않았는지, 중복된 호스트 이름이나 IP 주소가 없는지 확인합니다.
- Amazon EVS가 다음과 통신할 수 있도록 보안 그룹 및 네트워크 액세스 제어 목록(ACLs)을 구성합니다.
  - TCP/UDP 포트 53을 통한 DNS 서버.
  - HTTPS 및 SSH를 통한 호스트 관리 VLAN 서브넷입니다.
  - HTTPS 및 SSH를 통한 관리 VLAN 서브넷.

자세한 내용은 the section called “VPC DHCP 옵션 세트를 사용한 DNS 및 NTP 서버 구성” 단원을 참조하십시오.

VPC Route Server 인프라 생성 및 구성

Amazon EVS는 Amazon VPC Route Server를에 사용하여 VPC 언더레이 네트워크에 대한 BGP 기반 동적 라우팅을 활성화합니다. 서비스 액세스 서브넷에서 두 개 이상의 라우팅 서버 엔드포인트에 대한

경로를 공유하는 라우팅 서버를 지정해야 합니다. 라우팅 서버 피어에 구성된 피어 ASN은 일치해야 하며 피어 IP 주소는 고유해야 합니다.

Important

VPC Route Server 구성에 대한 다음 Amazon EVS 요구 사항을 충족하지 않으면 환경 배포가 실패합니다.

- 서비스 액세스 서브넷에서 라우팅 서버 엔드포인트를 두 개 이상 구성해야 합니다.
- Tier-0 게이트웨이에 대해 BGP(Border Gateway Protocol)를 구성할 때 VPC Route Server 피어 ASN 값은 NSX Edge 피어 ASN 값과 일치해야 합니다.
- 두 라우팅 서버 피어를 생성할 때 각 엔드포인트에 대해 NSX 업링크 VLAN의 고유한 IP 주소를 사용해야 합니다. 이 두 IP 주소는 Amazon EVS 환경 배포 중에 NSX 엣지에 할당됩니다.
- Route Server 전파를 활성화할 때 전파되는 모든 라우팅 테이블에 하나 이상의 명시적 서브넷 연결이 있는지 확인해야 합니다. 전파된 라우팅 테이블에 명시적 서브넷 연결이 없는 경우 BGP 라우팅 광고가 실패합니다.

Note

Route Server 피어 실시간 감지의 경우 Amazon EVS는 기본 BGP 연결 유지 메커니즘만 지원합니다. Amazon EVS는 다중 홉 양방향 전달 감지(BFD)를 지원하지 않습니다.

사전 조건

시작하려면 다음이 필요합니다.

- 라우팅 서버의 VPC 서브넷입니다.
- VPC Route Server 리소스를 관리하기 위한 IAM 권한.
- 라우팅 서버의 BGP ASN 값(Amazon 측 ASN). 값은 1~4294967295 범위에 있어야 합니다.
- 라우팅 서버를 NSX Tier-0 게이트웨이와 피어링하는 피어 ASN입니다. 라우팅 서버와 NSX Tier-0 게이트웨이에 입력된 피어 ASN 값이 일치해야 합니다. NSX Edge 어플라이언스의 기본 ASN은 65000입니다.

단계(Steps)

VPC Route Server를 설정하는 단계는 Route Server 시작하기 자습서를 참조하세요.

> **Note**
>
> NAT 게이트웨이 또는 전송 게이트웨이를 사용하는 경우 VPC 라우팅 테이블(들)에 NSX 경로를 전파하도록 라우팅 서버가 올바르게 구성되어 있는지 확인합니다.

> **Note**
>
> 라우팅 서버 인스턴스에 대해 지속 기간이 1~5분인 영구 경로를 활성화하는 것이 좋습니다. 활성화하면 모든 BGP 세션이 종료되더라도 라우팅 서버의 라우팅 데이터베이스에 경로가 보존됩니다.

> **Note**
>
> Amazon EVS 환경이 배포되고 작동할 때까지 BGP 연결 상태가 중단됩니다.

온프레미스 연결을 위한 전송 게이트웨이 생성

연결된 전송 게이트웨이와 Direct Connect 함께를 사용하거나 전송 게이트웨이에 AWS Site-to-Site VPN 연결을 사용하여 AWS 인프라에 대한 온프레미스 데이터 센터의 연결을 구성할 수 있습니다. 자세한 내용은 the section called “온프레미스 네트워크 연결 구성(선택 사항)” 단원을 참조하십시오.

Amazon EC2 용량 예약 생성

Amazon EVS는 Amazon EVS 환경에서 ESX 호스트를 나타내는 Amazon EC2 i4i.metal 인스턴스를 시작합니다. 필요할 때 사용할 수 있는 충분한 i4i.metal 인스턴스 용량이 있는지 확인하려면 Amazon EC2 용량 예약을 요청하는 것이 좋습니다. 언제든지 용량 예약을 생성할 수 있고, 시작 시기를 선택할 수 있습니다. 즉시 사용할 수 있도록 용량 예약을 요청하거나 향후 날짜에 대한 용량 예약을 요청할 수 있습니다. 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 EC2 온디맨드 용량 예약을 사용하여 컴퓨팅 용량 예약을 참조하세요.

설정 AWS CLI

AWS CLI 는 Amazon EVS를 AWS 서비스포함하여 작업을 위한 명령줄 도구입니다. 또한 로컬 시스템에서 Amazon EVS 가상화 환경 및 기타 AWS 리소스에 액세스할 수 있도록 IAM 사용자 또는 역할을 인증하는 데 사용됩니다. 명령줄에서 AWS 리소스를 프로비저닝하려면 명령줄에 사용할 AWS 액세스 키 ID와 보안 키를 얻어야 합니다. 그런 다음, AWS CLI에서 이러한 보안 인증 정보를 구성해야 합니다. 자세한 내용은 버전 2 사용 설명서의 설정을 AWS CLI 참조하세요. AWS Command Line Interface

Amazon EC2 키 페어 생성

Amazon EVS는 환경 생성 중에 제공하는 Amazon EC2 키 페어를 사용하여 호스트에 연결합니다. 키 페어를 생성하려면 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EC2 인스턴스에 대한 키 페어 생성 단계를 따르세요.

VMware Cloud Foundation(VCF)을 위한 환경 준비

Amazon EVS 환경을 배포하기 전에 환경이 VMware Cloud Foundation(VCF) 인프라 요구 사항을 충족해야 합니다. 자세한 VCF 사전 조건은 VMware Cloud Foundation 제품 설명서의 계획 및 준비 워크북을 참조하세요.

또한 VCF 5.2.x 요구 사항을 숙지해야 합니다. 관련 릴리스 정보는 VCF 5.2.x 릴리스 정보를 참조하세요.

> **Note**
>
> Amazon EVS에서 제공하는 VCF 버전에 대한 자세한 내용은 섹션을 참조하세요the section called “VCF 버전 및 EC2 인스턴스”.

VCF 라이선스 키 취득

Amazon EVS를 사용하려면 VCF 솔루션 키와 vSAN 라이선스 키를 제공해야 합니다. VCF 솔루션 키에는 256개 이상의 코어가 있어야 합니다. vSAN 라이선스 키에는 최소 110TiB의 vSAN 용량이 있어야 합니다. VCF 라이선스에 대한 자세한 내용은 VMware Cloud Foundation 관리 안내서의 VMware Cloud Foundation에서 라이선스 키 관리를 참조하세요. VMware

> **Important**
>
> SDDC Manager 사용자 인터페이스를 사용하여 VCF 솔루션 및 vSAN 라이선스 키를 관리합니다. Amazon EVS에서는 서비스가 제대로 작동하려면 SDDC Manager에서 유효한 VCF 솔루션 및 vSAN 라이선스 키를 유지해야 합니다.

> **Note**
>
> VCF 라이선스는 라이선스 규정 준수를 위해 모든 AWS 리전의 Amazon EVS에서 사용할 수 있습니다. Amazon EVS는 라이선스 키를 검증하지 않습니다. 라이선스 키를 검증하려면 Broadcom 지원을 방문하세요.

VMware HCX 사전 조건

VMware HCX를 사용하여 기존 VMware 기반 워크로드를 Amazon EVS로 마이그레이션할 수 있습니다. Amazon EVS에서 VMware HCX를 사용하기 전에 다음 사전 요구 작업이 완료되었는지 확인합니다.

> **Note**
>
> VMware HCX는 기본적으로 EVS 환경에 설치되지 않습니다.

- Amazon EVS에서 VMware HCX를 사용하려면 먼저 최소 네트워크 언더레이 요구 사항을 충족해야 합니다. 자세한 내용은 VMware HCX 사용 설명서의 네트워크 언더레이 최소 요구 사항을 참조하세요.
- VMware NSX가 환경에 설치 및 구성되어 있는지 확인합니다. 자세한 내용은 VMware NSX 설치 안내서를 참조하세요.
- VMware HCX가 활성화되어 환경에 설치되어 있는지 확인합니다. VMware HCX 활성화 및 설치에 대한 자세한 내용은 VMware HCX 시작하기 안내서의 VMware HCX 시작하기 정보를 참조하세요.
- HCX 인터넷 연결이 필요한 경우 다음 사전 필수 작업을 완료해야 합니다.
  - Amazon에서 제공하는 연속 퍼블릭 IPv4 CIDR 블록 넷마스크 길이에 대한 IPAM 할당량이 /28 이상인지 확인합니다.

> **Important**
>
> HCX 인터넷 연결의 경우 Amazon EVS는 넷마스크 길이가 /28 이상인 퍼블릭 IPAM 풀에서 IPv4 CIDR 블록을 사용해야 합니다. 넷마스크 길이가 /28보다 작은 CIDR 블록을 사용하면 HCX 연결 문제가 발생합니다. IPAM 할당량 증가에 대한 자세한 내용은 IPAM 할당량을 참조하세요.

- 최소 넷마스크 길이가 /28인 CIDR을 사용하여 IPAM 및 퍼블릭 IPv4 IPAM 풀을 생성합니다.
- HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스의 IPAM 풀에서 2개 이상의 탄력적 IP 주소(EIPs)를 할당합니다. 배포해야 하는 각 HCX 네트워크 어플라이언스에 대해 추가 탄력적 IP 주소를 할당합니다.
- 퍼블릭 IPv4 CIDR 블록을 VPC에 추가 CIDR로 추가합니다.

HCX 설정에 대한 자세한 내용은 the section called “HCX 연결 옵션 선택” 및 단원을 참조하십시오the section called “HCX 연결 옵션”.

Amazon EVS 배포 사전 조건 체크리스트

이 섹션에는 성공적인 Amazon EVS 환경 배포를 활성화하기 위해 완료해야 하는 사전 조건 목록이 포함되어 있습니다.

VCF 라이선스 키 정보

구성 요소	설명	최소 요구 사항	예제 값(들)
사이트 ID	Broadcom 지원 포털에 액세스하기 위해 Broadcom에서 제공하는 사이트 ID입니다.	EVS 환경 생성 요청에서 Broadcom의 사이트 ID를 제공해야 합니다.	01234567
VCF 솔루션 키	vSphere, NSX, SDDC Manager 및 vCenter Server를 포함하여 전체 VCF 스택의 기능을 잠금 해제하는 단일	EVS 환경 생성 요청에 유효한 활성 VCF 솔루션 키를 제공해야 합니다. 키는 기존 EVS 환경에서 이미 사용 중일 수 없습니다.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

구성 요소	설명	최소 요구 사항	예제 값(들)
	VCF 라이선스 키입니다.		
vSAN 라이선스 키	vSAN 라이선스 키를 사용하면 VCF 환경 내에서 vSAN 소프트웨어를 활성화하고 사용할 수 있습니다.	EVS 환경 생성 요청에 유효한 활성 vSAN 라이선스 키를 제공해야 합니다. 키는 기존 EVS 환경에서 이미 사용 중일 수 없습니다.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS 계정 및 리전 정보

구성 요소	설명	최소 요구 사항	예제 값(들)
AWS 계정 ID 번호	AWS 계정을 사용하면 AWS 리소스를 생성 및 관리하고 AWS 서비스에 액세스할 수 있습니다.	AWS 계정에 대한 액세스 권한이 있어야 합니다.	999999999999
AWS 리전	가 가용 영역이라고 하는 격리된 여러 데이터 센터를 AWS 유지하는 물리적 지리적 영역입니다.	Amazon EVS를 배포할 AWS 리전을 지정해야 합니다. Amazon EVS를 현재 사용할 수 있는 리전 목록은 AWS 일반 참조 안내서의 Amazon Elastic VMware Service 엔드포인트 및 할당량을 참조하세요.	미국 서부(오리건)

AWS 온프레미스 데이터 센터 연결을 위한 Transit Gateway

구성 요소	설명	최소 요구 사항	예제 값(들)
Transit Gateway ID	전송 게이트웨이는 VPC와 온프레미스 네트워크 간에 흐르는 트래픽을 위한 리전 가상 라우터 역할을 합니다.	전송 게이트웨이를 사용하여 Amazon EVS 환경을 온프레미스 네트워크에 연결해야 합니다.	tgw-0262a0e521EXAMPLE
연결 방법	온프레미스 네트워크를 Amazon EVS 환경에 연결하려면 AWS Direct Connect 또는 AWS Site-to-Site VPN과 함께 전송 게이트웨이를 사용해야 합니다.	AWS Direct Connect, AWS Site-to-Site VPN 또는 둘 다를 사용할지 결정합니다. Direct Connect에서 Site-to-Site VPN을 사용하는 방법에 대한 자세한 내용은 AWS Direct Connect에서 프라이빗 IP AWS Site-to-Site VPN을 참조하세요.	AWS Direct Connect를 사용한 AWS Site-to-Site VPN

Amazon EVS 환경용 VPC

구성 요소	설명	최소 요구 사항	예제 값(들)
VPC ID	VPC는 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사한 가상 네트워크입니다.	모든 Amazon VPC를 환경 배포에 사용할 수 있습니다.	vpc-0abcdef1234567890
VPC CIDR 블록	Amazon VPC에서 CIDR 블록은 VPC 내에서 사용 가능한 IP 주소 범위를 정의합니다.	최소 크기가 /22 넷마스크인 RFC 1918 CIDR 블록. VPC CIDR 블록은 VPC에 배포할 모든 EVS 서브넷 및 호스트를 수용할	10.1.0.0/20

구성 요소	설명	최소 요구 사항	예제 값(들)
		수 있는 적절한 크기여야 합니다. 이 CIDR 블록은 환경 전체에서 고유해야 합니다.	

EVS 환경용 VPC 서브넷

구성 요소	설명	최소 요구 사항	예제 값(들)
서비스 액세스 서브넷 ID	서비스 액세스 서브넷은 Amazon EVS 서비스 액세스를 활성화하는 표준 VPC 서브넷입니다. 자세한 내용은 the section called “서비스 액세스 서브넷” 단원을 참조하십시오.	서브넷의 크기가 VPC 내에 적절한 경우 모든 VPC 서브넷을 사용할 수 있습니다. 넷마스크가 /24인 VPC 서브넷 CIDR 블록을 지정하는 것이 좋습니다.	subnet-abcdef1234567890e
서비스 액세스 서브넷 CIDR	VPC 서브넷 CIDR 블록은 VPC 내의 특정 서브넷에 할당되는 CIDR 표기법을 사용하여 정의된 IP 주소의 범위입니다.	서비스 액세스 서브넷은 VPC에 배포할 다른 EVS 서브넷 및 호스트도 수용할 수 있는 적절한 크기여야 합니다. 넷마스크가 /24인 VPC 서브넷 CIDR 블록을 지정하는 것이 좋습니다.	10.1.0.0/24
AWS 리전 내 가용 영역 ID	AWS 리전 내의 고유한 위치로, 다른 AZs의 장애로부터 격리되도록 설계되었으며 하나 이상의 데이터 센터로 구성됩니다.	서브넷 생성 중에 VPC 서브넷이 배포되는 가용 영역을 지정할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 서브넷 생성을 참조하세요.	us-west-2a

EVS 환경용 EVS VLAN 서브넷

구성 요소	설명	최소 요구 사항	예제 값(들)
호스트 관리 VLAN CIDR	호스트 관리 VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called “호스트 관리 VLAN 서브넷” 단원을 참조하십시오.	최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. VPC와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.	10.1.1.0/24
vMotion VLAN CIDR	vMotion VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called “vMotion VLAN 서브넷” 단원을 참조하십시오.	호스트 관리 VLAN과 크기가 같아야 합니다.	10.1.2.0/24
vSAN VLAN CIDR	vSAN VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called “vSAN VLAN 서브넷” 단원을 참조하십시오.	호스트 관리 VLAN과 크기가 같아야 합니다.	10.1.3.0/24
VTEP VLAN CIDR	VTEP VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called “VTEP VLAN 서브넷” 단원을 참조하십시오.	호스트 관리 VLAN과 크기가 같아야 합니다.	10.1.4.0/24
엣지 VTEP VLAN CIDR	엣지 VTEP VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called “엣	최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. VPC와 연결된	10.1.5.0/24

구성 요소	설명	최소 요구 사항	예제 값(들)
	지 VTEP VLAN 서브넷" 단원을 참조하십시오.	기존 CIDR 블록과 겹치지 않아야 합니다.	
관리 VM VLAN CIDR	관리 VM VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called "관리 VM VLAN 서브넷" 단원을 참조하십시오.	최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. VPC와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.	10.1.6.0/24
HCX 업링크 VLAN CIDR	HCX 업링크 VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called "HCX 업링크 VLAN 서브넷" 단원을 참조하십시오.	최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. VPC와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.	10.1.7.0/24
NSX 업링크 VLAN CIDR	NSX 업링크 VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called "NSX 업링크 VLAN 서브넷" 단원을 참조하십시오.	최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. VPC와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.	10.1.8.0/24
확장 VLAN 1 CIDR	확장 VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called "확장 VLAN 서브넷" 단원을 참조하십시오.	최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. VPC와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.	10.1.9.0/24

구성 요소	설명	최소 요구 사항	예제 값(들)
확장 VLAN 2 CIDR	확장 VLAN 서브넷의 CIDR 블록입니다. 자세한 내용은 the section called “확장 VLAN 서브넷” 단원을 참조하십시오.	최소 크기는 /28 넷마스크이고 최대 크기는 /24 넷마스크여야 합니다. VPC와 연결된 기존 CIDR 블록과 겹치지 않아야 합니다.	10.1.10.0/24

DNS 및 NTP 인프라

구성 요소	설명	최소 요구 사항	예제 값(들)
기본 DNS 서버 IP 주소	도메인의 모든 DNS 레코드에 대한 신뢰할 수 있는 소스로 사용되는 기본 도메인 이름 시스템(DNS) 서버입니다.	사용 가능한 호스트 범위 내에서 유효한 미사용 IPv4 주소를 사용할 수 있습니다.	10.1.1.10
보조 DNS 서버 IP 주소	도메인의 DNS 레코드를 위한 백업 DNS 서버입니다.	사용 가능한 호스트 범위 내에서 유효한 미사용 IPv4 주소를 사용할 수 있습니다.	10.1.5.25
NTP 서버 IP 주소	네트워크 시간 프로토콜(NTP) 서버는 NTP 표준을 사용하여 네트워크 내에서 클럭을 동기화하는 디바이스 또는 애플리케이션입니다.	로컬 `169.254.169.123` IP 주소 또는 다른 NTP 서버 IP 주소와 함께 기본 Amazon Time Sync Service를 사용할 수 있습니다.	169.254.169.123(Amazon Time Sync Service)
VCF 배포를 위한 FQDN	정규화된 도메인 이름(FQDN)은 네트워크에 있는 디바이스의 절대 이름입니다. FQDN은	FQDN에는 영숫자 문자, 마이너스 기호(-) 및 레이블 간의 구분 기호로 사용되는 마침표만 포함될 수 있습니	evs.local

구성 요소	설명	최소 요구 사항	예제 값(들)
	호스트 이름과 도메인 이름으로 구성됩니다.	다. 유효하고 만료되지 않은 고유한 FQDN이어야 합니다.	

VPC DHCP 옵션 세트

구성 요소	설명	최소 요구 사항	예제 값(들)
DHCP 옵션 세트 ID	DHCP 옵션 세트는 EC2 인스턴스와 같은 VPC의 리소스가 가상 네트워크를 통해 통신하는 데 사용하는 네트워크 설정 그룹입니다.	최소 2개의 DNS 서버를 포함해야 합니다. Route 53 또는 사용자 지정 DNS 서버를 사용할 수 있습니다. DNS 도메인 이름과 NTP 서버도 포함해야 합니다.	dopt-0a1b2c3d

EC2 키 페어

구성 요소	설명	최소 요구 사항	예제 값(들)
EC2 키 페어 이름	EC2 키 페어는 Amazon EC2 인스턴스에 안전하게 연결하는 데 사용되는 보안 자격 증명 세트입니다.	키 페어 이름은 고유해야 합니다.	`my-ec2-key-pair`

VPC 라우팅 테이블

구성 요소	설명	최소 요구 사항	예제 값(들)
기본 라우팅 테이블 ID	Amazon VPC에서 기본 라우팅 테이블은 VPC로 자동으로 생성되는 기본 라우팅 테이블이며, 다른 라우	환경 배포가 성공하려면 DNS 또는 온프레미스 시스템과 같은 종속 서비스에 연결할 수 있도록 구성해야 합니다.	rtb-0123456789abcdef0

구성 요소	설명	최소 요구 사항	예제 값(들)
	팅 테이블과 명시적으로 연결되지 않은 모든 VPC 서브넷의 트래픽을 제어합니다. EVS VLAN 서브넷은 Amazon EVS가 생성할 때 VPC의 기본 라우팅 테이블에 암시적으로 연결됩니다.		

네트워크 액세스 제어 목록(ACL)

구성 요소	설명	최소 요구 사항	예제 값(들)
네트워크 ACL ID	네트워크 액세스 제어 목록(ACL)은 서브넷 수준에서 인바운드 또는 아웃바운드 트래픽을 허용하거나 거부합니다.	Amazon EVS가 다음과 통신할 수 있도록 허용해야 합니다. • TCP/UDP 포트 53을 통한 DNS 서버. • HTTPS 및 SSH를 통한 호스트 관리 VLAN 서브넷입니다. • HTTPS 및 SSH를 통한 VM VLAN 서브넷 관리.	acl-0f62c640e793a38a3

VCF 구성 요소에 대한 DNS 레코드

구성 요소	설명	최소 요구 사항	예제 IP 주소	호스트 이름 예
ESX 호스트 1	ESX 호스트 1의 A 레코드 및 PTR 레코드에 정의된	Amazon EVS에는 A 레코드가 있는 DNS 순방향	10.1.0.10	esxi01

구성 요소	설명	최소 요구 사항	예제 IP 주소	호스트 이름 예
	IP 주소 및 호스트 이름입니다.	조회 영역과 각 EVS 배포의 각 ESX 호스트에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.		
ESX 호스트 2	ESX 호스트 2의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 ESX 호스트에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.0.11	esxi02
ESX 호스트 3	ESX 호스트 3의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 ESX 호스트에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.0.12	esxi03

구성 요소	설명	최소 요구 사항	예제 IP 주소	호스트 이름 예
ESX 호스트 4	ESX 호스트 4의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 ESX 호스트에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.0.13	esxi04
vCenter Server 어플라이언스	vCenter Server 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.10	vc01
NSX 관리자 클러스터	NSX Manager 클러스터의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.11	nsx

구성 요소	설명	최소 요구 사항	예제 IP 주소	호스트 이름 예
SDDC Manager 어플라이언스	SDDC Manager 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.12	sddcm01
Cloud Builder 어플라이언스	Cloud Builder 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.13	cb01
NSX Edge 1 어플라이언스	NSX Edge 1 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.14	edge01

구성 요소	설명	최소 요구 사항	예제 IP 주소	호스트 이름 예
NSX Edge 2 어플라이언스	NSX Edge 2 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.15	edge02
NSX Manager 1 어플라이언스	NSX Manager 1 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.16	nsx01
NSX Manager 2 어플라이언스	NSX Manager 2 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.17	nsx02

구성 요소	설명	최소 요구 사항	예제 IP 주소	호스트 이름 예
NSX Manager 3 어플라이언스	NSX Manager 3 어플라이언스의 A 레코드 및 PTR 레코드에 정의된 IP 주소 및 호스트 이름입니다.	Amazon EVS에는 A 레코드가 있는 DNS 순방향 조회 영역과 각 EVS 배포의 각 VCF 관리 어플라이언스에 대해 생성된 PTR 레코드가 있는 역방향 조회 영역이 필요합니다.	10.1.5.18	nsx03

VPC Route Server 인프라

구성 요소	설명	최소 요구 사항	예제 값(들)
라우팅 서버 ID	Amazon EVS는 Amazon VPC Route Server를 사용하여 VPC 언더레이 네트워크에 대한 BGP 기반 동적 라우팅을 활성화합니다.	서비스 액세스 서브넷에서 두 개 이상의 라우팅 서버 엔드포인트에 대한 경로를 공유하는 라우팅 서버를 지정해야 합니다. 라우팅 서버와 NSX Edge 피어에 구성된 피어 ASN은 일치해야 하며 피어 IP 주소는 고유해야 합니다.	rs-0a1b2c3d4e5f67890
라우팅 서버 연결	라우팅 서버와 VPC 간의 연결입니다.	라우팅 서버가 VPC에 연결되어 있어야 합니다.	{ "RouteServerAssociation": { "RouteServerId": "rs-0a1b2c3d4e5f67890",

구성 요소	설명	최소 요구 사항	예제 값(들)
			<pre>"VpcId": "vpc-1", "State": "associating" } }</pre>
VPC Route Server 측의 BGP ASN(Amazon 측 ASN)	Amazon 측 ASN은 VPC 라우팅 서버와 NSX Edge 피어 간의 BGP 세션 AWS 측을 나타냅니다. 라우팅 서버를 생성할 때이 BGP ASN을 지정합니다. 자세한 내용은 Amazon VPC 사용 설명서의 라우팅 서버 생성을 참조하세요.	이 값은 고유해야 하며 64512~65534(16비트 ASN) 또는 1-4294967295~4200000000004294967294(32비트 ASN) 범위의 프라이빗 ASN을 사용하는 것이 AWS 좋습니다.	65001
라우팅 서버 엔드포인트 1 ID	라우팅 서버 엔드포인트는 라우팅 서버와 BGP 피어 간의 BGP(Border Gateway Protocol) 연결을 용이하게 하는 서브넷 내의 AWS관리형 구성 요소입니다.	라우팅 서버 엔드포인트를 서비스 액세스 서브넷에 배포해야 합니다.	rse-0123456789abcdef0
라우팅 서버 피어 1 ID	라우팅 서버 피어는 라우팅 서버 엔드포인트와 AWS (NSX Edge)에 배포된 디바이스 간의 BGP 피어링 세션입니다.	라우팅 서버 피어에 지정된 피어 ASN 값은 NSX Edge Tier-0 게이트웨이에 사용되는 피어 ASN 값과 일치해야 합니다.	rsp-0123456789abcdef0

구성 요소	설명	최소 요구 사항	예제 값(들)
라우팅 서버 피어 1 IP 주소(EVS NSX Edge 1 측)	라우팅 서버 피어(`PeerAddress`)의 IP 주소입니다.	NSX 업링크 VLAN에서 고유한 미사용 IP 주소를 사용해야 합니다. Amazon EVS는 배포 및 라우팅 서버 엔드포인트 피어와의 피어링의 일부로이 IP 주소를 NSX Edge 1에 적용합니다.	10.1.7.10
라우팅 서버 피어 1 엔드포인트 ENI 주소	라우팅 서버 피어()의 엔드포인트 ENI IP 주소입니다`EndpointEniAddress` .	피어 생성 시 라우팅 서버에서 자동으로 생성됩니다.	10.1.7.11
라우팅 서버 엔드포인트 2 ID	라우팅 서버 엔드포인트는 라우팅 서버와 BGP 피어 간의 BGP(Border Gateway Protocol) 연결을 용이하게 하는 서브넷 내의 AWS관리형 구성 요소입니다.	라우팅 서버 엔드포인트를 서비스 액세스 서브넷에 배포해야 합니다.	rse-fedcba9876543210f
라우팅 서버 피어 2 ID(EVS NSX Edge 2 측)	라우팅 서버 피어는 라우팅 서버 엔드포인트와 AWS (NSX Edge)에 배포된 디바이스 간의 BGP 피어링 세션입니다.	라우팅 서버 피어에 지정된 피어 ASN 값은 NSX Edge Tier-0 게이트웨이에 사용되는 피어 ASN 값과 일치해야 합니다.	rsp-fedcba9876543210f

구성 요소	설명	최소 요구 사항	예제 값(들)
라우팅 서버 피어 2 IP 주소	라우팅 서버 피어(`PeerAddress`)의 IP 주소입니다.	NSX 업링크 VLAN의 고유한 IP 주소를 사용해야 합니다. Amazon EVS는 배포 및 라우팅 서버 엔드포인트 피어와의 피어링의 일부로이 IP 주소를 NSX Edge 2에 적용합니다.	10.1.7.200
라우팅 서버 피어 2 엔드포인트 ENI 주소	라우팅 서버 피어()의 엔드포인트 ENI IP 주소입니다`EndpointEniAddress` .	피어 생성 시 라우팅 서버에서 자동으로 생성됩니다.	10.1.7.201
라우팅 서버 전파	라우팅 서버 전파는 지정한 라우팅 테이블의 FIB에 경로를 설치합니다.	서비스 액세스 서브넷과 연결된 라우팅 테이블을 지정해야 합니다. Amazon EVS는 현재 IPv4 네트워킹만 지원합니다.	`{ "RouteServerEndpoint": { "RouteServerId": "rs-1", "RouteServerEndpointId": "rse-1", "VpcId": "vpc-1", "SubnetId": "subnet-1", "State": "pending" } }`
NSX 피어 측의 BGP ASN	연결의 NSX 측에 대한 BGP ASN입니다.	NSX 기본 ASN 65000 사용 제안	65000

HCX 인터넷 액세스 리소스(선택 사항)

구성 요소	설명	최소 요구 사항	예제 값(들)
IPAM ID	HCX 인터넷 액세스를 위한 IP 주소를 관리하는 데 사용되는 Amazon VPC IP 주소 관리자(IPAM)입니다.	퍼블릭 IPv4 주소를 제공하도록 구성해야 합니다. HCX 인터넷 액세스 구성에만 필요합니다.	ipam-0123456789abcdef0
IPAM 풀 ID	HCX 구성 요소에 대한 주소를 제공하는 Amazon 소유 퍼블릭 IPv4 IPAM 풀입니다.	퍼블릭 IPv4 풀로 구성해야 합니다. HCX 인터넷 액세스 구성에만 필요합니다.	ipam-pool-0123456789abcdef0
HCX 퍼블릭 VLAN CIDR 블록	HCX 퍼블릭 VLAN 서브넷의 IPAM 풀에서 할당된 보조 퍼블릭 IPv4 CIDR 블록입니다.	/28 넷마스크가 있어야 하며 Amazon 소유 IPAM 퍼블릭 풀에서 할당되어야 합니다. HCX 인터넷 액세스 구성에만 필요합니다.	18.97.137.0/28
탄력적 IP 주소	HCX 구성 요소의 IPAM 풀에서 할당된 순차적 탄력적 IP 주소입니다.	HCX Manager, HCX Interconnect Appliance(HCX-IX) 및 HCX Network Extension(HCX-NE)에 대해 동일한 IPAM 풀에서 최소 3EIPs. HCX 인터넷 액세스 구성에만 필요합니다.	eipalloc-0123456789abcdef0, eipalloc-0123456789abcdef1, eipalloc-0123456789abcdef2

Amazon Elastic VMware Service 시작하기

이 가이드를 사용하여 Amazon Elastic VMware Service(Amazon EVS)를 시작합니다. 자체 Amazon Virtual Private Cloud(VPC) 내에 호스트가 있는 Amazon EVS 환경을 생성하는 방법을 알아봅니다.

