aws

사용 설명서

Red Hat OpenShift Service on AWS

Red Hat OpenShift Service on AWS: 사용 설명서

Table of Contents

Red Hat OpenShift Service on AWS란 무엇인가요?

Red Hat OpenShift Service on AWS (ROSA)는 Red Hat OpenShift 엔터프라이즈 Kubernetes 플랫폼을 사용하여 컨테이너화된 애플리케이션을 빌드, 확장 및 배포하는 데 사용할 수 있는 관리형 서비스입니다 AWS.는 온프레미스 Red Hat OpenShift 워크로드를 다른 로 이전하는 과정을 ROSA 간소화하고 AWS다른와 긴밀하게 통합합니다 AWS 서비스.

특성

ROSA 는 AWS 및 Red Hat에서 공동으로 지원 및 운영됩니다. 각 ROSA 클러스터에는 Red Hat의 99.95% 가동 시간 서비스 수준 계약(SLA)을 기반으로 클러스터 관리에 대한 24시간 Red Hat 사이트 신뢰성 엔지니어(SRE) 지원이 제공됩니다. 서비스의 지원 모델에 대한 자세한 내용은 섹션을 참조하세요the section called “지원 받기”.

ROSA 는 다음 기능도 제공합니다.

- Red Hat SRE 지원 클러스터 설치, 클러스터 유지 관리, 클러스터 업그레이드.
- AWS 서비스 통합에는 AWS 컴퓨팅, 데이터베이스, 분석, 기계 학습, 네트워킹 및 모바일이 포함됩니다.
- 여러 AWS 가용 영역에서 Kubernetes 컨트롤 플레인을 실행하고 확장하여 고가용성을 보장합니다.
- OpenShift API와 개발자 생산성 도구(서비스 메시, CodeReady Workspaces, 서버리스 등)를 사용하여 클러스터를 운영합니다.

액세스 ROSA

다음 인터페이스를 사용하여 ROSA 서비스 배포를 정의하고 구성할 수 있습니다.

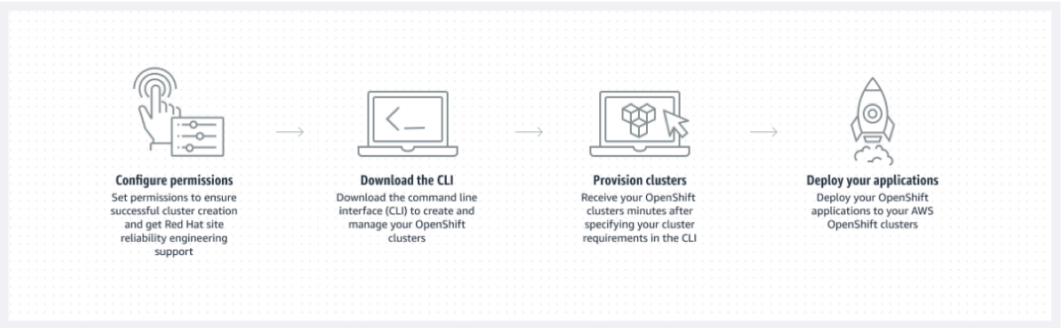
AWS

- ROSA 콘솔 - ROSA 구독을 활성화하고 ROSA 소프트웨어 계약을 구매할 수 있는 웹 인터페이스를 제공합니다.
- AWS Command Line Interface (AWS CLI) - 광범위한에 대한 명령을 제공하며 Windows, macOS 및 Linux에서 지원 AWS 서비스 됩니다. 자세한 내용은 AWS Command Line Interface 단원을 참조하십시오.

Red Hat OpenShift

- Red Hat Hybrid Cloud Console - ROSA 클러스터를 생성, 업데이트 및 관리하고, 클러스터 추가 기능을 설치하고, 클러스터에 애플리케이션을 생성 및 배포할 수 있는 웹 인터페이스를 제공합니다 ROSA .
- ROSA CLI(rosa) - ROSA 클러스터를 생성, 업데이트 및 관리하는 명령을 제공합니다.
- OpenShift CLI(oc) - 애플리케이션을 생성하고 OpenShift 컨테이너 플랫폼 프로젝트를 관리하는 명령을 제공합니다.
- Knative CLI(kn) - Knative Serving 및 Eventing과 같은 OpenShift Serverless 구성 요소와 상호 작용하는 데 사용할 수 있는 명령을 제공합니다.
- 파이프라인 CLI(tkn) - 터미널을 사용하여 OpenShift 파이프라인과 상호 작용하는 명령을 제공합니다.
- opm CLI - 운영자 개발자와 클러스터 관리자가 터미널에서 OpenShift 운영자 카탈로그를 생성하고 유지 관리하는 데 도움이 되는 명령을 제공합니다.
- 운영자 SDK CLI - 운영자 개발자가 OpenShift 운영자를 빌드, 테스트 및 배포하는 데 사용할 수 있는 명령을 제공합니다.

를 시작하는 방법 ROSA



다음은 시작하기 프로세스를 요약한 것입니다 ROSA. 자세한 시작 지침은 단원을 참조하십시오시작하기 ROSA .

AWS Management Console/AWS CLI

1. 서비스 기능을 제공하기 위해에 ROSA 의존 AWS 서비스 하는에 대한 권한을 구성합니다. 자세한 내용은 the section called “사전 조건” 단원을 참조하십시오.
2. 최신 AWS CLI 도구를 설치하고 구성합니다. 자세한 내용은 AWS CLI 사용 설명서의 최신 버전 업데이트를 AWS CLI 참조하세요.
3. ROSA 콘솔 ROSA 에서를 활성화합니다.

Red Hat 하이브리드 클라우드 콘솔/ROSA CLI

1. Red Hat Hybrid Cloud 콘솔에서 최신 버전의 ROSA CLI 및 OpenShift CLI를 다운로드합니다. 자세한 내용은 Red Hat 설명서의 ROSA CLI 시작하기를 참조하세요.
2. Red Hat Hybrid Cloud Console 또는 ROSA CLI를 사용하여 ROSA 클러스터를 생성합니다.
3. 클러스터가 준비되면 사용자에게 클러스터 액세스 권한을 부여하도록 ID 공급자를 구성합니다.
4. 다른 OpenShift 환경과 동일한 방식으로 ROSA 클러스터에 워크로드를 배포하고 관리합니다.

가격 책정

의 총 비용은 ROSA 서비스 요금과 AWS 인프라 요금이라는 두 가지 구성 요소로 ROSA 구성됩니다. 요금에 대한 자세한 내용은 Red Hat OpenShift Service on AWS 요금을 참조하십시오.

ROSA 서비스 요금

기본적으로 ROSA 서비스 요금은 작업자 노드에서 사용하는 vCPU 4개당 시간당 요금으로 온디맨드로 발생합니다. 서비스 요금은 지원되는 모든 AWS 표준 리전에서 동일합니다. 호스팅된 컨트롤 플레인(HCP) 클러스터가 있는 ROSA에는 작업자 노드 서비스 요금 외에도 시간당 클러스터 요금이 발생합니다.

ROSA 는 작업자 노드에 대한 온디맨드 서비스 요금을 절감하기 위해 구매할 수 있는 1년 및 3년 서비스 요금 계약을 제공합니다. 자세한 내용은 the section called “ROSA 계약 구매” 단원을 참조하십시오.

AWS 인프라 요금

AWS 인프라 요금은 AWS 글로벌 인프라에서 호스팅되는 기본 작업자 노드, 인프라 노드, 컨트롤 플레인 노드, 스토리지 및 네트워크 리소스에 적용됩니다. AWS 인프라 요금은 다양합니다 AWS 리전.

에 대한 책임 개요 ROSA

이 설명서에서는 Amazon Web Services ()ROSA관리형 서비스에 대한 Red Hat OpenShift Service on AWS (AWS), Red Hat 및 고객의 책임을 간략하게 설명합니다. ROSA 및 해당 구성 요소에 대한 자세한 내용은 Red Hat 설명서의 정책 및 서비스 정의를 참조하세요.

AWS 공동 책임 모델은 서비스를 실행하는 ROSA AWS 하드웨어 AWS 클라우드, 소프트웨어, 네트워킹 및 시설을 포함하여에서 제공되는 모든 서비스를 실행하는 인프라를 보호할 AWS 책임을 정의합니다 AWS 클라우드 . 이러한 AWS 책임을 일반적으로 “클라우드의 보안”이라고 합니다. 완전 관리

ROSA 형 서비스로 운영하기 위해 Red Hat과 고객은 AWS 책임 모델이 “클라우드의 보안”으로 정의하는 서비스의 요소에 대한 책임이 있습니다.

Red Hat은 ROSA 클러스터 인프라, 기본 애플리케이션 플랫폼 및 운영 체제의 지속적인 관리 및 보안을 담당합니다. ROSA 클러스터는 고객의 AWS 리소스에서 호스팅되지만 AWS 계정고객이 생성하는 IAM 역할을 통해 ROSA 서비스 구성 요소와 Red Hat 사이트 신뢰성 엔지니어(SREs)에 의해 원격으로 액세스됩니다. Red Hat은 이 액세스 권한을 사용하여 클러스터에 있는 모든 컨트롤 플레인 및 인프라 노드의 배포 및 용량을 관리하고 컨트롤 플레인 노드, 인프라 노드, 워커 노드의 버전을 유지 관리합니다.

Red Hat과 고객은 ROSA 네트워크 관리, 클러스터 로깅, 클러스터 버전 관리 및 용량 관리에 대한 책임을 공유합니다. Red Hat이 ROSA 서비스를 관리하는 동안 고객은 배포된 모든 애플리케이션, 워크로드 및 데이터를 관리하고 보호할 전적인 책임이 있습니다 ROSA.

개요

다음 표에는 AWS Red Hat 및 고객 책임에 대한 개요가 나와 있습니다 Red Hat OpenShift Service on AWS.

> **Note**
>
> 사용자에게 `cluster-admin` 역할이 추가된 경우, Red Hat 엔터프라이즈 계약 부록 4(온라인 구독 서비스)의 책임 및 제외 내용을 참조하십시오.

리소스	인시던트 및 운영 관리	변경 관리	액세스 및 ID 인증	보안 및 규정 준수	재해 복구
고객 데이터	고객	고객	고객	고객	Customer
고객 애플리케이션	고객	고객	고객	고객	Customer
개발자 서비스	고객	고객	고객	고객	Customer
플랫폼 모니터링	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat

리소스	인시던트 및 운영 관리	변경 관리	액세스 및 ID 인증	보안 및 규정 준수	재해 복구
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 관리	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객	Red Hat 및 고객
가상 컴퓨팅 관리(컨트롤 플레인, 인프라, 워커 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 관리	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS 소프트웨어(퍼블릭 AWS 서비스)	AWS	AWS	AWS	AWS	AWS
하드웨어/ AWS 글로벌 인프라	AWS	AWS	AWS	AWS	AWS

영역별 공동 책임을 위한 작업

AWS, Red Hat 및 고객은 ROSA 구성 요소의 모니터링 및 유지 관리에 대한 책임을 공유합니다. 이 설명서는 영역 및 작업별로 ROSA 서비스 책임을 정의합니다.

인시던트 및 운영 관리

AWS 는에서 제공하는 모든 서비스를 실행하는 하드웨어 인프라를 보호할 책임이 있습니다 AWS 클라우드. Red Hat은 기본 플랫폼 네트워킹에 필요한 서비스 구성 요소를 관리해야 합니다. 고객 애플리케이션 데이터와 고객이 구성했을 수 있는 모든 사용자 지정 네트워킹의 인시던트 및 운영 관리는 고객의 책임입니다.

리소스	서비스 책임	고객 책임
애플리케이션 네트워킹	Red Hat • 네이티브 OpenShift 라우터 서비스를 모니터링하고 경고에 대응합니다.	고객 • 애플리케이션 경로와 이를 뒷받침하는 엔드포인트의 상태를 모니터링합니다. • AWS 및 Red Hat에 중단을 보고합니다.
가상 네트워킹 관리	Red Hat • 기본 플랫폼 네트워킹에 필요한 AWS 로드 밸런서, Amazon VPC 서브넷 및 AWS 서비스 구성 요소를 모니터링합니다. 경고에 대응합니다.	고객 • AWS 로드 밸런서 엔드포인트의 상태를 모니터링합니다. • Amazon VPC VPC 연결 Site-to-Site VPN , 연결 또는 잠재적 문제나 보안 위협에 Direct Connect 대해 선택적으로 구성된 네트워크 트래픽을 모니터링합니다.
가상 스토리지 관리	Red Hat • 클러스터 노드에 사용되는 Amazon EBS 볼륨과 ROSA 서비스의 내장 컨테이너 이	고객 • 애플리케이션 데이터 상태를 모니터링합니다.

리소스	서비스 책임	고객 책임
	미지 레지스트리에 사용되는 Amazon S3 버킷을 모니터링합니다. 경고에 대응합니다.	• 고객 관리 AWS KMS keys 형를 사용하는 경우 Amazon EBS 암호화를 위한 키 수명 주기 및 키 정책을 생성하고 제어합니다.
AWS 소프트웨어(퍼블릭 AWS 서비스)	AWS • AWS 인시던트 및 운영 관리에 대한 자세한 내용은 AWS 백서에서 가 운영 복원성과 서비스 연속성을 AWS 유지하는 방법을 참조하세요.	Customer • 고객 계정의 AWS 리소스 상태를 모니터링합니다. • IAM 도구를 사용하여 고객 계정의 AWS 리소스에 적절한 권한을 적용합니다.
하드웨어/AWS 글로벌 인프라	AWS • AWS 인시던트 및 운영 관리에 대한 자세한 내용은 AWS 백서에서 가 운영 복원성과 서비스 연속성을 AWS 유지하는 방법을 참조하세요.	고객 • 고객 애플리케이션과 데이터를 구성, 관리, 모니터링하여 애플리케이션 및 데이터 보안 제어가 적절하게 적용되도록 합니다.

변경 관리

AWS 는에서 제공하는 모든 서비스를 실행하는 하드웨어 인프라를 보호할 책임이 있습니다 AWS 클라우드. Red Hat은 컨트롤 플레인 노드, 인프라 노드, 워커 노드의 버전을 유지 관리할 뿐만 아니라 고객이 제어할 클러스터 인프라 및 서비스를 변경할 수 있도록 지원할 책임이 있습니다. 인프라 변경을 시작하는 것은 고객의 책임입니다. 또한 고객은 옵션 서비스, 클러스터 네트워킹 구성, 고객 데이터 및 애플리케이션 변경을 설치하고 유지 관리할 책임이 있습니다.

리소스	서비스 책임	고객 책임
로깅	Red Hat	고객

리소스	서비스 책임	고객 책임
	• 플랫폼 감사 로그를 중앙에서 집계하고 모니터링합니다. • 고객이 기본 애플리케이션 로깅 목적으로 로깅 스택을 배포할 수 있도록 로깅 운영자를 제공하고 유지 관리합니다. • 고객 요청 시 감사 로그를 제공합니다.	• 클러스터에 선택적 기본 애플리케이션 로깅 운영자를 설치합니다. • 로깅 사이드카 컨테이너 또는 타사 로깅 애플리케이션과 같은 선택적 앱 로깅 솔루션을 설치, 구성, 유지 관리합니다. • 로깅 스택 또는 클러스터의 안정성에 영향을 미치는 경우 고객 애플리케이션에서 생성되는 애플리케이션 로그의 크기와 빈도를 조정합니다. • 지원 사례를 통해 플랫폼 감사 로그를 요청하여 특정 인시던트를 조사합니다.

리소스	서비스 책임	고객 책임
애플리케이션 네트워킹	Red Hat • 퍼블릭 로드 밸런서를 설정합니다. 필요한 경우 사설 로드 밸런서와 최대 1개의 추가 로드 밸런서를 설정할 수 있는 기능을 제공합니다. • 네이티브 OpenShift 라우터 서비스를 설정합니다. 라우터를 비공개로 설정하고 라우터 샤드를 최대 1개까지 추가할 수 있는 기능을 제공합니다. • 기본 내부 포드 트래픽을 위한 OpenShift SDN 구성 요소를 설치, 구성, 유지 관리합니다. • 고객이 `NetworkPolicy` 및 `EgressNetworkPolicy` (방화벽) 객체를 관리할 수 있는 기능을 제공합니다.	고객 • `NetworkPolicy` 객체를 사용한 프로젝트 및 포드 네트워크, 포드 수신, 포드 송신 등에 기본이 아닌 포드 네트워크 권한을 구성합니다. • OpenShift 클러스터 관리자를 사용하여 기본 애플리케이션 경로에 대한 프라이빗 로드 밸런서를 요청합니다. • OpenShift 클러스터 관리자를 사용하여 최대 1개의 퍼블릭 또는 프라이빗 라우터 샤드와 해당 로드 밸런서를 추가로 구성합니다. • 특정 서비스를 위한 추가 서비스 로드 밸런서를 요청하고 구성합니다. • 필요한 DNS 전달 규칙을 모 구성합니다.

리소스	서비스 책임	고객 책임
클러스터 네트워킹	Red Hat • 퍼블릭 또는 프라이빗 서비스 엔드포인트 및 구성 요소와의 필수 통합과 같은 클러스터 관리 Amazon VPC구성 요소를 설정합니다. • 워커, 인프라, 컨트롤 플레인 노드 간의 내부 클러스터 통신에 필요한 내부 네트워킹 구성 요소를 설정합니다.	고객 • 클러스터가 프로비저닝될 때 필요한 경우 OpenShift 클러스터 관리자를 통해 시스템 CIDR, 서비스 CIDR, 포드 CIDR에 대해 기본이 아닌 IP 주소 범위를 선택 사항으로 제공합니다. • OpenShift 클러스터 관리자를 통해 클러스터를 생성할 때, 또는 클러스터를 생성한 후에 API 서비스 엔드포인트를 퍼블릭 또는 프라이빗으로 설정하도록 요청합니다.

리소스	서비스 책임	고객 책임
가상 네트워킹 관리	Red Hat • 서브넷, 로드 밸런서, 인터넷 게이트웨이, NAT 게이트웨이 등 클러스터를 프로비저닝하는 데 필요한 Amazon VPC 구성 요소를 설정하고 구성합니다. • 고객이 OpenShift Cluster Manager를 통해 필요에 Direct Connect 따라 온프레미스 리소스와의 Site-to-Site VPN 연결, VPC Amazon VPC간 연결을 관리할 수 있는 기능을 제공합니다. • 고객이 서비스 AWS 로드 밸런서에 사용할 로드 밸런서를 생성하고 배포할 수 있습니다.	Customer • Amazon VPC VPC 연결, 연결 Site-to-Site VPN 또는 같은 선택적 Amazon VPC 구성 요소를 설정하고 유지 관리합니다 Direct Connect. • 특정 서비스를 위한 추가 로드 밸런서를 요청하고 구성합니다.
가상 컴퓨팅 관리	Red Hat • 클러스터 컴퓨팅에 Amazon EC2 인스턴스를 사용하도록 ROSA 컨트롤 플레인과 데이터 플레인을 설정하고 구성합니다. • 클러스터에서 Amazon EC2 컨트롤 플레인 및 인프라 노드의 배포를 모니터링하고 관리합니다.	Customer • OpenShift Cluster Manager 또는 ROSA CLI를 사용하여 머신 풀을 생성하여 Amazon EC2 작업자 노드를 모니터링하고 관리합니다. • 고객이 배포한 애플리케이션 및 애플리케이션 데이터의 변경 사항을 관리합니다.

리소스	서비스 책임	고객 책임
클러스터 버전	Red Hat • 업그레이드 예약 프로세스를 활성화합니다. • 업그레이드 진행 상황을 모니터링하고 문제가 발생할 경우 해결합니다. • 마이너 업그레이드 및 유지 관리 업그레이드의 변경 로그와 릴리스 노트를 게시합니다.	고객 • 유지 관리 버전 업그레이드를 즉시 예약하거나 향후 자동 업그레이드합니다. • 마이너 버전 업그레이드를 확인하고 예약합니다. • 클러스터 버전이 지원되는 마이너 버전으로 유지되는지 확인합니다. • 마이너 버전과 유지 관리 버전에서 고객 애플리케이션을 테스트하여 호환성을 보장합니다.
용량 관리	Red Hat • 컨트롤 플레인 사용을 모니터링합니다. 컨트롤 플레인에는 컨트롤 플레인 노드와 인프라 노드가 포함됩니다. • 컨트롤 플레인 노드의 규모와 크기를 조정하여 서비스 품질을 유지합니다.	고객 • 워커 노드 사용률을 모니터링하고 필요한 경우 Auto Scaling 기능을 활성화합니다. • 클러스터의 규모 조정 전략을 결정합니다. • 제공된 OpenShift 클러스터 관리자 컨트롤을 사용하여 필요에 따라 워커 노드를 추가하거나 제거합니다. • 클러스터 리소스 요구 사항에 관한 Red Hat 알림에 대응합니다.

리소스	서비스 책임	고객 책임
가상 스토리지 관리	Red Hat • 클러스터에 로컬 노드 스토리지와 영구 볼륨 스토리지를 프로비저닝 Amazon EBS 하도록를 설정하고 구성합니다. • Amazon S3 버킷 스토리지를 사용하도록 내장 이미지 레지스트리를 설정하고 구성합니다. • 에서 이미지 레지스트리 리소스를 정기적으로 정리 Amazon S3 하여 Amazon S3 사용량과 클러스터 성능을 최적화합니다.	Customer • 선택적으로 클러스터에 영구 볼륨을 프로비저닝하도록 Amazon EBS CSI 드라이버 또는 Amazon EFS CSI 드라이버를 구성합니다.

리소스	서비스 책임	고객 책임

AWS 소프트웨어(퍼블릭 AWS 서비스)	AWS
	
	컴퓨팅
	
	• ROSA 컨트롤 플레인, 인프라 및 작업자 노드에 사용되는 Amazon EC2 서비스를 제공합니다.
	
	스토리지
	
	• ROSA 서비스가 클러스터에 로컬 노드 스토리지와 영구 볼륨 스토리지를 프로비저닝할 수 Amazon EBS 있도록를 제공합니다.
	
	네트워킹
	
	• ROSA 가상 네트워킹 인프라 요구 사항을 충족하기 위해 다음 AWS 클라우드 서비스를 제공합니다.
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• ROSA다음과 같은 선택적 AWS 서비스 통합을 제공합니다.
	  • Site-to-Site VPN
	  • Direct Connect
	  • AWS PrivateLink
	  • AWS Transit Gateway
		Customer
		
		• 보안 IAM 주체 또는 AWS STS 임시 보안 자격 증명과 연결된 액세스 키 ID 및 보안 액세스 키를 사용하여 요청에 서명합니다.
		• 클러스터 생성 시 사용할 클러스터의 VPC 서브넷을 지정합니다.
		• 선택적으로 ROSA 클러스터에 사용할 고객 관리형 VPC를 구성합니다.

리소스	서비스 책임	고객 책임
하드웨어/AWS 글로벌 인프라	AWS • AWS 데이터 센터의 관리 제어에 대한 자세한 내용은 AWS 클라우드 보안 페이지의 제어 섹션을 참조하세요. • 변경 관리 모범 사례에 대한 자세한 내용은 AWS 솔루션 라이브러리의 에서 변경 관리를 위한 지침을 AWS 참조하세요.	Customer • AWS 클라우드에서 호스팅되는 고객 애플리케이션 및 데이터에 대한 변경 관리 모범 사례를 구현합니다.

액세스 및 ID 인증

액세스 및 ID 인증에는 클러스터, 애플리케이션, 인프라 리소스에 대하여 승인된 액세스를 관리할 책임이 포함됩니다. 여기에는 액세스 제어 메커니즘 제공, 인증, 권한 부여, 리소스 액세스 관리 등의 작업이 포함됩니다.

리소스	서비스 책임	고객 책임
로깅	Red Hat • 플랫폼 감사 로그에 대한 업계 표준 기반 계층형 내부 액세스 프로세스를 준수합니다. • 네이티브 OpenShift RBAC 기능을 제공합니다.	고객 • 프로젝트 액세스는 물론 프로젝트의 애플리케이션 로그까지 제어하도록 OpenShift RBAC를 구성합니다. • 타사 또는 맞춤형 애플리케이션 로깅 솔루션의 경우 액세스 관리는 고객의 책임입니다.
애플리케이션 네트워킹	Red Hat	고객 • 필요에 따라 경로 구성에 대한 액세스를 제어하도록

리소스	서비스 책임	고객 책임
	• 네이티브 OpenShift RBAC 및 `dedicated-admin` 기능을 제공합니다.	OpenShift `dedicated-admin` 및 RBAC를 구성합니다. • Red Hat에서 OpenShift 클러스터 관리자 액세스 권한을 부여할 수 있도록 Red Hat 조직 관리자를 관리합니다. 클러스터 관리자는 라우터 옵션을 구성하고 서비스 로드 밸런서 할당량을 제공하는 데 사용됩니다.
클러스터 네트워킹	Red Hat • OpenShift 클러스터 관리자를 통해 고객 액세스 제어를 제공합니다. 네이티브 OpenShift RBAC 및 `dedicated-admin` 기능을 제공합니다.	고객 • 필요에 따라 경로 구성에 대한 액세스를 제어하도록 OpenShift `dedicated-admin` 및 RBAC를 구성합니다. • Red Hat 계정의 Red Hat 조직 멤버십을 관리합니다. • Red Hat에서 OpenShift 클러스터 관리자 액세스 권한을 부여할 수 있도록 조직 관리자를 관리합니다.
가상 네트워킹 관리	Red Hat • OpenShift 클러스터 관리자를 통해 고객 액세스 제어를 제공합니다.	고객 • OpenShift Cluster Manager를 통해 구성 AWS 요소에 대한 선택적 사용자 액세스를 관리합니다.

리소스	서비스 책임	고객 책임
가상 컴퓨팅 관리	Red Hat • OpenShift 클러스터 관리자를 통해 고객 액세스 제어를 제공합니다.	고객 • OpenShift Cluster Manager를 통해 구성 AWS 요소에 대한 선택적 사용자 액세스를 관리합니다. • ROSA 서비스 액세스를 활성화하는 데 필요한 IAM 역할 및 연결된 정책을 생성합니다.
가상 스토리지 관리	Red Hat • OpenShift 클러스터 관리자를 통해 고객 액세스 제어를 제공합니다.	고객 • OpenShift Cluster Manager를 통해 구성 AWS 요소에 대한 선택적 사용자 액세스를 관리합니다. • ROSA 서비스 액세스를 활성화하는 데 필요한 IAM 역할 및 연결된 정책을 생성합니다.

리소스	서비스 책임	고객 책임
AWS 소프트웨어(퍼블릭 AWS 서비스)	AWS 컴퓨팅 • ROSA 컨트롤 플레인, 인프라 및 작업자 노드에 사용되는 Amazon EC2 서비스를 제공합니다. 스토리지 • 가 클러스터에 로컬 노드 스토리지와 영구 볼륨 스토리지를 프로비저닝 ROSA 하도록 허용하는 데 Amazon EBS사용되는를 제공합니다. • 서비스의 기본 제공 이미지 레지스트리에 Amazon S3사용되는를 제공합니다. 네트워킹 • 고객이 고객 계정에서 실행되는 ROSA 리소스에 대한 액세스를 제어하는 데 사용하는 Provide AWS Identity and Access Management (IAM)입니다.	Customer • ROSA 서비스 액세스를 활성화하는 데 필요한 IAM 역할 및 연결된 정책을 생성합니다. • IAM 도구를 사용하여 고객 계정의 AWS 리소스에 적절한 권한을 적용합니다. • AWS 조직 ROSA 전체에서를 활성화하기 위해 고객은 AWS Organizations 관리자를 관리할 책임이 있습니다. • AWS 조직 ROSA 전체에서를 활성화하기 위해 고객은를 사용하여 ROSA 권한 부여를 배포할 책임이 있습니다 AWS License Manager.

