Red Hat OpenShift Service on AWS 4

ROSA 소개

AWS 아키텍처의 Red Hat OpenShift Service 개요

Last Updated: 2024-09-28

Red Hat OpenShift Service on AWS 4 ROSA 소개

AWS 아키텍처의 Red Hat OpenShift Service 개요

법적 공지

초록

이 문서에서는 ROSA(Red Hat OpenShift Service on AWS)의 플랫폼 및 애플리케이션 아키텍처에 대한 개요를 제공합니다.

차례

1장. ROSA 이해

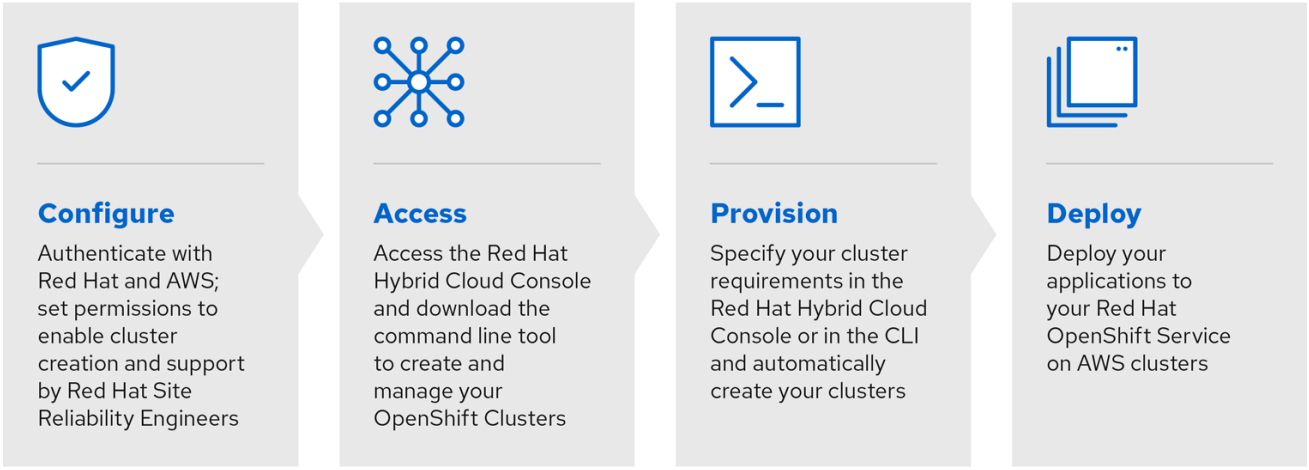
Red Hat OpenShift Cluster Manager 및 CLI(명령줄 인터페이스) 툴, 소비 환경 및 AWS(Amazon Web Services) 서비스와의 통합을 사용하여 ROSA(Red Hat OpenShift Cluster Manager)와 상호 작용하여 Red Hat OpenShift Service on AWS에 대해 알아보십시오.

1.1. ROSA 정보

ROSA는 완전히 관리되는 turnkey 애플리케이션 플랫폼으로, 애플리케이션을 빌드하고 배포하여 고객에게 가치를 제공하는 데 집중할 수 있습니다. Red Hat 및 AWS SRE(Site reliability engineering) 전문가가 기본 플랫폼을 관리하므로 인프라 관리의 복잡성에 대해 우려할 필요가 없습니다. ROSA는 광범위한 AWS 컴퓨팅, 데이터베이스, 분석, 머신 러닝, 네트워킹, 모바일 및 기타 서비스와의 원활한 통합을 제공하여 고객에게 차별화된 환경을 구축하고 더욱 가속화합니다.

AWS 계정에서 직접 서비스에 가입합니다. 클러스터가 생성되면 OpenShift 웹 콘솔 또는 Red Hat OpenShift Cluster Manager를 통해 클러스터를 작동할 수 있습니다. ROSA 서비스는 OpenShift API 및 CLI(명령줄 인터페이스) 툴도 사용합니다. 이러한 툴은 표준화된 OpenShift 환경을 제공하여 기존 기술 및 툴 지식을 사용할 수 있습니다.

새로운 기능 릴리스와 OpenShift Container Platform에 맞게 공유된 공통 소스를 통한 OpenShift 업데이트를 받습니다. ROSA는 버전 일관성을 달성하기 위해 Red Hat OpenShift Dedicated 및 OpenShift Container Platform과 동일한 버전의 OpenShift를 지원합니다.



1.2. 인증 정보 모드

작은 정보

AWS STS(Security Token Service)는 강화된 보안을 제공하기 때문에 AWS의 Red Hat OpenShift Service on AWS(ROSA)에 클러스터를 설치하고 상호 작용하는 데 권장되는 인증 정보 모드입니다.

ROSA 클러스터에는 두 가지 인증 정보 모드가 지원됩니다. 하나는 권장되는 AWS Security Token Service(STS)를 사용하며, 다른 하나는 IAM(Identity Access Management) 역할을 사용합니다.

1.2.1. STS를 사용하는 ROSA

AWS STS는 IAM 또는 페더레이션 사용자에 대한 단기 인증 정보를 제공하는 글로벌 웹 서비스입니다.

STS를 사용하는 ROSA는 ROSA 클러스터에 권장되는 인증 정보 모드입니다. ROSA와 함께 AWS STS를 사용하여 구성 요소별 IAM 역할에 대해 제한된 임시 인증 정보를 할당할 수 있습니다. 이 서비스를 사용하면 클러스터 구성 요소가 보안 클라우드 리소스 관리 방법을 사용하여 AWS API를 호출할 수 있습니다.

rosa CLI를 사용하여 STS를 사용하는 ROSA 클러스터에 필요한 IAM 역할, 정책 및 ID 공급자 리소스를 생성할 수 있습니다.

AWS STS는 클라우드 서비스 리소스 관리에서 최소 권한 및 보안 관행의 원칙에 맞게 조정됩니다. **rosa** CLI는 고유한 작업에 할당된 STS 자격 증명을 관리하고 OpenShift 기능의 일부로 AWS 리소스에 대해 작업을 수행합니다. STS 사용의 한 가지 제한은 각 ROSA 클러스터에 대해 역할을 생성해야 한다는 것입니다.

STS 인증 정보 모드는 다음과 같은 이유로 더 안전합니다.

- 미리 생성하고 사용된 모든 역할에 대해 요청한 모든 권한을 추적할 수 있는 명시적 및 제한된 역할 및 정책 세트를 지원합니다.
- 서비스는 세트 권한으로 제한됩니다.
- 서비스가 실행되면 1시간 후에 만료되는 인증 정보를 얻을 수 있으므로 자격 증명을 순환하거나 취소할 필요가 없습니다. 또한 만료되면 인증 정보가 유출되고 재사용될 위험이 줄어듭니다.

STS를 사용하는 ROSA 클러스터용 IAM 리소스 정보에서 계정 전체 및 클러스터 별 역할 목록이 제공됩니다.

1.2.2. STS를 사용하지 않는 ROSA

이 모드에서는 필요에 따라 다른 역할 및 리소스를 생성하는 데 적절한 권한이 있는 계정 내에서 **AdministratorAccess** 가 있는 사전 생성된 IAM 사용자를 사용합니다. 이 계정을 사용하면 서비스는 클러스터에 필요한 모든 리소스를 생성합니다.

1.3. 청구 및 가격

ROSA는 귀하의 AWS 계정에 직접 청구됩니다. ROSA 가격은 연간 약정 또는 더 큰 할인을 위한 3년 약속으로 소비할 수 있습니다. ROSA의 총 비용은 두 가지 구성 요소로 이루어져 있습니다.

- ROSA 서비스 요금
- AWS 인프라 요금

자세한 내용은 AWS 가격 페이지를 참조하십시오.

1.4. 시작하기

클러스터 배포를 시작하려면 AWS 계정이 사전 요구 사항을 충족했는지 확인하고 Red Hat 계정을 준비하고 AWS에서 Red Hat OpenShift Service 시작하기에 설명된 절차를 따르십시오.

추가 리소스

- OpenShift Cluster Manager
- STS를 사용하는 ROSA 클러스터의 IAM 리소스 정보
- AWS에서 Red Hat OpenShift Service 시작하기
- AWS 가격 페이지

2장. ROSA 아키텍처

2.1. 아키텍처 개념

AWS 아키텍처의 Red Hat OpenShift Service에 사용되는 OpenShift 및 컨테이너 기본 개념에 대해 알아보십시오.

2.1.1. OpenShift

OpenShift는 엔터프라이즈 워크로드를 실행하는 신뢰할 수 있는 환경을 제공하는 Kubernetes 컨테이너 플랫폼입니다. Kubernetes 플랫폼을 내장 소프트웨어로 확장하여 앱 라이프사이클 개발, 운영 및 보안을 향상시킵니다. OpenShift를 사용하면 하이브리드 클라우드 공급자 및 환경에 워크로드를 일관되게 배포할 수 있습니다.

2.1.2. Kubernetes

ROSA(Red Hat OpenShift Service on AWS)는 엔터프라이즈 Kubernetes 플랫폼인 Red Hat OpenShift를 사용합니다. Kubernetes는 여러 호스트에서 컨테이너화된 워크로드 및 서비스를 관리하기 위한 오픈 소스 플랫폼으로, 수동 개입 없이 컨테이너화된 애플리케이션을 배포, 자동화, 모니터링 및 스케일링하기 위한 관리 툴을 제공합니다. Kubernetes에 대한 자세한 내용은 Kubernetes 설명서 를 참조하십시오.

클러스터, 컴퓨팅 풀 및 컴퓨팅 노드

Kubernetes 클러스터는 컨트롤 플레인과 하나 이상의 컴퓨팅 노드로 구성됩니다. 컴퓨팅 노드는 CPU, 메모리, 운영 체제, 연결된 디스크 및 기타 속성의 유형 또는 프로파일의 컴퓨팅 풀로 구성됩니다. 컴퓨팅 노드는 Kubernetes 노드 리소스에 **해당하며** 클러스터의 모든 Kubernetes 리소스를 중앙에서 제어하고 모니터링하는 Kubernetes 컨트롤 플레인에 의해 관리됩니다.
컨테이너화된 앱의 리소스를 배포할 때 Kubernetes 컨트롤 플레인은 클러스터의 배포 요구 사항 및 사용 가능한 용량을 고려하여 해당 리소스를 배포할 컴퓨팅 노드를 결정합니다. Kubernetes 리소스에는 서비스, 배포, Pod가 포함됩니다.

네임스페이스

Kubernetes 네임스페이스는 여러 팀과 클러스터를 공유하려는 경우와 같이 애플리케이션을 배포하고 액세스를 제한할 수 있는 별도의 영역으로 클러스터 리소스를 분할하는 방법입니다. 예를 들어, 사용자를 위해 구성된 시스템 리소스는 **kube-system** 과 같은 별도의 네임스페이스에 유지됩니다.
Kubernetes 리소스를 생성할 때 네임스페이스를 지정하지 않으면 리소스가 **기본** 네임스페이스에 자동으로 생성됩니다.

Pod

클러스터에 배포된 모든 컨테이너화된 앱은 Pod라고 하는 Kubernetes 리소스에서 배포, 실행 및 관리합니다. Pod는 Kubernetes 클러스터에서 소규모 배포 가능 단위이며 단일 단위로 처리해야 하는 컨테이너를 그룹화하는 데 사용됩니다. 대부분의 경우 각 컨테이너는 자체 Pod에 배포됩니다. 그러나 앱에는 동일한 개인 IP 주소를 사용하여 해당 컨테이너를 처리할 수 있도록 컨테이너 및 기타 도우미 컨테이너를 하나의 포드에 배포해야 할 수 있습니다.

app

앱은 전체 앱 또는 앱의 구성 요소를 참조할 수 있습니다. 별도의 Pod 또는 컴퓨팅 노드에 앱의 구성 요소를 배포할 수 있습니다.

Service

서비스는 Pod 세트를 그룹화하고 각 Pod의 실제 개인 IP 주소를 노출하지 않고 이러한 Pod에 네트워크 연결을 제공하는 Kubernetes 리소스입니다. 서비스를 사용하여 클러스터 내에서 또는 공용 인터넷 내에서 앱을 사용할 수 있도록 할 수 있습니다.

Deployment

배포는 서비스, 영구 스토리지 또는 주석과 같이 앱을 실행하는 데 필요한 다른 리소스 또는 기능에 대한 정보를 지정할 수 있는 Kubernetes 리소스입니다. 구성 YAML 파일에서 배포를 구성한 다음 클러스터에 적용합니다. Kubernetes 기본 리소스는 리소스를 구성하고 사용 가능한 용량이 있는 컴퓨팅 노드의 포드에 컨테이너를 배포합니다.
롤링 업데이트 중에 추가할 Pod 수 및 한 번에 사용할 수 없는 Pod 수를 포함하여 앱에 대한 업데이트 전략을 정의합니다. 롤링 업데이트를 수행하면 배포에서 업데이트가 작동하는지 확인하고 오류가 감지되면 롤아웃을 중지합니다.

배포는 Pod를 관리하는 데 사용할 수 있는 하나의 유형의 워크로드 컨트롤러일 뿐입니다.

2.1.3. 컨테이너

컨테이너에서는 애플리케이션 코드, 구성 및 종속 항목을 단일 단위로 패키징하는 표준 방법을 제공합니다. 컨테이너는 컴퓨팅 호스트에서 격리된 프로세스로 실행되며 호스트 운영 체제 및 해당 하드웨어 리소스를 공유합니다. 컨테이너를 환경 간에 이동하고 변경 없이 실행할 수 있습니다. 컨테이너는 가상 머신과 달리 장치, 운영 체제 및 기본 하드웨어를 가상화하지 않습니다. 앱 코드, 런타임, 시스템 도구, 라이브러리 및 설정만 컨테이너 내부에 패키지됩니다. 이 방법을 사용하면 컨테이너를 가상 머신보다 가볍고 이식 가능하며 효율적으로 사용할 수 있습니다.

기존 Linux 컨테이너 기술(LXC)을 기반으로 구축된 OCI 호환 컨테이너 이미지는 앱을 실행하는 데 필요한 모든 요소를 포함하는 표준화된 단위로 소프트웨어를 패키징하는 방법에 대한 템플릿을 정의합니다. Red Hat OpenShift Service on AWS(ROSA)는 CRI-O를 컨테이너 런타임으로 사용하여 클러스터에 컨테이너를 배포합니다.

ROSA의 Kubernetes에서 앱을 실행하려면 먼저 컨테이너 레지스트리에 저장한 컨테이너 이미지를 생성하여 앱을 컨테이너화해야 합니다.

Image

컨테이너 이미지는 실행하려는 모든 컨테이너의 기본입니다. 컨테이너 이미지는 이미지를 빌드하는 방법 및 앱, 앱 구성 및 해당 종속 항목과 같이 이미지를 빌드하는 방법을 정의하는 텍스트 파일인 Dockerfile에서 빌드됩니다. 이미지는 항상 다른 이미지에서 빌드되므로 빠르게 구성합니다.

Registry

이미지 레지스트리는 컨테이너 이미지를 저장, 검색 및 공유할 수 있는 위치입니다. 레지스트리에 저장된 이미지는 공개적으로 사용 가능(공용 레지스트리)되거나 소규모 사용자 그룹(개인 레지스트리)에서 액세스할 수 있습니다. ROSA는 컨테이너화된 첫 번째 앱을 생성하는 데 사용할 수 있는 공용 이미지를 제공합니다. 엔터프라이즈 애플리케이션의 경우 프라이빗 레지스트리를 사용하여 권한이 없는 사용자가 이미지를 사용하지 않도록 보호합니다.

2.2. 아키텍처 모델

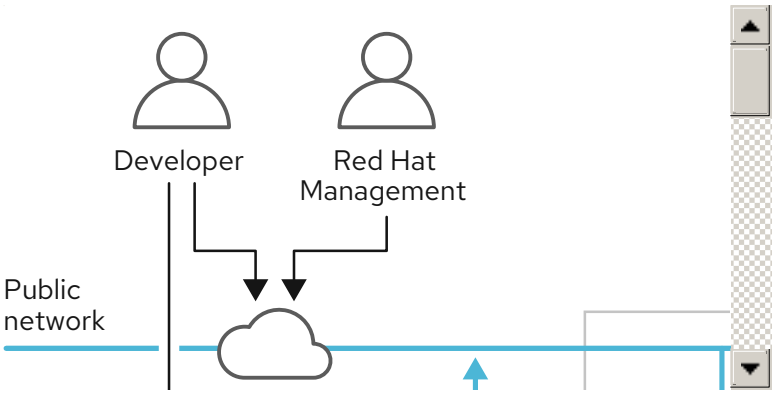
ROSA 아키텍처는 다음과 같은 네트워크 구성 유형을 지원합니다.

- 공용 네트워크
- 프라이빗 네트워크
- AWS PrivateLink

2.2.1. 공개 및 사설 네트워크의 ROSA 아키텍처

공용 또는 사설 네트워크를 사용하여 ROSA를 설치할 수 있습니다. 클러스터 생성 프로세스 중 또는 이후에 개인 클러스터 및 사설 네트워크 연결을 구성합니다. Red Hat은 공용 네트워크를 통한 제한된 액세스 권한으로 클러스터를 관리합니다. 자세한 내용은 서비스 정의를 참조하십시오.

그림 2.1. ROSA는 공개 및 사설 네트워크에 배포



또는 프라이빗 서브넷에서만 호스팅되는 AWS PrivateLink를 사용하여 클러스터를 설치합니다.

2.2.2. AWS PrivateLink 아키텍처

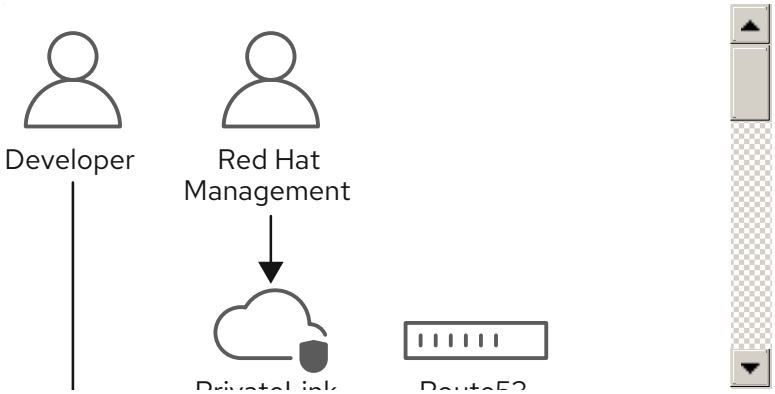
AWS PrivateLink 클러스터를 생성하는 Red Hat 관리 인프라는 프라이빗 서브넷에서 호스팅됩니다. Red Hat과 고객 제공 인프라 간의 연결은 AWS PrivateLink VPC 엔드포인트를 통해 생성됩니다.

참고

AWS PrivateLink는 기존 VPC에서만 지원됩니다.

다음 다이어그램은 PrivateLink 클러스터의 네트워크 연결을 보여줍니다.

그림 2.2. 프라이빗 서브넷에 배포된 다중 AZ AWS PrivateLink 클러스터



2.2.2.1. AWS 참조 아키텍처

AWS는 AWS PrivateLink를 사용하는 구성을 설정하는 방법을 계획할 때 고객에게 유용할 수 있는 여러 참조 아키텍처를 제공합니다. 다음은 세 가지 예입니다.

- 프라이빗 서브넷 및 AWS Site-to-Site VPN 액세스가 있는 VPC
  이 구성을 사용하면 네트워크를 인터넷에 노출하지 않고도 네트워크를 클라우드로 확장할 수 있습니다.

  IPsec(Internet Protocol Security) VPN 터널을 통해 네트워크와 통신할 수 있도록 이 구성에는 단일 프라이빗 서브넷과 가상 프라이빗 게이트웨이가 있는 VPC(가상 프라이빗 클라우드)가 포함되어 있습니다. 인터넷을 통한 통신은 인터넷 게이트웨이를 사용하지 않습니다.

  자세한 내용은 AWS 문서의 프라이빗 서브넷만 있는 VPC 및 AWS Site-to-Site VPN 액세스 를 참조하십시오.

- 퍼블릭 및 프라이빗 서브넷 (NAT)이 있는 VPC
  이 구성을 사용하면 공용 서브넷에 연결할 수 있지만 프라이빗 서브넷이 없도록 네트워크를 분리할 수 있습니다.

  공용 서브넷만 아웃바운드 트래픽을 인터넷에 직접 보낼 수 있습니다. 프라이빗 서브넷은 공용 서브넷에 상주하는 NAT(네트워크 주소 변환) 게이트웨이를 사용하여 인터넷에 액세스할 수 있습니다. 이를 통해 데이터베이스 서버는 NAT 게이트웨이를 사용하여 소프트웨어 업데이트를 위해 인터넷에 연결할 수 있지만, 인터넷에서 데이터베이스 서버로 직접 연결할 수는 없습니다.

  자세한 내용은 AWS 문서의 퍼블릭 및 프라이빗 서브넷(NAT)이 있는 VPC 를 참조하십시오.

- 퍼블릭 및 프라이빗 서브넷 및 AWS Site-to-Site VPN 액세스가 있는 VPC
  이 구성을 사용하면 네트워크를 클라우드로 확장하고 VPC에서 인터넷에 직접 액세스할 수 있습니다.