완료되면 VMware vSphere 기반 워크로드를 로 마이그레이션하는 데 사용할 수 있는 Amazon EVS 환경이 생깁니다 AWS 클라우드.

> **Important**
>
> 가능한 한 간단하고 빠르게 시작하기 위해이 주제에는 VPC를 생성하는 단계가 포함되어 있으며 DNS 서버 구성 및 Amazon EVS 환경 생성을 위한 최소 요구 사항을 지정합니다. 이러한 리소스를 생성하기 전에 요구 사항에 맞는 IP 주소 공간 및 DNS 레코드 설정을 계획하는 것이 좋습니다. 또한 VCF 5.2.x 요구 사항을 숙지해야 합니다. 관련 릴리스 정보는 VCF 5.2.x 릴리스 정보를 참조하세요.

> **Important**
>
> Amazon EVS에서 제공하는 VCF 버전에 대한 자세한 내용은 섹션을 참조하세요the section called “VCF 버전 및 EC2 인스턴스”.

주제

- Amazon EVS VLAN 서브넷을 VPC 라우팅 테이블에 명시적으로 연결
- VCF 자격 증명 검색 및 VCF 관리 어플라이언스 액세스
- 정리
- 다음 단계

사전 조건

시작하기 전에 Amazon EVS 사전 조건 작업을 완료해야 합니다. 자세한 내용은 Amazon Elastic VMware Service 설정 단원을 참조하십시오.

서브넷 및 라우팅 테이블이 있는 VPC 생성

> **Note**
>
> VPC, 서브넷 및 Amazon EVS 환경은 모두 동일한 계정에서 생성되어야 합니다. Amazon EVS는 VPC 서브넷 또는 Amazon EVS 환경의 교차 계정 공유를 지원하지 않습니다.

Example

Amazon VPC console

1. Amazon VPC 콘솔을 엽니다.
2. VPC 대시보드에서 VPC 생성을 선택합니다.
3. 생성할 리소스에서 VPC 등을 선택합니다.
4. 이름 태그 자동 생성을 선택한 상태로 유지하여 VPC 리소스에 이름 태그를 생성하거나 선택을 취소하여 VPC 리소스에 고유한 이름 태그를 제공합니다.
5. IPv4 CIDR 블록에 IPv4 CIDR 블록을 입력합니다. VPC에 IPv4 CIDR 블록이 있어야 합니다. Amazon EVS 서브넷을 수용할 수 있는 적절한 크기의 VPC를 생성해야 합니다. 자세한 내용은 the section called “Amazon EVS 네트워킹 고려 사항” 단원을 참조하십시오.

   > **Note**
   >
   > Amazon EVS는 현재 IPv6를 지원하지 않습니다.

6. 테넌시를 로 유지합니다`Default`. 이 옵션을 선택하면이 VPC로 시작되는 EC2 인스턴스는 인스턴스가 시작될 때 지정된 테넌시 속성을 사용합니다. Amazon EVS는 사용자를 대신하여 베어 메탈 EC2 인스턴스를 시작합니다.
7. 가용 영역(AZ) 수는1을 선택합니다.

> **Note**
>
> Amazon EVS는 현재 단일 AZ 배포만 지원합니다.

8. AZs 사용자 지정을 확장하고 서브넷의 AZ를 선택합니다.

> **Note**
>
> Amazon EVS가 지원되는 AWS 리전에를 배포해야 합니다. Amazon EVS 리전 가용성에 대한 자세한 내용은 AWS 일반 참조 안내서의 Amazon Elastic VMware Service 엔드포인트 및 할당량을 참조하세요.

9. (선택 사항) 인터넷 연결이 필요한 경우 퍼블릭 서브넷 수에서 1을 선택합니다.
10. 프라이빗 서브넷 수에서 1을 선택합니다. 이 프라이빗 서브넷은 환경 생성 단계에서 Amazon EVS에 제공한 서비스 액세스 서브넷으로 사용됩니다. 자세한 내용은 the section called “서비스 액세스 서브넷” 단원을 참조하십시오.
11. 서브넷의 IP 주소 범위를 선택하려면 서브넷 CIDR 블록 사용자 지정을 확장합니다.

> **Note**
>
> Amazon EVS VLAN 서브넷도이 VPC CIDR 공간에서 생성해야 합니다. 서비스에 필요한 VLAN 서브넷에 대해 VPC CIDR 블록에 충분한 공간을 두어야 합니다. 자세한 내용은 the section called “Amazon EVS 네트워킹 고려 사항” 섹션을 참조하세요.

12. (선택 사항) IPv4를 통해 리소스에 대한 인터넷 액세스 권한을 부여하려면 NAT 게이트웨이에서 In 1 AZ를 선택합니다. NAT 게이트웨이와 관련된 비용이 있습니다. 자세한 내용은 NAT 게이트웨이 요금을 참조하세요.

> **Note**
>
> Amazon EVS에서는 아웃바운드 인터넷 연결을 활성화하기 위해 NAT 게이트웨이를 사용해야 합니다.

13. VPC 엔드포인트는 없음을 선택합니다.

> **Note**
>
> Amazon EVS는 현재에 대한 게이트웨이 VPC 엔드포인트 Amazon S3 를 지원하지 않습니다. Amazon S3 연결을 활성화하려면 AWS PrivateLink for를 사용하여 인터페이스 VPC 엔드포인트를 설정해야 합니다 Amazon S3. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 용 섹션을 참조AWS PrivateLink 하세요 Amazon S3.

14. DNS 옵션의 경우 기본값을 선택한 상태로 유지합니다. Amazon EVS를 사용하려면 VPC에 모든 VCF 구성 요소에 대한 DNS 확인 기능이 있어야 합니다.
15. (선택 사항) VPC에 태그를 추가하려면 추가 태그를 확장하고 새 태그 추가를 선택하여 태그 키와 태그 값을 입력합니다.
16. VPC 생성을 선택합니다.

> **Note**
>
> VPC 생성 중에는 기본 라우팅 테이블을 Amazon VPC 자동으로 생성하고 기본적으로 서브넷을 여기에 암시적으로 연결합니다.

AWS CLI

1. 터미널 세션을 엽니다.
2. 단일 가용 영역에 프라이빗 서브넷과 선택적 퍼블릭 서브넷이 있는 VPC를 생성합니다.

```
aws ec2 create-vpc \
  --cidr-block 10.0.0.0/16 \
  --instance-tenancy default \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=evs-vpc}]'
---
. Store the VPC ID for use in subsequent commands.
+
[source,bash]
```

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

3. DNS 호스트 이름 및 DNS 지원을 활성화합니다.

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

4. VPC에서 프라이빗 서브넷을 생성합니다.

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

5. 후속 명령에 사용할 프라이빗 서브넷 ID를 저장합니다.

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

6. (선택 사항) 인터넷 연결이 필요한 경우 퍼블릭 서브넷을 생성합니다.

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

7. (선택 사항) 후속 명령에 사용할 퍼블릭 서브넷 ID를 저장합니다.

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

8. (선택 사항) 퍼블릭 서브넷이 생성된 경우 인터넷 게이트웨이를 생성하고 연결합니다.

```
aws ec2 create-internet-gateway \
```

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

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

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

9. (선택 사항) 인터넷 연결이 필요한 경우 NAT 게이트웨이를 생성합니다.

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

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

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

10.필요한 라우팅 테이블을 생성하고 구성합니다.

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

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

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

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

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

11라우팅 테이블에 필요한 경로를 추가합니다.

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

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

12라우팅 테이블을 서브넷과 연결합니다.

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

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

> **Note**
>
> VPC 생성 중에는 기본 라우팅 테이블을 Amazon VPC 자동으로 생성하고 기본적으로 서브넷을 여기에 암시적으로 연결합니다.

HCX 연결 옵션 선택

Amazon EVS 환경에 대한 연결 옵션 하나를 선택합니다.

- 프라이빗 연결: HCX를 위한 고성능 네트워크 경로를 제공하여 안정성과 일관성을 최적화합니다. 외부 네트워크 연결을 위해 AWS Direct Connect 또는 Site-to-Site VPN을 사용해야 합니다.
- 인터넷 연결: 퍼블릭 인터넷을 사용하여 빠르게 설정할 수 있는 유연한 마이그레이션 경로를 설정합니다. VPC IP 주소 관리자(IPAM) 및 탄력적 IP 주소를 사용해야 합니다.

자세한 분석은 단원을 참조하십시오the section called “HCX 연결 옵션”.

옵션을 선택합니다.

- 옵션 A: 프라이빗 연결만 해당 → 로 계속합니다the section called “VPC 기본 라우팅 테이블 구성”.
- 옵션 B: 인터넷 연결 → 로 계속합니다the section called “HCX 인터넷 연결 설정”.

HCX 인터넷 연결 설정

> **Note**
>
> HCX 프라이빗 연결을 선택한 경우이 섹션을 건너뛰고 로 계속 진행합니다the section called “VPC 기본 라우팅 테이블 구성”.

Amazon EVS에 대한 HCX 인터넷 연결을 활성화하려면 다음을 수행해야 합니다.

- Amazon에서 제공하는 연속 퍼블릭 IPv4 CIDR 블록 넷마스크 길이에 대한 VPC IP 주소 관리자(IPAM) 할당량이 /28 이상인지 확인합니다.

  > **Important**
  >
  > 넷마스크 길이가 /28보다 작은 Amazon 제공 연속 퍼블릭 IPv4 CIDR 블록을 사용하면 HCX 연결 문제가 발생합니다. IPAM 할당량 증가에 대한 자세한 내용은 IPAM 할당량을 참조하세요.

- 최소 넷마스크 길이가 /28인 CIDR을 사용하여 IPAM 및 퍼블릭 IPv4 IPAM 풀을 생성합니다.
- HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스의 IPAM 풀에서 2개 이상의 탄력적 IP 주소(EIPs)를 할당합니다. 배포해야 하는 각 HCX 네트워크 어플라이언스에 대해 추가 탄력적 IP 주소를 할당합니다.
- 퍼블릭 IPv4 CIDR 블록을 VPC에 추가 CIDR로 추가합니다.

환경 생성 후 HCX 인터넷 연결 관리에 대한 자세한 내용은 섹션을 참조하세요the section called “HCX 퍼블릭 연결”.

IPAM 생성

다음 단계에 따라 IPAM을 생성합니다.

> **Note**
>
> IPAM 프리 티어를 사용하여 Amazon EVS에 사용할 IPAM 리소스를 생성할 수 있습니다. IPAM 자체는 프리 티어에서 무료이지만 NAT 게이트웨이 및 프리 티어 제한을 초과하는 퍼블릭 IPv4 주소와 같이 IPAM과 함께 사용되는 다른 AWS 서비스의 비용은 사용자가 부담합니다. IPAM 요금에 대한 자세한 내용은 Amazon VPC 요금 페이지를 참조하세요.

> **Note**
>
> Amazon EVS는 현재 프라이빗 IPv6 글로벌 유니캐스트 주소(GUA) CIDRs 지원하지 않습니다.

퍼블릭 IPv4 IPAM 풀 생성

다음 단계에 따라 퍼블릭 IPv4 풀을 생성합니다.

IPAM console

1. IPAM 콘솔을 엽니다.
2. 탐색 창에서 Pools를 선택합니다.
3. 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 IPAM 작동 방식을 참조하세요.
4. 풀 생성(Create pool)을 선택합니다.
5. (선택 사항) 풀에 대한 이름 태그(Name tag) 및 설명(Description)을 추가합니다.
6. 주소 패밀리(Address family)에서 IPv4를 선택합니다.
7. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다.
8. 로캘(Locale)에서 풀에 대한 로캘을 선택합니다. 로캘은이 IPAM 풀을 할당에 사용할 수 있게 하려는 AWS 리전입니다. 선택한 로캘은 VPC가 배포된 AWS 리전과 일치해야 합니다.
9. 서비스(Service)에서 EC2(EIP/VPC)를 선택합니다. 그러면 Amazon EC2 서비스(탄력적 IP 주소용)에 대해이 풀에서 할당된 CIDRs이 알립니다.

10.퍼블릭 IP 소스에서 Amazon 소유를 선택합니다.

11.프로비저닝할 CIDRs에서 Amazon 소유 퍼블릭 CIDR 추가를 선택합니다.

12.넷마스크에서 CIDR 넷마스크 길이를 선택합니다. /28은 필요한 최소 넷마스크 길이입니다.

13.풀 생성(Create pool)을 선택합니다.

AWS CLI

1. 터미널 세션을 엽니다.
2. IPAM에서 퍼블릭 범위 ID를 가져옵니다.

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

3. 퍼블릭 범위에서 IPAM 풀을 생성합니다.

```
aws ec2 create-ipam-pool \
  --ipam-scope-id $SCOPE_ID \
  --address-family ipv4 \
  --no-auto-import \
  --locale us-east-2 \
  --description "Public IPv4 pool for HCX" \
  --tag-specifications 'ResourceType=ipam-pool,Tags=[{Key=Name,Value=evs-hcx-
public-pool}]' \
  --public-ip-source amazon \
  --aws-service ec2
```

4. 후속 명령에 사용할 풀 ID를 저장합니다.

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

5. 최소 넷마스크 길이가 /28인 풀에서 CIDR 블록을 프로비저닝합니다.

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

IPAM 풀에서 탄력적 IP 주소 할당

다음 단계에 따라 HCX Service Mesh 어플라이언스의 IPAM 풀에서 탄력적 IP 주소(EIPs)를 할당합니다.

Amazon VPC console

1. Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Elastic IPs를 선택합니다.
3. 탄력적 IP 주소 할당을 선택합니다.
4. IPv4 IPAM 풀을 사용하여 할당을 선택합니다.
5. 이전에 구성한 Amazon 소유 퍼블릭 IPv4 풀을 선택합니다.
6. IPAM 메서드 할당에서 IPAM 풀 내의 주소 수동 입력을 선택합니다.

> **Important**
>
> 퍼블릭 IPAM CIDR 블록의 처음 두 EIPs 또는 마지막 EIP를 VLAN 서브넷에 연결할 수 없습니다. 이러한 EIPs는 네트워크, 기본 게이트웨이 및 브로드캐스트 주소로 예약됩니다. 이러한 EIPs를 VLAN 서브넷과 연결하려고 하면 Amazon EVS에서 검증 오류가 발생합니다.

> **Important**
>
> Amazon EVS가 예약하는 EIPs가 할당되지 않도록 IPAM 풀 내에 주소를 수동으로 입력합니다. IPAM이 EIP를 선택하도록 허용하는 경우 IPAM은 Amazon EVS가 예약하는 EIP를 할당하여 EIP를 VLAN 서브넷에 연결하는 동안 오류가 발생할 수 있습니다.

7. IPAM 풀에서 할당할 EIP를 지정합니다.
8. 할당을 선택합니다.
9. 이 프로세스를 반복하여 필요한 나머지 EIPs를 할당합니다. HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스에 대해 IPAM 풀에서 최소 2개의 EIPs를 할당해야 합니다. 배포해야 하는 각 HCX 네트워크 어플라이언스에 대해 추가 EIP를 할당합니다.

AWS CLI

1. 터미널 세션을 엽니다.

2. 이전에 생성한 IPAM 풀 ID를 가져옵니다.

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

3. IPAM 풀에서 탄력적 IP 주소를 할당합니다. HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스에 대해 IPAM 풀에서 최소 2개의 EIPs를 할당해야 합니다. 배포해야 하는 각 HCX 네트워크 어플라이언스에 대해 추가 EIP를 할당합니다.

> **Important**
>
> 퍼블릭 IPAM CIDR 블록의 처음 두 EIPs 또는 마지막 EIP를 VLAN 서브넷과 연결할 수 없습니다. 이러한 EIPs는 네트워크, 기본 게이트웨이 및 브로드캐스트 주소로 예약됩니다. 이러한 EIPs를 VLAN 서브넷과 연결하려고 하면 Amazon EVS에서 검증 오류가 발생합니다.

> **Important**
>
> Amazon EVS가 예약하는 EIPs가 할당되지 않도록 IPAM 풀 내에 주소를 수동으로 입력합니다. IPAM이 EIP를 선택하도록 허용하는 경우 IPAM은 Amazon EVS가 예약하는 EIP를 할당하여 EIP를 VLAN 서브넷에 연결하는 동안 오류가 발생할 수 있습니다.

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

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

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

HCX 인터넷 연결을 위해 IPAM 풀에서 VPC로 퍼블릭 IPv4 CIDR 블록 추가

HCX 인터넷 연결을 활성화하려면 IPAM 풀의 퍼블릭 IPv4 CIDR 블록을 VPC에 추가 CIDR로 추가해야 합니다. Amazon EVS는이 CIDR 블록을 사용하여 VMware HCX를 네트워크에 연결합니다. 다음 단계에 따라 VPC에 CIDR 블록을 추가합니다.

> **Important**
>
> VPC에 추가하는 IPv4 CIDR 블록을 수동으로 입력해야 합니다. Amazon EVS는 현재 IPAM 할당 CIDR 블록 사용을 지원하지 않습니다. IPAM 할당 CIDR 블록을 사용하면 EIP 연결에 실패할 수 있습니다.

Amazon VPC console

1. Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Your VPCs를 선택합니다.
3. 이전에 생성한 VPC를 선택하고 작업, CIDRs 선택합니다.
4. 새 IPV4 CIDR 추가를 선택합니다.
5. IPV4 CIDR 수동 입력을 선택합니다.
6. 이전에 생성한 퍼블릭 IPAM 풀에서 CIDR 블록을 지정합니다.

AWS CLI

1. 터미널 세션을 엽니다.
2. IPAM 풀 ID와 프로비저닝된 CIDR 블록을 가져옵니다.