리소스	서비스 책임	고객 책임
하드웨어/AWS 글로벌 인프라	AWS • AWS 데이터 센터의 물리적 액세스 제어에 대한 자세한 내용은 AWS 클라우드 보안 페이지의 제어 섹션을 참조하세요.	Customer • 고객은 AWS 글로벌 인프라에 대해 책임을 지지 않습니다.

보안 및 규정 준수

규정 준수와 관련된 책임 및 제어는 다음과 같습니다.

리소스	서비스 책임	고객 책임
로깅	Red Hat • 보안 이벤트 분석을 위해 클러스터 감사 로그를 Red Hat SIEM으로 전송합니다. 포렌식 분석을 지원하기 위해 지정된 기간 동안 감사 로그를 보존합니다.	고객 • 애플리케이션 로그에서 보안 이벤트를 분석합니다. • 애플리케이션 로그를 기본 로깅 스택에서 제공하는 것보다 더 오래 보존해야 하는 경우 로깅 사이드카 컨테이너 또는 타사 로깅 애플리케이션을 통해 외부 엔드포인트로 전송합니다.
가상 네트워킹 관리	Red Hat • 가상 네트워킹 구성 요소를 모니터링하여 잠재적 문제 및 보안 위협을 확인합니다. • 추가 모니터링 및 보호를 위해 퍼블릭 AWS 도구를 사용합니다.	고객 • 선택적으로 구성된 가상 네트워킹 구성 요소를 모니터링하여 잠재적 문제 및 보안 위협을 확인합니다. • 필요에 따라 필수 방화벽 규칙 또는 고객 데이터 센터 보호를 구성합니다.

리소스	서비스 책임	고객 책임
가상 컴퓨팅 관리	Red Hat • 가상 컴퓨팅 구성 요소를 모니터링하여 잠재적 문제 및 보안 위협을 확인합니다. • 추가 모니터링 및 보호를 위해 퍼블릭 AWS 도구를 사용합니다.	고객 • 선택적으로 구성된 가상 네트워킹 구성 요소를 모니터링하여 잠재적 문제 및 보안 위협을 확인합니다. • 필요에 따라 필수 방화벽 규칙 또는 고객 데이터 센터 보호를 구성합니다.

리소스	서비스 책임	고객 책임
가상 스토리지 관리	Red Hat • 가상 스토리지 구성 요소를 모니터링하여 잠재적 문제 및 보안 위협을 확인합니다. • 추가 모니터링 및 보호를 위해 퍼블릭 AWS 도구를 사용합니다. • 에서 Amazon EBS 제공하는 AWS 관리형 KMS 키를 사용하여 기본적으로 컨트롤 플레인, 인프라 및 작업자 노드 볼륨 데이터를 암호화하도록 ROSA 서비스를 구성합니다. • 가 Amazon EBS 제공하는 AWS 관리형 KMS 키로 기본 스토리지 클래스를 사용하는 고객 영구 볼륨을 암호화하도록 ROSA 서비스를 구성합니다. • 고객이 고객 관리형를 사용하여 영구 볼륨을 암호화 KMS key 할 수 있는 기능을 제공합니다. • Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-3)를 사용하여 유휴 이미지 레지스트리 데이터를 암호화하도록 컨테이너 이미지 레지스트리를 구성합니다. • 고객이 퍼블릭 또는 프라이빗 Amazon S3 이미지 레지스트리를 생성하여 무단 사용자 액세스로부터 컨테이너	Customer • Amazon EBS 볼륨을 프로비저닝합니다. • Amazon EBS 볼륨 스토리지를 관리하여 볼륨으로 탑재할 수 있는 충분한 스토리지를 확보합니다 ROSA. • OpenShift 클러스터 관리자를 통해 영구 볼륨 클레임을 만들고 영구 볼륨을 생성합니다.

리소스	서비스 책임	고객 책임
	이미지를 보호할 수 있는 기능을 제공합니다.	

리소스	서비스 책임	고객 책임
AWS 소프트웨어(퍼블릭 AWS 서비스)	AWS 컴퓨팅 • ROSA 컨트롤 플레 Amazon EC2인, 인프라 및 작업자 노드에 사용되는를 제공합니다. 자세한 내용은 Amazon EC2 사용 설명서의의 인프라 보안을 Amazon EC2 참조하세요. 스토리지 • ROSA 컨트롤 플레 Amazon EBS인, 인프라 및 작업자 노드 볼륨과 Kubernetes 영구 볼륨에 사용되는를 제공합니다. 자세한 내용은 Amazon EC2 사용 설명서의의 데이터 보호를 Amazon EC2 참조하세요. • AWS KMS를 ROSA 사용하여 컨트롤 플레인, 인프라, 작업자 노드 볼륨 및 영구 볼륨을 암호화합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EBS 암호화를 참조하세요. • ROSA 서비스의 기본 제공 컨테이너 이미지 레지스트리에 Amazon S3사용되는를 제공합니다. 자세한 내용은 Amazon S3 사용 설명서의	Customer • Amazon EC2 인스턴스의 데이터를 보호하기 위해 보안 모범 사례와 최소 권한 원칙을 따라야 합니다. 자세한 내용은 Amazon EC2인프라 보안 및 Amazon EC2데이터 보호를 참조하세요. • 선택적으로 구성된 가상 네트워킹 구성 요소를 모니터링하여 잠재적 문제 및 보안 위협을 확인합니다. • 필요에 따라 필수 방화벽 규칙 또는 고객 데이터 센터 보호를 구성합니다. • 선택적 고객 관리형 KMS 키를 생성하고 KMS 키를 사용하여 Amazon EBS 영구 볼륨을 암호화합니다. • 가상 스토리지에서 고객 데이터를 모니터링하여 잠재적 문제 및 보안 위협을 확인합니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

리소스	서비스 책임	고객 책임
	Amazon S3 보안을 참조하세요. 네트워킹 • 보안 기능 및 서비스를 제공하여 내장된 네트워크 방화벽, Amazon VPC프라이빗 또는 전용 네트워크 연결, AWS 보안 시설 간 AWS 글로벌 및 리전 네트워크의 모든 트래픽 자동 암호화를 포함하여 AWS 글로벌 인프라에서 개인 정보 보호를 강화하고 네트워크 액세스를 제어합니다. 자세한 내용은 보안 소개 백서의 AWS 공동 책임 모델 및 인프라 AWS 보안을 참조하세요.	
하드웨어/AWS 글로벌 인프라	AWS • 가 서비스 기능을 제공하는 데 ROSA 사용하는 AWS 글로벌 인프라를 제공합니다. AWS 보안 제어에 대한 자세한 내용은 AWS 백서의 AWS 인프라 보안을 참조하세요. • 고객이 규정 준수 요구 사항을 관리하고 AWS Artifact 및 AWS Security Hub와 같은 도구를 AWS 사용하여에서 보안 상태를 확인할 수 있도록 설명서를 제공합니다.	고객 • 고객 애플리케이션과 데이터를 구성, 관리, 모니터링하여 애플리케이션 및 데이터 보안 제어가 적절하게 적용되도록 합니다. • IAM 도구를 사용하여 고객 계정의 AWS 리소스에 적절한 권한을 적용합니다.

재해 복구

재해 복구에는 데이터 및 구성 백업, 데이터 복제 및 재해 복구 환경 구성, 재해 이벤트 시 장애 조치가 포함됩니다.

리소스	서비스 책임	고객 책임
가상 네트워킹 관리	Red Hat • 플랫폼이 작동하는 데 필요하며 영향이 있는 가상 네트워크 구성 요소를 복원하거나 다시 생성합니다.	고객 • 가능한 경우, 중단 상황 시 보호할 수 있도록 둘 이상의 터널로 가상 네트워킹 연결을 구성합니다. • 여러 클러스터가 있는 글로벌 로드 밸런서를 사용하는 경우 장애 조치 DNS 및 부하 분산을 유지합니다.
가상 컴퓨팅 관리	Red Hat • 클러스터를 모니터링하고 실패한 Amazon EC2 컨트롤 플레인 또는 인프라 노드를 교체합니다. • 장애가 발생한 워커 노드를 수동 또는 자동으로 교체할 수 있는 기능을 고객에게 제공합니다.	고객 • OpenShift Cluster Manager 또는 ROSA CLI를 통해 머신 풀 구성을 편집하여 장애가 발생한 Amazon EC2 작업자 노드를 교체합니다.
가상 스토리지 관리	Red Hat • IAM 사용자 자격 증명으로 AWS 생성된 ROSA 클러스터의 경우 시간별, 일별 및 주별 볼륨 스냅샷을 통해 클러스터의 모든 Kubernetes 객체를 백업합니다.	고객 • 고객 애플리케이션과 애플리케이션 데이터를 백업합니다.

리소스	서비스 책임	고객 책임
AWS 소프트웨어(퍼블릭 AWS 서비스)	AWS 컴퓨팅 • Amazon EBS 스냅샷 및와 같은 데이터 복원력을 지원하는 Amazon EC2 기능을 제공합니다 Amazon EC2 Auto Scaling. 자세한 내용은 Amazon EC2 사용 설명서의 의 복원력을 Amazon EC2 참조하세요. 스토리지 • ROSA 서비스 및 고객이 Amazon EBS 볼륨 스냅샷을 통해 클러스터에 Amazon EBS 볼륨을 백업할 수 있는 기능을 제공합니다. • 데이터 복원력을 지원하는 Amazon S3 기능에 대한 자세한 내용은 Resilience in Amazon S3을 참조하세요. 네트워킹 • 데이터 복원력을 지원하는 Amazon VPC 기능에 대한 자세한 내용은 Amazon VPC 사용 설명서의 의 복원력을 Amazon Virtual Private Cloud 참조하세요.	Customer • 내결함성 및 클러스터 가용성을 개선하도록 ROSA 다중 AZ 클러스터를 구성합니다. • Amazon EBS CSI 드라이버를 사용하여 영구 볼륨을 프로비저닝하여 볼륨 스냅샷을 활성화합니다. • Amazon EBS 영구 볼륨의 CSI 볼륨 스냅샷을 생성합니다.

리소스	서비스 책임	고객 책임
하드웨어/AWS 글로벌 인프라	AWS • 가 가용 영역 전체에서 컨트롤 플레인, 인프라 및 작업자 노드 ROSA 를 확장할 수 있는 AWS 글로벌 인프라를 제공합니다. 이 기능을 사용하면 ROSA 가 중단 없이 영역 간에 자동 장애 조치를 조정할 수 있습니다. • 재해 복구 모범 사례에 대한 자세한 내용은 AWS Well-Architected Framework의 클라우드에서 재해 복구 옵션을 참조하세요.	Customer • 내결함성 및 클러스터 가용성을 개선하도록 ROSA 다중 AZ 클러스터를 구성합니다.

데이터 및 애플리케이션에 대한 고객 책임

고객은 배포하는 애플리케이션, 워크로드 및 데이터에 대한 책임이 있습니다 Red Hat OpenShift Service on AWS. 그러나 AWS 및 Red Hat은 고객이 플랫폼에서 데이터와 애플리케이션을 관리하는 데 도움이 되는 다양한 도구를 제공합니다.

리소스	AWS 및 Red Hat이 도움이 되는 방법	고객 책임
고객 데이터	Red Hat • 업계 보안 및 규정 준수 표준에 정의된 대로 데이터 암호화 시 플랫폼 수준의 표준을 유지합니다. • 비밀 등 애플리케이션 데이터를 관리하는 데 도움이 되	고객 • 플랫폼에 저장된 모든 고객 데이터 및 고객 애플리케이션이 데이터를 소비하고 노출하는 방식에 대한 책임을 유지합니다.

리소스	AWS 및 Red Hat이 도움이 되는 방법	고객 책임
	는 OpenShift 구성 요소를 제공합니다. • 와 같은 데이터 서비스와의 통합을 활성화 Amazon RDS 하여 클러스터 외부 및/또는 외부에서 데이터를 저장하고 관리합니다 AWS. AWS • 고객이 클러스터 외부에서 데이터를 저장하고 관리할 수 Amazon RDS 있도록를 제공합니다.	

리소스	AWS 및 Red Hat이 도움이 되는 방법	고객 책임
고객 애플리케이션	Red Hat • 고객이 OpenShift 및 Kubernetes APIs하여 컨테이너화된 애플리케이션을 배포하고 관리할 수 있도록 OpenShift 구성 요소가 설치된 클러스터를 프로비저닝합니다. • 고객 배포 시 Red Hat 컨테이너 카탈로그 레지스트리에서 이미지를 가져올 수 있도록 이미지 풀 보안 암호가 있는 클러스터를 생성합니다. • 고객이 클러스터에 커뮤니티, 타사 AWS및 Red Hat 서비스를 추가하도록 연산자를 설정하는 데 사용할 수 있는 OpenShift APIs에 대한 액세스 권한을 제공합니다. • 고객 애플리케이션에서 사용할 영구 볼륨을 지원하는 스토리지 클래스 및 플러그인을 제공합니다. • 고객이 클러스터에 애플리케이션 컨테이너 이미지를 안전하게 저장하여 애플리케이션을 배포하고 관리할 수 있도록 컨테이너 이미지 레지스트리를 제공합니다. AWS	고객 • 고객 애플리케이션과 타사 애플리케이션, 데이터, 전체 애플리케이션 수명에 대한 책임을 유지합니다. • 고객이 운영자 또는 외부 이미지를 사용하여 Red Hat 서비스, 커뮤니티 서비스, 타사 서비스, 자체 서비스 또는 기타 서비스를 클러스터에 추가하는 경우, 이러한 서비스에 대한 책임 및 적절한 제공업체(Red Hat 포함)와 협력하여 문제를 해결할 책임은 고객에게 있습니다. • 구성 및 배포, 최신 상태 유지, 리소스 요청 및 제한 설정, 앱 실행에 충분한 리소스를 보유하도록 클러스터 크기 조정 , 권한 설정, 다른 서비스와의 통합, 고객이 배포한 이미지 스트림 또는 템플릿 관리, 외부 서비스, 데이터 저장, 백업, 복원, 기타 가용성과 복원력이 뛰어난 워크로드 관리 등을 수행하기 위해 제공된 도구 및 기능을 사용합니다. • 지표를 수집하고 Red Hat OpenShift Service on AWS, 알림을 생성하고, 애플리케이션의 보안 암호를 보호하

리소스	AWS 및 Red Hat이 도움이 되는 방법	고객 책임
	• Amazon EBS 를 제공하여 고객 애플리케이션에 사용할 영구 볼륨을 지원합니다. • Amazon S3 를 제공하여 컨테이너 이미지 레지스트리의 Red Hat 프로비저닝을 지원합니다.	기 위한 소프트웨어 설치 및 운영 등에서 실행되는 애플리케이션을 모니터링할 책임을 유지합니다.

ROSA 아키텍처

Red Hat OpenShift Service on AWS (ROSA)에는 다음과 같은 클러스터 토폴로지가 있습니다.

- 호스팅 컨트롤 플레인(HCP) - 컨트롤 플레인은 Red Hat의 내에서 호스팅 AWS 계정 되고 Red Hat 에서 관리합니다. 작업자 노드는 고객의에 배포됩니다 AWS 계정.
- 클래식 - 컨트롤 플레인 및 작업자 노드가 고객의에 배포됩니다 AWS 계정.

ROSA with HCP는 실행 시 발생하는 AWS 인프라 비용을 줄이고 클러스터 생성 시간을 단축하는 데 도움이 되는 보다 효율적인 컨트롤 플레인 아키텍처 ROSA 를 제공합니다. ROSA 콘솔에서 ROSA with HCP 및 ROSA 클래식을 AWS 모두 활성화할 수 있습니다. ROSA CLI를 사용하여 ROSA 클러스터를 프로비저닝할 때 사용할 아키텍처를 선택할 수 있습니다.

> **Note**
>
> - ROSA 는 클래식 및 호스팅 컨트롤 플레인 아키텍처 모두에서 FedRAMP High 및 HIPAA 적격 규정 준수 인증을 AWS GovCloud에 제공합니다. 자세한 내용은 Red Hat 설명서에서 규정 준수를 참조하세요.
> - ROSA 는 클래식 및 호스팅 컨트롤 플레인 아키텍처 모두에서 Federal Information Processing Standard(FIPS) 엔드포인트 in AWS GovCloud를 제공합니다.

ROSA와 HCP 및 ROSA 클래식 비교

다음 표에서는 ROSA를 HCP 및 ROSA 클래식 아키텍처 모델과 비교합니다.

	ROSA with HCP	ROSA 클래식
클러스터 인프라 호스팅	etcd, API 서버 및 oauth와 같은 컨트롤 플레인 구성 요소는 Red Hat 소유에서 호스팅됩니다 AWS 계정.	etcd, API 서버 및 oauth와 같은 컨트롤 플레인 구성 요소는 고객 소유의에서 호스팅됩니다 AWS 계정.
Amazon VPC	작업자 노드는를 통해 컨트롤 플레인과 통신합니다AWS PrivateLink.	작업자 노드와 컨트롤 플레인 노드는 고객의 VPC에 배포됩니다.
AWS Identity and Access Management	AWS 관리형 정책을 사용합니다.	서비스에서 정의한 고객 관리형 정책을 사용합니다.
다중 영역 배포	컨트롤 플레인은 여러 가용 영역(AZs.	컨트롤 플레인은 단일 AZ 내에 또는 여러 AZs.
인프라 노드	전용 인프라 노드를 사용하지 않습니다. 플랫폼 구성 요소는 작업자 노드에 배포됩니다.	단일 AZ 2개 또는 다중 AZ 전용 노드 3개를 사용하여 플랫폼 구성 요소를 호스팅합니다.
OpenShift 기능	플랫폼 모니터링, 이미지 레지스트리 및 수신 컨트롤러는 작업자 노드에 배포됩니다.	플랫폼 모니터링, 이미지 레지스트리 및 수신 컨트롤러는 전용 인프라 노드에 배포됩니다.
클러스터 업그레이드	컨트롤 플레인과 각 머신 풀은 별도로 업그레이드할 수 있습니다.	전체 클러스터를 동시에 업그레이드해야 합니다.
최소 Amazon EC2 공간	클러스터를 생성하려면 두 개의 Amazon EC2 인스턴스가 필요합니다.	클러스터를 생성하려면 단일 AZ 인스턴스 7개 또는 다중 AZ Amazon EC2 인스턴스 9개가 필요합니다.
AWS 리전	AWS 리전 가용성은 AWS 일반 참조 안내서의 Red Hat OpenShift Service on AWS 엔	AWS 리전 가용성은 AWS 일반 참조 안내서의 Red Hat OpenShift Service on AWS 엔

	ROSA with HCP	ROSA 클래식
	드포인트 및 할당량을 참조하세요.	드포인트 및 할당량을 참조하세요.

시작하기 ROSA

Red Hat OpenShift Service on AWS (ROSA)는 Red Hat OpenShift 엔터프라이즈 Kubernetes 플랫폼을 사용하여 컨테이너화된 애플리케이션을 빌드, 확장 및 배포하는 데 사용할 수 있는 관리형 서비스입니다 AWS.

다음 가이드를 사용하여 첫 번째 ROSA 클러스터를 생성하고, 사용자에게 액세스 권한을 부여하고, 첫 번째 애플리케이션을 배포하고, 사용자 액세스를 취소하고 클러스터를 삭제하는 방법을 배울 수 있습니다.

- the section called “ ROSA HCP 클러스터 생성 - CLI” - AWS STS 및 ROSA CLI를 사용하여 첫 번째 ROSA with HCP 클러스터를 생성합니다.
- the section called “ROSA 클래식 클러스터 생성 - AWS PrivateLink ” -를 사용하여 첫 번째 ROSA 클래식 클러스터를 생성합니다 AWS PrivateLink.
- the section called “ROSA 클래식 클러스터 생성 - CLI” - AWS STS 및 ROSA CLI를 사용하여 첫 번째 ROSA 클래식 클러스터를 생성합니다.

를 사용하도록 설정 ROSA

ROSA 클러스터 생성을 위한 환경을 준비하려면 다음 작업을 완료해야 합니다.

사전 조건

ROSA 클러스터 생성을 활성화하려면 다음 사전 조건을 충족해야 합니다.

- 최신를 설치하고 구성합니다 AWS CLI. 자세한 내용은 최신 버전의 AWS CLI설치 또는 업데이트를 참조하세요.
- 최신 ROSA CLI 및 OpenShift 컨테이너 플랫폼 CLI를 설치하고 구성합니다. 자세한 내용은 ROSA CLI 시작하기를 참조하세요.
- Amazon EC2 Amazon VPC Amazon EBS, 및에 대해 필수 서비스 할당량이 설정되어 있어야 합니다 Elastic Load Balancing. AWS 또는 문제 해결에 필요한 경우 Red Hat이 사용자를 대신하여 서비스 할당량 증가를 요청할 수 있습니다. 에 필요한 서비스 할당량을 보려면 AWS 일반 참조의 엔드포인트 및 할당량을 ROSA참조하세요. Red Hat OpenShift Service on AWS
- 에 대한 AWS 지원을 받으려면 AWS Business ROSA, Enterprise On-Ramp 또는 Enterprise 지원 플랜을 활성화해야 합니다. Red Hat은 문제 해결에 필요한 경우 사용자를 대신하여 AWS 지원을 요청

할 수 있습니다. 자세한 내용은 the section called “지원 받기” 단원을 참조하십시오. 활성화하려면 지원 페이지를 지원참조하세요.

- AWS Organizations 를 사용하여 ROSA 서비스를 호스팅 AWS 계정 하는를 관리하는 경우 Red Hat 이 제한 없이 SCP에 나열된 정책 작업을 수행할 수 있도록 조직의 서비스 제어 정책(SCP)을 구성해야 합니다. 자세한 내용은 the section called “AWS Organizations 서비스 제어 정책에서 필요한 AWS Marketplace 권한 거부” 단원을 참조하십시오. SCP에 대한 자세한 내용은 서비스 제어 정책(SCP)을 참조하세요.
- 기본적으로 비활성화 AWS 리전 된 활성화된 AWS STS 에 클러스터 를 ROSA 배포하는 경우 다음 명령을 사용하여의 모든 리전에 대해 보안 토큰을 버전 2 AWS 계정 로 업데이트해야 합니다.

```
aws iam set-security-token-service-preferences --global-endpoint-token-version
 v2Token
```

리전 활성화에 대한 자세한 내용은 link:accounts/latest/reference/manage를 참조하세요.

AWS 사전 조건 활성화 ROSA 및 구성

를 ROSA 생성하려면 ROSA 콘솔에서 ROSA AWS 서비스를 활성화 클러스터해야 합니다. ROSA 콘솔은 AWS 에 필요한 AWS Marketplace 권한, 서비스 할당량 및 라는 Elastic Load Balancing (ELB) 서비스 연결 역할 AWS 계정 이 있는지 확인합니다`AWSServiceRoleForElasticLoadBalancing`. 이러한 사전 요구 사항 중 하나라도 누락된 경우 콘솔에서는 사전 요구 사항을 충족하도록 계정을 구성하는 방법에 대한 지침을 제공합니다.

1. ROSA 콘솔로 이동합니다.
2. Get started를 선택합니다.
3. ROSA 사전 조건 확인 페이지에서 연락처 정보를 Red Hat과 공유하는 데 동의합니다를 선택합니다.
4. ROSA 활성화를 선택합니다.
5. 페이지에서 서비스 할당량이 ROSA 사전 조건을 충족하는지 확인하고 ELB 서비스 연결 역할이 생성되면 ROSA CLI를 클러스터 사용하여 새 터미널 세션을 열어 첫 ROSA 번째를 생성합니다.

ROSA CLI를 사용하여 ROSA with HCP 클러스터 생성

다음 섹션에서는 AWS STS 및 ROSA CLI를 사용하여 호스팅된 컨트롤 플레인(ROSA with HCP)으로 ROSA를 시작하는 방법을 설명합니다. Terraform을 사용하여 ROSA with HCP 클러스터를 생성하는

단계는 Red Hat 설명서를 참조하세요. ROSA 클러스터 생성을 위한 Terraform 공급자에 대한 자세한 내용은 Terraform 설명서를 참조하세요.

ROSA CLI는 `auto` 모드 또는 `manual` 모드를 사용하여를 생성하는 데 필요한 IAM 리소스 및 OpenID Connect(OIDC) 구성을 생성합니다 ROSA 클러스터. `auto` 모드는 필요한 IAM 역할 및 정책과 OIDC 공급자를 자동으로 생성합니다. `manual` 모드는 IAM 리소스를 수동으로 생성하는 데 필요한 AWS CLI 명령을 출력합니다. `manual` 모드를 사용하면 생성된 AWS CLI 명령을 수동으로 실행하기 전에 검토할 수 있습니다. `manual` 모드를 사용하면 조직의 다른 관리자나 그룹에 명령을 전달하여 해당 관리자나 그룹이 리소스를 생성하도록 할 수도 있습니다.

이 문서의 절차는 ROSA CLI `auto` 모드를 사용하여 ROSA with HCP에 필요한 IAM 리소스 및 OIDC 구성을 생성합니다. 시작하는 방법에 대한 자세한 내용은 단원을 참조하십시오시작하기 ROSA .

주제

사전 조건

에 나열된 사전 조건 작업을 완료합니다the section called “설정”.

Amazon VPC 아키텍처 생성

다음 절차에서는 클러스터를 호스팅하는 데 사용할 수 있는 Amazon VPC 아키텍처를 생성합니다. 모든 클러스터 리소스는 프라이빗 서브넷에서 호스팅됩니다. 퍼블릭 서브넷은 NAT 게이트웨이를 통해 프라이빗 서브넷에서 퍼블릭 인터넷으로 아웃바운드 트래픽을 라우팅합니다. 이 예에서는 CIDR 블록 `10.0.0.0/16`를 Amazon VPC에 사용합니다. 하지만 다른 CIDR 블록을 선택할 수도 있습니다. 자세한 내용은 VPC 크기 조정을 참조하세요.

> **Important**
>
> Amazon VPC 요구 사항이 충족되지 않으면 클러스터 생성이 실패합니다.

Example

Terraform

1. Terraform CLI를 설치합니다. 자세한 내용은 Terraform 설명서의 설치 지침을 참조하세요.
2. 터미널 세션을 열고 Terraform VPC 리포지토리를 복제합니다.

   ```
   git clone https://github.com/openshift-cs/terraform-vpc-example
   ```

3. 생성된 디렉터리로 이동합니다.

   ```
   cd terraform-vpc-example
   ```

4. Terraform 파일을 시작합니다.

   ```
   terraform init
   ```

   완료되면 CLI는 Terraform이 성공적으로 초기화되었다는 메시지를 반환합니다.

5. 기존 템플릿을 기반으로 Terraform 계획을 빌드하려면 다음 명령을 실행합니다. 를 지정해야 AWS 리전 합니다. 선택적으로 클러스터 이름을 지정하도록 선택할 수 있습니다.

   ```
   terraform plan -out rosa.tfplan -var region=<region>
   ```

   명령이 실행되면 `hypershift-tf` 디렉터리에 `rosa.tfplan` 파일이 추가됩니다. 자세한 옵션은 Terraform VPC 리포지토리의 README 파일을 참조하세요.

6. 계획 파일을 적용하여 VPC를 빌드합니다.

```
terraform apply rosa.tfplan
```

완료되면 CLI는 추가된 리소스를 확인하는 성공 메시지를 반환했습니다.

a. (선택 사항) ROSA with HCP 클러스터를 생성할 때 사용할 Terraform 프로비저닝된 프라이빗, 퍼블릭 및 머신풀 서브넷 IDs에 대한 환경 변수를 생성합니다.

```
export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
```

b. (선택 사항) 환경 변수가 올바르게 설정되었는지 확인합니다.

