Red Hat OpenShift Service on AWS 4

환경 준비

AWS에서 Red Hat OpenShift Service의 계획, 제한 및 확장성

Last Updated: 2024-11-07

Red Hat OpenShift Service on AWS 4 환경 준비

AWS에서 Red Hat OpenShift Service의 계획, 제한 및 확장성

법적 공지

초록

이 문서에서는 클러스터 제한 및 확장성에 대한 정보를 포함하여 ROSA(Red Hat OpenShift Service on AWS) 클러스터 배포에 대한 계획을 설명합니다.

차례

1장. STS를 사용하는 ROSA의 AWS 사전 요구 사항

Red Hat OpenShift Service on AWS(ROSA)는 Red Hat이 고객의 기존 AWS(Amazon Web Service) 계정에 클러스터를 배포할 수 있는 모델을 제공합니다.

작은 정보

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

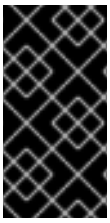
STS를 사용하여 ROSA를 설치하기 전에 다음 AWS 사전 요구 사항이 충족되었는지 확인합니다.

1.1. 배포 사전 요구 사항

Red Hat OpenShift Service on AWS (ROSA)를 기존 AWS(Amazon Web Services) 계정에 배포하려면 Red Hat에서 몇 가지 사전 요구 사항을 충족해야 합니다.

Red Hat은 AWS 조직을 사용하여 여러 AWS 계정을 관리할 것을 권장합니다. 고객이 관리하는 AWS 조직은 여러 AWS 계정을 호스팅합니다. 조직에는 모든 계정이 계정 계층에서 참조할 루트 계정이 있습니다.

ROSA 클러스터를 AWS 조직 단위 내의 AWS 계정에서 호스팅하는 것이 모범 사례입니다. AWS 하위 계정에서 액세스할 수 있는 서비스를 관리하는 AWS Organizational Unit에 SCP(서비스 제어 정책)가 생성되고 적용됩니다. SCP는 조직 단위 내의 모든 AWS 하위 계정에 대해 단일 AWS 계정 내에서 사용 가능한 권한에만 적용됩니다. SCP를 단일 AWS 계정에 적용할 수도 있습니다. 고객의 AWS 조직의 다른 모든 계정은 고객이 요구하는 방식으로 관리합니다. Red Hat 사이트 안정성 엔지니어(SRE)는 AWS 조직 내에서 SCP를 제어할 수 없습니다.



중요

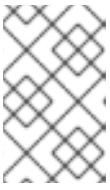
AWS STS를 사용하여 ROSA 클러스터를 생성하면 관련 AWS OpenID Connect(OIDC) ID 공급자도 생성됩니다. 이 OIDC 공급자 구성은 **us-east-1** AWS 리전에 있는 공개 키를 사용합니다. AWS SCP를 보유한 고객은 이러한 클러스터를 다른 리전에 배포하더라도 **us-east-1** AWS 리전 사용을 허용해야 합니다.

1.2. 배포에 STS를 사용할 때 고객 요구 사항

AWS STS(Security Token Service)를 사용하는ROSA(Red Hat OpenShift Service on AWS) 클러스터를 배포하기 전에 다음 사전 요구 사항을 완료해야 합니다.

1.2.1. 계정

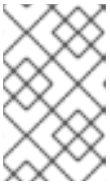
- AWS 제한은 AWS 계정 내에서 프로비저닝된 AWS에서 Red Hat OpenShift Service를 지원하기에 충분한지 확인해야 합니다. CLI에서 **rosa 확인 할당량** 을 실행하면 클러스터를 실행하는 데 필요한 할당량이 있는지 확인합니다.



참고

할당량 확인에서는 AWS 할당량을 검사하지만 사용량을 AWS 할당량과 비교하지는 않습니다. 자세한 내용은 추가 리소스의 "Limits and scalability" 링크를 참조하십시오.

- SCP 정책을 적용하고 시행하는 경우, 이러한 정책은 클러스터가 요구하는 역할과 정책보다 제한적이 아니어야 합니다.
- AWS 계정을 Red Hat으로 이전해서는 안 됩니다.
- Red Hat 활동에 대해 정의된 역할 및 정책 이외의 AWS 사용 제한을 추가로 적용하지 않아야 합니다. 제한 사항을 부과하면 Red Hat의 사고 대응 능력을 크게 방해할 수 있습니다.
- 동일한 AWS 계정 내에 기본 AWS 서비스를 배포할 수 있습니다.
- ELB(Elastic Load Balancing)를 구성하는 데 필요하므로 계정에 서비스 링크된 역할이 설정되어 있어야 합니다. 이전에 AWS 계정에 로드 밸런서를 생성하지 않은 경우 ELB에 대한 서비스 링크 역할을 생성하는 방법에 대한 정보는 추가 리소스의 "Elastic Load Balancing(ELB) 서비스 연결 역할 생성" 링크를 참조하십시오.



참고

AWS 및 기타 Red Hat 지원 서비스에 Red Hat OpenShift Service를 호스팅하는 VPC와 별도로 VPC(Virtual Private Cloud)에 리소스를 배포하는 것이 좋지만 필수 사항은 아닙니다.

추가 리소스

- 제한 및 확장성
- ELB(Elastic Load Balancing) 서비스 연결 역할 생성

1.2.2. 액세스 요구 사항

- Red Hat은 고객이 제공하는 AWS 계정에 대한 AWS 콘솔 액세스 권한이 있어야 합니다. Red Hat은 이 액세스를 보호하고 관리합니다.
- AWS 클러스터의 Red Hat OpenShift Service 내에서 권한을 승격하려면 AWS 계정을 사용해서는 안 됩니다.
- **rosa** CLI 유틸리티 또는 OpenShift Cluster Manager Hybrid Cloud Console 에서 제공되는 작업은 AWS 계정에서 직접 수행하지 않아야 합니다.
- ROSA 클러스터를 배포하기 위해 사전 구성된 도메인이 필요하지 않습니다. 사용자 정의 도메인을 사용하려면 추가 리소스를 참조하십시오.

추가 리소스

- 애플리케이션용 사용자 정의 도메인 구성을 참조하십시오 .

1.2.3. 지원 요구사항

- Red Hat은 고객이 최소한 AWS의 비즈니스 지원을 받을 것을 권장합니다.
- Red Hat은 고객으로부터 AWS 지원을 요청할 수 있습니다.
- Red Hat은 고객 계정의 AWS 리소스 제한 증가를 요청할 수 있는 권한을 고객으로부터 보유할 수 있습니다.

- Red Hat은 이 요구 사항 섹션에 달리 지정하지 않는 한 AWS 클러스터의 모든 Red Hat OpenShift Service의 제한 사항, 제한 사항, 기대치 및 기본값을 동일한 방식으로 관리합니다.

1.2.4. 보안 요구사항

- Red Hat은 허용된 IP 주소에서 EC2 호스트 및 API 서버에 대한 수신 액세스 권한이 있어야 합니다.
- Red Hat은 문서화된 도메인에 허용되는 송신을 보유해야 합니다. 지정된 도메인의 "AWS 방화벽 사전 요구 사항" 섹션을 참조하십시오.

추가 리소스

- AWS 방화벽 사전 요구 사항

1.2.5. OpenShift Cluster Manager 사용 요구사항

다음 섹션에서는 OpenShift Cluster Manager Hybrid Cloud Console 의 요구 사항에 대해 설명합니다. CLI 툴을 독점적으로 사용하는 경우 요구 사항을 무시할 수 있습니다.

OpenShift Cluster Manager를 사용하려면 AWS 계정을 연결해야 합니다. 이러한 연결 개념은 계정 연관이라고도 합니다.

1.2.5.1. AWS 계정 연결

ROSA(Red Hat OpenShift Service on AWS) 클러스터 프로비저닝 작업을 수행하려면ARN(Amazon Resource Name)을 사용하여 **ocm -role 및 사용자** 역할 OpenShift Cluster Manager IAM 역할을 AWS 계정에 연결해야 합니다.

ocm-role ARN은 Red Hat 조직에 레이블로 저장되고 **사용자 역할** ARN은 Red Hat 사용자 계정 내부에 레이블로 저장됩니다. Red Hat은 이러한 ARN 라벨을 사용하여 사용자가 유효한 계정 소유자이고 올바른 권한을 사용하여 AWS 계정에서 필요한 작업을 수행할 수 있는지 확인합니다.

1.2.5.2. AWS 계정 연결

rosa CLI를 사용하여 AWS 계정을 기존 IAM 역할에 연결할 수 있습니다.

사전 요구 사항

- AWS 계정이 있습니다.
- OpenShift Cluster Manager Hybrid Cloud Console 을 사용하여 클러스터 생성
- AWS 계정 전체 역할을 설치하는 데 필요한 권한이 있습니다. 자세한 내용은 이 섹션의 "해결 리소스"를 참조하십시오.
- 설치 호스트에 최신 AWS(**aws**) 및 ROSA(**rosa**) CLI를 설치하고 구성했습니다.
- **ocm-role** 및 **user-role** IAM 역할을 생성했지만 아직 AWS 계정에 연결되지 않았습니다. 다음 명령을 실행하여 IAM 역할이 이미 연결되어 있는지 확인할 수 있습니다.

```
$ rosa list ocm-role
```

```
$ rosa list user-role
```

두 역할의 **Linked** 열에 **Yes** 가 표시되면 이미 역할을 AWS 계정에 연결한 것입니다.

절차

1. CLI에서 ARM(Amazon Resource Name)을 사용하여 **ocm-role** 리소스를 Red Hat 조직에 연결합니다.

참고

rosa link 명령을 실행하려면 Red Hat 조직 관리자 권한이 있어야 합니다. **ocm-role** 리소스를 AWS 계정과 연결하면 조직의 모든 사용자에게 표시됩니다.

```
$ rosa link ocm-role --role-arn <arn>
```

출력 예

```
I: Linking OCM role
? Link the '<AWS ACCOUNT ID>` role with organization '<ORG ID>'? Yes
I: Successfully linked role-arn '<AWS ACCOUNT ID>' with organization account '<ORG ID>'
```

2. CLI에서 ARM(Amazon Resource Name)을 사용하여 사용자 **역할** 리소스를 Red Hat 사용자 계정에 연결합니다.

```
$ rosa link user-role --role-arn <arn>
```

출력 예

```
I: Linking User role
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' role with
organization '<AWS ID>'? Yes
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125'
with organization account '<AWS ID>'
```

추가 리소스

- 클러스터 생성에 필요한 IAM 역할 목록은 계정 전체 IAM 역할 및 정책 참조 를 참조하십시오.