  퍼블릭 서브넷에서 확장 가능한 웹 프런트 엔드를 사용하여 다중 계층 애플리케이션을 실행하고 IPsec AWS 사이트 간 VPN 연결을 통해 네트워크에 연결된 프라이빗 서브넷에 데이터를 저장할 수 있습니다.

  자세한 내용은 AWS 문서의 퍼블릭 및 프라이빗 서브넷 및 AWS Site-to-Site VPN 액세스 권한이 있는 VPC 를 참조하십시오.

3장. 정책 및 서비스 정의

3.1. AWS에서 RED HAT OPENSHIFT SERVICE의 가용성 정보

가용성 및 재해 방지는 모든 애플리케이션 플랫폼에서 매우 중요한 요소입니다. Red Hat OpenShift Service on AWS(ROSA)는 여러 수준에서 장애에 대해 다양한 보호 기능을 제공하지만 고가용성을 위해 고객 배포된 애플리케이션을 적절하게 구성해야 합니다. 클라우드 공급자에서 발생할 수 있는 중단을 고려하여 여러 가용성 영역에 클러스터를 배포하고 장애 조치 메커니즘을 사용하여 여러 클러스터를 유지보수하는 등의 추가 옵션을 사용할 수 있습니다.

3.1.1. 잠재적인 실패 지점

Red Hat OpenShift Service on AWS(ROSA)는 워크로드를 다운타임으로부터 보호할 수 있는 다양한 기능과 옵션을 제공하지만, 애플리케이션은 이러한 기능을 활용하기 위해 적절하게 설계해야 합니다.

ROSA는 Red Hat 사이트 안정성 엔지니어링(SRE) 지원 및 여러 가용 영역 클러스터를 배포하는 옵션을 추가하여 많은 일반적인 Kubernetes 문제로부터 사용자를 보호할 수 있지만 컨테이너나 인프라가 여전히 실패할 수 있는 여러 가지 방법이 있습니다. 잠재적인 장애 지점을 이해하면 위험을 이해하고 애플리케이션과 클러스터를 각각의 특정 수준에서 필요에 따라 탄력적으로 조정할 수 있습니다.

참고

중단은 여러 수준의 인프라 및 클러스터 구성 요소에서 발생할 수 있습니다.

3.1.1.1. 컨테이너 또는 Pod 실패

Pod는 설계상 짧은 기간 동안 존재해야 합니다. 애플리케이션 Pod의 여러 인스턴스가 실행되는 경우 개별 Pod 또는 컨테이너의 문제를 방지할 수 있도록 서비스를 적절하게 스케일링합니다. OpenShift 노드 스케줄러는 복원력을 추가로 개선하기 위해 이러한 워크로드가 다른 작업자 노드에 분산되어 있는지도 확인할 수 있습니다.

가능한 Pod 오류를 처리할 때 스토리지가 애플리케이션에 연결된 방식을 이해하는 것도 중요합니다. 단일 포드에 연결된 단일 영구 볼륨은 포드 확장의 모든 이점을 활용할 수 없지만 복제된 데이터베이스, 데이터베이스 서비스 또는 공유 스토리지는 가능합니다.

계획된 유지 관리 기간(예: 업그레이드) 동안 애플리케이션의 중단을 방지하려면 Pod 중단 예산을 정의하는 것이 중요합니다. 이는 Kubernetes API의 일부이며 다른 오브젝트 유형과 같은 **oc** 명령으로 관리할 수 있습니다. 유지 관리를 위해 노드를 드레이닝하는 것과 같이 작업 중에 Pod에 대한 보안 제약 조건을 지정할 수 있습니다.

3.1.1.2. 작업자 노드 장애

작업자 노드는 애플리케이션 pod가 포함된 가상 머신입니다. 기본적으로 ROSA 클러스터에는 단일 가용성 영역 클러스터에 대해 최소 두 개의 작업자 노드가 있습니다. 작업자 노드 오류가 발생하는 경우 기존 노드와 관련된 문제가 해결되거나 노드가 교체될 때까지 충분한 용량이 있는 한 작업자 노드가 작동되도록 Pod가 재배치됩니다. 더 많은 작업자 노드는 단일 노드 중단을 방지할 수 있으며 노드 장애가 발생할 경우 Pod를 다시 예약하기 위한 적절한 클러스터 용량을 보장합니다.

참고

가능한 노드 오류를 처리할 때 스토리지의 영향을 이해하는 것도 중요합니다. EFS 볼륨은 노드 장애의 영향을 받지 않습니다. 그러나 실패한 노드에 연결된 경우 EBS 볼륨에 액세스할 수 없습니다.

3.1.1.3. 클러스터 장애

단일 AZ ROSA 클러스터에는 프라이빗 서브넷에서 동일한 가용 영역(AZ)에 3개 이상의 컨트롤 플레인과 두 개의 인프라 노드가 있습니다.

다중 AZ ROSA 클러스터에는 선택한 클러스터 유형에 따라 단일 영역 또는 여러 영역에서 고가용성을 위해 사전 구성된 컨트롤 플레인 노드와 세 개의 인프라 노드가 있습니다. 컨트롤 플레인 및 인프라 노드는 작업자 노드와 동일한 복원력을 가지며 Red Hat에서 완전히 관리할 수 있는 추가 이점이 있습니다.

완전한 컨트롤 플레인 중단이 발생하면 OpenShift API가 작동하지 않으며 기존 작업자 노드 Pod는 영향을 받지 않습니다. 그러나 Pod 또는 노드 중단이 동시에 발생하는 경우 새 Pod 또는 노드를 추가하거나 예약하기 전에 컨트롤 플레인을 복구해야 합니다.

인프라 노드에서 실행되는 모든 서비스는 Red Hat에서 고가용성으로 구성하고 인프라 노드에 분산합니다. 완전한 인프라 중단이 발생하는 경우 이러한 노드가 복구될 때까지 이러한 서비스를 사용할 수 없습니다.

3.1.1.4. 영역 장애

AWS의 영역 오류는 단일 가용성 영역과 관련된 작업자 노드, 블록 또는 공유 스토리지, 로드 밸런서와 같은 모든 가상 구성 요소에 영향을 미칩니다. 영역 장애로부터 보호하기 위해 ROSA는 여러 가용성 영역 클러스터라는 세 가지 가용성 영역에 분산된 클러스터에 대한 옵션을 제공합니다. 기존 상태 비저장 워크로드는 충분한 용량이 있는 경우 중단 시 영향을 받지 않는 영역에 재배포됩니다.

3.1.1.5. 스토리지 장애

상태 저장 애플리케이션을 배포한 경우 스토리지는 중요한 구성 요소이며 고가용성을 고려할 때 고려해야 합니다. 단일 블록 스토리지 PV는 Pod 수준에서도 중단을 방지할 수 없습니다. 스토리지의 가용성을 유지하는 가장 좋은 방법은 복제된 스토리지 솔루션, 중단의 영향을 받지 않는 공유 스토리지 또는 클러스터와 무관한 데이터베이스 서비스를 사용하는 것입니다.

3.2. 책임 할당 매트릭스

이 문서에서는 ROSA(Red Hat OpenShift Service on AWS) 관리 서비스에 대한 Red Hat, 클라우드 공급자 및 고객 업무를 간략하게 설명합니다.

3.2.1. AWS의 Red Hat OpenShift Service 책임 개요

Red Hat과 Amazon Web Services(AWS)는 AWS 서비스에서 Red Hat OpenShift Service를 관리하는 반면 고객은 특정 책임을 공유합니다. AWS 서비스상의 Red Hat OpenShift Service는 원격으로 액세스되며 퍼블릭 클라우드 리소스에서 호스팅되고, 고객 소유의 AWS 계정에서 생성되며, Red Hat이 소유한 기본 플랫폼 및 데이터 보안을 보유하고 있습니다.

중요

cluster-admin 역할이 사용자에게 추가되면 Red Hat Enterprise Agreement 부록 4 (Online Subscription Services) 의 책임 및 제외 노트를 참조하십시오.

리소스	사고 및 운영 관리	변경 관리	액세스 및 ID 권한 부여	보안 및 규정 준수	재해 복구
고객 데이터	고객	고객	고객	고객	고객

리소스	사고 및 운영 관리	변경 관리	액세스 및 ID 권한 부여	보안 및 규정 준수	재해 복구
고객 애플리케이션	고객	고객	고객	고객	고객
개발자 서비스	고객	고객	고객	고객	고객
플랫폼 모니터링	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
로깅	Red Hat	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객	Red Hat
애플리케이션 네트워킹	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객	Red Hat	Red Hat
클러스터 네트워킹	Red Hat	Red Hat 및 고객	Red Hat 및 고객	Red Hat	Red Hat
가상 네트워킹	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객
컨트롤 플레인 및 인프라 노드	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
작업자 노드	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
클러스터 버전	Red Hat	Red Hat 및 고객	Red Hat	Red Hat	Red Hat
용량 관리	Red Hat	Red Hat 및 고객	Red Hat	Red Hat	Red Hat
가상 스토리지	Red Hat과 AWS	Red Hat과 AWS	Red Hat과 AWS	Red Hat과 AWS	Red Hat과 AWS
물리적 인프라 및 보안	AWS	AWS	AWS	AWS	AWS

3.2.2. 공유 책임 매트릭스

고객, Red Hat 및 AWS(Amazon Web Services)는 AWS 클러스터에서 Red Hat OpenShift Service의 모니터링 및 유지 관리에 대한 책임이 있습니다. 이 문서는 영역과 작업 단위를 설명합니다.

3.2.2.1. 사고 및 운영 관리

고객은 고객 애플리케이션 데이터의 사고 및 운영 관리를 담당하며 고객이 클러스터 네트워크 또는 가상 네트워크에 대해 구성한 사용자 지정 네트워킹을 담당합니다.

리소스	Red Hat과 AWS의 책임	고객 책임
애플리케이션 네트워킹	클라우드 로드 밸런서 및 기본 OpenShift 라우터 서비스를 모니터링하고 경고에 응답합니다.	• 서비스 로드 밸런서 끝점의 상태를 모니터링합니다. • 애플리케이션 경로 및 그 뒤에 있는 엔드 포인트의 상태를 모니터링합니다. • Red Hat에 시스템 중단 보고.
가상 네트워킹	기본 플랫폼 네트워킹에 필요한 클라우드 로드 밸런서, 서브넷 및 퍼블릭 클라우드 구성 요소를 모니터링하고 경고에 응답합니다.	잠재적인 문제 또는 보안 위협에 대한 VPC에서 VPC 연결, VPN 연결 또는 직접 연결을 통해 선택적으로 구성된 네트워크 트래픽을 모니터링합니다.

3.2.2.2. 변경 관리

Red Hat은 고객이 제어할 클러스터 인프라 및 서비스를 변경하고 컨트롤 플레인 노드, 인프라 노드 및 서비스, 작업자 노드의 버전을 유지 관리하는 역할을 담당합니다. 고객은 인프라 변경 요청을 시작하고 클러스터에서 선택적 서비스 및 네트워킹 구성을 설치 및 유지 관리하고 고객 데이터 및 고객 애플리케이션에 대한 모든 변경을 담당합니다.

리소스	Red Hat 책임	고객 책임
로깅	• 플랫폼 감사 로그를 중앙에서 집계하고 모니터링합니다. • 고객이 기본 애플리케이션 로깅을 위해 로깅 스택을 배포할 수 있도록 로깅 Operator를 제공하고 유지 관리합니다. • 고객 요청에 따라 감사 로그를 제공합니다.	• 클러스터에 선택적 기본 애플리케이션 로깅 Operator를 설치합니다. • 사이드카 컨테이너 또는 타사 로깅 애플리케이션과 같은 선택적 앱 로깅 솔루션을 설치, 구성 및 유지 관리합니다. • 로깅 스택 또는 클러스터의 안정성에 영향을 미치는 경우 고객 애플리케이션에서 생성되는 애플리케이션 로그의 크기와 빈도를 조정합니다. • 특정 문제 조사를 위해 지원 케이스를 통해 플랫폼 감사 로그를 요청합니다.

리소스	Red Hat 책임	고객 책임
애플리케이션 네트워킹	• 퍼블릭 클라우드 로드 밸런서를 설정합니다. 필요한 경우 프라이빗 로드 밸런서와 최대 1개의 추가 로드 밸런서를 설정하는 기능을 제공합니다. • 기본 OpenShift 라우터 서비스를 설정합니다. 라우터를 프라이빗으로 설정하고 하나의 추가 라우터 shard를 추가하는 기능을 제공합니다. • 기본 내부 pod 트래픽에 대한 OpenShift SDN 구성 요소를 설치, 구성 및 유지 관리합니다. • 고객이 **NetworkPolicy** 및 **EgressNetworkPolicy** (firewall) 오브젝트를 관리할 수 있는 기능을 제공합니다.	• **NetworkPolicy** 오브젝트를 사용하여 프로젝트 및 Pod 네트워크, Pod 수신 및 Pod 송신에 대한 기본 Pod 네트워크 권한을 구성합니다. • OpenShift Cluster Manager를 사용하여 기본 애플리케이션 경로에 대한 프라이빗 로드 밸런서를 요청합니다. • OpenShift Cluster Manager를 사용하여 최대 하나의 추가 퍼블릭 또는 프라이빗 라우터 shard 및 해당 로드 밸런서를 구성합니다. • 특정 서비스에 대한 추가 서비스 로드 밸런서를 요청하고 구성합니다. • 필요한 모든 DNS 전달 규칙을 구성합니다.
클러스터 네트워킹	• 퍼블릭 또는 프라이빗 서비스 엔드포인트와 같은 클러스터 관리 구성 요소와 가상 네트워킹 구성 요소와의 통합이 필요합니다. • 작업자, 인프라 및 컨트롤 플레인 노드 간의 내부 클러스터 통신에 필요한 내부 네트워킹 구성 요소를 설정합니다.	• 클러스터를 프로비저닝할 때 OpenShift Cluster Manager를 통해 필요한 경우 시스템 CIDR, 서비스 CIDR 및 Pod CIDR에 대한 기본이 아닌 IP 주소 범위 옵션을 제공합니다. • 클러스터 생성 시 또는 OpenShift Cluster Manager를 통해 클러스터 생성 후 API 서비스 엔드포인트를 공개 또는 비공개로 요청합니다.
가상 네트워킹	• 가상 프라이빗 클라우드, 서브넷, 로드 밸런서, 인터넷 게이트웨이, NAT 게이트웨이를 포함하여 클러스터를 프로비저닝하는 데 필요한 가상 네트워킹 구성 요소를 설정하고 구성합니다. • 고객이 온프레미스 리소스와 VPC 연결, OpenShift Cluster Manager를 통해 필요에 따라 직접 연결을 관리할 수 있는 기능을 제공합니다. • 고객이 서비스 로드 밸런서와 함께 사용할 퍼블릭 클라우드 로드 밸런서를 생성하고 배포할 수 있습니다.	• VPC에서 VPC 연결, VPN 연결 또는 직접 연결과 같은 선택적 퍼블릭 클라우드 네트워킹 구성 요소를 설정하고 유지 관리합니다. • 특정 서비스에 대한 추가 서비스 로드 밸런서를 요청하고 구성합니다.

리소스	Red Hat 책임	고객 책임
클러스터 버전	• 업그레이드 스케줄링 프로세스를 활성화합니다. • 업그레이드 진행 상황을 모니터링하고 발생한 모든 문제를 해결합니다. • 마이너 및 유지 관리 업그레이드를 위해 변경 로그 및 릴리스 정보를 게시합니다.	• 유지 관리 버전 업그레이드를 즉시 예약하거나 향후 자동 업그레이드가 가능합니다. • 마이너 버전 업그레이드를 승인하고 예약합니다. • 클러스터 버전이 지원되는 마이너 버전을 사용하고 있는지 확인합니다. • 마이너 및 유지 관리 버전에서 고객 애플리케이션을 테스트하여 호환성을 보장합니다.
용량 관리	• 컨트롤 플레인 사용을 모니터링합니다. 컨트롤 플레인에는 컨트롤 플레인 노드와 인프라 노드가 포함됩니다. • 컨트롤 플레인 노드의 확장 및 크기를 조정하여 서비스 품질을 유지합니다.	• 작업자 노드 사용률을 모니터링하고 적절한 경우 자동 확장 기능을 활성화합니다. • 클러스터의 스케일링 전략을 결정합니다. 머신 풀에 대한 자세한 내용은 추가 리소스를 참조하십시오. • 제공된 OpenShift Cluster Manager 제어를 사용하여 필요에 따라 추가 작업자 노드를 추가하거나 제거합니다. • 클러스터 리소스 요구 사항에 대한 Red Hat 알림에 응답합니다.

3.2.2.3. 액세스 및 ID 권한 부여

액세스 및 ID 권한 부여 매트릭스에는 클러스터, 애플리케이션 및 인프라 리소스에 대한 권한 있는 액세스를 관리하는 책임이 포함됩니다. 여기에는 액세스 제어 메커니즘, 인증, 권한 부여 및 리소스에 대한 액세스 관리와 같은 작업이 포함됩니다.

리소스	Red Hat 책임	고객 책임
로깅	• 플랫폼 감사 로그를 위해 업계 표준 기반 계층화된 내부 액세스 프로세스를 준수합니다. • 기본 OpenShift RBAC 기능을 제공합니다.	• 프로젝트에 대한 액세스 권한을 제어하고 프로젝트의 애플리케이션 로그를 확장함으로써 OpenShift RBAC를 구성합니다. • 타사 또는 사용자 지정 애플리케이션 로깅 솔루션의 경우 고객은 액세스 관리를 담당합니다.

리소스	Red Hat 책임	고객 책임
애플리케이션 네트워킹	네이티브 OpenShift RBAC 및 **dedicated-admin** 기능을 제공합니다.	• 필요에 따라 경로 구성에 대한 액세스를 제어하도록 OpenShift **dedicated-admin** 및 RBAC를 구성합니다. • OpenShift Cluster Manager에 대한 액세스 권한을 부여하도록 Red Hat의 조직 관리자를 관리합니다. 클러스터 관리자는 라우터 옵션을 구성하고 서비스 로드 밸런서 할당량을 제공하는 데 사용됩니다.
클러스터 네트워킹	• OpenShift Cluster Manager를 통해 고객 액세스 제어 제공. • 네이티브 OpenShift RBAC 및 **dedicated-admin** 기능을 제공합니다.	• Red Hat 계정의 Red Hat 조직 멤버십을 관리합니다. • OpenShift Cluster Manager에 대한 액세스 권한을 부여하도록 Red Hat의 조직 관리자를 관리합니다. • 필요에 따라 경로 구성에 대한 액세스를 제어하도록 OpenShift **dedicated-admin** 및 RBAC를 구성합니다.
가상 네트워킹	OpenShift Cluster Manager를 통해 고객 액세스 제어 제공.	OpenShift Cluster Manager를 통해 퍼블릭 클라우드 구성 요소에 대한 선택적 사용자 액세스를 관리합니다.

3.2.2.4. 보안 및 규정 준수

다음은 규정 준수와 관련된 책임 및 제어입니다.

리소스	Red Hat 책임	고객 책임

리소스	Red Hat 책임	고객 책임
로깅	클러스터 감사 로그를 Red Hat SIEM에 전송하여 보안 이벤트를 분석합니다. 법의학 분석을 지원하기 위해 정의된 기간 동안 감사 로그를 유지합니다.	보안 이벤트에 대한 애플리케이션 로그를 분석합니다. 기본 로깅 스택에서 제공하는 것보다 오래 보존해야 하는 경우 로깅 사이드카 컨테이너 또는 타사 로깅 애플리케이션을 통해 애플리케이션 로그를 외부 엔드포인트에 보냅니다.
가상 네트워킹	• 잠재적인 문제 및 보안 위협에 대해 가상 네트워킹 구성 요소를 모니터링합니다. • 추가 모니터링 및 보호를 위해 추가 퍼블릭 클라우드 공급자 툴을 활용합니다.	• 잠재적인 문제 및 보안 위협에 대해 구성된 선택적 가상 네트워킹 구성 요소를 모니터링합니다. • 필요에 따라 필요한 방화벽 규칙 또는 데이터 센터 보호를 구성합니다.

3.2.2.5. 재해 복구

재해 복구에는 데이터 및 구성 백업, 재해 복구 환경에 데이터 및 구성 복제, 재해 이벤트에 대한 장애 조치(failover)가 포함됩니다.

리소스	Red Hat 책임	고객 책임
가상 네트워킹	플랫폼이 작동하는 데 필요한 영향을 받는 가상 네트워크 구성 요소를 복원하거나 다시 생성합니다.	• 퍼블릭 클라우드 공급자가 권장하는 대로 중단을 방지할 수 있는 터널을 두 개 이상 사용하여 가상 네트워킹 연결을 구성합니다. • 여러 클러스터와 함께 글로벌 로드 밸런서를 사용하는 경우 페일오버 DNS 및 로드 밸런싱을 유지합니다.

추가 리소스

- 머신 풀 정보

3.2.3. 데이터 및 애플리케이션에 대한 고객 책임

고객은 AWS의 Red Hat OpenShift Service에 배포하는 애플리케이션, 워크로드 및 데이터를 담당합니다. 그러나 Red Hat은 고객이 플랫폼에서 데이터 및 애플리케이션을 관리할 수 있도록 다양한 도구를 제공합니다.