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

```
  --output text)

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

3. VPC에 CIDR 블록을 추가합니다.

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

VPC 기본 라우팅 테이블 구성

Amazon EVS VLAN 서브넷은 VPC 기본 라우팅 테이블에 암시적으로 연결됩니다. 성공적인 환경 배포를 위해 DNS 또는 온프레미스 시스템과 같은 종속 서비스에 대한 연결을 활성화하려면 이러한 시스템에 대한 트래픽을 허용하도록 기본 라우팅 테이블을 구성해야 합니다. 기본 라우팅 테이블에는 VPC의 CIDR에 대한 경로가 포함되어야 합니다. 기본 라우팅 테이블 사용은 초기 Amazon EVS 환경 배포에만 필요합니다. 환경 배포 후 사용자 지정 라우팅 테이블을 사용하도록 환경을 구성할 수 있습니다. 자세한 내용은 the section called “사용자 지정 라우팅 테이블 구성” 단원을 참조하십시오.

환경 배포 후에는 각 Amazon EVS VLAN 서브넷을 VPC의 라우팅 테이블과 명시적으로 연결해야 합니다. VLAN 서브넷이 VPC 라우팅 테이블과 명시적으로 연결되지 않으면 NSX 연결이 실패합니다. 환경 배포 후 서브넷을 사용자 지정 라우팅 테이블과 명시적으로 연결하는 것이 좋습니다. 자세한 내용은 the section called “VPC 기본 라우팅 테이블 구성” 단원을 참조하십시오.

Important

Amazon EVS는 Amazon EVS 환경이 생성된 후에만 사용자 지정 라우팅 테이블 사용을 지원합니다. Amazon EVS 환경 생성 중에는 사용자 지정 라우팅 테이블을 사용해서는 안 됩니다. 연결 문제가 발생할 수 있습니다.

VPC DHCP 옵션 세트를 사용한 DNS 및 NTP 서버 구성

Important

이러한 Amazon EVS 요구 사항을 충족하지 않으면 환경 배포가 실패합니다.

- DHCP 옵션 세트에 기본 DNS 서버 IP 주소와 보조 DNS 서버 IP 주소를 포함합니다.
- 배포의 각 VCF 관리 어플라이언스 및 Amazon EVS 호스트에 대한 A 레코드와 함께 DNS 순방향 조회 영역을 포함합니다.
- 배포의 각 VCF 관리 어플라이언스 및 Amazon EVS 호스트에 대한 PTR 레코드와 함께 DNS 역방향 조회 영역을 포함합니다.
- DNS 서버로의 경로가 존재하도록 VPC의 기본 라우팅 테이블을 구성합니다.
- 도메인 이름 등록이 유효하며 만료되지 않았는지, 중복된 호스트 이름이나 IP 주소가 없는지 확인합니다.
- Amazon EVS가 다음과 통신할 수 있도록 보안 그룹 및 네트워크 액세스 제어 목록(ACLs)을 구성합니다.
  - TCP/UDP 포트 53을 통한 DNS 서버.
  - HTTPS 및 SSH를 통한 호스트 관리 VLAN 서브넷입니다.
  - HTTPS 및 SSH를 통한 VLAN 서브넷 관리.

Amazon EVS는 VPC의 DHCP 옵션 세트를 사용하여 다음을 검색합니다.

- 호스트 IP 주소 확인을 위한 도메인 이름 시스템(DNS) 서버입니다.
- DNS 확인을 위한 도메인 이름입니다.
- 시간 동기화를 위한 NTP(Network Time Protocol) 서버입니다.

Amazon VPC 콘솔 또는를 사용하여 DHCP 옵션 세트를 생성할 수 있습니다 AWS CLI. 자세한 내용은 Amazon VPC 사용 설명서의 DHCP 옵션 세트 생성을 참조하세요.

DNS 서버 구성

DNS 구성을 사용하면 Amazon EVS 환경에서 호스트 이름을 확인할 수 있습니다. Amazon EVS 환경을 성공적으로 배포하려면 VPC의 DHCP 옵션 세트에 다음 DNS 설정이 있어야 합니다.

- DHCP 옵션 세트의 기본 DNS 서버 IP 주소 및 보조 DNS 서버 IP 주소입니다.
- 배포의 각 VCF 관리 어플라이언스 및 Amazon EVS 호스트에 대한 A 레코드가 있는 DNS 순방향 조회 영역입니다.

- 배포의 각 VCF 관리 어플라이언스 및 Amazon EVS 호스트에 대한 PTR 레코드가 있는 역방향 조회 영역입니다. NTP 구성의 경우 기본 Amazon NTP 주소 `169.254.169.123`또는 선호하는 다른 IPv4 주소를 사용할 수 있습니다.

DHCP 옵션 세트에서 DNS 서버를 구성하는 방법에 대한 자세한 내용은 DHCP 옵션 세트 생성을 참조하세요.

온프레미스 연결을 위한 DNS 구성

온프레미스 연결의 경우 인바운드 해석기와 함께 Route 53 프라이빗 호스팅 영역을 사용하는 것이 좋습니다. 이 설정을 사용하면 VPC 내의 내부 DNS에 Route 53를 사용하고 이를 기존 온프레미스 DNS 인프라와 통합할 수 있는 하이브리드 DNS 확인이 가능합니다. 이를 통해 VPC 내의 리소스는 복잡한 구성 없이 온프레미스 네트워크에서 호스팅되는 도메인 이름을 확인할 수 있으며 그 반대의 경우도 마찬가지입니다. 필요한 경우 Route 53 아웃바운드 해석기와 함께 자체 DNS 서버를 사용할 수도 있습니다. 구성 단계는 Amazon Route 53 개발자 안내서의 프라이빗 호스팅 영역 생성 및 VPC로 인바운드 DNS 쿼리 전달을 참조하세요.

> **Note**
>
> DHCP 옵션 세트에서 Route 53과 사용자 지정 도메인 이름 시스템(DNS) 서버를 모두 사용하면 예기치 않은 동작이 발생할 수 있습니다.

> **Note**
>
> 의 프라이빗 호스팅 영역에 정의된 사용자 지정 DNS 도메인 이름을 사용하거나 인터페이스 VPC 엔드포인트(AWS PrivateLink)와 함께 프라이빗 DNS를 Route 53사용하는 경우 `enableDnsHostnames` 및 `enableDnsSupport` 속성을 모두 로 설정해야 합니다`true`. 자세한 내용은 VPC의 DNS 속성을 참조하세요.

DNS 연결성 문제 해결

Amazon EVS는 DNS 레코드에 도달하기 위해 VPC의 DHCP 옵션 세트에서 SDDC Manager 및 DNS 서버에 지속적으로 연결해야 합니다. SDDC Manager에 대한 지속적인 연결을 사용할 수 없게 되면 Amazon EVS는 더 이상 환경 상태를 검증할 수 없으며 환경 액세스 권한이 손실될 수 있습니다. 이 문제를 해결하는 단계는 섹션을 참조하세요the section called “연결성 확인 실패”.

NTP 서버 구성

NTP 서버는 네트워크에 시간을 제공합니다. Amazon EC2 인스턴스에 대한 일관되고 정확한 시간 참조는 많은 VCF 환경 작업 및 프로세스에 매우 중요합니다. 시간 동기화는 다음과 같은 경우에 필수적입니다.

- 시스템 로깅 및 감사
- 보안 운영
- 분산 시스템 관리
- 문제 해결

VPC의 DHCP 옵션 세트에 최대 4개의 NTP 서버의 IPv4 주소를 입력할 수 있습니다. IPv4 주소에서 Amazon Time Sync Service를 지정할 수 있습니다`169.254.169.123`. 기본적으로 Amazon EVS가 배포하는 Amazon EC2 인스턴스는 IPv4 주소의 Amazon Time Sync Service를 사용합니다`169.254.169.123`.

NTP 서버에 대한 자세한 내용은 RFC 2123을 참조하세요. Amazon Time Sync Service에 대한 자세한 내용은 VMware Cloud Foundation VMware 설명서의 EC2 인스턴스의 정밀도 클럭 및 시간 동기화와 VMware Cloud Foundation Hosts에서 NTP 구성을 참조하세요. VMware

NTP 설정을 구성하려면

1. NTP 소스를 선택합니다.
   - Amazon Time Sync Service(권장)
   - 사용자 지정 NTP 서버
2. DHCP 옵션 세트에 NTP 서버를 추가합니다. 자세한 내용은 Amazon VPC 사용 설명서의 DHCP 옵션 세트 생성을 참조하세요.
3. 시간 동기화를 확인합니다. DHCP 옵션 세트 구성에 대한 자세한 내용은 섹션을 참조하세요the section called “VPC의 DHCP 옵션 세트 구성”.

온프레미스 네트워크 연결 구성(선택 사항)

연결된 전송 게이트웨이와 Direct Connect 함께를 사용하거나 전송 게이트웨이에 AWS Site-to-Site VPN 연결을 사용하여 AWS 인프라에 대한 온프레미스 데이터 센터의 연결을 구성할 수 있습니다.

성공적인 환경 배포를 위해 온프레미스 시스템에 대한 연결을 활성화하려면 이러한 시스템으로의 트래픽을 허용하도록 VPC의 기본 라우팅 테이블을 구성해야 합니다. 자세한 내용은 the section called "VPC 기본 라우팅 테이블 구성" 단원을 참조하십시오.

Amazon EVS 환경을 생성한 후에는 전송 게이트웨이 라우팅 테이블을 Amazon EVS 환경 내에서 생성된 VPC CIDRs로 업데이트해야 합니다. 자세한 내용은 the section called "온프레미스 연결을 위한 전송 게이트웨이 라우팅 테이블 및 Direct Connect 접두사 구성(선택 사항)" 단원을 참조하십시오.

Direct Connect 연결 설정에 대한 자세한 내용은 Direct Connect 게이트웨이 및 전송 게이트웨이 연결을 참조하세요. AWS Transit Gateway와 함께 AWS Site-to-Site VPN을 사용하는 방법에 대한 자세한 내용은 Amazon VPC Transit Gateway 사용 설명서의 AWSAmazon VPC Transit Gateways의 Site-to-Site VPN 연결을 참조하세요.

> **Note**
>
> Amazon EVS는 AWS Direct Connect 프라이빗 가상 인터페이스(VIF) 또는 언더레이 VPC로 직접 종료되는 AWS Site-to-Site VPN 연결을 통한 연결을 지원하지 않습니다.

엔드포인트 및 피어를 사용하여 VPC Route Server 인스턴스 설정

Amazon EVS는 Amazon VPC Route Server를에 사용하여 VPC 언더레이 네트워크에 대한 BGP 기반 동적 라우팅을 활성화합니다. 서비스 액세스 서브넷에서 두 개 이상의 라우팅 서버 엔드포인트에 대한 경로를 공유하는 라우팅 서버를 지정해야 합니다. 라우팅 서버 피어에 구성된 피어 ASN은 일치해야 하며 피어 IP 주소는 고유해야 합니다.

HCX 인터넷 연결을 위해 Route Server를 구성하는 경우 이 절차의 첫 번째 단계에서 생성한 서비스 액세스 서브넷과 퍼블릭 서브넷 모두에 대해 Route Server 전파를 구성해야 합니다.

> **Important**
>
> VPC Route Server 구성에 대한 다음 Amazon EVS 요구 사항을 충족하지 않으면 환경 배포가 실패합니다.
>
> - 서비스 액세스 서브넷에서 라우팅 서버 엔드포인트를 두 개 이상 구성해야 합니다.
> - Tier-0 게이트웨이에 대해 BGP(Border Gateway Protocol)를 구성할 때 VPC Route Server 피어 ASN 값은 NSX Edge 피어 ASN 값과 일치해야 합니다.
> - 두 라우팅 서버 피어를 생성할 때 각 엔드포인트에 대해 NSX 업링크 VLAN의 고유한 IP 주소를 사용해야 합니다. 이 두 IP 주소는 Amazon EVS 환경 배포 중에 NSX 엣지에 할당됩니다.

- Route Server 전파를 활성화할 때 전파되는 모든 라우팅 테이블에 하나 이상의 명시적 서브넷 연결이 있는지 확인해야 합니다. 전파된 라우팅 테이블에 명시적 서브넷 연결이 없는 경우 BGP 라우팅 광고가 실패합니다.

VPC Route Server 설정에 대한 자세한 내용은 Route Server 시작하기 자습서를 참조하세요.

Important

Route Server 전파를 활성화할 때 전파되는 모든 라우팅 테이블에 하나 이상의 명시적 서브넷 연결이 있는지 확인합니다. 라우팅 테이블에 명시적 서브넷 연결이 있는 경우 BGP 라우팅 광고가 실패합니다.

Note

Route Server 피어 실시간 감지의 경우 Amazon EVS는 기본 BGP 연결 유지 메커니즘만 지원합니다. Amazon EVS는 다중 홉 양방향 전달 감지(BFD)를 지원하지 않습니다.

Note

라우팅 서버 인스턴스에 대해 지속 기간이 1~5분인 영구 경로를 활성화하는 것이 좋습니다. 활성화하면 모든 BGP 세션이 종료되더라도 라우팅 서버의 라우팅 데이터베이스에 경로가 보존됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 라우팅 서버 생성을 참조하세요.

Note

NAT 게이트웨이 또는 전송 게이트웨이를 사용하는 경우 VPC 라우팅 테이블(들)에 NSX 경로를 전파하도록 라우팅 서버가 올바르게 구성되어 있는지 확인합니다.

문제 해결

문제가 발생하는 경우:

- 각 라우팅 테이블에 명시적 서브넷 연결이 있는지 확인합니다.

- 라우팅 서버에 대해 입력한 피어 ASN 값과 NSX Tier-0 게이트웨이가 일치하는지 확인합니다.
- Route Server 엔드포인트 IP 주소가 고유한지 확인합니다.
- 라우팅 테이블에서 라우팅 전파 상태를 검토합니다.
- VPC Route Server 피어 로깅을 사용하여 BGP 세션 상태를 모니터링하고 연결 문제를 해결합니다. 자세한 내용은 Amazon VPC 사용 설명서의 라우팅 서버 피어 로깅을 참조하세요.

네트워크 ACL을 생성하여 Amazon EVS VLAN 서브넷 트래픽 제어

Amazon EVS는 네트워크 액세스 제어 목록(ACL)을 사용하여 Amazon EVS VLAN 서브넷과 주고받는 트래픽을 제어합니다. VPC에 기본 네트워크 ACL을 사용하거나 보안 그룹의 규칙과 유사한 규칙을 사용하여 VPC에 대한 사용자 지정 네트워크 ACL을 생성하여 VPC에 보안 계층을 추가할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC용 네트워크 ACL 생성을 참조하세요.

HCX 인터넷 연결을 구성하려는 경우 구성하는 네트워크 ACL 규칙이 HCX 구성 요소에 필요한 인바운드 및 아웃바운드 연결을 허용하는지 확인합니다. HCX 포트 요구 사항에 대한 자세한 내용은 VMware HCX 사용 설명서를 참조하세요.

> **Important**
>
> 인터넷을 통해 연결하는 경우 탄력적 IP 주소를 VLAN과 연결하면 해당 VLAN 서브넷의 모든 리소스에 대한 직접 인터넷 액세스가 가능합니다. 보안 요구 사항에 따라 액세스를 제한하도록 구성된 적절한 네트워크 액세스 제어 목록이 있는지 확인합니다.

> **Important**
>
> EC2 보안 그룹은 Amazon EVS VLAN 서브넷에 연결된 탄력적 네트워크 인터페이스에서 작동하지 않습니다. Amazon EVS VLAN 서브넷과 주고받는 트래픽을 제어하려면 네트워크 액세스 제어 목록을 사용해야 합니다.

Amazon EVS 환경 생성

> **Important**
>
> 이 주제에는 가능한 한 간단하고 빠르게 시작하기 위해 기본 설정으로 Amazon EVS 환경을 생성하는 단계가 포함되어 있습니다. 환경을 생성하기 전에 모든 설정을 숙지하고 요구 사항에

맞는 설정을 환경에 배포하는 것이 좋습니다. 환경은 초기 환경 생성 중에만 구성할 수 있습니다. 환경을 생성한 후에는 수정할 수 없습니다. 가능한 모든 Amazon EVS 환경 설정에 대한 개요는 Amazon EVS API 참조 가이드를 참조하세요.

> **Note**
>
> 환경 ID는 VCF 라이선스 규정 준수 요구 사항에 따라 모든 AWS 리전의 Amazon EVS에서 사용할 수 있습니다.

> **Note**
>
> Amazon EVS 환경은 VPC 및 VPC 서브넷과 동일한 리전 및 가용 영역에 배포해야 합니다.

호스트 및 VLAN 서브넷이 있는 Amazon EVS 환경을 생성하려면이 단계를 완료하세요.

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.

   > **Note**
   >
   > 콘솔의 오른쪽 상단에 표시된 AWS 리전이 환경을 생성하려는 AWS 리전인지 확인합니다. 그렇지 않은 경우 AWS 리전 이름 옆의 드롭다운을 선택하고 사용할 AWS 리전을 선택합니다.

2. 탐색 창에서 환경을 선택합니다.
3. 환경 생성을 선택합니다.
4. Amazon EVS 요구 사항 검증 페이지에서 서비스 요구 사항이 충족되었는지 확인합니다. 자세한 내용은 Amazon Elastic VMware Service 설정 단원을 참조하십시오.
   a. (선택 사항) 이름에 환경 이름을 입력합니다.
   b. 환경 버전에서 VCF 버전을 선택합니다. Amazon EVS에서 제공하는 VCF 버전에 대한 자세한 내용은 섹션을 참조하세요the section called “VCF 버전 및 EC2 인스턴스”.

c. 사이트 ID에 Broadcom 사이트 ID를 입력합니다.

d. VCF 솔루션 키에 VCF 솔루션 키(VCF용 VMware vSphere 8 Enterprise Plus)를 입력합니다. 이 라이선스 키는 기존 환경에서 사용할 수 없습니다.

> **Note**
>
> VCF 솔루션 키에는 256개 이상의 코어가 있어야 합니다.

> **Note**
>
> VCF 라이선스는 라이선스 규정 준수를 위해 모든 AWS 리전의 Amazon EVS에서 사용할 수 있습니다. Amazon EVS는 라이선스 키를 검증하지 않습니다. 라이선스 키를 검증하려면 Broadcom 지원을 방문하세요.

> **Note**
>
> Amazon EVS에서는 서비스가 제대로 작동하려면 SDDC Manager에서 유효한 VCF 솔루션 키를 유지해야 합니다. 배포 후 vSphere Client를 사용하여 VCF 솔루션 키를 관리하는 경우 SDDC Manager 사용자 인터페이스의 라이선스 화면에도 키가 표시되는지 확인해야 합니다.

e. vSAN 라이선스 키에 vSAN 라이선스 키를 입력합니다. 이 라이선스 키는 기존 환경에서 사용할 수 없습니다.

> **Note**
>
> vSAN 라이선스 키에는 최소 110TiB의 vSAN 용량이 있어야 합니다.

> **Note**
>
> VCF 라이선스는 라이선스 규정 준수를 위해 모든 AWS 리전의 Amazon EVS에서 사용할 수 있습니다. Amazon EVS는 라이선스 키를 검증하지 않습니다. 라이선스 키를 검증하려면 Broadcom 지원을 방문하세요.

> **Note**
>
> Amazon EVS에서는 SDDC Manager에서 올바른 vSAN 라이선스 키를 유지해야 합니다.이 경우 서비스가 제대로 작동하도록 선택했습니다. 배포 후 vSphere Client를 사용하여 vSAN 라이선스 키를 관리하는 경우 SDDC Manager 사용자 인터페이스의 라이선스 화면에도 키가 표시되는지 확인해야 합니다.

f. VCF 라이선스 약관의 경우 확인란을 선택하여 Amazon EVS 환경의 모든 물리적 프로세서 코어를 포함하는 데 필요한 수의 VCF 소프트웨어 라이선스를 구매했으며 계속 유지할 것임을 확인합니다. Amazon EVS의 VCF 소프트웨어에 대한 정보는 라이선스 규정 준수를 확인하기 위해 Broadcom과 공유됩니다.

g. 다음을 선택합니다.

5. 호스트 세부 정보 지정 페이지에서 다음 단계를 네 번 완료하여 환경에 호스트 4개를 추가합니다. Amazon EVS 환경에는 초기 배포를 위해 4개의 호스트가 필요합니다.

a. 호스트 세부 정보 추가를 선택합니다.

b. DNS 호스트 이름에 호스트의 호스트 이름을 입력합니다.

c. 인스턴스 유형에서 EC2 인스턴스 유형을 선택합니다.

d. ESX 호스트 버전의 경우 환경 생성 중에 선택한 VCF 버전의 기본 ESX 버전이 사용됩니다. 자세한 정보는 the section called “VCF 버전 및 EC2 인스턴스”을 참조하세요.

> **Important**
>
> Amazon EVS가 배포하는 EC2 인스턴스를 중지하거나 종료하지 마십시오. 이 작업을 수행하면 데이터가 손실됩니다.

> **Note**
>
> Amazon EVS는 현재 i4i.metal EC2 인스턴스만 지원합니다.

e. SSH 키 페어에서 호스트에 대한 SSH 액세스를 위한 SSH 키 페어를 선택합니다.

f. 호스트 추가를 선택합니다.

6. 네트워크 및 연결 구성 페이지에서 다음을 수행합니다.

a. HCX 연결 요구 사항에서 프라이빗 연결 또는 인터넷을 통해 HCX를 사용할지 여부를 선택합니다.

b. VPC에서 이전에 생성한 VPC를 선택합니다.

c. (HCX 인터넷 연결만 해당) HCX 네트워크 ACL의 경우 HCX VLAN을 연결할 네트워크 ACL을 선택합니다.

> **Important**
>
> HCX VLAN 전용 사용자 지정 네트워크 ACL을 생성하는 것이 좋습니다. 자세한 내용은 the section called “네트워크 ACL 구성” 단원을 참조하십시오.

d. 서비스 액세스 서브넷에서 VPC를 생성할 때 생성된 프라이빗 서브넷을 선택합니다.

e. 보안 그룹 - 선택 사항의 경우 Amazon EVS 컨트롤 플레인과 VPC 간의 통신을 제어하는 보안 그룹을 최대 2개까지 선택할 수 있습니다. 보안 그룹을 선택하지 않은 경우 Amazon EVS는 기본 보안 그룹을 사용합니다.

> **Note**
>
> 선택한 보안 그룹이 DNS 서버 및 Amazon EVS VLAN 서브넷에 대한 연결을 제공하는지 확인합니다.

f. 관리 연결에서 Amazon EVS VLAN 서브넷에 사용할 CIDR 블록을 입력합니다. HCX 업링크 VLAN CIDR 블록의 경우 퍼블릭 HCX VLAN을 구성하는 경우 넷마스크 길이가 정확히 /28인 CIDR 블록을 지정해야 합니다. 퍼블릭 HCX VLAN에 다른 CIDR 블록 크기가 지정된 경우 Amazon EVS에서 검증 오류가 발생합니다. 프라이빗 HCX VLAN 및 기타 모든 VLANs CIDR 블록의 경우 사용할 수 있는 최소 넷마스크 길이는 /28이고 최대 길이는 /24입니다.

> **Important**
>
> Amazon EVS VLAN 서브넷은 Amazon EVS 환경 생성 중에만 생성할 수 있으며 환경이 생성된 후에는 수정할 수 없습니다. 환경을 생성하기 전에 VLAN 서브넷 CIDR 블록의 크기가 적절한지 확인해야 합니다. 환경이 배포된 후에는 VLAN 서브넷을 추가할 수 없습니다. 자세한 내용은 the section called “Amazon EVS 네트워킹 고려 사항” 단원을 참조하십시오.

g. 확장 VLANs에서 NSX 페더레이션 활성화와 같은 Amazon EVS 내에서 VCF 기능을 확장하는 데 사용할 수 있는 추가 Amazon EVS VLAN 서브넷의 CIDR 블록을 입력합니다.

h. 워크로드/VCF 연결에서 NSX 업링크 VLAN의 CIDR 블록을 입력하고 NSX 업링크를 통해 Route Server 엔드포인트에 피어링하는 두 개의 VPC Route Server 피어 IDs를 선택합니다.

> **Note**
>
> Amazon EVS에는 EVS 배포 전에 두 개의 Route Server 엔드포인트 및 두 개의 Route Server 피어와 연결된 VPC Route Server 인스턴스가 필요합니다. 이 구성은 NSX 업링크를 통한 동적 BGP 기반 라우팅을 활성화합니다. 자세한 내용은 the section called “엔드포인트 및 피어를 사용하여 VPC Route Server 인스턴스 설정” 단원을 참조하십시오.

i. 다음을 선택합니다.

7. 관리 DNS 호스트 이름 지정 페이지에서 다음을 수행합니다.

a. 관리 어플라이언스 DNS 호스트 이름에 VCF 관리 어플라이언스를 호스팅할 가상 머신의 DNS 호스트 이름을 입력합니다. Route 53를 DNS 공급자로 사용하는 경우 DNS 레코드가 포함된 호스팅 영역도 선택합니다.

b. 자격 증명에서 Secrets Manager용 AWS 관리형 KMS 키를 사용할지 아니면 제공하는 고객 관리형 KMS 키를 사용할지 선택합니다. 이 키는 SDDC Manager, NSX Manager 및 vCenter 어플라이언스를 사용하는 데 필요한 VCF 자격 증명을 암호화하는 데 사용됩니다.

> **Note**
>
> 고객 관리형 KMS 키와 관련된 사용 비용이 있습니다. 자세한 내용은 AWS KMS 요금 페이지를 참조하세요.

c. 다음을 선택합니다.

8. (선택 사항) 태그 추가 페이지에서이 환경에 할당하려는 태그를 추가하고 다음을 선택합니다.

> **Note**
>
> 이 환경의 일부로 생성된 호스트는 태그를 수신합니다`DoNotDelete-EVS-<environmentid>-<hostname>`.

> **Note**
>
> Amazon EVS 환경과 연결된 태그는 EC2 인스턴스와 같은 기본 AWS 리소스로 전파되지 않습니다. 각 서비스 콘솔 또는를 사용하여 기본 AWS 리소스에 태그를 생성할 수 있습니다 AWS CLI.

9. 검토 및 생성 페이지에서 구성을 검토하고 환경 생성을 선택합니다.

> **Important**
>
> 환경 배포 중에 Amazon EVS는 EVS VLAN 서브넷을 생성하고 이를 기본 라우팅 테이블과 암시적으로 연결합니다. 배포가 완료되면 NSX 연결을 위해 Amazon EVS VLAN 서브넷을 라우팅 테이블과 명시적으로 연결해야 합니다. 자세한 내용은 the section called "Amazon EVS VLAN 서브넷을 VPC 라우팅 테이블에 명시적으로 연결" 단원을 참조하십시오.

> **Note**
>
> Amazon EVS는 비동기 패치라고 하는 개별 제품 업데이트가 포함되지 않을 수 있는 VMware Cloud Foundation의 최신 번들 버전을 배포합니다. 이 배포가 완료되면 Broadcom의 Async Patch Tool(AP Tool) 또는 SDDC Manager 제품 내 LCM 자동화를 사용하여 개별 제품을 검토하고 업데이트하는 것이 좋습니다. NSX 업그레이드는 SDDC Manager 외부에서 수행해야 합니다.

> **Note**
>
> 환경 생성에는 몇 시간이 걸릴 수 있습니다.

AWS CLI

1. 터미널 세션을 엽니다.
2. Amazon EVS 환경을 생성합니다. 다음은 샘플 `aws evs create-environment` 요청입니다.

Important

`aws evs create-environment` 명령을 실행하기 전에 모든 Amazon EVS 사전 조건이 충족되었는지 확인합니다. 사전 조건이 충족되지 않으면 환경 배포가 실패합니다. 자세한 내용은 Amazon Elastic VMware Service 설정 단원을 참조하십시오.

Important

환경 배포 중에 Amazon EVS는 EVS VLAN 서브넷을 생성하고 이를 기본 라우팅 테이블과 암시적으로 연결합니다. 배포가 완료되면 NSX 연결을 위해 Amazon EVS VLAN 서브넷을 라우팅 테이블과 명시적으로 연결해야 합니다. 자세한 내용은 the section called "Amazon EVS VLAN 서브넷을 VPC 라우팅 테이블에 명시적으로 연결" 단원을 참조하십시오.

Note

Amazon EVS는 비동기 패치라고 하는 개별 제품 업데이트가 포함되지 않을 수 있는 VMware Cloud Foundation의 최신 번들 버전을 배포합니다. 이 배포가 완료되면 Broadcom의 Async Patch Tool(AP Tool) 또는 SDDC Manager 제품 내 LCM 자동화를 사용하여 개별 제품을 검토하고 업데이트하는 것이 좋습니다. NSX 업그레이드는 SDDC Manager 외부에서 수행해야 합니다.

Note

환경 배포에는 몇 시간이 걸릴 수 있습니다.

- 의 경우 최소 IPv4 CIDR 범위 /22로 이전에 생성한 VPC를 `--vpc-id`지정합니다.
- 의 경우 VPC를 생성할 때 생성된 프라이빗 서브넷의 고유 ID를 `--service-access-subnet-id`지정합니다.
- `--vcf-version`의 경우 Amazon EVS에서 제공하는 VCF 버전the section called "VCF 버전 및 EC2 인스턴스"은 섹션을 참조하세요.

- 를 사용하면 Amazon EVS 환경의 모든 물리적 프로세서 코어를 포함하는 데 필요한 수의 VCF 소프트웨어 라이선스를 구매했으며 계속 유지할 것임을 `--terms-accepted`확인합니다. Amazon EVS의 VCF 소프트웨어에 대한 정보는 라이선스 규정 준수를 확인하기 위해 Broadcom과 공유됩니다.
- 에 VCF 솔루션 키(VCF용 VMware vSphere 8 Enterprise Plus)와 vSAN 라이선스 키를 `--license-info`입력합니다.

> **Note**
>
> VCF 솔루션 키에는 256개 이상의 코어가 있어야 합니다. vSAN 라이선스 키에는 최소 110TiB의 vSAN 용량이 있어야 합니다.

> **Note**
>
> Amazon EVS에서는 서비스가 제대로 작동하려면 SDDC Manager에 유효한 VCF 솔루션 키와 vSAN 라이선스 키를 유지해야 합니다. 배포 후 vSphere Client를 사용하여 이러한 라이선스 키를 관리하는 경우 SDDC Manager 사용자 인터페이스의 라이선스 화면에도 이러한 키가 표시되는지 확인해야 합니다.

> **Note**
>
> VCF 솔루션 키와 vSAN 라이선스 키는 기존 Amazon EVS 환경에서 사용할 수 없습니다.

- 에는 Amazon EVS가 사용자를 대신하여 생성하는 Amazon EVS VLAN 서브넷의 CIDR 범위를 `--initial-vlans` 지정합니다. 이러한 VLANs은 VCF 관리 어플라이언스를 배포하는 데 사용됩니다. 퍼블릭 HCX VLAN을 구성하는 경우 넷마스크 길이가 정확히 /28인 CIDR 블록을 지정해야 합니다. 퍼블릭 HCX VLAN에 다른 CIDR 블록 크기가 지정된 경우 Amazon EVS에서 검증 오류가 발생합니다. 프라이빗 HCX VLAN 및 기타 모든 VLANs CIDR 블록의 경우 사용할 수 있는 최소 넷마스크 길이는 /28이고 최대 길이는 /24입니다.
- `hcxNetworkAclId` HCX 인터넷 연결을 구성하는 경우가 사용됩니다. 퍼블릭 HCX VLAN에 대한 사용자 지정 네트워크 ACL을 지정합니다.

> **Important**
>
> HCX VLAN 전용 사용자 지정 네트워크 ACL을 생성하는 것이 좋습니다. 자세한 내용은 the section called “네트워크 ACL 구성” 단원을 참조하십시오.

> **Important**
>
> Amazon EVS VLAN 서브넷은 Amazon EVS 환경 생성 중에만 생성할 수 있으며 환경이 생성된 후에는 수정할 수 없습니다. 환경을 생성하기 전에 VLAN 서브넷 CIDR 블록의 크기가 적절한지 확인해야 합니다. 환경이 배포된 후에는 VLAN 서브넷을 추가할 수 없습니다. 자세한 내용은 the section called “Amazon EVS 네트워킹 고려 사항” 단원을 참조하십시오.

- 의 경우 Amazon EVS가 환경 배포에 필요한 호스트의 호스트 세부 정보를 `--hosts`지정합니다. 각 호스트에 대해 DNS 호스트 이름, EC2 SSH 키 이름 및 EC2 인스턴스 유형을 포함합니다. 전용 호스트 ID는 선택 사항입니다.

> **Important**
>
> Amazon EVS가 배포하는 EC2 인스턴스를 중지하거나 종료하지 마십시오. 이 작업을 수행하면 데이터가 손실됩니다.

> **Note**
>
> Amazon EVS는 현재 i4i.metal EC2 인스턴스만 지원합니다.

- 의 경우 이전 단계에서 생성한 VPC Route Server 피어 IDs개를 `--connectivity-info`지정합니다.

> **Note**
>
> Amazon EVS에는 EVS 배포 전에 두 개의 Route Server 엔드포인트 및 두 개의 Route Server 피어와 연결된 VPC Route Server 인스턴스가 필요합니다. 이 구성은 NSX 업링크를 통한 동적 BGP 기반 라우팅을 활성화합니다. 자세한 내용은 the section called

"엔드포인트 및 피어를 사용하여 VPC Route Server 인스턴스 설정" 단원을 참조하십시오.

- 에 VCF 관리 어플라이언스를 호스팅할 가상 머신의 DNS 호스트 이름을 `--vcf-hostnames`입력합니다.
- 에 고유한 Broadcom 사이트 ID를 `--site-id`입력합니다. 이 ID는 Broadcom 포털에 액세스하는 데 필요하며, 소프트웨어 계약 또는 계약 갱신이 체결될 때 Broadcom에서 제공됩니다.
- (선택 사항)에 환경을 배포할 리전을 `--region`입력합니다. 리전을 지정하지 않으면 기본 리전이 사용됩니다.

```
aws evs create-environment \
--environment-name testEnv \
--vpc-id vpc-1234567890abcdef0 \
--service-access-subnet-id subnet-01234a1b2cde1234f \
--vcf-version VCF-5.2.2 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"isHcxPublic\": true,
      \"hcxNetworkAclId\": \"nacl-abcd1234\",
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
```

```
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07879acf49EXAMPLE\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07878bde50EXAMPLE\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07877eio51EXAMPLE\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07863ghi52EXAMPLE\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
```

```
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

다음은 응답 예입니다.

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATING",
        "stateDetails": "The environment is being initialized, this operation
 may take some time to complete.",
        "createdAt": "2025-04-13T12:03:39.718000+00:00",
        "modifiedAt": "2025-04-13T12:03:39.718000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-1234567890abcdef0",
        "serviceAccessSubnetId": "subnet-01234a1b2cde1234f",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-1234567890abcdef0",
                "rsp-abcdef01234567890"
            ]
        },
```

```
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        }
    }
}
```

Amazon EVS 환경 생성 확인

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 창에서 환경을 선택합니다.
3. 환경을 선택합니다.
4. 세부 정보 탭을 선택합니다.
5. 환경 상태가 통과이고 환경 상태가 생성됨인지 확인합니다. 이를 통해 환경을 사용할 준비가 되었음을 알 수 있습니다.

> **Note**
>
> 환경 생성에는 몇 시간이 걸릴 수 있습니다. 환경 상태에 여전히 생성 중이 표시되면 페이지를 새로 고칩니다.

AWS CLI

1. 터미널 세션을 엽니다.
2. 환경의 환경 ID와 리소스가 포함된 리전 이름을 사용하여 다음 명령을 실행합니다. 가 인 경우 환경을 사용할 준비가 `environmentState`된 것입니다`CREATED`.

> **Note**
>
> 환경 생성에는 몇 시간이 걸릴 수 있습니다. 에 `environmentState` 여전히가 표시되면 명령을 다시 `CREATING`실행하여 출력을 새로 고칩니다.

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

다음은 응답 예입니다.

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATED",
        "createdAt": "2025-04-13T13:39:49.546000+00:00",
        "modifiedAt": "2025-04-13T13:40:39.355000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-0c6def5b7b61c9f41",
        "serviceAccessSubnetId": "subnet-06a3c3b74d36b7d5e",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
```

```
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

Amazon EVS VLAN 서브넷을 VPC 라우팅 테이블에 명시적으로 연결

각 Amazon EVS VLAN 서브넷을 VPC의 라우팅 테이블과 명시적으로 연결합니다. 이 라우팅 테이블은 AWS 리소스가 Amazon EVS로 실행되는 NSX 네트워크 세그먼트의 가상 머신과 통신할 수 있도록 하는 데 사용됩니다. 퍼블릭 HCX VLAN을 생성한 경우 퍼블릭 HCX VLAN 서브넷을 인터넷 게이트웨이로 라우팅되는 VPC의 퍼블릭 라우팅 테이블과 명시적으로 연결해야 합니다.

Example

Amazon VPC console

1. VPC 콘솔로 이동합니다.
2. 탐색 창에서 Route tables을 선택합니다.
3. Amazon EVS VLAN 서브넷과 연결할 라우팅 테이블을 선택합니다.
4. 서브넷 연결 탭을 선택합니다.
5. 명시적 서브넷 연결에서 서브넷 연결 편집을 선택합니다.
6. 모든 Amazon EVS VLAN 서브넷을 선택합니다.
7. [연결 저장(Save associations)]을 선택합니다.

AWS CLI

1. 터미널 세션을 엽니다.
2. Amazon EVS VLAN 서브넷 IDs.

```
aws ec2 describe-subnets
```

3. Amazon EVS VLAN 서브넷을 VPC의 라우팅 테이블과 연결합니다.

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

EIPs HCX 퍼블릭 VLAN 서브넷에 연결(HCX 인터넷 연결용)

다음 단계에 따라 IPAM 풀의 탄력적 IP 주소(EIPs)를 HCX 인터넷 연결을 위한 HCX 퍼블릭 VLAN에 연결합니다. HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스에 대해 두 개 이상의 EIPs를 연결해야 합니다. 배포해야 하는 각 HCX 네트워크 어플라이언스에 대해 추가 EIP를 연결합니다. HCX 퍼블릭 VLAN과 연결된 IPAM 풀에서 최대 13EIPs를 보유할 수 있습니다.

Important

IPAM 풀의 EIPs를 HCX 퍼블릭 VLAN 서브넷과 두 개 이상 연결하지 않으면 HCX 퍼블릭 인터넷 연결이 실패합니다.

Note

Amazon EVS는 현재 EIPs HCX VLAN과 연결하는 것만 지원합니다.

Note

퍼블릭 IPAM CIDR 블록의 처음 두 EIPs 또는 마지막 EIP를 VLAN 서브넷과 연결할 수 없습니다. 이러한 EIPs는 네트워크, 기본 게이트웨이 및 브로드캐스트 주소로 예약됩니다. 이러한 EIPs를 VLAN 서브넷과 연결하려고 하면 Amazon EVS에서 검증 오류가 발생합니다.

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 메뉴에서 환경을 선택합니다.

3. 환경을 선택합니다.
4. 네트워크 및 연결 탭에서 HCX 퍼블릭 VLAN을 선택합니다.
5. EIP를 VLAN에 연결을 선택합니다.
6. HCX 퍼블릭 VLAN과 연결할 탄력적 IP 주소(들)를 선택합니다.
7. EIPs 연결을 선택합니다.
8. EIP 연결을 확인하여 EIPs HCX 퍼블릭 VLAN과 연결되었는지 확인합니다.

AWS CLI

1. 탄력적 IP 주소를 VLAN과 연결하려면 예제 `associate-eip-to-vlan` 명령을 사용합니다.
   - `environment-id` - Amazon EVS 환경의 ID입니다.
   - `vlan-name` - 탄력적 IP 주소와 연결할 VLAN의 이름입니다.
   - `allocation-id` - 탄력적 IP 주소의 할당 ID입니다.

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

   명령은 새 EIP 연결을 포함하여 VLAN에 대한 세부 정보를 반환합니다.

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

```
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

`eipAssociations` 배열은 다음을 포함한 새 연결을 보여줍니다.

- `associationId` - 연결 해제에 사용되는이 EIP 연결의 고유 ID입니다.
- `allocationId` - 연결된 탄력적 IP 주소의 할당 ID입니다.
- `ipAddress` - VLAN에 할당된 IP 주소입니다.

2. 단계를 반복하여 추가 EIPs 연결합니다.

온프레미스 연결을 위한 전송 게이트웨이 라우팅 테이블 및 Direct Connect 접두사 구성 (선택 사항)

전송 게이트웨이와 함께 Direct Connect or AWS Site-to-Site VPN을 사용하여 온프레미스 네트워크 연결을 구성하는 경우 Amazon EVS 환경 내에서 생성된 VPC CIDRs로 전송 게이트웨이 라우팅 테이블을 업데이트해야 합니다. 자세한 내용은 Amazon VPC Transit Gateways의 Transit Gateway 라우팅 테이블을 참조하세요.

AWS Direct Connect를 사용하는 경우 Direct Connect 접두사를 업데이트하여 VPC에서 업데이트된 경로를 보내고 받아야 할 수도 있습니다. 자세한 내용은 AWS Direct Connect 게이트웨이에 대한 접두사 상호 작용 허용을 참조하세요.

VCF 자격 증명 검색 및 VCF 관리 어플라이언스 액세스

Amazon EVS는 AWS Secrets Manager를 사용하여 계정에 관리형 보안 암호를 생성, 암호화 및 저장합니다. 이러한 보안 암호에는 vCenter Server, NSX 및 SDDC Manager와 같은 VCF 관리 어플라이언스를 설치하고 액세스하는 데 필요한 VCF 보안 인증 정보와 ESX 루트 암호가 포함됩니다. 보안 암호 검색에 대한 자세한 내용은 AWS Secrets Manager 사용 설명서의 Secrets Manager에서 보안 암호 가져오기를 참조하세요 AWS .

> **Note**
>
> Amazon EVS는 시크릿의 관리형 교체를 제공하지 않습니다. 시크릿이 오랫동안 유지되지 않도록 교체 주기를 설정하여 정기적으로 시크릿을 교체하는 것이 좋습니다.

AWS Secrets Manager에서 VCF 자격 증명을 검색한 후 이를 사용하여 VCF 관리 어플라이언스에 로그인할 수 있습니다. 자세한 내용은 VMware 제품 설명서의 SDDC 관리자 사용자 인터페이스에 로그인 및 vSphere 클라이언트를 사용하고 구성하는 방법을 참조하세요.

EC2 직렬 콘솔 구성(선택 사항)

기본적으로 Amazon EVS는 새로 배포된 Amazon EVS 호스트에서 ESX 쉘을 활성화합니다. 이 구성을 사용하면 부팅, 네트워크 구성 및 기타 문제를 해결하는 데 사용할 수 있는 EC2 직렬 콘솔을 통해 Amazon EC2 EC2 인스턴스의 직렬 포트에 액세스할 수 있습니다. 직렬 콘솔은 인스턴스에서 네트워킹 기능 없이 사용할 수 있습니다. 직렬 콘솔을 사용하면 키보드와 모니터가 인스턴스의 직렬 포트에 직접 연결된 것처럼 실행 중인 EC2 인스턴스에 명령을 입력할 수 있습니다.

EC2 콘솔 또는를 사용하여 EC2 직렬 콘솔에 액세스할 수 있습니다 AWS CLI. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스용 EC2 직렬 콘솔을 참조하세요. Amazon EC2

> **Note**
>
> EC2 직렬 콘솔은 ESX 호스트와 로컬로 상호 작용하기 위해 Direct Console 사용자 인터페이스(DCUI)에 액세스하는 유일한 Amazon EVS 지원 메커니즘입니다.

> **Note**
>
> Amazon EVS는 기본적으로 원격 SSH를 비활성화합니다. SSH가 원격 ESX 쉘에 액세스할 수 있도록 하는 방법에 대한 자세한 내용은 VMware vSphere 제품 설명서의 SSH를 사용한 원격 ESX 쉘 액세스를 참조하세요.

EC2 직렬 콘솔에 연결

EC2 직렬 콘솔에 연결하고 문제 해결을 위해 선택한 도구를 사용하려면 특정 사전 조건 작업을 완료해야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 EC2 직렬 콘솔의 사전 조건 및 EC2 직렬 콘솔에 연결을 참조하세요. Amazon EC2

> **Note**
>
> EC2 직렬 콘솔에 연결하려면 EC2 인스턴스 상태가 여야 합니다`running`. 인스턴스가 `pending`, , `stopping`, `stopped` `shutting-down`또는 `terminated` 상태인 경우 직렬 콘솔

에 연결할 수 없습니다. 인스턴스 상태 변경에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 인스턴스 상태 변경을 참조하세요. Amazon EC2

EC2 직렬 콘솔에 대한 액세스 구성

EC2 직렬 콘솔에 대한 액세스를 구성하려면 사용자 또는 관리자가 계정 수준에서 직렬 콘솔 액세스 권한을 부여한 다음 사용자에게 액세스 권한을 부여하도록 IAM 정책을 구성해야 합니다. Linux 인스턴스의 경우 사용자가 문제 해결을 위해 직렬 콘솔을 사용할 수 있도록 모든 인스턴스에서 암호 기반 사용자를 구성해야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 EC2 직렬 콘솔에 대한 액세스 구성을 참조하세요. Amazon EC2

정리

다음 단계에 따라 생성된 AWS 리소스를 삭제합니다.

