



# OpenShift Dedicated 4

## AWS의 OpenShift Dedicated 클러스터

AWS에 OpenShift Dedicated 클러스터 설치



## OpenShift Dedicated 4 AWS의 OpenShift Dedicated 클러스터

---

AWS에 OpenShift Dedicated 클러스터 설치

## Legal Notice

Copyright © 2025 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Abstract

이 문서에서는 AWS에 OpenShift Dedicated 클러스터를 설치하는 방법에 대한 정보를 제공합니다. 이 문서에서는 클러스터를 구성하는 방법에 대한 세부 정보도 제공합니다.

## Table of Contents

<b>1장. AWS에서 클러스터 생성</b> .....	<b>3</b>
1.1. 사전 요구 사항	3
1.2. AWS에서 클러스터 생성	3
1.3. 추가 리소스	9
<b>2장. AWS에서 OPENSIFT DEDICATED 클러스터 삭제</b> .....	<b>10</b>
2.1. 클러스터 삭제	10



## 1장. AWS에서 클러스터 생성

CCO(Customer Cloud Subscription) 모델을 통해 자체 AWS 계정을 사용하거나 Red Hat이 소유한 AWS 인프라 계정을 사용하여 AWS에 OpenShift Dedicated를 배포할 수 있습니다.

### 1.1. 사전 요구 사항

- [OpenShift Dedicated](#) 및 [아키텍처 개념](#)에 대한 설명서를 검토했습니다.
- [OpenShift Dedicated 클라우드 배포 옵션](#)을 검토했습니다.

### 1.2. AWS에서 클러스터 생성

CCO(Customer Cloud Subscription) 청구 모델을 사용하면 사용자가 소유한 기존 AWS(Amazon Web Services) 계정에서 OpenShift Dedicated 클러스터를 생성할 수 있습니다.

Red Hat 클라우드 계정 인프라 유형을 선택하여 Red Hat이 소유한 클라우드 공급자 계정에 OpenShift Dedicated를 배포할 수도 있습니다.

CCS 모델을 사용하여 AWS 계정에 OpenShift Dedicated를 배포 및 관리하려면 다음 사전 요구 사항을 완료합니다.

#### 사전 요구 사항

- OpenShift Dedicated에서 사용할 AWS 계정을 구성했습니다.
- AWS 계정에 서비스를 배포하지 않았습니다.
- 원하는 클러스터 크기를 지원하는 데 필요한 AWS 계정 할당량 및 제한을 구성했습니다.
- **AdministratorAccess** 정책이 연결된 **osdCcsAdmin** AWS IAM(Identity and Access Management) 사용자가 있습니다.
- AWS 조직에 SCP(서비스 제어 정책)를 설정했습니다. 자세한 내용은 [최소 필요한 서비스 제어 정책\(SCP\)](#)을 참조하십시오.
- AWS에서 **비즈니스 지원** 이상을 지원하는 것이 좋습니다.
- 클러스터 전체 프록시를 구성하는 경우 VPC에서 클러스터가 설치되고 있음을 프록시에 액세스할 수 있는지 확인합니다. VPC의 프라이빗 서브넷에서도 프록시에 액세스할 수 있어야 합니다.

#### 프로세스

1. [OpenShift Cluster Manager](#)에 로그인합니다.
2. 개요 페이지의 **Red Hat OpenShift Dedicated** 카드에서 **클러스터 생성**을 선택합니다.
3. **billing 모델**에서 서브스크립션 유형 및 인프라 유형을 구성합니다.
  - a. 서브스크립션 유형을 선택합니다. OpenShift Dedicated 서브스크립션 옵션에 대한 자세한 내용은 [OpenShift Cluster Manager 설명서의 클러스터 서브스크립션 및 등록](#)을 참조하십시오.



### 참고

OpenShift Dedicated 서브스크립션 및 리소스 할당량에 따라 사용할 수 있는 서브스크립션 유형입니다. 자세한 내용은 영업 담당자 또는 Red Hat 지원에 문의하십시오.

