



OpenShift Container Platform 4.17

설치 개요

OpenShift Container Platform 설치를 위한 개요 콘텐츠

OpenShift Container Platform 4.17 설치 개요

OpenShift Container Platform 설치를 위한 개요 콘텐츠

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[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

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

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] 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[®] 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 OpenShift Container Platform을 설치하는 방법에 대한 개요를 설명합니다.

Table of Contents

1장. OPENSIFT CONTAINER PLATFORM 설치 프로그램 개요	3
1.1. OPENSIFT CONTAINER PLATFORM 설치 정보	3
1.2. OPENSIFT CONTAINER PLATFORM 클러스터에서 지원되는 플랫폼	11
2장. 클러스터 설치 방법 선택 및 사용자를 위한 준비	14
2.1. 클러스터 설치 유형 선택	14
2.2. 설치 후 사용자용 클러스터 준비	16
2.3. 워크로드를 위한 클러스터 준비	16
2.4. 다른 플랫폼에 지원되는 설치 방법	17
3장. 클러스터 기능	21
3.1. 클러스터 기능 활성화	21
3.2. OPENSIFT CONTAINER PLATFORM 4.17의 선택적 클러스터 기능	23
3.3. 클러스터 기능 보기	32
3.4. 기존 기능 세트를 설정하여 클러스터 기능 활성화	32
3.5. 추가 활성화된 기능을 설정하여 클러스터 기능 활성화	33
4장. FIPS 암호화 지원	35
4.1. OC ADM EXTRACT를 사용하여 FIPS 지원 설치 프로그램 가져오기	35
4.2. 공용 OPENSIFT 미러를 사용하여 FIPS 지원 설치 프로그램 가져오기	36
4.3. OPENSIFT CONTAINER PLATFORM에서 FIPS 검증	37
4.4. 클러스터가 사용되는 구성 요소에서 FIPS 지원	38
4.5. FIPS 모드에서 클러스터 설치	39

1장. OPENSIFT CONTAINER PLATFORM 설치 프로그램 개요

1.1. OPENSIFT CONTAINER PLATFORM 설치 정보

OpenShift Container Platform 설치 프로그램은 클러스터를 배포하는 네 가지 방법을 제공하며, 다음 목록에서 자세히 설명합니다:

- **대화형:** 웹 기반 [지원 설치 관리자](#)를 사용하여 클러스터를 배포할 수 있습니다. 이는 인터넷에 연결된 네트워크가 있는 클러스터에 이상적인 방법입니다. 지원 설치 프로그램은 OpenShift Container Platform을 설치하는 가장 쉬운 방법이며, 스마트 기본값을 제공하며 클러스터를 설치하기 전에 사전 진행 중 검증을 수행합니다. 자동화 및 고급 구성 시나리오를 위한 RESTful API도 제공합니다.
- **로컬 에이전트 기반:** 연결이 끊긴 환경 또는 제한된 네트워크를 위해 에이전트 기반 설치 관리자를 사용하여 로컬로 클러스터를 배포할 수 있습니다. 지원 설치 관리자의 많은 이점을 제공하지만 먼저 [에이전트 기반 설치 관리자](#)를 다운로드하고 구성해야 합니다. 구성은 명령줄 인터페이스를 사용하여 수행됩니다. 이 방법은 연결이 끊긴 환경에 이상적입니다.
- **자동화:** 설치 관리자 프로비저닝 인프라에 클러스터를 배포할 수 있습니다. 설치 프로그램은 프로비저닝에 각 클러스터 호스트의 BMC(Baseboard Management Controller)를 사용합니다. 연결되거나 연결이 끊긴 환경에서 클러스터를 배포할 수 있습니다.
- **전체 제어:** 준비 및 유지 관리하는 인프라에 클러스터를 배포하여 최대 사용자 지정 가능성을 제공할 수 있습니다. 연결되거나 연결이 끊긴 환경에서 클러스터를 배포할 수 있습니다.

각 방법은 다음과 같은 특성을 가진 클러스터를 배포합니다.

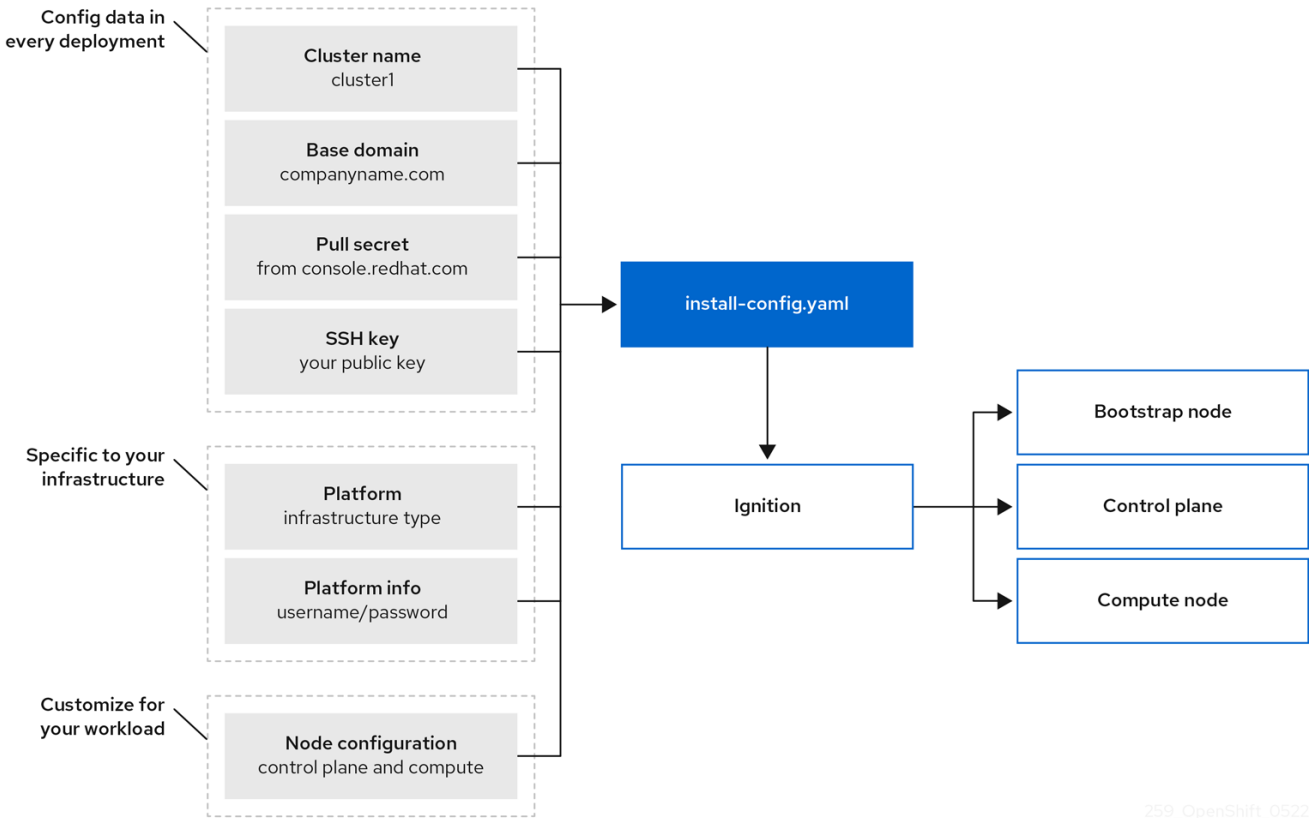
- 기본적으로 사용 가능한 단일 장애 지점이 없는고가용성 인프라입니다.
- 관리자는 적용되는 업데이트 및 시기를 제어할 수 있습니다.

1.1.1. 설치 프로그램 정보

설치 프로그램을 사용하여 각 유형의 클러스터를 배포할 수 있습니다. 설치 프로그램은 부트스트랩, 컨트롤 플레인 및 컴퓨팅 머신의 Ignition 구성 파일과 같은 주요 자산을 생성합니다. 인프라를 올바르게 구성한 경우 세 가지 머신 구성으로 OpenShift Container Platform 클러스터를 시작할 수 있습니다.

OpenShift Container Platform 설치 프로그램은 일련의 대상 및 종속 항목을 사용하여 클러스터 설치를 관리합니다. 설치 프로그램에는 달성해야 할 대상 세트가 있으며 각 대상에는 종속 항목 세트가 있습니다. 각 대상은 자체 종속 항목에만 관련되므로 설치 프로그램은 최종 대상과 동시에 여러 대상을 실행 중인 클러스터가 되도록 할 수 있습니다. 설치 프로그램은 종속성을 충족하기 때문에 명령을 실행하여 다시 생성하는 대신 기존 구성 요소를 인식하고 사용합니다.

그림 1.1. OpenShift Container Platform 설치 대상 및 종속 항목



259_OpenShift_0522

1.1.2. RHCOS(Red Hat Enterprise Linux CoreOS) 정보

설치 후 각 클러스터 시스템은 운영 체제로 RHCOS (Red Hat Enterprise Linux CoreOS)를 사용합니다. RHCOS는 RHEL(Red Hat Enterprise Linux)의 변경 불가능한 컨테이너 호스트 버전이며 기본적으로 SELinux가 활성화된 RHEL 커널을 제공합니다. RHCOS에는 Kubernetes 노드 에이전트인 **kubelet** 과 Kubernetes에 최적화된 CRI-O 컨테이너 런타임이 포함됩니다.

OpenShift Container Platform 4.17 클러스터의 모든 컨트롤 플레인 시스템은 Ignition이라는 중요한 최초 부팅 프로비저닝 도구를 포함하는 RHCOS를 사용해야 합니다. 이 도구를 사용하면 클러스터가 머신을 구성할 수 있습니다. 운영 체제 업데이트는 **OSTree** 를 백엔드로 사용하여 Machine Config Operator에 의해 클러스터 전체에 배포되는 부팅 가능한 컨테이너 이미지로 제공됩니다. 실제 운영 체제 변경은 **rpm-ostree** 를 사용하여 각 머신에서 원자 작업으로 수행됩니다. 이러한 기술을 함께 사용하면 OpenShift Container Platform에서 전체 플랫폼을 최신 상태로 유지하는 인플레이스 업그레이드를 통해 클러스터의 다른 애플리케이션을 관리하는 것처럼 운영 체제를 관리할 수 있습니다. 이러한 내부 업데이트는 운영 팀의 부담을 줄일 수 있습니다.

모든 클러스터 머신의 운영 체제로 RHCOS를 사용하는 경우 클러스터가 운영 체제를 포함한 구성 요소 및 머신의 모든 측면을 관리합니다. 그러면 설치 프로그램 및 Machine Config Operator만 머신을 변경할 수 있습니다. 설치 프로그램에서는 Ignition 구성 파일을 사용하여 각 머신의 정확한 상태를 설정하고 Machine Config Operator는 설치 후 새 인증서 또는 키 적용과 같은 머신에 대한 추가 변경을 완료합니다.

1.1.3. OpenShift Container Platform 설치를 위한 일반 용어집

용어집은 설치 콘텐츠와 관련된 일반적인 용어를 정의합니다. 설치 프로세스를 더 잘 이해하기 위해 다음 용어 목록을 읽으십시오.

지원되는 설치 관리자

클러스터 구성을 생성하기 위한 웹 기반 사용자 인터페이스 또는 RESTful API를 제공하는

console.redhat.com에서 호스팅되는 설치 관리자입니다. 지원 설치 관리자는 검색 이미지를 생성합니다. 클러스터 머신은 검색 이미지로 부팅되며 RHCOS와 에이전트를 설치합니다. 지원 설치 관리자 및 에이전트는 함께 클러스터에 사전 설치 검증 및 설치를 제공합니다.

에이전트 기반 설치 관리자

지원 설치 관리자와 유사한 설치 관리자이지만 먼저 에이전트 기반 설치 관리자를 다운로드해야 합니다. 에이전트 기반 설치 프로그램은 연결이 끊긴 환경에 이상적입니다.

부트스트랩 노드

OpenShift Container Platform 컨트롤 플레인을 배포하는 데 필요한 최소 Kubernetes 구성을 실행하는 임시 머신입니다.

