OpenShift Container Platform 4.11

릴리스 노트

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항

Last Updated: 2024-03-29

OpenShift Container Platform 4.11 릴리스 노트

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항

법적 공지

초록

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

차례

1장. OPENSHIFT CONTAINER PLATFORM 4.11 릴리스 노트 3
1.1. 릴리스 정보 3
1.2. OPENSHIFT CONTAINER PLATFORM 계층화된 종속 구성 요소 지원 및 호환성 3
1.3. 새로운 기능 및 개선 사항 3
1.4. 주요 기술 변경 사항 29
1.5. 사용되지 않거나 삭제된 기능 30
1.6. 버그 수정 34
1.7. 기술 프리뷰 기능 54
1.8. 확인된 문제 58
1.9. 비동기 에라타 업데이트 64

1장. OPENSHIFT CONTAINER PLATFORM 4.11 릴리스 노트

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

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-2022:5069)을 사용할 수 있습니다. 이 릴리스에서는 Kubernetes 1.24를 CRI-O 런타임과 함께 사용합니다. 다음은 OpenShift Container Platform 4.11과 관련된 새로운 기능, 변경 사항 및 알려진 문제에 대해 설명합니다.

OpenShift Container Platform 4.11 클러스터는 https://console.redhat.com/openshift에서 사용할 수 있습니다. OpenShift Container Platform용 Red Hat OpenShift Cluster Manager 애플리케이션을 사용하면 온프레미스 또는 클라우드 환경에 OpenShift 클러스터를 배포할 수 있습니다.

OpenShift Container Platform 4.11은 Red Hat Enterprise Linux 8.5-8.9 및 RHCOS(Red Hat Enterprise Linux CoreOS) 4.11에서 지원됩니다.

컨트롤 플레인에는 RHCOS 머신을 사용해야 하며 컴퓨팅 머신에 RHCOS 또는 RHEL을 사용할 수 있습니다.

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. RHCOS(Red Hat Enterprise Linux CoreOS)

1.3.1.1. Fabrics 보다 NVMe 에 대한 지원 개선

OpenShift Container Platform 4.11에는 NVMe 장치를 관리하기 위한 인터페이스를 제공하는 **nvme-cli** 패키지가 도입되었습니다.

1.3.1.2. kdump를 사용하여 AMD64 머신에서 커널 충돌 조사

RHCOS는 OpenShift Container Platform 4.11에서 **x86_64** 아키텍처에 대한 **kdump**를 지원합니다. 다른 아키텍처에서 **kdump**에 대한 지원은 기술 프리뷰로 남아 있습니다.

1.3.1.3. kdump를 사용하여 ARM64 시스템에서 커널 충돌 조사 (기술 프리뷰)

RHCOS는 이제 OpenShift Container Platform 4.11의 **arm64** 아키텍처에 대한 **kdump**를 기술 프리뷰로 지원합니다.

1.3.1.4. RHCOS에서 RHEL 8.6 사용

RHCOS는 OpenShift Container Platform 4.11 이상에서 RHEL (Red Hat Enterprise Linux) 8.6 패키지를 사용합니다. 이를 통해 최신 수정 사항, 기능 및 향상된 기능은 물론 최신 하드웨어 지원 및 드라이버 업데이트를 받을 수 있습니다.

1.3.1.5. 업데이트된 RHCOS 레지스트리 URL

RHCOS 부팅 이미지를 다운로드하는 리디렉션 프로그램 호스트 이름이 이제 **rhcos.mirror.openshift.com** 입니다. 부트 이미지에 대한 액세스 권한을 부여하도록 방화벽을 구성해야 합니다. 자세한 내용은 OpenShift Container Platform의 방화벽 구성 을 참조하십시오.

1.3.2. 설치 및 업그레이드

1.3.2.1. OpenShift 설치 프로그램에 대한 RHEL 9 지원

OpenShift 설치 프로그램(openshift-install)과 함께 RHEL(Red Hat Enterprise Linux) 9 사용이 지원됩니다.

자세한 내용은 플랫폼에 대한 설치 설명서의 "설치 프로그램 받기" 섹션을 참조하십시오.

1.3.2.2. 단일 노드에 OpenShift Container Platform을 설치하기 위한 새로운 최소 시스템 요구 사항

이번 릴리스에서는 단일 노드에 OpenShift Container Platform을 설치하기 위한 최소 시스템 요구 사항이 업데이트됩니다. 단일 노드에 OpenShift Container Platform을 설치할 때 최소 16GB의 RAM을 구성해야 합니다. 특정 워크로드 요구 사항은 추가 RAM이 필요할 수 있습니다. 지원되는 플랫폼의 전체 목록은 베어 메탈, vSphere, RHOSP(Red Hat OpenStack Platform) 및 Red Hat Virtualization 플랫폼을 포함하도록 업데이트되었습니다. 모든 경우에 **openshift-installer** 바이너리가 단일 노드 OpenShift를 설치하는 데 사용되는 경우 **install-config.yaml** 구성 파일에서 **platform.none: {}** 매개 변수를 지정해야 합니다.

1.3.2.3. ARM의 OpenShift Container Platform

OpenShift Container Platform 4.11은 이제 ARM 아키텍처 기반 AWS 사용자 프로비저닝 인프라 및 베어 메탈 설치 관리자 프로비저닝 인프라에서 지원됩니다. 인스턴스 가용성 및 설치 설명서에 대한 자세한 내용은 다른 플랫폼에서 지원되는 설치 방법 을 참조하십시오.

ARM의 OpenShift Container Platform에서 지원되는 기능은 다음과 같습니다.

- 연결이 해제된 설치 지원
- AWS용 EBS(Elastic File System)
- 베어 메탈의 로컬 스토리지 Operator
- 베어 메탈의 경우 iSCSI(Internet Small Computer Systems Interface)

다음 Operator는 ARM의 OpenShift Container Platform에서 지원됩니다.

- SRO(Special Resource Operator)

1.3.2.4. AWS에 설치 중 부트스트랩 오류 문제 해결

이제 설치 프로그램에서 AWS의 부트스트랩 및 컨트롤 플레인 호스트에서 직렬 콘솔 로그를 수집합니다. 이 로그 데이터는 표준 부트스트랩 로그 번들에 추가됩니다.

자세한 내용은 설치 문제 해결을 참조하십시오.

1.3.2.5. Microsoft Hyper-V generation 버전 2에 대한 지원

기본적으로 설치 프로그램은 이제 Hyper-V generation 버전 2 VM(가상 머신)을 사용하여 Microsoft Azure 클러스터를 배포합니다. 설치 프로그램에서 VM에 대해 선택한 인스턴스 유형이 버전 2를 지원하지 않는 것을 탐지하는 경우 배포에 버전 1을 사용합니다.

1.3.2.6. 기본 AWS 및 VMware vSphere 컴퓨팅 노드 리소스

기본적으로 OpenShift Container Platform 4.11부터 설치 프로그램은 이제 4개의 vCPU 및 16GB의 가상 RAM을 사용하여 AWS 및 VMware vSphere 컴퓨팅 노드를 배포합니다.

1.3.2.7. AWS SC2S 리전 지원

OpenShift Container Platform 4.11에서는 AWS Secret Commercial Cloud Services (SC2S) 리전을 지원합니다. 이제 **us-isob-east-1** SC2S 리전에 OpenShift Container Platform 클러스터를 설치하고 업데이트할 수 있습니다.

자세한 내용은 시크릿 또는 최상위 시크릿 리전에 AWS의 클러스터 설치 를 참조하십시오.

1.3.2.8. 설치 관리자 프로비저닝 인프라를 사용하여 Nutanix에 클러스터 설치

OpenShift Container Platform 4.11에서는 설치 관리자 프로비저닝 인프라를 사용하여 Nutanix에 클러스터를 설치할 수 있도록 지원합니다. 이러한 유형의 설치를 통해 설치 프로그램이 프로비저닝하고 클러스터가 유지보수하는 인프라에 클러스터를 배포할 수 있습니다.

자세한 내용은 Nutanix에 클러스터 설치를 참조하십시오.

1.3.2.9. Azure Ultra SSD를 사용하여 OpenShift Container Platform 설치

Azure에 OpenShift Container Platform을 설치할 때 Ultra SSD 스토리지를 활성화할 수 있습니다. 이 기능을 사용하려면 OpenShift Container Platform을 설치하는 Azure 리전 및 영역 모두 Ultra 스토리지를 제공해야 합니다.

자세한 내용은 추가 Azure 구성 매개변수를 참조하십시오.

1.3.2.10. bootstrapExternalStaticIP 및 bootstrapExternalStaticGateway 구성 설정에 대한 지원 추가

설치 프로그램이 프로비저닝한 OpenShift Container Platform 클러스터를 고정 IP 주소가 있고 **baremetal** 네트워크의 DHCP 서버가 없는 베어 메탈에 배포하는 경우 부트스트랩 VM의 고정 IP 주소 및 부트스트랩 VM의 게이트웨이의 고정 IP 주소를 지정해야 합니다. OpenShift Container Platform 4.11에서는 배포 전에 **install-config.yaml** 파일에서 설정할 수 있는 **bootstrapExternalStaticIP** 및 **bootstrapExternalStaticGateway** 구성 설정을 제공합니다. 이러한 설정을 도입하면 OpenShift Container Platform 4.10 릴리스의 DHCP 서버가 없는 베어 메탈 네트워크의 IP 주소로 부트스트랩 VM 할당 절차가 교체됩니다.

자세한 내용은 install-config.yaml 파일 구성 및 추가 install-config 매개변수를 참조하십시오.

1.3.2.11. Fujitsu 하드웨어 구성

OpenShift Container Platform 4.11에서는 Fujitsu 하드웨어를 사용하여 베어 메탈에 OpenShift Container Platform을 설치할 때 컨트롤 플레인 노드의 BIOS 및 RAID 어레이를 구성할 수 있습니다. OpenShift Container Platform 4.10에서는 Fujitsu 하드웨어에서 BIOS 및 RAID 어레이를 구성하는 작업이 작업자 노드로 제한되었습니다.

자세한 내용은 BIOS 구성 및 RAID 구성을 참조하십시오.

1.3.2.12. oc-mirror CLI 플러그인으로 연결이 끊긴 미러링을 사용할 수 있습니다.

oc-mirror OpenShift CLI(**oc**) 플러그인을 사용하여 연결이 끊긴 환경의 이미지를 미러링할 수 있습니다. 이 기능은 이전에 OpenShift Container Platform 4.10에서 기술 프리뷰로 소개되었으며 현재 OpenShift Container Platform 4.11에서 일반적으로 사용할 수 있습니다.

oc-mirror 플러그인의 이번 릴리스에는 다음과 같은 새로운 기능이 포함되어 있습니다.

- 대상 미러 레지스트리에서 이미지 정리
- Operator 패키지 및 OpenShift Container Platform 릴리스의 버전 범위 지정
- OpenShift Update Service (OSUS) 사용에 대한 지원 아티팩트 생성
- 초기 이미지 세트 구성에 대한 템플릿 가져오기

중요

OpenShift Container Platform 4.10용 oc-mirror 플러그인의 기술 프리뷰 버전을 사용한 경우 미러 레지스트리를 OpenShift Container Platform 4.11로 마이그레이션할 수 없습니다. 새 oc-mirror 플러그인을 다운로드하고 새 스토리지 백엔드를 사용하고 대상 미러 레지스트리에서 새로운 최상위 네임스페이스를 사용해야 합니다.

자세한 내용은 oc-mirror 플러그인을 사용하여 연결이 끊긴 설치의 이미지 미러링을 참조하십시오 .

1.3.2.13. 사용자 관리 암호화 키를 사용하여 Azure에 클러스터 설치

OpenShift Container Platform 4.11에서는 사용자 관리 디스크 암호화를 사용하여 Azure에 클러스터를 설치할 수 있도록 지원합니다.

자세한 내용은 Azure에 대한 사용자 관리 암호화 활성화 를 참조하십시오.

1.3.2.14. 기본적으로 활성화된 Azure용 가속화 네트워킹

Azure의 OpenShift Container Platform 4.11은 컨트롤 플레인 및 컴퓨팅 노드에 대한 가속화 네트워킹을 제공합니다. 가속화 네트워킹은 설치 관리자가 프로비저닝한 인프라 설치에서 지원되는 인스턴스 유형에 대해 기본적으로 활성화됩니다.

자세한 내용은 Azure의 Openshift 4 - 가속화 네트워킹 을 참조하십시오.

1.3.2.15. AWS VPC 엔드 포인트 및 제한된 설치

AWS에 제한된 OpenShift Container Platform 클러스터를 설치할 때 더 이상 AWS VPC 엔드 포인트를 설정할 필요가 없습니다. VPC 엔드 포인트를 구성하는 동안 VPC 엔드 포인트없이 프록시를 구성하거나 VPC 엔드 포인트로 프록시를 구성하도록 선택할 수도 있습니다.

자세한 내용은 VPC 사용 요구사항을 참조하십시오.

1.3.2.16. OpenShift Container Platform을 설치할 때 추가 사용자 정의

OpenShift Container Platform 4.11을 사용하면 **baremetal** 및 **marketplace** Operator의 설치와 **openshift** 네임스페이스에 저장된 **openshift-samples** 콘텐츠를 비활성화할 수 있습니다. 설치 전에 **baselineCapabilitySet** 및 **additionalEnabledCapabilities** 매개변수를 **install-config.yaml** 구성 파일에 추가하여 이러한 기능을 비활성화할 수 있습니다. 설치 중에 이러한 기능을 비활성화하면 클러스터를 설치한 후 활성화할 수 있습니다. 기능을 활성화한 후에는 다시 비활성화할 수 없습니다.

자세한 내용은 플랫폼에 대한 설치 문서의 "설치 구성 매개변수" 섹션을 참조하십시오.

1.3.2.17. Azure Marketplace 오퍼링

OpenShift Container Platform은 Azure Marketplace에서 사용할 수 있습니다. Azure Marketplace 제품은 북미 및 EMEA에서 OpenShift Container Platform을 구매한 고객에게 제공됩니다.

자세한 내용은 Azure Marketplace를 사용하여 OpenShift 설치 를 참조하십시오.

1.3.2.18. AWS Marketplace 오퍼링

OpenShift Container Platform은 이제 AWS Marketplace에서 사용할 수 있습니다. AWS Marketplace 제품은 북미에서 OpenShift Container Platform을 구매한 고객이 사용할 수 있습니다.

자세한 내용은 AWS Marketplace를 사용하여 OpenShift 설치 를 참조하십시오.

1.3.2.19. vSphere 클러스터에 CSI 드라이버 설치

vSphere에서 실행되는 클러스터에 CSI 드라이버를 설치하려면 다음 구성 요소가 설치되어 있어야 합니다.

- 가상 하드웨어 버전 15 이상
- vSphere 버전 7.0 업데이트 2 이상, 버전 8을 포함하지만 포함하지 않습니다. vSphere 8은 지원되지 않습니다.
- VMware ESXi 버전 7.0 업데이트 2 이상

위의 버전보다 이전 버전이 있는 구성 요소는 더 이상 사용되지 않거나 제거됩니다. 더 이상 사용되지 않는 버전은 여전히 완전하게 지원되지만 Red Hat은 ESXi 7.0 Update 2 이상 및 vSphere 7.0 업데이트 2를 버전 8을 포함하지만 제외하는 것이 좋습니다. vSphere 8은 지원되지 않습니다.

자세한 내용은 더 이상 사용되지 않고 삭제된 기능을 참조하십시오.

1.3.3. 설치 후 구성

1.3.3.1. 클러스터 기능

클러스터 관리자는 클러스터 기능을 활성화하여 설치 전이나 설치 후에 하나 이상의 선택적 구성 요소를 선택하거나 선택 취소할 수 있습니다.

자세한 내용은 클러스터 기능을 참조하십시오.

1.3.3.2. 다중 아키텍처 컴퓨팅 머신이 있는 OpenShift Container Platform 클러스터 (기술 프리뷰)

OpenShift Container Platform 4.11에는 기술 프리뷰에서 Azure 설치 관리자 프로비저닝 인프라를 사용하여 다중 아키텍처 컴퓨팅 머신이 지원하는 클러스터가 도입되었습니다. 이 기능은 Day-two 작업으로 다중 아키텍처 설치 관리자 바이너리로 프로비저닝된 설치 관리자인 기존 **x86_64** Azure 클러스터에 fabric **64** 컴퓨팅 노드를 추가할 수 있는 기능을 제공합니다. 수동으로 생성된 **ARM64** 부팅 이미지를 사용하는 사용자 정의 Azure 머신 세트를 생성하여 collect **64** 컴퓨팅 노드를 클러스터에 추가할 수 있습니다. **arm64** 아키텍처의 컨트롤 플레인은 현재 지원되지 않습니다. 자세한 내용은 다중 아키텍처 클러스터 구성을 참조하십시오.

참고

release **image-pullsec** 을 사용하여 클러스터를 최신 다중 아키텍처 릴리스 이미지로 수동으로 업그레이드할 수 있습니다. 자세한 내용은 다중 아키텍처 컴퓨팅 머신 업그레이드를 참조하십시오.

