Red Hat OpenShift Service on AWS 4

정보

AWS의 OpenShift 서비스 설명서.

Last Updated: 2024-11-03

Red Hat OpenShift Service on AWS 4 정보

AWS의 OpenShift 서비스 설명서.

법적 공지

초록

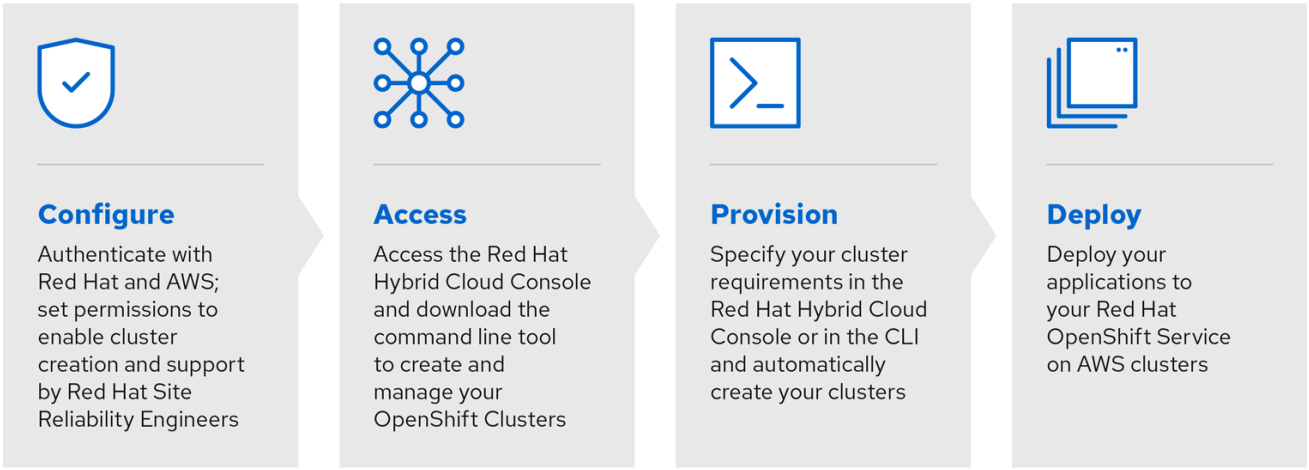
AWS의 OpenShift Service에 대해 알아보고 해당 기능을 탐색할 수 있는 AWS의 공식 OpenShift Service에 오신 것을 환영합니다.

차례

1장. RED HAT OPENSHIFT SERVICE ON AWS 4 문서

목차

ROSA(Red Hat OpenShift Service on AWS) 문서에 오신 것을 환영합니다. 여기에서 ROSA에 대해 알아보고 기능을 탐색할 수 있습니다. ROSA에 대해 알아보려면 Red Hat OpenShift Cluster Manager 및 CLI(명령줄 인터페이스) 툴, 사용 경험 및 AWS(Amazon Web Services) 서비스와의 통합을 통해 ROSA와 상호 작용 하려면 ROSA 소개 문서 부터 시작하십시오.



ROSA 문서를 탐색하려면 왼쪽 탐색 모음을 사용합니다.

2장. HCP를 사용하여 ROSA에 대해 자세히 알아보기

HCP(Red Hat OpenShift Service on AWS)는 효율성에 중점을 두고 관리형 ROSA 클러스터를 생성할 수 있는 비용 절감 솔루션을 제공합니다. 새 클러스터를 빠르게 생성하고 몇 분 내에 애플리케이션을 배포할 수 있습니다.

2.1. HCP를 사용하는 ROSA의 주요 기능

- HCP를 사용하는 ROSA에는 최소 두 개의 노드가 필요하므로 소규모 프로젝트에는 이상적이며 대규모 프로젝트와 엔터프라이즈를 지원하기 위해 확장할 수 있습니다.
- 기본 컨트롤 플레인 인프라는 완전히 관리됩니다. API 서버 및 etcd 데이터베이스와 같은 컨트롤 플레인 구성 요소는 Red Hat 소유 AWS 계정에서 호스팅됩니다.
- 프로비저닝 시간은 약 10분입니다.
- 고객은 컨트롤 플레인과 머신 풀을 별도로 업그레이드할 수 있으므로 업그레이드 중에 전체 클러스터를 종료할 필요가 없습니다.