컨트롤 플레인

컨테이너의 라이프사이클을 정의, 배포, 관리하는 API 및 인터페이스를 노출하는 컨테이너 오케스트레이션 계층입니다. 컨트롤 플레인 시스템이라고도 합니다.

컴퓨팅 노드

클러스터 사용자에게 대한 워크로드를 실행하는 노드입니다. 작업자 노드라고도 합니다.

연결이 해제된 설치

데이터 센터의 일부는 프록시 서버를 통해서도 인터넷에 액세스하지 못할 수 있습니다. 이러한 환경에 OpenShift Container Platform을 계속 설치할 수 있지만 필요한 소프트웨어 및 이미지를 다운로드하여 연결이 끊긴 환경에서 사용할 수 있도록 해야 합니다.

OpenShift Container Platform 설치 프로그램

인프라를 프로비저닝하고 클러스터를 배포하는 프로그램입니다.

설치 관리자 프로비저닝 인프라

설치 프로그램은 클러스터가 실행되는 인프라를 배포하고 구성합니다.

Ignition 구성 파일

Ignition 도구가 운영 체제 초기화 중에 RHCOS(Red Hat Enterprise Linux CoreOS)를 구성하는 데 사용하는 파일입니다. 설치 프로그램은 부트스트랩, 컨트롤 플레인 및 작업자 노드를 초기화하기 위해 다른 Ignition 구성 파일을 생성합니다.

Kubernetes 매니페스트

JSON 또는 YAML 형식의 Kubernetes API 오브젝트의 사양입니다. 구성 파일에는 배포, 구성 맵, 시크릿, 데몬 세트 등이 포함될 수 있습니다.

kubelet

Pod에서 컨테이너가 실행 중인지 확인하기 위해 클러스터의 각 노드에서 실행되는 기본 노드 에이전트입니다.

로드 밸런서

로드 밸런서는 클라이언트의 단일 연락처 지점 역할을 합니다. API를 위한 로드 밸런서는 들어오는 트래픽을 컨트롤 플레인 노드에 배포합니다.

Machine Config Operator

클러스터의 노드에 커널과 kubelet 사이의 모든 항목을 포함하여 기본 운영 체제 및 컨테이너 런타임의 구성 및 업데이트를 관리하고 적용하는 Operator입니다.

Operator

OpenShift Container Platform 클러스터에서 Kubernetes 애플리케이션을 패키징, 배포 및 관리하는 기본 방법입니다. Operator는 사람의 운영 지식을 사용하여 쉽게 패키지와 고객과 공유할 수 있는 소프트웨어로 인코딩합니다.

사용자 프로비저닝 인프라

사용자가 제공하는 인프라에 OpenShift Container Platform을 설치할 수 있습니다. 설치 프로그램을 사용하여 클러스터 인프라를 프로비저닝하고 클러스터 인프라를 생성한 다음 제공한 인프라에 클러스터를 배포하는 데 필요한 자산을 생성할 수 있습니다.

1.1.4. 설치 프로세스

지원 설치 관리자를 제외하고 OpenShift Container Platform 클러스터를 설치할 때 OpenShift **Cluster Manager Hybrid Cloud Console**의 **적절한 클러스터 유형** 페이지에서 설치 프로그램을 다운로드해야 합니다. 이 콘솔은 다음을 관리합니다.

- 계정용 REST API.
- 필수 구성 요소를 가져오는 데 사용하는 풀 시크릿인 레지스트리 토큰입니다.
- 사용 지표 수집이 용이하도록 클러스터 ID를 Red Hat 계정에 연결하는 클러스터 등록.

OpenShift Container Platform 4.17에서 설치 프로그램은 자산 세트에서 일련의 파일 변환을 수행하는 Go 바이너리 파일입니다. 설치 프로그램과 상호 작용하는 방법은 설치 유형에 따라 다릅니다. 다음 설치 사용 사례를 고려하십시오.

- 지원 설치 관리자를 사용하여 클러스터를 배포하려면 **지원 설치 관리자**를 사용하여 클러스터 설정을 구성해야 합니다. 다운로드 및 구성할 설치 프로그램이 없습니다. 클러스터 구성 설정을 완료한 후 검색 ISO를 다운로드한 다음 해당 이미지를 사용하여 클러스터 시스템을 부팅합니다. Nutanix, vSphere 및 베어 메탈에 지원 설치 관리자를 사용하여 클러스터를 완전히 통합 및 기타 플랫폼에 설치할 수 있습니다. 베어 메탈에 설치하는 경우 네트워킹, 로드 밸런싱, 스토리지 및 개별 클러스터 머신을 포함한 모든 클러스터 인프라 및 리소스를 제공해야 합니다.
- 에이전트 기반 설치 관리자를 사용하여 클러스터를 배포하려면 먼저 **에이전트 기반 설치 관리자**를 다운로드할 수 있습니다. 그런 다음 클러스터를 구성하고 검색 이미지를 생성할 수 있습니다. 검색 이미지를 사용하여 클러스터 시스템을 부팅합니다. 이 에이전트는 설치 프로그램과 상호 작용하거나 프로비저너 시스템을 직접 설정하는 대신 설치 프로그램과 통신하는 에이전트를 처리합니다. 네트워킹, 로드 밸런싱, 스토리지 및 개별 클러스터 시스템을 포함하여 모든 클러스터 인프라 및 리소스를 제공해야 합니다. 이 방법은 연결이 끊긴 환경에 이상적입니다.
- 설치 관리자 프로비저닝 인프라가 있는 클러스터의 경우 인프라 부트스트랩 및 프로비저닝을 직접 수행하는 대신 설치 프로그램에 위임합니다. 설치 프로그램은 베어 메탈에 설치하는 경우를 제외하고 클러스터를 지원하는 데 필요한 모든 네트워킹, 머신 및 운영 체제를 생성합니다. 베어 메탈에 설치하는 경우 부트스트랩 머신, 네트워킹, 로드 밸런싱, 스토리지 및 개별 클러스터 머신을 포함한 모든 클러스터 인프라 및 리소스를 제공해야 합니다.
- 클러스터의 인프라를 프로비저닝하고 관리하는 경우 부트스트랩 머신, 네트워킹, 부하 분산, 스토리지 및 개별 클러스터 머신을 포함한 모든 클러스터 인프라 및 리소스를 제공해야 합니다.

설치 프로그램의 경우 프로그램은 설치 중에 **install-config.yaml**, Kubernetes 매니페스트 및 머신 유형에 대한 Ignition 구성 파일의 세 가지 파일 세트를 사용합니다.



중요

설치 중에 기본 RHCOS 운영 체제를 제어하는 Kubernetes 및 Ignition 구성 파일을 수정할 수 있습니다. 그러나 이러한 오브젝트를 수정한 내용이 적합한지 확인할 수 있는 유효성 검사는 없습니다. 이러한 오브젝트를 수정하면 클러스터가 작동하지 않을 수 있습니다. 이 위험 때문에 문서화된 절차를 따르거나 Red Hat 지원 부서에서 지시하지 않는 한 Kubernetes 및 Ignition 구성 파일 수정은 지원되지 않습니다.

설치 구성 파일은 Kubernetes 매니페스트로 변환된 다음 매니페스트가 Ignition 구성 파일로 래핑됩니다. 설치 프로그램은 이러한 Ignition 구성 파일을 사용하여 클러스터를 생성합니다.

설치 프로그램을 실행할 때 설치 구성 파일이 모두 정리되므로 다시 사용하려는 모든 구성 파일을 백업하십시오.



중요

설치 중에 설정한 매개변수는 수정할 수 없지만 설치 후에는 많은 클러스터 속성을 수정할 수 있습니다.

1.1.4.1. 지원 설치 관리자를 사용한 설치 프로세스

지원 설치 관리자를 사용하여 설치하려면 웹 기반 사용자 인터페이스 또는 RESTful API를 사용하여 대화식으로 클러스터 구성을 생성해야 합니다. 지원 설치 관리자 사용자 인터페이스에서 필요한 값을 입력하라는 메시지를 표시하고 사용자 인터페이스 또는 API에서 변경하지 않는 한 나머지 매개변수에 대한 적절한 기본값을 제공합니다. 지원 설치 프로그램은 다운로드하여 클러스터 시스템을 부팅하는 데 사용하는 검색 이미지를 생성합니다. 이 이미지는 RHCOS 및 에이전트를 설치하고 에이전트가 프로비저닝을 처리합니다. 지원 설치 관리자를 사용하여 OpenShift Container Platform을 설치하고 Nutanix, vSphere 및 베어 메탈에서 전체 통합을 설치할 수 있습니다. 또한 통합 없이 다른 플랫폼에 지원 설치 프로그램을 사용하여 OpenShift Container Platform을 설치할 수 있습니다.

OpenShift Container Platform은 운영 체제 자체를 포함하여 클러스터의 모든 측면을 관리합니다. 각 머신은 결합하는 클러스터에서 호스팅되는 리소스를 참조하는 구성으로 부팅됩니다. 이 구성을 사용하면 업데이트가 적용될 때 클러스터가 자체적으로 관리될 수 있습니다.

가능한 경우 지원 설치 관리자 기능을 사용하여 에이전트 기반 설치 관리자를 다운로드하고 구성할 필요가 없습니다.

1.1.4.2. 에이전트 기반 인프라를 사용하는 설치 프로세스

에이전트 기반 설치에는 **에이전트 기반 설치 관리자**를 다운로드하여 설치해야 한다는 점을 제외하고 지원 설치 관리자를 사용하는 것과 유사합니다. 에이전트 기반 설치에는 지원 설치 프로그램의 편의를 원하지만 연결이 끊긴 환경에 클러스터를 설치해야 하는 경우 유용합니다.

가능한 경우 에이전트 기반 설치 기능을 사용하여 부트스트랩 VM으로 프로비저너 시스템을 생성한 다음 클러스터 인프라를 프로비저닝 및 유지 관리할 필요가 없습니다.

1.1.4.3. 설치 관리자가 프로비저닝한 인프라를 사용하는 설치 프로세스

기본 설치 유형에서는 설치 관리자 프로비저닝 인프라를 사용합니다. 기본적으로 설치 프로그램은 설치 마법사 역할을 하여 자체적으로 결정할 수 없는 값을 입력하라는 메시지를 표시하고 나머지 매개변수에 대한 적절한 기본값을 제공합니다. 고급 인프라 시나리오를 지원하도록 설치 프로세스를 사용자 정의할 수도 있습니다. 설치 프로그램은 클러스터의 기본 인프라를 프로비저닝합니다.

표준 클러스터 또는 사용자 정의된 클러스터를 설치할 수 있습니다. 표준 클러스터에서는 클러스터를 설치하는 데 필요한 최소 세부 정보를 제공합니다. 사용자 지정 클러스터를 사용하면 컨트롤 플레인에서 사용하는 머신 수, 클러스터가 배포하는 가상 머신 유형 또는 Kubernetes 서비스 네트워크의 CIDR 범위와 같은 플랫폼에 대한 세부 정보를 지정할 수 있습니다.

가능하면 이 기능을 사용하여 클러스터 인프라를 프로비저닝 및 유지보수하지 않아도 됩니다. 다른 모든 환경에서는 설치 프로그램을 사용하여 클러스터 인프라를 프로비저닝하는 데 필요한 자산을 생성합니다.

OpenShift Container Platform은 설치 프로그램에서 프로비저닝한 인프라 클러스터를 통해 운영 체제 자체를 포함하여 클러스터의 모든 측면을 관리합니다. 각 머신은 결합하는 클러스터에서 호스팅되는 리소스를 참조하는 구성으로 부팅됩니다. 이 구성을 사용하면 업데이트가 적용될 때 클러스터가 자체적으로 관리될 수 있습니다.

1.1.4.4. 사용자 프로비저닝 인프라를 사용하는 설치 프로세스

제공하는 인프라에 OpenShift Container Platform도 설치할 수 있습니다. 설치 프로그램을 사용하여 클러스터 인프라를 프로비저닝하고 클러스터 인프라를 생성한 다음 제공한 인프라에 클러스터를 배포하는 데 필요한 자산을 생성합니다.

설치 프로그램이 프로비저닝한 인프라를 사용하지 않는 경우 클러스터 리소스를 직접 관리하고 유지보수해야 합니다. 다음 목록에서는 이러한 자체 관리 리소스 중 일부를 자세히 설명합니다.