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Amazon VPC 콘솔을 엽니다.
2. VPC 대시보드에서 VPC 생성을 선택합니다.
3. 생성할 리소스에서 VPC 등을 선택합니다.
4. 이름 태그 자동 생성을 선택한 상태로 유지하여 VPC 리소스에 이름 태그를 생성하거나 선택을 취소하여 VPC 리소스에 고유한 이름 태그를 제공합니다.
5. IPv4 CIDR 블록에 VPC의 IPv4 주소 범위를 입력합니다. VPC는 IPv4 주소 범위를 가져야 합니다.
6. (선택 사항) IPv6 트래픽을 지원하려면 IPv6 CIDR 블록, Amazon 제공 IPv6 CIDR 블록을 선택합니다.
7. 테넌시를 로 둡니다`Default`.
8. 가용 영역(AZs) 수에서 필요한 번호를 선택합니다. 다중 AZ 배포의 경우 에는 세 개의 가용 영역이 ROSA 필요합니다. 서브넷의 AZ를 선택하려면 AZ 사용자 지정을 확장합니다.

> **Note**
>
> 일부 ROSA 인스턴스 유형은 일부 가용 영역에서만 사용할 수 있습니다. ROSA CLI 명령 `rosa list instance-types` 명령을 사용하여 사용 가능한 모든 ROSA 인스턴스 유형을 나열할 수 있습니다. 지정된 가용 영역에 인스턴스 유형을 사용할 수 있는지 확인하려면 AWS CLI 명령을 사용합니다`aws ec2 describe-instance-`

```
type-offerings --location-type availability-zone --filters
Name=location,Values=<availability_zone> --region <region> --
output text | egrep "<instance_type>".
```

9. 서브넷을 구성하려면 퍼블릭 서브넷 수 및 프라이빗 서브넷 수의 값을 선택합니다. 서브넷의 IP 주소 범위를 선택하려면 서브넷 CIDR 블록 사용자 지정을 확장합니다.

> **Note**
>
> ROSA with HCP를 사용하려는 고객은 클러스터를 만드는 데 사용되는 가용 영역당 하나 이상의 퍼블릭 및 프라이빗 서브넷을 구성해야 합니다.

10. 프라이빗 서브넷의 리소스에 IPv4를 통해 퍼블릭 인터넷에 대한 액세스 권한을 부여하려면 NAT 게이트웨이의 경우 NAT 게이트웨이를 생성할 AZs 수를 선택합니다. 프로덕션 환경에서는 퍼블릭 인터넷에 액세스해야 하는 리소스가 있는 각 AZ에 NAT 게이트웨이를 배포하는 것이 좋습니다.
11. (선택 사항) VPC에서 Amazon S3 직접에 액세스해야 하는 경우 VPC 엔드포인트인 S3 게이트웨이를 선택합니다.
12. 기본 DNS 옵션을 선택한 상태로 둡니다. VPC에서 DNS 호스트 이름 지원이 ROSA 필요합니다.
13. 추가 태그를 확장하고 새 태그 추가를 선택한 다음 다음 태그 키를 추가합니다.는 이러한 태그가 사용되는지 확인하는 자동화된 사전 검사를 ROSA 사용합니다.
    - 키: `kubernetes.io/role/elb`
    - 키: `kubernetes.io/role/internal-elb`
14. VPC 생성을 선택합니다.

AWS CLI

1. CIDR 블록이 `10.0.0.0/16`인 VPC를 만듭니다.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

앞의 명령은 VPC ID를 반환합니다. 다음은 예시 출력입니다.

```
vpc-1234567890abcdef0
```

2. 환경 변수에 VPC ID를 저장합니다.

```
export VPC_ID=vpc-1234567890abcdef0
```

3. VPC_ID 환경 변수를 사용하여 VPC에 대한 Name 태그를 생성합니다.

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. VPC에서 DNS 호스트 이름 지원을 활성화합니다.

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

5. 리소스를 생성해야 하는 가용 영역을 지정하여 VPC에서 퍼블릭 및 프라이빗 서브넷을 생성합니다.

> **Important**
>
> ROSA with HCP를 사용하려는 고객은 클러스터를 만드는 데 사용되는 가용 영역당 하나 이상의 퍼블릭 및 프라이빗 서브넷을 구성해야 합니다. 다중 AZ 배포의 경우 3개의 가용 영역이 필요합니다. 이러한 요구 사항이 충족되지 않으면 클러스터 생성에 실패합니다.

> **Note**
>
> 일부 ROSA 인스턴스 유형은 일부 가용 영역에서만 사용할 수 있습니다. ROSA CLI 명령 `rosa list instance-types` 명령을 사용하여 사용 가능한 모든 ROSA 인스턴스 유형을 나열할 수 있습니다. 지정된 가용 영역에 인스턴스 유형을 사용할 수 있는지 확인하려면 AWS CLI 명령을 사용합니다`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

```
aws ec2 create-subnet \
```

```
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. 퍼블릭 및 프라이빗 서브넷 IDs 환경 변수에 저장합니다.

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. VPC subnets. ROSA uses에 대해 다음 태그를 생성하여 이러한 태그가 사용되는지 확인합니다.

> **Note**
>
> 하나 이상의 프라이빗 서브넷과 해당하는 경우 하나의 퍼블릭 서브넷에 태그를 지정해야 합니다.

```
aws ec2 create-tags --resources $PUBLIC_SUB --tags Key=kubernetes.io/role/
elb,Value=1
aws ec2 create-tags --resources $PRIVATE_SUB --tags Key=kubernetes.io/role/
internal-elb,Value=1
```

8. 아웃바운드 트래픽에 대한 인터넷 게이트웨이와 라우팅 테이블을 생성합니다. 프라이빗 트래픽에 대한 라우팅 테이블과 탄력적 IP 주소를 생성합니다.

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
```

```
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

9. 환경 변수에 IDs 저장합니다.

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

10. 인터넷 게이트웨이를 VPC에 연결합니다.

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

11. 퍼블릭 라우팅 테이블을 퍼블릭 서브넷에 연결하고 인터넷 게이트웨이로 라우팅하도록 트래픽을 구성합니다.

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

12. NAT 게이트웨이를 생성하고 탄력적 IP 주소와 연결하여 프라이빗 서브넷으로 트래픽을 활성화합니다.

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

13. 프라이빗 라우팅 테이블을 프라이빗 서브넷에 연결하고 NAT 게이트웨이로 라우팅하도록 트래픽을 구성합니다.

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

14. (선택 사항) 다중 AZ 배포의 경우 위의 단계를 반복하여 퍼블릭 및 프라이빗 서브넷으로 두 개의 추가 가용 영역을 구성합니다.

필요한 IAM 역할 및 OpenID Connect 구성 생성

ROSA with HCP 클러스터를 생성하기 전에 필요한 IAM 역할 및 정책과 OpenID Connect(OIDC) 구성을 생성해야 합니다. ROSA with HCP의 IAM 역할 및 정책에 대한 자세한 내용은 섹션을 참조하세요the section called “ AWS 관리형 정책”.

이 절차에서는 ROSA CLI `auto` 모드를 사용하여 ROSA with HCP 클러스터를 생성하는 데 필요한 OIDC 구성을 자동으로 생성합니다.

1. 필요한 IAM 계정 역할 및 정책을 생성합니다. `--force-policy-creation` 파라미터는 존재하는 모든 기존 역할 및 정책을 업데이트합니다. 역할 및 정책이 없는 경우 명령은 이러한 리소스를 대신 생성합니다.

```
rosa create account-roles --force-policy-creation
```

> **Note**
>
> 오프라인 액세스 토큰이 만료된 경우 ROSA CLI는 권한 부여 토큰을 업데이트해야 한다는 오류 메시지를 출력합니다. 문제 해결 단계는 섹션을 참조하세요the section called “ROSA CLI 만료된 오프라인 액세스 토큰 문제 해결”.

2. 클러스터에 대한 사용자 인증을 가능하게 하는 OpenID Connect(OIDC) 구성을 생성합니다. 이 구성은 OpenShift 클러스터 관리자(OCM)와 함께 사용하도록 등록되었습니다.

```
rosa create oidc-config --mode=auto
```

3. ROSA CLI 출력에 제공된 OIDC 구성 ID를 복사합니다. ROSA with HCP 클러스터를 생성하려면 나중에 OIDC 구성 ID를 제공해야 합니다.
4. 사용자 조직과 연결된 클러스터에 사용할 수 있는 OIDC 구성을 확인하려면 다음 명령을 실행합니다.

```
rosa list oidc-config
```

5. 를 이전에 복사한 OIDC 구성 ID<OIDC_CONFIG_ID>로 바꾸어 필요한 IAM 운영자 역할을 생성합니다.

   Example

> **Important**
>
> 운영자 역할을 생성할 때 <PREFIX_NAME>에 접두사를 입력해야 합니다. 이렇게 하지 않으면 오류가 발생합니다.

```
rosa create operator-roles --prefix <PREFIX_NAME> --oidc-config-id <OIDC_CONFIG_ID>
 --hosted-cp
```

6. IAM 연산자 역할이 생성되었는지 확인하려면 다음 명령을 실행합니다.

```
rosa list operator-roles
```

ROSA CLI 및를 사용하여 ROSA with HCP 클러스터 생성 AWS STS

AWS Security Token Service (AWS STS) 및 ROSA CLI에 제공된 auto 모드를 클러스터 사용하여 HCP가 포함된 ROSA를 생성할 수 있습니다. 퍼블릭 API와 Ingress 또는 프라이빗 API와 Ingress를 사용하여 클러스터를 생성할 수 있습니다.

단일 가용 영역(단일 AZ) 또는 다중 가용 영역(다중 AZ) 클러스터 을 사용하여를 생성할 수 있습니다. 어느 경우든 시스템의 CIDR 값이 VPC의 CIDR 값과 일치해야 합니다.

다음 절차에서는 rosa create cluster --hosted-cp 명령을 사용하여 HCP로 단일 AZ ROSA를 생성합니다 클러스터. 다중 AZ를 생성하려면 명령multi-az에서를 클러스터지정하고 배포하려는 각 프라이빗 서브넷IDs를 지정합니다.

1. 다음 명령을 사용하여 ROSA with HCP 클러스터를 생성합니다.
   - 퍼블릭 API 및 Ingress를 사용하여 ROSA with HCP 클러스터를 생성하며, 클러스터 이름, 운영자 역할 접두사, OIDC 구성 ID, 퍼블릭 및 프라이빗 서브넷 ID를 지정합니다.

     ```
     rosa create cluster --cluster-name=<CLUSTER_NAME> --sts --mode=auto --hosted-cp --
     operator-roles-prefix <OPERATOR_ROLE_PREFIX> --oidc-config-id <OIDC_CONFIG_ID> --
     subnet-ids=<PUBLIC_SUBNET_ID>,<PRIVATE_SUBNET_ID>
     ```

   - 프라이빗 API 및 Ingress를 사용하여 ROSA with HCP 클러스터를 생성하며, 클러스터 이름, 운영자 역할 접두사, OIDC 구성 ID, 프라이빗 서브넷 ID를 지정합니다.

     ```
     rosa create cluster --private --cluster-name=<CLUSTER_NAME> --sts --mode=auto --
     hosted-cp --subnet-ids=<PRIVATE_SUBNET_ID>
     ```

2. 의 상태를 확인합니다 클러스터.

   ```
   rosa describe cluster -c <CLUSTER_NAME>
   ```

   > **Note**
   >
   > 생성 프로세스가 실패하거나 10분 후에도 `State` 필드가 준비 상태로 변경되지 않는 경우 섹션을 참조하세요문제 해결.
   > 지원 또는 Red Hat 지원팀에 문의하여 지원을 받으려면 섹션을 참조하세요the section called “지원 받기”.

3. OpenShift 설치 관리자 로그를 확인하여 클러스터 생성 진행 상황을 추적합니다.

   ```
   rosa logs install -c <CLUSTER_NAME> --watch
   ```

자격 증명 공급자 구성 및 클러스터 액세스 권한 부여

ROSA 에는 기본 제공 OAuth 서버가 포함되어 있습니다. 클러스터 를 생성한 후에는 자격 증명 공급자를 사용하도록 OAuth를 구성해야 합니다. 그런 다음 구성된 ID 공급자에 사용자를 추가하여 클러스터액세스 권한을 부여할 수 있습니다. 필요에 따라 이러한 사용자에게 `cluster-admin` 또는 `dedicated-admin` 권한을 부여할 수 있습니다.

ROSA 클러스터에 맞게 다양한 ID 제공자 유형을 구성할 수 있습니다 . 지원되는 유형으로는 GitHub, GitHub Enterprise, GitLab, Google, LDAP, OpenID Connect, HTPasswd ID 공급자 등이 있습니다.

> **Important**
>
> HTPasswd ID 공급자는 한 명의 정적 관리자 사용자를 생성할 수 있도록 하기 위한 용도로만 포함됩니다. HTPassWD는 ROSA범용 ID 공급자로는 지원되지 않습니다.

다음 절차는 GitHub ID 공급자를 예로 구성합니다. 지원되는 각 ID 제공자 유형을 구성하는 방법에 대한 지침은 AWS STS ID 제공자 구성을 참조하세요.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. 의 자격 증명 프로비저닝에 사용할 GitHub 조직이 없는 경우 클러스터생성합니다. 자세한 내용을 알아보려면 GitHub의 설명서의 단계를 참조하세요.
3. ROSA CLI의 대화형 모드를 사용하여 클러스터의 자격 증명 공급자를 구성합니다.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 출력의 구성 프롬프트에 따라 GitHub 조직의 멤버에 대한 클러스터 액세스를 제한합니다.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 출력에서 URL을 열고 <GITHUB_ORG_NAME>를 GitHub 조직의 이름으로 대체합니다.
6. GitHub 웹 페이지에서 애플리케이션 등록을 선택하여 GitHub 조직에 새 OAuth 애플리케이션을 등록합니다.

7. GitHub OAuth 페이지의 정보를 사용해 다음 명령어를 실행하여 나머지 `rosa create idp` 대화형 프롬프트를 채웁니다. <GITHUB_CLIENT_ID> 및 <GITHUB_CLIENT_SECRET>를 GitHub OAuth 애플리케이션의 보안 인증 정보로 교체합니다.

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> ID 공급자 구성이 활성화되는 데 약 2분 정도 걸릴 수 있습니다. `cluster-admin` 사용자를 구성한 경우 `oc get pods -n openshift-authentication --watch`를 실행하여 업데이트된 구성으로 OAuth 포드가 재배포되는 것을 관찰할 수 있습니다.

8. ID 공급자가 올바르게 구성되었는지 확인합니다.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

사용자에게에 대한 액세스 권한 부여 클러스터

구성된 자격 증명 공급자에 추가하여 사용자에게에 대한 액세스 권한을 부여할 수 클러스터 있습니다.

다음 절차는 클러스터에 ID를 프로비저닝하도록 구성된 GitHub 조직에 사용자를 추가합니다.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. GitHub 조직에 클러스터 액세스해야 하는 사용자를 초대합니다. 자세한 내용은 GitHub 설명서에서 조직에 가입하도록 사용자 초대하기를 참조하세요.

cluster-admin 권한 구성

1. 다음 명령을 실행하여 cluster-admin 권한을 부여합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>을 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 cluster-admins 그룹 구성원으로 등록되어 있는지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

dedicated-admin 권한 구성

1. 다음 명령을 사용하여 dedicated-admin 권한을 부여합니다. 다음 명령을 실행하여 <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 cluster-admins 그룹 구성원으로 등록되어 있는지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 액세스

Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 로그인합니다.

1. 다음 명령을 클러스터 사용하여의 콘솔 URL을 가져옵니다. 를의 이름으로 <CLUSTER_NAME> 바꿉니다 클러스터.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 출력에서 콘솔 URL로 이동하여 로그인합니다.

   다음으로 로그인... 대화 상자에서 ID 공급자 이름을 선택하고, 공급자가 제시한 권한 부여 요청을 모두 완료합니다.

개발자 카탈로그에서 애플리케이션 배포

Red Hat 하이브리드 클라우드 콘솔에서 개발자 카탈로그 테스트 애플리케이션을 배포하고 경로를 통해 공개할 수 있습니다.

1. Red Hat 하이브리드 클라우드 콘솔로 이동하여 앱을 배포할 클러스터를 선택합니다.
2. 클러스터 페이지에서 콘솔 열기를 선택합니다.
3. 관리자 시점에서 홈 > 프로젝트 > 프로젝트 생성을 선택합니다.
4. 프로젝트 이름을 입력하고 선택적으로 표시 이름 및 설명을 추가합니다.
5. 프로젝트를 생성하려면 생성을 선택합니다.
6. 개발자 시점으로 전환하고 +추가를 선택합니다. 선택한 프로젝트가 방금 만든 프로젝트인지 확인합니다.
7. 개발자 카탈로그 대화 상자에서 모든 서비스를 선택합니다.
8. 개발자 카탈로그 페이지의 메뉴에서 언어 > JavaScript를 선택합니다.
9. Node.js를 선택한 다음 애플리케이션 생성을 선택하여 Source-to-Image 애플리케이션 생성 페이지를 엽니다.

> **Note**
>
> Node.js 옵션을 표시하려면 모든 필터 지우기를 선택해야 할 수도 있습니다.

10. Git 섹션에서 샘플 사용해보기를 선택합니다.
11. 이름 필드에 고유한 이름을 추가합니다.
12. 생성(Create)을 선택합니다.

> **Note**
>
> 새 애플리케이션을 배포하는 데 몇 분 정도 걸립니다.

13. 배포가 완료되면 애플리케이션 경로 URL을 선택합니다.

    브라우저의 새 탭이 열리고 다음과 비슷한 메시지가 표시됩니다.

```
Welcome to your Node.js application on OpenShift
```

14. (선택 사항) 애플리케이션을 삭제하고 리소스를 정리합니다.

a. 관리자 시점에서 홈 > 프로젝트를 선택합니다.

b. 프로젝트의 작업 메뉴를 열고 프로젝트 삭제를 선택합니다.

사용자의 **cluster-admin** 권한 취소

1. 다음 명령을 사용하여 cluster-admin 권한을 취소합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 cluster-admins 그룹 구성원으로 등록되어 있지 않은지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

사용자의 **dedicated-admin** 권한 취소

1. 다음 명령을 사용하여 dedicated-admin 권한을 취소합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 dedicated-admins 그룹 구성원으로 등록되어 있지 않은지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

에 대한 사용자 액세스 취소 클러스터

구성된 자격 증명 공급자에서 자격 증명 공급자 사용자를 제거하여 자격 증명 공급자 사용자의 클러스터 액세스를 취소할 수 있습니다.

클러스터에 다양한 ID 공급자 유형을 구성할 수 있습니다. 다음 절차는 GitHub 조직의 멤버에 대한 클러스터 액세스를 취소합니다.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. GitHub 조직에서 사용자를 제거합니다. 자세한 내용은 GitHub 설명서에서 조직에서 사용자 제거하기를 참조하세요.

클러스터 및 AWS STS 리소스 삭제

ROSA CLI를 사용하여 AWS Security Token Service ()를 사용하는 클러스터 를 삭제할 수 있습니다 AWS STS. ROSA CLI를 사용하여에서 생성한 IAM 역할 및 OIDC 공급자를 삭제할 수도 있습니다 ROSA. 에서 생성한 IAM 정책을 삭제하려면 IAM 콘솔을 사용할 ROSA수 있습니다.

> **Note**
>
> IAM 에서 생성한 역할 및 정책은 동일한 계정의 다른 ROSA 클러스터에서 사용할 ROSA 수 있습니다.

1. 를 삭제 클러스터 하고 로그를 확인합니다. <CLUSTER_NAME>을 클러스터이름 또는 ID로 바꿉니다.

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> IAM 역할, 정책 및 OIDC 공급자 클러스터 를 제거하기 전에가 완전히 삭제될 때까지 기다려야 합니다. 설치 관리자가 생성한 리소스를 삭제하려면 계정 IAM 역할이 필요합니다. OpenShift 운영자가 생성한 리소스를 정리하려면 운영자 IAM 역할이 필요합니다. 운영자는 인증 시 OIDC 공급자를 사용합니다.

2. 다음 명령을 실행하여 클러스터 운영자가 인증에 사용하는 OIDC 공급자를 삭제합니다.

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 클러스터별 연산자 IAM 역할을 삭제합니다.

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 다음 명령을 사용하여 계정 IAM 역할을 삭제합니다. <PREFIX>를 삭제할 계정 IAM 역할의 접두사로 바꿉니다. 계정 IAM 역할을 생성할 때 사용자 지정 접두사를 지정한 경우 기본 ManagedOpenShift 접두사를 지정합니다.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 에서 생성한 IAM 정책을 삭제합니다 ROSA.

   a. IAM 콘솔에 로그인합니다.

b. 왼쪽 메뉴의 액세스 관리에서 정책을 선택합니다.

c. 삭제하려는 정책을 선택하고 작업 > 삭제를 선택합니다.

d. 정책 이름을 입력하고 삭제를 선택합니다.

e. 이 단계를 반복하여 클러스터에 대한 IAM 정책을 각각 삭제합니다.

ROSA CLI를 사용하여 ROSA 클래식 클러스터 생성

다음 섹션에서는 AWS STS 및 ROSA CLI를 사용하여 ROSA 클래식을 시작하는 방법을 설명합니다. Terraform을 사용하여 ROSA 클래식 클러스터를 생성하는 단계는 Red Hat 설명서를 참조하세요. ROSA 클러스터 생성을 위한 Terraform 공급자에 대한 자세한 내용은 Terraform 설명서를 참조하세요.

ROSA CLI는 `auto` 모드 또는 `manual` 모드를 사용하여를 프로비저닝 ROSA 하는 데 필요한 IAM 리소스를 생성합니다 클러스터. `auto` 모드는 필요한 IAM 역할 및 정책과 OpenID Connect(OIDC) 공급자를 즉시 생성합니다. `manual` 모드는 IAM 리소스를 생성하는 데 필요한 AWS CLI 명령을 출력합니다. `manual` 모드를 사용하면 생성된 AWS CLI 명령을 수동으로 실행하기 전에 검토할 수 있습니다. `manual` 모드를 사용하면 조직의 다른 관리자나 그룹에 명령을 전달하여 해당 관리자나 그룹이 리소스를 생성하도록 할 수도 있습니다.

시작하는 방법에 대한 자세한 내용은 단원을 참조하십시오시작하기 ROSA .

주제

- 사전 조건
- ROSA CLI 및를 사용하여 ROSA 클래식 클러스터 생성 AWS STS
- 자격 증명 공급자 구성 및 클러스터 액세스 권한 부여
- 사용자에게에 대한 액세스 권한 부여 클러스터
- cluster-admin 권한 구성
- dedicated-admin 권한 구성
- Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 액세스
- 개발자 카탈로그에서 애플리케이션 배포
- 사용자의 cluster-admin 권한 취소
- 사용자의 dedicated-admin 권한 취소
- 에 대한 사용자 액세스 취소 클러스터
- 클러스터 및 AWS STS 리소스 삭제

사전 조건

에 나열된 사전 조건 작업을 완료합니다the section called “설정”.

ROSA CLI 및를 사용하여 ROSA 클래식 클러스터 생성 AWS STS

ROSA CLI 및를 클러스터 사용하여 ROSA 클래식을 생성할 수 있습니다 AWS STS.

1. `--mode auto` 또는를 사용하여 필요한 IAM 계정 역할 및 정책을 생성합니다`--mode manual`.

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

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

     > **Note**
     >
     > 오프라인 액세스 토큰이 만료된 경우 ROSA CLI는 권한 부여 토큰을 업데이트해야 한다는 오류 메시지를 출력합니다. 문제 해결 단계는 섹션을 참조하세요the section called “ROSA CLI 만료된 오프라인 액세스 토큰 문제 해결”.

2. `--mode auto` 또는를 클러스터 사용하여를 생성합니다`--mode manual`. `auto` 모드를 사용하면 클러스터를 더 빠르게 생성할 수 있습니다. `manual` 모드는 클러스터에 대한 사용자 지정 설정을 지정하라는 메시지를 표시합니다.

   - ```
     rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode auto
     ```

     > **Note**
     >
     > `--mode auto`를 지정하면 `rosa create cluster` 명령이 클러스터별 연산자 IAM 역할과 OIDC 공급자를 자동으로 생성합니다. 운영자는 인증 시 OIDC 공급자를 사용합니다.

     > **Note**
     >
     > `--mode auto` 기본값을 사용하면 안정적인 최신 OpenShift 버전이 설치됩니다.
     ```

- ```
  rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode manual
  ```

  Important

  `manual` 모드에서 etcd 암호화를 활성화하면 약 20%의 성능 오버헤드가 발생합니다. 오버헤드는 etcd 볼륨을 암호화하는 기본 Amazon EBS 암호화 외에도이 두 번째 암호화 계층을 도입한 결과입니다.

  Note

  `manual` 모드를 실행하여 클러스터를 생성한 후에는 클러스터별 운영자 IAM 역할과 클러스터 운영자가 인증에 사용하는 OpenID Connect 공급자를 수동으로 생성해야 합니다.

3. 의 상태를 확인합니다 클러스터.

```
rosa describe cluster -c <CLUSTER_NAME>
```

Note

프로비저닝 프로세스가 실패하거나 40분 후에도 `State` 필드가 준비 상태로 변경되지 않는 경우 섹션을 참조하세요문제 해결. 지원 또는 Red Hat 지원팀에 문의하여 지원을 받으려면 섹션을 참조하세요the section called “지원 받기”.