리소스	Red Hat 책임	고객 책임
고객 데이터	• 데이터 암호화를 위한 플랫폼 수준 표준을 유지 관리합니다. • 시크릿과 같은 애플리케이션 데이터를 관리하는 데 도움이 되도록 OpenShift 구성 요소를 제공합니다. • 타사 데이터 서비스인 AWS RDS와의 통합을 활성화하여 클러스터 및 클라우드 공급자 외부의 데이터를 저장 및 관리할 수 있습니다.	플랫폼에 저장된 모든 고객 데이터 및 고객 애플리케이션이 이러한 데이터를 소비하고 노출하는 방법에 대한 책임을 유지합니다.
고객 애플리케이션	• 고객이 컨테이너화된 애플리케이션을 배포 및 관리하기 위해 OpenShift 및 Kubernetes API에 액세스할 수 있도록 OpenShift 구성 요소가 설치된 클러스터를 프로비저닝합니다. • 고객 배포가 Red Hat Container Catalog 레지스트리에서 이미지를 가져올 수 있도록 이미지 가져오기 보안이 포함된 클러스터를 생성합니다. • 고객이 커뮤니티, 타사 및 Red Hat 서비스를 클러스터에 추가하기 위해 Operator를 설정하는 데 사용할 수 있는 OpenShift API를 제공합니다. • 고객 애플리케이션과 함께 사용할 영구 볼륨을 지원하는 스토리지 클래스 및 플러그인을 제공합니다. • 고객이 애플리케이션을 배포 및 관리하기 위해 클러스터에 애플리케이션 컨테이너 이미지를 안전하게 저장할 수 있도록 컨테이너 이미지 레지스트리를 제공합니다.	• 고객 및 타사 애플리케이션, 데이터 및 전체 라이프사이클에 대한 책임을 유지합니다. • 고객이 Operator 또는 외부 이미지를 사용하여 Red Hat, 커뮤니티, 타사, 자체 또는 기타 서비스를 클러스터에 추가하는 경우 고객은 이러한 서비스 및 Red Hat을 포함한 적절한 공급자와 협력하여 문제를 해결합니다. • 제공된 툴과 기능을 사용하여 구성 및 배포, 리소스 요청 및 제한 유지, 애플리케이션 실행을 위한 충분한 리소스를 확보할 클러스터 크기, 권한을 설정하고, 다른 서비스와 통합하며, 외부적으로 제공하는 이미지 스트림 또는 템플릿을 관리하고, 데이터를 저장, 백업 및 복원하며, 고가용성 및 복원 워크로드를 관리하는 것입니다. • 메트릭을 수집하고 경고를 생성하기 위한 설치 및 운영 소프트웨어 등 AWS의 Red Hat OpenShift Service에서 실행되는 애플리케이션 모니터링에 대한 책임을 유지합니다.

3.3. RED HAT OPENSHIFT SERVICE ON AWS 서비스 정의

이 문서에서는 ROSA(Red Hat OpenShift Service on AWS) 관리 서비스의 서비스 정의에 대해 간단히 설명합니다.

3.3.1. 계정 관리

이 섹션에서는 AWS 계정 관리의 Red Hat OpenShift Service 서비스 정의에 대해 설명합니다.

3.3.1.1. 청구

AWS의 Red Hat OpenShift Service는 OpenShift 서비스용 로드 밸런서, 스토리지, EC2 인스턴스, 기타 구성 요소 및 Red Hat 서브스크립션과 같은 서비스에서 사용하는 AWS(Amazon Web Services)를 통해 청구됩니다.

추가 Red Hat 소프트웨어는 별도로 구매해야 합니다.

3.3.1.2. 클러스터 셀프 서비스

고객은 다음을 포함하여 클러스터를 셀프 서비스할 수 있습니다.

- 클러스터 생성
- 클러스터 삭제
- ID 공급자 추가 또는 제거
- 승격된 그룹에서 사용자 추가 또는 제거
- 클러스터 개인 정보 보호 설정
- 머신 풀 추가 또는 제거 및 자동 스케일링 구성
- 업그레이드 정책 정의

이러한 작업은 **rosa** CLI 유틸리티를 사용하여 셀프 서비스를 수행할 수 있습니다.

3.3.1.3. 인스턴스 유형

단일 가용성 영역 클러스터에는 최소 3개의 컨트롤 플레인 노드, 인프라 노드 2개, 단일 가용성 영역에 배포된 작업자 노드 2개가 필요합니다.

여러 가용성 영역 클러스터에는 최소 3개의 컨트롤 플레인 노드가 필요합니다. 인프라 노드 3개와 작업자 노드 3개 적절한 노드 배포를 유지하려면 3개의 여러 노드에서 추가 노드를 구입해야 합니다.

AWS 클러스터의 모든 Red Hat OpenShift Service는 최대 180개의 작업자 노드를 지원합니다.

참고

클러스터를 생성한 후에는 **Default** 머신 풀 노드 유형 및 크기는 변경할 수 없습니다.

컨트롤 플레인 및 인프라 노드는 Red Hat에서 배포 및 관리합니다. 클라우드 공급자 콘솔을 통해 기본 인프라를 종료하면 지원되지 않으며 데이터가 손실될 수 있습니다. etcd 및 API 관련 워크로드를 처리하는 컨트롤 플레인 노드가 3개 이상 있습니다. 메트릭, 라우팅, 웹 콘솔 및 기타 워크로드를 처리하는 인프라 노드가 두 개 이상 있습니다. 제어 및 인프라 노드에서 워크로드를 실행하지 않아야 합니다. 실행하려는 워크로드는 작업자 노드에 배포해야 합니다. 작업자 노드에 배포해야 하는 Red Hat 워크로드에 대한 자세한 내용은 아래 Red Hat Operator 지원 섹션을 참조하십시오.

참고

약 1개의 vCPU 코어 및 1GiB의 메모리가 각 작업자 노드에 예약되며 할당 가능한 리소스에서 제거됩니다. 기본 플랫폼에 필요한 프로세스를 실행하려면 이 리소스 예약이 필요합니다. 이러한 프로세스에는 udev, kubelet 및 컨테이너 런타임과 같은 시스템 데몬이 포함됩니다. 예약된 리소스는 커널 예약도 계정합니다.

감사 로그 집계, 지표 수집, DNS, 이미지 레지스트리, SDN 등과 같은 OpenShift Container Platform 코어 시스템은 클러스터의 안정성과 유지 관리를 위해 추가 할당 가능한 리소스를 사용할 수 있습니다. 소비되는 추가 리소스는 사용량에 따라 다를 수 있습니다.

자세한 내용은 Kubernetes 설명서 를 참조하십시오.

중요

AWS 버전 4.8.35의 Red Hat OpenShift Service, 4.9.26, 4.10.6, AWS 기본값인 Red Hat OpenShift Service는 **4096** 입니다. 이 PID 제한을 활성화하려면 AWS 클러스터에서 이러한 버전 이상으로 Red Hat OpenShift Service를 업그레이드해야 합니다. 이전 버전이 있는 AWS 클러스터의 Red Hat OpenShift Service는 기본 PID 제한 **1024** 를 사용합니다.

AWS 클러스터의 모든 Red Hat OpenShift Service에서 Pod별 PID 제한을 구성할 수 없습니다.

추가 리소스

- Red Hat Operator 지원

3.3.1.4. AWS 인스턴스 유형

AWS의 Red Hat OpenShift Service는 다음과 같은 작업자 노드 인스턴스 유형 및 크기를 제공합니다.

예 3.1. 일반 목적

- m5.metal (96ovn vCPU, 384GiB)
- m5.xlarge (4 vCPU, 16GiB)
- m5.2xlarge (8 vCPU, 32GiB)
- m5.4xlarge (16 vCPU, 64GiB)
- m5.8xlarge(32 vCPU, 128GiB)
- m5.12xlarge(48 vCPU, 192GiB)
- m5.16xlarge(64 vCPU, 256GiB)
- m5.24xlarge (96 vCPU, 384GiB)
- m5a.xlarge (4 vCPU, 16GiB)
- m5a.2xlarge (8 vCPU, 32GiB)
- m5a.4xlarge (16 vCPU, 64GiB)
- m5a.8xlarge(32 vCPU, 128GiB)

- m5a.12xlarge(48 vCPU, 192GiB)
- m5a.16xlarge(64 vCPU, 256GiB)
- m5a.24xlarge (96 vCPU, 384GiB)
- m5ad.xlarge (4 vCPU, 16GiB)
- m5ad.2xlarge (8 vCPU, 32GiB)
- m5ad.4xlarge (16 vCPU, 64GiB)
- m5ad.8xlarge(32 vCPU, 128GiB)
- m5ad.12xlarge (48 vCPU, 192GiB)
- m5ad.16xlarge (64 vCPU, 256GiB)
- m5ad.24xlarge (96 vCPU, 384GiB)
- m5d.metal (96ovn vCPU, 384GiB)
- m5d.xlarge (4 vCPU, 16GiB)
- m5d.2xlarge (8 vCPU, 32GiB)
- m5d.4xlarge (16 vCPU, 64GiB)
- m5d.8xlarge(32 vCPU, 128GiB)
- m5d.12xlarge(48 vCPU, 192GiB)
- m5d.16xlarge(64 vCPU, 256GiB)
- m5d.24xlarge(96 vCPU, 384GiB)
- m5n.metal (96 vCPU, 384GiB)
- m5n.xlarge (4 vCPU, 16GiB)
- m5n.2xlarge (8 vCPU, 32GiB)
- m5n.4xlarge (16 vCPU, 64GiB)
- m5n.8xlarge(32 vCPU, 128GiB)
- m5n.12xlarge(48 vCPU, 192GiB)
- m5n.16xlarge(64 vCPU, 256GiB)
- m5n.24xlarge (96 vCPU, 384GiB)
- m5dn.metal (96 vCPU, 384GiB)
- m5dn.xlarge (4 vCPU, 16GiB)
- m5dn.2xlarge (8 vCPU, 32GiB)

- m5dn.4xlarge (16 vCPU, 64GiB)
- m5dn.8xlarge(32 vCPU, 128GiB)
- m5dn.12xlarge(48 vCPU, 192GiB)
- m5dn.16xlarge(64 vCPU, 256GiB)
- m5dn.24xlarge (96 vCPU, 384GiB)
- m5zn.metal (48 vCPU, 192GiB)
- m5zn.xlarge (4 vCPU, 16GiB)
- m5zn.2xlarge (8 vCPU, 32GiB)
- m5zn.3xlarge (12 vCPU, 48GiB)
- m5zn.6xlarge (24 vCPU, 96GiB)
- m5zn.12xlarge (48 vCPU, 192GiB)
- m6a.xlarge (4 vCPU, 16GiB)
- m6a.2xlarge (8 vCPU, 32GiB)
- m6a.4xlarge (16 vCPU, 64GiB)
- m6a.8xlarge(32 vCPU, 128GiB)
- m6a.12xlarge(48 vCPU, 192GiB)
- m6a.16xlarge(64 vCPU, 256GiB)
- m6a.24xlarge (96 vCPU, 384GiB)
- m6a.32xlarge(128 vCPU, 512GiB)
- m6a.48xlarge(192 vCPU, 768GiB)
- m6i.metal (128 vCPU, 512GiB)
- m6i.xlarge (4 vCPU, 16GiB)
- m6i.2xlarge (8 vCPU, 32GiB)
- m6i.4xlarge (16 vCPU, 64GiB)
- m6i.8xlarge(32 vCPU, 128GiB)
- m6i.12xlarge (48 vCPU, 192GiB)
- m6i.16xlarge(64 vCPU, 256GiB)
- m6i.24xlarge (96 vCPU, 384GiB)
- m6i.32xlarge(128 vCPU, 512GiB)

- m6id.xlarge (4 vCPU, 16GiB)
- m6id.2xlarge (8 vCPU, 32GiB)
- m6id.4xlarge (16 vCPU, 64GiB)
- m6id.8xlarge(32 vCPU, 128GiB)
- m6id.12xlarge (48 vCPU, 192GiB)
- m6id.16xlarge (64 vCPU, 256GiB)
- m6id.24xlarge (96 vCPU, 384GiB)
- m6id.32xlarge(128 vCPU, 512GiB)

이러한 인스턴스 유형은 48개의 물리적 코어에서 96개의 논리 프로세서를 제공합니다. 두 개의 물리적 Intel 소켓이 있는 단일 서버에서 실행됩니다.

예 3.2. Burstable 일반 목적

- t3.xlarge (4 vCPU, 16GiB)
- t3.2xlarge (8 vCPU, 32GiB)
- t3a.xlarge (4 vCPU, 16GiB)
- t3a.2xlarge (8 vCPU, 32GiB)

예 3.3. 메모리 집약적

- x1.16xlarge(64 vCPU, 976GiB)
- X1.32xlarge(128 vCPU, 1952GiB)
- X1e.xlarge (4 vCPU, 122GiB)
- X1e.2xlarge (8 vCPU, 244GiB)
- X1e.4xlarge (16 vCPU, 488GiB)
- X1e.8xlarge(32 vCPU, 976GiB)
- X1e.16xlarge(64 vCPU, 1,952GiB)
- X1e.32xlarge(128 vCPU, 3,904GiB)
- x2idn.16xlarge (64 vCPU, 1024GiB)
- X2idn.24xlarge (96 vCPU, 1536GiB)
- x2idn.32xlarge(128 vCPU, 2048GiB)
- x2iedn.xlarge (4 vCPU, 128GiB)

- X2iedn.2xlarge (8 vCPU, 256GiB)
- X2iedn.4xlarge (16 vCPU, 512GiB)
- X2iedn.8xlarge(32 vCPU, 1024GiB)
- x2iedn.16xlarge (64 vCPU, 2048GiB)
- X2iedn.24xlarge (96 vCPU, 3072GiB)
- x2iedn.32xlarge(128 vCPU, 4096GiB)
- X2iezn.2xlarge (8 vCPU, 256GiB)
- X2iezn.4xlarge (16vCPU, 512GiB)
- X2iezn.6xlarge (24vCPU, 768GiB)
- X2iezn.8xlarge(32vCPU, 1,024GiB)
- X2iezn.12xlarge (48vCPU, 1,536GiB)
- x2idn.metal(128vCPU, 2,048GiB)
- x2iedn.metal (128vCPU, 4,096GiB)
- x2iezn.metal (48 vCPU, 1,536GiB)

예 3.4. 최적화된 메모리

- r4.xlarge (4 vCPU, 30.5GiB)
- r4.2xlarge (8 vCPU, 61GiB)
- r4.4xlarge (16 vCPU, 122GiB)
- r4.8xlarge(32 vCPU, 244GiB)
- r4.16xlarge(64 vCPU, 488GiB)
- r5.metal (96ECDHE vCPU, 768GiB)
- r5.xlarge (4 vCPU, 32GiB)
- r5.2xlarge (8 vCPU, 64GiB)
- r5.4xlarge (16 vCPU, 128GiB)
- r5.8xlarge(32 vCPU, 256GiB)
- r5.12xlarge (48 vCPU, 384GiB)
- r5.16xlarge(64 vCPU, 512GiB)
- r5.24xlarge (96 vCPU, 768GiB)
- r5a.xlarge (4 vCPU, 32GiB)

- r5a.2xlarge (8 vCPU, 64GiB)
- r5a.4xlarge (16 vCPU, 128GiB)
- r5a.8xlarge(32 vCPU, 256GiB)
- r5a.12xlarge(48 vCPU, 384GiB)
- r5a.16xlarge(64 vCPU, 512GiB)
- r5a.24xlarge(96 vCPU, 768GiB)
- r5ad.xlarge (4 vCPU, 32GiB)
- r5ad.2xlarge (8 vCPU, 64GiB)
- r5ad.4xlarge (16 vCPU, 128GiB)
- r5ad.8xlarge(32 vCPU, 256GiB)
- r5ad.12xlarge(48 vCPU, 384GiB)
- r5ad.16xlarge(64 vCPU, 512GiB)
- r5ad.24xlarge (96 vCPU, 768GiB)
- r5d.metal (96ECDHE vCPU, 768GiB)
- r5d.xlarge (4 vCPU, 32GiB)
- r5d.2xlarge (8 vCPU, 64GiB)
- r5d.4xlarge (16 vCPU, 128GiB)
- r5d.8xlarge(32 vCPU, 256GiB)
- r5d.12xlarge(48 vCPU, 384GiB)
- r5d.16xlarge(64 vCPU, 512GiB)
- r5d.24xlarge(96 vCPU, 768GiB)
- r5n.metal (96 vCPU, 768GiB)
- r5n.xlarge (4 vCPU, 32GiB)
- r5n.2xlarge (8 vCPU, 64GiB)
- r5n.4xlarge (16 vCPU, 128GiB)
- r5n.8xlarge(32 vCPU, 256GiB)
- r5n.12xlarge(48 vCPU, 384GiB)
- r5n.16xlarge(64 vCPU, 512GiB)
- r5n.24xlarge (96 vCPU, 768GiB)

- r5dn.metal (96 vCPU, 768GiB)
- r5dn.xlarge (4 vCPU, 32GiB)
- r5dn.2xlarge (8 vCPU, 64GiB)
- r5dn.4xlarge (16 vCPU, 128GiB)
- r5dn.8xlarge(32 vCPU, 256GiB)
- r5dn.12xlarge(48 vCPU, 384GiB)
- r5dn.16xlarge(64 vCPU, 512GiB)
- r5dn.24xlarge (96 vCPU, 768GiB)
- r6a.xlarge (4 vCPU, 32GiB)
- r6a.2xlarge (8 vCPU, 64GiB)
- r6a.4xlarge (16 vCPU, 128GiB)
- r6a.8xlarge(32 vCPU, 256GiB)
- r6a.12xlarge(48 vCPU, 384GiB)
- r6a.16xlarge(64 vCPU, 512GiB)
- r6a.24xlarge (96 vCPU, 768GiB)
- r6a.32xlarge(128 vCPU, 1,024GiB)
- r6a.48xlarge(192 vCPU, 1,536GiB)
- r6i.metal (128 vCPU, 1,024GiB)
- r6i.xlarge (4 vCPU, 32GiB)
- r6i.2xlarge (8 vCPU, 64GiB)
- r6i.4xlarge (16 vCPU, 128GiB)
- r6i.8xlarge(32 vCPU, 256GiB)
- r6i.12xlarge(48 vCPU, 384GiB)
- r6i.16xlarge(64 vCPU, 512GiB)
- r6i.24xlarge (96 vCPU, 768GiB)
- r6i.32xlarge(128 vCPU, 1,024GiB)
- r6id.xlarge (4 vCPU, 32GiB)
- r6id.2xlarge (8 vCPU, 64GiB)
- r6id.4xlarge (16 vCPU, 128GiB)

- r6id.8xlarge(32 vCPU, 256GiB)
- r6id.12xlarge (48 vCPU, 384GiB)
- r6id.16xlarge (64 vCPU, 512GiB)
- r6id.24xlarge (96 vCPU, 768GiB)
- r6id.32xlarge(128 vCPU, 1,024GiB)
- z1d.metal (48ECDHE vCPU, 384GiB)
- z1d.xlarge (4 vCPU, 32GiB)
- z1d.2xlarge (8 vCPU, 64GiB)
- z1d.3xlarge (12 vCPU, 96GiB)
- z1d.6xlarge (24 vCPU, 192GiB)
- z1d.12xlarge(48 vCPU, 384GiB)

이러한 인스턴스 유형은 48개의 물리적 코어에서 96개의 논리 프로세서를 제공합니다. 두 개의 물리적 Intel 소켓이 있는 단일 서버에서 실행됩니다.

이 인스턴스 유형은 24개의 물리적 코어에서 48개의 논리 프로세서를 제공합니다.

예 3.5. 가속화된 컴퓨팅

- p3.2xlarge (8 vCPU, 61GiB)
- p3.8xlarge(32 vCPU, 244GiB)
- p3.16xlarge(64 vCPU, 488GiB)
- p3dn.24xlarge (96 vCPU, 768GiB)
- p4d.24xlarge(96 vCPU, 1,152GiB)
- g4dn.xlarge (4 vCPU, 16GiB)
- g4dn.2xlarge (8 vCPU, 32GiB)
- g4dn.4xlarge (16 vCPU, 64GiB)
- g4dn.8xlarge(32 vCPU, 128GiB)
- g4dn.12xlarge(48 vCPU, 192GiB)
- g4dn.16xlarge(64 vCPU, 256GiB)
- g4dn.metal (96 vCPU, 384GiB)
- g5.xlarge (4 vCPU, 16GiB)
- g5.2xlarge (8 vCPU, 32GiB)

- g5.4xlarge (16 vCPU, 64GiB)
- g5.8xlarge(32 vCPU, 128GiB)
- g5.16xlarge(64 vCPU, 256GiB)
- g5.12xlarge(48 vCPU, 192GiB)
- g5.24xlarge(96 vCPU, 384GiB)
- g5.48xlarge(192 vCPU, 768GiB)
- dl1.24xlarge (96 vCPU, 768GiB)

ECDHE Intel specific; Nvidia의 적용을 받지 않음

AWS에서는 GPU 인스턴스 유형 소프트웨어 스택에 대한 지원이 제공됩니다. AWS 서비스 할당량이 원하는 GPU 인스턴스 유형을 수용할 수 있는지 확인합니다.

