



## OpenShift Dedicated 4

# OpenShift Dedicated 클러스터 설치, 액세스 및 삭제

OpenShift Dedicated 클러스터 설치, 액세스 및 삭제



# OpenShift Dedicated 4 OpenShift Dedicated 클러스터 설치, 액세스 및 삭제

---

OpenShift Dedicated 클러스터 설치, 액세스 및 삭제

## 법적 공지

Copyright © 2024 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.

## 초록

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

## 차례

<b>1장. AWS에서 클러스터 생성</b> .....	<b>3</b>
1.1. 사전 요구 사항	3
1.2. CCS를 사용하여 AWS에서 클러스터 생성	3
1.3. RED HAT 클라우드 계정으로 AWS에서 클러스터 생성	8
1.4. 추가 리소스	11
<b>2장. GCP에서 클러스터 생성</b> .....	<b>12</b>
2.1. 사전 요구 사항	12
2.2. CCS를 사용하여 GCP에서 클러스터 생성	12
2.3. GOOGLE CLOUD MARKETPLACE를 사용하여 GCP에 클러스터 생성	18
2.4. RED HAT 클라우드 계정으로 GCP에서 클러스터 생성	22
2.5. RED HAT MARKETPLACE를 사용하여 GCP에 클러스터 생성	25
2.6. 추가 리소스	30
<b>3장. ID 공급자 구성</b> .....	<b>31</b>
3.1. ID 공급자 이해	31
3.2. GITHUB ID 공급자 구성	32
3.3. GITLAB ID 공급자 구성	33
3.4. GOOGLE ID 공급자 구성	34
3.5. LDAP ID 공급자 구성	35
3.6. OPENID ID 공급자 구성	37
3.7. HTPASSWD ID 공급자 구성	39
3.8. 클러스터에 액세스	40
<b>4장. OPENSIFT DEDICATED 클러스터에 대한 권한 및 액세스 권한 취소</b> .....	<b>42</b>
4.1. 사용자의 관리자 권한 해지	42
4.2. 클러스터에 대한 사용자 액세스 해지	42
<b>5장. OPENSIFT DEDICATED 클러스터 삭제</b> .....	<b>44</b>
5.1. 클러스터 삭제	44



## 1장. AWS에서 클러스터 생성

CCO(Customer Cloud Subscription) 모델을 통해 자체 AWS 계정을 사용하거나 Red Hat이 소유한 AWS 인프라 계정을 사용하여 AWS에 OpenShift Dedicated를 설치할 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. CCS를 사용하여 AWS에서 클러스터 생성

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

CCS 모델을 사용하여 AWS 계정에 OpenShift Dedicated를 배포하고 관리하는 경우 여러 사전 요구 사항을 충족해야 합니다.

#### 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 *Minimum required service control policy (SCP)*에서 참조하십시오.
- AWS에서 **비즈니스 지원** 이상을 사용하는 것이 좋습니다.
- 클러스터 전체 프록시를 구성하는 경우 클러스터가 설치 중인 VPC에서 프록시에 액세스할 수 있는지 확인했습니다. VPC의 프라이빗 서브넷에서도 프록시에 액세스할 수 있어야 합니다.

#### 절차

1. [OpenShift Cluster Manager](#)에 로그인하고 **클러스터 생성**을 클릭합니다.
2. **OpenShift 클러스터 생성** 페이지의 **Red Hat OpenShift Dedicated** 행에서 **클러스터 생성**을 선택합니다.
3. **청구 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. 보유한 기존 클라우드 공급자 계정에 OpenShift Dedicated를 배포하려면 **Customer Cloud Subscription** 인프라 유형을 선택합니다.
- c. 다음을 클릭합니다.
- 4. **Amazon Web Services**에서 **실행**을 선택합니다.
- 5. 클라우드 공급자를 선택한 후 나열된 **사전 요구 사항**을 검토하고 완료합니다. 확인란을 선택하여 모든 사전 요구 사항을 읽고 완료했음을 확인합니다.
- 6. AWS 계정 세부 정보를 입력합니다.
  - a. **AWS 계정 ID**를 입력합니다.
  - b. **AWS 액세스 키 ID**와 **AWS IAM 사용자 계정의 AWS 시크릿 액세스 키**를 입력합니다.



**참고**

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

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



**참고**

일부 AWS SCP는 필요한 권한이 있더라도 설치에 실패할 수 있습니다. SCP 검사를 비활성화하면 설치를 진행할 수 있습니다. 검사 결과가 무시되더라도 SCP가 계속 적용됩니다.

- 7. 다음을 클릭하여 클라우드 공급자 계정을 확인하고 **클러스터 세부 정보** 페이지로 이동합니다.
- 8. **Cluster details** 페이지에서 클러스터 이름을 제공하고 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. **리전** 드롭다운 메뉴에서 클라우드 공급자 **리전**을 선택합니다.
  - e. **단일 영역** 또는 **다중 영역** 구성을 선택합니다.



- f. **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat site Reliability Engineer (SRE) 플랫폼 메트릭과 별도로 자체 프로젝트를 모니터링하도록 선택한 사용자 워크로드 모니터링 활성화. 이 옵션은 기본적으로 활성화되어 있습니다.
- g. 선택사항: **etcd 키 값 암호화가 필요한 경우 추가 etcd 암호화 사용**을 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 etcd 암호화를 활성화하면 약 20%의 성능 오버헤드가 발생합니다. 오버헤드는 etcd 볼륨을 암호화하는 기본 컨트롤 플레인 스토리지 암호화 외에도 이 두 번째 암호화 계층이 도입된 결과입니다. etcd 암호화를 특히 사용 사례에 필요한 경우에만 활성화하는 것이 좋습니다.

- h. 선택 사항: AWS Key Management Service(KMS) 키 **Amazon Resource Name(ARN)**을 제공하려면 **고객 키를 사용하여 영구 볼륨 암호화**를 선택합니다. 키는 클러스터의 모든 컨트롤 플레인, 인프라, 작업자 노드 루트 볼륨 및 영구 볼륨을 암호화하는 데 사용됩니다.



### 중요

기본 스토리지 클래스에서 생성된 PV(영구 볼륨)만 이 특정 키로 암호화됩니다.

다른 스토리지 클래스를 사용하여 생성한 PV는 계속 암호화되지만 스토리지 클래스가 이 키를 사용하도록 특별히 구성되지 않는 한 PV는 이 키로 암호화되지 않습니다.

- i. 다음을 클릭합니다.

9. **Default** 머신 풀 페이지에서 **컴퓨팅 노드 인스턴스 유형과 컴퓨팅 노드 수**를 선택합니다. 사용 가능한 노드의 수 및 유형은 OpenShift Dedicated 서브스크립션에 따라 다릅니다. 여러 가용성 영역을 사용하는 경우 컴퓨팅 노드 수는 영역별로 계산됩니다.



### 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 데이터를 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 **공용** 또는 **프라이빗 API** 끝점과 클러스터의 애플리케이션 경로를 사용하려면 **Public** 또는 **Private** 을 선택합니다.



**중요**

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

13. 선택사항: 기존 AWS VPC(Virtual Private Cloud)에 클러스터를 설치하려면 다음을 수행합니다.
  - a. **기존 VPC에 설치**를 선택합니다.
  - b. 기존 VPC에 설치하고 프라이빗 API 엔드포인트를 사용하도록 선택한 경우 **PrivateLink 사용** 을 선택할 수 있습니다. 이 옵션을 사용하면 AWS PrivateLink 끝점만 사용하여 Red Hat SRE(Site Reliability Engineering)의 클러스터에 연결할 수 있습니다.



**참고**

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

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



**참고**

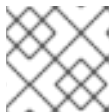
클러스터를 설치할 각 가용성 영역의 퍼블릭 및 프라이빗 서브넷으로 VPC가 구성되어 있는지 확인해야 합니다. PrivateLink를 사용하도록 선택한 경우 프라이빗 서브넷만 필요합니다.

- 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.

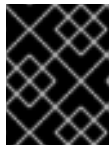
자세한 내용은 추가 리소스에서 보안 그룹에 대한 요구 사항을 참조하십시오.

16. 클러스터 전체 프록시를 구성하도록 선택하는 경우 클러스터 전체 프록시 페이지에 프록시 설정 세부 정보를 입력합니다.
  - a. 다음 필드 중 하나 이상에 값을 입력합니다.
    - 유효한 HTTP 프록시 URL 을 지정합니다.
    - 유효한 HTTPS 프록시 URL 을 지정합니다.
    - 추가 신뢰 번들 필드에서 PEM 인코딩 X.509 인증서 번들을 제공합니다. 번들은 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** 인수 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 클래스 없는 도메인 간 라우팅) 범위를 구성하거나 제공된 기본값을 사용합니다.



#### 참고

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



#### 중요

CIDR 구성은 나중에 변경할 수 없습니다. 계속하기 전에 네트워크 관리자에게 선택 사항을 확인합니다.

18. **Cluster update strategy** 페이지에서 업데이트 기본 설정을 구성합니다.
  - a. 클러스터 업데이트 방법을 선택합니다.
    - 각 업데이트를 개별적으로 예약하려면 개별 업데이트를 선택합니다. 이는 기본 옵션입니다.
    - **Recurring updates** to update your cluster on your preferred day and start time, when updates are available을 선택합니다.



#### 참고

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

- b. 클러스터 업데이트 방법에 따라 관리자 승인을 제공합니다.
  - 개별 업데이트: 승인이 필요한 업데이트 버전을 선택하는 경우 관리자의 승인을 제공하고

승인을 클릭하고 계속.

- 반복 업데이트: 클러스터에 대해 반복적인 업데이트를 선택한 경우 관리자의 승인을 제공한 후 승인을 **클릭하고 계속**. OpenShift Cluster Manager는 관리자의 승인을 받지 않고 마이너 버전에 대해 예정된 y-stream 업데이트를 시작하지 않습니다.
- c. 반복 업데이트를 선택한 경우 해당 요일을 선택하고 드롭다운 메뉴에서 UTC로 시작 시간을 업그레이드하십시오.
- d. 선택 사항: 클러스터 업그레이드 중에 **노드 드레이닝**에 대한 유예 기간을 설정할 수 있습니다. 기본적으로 **1시간** 유예 기간이 설정됩니다.
- e. **다음**을 클릭합니다.



참고

클러스터의 보안 또는 안정성에 큰 영향을 미치는 심각한 보안 문제가 있는 경우 Red Hat 사이트 안정성 엔지니어링(SRE)은 영향을 받지 않는 최신 z-stream 버전에 대한 자동 업데이트를 예약할 수 있습니다. 업데이트는 고객 알림이 제공된 후 48시간 이내에 적용됩니다. 심각한 영향을 미치는 보안 **등급**에 대한 자세한 내용은 [Red Hat 보안 등급 이해](#)를 참조하십시오.

19. 선택 사항 요약을 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 **Status** 가 **Ready** 로 표시되면 클러스터가 준비 상태가 됩니다.

### 1.3. RED HAT 클라우드 계정으로 AWS에서 클러스터 생성

[OpenShift Cluster Manager](#) 를 통해 Red Hat이 소유한 표준 클라우드 공급자 계정을 사용하여 AWS(Amazon Web Services)에서 OpenShift Dedicated 클러스터를 생성할 수 있습니다.

절차

1. [OpenShift Cluster Manager](#) 에 로그인하고 **클러스터 생성**을 클릭합니다.
2. **Cloud** 탭의 **Red Hat OpenShift Dedicated** 행에서 **클러스터 생성**을 클릭합니다.
3. **청구 모델**에서 서브스크립션 유형 및 인프라 유형을 구성합니다.
  - a. **연간** 구독 유형을 선택합니다. Red Hat 클라우드 계정을 사용하여 클러스터를 배포할 때는 **Annual** 서브스크립션 유형만 사용할 수 있습니다. OpenShift Dedicated 서브스크립션 옵션에 대한 자세한 내용은 [OpenShift Cluster Manager 설명서의 클러스터 서브스크립션 및 등록](#)을 참조하십시오.