4. OpenShift 설치 관리자 로그를 확인하여 클러스터 생성 진행 상황을 추적합니다.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

자격 증명 공급자 구성 및 클러스터 액세스 권한 부여

ROSA 에는 기본 제공 OAuth 서버가 포함되어 있습니다. 클러스터 를 생성한 후에는 자격 증명 공급자를 사용하도록 OAuth를 구성해야 합니다. 그런 다음 구성된 ID 공급자에 사용자를 추가하여 클러스터액세스 권한을 부여할 수 있습니다. 필요에 따라 이러한 사용자에게 `cluster-admin` 또는 `dedicated-admin` 권한을 부여할 수 있습니다.
```

ROSA 클러스터에 맞게 다양한 ID 제공자 유형을 구성할 수 있습니다 . 지원되는 유형으로는 GitHub, GitHub Enterprise, GitLab, Google, LDAP, OpenID Connect, HTPasswd ID 공급자 등이 있습니다.

> **Important**
>
> HTPasswd ID 공급자는 한 명의 정적 관리자 사용자를 생성할 수 있도록 하기 위한 용도로만 포함됩니다. HTPassWD는 ROSA범용 ID 공급자로는 지원되지 않습니다.

다음 절차는 GitHub ID 공급자를 예로 구성합니다. 지원되는 각 ID 제공자 유형을 구성하는 방법에 대한 지침은 AWS STS ID 제공자 구성을 참조하세요.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. 의 자격 증명 프로비저닝에 사용할 GitHub 조직이 없는 경우 조직을 클러스터생성합니다. 자세한 내용을 알아보려면 GitHub의 설명서의 단계를 참조하세요.
3. ROSA CLI의 대화형 모드를 사용하여 클러스터의 자격 증명 공급자를 구성합니다.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 출력의 구성 프롬프트에 따라 GitHub 조직의 멤버에 대한 클러스터 액세스를 제한합니다.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 출력에서 URL을 열고 <GITHUB_ORG_NAME>를 GitHub 조직의 이름으로 대체합니다.

6. GitHub 웹 페이지에서 애플리케이션 등록을 선택하여 GitHub 조직에 새 OAuth 애플리케이션을 등록합니다.
7. GitHub OAuth 페이지의 정보를 사용해 다음 명령어를 실행하여 나머지 `rosa create idp` 대화형 프롬프트를 채웁니다. `<GITHUB_CLIENT_ID>` 및 `<GITHUB_CLIENT_SECRET>`를 GitHub OAuth 애플리케이션의 보안 인증 정보로 교체합니다.

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> ID 공급자 구성이 활성화되는 데 약 2분 정도 걸릴 수 있습니다. `cluster-admin` 사용자를 구성한 경우 `oc get pods -n openshift-authentication --watch`를 실행하여 업데이트된 구성으로 OAuth 포드가 재배포되는 것을 관찰할 수 있습니다.

8. ID 공급자가 올바르게 구성되었는지 확인합니다.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

사용자에게에 대한 액세스 권한 부여 클러스터

구성된 자격 증명 공급자에 추가하여 사용자에게에 대한 액세스 권한을 부여할 수 클러스터 있습니다.

다음 절차는 클러스터에 ID를 프로비저닝하도록 구성된 GitHub 조직에 사용자를 추가합니다.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. GitHub 조직에 클러스터 액세스해야 하는 사용자를 초대합니다. 자세한 내용은 GitHub 설명서에서 조직에 가입하도록 사용자 초대하기를 참조하세요.

cluster-admin 권한 구성

1. 다음 명령을 실행하여 cluster-admin 권한을 부여합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>을 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 cluster-admins 그룹 구성원으로 등록되어 있는지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

dedicated-admin 권한 구성

1. 다음 명령을 사용하여 dedicated-admin 권한을 부여합니다. 다음 명령을 실행하여 <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 cluster-admins 그룹 구성원으로 등록되어 있는지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 액세스

클러스터 관리자 사용자를 생성하거나 구성된 자격 증명 공급자에 사용자를 추가한 후 Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 로그인할 수 있습니다.

1. 다음 명령을 클러스터 사용하여의 콘솔 URL을 가져옵니다. 를의 이름으로 <CLUSTER_NAME> 바꿉니다 클러스터.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 출력에서 콘솔 URL로 이동하여 로그인합니다.
   - cluster-admin 사용자를 생성한 경우 제공된 보안 인증 정보를 사용하여 로그인합니다.
   - 에 대한 자격 증명 공급자를 구성한 경우 로그인... 대화 상자에서 자격 클러스터증명 공급자 이름을 선택하고 공급자가 제시한 권한 부여 요청을 완료합니다.

개발자 카탈로그에서 애플리케이션 배포

Red Hat 하이브리드 클라우드 콘솔에서 개발자 카탈로그 테스트 애플리케이션을 배포하고 경로를 통해 공개할 수 있습니다.

1. Red Hat 하이브리드 클라우드 콘솔로 이동하여 앱을 배포할 클러스터를 선택합니다.
2. 클러스터 페이지에서 콘솔 열기를 선택합니다.
3. 관리자 시점에서 홈 > 프로젝트 > 프로젝트 생성을 선택합니다.
4. 프로젝트 이름을 입력하고 선택적으로 표시 이름 및 설명을 추가합니다.
5. 프로젝트를 생성하려면 생성을 선택합니다.
6. 개발자 시점으로 전환하고 +추가를 선택합니다. 선택한 프로젝트가 방금 만든 프로젝트인지 확인합니다.
7. 개발자 카탈로그 대화 상자에서 모든 서비스를 선택합니다.
8. 개발자 카탈로그 페이지의 메뉴에서 언어 > JavaScript를 선택합니다.
9. Node.js를 선택한 다음 애플리케이션 생성을 선택하여 Source-to-Image 애플리케이션 생성 페이지를 엽니다.

> **Note**
>
> Node.js 옵션을 표시하려면 모든 필터 지우기를 선택해야 할 수도 있습니다.

10. Git 섹션에서 샘플 사용해보기를 선택합니다.
11. 이름 필드에 고유한 이름을 추가합니다.
12. 생성(Create)을 선택합니다.

> **Note**
>
> 새 애플리케이션을 배포하는 데 몇 분 정도 걸립니다.

13. 배포가 완료되면 애플리케이션 경로 URL을 선택합니다.

    브라우저의 새 탭이 열리고 다음과 비슷한 메시지가 표시됩니다.

```
Welcome to your Node.js application on OpenShift
```

14. (선택 사항) 애플리케이션을 삭제하고 리소스를 정리합니다.

a. 관리자 시점에서 홈 > 프로젝트를 선택합니다.

b. 프로젝트의 작업 메뉴를 열고 프로젝트 삭제를 선택합니다.

사용자의 **cluster-admin** 권한 취소

1. 다음 명령을 사용하여 cluster-admin 권한을 취소합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 cluster-admins 그룹 구성원으로 등록되어 있지 않은지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

사용자의 **dedicated-admin** 권한 취소

1. 다음 명령을 사용하여 dedicated-admin 권한을 취소합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 dedicated-admins 그룹 구성원으로 등록되어 있지 않은지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

에 대한 사용자 액세스 취소 클러스터

구성된 자격 증명 공급자에서 자격 증명 공급자를 제거하여 자격 증명 공급자 사용자의 클러스터 액세스를 취소할 수 있습니다.

클러스터에 다양한 ID 공급자 유형을 구성할 수 있습니다. 다음 절차는 GitHub 조직의 멤버에 대한 클러스터 액세스를 취소합니다.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. GitHub 조직에서 사용자를 제거합니다. 자세한 내용은 GitHub 설명서에서 조직에서 사용자 제거하기를 참조하세요.

클러스터 및 AWS STS 리소스 삭제

ROSA CLI를 사용하여 AWS Security Token Service ()를 사용하는 클러스터 를 삭제할 수 있습니다 AWS STS. ROSA CLI를 사용하여에서 생성한 IAM 역할 및 OIDC 공급자를 삭제할 수도 있습니다 ROSA. 에서 생성한 IAM 정책을 삭제하려면 IAM 콘솔을 사용할 ROSA수 있습니다.

> **Important**
>
> IAM 에서 생성한 역할 및 정책은 동일한 계정의 다른 ROSA 클러스터에서 사용할 ROSA 수 있습니다.

1. 를 삭제 클러스터 하고 로그를 확인합니다. <CLUSTER_NAME>을 클러스터이름 또는 ID로 바꿉니다.

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> IAM 역할, 정책 및 OIDC 공급자 클러스터 를 제거하기 전에가 완전히 삭제될 때까지 기다려야 합니다. 설치 관리자가 생성한 리소스를 삭제하려면 계정 IAM 역할이 필요합니다. OpenShift 운영자가 생성한 리소스를 정리하려면 운영자 IAM 역할이 필요합니다. 운영자는 인증 시 OIDC 공급자를 사용합니다.

2. 다음 명령을 실행하여 클러스터 운영자가 인증에 사용하는 OIDC 공급자를 삭제합니다.

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 클러스터별 연산자 IAM 역할을 삭제합니다.

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 다음 명령을 사용하여 계정 IAM 역할을 삭제합니다. <PREFIX>를 삭제할 계정 IAM 역할의 접두사로 바꿉니다. 계정 IAM 역할을 생성할 때 사용자 지정 접두사를 지정한 경우 기본 `ManagedOpenShift` 접두사를 지정합니다.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 에서 생성한 IAM 정책을 삭제합니다 ROSA.

a. IAM 콘솔에 로그인합니다.

b. 왼쪽 메뉴의 액세스 관리에서 정책을 선택합니다.

c. 삭제하려는 정책을 선택하고 작업 > 삭제를 선택합니다.

d. 정책 이름을 입력하고 삭제를 선택합니다.

e. 이 단계를 반복하여 클러스터에 대한 IAM 정책을 각각 삭제합니다.

를 사용하는 ROSA 클래식 클러스터 생성 AWS PrivateLink

ROSA 클래식 클러스터는 퍼블릭, 프라이빗 또는 프라이빗 등 몇 가지 방법으로 배포할 수 있습니다 AWS PrivateLink. ROSA 클래식에 대한 자세한 내용은 섹션을 참조하세요the section called “아키텍처”. 퍼블릭 및 프라이빗 클러스터 구성 모두에서 OpenShift 클러스터 는 인터넷에 액세스할 수 있으며 애플리케이션 계층의 애플리케이션 워크로드에 개인 정보가 설정됩니다.

클러스터 및 애플리케이션 워크로드를 모두 프라이빗으로 설정해야 하는 경우 ROSA 클래식 AWS PrivateLink 으로를 구성할 수 있습니다. AWS PrivateLink 는를 ROSA 사용하여 AWS 고객 계정의 ROSA 서비스와 클러스터 리소스 간에 프라이빗 연결을 생성하는 가용성과 확장성이 뛰어난 기술입니다. AWS PrivateLink Red Hat 사이트 신뢰성 엔지니어링(SRE) 팀은 클러스터의 AWS PrivateLink 엔드포인트에 연결된 프라이빗 서브넷을 사용하여 지원 및 문제 해결을 위해 클러스터에 액세스할 수 있습니다.

에 대한 자세한 내용은 란 무엇입니까 AWS PrivateLink?를 AWS PrivateLink참조하십시오.

주제

- 사전 조건
- Amazon VPC 아키텍처 생성
- ROSA CLI 및를 사용하여 ROSA 클래식 클러스터 생성 AWS PrivateLink
- AWS PrivateLink DNS 전달 구성
- 자격 증명 공급자 구성 및 클러스터 액세스 권한 부여
- 사용자에게에 대한 액세스 권한 부여 클러스터
- cluster-admin 권한 구성
- dedicated-admin 권한 구성
- Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 액세스
- 개발자 카탈로그에서 애플리케이션 배포

- 사용자의 cluster-admin 권한 취소
- 사용자의 dedicated-admin 권한 취소
- 에 대한 사용자 액세스 취소 클러스터
- 클러스터 및 AWS STS 리소스 삭제

사전 조건

에 나열된 사전 조건 작업을 완료합니다the section called “설정”.

Amazon VPC 아키텍처 생성

다음 절차에서는 클러스터를 호스팅하는 데 사용할 수 있는 Amazon VPC 아키텍처를 생성합니다. 모든 클러스터 리소스는 프라이빗 서브넷에서 호스팅됩니다. 퍼블릭 서브넷은 NAT 게이트웨이를 통해 프라이빗 서브넷에서 퍼블릭 인터넷으로 아웃바운드 트래픽을 라우팅합니다. 이 예에서는 CIDR 블록 `10.0.0.0/16`를 Amazon VPC에 사용합니다. 하지만 다른 CIDR 블록을 선택할 수도 있습니다. 자세한 내용은 VPC 크기 조정을 참조하세요.

> **Important**
>
> Amazon VPC 요구 사항이 충족되지 않으면 클러스터 생성이 실패합니다.

Example

Amazon VPC console

1. Amazon VPC 콘솔을 엽니다.
2. VPC 대시보드에서 VPC 생성을 선택합니다.
3. 생성할 리소스에서 VPC 등을 선택합니다.
4. 이름 태그 자동 생성을 선택한 상태로 유지하여 VPC 리소스에 이름 태그를 생성하거나 선택을 취소하여 VPC 리소스에 고유한 이름 태그를 제공합니다.
5. IPv4 CIDR 블록에 VPC의 IPv4 주소 범위를 입력합니다. VPC는 IPv4 주소 범위를 가져야 합니다.
6. (선택 사항) IPv6 트래픽을 지원하려면 IPv6 CIDR 블록, Amazon 제공 IPv6 CIDR 블록을 선택합니다.

7. 테넌시를 로 둡니다`Default`.
8. 가용 영역(AZs) 수에서 필요한 번호를 선택합니다. 다중 AZ 배포의 경우 에는 세 개의 가용 영역이 ROSA 필요합니다. 서브넷의 AZ를 선택하려면 AZ 사용자 지정을 확장합니다.

> **Note**
>
> 일부 ROSA 인스턴스 유형은 일부 가용 영역에서만 사용할 수 있습니다. ROSA CLI 명령 `rosa list instance-types` 명령을 사용하여 사용 가능한 모든 ROSA 인스턴스 유형을 나열할 수 있습니다. 지정된 가용 영역에 인스턴스 유형을 사용할 수 있는지 확인하려면 AWS CLI 명령을 사용합니다`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. 서브넷을 구성하려면 퍼블릭 서브넷 수 및 프라이빗 서브넷 수의 값을 선택합니다. 서브넷의 IP 주소 범위를 선택하려면 서브넷 CIDR 블록 사용자 지정을 확장합니다.

> **Note**
>
> ROSA 에서는 고객이 클러스터를 생성하는 데 사용되는 가용 영역당 하나 이상의 프라이빗 서브넷을 구성해야 합니다.

10. 프라이빗 서브넷의 리소스에 IPv4를 통해 퍼블릭 인터넷에 대한 액세스 권한을 부여하려면 NAT 게이트웨이의 경우 NAT 게이트웨이를 생성할 AZs 수를 선택합니다. 프로덕션 환경에서는 퍼블릭 인터넷에 액세스해야 하는 리소스가 있는 각 AZ에 NAT 게이트웨이를 배포하는 것이 좋습니다.
11. (선택 사항) VPC에서 Amazon S3 직접에 액세스해야 하는 경우 VPC 엔드포인트인 S3 Gateway를 선택합니다.
12. 기본 DNS 옵션을 선택한 상태로 둡니다. VPC에서 DNS 호스트 이름 지원이 ROSA 필요합니다.
13. VPC 생성을 선택합니다.

AWS CLI

1. CIDR 블록이 `10.0.0.0/16`인 VPC를 만듭니다.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
```

```
    --query Vpc.VpcId \
    --output text
```

앞의 명령은 VPC ID를 반환합니다. 다음은 예시 출력입니다.

```
vpc-1234567890abcdef0
```

2. 환경 변수에 VPC ID를 저장합니다.

```
export VPC_ID=vpc-1234567890abcdef0
```

3. VPC_ID 환경 변수를 사용하여 VPC에 대한 Name 태그를 생성합니다.

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. VPC에서 DNS 호스트 이름 지원을 활성화합니다.

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

5. 리소스를 생성해야 하는 가용 영역을 지정하여 VPC에 퍼블릭 및 프라이빗 서브넷을 생성합니다.

> **Important**
>
> ROSA 에서는 고객이 클러스터를 생성하는 데 사용되는 가용 영역당 하나 이상의 프라이빗 서브넷을 구성해야 합니다. 다중 AZ 배포의 경우 3개의 가용 영역이 필요합니다. 이러한 요구 사항이 충족되지 않으면 클러스터 생성에 실패합니다.

> **Note**
>
> 일부 ROSA 인스턴스 유형은 일부 가용 영역에서만 사용할 수 있습니다. ROSA CLI 명령 `rosa list instance-types` 명령을 사용하여 사용 가능한 모든 ROSA 인스턴스 유형을 나열할 수 있습니다. 지정된 가용 영역에 인스턴스 유형을 사용할 수 있는지 확인하려면 AWS CLI 명령을 사용합니다`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters`

```
    Name=location,Values=<availability_zone> --region <region> --
    output text | egrep "<instance_type>".
```

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. 퍼블릭 및 프라이빗 서브넷 IDs 환경 변수에 저장합니다.

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. 아웃바운드 트래픽에 대한 인터넷 게이트웨이와 라우팅 테이블을 생성합니다. 프라이빗 트래픽에 대한 라우팅 테이블과 탄력적 IP 주소를 생성합니다.

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

8. 환경 변수에 IDs 저장합니다.

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

9. 인터넷 게이트웨이를 VPC에 연결합니다.

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

10. 퍼블릭 라우팅 테이블을 퍼블릭 서브넷에 연결하고 인터넷 게이트웨이로 라우팅하도록 트래픽을 구성합니다.

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

11. NAT 게이트웨이를 생성하고 탄력적 IP 주소와 연결하여 프라이빗 서브넷으로의 트래픽을 활성화합니다.

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

12. 프라이빗 라우팅 테이블을 프라이빗 서브넷에 연결하고 NAT 게이트웨이로 라우팅하도록 트래픽을 구성합니다.

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

13(선택 사항) 다중 AZ 배포의 경우 위의 단계를 반복하여 퍼블릭 및 프라이빗 서브넷이 있는 두 개의 추가 가용 영역을 구성합니다.

ROSA CLI 및를 사용하여 ROSA 클래식 클러스터 생성 AWS PrivateLink

ROSA CLI 및를 사용하여 단일 가용 영역(단일 AWS PrivateLink AZ) 또는 다중 가용 영역(다중 AZ) 클러스터 으로를 생성할 수 있습니다. 어느 경우든 시스템의 CIDR 값이 VPC의 CIDR 값과 일치해야 합니다.

다음 절차에서는 `rosa create cluster` 명령을 사용하여 ROSA 클래식을 생성합니다 클러스터. 다중 AZ를 생성하려면 명령`--multi-az`에서를 클러스터지정한 다음 메시지가 표시되면 사용할 프라이빗 서브넷 IDs를 선택합니다.

> **Note**
>
> 방화벽을 사용하는 경우가 작동하는 데 필요한 사이트에 액세스할 ROSA 수 있도록 방화벽을 구성해야 합니다.
> 자세한 내용은 Red Hat 설명서의 Requirements for using AWS PrivateLink clusters를 참조하세요.

1. `--mode auto` 또는를 사용하여 필요한 IAM 계정 역할 및 정책을 생성합니다`--mode manual`.

   - ```
     rosa create account-roles --classic --mode auto
     ```
   - ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     >
     > 오프라인 액세스 토큰이 만료된 경우 ROSA CLI는 권한 부여 토큰을 업데이트해야 한다는 오류 메시지를 출력합니다. 문제 해결 단계는 섹션을 참조하세요the section called “ROSA CLI 만료된 오프라인 액세스 토큰 문제 해결”.

2. 다음 명령 중 하나를 실행 클러스터 하여를 생성합니다.

   - 단일 AZ

```
rosa create cluster --private-link --cluster-name=<CLUSTER_NAME> --machine-
cidr=10.0.0.0/16 --subnet-ids=<PRIVATE_SUBNET_ID>
```

- 다중 AZ

```
rosa create cluster --private-link --multi-az --cluster-name=<CLUSTER_NAME> --
machine-cidr=10.0.0.0/16
```

> **Note**
>
> AWS Security Token Service (AWS STS) 단기 자격 증명과 AWS PrivateLink 함께를 사용하는 클러스터`--sts --mode manual`를 생성하려면 `rosa create cluster` 명령 끝에 `--sts --mode auto` 또는를 추가합니다.

3. 대화형 프롬프트에 따라 클러스터 연산자 IAM 역할을 생성합니다.

```
rosa create operator-roles --interactive -c <CLUSTER_NAME>
```

4. 클러스터 운영자가 인증에 사용하는 OpenID Connect(OIDC) 공급자를 생성합니다.

```
rosa create oidc-provider --interactive -c <CLUSTER_NAME>
```

5. 의 상태를 확인합니다 클러스터.

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> `State` 필드가 `ready` 상태를 표시하는 데 최대 40분이 클러스터 걸릴 수 있습니다. 프로비저닝이 실패하거나 40분 `ready` 후에 로 표시되지 않는 경우 섹션을 참조하세요문제 해결. 지원 또는 Red Hat 지원팀에 문의하여 지원을 받으려면 섹션을 참조하세요the section called “지원 받기”.

6. OpenShift 설치 관리자 로그를 확인하여 클러스터 생성 진행 상황을 추적합니다.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

AWS PrivateLink DNS 전달 구성

를 사용하는 클러스터는에서 퍼블릭 호스팅 영역과 프라이빗 호스팅 영역을 AWS PrivateLink 생성합니다 Route 53. Route 53 프라이빗 호스팅 영역 내의 레코드는 할당된 VPC 내에서만 확인할 수 있습니다.

Let's Encrypt DNS-01 검증에는 유효하고 공개적으로 신뢰할 수 있는 인증서를 도메인에 발급할 수 있는 공개 영역이 필요합니다. 검증 레코드는 Let's Encrypt 검증이 완료된 후에 삭제됩니다. 영역은 인증서를 발급하고 갱신하는 데 계속 필요하며, 일반적으로 60일마다 필요합니다. 영역은 일반적으로 비어 있는 것처럼 보이지만 검증 프로세스에서 공개 영역의 역할은 중요합니다.

AWS 프라이빗 호스팅 영역에 대한 자세한 내용은 프라이빗 영역 작업을 참조하세요. 퍼블릭 호스팅 영역에 대한 자세한 정보는 퍼블릭 호스팅 영역 작업을 참조하세요.

Route 53 Resolver 인바운드 엔드포인트 구성

1. `api.<cluster_domain>` 및와 같은 레코드가 VPC 외부에서 확인`*.apps.<cluster_domain>`되도록 하려면 Route 53 Resolver 인바운드 엔드포인트를 구성합니다.

   > **Note**
   >
   > 인바운드 엔드포인트를 구성할 때 중복성을 위해 최소 2개의 IP 주소를 지정해야 합니다. 최소한 2개의 가용 영역에 IP 주소를 지정하는 것이 좋습니다. 선택적으로 그러한 가용 영역 또는 다른 가용 영역에 추가 IP 주소를 지정할 수 있습니다.

2. 인바운드 엔드포인트를 구성할 때 클러스터를 생성할 때 사용된 VPC 및 프라이빗 서브넷을 선택합니다.

클러스터의 DNS 전달 구성

Route 53 Resolver 내부 엔드포인트가 연결되고 작동한 후 네트워크의 지정된 서버에서 DNS 쿼리를 처리할 수 있도록 DNS 전달을 구성합니다.

1. DNS 쿼리를 최상위 도메인의 IP 주소(예:`drow-pl-01.htno.p1.openshiftapps.com`)로 전달하도록 회사 네트워크를 구성합니다.
2. 한 VPC에서 다른 VPC로 DNS 쿼리를 전달하는 경우 전달 규칙 관리 지침을 따르세요.
3. 원격 네트워크 DNS 서버를 구성하는 경우 특정 DNS 서버 설명서를 참조하여 설치된 클러스터 도메인에 대한 선택적 DNS 전달을 구성합니다.

자격 증명 공급자 구성 및 클러스터 액세스 권한 부여

ROSA 에는 기본 제공 OAuth 서버가 포함되어 있습니다. ROSA 클러스터 생성 이후 ID 공급자를 사용하려면 OAuth를 구성해야 합니다. 그런 다음 구성된 ID 공급자에 사용자를 추가하여 클러스터액세스 권한을 부여할 수 있습니다. 필요에 따라 이러한 사용자에게 `cluster-admin` 또는 `dedicated-admin` 권한을 부여할 수 있습니다.

클러스터에 맞게 다양한 ID 제공자 유형을 구성할 수 있습니다 . 지원되는 유형으로는 GitHub, GitHub Enterprise, GitLab, Google, LDAP, OpenID Connect, HTPasswd ID 공급자 등이 있습니다.

> **Important**
>
> HTPasswd ID 공급자는 한 명의 정적 관리자 사용자를 생성할 수 있도록 하기 위한 용도로만 포함됩니다. HTPassWD는 ROSA범용 ID 공급자로는 지원되지 않습니다.

다음 절차는 GitHub ID 공급자를 예로 구성합니다. 지원되는 각 ID 제공자 유형을 구성하는 방법에 대한 지침은 AWS STS ID 제공자 구성을 참조하세요.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. ROSA 클러스터 ID 프로비저닝에 사용할 GitHub 조직이 없는 경우 하나 생성합니다. 자세한 내용을 알아보려면 GitHub의 설명서의 단계를 참조하세요.
3. ROSA CLI의 대화형 모드를 사용하여 다음 명령을 실행하여 클러스터의 자격 증명 공급자를 구성합니다.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 출력의 구성 프롬프트에 따라 GitHub 조직의 멤버에 대한 클러스터 액세스를 제한합니다.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
```

```
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 출력에서 URL을 열고 <GITHUB_ORG_NAME>를 GitHub 조직의 이름으로 대체합니다.
6. GitHub 웹 페이지에서 애플리케이션 등록을 선택하여 GitHub 조직에 새 OAuth 애플리케이션을 등록합니다.
7. GitHub OAuth 페이지의 정보를 사용하여 나머지 `rosa create idp` 대화형 프롬프트를 채우고 GitHub OAuth 애플리케이션의 자격 증명으로 <GITHUB_CLIENT_ID> 및 <GITHUB_CLIENT_SECRET>을 대체합니다.

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> ID 공급자 구성이 활성화되는 데 2분 정도 걸릴 수 있습니다. `cluster-admin` 사용자를 구성한 경우 `oc get pods -n openshift-authentication --watch` 명령을 실행하여 업데이트된 구성으로 OAuth 포드가 재배포되는 것을 관찰할 수 있습니다.

8. ID 공급자가 올바르게 구성됐는지 확인합니다.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

사용자에게에 대한 액세스 권한 부여 클러스터

구성된 자격 증명 공급자에 추가하여 사용자에게에 대한 액세스 권한을 부여할 수 클러스터 있습니다.

다음 절차는 클러스터에 ID를 프로비저닝하도록 구성된 GitHub 조직에 사용자를 추가합니다.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. GitHub 조직에 클러스터 액세스해야 하는 사용자를 초대합니다. 자세한 내용은 GitHub 설명서에서 조직에 가입하도록 사용자 초대하기를 참조하세요.

`cluster-admin` 권한 구성

1. 다음 명령을 사용하여 `cluster-admin` 권한을 부여합니다. `<IDP_USER_NAME>` 및 `<CLUSTER_NAME>`을 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 `cluster-admins` 그룹 구성원으로 등록되어 있는지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

`dedicated-admin` 권한 구성

1. 다음 명령으로 `dedicated-admin` 권한을 부여합니다. `<IDP_USER_NAME>` 및 `<CLUSTER_NAME>`를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 `cluster-admins` 그룹 구성원으로 등록되어 있는지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 액세스

클러스터 관리자 사용자를 생성하거나 구성된 자격 증명 공급자에 사용자를 추가한 후 Red Hat Hybrid Cloud 콘솔을 클러스터 통해에 로그인할 수 있습니다.

1. 다음 명령을 클러스터 사용하여의 콘솔 URL을 가져옵니다. 를의 이름으로 `<CLUSTER_NAME>` 바꿉니다 클러스터.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 출력에서 콘솔 URL로 이동하여 로그인합니다.
   - `cluster-admin` 사용자를 생성한 경우 제공된 보안 인증 정보를 사용하여 로그인합니다.
   - 에 대한 자격 증명 공급자를 구성한 경우 로그인... 대화 상자에서 자격 클러스터증명 공급자 이름을 선택하고 공급자가 제시한 권한 부여 요청을 완료합니다.

개발자 카탈로그에서 애플리케이션 배포

Red Hat 하이브리드 클라우드 콘솔에서 개발자 카탈로그 테스트 애플리케이션을 배포하고 경로를 통해 공개할 수 있습니다.

1. Red Hat 하이브리드 클라우드 콘솔로 이동하여 앱을 배포할 클러스터를 선택합니다.
2. 클러스터 페이지에서 콘솔 열기를 선택합니다.
3. 관리자 시점에서 홈 > 프로젝트 > 프로젝트 생성을 선택합니다.
4. 프로젝트 이름을 입력하고 선택적으로 표시 이름 및 설명을 추가합니다.
5. 프로젝트를 생성하려면 생성을 선택합니다.
6. 개발자 시점으로 전환하고 +추가를 선택합니다. 선택한 프로젝트가 방금 만든 프로젝트인지 확인합니다.
7. 개발자 카탈로그 대화 상자에서 모든 서비스를 선택합니다.
8. 개발자 카탈로그 페이지의 메뉴에서 언어 > JavaScript를 선택합니다.
9. Node.js를 선택한 다음 애플리케이션 생성을 선택하여 Source-to-Image 애플리케이션 생성 페이지를 엽니다.

> **Note**
>
> Node.js 옵션을 표시하려면 모든 필터 지우기를 선택해야 할 수도 있습니다.

10. Git 섹션에서 샘플 사용해보기를 선택합니다.
11. 이름 필드에 고유한 이름을 추가합니다.
12. 생성(Create)을 선택합니다.

> **Note**
>
> 새 애플리케이션을 배포하는 데 몇 분 정도 걸립니다.

13.배포가 완료되면 애플리케이션 경로 URL을 선택합니다.

브라우저의 새 탭이 열리고 다음과 비슷한 메시지가 표시됩니다.