예 3.6. 컴퓨팅 최적화

- c5.metal (96 vCPU, 192GiB)
- c5.xlarge (4 vCPU, 8GiB)
- c5.2xlarge (8 vCPU, 16GiB)
- c5.4xlarge (16 vCPU, 32GiB)
- c5.9xlarge(36 vCPU, 72GiB)
- c5.12xlarge(48 vCPU, 96GiB)
- c5.18xlarge (72 vCPU, 144GiB)
- c5.24xlarge (96 vCPU, 192GiB)
- c5d.metal (96 vCPU, 192GiB)
- c5d.xlarge (4 vCPU, 8GiB)
- c5d.2xlarge (8 vCPU, 16GiB)
- c5d.4xlarge (16 vCPU, 32GiB)
- c5d.9xlarge(36 vCPU, 72GiB)
- c5d.12xlarge(48 vCPU, 96GiB)
- c5d.18xlarge(72 vCPU, 144GiB)
- c5d.24xlarge (96 vCPU, 192GiB)
- c5a.xlarge (4 vCPU, 8GiB)
- c5a.2xlarge (8 vCPU, 16GiB)

- c5a.4xlarge (16 vCPU, 32GiB)
- c5a.8xlarge(32 vCPU, 64GiB)
- c5a.12xlarge(48 vCPU, 96GiB)
- c5a.16xlarge(64 vCPU, 128GiB)
- c5a.24xlarge (96 vCPU, 192GiB)
- c5ad.xlarge (4 vCPU, 8GiB)
- c5ad.2xlarge (8 vCPU, 16GiB)
- c5ad.4xlarge (16 vCPU, 32GiB)
- c5ad.8xlarge(32 vCPU, 64GiB)
- c5ad.12xlarge(48 vCPU, 96GiB)
- c5ad.16xlarge (64 vCPU, 128GiB)
- c5ad.24xlarge (96 vCPU, 192GiB)
- c5n.metal (72 vCPU, 192GiB)
- c5n.xlarge (4 vCPU, 10.5GiB)
- c5n.2xlarge (8 vCPU, 21GiB)
- c5n.4xlarge (16 vCPU, 42GiB)
- c5n.9xlarge(36 vCPU, 96GiB)
- c5n.18xlarge (72 vCPU, 192GiB)
- c6a.xlarge (4 vCPU, 8GiB)
- c6a.2xlarge (8 vCPU, 16GiB)
- c6a.4xlarge (16 vCPU, 32GiB)
- c6a.8xlarge(32 vCPU, 64GiB)
- c6a.12xlarge(48 vCPU, 96GiB)
- c6a.16xlarge(64 vCPU, 128GiB)
- c6a.24xlarge (96 vCPU, 192GiB)
- c6a.32xlarge(128 vCPU, 256GiB)
- c6a.48xlarge(192 vCPU, 384GiB)
- c6i.metal (128 vCPU, 256GiB)
- c6i.xlarge (4 vCPU, 8GiB)

- c6i.2xlarge (8 vCPU, 16GiB)
- c6i.4xlarge (16 vCPU, 32GiB)
- c6i.8xlarge(32 vCPU, 64GiB)
- c6i.12xlarge (48 vCPU, 96GiB)
- c6i.16xlarge (64 vCPU, 128GiB)
- c6i.24xlarge (96 vCPU, 192GiB)
- c6i.32xlarge(128 vCPU, 256GiB)
- c6id.xlarge (4 vCPU, 8GiB)
- c6id.2xlarge (8 vCPU, 16GiB)
- c6id.4xlarge (16 vCPU, 32GiB)
- c6id.8xlarge(32 vCPU, 64GiB)
- c6id.12xlarge (48 vCPU, 96GiB)
- c6id.16xlarge (64 vCPU, 128GiB)
- c6id.24xlarge (96 vCPU, 192GiB)
- c6id.32xlarge(128 vCPU, 256GiB)

예 3.7. 최적화된 스토리지

- i3.metal (72ECDHE vCPU, 512GiB)
- i3.xlarge (4 vCPU, 30.5GiB)
- i3.2xlarge (8 vCPU, 61GiB)
- i3.4xlarge (16 vCPU, 122GiB)
- i3.8xlarge(32 vCPU, 244GiB)
- i3.16xlarge(64 vCPU, 488GiB)
- i3en.metal (96 vCPU, 768GiB)
- i3en.xlarge (4 vCPU, 32GiB)
- i3en.2xlarge (8 vCPU, 64GiB)
- i3en.3xlarge (12 vCPU, 96GiB)
- i3en.6xlarge (24 vCPU, 192GiB)
- i3en.12xlarge(48 vCPU, 384GiB)
- i3en.24xlarge (96 vCPU, 768GiB)

> 이 인스턴스 유형은 36 개의 물리적 코어에서 72 개의 논리 프로세서를 제공합니다.

참고

가상 인스턴스 유형은 ".metal" 인스턴스 유형보다 더 빨리 초기화됩니다.

추가 리소스

- AWS 인스턴스 유형

3.3.1.5. 지역 및 가용성 영역

다음 AWS 리전은 Red Hat OpenShift 4에서 지원되며 AWS의 Red Hat OpenShift Service에서 지원됩니다. 참고: OpenShift 4에 대한 지원에 관계없이 중국 및 GovCloud (US) 리전은 지원되지 않습니다.

- af-south-1 (AWS opt-in 필요)
- ap-east-1 (홍콩, AWS 옵트인 필요)
- ap-northeast-1(도쿄)
- ap-northeast-2(서울)
- ap-northeast-3 (오사카)
- ap-south-1(뭄바이)
- ap-southeast-1(싱가포르)
- ap-southeast-2(시드니)
- ap-southeast-3 (AWS 옵트인 필요)
- ca-central-1 (캐나다)
- eu-central-1(프랑크푸르트)
- eu-north-1(스톡홀름)
- eu-south-1 (AWS 옵트인 필요)
- eu-west-1(아일랜드)
- eu-west-2(런던)
- eu-west-3(파리)
- me-south-1 (Bahrain, AWS opt-in 필요)
- sa-east-1(상파울루)
- us-east-1(버지니아 북부)
- us-east-2(오하이오)

- us-west-1(캘리포니아 북부)
- us-west-2(오레곤)

여러 가용성 영역 클러스터는 가용성 영역이 3개 이상인 지역에만 배포할 수 있습니다. 자세한 내용은 AWS 문서의 리전 및 가용 영역 섹션을 참조하십시오.

AWS의 새로운 Red Hat OpenShift Service는 단일 리전의 설치 관리자 생성 또는 기존 VPC(Virtual Private Cloud) 내에 설치됩니다. 이 옵션을 통해 단일 가용성 영역(Single-AZ) 또는 여러 가용성 영역(Multi-AZ)에 배포할 수 있습니다. 이를 통해 클러스터 수준 네트워크 및 리소스 분리를 제공하고 VPN 연결 및 VPC 피어링과 같은 클라우드 공급자 VPC 설정을 활성화합니다. PV(영구 볼륨)는 AWS EBS(Elastic Block Storage)에서 지원하며, 프로비저닝되는 가용성 영역에 따라 다릅니다. PVC(영구 볼륨 클레임)는 예약할 수 없는 Pod를 방지하기 위해 연결된 Pod 리소스가 특정 가용 영역에 할당될 때까지 볼륨에 바인딩되지 않습니다. 가용성 영역별 리소스는 동일한 가용성 영역의 리소스에서만 사용할 수 있습니다.

주의

클러스터를 배포한 후에는 단일 또는 여러 가용성 영역의 리전 및 선택 사항을 변경할 수 없습니다.

3.3.1.6. SLA(서비스 수준 계약)

서비스 자체에 대한 SLA는 Red Hat Enterprise Agreement 부록 4 (Online Subscription Services)의 부록 4 에 정의되어 있습니다.

3.3.1.7. 제한된 지원 상태

클러스터가 *제한된 지원* 상태로 전환되면 Red Hat은 더 이상 클러스터를 적극적으로 모니터링하지 않으며 SLA는 더 이상 적용되지 않으며 SLA에 대해 요청된 자립이 거부됩니다. 이는 더 이상 제품 지원이 없다는 의미는 아닙니다. 일부 경우 위반 요인을 수정하면 클러스터가 완전히 지원되는 상태로 돌아갈 수 있습니다. 그러나 다른 경우에는 클러스터를 삭제하고 다시 생성해야 할 수도 있습니다.

다음 시나리오를 포함하여 여러 가지 이유로 클러스터가 제한된 지원 상태로 이동할 수 있습니다.

라이프 사이클 종료일 전에 클러스터를 지원되는 버전으로 업그레이드하지 않는 경우

Red Hat은 라이프 사이클 종료일 이후 버전에 대해 런타임 또는 SLA를 보장하지 않습니다. 지속적인 지원을 받으려면 종료일 이전에 클러스터를 지원되는 버전으로 업그레이드하십시오. 라이프 사이클 종료일 이전에 클러스터를 업그레이드하지 않으면 클러스터가 지원되는 버전으로 업그레이드될 때까지 제한된 지원 상태로 전환됩니다.
Red Hat은 지원되지 않는 버전에서 지원되는 버전으로 업그레이드하기 위해 상업적으로 합리적인 지원을 제공합니다. 그러나 지원되는 업그레이드 경로를 더 이상 사용할 수 없는 경우 새 클러스터를 생성하고 워크로드를 마이그레이션해야 할 수 있습니다.

AWS 구성 요소에서 기본 Red Hat OpenShift Service 또는 Red Hat에서 설치 및 관리하는 기타 구성 요소를 제거하거나 교체하는 경우

클러스터 관리자 권한을 사용한 경우 Red Hat은 인프라 서비스, 서비스 가용성 또는 데이터 손실에 영향을 미치는 사용자 또는 사용자의 권한이 있는 사용자의 조치에 대해 책임을 지지 않습니다. Red Hat에서 이러한 작업을 감지하면 클러스터가 제한된 지원 상태로 전환될 수 있습니다. Red Hat은 상태 변경을 알리며 클러스터를 삭제하고 다시 생성해야 할 수 있는 수정 단계를 탐색할 수 있는 조치를 되돌리거나 지원 케이스를 생성해야 합니다.

클러스터가 제한된 지원 상태로 이동하거나 추가 지원이 필요한 특정 작업에 대한 질문이 있는 경우 지원 티켓을 엽니다.

3.3.1.8. 지원

AWS의 Red Hat OpenShift Service에는 Red Hat 고객 포털을 사용하여 액세스할 수 있는 Red Hat Premium 지원이 포함되어 있습니다.

지원 응답 시간은 Red Hat OpenShift Service on AWS SLA 를 참조하십시오.

AWS 지원은 AWS와 고객의 기존 지원 계약의 적용을 받습니다.

3.3.2. 로깅

AWS의 Red Hat OpenShift Service는 Amazon (AWS) 10.0.0.1에 선택적 통합 로그 전달 기능을 제공합니다.

3.3.2.1. 클러스터 감사 로깅

통합이 활성화된 경우 클러스터 감사 로그를 AWS3-4를 통해 사용할 수 있습니다. 통합이 활성화되지 않은 경우 지원 케이스를 열어 감사 로그를 요청할 수 있습니다.

3.3.2.2. 애플리케이션 로깅

STDOUT 으로 전송된 애플리케이션 로그는 Fluentd에 의해 수집되며 설치된 경우 클러스터 로깅 스택을 통해 AWS#177로 전달됩니다.

3.3.3. 모니터링

이 섹션에서는 AWS 모니터링 시 Red Hat OpenShift Service의 서비스 정의에 대해 설명합니다.

3.3.3.1. 클러스터 메트릭

AWS 클러스터의 Red Hat OpenShift Service에는 CPU, 메모리, 네트워크 기반 메트릭을 포함한 클러스터 모니터링을 위해 통합된 Prometheus 스택이 제공됩니다. 웹 콘솔을 통해 액세스할 수 있습니다. 또한 이러한 메트릭을 사용하면 AWS 사용자의 Red Hat OpenShift Service에서 제공하는 CPU 또는 메모리 메트릭을 기반으로 수평 Pod 자동 스케일링을 수행할 수 있습니다.

3.3.3.2. 클러스터 상태 알림

Red Hat은 OpenShift Cluster Manager에서 사용 가능한 클러스터 대시보드의 조합과 원래 클러스터를 배포한 연락처의 이메일 주소 및 고객이 지정한 추가 연락처로 전송된 이메일 알림을 통해 AWS 클러스터에서 Red Hat OpenShift Service의 상태 및 상태를 전달합니다.

3.3.4. 네트워킹

이 섹션에서는 AWS 네트워킹의 Red Hat OpenShift Service의 서비스 정의에 대해 설명합니다.

3.3.4.1. 애플리케이션용 사용자 정의 도메인

경로에 사용자 지정 호스트 이름을 사용하려면 CNAME(정규 이름) 레코드를 생성하여 DNS 공급자를 업데이트해야 합니다. CNAME 레코드는 OpenShift 표준 라우터 호스트 이름을 사용자 정의 도메인에 매핑해야 합니다. 경로를 생성한 후 OpenShift 정식 라우터 호스트 이름은 *경로 세부 정보* 페이지에 표시됩니

다. 또는 와일드카드 CNAME 레코드를 한 번 생성하여 지정된 호스트 이름의 모든 하위 도메인을 클러스터의 라우터로 라우팅할 수 있습니다.

3.3.4.2. 도메인 검증 인증서

AWS의 Red Hat OpenShift Service에는 클러스터의 내부 및 외부 서비스에 필요한 TLS 보안 인증서가 포함되어 있습니다. 외부 경로의 경우 각 클러스터에 제공 및 설치된 두 개의 TLS 와일드카드 인증서가 있습니다. 하나는 웹 콘솔과 라우팅 기본 호스트 이름이며 다른 하나는 API 엔드포인트용입니다. Let's Encrypt는 인증서에 사용되는 인증 기관입니다. 내부 API 끝점 과 같은 클러스터 내의 경로는 클러스터의 내장 인증 기관에서 서명한 TLS 인증서를 사용하며, TLS 인증서를 신뢰하기 위해 모든 Pod에서 CA 번들을 사용할 수 있어야 합니다.

3.3.4.3. 빌드를 위한 사용자 정의 인증 기관

AWS의 Red Hat OpenShift Service에서는 이미지 레지스트리에서 이미지를 가져올 때 빌드에서 신뢰할 사용자 정의 인증 기관을 사용할 수 있습니다.

3.3.4.4. 로드 밸런서

AWS의 Red Hat OpenShift Service는 최대 5개의 로드 밸런서를 사용합니다.

- 내부 클러스터 통신을 위해 트래픽의 균형을 조정하는 데 사용되는 내부 컨트롤 플레인 로드 밸런서입니다.
- OpenShift 및 Kubernetes API에 액세스하는 데 사용되는 외부 컨트롤 플레인 로드 밸런서입니다. OpenShift Cluster Manager에서 이 로드 밸런서를 비활성화할 수 있습니다. 이 로드 밸런서가 비활성화된 경우 Red Hat은 내부 컨트롤 플레인 로드 밸런서를 가리키도록 API DNS를 재구성합니다.
- Red Hat에서 클러스터 관리용으로 예약한 Red Hat의 외부 컨트롤 플레인 로드 밸런서입니다. 액세스는 엄격하게 제어되며 허용 목록에 있는 베스천 호스트에서만 통신이 가능합니다.
- URL의 **앱에** 표시된 기본 외부 라우터/수신 로드 밸런서입니다. OpenShift Cluster Manager에서 기본 로드 밸런서를 인터넷을 통해 공개적으로 액세스하거나 기존 개인 연결을 통해 비공개로만 액세스할 수 있도록 구성할 수 있습니다. 클러스터의 모든 애플리케이션 경로는 로깅 UI, 지표 API 및 레지스트리와 같은 클러스터 서비스를 포함하여 기본 라우터 로드 밸런서에 노출됩니다.
- 선택 사항: URL의 **apps2** 에 표시된 보조 애플리케이션 로드 밸런서인 보조 라우터/수신 로드 밸런서입니다. 보조 로드 밸런서는 인터넷을 통해 공개적으로 액세스하거나 기존 개인 연결을 통해 비공개로만 액세스할 수 있도록 OpenShift Cluster Manager에서 구성할 수 있습니다. **레이블 일치** 가 이 라우터 로드 밸런서에 구성된 경우 이 레이블과 일치하는 애플리케이션 경로만 이 라우터 로드 밸런서에 노출됩니다. 그렇지 않으면 모든 애플리케이션 경로도 이 라우터 로드 밸런서에 노출됩니다.
- 선택사항: 서비스용 로드 밸런서입니다. 서비스에 대해 비HTTP/SNI 트래픽 및 비표준 포트를 활성화합니다. 이러한 로드 밸런서는 AWS의 Red Hat OpenShift Service에서 실행되는 서비스에 매핑되어 비HTTP/SNI 트래픽 또는 비표준 포트 사용과 같은 고급 수신 기능을 활성화할 수 있습니다. 각 AWS 계정에는 각 클러스터 내에서 사용할 수 있는 클래식 로드 밸런서의 수를 제한하는 할당량이 있습니다.

3.3.4.5. 클러스터 인그레스

프로젝트 관리자는 IP 허용 목록을 통한 수신 제어를 포함하여 다양한 용도로 경로 주석을 추가할 수 있습니다.

ovs-networkpolicy 플러그인을 활용하는 **NetworkPolicy** 오브젝트를 사용하여 Ingress 정책을 변경할 수도 있습니다. 이를 통해 동일한 클러스터의 Pod와 동일한 네임스페이스에도 Pod 수준을 포함하여 수신 네트워크 정책을 완전히 제어할 수 있습니다.

모든 클러스터 인그레스 트래픽은 정의된 로드 밸런서를 통해 이동합니다. 클라우드 구성에 의해 모든 노드에 대한 직접 액세스가 차단됩니다.

3.3.4.6. 클러스터 송신

EgressNetworkPolicy 오브젝트를 통한 Pod 송신 트래픽 제어를 사용하여 AWS의 Red Hat OpenShift Service에서 아웃바운드 트래픽을 방지하거나 제한할 수 있습니다.

컨트롤 플레인 및 인프라 노드의 공용 아웃바운드 트래픽이 필요하며 클러스터 이미지 보안 및 클러스터 모니터링을 유지 관리하는 데 필요합니다. **0.0.0.0/0** 경로는 인터넷 게이트웨이에만 속해야 합니다. 이 범위를 프라이빗 연결을 통해 라우팅할 수 없습니다.

OpenShift 4 클러스터는 NAT 게이트웨이를 사용하여 클러스터를 나가는 공용 아웃바운드 트래픽에 대한 공용 고정 IP를 제공합니다. 클러스터가 배포된 각 가용성 영역은 별도의 NAT 게이트웨이를 수신하므로 클러스터 송신 트래픽에 대해 최대 3개의 고유한 고정 IP 주소가 존재할 수 있습니다. 클러스터 내부에 남아 있거나 공용 인터넷으로 전달하지 않는 트래픽은 NAT 게이트웨이를 통과하지 않으며 트래픽이 시작된 노드에 속하는 소스 IP 주소를 갖습니다. 노드 IP 주소는 동적이므로 고객은 개인 리소스에 액세스할 때 개별 IP 주소를 허용 목록에 사용하지 않아야 합니다.

