



# OpenShift Container Platform 4.9

## 릴리스 노트

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항



# OpenShift Container Platform 4.9 릴리스 노트

---

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항

## 법적 공지

Copyright © 2023 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

OpenShift Container Platform 릴리스 노트에는 새로운 기능, 향상된 기능, 주요 기술 변경 사항, 이전 버전의 주요 수정 사항, GA 관련 알려진 문제가 요약되어 있습니다.

---

## 차례

<b>1장. OPENSIFT CONTAINER PLATFORM 4.9 릴리스 노트</b> .....	<b>3</b>
1.1. 릴리스 정보	3
1.2. OPENSIFT CONTAINER PLATFORM 계층화된 종속 구성 요소 지원 및 호환성	3
1.3. 새로운 기능 및 개선 사항	3
1.4. 주요 기술 변경 사항	24
1.5. 사용되지 않거나 삭제된 기능	25
1.6. 버그 수정	30
1.7. 기술 프리뷰 기능	41
1.8. 확인된 문제	44
1.9. 비동기 에라타 업데이트	50



# 1장. OPENSIFT CONTAINER PLATFORM 4.9 릴리스 노트

Red Hat OpenShift Container Platform은 개발자 및 IT 조직에 새로운 애플리케이션과 기존 애플리케이션을 안전하고 확장 가능한 리소스에 배포할 수 있는 하이브리드 클라우드 애플리케이션 플랫폼을 최소한의 구성 및 관리 비용으로 제공합니다. OpenShift Container Platform은 Java, JavaScript, Python, Ruby, PHP와 같은 다양한 프로그래밍 언어 및 프레임워크를 지원합니다.

Red Hat Enterprise Linux (RHEL) 및 Kubernetes를 기반으로 하는 OpenShift Container Platform은 오늘날의 엔터프라이즈급 애플리케이션을 위해 보다 안전하고 확장 가능한 다중 테넌트 운영 체제를 제공하는 동시에 통합된 애플리케이션 런타임 및 라이브러리를 제공합니다. 조직은 OpenShift Container Platform을 통해 보안, 개인 정보 보호, 규정 준수 및 거버넌스 요구 사항을 충족할 수 있습니다.

## 1.1. 릴리스 정보

OpenShift Container Platform ([RHSA-2021:3759](#))을 사용할 수 있습니다. 이 릴리스에서는 [Kubernetes 1.22](#)를 CRI-O 런타임과 함께 사용합니다. 이 문서에는 OpenShift Container Platform 4.9와 관련된 새로운 기능, 변경 사항, 알려진 문제가 포함되어 있습니다.

OpenShift Container Platform 4.9 클러스터는 <https://console.redhat.com/openshift> 에서 사용할 수 있습니다. OpenShift Container Platform용 Red Hat OpenShift Cluster Manager 애플리케이션을 사용하면 온프레미스 또는 클라우드 환경에 OpenShift 클러스터를 배포할 수 있습니다.

OpenShift Container Platform 4.9는 Red Hat Enterprise Linux 7.9~8.7과 RHCOS(Red Hat Enterprise Linux CoreOS) 4.9에서 지원됩니다.

컨트롤 플레인에는 RHCOS 머신을 사용해야 하며 컴퓨팅 머신에 RHCOS 또는 Red Hat Enterprise Linux (RHEL)를 사용할 수 있습니다.

## 1.2. OPENSIFT CONTAINER PLATFORM 계층화된 종속 구성 요소 지원 및 호환성

OpenShift Container Platform의 계층화된 종속 구성 요소에 대한 지원 범위는 OpenShift Container Platform 버전에 따라 달라집니다. 애드온의 현재 지원 상태 및 호환성을 확인하려면 해당 릴리스 노트를 참조하십시오. 자세한 내용은 [Red Hat OpenShift Container Platform 라이프 사이클 정책](#) 을 참조하십시오.

## 1.3. 새로운 기능 및 개선 사항

이 릴리스에는 다음 구성 요소 및 개념과 관련된 개선 사항이 추가되었습니다.

### 1.3.1. RHCOS(Red Hat Enterprise Linux CoreOS)

#### 1.3.1.1. 부팅 시 설치 Ignition 구성 제거

**coreos-installer** 프로그램으로 설치된 노드는 이전에 **/boot/ignition/config.ign** 파일에 설치 Ignition 구성을 유지했습니다. OpenShift Container Platform 4.9 설치 이미지부터 노드가 프로비저닝될 때 해당 파일이 제거됩니다. 이 변경 사항은 이전 bootimage를 계속 사용하므로 이전 OpenShift Container Platform 버전에 설치된 클러스터에는 영향을 미치지 않습니다.

#### 1.3.1.2. RHCOS에서 RHEL 8.4 사용

RHCOS는 이제 OpenShift Container Platform 4.9에서 RHEL (Red Hat Enterprise Linux) 8.4 패키지를 사용합니다. 이러한 패키지는 NetworkManager 기능과 같은 최신 수정 사항, 기능 및 개선 사항 및 최신 하드웨어 지원 및 드라이버 업데이트를 제공합니다.

### 1.3.2. 설치 및 업그레이드

#### 1.3.2.1. 사용자 프로비저닝 인프라를 사용하여 Microsoft Azure Stack Hub에 클러스터 설치

OpenShift Container Platform 4.9에서는 사용자 프로비저닝 인프라를 사용하여 Azure Stack Hub에 클러스터를 설치할 수 있도록 지원합니다.

배포 프로세스를 지원하기 위해 Red Hat에서 제공하는 ARM(Azure Resource Manager) 템플릿 샘플을 통합하거나 템플릿을 직접 만들 수 있습니다. 다른 방법을 통해 필요한 리소스를 자유롭게 만들 수도 있습니다. ARM 템플릿은 샘플 용으로만 제공됩니다.

자세한 내용은 [ARM 템플릿을 사용하여 Azure Stack Hub에 클러스터 설치](#) 를 참조하십시오.

#### 1.3.2.2. 클러스터를 업데이트하기 전에 시스템 상태 점검 일시 중지

업그레이드 프로세스 중에 클러스터의 노드를 일시적으로 사용할 수 없게 될 수 있습니다. 작업자 노드의 경우 시스템 상태 점검에서 이러한 노드를 비정상적으로 식별하고 재부팅할 수 있습니다. 이러한 노드를 재부팅하지 않도록 OpenShift Container Platform 4.9에는 `cluster.x-k8s.io/paused=""` 주석이 도입되어 클러스터를 업데이트하기 전에 **MachineHealthCheck** 리소스를 일시 중지할 수 있습니다.

자세한 내용은 [Pausing a MachineHealthCheck resource](#) 에서 참조하십시오.

#### 1.3.2.3. 머신 CIDR 내에서 Azure 서브넷의 크기 증가

Microsoft Azure용 OpenShift Container Platform 설치 프로그램은 이제 머신 CIDR 내에서 최대한 큰 서브넷을 생성합니다. 이를 통해 클러스터는 적절한 크기의 시스템 CIDR을 사용하여 클러스터의 노드 수를 수용할 수 있습니다.

#### 1.3.2.4. AWS 중국 리전 지원

OpenShift Container Platform 4.9에서는 AWS 중국 리전에 대한 지원이 도입되었습니다. 이제 **cn-north-1** (Beijing) 및 **cn-northwest-1** (Ningxia) 리전에 OpenShift Container Platform 클러스터를 설치하고 업데이트할 수 있습니다.

자세한 내용은 [AWS 중국 리전에 클러스터 설치](#) 를 참조하십시오.

#### 1.3.2.5. 베어 메탈 네트워크에서 가상 미디어를 사용하여 클러스터 확장

OpenShift Container Platform 4.9에서는 **baremetal** 네트워크에서 Virtual Media를 사용하여 **provisioning** 네트워크를 사용하여 배포한 설치 관리자 프로비저닝 클러스터를 확장할 수 있습니다. **ProvisioningNetwork** 구성 설정이 **Managed**로 설정된 경우 이 기능을 사용할 수 있습니다. 이 기능을 사용하려면 **provisioning** CR(사용자 정의 리소스)에서 **virtualœViaExternalNetwork** 구성 설정을 **true**로 설정해야 합니다. API VIP 주소를 사용하도록 머신 세트도 편집해야 합니다. 자세한 내용은 [베어 메탈 네트워크에 가상 미디어를 사용하여 배포 준비](#)에서 참조하십시오.

#### 1.3.2.6. OpenShift Container Platform 4.8에서 4.9로 업그레이드할 때 관리자 승인 필요

OpenShift Container Platform 4.9에서는 Kubernetes 1.22를 사용하며, 이에 **더 이상 사용되지 않는 많은 수의 v1beta1 API**가 제거되어 있습니다.



OpenShift Container Platform 4.8.14에서는 OpenShift Container Platform 4.8에서 4.9로 클러스터를 업그레이드하기 전에 관리자가 수동으로 승인을 제공해야 한다는 요구 사항을 도입했습니다. 이는 OpenShift Container Platform 4.9로 업그레이드한 후에도 문제를 방지하기 위한 것입니다. 여기에서 제거된 API는 클러스터에서 실행 중인 워크로드, 툴 또는 기타 구성 요소에서 여전히 사용되고 있습니다. 관리자는 제거될 모든 API에 대해 클러스터를 평가하고 영향을 받는 구성 요소를 마이그레이션하여 적절한 새 API 버전을 사용해야 합니다. 이 작업이 완료되면 관리자는 관리자 승인을 제공할 수 있습니다.

모든 OpenShift Container Platform 4.8 클러스터에는 OpenShift Container Platform 4.9로 업그레이드하기 전에 이 관리자가 승인해야 합니다.

자세한 내용은 [OpenShift Container Platform 4.9로 업데이트할 준비](#) 에서 참조하십시오.

### 1.3.2.7. PCI 패스스루를 사용하는 RHOSP 배포에 설치 지원

OpenShift Container Platform 4.9에서는 [PCI 통과](#)를 사용하는 RHOSP(Red Hat OpenStack Platform) 배포에 대한 설치를 지원합니다.

### 1.3.2.8. etcd 버전 3.4를 3.5로 업그레이드

OpenShift Container Platform 4.9에서는 etcd 3.5를 지원합니다. 클러스터를 업그레이드하기 전에 유효한 etcd 백업이 있는지 확인합니다. etcd 백업을 사용하면 업그레이드 실패가 발생할 경우 클러스터를 복원할 수 있습니다. OpenShift Container Platform 4.9에서는 etcd 업그레이드가 자동으로 수행됩니다. 클러스터의 버전 4.9로의 전환 상태에 따라 etcd 백업을 사용할 수 있습니다. 그러나 클러스터 업그레이드를 시작하기 전에 백업이 있는지 확인합니다.

### 1.3.2.9. 설치 관리자 프로비저닝 인프라를 사용하여 IBM Cloud에 클러스터 설치

OpenShift Container Platform 4.9에서는 설치 관리자 프로비저닝 인프라를 사용하여 IBM Cloud®에 클러스터를 설치할 수 있도록 지원합니다. 절차는 다음과 같은 차이점이 있지만 베어 메탈에서 설치 프로그램이 프로비저닝한 인프라와 거의 동일합니다.

- IBM Cloud에서 OpenShift Container Platform 4.9를 설치하려면 **provisioning** 네트워크, IPMI 및 PXE 부팅이 필요합니다. Red Hat은 IBM Cloud에서 Redfish 및 가상 미디어를 사용한 배포를 지원하지 않습니다.
- IBM Cloud에서 퍼블릭 및 프라이빗 VLAN을 생성하고 구성해야 합니다.
- IBM Cloud 노드는 설치 프로세스를 시작하기 전에 사용할 수 있어야 합니다. 따라서 먼저 IBM Cloud 노드를 만들어야 합니다.
- 프로비저너 노드를 준비해야 합니다.
- 퍼블릭 **baremetal** 네트워크에 DHCP 서버를 설치하고 구성해야 합니다.
- 각 노드가 IPMI를 사용하여 BMC를 가리키도록 **install-config.yaml** 파일을 구성하고 IPMI 권한 수준을 **OPERATOR**로 설정해야 합니다.

자세한 내용은 [IBM Cloud에 설치 프로그램 프로비저닝 클러스터 배포](#) 를 참조하십시오.

### 1.3.2.10. 설치 관리자 프로비저닝 클러스터에서 Fujitsu 하드웨어 지원 개선

OpenShift Container Platform 4.9에서는 Fujitsu 하드웨어에 설치 관리자 프로비저닝 클러스터를 배포하고 Fujitsu iRMC(Integrated Remote Management Controller)를 사용하여 작업자 노드에 대한 BIOS 구성 지원을 추가합니다. 자세한 내용은 [작업자 노드에 대한 BIOS 구성](#) 을 참조하십시오.

### 1.3.3. 웹 콘솔

#### 1.3.3.1. 노드 페이지에서 노드 로그에 액세스

이번 업데이트를 통해 관리자는 이제 **Node** 페이지에서 노드 로그에 액세스할 수 있습니다. 노드 로그를 검토하려면 **로그** 탭을 클릭하여 개별 로그 파일과 저널 로그 단위 간에 전환할 수 있습니다.

#### 1.3.3.2. 노드 유형별 클러스터 사용률 분석

이제 클러스터 대시보드의 **클러스터 사용률** 카드에서 노드 유형별로 필터링할 수 있습니다. 생성 시 추가 노드 유형이 목록에 표시됩니다.

#### 1.3.3.3. 사용자 환경 설정

이번 업데이트에서는 기본 프로젝트, 화면 및 토폴로지 뷰와 같은 설정을 사용자 지정하기 위해 **사용자 환경 설정** 페이지가 추가됩니다.

#### 1.3.3.4. 프로젝트 목록에서 기본 프로젝트 숨기기

이번 업데이트를 통해 웹 콘솔 마스트 헤드의 **프로젝트** 드롭다운 메뉴에서 **default projects**를 숨길 수 있습니다. 검색 및 필터링 전에 **default projects**를 표시하도록 전환할 수 있습니다.

#### 1.3.3.5. 웹 콘솔에서 사용자 환경 설정 추가

이번 업데이트를 통해 이제 웹 콘솔에 사용자 기본 설정을 추가할 수 있습니다. 사용자는 기본 화면, 프로젝트, 토폴로지 및 기타 기본 설정을 선택할 수 있습니다.

#### 1.3.3.6. 개발자 화면

- 배포를 추가로 사용자 지정하기 위해 Git 리포지토리를 통해 devfile, Dockerfile 또는 빌더 이미지를 추가로 가져올 수 있습니다. 파일 가져오기 유형을 편집하고 다른 전략을 선택하여 파일을 가져올 수도 있습니다.
- 이제 개발자 콘솔에서 **파이프라인 빌더**의 업데이트된 사용자 인터페이스를 사용하여 **작업 추가** 및 **빠른 검색**을 통해 파이프라인에 작업을 추가할 수 있습니다. 이러한 개선된 환경을 통해 사용자는 **Tekton Hub**에서 작업을 추가할 수 있습니다.
- 빌드 구성을 편집하려면 **개발자 화면**의 **빌드 보기**에서 **빌드 구성 편집** 옵션을 사용합니다. 사용자는 **양식 보기** 및 **YAML 보기**를 사용하여 빌드 구성을 편집할 수 있습니다.
- 토폴로지 **그래프 보기**의 컨텍스트 메뉴를 사용하여 서비스를 추가하거나 operator 지원 서비스와의 연결을 프로젝트에 생성할 수 있습니다.
- 토폴로지 **그래프 보기**의 컨텍스트 메뉴에서 **+추가** 작업을 사용하여 서비스를 추가하거나 애플리케이션 그룹에서 서비스를 제거할 수 있습니다.
- 이제 OpenShift Pipelines Operator에서 활성화한 **Pipelines Repository** 목록 보기에서 **코드로서의 파이프라인**에 대한 초기 지원을 사용할 수 있습니다.
- 토폴로지의 **모니터링** 페이지에 있는 **애플리케이션 모니터링** 섹션에 대한 사용성이 개선되었습니다.

### 1.3.4. IBM Z 및 LinuxONE

이번 릴리스에서 IBM Z 및 LinuxONE은 이제 OpenShift Container Platform 4.9과 호환됩니다. z/VM 또는 RHEL KVM을 사용하여 설치할 수 있습니다. 설치 지침은 다음 설명서를 참조하십시오.

- [IBM Z 및 LinuxONE에 z/VM으로 클러스터 설치](#)
- [네트워크가 제한된 환경에서 IBM Z 및 LinuxONE에 z/VM으로 클러스터 설치](#)
- [IBM Z 및 LinuxONE에 RHEL KVM으로 클러스터 설치](#)
- [네트워크가 제한된 환경에서 IBM Z 및 LinuxONE에 RHEL KVM으로 클러스터 설치](#)

### 주요 개선 사항

OpenShift Container Platform 4.9의 IBM Z 및 LinuxONE에서 지원되는 새로운 기능은 다음과 같습니다.

- Helm
- 다중 네트워크 인터페이스 지원
- Service Binding Operator

### 지원되는 기능

다음 기능은 IBM Z 및 LinuxONE에서도 지원됩니다.

- 현재 다음 Operator가 지원됩니다.
  - Cluster Logging Operator
  - NFD Operator
  - OpenShift Elasticsearch Operator
  - Local Storage Operator
  - Service Binding Operator
- etcd에 저장된 데이터 암호화
- 다중 경로
- iSCSI를 사용하는 영구 스토리지
- 로컬 볼륨을 사용하는 영구저장장치(Local Storage Operator)
- hostPath를 사용하는 영구 스토리지
- 파이버 채널을 사용하는 영구 스토리지
- Raw Block을 사용하는 영구 스토리지
- OVN-Kubernetes
- 3-노드 클러스터 지원
- SCSI 디스크의 z/VM Emulated FBA 장치
- 4K FCP 블록 장치

이러한 기능은 IBM Z 및 LinuxONE의 OpenShift Container Platform 4.9에서만 사용할 수 있습니다.

- FICON의 ECKD 스토리지에 연결된 가상 머신에 대해 IBM Z 및 LinuxONE에서 HyperPAV 활성화

### 제한 사항

IBM Z 및 LinuxONE의 OpenShift Container Platform에 대한 다음 제한 사항을 참고하십시오.

- 다음 OpenShift Container Platform 기술 프리뷰 기능은 지원되지 않습니다.
  - PTP(Precision Time Protocol) 하드웨어
- 다음 OpenShift Container Platform 기능은 지원되지 않습니다:
  - 시스템 상태 점검으로 손상된 시스템 자동 복구
  - CRC(CodeReady Containers)
  - 노드에서 오버 커밋 제어 및 컨테이너 밀도 관리
  - CSI 볼륨 복제
  - CSI 볼륨 스냅샷
  - FIPS 암호화
  - Multus CNI 플러그인
  - NVMe
  - OpenShift Metering
  - OpenShift Virtualization
  - OpenShift Container Platform 배포 시 Tang 모드 디스크 암호화
- 작업자 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행해야 합니다.
- 영구 공유 스토리지는 NFS 또는 기타 지원되는 스토리지 프로토콜을 사용하여 프로비저닝해야 합니다.
- 영구 비공유 스토리지는 iSCSI, FC와 같은 로컬 스토리지를 사용하거나 DASD, FCP 또는 EDEV/FBA 함께 LSO를 사용하여 프로비저닝해야 합니다.

### 1.3.5. IBM Power Systems

이 릴리스에서 IBM Power Systems는 이제 OpenShift Container Platform 4.9과 호환됩니다. 설치 지침은 다음 설명서를 참조하십시오.

- [IBM Power Systems에 클러스터 설치](#)
- [네트워크가 제한된 환경에서 IBM Power System에 클러스터 설치](#)

### 주요 개선 사항

OpenShift Container Platform 4.9의 IBM Power Systems에서 다음과 같은 새로운 기능이 지원됩니다.

- Helm
- Power10 지원
- 다중 네트워크 인터페이스 지원

- Service Binding Operator

### 지원되는 기능

다음 기능은 IBM Power Systems에서도 지원됩니다.

- 현재 다음 Operator가 지원됩니다.
  - Cluster Logging Operator
  - NFD Operator
  - OpenShift Elasticsearch Operator
  - Local Storage Operator
  - SR-IOV 네트워크 Operator
  - Service Binding Operator
- 다중 경로
- iSCSI를 사용하는 영구 스토리지
- 로컬 볼륨을 사용하는 영구저장장치(Local Storage Operator)
- hostPath를 사용하는 영구 스토리지
- 파이버 채널을 사용하는 영구 스토리지
- Raw Block을 사용하는 영구 스토리지
- OVN-Kubernetes
- 4K 디스크 지원
- NVMe
- etcd에 저장된 데이터 암호화
- 3-노드 클러스터 지원
- Multus SR-IOV

### 제한 사항

IBM Power Systems의 OpenShift Container Platform에 대한 다음 제한 사항을 참고하십시오.

- 다음 OpenShift Container Platform 기술 프리뷰 기능은 지원되지 않습니다.
  - PTP(Precision Time Protocol) 하드웨어
- 다음 OpenShift Container Platform 기능은 지원되지 않습니다:
  - 시스템 상태 점검으로 손상된 시스템 자동 복구
  - CRC(CodeReady Containers)
  - 노드에서 오버 커밋 제어 및 컨테이너 밀도 관리
  - FIPS 암호화

- OpenShift Metering
- OpenShift Virtualization
- OpenShift Container Platform 배포 시 Tang 모드 디스크 암호화
- 작업자 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행해야 합니다.
- 영구 스토리지는 로컬 볼륨, NFS(Network File System), 또는 CSI(Container Storage Interface)를 사용하는 Filesystem 유형이어야 합니다.

### 1.3.6. 보안 및 컴플라이언스

#### 1.3.6.1. 사용자 정의 규칙을 사용하여 감사 로그 정책 구성

이제 OpenShift Container Platform의 감사 로깅 수준을 보다 세밀하게 제어할 수 있습니다. 사용자 지정 규칙을 사용하여 다른 그룹에 대해 다른 감사 정책 프로필(**Default**, **WriteRequestBodies**, **AllRequestBodies**, **None**)을 지정할 수 있습니다.

자세한 내용은 [사용자 정의 규칙을 사용하여 감사 로그 정책 구성](#) 을 참조하십시오.

#### 1.3.6.2. 감사 로깅 비활성화

이제 **None** 감사 정책 프로필을 사용하여 OpenShift Container Platform의 감사 로깅을 비활성화할 수 있습니다.



#### 주의

문제를 해결할 때 도움이 될 수 있는 데이터를 기록하지 않을 경우의 위험을 완전히 인식하지 않는 한 감사 기록을 비활성화하는 것이 좋습니다. 감사 로깅을 비활성화하고 지원 상황이 발생하는 경우 적절하게 해결하려면 감사 로깅을 활성화하고 문제를 재현해야 할 수 있습니다.

자세한 내용은 [감사 로깅 비활성화](#) 를 참조하십시오.

#### 1.3.6.3. OAuth 서버 URL 사용자 정의

이제 내부 OAuth 서버의 URL을 사용자 지정할 수 있습니다. 자세한 내용은 [내부 OAuth 서버 URL 사용자 지정](#) 을 참조하십시오.

#### 1.3.6.4. NBDE (Network-Bound Disk Encryption)

OpenShift Container Platform 4.9에서는 NBDE 구성 시스템을 지속적으로 유지 관리하기 위한 새로운 절차를 제공합니다. NBDE를 사용하면 시스템을 다시 시작할 때 암호를 수동으로 입력하지 않고도 실제 및 가상 시스템에서 하드 드라이브의 root 볼륨을 암호화할 수 있습니다. 자세한 내용은 [디스크 암호화 기술 정보](#) 를 참조하십시오.

### 1.3.7. etcd

### 1.3.7.1. etcd 인증서 자동 교체

OpenShift Container Platform 4.9에서는 etcd 인증서가 자동으로 교체되며 시스템에서 관리됩니다.

### 1.3.7.2. API 서버의 추가 TLS 보안 프로파일 설정

이제 Kubernetes API 서버 TLS 보안 프로파일 설정도 etcd에서 지원됩니다.

## 1.3.8. 네트워킹

### 1.3.8.1. linuxptp 서비스 개선

OpenShift Container Platform 4.9에서는 PTP에 다음 업데이트가 도입되었습니다.

- 새 **ptp4lConf** 필드
- **linuxptp** 서비스를 경계 클록으로 구성하는 새로운 옵션

자세한 내용은 [linuxptp 서비스를 경계 클록으로 구성](#) 을 참조하십시오.

### 1.3.8.2. PTP 빠른 이벤트 알림 프레임워크를 사용하여 PTP 빠른 이벤트 모니터링

베어 메탈 클러스터에서 PTP 이벤트에 대한 빠른 이벤트 알림을 사용할 수 있습니다. PTP Operator는 구성된 모든 PTP 가능 네트워크 인터페이스에 대한 이벤트 알림을 생성합니다. 이벤트는 동일한 노드에서 실행되는 애플리케이션에 REST API를 통해 사용할 수 있습니다. 빠른 이벤트 알림은 AMQ Interconnect Operator에서 제공하는 AMQP(Advanced Message Queuing Protocol) 메시지 버스에서 전송합니다.

자세한 내용은 [PTP 및 클럭 동기화 오류 이벤트 정보](#) 를 참조하십시오.

### 1.3.8.3. 노드 간에 OVN-Kubernetes 클러스터 네트워크 공급자 송신 IP 기능의 균형 조정

OVN-Kubernetes의 송신 IP 기능은 해당 네임스페이스에 여러 송신 IP 주소가 할당된 경우 지정된 네임스페이스의 노드 간에 네트워크 트래픽을 거의 균등하게 조정합니다. 각 IP 주소는 다른 노드에 있어야 합니다. 자세한 내용은 OVN-Kubernetes [프로젝트의 송신 IP 구성](#) 을 참조하십시오.

### 1.3.8.4. SR-IOV 컨테이너화된 DPDK(Data Plane Development Kit)는 GA로 제공

OpenShift Container Platform 4.9에서 DPDK(컨테이너 데이터 플레인 개발 키트)가 GA로 제공됩니다. 자세한 내용은 [DPDK 및 RDMA 모드와 함께 VF\(가상 기능\) 사용](#) 을 참조하십시오.

### 1.3.8.5. Fast Datapath DPDK 애플리케이션과 함께 vhost-net을 사용하기 위한 SR-IOV 지원

SR-IOV는 Intel 및 Mellanox NIC의 Fast Datapath DPDK 애플리케이션과 함께 사용할 수 있도록 vhost-net을 지원합니다. **SriovNetworkNodePolicy** 리소스를 구성하여 이 기능을 활성화할 수 있습니다. 자세한 내용은 [SR-IOV 네트워크 노드 구성 오브젝트](#) 를 참조하십시오.

### 1.3.8.6. 단일 노드 클러스터에 대한 SR-IOV 지원

단일 노드 클러스터는 SR-IOV 하드웨어 및 SR-IOV Network Operator를 지원합니다. SR-IOV 네트워크 장치를 구성하면 단일 노드가 재부팅되고 Operator의 **disableDrain** 필드를 구성해야 합니다. 자세한 내용은 [SR-IOV Network Operator 구성](#) 을 참조하십시오.