```
Welcome to your Node.js application on OpenShift
```

14.(선택 사항) 애플리케이션을 삭제하고 리소스를 정리합니다.

a. 관리자 시점에서 홈 > 프로젝트를 선택합니다.

b. 프로젝트의 작업 메뉴를 열고 프로젝트 삭제를 선택합니다.

사용자의 **cluster-admin** 권한 취소

1. 다음 명령을 사용하여 `cluster-admin` 권한을 취소합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 `cluster-admins` 그룹 구성원으로 등록되어 있지 않은지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

사용자의 **dedicated-admin** 권한 취소

1. 다음 명령을 사용하여 `dedicated-admin` 권한을 취소합니다. <IDP_USER_NAME> 및 <CLUSTER_NAME>를 사용자 및 클러스터 이름으로 바꿉니다.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 사용자가 `dedicated-admins` 그룹 구성원으로 등록되어 있지 않은지 확인합니다.

```
rosa list users --cluster=<CLUSTER_NAME>
```

에 대한 사용자 액세스 취소 클러스터

구성된 자격 증명 공급자에서 자격 증명 공급자를 제거하여 자격 증명 공급자 사용자의 클러스터 액세스를 취소할 수 있습니다.

클러스터에 다양한 ID 공급자 유형을 구성할 수 있습니다. 다음 절차는 GitHub 조직의 멤버에 대한 클러스터 액세스를 취소합니다.

1. github.com으로 이동하여 GitHub 계정에 로그인합니다.
2. GitHub 조직에서 사용자를 제거합니다. 자세한 내용은 GitHub 설명서에서 조직에서 사용자 제거하기를 참조하세요.

클러스터 및 AWS STS 리소스 삭제

ROSA CLI를 사용하여 AWS Security Token Service ()를 사용하는 클러스터 를 삭제할 수 있습니다 AWS STS. ROSA CLI를 사용하여에서 생성한 IAM 역할 및 OIDC 공급자를 삭제할 수도 있습니다 ROSA. 에서 생성한 IAM 정책을 삭제하려면 IAM 콘솔을 사용할 ROSA수 있습니다.

> **Important**
>
> IAM 에서 생성한 역할 및 정책은 동일한 계정의 다른 ROSA 클러스터에서 사용할 ROSA 수 있습니다.

1. 를 삭제 클러스터 하고 로그를 확인합니다. <CLUSTER_NAME>을 클러스터이름 또는 ID로 바꿉니다.

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> IAM 역할, 정책 및 OIDC 공급자 클러스터 를 제거하기 전에가 완전히 삭제될 때까지 기다려야 합니다. 설치 관리자가 생성한 리소스를 삭제하려면 계정 IAM 역할이 필요합니다. OpenShift 운영자가 생성한 리소스를 정리하려면 운영자 IAM 역할이 필요합니다. 운영자는 인증 시 OIDC 공급자를 사용합니다.

2. 다음 명령을 실행하여 클러스터 운영자가 인증에 사용하는 OIDC 공급자를 삭제합니다.

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 클러스터별 연산자 IAM 역할을 삭제합니다.

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 다음 명령을 사용하여 계정 IAM 역할을 삭제합니다. <PREFIX>를 삭제할 계정 IAM 역할의 접두사로 바꿉니다. 계정 IAM 역할을 생성할 때 사용자 지정 접두사를 지정한 경우 기본 ManagedOpenShift 접두사를 지정합니다.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 에서 생성한 IAM 정책을 삭제합니다 ROSA.
   a. IAM 콘솔에 로그인합니다.
   b. 왼쪽 메뉴의 액세스 관리에서 정책을 선택합니다.
   c. 삭제하려는 정책을 선택하고 작업 > 삭제를 선택합니다.
   d. 정책 이름을 입력하고 삭제를 선택합니다.
   e. 이 단계를 반복하여 클러스터에 대한 IAM 정책을 각각 삭제합니다.

의 보안 ROSA

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

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

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 AWS 서비스 규정 준수 프로그램 제공 범위 섹션을 ROSA참조하세요.
- 클라우드의 보안 - 사용자의 책임은 AWS 서비스 사용하는에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다 ROSA. 보안 및 규정 준수 목표를 충족하도록 ROSA 를 구성하는 방법을 보여줍니다. 또한 ROSA 리소스를 모니터링하고 보호하는 데 도움이 AWS 서비스 되는 다른를 사용하는 방법을 알아봅니다.

내용

- 의 데이터 보호 ROSA
- 에 대한 자격 증명 및 액세스 관리 ROSA
- 의 복원력 ROSA
- 의 인프라 보안 ROSA

의 데이터 보호 ROSA

the section called “책임” 설명서 및 AWS 공동 책임 모델은 in ROSA.의 데이터 보호를 정의합니다. AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. Red Hat은 클러스터 인프라와 기본 서비스 플랫폼을 보호할 책임이 있습니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 고객의 책임입니다. 이 콘텐츠에는 AWS 서비스 사용하는에 대한 보안 구성 및 관리 작업이 포함됩니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하

세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

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

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- 와 같은 고급 관리형 보안 서비스를 사용하면 Amazon Macie에 저장된 민감한 데이터를 검색하고 보호할 수 있습니다 Amazon S3.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-2 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2 섹션을 참조하세요.

명칭 필드와 같은 자유 형식 필드에 고객 계정 번호와 같은 중요 식별 정보를 절대 입력하지 마세요. 여기에는 ROSA 또는 기타에서 콘솔, API AWS CLI또는 AWS SDKs를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. ROSA 또는 다른 서비스에 입력하는 모든 데이터가 진단 로그에 포함되도록 선택될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함하지 마십시오.

주제

- 암호화를 사용하여 데이터 보호

암호화를 사용하여 데이터 보호

데이터 보호는 전송 중(전송 중) 및 저장 중(데이터 센터의 디스크에 저장되는 동안 ROSA) AWS 데이터를 보호하는 것을 말합니다.

Red Hat OpenShift Service on AWS 는 ROSA 컨트롤 플레인, 인프라 및 작업자 노드용 Amazon EC2 인스턴스에 연결된 Amazon Elastic Block Store (Amazon EBS) 스토리지 볼륨과 영구 스토리지용 Kubernetes 영구 볼륨에 대한 보안 액세스를 제공합니다.는 저장 및 전송 중인 볼륨 데이터를 ROSA 암호화하고 AWS Key Management Service (AWS KMS)를 사용하여 암호화된 데이터를 보호합니다.

서비스는 기본적으로 저장 시 암호화된 컨테이너 이미지 레지스트리 스토리지 Amazon S3 에를 사용합니다.

> **Important**
>
> ROSA 는 관리형 서비스이며 AWS Red Hat은가 ROSA 사용하는 인프라를 관리합니다. 고객은 AWS 콘솔 또는 CLI에서가 ROSA 사용하는 Amazon EC2 인스턴스를 수동으로 종료하려고 해서는 안 됩니다. 이 작업은 고객 데이터 손실로 이어질 수 있습니다.

지원 스토리지 볼륨 Amazon EBS에 대한 데이터 암호화

Red Hat OpenShift Service on AWS 는 Kubernetes 영구 볼륨(PV) 프레임워크를 사용하여 클러스터 관리자가 영구 스토리지로 클러스터를 프로비저닝할 수 있도록 합니다. 영구 볼륨과 컨트롤 플레인, 인프라 및 작업자 노드는 Amazon EC2 인스턴스에 연결된 Amazon Elastic Block Store (Amazon EBS) 스토리지 볼륨에 의해 지원됩니다.

에서 지원하는 ROSA 영구 볼륨 및 노드의 경우 EC2 인스턴스를 호스팅하는 서버에서 Amazon EBS 암호화 작업이 수행되므로 인스턴스와 연결된 스토리지 간에 저장된 데이터와 전송 중인 데이터의 보안이 보장됩니다. 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EBS 암호화를 참조하세요.

Amazon EBS CSI 드라이버 및 Amazon EFS CSI 드라이버의 데이터 암호화

ROSA 는 기본적으로 Amazon EBS CSI 드라이버를 사용하여 Amazon EBS 스토리지를 프로비저닝합니다. Amazon EBS CSI 드라이버와 Amazon EBS CSI 드라이버 연산자는 기본적으로 `openshift-cluster-csi-drivers` 네임스페이스에 클러스터에 설치됩니다. Amazon EBS CSI 드라이버와 연산자를 사용하면 영구 볼륨을 동적으로 프로비저닝하고 볼륨 스냅샷을 생성할 수 있습니다.

ROSA 는 CSI 드라이버 및 Amazon EFS Amazon EFS CSI 드라이버 운영자를 사용하여 영구 볼륨을 프로비저닝할 수도 있습니다. 또한 Amazon EFS 드라이버와 연산자를 사용하면 포드 간에 또는 Kubernetes 내부 또는 외부의 다른 애플리케이션과 파일 시스템 데이터를 공유할 수 있습니다.

볼륨 데이터는 Amazon EBS CSI 드라이버와 Amazon EFS CSI 드라이버 모두에 대해 전송 중에 보호됩니다. 자세한 내용은 Red Hat 설명서의 컨테이너 스토리지 인터페이스(CSI) 사용을 참조하십시오.

> **Important**
>
> Amazon EFS CSI 드라이버를 사용하여 ROSA 영구 볼륨을 동적으로 프로비저닝하는 경우 파일 시스템 권한을 평가할 때 액세스 포인트의 사용자 ID, 그룹 ID(GID) 및 보조 그룹 IDs를

Amazon EFS 고려합니다.는 파일의 사용자 및 그룹 IDs를 액세스 포인트의 사용자 및 그룹 IDs로 Amazon EFS 바꾸고 NFS 클라이언트 IDs. 따라서는 `fsGroup` 설정을 Amazon EFS 자동으로 무시합니다. ROSA 는를 사용하여 파일의 GIDs를 교체할 수 없습니다`fsGroup`. 탑재된 Amazon EFS 액세스 포인트에 액세스할 수 있는 모든 포드는 볼륨의 모든 파일에 액세스할 수 있습니다. 자세한 내용은 Amazon EFS 사용 설명서의 Amazon EFS 액세스 포인트 작업을 참조하세요.

etcd 암호화

ROSA 는 클러스터 생성 중에 `etcd` 볼륨 내의 `etcd` 키 값 암호화를 활성화하여 추가 암호화 계층을 추가하는 옵션을 제공합니다. `etcd`가 암호화된 후 약 20%의 성능 오버헤드가 추가적으로 발생합니다. 사용 사례에 특별히 필요한 경우에만 `etcd` 암호화를 활성화하는 것이 좋습니다. 자세한 내용은 ROSA 서비스 정의의 etcd 암호화를 참조하세요.

키 관리

ROSA 는 KMS keys 를 사용하여 고객 애플리케이션의 컨트롤 플레인, 인프라, 작업자 데이터 볼륨 및 영구 볼륨을 안전하게 관리합니다. 클러스터를 생성하는 동안에서 KMS key 제공하는 기본 AWS 관리형 키를 사용하거나 자체 고객 관리형 키를 Amazon EBS지정할 수 있습니다. 자세한 내용은 the section called “키 관리” 단원을 참조하십시오.

내장 이미지 레지스트리의 데이터 암호화

ROSA 는 Amazon S3 버킷 스토리지를 통해 컨테이너 이미지를 저장, 검색 및 공유할 수 있는 기본 제공 컨테이너 이미지 레지스트리를 제공합니다. 레지스트리는 OpenShift 이미지 레지스트리 운영자가 구성하고 관리합니다. 사용자가 워크로드를 실행하는 이미지를 관리할 수 있는 즉시 사용 가능한 솔루션을 제공하며 기존 클러스터 인프라에서 실행됩니다. 자세한 내용은 Red Hat 설명서에서 레지스트리를 참조하세요.

ROSA 는 퍼블릭 및 프라이빗 이미지 레지스트리를 제공합니다. 엔터프라이즈 애플리케이션의 경우 권한이 없는 사용자가 이미지를 사용하지 못하도록 프라이빗 레지스트리를 사용하는 것이 좋습니다. 레지스트리의 저장 데이터를 보호하기 위해는 기본적으로 Amazon S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화를 ROSA 사용합니다. 이 작업에 대한 조치는 필요하지 않으며 추가 비용 없이 제공됩니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 관리형 암호화 키(SSE-S3)를 사용한 서버 측 암호화를 사용하여 데이터 보호를 참조하세요.

ROSA 는 TLS(전송 계층 보안) 프로토콜을 사용하여 이미지 레지스트리와 주고받는 전송 중 데이터를 보호합니다. 자세한 내용은 Red Hat 설명서에서 레지스트리를 참조하세요.

인터네트워크 트래픽 개인 정보

Red Hat OpenShift Service on AWS 는 Amazon Virtual Private Cloud (Amazon VPC)를 사용하여 ROSA 클러스터의 리소스 간에 경계를 생성하고 해당 리소스, 온프레미스 네트워크 및 인터넷 간의 트래픽을 제어합니다. Amazon VPC 보안에 대한 자세한 내용은 Amazon VPC 사용 설명서의 의 Internetwork 트래픽 개인 정보 보호를 Amazon VPC 참조하세요.

VPC 내에서 HTTP 또는 HTTPS 프록시 서버를 사용하여 직접 인터넷 액세스를 거부하도록 ROSA 클러스터를 구성할 수 있습니다. 클러스터 관리자인 경우 인터네트워크 트래픽을 ROSA 클러스터의 포드로 제한하는 포드 수준에서 네트워크 정책을 정의할 수도 있습니다. 자세한 내용은 the section called “인프라 보안” 단원을 참조하십시오.

KMS를 사용하여 데이터 암호화

ROSA 는 AWS KMS 를 사용하여 암호화된 데이터의 키를 안전하게 관리합니다. 컨트롤 플레인, 인프라 및 작업자 노드 볼륨은 기본적으로에서 KMS key 제공하는 AWS 관리형를 사용하여 암호화됩니다 Amazon EBS. 여기에는 별칭 KMS key 이 있습니다`aws/ebs`. 기본 gp3 스토리지 클래스를 사용하는 영구 볼륨도 기본적으로 이 KMS key를 사용하여 암호화됩니다.

새로 생성된 ROSA 클러스터는 기본 gp3 스토리지 클래스를 사용하여 영구 볼륨을 암호화하도록 구성됩니다. 다른 스토리지 클래스를 사용하여 생성된 영구 볼륨은 스토리지 클래스가 암호화되도록 구성된 경우에만 암호화됩니다. ROSA 사전 구축된 스토리지 클래스에 대한 자세한 내용은 Red Hat 설명서의 영구 스토리지 구성을 참조하세요.

클러스터를 생성하는 동안 기본 Amazon EBS제공 키를 사용하여 클러스터의 영구 볼륨을 암호화하거나 자체 고객 관리형 대칭을 지정할 수 있습니다 KMS key. 키 생성에 대한 자세한 내용은 AWS KMS 개발자 안내서의 대칭 암호화 KMS 키 생성을 참조하세요.

또한 KMS key를 정의하여 클러스터 내 개별 컨테이너의 영구 볼륨을 암호화할 수도 있습니다. 이는에 배포할 때 명시적인 규정 준수 및 보안 지침이 있는 경우에 유용합니다 AWS. 자세한 내용은 Red Hat 설명서의 를 AWS 사용하여에서 컨테이너 영구 볼륨 암호화 KMS key를 참조하세요.

자체 KMS keys를 사용하여 영구 볼륨을 암호화할 때는 다음 사항을 고려해야 합니다.

- KMS 암호화를 자체 암호화와 함께 사용하는 경우 키 KMS key는 클러스터 AWS 리전 와 동일한에 있어야 합니다.
- 자체 생성 및 사용과 관련된 비용이 있습니다 KMS keys. 자세한 내용은 AWS Key Management Service 요금을 참조하십시오.

에 대한 자격 증명 및 액세스 관리 ROSA

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 AWS 서비스 도와주는 입니다. IAM 관리자는 ROSA 누가 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)될 수 있는지를 제어합니다. IAM 는 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

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

서비스 사용자 - ROSA 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 ROSA 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. 의 기능에 액세스할 수 없는 경우 섹션을 ROSA참조하세요the section called “문제 해결”.

서비스 관리자 - 회사에서 ROSA 리소스를 책임지고 있는 경우에 대한 전체 액세스 권한을 가지고 있을 것입니다 ROSA. 서비스 관리자는 서비스 사용자가 액세스해야 하는 ROSA 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여의 기본 개념을 이해합니다 IAM.

IAM 관리자 - IAM 관리자인 경우 액세스를 관리하는 데 사용되는 정책에 대한 세부 정보를 알고 싶을 수 있습니다 ROSA. 에서 사용할 수 있는 자격 ROSA 증명 기반 정책 예제를 보려면 섹션을 IAM참조하세요the section called “ ROSA 자격 증명 기반 정책 예제”.

ID를 통한 인증

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

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

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

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하세요.

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

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하세요.

페더레이션 ID

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

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

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

IAM 사용자 및 그룹

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

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

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

IAM 역할

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

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 자격 증명에 권한을 할당하려면 역할을 생성하고 역할에 대한 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 관리하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 IAM Identity Center(Single Sign-On 후속) 사용 설명서의 권한 세트를 참조하세요. AWS AWS
- 임시 IAM 사용자 권한 -는 IAM 역할을 수임하여 특정 작업에 대해 다른 권한을 일시적으로 수임할 IAM 사용자 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 교차 계정 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할이 리소스 기반 정책과 어떻게 다른지 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가에서 애플리케이션을 실행 Amazon EC2 하거나에 객체를 저장하는 것이 일반적입니다 Amazon S3. 서비스는 직접 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다 IAM. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 IAM 계정에 표시되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- 에서 Amazon EC2 실행되는 애플리케이션 - IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 Amazon EC2 인스턴스 내에 액세스 키를 저장하는 것보다 더 좋습니다. Amazon EC2 인스

턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되며 Amazon EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

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

정책을 사용하여 액세스 관리

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

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

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하기 위해 IAM 관리자는 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

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

ID 기반 정책

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

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩

니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

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

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책의 IAM 에서는 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

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

Amazon S3 AWS WAF, 및 Amazon VPC 는 ACLs. ACLs에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 유형

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

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책의 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 개체에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 AWS 계정 루트 사용자를 포

함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다. 조직 및 SCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책(SCPs)을 참조하세요.

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

여러 정책 유형

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

ROSA 자격 증명 기반 정책 예제

기본적으로 IAM 사용자 및 역할에는 AWS 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 AWS API를 사용하여 작업을 수행할 수 없습니다. IAM 관리자는 사용자 및 역할에 필요한 지정된 리소스에 대해 특정 API 작업을 수행할 수 있는 권한을 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 해당 정책을 연결해야 합니다.

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

ROSA 콘솔 사용

콘솔 ROSA 에서를 구독하려면 IAM 보안 주체에 필요한 AWS Marketplace 권한이 있어야 합니다. 권한을 통해 보안 주체는의 ROSA 제품 목록을 구독 및 구독 취소 AWS Marketplace 하고 AWS Marketplace 구독을 볼 수 있습니다. 필요한 권한을 추가하려면 ROSA 콘솔로 이동하여 AWS 관리형 정책을 IAM 보안 주체ROSAManageSubscription에 연결합니다. ROSAManageSubscription에 대한 자세한 정보는 the section called “AWS 관리형 정책: ROSAManageSubscription” 섹션을 참조하세요.

리소스 관리를 위한 ROSA with HCP 권한 부여 AWS

호스팅 컨트롤 플레인(HCP)이 있는 ROSA는 서비스 운영 및 지원에 필요한 권한이 있는 AWS 관리형 정책을 사용합니다. ROSA CLI 또는 IAM 콘솔을 사용하여 이러한 정책을의 서비스 역할에 연결합니다 AWS 계정.

자세한 내용은 the section called “ AWS 관리형 정책” 단원을 참조하십시오.

ROSA 클래식에 AWS 리소스 관리 권한 부여

ROSA 클래식은 서비스에 의해 사전 정의된 권한이 있는 고객 관리형 IAM 정책을 사용합니다. ROSA CLI를 사용하여 이러한 정책을 생성하고의 서비스 역할에 연결합니다 AWS 계정. 에서는 지속적인 운영 및 서비스 지원을 보장하기 위해 이러한 정책을 서비스에서 정의한 대로 구성해야 ROSA 합니다.

> **Note**
>
> 먼저 Red Hat과 상의하지 않고 ROSA 클래식 정책을 변경해서는 안 됩니다. 이렇게 하면 Red Hat의 99.95% 클러스터 가동 시간 서비스 수준 계약이 무효화될 수 있습니다. 호스팅된 컨트롤 플레인이 있는 ROSA는 보다 제한된 권한 집합의 AWS 관리형 정책을 사용합니다. 자세한 내용은 the section called “ AWS 관리형 정책” 단원을 참조하십시오.

에는 계정 정책 및 운영자 정책 ROSA이라는 두 가지 유형의 고객 관리형 정책이 있습니다. 계정 정책은 서비스가 사이트 신뢰성 엔지니어(SRE) 지원, 클러스터 생성 및 컴퓨팅 기능을 위해 Red Hat과 신뢰 관계를 설정하는 데 사용하는 IAM 역할에 연결됩니다. 운영자 정책은 OpenShift 운영자가 수신, 스토리지, 이미지 레지스트리 및 노드 관리와 관련된 클러스터 작업에 사용하는 IAM 역할에 연결됩니다. 계정 정책은 1개당 1회 생성되는 반면 AWS 계정, 운영자 정책은 클러스터당 1회 생성됩니다.

자세한 내용은 the section called “ROSA 클래식 계정 정책” 및 the section called “ROSA 클래식 연산자 정책” 섹션을 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는가 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 IAM 사용자 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함되어 있습니다 AWS CLI.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

```
            ],
            "Effect": "Allow",
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

ROSA 클래식 계정 정책

이 섹션에서는 ROSA 클래식에 필요한 계정 정책에 대한 세부 정보를 제공합니다. 이러한 권한은 ROSA 클래식이 클러스터가 실행되는 AWS 리소스를 관리하고 클러스터에 대한 Red Hat 사이트 신뢰성 엔지니어 지원을 활성화하는 데 필요합니다. 정책 이름에 사용자 지정 접두사를 할당할 수 있지만, 그렇지 않으면이 페이지에 정의된 대로 이러한 정책의 이름을 지정해야 합니다(예: `ManagedOpenShift-Installer-Role-Policy`).

계정 정책은 OpenShift 마이너 릴리스 버전에 고유하며 이전 버전과 호환됩니다. 클러스터를 생성하거나 업그레이드하기 전에를 실행하여 정책 버전과 클러스터 버전이 동일한지 확인해야 합니다`rosa list account-roles`. 정책 버전이 클러스터 버전보다 작은 경우를 실행`rosa upgrade account-roles`하여 역할 및 연결된 정책을 업그레이드합니다. 동일한 마이너 릴리스 버전의 여러 클러스터에 대해 동일한 계정 정책 및 역할을 사용할 수 있습니다.

[접두사]-Installer-Role-Policy

`[Prefix]-Installer-Role-Policy`를 IAM 엔티티에 연결할 수 있습니다. ROSA 클래식 클러스터를 생성하려면 먼저이 정책을 라는 IAM 역할에 연결해야 합니다`[Prefix]-Installer-Role`. 이 정책은 ROSA 설치 관리자가 클러스터 생성에 필요한 AWS 리소스를 관리할 수 있는 필수 권한을 부여합니다.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "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:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "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:DescribeAccountLimits",
                "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:TagInstanceProfile",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfiles",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
```

```
                "iam:ListUsers",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:SimulatePrincipalPolicy",
                "iam:TagRole",
                "iam:UntagRole",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone",
                "route53:GetAccountLimit",
                "route53:GetChange",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53:ListTagsForResource",
                "route53:UpdateHostedZoneComment",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketAcl",
                "s3:GetBucketCORS",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetReplicationConfiguration",
                "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:PutBucketVersioning",
                "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"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

[접두사]-ControlPlane-Role-Policy

`[Prefix]-ControlPlane-Role-Policy`를 IAM 엔티티에 연결할 수 있습니다. ROSA 클래식 클러스터를 생성하려면 먼저이 정책을 라는 IAM 역할에 연결해야 합니다`[Prefix]-ControlPlane-`

Role. 이 정책은 ROSA 클래식에 ROSA 컨트롤 플레인을 호스팅하는 Amazon EC2 Elastic Load Balancing 리소스와 읽기를 관리하는 데 필요한 권한을 부여합니다 KMS keys.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

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

[접두사]-Worker-Role-Policy

`[Prefix]-Worker-Role-Policy`를 IAM 엔티티에 연결할 수 있습니다. ROSA 클래식 클러스터를 생성하려면 먼저이 정책을 라는 IAM 역할에 연결해야 합니다`[Prefix]-Worker-Role`. 이 정책은 ROSA 클래식에 작업자 노드로 실행되는 EC2 인스턴스를 설명하는 데 필요한 권한을 부여합니다.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

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

[접두사]-Support-Role-Policy

`[Prefix]-Support-Role-Policy`를 IAM 엔티티에 연결할 수 있습니다. ROSA 클래식 클러스터를 생성하려면 먼저이 정책을 라는 IAM 역할에 연결해야 합니다`[Prefix]-Support-Role`. 이 정책은 클러스터 노드 상태를 변경하는 기능을 포함하여 ROSA 클래식 클러스터가 사용하는 AWS 리소스를 관찰, 진단 및 지원하는 데 필요한 권한을 Red Hat 사이트 신뢰성 엔지니어링에 부여합니다.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "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:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "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"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

ROSA 클래식 연산자 정책

이 섹션에서는 ROSA 클래식에 필요한 연산자 정책에 대한 세부 정보를 제공합니다. ROSA 클래식 클러스터를 생성하려면 먼저 관련 운영자 역할에 이러한 정책을 연결해야 합니다. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이러한 권한은 OpenShift 연산자가 ROSA 클래식 클러스터 노드를 관리할 수 있도록 하는 데 필요합니다. 정책 이름에 사용자 지정 접두사를 할당하여 정책 관리를 간소화할 수 있습니다(예: `ManagedOpenShift-openshift-ingress-operator-cloud-credentials`).