2.2. HCP로 ROSA 시작하기

다음 섹션을 사용하여 HCP와 ROSA에 대해 알아보고 사용하는 데 도움이 되는 콘텐츠를 찾습니다.

2.2.1. 아키텍트

HCP를 사용하여 ROSA에 대해 알아보기	HCP 배포를 통한 ROSA 계획	추가 리소스
아키텍처 개요	백업 및 복원	HCP 라이프 사이클을 사용하는 ROSA
HCP 아키텍처가 있는 ROSA		HCP 서비스 정의를 사용하는 ROSA
		지원 요청

2.2.2. 클러스터 관리자

HCP를 사용하여 ROSA에 대해 알아보기	HCP를 사용하여 ROSA 배포	HCP로 ROSA 관리	추가 리소스
HCP 아키텍처가 있는 ROSA	HCP를 사용하여 ROSA 설치	지원 요청	OpenShift Interactive Learning Portal
스토리지	모니터링 개요	HCP 라이프 사이클을 사용하는 ROSA	
백업 및 복원			

2.2.3. 개발자

HCP를 사용한 ROSA의 애플리케이션 개발에 대해 알아보기	애플리케이션 배포	추가 리소스
Red Hat Developers 사이트	애플리케이션 빌드 개요	지원 요청
Red Hat OpenShift Dev Spaces (이전 Red Hat CodeReady Workspaces)	Operator 개요	
	이미지	
	개발자 중심 CLI	

3장. AWS STS 및 HCP를 사용하는 ROSA 설명

Red Hat OpenShift Service on AWS (ROSA) with hosted control Planes (HCP)는 AWS 계정의 리소스와 상호 작용하는 데 필요한 인증 정보를 얻기 위해 AWS(Amazon Web Services)용 AWS(Amazon Web Services) 보안 토큰 서비스(STS)를 사용합니다.

3.1. AWS STS 인증 정보 방법

HCP를 사용하는 ROSA의 일부로 Red Hat은 AWS 계정에서 인프라 리소스를 관리하는 데 필요한 권한을 부여해야 합니다. HCP를 사용하는 ROSA는 클러스터의 자동화 소프트웨어를 AWS 계정의 리소스에 대한 단기 액세스 권한을 부여합니다.

STS 메서드는 사전 정의된 역할 및 정책을 사용하여 IAM 역할에 임시 최소 권한 권한을 부여합니다. 인증 정보는 일반적으로 요청 후 1시간 후에 만료됩니다. 만료되면 AWS에서 더 이상 인식되지 않으며 해당 API 요청에서 더 이상 계정 액세스 권한이 없습니다. 자세한 내용은 AWS 설명서 를 참조하십시오.

HCP 클러스터의 각 ROSA에 대해 AWS IAM STS 역할을 생성해야 합니다. ROSA CLI(명령줄 인터페이스) (**rosa**)는 STS 역할을 관리하고 ROSA별 AWS 관리 정책을 각 역할에 연결하는 데 도움이 됩니다. CLI는 역할을 생성하는 명령과 파일을 제공하고, AWS 관리 정책을 연결하며, CLI에서 역할을 자동으로 생성하고 정책을 연결할 수 있는 옵션을 제공합니다.

3.2. AWS STS 보안

AWS STS의 보안 기능은 다음과 같습니다.