Amazon EVS 호스트 및 환경 삭제

다음 단계에 따라 Amazon EVS 호스트 및 환경을 삭제합니다. 이 작업은 Amazon EVS 환경에서 실행되는 VMware VCF 설치를 삭제합니다.

> **Note**
>
> Amazon EVS 환경을 삭제하려면 먼저 환경 내의 모든 호스트를 삭제해야 합니다. 환경과 연결된 호스트가 있는 경우 환경을 삭제할 수 없습니다.

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 창에서 환경을 선택합니다.
3. 삭제할 호스트가 포함된 환경을 선택합니다.
4. 호스트 탭을 선택합니다.
5. 호스트를 선택하고 호스트 탭에서 삭제를 선택합니다. 환경의 각 호스트에 대해이 단계를 반복합니다.
6. 환경 페이지 상단에서 삭제를 선택한 다음 환경 삭제를 선택합니다.

> **Note**
>
> 환경 삭제는 Amazon EVS VLAN 서브넷도 삭제하고 생성한 AWS Amazon EVS. AWS resources는 삭제되지 않습니다. 이러한 리소스에는 계속 비용이 발생할 수 있습니다.

7. 더 이상 필요하지 않은 Amazon EC2 용량 예약이 있는 경우 취소했는지 확인합니다. 자세한 내용은 Amazon EC2 사용 설명서의 용량 예약 취소를 참조하세요.

AWS CLI

1. 터미널 세션을 엽니다.
2. 삭제할 호스트가 포함된 환경을 식별합니다.

```
aws evs list-environments
```

다음은 응답 예입니다.

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

```
}
```

3. 환경에서 호스트를 삭제합니다. 다음은 샘플 `aws evs delete-environment-host` 요청입니다.

> **Note**
>
> 환경을 삭제하려면 먼저 환경에 포함된 모든 호스트를 삭제해야 합니다.

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

4. 이전 단계를 반복하여 환경에서 나머지 호스트를 삭제합니다.
5. 환경을 삭제합니다.

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

> **Note**
>
> 환경 삭제는 Amazon EVS가 생성한 Amazon EVS VLAN 서브넷 및 AWS Secrets Manager 보안 암호도 삭제합니다. 생성한 다른 AWS 리소스는 삭제되지 않습니다. 이러한 리소스에는 계속 비용이 발생할 수 있습니다.

6. 더 이상 필요하지 않은 Amazon EC2 용량 예약이 있는 경우 취소했는지 확인합니다. 자세한 내용은 Amazon EC2 사용 설명서의 용량 예약 취소를 참조하세요.

IPAM 리소스 삭제(HCX 인터넷 연결용)

HCX 인터넷 연결을 구성한 경우 다음 단계에 따라 IPAM 리소스를 삭제합니다.

1. 퍼블릭 IPAM 풀에서 EIP 할당을 해제합니다. 자세한 내용은 VPC IP 주소 관리자 사용 설명서의 할당 해제를 참조하세요.
2. IPAM 풀에서 퍼블릭 IPv4 CIDR의 프로비저닝을 해제합니다. 자세한 내용은 VPC IP Address Manager 사용 설명서의 풀에서 CIDRs 프로비저닝 해제를 참조하세요.
3. 퍼블릭 IPAM 풀을 삭제합니다. 자세한 내용은 VPC IP 주소 관리자 사용 설명서의 풀 삭제를 참조하세요.

4. IPAM을 삭제합니다. 자세한 내용은 VPC IP 주소 관리자 사용 설명서의 IPAM 삭제를 참조하세요.

VPC Route Server 구성 요소 삭제

생성한 Amazon VPC Route Server 구성 요소를 삭제하는 단계는 Amazon VPC 사용 설명서의 Route Server 정리를 참조하세요.

네트워크 액세스 제어 목록(ACL) 삭제

네트워크 액세스 제어 목록을 삭제하는 단계는 Amazon VPC 사용 설명서의 VPC의 네트워크 ACL 삭제를 참조하세요.

서브넷 라우팅 테이블 연결 해제 및 삭제

서브넷 라우팅 테이블의 연결을 해제하고 삭제하는 단계는 Amazon VPC 사용 설명서의 서브넷 라우팅 테이블을 참조하세요.

서브넷 삭제

서비스 액세스 서브넷을 포함하여 VPC 서브넷을 삭제합니다. VPC 서브넷을 삭제하는 단계는 Amazon VPC 사용 설명서의 서브넷 삭제를 참조하세요.

> **Note**
>
> DNS에 Route 53를 사용하는 경우 서비스 액세스 서브넷을 삭제하기 전에 인바운드 엔드포인트를 제거합니다. 그렇지 않으면 서비스 액세스 서브넷을 삭제할 수 없습니다.

> **Note**
>
> Amazon EVS는 환경이 삭제될 때 사용자를 대신하여 VLAN 서브넷을 삭제합니다. Amazon EVS VLAN 서브넷은 환경이 삭제된 경우에만 삭제할 수 있습니다.

VPC 삭제

VPC를 삭제하는 단계는 Amazon VPC 사용 설명서의 VPC 삭제를 참조하세요.

다음 단계

VMware Hybrid Cloud Extension(VMware HCX)을 사용하여 워크로드를 Amazon EVS로 마이그레이션합니다. 자세한 내용은 마이그레이션 단원을 참조하십시오.

VMware HCX를 사용하여 Amazon EVS로 워크로드 마이그레이션

Amazon EVS를 배포한 후에는 프라이빗 또는 퍼블릭 인터넷 연결로 VMware HCX를 배포하여 워크로드를 Amazon EVS로 쉽게 마이그레이션할 수 있습니다. 자세한 내용은 VMware HCX 사용 설명서의 VMware HCX 시작하기를 참조하세요. VMware

Important

HCX 인터넷 기반 마이그레이션은 일반적으로 다음과 같은 경우에는 권장되지 않습니다.

- 네트워크 지터 또는 지연 시간에 민감한 애플리케이션.
- 시간이 중요한 vMotion 작업입니다.
- 엄격한 성능 요구 사항이 적용되는 대규모 마이그레이션.

이러한 시나리오에서는 HCX 프라이빗 연결을 사용하는 것이 좋습니다. 프라이빗 전용 연결은 인터넷 기반 연결에 비해 더 안정적인 성능을 제공합니다.

HCX 연결 옵션

AWS Direct Connect 또는 Site-to-Site VPN 연결을 통한 프라이빗 연결 또는 퍼블릭 연결을 사용하여 워크로드를 Amazon EVS로 마이그레이션할 수 있습니다.

상황 및 연결 옵션에 따라 HCX와의 퍼블릭 또는 프라이빗 연결을 사용하는 것이 좋습니다. 예를 들어 일부 사이트는 성능 일관성은 높지만 VPN 암호화 또는 제한된 링크 속도로 인해 처리량은 낮은 프라이빗 연결을 가질 수 있습니다. 마찬가지로 처리량이 많은 퍼블릭 인터넷 연결이 있어 성능이 더 많이 달라질 수 있습니다. Amazon EVS를 사용하면 가장 적합한 연결 옵션을 사용할 수 있습니다.

다음 표에서는 HCX 프라이빗 연결과 퍼블릭 연결의 차이점을 비교합니다.

프라이빗 연결	퍼블릭 연결
개요	개요

프라이빗 연결	퍼블릭 연결
VPC 내에서 프라이빗 연결만 사용합니다. 외부 네트워크 연결을 위해 전송 게이트웨이와 함께 AWS Direct Connect 또는 Site-to-Site VPN을 선택적으로 사용할 수 있습니다.	탄력적 IP 주소와 퍼블릭 인터넷 연결을 사용하여 전용 프라이빗 연결 없이 마이그레이션할 수 있습니다.
에 가장 적합	에 가장 적합
• 시간에 민감한 vMotion 작업. • 대규모 마이그레이션. • 지연 시간/지터에 민감한 애플리케이션. • 대용량 데이터 전송. • 기존 AWS Direct Connect/AWS Site-to-Site VPN이 있는 조직.	• AWS Direct Connect/AWS Site-to-Site VPN이 없는 위치입니다. • 비용에 민감한 프로젝트.
주요 이점	주요 이점
• 지연 시간이 짧은 일관된 연결. • 전용 대역폭 할당. • 더 안정적인 네트워크 성능. • 성능을 최적화하기 위해 프라이빗 환경에서 기본 HCX 암호화를 비활성화할 수 있습니다. • 퍼블릭 IP 관리는 필요하지 않습니다.	• 프라이빗 연결보다 빠른 설정. • 소규모 마이그레이션에 비용 효율적입니다.
주요 고려 사항	주요 고려 사항
• 더 복잡한 초기 설정. • 더 높은 선결제 인프라 비용. • 더 긴 구현 타임라인. • HCX 구성 요소에는 직접 인터넷 연결이 없습니다.	• 더 가변적인 네트워크 성능. • 대역폭 제한이 있을 수 있습니다. • 프라이빗 연결보다 지연 시간이 깁니다. • 각 구성 요소에는 퍼블릭 IPAM 풀에서 할당된 전용 탄력적 IP 주소가 필요합니다. • EIP 연결을 사용하면 각 HCX 구성 요소에 대한 직접 인터넷 연결이 가능합니다.

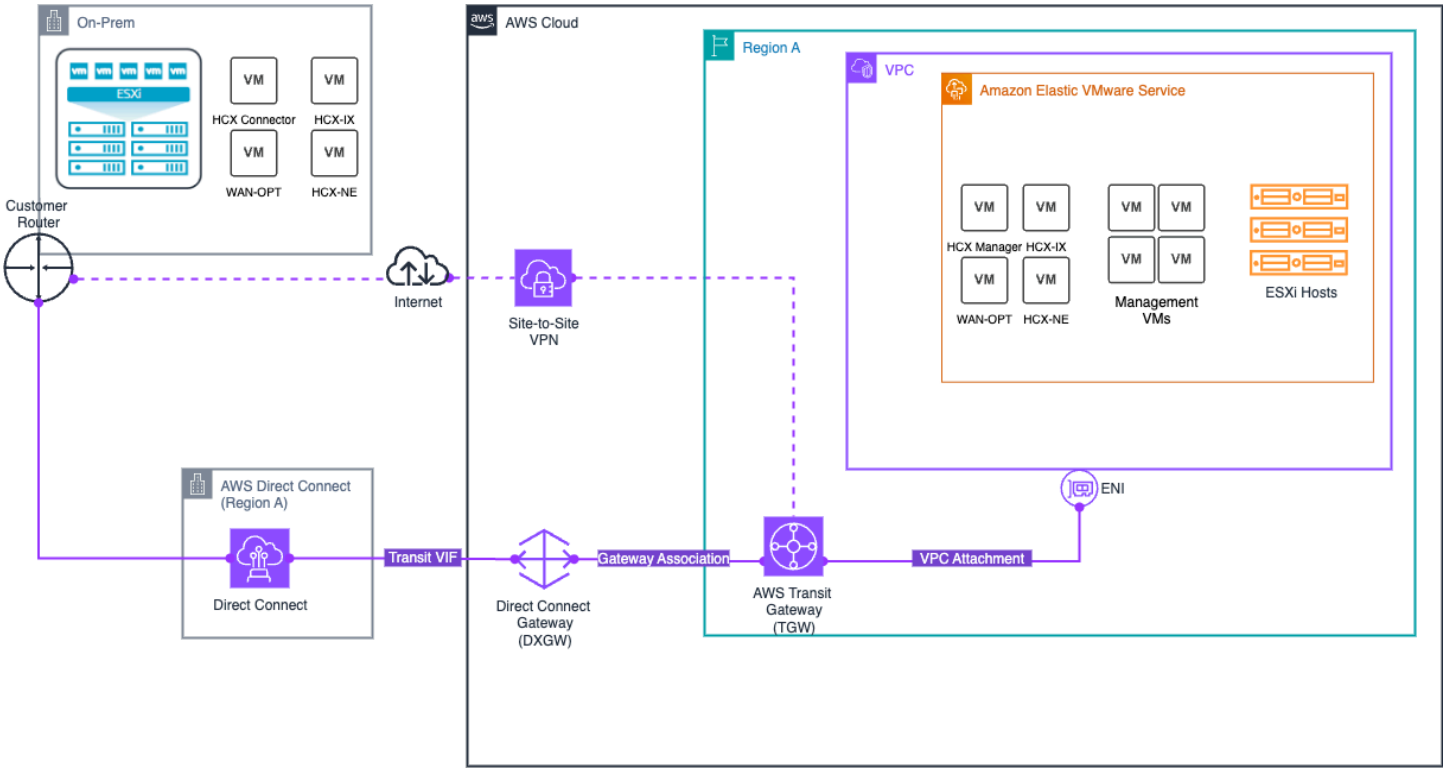
HCX 프라이빗 연결 아키텍처

HCX 프라이빗 연결 솔루션은 여러 구성 요소를 통합합니다.

- Amazon EVS 네트워크 구성 요소
  - 프라이빗 HCX VLAN을 포함한 보안 통신에는 프라이빗 VLAN 서브넷만 사용합니다.
  - 트래픽 제어를 위한 네트워크 ACLs을 지원합니다.
  - 프라이빗 VPC 라우팅 서버를 통한 경로의 동적 BGP 전파를 지원합니다.
- AWS 온프레미스 연결을 위한 관리형 네트워크 전송 옵션
  - AWS Direct Connect + AWS Transit Gateway를 사용하면 프라이빗 전용 연결을 통해 온프레미스 네트워크를 Amazon EVS에 연결할 수 있습니다. 자세한 내용은 AWS Direct Connect + AWS Transit Gateway를 참조하세요.
  - AWS Site-to-Site VPN + AWS Transit Gateway는 인터넷을 통해 원격 네트워크와 전송 게이트웨이 간에 IPsec VPN 연결을 생성하는 옵션을 제공합니다. 자세한 내용은 AWS Transit Gateway + AWS Site-to-Site VPN을 참조하세요.

> **Note**
>
> Amazon EVS는 AWS Direct Connect 프라이빗 가상 인터페이스(VIF) 또는 언더레이 VPC로 직접 종료되는 AWS Site-to-Site VPN 연결을 통한 연결을 지원하지 않습니다.

다음 다이어그램은 전송 게이트웨이와 함께 AWS Direct Connect 및 Site-to-Site VPN을 사용하여 프라이빗 전용 연결을 통해 안전한 워크로드 마이그레이션을 지원하는 방법을 보여주는 HCX 프라이빗 연결 아키텍처를 보여줍니다.



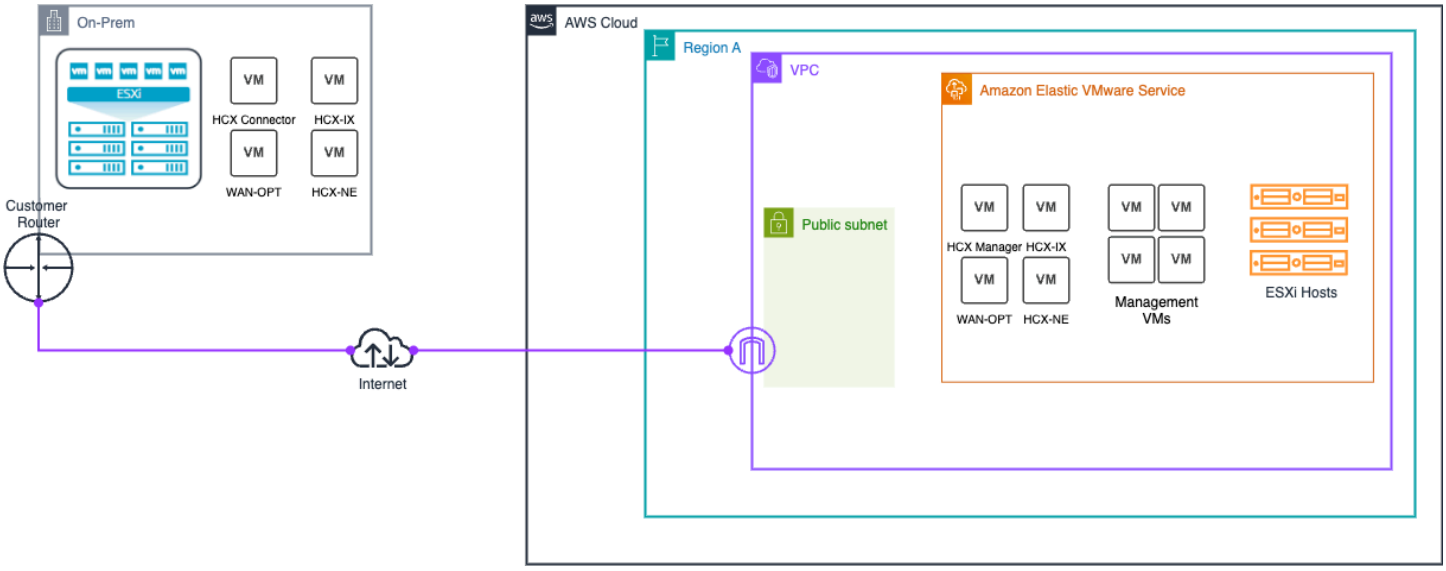
HCX 인터넷 연결 아키텍처

HCX 인터넷 연결 솔루션은 함께 작동하는 여러 구성 요소로 구성됩니다.

- Amazon EVS 네트워크 구성 요소
  - 격리된 퍼블릭 HCX VLAN 서브넷을 사용하여 Amazon EVS와 온프레미스 HCX 어플라이언스 간의 인터넷 연결을 활성화합니다.
  - 트래픽 제어를 위한 네트워크 ACLs을 지원합니다.
  - 퍼블릭 VPC 라우팅 서버를 통한 경로의 동적 BGP 전파를 지원합니다.
- IPAM 및 퍼블릭 IP 관리
  - Amazon VPC IP 주소 관리자(IPAM)는 Amazon 소유 퍼블릭 IPAM 풀에서 퍼블릭 IPv4 주소 할당을 관리합니다.
  - 보조 VPC CIDR 블록(/28)은 IPAM 풀에서 할당되어 기본 VPC CIDR과 별도로 격리된 퍼블릭 서브넷을 생성합니다.

자세한 내용은 the section called “HCX 퍼블릭 연결” 단원을 참조하십시오.

다음 다이어그램은 HCX 인터넷 연결 아키텍처를 보여줍니다.



HCX 마이그레이션 설정

이 자습서에서는 워크로드를 Amazon EVS로 마이그레이션하도록 VMware HCX를 구성하는 방법을 설명합니다.

사전 조건

Amazon EVS에서 VMware HCX를 사용하기 전에 HCX 사전 조건이 충족되었는지 확인합니다. 자세한 내용은 the section called “VMware HCX 사전 조건” 단원을 참조하십시오.

Important

Amazon EVS에는 HCX 퍼블릭 인터넷 연결에 대한 고유한 요구 사항이 있습니다.
HCX 퍼블릭 연결이 필요한 경우 다음 요구 사항을 충족해야 합니다.

- 최소 넷마스크 길이가 /28인 CIDR을 사용하여 IPAM 및 퍼블릭 IPv4 IPAM 풀을 생성합니다.
- HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스의 IPAM 풀에서 2개 이상의 탄력적 IP 주소(EIPs)를 할당합니다. 배포해야 하는 각 HCX 네트워크 어플라이언스에 대해 추가 탄력적 IP 주소를 할당합니다.
- 퍼블릭 IPv4 CIDR 블록을 VPC에 추가 CIDR로 추가합니다.

자세한 내용은 the section called “HCX 인터넷 연결 설정” 단원을 참조하십시오.

HCX VLAN 서브넷의 상태 확인

VLAN은 표준 Amazon EVS 배포의 일부로 HCX용으로 생성됩니다. 다음 단계에 따라 HCX VLAN 서브넷이 올바르게 구성되었는지 확인합니다.

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 창에서 환경을 선택합니다.
3. Amazon EVS 환경을 선택합니다.
4. 네트워크 및 연결 탭을 선택합니다.
5. VLANs에서 HCX VLAN을 식별하고 상태가 생성됨이고 퍼블릭이 true인지 확인합니다.

AWS CLI

1. 환경의 환경 ID와 리소스가 포함된 리전 이름을 사용하여 다음 명령을 실행합니다.

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

2. 응답 출력에서가 인 VLAN을 식별하고 `functionName` `hcx` `vlanState`가 `CREATED` 이고 `isPublic`가 로 설정되어 있는지 확인합니다`true`. 다음은 응답 예입니다.

```
{
    "environmentVlans": [{
            "vlanId": 50,
            "cidr": "10.10.4.0/24",
            "availabilityZone": "us-east-2b",
            "functionName": "vTep",
            "subnetId": "subnet-0ce640ac79e7f4dbc",
            "createdAt": "2025-09-09T12:09:37.526000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.596000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [],
            "isPublic": false
        },
        {
```

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


HCX VLAN 서브넷이 네트워크 ACL과 연결되어 있는지 확인

다음 단계에 따라 HCX VLAN 서브넷이 네트워크 ACL과 연결되어 있는지 확인합니다. 네트워크 ACL 연결에 대한 자세한 내용은 섹션을 참조하세요the section called “네트워크 ACL을 생성하여 Amazon EVS VLAN 서브넷 트래픽 제어”.

> **Important**
>
> 인터넷을 통해 연결하는 경우 탄력적 IP 주소를 VLAN과 연결하면 해당 VLAN의 모든 리소스에 대한 직접 인터넷 액세스가 가능합니다. 보안 요구 사항에 따라 액세스를 제한하도록 구성된 적절한 네트워크 액세스 제어 목록이 있는지 확인합니다.

> **Important**
>
> EC2 보안 그룹은 Amazon EVS VLAN 서브넷에 연결된 탄력적 네트워크 인터페이스에서 작동하지 않습니다. Amazon EVS VLAN 서브넷과 주고받는 트래픽을 제어하려면 네트워크 액세스 제어 목록(ACL)을 사용해야 합니다.

Example

Amazon VPC console

1. Amazon VPC 콘솔로 이동합니다.
2. 탐색 창에서 Network ACLs를 선택합니다.
3. VLAN 서브넷이 연결된 네트워크 ACL을 선택합니다.
4. 서브넷 연결 탭을 선택합니다.
5. HCX VLAN 서브넷이 연결된 서브넷에 나열되어 있는지 확인합니다.

AWS CLI

1. `Values` 필터에서 HCX VLAN 서브넷 ID를 사용하여 다음 명령을 실행합니다.

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

2. 응답에 올바른 네트워크 ACL이 반환되는지 확인합니다.

EVS VLAN 서브넷이 라우팅 테이블과 명시적으로 연결되어 있는지 확인

Amazon EVS에서는 모든 EVS VLAN 서브넷을 VPC의 라우팅 테이블과 명시적으로 연결해야 합니다. HCX 인터넷 연결의 경우 HCX 퍼블릭 VLAN 서브넷이 인터넷 게이트웨이로 라우팅되는 VPC의 퍼블릭 라우팅 테이블과 명시적으로 연결되어야 합니다. 다음 단계에 따라 명시적 라우팅 테이블 연결을 확인합니다.

Example

Amazon VPC console

1. VPC 콘솔로 이동합니다.

2. 탐색 창에서 Route tables을 선택합니다.
3. EVS VLAN 서브넷이 명시적으로 연결되어야 하는 라우팅 테이블을 선택합니다.
4. 서브넷 연결 탭을 선택합니다.
5. 명시적 서브넷 연결에서 모든 EVS VLAN 서브넷이 나열되어 있는지 확인합니다. VLAN 서브넷이 여기에 나열되지 않은 경우 VLAN 서브넷은 기본 라우팅 테이블과 암시적으로 연결됩니다. Amazon EVS가 제대로 작동하려면 모든 VLAN 서브넷을 라우팅 테이블과 명시적으로 연결해야 합니다. HCX 퍼블릭 VLAN 서브넷의 경우 인터넷 게이트웨이를 대상으로 하는 연결된 퍼블릭 라우팅 테이블이 있어야 합니다. 이 문제를 해결하려면 서브넷 연결 편집을 선택하고 누락된 VLAN 서브넷(들)을 추가합니다.

AWS CLI

1. 터미널 세션을 엽니다.
2. 다음 예제 명령을 실행하여 라우팅 테이블 연결을 포함하여 모든 EVS VLAN 서브넷에 대한 세부 정보를 검색합니다. VLAN 서브넷이 여기에 나열되지 않은 경우 VLAN 서브넷은 기본 라우팅 테이블과 암시적으로 연결됩니다. Amazon EVS가 제대로 작동하려면 모든 VLAN 서브넷을 라우팅 테이블과 명시적으로 연결해야 합니다. HCX 퍼블릭 VLAN 서브넷의 경우 인터넷 게이트웨이를 대상으로 하는 연결된 퍼블릭 라우팅 테이블이 있어야 합니다.

```
aws ec2 describe-subnets
```

3. EVS VLAN 서브넷을 VPC의 라우팅 테이블과 명시적으로 연결합니다. 다음은 예제 명령입니다.

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

(HCX 인터넷 연결의 경우) EIPs HCX VLAN 서브넷과 연결되어 있는지 확인합니다.

배포하는 각 HCX 네트워크 어플라이언스에 대해 HCX 퍼블릭 VLAN 서브넷과 연결된 IPAM 풀의 EIP가 있어야 합니다. HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스의 HCX 퍼블릭 VLAN 서브넷에 두 개 이상의 EIPs를 연결해야 합니다. 다음 단계에 따라 필요한 EIP 연결이 존재하는지 확인합니다.

Important

IPAM 풀의 EIPs를 HCX 퍼블릭 VLAN 서브넷과 두 개 이상 연결하지 않으면 HCX 퍼블릭 인터넷 연결이 실패합니다.

Note

퍼블릭 IPAM CIDR 블록의 처음 두 EIPs 또는 마지막 EIP를 VLAN 서브넷과 연결할 수 없습니다. 이러한 EIPs는 네트워크, 기본 게이트웨이 및 브로드캐스트 주소로 예약됩니다. 이러한 EIPs를 VLAN 서브넷과 연결하려고 하면 Amazon EVS에서 검증 오류가 발생합니다.

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 메뉴에서 환경을 선택합니다.
3. 환경을 선택합니다.
4. 네트워크 및 연결 탭에서 HCX 퍼블릭 VLAN을 선택합니다.
5. EIP 연결 탭을 확인하여 EIPs가 HCX 퍼블릭 VLAN과 연결되었는지 확인합니다.

AWS CLI

1. HCX VLAN 서브넷과 연결된 EIPs를 확인하려면 `list-environment-vlans` 명령을 사용합니다. 의 경우 `environment-id`HCX VLAN이 포함된 EVS 환경의 고유 ID를 사용합니다.

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

명령은 EIP 연결을 포함하여 VLANs 대한 세부 정보를 반환합니다.

```
{
  "environmentVlans": [
    {
      "vlanId": 80,
```

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


`eipAssociations` 배열은 다음을 포함한 EIP 연결을 보여줍니다.

- `associationId` -이 EIP 연결의 고유 ID입니다.
- `allocationId` - 연결된 탄력적 IP 주소의 할당 ID입니다.
- `ipAddress` - VLAN에 할당된 IP 주소입니다.

HCX 퍼블릭 업링크 VLAN ID를 사용하여 분산 포트 그룹 생성

vSphere 클라이언트 인터페이스로 이동하여 분산 포트 그룹 추가의 단계에 따라 vSphere 분산 스위치에 분산 포트 그룹을 추가합니다.

vSphere Client 인터페이스 내에서 장애 복구를 구성할 때는 업링크1이 활성 업링크이고 업링크2가 활성/대기 장애 조치를 활성화하는 대기 업링크인지 확인합니다. vSphere Client 인터페이스의 VLAN 설정에 이전에 식별한 HCX VLAN ID를 입력합니다.

(선택 사항) HCX WAN 최적화 설정

> **Note**
>
> HCX 4.11.3에서는 WAN 최적화 기능을 더 이상 사용할 수 없습니다. 자세한 내용은 HCX 4.11.3 릴리스 정보를 참조하세요.

HCX WAN 최적화 서비스(HCX-WO)는 데이터 축소 및 WAN 경로 조정과 같은 WAN 최적화 기술을 적용하여 프라이빗 라인 또는 인터넷 경로의 성능 특성을 개선합니다. HCX WAN 최적화 서비스는 마이그레이션에 10Gbit 경로를 전용할 수 없는 배포에 권장됩니다. 10Gbit에서는 지연 시간이 짧은 배포에서 WAN 최적화를 사용하면 마이그레이션 성능이 향상되지 않을 수 있습니다. 자세한 내용은 VMware HCX 배포 고려 사항 및 모범 사례를 참조하세요.

HCX WAN 최적화 서비스는 HCX WAN Interconnect 서비스 어플라이언스(HCX-IX)와 함께 배포됩니다. HCX-IX는 엔터프라이즈 환경과 Amazon EVS 환경 간의 데이터 복제를 담당합니다.

Amazon EVS에서 HCX WAN 최적화 서비스를 사용하려면 HCX VLAN 서브넷에서 분산 포트 그룹을 사용해야 합니다. 이전 단계에서 생성된 분산 포트 그룹을 사용합니다.

(선택 사항) HCX 모빌리티 최적화 네트워킹 활성화

HCX Mobility Optimized Networking(MON)은 HCX Network Extension Service의 기능입니다. MON 지원 네트워크 확장은 Amazon EVS 환경 내에서 선택적 라우팅을 활성화하여 마이그레이션된 가상 머신의 트래픽 흐름을 개선합니다. MON을 사용하면 계층 2 네트워크를 확장할 때 Amazon EVS로 워크로드 트래픽을 마이그레이션하기 위한 최적의 경로를 구성하여 소스 게이트웨이를 통한 긴 왕복 네트워크 경로를 피할 수 있습니다. 이 기능은 모든 Amazon EVS 배포에 사용할 수 있습니다. 자세한 내용은 VMware HCX 사용 설명서의 이동성 최적화 네트워킹 구성을 참조하세요.

> **Important**
>
> HCX MON을 활성화하기 전에 HCX Network Extension에 대해 다음 제한 사항과 지원되지 않는 구성을 읽으십시오.
> 네트워크 확장에 대한 제한 및 제한 사항

이동성 최적화 네트워킹 토폴로지에 대한 제한 및 제한 사항

Important

HCX MON을 활성화하기 전에 NSX 인터페이스에서 대상 네트워크 CIDR에 대한 라우팅 재배포를 구성했는지 확인합니다. 자세한 내용은 VMware NSX 설명서의 BGP 구성 및 경로 재배포를 참조하세요.

HCX 연결 확인

VMware HCX에는 연결을 테스트하는 데 사용할 수 있는 진단 도구가 내장되어 있습니다. 자세한 내용은 VMware HCX 사용 설명서의 VMware HCX 문제 해결을 참조하세요. VMware

HCX 퍼블릭 인터넷 연결 구성

탄력적 IP 주소를 VLAN과 연결하여 HCX 퍼블릭 VLAN에 대한 퍼블릭 인터넷 액세스를 구성할 수 있습니다. 이를 통해 마이그레이션 작업에 인터넷 액세스가 필요한 VMware HCX 어플라이언스 및 워크로드에 대한 직접 인터넷 연결이 가능합니다.

관련 주제

이 주제에서는 HCX 퍼블릭 VLAN에 대한 인터넷 액세스 관리를 다룹니다. 완전한 구현을 위해:

1. 에서 사전 조건을 완료합니다Amazon Elastic VMware Service 설정.
2. 에서 초기 설정을 구성합니다시작하기.
3. 인터넷 액세스를 구성합니다(이 주제).

HCX VLAN 인터넷 액세스 정보

VMware HCX 어플라이언스에 대한 인터넷 액세스를 구성하여 인터넷을 통해 워크로드를 Amazon EVS로 HCX 마이그레이션할 수 있습니다.

