OpenShift Container Platform 4.17

릴리스 노트

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항

Last Updated: 2025-12-05

OpenShift Container Platform 4.17 릴리스 노트

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항

Legal Notice

Abstract

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

Table of Contents

1장. OPENSHIFT CONTAINER PLATFORM 4.17 릴리스 노트

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

RHEL(Red Hat Enterprise Linux) 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, 컴플라이언스 및 거버넌스 요구 사항을 충족할 수 있습니다.

1.1. 릴리스 정보

OpenShift Container Platform (RHSA-2024:3718)을 사용할 수 있습니다. 이 릴리스에서는 Kubernetes 1.30 을 CRI-O 런타임과 함께 사용합니다. 다음은 OpenShift Container Platform 4.17과 관련된 새로운 기능, 변경 사항, 알려진 문제에 대해 설명합니다.

OpenShift Container Platform 4.17 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 Container Platform 클러스터를 배포할 수 있습니다.

OpenShift Container Platform 4.17은 RHEL (Red Hat Enterprise Linux) 8.8 이상 버전 및 OpenShift Container Platform 4.17 종료 전에 릴리스된 RHEL (Red Hat Enterprise Linux) 8 이상 버전에서 지원됩니다. OpenShift Container Platform 4.17은 RHCOS(Red Hat Enterprise Linux CoreOS) 4.17에서도 지원됩니다. RHCOS에서 사용하는 RHEL 버전을 이해하려면 RHCOS(Red Hat Enterprise Linux CoreOS) 및 OpenShift Container Platform (Knowledgebase)에서 사용하는 RHEL 버전을 참조하십시오.

컨트롤 플레인에는 RHCOS 머신을 사용해야 하며 컴퓨팅 머신에 RHCOS 또는 RHEL을 사용할 수 있습니다. RHEL 머신은 OpenShift Container Platform 4.16에서 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.

x86_64, 64비트 ARM(**aarch64**), IBM Power®(**ppc64le**) 및 IBM Z®(**s390x**) 아키텍처를 포함하여 지원되는 모든 아키텍처에서 OpenShift Container Platform 4.17과 같은 홀수 릴리스의 지원 라이프사이클은 18개월입니다. 모든 버전 지원에 대한 자세한 내용은 Red Hat OpenShift Container Platform 라이프 사이클 정책을 참조하십시오.

OpenShift Container Platform 4.14 릴리스부터 Red Hat은 세 가지 새로운 라이프 사이클 분류 (Platform Aligned, Platform Agnostic, Rolling Stream)를 도입하여 Red Hat의 관리 및 관리를 단순화하고 있습니다. 이러한 라이프 사이클 분류를 통해 클러스터 관리자는 각 Operator의 라이프 사이클 정책을 이해하고 클러스터 유지 관리 및 예측 가능한 지원 범위를 가진 업그레이드 계획을 수립할 수 있습니다. 자세한 내용은 OpenShift Operator 라이프 사이클 을 참조하십시오.

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

NIST 검증 프로그램에 대한 자세한 내용은 암호화 모듈 유효성 검사 프로그램을 참조하십시오. 검증을 위해 제출된 RHEL 암호화 라이브러리의 개별 버전에 대한 최신 NIST 상태는 규정 준수 활동 및 정부 표준을 참조하세요.

1.2. OPENSHIFT 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. Cluster Resource Override Admission Operator

1.3.1.1. Cluster Resource Override Operator 이동

기본적으로 설치 프로세스는 작업자 노드에 Cluster Resource Override Operator Pod를 생성하고 컨트롤 플레인 노드에서 Cluster Resource Override Pod를 생성합니다. 필요에 따라 이러한 Pod를 인프라 노드와 같은 다른 노드로 이동할 수 있습니다. 자세한 내용은 Cluster Resource Override Operator Pod 이동을 참조하십시오.

1.3.1.2. Cluster Resource Override Operator Pod는 배포 오브젝트에서 소유

Cluster Resource Override Operator Pod는 이제 deployment 오브젝트에서 소유합니다. 이전에는 Operator가 데몬 세트 오브젝트에서 소유했습니다. Operator에 배포를 사용하면 추가 보안을 포함하여 여러 문제가 해결됩니다. 작업자 노드에서 Pod를 실행하는 기능을 추가합니다.

1.3.2. 확장 (OLM v1)

1.3.2.1. OLM(Operator Lifecycle Manager) v1 문서가 새 Extensions 가이드(기술 프리뷰)로 이동됨

OpenShift Container Platform 4.14부터 기술 프리뷰에 있는 OLM v1에 대한 문서가 이제 Extensions 라는 별도의 가이드로 이동 및 재작업되었습니다. 이전에는 OLM v1 설명서가 기존 Operator 가이드의 하위 섹션이며, 그렇지 않으면 기존 OLM 기능 세트를 문서화했습니다.

업데이트된 위치 및 가이드 이름은 보다 집중된 문서 환경을 반영하고 OLM v1과 기존 OLM을 구별하는 것을 목표로 합니다.

1.3.2.2. OLM v1 기술 프리뷰 기능

OLM v1의 이 기술 프리뷰 단계에서는 다음과 같은 기능이 도입되었습니다.

CRD(사용자 정의 리소스 정의) 업그레이드 안전성

클러스터 확장에서 제공하는 CRD를 업데이트하면 OLM v1에서 CRD 업그레이드 안전 전지 검사를 실행하여 이전 버전의 CRD CRD와 이전 버전과의 호환성을 보장합니다. CRD 업데이트에서는 클러스터에서 변경 사항을 진행하기 전에 검증 검사를 전달해야 합니다.
자세한 내용은 CRD(Custom Resource Definition) 업그레이드 보안 을 참조하십시오.

클러스터 확장을 위한 단일 오브젝트 소유권

OLM v1에서 Kubernetes 오브젝트는 한 번에 단일 **ClusterExtension** 오브젝트에서만 소유할 수 있습니다. 이렇게 하면 OpenShift Container Platform 클러스터 내의 오브젝트를 일관되게 관리하고 동일한 오브젝트를 제어하려고 하는 여러 클러스터 확장 간의 충돌을 방지할 수 있습니다.
자세한 내용은 클러스터 확장의 오브젝트 소유권을 참조하십시오.

보안 강화

OLM v1에는 클러스터 확장의 설치, 업데이트 및 관리를 위한 전용 서비스 계정이 필요합니다. 또한 catalogd는 HTTPS 암호화를 사용하여 카탈로그 서버 응답을 보호합니다.
자세한 내용은 클러스터 확장을 관리하기 위한 서비스 계정 생성을 참조하십시오.

상태 조건 개선

이번 릴리스에서는 OLM v1에 **ClusterExtension** API를 통한 향상된 상태 조건 및 오류 메시지가 포함되어 있습니다.

1.3.2.3. OLM v1에서 확장 및 알려진 문제가 지원됨

현재 OLM(Operator Lifecycle Manager) v1에서는 다음 기준을 모두 충족하는 클러스터 확장 설치를 지원합니다.

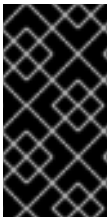
- 확장 기능은 기존 OLM에 도입된 **registry+v1** 번들 형식을 사용해야 합니다.
- 확장 기능은 **AllNamespaces** 설치 모드를 통한 설치를 지원해야 합니다.
- 확장에서는 Webhook를 사용하지 않아야 합니다.
- 확장자는 다음 파일 기반 카탈로그 속성을 사용하여 종속성을 선언해서는 안 됩니다.
  - **olm.gvk.required**
  - **olm.package.required**
  - **olm.constraint**

OLM v1은 설치하려는 확장이 이러한 제약 조건을 충족하는지 확인합니다. 설치하려는 확장이 이러한 제약 조건을 충족하지 않으면 클러스터 확장 상태에 오류 메시지가 출력됩니다.

OLM(Operator Lifecycle Manager) v1은 기존 OLM에 도입된 **OperatorConditions** API를 지원하지 않습니다.

확장 프로그램이 **OperatorConditions** API만 사용하여 업데이트를 관리하는 경우 확장이 올바르게 설치되지 않을 수 있습니다. 이 API에 의존하는 대부분의 확장은 시작 시 실패하지만 조정 중에 일부 확장이 실패할 수 있습니다.

이 문제를 해결하려면 확장 기능을 특정 버전에 고정할 수 있습니다. 확장을 업데이트하려는 경우 확장 기능을 참조하여 확장 기능을 새 버전에 고정하는 것이 안전한지 확인합니다.



중요

현재 OLM(Operator Lifecycle Manager) v1은 Red Hat 제공 Operator 카탈로그와 같은 프라이빗 레지스트리를 인증할 수 없습니다. 이것은 확인된 문제입니다. 결과적으로 Red Hat Operator 카탈로그를 설치하는 데 사용하는 OLM v1 절차가 작동하지 않습니다.
(OCPBUGS-36364)

1.3.3. 엣지 컴퓨팅

1.3.3.1. GitOps ZTP를 사용하여 호스트 펌웨어 설정 관리

GitOps ZTP로 배포하는 관리 클러스터의 호스트 펌웨어 설정을 구성할 수 있습니다. 관리 클러스터를 배포하는 데 사용하는 **SiteConfig** CR(사용자 정의 리소스)과 함께 호스트 프로필 YAML 파일을 저장합니다.

GitOps ZTP는 호스트 프로필을 사용하여 배포 중에 관리 클러스터 호스트에서 펌웨어 설정을 구성합니다. hub 클러스터에서 **FirmwareSchema** CR을 사용하여 관리 클러스터 호스트 펌웨어 스키마 및 **HostFirmwareSettings** CR을 검색하고 관리되는 클러스터 펌웨어 설정을 검색할 수 있습니다.

자세한 내용은 GitOps ZTP를 사용하여 호스트 펌웨어 설정 관리를 참조하십시오.

1.3.3.2. 이미지 기반 업그레이드 개선 사항

이번 릴리스에서는 이미지 기반 업그레이드로 다음과 같은 향상된 기능이 추가되었습니다.

- 허브에 **ImageBasedGroupUpgrade** API를 추가하여 대규모 관리 클러스터 그룹의 업그레이드 프로세스를 단순화합니다.
- **ImageBasedGroupUpgrade** API를 사용할 때 작업 완료를 위해 관리 클러스터에 레이블을 지정합니다.
- 시드 이미지 생성 전에 시드 클러스터 검증 개선
- 사용량이 관리 클러스터의 특정 임계값에 도달하면 컨테이너 스토리지 디스크 자동 정리
- **ImageBasedUpgrade** CR의 새 **status.history** 필드에 포괄적인 이벤트 기록 추가

ImageBasedGroupUpgrade API에 대한 자세한 내용은 허브의 ImageBasedGroupUpgrade CR을 사용하여 스케일링 시 이미지 기반 업그레이드 관리를 참조하십시오.

1.3.3.3. TPM 및 PCR 보호를 통한 디스크 암호화 (기술 프리뷰)

이번 릴리스에서는 신뢰할 수 있는 플랫폼 모듈(TPM) 및 플랫폼 구성 등록(PCR) 보호로 디스크 암호화를 활성화할 수 있습니다. **SiteConfig** CR(사용자 정의 리소스)의 **diskEncryption** 필드를 사용하여 디스크 암호화를 구성할 수 있습니다. **SiteConfig** CR을 구성하면 클러스터 설치 시 디스크 암호화가 가능합니다.

자세한 내용은 TPM 및 PCR 보호로 디스크 암호화 활성화를 참조하십시오.

1.3.3.4. GitOps ZTP 및 siteConfig 리소스를 사용하는 다중 노드 클러스터의 IPsec 암호화

GitOps ZTP 및 RHACM(Red Hat Advanced Cluster Management)으로 배포하는 관리형 다중 노드 클러스터에서 IPsec 암호화를 활성화할 수 있습니다. 관리 클러스터와 관리 클러스터 외부의 IPsec 끝점 간 트래픽을 암호화할 수 있습니다. OVN-Kubernetes 클러스터 네트워크의 노드 간 모든 네트워크 트래픽은 전송 모드에서 IPsec으로 암호화됩니다.

자세한 내용은 GitOps ZTP 및 SiteConfig 리소스를 사용하여 다중 노드 클러스터에 대한 IPsec 암호화 구성 을 참조하십시오.

1.3.3.5. 단일 노드 OpenShift 클러스터용 이미지 기반 설치

이미지 기반 설치는 설치 및 배포 시간을 크게 줄여 단일 노드 OpenShift 클러스터의 설치 및 배포 프로세스를 간소화합니다.

이미지 기반 워크플로를 사용하여 대상 호스트에 단일 노드 OpenShift의 인스턴스를 사전 설치할 수 있습니다. 이러한 사전 설치된 호스트는 최소한의 개입으로 연결이 끊긴 환경을 포함하여 네트워크의 맨 에지에서 신속하게 재구성하고 배포할 수 있습니다.

자세한 내용은 단일 노드 OpenShift 클러스터의 이미지 기반 설치 및 배포 이해를 참조하십시오 .

1.3.4. IBM Z 및 IBM LinuxONE

이번 릴리스에서 IBM Z® 및 IBM® LinuxONE은 이제 OpenShift Container Platform 4.17과 호환됩니다. z/VM, LPAR 또는 RHEL(Red Hat Enterprise Linux) KVM(커널 기반 가상 시스템)을 사용하여 설치를 수행할 수 있습니다. 설치 지침은 IBM Z 및 IBM LinuxONE에 설치 준비를 참조하십시오.

중요

컴퓨팅 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행해야 합니다.

1.3.4.1. IBM Z 및 IBM LinuxONE 주요 개선 사항

OpenShift Container Platform 4.17의 IBM Z® 및 IBM® LinuxONE 릴리스에서는 OpenShift Container Platform 구성 요소 및 개념에 향상된 기능과 새로운 기능이 추가되었습니다.

이번 릴리스에서는 IBM Z® 및 IBM® LinuxONE에서 다음 기능을 지원합니다.

- CPU 관리자
- Multiarch Tuning Operator
- LPAR에 대한 NVMe(Non-volatile Memory express) 지원
- Secondary Scheduler Operator
- etcd 대기 오차 튜닝

1.3.5. IBM Power

IBM Power®는 이제 OpenShift Container Platform 4.17과 호환됩니다. 설치 지침은 다음 설명서를 참조하십시오.

- IBM Power®에 클러스터 설치
- 네트워크가 제한된 환경에서 IBM Power®에 클러스터 설치

중요

컴퓨팅 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행해야 합니다.

1.3.5.1. IBM Power 주요 개선 사항

OpenShift Container Platform 4.17의 IBM Power® 릴리스는 OpenShift Container Platform 구성 요소에 개선 사항 및 새로운 기능을 추가합니다.

이 릴리스에서는 IBM Power에서 다음 기능을 지원합니다.

- Multiarch Tuning Operator
- Secondary Scheduler Operator
- etcd 대기 오차 튜닝
- 설치 프로그램이 프로비저닝한 IBM PowerVS용 인프라 - 클러스터 API로 이동

1.3.6. IBM Power, IBM Z 및 IBM LinuxONE 지원 매트릭스

OpenShift Container Platform 4.14부터 EUS (Extended Update Support)는 IBM Power® 및 IBM Z® 플랫폼으로 확장됩니다. 자세한 내용은 OpenShift EUS 개요 를 참조하십시오.

표 1.1. OpenShift Container Platform 기능

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
대체 인증 공급자	지원됨	지원됨
에이전트 기반 설치 관리자	지원됨	지원됨
지원되는 설치 관리자	지원됨	지원됨
로컬 스토리지 Operator를 통한 자동 장치 검색	지원되지 않음	지원됨
시스템 상태 점검으로 손상된 시스템 자동 복구	지원되지 않음	지원되지 않음
IBM Cloud®용 클라우드 컨트롤러 관리자	지원됨	지원되지 않음
노드에서 오버 커밋 제어 및 컨테이너 밀도 관리	지원되지 않음	지원되지 않음
CPU 관리자	지원됨	지원됨
Cron 작업	지원됨	지원됨
Descheduler	지원됨	지원됨
송신 IP	지원됨	지원됨
etcd에 저장된 데이터 암호화	지원됨	지원됨
FIPS 암호화	지원됨	지원됨
Helm	지원됨	지원됨
수평 Pod 자동 스케일링	지원됨	지원됨
호스팅된 컨트롤 플레인	지원됨	지원됨
IBM Secure Execution	지원되지 않음	지원됨
IBM Power® Virtual Server용 설치 관리자 프로비저닝 인프라 활성화	지원됨	지원되지 않음
단일 노드에 설치	지원됨	지원됨
IPv6	지원됨	지원됨

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
사용자 정의 프로젝트 모니터링	지원됨	지원됨
다중 아키텍처 컴퓨팅 노드	지원됨	지원됨
다중 아키텍처 컨트롤 플레인	지원됨	지원됨
다중 경로	지원됨	지원됨
network-Bound 디스크 암호화 - 외부 Tang 서버	지원됨	지원됨
NVMe(Non-volatile Memory express drives)	지원됨	지원되지 않음
NX-gzip for Power10 (Hardware Acceleration)	지원됨	지원되지 않음
oc-mirror 플러그인	지원됨	지원됨
OpenShift CLI(**oc**) 플러그인	지원됨	지원됨
Operator API	지원됨	지원됨
OpenShift Virtualization	지원되지 않음	지원되지 않음
IPsec 암호화를 포함한 OVN-Kubernetes	지원됨	지원됨
PodDisruptionBudget	지원됨	지원됨
PTP(Precision Time Protocol) 하드웨어	지원되지 않음	지원되지 않음
Red Hat OpenShift Local	지원되지 않음	지원되지 않음
스케줄러 프로파일	지원됨	지원됨
Secure Boot	지원되지 않음	지원됨
SCTP(스트림 제어 전송 프로토콜)	지원됨	지원됨
다중 네트워크 인터페이스 지원	지원됨	지원됨
IBM Power® (Hardware Acceleration)에서 다양한 SMT 수준을 지원하는 **openshift-install** 유틸리티	지원됨	지원됨
3-노드 클러스터 지원	지원됨	지원됨
토폴로지 관리자	지원됨	지원되지 않음

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
SCSI 디스크의 z/VM Emulated FBA 장치	지원되지 않음	지원됨
4K FCP 블록 장치	지원됨	지원됨

표 1.2. 영구 스토리지 옵션

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
iSCSI를 사용하는 영구 스토리지	지원됨 [1]	지원됨 [1], [2]
로컬 볼륨(LSO)을 사용한 영구 스토리지	지원됨 [1]	지원됨 [1], [2]
hostPath를 사용하는 영구 스토리지	지원됨 [1]	지원됨 [1], [2]
파이버 채널을 사용하는 영구 스토리지	지원됨 [1]	지원됨 [1], [2]
Raw Block을 사용하는 영구 스토리지	지원됨 [1]	지원됨 [1], [2]
EDEV/FBA를 사용하는 영구 스토리지	지원됨 [1]	지원됨 [1], [2]

1. 영구 공유 스토리지는 Red Hat OpenShift Data Foundation 또는 기타 지원되는 스토리지 프로토콜을 사용하여 프로비저닝해야 합니다.
2. 영구 비공유 스토리지는 iSCSI, FC와 같은 로컬 스토리지를 사용하거나 DASD, FCP 또는 EDEV/FBA와 LSO를 사용하여 프로비저닝해야 합니다.

표 1.3. Operator

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
cert-manager Operator for Red Hat OpenShift	지원됨	지원됨
Cluster Logging Operator	지원됨	지원됨
Cluster Resource Override Operator	지원됨	지원됨
Compliance Operator	지원됨	지원됨
Cost Management Metrics Operator	지원됨	지원됨
File Integrity Operator	지원됨	지원됨

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
HyperShift Operator	기술 프리뷰	기술 프리뷰
IBM Power® Virtual Server Block CSI Driver Operator	지원됨	지원되지 않음
Ingress 노드 방화벽 Operator	지원됨	지원됨
Local Storage Operator	지원됨	지원됨
MetalLB Operator	지원됨	지원됨
Multiarch Tuning Operator	지원됨	지원됨
Network Observability Operator	지원됨	지원됨
NFD Operator	지원됨	지원됨
NMState Operator	지원됨	지원됨
OpenShift Elasticsearch Operator	지원됨	지원됨
Secondary Scheduler Operator	지원됨	지원됨
Vertical Pod Autoscaler Operator	지원됨	지원됨

표 1.4. Multus CNI 플러그인

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
Bridge	지원됨	지원됨
Host-device	지원됨	지원됨
IPAM	지원됨	지원됨
IPVLAN	지원됨	지원됨

표 1.5. CSI 볼륨

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
복제	지원됨	지원됨

기능	IBM Power®	IBM Z® 및 IBM® LinuxONE
확장	지원됨	지원됨
스냅샷	지원됨	지원됨

1.3.7. Insights Operator

이제 Insights Operator에서 **openshift-** 또는 **kube-** 접두사가 붙은 네임스페이스에서 더 많은 OpenShift Container Platform 컨테이너 로그 데이터를 수집하고 권장 사항을 훨씬 더 빠르게 생성합니다. 또한 수집된 데이터가 서비스에 대해 정의되는 방법에 더 많은 유연성을 제공하기 위해 개선되었습니다.

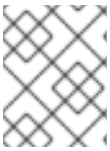
1.3.7.1. 빠른 권장 사항

이번 릴리스에서는 Rapid Recommendations라는 새로운 기능을 도입하여 Insights Operator가 수집하는 규칙을 원격으로 구성하는 보다 동적이고 버전 독립적인 메커니즘을 제공합니다.

빠른 권장 사항은 기존의 조건부 데이터 수집 메커니즘을 기반으로 합니다. Insights Operator는 **/console.redhat.com** 에서 실행되는 안전한 원격 엔드포인트 서비스에 연결하여 Red Hat에서 필터링하고 수집하는 컨테이너 로그 메시지를 결정하는 규칙이 포함된 정의를 검색합니다.

규칙이라고도 하는 조건부 데이터 수집 정의는 **pod.yml** 구성 파일에서 **conditionalGathererEndpoint** 라는 특성을 통해 구성됩니다.

```
conditionalGathererEndpoint: https://console.redhat.com/api/gathering/v2/%s/gathering_rules
```



참고

이전에는 Insights Operator가 수집하는 데이터를 결정하는 규칙이 해당 OpenShift Container Platform 버전에 하드 코딩되어 연결되었습니다.

이제 사전 구성된 끝점 URL에서 대상 버전의 OpenShift Container Platform을 정의하는 자리 표시자(**%s**)를 제공합니다.

1.3.7.2. 더 많은 데이터 수집 및 권장 사항 추가

이제 Insights Operator에서 더 많은 데이터를 수집하여 다른 애플리케이션에서 OpenShift Container Platform 배포를 사전에 관리하기 위해 수정 권장 사항을 생성하는 데 사용할 수 있는 다음 시나리오를 감지합니다.

- 더 이상 사용되지 않는 OpenShift SDN CNI 플러그인 을 사용하는 Pod 및 네임스페이스를 감지하고 배포에서 수집된 데이터에 따라 수행할 수 있는 작업에 대한 권장 사항을 생성합니다.
- RHOSP에서 CRD(사용자 정의 리소스 정의)를 수집합니다.
- **haproxy_exporter_server_threshold** 메트릭을 수집하여 OCPBUGS-36687 에 보고된 문제 및 수정을 탐지합니다.
- 데이터를 수집하여 해당 리소스의 관리에 잠재적으로 영향을 미칠 수 있으므로 **openshift-monitoring** 네임스페이스에 없는 사용자 정의 Prometheus Alertmanager 인스턴스를 감지합니다.

- 다른 애플리케이션 및 서비스에서 만료일 전에 인증서를 갱신하는 권장 사항을 생성하는 데 사용할 수 있는 기본 Ingress 컨트롤러 만료 인증서의 향후 만료를 감지합니다.
    - 이번 업데이트 이전에는 Insights Operator에서 **NotBefore** 및 **NotAfter** 날짜를 포함하여 모든 Ingress 컨트롤러 인증서에 대한 정보를 수집했습니다. 이 데이터는 이제 클러스터 전체에서 인증서 유효성을 더 쉽게 모니터링하기 위해 **aggregated/ingress_controllers_certs.json** 에 있는 **JSON** 파일로 컴파일됩니다. (OCPBUGS-35727)

1.3.8. 설치 및 업데이트

1.3.8.1. GCP의 사용자 정의 라벨 및 태그

이번 업데이트를 통해 Google Cloud의 사용자 정의 레이블 및 태그는 일반적으로 사용할 수 있습니다.

자세한 내용은 GCP의 사용자 정의 라벨 및 태그 관리를 참조하십시오 .

1.3.8.2. GPU를 사용하여 컴퓨팅 머신과 함께 Nutanix에 클러스터 설치

이번 업데이트를 통해 처리를 위해 GPU를 사용하는 컴퓨팅 머신과 함께 Nutanix에 클러스터를 설치할 수 있습니다. **install-config.yaml** 파일의 **compute.platform.nutanix.gpus** 매개변수를 사용하여 GPU를 컴퓨팅 노드에 연결합니다.

자세한 내용은 Nutanix의 설치 구성 매개변수를 참조하십시오 .

1.3.8.3. 여러 디스크를 사용하여 컴퓨팅 노드로 Nutanix에 클러스터 설치

이번 업데이트를 통해 여러 디스크가 연결된 컴퓨팅 머신과 함께 Nutanix에 클러스터를 설치할 수 있습니다. **install-config.yaml** 파일의 **compute.platform.nutanix.dataDisks** 매개변수를 사용하여 여러 디스크를 컴퓨팅 노드에 연결합니다.

자세한 내용은 Nutanix의 설치 구성 매개변수를 참조하십시오 .

1.3.8.4. 중앙 스페인 리전의 Azure에 클러스터 설치

이제 Azure에 **spaincentral** 인 중앙 스페인 리전의 OpenShift Container Platform 클러스터를 설치할 수 있습니다.

자세한 내용은 지원되는 Azure 리전 을 참조하십시오.

1.3.8.5. 다중 아키텍처 컴퓨팅 머신 구성을 지원하는 클러스터 설치

이번 릴리스에서는 다중 아키텍처 컴퓨팅 머신 구성을 지원하는 AWS(Amazon Web Services) 클러스터 및 Google Cloud 클러스터를 설치할 수 있습니다. 클러스터를 설치하는 동안 다음과 같은 방법으로 컨트롤 플레인 및 컴퓨팅 시스템에 대해 다른 CPU 아키텍처를 지정할 수 있습니다.

- 64비트 x86 컴퓨팅 시스템 및 64비트 ARM 컨트롤 플레인 시스템
- 64비트 ARM 컴퓨팅 시스템 및 64비트 x86 컨트롤 플레인 시스템

다중 아키텍처 컴퓨팅 머신이 있는 OpenShift Container Platform 클러스터는 다양한 아키텍처가 있는 컴퓨팅 머신을 지원합니다. 자세한 내용은 다음 설명서를 참조하십시오.

- 다중 아키텍처 지원으로 클러스터 설치 (AWS: 설치 관리자 프로비저닝 인프라)

- 다중 아키텍처 지원을 사용하여 클러스터 설치(AWS: 사용자 프로비저닝 인프라)
- 다중 아키텍처 지원(Google Cloud)을 사용하여 클러스터 설치

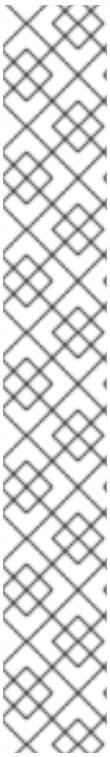
1.3.8.6. Flow Virtual Networking을 사용하여 Nutanix에 클러스터 설치

OpenShift Container Platform 4.17에서는 Flow Virtual Networking이 활성화된 Nutanix에 클러스터를 설치할 수 있습니다. 흐름 가상 네트워킹은 물리적 네트워크와 별도의 VPC, 서브넷 및 기타 가상 구성 요소를 사용하여 다중 테넌트 격리, 셀프 서비스 프로비저닝 및 IP 주소 보존을 제공하는 Nutanix AHV 클러스터용 소프트웨어 정의 네트워킹 솔루션입니다. 이 설치를 수행하려면 설치 전에 Nutanix AHV 환경에서 Flow Virtual Networking을 활성화합니다.

자세한 내용은 Flow Virtual Networking 개요 를 참조하십시오.

1.3.8.7. Cluster API는 Microsoft Azure 설치를 위한 Terraform을 대체합니다.

OpenShift Container Platform 4.17에서 설치 프로그램은 Terraform 대신 Cluster API를 사용하여 Azure에 설치하는 동안 클러스터 인프라를 프로비저닝합니다.



참고

Terraform을 교체하면 제한된 권한으로 서비스 주체를 사용하는 경우 다음 권한이 필요합니다.

- **Microsoft.Network/loadBalancers/inboundNatRules/read**
- **Microsoft.Network/loadBalancers/inboundNatRules/write**
- **Microsoft.Network/loadBalancers/inboundNatRules/join/action**
- **Microsoft.Network/loadBalancers/inboundNatRules/delete**
- **Microsoft.Network/routeTables/read**
- **Microsoft.Network/routeTables/write**
- **Microsoft.Network/routeTables/join/action**

필요한 권한에 대한 자세한 내용은 설치 관리자 프로비저닝 인프라에 대한 필수 Azure 권한을 참조하십시오.

1.3.8.8. 기존 서비스 계정을 사용하여 Google Cloud에 클러스터 설치

이번 업데이트를 통해 기존 서비스 계정을 사용하여 Google Cloud에 클러스터를 설치할 수 있으므로 설치 프로그램에서 사용하는 서비스 계정에 부여한 권한을 최소화할 수 있습니다. **install-config.yaml** 파일의 **compute.platform.gcp.serviceAccount** 및 **controlPlane.platform.gcp.serviceAccount** 매개변수에 이 서비스 계정을 지정할 수 있습니다. 자세한 내용은 Google Cloud에 대한 사용 가능한 설치 구성 매개변수를 참조하십시오.

1.3.8.9. 기존 IAM 프로필을 사용하여 AWS에 클러스터 설치

이번 릴리스에서는 기존 IAM(Identity and Access Management) 인스턴스 프로필을 사용하여 AWS(Amazon Web Services)에 OpenShift Container Platform을 설치할 수 있습니다. 자세한 내용은 선택적 AWS 구성 매개변수를 참조하십시오.

1.3.8.10. N4 머신 시리즈를 사용하여 Google Cloud에 클러스터 설치

이번 릴리스에서는 컴퓨팅 또는 컨트롤 플레인 시스템에 N4 머신 시리즈를 사용하여 Google Cloud에 클러스터를 배포할 수 있습니다. N4 시스템 시리즈의 지원되는 디스크 유형은 **hyperdisk-balanced** 입니다. 자세한 내용은 GCP의 설치 구성 매개변수를 참조하십시오.

1.3.8.11. 클러스터 API는 Google Cloud 설치를 위한 Terraform을 대체합니다.

이번 릴리스에서는 설치 프로그램에서 Terraform 대신 Cluster API를 사용하여 Google Cloud에 설치하는 동안 클러스터 인프라를 프로비저닝합니다.

1.3.8.12. RHOSP에 대한 3-노드 클러스터 지원

이제 설치 관리자 프로비저닝 인프라에 3-노드 클러스터 배포가 RHOSP(Red Hat OpenStack Platform)에서 지원됩니다.

자세한 내용은 OpenStack에 3-노드 클러스터 설치를 참조하십시오.

1.3.8.13. 로컬 디스크에 루트 볼륨 및 etcd를 사용하여 RHOSP(Red Hat OpenStack Platform) 배포 (일반 사용 가능)

이제 이 일반적으로 사용 가능한 기능을 사용하여 2일 차 배포로 etcd를 루트 볼륨(Cinder)에서 전용 임시 로컬 디스크로 이동할 수 있습니다.

자세한 내용은 로컬 디스크에 rootVolume 및 etcd를 사용하여 OpenStack에 배포를 참조하십시오.

1.3.9. Operator 라이프사이클

1.3.9.1. OLM(Operator Lifecycle Manager) v1의 새로운 가이드 위치 및 릴리스 노트 섹션(기술 프리뷰)

이 릴리스를 시작하는 새로운 가이드 위치를 포함하여 OpenShift Container Platform 4.17 이상의 OLM v1에 대한 릴리스 노트는 OLM v1의 새로운 기능 및 개선 사항 섹션을 참조하십시오 .

이 "Operator 라이프사이클" 섹션은 향후 릴리스에서 기존 OLM의 새로운 기능 및 개선 사항을 계속 설명합니다.

1.3.9.2. 더 이상 사용되지 않는 Operator에 대한 웹 콘솔 경고

더 이상 사용되지 않는 패키지, 채널 또는 버전이 카탈로그의 Operator에 대해 정의되면 OpenShift Container Platform 웹 콘솔에 OperatorHub의 사전 설치 및 설치 후 페이지에서 사용자 정의 사용 중단 메시지를 포함하여 Operator의 영향을 받는 요소에 대한 경고 배지가 표시됩니다.

Operator 카탈로그의 사용 중단 스키마에 대한 자세한 내용은 Operator Framework 패키징 형식 → 스키마 → olm.deprecations 스키마 를 참조하십시오.

1.3.10. Operator 개발

1.3.10.1. 클라우드 공급자의 Operator에 대한 토큰 인증: GCP 워크로드 ID

이번 릴리스에서는 OLM(Operator Lifecycle Manager)에서 관리하는 Operator는 GCP 워크로드 ID에 대해 구성된 Google Cloud 클러스터에서 실행할 때 토큰 인증을 지원할 수 있습니다. Operator 작성자가 Operator에서 GCP Workload Identity를 지원할 수 있는 경우 CCO(Cloud Credential Operator)를 업데이

트하면 특정 단기 인증 정보를 반자동으로 프로비저닝할 수 있습니다.

자세한 내용은 GCP Workload Identity를 사용하여 OLM 관리 Operator의 CCO 기반 워크플로를 참조하십시오.

1.3.11. OpenShift CLI(oc)

1.3.11.1. HyperShift KubeVirt CoreOS 컨테이너를 포함하는 oc-mirror

이번 릴리스에서는 OpenShift Container Platform 릴리스 페이로드를 미러링할 때 oc-mirror에 HyperShift KubeVirt 공급자에 대한 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지가 포함됩니다.

KubeVirt Container RHCOS를 추출하려면 **imageSetConfig.yaml** 파일에서 false로 설정된 **kubeVirtContainer** 플래그를 **true** 로 설정해야 합니다. 이렇게 하면 호스팅된 클러스터의 노드 역할을 하는 KubeVirt 가상 머신에 필요한 이미지를 포함하여 연결이 끊긴 환경을 지원합니다.

1.3.12. Machine Config Operator

1.3.12.1. MCO에서 지원하는 컨트롤 플레인 TLS 보안 프로필

MCO(Machine Config Operator) 및 Machine Config Server는 이제 컨트롤 플레인 구성 요소에 대해 구성된 TLS 보안 프로필을 사용합니다. 자세한 내용은 컨트롤 플레인의 TLS 보안 프로필 구성을 참조하십시오.

1.3.12.2. AWS의 업데이트된 부팅 이미지 지원 (기술 프리뷰)

업데이트된 부팅 이미지가 AWS(Amazon Web Services) 클러스터의 기술 프리뷰 기능으로 지원됩니다. 이 기능을 사용하면 클러스터를 업데이트할 때마다 노드 부팅 이미지를 업데이트하도록 클러스터를 구성할 수 있습니다. 기본적으로 클러스터의 부팅 이미지는 클러스터와 함께 업데이트되지 않습니다. 자세한 내용은 업데이트된 부팅 이미지 업데이트를 참조하십시오.

1.3.12.3. GA로 승격된 GCP 클러스터의 업데이트된 부팅 이미지

업데이트된 부팅 이미지가 GCP(Google Cloud Platform) 클러스터의 GA로 승격되었습니다. 자세한 내용은 업데이트된 부팅 이미지 업데이트를 참조하십시오.

1.3.12.4. GA로 승격된 노드 중단 정책

노드 중단 정책 기능이 GA로 승격되었습니다. 노드 중단 정책을 사용하면 워크로드에 대한 중단이 거의 또는 전혀 필요하지 않은 Ignition 구성 오브젝트 변경 세트를 정의할 수 있습니다. 자세한 내용은 노드 중단 정책을 사용하여 머신 구성 변경으로 인한 중단을 최소화합니다.

1.3.13. 머신 관리

1.3.13.1. AWS 배치 그룹 파티션 번호 지원

이번 릴리스에서는 AWS(Amazon Web Services)에서 OpenShift Container Platform **MachineSet** 의 **placementGroup** Cryostat 필드가 도입되었습니다. 이 기능을 사용하면 기존 배치 그룹 내에서 파티션 번호를 지정하여 정확한 인스턴스 할당 및 개선된 내결함성을 활성화할 수 있습니다. 예를 들어 머신 세트를 사용하여 Elastic Fabric Adapter 인스턴스의 배치 그룹에 머신 할당을 참조하십시오.

1.3.13.2. 머신 세트를 사용하여 용량 예약 구성

OpenShift Container Platform 릴리스 4.17에서는 Microsoft Azure 클러스터에서 용량 예약 그룹을 사용하여 온디맨드 용량 예약을 지원합니다. 자세한 내용은 컴퓨팅 또는 컨트롤 플레인 *머신 세트의 머신 세트를 사용하여 용량 예약 구성*을 참조하십시오.

1.3.14. 모니터링

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

1.3.14.1. 모니터링 스택 구성 요소 및 종속 항목에 대한 업데이트

이 릴리스에는 클러스터 내 모니터링 스택 구성 요소 및 종속 항목에 대한 다음 버전 업데이트가 포함되어 있습니다.

- Alertmanager 0.27.0
- Prometheus Operator to Cryostat5.2
- Prometheus에서 2.53.1로
- prom-label-proxy to 0.11.0
- kube-state-metrics to 2.13.0
- node-exporter to 1.8.2
- Thanos 0.35.1

1.3.14.2. 경고 규칙 변경

참고

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

- 연결할 수 없는 API 및 권한 문제와 같은 Prometheus 및 Kubernetes API 오류에 대해 사용자에게 경고하기 위해 **PrometheusKubernetesListWatchFailures** 경고가 추가되어 서비스 검색이 자동으로 실패할 수 있습니다.

1.3.14.3. 사용자 정의 프로젝트에 스크랩 시 지터를 허용하도록 Prometheus 업데이트

이번 업데이트를 통해 사용자 정의 프로젝트에 대한 모니터링에 대한 Prometheus 구성이 스크랩 시 지터를 허용합니다. 이번 업데이트에서는 데이터 스토리지에 대한 하위 최적화 청크 압축을 표시하는 모니터링에 대한 데이터 압축을 최적화하여 이러한 배포의 시계열 데이터베이스에서 사용하는 디스크 공간을 줄입니다.

1.3.14.4. Network Observability Operator

Network Observability Operator는 OpenShift Container Platform 마이너 버전 릴리스 스트림과 독립적으로 업데이트를 릴리스합니다. 업데이트는 현재 지원되는 모든 OpenShift Container Platform 4 버전에서 지원되는 단일 롤링 스트림을 통해 제공됩니다. Network Observability Operator의 새로운 기능, 개선 사항 및 버그 수정에 대한 정보는 Network Observability 릴리스 노트 에서 확인할 수 있습니다.

1.3.15. 노드

1.3.15.1. 새로운 CRIO 명령 동작

OpenShift Container Platform 4.17부터 노드가 재부팅되면 **crio wipe** 명령은 CRI-O 바이너리가 완전히 종료되었는지 확인합니다. 깔끔하게 종료되지 않은 이미지는 손상되고 제거되는 이미지를 대상으로 합니다. 이 동작은 반 풀된 이미지 또는 기타 동기화되지 않은 파일로 인해 CRI-O가 시작되지 않도록 합니다. OpenShift Container Platform 4.15 및 4.16에서 **crio wipe** 명령은 노드가 재부팅될 때 모든 이미지를 제거합니다. **crio wipe** 명령의 새로운 동작은 효율성을 높이는 동시에 노드를 재부팅할 때 이미지 손상 위험을 줄일 수 있습니다.

1.3.15.2. must-gather 명령에 대한 새 플래그 추가

OpenShift Container Platform 릴리스 4.17에는 **oc adm must-gather** 명령과 함께 사용할 새 플래그 두 개를 추가하여 수집된 정보의 수명을 제한합니다. 다음 플래그 중 하나만 한 번에 사용할 수 있습니다. 플러그인이 권장되지만 이러한 플래그를 지원할 필요는 없습니다.

- **--since**: 5s, 2m 또는 3h와 같은 상대 기간보다 최신 로그만 반환합니다. 기본값은 모든 로그입니다.
- **--since-time**: RFC3339 형식으로 표시된 특정 날짜 이후의 로그만 반환합니다. 기본값은 모든 로그입니다.

oc adm must-gather 명령과 함께 사용할 전체 플래그 목록은 Must- gather 플래그 를 참조하십시오.

1.3.15.3. Pod에서 Linux 사용자 네임스페이스 지원 (기술 프리뷰)

OpenShift Container Platform 릴리스 4.17에서는 Pod 및 컨테이너를 Linux 사용자 네임스페이스에 배포할 수 있도록 지원합니다. 개별 사용자 네임스페이스에서 Pod 및 컨테이너를 실행하면 손상된 컨테이너가 다른 Pod 및 노드 자체를 초래할 수 있는 몇 가지 취약점을 완화할 수 있습니다. 자세한 내용은 Linux 사용자 네임스페이스에서 Pod 실행을 참조하십시오.