- 사용자가 미리 생성하는 명시적 및 제한된 정책 집합입니다.
  - 사용자는 플랫폼에 필요한 모든 요청된 권한을 검토할 수 있습니다.
- 서비스는 해당 권한 외부에서는 아무 작업도 수행할 수 없습니다.
- 인증 정보를 교체하거나 취소할 필요가 없습니다. 서비스가 작업을 수행해야 할 때마다 1시간 이내에 만료되는 인증 정보를 가져옵니다.
- 인증 정보 만료를 사용하면 인증 정보 누출 및 재사용 위험이 줄어듭니다.

HCP를 사용하는 ROSA는 단기 보안 인증 정보를 사용하여 클러스터 소프트웨어 구성 요소를 특정 및 분리된 IAM 역할에 대한 권한보다 적은 권한을 부여합니다. 인증 정보는 AWS API 호출을 수행하는 각 구성 요소 및 클러스터와 관련된 IAM 역할과 연결됩니다. 이 방법은 클라우드 서비스 리소스 관리에서 최소 권한 및 보안 관행의 원칙에 맞게 조정됩니다.

3.3. HCP를 사용한 ROSA의 구성 요소

- **AWS 인프라** - Amazon EC2 인스턴스, Amazon EBS 스토리지 및 네트워킹 구성 요소를 포함한 클러스터에 필요한 인프라입니다. 클라우드 리소스 구성에 대한 자세한 내용은 컴퓨팅 노드 및 프로비저닝된 AWS 인프라에 대해 지원되는 인스턴스 유형을 보려면 AWS 컴퓨팅 유형을 참조하십시오. https://docs.redhat.com/en/documentation/red_hat_openshift_service_on_aws/4/html-single/introduction_to_rosa/#rosa-sdpolicy-aws-compute-types_rosa-service-definition
- **AWS STS** - 사용자에게 AWS 계정 리소스와 일시적으로 상호 작용하는 데 필요한 권한을 제공하기 위해 단기적이고 동적 토큰을 부여하는 방법입니다.
- **OpenID Connect(OIDC)** - 클러스터 Operator가 AWS로 인증하고, 신뢰 정책을 통해 클러스터 역할을 가정하고, 필요한 API 호출을 수행하기 위해 AWS IAM STS에서 임시 인증 정보를 가져옵니다.

- **역할 및 정책** - ROSA에서 HCP와 함께 사용하는 역할과 정책은 계정 전체 역할 및 정책 및 Operator 역할 및 정책으로 나눌 수 있습니다.
  정책에 따라 각 역할에 허용되는 작업이 결정됩니다. 신뢰 정책에 대한 자세한 내용은 개별 역할 및 정책 및 ROSA IAM 역할 리소스에 대한 자세한 내용은 STS를 사용하는 ROSA 클러스터 의 IAM 리소스 정보를 참조하십시오.

  - 계정 전체 역할은 다음과 같습니다.
    - ManagedOpenShift-Installer-Role
    - ManagedOpenShift-Worker-Role
    - ManagedOpenShift-Support-Role
  - 계정 전체 AWS 관리 정책은 다음과 같습니다.
    - ROSAInstallerPolicy
    - ROSAWorkerInstancePolicy
    - ROSASRESupportPolicy
    - ROSAIngressOperatorPolicy
    - ROSAAmazonEBSCSIDriverOperatorPolicy
    - ROSACloudNetworkConfigOperatorPolicy
    - ROSAControlPlaneOperatorPolicy
    - ROSAImageRegistryOperatorPolicy
    - ROSAKMSProviderPolicy
    - ROSAKubeControllerPolicy
    - ROSAManageSubscription
    - ROSANodePoolManagementPolicy

참고

아래에 나열된 특정 정책은 클러스터 Operator 역할에서 사용합니다. Operator 역할은 기존 클러스터 이름에 따라 달라지며 계정 전체 역할과 동시에 생성할 수 없기 때문에 두 번째 단계에서 생성됩니다.