1.3.4. 웹 콘솔

1.3.4.1. 개발자 화면

- 이번 업데이트를 통해 개발자 화면에서 파이프라인을 포함하는 GitHub 리포지토리를 OpenShift Container Platform 클러스터에 추가할 수 있습니다. 이제 푸시 또는 가져오기 요청과 같은 관련 Git 이벤트가 트리거되면 클러스터의 GitHub 리포지토리에서 파이프라인 및 작업을 실행할 수 있습니다.
    - 관리자 화면에서 파이프라인을 코드로 사용하도록 OpenShift 클러스터를 사용하여 GitHub 애플리케이션을 구성할 수 있습니다. 이 구성을 사용하면 빌드 배포에 필요한 작업 세트를 실행할 수 있습니다.
- 이번 업데이트를 통해 고유한 큐레이션 작업 세트를 사용하여 사용자 지정 파이프라인을 생성할 수 있습니다. 개발자 콘솔에서 작업을 직접 검색, 설치 및 업그레이드할 수 있습니다.
- 이번 업데이트를 통해 웹 터미널에 여러 개의 탭이 있고 bash 기록을 볼 수 있으며 웹 터미널은 브라우저 창 또는 탭을 닫을 때까지 계속 열린 상태로 유지됩니다.
- 이번 업데이트를 통해 개발자 화면의 **Add+** 페이지에서 프로젝트에 사용자를 추가하거나 제거할 수 있는 프로젝트 및 Helm 차트 리포지터리를 공유하는 새 메뉴가 추가되었습니다.

1.3.4.2. 동적 플러그인 업데이트

이번 업데이트를 통해 새 **console.openshift.io/use-i18 next** 주석을 사용하여 **ConsolePlugin**에 현지화 리소스가 포함되어 있는지 확인할 수 있습니다. 주석이 **"true"** 로 설정된 경우 동적 플러그인 다음에 이름이 지정된 i18n 네임스페이스의 지역화 리소스가 로드됩니다. 주석이 다른 값으로 설정되거나 **ConsolePlugin** 리소스에서 누락된 경우 현지화 리소스가 로드되지 않습니다.

자세한 내용은 동적 플러그인 개요를 참조하십시오.

1.3.4.3. 다크 모드 주제 지원

OpenShift Container Platform 웹 콘솔은 이제 다크 모드 주제를 지원합니다. **사용자 환경 설정** 페이지에서 원하는 주제를 선택하여 웹 콘솔을 확인합니다.

1.3.4.4. 설치된 Operator 페이지에 있는 모든 관리 네임스페이스의 피연산자 인스턴스 표시

이번 업데이트를 통해 **Operator → 설치된 Operator** 페이지에 모든 네임스페이스의 모든 Operator가 표시됩니다. 프로젝트 선택기 내에서 선택한 네임스페이스의 인스턴스만 볼 수 있습니다. 피연산자 인스턴스를 볼 때 새 전환 컨트롤을 사용하면 모든 네임스페이스의 모든 피연산자 인스턴스 또는 현재 네임스페이스만 표시할 수 있습니다.

1.3.4.5. 조건부 업데이트

이번 업데이트를 통해 조건부 업데이트가 제공되는 경우 **업데이트 클러스터** 모달의 **Select new version** 드롭다운에서 **Include supported but not recommended versions**를 활성화하여 드롭다운 목록을 조건부 업데이트로 채울 수 있습니다. **Supported but not recommended** 버전이 선택되면 버전에 잠재적인 문제가 표시되는 드롭다운 메뉴에 경고가 표시됩니다.

1.3.4.6. PDB(Pod 중단 예산)

이번 업데이트에서는 OpenShift Container Platform 웹 콘솔에 대한 PDB(Pod 중단 예산)를 지원합니다. **워크로드 → PodDisruptionBudgets**에서 Pod 리소스에 대한 PDB를 생성할 수 있습니다. 가용성 요구 사항 목록에서 **maxUnavailable** 및 **minAvailable**을 선택하고 실행 중인 Pod 값을 설정할 수 있습니다. 또는 **pod controller resources** 목록 및 **세부 정보** 페이지에서 Pod 중단 예산을 생성할 수 있습니다. 예를 들어 **워크로드 → 배포**에서 **Add PodDisruptionBudget**을 클릭합니다.

자세한 내용은 Pod 선점 및 기타 스케줄러 설정 을 참조하십시오.

1.3.5. OpenShift CLI(oc)

1.3.5.1. OpenShift CLI(oc)에 대한 RHEL 9 지원

OpenShift CLI(**oc**)와 함께 RHEL(Red Hat Enterprise Linux) 9 사용이 지원됩니다.

참고

RHEL(Red Hat Enterprise Linux) 9의 RPM으로 OpenShift CLI(**oc**)를 설치할 수 없습니다. 바이너리를 다운로드하여 RHEL 9용 OpenShift CLI를 설치해야 합니다.

자세한 내용은 OpenShift CLI 설치를 참조하십시오.

1.3.6. IBM Z 및 LinuxONE

이 릴리스에서 IBM Z 및 LinuxONE은 이제 OpenShift Container Platform 4.11과 호환됩니다. z/VM 또는 RHEL KVM을 사용하여 설치할 수 있습니다. 설치 지침은 다음 설명서를 참조하십시오.

- IBM Z 및 LinuxONE에 z/VM으로 클러스터 설치
- 네트워크가 제한된 환경에서 IBM Z 및 LinuxONE에 z/VM으로 클러스터 설치
- IBM Z 및 LinuxONE에 RHEL KVM으로 클러스터 설치
- 네트워크가 제한된 환경에서 IBM Z 및 LinuxONE에 RHEL KVM으로 클러스터 설치

주요 개선 사항
OpenShift Container Platform 4.11을 사용하는 IBM Z 및 LinuxONE에서 지원되는 새로운 기능은 다음과 같습니다.

- 대체 인증 공급자

- 로컬 스토리지 Operator를 통한 자동 장치 검색
- CSI 볼륨
  - 복제
  - 확장
  - 스냅샷
- File Integrity Operator
- 사용자 정의 프로젝트 모니터링
- Operator API
- OC CLI 플러그인

지원되는 기능
다음 기능은 IBM Z 및 LinuxONE에서도 지원됩니다.

- 현재 다음 Operator가 지원됩니다.
  - Cluster Logging Operator
  - Compliance Operator
  - Local Storage Operator
  - NFD Operator
  - NMState Operator
  - OpenShift Elasticsearch Operator
  - Service Binding Operator
  - Vertical Pod Autoscaler Operator
- 다음 Multus CNI 플러그인이 지원됩니다.
  - Bridge
  - Host-device
  - IPAM
  - IPVLAN
- etcd에 저장된 데이터 암호화
- Helm
- 수평 Pod 자동 스케일링
- 다중 경로
- iSCSI를 사용하는 영구 스토리지

- 로컬 볼륨을 사용하는 영구저장장치(Local Storage Operator)
- hostPath를 사용하는 영구 스토리지
- 파이버 채널을 사용하는 영구 스토리지
- Raw Block을 사용하는 영구 스토리지
- IPsec 암호화를 포함한 OVN-Kubernetes
- 다중 네트워크 인터페이스 지원
- 3-노드 클러스터 지원
- SCSI 디스크의 z/VM Emulated FBA 장치
- 4K FCP 블록 장치

이러한 기능은 IBM Z의 OpenShift Container Platform 및 4.11용 LinuxONE에서만 사용할 수 있습니다.

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

제한 사항
다음 제한 사항은 IBM Z 및 LinuxONE의 OpenShift Container Platform에 영향을 미칩니다.

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

1.3.7. IBM Power

이 릴리스에서 IBM Power는 이제 OpenShift Container Platform 4.11과 호환됩니다. 설치 지침은 다음 설명서를 참조하십시오.

- IBM Power에 클러스터 설치
- 네트워크가 제한된 환경에서 IBM Power에 클러스터 설치

주요 개선 사항
OpenShift Container Platform 4.11을 사용하는 IBM Power에서 지원되는 새로운 기능은 다음과 같습니다.

- 대체 인증 공급자
- CSI 볼륨
  - 복제
  - 확장
  - 스냅샷
- File Integrity Operator
- IPv6
- 사용자 정의 프로젝트 모니터링
- Operator API
- OC CLI 플러그인

지원되는 기능
다음 기능은 IBM Power에서도 지원됩니다.

- 현재 다음 Operator가 지원됩니다.
  - Cluster Logging Operator
  - Compliance Operator
  - Local Storage Operator
  - NFD Operator
  - NMState Operator
  - OpenShift Elasticsearch Operator
  - SR-IOV 네트워크 Operator
  - Service Binding Operator
  - Vertical Pod Autoscaler Operator
- 다음 Multus CNI 플러그인이 지원됩니다.
  - Bridge
  - Host-device

    - IPAM
    - IPVLAN
- etcd에 저장된 데이터 암호화
- Helm
- 수평 Pod 자동 스케일링
- 다중 경로
- Multus SR-IOV
- IPsec 암호화를 포함한 OVN-Kubernetes
- iSCSI를 사용하는 영구 스토리지
- 로컬 볼륨을 사용하는 영구저장장치(Local Storage Operator)
- hostPath를 사용하는 영구 스토리지
- 파이버 채널을 사용하는 영구 스토리지
- Raw Block을 사용하는 영구 스토리지
- 다중 네트워크 인터페이스 지원
- Power10 지원
- 3-노드 클러스터 지원
- 4K 디스크 지원

제한 사항
IBM Power의 OpenShift Container Platform에 영향을 미치는 제한 사항은 다음과 같습니다.

- 다음 OpenShift Container Platform 기술 프리뷰 기능은 지원되지 않습니다.
    - PTP(Precision Time Protocol) 하드웨어
- 다음 OpenShift Container Platform 기능은 지원되지 않습니다 :
    - 시스템 상태 점검으로 손상된 시스템 자동 복구
    - Red Hat OpenShift Local
    - 노드에서 오버 커밋 제어 및 컨테이너 밀도 관리
    - FIPS 암호화
    - OpenShift Metering
    - OpenShift Virtualization
    - OpenShift Container Platform 배포 시 Tang 모드 디스크 암호화
- 컴퓨팅 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행

- 영구 스토리지는 로컬 볼륨, Red Hat OpenShift Data Foundation, NFS(Network File System) 또는 CSI(Container Storage Interface)를 사용하는 Filesystem 유형이어야 합니다.

1.3.8. 보안 및 컴플라이언스

1.3.8.1. 감사 로그에서 OAuth 서버 감사 이벤트 포함

이제 로그인 이벤트 주석이 추가된 OAuth 서버 감사 이벤트가 감사 로그의 메타데이터 수준에서 기록됩니다. 로그인 이벤트에는 실패한 로그인 시도가 포함됩니다.

자세한 내용은 감사 로그 정책 프로필 정보 를 참조하십시오.

1.3.9. 네트워킹

1.3.9.1. 보조 네트워크에 대한 Pod 수준 본딩

Pod 수준의 본딩은 고가용성과 처리량이 필요한 Pod 내부의 워크로드를 활성화하는 데 중요합니다. Pod 수준 본딩을 사용하면 커널 모드 인터페이스에서 여러 개의 SR-IOV(root I/O Virtualization) 가상 기능 인터페이스에서 본딩 인터페이스를 생성할 수 있습니다. SR-IOV 가상 기능은 Pod에 전달되고 커널 드라이버에 연결됩니다.

Pod 수준 본딩이 필요한 시나리오에는 다양한 물리적 기능의 여러 SR-IOV 가상 함수에서 본딩 인터페이스 생성이 포함됩니다. 호스트에서 두 가지 물리적 함수에서 본딩 인터페이스를 생성하여 Pod 수준에서 고가용성을 실현할 수 있습니다.

자세한 내용은 두 개의 SR-IOV 인터페이스에서 본딩 인터페이스 구성을 참조하십시오.

1.3.9.2. 호스트 네트워크 엔드포인트를 사용하는 Ingress 컨트롤러의 새 옵션

이번 업데이트에서는 **hostnetwork** 엔드포인트 전략을 사용하여 Ingress 컨트롤러에 대한 새 옵션이 도입되었습니다. **httpPort**,**httpsPort** 및 **statsPort** 바인딩 포트를 사용하여 동일한 작업자 노드에서 여러 Ingress 컨트롤러를 호스팅할 수 있습니다.

1.3.9.3. 컨트롤 플레인 및 작업자 노드에 대한 다중 노드 구성

클러스터의 여러 베어 메탈, 설치 관리자 프로비저닝 인프라 노드에 단일 구성을 동시에 적용할 수 있습니다. 단일 구성을 여러 노드에 적용하면 단일 프로비저닝 프로세스로 인한 구성 오류의 위험이 줄어듭니다.

이 메커니즘은 **install-config** 파일이 사용되는 초기 배포에만 사용할 수 있습니다.

1.3.9.4. AWS에서 Classic Load Balancer(CLB) 시간 제한 구성 지원

Ingress 컨트롤러에서 AWS Classic Load Balancer(CLB)에 대한 유휴 연결 시간 제한을 구성할 수 있습니다.

자세한 내용은 클래식 로드 밸런서 시간 구성 을 참조하십시오.

1.3.9.5. HAProxy 2.2.24로 업데이트

OpenShift Container Platform이 HAProxy 2.2.24로 업데이트되었습니다.

1.3.9.6. HAProxy 프로세스에 대한 최대 연결 수 구성 지원

Ingress 컨트롤러의 HAProxy 프로세스별로 설정할 수 있는 최대 동시 연결 수를 2000에서 2,000,000 사이의 값으로 설정할 수 있습니다.

자세한 내용은 Ingress 컨트롤러 구성 매개변수를 참조하십시오.

1.3.9.7. Ingress 컨트롤러 상태 점검 간격 설정

이번 업데이트를 통해 클러스터 관리자는 상태 점검 간격을 설정하여 연속된 두 상태 점검 간에 라우터가 대기하는 시간을 정의할 수 있습니다. 이 값은 모든 경로에 대한 기본값으로 전역적으로 적용됩니다. 기본값은 5초입니다.

자세한 내용은 Ingress 컨트롤러 구성 매개변수를 참조하십시오.

1.3.9.8. 인터페이스 수준의 안전 네트워크 sysctl 구성 지원

새로운 **tuning-cni** 메타 플러그인을 사용하여 특정 인터페이스에만 적용되는 인터페이스 수준 안전한 네트워크 sysctl을 설정합니다. 예를 들어 **tuning-cni** 플러그인을 구성하여 특정 네트워크 인터페이스에서 **accept_redirects** 의 동작을 변경할 수 있습니다. 설정할 수 있는 인터페이스별 안전한 sysclts의 전체 목록은 설명서에서 확인할 수 있습니다.

이 향상된 기능 외에도 **net.ipv4.ping_group_range** 및 **net.ipv4.ip_unprivileged_port_start**를 지원하기 위해 설정할 수 있는 시스템 전체의 안전한 sysctl 세트가 증가했습니다.

tuning-cni 플러그인 구성에 대한 자세한 내용은 인터페이스 수준 네트워크 sysctl 설정 을 참조하십시오.

새로 지원되는 인터페이스 수준 네트워크 안전 sysclts 및 지원되는 시스템 전체 안전 sysclts 목록 업데이트에 대한 자세한 내용은 컨테이너에서 sysctl 사용 을 참조하십시오.

1.3.9.9. TLS를 통해 DNS 요청을 전달하는 CoreDNS 지원

고도로 규제된 환경에서 작업하는 경우 추가 DNS 트래픽 및 데이터 개인 정보를 보장할 수 있도록 요청을 업스트림 해석기로 전달할 때 DNS(Domain Name System) 트래픽을 보호할 수 있는 기능이 필요할 수 있습니다. 클러스터 관리자는 전달된 DNS 쿼리에 대해 TLS(전송 계층 보안)를 구성할 수 있습니다. 이 기능은 Machine Config Operator에서 관리하는 CoreDNS 인스턴스가 아닌 DNS Operator에만 적용됩니다.

자세한 내용은 DNS 전달 사용 을 참조하십시오.

1.3.9.10. OVN-Kubernetes 내부 트래픽 지원

클러스터 관리자는 OVN-Kubernetes CNI(Container Network Interface) 클러스터 네트워크 공급자를 사용하는 경우 Kubernetes 서비스 오브젝트에 **internalTrafficPolicy=Local**를 구성할 수 있습니다. 이 기능을 통해 클러스터 관리자는 트래픽이 시작된 노드와 동일한 노드의 엔드포인트로 트래픽을 라우팅할 수 있습니다. 로컬 노드 엔드포인트가 없으면 트래픽이 삭제됩니다.

자세한 내용은 서비스 내부 트래픽 정책 을 참조하십시오.

1.3.9.11. AWS Load Balancer Operator 지원 (기술 프리뷰)

클러스터 관리자는 OpenShift Container Platform 웹 콘솔 또는 CLI를 사용하여 OperatorHub에서 AWS Load Balancer Operator를 설치할 수 있습니다. AWS Load Balancer Operator는 기술 프리뷰에 있습니다.

자세한 내용은 AWS Load Balancer Operator 설치 를 참조하십시오.