이 접근 방식은 다음과 같습니다.

- 전용 프라이빗 연결 없이 가상 머신 마이그레이션을 활성화합니다.

- 유연하고 비용 효율적인 마이그레이션 솔루션을 제공합니다.

> **Important**
>
> HCX 인터넷 기반 마이그레이션은 일반적으로 다음과 같은 경우에는 권장되지 않습니다.
>
> - 네트워크 지터 또는 지연 시간에 민감한 애플리케이션.
> - 시간이 중요한 vMotion 작업입니다.
> - 엄격한 성능 요구 사항이 적용되는 대규모 마이그레이션.
>
> 이러한 시나리오에서는 HCX 프라이빗 연결을 사용하는 것이 좋습니다. 프라이빗 전용 연결은 인터넷 기반 연결에 비해 더 안정적인 성능을 제공합니다.

인터넷 연결 개요

다음 고려 사항을 검토합니다.

HCX 네트워킹 요구 사항 및 DNAT

HCX에는 퍼블릭 인터넷 액세스를 설정하는 방법에 영향을 미치는 특정 네트워킹 제약이 있습니다.

HCX는 대상 네트워크 주소 변환(DNAT)을 지원하지 않습니다. 대신 HCX를 사용하려면 업링크 네트워크를 기본 게이트웨이 IP 주소로 라우팅할 수 있어야 합니다.

Amazon EVS VLAN 서브넷에는 다른 VPC 서브넷과 같은 기본 게이트웨이 IP 주소가 포함됩니다. 그러나 이러한 서브넷은 RFC1918 주소 범위 외부에서 CIDR 블록을 사용하는 경우에도 항상 프라이빗 서브넷입니다.

HCX 인터넷 연결 활성화

DNAT 없이 인터넷 연결을 활성화하기 위해 Amazon EVS는 특정 CIDR 구성 접근 방식을 사용합니다.

- 인터넷 라우팅 가능 CIDR 요구 사항: Amazon EVS에는 HCX VLAN 서브넷 CIDR과 일치하는 인터넷 라우팅 가능 CIDR이 필요합니다.
- IPAM 할당: Amazon EVS는 최소 넷마스크 길이가 /28인 퍼블릭 IPAM 할당 CIDR을 인터넷 라우팅 가능 CIDR로 사용합니다.

- VPC 구성: VPC에 퍼블릭 IPAM 할당 CIDR을 보조 VPC CIDR로 수동으로 추가해야 합니다.
- VLAN 서브넷 배포: IPAM 및 VPC가 구성된 후 Amazon EVS 배포 중에 HCX VLAN 서브넷에서 퍼블릭 IPAM 할당 CIDR을 사용할 수 있습니다.
- 탄력적 IP 구성: Amazon EVS에는 다음 구성이 필요합니다.
  - 탄력적 IPs 할당: IPAM 할당 CIDR에서 탄력IPs. HCX Manager 및 HCX Interconnect(HCX-IX) 어플라이언스의 IPAM 풀에서 최소 2개의 탄력적 IP 주소(EIPs)를 할당해야 합니다. 배포해야 하는 각 HCX 네트워크 어플라이언스에 대해 추가 탄력적 IP 주소를 할당합니다.
  - VLAN과 연결: HCX 어플라이언스와 함께 사용할 각 탄력적 IP를 HCX VLAN 서브넷에 연결합니다. 이 연결에는 Amazon EVS 콘솔 또는 AWS CLI 를 사용합니다.
  - 게이트웨이 주소 구성: CIDR에서 사용 가능한 첫 번째 주소는 HCX 어플라이언스에서 구성하는 게이트웨이 주소가 됩니다.
  - 트래픽 라우팅: 연결된 각 탄력적 IP의 트래픽은 DNAT 없이 동일한 IP 주소를 가진 대상 HCX 어플라이언스로 직접 라우팅됩니다.

Amazon EVS 환경 배포를 위한 인터넷 연결로 HCX를 구성하는 단계는 Amazon Elastic VMware Service 설정 및 섹션을 참조하세요시작하기.

작업 고려 사항

- HCX 퍼블릭 VLAN CIDR 블록의 넷마스크 길이는 /28이어야 합니다.
- EIPs는 Amazon EVS 콘솔을 사용하여 배포한 후 HCX 퍼블릭 VLAN과 연결하거나 연결 해제할 수 AWS CLI있지만 동일한 IPAM 풀에서 연결해야 합니다.
- 각 EIP 연결에는 고유한 연결 ID가 있습니다.
- /28 HCX 퍼블릭 VLAN과 연결된 퍼블릭 IPAM 풀에서 최대 13EIPs를 보유할 수 있습니다. 퍼블릭 IPAM 할당 CIDR 블록의 처음 두 EIPs 또는 마지막 EIP를 HCX 퍼블릭 VLAN 서브넷과 연결할 수 없습니다. 이러한 EIPs는 네트워크, 기본 게이트웨이 및 브로드캐스트 주소로 예약됩니다. 이러한 EIPs를 VLAN과 연결하려고 하면 Amazon EVS에서 검증 오류가 발생합니다.

보안 고려 사항

- 네트워크 액세스 제어 목록(ACLs HCX 퍼블릭 VLAN 서브넷을 통해 흐르는 트래픽에 계속 적용됩니다.
- 보안 그룹 규칙은 HCX 퍼블릭 VLAN 서브넷의 트래픽에는 적용되지 않습니다. 트래픽 제어에 네트워크 ACLs 사용합니다.

> **Important**
>
> 인터넷을 통해 연결하는 경우 탄력적 IP 주소를 VLAN과 연결하면 해당 VLAN의 모든 리소스에 대한 직접 인터넷 액세스가 가능합니다. 보안 요구 사항에 따라 액세스를 제한하도록 구성된 적절한 네트워크 액세스 제어 목록이 있는지 확인합니다.

VLANs의 탄력적 IP 주소 관리

Amazon EVS 콘솔 또는를 사용하여 탄력적 IP 주소를 HCX 퍼블릭 VLAN과 연결 및 연결 해제할 수 있습니다 AWS CLI.

> **Note**
>
> Amazon EVS는 현재 탄력적 IP 주소와 HCX 퍼블릭 VLAN의 연결 및 연결 해제만 지원합니다.

탄력적 IP 주소를 VLAN과 연결

사전 조건

다음이 있는지 확인합니다.

- 탄력적 IP 주소는 Amazon 소유 퍼블릭 IPAM 풀에서 할당됩니다.
- Amazon EVS 환경이 이미 생성되었습니다.

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 메뉴에서 환경을 선택합니다.
3. 환경을 선택합니다.
4. 네트워크 및 연결 탭에서 HCX 퍼블릭 VLAN을 선택합니다.

> **Note**
>
> Amazon EVS는 현재 EIPs HCX VLAN의 연결만 지원합니다.

5. EIP를 VLAN에 연결을 선택합니다.
6. HCX 퍼블릭 VLAN과 연결할 탄력적 IP 주소(들)를 선택합니다.
7. EIPs 연결을 선택합니다. HCX 퍼블릭 VLAN과 최대 13EIPs를 연결할 수 있습니다.

> **Note**
>
> 퍼블릭 IPAM CIDR 블록의 처음 두 EIPs VLAN 서브넷에 연결할 수 없습니다. 이러한 EIPs는 네트워크 및 기본 게이트웨이 주소로 예약됩니다.

8. EIP 연결을 확인하여 EIPs가 HCX 퍼블릭 VLAN과 연결되었는지 확인합니다.

AWS CLI

1. 탄력적 IP 주소를 VLAN과 연결하려면 예제 `associate-eip-to-vlan` 명령을 사용합니다.
   - `environment-id` - Amazon EVS 환경의 ID입니다.
   - `vlan-name` - 여야 합니다`hcx`. Amazon EVS는 현재 HCX VLAN과의 EIP 연결만 지원합니다.
   - `allocation-id` - 탄력적 IP 주소의 할당 ID입니다.

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

명령은 새 EIP 연결을 포함하여 VLAN에 대한 세부 정보를 반환합니다.

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [
            {
                "associationId": "eipassoc-09e966faad7ecc58a",
```

```
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

`eipAssociations` 배열은 다음을 포함한 새 연결을 보여줍니다.

- `associationId` - 연결 해제에 사용되는이 EIP 연결의 고유 ID입니다.
- `allocationId` - 연결된 탄력적 IP 주소의 할당 ID입니다.
- `ipAddress` - VLAN에 할당된 IP 주소입니다.

2. 단계를 반복하여 추가 EIPs 연결합니다. HCX 퍼블릭 VLAN과 최대 13EIPs를 연결할 수 있습니다.

VLAN에서 탄력적 IP 주소 연결 해제

사전 조건

다음이 있는지 확인합니다.

- Amazon EVS 환경이 이미 생성되었습니다.
- EIP는 Amazon EVS 환경과 연결됩니다.

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 메뉴에서 환경을 선택합니다.
3. 환경을 선택합니다.
4. 네트워크 및 연결 탭에서 HCX 퍼블릭 VLAN을 선택합니다.
5. VLAN에서 EIP 연결 해제를 선택합니다.
6. HCX 퍼블릭 VLAN에서 연결을 해제할 탄력적 IP 주소(들)를 선택합니다.

> **Important**
>
> EIPs 연결 해제하면 퍼블릭 VLAN 서브넷을 사용하는 어플라이언스의 인터넷 연결이 끊어질 수 있습니다.

7. EIPs 선택합니다.
8. EIP 연결을 확인하여 EIPs가 HCX 퍼블릭 VLAN에서 연결 해제되었는지 확인합니다.

AWS CLI

VLAN에서 탄력적 IP 주소를 연결 해제하려면 예제 `disassociate-eip-from-vlan` 명령을 사용합니다.

- `environment-id` - Amazon EVS 환경의 ID입니다.
- `vlan-name` - 여야 합니다`hcx`. Amazon EVS는 현재 HCX VLAN과의 EIP 연결만 지원합니다.
- `association-id` - 제거할 EIP 연결의 연결 ID입니다.

> **Important**
>
> EIPs 연결 해제하면 퍼블릭 VLAN 서브넷을 사용하는 어플라이언스의 인터넷 연결이 끊어질 수 있습니다.

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

명령은 EIP 연결이 제거된 VLAN에 대한 세부 정보를 반환합니다.


```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
```

```
        "modifiedAt": "2025-08-23T13:48:49.846000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

빈 `eipAssociations` 배열은 탄력적 IP 주소가 VLAN에서 성공적으로 연결 해제되었음을 확인합니다.

인터넷 기반 마이그레이션을 위한 HCX WAN 최적화 정보

> **Note**
>
> HCX 4.11.3에서는 WAN 최적화 기능을 더 이상 사용할 수 없습니다. 자세한 내용은 HCX 4.11.3 릴리스 정보를 참조하세요.

인터넷을 통해 마이그레이션을 수행할 때 HCX WAN 최적화(HCX-WO)는 마이그레이션 성능을 개선할 수 있습니다. 서비스는 HCX Interconnect 어플라이언스(HCX-IX)와 함께 작동하여 다음을 수행합니다.

- 데이터 감소 기술을 적용하여 대역폭 사용량을 최소화합니다.
- WAN 경로 조정을 구현하여 네트워크 성능을 최적화합니다.
- 지연 시간이 긴 인터넷 연결을 통해 마이그레이션 속도를 개선합니다.
- 인터넷 기반 마이그레이션의 신뢰성을 높입니다.

HCX WAN 최적화는 다음과 같은 인터넷 기반 마이그레이션에 특히 유용합니다.

- 네트워크 지연 시간은 프라이빗 연결 옵션보다 높을 수 있습니다.
- 사용 가능한 대역폭은 제한되거나 가변적일 수 있습니다.
- 인터넷 트래픽 패턴으로 인해 네트워크 조건이 변동할 수 있습니다.

인터넷 연결을 구성한 후 HCX WAN 최적화를 설정하는 방법에 대한 자세한 지침은 섹션을 참조하세요the section called “(선택 사항) HCX WAN 최적화 설정”.

> **Note**
>
> WAN 최적화는 인터넷 기반 마이그레이션 성능을 크게 개선할 수 있지만 지연 시간이 짧은 전용 10Gbit 연결이 있는 환경에서는 추가 이점을 제공하지 않을 수 있습니다. 이 기능을 활성화할지 여부를 결정할 때는 네트워크 특성을 고려하세요.

Amazon EVS 환경 관리

이 장에는 환경을 관리하는 데 도움이 되는 다음 주제가 포함되어 있습니다.

- the section called “VCF 구독” - VCF 구독이 Amazon EVS와 작동하는 방식과 VCF 구독 관리에 대한 고객 책임을 설명합니다.
- the section called “VCF 버전 및 EC2 인스턴스” - 지원되는 VCF 및 ESX 버전과 Amazon EVS에서 버전 가용성을 확인하는 방법을 설명합니다.
- the section called “수명 주기 관리” - 기본 인프라 관리, VCF 업그레이드 관리, ESX 호스트 수명 주기 관리를 포함하여 Amazon EVS 환경 내의 수명 주기 관리 책임을 설명합니다.
- the section called “환경 유지 관리” - 네트워킹 구성, ESX 호스트 유지 관리, 환경 상태 확인, VCF 자격 증명의 보안 암호 교체 일정 관리 등 Amazon EVS 환경에 대한 일반적인 유지 관리 작업을 수행하는 방법을 설명합니다.
- the section called “호스트 생성” - 환경이 배포된 후 Amazon EVS 호스트를 생성하고 호스트를 클러스터에 추가하는 방법을 설명합니다.
- the section called “호스트 삭제” - Amazon EVS 호스트를 삭제하고 클러스터에서 제거하는 방법을 설명합니다.

VCF 구독

> **Note**
>
> Amazon EVS는 영구 vSphere 라이선스를 지원하지 않습니다. Amazon EVS를 사용하려면 유효하고 활성 상태인 VMware Cloud Foundation 구독이 있어야 합니다.

Amazon EVS는 (BYOS)에 제공하는 라이선스 이동성 권한과 함께 VMware Cloud Foundation AWS (VCF) 구독을 사용합니다. Amazon EVS 환경을 성공적으로 배포하려면 환경 생성 요청에 유효한 VCF 솔루션 키와 vSAN 라이선스 키를 제공해야 합니다. vSphere 라이선스 키는 VCF의 솔루션 키 역할을 합니다. 각 VCF 라이선스 키는 하나의 Amazon EVS 환경에만 사용할 수 있습니다. 다른 환경에서 이미 사용 중인 VCF 라이선스 키를 사용하려고 하면 환경 생성이 실패합니다.

환경 생성 시 Amazon EVS가 배포하는 4개의 초기 EC2 i4i.metal 호스트에 적절한 코어 용량을 제공하려면 VCF 솔루션 키에 256개 이상의 코어가 있어야 합니다. 각 i4i.metal 호스트에는 64개의 코어가 필

요합니다. vSAN 라이선스 키에는 최소 110TiB의 vSAN 용량이 있어야 합니다. 크기가 작은 라이선스 키를 사용하려고 하면 환경 생성이 실패합니다.

> **Note**
>
> VCF 구독은 라이선스 규정 준수를 위해 모든 AWS 리전의 Amazon EVS에서 사용할 수 있습니다. Amazon EVS는 라이선스 키를 검증하지 않습니다. 라이선스 키를 검증하려면 Broadcom 지원을 방문하세요.

> **Note**
>
> Amazon EVS의 VCF 소프트웨어에 대한 정보는 라이선스 규정 준수를 확인하기 위해 Broadcom과 공유됩니다.

구독 관리

VCF 구독 관리는 사용자의 책임입니다. VCF 구독은 SDDC Manager에서 관리해야 합니다. SDDC Manager에서 라이선스 키를 제거하거나 사용 중인 라이선스 키로 교체하면 환경 상태 확인이 실패하여 Amazon EVS 환경에 호스트를 추가할 수 없습니다. 환경 상태 확인에 대한 자세한 내용은 the section called “환경 상태 모니터링” 및 단원을 참조하십시오the section called “실패한 환경 상태 확인 문제 해결”. VCF 라이선스 키에 대한 자세한 내용은 VMware Cloud Foundation 설명서의 VMware Cloud Foundation에서 라이선스 키 관리를 참조하세요. VMware

> **Important**
>
> SDDC Manager 사용자 인터페이스를 사용하여 VCF 솔루션 및 vSAN 라이선스 키를 관리합니다. Amazon EVS에서는 서비스가 제대로 작동하려면 SDDC Manager에서 유효한 VCF 솔루션 및 vSAN 라이선스 키를 유지해야 합니다. vSphere Client를 사용하여 호스트 및 vSAN 클러스터에 키를 할당해야 하지만 이러한 키가 SDDC Manager 사용자 인터페이스의 라이선스 화면에도 표시되는지 확인해야 합니다.

VCF 라이선스 키 추가

Broadcom 지원 포털에서 추가 VCF 라이선스 키를 구매하거나, 이미 큰 키가 있는 경우 라이선스 키를 분할하거나, 여러 라이선스 키를 병합할 수 있습니다. 이렇게 하면 초기 배포 후 환경에 추가한 호

스트에 라이선스를 부여하거나 추가 환경에 라이선스를 부여할 수 있습니다. 구매한 라이선스 키가 vCenter Sever 및 SDDC Manager 인벤토리에 추가되었는지 확인합니다. 호스트를 추가하는 경우 라이선스가 vSphere의 올바른 호스트에 할당되고 적절한 코어와 vSAN 스토리지 용량이 있는지 확인합니다. Amazon EVS는 라이선스가 없는 호스트를 지원하지 않습니다. 자세한 내용은 VMware 설명서의 vSphere Client에서 자산에 대한 라이선스 설정 구성을 참조하세요.

라이선스 키의 평가 기간이 만료되어 활성 상태를 유지하려면 만료되지 않은 새 라이선스 키를 vCenter Server에 할당해야 합니다. Amazon EVS 환경을 성공적으로 설정하려면 활성 라이선스 키가 필요합니다. 만료된 라이선스 키가 제공되면 환경이 배포되지 않습니다. VCF 라이선스 키 생성에 대한 자세한 내용은 VMware 설명서의 새 라이선스 생성을 참조하세요. 추가된 라이선스 키에 문제가 있는 경우 섹션을 참조하세요the section called “키 적용 범위 확인 실패”.

VCF 라이선스 키 제거

SDDC Manager 인벤토리에서 VCF 라이선스 키를 제거하여 환경에서 호스트를 삭제한 후 코어 및 vSAN 용량을 줄일 수 있습니다. vSphere와 함께 사용하는 제품의 라이선스 모델을 준수하려면 인벤토리에서 할당되지 않은 모든 라이선스 키를 제거해야 합니다. Broadcom 지원 포털에서 라이선스 키를 분할, 병합 또는 업그레이드한 경우 이전 라이선스 키를 제거해야 합니다. 자세한 내용은 VMware 설명서의 라이선스 제거를 참조하세요.

Amazon EVS에서 제공하는 VCF 버전 및 EC2 인스턴스 유형

Amazon EVS는 환경을 생성하고 호스트를 생성할 때 선택할 수 있는 VMware Cloud Foundation(VCF), ESX 및 EC2 인스턴스 유형의 여러 버전을 제공합니다.

제공된 VCF 버전, ESX 버전 및 EC2 인스턴스 유형 확인

AWS 콘솔에는 환경 생성 마법사에서 Amazon EVS가 제공하는 VCF 버전 목록이 표시됩니다. 기존 환경에 호스트를 추가하는 동안 인스턴스 유형을 선택하면 사용 가능한 ESX 버전이 표시됩니다. CLI를 사용하여 VCF 버전, ESX 버전 및 EC2 인스턴스 유형을 볼 수도 있습니다.

Example

Amazon EVS console

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 메뉴에서 환경을 선택합니다.
3. 다음 중 하나를 수행하세요.

VCF 버전을 확인하려면:

a. 환경 생성을 선택합니다.

b. Amazon EVS 요구 사항 검증에서 VCF 버전을 선택하여 상태가 사용 가능한지 또는 제한된지 확인합니다.

ESX 버전을 확인하려면:

a. 기존 환경을 선택합니다.

b. [호스트 생성(Create host)]을 선택합니다.

c. 인스턴스 유형을 선택하여 사용 가능한 ESX 버전을 확인합니다.

AWS CLI

다음 명령을 실행하여 VCF 및 ESX 버전에 대한 정보를 검색합니다.

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

응답 예제:

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

```
}
```

> **Note**
>
> 필요한 버전에가 표시되고 특정 요구 사항이 있는 경우 해당 버전에 액세스하는 방법에 the section called “제한된 VCF 버전에 대한 액세스 요청” 대한 자세한 내용은 섹션을 참조RESTRICTED하세요.

Amazon EVS의 현재 VCF 버전

Amazon EVS는 현재 환경 생성을 위해 다음과 같은 VCF 버전을 제공합니다.

VCF 버전	기본 ESX 버전	Status	EC2 인스턴스 유형
VCF-5.2.2	ESXi-8.0U3g-24859861	AVAILABLE	i4i.metal
VCF-5.2.1	ESXi-8.0U3b-24280767	제한됨	i4i.metal

> **Note**
>
> 새 Amazon EVS 환경을 생성할 때 VCF 버전을 지정해야 합니다.

ESX 버전 고려 사항

각 VCF 버전에는 Broadcom VCF BOM(Bill of Materials)을 기반으로 하는 기본 ESX 버전이 있습니다. 새 환경을 생성할 때는 특정 ESX 버전을 선택할 수 없습니다. 선택한 VCF 버전의 기본 ESX 버전이 자동으로 적용됩니다.

그러나 호스트를 환경에 추가할 때 선택한 인스턴스 유형에 사용 가능한 ESX 버전을 선택할 수 있습니다. 지정하지 않으면 Amazon EVS는 환경의 VCF 버전과 연결된 기본 ESX 버전을 사용합니다.

호스트를 추가한 후에는 vCenter Lifecycle Manager를 사용해서만 해당 ESX 버전을 업그레이드할 수 있습니다.

> **Note**
>
> Amazon EVS는 Broadcom에서 릴리스한 VCF 및 ESX의 일부 버전을 제공하지 않습니다. 소프트웨어 상호 운용성 정보는 Broadcom 상호 운용성 매트릭스를 참조하세요. AWS EC2 인스턴스와의 전체 하드웨어 호환성은 Broadcom 호환성 가이드를 참조하세요.

제한된 VCF 버전에 대한 액세스 요청

`RESTRICTED` 상태가 인 VCF 버전에 액세스해야 하는 경우 다음 정보를 사용하여 AWS Support에 문의하세요.

- AWS 계정 ID
- AWS 리전
- 필요한 특정 VCF 버전
- 사용 사례 및 비즈니스 근거(예: 보안/규정 준수, 호환성/종속성 등)

AWS Support는 요청을 검토하고 추가 정보를 승인하거나 요청합니다. 승인 후 AWS 콘솔 또는 `get-versions` API 응답`AVAILABLE`에서 버전 상태가 로 변경됩니다.

Amazon EVS 환경 수명 주기 관리

이 페이지에서는 Amazon EVS 환경 내의 수명 주기 관리 책임을 설명합니다.

Amazon EVS의 주요 이점은 클라우드에서 VMware 아키텍처를 완벽하게 제어할 수 있다는 것입니다. VMware Cloud Foundation(VCF) 소프트웨어 스택을 최적화하여 애플리케이션의 고유한 요구 사항을 충족할 수 있습니다. Amazon EVS는 자체 관리형 서비스이므로 ESX, vSphere, vSAN, NSX 및 SDDC Manager와 같은 Amazon EVS 환경에서 사용되는 VMware 소프트웨어의 수명 주기 관리 및 유지 관리에 대한 책임은 사용자에게 있습니다. 또한 Amazon EVS 호스트에 통합하는 데이터 보호 솔루션과 같은 타사 통합을 유지 관리할 책임이 있습니다.

VPC 라우팅 테이블, 보안 그룹 및 네트워크 액세스 제어 목록(ACL) 규칙, VPC Route Server 구성, 인터넷 게이트웨이, NAT 게이트웨이 및 전송 게이트웨이(온프레미스 연결용)를 포함하여 Amazon EVS가 사용하는 기본 AWS 네트워킹 구성 요소의 구성은 사용자의 책임입니다.

AWS 는 사용자가 제공하는 네트워킹 구성으로 Amazon EVS 환경을 배포하는 역할을 합니다. 환경 배포에는 다음이 포함됩니다.

- Amazon EVS 환경의 네트워크 구성을 부트스트래핑합니다.
- 제공한 VPC Route Server 인스턴스를 사용하여 남북 라우팅을 활성화합니다.
- 필요한 EVS VLAN 서브넷, 탄력적 네트워크 인터페이스 및 4개의 초기 ESX 호스트를 배포합니다.
- Tier-0 게이트웨이와 Tier-1 게이트웨이를 사용하여 NSX 오버레이 네트워크 구성.
- 활성/대기 모드에서 두 개의 NSX Edge 노드가 있는 NSX Edge 클러스터 배포.
- 초기 vSAN 클러스터를 생성 및 구성하고 데이터 스토어를 탑재합니다.

네트워크 세그먼트, 분산 방화벽 규칙 및 로드 밸런서를 포함한 VMware NSX 구성에 대한 책임은 사용자에게 있습니다. 또한 VMware HCX 구성 및 추가 NSX Tier-1 게이트웨이를 포함하여 EVS 환경이 배포된 후 Amazon EVS로 구현하는 모든 통합 솔루션의 구성에 대한 책임이 있습니다.

AWS 및 고객 책임에 대한 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

> **Note**
>
> Tier-0 게이트웨이와 Tier-1 게이트웨이는 Amazon EVS 환경 배포의 일부로 생성 및 구성됩니다. Amazon EVS는 현재 단일 Tier-0 게이트웨이만 지원합니다. 이러한 논리적 라우터 또는 NSX 엣지 노드 VMs을 수정하면 연결에 영향을 미칠 수 있으므로 피해야 합니다.

VMware 소프트웨어 업데이트

> **Warning**
>
> Amazon EVS 환경 배포 후 ESX 버전을 업데이트한 경우 수수료 호스트 단계에서 VCF 호스트 검증 중에 SDDC 관리자가 실패할 수 있습니다. 이 문제를 해결하는 단계는 섹션을 참조하세요the section called “SDDC Manager가 호스트 커미셔닝 중에 VCF 호스트 검증에 실패함”.

Amazon EVS에서 제공하는 VCF 버전에 대한 자세한 내용은 섹션을 참조하세요the section called “VCF 버전 및 EC2 인스턴스”. AWS 공동 책임 모델에 따라 EVS 환경에서 ESX, vCenter Server, vSAN, NSX, SDDC Manager 및 기타 통합 솔루션을 포함한 VCF 소프트웨어에 패치, 업데이트 또는 업그레이드를 적용할 책임은 사용자에게 있습니다. 배포 후 Amazon EVS에서 배포한 VCF 소프트웨어 버전을 검토하고 필요에 따라 업데이트하는 것이 좋습니다. Broadcom 지원 포털을 통해 VCF 업데이트를 받을 수 있습니다. 또한 업데이트 및 패치에 대한 정기 유지 관리 일정을 설정하고 준수하는 것이 좋습니다.

> **Note**
>
> Amazon EVS는 현재 VMware Cloud Foundation 9를 지원하지 않습니다.

> **Note**
>
> Amazon EVS는 Broadcom에서 릴리스한 VCF 및 ESX의 일부 버전을 제공하지 않습니다. 소프트웨어 상호 운용성 정보는 Broadcom 상호 운용성 매트릭스를 참조하세요. AWS EC2 인스턴스와의 전체 하드웨어 호환성은 Broadcom 호환성 가이드를 참조하세요.

특정 패치, 업데이트 또는 업그레이드는 환경에서 실행되는 워크로드에 영향을 미칠 수 있습니다. VCF 소프트웨어를 패치, 업데이트 또는 업그레이드하기 전에 VCF 수명 주기 관리 가이드를 검토하여 이러한 변경 사항이 환경에 미치는 영향을 이해하는 것이 좋습니다. 또한 프로덕션에 배포하기 전에 스테이징 환경에서 변경 사항을 테스트하는 것이 좋습니다. VCF 5.2.x 릴리스 정보를 검토하여 최신 VCF 5.2.x 업데이트를 이해할 수 있습니다.

ESX 호스트 수명 주기 및 유지 관리

호스트 상태 모니터링 및 호스트 문제 해결을 포함하여 Amazon EVS 환경 내에서 ESX 호스트 수명 주기 관리 및 유지 관리에 대한 책임은 사용자에게 있습니다. 자세한 내용은 the section called “환경 유지 관리” 단원을 참조하십시오.

AWS 는 인프라의 신뢰성, 가용성 및 성능을 보장하기 위해 기본 i4i.metal EC2 인스턴스에 대해 예약된 유지 관리를 수행합니다. 자세한 내용은 the section called “EC2 인스턴스의 AWS 예약된 유지 관리 정보” 단원을 참조하십시오.

환경에 대한 유지 관리 수행

이 섹션에서는 Amazon EVS 환경에 대한 일반적인 유지 관리 작업을 수행하는 방법을 설명합니다.

주제

- 환경의 상태 및 리소스 모니터링
- AMI 유지 관리
- Amazon EVS 호스트 유지 관리

- Amazon EVS 서브넷에 대한 사용자 지정 라우팅 테이블 구성
- Amazon EVS VLAN 서브넷 트래픽을 제어하도록 네트워크 액세스 제어 목록 구성
- 보안 암호 관리 수명 주기

환경의 상태 및 리소스 모니터링

Amazon EVS 콘솔 또는를 사용하여 Amazon EVS 환경 및 기본 AWS 리소스의 다양한 측면을 모니터링할 수 있습니다 AWS CLI.

> **Note**
>
> VMware Cloud Foundation(VCF) 구성 요소는 SDDC Manager에서 모니터링됩니다. Amazon EVS 콘솔 또는를 사용하여 VCF 구성 요소를 모니터링할 수 없습니다 AWS CLI. SDDC Manager를 사용하여 VMware Cloud Foundation(VCF) 구성 요소를 모니터링하는 방법에 대한 자세한 내용은 SDDC Manager 시작하기를 참조하세요.

환경 상태 및 리소스 보기

환경 상태는 환경에 주의가 필요한 문제가 있는지 확인하는 데 도움이 됩니다. 다음 절차에 따라 환경의 상태를 확인하고 기본 리소스를 확인합니다.

Example

Amazon EVS console

1. Amazon EVS 콘솔을 엽니다.
2. 탐색 창에서 환경을 선택합니다.
3. 환경 ID를 선택하여 환경 세부 정보 페이지를 엽니다.
4. 세부 정보에서 환경 상태를 확인합니다.

   환경이 정상이면 상태가 통과로 표시됩니다. 문제가 있는 경우 상태가 실패로 표시됩니다. 상태가 실패인 경우 네 가지 환경 상태 확인 결과를 보여주는 팝오버를 볼 수 있습니다.
   - 키 재사용 - 통과 또는 실패를 표시하여 VCF 라이선스 키가 유효한지 여부를 나타냅니다.
   - 호스트 수 - 호스트 연결 상태를 알 수 없음, 통과 또는 실패로 표시합니다.
   - 키 적용 범위 - VCF 라이선스 키가 모든 호스트를 포함하는지 여부를 나타내는 데 성공 또는 실패를 표시합니다.

- 연결성 - SDDC Manager에 대한 연결 가능성을 나타내는 데 성공 또는 실패를 표시합니다.

  환경 상태 확인 실패 문제 해결에 대한 자세한 내용은 섹션을 참조하세요문제 해결.

  환경의 리소스를 보려면

  다음 탭 중 하나를 선택합니다.
- 호스트 - 환경의 호스트를 표시합니다.
- 네트워크 및 연결 - 환경과 연결된 VPC, EVS 서브넷 및 VPC Route Server 리소스를 표시합니다.
- 관리 어플라이언스 - 환경의 VCF 관리 어플라이언스를 DNS 호스트 이름 및 관련 자격 증명과 함께 표시합니다.
- 태그 - 환경과 연결된 태그를 표시합니다.

AWS CLI

AWS CLI 를 사용하여 환경 상태 및 리소스를 확인할 수 있습니다.

모든 환경 및 상태를 나열하려면