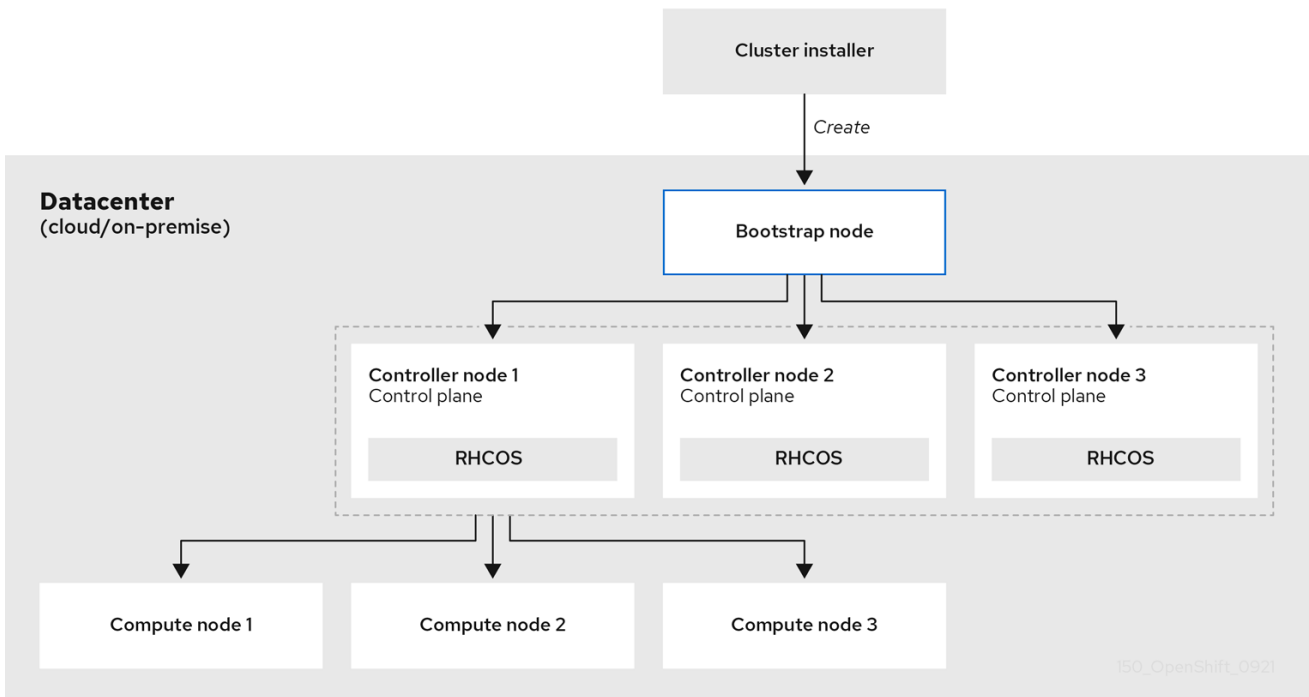
- 클러스터를 구성하는 컨트롤 플레인 및 컴퓨팅 머신의 기본 인프라
- 로드 밸런서
- DNS 레코드 및 필수 서브넷을 포함한 클러스터 네트워킹
- 클러스터 인프라 및 애플리케이션용 스토리지

클러스터가 사용자 프로비저닝 인프라를 사용하는 경우 RHEL 컴퓨팅 머신을 클러스터에 추가할 수 있습니다.

1.1.4.5. 설치 프로세스 세부사항

클러스터가 프로비저닝되면 클러스터의 각 시스템에 클러스터에 대한 정보가 필요합니다. OpenShift Container Platform은 초기 구성 중에 임시 부트스트랩 머신을 사용하여 필요한 정보를 영구 컨트롤 플레인에 제공합니다. 임시 부트스트랩 머신은 클러스터 생성 방법을 설명하는 Ignition 구성 파일을 사용하여 부팅됩니다. 부트스트랩 시스템은 컨트롤 플레인을 구성하는 컨트롤 플레인 시스템을 생성합니다. 그런 다음 컨트롤 플레인 시스템에서는 작업자 머신이라고도 하는 컴퓨팅 머신을 만듭니다. 다음 그림은 이 프로세스를 보여줍니다.

그림 1.2. 부트스트랩, 컨트롤 플레인 및 컴퓨팅 시스템 생성





중요

클러스터를 배포하려는 동안 성능 및 확장성에 대한 권장 사례, 특히 etcd 스토리지에 대한 입력/출력 대기 시간 요구 사항 및 권장 컨트롤 플레인 노드 크기 조정에 대한 요구 사항을 숙지해야 합니다. 자세한 내용은 "Recommended etcd practices" 및 "Control Plane 노드 크기 조정"을 참조하십시오.

클러스터 머신이 초기화되면 부트스트랩 머신이 손상됩니다. 모든 클러스터에서는 부트스트랩 프로세스를 사용하여 클러스터를 초기화하지만, 클러스터의 인프라를 프로비저닝하는 경우 많은 단계를 수동으로 완료해야 합니다.



중요

- 설치 프로그램에서 생성하는 Ignition 구성 파일에 24시간 후에 만료되는 인증서가 포함되어 있습니다. 이 인증서는 그 후에 갱신됩니다. 인증서를 갱신하기 전에 클러스터가 종료되고 24시간이 지난 후에 클러스터가 다시 시작되면 클러스터는 만료된 인증서를 자동으로 복구합니다. 예외적으로 kubelet 인증서를 복구하려면 대기 중인 **node-bootstrapper** 인증서 서명 요청(CSR)을 수동으로 승인해야 합니다. 자세한 내용은 *만료된 컨트롤 플레인 인증서에서 복구* 문서를 참조하십시오.
- 24시간 인증서는 클러스터를 설치한 후 16시간에서 22시간 사이에 회전하므로 생성된 후 12시간 이내에 Ignition 구성 파일을 사용하는 것이 좋습니다. 12시간 이내에 Ignition 구성 파일을 사용하면 설치 중에 인증서 업데이트가 실행되는 경우 설치 실패를 방지할 수 있습니다.

클러스터 부트스트랩에는 다음 단계가 포함됩니다.

1. 부트스트랩 머신이 부팅되고 컨트롤 플레인 머신을 부팅하는 데 필요한 원격 리소스 호스팅이 시작됩니다. 인프라를 프로비저닝하는 경우 이 단계에는 수동 개입이 필요합니다.
2. 부트스트랩 머신은 단일 노드 etcd 클러스터와 임시 Kubernetes 컨트롤 플레인을 시작합니다.
3. 컨트롤 플레인 머신은 부트스트랩 머신에서 원격 리소스를 가져오고 부팅을 완료합니다. 인프라를 프로비저닝하는 경우 이 단계에는 수동 개입이 필요합니다.
4. 임시 컨트롤 플레인은 프로덕션 컨트롤러 플레인을 프로덕션 컨트롤 플레인 머신에 예약합니다.
5. CVO(Cluster Version Operator)가 온라인 상태가 되어 etcd Operator를 설치합니다. etcd Operator는 모든 컨트롤 플레인 노드에서 etcd를 확장합니다.
6. 임시 컨트롤 플레인이 종료되고 제어를 프로덕션 컨트롤 플레인에 전달합니다.
7. 부트스트랩 머신은 OpenShift Container Platform 구성 요소를 프로덕션 컨트롤 플레인에 주입합니다.
8. 설치 프로그램이 부트 스트랩 머신을 종료합니다. 인프라를 프로비저닝하는 경우 이 단계에는 수동 개입이 필요합니다.
9. 컨트롤 플레인이 컴퓨팅 노드를 설정합니다.
10. 컨트롤 플레인은 일련의 Operator 형태로 추가 서비스를 설치합니다.

이 부트스트랩 프로세스의 결과는 실행 중인 OpenShift Container Platform 클러스터입니다. 그런 다음 클러스터는 지원되는 환경에서 컴퓨팅 머신 생성을 포함하여 일상적인 작업에 필요한 나머지 구성 요소를 다운로드하고 구성합니다.

추가 리소스

- [etcd 관련 권장 사례](#)
- [컨트롤 플레인 노드 크기 조정](#)
- [Red Hat OpenShift Network 계산기](#)

1.1.5. 설치 후 노드 상태 확인

다음 설치 상태 점검이 성공하면 OpenShift Container Platform 설치가 완료됩니다.

- 프로비저너는 OpenShift Container Platform 웹 콘솔에 액세스할 수 있습니다.
- 모든 컨트롤 플레인 노드가 준비되었습니다.
- 모든 클러스터 Operator를 사용할 수 있습니다.



참고

설치가 완료되면 작업자 노드를 담당하는 특정 클러스터 Operator가 모든 작업자 노드를 지속적으로 프로비저닝하려고 합니다. 모든 작업자 노드가 **READY** 로 보고되기 전에 시간이 필요합니다. 베어 메탈에 설치하는 경우 작업자 노드의 문제를 해결하기 전에 최소 60분 정도 기다립니다. 다른 모든 플랫폼에 설치하려면 작업자 노드의 문제를 해결하기 전에 최소 40 분 정도 기다립니다. 작업자 노드를 담당하는 클러스터 Operator의 **DEGRADED** 상태는 노드의 상태가 아닌 Operator의 자체 리소스에 따라 다릅니다.

설치가 완료되면 클러스터의 노드 상태를 계속 모니터링할 수 있습니다.

사전 요구 사항

- 터미널에서 설치 프로그램이 성공적으로 해결됩니다.

프로세스

1. 모든 작업자 노드의 상태를 표시합니다.

```
$ oc get nodes
```

출력 예

NAME	STATUS	ROLES	AGE	VERSION
example-compute1.example.com	Ready	worker	13m	v1.21.6+bb8d50a
example-compute2.example.com	Ready	worker	13m	v1.21.6+bb8d50a
example-compute4.example.com	Ready	worker	14m	v1.21.6+bb8d50a
example-control1.example.com	Ready	master	52m	v1.21.6+bb8d50a
example-control2.example.com	Ready	master	55m	v1.21.6+bb8d50a
example-control3.example.com	Ready	master	55m	v1.21.6+bb8d50a

2. 모든 작업자 머신 노드의 단계를 표시합니다.

```
$ oc get machines -A
```

출력 예

NAMESPACE	NAME	PHASE	TYPE	REGION	ZONE	AGE
openshift-machine-api	example-zbbt6-master-0	Running				95m
openshift-machine-api	example-zbbt6-master-1	Running				95m
openshift-machine-api	example-zbbt6-master-2	Running				95m
openshift-machine-api	example-zbbt6-worker-0-25bhp	Running				49m
openshift-machine-api	example-zbbt6-worker-0-8b4c2	Running				49m
openshift-machine-api	example-zbbt6-worker-0-jkbqt	Running				49m
openshift-machine-api	example-zbbt6-worker-0-qr15b	Running				49m

추가 리소스

- [BareMetalHost 리소스 가져오기](#)
- [설치 진행 상황](#)
- [설치 검증](#)
- [에이전트 기반 설치 관리자](#)
- [OpenShift Container Platform 용 지원되는 설치 관리자](#)

1.1.6. 설치 범위

OpenShift Container Platform 설치 프로그램의 범위는 의도적으로 한정됩니다. 단순성과 성공을 보장하도록 설계되었습니다. 설치가 완료된 후 많은 추가 구성 작업을 완료할 수 있습니다.

추가 리소스

- [OpenShift Container Platform 구성 리소스에 대한 자세한 내용은 사용 가능한 클러스터 사용자 정의를 참조하십시오.](#)

1.1.7. OpenShift 로컬 개요

OpenShift Local은 OpenShift Container Platform 클러스터 빌드를 시작할 수 있도록 빠른 애플리케이션 개발을 지원합니다. OpenShift Local은 로컬 컴퓨터에서 실행되어 설정 및 테스트를 단순화하고 컨테이너 기반 애플리케이션을 개발하는 데 필요한 모든 툴을 사용하여 클라우드 개발 환경을 로컬로 에뮬레이션하도록 설계되었습니다.