[접두사]-openshift-ingress-operator-cloud-credentials

`[Prefix]-openshift-ingress-operator-cloud-credentials`를 IAM 엔티티에 연결할 수 있습니다. 이 정책은 수신 연산자에게 외부 클러스터 액세스를 위한 로드 밸런서 및 DNS 구성을 프로비저닝하고 관리하는 데 필요한 권한을 부여합니다. 또한이 정책은 수신 연산자가 Route 53 리소스 태그 값을 읽고 필터링하여 호스팅 영역을 검색하도록 허용합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서에서 OpenShift 수신 운영자를 참조하세요.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

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

[접두사]-openshift-cluster-csi-drivers-ebs-cloud-credentials

`[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials`를 IAM 엔티티에 연결할 수 있습니다. 이 정책은 Amazon EBS CSI 드라이버 운영자에게 ROSA 클래식 클러스터에 Amazon EBS CSI 드라이버를 설치하고 유지 관리하는 데 필요한 권한을 부여합니다. 연산자에 대한 자세한 내용은 OpenShift GitHub 설명서의 aws-ebs-csi-driver-operator를 참조하세요.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

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

[접두사]-openshift-machine-api-aws-cloud-credentials

`[Prefix]-openshift-machine-api-aws-cloud-credentials`를 IAM 엔티티에 연결할 수 있습니다. 이 정책은 Machine Config Operator에 작업자 노드로 관리되는 Amazon EC2 인스턴스를 설

명, 실행 및 종료하는 데 필요한 권한을 부여합니다. 또한이 정책은를 사용하여 작업자 노드 루트 볼륨의 디스크 암호화를 허용하는 권한을 부여합니다 AWS KMS keys. 연산자에 대한 자세한 내용은 OpenShift GitHub 설명서의 machine-config-operator를 참조하세요.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
```

```
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

[접두사]-openshift-cloud-credential-operator-cloud-credentials

`[Prefix]-openshift-cloud-credential-operator-cloud-credentials`를 IAM 엔티티에 연결할 수 있습니다. 이 정책은 액세스 키 IDs, 연결된 인라인 정책 문서, 사용자의 생성 날짜, 경로, 사용자 ID 및 Amazon 리소스 이름(ARN)을 포함한 IAM 사용자 세부 정보를 검색하는 데 필요한 권한을 클라우드 자격 증명 운영자에게 부여합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서의 cloud-credential-operator를 참조하세요.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:ListAccessKeys"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[접두사]-openshift-image-registry-installer-cloud-credentials

`[Prefix]-openshift-image-registry-installer-cloud-credentials`를 IAM 엔티티에 연결할 수 있습니다. 이 정책은 Image Registry Operator에 다음을 포함한 ROSA Classic의 클러스터 내 이미지 레지스트리 및 종속 서비스에 대한 리소스를 프로비저닝하고 관리하는 데 필요한 권한을 부여합니다 Amazon S3. 이는 운영자가 ROSA 클래식 클러스터의 내부 레지스트리를 설치하고 유지 관리하기 위해 필요합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서에서 이미지 레지스트리 운영자를 참조하세요.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

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

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[접두사]-openshift-cloud-network-config-controller-cloud-cr

`[Prefix]-openshift-cloud-network-config-controller-cloud-cr`를 IAM 엔티티에 연결할 수 있습니다. 이 정책은 ROSA 클래식 클러스터 네트워킹 오버레이에서 사용할 네트워킹 리소스를 프로비저닝하고 관리하는 데 필요한 권한을 클라우드 네트워크 구성 컨트롤러 운영자에게 부여합니다. 연산자는 이러한 권한을 사용하여 ROSA 클래식 클러스터의 일부로 Amazon EC2 인스턴스의 프라이빗 IP 주소를 관리합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서에서 Cloud-network-config-controller를 참조하세요.

권한 정책

이 정책 문서에 정의된 권한은 허용되거나 거부되는 작업을 지정합니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignIpv6Addresses",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 에 대한 관리형 정책 ROSA

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

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

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

AWS 관리형 정책: ROSAManageSubscription

`ROSAManageSubscription` 정책을 IAM 엔터티에 연결할 수 있습니다. ROSA 콘솔 ROSA 에서를 AWS 활성화하기 전에 먼저이 정책을 IAM 역할에 연결해야 합니다.

이 정책은 ROSA 구독을 관리하는 데 필요한 AWS Marketplace 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `aws-marketplace:Subscribe` - AWS Marketplace 제품을 구독할 수 있는 권한을 부여합니다 ROSA.
- `aws-marketplace:Unsubscribe` - 보안 주체가 AWS Marketplace 제품에 대한 구독을 제거할 수 있습니다.
- `aws-marketplace:ViewSubscriptions` - 보안 주체가 구독을 볼 수 있도록 허용합니다 AWS Marketplace. 이는 보안 IAM 주체가 사용 가능한 AWS Marketplace 구독을 볼 수 있도록 하기 위해 필요합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAManageSubscription을 참조하세요.

ROSA with HCP 계정 정책

이 섹션에서는 호스팅된 컨트롤 플레인(HCP)이 있는 ROSA에 필요한 계정 정책에 대한 세부 정보를 제공합니다. 이러한 AWS 관리형 정책은 ROSA에서 HCP IAM 역할과 함께 사용하는 권한을 추가합니다. Red Hat 사이트 신뢰성 엔지니어링(SRE) 기술 지원, 클러스터 설치, 컨트롤 플레인 및 컴퓨팅 기능에 권한이 필요합니다.

> **Note**
>
> AWS 관리형 정책은 ROSA에서 호스팅된 컨트롤 플레인(HCP)과 함께 사용하기 위한 것입니다. ROSA 클래식 클러스터는 고객 관리형 IAM 정책을 사용합니다. ROSA 클래식 정책에 대한 자세한 내용은 the section called “ROSA 클래식 계정 정책” 및 섹션을 참조하세요the section called “ROSA 클래식 연산자 정책”.

AWS 관리형 정책: ROSAWorkerInstancePolicy

IAM 엔터티`ROSAWorkerInstancePolicy`에를 연결할 수 있습니다. 클러스터를 생성하기 전에이 정책이 연결된 IAM 역할이 있어야 합니다. ROSA 서비스는 사용자를 대신하여 다른 AWS 서비스 를 호출합니다. 이렇게 하면 각 클러스터에서 사용하는 리소스를 관리할 수 있습니다.

권한 세부 정보

이 정책에는 ROSA 작업자 노드가 다음 작업을 완료할 수 있도록 허용하는 다음 권한이 포함되어 있습니다.

- `ec2` - ROSA 클러스터 작업자 노드 수명 주기 관리의 일환으로 AWS 리전 및 Amazon EC2 인스턴스 세부 정보를 평가합니다.
- `ecr` - 클러스터 설치 및 작업자 노드 수명 주기 관리에 필요한 ROSA 관리형 ECR 리포지토리의 이미지를 평가하고 가져옵니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAWorkerInstancePolicy를 참조하세요.

AWS 관리형 정책: ROSASRESupportPolicy

`ROSASRESupportPolicy`를 IAM 엔티티에 연결할 수 있습니다.

호스팅된 컨트롤 플레인 클러스터가 있는 ROSA를 생성하기 전에 먼저이 정책을 IAM 역할에 연결해야 합니다. 이 정책은 ROSA 클러스터 노드 상태를 변경하는 기능을 포함하여 ROSA 클러스터와 연

결된 AWS 리소스를 직접 관찰, 진단 및 지원하는 데 필요한 권한을 Red Hat 사이트 신뢰성 엔지니어(SREs)에게 부여합니다.

권한 세부 정보

이 정책에는 Red Hat SRE가 다음 태스크를 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- `cloudtrail` - 클러스터와 관련된 AWS CloudTrail 이벤트 및 추적을 읽습니다.
- `cloudwatch` - 클러스터와 관련된 Amazon CloudWatch 지표를 읽습니다.
- `ec2` - 보안 그룹, VPC 엔드포인트 연결, 볼륨 상태 등 클러스터 상태와 관련된 Amazon EC2 구성 요소를 읽고 설명하고 검토합니다. Amazon EC2 인스턴스를 시작, 중지, 재부팅 및 종료합니다.
- `elasticloadbalancing` - 클러스터 상태와 관련된 Elastic Load Balancing 파라미터를 읽고, 설명하고, 검토합니다.
- `iam` - 클러스터 상태와 관련된 IAM 역할을 평가합니다.
- `route53` - 클러스터 상태와 관련된 DNS 설정을 검토합니다.
- `sts` - `DecodeAuthorizationMessage`- 디버깅을 위해 IAM 메시지를 읽습니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSASRESupportPolicy를 참조하세요.

AWS 관리형 정책: ROSAInstallerPolicy

IAM 엔터티`ROSAInstallerPolicy`에를 연결할 수 있습니다.

호스팅된 컨트롤 플레인 클러스터가 있는 ROSA를 생성하기 전에 먼저이 정책을 라는 IAM 역할에 연결해야 합니다`[Prefix]-ROSA-Worker-Role`. 이 정책을 통해 엔티티는 `[Prefix]-ROSA-Worker-Role` 패턴을 따르는 모든 역할을 인스턴스 프로파일에 추가할 수 있습니다. 이 정책은 ROSA 클러스터 설치를 지원하는 AWS 리소스를 관리하는 데 필요한 권한을 설치 프로그램에 부여합니다.

권한 세부 정보

이 정책에는 설치 관리자가 다음 태스크를 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- `ec2` - Red Hat에서 AWS 계정 소유하고 관리하는에서 호스팅되는 AMIs 사용하여 Amazon EC2 인스턴스를 실행합니다. Amazon EC2 노드와 연결된 Amazon EC2 인스턴스, 볼륨 및 네트워크 리소스를 설명합니다. 이 권한은 Kubernetes 컨트롤 플레인이 인스턴스를 클러스터에 조인하고 클러스

터가 클러스터 내에서 인스턴스의 존재를 평가할 수 있도록 하기 위해 필요합니다 Amazon VPC. Amazon EC2 용량 예약을 검사하여 ROSA의 새로운 용량 예약 기능을 지원합니다. 와 일치하는 태그 키를 사용하여 서브넷의 태그에 태그를 지정하고 삭제합니다"`kubernetes.io/cluster/*`". 이는 클러스터 수신에 사용되는 로드 밸런서가 적용 가능한 서브넷에서만 생성되도록 하고 Kubernetes 클러스터 식별 태그를 관리하는 데 필요합니다.

- `elasticloadbalancing` - 클러스터의 대상 노드에 로드 밸런서를 추가합니다. 클러스터의 대상 노드에서 로드 밸런서를 제거합니다. 이 권한은 Kubernetes 컨트롤 플레인이 Kubernetes 서비스 및 OpenShift 애플리케이션 서비스에서 요청한 로드 밸런서를 동적으로 프로비저닝할 수 있도록 하기 위해 필요합니다.
- `kms` - AWS KMS 키를 읽고, 권한 부여를 생성 및 관리하고 Amazon EC2, 외부에서 사용할 고유한 대칭 데이터 키를 반환합니다 AWS KMS. 클러스터 생성 시 `etcd` 암호화가 활성화된 경우 암호화된 `etcd` 데이터를 사용하는 데 필요합니다.
- `iam` - IAM 역할 및 정책을 검증합니다. 클러스터와 관련된 Amazon EC2 인스턴스 프로파일을 동적으로 프로비저닝하고 관리합니다. `iam:TagInstanceProfile` 권한을 사용하여 IAM 인스턴스 프로파일에 태그를 추가합니다. 고객 지정 클러스터 OIDC 공급자가 누락되어 클러스터 설치에 실패하면 설치 관리자 오류 메시지를 제공합니다.
- `route53` - 클러스터를 생성하는 데 필요한 Route 53 리소스를 관리합니다.
- `servicequotas` - 클러스터를 생성하는 데 필요한 서비스 할당량을 평가합니다.
- `sts` - ROSA 구성 요소에 대한 임시 AWS STS 자격 증명을 생성합니다. 클러스터 생성을 위해 자격 증명을 수임합니다.
- `secretsmanager` - 클러스터 프로비저닝의 일환으로 고객 관리형 OIDC 구성을 안전하게 허용하는 비밀 값을 읽습니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAInstallerPolicy를 참조하세요.

AWS 관리형 정책: ROSASharedVPCRoute53Policy

IAM 엔터티`ROSASharedVPCRoute53Policy`에를 연결할 수 있습니다. ROSA 클러스터가 AWS 서비스 공유 VPC 환경에서 다른를 호출할 수 있도록 하려면이 정책을 IAM 역할에 연결해야 합니다.

이 정책은 ROSA 설치 관리자가 Route 53 레코드를 구성하도록 허용합니다. 이 정책은 공유 VPC에서 사용하기 위한 것이며 공유 VPC 사용 사례에 맞게 조정된 Route 53 권한의 하위 집합을 제공합니다.

권한 세부 정보

이 정책에는 ROSA 설치 관리자가 다음 작업을 완료할 수 있도록 허용하는 다음 권한이 포함되어 있습니다.

- `route53` - DNS 영역 정보와 기존 DNS 레코드를 읽고 현재 DNS 구성을 이해합니다. , , , ,를 포함한 특정 ROSA 관련 도메인 패턴에 대해서만 DNS 레코드`.hypershift.local`,`openshiftapps.com`를 생성`.devshift.org`,`openshiftusgov.com`, 수정 및 삭제합니다`.devshiftusgov.com`. 리소스 관리 및 조직을 위해 Route 53 리소스에 태그를 추가, 수정 또는 제거합니다.
- `tag` - ROSA에서 관리하는 AWS 리소스를 식별하는 데 유용한 태그를 기반으로 리소스를 검색하고 나열합니다.

최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 자세한 내용은 AWS 관리형 정책 참조 안내서의 ROSASharedVPCRoute53Policy를 참조하세요.

AWS 관리형 정책: ROSASharedVPCEndpointPolicy

IAM 엔터티`ROSASharedVPCEndpointPolicy`에를 연결할 수 있습니다. ROSA 클러스터가 AWS 서비스 공유 VPC 환경에서 다른를 호출할 수 있도록 하려면이 정책을 IAM 역할에 연결해야 합니다.

이 정책은 ROSA 설치 관리자가 공유 VPC 환경에서 VPC 엔드포인트 및 보안 그룹을 구성할 수 있도록 허용합니다.

권한 세부 정보

이 정책에는 ROSA 설치 관리자가 다음 작업을 완료할 수 있도록 허용하는 다음 권한이 포함되어 있습니다.

- `ec2` - 네트워크 환경을 이해하기 위해 VPC 엔드포인트, VPCs 관련 리소스를 설명하는 읽기 전용 권한입니다. 태그 기반 제한이 있는 보안 그룹을 생성, 삭제 및 수정하여 ROSA가 클러스터 네트워킹을 위한 보안 그룹을 생성하고 관리하는 동시에 작업을 ROSA 태그가 지정된 리소스로만 제한할 수 있습니다. 태그 기반 제한이 있는 VPC 엔드포인트를 생성, 수정 및 삭제하면 ROSA AWS 서비스 가 공유 VPC 환경에서에 대한 프라이빗 연결을 위해 VPC 엔드포인트를 생성하고 관리할 수 있습니다. 적절한 리소스 식별 및 관리를 위해 새로 생성된 VPC 엔드포인트 및 보안 그룹에 태그를 적용합니다.

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

ROSA와 HCP 운영자 정책

이 섹션에서는 호스팅된 컨트롤 플레인(HCP)이 있는 ROSA에 필요한 운영자 정책에 대한 세부 정보를 제공합니다. 이러한 AWS 관리형 정책을 HCP와 함께 ROSA를 사용하는 데 필요한 운영자 역할에 연

결할 수 있습니다. OpenShift 운영자가 ROSA with HCP 클러스터 노드를 관리할 수 있도록 하려면 권한이 필요합니다.

> **Note**
>
> AWS 관리형 정책은 ROSA에서 호스팅된 컨트롤 플레인(HCP)과 함께 사용하기 위한 것입니다. ROSA 클래식 클러스터는 고객 관리형 IAM 정책을 사용합니다. ROSA 클래식 정책에 대한 자세한 내용은 the section called “ROSA 클래식 계정 정책” 및 섹션을 참조하세요the section called “ROSA 클래식 연산자 정책”.

AWS 관리형 정책: ROSAAmazonEBSCSIDriverOperatorPolicy

IAM 엔터티ROSAAmazonEBSCSIDriverOperatorPolicy에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다 AWS 서비스. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 ROSA 클러스터에 Amazon EBS CSI 드라이버를 설치하고 유지 관리하는 데 필요한 권한을 Amazon EBS CSI 드라이버 운영자에게 부여합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서에서 aws-ebs-csi-driver 운영자를 참조하세요.

권한 세부 정보

이 정책에는 Amazon EBS 드라이버 운영자가 다음 작업을 완료할 수 있도록 허용하는 다음 권한이 포함되어 있습니다.

- ec2 - Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨을 생성, 수정, 연결, 분리 및 삭제합니다. Amazon EBS 볼륨 스냅샷을 생성 및 삭제하고 Amazon EC2 인스턴스, 볼륨 및 스냅샷을 나열합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAAmazonEBSCSIDriverOperatorPolicy를 참조하세요.

AWS 관리형 정책: ROSAIngressOperatorPolicy

IAM 엔터티ROSAIngressOperatorPolicy에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다 AWS 서비스. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 수신 연산자에게 ROSA 클러스터에 대한 로드 밸런서 및 DNS 구성을 프로비저닝하고 관리하는 데 필요한 권한을 부여합니다. 이 정책은 태그 값에 대한 읽기 액세스를 허용합니다. 그런 다음 연산자는 Route 53 리소스의 태그 값을 필터링하여 호스팅 영역을 검색합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서에서 OpenShift 수신 운영자를 참조하세요.

권한 세부 정보

이 정책에는 수신 운영자가 다음 태스크를 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- `elasticloadbalancing` - 프로비저닝된 로드 밸런서의 상태를 설명합니다.
- `route53` - ROSA 클러스터에서 제어하는 DNS를 관리하는 Route 53 호스팅 영역을 나열하고 레코드를 편집합니다.
- `tag` - `tag:GetResources` 권한을 사용하여 태그가 지정된 리소스를 관리합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAIngressOperatorPolicy를 참조하세요.

AWS 관리형 정책: ROSAImageRegistryOperatorPolicy

IAM 엔터티ROSAImageRegistryOperatorPolicy에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다 AWS 서비스. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 Image Registry Operator에 클러스터 ROSA 내 이미지 레지스트리 및 S3를 포함한 종속 서비스에 대한 리소스를 프로비저닝하고 관리하는 데 필요한 권한을 부여합니다. 이는 운영자가 ROSA 클러스터의 내부 레지스트리를 설치하고 유지 관리하기 위해 필요합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서에서 이미지 레지스트리 운영자를 참조하세요.

권한 세부 정보

이 정책에는 이미지 레지스트리 운영자가 다음 동작을 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- `s3` - Amazon S3 버킷을 컨테이너 이미지 콘텐츠 및 클러스터 메타데이터의 영구 스토리지로 관리하고 평가합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAImageRegistryOperatorPolicy를 참조하세요.

AWS 관리형 정책: ROSACloudNetworkConfigOperatorPolicy

IAM 엔터티ROSACloudNetworkConfigOperatorPolicy에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다 AWS 서비스. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 ROSA 클러스터 네트워킹 오버레이에 대한 네트워킹 리소스를 프로비저닝하고 관리하는 데 필요한 권한을 Cloud Network Config Controller Operator에 부여합니다. 운영자는 이러한 권한을 사용하여 ROSA 클러스터의 일부로 Amazon EC2 인스턴스의 프라이빗 IP 주소를 관리합니다. 운영자에 대한 자세한 내용은 OpenShift GitHub 설명서에서 Cloud-network-config-controller를 참조하세요.

권한 세부 정보

이 정책에는 클라우드 네트워크 구성 컨트롤러 운영자가 다음 태스크를 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- ec2 - ROSA 클러스터에서 Amazon EC2 인스턴스, Amazon VPC 서브넷 및 탄력적 네트워크 인터페이스를 연결하기 위한 구성을 읽고 할당하고 설명합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSACloudNetworkConfigOperatorPolicy를 참조하세요.

AWS 관리형 정책: ROSAKubeControllerPolicy

IAM 엔터티ROSAKubeControllerPolicy에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다 AWS 서비스. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 kube 컨트롤러에 필요한 관리 권한 Amazon EC2 Elastic Load Balancing과 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA에 대한 AWS KMS 리소스를 부여합니다. 이 컨트롤러에 대한 자세한 내용은 OpenShift 설명서의 컨트롤러 아키텍처를 참조하세요.

권한 세부 정보

이 정책에는 kube 컨트롤러가 다음 태스크를 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- ec2 - Amazon EC2 인스턴스 보안 그룹에 태그를 생성, 삭제 및 추가합니다. 인바운드 규칙을 보안 그룹에 추가합니다. 가용 영역, Amazon EC2 인스턴스, 라우팅 테이블, 보안 그룹, VPC, 서브넷을 설명합니다.

- `elasticloadbalancing` - 로드 밸런서 및 해당 정책을 생성하고 관리합니다. 로드 밸런서 리스너를 생성하고 관리합니다. 대상 그룹에 대상을 등록 및 등록 취소하고 대상 그룹을 관리합니다. 로드 밸런서에 Amazon EC2 인스턴스를 등록 및 등록 취소하고 로드 밸런서에 태그를 추가합니다.
- `kms` - AWS KMS 키에 대한 세부 정보를 검색합니다. 클러스터 생성 시 `etcd` 암호화가 활성화된 경우 암호화된 `etcd` 데이터를 사용하는 데 필요합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAKubeControllerPolicy를 참조하세요.

AWS 관리형 정책: ROSANodePoolManagementPolicy

IAM 엔터티`ROSANodePoolManagementPolicy`에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른 AWS 서비스를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 작업자 노드로 관리되는 Amazon EC2 인스턴스를 설명, 실행 및 종료하는 데 필요한 권한을 NodePool 컨트롤러에 부여합니다. 또한이 정책은 AWS KMS 키를 사용하여 작업자 노드 루트 볼륨의 디스크 암호화를 허용하고, 작업자 노드에 연결된 탄력적 네트워크 인터페이스에 태그를 지정하고, Amazon EC2 용량 예약에 액세스할 수 있는 권한을 부여합니다. 이 컨트롤러에 대한 자세한 내용은 OpenShift 설명서의 컨트롤러 아키텍처를 참조하세요.

권한 세부 정보

이 정책에는 노드 풀 컨트롤러가 다음 태스크를 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- `ec2` - Red Hat에서 AWS 계정 소유하고 관리하는에서 호스팅되는 AMIs 사용하여 Amazon EC2 인스턴스를 실행합니다. ROSA 클러스터에서 EC2 수명 주기를 관리합니다. 작업자 노드를 동적으로 생성하고 Elastic Load Balancing Amazon VPC, Route 53 Amazon EBS, 및와 통합합니다 Amazon EC2. ROSA의 용량 예약 기능을 지원하기 위해 용량 예약에 액세스하고 설명합니다.
- `iam` - 라는 서비스 연결 역할을 Elastic Load Balancing 통해를 사용합니다`AWSServiceRoleForElasticLoadBalancing`. Amazon EC2 인스턴스 프로파일에 역할을 할당합니다.
- `kms` - AWS KMS 키를 읽고, 권한 부여를 생성 및 관리하고 Amazon EC2, 외부에서 사용할 고유한 대칭 데이터 키를 반환합니다 AWS KMS. 워커 노드 루트 볼륨의 디스크 암호화를 허용하는 데 필요합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSANodePoolManagementPolicy를 참조하세요.

AWS 관리형 정책: ROSAKMSProviderPolicy

IAM 엔터티ROSAKMSProviderPolicy에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다 AWS 서비스. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 etcd 데이터 암호화를 지원하는 AWS KMS 키를 관리하는 데 필요한 권한을 기본 제공 AWS 암호화 공급자에게 부여합니다. 이 정책은 Amazon EC2 가 AWS 암호화 공급자가 etcd 데이터를 암호화하고 해독하기 위해 제공하는 KMS 키를 사용하도록 허용합니다. 이 제공자에 대한 자세한 내용은 Kubernetes GitHub 설명서의 AWS 암호화 공급자를 참조하세요.

권한 세부 정보

이 정책에는 AWS 암호화 공급자가 다음 작업을 완료할 수 있도록 허용하는 다음 권한이 포함되어 있습니다.

- kms - AWS KMS 키를 암호화, 복호화 및 검색합니다. 클러스터 생성 시 etcd 암호화가 활성화된 경우 암호화된 etcd 데이터를 사용하는 데 필요합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAKMSProviderPolicy를 참조하세요.

AWS 관리형 정책: ROSAControlPlaneOperatorPolicy

IAM 엔터티ROSAControlPlaneOperatorPolicy에를 연결할 수 있습니다. 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA가 다른를 호출할 수 있도록 하려면이 정책을 운영자 IAM 역할에 연결해야 합니다 AWS 서비스. 각 클러스터에는 고유한 운영자 역할 집합이 필요합니다.

이 정책은 컨트롤 플레인 운영자에 호스팅된 컨트롤 플레인 클러스터가 있는 ROSA에 대한 Amazon EC2 및 Route 53 리소스를 관리하는 데 필요한 권한을 부여합니다. 이 운영자에 대한 자세한 내용은 OpenShift 설명서의 컨트롤러 아키텍처를 참조하세요.

권한 세부 정보

이 정책에는 컨트롤 플레인 운영자가 다음 태스크를 완료할 수 있도록 허용하는 다음과 같은 권한이 포함되어 있습니다.

- ec2 - Amazon VPC 엔드포인트를 생성하고 관리합니다.

- `route53` - Route 53 레코드 세트를 나열 및 변경하고 호스팅 영역을 나열합니다.
- RedHatManagedSecurityGroups에 태그 추가: 생성 후 컨트롤 플레인 운영자가 Red Hat 관리형 보안 그룹에 태그를 지정할 수 있습니다. 이는 적절한 리소스 수명 주기 관리 및 HCP 클러스터를 사용한 ROSA와 관련된 보안 그룹 정리에 필요합니다.
- ManageVPCEndpointWithCondition에 security-group/* 추가: 클러스터 업그레이드 중에 VPCE 조정 실패를 수정합니다. 운영자는 보안 그룹을 참조하는 VPC 엔드포인트를 수정할 수 있는 권한이 필요합니다.

전체 JSON 정책 문서를 보려면 AWS 관리형 정책 참조 안내서의 ROSAControlPlaneOperatorPolicy를 참조하세요.