  - Operator 역할은 다음과 같습니다.
    - <operator_role_prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
    - <operator_role_prefix>-openshift-cloud-network-config-controller-cloud-credentials
    - <operator_role_prefix>-openshift-machine-api-aws-cloud-credentials
    - <operator_role_prefix>-openshift-cloud-credential-operator-cloud-credentials
    - <operator_role_prefix>-openshift-image-registry-installer-cloud-credentials

- <operator_role_prefix>-openshift-ingress-operator-cloud-credentials

- 각 계정 전체 역할 및 각 Operator 역할에 대한 신뢰 정책이 생성됩니다.

3.4. HCP 클러스터를 사용하여 ROSA 배포

HCP 클러스터를 사용하여 ROSA를 배포하는 방법은 다음과 같습니다.

1. 계정 전체 역할을 생성합니다.
2. Operator 역할을 생성합니다.
3. Red Hat은 AWS STS를 사용하여 AWS가 해당 AWS 관리 Operator 정책을 생성하고 연결할 수 있는 필요한 권한을 AWS에 보냅니다.
4. OIDC 공급자를 생성합니다.
5. 클러스터를 생성합니다.

클러스터 생성 프로세스 중에 ROSA CLI는 사용자에게 필요한 JSON 파일을 생성하고 필요한 명령을 출력합니다. 필요한 경우 ROSA CLI도 명령을 실행할 수 있습니다.

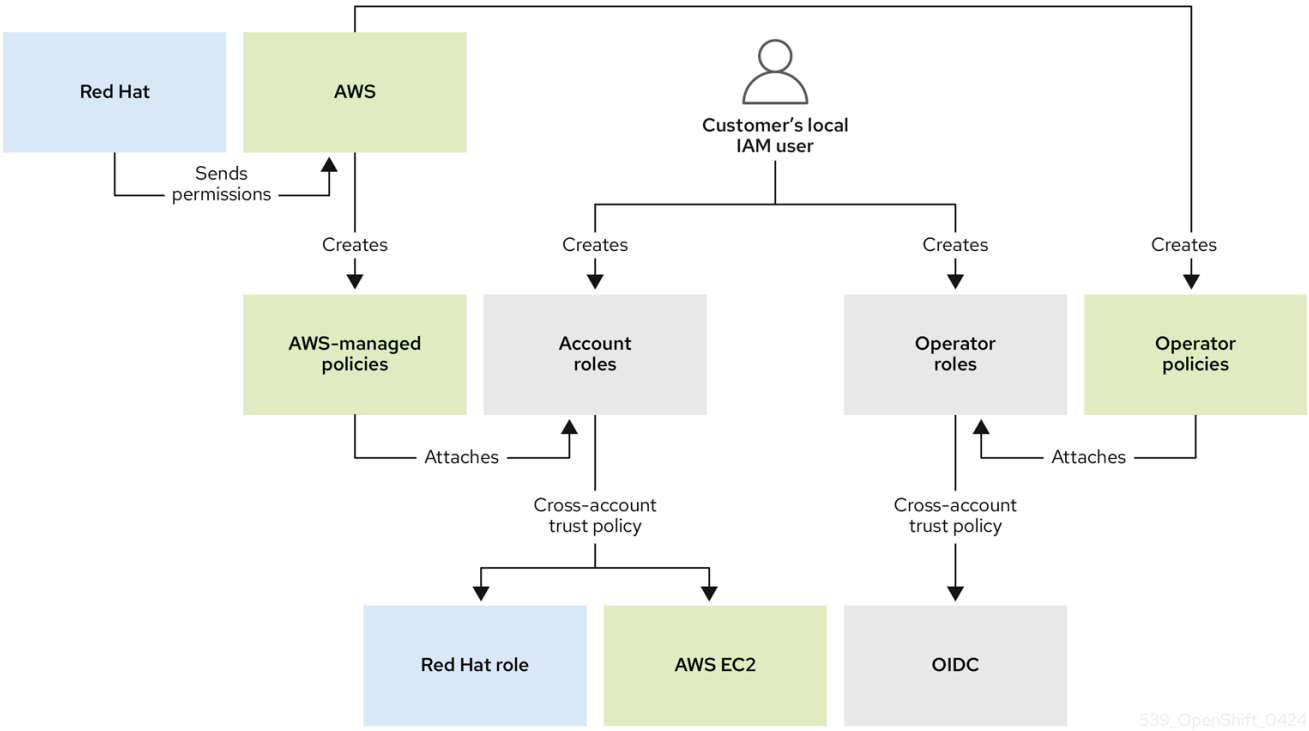
ROSA CLI는 역할을 자동으로 생성하거나 **--mode 수동 또는 --mode 자동** 플래그를 사용하여 수동으로 생성할 수 있습니다. 배포에 대한 자세한 내용은 사용자 지정으로 클러스터 생성 을 참조하십시오.