사용하는 프로그래밍 언어와 관계없이 OpenShift Local은 애플리케이션을 호스팅하고 서버 기반 인프라 없이도 로컬 PC에 사전 구성된 최소 Red Hat OpenShift Container Platform 클러스터를 제공합니다.

호스팅된 환경에서 OpenShift Local은 Linux, macOS 또는 Windows 10 이상을 실행하는 랩탑 또는 데스크탑에서 직접 마이크로서비스를 생성하고 이미지로 변환한 컨테이너에서 직접 실행할 수 있습니다.

OpenShift Local에 대한 자세한 내용은 [Red Hat OpenShift 로컬 개요](#) 를 참조하십시오.

1.2. OPENSIFT CONTAINER PLATFORM 클러스터에서 지원되는 플랫폼

OpenShift Container Platform 4.17에서는 다음 플랫폼에서 설치 관리자 프로비저닝 인프라를 사용하는 클러스터를 설치할 수 있습니다.

- [AWS\(Amazon Web Services\)](#)

- 베어 메탈
- GCP(Google Cloud Platform)
- IBM Cloud®
- Microsoft Azure
- Microsoft Azure Stack Hub
- Nutanix
- Red Hat OpenStack Platform (RHOSP)
 - 최신 OpenShift Container Platform 릴리스는 최신 RHOSP 긴 수명 릴리스 및 중간 릴리스를 모두 지원합니다. 완전한 RHOSP 릴리스 호환성에 대해서는 [RHOSP의 OpenShift Container Platform on RHOSP 지원 매트릭스](#)를 참조하십시오.
- VMware vSphere

이러한 클러스터의 경우, 설치 프로세스를 실행하는 컴퓨터를 포함한 모든 머신은 플랫폼 컨테이너의 이미지를 가져오고 원격 분석 데이터를 Red Hat에 제공하기 위해 인터넷에 직접 액세스할 수 있어야 합니다.



중요

설치 후 다음 변경 사항은 지원되지 않습니다.

- 클라우드 공급자 플랫폼 혼합.
- 클라우드 공급자 구성 요소 혼합. 예를 들어 클러스터를 설치한 플랫폼의 다른 플랫폼의 영구 스토리지 프레임워크를 사용합니다.

OpenShift Container Platform 4.17에서는 다음 플랫폼에서 사용자 프로비저닝 인프라를 사용하는 클러스터를 설치할 수 있습니다.

- AWS
- Azure
- Azure Stack Hub
- 베어 메탈
- GCP
- IBM Power®
- IBM Z® 또는 IBM® LinuxONE
- RHOSP
 - 최신 OpenShift Container Platform 릴리스는 최신 RHOSP 긴 수명 릴리스 및 중간 릴리스를 모두 지원합니다. 완전한 RHOSP 릴리스 호환성에 대해서는 [RHOSP의 OpenShift Container Platform on RHOSP 지원 매트릭스](#)를 참조하십시오.
- AWS의 VMware Cloud

- VMware vSphere

플랫폼의 지원되는 사례에 따라 사용자 프로비저닝 인프라에서 설치를 수행하여 완전한 인터넷 액세스 권한이 있는 머신을 실행하거나 클러스터를 프록시 뒤에 배치하거나, 연결이 끊긴 설치를 수행할 수 있습니다.

연결이 끊긴 설치에서는 클러스터를 설치하는 데 필요한 이미지를 다운로드하여 미리 레지스트리에 배치한 다음 해당 데이터를 사용하여 클러스터를 설치할 수 있습니다. vSphere 또는 베어 메탈 인프라에 연결이 끊긴 설치와 함께 플랫폼 컨테이너의 이미지를 가져오려면 인터넷 액세스가 필요하지만 클러스터 시스템에는 직접 인터넷 액세스가 필요하지 않습니다.

다른 플랫폼의 통합 테스트에 대한 자세한 내용은 [OpenShift Container Platform 4.x 통합 테스트](#) 페이지를 참조하십시오.

추가 리소스

- 지원되는 각 플랫폼에서 사용할 수 있는 설치 유형에 대한 자세한 내용은 [다른 플랫폼의 지원 설치 방법](#)을 참조하십시오.
- [설치 방법 선택 및 필요한 리소스 준비에 대한 정보는 클러스터 설치 방법 선택 및 사용자](#)를 위한 준비를 참조하십시오.
- [Red Hat OpenShift Network 계산기](#)를 사용하면 배포 및 확장 단계에서 클러스터 네트워크를 설계할 수 있습니다. 클러스터 네트워크와 관련된 일반적인 질문을 해결하고 편리한 JSON 형식으로 출력을 제공합니다.

2장. 클러스터 설치 방법 선택 및 사용자를 위한 준비

OpenShift Container Platform을 설치하기 전에 실행할 설치 프로세스를 결정하고 사용자를 위해 클러스터를 준비하는 데 필요한 모든 리소스가 있는지 확인합니다.

2.1. 클러스터 설치 유형 선택

OpenShift Container Platform 클러스터를 설치하기 전에 실행할 최상의 설치 지침을 선택해야 합니다. 최상의 옵션을 선택하기 위해 다음 질문에 대한 답변을 고려하십시오.

2.1.1. OpenShift Container Platform 클러스터를 직접 설치 및 관리하시겠습니까?

OpenShift Container Platform을 직접 설치하고 관리하려면 다음 플랫폼에 설치할 수 있습니다.

- 64비트 x86 인스턴스의 AWS(Amazon Web Services)
- 64비트 ARM 인스턴스의 AWS(Amazon Web Services)
- 64비트 x86 인스턴스의 Microsoft Azure
- 64비트 ARM 인스턴스의 Microsoft Azure
- Microsoft Azure Stack Hub
- 64비트 x86 인스턴스의 Google Cloud
- 64비트 ARM 인스턴스의 Google Cloud
- Red Hat OpenStack Platform (RHOSP)
- IBM Cloud®
- IBM Z® 또는 IBM® LinuxONE with z/VM
- IBM Z® 또는 IBM® LinuxONE with Red Hat Enterprise Linux (RHEL) KVM
- LPAR의 IBM Z® 또는 IBM® LinuxONE
- IBM Power®
- IBM Power® Virtual Server
- Nutanix
- VMware vSphere
- 베어 메탈 또는 기타 플랫폼과 무관한 인프라

온프레미스 하드웨어 및 클라우드 호스팅 서비스에 모두 OpenShift Container Platform 4 클러스터를 배포할 수 있지만 클러스터의 모든 시스템은 동일한 데이터 센터 또는 클라우드 호스팅 서비스에 있어야 합니다.

OpenShift Container Platform을 사용하지만 클러스터를 직접 관리하지 않으려면 여러 관리 서비스 옵션 중에서 선택할 수 있습니다. Red Hat에서 완전히 관리하는 클러스터를 원하는 경우 [OpenShift Dedicated](#)를 사용할 수 있습니다. Azure, AWS, IBM Cloud® 또는 Google Cloud에서 OpenShift를 관리형 서비스로

사용할 수도 있습니다. 관리 서비스에 대한 자세한 내용은 [OpenShift 제품](#) 페이지를 참조하십시오. 클라우드 가상 머신을 가상 베어 메탈로 사용하여 OpenShift Container Platform 클러스터를 설치하는 경우 해당 클라우드 기반 스토리지가 지원되지 않습니다.

2.1.2. OpenShift Container Platform 3을 사용한 적이 있으며 OpenShift Container Platform 4를 사용하고 싶으신가요?

OpenShift Container Platform 3을 사용했으며 OpenShift Container Platform 4를 시도하려면 OpenShift Container Platform 4가 어떻게 다른지 이해해야 합니다. OpenShift Container Platform 4는 Kubernetes 애플리케이션과 플랫폼이 실행되는 운영 체제인 RHCOS(Red Hat Enterprise Linux CoreOS)를 함께 원활하게 패키지, 배포, 관리하는 Operator를 만듭니다. OpenShift Container Platform을 설치하기 위해 머신을 배포하고 운영 체제를 구성하는 대신 RHCOS 운영 체제는 OpenShift Container Platform 클러스터의 통합된 부분입니다. 클러스터 머신의 운영 체제를 배포하는 것은 OpenShift Container Platform의 설치 프로세스의 일부입니다. [OpenShift Container Platform 3과 4의 차이점](#) 을 참조하십시오.

OpenShift Container Platform 클러스터 설치 프로세스의 일부로 머신을 프로비저닝해야 하므로 OpenShift Container Platform 3 클러스터를 OpenShift Container Platform 4로 업그레이드할 수 없습니다. 대신 새로운 OpenShift Container Platform 4 클러스터를 생성하고 OpenShift Container Platform 3 워크로드를 마이그레이션해야 합니다. 마이그레이션에 대한 자세한 내용은 [OpenShift Container Platform 3에서 4로 마이그레이션을 참조하십시오](#). OpenShift Container Platform 4로 마이그레이션해야 하므로 모든 유형의 프로덕션 클러스터 설치 프로세스를 사용하여 새 클러스터를 생성할 수 있습니다.

2.1.3. 클러스터에서 기존 구성 요소를 사용하시겠습니까?

운영 체제는 OpenShift Container Platform에 통합되므로 OpenShift Container Platform용 설치 프로그램이 모든 인프라를 가동하도록 하는 것이 더 쉬워집니다. 이는 *설치 관리자가 프로비저닝한 인프라* 설치라고 합니다. 이 유형의 설치에서는 클러스터에 일부 기존 인프라를 제공할 수 있지만, 설치 프로그램은 클러스터가 처음에 필요한 모든 머신을 배포합니다.

[AWS](#), [Azure](#), [Azure Stack Hub](#), [Google Cloud](#), [Nutanix](#).에 대한 클러스터 또는 해당 기본 머신에 사용자 지정을 지정하지 않고 설치 관리자가 프로비저닝한 인프라 클러스터를 배포할 수 있습니다.

클러스터 머신의 인스턴스 유형과 같이 설치 관리자가 프로비저닝한 인프라 클러스터에 대한 기본 구성을 수행해야 하는 경우 [AWS](#), [Azure](#), [Google Cloud](#), [Nutanix](#) 에 대한 설치를 사용자 지정할 수 있습니다.

설치 관리자가 프로비저닝한 인프라 설치의 경우 [AWS의 기존 VPC](#), [Azure의 vNet](#) 또는 [Google Cloud의 VPC](#) 를 사용할 수 있습니다. [AWS](#), [Azure](#), [Google Cloud](#) 의 클러스터가 환경의 기존 IP 주소 할당과 공존하고 기존 MTU 및 VXLAN 구성과 통합할 수 있도록 네트워킹 인프라의 부분을 재사용할 수도 있습니다. 이러한 클라우드에 기존 계정과 인증 정보가 있는 경우 다시 사용할 수 있지만 계정을 수정하여 OpenShift Container Platform 클러스터를 설치하는 데 필요한 권한이 있어야 할 수 있습니다.

설치 관리자 프로비저닝 인프라 방법을 사용하여 하드웨어에 [vSphere](#) 및 [베어 메탈](#)에 적절한 머신 인스턴스를 생성할 수 있습니다. 또한 [vSphere](#) 의 경우 설치 중에 추가 네트워크 매개변수를 사용자 지정할 수도 있습니다.

일부 설치 관리자 프로비저닝 인프라 설치(예: VMware vSphere 및 베어 메탈 플랫폼)의 경우 수신 가상 IP(VIP)에 도달하는 외부 트래픽은 기본 [IngressController](#) 복제본 간에 분산되지 않습니다. 기본 [IngressController](#) 라우터 성능을 초과하는 vSphere 및 베어 메탈 설치 관리자 프로비저닝 인프라 설치의 경우 외부 로드 밸런서를 구성해야 합니다. 외부 로드 밸런서를 구성하면 여러 [IngressController](#) 복제본의 성능이 향상됩니다. 기본 [IngressController](#) 성능에 대한 자세한 내용은 [Baseline Ingress Controller \(router\) 성능](#)을 참조하십시오. 외부 로드 밸런서 구성에 대한 자세한 내용은 [사용자 관리 로드 밸런서 구성](#)을 참조하십시오.