1.3.9.12. 라우트 API 기능 개선

이전에는 경로의 하위 도메인을 지정할 수 없어 호스트 이름을 설정하는 데 **spec.host** 필드가 필요했습니다. 이제 **spec.subdomain** 필드를 지정하고 경로의 **spec.host** 필드를 생략할 수 있습니다. 경로를 노출하는 라우터 배포는 **spec.subdomain** 값을 사용하여 호스트 이름을 결정합니다.

이 향상된 기능을 사용하여 경로를 노출하는 각 라우터 배포에서 결정된 서로 다른 여러 고유 호스트 이름을 경로에 사용할 수 있도록 설정하여 라우팅을 단순화할 수 있습니다.

1.3.9.13. 외부 DNS Operator

OpenShift Container Platform 4.11에서 외부 DNS Operator는 AWS Route53, Azure DNS, GCP DNS 및 GA (일반 가용성) 상태에서 Infoblox에서 사용할 수 있습니다. 외부 DNS Operator는 여전히 GovCloud의 BlueCat 및 AWS Route53에 대한 TP(기술 프리뷰) 상태입니다. 이번 업데이트를 통해 외부 DNS Operator는 다음과 같은 향상된 기능을 제공합니다.

- Infoblox의 DNS 영역에서 DNS 레코드를 만들 수 있습니다.
- 기본적으로 External DNS Operator는 네임스페이스 **external-dns-operator** 에 피연산자를 생성합니다. 설치하기 전에 피연산자 및 역할 기반 액세스 제어(RBAC)에 대한 네임스페이스를 수동으로 만들 필요가 없습니다.
- 경로 상태를 사용하여 DNS FQDN 이름을 검색할 수 있습니다.
- 이제 BlueCat DNS 공급자에 대한 프록시 지원을 사용할 수 있습니다.
- BlueCat DNS 공급자를 사용하는 동안 자동 DNS 구성 배포를 활성화할 수 있습니다.

TP에서 GA로 마이그레이션했는지 확인합니다. OpenShift Container Platform 4.11의 **ExternalDNS** 업스트림 버전은 **v0.12.0**이며 TP의 경우 **v0.10.2**입니다. 자세한 내용은 외부 DNS Operator 정보를 참조하십시오.

1.3.9.14. 듀얼 NIC 경계 클럭에 대한 PTP 지원

각 NIC 채널의 **PtpConfig** 프로필을 사용하여 이중 네트워크 인터페이스(NIC)를 경계 클럭으로 구성할 수 있습니다.

자세한 내용은 듀얼 NIC 하드웨어에서 PTP 사용 을 참조하십시오.

1.3.9.15. PTP 이벤트 개선 사항

새로운 PTP 이벤트 API 엔드포인트를 사용할 수 있습니다. **api/cloudNotifications/v1/publishers**. 이 엔드포인트를 사용하면 클러스터 노드에 대한 PTP **os-clock-sync-state**,**ptp-clock-class-change** 및 **lock-state** 세부 정보를 가져올 수 있습니다.

자세한 내용은 DU 애플리케이션을 PTP 이벤트 REST API 참조에 구독 에서 확인하십시오.

1.3.9.16. PensandoECDHE 카드에 대한 SR-IOV 지원

이제 Pensando DSC 카드에서 SR-IOV 지원을 사용할 수 있습니다. OpenShift SR-IOV는 지원되지만 SR-IOV를 사용할 때 SR-IOV CNI 구성 파일을 사용하여 고정 VF(가상 기능) 미디어 액세스 제어(MAC) 주소를 설정해야 합니다.

1.3.9.17. Mellanox MT2892 카드에 대한 SR-IOV 지원

Mellanox MT2892 카드에 SR-IOV 지원을 사용할 수 있습니다.

1.3.9.18. 네트워크의 OpenShift Container Platform CIDR 범위

클러스터 설치 후에는 네트워크의 CIDR 범위를 조정할 수 없습니다. Red Hat은 생성된 POD 수를 신중하게 고려해야 하므로 범위를 결정하는 방법에 대한 직접적인 지침을 제공하지 않습니다.

1.3.9.19. OVN-Kubernetes 네트워크 공급자: 런타임 시 IPsec 활성화

OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 경우 클러스터 설치 후 IPsec 암호화를 활성화할 수 있습니다. IPsec 활성화 방법에 대한 자세한 내용은 IPsec 암호화 구성 을 참조하십시오.

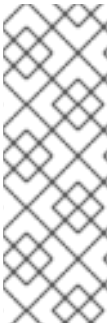
1.3.9.20. 추가 MetalLB CRD 지원 및 로깅 세부 정보 표시 제어

더 복잡한 구성을 지원하기 위해 추가 MetalLB CRD(사용자 정의 리소스 정의)가 추가되었습니다.

다음 CRD가 추가되었습니다.

- **IPAddressPools**
- **L2Advertisement**
- **BGPAdvertisement**
- **Community**

이러한 개선 사항을 통해 더 복잡한 구성에 Operator를 사용할 수 있습니다. 예를 들어 기능 향상을 사용하여 노드를 분리하거나 네트워크를 분할할 수 있습니다. 또한 FRRouting (FRR) 로깅 구성 요소의 개선 사항을 통해 생성된 로그의 상세 수준을 제어할 수 있습니다.



참고

OpenShift Container Platform 4.10에 설명된 CRD와 MetalLB 및 MetalLB Operator에 설명된 대로 MetalLB를 구성하는 기존 방법은 계속 지원되지만 더 이상 사용되지 않습니다. **AddressPool** 구성은 더 이상 사용되지 않습니다.

4.10에서는 **AddressPool**을 사용하는 계층 2 및 BGP IP 주소가 다른 주소 풀에서 할당되었습니다. OpenShift Container Platform 4.11에서 계층 2 및 BGP IP 주소는 동일한 주소 풀에서 할당할 수 있습니다.

자세한 내용은 Metal LB 및 MetalLB Operator 정보 를 참조하십시오.

1.3.9.21. Ingress 주석의 대상 CA 인증서를 사용하여 경로를 생성하는 기능

이제 Ingress 오브젝트에서 **route.openshift.io/destination-ca-certificate-secret** 주석을 사용하여 사용자 정의 인증서(CA)로 경로를 정의할 수 있습니다.

자세한 내용은 Ingress 주석에서 대상 CA 인증서를 사용하여 경로 생성 을 참조하십시오.

1.3.9.22. 호스트된 컨트롤 플레인(기술 프리뷰)

OpenShift Container Platform의 호스트된 컨트롤 플레인을 사용하면 규모에 따라 클러스터를 호스팅하여 관리 비용을 줄이고, 클러스터 배포 시간을 최적화하며 관리 및 워크로드 관련 문제를 분리할 수 있습니다. Kubernetes Operator 버전 2.0의 다중 클러스터 엔진을 설치할 때 이 배포 모델을 기술 프리뷰 기능으로 활성화할 수 있습니다. 자세한 내용은 호스팅되는 컨트롤 플레인 개요(기술 프리뷰)를 참조하십시오.

OVN(Open Virtual Network)은 클러스터의 컨트롤 플레인과 데이터 저장소를 호스팅하도록 설계되었습니다. OVN은 호스팅된 컨트롤 플레인을 사용하여 분할 컨트롤 플레인을 지원합니다.

1.3.9.23. OVN-Kubernetes 클러스터 네트워크 공급자가 있는 사용자 프로비저닝 베어 메탈 인프라에서 IPv6 단일 및 듀얼 스택 지원

사용자 프로비저닝 베어 메탈 인프라의 클러스터의 경우 OVN-Kubernetes 클러스터 네트워크 공급자는 IPv4 및 IPv6 주소 제품군을 모두 지원합니다.

1.3.9.24. RHOSP에서 OVS 하드웨어 오프로드

RHOSP에서 실행되는 클러스터의 경우 OVS(Open vSwitch) 하드웨어 오프로드를 일반적으로 사용할 수 있습니다.

자세한 내용은 OVS 하드웨어 오프로드 활성화를 참조하십시오.

1.3.9.25. RHOSP에서 NFV 사용자 개선 사항

RHOSP에서 실행되는 클러스터의 경우 네트워크 기능 가상화 배포 환경이 향상됩니다. 이 릴리스의 변경 사항은 다음과 같습니다.

- 구성 드라이브가 아닌 메타데이터 서비스 URL에서 가져오는 네트워크 데이터
- 검색된 모든 장치에 대해 no-IOMMU를 사용한 자동 VFIO 로드
- DPDK vHost 사용자 포트

이러한 변경 사항은 간단한 설치 후 및 네트워크 구성 설명서에 반영됩니다.

1.3.9.26. Red Hat OpenStack Platform, VMware vSphere 또는 oVirt에 설치할 때 유니캐스트를 기본값으로 사용하여 keepalived를 구성합니다.

RHOSP(Red Hat OpenStack Platform), VMware vSphere 또는 oVirt에 OpenShift Container Platform 설치 관리자 프로비저닝 설치 프로그램의 경우 keepalived가 멀티 캐스트 대신 기본적으로 유니캐스트로 구성됩니다. 더 이상 멀티 캐스트 트래픽을 허용할 필요가 없습니다. 모든 노드가 동시에 마이그레이션해야 하므로 클러스터 업그레이드가 완료된 후 몇 분 후에 유니캐스트 마이그레이션이 수행됩니다. 동시에 멀티 캐스트 및 유니캐스트 클러스터를 동시에 보유하면 keepalived가 유니캐스트 및 멀티 캐스트를 완전히 분리하므로 문제가 발생하지 않습니다.

1.3.10. 스토리지

1.3.10.1. Microsoft Azure File CSI Driver Operator를 사용하는 영구 스토리지 사용 가능

OpenShift Container Platform은 Azure 파일의 CSI(Container Storage Interface) 드라이버를 사용하여 PV(영구 볼륨)를 프로비저닝할 수 있습니다. 이 기능은 이전에 OpenShift Container Platform 4.10에서 기술 프리뷰 기능으로 소개되었으며 OpenShift Container Platform 4.11에서 일반적으로 사용 가능하며 기본적으로 활성화되어 있습니다.

자세한 내용은 Azure File CSI Driver Operator 를 참조하십시오.

1.3.10.2. OpenStack Cinder용 자동 CSI 마이그레이션은 일반적으로 사용 가능

OpenShift Container Platform 4.8부터 동등한 CSI(Container Storage Interface) 드라이버로 in-tree 볼륨 플러그인에 대한 자동 마이그레이션이 기술 프리뷰 기능으로 사용 가능하게 되었습니다. Cinder에 대

한 지원은 OpenShift Container Platform 4.8에서 이 기능을 통해 제공되며 OpenShift Container Platform 4.11에서는 일반적으로 사용 가능한 Cinder에 대한 자동 마이그레이션을 지원합니다. Cinder용 CSI 마이그레이션이 기본적으로 활성화되어 있으며 관리자가 조치를 취할 필요가 없습니다.

이 기능은 in-tree 오브젝트를 해당하는 CSI 표현으로 자동 변환하므로 사용자에게 완전히 투명해야 합니다. 번역된 오브젝트는 디스크에 저장되지 않으며 사용자 데이터는 마이그레이션되지 않습니다.

in-tree 스토리지 플러그인에 대한 스토리지 클래스가 계속 작동하지만 기본 스토리지 클래스를 CSI 스토리지 클래스로 전환하는 것이 좋습니다.

자세한 내용은 CSI 자동 마이그레이션 을 참조하십시오.

1.3.10.3. Microsoft Azure Disk의 자동 CSI 마이그레이션은 일반적으로 사용 가능합니다.

OpenShift Container Platform 4.8부터 동등한 CSI(Container Storage Interface) 드라이버로 in-tree 볼륨 플러그인에 대한 자동 마이그레이션이 기술 프리뷰 기능으로 사용 가능하게 되었습니다. Azure Disk에 대한 지원은 OpenShift Container Platform 4.9에서 이 기능을 통해 제공되며 OpenShift Container Platform 4.11은 이제 일반적으로 사용 가능한 Azure Disk에 대한 자동 마이그레이션을 지원합니다. Azure Disk 용 CSI 마이그레이션이 기본적으로 활성화되므로 관리자가 작업을 수행할 필요가 없습니다.

이 기능은 in-tree 오브젝트를 해당하는 CSI 표현으로 자동 변환하므로 사용자에게 완전히 투명해야 합니다. 번역된 오브젝트는 디스크에 저장되지 않으며 사용자 데이터는 마이그레이션되지 않습니다.

in-tree 스토리지 플러그인에 대한 스토리지 클래스가 계속 작동하지만 기본 스토리지 클래스를 CSI 스토리지 클래스로 전환하는 것이 좋습니다.

자세한 내용은 CSI 자동 마이그레이션 을 참조하십시오.

1.3.10.4. CSI 볼륨 확장 사용 가능

OpenShift Container Platform 4.3부터 이미 기술 프리뷰 기능으로 출시된 후 CSI(Container Storage Interface) 스토리지 볼륨이 확장되었으며 OpenShift Container Platform 4.11에서 일반적으로 사용할 수 있습니다.

자세한 내용은 CSI 볼륨 확장 을 참조하십시오.

1.3.10.5. CSI 일반 임시 볼륨 지원

OpenShift Container Platform 4.11은 일반적으로 사용 가능한 CSI(Container Storage Interface) 일반 임시 볼륨을 지원합니다. 일반 임시 볼륨은 영구 볼륨 및 동적 프로비저닝을 지원하는 모든 스토리지 드라이버에서 제공할 수 있는 임시 볼륨의 유형입니다.

자세한 내용은 일반 임시 볼륨을 참조하십시오.

1.3.10.6. VMware vSphere에서 크기 조정 및 스냅샷 지원

OpenShift Container Platform 4.11은 다음과 같은 제한 사항이 있는 vSphere CSI(Container Storage Interface) Driver Operator의 볼륨 크기 조정 및 스냅샷을 지원합니다.

- 스냅샷:
  - vSphere 버전 7.0 업데이트 3 이상이 필요합니다. 버전 8을 포함하되는 안 됩니다. vSphere 8은 vCenter Server 및 ESXi 모두에서 지원되지 않습니다.
  - fileshare 볼륨을 지원하지 않습니다.

- 크기 조정:
  - 오프라인 볼륨 확장: 필요한 최소 vSphere 버전은 6.7 업데이트 3 P06입니다.
  - 온라인 볼륨 확장: 필요한 최소 vSphere 버전은 7.0 업데이트 2입니다.

자세한 내용은 OpenShift Container Platform에서 지원하는 CSI 드라이버 를 참조하십시오.

1.3.11. 레지스트리

1.3.11.1. 가용성 영역에 대한 이미지 레지스트리 Operator 배포

이제 이미지 레지스트리 Operator의 기본 구성에서 모든 Pod가 영향을 받는 전체 영역 실패의 경우 지연된 복구 시간을 방지하기 위해 이미지 레지스트리 Pod를 토폴로지 영역에 분배합니다.

자세한 내용은 가용성 영역 간 이미지 레지스트리 Operator 배포 를 참조하십시오.

1.3.11.2. Red Hat OpenShift Data Foundation 레지스트리 스토리지

OpenShift Container Platform 4.11에서 지원되는 Red Hat OpenShift Data Foundation 레지스트리 스토리지

OpenShift Data Foundation은 다음을 포함하여 내부 이미지 레지스트리와 함께 사용할 수 있는 여러 스토리지 유형을 통합합니다.

- 온-프레미스 오브젝트 스토리지가 있는 공유 및 분산 파일 시스템인 Ceph
- Multicloud Object Gateway를 제공하는 NooBaa

1.3.12. Operator 라이프사이클

1.3.12.1. 파일 기반 카탈로그 형식

파일 기반 카탈로그 형식의 OpenShift Container Platform 4.11 릴리스에 대한 기본 Red Hat 제공 Operator 카탈로그입니다. OpenShift Container Platform 4.6 through 4.10은 SQLite 데이터베이스 형식으로 릴리스되었습니다. 파일 기반 카탈로그는 OLM(Operator Lifecycle Manager) 카탈로그 형식의 최신 버전입니다. JSON 또는 YAML의 일반 텍스트 기반 파일이며 이전 SQLite 데이터베이스 형식의 선언적 구성 진화입니다. 클러스터 관리자와 사용자는 새 카탈로그 형식을 사용하여 설치 워크플로 및 Operator 소비에 대한 변경 사항을 볼 수 없습니다.

자세한 내용은 파일 기반 카탈로그를 참조하십시오.

1.3.13. Operator 개발

1.3.13.1. Java 기반 Operator(기술 프리뷰)

OpenShift Container Platform 4.11에서 기술 프리뷰 기능으로부터 Operator SDK에는 Java 기반 Operator를 개발하는 툴 및 라이브러리가 포함되어 있습니다. Operator 개발자는 Operator SDK에서 Java 프로그래밍 언어 지원을 활용하여 Java 기반 Operator를 빌드하고 라이프사이클을 관리할 수 있습니다.

자세한 내용은 Java 기반 Operator용 Operator SDK 시작하기 를 참조하십시오.

1.3.13.2. 파일 기반 카탈로그에 대한 Operator SDK 지원

OpenShift Container Platform 4.11부터 **run bundle** 명령은 기본적으로 Operator 카탈로그의 파일 기반 카탈로그 형식을 지원합니다. Operator 카탈로그의 더 이상 사용되지 않는 SQLite 데이터베이스 형식은 계속 지원되지만 향후 릴리스에서 제거됩니다.