ROSA AWS 관리형 정책에 대한 업데이트

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

변경	설명	Date
ROSAControlPlaneOperatorPolicy - 정책 업데이트	ROSA는 적절한 리소스 수명 주기 관리를 위해 Red Hat 관리형 보안 그룹의 태그 지정을 허용하고 ManageVPCEndpointWithCondition에 security-group/*를 추가하여 클러스터 업그레이드 중에 VPCE 조정 실패를 수정하도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAControlPlaneOperatorPolicy”를 참조하세요.	2026년 4월 9일
ROSAKubeControllerPolicy - 정책 업데이트	ROSA는 대상 그룹에 대상을 등록 및 등록 취소하기 위한 Elastic Load Balancing 권한을 명확히 하기 위해 정책을 업데	2026년 3월 5일

변경	설명	Date
	이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAKubeControllerPolicy”를 참조하세요.	
ROSANodePoolManagementPolicy - 정책 업데이트	ROSA는 Amazon EC2 용량 예약에 대한 리소스 액세스를 추가하도록 정책을 업데이트했습니다. 이 변경 사항을 통해 NodePool 컨트롤러는 향상된 리소스 관리를 위해 용량 예약에 액세스하고 설명할 수 있습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSANodePoolManagementPolicy”를 참조하세요.	2025년 9월 3일
ROSASharedVPCEndpointPolicy - 새 정책 추가	ROSA는 ROSA 설치 관리자가 공유 VPC 환경에서 VPC 엔드포인트 및 보안 그룹을 구성할 수 있도록 허용하는 새 정책을 추가했습니다. 이 정책은 공유 VPC 사용 사례에 맞게 조정된 EC2 권한의 하위 집합을 제공합니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSASharedVPCEndpointPolicy”를 참조하세요.	2025년 8월 7일

변경	설명	Date
ROSASharedVPCRoute53Policy - 새 정책 추가	ROSA는 ROSA 설치 관리자가 공유 VPC 환경에서 Route 53 레코드를 구성할 수 있도록 허용하는 새 정책을 추가했습니다. 이 정책은 공유 VPC 사용 사례에 맞게 조정된 Route 53 권한의 하위 집합을 제공합니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSASharedVPCRoute53Policy”를 참조하세요.	2025년 8월 7일
ROSAInstallerPolicy - 정책 업데이트	ROSA는 설치 ROSA 관리자가 ROSA의 새로운 용량 예약 기능을 지원하기 위해 Amazon EC2 용량 예약을 검사할 수 있도록 정책을 업데이트했습니다. 또한이 업데이트를 통해 설치 관리자는 향상된 Kubernetes 클러스터 태그 관리를 `"kubernetes.io/cluster/*"` 위해 태그 키 일치를 사용하여 서브넷의 태그를 삭제할 수 있습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAInstallerPolicy”를 참조하세요.	2025년 8월 7일

변경	설명	Date
ROSAImageRegistryOperatorPolicy - 정책 업데이트	ROSA는 권한이 S3 버킷 리소스 수준으로 범위가 축소되도록 정책을 업데이트했습니다. 이 변경 사항은 AWS 상용 및 GovCloud 리전 모두에 대한 ROSA 스토리지 요구 사항을 충족합니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAImageRegistryOperatorPolicy”를 참조하세요.	2025년 5월 19일
ROSANodePoolManagementPolicy - 정책 업데이트	ROSA는 작업자 노드에 연결된 탄력적 네트워크 인터페이스의 태그 지정을 허용하도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSANodePoolManagementPolicy”를 참조하세요.	2025년 5월 5일
ROSAImageRegistryOperatorPolicy - 정책 업데이트	ROSA는 Red Hat OpenShift Image Registry Operator가 ROSA 클러스터 내 이미지 레지스트리에서 사용할 Amazon S3 버킷 및 객체를 AWS GovCloud 리전에서 프로비저닝하고 관리할 수 있도록 정책을 업데이트했습니다. 이 변경 사항은 AWS GovCloud 리전에 대한 ROSA 스토리지 요구 사항을 충족합니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAImageRegistryOperatorPolicy”를 참조하세요.	2025년 4월 16일

변경	설명	Date
ROSAWorkerInstancePolicy - 정책 업데이트	ROSA는 작업자 노드가 클러스터 설치 및 작업자 노드 수명 주기 관리에 필요한 ROSA 관리형 ECR 리포지토리에서 이미지를 평가하고 가져올 수 있도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAWorkerInstancePolicy”를 참조하세요.	2025년 3월 3일
ROSANodePoolManagementPolicy - 정책 업데이트	ROSA는 요청에 태그가 포함된 경우 ecEC2:RunInstances 호출 중에만 EC2 인스턴스와 유사하게 탄력적 네트워크 인터페이스에 태그를 지정할 수 있도록 정책을 업데이트했습니다`red-hat-managed: true` . 이러한 권한은 HCP 4.17 클러스터에서 ROSA를 지원하는 데 필요합니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSANodePoolManagementPolicy”를 참조하세요.	2025년 2월 24일
ROSAAmazonEBSCSIDriverOperatorPolicy - 정책 업데이트	ROSA는 새 Amazon EBS 스냅샷 권한 부여 API를 지원하도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAAmazonEBSCSIDriverOperatorPolicy”를 참조하세요.	2025년 1월 17일

변경	설명	Date
ROSANodePoolManagementPolicy - 정책 업데이트	ROSA는 적절한 프라이빗 DNS 이름을 설정하기 위해 ROSA 노드 풀 관리자가 DHCP 옵션 세트를 설명할 수 있도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSANodePoolManagementPolicy”를 참조하세요.	2024년 5월 2일
ROSAInstallerPolicy - 정책 업데이트	ROSA는 ROSA 설치 관리자가 일치하는 태그 키를 사용하여 서브넷에 태그를 추가할 수 있도록 정책을 업데이트했습니다`"kubernetes.io/cluster/*"` . 자세한 내용은 the section called “AWS 관리형 정책: ROSAInstallerPolicy”를 참조하세요.	2024년 4월 24일
ROSASRESupportPolicy - 정책 업데이트	ROSA는 SRE 역할이에서 ROSA 로 태그가 지정된 인스턴스 프로파일에 대한 정보를 검색할 수 있도록 정책을 업데이트했습니다`red-hat-managed` . 자세한 내용은 the section called “AWS 관리형 정책: ROSASRESupportPolicy”를 참조하세요.	2024년 4월 10일

변경	설명	Date
ROSAInstallerPolicy - 정책 업데이트	ROSA는 ROSA 설치 관리자가에 대한 AWS 관리형 정책 ROSA 이에서 사용하는 IAM 역할에 연결되어 있는지 확인할 수 있도록 정책을 업데이트했습니다 ROSA. 또한이 업데이트를 통해 설치 관리자는 고객 관리형 정책이 ROSA 역할에 연결되었는지 여부를 식별할 수 있습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAInstallerPolicy”를 참조하세요.	2024년 4월 10일
ROSAInstallerPolicy - 정책 업데이트	ROSA는 고객이 지정한 클러스터 OIDC 공급자 누락으로 인해 클러스터 설치에 실패할 때 서비스가 설치 관리자 알림 메시지를 제공할 수 있도록 정책을 업데이트했습니다. 또한이 업데이트를 통해 서비스는 기존 DNS 이름 서버를 검색하여 클러스터 프로비저닝 작업이 멱등성을 갖도록 할 수 있습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAInstallerPolicy”를 참조하세요.	2024년 1월 26일

변경	설명	Date
ROSASRESupportPolicy - 정책 업데이트	ROSA 는 서비스가 DescribeSecurityGroups API를 사용하여 보안 그룹에 대한 읽기 작업을 수행할 수 있도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSASRESupportPolicy”를 참조하세요.	2024년 1월 22일
ROSAImageRegistryOperatorPolicy - 정책 업데이트	ROSA 는 Image Registry Operator가 14자 이름을 가진 리전의 Amazon S3 버킷에 대해 작업을 수행할 수 있도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAImageRegistryOperatorPolicy”를 참조하세요.	2023년 12월 12일
ROSAKubeControllerPolicy - 정책 업데이트	ROSA 는 kube-controller-manager가 가용 영역, Amazon EC2 인스턴스, 라우팅 테이블, 보안 그룹, VPCs 및 서브넷을 설명할 수 있도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAKubeControllerPolicy”를 참조하세요.	2023년 10월 16일

변경	설명	Date
ROSAManageSubscription - 정책 업데이트	ROSA 는 호스팅된 컨트롤 플레인 ProductId가 있는 ROSA를 추가하도록 정책을 업데이트했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAManageSubscription”를 참조하세요.	2023년 8월 1일
ROSAKubeControllerPolicy - 정책 업데이트	ROSA 는 kube-controller-manager가 Network Load Balancer를 Kubernetes 서비스 로드 밸런서로 생성할 수 있도록 정책을 업데이트했습니다. Network Load Balancer는 변동성이 큰 워크로드를 처리하고 로드 밸런서에 고정 IP 주소를 지원할 수 있는 강력한 기능을 제공합니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAKubeControllerPolicy”를 참조하세요.	2023년 7월 13일
ROSANodePoolManagementPolicy - 새 정책 추가	ROSA 는 NodePool 컨트롤러가 작업자 노드로 관리되는 Amazon EC2 인스턴스를 설명, 실행 및 종료할 수 있도록 허용하는 새 정책을 추가했습니다. 또한이 정책은 AWS KMS 키를 사용하여 작업자 노드 루트 볼륨의 디스크 암호화를 활성화합니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSANodePoolManagementPolicy”를 참조하세요.	2023년 6월 8일

변경	설명	Date
ROSAInstallerPolicy - 새 정책 추가됨	ROSA 는 설치 관리자가 클러스터 설치를 지원하는 AWS 리소스를 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAInstallerPolicy”를 참조하세요.	2023년 6월 6일
ROSASRESupportPolicy - 새 정책 추가	ROSA 는 Red Hat SREs ROSA 클러스터 노드 상태를 변경하는 기능을 포함하여 ROSA 클러스터와 연결된 AWS 리소스를 직접 관찰, 진단 및 지원할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSASRESupportPolicy”를 참조하세요.	2023년 6월 1일
ROSAKMSProviderPolicy - 새 정책 추가	ROSA 는 내장 AWS 암호화 공급자가 etcd 데이터 암호화를 지원하는 AWS KMS 키를 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAKMSProviderPolicy”를 참조하세요.	2023년 4월 27일

변경	설명	Date
ROSAKubeControllerPolicy - 새 정책 추가	ROSA 는 kube 컨트롤러가 및 호스팅된 컨트롤 플레인 클러스터가 ROSA 있는의 Amazon EC2 Elastic Load Balancing AWS KMS 리소스를 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAKubeControllerPolicy”를 참조하세요.	2023년 4월 27일
ROSAImageRegistryOperatorPolicy - 새 정책 추가	ROSA 는 Image Registry Operator가 클러스터 ROSA 내 이미지 레지스트리 및 S3를 포함한 종속 서비스에 대한 리소스를 프로비저닝하고 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAImageRegistryOperatorPolicy”를 참조하세요.	2023년 4월 27일
ROSAControlPlaneOperatorPolicy - 새 정책 추가	ROSA 는 컨트롤 플레인 운영자가 호스팅된 컨트롤 플레인 클러스터를 ROSA 사용하여에 대한 Amazon EC2 및 Route 53 리소스를 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAControlPlaneOperatorPolicy”를 참조하세요.	2023년 4월 24일

변경	설명	Date
ROSACloudNetworkConfigOperatorPolicy - 새 정책 추가	ROSA 는 Cloud Network Config Controller Operator가 ROSA 클러스터 네트워킹 오버레이에 대한 네트워킹 리소스를 프로비저닝하고 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSACloudNetworkConfigOperatorPolicy”를 참조하세요.	2023년 4월 20일
ROSAIngressOperatorPolicy - 새 정책 추가	ROSA 는 수신 운영자가 ROSA 클러스터에 대한 로드 밸런서 및 DNS 구성을 프로비저닝하고 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAIngressOperatorPolicy”를 참조하세요.	2023년 4월 20일
ROSAAmazonEBSCSIDriverOperatorPolicy - 새 정책이 추가됨	ROSA 는 Amazon EBS CSI 드라이버 운영자가 ROSA 클러스터에 Amazon EBS CSI 드라이버를 설치하고 유지 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAAmazonEBSCSIDriverOperatorPolicy”를 참조하세요.	2023년 4월 20일

변경	설명	Date
ROSAWorkerInstancePolicy - 새 정책 추가	ROSA 는 서비스가 클러스터 리소스를 관리할 수 있도록 허용하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAWorkerInstancePolicy”를 참조하세요.	2023년 4월 20일
ROSAManageSubscription - 새 정책 추가	ROSA 는 ROSA 구독을 관리하는 데 필요한 AWS Marketplace 권한을 부여하는 새 정책을 추가했습니다. 자세한 내용은 the section called “AWS 관리형 정책: ROSAManageSubscription”를 참조하세요.	2022년 4월 11일
Red Hat OpenShift Service on AWS 에서 변경 내용 추적 시작	Red Hat OpenShift Service on AWS 가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2022년 3월 2일

ROSA 자격 증명 및 액세스 문제 해결

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

AWS Organizations 서비스 제어 정책에서 필요한 AWS Marketplace 권한 거부

활성화를 시도할 때 AWS Organizations 서비스 제어 정책(SCP)이 필요한 AWS Marketplace 구독 권한을 허용하지 않는 경우 ROSA다음 콘솔 오류가 발생합니다.

```
An error occurred while enabling ROSA, because a service control policy (SCP) is
 denying required permissions. Contact your management account administrator, and
 consult the documentation for troubleshooting.
```

이 오류가 발생하면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 조직의 계정을 관리하는 사람입니다. 해당 사용자에게 다음을 수행하도록 요청합니다.

1. `aws-marketplace:Subscribe`, `aws-marketplace:Unsubscribe`및 `aws-marketplace:ViewSubscriptions` 권한을 허용하도록 SCP를 구성합니다. 자세한 내용은 AWS Organizations 사용 설명서의 SCP 업데이트를 참조하세요.
2. 조직의 관리 계정 ROSA 에서를 활성화합니다.
3. 조직 내에서 액세스가 필요한 멤버 계정에 ROSA 구독을 공유합니다. 자세한 내용은 AWS Marketplace 구매자 안내서의 조직에서 구독 공유를 참조하세요.

사용자 또는 역할에 필요한 AWS Marketplace 권한이 없음

활성화를 시도할 때 보안 IAM 주체에 필요한 AWS Marketplace 구독 권한이 없는 경우 ROSA다음 콘솔 오류가 발생합니다.

```
An error occurred while enabling ROSA, because your user or role does not have the
 required permissions.
```

이 문제를 해결하려면 다음 단계에 따릅니다.

1. IAM 콘솔로 이동하여 AWS 관리형 정책을 IAM 자격 증명`ROSAManageSubscription`에 연결합니다. 자세한 내용은 AWS 관리형 정책 참조 안내서의 ROSAManageSubscription을 참조하세요.
2. the section called “AWS 사전 조건 활성화 ROSA 및 구성”의 프로시저를 따르세요.

에서 권한 세트를 보거나 업데이트할 권한이 IAM 없거나 오류가 발생하는 경우 관리자에게 문의하여 도움을 받아야 합니다. 그 사람에게 자격 IAM 증명`ROSAManageSubscription`에 연결하고의 절차를 따르도록 요청합니다the section called “AWS 사전 조건 활성화 ROSA 및 구성”. 관리자가이 작업을 수행하면 아래의 모든 자격 증명에 대한 권한 세트를 업데이트 ROSA 하여 IAM 를 활성화합니다 AWS 계정.

관리자가 차단한 필수 AWS Marketplace 권한

계정 관리자가 필요한 AWS Marketplace 구독 권한을 차단한 경우 활성화를 시도할 때 다음 콘솔 오류가 발생합니다 ROSA.

```
An error occurred while enabling ROSA because required permissions have been blocked by
 an administrator. ROSAManageSubscription includes the permissions required to enable
 ROSA. Consult the documentation and try again.
```

이 오류가 발생하면 관리자에게 문의하여 도움을 받아야 합니다. 해당 사용자에게 다음을 수행하도록 요청합니다.

1. ROSA 콘솔로 이동하여 AWS 관리형 정책을 IAM 자격 증명ROSAManageSubscription에 연결합니다. 자세한 내용은 AWS 관리형 정책 참조 안내서의 ROSAManageSubscription을 참조하세요.
2. 의 절차에 따라 the section called “AWS 사전 조건 활성화 ROSA 및 구성”를 활성화합니다 ROSA. 이 절차는 아래의 모든 자격 증명에 대한 권한 세트를 업데이트 ROSA 하여 IAM 를 활성화합니다 AWS 계정.

로드 밸런서 생성 오류: AccessDenied

로드 밸런서를 생성하지 않은 경우 계정에 AWSServiceRoleForElasticLoadBalacing 서비스 연결 역할이 없을 수 있습니다. 계정에 AWSServiceRoleForElasticLoadBalacing 역할 클러스터 없이 ROSA 를 생성하려고 하면 다음 오류가 발생합니다.

```
Error creating network Load Balancer: AccessDenied
```

이 문제를 해결하려면 다음 단계에 따릅니다.

1. 계정에 AWSServiceRoleForElasticLoadBalancing 역할이 있는지 확인하세요.

   ```
   aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing"
   ```

2. 이 역할이 없는 경우 지침에 따라 Elastic Load Balancing 사용 설명서의 서비스 연결 역할 생성에 있는 역할을 생성합니다.

의 복원력 ROSA

AWS 글로벌 인프라 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹을 통해 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극

복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

ROSA 는 단일 AWS 가용 영역 또는 여러 가용 영역에서 Kubernetes 컨트롤 플레인 및 데이터 플레인을 실행할 수 있는 옵션을 고객에게 제공합니다. 단일 AZ 클러스터는 실험 목적에 유용할 수 있지만, 고객은 둘 이상의 가용 영역에서 워크로드를 실행하는 것이 좋습니다. 그러면 애플리케이션은 완전한 가용 영역 장애 상황(아주 드문 경우)도 견딜 수 있습니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

ROSA 클러스터 복원력

ROSA 컨트롤 플레인은 최소 3개의 OpenShift 컨트롤 플레인 노드로 구성됩니다. 각 컨트롤 플레인 노드는 API 서버 인스턴스, `etcd` 인스턴스, 컨트롤러로 구성됩니다. 컨트롤 플레인 노드에 장애가 발생하는 경우 클러스터 가용성을 보장하기 위해 모든 API 요청이 사용 가능한 다른 노드로 자동 라우팅됩니다.

ROSA 데이터 영역은 최소 2개의 OpenShift 인프라 노드와 2개의 OpenShift 작업자 노드로 구성됩니다. 인프라 노드는 기본 라우터, 기본 제공 OpenShift 레지스트리, 클러스터 메트릭 및 모니터링 목적의 구성 요소 등 OpenShift 클러스터 인프라 구성 요소를 지원하는 포드를 실행합니다. OpenShift 워커 노드는 최종 사용자 애플리케이션 포드를 실행합니다.

Red Hat 사이트 신뢰성 엔지니어(SRE) 는 컨트롤 플레인 및 인프라 노드를 모두 관리합니다. Red Hat SREs ROSA 클러스터를 사전에 모니터링하고 장애가 발생한 컨트롤 플레인 노드 및 인프라 노드를 교체할 책임이 있습니다. 자세한 내용은 the section called “책임” 단원을 참조하십시오.

> **Important**
>
> ROSA 는 관리형 서비스이므로 Red Hat은가 ROSA 사용하는 기본 AWS 인프라를 관리할 책임이 있습니다. 고객은 AWS 콘솔 또는에서를 ROSA 사용하는 Amazon EC2 인스턴스를 수동으로 종료하려고 해서는 안 됩니다 AWS CLI. 이 작업은 고객 데이터 손실로 이어질 수 있습니다.

데이터 영역에서 워커 노드에 장애가 발생할 경우, 컨트롤 플레인은 장애가 발생한 노드가 복구되거나 교체될 때까지 예정되지 않은 포드를 작동이 원활한 워커 노드로 재배치합니다. 클러스터 내 시스템의 자동 규모 조정을 활성화하면 장애가 발생한 워커 노드를 수동 또는 자동으로 교체할 수 있습니다. 자세한 내용은 Red Hat 설명서에서 클러스터 자동 규모 조정을 참조하세요.

고객 배포 애플리케이션 복원력

ROSA 는 서비스의 고가용성을 보장하기 위해 많은 보호를 제공하지만 고객은 워크로드를 가동 중지 시간으로부터 보호하기 위해 고가용성을 위해 배포된 애플리케이션을 구축할 책임이 있습니다. 가용 영역에 대한 자세한 내용은 Red Hat 설명서의 ROSA가용성 정보를 참조하세요.

의 인프라 보안 ROSA

관리형 서비스인 Red Hat OpenShift Service on AWS 는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙의 인프라 보호 - Well-Architected Framework를 참조하세요. AWS

AWS 에서 게시한 API 호출을 사용하여 AWS 네트워크를 ROSA 통해에 액세스합니다. 클라이언트는 다음을 지원해야 합니다.

- Transport Layer Security(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 시크릿 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

클러스터 네트워크 격리

Red Hat 사이트 신뢰성 엔지니어(SRE) 는 클러스터 및 기반 애플리케이션 플랫폼의 지속적인 관리 및 네트워크 보안을 담당합니다. 에 대한 Red Hat 책임에 대한 자세한 내용은 섹션을 ROSA참조하세요the section called “책임”.

새 클러스터를 생성할 때는 퍼블릭 Kubernetes API 서버 엔드포인트 및 애플리케이션 경로 또는 프라이빗 Kubernetes API 엔드포인트 및 애플리케이션 경로를 생성하는 옵션을 ROSA 제공합니다. 이 연결은 클러스터와 통신하는 데 사용됩니다(ROSA CLI 및 OpenShift CLI와 같은 OpenShift 관리 도구 사용). 프라이빗 연결을 통해 노드와 API 서버 간의 모든 통신이 VPC 내에 유지될 수 있습니다. API 서버 및 애플리케이션 경로에 대한 프라이빗 액세스를 활성화하는 경우 기존 VPC 및를 사용하여 VPC AWS PrivateLink 를 OpenShift 백엔드 서비스에 연결해야 합니다.

Kubernetes API 서버 액세스는 AWS Identity and Access Management (IAM)와 네이티브 Kubernetes 역할 기반 액세스 제어(RBAC)의 조합을 사용하여 보호됩니다. 자세한 내용은 Kubernetes 문서의 RBAC 승인 사용을 참조하십시오.

ROSA 를 사용하면 여러 유형의 TLS 종료를 사용하여 보안 애플리케이션 경로를 생성하여 클라이언트에 인증서를 제공할 수 있습니다. 자세한 내용은 Red Hat 설명서에서 보안 경로를 참조하세요.

기존 VPC에서 ROSA 클러스터를 생성하는 경우 클러스터에서 사용할 VPC 서브넷 및 가용 영역을 지정합니다. 또한 클러스터 네트워크에서 사용할 CIDR 범위를 정의하고 이러한 CIDR 범위를 VPC 서브넷과 맞춥니다. 자세한 내용은 Red Hat 설명서에서 CIDR 범위 정의를 참조하세요.

퍼블릭 API 엔드포인트를 사용하는 클러스터의 경우는 클러스터를 배포할 각 가용 영역에 대해 퍼블릭 및 프라이빗 서브넷으로 VPC를 구성 ROSA 해야 합니다. 프라이빗 API 엔드포인트를 사용하는 클러스터의 경우 프라이빗 서브넷만 필요합니다.

기존 VPC를 사용하는 경우 ROSA 클러스터 생성 중 또는 이후에 HTTP 또는 HTTPS 프록시 서버를 사용하여 클러스터 웹 트래픽을 암호화하도록 클러스터를 구성하여 데이터에 대한 또 다른 보안 계층을 추가할 수 있습니다. 프록시를 활성화하면 핵심 클러스터 구성 요소에서 인터넷에 직접 액세스할 수 없게 됩니다. 인터넷의 사용자 워크로드 인터넷 액세스는 프록시에서 거부되지 않습니다. 자세한 내용은 Red Hat 설명서에서 클러스터 전체 프록시 구성을 참조하세요.

포드 네트워크 격리

클러스터 관리자인 경우 트래픽을 ROSA 클러스터의 포드로 제한하는 포드 수준에서 네트워크 정책을 정의할 수 있습니다.

ROSA 서비스 할당량

Red Hat OpenShift Service on AWS (ROSA)는 Amazon EC2및에 대한 서비스 할당량을 사용하여 클러스터 Amazon Virtual Private Cloud Amazon Elastic Block Store Elastic Load Balancing 를 프로비저닝합니다. 자세한 내용은 AWS 일반 참조 안내서의 Red Hat OpenShift Service on AWS 엔드포인트 및 할당량을 참조하세요.

AWS 와 통합된 서비스 ROSA

ROSA 는 다른와 협력하여 비즈니스 과제 AWS 서비스 에 대한 추가 솔루션을 제공합니다. 이 주제에서는가 기능을 추가하는 ROSA 데 사용하는 서비스 또는가 작업을 수행하는 데 ROSA 사용하는 서비스를 식별합니다.

주제

- 에서를 ROSA 사용하는 방법 AWS Marketplace

에서를 ROSA 사용하는 방법 AWS Marketplace

AWS Marketplace 는 솔루션을 구축하고 비즈니스를 운영하는 데 필요한 타사 소프트웨어, 데이터 및 서비스를 찾고, 구매하고, 배포하고, 관리하는 데 사용할 수 있는 엄선된 디지털 카탈로그입니다.는 유연한 요금 옵션과 여러 배포 방법을 사용하여 소프트웨어 라이선스 및 조달을 간소화 AWS Marketplace 합니다.

ROSA 는 서비스 측정 및 결제 AWS Marketplace 에 사용합니다. ROSA 클래식은 AWS Marketplace Amazon Machine Image(AMI) 기반 제품을 통해 측정 및 청구되는 반면, 호스팅 컨트롤 플레인(HCP)이 있는 ROSA는 서비스형 AWS Marketplace 소프트웨어(SaaS) 기반 제품을 통해 측정 및 청구됩니다.

이 페이지에서는 결제, 결제, 구독 및 계약 구매를 AWS Marketplace 위해에서를 ROSA 사용하는 방법을 설명합니다.

용어

이 페이지에서는 ROSA와 ROSA의 통합을 논의할 때 다음 용어를 사용합니다 AWS Marketplace.

Amazon Machine Image(AMI)

AWS에서 실행되는 운영 체제 및 추가 소프트웨어를 포함한 서버의 이미지입니다.

AMI 구독

에서 ROSA 클래식과 같은 AWS Marketplace AMI 기반 소프트웨어 제품은 연간 구독 요금 모델과 함께 시간당를 사용합니다. 시간당 요금은 기본 요금 모델이지만 한 Amazon EC2 인스턴스 유형에 대해 연간 사용량을 미리 구매할 수 있습니다.

SaaS 구독

에서 ROSA with HCP와 같은 서비스형 AWS Marketplace소프트웨어(SaaS) 제품은 사용량 기반 구독 모델을 채택합니다. software-as-a-service 소프트웨어 판매자가 사용량을 추적하고, 고객은 사용한 만큼 요금을 지불합니다.

공개 제안

공개 제안을 통해에서 직접 AWS Marketplace 소프트웨어 및 서비스를 구매할 수 있습니다 AWS Management Console.

비공개 제안

비공개 제안은 판매자와 구매자가에서 구매에 대한 사용자 지정 가격 및 최종 사용자 라이선스 계약(EULA) 조건을 협상할 수 있는 구매 프로그램입니다 AWS Marketplace.

ROSA 서비스 수수료

Red Hat 사이트 신뢰성 엔지니어(SREs)가 OpenShift 소프트웨어 및 클러스터 관리에 ROSA 부과하는 요금입니다. ROSA 서비스 요금은를 통해 측정되고 AWS 청구서에 AWS Marketplace 표시됩니다.

AWS 인프라 수수료

Amazon EC2 Amazon EBS Amazon S3및를 포함하여 AWS 서비스 기본 ROSA 클러스터에 대해 AWS 요금을 부과하는 표준 요금입니다 Elastic Load Balancing. 요금은 사용 AWS 서비스 중인를 통해 측정되며 AWS 청구서에 표시됩니다.

ROSA 결제 및 결제

ROSA 는와 통합되어 ROSA 서비스 요금의 측정 및 청구 AWS Marketplace 를 지원합니다. ROSA 서비스 요금에는 Red Hat 사이트 신뢰성 엔지니어(SREs)의 OpenShift 소프트웨어 및 클러스터 관리에 대한 액세스가 포함됩니다. ROSA 서비스 요금은 지원되는 모든 AWS 표준 리전에서 동일합니다. HCP를 사용하는 ROSA 서비스 요금은 기본적으로 실행 중인 클러스터 및 해당 클러스터에서 실행 중인 워커 노드 vCPU 수에 따라 고정 시간당 요율로 온디맨드 방식으로 부과됩니다. ROSA 클래식 서비스 요금은 워커 노드 vCPU 수를 기준으로 온디맨드 방식으로 부과됩니다. ROSA 클래식은 컨트롤 플레인 또는 필수 인프라 노드에 대한 서비스 요금을 부과하지 않습니다.