```
aws evs list-environments
```

> **Tip**
>
> `--query` 파라미터를 사용하여 출력을 필터링합니다. 예제:

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

환경 호스트를 나열하려면

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

환경 VLANs 나열하려면

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

```
    --environment-id environment-id
```

API 작업에 대한 자세한 내용은 Amazon EVS API 참조 안내서의 다음을 참조하세요.

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

AMI 유지 관리

Amazon EVS는 사용자 지정 EVS Amazon Machine Image(AMI)를 사용하여 ESX 호스트를 배포합니다. AMI에는 Amazon EC2에서 ESX를 실행하는 데 필요한 패키지가 포함된 사용자 지정 공급업체 추가 기능이 포함되어 있습니다.

호환되지 않는 클러스터 이미지로 인한 호스트 추가 실패 문제 해결

호스트를 환경에 추가하면 호스트에 사용 가능한 최신 버전의 EVS 사용자 지정 공급업체 추가 기능이 제공됩니다. 환경에서 이전 추가 기능 버전의 호스트를 사용하는 경우 새 호스트가 클러스터 이미지와 호환되지 않는다는 오류와 함께 새 호스트 추가가 실패합니다. 이 문제를 해결하는 자세한 단계는 섹션을 참조하세요the section called “호환되지 않는 클러스터 이미지로 인한 호스트 실패 추가”.

Amazon EVS 호스트 유지 관리

Amazon EVS는 자체 관리형 서비스이므로 호스트에서 실행되는 VMware Cloud Foundation(VCF) 소프트웨어의 유지 관리, 호스트 상태 모니터링, 호스트 장애 발생 시 호스트 교체를 포함한 호스트 문제 해결은 사용자의 책임입니다. VMware Cloud Foundation(VCF)에서 ESX 호스트를 관리하는 방법에 대한 자세한 내용은 VMware Cloud Foundation 설명서의 호스트 관리를 참조하세요.

기본 EC2 인스턴스의 상태 확인

Amazon EC2는 실행 중인 모든 EC2 인스턴스에서 자동 확인을 수행하여 하드웨어 및 소프트웨어 문제를 식별합니다. EC2 콘솔 또는에서 이러한 상태 확인의 결과를 보고 구체적이고 감지 가능한 문제를 AWS CLI 식별할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 인스턴스에 대한 상태 확인 보기 및 명령줄 참조의 describe-instance-status를 참조하세요. Amazon EC2 AWS CLI

CloudWatch 경보를 생성하여 특정 인스턴스에서 상태 확인에 실패할 경우 경고할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 상태 확인에 실패한 Amazon EC2 인스턴스에 대한 CloudWatch 경보 생성을 참조하세요. Amazon EC2

EC2 인스턴스의 AWS 예약된 유지 관리 정보

AWS 는 신뢰성, 가용성 및 성능을 보장하기 위해 기본 EC2 인스턴스에 대해 예약된 유지 관리를 수행합니다. EC2 베어 메탈 인스턴스에는 다른 EC2 인스턴스와 동일한 유형의 예약된 이벤트가 적용됩니다.는 기본 하드웨어 문제 또는 예약된 유지 관리로 인해 인스턴스를 재부팅, 중지 및 사용 중지하도록 이벤트를 예약할 AWS 수 있습니다. 이러한 이벤트들은 자주 발생하지 않습니다. 자세한 내용은 Amazon EC2 사용 설명서의 예약된 이벤트 유형을 참조하세요.

> **Note**
>
> 예약된 재부팅 이벤트 전에 vSphere Client에서 호스트를 유지 관리 모드로 전환해야 합니다.

인스턴스 중 하나가 예약된 이벤트의 영향을 받는 경우는 사용자와 연결된 이메일 주소를 사용하여 이메일로 미리 AWS 알립니다 AWS 계정. AWS 또한는 Amazon EventBridge를 사용하여 모니터링하고 관리할 수 있는 AWS 상태 이벤트를 전송합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EventBridge를 사용한 AWS 상태 이벤트 모니터링 및 Amazon EC2 인스턴스에 대한 예약된 이벤트를 참조하세요. Amazon EC2 Amazon EC2

언제든지 이벤트를 다시 예약하여 자신에게 적합한 특정 날짜 및 시간에 이벤트가 발생하도록 할 수 있습니다. 이 이벤트는 이벤트 기한까지 다시 예약될 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 EC2 인스턴스에 예약된 이벤트 다시 예약을 참조하세요. Amazon EC2

EC2 온디맨드 용량 예약 사용

EC2 온디맨드 용량 예약을 사용하여 유지 관리 기간 동안 클러스터에 충분한 용량이 있는지 확인할 수 있습니다. 언제든지 특정 가용 영역에서 용량을 예약할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 EC2 온디맨드 용량 예약을 사용하여 컴퓨팅 용량 예약을 참조하세요. Amazon EC2

용량 예약을 생성하는 단계는 Amazon EC2 사용 설명서의 용량 예약 생성을 참조하세요.

> **Note**
>
> EC2 온디맨드 용량 예약 또는 EC2 전용 호스트를 사용하는 경우 미션 크리티컬 워크로드를 위한 예비 호스트를 유지하는 것이 좋습니다. 용량 예약을 통해 지정된 가용 영역에서 특정 양의 EC2 인스턴스 용량에 액세스할 수 있지만 예비 호스트를 보유하면 미션 크리티컬 워크로드에 중요한 추가 중복 계층이 제공됩니다. 전용 호스트의 경우 예비 호스트를 사용하면 기본 호스트에 유지 관리가 필요하거나 문제가 발생하더라도 미션 크리티컬 워크로드의 환경을 유지할 수 있습니다.

AWS 예약된 이벤트 `system-maintenance` 및 `instance-retirement` 이벤트 준비

AWS 는 네트워크 유지 관리와 전원 유지 관리라는 두 가지 유형의 `system-maintenance` 이벤트를 예약합니다.

- 네트워크 유지 관리 시에는 예약된 인스턴스의 네트워크 연결이 잠시 동안 끊어집니다. 유지 관리가 완료되면 인스턴스의 네트워크 연결이 평소처럼 복구됩니다.
- 전력 유지 관리 시에는 예약된 인스턴스가 잠시 동안 오프라인 상태로 전환되었다가 재부팅됩니다. EC2 베어 메탈 인스턴스에서 재부팅을 수행하면 인스턴스 스토어 볼륨 데이터가 보존되지 않습니다.

AWS 는 EC2 인스턴스를 호스팅하는 기본 하드웨어의 성능 저하가 감지되면 EC2 `instance-retirement` 이벤트를 예약합니다.

`system-maintenance` 및 `instance-retirement` 이벤트를 해결하려면 유지 관리 이벤트가 발생하기 전에 Amazon EVS 콘솔 또는 AWS CLI 및 SDDC Manager를 사용하여 장애가 발생한 호스트를 새 호스트로 바꿉니다. 유지 관리 이벤트가 발생할 때까지 기다렸다가 EC2 인스턴스를 재부팅해야 하는 경우 인스턴스 스토어 볼륨에 저장된 vSAN 데이터가 손실됩니다. 자세한 단계는 the section called “Amazon EVS 호스트 교체” 섹션을 참조하세요.

> **Important**
>
> EC2 콘솔은 중지, 시작 및 종료를 포함하여 Amazon EVS 호스트의 상태를 관리하는 데 사용해서는 안 됩니다. Amazon EVS가 배포하는 EC2 인스턴스를 시작, 중지 또는 종료하지 마십시오. 이 작업을 수행하면 vSAN 데이터가 손실됩니다.

Amazon EVS 호스트 교체

다음 절차에 따라 Amazon EVS 호스트를 교체합니다.

> **Warning**
>
> Amazon EVS 호스트는 사용자 지정 공급업체 추가 기능을 사용하여 중요한 호스트 기능을 제공합니다. 환경에 호스트를 추가하면 사용 가능한 최신 버전의 Amazon EVS 사용자 지정 추가 기능이 제공됩니다. 환경에서 이전 추가 기능 버전의 호스트를 사용하는 경우 vSphere 클러스터에 호스트를 추가하면 클러스터 이미지 수정이 실패합니다. 이 문제를 해결하는 단계는 섹션

을 참조하세요the section called “호환되지 않는 클러스터 이미지로 인한 호스트 추가 실패 문제 해결”.

Warning

배포 후 ESX 버전을 업데이트한 경우 수수료 호스트 단계에서 VCF 호스트 검증 중에 SDDC 관리자가 실패할 수 있습니다. 이 문제를 해결하는 단계는 섹션을 참조하세요the section called “SDDC Manager가 호스트 커미셔닝 중에 VCF 호스트 검증에 실패함”.

Note

호스트가 성공적으로 생성되도록 EVS 환경 할당량당 Amazon EVS 호스트 수가 올바르게 설정되어 있는지 확인합니다. 이 할당량 값이 단일 Amazon EVS 환경 내에서 프로비저닝하려는 호스트 수보다 작으면 호스트 생성이 실패합니다. 호스트 교체가 필요한 유지 관리 작업에 대해 할당량 증가를 요청해야 할 수 있습니다. 자세한 내용은 Service Quotas 단원을 참조하십시오.

Example

Amazon EVS console and SDDC Managuer UI

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 창에서 환경을 선택합니다.
3. 교체할 호스트가 포함된 환경을 선택합니다.
4. 호스트 탭을 선택합니다.
5. [호스트 생성(Create host)]을 선택합니다.
6. 호스트 세부 정보를 지정하고 호스트 생성을 선택합니다.
7. 완료를 확인하려면 호스트 상태가 생성됨으로 변경되었는지 확인합니다.
8. AWS Secrets Manager에서 ESX 루트 암호의 자격 증명을 검색합니다. 보안 암호 검색에 대한 자세한 내용은 AWS Secrets Manager 사용 설명서의 Secrets Manager에서 보안 암호 가져오기를 참조하세요 AWS .
9. SDDC 관리자로 이동합니다.

10. 이전 단계에서 검색한 ESX 루트 자격 증명을 사용하여 SDDC Manager에서 새 호스트를 커미셔닝합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Commission Hosts를 참조하세요.
11. 클러스터에 새 호스트를 추가합니다. 자세한 내용은 vSphere 설명서의 Quickstart 워크플로를 사용하여 vSphere 클러스터에 ESX 호스트를 추가하는 방법을 참조하세요. vSphere
12. SDDC Manager에서 제거하려는 SDDC Manager의 이전 호스트를 폐기합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 호스트 폐기를 참조하세요.
13. Amazon EVS 콘솔로 돌아갑니다.
14. 호스트 탭에서 실패한 호스트를 선택하고 삭제 > 호스트 삭제를 선택합니다.

AWS CLI and SDDC Manager UI

1. 새 터미널 세션을 엽니다.
2. 새 호스트를 생성합니다. 참조는 아래 예제 명령을 참조하세요.

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
        "instanceType": "i4i.metal" \
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. AWS Secrets Manager에서 ESX 루트 암호의 자격 증명을 검색합니다. 보안 암호 검색에 대한 자세한 내용은 AWS Secrets Manager 사용 설명서의 Secrets Manager에서 보안 암호 가져오기를 참조하세요 AWS .
4. SDDC 관리자로 이동합니다.
5. 이전 단계에서 검색한 ESX 루트 자격 증명을 사용하여 SDDC Manager에서 새 호스트를 커미셔닝합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Commission Hosts를 참조하세요.
6. 손상된 호스트가 포함된 클러스터에 새 호스트를 추가합니다.
7. SDDC Manager에서 손상된 호스트를 폐기합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Decommission Hosts를 참조하세요.
8. 터미널로 돌아갑니다.
9. 실패한 호스트를 삭제합니다. 참조는 아래 예제 명령을 참조하세요.

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

문제 해결

문제 해결 팁은 문제 해결 섹션을 참조하세요. 문제 해결 지침을 검토한 후에도 문제가 계속 발생하면 AWS Support에 문의하여 추가 지원을 받으세요.

Amazon EVS 서브넷에 대한 사용자 지정 라우팅 테이블 구성

Amazon EVS는 Amazon EVS 환경이 생성된 후에만 사용자 지정 라우팅 테이블 사용을 지원합니다. 환경 생성을 성공적으로 활성화하려면 DNS 및 온프레미스 시스템과 같은 종속 서비스로의 트래픽을 허용하도록 기본 라우팅 테이블을 구성해야 합니다. 이는 Amazon EVS VLAN 서브넷이 환경 배포 중에 VPC의 기본 라우팅 테이블에 암시적으로 연결되기 때문입니다.

환경이 배포된 후에는 각 Amazon EVS VLAN 서브넷을 VPC의 라우팅 테이블과 명시적으로 연결해야 합니다. VLAN 서브넷이 VPC 라우팅 테이블과 명시적으로 연결되지 않으면 NSX 연결이 실패합니다. 서브넷을 사용자 지정 라우팅 테이블과 명시적으로 연결하는 것이 좋습니다. 사용자 지정 라우팅 테이블은 VPC 내의 네트워크 트래픽 라우팅을 보다 세밀하게 제어하여 특정 서브넷 또는 게이트웨이에 대한 맞춤형 라우팅 규칙을 허용합니다. 사용자 지정 라우팅 테이블 생성에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC에 대한 라우팅 테이블 생성을 참조하세요.

Amazon EVS VLAN 서브넷 트래픽을 제어하도록 네트워크 액세스 제어 목록 구성

네트워크 액세스 제어 목록(ACL)은 서브넷 수준에서 특정 인바운드 또는 아웃바운드 트래픽을 허용하거나 거부합니다. 네트워크 ACLs 사용하여 Amazon EVS VLAN 서브넷의 인바운드 및 아웃바운드 트래픽을 제어할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC용 네트워크 ACL 생성을 참조하세요.

> **Important**
>
> EC2 보안 그룹은 Amazon EVS VLAN 서브넷에 연결된 탄력적 네트워크 인터페이스에서 작동하지 않습니다. Amazon EVS VLAN 서브넷과 주고받는 트래픽을 제어하려면 네트워크 액세스 제어 목록을 사용해야 합니다.

Warning

Amazon EVS는 VCF 배포에 대한 액세스 권한이 필요합니다. Amazon EVS가 다음과 통신할 수 있도록 보안 그룹 및 네트워크 액세스 제어 목록(ACLs)을 구성해야 합니다.

- TCP/UDP 포트 53을 통한 DNS 서버.
- HTTPS 및 SSH를 통한 호스트 관리 VLAN 서브넷입니다.
- HTTPS 및 SSH를 통한 VM VLAN 서브넷 관리.

보안 그룹 및 네트워크 ACLs이 액세스를 허용하지 않으면 Amazon EVS 환경 배포가 실패하고 기존 환경의 규정 준수 상태가 저하될 수 있습니다.

보안 암호 관리 수명 주기

Amazon EVS는 AWS Secrets Manager를 사용하여 초기 환경 배포 시 계정에 암호를 생성, 암호화 및 저장합니다. 이러한 보안 암호에는 vCenter Server, NSX 및 SDDC Manager와 같은 VCF 관리 어플라이언스를 설치하고 액세스하는 데 필요한 VCF 보안 인증 정보와 ESX 호스트 루트 암호가 포함됩니다. 또한 Amazon EVS는 EVS 환경이 삭제될 때 사용자를 대신하여 관리형 보안 암호를 삭제합니다.

보안 암호 교체를 포함하여 보안 암호 수명 주기 관리에 대한 책임은 사용자에게 있습니다. Amazon EVS는 시크릿의 관리형 교체를 제공하지 않습니다. 보안 암호가 오래 지속되지 않도록 설정된 교체 기간에 보안 암호를 정기적으로 교체하는 것이 좋습니다. 자세한 내용은 AWS Secrets Manager 사용 설명서의 교체 일정을 참조하세요.

Amazon EVS 호스트 생성

Amazon EVS 환경을 배포한 후 호스트를 추가하여 용량과 워크로드 복원력을 높일 수 있습니다. Amazon EVS는 환경당 4~16개의 호스트를 지원합니다. 이 작업은 Amazon EVS 환경이 배포된 후에만 사용할 수 있습니다.

Note

SDDC Manager 사용자 인터페이스 내에서 호스트를 할당하고 커미셔닝해야 합니다.

Amazon EVS 호스트를 생성하려면

다음 단계에 따라 Amazon EVS 호스트를 생성합니다.

> **Warning**
>
> Amazon EVS 호스트는 사용자 지정 공급업체 추가 기능을 사용하여 중요한 호스트 기능을 제공합니다. 환경에 호스트를 추가하면 사용 가능한 최신 버전의 Amazon EVS 사용자 지정 추가 기능이 제공됩니다. 환경에서 이전 추가 기능 버전의 호스트를 사용하는 경우 vSphere 클러스터에 호스트를 추가하면 클러스터 이미지 수정이 실패합니다. 이 문제를 해결하는 단계는 섹션을 참조하세요the section called “호환되지 않는 클러스터 이미지로 인한 호스트 추가 실패 문제 해결”.

> **Warning**
>
> Amazon EVS 환경 배포 후 ESX 버전을 업데이트한 경우 커미션 호스트 단계에서 VCF 호스트 검증 중에 SDDC 관리자가 실패할 수 있습니다. 이 문제를 해결하는 단계는 섹션을 참조하세요the section called “SDDC Manager가 호스트 커미셔닝 중에 VCF 호스트 검증에 실패함”.

> **Note**
>
> 호스트가 성공적으로 생성되도록 EVS 환경 할당량당 Amazon EVS 호스트 수가 올바르게 설정되어 있는지 확인합니다. 이 할당량 값이 단일 Amazon EVS 환경 내에서 프로비저닝하려는 호스트 수보다 작으면 호스트 생성이 실패합니다. 할당량을 늘리려면 할당량 증가를 요청할 수 있습니다. 자세한 내용은 Service Quotas 단원을 참조하십시오.

> **Note**
>
> 환경에 호스트를 추가할 때 ESX 버전을 지정하지 않으면 Amazon EVS는 환경의 VCF 버전과 연결된 기본 ESX 버전을 자동으로 사용합니다. 자세한 정보는 the section called “VCF 버전 및 EC2 인스턴스”을 참조하세요.

> **Important**
>
> ESX 호스트를 추가할 때 대상 vSphere 클러스터와 일치하는 ESX 버전을 선택합니다. 동일한 버전을 사용할 수 없는 경우 이전 버전을 배포하고 vSphere Lifecycle Manager를 사용하여 업

그레이드합니다. 자세한 내용은 the section called “SDDC Manager가 호스트 커미셔닝 중에 VCF 호스트 검증에 실패함” 단원을 참조하십시오. 업그레이드를 수행하려면 호스트를 재부팅하고 호스트를 커미셔닝하는 데 걸리는 시간을 늘려야 할 수 있습니다.
vSphere 클러스터 이미지 ESX 버전보다 최신 버전인 호스트는 다운그레이드할 수 없습니다. 호스트를 삭제하고 올바른 ESX 버전으로 다시 생성해야 합니다.

Example

Amazon EVS console and SDDC Managuer UI

1. Amazon EVS 콘솔로 이동합니다.
2. 탐색 창에서 환경을 선택합니다.
3. 호스트를 생성할 환경을 선택합니다.
4. 호스트 탭을 선택합니다.
5. [호스트 생성(Create host)]을 선택합니다.
6. 호스트 세부 정보를 지정하고 호스트 생성을 선택합니다.
7. 완료를 확인하려면 호스트 상태가 생성됨으로 변경되었는지 확인합니다.
8. SDDC 관리자로 이동합니다.
9. SDDC Manager에서 새 호스트를 커미셔닝합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Commission Hosts를 참조하세요.
10. SDDC Manager를 사용하여 클러스터에 새 호스트를 추가합니다. 자세한 내용은 vSphere 설명서의 Quickstart 워크플로를 사용하여 vSphere 클러스터에 ESX 호스트를 추가하는 방법을 참조하세요. vSphere

AWS CLI and SDDC Manager UI

1. 새 터미널 세션을 엽니다.
2. 새 호스트를 생성합니다. 참조는 아래 예제 명령을 참조하세요.

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
        "instanceType": "i4i.metal",\
```

```
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. SDDC 관리자로 이동합니다.
4. SDDC Manager에서 새 호스트를 커미셔닝합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Commission Hosts를 참조하세요.
5. SDDC Manager를 사용하여 클러스터에 새 호스트를 추가합니다. 자세한 내용은 vSphere 설명서의 Quickstart 워크플로를 사용하여 vSphere 클러스터에 ESX 호스트를 추가하는 방법을 참조하세요. vSphere

Amazon EVS 호스트 삭제

호스트가 더 이상 필요하지 않은 경우 환경에서 Amazon EVS 호스트를 삭제할 수 있습니다. Amazon EVS를 사용하려면 환경에 최소 4개의 호스트가 있어야 합니다. Amazon EVS는 호스트가 4개 미만인 환경을 지원하지 않습니다.

> **Warning**
>
> 폐기하지 않고 호스트를 삭제하면 vCenter 및 SDDC Manager에 오래된 데이터가 남아 정리를 위해 추가 노력이 필요할 수 있습니다. Amazon EVS 콘솔 또는 API에서 호스트를 삭제하기 전에 호스트가 폐기되었는지 확인합니다.

> **Warning**
>
> 항상 Amazon EVS 콘솔 또는 API를 사용하여 Amazon EVS 호스트를 제거합니다. EC2 콘솔에서 호스트를 삭제하면 환경이 일관되지 않은 상태로 유지될 수 있습니다.

Amazon EVS 호스트를 삭제하려면

다음 단계에 따라 Amazon EVS 호스트를 삭제합니다.

Example

SDDC Managuer UI and Amazon EVS console

1. SDDC 관리자로 이동합니다.

2. SDDC Manager에서 클러스터를 제거합니다.
3. SDDC Manager에서 호스트를 폐기합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Decommission Hosts를 참조하세요.
4. Amazon EVS 콘솔로 이동합니다.
5. 탐색 창에서 환경을 선택합니다.
6. 삭제할 호스트가 포함된 환경을 선택합니다.
7. 호스트 탭을 선택합니다.
8. 호스트 삭제를 선택합니다.
9. 호스트를 선택하고 호스트 탭에서 삭제를 선택합니다. 삭제하려는 각 호스트에 대해이 단계를 반복합니다.

SDDC Manager UI and AWS CLI

1. SDDC 관리자로 이동합니다.
2. SDDC Manager에서 클러스터를 제거합니다.
3. SDDC Manager에서 호스트를 폐기합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Decommission Hosts를 참조하세요.
4. 새 터미널 세션을 엽니다.
5. 호스트를 삭제합니다. 참조는 아래 예제 명령을 참조하세요.

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

Amazon Elastic VMware Service의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 서비스 에서 실행되는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Amazon Elastic VMware Service(Amazon EVS)에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 AWS 서비스 준수 프로그램 제공 범위의 섹션을 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 AWS 서비스 사용하는에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon EVS를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 보안 및 규정 준수 목표에 맞게 Amazon EVS를 구성하는 방법을 보여줍니다. 또한 Amazon EVS 리소스를 모니터링하고 보호하는 데 도움이 AWS 서비스 되는 다른를 사용하는 방법을 알아봅니다.

내용

Amazon EVS의 데이터 보호

AWS 공동 책임 모델은 Amazon Elastic VMware Service의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. VMware Cloud Foundation(VCF) 구성 요소를 포함하여이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지할 책임은 사용자에게 있습니다. 또한 사용하는의 보안 구성 및 관리 작업에 대한 책임이 AWS 서비스 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 AWS 계정 증명을 보호하고 AWS IAM Identity Center 또는를 사용하여 개별 사용자를 설정하는 것이 좋습니다 AWS Identity and Access Management. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.

> **Note**
>
> Amazon EVS는 VCF 환경 내 활동과 같은 비AWS 구성 요소에 대한 사용자 활동을 로깅하지 않습니다. 이러한 활동은 vSphere 및 NSX Manager와 같은 다양한 VMware 콘솔에 기록됩니다. 중앙 집중식 VCF 로깅을 원하는 경우 VMware Aria Operations 또는 VMware Tanzu Observability와 같은 VCF 모니터링 솔루션을 구성하여이 결과를 얻을 수 있습니다. 자세한 내용은 VCF 설명서의 VMware Cloud Foundation with VMware Tanzu 및 VMware Aria Suite Lifecyle in VMware Cloud Foundation 모드를 참조하세요.

- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- 와 같은 고급 관리형 보안 서비스를 사용하면 Amazon Macie에 저장된 민감한 데이터를 검색하고 보호할 수 있습니다 Amazon S3.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 민감한 식별 정보를 태그 또는 이름 필드와 같은 자유 형식 텍스트 필드에 절대 입력하지 않는 것이 좋습니다. 여기에는 Amazon EVS 또는 기타에서 콘솔 AWS CLI, API 또는 AWS SDKs를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

Amazon EVS는 인스턴스 스토어 볼륨에 저장된 데이터에 대해 기본적으로 투명한 AES-256 암호화를 사용하는 i4i.metal EC2 인스턴스를 배포합니다. AES-256 Amazon EVS는 현재 EBS 부팅 볼륨 암호화를 지원하지 않습니다.

Amazon EBS 부팅 볼륨

Amazon EVS i4i.metal 인스턴스는 Amazon EBS 부팅 볼륨을 사용합니다. 부팅 볼륨에는 EC2 인스턴스를 부팅하고 실행하는 데 필요한 운영 체제 및 기타 파일이 포함되어 있습니다. 부팅 볼륨은 암호화되지 않습니다. Amazon EVS는 현재 부팅 볼륨 암호화를 지원하지 않습니다. 부팅 볼륨에는 가상 머신의 사용자 데이터가 포함되지 않습니다.

인스턴스 저장소 볼륨

Amazon EVS i4i.metal EC2 인스턴스는 인스턴스 하드웨어의 일부인 로컬 NVMe SSD 스토리지와 함께 제공됩니다. Amazon EVS는 NVMe 인스턴스 스토어 볼륨을 vSAN 데이터 스토어의 디스크로 사용합니다. vSAN 데이터 스토어는 Amazon EVS 환경을 배포한 후 관리 및 워크로드 가상 머신을 보관합니다.

인스턴스의 하드웨어 모듈에 구현된 XTS-AES-256 암호를 사용하여 NVMe 인스턴스 저장소 볼륨의 데이터를 암호화합니다. 로컬로 연결된 NVMe 스토리지 디바이스에 기록된 데이터를 암호화하는 데 사용되는 키는 고객별 및 볼륨별입니다. 자세한 내용은 Amazon EC2 사용 설명서의 저장된 암호화를 참조하세요.

Amazon EVS 환경을 배포한 후 vSAN data-at-rest 스토어에 저장된 모든 데이터, 개별 가상 머신(VMs) 또는 VMs. 이 세분화된 제어는 일부 VMs 필요하지만 다른 VM에는 필요하지 않거나 VM 내의 특정 디스크 또는 파일을 암호화해야 할 때 유용할 수 있습니다. 자세한 내용은 VMware vSAN 설명서의 vSAN Data-At-Rest Encryption 작동 방식을 참조하세요.

전송 중 암호화

Amazon EVS는 기본적으로 전송 중 트래픽을 암호화하지 않습니다. Amazon EVS를 통과하는 전송 중 데이터를 암호화하려면 TLS(전송 계층 보안)와 같은 프로토콜을 사용하여 애플리케이션 계층 암호화를 사용할 수 있습니다. EC2 인스턴스 트래픽 암호화에 대한 자세한 내용은 Amazon EC2 사용 설명서의 전송 중 암호화를 참조하세요.

> **Note**
>
> Nitro 네트워크 암호화는 Amazon EVS가 배포하는 EC2 인스턴스에는 적용되지 않습니다. Amazon EVS는 호스트 간 트래픽의 전송 중 암호화를 지원하지 않습니다.

온프레미스 연결을 위한 전송 중 암호화 옵션

온프레미스 데이터 센터와 Amazon EVS 간의 트래픽을 암호화하기 위해 AWS Direct Connect 및 AWS Site-To-Site VPN 사용을 AWS Transit Gateway와 결합할 수 있습니다. 이 조합은 IPsec으로 암호화된 프라이빗 연결을 제공하여 네트워크 비용을 줄이고, 대역폭 처리량을 늘리고, 인터넷 기반 VPN 연결보다 더 일관된 네트워크 환경을 제공합니다. 자세한 내용은 AWS Direct Connect를 사용하는 프라이빗 IP AWS Site-to-Site VPN을 참조하세요.

> **Note**
>
> Amazon EVS는 AWS Direct Connect 프라이빗 가상 인터페이스(VIF) 또는 언더레이 VPC로 직접 종료되는 AWS Site-to-Site VPN 연결을 통한 연결을 지원하지 않습니다. Amazon EVS는 NSX Edge Tier-0 또는 Tier-1 게이트웨이에서 IPSec VPN 종료를 지원합니다. 자세한 내용은 VMware NSX 설명서의 NSX IPSec VPN 서비스 추가를 참조하세요.

MAC 보안(MACsec)은 데이터 기밀성, 데이터 무결성 및 데이터 원본 인증을 제공하는 IEEE 표준입니다. MACsec을 지원하는 AWS Direct Connect 연결을 사용하여 회사 데이터 센터에서 AWS Direct Connect 위치로 데이터를 암호화할 수 있습니다. 자세한 내용은 AWS Direct Connect 사용 설명서의 Direct Connect의 MAC 보안을 참조하세요. AWS

VMware 네트워크 데이터에 대한 전송 중 암호화

Amazon EVS 환경을 배포한 후에는 VMware VCF 계층에서 전송 중 데이터 암호화를 적용하는 여러 옵션이 있습니다.

- VMware vDefend 분산 방화벽 - 세분화된 네트워크 세분화를 구현하고 가상 머신 간에 TLS/SSL 암호화를 적용할 수 있습니다. 자세한 내용은 VMware VCF 설명서의 사용자 인터페이스를 사용하여 분산 방화벽의 보안 설정 구성을 참조하세요.
- vSAN data-in-transit 암호화 - vSAN 클러스터의 호스트 간에 모든 데이터와 메타데이터를 암호화하는 데 사용할 수 있습니다. 자세한 내용은 VMware vSAN 설명서의 vSAN Data-In-Transit 암호화를 참조하세요.

- 암호화된 vSphere vMotion - vSphere vMotion으로 전송되는 데이터의 기밀성, 무결성 및 신뢰성을 보호합니다. 자세한 내용은 vSphere 설명서의 암호화된 vSphere vMotion이란 무엇입니까?를 참조하세요. vSphere

키 및 보안 암호 관리

Amazon EVS 환경 배포 중에 Amazon EVS는 AWS Secrets Manager를 사용하여 VMware VCF 관리 어플라이언스를 설치하고 액세스하는 데 필요한 VCF 자격 증명과 ESX 루트 암호가 포함된 보안 암호를 생성, 암호화 및 저장합니다. 또한 Amazon EVS는 EVS 환경이 삭제될 때 사용자를 대신하여 관리형 보안 암호를 삭제합니다. 자세한 내용은 Secrets Manager 사용 설명서의 Secrets Manager 보안 암호의 내용을 참조하세요 AWS .

Secrets Manager는 AWS KMS 키 및 데이터 키와 함께 봉투 암호화를 사용하여 각 보안 암호 값을 보호합니다. 다르게 지정하지 않는 한 Secrets Manager의 기본 AWS 관리형 키가 사용됩니다. 또는 환경 생성 중에 고객 관리형 키를 지정하여 보안 암호를 암호화할 수 있습니다. 자세한 내용은 Secrets Manager 사용 설명서의 AWS Secrets Manager의 보안 암호 암호화 및 복호화를 참조하세요. AWS

> **Note**
>
> 고객 관리형 키에는 추가 사용 요금이 부과됩니다. 기본 AWS 관리형 키는 무료로 제공됩니다. 자세한 내용은 AWS Secrets Manager 사용 설명서의 요금을 참조하세요.

Amazon EVS는 배포 후 AWS Secrets Manager와 VCF 소프트웨어 간에 자격 증명을 동기화하지 않습니다. 사용자는 VCF 암호 만료 및 VCF 소프트웨어에 대한 액세스 손실을 방지하기 위해 Amazon EVS 환경과 연결된 보안 암호가 SDDC Manager의 자격 증명과 동기화되도록 할 책임이 있습니다.

Amazon EVS는 사용자를 대신하여 보안 암호를 교체하지 않습니다. 환경과 연결된 보안 암호를 교체하는 것은 사용자의 책임입니다. 환경이 생성되는 즉시 보안 암호를 교체하고 교체 일정을 구현하여 보안 암호를 정기적으로 업데이트하는 것이 좋습니다. AWS Secrets Manager 보안 암호 교체에 대한 자세한 내용은 Secrets Manager 사용 설명서의 Lambda 함수에 의한 교체를 참조하세요. AWS VCF 암호 관리에 대한 자세한 내용은 VMware Cloud Foundation 설명서의 암호 관리를 참조하세요.

> **Important**
>
> Amazon EVS는 배포 후 AWS Secrets Manager와 VCF 소프트웨어 간에 자격 증명을 동기화하지 않습니다. 배포 후 AWS Secrets Manager를 사용하는 경우 VCF 암호 만료 문제를 방지하려면 AWS Secrets Manager와 SDDC Manager 간의 자격 증명을 동기화된 상태로 유지해야

합니다. SDDC Manager 자격 증명을 최신 상태로 유지하지 않으면 VCF 소프트웨어에 대한 액세스 권한이 손실될 수 있습니다.

Note

Amazon EVS는 보안 암호의 관리형 교체를 제공하지 않습니다.

Note

AWS Secrets Manager 보안 암호 교체를 위해 Lambda 함수를 사용하는 데는 비용이 발생합니다. 자세한 내용은 AWS Secrets Manager 사용 설명서의 요금을 참조하세요.

인터네트워크 트래픽 개인 정보

Amazon EVS는 고객 제공 VPC를 사용하여 Amazon EVS 환경의 리소스 간에 경계를 생성하고 리소스, 온프레미스 네트워크 및 인터넷 간의 트래픽을 제어합니다. Amazon VPC 보안에 대한 자세한 내용은 Amazon VPC 사용 설명서의 에서 인터넷 작업 트래픽 개인 정보 보호 보장 Amazon VPC을 참조하세요.

기본적으로 Amazon EVS는 환경 생성 중에 직접 인터넷 액세스를 거부하는 프라이빗 VLAN 서브넷을 생성합니다. VPC에 다른 보안 계층을 추가하려면 인터넷 연결을 추가로 제한하는 규칙을 사용하여 VPC에 대한 사용자 지정 네트워크 액세스 제어 목록을 생성할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC용 네트워크 ACL 생성을 참조하세요.

Important

EC2 보안 그룹은 Amazon EVS VLAN 서브넷에 연결된 탄력적 네트워크 인터페이스에서 작동하지 않습니다. Amazon EVS VLAN 서브넷과 주고받는 트래픽을 제어하려면 네트워크 액세스 제어 목록을 사용해야 합니다.

NSX 관리자인 경우 네트워크 트래픽을 보호하도록 다음 NSX 기능을 구성할 수 있습니다.

- VMware vDefend Gateway 방화벽 - 네트워크 경계를 보호하여 외부 위협(북남 트래픽)으로부터 보호합니다. 자세한 내용은 VMware NSX 설명서의 게이트웨이 방화벽 정책 및 규칙 추가를 참조하세요.
- VMware vDefend 분산 방화벽 - 내부 네트워크(동서 트래픽) 내에서 발생하는 공격으로부터 보호합니다. 자세한 내용은 VMware NSX 설명서의 분산 방화벽 추가를 참조하세요.

Amazon Elastic VMware Service의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 AWS 서비스 도와주는 입니다. IAM 관리자는 Amazon Elastic VMware Service(Amazon EVS) 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는 사용자를 제어합니다. IAM 는 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 Amazon EVS에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Amazon EVS 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Amazon EVS 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다.

Amazon EVS의 기능에 액세스할 수 없는 경우 섹션을 참조하세요the section called “Amazon EVS 자격 증명 및 액세스 문제 해결”.

서비스 관리자 - 회사에서 Amazon EVS 리소스를 책임지고 있는 경우 Amazon EVS에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Amazon EVS 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여의 기본 개념을 이해합니다 IAM. 회사가 Amazon EVS IAM에서를 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요the section called “Amazon EVS의 작동 방식 IAM”.

IAM 관리자 - IAM 관리자인 경우 Amazon EVS에 대한 액세스를 관리하는 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. 에서 사용할 수 있는 Amazon EVS 자격 증명 기반 정책 예제를 보려면 섹션을 IAM참조하세요the section called “Amazon EVS 자격 증명 기반 정책 예제”.

ID를 통한 인증

인증은 AWS 자격 증명으로에 로그인하는 방법입니다. IAM 역할을 수임하여 AWS 계정 루트 사용자 IAM 사용자, 또는 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션 ID로 로그인하면 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 AWS 일반 참조의 서명 버전 4 서명 프로세스를 참조하세요.

사용하는 인증 방법에 상관 없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center(AWS Single Sign-On 후속) 사용 설명서의 멀티 팩터 인증 및 IAM 사용 설명서의 의 멀티 팩터 인증(MFA) 사용을 AWS 참조하세요.

AWS 계정 루트 사용자

를 처음 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하

는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 계정 관리 참조 안내서의 루트 사용자 자격 증명이 필요한 작업을 참조하세요.

페더레이션 ID

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명 액세스 시 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 IAM Identity Center(Single Sign-On 후속) 사용 설명서의 IAM Identity Center란 무엇입니까?를 참조하세요 AWS AWS .

IAM 사용자 및 그룹

IAM 사용자 는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자 사람을 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 그러나 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 IAM 사용자것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 자격 증명이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 컬렉션을 지정하는 자격 증명입니다 IAM 사용자. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합에 대한 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 IAMAdmins라는 그룹이 있고 해당 그룹에 IAM 리소스를 관리할 수 있는 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 (역할 대신) 생성 시기를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 와 비슷 IAM 사용자하지만 특정 사람과는 관련이 없습니다. IAM 역할을 전환 AWS Management Console 하여에서 역할을 일시적으로 수임할 수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 관리하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 IAM Identity Center(Single Sign-On 후속) 사용 설명서의 권한 세트를 참조하세요. AWS AWS
- 임시 IAM 사용자 권한 -는 IAM 역할을 수임하여 특정 작업에 대한 다른 권한을 일시적으로 수임할 IAM 사용자 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 교차 계정 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할이 리소스 기반 정책과 어떻게 다른지 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가에서 애플리케이션을 실행 Amazon EC2 하거나에 객체를 저장하는 것이 일반적입니다 Amazon S3. 서비스는 직접 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 보안 주체 권한 - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 정책은 보안 주체에게 권한을 부여합니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 작업을 트리거하는 작업을 수행할 수 있습니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다 IAM. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- 에서 Amazon EC2 실행되는 애플리케이션 - IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 Amazon EC2 인스턴스 내에 액세스 키를 저장하는 것보다 더 좋습니다. Amazon EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 Amazon EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 여부를 알아보려면 IAM 사용 설명서의 IAM 역할 생성 시기(사용자 대신)를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

모든 IAM 엔터티(사용자 또는 역할)는 권한 없이 시작됩니다. 기본적으로 사용자는 아무 작업도 할 수 없으며 자신의 암호를 변경할 수도 없습니다. 사용자에게 태스크를 수행할 권한을 부여하기 위해 관리자는 사용자에게 권한 정책을 연결해야 합니다. 또한 관리자는 의도한 권한을 가지고 있는 그룹에 사용자를 추가할 수 있습니다. 관리자가 그룹에 권한을 부여하면 해당 그룹의 모든 사용자에게 해당 권한이 부여됩니다.

IAM 정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

자격 증명 기반 정책

자격 증명 기반 정책은 IAM 사용자자격 증명, 역할 또는 그룹과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 Amazon S3 버킷과 같은 리소스에 연결하는 JSON 정책 문서입니다. 서비스 관리자는 이러한 정책을 사용하여 지정된 보안 주체(계정 멤버, 사용자 또는 역할)가 해당 리소스에 대해 수행할 수 있는 작업과 어떤 조건에서 수행할 수 있는지를 정의할 수 있습니다. 리소스 기반 정책은 인라인 정책입니다. 관리형 리소스 기반 정책은 없습니다.

액세스 제어 목록(ACL)

ACL(액세스 제어 목록)은 리소스에 액세스할 수 있는 권한을 가진 보안 주체(계정 멤버, 사용자 또는 역할)를 제어하는 정책의 유형입니다. ACL은 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지 않습니다. Amazon S3 AWS WAF, 및 Amazon VPC 는 ACLs. ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 참조하십시오.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책의 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 기업이 소유한 여러 AWS 계정 를 그룹화하

고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 계정 루트 사용자를 포함하여 멤버 AWS 계정의 엔터티에 대한 권한을 제한합니다. 조직 및 SCPs에 대한 자세한 내용은 조직 사용 설명서의 SCPs 작동 방식을 참조하세요. AWS

- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 자격 증명 기반 정책과 세션 정책의 교집합입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Amazon EVS의 작동 방식 IAM

IAM 를 사용하여 Amazon EVS에 대한 액세스를 관리하기 전에 Amazon EVS에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

IAM 기능	Amazon EVS 지원
the section called “Amazon EVS에 대한 자격 증명 기반 정책”	예
the section called “Amazon EVS 내의 리소스 기반 정책”	아니요
the section called “Amazon EVS에 대한 정책 작업”	예
the section called “Amazon EVS에 대한 정책 리소스”	부분적
the section called “Amazon EVS에 사용되는 정책 조건 키”	예

IAM 기능	Amazon EVS 지원
the section called “Amazon EVS의 액세스 제어 목록(ACLs)”	아니요
the section called “Amazon EVS를 사용한 ABAC(속성 기반 액세스 제어)”	예
the section called “Amazon EVS에서 임시 자격 증명 사용”	예
the section called “Amazon EVS에 대한 전달 액세스 세션”	예
the section called “Amazon EVS의 서비스 역할”	아니요
the section called “Amazon EVS의 서비스 연결 역할”	예

Amazon EVS 및 기타에서 AWS 서비스 작업하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS 서비스 에서 작업하는 IAM 섹션을 IAM참조하세요.

Amazon EVS에 대한 자격 증명 기반 정책

자격 증명 기반 정책 지원: 예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

자격 IAM 증명 기반 정책을 사용하면 허용되거나 거부된 작업 및 리소스와 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Amazon EVS의 자격 증명 기반 정책 예제

Amazon EVS 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요the section called “Amazon EVS 자격 증명 기반 정책 예제”.

Amazon EVS 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 교차 계정 위탁자를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.

Amazon EVS에 대한 정책 작업

작업 지원 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

자격 IAM 증명 기반 정책의 `Action` 요소는 정책에 의해 허용되거나 거부될 특정 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 이 작업은 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에서 사용됩니다.

Amazon EVS의 정책 작업은 작업 앞에 접두사를 사용합니다`evs:`. 예를 들어 Amazon EVS `CreateEnvironment` API 작업을 사용하여 환경을 생성할 수 있는 권한을 부여하려면 해당 정책에 `evs:CreateEnvironment` 작업을 포함합니다. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Amazon EVS는이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

명령문 하나에 여러 태스크를 지정하려면 다음과 같이 쉼표로 구분합니다.

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