1.2.5.3. 여러 AWS 계정을 Red Hat 조직과 연결

여러 AWS 계정을 Red Hat 조직과 연결할 수 있습니다. 여러 계정을 연결하면 Red Hat 조직의 관련 AWS 계정에서 Red Hat OpenShift Service on AWS(ROSA) 클러스터를 생성할 수 있습니다.

이 기능을 사용하면 여러 AWS 프로필을 리전 바인딩 환경으로 사용하여 다양한 AWS 리전에서 클러스터를 생성할 수 있습니다.

사전 요구 사항

- AWS 계정이 있습니다.
- OpenShift Cluster Manager Hybrid Cloud Console 을 사용하여 클러스터 생성
- AWS 계정 전체 역할을 설치하는 데 필요한 권한이 있습니다.

- 설치 호스트에 최신 AWS(**aws**) 및 ROSA(**rosa**) CLI를 설치하고 구성했습니다.
- **ocm-role** 및 **사용자 역할 IAM 역할을** 생성했습니다.

절차

추가 AWS 계정을 연결하려면 먼저 로컬 AWS 구성에 프로필을 생성합니다. 그런 다음 추가 AWS 계정에 **ocm-role**, user, account 역할을 생성하여 계정을 Red Hat 조직과 연결합니다.

추가 리전에 역할을 생성하려면 **rosa create 명령을 실행할 때 --profile <aws-profile>** > 매개변수를 지정하고 < **aws_profile** >을 추가 계정 프로필 이름으로 교체합니다.

- OpenShift Cluster Manager 역할을 생성할 때 AWS 계정 프로필을 지정하려면 다음을 수행합니다.

```
$ rosa create --profile <aws_profile> ocm-role
```

- 사용자 역할을 생성할 때 AWS 계정 프로필을 지정하려면 다음을 수행합니다.

```
$ rosa create --profile <aws_profile> user-role
```

- 계정 역할을 생성할 때 AWS 계정 프로필을 지정하려면 다음을 수행합니다.

```
$ rosa create --profile <aws_profile> account-roles
```

참고

프로필을 지정하지 않으면 기본 AWS 프로필이 사용됩니다.

1.3. 옵트인 리전에 클러스터 배포 요구사항

AWS 옵트인 리전은 기본적으로 활성화되어 있지 않은 리전입니다. 옵트인 리전에서 AWS STS(보안 토큰 서비스)를 사용하는 AWS(ROSA) 클러스터에 Red Hat OpenShift Service를 배포하려면 다음 요구사항을 충족해야 합니다.

- AWS 계정에서 리전을 활성화해야 합니다. 옵트인 리전 활성화에 대한 자세한 내용은 AWS 문서의 AWS 리전 관리를 참조하십시오.
- AWS 계정의 보안 토큰 버전을 버전 2로 설정해야 합니다. 옵트인 리전에는 버전 1 보안 토큰을 사용할 수 없습니다.

중요

보안 토큰 버전 2로 업데이트하면 토큰 길이가 증가하여 토큰을 저장하는 시스템에 영향을 미칠 수 있습니다. 자세한 내용은 STS 기본 설정의 AWS 설명서를 참조하십시오.

1.3.1. AWS 보안 토큰 버전 설정

AWS 옵트인 리전에서 AWS Security Token Service(STS)를 사용하여 AWS(ROSA)의 Red Hat OpenShift Service 클러스터를 생성하려면 AWS 계정에서 보안 토큰 버전을 버전 2로 설정해야 합니다.

사전 요구 사항

- 설치 호스트에 최신 AWS CLI를 설치하고 구성했습니다.

절차

1. AWS CLI 구성에 정의된 AWS 계정의 ID를 나열합니다.

```
$ aws sts get-caller-identity --query Account --output json
```

출력이 관련 AWS 계정의 ID와 일치하는지 확인합니다.

2. AWS 계정에 설정된 보안 토큰 버전을 나열합니다.

```
$ aws iam get-account-summary --query SummaryMap.GlobalEndpointTokenVersion --
output json
```

출력 예

```
1
```

3. AWS 계정의 모든 리전에서 보안 토큰 버전을 버전 2로 업데이트하려면 다음 명령을 실행합니다.

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

중요

보안 토큰 버전 2로 업데이트하면 토큰 길이가 증가하여 토큰을 저장하는 시스템에 영향을 미칠 수 있습니다. 자세한 내용은 STS 기본 설정의 AWS 설명서를 참조하십시오.

1.4. AWS에 대한 RED HAT 관리 IAM 참조

STS 배포 모델을 사용하면 Red Hat은 더 이상 AWS(Amazon Web Services) IAM 정책, IAM 사용자 또는 IAM 역할을 생성 및 관리할 책임이 없습니다. 이러한 역할 및 정책 생성에 대한 자세한 내용은 IAM 역할에 대한 다음 섹션을 참조하십시오.

- **ocm** CLI를 사용하려면 **ocm-role** 및 **user-role** 리소스가 있어야 합니다. OpenShift Cluster Manager IAM 역할 리소스를 참조하십시오.
- 단일 클러스터가 있는 경우 계정 전체 IAM 역할 및 정책 참조 를 참조하십시오.
- 모든 클러스터에 필요한 Operator 역할이 있어야 합니다. Cluster-specific Operator IAM 역할 참조 를 참조하십시오.

1.5. 프로비저닝된 AWS 인프라

이는 배포된 Red Hat OpenShift Service on AWS(ROSA) 클러스터에 프로비저닝된 AWS(Amazon Web Services) 구성 요소에 대한 개요입니다. 프로비저닝된 모든 AWS 구성 요소의 자세한 목록은 OpenShift Container Platform 설명서 를 참조하십시오.

1.5.1. EC2 인스턴스

AWS EC2 인스턴스는 AWS 퍼블릭 클라우드에 ROSA의 컨트롤 플레인 및 데이터 플레인 기능을 배포하는 데 필요합니다.

인스턴스 유형은 작업자 노드 수에 따라 컨트롤 플레인 및 인프라 노드에 따라 다를 수 있습니다. 최소한 다음 EC2 인스턴스가 배포됩니다.

- 3개의 **m5.2xlarge** 컨트롤 플레인 노드
- **r5.xlarge** 인프라 노드 2개
- 2개의 **m5.xlarge** 사용자 정의 작업자 노드

작업자 노드 수에 대한 자세한 내용은 이 페이지의 "ECDHE 리소스" 섹션에 나열된 "Limits and scalability" 주제의 초기 계획 고려 사항에 대한 정보를 참조하십시오.

1.5.2. AWS EBS(Elastic Block Store) 스토리지

Amazon EBS 블록 스토리지는 로컬 노드 스토리지 및 영구 볼륨 스토리지 모두에 사용됩니다.

각 EC2 인스턴스의 볼륨 요구 사항:

- 컨트롤 플레인 볼륨
  - 크기: 350GB
  - 유형: io1
  - 초당 입력/출력 작업: 1000개
- 인프라 볼륨
  - 크기: 300GB
  - 유형: gp3
  - 초당 입력/출력 작업: 900
- 작업자 볼륨
  - 크기: 300GB
  - 유형: gp3
  - 초당 입력/출력 작업: 900

참고

OpenShift Container Platform 4.11 릴리스 전에 배포된 클러스터는 기본적으로 gp2 유형 스토리지를 사용합니다.

1.5.3. Elastic Load Balancing

API용 최대 두 개의 NLB(Network Load Balancer)와 애플리케이션 라우터용 최대 2개의 클래식 로드 밸런서(CLB)입니다. 자세한 내용은 AWS에 대한 ELB 설명서를 참조하십시오.

1.5.4. S3 스토리지

이미지 레지스트리는 AWS S3 스토리지에서 지원합니다. 리소스 정리는 S3 사용량 및 클러스터 성능을 최적화하기 위해 정기적으로 수행됩니다.

참고

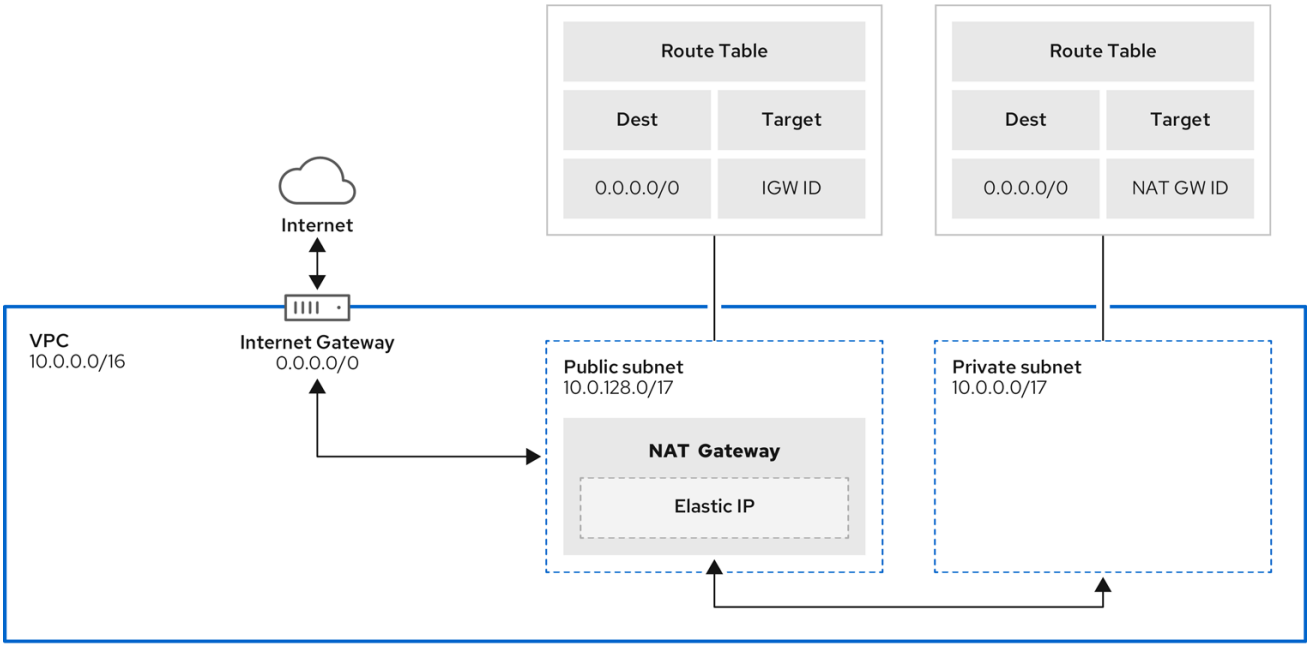
일반적인 크기가 2TB인 경우 각각 두 개의 버킷이 필요합니다.