- b. **고객 클라우드 서브스크립션** 인프라 유형을 선택하여 사용자가 소유한 기존 클라우드 공급자 계정에 OpenShift Dedicated를 배포하거나 **Red Hat 클라우드 계정 인프라 유형**을 선택하여 **Red Hat** 이 소유한 클라우드 공급자 계정에 OpenShift Dedicated를 배포합니다.
  - c. 다음을 클릭합니다.
4. **Amazon Web Services**에서 **실행**을 선택합니다. AWS 계정에서 클러스터를 프로비저닝하는 경우 다음 하위 단계를 완료합니다.
- a. 나열된 **사전 요구 사항**을 검토하고 완료합니다.
  - b. 확인란을 선택하여 모든 사전 요구 사항을 읽고 완료했음을 확인합니다.
  - c. AWS 계정 세부 정보를 제공합니다.
    - i. **AWS 계정 ID**를 입력합니다.
    - ii. **AWS IAM 사용자 계정의AWS 액세스 키 ID** 및 **AWS 시크릿 액세스 키**를 입력합니다.



### 참고

AWS에서 이러한 인증 정보를 취소하면 이러한 인증 정보를 사용하여 생성된 클러스터에 대한 액세스 권한이 손실됩니다.

- iii. 선택 사항: **AWS 서비스 제어 정책(SCP)** 검사를 선택하여 **SCP** 검사를 비활성화할 수 있습니다.



### 참고

일부 AWS SCP는 필요한 권한이 있는 경우에도 설치에 실패할 수 있습니다. SCP 검사를 비활성화하면 설치를 진행할 수 있습니다. SCP는 검사가 무시되더라도 여전히 강제됩니다.

5. 다음을 클릭하여 클라우드 공급자 계정을 확인하고 **클러스터 세부 정보** 페이지로 이동합니다.
6. **클러스터 세부 정보** 페이지에서 클러스터 이름을 지정하고 클러스터 세부 정보를 지정합니다.
  - a. **클러스터 이름**을 추가합니다.
  - b. 선택 사항: 클러스터 생성은 **openshiftapps.com**에서 프로비저닝된 클러스터의 하위 도메인으로 도메인 접두사를 생성합니다. 클러스터 이름이 15자 미만이면 도메인 접두사에 해당 이름이 사용됩니다. 클러스터 이름이 15자를 초과하면 도메인 접두사가 15자 문자열로 임의로 생성됩니다.  
하위 도메인을 사용자 지정하려면 **사용자 지정 도메인 접두사 만들기** 확인란을 선택하고 도메인 접두사 필드에 **도메인 접두사** 이름을 입력합니다. 도메인 접두사는 15자를 초과할 수 없으며 조직 내에서 고유해야 하며 클러스터 생성 후에는 변경할 수 없습니다.
  - c. **버전** 드롭다운 메뉴에서 클러스터 버전을 선택합니다.



- d. **Region** 드롭다운 메뉴에서 클라우드 공급자 리전을 선택합니다.
- e. **단일 영역 또는 다중 영역** 구성을 선택합니다.
- f. **사용자 워크로드 모니터링 활성화**를 선택하여 Red Hat site Reliability Engineer(SRE) 플랫폼 지표와 별도로 자체 프로젝트를 모니터링합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- g. 선택 사항: **고급 암호화**를 확장하여 암호화 설정을 변경합니다.
  - i. 기본 KMS 키를 **사용하여 기본 KMS 키** 사용을 수락하거나 사용자 정의 KMS 키를 **사용하여 사용자 정의 KMS 키** 사용을 선택합니다.
    - A. **Use Custom KMS** 키를 선택한 경우 **Key ARN** 필드에 AWS Key Management Service (KMS) 사용자 정의 키 ARN(Amazon Resource Name) ARN을 입력합니다. 키는 클러스터의 모든 컨트롤 플레인, 인프라, 작업자 노드 루트 볼륨 및 영구 볼륨을 암호화하는 데 사용됩니다.
  - ii. 선택 사항: 클러스터가 **FIPS 검증이 필요한 경우 FIPS 암호화**활성화를 선택합니다.



#### 참고

**FIPS 암호화 활성화**가 선택되면 기본적으로 추가 **etcd 암호화**를 활성화하며 비활성화할 수 없습니다. **FIPS 암호화**를 선택하지 않고 추가 **etcd 암호화** 사용을 선택할 수 있습니다.

- iii. 선택 사항: **etcd 키 값 암호화**가 필요한 경우 추가 **etcd 암호화** 사용을 선택합니다. 이 옵션을 사용하면 etcd 키 값이 암호화되지만 키는 암호화되지 않습니다. 이 옵션은 기본적으로 OpenShift Dedicated 클러스터의 etcd 볼륨을 암호화하는 컨트롤 플레인 스토리지 암호화에 추가됩니다.



#### 참고

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

- h. **다음**을 클릭합니다.