### 참고

사용할 수 있는 **Annual** 구독 형식에 필요한 리소스 할당량이 있어야 합니다. 자세한 내용은 영업 담당자 또는 Red Hat 지원에 문의하십시오.

- b. **Red Hat**이 소유한 클라우드 공급자 계정에 OpenShift Dedicated를 배포하려면 Red Hat 클라우드 계정 인프라 유형을 선택합니다.
  - c. 다음을 클릭합니다.
4. **Amazon Web Services**에서 실행을 선택하고 다음을 클릭합니다.
5. **Cluster details** 페이지에서 클러스터 이름을 제공하고 클러스터 세부 정보를 지정합니다.
- a. 클러스터 이름을 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. 리전 드롭다운 메뉴에서 클라우드 공급자 **리전**을 선택합니다.
  - e. **단일 영역** 또는 **다중 영역** 구성을 선택합니다.
  - f. 클러스터의 **영구 스토리지** 용량을 선택합니다. 자세한 내용은 OpenShift Dedicated 서비스 정의의 **스토리지** 섹션을 참조하십시오.
  - g. 클러스터에 필요한 **로드 밸런서** 수를 지정합니다. 자세한 내용은 OpenShift Dedicated 서비스 정의의 **로드 밸런서** 섹션을 참조하십시오.
  - h. **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat site Reliability Engineer (SRE) 플랫폼 메트릭과 별도로 자체 프로젝트를 모니터링하도록 선택한 사용자 워크로드 모니터링 활성화. 이 옵션은 기본적으로 활성화되어 있습니다.
  - i. 선택사항: **etcd 키 값 암호화가 필요한 경우 추가 etcd 암호화 사용**을 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 etcd 암호화를 활성화하면 약 20%의 성능 오버헤드가 발생합니다. 오버헤드는 etcd 볼륨을 암호화하는 기본 컨트롤 플레인 스토리지 암호화 외에도 이 두 번째 암호화 계층이 도입된 결과입니다. etcd 암호화를 특히 사용 사례에 필요한 경우에만 활성화하는 것이 좋습니다.

- j. 다음을 클릭합니다.

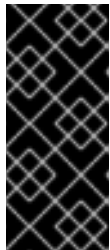
6. **Default** 머신 풀 페이지에서 **컴퓨팅 노드 인스턴스 유형과 컴퓨팅 노드 수를 선택합니다**. 사용 가능한 노드의 수 및 유형은 OpenShift Dedicated 서브스크립션에 따라 다릅니다. 여러 가용성 영역을 사용하는 경우 컴퓨팅 노드 수는 영역별로 계산됩니다.



**참고**

클러스터가 생성되면 컴퓨팅 노드 수를 변경할 수 있지만 머신 풀에서 컴퓨팅 노드 인스턴스 유형을 변경할 수 없습니다. CCS 모델을 사용하는 클러스터의 경우 다른 인스턴스 유형을 사용하는 설치 후 머신 풀을 추가할 수 있습니다. OpenShift Dedicated 서브스크립션에 따라 사용할 수 있는 노드의 수 및 유형입니다.

7. 선택 사항: **노드 라벨 편집** 을 확장하여 노드에 라벨을 추가합니다. **레이블 추가** 를 클릭하여 노드 레이블을 추가하고 **다음** 을 선택합니다.
8. **클러스터 개인 정보** 대화 상자에서 공개 또는 프라이빗 API 끝점과 클러스터의 애플리케이션 경로를 사용하려면 **Public** 또는 **Private** 을 선택합니다.
9. **다음** 을 클릭합니다.
10. **CIDR 범위** 대화 상자에서 CIDR(사용자 정의 클래스 없는 도메인 간 라우팅) 범위를 구성하거나 제공된 기본값을 사용합니다.



**중요**

CIDR 구성은 나중에 변경할 수 없습니다. 계속하기 전에 네트워크 관리자에게 선택 사항을 확인합니다.

클러스터 개인 정보 보호가 **Private** 로 설정된 경우 클라우드 공급자의 프라이빗 연결을 구성할 때까지 클러스터에 액세스할 수 없습니다.

11. **Cluster update strategy** 페이지에서 업데이트 기본 설정을 구성합니다.
  - a. 클러스터 업데이트 방법을 선택합니다.
    - 각 업데이트를 개별적으로 예약하려면 개별 업데이트를 선택합니다. 이는 기본 옵션입니다.
    - **Recurring updates** to update your cluster on your preferred day and start time, when updates are available을 선택합니다.



**참고**

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

- b. 클러스터 업데이트 방법에 따라 관리자 승인을 제공합니다.
  - 개별 업데이트: 승인이 필요한 업데이트 버전을 선택하는 경우 관리자의 승인을 제공하고 승인을 **클릭하고 계속**.
  - 반복 업데이트: 클러스터에 대해 반복적인 업데이트를 선택한 경우 관리자의 승인을 제공한 후 승인을 **클릭하고 계속**. OpenShift Cluster Manager는 관리자의 승인을 받지 않고 마이너 버전에 대해 예정된 y-stream 업데이트를 시작하지 않습니다.

- c. 반복 업데이트를 선택한 경우 해당 요일을 선택하고 드롭다운 메뉴에서 UTC로 시작 시간을 업그레이드하십시오.
- d. 선택 사항: 클러스터 업그레이드 중에 **노드 드레이닝**에 대한 유예 기간을 설정할 수 있습니다. 기본적으로 **1시간** 유예 기간이 설정됩니다.
- e. 다음을 클릭합니다.



#### 참고

클러스터의 보안 또는 안정성에 큰 영향을 미치는 심각한 보안 문제가 있는 경우 Red Hat 사이트 안정성 엔지니어링(SRE)은 영향을 받지 않는 최신 z-stream 버전에 대한 자동 업데이트를 예약할 수 있습니다. 업데이트는 고객 알림이 제공된 후 48시간 이내에 적용됩니다. 심각한 영향을 미치는 보안 **등급**에 대한 자세한 내용은 [Red Hat 보안 등급 이해](#)를 참조하십시오.

- 12. 선택 사항 요약을 검토하고 **클러스터 생성**을 클릭하여 클러스터 설치를 시작합니다. 설치를 완료하는 데 약 30~40분이 걸립니다.
- 13. 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 **Status** 가 **Ready** 로 표시되면 클러스터가 준비 상태가 됩니다.

## 1.4. 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.



## 2장. GCP에서 클러스터 생성

CCO(Customer Cloud Subscription) 모델을 통해 자체 GCP 계정을 사용하거나 Red Hat이 소유한 GCP 인프라 계정을 사용하여 GCP(Google Cloud Platform)에 OpenShift Dedicated를 설치할 수 있습니다.

### 2.1. 사전 요구 사항

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

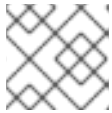
### 2.2. CCS를 사용하여 GCP에서 클러스터 생성

CCO(Customer Cloud Subscription) 청구 모델을 사용하면 사용자가 소유한 기존 GCP(Google Cloud Platform) 계정에 OpenShift Dedicated 클러스터를 생성할 수 있습니다.

CCS 모델을 사용하여 GCP 계정에 OpenShift Dedicated를 배포하고 관리하는 경우 여러 사전 요구 사항을 충족해야 합니다.

#### 사전 요구 사항

- OpenShift Dedicated와 함께 사용하도록 GCP 계정을 구성했습니다.
- 원하는 클러스터 크기를 지원하는 데 필요한 GCP 계정 할당량 및 제한을 구성했습니다.
- GCP 프로젝트를 생성했습니다.



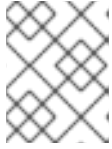
#### 참고

프로젝트 이름은 10자 미만이어야 합니다.

- GCP 프로젝트에서 Google Cloud Resource Manager API를 활성화했습니다. 프로젝트에 대한 API 활성화에 대한 자세한 내용은 [Google Cloud 설명서](#)를 참조하십시오.
- GCP에 다음 역할이 연결된 **osd-ccs-admin**이라는 IAM 서비스 계정이 있습니다.
  - 컴퓨팅 관리자
  - DNS 관리자
  - 보안 관리자
  - 서비스 계정 관리자
  - 서비스 계정 키 관리자
  - 서비스 계정 사용자
  - 조직 정책 뷰어
  - 서비스 관리 관리자
  - 서비스 사용량 관리자
  - 스토리지 관리자



- Compute Load Balancer 관리자
- 역할 뷰어
- 역할 관리자
- **osd-ccs-admin** GCP 서비스 계정의 키를 생성하고 **osServiceAccount.json** 이라는 파일로 내보냈습니다.



### 참고

GCP 서비스 계정의 키를 생성하고 JSON 파일로 내보내는 방법에 대한 자세한 내용은 Google Cloud 설명서에서 [서비스 계정 키 생성](#)을 참조하십시오.

- GCP에서 [향상된 지원](#) 또는 높은 수준을 갖는 것이 좋습니다.
- 잠재적인 충돌을 방지하려면 OpenShift Dedicated를 설치하기 전에 프로젝트에서 프로비저닝한 다른 리소스가 없는 것이 좋습니다.
- 클러스터 전체 프록시를 구성하는 경우 클러스터가 설치 중인 VPC에서 프록시에 액세스할 수 있는지 확인했습니다.

### 절차

1. [OpenShift Cluster Manager](#) 에 로그인하고 [클러스터 생성](#)을 클릭합니다.
2. [OpenShift 클러스터 생성](#) 페이지의 **Red Hat OpenShift Dedicated** 행에서 [클러스터 생성](#)을 선택합니다.
3. [청구 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. 보유한 기존 클라우드 공급자 계정에 OpenShift Dedicated를 배포하려면 **Customer Cloud Subscription** 인프라 유형을 선택합니다.
  - c. [다음](#)을 클릭합니다.
4. [Google Cloud Platform](#)에서 [실행](#)을 선택합니다.
  5. 클라우드 공급자를 선택한 후 나열된 **사전 요구 사항**을 검토하고 완료합니다. 확인란을 선택하여 모든 사전 요구 사항을 읽고 완료했음을 확인합니다.
  6. JSON 형식의 GCP 서비스 계정 개인 키를 입력합니다. [찾아보기](#)를 클릭하여 JSON 파일을 찾아서 연결하거나 **서비스 계정 JSON** 필드에 세부 정보를 추가할 수 있습니다.
  7. [다음](#)을 클릭하여 클라우드 공급자 계정을 확인하고 [클러스터 세부 정보](#) 페이지로 이동합니다.

8. **Cluster details** 페이지에서 클러스터 이름을 제공하고 클러스터 세부 정보를 지정합니다.

- a. 클러스터 이름을 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. **리전** 드롭다운 메뉴에서 클라우드 공급자 **리전** 을 선택합니다.
- e. **단일 영역** 또는 **다중 영역** 구성을 선택합니다.
- f. 선택 사항: 클러스터를 설치할 때 **보호된 VM을 사용하도록 Secure Boot forShielded VM**을 선택합니다. 자세한 내용은 **Shielded VMs** 를 참조하십시오.



**중요**

클러스터를 성공적으로 만들려면 조직에 정책 **제한 조건 제약 조건/compute.requireShieldedVm** 이 활성화된 경우 **Shielded VM에 대해 Secure Boot 지원** 활성화를 선택해야 합니다. GCP 조직 정책 제약 조건에 대한 자세한 내용은 조직 정책 제약 **조건** 을 참조하십시오.

- g. **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat site Reliability Engineer (SRE) 플랫폼 매트릭과 별도로 자체 프로젝트를 모니터링하도록 선택한 사용자 워크로드 모니터링 활성화. 이 옵션은 기본적으로 활성화되어 있습니다.

9. 선택 사항: **고급** 암호화를 확장하여 암호화 설정을 변경합니다.

- a. 사용자 정의 KMS 키를 사용하려면 **Use Custom KMS keys**를 선택합니다. 사용자 정의 KMS 키를 사용하지 않으려면 기본 설정 **Use default KMS Keys**를 그대로 두십시오.