광범위한 클라우드 인프라를 재사용하려면 *사용자가 프로비저닝한 인프라* 설치를 완료할 수 있습니다. 이러한 설치를 통해 설치 프로세스 중에 클러스터에 필요한 머신을 수동으로 배포합니다. [AWS](#), [Azure](#)

,[Azure Stack Hub](#) 에서 사용자가 프로비저닝한 인프라 설치를 수행하는 경우, 제공된 템플릿을 사용하여 모든 필수 구성 요소를 유지할 수 있습니다. [Google Cloud](#)에서 [공유 VPC](#) 를 재사용할 수도 있습니다. 그렇지 않으면 [공급자와 무관한](#) 설치 방법을 사용하여 다른 클라우드에 클러스터를 배포할 수 있습니다.

기존 하드웨어에서 사용자가 프로비저닝한 인프라 설치를 완료할 수도 있습니다. [LPAR](#) ,[IBM Power](#) , 또는 [vSphere](#) 에서는 [RHOSP](#) ,[IBM Z](#)® 또는 [IBM® LinuxONE](#) , [IBM Z](#)® 및 [IBM® LinuxONE](#) 을 사용하는 경우 특정 설치 지침을 사용하여 클러스터를 배포합니다. 다른 지원되는 하드웨어를 사용하는 경우 [베어 메탈 설치](#) 절차를 따르십시오. [vSphere](#) 및 [베어 메탈](#) 과 같은 일부 플랫폼의 경우 설치 중에 추가 네트워크 매개변수를 사용자 지정할 수도 있습니다.

2.1.4. 클러스터에 추가 보안이 필요하십니까?

사용자가 프로비저닝한 설치 메서드를 사용하는 경우 클러스터에 대한 프록시를 구성할 수 있습니다. 지침은 각 설치 절차에 포함됩니다.

퍼블릭 클라우드의 클러스터가 외부에서 끝점을 노출하지 못하도록 하려면 [AWS](#) ,[Azure](#) 또는 [Google Cloud](#) 에 설치 관리자 프로비저닝 인프라가 있는 프라이빗 클러스터를 배포할 수 있습니다.

연결이 끊긴 또는 제한된 네트워크 클러스터와 같은 인터넷에 대한 액세스가 제한된 클러스터를 설치해야 하는 경우 [설치 패키지를 미러링](#) 하고 여기에서 클러스터를 설치할 수 있습니다. [LPAR](#) ,[IBM Power](#)® , [vSphere](#) 또는 베어 메탈 의 제한된 네트워크에 사용자가 프로비저닝한 인프라 설치에 대한 자세한 지침을 따르십시오. https://docs.redhat.com/en/documentation/openshift_container_platform/4.17/html-single/installing_on_ibm_z_and_ibm_linuxone/#installing-restricted-networks-ibm-z-kvm [AWS](#) ,[Google Cloud](#) ,[IBM Cloud](#)®, [Nutanix](#) ,[RHOSP](#) , [vSphere](#) 에 대한 자세한 지침에 따라 설치 관리자 프로비저닝 인프라를 사용하여 클러스터를 제한된 네트워크에 설치할 수도 있습니다.

[AWS GovCloud 리전](#) ,[AWS China 리전](#) 또는 [Azure 정부 리전](#) 에 클러스터를 배포해야 하는 경우 설치 관리자가 프로비저닝한 인프라 설치 중에 해당 사용자 지정 리전을 구성할 수 있습니다.

설치 중에 [FIPS 140-2/140-3 검증](#) 에 대해 NIST에 제출된 RHEL 암호화 라이브러리를 사용하도록 클러스터 머신을 구성할 수도 있습니다.



중요

FIPS 모드에서 부팅된 RHEL(Red Hat Enterprise Linux CoreOS) 또는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행하는 경우 OpenShift Container Platform 코어 구성 요소는 x86_64, ppc64le 및 s390x 아키텍처에서만 FIPS 140-2/140-3 Validation에 대해 NIST에 제출된 RHEL 암호화 라이브러리를 사용합니다.

2.2. 설치 후 사용자용 클러스터 준비

사용자가 클러스터에 액세스하기 전에 클러스터를 설치하는 데는 일부 구성이 필요하지 않습니다. 클러스터를 구성하는 Operator를 [사용자 지정하여](#) 클러스터 자체를 사용자 지정하고 ID 공급자와 같은 다른 필수 시스템과 클러스터를 통합할 수 있습니다.

프로덕션 클러스터의 경우 다음과 같은 통합을 구성해야 합니다.

- [영구 스토리지](#)
- [ID 공급자](#)
- [핵심 OpenShift Container Platform 구성 요소 모니터링](#)

2.3. 워크로드를 위한 클러스터 준비

워크로드 요구 사항에 따라 애플리케이션 배포를 시작하기 전에 추가 단계를 수행해야 할 수 있습니다. 예를 들어 애플리케이션 빌드 전략을 지원하기 위해 인프라를 준비한 후 대기 시간이 짧은 워크로드를 프로비저닝하거나 중요한 워크로드를 보호해야 할 수 있습니다. 애플리케이션 워크로드에 대한 모니터링을 구성할 수도 있습니다. Windows 워크로드를 실행하려는 경우 설치 프로세스 중에 OVN-Kubernetes를 사용하여 하이브리드 네트워킹을 활성화해야 합니다. 클러스터를 설치한 후에는 하이브리드 네트워킹을 활성화할 수 없습니다.

2.4. 다른 플랫폼에 지원되는 설치 방법

다른 플랫폼에서 다른 유형의 설치를 수행할 수 있습니다.



참고

다음 표에 표시된 대로 모든 플랫폼에서 모든 설치 옵션이 지원되는 것은 아닙니다. 확인 표시는 옵션이 지원되고 관련 섹션에 대한 링크가 있음을 나타냅니다.

표 2.1. 설치 프로그램에서 제공하는 인프라 옵션

	AWS (64비트 x86_64)	Azure (64비트 x86_64)	Azure (64비트 ARM)	Google Cloud (64비트 x86_64)	Google Cloud (64비트 ARM)	Google Cloud (64비트 ARM)	Nutanix RH OS P	RHEL OS P	베어페탈 (64비트 x86_64)	베어페탈 (64비트 ARM)	vSphere	IBM Cloud®	IBM Z®	IBM Power®	IBM Virtual Server	
Default	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
사용자 지정	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓				✓
네트워크 사용자 지정	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓				

	AWS (64 비트 x86)	AWS (64 비트 ARM)	Azure (64 비트 x86)	Azure (64 비트 ARM)	Azure Stack Hub	Google Cloud (64-bit x86)	Google Cloud (64 비트 ARM)	Nutanix	RHOS P	메이메탈 (64 비트 x86)	메이메탈 (64 비트 ARM)	vSphere	IBM Cloud [®]	IBM Z [®]	IBM Power [®]	IBM Power [®] Virtual Server
제한된 네트워크	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓			✓
프라이빗 클러스터	✓	✓	✓	✓		✓	✓						✓			✓
기존 가상사설망	✓	✓	✓	✓		✓	✓						✓			✓
정부 리전	✓		✓													
시크릿 리전	✓															
중국 리전	✓															

표 2.2. 사용자가 제공하는 인프라 옵션

	AWS (64비트 x86)	AWS(64비트 ARM)	Azure (64비트 x86)	Azure (64비트 ARM)	Azure Stack Hub	Google Cloud (64-bit x86)	Google Cloud (64비트 ARM)	Nutanix	RHOSP	베어메탈 (64비트 x86)	베어메탈 (64비트 ARM)	vSphere	IBM Cloud [®]	IBM Z [®]	IBM Z [®] with HELIX VM	IBM Power [®]	플랫폼에 구애받지 않음
사용자 지정	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
네트워크 사용자 지정										✓	✓	✓					
제한된 네트워크	✓	✓				✓	✓			✓	✓	✓		✓	✓	✓	

AWS (64 비트 x86)	AWS (64 비트 ARM)	Azure (64 비트 x86)	Azure (64 비트 ARM)	Azure Stack Hub	Google Cloud (64-bit x86)	Google Cloud (64 비트 ARM)	Nutanix	RHOSP	베어메탈 (64 비트 x86)	베어메탈 (64 비트 ARM)	vSphere	IBM Cloud®	IBM Z®	IBM Z® with RHEL KVM	IBM Power®	플랫폼에 구애받지 않음
클러스터 프로젝트의 부에서 호스팅되는 공유 VPC					✓	✓										

3장. 클러스터 기능

클러스터 관리자는 클러스터 기능을 사용하여 설치 전에 선택적 구성 요소를 활성화하거나 비활성화할 수 있습니다. 클러스터 관리자는 설치 후 언제든지 클러스터 기능을 활성화할 수 있습니다.

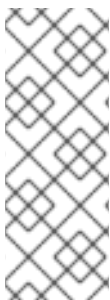


참고

클러스터 관리자는 활성화된 후에는 클러스터 기능을 비활성화할 수 없습니다.

3.1. 클러스터 기능 활성화

`install-config.yaml` 파일을 생성하여 클러스터를 사용자 정의하는 데 필요한 설치 방법을 사용하는 경우 클러스터에서 사용할 클러스터 기능을 선택할 수 있습니다.



참고

특정 클러스터 기능을 활성화하거나 비활성화하여 클러스터를 사용자 지정하는 경우 `install-config.yaml` 파일을 수동으로 유지 관리해야 합니다. 새로운 OpenShift Container Platform 업데이트는 기존 구성 요소에 대한 새로운 기능 처리를 선언하거나 새 구성 요소를 완전히 도입할 수 있습니다. `install-config.yaml` 파일을 사용자 지정하는 사용자는 OpenShift Container Platform이 업데이트되므로 `install-config.yaml` 파일을 정기적으로 업데이트하는 것이 좋습니다.

다음 구성 매개변수를 사용하여 클러스터 기능을 선택할 수 있습니다.

capabilities:

```
baselineCapabilitySet: v4.11 1
additionalEnabledCapabilities: 2
- CSISnapshot
- Console
- Storage
```

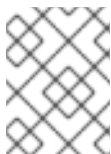
- 1 설치할 기본 기능 세트를 정의합니다. 유효한 값은 **None**, **v Current** 및 **v4.x**입니다. **None**을 선택하면 모든 선택적 기능이 비활성화됩니다. 기본값은 모든 선택적 기능을 활성화하는 **v current**입니다.



참고

v4.x는 현재 클러스터 버전을 포함하여 최대 값을 나타냅니다. 예를 들어 OpenShift Container Platform 4.12 클러스터에 유효한 값은 **v4.11** 및 **v4.12**입니다.

- 2 명시적으로 활성화할 기능 목록을 정의합니다. 이러한 기능은 `baselineCapabilitySet`에 지정된 기능 외에 사용할 수 있습니다.



참고

이 예에서 기본 기능은 **v4.11**로 설정됩니다. `additionalEnabledCapabilities` 필드는 기본 **v4.11** 기능 세트를 통해 추가 기능을 활성화합니다.

다음 표에서는 `baselineCapabilitySet` 값을 설명합니다.

표 3.1. 클러스터 기능 **baselineCapabilitySet** 값 설명

현재의	설명
vCurrent	새 릴리스에 도입된 새로운 기본 기능을 자동으로 추가하려는 경우 이 옵션을 지정합니다.
v4.11	OpenShift Container Platform 4.11의 기본 기능을 활성화하려면 이 옵션을 지정합니다. v4.11 을 지정하면 최신 버전의 OpenShift Container Platform에 도입된 기능이 활성화되어 있지 않습니다. OpenShift Container Platform 4.11의 기본 기능은 baremetal,MachineAPI,marketplace 및 openshift-samples 입니다.
v4.12	OpenShift Container Platform 4.12의 기본 기능을 활성화하려면 이 옵션을 지정합니다. v4.12 를 지정하면 최신 버전의 OpenShift Container Platform에 도입된 기능이 활성화되어 있지 않습니다. OpenShift Container Platform 4.12의 기본 기능은 baremetal,MachineAPI,marketplace,openshift-samples,Console,Insights,Storage, CSISnapshot 입니다.
v4.13	OpenShift Container Platform 4.13의 기본 기능을 활성화하려면 이 옵션을 지정합니다. v4.13 을 지정하면 최신 버전의 OpenShift Container Platform에 도입된 기능이 활성화되어 있지 않습니다. OpenShift Container Platform 4.13의 기본 기능은 baremetal,MachineAPI,marketplace,openshift-samples,Console,Insights,Storage,CSISnapshot, NodeTuning 입니다.
v4.14	OpenShift Container Platform 4.14의 기본 기능을 활성화하려면 이 옵션을 지정합니다. v4.14 를 지정하면 최신 버전의 OpenShift Container Platform에 도입된 기능이 활성화되어 있지 않습니다. OpenShift Container Platform 4.14의 기본 기능은 baremetal,MachineAPI,marketplace,openshift-samples,콘솔,Insights,Storage,CSISnapshot,NodeTuning,ImageRegistry,Build, DeploymentConfig 입니다.
v4.15	OpenShift Container Platform 4.15의 기본 기능을 활성화하려면 이 옵션을 지정합니다. v4.15 를 지정하면 최신 버전의 OpenShift Container Platform에 도입된 기능이 활성화되어 있지 않습니다. OpenShift Container Platform 4.15의 기본 기능은 baremetal, MachineAPI, marketplace, OperatorLifecycleManager, openshift-samples, Console, Insights, Storage, CSISnapshot, NodeTuning, ImageRegistry, Build, CloudCredential, and DeploymentConfig 입니다.