1.5.5. VPC

고객은 클러스터당 하나의 VPC를 확인해야 합니다. 또한 VPC에는 다음 구성이 필요합니다.

- **서브넷: 단일 가용성 영역이 있는 클러스터의** 두 서브넷 또는 여러 가용성 영역이 있는 클러스터의 경우 6개의 서브넷입니다.
- **라우팅 테이블**: 프라이빗 서브넷당 하나의 라우팅 테이블과 클러스터당 하나의 추가 테이블입니다.
- **인터넷 게이트웨이**: 클러스터당 하나의 인터넷 게이트웨이.
- **NAT 게이트웨이**: 퍼블릭 서브넷당 하나의 NAT 게이트웨이.

1.5.5.1. 샘플 VPC 아키텍처



1.5.6. 보안 그룹

AWS 보안 그룹은 프로토콜 및 포트 액세스 수준의 보안을 제공하며 EC2 인스턴스 및 Elastic Load Balancer와 연결됩니다. 각 보안 그룹에는 EC2 인스턴스가 들어오고 나가는 트래픽을 필터링하는 규칙 세트가 포함되어 있습니다. 네트워크에서 OpenShift 설치에 필요한 포트가 열려 있고 호스트 간 액세스를 허용하도록 구성되어 있는지 확인해야 합니다.

그룹	유형	IP 프로토콜	포트 범위
MasterSecurityGroup	**AWS::EC2::SecurityGroup**	**icmp**	**0**
		tcp	**22**
		tcp	**6443**
		tcp	**22623**
WorkerSecurityGroup	**AWS::EC2::SecurityGroup**	**icmp**	**0**
		tcp	**22**
BootstrapSecurityGroup	**AWS::EC2::SecurityGroup**	**tcp**	**22**
		tcp	**19531**

1.6. AWS 방화벽 사전 요구 사항

중요

PrivateLink를 사용하여 배포된 ROSA 클러스터만 방화벽을 사용하여 송신 트래픽을 제어할 수 있습니다.

이 섹션에서는 AWS 클러스터의 Red Hat OpenShift Service에서 송신 트래픽을 제어하는 데 필요한 세부 정보를 제공합니다. 방화벽을 사용하여 송신 트래픽을 제어하는 경우 아래의 도메인 및 포트 조합에 대한 액세스 권한을 부여하도록 방화벽을 구성해야 합니다. AWS의 Red Hat OpenShift Service에는 완전히 관리되는 OpenShift 서비스를 제공하기 위해 이 액세스 권한이 필요합니다.

절차

1. 패키지 및 툴을 설치 및 다운로드하는 데 사용되는 다음 URL을 허용 목록에 추가하십시오.

domain	포트	함수
registry.redhat.io	443	코어 컨테이너 이미지를 제공합니다.
quay.io	443	코어 컨테이너 이미지를 제공합니다.
***.quay.io**	443	코어 컨테이너 이미지를 제공합니다.

domain	포트	함수
sso.redhat.com	443, 80	필수 항목입니다. **https://console.redhat.com/openshift** 사이트에서는 **sso.redhat.com** 의 인증을 사용하여 풀 시크릿을 다운로드하고 Red Hat SaaS 솔루션을 사용하여 서브스크립션, 클러스터 인벤토리, 예상 보고 등을 쉽게 모니터링할 수 있습니다.
quay-registry.s3.amazonaws.com	443	코어 컨테이너 이미지를 제공합니다.
ocm-quay-production-s3.s3.amazonaws.com	443	코어 컨테이너 이미지를 제공합니다.
quayio-production-s3.s3.amazonaws.com	443	코어 컨테이너 이미지를 제공합니다.
cart-rhcos-ci.s3.amazonaws.com	443	RHCOS(Red Hat Enterprise Linux CoreOS) 이미지를 제공합니다.
openshift.org	443	RHCOS(Red Hat Enterprise Linux CoreOS) 이미지를 제공합니다.
registry.access.redhat.com	443	개발자가 OpenShift 및 Kubernetes에서 빌드하는 데 도움이 되는 **odo** CLI 툴에 대한 액세스를 제공합니다.
console.redhat.com	443, 80	필수 항목입니다. 클러스터와 OpenShift Console Manager 간의 상호 작용을 통해 예약 업그레이드와 같은 기능을 활성화할 수 있습니다.
sso.redhat.com	443	**https://console.redhat.com/openshift** 사이트에서 **sso.redhat.com** 의 인증을 사용합니다.
pull.q1w2.quay.rhcloud.com	443	quay.io를 사용할 수 없는 경우 코어 컨테이너 이미지를 폴백으로 제공합니다.
.q1w2.quay.rhcloud.com	443	quay.io를 사용할 수 없는 경우 코어 컨테이너 이미지를 폴백으로 제공합니다.
www.okd.io	443	**openshift.org** 사이트는 **www.okd.io** 을 통해 리디렉션됩니다.
www.redhat.com	443, 80	**sso.redhat.com** 사이트는 **www.redhat.com** 을 통해 리디렉션됩니다.

domain	포트	함수
aws.amazon.com	443	**iam.amazonaws.com** 및 **sts.amazonaws.com** 사이트는 **aws.amazon.com** 을 통해 리디렉션됩니다.
catalog.redhat.com	443	**registry.access.redhat.com** 및 **https://registry.redhat.io** 사이트는 **catalog.redhat.com** 을 통해 리디렉션됩니다.

허용 목록에 **quay.io**와 같은 사이트를 추가할 때 ***.quay.io**와 같은 와일드카드 항목을 거부 목록에 추가하지 마십시오. 대부분의 경우 이미지 레지스트리는 CDN(Content deliver network)을 사용하여 이미지를 제공합니다. 방화벽 블록에 액세스하는 경우 초기 다운로드 요청이 **cdn01.quay.io**와 같은 호스트 이름에 리디렉션될 때 이미지 다운로드가 거부됩니다.

cdn01.quay.io 와 같은 CDN 호스트 이름은 허용 목록에 **.quay.io** 와 같은 와일드카드 항목을 추가할 때 적용됩니다.

2. 다음 Telemetry URL을 허용 목록에 추가합니다.

domain	포트	함수
cert-api.access.redhat.com	443	Telemetry에 필요합니다.
api.access.redhat.com	443	Telemetry에 필요합니다.
infogw.api.openshift.com	443	Telemetry에 필요합니다.
console.redhat.com	443	Telemetry 및 Red Hat Insights에 필요합니다.
observatorium.api.openshift.com	443	관리형 OpenShift별 Telemetry에 필요합니다.

관리형 클러스터를 사용하려면 Telemetry를 통해 Red Hat이 문제에 보다 신속하게 대응하고, 고객 지원을 개선하며, 제품 업그레이드가 클러스터에 미치는 영향을 보다 잘 이해할 수 있어야 합니다. Red Hat에서 원격 상태 모니터링 데이터를 사용하는 방법에 대한 자세한 내용은 원격 상태 모니터링 정보를 참조하십시오.

3. 다음 AWS(Amazon Web Services) API URls를 나열하십시오.

domain	포트	함수
.amazonaws.com	443	AWS 서비스 및 리소스에 액세스하는데 필요합니다.

또는 AWS(Amazon Web Services) API에 와일드카드를 사용하지 않도록 선택하는 경우 다음 URL을 허용해야 합니다.

domain	포트	함수
ec2.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다.
events.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다.
iam.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다.
route53.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다.
sts.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다.
tagging.us-east-1.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다. 이 끝점은 클러스터가 배포된 지역에 관계없이 항상 us-east-1입니다.
ec2.<aws_region>.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다.
elasticloadbalancing.<aws_region>.amazonaws.com	443	AWS 환경에서 클러스터를 설치하고 관리하는 데 사용됩니다.
servicequotas.<aws_region>.amazonaws.com	443, 80	필수 항목입니다. 서비스 배포에 대한 할당량을 확인하는 데 사용됩니다.
tagging.<aws_region>.amazonaws.com	443, 80	태그 형태로 AWS 리소스에 대한 메타데이터를 할당할 수 있습니다.