### 1.3.8.7. SR-IOV에서 지원되는 하드웨어

OpenShift Container Platform 4.9에서는 Broadcom 및 Intel 하드웨어를 추가로 지원합니다.

- Broadcom BCM57414 및 BCM57508

자세한 내용은 [지원되는 장치를](#) 참조하십시오.

### 1.3.8.8. MetalLB 로드 밸런서

이 릴리스에서는 MetalLB Operator가 도입되었습니다. MetalLB Operator를 설치하고 구성된 후 MetalLB를 배포하여 베어 메탈 클러스터에서 서비스에 대한 기본 로드 밸런서 구현을 제공할 수 있습니다. 베어 메탈과 같은 기타 온프레미스 인프라도 유용할 수 있습니다.

Operator에는 사용자 정의 리소스 **AddressPool**이 도입되었습니다. MetalLB에서 서비스에 할당할 수 있는 IP 주소 범위를 사용하여 주소 풀을 구성합니다. **LoadBalancer** 유형의 서비스를 추가하면 MetalLB에서 풀의 IP 주소를 할당합니다.

이번 릴리스에서는 Red Hat은 계층 2 모드에서만 MetalLB 사용 방법을 지원합니다.

자세한 내용은 [MetalLB 및 MetalLB Operator 정보](#)를 참조하십시오.

### 1.3.8.9. CNI VRF 플러그인 사용 가능

CNI VRF 플러그인은 이전에 OpenShift Container Platform 4.7에서 기술 프리뷰 기능으로 소개되었으며 현재 OpenShift Container Platform 4.9에서 일반적으로 사용할 수 있습니다.

자세한 내용은 [VRF에 보조 네트워크 할당](#)을 참조하십시오.

### 1.3.8.10. Ingress 컨트롤러 시간 제한 구성 매개변수

이 릴리스에서는 Ingress 컨트롤러 **tuningOptions** 매개변수에 대한 6개의 시간 제한 구성이 도입되었습니다.

- **ClientTimeout**은 클라이언트 응답을 기다리는 동안 연결이 열린 상태로 유지되는 시간을 지정합니다.
- **serverFinTimeout**은 연결을 종료하는 클라이언트에 대한 서버 응답을 기다리는 동안 연결이 열린 상태로 유지되는 시간을 지정합니다.
- **ServerTimeout**은 서버 응답을 기다리는 동안 연결이 열린 상태로 유지되는 시간을 지정합니다.
- **clientFinTimeout**은 연결을 닫는 서버에 대한 클라이언트 응답을 기다리는 동안 연결이 열린 상태로 유지되는 시간을 지정합니다.
- **tlsInspectDelay**는 라우터에서 일치하는 경로를 찾기 위해 데이터를 보유할 수 있는 시간을 지정합니다.
- **tunnelTimeout**은 WebSocket 연결을 포함하여 터널이 유향 상태인 동안 터널 연결이 열려 있는 시간을 지정합니다.

자세한 내용은 [Ingress 컨트롤러 구성 매개변수](#)를 참조하십시오.

### 1.3.8.11. 상호 TLS 인증

**spec.clientTLS**를 설정하여 상호 TLS(mTLS) 인증을 사용하도록 Ingress 컨트롤러를 구성할 수 있습니다. **clientTLS** 필드에서는 클라이언트 인증서를 확인하기 위한 Ingress 컨트롤러의 구성을 지정합니다.



자세한 내용은 [상호 TLS 인증 구성](#) 을 참조하십시오.

### 1.3.8.12. HAProxy 오류 코드 응답 페이지 사용자 정의

클러스터 관리자는 503, 404 또는 두 오류 페이지의 사용자 정의 HTTP 오류 코드 응답 페이지를 지정할 수 있습니다.

자세한 내용은 [HAProxy 오류 코드 응답 페이지 사용자 지정](#) 을 참조하십시오.

### 1.3.8.13. provisioningNetworkInterface 구성 설정은 선택 사항임

OpenShift Container Platform 4.9에서 설치 관리자 프로비저닝 클러스터에 대한 **provisioningNetworkInterface** 구성 설정은 선택 사항입니다. **provisioningNetworkInterface** 구성 설정은 **provisioning** 네트워크에 사용되는 NIC 이름을 식별합니다. OpenShift Container Platform 4.9에서는 Ironic에서 **provisioning** 네트워크에 연결된 NIC의 IP 주소를 식별하고 바인딩할 수 있도록 **install-config.yml** 파일에 **bootMACAddress** 구성 설정을 지정할 수도 있습니다. provisioning 사용자 정의 리소스에서 **bootMACAddress** 구성 설정을 대신 사용하도록 **provisioningInterface** 구성 설정을 생략할 수도 있습니다.

### 1.3.8.14. DNS Operator managementState

OpenShift Container Platform 4.9에서 DNS Operator **managementState**를 변경할 수 있습니다. DNS Operator의 **managementState**는 기본적으로 **Managed**로 설정되어 있으며 이는 DNS Operator가 리소스를 적극적으로 관리하고 있음을 의미합니다. **Unmanaged**로 변경할 수 있습니다. 이는 DNS Operator가 해당 리소스를 관리하지 않음을 의미합니다.

다음은 DNS Operator **managementState**를 변경하는 사용 사례입니다.

- 사용자가 개발자이며 구성 변경을 테스트하여 CoreDNS의 문제가 해결되었는지 확인하려고 합니다. **managementState**를 **Unmanaged**로 설정하여 DNS Operator가 변경 사항을 덮어쓰지 않도록 할 수 있습니다.
- 클러스터 관리자이며 CoreDNS 관련 문제를 보고했지만 문제가 해결될 때까지 해결 방법을 적용해야 합니다. DNS Operator의 **managementState** 필드를 **Unmanaged**로 설정하여 해결 방법을 적용할 수 있습니다.

자세한 내용은 [DNS Operator managementState 변경](#)에서 참조하십시오.

### 1.3.8.15. RHOSP에서 클러스터의 클라우드 공급자 옵션으로 로드 밸런서 구성

RHOSP에서 실행되는 클러스터의 경우 로드 밸런싱을 위해 Octavia를 클라우드 공급자 옵션으로 구성할 수 있습니다.

자세한 내용은 [클라우드 공급자 옵션 설정](#) 을 참조하십시오.

### 1.3.8.16. TLS 1.3 및 Modern 프로파일에 대한 지원 추가

이번 릴리스에서는 HAProxy의 TLS 1.3 및 **Modern** 프로파일에 대한 Ingress 컨트롤러 지원이 추가되었습니다.

자세한 내용은 [Ingress 컨트롤러 TLS 보안 프로필](#) 을 참조하십시오.

### 1.3.8.17. HTTP Strict Transport Security 요구사항을 위한 글로벌 승인 플러그인

클러스터 관리자는 **route.openshift.io/RequiredRouteAnnotations** 라는 라우터에 대한 승인 플러그인

을 추가하여 도메인별로 HTTP Strict Transport Security(HSTS) 확인을 구성할 수 있습니다. 클러스터 관리자가 HSTS를 적용하도록 이 플러그인을 구성하는 경우 클러스터 Ingress 구성의 글로벌 설정에 대해 확인된 규정 준수 HSTS 정책( [ingresses.config.openshift.io/cluster](https://ingresses.config.openshift.io/cluster) )을 사용하여 새로 생성된 경로를 구성해야 합니다.

자세한 내용은 [HTTP Strict Transport Security](#) 를 참조하십시오.

### 1.3.8.18. Ingress 빈 요청 정책

OpenShift Container Platform 4.9에서는 **logEmptyRequests** 및 **HTTPEmptyRequestsPolicy** 필드를 설정하여 빈 요청을 기록하거나 무시하도록 Ingress 컨트롤러를 구성할 수 있습니다.

자세한 내용은 [Ingress 컨트롤러 구성 매개변수](#) 를 참조하십시오.

### 1.3.8.19. 웹 콘솔에서 네트워크 정책 만들기

**cluster-admin** 역할을 사용하여 웹 콘솔에 로그인하면 이제 콘솔의 양식에서 클러스터의 모든 네임스페이스에 새 네트워크 정책을 생성할 수 있습니다. 이전에는 YAML에서 직접 수행할 수 있었습니다.

## 1.3.9. 스토리지

### 1.3.9.1. AWS EBS CSI 드라이버 Operator를 사용하는 영구 스토리지 사용 가능

OpenShift Container Platform은 AWS EBS(Elastic Block Store)의 CSI(Container Storage Interface) 드라이버를 사용하여 PV(영구 볼륨)를 프로비저닝할 수 있습니다. 이 기능은 이전에 OpenShift Container Platform 4.5에서 기술 프리뷰 기능으로 소개되었으며 현재 OpenShift Container Platform 4.9에서 일반적으로 사용 가능하며 활성화되어 있습니다.

자세한 내용은 [AWS EBS CSI Driver Operator](#) 를 참조하십시오.

### 1.3.9.2. Azure Stack Hub CSI Driver Operator를 사용한 영구 스토리지 (일반 사용 가능)

OpenShift Container Platform은 Azure Stack Hub 스토리지용 CSI 드라이버를 사용하여 PV를 프로비저닝할 수 있습니다. Azure Stack 포트폴리오의 일부인 Azure Stack Hub를 사용하면 온프레미스 환경에서 애플리케이션을 실행하고 데이터 센터에 Azure 서비스를 제공할 수 있습니다. 이 드라이버를 관리하는 Azure Stack Hub CSI Driver Operator는 4.9의 경우 새로 사용할 수 있으며 일반적으로 사용할 수 있습니다.

자세한 내용은 [Azure Stack Hub CSI Driver Operator](#) 를 참조하십시오.

### 1.3.9.3. AWS EFS CSI Driver Operator를 사용한 영구 스토리지 (기술 프리뷰)

OpenShift Container Platform은 AWS EFS(Elastic File Service)용 CSI 드라이버를 사용하여 PV를 프로비저닝할 수 있습니다. 이 드라이버를 관리하는 AWS EFS CSI Driver Operator는 기술 프리뷰로 사용할 수 있습니다.

자세한 내용은 [AWS EFS CSI Driver Operator](#) 에서 참조하십시오.

### 1.3.9.4. 자동 CSI 마이그레이션에서 GCE 지원 (기술 프리뷰)

OpenShift Container Platform 4.8부터 동등한 CSI 드라이버로 인트리 볼륨 플러그인의 자동 마이그레이션을 기술 프리뷰 기능으로 사용할 수 있게 되었습니다. 이 기능은 이제 GCE PD(Google Compute Engine Persistent Disk) in-tree 플러그인에서 GCP(Google Cloud Platform) 영구 디스크 CSI 드라이버로 자동 마이그레이션을 지원합니다.

자세한 내용은 [CSI 자동 마이그레이션](#) 을 참조하십시오.

### 1.3.9.5. 자동 CSI 마이그레이션에서 Azure Disk 지원 (기술 프리뷰)

OpenShift Container Platform 4.8부터 동등한 CSI 드라이버로 인트리 볼륨 플러그인의 자동 마이그레이션을 기술 프리뷰 기능으로 사용할 수 있게 되었습니다. 이 기능은 Azure Disk in-tree 플러그인에서 Azure Disk CSI 드라이버로 자동 마이그레이션을 지원합니다.

자세한 내용은 [CSI 자동 마이그레이션](#) 을 참조하십시오.

### 1.3.9.6. VMware vSphere CSI Driver Operator가 스토리지 정책을 자동으로 생성 (기술 프리뷰)

vSphere CSI Operator Driver 스토리지 클래스에서 vSphere의 스토리지 정책을 사용합니다. OpenShift Container Platform은 클라우드 설정에 구성된 데이터 저장소를 대상으로 하는 스토리지 정책을 자동으로 생성합니다.

자세한 내용은 [VMWare vSphere CSI Driver Operator](#) 에서 참조하십시오.

### 1.3.9.7. Local Storage Operator에 제공되는 새 지표

OpenShift Container Platform 4.9에서는 Local Storage Operator에 대한 다음과 같은 새로운 지표를 제공합니다.

- **Iso\_discovery\_disk\_count:** 각 노드에서 발견된 총 장치 수
- **Iso\_lvset\_provisioned\_PV\_count:** LocalVolumeSet 개체에서 생성한 총 PV 수
- **Iso\_lvset\_unmatched\_disk\_count:** 기준 불일치로 인해 Local Storage Operator가 프로비저닝을 위해 선택하지 않은 총 디스크 수
- **Iso\_lvset\_orphaned\_symlink\_count:** LocalVolumeSet 개체 기준과 더 이상 일치하지 않는 PV가 있는 장치 수
- **Iso\_lv\_orphaned\_symlink\_count:** LocalVolume 오브젝트 기준과 더 이상 일치하지 않는 PV가 있는 장치 수
- **Iso\_lv\_provisioned\_PV\_count:** LocalVolume의 프로비저닝된 총 PV 수

자세한 내용은 [로컬 볼륨을 사용한 영구 저장 장치](#) 를 참조하십시오.

### 1.3.9.8. ovirt CSI 드라이버 크기 조정 기능 사용 가능

OpenShift Container Platform 4.9에서는 oVirt CSI Driver에 크기 조정 기능을 추가하여 사용자가 기존 PVC(영구 볼륨 클레임)의 크기를 늘릴 수 있습니다. 이 기능을 사용하기 전에는 사용자가 크기가 증가된 새 PVC를 만들고 모든 콘텐츠를 이전 PV(영구 볼륨)에서 새 PV로 이동해야 했기 때문에 데이터가 손실될 수 있었습니다. 이제 사용자가 기존 PVC를 편집할 수 있으며 oVirt CSI 드라이버는 기본 oVirt 디스크의 크기를 조정합니다.

## 1.3.10. Registry

### 1.3.10.1. 이미지 레지스트리는 Azure Stack Hub 설치 시 Azure Blob 스토리지를 사용

OpenShift Container Platform 4.9에서 통합 이미지 레지스트리는 사용자 프로비저닝 인프라를 사용하여 Microsoft Azure Stack Hub에 설치된 클러스터에 Azure Blob Storage를 사용합니다.

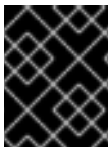
자세한 내용은 [ARM 템플릿을 사용하여 Azure Stack Hub에 클러스터 설치](#) 를 참조하십시오.

### 1.3.11. Operator 라이프사이클

다음과 같은 새로운 기능 및 개선 사항은 OLM(Operator Lifecycle Manager)을 사용하여 Operator를 실행하는 것과 관련이 있습니다.

#### 1.3.11.1. Operator Lifecycle Manager가 Kubernetes 1.22로 업그레이드

OpenShift Container Platform 4.9부터 OLM(Operator Lifecycle Manager)은 Kubernetes 1.22를 지원합니다. 결과적으로 상당한 수의 **v1beta1 API가 제거되고 v1로 업데이트**되었습니다. 제거된 **v1beta1 API**에 의존하는 Operator는 OpenShift Container Platform 4.9에서 실행되지 않습니다. 클러스터 관리자는 클러스터를 OpenShift Container Platform 4.9로 업그레이드하기 전에 **설치된 Operator**를 **최신 채널**로 업그레이드해야 합니다.



중요

Kubernetes 1.22에는 **CustomResourceDefinition API**의 **v1**에 대해 **몇 가지 주요 변경 사항**이 추가되었습니다.

#### 1.3.11.2. 파일 기반 카탈로그

파일 기반 카탈로그는 OLM(Operator Lifecycle Manager) 카탈로그 형식의 최신 버전입니다. 형식은 일반 텍스트 기반(JSON 또는 YAML) 및 이전 버전의 선언적 구성 진화로 이제 더 이상 사용되지 않는 **SQLite 데이터베이스 형식**이며 이전 버전과 완전히 호환됩니다. 이 형식의 목표는 Operator 카탈로그 편집, 구성 가능성 및 확장성을 활성화하는 것입니다.

파일 기반 카탈로그 사양에 대한 자세한 내용은 [Operator Framework 패키지 형식](#)을 참조하십시오.

**opm** CLI를 사용하여 파일 기반 카탈로그 생성에 대한 지침은 [사용자 정의 카탈로그 관리](#)를 참조하십시오.

#### 1.3.11.3. 단일 노드 OpenShift에 대한 Operator Lifecycle Manager 지원

이제 OLM(Operator Lifecycle Manager)을 Single Node OpenShift(SNO) 클러스터에서 사용할 수 있으므로 셀프 서비스 Operator 설치가 가능합니다.

#### 1.3.11.4. 클러스터 관리자의 오류 보고 기능 향상

관리자는 이러한 문제를 성공적으로 디버깅하기 위해 다양한 하위 수준 API 또는 OLM(Operator Lifecycle Manager) Pod 로그 간의 상호 작용 프로세스를 이해할 필요가 없기 때문에 OpenShift Container Platform 4.9에서는 OLM의 다음과 같은 개선 사항이 도입되어 관리자에게 보다 이해하기 쉬운 오류 보고 및 메시지를 제공합니다.

##### 1.3.11.4.1. Operator 그룹 상태 조건 업데이트

이전 버전에서는 네임스페이스에 여러 Operator 그룹이 포함되어 있거나 서비스 계정을 찾을 수 없는 경우 Operator 그룹의 상태가 오류를 보고하지 않았습니다. 이번 개선된 기능을 통해 이러한 시나리오에서 Operator 그룹의 상태 조건을 업데이트하여 오류를 보고합니다.

##### 1.3.11.4.2. 설치 계획 실패 이유 표시

이번 릴리스 이전에는 설치 계획이 실패한 경우 서브스크립션 조건이 실패한 이유를 설명하지 않았습니다. 이제 설치 계획이 실패하면 서브스크립션 상태 조건에서 실패 이유를 나타냅니다.

### 1.3.11.4.3. 서브스크립션 상태에 대한 해결 실패 오류 표시

종속성 확인은 네임스페이스의 모든 구성 요소를 단일 단위로 처리하므로 해결이 실패하면 네임스페이스의 모든 서브스크립션에 오류가 표시됩니다.

### 1.3.11.5. 사용자 정의 카탈로그 소스의 이미지 템플릿

클러스터 업그레이드를 방지하기 위해 Operator 설치가 지원되지 않거나 지속적인 업데이트 경로가 없는 경우 클러스터 업그레이드의 일부로 Operator 카탈로그의 인덱스 이미지 버전을 자동으로 변경할 수 있습니다.

**olm.catalogImageTemplate** 주석을 카탈로그 이미지 이름으로 설정하고 이미지 태그에 대한 템플릿을 구성할 때 Kubernetes 클러스터 버전 변수 중 하나 이상을 사용합니다.

자세한 내용은 [사용자 정의 카탈로그 소스에 대한 이미지 템플릿](#) 을 참조하십시오.

## 1.3.12. Operator 개발

다음과 같은 새로운 기능 및 개선 사항은 Operator SDK를 사용하는 Operator 개발과 관련이 있습니다.

### 1.3.12.1. 고가용성 또는 단일 노드 클러스터 감지 및 지원

OpenShift Container Platform 클러스터는 여러 노드를 사용하는 HA(고가용성) 모드로 구성하거나 단일 노드를 사용하는 비-HA 모드로 구성할 수 있습니다. 단일 노드 클러스터(SNO(Single Node OpenShift))라고 고도 하는 단일 노드 클러스터는 보다 보수적인 리소스 제약 조건이 있을 수 있습니다. 따라서 단일 노드 클러스터에 설치된 Operator가 적절하게 조정되고 제대로 실행되는 것이 중요합니다.

OpenShift Container Platform에 제공된 클러스터 고가용성 모드 API에 액세스하여 Operator 작성자는 Operator SDK를 사용하여 Operator가 HA 또는 비HA 모드 중 하나의 클러스터 인프라 토폴로지를 감지할 수 있습니다. 감지된 클러스터 토폴로지를 사용하여 Operator 및 관리하는 Operand 또는 워크로드 모두에 대해 리소스 요구 사항을 토폴로지에 가장 적합한 프로파일로 자동 전환하는 사용자 정의 Operator 논리를 개발할 수 있습니다.

자세한 내용은 [고가용성 또는 단일 노드 클러스터 감지 및 지원](#) 을 참조하십시오.

### 1.3.12.2. 네트워크 프록시에 대한 Operator 지원

Operator 작성자는 이제 네트워크 프록시를 지원하는 Operator를 개발할 수 있습니다. 프록시가 지원되는 Operator는 환경 변수에 대한 Operator 배포를 검사하고 필요한 Operand에 변수를 전달합니다. 클러스터 관리자는 OLM(Operator Lifecycle Manager)에서 처리하는 환경 변수에 대한 프록시 지원을 구성합니다. 자세한 내용은 [Go](#), [Ansible](#) 및 [Helm](#) 을 사용하여 Operator 개발을 위한 Operator SDK 튜토리얼을 참조하십시오.

### 1.3.12.3. Kubernetes 1.22에서 제거된 API의 번들 매니페스트 검증

이제 **bundle validate** 하위 명령으로 Operator Framework 테스트 제품군을 사용하여 Kubernetes 1.22에서 제거된 API에 대한 번들 매니페스트를 확인할 수 있습니다.

예를 들면 다음과 같습니다.

```
$ operator-sdk bundle validate .<bundle_dir_or_image> \
  --select-optional suite=operatorframework \
  --optional-values=k8s-version=1.22
```

번들 매니페스트에 Kubernetes 1.22에서 제거된 API가 포함된 경우 명령에서 경고 메시지를 표시합니다. 경고 메시지는 마이그레이션해야 하는 API와 Kubernetes API 마이그레이션 가이드에 대한 링크가 표시됩니다.

자세한 내용은 [Kubernetes 1.22에서 제거된 베타 API 표](#) 및 [Operator SDK CLI 참조](#)에서 확인하십시오.

### 1.3.13. 빌드

빌드에 OpenShift Container Platform을 사용하는 개발자는 이 업데이트와 함께 다음과 같은 새 기능을 사용할 수 있습니다.

- 빌드 볼륨을 마운트하여 출력 컨테이너 이미지에 유지하려고 하지 않는 정보에 대한 액세스 권한을 실행 중인 빌드에 부여할 수 있습니다. 빌드 볼륨은 빌드 환경 또는 구성에만 필요한 리포지토리 인증 정보와 같은 중요한 정보를 제공할 수 있습니다. 빌드 볼륨은 출력 컨테이너 이미지에 데이터가 지속될 수 있는 빌드 입력과 다릅니다.
- BuildConfig 상태에 기록된 정보를 기반으로 빌드를 트리거하도록 이미지 변경을 구성할 수 있습니다. 이렇게 하면 GitOps 워크플로우에서 빌드와 함께 **ImageChange** 트리거를 사용할 수 있습니다.

### 1.3.14. 이미지

#### 1.3.14.1. 레지스트리 소스로 와일드카드 도메인 사용

이 릴리스에서는 이미지 레지스트리 설정에서 와일드카드 도메인을 레지스트리 소스로 사용할 수 있도록 지원합니다. 와일드카드 도메인(예: **\*.example.com**)을 사용하면 각각 수동으로 입력하지 않고도 여러 하위 도메인에서 이미지를 푸시하고 가져오도록 클러스터를 설정할 수 있습니다. 자세한 내용은 [이미지 컨트롤러 구성 매개 변수](#)를 참조하십시오.

### 1.3.15. 머신 API

#### 1.3.15.1. 컴퓨팅 머신에서 RHEL (Red Hat Enterprise Linux) 8 지원

OpenShift Container Platform 4.9부터 컴퓨팅 머신에 RHEL (Red Hat Enterprise Linux) 8.4를 사용할 수 있습니다. 이전에는 컴퓨팅 머신에서 RHEL 8이 지원되지 않았습니다.

RHEL 7 컴퓨팅 머신을 RHEL 8로 업그레이드할 수 없습니다. 새 RHEL 8 호스트를 배포해야 하며 이전 RHEL 7 호스트를 제거해야 합니다.

### 1.3.16. 노트

#### 1.3.16.1. 스케줄러 프로필 GA

이제 스케줄러 프로필을 사용하여 Pod를 예약할 수 있습니다. 이는 스케줄러 정책을 설정하는 대신 실행됩니다. 다음 스케줄러 프로필을 사용할 수 있습니다.

- **LowNodeUtilization:** 이 프로파일은 노트 간에 Pod를 균등하게 분산하여 노트당 리소스 사용량을 줄입니다.
- **HighNodeUtilization:** 이 프로파일은 노트 당 사용량이 높은 노트 수를 최소화하기 위해 가능한 한 적은 노트에 최대한 많은 Pod를 배치합니다.
- **NoScoring:** 모든 점수 플러그인을 비활성화하여 가장 빠른 스케줄링 주기를 위해 대기 시간이 짧은 프로파일입니다. 이렇게 하면 보다 신속하게 더 나은 스케줄링 결정을 내릴 수 있습니다.

자세한 내용은 [스케줄러 프로필을 사용하여 Pod 예약](#) 을 참조하십시오.

### 1.3.16.2. 새로운 Descheduler 프로필 및 사용자 정의

다음 Descheduler 프로필을 사용할 수 있습니다.

- **soft TopologyAndDuplicates:** 이 프로필은 **whenUnsatisfiable: ScheduleAnyway** 와 같은 소프트웨어 토폴로지 제약 조건이 있는 Pod도 제거로 간주된다는 점을 제외하고 **TopologyAndDuplicates**와 동일합니다.
- **EvictPodsWithLocalStorage:** 이 프로필을 사용하면 로컬 스토리지가 있는 Pod를 제거할 수 있습니다.
- **EvictPodsWithPVC:** 이 프로필을 사용하면 영구 볼륨 클레임이 있는 Pod를 제거할 수 있습니다.

**LifecycleAndUtilization** 프로필에 대한 Pod 수명 값을 사용자 지정할 수도 있습니다.

자세한 내용은 [Descheduler를 사용하여 Pod 제거](#) 를 참조하십시오.

### 1.3.16.3. 동일한 레지스트리에 여러 로그인

Pod가 프라이빗 레지스트리에서 이미지를 가져올 수 있도록 **docker/config.json** 파일을 구성할 때 이제 각각 해당 레지스트리 경로와 관련된 인증 정보를 사용하여 동일한 레지스트리의 특정 리포지토리를 나열할 수 있습니다. 이전에는 지정된 레지스트리에서 하나의 리포지토리만 나열할 수 있었습니다. 이제 특정 네임스페이스로 레지스트리를 정의할 수도 있습니다.

### 1.3.16.4. 노드 리소스 모니터링 강화

노드 관련 지표 및 경고가 개선되어 노드의 안정성이 손상되는 시기를 미리 알 수 있습니다.

### 1.3.16.5. Poison Pill Operator를 통한 수정 개선

Poison Pill Operator에서 위치독 장치 사용으로 개선된 수정 기능을 제공합니다. 자세한 내용은 [위치독 장치](#) 정보를 참조하십시오.