1.3.15.4. CRI-O 메트릭 포트에서 TLS 사용

OpenShift Container Platform 모니터링에서는 TLS 지원 끝점을 사용하여 CRI-O 컨테이너 런타임 메트릭을 가져옵니다. 이러한 인증서는 사용자가 아닌 시스템에서 관리합니다. OpenShift Container Platform 모니터링 쿼리가 새 포트로 업데이트되었습니다. 모니터링에서 사용하는 인증서에 대한 자세한 내용은 모니터링 및 OpenShift Logging Operator 구성 요소 인증서를 참조하십시오.

1.3.15.5. 온프레미스 클러스터에 컴퓨팅 노드 추가

이번 릴리스에서는 OpenShift CLI(**oc**)를 사용하여 ISO 이미지를 생성하여 컴퓨팅 노드를 추가할 수 있습니다. 이 노드를 사용하여 대상 클러스터에서 하나 이상의 노드를 부팅할 수 있습니다. 클러스터 설치 방법과 관계없이 이 프로세스를 사용할 수 있습니다.

자세한 내용은 온프레미스 클러스터에 작업자 노드 추가를 참조하십시오.

1.3.16. 네트워킹

1.3.16.1. PTP 할 마스터 클록으로 듀얼 NIC Intel E810 Logan Beach

이제 듀얼 Intel E810 Logan Beach 네트워크 인터페이스 컨트롤러(NIC)의 경우 **linuxptp** 서비스를 마스터 클록(T-GM)으로 구성할 수 있습니다. 다음 듀얼 E810 NIC의 경우 **linuxptp** 서비스를 T-GM으로 구성할 수 있습니다.

- Intel E810-XXVDA4T Westport 채널 NIC

- Intel E810-CQDA2T Logan Beach NIC

호스트 시스템 클록은 GNSS(Global Navigation Satellite Systems) 시간 소스에 연결된 NIC에서 동기화됩니다. 두 번째 NIC는 GNSS에 연결된 NIC에서 제공하는 1PPS 타이밍 출력과 동기화됩니다. 자세한 내용은 Configuring linuxptp services as a grandmaster clock for dual E810 NIC를 참조하십시오 .

1.3.16.2. 새 클러스터의 가상 서브넷 변경

OpenShift Container Platform 4.17 이상 버전의 경우 클러스터는 IPv4에 169.254.0.0/17을 사용하고 IPv6의 경우 fd69::/112를 기본 masquerade 서브넷으로 사용합니다. 이러한 범위는 사용자가 피해야 합니다. 업그레이드된 클러스터의 경우 기본 masquerade 서브넷이 변경되지 않습니다. masquerade 서브넷을 Day 2 작업으로 변경하는 방법에 대한 자세한 내용은 OVN-Kubernetes masquerade 서브넷을 Day 2 작업으로 구성을 참조하십시오.

1.3.16.3. SR-IOV 네트워크 지표 내보내기 활성화

이번 릴리스에서는 OpenShift Container Platform 웹 콘솔을 사용하여 SR-IOV Pod의 네트워킹 활동을 모니터링하여 SR-IOV(Single Root I/O Virtualization) VF(가상 기능) 메트릭을 쿼리할 수 있습니다. 웹 콘솔을 사용하여 SR-IOV VF 지표를 쿼리하면 SR-IOV 네트워크 지표 내보내기가 VF 네트워크 통계를 가져오고 VF가 연결된 Pod의 이름 및 네임스페이스와 함께 VF 네트워크 통계를 반환합니다.

자세한 내용은 SR-IOV 네트워크 지표 내보내기 활성화를 참조하십시오.

1.3.16.4. Border Gateway Protocol용 MetalLB 업데이트

이번 릴리스에서는 MetalLB에 BGP(Border Gateway Protocol) 피어 사용자 정의 리소스의 새 필드가 포함됩니다. **dynamicASN** 필드를 사용하여 BGP 세션의 원격 끝에 사용할 ASN(Autonomous System Number)을 감지할 수 있습니다. **spec.peerASN** 필드에서 ASN을 명시적으로 설정하는 대안입니다.

1.3.16.5. Kubernetes NMState Operator용 Microsoft Azure

Red Hat 지원은 Microsoft Azure에서 Kubernetes NMState Operator를 사용하지만 용량은 제한되어 있습니다. 지원은 시스템의 DNS 서버를 설치 후 작업으로 구성하는 것으로 제한됩니다.

자세한 내용은 Kubernetes NMState Operator 정보를 참조하십시오.

1.3.16.6. Kubernetes NMState Operator에서 수집한 메트릭 보기

Kubernetes NMState Operator, **kubernetes-nmstate-operator** 에서는 **kubernetes_nmstate_features_applied** 구성 요소에서 지표를 수집하여 즉시 사용할 수 있는 메트릭으로 노출할 수 있습니다. **관리자** 및 **개발자** 화면을 사용하여 이러한 메트릭을 볼 수 있습니다.

자세한 내용은 Kubernetes NMState Operator 정보를 참조하십시오.

1.3.16.7. 새로운 PTP 빠른 이벤트 REST API 버전 2 사용 가능

새로운 PTP 빠른 이벤트 O-RAN 릴리스 3 호환 REST API 버전 2를 사용할 수 있습니다. 이제 PTP Operator 관리 Pod에서 직접 호스트 하드웨어 PTP 이벤트를 수신하는 PTP 이벤트 소비자 애플리케이션을 개발할 수 있습니다.

PTP 이벤트 REST API v1 및 PTP 이벤트 소비자 애플리케이션 사이드카는 더 이상 사용되지 않습니다.

참고

이벤트 소비자 3.0의 O-RAN O-Cloud 알림 API 사양에서 리소스는 알림을 생성하는 하위 시스템의 계층적 경로로 정의됩니다. PTP 이벤트 REST API v2에는 리소스 경로에 포함된 모든 하위 계층 리소스에 대한 글로벌 서브스크립션이 없습니다. 사용 가능한 다양한 이벤트 유형에 소비자 애플리케이션을 별도로 서브스크립션합니다.

자세한 내용은 REST API v2를 사용하여 PTP 이벤트 소비자 애플리케이션 개발을 참조하십시오.

1.3.16.8. PTP 할 마스터 클록에 대한 자동 윤초 처리

PTP Operator는 이제 GPS(Global positioning System) 공지를 사용하여 윤초 파일을 자동으로 업데이트합니다.

윤초 정보는 **openshift-ptp** 네임스페이스에 **leap-configmap** 이라는 자동으로 생성된 **ConfigMap** 리소스에 저장됩니다.

자세한 내용은 PTP 할 마스터 클록에 대한 동적 윤초 처리 구성을 참조하십시오 .

1.3.16.9. SR-IOV 장치의 NIC 파티셔닝 (일반 사용 가능)

이번 업데이트를 통해 설치 시 SR-IOV(Single Root I/O Virtualization) 장치에 대해 NIC 파티셔닝을 활성화하는 기능이 일반적으로 사용 가능합니다.

자세한 내용은 SR-IOV 장치의 NIC 파티셔닝을 참조하십시오.

1.3.16.10. SR-IOV VF의 호스트 네트워크 설정 (일반 사용 가능)

이번 업데이트를 통해 기존 클러스터에서 SR-IOV(Single Root I/O Virtualization) 네트워크 가상 기능에 대한 호스트 네트워크 설정을 업데이트할 수 있습니다.

자세한 내용은 가상 기능에 대한 노드 네트워크 구성 정책을 참조하십시오.

1.3.16.11. 사용자 정의 네트워크 분할 (기술 프리뷰)

OpenShift Container Platform 4.17을 사용하면 사용자가 여러 네트워크를 생성하고 UDN(**UserDefinedNetwork**) CRD(사용자 정의 리소스 정의)의 기술 프리뷰를 통해 워크로드를 위한 기본 네트워크 또는 보조 네트워크로 선언할 수 있습니다. UDN을 사용하면 복잡한 네트워크 정책을 구성 및 관리하지 않고도 네임스페이스를 격리할 수 있습니다.

자세한 내용은 사용자 정의 네트워크 이해를 참조하십시오.

1.3.16.12. CoreDNS 버전 1.11.3으로 업데이트

OpenShift Container Platform 4.17에는 CoreDNS 버전 1.11.3이 포함되어 있습니다.

1.3.16.13. eBPF Manager Operator (기술 프리뷰)

기술 프리뷰로 제공되는 eBPF 관리자 Operator를 사용하면 eBPF 프로그램을 안전하게 배포 및 관리할 수 있습니다. OpenShift Container Platform 클러스터에서 eBPF 프로그램의 보안 로드, 언로드, 수정 및 모니터링을 용이하게 합니다. bpfman Operator 배포에 대한 자세한 내용은 eBPF Manager Operator 정보를 참조하십시오.

1.3.16.14. Ingress Node Firewall Operator에 대한 eBPF 프로그램 지원 (기술 프리뷰)

Ingress Node Firewall Operator에 대한 eBPF 프로그램의 보안 관리를 기술 프리뷰로 사용할 수 있습니다. 이 기능을 사용하려면 eBPF 관리자 Operator를 설치해야 하며 기술 프리뷰로도 사용할 수 있습니다. 자세한 내용은 Ingress Node Firewall Operator 통합을 참조하십시오.

1.3.16.15. MetalLB 변경

이번 업데이트를 통해 MetalLB는 **FRR-K8s** 를 기본 백엔드로 사용합니다. 이전에는 기술 프리뷰에서 사용할 수 있는 선택적 기능이었습니다. 자세한 내용은 MetalLB 및 FRR-K8의 통합 구성 을 참조하십시오.

MetalLB에는 BGP(Border Gateway Protocol) 피어 사용자 지정 리소스인 **connectTime** 의 새 필드도 포함됩니다. 이 필드를 사용하여 BGP가 인접한 연결 시도 사이에 대기하는 시간을 지정할 수 있습니다. 자세한 내용은 BGP 피어 사용자 지정 리소스 정보를 참조하십시오.

1.3.16.16. vfio-pci SR-IOV 장치에 대한 MTU 노출

이번 릴리스에서는 **vfio-pci** 드라이버를 사용하여 가상 기능의 MTU(최대 전송 단위)를 network-status pod 주석과 컨테이너 내부에서 사용할 수 있습니다.

자세한 내용은 vfio-pci SR-IOV 장치의 MTU 노출을 Pod에 참조하십시오 .

1.3.16.17. MetalLB 메트릭 이름 지정 업데이트

이번 릴리스에서는 MetalLB BGP 및 BFD 메트릭에 대한 이름 지정 규칙이 업데이트되었습니다.

- BGP 지표의 이름 지정은 **metallb_bgp_<metric_name** >에서 **frrk8s_bgp_<metric_name** >로 업데이트되었습니다.
- BFD 지표의 이름 지정은 **metallb_bfd_<metric_name** >에서 **frrk8s_bfd_<metric_name** >로 업데이트되었습니다.

새 형식의 모든 메트릭을 보려면 BGP 및 BFD에 대한 MetalLB 메트릭을 참조하십시오.

1.3.17. 레지스트리

1.3.17.1. S3 레지스트리 스토리지의 새로운 chunkSizeMiB 구성 매개변수

S3 API 호환 백엔드 스토리지를 사용하는 배포에 새로운 선택적 구성 매개변수인 **chunkSizeMiB** 를 사용할 수 있습니다. 구성된 경우 S3 API의 multipart 업로드 청크 크기를 결정합니다. 기본값은 **10** MiB이며 최소 **5** MiB입니다.

자세한 내용은 AWS S3의 이미지 레지스트리 Operator 구성 매개변수를 참조하십시오 .

1.3.18. RHCOS(Red Hat Enterprise Linux CoreOS)

1.3.18.1. RHCOS에서 RHEL 9.4 사용

RHCOS는 OpenShift Container Platform 4.17에서 RHEL (Red Hat Enterprise Linux) 9.4 패키지를 사용합니다. 이러한 패키지는 OpenShift Container Platform 인스턴스가 최신 수정 사항, 기능, 개선 사항, 하드웨어 지원 및 드라이버 업데이트를 받을 수 있도록 합니다.

1.3.18.2. DNF 패키지 관리자 지원

이번 릴리스에서는 DNF를 사용하여 사용자 지정 RHCOS(Red Hat Enterprise Linux CoreOS) 빌드에 주가 패키지를 설치할 수 있습니다. 자세한 내용은 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층 지정을 참조하십시오.

1.3.19. 스토리지

1.3.19.1. AWS EFS CSI 스토리지 사용량 메트릭 사용 가능

AWS(Amazon Web Services) EFS(Elastic File Service) 사용량 메트릭을 사용하면 EFS 볼륨에서 사용하는 공간을 모니터링할 수 있습니다. 이 기능은 일반적으로 사용할 수 있습니다.

중요

CSI 드라이버가 전체 볼륨을 통과하므로 이러한 메트릭을 켜면 성능이 저하될 수 있습니다. 따라서 이 옵션은 기본적으로 비활성화되어 있습니다. 관리자는 이 기능을 명시적으로 활성화해야 합니다.

자세한 내용은 AWS EFS 스토리지 CSI 사용 메트릭 을 참조하십시오.

1.3.19.2. 무단 볼륨 모드 변환 방지 일반적으로 사용 가능

이전에는 스냅샷이 수행된 원래 볼륨(filesystem 또는 raw 블록)의 모드가 새로 생성된 볼륨의 모드와 일치하는지의 검증이 없었습니다. 이로 인해 악의적인 사용자가 호스트 운영 체제의 알려진 취약점을 악용할 수 있는 보안 격차가 발생했습니다.

그러나 일부 사용자에게는 이러한 변환을 수행해야 하는 정당한 필요성이 있습니다. 이 기능을 통해 클러스터 관리자는 백업 벤더와 같은 신뢰할 수 있는 사용자 또는 애플리케이션에만 이러한 권한(**VolumeSnapshotContents 오브젝트**에서 업데이트 또는 패치 작업을 수행할 수 있음)을 제공할 수 있습니다.

볼륨 모드를 변환하려면 권한이 있는 사용자가 스냅샷 소스의 **snapshot.storage.kubernetes.io/allow-volume-mode-change: "true"** 를 변경해야 합니다.

이 기능은 일반적으로 사용 가능한 대로 지원됩니다.

1.3.19.3. GCP 파일 저장소의 리소스 자동 삭제를 일반적으로 사용할 수 있습니다.

이전 버전의 OpenShift Container Platform에서는 클러스터를 삭제할 때 GCP(Google Compute Platform) Filestore 스토리지에서 해당 클러스터에 속하는 모든 클라우드 리소스를 삭제하지 않았습니다. 이를 위해 클러스터를 제거하기 전에 Filestore 스토리지 클래스를 사용한 모든 PVC(영구 볼륨 클레임)를 수동으로 삭제해야 합니다.

OpenShift Container Platform 4.17에서는 클러스터를 삭제할 때 OpenShift Container Platform 설치 프로그램은 일반적으로 해당 클러스터에 속하는 모든 클라우드 리소스를 삭제해야 하므로 PVC를 수동으로 삭제할 필요는 없습니다. 그러나 GCP(Google Compute Platform) Filestore 리소스의 특수 특성으로 인해 자동화된 정리 프로세스에서 일부 드문 경우에서 모든 리소스를 제거하지 못할 수 있습니다. 이 기능은 일반적으로 사용 가능한 대로 지원됩니다.

자세한 내용은 클러스터 및 GCP 파일 저장소 삭제 를 참조하십시오.

1.3.19.4. Azure File CSI에서 스냅샷 지원 (기술 프리뷰)

OpenShift Container Platform 4.17에서는 Microsoft Azure File Container Storage Interface(CSI) Driver Operator에 대한 볼륨 스냅샷 지원이 도입되었습니다. 이 기능은 기술 프리뷰 기능으로 지원됩니다.

자세한 내용은 OpenShift Container Platform 및 CSI 볼륨 스냅샷에서 지원하는 CSI 드라이버 를 참조하십시오.

1.3.19.5. vSphere CSI에 대한 여러 vCenter 지원 (기술 프리뷰)

OpenShift Container Platform v4.17에서는 여러 vSphere 클러스터(vCenters)에 OpenShift Container Platform을 배포하는 기능이 도입되었습니다. 이 기능은 기술 프리뷰 상태에서 지원됩니다.

여러 vCenter는 설치 중에만 구성할 수 있습니다. 지원되는 최대 vCenter 클러스터 수는 3개입니다.

자세한 내용은 vSphere CSI에 대한 여러 vCenter 지원 및 vSphere 의 설치 구성 매개변수를 참조하십시오.

1.3.19.6. vSphere에서 스토리지 비활성화 및 활성화 (기술 프리뷰)

클러스터 관리자는 VMWare vSphere CSI(Container Storage Interface) 드라이버를 Day 2 작업으로 비활성화하여 vSphere CSI 드라이버가 vSphere 설정과 상호 작용하지 않도록 할 수 있습니다. 이 기능은 기술 프리뷰 수준에서 지원됩니다.

자세한 내용은 vSphere에서 스토리지 비활성화 및 활성화를 참조하십시오.

1.3.19.7. RWX/RWO SELinux 마운트(개발자 프리뷰)

볼륨에 많은 수의 파일이 포함된 경우 Pod를 시작하는 데 시간이 오래 걸릴 수 있습니다. SELinux 제한을 유지하는 동안 SELinux 레이블 지정 문제를 방지하려면 ReadWriteMany/ReadWriteOnce(RWX/RWO) SELinux 마운트 기능을 활성화할 수 있습니다. RWX/RWO SELinux 마운트 기능은 개발자 프리뷰 기능입니다. Red Hat에서 지원하지 않으며 시간이 지남에 따라 유지 관리하려는 프로덕션 또는 클러스터에서 이 기능을 활성화해서는 안 됩니다.

중요

RWX/RWO SELinux 마운트는 개발자 프리뷰 기능 전용입니다. 개발자 프리뷰 기능은 Red Hat에서 지원하지 않으며 기능적으로 완전하거나 프로덕션 준비가 되지 않습니다. 프로덕션 또는 비즈니스 크리티컬 워크로드에는 개발자 프리뷰 기능을 사용하지 마십시오. 개발자 프리뷰 기능을 사용하면 Red Hat 제품 오퍼링에 포함된 제품 기능에 미리 미리 액세스할 수 있으므로 개발 프로세스 중에 기능을 테스트하고 피드백을 제공할 수 있습니다. 이러한 기능에는 문서가 없을 수 있으며 언제든지 변경 또는 제거될 수 있으며 테스트는 제한됩니다. Red Hat은 관련 SLA 없이 개발자 프리뷰 기능에 대한 피드백을 제출하는 방법을 제공할 수 있습니다.

RWX/RWO SELinux 마운트 기능에 대한 자세한 내용은 RWX/RWO SELinux 마운트 기능 지식 센터 서비스 문서를 참조하십시오.

1.3.19.8. cns-migration을 사용하여 데이터 저장소 간에 CNS 볼륨 마이그레이션(개발자 프리뷰)

OpenShift Container Platform 4.17에서는 현재 데이터 저장소에 공간이 부족하거나 더 많은 고성능 데이터 저장소로 이동하려는 경우 데이터 저장소 간에 볼륨을 마이그레이션할 수 있습니다. 이 기능은 개발자 프리뷰 기능입니다. Red Hat에서 지원하지 않습니다.

중요

데이터 저장소 간 CNS 볼륨 마이그레이션은 개발자 프리뷰 기능 전용입니다. 개발자 프리뷰 기능은 Red Hat에서 지원하지 않으며 기능적으로 완전하거나 프로덕션 준비가 되지 않습니다. 프로덕션 또는 비즈니스 크리티컬 워크로드에는 개발자 프리뷰 기능을 사용하지 마십시오. 개발자 프리뷰 기능을 사용하면 Red Hat 제품 오퍼링에 포함된 제품 기능에 미리 미리 액세스할 수 있으므로 개발 프로세스 중에 기능을 테스트하고 피드백을 제공할 수 있습니다. 이러한 기능에는 문서가 없을 수 있으며 언제든지 변경 또는 제거될 수 있으며 테스트는 제한됩니다. Red Hat은 관련 SLA 없이 개발자 프리뷰 기능에 대한 피드백을 제출하는 방법을 제공할 수 있습니다.

cns-migration에 대한 자세한 내용은 데이터 저장소 간 CNS 볼륨 이동을 참조하십시오.

1.3.19.9. Secrets Store CSI Driver Operator에서 Google Secret Manager를 사용할 수 있습니다(기술 프리뷰)

이제 Secrets Store CSI Driver Operator를 사용하여 Google Secret Manager의 시크릿을 OpenShift Container Platform의 CSI(Container Storage Interface) 볼륨에 마운트할 수 있습니다. Secrets Store CSI Driver Operator는 기술 프리뷰 기능으로 사용할 수 있습니다.

사용 가능한 시크릿 저장소 공급자의 전체 목록은 시크릿 저장소 공급자 를 참조하십시오.

Secrets Store CSI Driver Operator를 사용하여 Google Secret Manager의 시크릿을 마운트하는 방법에 대한 자세한 내용은 Google Secret Manager 의 시크릿 마운트를 참조하십시오.

1.3.20. 확장 및 성능

1.3.20.1. 커널 모듈 관리 Operator

이번 릴리스에서는 지정된 경로의 콘텐츠를 **worker.setFirmwareClassPath** 에 지정된 경로로 복사하도록 펌웨어 검색 경로가 업데이트되었습니다(기본값: **/var/lib/firmware**). 자세한 내용은 예제 모듈 CR 을 참조하십시오.

1.3.20.2. etcd의 노드 확장

이번 릴리스에서는 클러스터가 베어 메탈 플랫폼에 설치된 경우 설치 후 작업으로 클러스터 컨트롤 플레인을 5개의 노드로 확장할 수 있습니다. etcd Operator는 추가 컨트롤 플레인 노드를 고려하여 적절하게 확장됩니다. 자세한 내용은 etcd의 노드 스케일링을 참조하십시오.

1.3.20.3. AMD EPYC Cryostat 4 CPU로 컴퓨팅 노드 지원

4.17.10 릴리스부터 **PerformanceProfile** CR(사용자 정의 리소스)을 사용하여 gRPCoa 및 Bergamo와 같은 AMD EPYC Cryostat 4 CPU가 있는 시스템에서 컴퓨팅 노드를 구성할 수 있습니다. 단일 NUMA 도메인(NPS=1) 구성만 지원됩니다. 현재 Pod별 전원 관리는 AMD에서 지원되지 않습니다.

1.3.21. 보안

1.3.21.1. 서명자 인증서 자동 교체

이번 릴리스에서는 모든 **etcd** 인증서가 새 네임스페이스인 **openshift-etcd** 에서 시작됩니다. 새 서명자 인증서가 만료 날짜에 근접하면 다음과 같은 작업이 수행됩니다.

1. 서명자 인증서의 자동 순환이 활성화됩니다.

2. 인증서 번들이 업데이트됩니다.

3. 모든 인증서는 새 서명자를 사용하여 다시 생성됩니다.

특정 보안을 삭제하고 상태 Pod 롤아웃이 완료될 때까지 대기하여 서명자 인증서의 수동 교체는 계속 지원됩니다.

1.3.21.2. sigstore 서명 이미지 확인

이번 릴리스에서는 기술 프리뷰 클러스터에서 Sigstore 서명을 사용하여 **quay.io/openshift-release-dev/ocp-release** 리포지토리를 참조하는 가져오기 사양을 사용하여 검색된 이미지를 확인합니다.

현재 이미지를 미러링하는 경우 이미지 확인이 성공하려면 **quay.io/openshift-release-dev/ocp-release:<release_image_digest_with_dash>.sig** Sigstore 서명도 미러링해야 합니다.

1.3.22. 웹 콘솔

1.3.22.1. OpenShift Lightspeed Operator는 웹 콘솔에서 사용 가능

OpenShift Container Platform 4.16부터는 웹 콘솔에서 OpenShift Lightspeed Operator를 사용할 수 있습니다. 이번 릴리스에서는 OpenShift Lightspeed를 검색할 수 있도록 마우스 가리키기 버튼이 추가되었습니다. 마우스 버튼을 클릭하면 클러스터에서 OpenShift Lightspeed를 활성화하고 설치하는 방법에 대한 지침과 함께 채팅 창이 표시됩니다. 기본 사용자 기본 설정을 변경할 때 OpenShift Lightspeed 버튼을 숨길 수 있습니다.

1.3.22.2. 관리자 화면

이번 릴리스에서는 웹 콘솔의 **관리자** 화면에 다음 업데이트가 도입되었습니다.

- 더 이상 사용되지 않는 Operator는 설치 전후에 Operator가 더 이상 사용되지 않는 경고 알림과 함께 OperatorHub에 표시됩니다.
- 콘텐츠를 수동으로 검색할 필요 없이 **MachineConfig** 오브젝트에 대한 구성 파일의 contnet을 확인할 수 있습니다.
- 클러스터가 Google Cloud with Workload Identity Foundation (WIF)에 있는 경우 **Operator 세부 정보 페이지 및 Operator 설치** 페이지에 경고가 추가되었습니다.
- ShipWright **BuildStrategy** 의 페이지가 **ClusterBuildStrategy** 및 **BuildStrategy** 탭이 있는 **shipwright** 페이지에 추가되었습니다.

1.3.22.2.1. 동적 플러그인을 사용하여 **프로젝트 생성** 모달 사용자 정의

이번 릴리스에서는 새로운 확장 포인트가 추가되어 동적 플러그인 작성자가 기본 **Create Project** 모달 대신 렌더링되는 구성 요소를 전달할 수 있습니다.

OpenShift Container Platform 콘솔 동적 플러그인 SDK 확장 기능에 대한 자세한 내용은 동적 플러그인 확장 유형을 참조하십시오.

1.3.22.2.2. 외부 **OpenID Connect (OIDC)** 토큰 발행자가 웹 콘솔에서 작동합니다.

이번 업데이트를 통해 내부 **oauth-server** 리소스 및 **oauth-apiserver** 리소스가 제거되고 외부 OpenID Connect(OIDC) 발행기로 교체되는 경우 웹 콘솔이 예상대로 작동합니다.

1.3.22.3. 개발자 화면

이번 릴리스에서는 웹 콘솔의 **개발자** 화면에 다음과 같은 업데이트가 도입되었습니다.

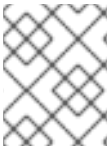
- 추가 흐름 중 하나를 사용하여 새 배포를 생성하면 **Git에서 가져오기** 또는 컨테이너 **이미지가** 자동으로 사이드바에 열립니다.
- OpenShift Container Platform에서 **유형을 식별할 수 없는 경우 목록을 사용하지 않고도 원하는 Git** 유형을 쉽게 선택할 수 있습니다.
- **Git에서 가져오기** 는 GitHub로 오픈 소스 변경 사항인 GitEA를 지원합니다.
- **PodDisruptionBudget** 제한에 도달하면 **토폴로지** 페이지에 경고 알림이 표시됩니다.
- **Git에서 가져오기** 흐름을 통해 애플리케이션을 가져올 때 S2I, buildpack, buildah 전략과 같은 shipwright 빌드 전략을 사용하여 이미지를 빌드할 수 있습니다.

1.4. 주요 기술 변경 사항

OpenShift Container Platform 4.17에는 다음과 같은 주요 기술 변경 사항이 추가되었습니다.

1.4.1. Operator SDK 1.36.1

OpenShift Container Platform 4.17은 Operator SDK 1.36.1을 지원합니다. 이 최신 버전을 설치하거나 업데이트하려면 Operator SDK CLI 설치를 참조하십시오.



참고

Operator SDK 1.36.1은 이제 Kubernetes 1.29를 지원하며 RHEL(Red Hat Enterprise Linux) 9 기본 이미지를 사용합니다.

Operator SDK 1.31.0을 사용하여 이전에 생성되거나 유지 관리되는 Operator 프로젝트가 있는 경우 Operator SDK 1.36.1과의 호환성을 유지하도록 프로젝트를 업데이트합니다.

- Go 기반 Operator 프로젝트 업데이트
- Ansible 기반 Operator 프로젝트 업데이트
- Helm 기반 Operator 프로젝트 업데이트
- 하이브리드 Helm 기반 Operator 프로젝트 업데이트
- Java 기반 Operator 프로젝트 업데이트

1.4.2. kube-apiserver의 경우 루프백 인증서 유효 기간을 3년으로 연장

이전에는 Kubernetes API Server의 자체 서명 루프백 인증서가 1년 후에 만료되었습니다. 이번 릴리스를 통해 인증서의 만료일이 3년으로 연장되었습니다.

1.4.3. VMware vSphere 7 및 VMware Cloud Foundation 4 일반 지원 종료

Broadcom은 VMware vSphere 7 및 VMware Cloud Foundation (VCF) 4에 대한 일반 지원을 종료합니다. 기존 OpenShift Container Platform 클러스터가 이러한 플랫폼 중 하나에서 실행 중인 경우 VMware 인프라를 지원되는 버전으로 마이그레이션하거나 업그레이드해야 합니다. OpenShift Container Platform은

vSphere 8 Update 1 이상 또는 VCF 5 이상에 설치를 지원합니다.

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 4.17에서 더 이상 사용되지 않고 삭제된 주요 기능의 최신 목록은 아래 표를 참조하십시오. 더 이상 사용되지 않고 삭제된 기능에 대한 자세한 내용은 표 뒤에 나열되어 있습니다.

다음 표에서 기능은 다음 상태로 표시됩니다.

- *사용할 수 없음*
- *기술 프리뷰*
- *정식 출시일 (GA)*
- *더 이상 사용되지 않음*
- *제거됨*

1.5.1. 더 이상 사용되지 않거나 삭제된 베어 메탈 모니터링

표 1.6. Bare Metal Event Relay Operator 추적기

기능	4.15	4.16	4.17
Bare Metal Event Relay Operator	제거됨	제거됨	제거됨

1.5.2. 더 이상 사용되지 않거나 삭제된 기능 이미지

표 1.7. Cluster Samples Operator 더 이상 사용되지 않거나 추적기 제거

기능	4.15	4.16	4.17
Cluster Samples Operator	정식 출시일 (GA)	더 이상 사용되지 않음	더 이상 사용되지 않음

1.5.3. 더 이상 사용되지 않거나 삭제된 기능 설치

표 1.8. 더 이상 사용되지 않거나 삭제된 추적기 설치

기능	4.15	4.16	4.17
oc adm release extract의 **--cloud** 매개변수	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
cluster.local 도메인에 대한 CoreDNS 와일드카드 쿼리	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

기능	4.15	4.16	4.17
compute.platform.openstack.rootVolume.type for RHOSP	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
controlPlane.platform.openstack.rootVolume.type for RHOSP	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
설치 관리자 프로비저닝 인프라 클러스터의 **install-config.yaml** 파일의 **ingressVIP** 및 **apiVIP** 설정	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
패키지 기반 RHEL 컴퓨팅 머신	정식 출시일(GA)	더 이상 사용되지 않음	더 이상 사용되지 않음
AWS(Amazon Web Services)의 **platform.aws.preserveBootstrapIgnition** 매개변수	정식 출시일(GA)	더 이상 사용되지 않음	더 이상 사용되지 않음
AWS(Amazon Web Services), VMware vSphere 및 Nutanix용 Terraform 인프라 공급자	정식 출시일(GA)	제거됨	제거됨
설치 관리자 프로비저닝 인프라를 사용하여 Alibaba Cloud에 클러스터 설치	기술 프리뷰	제거됨	제거됨
AWS Outposts의 컴퓨팅 노드를 사용하여 AWS에 클러스터 설치	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

1.5.4. Operator 라이프사이클 및 개발 중단 및 제거된 기능

표 1.9. Operator 라이프사이클 및 개발이 더 이상 사용되지 않거나 삭제된 추적기

기능	4.15	4.16	4.17
Operator SDK	정식 출시일(GA)	더 이상 사용되지 않음	더 이상 사용되지 않음
Ansible 기반 Operator 프로젝트를 위한 Scaffolding 툴	정식 출시일(GA)	더 이상 사용되지 않음	더 이상 사용되지 않음
Helm 기반 Operator 프로젝트의 스캐폴딩 툴	정식 출시일(GA)	더 이상 사용되지 않음	더 이상 사용되지 않음
Go 기반 Operator 프로젝트를 위한 Scaffolding 툴	정식 출시일(GA)	더 이상 사용되지 않음	더 이상 사용되지 않음
하이브리드 Helm 기반 Operator 프로젝트의 스캐폴딩 툴	기술 프리뷰	더 이상 사용되지 않음	더 이상 사용되지 않음

기능	4.15	4.16	4.17
Java 기반 Operator 프로젝트를 위한 Scaffolding 툴	기술 프리뷰	더 이상 사용되지 않음	더 이상 사용되지 않음
Platform Operator	기술 프리뷰	제거됨	제거됨
일반 번들	기술 프리뷰	제거됨	제거됨
Operator 카탈로그의 SQLite 데이터베이스 형식	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

1.5.5. 머신 관리 더 이상 사용되지 않거나 삭제된 기능

표 1.10. 머신 관리 더 이상 사용되지 않거나 삭제된 추적기

기능	4.15	4.16	4.17
Alibaba Cloud용 머신 API로 머신 관리	기술 프리뷰	제거됨	제거됨
vGPU Cloud의 클라우드 컨트롤러 관리자	기술 프리뷰	제거됨	제거됨

1.5.6. 더 이상 사용되지 않거나 삭제된 기능 모니터링

표 1.11. 더 이상 사용되지 않거나 삭제된 추적기 모니터링

기능	4.15	4.16	4.17
핵심 플랫폼 모니터링을 위한 전용 서비스 모니터를 활성화하는 **dedicatedServiceMonitors** 설정	더 이상 사용되지 않음	제거됨	제거됨
Prometheus의 리소스 지표를 쿼리하고 메트릭 API에 노출하는 Prometheus-adapter 구성 요소	더 이상 사용되지 않음	제거됨	제거됨
Alertmanager v1 API	더 이상 사용되지 않음	더 이상 사용되지 않음	제거됨

1.5.7. 더 이상 사용되지 않거나 삭제된 네트워킹

표 1.12. 더 이상 사용되지 않거나 삭제된 추적기 네트워킹

기능	4.15	4.16	4.17
OpenShift SDN 네트워크 플러그인	더 이상 사용되지 않음	더 이상 사용되지 않음	제거됨

기능	4.15	4.16	4.17
iptables	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
OpenShift SDN에서 OVN-Kubernetes로 실시간 마이그레이션 제한	사용할 수 없음	정식 출시일 (GA)	제거됨
PTP 이벤트 REST API v1 및 PTP 이벤트 소비자 애플리케이션 사이드카	정식 출시일 (GA)	정식 출시일 (GA)	더 이상 사용되지 않음

1.5.8. 스토리지 더 이상 사용되지 않거나 삭제된 기능

표 1.13. 더 이상 사용되지 않거나 삭제된 추적기 스토리지

기능	4.15	4.16	4.17
FlexVolume을 사용하는 영구 스토리지	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
AliCloud Disk CSI Driver Operator	정식 출시일 (GA)	제거됨	제거됨
공유 리소스 CSI 드라이버 [1]	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

1. 이제 Red Hat OpenShift 1.1 빌드에서 공유 리소스 CSI 드라이버 기능을 사용할 수 있습니다. 이 기능은 OpenShift Container Platform에서 더 이상 사용되지 않습니다. 이 기능을 사용하려면 Red Hat OpenShift 1.1 또는 최신 버전의 빌드를 사용해야 합니다.

1.5.9. 더 이상 사용되지 않거나 삭제된 노드 기능

표 1.14. 더 이상 사용되지 않거나 삭제된 추적기 노드

기능	4.15	4.16	4.17
ImageContentSourcePolicy (ICSP) 오브젝트	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
Kubernetes 토폴로지 레이블 **failure-domain.beta.kubernetes.io/zone**	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
Kubernetes 토폴로지 레이블 **failure-domain.beta.kubernetes.io/region**	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
cgroup v1	정식 출시일 (GA)	더 이상 사용되지 않음	더 이상 사용되지 않음

1.5.10. 웹 콘솔 더 이상 사용되지 않거나 삭제된 기능

표 1.15. 웹 콘솔 더 이상 사용되지 않거나 삭제된 추적기

기능	4.15	4.16	4.17
PatternFly 4	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
React Router 5	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

1.5.11. 워크로드 더 이상 사용되지 않거나 삭제된 기능

표 1.16. 워크로드 더 이상 사용되지 않거나 삭제된 추적기

기능	4.15	4.16	4.17
DeploymentConfig 오브젝트	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

1.5.12. 더 이상 사용되지 않는 기능

1.5.12.1. AWS Public Cloud에 배포된 클러스터의 경우 컴퓨팅 노드를 AWS Outposts로 확장하는 사용 중단 발표

이번 릴리스에서는 AWS Public Cloud에 배포된 클러스터의 AWS Outposts로 컴퓨팅 노드를 확장하는 것은 더 이상 사용되지 않습니다. 공용 AWS 리전에서 작동하는 기존 OpenShift Container Platform 클러스터의 확장으로 설치 후 AWS Outpost에 컴퓨팅 노드를 배포하는 기능은 OpenShift Container Platform 버전 4.20 릴리스와 함께 제거됩니다.

자세한 내용은 AWS VPC 클러스터를 AWS Outpost로 확장에서 참조하십시오.

1.5.12.2. AWS의 preserveBootstrapIgnition 매개변수

install-config.yaml 파일에서 AWS의 **preserveBootstrapIgnition** 매개변수가 더 이상 사용되지 않습니다. **bestEffortDeleteIgnition** 매개변수를 대신 사용할 수 있습니다. (OCPBUGS-33661)

1.5.12.3. kube-apiserver에서 더 이상 유효한 클라우드 구성 오브젝트를 가져오지 않음

OpenShift Container Platform 4.17에서 **kube-apiserver** 는 더 이상 유효한 클라우드 구성 오브젝트를 가져오지 않습니다. 결과적으로 **PersistentVolumeLabel** 승인 플러그인은 올바른 토폴로지가 없는 in-tree GCE(Google Compute Engine) 영구 디스크 PV(영구 디스크 영구 볼륨)를 거부합니다. (OCPBUGS-34544)

1.5.12.4. Patternfly 4 및 React Router 5의 사용 중단

OpenShift Container Platform 4.16에서는 Patternfly 4 및 React Router 5가 더 이상 사용되지 않습니다. 더 이상 사용되지 않는 정적은 OpenShift Container Platform 4.17에서 동일하게 유지됩니다. 모든 플러그인은 가능한 한 빨리 Patternfly 5 및 React Router 6로 마이그레이션해야합니다. (OCPBUGS-34538)

1.5.13. 삭제된 기능

1.5.13.1. TLS 1.2 사용자 정의 프로파일 암호에 대한 지원 삭제

OpenShift Container Platform은 다음 TLS(Transport Layer Security) 1.2 암호화 제품군을 더 이상 지원하지 않습니다. TLS v1.2의 사용자 지정 TLS 프로필의 일부로 이러한 암호화 제품군을 포함하면 예상되는 결과가 제공되지 않습니다.

- **TLS_RSA_WITH_AES_128_GCM_SHA256**
- **TLS_RSA_WITH_AES_256_GCM_SHA384**
- **TLS_RSA_WITH_AES_128_CBC_SHA**
- **TLS_RSA_WITH_AES_256_CBC_SHA**
- **TLS_RSA_WITH_3DES_EDE_CBC_SHA**

TLS v1.2를 사용해야 하는 경우 Intermediate TLS 프로파일 유형의 v1.2 암호화 제품군만 사용하여 TLS 핸드셰이크에서 v1.2를 올바르게 선택하도록 합니다. **intermediate** 는 기본 TLS v1.2 프로파일이며 다음 암호화 제품군을 포함합니다.

- **TLS_AES_128_GCM_SHA256**
- **TLS_AES_256_GCM_SHA384**
- **TLS_CHACHA20_POLY1305_SHA256**
- **ECDHE-ECDSA-AES128-GCM-SHA256**
- **ECDHE-RSA-AES128-GCM-SHA256**
- **ECDHE-ECDSA-AES256-GCM-SHA384**
- **ECDHE-RSA-AES256-GCM-SHA384**
- **ECDHE-ECDSA-CHACHA20-POLY1305**
- **ECDHE-RSA-CHACHA20-POLY1305**
- **DHE-RSA-AES128-GCM-SHA256**
- **DHE-RSA-AES256-GCM-SHA384**

TLS v1.2에서 보다 광범위한 암호의 경우 Custom TLS 프로파일 유형이 아닌 Intermediate TLS 프로필 유형을 사용합니다. TLS v1.2가 필요하지 않은 경우 암호화 암호가 있는 Modern 프로파일 유형을 사용합니다.

1.5.13.2. OpenShift SDN 네트워크 플러그인(Removed)

OpenShift SDN 네트워크 플러그인은 4.15 및 4.16에서 더 이상 사용되지 않습니다. 이번 릴리스에서는 SDN 네트워크 플러그인이 더 이상 지원되지 않으며 해당 콘텐츠가 문서에서 제거되었습니다.

1.5.13.3. RukPak 제거 (기술 프리뷰)

RukPak은 OpenShift Container Platform 4.12에서 기술 프리뷰 기능으로 도입되었습니다. OpenShift Container Platform 4.14부터는 OLM(Operator Lifecycle Manager) v1의 기술 프리뷰에서 구성 요소로 사용되었습니다.

OpenShift Container Platform 4.17부터 RukPak이 제거되고 OLM v1에서 사용하는 관련 기능이 다른 구성 요소로 이동되었습니다.