4. 다음 OpenShift URL을 허용 목록에 추가합니다.

domain	포트	함수
mirror.openshift.com	443	미러링된 설치 콘텐츠 및 이미지에 액세스하는 데 사용됩니다. 이 사이트는 릴리스 이미지 서명의 소스이기도 하지만 CVO(Cluster Version Operator)에는 단일 기능 소스만 필요합니다.
storage.googleapis.com/openshift-release (권장)	443	mirror.openshift.com/에 대한 대체 사이트입니다. 클러스터에서 사용하는 플랫폼 릴리스 서명을 다운로드하여 quay.io에서 가져올 이미지를 확인하는 데 사용됩니다.
api.openshift.com	443	클러스터에 사용 가능한 업데이트가 있는지 확인하는 데 사용됩니다.

domain	포트	함수

5. Allowlist the following site reliability engineering (SRE) 및 관리 URL:

domain	포트	함수
api.pagerduty.com	443	이 경고 서비스는 클러스터 내 alertmanager가 수행할 이벤트의 Red Hat SRE에 알리는 경고를 보내는 데 사용됩니다.
events.pagerduty.com	443	이 경고 서비스는 클러스터 내 alertmanager가 수행할 이벤트의 Red Hat SRE에 알리는 경고를 보내는 데 사용됩니다.
api.deadmanssnitch.com	443	AWS에서 Red Hat OpenShift Service에서 클러스터가 사용 가능하고 실행 중인지를 나타내는 주기적인 ping을 보내는 데 사용하는 경고 서비스입니다.
nosnch.in	443	AWS에서 Red Hat OpenShift Service에서 클러스터가 사용 가능하고 실행 중인지를 나타내는 주기적인 ping을 보내는 데 사용하는 경고 서비스입니다.
***.osdsecuritylogs.splunkcloud.comOR inputs1**.osdsecuritylogs.complunkcloud.comcom**inputs2.osdsecuritylogs.splunkcloud.cominputs4.osdsecuritylogs.splunkcloud.cominputs5.osdsecuritylogs.splunkcloud.cominputs6.osdsecuritylogs.splunkcloud.comsinputs.splunkcloud.com storeds.complunkcloud.com**	9997	**splunk-forwarder-operator** 에서 로그 기반 경고에 사용할 로깅 전달 끝점으로 사용합니다.
http-inputs-osdsecuritylogs.splunkcloud.com	443	필수 항목입니다. **splunk-forwarder-operator** 에서 로그 기반 경고에 사용할 로깅 전달 끝점으로 사용합니다.
SFTP.access.redhat.com (권장)	22	클러스터 문제를 해결하기 위해 진단 로그를 업로드하기 위해 **must-gather-operator** 에서 사용하는 SFTP 서버입니다.

6. AWS(Amazon Web Services) API에 와일드카드를 허용하지 않은 경우 내부 OpenShift 레지스트리에 사용된 S3 버킷도 허용해야 합니다. 해당 끝점을 검색하려면 클러스터가 성공적으로 프로비저닝된 후 다음 명령을 실행합니다.

```
$ oc -n openshift-image-registry get pod -l docker-registry=default -o json | jq
'.items[].spec.containers[].env[] | select(.name=="REGISTRY_STORAGE_S3_BUCKET")'
```

S3 끝점은 '<cluster-name>-<random-string>-image-registry-<cluster-region>-<random-string>.s3.dualstack.<cluster-region>.amazonaws.com 형식이어야 합니다.

7. 빌드에 필요한 언어 또는 프레임 워크에 대한 리소스를 제공하는 사이트를 허용 목록에 추가합니다.

8. OpenShift에 사용된 언어 및 프레임워크에 의존하는 아웃바운드 URL을 허용 목록에 추가합니다. 방화벽 또는 프록시에서 허용되는 권장 URL 목록은 OpenShift Outbound URL을 참조하십시오.

1.7. 다음 단계

- 필요한 AWS 서비스 할당량 검토

1.8. 추가 리소스

- AWS 클러스터의 모든 Red Hat OpenShift Service에 대한 SRE 액세스
- 애플리케이션의 사용자 정의 도메인 구성
- 인스턴스 유형

2장. OPENSHIFT CLUSTER MANAGER IAM 역할 리소스

Red Hat OpenShift Service on AWS (ROSA) 웹 UI를 사용하려면 OpenShift Cluster Manager Hybrid Cloud Console 및 **rosa** CLI(명령줄 인터페이스)에서 최종 사용자 환경을 제공하기 위해 신뢰 관계를 생성하는 AWS 계정에 대한 특정 권한이 있어야 합니다.

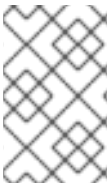
이러한 신뢰 관계가 **ocm-role** AWS IAM 역할의 생성 및 연관을 통해 이루어집니다. 이 역할에는 Red Hat 계정을 AWS 계정에 연결하는 AWS 설치 프로그램과의 신뢰 정책이 있습니다. 또한 이러한 **사용자를 식별하는 데 사용되는 각 웹 UI 사용자에 대한 사용자 역할** AWS IAM 역할도 필요합니다. 이 **사용자 역할** AWS IAM 역할에는 권한이 없습니다.

OpenShift Cluster Manager를 사용하는 데 필요한 AWS IAM 역할은 다음과 같습니다.

- **ocm-role**
- **user-role**

rosa CLI 또는 OpenShift Cluster Manager 웹 UI를 사용하여 클러스터를 관리하든, rosa CLI를 사용하여 **rosa** CLI에서 **account-roles** 라는 계정 전체 역할을 생성해야 합니다. 이러한 계정 역할은 첫 번째 클러스터에 필요하며 이러한 역할을 여러 클러스터에서 사용할 수 있습니다. 이러한 필수 계정 역할은 다음과 같습니다.

- **worker-Role**
- **support-Role**
- **installer-Role**
- **ControlPlane-Role**



참고

역할 생성에서는 AWS 액세스 또는 시크릿 키를 요청하지 않습니다. AWS STS(Security Token Service)는 이 워크플로의 기반으로 사용됩니다. AWS STS는 제한된 임시 자격 증명을 사용하여 인증을 제공합니다.

이러한 역할 생성에 대한 자세한 내용은 계정 전체 IAM 역할 및 정책 참조 를 참조하십시오.

rosa CLI에서 **operator-roles** 라고 하는 클러스터별 Operator 역할은 백엔드 스토리지, 수신 및 레지스트리 관리와 같은 클러스터 작업을 수행하는 데 필요한 임시 권한을 얻습니다. 이러한 역할은 사용자가 생성하는 클러스터에 필요합니다. 이러한 필수 Operator 역할은 다음과 같습니다.

- **<cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credentials**
- **<cluster_name>-<hash>-openshift-cloud-network-config-controller-credentials**
- **<cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials**
- **<cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-credentials**
- **<cluster_name>-<hash>-openshift-image-registry-installer-cloud-credentials**
- **<cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials**

이러한 역할 생성에 대한 자세한 내용은 클러스터별 Operator IAM 역할 참조 를 참조하십시오.

2.1. OCM-ROLE IAM 리소스 정보

ROSA 클러스터를 생성하려면 **ocm-role** IAM 리소스를 생성하여 Red Hat 사용자 조직을 활성화해야 합니다. AWS와의 연결 컨텍스트에서 Red Hat 조직은 OpenShift Cluster Manager 내의 단일 사용자입니다.

ocm-role IAM 리소스에 대한 몇 가지 고려 사항은 다음과 같습니다.

- Red Hat 조직당 하나의 **ocm-role** IAM 역할만 연결할 수 있지만 AWS 계정마다 여러 개의 **ocm-role** IAM 역할을 보유할 수 있습니다. 웹 UI를 사용하려면 이러한 역할 중 하나만 한 번에 연결할 수 있어야 합니다.
- Red Hat 조직의 모든 사용자는 **ocm-role** IAM 리소스를 생성하고 연결할 수 있습니다.
- Red Hat 조직 관리자만 **ocm-role** IAM 리소스의 연결을 해제할 수 있습니다. 이러한 제한은 다른 Red Hat 조직 멤버가 다른 사용자의 인터페이스 기능을 방해하지 않도록하기 위한 것입니다.

참고

기존 조직에 포함되지 않은 Red Hat 계정을 생성한 경우 이 계정도 Red Hat 조직 관리자입니다.

- 기본 및 관리자 **ocm-role** IAM 리소스에 대한 AWS 권한 정책 목록은 이 섹션의 추가 리소스에서 "OpenShift Cluster Manager 역할 이해"를 참조하십시오.

rosa CLI를 사용하면 이를 생성할 때 IAM 리소스를 연결할 수 있습니다.

참고

AWS 계정과 IAM 리소스를 "연결"하거나 "연결"한다는 것은 **ocm-role** IAM 역할 및 Red Hat OpenShift Cluster Manager AWS 역할로 trust-policy를 생성하는 것을 의미합니다. IAM 리소스를 생성 및 연결하면 **arn:aws:iam::7333:role/RH-Managed-OpenShift-Installer** 리소스와 함께 AWS의 **ocm-role** IAM 리소스에서 신뢰 관계가 표시됩니다.

Red Hat 조직 관리자가 **ocm-role** IAM 리소스를 생성하고 연결한 후에는 모든 조직 멤버가 고유한 **사용자 역할 IAM 역할을** 생성하고 연결할 수 있습니다. 이 IAM 리소스는 사용자당 한 번만 생성하고 연결해야 합니다. Red Hat 조직의 다른 사용자가 이미 **ocm-role** IAM 리소스를 생성하고 연결된 경우 자체 **user-role** IAM 역할을 생성하고 연결했는지 확인해야 합니다.

추가 리소스

- OpenShift Cluster Manager 역할 이해를 참조하십시오.

2.1.1. OpenShift Cluster Manager IAM 역할 생성

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

사전 요구 사항

- AWS 계정이 있습니다.
- OpenShift Cluster Manager 조직에 Red Hat 조직 관리자 권한이 있어야 합니다.
- AWS 계정 전체 역할을 설치하는 데 필요한 권한이 있습니다.
- 설치 호스트에 최신 AWS(**aws**) 및 ROSA(**rosa**) CLI를 설치하고 구성했습니다.

절차

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

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

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

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

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

출력 예

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

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

참고

--admin 옵션을 사용한 경우 이 프롬프트가 표시되지 않습니다.

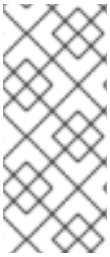
3. 권한 경계를 설정하는 정책의 Amazon 리소스 이름(ARN)입니다.
4. AWS 역할을 생성하는 방법을 선택합니다. **auto** 를 사용하면 **rosa** CLI 툴이 역할 및 정책을 생성하고 연결합니다. **자동** 모드에서는 AWS 역할을 생성하는 몇 가지 다른 프롬프트가 표시됩니다.
5. auto 방법은 접두사를 사용하여 특정 **ocm-role** 을 생성할지 여부를 요청합니다.
6. IAM 역할을 OpenShift Cluster Manager와 연결할지 확인합니다.
7. 생성된 역할을 AWS 조직과 연결합니다.