**중요**

사용자 정의 KMS 키를 사용하려면 IAM 서비스 계정 **osd-ccs-admin** 에 **Cloud KMS CryptoKey Encrypter/Decrypter** 역할을 부여해야 합니다. 리소스에 역할을 부여하는 방법에 대한 자세한 내용은 **리소스에 대한 역할 부여**를 참조하십시오.

**Use Custom KMS keys**가 선택되어 있는 경우:

- i. 키 링 위치 드롭다운 메뉴에서 **키 링 위치**를 선택합니다.
- ii. 키 링 드롭다운 메뉴에서 **키 링** 을 선택합니다.
- iii. 키 이름 드롭다운 메뉴에서 **키 이름**을 선택합니다.
- iv. **KMS 서비스 계정**을 제공합니다.
- b. 선택사항: **etcd 키 값 암호화가 필요한 경우 추가 etcd 암호화 사용**을 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 etcd 암호화를 활성화하면 약 20%의 성능 오버헤드가 발생합니다. 오버헤드는 etcd 볼륨을 암호화하는 기본 컨트롤 플레인 스토리지 암호화 외에도 이 두 번째 암호화 계층이 도입된 결과입니다. etcd 암호화를 특히 사용 사례에 필요한 경우에만 활성화하는 것이 좋습니다.

- c. 선택 사항: 클러스터가 **FIPS 검증이 필요한 경우 FIPS 암호화**활성화를 선택합니다.
  - d. 다음을 클릭합니다.
10. **Default** 머신 풀 페이지에서 **컴퓨팅 노드 인스턴스 유형과 컴퓨팅 노드 수를 선택합니다**. 사용 가능한 노드의 수 및 유형은 OpenShift Dedicated 서브스크립션에 따라 다릅니다. 여러 가용성 영역을 사용하는 경우 컴퓨팅 노드 수는 영역별로 계산됩니다.



### 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.

- 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 **공용** 또는 **프라이빗 API** 끝점과 클러스터의 애플리케이션 경로를 사용하려면 **Public** 또는 **Private** 을 선택합니다.



### 중요

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

- 13. 선택사항: 기존 GCP VPC(Virtual Private Cloud)에 클러스터를 설치하려면 다음을 수행합니다.
  - a. **기존 VPC에 설치**를 선택합니다.
  - b. 기존 VPC에 설치하고 클러스터에 대해 HTTP 또는 HTTPS 프록시를 활성화하려면 클러스터 **전체 프록시** 구성을 선택합니다.
- 14. 다음을 클릭합니다.
- 15. 선택 사항: 클러스터를 GCP 공유 VPC에 설치하려면 다음을 수행합니다.



### 중요

공유 VPC에 클러스터를 설치하려면 OpenShift Dedicated 버전 4.13.15 이상을 사용해야 합니다. 또한 **호스트 프로젝트**의 VPC 소유자는 Google Cloud 콘솔에서 **호스트 프로젝트**로 프로젝트를 활성화해야 합니다. 자세한 내용은 [호스트 프로젝트 사용](#)을 참조하십시오.

- a. **GCP 공유 VPC에 설치**를 선택합니다.

- b. **Host 프로젝트 ID** 를 지정합니다. 지정된 호스트 프로젝트 ID가 잘못된 경우 클러스터 생성에 실패합니다.



**중요**

클러스터 구성 마법사에서 단계를 완료하고 클러스터 **생성** 을 클릭하면 클러스터가 "설치 대기 중" 상태로 전환됩니다. 이때 **Compute Network Administrator, Compute Security Administrator, DNS Administrator** 라는 역할을 동적으로 생성한 서비스 계정을 할당해야 하는 호스트 프로젝트의 VPC 소유자에 문의해야 합니다. 호스트 프로젝트의 VPC 소유자는 클러스터 생성에 실패하기 전에 나열된 권한을 부여하는 데 30일이 걸립니다. 공유 VPC 권한에 대한 자세한 내용은 [공유 VPC 프로비저닝](#) 을 참조하십시오.

- 16. 기존 GCP VPC에 클러스터를 설치하도록 선택한 경우 **VPC(Virtual Private Cloud) 서브넷 설정** 을 제공하고 **다음** 을 선택합니다. Cloud NAT(네트워크 주소 변환) 및 클라우드 라우터를 생성해야 합니다. Cloud NAT 및 Google VPC에 대한 자세한 내용은 "추가 리소스" 섹션을 참조하십시오.



**참고**

Shared VPC에 클러스터를 설치하는 경우 호스트 프로젝트에서 VPC 이름과 서브넷이 공유됩니다.

- 17. 클러스터 전체 프록시를 구성하도록 선택하는 경우 클러스터 전체 프록시 페이지에 **프록시 설정** 세부 정보를 입력합니다.

- a. 다음 필드 중 하나 이상에 값을 입력합니다.

- 유효한 **HTTP 프록시 URL** 을 지정합니다.
- 유효한 **HTTPS 프록시 URL** 을 지정합니다.
- **추가 신뢰 번들** 필드에서 PEM 인코딩 X.509 인증서 번들을 제공합니다. 번들은 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** 인수 및 **https-proxy** 인수를 사용하여 명시적 구성이 필요한지 여부와 관계없이 적용됩니다.

- b. **다음** 을 클릭합니다.

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

- 18. **CIDR 범위** 대화 상자에서 CIDR(사용자 정의 클래스 없는 도메인 간 라우팅) 범위를 구성하거나 제공된 기본값을 사용합니다.



**참고**

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



**중요**

CIDR 구성은 나중에 변경할 수 없습니다. 계속하기 전에 네트워크 관리자에게 선택 사항을 확인합니다.

19. **Cluster update strategy** 페이지에서 업데이트 기본 설정을 구성합니다.

a. 클러스터 업데이트 방법을 선택합니다.

- 각 업데이트를 개별적으로 예약하려면 개별 업데이트를 선택합니다. 이는 기본 옵션입니다.
- **Recurring updates** to update your cluster on your preferred day and start time, when updates are available을 선택합니다.



#### 참고

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

b. 클러스터 업데이트 방법에 따라 관리자 승인을 제공합니다.

- 개별 업데이트: 승인이 필요한 업데이트 버전을 선택하는 경우 관리자의 승인을 제공하고 승인을 **클릭하고 계속**.
- 반복 업데이트: 클러스터에 대해 반복적인 업데이트를 선택한 경우 관리자의 승인을 제공한 후 승인을 **클릭하고 계속**. OpenShift Cluster Manager는 관리자의 승인을 받지 않고 마이너 버전에 대해 예정된 y-stream 업데이트를 시작하지 않습니다.

c. 반복 업데이트를 선택한 경우 해당 요일을 선택하고 드롭다운 메뉴에서 UTC로 시작 시간을 업그레이드하십시오.

d. 선택 사항: 클러스터 업그레이드 중에 **노드 트레이닝** 에 대한 유예 기간을 설정할 수 있습니다. 기본적으로 **1시간** 유예 기간이 설정됩니다.

e. 다음을 클릭합니다.



#### 참고

클러스터의 보안 또는 안정성에 큰 영향을 미치는 심각한 보안 문제가 있는 경우 Red Hat 사이트 안정성 엔지니어링(SRE)은 영향을 받지 않는 최신 z-stream 버전에 대한 자동 업데이트를 예약할 수 있습니다. 업데이트는 고객 알림이 제공된 후 48시간 이내에 적용됩니다. 심각한 영향을 미치는 보안 **등급에 대한 자세한 내용은 Red Hat 보안 등급 이해** 를 참조하십시오.

20. 선택 사항 요약을 검토하고 **클러스터 생성** 을 클릭하여 클러스터 설치를 시작합니다. 설치를 완료하는 데 약 30~40분이 걸립니다.

21. 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.



#### 참고

GCP Shared VPC에 설치된 클러스터를 삭제하는 경우 VPC에게 호스트 프로젝트에게 클러스터 생성 중에 참조된 서비스 계정에 부여된 IAM 정책을 제거하도록 알립니다.

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

### 2.3. GOOGLE CLOUD MARKETPLACE를 사용하여 GCP에 클러스터 생성

OpenShift Cluster Manager Hybrid Cloud Console을 통해 Google Cloud에서 OpenShift Dedicated(OSD) 클러스터를 생성할 때 고객은 선호하는 청구 모델로 Google Cloud Marketplace를 선택할 수 있습니다. 이 청구 모델을 통해 Red Hat 고객은 [Google Cloud Marketplace를 통해 구매한 OpenShift Dedicated에 대한 Google Committed Use Cryostat\(CUD\)](#) 를 활용할 수 있습니다. 또한 OSD 가격은 사용량 기반이며 고객은 Google Cloud 계정을 통해 직접 청구됩니다.

#### 절차

1. [OpenShift Cluster Manager](#) 에 로그인하고 **클러스터 생성**을 클릭합니다.
2. **Cloud** 탭의 **Red Hat OpenShift Dedicated** 행에서 **클러스터 생성**을 클릭합니다.
3. **청구 모델**에서 서브스크립션 유형 및 인프라 유형을 구성합니다.
  - a. 온 디맨드 서브스크립션 유형을 선택합니다.
  - b. 드롭다운 메뉴에서 **Google Cloud Marketplace** 를 선택합니다.
  - c. **Customer Cloud Subscription** 인프라 유형을 선택합니다.
  - d. 다음을 클릭합니다.
4. **클라우드 공급자** 페이지에서 제공된 사전 요구 사항 및 Google 약관을 확인하십시오. 서비스 계정 키를 추가합니다.
  - a. **Review Google terms and Agreements** 링크를 클릭합니다.
  - b. 클러스터를 계속 생성하려면 Google 이용 약관에 동의함을 나타내는 체크박스를 클릭합니다.
  - c. 서비스 계정 키를 추가합니다.



#### 참고

서비스 계정 키에 대한 자세한 내용은 **Service account 키** 옆에 있는 정보 아이콘을 클릭합니다.

- d. 다음을 클릭하여 클라우드 공급자 계정을 확인하고 **클러스터 세부 정보** 페이지로 이동합니다.
5. **Cluster details** 페이지에서 클러스터 이름을 제공하고 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. 리전 드롭다운 메뉴에서 클라우드 공급자 리전을 선택합니다.
- e. 단일 영역 또는 다중 영역 구성을 선택합니다.
- f. 선택 사항: 클러스터를 설치할 때 보호된 VM을 사용하도록 **Secure Boot forShielded VM**을 선택합니다. 자세한 내용은 [Shielded VMs](#) 를 참조하십시오.



### 중요

클러스터를 성공적으로 만들려면 조직에 정책 제약 조건 제약 조건/`compute.requireShieldedVm` 이 활성화된 경우 **Shielded VM**에 대해 **Secure Boot** 지원 활성화를 선택해야 합니다. GCP 조직 정책 제약 조건에 대한 자세한 내용은 조직 정책 제약 조건을 참조하십시오.

- g. **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat site Reliability Engineer (SRE) 플랫폼 메트릭과 별도로 자체 프로젝트를 모니터링하도록 선택한 사용자 워크로드 모니터링 활성화. 이 옵션은 기본적으로 활성화되어 있습니다.
6. 선택 사항: 고급 암호화를 확장하여 암호화 설정을 변경합니다.
- a. 사용자 정의 KMS 키를 사용하려면 **Use Custom KMS keys**를 선택합니다. 사용자 정의 KMS 키를 사용하지 않으려면 기본 설정 **Use default KMS Keys**를 그대로 두십시오.



### 중요

사용자 정의 KMS 키를 사용하려면 IAM 서비스 계정 **osd-ccs-admin**에 **Cloud KMS CryptoKey Encrypter/Decrypter** 역할을 부여해야 합니다. 리소스에 역할을 부여하는 방법에 대한 자세한 내용은 [리소스에 대한 역할 부여](#)를 참조하십시오.