현재의	설명
v4.16	OpenShift Container Platform 4.16의 기본 기능을 활성화하려면 이 옵션을 지정합니다. v4.16 을 지정하면 최신 버전의 OpenShift Container Platform에 도입된 기능이 활성화되어 있지 않습니다. OpenShift Container Platform 4.16의 기본 기능은 baremetal, MachineAPI, marketplace, OperatorLifecycleManager, openshift-samples, Console, Insights, Storage, CSISnapshot, NodeTuning, ImageRegistry, Build, CloudCredential, DeploymentConfig, CloudControllerManager 입니다.
v4.17	OpenShift Container Platform 4.17의 기본 기능을 활성화하려면 이 옵션을 지정합니다. v4.17 을 지정하면 최신 버전의 OpenShift Container Platform에 도입된 기능이 활성화되어 있지 않습니다. OpenShift Container Platform 4.17의 기본 기능은 baremetal, MachineAPI, marketplace, OperatorLifecycleManager, openshift-samples, Console, Storage, CSISnapshot, NodeTuning, ImageRegistry, Build, CloudCredential, DeploymentConfig 및 CloudControllerManager 입니다.
없음	다른 세트가 너무 클 때를 지정하고 기능이 필요하지 않거나 additionalEnabledCapabilities 를 통해 미세 조정하려는 시기를 지정합니다.

추가 리소스

- [사용자 지정으로 AWS에 클러스터 설치](#)
- [사용자 지정으로 Google Cloud에 클러스터 설치](#)

3.2. OPENSIFT CONTAINER PLATFORM 4.17의 선택적 클러스터 기능

현재 클러스터 Operator는 이러한 선택적 기능에 대한 기능을 제공합니다. 다음은 각 기능에서 제공하는 기능과 비활성화된 경우 어떤 기능이 손실되는지를 요약한 것입니다.

추가 리소스

- [클러스터 Operator 참조](#)

3.2.1. 베어 메탈 기능

Cluster Baremetal Operator는 **baremetal** 기능에 대한 기능을 제공합니다.

CNO(Cluster Baremetal Operator)는 베어 메탈 서버를 사용하여 OpenShift Container Platform 컴퓨팅

노드를 실행할 준비가 된 작업자 노드에 모든 구성 요소를 배포합니다. CBO를 사용하면 Bare Metal Operator(BMO) 및 Ironic 컨테이너로 구성된 metal3 배포가 OpenShift Container Platform 클러스터 내의 컨트롤 플레인 노드 중 하나에서 실행됩니다. CBO는 또한 조사하여 적절한 조치를 취하는 리소스에 대한 OpenShift Container Platform 업데이트를 수신 대기합니다.

베어 메탈 기능은 설치 관리자 프로비저닝 인프라를 사용하는 배포에 필요합니다. 베어 메탈 기능을 비활성화하면 이러한 배포에 예기치 않은 문제가 발생할 수 있습니다.



중요

베어 메탈 기능이 비활성화된 경우 클러스터는 베어 메탈 노드를 프로비저닝하거나 관리할 수 없습니다. 배포에 **BareMetalHost** 리소스가 없는 경우에만 기능을 비활성화합니다. **baremetal** 기능은 **MachineAPI** 기능에 따라 다릅니다. **baremetal** 기능을 활성화하는 경우 **MachineAPI** 도 활성화해야 합니다.



참고

클러스터 관리자는 클러스터에 **BareMetalHost** 리소스가 없는 사용자 프로비저닝 인프라를 사용하여 설치하는 동안 베어 메탈 기능만 비활성화하는 것이 좋습니다.

추가 리소스

- [베어 메탈에 설치 프로그램이 프로비저닝 한 클러스터 배포](#)
- [베어 메탈 클러스터 설치 준비](#)
- [Bare Metal Operator를 사용한 구성](#)

3.2.2. 빌드 기능

3.2.2.1. 목적

빌드 기능을 사용하면 빌드 API가 활성화됩니다. **Build API**는 **Build** 및 **BuildConfig** 오브젝트의 라이프사이클을 관리합니다.



중요

빌드 기능을 비활성화하면 클러스터에서 다음 리소스를 사용할 수 없습니다.

- 빌드 및 **BuildConfig** 리소스
- 빌더 서비스 계정

빌드 및 **BuildConfig** 리소스 또는 클러스터의 **builder** 서비스 계정이 필요하지 않은 경우에만 **Build** 기능을 비활성화합니다.

3.2.3. 클라우드 컨트롤러 관리자 기능

Cloud Controller Manager Operator는 **CloudControllerManager** 기능에 대한 기능을 제공합니다.



참고

현재 모든 플랫폼에서 **CloudControllerManager** 기능 비활성화가 지원되지 않습니다.

클러스터의 설치 구성(**install-config.yaml**) 파일에서 값을 확인하여 클러스터가 **CloudControllerManager** 기능 비활성화를 지원하는지 확인할 수 있습니다.

install-config.yaml 파일에서 **platform** 매개변수를 찾습니다.

- **platform** 매개변수 값이 **Baremetal** 또는 **None** 인 경우 클러스터에서 **CloudControllerManager** 기능을 비활성화할 수 있습니다.
- **platform** 매개변수 값이 **External** 이면 **platform.external.cloudControllerManager** 매개변수를 찾습니다. **platform.external.cloudControllerManager** 매개변수 값이 **None** 인 경우 클러스터에서 **CloudControllerManager** 기능을 비활성화할 수 있습니다.



중요

이러한 매개변수에 나열된 값이 아닌 다른 매개변수가 포함된 경우 클러스터에서 **CloudControllerManager** 기능을 비활성화할 수 없습니다.



참고

이 Operator의 상태는 AWS(Amazon Web Services), Google Cloud, IBM Cloud®, 글로벌 Microsoft Azure, Microsoft Azure Stack Hub, Nutanix, RHOSP(Red Hat OpenStack Platform) 및 VMware vSphere의 일반 가용성입니다.

Operator는 IBM Power® Virtual Server용 [기술 프리뷰로](#) 사용할 수 있습니다.

Cloud Controller Manager Operator는 OpenShift Container Platform 상단에 배포된 클라우드 컨트롤러 관리자를 관리하고 업데이트합니다. Operator는 Kubebuilder 프레임워크 및 **controller-runtime** 라이브러리를 기반으로 합니다. CVO(Cluster Version Operator)를 사용하여 Cloud Controller Manager Operator를 설치할 수 있습니다.

Cloud Controller Manager Operator에는 다음 구성 요소가 포함되어 있습니다.

- Operator
- 클라우드 구성 관찰자

기본적으로 Operator는 **metrics** 서비스를 통해 Prometheus 지표를 표시합니다.

3.2.4. 클라우드 인증 정보 기능

Cloud Credential Operator는 **CloudCredential** 기능에 대한 기능을 제공합니다.



참고

현재 **CloudCredential** 기능 비활성화는 베어 메탈 클러스터에만 지원됩니다.

CCO(Cloud Credential Operator)는 클라우드 공급자 인증 정보를 Kubernetes CRD(사용자 지정 리소스 정의)로 관리합니다. CCO는 **CredentialsRequest** CR(사용자 정의 리소스)에서 동기화되어 OpenShift Container Platform 구성 요소가 클러스터를 실행하는 데 필요한 특정 권한이 있는 클라우드 공급자 자격 증명을 요청할 수 있습니다.

install-config.yaml 파일에서 **credentialsMode** 매개변수에 다양한 값을 설정하면 CCO를 여러 모드에서 작동하도록 구성할 수 있습니다. 모드가 지정되지 않거나 **credentialsMode** 매개변수가 빈 문자열("")로 설정되면 CCO는 기본 모드에서 작동합니다.

추가 리소스

- [Cloud Credential Operator 정보](#)

3.2.5. 클러스터 이미지 레지스트리 기능

Cluster Image Registry Operator는 **ImageRegistry** 기능에 대한 기능을 제공합니다.

Cluster Image Registry Operator는 OpenShift 이미지 레지스트리의 단일 인스턴스를 관리합니다. 스토리지 생성을 포함하여 레지스트리의 모든 구성을 관리합니다.

처음 시작 시 Operator는 클러스터에서 탐지된 구성에 따라 기본 **image-registry** 리소스 인스턴스를 생성합니다. 이는 클라우드 공급자를 기반으로 사용할 클라우드 스토리지 유형을 나타냅니다.

완전한 **image-registry** 리소스를 정의하는 데 사용할 수 있는 정보가 충분하지 않으면 불완전한 리소스가 정의되고 Operator는 누락된 항목에 대한 정보를 사용하여 리소스 상태를 업데이트합니다.

Cluster Image Registry Operator는 **openshift-image-registry** 네임스페이스에서 실행되며 해당 위치의 레지스트리 인스턴스도 관리합니다. 레지스트리의 모든 설정 및 워크로드 리소스는 해당 네임스페이스에 있습니다.

이미지 레지스트리를 클러스터의 사용자 인증 및 권한 부여 시스템에 통합하기 위해 클러스터의 각 서비스 계정에 대한 이미지 풀 시크릿이 생성됩니다.



중요

ImageRegistry 기능을 비활성화하거나 Cluster Image Registry Operator 구성에서 통합 OpenShift 이미지 레지스트리를 비활성화하는 경우 각 서비스 계정에 대해 이미지 풀 시크릿이 생성되지 않습니다.

ImageRegistry 기능을 비활성화하면 Telco 환경에서 OpenShift Container Platform의 전체 리소스 공간을 줄일 수 있습니다. 배포에 따라 필요하지 않은 경우 이 구성 요소를 비활성화할 수 있습니다.

3.2.5.1. 프로젝트

[cluster-image-registry-operator](#)

추가 리소스

- [OpenShift Container Platform의 이미지 레지스트리 Operator](#)
- [자동 생성된 보안](#)

3.2.6. 클러스터 스토리지 기능

Cluster **Storage** Operator는 스토리지 기능에 대한 기능을 제공합니다.

Cluster Storage Operator는 OpenShift Container Platform 클러스터 수준 스토리지 기본값을 설정합니다. 이는 OpenShift Container Platform 클러스터에 기본 **스토리지 클래스**가 있는지 확인합니다. 또한 클러스터가 다양한 스토리지 백엔드를 사용할 수 있는 CSI(Container Storage Interface) 드라이버를 설치

합니다.



중요

클러스터 스토리지 기능이 비활성화된 경우 클러스터에 기본 스토리지 클래스 또는 CSI 드라이버가 없습니다. 관리자 권한이 있는 사용자는 기본 스토리지 클래스를 생성하고 클러스터 스토리지 기능이 비활성화된 경우 CSI 드라이버를 수동으로 설치할 수 있습니다.

3.2.6.1. 참고

- Operator에서 생성하는 스토리지 클래스는 주석을 편집하여 기본이 아닌 상태로 만들 수 있지만 Operator가 실행되는 동안 이 스토리지 클래스를 삭제할 수 없습니다.

3.2.7. 콘솔 기능

Console Operator는 콘솔 기능에 대한 기능을 제공합니다.