고객은 클러스터에서 Pod를 실행한 다음 외부 서비스를 쿼리하여 공용 고정 IP 주소를 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
$ oc run ip-lookup --image=busybox -i -t --restart=Never --rm -- /bin/sh -c "/bin/nslookup -type=a
myip.opendns.com resolver1.opendns.com | grep -E 'Address: [0-9.]+'"
```

3.3.4.7. 클라우드 네트워크 구성

Red Hat OpenShift Service on AWS를 사용하면 AWS 관리 기술을 통한 프라이빗 네트워크 연결을 설정할 수 있습니다.

- VPN 연결
- VPC 피어링
- Transport Gateway
- Direct Connect

중요

Red Hat 사이트 안정성 엔지니어(SRE)는 사설 네트워크 연결을 모니터링하지 않습니다. 이러한 연결을 모니터링하는 것은 고객의 책임입니다.

3.3.4.8. DNS 전달

프라이빗 클라우드 네트워크 구성이 있는 AWS 클러스터의 Red Hat OpenShift Service의 경우 고객은 해당 프라이빗 연결에서 사용 가능한 내부 DNS 서버를 지정할 수 있습니다. 이 서버는 명시적으로 제공된 도메인에 대해 쿼리해야 합니다.

3.3.5. 스토리지

이 섹션에서는 AWS 스토리지의 Red Hat OpenShift Service의 서비스 정의에 대해 설명합니다.

3.3.5.1. encrypted-at-rest OS 및 노드 스토리지

컨트롤 플레인, 인프라 및 작업자 노드는 encrypted-at-rest AWS EBS(Elastic Block Store) 스토리지를 사용합니다.

3.3.5.2. encrypted-at-rest PV

PV에 사용되는 EBS 볼륨은 기본적으로 암호화-at-rest입니다.

3.3.5.3. 블록 스토리지(RWO)

PV(영구 볼륨)는 AWS EBS에서 지원합니다. 이는 Read-Write-Once입니다.

PV는 한 번에 단일 노드에만 연결할 수 있으며 프로비저닝된 가용성 영역과 관련이 있습니다. 그러나 가용성 영역의 모든 노드에 PV를 연결할 수 있습니다.

각 클라우드 공급자에는 단일 노드에 연결할 수 있는 PV 수에 대한 자체 제한이 있습니다. 자세한 내용은 AWS 인스턴스 유형 제한을 참조하십시오.

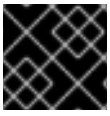
3.3.5.4. 공유 스토리지(RWX)

AWS CSI 드라이버는 AWS의 Red Hat OpenShift Service에 대한 RWX 지원을 제공하는 데 사용할 수 있습니다. 커뮤니티 Operator가 설정을 단순화하기 위해 제공됩니다. 자세한 내용은 AWS Dedicated 및 Red Hat OpenShift Service용 AWS EFS 설정을 참조하십시오.

3.3.6. 플랫폼

이 섹션에서는 ROSA(Red Hat OpenShift Service on AWS) 플랫폼의 서비스 정의에 대해 설명합니다.

3.3.6.1. 클러스터 백업 정책



중요

고객은 애플리케이션 및 애플리케이션 데이터에 대한 백업 계획을 가지고 있어야 합니다.

애플리케이션 및 애플리케이션 데이터 백업은 AWS 서비스의 Red Hat OpenShift Service의 일부가 아닙니다. 다음 표에는 클러스터 백업 정책이 요약되어 있습니다.

구성 요소	스냅샷 빈도	보존	참고
전체 오브젝트 저장소 백업, 모든 클러스터 PV(영구 볼륨)	daily	7일	이는 etcd와 같은 모든 Kubernetes 오브젝트와 클러스터의 모든 PV에 대한 전체 백업입니다.
	weekly	30일	
전체 오브젝트 저장소 백업	hourly	24시간	이는 etcd와 같은 모든 Kubernetes 오브젝트의 전체 백업입니다. 이 백업 일정에는 PV가 백업되지 않습니다.

구성 요소	스냅샷 빈도	보존	참고
노드 루트 볼륨	Never	해당 없음	노드는 단기적으로 간주됩니다. 중요한 것은 노드의 루트 볼륨에 저장해야 합니다.

3.3.6.2. 자동 확장

AWS의 Red Hat OpenShift Service에서 노드 자동 스케일링을 사용할 수 있습니다. 클러스터의 머신 수를 자동으로 확장하도록 자동 스케일러 옵션을 구성할 수 있습니다.

추가 리소스

- 클러스터의 노드 자동 스케일링 정보

3.3.6.3. DaemonSets

고객은 AWS의 Red Hat OpenShift Service에서 daemonsets를 생성하고 실행할 수 있습니다. 데몬 세트를 작업자 노드에서만 실행되도록 제한하려면 다음 **nodeSelector** 를 사용합니다.

```
...
spec:
  nodeSelector:
    role: worker
...
```

3.3.6.4. 다중 가용성 영역

여러 가용성 영역 클러스터에서 컨트롤 플레인 노드는 가용성 영역에 분산되어 있으며 각 가용성 영역에 하나 이상의 작업자 노드가 필요합니다.

3.3.6.5. 노드 라벨

사용자 정의 노드 레이블은 노드 생성 중에 Red Hat에서 생성하며 현재 AWS 클러스터의 Red Hat OpenShift Service에서 변경할 수 없습니다. 그러나 새 머신 풀을 생성할 때 사용자 정의 라벨이 지원됩니다.

3.3.6.6. OpenShift 버전

AWS의 Red Hat OpenShift Service는 서비스로 실행되며 최신 OpenShift Container Platform 버전으로 최신 상태로 유지됩니다. 최신 버전으로 스케줄링을 사용할 수 있습니다.

3.3.6.7. 업그레이드

Rosa CLI 유틸리티를 사용하거나 OpenShift Cluster Manager를 통해 업그레이드를 예약할 수 있습니다.

업그레이드 정책 및 절차에 대한 자세한 내용은 AWS 라이프 사이클의 Red Hat OpenShift Service 를 참조하십시오.

3.3.6.8. Windows 컨테이너

Windows Containers 용 Red Hat OpenShift 지원은 현재 AWS의 Red Hat OpenShift Service에서 사용할 수 없습니다.

3.3.6.9. 컨테이너 엔진

AWS의 Red Hat OpenShift Service는 OpenShift 4에서 실행되며 CRI-O 를 사용 가능한 유일한 컨테이너 엔진으로 사용합니다.

3.3.6.10. 운영 체제

AWS의 Red Hat OpenShift Service는 OpenShift 4에서 실행되며 Red Hat CoreOS를 모든 컨트롤 플레인 및 작업자 노드의 운영 체제로 사용합니다.

3.3.6.11. Red Hat Operator 지원

일반적으로 Red Hat 워크로드는 Operator Hub를 통해 제공되는 Red Hat 제공 Operator를 참조합니다. Red Hat 워크로드는 Red Hat SRE 팀에서 관리하지 않으며 작업자 노드에 배포해야 합니다. 이러한 Operator에는 추가 Red Hat 서브스크립션이 필요할 수 있으며 추가 클라우드 인프라 비용이 발생할 수 있습니다. Red Hat에서 제공하는 Operator의 예는 다음과 같습니다.

- Red Hat Quay
- Red Hat Advanced Cluster Management
- Red Hat Advanced Cluster Security
- Red Hat OpenShift Service Mesh
- OpenShift Serverless
- Red Hat OpenShift Logging
- Red Hat OpenShift Pipelines

3.3.6.12. Kubernetes Operator 지원

Operator Hub 마켓플레이스에 나열된 모든 Operator를 설치할 수 있어야 합니다. 이러한 운영자는 고객 워크로드로 간주되며 Red Hat SRE에서 모니터링하지 않습니다.

3.3.7. 보안

이 섹션에서는 AWS 보안의 Red Hat OpenShift Service의 서비스 정의에 대해 설명합니다.

3.3.7.1. 인증 공급자

클러스터 인증은 OpenShift Cluster Manager Hybrid Cloud Console 또는 클러스터 생성 프로세스를 사용하거나 **rosa** CLI를 사용하여 구성할 수 있습니다. AWS의 Red Hat OpenShift Service는 ID 공급자가 아니며 클러스터에 대한 모든 액세스는 고객이 통합 솔루션의 일부로 관리해야 합니다. 동시에 프로비저닝된 여러 ID 공급자를 사용하는 것이 지원됩니다. 지원되는 ID 공급자는 다음과 같습니다.

- GitHub 또는 GitHub Enterprise
- GitLab
- Google

- LDAP
- OpenID Connect

3.3.7.2. 권한 있는 컨테이너

cluster-admin 역할을 가진 사용자는 권한 있는 컨테이너를 사용할 수 있습니다. **cluster-admin** 으로 권한 있는 컨테이너의 사용은 Red Hat Enterprise Agreement 부록 4 (Online Subscription Services)의 책임 및 제외 노트의 적용을 받습니다.

3.3.7.3. 고객 관리자

일반 사용자 외에도 AWS의 Red Hat OpenShift Service는 AWS별 그룹인 **dedicated-admin** 그룹의 Red Hat OpenShift Service에 액세스할 수 있습니다. **dedicated-admin** 그룹의 멤버인 클러스터의 모든 사용자:

- 클러스터의 모든 고객 생성 프로젝트에 대한 관리자 액세스 권한이 있어야 합니다.
- 클러스터의 리소스 할당량 및 제한을 관리할 수 있습니다.
- **NetworkPolicy** 오브젝트를 추가하고 관리할 수 있습니다.
- 스케줄러 정보를 포함하여 클러스터의 특정 노드 및 PV에 대한 정보를 볼 수 있습니다.
- 클러스터에서 예약된 **dedicated-admin** 프로젝트에 액세스할 수 있으므로 승격된 권한이 있는 서비스 계정을 생성할 수 있으며 클러스터에서 프로젝트의 기본 제한 및 할당량을 업데이트할 수도 있습니다.

3.3.7.4. 클러스터 관리 역할

AWS의 Red Hat OpenShift Service 관리자는 조직의 클러스터의 **cluster-admin** 역할에 대한 기본 액세스 권한이 있습니다. **cluster-admin** 역할로 계정에 로그인되어 있는 동안 사용자에게 권한 있는 보안 컨텍스트를 실행할 수 있는 권한이 향상되었습니다.

3.3.7.5. 프로젝트 셀프 서비스

기본적으로 모든 사용자는 프로젝트를 생성, 업데이트 및 삭제할 수 있습니다. **dedicated-admin** 그룹의 멤버가 인증된 사용자에서 **self-provisioner** 역할을 제거하는 경우 이를 제한할 수 있습니다.

```
$ oc adm policy remove-cluster-role-from-group self-provisioner system:authenticated:oauth
```

적용을 통해 제한 사항을 되돌릴 수 있습니다.