1.5.13.4. Alertmanager v1 API

Alertmanager **v0.27.0** 에서는 Alertmanager v1 API가 제거되어 더 이상 지원되지 않습니다. **api/v1/alerts** 와 같은 **alertmanager-main /api/v1/** 엔드포인트에 대한 모든 요청은 실패합니다. 문제를 완화하려면 Alertmanager v0.16.0 이후 지원되는 v2 API를 지원하도록 영향을 받는 Alertmanager 인스턴스를 업그레이드하고 v2 스키마를 사용하도록 모니터링 구성을 업데이트합니다.

1.6. 버그 수정

1.6.1. 베어 메탈 하드웨어 프로비저닝

- 이전 버전에서는 Redfish를 사용하여 특정 하드웨어 모델에 RAID를 구성하려고 하면 다음과 같은 오류가 발생할 수 있었습니다. **리소스에서 StorageControllers/Name 속성이 누락되었습니다**. 이번 업데이트를 통해 Redfish 표준에서 필드가 필요하지 않기 때문에 검증 논리에 더 이상 **Name** 필드가 필요하지 않습니다. (OCPBUGS-38465)

- 이전에는 Redfish Bare Metal Operator(BMO) 모듈에서 iDRAC9 Redfish 관리 인터페이스의 관리 인터페이스가 iPXE로 잘못 설정되었습니다. 이로 인해 **ironic.hardware.interfaces.management 진입점에서 could not find the following interface: ipxe** 오류가 발생했으며 Dell iDRAC(Remote Access Controller) 기반 서버에서 배포에 실패했습니다. 이번 릴리스에서는 문제가 해결되었습니다. (OCPBUGS-37261)

1.6.2. 빌드

- 이전에는 빌드에서 **GIT_LFS_SKIP_SMUDGE** 환경 변수를 설정할 수 없어 소스 코드를 복제할 때 해당 값을 사용할 수 없었습니다. 이로 인해 LFS 파일이 있는 일부 Git 리포지토리에 대한 빌드가 실패했습니다. 이번 릴리스에서는 빌드에서 이 환경 변수를 설정하고 빌드의 **git clone** 단계에서 이 변수를 사용하여 문제를 해결할 수 있습니다. (OCPBUGS-33215)

- 이전에는 개발자 또는 클러스터 관리자가 프록시 정보에 소문자 환경 변수 이름을 사용하는 경우 이러한 환경 변수가 빌드 출력 컨테이너 이미지로 전달되었습니다. 런타임 시 프록시 설정이 활성화되었으며 설정되지 않아야 했습니다. 이번 릴리스에서는 **_PROXY** 환경 변수의 소문자 버전이 빌드된 컨테이너 이미지로 유출되지 않습니다. 이제 **buildDefaults** 는 빌드 프로세스에 대해 생성된 빌드 및 설정 중에만 유지됩니다. 레지스트리에서 이미지를 푸시하기 전에만 제거됩니다. (OCPBUGS-12699)

1.6.3. 클라우드 컴퓨팅

- 이전에는 머신 컨트롤러에서 인스턴스 템플릿 복제 작업의 VMware vSphere 작업 ID를 저장하지 못했습니다. 이로 인해 머신이 **프로비저닝** 상태로 전환되고 전원이 꺼졌습니다. 이번 릴리스에서는 VMware vSphere 머신 컨트롤러에서 이 상태를 감지하고 복구할 수 있습니다. (OCPBUGS-1735)

- 이전에는 **machine-api** Operator가 **ERROR** 상태인 서버를 삭제할 때 반응했습니다. 이 문제는 서버가 포트 목록을 전달하지 않았기 때문에 발생했습니다. 이번 릴리스에서는 **ERROR** 상태에서 머신을 삭제해도 Operator 반응이 발생하지 않습니다. (OCPBUGS-33806)

- 이전에는 권한이 누락되어 Microsoft Azure 워크로드 ID 클러스터에서 용량 예약을 구성할 수 없었습니다. 이번 릴리스에서는 < **infra-name>-openshift-machine-api-azure-cloud-credentials** 사용자 정의 역할의 기본 인증 정보 요청으로 **Microsoft.Compute/capacityReservationGroups/deploy/action** 권한이 추가되어 용량 예약을 예상대로 구성할 수 있습니다. (OCPBUGS-37154)

- 이전에는 클러스터 자동 스케일러의 선택적 내부 기능으로 인해 구현되지 않은 경우 반복된 로그 항목이 발생했습니다. 이번 릴리스에서는 이 문제가 해결되었습니다. (OCPBUGS-33592)

- 이전 버전에서는 재시작 머신과 관련된 노드가 간단히 **Ready=Unknown** 상태가 되면 Control Plane Machine Set Operator에서 **UnavailableReplicas** 조건이 트리거되었습니다. 이 조건으로 인해 Operator가 **Available=False** 상태가 되고 해당 상태가 즉시 관리자 개입이 필요한 작동하지 않는 구성 요소를 나타내기 때문에 트리거 경고를 트리거했습니다. 이 경고는 다시 시작하는 동안 짧고 예상되지 않은 상태로 트리거되지 않아야 합니다. 이번 릴리스에서는 불필요한 경고를 트리거하지 않도록 노드 unreadiness의 유예 기간이 추가되었습니다. (OCPBUGS-20061)

- 이전 버전에서는 기능이 없는 OpenShift Container Platform 클러스터를 설치하고 나중에 Build 기능을 활성화하면 관련 Build 클러스터 구성 CRD(사용자 정의 리소스 정의)가 생성되지 않았습니다. 이번 릴리스에서는 Build 클러스터 구성 CRD 및 기본 인스턴스가 생성됩니다. 그러면 Build 기능을 완전히 구성하고 사용자 지정할 수 있습니다. (OCPBUGS-34395)

- 이전에는 기능이 비활성화된 경우에도 이미지 레지스트리, 빌드 및 **DeploymentConfig** 기능과 관련된 역할 바인딩이 모든 네임스페이스에서 생성되었습니다. 이번 릴리스에서는 클러스터에서 기능이 활성화된 경우에만 역할 바인딩이 생성됩니다. (OCPBUGS-34077)

1.6.4. Cloud Credential Operator

- 이전에는 클러스터의 시크릿을 단일 호출으로 가져왔습니다. 많은 수의 시크릿이 있을 때 API가 시간 초과되었습니다. 이번 릴리스에서는 Cloud Credential Operator가 100개의 시크릿으로 제한된 배치로 시크릿을 가져옵니다. 이러한 변경으로 인해 클러스터에 많은 시크릿이 있을 때 시간 초과가 방지됩니다. (OCPBUGS-41233)

- 이전에는 AWS Security Token Service에서 수동 모드를 사용하는 클러스터에 **awsSTSIAMRoleARN** 역할이 없는 경우 Cloud Credential Operator에서 오류를 보고했습니다. 이번 릴리스에서는 Cloud Credential Operator에서 더 이상 오류로 보고하지 않습니다. (OCPBUGS-33566)

- 이전 버전에서는 패스스루 권한이 충분한지 여부를 확인할 때 Cloud Credential Operator에서 프로젝트에 대한 권한이 유효하지 않은 Google Cloud API에서 응답을 수신한 경우가 있었습니다. 이 응답으로 인해 Operator의 성능이 저하되고 설치가 실패했습니다. 이번 릴리스에서는 이 오류를 정상적으로 처리하도록 Operator가 업데이트되었습니다. (OCPBUGS-36140)

1.6.5. Cluster Version Operator

- 이전 버전에서는 Go 루틴 간에 경쟁 조건이 거의 발생하지 않아 CVO가 시작된 후 CVO (Cluster Version Operator)가 패닉 상태가 되었습니다. 이번 릴리스에서는 Go 루틴 동기화가 개선되어 문제가 해결되었습니다. (OCPBUGS-32678)

1.6.6. 개발자 콘솔

- 이전에는 일부 브라우저에서 샘플 카탈로그의 일부 아이콘이 확장되어 읽기가 어려웠습니다. 이번 업데이트를 통해 아이콘의 크기를 올바르게 조정하여 더 이상 아이콘이 확장되지 않고 읽기 쉽습니다. (OCPBUGS-34516)

- 이전에는 s2i 빌드 전략이 **func.yml** 에 명시적으로 언급되지 않았습니다. 따라서 리포지터리를 사

용하여 OpenShift Serverless 함수를 생성할 수 없습니다. 또한 s2i가 언급되지 않았거나 **func.yml** 인 경우 오류 메시지를 사용할 수 없었습니다. 결과적으로 실패 이유를 식별할 수 없었습니다. 이번 업데이트를 통해 s2i 빌드 전략이 언급되지 않은 경우에도 사용자는 여전히 함수를 생성할 수 있습니다. s2i가 아닌 경우 사용자는 함수를 생성할 수 없습니다. 이제 두 경우 모두 오류 메시지가 다릅니다. (OCPBUGS-33733)

- 이전 버전에서는 OpenShift Container Platform 웹 콘솔에서 빠른 시작 가이드 둘러보기를 사용할 때 **작업** 대화 상자를 무시하면 **다음** 버튼을 여러 번 클릭하여 다음 단계로 건너뛰었습니다. 이번 업데이트를 통해 **확인란** 의 상태에 관계없이 한 번의 클릭만 필요합니다. (OCPBUGS-25929)

1.6.7. 드라이버 툴Kit(DTK)

- 이전에는 DTK가 **/etc/driver-toolkit-release.json** 구성 파일에 있는 **KERNEL_VERSION 및 RT** _KERNEL_VERSION과 동일한 값을 잘못 포함했습니다. 이번 업데이트를 통해 **RT_KERNEL_VERSION** 이 올바르게 표시됩니다. (OCPBUGS-33699)

1.6.8. etcd Cluster Operator

- 이전 버전의 etcd Operator는 단일 멤버 시간 초과와 일치하는 all-member 시간 초과와 함께 직렬로 etcd 멤버의 상태를 확인했습니다. 결과적으로 하나의 느린 멤버 확인에서 전체 시간 초과를 사용할 수 있으며 이후 멤버의 상태에 관계없이 나중에 멤버 확인이 실패할 수 있었습니다. 이번 릴리스에서는 etcd Operator가 멤버의 상태를 병렬로 확인하므로 한 구성원 검사의 상태 및 속도가 다른 멤버의 확인에는 영향을 미치지 않습니다. (OCPBUGS-36301)

- 이전에는 etcd Operator의 상태 점검이 주문되지 않았습니다. 결과적으로 모든 etcd 멤버가 정상이지만 상태 점검이 실패하는 경우가 있었습니다. 상태 점검 실패로 인해 Operator가 정상 멤버가 조기에 제거되는 스케일 다운 이벤트가 발생했습니다. 이번 릴리스에서는 Operator의 상태 점검이 정렬됩니다. 결과적으로 상태 점검은 etcd 멤버의 상태를 올바르게 반영하고 잘못된 스케일 다운 이벤트가 발생하지 않습니다. (OCPBUGS-36462)

1.6.9. 호스팅된 컨트롤 플레인

OpenShift Container Platform 4.17에서 호스팅된 컨트롤 플레인의 버그 수정 사항을 보려면 버그 수정 을 참조하십시오.

1.6.10. 이미지 레지스트리

- 이전에는 내부 이미지 레지스트리가 외부 OIDC(OpenID Connect) 사용자로 구성된 클러스터에서 사용자를 올바르게 인증하지 않았습니다. 이로 인해 사용자가 내부 이미지 레지스트리로 이미지를 내보내거나 가져올 수 없었습니다. 이번 업데이트를 통해 내부 이미지 레지스트리는 **SelfSubjectReview** API를 사용하여 시작되어 외부 OIDC **사용자로 구성된 클러스터에서 사용할 수 없는 openshift 특정 사용자** API의 사용을 삭제합니다. 결과적으로 내부 이미지 레지스트리로 다시 인증할 수 있습니다. (OCPBUGS-35335)

- 이전에는 인증서 디렉터리의 권한 오류로 인해 이미지 레지스트리를 실행할 수 없었습니다. 이 문제가 해결되었습니다. (OCPBUGS-38885)

- 이전 버전에서는 이미지 레지스트리 Operator 구성에 **regionEndpoint** 가 설정된 **virtualHostedStyle** 을 활성화하면 이미지 레지스트리에서 가상 호스팅 스타일 구성을 무시하고 시작할 수 없었습니다. 이번 업데이트에서는 가상 호스팅 스타일인 다운스트림 전용 버전을 사용하도록 강제 경로 스타일인 새 업스트림 배포 구성을 사용하여 문제를 해결합니다. (OCPBUGS-32710)

- 이전 버전에서는 OpenShift Container Platform이 Workload ID가 있는 Azure 클러스터에 배포된 경우 클러스터에 대해 생성된 스토리지 계정 및 이미지 레지스트리에 기본적으로 **스토리지 계정 키** 액세스가 활성화되어 배포에 보안 위험이 발생할 수 있었습니다.
이번 업데이트를 통해 Workload ID를 사용하는 새 설치에서 공유 액세스 키가 기본적으로 비활성화되어 공유 액세스 키를 사용하지 않도록 하여 보안이 향상됩니다.

중요

공유 액세스 키는 클러스터가 Workload ID를 사용하도록 구성된 경우에만 비활성화해야 합니다. Microsoft Entra Workload ID로 구성되지 않은 클러스터에서 공유 액세스 키를 비활성화하면 Image Registry Operator의 성능이 저하될 수 있습니다.

이 업데이트 이전에 생성된 기존 스토리지 계정의 경우 공유 액세스 키가 자동으로 비활성화되지 않습니다. 공유 키 사용을 방지하려면 관리자가 이러한 스토리지 계정에서 공유 액세스 키 지원을 수동으로 비활성화해야 합니다. 공유 액세스 키 비활성화에 대한 자세한 내용은 Azure Storage 계정에 대한 공유 키 권한 부여 방지를 참조하십시오.

OCPBUGS-39428

1.6.11. 설치 프로그램

- 이전에는 Cluster API Machine 오브젝트에서 IP 주소를 추출하면 단일 주소만 반환되었습니다. VMware vSphere에서 반환된 주소는 항상 IPv6 주소이며 이로 인해 주소를 라우팅할 수 없는 경우 **must-gather** 구현에 문제가 발생했습니다. 이번 릴리스에서는 Cluster API Machine 오브젝트가 IPv4를 포함한 모든 IP 주소를 반환하므로 **must-gather** 문제가 더 이상 VMware vSphere에서 발생하지 않습니다. (OCPBUGS-37427)

- 이전에는 IBM Cloud®의 클러스터를 기존 VPC에 설치할 때 설치 프로그램에서 지원되지 않는 VPC 리전을 검색했습니다. 지원되지 않는 VPC 리전을 알파벳순으로 설치하는 지원되는 VPC 리전에 설치하려고 하면 설치 프로그램이 충돌했습니다. 이번 릴리스에서는 리소스 조회 중에 완전히 사용할 수 없는 VPC 리전을 무시하도록 설치 프로그램이 업데이트되었습니다. (OCPBUGS-14963)

- 이전에는 설치 프로그램이 template 필드가 정의되었는지 여부에 관계없이 VMware vSphere에서 OVA를 다운로드하려고 했습니다. 이번 업데이트를 통해 문제가 해결되었습니다. 설치 프로그램은 template 필드가 정의되어 있는지 확인합니다. template 필드가 정의되지 않은 경우 OVA가 다운로드됩니다. template 필드가 정의되면 OVA가 다운로드되지 않습니다. (OCPBUGS-39240)

- 이전 버전에서는 사용자 지정 기능 게이트를 활성화하면 기능 게이트 **ClusterAPIInstallAWS=true** 가 활성화되지 않은 경우 AWS 클러스터에 설치가 실패하는 경우가 있었습니다. 이번 릴리스에서는 **ClusterAPIInstallAWS=true** 기능 게이트가 필요하지 않습니다. (OCPBUGS-34708)

- 이전에는 인프라 프로비저닝 실패로 인해 설치 프로그램이 종료되면 일부 프로세스가 계속 실행될 수 있었습니다. 이번 업데이트를 통해 설치 프로그램이 종료되면 모든 설치 관련 프로세스가 종료됩니다. (OCPBUGS-36378)

- 이전에는 기존 IAM 역할이 제공된 경우에도 설치 프로그램에서 AWS에 클러스터를 설치할 때 IAM 역할을 생성하고 삭제할 수 있는 권한이 필요했습니다. 이번 업데이트를 통해 설치 프로그램은 IAM 역할을 생성하는 경우에만 이러한 권한이 필요합니다. (OCPBUGS-36390)

- 이전에는 사용자에게 경고하지 않고 긴 클러스터 이름이 손상되었습니다. 이번 업데이트를 통해 설치 프로그램은 긴 클러스터 이름을 트리밍할 때 사용자에게 경고합니다. (OCPBUGS-33840)

- 이전에는 부트스트랩 수집 로그를 수집할 때 **openshift-install** CLI가 부트스트랩 노드에 연결하

지 못하는 경우가 있었습니다. 설치 프로그램에서 **부트스트랩 시스템과 같은 오류 메시지를 보고하여 release-image.service systemd 장치를 실행하지 않았습니다**. 이번 릴리스에서는 및 부트스트랩 수집 로그 문제가 발생한 후 설치 프로그램에서 **잘못된 로그 번들로 보고하거나 부트스트랩 시스템에 연결할 수 없어 부트스트랩 로그가 수집되지 않았습니다**. 이는 보다 정확한 오류 메시지입니다. (OCPBUGS-34953)

- 이전 버전에서는 AWS에 클러스터를 설치할 때 생성된 서브넷이 **kubernetes.io/cluster/<clusterID>: shared** 태그로 잘못 태그되었습니다. 이번 업데이트를 통해 이러한 서브넷에 **kubernetes.io/cluster/<clusterID>: owned** 태그로 올바르게 태그가 지정됩니다. (OCPBUGS-36904)

- 이전에는 설치 중에 저장된 로컬 etcd 데이터 저장소에서 설치에 실패한 경우 삭제되지 않고 설치 호스트에서 추가 공간을 소비했습니다. 이번 업데이트를 통해 인프라 프로비저닝 실패로 인해 설치가 성공적으로 수행되지 않으면 데이터 저장소가 삭제됩니다. (OCPBUGS-36284)

- 이전에는 폴더가 정의되지 않았으며 데이터 센터가 데이터 센터 폴더에 있는 경우 vCenter 서버의 루트부터 잘못된 폴더 구조가 생성되었습니다. Govmomi **DatacenterFolders.VmFolder** 를 사용하면 잘못된 경로를 사용했습니다. 이번 릴리스에서는 폴더 구조가 데이터 센터 인벤토리 경로를 사용하여 VM(가상 머신) 및 클러스터 ID 값과 결합하고 문제가 해결되었습니다. (OCPBUGS-38616)

- 이전 버전에서는 각 실패 도메인에 대해 템플릿을 정의할 때 설치 프로그램에 VMware vSphere에서 OVA를 다운로드하는 데 외부 연결이 필요했습니다. 이번 릴리스에서는 문제가 해결되었습니다. (OCPBUGS-39239)

- 이전에는 Nutanix에서 DHCP(Dynamic Host Configuration Protocol) 네트워크가 있는 클러스터를 설치하는 데 실패했습니다. 이번 릴리스에서는 이 문제가 해결되었습니다. (OCPBUGS-38934)

- 이전에는 SCOS의 EFI Secure Boot 실패로 인해 FCOS가 SCOS로 피벗된 경우 VM(가상 머신)이 부팅되지 않았습니다. 이번 릴리스에서는 **coreos.ovf** 구성 파일에서 Secure Boot가 활성화된 경우에만 Secure Boot가 비활성화되어 문제가 해결되었습니다. (OCPBUGS-37736)

- 이전에는 **install-config.yaml** 파일에서 지원되지 않는 아키텍처를 지정한 경우 **connection** reject 메시지와 함께 설치 프로그램이 실패했습니다. 이번 업데이트를 통해 설치 프로그램은 클러스터 아키텍처 매개변수를 올바르게 검증하여 설치에 성공합니다. (OCPBUGS-38841)

- 이전에는 드문 조건 om VMware vSphere Cluster API 머신으로 인해 vCenter 세션 관리 시간이 예기치 않게 발생했습니다. 이번 릴리스에서는 현재 및 이후 버전의 CAPV에서 Keep Alive 지원이 비활성화되어 문제가 해결되었습니다. (OCPBUGS-38677)

- 이전에는 AWS(Amazon Web Services)의 설치 프로그램에서 Amazon에서 비용을 청구하기 시작한 여러 IPv4 공용 IP 주소를 사용했습니다. 이번 릴리스에서는 사용자가 서비스에서 사용하는 IP 주소를 제어할 수 있도록 OpenShift Container Platform에서 고유한 BYO(공용 IPv4 풀을 가져올 수 있음) 지원이 제공됩니다. BYO 공용 IPv4 풀 기능이 활성화된 경우 새 권한 두 개, **ec2:DescribePublicIpv4Pools** 및 **ec2:DisassociateAddress** 가 필요하며 문제가 해결되었습니다. (OCPBUGS-35504)

- 이전 버전에서는 사용자가 기존 서브넷을 사용하고 프라이빗 클러스터를 만드는 동안 퍼블릭 서브넷을 제공할 때 설치 프로그램은 때때로 퍼블릭 서브넷에 생성된 로드 밸런서를 공용 인터넷에 노출했습니다. 이로 인해 프라이빗 클러스터의 원인이 무효화되었습니다. 이번 릴리스에서는 퍼블릭 서브넷을 제공하는 것이 프라이빗 클러스터를 중단하고 이를 방지하기 위해 사용자가 입력을 수정해야 함을 프라이빗 설치 중에 경고를 표시하여 문제를 해결합니다. (OCPBUGS-38963)

- 이전 버전에서는 설치 중에 **oc adm node-image create** 명령에서 kube-system/cluster-config-v1 리소스를 사용하여 플랫폼 유형을 확인했습니다. 이번 릴리스에서는 설치 프로그램에서 플랫폼 유형에 대한 보다 정확한 정보를 제공하는 인프라 리소스를 사용합니다. (OCPBUGS-39092)

- 이전에는 명령이 클러스터 전체 프록시 설정을 무시했기 때문에 프록시가 있는 제한된 환경에서 클러스터에 대해 실행할 때 **oc adm node-image create** 명령이 실패했습니다. 이번 릴리스에서는 명령이 실행되면 사용 가능한 클러스터 프록시 리소스 설정을 확인하여 명령이 성공적으로 실행되고 문제가 해결되었는지 확인합니다. (OCPBUGS-39090)

- 이전에는 에이전트 기반 설치 프로그램을 사용하여 클러스터를 설치할 때 클러스터에 컨트롤 플레인 노드를 추가하려고 할 때 assisted-installer 프로세스가 시간 초과될 수 있었습니다. 이번 업데이트를 통해 assisted-installer 프로세스는 assisted-service 프로세스에서 새로운 데이터를 로드하여 시간 초과를 방지합니다. (OCPBUGS-36779)

- 이전 버전에서는 VMware vSphere vCenter 클러스터에 표준 포트 그룹이 정의되어 있지 않은 ESXi 호스트가 포함되어 있고 설치 프로그램에서 OVA를 가져오기 위해 해당 호스트를 선택하려고 하면 가져오기에 실패하고 **장치 0에 대한 잘못된** 구성이 보고되었습니다. 이번 릴리스에서는 설치 프로그램에서 ESXi 호스트의 표준 포트 그룹이 정의되어 있는지 여부를 확인하고, 그렇지 않은 경우 정의된 표준 포트 그룹이 있는 ESXi 호스트를 찾을 때까지 계속하거나 문제를 해결하여 오류 메시지를 보고합니다. (OCPBUGS-38560)

- 이전에는 Cluster API Machine 오브젝트에서 IP 주소를 추출하면 단일 IP 주소만 반환되었습니다. VMware vSphere에서 반환된 주소는 항상 IPv6 주소이며 이로 인해 주소를 라우팅할 수 없는 경우 **must-gather** 구현에 문제가 발생했습니다. 이번 릴리스에서는 Cluster API Machine 오브젝트가 IPv4를 포함한 모든 IP 주소를 반환하므로 **must-gather** 문제가 더 이상 VMware vSphere에서 발생하지 않습니다. (OCPBUGS-37607)

- 이전에는 AWS에 클러스터를 설치할 때 EKS를 비활성화해야 하는 경우에도 설치 로그에 EBS(Elastic Kubernetes Service) 메시지가 표시될 수 있었습니다. 이번 업데이트를 통해 EKS 로그 메시지가 비활성화되었습니다. (OCPBUGS-35752)

- 이전에는 설치 관리자 프로비저닝 인프라 클러스터를 생성할 때 터미널에 예기치 않은 출력이 표시되었습니다. 이번 릴리스에서는 문제가 해결되어 예기치 않은 출력이 더 이상 표시되지 않습니다. (OCPBUGS-35547)

- 이전 버전에서는 **./openshift-install destroy cluster** 명령을 사용하여 클러스터를 삭제한 후 AWS에 클러스터를 설치할 때 이미 실행 중인 클러스터가 있다는 오류와 함께 설치에 실패했습니다. 이번 업데이트를 통해 클러스터가 삭제될 때 모든 남은 아티팩트가 제거되어 나중에 설치가 성공적으로 수행됩니다. (OCPBUGS-35542)

- 이전 버전에서는 AWS에 클러스터를 설치할 때 로드 밸런서 인그레스 규칙이 지속적으로 취소 및 재인증되어 클러스터 프로비저닝에 불필요한 API 호출 및 지연이 발생했습니다. 이번 업데이트를 통해 설치 중에 로드 밸런서 인그레스 규칙이 더 이상 취소되지 않으므로 API 트래픽 및 설치 지연이 줄어듭니다. (OCPBUGS-35440)

- 이전 버전에서는 **fixedIPs** 값 없이 **platform.openstack.controlPlanePort.network** 를 설정할 때 설치 프로그램에서 네트워크 누락된 서브넷에 대한 잘못된 오류 메시지를 출력했습니다. 이번 릴리스에서는 설치 프로그램에서 **install-config** 필드 **controlPlanePort** 에 필수 값이므로 유효한 서브넷 필터가 설정되어 있는지 확인합니다. (OCPBUGS-37104)

- 이전 버전에서는 사용자 프로비저닝 설치 플랫폼에 대한 IPv6 지원을 추가하면 특히 동일한 RHOSP(Red Hat OpenStack Platform) 플랫폼에서 두 개의 사용자 프로비저닝 설치 클러스터를 실행할 때 RHOSP(Red Hat OpenStack Platform) 리소스 이름 지정 문제가 발생했습니다. 이 문제는 두 클러스터가 네트워크, 서브넷 및 라우터 리소스에 대해 동일한 이름을 공유했기 때문에 발생했습니다. 이번 릴리스에서는 클러스터의 모든 리소스 이름이 해당 클러스터에 대해 고유하게 유지되므로 간섭이 발생하지 않습니다. (OCPBUGS-33973)

- 이전 버전에서는 설치 관리자 프로비저닝 인프라가 있는 IBM Power® Virtual Server에 클러스터를 설치할 때 로드 밸런서 시간 초과로 인해 설치에 실패할 수 있었습니다. 이번 업데이트를 통해 설치 프로그램은 시간 초과 대신 로드 밸런서를 사용할 수 있을 때까지 기다립니다. (OCPBUGS-34869)

- 이전에는 지원 설치 관리자를 사용할 때 콜론 문자(**:**)가 포함된 암호를 사용하여 설치에 실패했습니다. 이번 업데이트를 통해 암호에 콜론이 포함된 풀 시크릿으로 인해 지원 설치 프로그램이 실패하지 않습니다. (OCPBUGS-31727)

- 이전에는 SATA 하드웨어를 사용한 SSD(Solid State Drive)가 이동식 것으로 확인되었습니다. OpenShift Container Platform 지원 설치 관리자에서 적합한 디스크를 찾을 수 없고 설치가 중지되었다고 보고했습니다. 이번 릴리스에서는 이동식 디스크를 설치할 수 있습니다. (OCPBUGS-33404)

- 이전 버전에서는 설치 관리자 프로비저닝 인프라를 사용하여 베어 메탈에 클러스터를 설치할 때 부트스트랩 가상 머신의 네트워크가 느린 경우 설치 시간이 초과될 수 있었습니다. 이번 업데이트를 통해 광범위한 네트워크 성능 시나리오를 포함하도록 시간 초과 기간이 증가했습니다. (OCPBUGS-41500)

- 이전 버전에서는 IBM Power® Virtual Server에 클러스터를 설치할 때 설치 프로그램에 **madrid** 리전에 **e980** 시스템 유형이 나열되지 않았습니다. 이번 업데이트를 통해 설치 프로그램에 이 리전이 올바르게 나열됩니다. (OCPBUGS-38439)

- 이전에는 단일 노드 OpenShift 클러스터를 설치한 후 모니터링 시스템에서 여러 노드가 있는 클러스터에 적용되는 경고를 생성할 수 있었습니다. 이번 업데이트를 통해 단일 노드 OpenShift 클러스터는 단일 노드 OpenShift 클러스터에 적용되는 모니터링 경고만 생성합니다. (OCPBUGS-35833)

- 이전 버전에서는 IBM Power® Virtual Server에 클러스터를 설치할 때 DHCP 서버 네트워크 충돌로 인해 설치에 실패할 수 있었습니다. 이번 업데이트를 통해 설치 프로그램은 충돌을 방지하기 위해 DHCP 네트워크를 생성할 임의 번호를 선택합니다. (OCPBUGS-33912)

- 이전에는 설치 프로그램에서 Neutron API 엔드포인트를 사용하여 보안 그룹에 태그를 지정했습니다. 이 API는 특수 문자를 지원하지 않으므로 일부 RHOSP(Red Hat OpenStack Platform) 클러스터는 RHOSP에 설치되지 않았습니다. 이번 릴리스에서는 설치 프로그램에서 대체 엔드포인트를 사용하여 보안 그룹에 태그를 지정하여 문제가 더 이상 유지되지 않습니다. (OCPBUGS-36913)

- 이전 버전에서는 **install-config** 구성 파일에서 머신 풀의 **additionalNetworkIDs** 매개변수에 대해 잘못된 UUID(Universally Unique Identifier)를 설정하면 설치 프로그램이 클러스터 설치를 종료할 수 있었습니다. 이번 릴리스에서는 설치 프로그램이 클러스터 설치를 계속하기 전에 **additionalNetworkIDs** 매개변수의 유효성을 확인하여 이 문제가 더 이상 유지되지 않도록 합니다. (OCPBUGS-35420)

- 이전 버전에서는 IBM Power® Virtual Server 설치 관리자 프로비저닝 인프라 클러스터의 경우 DHCP(Dynamic Host Configuration Protocol)에 대한 네트워크 이름이 없는 경우 제거 코드에서 DHCP 리소스 삭제를 건너뛰었습니다. 이번 릴리스에서는 DHCP 리소스가 삭제되도록 DHCP가 **ERROR** 상태인지 확인합니다. (OCPBUGS-35039)

1.6.12. Insights Operator

- 이전 버전에서는 일부 Hypershift 호스트 클러스터에서 IO 아카이브에 네트워크 난독이 활성화된 경우에도 호스트 이름이 포함되었습니다. 이 문제는 해결되었으며 IO 아카이브에는 난독 처리 시 더 이상 호스트 이름이 포함되지 않습니다. (OCPBUGS-33082)

1.6.13. Machine Config Operator

- 이전 버전에서는 Telco RAN DU 참조 구성으로 OpenShift Container Platform 4.16을 실행하는 클러스터에서 오랜 기간 **cyclictest** 또는 **timerlat** 테스트가 **20** 이상 감지된 최대 대기 시간으로 실패할 수 있었습니다. 이 문제는 cgroup v2가 활성화되면 **psi** 커널 명령줄 인수가 기본적으로 **1**로 설정되었기 때문에 발생했습니다. 이번 릴리스에서는 cgroup v2를 활성화할 때 커널 인수에서 **psi=0**을 설정하여 문제가 해결되었습니다. OCPBUGS-34022 에서 보고된 **cyclictest** 대기 시간 문제도 해결되었습니다. (OCPBUGS-37271)

- 이전 버전에서는 클러스터 관리자가 기존 풀 시크릿을 참조하는 새 **MachineOSConfig** 오브젝트를 생성하는 경우 원래 풀 시크릿이 변경될 때마다 생성되는 이 보안의 정식 버전이 업데이트되지 않았습니다. 이번 릴리스에서는 문제가 해결되었습니다. (OCPBUGS-34079)

- 이전에는 **/etc/mco/internal-registry-pull-secret.json** 시크릿이 MCO(Machine Config Operator)에 의해 관리되었습니다. 최근 변경으로 인해 이 시크릿은 시간별로 순환됩니다. MCO가 이 시크릿에 대한 변경 사항을 감지할 때마다 클러스터의 각 노드에 시크릿을 롤아웃하여 중단되었습니다. 이번 수정을 통해 반복된 MachineConfig 업데이트가 롤아웃되지 않도록 다른 내부 메커니즘 프로세스가 내부 레지스트리 풀 시크릿으로 변경됩니다. (OCPBUGS-33913)

- 이전에는 정식 시크릿이 필요한 둘 이상의 **MachineOSConfig** 오브젝트를 생성한 경우 첫 번째 오브젝트만 빌드했습니다. 이번 수정으로 빌드 컨트롤러는 동일한 표준 시크릿을 사용하는 여러 **MachineOSBuilds**를 처리합니다. (OCPBUGS-33671)

- 이전 버전에서는 MCP(머신 구성 풀)의 사용 불가능한 노드 수보다 **maxUnavailable** 값이 높은 경우 차단된 노드를 업데이트 후보로 잘못 선택할 수 있었습니다. 이번 수정에서는 노드 컨트롤러에 노드 준비 상태 점검을 추가하여 차단된 노드가 업데이트를 대기열에 넣습니다. (OCPBUGS-33397)

- 이전에는 노드가 드레이닝 컨트롤러에서 여러 번 대기열에 있는 경우 노드를 두 번 드레이닝할 수 있었습니다. 이 동작은 클러스터상의 계층화 기능을 통해 노드 오브젝트에서 활동이 증가했기 때문일 수 있습니다. 이번 수정을 통해 드레이닝에 대해 노드가 한 번만 드레이닝되었습니다. (OCPBUGS-33134)

- 이전에는 빌드 상태를 읽기 위해 역참조가 실수로 삭제 **MachineOSConfig/MachineOSBuild** 인 경우 Machine Config Controller 및 Machine Build Controller 오브젝트에 잠재적인 패닉이 표시되었습니다. 패닉은 허용된 MachineOSConfig 삭제에 대해 경고하기 위해 추가 오류 조건으로 제어됩니다. (OCPBUGS-33129)

- 이전 버전에서는 OpenShift Container Platform 4.1 또는 4.2에서 버전 4.15로 업그레이드한 후 일부 머신은 프로비저닝 중에 중단되어 사용할 수 없었습니다. 이는 해당 노드에서 호환되지 않는 **machine-config-daemon** -daemon 바이너리로 인해 **machine-config-daemon-firstboot** 서비스가 실패했기 때문입니다. 이번 릴리스에서는 부팅하기 전에 올바른 **machine-config-daemon** 바이너리가 노드에 복사됩니다. (OCPBUGS-28974)

- 이전에는 RHCOS가 아닌 노드에서 클러스터 내 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층 지정을 구성하려고 하면 노드의 성능이 저하되었습니다. 이번 수정을 통해 노드 로그에 오류 메시지가 생성되지만 노드의 성능이 저하되지 않습니다. (OCPBUGS-19537)

1.6.14. 관리 콘솔

- 이전에는 **클러스터 개요** 페이지에 AWS 및 Red Hat OpenShift Dedicated 클러스터의 Red Hat OpenShift Service에 대한 404 오류가 발생하는 **문서 링크의 모든 단계 보기** 가 포함되어 있었습니다. 이번 업데이트를 통해 AWS 및 Red Hat OpenShift Dedicated 클러스터의 Red Hat OpenShift Service에 링크가 표시되지 않습니다. (OCPBUGS-37054)

- 이전에는 GCP Workload Identity를 지원하는 Google Cloud 클러스터에 있고 Operator에서 지원

하는 경우 경고가 표시되지 않았습니다. 이번 릴리스에서는 GCP Workload Identity 및 Federated Identity Operator 설치를 지원하기 위해 논리가 추가되어 이제 Google Cloud 클러스터에 있을 때 경고가 표시됩니다. (OCPBUGS-38591)

- 이전에는 **클러스터 설정** 페이지의 **업데이트** 그래프의 버전 번호 텍스트는 Firefox를 다크 모드에서 사용할 때 어두운 배경에 검정색 텍스트로 표시되었습니다. 이번 업데이트를 통해 텍스트가 흰색 텍스트로 표시됩니다. (OCPBUGS-38427)

- 이전에는 OpenShift Container Platform 4.15 이상에서 사용할 수 없는 PatternFly 4 참조 변수를 사용하는 동적 플러그인입니다. 이로 인해 RHACM(Red Hat Advanced Cluster Management)에 대한 비교 문제가 발생했습니다. 이번 업데이트를 통해 이제 동적 플러그인에서 사용하는 PatternFly 4 차트를 지원하는 이전 차트 스타일을 사용할 수 있습니다. (OCPBUGS-36816)

- 이전 버전에서는 **Display Admission Webhook** 경고 구현에서 일부 잘못된 코드와 관련된 문제가 발생했습니다. 이번 업데이트를 통해 불필요한 경고 메시지가 제거되었습니다. (OCPBUGS-35940)

- 이전 버전에서는 모든 HTTP 서버에 적용되는 글로벌 동기화 잠금을 통해 각 새로 고침 토큰과 관련된 동기화 잠금이 있는 goroutines가 생성되었습니다. 이번 릴리스에서는 외부 OIDC 환경이 있는 클러스터의 글로벌 새로 고침 동기화 잠금이 각 토큰에 대해 새로 고침되는 동기화로 교체되었습니다. 결과적으로 새로 고침 토큰 성능이 30%에서 50%로 향상되었습니다. (OCPBUGS-35080)

- 이전에는 **PodDisruptionBudget** create 및 edit 양식에서 **minAvailable** 경고에 대한 경고가 표시되지 않았습니다. 이번 업데이트를 통해 **minAvailable** 경고를 표시하는 코드 논리가 추가되어 위반하면 **minAvailable** 경고가 표시됩니다. (OCPBUGS-34937)

- 이전에는 **Operand Details** 페이지에 name과 일치하는 첫 번째 CRD에 대한 정보가 표시되었습니다. 이번 수정 후 **피연산자 세부 정보** 페이지에는 이름 및 피연산자 버전으로 일치하는 CRD에 대한 정보가 표시됩니다. (OCPBUGS-34901)

- 이전에는 하나의 비활성 또는 유휴 브라우저 탭으로 인해 다른 모든 탭에 대한 세션 만료가 발생했습니다. 이 변경으로 인해 비활성 브라우저 탭 또는 유휴 브라우저 탭이 하나만 있는 경우에도 모든 탭의 활동이 세션 만료를 방지합니다. (OCPBUGS-34387)

- 이전에는 텍스트 영역을 재조정할 수 없었습니다. 이번 업데이트를 통해 이제 텍스트 영역의 크기를 조정할 수 있습니다. (OCPBUGS-34200)

- 이전에는 **Completed 상태의 Pod에 대해 디버그 컨테이너** 링크가 표시되지 않았습니다. 이 변경으로 인해 이제 링크가 표시됩니다. (OCPBUGS-33631)

- 이전에는 잘못된 Prometheus 쿼리로 인해 OpenShift Container Platform 웹 콘솔에 **노드 목록** 페이지에 **파일 시스템** 지표가 표시되지 않았습니다. 이번 업데이트를 통해 **파일 시스템** 지표가 올바르게 표시됩니다. (OCPBUGS-33136)

- 이전에는 구성 문제로 인해 pseudolocalization이 작동하지 않았습니다. 이번 수정 후 pseudolocalization이 다시 작동합니다. (OCPBUGS-30218)

- 이전에는 **--user-auth** 플래그가 **disabled** 로 설정된 경우 콘솔 Pod가 루프 충돌했습니다. 이번 업데이트를 통해 콘솔 백엔드에서 이 값을 올바르게 처리합니다. (OCPBUGS-29510)

- 이전에는 사용률 카드에 용량과 **제한** 간의 관계를 잘못 나타내는 제한이 표시되었습니다. 이번 업데이트를 통해 **제한** 위치가 변경되었으며 문구가 업데이트되었습니다. (OCPBUGS-23332)

- 이전 버전에서는 일부 에지 사례에서 websockets를 사용하여 네임스페이스를 제공하지 않고 네임스페이스를 조사할 때 잘못된 리소스를 가져올 수 있었습니다. 이번 업데이트를 통해

websocket 요청을 방지하기 위해 리소스 감시 논리에 대한 검증이 추가되어 이 조건에서 오류를 기록합니다. (OCPBUGS-19855)

- 이전에는 화면 전환이 제대로 처리되지 않았습니다. 이번 업데이트를 통해 URL 검색 매개변수 또는 플러그인 경로 페이지 확장으로 전달되는 관점이 이제 관점을 올바르게 전환하고 올바른 URL 경로를 유지합니다. (OCPBUGS-19048)