7. **Default** 머신 풀 페이지의 드롭다운 메뉴에서 **컴퓨팅 노드 인스턴스 유형**을 선택합니다.
8. 선택 사항: **자동 스케일링 활성화** 확인란을 선택합니다.
  - a. **클러스터 자동 스케일링 설정 편집**을 클릭하여 자동 스케일링 설정을 변경합니다.
  - b. 원하는 변경을 수행한 후 **닫기**를 클릭합니다.
  - c. 최소 및 최대 노드 수를 선택합니다. 사용 가능한 더하기 및 마이너스 기호를 참여하거나 원하는 노드 수를 숫자 입력 필드에 입력하여 노드 수를 선택할 수 있습니다.
9. 드롭다운 메뉴에서 **컴퓨팅 노드 수**를 선택합니다.



### 참고

클러스터가 생성되면 클러스터의 컴퓨팅 노드 수를 변경할 수 있지만 머신 풀에서 컴퓨팅 노드 인스턴스 유형을 변경할 수 없습니다. OpenShift Dedicated 서브스크립션에 따라 사용할 수 있는 노드의 수 및 유형입니다.

10. IMDSv1 및 IMDSv2 유형을 모두 사용하거나 EC2 인스턴스에서 IMDSv2만 사용해야 하는 인스턴스 메타데이터 서비스(IMDS) 유형에 대한 기본 설정을 선택합니다. 다음 두 가지 방법으로 실행 중인 인스턴스에서 인스턴스 메타데이터에 액세스할 수 있습니다.

- 인스턴스 메타데이터 서비스 버전 1(IMDSv1) - 요청/응답 방법
- 인스턴스 메타데이터 서비스 버전 2(IMDSv2) - 세션 지향 방법



### 중요

클러스터를 생성한 후에는 인스턴스 메타데이터 서비스 설정을 변경할 수 없습니다.



### 참고

IMDSv2는 세션 지향 요청을 사용합니다. 세션 지향 요청을 사용하면 세션 기간을 정의하는 세션 토큰을 생성합니다. 세션 기간은 최소 1초에서 최대 6시간 사이입니다. 지정된 기간 동안 후속 요청에 동일한 세션 토큰을 사용할 수 있습니다. 지정된 기간이 만료된 후 향후 요청에 사용할 새 세션 토큰을 생성해야 합니다.

IMDS에 대한 자세한 내용은 AWS 문서의 [인스턴스 메타데이터 및 사용자 데이터](#)를 참조하십시오.

11. 선택 사항: **노드 라벨 편집**을 확장하여 노드에 라벨을 추가합니다. **레이블 추가**를 클릭하여 노드 레이블을 추가하고 **다음**을 선택합니다.
12. **네트워크 구성** 페이지에서 클러스터의 **공용** 또는 **프라이빗** API 끝점 및 애플리케이션 경로를 사용하려면 **공용** 또는 **프라이빗**을 선택합니다.



### 중요

프라이빗 API 끝점을 사용하는 경우 클라우드 공급자 계정의 네트워크 설정을 업데이트할 때까지 클러스터에 액세스할 수 없습니다.

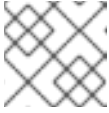
13. 선택 사항: 기존 AWS VPC(Virtual Private Cloud)에 클러스터를 설치하려면 다음을 수행합니다.



### 참고

다른 클러스터에 대해 설치 프로그램에서 자동으로 생성된 VPC에 OpenShift Dedicated 클러스터를 설치하는 것은 지원되지 않습니다.

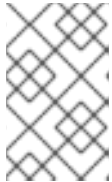
- a. **기존 VPC에 설치**를 선택합니다.
- b. 기존 VPC에 설치하고 프라이빗 API 엔드포인트 사용을 선택한 경우 **PrivateLink 사용**을 선택할 수 있습니다. 이 옵션을 사용하면 AWS PrivateLink 엔드포인트만 사용하여 Red Hat 사이트 안정성 엔지니어링(SRE)의 클러스터 연결을 활성화합니다.



## 참고

**PrivateLink 사용** 옵션은 클러스터를 생성한 후에는 변경할 수 없습니다.

- c. 기존 VPC에 설치하고 클러스터에 대해 HTTP 또는 HTTPS 프록시를 활성화하려면 클러스터 **전체 프록시 구성**을 선택합니다.
14. 기존 AWS VPC에 클러스터를 설치하도록 선택한 경우 **VPC(Virtual Private Cloud) 서브넷 설정**을 제공하고 **Next** 를 선택합니다. Cloud NAT(네트워크 주소 변환) 및 Cloud 라우터를 생성해야 합니다. Cloud NAT 및 Google VPC에 대한 자세한 내용은 "추가 리소스" 섹션을 참조하십시오.