자세한 내용은 번들 이미지 작업을 참조하십시오.

1.3.13.3. Operator 번들 검증

Operator 작성자는 Operator SDK에서 **bundle validate** 명령을 실행하여 Operator 번들의 콘텐츠 및 형식을 검증할 수 있습니다. 기본 테스트 외에도 선택적 검증기를 실행하여 빈 CRD 설명 또는 지원되지 않는 OLM(Operator Lifecycle Manager) 리소스와 같은 번들의 문제를 테스트할 수 있습니다.

자세한 내용은 Operator 번들 유효성 검사에서 참조하십시오. 이전 버전의 OpenShift Container Platform에서 Performance Addon Operator는 애플리케이션에 대한 짧은 대기 시간 성능 튜닝을 제공합니다. OpenShift Container Platform 4.11에서 이러한 함수는 Node Tuning Operator의 일부입니다. Node Tuning Operator는 OpenShift Container Platform 4.11의 표준 설치의 일부입니다. OpenShift Container Platform 4.11로 업그레이드하는 경우 Node Tuning Operator는 시작 시 Performance Addon Operator 및 모든 관련 아티팩트를 제거합니다.

자세한 내용은 Node Tuning Operator를 참조하십시오.

1.3.14. Jenkins

- 이번 개선된 기능에는 FIPS 노드에서 JVM이 작동하는 방식을 제어하는 새로운 Jenkins 환경 변수 **JAVA_FIPS_OPTIONS**가 추가되었습니다. 자세한 내용은 OpenJDK 지원 문서 (BZ#2066019)를 참조하십시오.

1.3.15. 머신 API

1.3.15.1. Amazon EC2 인스턴스 메타데이터 서비스에 대한 구성 옵션

이제 머신 세트를 사용하여 특정 버전의 Amazon EC2 Instance Metadata Service(IMDS)를 사용하는 컴퓨팅 머신을 생성할 수 있습니다. 머신 세트는 IMDSv1 및 IMDSv2 또는 IMDSv2를 사용해야 하는 컴퓨팅 머신을 생성할 수 있습니다.

자세한 내용은 Amazon EC2 인스턴스 메타데이터 서비스에 대한 머신 세트 옵션 을 참조하십시오.

1.3.15.2. Azure Ultra Disk에 대한 머신 API 지원

Azure에서 실행되는 머신 세트를 생성하여 대규모 디스크가 있는 머신을 배포할 수 있습니다. 울트라 디스크가 있는 머신을 데이터 디스크로 배포하거나 트리 내 또는 CSI(Container Storage Interface) PVC를 사용하는 PVC(영구 볼륨 클레임)를 사용하여 배포할 수 있습니다.

자세한 내용은 다음 항목을 참조하십시오.

- 울트라 디스크가 있는 머신을 데이터 디스크로 배포하는 머신 세트
- CSI PVC를 사용하여 울트라 디스크가 있는 머신을 배포하는 머신 세트
- 트리 내 PVC를 사용하여 울트라 디스크가 있는 머신을 배포하는 머신 세트

1.3.15.3. Google Cloud Platform 영구 디스크 유형의 구성 옵션

GCP(Google Cloud Platform) Compute Engine의 **pd-balanced** 영구 디스크 유형이 지원됩니다. 자세한 내용은 머신 세트를 사용하여 영구 디스크 유형 구성 을 참조하십시오.

1.3.15.4. Nutanix 클러스터에 대한 머신 API 지원

Nutanix 클러스터에 대한 새로운 플랫폼 지원에는 Machine API 머신 세트를 사용하여 머신을 관리하는 기능이 포함되어 있습니다. 자세한 내용은 Nutanix에서 머신 세트 생성 을 참조하십시오.

1.3.15.5. 클러스터 API로 머신 관리 (기술 프리뷰)

OpenShift Container Platform 4.11에서는 OpenShift Container Platform에 통합된 업스트림 Cluster API를 AWS 및 GCP 클러스터의 기술 프리뷰로 사용하여 머신을 관리할 수 있는 기능을 도입했습니다. 이 기능은 Machine API를 사용하여 머신 관리하는 것에 대한 대안이나 추가 기능입니다. 자세한 내용은 클러스터 API를 사용하여 시스템 관리를 참조하십시오.

1.3.16. Machine Config Operator

1.3.16.1. MCO는 영역 및 기간 별로 노드를 업데이트합니다.

MCO(Machine Config Operator)는 **topology.kubernetes.io/zone** 레이블을 기반으로 영역별로 영향을 받는 노드를 사전순으로 업데이트합니다. 영역에 둘 이상의 노드가 있으면 가장 오래된 노드가 먼저 업데이트됩니다. 베어 메탈 배포에서와 같이 영역을 사용하지 않는 노드의 경우 노드가 사용 기간으로 업그레이드되며 가장 오래된 노드가 먼저 업데이트됩니다. 이전에는 MCO에서 영역 또는 노드 기간을 고려하지 않았습니다.

자세한 내용은 머신 구성 개요를 참조하십시오.

1.3.16.2. 인증서 갱신 시 일시 중지된 머신 구성 풀에 대한 알림 기능 개선

일시 중지된 MCP(머신 구성 풀)에서 MCO가 만료된 **kube-apiserver-to-kubelet-signer** CA 인증서를 갱신하려고 하면 OpenShift Container Platform 웹 콘솔의 알림 UI에 경고가 표시됩니다. MCP가 일시 중지되면 MCO가 새로 교체된 인증서를 해당 노드로 푸시할 수 없으므로 오류가 발생할 수 있습니다.

자세한 내용은 머신 구성 풀 일시 중지 를 참조하십시오.

1.3.17. 노드

1.3.17.1. Poison Pill Operator를 Self Node Remediation Operator로 대체

OpenShift Container Platform 4.11에는 Poison Pill Operator를 대체하는 Self Node Remediation Operator가 도입되었습니다.

Self Node Remediation Operator는 다음과 같은 향상된 기능을 제공합니다.

- 수정 전략에 따라 별도의 수정 템플릿을 도입합니다.
- 수정에 실패한 경우 마지막 오류 메시지를 캡처합니다.
- 매개변수에 대한 최소 값을 제공하여 Self Node Remediation Operator의 구성 매개변수에 대한 메트릭을 개선합니다.

자세한 내용은 Self Node Remediation Operator를 사용하여 노드 수정 을 참조하십시오.

1.3.17.2. 단일 노드 OpenShift 클러스터의 작업자 노드

이제 단일 노드 OpenShift 클러스터에 작업자 노드를 추가할 수 있습니다. 이는 리소스가 제한적인 환경이나 클러스터에 용량을 추가해야 하는 경우 네트워크 에지에 배포하는데 유용합니다.

자세한 내용은 단일 노드 OpenShift 클러스터의 작업자 노드를 참조하십시오.

1.3.17.3. 디스케줄러는 기본적으로 Pod 제거 시뮬레이션으로 설정됨

기본적으로 디스케줄러는 이제 예측 모드에서 실행되므로 Pod 제거만 시뮬레이션합니다. 디스케줄러 지표를 검토하여 제거할 Pod에 대한 세부 정보를 확인할 수 있습니다.

제거 시뮬레이션을 수행하는 대신 Pod를 제거하려면 디스케줄러 모드를 자동으로 변경합니다.

자세한 내용은 디스케줄러를 사용하여 Pod 제거 를 참조하십시오.

1.3.17.4. 새 디스케줄러 사용자 정의

이번 릴리스에서는 디스케줄러에 대해 다음과 같은 사용자 지정이 도입되었습니다.

- 우선순위 임계값 필터링: 클래스 이름(**thresholdPriorityClassName**) 또는 숫자 값(**thresholdPriority**)에 따라 우선순위 임계값을 설정하거나 우선 순위가 해당 값보다 크거나 같은 Pod를 제거하지 않도록 합니다.
- 네임스페이스 필터링: 디스케줄러 작업을 포함하거나 제외하도록 사용자 생성 네임스페이스 목록을 설정합니다. 보호된 네임스페이스(**openshift-***, **kube-system**,**hypershift**)는 항상 제외됩니다.
- **LowNodeUtilization** 전략의 임계값: **LowNodeUtilization** 전략에 대한 과소 활용 및 과다 활용에 대한 실험 임계값을 설정합니다.

자세한 내용은 디스케줄러를 사용하여 Pod 제거 를 참조하십시오.

1.3.17.5. 노드 유지보수 Operator 기능 개선 사항

Node Maintenance Operator는 다음과 같은 향상된 기능을 제공합니다.

- **NodeMaintenance** CR 작업의 상태와 관련하여 추가 피드백, **drainProgress** 및 **lastUpdate**가 제공됩니다.
- 베어 메탈 노드가 있는 클러스터의 경우 이제 웹 콘솔에서 노드를 유지 관리 모드로 전환하고 유지 관리 모드에서 노드를 재개할 수 있는 더 쉬운 방법을 사용할 수 있습니다.

자세한 내용은 Node Maintenance Operator를 사용하여 노드를 유지 관리 모드로 설정 을 참조하십시오.

1.3.18. 로깅

1.3.18.1. RHV 로깅 시 Red Hat OpenShift (기술 프리뷰)

OpenShift Container Platform 4.11에는 클러스터의 모든 설치 및 oVirt 구성 요소에 대해 자동화된 로그 메시지를 추가하는 RHV API의 새로운 커넥터가 도입되었습니다.

1.3.19. 모니터링

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

1.3.19.1. 모니터링 스택 구성 요소 및 종속 항목에 대한 업데이트

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

- Alertmanager - 0.24.0
- kube-state-metrics - 2.5.0
- Prometheus - 2.36.2
- Prometheus operator - 0.57.0
- Thanos - 0.26.0

1.3.19.2. 경고 규칙 변경

참고

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

- **새로운 사항**
  - **KubePersistentVolumeInodesFillingUp** 경고가 추가되어 기존 **KubePersistentVolumeFillingUp** 경고와 유사하게 작동하지만 볼륨 공간이 아닌 inode에 적용됩니다.
  - **PrometheusScrapeBodySizeLimitHit** 경고를 추가하여 대상이 본문 크기 제한에 도달한 것을 감지합니다.
  - 샘플 제한에 도달한 대상을 탐지하기 위해 **PrometheusScrapeSampleLimitHit** 경고가 추가되었습니다.
- **변경 사항**
  - **kube-state-metrics**에서 업데이트된 지표 **kube_daemonset_status_updated_number_scheduled**을 사용하도록 **KubeDaemonSetRolloutStuck** 경고를 수정했습니다.
  - **KubeJobCompletion** 경고를 **KubeJobNotCompleted**로 교체했습니다. 새 **KubeJobNotCompleted** 경고는 이전 작업이 실패했지만 가장 최근 작업이 성공했을 때 false positive를 방지합니다.
  - 경고 표현식에서 **tunbr** 인터페이스를 제외하도록 **NodeNetworkInterfaceFlapping** 경고를 업데이트했습니다.

1.3.19.3. 사용자 워크로드 모니터링에 대한 경고 라우팅 활성화

이제 클러스터 관리자가 사용자 워크로드 모니터링에 대한 경고 라우팅을 활성화하여 개발자와 기타 사용자가 사용자 정의 프로젝트에 대한 사용자 정의 경고 및 경고 라우팅을 구성할 수 있습니다.

1.3.19.4. 사용자 정의 경고에 대해 전용 Alertmanager 인스턴스 활성화

이제 사용자 정의 프로젝트에 대한 경고만 전송하기 위해 Alertmanager 전용의 별도의 인스턴스를 활성화할 수 있는 옵션이 있습니다. 이 기능을 사용하면 기본 플랫폼 Alertmanager 인스턴스의 부하를 줄이는 데 도움이 되며 기본 플랫폼 경고와 사용자 정의 경고를 더 잘 분리할 수 있습니다.

1.3.19.5. 원격 쓰기 구성에 추가 인증 설정 사용

이제 AWS 서명 버전 4, 사용자 지정 권한 부여 헤더 및 OAuth 2.0과 같은 인증 방법을 사용하여 원격 쓰기 엔드포인트에 액세스할 수 있습니다. 이 릴리스 이전에는 TLS 클라이언트 및 기본 인증만 사용할 수 있었습니다.

1.3.19.6. 웹 콘솔에서 PromQL 쿼리 생성, 검색 및 관리

OpenShift Container Platform 웹 콘솔의 **Observe → Metrics** 페이지의 쿼리 브라우저에는 PromQL 쿼리를 생성, 검색 및 관리할 수 있는 다양한 개선 사항이 추가되었습니다. 예를 들어 관리자는 기존 쿼리를 복제하고 쿼리를 작성하고 편집할 때 자동 완성 제안을 사용할 수 있습니다.

1.3.19.7. 단일 노드 배포에서 ServiceMonitor의 스크랩 간격 두 배로 늘어남

단일 노드 OpenShift Container Platform 배포에서 모든 CCMO(Cluster Monitoring Operator) 제어 ServiceMonitor에 대해 스크랩 간격이 두 배가로 늘어났습니다. 최대 간격은 이제 2분입니다.

1.3.19.8. 플랫폼 모니터링 메트릭을 기반으로 경고 규칙 생성 (기술 프리뷰)

이 릴리스에서는 관리자가 기존 플랫폼 모니터링 메트릭을 기반으로 경고 규칙을 생성할 수 있는 기술 프리뷰 기능이 도입되었습니다. 이 기능을 통해 관리자는 자신의 환경에 맞는 새로운 경고 규칙을 보다 빠르고 쉽게 생성할 수 있습니다.

1.3.19.9. 원격 쓰기 스토리지에 클러스터 ID 레이블 추가

이제 원격 쓰기 스토리지로 전송되는 지표에 클러스터 ID 레이블을 추가할 수 있습니다. 그런 다음 이러한 레이블을 쿼리하여 지표에 대한 소스 클러스터를 식별하고 지표 데이터를 다른 클러스터에서 보낸 유사한 지표 데이터와 구분할 수 있습니다.

1.3.19.10. 사용자 워크로드 모니터링에 대한 페더레이션 엔드포인트를 사용하여 쿼리 지표

이제 Prometheus **/federate** 엔드포인트를 사용하여 클러스터 외부의 네트워크 위치에서 사용자 정의 지표를 스크랩할 수 있습니다. 이번 릴리스 이전에는 페더레이션 엔드포인트에만 액세스하여 기본 플랫폼 모니터링에서 메트릭을 스크랩할 수 있었습니다.

1.3.19.11. 기본 플랫폼 모니터링에 대한 지표 스크랩에 대한 본문 크기 제한 활성화

기본 플랫폼 모니터링에 대해 **enforcedBodySizeLimit** 구성 맵 옵션을 설정하여 메트릭 스크랩에 대한 본문 크기 제한을 활성화할 수 있습니다. 이 설정은 구성된 **enforcedBodySizeLimit** 보다 큰 응답 본문으로 하나 이상의 Prometheus 스크랩 대상 응답이 있는 경우 새 **PrometheusScrapeBodySizeLimitHit** 경고를 트리거합니다. 설정을 사용하면 악의적인 대상이 Prometheus 구성 요소와 클러스터 전체에 미치는 영향을 제한할 수 있습니다.

1.3.19.12. 메트릭 스토리지에 대한 보존 크기 설정 구성

이제 기본 플랫폼 모니터링과 사용자 워크로드 모니터링 모두에 대해 보유된 메트릭 스토리지에 예약된 최대 디스크 공간을 구성할 수 있습니다. 이 릴리스 이전에는 이 설정을 구성할 수 없었습니다.

1.3.19.13. 사용자 정의 프로젝트에서 Thanos Ruler의 보존 기간 구성

사용자 정의 프로젝트에서 Thanos Ruler 데이터에 대한 보존 기간을 구성할 수 있습니다. 이 릴리스 이전에는 기본값 **24h**를 변경할 수 없었습니다.

1.3.20. Network Observability Operator

관리자는 이제 Network Observability Operator를 설치하여 콘솔에서 OpenShift Container Platform 클러

스터의 네트워크 트래픽을 관찰할 수 있습니다. 다른 그래픽 표현에서 네트워크 트래픽 데이터를 보고 모니터링할 수 있습니다. Network Observability Operator는 eBPF 기술을 사용하여 네트워크 흐름을 생성합니다. 네트워크 흐름은 OpenShift Container Platform 정보로 보강되고 로키에 저장됩니다. 자세한 문제 해결 및 분석을 위해 네트워크 트래픽 정보를 사용할 수 있습니다.

자세한 내용은 네트워크 관찰 기능을 참조하십시오.

1.3.21. 확장 및 성능

1.3.21.1. Node Tuning Operator의 워크로드 팁

OpenShift Container Platform 4.11은 다양한 산업 환경의 요구를 충족하기 위해 **PerformanceProfile** 을 조정할 수 있는 Node Tuning Operator의 힌트 메커니즘을 지원합니다. 이번 릴리스에서는 **높은 PowerConsumption** (출력 소비 증가 시 대기 시간이 짧은 대기 시간) 및 **실시간** (최적화 대기 시간으로 지정된 우선순위)에 대해 워크로드 힌트를 사용할 수 있습니다. 이러한 힌트에 대한 true/false 설정의 조합을 사용하여 애플리케이션별 워크로드 프로필 및 요구 사항을 처리할 수 있습니다.