1.6.15. 네트워킹

- 이전에는 SR-IOV Network Operator에 **SriovNetworkNodePolicies** 리소스가 무작위로 나열되었습니다. 이로 인해 **sriov-device-plugin** Pod가 연속 재시작 루프가 입력되었습니다. 이번 릴리스에서는 SR-IOV Network Operator가 결정적 순서로 정책을 나열하므로 **sriov-device-plugin** Pod가 연속 재시작 루프에 들어가지 않습니다. (OCPBUGS-36243)

- 이전에는 새 Pod 내에서 생성된 인터페이스가 비활성 상태로 유지되어 GARP(Gratuitous Address Resolution Protocol) 알림이 생성되었습니다. 알림이 클러스터에 도달하지 않아 클러스터 내부의 다른 pod의 ARP 테이블이 새 pod의 MAC 주소를 업데이트하지 못했습니다. 이 경우 ARP 테이블 항목이 만료될 때까지 클러스터 트래픽이 중단되었습니다. 이번 릴리스에서는 GARP 알림이 클러스터에 도달하도록 Pod 내부의 인터페이스가 활성화된 후 GARP 알림이 전송됩니다. 결과적으로 주변 Pod는 이전 동작을 통해 새 Pod보다 먼저 새 Pod를 식별할 수 있습니다. (OCPBUGS-30549)

- 이전에는 클러스터의 FIPS를 활성화하면 SR-IOV 장치 플러그인 Pod가 실패했습니다. 이번 릴리스에서는 SR-IOV 장치 플러그인 Pod에 FIPS가 활성화되어 클러스터에 FIPS가 작동하지 않습니다. (OCPBUGS-41131)

- 이전에는 예약된 CPU 수가 적은 성능 프로필을 사용하는 OpenShift Container Platform 노드를 재부팅한 후 경쟁 조건이 생성되었습니다. 이는 SR-IOV(Single Root I/O Virtualization) 가상 기능(VF)이 동일한 MAC 주소를 공유하고 VF를 사용하는 모든 Pod에 통신 문제가 발생하기 때문에 발생했습니다. 이번 릴리스에서는 SR-IOV Network Operator 구성 데몬을 업데이트하면 Operator에서 VF에 중복 MAC 주소가 없는지 확인합니다. (OCPBUGS-33137)

- 이전에는 **sriovOperatorConfig** CR(사용자 정의 리소스)을 삭제한 경우 새 **sriovOperatorConfig** CR을 생성할 수 없었습니다. 이번 릴리스에서는 **sriovOperatorConfig** CR을 삭제할 때 SR-IOV(Single Root I/O Virtualization) Network Operator에서 검증 Webhook를 제거하여 새 **sriovOperatorConfig** CR을 생성할 수 있습니다. (OCPBUGS-37567)

- 이전 버전에서는 다른 로드 밸런서를 사용하도록 클러스터를 전환하면 Ingress Operator에서 **IngressController** CR(사용자 정의 리소스) 상태의 **classicLoadBalancer** 및 **networkLoadBalancer** 매개변수에서 값을 제거하지 않았습니다. 이로 인해 CR의 상태가 **ClassicLoadBalancer 및 networkLoadBalancer 매개변수** 의 잘못된 정보를 보고했습니다. 이번 릴리스에서는 다른 로드 밸런서를 사용하도록 클러스터를 전환한 후 Ingress Operator가 이러한 매개변수에서 값을 제거하여 CR에서 보다 정확하고 혼란스러운 메시지 상태를 보고할 수 있습니다. (OCPBUGS-38646)

- 이전에는 멀티 캐스트 발신자와 멀티 캐스트 수신자가 동일한 노드에 있을 때 멀티 캐스트 패킷이 의도한 대상 노드에 도달하지 않았습니다. 이는 OVN-Kubernetes RPM 패키지 업데이트로 인해 발생했습니다. 이번 릴리스에서는 이 회귀 문제가 OVN-Kubernetes RPM 패키지에서 수정되어 문제가 더 이상 유지되지 않습니다. (OCPBUGS-34778)

- 이전에는 Ingress Operator에 대한 **LoadBalancer** 서비스를 생성할 때 변경 사항이 적용되지 않았음을 나타내는 로그 메시지가 생성되었습니다. 이 로그 메시지는 **Infra** 사용자 정의 리소스 변경 시에만 트리거해야 합니다. 이번 릴리스에서는 Ingress Operator에 대한 **LoadBalancer** 서비스를 생성할 때 이 로그 메시지가 더 이상 생성되지 않습니다. (OCPBUGS-34413)

- 이전에는 **DNSNameResolver** 컨트롤러에서 TTL(Time-to-live) 값이 만료된 IP 주소가 있는 DNS 이름의 DNS 요청을 CoreDNS Pod로 전송했습니다. 이로 인해 해당 Pod에 대한 DNS 요청 및 메모리 누수 문제가 발생했습니다. 이번 릴리스에서는 **DNSNameResolver** 컨트롤러에서 DNS 이름에 대한 업데이트된 IP 주소 및 TTL 값 목록을 수신할 때까지 대기합니다. 결과적으로 컨트롤러는 더 이상 잘못된 요청을 생성하여 Pod에 보내지 않습니다. CoreDNS Pod는 적절한 방식으로 DNS 요청에 응답하고 최신 IP 주소 및 TTL으로 **DNSNameResolver** 오브젝트를 업데이트할 수 있습니다. (OCPBUGS-33750)

- 이전 버전에서는 **must-gather** 툴을 사용할 때 Multus CNI(Container Network Interface) 로그 파일인 **multus.log** 가 노드의 파일 시스템에 저장되었습니다. 이로 인해 도구가 노드에서 불필요한 디버그 Pod를 생성했습니다. 이번 릴리스에서는 Multus CNI에서 더 이상 **multus.log** 파일을 생성하지 않고 CNI 플러그인 패턴을 사용하여 **openshift-multus** 네임스페이스에서 Multus DaemonSet Pod의 로그를 검사합니다. (OCPBUGS-33959)

- 이전에는 **OVNKubernetesNorthdInactive** 에 대한 경고가 실행되어야 하는 상황에서 실행되지 않았습니다. 이번 릴리스에서는 **OVNKubernetesNorthdInactive** 에 대한 경고가 예상대로 실행되도록 문제가 해결되었습니다. (OCPBUGS-33758)

- 이전 버전에서는 기본 경로가 사용자 지정된 모든 Pod의 경우 Kubernetes-OVN masquerade 주소에 대한 누락된 경로로 인해 백엔드 역할을 하는 서비스를 통해 각 Pod가 자체적으로 연결할 수 없었습니다. 이번 릴리스에서는 Kubernetes-OVN masquerade 주소에 대한 누락된 경로가 Pod에 추가되어 문제가 더 이상 발생하지 않습니다. (OCPBUGS-36865)

- 이전에는 **iptables-alerter** Pod에서 **crictl** 명령줄 인터페이스의 오류를 처리하지 않아 Pod가 **호스트 네트워크** Pod의 이벤트를 잘못 기록하거나 Pod를 다시 시작할 수 있었습니다. 이번 릴리스에서는 이러한 문제가 더 이상 유지되지 않도록 오류가 올바르게 처리됩니다. (OCPBUGS-37713)

- 이전 버전에서는 클러스터가 컴퓨팅 노드에서 컨트롤 플레인에 도달하기 위해 프록시를 사용하여 호스팅 클러스터를 생성한 경우 클러스터에서 컴퓨팅 노드를 사용할 수 없었습니다. 이번 릴리스에서는 노드가 프록시를 사용하여 컨트롤 플레인과 성공적으로 통신할 수 있도록 노드에 대한 프록시 설정이 업데이트됩니다. (OCPBUGS-37786)

- 이전 버전에서는 로드 밸런서가 구성된 온프레미스 플랫폼에 클러스터를 설치하지 못하면 **LoadBalancer** 서비스의 **LoadBalancerReady** 조건이 **SyncLoadBalancerFailed** 상태를 수신했습니다. 상태는 다음 메시지를 생성했습니다.

  > The kube-controller-manager logs might contain more details.

  로그는 프로젝트의 **cloud-controller-manager** 네임스페이스에 저장되므로 이 메시지가 잘못되었습니다. 이번 릴리스에서는 **SyncLoadBalancerFailed** 상태가 이제 올바른 메시지를 전달합니다.

  > The cloud-controller-manager logs may contain more details.

  (OCPBUGS-31664)

- 이전에는 클러스터 노드의 IP 주소를 선택하는 내부 구성 요소의 로그 수준을 제어할 수 없었습니다. 이번 릴리스에서는 필요에 따라 로그 수준을 늘리거나 줄일 수 있도록 디버그 로그 수준을 활성화할 수 있습니다. 로그 수준을 조정하려면 다음과 유사한 구성으로 구성 맵 매니페스트 파일을 생성해야 합니다.

  ```
  apiVersion: v1
  data:
    enable-nodeip-debug: "true"
  ```

```
kind: ConfigMap
metadata:
  name: logging
  namespace: openshift-vsphere-infra
# ...
```

(OCPBUGS-32348)

- 이전에는 Operator에서 기존 경로에서 **spec.host** 또는 **spec.subdomain** 필드를 업데이트할 수 있는 권한이 없기 때문에 Ingress Operator에서 카나리아 경로를 성공적으로 업데이트할 수 없었습니다. 이번 릴리스에서는 Operator 서비스 계정의 클러스터 역할에 필요한 권한이 추가되고 Ingress Operator는 카나리아 경로를 업데이트할 수 있습니다. (OCPBUGS-36465)

- 이전에는 지원되는 온프레미스 플랫폼에서 Keepalived와 같은 일부 네트워킹 컨테이너를 실행하려면 관리자 권한이 필요했습니다. 이번 릴리스에서는 이러한 컨테이너에 더 이상 지원되는 온프레미스 플랫폼에서 관리자 권한이 필요하지 않습니다. (OCPBUGS-36175)

- 이전 버전에서는 **NodeNetworkConfigurationPolicy** (NNCP) 사용자 정의 리소스(CR)가 기본 STP(패치 트리 프로토콜) 구현을 사용하도록 설정된 경우 CR 구성 파일에 **stp.enabled: true** 가 표시되지만 OpenShift Container Platform 웹 콘솔에서 STP 확인란을 지웁니다. 이번 릴리스에서는 NNCP CR YAML 파일에서 **stp.enabled: false** 를 정의한 후 웹 콘솔에서 STEP 확인란만 지웁니다. (OCPBUGS-36238)

- 이전에는 **CanaryRepetitiveFailures** 조건의 타이밍 업데이트 문제로 인해 Ingress 컨트롤러 상태가 **Degraded=False** 로 잘못 표시되었습니다. 이번 릴리스에서는 **CanaryRepetitiveFailures** 조건이 존재하는 적절한 기간 동안 Ingress 컨트롤러 상태가 **Degraded=True** 로 올바르게 표시됩니다. (OCPBUGS-39220)

1.6.16. 노드

- 이전에는 Container Runtime Config 컨트롤러에서 **ClusterImagePolicy** CR의 범위를 **/etc/containers/registries.d/sigstore-registries.yaml** 파일에 추가하기 전에 미러 구성이 사용 중인지 감지하지 못했습니다. 결과적으로 **Notigstore attachments** 메시지와 함께 이미지 확인에 실패했습니다. 이번 수정을 통해 미러 레지스트리에서 이미지를 예상대로 가져옵니다. (OCPBUGS-36344)

- 이전에는 **spec.securityContext.runAsGroup** 속성이 Pod 사양에 설정된 경우 컨테이너 내의 **/etc/group** 디렉터리에 그룹 ID가 추가되지 않았습니다. 이번 릴리스에서는 이 문제가 해결되었습니다. (OCPBUGS-39478)

- 이전에는 RHEL 9.4 커널에서 **5.14.0-427.26.1.el9_4** 이전의 심각한 회귀 문제로 인해 **mglru** 기능이 메모리 관리를 비활성화했습니다. 이번 릴리스에서는 OpenShift Container Platform 4.17에서 **mglru** 기능이 활성화되도록 회귀 문제가 해결되었습니다. (OCPBUGS-35436)

1.6.17. Node Tuning Operator (NTO)

- 이전 버전에서는 내부 버그로 인해 머신에 256개 이상의 CPU가 있는 경우 Node Tuning Operator에서 인터럽트 및 네트워크 처리 CPU의 CPU 마스크를 잘못 계산했습니다. 이로 인해 해당 시스템에서 적절한 CPU 분리가 발생하여 **systemd** 장치 오류가 발생했습니다. 이번 릴리스에서는 Node Tuning Operator에서 마스크를 올바르게 계산합니다. (OCPBUGS-39164)

- 이전에는 OVS(Open vSwitch) 고정 프로시저에서 기본 스레드의 CPU 선호도를 설정했지만 다른 CPU 스레드에서 이미 생성된 경우 이 선호도를 선택하지 않았습니다. 그 결과 일부 OVS 스레드가 올바른 CPU 세트에서 실행되지 않아 QoS(Quality of Service) 클래스가 **Guaranteed** 인 Pod

성능이 방해될 수 있었습니다. 이번 업데이트를 통해 OVS 고정 프로시저는 모든 OVS 스레드의 선호도를 업데이트하여 모든 OVS 스레드가 올바른 CPU 세트에서 실행되도록 합니다. (OCPBUGS-35347)

1.6.18. 가시성

- 이전 버전에서는 OpenShift Container Platform 웹 콘솔의 **관리자** 화면에서 로그인하고 **Observe → Alerting** 기능을 사용할 때 **S는 경고 메트릭 그래프에 표시되는 함수가 아닙니다**. 이 문제는 함수 검증 검사가 누락되어 발생했습니다. 이번 릴리스에서는 기능 검증 검사가 추가되어 경고 지표 차트에 수집된 지표가 표시됩니다. (OCPBUGS-37291)

1.6.19. OpenShift CLI(oc)

- 이전 버전에서는 oc-mirror 플러그인 v2를 **--delete** 플래그와 함께 사용하여 미러 레지스트리에서 Operator 카탈로그를 제거할 때 다음 오류와 함께 프로세스가 실패했습니다.

  > 2024/08/02 12:18:03 [ERROR]: [OperatorImageCollector] pinging container registry localhost:55000: Get "https://localhost:55000/v2/": http: server gave HTTP response to HTTPS client.

  이는 oc-mirror 플러그인 v2가 HTTP 대신 HTTPS를 사용하여 로컬 캐시를 쿼리했기 때문에 발생했습니다. 이번 업데이트를 통해 이제 쿼리 전에 HTTP 클라이언트가 올바르게 구성되어 문제를 해결합니다. (OCPBUGS-41503)

- 이전 버전에서는 mirror-to-disk 모드에서 oc-mirror 플러그인 v2를 사용할 때 이미지 다이제스트를 기반으로 카탈로그 이미지 및 콘텐츠가 **working-dir 의 하위 폴더에** 저장되었습니다. 완전히 연결이 끊긴 환경의 disk-to-mirror 프로세스 중에 플러그인은 사용할 수 없는 소스 레지스트리를 통해 카탈로그 이미지 태그를 확인하려고 시도하여 이러한 오류가 발생합니다.

  > [ERROR] : [OperatorImageCollector] pinging container registry registry.redhat.io: Get "http://registry.redhat.io/v2/": dial tcp 23.217.255.152:80: i/o timeout

  이번 업데이트를 통해 플러그인은 disk-to-mirror 프로세스 중에 로컬 캐시를 확인하여 다이제스트를 확인하여 레지스트리를 쿼리할 필요가 없습니다. (OCPBUGS-36214)

- 이전 버전에서는 연결이 끊긴 환경의 mirror-to-disk 모드에서 oc-mirror 플러그인 v2를 사용할 때 플러그인이 graph **.openshift.com에 액세스하여 graph. tar.gz** 를 다운로드할 수 없어 미러링 오류가 발생했습니다. 이번 업데이트를 통해 플러그인은 **UPDATE_URL_OVERRIDE** 환경 변수가 설정된 연결이 끊긴 환경에서 그래프 이미지의 로컬 캐시를 검색합니다. 그래프 이미지가 없으면 플러그인이 실패하지 않고 건너뜁니다. (OCPBUGS-38469)

- 이전에는 oc-mirror 플러그인 v2가 완전히 연결이 끊긴 환경의 disk-to-mirror에서 Operator 카탈로그를 미러링하지 못했습니다. 이 문제는 **ImageSetConfiguration** 파일에서 **targetCatalog** 를 지정한 카탈로그에도 영향을 미쳤습니다. 이번 업데이트를 통해 플러그인은 완전히 연결이 끊긴 환경에서 카탈로그를 성공적으로 미러링할 수 있으며 **targetCatalog** 기능이 예상대로 작동합니다. (OCPBUGS-34521)

- 이전 버전에서는 oc-mirror 플러그인 v2를 사용하여 **oc-mirror** 명령에 대한 **-v2** vs **--v2** 플래그에 대한 검증이 없었습니다. 결과적으로 oc-mirror 플러그인 v2로 전환되는 **--v2** 대신 로그 수준을 2로 설정하는 **-v2**.v2를 잘못 사용한 사용자는 불명확한 오류 메시지를 수신했습니다. 이번 업데이트를 통해 플래그 유효성 검사가 제공됩니다. **ImageSetConfig** 에서 **v2alpha1** API를 사용하는 동안 **-v2** 플래그가 사용되고 **--v2** 가 지정되지 않은 경우 오류 메시지가 표시됩니다. 이제 사용자에게 명확한 지침을 제공하는 다음 메시지가 활성화됩니다.

> [ERROR]: Detected a v2 ImageSetConfiguration, please use --v2 instead of -v2.

(OCPBUGS-33121)

- 이전 버전에서는 oc-mirror 플러그인 v2가 시간 초과, 만료된 인증 토큰, HTTP 500 오류 등과 같은 레지스트리에 오류가 발생하면 자동으로 재시도를 수행하지 않았습니다. 이번 업데이트를 통해 이러한 오류에 대한 재시도가 구현되고 사용자는 다음 플래그를 사용하여 재시도 동작을 구성할 수 있습니다.
  - **--retry-times**: 재시도 시도 횟수를 지정합니다. 기본값은 2입니다.
  - **--retry-delay**: 재시도 사이에 지연을 설정합니다. 기본값은 1초입니다.
  - **--image-timeout**: 이미지 미러링을 위한 시간 초과 기간을 정의합니다. 기본값은 10분입니다.
  - **--max-parallel-downloads**: 단일 복사 작업 중에 동시에 가져올 최대 계층 수를 제어합니다. 기본값은 6입니다.
    (OCPBUGS-34021)

- 이전 버전에서는 **--rebuild-catalogs** 플래그와 함께 oc-mirror 플러그인 v2를 사용할 때 카탈로그 캐시가 로컬에서 다시 생성되어 **opm** 바이너리 및 플랫폼과의 호환성 문제 또는 클러스터의 캐시 무결성 문제로 인해 오류가 발생했습니다. 이번 업데이트를 통해 기본적으로 **--rebuild-catalogs** 플래그는 true로 설정되므로 내부 캐시를 다시 생성하지 않고 카탈로그를 다시 빌드할 수 있습니다. 또한 pod를 시작하는 동안 캐시를 생성하도록 image 명령이 수정되어 Pod 초기화가 지연될 수 있습니다. (OCPBUGS-37667)

- 이전에는 oc-mirror 플러그인 v2에서 시스템 프록시 설정을 사용하여 프록시 뒤에서 실행할 때 릴리스의 서명을 복구하기 위해 시스템 프록시 구성을 사용하지 않았습니다. 이번 릴리스에서는 서명 복구 프로세스 중에 시스템 프록시 설정이 적용됩니다. (OCPBUGS-37055)

- 이전 버전에서는 oc-mirror 플러그인 v2에서 의미 체계 버전ing과 호환되지 않는 번들 버전을 사용하여 Operator가 있는 경우 미러링 프로세스를 중지하여 IDMS, ITMS, **CatalogSource** 오브젝트와 같은 클러스터 리소스도 생성할 수 없었습니다. 이번 수정으로 플러그인은 프로세스를 중지하는 대신 이러한 문제가 있는 이미지를 건너뜁니다. 이미지에서 잘못된 의미 체계 버전 관리를 사용하는 경우 관련 이미지 세부 정보가 포함된 콘솔에 경고 메시지가 표시됩니다. (OCPBUGS-33081)

- 이전에는 네트워크 문제 또는 잘못된 Operator 카탈로그로 인해 미러링에 실패한 경우 oc-mirror 플러그인 v2에서 **ImageDigestMirrorSet** (IDMS) 또는 **ImageTagMirrorSet** (ITMS) 파일을 생성하지 않았습니다. 이번 업데이트를 통해 Operator 또는 추가 이미지가 실패할 때 **oc-mirror** 가 다른 이미지를 계속 미러링하고 릴리스 이미지가 실패하는 경우에만 중지됩니다. 성공적으로 미러링된 이미지를 기반으로 클러스터 리소스가 생성되고 검토를 위해 모든 오류가 로그 파일에 수집됩니다. (OCPBUGS-34020)

- 이전에는 OpenShift Container Platform 릴리스 이미지가 Red Hat Quay와 같은 특정 레지스트리에 표시되지 않았습니다. 이로 인해 사용자가 릴리스 이미지가 누락되어 OpenShift Container Platform을 설치할 수 없었습니다. 이번 업데이트를 통해 Red Hat Quay와 같은 레지스트리에 표시되도록 릴리스 이미지에 항상 태그가 지정되어 올바른 설치를 활성화합니다. (OCPBUGS-36410)

- 이전에는 **oc adm must-gather** 명령이 대규모 클러스터에서 CPU 관련 성능 데이터를 수집하는 데 오랜 시간이 걸렸습니다. 이번 릴리스에서는 데이터가 순차적 대신 병렬로 수집되어 데이터 수집 시간이 단축됩니다. (OCPBUGS-34360)

- 이전에는 **oc set env** 명령에서 **Route** 및 **DeploymentConfig** 오브젝트의 API 버전을 잘못 변경했습니다(예: **apps.openshift.io/v1** 은 **v1**). 이로 인해 명령이 종료되었으며 **종류 오류가 일치하**

는 것을 인식하지 못했습니다. 이번 릴리스에서는 **os set env** 명령이 **Route** 및 **DeploymentConfig** 오브젝트에 올바른 API 버전을 유지하도록 오류가 수정되었습니다. (OCPBUGS-32108)

- 이전 버전에서는 **must-gather** 작업이 어떤 이유로든 실패하고 사용자가 남은 네임스페이스를 수동으로 삭제한 경우 **must-gather** 명령으로 생성된 클러스터 역할 바인딩이 클러스터에 남아 있었습니다. 이번 릴리스에서는 임시 **must-gather** 네임스페이스가 삭제되면 연결된 클러스터 역할 바인딩이 자동으로 삭제됩니다. (OCPBUGS-31848)

- 이전 버전에서는 oc-mirror 플러그인 v2와 함께 **--v2** 플래그를 사용할 때 미러링된 이미지가 없고 일부는 건너뛰고 빈 **imds.yaml** 및 **itms.yaml** 파일이 생성되었습니다. 이번 릴리스에서는 하나 이상의 이미지가 성공적으로 미러링된 경우에만 사용자 정의 리소스 생성이 트리거되어 빈 파일이 생성되지 않습니다. (OCPBUGS-33775)

1.6.20. OLM(Operator Lifecycle Manager)

- 이전 버전에서는 많은 CR(사용자 정의 리소스)이 있는 클러스터에 API 서버에서 시간 초과가 발생하고 유일한 해결 방법이 제거되고 중단된 Operator를 다시 설치하는 작업이 진행되었습니다. 이는 OLM이 동적 클라이언트 목록러를 사용하여 잠재적인 업데이트를 평가했기 때문에 발생했습니다. 이번 수정으로 OLM은 CRD(사용자 정의 리소스 정의)에 페이징 선택기를 사용하여 시간 초과 및 중단된 업데이트를 방지합니다. (OCPBUGS-41549)

- 이전에는 **registryPoll** 매개변수가 설정되지 않은 경우 카탈로그 소스 Pod가 클러스터 노드 장애에서 복구할 수 없었습니다. 이번 수정으로 OLM은 종료된 Pod를 확인하기 위해 논리를 업데이트합니다. 결과적으로 카탈로그 소스 Pod는 이제 예상대로 노드 오류를 복구합니다. (OCPBUGS-39574)

- 이전 버전에서는 OpenShift Container Platform 업데이트 후 이전에 삭제된 Operator를 설치하려고 하면 설치에 실패할 수 있었습니다. 이는 OLM에서 이전에 생성된 번들 압축 풀기 작업을 찾을 수 없기 때문에 발생했습니다. 이번 수정으로 OLM은 이전에 설치한 Operator를 올바르게 설치합니다. (OCPBUGS-32439)

- 이전에는 새 버전의 CRD(사용자 정의 리소스 정의)에서 새 변환 전략을 지정할 때 이 변환 전략이 리소스를 성공적으로 변환해야 했습니다. 그러나 OLM은 실제로 업데이트 작업을 수행하지 않고 CRD 검증을 위해 새 변환 전략을 실행할 수 없습니다. 이번 릴리스에서는 CRD 검증이 기존 변환 전략으로 실패할 때 업데이트 프로세스 중에 OLM에서 경고 메시지를 생성하고 새 버전의 CRD에 새 변환 전략이 지정됩니다. (OCPBUGS-31522)

- 이전 버전에서는 **CatalogSource** 오브젝트의 **spec.grpcPodConfig.securityContextConfig** 필드가 **PodSecurityAdmission** (PSA) 수준 값이 **restricted** 인 네임스페이스 내에 설정되지 않은 경우 카탈로그 Pod에서 PSA 검증을 전달하지 않았습니다. 이번 릴리스에서는 OLM Catalog Operator에서 PSA 검증을 전달하는 데 필요한 **securityContexts** 로 카탈로그 Pod를 구성합니다. (OCPBUGS-29729)

- 이전 버전에서는 **catalogd-controller-manager** Pod가 스케줄링 대기열에 있어도 노드에 배포되지 않았으며 OLM Operator를 설치하지 못했습니다. 이번 수정을 통해 관련 리소스에 대한 CPU 요청이 감소되고 더 이상 문제가 발생하지 않습니다. (OCPBUGS-29705)

- 이전에는 Catalog Operator에서 캐시에 저장된 삭제된 카탈로그 소스에 연결하려고 시도한 경우가 있었습니다. 이번 수정으로 Catalog Operator는 클라이언트를 쿼리하여 클러스터의 카탈로그 소스를 나열합니다. (OCPBUGS-8659)

1.6.21. RHCOS(Red Hat Enterprise Linux CoreOS)

- 이전에는 512 에뮬레이션 디스크를 사용하는 시스템의 LUKS 암호화로 인해 **sfdisk** 정렬 문제로

인해 **ignition-ostree-growfs** 단계에서 프로비저닝이 실패했습니다. 이번 릴리스에서는 **ignition-ostree-growfs** 스크립트에서 이 상황을 감지하고 정렬을 자동으로 수정합니다. 결과적으로 프로비저닝 중에 시스템이 더 이상 실패하지 않습니다. (OCPBUGS-35410)

- 이전에는 **growpart** 유틸리티의 버그로 인해 LUKS 장치가 잠겼습니다. 이로 인해 시스템이 긴급 모드로 부팅되었습니다. 이번 릴리스에서는 **growpart** 유틸리티 호출이 제거되고 문제가 없이 시스템이 성공적으로 부팅됩니다. (OCPBUGS-33124)

- 이전 버전에서는 새 배포가 호스트의 OSTree 수준에서 수행되면 다른 stateroot의 현재 배포와 동일한 방식으로 OSTree가 식별되었습니다. 이 동작으로 인해 OSTree에서 두 stateroot를 배포의 다른 요인으로 인식하지 못했기 때문에 **set-default** 명령이 호출될 때 부트로더가 업데이트되지 않았습니다. 이번 릴리스에서는 stateroot를 고려하도록 OSTree의 논리가 수정되었습니다. 결과적으로 OSTree는 stateroots가 다른 새 배포로 기본 배포를 올바르게 설정합니다. (OCPBUGS-30276)

1.6.22. 스토리지

- 이전에는 호스팅된 컨트롤 플레인의 CSI(Secrets Store Container Storage Interface) 드라이버에서 호스팅된 컨트롤 플레인 명령줄 인터페이스인 **hcp** 를 사용하여 Amazon Web Services에서 OpenID Connect(OIDC) 인프라를 생성할 때 문제가 발생하여 시크릿을 마운트하지 못했습니다. 이번 릴리스에서는 드라이버가 볼륨을 마운트할 수 있도록 문제가 해결되었습니다. (OCPBUGS-18711)

1.7. 기술 프리뷰 기능 상태

이 릴리스의 일부 기능은 현재 기술 프리뷰 단계에 있습니다. 이러한 실험적 기능은 프로덕션용이 아닙니다. 다음 기능은 Red Hat 고객 포털에서 다음 지원 범위를 참조하십시오.

기술 프리뷰 기능 지원 범위

다음 표에서 기능은 다음 상태로 표시됩니다.

- *사용할 수 없음*
- *기술 프리뷰*
- *정식 출시일 (GA)*
- *더 이상 사용되지 않음*
- *제거됨*

1.7.1. 네트워킹 기술 프리뷰 기능

표 1.17. 네트워킹 기술 프리뷰 추적기

기능	4.15	4.16	4.17
Ingress 노드 방화벽 Operator	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
eBPF 관리자 Operator	해당 없음	해당 없음	기술 프리뷰

기능	4.15	4.16	4.17
특정 IP 주소 풀을 사용하여 노드 하위 집합에서 MetalLB 서비스를 사용하여 L2 모드를 사용하여 알립니다.	기술 프리뷰	기술 프리뷰	기술 프리뷰
SR-IOV 네트워크에 대한 다중 네트워크 정책	정식 출시일(GA)	정식 출시일(GA)	정식 출시일(GA)
인터페이스별 안전한 sysctl 목록 업데이트	기술 프리뷰	기술 프리뷰	기술 프리뷰
송신 서비스 사용자 정의 리소스	기술 프리뷰	기술 프리뷰	기술 프리뷰
BGPPeer 사용자 정의 리소스의 VRF 사양	기술 프리뷰	기술 프리뷰	기술 프리뷰
NodeNetworkConfigurationPolicy 사용자 정의 리소스의 VRF 사양	기술 프리뷰	기술 프리뷰	기술 프리뷰
관리 네트워크 정책 (**관리자NetworkPolicy**)	기술 프리뷰	정식 출시일(GA)	정식 출시일(GA)
IPsec 외부 트래픽(north-south)	정식 출시일(GA)	정식 출시일(GA)	정식 출시일(GA)
SR-IOV VF의 호스트 네트워크 설정	기술 프리뷰	기술 프리뷰	정식 출시일(GA)
MetalLB 및 FRR-K8s 통합	사용할 수 없음	기술 프리뷰	정식 출시일(GA)
고가용성 시스템 클럭으로 듀얼 NIC Intel E810 PTP 경계 클럭	사용할 수 없음	정식 출시일(GA)	정식 출시일(GA)
Intel E810 Westport Channel NIC as PTP grandmaster clock	기술 프리뷰	정식 출시일(GA)	정식 출시일(GA)
PTP 할 마스터 클록으로 듀얼 NIC Intel E810 Westport 채널	기술 프리뷰	정식 출시일(GA)	정식 출시일(GA)
PTP 할 마스터 클록에 대한 자동 윤초 처리	사용할 수 없음	사용할 수 없음	정식 출시일(GA)
PTP 이벤트 REST API v2	사용할 수 없음	사용할 수 없음	정식 출시일(GA)
OVN-Kubernetes에 필요한 **br-ex** 브리지 구성 NMState	사용할 수 없음	정식 출시일(GA)	정식 출시일(GA)
Whereabouts를 사용하여 다중 테넌트 네트워크에 대한 IP 구성 중복	사용할 수 없음	정식 출시일(GA)	정식 출시일(GA)

기능	4.15	4.16	4.17
사용자 정의 네트워크 분할	사용할 수 없음	사용할 수 없음	기술 프리뷰

1.7.2. 스토리지 기술 프리뷰 기능

표 1.18. 스토리지 기술 프리뷰 추적기

기능	4.15	4.16	4.17
AWS EFS 스토리지 CSI 사용 메트릭	사용할 수 없음	사용할 수 없음	정식 출시일(GA)
Local Storage Operator를 통한 자동 장치 검색 및 프로비저닝	기술 프리뷰	기술 프리뷰	기술 프리뷰
Azure File CSI 스냅샷 지원	사용할 수 없음	사용할 수 없음	기술 프리뷰
IBM Power® Virtual Server Block CSI Driver Operator	정식 출시일(GA)	정식 출시일(GA)	정식 출시일(GA)
Read Write once Pod 액세스 모드	기술 프리뷰	정식 출시일(GA)	정식 출시일(GA)
secrets Store CSI Driver Operator	기술 프리뷰	기술 프리뷰	기술 프리뷰
CIFS/SMB CSI Driver Operator	사용할 수 없음	기술 프리뷰	기술 프리뷰
VMware vSphere 다중 vCenter 지원	사용할 수 없음	사용할 수 없음	기술 프리뷰
vSphere에서 스토리지 비활성화/활성화	사용할 수 없음	사용할 수 없음	기술 프리뷰
RWX/RWO SELinux 마운트	사용할 수 없음	사용할 수 없음	개발자 프리뷰
데이터 저장소 간에 CNS 볼륨 마이그레이션	사용할 수 없음	사용할 수 없음	개발자 프리뷰

1.7.3. 설치 기술 프리뷰 기능

표 1.19. 설치 기술 프리뷰 추적기

기능	4.15	4.16	4.17
VM을 사용하여 Oracle® Cloud Infrastructure(OCI)에 OpenShift Container Platform 설치	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
베어 메탈의 OCI(Oracle® Cloud Infrastructure)에 OpenShift Container Platform 설치	개발자 프리뷰	개발자 프리뷰	개발자 프리뷰
kvc로 노드에 커널 모듈 추가	기술 프리뷰	기술 프리뷰	기술 프리뷰
SR-IOV 장치의 NIC 파티셔닝 활성화	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
Google Cloud의 사용자 정의 레이블 및 태그	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
설치 관리자 프로비저닝 인프라를 사용하여 Alibaba Cloud에 클러스터 설치	기술 프리뷰	사용할 수 없음	사용할 수 없음
지원 설치 관리자를 사용하여 Alibaba Cloud에 클러스터 설치	사용할 수 없음	기술 프리뷰	기술 프리뷰
RHEL의 BuildConfig에 공유 인타이틀먼트 마운트	기술 프리뷰	기술 프리뷰	기술 프리뷰
선택 가능한 Cluster Inventory	기술 프리뷰	기술 프리뷰	기술 프리뷰
VMware vSphere(IPI만 해당)가 있는 고정 IP 주소	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
RHCOS에서 iSCSI 장치 지원	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
클러스터 API 구현을 사용하여 Google Cloud에 클러스터 설치	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
RHCOS에서 Intel® VROC 지원 RAID 장치 지원	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)

1.7.4. 노드 기술 프리뷰 기능

표 1.20. 노드 기술 프리뷰 추적기

기능	4.15	4.16	4.17
MaxUnavailableStatefulSet featureset	기술 프리뷰	기술 프리뷰	기술 프리뷰

기능	4.15	4.16	4.17
Linux 사용자 네임스페이스 지원	사용할 수 없음	사용할 수 없음	기술 프리뷰

1.7.5. 다중 아카이브 기술 프리뷰 기능

표 1.21. Multi-Architecture Technology Preview 추적기

기능	4.15	4.16	4.17
설치 관리자 프로비저닝 인프라를 사용하는 IBM Power® Virtual Server	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
arm64 아키텍처의 **kdump**	기술 프리뷰	기술 프리뷰	기술 프리뷰
s390x 아키텍처의 **kdump**	기술 프리뷰	기술 프리뷰	기술 프리뷰
ppc64le 아키텍처의 **kdump**	기술 프리뷰	기술 프리뷰	기술 프리뷰
Multiarch Tuning Operator	사용할 수 없음	정식 출시일 (GA)	정식 출시일 (GA)

1.7.6. 확장성 및 성능 기술 프리뷰 기능

표 1.22. 확장성 및 성능 기술 프리뷰 추적기

기능	4.15	4.16	4.17
factory-precaching-cli 툴	기술 프리뷰	기술 프리뷰	기술 프리뷰
하이퍼 스레딩 인식 CPU 관리자 정책	기술 프리뷰	기술 프리뷰	기술 프리뷰
PTP 및 베어 메탈 이벤트의 AMQP를 HTTP 전송	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
마운트 네임스페이스 캡슐화	기술 프리뷰	기술 프리뷰	기술 프리뷰
Node Observability Operator	기술 프리뷰	기술 프리뷰	기술 프리뷰
etcd 대기 오차 튜닝	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
etcd 데이터베이스 크기 증가	사용할 수 없음	기술 프리뷰	기술 프리뷰

기능	4.15	4.16	4.17
RHACM **PolicyGenerator** 리소스를 사용하여 GitOps ZTP 클러스터 정책 관리	사용할 수 없음	기술 프리뷰	기술 프리뷰
고정된 이미지 세트	사용할 수 없음	기술 프리뷰	기술 프리뷰

1.7.7. Operator 라이프사이클 및 개발 기술 프리뷰 기능

표 1.23. Operator 라이프사이클 및 개발 기술 프리뷰 추적기

기능	4.15	4.16	4.17
Operator Lifecycle Manager (OLM) v1	기술 프리뷰	기술 프리뷰	기술 프리뷰
RukPak	기술 프리뷰	기술 프리뷰	제거됨
Platform Operator	기술 프리뷰	제거됨	제거됨
하이브리드 Helm 기반 Operator 프로젝트의 스캐폴딩 툴	기술 프리뷰	더 이상 사용되지 않음	더 이상 사용되지 않음
Java 기반 Operator 프로젝트를 위한 Scaffolding 툴	기술 프리뷰	더 이상 사용되지 않음	더 이상 사용되지 않음

1.7.8. OpenShift CLI (oc) 기술 프리뷰 기능

표 1.24. OpenShift CLI(oc) 기술 프리뷰 추적기

기능	4.15	4.16	4.17
oc-mirror 플러그인 v2	사용할 수 없음	기술 프리뷰	기술 프리뷰
Enclave 지원	사용할 수 없음	기술 프리뷰	기술 프리뷰
기능 삭제	사용할 수 없음	기술 프리뷰	기술 프리뷰

1.7.9. 기술 프리뷰 기능 모니터링

표 1.25. 기술 프리뷰 추적기 모니터링

기능	4.15	4.16	4.17
메트릭 컬렉션 프로필	기술 프리뷰	기술 프리뷰	기술 프리뷰
지표 서버	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)

1.7.10. 기술 프리뷰 기능 모니터링

표 1.26. 기술 프리뷰 추적기 모니터링

기능	4.15	4.16	4.17
OpenShift Container Platform 웹 콘솔의 Red Hat OpenShift Lightspeed	사용할 수 없음	개발자 프리뷰	개발자 프리뷰

1.7.11. RHOSP(Red Hat OpenStack Platform) 기술 프리뷰 기능

표 1.27. RHOSP 기술 프리뷰 추적기

기능	4.15	4.16	4.17
설치 관리자 프로비저닝 인프라를 사용한 듀얼 스택 네트워킹	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
사용자 프로비저닝 인프라를 사용한 듀얼 스택 네트워킹	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
Cluster CAPI Operator에 RHOSP 통합	기술 프리뷰	기술 프리뷰	기술 프리뷰
로컬 디스크 의 **rootVolume** 및 **etcd** 를 사용한 컨트롤 플레인	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)

참고

OpenShift Container Platform 4.17에서 호스팅되는 컨트롤 플레인 기능의 상태를 확인하려면 호스팅 컨트롤 플레인 릴리스 노트의 일반 사용 가능 및 기술 프리뷰 기능을 참조하십시오.