**Use Custom KMS keys**가 선택되어 있는 경우:

- i. 키 링 위치 드롭다운 메뉴에서 키 링 위치를 선택합니다.
  - ii. 키 링 드롭다운 메뉴에서 키 링을 선택합니다.
  - iii. 키 이름 드롭다운 메뉴에서 키 이름을 선택합니다.
  - iv. **KMS 서비스 계정을** 제공합니다.
- b. 선택사항: **etcd 키 값 암호화가 필요한 경우 추가 etcd 암호화 사용**을 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.

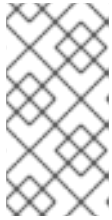


### 참고

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 계층이 도입된 결과입니다. etcd 암호화를 특히 사용 사례에 필요한 경우에만 활성화하는 것이 좋습니다.

- c. 선택 사항: 클러스터가 **FIPS 검증이 필요한 경우 FIPS 암호화** 활성화를 선택합니다.

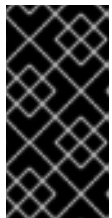
7. 다음을 클릭합니다.
8. 머신 풀 페이지에서 **컴퓨팅 노드 인스턴스 유형과 컴퓨팅 노드수를 선택합니다**. 사용 가능한 노드의 수 및 유형은 OpenShift Dedicated 서브스크립션에 따라 다릅니다. 여러 가용성 영역을 사용하는 경우 컴퓨팅 노드 수는 영역별로 계산됩니다.



**참고**

클러스터가 생성되면 컴퓨팅 노드 수를 변경할 수 있지만 생성된 머신 풀에서 컴퓨팅 노드 인스턴스 유형을 변경할 수 없습니다. 사용자 지정 인스턴스 유형을 사용하는 설치 후 머신 풀을 추가할 수 있습니다. OpenShift Dedicated 서브스크립션에 따라 사용할 수 있는 노드의 수 및 유형입니다.

9. 선택 사항: **노드 라벨 추가**를 확장하여 노드에 라벨을 추가합니다. 노드 레이블을 추가하려면 **Add additional label**를 클릭합니다.
10. 다음을 클릭합니다.
11. 클러스터 개인 정보 대화 상자에서 공개 또는 프라이빗 API 끝점과 클러스터의 애플리케이션 경로를 사용하려면 **Public** 또는 **Private**을 선택합니다.
12. 선택사항: 기존 GCP VPC(Virtual Private Cloud)에 클러스터를 설치하려면 다음을 수행합니다.
  - a. 기존 VPC에 설치를 선택합니다.
  - b. 기존 VPC에 설치하고 클러스터에 대해 HTTP 또는 HTTPS 프록시를 활성화하려면 클러스터 전체 프록시 구성을 선택합니다.
13. 다음을 클릭합니다.
14. 선택 사항: 클러스터를 GCP 공유 VPC에 설치하려면 다음을 수행합니다.



**중요**

공유 VPC에 클러스터를 설치하려면 OpenShift Dedicated 버전 4.13.15 이상을 사용해야 합니다. 또한 호스트 프로젝트의 VPC 소유자는 Google Cloud 콘솔에서 호스트 프로젝트로 프로젝트를 활성화해야 합니다. 자세한 내용은 [호스트 프로젝트 사용](#)을 참조하십시오.

- a. **GCP 공유 VPC에 설치**를 선택합니다.
- b. **Host 프로젝트 ID**를 지정합니다. 지정된 호스트 프로젝트 ID가 잘못된 경우 클러스터 생성에 실패합니다.



**중요**

클러스터 구성 마법사에서 단계를 완료하고 클러스터 **생성**을 클릭하면 클러스터가 "설치 대기 중" 상태로 전환됩니다. 이때 **Compute Network Administrator, Compute Security Administrator, DNS Administrator** 라는 역할을 동적으로 생성한 서비스 계정을 할당해야 하는 호스트 프로젝트의 VPC 소유자에 문의해야 합니다. 호스트 프로젝트의 VPC 소유자는 클러스터 생성에 실패하기 전에 나열된 권한을 부여하는 데 30일이 걸립니다. 공유 VPC 권한에 대한 자세한 내용은 [공유 VPC 프로비저닝](#)을 참조하십시오.



15. 기존 GCP VPC에 클러스터를 설치하도록 선택한 경우 **VPC(Virtual Private Cloud) 서브넷 설정**을 제공하고 **다음**을 선택합니다. Cloud NAT(네트워크 주소 변환) 및 클라우드 라우터를 생성해야 합니다. Cloud NAT 및 Google VPC에 대한 자세한 내용은 "추가 리소스" 섹션을 참조하십시오.



### 참고

Shared VPC에 클러스터를 설치하는 경우 호스트 프로젝트에서 VPC 이름과 서브넷이 공유됩니다.

16. **다음**을 클릭합니다.
17. 클러스터 전체 프록시를 구성하도록 선택하는 경우 클러스터 전체 프록시 페이지에 **프록시** 설정 세부 정보를 입력합니다.
- 다음 필드 중 하나 이상에 값을 입력합니다.
    - 유효한 **HTTP 프록시 URL** 을 지정합니다.
    - 유효한 **HTTPS 프록시 URL** 을 지정합니다.
    - 추가 신뢰 번들 필드에서 PEM 인코딩 X.509 인증서 번들을 제공합니다. 번들은 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** 인수 및 **https-proxy** 인수를 사용하여 명시적 구성이 필요한지 여부와 관계없이 적용됩니다.
  - 다음**을 클릭합니다.  
OpenShift Dedicated를 사용하여 프록시 구성에 대한 자세한 내용은 *클러스터 전체 프록시 구성*을 참조하십시오.
18. **CIDR 범위** 대화 상자에서 CIDR(사용자 정의 클래스 없는 도메인 간 라우팅) 범위를 구성하거나 제공된 기본값을 사용합니다.



### 중요

CIDR 구성은 나중에 변경할 수 없습니다. 계속하기 전에 네트워크 관리자에게 선택 사항을 확인합니다.

클러스터 개인 정보 보호가 **Private** 로 설정된 경우 클라우드 공급자의 프라이빗 연결을 구성할 때까지 클러스터에 액세스할 수 없습니다.

19. **Cluster update strategy** 페이지에서 업데이트 기본 설정을 구성합니다.
- 클러스터 업데이트 방법을 선택합니다.
    - 각 **업데이트**를 개별적으로 예약하려면 개별 업데이트를 선택합니다. 이는 기본 옵션입니다.
    - Recurring updates** to update your cluster on your preferred day and start time, when updates are available을 선택합니다.



**참고**

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

- b. 클러스터 업데이트 방법에 따라 관리자 승인을 제공합니다.
  - 개별 업데이트: 승인이 필요한 업데이트 버전을 선택하는 경우 관리자의 승인을 제공하고 승인을 **클릭하고 계속**.
  - 반복 업데이트: 클러스터에 대해 반복적인 업데이트를 선택한 경우 관리자의 승인을 제공한 후 승인을 **클릭하고 계속**. OpenShift Cluster Manager는 관리자의 승인을 받지 않고 마이너 버전에 대해 예정된 y-stream 업데이트를 시작하지 않습니다.
- c. 반복 업데이트를 선택한 경우 해당 요일을 선택하고 드롭다운 메뉴에서 UTC로 시작 시간을 업그레이드하십시오.
- d. 선택 사항: 클러스터 업그레이드 중에 **노드 트레이닝** 에 대한 유예 기간을 설정할 수 있습니다. 기본적으로 **1시간** 유예 기간이 설정됩니다.
- e. 다음을 클릭합니다.



**참고**

클러스터의 보안 또는 안정성에 큰 영향을 미치는 심각한 보안 문제가 있는 경우 Red Hat 사이트 안정성 엔지니어링(SRE)은 영향을 받지 않는 최신 z-stream 버전에 대한 자동 업데이트를 예약할 수 있습니다. 업데이트는 고객 알림이 제공된 후 48시간 이내에 적용됩니다. 심각한 영향을 미치는 보안 **등급**에 대한 자세한 내용은 [Red Hat 보안 등급 이해](#) 를 참조하십시오.

- 20. 선택 사항 요약을 검토하고 **클러스터 생성** 을 클릭하여 클러스터 설치를 시작합니다. 설치를 완료하는 데 약 30~40분이 걸립니다.
- 21. 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 **Status** 가 **Ready** 로 표시되면 클러스터가 준비 상태가 됩니다.

## 2.4. RED HAT 클라우드 계정으로 GCP에서 클러스터 생성

[OpenShift Cluster Manager](#) 를 통해 Red Hat이 소유한 표준 클라우드 공급자 계정을 사용하여 GCP(Google Cloud Platform)에 OpenShift Dedicated 클러스터를 생성할 수 있습니다.

**절차**

1. [OpenShift Cluster Manager](#) 에 로그인하고 **클러스터 생성** 을 클릭합니다.
2. **Cloud** 탭의 **Red Hat OpenShift Dedicated** 행에서 **클러스터 생성** 을 클릭합니다.

## 3. 청구 모델에서 서브스크립션 유형 및 인프라 유형을 구성합니다.

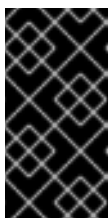
- a. 연간 구독 유형을 선택합니다. Red Hat 클라우드 계정을 사용하여 클러스터를 배포할 때는 **Annual** 서브스크립션 유형만 사용할 수 있습니다. OpenShift Dedicated 서브스크립션 옵션에 대한 자세한 내용은 OpenShift [Cluster Manager 설명서의 클러스터 서브스크립션 및 등록](#)을 참조하십시오.

**참고**

사용할 수 있는 **Annual** 구독 형식에 필요한 리소스 할당량이 있어야 합니다. 자세한 내용은 영업 담당자 또는 Red Hat 지원에 문의하십시오.

- b. **Red Hat이 소유한 클라우드 공급자 계정에** OpenShift Dedicated를 배포하려면 Red Hat 클라우드 계정 인프라 유형을 선택합니다.
  - c. 다음을 클릭합니다.
4. **Google Cloud Platform에서 실행**을 선택하고 다음을 클릭합니다.
5. **Cluster details** 페이지에서 클러스터 이름을 제공하고 클러스터 세부 정보를 지정합니다.

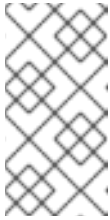
- a. 클러스터 이름을 추가합니다.
- b. 선택 사항: 클러스터 생성은 [openshiftapps.com](#)에서 프로비저닝된 클러스터의 하위 도메인으로 도메인 접두사를 생성합니다. 클러스터 이름이 15자 미만이면 도메인 접두사에 해당 이름이 사용됩니다. 클러스터 이름이 15자를 초과하면 도메인 접두사가 15자 문자열로 임의로 생성됩니다. 하위 도메인을 사용자 지정하려면 **사용자 지정 도메인 접두사 만들기** 확인란을 선택하고 도메인 접두사 필드에 **도메인 접두사** 이름을 입력합니다. 도메인 접두사는 15자를 초과할 수 없으며 조직 내에서 고유해야 하며 클러스터 생성 후에는 변경할 수 없습니다.
- c. **버전** 드롭다운 메뉴에서 클러스터 버전을 선택합니다.
- d. **리전** 드롭다운 메뉴에서 클라우드 공급자 **리전**을 선택합니다.
- e. **단일 영역** 또는 **다중 영역** 구성을 선택합니다.
- f. 선택 사항: 클러스터를 설치할 때 **보호된 VM을 사용하도록 Secure Boot forShielded VM**을 선택합니다. 자세한 내용은 [Shielded VMs](#)를 참조하십시오.

**중요**

클러스터를 성공적으로 만들려면 조직에 정책 **제약 조건 제약 조건/compute.requireShieldedVm**이 활성화된 경우 **Shielded VM에 대해 Secure Boot 지원** 활성화를 선택해야 합니다. GCP 조직 정책 제약 조건에 대한 자세한 내용은 조직 정책 제약 [조건](#)을 참조하십시오.