1.3.21.2. etcd 클러스터의 확장 작업 기능 개선

Raft 알고리즘을 사용하면 새로운 **learner** 상태를 사용하여 etcd 멤버를 확장할 수 있습니다. 결과적으로 클러스터 쿼럼을 유지 관리하고, 새 멤버를 추가 및 제거하고, 클러스터 작업을 중단하지 않고 **learners**에게 발생하는 작업을 승격합니다.

OpenShift Container Platform 4.11에는 **AgentServiceConfig** 사용자 정의 리소스의 일부로 **imageStorage** 옵션이 도입되었습니다. 이 옵션을 사용하면 사용자가 이미지 서비스와 함께 사용할 영구 스토리지 클레임 세부 정보를 지정할 수 있으므로 애플리케이션 성능이 향상됩니다.

ClusterImageSet 사용자 정의 리소스의 **releaseImage** 매개변수에서 이제 운영 체제 이미지 버전 확인을 지원합니다. 검색 ISO는 운영 체제 이미지 버전을 releaseImage로 기반으로 하거나 지정된 버전을 사용할 수 없는 경우 최신 버전을 기반으로 합니다.

AgentServiceConfig CR(사용자 정의 리소스)의 **openshiftVersion** 매개변수는 이제 "x.y"(major.minor) 또는 "x.y.z"(major.minor.patch) 형식을 지원합니다.

1.3.21.3. Ingress 컨트롤러(라우터) 활성 상태, 준비 및 시작 프로브 구성

OpenShift Container Platform 4.11에서는 OpenShift Container Platform 인그레스 Operator가 관리하는 라우터 배포를 위해 kubelet의 활성 상태, 준비 상태 및 시작 프로브에 대한 시간 초과 값을 구성할 수 있습니다. 더 큰 시간 초과 값을 설정하는 기능을 사용하면 1초의 짧은 기본 시간 초과로 인해 발생하는 불필요한 재시작 위험을 줄일 수 있습니다.

자세한 내용은 Ingress 컨트롤러 (라우터) 활성 상태, 준비 및 시작 프로브 구성 을 참조하십시오.

1.3.21.4. 새로운 전원 감소 CPU 기능

성능 프로필의 **offlined** 필드에 CPU를 지정하여 Node Tuning Operator를 통해 전력 소비를 줄일 수 있습니다. 자세한 내용은 오프 라인 CPU를 사용하여 전원 소비 감소 를 참조하십시오.

1.3.21.5. Node Observability Operator (기술 프리뷰)

OpenShift Container Platform 4.11에는 노드 Observability Operator가 기술 프리뷰에 도입되었습니다.

Node Observability Operator는 다음을 수행할 수 있는 기능을 제공합니다.

- 작업자 노드에 노드 Observability 에이전트를 배포합니다.

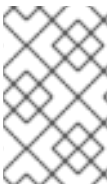
- CRIO-O 및 Kubelet 프로파일링을 트리거합니다.
- 추가 분석을 위해 프로파일링 데이터 파일을 사용할 수 있도록 합니다.

자세한 내용은 노드 Observability Operator를 사용하여 CRI-O 및 Kubelet 프로파일링 데이터 요청 을 참조하십시오.

1.3.21.6. Performance Addon Operator 기능이 Node Tuning Operator로 이동

이전 버전의 OpenShift Container Platform에서 Performance Addon Operator는 애플리케이션에 대한 짧은 대기 시간 성능 튜닝을 제공합니다. OpenShift Container Platform 4.11에서 이러한 함수는 Node Tuning Operator의 일부입니다. Node Tuning Operator는 OpenShift Container Platform 4.11의 표준 설치의 일부입니다. OpenShift Container Platform 4.11로 업그레이드하는 경우 Node Tuning Operator는 시작 시 Performance Addon Operator 및 모든 관련 아티팩트를 제거합니다.

자세한 내용은 Node Tuning Operator를 참조하십시오.



참고

must-gather 명령을 Performance Profile Creator로 실행할 때 **performance-addon-operator-must-gather** 이미지를 계속 사용해야 합니다. 자세한 내용은 must-gather를 사용하여 클러스터에 대한 데이터 수집을 참조하십시오.

1.3.21.7. 짧은 대기 시간 튜닝 설명서 업데이트

이전 버전의 OpenShift Container Platform에서 대기 시간이 짧은 튜닝 설명서에 Performance Addon Operator에 대한 참조가 포함되어 있습니다. Node Tuning Operator는 이제 짧은 지연 시간 조정을 제공하므로 문서 제목이 "낮은 지연 시간 노드를 위한 Performance Addon Operator"에서 "짧은 대기 시간 조정"으로 변경되었으며 이에 따라 이 문서에 대한 여러 상호 참조가 업데이트되었습니다. 자세한 내용은 짧은 대기 시간 조정을 참조하십시오.

1.3.21.8. Hub 및 spoke 클러스터 지원

spoke-of-tree 드라이버 지원이 필요한 허브 및 스포크 배포의 경우 허브 클러스터에 배포된 Special Resource Operator (SRO)를 사용하여 하나 이상의 관리 클러스터에 필요한 커널 모듈 배포를 관리할 수 있습니다. 이는 RHACM(Red Hat Advanced Cluster Management)을 사용하며 더 이상 NFD(Node Feature Discovery)를 사용할 필요가 없습니다. 자세한 내용은 hub-and-spoke 토폴로지를 위한 simple-kmod SpecialResource 빌드 및 실행을 참조하십시오.

1.3.21.9. SRO 클러스터 업그레이드 지원 개선

특수 리소스가 관리되는 클러스터를 업그레이드할 때 사전 업그레이드 사용자 정의 리소스를 실행하여 커널 업데이트를 지원하는 새 드라이버 컨테이너가 있는지 확인할 수 있습니다. 이를 통해 관리 대상 특수 리소스의 잠재적인 중단을 방지할 수 있습니다. 이 기능에 대한 문서는 현재 사용할 수 없으며 나중에 릴리스될 예정입니다.

1.3.21.10. SRO의 디버깅 및 로깅 기능 개선

SRO(Special Resource Operator)에는 문제 해결을 위한 메시지 세부 정보가 포함된 일관된 로그 출력 형식이 포함되어 있습니다.

1.3.21.11. 외부 레지스트리 지원

이번 업데이트 이전에는 SRO가 연결이 끊긴 환경의 레지스트리에 대한 연결을 지원하지 않았습니다. 이 릴리스에서는 드라이버 컨테이너가 OpenShift Container Platform 클러스터 외부의 레지스트리에서 호스팅되는 연결이 끊긴 환경을 지원합니다.

1.3.22. Insights Operator

1.3.22.1. Insights Operator 데이터 수집 기능 개선 사항

OpenShift Container Platform 4.11에서 Insights Operator는 다음과 같은 추가 정보를 수집합니다.

- **images.config.openshift.io** 리소스 정의
- **kube-controller-manager** 컨테이너는 **"Internal error occurred: error resolving resource"** 또는 **"syncing garbage collector with updated resources from discovery"** 오류 메시지가 있는 경우 기록함
- **storageclusters.ocs.openshift.io/v1** 리소스

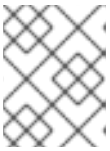
Red Hat은 이러한 추가 정보를 통해 OpenShift Container Platform 기능을 개선하고 Insights Advisor 권장 사항을 향상시킵니다.

1.3.23. 인증 및 권한 부여

1.3.23.1. 지원되는 추가 OIDC 공급자

이제 OpenShift Container Platform에서 다음 OpenID Connect (OIDC) 공급자를 테스트하고 지원합니다.

- Windows Server용 Active Directory Federation Services



참고

현재 사용자 정의 클레임을 사용할 때 OpenShift Container Platform과 함께 Windows Server용 Active Directory Federation Services를 사용할 수 없습니다.

- Microsoft ID 플랫폼(Azure Active Directory v2.0)

참고

현재는 그룹 이름을 동기화해야 하는 경우 Microsoft ID 플랫폼을 사용하는 것은 지원되지 않습니다.

OIDC 공급자의 전체 목록은 지원되는 OIDC 공급자를 참조하십시오.

1.3.23.2. Pod 보안 승인

OpenShift Container Platform에서 Pod 보안 승인이 활성화됩니다.

Pod 승인은 Pod 보안 및 SCC(보안 컨텍스트 제약 조건) 허용에 모두 적용됩니다. Pod 보안 승인은 **privileged** 및 **restricted** 감사 로깅 및 API 경고와 함께 전 세계적으로 실행됩니다.

컨트롤러는 사용자가 생성한 네임스페이스에서 서비스 계정의 SCC 관련 권한을 모니터링하고 Pod 보안 승인 **warn** 및 **audit** 라벨을 사용하여 이러한 네임스페이스에 자동으로 레이블을 지정합니다.

restricted Pod 보안 프로필에 따라 워크로드 보안을 개선하기 위해 이 릴리스에서는 새로운 Pod 보안 허용 제어에 따라 Pod 보안을 적용하는 SCC를 도입합니다. 이러한 SCC는 다음과 같습니다.

- **restricted-v2**
- **hostnetwork-v2**
- **nonroot-v2**

이름이 지정된 이전 SCC에 해당하지만 다음과 같은 향상된 기능이 있습니다.

- **ALL** 기능은 컨테이너에서 삭제됩니다. 이전에는 **KILL,MKNOD,SETUID** 및 **SETGID** 기능만 삭제되었습니다.
- 이제 **NET_BIND_SERVICE** 기능을 명시적으로 추가할 수 있습니다.
- 설정되지 않은 경우 **seccompProfile**은 **runtime/default**로 설정됩니다. 이전 릴리스에서는 이 필드가 비어 있어야 했습니다.
- 보안 컨텍스트에서 **allowPrivilegeEscalation**을 설정하지 않거나 **false**로 설정해야 합니다. 이전에는 **true** 값이 허용되었습니다.

OpenShift Container Platform 4.11에서 **restricted -v2** SCC는 제한된 SCC 대신 새 설치에 사용할 수 있는 기본 SCC가 부여되었습니다. 새 클러스터에서 **restricted -v2** SCC는 제한된 SCC 대신 인증된 모든 사용자에게 사용됩니다. 액세스 권한이 명시적으로 부여되지 않는 한 **restricted** SCC는 새 클러스터의 사용자에게 더 이상 사용할 수 없습니다. OpenShift Container Platform 4.10 또는 이전 버전에 원래 설치된 클러스터에서 인증된 모든 사용자는 OpenShift Container Platform 4.11 이상으로 업그레이드할 때 **제한된** SCC를 사용할 수 있습니다. 이렇게 하면 OpenShift Container Platform의 기본 보안 권한이 보안 단위로 유지되며 업스트림 Kubernetes 프로젝트의 Pod 보안 승인 및 Pod 보안 표준에 맞게 조정되며 업그레이드된 클러스터의 권한은 이전 상태와 일치하도록 유지합니다.

대부분의 네임스페이스에 대한 동기화를 활성화하고 모든 네임스페이스에 대한 동기화를 비활성화할 수 있습니다.

이번 릴리스에서는 **openshift-** 접두사가 있는 네임스페이스에는 적용이 제한되지 않습니다. 이러한 네임스페이스에 대한 제한된 적용은 향후 릴리스에 포함될 예정입니다.

자세한 내용은 Pod 보안 승인 이해 및 관리 를 참조하십시오.

1.4. 주요 기술 변경 사항

OpenShift Container Platform 4.11에는 다음과 같은 주요 기술 변경 사항이 추가되었습니다.

네트워크 흐름 관찰을 위한 네트워크 관찰 Operator
Network Observability Operator는 4.12 버전의 OpenShift Container Platform의 GA(General Availability) 상태이며 OpenShift Container Platform 4.11에서도 지원됩니다.

자세한 내용은 네트워크 관찰 기능을 참조하십시오.

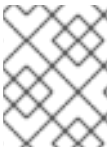
라우터 로드 밸런싱 알고리즘을 설정하기 위한 기본값 업데이트
라우터 로드 밸런싱 알고리즘을 설정하는 **haproxy.router.openshift.io/balance** 변수는 이제 **leastconn**이 아닌 값 **random**으로 설정됩니다. 자세한 내용은 경로별 주석을 참조하십시오.

LegacyServiceAccountTokenNoAutoGeneration이 기본적으로 설정되어 있습니다.
이전 릴리스에서는 서비스 계정이 생성될 때 두 개의 서비스 계정 토큰 시크릿이 생성되었습니다.

- 내부 OpenShift Container Platform 레지스트리에 인증하기 위한 서비스 계정 토큰 시크릿

- Kubernetes API에 액세스하기 위한 서비스 계정 토큰 시크릿

OpenShift Container Platform 4.11부터 Kubernetes API에 액세스하기 위한 두 번째 서비스 계정 토큰 시크릿이 더 이상 생성되지 않습니다. 이는 Kubernetes API에 액세스하기 위한 시크릿 기반 서비스 계정 토큰 자동 생성을 중지하는 Kubernetes 1.24에서 **LegacyServiceAccountTokenNoAutoGeneration** 업스트림 Kubernetes 기능 게이트가 활성화되었기 때문입니다. OpenShift Container Platform 4.11로 업그레이드한 후에는 기존 서비스 계정 토큰 시크릿이 삭제되지 않고 계속 작동합니다.



참고

자동으로 생성된 시크릿을 사용하지 마십시오. 향후 OpenShift Container Platform 릴리스에서 제거될 수 있습니다.

바인딩된 서비스 계정 토큰을 얻기 위해 예상 볼륨과 함께 워크로드가 자동으로 삽입됩니다. 워크로드에 추가 서비스 계정 토큰이 필요한 경우 워크로드 매니페스트에 예상 볼륨을 추가합니다. 자세한 내용은 바인딩된 서비스 계정 토큰 사용을 참조하십시오.

읽을 수 있는 API 오브젝트에서 만료되지 않은 토큰을 보안 노출하는 경우 토큰을 얻기 위해 서비스 계정 토큰 시크릿을 수동으로 생성할 수도 있습니다. 자세한 내용은 서비스 계정 토큰 시크릿 생성 을 참조하십시오.

Operator SDK 1.22.2
OpenShift Container Platform 4.11은 Operator SDK 1.22.2를 지원합니다. 이 최신 버전을 설치하거나 업데이트하려면 Operator SDK CLI 설치 를 참조하십시오.

참고

Operator SDK 1.22.2는 Kubernetes 1.24를 지원합니다.

Operator SDK 1.16.0을 사용하여 이전에 생성되거나 유지 관리되는 Operator 프로젝트가 있는 경우 Operator SDK 1.22.2와의 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

Cluster Operator를 플랫폼 Operator라고 하지 않습니다.
이전에 OpenShift Container Platform 설명서에서는 "platform Operators"라는 대체 이름 지정과 서로 바꿔서 클러스터 Operator를 참조했습니다. 이 두 가지 이름 지정으로 인해 설명되는 Operator 유형에 대한 혼동이 발생할 수 있으므로 **ClusterOperator** API 오브젝트에서 표시되는 클러스터 Operator를 참조할 때 "platform Operator"라는 용어는 더 이상 사용되지 않습니다. OpenShift Container Platform 4.11 및 이전 버전에 대한 문서 세트가 이제 "cluster Operator"라는 용어를 사용하도록 업데이트되었습니다.

예를 들어 Cluster Operators 참조 에서 참조하십시오.

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 4.11에서 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.

아래 표에서 기능은 다음과 같은 상태로 표시되어 있습니다.

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

표 1.1. 사용되지 않거나 삭제된 기능 추적

기능	OCP 4.9	OCP 4.10	OCP 4.11
Operator 카탈로그의 SQLite 데이터베이스 형식	DEP	DEP	DEP
Cluster Samples Operator의 **ImageChangesInProgress** 상태	DEP	DEP	DEP
Cluster Samples Operator의 **MigrationInProgress** 상태	DEP	DEP	DEP
클러스터 로더	DEP	REM	REM
사용자의 RHEL 7 컴퓨팅 머신 가져오기	DEP	REM	REM
Jenkins Operator	DEP	REM	REM
모니터링 스택의 Grafana 구성 요소	-	DEP	REM
모니터링 스택에서 Prometheus 및 Grafana UI에 액세스		DEP	REM
vSphere 6.7 Update 2 또는 이전 버전	DEP	DEP	REM
vSphere 7.0 업데이트 1 이상	-	-	DEP
가상 하드웨어 버전 13	DEP	DEP	REM
VMware ESXi 6.7 업데이트 2 또는 이전 버전	DEP	DEP	REM
VMware ESXi 7.0 업데이트 1 이상	-	-	DEP
snapshot.storage.k8s.io/v1beta1 API 끝점	DEP	DEP	REM
Microsoft Azure 클러스터의 인증 정보 축소	GA	REM	REM
FlexVolume을 사용하는 영구 스토리지	-	DEP	DEP

기능	OCP 4.9	OCP 4.10	OCP 4.11
서비스 계정 토큰 시크릿 자동 생성	GA	GA	REM
설치 페이로드에서 Jenkins 이미지 제거	GA	GA	REM
멀티 클러스터 콘솔 (기술 프리뷰)	-	REM	REM

1.5.1. 더 이상 사용되지 않는 기능

1.5.1.1. 토큰 요청의 OpenShift CLI (oc) 명령 및 플래그가 더 이상 사용되지 않습니다.