## 참고

클러스터를 설치할 각 가용성 영역의 퍼블릭 및 프라이빗 서브넷으로 VPC가 구성되어 있는지 확인해야 합니다. PrivateLink를 사용하도록 선택한 경우 프라이빗 서브넷만 필요합니다.

- a. 선택 사항: **추가 보안 그룹**을 확장하고 기본적으로 생성된 머신 풀의 노드에 적용할 추가 사용자 지정 보안 그룹을 선택합니다. 보안 그룹을 이미 생성하여 이 클러스터에 대해 선택한 VPC와 연결되어야 합니다. 클러스터를 생성한 후에는 보안 그룹을 기본 머신 풀에 추가하거나 편집할 수 없습니다.  
기본적으로 지정한 보안 그룹이 모든 노드 유형에 추가됩니다. **모든 노드 유형에 동일한 보안 그룹 적용 확인란의 선택을 해제하여 각 노드 유형에 대해 다른 보안 그룹을 적용합니다.**  
  
자세한 내용은 **추가 리소스** 에서 **보안 그룹**에 대한 요구 사항을 참조하십시오.
15. 기본 애플리케이션 인그레스 설정을 수락하거나 고유한 사용자 지정 설정을 생성하려면 사용자 지정 설정을 선택합니다.
  - a. 선택 사항: 경로 선택기를 제공합니다.
  - b. 선택 사항: 제외된 네임스페이스를 제공합니다.
  - c. 네임스페이스 소유권 정책을 선택합니다.
  - d. 와일드카드 정책을 선택합니다.  
사용자 지정 애플리케이션 인그레스 설정에 대한 자세한 내용은 각 설정에 제공된 정보 아이콘을 클릭합니다.
16. 클러스터 전체 프록시를 구성하도록 선택한 경우 클러스터 전체 프록시 페이지에서 **프록시 설정** 세부 정보를 제공합니다.
  - a. 다음 필드 중 하나 이상에 값을 입력합니다.
    - 유효한 **HTTP 프록시 URL** 을 지정합니다.
    - 유효한 **HTTPS 프록시 URL** 을 지정합니다.
    - **additional trust bundle** 필드에 PEM 인코딩 X.509 인증서 번들을 제공합니다. 번들이 클러스터 노드의 신뢰할 수 있는 인증서 저장소에 추가됩니다. 프록시의 ID 인증서가 RHCOS(Red Hat Enterprise Linux CoreOS) 신뢰 번들의 기관에서 서명되지 않는 한 TLS 지정 프록시를 사용하는 경우 추가 신뢰 번들 파일이 필요합니다. 이 요구 사항은 프록시가 투명했는지 또는 **http-proxy** 인수를 및 **https-proxy** 인수를 사용하여 명시적 구성이 필요한지 여부와 관계없이 적용됩니다.
  - b. 다음을 클릭합니다.

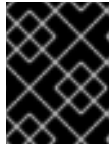
OpenShift Dedicated를 사용하여 프록시 구성에 대한 자세한 내용은 *클러스터 전체 프록시 구성*을 참조하십시오.

17. **CIDR 범위** 대화 상자에서 CIDR(사용자 정의 클래스리스 도메인 간 라우팅) 범위를 구성하거나 제공된 기본값을 사용합니다.



#### 참고

VPC에 설치하는 경우 **Machine CIDR** 범위가 VPC 서브넷과 일치해야 합니다.



#### 중요

CIDR 구성은 나중에 변경할 수 없습니다. 계속하기 전에 네트워크 관리자로 선택을 확인합니다.

18. **클러스터 업데이트 전략** 페이지에서 업데이트 기본 설정을 구성합니다.

- a. 클러스터 업데이트 방법을 선택합니다.

- **각 업데이트**를 개별적으로 예약하려면 개별 업데이트를 선택합니다. 이는 기본 옵션입니다.
- 업데이트를 사용할 수 있는 경우 **Recurring updates**를 선택하여 원하는 날짜에 클러스터를 업데이트하고 시작 시간을 선택합니다.



#### 참고

OpenShift Dedicated의 업데이트 라이프사이클 설명서에서 라이프 사이클 종료 날짜를 검토할 수 있습니다. 자세한 내용은 [OpenShift Dedicated 업데이트 라이프 사이클](#)을 참조하십시오.