```
$ oc adm policy add-cluster-role-to-group self-provisioner system:authenticated:oauth
```

3.3.7.6. 규정 준수

최신 규정 준수 정보는 ROSA의 프로세스 및 보안 이해를 참조하십시오.

3.3.7.7. 네트워크 보안

AWS의 Red Hat OpenShift Service를 통해 AWS는 모든 로드 밸런서에 대해 AWS Shield라는 표준 CloudEvent 보호 기능을 제공합니다. 이는 AWS의 Red Hat OpenShift Service에 사용되는 모든 공용 로드 밸런서에 대한 가장 일반적으로 사용되는 로드 밸런서에 대한 가장 일반적으로 사용되는 레벨 3 및 4

공격에 대해 95%의 보호를 제공합니다. 응답을 수신하기 위해 **haproxy** 라우터로 들어오는 HTTP 요청에 대해 10초의 시간 초과가 추가되거나 추가 보호를 제공하기 위해 연결이 닫힙니다.

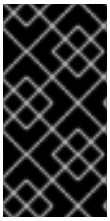
3.3.7.8. etcd 암호화

AWS의 Red Hat OpenShift Service에서 컨트롤 플레인 스토리지는 기본적으로 암호화되며 여기에는 etcd 볼륨의 암호화가 포함됩니다. 이 스토리지 수준 암호화는 클라우드 공급자의 스토리지 계층을 통해 제공됩니다.

etcd 암호화를 활성화하여 etcd의 키 값을 암호화하지만 키를 암호화할 수도 없습니다. etcd 암호화를 활성화하면 다음 Kubernetes API 서버 및 OpenShift API 서버 리소스가 암호화됩니다.

- 보안
- 구성 맵
- 라우트
- OAuth 액세스 토큰
- OAuth 승인 토큰

etcd 암호화 기능은 기본적으로 활성화되어 있지 않으며 클러스터 설치 시에만 활성화할 수 있습니다. etcd 암호화가 활성화된 상태에서도 etcd 키 값은 컨트롤 플레인 노드 또는 **cluster-admin** 권한에 액세스할 수 있는 모든 사용자가 액세스할 수 있습니다.



중요

etcd의 키 값에 etcd 암호화를 활성화하면 약 20%의 성능 오버헤드가 발생합니다. 오버헤드는 etcd 볼륨을 암호화하는 기본 컨트롤 플레인 스토리지 암호화 외에도 이 두 번째 암호화 계층이 도입된 결과입니다. 특히 사용 사례에 필요한 경우에만 etcd 암호화를 활성화하는 것이 좋습니다.

추가 리소스

- 최신 규정 준수 정보는 ROSA의 프로세스 및 보안 이해를 참조하십시오.
- ROSA 라이프 사이클 보기

3.4. RED HAT OPENSHIFT SERVICE ON AWS UPDATE 라이프 사이클

3.4.1. 개요

Red Hat은 고객 및 파트너사가 플랫폼에서 실행되는 애플리케이션을 효과적으로 계획, 배포 및 지원할 수 있도록 AWS의 Red Hat OpenShift Service의 제품 라이프 사이클을 제공합니다. Red Hat은 투명성을 제공하기 위해 라이프 사이클을 공개하고 문제가 발생할 경우 이러한 정책에 예외가 있을 수 있습니다.

AWS의 Red Hat OpenShift Service는 Red Hat OpenShift의 관리형 인스턴스이며 별도의 릴리스 일정을 유지합니다. 관리형 오퍼링에 대한 자세한 내용은 AWS 서비스 정의의 Red Hat OpenShift Service에서 확인할 수 있습니다. 특정 버전에 대한 보안 권고 및 버그 수정 권고는 Red Hat OpenShift Container Platform 라이프 사이클 정책에 따라 AWS 유지 관리 일정에 따라 Red Hat OpenShift Service에 따라 다릅니다.

추가 리소스

- Red Hat OpenShift Service on AWS 서비스 정의

3.4.2. 정의

표 3.1. 버전 참조

버전 형식	메이저	마이너	패치	Major.minor.patch
	x	y	z	x.y.z
예제	4	5	21	4.5.21

주요 릴리스 또는 X 릴리스

주요 릴리스 또는 *X-release(X*.y.z)로만 참조됩니다.

예

- "major 릴리스 5" → 5.y.z
- "major 릴리스 4" → 4.y.z
- "major 릴리스 3" → 3.y.z

마이너 릴리스 또는 Y 릴리스

마이너 릴리스 또는 *Y-release(x.Y*.z)로만 참조됩니다.

예

- "최소 릴리스 4" → 4.4.z
- "minor 릴리스 5" → 4.5.z
- "minor 릴리스 6" → 4.6.z

패치 릴리스 또는 Z 릴리스

패치 릴리스 또는 *Z-release* (x.y.Z)라고 합니다.

예

- "마이너 릴리스 5의 패치 릴리스 14" → 4.5.14
- "마이너 릴리스 5의 패치 릴리스 25" → 4.5.25
- "마이너 릴리스 6의 패치 릴리스 26" → 4.6.26

3.4.3. 주요 버전 (X.y.z)

AWS의 Red Hat OpenShift Service 주요 버전(예: 버전 4)은 후속 주요 버전 릴리스 또는 제품 종료 후 1년 동안 지원됩니다.

예제

- 1월 1일 AWS의 Red Hat OpenShift Service에서 버전 5를 사용할 수 있는 경우 12월 31일까지 12개월 동안 관리 클러스터에서 계속 실행할 수 있습니다. 이 기간 후에 클러스터를 업그레이드하거나 버전 5로 마이그레이션해야 합니다.

3.4.4. 마이너 버전 (x.Y.z)

4.8 OpenShift Container Platform 마이너 버전부터 Red Hat은 지정된 마이너 버전이 공식적으로 출시된 후 최소 14개월 동안 모든 마이너 버전을 지원합니다. 패치 버전은 지원 기간의 영향을 받지 않습니다.

지원 기간이 종료되기 전 60일, 30일, 15일 전에 고객에게 통지를 받습니다. 지원 기간이 종료되기 전에 지원되는 마이너 버전으로 클러스터를 업그레이드해야 합니다. 그렇지 않으면 클러스터는 "제한된 지원" 상태가 됩니다.

예제

1. 고객의 클러스터가 현재 4.8.14에서 실행되고 있습니다. 4.8 버전은 2021년 7월 27일에 일반적으로 사용 가능합니다.
2. 클러스터가 아직 지원되는 마이너 버전으로 업그레이드되지 않은 경우 2022년 7월 28일 및 2022년 9월 28일, 고객은 클러스터에서 "제한 지원" 상태가 2022년 9월 27일에 "제한 지원" 상태가 됩니다.
3. 클러스터는 2022년 9월 27일까지 4.9 이상으로 업그레이드해야 합니다.
4. 업그레이드가 수행되지 않은 경우 클러스터는 "제한된 지원" 상태로 표시됩니다.

추가 리소스

- Red Hat OpenShift Service on AWS limited support status

3.4.5. 패치 버전 (x.y.Z)

마이너 버전이 지원되는 기간에 Red Hat은 별도로 지정하지 않는 한 모든 OpenShift Container Platform 패치 버전을 지원합니다.

플랫폼 보안 및 안정성의 이유로 패치 릴리스가 더 이상 사용되지 않을 수 있으므로 해당 릴리스의 설치를 방지하고 필수 업그레이드를 트리거할 수 있습니다.

예제

1. 4.7.6에는 중요한 CVE가 포함되어 있습니다.
2. CVE의 영향을 받는 모든 릴리스는 지원되는 패치 릴리스 목록에서 제거됩니다. 또한 4.7.6을 실행하는 모든 클러스터는 48시간 이내에 자동 업그레이드를 위해 예약됩니다.

3.4.6. 제한된 지원 상태

클러스터가 *제한된 지원* 상태로 전환되면 Red Hat은 더 이상 클러스터를 적극적으로 모니터링하지 않으며 SLA는 더 이상 적용되지 않으며 SLA에 대해 요청된 자립이 거부됩니다. 이는 더 이상 제품 지원이 없다는 의미는 아닙니다. 일부 경우 위반 요인을 수정하면 클러스터가 완전히 지원되는 상태로 돌아갈 수 있습니다. 그러나 다른 경우에는 클러스터를 삭제하고 다시 생성해야 할 수도 있습니다.

다음 시나리오를 포함하여 여러 가지 이유로 클러스터가 제한된 지원 상태로 전환될 수 있습니다.

라이프 사이클 종료일 전에 클러스터를 지원되는 버전으로 업그레이드하지 않는 경우

Red Hat은 라이프 사이클 종료일 이후 버전에 대해 런타임 또는 SLA를 보장하지 않습니다. 지속적인 지원을 받으려면 종료일 이전에 클러스터를 지원되는 버전으로 업그레이드하십시오. 라이프 사이클 종료일 이전에 클러스터를 업그레이드하지 않으면 클러스터가 지원되는 버전으로 업그레이드될 때까지 제한된 지원 상태로 전환됩니다.

Red Hat은 지원되지 않는 버전에서 지원되는 버전으로 업그레이드하기 위해 상업적으로 합리적인 지원을 제공합니다. 그러나 지원되는 업그레이드 경로를 더 이상 사용할 수 없는 경우 새 클러스터를 생성하고 워크로드를 마이그레이션해야 할 수 있습니다.

AWS 구성 요소에서 기본 Red Hat OpenShift Service 또는 Red Hat에서 설치 및 관리하는 기타 구성 요소를 제거하거나 교체하는 경우

클러스터 관리자 권한을 사용한 경우 Red Hat은 인프라 서비스, 서비스 가용성 또는 데이터 손실에 영향을 미치는 사용자 또는 사용자의 권한이 있는 사용자의 조치에 대해 책임을 지지 않습니다. Red Hat에서 이러한 작업을 감지하면 클러스터가 제한된 지원 상태로 전환될 수 있습니다. Red Hat은 상태 변경을 알리며 클러스터를 삭제하고 다시 생성해야 할 수 있는 수정 단계를 탐색할 수 있는 조치를 되돌리거나 지원 케이스를 생성해야 합니다.

클러스터가 제한된 지원 상태로 전환되거나 추가 지원이 필요한 특정 작업에 대한 질문이 있는 경우 지원 티켓을 엽니다.

3.4.7. 지원되는 버전 예외 정책

Red Hat은 새로운 버전 또는 기존 버전을 추가하거나 제거하거나 향후 마이너 릴리스 버전을 지연할 수 있습니다. 이 버전은 사전 공지 없이 버그 또는 보안 문제에 영향을 미치는 하나 이상의 중요한 프로덕션 문제로 확인되었습니다.

3.4.8. 설치 정책

Red Hat은 최신 지원 릴리스를 설치하는 것을 권장하지만 AWS의 Red Hat OpenShift Service는 이전 정책에서 적용되는 모든 지원 릴리스의 설치를 지원합니다.

3.4.9. 필수 업그레이드

심각 또는 중요한 CVE 또는 Red Hat에서 식별한 기타 버그가 클러스터의 보안 또는 안정성에 크게 영향을 미치는 경우 고객은 영업일 기준 2일 이내에 다음 지원 패치 릴리스로 업그레이드해야 합니다.

드문 경우지만 환경에 대한 Red Hat의 CVE 중요도 평가에 따라 Red Hat은 고객이 클러스터를 최신 보안 패치 릴리스로 예약하거나 수동으로 업데이트할 수 있는 2 일(영업일)이라는 사실을 고객에게 알립니다. 업데이트가 수행되지 않은 경우 Red Hat은 클러스터를 최신 보안 패치 릴리스, 보안 패치 릴리스로 자동 업데이트하여 잠재적인 보안 위반 또는 불안정성을 완화합니다. Red Hat은 재량에 따라 지원 케이스를 통해 고객이 요청한 경우 자동 업데이트를 일시적으로 지연할 수 있습니다.

3.4.10. 라이프 사이클 날짜

버전	정식 출시일 (GA)	종료일
4.12	2023년 1월 17일	2024년 3월 17일
4.11	2022년 8월 10일	2023년 10월 10일
4.10	2022년 3월 10일	2023년 7월 10일

버전	정식 출시일 (GA)	종료일
4.9	2021년 10월 18일	2022년 12월 18일
4.8	2021년 7월 27일	2022년 9월 27일

3.5. AWS에서 RED HAT OPENSHIFT SERVICE의 프로세스 및 보안 이해

이 문서에서는 ROSA(Red Hat OpenShift Service on AWS)를 관리하는 Red Hat의 역할에 대해 자세히 설명합니다.

약어 및 용어

- **AWS** - Amazon Web Services
- **CEE** - 고객 경험 및 참여 (Red Hat 지원)
- **CI/CD** - 지속적 통합/지속적인 제공
- **CVE** - Common Vulnerabilities and Exposures
- **PV** - 영구 볼륨
- **ROSA** - Red Hat OpenShift Service on AWS
- **SRE** - Red Hat 사이트 안정성 엔지니어링
- **VPC** - 가상 프라이빗 클라우드

3.5.1. 사고 및 운영 관리

이 문서에서는 ROSA(Red Hat OpenShift Service on AWS) 관리 서비스에 대한 Red Hat 책임이 자세히 설명되어 있습니다.

3.5.1.1. 플랫폼 모니터링

Red Hat 사이트 안정성 엔지니어(SRE)는 모든 ROSA 클러스터 구성 요소, SRE 서비스 및 기본 AWS 계정에 대한 중앙 집중식 모니터링 및 경고 시스템을 유지합니다. 플랫폼 감사 로그는 중앙 집중식 보안 정보 및 이벤트 모니터링(SIEM) 시스템으로 안전하게 전달되며, 여기서 SRE 팀에 구성된 경고를 트리거할 수 있으며 수동 검토도 받습니다. 감사 로그는 SIEM 시스템에 1년 동안 유지됩니다. 지정된 클러스터에 대한 감사 로그는 클러스터를 삭제할 때 삭제되지 않습니다.

3.5.1.2. 사고 관리

사고는 하나 이상의 Red Hat 서비스의 성능 저하 또는 중단을 초래하는 이벤트입니다. 기술 지원 케이스를 통해 고객 또는 고객 경험 및 참여(CEE)의 사고는 중앙 집중식 모니터링 및 경고 시스템에 의해 직접 발생하거나 SRE 팀의 구성원에 의해 발생할 수 있습니다.

서비스 및 고객에 미치는 영향에 따라 보안 사고는 심각도 별로 분류됩니다.

Red Hat은 새로운 사고를 관리할 때 다음과 같은 일반 워크플로를 사용합니다.

1. SRE 첫 번째 대응자는 새로운 사고에 대한 경고를 받고 있으며 초기 조사를 시작합니다.
2. 초기 조사 후 사고의 선두주자가 할당되며, 이는 복구 노력을 조정합니다.
3. 사고 대응자는 관련 알림 및 지원 케이스 업데이트를 포함하여 모든 통신을 관리하고 복구에 대한 조정을 관리합니다.
4. 이 사고는 복구되었습니다.
5. 이 사고는 문서화되어 있으며 근본적인 원인 분석 (RCA)은 사고 후 5 일 이내에 수행됩니다.
6. RCA 초안 문서는 사고 후 7일 이내에 고객과 공유됩니다.

3.5.1.3. 알림

플랫폼 알림은 이메일을 사용하여 구성됩니다. 일부 고객 알림은 필요한 경우 기술 계정 관리자를 포함하여 계정의 해당 Red Hat 계정 팀으로 전송됩니다.

다음 활동을 통해 알림을 트리거할 수 있습니다.

- 플랫폼 사고
- 성능 저하
- 클러스터 용량 경고
- 심각한 취약점 및 해결 방법
- 업그레이드 스케줄링

3.5.1.4. 인프라 및 데이터 복원력

고객은 데이터의 정기적인 백업을 수행해야 하며 Kubernetes 모범 사례를 따르는 워크로드가 포함된 다중 AZ 클러스터를 배포하여 한 리전 내에서 고가용성을 보장해야 합니다. 전체 클라우드 리전을 사용할 수 없는 경우 고객은 다른 지역에 새 클러스터를 설치하고 백업 데이터를 사용하여 앱을 복원해야 합니다.

STS를 사용하는 ROSA 클러스터에 사용할 수 있는 Red Hat 제공 백업 방법은 없습니다. Red Hat은 PREO (Resupation Point Objective) 또는 RTO (RTO)에 커밋하지 않습니다.

3.5.1.5. 클러스터 용량

클러스터 용량을 평가하고 관리하는 것은 Red Hat과 고객 간에 공유됩니다. Red Hat SRE는 클러스터의 모든 컨트롤 플레인 및 인프라 노드의 용량을 담당합니다.

Red Hat SRE는 업그레이드 중 및 클러스터 경고에 대한 응답으로 클러스터 용량도 평가합니다. 용량에 대한 클러스터 업그레이드의 영향은 업그레이드 테스트 프로세스의 일부로 평가되어 클러스터에 새로 추가된 용량의 부정적인 영향을 받지 않도록 합니다. 클러스터 업그레이드 중에 업그레이드 프로세스 중에 총 클러스터 용량을 유지하도록 추가 작업자 노드가 추가됩니다.

Red Hat SRE 직원의 용량 평가는 특정 기간 동안 사용량 임계값을 초과한 후 클러스터의 경고에 대한 응답으로도 수행됩니다. 이러한 경고는 고객에게 통지가 발생할 수도 있습니다.

3.5.2. 변경 관리

이 섹션에서는 클러스터 및 구성 변경, 패치 및 릴리스를 관리하는 방법에 대한 정책에 대해 설명합니다.

3.5.2.1. 고객 시작 변경

클러스터 배포, 작업자 노드 확장 또는 클러스터 삭제와 같은 셀프 서비스 기능을 사용하여 변경 사항을 시작할 수 있습니다.

변경 내역은 OpenShift **Cluster** Manager **개요 탭** 의 클러스터 기록 섹션에서 캡처되며 사용자가 확인할 수 있습니다. 변경 내역에는 다음이 포함되지만 이에 국한되지는 않으며 다음 변경 사항의 로그가 포함됩니다.

- ID 공급자 추가 또는 제거
- **dedicated-admins** 그룹에 사용자 추가 또는 제거
- 클러스터 컴퓨팅 노드 확장
- 클러스터 로드 밸런서 스케일링
- 클러스터 영구 스토리지 스케일링
- 클러스터 업그레이드

다음 구성 요소에 대해 OpenShift Cluster Manager의 변경 사항을 방지하여 유지 관리 제외를 구현할 수 있습니다.

- 클러스터 삭제
- ID 공급자 추가, 수정 또는 제거
- 승격된 그룹에서 사용자 추가, 수정 또는 제거
- 애드온 설치 또는 제거
- 클러스터 네트워킹 구성 수정
- 머신 풀 추가, 수정 또는 제거
- 사용자 워크로드 모니터링 활성화 또는 비활성화
- 업그레이드 시작

중요

유지 관리 제외를 적용하려면 머신 풀 자동 스케일링 또는 자동 업그레이드 정책을 비활성화해야 합니다. 유지 관리 제외가 해제된 후 필요에 따라 머신 풀 자동 스케일링 또는 자동 업그레이드 정책 활성화를 진행합니다.

3.5.2.2. Red Hat 시작 변경

Red Hat 사이트 안정성 엔지니어링(SRE)은 GitOps 워크플로 및 완전 자동화된 CI/CD 파이프라인을 사용하여 AWS에서 Red Hat OpenShift Service의 인프라, 코드 및 구성을 관리합니다. 이 프로세스를 통해 Red Hat은 고객에게 부정적인 영향을 미치지 않고 지속적으로 서비스 개선을 지속적으로 개선할 수 있습니다.

제안된 모든 변경 사항은 점검 즉시 일련의 자동 검증을 거칩니다. 그런 다음 변경 사항이 자동화된 통합 테스트를 받는 스테이징 환경에 배포됩니다. 마지막으로 변경 사항이 프로덕션 환경에 배포됩니다. 각 단계는 완전히 자동화됩니다.

승인된 SRE 검토자는 각 단계에 대한 진행을 승인해야 합니다. 검토자는 변경 사항을 제안한 동일한 개인일 수 없습니다. 모든 변경 사항 및 승인은 GitOps 워크플로우의 일부로 완전히 감사할 수 있습니다.

기능 플래그를 사용하여 지정된 클러스터 또는 고객에 대한 새 기능의 가용성을 제어하는 일부 변경 사항이 증분적으로 릴리스됩니다.

3.5.2.3. 패치 관리

OpenShift Container Platform 소프트웨어 및 기본 변경 불가능한 RHCOS (Red Hat CoreOS) 운영 체제 이미지는 일반 z-stream 업그레이드의 버그 및 취약점에 대해 패치됩니다. OpenShift Container Platform 설명서에서 RHCOS 아키텍처에 대해 자세히 알아보십시오.

3.5.2.4. 릴리스 관리

Red Hat은 클러스터를 자동으로 업그레이드하지 않습니다. OpenShift Cluster Manager 웹 콘솔을 사용하여 클러스터를 정기적인 간격으로 업그레이드하거나 (개인 업그레이드) 한 번만 예약할 수 있습니다. Red Hat은 클러스터가 심각한 영향 CVE의 영향을 받는 경우에만 클러스터를 새 z-stream 버전으로 강제로 업그레이드할 수 있습니다.

참고

필요한 권한이 y-stream 릴리스 간에 변경될 수 있으므로 업그레이드를 수행하기 전에 정책을 업데이트해야 할 수 있습니다. 따라서 STS를 사용하여 ROSA 클러스터에서 반복 업그레이드를 예약할 수 없습니다.

OpenShift Cluster Manager 웹 콘솔에서 모든 클러스터 업그레이드 이벤트 기록을 검토할 수 있습니다. 릴리스에 대한 자세한 내용은 라이프 사이클 정책을 참조하십시오.

3.5.3. ID 및 액세스 관리

대부분의 SRE(사이트 안정성 엔지니어링) 팀은 자동화된 구성 관리를 통해 클러스터 Operator를 사용하여 수행됩니다.

3.5.3.1. 하위 프로세서

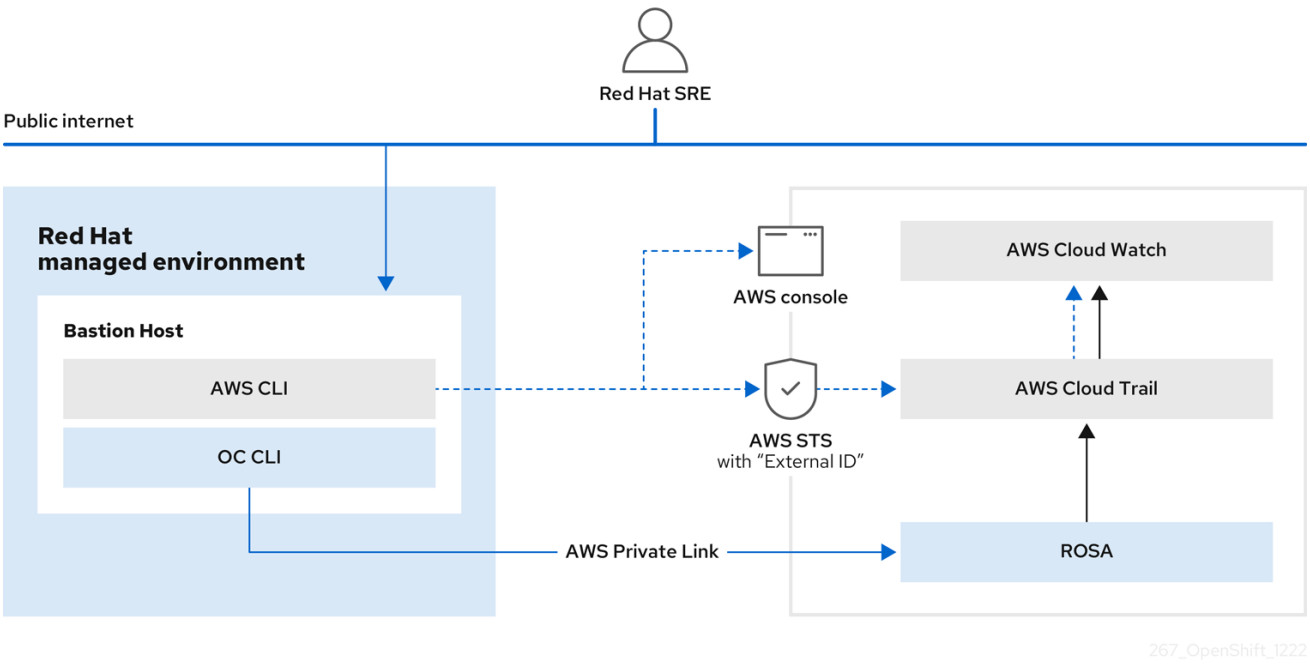
사용 가능한 하위 프로세서 목록은 Red Hat 고객 포털의 Red Hat 하위 프로세서 목록을 참조하십시오.

3.5.3.2. AWS 클러스터의 모든 Red Hat OpenShift Service에 대한 SRE 액세스

SRES는 웹 콘솔 또는 명령줄 툴을 통해 AWS 클러스터의 Red Hat OpenShift Service에 액세스합니다. 인증에는 암호 복잡성 및 계정 잠금에 대한 업계 표준 요구 사항이 있는 MFA(다중 인증)가 필요합니다. SRES는 감사성을 보장하기 위해 개인으로 인증해야 합니다. 모든 인증 시도가 SIEM(Security Information and Event Management) 시스템에 기록됩니다.

SRES는 암호화된 HTTP 연결을 사용하여 프라이빗 클러스터에 액세스합니다. 연결은 IP 허용 목록 또는 프라이빗 클라우드 공급자 링크를 사용하는 Red Hat 네트워크에서만 허용됩니다.

그림 3.1. ROSA 클러스터에 대한 SRE 액세스



3.5.3.3. AWS의 Red Hat OpenShift Service에서 권한 있는 액세스 제어

SRE는 AWS 및 AWS 구성 요소에서 Red Hat OpenShift Service에 액세스할 때 최소 권한 원칙을 준수합니다. 수동 SRE 액세스의 네 가지 기본 카테고리가 있습니다.

- 일반적인 2 단계 인증 및 권한 없는 고도와 함께 Red Hat 포털을 통해 SRE 관리자 액세스.
- 정상적인 2 단계 인증으로 Red Hat 기업 SSO를 통한 SRE 관리자 액세스 및 권한 없는 고도.
- Red Hat SSO를 사용한 수동 승격인 OpenShift 승격. 액세스는 2시간으로 제한되며 완전히 감사되며 관리 승인이 필요합니다.
- AWS 콘솔 또는 CLI 액세스에 대한 수동 승격인 AWS 액세스 또는 승격. 액세스는 60분으로 제한되며 완전히 감사됩니다.

이러한 액세스 유형에는 각각 다른 수준의 구성 요소에 대한 액세스 수준이 있습니다.

구성 요소	일반적인 SRE 관리자 액세스 (Red Hat Portal)	일반적인 SRE 관리자 액세스(Red Hat SSO)	OpenShift 고도	클라우드 공급자 액세스 또는 승격
OpenShift Cluster Manager	R/W	액세스 권한 없음	액세스 권한 없음	액세스 권한 없음
OpenShift 콘솔	액세스 권한 없음	R/W	R/W	액세스 권한 없음
노드 운영 체제	액세스 권한 없음	승격된 OS 및 네트워크 권한의 특정 목록입니다.	승격된 OS 및 네트워크 권한의 특정 목록입니다.	액세스 권한 없음

구성 요소	일반적인 SRE 관리자 액세스 (Red Hat Portal)	일반적인 SRE 관리자 액세스(Red Hat SSO)	OpenShift 고도	클라우드 공급자 액세스 또는 승격
AWS Console	액세스 권한 없음	액세스 권한은 없지만 클라우드 공급자 액세스를 요청하는 데 사용되는 계정입니다.	액세스 권한 없음	SRE ID를 사용하는 모든 클라우드 공급자 권한.

3.5.3.4. AWS 계정에 대한 SRE 액세스

Red Hat 인력은 일상적인 Red Hat OpenShift Service 과정에서 AWS 작업에 대한 AWS 계정에 액세스하지 않습니다. 긴급 문제 해결을 위해 SRE는 클라우드 인프라 계정에 액세스하기 위한 잘 정의되고 감사 가능한 절차가 있습니다.

SRES는 AWS STS(보안 토큰 서비스)를 사용하여 예약된 역할에 대한 단기 AWS 액세스 토큰을 생성합니다. STS 토큰에 대한 액세스는 감사로 기록되고 개별 사용자로 추적할 수 있습니다. STS 및 비STS 클러스터 모두 SRE 액세스에 AWS STS 서비스를 사용합니다. STS가 아닌 클러스터의 경우 **BYOCAdminAccess** 역할에 **AdministratorAccess** IAM 정책이 연결되어 있으며 이 역할은 관리에 사용됩니다. STS 클러스터의 경우 **ManagedOpenShift-Support-Role** 에 **ManagedOpenShift-Support-Access** 정책이 연결되었으며 이 역할은 관리에 사용됩니다.

3.5.3.5. Red Hat 지원 액세스

Red Hat CEE(Customer Experience and Engagement) 팀의 구성원은 일반적으로 클러스터의 일부에 대한 읽기 전용 권한을 갖습니다. 특히 CEE는 핵심 및 제품 네임스페이스에 대한 액세스를 제한하고 고객 네임스페이스에 대한 액세스 권한이 없습니다.

Role	코어 네임스페이스	계층화된 제품 네임스페이스	고객 네임스페이스	AWS 계정*
OpenShift SRE	읽기: 모두 쓰기: Very 제한된 [1]	읽기: 모두 쓰기: 없음	읽기: None[2] 쓰기: 없음	읽기: 모두 [3] 모두 쓰기 [3]
CEE	읽기: 모두 쓰기: 없음	읽기: 모두 쓰기: 없음	읽기: None[2] 쓰기: 없음	읽기: 없음 쓰기: 없음
고객 관리자	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: 모두 쓰기: 모두	읽기: 모두 쓰기: 모두
고객 사용자	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: Limited[4] 쓰기: 제한됨[4]	읽기: 없음 쓰기: 없음

Role	코어 네임스페이스	계층화된 제품 네임스페이스	고객 네임스페이스	AWS 계정*
다른 모든 사람	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음	읽기: 없음 쓰기: 없음

1. 실패한 배포, 클러스터 업그레이드, 잘못된 작업자 노드 교체와 같은 일반적인 사용 사례 처리로 제한됩니다.
2. Red Hat 직원은 기본적으로 고객 데이터에 액세스할 수 없습니다.
3. AWS 계정에 대한 SRE 액세스는 문서화된 사고 중에 예외적인 문제 해결을 위한 긴급 절차입니다.
4. 고객 관리자가 RBAC를 통해 부여한 항목 및 사용자가 생성한 네임스페이스로 제한됩니다.

3.5.3.6. 고객 액세스

고객 액세스는 고객이 생성한 네임스페이스 및 고객 관리자 역할에서 RBAC를 사용하여 부여하는 권한으로 제한됩니다. 기본 인프라 또는 제품 네임스페이스에 대한 액세스는 일반적으로 **cluster-admin** 액세스 없이 허용되지 않습니다. 고객 액세스 및 인증에 대한 자세한 내용은 문서의 "기술 이해" 섹션에서 확인할 수 있습니다.

3.5.3.7. 액세스 승인 및 검토

새로운 SRE 사용자 액세스에는 관리 승인이 필요합니다. 분리되거나 전송된 SRE 계정은 자동화된 프로세스를 통해 권한 있는 사용자로 제거됩니다. 또한 SRE는 권한 있는 사용자 목록의 관리 서명을 포함하여 정기적인 액세스 검토를 수행합니다.

3.5.4. 보안 및 규정 준수

보안 및 규정 준수에는 보안 제어 및 컴플라이언스 인증 구현과 같은 작업이 포함됩니다.

3.5.4.1. 데이터 분류

Red Hat은 데이터 분류 표준을 정의하고 준수하여 데이터의 민감도를 결정하고 수집, 사용, 전송, 저장 및 처리되는 데이터의 기밀성 및 무결성에 대한 내재적인 위험을 강조합니다. 고객 소유 데이터는 최고 수준의 민감도 및 처리 요구 사항으로 분류됩니다.

3.5.4.2. 데이터 관리

Red Hat OpenShift Service on AWS (ROSA)는 AWS KMS(Key Management Service)를 사용하여 암호화된 데이터의 키를 안전하게 관리합니다. 이러한 키는 기본적으로 암호화된 컨트롤 플레인, 인프라 및 작업자 데이터 볼륨에 사용됩니다. 고객 애플리케이션의 PV(영구 볼륨)도 키 관리를 위해 AWS KMS를 사용합니다.

고객이 ROSA 클러스터를 삭제하면 컨트롤 플레인 데이터 볼륨 및 PV(영구 볼륨)와 같은 고객 애플리케이션 데이터 볼륨을 포함하여 모든 클러스터 데이터가 영구적으로 삭제됩니다.

3.5.4.3. 취약점 관리

Red Hat은 산업 표준 툴을 사용하여 ROSA의 정기적인 취약점 검사를 수행합니다. 확인된 취약점은 심각도에 따라 타임라인에 따라 수정에 추적됩니다. 취약점 스캔 및 수정 활동에는 규정 준수 인증 감사 과정에서 타사 평가자가 확인할 수 있도록 문서화되어 있습니다.

3.5.4.4. 네트워크 보안

3.5.4.4.1. 방화벽 및 CloudEvent 보호

각 ROSA 클러스터는 AWS 보안 그룹에 대한 방화벽 규칙을 사용하여 보안 네트워크 구성으로 보호됩니다. ROSA 고객은 AWS Shield Standard 를 사용하여 CloudEvent 보안 공격을 방지할 수 있습니다.

3.5.4.4.2. 프라이빗 클러스터 및 네트워크 연결

고객은 선택적으로 웹 콘솔, API 및 애플리케이션 라우터와 같은 ROSA 클러스터 끝점을 구성하여 비공개로 설정하여 클러스터 컨트롤 플레인 및 애플리케이션에 액세스할 수 없습니다. Red Hat SRE는 여전히 IP 허용 목록으로 보호되는 인터넷 액세스 가능한 엔드 포인트가 필요합니다.

AWS 고객은 AWS VPC 피어링, AWS VPN 또는 AWS Direct Connect와 같은 기술을 통해 ROSA 클러스터에 대한 프라이빗 네트워크 연결을 구성할 수 있습니다.

3.5.4.4.3. 클러스터 네트워크 액세스 제어

고객이 **NetworkPolicy** 오브젝트 및 OpenShift SDN을 사용하여 세분화된 네트워크 액세스 제어 규칙을 프로젝트별로 구성할 수 있습니다.

3.5.4.5. Penetration 테스트

Red Hat은 ROSA에 대해 정기적인 검사 테스트를 수행합니다. 테스트는 산업 표준 툴과 모범 사례를 사용하여 독립적인 내부 팀에서 수행합니다.

발견된 문제는 심각도에 따라 우선 순위가 지정됩니다. 오픈 소스 프로젝트에 속하는 모든 문제는 해결을 위해 커뮤니티와 공유됩니다.

3.5.4.6. 컴플라이언스

AWS 기반의 Red Hat OpenShift Service는 보안 및 제어를 위한 일반적인 업계 모범 사례를 따릅니다. 인증은 다음 표에 설명되어 있습니다.

표 3.2. AWS의 Red Hat OpenShift Service에 대한 보안 및 제어 인증

인증	Red Hat Openshift Service on AWS
HIPAA	제공됨
ISO 27001	제공됨
ISO 27017	제공됨
ISO 27018	제공됨
PCI DSS	제공됨

인증	Red Hat Openshift Service on AWS
SOC 2 Type 2	제공됨

추가 리소스

- SRE residency에 대한 정보는 Red Hat Subprocessor List 를 참조하십시오.

3.5.5. 재해 복구

Red Hat OpenShift Service on AWS(ROSA)는 Pod, 작업자 노드, 인프라 노드, 컨트롤 플레인 노드 및 가용 영역 수준에서 발생하는 장애 발생을 위한 재해 복구 기능을 제공합니다.

모든 재해 복구를 위해서는 고객이 원하는 가용성 수준을 고려하여 고가용성 애플리케이션, 스토리지 및 클러스터 아키텍처(예: 단일 영역 배포 또는 다중 영역 배포)를 배포하는 모범 사례를 사용해야 합니다.

하나의 단일 영역 클러스터는 가용성 영역 또는 지역 중단 시 재해 방지 또는 복구를 제공하지 않습니다. 고객이 유지보수하는 장애 조치가 있는 여러 단일 영역 클러스터에서는 해당 영역 또는 지역 수준에서의 중단을 설명할 수 있습니다.

하나의 다중 영역 클러스터는 전체 리전 중단 시 재해 방지 또는 복구를 제공하지 않습니다. 고객이 유지보수하는 장애 조치가 있는 여러 다중 영역 클러스터는 지역 수준에서의 중단을 설명할 수 있습니다.

추가 리소스

- 고객 또는 공유 책임에 대한 자세한 내용은 ROSA Responsibilities 문서를 참조하십시오.
- ROSA 및 해당 구성 요소에 대한 자세한 내용은 ROSA 서비스 정의를 참조하십시오.

4장. STS를 사용하는 ROSA 클러스터의 IAM 리소스 정보

AWS STS(Security Token Service)를 사용하는 AWS(ROSA) 클러스터에 Red Hat OpenShift Service를 배포하려면 다음 AWS IAM(Identity Access Management) 리소스를 생성해야 합니다.

- ROSA 지원, 설치, 컨트롤 플레인 및 컴퓨팅 기능에 필요한 STS 권한을 제공하는 특정 계정 전체 IAM 역할 및 정책입니다. 여기에는 계정 전체 Operator 정책이 포함됩니다.
- ROSA 클러스터 Operator가 핵심 OpenShift 기능을 수행할 수 있도록 하는 클러스터별 Operator IAM 역할입니다.
- 클러스터 Operator가 인증하는 데 사용하는 OpenID Connect(OIDC) 공급자입니다.
- OpenShift Cluster Manager를 사용하여 ROSA를 배포하는 경우 추가 리소스를 생성해야 합니다.
  - 클러스터에 설치를 완료하는 OpenShift Cluster Manager IAM 역할입니다.
  - AWS 계정 ID를 확인할 수 있는 권한이 없는 사용자 역할입니다.

이 문서에서는 STS를 사용하는 ROSA 클러스터를 생성할 때 배포해야 하는 IAM 리소스에 대한 참조 정보를 제공합니다. **rosa create** 명령과 함께 **수동** 모드를 사용할 때 생성되는 **aws** CLI 명령도 포함되어 있습니다.

추가 리소스

- AWS IAM 리소스를 포함하여 STS를 사용하여 ROSA 클러스터를 빠르게 생성하는 단계는 기본 옵션을 사용하여 STS를 사용하여 ROSA 클러스터 생성을 참조하십시오.
- AWS IAM 리소스를 포함하여 사용자 정의를 사용하여 STS를 사용하여 ROSA 클러스터를 생성하는 단계는 사용자 지정을 사용하여 STS를 사용하여 ROSA 클러스터 생성을 참조하십시오.

4.1. OPENSHIFT CLUSTER MANAGER 역할 및 권한

OpenShift Cluster Manager Hybrid Cloud Console 을 사용하여 ROSA 클러스터를 생성하는 경우 클러스터를 생성하고 관리하려면 다음 AWS IAM 역할이 연결되어 있어야 합니다. IAM 역할을 AWS 계정과 연결하는 방법에 대한 자세한 내용은 AWS 계정 지원을 참조하십시오.

작은 정보

rosa CLI 도구만 사용하는 경우 이러한 IAM 역할을 생성할 필요가 없습니다.

이러한 AWS IAM 역할은 다음과 같습니다.

- ROSA 사용자 역할은 Red Hat에서 고객의 AWS ID를 확인하는 데 사용하는 AWS 역할입니다. 이 역할에는 추가 권한이 없으며 이 역할에는 Red Hat 설치 프로그램 계정과 신뢰 관계가 있습니다.
- **ocm-role** 리소스는 OpenShift Cluster Manager에 ROSA 클러스터 설치에 필요한 권한을 부여합니다. **ocm-role** 리소스에 기본 또는 관리 권한을 적용할 수 있습니다. 관리 **ocm-role** 리소스를 생성하는 경우 OpenShift Cluster Manager에서 필요한 AWS Operator 역할 및 OIDC(OpenID Connect) 공급자를 생성할 수 있습니다. 이 IAM 역할은 Red Hat 설치 프로그램 계정과도 신뢰 관계를 생성합니다.

참고

ocm-role IAM 리소스는 IAM 역할과 생성된 필요한 정책의 조합을 나타냅니다.

OpenShift Cluster Manager에서 auto 모드를 사용하여 Operator 역할 및 OIDC 공급자를 생성하려면 이 사용자 역할 및 관리자 **ocm-role** 리소스를 생성해야 합니다.

4.1.1. OpenShift Cluster Manager 역할 이해

OpenShift Cluster Manager 하이브리드 클라우드 콘솔에서 ROSA 클러스터를 생성하려면 **ocm-role** IAM 역할이 필요합니다. 기본 **ocm-role** IAM 역할 권한을 사용하면 OpenShift Cluster Manager 내에서 클러스터 유지 관리를 수행할 수 있습니다. Operator 역할 및 OIDC(OpenID Connect) 공급자를 자동으로 생성하려면 **rosa create** 명령에 **--admin** 옵션을 추가해야 합니다. 이 명령은 관리 작업에 필요한 추가 권한이 있는 **ocm-role** 리소스를 생성합니다.

참고

이 상승된 IAM 역할을 통해 OpenShift Cluster Manager는 클러스터 생성 중에 클러스터별 Operator 역할 및 OIDC 공급자를 자동으로 생성할 수 있습니다. 이 자동 역할 및 정책 생성에 대한 자세한 내용은 추가 리소스의 " account-wide 역할 생성 방법" 링크를 참조하십시오.

4.1.1.1. 사용자 역할 이해

ocm-role IAM 역할 외에도 AWS의 Red Hat OpenShift Service가 AWS ID를 확인할 수 있도록 사용자 역할을 생성해야 합니다. 이 역할에는 권한이 없으며 설치 프로그램 계정과 **ocm-role** 리소스 간의 신뢰 관계를 생성하는 데만 사용됩니다.

다음 표에는 **ocm-role** 리소스에 대한 관련 기본 및 관리 권한이 표시되어 있습니다.

표 4.1. 기본 ocm-role 리소스에 대한 관련 권한

리소스	설명
iam:GetOpenIDConnectProvider	이 권한을 사용하면 기본 역할이 지정된 OIDC(OpenID Connect) 공급자에 대한 정보를 검색할 수 있습니다.
iam:GetRole	이 권한을 사용하면 기본 역할이 지정된 역할에 대한 정보를 검색할 수 있습니다. 반환된 일부 데이터에는 역할을 가정할 권한을 부여하는 역할의 경로, GUID, ARN 및 역할의 신뢰 정책이 포함됩니다.
iam:ListRoles	이 권한을 사용하면 기본 역할이 경로 접두사 내의 역할을 나열할 수 있습니다.
iam:ListRoleTags	이 권한을 사용하면 기본 역할이 지정된 역할의 태그를 나열할 수 있습니다.
ec2:DescribeRegions	이 권한을 통해 기본 역할은 계정의 활성화된 모든 지역에 대한 정보를 반환할 수 있습니다.
ec2:DescribeRouteTables	이 권한을 통해 기본 역할은 모든 경로 테이블에 대한 정보를 반환할 수 있습니다.
ec2:DescribeSubnets	이 권한을 통해 기본 역할은 모든 서브넷에 대한 정보를 반환할 수 있습니다.

리소스	설명
ec2:DescribeVpcs	이 권한을 통해 기본 역할은 모든 가상 프라이빗 클라우드(VPC)에 대한 정보를 반환할 수 있습니다.
sts:AssumeRole	이 권한을 사용하면 기본 역할이 임시 보안 자격 증명을 검색하여 일반 권한을 벗어나는 AWS 리소스에 액세스할 수 있습니다.
sts:AssumeRoleWithWebIdentity	이 권한을 사용하면 기본 역할이 웹 ID 공급자로 계정을 인증한 사용자의 임시 보안 자격 증명을 검색할 수 있습니다.

표 4.2. admin **ocm-role** 리소스에 대한 추가 권한

리소스	설명
iam:AttachRolePolicy	이 권한을 사용하면 admin 역할이 지정된 정책을 원하는 IAM 역할에 연결할 수 있습니다.
iam:CreateOpenIDConnectProvider	이 권한은 OIDC(OpenID Connect)를 지원하는 ID 공급자를 설명하는 리소스를 생성합니다. 이 권한이 있는 OIDC 공급자를 생성할 때 이 공급자는 공급자와 AWS 간의 신뢰 관계를 설정합니다.
iam:CreateRole	이 권한을 사용하면 admin 역할이 AWS 계정에 대한 역할을 생성할 수 있습니다.
iam:ListPolicies	이 권한을 사용하면 admin 역할이 AWS 계정과 연결된 모든 정책을 나열할 수 있습니다.
iam:ListPolicyTags	이 권한을 사용하면 admin 역할이 지정된 정책의 태그를 나열할 수 있습니다.
iam:PutRolePermissionsBoundary	이 권한을 사용하면 admin 역할이 지정된 정책에 따라 사용자에 대한 권한 경계를 변경할 수 있습니다.
iam:TagRole	이 권한을 사용하면 admin 역할이 IAM 역할에 태그를 추가할 수 있습니다.

추가 리소스

- 계정 전체 역할 생성 방법

OpenShift Cluster Manager IAM 역할 생성

CLI(명령줄 인터페이스)를 사용하여 OpenShift Cluster Manager IAM 역할을 생성합니다.

사전 요구 사항

- AWS 계정이 있습니다.
- OpenShift Cluster Manager 조직에 Red Hat 조직 관리자 권한이 있어야 합니다.
- AWS 계정 전체 역할을 설치하는 데 필요한 권한이 있습니다.

- 설치 호스트에 최신 AWS(**aws**) 및 ROSA(**rosa**) CLI를 설치하고 구성했습니다.

절차

- 기본 권한으로 ocm-role IAM 역할을 생성하려면 다음 명령을 실행합니다.