토큰 요청의 다음 **oc** 명령 및 플래그는 더 이상 사용되지 않습니다.

- **oc serviceaccounts create-kubeconfig** 명령
- **oc serviceaccounts get-token** 명령
- **oc serviceaccounts new-token** 명령
- **oc registry login** 명령의 **--service-account/-z** 플래그

대신 **oc create token** 명령을 사용하여 토큰을 요청합니다.

1.5.1.2. OpenShift Container Platform 호스트 플랫폼으로 RHV(Red Hat Virtualization)는 더 이상 사용되지 않습니다.

RHV(Red Hat Virtualization)는 향후 OpenShift Container Platform 릴리스에서 더 이상 사용되지 않습니다. RHV의 OpenShift Container Platform 지원은 현재 OpenShift Container Platform 4.14로 예정된 OpenShift Container Platform 릴리스에서 제거될 예정입니다.

1.5.1.3. vSphere 7.0 Update 1 또는 이전 버전에 대한 지원이 더 이상 사용되지 않음

OpenShift Container Platform 4.11에서는 VMware vSphere 7.0 Update 1 또는 이전 버전에 대한 지원이 더 이상 사용되지 않습니다. vSphere 7.0 업데이트 1 이하는 완전하게 지원되지만 Red Hat은 vSphere 7.0 Update 2 이상을 사용할 것을 권장합니다. 버전 8은 지원되지 않습니다.

1.5.1.4. ESXi 7.0 Update 1 또는 이전 버전에 대한 지원은 더 이상 사용되지 않음

OpenShift Container Platform 4.11에서는 VMware ESXi 7.0 업데이트 1 또는 이전 버전에 대한 지원이 더 이상 사용되지 않습니다. EXSi 7.0 Update 1 또는 이전 버전은 완전히 지원되지만 Red Hat은 ESXi 7.0 Update 2 이상을 사용하는 것이 좋습니다.

1.5.1.5. pidsLimit 및 logSizeMax CRI-O 매개변수 지원은 더 이상 사용되지 않습니다.

OpenShift Container Platform 4.11에서 **ContainerRuntimeConfig** CR의 **pidsLimit** 및 **logSizeMax** 필드는 향후 릴리스에서 더 이상 사용되지 않고 제거됩니다. 대신 **KubeletConfig** CR에서 **podPidsLimit** 및 **containerLogMaxSize** 필드를 사용합니다. **podPidsLimit** 필드의 기본값은 **4096** 입니다.

1.5.2. 삭제된 기능

1.5.2.1. OpenShift CLI(oc)에 대한 RHEL 7 지원이 제거되었습니다.

oc(OpenShift CLI)에서 RHEL(Red Hat Enterprise Linux) 7 사용에 대한 지원이 제거되었습니다. RHEL에서 OpenShift CLI(**oc**)를 사용하는 경우 RHEL 8 이상을 사용해야 합니다.

1.5.2.2. OpenShift CLI(oc) 명령이 제거됨

이 릴리스에서는 다음 OpenShift**CLI**(oc) 명령이 제거되었습니다.

- **oc adm migrate etcd-ttl**
- **oc adm migrate image-references**
- **oc adm migrate legacy-hpa**
- **oc adm migrate storage**

1.5.2.3. 모니터링 스택에서 제거된 Grafana 구성 요소

Grafana 구성 요소는 더 이상 OpenShift Container Platform 4.11 모니터링 스택의 일부가 아닙니다. 또는 OpenShift Container Platform 웹 콘솔에서 **Observe → Dashboards**로 이동하여 모니터링 대시보드를 확인합니다.

1.5.2.4. 모니터링 스택에서 제거된 Prometheus 및 Grafana 사용자 인터페이스 액세스

타사 Prometheus 및 Grafana 사용자 인터페이스에 대한 액세스는 OpenShift Container Platform 4.11 모니터링 스택에서 제거되었습니다. 또는 OpenShift Container Platform 웹 콘솔에서 **Observe**를 클릭하여 모니터링 구성 요소에 대한 경고, 메트릭, 대시보드 및 지표 대상을 확인합니다.

1.5.2.5. 가상 하드웨어 버전 13에 대한 지원이 제거되었습니다.

OpenShift Container Platform 4.11에서는 가상 하드웨어 버전 13에 대한 지원이 제거되었습니다. OpenShift Container Platform 4.9에서는 가상 하드웨어 버전 13에 대한 지원이 더 이상 사용되지 않습니다. 가상 하드웨어 버전 15 이상을 사용하는 것이 좋습니다.

1.5.2.6. vSphere 6.7 Update 2 또는 이전 버전에 대한 지원이 제거되었습니다.

OpenShift Container Platform 4.11에서는 VMware vSphere 6.7 Update 2 또는 이전 버전에 대한 지원이 제거되었습니다. vSphere 6.7 Update 2 또는 이전 버전에 대한 지원은 OpenShift Container Platform 4.9에서 더 이상 사용되지 않습니다. Red Hat은 vSphere 7.0 Update 2 이상을 사용하는 것이 좋습니다. 버전 8은 포함되어 있지 않습니다. vSphere 8은 지원되지 않습니다.

1.5.2.7. ESXi 6.7 Update 2 또는 이전 버전에 대한 지원이 제거되었습니다.

OpenShift Container Platform 4.11에서는 VMware ESXi 6.7 Update 2 또는 이전 버전에 대한 지원이 제거되었습니다. OpenShift Container Platform 4.10에서는 ESXi 6.7 Update 2 또는 이전 버전에 대한 지원이 더 이상 사용되지 않습니다. ESXi 7.0 Update 2 이상을 사용하는 것이 좋습니다.

1.5.2.8. 스냅샷 v1beta1 API 엔드 포인트가 제거되었습니다.

OpenShift Container Platform 4.11에서 **snapshot.storage.k8s.io/v1beta1** API 끝점에 대한 지원이 제거되었습니다. OpenShift Container Platform 4.7에서는 **snapshot.storage.k8s.io/v1beta1** API 끝점에 대한 지원이 더 이상 사용되지 않습니다. Red Hat은 **snapshot.storage.k8s.io/v1** 을 사용할 것을 권장합니다. **v1beta1** 으로 생성된 모든 오브젝트는 v1 끝점을 통해 사용할 수 있습니다.

1.5.2.9. 사용자 정의 스케줄러 수동 배포 지원이 제거되었습니다.

이 릴리스에서 사용자 정의 스케줄러를 수동으로 배포하기 위한 지원이 제거되었습니다. Red Hat OpenShift에 Secondary Scheduler Operator를 사용하여 OpenShift Container Platform에 사용자 정의 보조 스케줄러를 배포합니다.

1.5.2.10. OpenShiftSDN을 사용하여 단일 노드 OpenShift 배포 지원이 제거되었습니다.

이 릴리스에서 OpenShiftSDN을 사용하여 단일 노드 OpenShift 클러스터 배포 지원이 제거되었습니다. OVN-Kubernetes는 단일 노드 OpenShift 배포를 위한 기본 네트워킹 솔루션입니다.

1.5.2.11. 설치 페이로드에서 Jenkins 이미지 제거

- OpenShift Container Platform 4.11은 Red Hat이 OpenShift Container Platform 라이프사이클 외부에서 이미지를 생성하고 업데이트할 수 있도록 "OpenShift Jenkins" 및 "OpenShift Agent Base" 이미지를 **registry.redhat.io**의 **ocp-tools-4** 리포지토리로 이동합니다. 이전에는 이러한 이미지가 OpenShift Container Platform 설치 페이로드에 있고 **registry.redhat.io**의 **openshift4** 리포지토리에 있었습니다. 자세한 내용은 OpenShift Jenkins를 참조하십시오.

- OpenShift Container Platform 4.11은 페이로드에서 "OpenShift Jenkins Maven" 및 "NodeJS Agent" 이미지를 제거합니다. 이전에 OpenShift Container Platform 4.10에서는 이러한 이미지를 더 이상 사용하지 않습니다. Red Hat은 더 이상 이러한 이미지를 생성하지 않으며 **registry.redhat.io**의 **ocp-tools-4** 리포지토리에서 사용할 수 없습니다.
  그러나 OpenShift Container Platform 4.11로 업그레이드해도 4.10 및 이전 릴리스의 "OpenShift Jenkins Maven" 및 "NodeJS Agent" 이미지는 제거되지 않습니다. Red Hat은 OpenShift Container Platform 라이프 사이클 정책에 따라 4.10 릴리스 라이프 사이클 종료를 통해 이러한 이미지에 대한 버그 수정 및 지원을 제공합니다.

  자세한 내용은 OpenShift Jenkins를 참조하십시오.

1.5.3. 향후 Kubernetes API 제거

OpenShift Container Platform의 다음 마이너 릴리스에서는 Kubernetes 1.25를 사용할 것으로 예상됩니다. 현재 Kubernetes 1.25는 더 이상 사용되지 않는 몇 가지 **v1beta1** 및 **v2beta1** API를 제거하도록 예정되어 있습니다.

예정된 Kubernetes API 제거 목록은 업스트림 Kubernetes 설명서에서 더 이상 사용되지 않는 API 마이그레이션 가이드를 참조하십시오.

제거하려는 Kubernetes API의 클러스터를 확인하는 방법에 대한 자세한 내용은 Kubernetes API 사용 중단 및 제거를 참조하십시오.

1.6. 버그 수정

베어 메탈 하드웨어 프로비저닝

- 이전 버전에서는 일부 디스크에 RHCOS 이미지를 작성할 때 스파스 영역을 포함하여 **qemu-img**가 전체 디스크에 공간을 할당했습니다. 이는 일부 하드웨어에서 쓰기 프로세스 시간이 연장되었습니다. 이번 업데이트에서는 이미지 생성에서 **qemu-img** 스파스를 비활성화합니다. 결과적으로 이미지 작성에 더 이상 영향을 받는 하드웨어에 시간이 오래 걸리지 않았습니다. (BZ#2002009)

- 이전 버전에서는 **rotational** 필드가 **RootDeviceHints** 에 대해 설정된 경우 호스트는 프로비저닝에 실패할 수 있었습니다. 이번 업데이트를 통해 **RootDeviceHints** 의 **rotational** 필드가 올바르게 복사 및 검사됩니다. 결과적으로 **rotational** 필드를 사용할 때 프로비저닝이 성공합니다.

(BZ#2053721)

- 이전에는 BMC에서 **TransferProtocolType** 속성을 선택적 속성이지만 요청에 명시적으로 설정해야 하므로 Ironic에서 가상 미디어를 사용하여 Nokia OE 20 서버를 프로비저닝할 수 없었습니다. 또한 BMC는 전용 **RedFish** 설정 리소스를 사용하여 부팅 순서를 재정의해야 하지만 대부분의 BMC는 **system** 리소스만 사용해야 합니다. 이 오류는 Nokia OE 20은 vMedia 첨부 파일에 대한 선택적 **TransferProtocolType** 특성이 엄격하게 필요하며 부팅 시퀀스를 재정의하기 위해 **RedFish** 설정 리소스를 사용해야하기 때문에 발생했습니다. 결과적으로 가상 미디어 기반 프로비저닝이 Nokia OE 20에서 실패했습니다. 이 문제에 대한 두 가지 해결 방법이 있습니다.

  1. **TransferProtocolType** 속성이 누락되었음을 나타내는 오류와 함께 vMedia 첨부 요청이 실패하면 요청을 다시 시도한 후 이 속성을 명시적으로 지정합니다.

  2. 시스템에 RedFish 설정 리소스가 있는지 확인합니다. 부팅 시퀀스 재정의에 이를 사용합니다.

  이러한 해결 방법으로 인해 가상 미디어 기반 프로비저닝이 Nokia OE 20 시스템에서 성공합니다. (BZ#2059567)

- 이전에는 OpenShift Container Platform 베어 메탈 IPI 배포를 사용할 때 Ironic API 검사기 이미지가 패시브 다중 경로 설정의 일부인 디스크를 정리하지 못했습니다. 이번 업데이트에서는 활성 또는 수동 스토리지 어레이를 사용 중인 경우 오류를 수정합니다. 결과적으로 고객이 활성 또는 수동 상태인 다중 경로 설정을 사용하려는 경우 OpenShift Container Platform 베어 메탈 IPI를 사용할 수 있습니다. (BZ#2089309)

- 이전에는 Ironic에서 **wwn** 일련 번호를 다중 경로 장치에 일치시킬 수 없었습니다. 결과적으로 장치 매퍼 장치의 **wwn** 일련 번호는 **install-config.yaml** 구성 파일의 **rootDeviceHint** 매개변수에서 사용할 수 없었습니다. 이번 업데이트를 통해 Ironic은 이제 **wwn** 일련 번호를 다중 경로 장치의 고유 식별자로 인식합니다. 결과적으로 **install-config.yaml** 파일의 장치 매퍼 장치에 **wwn** 일련 번호를 사용할 수 있습니다. (BZ#2098392)

- 이번 업데이트 이전에는 Redfish 시스템에 설정 URI가 있는 경우 Ironic 프로비저닝 서비스에서 항상 이 URI를 사용하여 부팅 관련 BIOS 설정을 변경합니다. 그러나 BMC(Baseboard Management Controller)에 설정 URI가 있지만 이 설정 URI를 사용하여 특정 BIOS 설정 변경을 지원하지 않는 경우 베어 메탈 프로비저닝이 실패합니다. OpenShift Container Platform 4.11 이상에서 시스템에 설정 URI가 있는 경우 Ironic은 계속하기 전에 설정 URI를 사용하여 특정 BIOS 설정을 변경할 수 있는지 확인합니다. 그렇지 않으면 Ironic은 시스템 URI를 사용하여 변경 사항을 구현합니다. 이 추가 논리를 통해 Ironic에서 부팅 관련 BIOS 설정 변경 사항을 적용할 수 있으며 베어 메탈 프로비저닝이 성공할 수 있습니다. (OCPBUGS-2052)

빌드

- 이전에는 **BuildConfig** 인스턴스의 **ImageLabel** 이름에 슬래시(/)를 사용하면 오류가 발생했습니다. 이번 수정에서는 검증에 사용되는 유틸리티를 변경하여 문제를 해결합니다. 결과적으로 **BuildConfig** 인스턴스의 **ImageLabel** 이름에 슬래시를 사용할 수 있습니다. (BZ#2105167)

- 이전 버전에서는 **$ oc new-app --search <image_stream_name>** 명령을 사용할 때 **docker.io** 이미지와 관련된 잘못된 메시지가 표시될 수 있었습니다. 이로 인해 OpenShift Container Platform에서 **docker.io** 를 가리키는 이미지 스트림을 사용하지 않기 때문에 사용자에게 혼동이 발생했습니다. 이번 수정에서는 **docker.io**에 대한 참조가 발생하지 않도록 코드 검사를 추가합니다. 결과적으로 해당 명령의 출력에는 메시지가 포함되지 않습니다. (BZ#2049889)

- 이전에는 Shared Resource CSI Driver 지표를 Telemetry 서비스로 내보내지 않았습니다. 결과적으로 공유 리소스 CSI 드라이버의 사용량 지표를 분석할 수 없었습니다. 이번 수정을 통해 공유 리소스 CSI 드라이버 지표가 Telemetry 서비스에 노출됩니다. 결과적으로 공유 리소스 CSI 드라이버의 사용 지표를 수집하고 분석할 수 있습니다. (BZ#2058225)

- 기본적으로 Buildah는 빌드 입력 시크릿을 포함할 수 있는 환경 변수의 내용을 포함하여 로그 파

일에 단계를 출력합니다. **--quiet** build 인수를 사용하여 해당 환경 변수 출력을 억제할 수 있지만 S2I(Source-to-Image) 빌드 전략을 사용하는 경우 이 인수를 사용할 수 없습니다. 현재 릴리스에서는 이 문제가 해결되었습니다. 환경 변수 출력을 표시하지 않으려면 빌드 구성에서 **BUILDAH_QUIET** 환경 변수를 설정합니다.

```
sourceStrategy:
...
  env:
    - name: "BUILDAH_QUIET"
      value: "true"
```

- 이번 업데이트 이전에는 **$ oc new-app --search <image_stream_name> 명령을 사용하여 컨테이너 이미지 "docker.io/tekton /<image_name>:<tag>"** 에 액세스할 수 없다는 경고가 표시되었습니다. 이로 인해 OpenShift Container Platform에 **docker.io** 를 가리키는 이미지 스트림이 있다고 혼동되었습니다. 이번 업데이트에서는 'docker.io'에 대한 혼란스러운 참조를 방지하기 위해 코드 검사를 추가하여 문제를 해결합니다. 이제 해당 명령의 출력에 **docker.io** 에 대한 메시지가 포함되지 않습니다(BZ#2049889)