- g. 클러스터의 **영구 스토리지** 용량을 선택합니다. 자세한 내용은 OpenShift Dedicated 서비스 정의의 **스토리지** 섹션을 참조하십시오.
- h. 클러스터에 필요한 **로드 밸런서** 수를 지정합니다. 자세한 내용은 OpenShift Dedicated 서비스 정의의 **로드 밸런서** 섹션을 참조하십시오.
- i. **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat site Reliability Engineer (SRE) 플랫폼 메트릭과 별도로 자체 프로젝트를 모니터링하도록 선택한 사용자 워크로드 모니터링 활성화. 이 옵션은 기본적으로 활성화되어 있습니다.

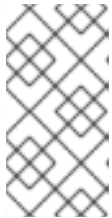
- j. 선택사항: **etcd 키 값 암호화가 필요한 경우 추가 etcd 암호화 사용을** 선택합니다. 이 옵션을 사용하면 etcd 키 값이 암호화되지만 키는 암호화되지 않습니다. 이 옵션은 기본적으로 OpenShift Dedicated 클러스터의 etcd 볼륨을 암호화하는 컨트롤 플레인 스토리지 암호화에 추가됩니다.



**참고**

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

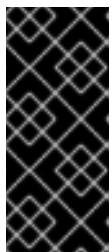
- k. 다음을 클릭합니다.
6. **Default** 머신 풀 페이지에서 **컴퓨팅 노드 인스턴스 유형과 컴퓨팅 노드 수를 선택**합니다. 사용 가능한 노드의 수 및 유형은 OpenShift Dedicated 서브스크립션에 따라 다릅니다. 여러 가용성 영역을 사용하는 경우 컴퓨팅 노드 수는 영역별로 계산됩니다.



**참고**

클러스터가 생성되면 컴퓨팅 노드 수를 변경할 수 있지만 머신 풀에서 컴퓨팅 노드 인스턴스 유형을 변경할 수 없습니다. CCS 모델을 사용하는 클러스터의 경우 다른 인스턴스 유형을 사용하는 설치 후 머신 풀을 추가할 수 있습니다. OpenShift Dedicated 서브스크립션에 따라 사용할 수 있는 노드의 수 및 유형입니다.

7. 선택 사항: **노드 라벨 편집** 을 확장하여 노드에 라벨을 추가합니다. **레이블 추가** 를 클릭하여 노드 레이블을 추가하고 다음을 선택합니다.
8. 클러스터 **개인 정보** 대화 상자에서 **공개** 또는 **프라이빗** API 끝점과 클러스터의 애플리케이션 경로를 사용하려면 **Public** 또는 **Private** 을 선택합니다.
9. 다음을 클릭합니다.
10. **CIDR 범위** 대화 상자에서 CIDR(사용자 정의 클래스 없는 도메인 간 라우팅) 범위를 구성하거나 제공된 기본값을 사용합니다.



**중요**

CIDR 구성은 나중에 변경할 수 없습니다. 계속하기 전에 네트워크 관리자에게 선택 사항을 확인합니다.

클러스터 개인 정보 보호가 **Private** 로 설정된 경우 클라우드 공급자의 프라이빗 연결을 구성할 때까지 클러스터에 액세스할 수 없습니다.

11. **Cluster update strategy** 페이지에서 업데이트 기본 설정을 구성합니다.
  - a. 클러스터 업데이트 방법을 선택합니다.
    - 각 업데이트를 개별적으로 예약하려면 개별 업데이트를 선택합니다. 이는 기본 옵션입니다.
    - **Recurring updates** to update your cluster on your preferred day and start time, when updates are available을 선택합니다.



### 참고

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

- b. 클러스터 업데이트 방법에 따라 관리자 승인을 제공합니다.
  - 개별 업데이트: 승인이 필요한 업데이트 버전을 선택하는 경우 관리자의 승인을 제공하고 승인을 **클릭하고 계속**.
  - 반복 업데이트: 클러스터에 대해 반복적인 업데이트를 선택한 경우 관리자의 승인을 제공한 후 승인을 **클릭하고 계속**. OpenShift Cluster Manager는 관리자의 승인을 받지 않고 마이너 버전에 대해 예정된 y-stream 업데이트를 시작하지 않습니다.
- c. 반복 업데이트를 선택한 경우 해당 요일을 선택하고 드롭다운 메뉴에서 UTC로 시작 시간을 업그레이드하십시오.
- d. 선택 사항: 클러스터 업그레이드 중에 **노드 트레이닝** 에 대한 유예 기간을 설정할 수 있습니다. 기본적으로 **1시간** 유예 기간이 설정됩니다.
- e. **다음**을 클릭합니다.



### 참고

클러스터의 보안 또는 안정성에 큰 영향을 미치는 심각한 보안 문제가 있는 경우 Red Hat 사이트 안정성 엔지니어링(SRE)은 영향을 받지 않는 최신 z-stream 버전에 대한 자동 업데이트를 예약할 수 있습니다. 업데이트는 고객 알림이 제공된 후 48시간 이내에 적용됩니다. 심각한 영향을 미치는 보안 **등급**에 대한 자세한 내용은 [Red Hat 보안 등급 이해](#) 를 참조하십시오.

12. 선택 사항 요약을 검토하고 **클러스터 생성**을 클릭하여 클러스터 설치를 시작합니다. 설치를 완료하는 데 약 30~40분이 걸립니다.
13. 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 **Status** 가 **Ready** 로 표시되면 클러스터가 준비 상태가 됩니다.

## 2.5. RED HAT MARKETPLACE를 사용하여 GCP에 클러스터 생성

OpenShift Cluster Manager Hybrid Cloud Console을 통해 Google Cloud에서 OpenShift Dedicated (OSD) 클러스터를 생성할 때 고객은 선호하는 청구 모델로 Red Hat Marketplace를 선택할 수 있습니다. OSD 가격은 사용량 기반이며 고객은 Red Hat Marketplace 계정을 통해 직접 청구됩니다.

### 절차

1. [OpenShift Cluster Manager](#) 에 로그인하고 **클러스터 생성**을 클릭합니다.
2. **Cloud** 탭의 **Red Hat OpenShift Dedicated** 행에서 **클러스터 생성**을 클릭합니다.

3. **청구 모델에서** 서브스크립션 유형 및 인프라 유형을 구성합니다.
  - a. **온 디맨드** 서브스크립션 유형을 선택합니다.
  - b. 드롭다운 메뉴에서 **Red Hat Marketplace** 를 선택합니다.
  - c. **다음**을 클릭합니다.
4. **클라우드 공급자** 페이지에서 다음을 수행합니다.
  - a. 클라우드 공급자로 **Google Cloud** 를 선택합니다.
  - b. 클러스터를 계속 생성하는 데 필요한 모든 사전 요구 사항을 읽고 완료했음을 나타내는 확인란을 클릭합니다.
  - c. 서비스 계정 키를 추가합니다.



**참고**

서비스 계정 키에 대한 자세한 내용은 **Service account 키** 옆에 있는 정보 아이콘을 클릭합니다.

- d. **다음**을 클릭하여 클라우드 공급자 계정을 확인하고 **클러스터 세부 정보** 페이지로 이동합니다.
5. **Cluster details** 페이지에서 클러스터 이름을 제공하고 클러스터 세부 정보를 지정합니다.
    - a. 클러스터 이름을 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. **리전** 드롭다운 메뉴에서 클라우드 공급자 **리전** 을 선택합니다.
    - e. **단일 영역** 또는 **다중 영역** 구성을 선택합니다.
    - f. 선택 사항: 클러스터를 설치할 때 **보호된 VM을 사용하도록 Secure Boot forShielded VM**을 선택합니다. 자세한 내용은 **Shielded VMs** 를 참조하십시오.



**중요**

클러스터를 성공적으로 만들려면 조직에 정책 **제약 조건 제약 조건/compute.requireShieldedVm** 이 활성화된 경우 **Shielded VM에 대해 Secure Boot 지원** 활성화를 선택해야 합니다. GCP 조직 정책 제약 조건에 대한 자세한 내용은 조직 정책 제약 **조건** 을 참조하십시오.

- g. **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat site Reliability Engineer (SRE) 플랫폼 메트릭과 별도로 자체 프로젝트를 모니터링하도록 선택한 사용자 워크로드 모니터링 활성화. 이 옵션은 기본적으로 활성화되어 있습니다.

6. 선택 사항: **고급 암호화를 확장하여 암호화 설정을 변경합니다.**
- 사용자 정의 KMS 키를 사용하려면 **Use Custom KMS keys**를 선택합니다. 사용자 정의 KMS 키를 사용하지 않으려면 기본 설정 **Use default KMS Keys**를 그대로 두십시오.



### 중요

사용자 정의 KMS 키를 사용하려면 IAM 서비스 계정 **osd-ccs-admin**에 **Cloud KMS CryptoKey Encrypter/Decrypter** 역할을 부여해야 합니다. 리소스에 역할을 부여하는 방법에 대한 자세한 내용은 [리소스에 대한 역할 부여](#)를 참조하십시오.

**Use Custom KMS keys**가 선택되어 있는 경우:

- 키 링 위치 드롭다운 메뉴에서 **키 링 위치**를 선택합니다.
  - 키 링 드롭다운 메뉴에서 **키 링**을 선택합니다.
  - 키 이름 드롭다운 메뉴에서 **키 이름**을 선택합니다.
  - KMS 서비스 계정을** 제공합니다.
- 선택사항: **etcd 키 값 암호화가 필요한 경우 추가 etcd 암호화 사용**을 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.



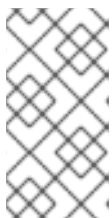
### 참고

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 계층이 도입된 결과입니다. etcd 암호화를 특히 사용 사례에 필요한 경우에만 활성화하는 것이 좋습니다.

- 선택 사항: 클러스터가 **FIPS 검증이 필요한 경우 FIPS 암호화**활성화를 선택합니다.

7. 다음을 클릭합니다.

- 머신 풀 페이지에서 **컴퓨팅 노드 인스턴스 유형과 컴퓨팅 노드 수**를 선택합니다. 사용 가능한 노드의 수 및 유형은 OpenShift Dedicated 서브스크립션에 따라 다릅니다. 여러 가용성 영역을 사용하는 경우 컴퓨팅 노드 수는 영역별로 계산됩니다.



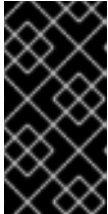
### 참고

클러스터가 생성되면 컴퓨팅 노드 수를 변경할 수 있지만 생성된 머신 풀에서 컴퓨팅 노드 인스턴스 유형을 변경할 수 없습니다. 사용자 지정 인스턴스 유형을 사용하는 설치 후 머신 풀을 추가할 수 있습니다. OpenShift Dedicated 서브스크립션에 따라 사용할 수 있는 노드의 수 및 유형입니다.

- 선택 사항: **노드 라벨 추가**를 확장하여 노드에 라벨을 추가합니다. 노드 레이블을 추가하려면 **Add additional label**를 클릭합니다.
- 다음을 클릭합니다.



11. 클러스터 개인 정보 대화 상자에서 공개 또는 프라이빗 API 끝점과 클러스터의 애플리케이션 경로를 사용하려면 **Public** 또는 **Private** 을 선택합니다.
12. 선택사항: 기존 GCP VPC(Virtual Private Cloud)에 클러스터를 설치하려면 다음을 수행합니다.
  - a. 기존 VPC에 설치를 선택합니다.
  - b. 기존 VPC에 설치하고 클러스터에 대해 HTTP 또는 HTTPS 프록시를 활성화하려면 클러스터 전체 프록시 구성을 선택합니다.
13. 다음을 클릭합니다.
14. 선택 사항: 클러스터를 GCP 공유 VPC에 설치하려면 다음을 수행합니다.