```
      "evs:action2"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `List`라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "evs:List*"
```

Amazon EVS 작업 목록을 보려면 서비스 승인 참조의 Amazon EVS에서 정의한 작업을 참조하세요.

Amazon EVS에 대한 정책 리소스

정책 리소스 지원: 부분적

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 명령문이 모든 리소스에 적용됨을 나타냅니다.

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

Amazon EVS 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 Amazon Elastic VMware Service에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Amazon Elastic VMware Service에서 정의한 작업을 참조하세요.

일부 Amazon EVS API 작업은 여러 리소스를 지원합니다. 예를 들어 `ListEnvironments` API 작업을 호출할 때 여러 환경을 참조할 수 있습니다. 단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

예를 들어 Amazon EVS 환경 리소스의 ARN은 다음과 같습니다.

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

문my-environment-2에서 환경 my-environment-1 및를 지정하려면 다음 예제 ARNs 사용합니다.

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

특정 계정에 속하는 모든 환경을 지정하려면 와일드카드(*)를 사용합니다.

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

Amazon EVS에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 문이 적용되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 AND 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 이름 태그가 지정된 경우에만 리소스에 액세스할 수 있는 IAM 사용자 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

Amazon EVS는 자체 조건 키 세트를 정의하고 일부 전역 조건 키 사용을 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

모든 Amazon EC2 작업은 aws:RequestedRegion 및 ec2:Region 조건 키를 지원합니다. 자세한 내용은 예제: 특정 리전으로 액세스 제한을 참조하세요.

Amazon EVS 조건 키 목록을 보려면 서비스 승인 참조의 Amazon EVS에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon EVS에서 정의한 작업을 참조하세요.

Amazon EVS의 액세스 제어 목록(ACLs)

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon EVS를 사용한 ABAC(속성 기반 액세스 제어)

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

Amazon EVS 리소스에 태그를 연결하거나 Amazon EVS에 대한 요청에서 태그를 전달할 수 있습니다. 태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/<key-name>`, `aws:RequestTag/<key-name>`또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다. 조건 키에서 태그를 사용할 수 있는 작업에 대한 자세한 내용은 서비스 승인 참조의 Amazon EVS에서 정의한 작업을 참조하세요.

Amazon EVS에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름 및 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 access AWS. AWS recommds에 액세스할 수 있습니다. 자세한 내용은 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

Amazon EVS에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Amazon EVS의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

Amazon EVS의 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Amazon EVS 서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 섹션을 참조하세요the section called “서비스 연결 역할 사용”.

Amazon EVS 자격 증명 기반 정책 예제

기본적으로 IAM 사용자 및 역할에는 Amazon EVS 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 AWS API를 사용하여 작업을 수행할 수 없습니다. IAM 관리자는 사용자 및 역할에 필요한 지정된 리소스에 대해 특정 API 작업을 수행할 수 있는 권

한을 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 해당 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 편집기를 사용하여 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Amazon EVS 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- Amazon EVS 환경 생성 및 관리
- Amazon EVS 환경, 호스트 및 VLANs 가져오기 및 나열

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 Amazon EVS 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 - IAM 정책으로 권한을 설정할 때 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 적용하는 IAM 방법에 대한 자세한 내용은 IAM 사용 설명서의 의 정책 및 권한을 IAM 참조하세요.
- IAM 정책의 조건을 사용하여 액세스를 추가로 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer 를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다.는 정책 IAM 언어(JSON) 및 IAM 모범 사례를 준수하도록 신규 및 기존 정책을 IAM Access Analyzer 검증합니다.는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가

능한 권장 사항을 IAM Access Analyzer 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.

- 다중 인증(MFA) 필요 - 계정의 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 켭니다. API 작업을 직접적으로 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

Amazon EVS 콘솔 사용

Amazon EVS 콘솔에 액세스하려면 IAM 보안 주체에 최소 권한 집합이 있어야 합니다. 이러한 권한은 보안 주체가의 Amazon EVS 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 보안 인증 정보 기반 정책을 만들면 콘솔이 해당 정책이 연결된 보안 주체에 대해 의도대로 작동하지 않습니다.

IAM 보안 주체가 Amazon EVS 콘솔을 계속 사용할 수 있도록 하려면와 같이 고유한 이름으로 정책을 생성합니다`AmazonEVSAdminPolicy`. 정책을 보안 주체에게 연결하세요. 자세한 내용은 IAM 사용자 설명서의 사용자에게 권한 추가를 참조하세요.

```
{
    "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 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는가 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 IAM 사용자 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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 환경 생성 및 관리

이 예제 정책에는 Amazon EVS 환경을 생성 및 삭제하고 환경이 생성된 후 호스트를 추가 또는 삭제하는 데 필요한 권한이 포함되어 있습니다.

를 환경을 생성하려는 AWS 리전 AWS 리전 로 바꿀 수 있습니다. 계정에 이미 `AWSServiceRoleForAmazonEVS` 역할이 있는 경우 정책에서 `iam:CreateServiceLinkedRole` 작업을 제거할 수 있습니다. 계정에서 Amazon EVS 환경을 생성한 적이 있는 경우 삭제하지 않는 한 이러한 권한이 있는 역할이 이미 존재합니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeHosts",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeRouteServers",
                "ec2:DescribeRouteServerEndpoints",
                "ec2:DescribeRouteServerPeers",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "support:DescribeServices",
                "support:DescribeSupportLevel",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListServiceQuotas"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ModifyNetworkInterfaceStatement",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "ModifyNetworkInterfaceStatementForSubnetAssociation",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceAdditionalResources",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "TagOnCreateEC2Resources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateNetworkInterface",
                        "RunInstances",
                        "CreateSubnet",
                        "CreateVolume"
                    ]
                },
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "DetachNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachNetworkInterface"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithTagResource",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithoutTag",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:image/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:placement-group/*"
            ]
        },
        {
            "Sid": "TerminateInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithoutTagForExistingVPC",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "DeleteSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSubnet"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDeletion",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
             "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDetachment",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
```

```
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RouteServerAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:GetRouteServerAssociations"
            ],
            "Resource": "arn:aws:ec2:*:*:route-server/*"

        },
        {
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SecretsManagerCreateWithTag",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "SecretsManagerTagging",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true",
                    "aws:ResourceTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerOps",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DeleteSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "SecretsManagerRandomPassword",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "EVSPermissions",
            "Effect": "Allow",
            "Action": [
                "evs:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyAccessInConsole",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        },

        {
            "Sid": "KMSKeyAliasAccess",
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon EVS 환경, 호스트 및 VLANs 가져오기 및 나열

이 예제 정책에는 관리자가 us-east-2의 지정된 계정 내에서 모든 Amazon EVS 환경, 호스트 및 VLANs을 가져오고 나열하는 데 필요한 최소 권한이 포함되어 있습니다 AWS 리전.

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

```
  ]
}
```

Amazon EVS 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Amazon EVS 및 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다 IAM.

주제

- AccessDeniedException
- 내 외부의 사람이 내 Amazon EVS 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

AccessDeniedException

AWS API 작업을 호출할 `AccessDeniedException` 때를 수신하면 사용 중인 IAM 보안 주체 자격 증명에 해당 호출에 필요한 권한이 없는 것입니다.

```
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
```

이전 예제 메시지에서 사용자는 Amazon EVS `CreateEnvironment` API 작업을 호출할 권한이 없습니다. IAM 보안 주체에 Amazon EVS 관리자 권한을 제공하려면 섹션을 참조하세요the section called “Amazon EVS 자격 증명 기반 정책 예제”.

IAM에 대한 자세한 내용은 IAM 사용 설명서의 정책을 사용하여 AWS 리소스에 대한 액세스 제어를 참조하세요.

내 외부의 사람이 내 Amazon EVS 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Amazon EVS가 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요the section called “Amazon EVS의 작동 방식 IAM”.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서IAM 사용자 의 소유 AWS 계정 한 다른의에 대한 액세스 권한 제공을 참조하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- 자격 증명 연동을 통해 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부 인증 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하세요.
- 교차 계정 액세스를 위한 역할 및 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할이 리소스 기반 정책과 어떻게 다른지 참조하세요.

AWS Amazon EVS에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 AWS 관리형 정책에 정의된 권한을 AWS 업데이트하는 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonEVSServiceRolePolicy

`AmazonEVSServiceRolePolicy`를 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Amazon EVS가 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 the section called “서비스 연결 역할 사용” 단원을 참조하십시오. `iam:CreateServiceLinkedRole` 권한이 있는 IAM 보안 주체를 사용하여 환경을 생성하면이 정책이 연결된 상태에서 `AWSServiceRoleforAmazonEVS` 서비스 연결 역할이 자동으로 생성됩니다.

이 정책은 `AWSServiceRoleForAmazonEVS` 서비스 연결 역할이 사용자를 대신하여 AWS 서비스 를 호출하도록 허용합니다.

권한 세부 정보

이 정책에는 Amazon EVS가 다음 작업을 완료할 수 있도록 허용하는 다음 권한이 포함되어 있습니다.

- `ec2` - 서브넷 및 VPC를 포함한 VPCs 네트워킹 구성 요소를 검색합니다. Amazon EVS와 VPC 서브넷의 VMware Virtual Cloud Foundation(VCF) SDDC Manager 어플라이언스 간에 지속적인 연결을 설정하는 데 사용되는 탄력적 네트워크 인터페이스를 생성, 수정, 태그 지정 및 삭제합니다. 이 연결은 Amazon EVS가 VCF 배포를 배포, 관리 및 모니터링하는 데 필요합니다.
- `ec2` - EVS 호스트 삭제 요청을 할 때 Amazon EVS가 생성하는 EC2 인스턴스를 삭제합니다. EVS 호스트 삭제를 지원하는 데 필요한 경우 기본 EC2 인스턴스 종료 및 중지 보호를 비활성화할 수 있도록 EC2 인스턴스 속성을 설명하고 수정합니다.
- `ec2` - Cloud Builder 설치 및 정리를 위한 EBS 볼륨을 관리합니다. 환경을 생성하는 동안 Cloud Builder는 VCF 구성 변경을 수행하기 위해 Amazon EVS 배포 호스트 중 하나에 설치됩니다. 완료되면 Amazon EVS는 저장된 EC2 볼륨을 분리하고 삭제하여 Cloud Builder를 제거합니다.
- `ec2` - 환경 삭제를 요청하는 경우 사용자를 대신하여 EVS VLAN 서브넷을 삭제합니다.
- `secretsmanager` - 환경 생성 중에 Amazon EVS가 생성하고 AWS Secrets Manager에 저장하는 VCF 암호를 삭제합니다. Amazon EVS는 환경 생성에 실패하거나 환경 삭제를 요청하는 경우 서비스가 계정에서 생성하는 모든 보안 암호를 삭제합니다. 보안 암호 ARN을 제공하여 vCenter 커넥터를 구성할 때 AWS Secrets Manager에서 vCenter 자격 증명을 검색합니다. 권한은 Amazon EVS가 Amazon EVS vCenter 액세스`EvsAccess=true`에 대해 명시적으로 태그가 지정된 보안 암호에만 액세스할 수 있도록 리소스 태그 조건으로 범위가 지정됩니다.
- `kms` - Secrets Manager에 저장된 vCenter 보안 인증 정보가 KMS 키로 암호화될 때 보안 암호를 해독하고 KMS 키를 설명합니다. 권한의 범위는 리소스 태그 조건으로 지정되어 Amazon EVS가 vCenter 액세스에 대해 명시적으로 태그가 지정된 KMS 키에만 액세스`EvsAccess=true`하도록 합니다.
- `cloudwatch` - 할당량이 있는 Amazon EVS 리소스에 CloudWatch 대한 AWS 사용 지표를에 게시합니다.

최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 자세한 내용은 AWS 관리형 정책 참조 안내서의 AmazonEVSServiceRolePolicy를 참조하세요.

AWS 관리형 정책에 대한 Amazon EVS 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 Amazon EVS의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 문서 이력 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AmazonEVSServiceRolePolicy - 정책 업데이트	Amazon EVS는 서비스가 AWS Secrets Manager에서 vCenter 자격 증명을 검색하고 KMS 키로 암호화된 암호를 해독할 수 있도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: AmazonEVSServiceRolePolicy”를 참조하세요.	2026년 3월 23일
AmazonEVSServiceRolePolicy - 정책 업데이트	Amazon EVS는 EC2 인스턴스 관리, EBS 볼륨 작업, AWS Secrets Manager 통합을 포함한 포괄적인 리소스 관리 기능을 추가하도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: AmazonEVSServiceRolePolicy”를 참조하세요.	2025년 8월 14일
AmazonEVSServiceRolePolicy - 정책 업데이트	Amazon EVS는 서비스가 EVS VLAN 서브넷을 삭제하고 Amazon EVS 사용량 지표를 게시할 수 있도록 정책을 업데이트했습니다 CloudWatch. 자세한 내용은 the section called “AWS 관리형 정책: AmazonEVSServiceRolePolicy”를 참조하세요.	2025년 7월 14일
AmazonEVSServiceRolePolicy - 새 정책 추가	Amazon EVS는 서비스가 고객 계정의 VPC 서브넷에 연결할 수 있도록 허용하는 새 정책을 추가했습니다. 이	2025년 6월 9일

변경	설명	Date
	연결은 서비스 기능에 필요합니다. 자세한 내용은 the section called “AWS 관리형 정책: AmazonEVSServiceRolePolicy”를 참조하세요.	
Amazon EVS에서 변경 사항 추적 시작	Amazon EVS가 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2025년 6월 9일

Amazon EVS에 서비스 연결 역할 사용

Amazon Elastic VMware Service는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Amazon EVS에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Amazon EVS에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할을 사용하면 Amazon EVS를 더 쉽게 설정할 수 있습니다. Amazon EVS는 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않은 한 Amazon EVS만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 수 없기 때문에 Amazon EVS 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 참조하세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

Amazon EVS에 대한 서비스 연결 역할 권한

Amazon EVS는 라는 서비스 연결 역할을 사용합니다`AWSServiceRoleForAmazonEVS`. 이 역할을 통해 Amazon EVS는 계정의 환경을 관리할 수 있습니다. 연결된 정책은 역할이 EVS 탄력적 네트워크 인터페이스, EVS VLAN 서브넷, EVS 호스트, VPCs 및 CloudWatch 지표와 같은 리소스를 관리할 수 있도록 허용합니다.

AWSServiceRoleForAmazonEVS 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- evs.amazonaws.com

역할 권한 정책은 Amazon EVS가 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- AmazonEVSServiceRolePolicy

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Amazon EVS에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API에서 환경을 생성하면 Amazon EVS가 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 환경을 생성하면 Amazon EVS가 서비스 연결 역할을 다시 생성합니다.

Amazon EVS에 대한 서비스 연결 역할 편집

Amazon EVS에서는 AWSServiceRoleForAmazonEVS 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Amazon EVS에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할을 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할을 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다. 호스트가 있는 Amazon EVS 환경을 삭제하는 단계는 섹션을 참조하세요the section called “Amazon EVS 호스트 및 환경 삭제”.

> **Note**
>
> 리소스를 삭제하려고 할 때 Amazon EVS 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 `AWSServiceRoleForAmazonEVS` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

Amazon EVS 서비스 연결 역할에 지원되는 리전

Amazon EVS는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 일반 참조 안내서의 Amazon Elastic VMware Service 엔드포인트 및 할당량을 참조하세요.

Amazon EVS의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹을 통해 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

Amazon EVS 환경은 단일 AWS 가용 영역에서 사용할 수 있습니다. Amazon EVS Single-AZ 인프라의 고가용성을 보장하기 위해 Amazon EVS는 다음 기능을 제공합니다.

> **Note**
>
> Amazon EVS는 현재 단일 AZ 배포만 지원합니다.

- Amazon EVS는 AWS Elastic Disaster Recovery 사용을 지원하여 데이터의 백업 및 복구를 자동화합니다.
- Amazon EVS는 VCF 요구 사항당 2개의 NSX Edge 노드가 있는 Active/Standby NSX Edge 클러스터를 배포합니다. NSX Edge 노드는 고가용성을 보장하고 드물게 NSX Edge 노드에 장애가 발생하는 경우 빠른 장애 조치를 위해 여러 호스트에서 실행됩니다.

- Amazon EVS는 VCF에 필요한 4개의 ESX 호스트로 구성된 최소 환경을 배포합니다. 배포 후 추가 호스트를 추가할 수 있습니다. 이는 적절한 vSAN 쿼럼을 보장하고 유지 관리 작업 및 호스트 장애 중에 가용성을 유지하기 위한 VMware 설계 요구 사항입니다. 자세한 내용은 VMware Cloud Foundation 설명서의 vSphere Cluster Design for VMware Cloud Foundation을 참조하세요.
- Amazon EVS는 EC2 호스트에 대한 EC2 파티션 배치 그룹 또는 클러스터 배치 그룹의 사용을 지원합니다. 파티션 배치 그룹은 EC2 인스턴스를 논리적 파티션에 분산시켜 한 파티션의 인스턴스 그룹이 다른 파티션의 인스턴스 그룹과 기본 하드웨어를 공유하지 않도록 합니다. 이 전략은 대규모 분산 워크로드에서 상관관계가 있는 하드웨어 장애 가능성을 줄이는 데 도움이 됩니다. 클러스터 배치 그룹은 지연 시간을 줄이기 위해 동일한 물리적 랙 내에 EC2 인스턴스를 배치하는 데 사용됩니다. 자세한 내용은 Amazon EC2 사용 설명서의 파티션 배치 그룹을 참조하세요.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

VMware 구성 요소 복원력

Amazon EVS 고객은 가상 머신(VMs)의 고가용성과 워크로드 복원력을 보장하기 위해 Amazon EVS에서 실행되는 VMware 구성 요소를 구성할 책임이 있습니다.

Amazon EVS는 다음과 같은 VMware Cloud Foundation(VCF) 복원력 기능을 지원합니다.

- vSphere 복제 - 재해 복구 및 워크로드 마이그레이션을 위해 VMs의 호스트 기반 비동기 복제를 제공합니다. 자세한 내용은 VMware vSphere Replication 설명서의 vSphere Replication 작동 방식을 참조하세요. vSphere
- vSAN 데이터 보호 - vSAN 클러스터에 로컬로 저장된 기본 스냅샷을 사용하여 랜섬웨어 공격의 운영 실패로부터 VMs을 신속하게 복구할 수 있습니다. 자세한 내용은 vSAN 설명서의 vSAN 데이터 보호 사용을 참조하세요.
- vSphere HA - 호스트 장애 발생 시 VMs에 대한 자동 장애 조치를 제공합니다. 자세한 내용은 VCF 설명서의 vCenter Server for VMware Cloud Foundation의 고가용성 설계를 참조하세요.
- vSphere 내결함성(FT) - 장애 조치 상황에서 대체할 수 있는 동일하고 지속적으로 사용할 수 있는 다른 VM을 생성하고 유지 관리 VMs 하여 미션 크리티컬 VM에 대한 지속적인 가용성을 제공합니다. 자세한 내용은 vSphere 설명서의 내결함성 작동 방식을 참조하세요.
- vSAN FTT(Failator to Tolerate) - VM이 액세스할 수 없게 되기 전에 견딜 수 있는 호스트 장애 수를 결정하는 vSAN 설정입니다. 이는 vSAN 클러스터 내의 가상 머신에 대한 중복성 및 내결함성 수준을 정의합니다. 자세한 내용은 vSAN 설명서의 vSAN 클러스터에서 Tolerate Additional Failures with Fault Domain을 참조하세요.

다른 AWS 서비스와 함께 Amazon EVS 사용

Amazon EVS는 다른와 통합되어 추가 솔루션을 AWS 서비스 제공합니다. 이 주제에서는 Amazon EVS가 기능을 추가하기 위해 사용하는 일부 서비스를 설명합니다.