1.7.12. 호스팅된 컨트롤 플레인 기술 프리뷰 기능

표 1.28. 호스팅된 컨트롤 플레인 기술 프리뷰 추적기

기능	4.15	4.16
AWS(Amazon Web Services)의 OpenShift Container Platform용 호스팅 컨트롤 플레인	기술 프리뷰	정식 출시일 (GA)

기능	4.15	4.16
베어 메탈의 OpenShift Container Platform의 호스트된 컨트롤 플레인	정식 출시일 (GA)	정식 출시일 (GA)
OpenShift Virtualization에서 OpenShift Container Platform의 호스트된 컨트롤 플레인	정식 출시일 (GA)	정식 출시일 (GA)
베어 메탈이 아닌 에이전트 시스템을 사용하는 OpenShift Container Platform용 호스팅 컨트롤 플레인	기술 프리뷰	기술 프리뷰
Amazon Web Services에서 ARM64 OpenShift Container Platform 클러스터용 호스팅 컨트롤 플레인	기술 프리뷰	기술 프리뷰
IBM Power의 OpenShift Container Platform용 호스팅 컨트롤 플레인	기술 프리뷰	기술 프리뷰
IBM Z의 OpenShift Container Platform용 호스팅 컨트롤 플레인	기술 프리뷰	기술 프리뷰
RHOSP의 OpenShift Container Platform용 호스팅 컨트롤 플레인	사용할 수 없음	사용할 수 없음

1.7.13. 머신 관리 기술 프리뷰 기능

표 1.29. 머신 관리 기술 프리뷰 추적기

기능	4.15	4.16	4.17
Amazon Web Services용 클러스터 API로 머신 관리	기술 프리뷰	기술 프리뷰	기술 프리뷰
Google Cloud용 클러스터 API로 머신 관리	기술 프리뷰	기술 프리뷰	기술 프리뷰
IBM Power® Virtual Server용 클러스터 API로 머신 관리	기술 프리뷰	기술 프리뷰	기술 프리뷰
RHOSP용 클러스터 API로 머신 관리	기술 프리뷰	기술 프리뷰	기술 프리뷰
VMware vSphere용 클러스터 API로 머신 관리	사용할 수 없음	기술 프리뷰	기술 프리뷰
컨트롤 플레인 머신 세트의 vSphere 실패 도메인 정의	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
vGPU Cloud의 클라우드 컨트롤러 관리자	기술 프리뷰	제거됨	제거됨
Google Cloud용 클라우드 컨트롤러 관리자	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
IBM Power® Virtual Server용 클라우드 컨트롤러 관리자	기술 프리뷰	기술 프리뷰	기술 프리뷰

1.7.14. 인증 및 권한 부여 기술 프리뷰 기능

표 1.30. 인증 및 권한 부여 기술 프리뷰 추적기

기능	4.15	4.16	4.17
Pod 보안 승인 제한	기술 프리뷰	기술 프리뷰	기술 프리뷰

1.7.15. Machine Config Operator 기술 프리뷰 기능

표 1.31. Machine Config Operator 기술 프리뷰 추적기

기능	4.15	4.16	4.17
MCO 상태 보고 개선	기술 프리뷰	기술 프리뷰	기술 프리뷰
클러스터 내 RHCOS 이미지 계층화	사용할 수 없음	기술 프리뷰	기술 프리뷰
노드 중단 정책	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
GCP 클러스터의 부팅 이미지 업데이트	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
AWS 클러스터의 부팅 이미지 업데이트	사용할 수 없음	사용할 수 없음	기술 프리뷰

1.7.16. 엣지 컴퓨팅 기술 프리뷰 기능

표 1.32. 엣지 컴퓨팅 기술 프리뷰 추적기

기능	4.15	4.16	4.17
GitOps ZTP 프로비저닝 가속화	사용할 수 없음	기술 프리뷰	기술 프리뷰
TPM 및 PCR 보호로 디스크 암호화 활성화	사용할 수 없음	사용할 수 없음	기술 프리뷰

1.8. 확인된 문제

- 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)
- 알려진 문제는 **UserDefinedNetwork** 리소스에서 생성한 **NetworkAttachmentDefinition** (NAD) 리소스를 삭제할 때 존재합니다. CryostatD를 삭제하기 전에 pod가 CryostatD를 참조하는지 확인해야 합니다. pod는 CryostatD 전에 삭제해야 합니다. 그러지 않으면 Pod가 예기치 않은 상태

가 될 수 있습니다. (OCPBUGS-39185)

- RHCOS(Red Hat Enterprise Linux CoreOS) 이미지에 포함된 DNF 패키지 관리자는 런타임에 사용할 수 없습니다. DNF는 Red Hat 서브스크립션 아래에 있는 클러스터의 권한이 있는 노드에 액세스하기 위해 추가 패키지를 사용합니다. 이 문제를 해결하려면 **rpm-ostree** 명령을 대신 사용하십시오. (OCPBUGS-35247)

- Microsoft Azure에 클러스터를 설치할 때 **install-config.yaml** 파일이 제공되지 않으면 설치에 실패합니다. **install-config.yaml** 파일이 제공되며 **controlPlane.platform** 이 있지만 **controlPlane.platform.azure** 는 제공되지 않는 경우 설치에 실패합니다. (OCPBUGS-42296) 샘플 구성 파일의 경우 Azure의 사용자 지정 install-config.yaml 파일 샘플을 참조하거나 다음 예제와 같이 null이 아닌 매개변수를 설정합니다.

```
controlPlane:
  platform:
    azure: {}
```

- Microsoft Azure에 여러 클러스터를 설치할 때 동일한 설치 호스트에서 동시에 여러 설치를 실행하면 클러스터 중 하나만 성공적으로 설치됩니다. 동시에 설치를 실행하는 경우 동일한 설치 호스트에서 Azure에 여러 클러스터를 설치할 수 있습니다. (OCPBUGS-36202)

- Microsoft Azure에 클러스터를 설치할 때 컨트롤 플레인 시스템의 **Standard_M8-4ms** 인스턴스 유형을 지정하면 정수 형식 대신 10진수 형식으로 메모리를 지정하기 때문에 오류가 발생합니다. (OCPBUGS-42241)

- OpenShift Container Platform 4.17이 릴리스될 때 스토리지 계정 이름 변경으로 인해 이미지 레지스트리가 프라이빗으로 구성된 경우 CSI(Azure File Container Storage Interface) 드라이버가 모든 볼륨을 마운트하지 못하는 문제가 발생했습니다. CSI 드라이버가 작업자 서브넷의 연결을 허용하도록 구성되지 않은 Image Registry Operator의 스토리지 계정을 사용하려고했기 때문에 마운트 오류가 발생했습니다. 이 문제는 OpenShift Container Platform 4.17.5 에서 해결되었으며 이후 릴리스에 적용됩니다.

- Azure에 클러스터를 설치할 때 고객 관리 암호화 키가 지정된 경우 설치에 실패합니다. (OCPBUGS-42349)

- Operator 및 추가 이미지를 미러링하는 동안 오류가 발생하면 파일이 생성되지 않은 경우에도 로그 메시지 "카탈로그 소스 생성"이 계속 표시될 수 있습니다. (OCPBUGS-42503)

- 클러스터에서 IPsec을 활성화한 경우 north-south IPsec 연결을 호스팅하는 노드에서 **ipsec.service** systemd 장치를 다시 시작하거나 **ovn-ipsec-host** Pod를 다시 시작하면 IPsec 연결이 손실됩니다. (RHEL-26878)

- Run Once Duration Override Operator (RODOO)는 Hypershift Operator가 관리하는 클러스터에 설치할 수 없습니다. (OCPBUGS-17533)

- OpenShift Container Platform 클러스터에서 CNF(Cloud-native Network Functions) 대기 시간 테스트를 실행하는 경우 테스트에서 테스트의 대기 시간 임계값보다 큰 결과를 반환할 수 있습니다(예: **cyclictest** 테스트의 경우 20microseconds). 이로 인해 테스트 실패가 발생합니다. (OCPBUGS-42328)

- 각 노드 그룹은 하나의 **MachineConfigPool** 오브젝트만 일치해야 합니다. 경우에 따라 NUMA Resources Operator는 노드 그룹이 두 개 이상의 **MachineConfigPool** 오브젝트와 일치하는 구성을 허용할 수 있습니다. 이 문제로 인해 리소스 관리에서 예기치 않은 동작이 발생할 수 있습니다. (OCPBUGS-42523)

- NUMA Resources Operator를 배포하려면 OpenShift Container Platform 버전 4.17.7 또는 4.17.8을 사용하지 마십시오. (OCPBUGS-45639)
- **NetworkNodeConfigurationPolicy** 의 본딩 모드가 **br-ex** 인터페이스에 연결된 커널 본딩의 **balance-rr** 에서 **active-backup** 으로 변경되면 임의의 노드에서 변경 사항이 실패할 수 있습니다. 이 문제를 해결하려면 본딩 포트 구성을 지정하지 않고 **NetworkNodeConfigurationPolicy** 오브젝트를 생성합니다. (OCPBUGS-42031)
- 복제 중 컨트롤러 Pod가 종료되거나 볼륨 스냅샷을 생성하거나 복원하는 경우 Microsoft Azure File 복제 또는 스냅샷 PVC(영구 볼륨 클레임)가 Pending 상태로 유지됩니다. 이 문제를 해결하려면 영향을 받는 복제 또는 스냅샷 PVC를 삭제한 다음 해당 PVC를 다시 생성합니다. (OCPBUGS-35977)
- **bootstrap-kubeconfig** 파일에서 잘못된 KAS 포트를 사용하므로 AWS에 자체 관리형 개인 호스팅 클러스터를 배포하는 데 실패합니다. 결과적으로 AWS 인스턴스가 프로비저닝되지만 호스팅된 클러스터에 노드로 참여할 수 없습니다. (OCPBUGS-31840)

1.9. 비동기 에라타 업데이트

OpenShift Container Platform 4.17의 보안, 버그 수정 및 개선 사항 업데이트는 Red Hat Network를 통해 비동기 에라타로 릴리스됩니다. 모든 OpenShift Container Platform 4.17 에라타는 Red Hat Customer Portal을 통해 제공됩니다. 비동기 에라타에 대한 자세한 내용은 OpenShift Container Platform 라이프 사이클에서 참조하십시오.

Red Hat Customer Portal 사용자는 RHSM(Red Hat Subscription Management) 계정 설정에서 에라타 알림을 활성화할 수 있습니다. 에라타 알림이 활성화되면 사용자는 등록된 시스템과 관련된 새 에라타가 릴리스될 때마다 이메일을 통해 통지를 받습니다.

참고

Red Hat Customer Portal 사용자 계정에는 OpenShift Container Platform 에라타 알림 이메일을 생성하기 위해 OpenShift Container Platform에 대한 등록된 시스템 및 사용 권한이 있어야 합니다.

이 섹션은 향후 OpenShift Container Platform 4.17의 비동기 에라타 릴리스의 개선 사항 및 버그 수정에 대한 정보 제공을 위해 지속적으로 업데이트됩니다. OpenShift Container Platform 4.17.z와 같은 비동기 버전 릴리스 정보는 하위 섹션에 자세히 설명되어 있습니다. 또한 공간 제한으로 인해 릴리스 정보에 포함되지 않은 에라타 컨텐츠도 다음 하위 섹션에 자세히 설명되어 있습니다.

중요

OpenShift Container Platform 릴리스의 경우 항상 클러스터 업데이트 지침을 검토하십시오.

1.9.1. RHBA-2025:21225 - OpenShift Container Platform 4.17.44 버그 수정 권고

출시 날짜: 2025년 11월 19일

OpenShift Container Platform 릴리스 4.17.44가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:21225 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:21221 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.44--pullspecs
```

1.9.2. 버그 수정

이 릴리스에 대해 다음 버그가 수정되었습니다.

- 이번 업데이트 이전에는 사용자 관리 로드 밸런서를 사용 중인 경우에도 API 및 Ingress 가상 IP(VIP) 주소가 자동으로 할당되었습니다. 이번 릴리스에서는 API 및 Ingress VIP가 더 이상 자동으로 할당되지 않습니다. 이러한 값이 **install-config.yaml** 에 명시적으로 설정되지 않은 경우 설치에 실패하고 오류와 함께 제공하여 제공할 것을 요청합니다. (OCPBUGS-53236)

- 이번 업데이트 이전에는 **인증 오류** 메시지 페이지가 올바르게 렌더링되지 않아 빈 페이지가 생성되어 오류 메시지가 사용자에게 표시되지 않습니다. 이번 릴리스에서는 **인증 오류** 메시지 페이지에 콘텐츠가 표시되고 사용자 환경이 향상됩니다. (OCPBUGS-62631)

- 이번 업데이트 이전에는 OVN(Open Virtual Network)-Kubernetes 컨트롤러에서 Kubernetes API 서버의 업데이트를 처리하고 각 노드에서 OVN 데이터베이스를 구성하지 않은 경우 이 데이터베이스를 사용하는 OVN-Controller가 OVN-Kubernetes 컨트롤러에서 데이터베이스에 연결했을 수 있습니다. 그 결과 OVN-Controller는 오래된 OVN 데이터베이스와 동기화되고, 송신 IP를 지원하도록 구성된 SNAT(소스 네트워크 주소 변환)를 사용하고 해당 IP 주소가 다른 노드로 이동했을 수 있지만 관련 IP 주소에 대해 적절한 주소 확인 프로토콜(GARP)으로 진행되었습니다. 이번 릴리스에서는 OVN-Kubernetes 컨트롤러가 업데이트를 처리하지 않으면 이러한 GARP가 차단됩니다. (OCPBUGS-63154)

- 이번 업데이트 이전에는 Node Tuning Operator(NTO)가 소유한 **ocp-tuned-one-shot.service** systemd 장치를 실행할 때 kubelet에 대한 종속성 오류가 발생할 수 있었습니다. 그 결과 kubelet이 시작되지 않았습니다. 이번 릴리스에서는' ocp-tuned-one-shot.service 장치를 실행하면 종속성 실패가 발생하지 않습니다. 결과적으로 장치를 실행할 때 kubelet이 시작됩니다. (OCPBUGS-63504)

- 이번 업데이트 이전에는 gRPC 연결 로그가 매우 자세한 로그 수준으로 설정되었습니다. 이로 인해 과도한 수의 메시지가 생성되어 로그가 오버플로되었습니다. 이번 릴리스에서는 gRPC 연결 로그가 V(4) 로그 수준으로 이동되었습니다. 결과적으로 이러한 특정 메시지가 기본적으로 세부 정보가 줄어들기 때문에 로그가 더 이상 오버플로되지 않습니다. (OCPBUGS-63682)

- 이번 업데이트 이전에는 Azure 머신 공급자가 **MachineSet** 의 **dataDisks** 구성을 Azure Stack Hub의 가상 머신 생성 API 요청에 전달하지 않았습니다. 결과적으로 VM 생성 프로세스 중에 구성이 자동으로 무시되었기 때문에 지정된 데이터 디스크 없이 새 머신이 생성되었습니다. 이번 릴리스에서는 **dataDisks** 구성을 포함하도록 Azure Stack Hub의 VM 생성이 업데이트되었습니다. 추가 업데이트는 Azure Stack Hub에서 기본적으로 이 옵션을 지원하지 않기 때문에 컨트롤러에서 **deletionPolicy: Delete** 매개변수의 동작을 수동으로 구현합니다. 결과적으로 Azure Stack Hub VM에 데이터 디스크가 올바르게 프로비저닝됩니다. **Delete** 정책도 기능적으로 지원되므로 머신이 제거될 때 디스크가 올바르게 제거됩니다. (OCPBUGS-63700)

1.9.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.4. RHBA-2025:19314 - OpenShift Container Platform 4.17.43 버그 수정 업데이트 및 보안

출시 날짜: 2025년 11월 5일

OpenShift Container Platform 릴리스 4.17.43이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:19314 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:19312 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.43 --pullspecs
```

1.9.4.1. 버그 수정

- 이번 업데이트 이전에는 DNS(Domain Name System) Egress Firewall 규칙에 해당하는 **address_set** 의 오래된 IP 주소가 제거되지 않았습니다. 이로 인해 **address_set** 이 지속적으로 증가하여 메모리 누수 문제가 발생했습니다. 이번 릴리스에서는 5초 유예 기간이 지나면 오래된 IP 주소가 **address_set** 에서 제거됩니다. (OCPBUGS-61749)

- 이번 업데이트 이전에는 새로 선택한 네임스페이스로 대시보드 쿼리 템플릿이 업데이트되지 않았습니다. 그 결과 namespace 매개변수와 쿼리 간에 차이가 있어 요청이 거부되었습니다. 이번 릴리스에서는 콘솔에서 대시보드 네임스페이스 변수가 콘솔의 선택한 네임스페이스와 동기화됩니다. 결과적으로 동기화된 대시보드 변수가 쿼리 템플릿에 채워지고 백엔드는 올바른 결과를 반환합니다. (OCPBUGS-62282)

- 이번 업데이트 이전에는 연결된 URL이 개발자 화면에 있었지만 링크를 클릭하면 관점이 전환되지 않았습니다. 그 결과 빈 페이지가 표시되었습니다. 이번 릴리스에서는 링크를 클릭하면 관점이 변경되고 페이지가 올바르게 표시됩니다. (OCPBUGS-63212)

- 이번 업데이트 이전에는 하나 이상의 머신 세트에서 **capacity.cluster-autoscaler.kubernetes.io/labels** 주석의 여러 레이블로 인해 MCO(Machine Config Operator)가 실패했습니다. 이번 릴리스에서는 MCO에서 **capacity.cluster-autoscaler.kubernetes.io/labels** 주석에서 여러 레이블을 허용합니다. 결과적으로 4.19.6로 업데이트하는 동안 MCO가 실패하지 않습니다. (OCPBUGS-63364)

- 이번 업데이트 이전에는 **--dry-run=server** 옵션을 사용하여 **istag** 리소스를 실수로 삭제하여 서버에서 이미지를 실제로 삭제했습니다. 이 예기치 않은 삭제는 **oc delete istag** 명령에서 **시험 실행** 옵션이 잘못 구현되어 발생했습니다. 이번 릴리스에서는 이제 **oc delete istag** 명령에 **시험 실행** 옵션이 연결되어 실수로 이미지 오브젝트가 삭제되지 않습니다. **--dry-run=server** 옵션을 사용할 때 **istag** 오브젝트는 그대로 유지됩니다. (OCPBUGS-63392)

- 이번 업데이트 이전에는 일반 사용자가 프로젝트를 아직 생성하지 않은 경우 **역할** 목록 페이지에 잘못된 데이터를 표시할 수 있었습니다. 이번 릴리스에서는 **역할** 목록 페이지가 올바르게 표시됩니다. (OCPBUGS-63397)

- 이번 업데이트 이전에는 요청에 대한 감사 로그 항목을 생성하는 동안 Webhook 실패가 **kube-apiserver** 충돌을 트리거할 수 있었습니다. 그 결과 API 서버 중단이 가능했습니다. 이번 릴리스에서는 **kube-apiserver** 가 더 이상 충돌하지 않고 API 중단이 해결되도록 감사 시스템이 업데이트되었습니다. (OCPBUGS-63460)

- 이번 업데이트 이전에는 OpenShift Container Platform 4.12 전에 생성된 컨트롤 플레인 노드에 **node-role.kubernetes.io/control-plane** 레이블이 없었습니다. 이번 릴리스에서는 라벨이 누락된 경우 MCO(Machine Config Operator)에서 컨트롤 플레인 노드를 해제할 때마다 라벨을 추가합니다. (OCPBUGS-63540)

1.9.4.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.5. RHBA-2025:18235 - OpenShift Container Platform 4.17.42 버그 수정 업데이트 및 보안

출시 날짜: 2025년 10월 22일

OpenShift Container Platform 릴리스 4.17.42가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:18235 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.42 --pullspecs
```

1.9.5.1. 버그 수정

- 이번 업데이트 이전에는 호스팅된 컨트롤 플레인 페이로드의 여러 미러로 인해 이미지 조회 실패로 인해 여러 미러 이미지가 처리되었을 때 호스트된 컨트롤 플레인 생성 오류가 발생했습니다. 이번 릴리스에서는 호스트된 컨트롤 플레인 페이로드에서 여러 미러를 지원하고, 사용할 수 없는 미러를 올바르게 처리하고, 클러스터 생성에 성공합니다. (OCPBUGS-57143)

- 이번 업데이트 이전에는 OpenShift Container Platform 버전 4.17에서 수정된 업스트림 문제가 재현할 수 없으며 다운스트림에 문제를 사용하여 트리거되었습니다. 이로 인해 사용자에게 데이터 불일치가 발생했습니다. 이번 릴리스에서는 **외부 재라이저 메커니즘의** 업스트림 문제가 수정되어 다운스트림의 잠재적인 소비를 줄일 수 있습니다. 결과적으로 OpenShift Container Platform 버전 4.17에서 문제가 발생하지 않습니다. (OCPBUGS-62466)

- 이번 업데이트 이전에는 **/etc/docker** 디렉터리에 대한 잘못된 **hostPath** 구성으로 인해 OLM(Operator Lifecycle Manager) v1 Pod 문제가 발생했습니다. 그 결과 **hostPath** 유형 검사 오류로 인해 OLM v1 Pod가 작동하지 않았습니다. 이번 릴리스에서는 **hostPath** 에서 **/etc/docker** 에 대한 올바른 디렉터리를 확인하고 OLM v1 Pod 문제를 해결합니다. 결과적으로 OpenShift Container Platform 클러스터가 원활하게 작동합니다. (OCPBUGS-62741)

1.9.5.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.6. RHSA-2025:17232 - OpenShift Container Platform 4.17.41 버그 수정 업데이트 및 보안

출시 날짜: 2025년 10월 8일

OpenShift Container Platform 릴리스 4.17.41이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:17232 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:17230 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.41 --pullspecs
```

1.9.6.1. 버그 수정

- 이번 릴리스 이전에는 동일한 노드의 Pod가 **br-ex** 브리지의 Pod의 보조 **Localnet** 인터페이스에 연결할 수 없어 Pod가 기본 네트워크였습니다. 이번 릴리스에서는 **Localnet** 네트워크의 IP 주소가 호스트 네트워크와 동일한 서브넷에 있는 경우 **Localnet** pod와 동일한 노드에서 실행되는 포드 간 통신이 가능합니다. (OCPBUGS-59381)

- 이번 릴리스 이전에는 **configure-ovs.sh** 스크립트가 연결 프로필을 활성화하면 스위치 측에서 포트가 비활성화된 오류 상태가 트리거되었습니다. 이번 릴리스에서는 **configure-ovs.sh** 스크립트가 정상적인 활성화가 발생할 때까지 대기하고 필요한 경우가 아니면 프로필 상태를 변경하지 않습니다. 이러한 변경으로 인해 이전에 문제가 발생한 링크가 표시되지 않습니다. (OCPBUGS-60890)

- 이번 릴리스 이전에는 원격 끝점이 데이터를 수신하지 않은 경우에도 **PrometheusRemoteWriteBehind** 경고를 활성화할 수 있었습니다. 이번 릴리스에서는 원격 끝점이 데이터를 수신하지 않으면 이러한 경고가 활성화되지 않습니다. (OCPBUGS-61766)

- 이번 릴리스 이전에는 Kubernetes 클러스터에서 **virt-launcher** Pod의 명령줄 로그가 수집되지 않아 가상 머신 문제를 해결하기가 어려웠습니다. 이번 릴리스에서는 **virt-launcher** Pod의 명령줄 로그가 수집되어 **네임스페이스/{namespace-name}/pods/{pod-name}/virt-launcher.json** 에서 JSON 형식으로 저장되므로 디버깅이 가능합니다. (OCPBUGS-61775)

- 이번 릴리스 이전에는 **nmstate-2.2.48** 의 **systemd** 서비스 종속성 문제로 인해 특정 노드에서 서비스가 시작되지 않았습니다. 이번 릴리스에서는 업스트림의 고정 **systemd** 장치가 배포되고 수정 사항이 포함된 새 **nmstate** 패키지가 보류 중인 동안 서비스가 올바르게 시작됩니다. (OCPBUGS-61859)

1.9.6.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.7. RHBA-2025:16133 - OpenShift Container Platform 4.17.40 버그 수정 업데이트 및 보안

출시 날짜: 2025년 9월 24일

OpenShift Container Platform 릴리스 4.17.40이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:16133 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:16131 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.40 --pullspecs
```

1.9.7.1. 기능 개선

- 이번 업데이트를 통해 **cluster-etcd-operator** 는 **etcdDatabaseQuotaLowSpace** 경고에 대한 다단계 알림 시스템을 구현하여 etcd 스토리지 할당량을 사전에 관리합니다. 이 향상된 기능은 낮은 데이터베이스 공간의 이전 경고를 제공하여 API 서버 불안정을 방지하도록 설계되었습니다. etcd 디스크 공간 사용량이 Cryostat, 75% 및 85%에 도달하면 관리자가 심각도 수준의 정보, 경고 또는 심각으로 경고를 수신합니다. (OCPBUGS-61337)

1.9.7.2. 버그 수정

- 이번 업데이트 이전에는 미러 레지스트리가 설정된 경우에도 해당 레지스트리가 **NeverContactSource** 값으로 구성된 경우 이미지 가져오기 차단 레지스트리가 실패했습니다. 이번 업데이트를 통해 레지스트리에 미러가 구성된 경우 이미지 가져오기가 차단되지 않습니다. 이번 수정을 통해 **ImageDigestMirrorSet** 또는 **ImageTagMirrorSet** 리소스에서 원래 소스가 **NeverContactSource** 로 설정되어 있어도 이미지 가져오기가 성공적으로 수행됩니다. (OCPBUGS-53382)

- 이번 업데이트 이전에는 오래된 버전의 Azure API로 인해 **MachineSet** 의 용량 예약 그룹 사양이 발생하지 않았습니다. 해당 그룹이 서버 생성과 다른 서브스크립션에 있는 경우입니다. 이번 릴리스에서는 가장 최신 버전의 Azure API가 사용되어 해당 그룹이 서버의 생성 지점에서 별도의 서브스크립션에 있는 경우에도 **MachineSet** 의 용량 예약 그룹을 지정할 수 있습니다. (OCPBUGS-56168)

- 이번 업데이트 이전에는 **MachineSet** 이 축소되어 최소 크기에 도달하면 클러스터 자동 스케일러에서 노드 사용을 방지하는 **NoSchedule** 테인트가 있는 마지막 나머지 노드를 유지할 수 있었습니다. 이 문제는 클러스터 자동 스케일러의 계산 오류로 인해 발생했습니다. 이번 릴리스에서는 **MachineSet** 이 축소되고 최소 크기에 도달했을 때 클러스터 자동 스케일러가 예상대로 작동하도록 계산 오류가 수정되었습니다. (OCPBUGS-59266)

- 이번 업데이트 이전에는 OpenShift Container Platform 이미지 레지스트리를 비활성화하면 네임스페이스를 삭제하는 동안 기존 pull secret이 삭제되었습니다. 결과적으로 OpenShift Container Platform 이미지 레지스트리를 비활성화한 후 **Dockercfg** 보안을 삭제할 수 없었습니다. 이번 릴리스에서는 레지스트리를 제거한 후 기존 풀 시크릿에서 네임스페이스 삭제를 차단하지 않습니다. (OCPBUGS-61199)

- 이번 업데이트 이전에는 잘못된 **semver** 구문 분석 문제로 인해 빌드 오류가 발생했습니다. 이번 릴리스에서는 **machine-api-provider-powervs** 패키지의 **semver** 구문 분석 문제가 수정되었습니다. 결과적으로 **PowerVS machine-api-provider** 매개변수의 의미 체계 버전 구문 분석 오류가 해결되어 올바른 버전 처리 및 안정성이 향상됩니다. (OCPBUGS-61204)

- 이번 업데이트 이전에는 기본 **node-monitor-grace-period** 값이 50초였습니다. 결과적으로 노드는 Kubernetes 구성 요소가 요청을 다시 연결, 조정 및 완료하는 데 필요한 기간 동안 준비되지 않았습니다. 이번 릴리스에서는 기본 **node-monitor-grace-period** 값은 55초입니다. 따라서 배포를 완료하는 데 충분한 시간이 있습니다. (OCPBUGS-61290)

1.9.7.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.8. RHBA-2025:15344 - OpenShift Container Platform 4.17.39 버그 수정 업데이트 및 보안

출시 날짜: 2025년 9월 10일

OpenShift Container Platform 릴리스 4.17.39가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:15344 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:15323 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.39 --pullspecs
```

1.9.8.1. 기능 개선

1.9.8.1.1. 네트워크 포트가 외부 네트워크에 잘못 열려 있음

이번 개선된 기능을 통해 **localhost** 의 연결만 허용하도록 **cluster-policy-controller** 가 재구성되어 노드 네트워크 외부에서 네트워크 포트(10357)가 노출되지 않습니다. (OCPBUGS-60249)

1.9.8.2. 버그 수정

- 이번 업데이트 이전에는 최근 CSRF(Cross-Site Request Forgery) 보호 기능이 포함된 인증을 요구하도록 '/metrics/usage' 엔드포인트가 업데이트되었습니다. 엔드포인트에 대한 요청은 요청에 새로 필요한 CSRF 토큰이 쿠키 내에 포함되지 않았기 때문에 **금지된** 응답으로 실패하기 시작했습니다. 이번 릴리스에서는 '/metrics/usage' 엔드포인트에 대한 모든 호출에 대한 요청 템플릿에 CSRF 토큰이 추가되어 **금지된** 오류가 제거되었습니다. (OCPBUGS-58365)

- 이번 업데이트 이전에는 클러스터 Operator가 업그레이드하는 데 시간이 오래 걸리는 경우 Cluster Version Operator는 업그레이드가 계속 진행 중이거나 이미 중단되었는지 여부를 결정할 수 없기 때문에 아무것도 보고하지 않습니다. 이번 릴리스에서는 Cluster Version Operator가 보고한 클러스터 vVersion의 상태에 실패한 상태에 대해 새로운 알 수 없는 상태가 추가되었습니다. 이렇게 하면 클러스터 관리자가 클러스터를 확인하고 차단된 클러스터 Operator 업그레이드를 기다리지 않도록 경고합니다. (OCPBUGS-58451)

- 이번 업데이트 이전에는 다운로드 및 콘솔 Pod의 노드 선택기가 일치하지 않기 때문에 컨트롤 플레인 노드의 다운로드가 일관되지 않게 예약되었습니다. 그 결과 임의의 노드에 다운로드가 예약되어 잠재적인 리소스 경합 및 하위 성능이 발생했습니다. 이번 릴리스에서는 컨트롤 플레인 노드에서 다운로드된 워크로드를 일관되게 예약하여 리소스 할당을 개선합니다. (OCPBUGS-60298)

- 이번 업데이트 이전에는 호스트된 클러스터의 Insights 아카이브에 호스트 이름이 충분히 난독 지정되지 않았습니다. 이는 클라이언트 호스트 주소에 의존하는 익명화 방식으로 인해 발생했습니다. 이번 릴리스에서는 호스팅된 클러스터의 Insights 아카이브에서 모든 호스트 이름이 올바르게 난독화됩니다. (OCPBUGS-60395)

- 이번 업데이트 이전에는 버전 4.16 및 4.17의 OpenShift Container Platform 웹 콘솔에서 노드 필터링에 문제가 발생하여 필터링된 역할 대신 모든 노드를 표시했습니다. 결과적으로 사용자는 클러스터의 모든 노드를 표시하여 혼란과 잠재적 관리 문제가 발생했습니다. 이번 릴리스에서는 노드를 필터링하면 영향을 받는 역할만 표시하여 클러스터 가시성을 개선할 수 있습니다. 결과적으로 사용자 환경이 향상됩니다. (OCPBUGS-60441)

- 이번 업데이트 이전에는 Pod에 패닉이 발생했습니다. 특히 **nil 맵 오류 및 RPC(원격 프로시저 호출) keep-alive ping 시간 초과에 대한 할당** 이 발생한 후 Azure Disk CSI Driver Operator에 성능이 저하되었습니다. 이로 인해 Operator가 고정 리소스를 조정하여 향후 클러스터 업그레이드 중에 오류가 발생할 위험이 발생했습니다. 이번 릴리스에서는 **clustercsidriver** 사용자 정의 리소스가 삭제되어 Operator에서 오브젝트를 다시 생성 및 조정하고 패닉을 해결하고 클러스터의 안정성을 보장합니다. (OCPBUGS-60597)

- 이번 업데이트 이전에는 VPA(Vertical Pod Autoscaler)에 여러 권장자를 사용할 때 버그로 인해 기본 권장자가 기본값이 아닌 권장 사항과 연결된 **VPACheckpoint** 오브젝트에 속하는 VPACheckpoint 오브젝트를 잘못 삭제했습니다. 이번 릴리스에서는 기본 권장 사항이 아닌 권장 사항에 속하는 **VPACheckpoint** 오브젝트를 더 이상 삭제하지 않습니다. (OCPBUGS-60608)

- 이번 업데이트 이전에는 IdM(ID 공급자) 검증의 HTTP 클라이언트에 IdP 엔드포인트 요청을 검증하는 데 사용된 번들에 시스템 신뢰 번들이 포함되지 않았습니다. 이로 인해 IdP에서 공개적으로 신뢰할 수 있는 끝점을 사용하는 경우 IdP 검증이 실패했습니다. 이번 릴리스에서는 IdP 끝점을 검증할 때 시스템 신뢰 번들과 사용자 제공 추가 신뢰 번들이 모두 포함됩니다. (OCPBUGS-61101)

1.9.8.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.9. RHSA-2025:14060 - OpenShift Container Platform 4.17.38 버그 수정 업데이트 및 보안

출시 날짜: 2025년 8월 27일

OpenShift Container Platform 릴리스 4.17.38이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:14060 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:13976 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.38 --pullspecs
```

1.9.9.1. 기능 개선

1.9.9.1.1. sos 명령의 기본 구성

- 이번 개선된 기능에는 OpenShift Container Platform 내의 툴 **이미지 스트림에 sosreport** 명령이 추가되어 연결이 끊긴 환경에서 Telco Operator에 대한 디버깅을 간소화합니다. (OCPBUGS-56734)

1.9.9.2. 버그 수정

- 이번 릴리스 이전에는 사용자 인터페이스와 API가 일치하지 않기 때문에 vSphere 연결 구성이 포함된 리소스가 중단되었습니다. 이번 릴리스에서는 사용자 인터페이스에서 업데이트된 API 정의를 사용하므로 리소스가 중단되지 않습니다. (OCPBUGS-58337)

- 이번 릴리스 이전에는 머신 세트가 축소되어 최소 크기에 도달하면 클러스터 자동 스케일러에서 노드 사용을 방지하는 **NoSchedulle** 테인트가 있는 마지막 나머지 노드를 유지할 수 있었습니다. 이는 클러스터 자동 스케일러의 계산 오류로 인해 발생했습니다. 이번 릴리스에서는 머신 세트 축소 및 최소 크기에 도달할 때 클러스터 자동 스케일러가 예상대로 작동하도록 계산 오류가 수정되었습니다. (OCPBUGS-59266)

- 이번 릴리스 이전에는 동일한 노드의 Pod가 **br-ex** 브리지의 Pod의 보조 **Localnet** 인터페이스에 연결할 수 없어 Pod가 기본 네트워크였습니다. 이번 릴리스에서는 **Localnet** 네트워크의 IP 주소가 호스트 네트워크와 동일한 서브넷에 있는 경우 **Localnet** pod와 동일한 노드에서 실행되는 포드 간의 통신이 가능합니다. (OCPBUGS-59381)

- 이번 릴리스 이전에는 영역당 단일 작업자가 있는 다중 영역 클러스터에서 Prometheus Pod를 실행하는 두 노드가 순차적으로 재부팅되고 각각 복구하는 데 15분 이상 걸리는 경우 Monitoring Operator에서 성능이 저하될 수 있었습니다. 이번 릴리스에서는 시간 제한이 20분으로 확장되어 Monitoring Operator가 공통 클러스터 토폴로지에서 성능이 저하될 가능성이 높아집니다. (OCPBUGS-60017)

- 이번 릴리스 이전에는 경우에 따라 s3 호환 스토리지 공급자에서 실패한 업로드를 제거하려고 할 때 이미지 레지스트리가 패닉 상태가 됩니다. 이는 이미지 레지스트리의 s3 드라이버가 빈 디렉터리 경로를 잘못 처리했기 때문입니다. 이번 업데이트를 통해 이미지 레지스트리에서 빈 디렉터리 경로를 올바르게 처리합니다. (OCPBUGS-60090)

- 이번 업데이트 이전에는 업그레이드 중에 MCO(Machine Config Operator)에서 **CoreDNS** 템플릿을 업데이트하면 **CoreDNS** Pod를 일시적으로 사용할 수 없는 동안 DNS 조회 오류와 함께 다음 **rpm-ostree** 이미지 가져오기 작업이 실패했습니다. 이번 릴리스에서는 이미지 가져오기 재시도를 허용하는 운영 체제 업데이트 작업에 재시도 메커니즘이 있어 노드 업그레이드가 진행되고 완료될 수 있습니다. (OCPBUGS-60239)

- 이번 릴리스 이전에는 **cloud-event-proxy** 컨테이너 또는 Pod가 재부팅될 때 이벤트 데이터를 아직 사용할 수 없는 기간이 있었습니다. 이로 인해 **getCurrenState** 함수가 0의 **클럭 클래스** 를 잘못 반환했습니다. 이번 릴리스에서는 **getCurrentState** 함수가 더 이상 잘못된 **클럭 클래스** 를 반환하지 않고 HTTP **400 Bad Request** 또는 **404 Not Found Error** 를 반환합니다. (OCPBUGS-60267)

1.9.9.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.10. RHSA-2025:12437 - OpenShift Container Platform 4.17.37 버그 수정 업데이트 및 보안

출시 날짜: 2025년 8월 6일

OpenShift Container Platform 릴리스 4.17.37이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:12437 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:12438 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.37 --pullspecs
```

1.9.10.1. 버그 수정

- 이번 업데이트 이전에는 **catalog-operator** 에서 5분마다 스냅샷을 캡처하여 여러 네임스페이스, 서브스크립션 및 대규모 카탈로그 소스를 처리할 때 CPU가 급증했습니다. 이로 인해 카탈로그 소스 Pod에 대한 로드가 증가하여 사용자가 Operator를 설치하거나 업그레이드할 수 없었습니다. 이번 릴리스에서는 카탈로그 스냅샷 캐시 수명이 30분으로 증가하여 Operator 설치 및 업그레이드 프로세스를 유발하지 않고 카탈로그 소스가 시도를 해결할 충분한 시간을 허용합니다. (OCPBUGS-57428)

- 이번 업데이트 이전에는 **console.tab/horizontalNav href** 값에 슬래시가 허용되었습니다. 4.15부터 회귀 문제로 인해 **href** 값에서 사용할 때 슬래시가 더 이상 제대로 작동하지 않습니다. 이번 릴

리스에서는 **console.tab/horizontalNav href** 값의 슬래시가 예상대로 작동합니다. (OCPBUGS-59265)

- 이번 업데이트 이전에는 **Observe → Metrics → query → QueryKebab → Export as csv** 드롭다운 항목에서는 정의되지 않은 제목 요소를 처리하지 않았습니다. 그 결과 OpenShift Lister 버전 4.17의 **Metrics** 탭에서 특정 쿼리에 대한 CSV 파일을 내보낼 수 없었습니다. 이번 릴리스에서는 모든 쿼리에 대한 메트릭이 드롭다운 메뉴 항목에서 오브젝트 속성을 올바르게 처리하여 CSV 내보내기에 성공합니다. (OCPBUGS-52592)

1.9.10.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.11. RHSA-2025:11359 - OpenShift Container Platform 4.17.36 버그 수정 업데이트 및 보안

출시 날짜: 2025년 7월 23일

OpenShift Container Platform 릴리스 4.17.36이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:11359 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:11360 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.36 --pullspecs
```

1.9.11.1. 버그 수정

- 이번 업데이트 이전에는 네트워크 플러그인 페이지의 초기 로드 시간이 10초로 증가했습니다. 이번 릴리스에서는 네트워크 플러그인 페이지 지연을 수정하여 초기 로드 시간이 단축됩니다. (OCPBUGS-58318)

- 이번 업데이트 이전에는 동일한 **useModal** 후크를 사용하는 여러 플러그인으로 인해 모달이 서로 덮어쓰고 사용자 인터페이스에서 여러 플러그인에 대한 기능이 손실되었습니다. 이번 릴리스에서는 고유 식별자가 사용되며 모달은 서로 덮어쓰지 않습니다. (OCPBUGS-58224)

- 이번 업데이트 이전에는 MCO(Machine Config Operator)가 성능 저하 없이 기본이 아닌 부팅 이미지를 업데이트하지 않아 시스템 불안정성이 발생했습니다. 이번 릴리스에서는 기본이 아닌 부팅 이미지 업데이트에 대한 MCO 성능 저하가 수정되었으며 부팅 이미지 업데이트 문제가 발생하지 않습니다. (OCPBUGS-58219)

- 이번 업데이트 이전에는 서비스 계정 시크릿 검색이 누락되어 빌드 오류가 발생했습니다. 이번 릴리스에서는 서비스 계정 시크릿을 검색할 때 오류가 발생하지 않으며 **CannotRetrieveServiceAccount** 오류로 인해 오류가 제거됩니다. (OCPBUGS-57950)

- 이번 업데이트 이전에는 OperatorGroup 리소스 조정으로 인해 집계 규칙 선택기가 변경되어 불필요한 **ClusterRole** 업데이트가 발생했습니다. 결과적으로 불필요한 etcd 쓰기 및 인증 캐시 무효화가 발생했습니다. 이번 릴리스에서는 **ClusterRole** 집계 규칙 선택기의 특정 순서에 따라 불필요한 API 서버 쓰기가 줄어듭니다. (OCPBUGS-57438)

- 이번 업데이트 이전에는 **chroot** 에서 **SYS_CHROOT** 권한이 누락되어 ingress 가상 IP(VIP) 검사의 Keepalived 스크립트가 실패했습니다. 결과적으로 잘못된 VIP 배치로 인해 핵심 수신 서비스에

액세스할 수 없었습니다. 이번 릴리스에서는 ingress VIP 검사를 위해 Keepalived 스크립트에 **chroot** 권한이 추가됩니다. 결과적으로 잘못된 **chk_default_ingress** 권한이 수정되어 수신 VIP가 올바르게 배치됩니다. (OCPBUGS-56625)

1.9.11.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.12. RHSA-2025:10294 - OpenShift Container Platform 4.17.35 버그 수정 업데이트 및 보안

출시 날짜: 2025년 7월 9일

OpenShift Container Platform 릴리스 4.17.35가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:10294 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2025:10295 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.35 --pullspecs
```

1.9.12.1. 기능 개선

1.9.12.1.1. 확장되는 루프백 인증서 만료일

- 이번 개선된 기능을 통해 Kubernetes API 서버의 자체 서명된 **루프백** 인증서의 만료 날짜가 1년에서 3년으로 연장되었습니다. (OCPBUGS-57196)