**중요**

공유 VPC에 클러스터를 설치하려면 OpenShift Dedicated 버전 4.13.15 이상을 사용해야 합니다. 또한 호스트 프로젝트의 VPC 소유자는 Google Cloud 콘솔에서 호스트 프로젝트로 프로젝트를 활성화해야 합니다. 자세한 내용은 [호스트 프로젝트 사용](#)을 참조하십시오.

- a. **GCP 공유 VPC에 설치를 선택합니다.**
- b. **Host 프로젝트 ID** 를 지정합니다. 지정된 호스트 프로젝트 ID가 잘못된 경우 클러스터 생성에 실패합니다.



**중요**

클러스터 구성 마법사에서 단계를 완료하고 클러스터 생성 을 클릭하면 클러스터가 "설치 대기 중" 상태로 전환됩니다. 이때 **Compute Network Administrator, Compute Security Administrator, DNS Administrator** 라는 역할을 동적으로 생성한 서비스 계정을 할당해야 하는 호스트 프로젝트의 VPC 소유자에 문의해야 합니다. 호스트 프로젝트의 VPC 소유자는 클러스터 생성에 실패하기 전에 나열된 권한을 부여하는 데 30일이 걸립니다. 공유 VPC 권한에 대한 자세한 내용은 [공유 VPC 프로비저닝](#) 을 참조하십시오.

15. 기존 GCP VPC에 클러스터를 설치하도록 선택한 경우 **VPC(Virtual Private Cloud) 서브넷 설정** 을 제공하고 다음을 선택합니다. Cloud NAT(네트워크 주소 변환) 및 클라우드 라우터를 생성해야 합니다. Cloud NAT 및 Google VPC에 대한 자세한 내용은 "추가 리소스" 섹션을 참조하십시오.



**참고**

Shared VPC에 클러스터를 설치하는 경우 호스트 프로젝트에서 VPC 이름과 서브넷이 공유됩니다.

16. 다음을 클릭합니다.
17. 클러스터 전체 프록시를 구성하도록 선택하는 경우 클러스터 전체 프록시 페이지에 **프록시 설정** 세부 정보를 입력합니다.
  - a. 다음 필드 중 하나 이상에 값을 입력합니다.
    - 유효한 **HTTP 프록시 URL** 을 지정합니다.
    - 유효한 **HTTPS 프록시 URL** 을 지정합니다.

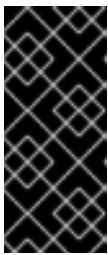


- 추가 신뢰 번들 필드에서 PEM 인코딩 X.509 인증서 번들을 제공합니다. 번들은 클러스터 노드의 신뢰할 수 있는 인증서 저장소에 추가됩니다. 프록시의 ID 인증서가 RHCOS(Red Hat Enterprise Linux CoreOS) 신뢰 번들의 기관에서 서명되지 않는 한 TLS 지정 프록시를 사용하는 경우 추가 신뢰 번들 파일이 필요합니다. 이 요구 사항은 프록시가 투명했는지 또는 **http-proxy** 인수 및 **https-proxy** 인수를 사용하여 명시적 구성이 필요한지 여부와 관계없이 적용됩니다.

b. 다음을 클릭합니다.

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

18. **CIDR 범위** 대화 상자에서 CIDR(사용자 정의 클래스 없는 도메인 간 라우팅) 범위를 구성하거나 제공된 기본값을 사용합니다.



### 중요

CIDR 구성은 나중에 변경할 수 없습니다. 계속하기 전에 네트워크 관리자에게 선택 사항을 확인합니다.

클러스터 개인 정보 보호가 **Private** 로 설정된 경우 클라우드 공급자의 프라이빗 연결을 구성할 때까지 클러스터에 액세스할 수 없습니다.

19. **Cluster update strategy** 페이지에서 업데이트 기본 설정을 구성합니다.

a. 클러스터 업데이트 방법을 선택합니다.

- 각 업데이트를 개별적으로 예약하려면 개별 업데이트를 선택합니다. 이는 기본 옵션입니다.
- **Recurring updates** to update your cluster on your preferred day and start time, when updates are available을 선택합니다.



### 참고

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

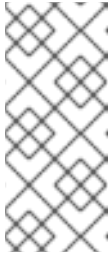
b. 클러스터 업데이트 방법에 따라 관리자 승인을 제공합니다.

- 개별 업데이트: 승인이 필요한 업데이트 버전을 선택하는 경우 관리자의 승인을 제공하고 승인을 **클릭하고 계속**.
- 반복 업데이트: 클러스터에 대해 반복적인 업데이트를 선택한 경우 관리자의 승인을 제공한 후 승인을 **클릭하고 계속**. OpenShift Cluster Manager는 관리자의 승인을 받지 않고 마이너 버전에 대해 예정된 y-stream 업데이트를 시작하지 않습니다.

c. 반복 업데이트를 선택한 경우 해당 요일을 선택하고 드롭다운 메뉴에서 UTC로 시작 시간을 업그레이드하십시오.

d. 선택 사항: 클러스터 업그레이드 중에 **노드 트레이닝**에 대한 유예 기간을 설정할 수 있습니다. 기본적으로 **1시간** 유예 기간이 설정됩니다.

e. 다음을 클릭합니다.



### 참고

클러스터의 보안 또는 안정성에 큰 영향을 미치는 심각한 보안 문제가 있는 경우 Red Hat 사이트 안정성 엔지니어링(SRE)은 영향을 받지 않는 최신 z-stream 버전에 대한 자동 업데이트를 예약할 수 있습니다. 업데이트는 고객 알림이 제공된 후 48시간 이내에 적용됩니다. 심각한 영향을 미치는 보안 등급에 대한 자세한 내용은 [Red Hat 보안 등급 이해](#)를 참조하십시오.

20. 선택 사항 요약을 검토하고 **클러스터 생성**을 클릭하여 클러스터 설치를 시작합니다. 설치를 완료하는 데 약 30~40분이 걸립니다.
21. 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 **Status** 가 **Ready** 로 표시되면 클러스터가 준비 상태가 됩니다.

## 2.6. 추가 리소스

- OpenShift Dedicated를 사용하여 프록시를 구성하는 방법에 대한 자세한 내용은 [클러스터 전체 프록시 구성](#)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.
- 클러스터 전체 프록시에 필요한 Cloud NAT(네트워크 주소 변환)에 대한 일반적인 정보는 Google 문서의 [Cloud NAT 개요](#)를 참조하십시오.
- 클러스터 전체 프록시에 필요한 클라우드 라우터에 대한 일반적인 정보는 Google 문서의 [클라우드 라우터 개요](#)를 참조하십시오.
- Google Cloud Provider 계정 내에서 VPC를 생성하는 방법에 대한 자세한 내용은 Google 문서에서 [VPC 네트워크 생성 및 관리](#)를 참조하십시오.

## 3장. ID 공급자 구성

OpenShift Dedicated 클러스터가 생성된 후 사용자가 클러스터에 액세스하기 위해 로그인하는 방법을 결정하도록 ID 공급자를 구성해야 합니다.

### 3.1. ID 공급자 이해

OpenShift Dedicated에는 기본 제공 OAuth 서버가 포함되어 있습니다. 개발자와 관리자는 OAuth 액세스 토큰을 가져와 API 인증을 수행합니다. 관리자는 클러스터를 설치한 후 ID 공급자를 지정하도록 OAuth를 구성할 수 있습니다. ID 공급자를 구성하면 사용자가 클러스터에 로그인하고 액세스할 수 있습니다.

#### 3.1.1. 지원되는 ID 공급자

다음 유형의 ID 공급자를 구성할 수 있습니다.

ID 공급자	설명
GitHub 또는 GitHub Enterprise	GitHub 또는 GitHub Enterprise의 OAuth 인증 서버에 대해 사용자 이름 및 암호의 유효성을 확인하도록 GitHub ID 공급자를 구성합니다.
GitLab	<a href="https://gitlab.com">GitLab.com</a> 또는 기타 GitLab 인스턴스를 ID 공급자로 사용하도록 GitLab ID 공급자를 구성합니다.
Google	Google의 <a href="#">OpenID Connect</a> 통합을 사용하여 Google ID 공급자를 구성합니다.
LDAP	간단한 바인드 인증을 사용하여 LDAPv3 서버에 대해 사용자 이름 및 암호의 유효성을 확인하도록 LDAP ID 공급자를 구성합니다.
OpenID Connect	<a href="#">인증 코드 Flow</a> 를 사용하여 OIDC ID 공급자와 통합하도록 OIDC(OpenID Connect) ID 공급자를 구성합니다.
htpasswd	<p>단일 정적 관리 사용자에게 대해 htpasswd ID 공급자를 구성합니다. 사용자로 클러스터에 로그인하여 문제를 해결할 수 있습니다.</p> <div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  </div> <div style="flex: 2;"> <p><b>중요</b></p> <p>htpasswd ID 공급자 옵션은 단일 정적 관리 사용자를 생성할 수 있도록만 포함됩니다. htpasswd는 OpenShift Dedicated의 일반 ID 공급자로 지원되지 않습니다. 단일 사용자를 구성하는 단계는 <i>htpasswd ID 공급자 구성</i>을 참조하십시오.</p> </div> </div>

#### 3.1.2. ID 공급자 매개변수

다음 매개변수는 모든 ID 공급자에 공통입니다.

매개변수	설명
<b>name</b>	공급자 사용자 이름에 접두어로 공급자 이름을 지정하여 ID 이름을 만듭니다.

매개변수	설명
<b>mappingMethod</b>	<p>사용자가 로그인할 때 새 ID를 사용자에게 매핑하는 방법을 정의합니다. 다음 값 중 하나를 입력하십시오.</p> <p><b>claim</b> 기본값입니다. 사용자에게 ID의 기본 사용자 이름을 프로비저닝합니다. 해당 사용자 이름의 사용자가 이미 다른 ID에 매핑되어 있는 경우 실패합니다.</p> <p><b>lookup</b> 기존 ID, 사용자 ID 매핑 및 사용자를 조회하지만 사용자 또는 ID를 자동으로 프로비저닝하지는 않습니다. 클러스터 관리자는 이를 통해 수동으로 또는 외부 프로세스를 사용하여 ID 및 사용자를 설정할 수 있습니다. 이 방법을 사용하려면 사용자를 수동으로 프로비저닝해야 합니다.</p> <p><b>add</b> 사용자에게 ID의 기본 사용자 이름을 프로비저닝합니다. 해당 사용자 이름을 가진 사용자가 이미 존재하는 경우 ID가 기존 사용자에게 매핑되고 그 사용자의 기존 ID 매핑에 추가됩니다. 동일한 사용자 집합을 식별하고 동일한 사용자 이름에 매핑되는 ID 공급자를 여러 구성한 경우 필요합니다.</p>



**참고**

ID 공급자를 추가하거나 변경할 때 **mappingMethod** 매개변수를 **add**로 설정하면 새 공급자의 ID를 기존 사용자에게 매핑할 수 있습니다.

### 3.2. GITHUB ID 공급자 구성

GitHub 또는 GitHub Enterprise의 OAuth 인증 서버에 대해 사용자 이름 및 암호의 유효성을 검사하고 OpenShift Dedicated 클러스터에 액세스하도록 GitHub ID 공급자를 구성합니다. OAuth는 OpenShift Dedicated와 GitHub 또는 GitHub Enterprise 간의 토큰 교환 흐름을 용이하게 합니다.



**주의**

GitHub 인증을 구성하면 사용자가 GitHub 자격 증명을 사용하여 OpenShift Dedicated에 로그인할 수 있습니다. GitHub 사용자 ID가 있는 사람이 OpenShift Dedicated 클러스터에 로그인하지 못하도록 특정 GitHub 조직 또는 팀의 사용자만 액세스를 제한해야 합니다.

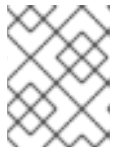
**사전 요구 사항**

- OAuth 애플리케이션은 GitHub 조직 관리자가 [GitHub 조직 설정에서](#) 직접 생성해야 합니다.
- [GitHub 조직 또는 팀](#)은 GitHub 계정에 설정됩니다.