클라우드 컴퓨팅

- CSR (**CertificateSigningRequest**) 리소스 갱신은 Kubernetes 컨트롤러 관리자에서 처리하며 Cluster Machine Approver Operator에 의해 올바르게 보류 중이어서 **mapi_current_pending_csr** 지표의 값이 **1**로 증가합니다. 이전 버전에서는 Kubernetes 컨트롤러 관리자가 CSR을 승인할 때 Operator는 이를 무시하고 지표를 변경하지 않고 그대로 유지했습니다. 그 결과 Operator가 다음에 조정될 때까지 **mapi_current_pending_csr** 지표가 **1**에 고정되었습니다. 이번 릴리스에서는 다른 컨트롤러의 CSR 승인이 항상 조정되어 지표 업데이트를 위해 조정되고 모든 조정 후 **mapi_current_pending_csr** 메트릭 값이 업데이트됩니다. (BZ#2047702)

- 이전에는 AWS SDK 내의 알려진 리전 목록에 포함된 리전만 검증되었으며 다른 리전을 지정하면 오류가 발생했습니다. 즉, 새로운 리전이 추가되었으므로 새 지역 정보를 포함하도록 SDK가 업데이트될 때까지 사용할 수 없었습니다. 이번 릴리스에서는 리전이 인식되지 않는 경우 사용자에게 경고하는 설정으로 리전이 검증됩니다. 결과적으로 새 지역에는 경고 메시지가 표시될 수 있지만 즉시 사용할 수 있습니다. (BZ#2065510)

- 이전에는 Cluster Machine Approver Operator에서 **"Approved"** 상태 조건을 조건 목록에 추가했습니다. 결과적으로 Kubernetes API 서버는 **[SHOULD NOT HAPPEN] failed to update managedFields** 메시지가 포함된 오류를 기록했습니다. 이번 릴리스에서는 목록에 추가하기 전에 조건을 확인하도록 Operator가 업데이트되어 필요한 경우에만 조건을 업데이트합니다. 결과적으로 **CertificateSigningRequest** 리소스에서 조건이 더 이상 중복되지 않으며 Kubernetes API 서버는 더 이상 중복에 대한 오류를 기록하지 않습니다. (BZ#1978303)

- 이전 버전에서는 RHOSP(Red Hat OpenStack Platform) 버전 16에 존재하는 Cisco ACI neutron 구현의 결함으로 인해 지정된 네트워크에 속한 서브넷 쿼리가 예기치 않은 결과를 반환했습니다. 결과적으로 RHOSP Cluster API 공급자는 동일한 서브넷에 중복된 포트가 있는 인스턴스를 프로비저닝하여 프로비저닝에 실패할 수 있었습니다. 이번 릴리스에서는 RHOSP Cluster API 공급자의 추가 필터링을 통해 서브넷당 여러 개의 포트가 없으므로 Cisco ACI를 사용하여 RHOSP 버전 16에 OpenShift Container Platform을 배포할 수 있습니다. (BZ#2033862)

- 이전에는 RHOSP(Red Hat OpenStack Platform) Machine API 공급자가 프록시 환경 변수 지시문을 사용하지 않아 HTTP 또는 HTTPS 프록시 뒤에 설치에 실패했습니다. 이번 릴리스에서는 공급자는 프록시를 통해서만 송신 트래픽이 허용되는 제한된 환경에서 프록시 지시문 및 기능을 올바르게 따릅니다. (BZ#2046133)

- 이전에는 OpenShift Container Platform 4.9에서 4.10으로 업그레이드할 때 여러 컨트롤러 간의 불일치로 인해 버전 번호가 올바르지 않았습니다. 결과적으로 버전 번호가 일치하지 않았습니다.

이번 릴리스에서는 버전 번호에 대한 일관된 읽기가 적용되어 클러스터 Operator 상태에서 릴리스 버전이 안정적으로 제공됩니다. (BZ#2059716)

- 이전에는 AWS Machine API 공급자의 로드 밸런서 대상 누출이 발생할 수 있었습니다. 컨트롤 플레인 시스템을 교체할 때 IP 기반 로드 밸런서 첨부 파일이 로드 밸런서 등록 내에 남아 있을 수 있기 때문입니다. 이번 릴리스에서는 AWS에서 Amazon EC2 인스턴스를 제거하기 전에 IP 기반 로드 밸런서 첨부 파일이 로드 밸런서에서 제거됩니다. 결과적으로 누수를 피할 수 있습니다. (BZ#2065160)

- 이전 버전에서는 업그레이드 중에 Machine API를 통해 생성된 새 머신이 HW-13으로 기본 설정되어 클러스터의 성능이 저하되었습니다. 이번 릴리스에서는 머신 컨트롤러가 템플릿 복제에서 머신 생성 중에 가상 머신의 하드웨어 버전을 확인합니다. 템플릿의 하드웨어 버전이 OpenShift Container Platform 4.11 이상 버전에서 지원되는 최소 하드웨어 버전인 15 미만이면 시스템이 **failed** 상태가 됩니다. (BZ#2059338)

- 이전 버전에서는 Azure 가용성 세트의 절차 이름 생성기가 최대 80자 제한을 초과했습니다. 이로 인해 Machine API가 여러 가용성 세트를 생성하지 않고 이름 잘림 중에 동일한 세트를 재사용할 수 있습니다. 이번 릴리스에서는 이름이 80자를 초과하여 클러스터 이름이 설정되지 않고 클러스터 이름이 중복되지 않도록 할 수 있습니다. 결과적으로 Azure 가용성 세트는 더 이상 예기치 않은 이름 생성기로 잘리지 않습니다. (BZ#2093044)

- 리더 선택 매개변수를 설정하지 않고 Cluster Autoscaler Operator에서 클러스터 자동 스케일러를 배포했기 때문에 클러스터 자동 스케일러가 예기치 않게 실패하고 클러스터 재시작 후 다시 시작할 수 있었습니다. 이번 수정으로 Cluster Autoscaler Operator는 이제 잘 정의된 리더 선택 플래그와 함께 클러스터 자동 스케일러를 배포합니다. 결과적으로 클러스터를 다시 시작한 후 클러스터 자동 스케일러가 예상대로 작동합니다. (BZ#2063194)"

- 이전 버전에서는 CSR(인증서 서명 요청) 갱신이 **kube-controller-manager** 에 의해 처리되었으며 시스템 승인자가 보류 중인 상태로 올바르게 남아 이로 인해 **mapi_current_pending_csr** 이 **1** 로 증가했습니다. 이후 **kube-controller-manager** 가 CSR을 승인했지만 머신 승인자는 이를 무시하며 지표는 변경되지 않았습니다. 그 결과 **mapi_current_pending_csr** 은 다른 머신 승인자가 조정될 때까지 **1** 에 고정되었습니다. 이번 업데이트를 통해 CSR 승인이 다른 컨트롤러에서 조정되어 메트릭을 올바르게 업데이트합니다. 그 결과 **mapi_current_pending_csr** 은 조정마다 항상 최신 상태가 됩니다. (BZ#2072195)

- 이전 버전에서는 다른 Operator가 성능 저하된 것으로 보고되어도 클러스터 설치 시 시작된 작업자 노드 수가 충분하지 않은 경우 Machine API Operator가 성능이 저하된 것으로 보고하지 않았습니다. 이번 릴리스에서는 Machine API Operator가 성능 저하된 것으로 보고되고 이 시나리오의 설치 로그에 오류가 게시됩니다. 결과적으로 Machine API Operator가 실패한 Operator 목록에 표시되고 사용자는 작업자 노드가 충분하지 않은 이유로 머신의 상태를 검사합니다. (BZ#1994820)

- Machine API Operator에서 프록시 환경 변수 지시문을 준수하지 않았기 때문에 HTTP 또는 HTTPS 프록시 뒤의 설치에 실패했습니다. 이번 수정으로 Machine API Operator의 HTTP 전송 논리가 이제 프록시 지시문을 따릅니다. 결과적으로 Machine API Operator는 이제 프록시를 통해서만 송신 트래픽이 허용되는 제한된 환경에서 작동합니다. (BZ#2082667)

- 이전에는 태그가 수천 개이고 API 로드가 많은 클러스터의 vSphere에 설치되지 않았습니다. 이제 머신 컨트롤러에서 특정 OpenShift Container Platform 설치와 관련된 태그만 쿼리합니다. 결과적으로 OpenShift Container Platform은 이러한 클러스터의 vSphere에 올바르게 설치됩니다. (BZ#2097153)

- kubelet은 노드 영역 레이블을 가져오기 위해 vCenter에 문의해야 하므로 vCenter 인증 정보가 시크릿에 저장된 경우 kube 클라이언트가 동시에 생성되지 않았기 때문에 kubelet을 시작할 수 없었습니다. 결과적으로 **cloud-provider-config** 구성 맵을 편집할 때 노드를 재부팅하지 않은 경우 노드가 작동하지 않았습니다. 이번 수정으로 인증 정보가 시크릿에 저장된 경우 노드 등록 후 kubelet이 영역 라벨을 얻습니다. 결과적으로 노드가 예상대로 재부팅됩니다. (BZ#1902307)

- 이전에는 **timeout** 옵션 부족으로 인해 컨트롤러 차단으로 인해 vCenter가 중단되지 않거나 매우 느리게 응답할 수 있었습니다. 이번 릴리스에서는 vSphere 머신 컨트롤러 내의 vCenter 클라이언트에 대한 **timeout** 옵션이 추가되었습니다. (BZ#2083237)

Cluster Version Operator

- 이전 버전에서는 업그레이드 중 오류가 발생하면 CVO(Cluster Version Operator)가 현재 릴리스 매니페스트를 조정하지 않았습니다. 이번 업데이트를 통해 릴리스 로드는 조정과 분리되므로 후자는 릴리스 로드 상태를 명확히하기 위해 이전 및 새 조건 **Releasedatabinded**를 차단하지 않습니다. (BZ#1822752)

Console Metal3 플러그인

- 이전에는 UI에 **bootMode** 전략을 설정하는 옵션이 누락되었습니다. 결과적으로 UI는 항상 기본값(UEFI) 부팅 전략을 사용하므로 일부 유형의 베어 메탈 배포 유형을 부팅하는 데 문제가 발생했습니다. 이번 업데이트에서는 **베어 메탈 호스트 추가** 양식에 새 필드를 노출하여 적절한 부팅 모드 전략을 선택합니다. 결과적으로 베어 메탈 머신이 올바르게 시작됩니다. (BZ#2091030)

- 이전에는 노드 유지보수 기능이 새 프로젝트로 이동되어 API가 변경되었습니다. 결과적으로 노드 유지보수의 작동이 중지되었습니다. 이번 업데이트에서는 새 API에서 제대로 작동하도록 코드가 수정되었습니다. 결과적으로 노드 유지보수가 다시 작동합니다. (BZ#2090621)

- 이전에는 지원 설치 프로그램에서 생성된 클러스터의 경우 2일차 (Day2)의 작업에게 가 기본 베어 메탈 호스트 및 머신 리소스가 누락되었습니다. 결과적으로 작업자 노드의 세부 정보를 표시하려고 할 때 UI가 실패했습니다. 이번 업데이트를 통해 베어 메탈 호스트 및 머신 리소스가 더 정상적으로 처리되고 UI에 사용 가능한 모든 세부 정보가 표시됩니다. (BZ#2090993)

DNS(Domain Name System)

- 토폴로지 인식 힌트는 OpenShift Container Platform 4.11의 새로운 기능으로 **EndpointSlice** 컨트롤러가 컨테이너 네트워크 인터페이스(CNI)에 대한 힌트를 서비스 엔드포인트로 라우팅해야 하는 방법에 대한 힌트를 지정할 수 있습니다. DNS Operator는 클러스터 DNS 서비스에 대한 토폴로지 인식 힌트를 활성화하지 않았습니다. 그 결과 CNI 네트워크 공급자는 DNS 트래픽을 영역 또는 노드에 로컬로 유지하지 않았습니다. 이번 수정으로 DNS Operator가 클러스터 DNS 서비스에 대한 토폴로지 인식 힌트를 지정하도록 업데이트되었습니다. (BZ#2095941)

- 이전에는 kubelet에서 노드 호스트에서 **/etc/resolv.conf**를 기반으로 Pod의 기본 **/etc/resolv.conf**를 생성했습니다. 결과적으로 잘못된 형식의 **resolv.conf** 파일을 사용하면 확인자가 **resolv.conf**를 구문 분석하지 않아 Pod에서 DNS 확인이 손상될 수 있습니다. 이번 업데이트를 통해 kubelet에서 **resolv.conf** 파일을 수락하고 Pod에서 유효한 **resolv.conf** 파일을 가져옵니다. (BZ#2063414)

- 이전에는 DNS Operator에서 DNS Pod에 **cluster-autoscaler.kubernetes.io/enable-ds-eviction** 주석을 설정하지 않았습니다. 결과적으로 클러스터 자동 스케일러는 노드를 제거하기 전에 노드에서 DNS Pod를 제거하지 않았습니다. 이번 업데이트를 통해 DNS Operator가 **cluster-autoscaler.kubernetes.io/enable-ds-eviction** 주석을 DNS Pod에 추가하도록 변경되었습니다. 이제 클러스터 자동 스케일러로 노드를 제거하기 전에 노드에서 DNS Pod를 제거할 수 있습니다. (BZ#2061244)

이미지 레지스트리

- 이전에는 이미지 레지스트리가 정확히 일치하는 경우에만 소스로 **ImageContentSourcePolicy** (ICSP)를 사용했습니다. 모든 하위 리포지토리에 대해 동일한 소스 파일을 가져와야 했습니다. ICSP 이름과 경로가 하위 리포지토리와 일치하지 않았습니다. 그 결과 이미지가 사용되지 않았습니다. 이제 ICSP가 미러링된 이미지를 사용할 수 있는 하위 리포지토리에 성공적으로 적용됩니다. (BZ#2014240)

- 이전에는 pruner가 실패하면 pruner가 성공적으로 실행될 때까지 이미지 레지스트리 Operator가 성능이 저하된 것으로 보고되었습니다. 이번 업데이트를 통해 Operator는 pruner에 대한 복원력이 향상됩니다. (BZ#1990125)

- 이전에는 ICSP(**ImagetentSourcePolicy**)를 적용할 때 레지스트리가 정확히 일치했습니다. 이번 업데이트를 통해 ICSP가 하위 리포지터리에 적용되고 미러가 이제 예상대로 작동합니다. (BZ#2014240)

- 이전에는 Image Registry Operator가 RHOSP의 AWS S3에서 작동하지 않았습니다. 이번 업데이트를 통해 이미지 레지스트리 Operator는 모든 플랫폼에서 AWS S3를 신뢰합니다. (BZ#2007611)

- 이전에는 OpenShift Container Platform 이미지 레지스트리가 Ceph Radosgw에서 작동하지 않았습니다. 이번 업데이트를 통해 이미지 레지스트리는 Ceph Radosgw에서 작동합니다. (BZ#1976782)

- 이전에는 Image Registry Operator에서 데이터를 사용할 수 없는 것처럼 업스트림 레지스트리에서 **429** 오류 메시지를 해석했습니다. Operator는 **429 Too Many Requests** 대신 **404 Not Found** 메시지를 반환했습니다. 이번 업데이트를 통해 관리자가 요청을 재시도할 수 있도록 적절한 **429 Too Many Requests** 메시지가 반환됩니다. (BZ#1923536)

- 이전에는 Image Registry Operator를 CloudFront를 구성하는 데 사용할 수 없었습니다. 이번 업데이트를 통해 Image Registry Operator에서 CloudFront를 구성할 수 있습니다. (BZ#2065224)

- 이전에는 KMS 암호화가 활성화되었지만 가져오지 않은 경우 Image Registry Operator에서 이미지를 푸시했습니다. 이번 업데이트를 통해 KMS 암호화를 활성화된 상태에서 이미지를 푸시하고 가져올 수 있습니다. (BZ#2048214)

- 이전에는 인증 정보가 제공되지 않아 Image Registry Operator에서 익명으로 공용 이미지를 가져올 수 없었습니다. 이번 업데이트를 통해 고객은 익명으로 공개 이미지를 가져올 수 있습니다. (BZ#2060605)

- 이전에는 이미지 레지스트리 Operator에서 **ap-southeast-3** AWS 리전을 사용할 수 없었습니다. 이번 업데이트를 통해 레지스트리를 **ap-southeast-3** 으로 구성할 수 있습니다. (BZ#2065552)

설치 프로그램

- 이전 버전에서는 사용자가 기간으로 OpenShift Container Platform 클러스터 이름을 지정한 경우 설치에 실패했습니다. 이번 업데이트에서는 설치 프로그램에 검증 검사가 추가되어 클러스터 이름에 기간이 있는 경우 오류를 반환합니다. (BZ#2084580)

- 이전 버전에서는 설치 프로그램을 사용하여 **install-config.yaml** 파일을 만들 때 사용자가 AWS **us-gov-east-1** 리전을 선택할 수 있었습니다. 이로 인해 설치 프로그램이 공용 AWS 리전의 **install-config.yaml** 파일을 생성하는 데만 사용할 수 있었기 때문에 배포가 실패했습니다. 이번 업데이트에서는 공용 AWS 클라우드에서 지원하지 않는 설치 프로그램에서 AWS 리전을 모두 제거합니다. (BZ#2048222)

- 이전에는 설치 프로그램을 사용하여 **install-config.yaml** 파일을 만들 때 **ap-north-east-3** 리전을 선택할 수 없었습니다. 이 문제를 발생시킨 AWS SDK가 업데이트되어 사용자가 **ap-north-east-3** 리전을 선택할 수 있습니다. (BZ#1996544)