```
$ rosa create ocm-role
```

- admin 권한으로 ocm-role IAM 역할을 생성하려면 다음 명령을 실행합니다.

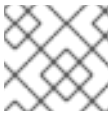
```
$ rosa create ocm-role --admin
```

이 명령을 사용하면 특정 특성을 지정하여 역할을 생성할 수 있습니다. 다음 예제 출력에서는 로사 CLI에서 Operator 역할 및 정책을 생성할 **수** 있는 "자동 모드"를 보여줍니다. 자세한 내용은 추가 리소스의 " account-wide 역할 생성 방법"을 참조하십시오.

출력 예

```
I: Creating ocm role
? Role prefix: ManagedOpenShift 1
? Enable admin capabilities for the OCM role (optional): No 2
? Permissions boundary ARN (optional): 3
? Role creation mode: auto 4
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes 5
I: Created role 'ManagedOpenShift-OCM-Role-182' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-OCM-Role-182'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182 6
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization
'<AWS ARN'? Yes 7
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' with
organization account '<AWS ARN>'
```

1. 생성된 모든 AWS 리소스의 접두사 값입니다. 이 예제에서 **ManagedOpenShift** 는 모든 AWS 리소스 앞에 추가합니다.
2. 이 역할에 추가 관리자 권한이 필요한 경우 선택합니다.



참고

--admin 옵션을 사용한 경우 이 프롬프트가 표시되지 않습니다.

3. 권한 경계를 설정하는 정책의 Amazon 리소스 이름(ARN)입니다.
4. AWS 역할을 생성하는 방법을 선택합니다. **auto** 를 사용하면 **rosa** CLI 툴이 역할 및 정책을 생성하고 연결합니다. **자동** 모드에서는 AWS 역할을 생성하는 몇 가지 다른 프롬프트가 표시됩니다.
5. auto 방법은 접두사를 사용하여 특정 **ocm-role** 을 생성할지 여부를 요청합니다.
6. IAM 역할을 OpenShift Cluster Manager와 연결할지 확인합니다.
7. 생성된 역할을 AWS 조직과 연결합니다.

AWS IAM 역할은 클러스터를 생성하고 관리하기 위해 AWS 계정에 연결됩니다. IAM 역할을 AWS 계정과 연결하는 방법에 대한 자세한 내용은 AWS 계정 지원을 참조하십시오.

추가 리소스

- AWS Identity and Access Management Data Types
- Amazon Elastic Computer Cloud 데이터 유형
- AWS 토큰 보안 서비스 데이터 유형
- 계정 전체 역할 생성 방법

4.2. 계정 전체 IAM 역할 및 정책 참조

중요

AWS ROSA 4.12 클러스터 생성 시 Red Hat OpenShift Service의 경우 시간이 오래 걸리거나 실패할 수 있습니다. ROSA의 기본 버전은 4.11로 설정되어 있으므로 기본 설정을 사용하여 계정 역할 또는 ROSA 클러스터를 생성할 때 4.11 리소스만 생성됩니다. 4.12의 계정 역할은 이전 버전과 호환되며 이는 **account-role** 정책 버전의 경우입니다. **--version** 플래그를 사용하여 4.12 리소스를 생성할 수 있습니다.

자세한 내용은 ROSA 4.12 클러스터 생성 실패 솔루션을 참조하십시오.

이 섹션에서는 Operator 정책을 포함하여 STS를 사용하는 ROSA 배포에 필요한 계정 전체 IAM 역할 및 정책에 대해 자세히 설명합니다. 정책을 정의하는 JSON 파일도 포함되어 있습니다.

계정 전체 역할 및 정책은 OpenShift 마이너 릴리스 버전 (예: OpenShift 4.8)과 관련이 있으며 이전 버전과 호환됩니다. 패치 버전에 관계없이 동일한 마이너 버전의 여러 클러스터에 대해 계정 전체 역할 및 정책을 재사용하여 필요한 STS 리소스를 최소화할 수 있습니다.

4.2.1. 계정 전체 역할 생성 방법

rosa CLI 도구 또는 OpenShift Cluster Manager Hybrid Cloud Console 안내 설치를 사용하여 계정 전체 역할을 생성할 수 있습니다. 역할을 수동으로 생성하거나 이러한 역할 및 정책에 대해 사전 정의된 이름을 사용하는 자동 프로세스를 사용할 수 있습니다.

rosa CLI 툴을 사용하여 계정 전체 역할을 생성할 수 있습니다. 역할을 수동으로 생성하거나 이러한 역할 및 정책에 대해 사전 정의된 이름을 사용하는 자동 프로세스를 사용할 수 있습니다.

수동 ocm-role 리소스 생성
필요한 CLI 액세스 권한이 있는 경우 수동 생성 방법을 사용하여 시스템에서 이러한 역할을 생성할 수 있습니다. 원하는 CLI 툴 또는 OpenShift Cluster Manager에서 이 옵션을 실행할 수 있습니다. 수동 생성 프로세스를 시작한 후 CLI는 해당 역할을 생성하여 필요한 정책에 연결할 수 있는 일련의 명령을 제공합니다.

자동 ocm-role 리소스 생성
관리 권한이 있는 **ocm-role** 리소스를 생성한 경우 OpenShift Cluster Manager에서 자동 생성 방법을 사용할 수 있습니다. **rosa** CLI에는 이러한 역할 및 정책을 자동으로 생성하기 위해 관리자 **ocm-role** IAM 리소스가 필요하지 않습니다. 이 방법을 선택하면 기본 이름을 사용하는 역할과 정책이 생성됩니다.

OpenShift Cluster Manager에서 ROSA 안내 설치를 사용하는 경우 안내 클러스터 설치의 첫 번째 단계에서 관리 권한이 있는 **ocm-role** 리소스를 생성해야 합니다. 이 역할이 없으면 자동 Operator 역할 및 정책 생성 옵션을 사용할 수 없지만 수동 프로세스를 사용하여 클러스터 및 해당 역할 및 정책을 생성할 수 있

습니다.

참고

sts_installer_trust_policy.json 및 **sts_support_trust_policy.json** 샘플에 있는 계정 번호는 필요한 역할을 가정할 수 있는 Red Hat 계정을 나타냅니다.

표 4.3. ROSA 설치 프로그램 역할, 정책 및 정책 파일

리소스	설명
ManagedOpenShift-Installer-Role	ROSA 설치 프로그램에서 사용하는 IAM 역할입니다.
ManagedOpenShift-Installer-Role-Policy	ROSA 설치 프로그램에 클러스터 설치 작업을 완료하는 데 필요한 권한을 제공하는 IAM 정책입니다.

예 4.1. sts_installer_trust_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

예 4.2. sts_installer_permission_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
```

```
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CopyImage",
                "ec2:CreateDhcpOptions",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteDhcpOptions",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteSubnet",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeleteVpc",
                "ec2:DeleteVpcEndpoints",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
```

```
                "ec2:DescribeVpcs",
                "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfiles",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
```

```
                "iam:ListUsers",
                "iam:PassRole",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:SimulatePrincipalPolicy",
                "iam:TagRole",
                "iam:UntagRole",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone",
                "route53:GetChange",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53:ListTagsForResource",
                "route53:UpdateHostedZoneComment",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketAcl",
                "s3:GetBucketCORS",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketReplication",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "sts:AssumeRole",
                "sts:AssumeRoleWithWebIdentity",
                "sts:GetCallerIdentity",
                "tag:GetResources",
                "tag:UntagResources",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions"
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        }
    ]
}
```

표 4.4. ROSA 컨트롤 플레인 역할, 정책 및 정책 파일

리소스	설명
ManagedOpenShift-ControlPlane-Role	ROSA 컨트롤 플레인에서 사용하는 IAM 역할입니다.
ManagedOpenShift-ControlPlane-Role-Policy	ROSA 컨트롤 플레인에 구성 요소를 관리하는 데 필요한 권한을 제공하는 IAM 정책입니다.

예 4.3. sts_instance_controlplane_trust_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

예 4.4. sts_instance_controlplane_permission_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
```

```
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

표 4.5. ROSA 컴퓨팅 노드 역할, 정책 및 정책 파일

리소스	설명
ManagedOpenShift-Worker-Role	ROSA 컴퓨팅 인스턴스에서 사용하는 IAM 역할입니다.
ManagedOpenShift-Worker-Role-Policy	ROSA 컴퓨팅 인스턴스에 구성 요소를 관리하는 데 필요한 권한이 있는 IAM 정책입니다.