3.5. HCP 워크플로우를 사용하는 ROSA

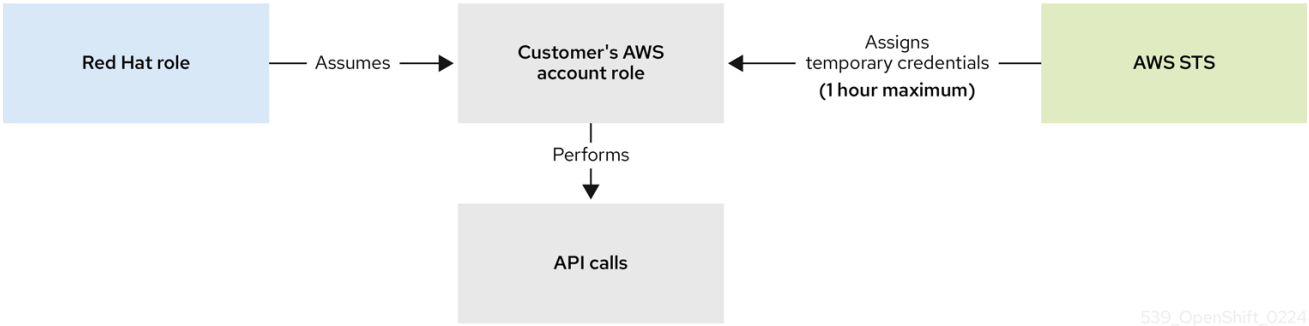
사용자는 필요한 계정 전체 역할을 생성합니다. 역할 생성 중에 교차 계정 신뢰 정책이라는 신뢰 정책이 생성되어 Red Hat 소유 역할이 역할을 수행할 수 있습니다. EC2 인스턴스의 워크로드가 역할을 가정하고 인증 정보를 얻을 수 있는 EC2 서비스에 대한 신뢰 정책도 생성됩니다. AWS는 각 역할에 해당 권한 정책을 할당합니다.

계정 전체 역할 및 정책이 생성되면 사용자가 클러스터를 생성할 수 있습니다. 클러스터 생성이 시작되면 사용자는 Operator 역할을 생성하여 클러스터 Operator가 AWS API 호출을 수행할 수 있습니다. 그런 다음 이러한 역할은 이전에 생성된 해당 권한 정책과 OIDC 공급자를 사용하는 신뢰 정책에 할당됩니다. Operator 역할은 궁극적으로 AWS 리소스에 액세스해야 하는 Pod를 나타내는 계정 전체 역할과 다릅니다. 사용자는 IAM 역할을 Pod에 연결할 수 없으므로 Operator와 Pod가 필요한 역할에 액세스할 수 있도록 OIDC 공급자를 사용하여 신뢰 정책을 생성해야 합니다.