### 1.3.16.6. Node Health Check Operator를 사용하여 노드 상태 점검 배포(기술 프리뷰)

Node Health Check Operator를 사용하여 **NodeHealthCheck** 컨트롤러를 배포할 수 있습니다. 컨트롤러는 비정상 노드를 식별하고 Poison Pill Operator를 사용하여 비정상 노드를 수정합니다.

## 1.3.17. Red Hat OpenShift Logging

OpenShift Container Platform 4.7에서 *Cluster Logging*은 *Red Hat OpenShift Logging*이 되었습니다. 자세한 내용은 [Red Hat OpenShift Logging 릴리스 노트](#) 를 참조하십시오.

## 1.3.18. 모니터링

이 릴리스의 모니터링 스택에는 다음과 같은 새로운 수정된 기능이 포함되어 있습니다.

### 1.3.18.1. 스택 구성 요소 및 종속 항목 모니터링

모니터링 스택 구성 요소 및 종속 항목에 대한 업데이트에는 다음이 포함됩니다.

- Prometheus 2.29.2

- prometheus Operator 0.49.0
- Prometheus Adapter 0.9.0
- Alertmanager 0.22.2
- Thanos 0.22.0

### 1.3.18.2. 경고 규칙

- 새로운 사항
  - **HighlyAvailableWorkloadIncorrectlySpread** 는 고가용성 모니터링 구성 요소의 두 인스턴스가 동일한 노드에서 실행되고 영구 불륨이 연결된 경우 잠재적인 문제에 대해 알려줍니다.
  - 노드 커널이 사용 가능한 파일 설명자가 없으면 **NodeFileDescriptorLimit**가 경고를 트리거합니다. 경고 수준 경고는 사용량이 70%를 초과하면 발생하고 위험 수준 경고는 사용량이 90%를 초과하면 발생합니다.
  - **PrometheusLabelLimitHit**은 대상이 정의된 라벨 제한을 초과할 때 감지합니다.
  - **PrometheusTargetSyncFailure**는 Prometheus가 대상을 동기화하지 못했을 때 감지합니다.
  - 모든 위험 경고 규칙에는 runbooks에 대한 링크가 포함되어 있습니다.
- 개선 사항
  - **AlertManagerReceiversNotConfigured** 및 **KubePodCrashLooping**에는 더 적은 false 양수가 포함됩니다.
  - **KubeCPUOvercommit** 및 **KubeMemoryOvercommit**는 이기종 환경에서 더욱 강력해졌습니다.
  - **NodeFilesystemAlmostOutOfSpace** 경고 규칙의 **for** 기간 설정이 1시간에서 30분으로 변경되어 디스크 공간이 부족할 때 시스템에서 더 빠르게 감지할 수 있습니다.
  - **KubeDeploymentReplicasMismatch**가 예상대로 실행됩니다. 이전 버전에서는 이 경고가 실행되지 않았습니다.
  - 이제 다음 경고에 **namespace** 라벨이 포함됩니다.
    - **AlertmanagerReceiversNotConfigured**
    - **KubeClientErrors**
    - **KubeCPUOvercommit**
    - **KubeletDown**
    - **KubeMemoryOvercommit**
    - **MultipleContainersOOMKilled**
    - **ThanosQueryGrpcClientErrorRate**
    - **ThanosQueryGrpcServerErrorRate**
    - **ThanosQueryHighDNSFailures**



- ThanosQueryHttpRequestQueryErrorRateHigh
- ThanosQueryHttpRequestQueryRangeErrorRateHigh
- ThanosSidecarPrometheusDown
- Watchdog

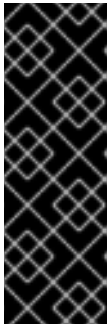


#### 참고

Red Hat은 지표, 기록 규칙 또는 경고 규칙에 대한 이전 버전과의 호환성을 보장하지 않습니다.

### 1.3.18.3. Alertmanager

- 플랫폼과 사용자 정의 프로젝트 모니터링 스택 모두에 대해 외부 Alertmanager를 추가하고 구성할 수 있습니다.
- 로컬 Alertmanager 인스턴스를 비활성화할 수 있습니다.
- 새 **monitoring-alertmanager-edit** 사용자 역할을 통해 관리자가 아닌 사용자는 기본 플랫폼 모니터링에 대한 경고를 생성하고 음소거할 수 있습니다. 이러한 사용자가 경고를 생성하고 음소거할 수 있도록 하려면 **cluster-monitoring-view** 역할 외에도 새 **monitoring-alertmanager-edit** 역할을 할당해야 합니다.



#### 중요

이번 릴리스에서는 Alertmanager에 대한 액세스를 허용하도록 **cluster-monitoring-view** 역할이 제한되어 있습니다. 이전 버전의 OpenShift Container Platform에서 경고를 생성하고 음소거할 수 있는 관리자 이외의 사용자는 이제 이 역할에 할당될 수 없습니다. 관리자가 아닌 사용자가 OpenShift Container Platform 4.9에서 Alertmanager에서 경고를 생성 및 음소거할 수 있도록 하려면 **cluster-monitoring-view** 역할 외에도 새 **monitoring-alertmanager-edit** 역할을 할당해야 합니다.

### 1.3.18.4. Prometheus

- Prometheus에서 플랫폼 모니터링 및 사용자 정의 프로젝트 모두에 대해 원격 쓰기 스토리지를 활성화하고 구성할 수 있습니다. 이 기능을 사용하면 수집된 메트릭을 장기 스토리지로 보낼 수 있습니다.
- Prometheus의 전체 메모리 사용을 줄이기 위해 빈 **Pod** 및 **namespace** 라벨이 모두 있는 다음 cAdvisor 메트릭이 삭제되었습니다.
  - **container\_fs\_\***
  - **container\_spec\_\***
  - **container\_blkio\_device\_usage\_total**
  - **container\_file\_descriptors**
  - **container\_sockets**
  - **container\_threads\_max**

- **container\_threads**
- **container\_start\_time\_seconds**
- **container\_last\_seen**
- 영구 스토리지가 플랫폼 모니터링용으로 구성되지 않은 경우 업그레이드 및 클러스터 중단으로 인해 데이터가 손실될 수 있습니다. 시스템에서 플랫폼 모니터링을 위해 영구 스토리지가 구성되지 않았음을 감지하면 경고 메시지가 **Degraded** 상태에 추가되었습니다.
- **openshift.io/user-monitoring: "false"** 레이블을 추가하여 **openshift-user-workload-monitoring** 프로젝트에서 개별 사용자 정의 프로젝트를 제외할 수 있습니다.
- **openshift-user-workload-monitoring** 프로젝트에 **enforcedTargetLimit** 매개변수를 구성하여 스크랩된 대상 수에 대한 전체 제한을 설정할 수 있습니다.

### 1.3.18.5. 삭제된 Prometheus UI 링크

타사 Prometheus UI에 대한 링크는 OpenShift Container Platform 웹 콘솔의 Observe → **Metrics** 페이지에서 제거됩니다. **openshift-monitoring** 프로젝트의 **네트워킹 → 경로 페이지**로 이동하여 관리자 관점에서 웹 콘솔에서 **Prometheus UI에 대한 경로**에 계속 액세스할 수 있습니다.

### 1.3.18.6. Grafana

기본 Grafana 대시보드를 실행하면 사용자 워크로드에서 리소스를 가져올 수 있으므로 Grafana 대시보드 배포를 비활성화할 수 있습니다.

### 1.3.19. 미터링

이 릴리스에서는 OpenShift Container Platform Metering Operator를 제거합니다.

### 1.3.20. 확장 및 성능

#### 1.3.20.1. Special Resource Operator (기술 프리뷰)

이제 SRO(Special Resource Operator)를 사용하여 기존 OpenShift Container Platform 클러스터에서 커널 모듈 및 드라이버 배포를 관리할 수 있습니다. 현재 기술 프리뷰 기능입니다.

자세한 내용은 [Special Resource Operator 정보](#)를 참조하십시오.

#### 1.3.20.2. 메모리 관리자는 일반적으로 사용 가능

Performance Addon Operator에서 구성한 kubelet 하위 구성 요소인 Memory Manager가 이제 다음 토폴로지 관리자 정책 중 하나로 구성된 노드에서 실행되는 모든 Pod에 대해 기본적으로 활성화됩니다.

- **single-numa-node**
- **restricted**

#### 1.3.20.3. 대기 시간 테스트를 위한 추가 도구

OpenShift Container Platform 4.9에는 시스템 대기 시간을 측정하는 두 개의 추가 도구가 도입되었습니다.

- **Hwlatdetect**는 베어 하드웨어가 달성할 수 있는 기준을 측정합니다.
- **activationlictest**는 **hwlatdetect**가 검증을 통과한 후 반복 타이머를 스케줄링하고 원하는 실제 트리거 시간 간의 차이점을 측정합니다.

자세한 내용은 [대기 시간 테스트 실행](#) 을 참조하십시오.

#### 1.3.20.4. 클러스터 최대값

OpenShift Container Platform 4.9의 [클러스터 최대값](#) 지침이 업데이트되었습니다.



##### 중요

이번 릴리스에서는 OVN-Kubernetes 테스트에 대한 대규모 성능 테스트가 실행되지 않았습니다.

해당 환경의 클러스터 한도를 추정하려면 [OpenShift Container Platform Limit Calculator](#) 를 사용하십시오.

#### 1.3.20.5. 제로 터치 프로비저닝 (기술 프리뷰)

OpenShift Container Platform 4.9에서는 원격 사이트에서 베어 메탈 장비의 선언적 구성으로 새로운 에지 사이트를 프로비저닝할 수 있는 제로 터치 프로비저닝(ZTP)을 지원합니다. ZTP는 인프라 배포에 GitOps 배포 사례를 사용합니다. GitOps는 인프라 배포를 위한 프레임워크를 제공하기 위해 YAML 파일 및 기타 정의된 패턴과 같은 Git 리포지토리에 저장된 선언적 사양을 사용하여 이러한 작업을 수행합니다. 선언적 출력은 다중 사이트 배포를 위해 OCI(Open Cluster Manager)에서 활용됩니다. 자세한 내용은 [대규모로 에지 사이트 프로비저닝](#) 을 참조하십시오.

### 1.3.21. Insights Operator

#### 1.3.21.1. RHEL Simple Content Access 인증서 가져오기 (기술 프리뷰)

OpenShift Container Platform 4.9에서 Insights Operator는 Red Hat OpenShift Cluster Manager에서 RHEL SCA(Simple Content Access) 인증서를 가져올 수 있습니다.

자세한 내용은 [Insights Operator를 사용하여 RHEL Simple Content Access 인증서 가져오기](#) 를 참조하십시오.

#### 1.3.21.2. Insights Operator 데이터 수집 기능 개선 사항

OpenShift Container Platform 4.9에서 Insights Operator는 다음과 같은 추가 정보를 수집합니다.

- 클러스터의 모든 **MachineConfig** 리소스 정의
- 클러스터에 설치된 **PodSecurityPolicies**의 이름
- 설치된 경우 **ClusterLogging** 리소스 정의
- **SamplesImagestreamImportFailing** 경고 발생의 경우 **ImageStream** 정의 및 **openshift-cluster-samples-operator** 네임스페이스에서 마지막 100행의 컨테이너 로그 생성

Red Hat은 이러한 추가 정보를 사용하여 Insights Advisor에서 개선된 수정 단계를 제공할 수 있습니다.

#### 1.3.22. 인증 및 권한 부여

### 1.3.22.1. 수동 모드에서 Cloud Credential Operator를 사용한 Microsoft Azure Stack Hub 지원

이번 릴리스에서는 수동 모드에서 CCO(Cloud Credential Operator)를 구성하여 Microsoft Azure Stack Hub에 설치를 수행할 수 있습니다.

자세한 내용은 [수동 모드 사용](#)을 참조하십시오.

### 1.3.23. OpenShift Container Platform에서 OpenShift 샌드박스 컨테이너 지원(기술 프리뷰)

OpenShift 샌드박스 컨테이너 새 기능, 버그 수정, 알려진 문제 및 비동기 에라타 업데이트를 검토하려면 [OpenShift 샌드박스 컨테이너 1.1 릴리스 노트](#)를 참조하십시오.

## 1.4. 주요 기술 변경 사항

OpenShift Container Platform 4.9에는 다음과 같은 주요 기술 변경 사항이 추가되었습니다.

#### etcd 데이터의 자동 조각 모음

OpenShift Container Platform 4.9에서 etcd 데이터는 etcd Operator에 의해 자동으로 조각 모음됩니다.

#### Octavia OVN NodePort 변경

이전에는 RHOSP(Red Hat OpenStack Platform) 배포에서 NodePorts에서 트래픽을 여는 데 노드 서브넷의 CIDR이 제한되었습니다. Octavia OVN(Open Virtual Network) 공급자를 사용하여 LoadBalancer 서비스를 지원하기 위해 NodePort 트래픽을 마스터 및 작업자 노드에 허용하는 보안 그룹 규칙이 이제 **0.0.0.0/0**을 열도록 변경됩니다.

#### OpenStack Platform LoadBalancer 구성 변경

RHOSP(Red Hat OpenStack Platform) 클라우드 공급자 LoadBalancer 구성의 기본값은 **use-octavia=True**입니다. 이 규칙의 예외는 Kuryr를 사용한 배포입니다. 이 경우 Kuryr는 LoadBalancer 서비스를 자체적으로 처리하기 때문에 **use-octavia**가 **false**로 설정됩니다.

#### Ingress 컨트롤러가 HAProxy 2.2.15로 업그레이드

OpenShift Container Platform Ingress 컨트롤러가 HAProxy 버전 2.2.15로 업그레이드되었습니다.

#### CoreDNS 버전 1.8.4로 업데이트

OpenShift Container Platform 4.9에서 CoreDNS는 버그 수정이 포함된 버전 1.8.4를 사용합니다.

#### 클라우드 공급자를 위한 클라우드 컨트롤러 관리자 구현

클라우드 공급자 배포를 관리하는 Kubernetes 컨트롤러 관리자에는 Azure Stack Hub를 공급업체로 지원하지 않습니다. 클라우드 컨트롤러 관리자를 사용하는 것이 기본 클라우드 플랫폼과 상호 작용하는 데 선호되는 방법이므로 이 지원을 추가할 계획은 없습니다. 결과적으로 OpenShift Container Platform의 Azure Stack Hub 구현에서는 클라우드 컨트롤러 관리자를 사용합니다.

또한 이번 릴리스에서는 AWS(Amazon Web Services), Microsoft Azure 및 RHOSP(Red Hat OpenStack Platform)를 [기술 프리뷰](#)로 클라우드 컨트롤러 관리자 사용을 지원합니다. OpenShift Container Platform에 추가된 새로운 클라우드 플랫폼 지원도 클라우드 컨트롤러 관리자를 사용합니다.

클라우드 컨트롤러 관리자에 대한 자세한 내용은 [구성 요소에 대한 Kubernetes 설명서](#)를 참조하십시오.

클라우드 컨트롤러 관리자 및 클라우드 노드 관리자 배포 및 라이프사이클을 관리하기 위해 이번 릴리스에서는 Cluster Cloud Controller Manager Operator가 도입되었습니다.

자세한 내용은 [Red Hat Operator 참조](#)의 [Cluster Cloud Controller Manager Operator](#) 항목을 참조하십시오.

#### 카나리아 롤아웃 업데이트 수행

OpenShift Container Platform 4.9에서는 카나리아 롤아웃 업데이트를 수행하는 새 프로세스가 도입되었습니다. 이 프로세스에 대한 자세한 개요는 [카나리아 롤아웃 업데이트 수행](#) 을 참조하십시오.

### 대규모 Operator 번들 지원

OLM(Operator Lifecycle Manager)은 etcd에서 설정한 1MB 제한 아래로 유지되도록 대규모 CRD(사용자 정의 리소스 정의) 매니페스트와 같은 대량의 메타데이터로 Operator 번들을 압축합니다.

### Operator Lifecycle Manager의 리소스 사용량 감소

OLM(Operator Lifecycle Management) 카탈로그 Pod가 더 효율적이면서 더 적은 RAM을 사용합니다.

### "Extras" 권고의 Operator의 기본 업데이트 채널

[RHBA-2021:3760](#) 과 같은 OpenShift Container Platform "확장" 권고와 함께 제공되는 Operator는 Red Hat이 제공하는 카탈로그에 게시되며 OLM(Operator Lifecycle Manager)에서 실행됩니다. OpenShift Container Platform 4.9부터 이러한 Operator가 버전별 **4.9** 채널 외에도 **stable** 업데이트 채널에 포함됩니다.

OpenShift Container Platform 4.9 및 향후 릴리스의 경우 이러한 Operator의 기본 채널이 **stable** 입니다. 클러스터 관리자는 향후 클러스터 업그레이드를 통해 OLM에서 이러한 Operator의 업데이트 채널을 변경할 필요가 없도록 **stable** 채널을 사용해야 합니다.

OLM 기반 Operator에 대한 자세한 내용은 [Red Hat에서 제공하는 Operator 카탈로그 및 OperatorHub 이해](#) 를 참조하십시오. OLM의 업데이트 채널에 대한 자세한 내용은 [설치된 Operator 업그레이드](#) 를 참조하십시오.

### Operator SDK v1.10.1

OpenShift Container Platform 4.9에서는 Operator SDK v1.10.1을 지원합니다. 이 최신 버전을 설치하거나 업데이트하려면 [Operator SDK CLI](#) 설치를 참조하십시오.



참고

Operator SDK v1.10.1에서는 Kubernetes 1.21을 지원합니다.

Operator SDK v1.8.0을 사용하여 이전에 생성되거나 유지 관리되는 Operator 프로젝트가 있는 경우 [최신 Operator SDK 버전의 프로젝트 업그레이드](#) 를 참조하여 Operator SDK v1.10.1과의 호환성을 유지하도록 프로젝트를 업그레이드하십시오.

## 1.5. 사용되지 않거나 삭제된 기능

이전 릴리스에서 사용 가능하던 일부 기능이 더 이상 사용되지 않거나 삭제되었습니다.

더 이상 사용되지 않는 기능은 여전히 OpenShift Container Platform에 포함되어 있으며 계속 지원됩니다. 그러나 이 기능은 향후 릴리스에서 제거될 예정이므로 새로운 배포에는 사용하지 않는 것이 좋습니다. OpenShift Container Platform 4.9에서 더 이상 사용되지 않고 삭제된 주요 기능의 최신 목록은 아래 표를 참조하십시오. 더 이상 사용되지 않고 삭제된 기능에 대한 자세한 정보는 표 뒤에 나열되어 있습니다.

아래 표에서 기능은 다음과 같은 상태로 표시되어 있습니다.

- **GA:** 상용 버전
- **TP:** 기술 프리뷰
- **DEP:** 더 이상 사용되지 않음
- **REM:** 삭제된 기능

### 표 1.1. 사용되지 않거나 삭제된 기능 추적

기능	OCP 4.7	OCP 4.8	OCP 4.9
패키지 매니페스트 형식(Operator Framework)	DEP	REM	REM
Operator 카탈로그의 SQLite 데이터베이스 형식	GA	GA	DEP
<b>oc adm catalog build</b>	DEP	REM	REM
<b>oc adm catalog mirror</b> 의 <b>--filter-by-os</b> 플래그	DEP	REM	REM
v1beta1 CRDs	DEP	DEP	REM
Docker Registry v1 API	DEP	DEP	REM
Metering Operator	DEP	DEP	REM
스케줄러 정책	DEP	DEP	DEP
Cluster Samples Operator 의 <b>ImageChangesInProgress</b> 상태	DEP	DEP	DEP
Cluster Samples Operator의 <b>MigrationInProgress</b> 상태	DEP	DEP	DEP
OpenShift Container Platform 리소스의 <b>apiVersion</b> 에서 그룹 없이 <b>v1</b> 사용	DEP	DEP	REM
RHCOS에서 <b>dhclient</b> 사용	DEP	DEP	REM
클러스터 로더	GA	DEP	DEP
사용자의 RHEL 7 컴퓨팅 머신 가져오기	DEP	DEP	DEP
빌드 <b>BuildConfig</b> 사양의 <b>lastTriggeredImageID</b> 필드	GA	DEP	REM
Jenkins Operator	TP	DEP	DEP
Prometheus 기반 HPA 사용자 정의 지표 어댑터	TP	REM	REM
vSphere 6.7 업데이트 2 이전 버전 및 가상 하드웨어 버 전 13	GA	GA	DEP
RHV(Red Hat Virtualization)의 <b>instance_type_id</b> 설치 구성 매개 변수	DEP	DEP	DEP
Microsoft Azure 클러스터의 인증 정보 축소	GA	GA	REM

## 1.5.1. 더 이상 사용되지 않는 기능

### 1.5.1.1. Operator 카탈로그의 SQLite 데이터베이스 형식

관련 **opm** CLI 명령을 포함하여 카탈로그 및 인덱스 이미지에 OLM(Operator Lifecycle Manager)에서 사용하는 SQLite 데이터베이스 형식이 더 이상 사용되지 않습니다. 클러스터 관리자 및 카탈로그 유지 관리자는 OpenShift Container Platform 4.9에 도입된 새로운 **파일 기반 카탈로그 형식**을 숙지하고 카탈로그 워크플로 마이그레이션을 시작하는 것이 좋습니다.



#### 참고

OpenShift Container Platform 4.6 이상에 대한 기본 **Red Hat 제공 Operator 카탈로그**는 현재 SQLite 데이터베이스 형식으로 계속 제공됩니다.

### 1.5.1.2. vSphere 6.7 Update 2 및 이전 버전의 클러스터 설치 및 가상 하드웨어 버전 13이 더 이상 사용되지 않음

VMware vSphere 버전 6.7 Update 2 또는 이전 버전에 클러스터를 설치하는 경우 이제 가상 하드웨어 버전 13이 더 이상 사용되지 않습니다. 이러한 버전에 대한 지원은 향후 OpenShift Container Platform 버전으로 종료됩니다.

이제 OpenShift Container Platform의 vSphere 가상 머신의 하드웨어 버전 15가 기본값이 되었습니다. 하드웨어 버전 15는 향후 OpenShift Container Platform 버전에서 지원되는 유일한 버전입니다.

### 1.5.1.3. RHV(Red Hat Virtualization)의 instance\_type\_id 설치 구성 매개 변수

**instance\_type\_id** 설치 구성 매개 변수는 더 이상 사용되지 않으며 향후 릴리스에서 제거됩니다.

## 1.5.2. 삭제된 기능

### 1.5.2.1. 미터링

이 릴리스에서는 OpenShift Container Platform Metering Operator 기능이 제거됩니다.

### 1.5.2.2. Kubernetes 1.22에서 Beta API 제거

Kubernetes 1.22에서는 더 이상 사용되지 않는 **v1beta1** API를 제거했습니다. **v1** API 버전을 사용하도록 매니페스트 및 API 클라이언트를 마이그레이션합니다. 제거된 API 마이그레이션에 대한 자세한 내용은 [Kubernetes 설명서](#)를 참조하십시오.

표 1.2. Kubernetes 1.22에서 v1beta1 API 제거

리소스	API	주요 변경 사항
<b>APIService</b>	<b>apiregistration.k8s.io/v1beta1</b>	없음
<b>CertificateSigningRequest</b>	<b>certificates.k8s.io/v1beta1</b>	있음
<b>ClusterRole</b>	<b>rbac.authorization.k8s.io/v1beta1</b>	없음
<b>ClusterRoleBinding</b>	<b>rbac.authorization.k8s.io/v1beta1</b>	없음

리소스	API	주요 변경 사항
CSIDriver	storage.k8s.io/v1beta1	없음
CSINode	storage.k8s.io/v1beta1	없음
CustomResourceDefinition	apiextensions.k8s.io/v1beta1	있음
Ingress	extensions/v1beta1	있음
Ingress	networking.k8s.io/v1beta1	있음
IngressClass	networking.k8s.io/v1beta1	없음
Lease	coordination.k8s.io/v1beta1	없음
LocalSubjectAccessReview	authorization.k8s.io/v1beta1	있음
MutatingWebhookConfiguration	admissionregistration.k8s.io/v1beta1	있음
PriorityClass	scheduling.k8s.io/v1beta1	없음
Role	rbac.authorization.k8s.io/v1beta1	없음
RoleBinding	rbac.authorization.k8s.io/v1beta1	없음
SelfSubjectAccessReview	authorization.k8s.io/v1beta1	있음
StorageClass	storage.k8s.io/v1beta1	없음
SubjectAccessReview	authorization.k8s.io/v1beta1	있음
TokenReview	authentication.k8s.io/v1beta1	없음
ValidatingWebhookConfiguration	admissionregistration.k8s.io/v1beta1	있음
VolumeAttachment	storage.k8s.io/v1beta1	없음

### 1.5.2.3. Descheduler v1beta1 API 제거

Descheduler에 더 이상 사용되지 않는 **v1beta1** API가 OpenShift Container Platform 4.9에서 제거되었습니다. Descheduler **v1beta1** API 버전을 사용하여 모든 리소스를 **v1**로 마이그레이션합니다.

### 1.5.2.4. RHCOS에서 dhclient 사용 삭제

더 이상 사용되지 않는 **dhclient** 바이너리가 RHCOS에서 제거되었습니다. OpenShift Container Platform



4.6부터 RHCOS는 **initramfs**에서 **NetworkManager**를 사용하여 초기 부팅 중에 네트워킹을 구성하도록 전환되었습니다. 대신 네트워킹 구성에 **NetworkManager** 내부 DHCP 클라이언트를 사용합니다. 자세한 내용은 [BZ#1908462](#)에서 참조하십시오.

### 1.5.2.5. lastTriggeredImageID 필드를 업데이트하지 않고 무시함

현재 릴리스에서는 **buildConfig.spec.triggers[i].imageChage**에서 참조하는 **ImageStreamTag**가 새 이미지를 가리킬 때 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID** 필드의 업데이트를 중지합니다. 대신 이 릴리스에서는 **buildConfig.status.imageChangeTriggers[i].lastTriggeredImageID** 필드를 업데이트합니다.

또한 Build Image Change Trigger 컨트롤러는 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID** 필드를 무시합니다.

이제 Build Image Change Trigger 컨트롤러는 **buildConfig.status.imageChangeTriggers[i].lastTriggeredImageID** 필드 및 **buildConfig.spec.triggers[i].imageChange**에서 참조하는 **ImageStreamTag**가 참조하는 이미지 ID와 비교하는 방법을 기반으로 빌드를 시작합니다.

따라서 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID**를 검사하는 스크립트 및 작업을 업데이트합니다. ([BUILD-190](#))

### 1.5.2.6. OpenShift Container Platform 리소스의 apiVersion에 대한 그룹없이 v1 사용

OpenShift Container Platform 리소스의 **apiVersion** 리소스 그룹 없이 **v1** 사용을 위한 지원이 제거되었습니다. \*.**openshift.io**를 포함하는 모든 리소스는 [API 인덱스](#)에 있는 **apiVersion** 값과 일치해야 합니다.