예 4.5. sts_instance_worker_trust_policy.json

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "ec2.amazonaws.com"
            ]
         },
         "Action": [
            "sts:AssumeRole"
         ]
      }
   ]
}
```

예 4.6. sts_instance_worker_permission_policy.json

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeInstances"
            "ec2:DescribeRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

표 4.6. ROSA는 역할, 정책 및 정책 파일을 지원

리소스	설명
ManagedOpenShift-Support-Role	Red Hat SRE(Site Reliability Engineering) 지원 팀에서 사용하는 IAM 역할입니다.
ManagedOpenShift-Support-Role-Policy	ROSA 클러스터를 지원하는 데 필요한 권한을 Red Hat SRE 지원 팀에 제공하는 IAM 정책입니다.

예 4.7. sts_support_trust_policy.json

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

```
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::710019948333:role/RH-Technical-Support-Access"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

예 4.8. sts_support_permission_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
```

```
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
                "ec2:DescribeLocalGateways",
                "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
                "ec2:DescribeLocalGatewayVirtualInterfaces",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePlacementGroups",
                "ec2:DescribePrefixLists",
                "ec2:DescribePrincipalIdFormat",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeRouteTables",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGatewayConnectPeers",
                "ec2:DescribeTransitGatewayConnects",
                "ec2:DescribeTransitGatewayMulticastDomains",
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVpcAttribute",
```

```
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetAssociatedIpv6PoolCidrs",
                "ec2:GetConsoleOutput",
                "ec2:GetManagedPrefixListEntries",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:GetTransitGatewayAttachmentPropagations",
                "ec2:GetTransitGatewayMulticastDomainAssociations",
                "ec2:GetTransitGatewayPrefixListReferences",
                "ec2:GetTransitGatewayRouteTableAssociations",
                "ec2:GetTransitGatewayRouteTablePropagations",
                "ec2:ModifyInstanceAttribute",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:SearchLocalGatewayRoutes",
                "ec2:SearchTransitGatewayMulticastGroups",
                "ec2:SearchTransitGatewayRoutes",
                "ec2:StartInstances",
                "ec2:StartNetworkInsightsAnalysis",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListenerCertificates",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeSSLPolicies",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GetRole",
                "iam:ListRoles",
                "kms:CreateGrant",
                "route53:GetHostedZone",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetBucketTagging",
                "s3:GetObjectAcl",
```

```
                "s3:GetObjectTagging",
                "s3:ListAllMyBuckets"
                "sts:DecodeAuthorizationMessage",
                "tiros:CreateQuery",
                "tiros:GetQueryAnswer",
                "tiros:GetQueryExplanation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

표 4.7. ROSA Ingress Operator IAM 정책 및 정책 파일

리소스	설명
ManagedOpenShift-openshift-ingress-operator-cloud-credentials	ROSA Ingress Operator에 클러스터에 대한 외부 액세스를 관리하는 데 필요한 권한을 제공하는 IAM 정책입니다.

예 4.9. openshift_ingress_operator_cloud_credentials_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "route53:ChangeResourceRecordSets",
        "tag:GetResources"
      ],
      "Resource": "*"
    }
  ]
}
```

표 4.8. ROSA 백엔드 스토리지 IAM 정책 및 정책 파일

리소스	설명
ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials	CSI(Container Storage Interface)를 통해 백엔드 스토리지를 관리하는 데 ROSA에 필요한 IAM 정책입니다.

예 4.10. openshift_cluster_csi_drivers_ebs_cloud_credentials_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DetachVolume",
        "ec2:ModifyVolume"
      ],
      "Resource": "*"
    }
  ]
}
```

표 4.9. ROSA Machine Config Operator 정책 및 정책 파일

리소스	설명
ManagedOpenShift-openshift-machine-api-aws-cloud-credentials	ROSA Machine Config Operator에 핵심 클러스터 기능을 수행하는 데 필요한 권한을 제공하는 IAM 정책입니다.

예 4.11. openshift_machine_api_aws_cloud_credentials_policy.json

```
{
  "Version": "2012-10-17",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:RunInstances",
      "ec2:TerminateInstances",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:DeregisterTargets",
      "iam:PassRole",
      "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlainText",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:RevokeGrant",
      "kms:CreateGrant",
      "kms:ListGrants"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": true
      }
    }
  }
]
}
```

표 4.10. ROSA Cloud Credential Operator 정책 및 정책 파일

리소스	설명
ManagedOpenShift-openshift-cloud-credential-operator-cloud-credentials	ROSA Cloud Credential Operator에 클라우드 공급자 인증 정보를 관리하는 데 필요한 권한을 제공하는 IAM 정책입니다.

예 4.12. openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

표 4.11. ROSA Image Registry Operator 정책 및 정책 파일

리소스	설명
ManagedOpenShift-openshift-image-registry-installer-cloud-credentials	ROSA Image Registry Operator에 클러스터의 내부 레지스트리 스토리지를 관리하는 데 필요한 권한을 제공하는 IAM 정책입니다.

예 4.13. openshift_image_registry_installer_cloud_credentials_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
```

```
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": "*"
    }
  ]
}
```

추가 리소스

- OpenShift 메이저, 마이너 및 패치 버전에 대한 정의는 AWS 업데이트 라이프 사이클의 Red Hat OpenShift Service 를 참조하십시오.

4.2.2. 계정 전체 IAM 역할 및 정책 AWS CLI 참조

이 섹션에는 **rosa** 명령이 터미널에서 생성하는 **aws** CLI 명령이 나열됩니다. 수동 또는 자동 모드에서 명령을 실행할 수 있습니다.

계정 역할 생성에 수동 모드 사용
수동 역할 생성 모드는 검토 및 실행할 **aws** 명령을 생성합니다. 다음 명령은 해당 프로세스를 시작합니다.

```
$ rosa create account-roles --mode manual
```

참고

제공된 명령 예제에는 **ManagedOpenShift** 접두사가 포함됩니다. **--prefix** 옵션을 사용하여 사용자 정의 접두사를 지정하지 않는 경우 **ManagedOpenShift** 접두사는 기본값입니다.

명령 출력

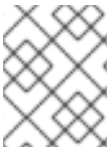
```
aws iam create-role \
 --role-name ManagedOpenShift-Installer-Role \
 --assume-role-policy-document file://sts_installer_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=installer

aws iam put-role-policy \
 --role-name ManagedOpenShift-Installer-Role \
 --policy-name ManagedOpenShift-Installer-Role-Policy \
 --policy-document file://sts_installer_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-ControlPlane-Role \
 --assume-role-policy-document file://sts_instance_controlplane_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=instance_controlplane
```

```
aws iam put-role-policy \
 --role-name ManagedOpenShift-ControlPlane-Role \
 --policy-name ManagedOpenShift-ControlPlane-Role-Policy \
 --policy-document file://sts_instance_controlplane_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-Worker-Role \
 --assume-role-policy-document file://sts_instance_worker_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=instance_worker

aws iam put-role-policy \
 --role-name ManagedOpenShift-Worker-Role \
 --policy-name ManagedOpenShift-Worker-Role-Policy \
 --policy-document file://sts_instance_worker_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-Support-Role \
 --assume-role-policy-document file://sts_support_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=support

aws iam put-role-policy \
 --role-name ManagedOpenShift-Support-Role \
 --policy-name ManagedOpenShift-Support-Role-Policy \
 --policy-document file://sts_support_permission_policy.json

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-ingress-operator-cloud-credentials \
 --policy-document file://openshift_ingress_operator_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-ingress-operator Key=operator_name,Value=cloud-
credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --policy-document file://openshift_cluster_csi_drivers_ebs_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-cluster-csi-drivers Key=operator_name,Value=ebs-cloud-
credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-machine-api-aws-cloud-credentials \
 --policy-document file://openshift_machine_api_aws_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-machine-api Key=operator_name,Value=aws-cloud-
credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-cloud-credential-operator-cloud-crede \
 --policy-document
file://openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-cloud-credential-operator
Key=operator_name,Value=cloud-credential-operator-iam-ro-creds
```

```
aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-image-registry-installer-cloud-creden \
 --policy-document file://openshift_image_registry_installer_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-image-registry Key=operator_name,Value=installer-
cloud-credentials
```

역할 생성에 자동 모드 사용
--mode auto 인수를 추가하면 **rosa** CLI 툴에서 역할과 정책을 생성합니다. 다음 명령은 해당 프로세스를 시작합니다.

```
$ rosa create account-roles --mode auto
```



참고

제공된 명령 예제에는 **ManagedOpenShift** 접두사가 포함됩니다. **--prefix** 옵션을 사용하여 사용자 정의 접두사를 지정하지 않는 경우 **ManagedOpenShift** 접두사는 기본값입니다.

명령 출력

```
I: Creating roles using 'arn:aws:iam::<ARN>:user/<UserID>'
? Create the 'ManagedOpenShift-Installer-Role' role? Yes
I: Created role 'ManagedOpenShift-Installer-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Installer-Role'
? Create the 'ManagedOpenShift-ControlPlane-Role' role? Yes
I: Created role 'ManagedOpenShift-ControlPlane-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-ControlPlane-Role'
? Create the 'ManagedOpenShift-Worker-Role' role? Yes
I: Created role 'ManagedOpenShift-Worker-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Worker-Role'
? Create the 'ManagedOpenShift-Support-Role' role? Yes
I: Created role 'ManagedOpenShift-Support-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Support-Role'
? Create the operator policies? Yes
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-machine-api-
aws-cloud-credentials'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cloud-
credential-operator-cloud-crede'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-image-registry-
installer-cloud-creden'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-ingress-
operator-cloud-credentials'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cluster-csi-
drivers-ebs-cloud-credent'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cloud-network-
config-controller-cloud'
I: To create a cluster with these roles, run the following command:
rosa create cluster --sts
```

4.3. 클러스터별 OPERATOR IAM 역할 참조

이 섹션에서는 STS를 사용하는 ROLE(Red Hat OpenShift Service on AWS) 배포에 필요한 Operator IAM

역할에 대해 자세히 설명합니다. 클러스터 Operator는 Operator 역할을 사용하여 백엔드 스토리지, 클라우드 공급자 인증 정보 관리, 클러스터에 대한 외부 액세스와 같은 클러스터 작업을 수행하는 데 필요한 임시 권한을 얻습니다.

Operator 역할을 생성하면 일치하는 클러스터 버전에 대한 계정 수준 Operator 정책이 역할에 연결됩니다. Operator 정책에는 Operator 및 호환되는 버전의 태그가 지정됩니다. Operator 역할에 대한 올바른 정책은 태그를 사용하여 결정됩니다.

참고

Operator 역할의 계정에서 두 개 이상의 일치하는 정책을 사용할 수 있는 경우 Operator를 생성할 때 대화형 옵션 목록이 제공됩니다.

표 4.12. ROSA 클러스터별 Operator 역할

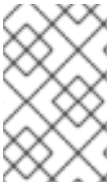
리소스	설명
<cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credentials	CSI(Container Storage Interface)를 통해 백엔드 스토리지를 관리하는 데 ROSA에 필요한 IAM 역할입니다.
<cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials	ROSA Machine Config Operator에서 핵심 클러스터 기능을 수행하는 데 필요한 IAM 역할입니다.
<cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-credentials	클라우드 공급자 인증 정보를 관리하는 데 ROSA Cloud Credential Operator에 필요한 IAM 역할입니다.
<cluster_name>-<hash>-openshift-cloud-network-config-controller-credentials	클러스터의 클라우드 네트워크 구성을 관리하는 데 클라우드 네트워크 구성 컨트롤러에 필요한 IAM 역할입니다.
<cluster_name>-<hash>-openshift-image-registry-installer-cloud-credentials	클러스터의 AWS S3의 내부 레지스트리 스토리지를 관리하는 데 ROSA Image Registry Operator에 필요한 IAM 역할입니다.
<cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials	ROSA Ingress Operator가 클러스터에 대한 외부 액세스를 관리하는 데 필요한 IAM 역할입니다.
<cluster_name>-<hash>-openshift-cloud-network-config-controller-cloud-credentials	클러스터의 클라우드 네트워크 인증 정보를 관리하는 데 클라우드 네트워크 구성 컨트롤러에 필요한 IAM 역할입니다.

4.3.1. Operator IAM 역할 AWS CLI 참조

이 섹션에는 **수동** 모드를 사용하여 다음 **rosa** 명령을 실행할 때 터미널에 표시되는 **aws** CLI 명령이 나열되어 있습니다.

-

```
$ rosa create operator-roles --mode manual --cluster <cluster_name>
```



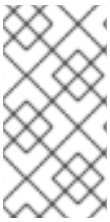
참고

수동 모드를 사용하는 경우 검토를 위해 **aws** 명령이 터미널에 출력됩니다. **aws** 명령을 검토한 후 수동으로 실행해야 합니다. 또는 **rosa create** 명령을 사용하여 **--mode auto** 를 지정하여 **aws** 명령을 즉시 실행할 수 있습니다.

명령 출력

```
aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --assume-role-policy-document file://operator_cluster_csi_drivers_ebs_cloud_credentials_policy.json
\
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-cluster-csi-drivers
Key=operator_name,Value=ebs-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-cluster-csi-drivers-
ebs-cloud-credent

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials \
 --assume-role-policy-document file://operator_machine_api_aws_cloud_credentials_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-machine-api
Key=operator_name,Value=aws-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-machine-api-aws-
cloud-credentials

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-crede \
 --assume-role-policy-document
file://operator_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-cloud-credential-operator
Key=operator_name,Value=cloud-credential-operator-iam-ro-creds

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-crede \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-cloud-credential-
operator-cloud-crede

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-image-registry-installer-cloud-creden \
 --assume-role-policy-document file://operator_image_registry_installer_cloud_credentials_policy.json
\
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-image-registry
Key=operator_name,Value=installer-cloud-credentials
```

```
aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-image-registry-installer-cloud-creden \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-image-registry-installer-cloud-creden

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials \
 --assume-role-policy-document file://operator_ingress_operator_cloud_credentials_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-ingress-operator
Key=operator_name,Value=cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-ingress-operator-cloud-credentials
```



참고

표에 제공된 명령 예제에는 **ManagedOpenShift** 접두사를 사용하는 Operator 역할이 포함되어 있습니다. Operator 정책을 포함하여 계정 전체 역할 및 정책을 생성할 때 사용자 정의 접두사를 정의한 경우 Operator 역할을 생성할 때 **--prefix <prefix_name>** 옵션을 사용하여 참조해야 합니다.

4.3.2. 사용자 정의 Operator IAM 역할 접두사 정보

AWS STS(Security Token Service)를 사용하는 각 Red Hat OpenShift Service on AWS (ROSA)에는 클러스터별 Operator IAM 역할이 필요합니다.

기본적으로 Operator 역할 이름 앞에 클러스터 이름 및 임의의 4자리 해시가 있습니다. 예를 들어 **mycluster** 라는 클러스터에 대한 Cloud Credential Operator IAM 역할에는 mycluster-< **hash>-openshift-cloud-credential-cloud-credentials** 라는 기본 이름이 있습니다. 여기서 < **hash** >는 임의의 4자리 문자열입니다.

이 기본 이름 지정 규칙을 사용하면 AWS 계정에서 클러스터의 Operator IAM 역할을 쉽게 확인할 수 있습니다.

클러스터에 대한 Operator 역할을 생성할 때 필요한 경우 < **cluster_name>-<hash** > 대신 사용할 사용자 정의 접두사를 지정할 수 있습니다. 사용자 정의 접두사를 사용하여 환경 요구 사항을 충족하기 위해 Operator 역할 이름에 논리 식별자를 추가할 수 있습니다. 예를 들어 클러스터 이름과 환경 유형(예: **mycluster-dev**)을 접두사로 지정할 수 있습니다. 이 예에서 사용자 지정 접두사가 있는 Cloud Credential Operator 역할 이름은 **mycluster-dev-openshift-cloud-credential-operator-cloud-credenti** 입니다.

참고

역할 이름은 64자로 잘립니다.

추가 리소스

- 사용자 정의 접두사를 사용하여 클러스터별 Operator IAM 역할을 생성하는 단계는 CLI를 사용하여 사용자 지정으로 클러스터 생성 또는 OpenShift Cluster Manager를 사용하여 사용자 지정으로 클러스터 생성을 참조하십시오.

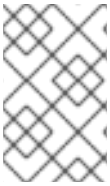
4.4. OPERATOR 인증을 위한 OIDC 공급자 요구 사항

STS를 사용하는 ROSA 설치의 경우 인증하기 위해 클러스터 Operator가 사용하는 클러스터별 OIDC 공급자를 생성해야 합니다.

4.4.1. OIDC 공급자 AWS CLI 참조

이 섹션에는 **수동** 모드를 사용하여 다음 **rosa** 명령을 실행할 때 터미널에 표시되는 **aws** CLI 명령이 나열되어 있습니다.

```
$ rosa create oidc-provider --mode manual --cluster <cluster_name>
```



참고

수동 모드를 사용하는 경우 검토를 위해 **aws** 명령이 터미널에 출력됩니다. **aws** 명령을 검토한 후 수동으로 실행해야 합니다. 또는 **rosa create** 명령을 사용하여 **--mode auto** 를 지정하여 **aws** 명령을 즉시 실행할 수 있습니다.

명령 출력

```
aws iam create-open-id-connect-provider \
 --url https://rh-oidc.s3.<aws_region>.amazonaws.com/<cluster_id> \
 --client-id-list openshift sts.amazonaws.com \
 --thumbprint-list <thumbprint> 1
```

1 **rosa create oidc-provider** 명령을 실행하면 지문이 자동으로 생성됩니다. IAM(Identity and Access Management) OpenID Connect(OIDC) ID 공급자와 함께 지문을 사용하는 방법에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

4.5. SCP(서비스 제어 정책)에 대한 최소 유효 권한 세트

SCP(서비스 제어 정책)는 조직 내의 권한을 관리하는 조직 정책의 유형입니다. SCP는 조직 내의 계정이 정의된 액세스 제어 지침에 따라 유지되도록 합니다. 이러한 정책은 AWS 조직에서 유지 관리되며 연결된 AWS 계정 내에서 사용 가능한 서비스를 제어합니다. SCP 관리는 고객의 책임입니다.

참고

AWS STS(Security Token Service)를 사용하는 경우 서비스 제어 정책에서 다음 리소스를 차단하지 않는지 확인해야 합니다.

- **ec2:{}**
- **iam:{}**
- **tag:***

SCP(서비스 제어 정책)에서 이러한 필수 권한을 제한하지 않는지 확인합니다.

	Service	작업	효과
필수 항목	Amazon EC2	All	허용
	Amazon EC2 Auto Scaling	All	허용
	Amazon S3	All	허용
	ID 및 액세스 관리	All	허용
	Elastic Load Balancing	All	허용
	Elastic Load Balancing V2	All	허용
	Amazon CloudWatch	All	허용
	Amazon CloudWatch Events	All	허용
	Amazon CloudWatch Logs	All	허용
	AWS 지원	All	허용
	AWS 키 관리 서비스	All	허용
	AWS 보안 토큰 서비스	All	허용
	AWS Marketplace	Subscription 구독 취소 서브스크립션 보기	허용
	AWS 리소스 태그	All	허용
	AWS Route53 DNS	All	허용

	Service	작업	효과
	AWS Service Quotas	ListServices GetRequestedServiceQuotaChange GetServiceQuota RequestServiceQuotaIncrease ListServiceQuotas	허용
선택 사항	AWS billinging	ViewAccount Viewbilling ViewUsage	허용
	AWS Cost and Usage Report	All	허용
	AWS Cost Explorer Services	All	허용

추가 리소스

- 서비스 제어 정책
- 권한에 대한 SCP 영향

5장. AWS에서 RED HAT OPENSHIFT SERVICE 지원 받기

ROSA(Red Hat OpenShift Service on AWS)를 지원합니다.

5.1. 지원 요청

이 문서에 설명된 절차를 수행하는 데 어려움이 있는 경우 Red Hat 고객 포털 을 참조하십시오. 고객 포털을 통해 다음을 수행할 수 있습니다.

- Red Hat 제품에 대한 기술 지원 문서의 Red Hat 지식베이스를 검색하거나 살펴보십시오.
- 다른 제품 설명서에 액세스 가능합니다.
- Red Hat 지원에 대한 지원 케이스 제출:
  a. **새 케이스 열기를** 클릭합니다.
  b. **Defect/Bug** 또는 **Account/Customer Service Request** 와 같은 지원 티켓의 이유를 선택합니다.
  c. **Product** 필드에 **OpenShift** 를 입력하여 목록을 필터링합니다. 드롭다운 메뉴에서 **AWS의 Red Hat OpenShift Service** 및 버전을 선택합니다.
  d. 나머지 필드를 완료합니다.
  e. *검토* 페이지에서 지원에 연결할 올바른 클러스터 ID를 선택하고 **제출을** 클릭합니다.

유효한 AWS 지원 계약을 맺고 AWS Business, Enterprise On-Ramp 또는 Enterprise 지원 계획을 활성화한 경우 AWS Support 에서 지원을 받을 수도 있습니다.

AWS 지원 계획을 활성화하려면 How do I sign up for an AWS Support plan?

AWS 지원 케이스 생성에 대한 자세한 내용은 AWS 지원 케이스 설명서를 참조하십시오.

이 문서를 개선하기 위한 제안이 있거나 오류를 발견한 경우 관련 문서 구성 요소에 대한 Jira 문제를 제출하십시오. AWS 버전의 섹션 이름 및 Red Hat OpenShift Service와 같은 구체적인 세부 정보를 제공해야 합니다.