**절차**

1. [OpenShift Cluster Manager](#) 에서 **Cluster List** 페이지로 이동하여 ID 공급자를 구성하는 데 필요한 클러스터를 선택합니다.

2. 액세스 제어 탭을 클릭합니다.
3. ID 공급자 추가를 클릭합니다.



#### 참고

클러스터 생성 후 표시된 경고 메시지에서 **Oauth 구성 추가** 링크를 클릭하여 ID 공급자를 구성할 수도 있습니다.

4. 드롭다운 메뉴에서 **GitHub** 를 선택합니다.
5. ID 공급자의 고유 이름을 입력합니다. 이 이름은 나중에 변경할 수 없습니다.
  - **OAuth 콜백 URL** 은 제공된 필드에 자동으로 생성됩니다. 이를 사용하여 GitHub 애플리케이션을 등록합니다.

```
https://oauth-openshift.apps.<cluster_name>.  
<cluster_domain>/oauth2callback/<idp_provider_name>
```

예를 들면 다음과 같습니다.

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/github
```

6. **GitHub에 애플리케이션을 등록** 합니다.
7. OpenShift Dedicated로 돌아가서 드롭다운 메뉴에서 매핑 방법을 선택합니다. 대부분의 경우 **클레임** 이 권장됩니다.
8. GitHub에서 제공하는 **클라이언트 ID** 및 **클라이언트 시크릿** 을 입력합니다.
9. **호스트 이름을 입력합니다.** 호스팅된 GitHub Enterprise 인스턴스를 사용하는 경우 호스트 이름을 입력해야 합니다.
10. 선택 사항: CA(인증 기관) 파일을 사용하여 구성된 GitHub Enterprise URL에 대한 서버 인증서를 검증할 수 있습니다. **찾아보기**를 클릭하여 **CA 파일**을 찾아 ID 공급자에 연결합니다.
11. **Use organizations** or **Use teams** to restrict access to a particular GitHub organization or a GitHub team을 선택합니다.
12. 액세스를 제한하려는 조직 또는 팀의 이름을 입력합니다. **추가** 를 클릭하여 사용자가 멤버가 될 수 있는 여러 조직 또는 팀을 지정합니다.
13. **Confirm** 을 클릭합니다.

#### 검증

- 이제 구성된 ID 공급자가 **클러스터 목록** 페이지의 **액세스 제어** 탭에 표시됩니다.

### 3.3. GITLAB ID 공급자 구성

[GitLab.com](https://gitlab.com) 또는 기타 GitLab 인스턴스를 ID 공급자로 사용하도록 GitLab ID 공급자를 구성합니다.

#### 사전 요구 사항

- GitLab 버전 7.7.0~11.0을 사용하는 경우 **OAuth 통합**을 사용하여 연결합니다. GitLab 버전 11.1 이상을 사용하는 경우 OAuth 대신 **OpenID Connect(OIDC)**를 사용하여 연결할 수 있습니다.

절차

1. **OpenShift Cluster Manager** 에서 **Cluster List** 페이지로 이동하여 ID 공급자를 구성하는 데 필요한 클러스터를 선택합니다.
2. **액세스 제어** 탭을 클릭합니다.
3. **ID 공급자 추가**를 클릭합니다.



참고

클러스터 생성 후 표시된 경고 메시지에서 **Oauth 구성 추가** 링크를 클릭하여 ID 공급자를 구성할 수도 있습니다.

4. 드롭다운 메뉴에서 **GitLab** 을 선택합니다.
5. ID 공급자의 고유 이름을 입력합니다. 이 이름은 나중에 변경할 수 없습니다.
  - **OAuth 콜백 URL** 은 제공된 필드에 자동으로 생성됩니다. 이 URL을 GitLab에 제공합니다.

```
https://oauth-openshift.apps.<cluster_name>.<cluster_domain>/oauth2callback/<idp_provider_name>
```

예를 들면 다음과 같습니다.

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/gitlab
```

6. **GitLab에 새 애플리케이션을 추가**합니다.
7. OpenShift Dedicated로 돌아가서 드롭다운 메뉴에서 매핑 방법을 선택합니다. 대부분의 경우 **클레임** 이 권장됩니다.
8. GitLab에서 제공하는 **클라이언트 ID** 및 **클라이언트 시크릿** 을 입력합니다.
9. GitLab 공급자의 **URL** 을 입력합니다.
10. 선택 사항: CA(인증 기관) 파일을 사용하여 구성된 GitLab URL에 대한 서버 인증서를 검증할 수 있습니다. **찾아보기**를 클릭하여 **CA 파일**을 찾아 ID 공급자에 연결합니다.
11. **Confirm** 을 클릭합니다.

검증

- 이제 구성된 ID 공급자가 **클러스터 목록** 페이지의 **액세스 제어** 탭에 표시됩니다.

### 3.4. GOOGLE ID 공급자 구성

사용자가 Google 자격 증명으로 인증할 수 있도록 Google ID 공급자를 구성합니다.



### 주의

Google을 ID 공급자로 사용하면 모든 Google 사용자가 서버 인증을 수행할 수 있습니다. **hostedDomain** 구성 속성을 사용하여 특정 호스트 도메인의 멤버 인증을 제한할 수 있습니다.

### 절차

1. **OpenShift Cluster Manager** 에서 **Cluster List** 페이지로 이동하여 ID 공급자를 구성하는 데 필요한 클러스터를 선택합니다.
2. **액세스 제어** 탭을 클릭합니다.
3. **ID 공급자 추가**를 클릭합니다.



### 참고

클러스터 생성 후 표시된 경고 메시지에서 **Oauth 구성 추가** 링크를 클릭하여 ID 공급자를 구성할 수도 있습니다.

4. 드롭다운 메뉴에서 **Google** 을 선택합니다.
5. ID 공급자의 고유 이름을 입력합니다. 이 이름은 나중에 변경할 수 없습니다.
  - **OAuth 콜백 URL** 은 제공된 필드에 자동으로 생성됩니다. 이 URL을 Google에 제공합니다.

```
https://oauth-openshift.apps.<cluster_name>.  
<cluster_domain>/oauth2callback/<idp_provider_name>
```

예를 들면 다음과 같습니다.

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/google
```

6. Google 의 **OpenID Connect** 통합을 사용하여 **Google ID** 공급자를 구성합니다.
7. OpenShift Dedicated로 돌아가서 드롭다운 메뉴에서 매핑 방법을 선택합니다. 대부분의 경우 **클레임** 이 권장됩니다.
8. 등록된 Google 프로젝트의 **클라이언트 ID** 와 Google에서 발행한 **클라이언트 시크릿** 을 입력합니다.
9. 사용자를 Google Apps 도메인으로 제한하려면 **호스팅 도메인** 을 입력합니다.
10. **Confirm** 을 클릭합니다.

### 검증

- 이제 구성된 ID 공급자가 **클러스터 목록** 페이지의 **액세스 제어** 탭에 표시됩니다.

## 3.5. LDAP ID 공급자 구성



간단한 바인드 인증을 사용하여 LDAPv3 서버에 대해 사용자 이름 및 암호의 유효성을 확인하도록 LDAP ID 공급자를 구성합니다.

### 사전 요구 사항

- LDAP ID 공급자를 구성할 때 구성된 **LDAP URL** 을 입력해야 합니다. 구성된 URL은 RFC 2255 URL로, 사용할 LDAP 호스트 및 검색 매개변수를 지정합니다. URL 구문은 다음과 같습니다.

```
ldap://host:port/basedn?attribute?scope?filter
```

URL 구성 요소	설명
<b>ldap</b>	일반 LDAP의 경우 <b>ldap</b> 문자열을 사용합니다. 보안 LDAP(LDAPS)의 경우 대신 <b>ldaps</b> 를 사용합니다.
<b>host:port</b>	LDAP 서버의 이름 및 포트입니다. ldap의 경우 기본값은 <b>localhost:389</b> 이고 LDAPS의 경우 <b>localhost:636</b> 입니다.
<b>basedn</b>	모든 검색을 시작해야 하는 디렉터리 분기의 DN입니다. 적어도 디렉터리 트리의 맨 위에 있어야 하지만 디렉터리에 하위 트리를 지정할 수도 있습니다.
<b>attribute</b>	검색할 속성입니다. RFC 2255에서는 쉼표로 구분된 속성 목록을 사용할 수 있지만 제공되는 속성 수와 관계없이 첫 번째 속성만 사용됩니다. 속성이 제공되지 않는 경우 기본값은 <b>uid</b> 를 사용하는 것입니다. 사용할 하위 트리의 모든 항목에서 고유한 속성을 선택하는 것이 좋습니다.
<b>scope</b>	검색 범위입니다. <b>one</b> 또는 <b>sub</b> 일 수 있습니다. 범위가 제공되지 않는 경우 기본값은 <b>sub</b> 범위를 사용하는 것입니다.
<b>filter</b>	유효한 LDAP 검색 필터입니다. 제공하지 않는 경우 기본값은 <b>(objectClass=*)</b> 입니다.

검색을 수행할 때 속성, 필터, 제공된 사용자 이름을 결합하여 다음과 같은 검색 필터가 생성됩니다.

```
(<(<filter>)<attribute>=<username>))
```



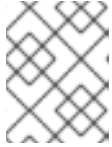
### 중요

LDAP 디렉터리에서 검색에 인증이 필요한 경우 항목을 검색하는 데 사용할 **bindDN** 및 **bindPassword**를 지정하십시오.

### 절차

- [OpenShift Cluster Manager](#) 에서 **Cluster List** 페이지로 이동하여 ID 공급자를 구성하는 데 필요한 클러스터를 선택합니다.
- 액세스 제어** 탭을 클릭합니다.
- ID 공급자 추가**를 클릭합니다.





## 참고

클러스터 생성 후 표시된 경고 메시지에서 **Oauth** 구성 추가 링크를 클릭하여 ID 공급자를 구성할 수도 있습니다.

4. 드롭다운 메뉴에서 **LDAP** 를 선택합니다.
5. ID 공급자의 고유 이름을 입력합니다. 이 이름은 나중에 변경할 수 없습니다.
6. 드롭다운 메뉴에서 매핑 방법을 선택합니다. 대부분의 경우 **클레임** 이 권장됩니다.
7. 사용할 LDAP 검색 매개변수를 지정하려면 **LDAP URL** 을 입력합니다.
8. 선택 사항: **DN 바인딩** 을 입력하고 **암호를 바인딩** 합니다.
9. LDAP 속성을 ID에 매핑할 속성을 입력합니다.
  - 해당 값을 사용자 **ID** 로 사용해야 하는 ID 특성을 입력합니다. **추가** 를 클릭하여 여러 ID 특성을 추가합니다.
  - 선택 사항: **표시 이름**으로 값을 사용해야 하는 미리 정의된 사용자 이름 특성을 입력합니다. **추가** 를 클릭하여 여러 기본 사용자 이름 속성을 추가합니다.
  - 선택 사항: 이메일 주소로 값을 사용해야 하는 **Email** 특성을 입력합니다. **추가** 를 클릭하여 여러 이메일 속성을 추가합니다.
10. 선택 사항: **고급 옵션 표시**를 클릭하여 LDAP ID 공급자에 CA(인증 기관) 파일을 추가하여 구성된 URL의 서버 인증서를 검증합니다. **찾아보기**를 클릭하여 **CA 파일**을 찾아 ID 공급자에 연결합니다.
11. 선택 사항: 고급 옵션 아래 LDAP 공급자를 **Insecure** 로 설정할 수 있습니다. 이 옵션을 선택하면 CA 파일을 사용할 수 없습니다.



## 중요

비보안 LDAP 연결(ldap:// 또는 포트 389)을 사용하는 경우 구성 마법사에서 **Insecure** 옵션을 확인해야 합니다.

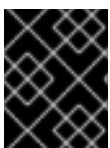
12. **Confirm** 을 클릭합니다.

## 검증

- 이제 구성된 ID 공급자가 클러스터 목록 페이지의 **액세스 제어** 탭에 표시됩니다.

## 3.6. OPENID ID 공급자 구성

**인증 코드 흐름**을 사용하여 OpenID Connect ID 공급자와 통합하도록 OpenID ID 공급자를 구성합니다.



## 중요

OpenShift Dedicated의 Authentication Operator는 구성된 OpenID Connect ID 공급자가 **OpenID Connect** 검색 사양을 구현해야 합니다.

클레임은 OpenID ID 공급자에서 반환된 JWT **id\_token** 및 Issuer URL에서 반환하는 JSON에서 읽습니다.

사용자 ID로 사용할 하나 이상의 클레임을 구성해야 합니다.

또한 사용자의 기본 사용자 이름, 표시 이름, 이메일 주소로 사용할 클레임을 나타낼 수도 있습니다. 여러 클레임이 지정되는 경우 비어 있지 않은 값이 있는 첫 번째 클레임이 사용됩니다. 표준 클레임은 다음과 같습니다.

클레임	설명
<b>preferred_username</b>	사용자를 프로비저닝할 때 사용하는 기본 사용자 이름입니다. 사용자가 사용하고자 하는 약칭입니다(예: <b>janedoe</b> ). 일반적으로 인증 시스템의 사용자 로그인 또는 사용자 이름에 해당하는 값입니다(예: 사용자 이름 또는 이메일).
<b>email</b>	이메일 주소입니다.
<b>name</b>	표시 이름입니다.

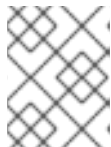
자세한 내용은 [OpenID 클레임 설명서](#)를 참조하십시오.

### 사전 요구 사항

- OpenID Connect를 구성하기 전에 OpenShift Dedicated 클러스터에서 사용하려는 Red Hat 제품 또는 서비스의 설치 사전 요구 사항을 확인하십시오.

### 절차

1. [OpenShift Cluster Manager](#) 에서 **Cluster List** 페이지로 이동하여 ID 공급자를 구성하는 데 필요한 클러스터를 선택합니다.
2. **액세스 제어** 탭을 클릭합니다.
3. **ID 공급자 추가**를 클릭합니다.



### 참고

클러스터 생성 후 표시된 경고 메시지에서 **OAuth 구성 추가** 링크를 클릭하여 ID 공급자를 구성할 수도 있습니다.

4. 드롭다운 메뉴에서 **OpenID** 를 선택합니다.
5. ID 공급자의 고유 이름을 입력합니다. 이 이름은 나중에 변경할 수 없습니다.
  - **OAuth 콜백 URL** 은 제공된 필드에 자동으로 생성됩니다.