### 1.5.2.7. Microsoft Azure에 대한 인증 정보 풀링 지원

OpenShift Container Platform 4.9.24부터 Microsoft Azure 클러스터의 mint 모드에서 CCO(Cloud Credential Operator) 사용에 대한 지원이 OpenShift Container Platform 4.9에서 제거되었습니다. 이러한 변경 사항은 [2022년 6월 30일에 예정된 Microsoft Azure AD Graph API 사용 중지](#)로 인한 것이며 z-stream 업데이트에서 지원되는 모든 OpenShift Container Platform 버전으로 백포트되고 있습니다.

mint 모드를 사용하는 이전에 설치된 Azure 클러스터의 경우 CCO는 기존 보안 업데이트를 시도합니다. 보안에 이전에 Mint된 앱 등록 서비스 주체의 인증 정보가 포함된 경우 **kube-system/azure-credentials**의 시크릿 콘텐츠로 업데이트됩니다. 이 동작은 통과 모드와 유사합니다.

인증 정보 모드가 기본값 ""으로 설정된 클러스터의 경우 업데이트된 CCO가 Mint 모드에서 작동되지 않도록 자동으로 변경됩니다. 클러스터에 인증 정보 모드가 명시적으로 Mint 모드("Mint")로 설정된 경우 값은 "" 또는 "Passthrough"로 변경해야 합니다.



#### 참고

Mint 모드에서 필요한 **Contributor** 역할 외에도 수정된 앱 등록 서비스 주체에는 이제 passthrough 모드에 사용되는 **User Access Administrator** 역할이 필요합니다.

Azure AD Graph API를 계속 사용할 수 있지만 업그레이드된 OpenShift Container Platform 버전의 CCO는 이전에 Mint된 앱 등록 서비스 주체를 정리하려고 합니다. Azure AD Graph API 전에 클러스터를 업그레이드하면 리소스를 수동으로 정리하지 않아도 될 수 있습니다.

Azure AD Graph API가 종료된 후 Mint 모드를 지원하지 않는 OpenShift Container Platform 버전으로 클러스터가 업그레이드되면 CCO는 연결된 **CredentialsRequest**에서 **OrphanedCloudResource** 조건을 설정하지만 오류를 치명적으로 처리하지는 않습니다. 조건에는 **unable to clean up App Registration /**

**Service Principal:** <app\_registration\_name> 것과 유사한 메시지가 포함됩니다. Azure AD Graph API 를 종료한 후에는 나머지 앱 등록 서비스 주체를 제거하기 위해 Azure CLI 도구 또는 Azure 웹 콘솔을 사용하여 수동 개입이 필요합니다.

리소스를 수동으로 정리하려면 영향을 받는 리소스를 찾아서 삭제해야 합니다.

1. Azure CLI 도구를 사용하여 다음 명령을 실행하여 **OrphanedCloudResource** 조건 메시지의 <app\_registration\_name> 을 사용하는 앱 등록 서비스 주체를 필터링합니다.

```
$ az ad app list --filter "displayname eq '<app_registration_name>'" --query '[].{objectId}'
```

출력 예

```
[
  "038c2538-7c40-49f5-abe5-f59c59c29244"
]
```

2. 다음 명령을 실행하여 앱 등록 서비스 주체를 삭제합니다.

```
$ az ad app delete --id 038c2538-7c40-49f5-abe5-f59c59c29244
```



#### 참고

수동으로 리소스를 정리한 후 CCO에서 리소스가 정리되었는지 확인할 수 없기 때문에 **OrphanedCloudResource** 조건이 지속됩니다.

## 1.6. 버그 수정

### API 서버 및 인증

- 이전에는 암호화 조건이 무기한 유지되어 일부 Operator의 성능이 저하된 상태로 보고될 수 있었습니다. 이제 오래된 암호화 조건이 올바르게 지워지고 더 이상 잘못 보고되지 않습니다. ([BZ#1974520](#))
- 이전에는 클러스터 수명 주기 초기에 API 서버 클라이언트 인증서용 CA가 교체되어 동일한 이름의 이전 CSR이 여전히 존재하기 때문에 Authentication Operator에서 CSR(인증서 서명 요청)을 생성하지 못했습니다. **TokenReview** 요청을 보낼 때 Kubernetes API 서버에서 OAuth API 서버에 자체 인증할 수 없어 인증에 실패했습니다. 이제 Authentication Operator에서 CSR을 생성할 때 생성된 이름을 사용하므로 API 서버 클라이언트 인증서에 대해 CA를 조기 교체해도 더 이상 인증 실패가 발생하지 않습니다. ([BZ#1978193](#))

### 베어 메탈 하드웨어 프로비저닝

- 이전에는 initContainers 생성 시퀀스로 인해 metal3 Pod에서 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지를 다운로드할 수 없었습니다. 이 문제는 **metal-static-ip-set** initContainer가 **metal3-machine-os-downloader** initContainer 이전에 생성되도록 initContainers 생성을 다시 정렬하여 해결되었습니다. RHCOS 이미지가 예상대로 다운로드됩니다. ([BZ#1973724](#))
- 이전 버전에서는 **idrac-virtualmedia**를 사용하도록 구성된 호스트가 있는 베어 메탈에 설치 관리자 프로비저닝 설치를 사용하는 경우 해당 호스트의 **bios\_interface**가 기본적으로 **idrac-wsman**로 설정되었습니다. 이로 인해 BIOS 설정을 사용할 수 없으며 예외가 발생했습니다. 이 문제는 **idrac-virtualmedia**를 사용하는 경우 기본 **bios\_interface**에 **idrac-redfish**를 사용하여 해결됩니다. ([BZ#1928816](#))

- 이전에는 UEFI 모드에서 RHCOS 이미지를 다운로드한 후 **ironic-python-agent**가 UEFI 부트로더 항목을 생성했습니다. RHEL 8.4 기반 RHCOS 이미지를 사용하는 경우 이 항목을 사용하여 이미지를 부팅하지 못하고 BIOS 오류 화면을 출력할 수 있었습니다. 이는 고정된 부팅 항목을 사용하는 대신 이미지에 있는 CSV 파일을 기반으로 부팅 항목을 구성하는 **ironic-python-agent**에 의해 해결됩니다. 이미지가 오류 없이 제대로 부팅됩니다. (BZ#1966129)
- 이전 버전에서는 **provisioningHostIP**가 **install-config**에 설정된 경우 프로비저닝 네트워크가 비활성화된 경우에도 metal3 Pod에 할당되었습니다. 이 문제가 해결되었습니다. (BZ#1972753)
- 이전에는 sushy 리소스 라이브러리가 일치하지 않아 지원 설치 프로그램에서 Supermicro X11/X12 기반 시스템을 프로비저닝할 수 없었습니다. 이러한 불일치로 인해 가상 미디어를 **Inserted** 및 **WriteProtected** 속성에 연결할 수 없고 **VirtualMedia.InsertMedia** 요청에서 허용되지 않아 설치 문제가 발생했습니다. 이 문제는 sushy 리소스 라이브러리를 수정하고 엄격하게 필요하지 않은 경우 이러한 선택적 속성 전송을 중지하는 조건을 추가하여 해결되어 이 지점에서 설치가 진행될 수 있도록 합니다. (BZ#1986238)
- 이전에는 프로비저닝된 상태의 일부 오류 유형으로 인해 호스트가 프로비저닝되지 않았습니다. 이는 metal3 pod를 다시 시작한 후 베어 메탈 호스트에 프로비저닝된 이미지를 사용할 수 없게 된 경우 발생했습니다. 이 경우 호스트는 프로비저닝 해제 상태가 됩니다. 이 문제는 이미지를 사용할 수 없게 되면 오류가 보고되지만 프로비저닝 해제는 시작되지 않도록 프로비저닝된 상태의 오류 동작을 수정하여 해결됩니다. (BZ#1972374)

## 빌드

- OpenShift Container Platform 이상에서 SCP 형식의 URL 기능을 제공하기 위해 BZ#1884270 버그 수정이 SSH 프로토콜 URL을 잘못 정리했습니다. 이 오류로 인해 **oc new-build** 명령이 자동 소스 복제 시크릿을 선택하지 않았습니다. 빌드에서 **build.openshift.io/sbuild.openshift.io/source-secret-match-uri-1** 주석을 사용하여 SSH 키를 관련 시크릿과 매핑할 수 없으므로 Git 복제를 수행할 수 없었습니다. 이번 업데이트에서는 빌드에서 주석을 사용하고 git 복제를 수행할 수 있도록 BZ#1884270의 변경 사항을 되돌립니다.
- 이번 업데이트 이전에는 클러스터 이미지 구성의 허용 및 차단 레지스트리 구성 옵션을 통해 Cluster Samples Operator가 이미지 스트림을 생성하지 못하도록 차단할 수 있었습니다. 이 문제가 발생하면 샘플 operator가 **degraded**로 표시하여 일반적인 OpenShift Container Platform 설치 및 업그레이드 상태에 영향을 미쳤습니다. Cluster Samples Operator는 다양한 상황에서 **removed**된 대로 부트스트랩할 수 있습니다. 이번 업데이트를 통해 이러한 상황에는 **이미지 컨트롤러 구성 매개 변수**가 기본 이미지 레지스트리를 사용하거나 **samplesRegistry** 설정에서 지정한 이미지 레지스트리를 사용하여 이미지 스트림 생성을 방지하는 경우가 포함됩니다. Operator 상태에는 클러스터 이미지 구성으로 인해 샘플 이미지 스트림 생성할 수 없는 경우도 표시됩니다.

## 클라우드 컴퓨팅

- 이전 버전에서는 새 서버에 대한 root 볼륨이 생성되고 서버가 생성되지 않은 경우 볼륨과 연결된 서버가 삭제되지 않았기 때문에 볼륨의 자동 삭제가 트리거되지 않았습니다. 이로 인해 많은 추가 볼륨이 생성되어 볼륨 할당량에 도달한 경우 오류가 발생했습니다. 이번 릴리스에서는 서버 생성 호출이 실패하면 새로 생성된 root 볼륨이 삭제됩니다. (BZ#1943378)
- 이전에는 **instanceType**에 기본값을 사용할 때 Machine API가 AWS에서 **m4.large** 인스턴스를 생성했습니다. 이는 OpenShift Container Platform 설치 프로그램에서 생성한 머신의 **m5.large** 인스턴스 유형과 다릅니다. 이번 릴리스에서는 Machine API에서 기본값이 지정되면 AWS에서 새 머신에 대해 **m5.large** 인스턴스를 생성합니다. (BZ#1953063)
- 이전에는 컴퓨팅 노드의 시스템 세트 정의에서 포트를 트렁크해야 하는지 여부를 지정할 수 없었습니다. 이는 사용자가 같은 시스템에 트렁크된 포트와 트렁크되지 않은 포트를 구성해야 하는 기술에 문제가 있었습니다. 이번 릴리스에서는 새 필드인 **spec.Port.Trunk = bool**이 추가되어 사용

자가 트렁크가 트렁크를 생성하는 포트를 보다 유연하게 결정할 수 있습니다. 값을 지정하지 않으면 **spec.Port.Trunk**는 **spec.Trunk**의 값을 상속하고 생성된 트렁크 이름은 사용된 포트의 이름과 일치합니다. ([BZ#1964540](#))

- 이전에는 Machine API Operator가 이미 연결되어 있어도 새 대상을 지속적으로 연결했습니다. AWS API에 대한 과도한 호출으로 인해 많은 오류가 발생했습니다. 이번 릴리스에서는 Operator에서 연결 프로세스를 시도하기 전에 로드 밸런서 연결이 필요한지 여부를 확인합니다. 이 변경으로 실패한 API 요청의 빈도가 줄어들었습니다. ([BZ#1965080](#))
- 이전에는 VM에 자동 고정을 사용할 때 속성 이름이 **disabled, existing, adjust**로 되었습니다. 이번 릴리스에서는 이름은 각 정책을 더 잘 설명하고 oVirt에서 차단되었기 때문에 **existing** 이름이 제거되었습니다. 새 속성 이름은 **none**이고 **resize\_and\_pin**은 oVirt 사용자 인터페이스와 일치합니다. ([BZ#1972747](#))
- 이전에는 클러스터 자동 확장기에서 **csidrivers.storage.k8s.io** 또는 **csistoragecapacities.storage.k8s.io** 리소스에 액세스할 수 없어 권한 오류가 발생했습니다. 이번 수정을 통해 클러스터 자동 스케일러에 할당된 역할이 업데이트되어 해당 리소스에 대한 권한이 포함됩니다. ([BZ#1973567](#))
- 이전에는 삭제된 노드로 머신을 삭제할 수 있었습니다. 이로 인해 머신이 삭제 단계에 무기한 유지되었습니다. 이번 수정을 통해 이 상태의 머신을 올바르게 삭제할 수 있습니다. ([BZ#1977369](#))
- **boot-from-volume** 이미지를 사용하는 경우 시스템 컨트롤러가 재부팅되는 경우 새 인스턴스를 생성하면 볼륨이 누출됩니다. 이로 인해 이전에 만든 볼륨이 정리되지 않았습니다. 이번 수정을 통해 이전에 만든 볼륨이 정리되거나 재사용됩니다. ([BZ#1983612](#))
- 이전에는 RHV(Red Hat Virtualization) 공급자가 머신의 **br-ex** 이름이 있는 NIC를 무시했습니다. **OVNKubernetes**의 네트워크 유형은 **br-ex** 이름으로 NIC를 생성하므로 머신에 OVN-Kubernetes에서 IP 주소가 할당되지 않았습니다. 이번 수정을 통해 네트워크를 **OVNKubernetes**로 설정하여 RHV에 OpenShift Container Platform을 설치할 수 있습니다. ([BZ#1984481](#))
- 이전에는 프록시와 사용자 정의 CA 인증서가 조합된 RHOSP(Red Hat OpenStack Platform)에 배포하면 클러스터가 완전히 작동하지 않았습니다. 이번 수정에서는 사용자 정의 CA 인증서로 연결할 때 사용되는 HTTP 전송에 프록시 설정을 전달하여 모든 클러스터 구성 요소가 예상대로 작동하도록 합니다. ([BZ#1986540](#))

## Cluster Version Operator

- 이전에는 CVO(Cluster Version Operator)가 프록시 구성 리소스의 **noProxy** 속성을 인식하지 못했습니다. 결과적으로 프록시되지 않은 연결만 완료되었을 때 CVO는 업데이트 권장 사항 또는 릴리스 서명에 대한 액세스가 거부되었습니다. 이제 프록시되지 않은 액세스를 프록시하지 않고 직접 요청하면 CVO가 업스트림 업데이트 서비스 및 서명 저장소에 직접 도달합니다. ([BZ#1978749](#))
- 이전에는 CVO(Cluster Version Operator)가 Network Operator에서 확인한 상태 속성 대신 프록시 리소스 사양 속성에서 프록시 구성을 로드했습니다. 결과적으로 잘못 구성된 값은 CVO가 업스트림 업데이트 서비스 또는 서명 저장소에 도달하지 못하게 했습니다. 이제 CVO는 확인된 상태 속성에서만 프록시 구성을 로드합니다. ([BZ#1978774](#))
- 이전에는 CVO(Cluster Version Operator)에서 매니페스트 외부에 추가된 볼륨 마운트를 제거하지 않았습니다. 이로 인해 볼륨 오류가 발생하는 동안 Pod 생성이 실패할 수 있었습니다. 이제 CVO는 매니페스트에 표시되지 않는 모든 볼륨 마운트를 제거합니다. ([BZ#2004568](#))

## 콘솔 스토리지 플러그인

- 이전에는 Ceph 스토리지로 작업할 때 Console Storage 플러그인에 namespace 매개변수의 중복 사용이 불필요하게 포함되었습니다. 이 버그에는 고객이 볼 수 있는 영향이 없었습니다. 그러나 네임스페이스를 중복 사용하지 않도록 플러그인이 업데이트되었습니다. (BZ#1982682)

## 이미지 레지스트리

- 레지스트리에서 사용자 정의 허용 오차를 사용해야 하는지 확인하는 Operator는 **spec.tolerations** 대신 **spec.nodeSelector**를 확인했습니다. **spec.tolerations**의 사용자 지정 허용 오차는 **spec.nodeSelector**가 설정된 경우에만 적용됩니다. 이번 수정에서는 **spec.tolerations** 필드를 사용하여 사용자 지정 허용 오차가 있는지 확인합니다. 이제 **spec.tolerations**가 설정된 경우 Operator는 사용자 정의 허용 오차를 사용합니다. (BZ#1973318)
- **configs.imageregistry**의 **spec.managementState**는 **Removed**로 설정되어 이미지 정리기 Pod가 **v1.21** 이상에서 더 이상 사용되지 않는 CronJob에 대한 경고를 생성했으며 **batch/v1**을 사용해야 했습니다. 이번 수정에서는 OpenShift Container Platform **oc**에서 **batch/v1**로 **batch/v1beta1**이 업데이트되었습니다. 이제 이미지 정리기 Pod에서 사용되지 않는 CronJob에 대한 경고가 더 이상 표시되지 않습니다. (BZ#1976112)

## 설치 프로그램

- 이전에는 Azure 컨트롤 플레인 노드의 네트워크 인터페이스에서 인터페이스 이름에 하이픈이 누락되었습니다. 이로 인해 다른 플랫폼과 비교했을 때 문제가 발생했습니다. 누락된 하이픈이 추가되었습니다. 이제 플랫폼에 관계없이 모든 컨트롤 플레인 노드의 이름이 동일하게 지정됩니다. (BZ#1882490)
- oVirt의 **install-config.yaml** 파일에서 **autoPinningPolicy** 및 **hugepages** 필드를 구성할 수 있습니다. **autoPinningPolicy** 필드를 사용하면 클러스터의 NUMA(Non-Uniform Memory Access) 고정 설정 및 CPU 토폴로지 변경을 자동으로 설정할 수 있습니다. **hugepages** 필드를 사용하면 하이퍼바이저의 Hugepages를 설정할 수 있습니다. (BZ#1925203)
- 이전에는 설치 프로그램을 사용할 수 없어도 FIPS 활성화와 함께 Ed25519 SSH 키 유형을 사용할 때 오류가 출력되지 않았습니다. 이제 설치 프로그램에서 SSH 키 유형을 검증하여 FIPS가 활성화된 상태에서 SSH 키 유형을 지원하지 않을 때 오류를 출력합니다. FIPS가 활성화되면 RSA 및 ECDSA SSH 키 유형만 허용됩니다. (BZ#1962414)
- 특정 조건에서 RHOSP(Red Hat OpenStack Platform) 네트워크 트렁크에는 트렁크가 클러스터에 속해 있음을 나타내는 태그가 없습니다. 결과적으로 클러스터 삭제는 트렁크 포트가 누락되어 시간이 초과될 때까지 루프에 갇혔습니다. 이제 클러스터를 삭제하면 태그가 지정된 포트가 상위 포트인 트렁크가 삭제됩니다. (BZ#1971518)
- 이전에는 RHOSP(Red Hat OpenStack Platform)에서 클러스터를 설치 제거할 때 비효율적인 알고리즘을 사용하여 리소스를 삭제했습니다. 비효율적인 알고리즘으로 인해 제거 프로세스에 필요한 시간보다 많은 시간이 소요되었습니다. 설치 프로그램은 클러스터를 더 신속하게 제거해야 하는 보다 효율적인 알고리즘으로 업데이트되었습니다. (BZ#1974598)
- 이전에는 **AWS\_SHARED\_CREDENTIALS\_FILE** 환경 변수가 빈 파일로 설정된 경우 설치 프로그램에서 인증 정보를 요청한 다음, 환경 변수의 값을 무시하고 기존 인증 정보를 덮어쓸 수 있는 **aws/credentials** 파일을 생성했습니다. 이번 수정으로 지정된 파일에 인증 정보를 저장하도록 설치 프로그램이 업데이트되었습니다. 지정된 파일에 잘못된 인증 정보가 있는 경우 설치 프로그램에서 파일을 덮어쓰는 대신 오류를 생성하고 정보가 손실될 위험을 감수합니다. (BZ#1974640)
- 이전에는 Azure에서 다른 클러스터와 리소스를 공유한 클러스터를 삭제할 때 애매모호한 오류 메시지가 표시되어 삭제 실패 이유를 이해하기 어려웠습니다. 이번 업데이트에서는 오류 발생 이유를 설명하는 오류 메시지가 추가되었습니다. (BZ#1976016)

- 이전에는 오타로 인해 Kuryr 배포가 잘못된 요구 사항에 대해 확인되었습니다. 즉 Kuryr의 최소 요구 사항을 충족하지 않아도 Kuryr를 사용한 설치는 성공할 수 있었습니다. 이번 수정을 통해 오류가 제거되어 설치 프로그램이 올바른 요구 사항을 확인할 수 있습니다. (BZ#1978213)
- 이번 업데이트 이전에는 **keepalived**에 대한 수신 검사에 fall 및 raise 지시문이 포함되지 않았습니다. 즉, 한 번의 실패한 검사로 인해 수신 가상 IP 페일오버가 발생할 수 있었습니다. 이 버그 수정을 통해 fall 및 raise 지시문을 도입하여 이러한 페일오버를 방지합니다. (BZ#1982766)

## Kubernetes API 서버

- 이전 버전에서는 배포 및 이미지 스트림이 동시에 생성될 때 경쟁 조건이 발생하여 배포 컨트롤러에서 무한 루프에 복제본 세트를 생성할 수 있었습니다. API 서버의 이미지 정책 플러그인이 낮아지고 배포 및 이미지 스트림을 동시에 생성하는 경우 더 이상 무한 복제본 세트가 발생하지 않습니다. (BZ#1925180), (BZ#1976775)
- 이전에는 동일한 경로에 작성 중인 설치 프로그램 pod와 cert-syncer 컨테이너 간에 경쟁이 있었습니다. 이로 인해 일부 인증서가 비어 있고 서버가 실행되지 않을 수 있었습니다. 이제 Kubernetes API 서버 인증서가 여러 프로세스 간의 경쟁을 방지하기 위해 원자적인 방식으로 작성됩니다. (BZ#1971624)

## 모니터링

- 이번 업데이트 이전에는 **cluster-monitoring-view** 사용자 역할을 목표로 하여 Alertmanager에 대한 액세스만 허용하더라도 이 역할에 할당된 관리자가 아닌 사용자는 여전히 경고를 생성하고 음소거할 수 있었습니다. 이번 업데이트를 통해 이 역할에만 할당된 사용자는 더 이상 경고를 생성하거나 음소거할 수 없습니다. 관리자가 아닌 사용자가 경고를 생성하고 음소거할 수 있도록 하려면 **cluster-monitoring-view** 역할 외에도 새 **monitoring-alertmanager-edit** 역할을 할당해야 합니다. (BZ#1947005)

## 네트워킹

- OVN-Kubernetes 클러스터 네트워크 공급자를 사용할 때 메모리 제한 없이 논리 흐름 캐시가 구성되었습니다. 결과적으로 메모리가 부족하면 노드를 사용할 수 없게 될 수 있었습니다. 이번 업데이트를 통해 논리 흐름 캐시는 기본적으로 1GB 메모리 제한으로 구성됩니다. (BZ#1961757)
- OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 경우 나중에 업그레이드된 OpenShift Container Platform 4.5 클러스터에서 생성된 모든 네트워크 정책에서 예기치 않은 트래픽을 허용하거나 제거할 수 있습니다. 최신 버전의 OpenShift Container Platform에서 OVN-Kubernetes는 IP 주소 세트를 관리하는 데 다른 규칙을 사용하고 OpenShift Container Platform 4.5에서 생성된 모든 네트워크 정책은 이 규칙을 사용하지 않았습니다. 이제 업그레이드하는 동안 모든 네트워크 정책이 새 규칙으로 마이그레이션됩니다. (BZ#1962387)
- OVN-Kubernetes 클러스터 네트워크 공급자의 경우 **must-gather**를 사용하여 OVS(Open vSwitch) 로그를 검색할 때 수집된 로깅 데이터에서 **INFO** 로그 수준이 누락되었습니다. 이제 모든 로그 수준이 OVS 로깅 데이터에 포함됩니다. (BZ#1970129)
- 이전 버전에서는 성능 테스트의 레이블 요구 사항으로 인해 서비스 컨트롤러 메트릭에서 cardinality가 크게 증가한 것으로 나타났습니다. 결과적으로 메모리 사용량이 OVN(Open Virtual Network) Prometheus Pod에서 증가했습니다. 이번 업데이트를 통해 레이블 요구 사항이 제거됩니다. 이제 서비스 컨트롤러 Cardinality 메트릭 및 메모리 사용량이 줄어듭니다. (BZ#1974967)
- 이전에는 **ovnkube-trace**에서 인터페이스 **link** 색인을 감지해야 했기 때문에 소스 및 대상 Pod에 iproute를 설치해야 했습니다. 이로 인해 iproute가 설치되지 않은 경우 Pod에서 **ovnkube-trace**가 실패했습니다. 이제 iproute 대신 **/sys/class/net/<interface>/iflink**에서 **link** 인덱스를 가져올 수 있습니다. 결과적으로 **ovnkube-trace**에서 더 이상 소스 및 대상 Pod에 iproute를 설치할 필요가 없습니다. (BZ#1978137)
- 이전에는 CNO(Cluster Network Operator)에서 올바른 주석 및 역할 기반 액세스 제어(RBAC) 없

이 Prometheus에서 검색할 수 있도록 **network-check-source** 서비스를 위한 서비스 모니터를 배포했습니다. 결과적으로 서비스와 해당 메트릭은 Prometheus에 채워지지 않았습니다. 이제 올바른 주석과 RBAC가 **network-check-source** 서비스의 네임스페이스에 추가됩니다. 이제 Prometheus를 통해 서비스 **network-check-source**의 메트릭이 스크랩됩니다. (BZ#1986061)

- 이전에는 IPv6 DHCP를 사용할 때 노드 인터페이스 주소가 /128 접두사로 임대될 수 있었습니다. 결과적으로 OVN-Kubernetes는 동일한 접두사를 사용하여 노드의 네트워크를 유추하고 게이트웨이를 통해 다른 클러스터 노드에 대한 트래픽을 포함한 다른 주소 트래픽을 라우팅합니다. 이번 업데이트를 통해 OVN-Kubernetes는 노드의 라우팅 테이블을 검사하고 노드의 인터페이스 주소에 대한 광범위한 라우팅 항목을 확인하여 해당 접두사를 사용하여 노드의 네트워크를 유추합니다. 결과적으로 다른 클러스터 노드로의 트래픽이 더 이상 게이트웨이를 통해 라우팅되지 않습니다. (BZ#1980135)
- 이전에는 클러스터에서 OVN-Kubernetes Container Network Interface 공급자를 사용할 때 IPv6 주소가 있는 송신 라우터를 추가하는 데 실패했습니다. 수정판에서는 IPv6에 대한 지원이 송신 라우터 CNI 플러그인에 추가되고 송신 라우터 추가에 성공합니다. (BZ#1989688)