Console Operator에서 클러스터에 OpenShift Container Platform 웹 콘솔을 설치하고 유지 관리합니다. Console Operator는 기본적으로 설치되고 콘솔을 자동으로 유지 관리합니다.

추가 리소스

- [웹 콘솔 개요](#)

3.2.8. CSI 스냅샷 컨트롤러 기능

Cluster CSI Snapshot Controller Operator는 **CSISnapshot** 기능에 대한 기능을 제공합니다.

Cluster CSI Snapshot Controller Operator는 CSI Snapshot Controller를 설치하고 유지 관리합니다. CSI Snapshot Controller는 **VolumeSnapshot** CRD 오브젝트를 모니터링하고 볼륨 스냅샷의 생성 및 삭제 라이프사이클을 관리합니다.

추가 리소스

- [CSI 볼륨 스냅샷](#)

3.2.9. DeploymentConfig 기능

3.2.9.1. 목적

DeploymentConfig 기능은 **DeploymentConfig** API를 활성화하고 관리합니다.



중요

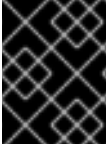
DeploymentConfig 기능을 비활성화하면 클러스터에서 다음 리소스를 사용할 수 없습니다.

- **DeploymentConfig** 리소스
- **deployer** 서비스 계정

클러스터에 **DeploymentConfig** 리소스 및 배포자 서비스 계정이 필요하지 않은 경우에만 **DeploymentConfig** 기능을 비활성화합니다.

3.2.10. Ingress 기능

Ingress Operator는 Ingress 기능 기능을 제공합니다. Ingress 기능은 기본적으로 활성화되어 있습니다.



중요

baselineCapabilitySet 필드를 **None** 으로 설정하는 경우 Ingress 기능이 비활성화된 경우 클러스터 설치에 실패하므로 Ingress 기능을 명시적으로 활성화해야 합니다.

Ingress Operator는 OpenShift Container Platform 라우터를 구성하고 관리합니다.

3.2.10.1. 프로젝트

[openshift-ingress-operator](#)

3.2.10.2. CRD

- **clusteringresses.ingress.openshift.io**
 - 범위: 네임스페이스
 - CR: **clusteringresses**
 - 검증: 아니요

3.2.10.3. 구성 오브젝트

- 클러스터 구성
 - 유형 이름: **clusteringresses.ingress.openshift.io**
 - 인스턴스 이름: **default**
 - 보기 명령:

```
$ oc get clusteringresses.ingress.openshift.io -n openshift-ingress-operator default -o yaml
```

3.2.10.4. 참고

Ingress Operator는 **openshift-ingress** 프로젝트에서 라우터를 설정하고 라우터용 배포를 생성합니다.

```
$ oc get deployment -n openshift-ingress
```

Ingress Operator는 **network/cluster** 상태의 **clusterNetwork[].cidr** 을 사용하여 관리형 Ingress 컨트롤러 (라우터)가 작동해야 하는 모드(IPv4, IPv6 또는 듀얼 스택)를 확인합니다. 예를 들어 **clusterNetwork** 에 v6 **cidr** 만 포함된 경우 Ingress 컨트롤러는 IPv6 전용 모드에서 작동합니다.

다음 예제에서는 클러스터 네트워크가 하나만 존재하고 네트워크가 IPv4 **cidr** 이므로 Ingress Operator에서 관리하는 Ingress 컨트롤러가 IPv4 전용 모드에서 실행됩니다.

```
$ oc get network/cluster -o jsonpath='{.status.clusterNetwork[*]}'
```

출력 예

```
map[cidr:10.128.0.0/14 hostPrefix:23]
```

3.2.11. Insights 기능

Insights Operator는 **Insights** 기능에 대한 기능을 제공합니다.

Insights Operator는 OpenShift Container Platform 구성 데이터를 수집하여 Red Hat으로 보냅니다. 데이터는 클러스터가 노출될 수 있는 문제에 대한 사전 예방적 인사이트 권장 사항을 생성하는 데 사용됩니다. 이러한 통찰력은 [console.redhat.com](#)의 Insights 권고 서비스를 통해 클러스터 관리자에게 전달됩니다.

3.2.11.1. 참고

Insights Operator는 OpenShift Container Platform Telemetry를 보완합니다.

추가 리소스

- [Insights Operator 사용](#)

3.2.12. 머신 API 기능

machine-api-operator, **cluster-autoscaler-operator** 및 **cluster-control-plane-machine-set-operator** Operator는 **MachineAPI** 기능의 기능을 제공합니다. 사용자 프로비저닝 인프라가 있는 클러스터를 설치하는 경우에만 이 기능을 비활성화할 수 있습니다.

Machine API 기능은 클러스터의 모든 머신 구성 및 관리를 담당합니다. 설치 중에 Machine API 기능을 비활성화하는 경우 모든 머신 관련 작업을 수동으로 관리해야 합니다.

추가 리소스

- [머신 관리 개요](#)
- [Machine API Operator](#)
- [Cluster Autoscaler Operator](#)
- [Control Plane Machine Set Operator](#)

3.2.13. 시장 기능

Marketplace Operator는 Marketplace 기능에 대한 기능을 제공합니다.

Marketplace Operator는 클러스터에서 기본 OLM(Operator Lifecycle Manager) 카탈로그 세트를 사용하여 클러스터 외부 Operator를 클러스터에 가져오는 프로세스를 간소화합니다. Marketplace Operator가 설치되면 **openshift-marketplace** 네임스페이스를 생성합니다. OLM은 **openshift-marketplace** 네임스페이스에 설치된 카탈로그 소스를 클러스터의 모든 네임스페이스에 사용할 수 있도록 합니다.

Marketplace 기능을 비활성화하면 Marketplace Operator에서 **openshift-marketplace** 네임스페이스를 생성하지 않습니다. 카탈로그 소스는 클러스터에서 수동으로 구성 및 관리할 수 있지만 클러스터의 모든 네임스페이스에서 카탈로그를 사용할 수 있도록 OLM은 **openshift-marketplace** 네임스페이스에 따라 다릅니다. 시스템 또는 클러스터 관리자와 같이 **openshift-** 접두사가 있는 네임스페이스를 생성할 수 있는 승격된 권한이 있는 사용자는 **openshift-marketplace** 네임스페이스를 수동으로 생성할 수 있습니다.

Marketplace 기능을 활성화하면 Marketplace Operator를 구성하여 개별 카탈로그를 활성화하고 비활성화할 수 있습니다.

추가 리소스

- [Red Hat 제공 Operator 카탈로그](#)

3.2.14. 노드 튜닝 기능

Node Tuning Operator는 **NodeTuning** 기능에 대한 기능을 제공합니다.

Node Tuning Operator는 **TuneD** 데몬을 오케스트레이션하여 노드 수준 튜닝을 관리하고 **Performance Profile** 컨트롤러를 사용하여 대기 시간이 짧은 성능을 달성하는 데 도움이 됩니다. 대부분의 고성능 애플리케이션에는 일정 수준의 커널 튜닝이 필요합니다. **Node Tuning Operator**는 노드 수준 **sysctls** 사용자에게 통합 관리 인터페이스를 제공하며 사용자의 필요에 따라 지정되는 사용자 정의 튜닝을 추가할 수 있는 유연성을 제공합니다.

NodeTuning 기능을 비활성화하면 일부 기본 튜닝 설정이 **control-plane** 노드에 적용되지 않습니다. 이로 인해 900개가 넘는 노드 또는 900개가 넘는 대규모 클러스터의 확장성 및 성능이 제한될 수 있습니다.

추가 리소스

- [Node Tuning Operator 사용](#)

3.2.15. OpenShift 샘플 기능

Cluster Samples Operator는 **openshift-samples** 기능에 대한 기능을 제공합니다.

Cluster Samples Operator는 **openshift** 네임스페이스에 저장된 샘플 이미지 스트림 및 템플릿을 관리합니다.

처음 시작 시 **Operator**는 기본 샘플 구성 리소스를 생성하여 이미지 스트림 및 템플릿을 생성하기 시작합니다. 구성 오브젝트는 키가 **cluster**이고 유형이 **configs.samples**인 클러스터 범위 지정 오브젝트입니다.

이미지 스트림은 registry.redhat.io의 이미지를 가리키는 RHCOS(Red Hat Enterprise Linux CoreOS) 기반 OpenShift Container Platform 이미지 스트림입니다. 마찬가지로 템플릿은 OpenShift Container Platform 템플릿으로 분류된 템플릿입니다.

샘플 기능을 비활성화하면 사용자가 제공하는 이미지 스트림, 샘플 및 템플릿에 액세스할 수 없습니다. 배포에 따라 필요하지 않은 경우 이 구성 요소를 비활성화해야 할 수 있습니다.

추가 리소스

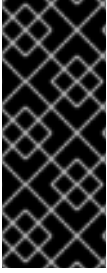
- [Cluster Samples Operator 구성](#)

3.2.16. Operator Lifecycle Manager 기능

OLM(*Operator Lifecycle Manager*)은 OpenShift Container Platform 클러스터에서 실행되는 Kubernetes 네이티브 애플리케이션(Operator) 및 관련 서비스의 라이프사이클을 설치, 업데이트, 관리하는 데 도움이 됩니다. Operator 프레임워크의 일부로, 효과적이고 자동화되었으며 확장 가능한 방식으로 Operator를 관리하도록 설계된 오픈 소스 툴킷입니다.

Operator에 다음 API가 필요한 경우 OperatorLifecycleManager 기능을 활성화해야 합니다.

- **ClusterServiceVersion**
- **CatalogSource**
- **서브스크립션**
- **InstallPlan**
- **OperatorGroup**



중요

Marketplace 기능은 OperatorLifecycleManager 기능에 따라 다릅니다. OperatorLifecycleManager 기능을 비활성화하고 Marketplace 기능을 활성화할 수 없습니다.

추가 리소스

- [Operator Lifecycle Manager 개념 및 리소스](#)

3.3. 클러스터 기능 보기

클러스터 관리자는 `clusterversion` 리소스 상태를 사용하여 기능을 볼 수 있습니다.

사전 요구 사항

- **OpenShift CLI(oc)**가 설치되어 있습니다.

프로세스

- 클러스터 기능의 상태를 보려면 다음 명령을 실행합니다.

```
$ oc get clusterversion version -o jsonpath='{.spec.capabilities}{"\n"}
{.status.capabilities}{"\n"}'
```

출력 예

```
{"additionalEnabledCapabilities":["openshift-
samples"],"baselineCapabilitySet":"None"}
{"enabledCapabilities":["openshift-samples"],"knownCapabilities":
["CSISnapshot","Console","Insights","Storage","baremetal","marketplace","openshift-
samples"]}
```

3.4. 기준 기능 세트를 설정하여 클러스터 기능 활성화

클러스터 관리자는 **baselineCapabilitySet** 구성 매개변수를 설정하여 **OpenShift Container Platform** 을 설치한 후 언제든지 클러스터 기능을 활성화할 수 있습니다.

사전 요구 사항

- **OpenShift CLI(oc)**가 설치되어 있습니다.

프로세스

- **baselineCapabilitySet** 구성 매개변수를 설정하려면 다음 명령을 실행합니다.

```
$ oc patch clusterversion version --type merge -p '{"spec":{"capabilities":{"baselineCapabilitySet":"vCurrent"}}}' 1
```

1

baselineCapabilitySet 의 경우 **vCurrent**, **v4.17** 또는 **None** 을 지정할 수 있습니다.

3.5. 추가 활성화된 기능을 설정하여 클러스터 기능 활성화

클러스터 관리자는 **additionalEnabledCapabilities** 구성 매개변수를 설정하여 **OpenShift Container Platform** 설치 후 언제든지 클러스터 기능을 활성화할 수 있습니다.

사전 요구 사항

- **OpenShift CLI(oc)**가 설치되어 있습니다.

프로세스

1. 다음 명령을 실행하여 추가 활성화된 기능을 확인합니다.

```
$ oc get clusterversion version -o jsonpath='{.spec.capabilities.additionalEnabledCapabilities}'
```

출력 예

`["openshift-samples"]`

2.