ROSA 또한 고객은 다음을 포함하여 AWS 서비스 기본 ROSA 클러스터에 대한 표준 AWS 인프라 요금을 지불합니다 Elastic Load Balancing. Amazon EC2 Amazon EBS Amazon S3인프라 AWS 요금은를 통해 측정되는 ROSA 서비스 요금과 별도의 결제 항목입니다 AWS Marketplace. AWS 인프라 요금은에 따라 다르 AWS 리전 며 기본적으로 시간당 사용량을 기준으로 합니다. 추가 AWS 인프라 비

용 절감을 위해 Amazon EC2 절감형 플랜 또는 예약 인스턴스를 구매할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 Compute Savings Plans 및 예약 인스턴스를 참조하세요.

ROSA 는 ROSA 클러스터를 생성하거나 ROSA 계약을 구매할 때까지 요금을 부과하지 않습니다. 자세한 내용은 Red Hat OpenShift Service on AWS 요금을 참조하십시오.

AWS Billing 콘솔에서 ROSA 서비스 요금 및 AWS 인프라 요금을 확인하고 결제를 관리할 수 있습니다. AWS Cost Explorer Service 인터페이스를 사용하여 비용을 보고 사용량을 무료로 모니터링할 수도 있습니다. 자세한 내용은 AWS 결제 및 비용 관리 사용 설명서의 청구서 보기 및 AWS 비용 관리 사용 설명서의 를 사용한 비용 분석을 참조하세요 AWS Cost Explorer Service.

콘솔을 통해 ROSA Marketplace 목록 구독

ROSA 콘솔 ROSA 에서를 활성화하면 AWS 계정 가 ROSA 클래식 및 ROSA with HCP 등록을 구독합니다 AWS Marketplace. ROSA 구독 활성화에는 요금이 부과되지 않습니다.

AWS Organizations 사용자의 경우를 ROSA 사용하면 ROSA 클래식 구독을 조직의 다른 계정과 공유할 수 있습니다. 자세한 내용은 AWS Marketplace 구매자 안내서의 조직에서 구독 공유를 참조하세요.

ROSA 계약 구매

ROSA 는 AWS Marketplace 를 사용하여 ROSA with HCP 및 ROSA 클래식에 대한 선택적 계약을 제공합니다. 계약은 ROSA 작업자 노드 서비스 요금을 절감합니다. ROSA 계약은 AWS 인프라에 부과되는 요금에 영향을 주지 않습니다.

12개월 계약

ROSA 콘솔에서 ROSA 클래식 및 ROSA with HCP에 대한 12개월 공개 제안 계약을 구매할 수 있습니다.

> **Note**
>
> 콘솔에서 12개월 계약을 구매하려면 먼저 계정에서 ROSA 클래식을 활성화해야 합니다.

> **Note**
>
> 12개월 계약은 비공개 제안으로 이전할 수 없습니다.

ROSA 클래식 12개월 계약 구매

ROSA 클래식 12개월 계약을 구매하면 연간 약정을 선결제하고 적용 대상 인스턴스에 대해 이후 12개월 동안 시간당 서비스 요금을 지불하지 않아도 됩니다. 계약 비용은 선택한 Amazon EC2 인스턴스 유형과 인스턴스 수를 기준으로 합니다. 이 계약에는 사용된 기본에 대해가 ROSA 부과 AWS 서비스 하는 AWS 인프라 요금은 포함되지 않습니다. 자세한 내용은 Red Hat OpenShift Service on AWS 요금을 참조하세요.

계약에는 계약 생성 시 지정하는 인스턴스 유형(예: m5.xlarge)에만 적용됩니다. 두 개 이상의 Amazon EC2 인스턴스 유형에 대한 비용 절감을 위해 12개월 계약을 추가로 구매할 수 있습니다. 12개월 계약 이외의 계약을 사용하면 온디맨드 요금으로 ROSA 서비스 요금이 발생합니다.

> **Note**
>
> ROSA 클래식 12개월 계약은 자동 갱신되지 않습니다.

ROSA 클래식 12개월 계약 구매하는 방법

> **Note**
>
> 아직 ROSA with HCP를 지원하지 않는 리전에서 ROSA 콘솔을 사용하는 경우이 워크플로를 아직 사용할 수 없습니다. ROSA with HCP를 지원하는 리전 목록은 섹션을 참조하세요the section called “ROSA와 HCP 및 ROSA 클래식 비교”.
> HCP를 사용하는 ROSA가 없는 지역에서 ROSA 클래식 계약을 구매하려면 ROSA 콘솔로 이동하여 소프트웨어 계약 구매와 기존 계약 보기를 선택합니다.

1. ROSA 콘솔로 이동합니다.
2. 왼쪽 탐색 창에서 계약을 선택합니다.
3. ROSA 클래식 계약을 선택합니다.
4. 구매 계약을 선택합니다.
5. EC2 인스턴스 유형을 선택하고 필요한 인스턴스 수를 입력합니다.
6. 계약 검토를 선택합니다.
7. 계약 세부 정보를 검토하고 구매 계약을 선택합니다.

> **Note**
>
> ROSA 콘솔을 사용하여 생성한 후에는 12개월 계약을 다운그레이드하거나 취소할 수 없습니다. 활성 계약 기간 중에 계약을 다운그레이드하거나 취소해야 하는 경우 지원 센터로 이동하여 지원 사례를 열어야합니다.

HCP를 사용하는 ROSA 구매 12개월 계약

콘솔에서 HCP를 사용하는 ROSA를 활성화하면 온디맨드 청구를 용이하게 하기 위해 처음에는 무료 12개월 HCP를 사용하는 ROSA 계약이 계정에 생성됩니다. 작업자 노드 서비스 요금을 절약하기 위해 HCP를 사용하는 ROSA 계약을 구입하기로 선택한 경우 지정한 워커 노드 vCPU 및 컨트롤 플레인의 사용 비용을 충당하도록 초기 계약이 수정됩니다.

HCP를 사용하는 ROSA 12개월 계약을 구입하면 연간 계약 금액을 선결제하고 적용 대상 워커 노드 vCPU 및 컨트롤 플레인에 대해 다음 12개월 동안 시간당 사용료를 지불하지 않아도 됩니다. 계약 비용은 선택한 워커 노드 vCPU 및 컨트롤 플레인의 수를 기준으로 합니다. 계약에는 계약 생성 시 지정하는 워커 노드 vCPU와 컨트롤 플레인만 포함됩니다. 이 계약에는 사용된 기본에 대해가 ROSA 부과 AWS 서비스 하는 AWS 인프라 요금은 포함되지 않습니다. 자세한 내용은 Red Hat OpenShift Service on AWS 요금을 참조하세요.

월간 사용 할당량

구매 시 선불 vCPU 및 컨트롤 플레인이 월간 사용 할당량으로 전환됩니다. 월간 할당량을 초과하는 vCPU 및 컨트롤 플레인 사용량에 대해서는 시간당 온디맨드 사용 요금이 적용됩니다. HCP를 사용하는 ROSA는 다음 공식을 사용하여 계약과 관련된 월별 할당량을 계산합니다.

- 워커 노드 vCPU: vCPU 수 x 24시간 x 365일/12개월
- 컨트롤 플레인: 컨트롤 플레인 수 x 24시간 x 365일/12개월

예를 들어 워커 노드 vCPUs개와 컨트롤 플레인 8개를 구매하면 워커 노드 vCPU 시간 2,920,000시간, 컨트롤 플레인 시간 5,840시간의 월별 할당량으로 변환됩니다.

HCP를 사용하는 ROSA 구매 12개월 계약

> **Note**
>
> 호스팅된 컨트롤 플레인에서 ROSA를 아직 지원하지 않는 리전에서 Red Hat OpenShift Service on AWS 콘솔을 사용하는 경우이 워크플로를 아직 사용할 수 없습니다. ROSA with

HCP를 지원하는 리전 목록은 섹션을 참조하세요the section called “ROSA와 HCP 및 ROSA 클래식 비교”.

1. ROSA 콘솔로 이동합니다.
2. 왼쪽 탐색 창에서 계약을 선택합니다.
3. HCP를 사용하는 ROSA에 대한 계약을 선택합니다.
4. 구매 계약을 선택합니다.
5. 구매할 vCPU 수를 입력합니다. 4의 배수로 지정해야 합니다.
6. 구매할 컨트롤 플레인 수를 입력합니다.
7. 계약 검토를 선택합니다.
8. 계약 세부 정보를 검토하고 구매 계약을 선택합니다.

Note

ROSA 콘솔을 사용하여 생성한 후에는 12개월 계약을 다운그레이드하거나 취소할 수 없습니다. 활성 계약 기간 중에 계약을 다운그레이드하거나 취소해야 하는 경우 지원 센터로 이동하여 지원 사례를 열어야합니다.

HCP를 사용하는 ROSA 12개월 계약 업그레이드

추가 작업자 노드 vCPU 및 컨트롤 플레인을 사용하여 언제든지 활성화된 HCP를 사용하는 ROSA 12개월 계약으로 업그레이드할 수 있습니다. HCP를 사용하는 ROSA 12개월 계약으로 업그레이드하는 경우 추가된 리소스에 대해 비례 배분하여 선결제 금액을 지불합니다. 일할 계산된 금액은 계약의 남은 일수를 기준으로 계산됩니다. 계약에는 계약 생성 시 지정하는 워커 노드 vCPU와 컨트롤 플레인만 포함됩니다. 계약 업그레이드는 AWS 인프라에 부과되는 요금에 영향을 주지 않습니다.

업그레이드 시 추가된 vCPU와 컨트롤 플레인은 최초 계약 구매와 동일한 공식을 사용하여 월간 사용량 할당량으로 변환됩니다. 월간 할당량을 초과하는 vCPU 및 컨트롤 플레인 사용량에 대해서는 시간당 온디맨드 사용 요금이 적용됩니다. 자세한 내용은 the section called “월간 사용 할당량” 단원을 참조하십시오.

HCP를 사용하는 ROSA 12개월 계약으로 업그레이드하는 방법

1. ROSA 콘솔로 이동합니다.

2. 왼쪽 탐색 창에서 계약을 선택합니다.
3. HCP를 사용하는 ROSA에 대한 계약을 선택합니다.
4. Upgrade(업그레이드)를 선택합니다.
5. 추가할 vCPU 수를 입력합니다. 4의 배수로 지정해야 합니다.
6. 계약에 추가할 컨트롤 플레인의 수를 입력합니다.
7. 업그레이드 검토를 선택합니다.
8. 계약 세부 정보를 검토하고 업그레이드 구매를 선택합니다.

> **Note**
>
> ROSA 클래식 12개월 계약은 업그레이드할 수 없습니다. ROSA 콘솔을 사용하여 언제든지 12개월 ROSA 클래식 계약을 추가로 구매할 수 있습니다.

비공개 제안 받기

Red Hat과 협상한 제품 요금 및 최종 사용자 라이선스 계약(EULA) 조건을 받기 위해 HCP가 포함된 ROSA 또는 ROSA 클래식에 대한 AWS Marketplace 비공개 제안을 요청할 수 있습니다. 자세한 내용은 AWS Marketplace 구매자 안내서의 비공개 제안을 참조하세요.

ROSA 비공개 제안을 받으려면

> **Note**
>
> AWS Organizations 사용자가 지급인 및 멤버 계정에 발급된 비공개 제안을 받은 경우 아래 절차에 따라 조직의 각 계정에서 ROSA 직접를 구독하세요.
> AWS Organizations 지급인 계정에만 발급된 ROSA 클래식 비공개 제안을 받은 경우 조직의 멤버 계정과 구독을 공유해야 합니다. 자세한 내용은 AWS Marketplace 구매자 안내서의 조직에서 구독 공유를 참조하세요.

1. 비공개 제안이 발행되면 AWS Marketplace 콘솔에 로그인합니다.
2. ROSA 비공개 제안 링크가 포함된 이메일을 엽니다.
3. 링크를 따라 비공개 제안에 직접 액세스합니다.

> **Note**
>
> 올바른 계정에 로그인하지 않고 이 링크를 따라가면 Page not found(404) 오류가 발생합니다.

4. 이용 약관을 검토합니다.
5. 약관에 동의를 선택합니다.

> **Note**
>
> AWS Marketplace 비공개 제안이 수락되지 않은 경우의 ROSA 서비스 요금은 퍼블릭 시간당 요금으로 AWS Marketplace 계속 청구됩니다.

6. 제안 세부 정보를 확인하려면 제품 목록에서 세부 정보 표시를 선택합니다.
7. 사용을 시작하려면 구성 계속을 ROSA선택합니다. ROSA 콘솔로 리디렉션됩니다.

Private Marketplace

Private Marketplace를 사용하면 관리자가 승인된 제품의 사용자 지정 디지털 카탈로그를 구축할 수 있습니다 AWS Marketplace. 관리자는에서 AWS 조직 단위 AWS Marketplace 에 사용할 수 있거나 조직 AWS 계정 내에서 구매할 수 있는 고유한 심사된 소프트웨어 세트를 생성할 수 있습니다.

조직에서 프라이빗 마켓플레이스를 사용하는 경우 관리자가 프라이빗 마켓플레이스에에 대한 AWS Marketplace 목록을 추가해야 사용자가 서비스를 활성화 ROSA 할 수 있습니다. 자세한 내용은 AWS Marketplace 구매자 안내서의 프라이빗 마켓플레이스 시작하기를 참조하세요.

문제 해결

다음 페이지에서는 ROSA 클러스터를 생성하거나 관리하는 동안 발생하는 몇 가지 일반적인 문제를 자세히 설명합니다.

주제

ROSA 클러스터 디버그 로그 액세스

애플리케이션 관련 문제 해결을 시작하려면 먼저 디버그 로그를 검토하세요. ROSA CLI 디버그 로그는 가 생성 클러스터 되지 않을 때 생성되는 오류 메시지에 대한 세부 정보를 제공합니다.

클러스터 디버그 정보를 표시하려면 다음 ROSA CLI 명령을 실행합니다. 명령에서를의 이름으로 `<cluster_name>` 바꿉니다 클러스터.

```
rosa describe cluster -c <cluster_name> --debug
```

ROSA 클러스터 클러스터 가 생성 중에 AWS 서비스 할당량 검사에 실패함

를 사용하려면 계정 ROSA의 서비스 할당량을 늘려야 할 수 있습니다. 자세한 내용은 Red Hat OpenShift Service on AWS 엔드포인트 및 할당량을 참조하세요.

1. 다음 명령을 실행하여 계정의 할당량을 확인합니다.

```
rosa verify quota
```

> **Note**
>
> 할당량은 AWS 리전마다 다릅니다. 해당 리전의 각 할당량을 확인하십시오.

2. 할당량을 늘려야 하는 경우 Service Quotas 콘솔로 이동하세요.
3. 탐색 창에서 AWS 서비스를 선택합니다.
4. 할당량 증가가 필요한 서비스를 선택합니다.
5. 늘려야 할 할당량을 선택하고 할당량 증가 요청을 선택합니다.
6. 할당량 증가 요청의 경우 원하는 할당량 총량을 입력하고 요청을 선택합니다.

ROSA CLI 만료된 오프라인 액세스 토큰 문제 해결

ROSA CLI를 사용하고 api.openshift.com 오프라인 액세스 토큰이 만료되면 오류 메시지가 나타납니다. 이 문제는 sso.redhat.com에서 토큰을 무효화할 때 발생합니다.

1. OpenShift 클러스터 관리자 API 토큰 페이지로 이동하여 토큰 로드를 선택합니다.
2. 다음 인증 명령을 복사하여 터미널에 붙여 넣습니다.

```
rosa login --token="<api_token>"
```

osdCcsAdmin 오류가 클러스터 있는를 생성하지 못했습니다.

> **Note**
>
> 이 오류는 ROSA 클러스터를 프로비저닝하는 비 STS 방법을 사용하는 경우에만 발생합니다. 이 문제를 방지하려면를 사용하여 ROSA 클러스터를 프로비저닝합니다 AWS STS. 자세한 내용은 the section called “ROSA 클래식 클러스터 생성 - CLI” 단원을 참조하십시오.

를 생성 클러스터 하지 못하면 다음과 같은 오류 메시지가 표시될 수 있습니다.

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for
 user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

1. 스택을 삭제합니다.

```
rosa init --delete-stack
```

2. 계정을 다시 초기화합니다.

```
rosa init
```

다음 단계

- OpenShift 설명서를 참조하세요.
- 지원 사례 또는 Red Hat Support 사례를 엽니다.
- 자주 묻는 질문에 대한 Red Hat OpenShift Service on AWS 답변을 찾아보세요.
- ROSA의 지원 모델에 대한 자세한 내용은 섹션을 참조하세요the section called “지원 받기”.

ROSA 지원 받기

ROSA를 사용하면 지원 및 Red Hat 지원 팀으로부터 지원을 받을 수 있습니다. 어느 조직에서든 지원 사례를 개설할 수 있으며, 지원 사례는 문제 해결을 위해 해당 팀에 전달됩니다.

지원 사례 열기

ROSA 기술 사례를 개설하려면 AWS 개발자 지원 플랜이 필요하지만 ROSA 기술 지원 및 아키텍처 지침에 지속적으로 액세스하려면 AWS Business, Enterprise 또는 Enterprise On-Ramp Support 플랜이 권장됩니다. Red Hat은 지원 API를 사용하여 필요한 경우 고객을 위한 사례를 엽니다. AWS 비즈니스, 엔터프라이즈 및 엔터프라이즈 온프레미스 지원 플랜을 사용하면 지원 엔지니어에게 전화, 웹 및 채팅 액세스를 지속적으로 제공할 수 있습니다. 지원 계획에 대한 자세한 내용은 단원을 참조하십시오지원.

지원 계획을 활성화하는 단계는 지원 계획에 가입하려면 어떻게 해야 하나요?를 참조하세요.

지원 사례 생성에 대한 자세한 내용은 지원 사례 및 사례 관리 생성을 참조하세요.

Red Hat 지원 사례 열기

ROSA 에는 Red Hat Premium Support가 포함되어 있습니다. Red Hat Premium Support를 받으려면 Red Hat 고객 포털로 이동하고 지원 사례 도구를 사용하여 지원 티켓을 생성하세요. 자세한 내용은 Red Hat 지원 서비스 이용 방법을 참조하세요.

문서 이력

다음 표에서는 설명서에 대한 중요 변경 사항을 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
ROSAControlPlaneOperatorPolicy 업데이트	적절한 리소스 수명 주기 관리를 위해 Red Hat 관리형 보안 그룹의 태그 지정을 허용하고 ManageVPCEndpointWithCondition에 security-group/*를 추가하여 클러스터 업그레이드 중에 VPCE 조정 실패를 수정하도록 AWS 관리형 정책 ROSAControlPlaneOperatorPolicy를 업데이트했습니다. 자세한 내용은 ROSAAWS 관리형 정책에 대한 업데이트를 참조하세요.	2026년 4월 9일
ROSAKubeControllerPolicy 업데이트	대상 그룹에 대상을 등록 및 등록 취소하기 위한 Elastic Load Balancing 권한을 명확히 하기 위해 AWS 관리형 정책 ROSAKubeControllerPolicy를 업데이트했습니다. 자세한 내용은 ROSAAWS 관리형 정책에 대한 업데이트를 참조하세요.	2026년 3월 5일
업데이트된 ROSANodePoolManagementPolicy	ROSA 는 용량 예약 기능을 지원하기 `ROSANodePoolManagementPolicy` 위해 용량 예약에 대한 리소스 액세스를 추가하도록 관리형 정책을 업데이트했습니다. 자	2025년 9월 3일

	세한 내용은 ROSAAWS 관리형 정책에 대한 업데이트를 참조하세요.	
ROSAInstallerPolicy 업데이트	ROSA의 새로운 용량 예약 기능을 지원하고 Kubernetes 클러스터 태그 관리를 개선하도록 AWS 관리형 정책 ROSAInstallerPolicy를 업데이트했습니다. ROSAInstallerPolicy 자세한 내용은 ROSAAWS 관리형 정책 업데이트를 참조하세요.	2025년 8월 7일
새로운 ROSASharedVPCRoute53Policy	ROSA 는 ROSA 설치 관리자가 공유 VPC 환경에서 Route 53 레코드를 구성할 수 `ROSASharedVPCRoute53Policy` 있도록 허용하는 새로운 관리형 정책을 릴리스했습니다. 자세한 내용은 ROSAAWS 관리형 정책에 대한 업데이트를 참조하세요.	2025년 8월 7일
새로운 ROSASharedVPCEndpointPolicy	ROSA 는 ROSA 설치 관리자가 공유 VPC 환경에서 VPC 엔드포인트 및 보안 그룹을 구성할 수 `ROSASharedVPCEndpointPolicy` 있도록 허용하는 새로운 관리형 정책을 릴리스했습니다. 이 정책은 공유 VPC 사용 사례에 맞게 조정된 EC2 권한의 하위 집합을 제공합니다. 자세한 내용은 ROSAAWS 관리형 정책에 대한 업데이트를 참조하세요.	2025년 8월 7일

ROSAImageRegistryOperatorPolicy 업데이트	AWS 관리형 정책 ROSAImageRegistryOperatorPolicy를 업데이트했습니다.	2025년 5월 19일
업데이트된 ROSANodePoolManagementPolicy	AWS 관리형 정책 ROSANodePoolManagementPolicy를 업데이트했습니다.	2025년 5월 5일
ROSAImageRegistryOperatorPolicy 업데이트	AWS 관리형 정책 ROSAImageRegistryOperatorPolicy를 업데이트했습니다.	2025년 4월 16일
ROSAWorkerInstancePolicy 업데이트	AWS 관리형 정책 ROSAWorkerInstancePolicy를 업데이트했습니다.	2025년 3월 3일
업데이트된 ROSANodePoolManagementPolicy	AWS 관리형 정책 ROSANodePoolManagementPolicy를 업데이트했습니다.	2025년 2월 24일
ROSAAmazonEBSCSIDriverOperatorPolicy 업데이트	AWS 관리형 정책 ROSAAmazonEBSCSIDriverOperatorPolicy를 업데이트했습니다.	2025년 1월 17일
ROSA와 HCP AWS 리전 확장	이제 중동(UAE)에서 호스팅 컨트롤 플레인(HCP)이 있는 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 5월 13일
ROSA와 HCP AWS 리전 확장	이제 유럽(파리)에서 호스팅 컨트롤 플레인(HCP)이 포함된 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 5월 6일

업데이트된 ROSANodePoolManagementPolicy	AWS 관리형 정책 ROSANodePoolManagementPolicy를 업데이트했습니다.	2024년 5월 2일
ROSA와 HCP AWS 리전 확장	이제 유럽(스페인)에서 호스팅 컨트롤 플레인(HCP)이 있는 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 4월 29일
ROSAInstallerPolicy 업데이트	AWS 관리형 정책 ROSAInstallerPolicy를 업데이트했습니다.	2024년 4월 24일
ROSA와 HCP AWS 리전 확장	이제 유럽(취리히)에서 호스팅 컨트롤 플레인(HCP)이 포함된 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 4월 19일
ROSA와 HCP AWS 리전 확장	이제 아시아 태평양(오사카)에서 호스팅 컨트롤 플레인(HCP)이 포함된 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 4월 17일
ROSAInstallerPolicy 및 ROSASRESupportPolicy 업데이트	AWS 관리형 정책 ROSAInstallerPolicy 및 ROSASRESupportPolicy가 업데이트되었습니다.	2024년 4월 10일
ROSA와 HCP AWS 리전 확장	이제 아시아 태평양(홍콩)에서 호스팅 컨트롤 플레인(HCP)이 포함된 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 4월 8일
ROSA와 HCP AWS 리전 확장	호스팅 컨트롤 플레인(HCP)이 있는 ROSA는 이제 남아메리카(상파울루)에서 사용할 수 있습니다 AWS 리전.	2024년 4월 1일

ROSA와 HCP AWS 리전 확장	이제 중동(바레인)에서 호스팅 컨트롤 플레인(HCP)이 있는 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 3월 25일
ROSA와 HCP AWS 리전 확장	이제 아시아 태평양(서울)에서 호스팅 컨트롤 플레인(HCP)이 포함된 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 3월 14일
ROSA와 HCP AWS 리전 확장	이제 아프리카(케이프타운)에서 호스팅 컨트롤 플레인(HCP)이 포함된 ROSA를 사용할 수 있습니다 AWS 리전.	2024년 3월 5일
ROSAInstallerPolicy 업데이트	AWS 관리형 정책 ROSAInstallerPolicy를 업데이트했습니다.	2024년 1월 26일
ROSASRESupportPolicy 업데이트	AWS 관리형 정책 ROSASRESupportPolicy를 업데이트했습니다.	2024년 1월 22일
ROSAImageRegistryOperatorPolicy 업데이트	AWS 관리형 정책 ROSAImageRegistryOperatorPolicy를 업데이트했습니다.	2023년 12월 12일
ROSAKubeControllerPolicy 업데이트	AWS 관리형 정책 ROSAKubeControllerPolicy를 업데이트했습니다.	2023년 10월 16일
ROSAManageSubscription 업데이트	AWS 관리형 정책 ROSAManageSubscription을 업데이트했습니다.	2023년 8월 1일
ROSAKubeControllerPolicy 업데이트	AWS 관리형 정책 ROSAKubeControllerPolicy를 업데이트했습니다.	2023년 7월 13일

ROSA 보안 페이지 추가	ROSA의 복원력, ROSA의 인프라 보안, ROSA의 데이터 보호 페이지가 추가되었습니다.	2023년 6월 30일
배포 옵션 페이지 추가	배포 옵션 페이지가 추가되었습니다.	2023년 6월 9일
새로운 AWS 관리형 정책 ROSANodePoolManagementPolicy 추가	새로운 AWS 관리형 정책 ROSANodePoolManagementPolicy가 추가되었습니다.	2023년 6월 8일
새로운 AWS 관리형 정책 ROSAInstallerPolicy 추가	새로운 AWS 관리형 정책 ROSAInstallerPolicy가 추가되었습니다.	2023년 6월 6일
새로운 AWS 관리형 정책 ROSASRESupportPolicy 추가	새로운 AWS 관리형 정책 ROSASRESupportPolicy가 추가되었습니다.	2023년 6월 1일
ROSA의 책임 개요 추가	ROSA의 책임 개요 페이지가 추가되었습니다.	2023년 5월 26일
업데이트된 정의 Red Hat OpenShift Service on AWS	정의 Red Hat OpenShift Service on AWS 페이지가 업데이트되었습니다.	2023년 5월 24일
ROSA 운영자 역할에 대한 새로운 AWS 관리형 정책 추가	새로운 AWS 관리형 정책 ROSAImageRegistryOperatorPolicy, ROSAKubeControllerPolicy 및 ROSAKMSProviderPolicy가 추가되었습니다.	2023년 4월 27일
새로운 AWS 관리형 정책 ROSAControlPlaneOperatorPolicy 추가	새로운 AWS 관리형 정책 ROSAControlPlaneOperatorPolicy가 추가되었습니다.	2023년 4월 24일

ROSA 계정 역할에 대한 새로운 AWS 관리형 정책 추가	ROSA 계정 및 운영자 역할 페이지에 대한 새로운 AWS 관리형 정책 페이지가 추가되었습니다.	2023년 4월 20일
ROSA 서비스 할당량 페이지 추가	ROSA 서비스 할당량 페이지가 추가되었습니다.	2022년 12월 22일
문제 해결 페이지 추가	문제 해결 페이지가 추가되었습니다.	2022년 11월 1일
시작 안내서 추가	시작하기 페이지가 추가되었습니다.	2022년 8월 12일
새로운 AWS 관리형 정책 ROSAManageSubscription 추가	새로운 AWS 관리형 정책 ROSAManageSubscription이 추가되었습니다.	2022년 4월 11일
최초 릴리스	Red Hat OpenShift Service on AWS 사용 설명서의 최초 릴리스입니다.	2021년 3월 24일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.