2.2. 사용자 역할 IAM 역할 정보

해당 **사용자가 ROSA 클러스터를 생성할 수 있도록 웹 UI 사용자당 사용자 역할** IAM 역할을 생성해야 합니다.

사용자 역할 IAM 역할에 대한 몇 가지 고려 사항은 다음과 같습니다.

- Red Hat **사용자 계정당 하나의 사용자 역할** IAM 역할만 필요하지만 Red Hat 조직에는 이러한 IAM 리소스가 많이 있을 수 있습니다.
- Red Hat 조직의 모든 사용자는 사용자 **역할 IAM 역할을** 생성하고 연결할 수 있습니다.
- Red Hat 조직당 AWS 계정당 다양한 **사용자 역할** IAM 역할이 있을 수 있습니다.
- Red Hat은 **사용자 역할** IAM 역할을 사용하여 사용자를 식별합니다. 이 IAM 리소스에는 AWS 계정 권한이 없습니다.
- AWS 계정에는 여러 **사용자 역할 IAM 역할이** 있을 수 있지만 각 IAM 역할을 Red Hat 조직의 각 사용자에게 연결해야 합니다. 어떤 사용자는 두 개 이상의 연결된 **사용자 역할 IAM 역할을** 가질 수 없습니다.



참고

AWS 계정과 IAM 리소스를 "연결"하거나 "연결"한다는 것은 **사용자 역할 IAM 역할** 및 Red Hat OpenShift Cluster Manager AWS 역할로 신뢰 정책을 생성하는 것을 의미합니다. 이 IAM 리소스를 생성하고 연결한 후 AWS의 **사용자 역할** IAM 역할에서 **arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer** 리소스를 사용하여 신뢰 관계가 표시됩니다.

2.2.1. 사용자 역할 IAM 역할 생성

CLI(명령줄 인터페이스)를 사용하여 OpenShift Cluster Manager IAM 역할을 생성할 수 있습니다.

사전 요구 사항

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

절차

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

```
$ rosa create user-role
```

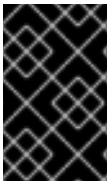
이 명령을 사용하면 특정 특성을 지정하여 역할을 생성할 수 있습니다. 다음 예제 출력에서는 로사 CLI에서 Operator 역할 및 정책을 생성할 **수** 있는 "자동 모드"를 보여줍니다. 자세한 내용은 추가 리소스의 "자동 및 수동 배포 모드 이해"를 참조하십시오.

출력 예

```
I: Creating User role
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
```

```
? Role creation mode: auto 3
I: Creating ocm user role using 'arn:aws:iam::2066:user'
? Create the 'ManagedOpenShift-User.osdocs-Role' role? Yes 4
I: Created role 'ManagedOpenShift-User.osdocs-Role' with ARN
'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role'
I: Linking User role
? User Role ARN: arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role
? Link the 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' role with account '1AGE'?
Yes 5
I: Successfully linked role ARN 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' with
account '1AGE'
```

1. 생성된 모든 AWS 리소스의 접두사 값입니다. 이 예제에서 **ManagedOpenShift** 는 모든 AWS 리소스 앞에 추가합니다.
2. 권한 경계를 설정하는 정책의 Amazon 리소스 이름(ARN)입니다.
3. AWS 역할을 생성하는 방법을 선택합니다. **auto** 를 사용하여 **rosa** CLI 툴에서 역할을 생성하고 AWS 계정에 연결합니다. **자동** 모드에서는 AWS 역할을 생성하는 몇 가지 다른 프롬프트가 표시됩니다.
4. auto 방법은 접두사를 사용하여 특정 **사용자 역할을** 생성할지 여부를 요청합니다.
5. 생성된 역할을 AWS 조직과 연결합니다.



중요

클러스터를 삭제하기 전에 **사용자 역할 IAM 역할을** 연결 해제하거나 삭제하면 클러스터를 삭제할 수 없습니다. 삭제 프로세스를 진행하려면 이 역할을 생성하거나 다시 연결해야 합니다. 자세한 내용은 삭제할 수 없는 클러스터를 참조하십시오.

2.3. AWS 계정 연결

ROSA(Red Hat OpenShift Service on AWS) 클러스터 프로비저닝 작업을 수행하려면ARN(Amazon Resource Name)을 사용하여 **ocm -role 및 사용자** 역할 OpenShift Cluster Manager IAM 역할을 AWS 계정에 연결해야 합니다.

ocm-role ARN은 Red Hat 조직에 레이블로 저장되고 **사용자 역할** ARN은 Red Hat 사용자 계정 내부에 레이블로 저장됩니다. Red Hat은 이러한 ARN 라벨을 사용하여 사용자가 유효한 계정 소유자이고 올바른 권한을 사용하여 AWS 계정에서 필요한 작업을 수행할 수 있는지 확인합니다.

2.3.1. AWS 계정 연결

rosa CLI를 사용하여 AWS 계정을 기존 IAM 역할에 연결할 수 있습니다.

사전 요구 사항

- AWS 계정이 있습니다.
- OpenShift Cluster Manager Hybrid Cloud Console 을 사용하여 클러스터 생성
- AWS 계정 전체 역할을 설치하는 데 필요한 권한이 있습니다. 자세한 내용은 이 섹션의 "해결 리소스"를 참조하십시오.
- 설치 호스트에 최신 AWS(**aws**) 및 ROSA(**rosa**) CLI를 설치하고 구성했습니다.

- **ocm-role** 및 **user-role** IAM 역할을 생성했지만 아직 AWS 계정에 연결되지 않았습니다. 다음 명령을 실행하여 IAM 역할이 이미 연결되어 있는지 확인할 수 있습니다.

```
$ rosa list ocm-role
```

```
$ rosa list user-role
```

두 역할의 **Linked** 열에 **Yes** 가 표시되면 이미 역할을 AWS 계정에 연결한 것입니다.

절차

1. CLI에서 ARM(Amazon Resource Name)을 사용하여 **ocm-role** 리소스를 Red Hat 조직에 연결합니다.

참고

rosa link 명령을 실행하려면 Red Hat 조직 관리자 권한이 있어야 합니다. **ocm-role** 리소스를 AWS 계정과 연결하면 조직의 모든 사용자에게 표시됩니다.

```
$ rosa link ocm-role --role-arn <arn>
```

출력 예

```
I: Linking OCM role
? Link the '<AWS ACCOUNT ID>` role with organization '<ORG ID>'? Yes
I: Successfully linked role-arn '<AWS ACCOUNT ID>' with organization account '<ORG ID>'
```

2. CLI에서 ARM(Amazon Resource Name)을 사용하여 사용자 **역할** 리소스를 Red Hat 사용자 계정에 연결합니다.

```
$ rosa link user-role --role-arn <arn>
```

출력 예

```
I: Linking User role
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' role with
organization '<AWS ID>'? Yes
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125'
with organization account '<AWS ID>'
```

2.3.2. 여러 AWS 계정을 Red Hat 조직과 연결

여러 AWS 계정을 Red Hat 조직과 연결할 수 있습니다. 여러 계정을 연결하면 Red Hat 조직의 관련 AWS 계정에서 Red Hat OpenShift Service on AWS(ROSA) 클러스터를 생성할 수 있습니다.

이 기능을 사용하면 여러 AWS 프로필을 리전 바인딩 환경으로 사용하여 다양한 AWS 리전에서 클러스터를 생성할 수 있습니다.

사전 요구 사항

- AWS 계정이 있습니다.

- OpenShift Cluster Manager Hybrid Cloud Console 을 사용하여 클러스터 생성
- AWS 계정 전체 역할을 설치하는 데 필요한 권한이 있습니다.
- 설치 호스트에 최신 AWS(**aws**) 및 ROSA(**rosa**) CLI를 설치하고 구성했습니다.
- **ocm-role** 및 **사용자 역할 IAM 역할을** 생성했습니다.

절차

추가 AWS 계정을 연결하려면 먼저 로컬 AWS 구성에 프로필을 생성합니다. 그런 다음 추가 AWS 계정에 **ocm-role**, user, account 역할을 생성하여 계정을 Red Hat 조직과 연결합니다.

추가 리전에 역할을 생성하려면 **rosa create 명령을 실행할 때 --profile <aws-profile>** > 매개변수를 지정하고 < **aws_profile** >을 추가 계정 프로필 이름으로 교체합니다.

- OpenShift Cluster Manager 역할을 생성할 때 AWS 계정 프로필을 지정하려면 다음을 수행합니다.

```
$ rosa create --profile <aws_profile> ocm-role
```

- 사용자 역할을 생성할 때 AWS 계정 프로필을 지정하려면 다음을 수행합니다.

```
$ rosa create --profile <aws_profile> user-role
```

- 계정 역할을 생성할 때 AWS 계정 프로필을 지정하려면 다음을 수행합니다.

```
$ rosa create --profile <aws_profile> account-roles
```

참고

프로필을 지정하지 않으면 기본 AWS 프로필이 사용됩니다.

2.4. 추가 리소스

- IAM 역할 문제 해결 참조
- 클러스터 생성에 필요한 IAM 역할 목록은 계정 전체 IAM 역할 및 정책 참조 를 참조하십시오.

3장. 제한 및 확장성

이 문서에서는 ROSA(Red Hat OpenShift Service on AWS) 클러스터의 테스트된 클러스터 최대값과 최대값 테스트에 사용되는 테스트 환경 및 구성에 대한 정보를 자세히 설명합니다. 컨트롤 플레인 및 인프라 노드 크기 조정 및 스케일링에 대한 정보도 제공됩니다.

3.1. ROSA 테스트된 클러스터 최대값

ROSA(Red Hat OpenShift Service on AWS) 클러스터 설치를 계획하는 경우 다음과 같은 테스트된 오브젝트 최대값을 고려하십시오. 테이블은 (ROSA) 클러스터에서 테스트된 각 유형에 대한 최대 제한을 지정합니다.