1.9.12.2. 버그 수정

- 이전 버전에서는 명령이 아티팩트를 디스크에 저장할 때 **oc adm node-image create** 명령에서 대상 자산 폴더의 기존 권한을 잘못 수정했습니다. 이번 릴리스에서는 명령에 대한 복사 작업이 대상 폴더 권한을 유지할 수 있도록 버그 수정을 통해 확인할 수 있습니다. (OCPBUGS-58091)

- 이전 버전에서는 AWS(Amazon Web Services)의 기존 VPC(가상 프라이빗 클라우드)에 설치할 때 컨트롤 플레인 노드의 머신 세트 사용자 정의 리소스와 해당 AWS EC2 인스턴스 간의 AWS 가용성 영역의 서브넷 정보에서 잠재적인 불일치가 발생할 수 있었습니다. 그 결과 컨트롤 플레인 노드가 세 개의 가용 영역에 분산되고 하나를 다시 생성한 경우 동일한 가용성 영역 내에서 두 노드가 발생하여 불일치가 불안정한 컨트롤 플레인이 발생할 수 있었습니다. 이번 릴리스에서는 머신 세트 사용자 정의 리소스 및 EC2 인스턴스의 서브넷 가용성 영역 정보가 일치하고 문제가 해결되었습니다. (OCPBUGS-57293)

- 이전에는 커널에서 **stat** 호출이 중단된 경우 kubelet에서 보고 메트릭을 중지했습니다. 예를 들어 디스크에 대한 통계 **호출이** NFS(Network File System)에서 실행된 경우입니다. 이번 릴리스에서는 디스크가 중단된 경우에도 kubelet에서 메트릭을 보고합니다. (OCPBUGS-57289)

- 이전에는 **/metrics** 엔드포인트가 내부 Prometheus 스크랩 요청의 권한 부여 헤더에서 전달자 토큰을 올바르게 구문 분석하지 못했습니다. 이로 인해 **TokenReviews** 가 실패하고 콘솔 지표 끝점에 대해 **TargetDown** 경고가 트리거되었습니다. 이번 릴리스에서는 **/metrics** 끝점이 인증 헤더에

서 전달자 토큰을 올바르게 구문 분석하고 **TokenReview** 단계가 의도한 대로 작동하며 **TargetDown** 경고가 더 이상 표시되지 않습니다. (OCPBUGS-57182)

- 이전에는 **iptables-alerter** Pod에서 클러스터에 대한 정보를 가져오기 위해 노드에 존재하는 각 pod에 대해 **crictl** CLI(명령줄 인터페이스)를 여러 번 호출해야 했습니다. 이러한 호출에는 클러스터 성능에 영향을 미치는 높은 CPU 사용량이 필요했습니다. 이번 릴리스에서는 **iptables-alerter** Pod가 노드에 있는 모든 Pod에 대한 정보를 가져오기 위해 **crictl** 을 한 번만 호출해야 합니다. (OCPBUGS-55518)

- 이전에는 Ingress 컨트롤러 API에 **IdleConnectionTerminationPolicy** API 설정이 없는 클러스터에 기본적으로 **idle-close-on-response** HAProxy 설정이 활성화되어 있었습니다. 이로 인해 응답 즉시 유휴 연결이 닫힙니다. 이번 릴리스에서는 **Deferred** 가 기본값으로 설정된 Ingress 컨트롤러 API 설정에 **IdleConnectionTerminationPolicy** API 설정이 추가되어 소프트 중지 후 마지막 응답이 처리될 때까지 HAProxy 설정을 활성화하고 유휴 연결을 유지할 수 있었습니다. (OCPBUGS-49702)

1.9.12.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.13. RHBA-2025:9289 - OpenShift Container Platform 4.17.34 버그 수정 업데이트

출시 날짜: 2025년 6월 25일

OpenShift Container Platform 릴리스 4.17.34가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:9289 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:9290 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.34 --pullspecs
```

1.9.13.1. 확인된 문제

- 기술 프리뷰 지원 클러스터에 **policy.json** 파일의 페이로드 이미지에 대한 Sigstore 확인이 있지만 기본 이미지의 Podman 버전에서는 Sigstore 구성을 지원하지 않으므로 새 노드를 사용할 수 없습니다. 이 문제를 해결하려면 기본 이미지의 Podman 버전이 Sigstore를 지원하지 않을 때 노드가 실행을 시작하므로 기본 이미지 4.11 이상인 경우 Sigstore 확인 기능이 없는 기본 **policy.json** 파일을 사용합니다. (OCPBUGS-52313)

1.9.13.2. 버그 수정

- 이전에는 인플레이스 업데이트를 사용한 호스팅 클러스터를 업데이트하려고 하면 프록시 변수가 적용되지 않고 업데이트가 실패했습니다. 이번 릴리스에서는 인플레이스 업그레이드를 수행하는 Pod가 클러스터 프록시 설정을 준수합니다. 결과적으로 인플레이스 업데이트를 사용하는 호스팅된 클러스터에서 업데이트가 작동합니다. (OCPBUGS-57432)

- 이전 버전에서는 **install-config.yaml** 구성 파일에서 **machineNetwork** 매개변수에 대한 BYOO(bring-your-own) 서브넷 CIDR을 여러 개 정의하면 부트스트랩 단계에서 설치에 실패했습니다. 이 상황은 필요한 설정 구성을 가져오기 위해 컨트롤 플레인 노드가 MCS(Machine config server)에 도달하지 못했기 때문에 발생했습니다. 근본 원인은 첫 번째 지정된 시스템 네트워크 CIDR로만

MCS 액세스를 제한하는 엄격하게 엄격한 AWS 보안 그룹 규칙이었습니다. 이번 릴리스에서는 AWS 보안 그룹에 대한 수정으로 **install-config.yaml** 의 **machineNetwork** 매개변수에 여러 CIDR이 지정되면 설치에 성공했음을 의미합니다. (OCPBUGS-57292)

- 이전에는 MCO(Machine Config Operator)에서 **Upgradeable=False** 조건을 클러스터에 추가된 모든 새 노드로 잘못 설정했습니다. **Upgradeable=False** 조건에 대해 **PoolUpdating** 이유가 제공되었습니다. 이번 릴리스에서는 MCO가 클러스터에 추가되는 모든 새 노드에 **Upgradeable=True** 조건을 올바르게 설정하여 문제를 해결합니다. (OCPBUGS-57135)

- 이전에는 설치 프로그램에서 VMware vSphere 클러스터 내에서 전원이 꺼진 ESXi 호스트를 확인하지 않아 OVA를 업로드할 수 없기 때문에 설치에 실패했습니다. 이번 릴리스에서는 설치 프로그램이 각 ESXi 호스트의 전원 상태를 확인하고 전원이 꺼진 모든 항목을 건너뛰어 문제를 해결하고 OVA를 성공적으로 가져올 수 있습니다. (OCPBUGS-56448)

- 이전 버전에서는 특정 상황에서 노드의 게이트웨이 IP 주소가 변경되어 **OVN** 클러스터 라우터에서 원래 IP 주소를 삭제하지 않고 새 게이트웨이 IP 주소가 있는 새 고정 경로를 추가했습니다. **OVN** 클러스터 라우터는 클러스터 서브넷에 대한 정적 경로를 관리합니다. 결과적으로 오래된 경로는 여전히 스위치 서브넷을 가리키며 이로 인해 송신 트래픽 전송 중에 간헐적으로 중단되었습니다. 이번 릴리스에서는 **OVN** 클러스터 라우터에 적용된 패치를 통해 게이트웨이 IP 주소가 변경되면 **OVN** 클러스터 라우터가 기존 정적 경로를 새 게이트웨이 IP 주소로 업데이트합니다. 오래된 경로는 더 이상 **OVN** 클러스터 라우터를 가리키므로 송신 트래픽 흐름이 떨어지지 않습니다. (OCPBUGS-56443)

- 이전 버전에서는 **br-ex** 인터페이스 브리지에 연결된 OVN-Kubernetes **Localnet** 네트워크에 보조 인터페이스가 있는 Pod가 동일한 노드의 다른 Pod에 의해 연결되지 않지만 통신에 기본 네트워크를 사용했습니다. 다른 노드의 Pod 간 통신에는 영향을 미치지 않았습니다. 이번 릴리스에서는 동일한 노드에서 실행되는 **Localnet** 포드와 기본 네트워크 포드 간 통신이 가능하지만 **Localnet** 네트워크에서 사용되는 IP 주소는 호스트 네트워크와 동일한 서브넷에 있어야 합니다. (OCPBUGS-56244)

1.9.13.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.14. RHSA-2025:8552 - OpenShift Container Platform 4.17.33 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2025년 6월 11일

OpenShift Container Platform 릴리스 4.17.33이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:8552 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:8553 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.33 --pullspecs
```

1.9.14.1. 확인된 문제

- Pod에 외부 시스템에 대한 연결이 설정된 동안 송신 IP가 다른 노드로 이동되면 Pod는 일부 트래픽을 통과할 때까지 동일한 연결의 외부 시스템에서 트래픽을 수신하지 않습니다. 현재 이 문제에

대한 해결방법이 없습니다. Pod가 연결된 상태를 유지하려면 송신 IP를 통해 열려 있는 연결을 통해 일부 트래픽을 정기적으로 전송하여 송신 IP 페일오버 중에 연결 방향을 모두 작동해야 합니다. (OCPBUGS-58355)

1.9.14.2. 버그 수정

- 이전에는 OpenShift Container Platform 웹 콘솔에서 컨트롤 플레인 노드를 업데이트한 후 60일 이내에 컴퓨팅 노드를 업데이트해야 한다는 경고를 전송했습니다. 이 작업 요청이 잘못되었습니다. 이번 업데이트를 통해 OpenShift Container Platform 웹 콘솔에서 더 이상 잘못된 경고를 보내지 않습니다. (OCPBUGS-56375)

1.9.14.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.15. RHSA-2025:8280 - OpenShift Container Platform 4.17.32 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2025년 6월 4일

OpenShift Container Platform 릴리스 4.17.31이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:8280 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:8281 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.32 --pullspecs
```

1.9.15.1. 버그 수정

- 이전 버전에서는 버그 수정으로 fault 도메인 수를 2로 고정하지 않고 사용 가능한 최대 값을 사용하도록 변경하여 가용성 세트 구성이 변경되었습니다. 이로 인해 컨트롤러에서 변경할 수 없는 가용성 세트를 수정하려고했기 때문에 버그 수정 전에 생성된 **MachineSet** 오브젝트에 대한 확장 문제가 발생했습니다. 이번 릴리스에서는 생성 후 가용성 세트가 더 이상 수정되지 않으므로 영향을 받는 **MachineSet** 오브젝트를 올바르게 확장할 수 있습니다. (OCPBUGS-56655)

- 이전에는 조건의 상태가 실제로 변경되지 않은 경우에도 Samples Operator에서 Progressing 조건의 **lastTransitionTime** 값을 업데이트했습니다. 이로 인해 최종 사용자가 잠재적인 설치 오류 및 인식되는 불안정성을 초래했습니다. 이번 릴리스에서는 상태 변경이 없는 한 Operator에서 **lastTransitionTime** 값을 업데이트할 수 없습니다. 이렇게 하면 Operator 안정성이 향상되고 설치 프로그램 오류를 최소화하고 더 원활한 사용자 환경을 보장합니다. (OCPBUGS-55800)

- 이전에는 Samples Operator가 클러스터의 모든 클러스터 Operator를 조사하여 Cluster Samples Operator 동기화 루프를 불필요하게 실행했습니다. 이 동작은 전반적인 성능에 부정적인 영향을 미쳤습니다. 이번 릴리스에서는 Cluster Samples Operator만 특정 클러스터 Operator를 감시합니다. (OCPBUGS-55795)

- 이전에는 Grandmaster Timekeeper(T-GM) 작업이 예기치 않게 PTP(Precision Time Protocol)에 메시지 내부 신호 플래그를 잘못 설정했습니다. 이로 인해 네트워크에서 시간 동기화가 손실되었습니다. 이번 릴리스에서는 PTP 발표 메시지 플래그가 올바르게 초기화되어 네트워크에서 정확하고 표준화된 시간 동기화 정보가 보급되도록 합니다. (OCPBUGS-55740)

- 이전에는 Zscaler 플랫폼에서 모든 데이터 전송을 스캔하여 이미지 풀 시간 초과가 발생했습니다. 이로 인해 이미지 가져오기가 시간 초과되었습니다. 이번 릴리스에서는 이미지 풀 시간 초과가 30초로 증가하여 성공적으로 업데이트할 수 있습니다. (OCPBUGS-54664)

1.9.15.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.16. RHBA-2025:8108 - OpenShift Container Platform 4.17.31 버그 수정

출시 날짜: 2025년 5월 28일

OpenShift Container Platform 릴리스 4.17.31이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:8108 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.31 --pullspecs
```

1.9.16.1. 버그 수정

- 이전에는 OLM(OpenShift Lifecycle Manager)에서 관리하는 OpenShift Container Platform 4.15 이상 버전에 **olm.managed: "true"** 레이블이 필요했습니다. 경우에 따라 레이블이 누락된 경우 솔루션을 시작하지 못하고 **CrashLoopBackOff** 상태를 입력합니다. 이 시나리오의 로그는 정보가 제공되어 근본 원인을 식별하는 것이 더 어려웠습니다. 이번 릴리스에서는 라벨이 누락될 때 문제를 더 명확하고 쉽게 진단하기 위해 로그 수준이 오류로 변경되었습니다. (OCPBUGS-56250)

- 이전 버전에서는 빌드 컨테이너에서 기본 프록시 환경 변수가 null로 설정된 경우 컨테이너의 일부 애플리케이션이 실행되지 않았습니다. 이번 릴리스에서는 프록시 환경 변수가 정의되어 있고 기본값이 null이 아닌 경우에만 빌드 컨테이너에 추가됩니다. (OCPBUGS-55826)

- 이전에는 조건의 상태가 실제로 변경되지 않은 경우에도 Operator에서 Progressing 조건의 **lastTransitionTime** 값을 업데이트했습니다. 이로 인해 최종 사용자가 잠재적인 설치 오류 및 인식되는 불안정성을 초래했습니다. 이번 릴리스에서는 상태 변경이 없는 한 Operator에서 **lastTransitionTime** 값을 업데이트할 수 없습니다. 이렇게 하면 Operator 안정성이 향상되고 설치 프로그램 오류를 최소화하고 더 원활한 사용자 환경을 보장합니다. (OCPBUGS-55800)

- 이전에는 Cluster Samples Operator가 클러스터의 모든 클러스터 Operator를 조사하여 Cluster Samples Operator 동기화 루프를 불필요하게 실행했습니다. 이 동작은 전반적인 성능에 부정적인 영향을 미쳤습니다. 이번 릴리스에서는 Cluster Samples Operator만 특정 클러스터 Operator를 감시합니다. (OCPBUGS-55795)

- 이전에는 Grandmaster Timekeeper(T-GM) 작업이 예기치 않게 PTP(Precision Time Protocol)에 메시지 내부 신호 플래그를 잘못 설정했습니다. 이로 인해 네트워크에서 시간 동기화가 손실되었습니다. 이번 릴리스에서는 메시지 내부 신호 플래그가 올바르게 초기화되어 네트워크에서 정확하고 표준화된 시간 동기화 정보가 보급되도록 합니다. (OCPBUGS-55740)

- 이전에는 프로토콜을 지정하지 않고 다중 네트워크 정책을 생성할 때 OVN(Open Virtual Network)이 충돌했습니다. 이번 릴리스에서는 프로토콜이 지정되지 않은 경우 TCP(Transmission Control Protocol)로 간주하여 OVN 충돌을 방지합니다. (OCPBUGS-52480)

1.9.16.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.17. RHSA-2025:7669 - OpenShift Container Platform 4.17.30 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 5월 21일

OpenShift Container Platform 릴리스 4.17.30이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:7669 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:7671 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.30 --pullspecs
```

1.9.17.1. 버그 수정

- 이전에는 실패한 ingress-to-route 변환에서 오류가 발생했을 때 이벤트가 기록되지 않았습니다. 이번 업데이트를 통해 이 오류가 **이벤트** 로그에 표시됩니다. (OCPBUGS-55943)

- 이전 버전에서는 버그로 인해 정렬되지 않은 이미지 가져오기로 인해 **진행** 중인 상태에 대한 과도한 업데이트가 발생했습니다. 이로 인해 사용자에게 불필요한 리소스 소비가 발생했습니다. 이번 릴리스에서는 이미지 가져오기 실패를 정렬하여 Samples Operator에서 과도한 업데이트가 수정되었습니다. 결과적으로 이미지 가져오기에 대한 불필요한 업데이트를 줄임으로써 Operator 성능이 향상됩니다. (OCPBUGS-55894)

- 이전 버전에서는 프로비저닝 중에 Microsoft Azure Spot 가상 머신(VM) 할당 해제가 발생했을 때 머신 컨트롤러가 루프에 진입하여 Spot 가상 머신 프로비저닝 실패 및 사용 불가능한 노드가 발생했습니다. 이번 릴리스에서는 Azure Spot 가상 머신 프로비저닝의 **삭제 제거 정책으로 deallocate 제거 정책이** 교체됩니다. 결과적으로 머신 컨트롤러는 복원력이 뛰어나며 프로비저닝 중에 더 이상 루프에 들어가지 않습니다. (OCPBUGS-55729)

1.9.17.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.18. RHSA-2025:4723 - OpenShift Container Platform 4.17.29 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 5월 15일

OpenShift Container Platform 릴리스 4.17.29가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:4723 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:4725 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.29 --pullspecs
```

1.9.18.1. 버그 수정

- 이전에는 호스트 이름의 경쟁 조건으로 인해 노드와 머신 호스트 이름 간에 불일치가 발생했습니다. 이번 릴리스에서는 경쟁 조건이 확인되어 운영 체제 설치 중에 Ignition 구성 파일에서 일관된 호스트 이름을 유지할 수 있습니다. (OCPBUGS-55680).

- 이전에는 사용자가 **hc.spec.configuration.apiServer.servingCerts.namedCertificates** 필드에 추가한 사용자 정의 인증서의 주체 대체 이름(SAN)이 Kubernetes 에이전트 서버(KAS)의 **hc.spec.services.servicePublishingStrategy** 필드에 설정된 호스트 이름과 충돌했습니다. 그 결과 새 페이로드를 생성하기 위해 인증서 세트에 KAS 인증서가 추가되지 않아 호스팅된 클러스터에 조인된 노드에 대한 인증서 유효성 검사 문제가 발생했습니다. 이번 릴리스에서는 사용자가 충돌하는 SAN 관련 문제에 대해 사용자에게 경고하기 위해 이전에 검증에 실패합니다. (OCPBUGS-55500).

- 이전에는 지정된 리전의 AMI(Amazon Machine Image)를 찾을 수 없는 경우 부팅 이미지 업데이트가 실패했습니다. 이 문제는 모든 리전의 AMI가 설치 프로그램의 **scos.json** 파일에 게시되지 않았기 때문에 발생했습니다. 이번 릴리스에서는 AWS(Amazon Web Services) 부팅 이미지 업데이트 중에 사용할 수 없는 모든 리전에 대해 기본적으로 **us-east-1** 리전을 사용하면 업데이트 오류가 발생하지 않습니다. (OCPBUGS-55490).

- 이전에는 설치된 Operator 목록을 볼 때 Operator가 목록에 두 번 표시되었습니다. 이 중복은 현재 선택한 프로젝트가 OLM(Operator Lifecycle Manager)에서 CSV(클러스터 서비스 버전)를 복사하는 동안 Operator의 기본 네임스페이스와 일치할 때 발생했습니다. 이번 릴리스에서는 Operator가 한 번 표시됩니다. (OCPBUGS-55415).

1.9.18.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.19. RHSA-2025:4431 - OpenShift Container Platform 4.17.28 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 5월 9일

OpenShift Container Platform 릴리스 4.17.28이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:4431 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:4433 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.28 --pullspecs
```

1.9.19.1. 버그 수정

- 이전에는 노드를 볼 수 있지만 CSR(인증서 서명 요청)이 아닌 경우 **노드 목록** 페이지에 액세스할 수 없었습니다. 이번 릴리스에서는 CSR을 볼 수 있는 권한이 더 이상 **노드 목록** 페이지에 액세스할 필요가 없습니다. (OCPBUGS-55202)

- 이전 버전에서는 **ClusterResourceOverride** 사용자 정의 리소스(CR)를 삭제하거나 Cluster

Resource Override Operator를 제거한 후 **ClusterResourceOverride** CR도 제거하면 **v1.admission.autoscaling.openshift.io** API 서비스에 연결할 수 없게 되었습니다. 이 상황은 다른 Operator 설치와 같은 다른 클러스터 기능에 영향을 미쳤습니다. 이번 릴리스에서는 Cluster Resource Override Operator를 삭제하면 **v1.admission.autoscaling.openshift.io** API 서비스도 제거됩니다. 결과적으로 설치 실패 없이 다른 Operator를 설치할 수 있습니다. (OCPBUGS-55355)

- 이전 버전에서는 Cluster Resource Override Operator를 OpenShift Container Platform 4.16에서 4.17으로 업그레이드하려고 하면 Cluster Resource Override webhook가 작동하지 않았습니다. 이로 인해 Cluster Resource Override가 활성화된 네임스페이스에 Pod가 생성되지 않았습니다. 이번 릴리스에서는 오래된 보안이 삭제되어 OpenShift Container Platform에서 업그레이드 작업 중에 올바른 매개변수 및 값으로 시크릿을 다시 생성합니다. 결과적으로 Operator 업그레이드가 성공하고 Cluster Resource Override가 활성화된 네임스페이스에서 Pod를 생성할 수 있습니다. (OCPBUGS-55239)

- 이전에는 지원 설치 프로그램이 파이버 채널 다중 경로 볼륨 검색 중에 WWN(World Wide Name) 세부 정보를 탐지하지 못했습니다. 결과적으로 파이버 채널 다중 경로 디스크를 WWN 루트 장치와 일치시킬 수 없었습니다. 즉, **wwn** 루트 장치 힌트를 지정하면 팁이 모든 파이버 채널 다중 경로 디스크를 제외했습니다. 이번 릴리스에서는 지원 설치 프로그램이 파이버 채널 다중 경로 디스크 검색 중에 WWN 세부 정보를 감지합니다. 여러 파이버 채널 다중 경로 디스크가 있는 경우 이제 **wwn** 루트 장치 힌트를 사용하여 클러스터의 기본 디스크를 선택할 수 있습니다. (OCPBUGS-55184)

- 이전에는 서비스 종속성이 누락되어 **nmstate** 를 사용하여 **br-ex** 브릿지를 관리할 때 **mtu-migration** 서비스가 제대로 작동하지 않았습니다. 이번 릴리스에서는 마이그레이션 프로세스가 시작되기 전에 **nmstate** 를 사용하여 **br-ex** 를 관리하는 네트워크 구성이 올바르게 배포되도록 서비스 종속성이 추가되었습니다. (OCPBUGS-54830)

1.9.19.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.20. RHSA-2025:4204 - OpenShift Container Platform 4.17.27 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 5월 6일

OpenShift Container Platform 릴리스 4.17.27이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:4204 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:4206 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.27 --pullspecs
```

1.9.20.1. 확인된 문제

- 마스터 클럭 (T-GM)이 Locked 상태로 너무 빨리 전환되는 알려진 문제가 있습니다. 이는 Digital Phase-Locked Cryostat (DPLL)가 **Locked-HO-Acquired** 상태로의 전환을 완료하고 GNSS(Global Navigation Satellite Systems) 시간 소스 복원 후에 수행됩니다. (**OCPBUGS-54534**)

1.9.20.2. 버그 수정

- 이전 버전에서는 로드 밸런서를 선택할 때 설치 프로그램은 고정 인터넷 프로토콜 (IP) 주소 (**10.0.0.100**)를 선택하고 IP가 머신 네트워크 또는 가상 네트워크의 범위를 벗어나는 경우에도 로드 밸런서에 주소를 연결했습니다. 이번 릴리스에서는 설치 프로그램에서 제공된 컨트롤 플레인 서브넷 또는 머신 네트워크에서 사용 가능한 IP를 확인하고 기본 IP가 범위 내에 없는 경우 예약되지 않은 IP를 선택합니다. (OCPBUGS-55224)

- 이전 버전에서는 스크랩에 실패한 경우 Prometheus는 다음 스크랩의 샘플을 중복으로 잘못 간주하여 삭제했습니다. 이 문제는 실패 후 즉시 스크랩에 영향을 준 반면 후속 스크랩은 올바르게 처리되었습니다. 이번 릴리스에서는 실패 후 스크랩이 올바르게 처리되어 유효한 샘플이 실수로 삭제되지 않습니다. (OCPBUGS-54941)

- 이전에는 **IngressWithoutClassName** 경고가 있는 Ingress 리소스의 경우 Ingress 컨트롤러에서 리소스 삭제와 함께 경고를 삭제하지 않았습니다. OpenShift Container Platform 웹 콘솔에 경고가 계속 표시됩니다. 이번 릴리스에서는 Ingress 컨트롤러가 컨트롤러가 Ingress 리소스를 삭제하기 전에 **openshift_ingress_to_route_controller_ingress_without_class_name** 지표를 **0** 으로 재설정하여 경고가 삭제되고 더 이상 웹 콘솔에 표시되지 않도록 합니다. (OCPBUGS-53077)

- 이전에는 클러스터 생성 중에 컨트롤 플레인 노드가 비정상으로 감지될 때 교체되었습니다. 이러한 교체로 인해 클러스터를 비활성화하여 클러스터가 생성되지 않습니다. 이번 수정을 통해 노드가 의도치 않게 교체되지 않아 컨트롤 플레인의 안정화와 클러스터가 성공적으로 생성됩니다. (OCPBUGS-52957)

- 이전에는 Pod가 삭제될 때 SR-IOV(Single Root I/O Virtualization) 가상 기능(VF)이 예기치 않은 값 변경 사항을 최대 전송 단위(MTU) 값으로 되돌리지 않았습니다. 이 문제는 Pod 내부의 애플리케이션에 MTU 값이 변경된 경우 발생했습니다. 결과적으로 Pod의 MTU 값도 변경되었습니다. 이번 릴리스에서는 SR-IOV CNI(Container Network Interface)가 예기치 않은 MTU 값 변경 사항을 원래 값으로 되돌려 이 문제가 더 이상 존재하지 않습니다. (OCPBUGS-54392)

1.9.20.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.21. RHSA-2025:4012 - OpenShift Container Platform 4.17.26 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 4월 24일

OpenShift Container Platform 릴리스 4.17.26이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:4012 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:4014 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.26 --pullspecs
```

1.9.21.1. 버그 수정

- 이전 버전에서는 **oauth** API 서버에서 관리하는 리소스에 대한 검증 Webhook를 생성하려고 하면 검증 웹 후크가 생성되지 않았습니다. 이 문제는 **oauth** API 서버 및 데이터 플레인과의 통신 문제로 인해 발생했습니다. 이번 릴리스에서는 oauth API 서버와 데이터 플레인 간의 통신을 연결하는

데 Konnectivity 프록시 사이드카가 추가되어 **oauth** API 서버에서 관리하는 리소스에 대한 검증 Webhook를 생성할 수 있습니다. (OCPBUGS-54841)

- 이전에는 연결된 NIC(네트워크 인터페이스 컨트롤러)가 **ProvisioningFailed** 상태에 있기 때문에 Microsoft Azure에서 실행된 클러스터의 VM(가상 머신)이 실패했습니다. 이번 릴리스에서는 Machine API 컨트롤러에서 NIC의 프로비저닝 상태를 확인하고 이 문제를 방지하기 위해 정기적으로 VM을 새로 고칩니다. (OCPBUGS-54393)

- 이전에는 불안정한 네트워크를 통해 Google Cloud 태그를 검색하거나 GCP 서버에 연결할 수 없는 경우 설치 프로그램이 오작동했습니다. 이번 릴리스에서는 문제가 해결되었습니다. (OCPBUGS-51210)

- 이전 버전에서는 클러스터에 설정된 MTU(최대 전송 단위) 값보다 큰 UDP(User Datagram Protocol) 패킷을 서비스를 사용하여 패킷의 끝점으로 보낼 수 없었습니다. 이번 릴리스에서는 패킷 크기와 관계없이 서비스 IP 주소 대신 Pod IP 주소가 사용되어 UDP 패킷을 엔드포인트로 보낼 수 있습니다. (OCPBUGS-50579)

1.9.21.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.22. RHSA-2025:3798 - OpenShift Container Platform 4.17.25 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 4월 16일

OpenShift Container Platform 릴리스 4.17.25가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:3798 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:3800 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.25 --pullspecs
```

1.9.22.1. 버그 수정

- 이전에는 /var/log의 호스트에서 컨테이너 로그를 볼 목적으로 **container_logreader_t** 의 SELinux 도메인을 사용하는 컨테이너에서 **/var/ log /containers** 하위 디렉터리의 로그에 액세스할 수 없었습니다. 이 문제는 심볼릭 링크가 누락되어 발생했습니다. 이번 릴리스에서는 컨테이너가 **/var/log/containers** 의 로그에 액세스할 수 있도록 **/var/log/containers** 에 대한 심볼릭 링크가 생성됩니다. (OCPBUGS-54343)

- 이전에는 머신 세트에서 머신이 실패할 때 클러스터 자동 스케일러가 스케일링을 중지했습니다. 이 상황은 클러스터 자동 스케일러가 실행 중이 아닌 다양한 단계에서 시스템을 계산하는 방식에서 부정확하기 때문에 발생했습니다. 이번 릴리스에서는 클러스터 자동 스케일러가 더 정확한 개수를 갖도록 부정확한 정보가 수정되었습니다. (OCPBUGS-54325)

- 이전에는 웹 콘솔의 개발자 화면의 **경고** 페이지가 Prometheus 테넌시 경로 쿼리를 중지했습니다. 이 문제로 인해 **경고 관리자 배너에서 음소거를 로드하는 동안 오류가** 페이지에 표시되었습니다. 이번 릴리스에서는 페이지가 Prometheus 테넌시 경로를 쿼리하고 페이지에서 개발자 화면 데이터 저장소에서 자동으로 경고 데이터를 검색하여 배너가 더 이상 페이지에 표시되지 않도록 합니다. (OCPBUGS-54211)

- 이전에는 컨테이너 런타임 구성에 대한 머신 구성이 누락되어 컨테이너 런타임 컨트롤러 실패로 인해 클러스터 업데이트 작업이 실패했습니다. 이번 릴리스에서는 클러스터 작업이 성공할 수 있도록 누락된 머신 구성이 무시됩니다. (OCPBUGS-52188)

1.9.22.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.23. RHSA-2025:3565 - OpenShift Container Platform 4.17.24 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 4월 9일

OpenShift Container Platform 릴리스 4.17.24가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:3565 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:3567 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.24 --pullspecs
```

1.9.23.1. 버그 수정

- 이전에는 IBM Cloud® Cloud Internet Services (CIS) 구현에 대한 업데이트는 업스트림 Terraform 플러그인에 영향을 미쳤습니다. IBM Cloud®에서 외부용 클러스터를 생성하려고 하면 오류가 발생했습니다. 이번 릴리스에서는 플러그인 문제 없이 OpenShift Container Platform에서 외부 클러스터를 생성할 수 있습니다. (OCPBUGS-54357)

- 이전에는 사용자가 연결 해제된 설정에서 에이전트 ISO 빌드를 시도하면 오류가 발생했습니다. 이번 릴리스에서는 오류 없이 설정이 완료됩니다. (OCPBUGS-53378)

- 이전에는 컨테이너 실행 중에 공유 라이브러리가 누락되어 RHEL 작업자 노드에서 **ovn-ipsec-host** Pod가 크래시 루프로 실패했습니다. 이번 릴리스에서는 오류 없이 **ovn-ipsec-host** Pod가 작업자 노드에서 성공적으로 시작됩니다. (OCPBUGS-52951)

- 이전 버전에서는 OLM(Operator Lifecycle Manager) CSV 주석에 예기치 않은 JSON 데이터가 포함되어 있었고 이로 인해 결과 값을 사용하려고 할 때 런타임 오류가 발생했습니다. 이번 릴리스에서는 사용하기 전에 OLM 주석의 JSON 값이 검증되고, 오류가 기록되고 주석에 예기치 않은 JSON이 수신되면 콘솔이 실패하지 않습니다. (OCPBUGS-51277)

1.9.23.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.24. RHSA-2025:3297 - OpenShift Container Platform 4.17.23 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 4월 3일

OpenShift Container Platform 릴리스 4.17.23이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:3297 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:3299 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.23 --pullspecs
```

1.9.24.1. 버그 수정

- 이전에는 Operator Marketplace 및 OLM(Operator Lifecycle Manager)에서 **pod-security.kubernetes.io/** 레이블의 이전 버전 v1.24를 사용했습니다. 이번 릴리스에서는 Operator Marketplace가 배포된 네임스페이스에서 이제 PSA(Pod Security Admission) 라벨을 **latest** 로 표시합니다. (OCPBUGS-53283)

- 이전에는 **openshift-install agent create pxe-files** 명령에서 **/tmp/agent** 에 임시 디렉터리를 생성했으며 명령이 명령 완료 시 이러한 디렉터리를 제거하지 않았습니다. 이번 릴리스에서는 명령이 완료되면 디렉터리를 제거하므로 디렉터리를 수동으로 삭제할 필요가 없습니다. (OCPBUGS-52961)

- 이전에는 웹 콘솔의 **관리자 화면** 의 **경고 세부 정보** 페이지에서 코드 마이그레이션 작업에서 외부 레이블을 올바르게 처리하지 못했습니다. 이러한 외부 레이블은 음소거된 경고 알림이 알림 벨 아이콘에 추가되지 않도록 하려면 필요합니다. **경고 세부 정보** 페이지가 외부 레이블을 올바르게 처리하지 않았기 때문에 알림 벨은 링크를 클릭했을 때 **일치하는 경고를 찾지 못한** 이러한 **경고 세부 정보** 페이지에 대한 링크를 제공했습니다. 이번 릴리스에서는 **경고 세부 정보** 페이지에서 외부 레이블을 허용하므로 알림 벨의 경고를 클릭하여 올바른 **경고 세부 정보** 페이지에 대한 링크를 클릭합니다. (OCPBUGS-51117)

- 이전 버전에서는 다음 **kubevirt** CR 구성이 포함된 클러스터를 생성할 때 **virt launcher 정책을 조정하지 못했습니다. <address_name>이 IPv4 또는 IPv6 주소의 오류 메시지인지 확인할 수** 없었습니다.

  ```
  # ...
  - service: APIServer
    servicePublishingStrategy:
      type: NodePort
      nodePort:
        address: <address_name>
        port: 305030
  # ...
  ```

  이 오류 메시지는 네트워크 정책이 VM(가상 머신) 네임스페이스에 올바르게 배포되지 않았기 때문에 생성되었습니다. 이번 릴리스에서는 네트워크 정책을 VM에 적절히 배포할 수 있도록 CR의 **nodePort.address** 구성에 호스트 이름 주소를 추가할 수 있습니다. (OCPBUGS-48439)

- 이전에는 SR-IOV가 IB(InfiniBand) 유형으로 구성된 경우 VF(가상 기능) 인터페이스에서 드라이버를 바인딩 해제하는 대신 SR-IOV(Single Root I/O Virtualization) 네트워크 구성 데몬에서 물리적 기능(PF) 인터페이스에서 네트워크 드라이버를 바인딩 해제했습니다. 이 바인딩 해제 워크플로우는 노드에서 IB 인터페이스를 제거했으며, 이로 인해 IB 인터페이스가 작동하지 않았습니다. 이번 릴리스에서는 SR-IOV 네트워크 구성 데몬에 대한 수정으로 VF 네트워크 인터페이스를 올바르게 바인딩 해제하면 IB 인터페이스가 계속 작동합니다. 또한 SR-IOV Network Operator는 IB 유형으로 SR-IOV를 구성할 때 PF 인터페이스 대신 VF 인터페이스의 네트워크 드라이버를 대상으로 합니다. (OCPBUGS-53254)

1.9.24.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.25. RHSA-2025:3059 - OpenShift Container Platform 4.17.22 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 3월 26일

OpenShift Container Platform 릴리스 4.17.22가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:3059 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2025:3061 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.22 --pullspecs
```

1.9.25.1. 버그 수정

- 이전 버전에서는 클러스터를 종료하는 동안 경쟁 조건으로 인해 배포가 재부팅 작업 중에 스테이징 위치로 이동하면 스테이지 **ostree** 배포가 완료되지 않았습니다. 이번 릴리스에서는 **ostree** 배포에서 경쟁 조건을 제거하여 재부팅 작업 중에도 스테이징된 배포를 완료할 수 있습니다. (OCPBUGS-53225)

1.9.25.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.26. RHSA-2025:2696 - OpenShift Container Platform 4.17.21 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 3월 19일

OpenShift Container Platform 릴리스 4.17.21이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:2696 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:2698 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.21 --pullspecs
```

1.9.26.1. 버그 수정

- 이전에는 **trusted-ca-bundle-managed** 구성 맵이 필수 구성 요소였습니다. 사용자 정의 PKI(Public Key Infrastructure)를 사용하려는 경우 OpenShift API 서버에서 **trusted-ca-bundle-managed** 구성 맵이 있어야 하므로 배포가 실패합니다. 이번 릴리스에서는 사용자 정의 PKI를 사

용할 때 **trusted-ca-bundle-managed** 구성 맵 없이 클러스터를 배포할 수 있습니다. (OCPBUGS-52657)

- 이전에는 모니터링과 관련된 특정 플래그가 설정되지 않은 한 웹 콘솔의 **Observe** 섹션에 플러그인에서 제공하는 항목이 표시되지 않았습니다. 그러나 이러한 플래그는 로깅, 분산 추적, 네트워크 관찰 기능 등과 같은 다른 플러그인에서 **Observe** 섹션에 항목을 추가하지 못했습니다. 이번 릴리스에서는 다른 플러그인이 **Observe** 섹션에 항목을 추가할 수 있도록 모니터링 플래그가 제거됩니다. (OCPBUGS-52205)

- 이전에는 사용자 정의 SCC(보안 컨텍스트 제약 조건)가 클러스터 버전 업그레이드를 수신하지 못하도록 Cluster Version Operator에서 생성한 Pod에 영향을 미쳤습니다. 이번 릴리스에서는 OpenShift Container Platform에서 기본 SCC를 각 Pod로 설정하여 생성된 모든 사용자 정의 SCC가 Pod에 영향을 미치지 않습니다. (OCPBUGS-50589)

- 이전에는 AWS 또는 Azure 플랫폼에서 ARM64 아키텍처로 **NodePool** 리소스를 생성할 수 없었습니다. 이 버그로 인해 베어 메탈 컴퓨팅 노드를 추가할 수 있는 유효성 검사 오류가 발생하고 **NodePool** 리소스를 생성할 때 CEL(Common Expression Language) 유효성 검사 블록이 발생했습니다. 이번 수정에서는 **self.platform.type** 섹션에 **None** 을 설정하여 AWS 또는 Azure 이외의 ARM64 아키텍처를 허용하도록 **NodePool** 사양 검증 규칙을 수정합니다. AWS 또는 Azure 베어 메탈 플랫폼에서 ARM64 아키텍처 사양을 사용하여 **NodePool** 을 생성할 수 있습니다. (OCPBUGS-46440)

- 이전에는 관련 데이터 이미지를 사용하여 베어 메탈 호스트를 삭제한 경우 데이터 이미지가 그대로 유지됩니다. 이번 릴리스에서는 문제가 해결되고 데이터 이미지가 예상대로 베어 메탈 호스트를 사용하여 삭제됩니다. (OCPBUGS-42387)

1.9.26.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.27. RHSA-2025:2445 - OpenShift Container Platform 4.17.20 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 3월 12일