## 노드

- 이전에는 컨테이너에서 CRI-O가 /proc/mounts 파일에서 /etc/mtab 파일에 대한 심볼릭 링크를 생성하지 않았습니다. 결과적으로 사용자는 컨테이너의 /etc/mtab 파일에 마운트된 장치 목록을 볼 수 없었습니다. CRI-O는 이제 심볼릭 링크를 추가합니다. 결과적으로 사용자는 컨테이너의 마운트된 장치를 볼 수 있습니다. (BZ#1868221)
- 이전에는 생성 후 Pod가 신속하게 삭제된 경우 kubelet에서 Pod를 올바르게 정리하지 못할 수 있었습니다. 이로 인해 Pod가 종료 상태가 되어 업그레이드 가용성에 영향을 미칠 수 있었습니다. 이번 수정을 통해 Pod 라이프사이클 논리가 개선되어 이러한 문제 발생을 방지할 수 있습니다. (BZ#1952224)
- 이전에는 시스템 메모리 사용량이 예약된 메모리의 90%를 초과하면 **SystemMemoryExceedsReserved** 경고가 발생했습니다. 이로 인해 클러스터에서 과도한 수의 경고를 실행할 수 있었습니다. 이 알람의 임계값이 예약된 메모리의 95%에서 실행되도록 변경되었습니다. (BZ#1980844)
- 이전에는 CRI-O의 버그로 인해 CRI-O에서 생성한 프로세스의 하위 PID가 유출되었습니다. 결과적으로 부하가 걸린 경우 systemd에서 상당한 수의 좀비 프로세스를 생성할 수 있습니다. 이로 인해 노드에서 PID가 실행된 경우 노드에 오류가 발생할 수 있습니다. CRI-O가 누출을 방지하기 위해 수정되었습니다. 따라서 이러한 좀비 프로세스가 더 이상 생성되지 않습니다. (BZ#2003197)

## OpenShift CLI(oc)

- 이전 버전에서는 레지스트리를 미러링하는 동안 **oc** 명령줄 툴이 충돌하여 **--max-components** 인수를 사용할 때 슬라이스에서 검사되지 않은 인덱스 작업으로 인해 **slice bounds out of range** 패닉 런타임 오류가 발생했습니다. 이번 수정을 통해 **--max-components** 인수를 사용할 때 **oc** 툴이 더 이상 패닉하지 않도록 구성 요소 검사에서 범위를 벗어난 인덱스 값을 요청하지 않도록 검사가 추가되었습니다. (BZ#1786835)
- 이전 버전에서는 **oc describe quota** 명령에 **ClusterResourceQuota** 값에 대해 **Used** 메모리에 일관되지 않은 유닛이 표시되었으며 예측할 수 없고 읽기 어려웠습니다. 이번 수정을 통해 이제 **Used** 메모리에서 항상 **Hard** 메모리와 동일한 유닛을 사용하므로 **oc describe quota** 명령에서 예측 가능한 값을 표시합니다. (BZ#1955292)
- 이전에는 클라이언트 설정이 누락되어 **oc logs** 명령이 파이프라인 빌드에서 작동하지 않았습니다. 이제 파이프라인 빌드와 함께 작동하도록 **oc logs** 명령에서 클라이언트 설정이 수정되었습니다. (BZ#1973643)

## OLM(Operator Lifecycle Manager)

- 이전에는 설치된 Operator가 **olm.maxOpenShiftVersion**을 현재 버전보다 작거나 같은 OpenShift Container Platform 마이너 버전으로 설정한 경우 OLM(Operator Lifecycle Manager) 업그레이드 가능 상태 메시지가 명확하게 표시되지 않았습니다. 이로 인해 **olm.maxOpenShiftVersion**이 현재 OpenShift Container Platform 버전과 다르게 설정된 경우 마이너 버전 및 주요 버전 업그레이드만 차단되도록 수정된 잘못된 오류 메시지가 발생했습니다. ([BZ#1992677](#))
- 이전에는 **opm** 명령이 인덱스에 있을 때 번들을 사용 중단하지 못했습니다. 결과적으로 동일한 호출에서 다른 사용 중단의 일부로 잘린 번들이 누락됨으로 보고되었습니다. 이번 업데이트에서는 더 이상 사용되지 않는 번들과 잘린 번들을 구분하기 위해 사용 중단이 발생하기 전에 번들에 대한 검사를 추가합니다. 결과적으로 동일한 업그레이드 경로를 통해 더 이상 사용되지 않는 번들이 누락된 것으로 보고되지 않습니다. ([BZ#1950534](#))
- OLM(Operator Lifecycle Manager)이 클러스터에서 CRD(사용자 정의 리소스 정의) 오브젝트를 업데이트하려고 하면 일시적인 오류가 발생할 수 있었습니다. 이로 인해 OLM이 CRD를 포함하는 설치 계획에 영구적으로 실패했습니다. 이번 버그 수정에서는 리소스 수정 충돌 오류에 대한 CRD 업데이트를 재시도하도록 OLM이 업데이트되었습니다. 결과적으로 OLM은 이러한 일시적인 오류에 대해 보다 탄력적으로 대응할 수 있게 되었습니다. OLM에서 재시도하고 해결할 수 있는 충돌 오류에 대해 설치 계획이 더 이상 영구적으로 실패하지 않습니다. ([BZ#1923111](#))
- **opm index|registry add** 명령은 인덱스에서 이미 잘렸는지 여부와 관계없이 교체된 인덱스에 Operator 번들이 있는지 확인하려고 시도했습니다. 해당 패키지에 대해 번들이 더 이상 사용되지 않는 경우에도 명령이 지속적으로 실패합니다. 이 버그 수정에서는 이 예외 케이스를 처리하도록 **opm** CLI를 업데이트하고 더 이상 잘린 번들이 있는지 확인하지 않습니다. 따라서 지정된 패키지에 대해 번들이 더 이상 사용되지 않으면 명령이 더 이상 실패하지 않습니다. ([BZ#1952101](#))
- OLM(Operator Lifecycle Manager)에서 카탈로그 소스 리소스의 레이블을 사용하여 우선순위 클래스를 레지스트리 Pod로 프로젝션할 수 있습니다. 기본 카탈로그 소스는 클러스터에서 관리하는 네임스페이스에서 중요한 구성 요소이며 우선순위 클래스를 지정합니다. 이번 개선된 기능을 통해 **openshift-marketplace** 네임스페이스의 모든 기본 카탈로그 소스에는 **system-cluster-critical** 우선순위 클래스가 있습니다. ([BZ#1954869](#))
- Marketplace Operator는 임대 소유자의 ID를 보유하는 구성 맵에 컨트롤러 Pod에 의해 배치된 소유자 참조가 있는 leader-for-life 구현을 사용하고 있었습니다. 이는 Pod가 예약된 노드를 사용할 수 없게 되어 Pod를 종료할 수 없는 경우 문제가 됩니다. 이로 인해 구성 맵이 올바르게 가비지 수집되지 않아 새 리더가 선택될 수 있었습니다. 최신 Marketplace Operator 버전이 리더를 선택할 수 없으므로 마이너 버전 클러스터 업그레이드가 차단되었습니다. 잠금을 해제하고 Marketplace 구성 요소의 업그레이드를 완료하려면 리더 선택 리스를 포함하는 구성 맵을 수동으로 정리해야 했습니다. 이 버그 수정을 통해 leader-for-lease 리더 선택 구현을 사용하도록 전환됩니다. 그 결과 리더 선택이 더 이상 이 시나리오로 되지 않습니다. ([BZ#1958888](#))
- 이전에는 설치 계획에 대한 새로운 **Failed** 단계가 도입되었습니다. 설치 계획이 생성된 네임스페이스에 대해 유효한 OG(Operator group) 또는 서비스 계정(SA) 리소스를 검색하지 못하면 설치 계획이 실패 상태로 전환됩니다. 즉, 설치 계획이 처음으로 조정되었을 때 이러한 리소스를 감지하지 못하는 것은 영구적인 실패로 간주되었습니다. 이는 다음과 같은 설치 계획의 이전 동작에서 회귀한 것입니다.
  - OG 또는 SA 리소스를 감지하지 못하면 조정 계획을 다시 큐에 추가합니다.
  - 번들 압축 해제 단계가 실패하지 않는 한 정보 제공 큐의 재시도 제한에 도달하기 전에 필요한 리소스를 생성하면 **Installing** 계획이 설치 단계에서 **Complete** 단계로 전환됩니다.

이러한 회귀 문제로 인해 필요한 OG 및 SA 리소스와 함께 설치 계획을 생성하는 Operator를 설치하기 위해 매니페스트 세트를 동시에 적용한 사용자에게는 비정상적인 동작이 발생했습니다. 이러한 경우 OG와 SA 조정에 지연이 발생할 때마다 설치 계획이 영구 오류 상태로 전환됩니다.



이번 버그 수정을 통해 설치 계획을 **Failed** 단계로 전환한 논리가 제거됩니다. 대신 조정 오류에 대해 설치 계획이 다시 큐에 추가됩니다. 결과적으로 OG가 탐지되지 않으면 다음 조건이 설정됩니다.

```
conditions:
- lastTransitionTime: ""2021-06-23T18:16:00Z""
lastUpdateTime: ""2021-06-23T18:16:16Z""
message: attenuated service account query failed - no operator group found that
is managing this namespace
reason: InstallCheckFailed
status: ""False""
type: Installed
```

유효한 OG가 생성되면 다음 조건이 설정됩니다.

```
conditions:
- lastTransitionTime: ""2021-06-23T18:33:37Z""
lastUpdateTime: ""2021-06-23T18:33:37Z""
status: ""True""
```

#### ([BZ#1960455](#))

- 카탈로그 소스를 업데이트할 때 **Get** 호출은 카탈로그 소스와 관련된 여러 리소스에 대한 **Delete** 호출이 즉시 이어집니다. 경우에 따라 리소스가 이미 삭제되었지만 리소스는 여전히 캐시에 존재했습니다. 이로 인해 **Get** 호출이 성공적으로 수행되었지만 클러스터에 리소스가 없으므로 다음 **Delete** 호출이 실패했습니다. 이번 버그 수정에서는 리소스를 찾을 수 없는 경우 **Delete** 호출에서 반환된 오류를 무시하도록 OLM(Operator Lifecycle Manager)을 업데이트합니다. 결과적으로 OLM에서 **Delete** 호출에서 "Resource Not Found" 오류가 발생하는 캐싱 문제로 인해 카탈로그 소스를 업데이트할 때 더 이상 오류를 보고하지 않습니다. ([BZ#1967621](#))
- 63자 제한을 초과하는 이름의 CSV(클러스터 서비스 버전)로 인해 잘못된 **ownerref** 레이블이 발생합니다. 이전 버전에서는 OLM(Operator Lifecycle Manager)에서 **ownerref** 참조를 사용하여 클러스터 역할 바인딩을 비롯한 소유된 리소스를 검색할 때 목록에서 잘못된 레이블로 인해 네임스페이스의 모든 클러스터 역할 바인딩을 반환했습니다. 이번 버그 수정에서는 다른 방법을 사용하여 OLM을 업데이트하여 서버가 잘못된 **ownerref** 레이블을 거부하도록 합니다. 결과적으로 CSV에 잘못된 이름이 있으면 OLM에서 더 이상 클러스터 역할 바인딩을 제거하지 않습니다. ([BZ#1970910](#))
- 이전에는 설치 시간 후에 Operator 종속 항목이 항상 유지되지 않았습니다. 종속성을 선언하는 Operator를 설치한 후 동일한 네임스페이스 내에서 나중에 업데이트 및 설치하면 이전에 설치된 Operator의 종속성을 준수하지 못할 수 있습니다. 이번 버그 수정으로 Operator의 **ClusterServiceVersion** (CSV) 오브젝트의 주석에서 Operator의 선언된 모든 속성과 함께 종속성이 유지됩니다. 결과적으로 설치된 Operator의 선언된 종속 항목은 향후 설치 시 계속 유지됩니다. ([BZ#1978310](#))
- 이전 버전에서는 더 이상 사용되지 않는 번들을 사용하여 Operator를 제거하면 사용 중단 내역이 가비지 컬렉션에 포함되지 않았습니다. 결과적으로 Operator를 다시 설치하는 경우 번들 버전에 더 이상 사용되지 않는 테이블이 표시되었습니다. 이번 업데이트에서는 더 이상 사용되지 않는 번들의 가비지 컬렉션이 개선되어 문제가 해결되었습니다. ([BZ#1982781](#))
- 이전에는 클러스터의 z-stream 버전이 Operator 호환성 계산에 사용되었습니다. 결과적으로 OpenShift Container Platform의 마이크로 릴리스가 차단되었습니다. 이번 업데이트에서는 Operator 호환성 비교에서 클러스터 z-stream 버전을 무시하여 문제가 해결되었습니다. ([BZ#1993286](#))

- 이전에는 서비스의 검색 끝점에 대한 단일 실패 요청으로 Operator에서 **Available=False**를 보고 할 수 있었습니다. 복원력을 높이기 위해 일부 Operator가 다양한 일시적인 오류로 인해 업데이트 중에 **Available=False**를 보고하지 못하도록 개선 사항이 추가되었습니다. ([BZ#1948089](#))

### OpenShift 업데이트 서비스

- 이전에는 웹 콘솔을 통해 업데이트 서비스 애플리케이션을 생성할 때 잘못된 호스트 오류가 발생했습니다. 이는 기본 OSUS(OpenShift Update Service) 애플리케이션 이름이 너무 길기 때문에 발생했습니다. 이제 더 짧은 기본 이름이 표시되어 더 이상 오류가 발생하지 않습니다. ([BZ#1939788](#))

### Performance Addon Operator

OpenShift Container Platform 4.9에서 Performance Addon Operator에 대한 다음 업데이트를 사용할 수 있습니다.

- 이전에는 대역폭 제한 연결이 있는 환경에서 Performance Addon Operator를 제대로 다시 시작할 수 없었습니다. 단일 노드 클러스터 또는 기타 예지 노드에서 이미지 레지스트리에 대한 연결이 끊어진 경우에도 제대로 다시 시작할 수 없었습니다. 이번 업데이트를 통해 노드에서 이미지를 이미 사용할 수 있는 경우 **registry.redhat.io** 에서 이미지를 가져오지 않도록 하면 문제가 해결됩니다. 이번 수정을 통해 Performance Addon Operator가 로컬 이미지 캐시의 이미지를 사용하여 올바르게 다시 시작됩니다. ([BZ#2055019](#))

### RHCOS(Red Hat Enterprise Linux CoreOS)

- 이전에는 systemd가 **/etc/kubernetes**의 환경 파일을 읽을 수 없었습니다. SELinux 정책으로 인해 이 문제가 발생하여 kubelet이 시작되지 않았습니다. 정책이 수정되었습니다. kubelet이 시작되고 환경 파일을 읽을 수 있습니다. ([BZ#1969998](#))
- ECKD DASD가 연결된 s390x KVM(커널 가상 시스템)에서 DASD는 일반 virtio 스토리지 장치인 것처럼 보이지만 VTOC가 제거된 경우 액세스할 수 없게 됩니다. 결과적으로 KVM에 RHCOS(Red Hat Enterprise Linux CoreOS)를 설치할 때 DASD를 virtio 블록 장치로 사용할 수 없었습니다. **coreos-installer** 프로그램이 업데이트되어 설치 대상이 KVM에 연결된 ECKD DASD와 같은 virtio 스토리지 장치인 경우 VTOC 형식 파티션 테이블이 있는 RHCOS(Red Hat Enterprise Linux CoreOS)를 설치합니다. ([BZ#1960485](#))
- 이전에는 **NetworkManager-wait-online-service**가 너무 빨리 시간 초과되어 **coreos-installer** 프로그램이 시작되기 전에 연결을 설정할 수 없었습니다. 결과적으로 네트워크를 시작하는 데 시간이 너무 오래 걸리는 경우 **coreos-installer** 프로그램에서 Ignition 구성을 가져오지 못했습니다. 이번 업데이트를 통해 **NetworkManager-wait-online-service** 시간 제한이 기본 업스트림 값으로 증가했습니다. 결과적으로 **coreos-installer** 프로그램에서 더 이상 Ignition 구성을 가져오지 못합니다. ([BZ#1967483](#))

### 라우팅

- 이전에는 CNO(Cluster Network Operator)가 프록시 구성을 삭제하려고 할 때 특히 **no\_proxy** 구성을 삭제하려고 할 때 구성 드리프트가 있었습니다. 이로 인해 **no\_proxy**에서 특정 IPv6 CIDR이 누락되었습니다. 이번 수정에서는 모든 시나리오에 듀얼 스택(IPV4 및 IPV6)을 업데이트하는 로직이 구현되었습니다. ([BZ#1981975](#))
- 이전에는 **dns.config.openshift.io** Operato의 **.spec.privateZone** 필드가 잘못 입력되어 Ingress Operator가 프라이빗 호스팅 영역을 찾을 수 없는 경우 Ingress Operator의 성능이 저하되었습니다. 그러나 **.spec.privateZone** 필드를 수정한 후에도 Ingress Operator의 성능이 저하되었습니다. Ingress Operator는 호스팅 영역을 찾고 **.apps** 리소스 레코드를 추가하지만 Ingress Operator는 성능이 저하된 상태를 재설정하지 않습니다. 이번 수정에서는 DNS 구성 오브젝트를 감시하고 **spec.privateZone** 필드와 관련된 변경 사항을 모니터링합니다. 이로 인해 적절한 논리를 적용하고 Operator 상태를 적절하게 업데이트합니다. 올바른 **.spec.privateZone** 필드가 설정되면 Operator 상태는 성능이 저하되거나 **False**로 돌아갑니다. ([BZ#1942657](#))

## 샘플

- 이전에는 연결 시간 초과가 부족하여 지연 시간이 길어졌습니다. 이는 **managementState**가 **Removed**로 설정된 Cluster Samples Operator에서 **registry.redhat.io**에 대한 연결을 테스트한 경우 발생했습니다. 연결 시간 초과를 추가하면 지연이 제거됩니다. ([BZ#1990140](#))

## 스토리지

- 이전에는 수동 정리가 필요한 사용 중인 PV가 있는 **LocalVolumeSet**을 삭제할 수 있었습니다. 이번 수정을 통해 릴리스된 모든 PV가 자동으로 정리됩니다. ([BZ#1862429](#))
- 이전에는 **oc get volumesnapshotcontent** 명령에서 볼륨 스냅샷의 네임스페이스를 표시하지 않았습니니다. 이로 인해 볼륨 스냅샷이 고유하게 식별되지 않았습니니다. 이제 이 명령은 볼륨 스냅샷의 네임스페이스를 표시합니다. ([BZ#1965263](#))
- 이전에는 Manila CSI Operator에서 자체 서명 인증서를 사용하는 RHOSP(Red Hat OpenStack Platform) 끝점과 통신할 때 사용자 정의 전송을 사용했습니다. 이 사용자 정의 전송에서 프록시 환경 변수를 사용하지 않았기 때문에 Manila CSI Operator가 Manila와 통신하지 못했습니다. 이번 업데이트를 통해 사용자 정의 전송에서 프록시 환경 변수를 사용할 수 있습니다. 결과적으로 Manila CSI Operator가 프록시 및 사용자 정의 CA 인증서와 함께 작동합니다. ([BZ#1960152](#))
- 이전 버전에서는 Cinder CSI Driver Operator에서 RHOSP(Red Hat OpenStack Platform) API에 연결하는 데 구성된 프록시를 사용하지 않아 설치가 실패할 수 있었습니다. 이번 업데이트를 통해 Cinder CSI Driver Operator 배포에 주석이 포함되어 프록시 환경 변수가 컨테이너에 설정됩니다. 결과적으로 설치에 더 이상 실패하지 않습니다. ([BZ#1985391](#))
- Local Storage Operator에서 새로 추가된 블록 장치를 검사하는 빈도가 5초에서 60초로 변경되었습니다. ([BZ#1994035](#))
- 이전에는 Manila CSI Operator와의 통신 실패로 클러스터 성능이 저하되었습니다. 이번 업데이트를 통해 Manila CSI Operator 끝점과의 통신 실패로 인해 치명적이지 않은 오류가 발생합니다. 결과적으로 클러스터를 저하시키는 대신 Manila CSI Operator가 비활성화됩니다. ([BZ#2001958](#))
- 이전에는 Local Storage Operator에서 분리된 PV(영구 볼륨)를 10초 지연으로 삭제하고 지연이 누적되었습니다. 여러 PVC(영구 볼륨 클레임)를 동시에 삭제하면 PV를 삭제하는 데 몇 분 또는 시간이 걸릴 수 있습니다. 결과적으로 새 PVC에서 해당 로컬 디스크를 여러 시간 동안 사용할 수 없었습니다. 이번 수정을 통해 10초 지연이 제거됩니다. 결과적으로 PV가 감지되고 해당 로컬 디스크를 새 PVC에 더 빨리 사용할 수 있게 됩니다. ([BZ#2007684](#))

## 웹 콘솔(관리자 화면)

- 이전에는 **PF4** 테이블의 모든 행이 다시 렌더링되었습니다. 이번 업데이트를 통해 **React.memo**의 콘텐츠가 래핑되어 모든 스크롤 이벤트에서 콘텐츠가 다시 렌더링되지 않습니다. ([BZ#1856355](#))
- 이전에는 OpenShift Container Platform 웹 콘솔의 **클러스터 사용률** 차트에서 데이터 시간이 혼동되는 방식으로 표시되었습니다. 예를 들어, 6시간 동안의 시간 범위 옵션을 선택했지만 마지막 3시간 동안만 데이터가 있는 경우 해당 세 개의 데이터 지점이 전체 차트를 채우도록 확장되었습니다. 처음 3시간은 표시되지 않았습니다. 이 경우 차트가 전체 6시간 동안의 시간 범위로 표시된 것으로 가정할 수 있었습니다. 혼동을 피하기 위해 이제 차트에 누락된 정보에 대한 빈 공간이 표시됩니다. 이 예에서 차트는 4시간부터 시작하는 데이터와 함께 전체 6시간 동안의 범위를 표시합니다. 처음 3시간은 비어두게 됩니다. ([BZ#1904155](#))
- 이전에는 **NetworkPolicy**가 웹 콘솔에서 한국어 또는 중국어로 번역되어 있지 않았습니다. 이번 업데이트를 통해 한국어 또는 중국어로 웹 콘솔을 볼 때 **NetworkPolicy**가 올바르게 번역됩니다. ([BZ#1965930](#))

- 이전 버전에서는 콘솔 개요 섹션의 **Needs Attention** 상태 문제에서 Operator가 업그레이드되지 않았더라도 Operator가 **upgrading**으로 표시되었습니다. 이번 업데이트에서는 Operator의 올바른 상태가 표시되도록 **Needs Attention** 상태가 수정되었습니다. ([BZ#1967047](#))
- 이전에는 CSV(클러스터 서비스 버전)에 대한 경고에 실패한 CSV 문제를 해결하는 데 도움이 되지 않은 일반 **status.message**가 표시되었습니다. 이번 업데이트를 통해 CSV 복사본에는 유용한 메시지와 문제 해결을 위한 원본 CSV에 대한 링크가 표시됩니다. ([BZ#1967658](#))
- 이전에는 사용자가 키보드로 마스트 헤드의 드롭다운 옵션을 사용할 수 없었습니다. 이번 업데이트를 통해 이제 사용자가 키보드를 사용하여 드롭다운 옵션에 액세스할 수 있습니다. ([BZ#1967979](#))
- 이전에는 Operator 소유 리소스를 해당 소유자와 일치시키는 데 사용된 유틸리티 함수가 잘못된 일치 항목을 반환했습니다. 이로 인해 Operator 소유 리소스 페이지의 **Managed by** 링크가 잘못된 URL로 연결되는 경우가 있었습니다. 이번 수정에서는 함수 논리가 소유 Operator와 올바르게 일치하도록 업데이트되었습니다. 결과적으로 **Managed by** 링크는 이제 올바른 URL에 연결됩니다. ([BZ#1970011](#))
- 이전에는 **OperatorHub** 웹 콘솔 인터페이스로 인해 사용자가 관련이 없는 설치 계획을 수행하도록 유도했습니다. 이번 업데이트를 통해 **OperatorHub**는 사용자를 Operator 서브스크립션 세부 정보 탭으로 연결하여 설치 진행 상황을 확인합니다. ([BZ#1970466](#))
- 이전에는 **OAuth** 세부 정보 페이지의 추가 드롭다운 목록에 있는 항목이 국제화되지 않았습니다. 이번 업데이트를 통해 이러한 항목이 국제화되고 비영어 사용자를 위한 사용자 환경이 개선되었습니다. ([BZ#1970604](#))
- 이전에는 잘못된 로컬라이제이션 속성으로 인해 일부 메시지가 국제화되지 않았습니다. 이번 업데이트에서는 잘못된 속성이 제거되었습니다. 결과적으로 이러한 메시지는 국제화되고 비영어 사용자를 위한 사용자 환경이 개선되었습니다. ([BZ#1970980](#))
- 이번 업데이트에서는 사용자 환경이 개선되지 않았기 때문에 목록 페이지의 리소스 링크를 사용할 때 표시되는 툴팁이 제거되었습니다. ([BZ#1971532](#))
- 이전 버전에서는 콘솔 Pod가 **preferredDuringSchedulingIgnoredDuringExecution** 유사성 방지 규칙을 사용하여 배포되어 두 콘솔 Pod가 동일한 컨트롤 플레인 노드에 예약되었습니다. 이번 수정을 통해 **requiredDuringSchedulingIgnoredDuringExecution** 규칙이 변경되어 조건이 일치하는 경우 다른 노드에서 Pod를 예약해야 합니다. ([BZ#1975379](#))
- 이전에는 Operator를 설치 제거하여 활성화된 모든 플러그인을 제거하지 못했습니다. 이번 릴리스에서는 Operator를 설치 제거하면 활성화된 모든 플러그인이 제거됩니다. ([BZ#1975820](#))
- 이전 버전에서는 프런트 엔드 OLM(Operator Lifecycle Manager) 설명자 처리에서 첫 번째 x-descriptor만 사용하여 operand 세부 정보 페이지에서 속성을 렌더링했습니다. 결과적으로 여러 x-descriptors가 속성에 정의되어 있고 목록의 첫 번째 항목이 유효하지 않거나 지원되지 않는 경우 예상대로 렌더링되지 않았습니다. 이번 수정에서는 지원되지 않는 x-descriptors보다 지원되는 x 설명자를 우선순위화하도록 디스크립터 유효성 검사 논리가 업데이트되었습니다. 그 결과 목록에 있는 첫 번째 유효한 지원 x-descriptor를 사용하여 descriptor-decorated 속성이 **Operand** 세부 정보 페이지에서 렌더링됩니다. ([BZ#1976072](#))
- 이전에는 문자열 데이터가 인코딩된 시크릿에 사용되었습니다. 결과적으로 웹 콘솔에서 바이너리 시크릿 데이터가 제대로 업로드되지 않았습니다. 이번 업데이트에서는 시크릿을 인코딩하고 API의 문자열 데이터 대신 데이터를 사용합니다. 결과적으로 바이너리 시크릿이 올바르게 업로드됩니다. ([BZ#1978724](#))
- 이전에는 클러스터에서 실행 중인 프로세스가 수동으로 종료될 때 **ps -aux** 명령이 일부 프로세스가 지워지지 않은 것으로 표시되었습니다. 이로 인해 스트레이 프로세스가 남아 클러스터가 잘못된 상태가 됩니다. 이번 수정을 통해 모든 프로세스가 클러스터에서 제대로 종료되고 터미널에 나