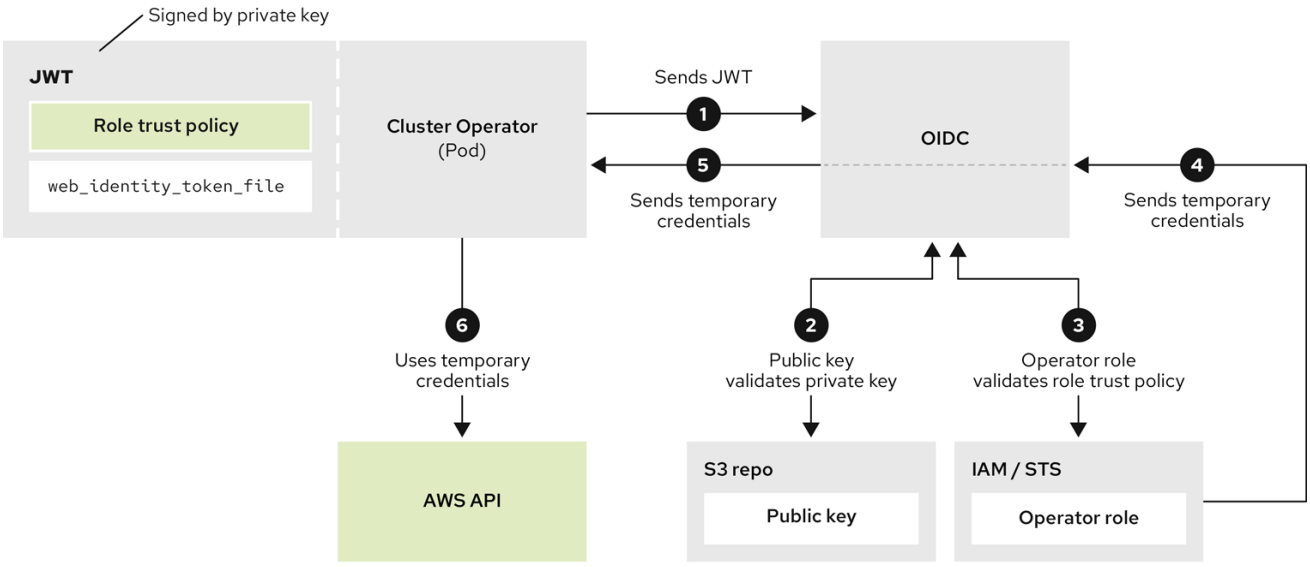
사용자가 해당 정책 권한에 역할을 할당하면 최종 단계는 OIDC 공급자를 생성합니다.



새 역할이 필요한 경우 현재 Red Hat 역할을 사용하는 워크로드는 AWS 계정에서 역할을 수행하고, AWS STS에서 임시 인증 정보를 가져오고, 가정된 역할의 권한 정책에서 허용하는 대로 사용자의 AWS 계정 내에서 API 호출을 사용하여 작업을 수행하기 시작합니다. 인증 정보는 임시이며 최대 1시간 동안 지속됩니다.



Operator는 다음 프로세스를 사용하여 작업을 수행하는 데 필요한 자격 증명을 가져옵니다. 각 Operator에는 Operator 역할, 권한 정책 및 OIDC 공급자가 있는 신뢰 정책이 할당됩니다. Operator는 역할이 포함된 JSON 웹 토큰과 토큰 파일(**web_identity_token_file**)을 OIDC 공급자에 전달하여 역할을 가정하고 공개 키로 서명된 키를 인증합니다. 공개 키는 클러스터 생성 중에 생성되어 S3 버킷에 저장됩니다. 그런 다음 Operator는 서명된 토큰 파일의 주체가 역할 신뢰 정책의 역할과 일치하는지 확인하여 OIDC 공급자가 허용된 역할만 가져올 수 있도록 합니다. 그런 다음 OIDC 공급자는 Operator가 AWS API 호출을 수행할 수 있도록 임시 인증 정보를 Operator에 반환합니다. 시각적 표현의 경우 다음 다이어그램을 참조하십시오.


Signed by private key
JWT
Role trust policy
web_identity_token_file
Cluster Operator
(Pod)
Sends JWT
1
5
Sends temporary
credentials
OIDC
4
Sends temporary
credentials
6
Uses temporary
credentials
2
Public key
validates private key
3
Operator role
validates role trust policy
AWS API
S3 repo
Public key
IAM / STS
Operator role
629_OpenShift_0424

4장. 법적 통지