이러한 지침은 다중 가용성 영역 구성의 102 컴퓨팅 노드 (작업자라고도 함)의 클러스터를 기반으로 합니다. 크기가 작은 클러스터의 경우 최대값이 더 낮습니다.

참고

모든 테스트에 사용되는 OpenShift Container Platform 버전은 OCP 4.8.0입니다.

표 3.1. 테스트된 클러스터 최대값

최대값 유형	4.8 테스트된 최대값
노드 수	102
Pod 수 [1]	20,400
노드당 Pod 수	250
코어당 Pod 수	기본값이 없습니다.
네임스페이스 수 [2]	3,400
네임스페이스당 Pod 수 [3]	20,400
서비스 수 [4]	10,000
네임스페이스당 서비스 수	10,000
서비스당 백엔드 수	10,000
네임스페이스당 배포 수 [3]	1,000

1. 여기에 표시된 Pod 수는 테스트 Pod 수입니다. 실제 Pod 수는 애플리케이션 메모리, CPU 및 스토리지 요구사항에 따라 달라집니다.

2. 활성 프로젝트 수가 많은 경우 키 공간이 지나치게 커져서 공간 할당량을 초과하면 etcd 성능이 저하될 수 있습니다. etcd 스토리지를 사용할 수 있도록 조각 모음을 포함하여 etcd를 정기적으로 유지보수하는 것이 좋습니다.

3. 시스템에는 일부 상태 변경에 대한 대응으로 지정된 네임스페이스의 모든 오브젝트에서 반복해야 하는 컨트롤 루프가 많습니다. 단일 네임스페이스에 형식의 오브젝트가 많으면 루프 비용이 많이 들고 상태 변경 처리 속도가 느려질 수 있습니다. 이 제한을 적용하면 애플리케이션 요구사항을 충족하기에 충분한 CPU, 메모리 및 디스크가 시스템에 있다고 가정합니다.

4. 각 서비스 포트와 각 서비스 백엔드는 iptables에 해당 항목이 있습니다. 지정된 서비스의 백엔드 수는 끝점 오브젝트의 크기에 영향을 미치므로 시스템 전체에서 전송되는 데이터의 크기에 영향을 미칩니다.

OpenShift Container Platform 4.8에서는 CPU 코어의 절반(500밀리코어)이 이전 버전의 OpenShift Container Platform과 비교하여 시스템에 의해 예약되어 있습니다.

3.2. OPENSHIFT CONTAINER PLATFORM 테스트 환경 및 구성

다음 표에는 AWS 클라우드 플랫폼에서 클러스터 최대값을 테스트하는 OpenShift Container Platform 환경 및 구성이 나열되어 있습니다.

노드	유형	vCPU	RAM(GiB)	디스크 유형	디스크 크기(GiB)/IOPS	수량	리전
컨트롤 플레인/etcd [1]	m5.4xlarge	16	64	io1	350 / 1,000	3	us-west-2
인프라 노드 [2]	r5.2xlarge	8	64	gp3	300 / 900	3	us-west-2
워크로드 [3]	m5.2xlarge	8	32	gp3	350 / 900	3	us-west-2
컴퓨팅 노드	m5.2xlarge	8	32	gp3	350 / 900	102	us-west-2

1. etcd는 I/O 집약적이고 대기 시간에 민감하기 때문에 io1 디스크는 컨트롤 플레인/etcd 노드에 사용됩니다. 사용량에 따라 더 많은 수의 IOPS가 필요할 수 있습니다.

2. Prometheus는 사용 패턴에 따라 대량의 메모리를 요청할 수 있기 때문에 인프라 노드는 모니터링 구성 요소를 호스팅하는 데 사용됩니다.

3. 워크로드 노드는 성능 및 확장 가능한 워크로드 생성기 실행 전용입니다.

더 큰 클러스터 크기 및 오브젝트 수가 많을 수 있습니다. 그러나 인프라 노드의 크기 조정에서는 Prometheus에서 사용할 수 있는 메모리 양을 제한합니다. 오브젝트를 생성, 수정 또는 삭제할 때 Prometheus는 디스크의 지표를 유지하기 위해 약 3시간 동안 해당 메모리에 지표를 저장합니다. 오브젝트 생성, 수정 또는 삭제 비율이 너무 높으면 메모리 리소스가 부족하여 Prometheus가 압도되고 실패할 수 있습니다.

3.3. 컨트롤 플레인 및 인프라 노드 크기 조정 및 스케일링

ROLE(Red Hat OpenShift Service on AWS) 클러스터를 설치하면 컴퓨팅 노드 수에 따라 컨트롤 플레인 및 인프라 노드의 크기 조정이 자동으로 결정됩니다.

설치 후 클러스터의 컴퓨팅 노드 수를 변경하면 Red Hat site Reliability Engineering(SRE) 팀이 클러스터의 안정성을 유지하기 위해 필요에 따라 컨트롤 플레인 및 인프라 노드를 스케일링합니다.

3.3.1. 설치 중 노드 크기 조정

설치 프로세스 중에 컨트롤 플레인 및 인프라 노드의 크기 조정이 동적으로 계산됩니다. 크기 조정 계산은 클러스터의 컴퓨팅 노드 수를 기반으로 합니다.

다음 표에는 설치 중에 적용되는 컨트롤 플레인 및 인프라 노드 크기 조정이 나열되어 있습니다.

컴퓨팅 노드 수	컨트롤 플레인 크기	인프라 노드 크기
1~25	m5.2xlarge	r5.xlarge
26~100	m5.4xlarge	r5.2xlarge
101 ~ 180 [1]	m5.8xlarge	r5.4xlarge

1. ROSA의 최대 컴퓨팅 노드 수는 180입니다.

3.3.2. 설치 후 노드 스케일링

설치 후 컴퓨팅 노드 수를 변경하면 필요에 따라 컨트롤 플레인 및 인프라 노드가 Red Hat SRE(Site Reliability Engineering) 팀에 의해 확장됩니다. 플랫폼의 안정성을 유지하기 위해 노드가 확장됩니다.

컨트롤 플레인 및 인프라 노드에 대한 설치 후 확장 요구 사항은 사례별로 평가됩니다. 노드 리소스 사용 및 수신 경고가 고려됩니다.

컨트롤 플레인 노드 크기 조정 경고 규칙

다음 시나리오 중 하나가 true인 경우 클러스터의 컨트롤 플레인 노드에 대해 경고 크기 조정이 트리거됩니다.

- 각 컨트롤 플레인 노드에는 16GiB 이상의 RAM이 있으며 컴퓨팅 노드는 25개 미만이며, 101개 미만의 컴퓨팅 노드가 있습니다.
- 각 컨트롤 플레인 노드에는 32GiB 이상의 RAM이 있으며 컴퓨팅 노드가 100개 이상 있습니다.

참고

ROSA의 최대 컴퓨팅 노드 수는 180입니다.

인프라 노드 크기 조정 경고 규칙

다음 시나리오 중 하나가 true인 경우 클러스터의 인프라 노드에 대해 경고 크기 조정이 트리거됩니다.

- 각 인프라 노드에는 16GiB 이상의 RAM 또는 CPU가 5개 미만이며, 컴퓨팅 노드는 25개 미만의 계산 노드가 있습니다.

- 각 인프라 노드에는 32GiB RAM 또는 9개 미만의 CPU가 있으며 컴퓨팅 노드가 100개 이상 있습니다.

참고

ROSA의 최대 컴퓨팅 노드 수는 180입니다.

예를 들어 노드의 리소스 사용량 증가를 관리하기 위해 SRE 팀은 추가 이유로 컨트롤 플레인 및 인프라 노드를 확장할 수 있습니다.

스케일링을 적용하면 서비스 로그 항목을 통해 고객에게 알립니다. 서비스 로그에 대한 자세한 내용은 *ROSA 클러스터에 대한 서비스 로그* 액세스를 참조하십시오.

3.3.3. 대규모 클러스터 크기 조정

대규모 클러스터의 경우 인프라 노드 크기 조정이 확장성에 큰 영향을 미칠 수 있습니다. etcd 버전 또는 스토리지 데이터 형식을 비롯하여 명시된 임계값에 영향을 주는 요인은 여러 가지가 있습니다.

이러한 제한을 초과해도 클러스터가 실패할 수 있음을 나타내는 것은 아닙니다. 대부분의 경우 이러한 수치를 초과하면 전체 성능이 저하됩니다.

3.4. 다음 단계

- 환경 계획

3.5. 추가 리소스

- ROSA 클러스터의 서비스 로그에 액세스

4장. 환경 계획

4.1. 테스트된 클러스터 최대값을 기반으로 환경 계획

이 문서에서는 테스트된 클러스터 최대값을 기반으로 AWS 환경에서 Red Hat OpenShift Service를 계획하는 방법을 설명합니다.

노드에서 물리적 리소스에 대한 서브스크립션을 초과하면 Pod를 배치하는 동안 Kubernetes 스케줄러가 보장하는 리소스에 영향을 미칩니다. 메모리 교체가 발생하지 않도록 하기 위해 수행할 수 있는 조치를 알아보십시오.

테스트된 최대값 중 일부는 단일 차원에서만 확장됩니다. 클러스터에서 실행되는 오브젝트가 많으면 최대값이 달라집니다.

이 문서에 명시된 수치는 Red Hat 테스트 방법론, 설정, 구성 및 튜닝을 기반으로 합니다. 고유한 개별 설정 및 환경에 따라 수치가 달라질 수 있습니다.

환경을 계획하는 동안 다음 공식을 사용하여 노드당 적합할 것으로 예상되는 Pod 수를 결정합니다.

```
required pods per cluster / pods per node = total number of nodes needed
```

노드당 최대 Pod 수는 현재 250입니다. 하지만 노드에 적합한 Pod 수는 애플리케이션 자체에 따라 달라집니다. 애플리케이션 요구 사항에 *따라 환경 계획에 설명된 대로 애플리케이션의 메모리, CPU 및 스토리지 요구 사항을* 고려하십시오.