열린 활성 프로세스 목록에 표시되지 않습니다. (BZ#1979571)

- 이전 버전에서는 새 프로젝트에 기본 풀 시크릿을 추가하고 여러 레지스트리의 인증 정보를 업로드할 때 첫 번째 인증 정보만 **Project Details** 페이지에 나열되었습니다. 또한 목록이 잘린 것을 표시하지 않았습니다. 그 결과 사용자가 **Default pull secret**에서 프로젝트 세부 정보를 클릭하면 첫 번째 인증 정보만 나열되었습니다. 이번 수정을 통해 모든 인증 정보가 나열되고, 사용자에게 현재 페이지에 나열되지 않은 경우 추가 인증 정보가 있음을 알립니다. (BZ#1980704)
- 이전 버전에서는 사용자가 기본 브라우저 언어를 중국어 간체로 변경하면 웹 콘솔의 **개요** 페이지에 영어 및 중국어 간체가 함께 표시되었습니다. 이번 수정을 통해 사용자는 선택한 언어로 클러스터 사용률 리소스를 전체적으로 볼 수 있습니다. (BZ#1982079)
- 이전에는 언어가 중국어 간체로 변경되었을 때 클러스터 사용률 통계가 **project, pod, node**의 왼쪽 메뉴에서 변환되지 않았습니다. 이번 업데이트에서는 클러스터 사용률 매트릭이 **top consumers** 필터와 일치하도록 중국어 간체 변환이 수정되었습니다. (BZ#1982090)
- 이전에는 서비스 계정에서 기본 풀 시크릿 대신 오류가 발생했습니다. 이로 인해 프로젝트 세부 정보 화면에 불완전한 정보가 표시되었습니다. 사용자는 기본 가져오기 보안의 전체 목록을 보려면 기본 ServiceAccount로 이동해야 했습니다. 이번 업데이트를 통해 사용자는 프로젝트 세부 정보 페이지의 기본 ServiceAccount에서 전체 풀 시크릿 목록을 볼 수 있습니다. (BZ#1983091)
- 이전에는 터미널 탭을 보는 동안 노드 또는 pod의 웹 페이지의 크기를 조정할 경우 브라우저에 두 개의 수직 스크롤 막대가 표시되는 경우가 있었습니다. 이제 창의 크기를 조정할 때만 스크롤바를 표시하도록 콘솔이 업데이트되었습니다. (BZ#1983220)
- 이전에는 단일 노드 개발자 프로필을 사용하여 OpenShift Container Platform 4.8.2를 설치할 때 웹 콘솔이 배포되지 않았습니다. 설치 계획이 생성된 네임스페이스에 대해 유효한 Operator 그룹 또는 서비스 계정이 감지되지 않으면 설치 계획이 실패 상태가 되었습니다. 추가 시도가 이루어지지 않았습니다. 이번 업데이트에서는 Operator 그룹 또는 서비스 계정이 감지될 때까지 실패한 설치 계획이 다시 실행되도록 설정됩니다. (BZ#1986129)
- 이전에는 **이벤트 대시보드**에서 **More** 및 **Show Less**가 국제화되지 않아 사용자 환경이 좋지 않았습니다. 이번 업데이트를 통해 텍스트가 국제화되었습니다. (BZ#1986754)
- 이전에는 콘솔 페이지에서 서비스의 FQDN(정규화된 도메인 이름)을 작성한 논리가 누락되었습니다. 이로 인해 서비스 세부 정보 페이지에서 FQDN 정보가 누락되었습니다. 이번 업데이트에서는 FQDN을 구성하는 논리가 추가되어 이제 페이지에서 서비스의 FQDN 정보를 사용할 수 있습니다. (BZ#1996816)

### 웹 콘솔 (개발자 화면)

- 이전에는 소스 kamelet과 함께 이벤트 소스의 카탈로그에 유형 **sink**의 kamelets가 표시되었습니다. 현재 릴리스에서 이벤트 소스의 카탈로그는 유형 **source**의 kamelets만 표시됩니다. (BZ#1971544)
- 이전에는 로그 파일에 줄 바꿈 없이 한 줄에 정보가 포함되어 있었습니다. 현재 릴리스에서는 로그 파일에 로그 헤더 주위에 줄 바꿈과 함께 예상되는 줄 바꿈이 포함되어 있습니다. (BZ#1985080)

## 1.7. 기술 프리뷰 기능

이 릴리스의 일부 기능은 현재 기술 프리뷰 단계에 있습니다. 이러한 실험적 기능은 프로덕션용이 아닙니다. 해당 기능은 Red Hat Customer Portal의 지원 범위를 참조하십시오.

### 기술 프리뷰 기능 지원 범위

아래 표에서 기능은 다음 상태로 표시됩니다.

- **TP:** 기술 프리뷰
- **GA:** 상용 버전
- **-:** 사용할 수 없음
- **DEP:** 더 이상 사용되지 않음

표 1.3. 기술 프리뷰

기능	OCP 4.7	OCP 4.8	OCP 4.9
일반 시계로 구성된 PTP(Precision Time Protocol) 하드웨어	TP	GA	GA
PTP 단일 NIC 하드웨어는 경계 클럭으로 구성됩니다.	-	-	TP
일반 시계가 있는 PTP 이벤트	-	-	TP
<b>oc</b> CLI 플러그인	TP	GA	GA
Descheduler	GA	GA	GA
메모리 활용을 위한 HPA	GA	GA	GA
서비스 바인딩	TP	TP	TP
Cinder 포함 원시 블록	TP	GA	GA
CSI 블록 스냅샷	GA	GA	GA
CSI 블록 확장	TP	TP	TP
vSphere Problem Detector Operator	GA	GA	GA
CSI Azure Disk Driver Operator	-	TP	TP
CSI Azure Stack Hub Driver Operator	-	-	GA
CSI GCP PD Driver Operator	TP	GA	GA
CSI OpenStack Cinder Driver Operator	GA	GA	GA
CSI AWS EBS Driver Operator	TP	TP	GA
CSI AWS EFS Driver Operator	-	-	TP
CSI 자동 마이그레이션	-	TP	TP
CSI 인라인 임시 블록	TP	TP	TP


기능	OCP 4.7	OCP 4.8	OCP 4.9
CSI vSphere Driver Operator	-	TP	TP
Local Storage Operator를 통한 자동 장치 검색 및 프로비저닝	TP	TP	TP
OpenShift Pipelines	TP	GA	GA
OpenShift GitOps	TP	GA	GA
OpenShift 샌드박스 컨테이너	-	TP	TP
Vertical Pod Autoscaler	TP	GA	GA
Cron 작업	TP	GA	GA
PodDisruptionBudget	TP	GA	GA
kvc로 노드에 커널 모듈 추가	TP	TP	TP
egress 라우터 CNI 플러그인	TP	GA	GA
스케줄러 프로파일	TP	TP	GA
선점되지 않은 우선 순위 클래스	TP	TP	TP
Kubernetes NMState Operator	TP	TP	TP
지원되는 설치 관리자	TP	TP	TP
AWS STS(보안 토큰 서비스)	TP	GA	GA
Kdump	TP	TP	TP
OpenShift Serverless	-	GA	GA
서버리스 기능	-	TP	TP
DPDK(Data Plane Development Kit) 지원	TP	TP	GA
메모리 관리자	-	-	GA
CNI VRF 플러그인	TP	TP	GA
Cluster Cloud Controller Manager Operator	-	-	GA
AWS의 클라우드 컨트롤러 관리자	-	-	TP

기능	OCP 4.7	OCP 4.8	OCP 4.9
Azure의 클라우드 컨트롤러 관리자	-	-	TP
OpenStack용 클라우드 컨트롤러 관리자	-	-	TP
CPU 관리자	GA	GA	GA
드라이버 툴킷	-	TP	TP
SRO(Special Resource Operator)	-	-	TP
Node Health Check Operator	-	-	TP

### 1.8. 확인된 문제

- OpenShift Container Platform 4.1에서는 익명 사용자가 검색 엔드 포인트에 액세스할 수 있었습니다. 이후 릴리스에서는 일부 검색 끝점이 통합된 API 서버로 전달되기 때문에 보안 악용에 대한 가능성을 줄이기 위해 이 액세스를 취소했습니다. 그러나 인증되지 않은 액세스는 기존 사용 사례가 손상되지 않도록 업그레이드된 클러스터에 보존됩니다.

OpenShift Container Platform 4.1에서 4.9로 업그레이드된 클러스터의 클러스터 관리자인 경우 인증되지 않은 액세스를 취소하거나 계속 허용할 수 있습니다. 특별히 필요한 경우가 아니면 인증되지 않은 액세스를 취소하는 것이 좋습니다. 인증되지 않은 액세스를 계속 허용하는 경우 이에 따라 보안 위험이 증가될 수 있다는 점에 유의하십시오.



**주의**

인증되지 않은 액세스에 의존하는 애플리케이션이 있는 경우 인증되지 않은 액세스를 취소하면 HTTP **403** 오류가 발생할 수 있습니다.

다음 스크립트를 사용하여 감지 끝점에 대한 인증되지 않은 액세스를 취소하십시오.

```
## Snippet to remove unauthenticated group from all the cluster role bindings
$ for clusterrolebinding in cluster-status-binding discovery system:basic-user
system:discovery system:openshift:discovery ;
do
### Find the index of unauthenticated group in list of subjects
index=$(oc get clusterrolebinding ${clusterrolebinding} -o json | jq 'select(.subjects!=null) |
.subjects | map(.name=="system:unauthenticated") | index(true)');
### Remove the element at index from subjects array
oc patch clusterrolebinding ${clusterrolebinding} --type=json --patch "[{'op': 'remove','path':
'/subjects/${index}'}]";
done
```

이 스크립트는 인증되지 않은 주제를 다음 클러스터 역할 바인딩에서 제거합니다.



- **cluster-status-binding**
- **discovery**
- **system:basic-user**
- **system:discovery**
- **system:openshift:discovery**

([BZ#1821771](#))

- OpenShift Container Platform 4.9로 업그레이드할 때 Cluster Version Operator는 사전 조건 검사에 실패하는 동안 약 5분 동안 업그레이드를 차단합니다. **It may not be safe to apply this update**라는 오류 텍스트는 잘못된 것일 수 있습니다. 이 오류는 하나 또는 여러 개의 사전 조건 검사에 실패할 때 발생합니다. 경우에 따라 이러한 사전 조건 검사는 예를 들어 etcd 백업 중에 단기간 동안만 실패할 수 있습니다. 이러한 경우 Cluster Version Operator 및 해당 Operator는 설계에 따라 실패한 사전 조건 검사를 자동으로 해결하며 CVO가 업그레이드를 성공적으로 시작합니다. 사용자는 클러스터 Operator의 상태 및 조건을 확인해야 합니다. Cluster Version Operator에서 **It may not be safe to apply this update** 오류가 표시되는 경우 이러한 상태 및 조건이 메시지의 심각도에 대한 자세한 정보를 제공합니다. 자세한 내용은 [BZ#1999777](#), [BZ#2061444](#), [BZ#2006611](#) 을 참조하십시오.
- 명령이 주석 이름과 값 간의 구분 기호로 등호(=)를 포함하는 LDAP 그룹 이름에 대해 **oc annotate** 명령은 작동하지 않습니다. 이 문제를 해결하려면 **oc patch** 또는 **oc edit**를 사용하여 주석을 추가합니다. ([BZ#1917280](#))
- 클러스터 관리자는 503, 404 또는 두 오류 페이지의 사용자 정의 HTTP 오류 코드 응답 페이지를 지정할 수 있습니다. 사용자 정의 오류 코드 응답 페이지에 올바른 형식을 지정하지 않으면 라우터 Pod 중단이 발생하고 해결되지 않습니다. 사용자 지정 오류 코드 페이지가 업데이트되도록 라우터가 다시 로드되지 않습니다. 이 문제를 해결하려면 **oc rsh** 명령을 사용하여 라우터 Pod에 로컬로 액세스할 수 있습니다. 그런 다음 사용자 정의 http 오류 코드 페이지를 제공하는 모든 라우터 Pod에서 **reload-haproxy**를 실행합니다.

```
$ oc -n openshift-ingress rsh router-default-6647d984d8-q7b58
sh-4.4$ bash -x /var/lib/haproxy/reload-haproxy
```

또는 경로에 주석을 추가하여 강제로 다시 로드할 수 있습니다. ([BZ#1990020](#)), ([BZ#2003961](#))

- OVN(Open Virtual Network) 버그로 인해 Octavia 로드 밸런서에 지속적으로 연결 문제가 발생합니다. Octavia 로드 밸런서가 생성되면 OVN을 일부 Neutron 서브넷에 연결하지 못할 수 있습니다. 이러한 로드 밸런서는 일부 Neutron 서브넷에 연결할 수 없습니다. 이 문제는 Kuryr를 구성할 때 각 OpenShift 네임스페이스에 대해 임의로 생성되는 Neutron 서브넷에 영향을 미칩니다. 결과적으로 이 문제가 발생하면 OpenShift **Service** 오브젝트를 구현하는 로드 밸런서가 문제의 영향을 받는 OpenShift 네임스페이스에서 연결할 수 없습니다. 이 버그로 인해 OVN 및 OVN Octavia가 구성된 RHOSP(Red Hat OpenStack Platform) 16.1에서는 Kuryr SDN을 사용하는 OpenShift Container Platform 4.8 배포가 권장되지 않습니다. 이 문제는 향후 RHOSP 릴리스에서 해결될 예정입니다. ([BZ#1937392](#))
- 클러스터 전체 프록시가 RHOSP API에 액세스해야 하는 경우 Kuryr를 사용하는 RHOSP(Red Hat OpenStack Platform)에 설치된 클러스터 전체 프록시로 구성되지 않습니다. ([BZ#1985486](#))
- 경쟁 조건으로 인해 RHOSP(Red Hat OpenStack Platform) 클라우드 공급자가 제대로 시작되지 않을 수 있습니다. 결과적으로 LoadBalancer 서비스에 **EXTERNAL-IP** 세트를 가져오지 못할 수 있습니다. 임시 해결 방법으로 [BZ#2004542](#)에 설명된 절차를 사용하여 kube-controller-manager Pod를 다시 시작할 수 있습니다.

- **ap-northeast-3** AWS 리전은 지원되는 AWS 리전인 경우에도 OpenShift Container Platform을 설치할 때 설치 프로그램에서 옵션으로 제공되지 않습니다. 임시 해결 방법으로 설치 프롬프트에서 다른 AWS 리전을 선택한 다음 클러스터를 설치하기 전에 생성된 **install-config.yaml** 파일에서 지역 정보를 업데이트할 수 있습니다. ([BZ#1996544](#))
- **us-east-1** 리전의 AWS에 클러스터를 설치할 때 로컬 AWS 영역을 사용할 수 없습니다. 임시 해결 방법으로 클러스터를 설치할 때 **install-config.yaml** 파일에서 로컬이 아닌 가용성 영역을 지정해야 합니다. ([BZ#1997059](#))
- 공개적으로 신뢰할 수 있는 CA(인증 기관)가 서명한 인증서로 보안되는 ARM 끝점과 같은 공용 끝점을 사용하여 Azure Stack Hub에 OpenShift Container Platform을 설치할 수 있습니다. 내부 CA에 대한 지원은 향후 OpenShift Container Platform z-stream 릴리스에 추가됩니다. ([BZ#2012173](#))
- 클러스터 관리자는 503, 404 또는 두 오류 페이지의 사용자 정의 HTTP 오류 코드 응답 페이지를 지정할 수 있습니다. 사용자 지정 오류 코드 페이지가 업데이트되도록 라우터가 다시 로드되지 않습니다. 이 문제를 해결하려면 라우터 pod에서 rsh를 실행하고 사용자 정의 http 오류 코드 페이지를 제공하는 모든 라우터 Pod에서 **reload-haproxy**를 실행합니다.

```
$ oc -n openshift-ingress rsh router-default-6647d984d8-q7b58
sh-4.4$ bash -x /var/lib/haproxy/reload-haproxy
```

또는 경로에 주석을 추가하여 강제로 다시 로드할 수 있습니다. ([BZ#1990020](#))

- 이 릴리스에는 알려진 문제가 포함되어 있습니다. OpenShift OAuth 경로의 호스트 이름과 인증서를 사용자 지정해도 Jenkins에서 더 이상 OAuth 서버 엔드포인트를 신뢰하지 않습니다. 결과적으로 OpenShift OAuth 통합을 사용하여 ID 및 액세스를 관리하는 경우 Jenkins 콘솔에 로그인할 수 없습니다. 현재 사용 가능한 해결 방법이 없습니다. ([BZ#1991448](#))
- 특정 높은 Cardinality 모니터링 메트릭이 의도치 않게 삭제되었으므로 **Pod,qos, System**이라는 컨테이너 성능 입력 및 출력 메트릭을 사용할 수 없습니다. 이 문제에 대한 해결 방법이 없습니다. 프로덕션 워크로드에 대해 이러한 메트릭을 추적하려면 초기 4.9 릴리스로 업그레이드하지 마십시오. ([BZ#2008120](#))
- SRO(Special Resource Operator)가 소프트웨어 정의 네트워크 정책으로 인해 Google Cloud Platform에 설치되지 않을 수 있습니다. 결과적으로 simple-kmod Pod가 생성되지 않습니다. 이는 OpenShift Container Platform 4.9.4 릴리스에서 수정되었습니다. ([BZ#1996916](#))
- OpenShift Container Platform 4.9에서 클러스터 역할의 사용자는 배포 또는 배포 구성에 대한 편집 권한이 없는 경우 콘솔을 사용하여 배포 또는 배포 구성을 확장할 수 없습니다. ([BZ#1886888](#))
- OpenShift Container Platform 4.9에서는 **Developer Console**에 최소 또는 데이터가 없는 경우 대부분의 모니터링 차트 또는 그래프(예: CPU 사용량, 메모리 사용량 및 대역폭)에 -1~1의 범위가 표시됩니다. 그러나 이러한 값은 0 이하로 내려갈 수 없으므로 음수 값을 사용하는 것은 올바르지 않습니다. ([BZ#1904106](#))
- **cgroup**이 일치하지 않아 **ip vrf exec** 명령이 작동하지 않습니다. 따라서 이 명령은 OpenShift pod 내에서 사용할 수 없습니다. VRF(가상 라우팅 및 전달)를 사용하려면 애플리케이션은 VRF를 인식하고 VRF 인터페이스에 직접 바인딩해야 합니다. ([BZ#1995631](#))
- NUMA(Nonuniform Memory Access) 버그로 인해 컨테이너에 대해 바람직하지 않은 NUMA 고정 이 발생하여 대기 시간 또는 성능 저하가 발생할 수 있습니다. 토폴로지 관리자는 **single-numa-node** 토폴로지 관리 정책에서 둘 이상의 NUMA 노드에 충족할 수 있는 리소스를 사용하여 컨테이너를 고정할 수 있습니다. 컨테이너는 보장된 QoS(Quality of Service) pod 아래에 고정됩니다. 이 문제를 해결하려면 컨테이너 메모리 리소스 요청이 **single-numa-node** 정책에서 제공할 수 있는 것보다 큰 경우 보장된 QoS Pod를 시작하지 마십시오. ([BZ#1999603](#))

- 삭제용으로 선택한 pod가 삭제되지 않는 경우도 있습니다. 이는 클러스터에 리소스가 부족할 때 발생합니다. 리소스를 회수하기 위해 시스템에서 삭제할 하나 이상의 Pod를 선택합니다. 리소스가 부족하여 처리 속도가 느려지면 삭제 작업이 설정된 삭제 유예 기간을 초과하여 오류가 발생할 수 있습니다. 이 경우 Pod를 수동으로 삭제합니다. 그런 다음 클러스터에서 사용 가능한 리소스를 회수합니다. (BZ#1997476)
- 간헐적으로 Pod는 OVS(Open vSwitch) 포트 바인딩을 기다리는 동안 **ContainerCreating** 상태로 중단되고 시간 초과될 수 있습니다. 보고된 이벤트는 **failed to configure pod interface: timed out waiting for OVS port binding**입니다. 이 문제는 OVN-Kubernetes 플러그인에 대해 많은 Pod가 생성될 때 발생할 수 있습니다. (BZ#2005598)
- 송신 노드를 재부팅한 후 **Ir-policy-list**에는 중복 레코드 또는 누락된 내부 IP 주소와 같은 오류가 포함됩니다. 예상된 결과는 **Ir-policy-list**가 송신 노드를 재부팅하기 전과 동일한 레코드를 보유하고 있다는 것입니다. 이 문제를 해결하려면 **ovn-kubemaster** Pod를 다시 시작할 수 있습니다. (BZ#1995887)
- 분산 게이트웨이 포트를 포함하는 논리 라우터에서 IP 멀티캐스트 릴레이를 활성화하면 멀티캐스트 트래픽이 분산 게이트웨이 포트에서 올바르게 전달되지 않습니다. 결과적으로 OVN-Kubernetes에서 IP 멀티캐스트 기능이 손상됩니다. (BZ#2010374)
- 웹 콘솔의 관리자 화면에서 노드 목록을 사용할 수 있기 전에 노드 목록을 표시해야 하는 페이지가 렌더링되어 페이지가 응답하지 않습니다. 해결방법은 없지만 이 문제는 향후 릴리스에서 해결될 예정입니다. (BZ#2013088)
- OLM(Operator Lifecycle Manager)은 타임스탬프 검사 및 사용되지 않는 API 호출의 조합을 사용하여 **skipRange** 업그레이드에는 작동하지 않는 특정 서브스크립션에 대한 업그레이드를 수행해야 하는지 여부를 결정합니다. **skipRange** 업그레이드를 사용하는 Operator의 경우 업그레이드 프로세스가 지연되어 문제를 해결하는 데 최대 15분이 걸릴 수 있으며 잠재적으로 훨씬 더 오랜 시간 동안 차단될 수 있습니다.  
이 문제를 해결하려면 클러스터 관리자가 **openshift-operator-lifecycle-manager** 네임스페이스에서 **catalog-operator** Pod를 삭제할 수 있습니다. 이로 인해 Pod가 자동으로 다시 생성되어 **skipRange** 업그레이드가 트리거됩니다. (BZ#2002276)
- 현재 FIPS 모드가 활성화된 Google Cloud Platform에서 RHEL(Red Hat Enterprise Linux) 8을 시작하면 Red Hat Update Infrastructure(RHUI)에서 패키지를 설치하려고 할 때 RHEL 8에서 메타데이터를 다운로드하지 못합니다. 임시 해결 방법으로 RHUI 리포지토리를 비활성화하고 Red Hat 서브스크립션 관리를 사용하여 콘텐츠를 가져올 수 있습니다. (BZ#2001464), (BZ#1997516).
- OpenShift Container Platform 단일 노드 재부팅 후 모든 Pod가 다시 시작되어 일반 Pod 생성 시간보다 오래 걸립니다. 이 문제는 CNI(컨테이너 네트워크 인터페이스)에서 **pod add** 이벤트를 충분히 신속하게 처리할 수 없기 때문에 발생합니다. **timed out waiting for OVS port binding**이라는 오류 메시지가 표시됩니다. OpenShift Container Platform 단일 노드 인스턴스는 결국 예상보다 느리게 복구됩니다. (BZ#1986216)
- MetalLB가 ARP 또는 NDP 요청에 응답하는 단일 노드가 아닌 OVN-Kubernetes Container Network Interface 네트워크 공급자를 사용하여 계층 2 모드에서 실행되면 클러스터의 모든 노드가 요청에 응답합니다. 예기치 않은 ARP 응답 수는 ARP 스푸핑 공격과 유사할 수 있습니다. 환경은 설계된 것과 다르지만, ARP를 차단하도록 호스트 또는 서브넷에 소프트웨어가 구성되지 않는 한 트래픽이 서비스로 라우팅됩니다. 이 버그는 향후 OpenShift Container Platform 릴리스에서 수정되었습니다. (BZ#1987445)
- Tang 디스크 암호화 및 고정 IP 주소 구성이 VMWare vSphere 사용자 프로비저닝 인프라 클러스터에 적용되면 처음 프로비저닝된 후 노드가 제대로 부팅되지 않습니다. (BZ#1975701)
- Operator는 로컬 소스에서 실행하도록 OLM(Operator Lifecycle Manager)의 관련 이미지를 나열해야 합니다. 현재 CSV( **ClusterServiceVersion** ) 오브젝트의 **relatedImages** 매개변수가 정의되지 않은 경우 **opm render**가 관련 이미지를 채우지 않습니다. 이 문제는 향후 릴리스에서 수정

될 예정입니다. (BZ#2000379)

- 이전 버전에서는 OVS(Open vSwitch)가 각 OpenShift Container Platform 클러스터 노드의 컨테이너에서 실행되었으며 노드 내보내기 에이전트는 노드에서 OVS CPU 및 메모리 메트릭을 수집했습니다. 이제 OVS가 클러스터 노드에서 systemd 단위로 실행되고 메트릭은 수집되지 않습니다. 이 문제는 향후 릴리스에서 수정될 예정입니다. OVS 패킷 메트릭은 계속 수집됩니다. (BZ#2002868)
- OpenShift Container Platform 웹 콘솔의 **스토리지** → **개요** 페이지를 숨기거나 표시하는 데 사용되는 플래그가 잘못 설정되어 있습니다. 결과적으로 OpenShift Cluster Storage를 포함하는 클러스터를 배포한 후에는 개요 페이지가 표시되지 않습니다. 이 문제는 향후 릴리스에서 수정될 예정입니다. (BZ#2013132)
- OpenShift Container Platform 4.6 이상에서는 풀에 대한 이미지 참조에서 다음 Red Hat 레지스트리를 지정해야 합니다.

- registry.redhat.io
- registry.access.redhat.com
- quay.io

그렇지 않으면 이러한 레지스트리를 지정하지 않으면 빌드 Pod에서 이미지를 가져올 수 없습니다.

이 문제를 해결하려면 이미지 가져오기 사양에서 **registry.redhat.io/ubi8/ubi:latest** 및 **registry.access.redhat.com/rhel7.7:latest** 와 같은 정규화된 이름을 사용하십시오.

필요한 경우 이미지 **단축 이름을 허용하는 레지스트리를 추가하여 이미지 레지스트리** 설정을 업데이트할 수 있습니다. (BZ#2011293)

- OpenShift Container Platform 4.8 이전에는 기본 로드 밸런싱 알고리즘이 **최소conn** 이었습니다. 비 패스스루 경로의 OpenShift Container Platform 4.8.0에서 기본값이 **임의**로 변경되었습니다. **임의**로 스위칭하면 해당 환경에서 메모리 사용량이 크게 증가하므로 장기 실행 웹 소켓 연결을 사용해야 하는 환경과 호환되지 않습니다. 이 중요한 메모리 사용을 완화하기 위해 기본 로드 밸런싱 알고리즘이 OpenShift Container Platform 4.9에서 **leastconn** 으로 되돌아갔습니다. 메모리 사용량이 많지 않은 솔루션이 있으면 향후 OpenShift Container Platform 릴리스에서 기본값이 **임의**로 변경됩니다.