`additionalEnabledCapabilities` 구성 매개 변수를 설정하려면 다음 명령을 실행합니다.

```
$ oc patch clusterversion/version --type merge -p '{"spec":{"capabilities":{"additionalEnabledCapabilities":["openshift-samples", "marketplace"]}}}'
```

중요

클러스터에서 이미 활성화되어 있는 기능을 비활성화할 수 없습니다. **CVO**(클러스터 버전 **Operator**)는 클러스터에서 이미 활성화된 기능을 계속 조정합니다.

기능을 비활성화하려고 하면 **CVO**에 다양한 사양이 표시됩니다.

```
$ oc get clusterversion version -o jsonpath='{.status.conditions[?(@.type=="ImplicitlyEnabledCapabilities")]}{"\n"}'
```

출력 예

```
{"lastTransitionTime":"2022-07-22T03:14:35Z","message":"The following capabilities could not be disabled: openshift-samples","reason":"CapabilitiesImplicitlyEnabled","status":"True","type":"ImplicitlyEnabledCapabilities"}
```

참고

클러스터 업그레이드 중에 지정된 기능을 암시적으로 활성화할 수 있습니다. 업그레이드하기 전에 리소스가 클러스터에서 이미 실행 중인 경우 리소스의 일부인 모든 기능이 활성화됩니다. 예를 들어 클러스터를 업그레이드하는 동안 클러스터에서 이미 실행 중인 리소스가 시스템의 **marketplace** 기능의 일부로 변경되었습니다. 클러스터 관리자가 **Marketplace** 기능을 명시적으로 활성화하지 않더라도 시스템에서 암시적으로 활성화합니다.

4장. FIPS 암호화 지원

FIPS 모드에서 OpenShift Container Platform 클러스터를 설치할 수 있습니다.

OpenShift Container Platform은 FIPS용으로 설계되었습니다. FIPS 모드에서 부팅된 RHEL(Red Hat Enterprise Linux CoreOS) 또는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행하는 경우 OpenShift Container Platform 코어 구성 요소는 x86_64, ppc64le 및 s390x 아키텍처에서만 FIPS 140-2/140-3 Validation에 대해 NIST에 제출된 RHEL 암호화 라이브러리를 사용합니다.

NIST 검증 프로그램에 대한 자세한 내용은 [암호화 모듈 유효성 검사 프로그램](#)을 참조하십시오. 검증을 위해 제출된 개별 RHEL 암호화 라이브러리의 최신 NIST 상태는 [규정 준수 활동 및 정부 표준](#)을 참조하십시오.

중요

클러스터에 대한 FIPS 모드를 활성화하려면 FIPS 모드에서 작동하도록 구성된 RHEL 9 컴퓨터에서 설치 프로그램을 실행해야 하며 FIPS 가능 버전의 설치 프로그램을 사용해야 합니다. '[oc adm extract](#)'를 사용하여 FIPS 지원 설치 프로그램 가져오기 섹션을 참조하십시오.

RHEL에서 FIPS 모드 구성에 대한 자세한 내용은 [FIPS 모드에서 시스템 설치](#)를 참조하십시오.

클러스터의 RHCOS (Red Hat Enterprise Linux CoreOS) 시스템의 경우 이 변경 사항은 사용자가 클러스터의 배치시 변경할 수 있는 클러스터 옵션을 제어하는 `install-config.yaml` 파일의 옵션 상태를 기반으로 시스템을 배치할 때 적용됩니다. Red Hat Enterprise Linux (RHEL) 시스템에서는 작업자 시스템으로 사용하려는 시스템에 운영 체제를 설치할 때 FIPS 모드를 활성화해야 합니다.

클러스터가 사용하는 운영 체제를 처음 부팅하기 전에 FIPS를 활성화해야하므로 클러스터를 배포한 후 FIPS를 활성화할 수 없습니다.

4.1. OC ADM EXTRACT를 사용하여 FIPS 지원 설치 프로그램 가져오기

OpenShift Container Platform에서는 FIPS 모드에서 클러스터를 설치하려면 FIPS 지원 설치 바이너리를 사용해야 합니다. OpenShift CLI(oc)를 사용하여 릴리스 이미지에서 추출하여 이 바이너리를 가져

을 수 있습니다. 바이너리를 가져온 후 클러스터 설치를 진행하여 **openshift-install** 명령의 모든 인스턴스를 **openshift-install-fips** 로 교체합니다.

사전 요구 사항

- 버전 4.16 이상과 함께 **OpenShift CLI(oc)**를 설치했습니다.

프로세스

1. 다음 명령을 실행하여 설치 프로그램에서 **FIPS** 가능 바이너리를 추출합니다.

```
$ oc adm release extract --registry-config "${pullsecret_file}" --command=openshift-install-fips --to "${extract_dir}" ${RELEASE_IMAGE}
```

다음과 같습니다.

<pullsecret_file>

풀 시크릿이 포함된 파일의 이름을 지정합니다.

<extract_dir>

바이너리를 추출할 디렉토리를 지정합니다.

<RELEASE_IMAGE>

사용 중인 **OpenShift Container Platform** 릴리스의 **Quay.io URL**을 지정합니다. 릴리스 이미지 검색에 대한 자세한 내용은 **OpenShift Container Platform 설치 프로그램 추출**을 참조하십시오.

2. **openshift-install** 명령의 모든 인스턴스를 **openshift-install-fips** 로 교체하여 클러스터 설치를 진행합니다.

추가 리소스

- [OpenShift Container Platform 설치 프로그램 추출](#)

4.2. 공용 OPENSIFT 미러를 사용하여 FIPS 지원 설치 프로그램 가져오기

OpenShift Container Platform에서는 FIPS 모드에서 클러스터를 설치하려면 FIPS 지원 설치 바이너리를 사용해야 합니다. 공용 OpenShift 미러에서 이 바이너리를 다운로드하여 가져올 수 있습니다. 바이너리를 가져온 후 클러스터 설치를 진행하여 `openshift-install` 바이너리의 모든 인스턴스를 `openshift-install-fips` 로 바꿉니다.

사전 요구 사항

- 인터넷에 액세스할 수 있습니다.

프로세스

1. <https://mirror.openshift.com/pub/openshift-v4/clients/ocp/latest-4.17/openshift-install-rhel9-amd64.tar.gz> 에서 설치 프로그램을 다운로드합니다.
2. 설치 프로그램 파일의 압축을 풉니다. 예를 들어 Linux 운영 체제를 사용하는 컴퓨터에서 다음 명령을 실행합니다.


```
$ tar -xvf openshift-install-rhel9-amd64.tar.gz
```
3. `openshift-install` 명령의 모든 인스턴스를 `openshift-install-fips` 로 교체하여 클러스터 설치를 진행합니다.

4.3. OPENSIFT CONTAINER PLATFORM에서 FIPS 검증

OpenShift Container Platform은 사용하는 운영 체제 구성 요소에 대해 RHEL 및 RHCOS에서 특정 FIPS 검증 또는 모듈 `In Process` 모듈을 사용합니다. [RHEL 핵심 암호화 구성 요소를 참조하십시오](#). 예를 들어 사용자가 SSH를 사용하여 OpenShift Container Platform 클러스터 및 컨테이너에 연결하면 해당 연결이 올바르게 암호화됩니다.

OpenShift Container Platform 구성 요소는 Go로 작성된 Red Hat의 `golang` 컴파일러를 사용하여 빌드됩니다. 클러스터의 FIPS 모드를 활성화하면 암호화 서명이 필요한 모든 OpenShift Container Platform 구성 요소에 대해 RHEL 및 RHCOS 암호화 라이브러리를 호출합니다.

표 4.1. OpenShift Container Platform 4.17의 FIPS 모드 속성 및 제한 사항

속성	제한
RHEL 9 및 RHCOS 운영 체제에서 FIPS 지원	FIPS 구현은 단일 단계에서 해시 계산 및 서명 생성 또는 검증을 수행하는 함수를 사용하지 않습니다. 이 제한은 향후 OpenShift Container Platform 릴리스에서 지속적으로 평가 및 개선될 예정입니다.
CRI-O 런타임에서 FIPS 지원	
OpenShift Container Platform 서비스에서 FIPS 지원	
RHEL 9 및 RHCOS 바이너리 및 이미지에서 얻은 FIPS 검증 또는 모듈 In Process 암호화 모듈 및 알고리즘	
FIPS 호환 golang 컴파일러 사용	TLS FIPS 지원은 완전히 구현되어 있지 않지만 향후 OpenShift Container Platform 버전에서 완전히 지원될 예정입니다.
여러 아키텍처에서 FIPS 지원	FIPS는 현재 x86_64,ppc64le 및 s390x 아키텍처를 사용하는 OpenShift Container Platform 배포에서만 지원됩니다.

4.4. 클러스터가 사용되는 구성 요소에서 FIPS 지원

OpenShift Container Platform 클러스터 자체는 FIPS 검증 또는 모듈 In Process 모듈을 사용하지만 OpenShift Container Platform 클러스터를 지원하는 시스템이 암호화에 FIPS 검증 또는 진행중인 모듈 (Modules In Process) 모듈을 사용하는지 확인하십시오.

4.4.1. etcd

etcd에 저장된 시크릿이 FIPS 검증 또는 진행중인 모듈 In Process 암호화를 사용하는지 확인하려면 FIPS 모드에서 노드를 부팅합니다. FIPS 모드에서 클러스터를 설치한 후 FIPS가 승인한 aes cbc 암호화 알고리즘을 사용하여 etcd 데이터를 암호화할 수 있습니다.

4.4.2. 스토리지

로컬 스토리지의 경우 RHEL 제공 디스크 암호화 또는 RHEL 제공 디스크 암호화를 사용하는 Container Native Storage를 사용합니다. RHEL 제공 디스크 암호화를 사용하는 볼륨에 모든 데이터를 저장하고 클러스터에 FIPS 모드를 활성화하면 미사용 데이터와 이동중인 데이터 또는 네트워크 데이터가 모두 FIPS 검증 또는 모듈 In Process 암호화로 보호됩니다. 노드 사용자 지정에 설명된 대로 각 노드의 루트 파일 시스템을 암호화하도록 클러스터를 구성할 수 있습니다.

4.4.3. Runtimes

컨테이너가 FIPS 검증 또는 모듈 In Process 암호화 모듈을 사용하는 호스트에서 실행 중인지 확인하

려면 **CRI-O**를 사용하여 런타임을 관리합니다.

4.5. FIPS 모드에서 클러스터 설치

FIPS 모드에서 클러스터를 설치하려면 해당 인프라에 사용자 정의된 클러스터를 설치하는 방법에 대한 프로세스를 따르십시오. 클러스터를 배포하기 전에 `install-config.yaml` 파일에 `fips: true`가 설정되어 있는지 확인하십시오.



중요

클러스터의 **FIPS** 모드를 활성화하려면 **FIPS** 모드에서 작동하도록 구성된 **RHEL** 컴퓨터에서 설치 프로그램을 실행해야 합니다. **RHEL**에서 **FIPS** 모드 구성에 대한 자세한 내용은 [FIPS 모드에서 시스템 설치를 참조하십시오](#).

- [Amazon Web Services](#)
- [Microsoft Azure](#)
- [베어 메탈](#)
- [Google Cloud](#)
- [IBM Cloud®](#)
- [IBM Power®](#)
- [IBM Z® 및 IBM® LinuxONE](#)
- [IBM Z® 및 IBM® LinuxONE with RHEL KVM](#)

- [LPAR의 IBM Z® 및 IBM® LinuxONE](#)
- [Red Hat OpenStack Platform \(RHOSP\)](#)
- [VMware vSphere](#)



참고

Azure File 스토리지를 사용하는 경우 **FIPS** 모드를 활성화할 수 없습니다.

etcd 데이터 저장소에 **AES CBC** 암호화를 적용하려면 클러스터를 설치한 후 **etcd 데이터 암호화** 프로세스를 따르십시오.

RHEL 노드를 클러스터에 추가하는 경우 초기 부팅 전에 머신에서 **FIPS** 모드를 활성화해야 합니다. **OpenShift Container Platform** 클러스터에 **RHEL** 컴퓨팅 머신 추가 및 **FIPS** 모드에서 시스템 설치를 참조하십시오.