주제

AWS CloudFormation을 사용하여 Amazon EVS 리소스 생성

Amazon EVS는 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 AWS 리소스를 모델링하고 설정하는 데 도움이 되는 서비스인 AWS CloudFormation과 통합됩니다. 예를 들어 Amazon EVS 환경 등 원하는 모든 AWS 리소스를 설명하는 템플릿을 생성하면 AWS CloudFormation에서 해당 리소스를 프로비저닝하고 구성합니다.

AWS CloudFormation을 사용하는 경우 템플릿을 재사용하여 Amazon EVS 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번만 설명한 다음 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝하기만 하면 됩니다.

Amazon EVS 및 AWS CloudFormation 템플릿

Amazon EVS 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이러한 템플릿은 AWS CloudFormation 스택에서 프로비저닝하려는 리소스를 설명합니다. JSON 또는 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하여 AWS CloudFormation 템플릿을 시작할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 CloudFormation Designer란 무엇입니까?를 참조하세요. AWS CloudFormation

Amazon EVS는 AWS CloudFormation에서 환경 생성을 지원합니다. 환경에 대한 JSON 및 YAML 템플릿의 예를 포함하여 자세한 내용은 AWS CloudFormation 사용 설명서의 Amazon EVS 리소스 유형 참조를 참조하세요.

AWS CloudFormation에 대해 자세히 알아보기

AWS CloudFormation에 대해 자세히 알아보려면 다음 리소스를 참조하세요.

- AWS CloudFormation

- AWS CloudFormation 사용 설명서
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

Amazon FSx for NetApp ONTAP을 사용하여 고성능 워크로드 실행

Amazon FSx for NetApp ONTAP은 클라우드에서 완전관리형 ONTAP 파일 시스템을 시작하고 실행할 수 있는 스토리지 서비스입니다. ONTAP은 널리 채택된 데이터 액세스 및 데이터 관리 기능의 집합을 제공하는 NetApp의 파일 시스템 기술입니다. FSx for ONTAP은 온프레미스 NetApp 파일 시스템의 기능, 성능 및 APIs에 완전 관리형 AWS 서비스의 민첩성, 확장성 및 단순성을 제공합니다. 자세한 내용은 FSx for ONTAP 사용 설명서를 참조하세요.

Amazon EVS는 Amazon FSx for NetApp ONTAP을 NFS/iSCSI 데이터 스토어 및 Amazon EVS에서 실행되는 VMware 가상 머신의 게스트 연결 스토리지로 사용할 수 있도록 지원합니다.

FSx for NetApp ONTAP을 NFS 데이터 스토어로 구성

다음 절차에서는 FSx 콘솔과 Amazon EVS에서 실행되는 VMware vSphere 클라이언트 인터페이스를 사용하여 FSx for NetApp ONTAP을 Amazon EVS용 NFS 데이터 스토어로 구성하는 데 필요한 최소 단계를 자세히 설명합니다. FSx

사전 조건

Amazon EVS를 Amazon FSx for NetApp ONTAP과 함께 사용하기 전에 다음 사전 조건 작업이 완료되었는지 확인합니다.

- Amazon EVS 환경은 Virtual Private Cloud(VPC)에 배포됩니다. 자세한 내용은 시작하기 단원을 참조하십시오.
- Amazon EVS에서 실행되는 vSphere 클라이언트에 액세스할 수 있습니다.
- 사용자 또는 스토리지 관리자는 VPC에서 FSx for ONTAP 파일 시스템을 생성하고 관리하는 데 필요한 권한이 있어야 합니다. 자세한 내용은 Amazon FSx for NetApp ONTAP의 ID 및 액세스 관리를 참조하세요.

IAM 보안 주체는 VPC에서 FSx for ONTAP 파일 시스템을 생성하고 관리할 수 있는 적절한 권한이 있습니다. 자세한 내용은 the section called “Amazon EVS 환경 생성 및 관리” 단원을 참조하십시오.

FSx for NetApp ONTAP 파일 시스템 생성

1. Amazon FSx 콘솔로 이동합니다.

2. 파일 시스템 생성을 선택합니다.
3. Amazon FSx for NetApp ONTAP을 선택합니다.
4. 다음을 선택합니다.
5. 표준 생성을 선택합니다.
6. 배포 유형에서 단일 AZ 배포 옵션을 선택합니다.

> **Note**
>
> Amazon EVS는 현재 단일 AZ 배포만 지원합니다.

7. SSD 스토리지 용량에 1024GiB를 지정합니다.
8. 처리량 용량에서 처리량 용량 지정을 선택합니다. 단일 AZ 1의 경우 최소 512MB/s를 선택하고 단일 AZ 2의 경우 최소 768MB/s를 선택합니다.
9. Amazon EVS VLAN 서브넷에 연결된 Amazon EVS VPC를 선택합니다.
10. Amazon EVS 호스트 VMkernel 관리 VLAN 서브넷으로의 모든 필수 FSx for ONTAP NFS 트래픽을 허용하는 보안 그룹을 선택합니다.
11. 파일 시스템을 배포할 Amazon EVS 서비스 액세스 서브넷을 선택합니다. 자세한 내용은 the section called “서비스 액세스 서브넷” 단원을 참조하십시오.
12. 정션 경로의 경우와 같이 의미 있는 이름을 지정/vol1하여 vSphere에서이 볼륨을 식별합니다.
13. 기본 볼륨 구성 내에서 스토리지 효율성을 활성화됨으로 설정합니다.
14. 나머지 설정을 기본값으로 두고 다음을 선택합니다.
15. 파일 시스템 속성을 검토하고 파일 시스템 생성을 선택합니다.

스토리지 가상 머신의 NFS DNS 이름 검색

1. Amazon FSx 콘솔로 이동합니다.
2. 왼쪽 메뉴에서 파일 시스템을 선택합니다.
3. 새로 생성된 파일 시스템을 선택합니다.
4. 스토리지 가상 머신 탭을 선택합니다.
5. 스토리지 가상 머신을 선택합니다.
6. 엔드포인트 탭을 선택합니다.
7. 나중에 VMware Vsphere에서 사용할 수 있도록 네트워크 파일 시스템(NFS) DNS 이름을 복사합니다.

FSx for ONTAP 볼륨을 사용하여 vSphere에서 NFS 데이터 스토어 생성 FSx

vSphere 환경에서 NFS 데이터 스토어 생성의 지침에 따라 Amazon FSx for NetApp ONTAP을 VMware vSphere의 외부 스토리지로 구성합니다. vSphere 클라이언트 인터페이스의 서버 설정의 경우 이전 단계에서 복사한 스토리지 가상 머신(SVM) NFS DNS 이름을 사용합니다.

FSx for NetApp ONTAP FSx를 iSCSI 데이터 스토어로 구성

다음 절차에서는 Amazon EVS에서 실행되는 FSx 콘솔 및 VMware vSphere 클라이언트 인터페이스를 사용하여 FSx for NetApp ONTAP을 Amazon EVS용 iSCSI 데이터 스토어로 구성하는 데 필요한 최소 단계를 자세히 설명합니다.

사전 조건

Amazon EVS를 Amazon FSx for NetApp ONTAP과 함께 사용하기 전에 다음 사전 조건 작업이 완료되었는지 확인합니다.

- Amazon EVS 환경은 Virtual Private Cloud(VPC)에 배포됩니다. 자세한 내용은 시작하기 단원을 참조하십시오.
- Amazon EVS에서 실행되는 vSphere 클라이언트에 액세스할 수 있습니다.
- 사용자 또는 스토리지 관리자는 VPC에서 FSx for ONTAP 파일 시스템을 생성하고 관리하는 데 필요한 권한이 있어야 합니다. 자세한 내용은 Amazon FSx for NetApp ONTAP의 ID 및 액세스 관리를 참조하세요.

FSx for NetApp ONTAP 파일 시스템 생성

1. Amazon FSx 콘솔로 이동합니다.
2. 파일 시스템 생성을 선택합니다.
3. Amazon FSx for NetApp ONTAP을 선택합니다.
4. 다음을 선택합니다.
5. 표준 생성을 선택합니다.
6. 배포 유형에서 단일 AZ 배포 옵션을 선택합니다.

> **Note**
>
> Amazon EVS는 현재 단일 AZ 배포만 지원합니다.

7. SSD 스토리지 용량에 1024GiB를 지정합니다.
8. 처리량 용량에서 처리량 용량 지정을 선택합니다. 단일 AZ 1의 경우 최소 512MB/s를 선택하고 단일 AZ 2의 경우 최소 768MB/s를 선택합니다.
9. Amazon EVS VLAN 서브넷에 연결된 Amazon EVS VPC를 선택합니다.
10. Amazon EVS 호스트 VMkernel 관리 VLAN 서브넷으로의 모든 필수 FSx for ONTAP iSCSI 트래픽을 허용하는 보안 그룹을 선택합니다.
11. 파일 시스템을 배포할 Amazon EVS 서비스 액세스 서브넷을 선택합니다. 자세한 내용은 the section called “서비스 액세스 서브넷” 단원을 참조하십시오.
12. 기본 볼륨 구성 내에서 스토리지 효율성을 활성화됨으로 설정합니다.
13. 나머지 설정을 기본값으로 두고 다음을 선택합니다.
14. 파일 시스템 속성을 검토하고 파일 시스템 생성을 선택합니다.

ESX 호스트 스토리지용 vSphere에서 소프트웨어 iSCSI 어댑터 구성

각 ESX 호스트에 대해 ESX 호스트가 이를 사용하여 iSCSI 스토리지에 액세스할 수 있도록 소프트웨어 iSCSI 어댑터를 구성해야 합니다. vSphere에서 ESX 호스트용 소프트웨어 iSCSI 어댑터를 구성하는 지침은 VMware vSphere 제품 설명서의 소프트웨어 iSCSI 어댑터 추가 또는 제거를 참조하세요.

소프트웨어 iSCSI 어댑터를 구성한 후 iSCSI 어댑터와 연결된 iSCSI 정규화된 이름(IQN)을 복사합니다. 이러한 값은 나중에 사용됩니다.

iSCSI LUN 생성

FSx for ONTAP을 사용하면 iSCSI 액세스를 위한 논리적 단위 번호(LUNs)를 생성하여 ESX 호스트에 공유 블록 스토리지를 제공할 수 있습니다. NetApp ONTAP CLI를 사용하여 LUN을 생성합니다.

다음은 샘플 명령입니다.

> **Note**
>
> LUN 크기를 볼륨 크기의 90%로 구성하는 것이 좋습니다.

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

자세한 내용은 FSx for ONTAP 사용 설명서의 iSCSI LUN 생성을 참조하세요. FSx

이니시에이터 그룹을 구성하고 iSCSI LUN에 매핑

이제 iSCSI LUN을 생성했으므로 프로세스의 다음 단계는 이니시에이터 그룹(igroup)을 생성하여 볼륨을 클러스터에 연결하고 LUN을 이니시에이터 그룹에 매핑하는 것입니다. NetApp ONTAP CLI를 사용하여 이러한 작업을 수행합니다.

1. 이니시에이터 그룹을 구성합니다.

   다음은 샘플 명령입니다. 의 경우 이전 단계에서 복사한 iSCSI 어댑터 IQNs을 `--initiator`사용합니다.

   ```
   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. 이 `igroup` 존재하는지 확인합니다.

   ```
   lun igroup show
   ```

3. LUN을 이니시에이터 그룹에 매핑합니다. 다음은 샘플 명령입니다.

   ```
   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` 명령을 사용하여 LUN이 생성, 온라인 및 매핑되었는지 확인합니다.

   ```
   lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
   ```

자세한 내용은 FSx for ONTAP 사용 설명서의 Linux용 iSCSI 프로비저닝 또는 Windows용 iSCSI 프로비저닝을 참조하세요. FSx

vSphere에서 iSCSI LUN의 동적 검색 구성

ESX 호스트가 iSCSI LUN을 볼 수 있도록 하려면 vSphere 클라이언트 인터페이스의 각 호스트에 대해 동적 검색을 구성해야 합니다. iSCSI 서버 필드에 이전 단계에서 복사한 (NFS) DNS 이름을 입력합니

다. 자세한 내용은 VMware vSphere 제품 설명서의 ESX 호스트에서 iSCSI 및 iSER에 대한 동적 또는 정적 검색 구성을 참조하세요.

iSCSI LUN을 사용하여 VMware vSphere에서 VMFS 데이터 스토어 생성

가상 머신 파일 시스템(VMFS) 데이터 스토어는 VMware 가상 머신의 리포지토리 역할을 합니다. vSphere VMFS 데이터 스토어 생성의 지침에 따라 이전에 구성한 iSCSI LUN을 사용하여 VMware vSphere에서 VMFS 데이터 스토어를 설정합니다.

문제 해결

이 장에서는 Amazon EVS 환경을 생성하거나 관리하는 동안 발생하는 몇 가지 일반적인 문제를 자세히 설명합니다.

실패한 환경 상태 확인 문제 해결

Amazon EVS는 환경을 자동으로 검사하여 문제를 식별합니다. 환경의 상태를 확인하여 탐지 가능한 특정 문제를 식별할 수 있습니다.

환경 상태 확인 정보 검토

Amazon EVS 콘솔을 사용하여 손상된 환경을 조사하려면

1. Amazon EVS 콘솔을 엽니다.
2. 탐색 창에서 환경을 선택한 다음 환경을 선택합니다.
3. 세부 정보 탭을 선택하여 환경의 개요를 확인합니다.
4. 환경 상태를 확인합니다. 이 필드를 마우스로 가리키면 각 환경 상태 확인에 대한 개별 결과가 포함된 팝오버가 확장됩니다.

연결성 확인 실패

연결성 검사는 Amazon EVS가 SDDC Manager에 지속적으로 연결되어 있는지 확인합니다. Amazon EVS가 환경에 연결할 수 없는 경우 이 검사는 실패합니다.

이 검사가 실패하면 Amazon EVS는 더 이상 SDDC Manager에 연결하여 환경 상태를 확인할 수 없으며 더 이상 호스트를 환경에 추가할 수 없습니다. 또한 연결성 검사가 실패하면 라이선스 키 재사용 및 키 적용 범위 확인이 실패하고 호스트 수 확인이 알 수 없음 응답을 반환하게 됩니다.

연결성을 보장하려면 다음을 확인하세요.

- 인증서가 유효하며 만료되지 않았는지 확인합니다. SDDC Manager UI 또는 vSphere 클라이언트를 사용하여 VCF 인스턴스의 인증서를 관리할 수 있습니다. 배포 후에는 VMware Cloud Foundation 관리 도메인의 모든 인증서를 교체하는 것이 좋습니다. 자세한 내용은 VMware Cloud Foundation 설명서의 VMware Cloud Foundation에서 인증서 관리를 참조하세요. VMware
- 서비스 액세스 서브넷에서 DNS 서버에 연결할 수 있고 DNS 레코드가 유효하며 중복 호스트 이름 또는 IP 주소가 없는지 확인합니다.

- 자체 방화벽 규칙을 생성하려면 다음 지침을 따르세요.
  - DNS 서버에 대한 TCP/UDP 액세스 허용
  - 호스트 관리 VLAN 서브넷에 대한 HTTPS/SSH 액세스 허용
  - 관리 VM VLAN 서브넷에 대한 HTTPS/SSH 액세스 허용

이 지침을 따른 후에도 여전히 문제를 해결할 수 없는 경우 AWS Support에 문의하여 추가 지원을 받는 것이 좋습니다.

호스트 수 확인 실패

이 검사는 환경에 최소 4개의 호스트가 있는지 확인합니다. 이는 VCF 5.2.x의 요구 사항입니다.

이 검사가 실패할 경우 환경이 이 최소 요구 사항을 충족하도록 호스트를 추가해야 합니다. Amazon EVS는 4~16개의 호스트가 있는 환경만 지원합니다.

키 재사용 검사 실패

이 검사는 VCF 라이선스 키가 다른 Amazon EVS 환경에서 사용되고 있지 않은지 확인합니다. VCF 라이선스는 하나의 Amazon EVS 환경에서만 사용할 수 있습니다. 다른 환경에서 이미 사용 중인 환경 생성 요청에 VCF 라이선스 키를 제공하면이 검사가 실패합니다.

이 검사가 실패하면 Amazon EVS 환경을 생성할 수 없다는 오류 응답을 받게 됩니다. 문제를 해결하려면 SDDC Manager에서 라이선스 설정을 검토하고 이전에 사용한 라이선스를 미사용 라이선스로 교체하세요.

> **Important**
>
> SDDC Manager 사용자 인터페이스를 사용하여 VCF 솔루션 및 vSAN 라이선스 키를 관리합니다. Amazon EVS에서는 서비스가 제대로 작동하려면 SDDC Manager에서 유효한 VCF 솔루션 및 vSAN 라이선스 키를 유지해야 합니다. vSphere Client를 사용하여 호스트 및 vSAN 클러스터에 키를 할당해야 하지만 이러한 키가 SDDC Manager 사용자 인터페이스의 라이선스 화면에도 표시되는지 확인해야 합니다.

키 적용 범위 확인 실패

이 검사는 vCenter Server에 배정된 VCF 라이선스 키가 배포된 모든 호스트에 충분한 vCPU 코어 및 vSAN 스토리지 용량(TiB)을 할당하는지 확인합니다.

이 검사가 실패하면 Amazon EVS 환경을 생성할 수 없다는 오류 응답을 받게 됩니다. 주요 적용 범위 검사의 실패는 다음 문제 중 하나를 나타낼 수 있습니다.

- VCF 라이선스가 vCenter Server에 제대로 할당되지 않았습니다. 평가 기간이 만료되거나 현재 할당된 라이선스가 만료되기 전에 vCenter Server에 라이선스를 할당해야 합니다. 이것이 문제인 경우 SDDC Manager에서 라이선스 할당을 검토하세요.
- 현재 VCF 라이선스는 vCPU 코어 및 vSAN 스토리지 용량 요구 사항을 다루지 않습니다. VCF 솔루션 키에는 256개 이상의 코어가 있어야 합니다. vSAN 라이선스 키에는 최소 110TiB의 vSAN 용량이 있어야 합니다. 이것이 문제인 경우 사용량 요구 사항이 충족되도록 SDDC Manager에서 vSAN 라이선스를 추가하세요.

위의 작업으로 문제가 해결되지 않는 경우 AWS Support에 문의하여 추가 지원을 받으세요.

> **Important**
>
> SDDC Manager 사용자 인터페이스를 사용하여 VCF 솔루션 및 vSAN 라이선스 키를 관리합니다. Amazon EVS에서는 서비스가 제대로 작동하려면 SDDC Manager에서 유효한 VCF 솔루션 및 vSAN 라이선스 키를 유지해야 합니다. vSphere Client를 사용하여 호스트 및 vSAN 클러스터에 키를 할당해야 하지만 이러한 키가 SDDC Manager 사용자 인터페이스의 라이선스 화면에도 표시되는지 확인해야 합니다.

이 호스트의 vSphere HA 에이전트가 격리 주소에 도달할 수 없음

vCenter 사용자 인터페이스에서 ESX 호스트를 선택하면 “이 호스트의 vSphere HA 에이전트가 격리 주소 <IPv6 주소>에 도달할 수 없습니다.”라는 메시지가 표시됩니다.

이 오류 메시지는 호스트의 vSphere HA 에이전트가 vSphere HA가 하트비트 검사에 사용하는 기본 IPv6 격리 주소에 도달할 수 없음을 나타냅니다. 오류 메시지는 문제를 나타내지 않으며 Amazon EVS가 현재 IPv6를 지원하지 않기 때문에 발생합니다. Amazon EVS에 대한 IPV6 지원의 부재는 vSphere HA의 핵심 기능에 영향을 미치지 않습니다.

ESX 호스트 클러스터에 대한 vSAN 업그레이드 사전 확인 실패

SDDC Manager를 사용하여 ESX 호스트 클러스터를 업그레이드하려고 하면 vSAN 디스크 관련 사전 확인이 실패할 수 있습니다. 이는 Amazon EVS가 vSAN Express 스토리지 아키텍처(ESA)를 사용하

며 업그레이드 사전 확인이 vSAN ESA에 적용되지 않기 때문입니다. 자세한 내용은 이 주제에 대한 Broadcom 지식 기반 문서를 참조하세요.

호환되지 않는 클러스터 이미지로 인한 호스트 실패 추가

문제

호스트를 환경에 추가하면 호스트에 사용 가능한 최신 버전의 EVS 사용자 지정 공급업체 추가 기능이 제공됩니다. 환경에서 이전 추가 기능 버전의 호스트를 사용하는 경우 새 호스트가 클러스터 이미지와 호환되지 않는다는 오류와 함께 새 호스트 추가가 실패합니다. 이 문제를 해결하려면 vSphere Lifecyle Manager를 사용하여 새로 추가된 호스트에서 사용 가능한 최신 추가 기능 버전을 추출해야 합니다.

솔루션

단계는 다음과 같습니다.

1. VMware vCenter Server의 호스트 및 클러스터 인벤토리로 이동합니다.
2. 임시 빈 클러스터를 생성하여 새로 추가된 호스트에서 추가 기능을 추출합니다.
3. 기본에서 vCenter 인벤토리의 기존 호스트에서 이미지 가져오기를 선택하고 클러스터를 생성합니다. 다른 모든 설정은 기본값으로 둡니다.
4. 추출된 이미지로이 임시 클러스터가 생성되면 임시 클러스터를 삭제할 수 있습니다. 이제 vSphere Lifecycle Manager 저장소에서 추가 기능을 사용할 수 있습니다.
5. 환경 클러스터로 이동하여 업데이트 탭을 선택합니다.
6. 클러스터 이미지를 편집하고 추가 기능 버전을 새로 추출된 버전으로 변경합니다.
7. 저장을 선택합니다.
8. SDDC Manager에서 실패한 호스트 추가 작업을 다시 시도합니다. 이렇게 하면 클러스터 호스트가 수정되어 모든 호스트가 최신 추가 기능 버전으로 업데이트됩니다. 클러스터 이미지 수정에는 호스트 재부팅이 필요합니다.

SDDC Manager가 호스트 커미셔닝 중에 VCF 호스트 검증에 실패함

문제

Amazon EVS 환경 배포 후 ESX 버전을 업데이트한 경우 수수료 호스트 단계에서 VCF 호스트 검증 중에 SDDC 관리자가 실패할 수 있습니다. 이 문제를 해결하려면 vSphere Lifecyle Manager를 사용하여 새로 추가된 호스트에서 ESX를 업그레이드해야 합니다.

솔루션

단계는 다음과 같습니다.

> **Important**
>
> 이 단계에서는 SDDC Manager 외부의 vCenter에 호스트를 일시적으로 추가해야 합니다. ESX 업그레이드 이외의 작업에 vSphere Lifecyle Manager를 사용하면 호스트를 사용할 수 없게 되어 새 Amazon EVS 호스트를 삭제하고 생성해야 할 수 있습니다.

1. VMware vCenter Server의 호스트 및 클러스터 인벤토리로 이동합니다.
2. 가상 데이터 센터에 호스트를 일시적으로 추가하여 이미지로 호스트 관리를 선택합니다. ESX 업그레이드가 완료된 후 이후 단계에서 호스트가 제거됩니다. 자세한 내용은 vSphere 설명서의 vSphere 데이터 센터 또는 폴더에 호스트를 추가하는 방법을 참조하세요. vSphere
3. 호스트가 vSphere에 추가되면 호스트에서 ESX 버전을 업그레이드합니다. 호스트의 업데이트 탭에서이 작업을 수행할 수 있습니다. 클러스터의 ESX 버전과 일치하도록 호스트 이미지를 편집합니다.
4. 업그레이드가 완료되면 vCenter 인벤토리에서 호스트를 제거합니다. 자세한 내용은 vSphere 설명서의 vCenter Server 인스턴스에서 ESX 호스트를 제거하는 방법을 참조하세요. vSphere
5. SDDC 관리자에서 호스트를 커미셔닝합니다. 자세한 내용은 VMware Cloud Foundation 설명서의 Commission Hosts를 참조하세요.
6. 호스트를 커미셔닝한 후 SDDC Manager를 사용하여 클러스터에 호스트를 추가합니다.

AWS CloudTrail을 사용하여 Amazon EVS API 호출 로깅

Amazon EVS는 Amazon EVS에서 IAM 사용자, IAM 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Amazon EVS에 대한 모든 AWS API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Amazon EVS 콘솔의 호출과 Amazon EVS API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Amazon EVS 이벤트를 포함하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. Amazon S3 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Amazon EVS에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

> **Note**
>
> Amazon EVS는 VCF 환경 내 활동과 같은 비AWS 구성 요소에 대한 사용자 활동을 로깅하지 않습니다. 이러한 활동은 vSphere 및 NSX Manager와 같은 다양한 VMware 콘솔에 로깅됩니다.
> 중앙 집중식 VCF 로깅을 원하는 경우 VMware Cloud Foundation Operations와 같은 VCF 모니터링 솔루션을 구성하여이 결과를 얻을 수 있습니다.

CloudTrail의 Amazon EVS 정보

AWS 계정을 생성할 때 계정에서 CloudTrail이 활성화됩니다. Amazon EVS에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다. 자세한 설명은 CloudTrail 이벤트 기록으로 이벤트 보기를 참조하세요.

Amazon EVS 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 추적을 생성하면 추적이 모든 AWS 리전에 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요

- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신
- 여러 계정에서 CloudTrail 로그 파일 수신

모든 Amazon EVS 작업은 CloudTrail에서 로깅되며 Amazon EVS API 참조에 문서화됩니다. 예를 들어 `CreateEnvironment`, `GetEnvironment`, `DeleteEnvironment` 작업을 직접 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Amazon EVS 로그 파일 항목 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출에 대한 순서가 지정된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

Amazon EVS 서비스 할당량

Amazon EVS는 중앙 위치에서 할당량을 보고 관리하는 데 사용할 수 AWS 서비스 있는 Service Quotas와 통합되었습니다. 자세한 내용은 Service Quotas 사용 설명서의 Service Quotas는 무엇인가요?를 참조하세요.

Service Quotas 통합을 사용하면 AWS Management Console 또는를 사용하여 Amazon EVS 할당량의 값을 AWS CLI 조회하고 조정 가능한 할당량에 대한 할당량 증가를 요청할 수 있습니다. 자세한 내용은 Service Quotas 사용 설명서의 할당량 증가 요청 및 명령 참조의 request-service-quota-increase를 참조하세요. AWS CLI

Amazon EVS 서비스 할당량에 대한 자세한 내용은 AWS 일반 참조 안내서의 Amazon EVS 할당량을 참조하세요.

Important

EC2 온디맨드 표준 인스턴스 실행 할당량에 Amazon EVS에서 사용할 모든 EC2 인스턴스에 필요한 vCPU 수가 반영되어 있는지 확인하세요. 각 i4i.metal 인스턴스는 128개의 vCPU를 사용합니다. EC2 서비스 할당량 증가에 대한 자세한 내용은 Amazon EC2 사용 설명서의 증가 요청을 참조하세요.

Note

Amazon EVS 환경에 EC2 전용 호스트를 사용하려는 경우 EC2 전용 i4i 호스트 할당량에 원하는 리전에 사용하려는 전용 호스트 수가 반영되어 있는지 확인하세요. EC2 서비스 할당량 증가에 대한 자세한 내용은 Amazon EC2 사용 설명서의 증가 요청을 참조하세요.

Note

HCX 인터넷 연결을 구성하는 경우 Amazon에서 제공하는 연속 퍼블릭 IPv4 CIDR 블록 넷마스크 길이에 대한 IPAM 할당량은 /28 이상이어야 합니다. 자세한 내용은 IPAM 할당량을 참조하세요.

> **Note**
>
> Amazon CloudWatch는 할당량(환경 및 호스트)이 있는 Amazon EVS 리소스에 대한 AWS 사용 지표를 수집합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서에서 CloudWatch 사용량 지표를 참조하세요.

에서 Amazon EVS 서비스 할당량 보기 AWS Management Console

1. Service Quotas Console을 엽니다.
2. 왼쪽 탐색 창에서 AWS 서비스를 선택합니다.
3. AWS 서비스 목록에서 Amazon Elastic VMware Service를 검색하고 선택합니다.
4. 할당량 보기를 선택합니다.

   서비스 할당량 목록에서 서비스 할당량 이름, 적용된 값(사용 가능한 경우), AWS 기본 할당량 및 할당량 값을 조정할 수 있는지 여부를 확인할 수 있습니다.
5. 설명 등 서비스 할당량에 대한 추가 정보를 보려면 할당량 이름을 선택합니다.
6. (선택 사항) 할당량 증가를 요청하려면 늘릴 할당량을 선택하고 계정 수준에서 증가 요청을 선택한 다음 필요한 정보를 입력하거나 선택하고 요청을 선택합니다.

를 사용하여 서비스 할당량에 대해 자세히 알아보려면 Service Quotas 사용 설명서를 AWS Management Console참조하세요. 할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

AWS CLI를 사용하여 Amazon EVS 서비스 할당량 보기

다음 명령을 실행하여 Amazon EVS 할당량을 확인합니다.

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
    --output table
```

> **Note**
>
> 반환되는 할당량은 현재 AWS 리전의이 계정에서 생성할 수 있는 Amazon EVS 환경 또는 호스트 수입니다.

AWS CLI를 사용하여 서비스 할당량에 대해 자세히 알아보려면 AWS CLI 명령 참조의 service-quotas를 참조하세요. 할당량 증가를 요청하려면 CLI 명령 참조의 request-service-quota-increase 명령을 참조하세요. AWS

Amazon Elastic VMware Service 사용 설명서의 문서 기록

다음 표에서는 Amazon Elastic VMware Service의 설명서 릴리스를 설명합니다.

변경 사항	설명	날짜
업데이트된 AmazonEVSServiceRolePolicy	Amazon EVS는 서비스가 AWS Secrets Manager에서 vCenter 자격 증명을 검색하고 고객 관리형 KMS 키로 암호화된 보안 암호를 해독AmazonEVSServiceRolePolicy 할 수 있도록 관리형 정책을 업데이트했습니다.	2026년 3월 23일
업데이트된 AmazonEVSServiceRolePolicy	Amazon EVS는 EC2 인스턴스 관리, EBS 볼륨 작업, AWS Secrets Manager 통합을 포함한 포괄적인 리소스 관리 기능을 추가AmazonEVSServiceRolePolicy 하도록 관리형 정책을 업데이트했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon EVS 업데이트를 참조하세요.	2025년 8월 14일
업데이트된 AmazonEVSServiceRolePolicy	AWS 관리형 정책 AmazonEVSServiceRolePolicy를 업데이트했습니다.	2025년 8월 4일
AWS 계정 할당량당 환경 수를 릴리스했습니다.	AWS 계정 할당량당 Amazon EVS 릴리스 환경 수입니다. AWS 계정 할당량당 환경 수는 지정된 계정 및 리전에서 생성할 수 있는 Amazon EVS 환경의 최대 수를 나타냅니다.	2025년 7월 8일

유럽(아일랜드) 리전에서 Amazon EVS 출시	Amazon EVS는 유럽(아일랜드) 리전에서 릴리스되었습니다.	2025년 6월 18일
AmazonEVSServiceRolePolicy 릴리스	AWS 관리형 정책 AmazonEVSServiceRolePolicy가 릴리스되었습니다.	2025년 6월 9일
초기 사용 설명서 릴리스	Amazon Elastic VMware Service 사용 설명서가 릴리스되었습니다. Amazon EVS 사용 설명서에서는 모든 Amazon EVS 개념을 설명하고 콘솔과 명령줄 인터페이스 모두에서 다양한 기능을 사용하는 방법에 대한 지침을 제공합니다.	2025년 6월 9일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.