```
https://oauth-openshift.apps.<cluster_name>.<cluster_domain>/oauth2callback/<idp_provider_name>
```

예를 들면 다음과 같습니다.

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/openid
```

6. **인증 요청을 생성하는** 단계에 따라 OpenID ID 공급자에 새 OpenID Connect 클라이언트를 등록합니다.
7. OpenShift Dedicated로 돌아가서 드롭다운 메뉴에서 매핑 방법을 선택합니다. 대부분의 경우 **클레임** 이 권장됩니다.
8. Open ID에서 제공하는 **클라이언트 ID 및 클라이언트 시크릿** 을 입력합니다.
9. **발급자 URL** 을 입력합니다. OpenID 공급자가 발급자 식별자로 간주하는 URL입니다. URL 쿼리 매개변수 또는 조각이 없는 https 스키마를 사용해야 합니다.
10. 이메일 주소로 값을 사용해야 하는 **Email** 속성을 입력합니다. **추가** 를 클릭하여 여러 이메일 속성을 추가합니다.
11. 기본 사용자 이름으로 사용해야 하는 **Name** 속성을 입력합니다. **추가** 를 클릭하여 여러 기본 사용자 이름을 추가합니다.
12. 표시 이름으로 값을 사용해야 하는 **Preferred username** 속성을 입력합니다. **추가** 를 클릭하여 여러 디스플레이 이름을 추가합니다.
13. 선택 사항: **고급 옵션 표시** 를 클릭하여 OpenID ID 공급자에 CA(인증 기관) 파일을 추가합니다.
14. 선택 사항: 고급 옵션 아래 **추가 범위** 를 추가할 수 있습니다. 기본적으로 **OpenID** 범위가 요청됩니다.
15. **Confirm** 을 클릭합니다.

#### 검증

- 이제 구성된 ID 공급자가 **클러스터 목록** 페이지의 **액세스 제어** 탭에 표시됩니다.

### 3.7. HTPASSWD ID 공급자 구성

htpasswd ID 공급자를 구성하여 클러스터 관리 권한이 있는 단일 정적 사용자를 생성합니다. 사용자로 클러스터에 로그인하여 문제를 해결할 수 있습니다.



#### 중요

htpasswd ID 공급자 옵션은 단일 정적 관리 사용자를 생성할 수 있도록만 포함됩니다. htpasswd는 OpenShift Dedicated의 일반 ID 공급자로 지원되지 않습니다.

#### 절차

1. [OpenShift Cluster Manager](#) 에서 **클러스터 목록** 페이지로 이동하여 클러스터를 선택합니다.
2. **액세스 제어** → **ID 공급자** 를 선택합니다.
3. **ID 공급자 추가** 를 클릭합니다.
4. **Identity Provider** 드롭다운 메뉴에서 **HTPasswd** 를 선택합니다.
5. ID 공급자의 **이름** 필드에 고유한 이름을 추가합니다.
6. 정적 사용자에 대해 제안된 사용자 이름과 암호를 사용하거나 고유한 사용자 이름을 만듭니다.



**참고**

이 단계에서 정의된 인증 정보는 다음 단계에서 **추가** 를 선택하면 표시되지 않습니다. 인증 정보가 손실된 경우 ID 공급자를 다시 생성하고 인증 정보를 다시 정의해야 합니다.

7. **추가** 를 선택하여 htpasswd ID 공급자 및 단일 정적 사용자를 생성합니다.
8. 클러스터를 관리할 수 있는 정적 사용자 권한을 부여합니다.
  - a. **액세스 제어** → **클러스터 역할 및 액세스**에서 **사용자 추가** 를 선택합니다.
  - b. 이전 단계에서 생성한 정적 사용자의 **사용자 ID** 를 입력합니다.
  - c. **그룹**을 선택합니다.
    - CCO(Customer Cloud Subscription) 인프라 유형을 사용하여 OpenShift Dedicated를 설치하는 경우 **dedicated-admins** 또는 **cluster-admins** 그룹을 선택합니다. **dedicated-admins** 그룹의 사용자는 OpenShift Dedicated에 대한 표준 관리 권한이 있습니다. **cluster-admins** 그룹의 사용자는 클러스터에 대한 전체 관리 액세스 권한이 있습니다.
    - Red Hat 클라우드 계정 인프라 유형을 사용하여 OpenShift Dedicated를 설치하는 경우 **dedicated-admins** 그룹이 자동으로 선택됩니다.
  - d. **Add user** 를 선택하여 사용자에게 관리 권한을 부여합니다.

**검증**

- 구성된 htpasswd ID 공급자는 **액세스 제어** → **ID 공급자** 페이지에 표시됩니다.



**참고**

ID 공급자를 생성한 후 일반적으로 동기화는 2분 이내에 완료됩니다. htpasswd ID 공급자를 사용 가능한 후 사용자로 클러스터에 로그인할 수 있습니다.

- 단일 관리 사용자는 **액세스 제어** → **클러스터 역할 및 액세스** 페이지에 표시됩니다. 사용자의 관리 그룹 멤버십도 표시됩니다.

**추가 리소스**

- [고객 관리자 사용자](#)

**3.8. 클러스터에 액세스**

ID 공급자를 구성한 후 사용자는 Red Hat OpenShift Cluster Manager에서 클러스터에 액세스할 수 있습니다.

**사전 요구 사항**

- [OpenShift Cluster Manager](#) 에 로그인했습니다.
- OpenShift Dedicated 클러스터를 생성하셨습니다.
- 클러스터의 ID 공급자를 구성했습니다.

- 구성된 ID 공급자에 사용자 계정을 추가했습니다.

#### 절차

1. [OpenShift Cluster Manager](#) 에서 액세스할 클러스터를 클릭합니다.
2. **콘솔 열기** 를 클릭합니다.
3. ID 공급자를 클릭하고 클러스터에 로그인할 수 있는 인증 정보를 제공합니다.
4. **콘솔 열기** 를 클릭하여 클러스터의 웹 콘솔을 엽니다.
5. ID 공급자를 클릭하고 클러스터에 로그인할 수 있는 인증 정보를 제공합니다. 공급자가 제공하는 권한 부여 요청을 완료합니다.

## 4장. OPENSIFT DEDICATED 클러스터에 대한 권한 및 액세스 권한 취소

클러스터 소유자는 OpenShift Dedicated 클러스터에 대한 관리자 권한 및 사용자 액세스를 취소할 수 있습니다.


### 4.1. 사용자의 관리자 권한 해지

이 섹션의 단계에 따라 사용자의 **dedicated-admin** 권한을 취소합니다.

#### 사전 요구 사항

- [OpenShift Cluster Manager](#) 에 로그인했습니다.
- OpenShift Dedicated 클러스터를 생성하셨습니다.
- 클러스터의 GitHub ID 공급자를 구성하고 ID 공급자 사용자를 추가했습니다.
- 사용자에게 **dedicated-admin** 권한이 부여되었습니다.

#### 절차

1. [OpenShift Cluster Manager](#) 로 이동하여 클러스터를 선택합니다.
2. **액세스 제어** 탭을 클릭합니다.
3. 클러스터 역할 및 액세스 탭에서 사용자 옆에 있는  를 선택하고 **삭제** 를 클릭합니다.

#### 검증

- 권한을 취소하면 사용자가 더 이상 **액세스 제어** → **클러스터 역할 및 클러스터 역할** 페이지에서 **dedicated-admins** 그룹의 일부로 나열되지 않습니다.

### 4.2. 클러스터에 대한 사용자 액세스 해지

구성된 ID 공급자 공급자에서 해당 ID를 제거하여 ID 공급자 사용자의 클러스터 액세스를 취소할 수 있습니다.

OpenShift Dedicated 클러스터에 대해 다양한 유형의 ID 공급자를 구성할 수 있습니다. 다음 예제 절차에서는 클러스터에 대한 ID 프로비저닝을 위해 구성된 GitHub 조직 또는 팀의 멤버의 클러스터 액세스를 취소합니다.

#### 사전 요구 사항

- OpenShift Dedicated 클러스터가 있어야 합니다.
- GitHub 사용자 계정이 있습니다.
- 클러스터의 GitHub ID 공급자를 구성하고 ID 공급자 사용자를 추가했습니다.

#### 절차

1. [github.com](https://github.com) 으로 이동하여 GitHub 계정에 로그인합니다.
2. GitHub 조직 또는 팀에서 사용자를 제거합니다.
  - ID 공급자 구성에서 GitHub 조직을 사용하는 경우 GitHub 설명서의 [조직에서 멤버 제거](#) 단계를 따르십시오.
  - ID 공급자 구성에서 GitHub 조직 내의 팀을 사용하는 경우 GitHub 문서의 [팀에서 조직 멤버 제거](#) 의 단계를 따르십시오.

#### 검증

- ID 공급자에서 사용자를 제거한 후 사용자가 클러스터에 인증할 수 없습니다.

## 5장. OPENSIFT DEDICATED 클러스터 삭제

클러스터 소유자는 OpenShift Dedicated 클러스터를 삭제할 수 있습니다.

### 5.1. 클러스터 삭제

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

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

#### 절차

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.



#### 참고

GCP Shared VPC에 설치된 클러스터를 삭제하는 경우 VPC에게 호스트 프로젝트에게 클러스터 생성 중에 참조된 서비스 계정에 부여된 IAM 정책 역할을 제거하도록 알립니다.