OpenShift Container Platform 릴리스 4.17.20이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:2445 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:2447 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.20 --pullspecs
```

1.9.27.1. 버그 수정

- 이전에는 LSO(Local Storage Operator)가 PV(영구 볼륨) 생성 중에 기존 SCSI(Small Computer System Interface) 심볼릭 링크를 무시했습니다. 이번 릴리스에서는 PV를 생성할 때 새 심볼릭 링크를 찾기 전에 LSO에서 이러한 심볼릭 링크를 더 이상 수집하지 않습니다. (OCPBUGS-51291)

- 이전 버전에서는 OVN-Kubernetes 네트워크 플러그인과 Kubernetes-NMState Operator가 서로 상호 작용할 때 예기치 않은 연결 프로필이 디스크 스토리지에 지속되었습니다. 이러한 연결 프로필로 인해 다시 시작될 때 **ovs-configuration** 서비스가 실패하는 경우가 있었습니다. 이번 릴리스

에서는 **ovs-configuration** 이 시작되기 전에 불필요한 연결 프로필이 정리되어 이 문제가 더 이상 발생하지 않습니다. (OCPBUGS-52257)

- 이전 버전에서는 VMware vSphere vCenter 주소가 올바르지 않거나 누락된 경우 **vmware-vsphere-csi-driver-operator** CSI(Container Storage Interface) 드라이버가 패닉 모드였습니다. 이번 릴리스에서는 VMware vSphere vCenter 주소가 올바르지 않거나 누락된 경우 CSI 드라이버가 패닉 모드로 전환되지 않습니다. (OCPBUGS-52207)

- 이전에는 **ClusterVersion 에서 Completed 업데이트가 수신되지 않은 경우 클러스터 업데이트 중에 클러스터 설정** 페이지가 제대로 렌더링되지 않았습니다. 이번 릴리스에서는 **ClusterVersion 에 Completed 업데이트가 수신되지 않은 경우에도 클러스터 설정** 페이지가 올바르게 렌더링됩니다. (OCPBUGS-51292)

- 이전에는 **개발자** 화면의 **경고 규칙** 페이지에 있는 경고 링크에 잘못된 링크에 대한 외부 레이블이 포함되었습니다. 이는 **경고** 페이지의 URL이 외부 레이블을 예상하지 않았기 때문에 발생했습니다. 이번 릴리스에서는 경고 **규칙** 페이지의 경고 URL에 더 이상 외부 레이블이 추가되지 않으므로 경고 링크가 정확합니다. (OCPBUGS-51126)

- 이전 버전에서는 호스트 클러스터의 노드에서 실행된 **kubevirt-csi** Pod의 경우 VM이 재부팅된 후 호스팅된 클러스터의 PVC(영구 볼륨 클레임)가 VM에서 제거되었습니다. 그러나 **VolumeAttachment** 리소스가 제거되지 않아 PVC가 VM에 연결되어 있을 것으로 예상되므로 클러스터에 문제가 발생했습니다. 이번 릴리스에서는 VM이 재부팅된 후 클러스터 문제가 더 이상 발생하지 않도록 **VolumeAttachment** 리소스가 제거됩니다. (OCPBUGS-44623)

- 이전에는 provisioning 네트워크가 비활성화되었지만 **bootstrapProvisioningIP** 필드가 설정된 베어 메탈 구성에서 베어 메탈 프로비저닝 구성 요소를 시작할 수 없었습니다. 이러한 오류는 프로비저닝 프로세스에서 컨테이너 이미지를 가져오는 프로세스 중에 부트스트랩 VM에서 외부 네트워크 인터페이스를 재구성할 때 발생합니다. 이번 릴리스에서는 네트워크가 유휴 상태일 때만 인터페이스 재구성이 발생하여 다른 프로세스와 충돌하지 않도록 종속성이 추가됩니다. 결과적으로 **bootstrapProvisioningIP** 필드가 설정되고 provisioning 네트워크가 비활성화된 경우에도 베어 메탈 프로비저닝 구성 요소가 안정적으로 시작됩니다. (OCPBUGS-43528)

1.9.27.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.28. RHSA-2025:1912 - OpenShift Container Platform 4.17.19 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 3월 5일

OpenShift Container Platform 릴리스 4.17.19가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:1912 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2025:1914 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.19 --pullspecs
```

1.9.28.1. 버그 수정

- 이전에는 보안 프록시가 활성화된 상태에서 OpenShift 클러스터를 생성하고 인증서가 **configuration.proxy.trustCA** 에 설정된 경우 클러스터가 프로비저닝을 완료하지 못했습니다. 이번 릴리스에서는 **configuration.proxy.trustCA** 에 설정된 인증서로 보안 프록시가 활성화된 클러스터를 생성할 수 있습니다. 또한 수정으로 인해 **oauth** 가 관리 클러스터 프록시를 사용하여 Cloud API에 연결할 수 없는 문제가 발생하지 않습니다. (OCPBUGS-51098)

- 이전 버전에서는 IBM Power Virtual Server 클러스터에서 DHCP(Dynamic Host Configuration Protocol) 네트워크를 삭제한 경우에도 하위 리소스가 남아 있었습니다. 이번 릴리스에서는 DHCP 네트워크를 삭제할 때 삭제 작업을 계속하기 전에 하위 리소스가 삭제됩니다. (OCPBUGS-50967)

- 이전 버전에서는 작업자 노드가 클러스터에 참여하려고 하면 프로세스가 완료되기 전에 해당 노드가 재부팅되었습니다. 작업자 노드는 ndezvous 노드와 통신할 수 없기 때문에 설치에 실패했습니다. 이번 릴리스에서는 rendezvous 노드가 조기 재부팅되고 문제가 해결되었습니다. (OCPBUGS-50011)

- 이전에는 DNS 기반 송신 방화벽이 대문자로 DNS 이름을 포함하는 규칙 생성을 잘못 허용하지 않았습니다. 이번 릴리스에서는 문제가 해결되어 송신 방화벽이 대문자 DNS 이름으로 생성됩니다. (OCPBUGS-49961)

- 이전에는 모든 호스트 검증 상태 로그에서 등록된 첫 번째 호스트의 이름을 참조했습니다. 호스트 검증에 실패하면 문제가 있는 호스트를 결정할 수 없었습니다. 이번 릴리스에서는 각 로그 메시지에서 올바른 호스트가 식별되고 호스트 검증 로그가 호스트가 연결되는 방식을 올바르게 기록합니다. (OCPBUGS-44058)

- 이전 버전에서는 VMware vSphere vCenter 클러스터에 표준 포트 그룹이 정의되어 있지 않은 ESXi 호스트가 포함되어 있고 설치 프로그램에서 해당 호스트를 선택하려고 하면 가져오기에 실패하고 **장치 0에 대한 잘못된** 구성이 보고되었습니다. 이번 릴리스에서는 설치 프로그램에서 ESXi 호스트의 표준 포트 그룹이 정의되어 있는지 여부를 확인하고, 그렇지 않은 경우 정의된 표준 포트 그룹이 있는 ESXi 호스트를 찾을 때까지 계속 확인하거나, 찾을 수 없는 경우 오류 메시지를 보고합니다. (OCPBUGS-37945)

1.9.28.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.29. RHSA-2025:1703 - OpenShift Container Platform 4.17.18 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 2월 26일

OpenShift Container Platform 릴리스 4.17.18이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:1703 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:1706 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.18 --pullspecs
```

1.9.29.1. 버그 수정

- 이전에는 컨트롤 플레인 Operator에서 API 끝점 가용성을 확인할 때 설정된 PROXY 환경 변수를 준수하지 않았습니다. 이번 릴리스에서는 문제가 해결되었습니다. (OCPBUGS-50596)

- 이전에는 AWS 로컬 영역 또는 Wavelength 영역과 같이 에지 영역에 있는 기존 서브넷의 AWS(Amazon Web Services)에 클러스터를 설치할 때 에지 영역의 서브넷 리소스에서 **kubernetes.io/cluster/<InfraID>:shared** 태그가 누락되었습니다. 이번 릴리스에서는 **install-config.yaml** 구성 파일에 사용되는 모든 서브넷에 필수 태그가 있는지 확인합니다. (OCPBUGS-49975)

- 이전 버전에서는 잘못된 주소가 클러스터의 Kubernetes **EndpointSlice** 로 전달되었으며 이 문제로 인해 IPv6 연결이 끊긴 환경의 에이전트 기반 클러스터에 MetalLB Operator를 설치할 수 없었습니다. 이번 릴리스에서는 수정 사항이 주소 평가 방법을 수정합니다. 이제 Red Hat Marketplace Pod가 클러스터 API 서버에 성공적으로 연결할 수 있으므로 MetalLB Operator를 설치하고 IPv6 연결이 끊긴 환경에서 수신 트래픽을 처리할 수 있습니다. (OCPBUGS-46665)

- 이전에는 컨테이너 이미지 아키텍처를 검증하는 방법이 이미지 메타데이터 공급자를 거치지 않았습니다. 그 결과 이미지 덮어쓰기가 적용되지 않았습니다. 이번 릴리스에서는 다중 아키텍처 검증을 허용하도록 이미지 메타데이터 공급자의 메서드가 수정되었으며 해당 방법은 이미지 검증 단계를 위해 모든 구성 요소를 통해 전파되었습니다. 결과적으로 이 문제가 해결되었습니다. (OCPBUGS-46664)

1.9.29.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.30. RHSA-2025:1403 - OpenShift Container Platform 4.17.17 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 2월 18일

OpenShift Container Platform 릴리스 4.17.17이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:1403 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:1405 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.17 --pullspecs
```

1.9.30.1. 버그 수정

- 이전에는 가용성 세트 fault 도메인 수가 **2** 로 하드 코딩되었습니다. 이 값은 결함 도메인 수가 일반적으로 **2** 개 이상이지만 **centraluseuap** 및 **eastusstg** 리전에서 실패하므로 Microsoft Azure의 대부분의 리전에서 작동합니다. 이번 릴리스에서는 리전의 가용성 세트 내결함성 도메인 수가 동적으로 설정되어 이 문제가 더 이상 발생하지 않습니다. (OCPBUGS-50017)

- 이전에는 Google Cloud에 클러스터를 설치할 때 인스턴스에 IP 전달을 비활성화해야 하는 경우 클러스터 설치에 실패했습니다. 이번 릴리스에서는 클러스터 설치 문제가 더 이상 발생하지 않도록 모든 Google Cloud 머신에 대해 IP 전달이 비활성화됩니다. (OCPBUGS-49993)

- 이전에는 OpenShift Container Platform 내부 레지스트리에서 이러한 리전을 지원하지 않았기 때문에 **ap-southeast-5** 리전 또는 기타 리전의 AWS에 클러스터를 설치할 수 없었습니다. 이번 릴리스에서는 다음 리전을 포함하도록 내부 레지스트리가 업데이트되어 이 문제가 더 이상 발생하

지 않습니다.

- **ap-southeast-5**
- **ap-southeast-7**
- **ca-west-1**
- **il-central-1**
- **mx-central-1**
  (OCPBUGS-49695)

- 이전 버전에서는 송신 IPv6가 할당된 노드에서 Pod가 실행 중이면 Pod가 듀얼 스택 클러스터에서 Kubernetes 서비스와 통신할 수 없었습니다. 이로 인해 IP 제품군의 트래픽이 **egressIP** 오브젝트가 적용되지 않고 삭제되었습니다. 이번 릴리스에서는 송신 IP가 적용된 IP 제품군의 소스 네트워크 주소 변환(SNAT)만 삭제되어 트래픽이 삭제될 위험이 제거됩니다. (OCPBUGS-48828)

- 이전에는 호스팅된 컨트롤 플레인 CLI를 사용하여 연결이 끊긴 환경에서 클러스터를 생성하려고 하면 설치 명령이 실패했습니다. 명령을 호스팅하는 레지스트리에 문제가 있었습니다. 이번 릴리스에서는 명령 레지스트리에 대한 수정으로 호스팅된 컨트롤 플레인 CLI를 사용하여 연결이 끊긴 환경에서 클러스터를 생성할 수 있습니다. (OCPBUGS-48170)

1.9.30.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.31. RHSA-2025:1120 - OpenShift Container Platform 4.17.16 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 2월 11일

OpenShift Container Platform 릴리스 4.17.16이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:1120 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2025:1122 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.16 --pullspecs
```

1.9.31.1. 버그 수정

- 이전에는 Bare Metal Operator(BMO)에서 지원하지 않는 지능형 플랫폼 관리 인터페이스(IPMI)를 기반으로 하는 모든 베어 메탈 호스트(BMH)에 대한 **HostFirmwareComponents** 사용자 정의 리소스를 생성했습니다. 이번 릴리스에서는 **HostFirmwareComponents** 사용자 정의 리소스가 이를 지원하는 BMH에만 생성됩니다. (OCPBUGS-49701)

- 이전 버전에서는 소스 레지스트리에서 잘못된 하위 최하위 결과를 반환하면 매니페스트 목록을 가져오면 API가 충돌할 수 있었습니다. 이번 업데이트를 통해 API는 가져온 태그에 오류가 충돌하지 않고 오류를 플래그합니다. (OCPBUGS-49399)

- 이전에는 컨트롤 플레인의 **openshift-apiserver** 에서 사용하는 Konnectivity 프록시에서 컨트롤 플레인에서 클라우드 API 접미사가 있는 레지스트리 이름을 확인한 다음 데이터 플레인을 통해 액세스하려고 했습니다.
ROSA에서 비 회귀 기능을 사용한 호스팅 클러스터와 Amazon VPC(Virtual Private Cloud) 끝점을 통해 액세스할 수 있는 컨테이너 레지스트리가 생성되었지만 컨테이너 레지스트리를 사용하는 **이미지 스트림을** 확인하지 않았기 때문에 설치할 수 없었습니다. 이번 릴리스에서는 Konnectivity 프록시가 확인되고 경로 호스트 이름이 일관되게 유지됩니다. (OCPBUGS-46465)

- 이전에는 레지스트리에 액세스하는 데 신뢰 번들이 필요한 빌드를 실행한 경우 클러스터 프록시에 구성된 번들을 가져오지 않았습니다. 사용자 정의 신뢰 번들에 필요한 레지스트리를 참조하는 경우 빌드가 실패했습니다. 이번 릴리스에서는 프록시 구성에 지정된 신뢰 번들이 필요하며 문제가 해결되었습니다. (OCPBUGS-45268)

- 이전에는 호스팅된 컨트롤 플레인 CLI를 사용하여 호스팅된 컨트롤 플레인 클러스터를 생성하려고 하면 다중 아키텍처 이미지에서 릴리스 이미지 검사로 인해 설치에 실패했습니다. 이번 릴리스에서는 호스팅된 컨트롤 플레인 CLI 코드베이스에 대한 업데이트가 문제를 해결하여 다중 아키텍처 이미지를 확인할 때 릴리스 이미지 검사가 실패하지 않도록 합니다. (OCPBUGS-44927)

- 이전 버전에서는 설치 프로그램에서 로드 밸런서에 지원되지 않는 보안 그룹을 추가했기 때문에 C2S(Commercial Cloud Services) 리전 또는 C2S(Secret Commercial Cloud Services) 리전에 AWS 클러스터를 설치할 수 없었습니다. 이번 릴리스에서는 설치 프로그램에서 C2S 리전 또는 SC2S 리전에 설치해야 하는 클러스터의 로드 밸런서에 지원되지 않는 보안 그룹을 더 이상 추가하지 않습니다. (OCPBUGS-42763)

1.9.31.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.32. RHSA-2025:0876 - OpenShift Container Platform 4.17.15 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 2월 5일

OpenShift Container Platform 릴리스 4.17.15가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:0876 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2025:0878 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.15 --pullspecs
```

1.9.32.1. 버그 수정

- 이전에는 설치 프로그램을 사용하여 Prism Central 환경에 클러스터를 설치할 때 RHCOS 이미지 시간 초과를 로드하는 **prism-api** 호출으로 인해 설치에 실패했습니다. 이 문제는 **prismAPICallTimeout** 매개변수가 **5** 분으로 설정되었기 때문에 발생했습니다. 이번 릴리스에서는 **install-config.yaml** 구성 파일의 **prismAPICallTimeout** 매개변수가 기본적으로 **10** 분으로 설정됩니다. **prism-api** 호출에 대한 시간 초과가 필요한 경우 매개변수를 구성할 수도 있습니다. (OCPBUGS-49362)

- 이전 버전에서는 서브크립션이 조정될 때마다 OLM 카탈로그 Operator에서 서브스크립션의 카탈로그 소스 Pod에서 카탈로그 메타데이터의 전체 보기를 요청했습니다. 이러한 요청으로 인해

카탈로그 Pod에 대한 성능 문제가 발생했습니다. 이번 릴리스에서는 OLM 카탈로그 Operator에서 주기적으로 새로 고쳐 모든 서브스크립션 조정에 의해 재사용되는 로컬 캐시를 사용하므로 카탈로그 Pod의 성능 문제가 더 이상 유지되지 않습니다. (OCPBUGS-48695)

- 이전 버전에서는 **ClusterResourceOverride** CR에 **forceSelinuxRelabel** 필드를 지정한 다음 이후 단계에서 CR을 수정한 경우 Cluster Resource Override Operator에서 관련 **ConfigMap** 리소스에 업데이트를 적용하지 않았습니다. 이 **ConfigMap** 리소스는 SELinux 레이블 재지정 기능인 **forceSelinuxRelabel** 에 중요합니다. 이번 릴리스에서는 Cluster Resource Override Operator가 적용되고 **ConfigMap** 리소스에 대한 **ClusterResourceOverride** CR 변경 사항을 추적합니다. (OCPBUGS-48691)

1.9.32.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.33. RHSA-2025:0654 - OpenShift Container Platform 4.17.14 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 1월 28일

OpenShift Container Platform 릴리스 4.17.14가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:0654 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2025:0656 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.14 --pullspecs
```

1.9.33.1. 버그 수정

- 이전에는 일부 클러스터 자동 스케일러 지표가 초기화되지 않았으며 사용할 수 없었습니다. 이번 릴리스에서는 클러스터 자동 스케일러 지표가 초기화되고 사용 가능합니다. (OCPBUGS-48606)

- 이전에는 노드 날짜 또는 시간이 부정확한 경우 **oc adm node-image create** 명령을 사용하여 새 작업자를 추가할 수 없었습니다. 이번 릴리스에서는 대상 클러스터 **machineconfig chrony** 리소스에 있는 동일한 NTP 구성을 노드 임시 라이브 환경에 적용하여 문제가 해결됩니다. (OCPBUGS-45344)

- 이전에는 리전의 모든 영역에 동일한 머신 유형 세트가 있는 것으로 간주되었기 때문에 영역에서 사용 가능한 모든 시스템 유형을 사용할 수 없었습니다. 이번 릴리스에서는 활성화된 모든 영역에서 모든 머신 유형을 사용할 수 있습니다. (OCPBUGS-46432)

- 이전에는 설치 프로그램이 PCI-DSS/BAFIN 규정을 준수하지 않았습니다. 이번 릴리스에서는 Microsoft Azure의 테넌트 간 복제가 비활성화되어 데이터 무단 액세스 가능성을 줄이고 데이터 거버넌스 정책을 엄격하게 준수할 수 있습니다. (OCPBUGS-48119)

- 이전에는 Red Hat Ansible Lightspeed 모달에 **don't show again** link를 클릭하면 다른 **User Preference 탭 중 하나가 열려 있을 때 올바른 일반**사용자 설정 탭이 표시되지 않았습니다. 이번 릴리스에서는 **don't show again** (다시 표시되지 않음) 링크를 클릭하면 올바른 **일반 사용자 설정** 탭으로 이동합니다. (OCPBUGS-48227)

- 이전에는 GCP(Google Cloud Platform) 서비스 계정이 생성되면 해당 계정을 항상 즉시 사용할

수 없었습니다. 업데이트에 계정을 사용할 수 없는 경우 계정에 권한을 추가할 때 설치 프로그램에서 오류가 발생했습니다. **Retry 실패한 요청에** 따라 서비스 계정이 생성될 수 있지만 최대 60초 동안 활성 상태가 아닙니다. 이번 릴리스에서는 서비스 계정이 지수 백오프에서 업데이트되어 계정을 올바르게 업데이트할 수 있는 충분한 시간을 제공합니다. (OCPBUGS-48359)

- 이전 버전에서는 RHEL 9 FIPS STIG 호환 머신에서 SHA-1 키로 인해 약한 키 사용 제한으로 인해 릴리스 서명 확인이 실패했습니다. 이번 릴리스에서는 릴리스 서명 확인을 위해 oc-mirror 플러그인에서 사용하는 키가 변경되고 릴리스 이미지는 이전 SHA-1 키와 다른 SHA256 trusted-key에서 서명합니다. (OCPBUGS-48363)

- 이전에는 OLM(Operator Lifecycle Manager)에서 클러스터에서 동일한 네임스페이스를 동시에 확인하는 경우가 있었습니다. 이로 인해 두 개의 동시 프로세스가 서브스크립션과 상호 작용하여 CSV 파일이 연결되지 않게 되었기 때문에 서브스크립션이 **ConstraintsNotSatisfiable** 터미널 상태에 도달했습니다. 이번 릴리스에서는 OLM에서 서브스크립션의 동시 네임스페이스를 확인할 수 있으므로 CSV가 연결되지 않은 상태로 유지됩니다. (OCPBUGS-45845)

1.9.33.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.34. RHSA-2025:0115 - OpenShift Container Platform 4.17.12 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 1월 14일

OpenShift Container Platform 릴리스 4.17.12가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2025:0115 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:0118 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.12 --pullspecs
```

1.9.34.1. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.35. RHBA-2025:0023 - OpenShift Container Platform 4.17.11 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 1월 8일

OpenShift Container Platform 릴리스 4.17.11이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2025:0023 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2025:0026 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.11 --pullspecs
```

1.9.35.1. 기능 개선

1.9.35.1.1. 워크로드 ID를 지원하는 GCP 파일 저장소 사용 가능

GCP(Google Compute Platform) 파일 저장소 CSI(Container Storage Interface) 스토리지는 워크로드 ID를 지원합니다. 이를 통해 사용자는 서비스 계정 키 대신 페더레이션 ID를 사용하여 Google Cloud 리소스에 액세스할 수 있습니다. 이 기능은 일반적으로 사용할 수 있습니다.

자세한 내용은 Google Compute Platform Filestore CSI Driver Operator 에서 참조하십시오.

1.9.35.2. 버그 수정

- 이전에는 CSR(인증서 서명 요청) 승인자가 시스템이 과부하될 때 인증서 승인을 중지해야 하는 경우 계산할 때 다른 시스템의 인증서를 포함했습니다. 다른 하위 시스템에서 CSR을 사용하는 대규모 클러스터에서 CSR 승인자는 승인되지 않은 CSR이 많으며 추가 승인을 방지했습니다. 이번 릴리스에서는 CSR 승인자가 관찰하는 **signerName** 값에 대한 CSR이 많이 있지만 승인할 수 없는 경우 새 승인을 방지합니다. CSR 승인자에는 이제 **signerName** 속성을 필터로 사용하여 승인할 수 있는 CSR만 포함됩니다. (OCPBUGS-46429)

- 이전 버전에서는 노드에서 Pod를 하드 제거로 인해 kubelet에 의해 Pod를 종료 및 삭제하는 대신 Pod가 종료 유예 기간이 표시되었습니다. 종료 유예 기간을 입력하는 각 Pod는 노드 리소스가 소모됩니다. 이번 릴리스에서는 버그 수정을 통해 Pod가 1초의 종료 유예 기간을 입력하여 kubelet을 종료한 다음 Pod를 삭제할 수 있습니다. (OCPBUGS-46364)

- 이전에는 **PublicIpv4Pool** 기능을 사용하면 권한 **ec2:AllocateAddress** 및 **ec2:AssociateAddress** 가 검증되지 않아 설치 중에 권한 오류가 발생했습니다. 이번 릴리스에서는 클러스터를 설치하기 전에 필요한 권한을 검증합니다. (OCPBUGS-46360)

- 이전에는 성능 프로필에 설정된 CPU에 대해 잘못된 문자열을 입력하여 클러스터가 손상될 수 있었습니다. 이번 릴리스에서는 유효한 문자열만 입력할 수 있으므로 클러스터 중단 위험이 제거됩니다. (OCPBUGS-45964)

- 이전에는 특정 시나리오에서 정보 표시기 조사 스트림에 의해 이벤트가 누락되었습니다. 이 연결이 끊어진 동안 개체가 삭제된 경우 정보가 예기치 않은 유형을 반환하여 오래된 상태가 발생했습니다. 결과적으로 잘못된 반환 유형으로 인해 문제가 발생했습니다. 이번 릴리스에서는 예기치 않은 유형이 올바르게 처리되고 일시적인 연결 해제 가능성이 성공적으로 수행됩니다. (OCPBUGS-46039)

1.9.35.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.36. RHBA-2024:11522 - OpenShift Container Platform 4.17.10 버그 수정 및 보안 업데이트 권고

출시 날짜: 2025년 1월 2일

OpenShift Container Platform 릴리스 4.17.10이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2024:11522 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:11525 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.10 --pullspecs
```

1.9.36.1. 기능 개선

1.9.36.1.1. Node Tuning Operator 아키텍처 탐지

Node Tuning Operator는 Intel 및 AMD CPU의 커널 인수 및 관리 옵션을 적절하게 선택할 수 있습니다. (OCPBUGS-43664)

1.9.36.2. 버그 수정

- 이전에는 웹 후크 토큰 인증기를 활성화하고 권한 부여 유형을 **None** 으로 설정하면 OpenShift Container Platform 웹 콘솔이 일관되게 충돌했습니다. 이번 릴리스에서는 버그 수정을 통해 이 구성으로 인해 OpenShift Container Platform 웹 콘솔이 충돌하지 않도록 합니다. (OCPBUGS-46390)

- 이전 버전에서는 클러스터에 대한 수신 규칙 및 sevices를 구성하는 **SiteConfig** CR(사용자 정의 리소스) 구성으로 **BareMetalHost** CR이 클러스터 정리 작업의 일부로 삭제되지 않고 삭제된 상태로 유지되었습니다. 이번 릴리스에서는 GitOps Operator를 버전 1.13 이상 버전으로 업데이트해도 이 문제가 더 이상 발생하지 않습니다. (OCPBUGS-46071)

- 이전 버전에서는 OLM(Operator Lifecycle Manager)을 사용하여 Operator를 업그레이드하려고 하면 업그레이드가 차단되었으며 **새 CRD의 스키마 메시지에 대한 기존 CR을 검증하는 동안 오류가 발생했습니다**. OLM에 문제가 있었습니다. 여기서 OLM은 새 Operator 버전의 CRD(사용자 정의 리소스 정의)에 대해 기존 CR(사용자 정의 리소스)을 검증하는 데 문제가 발생했습니다. 이번 릴리스에서는 Operator 업그레이드가 더 이상 차단되지 않도록 검증이 수정되었습니다. (OCPBUGS-46054)

- 이전에는 해결 프로그램을 사용한 **PipelineRuns** CR을 OpenShift Container Platform 웹 콘솔에서 재실행할 수 없었습니다. ro rerun the CR을 시도한 경우 **잘못된 PipelineRun 구성으로 Pipeline 메시지를 시작할 수 없었습니다**. 이번 릴리스에서는 이 문제가 발생하지 않고 해결자를 사용하는 **PipelineRuns** CR을 재실행할 수 있습니다. (OCPBUGS-45949)

- 이전 버전에서는 **양식 보기를** 사용하여 OpenShift Container Platform 웹 콘솔에서 **Deployment** 또는 **DeploymentConfig** API 오브젝트를 편집할 때 두 오브젝트의 YAML 구성에 **ImagePullSecrets** 매개변수가 있었습니다. 이번 릴리스에서는 중복 **ImagePullSecrets** 매개변수가 두 오브젝트에 대해 자동으로 추가되지 않도록 합니다. (OCPBUGS-45948)

- 이전에는 **aws-sdk-go-v2** 소프트웨어 개발 키트(SDK)가 AWS STS(Security Token Service) 클러스터에서 **AssumeRoleWithWebIdentity** API 작업을 인증하지 못했습니다. 이번 릴리스에서는 Pod ID Webhook에 이 문제가 더 이상 유지되지 않도록 기본 리전이 포함됩니다. (OCPBUGS-45938)

- 이전에는 **MachineSet** 오브젝트의 **publicIp** 매개변수가 **false** 로 설정된 경우 기존 서브넷의 특정 환경에서 AWS 클러스터를 설치하지 못했습니다. 이번 릴리스에서는 **공용Ip** 에 대해 설정된 구성 값이 더 이상 발생하지 않도록 합니다. 설치 프로그램에서 특정 환경에서 AWS 클러스터에 대한 시스템을 프로비저닝할 때 문제가 발생하지 않습니다. (OCPBUGS-45186)

- 이전에는 추가 필터링 속성이 **Operator 세부 정보** 페이지에서 피연산자를 나열하는 데 사용되는 구성 요소로 전달되었습니다. 추가 속성으로 인해 동적 플러그인에 의해 확장된 경우 목록이 항상

비어 있었습니다. 이번 릴리스에서는 사용 가능한 피연산자가 예상대로 나열되도록 추가 속성이 제거되었습니다. (OCPBUGS-45667)

- 이전 버전에서는 **oc adm node-image create** 명령을 실행할 때 명령이 실패하고 **이미지를 가져올 수 없는 경우가** 있었습니다. 이번 릴리스에서는 명령이 릴리스 워크로드에서 이미지를 가져오지 못하는 경우 명령이 예상대로 실행되도록 재시도 메커니즘을 명령에 추가합니다. (OCPBUGS-45517)

- 이전에는 설치 프로그램에서 **install-config.yaml** 구성 파일에 지정된 지정된 네트워크 유형을 사용하는 대신 임의의 네트워크 유형을 사용했기 때문에 IBM Power® Virtual Server 클러스터 설치에 설치 관리자가 프로비저닝한 인프라에서 실패했습니다. 이번 릴리스에서는 설치 프로그램에서 **install-config.yaml** 에 지정된 네트워크 유형을 사용하므로 이 문제가 더 이상 유지되지 않습니다. (OCPBUGS-45484)

- 이전에는 PPC(Performance Profile Creator)에서 논리 프로세서에 대해 다른 코어 ID 번호 지정(소켓당 코어)이 있고 노드가 동일한 노드 풀 아래에 있는 컴퓨팅 노드의 성능 프로필을 빌드하지 못했습니다. 예를 들어 PPC는 논리 프로세서 **2** 및 **18** 이 있는 두 개의 컴퓨팅 노드에서 실패했습니다. 여기서 한 노드는 코어 ID **2** 로 그룹화하고 다른 노드는 코어 ID **9** 로 그룹화합니다.
  이번 릴리스에서는 PPC에서 각각 논리 프로세서에 대해 서로 다른 코어 ID 번호가 있는 컴퓨팅 노드가 있는 클러스터에 대한 성능 프로필을 빌드할 수 있으므로 PPC에서 성능 프로필을 더 이상 생성하지 못합니다. 이제 PPC에서 생성된 성능 프로필을 신중하게 사용하도록 표시하는 경고 메시지를 출력합니다. 서로 다른 코어 ID 번호 지정에 시스템 최적화 및 격리된 작업에 영향을 줄 수 있기 때문입니다. (OCPBUGS-44644)

1.9.36.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.37. RHBA-2024:11010 - OpenShift Container Platform 4.17.9 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 12월 19일

OpenShift Container Platform 릴리스 4.17.9가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2024:11010 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:11013 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.9 --pullspecs
```

1.9.37.1. 확인된 문제

- NUMA Resources Operator를 배포하려면 OpenShift Container Platform 버전 4.17.7 또는 4.17.8을 사용하지 마십시오. (OCPBUGS-45639)

1.9.37.2. 버그 수정

- 이전에는 Google Cloud **Project Number 입력** 필드에 **GCP 풀 ID** 로 레이블이 잘못 지정되었습니다. 이번 릴리스에서는 Google Cloud **Project Number 입력** 필드에 올바르게 레이블이 지정됩니다. (OCPBUGS-46000)

- 이전에는 최대 대규모 삭제 제한이 10이었습니다. 이 제한으로 인해 **PreferNoSchedule** 테인트에 문제가 발생했습니다. 이번 릴리스에서는 최대 대규모 삭제 속도가 비활성화됩니다. (OCPBUGS-45929)

- 이전에는 사용자가 후행 기간이 포함된 사용자 정의 도메인 이름으로 설정된 Amazon Web Services DHCP 옵션을 구성하려고 했습니다. EC2 인스턴스의 호스트 이름이 Kubelet 노드 이름으로 변환되면 후행 기간이 제거되지 않았습니다. Kubernetes 오브젝트 이름에는 후행 기간이 허용되지 않습니다. 이번 릴리스에서는 DHCP 옵션 세트의 도메인 이름에 후행 기간이 허용됩니다. (OCPBUGS-45918)

- 이전에는 Performance Profile에 개별 CPU의 긴 문자열이 있는 경우 시스템 구성이 처리되지 않았습니다. 이번 릴리스에서는 커널 명령줄에서 일련의 숫자 또는 숫자 범위를 사용하도록 사용자 입력 프로세스가 업데이트되었습니다. (OCPBUGS-45627)

- 이전 버전에서는 릴리스 페이로드에서 이미지에 액세스하여 **oc adm node-image** 명령을 실행할 때 명령이 실패했습니다. 이번 릴리스에서는 이미지에 액세스할 때 임시 오류를 수정하기 위해 재시도 메커니즘이 추가되었습니다. (OCPBUGS-45517)

- 이전에는 s390x 하드웨어의 여러 이미지에 대해 FCP 또는 NVME 스토리지 장치를 사용하여 에이전트 기반 설치 관리자를 실행하는 동안 첫 번째 재부팅에 실패했습니다. 이번 릴리스에서는 이 문제가 해결되어 재부팅이 완료됩니다. (OCPBUGS-44904)

- 이전에는 사용자 정의 ID 및 액세스 관리(IAM) 프로필을 사용할 때 클러스터 deprovision이 실패했습니다. 이번 릴리스에서는 필수 권한 목록에 **tag:UntagResource** 가 포함되며 클러스터 프로비저닝이 완료됩니다. (OCPBUGS-44848)

- 이전에는 클러스터 작성자 계정에 프라이빗 DNS 호스팅 영역이 있는 공유 VPC를 사용하여 호스팅 클러스터를 생성할 때 프라이빗 링크 컨트롤러에서 로컬 영역에 **route53** DNS 레코드를 생성하지 못했습니다. 이번 릴리스에서는 Ingress 공유 역할이 개인 링크 컨트롤러에 레코드를 추가합니다. VPC 끝점은 VPC 소유자 계정에서 VPC 끝점을 생성하는 역할을 공유하는 데 사용됩니다. 호스팅 클러스터는 클러스터 작성자 계정에 개인 호스팅 영역이 있는 공유 VPC 구성에 생성됩니다. (OCPBUGS-44630)

- 이전에는 kdump 대상이 로컬 시스템에 액세스할 필요가 없는 원격 머신인 경우에도 로컬 암호화된 디스크를 열 때 **kdump initramfs** 에서 응답을 중지했습니다. 이번 릴리스에서는 이 문제가 해결되어 **kdump initranfs** 가 로컬 암호화된 디스크를 성공적으로 엽니다. (OCPBUGS-43079)

- 이전에는 CVO(Cluster Version Operator)에서 **ClusterVersion Failing 상태** 메시지에 지정된 내부 오류를 필터링하지 않았습니다. 그 결과 **ClusterVersion Failing 조건** 메시지에 대해 업데이트에 부정적인 영향을 미치지 않은 오류가 표시되었습니다. 이번 릴리스에서는 **ClusterVersion Failing 상태** 메시지에 전파되는 오류가 필터링됩니다. (OCPBUGS-39558)

1.9.37.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.38. RHSA-2024:10818 - OpenShift Container Platform 4.17.8 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 12월 11일

OpenShift Container Platform 릴리스 4.17.8이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:10818 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:10821 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.8 --pullspecs
```

1.9.38.1. 버그 수정

- 이전에는 **IBMPowerVSCluster** 오브젝트의 공급자 ID가 IBM Cloud Workspace ID를 부적절하게 검색했기 때문에 제대로 채워지지 않았습니다. 그 결과 호스트 클러스터에서 CSR(인증서 서명 요청)이 보류 중이었습니다. 이번 릴리스에서는 공급자 ID가 성공적으로 채워지고 문제가 해결되었습니다. (OCPBUGS-44880)

- 이전에는 finally 작업만 사용하여 파이프라인을 생성한 경우 편집 파이프라인 양식에서 finally 파이프라인 작업을 제거할 수 없었습니다. 이 변경으로 edit Pipeline 양식에서 finally 작업을 제거할 수 있으며 문제가 해결되었습니다. (OCPBUGS-44873)

- 이전 버전에서는 **oc adm node-image create** 명령을 사용한 후 이미지 생성 단계가 실패한 경우 간단한 오류를 보고하여 컨테이너의 로그를 표시하지 않았습니다. 결과적으로 오류 메시지에 이미지 생성 단계가 실패하는 기본 문제가 표시되지 않았습니다. 이번 릴리스에서는 **oc adm node-image create** 명령에서 컨테이너의 로그를 표시합니다. (OCPBUGS-44508)

- 이전 버전에서는 IBM Power®에 설치하려는 클러스터의 로드 밸런서를 생성하고 로드 밸런서를 생성한 경우 클러스터 설치에 실패하고 오류를 보고하지 않았습니다. 내부 및 외부 DNS 로드 밸런서 이름이 모두 생성되지 않았기 때문에 클러스터가 실패했습니다. 이번 릴리스에서는 클러스터 설치 중에 내부 및 외부 DNS 로드 밸런서 이름이 없는 경우 설치 프로그램에서 오류 알림을 생성하고 클러스터 설치 프로세스가 계속되도록 이름을 추가할 수 있습니다. (OCPBUGS-44247)

- 이전에는 대시보드 테이블의 행 수를 결정하는 데 사용된 ID가 고유하지 않았으며 ID가 동일한 경우 일부 행이 결합되었습니다. 이번 릴리스에서는 ID에서 추가 정보를 사용하여 중복 ID를 방지하고 테이블에서 예상되는 각 행을 표시할 수 있습니다. (OCPBUGS-43441)

1.9.38.2. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.39. RHSA-2024:10518 - OpenShift Container Platform 4.17.7 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 12월 3일

OpenShift Container Platform 릴리스 4.17.7이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:10518 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:10521 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.7 --pullspecs
```

1.9.39.1. 기능 개선

1.9.39.1.1. 더 이상 사용되지 않는 clusterTasks OpenShift Pipelines 버전 1.17

- OpenShift Container Platform 4.17 릴리스는 Red Hat OpenShift Pipelines 버전 1.17에서 **clusterTasks** 리소스를 더 이상 사용하지 않습니다. 이 릴리스에서는 OpenShift Container Platform 웹 콘솔의 OpenShift Pipelines 페이지에 있는 정적 플러그인에서 **clusterTasks** 리소스 종속성도 제거합니다. (OCPBUGS-44183)

1.9.39.2. 버그 수정

- 이전에는 개인 키와 같은 사용자 지정 템플릿에 여러 줄 매개변수를 입력할 수 없었습니다. 이번 릴리스에서는 템플릿 필드에 여러 줄 입력을 입력할 수 있도록 사용자 지정 템플릿에서 한 줄과 여러 줄 모드를 전환할 수 있습니다. (OCPBUGS-44699)

- 이전에는 CNO(Cluster Network Operator)를 사용하여 기존 **localnet** 네트워크가 있는 클러스터를 업그레이드하려고 하면 **ovnkube-control-plane** Pod가 실행되지 않았습니다. 이 문제는 **ovnkube-cluster-manager** 컨테이너에서 서브넷이 정의되지 않은 OVN-Kubernetes **localnet** 토폴로지 네트워크를 처리할 수 없기 때문에 발생했습니다. 이번 릴리스에서는 **ovnkube-cluster-manager** 컨테이너가 서브넷이 정의되지 않은 OVN-Kubernetes **localnet** 토폴로지 네트워크를 처리할 수 있도록 수정되어 있습니다. (OCPBUGS-43454)

- 이전 버전에서는 오브젝트의 **deploymentconfigs/scale** 하위 리소스에서 승인 Webhook를 사용하여 **DeploymentConfig** 오브젝트를 확장하려고 하면 **apiserver** 에서 요청을 처리하지 못했습니다. 이로 인해 **DeploymentConfig** 오브젝트를 확장할 수 없으므로 영향을 미쳤습니다. 이번 릴리스에서는 이 문제가 더 이상 발생하지 않도록 수정되어 있습니다. (OCPBUGS-42752)

1.9.39.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.40. RHBA-2024:10137 - OpenShift Container Platform 4.17.6 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 11월 26일

OpenShift Container Platform 릴리스 4.17.6이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2024:10137 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:10140 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.6 --pullspecs
```

1.9.40.1. 기능 개선

1.9.40.1.1. Kubernetes 버전 1.30.6으로 업데이트

OpenShift Container Platform 릴리스 4.17.6에는 업데이트에서 1.30.6으로의 변경 사항이 포함되어 있습니다. (OCPBUGS-44512)

1.9.40.2. 버그 수정

- 이전 버전에서는 CR(사용자 정의 리소스)에 사용자 정의 주석을 설정하면 SR-IOV Operator가 **SriovNetwork** CR의 모든 기본 주석을 덮어씁니다. 이번 릴리스에서는 CR에 사용자 정의 주석을 정의할 때 SR-IOV Operator가 기본 주석을 재정의하지 않습니다. (OCPBUGS-42252)

- 이전에는 알림에 외부 레이블이 포함되지 않았기 때문에 Red Hat OpenShift Container Platform 웹 콘솔 **알림** 섹션에서 알림 서랍에 음소거 경고가 표시되었습니다. 이번 릴리스에서는 알림 서랍에 음소거 경고가 표시되지 않도록 경고에 외부 라벨이 포함됩니다. (OCPBUGS-44722)

- 이전 버전에서는 Red Hat OpenShift Container Platform 웹 콘솔 **Edit BuildConfig** 페이지에서 **start lastrun** 옵션을 클릭하면 오류가 발생하여 **lastrun** 작업이 실행되지 않았습니다. 이번 릴리스에서는 업데이트를 통해 **start lastrun** 옵션이 예상대로 실행되도록 합니다. (OCPBUGS-44587)

- 이전에는 OpenShift Container Platform 4.17에서 Red Hat OpenShift Container Platform 웹 콘솔의 **관리자 관점에서 시작하기 섹션을** 축소하고 확장했습니다. 섹션을 축소하거나 확장하면 섹션을 닫을 수 없습니다. 이번 릴리스에서는 이제 **시작하기 섹션을** 닫을 수 있는 수정 사항을 확인할 수 있습니다. (OCPBUGS-44586)

- 이전에는 Red Hat OpenShift Container Platform 웹 콘솔의 **세부 정보** 페이지의 **MachineConfig** 탭에 선택 사항으로 표시된 데이터 필드가 포함되지 않은 경우 하나 이상의 **spec.config.storage.files** 에 오류가 표시되었습니다. 이번 업데이트를 통해 선택적 필드에 값을 입력하지 않으면 이 오류가 더 이상 표시되지 않도록 합니다. (OCPBUGS-44479)

- 이전에는 IBM® 플랫폼을 사용한 호스팅된 컨트롤 플레인 클러스터가 **oc login** 명령의 신뢰성을 허용하지 않았습니다. 이 동작으로 인해 브라우저가 클러스터에서 토큰을 가져올 수 없는 웹 브oswer에 오류가 발생했습니다. 이번 릴리스에서는 **oc login** 명령을 사용하여 인증이 예상대로 작동하도록 클라우드 기반 끝점이 프록시되지 않도록 합니다. (OCPBUGS-44276)

- 이전 버전에서는 **RendezvousIP** 가 컴퓨팅 노드 구성의 **next-hop-address** 필드에 있는 하위 문자열과 일치하는 경우 검증 오류가 발생했습니다. **RendezvousIP** 는 컨트롤 플레인 호스트 주소와 일치해야 합니다. 이번 릴리스에서는 **RendezvousIP** 에 대한 하위 문자열 비교가 컨트롤 플레인 호스트 주소에만 사용되어 오류가 더 이상 존재하지 않습니다. (OCPBUGS-44261)

- 이전 버전에서는 IBM Power®에 설치하려는 클러스터의 로드 밸런서를 생성하고 로드 밸런서를 생성할 때 클러스터 설치에 실패하고 오류를 보고하지 않았습니다. 내부 및 외부 DNS 로드 밸런서 이름이 모두 생성되지 않았기 때문에 클러스터가 실패했습니다. 이번 릴리스에서는 클러스터 설치 중에 내부 및 외부 DNS 로드 밸런서 이름이 없는 경우 설치 프로그램에서 오류를 출력하여 클러스터 설치 프로세스를 계속할 수 있도록 이름을 추가할 수 있습니다. (OCPBUGS-44247)

- 이전에는 씬 프로비저닝을 사용하는 물리적 스토리지 장치에서 디스크 정리 작업을 실행하려고 하면 정리 작업이 실패했습니다. 이번 릴리스에서는 버그 수정을 통해 정리 작업이 실패하지 않고 물리적 스토리지 장치에서 디스크 정리 작업을 실행할 수 있습니다. (OCPBUGS-31570)

- 이전에는 OLM(Operator Lifecycle Manager)이 서비스 계정과 연결된 보안에 액세스할 수 없는 경우 OLM에서 Kubernetes API 서버를 사용하여 전달자 토큰을 자동으로 생성했습니다. 이번 릴리스에서는 Kubernetes 버전 1.22 이상에서 전달자 토큰을 자동으로 생성하지 않습니다. 대신 OLM에서 **TokenRequest** API를 사용하여 새 Kubernetes API 토큰을 요청합니다. (OCPBUGS-44760)

1.9.40.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.41. RHSA-2024:9610 - OpenShift Container Platform 4.17.5 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 11월 19일

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.17.5를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:9610 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:9613 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.5 --pullspecs
```

1.9.41.1. 기능 개선

1.9.41.1.1. Cluster Monitoring Operator의 검증 기준 개선

- 이번 릴리스에서는 CCMO(Cluster Monitoring Operator)에서 검증 기준이 개선되었습니다. CMO는 지원되지 않는 필드 또는 잘못된 구성이 포함된 **openshift-monitoring/cluster-monitoring-config** 또는 **openshift-user-workload-monitoring/user-workload-monitoring-config** 에서 구성을 사용하여 클러스터 업데이트를 차단합니다. (OCPBUGS-43690)

1.9.41.2. 버그 수정

- 이전에는 Azure File Driver에서 기존 스토리지 계정을 재사용하려고 했습니다. 이번 릴리스에서는 Azure File Driver가 동적 프로비저닝 중에 스토리지 계정을 생성합니다. 업데이트된 클러스터의 경우 새로 생성된 영구 볼륨에서는 새 스토리지 계정을 사용합니다. 이전에 프로비저닝한 영구 볼륨은 클러스터 업데이트 전에 사용된 것과 동일한 스토리지 계정을 계속 사용합니다. (OCPBUGS-42949)

- 이전 버전에서는 **must-gather** 툴을 사용할 때 Multus CNI(Container Network Interface) 로그 파일인 **multus.log** 가 노드의 파일 시스템에 저장되었습니다. 이로 인해 도구가 노드에서 불필요한 디버그 Pod를 생성했습니다. 이번 릴리스에서는 Multus CNI에서 더 이상 **multus.log** 파일을 생성하지 않고 CNI 플러그인 패턴을 사용하여 **openshift-multus** 네임스페이스에서 Multus DaemonSet Pod의 로그를 검사합니다. (OCPBUGS-42835)

- 이전에는 파이프라인을 생성하려고 할 때 작업 데이터가 ArtifactHub에 완전히 로드되지 않았습니다. 이번 릴리스에서는 콘솔에서 ArtifactHub에서 데이터를 완전히 로드하고 문제가 해결되었습니다. (OCPBUGS-16141)

1.9.41.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.42. RHSA-2024:8981 - OpenShift Container Platform 4.17.4 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 11월 13일

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.17.4를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:8981 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:8984 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.4 --pullspecs
```

1.9.42.1. 기능 개선

1.9.42.1.1. GCP 워크로드 ID를 사용하여 고객 워크로드 인증

이번 릴리스에서는 Google Cloud Platform Workload Identity를 사용하는 OpenShift Container Platform 클러스터의 고객 워크로드의 애플리케이션은 GCP Workload Identity를 사용하여 인증할 수 있습니다.