시나리오 예

클러스터당 2200개의 Pod로 클러스터 범위를 지정하려면 노드당 최대 250개의 Pod가 있다고 가정하여 최소 9개의 노드가 있어야 합니다.

```
2200 / 250 = 8.8
```

노드 수를 20으로 늘리면 Pod 배포는 노드당 110개 Pod로 변경됩니다.

```
2200 / 20 = 110
```

다음과 같습니다.

```
required pods per cluster / total number of nodes = expected pods per node
```

4.2. 애플리케이션 요구 사항에 따라 환경 계획

이 문서에서는 애플리케이션 요구 사항에 따라 Red Hat OpenShift Service를 AWS 환경에서 계획하는 방법을 설명합니다.

예에 나온 애플리케이션 환경을 고려해 보십시오.

Pod 유형	Pod 수량	최대 메모리	CPU 코어 수	영구 스토리지
apache	100	500MB	0.5	1GB

Pod 유형	Pod 수량	최대 메모리	CPU 코어 수	영구 스토리지
node.js	200	1GB	1	1GB
postgresql	100	1GB	2	10GB
JBoss EAP	100	1GB	1	1GB

예상 요구 사항: CPU 코어 550개, RAM 450GB 및 스토리지 1.4TB입니다.

노드의 인스턴스 크기는 기본 설정에 따라 높게 또는 낮게 조정될 수 있습니다. 노드에서는 리소스 초과 커밋이 발생하는 경우가 많습니다. 이 배포 시나리오에서는 동일한 양의 리소스를 제공하는 데 더 작은 노드를 추가로 실행하도록 선택할 수도 있고 더 적은 수의 더 큰 노드를 실행하도록 선택할 수도 있습니다. 운영 민첩성 및 인스턴스당 비용과 같은 요인을 고려해야 합니다.

노드 유형	수량	CPU	RAM(GB)
노드(옵션 1)	100	4	16
노드(옵션 2)	50	8	32
노드(옵션 3)	25	16	64

어떤 애플리케이션은 초과 커밋된 환경에 적합하지만 어떤 애플리케이션은 그렇지 않습니다. 대부분의 Java 애플리케이션과 대규모 페이지를 사용하는 애플리케이션은 초과 커밋에 적합하지 않은 애플리케이션의 예입니다. 해당 메모리는 다른 애플리케이션에 사용할 수 없습니다. 위의 예에 나온 환경에서는 초과 커밋이 약 30%이며, 이는 일반적으로 나타나는 비율입니다.

애플리케이션 Pod는 환경 변수 또는 DNS를 사용하여 서비스에 액세스할 수 있습니다. 환경 변수를 사용하는 경우 노드에서 Pod가 실행될 때 활성 서비스마다 kubelet을 통해 변수를 삽입합니다. 클러스터 인식 DNS 서버는 새로운 서비스의 Kubernetes API를 확인하고 각각에 대해 DNS 레코드 세트를 생성합니다. 클러스터 전체에서 DNS가 활성화된 경우 모든 Pod가 자동으로 해당 DNS 이름을 통해 서비스를 확인할 수 있어야 합니다. 서비스가 5,000개를 넘어야 하는 경우 DNS를 통한 서비스 검색을 사용할 수 있습니다. 서비스 검색에 환경 변수를 사용하는 경우 네임스페이스에서 서비스가 5000개 이후에 인수 목록이 허용된 길이를 초과하면 Pod 및 배포가 실패하기 시작합니다.

이 문제를 해결하려면 배포의 서비스 사양 파일에서 서비스 링크를 비활성화하십시오.

예제

```
Kind: Template
apiVersion: template.openshift.io/v1
metadata:
  name: deploymentConfigTemplate
  creationTimestamp:
  annotations:
    description: This template will create a deploymentConfig with 1 replica, 4 env vars and a service.
    tags: ''
objects:
  - kind: DeploymentConfig
    apiVersion: apps.openshift.io/v1
```

```
  metadata:
    name: deploymentconfig${IDENTIFIER}
  spec:
    template:
      metadata:
        labels:
          name: replicationcontroller${IDENTIFIER}
      spec:
        enableServiceLinks: false
        containers:
        - name: pause${IDENTIFIER}
          image: "${IMAGE}"
          ports:
          - containerPort: 8080
            protocol: TCP
          env:
          - name: ENVVAR1_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR2_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR3_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR4_${IDENTIFIER}
            value: "${ENV_VALUE}"
          resources: {}
          imagePullPolicy: IfNotPresent
          capabilities: {}
          securityContext:
            capabilities: {}
            privileged: false
        restartPolicy: Always
        serviceAccount: ''
    replicas: 1
    selector:
      name: replicationcontroller${IDENTIFIER}
    triggers:
    - type: ConfigChange
    strategy:
      type: Rolling
- kind: Service
  apiVersion: v1
  metadata:
    name: service${IDENTIFIER}
  spec:
    selector:
      name: replicationcontroller${IDENTIFIER}
    ports:
    - name: serviceport${IDENTIFIER}
      protocol: TCP
      port: 80
      targetPort: 8080
    portalIP: ''
    type: ClusterIP
    sessionAffinity: None
  status:
    loadBalancer: {}
```

```
  parameters:
  - name: IDENTIFIER
    description: Number to append to the name of resources
    value: '1'
    required: true
  - name: IMAGE
    description: Image to use for deploymentConfig
    value: gcr.io/google-containers/pause-amd64:3.0
    required: false
  - name: ENV_VALUE
    description: Value to use for environment variables
    generate: expression
    from: "[A-Za-z0-9]{255}"
    required: false
  labels:
template: deploymentConfigTemplate
```

네임스페이스에서 실행할 수 있는 애플리케이션 Pod 수는 서비스 검색에 환경 변수가 사용될 때 서비스 수와 서비스 이름의 길이에 따라 달라집니다. **ARG_MAX** 는 새로운 프로세스의 최대 인수 길이를 정의하고 기본적으로 2097152바이트(2MiB)로 설정됩니다. kubelet은 네임스페이스에서 실행되도록 예약된 각 Pod에 환경 변수를 삽입합니다.

- **<SERVICE_NAME>_SERVICE_HOST=<IP>**
- **<SERVICE_NAME>_SERVICE_PORT=<PORT>**
- **<SERVICE_NAME>_PORT=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PROTO=tcp**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PORT=<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_ADDR=<ADDR>**

인수 길이가 허용된 값을 초과하고 서비스 이름의 문자 수에 영향을 미치는 경우 네임스페이스의 Pod가 실패합니다.

5장. 필수 AWS 서비스 할당량

AWS 클러스터에서 Red Hat OpenShift Service를 실행하는 데 필요한 필수 AWS(Amazon Web Service) 서비스 할당량 목록을 검토합니다.

5.1. 필수 AWS 서비스 할당량

아래 표는 AWS 클러스터에서 Red Hat OpenShift Service를 생성하고 실행하는 데 필요한 AWS 서비스 할당량 및 수준을 설명합니다.

참고

AWS SDK를 사용하면 ROSA에서 할당량을 확인할 수 있지만 AWS SDK 계산에서는 기존 사용량을 고려하지 않습니다. 따라서 할당량 검사가 AWS SDK에 전달할 수 있지만 클러스터 생성에 실패할 수 있습니다. 이 문제를 해결하려면 할당량을 늘립니다.

특정 할당량을 수정하거나 늘려야 하는 경우 할당량 증가를 요청하는 Amazon 문서를 참조하십시오. 대규모 할당량 요청은 검토를 위해 Amazon 지원에 제출되며 승인되는 데 시간이 다소 걸립니다. 할당량 요청이 긴급하면 AWS 지원에 문의하십시오.

중요

온 디맨드 표준(A, C, D, H, I, M, R, T, Z) Amazon EC2 인스턴스의 경우 ROSA 클러스터를 생성하려면 100개의 vCPU 이상이 필요합니다. 할당량을 늘리려면 AWS 콘솔에서 Service Quotas 콘솔을 엽니다.

표 5.1. ROSA-required 서비스 할당량

할당량 이름	서비스 코드	할당량 코드	Default	최소 요구 사항	설명
온 디맨드 표준 실행 (A, C, D, H, I, M, R, T, Z) 인스턴스 실행	ec2	L-1216C47A	100	100	실행 중인 온 디맨드 표준(A, C, D, H, I, M, R, T, Z) 인스턴스에 할당된 최대 vCPU 수입니다. ROSA 클러스터를 생성하기 위해 vCPU 5개의 값으로는 충분하지 않습니다. ROSA에는 클러스터 생성을 위해 최소 100개의 vCPU가 필요합니다.

할당량 이름	서비스 코드	할당량 코드	Default	최소 요구 사항	설명
TiB의 범용 SSD(gp2) 볼륨 스토리지용 스토리지	EBS	L-D18FCD1D	50	300	이 리전의 일반 용도 SSD(gp2) 볼륨에서 프로비저닝할 수 있는 최대 집계된 스토리지 양입니다.
TiB의 범용 SSD(gp3) 볼륨 스토리지용 스토리지	EBS	L-7A658B76	50	300	이 리전의 일반 용도 SSD(gp3) 볼륨에서 프로비저닝할 수 있는 최대 집계된 스토리지 양입니다. 300TiB의 스토리지는 최적의 성능을 위해 필요한 최소 용량입니다.
TiB에서 프로비저닝된 IOPS SSD(io1) 볼륨의 스토리지	EBS	L-FD252861	50	300	이 리전에서 프로비저닝된 IOPS SSD(io1) 볼륨에서 프로비저닝할 수 있는 최대 집계된 스토리지 양입니다. 300TiB의 스토리지는 최적의 성능을 위해 필요한 최소 용량입니다.

표 5.2. 일반 AWS 서비스 할당량

할당량 이름	서비스 코드	할당량 코드	Default	최소 요구 사항	설명
EC2-VPC Elastic IPs	ec2	L-0263D0A3	5	5	이 리전에서 EC2-VPC에 할당할 수 있는 최대 Elastic IP 주소 수입니다.