다음 명령을 입력하여 기본 설정을 확인할 수 있습니다.

```
$ oc get deployment -n openshift-ingress router-default -o yaml | grep -A 2 ROUTER_LOAD_BALANCE_ALGORITHM
- name: ROUTER_LOAD_BALANCE_ALGORITHM
  value: leastconn
```

**random** 옵션은 계속 사용할 수 있습니다. 그러나 이 알고리즘 선택으로 이점을 얻는 경로는 다음 명령을 입력하여 경로별로 주석에서 해당 옵션을 명시적으로 설정해야 합니다.

```
$ oc annotate -n <NAMESPACE> route/<ROUTE-NAME>
"haproxy.router.openshift.io/balance=random"
```

(BZ#2015829)

- 로컬 레지스트리에서 호스팅된 이미지가 지정되면 **oc adm release extract --tools** 명령이 실패합니다. (BZ#1823143)

- OpenShift Container Platform 단일 노드 구성에서 비실시간 커널을 사용할 때보다 실시간커널 (커널-rt)을 사용할 때 Pod 생성 시간이 2배 이상 느려집니다. **kernel-rt** 를 사용하는 경우 노드 재부팅 후 복구 시간이 영향을 받기 때문에 Pod 생성 속도가 느린 Pod의 최대 Pod 수에 영향을 미칩니다.  
이 문제를 해결하려면 **kernel-rt** 를 사용하는 경우 **rcupdate.rcu\_normal\_after\_boot=0** 커널 인수로 부팅하여 복구 시간을 개선할 수 있습니다. 이를 위해서는 실시간 커널 버전 **kernel-rt-4.18.0-305.16.1.rt7.88.el8\_4** 이상이 필요합니다. 이 알려진 문제는 OpenShift Container Platform 버전 4.8.15 이상에 적용됩니다. ([BZ#1975356](#))
- OpenShift Container Platform 단일 노드 재부팅 후 모든 Pod가 다시 시작되어 일반 Pod 생성 시간보다 오래 걸립니다. 이 문제는 CNI(컨테이너 네트워크 인터페이스)에서 **pod add** 이벤트를 충분히 신속하게 처리할 수 없기 때문에 발생합니다. **timed out waiting for OVS port binding**이라는 오류 메시지가 표시됩니다. OpenShift Container Platform 단일 노드 인스턴스는 결국 복구되지만 예상보다 느리게 복구됩니다. 이 알려진 문제는 OpenShift Container Platform 버전 4.8.15 이상에 적용됩니다. ([BZ#1986216](#))
- **bootkube** 가 클러스터 부트스트랩 프로세스 종료에 **oc** 를 사용하려고 하는 SNO 클러스터 프로비저닝 중에 오류가 발생합니다. kube API에서 종료 요청을 수신하고 이로 인해 클러스터 부트스트랩 프로세스가 실패합니다. ([BZ#2010665](#))
- 동일한 호스트에 4.8을 성공적으로 배포한 후 수정된 부팅 테이블 항목으로 인해 OpenShift Container Platform 버전 4.9 SNO 클러스터를 배포하는 데 실패합니다. ([BZ#2011306](#))
- DPDK 기반 워크로드가 OpenShift Container Platform 버전 4.8.5에 배포될 때 표시되는 inbox iavf 드라이버에는 불안정 문제가 있습니다. 또한 DPDK 워크로드를 실시간 8용 RHEL을 실행하는 호스트에 배포하면 드러납니다. 이 문제는 Intel XXV710 NIC가 설치된 호스트에서 발생합니다. ([BZ#2000180](#))
- PTP Operator가 배포하는 **linuxptp** 하위 시스템에서 클럭 건너뛰기 오류가 발생합니다. 보고된 오류 메시지는 **클럭이 뒤로 이동하거나 예상보다 느리게 실행됩니다!**. Intel Columbiaville E810 NIC가 OpenShift Container Platform 버전 4.8 또는 4.9 클러스터에 설치된 호스트에서 오류가 발생했습니다. 이 오류는 **linuxptp** 하위 시스템에서 오류가 아닌 Intel nova 드라이버와 관련이 있을 가능성이 큼니다. ([BZ#2013478](#))
- DU 노드의 제로 스크립팅 프로비저닝(ZTP) 설치 중에 Operator 설치에 실패하는 경우가 있습니다. **InstallPlan** API에서 오류를 보고합니다. 보고된 오류 메시지는 다음과 같습니다. **배포 압축을 해제하지 못했습니다. 이유: DeadlineExceeded.** Operator 설치 작업이 600초를 초과하면 오류가 발생합니다.  
이 문제를 해결하려면 실패한 Operator에 대해 다음 **oc** 명령을 실행하여 Operator 설치를 다시 시도합니다.

1. 카탈로그 소스를 삭제합니다.

```
$ oc -n openshift-marketplace delete catsrc <failed_operator_name>
```

2. 설치 계획을 삭제합니다.

```
$ oc -n <failed_operator_namespace> delete ip <failed_operator_install_plan>
```

3. 서브스크립션을 삭제하고 관련 사용자 정의 리소스 정책에서 Operator **CatalogSource** 및 **Subscription** 리소스를 다시 생성할 때까지 기다립니다.

```
$ oc -n <failed_operator_namespace> delete sub <failed_operator_subscription>
```

예상 결과

Operator **InstallPlan** 및 **ClusterServiceVersion** 리소스가 생성되고 Operator가 설치됩니다.

([BZ#2021456](#))

- SR-IOV Operator와 MCO(Machine Config Operator) 사이에 경합 조건이 존재합니다. 간헐적으로 발생하고 DU 노드의 ZTP 설치 프로세스 중에 서로 다른 방식으로 표시됩니다. 경합 조건은 다음과 같은 오류가 발생할 수 있습니다.
  - ZTP 설치 프로세스가 DU 노드 프로비저닝을 완료하면 성능 프로파일 구성이 적용되지 않는 경우가 있습니다. ZTP 설치 프로세스가 DU 노드 프로비저닝을 완료하면 성능 프로파일 구성이 노드에 적용되지 않으며 **MachineConfigPool** 리소스가 **Updating** 상태로 전환됩니다. 이 문제를 해결하려면 다음 절차를 수행합니다.

1. 실패한 DU 노드의 이름을 가져옵니다.

```
$ oc get mcp
```

출력 예

NAME	CONFIG	UPDATED	UPDATING	DEGRADED
control-plane-1	rendered-control-plane-1-90fe2b00c718	False	True	False
compute-1	rendered-compute-1-31197fc6da09	True	False	False

2. 오류가 발생한 노드를 분리하고 **machine-config-daemon** 이 성능 프로필을 적용할 때까지 기다립니다. 예를 들면 다음과 같습니다.

```
$ oc adm unordon compute-compute-1-31197fc6da09
```

예상 결과

**machine-config-daemon** 은 성능 프로파일 구성을 노드에 적용합니다.

- 성능 프로파일 구성이 DU 노드 구성 중에 적용되지 않는 경우가 있습니다. 이 문제를 해결하려면 DU 노드에서 정책을 적용하는 시퀀스를 변경합니다. MCO(Machine Config Operator) 및 PAO(Performance Addon Operator) 정책을 먼저 적용한 다음 SR-IOV 정책을 적용합니다.
- DU 노드의 정책 구성 중에 재부팅하는 데 수십 분이 걸릴 수 있습니다. 이 인스턴스에는 해결 방법이 필요하지 않습니다. 결국 시스템이 복구됩니다. ([BZ#2021151](#))
- VF(가상 기능)가 이미 존재하는 경우 물리적 기능(PF)에 macvlan을 생성할 수 없습니다. 이 문제는 Intel E810 NIC에 영향을 미칩니다. ([BZ#2120585](#))

## 1.9. 비동기 에라타 업데이트

OpenShift Container Platform 4.9의 보안, 버그 수정 및 개선 업데이트는 Red Hat Network를 통해 비동기 에라타로 릴리스됩니다. 모든 OpenShift Container Platform 4.9 에라타는 [Red Hat Customer Portal](#)을 통해 제공됩니다. 비동기 에라타에 대한 자세한 내용은 [OpenShift Container Platform 라이프 사이클](#)에서 참조하십시오.

Red Hat Customer Portal 사용자는 Red Hat 서브스크립션 관리(RHSM) 계정 설정에서 에라타 통지를 활성화할 수 있습니다. 에라타 통지가 활성화되면 사용자는 등록된 시스템과 관련된 새 에라타가 릴리스될 때마다 이메일을 통해 통지를 받습니다.



## 참고

Red Hat Customer Portal 사용자 계정에는 OpenShift Container Platform에서 에라타 통지 이메일을 생성하기 위해 OpenShift Container Platform을 사용할 수 있는 등록된 시스템 및 권한이 필요합니다.

이 섹션은 향후 OpenShift Container Platform 4.9와 관련된 비동기 에라타 릴리스의 개선 사항 및 버그 수정에 대한 정보 제공을 위해 지속적으로 업데이트됩니다. OpenShift Container Platform 4.9.z와 같은 비동기 버전 릴리스 정보는 하위 섹션에 자세히 설명되어 있습니다. 또한 공간 제한으로 인해 릴리스 정보에 포함되지 않은 에라타 콘텐츠도 다음 하위 섹션에 자세히 설명되어 있습니다.



## 중요

OpenShift Container Platform 릴리스의 경우 항상 **클러스터 업데이트** 지침을 확인하십시오.

### 1.9.1. RHSA-2021:3759 - OpenShift Container Platform 4.9.0 이미지 릴리스, 버그 수정 및 보안 업데이트 권고

출시 날짜: 2021-10-18

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.0을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2021:3759](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2021:3758](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.0 --pullspecs
```

### 1.9.2. RHBA-2021:3935 - OpenShift Container Platform 4.9.4 버그 수정 및 보안 업데이트

출시 날짜: 2021-10-26

OpenShift Container Platform 릴리스 4.9.4가 출시되었습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:3935](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2021:3934](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.4 --pullspecs
```

#### 1.9.2.1. 개선 사항

**SamplesImagestreamImportFailing** 경고에 대해 새 조건부 수집기가 구현되어 실행 시 **openshift-cluster-samples-operator** 네임스페이스의 로그 및 이미지 스트림을 수집합니다. 추가 데이터 수집을 사용하면 외부 레지스트리에서 이미지 스트림을 가져올 때 문제에 대한 자세한 정보를 얻을 수 있습니다. ([BZ#1966153](#))

#### 1.9.2.2. 버그 수정

- 이전에는 **노드 목록을 사용할 수 있기 전에 렌더링된 Nodes** 페이지가 있었습니다. 이번 업데이트를 통해 노드 목록을 사용할 수 있을 때 **Nodes** 페이지가 올바르게 렌더링됩니다. ([BZ#2013088](#))

### 1.9.2.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.3. RHBA-2021:4005 - OpenShift Container Platform 4.9.5 버그 수정 업데이트

출시 날짜: 2021-11-01

OpenShift Container Platform 릴리스 4.9.5가 공개되었습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:4005](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2021:4004](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.5 --pullspecs
```

### 1.9.3.1. 확인된 문제

- OpenShift Container Platform 웹 콘솔의 **스토리지** → **개요** 페이지를 숨기거나 표시하는 데 사용되는 플래그가 잘못 설정되어 있습니다. 결과적으로 OpenShift Cluster Storage가 포함된 클러스터를 배포한 후에는 **Overview** (개요) 페이지가 표시되지 않습니다. 이 버그에 대한 수정 사항은 향후 릴리스될 예정입니다. ([BZ#2013132](#))

### 1.9.3.2. 버그 수정

- **lastTriggeredImageID** 필드가 빌드 구성을 사용하지 않아 이미지 변경 트리거 컨트롤러에서 빌드를 시작하기 전에 ID 필드 확인을 중지했습니다. 결과적으로 클러스터가 OpenShift Container Platform 4.7 이상을 실행하는 동안 빌드 구성이 생성되고 이미지 변경 트리거가 시작되면 지속적으로 빌드를 트리거하려고 합니다. 이번 업데이트를 통해 빌드를 트리거하는 이러한 불필요한 시도가 더 이상 발생하지 않습니다. ([BZ#2006793](#))

### 1.9.3.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.4. RHBA-2021:4119 - OpenShift Container Platform 4.9.6 버그 수정 및 보안 업데이트

출시 날짜: 2021-11-10

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.6을 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:4119](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2021:4118](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.6 --pullspecs
```

### 1.9.4.1. 확인된 문제



- **hostsubnets.network.openshift.io** 는 현재 OVN 클러스터에 있지 않으므로 현재 옵트인 단독화는 OVN이 있는 클러스터에서 작동하지 않습니다. ([BZ#2014633](#))

#### 1.9.4.2. 버그 수정

- 이전에는 **nmstate-handler** Pod의 잠금 구현 버그로 인해 여러 노드가 제어할 수 있었습니다. 이번 업데이트에서는 하나의 노드만 잠금을 제어할 수 있도록 잠금 구현이 수정되었습니다. ([BZ#1954309](#))
- 이전에는 OpenStack 플레이버 검증에서 플레이버가 잘못된 유닛을 사용하여 RAM 요구 사항을 충족하지 못했습니다. 이번 업데이트를 통해 최소 RAM과 OpenStack에서 반환된 값의 비교에 올바른 단위가 사용됩니다. ([BZ#2009787](#))
- 이전에는 컨트롤 플레인 노드에 Ingress 보안 그룹 규칙이 누락되어 OpenStack에 OpenShift Container Platform 배포가 지정되지 않은 작업자가 있는 소형 클러스터에 실패했습니다. 이번 업데이트를 통해 컨트롤 플레인을 예약할 수 있을 때 Ingress 보안 그룹이 OpenStack에 추가되었습니다. ([BZ#2016267](#))
- 이전에는 전체 메모리 사용량을 줄이기 위해 일부 **cAdvisor** 지표가 삭제되었지만 콘솔에서 **Utilization** 대시보드에 결과가 표시되지 않았습니다. 이번 업데이트를 통해 대시보드가 다시 올바르게 표시됩니다. ([BZ#2018455](#))

#### 1.9.4.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.5. RHBA-2021:4579 - OpenShift Container Platform 4.9.7 버그 수정 업데이트

출시 날짜: 2021-11-15

OpenShift Container Platform 릴리스 4.9.7이 출시되었습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:4579](#) 권고에 나열되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.7 --pullspecs
```

#### 1.9.5.1. 기능

##### 1.9.5.1.1. Kubernetes 1.22.2의 업데이트

이번 업데이트에는 Kubernetes 1.22.2의 변경 사항이 포함되어 있습니다. 자세한 내용은 [1.22.2](#) 에서 확인할 수 있습니다.

#### 1.9.5.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.6. RHBA-2021:4712 - OpenShift Container Platform 4.9.8 버그 수정 업데이트

출시 날짜: 2021-11-22

OpenShift Container Platform 릴리스 4.9.8이 공개되었습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:4712](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2021:4711](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.8 --pullspecs
```

### 1.9.6.1. 버그 수정

- 이전 버전에서는 **SriovNetworkNodePolicy** CR(사용자 정의 리소스)을 추가하거나 삭제한 경우 **SriovNetworkNodeState** CR에 **Succeeded** 이외의 값이 있는 **syncStatus** 오브젝트가 있는 경우 SR-IOV 네트워크 구성 데몬 Pod는 노드를 차단하고 예약할 수 없음으로 표시합니다. 이번 업데이트에서는 문제가 해결되었습니다. ([BZ#2002508](#))

### 1.9.6.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.7. RHBA-2021:4834 - OpenShift Container Platform 4.□ 버그 수정 및 보안 업데이트

출시 날짜: 2021-11-29

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.□을 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:4834](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2021:4833](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.9 --pullspecs
```

### 1.9.7.1. 기능

#### 1.9.7.1.1. Kubernetes 1.22.3의 업데이트

이번 업데이트에는 Kubernetes 1.22.3의 변경 사항이 포함되어 있습니다. 자세한 내용은 [1.22.3 변경 로그](#)에서 확인할 수 있습니다.

### 1.9.7.2. 버그 수정

- 이전에는 매니페스트를 재정의할지 결정할 때 CVO(Cluster Version Operator)에서 **spec.overrides[].group** 을 무시했습니다. 결과적으로 재정의된 항목이 여러 리소스와 일치할 수 있으며, 이는 관리자가 의도한 것보다 더 많은 리소스를 재정의할 수 있습니다. 또한 잘못된 그룹이 있는 재정의된 항목은 일치하는 것으로 간주되어 **kubeadmin** 사용자가 알림 없이 잘못된 그룹 값을 사용할 수 있습니다. 이번 업데이트를 통해 구성된 덮어쓰기를 적용할 때 CVO가 일치하는 그룹이 필요합니다. 결과적으로 CVO는 더 이상 단일 덮어쓰기로 여러 매니페스트와 일치하지 않습니다. 대신 CVO는 올바른 그룹과 있는 매니페스트와만 일치합니다. 이전에 잘못된 그룹을 사용한 **kubeadmin 사용자**는 재정의가 계속 일치하도록 올바른 그룹으로 업데이트해야 합니다. ([BZ#2022570](#))

### 1.9.7.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.8. RHBA-2021:4889 - OpenShift Container Platform 4.9.10 버그 수정 업데이트

출시 날짜: 2021-12-06

OpenShift Container Platform 릴리스 4.9.10이 출시되었습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:4889](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2021:4888](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.10 --pullspecs
```

#### 1.9.8.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.9. RHBA-2021:5003 - OpenShift Container Platform 4.9.11 버그 수정 및 보안 업데이트

출시 날짜: 2021-12-13

OpenShift Container Platform 릴리스 4.9.11이 출시되었습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:5003](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2021:5002](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.11 --pullspecs
```

#### 1.9.9.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.10. RHBA-2021:5214 - OpenShift Container Platform 4.9.12 버그 수정 업데이트

출시 날짜: 2022-01-04

OpenShift Container Platform 릴리스 4.9.12가 출시되었습니다. 업데이트에 포함된 버그 수정은 [RHBA-2021:5214](#) 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2021:5213](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.12 --pullspecs
```

### 1.9.10.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.11. RHBA-2022:0110 - OpenShift Container Platform 4.9.15 버그 수정 업데이트

출시 날짜: 2022-01-17

OpenShift Container Platform 릴리스 4.9.15가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:0110](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:0109](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.15 --pullspecs
```

### 1.9.11.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.12. RHBA-2022:0195 - OpenShift Container Platform 4.9.17 버그 수정 업데이트

출시 날짜: 2022-01-24

OpenShift Container Platform 릴리스 4.9.17이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:0195](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:0194](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.17 --pullspecs
```

### 1.9.12.1. 버그 수정

- 이전에는 csi-driver Pod의 **livenessProbe** 에 시간 제한이 없었습니다. 결과적으로 프로브가 느린 클라우드에서 실패했습니다. 이로 인해 클러스터 성능이 저하되었습니다. 이번 업데이트를 통해 더 느린 환경을 수용할 수 있도록 **livenessProbe** 의 시간 초과가 설정됩니다. 결과적으로 cinder 속도가 느린 클라우드에서 클러스터는 더 이상 성능이 저하되지 않습니다. ([BZ#2037080](#))
- 이전 버전에서는 OpenShift Container Platform Jenkins 동기화 플러그인에서 Jenkins Kubernetes 플러그인 pod 템플릿에 매핑하기 위해 **role** 레이블이 **jenkins-agent** 로 설정된 구성 맵과 이미지 스트림을 동기화하지 않았습니다. 결과적으로 OpenShift Container Platform Jenkins 동기화 플러그인은 더 이상 구성 맵 또는 **jenkins-agent** 라벨을 사용하여 이미지 스트림에서 Pod 템플릿을 가져오지 않습니다. 이번 업데이트를 통해 허용되는 라벨 사양이 수정되었습니다. 결과적으로 OpenShift Container Platform Jenkins 동기화 플러그인은 **jenkins-agent** 라벨을 사용하여 구성 맵 또는 이미지 스트림에서 Pod 템플릿을 가져옵니다. ([BZ#2038961](#))

### 1.9.12.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.13. RHBA-2022:0279 - OpenShift Container Platform 4.9.18 bug fix update

출시 날짜: 2022-01-31

OpenShift Container Platform 릴리스 4.9.18이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:0279](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:0276](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.18 --pullspecs
```

#### 1.9.13.1. 버그 수정

- 이전에는 액세스가 제한된 사용자가 공유 네임스페이스에서 자체 ConfigMap에 액세스할 수 없었습니다. 결과적으로 고정 탐색 항목과 같은 사용자 기본 설정이 로컬 브라우저 스토리지에 저장되었으며 여러 브라우저 간에 공유되지 않았습니다. 이번 업데이트를 통해 Console Operator에서 각 사용자에게 대한 RBAC 규칙을 자동으로 생성합니다. 결과적으로 액세스가 제한된 사용자는 이제 자체 설정을 사용하고 브라우저 간에 쉽게 전환할 수 있습니다. ([BZ#2038607](#))
- 이전에는 여러 `oc set` 하위 명령에 `--dry-run` 플래그가 제대로 사용되지 않았습니다. 결과적으로 `--dry-run=server` 명령에서 리소스 업데이트를 수행합니다. 이번 업데이트에서는 명령이 서버에 정보를 올바르게 전송하도록 `--dry-run` 플래그가 수정되었습니다. 결과적으로 `oc set` 하위 명령이 예상대로 작동합니다. ([BZ#2038930](#))

#### 1.9.13.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

### 1.9.14. RHBA-2022:0340 - OpenShift Container Platform 4.9.19 bug fix and security update

출시 날짜: 2022-02-09

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.19를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:0340](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2022:0339](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.19 --pullspecs
```

#### 1.9.14.1. 다음 OpenShift Container Platform 릴리스로 업그레이드 준비

스케줄러 정책 API를 제거했기 때문에 OpenShift Container Platform 4.9.19에서는 OpenShift Container Platform 4.9에서 OpenShift Container Platform 4.10으로의 업그레이드를 차단하는 차단 조건을 도입했습니다. OpenShift Container Platform 4.9에서 OpenShift Container Platform 4.10으로 업그레이드하려면 스케줄러 정책 API 구성을 지우고 더 이상 사용하지 않아야 합니다. ([BZ#2037665](#))

#### 1.9.14.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.15. RHBA-2022:0488 - OpenShift Container Platform 4.9.21 bug fix update

출시 날짜: 2022-02-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.21을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:0488](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:0487](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.21 --pullspecs
```

### 1.9.15.1. 버그 수정

- Performance Addon Operator에 [BZ#2055019](#) 수정 사항이 포함되어 있습니다. 자세한 내용은 [버그 수정](#) 의 "Performance Addon Operator" 섹션을 참조하십시오.

### 1.9.15.2. 확인된 문제

- RHOSP(Red Hat OpenStack Platform) 인증 정보 시크릿 생성과 **kube-controller-manager** 가 시작되는 경쟁 조건이 있습니다. 이 경우 RHOSP 클라우드 공급자가 RHOSP 인증 정보로 구성되지 않으므로 **LoadBalancer** 서비스에 대한 Octavia 로드 밸런서 생성에 대한 지원이 중단됩니다. **kube-controller-manager** 프로세스 중에 성공할 때까지 RHOSP 인증 정보 시크릿 가져오기를 시도해야 합니다. 이를 통해 **kube-controller-manager** 가 시작될 때 RHOSP 클라우드 공급자를 일관되게 초기화할 수 있습니다. ([BZ#2039373](#))

### 1.9.15.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.16. RHSA-2022:0561 - OpenShift Container Platform 4.9.22 버그 수정 및 보안 업데이트

출시 날짜: 2022-02-22

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.22를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:0561](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2022:0557](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.22 --pullspecs
```

### 1.9.16.1. 버그 수정

- 이번 업데이트 이전에는 사용자 정의 리소스 정의 또는 Pod와 같은 리소스 세부 정보를 반복적으로 클릭하면 여러 코드 참조 오류가 발생하여 **t가 함수 오류가 발생하지 않습니다**. 이번 업데이트에서는 이러한 문제가 해결되었습니다. 이제 오류가 발생하면 애플리케이션에서 코드 참조를 확인하고 해결 상태를 저장하여 추가 오류를 올바르게 처리할 수 있습니다. 코드 참조 오류가 발생하면 애플리케이션이 더 이상 충돌하지 않습니다. ([BZ#2022158](#))

### 1.9.16.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

### 1.9.17. RHSA-2022:0655 - OpenShift Container Platform 4.9.23 버그 수정 및 보안 업데이트

출시 날짜: 2022-02-28

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.23을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:0655](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:0654](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.23 --pullspecs
```

#### 1.9.17.1. 확인된 문제

- OpenShift Container Platform 릴리스 4.9.23은 매니페스트에서 **application/vnd.oci.image.manifest.v1+json** 미디어 유형을 사용하는 이미지를 참조합니다. 이로 인해 OCI 미디어 유형을 지원하지 않는 이미지 레지스트리에 미러링할 때 문제가 발생할 수 있습니다. 현재 이 문제에 대한 작업이 진행되지 않았으며 향후 OpenShift Container Platform 4.9 버전에서 수정될 예정입니다. ([BZ#2059762](#))

#### 1.9.17.2. 버그 수정

- 이전에는 로컬 영역이 활성화된 리전에 설치할 때 설치에 실패했습니다. 이번 업데이트를 통해 설치 프로그램은 로컬 영역이 아닌 가용 영역만 고려합니다. 이제 로컬 영역이 활성화된 설치해당 리전의 가용성 영역에만 설치되고 로컬 영역에는 설치되지 않습니다. ([BZ#2052307](#))
- 이전 버전에서는 OVN-Kubernetes가 있는 OpenShift Container Platform에서 ExternalIP를 통해 서비스에 대한 수신 액세스를 관리했습니다. 4.9.22에서 4.9.23으로 업그레이드할 때 액세스 **ExternalIP**는 "경로에서 호스트 없음"과 같은 문제로 작업을 중지합니다. 이번 업데이트를 통해 관리자는 이제 externalIPs에서 클러스터로 트래픽을 전달해야 합니다. 지침은 ([KCS](#)) 및 ([Kubernetes 외부IP](#)) ([BZ#2076662](#))를 참조하십시오.

#### 1.9.17.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

### 1.9.18. RHBA-2022:0798 - OpenShift Container Platform 4.9.24 bug fix update

출시 날짜: 2022-03-16

OpenShift Container Platform 릴리스 4.9.24가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:0798](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:0794](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.24 --pullspecs
```

### 1.9.18.1. 기능

이번 업데이트에는 Kubernetes 1.22.5의 변경 사항이 포함되어 있습니다. 더 많은 정보는 다음의 changelog: [1.22.3](#) 에서 확인할 수 있습니다.