애플리케이션과 함께 이 인증 방법을 사용하려면 클라우드 공급자 콘솔 및 OpenShift Container Platform 클러스터에서 구성 단계를 완료해야 합니다.

자세한 내용은 Google Cloud에서 애플리케이션에 대한 GCP 워크로드 ID 인증 구성 을 참조하십시오.

1.9.42.1.2. ansible-operator 업스트림 버전 정보

- 이제 **ansible-operator** 버전에 해당 업스트림 버전 정보가 표시됩니다. (OCPBUGS-43836)

1.9.42.2. 버그 수정

- 이전 버전에서는 IBM 플랫폼에 클러스터를 설치하고 기존 VPC를 클러스터에 추가할 때 Cluster API Provider IBM Cloud에서 VPC의 보안 그룹에 포트 443, 5000 및 6443을 추가하지 않았습니다. 이로 인해 VPC가 클러스터에 추가되지 않았습니다. 이번 릴리스에서는 Cluster API Provider IBM Cloud가 VPC의 보안 그룹에 포트를 추가하여 VPC가 클러스터에 추가되도록 합니다. (OCPBUGS-44226)

- 이전에는 설치 프로그램에서 VMware vSphere 컨트롤 플레인 머신 세트 CR(사용자 정의 리소스)의 **spec.template.spec.providerSpec.value** 섹션에 **network.devices**, **template**, **workspace** 필드를 입력했습니다. 이러한 필드는 vSphere 실패 도메인에서 설정되어야 하며 설치 프로그램은 이로 인해 의도하지 않은 동작이 발생했습니다.
  이러한 필드를 업데이트해도 컨트롤 플레인 시스템에 대한 업데이트가 트리거되지 않았으며 컨트롤 플레인 머신 세트가 삭제될 때 이러한 필드가 지워졌습니다. 이번 릴리스에서는 실패 도메인 구성에 포함된 값을 더 이상 채우지 않도록 설치 프로그램이 업데이트되었습니다. 이러한 값이 실패 도메인 구성에 정의되지 않은 경우 예를 들어 이전 버전에서 OpenShift Container Platform 4.17으로 업데이트되는 클러스터의 경우 설치 프로그램에서 정의한 값이 사용됩니다. (OCPBUGS-44047)

- 이전 버전에서는 Open vSwitch의 연결된 인터페이스에서 IPSec를 사용하여 ESP 하드웨어 오프로드를 활성화하면 Open vSwitch의 버그로 인해 연결이 중단되었습니다. 이번 릴리스에서는 OpenShift에서 Open vSwitch 연결 인터페이스에서 ESP 하드웨어 오프로드를 자동으로 비활성화하고 문제가 해결됩니다. (OCPBUGS-43917)

- 이전 버전에서는 OAuth CR(사용자 정의 리소스)의 ID 공급자(IDP) 이름을 공백을 포함하도록 구성한 경우 **oauth-server** 가 충돌했습니다. 이번 릴리스에서는 공백이 포함된 IDP(ID 공급자) 이름으로 인해 **oauth-server** 가 충돌하지 않습니다. (OCPBUGS-44118)

- 이전 버전에서는 Go 1.22의 동작 회귀로 인해 IDP 구성에 **htpasswd** 와 같은 여러 암호 기반 IDP

가 포함되어 있고 해당 이름 중 하나가 공백이 있는 경우 **oauth-server** Pod가 충돌했습니다. 부트스트랩 사용자 ,**kubeadmin** 이 여전히 클러스터에 존재하는 경우에도 사용자는 암호 기반 IDP로 간주됩니다. 이번 릴리스에서는 **oauth-server** 에 대한 수정으로 이 문제가 해결되어 서버가 충돌하지 않습니다. (OCPBUGS-43587)

- 이전에는 에이전트 기반 설치 관리자를 사용하여 잘못된 날짜가 있는 노드에 클러스터를 설치할 때 클러스터 설치에 실패했습니다. 이번 릴리스에서는 에이전트 기반 설치 관리자 라이브 ISO 시간 동기화에 패치가 적용됩니다. 추가 NTP(Network Time Protocol) 서버 목록으로 **/etc/chrony.conf** 파일을 구성하므로 클러스터 설치 문제가 발생하지 않고 **agent-config.yaml** 에서 이러한 추가 NTP 서버를 설정할 수 있습니다. (OCPBUGS-43846)

- 이전 버전에서는 Google Cloud에 프라이빗 클러스터를 설치할 때 API 방화벽 규칙이 **0.0.0.0/0** 의 소스 범위를 사용했습니다. 이 주소를 통해 개인 클러스터에 대한 의도하지 않은 액세스 권한이 없는 클러스터 리소스가 허용되었습니다. 이번 릴리스에서는 API 방화벽 규칙에서 머신 네트워크에 소스 범위가 있는 리소스만 프라이빗 클러스터에 액세스할 수 있습니다. (OCPBUGS-43786)

- 이전에는 유효하지 않거나 연결할 수 없는 IDP(ID 공급자)가 호스팅된 컨트롤 플레인에 대한 업데이트를 차단했습니다. 이번 릴리스에서는 **HostedCluster** 오브젝트의 **ValidIDPConfiguration** 조건이 IDP 오류를 보고하여 이러한 오류가 호스팅되는 컨트롤 플레인에 대한 업데이트를 차단하지 않습니다. (OCPBUGS-43746)

- 이전에는 프록시 를 통해 명령을 실행한 경우 , **oc exec**, **port-forward** 명령에서 오류가 발생했습니다. 이번 릴리스에서는 kubectl에 적용된 패치가 이러한 명령으로 모든 프록시 오류를 처리할 수 있도록 하여 명령이 예상대로 실행되도록 합니다. (OCPBUGS-43696)

- 이전에는 MCO(Machine Config Operator)에서 제공하는 RHEL(Red Hat Enterprise Linux) CoreOS 템플릿으로 인해 RHOSP(Red Hat OpenStack Platform)에서 노드 확장이 실패했습니다. 이 문제는 **systemd** 와 관련된 문제와 이전 버전의 OpenShift Container Platform의 레거시 부팅 이미지가 있기 때문에 발생했습니다. 이번 릴리스에서는 **systemd** 와 관련된 문제를 수정하고 레거시 부팅 이미지를 제거하여 노드 스케일링을 예상대로 계속할 수 있습니다. (OCPBUGS-42577)

- 이전 버전에서는 Pod가 동기화 작업을 초기화하는 동안 CVO(Cluster Version Operator) Pod가 재시작되면 차단된 업그레이드 요청의 가드가 실패했습니다. 그 결과 차단된 업그레이드 요청이 예기치 않게 수락되었습니다. 이번 릴리스에서는 CVO Pod가 초기화 중에 요청 조정을 연기하여 CVO Pod가 재시작된 후 차단된 업그레이드 요청을 보호합니다. (OCPBUGS-42386)

1.9.42.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.43. RHSA-2024:8434 - OpenShift Container Platform 4.17.3 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 10월 29일

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.17.3을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:8434 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:8437 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.3 --pullspecs
```

1.9.43.1. 기능 개선

1.9.43.1.1. Cluster Network Operator를 사용하여 네트워크 중복 메트릭 노출

- 제한된 실시간 마이그레이션 방법을 시작하고 네트워크 중복과 관련된 문제가 발생하면 CNO(Cluster Network Operator)에서 문제에 대한 네트워크 중복 메트릭을 노출할 수 있습니다. 이는 **openshift_network_operator_live_migration_blocked** 메트릭에 새 **NetworkOverlap** 레이블이 포함되어 있기 때문에 가능합니다. (OCPBUGS-39121)

1.9.43.1.2. 리포지토리에서 자동으로 git 리포지토리 환경 변수 로드

- 이전 버전에서는 서버리스 가져오기 전략을 사용하여 git 리포지토리를 가져올 때 **func.yaml** 파일의 환경 변수가 양식에 자동으로 로드되지 않았습니다. 이번 업데이트를 통해 이제 가져오기 시 환경 변수가 로드됩니다. (OCPBUGS-42474)

1.9.43.2. 버그 수정

- 이전에는 Power VS 배포 중에 OpenShift 설치 프로그램에 회귀가 도입되었습니다. 결과적으로 OpenShift 설치에 필요한 보안 그룹 규칙이 생성되지 않았습니다. 이번 릴리스에서는 문제가 해결되었습니다. (OCPBUGS-43547)

- 이전 버전에서는 이미지 레지스트리 Operator가 Azure에서 **Internal** 로 설정된 **networkAccess** 필드를 사용하여 구성한 경우 권한 부여 오류로 인해 이미지 레지스트리 Operator가 스토리지 컨테이너를 삭제하고 **managementState** 필드가 **Removed** 로 설정되지 않았습니다. 이번 릴리스에서는 Operator에서 스토리지 계정 및 스토리지 컨테이너를 삭제할 수 있으며 **managementState** 필드를 **Removed** 로 설정할 수 있습니다. (OCPBUGS-43350)

- 이전에는 활성 및 수동 HA(고가용성) 배포 둘 다 필요한 두 개 대신 세 개의 복제본을 실행했습니다. 결과적으로 컨트롤 플레인에는 필요 이상의 Pod가 포함되어 문제를 스케일링했습니다. 이번 릴리스에서는 활성 및 수동 HA 배포의 복제본 수가 3에서 2로 줄어듭니다. (OCPBUGS-42704)

- 이전에는 INI가 성공할 때 구성 로더가 **yaml** 이라는 오류를 기록했습니다. 이번 릴리스에서는 INI가 성공하면 unmarshal 오류가 더 이상 기록되지 않습니다. (OCPBUGS-42327)

- 이전에는 MCO(Machine Config Operator)의 vSphere **resolve-prepender** 스크립트에서 OpenShift Container Platform 4에서 사용된 이전 bootimage 버전과 호환되지 않는 **systemd** 지시문을 사용했습니다. 이번 릴리스에서는 최신 bootimage 버전 4.17 4.13 이상을 사용하여 수동 조작을 통해 또는 이 수정 사항이 포함된 릴리스로 업그레이드하여 노드를 확장할 수 있습니다. (OCPBUGS-42108)

- 이전에는 설치 프로그램에서 RHCOS(Red Hat Enterprise Linux CoreOS)에서 사용자 지정 IPv6 네트워크의 MTU(최대 전송 단위)의 유효성을 확인하지 않았습니다. MTU에 낮은 값을 지정한 경우 클러스터 설치에 실패합니다. 이번 릴리스에서는 IPv6 네트워크의 최소 MTU 값이 **1380** 으로 설정됩니다. 여기서 **1280** 은 IPv6의 최소 MTU이고 **100** 은 OVN-Kubernetes 캡슐화 오버헤드입니다. 이번 릴리스에서는 설치 프로그램이 RHCOS(Red Hat Enterprise Linux CoreOS)에서 사용자 지정 IPv6 네트워크의 MTU를 검증합니다. (OCPBUGS-41812)

- 이전에는 라이브 환경에서 RHCOS를 실행할 때 **rpm-ostree-fix-shadow-mode.service** 서비스가 실행되었습니다. 결과적으로 **rpm-ostree-fix-shadow-mode.service** 서비스는 배포 또는 라이브 시스템에 영향을 미치지 않는 실패를 기록했습니다. 이번 릴리스에서는 RHCOS가 설치된 환경에서 실행되지 않고 문제가 해결된 경우 **rpm-ostree-fix-shadow-mode.service** 서비스가 실행되지 않습니다. (OCPBUGS-41621)

1.9.43.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.44. RHSA-2024:8229 - OpenShift Container Platform 4.17.2 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 10월 23일

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.17.2를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:8229 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:8232 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.2 --pullspecs
```

1.9.44.1. 기능 개선

- Operator SDK는 **kube-rbac-proxy** 에 대한 Dockerfile을 올바르게 스캐폴드합니다. 또한 Operator SDK에서 **-rhel9** 컨테이너 이미지를 사용할 수 있습니다. (OCPBUGS-42953)

- 제한된 실시간 마이그레이션 방법을 시작하고 네트워크 중복과 관련된 문제가 발생하면 CNO(Cluster Network Operator)에서 문제에 대한 네트워크 중복 메트릭을 노출할 수 있습니다. 이는 **openshift_network_operator_live_migration_blocked** 메트릭에 새 **NetworkOverlap** 레이블이 포함되어 있기 때문에 가능합니다. (OCPBUGS-39121)

1.9.44.2. 버그 수정

- 이전에는 CSR의 노드 이름 및 내부 DNS 항목이 문자 차이와 일치하지 않아 CSR(인증서 서명 요청)에 대한 승인 메커니즘이 실패했습니다. 이번 릴리스에서는 CSR에 대한 승인 메커니즘을 업데이트하면 대소문자를 구분하는 검사를 건너뛰어 노드 이름과 내부 DNS 항목이 일치하는 CSR이 문자 케이스 차이로 인해 검사가 실패하지 않습니다. (OCPBUGS-43312)

- 이전에는 CCO(Cloud Credential Operator) 및 **assisted-service** 오브젝트에서 포트가 충돌하여 VMware vSphere의 클러스터 설치에 실패했습니다. 이번 릴리스에서는 설치 프로그램이 **지원-서비스** 오브젝트의 **pprof** 모듈을 무시하여 포트 충돌이 더 이상 존재하지 않습니다. (OCPBUGS-43069)

- 이전 버전에서는 **oc import-image** 명령을 사용하여 호스팅된 컨트롤 플레인 클러스터에서 이미지를 가져오려고 하면 개인 이미지 레지스트리의 액세스 문제로 인해 명령이 실패했습니다. 이번 릴리스에서는 호스팅된 컨트롤 플레인 클러스터의 **openshift-apiserver** pod로 업데이트하면 데이터 플레인을 사용하는 이름이 확인되어 **oc import-image** 명령이 이제 개인 이미지 레지스트리에서 예상대로 작동합니다. (OCPBUGS-43051)

- 이전에는 호스팅된 컨트롤 플레인의 관리 서비스의 경우 감사 로그가 로컬 웹 후크 서비스인 **audit-webhook** 로 전송되었습니다. 이로 인해 **konnectivity** 서비스를 통해 감사 로그를 보낸 호스트 컨트롤 플레인 Pod에 대한 문제가 발생했습니다. 이번 릴리스에서는 호스팅된 컨트롤 플레인 Pod가 **audit-webhook** 서비스에 auti 로그를 보낼 수 있도록 **audit-webhook** 호스트가 **no_proxy** 호스트 목록에 추가됩니다. (OCPBUGS-42974)

- 이전 버전에서는 에이전트 기반 설치 관리자를 사용하여 클러스터를 설치할 때 **assisted-installer-controller** 가 rendezvous 호스트에서 **assisted-service** 를 사용할 수 없는지 여부에 따라 설치 프로세스를 시간 초과했습니다. 이로 인해 CSR 승인 확인 중에 클러스터 설치가 실패했습니다. 이번 릴리스에서는 **assisted-installer-controller** 에 대한 업데이트를 통해 **assisted-service** 를 사용할 수 없는 경우 컨트롤러가 시간 초과되거나 종료되지 않습니다. CSR 승인 검사가 예상대로 작동합니다. (OCPBUGS-42839)

- 이전 버전에서는 **openshift-install gather bootstrap --dir <workdir> 명령을 실행하면 설치 프로그램에서** 수집된 로그 분석을 건너뛸 수 있었습니다. 이 명령은 다음 메시지를 출력합니다.

  > Invalid log bundle or the bootstrap machine could not be reached and bootstrap logs were not collected

  이번 릴리스에서는 설치 프로그램에서 **gather bootstrap --dir <workdir** > 인수가 생성되는 로그 처리를 분석할 수 있습니다. (OCPBUGS-42806)

- 이전 버전에서는 OpenShift Container Platform 웹 콘솔에서 사용자 정의 편집기와 함께 **개발자** 화면을 사용한 경우 **n** 키보드 바로 가기를 입력하면 네임스페이스 메뉴가 예기치 않게 열립니다. 이 문제는 키보드 바로 가기 키가 사용자 지정 편집기를 고려하지 않았기 때문에 발생했습니다. 이번 릴리스에서는 네임스페이스 메뉴가 사용자 정의 편집기를 차지하며 **n** 키보드 바로 가기를 입력하면 예기치 않게 열려 있지 않습니다. (OCPBUGS-42607)

- 이전에는 설치 프로그램에서 RHCOS(Red Hat Enterprise Linux CoreOS)에서 사용자 지정 IPv6 네트워크의 MTU(최대 전송 단위)의 유효성을 확인하지 않았습니다. MTU에 낮은 값을 지정한 경우 클러스터 설치에 실패합니다. 이번 릴리스에서는 IPv6 네트워크의 최소 MTU 값이 **1380** 으로 설정됩니다. 여기서 **1280** 은 IPv6의 최소 MTU이고 **100** 은 OVN-Kubernetes 캡슐화 오버헤드입니다. 이번 릴리스에서는 설치 프로그램이 RHCOS(Red Hat Enterprise Linux CoreOS) (OCPBUGS-41812)에서 사용자 지정 IPv6 네트워크의 MTU를 검증합니다 .

- 이전에는 릴리스 이미지를 미러링하는 데 사용되는 호스팅된 컨트롤 플레인 클러스터로 인해 기존 노드 풀이 **NodePool** 버전 대신 호스팅된 클러스터의 운영 체제 버전을 사용할 수 있었습니다. 이번 릴리스에서는 노드 풀이 자체 버전을 사용할 수 있도록 수정되어 있습니다. (OCPBUGS-41552)

- 이전에는 Microsoft Azure에서 프라이빗 OpenShift Container Platform 클러스터를 생성한 후 설치 프로그램에서 생성된 스토리지 계정을 프라이빗으로 표시하지 않았습니다. 결과적으로 스토리지 계정을 공개적으로 사용할 수 있었습니다. 이번 릴리스에서는 클러스터를 공개적으로 또는 비공개로 사용할 수 있는지에 관계없이 설치 프로그램이 항상 스토리지 계정을 비공개로 표시합니다. (OCPBUGS-42349)

1.9.44.3. 업데이트

OpenShift Container Platform 4.17 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.45. RHSA-2024:7922 - OpenShift Container Platform 4.17.1 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 10월 16일

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.17.1을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:7922 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:7925 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.1 --pullspecs
```

1.9.45.1. 기능 개선

- Operator SDK가 **ansible-operator** 에 대해 Dockerfile을 올바르게 스캐폴드합니다. 또한 Operator SDK에서 **-rhel9** 컨테이너 이미지를 사용할 수 있습니다. (OCPBUGS-42853)
- Operator SDK는 이제 **helm-operator** 에 대한 Dockerfile을 올바르게 스캐폴드합니다. 또한 Operator SDK에서 **-rhel9** 컨테이너 이미지를 사용할 수 있습니다. (OCPBUGS-42786)
- 개발자 프리뷰 기능인 Red Hat OpenShift Lightspeed를 설치하면 클러스터 내 모니터링 활성화 확인란이 기본적으로 활성화됩니다. (OCPBUGS-42380)
- 이제 설치 프로그램에서 Transit Gateway 수정 사항이 포함된 최신 버전의 **cluster-api-provider-ibmcloud** 공급자를 사용합니다. (OCPBUGS-42483)
- 개발자 프리뷰 기능인 CNS 볼륨 마이그레이션 기능에는 다음과 같은 향상된 기능이 포함되어 있습니다.
  - 이제 CNS 볼륨을 VMware vSphere로 이동하기 전에 vCenter 버전이 있는지 확인합니다. (OCPBUGS-42006)
  - 일부 볼륨이 없는 경우에도 CNS 볼륨을 계속 마이그레이션하여 볼륨이 없는 경우 마이그레이션 작업이 종료되지 않습니다. (OCPBUGS-42008)
- vSphere CSI Driver Operator는 클러스터에서 제거된 vSphere CSI 드라이버의 모든 리소스를 삭제할 수 있습니다. (OCPBUGS-42007)

1.9.45.2. 버그 수정

- 이전에는 SR-IOV(Single-Root I/O Virtualization) Operator가 Operator의 종료 작업 중에 획득된 리스를 만료하지 않았습니다. 이로 인해 새 인스턴스가 새 인스턴스가 작동하기 전에 리스가 만료될 때까지 기다려야 하므로 Operator의 새 인스턴스에 영향을 미쳤습니다. 이번 릴리스에서는 Operator 종료 논리를 업데이트하면 Operator가 종료될 때 Operator가 리스를 만료할 수 있습니다. (OCPBUGS-37668)
- 이전 버전에서는 클러스터 리소스 그룹이 아닌 리소스 그룹에 있는 Microsoft Azure 스토리지 계정을 사용하도록 이미지 레지스트리를 구성하면 Image Registry Operator의 성능이 저하되었습니다. 이는 검증 오류로 인해 발생했습니다. 이번 릴리스에서는 Operator를 업데이트하면 스토리지 계정 키를 사용하여 인증만 허용합니다. 다른 인증 요구 사항을 검증할 필요는 없습니다. (OCPBUGS-42812)
- 이전 버전에서는 **install-config.yaml** 구성 파일의 가용성 영역이 특정 순서로 지정되지 않은 경우 컨트롤 플레인 머신 세트 매니페스트를 저장하기 전에 설치 프로그램에서 영역을 잘못 정렬했습니다. 프로그램에서 시스템을 생성할 때 각 영역에 머신을 조정하기 위해 추가 컨트롤 플레인 가상 머신이 생성되었습니다. 이로 인해 resource-constraint 문제가 발생했습니다. 이번 릴리스에서는 설치 프로그램이 더 이상 가용성 영역을 정렬하지 않으므로 이 문제가 더 이상 발생하지 않습니다. (OCPBUGS-42699)
- 이전에는 Red Hat OpenShift Container Platform 웹 콘솔에 필수 필드로 **Creator** 필드가 필요하지 않았습니다. API 변경은 이 필드에 빈 값을 지정했지만 사용자 프로필은 계속 자동으로 경고를 생성할 수 있습니다. 이번 릴리스에서는 API에서 **Creator** 필드를 사용자 프로필의 필수 필드로 표시합니다. (OCPBUGS-42606)

- 이전에는 루트 인증 교체 중에 Ingress Operator 및 DNS Operator를 시작하지 못했습니다. 이번 릴리스에서는 Ingress Operator 및 DNS Operator의 kubeconfigs를 업데이트하면 주석이 PKI(공개 키 인프라)를 관리하기 위한 조건을 설정해야 합니다. 이번 업데이트를 통해 루트 인증 교체 중에 두 Operator가 모두 예상대로 시작할 수 있습니다. (OCPBUGS-42261)

- 이전에는 루트 인증 교체 중에 데이터 플레인의 **metrics-server** Pod가 올바르게 시작되지 않았습니다. 이 문제는 인증서 문제로 인해 발생했습니다. 이번 릴리스에서는 **hostedClusterConfigOperator** 리소스가 데이터 플레인으로 올바른 인증서를 전송하여 **metrics-server** Pod가 예상대로 시작됩니다. (OCPBUGS-42098)

- 이전에는 설치 프로그램에서 Google Cloud 공유 VPC(Virtual Private Network)에 설치해야 하는 클러스터의 프라이빗 영역을 생성하려고 했습니다. 이로 인해 클러스터 설치에 실패했습니다. 이번 릴리스에서는 이 클러스터 설치 문제가 더 이상 존재하지 않도록 수정으로 프라이빗 영역 생성을 건너뜁니다. (OCPBUGS-42142)

- 이전 버전에서는 설치 프로그램이 Google Cloud VPC에 클러스터를 설치할 때 컨트롤 플레인 서비스 계정에 대한 역할 바인딩이 프로그램에서 제거되지 않았습니다. 이번 릴리스에서는 클러스터에 이러한 아티팩트가 더 이상 포함되지 않도록 수정으로 역할 바인딩이 제거됩니다. (OCPBUGS-42116)

- 이전 버전에서는 클러스터에 대해 클러스터의 온-클러스터 계층 지정을 활성화하고 머신 구성에서 커널 매개 변수를 구성하려고 하면 MCP(머신 구성 풀) 및 노드가 성능이 저하된 상태가 되었습니다. 이는 구성이 일치하지 않기 때문에 발생했습니다. 이번 릴리스에서는 OCL이 활성화된 클러스터의 커널 인수를 점검하면 인수가 구성되고 클러스터의 노드에 적용할 수 있습니다. 이번 업데이트에서는 머신 구성과 노드 구성 간에 이전에 발생한 항목이 일치하지 않습니다. (OCPBUGS-42081)

- 이전에는 클러스터의 Pod를 생성하기 위해 cron 작업을 생성하면 Pod를 가져오는 구성 요소가 실패했습니다. 이 문제로 인해 OpenShift Container Platform 웹 콘솔의 **토폴로지** 페이지가 실패했습니다. 이번 릴리스에서는 이 문제가 더 이상 존재하지 않도록 cron 작업에서 생성된 Pod를 가져오는 구성 요소에 대해 **3** 초 지연이 구성됩니다. (OCPBUGS-41685)

- 이전 버전에서는 RHOSP에 구성된 **TechPreviewNoUpgrade** 기능 게이트를 나열한 OpenShift Container Platform 클러스터를 배포할 때 **cluster-capi-operator** Pod가 충돌했습니다. 이는 Cluster CAPI Operator가 제공된 API와 다른 API 버전을 예상했기 때문에 발생했습니다. 이번 릴리스에서는 Cluster CAPI Operator를 업데이트하면 Operator에서 올바른 버전의 API를 사용하므로 이 문제가 더 이상 발생하지 않습니다. (OCPBUGS-41576)

- 이전 버전에서는 DNF를 사용하여 사용자 지정된 RHCOS(Red Hat Enterprise Linux CoreOS) 빌드에 추가 패키지를 설치하면 패키지를 찾을 수 없기 때문에 빌드가 실패했습니다. 이번 릴리스에서는 서브스크립션 관리자가 올바른 패키지를 RHCOS에 추가하여 이 문제가 더 이상 발생하지 않습니다. (OCPBUGS-41376)

- Previosuly, **active-backup** 모드에서 설정된 본딩에는 기본 링크가 ESP 오프로드를 지원하지 않는 경우에도 ESP(EFI 시스템 파티션) 오프로드가 활성화되어 있습니다. 이로 인해 IPsec 연결이 실패했습니다. 이번 릴리스에서는 IPsec 연결이 전달되도록 본딩에 대해 ESP 오프로드가 비활성화됩니다. (OCPBUGS-41255)

- 계정을 삭제할 때 새 사용자 계정의 리소스가 제거되지 않았습니다. 이로 인해 구성 맵, 역할 및 role-bindings에 불필요한 정보가 발생했습니다. 이번 릴리스에서는 **ownerRef** 태그가 이러한 리소스에 추가되어 사용자 계정을 삭제할 때 리소스가 모든 클러스터 리소스에서도 삭제됩니다. (OCPBUGS-39601)

- Previosuly, 코딩 문제로 인해 RHCOS 사용자 프로비저닝 설치 인프라에서 Ansible 스크립트가 실패했습니다. 이 문제는 3 노드 클러스터에 IPv6를 활성화할 때 발생했습니다. 이번 릴리스에서는 RHCOS에서 IPv6가 활성화된 3-노드 클러스터를 설치할 수 있는 지원이 있습니다. (OCPBUGS-

39409)

- 이전에는 **metadata.json** 파일이 생성되기 전에 실행하도록 Ansible 플레이북의 순서가 수정되어 이전 버전의 Ansible에 문제가 발생했습니다. 이번 릴리스에서는 플레이북이 누락된 파일을 더 용인하고 문제가 해결되었습니다. (OCPBUGS-39286)

- 이전에는 NTO(Node Tuning Operator)가 **PerformanceProfiles** 를 사용하도록 구성된 경우 NTO에서 **ocp-tuned-one-shot systemd** 서비스를 생성했습니다. **systemd** 서비스는 kubelet 전에 실행되고 실행을 차단했습니다. **systemd** 서비스는 NTO 이미지를 사용하는 Podman을 호출하지만 NTO 이미지에 여전히 Podman이 없는 경우 이미지를 가져오려고 하면 실패합니다. 이번 릴리스에서는 **/etc/mco/proxy.env** 에 정의된 클러스터 전체 프록시 환경 변수에 대한 지원이 추가되었습니다. 이제 Podman은 클러스터 외부 연결에 프록시를 사용해야 하는 환경에서 NTO 이미지를 가져옵니다. (OCPBUGS-39124)

- 이전 버전에서는 OpenShift Container Platform 웹 콘솔의 **이벤트** 페이지에 대한 리소스 유형 필터에서 세 개 이상의 리소스를 선택할 때 리소스 수를 잘못 보고했습니다. 이번 릴리스에서는 필터에서 리소스 선택에 따라 올바른 리소스 수를 보고합니다. (OCPBUGS-39091)

- 이전에는 블록 장치의 일련 번호에 특수하거나 유효하지 않은 문자가 있는 경우 Ironic 검사에 실패했습니다. 이 문제는 **lsblk** 명령이 문자를 이스케이프하지 못했기 때문에 발생했습니다. 이번 릴리스에서는 이제 명령에서 문자를 이스케이프하므로 이 문제가 더 이상 유지되지 않습니다. (OCPBUGS-39013)

- 이전에는 Redfish 가상 미디어를 사용하여 xFusion 베어 메탈 노드를 클러스터에 추가할 때 노드 등록 문제로 인해 노드가 추가되지 않았습니다. 하드웨어가 Redfish와 호환되지 않아 문제가 발생했습니다. 이번 릴리스에서는 xFusion 베어 메탈 노드를 클러스터에 추가할 수 있습니다. (OCPBUGS-38784)

- 이전 버전에서는 OpenShift Container Platform 웹 콘솔의 **개발자** 화면에 **Observe** > **Metrics** 로 이동할 때 두 개의 **Metrics** 탭이 있었습니다. 이번 릴리스에서는 중복 탭이 제거되고 이제 웹 콘솔의 **Metrics** 탭을 제공하는 **openshift-monitoring/monitoring-plugin** 애플리케이션에 존재합니다. (OCPBUGS-38462)

- 이전에는 구성 문제로 인해 **manila-csi-driver** 및 노드 등록 기관 Pod에 상태 점검이 누락되었습니다. 이번 릴리스에서는 이제 두 리소스 모두에 상태 점검이 추가됩니다. (OCPBUGS-38457)

- 이전에는 호스팅된 컨트롤 플레인 클러스터 구성에서 **additionalTrustBundle** 매개변수를 업데이트해도 컴퓨팅 노드에 적용되지 않았습니다. 이번 릴리스에서는 **additionalTrustBundle** 매개변수에 대한 업데이트가 호스팅된 컨트롤 플레인 클러스터에 있는 컴퓨팅 노드에 자동으로 적용되도록 합니다. (OCPBUGS-36680)

- 이전 버전에서는 oc-mirror 플러그인 v2 (기술 프리뷰)에서 **태그** 및 **다이제스트** 참조를 모두 참조하는 이미지가 지원되지 않았습니다. 완전히 연결이 끊긴 환경의 disk-to-mirror 프로세스 중에 이미지를 건너뛰고 이로 인해 아카이브 파일에 대한 빌드 문제가 발생했습니다. 이번 릴리스에서는 oc-mirror 플러그인 v2에서 이러한 참조가 모두 포함된 이미지를 지원합니다. 이제 **다이제스트** 참조에서 이미지를 가져와서 정보 목적으로 **태그** 참조를 유지하고 콘솔 출력에 적절한 경고 메시지가 표시됩니다. (OCPBUGS-42421)

- 이전에는 클러스터 API가 기본 비 클러스터 API 프로비저닝 설치와 비교했을 때 가상 네트워크 설치에 지원되지 않는 태그 템플릿을 사용했습니다. 이로 인해 **networkAccess: Internal** 로 구성된 경우 Image Registry Operator가 성능이 저하된 상태가 되었습니다. 이번 릴리스에서는 Image Registry Operator에서 두 태그 템플릿을 모두 지원하므로 이 문제가 더 이상 존재하지 않습니다. (OCPBUGS-42394)

- 이전에는 IBM Cloud 클러스터 설치에 사용된 CCO(Cloud Controller Manager) 활성 프로브에서 루프백을 사용할 수 없어 프로브가 지속적으로 다시 시작되었습니다. 이번 릴리스에서는 더 이상 문제가 발생하지 않도록 프로브에서 루프백을 사용할 수 있습니다. (OCPBUGS-41941)

- 이전에는 **PerformanceProfile** 오브젝트에서 **globallyDisableIrqLoadBalancing** 필드가 **true** 로 설정된 경우 분리된 CPU가 **IRQBALANCE_BANNED_CPULIST** 변수 대신 **IRQBALANCE_BANNED_CPUS** 변수에 나열되었습니다. 이러한 변수는 **/etc/sysconfig/irqbalance** 에 저장됩니다. **globallyDisableIrqLoadBalancing** 필드의 값을 **true** 에서 **false** 로 변경하면 **IRQBALANCE_BANNED_CPULIST** 변수가 올바르게 업데이트되지 않았습니다. 결과적으로 분리된 CPU가 **IRQBALANCE_BANNED_CPULIST** 변수에 남아 있기 때문에 부하 재조정에 사용할 수 있는 CPU 수가 증가하지 않았습니다. 이번 릴리스에서는 분리된 CPU가 **IRQBALANCE_BANNED_CPUS** 변수에 나열되도록 하여 부하 재조정에 사용할 수 있는 CPU 수가 예상대로 증가합니다. (OCPBUGS-42323)

1.9.45.3. 업데이트

OpenShift Container Platform 4.16 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.46. RHSA-2024:3718 - OpenShift Container Platform 4.17.0 이미지 릴리스, 버그 수정 및 보안 업데이트 권고

출시 날짜: 2024년 10월 1일

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.17.0을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:3718 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:3722 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.17.0 --pullspecs
```

1.9.46.1. 확인된 문제

- **PerformanceProfile** 오브젝트에서 **globallyDisableIrqLoadBalancing** 필드가 **true** 로 설정된 경우 분리된 CPU는 **IRQBALANCE_BANNED_CPULIST** 변수 대신 **IRQBALANCE_BANNED_CPU** LIST 변수에 나열됩니다. 그러나 **globallyDisableIrqLoadBalancing** 필드의 값을 **true** 에서 **false** 로 변경해도 **IRQBALANCE_BANNED_CPULIST** 변수가 올바르게 업데이트되지 않습니다. 결과적으로 분리된 CPU가 **IRQBALANCE_BANNED_CPULIST** 변수에 유지되므로 로드 재조정에 사용할 수 있는 CPU 수가 증가하지 않습니다.

  참고

  IRQBALANCE_BANNED_CPULIST 변수와 **IRQBALANCE_BANNED_CPUS** 변수는 **/etc/sysconfig/irqbalance** 파일에 저장됩니다.

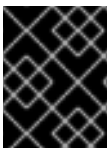
  (OCPBUGS-42323)

1.9.46.2. 업데이트

OpenShift Container Platform 4.16 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

2장. 추가 릴리스 정보

핵심 OpenShift Container Platform 4.17 릴리스 노트에 포함되지 않은 추가 관련 구성 요소 및 제품의 릴리스 노트는 다음 문서에서 확인할 수 있습니다.



중요

다음 릴리스 노트는 Red Hat 제품 다운스트림용입니다. 관련 제품의 업스트림 또는 커뮤니티 릴리스 노트는 포함되어 있지 않습니다.

A

AWS Load Balancer Operator

B

Red Hat OpenShift 빌드

C

cert-manager Operator for Red Hat OpenShift

Cluster Observability Operator (COO)

Compliance Operator

사용자 정의 지표 자동 스케일러 Operator

D

Red Hat Developer Hub Operator

E

외부 DNS Operator

F

File Integrity Operator

H

호스팅된 컨트롤 플레인

K

kube Descheduler Operator

L

로깅

M

Migration Toolkit for Containers (MTC)

N

Network Observability Operator

NBDE(Network-bound Disk Encryption) Tang Server Operator

O

OpenShift API for Data Protection (OADP)

Red Hat OpenShift Dev Spaces

Red Hat OpenShift Distributed Tracing Platform
Red Hat OpenShift GitOps