할당량 이름	서비스 코드	할당량 코드	Default	최소 요구 사항	설명
리전당 VPC	vpc	L-F678F1CE	5	5	리전당 최대 VPC 수입니다. 이 할당량은 리전당 최대 인터넷 게이트웨이 수에 직접 연결됩니다.
리전당 인터넷 게이트웨이	vpc	L-A4707A72	5	5	리전당 최대 인터넷 게이트웨이 수입니다. 이 할당량은 리전당 최대 VPC 수에 직접 연결됩니다. 이 할당량을 늘리려면 리전당 VPC 수를 늘립니다.
리전당 네트워크 인터페이스	vpc	L-DF5E4CA3	5,000	5,000	리전당 최대 네트워크 인터페이스 수입니다.
리전당 스냅샷	EBS	L-309BACF6	10,000	10,000	리전당 최대 스냅샷 수
프로비저닝된 IOPS SSD(Io1) 볼륨의 IOPS	EBS	L-B3A130E6	300,000	300,000	이 리전의 프로비저닝된 IOPS SDD(io1) 볼륨에서 프로비저닝할 수 있는 최대 집계된 IOPS 수입니다.
리전당 애플리케이션 로드 밸런서	elasticloadbalancing	L-53DA6B97	50	50	
리전당 클래식 로드 밸런서	elasticloadbalancing	L-E9E9831D	20	20	

5.1.1. 추가 리소스

- AWS CLI 명령을 사용하여 서비스 할당량을 요청, 보기 및 관리하려면 어떻게 요청을 늘릴 수 있습니까?
- ROSA 서비스 할당량
- 할당량 증가 요청

5.2. 다음 단계

- 환경 설정 및 ROSA 설치

6장. STS를 사용하도록 환경 설정

AWS 사전 요구 사항을 충족한 후 환경을 설정하고 AWS(ROSA)에 Red Hat OpenShift Service를 설치합니다.

작은 정보

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

6.1. STS를 위한 환경 설정

AWS STS(Security Token Service)를 사용하는 ROLE(Red Hat OpenShift Service on AWS) 클러스터를 생성하기 전에 다음 단계를 완료하여 환경을 설정합니다.

사전 요구 사항

- 배포 사전 요구 사항 및 정책을 검토하고 완료합니다.
- 아직 없는 경우 Red Hat 계정을 생성합니다. 그런 다음 이메일에서 확인 링크를 확인하십시오. ROSA를 설치하려면 이러한 인증 정보가 필요합니다.

절차

1. 사용하려는 AWS(Amazon Web Services) 계정에 로그인합니다.
   프로덕션 클러스터를 실행하려면 전용 AWS 계정을 사용하는 것이 좋습니다. AWS 조직을 사용하는 경우 조직 내에서 AWS 계정을 사용하거나 새 조직을 생성할 수 있습니다.

   AWS 조직을 사용하고자 하는 AWS 계정에 서비스 제어 정책(SCP)을 적용해야 하는 경우 이러한 정책은 클러스터에 필요한 역할 및 정책보다 제한적이지 않아야 합니다.

2. AWS 관리 콘솔에서 ROSA 서비스를 활성화합니다.

   a. AWS 계정에 로그인합니다.

   b. ROSA를 활성화하려면 ROSA 서비스로 이동하여 **OpenShift 사용을** 선택합니다.
   https://console.aws.amazon.com/rosa/

3. AWS CLI를 설치하고 구성합니다.

   a. AWS 명령줄 인터페이스 설명서에 따라 운영 체제에 대한 AWS CLI를 설치하고 구성합니다. **.aws/credentials** 파일에 올바른 **aws_access_key_id** 및 **aws_secret_access_key** 를 지정합니다. AWS 문서의 AWS 구성 기본 사항을 참조하십시오.

   b. 기본 AWS 리전을 설정합니다.

   참고

   환경 변수를 사용하여 기본 AWS 리전을 설정할 수 있습니다.

   ROSA 서비스는 다음 우선 순위 순서로 영역을 평가합니다.

   i. **--region** 플래그를 사용하여 **rosa** 명령을 실행할 때 지정된 영역입니다.

ii. **AWS_DEFAULT_REGION** 환경 변수에 설정된 리전입니다. AWS 문서 의 AWS CLI를 구성하려면 환경 변수 를 참조하십시오.

iii. AWS 구성 파일에 설정된 기본 리전입니다. AWS 문서의 aws 구성을 사용한 빠른 구성을 참조하십시오.

c. 선택 사항: AWS named profile을 사용하여 AWS CLI 설정 및 인증 정보를 구성합니다. **Rosa**는 다음 우선 순위 순서로 프로필이라는 AWS를 평가합니다.

i. **--profile** 플래그를 사용하여 **rosa** 명령을 실행할 때 지정된 프로필입니다.

ii. **AWS_PROFILE** 환경 변수에 설정된 프로필입니다. AWS 문서의 이름이 지정된 프로필을 참조하십시오.

d. 다음 명령을 실행하여 AWS API를 쿼리하여 AWS CLI가 올바르게 설치되어 구성되었는지 확인합니다.

```
$ aws sts get-caller-identity
```

4. ROSA CLI (**Rosa**)의 최신 버전을 설치합니다.

a. 운영 체제에 대한 **Rosa** CLI의 최신 릴리스를 다운로드합니다.

b. 선택 사항: 다운로드한 파일의 이름을 로사 **로** 변경하고 파일을 실행 가능하게 만듭니다. 이 문서에서는 **rosa** 를 사용하여 실행 파일을 참조합니다.

```
$ chmod +x rosa
```

c. 선택 사항: 경로에 **rosa** 를 추가합니다.

```
$ mv rosa /usr/local/bin/rosa
```

d. 다음 명령을 입력하여 설치를 확인합니다.

```
$ rosa
```

출력 예

```
Command line tool for ROSA.

Usage:
  rosa [command]

Available Commands:
  completion  Generates bash completion scripts
  create      Create a resource from stdin
  delete      Delete a specific resource
  describe    Show details of a specific resource
  edit        Edit a specific resource
  help        Help about any command
  init        Applies templates to support Managed OpenShift on AWS clusters
  list        List all resources of a specific type
  login       Log in to your Red Hat account
  logout      Log out
  logs        Show logs of a specific resource
```

```
  verify      Verify resources are configured correctly for cluster install
  version     Prints the version of the tool

Flags:
      --debug     Enable debug mode.
  -h, --help      help for rosa
  -v, --v Level   log level for V logs

Use "rosa [command] --help" for more information about a command.
```

e. **rosa** CLI에 대한 명령 완료 스크립트를 생성합니다. 다음 예제에서는 Linux 시스템에 대한 Bash 완료 스크립트를 생성합니다.

```
$ rosa completion bash | sudo tee /etc/bash_completion.d/rosa
```

f. 기존 터미널에서 **rosa** 명령 완료를 활성화하는 스크립트를 가져옵니다. 다음 예제에서는 Linux 시스템에서 로사에 대한 **Bash** 완료 스크립트를 제공합니다.

```
$ source /etc/bash_completion.d/rosa
```

5. **rosa** CLI를 사용하여 Red Hat 계정에 로그인합니다.

a. 다음 명령을 입력합니다.

```
$ rosa login
```

b. &lt **;my_offline_access_token>** 을 토큰으로 바꿉니다.

출력 예

```
To login to your Red Hat account, get an offline access token at
https://console.redhat.com/openshift/token/rosa
? Copy the token and paste it here: <my-offline-access-token>
```

계속된 출력 예

```
I: Logged in as '<rh-rosa-user>' on 'https://api.openshift.com'
```

6. AWS 계정에 ROSA 클러스터를 배포하는 데 필요한 할당량이 있는지 확인합니다.

```
$ rosa verify quota [--region=<aws_region>]
```

출력 예

```
I: Validating AWS quota...
I: AWS quota ok
```

참고

AWS 할당량이 리전에 따라 다를 수 있습니다. 오류가 발생하면 다른 리전을 사용해 보십시오.

할당량을 늘려야 하는 경우 AWS 관리 콘솔 로 이동하여 실패한 서비스에 대한 할당량 증가를 요청합니다.

할당량 검사가 성공하면 다음 단계로 진행합니다.

7. 클러스터 배포를 위해 AWS 계정을 준비합니다.

   a. 다음 명령을 실행하여 Red Hat 및 AWS 인증 정보가 올바르게 설정되었는지 확인합니다. AWS 계정 ID, 기본 리전 및 ARN이 예상한 내용과 일치하는지 확인합니다. 이제 OpenShift Cluster Manager로 시작하는 행을 무시해도 됩니다.

   ```
   $ rosa whoami
   ```

   출력 예

   ```
   AWS Account ID:               000000000000
   AWS Default Region:           us-east-1
   AWS ARN:                      arn:aws:iam::000000000000:user/hello
   OCM API:                      https://api.openshift.com
   OCM Account ID:               1DzGIdIhqEWyt8UUXQhSoWaaaaa
   OCM Account Name:             Your Name
   OCM Account Username:         you@domain.com
   OCM Account Email:            you@domain.com
   OCM Organization ID:          1HopHfA2hcmhup5gCr2uH5aaaaa
   OCM Organization Name:        Red Hat
   OCM Organization External ID: 0000000
   ```

8. ROSA(**rosa**) CLI에서 OpenShift CLI(**oc**), 버전 4.7.9 이상을 설치합니다.

   a. 이 명령을 입력하여 **oc** CLI의 최신 버전을 다운로드합니다.

   ```
   $ rosa download openshift-client
   ```

   b. **oc** CLI를 다운로드한 후 압축을 풀고 경로에 추가합니다.

   c. 다음 명령을 입력하여 **oc** CLI가 올바르게 설치되었는지 확인합니다.

   ```
   $ rosa verify openshift-client
   ```

역할 생성

이러한 단계를 완료하면 IAM 및 OIDC 액세스 기반 역할을 설정할 준비가 되었습니다.

6.2. 다음 단계

- STS를 사용하여 ROSA 클러스터를 빠르게 생성하거나 사용자 지정을 사용하여 클러스터를 생성합니다.

6.3. 추가 리소스

- AWS 사전 요구 사항
- 필수 AWS 서비스 할당량 및 요청 증가