### 1.9.18.2. 삭제된 기능

OpenShift Container Platform 4.9.24부터 Microsoft Azure 클러스터의 mint 모드에서 CCO(Cloud Credential Operator) 사용에 대한 지원이 OpenShift Container Platform 4.9에서 제거되었습니다. 이러한 변경 사항은 [2022년 6월 30일에 예정된 Microsoft Azure AD Graph API 사용 중지](#) 로 인한 것이며 z-stream 업데이트에서 지원되는 모든 OpenShift Container Platform 버전으로 백포트되고 있습니다. 자세한 내용은 [Microsoft Azure에 대한 자격 증명 추출](#) 지원을 참조하십시오.

### 1.9.18.3. 버그 수정

- 이전 버전에서는 OpenShift Container Platform 웹 콘솔에서 배포 편집 페이지를 열면 빈 브라우저 탭이 발생했습니다. 현재 릴리스에서는 존재하지 않는 배포 리소스에 대한 배포 편집 페이지를 열면 404 오류 페이지가 표시됩니다. ([BZ#2002273](#))
- 이전에는 **kube-apiserver** 의 재작성으로 인해 사용자 쪽 API가 변경되었습니다. 사용자는 DualStack 서비스에 대해 **ipFamilyPolicy:PreferDualStack** 또는 **ipFamilyPolicy:RequireDualStack** 중 하나를 명시적으로 지정해야 합니다. Users **.Users**. 이번 업데이트를 통해 API에 중요한 API 변경 사항을 사용자에게 알리는 경고가 표시됩니다. 이제 **ipFamilyPolicy:PreferDualStack** 또는 **ipFamilyPolicy:RequireDualStack** 을 명시적으로 지정하지 않고 DualStack 서비스를 생성할 수 없습니다. ([BZ#2045576](#))

### 1.9.18.4. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.19. RHBA-2022:0861 - OpenShift Container Platform 4.9.25 버그 수정 및 보안 업데이트

출시 날짜: 2022-03-21

OpenShift Container Platform 릴리스 4.9.25가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:0861](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2022:0860](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.25 --pullspecs
```

### 1.9.19.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.20. RHBA-2022:1022 - OpenShift Container Platform 4.9.26 버그 수정 및 보안 업데이트

출시 날짜: 2022-03-29



보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.26을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:1022](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2022:1021](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.26 --pullspecs
```

### 1.9.20.1. 확인된 문제

- 현재 etcd가 실패하는 알려진 문제가 있습니다. 이로 인해 etcd 데이터 불일치가 발생할 수 있으므로 클러스터가 불안정하고 데이터 복구가 어려워질 수 있습니다. 수정 사항이 제공될 때까지 OpenShift Container Platform 4.8에서 4.9로의 업데이트 권장 사항이 제거됩니다. 현재 이 문제에 대한 해결방법이 없습니다. ([BZ#2068601](#))

### 1.9.20.2. 버그 수정

- 이전에는 Ingress Operator에서 상태 점검을 완료한 후 TCP 연결이 닫히지 않았습니다. 결과적으로 TCP 연결이 누적되어 **LoadBalancer** 에서 빌드가 발생했습니다. 이번 수정을 통해 연결을 설정하는 동안 **keepalive** 가 비활성화됩니다. 이로 인해 각 상태 점검 후 TCP 연결이 닫히고 **LoadBalancer** 에서 빌드가 수행되지 않습니다. ([BZ#2064586](#))
- 이전 버전에서는 클러스터를 실행하는 동안 클라이언트 쓰로틀 메시지의 낮은 제한 번호가 표시되었습니다. 결과적으로 CRD(사용자 정의 리소스 정의)가 늘어나면 낮은 숫자 및 제한된 API 검색 요청이 생성되었습니다. 이번 수정으로 제한 수가 증가하여 메시지가 더 자주 나타납니다. ([BZ#2045008](#))
- 이번 업데이트 이전에는 **oc debug** 명령으로 사용자가 연결 시간 초과를 설정할 수 없으며 사용자가 클러스터 환경에서 로그아웃되지 않았습니다. 이번 업데이트를 통해 시간 초과 기능은 일정 시간 동안 활동이 없으면 클러스터를 종료합니다. ([BZ#2065302](#))

### 1.9.20.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.21. RHSA-2022:1158 - OpenShift Container Platform 4.9.27 버그 수정 및 보안 업데이트

출시 날짜: 2022-04-07

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.27을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:1158](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:1157](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.27 --pullspecs
```

### 1.9.21.1. 버그 수정

- 이번 업데이트 이전에는 Cisco의 ACI 버그로 인해 RHOSP(Red Hat OpenStack Platform)에서 새 VM(가상 머신)을 실행할 때 오류가 발생했습니다. 이번 업데이트를 통해 RHOSP cluster-API-provider에 추가 필터가 추가되었습니다. 이제 Cisco의 ACI에서 가상 머신이 올바르게 실행됩니

다. ([BZ#2064633](#))

### 1.9.21.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.22. RHBA-2022:1245 - OpenShift Container Platform 4.9.28 버그 수정 업데이트

출시 날짜: 2022-04-13

OpenShift Container Platform OpenShift Container Platform 릴리스 4.9.28을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:1245](#) 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.28 --pullspecs
```

### 1.9.22.1. 확인된 문제

- OpenShift Container Platform 4.9.28로 업데이트할 때 etcd pod가 시작되지 않고 etcd Operator가 성능이 저하 됩니다. 향후 OpenShift Container Platform 버전에서는 이 문제를 해결합니다. 자세한 내용은 다음 지식 베이스 솔루션을 참조하십시오.
  - [etcd pod는 OpenShift Container Platform 4.9.28 또는 4.10.9를 업데이트한 후 시작되지 않습니다.](#)
  - [OCP 4.9 및 4.10에서 잠재적인 etcd 데이터 불일치 문제](#)

### 1.9.22.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.23. RHSA-2022:1363 - OpenShift Container Platform 4.9.29 버그 수정 및 보안 업데이트

출시 날짜: 2022-04-20

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.29를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:1363](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:1362](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.29 --pullspecs
```

### 1.9.23.1. 버그 수정

- 이전 버전에서는 LSO(Local Storage Operator)에서 생성된 PV(영구 볼륨)에 **OwnerReference** 오브젝트를 추가했습니다. 이로 인해 PV에 대한 삭제 요청이 여전히 Pod에 연결된 상태에서 PV를 종료 할 수 있는 문제가 발생하는 경우가 있었습니다. 이번 업데이트를 통해 LSO에서 더 이상

**OwnerReference** 오브젝트를 생성하지 않으며 클러스터 관리자는 클러스터에서 노드를 제거한 후 사용되지 않은 PV를 삭제할 수 있습니다. ([BZ#2070617](#))

- 이전 버전에서는 지정된 이미지를 실행할 수 없을 때 **oc adm inspect** 명령에 `oc adm inspect` 명령을 다시 수집해야 했습니다. 그 결과 대체가 발생했을 때 로그의 정보를 이해하기 어려웠습니다. 이번 업데이트를 통해 대체 검사가 수행될 때 로그를 명시적으로 만들 수 있습니다. 결과적으로 **oc adm must gather**의 출력을 더 쉽게 이해할 수 있습니다. ([BZ#2051944](#))
- 이전에는 Docker의 하드 코딩 된 BusyBox 이미지가 스코어 카드에 사용되었습니다. 결과적으로 스코어 카드를 실행할 때 Docker의 새로운 속도 제한으로 인해 주기적인 오류가 발생했습니다. 이번 수정에서는 UBI(Universal Base Image) [registry.access.redhat.com/ubi8/ubi:8.4](#)를 스코어 카드에 사용하여 속도 제한으로 인해 실패하지 않는 것이 좋습니다. ([BZ#2064408](#))

### 1.9.23.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.24. RHBA-2022:1605 - OpenShift Container Platform 4.9.31 버그 수정 업데이트

출시 날짜: 2022-05-03

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.31을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:1605](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:1604](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.31 --pullspecs
```

### 1.9.24.1. Kubernetes 1.22.8의 업데이트

이번 업데이트에는 Kubernetes 1.22.6부터 1.22.8의 변경 사항이 포함되어 있습니다. 자세한 내용은 [1.22.6](#), [1.22.7](#) 및 [1.22.8](#)에서 확인할 수 있습니다.

### 1.9.24.2. 버그 수정

- 이전에는 Kubernetes API 서버가 OpenShift Container Platform 4.10에서 듀얼 스택 서비스의 API에 대해 향후 변경 사항에 대해 경고하지 않았습니다. 이번 수정에서는 **ipFamilyPolicy: PreferDualStack** 또는 **ipFamilyPolicy: OpenShift Container Platform 4.10에서 유효한 이중 스택 서비스에 대한 RequireDualStack**을 지정합니다. ([BZ#2050632](#))
- 이전 버전에서는 성능 개선 릴리스로 인해 **Git 가져오기** 페이지가 로드되지 않았습니다. 이번 수정으로 **Git 가져오기** 페이지가 더 이상 로드되지 않고 의도한 대로 실행됩니다. ([BZ#2069621](#))
- 이번 업데이트 이전에는 사용자가 **Git에서 가져오기** 양식에 개인 리포지토리에 대한 시크릿을 제공하면 시크릿을 디코딩하지 않았습니다. 이로 인해 **Git에서 가져오기** 양식이 리포지토리의 올바른 가져오기 전략 및 빌더 이미지를 탐지하지 못했습니다. 이번 업데이트를 통해 **Git에서 가져오기** 양식에서 시크릿을 사용하기 전에 디코딩하여 올바른 가져오기 전략 및 빌더 이미지를 감지할 수 있습니다. ([BZ#2069258](#))

### 1.9.24.3. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.25. RHBA-2022:1694 - OpenShift Container Platform 4.9.32 버그 수정 업데이트

출시 날짜: 2022-05-12

OpenShift Container Platform 릴리스 4.9.32가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:1694](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:1693](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.32 --pullspecs
```

### 1.9.25.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 마이너 버전에서 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.26. RHBA-2022:2206 - OpenShift Container Platform 4.9.33 버그 수정 및 보안 업데이트

출시 날짜: 2022-05-18

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.33을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:2206](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2022:2205](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.33 --pullspecs
```

### 1.9.26.1. 버그 수정

- 이전 버전에서는 콘솔 및 OAuth 플랫폼을 사용자 정의할 수 있는 API(애플리케이션 플랫폼 인터페이스)가 제한된 사용자가 클러스터 인그레스 구성에 사용자 지정 호스트 이름과 10진수 디지탈이 포함된 최상위 도메인으로 사용자 지정 호스트 이름을 지정할 수 없었습니다. 이번 업데이트를 통해 사용자는 10진수가 포함된 최상위 클러스터 도메인을 사용하고 경로에 유효한 호스트 이름을 사용하여 콘솔과 OAuth 경로를 사용자 지정할 수 있습니다. ([BZ#2075551](#))
- 이전에는 설치 관리자 프로비저닝 인프라(IPI)에서 Azure Stack Hub를 지원하지 않았습니다. 결과적으로 Ingress Operator는 Azure Stack Hub에서 수신에 대한 와일드카드 DNS 레코드를 구성하지 못했습니다. 이번 업데이트를 통해 Ingress Operator는 설치 프로그램에서 제공하는 Azure Resources Manager(ARM) 끝점에 대해 클러스터 인프라 구성 오브젝트를 확인할 수 있습니다. ([BZ#2032677](#))

### 1.9.26.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.27. RHSA-2022:2283 - OpenShift Container Platform 4.9.35 버그 수정 및 보안 업데이트

출시 날짜: 2022-05-24

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.35를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:2283](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:2282](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.35 --pullspecs
```

### 1.9.27.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.28. RHBA-2022:4741 - OpenShift Container Platform 4.9.36 버그 수정 업데이트

출시 날짜: 2022-05-31

OpenShift Container Platform 릴리스 4.9.36이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:4741](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:4740](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.36 --pullspecs
```

### 1.9.28.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.29. RHBA-2022:4906 - OpenShift Container Platform 4.9.37 버그 수정 업데이트

출시 날짜: 2022-06-07

OpenShift Container Platform 릴리스 4.9.37이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:4906](#) 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.37 --pullspecs
```

### 1.9.29.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.30. RHBA-2022:2283 - OpenShift Container Platform 4.9.38 버그 수정 및 보안 업데이트

출시 날짜: 2022-06-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.38을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:4973](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2022:4972](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.38 --pullspecs
```

#### 1.9.30.1. 버그 수정

- RHOSP(Red Hat OpenStack Platform) 인증 정보 시크릿 생성과 **kube-controller-manager** 가 시작되는 경쟁 조건이 있습니다. 이 경우 RHOSP 클라우드 공급자가 RHOSP 인증 정보로 구성되지 않으므로 **LoadBalancer** 서비스에 대한 Octavia 로드 밸런서 생성에 대한 지원이 중단됩니다. **kube-controller-manager** 프로세스 중에 성공할 때까지 RHOSP 인증 정보 시크릿 가져오기를 시도해야 합니다. 이를 통해 **kube-controller-manager** 가 시작될 때 RHOSP 클라우드 공급자를 일관되게 초기화할 수 있습니다. ([BZ#2059677\\*](#))

#### 1.9.30.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.31. RHBA-2022:5180 - OpenShift Container Platform 4.9.40 버그 수정 업데이트

출시 날짜: 2022-06-29

OpenShift Container Platform 릴리스 4.9.40이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:5180](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:5179](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.40 --pullspecs
```

#### 1.9.31.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.32. RHBA-2022:5434 - OpenShift Container Platform 4.9.41 버그 수정 업데이트

출시 날짜: 2022-07-05

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.41를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:5434](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:5433](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.41 --pullspecs
```

### 1.9.32.1. 버그 수정

- 이전 버전에서는 **volumeClaimTemplate** 을 사용하여 **PipelineRun** 을 생성할 때 파이프라인은 할당된 스토리지 클래스 이름이 아닌 **gp2** 의 하드 코딩된 값을 사용했습니다. 이번 수정을 통해 **volumeClaimTemplate** 을 사용하여 **PipelineRun** 을 시작할 때 적절한 스토리지 클래스 이름이 할당됩니다. ([BZ#2097618](#))
- 이전에는 HAProxy가 잘못된 HTTPS 경로로 리디렉션되었습니다. 그 결과 애플리케이션이 HTTPS로 리디렉션되지 않았으며 검증되지 않았습니다. 이번 수정에서는 리디렉션 맵에 플래그를 설정하여 HAProxy가 올바른 HTTPS 경로로 리디렉션되도록 합니다. ([BZ#2010227](#))

### 1.9.32.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.33. RHBA-2022:5509 - OpenShift Container Platform 4.9.42 버그 수정 업데이트

출시 날짜: 2022-07-12

OpenShift Container Platform 릴리스 4.9.42가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:5509](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:5508](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.42 --pullspecs
```

### 1.9.33.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.34. RHBA-2022:5561 - OpenShift Container Platform 4.9.43 버그 수정 업데이트

출시 날짜: 2022-07-20

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.43을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:5561](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:5560](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.43 --pullspecs
```

### 1.9.34.1. 버그 수정

- 이전 버전에서는 **LoadBalancer** 서비스에 수정된 주석이 없어 Ingress Operator에서 주석이 없는 업그레이드를 차단하도록 Ingress Operator가 수정된 주석을 보고했습니다. 이번 수정을 통해 논리에서 각 서비스 주석을 올바르게 확인하여 Ingress Operator에서 더 이상 업그레이드를 차단하지 않습니다. ([BZ#2097736](#))

- 이전에는 Ingress Operator 업데이트에서 기존 Ingress 컨트롤러에서 프록시 프로토콜을 활성화하지 못하여 사용자가 Ingress 컨트롤러를 다시 생성하여 프록시 프로토콜을 사용하도록 강제했습니다. 이번 수정으로 Ingress Operator가 프록시 프로토콜을 활성화하도록 성공적으로 업데이트되었습니다. ([BZ#2084336](#))

### 1.9.34.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.35. RHSA-2022:5879 - OpenShift Container Platform 4.9.45 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2022-08-09

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.45를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:5879](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:5878](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.45 --pullspecs
```

### 1.9.35.1. 버그 수정

- 이전 버전에서는 RHOSP(Red Hat OpenStack Platform) Manila 및 Cinder CSI Driver Operator의 메트릭 끝점에서 비보안 TLS(Transport Layer Security) 구성을 사용했습니다. 이러한 구성을 통해 취약한 암호화에 액세스할 수 있어 이러한 엔드포인트에서 트래픽을 암호 해독하거나 수정할 수 있습니다. 이번 업데이트를 통해 TLS 구성이 더 안전하고 취약한 암호화에 대한 액세스를 제거합니다. ([BZ#2110255](#))

### 1.9.35.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.36. RHSA-2022:6033 - OpenShift Container Platform 4.9.46 버그 수정 업데이트

출시 날짜: 2022-08-17

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.46을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:6033](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:6032](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.46 --pullspecs
```

### 1.9.36.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.



### 1.9.37. RHSA-2022:6147 - OpenShift Container Platform 4.9.47 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2022-08-31

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.47을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:6147](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:6146](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.47 --pullspecs
```

#### 1.9.37.1. 버그 수정

- 이전에는 AWS SDK에서 새 리전을 인식하지 못했으며 머신 컨트롤러에서 이를 사용할 수 없었습니다. 이 문제는 AWS SDK가 공급되는 시점의 리전만 인식되었기 때문에 발생했습니다. 이번 업데이트를 통해 관리자는 DescribeRegions를 사용하여 시스템의 지정된 리전을 확인하고 SDK에 알 수 없는 리전에서 새 머신을 생성할 수 있습니다. ([BZ#2111004](#))



참고

이는 새 AWS 권한이며 새 권한이 있는 수동 모드 클러스터의 인증 정보를 업데이트해야 합니다.

#### 1.9.37.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.38. RHSA-2022:6317 - OpenShift Container Platform 4.9.48 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2022-09-12

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.48를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:6317](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:6316](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.48 --pullspecs
```

#### 1.9.38.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.39. RHBA-2022:6678 - OpenShift Container Platform 4.9.49 버그 수정 업데이트

출시 날짜: 2022-09-29

OpenShift Container Platform 릴리스 4.9.49가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:6678](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:6677](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.49 --pullspecs
```

### 1.9.39.1. 버그 수정

- 이전에는 종료 상태의 라우터에서 **oc cp** 명령이 지연되어 **must-gather** 로그가 지연되었습니다. 이번 업데이트를 통해 각 **oc cp** 명령의 시간 제한이 설정되어 **must-gather** 로그의 지연이 제거됩니다. ([BZ#2108892](#))

### 1.9.39.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.40. RHSA-2022:6905 - OpenShift Container Platform 4.9.50 버그 수정 및 보안 업데이트

출시 날짜: 2022-10-19

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.50을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:6905](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:6903](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.50 --pullspecs
```

### 1.9.40.1. 버그 수정

- 이전 버전에서는 OpenShift Container Platform 4.8에서 HAProxy 구성 템플릿을 변경하면 구성에 바인딩이 두 개 이상인 경우 **accept-proxy** 옵션이 모든 바인딩 행에 설정되지 않았습니다. 이로 인해 프록시 프로토콜이 IPv6가 활성화되지 않고 IPv4가 활성화되지 않았습니다. 이번 업데이트를 통해 프록시 프로토콜이 구성될 때 HAProxy 구성 템플릿이 모든 바인딩 행에서 **accept-proxy**로 설정됩니다. 이제 OpenShift Container Platform에서는 프록시 프로토콜이 구성된 듀얼 스택 클러스터에서 IPv6 및 IPv4에 대한 프록시 프로토콜을 활성화합니다. ([OCBUGS-1338](#))
- 이전에는 Ingress Operator에서 **openshift-ingress** 네임스페이스의 kubernetes 서비스 오브젝트를 Ingress 컨트롤러에서 생성한지 확인하지 않았습니다. 그 결과 Ingress Operator는 동일한 이름과 네임스페이스를 사용하여 kubernetes 서비스를 수정하거나 제거했습니다. 이번 업데이트를 통해 Ingress Operator에 오류 메시지가 표시되고 **openshift-ingress** 네임스페이스에서 동일한 이름으로 kubernetes 서비스를 수정하거나 제거하지 않습니다. ([OCBUGS-1624](#))
- 이전에는 **openshift-router** 프로세스에서 런타임 시 **SIGTERM** 종료 신호가 손상되었습니다. 그 결과 컨테이너는 kubernetes 종료 요청을 무시하여 컨테이너가 종료되는 데 약 1시간이 걸립니다. 이번 업데이트를 통해 GO 코드의 **SIGTERM** 처리기가 캐시 초기화 함수에 전파되고 라우터는 초기화 중에 **SIGTERM** 신호에 응답합니다. ([OCBUGS-1620](#))

### 1.9.40.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.41. RHSA-2022:7216 - OpenShift Container Platform 4.9.51 버그 수정 및 보안 업데이트

출시 날짜: 2022-11-02

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.51을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:7216](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:7215](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.51 --pullspecs
```

#### 1.9.41.1. 주요 기술 변경 사항

- 이 번 릴리스에서는 서비스 계정 발행자가 사용자 지정 항목으로 변경되면 기존 바인딩된 서비스 토큰이 더 이상 즉시 무효화되지 않습니다. 대신 서비스 계정 발행자가 변경되면 이전 서비스 계정 발행자는 24시간 동안 계속 신뢰할 수 있습니다.

자세한 내용은 [볼륨 프로젝션을 사용하여 서비스 계정 토큰 구성](#) 을 참조하십시오.

#### 1.9.41.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.42. RHBA-2022:8485 - OpenShift Container Platform 4.9.52 버그 수정 업데이트

출시 날짜: 2022-11-23

OpenShift Container Platform 릴리스 4.9.52가 공개되었습니다. 이 릴리스에 대한 IBM Powerbuild가 없습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:8485](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:8582](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.52 --pullspecs
```

#### 1.9.42.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

### 1.9.43. RHBA-2022:8714 - OpenShift Container Platform 4.9.53 버그 수정 업데이트

출시 날짜: 2022-12-7

OpenShift Container Platform 릴리스 4.9.53이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2022:8714](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2022:8713](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.53 --pullspecs
```

### 1.9.43.1. 개선 사항

- IPv6 원하지 않는 서블러 알립 및 IPv4 불필요한 주소 확인 프로토콜이 SR-IOV CNI 플러그인에서 기본값으로 설정되어 있습니다. SR-IOV(Single Root I/O Virtualization) CNI 플러그인으로 생성된 Pod는 IP 주소 관리 CNI 플러그인이 IP를 할당하여 이제 IPv6 비호주 서블러 알립 및/또는 IPv4 비정상적인 주소 확인 프로토콜을 기본적으로 네트워크에 보냅니다. 이번 개선된 기능을 통해 특정 IP의 새 Pod MAC 주소 호스트에 올바른 정보로 ARP/NDP 캐시를 새로 고치도록 알립니다. 자세한 내용은 [지원되는 장치를](#) 참조하십시오.

### 1.9.43.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.44. RHSA-2022:9111 - OpenShift Container Platform 4.9.54 버그 수정 및 보안 업데이트

출시 날짜: 2023-12-06

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.54를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2022:9111](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2022:9110](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.54 --pullspecs
```

### 1.9.44.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.45. RHSA-2023:0574 - OpenShift Container Platform 4.9.55 버그 수정 및 보안 업데이트

출시 날짜: 2023-02-10

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.55를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2023:0574](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2023:0573](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.55 --pullspecs
```

### 1.9.45.1. 버그 수정

- 이전에는 일부 OpenStack 오브젝트 스토리지 인스턴스가 컨테이너 또는 오브젝트가 없는 요청

을 나열할 때 **204 No Content** 로 응답했습니다. 이 경우 OpenShift Container Platform에서 응답 나열을 올바르게 처리하지 못했습니다. 이번 업데이트를 통해 설치 프로그램은 나열할 0개의 항목 문제를 해결합니다. ([OCBUGS-6086](#))

### 1.9.45.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.46. RHSA-2023:0778 - OpenShift Container Platform 4.9.56 버그 수정 및 보안 업데이트

출시 날짜: 2023-02-22

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.56을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2023:0778](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHSA-2023:0777](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.56 --pullspecs
```

### 1.9.46.1. 버그 수정

- 이전 버전에서는 Pod 실패로 인해 인증서의 유효 기간을 인위적으로 연장하여 교체를 잘못했습니다. 이번 업데이트를 통해 인증서 유효 기간이 올바르게 확인되고 인증서가 올바르게 교체됩니다. ([OCBUGS-5938](#))

### 1.9.46.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트에서](#) 참조하십시오.

## 1.9.47. RHBA-2023:1026 - OpenShift Container Platform 4.9.57 버그 수정 및 보안 업데이트

출시 날짜: 2023-03-08

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.57을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2023:1026](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2023:1025](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.57 --pullspecs
```

### 1.9.47.1. 버그 수정

- 이전 버전에서는 `spec.provider` 에 대한 정의가 누락되어 `ClusterServiceVersion` 을 표시하려고 할 때 `Operator 세부 정보` 페이지가 실패했습니다. 이번 업데이트를 통해 `spec.provider` 없이 사용자 인터페이스가 작동하며 `Operator 세부 정보` 페이지가 실패하지 않습니다. ([OCBUGS-6694](#))

- 이전에는 Operator가 Swift에 연결할 수 없는 경우 **cluster-image-registry-operator** 가 PVC(영구 블록 클레임)를 사용하는 것으로 되돌아왔습니다. 이는 OpenShift Container Platform 클러스터가 OpenStack에서 실행되는 방식에 영향을 미칩니다. 이번 업데이트를 통해 **cluster-image-registry-operator**에는 초기 부팅 작업 중에 스토리지 백엔드를 자동으로 선택하기 위한 메커니즘이 포함되어 있습니다. Swift를 사용할 수 있는 경우 Operator는 Swift를 스토리지 백엔드로 선택합니다. 그러지 않으면 Operator에서 PVC를 발행하고 블록 스토리지를 사용합니다. PVC로 대체는 OpenStack 카탈로그가 있는 경우에만 발생합니다. ([OCBUGS-7371](#))

### 1.9.47.2. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.48. RHBA-2023:1322 - OpenShift Container Platform 4.9.58 버그 수정 업데이트

출시 날짜: 2023-03-28

OpenShift Container Platform 릴리스 4.9.58이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 [RHBA-2023:1322](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2023:1321](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.58 --pullspecs
```

### 1.9.48.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.

## 1.9.49. RHSA-2023:1525 - OpenShift Container Platform 4.9.59 버그 수정 및 보안 업데이트

출시 날짜: 2023-04-05

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.9.59를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 [RHSA-2023:1525](#) 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 [RHBA-2023:1524](#) 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.9.59 --pullspecs
```

### 1.9.49.1. update

기존 OpenShift Container Platform 4.9 클러스터를 최신 릴리스로 업데이트하려면 [CLI를 사용하여 클러스터 업데이트](#)에서 참조하십시오.