- b. 반복 업데이트를 선택한 경우 드롭다운 메뉴에서 원하는 요일을 선택하고 UTC의 시작 시간을 업그レード하십시오.
- c. 선택 사항: 클러스터 업그레이드 중에 **노드 드레이닝**의 유예 기간을 설정할 수 있습니다. **1시간** 유예 기간이 기본적으로 설정됩니다.
- d. 다음을 클릭합니다.



#### 참고

클러스터의 보안 또는 안정성에 큰 영향을 미치는 심각한 보안 문제가 발생하면 Red Hat SRE(Site Reliability Engineering)에서 영향을 받지 않는 최신 z-stream 버전에 대한 자동 업데이트를 예약할 수 있습니다. 업데이트는 고객 알림이 제공된 후 48 시간 이내에 적용됩니다. 심각한 영향을 미치는 보안 **등급**에 대한 설명은 [Red Hat 보안 등급 이해](#)를 참조하십시오.

19. 선택 사항에 대한 요약 검토하고 **클러스터 생성**을 클릭하여 클러스터 설치를 시작합니다. 설치를 완료하는 데 약 30-40분이 걸립니다.
20. 선택 사항: **개요** 탭에서 삭제 보호 : **Disabled** 아래에 있는 **Enable**을 선택하여 삭제 보호 기능을 활성화할 수 있습니다. 이렇게 하면 클러스터가 삭제되지 않습니다. 삭제 보호를 비활성화하려면 **Disable**을 선택합니다. 기본적으로 클러스터는 삭제 보호 기능을 비활성화하여 생성됩니다.

## 검증

- 클러스터의 **개요** 페이지에서 설치 진행 상황을 모니터링할 수 있습니다. 동일한 페이지에서 설치 로그를 볼 수 있습니다. 페이지의 **세부 정보** 섹션에 있는 상태가 **Ready**로 표시되면 클러스터가 준비되었습니다.

## 1.3. 추가 리소스

- OpenShift Dedicated를 사용하여 프록시를 구성하는 방법에 대한 자세한 내용은 [클러스터 전체 프록시 구성](#)을 참조하십시오.
- CCS 배포에 필요한 AWS 서비스 제어 정책에 대한 자세한 내용은 [최소 필요한 서비스 제어 정책 \(SCP\)](#)을 참조하십시오.
- OpenShift Dedicated의 영구 스토리지에 대한 자세한 내용은 OpenShift Dedicated 서비스 정의의 [스토리지](#) 섹션을 참조하십시오.
- OpenShift Dedicated의 로드 밸런서에 대한 자세한 내용은 OpenShift Dedicated 서비스 정의의 [로드 밸런서](#) 섹션을 참조하십시오.
- etcd 암호화에 대한 자세한 내용은 [etcd 암호화 서비스 정의](#)를 참조하십시오.
- OpenShift Dedicated 버전의 라이프 종료 날짜에 대한 자세한 내용은 [OpenShift Dedicated 업데이트 라이프 사이클](#)을 참조하십시오.
- 사용자 지정 추가 보안 그룹의 요구 사항에 대한 자세한 내용은 [추가 사용자 지정 보안 그룹](#)을 참조하십시오.
- ID 공급자 구성에 대한 자세한 내용은 ID 공급자 [구성](#)을 참조하십시오.
- 클러스터 권한 취소에 대한 자세한 내용은 [Revoking 권한 및 OpenShift Dedicated 클러스터에 대한 액세스](#)를 참조하십시오.

## 2장. AWS에서 OPENSHIFT DEDICATED 클러스터 삭제

클러스터 소유자는 OpenShift Dedicated 클러스터를 삭제할 수 있습니다.

### 2.1. 클러스터 삭제

Red Hat OpenShift Cluster Manager에서 OpenShift Dedicated 클러스터를 삭제할 수 있습니다.

사전 요구 사항

- [OpenShift Cluster Manager](#)에 로그인했습니다.
- OpenShift Dedicated 클러스터를 생성하셨습니다.

프로세스

1. [OpenShift Cluster Manager](#)에서 삭제할 클러스터를 클릭합니다.
2. 작업 드롭다운 메뉴에서 클러스터 삭제 를 선택합니다.
3. 굵게 강조 표시된 클러스터의 이름을 입력한 다음 삭제 를 클릭합니다. 클러스터 삭제가 자동으로 수행됩니다.