- 이전에는 설치 프로그램에서 API 가상 IP 주소에 대한 DNS 레코드를 생성하지 않았기 때문에 Azure Stack Hub에 프라이빗(내부) OpenShift Container Platform 클러스터를 설치할 수 없었습니다. 이번 업데이트에서는 이 문제가 발생한 잘못된 검사를 제거합니다. 이제 설치 프로그램에서 프라이빗 클러스터에 대한 DNS 레코드를 올바르게 생성합니다. (BZ#2061549)

- 이전에는 IBM Cloud VPC 클러스터를 설치 제거해도 예기치 않은 결과가 발생할 수 있었습니다. 사용자가 클러스터 (cluster 1)를 설치 제거하면 클러스터 1의 이름 (example)이 클러스터 2

(myexample)의 이름의 하위집합이거나 또는 두 클러스터가 기본 도메인을 공유하는 경우 다른 클러스터(cluster 2)의 DNS 레코드가 제거되었습니다. 이번 업데이트에서는 이 동작을 올바르게 수행합니다. 제거 중인 클러스터와 관련된 리소스만 제거됩니다. (BZ#2060617)

- 이전에는 Azure Stack Hub에서 Standard_LRS 이외의 디스크 유형을 지원하지 않았습니다. 이번 업데이트에서는 디스크 유형을 사용자 지정할 수 있는 기능이 추가되어 클러스터의 수동 사용자 정의 없이 기본 디스크 유형을 가질 수 있습니다. 이로 인해 디스크 유형을 하드 코딩하는 방식에서 사용자로부터의 입력을 수락하고 Stack Hub API에 대해 검증하는 방식으로 전환되었습니다. (BZ#2061544)

- 이전 버전에서는 클러스터를 삭제할 때 프라이빗 route5 호스팅 영역의 ID가 호스팅 영역에서 DNS 레코드가 삭제될 때 잘못 보고되었습니다. 이로 인해 제거자 로그에 잘못된 호스트 영역 ID가 보고되었습니다. 이번 업데이트에서는 로그에서 올바른 호스트 영역 ID를 사용합니다. 결과적으로 로그는 기본 도메인의 호스팅 영역에서 DNS 레코드를 제거할 때 올바른 호스팅 영역 ID를 표시합니다. (BZ#1965969)

- 이전에는 AWS 사용자 정의 서비스 엔드 포인트를 요청할 때 시스템 프록시 설정이 고려되지 않았습니다. 이번 업데이트에서는 AWS 사용자 지정 서비스 엔드 포인트에 대한 **HEAD** 요청과 함께 시스템 프록시 설정을 고려하도록 AWS 사용자 지정 서비스 엔드포인트 검증을 구성합니다. 결과적으로 사용자 시스템에서 AWS 사용자 지정 서비스 엔드 포인트에 액세스할 수 있습니다. (BZ#2048451)

- 이전에는 설치 프로그램에서 설치 프로그램 호스트의 **$PATH** 에 Terraform 공급자를 사용했습니다. 따라서 설치 프로그램에 포함된 공급자가 아닌 잘못된 버전 또는 공급자를 사용하는 **$PATH** 에 Terraform 공급자가 있으면 설치에 실패합니다. 이번 업데이트를 통해 설치 프로그램은 공급자를 알려진 디렉터리에 포함시키고 알려진 디렉터리를 사용하도록 Terraform을 설정합니다. 결과적으로 설치 프로그램이 항상 알려진 디렉터리의 공급자를 사용하므로 설치가 성공적으로 수행됩니다. (BZ#1932812)

- 이전에는 새 로드 밸런서를 업데이트할 때 AWS Terraform 공급자에 궁극적으로 일관성 문제가 있었습니다. 따라서 새 로드 밸런서에 액세스하려고 할 때 설치에 실패합니다. 이번 수정으로 설치 프로그램이 업스트림 Terraform 공급자로 업데이트되어 최종 일관성이 보장됩니다. 이로 인해 설치에 실패하지 않습니다. (BZ#1898265)

- 이전 버전에서는 설치 프로그램에 할당량 및 권한을 확인하는 필수 API 목록이 있었으며, 목록에 권한을 제공하지 않은 경우 실패한 몇 가지 불필요한 API가 포함되어 있었습니다. 이번 업데이트를 통해 API 목록이 **optional** API에 대해 액세스할 수 없는 **required** 및 **optional**로 분할됩니다. **optional** API에 대한 경고 메시지가 표시됩니다. (BZ#2084280)

- 이전에는 **.apps** 항목에 설치 프로그램에서 지정된 클러스터에 대해 생성된 모든 리소스를 격리하고 삭제하는 데이터베이스에서 코드를 삭제하는 데 사용한 태그 **kubernetes.io_cluster<infraID>**가 없었습니다. 이번 업데이트를 통해 생성 시 클러스터 Ingress Operator에 태그가 추가되어 항목을 삭제할 수 있습니다. (BZ#2055601)

- 이전에는 내부 게시 전략을 사용할 때 **openshift-install** 명령이 실패했습니다. 이번 업데이트를 통해 **openshift-install** 명령이 더 이상 실패하지 않습니다. (BZ#2047670)

- 이전에는 새로 생성된 VPC(Virtual Private Clouds)로 업데이트할 때 AWS Terraform 공급자에 최종 일관성 문제가 있었습니다. 그 결과 VPC에 액세스하려고 할 때 설치 프로그램이 실패했습니다. 이번 업데이트를 통해 설치 프로그램이 업스트림 Terraform 공급자로 업데이트되고 설치가 실패하지 않습니다. (BZ#2043080)

- 이전에는 새로 생성된 네트워크 인터페이스로 업데이트할 때 AWS Terraform 공급자에 최종 일관성 문제가 발생했습니다. 이로 인해 설치에서 네트워크 인터페이스에 액세스하지 못했습니다. 이번 업데이트를 통해 최종 일관성 및 설치를 수락하도록 Terraform 공급자가 업데이트되지 않습니다. (BZ#2047741)

- 이전에는 설치 관리자 프로비저닝 인프라를 사용하여 VMware 클러스터를 설치할 때 **corespersocket** 값이 **numCores** 값보다 높을 수 있었습니다. 이로 인해 설치 중에 예기치 않은 결과가 발생할 수 있습니다. 이번 업데이트를 통해 사용자는 클러스터를 생성하기 전에 이러한 값을 수정할 수 있는 경고가 표시됩니다. (BZ#2034147)

- 이전에는 AWS 클러스터 설치 중에 드문 버그로 인해 불일치가 발생했습니다. 이를 피하기 위해 설치 프로그램이 업데이트되었습니다. (BZ#2046277)

- 이전 버전에서는 지원되는 사용자 정의 태그 수가 8이었으며 예약된 OpenShift Container Platform 태그는 AWS 리소스에 대해 2였습니다. 이번 릴리스에서는 지원되는 사용자 정의 태그 수가 25개이며 예약된 OpenShift Container Platform 태그는 AWS 리소스의 경우 25개입니다. 이제 설치 중에 최대 25개의 사용자 태그를 추가할 수 있습니다. (CFE#592)

- 이전에는 설치 관리자 프로비저닝 인프라를 사용하여 Azure에 설치할 때 부트스트랩 머신에서 기본 크기 및 인스턴스 유형을 사용했습니다. 이번 업데이트를 통해 부트스트랩 시스템은 컨트롤 플레인 시스템의 크기와 인스턴스 유형을 사용합니다. 이제 설치 구성의 컨트롤 플레인 설정을 수정하여 부트스트랩 시스템의 크기 및 인스턴스 유형을 제어할 수 있습니다. (BZ#2026356)

- 이전에는 설치 프로그램에서 Terraform에 모호한 네트워크 이름을 제공했습니다. 이로 인해 Terraform이 사용할 올바른 네트워크를 결정할 수 없습니다. 이 업데이트를 통해 설치 프로그램은 설치가 성공할 수 있도록 Terraform에 고유한 네트워크 ID를 제공합니다. (BZ#1918005)

- 이전에는 AWS에 클러스터를 설치할 때 종속 NAT 게이트웨이를 생성하기 전에 컨트롤 플레인 머신이 생성되어 설치가 실패할 수 있었습니다. 이번 업데이트를 통해 Terraform은 컨트롤 플레인 시스템을 생성하기 전에 NAT 게이트웨이가 생성되었는지 확인합니다. 이렇게 하면 설치에 성공할 수 있습니다. (BZ#2049108)

- 이전 버전에서는 기본 OSN 네트워크가 아닌 OVN 네트워크를 사용한 경우 필요한 최대 시간보다 오래 걸리기 때문에 스케일 업 작업이 실패했습니다. 이번 업데이트에서는 작업을 완료할 수 있도록 확장 작업 동안 재시도 횟수를 두 배로 늘립니다. (BZ#2090151)

- 이전 버전에서는 데이터베이스에서 여러 클러스터를 병렬로 삭제하려고 하면 **vmware** 및 **govmomi** 라이브러리의 버그로 인해 삭제 프로세스가 실패했습니다. 버그로 인해 클러스터의 태그 중 하나가 삭제되어 삭제 프로세스에서 태그를 찾을 수 없는 경우 404 오류가 발생했습니다. 이번 업데이트에서는 찾을 수 없는 태그를 무시하고 오류 없이 완료되도록 삭제 프로세스를 계속합니다. (BZ#2021041)

- 이번 업데이트를 통해 RHV(Red Hat Virtualization)의 OpenShift Container Platform은 설치 관리자 프로비저닝 인프라의 컨트롤 플레인 및 작업자 노드에 대해 사전 할당된 디스크를 지원합니다. 로드가 많은 환경에서 사전 할당된 디스크는 etcd 및 기타 구성 요소를 위한 성능을 얻을 수 있습니다. (BZ#2035334)

- 이전 버전에서는 여러 클러스터를 병렬로 삭제하려고 하면 **vmware/govmomi** 라이브러리의 버그로 인해 프로세스가 실패했습니다. 버그로 인해 클러스터 태그가 삭제되어 삭제 프로세스에서 태그를 찾을 수 없는 경우 **404** 오류가 발생했습니다. 이번 업데이트에서는 찾을 수 없는 태그를 무시하고 계속 삭제되어 오류 없이 완료될 수 있습니다. (BZ#2021041)

- 이전에는 VMware vSphere의 설치 방법에 구성 파일을 생성하는 동안 네트워크를 확인하는 검증 방법이 포함되었습니다. 이로 인해 사용자 프로비저닝 인프라 및 인프라 프로비저닝의 일부로 네트워크를 생성할 수 있는 기타 설치 방법에 대한 오류가 발생했습니다. 이 경우 구성 파일이 생성될 때 네트워크가 존재하지 않을 수 있었습니다. 이번 수정에서는 설치 프로그램에서 프로비저닝한 인프라 설치에서만 네트워크 검증을 수행하도록 설치 프로그램을 업데이트합니다. 결과적으로 사용자가 프로비저닝한 인프라 및 기타 설치 방법은 네트워크 존재와 관계없이 구성 파일을 생성할 수 있습니다. (BZ#2050767)

- 이전에는 **runc**에 **libseccomp** 2.5 이상에 대한 버전 종속성이 있었기 때문에 버전 8.3 이상을 사용하여 운영 체제가 설치되고 8.4 이상으로 완전히 업데이트되지 않은 문제가 발생했습니다. 이번

업데이트를 통해 RHEL 호스트가 성공적으로 설치되고 초기 버전의 패키지에 문제가 발생하지 않습니다. (BZ#2060147)

- 이전에는 설치 프로그램에서 상대 경로를 통해 네트워크 리소스를 terraform으로 지정했습니다. 네트워크 리소스가 폴더에 중첩된 경우 테라폼 공급자가 리소스를 찾을 수 없습니다. 이번 업데이트를 통해 이제 네트워크 리소스가 ID로 지정되고 설치에 성공합니다. (BZ#2063829)

- 이전에는 vSphere RHCOS 이미지에 **/etc/resolv.conf** 파일이 없었습니다. 이로 인해 기본 **networkmanager** 설정이 **/etc/resolv.conf**에 대한 오류를 표시했습니다. 이번 업데이트를 통해 **rc-manager=unmanaged** 값이 설정되고 **networkmanager** 설정은 **/etc/resolv.conf**로 직접 이동하지 않습니다. (BZ#2029438)

- 이전에는 AWS(Amazon Web Services)에 필요하지 않기 때문에 설치 프로그램에서 클라우드 공급자 구성을 생성하지 않았습니다. 이로 인해 Kubernetes API 서버가 클라우드 공급자 구성없이 오류를 제공하게 되었습니다. 이번 업데이트를 통해 AWS의 빈 클라우드 공급자 구성이 생성되고 Kubernetes API 서버가 성공적으로 실행될 수 있습니다. (BZ#1926975)

Kubernetes API 서버

- 이전에는 **KubeAPIErrorBudgetBurn** 계산에 대해 스트리밍에 사용되는 장기 실행 요청이 고려되었습니다. 그 결과 **KubeAPIErrorBudgetBurn**의 경고가 트리거되어 false positive가 발생합니다. 이번 업데이트에서는 **KubeAPIErrorBudgetBurn** 계산에서 장기 실행 중인 요청이 제외되었습니다. 결과적으로 **KubeAPIErrorBudgetBurn** 메트릭에서 false positives가 줄어듭니다. (BZ#1982704)

Kubernetes 스케줄러

- OpenShift Container Platform 4.11에서 호스트된 컨트롤 플레인이 활성화된 클러스터에 Descheduler가 설치되면 호스팅 컨트롤 플레인 네임스페이스가 제거에서 제외됩니다. 결과적으로 Descheduler가 설치될 때 호스트된 컨트롤 플레인 네임스페이스에서 Pod가 더 이상 제거되지 않습니다. (BZ#2000653)

- 이전에는 리소스가 **kubedescheduler** CR(사용자 정의 리소스)의 소유자 참조에 API 버전을 잘못 지정했습니다. 그 결과 소유자 참조가 유효하지 않았으며 **kubedescheduler** CR을 실행할 때 영향을 받는 리소스가 삭제되지 않았습니다. 이번 업데이트에서는 모든 소유자 참조에서 올바른 API 버전을 지정합니다. 결과적으로 CR을 삭제한 후 **kubedescheduler** CR에 대한 소유자 참조가 있는 모든 리소스가 삭제됩니다. (BZ#1957012)

Machine Config Operator

- **keyFile** 이 RHEL 노드에서 NetworkManager의 기본 플러그인으로 구성되지 않았으므로 RHEL 노드는 재부팅 후 준비 상태에 도달하지 않을 수 있습니다. 이번 수정으로 **keyFile** 은 모든 클러스터 노드에서 기본 NetworkManager 플러그인으로 설정됩니다. 결과적으로 노드가 재부팅 후 **준비** 상태에 올바르게 도달합니다. (BZ#2060133)

- vSphere UPI 클러스터는 설치 시 **PlatformStatus.VSphere** 매개변수를 설정하지 않기 때문에 매개변수가 **nil**로 설정되었습니다. 이로 인해 MCO 로그가 이 매개변수의 값 **nil**을 가질 수 없는 불필요한 반복적인 메시지로 채워집니다. 이번 수정에서는 별도의 문제를 해결하기 위해 추가된 경고를 제거합니다. 결과적으로 로그에 더 이상 vSphere UPI 설치에 이 메시지가 나열되지 않습니다. (BZ#2080267)

- 이전에는 코드 내에서 병합 논리 문제로 인해 FIPS 및 **realTimeKernel** 으로 MCO(Machine Config Operator)가 성능이 저하된 클러스터를 생성하려고 했습니다. 이번 업데이트를 통해 FIPS 및 **realTimeKernel** 으로 클러스터를 생성할 때 MCO가 더 이상 저하되지 않습니다. (BZ#2096496)

Compliance Operator

- 이전에는 Compliance Operator에서 머신 구성 데이터에 대한 참조를 유지하여 메모리 사용량이 크게 증가했습니다. 그 결과 메모리 부족 예외로 인해 Compliance Operator가 **CrashLoopBackoffs**로 실패했습니다. 이 문제를 해결하려면 업데이트된 버전의 Compliance Operator를 사용해야 합니다. 예: 0.1.53: 메모리에서 대규모 머신 구성 데이터 세트를 더 잘 처리할 수 있습니다. 결과적으로 Compliance Operator는 대규모 머신 구성 데이터 세트를 처리할 때 계속 실행됩니다. (BZ#2094854)

관리 콘솔

- 이전에는 **InstallPlans**를 승인할 때 웹 콘솔에서 권한을 제대로 인증하지 않았습니다. 이로 인해 처리되지 않은 오류가 발생할 수 있었습니다. 이번 업데이트를 통해 일관성을 위해 권한이 변경되었으며 웹 콘솔에 오류 메시지가 올바르게 표시됩니다. (BZ#2006067)

모니터링

- 이번 업데이트 이전에는 **container_fs*** 지표의 컨테이너 레이블을 사용하여 쿼리를 포함하는 OpenShift Container Platform 웹 콘솔의 대시보드는 높은 카디널리티로 인해 컨테이너 레이블이 삭제되었기 때문에 데이터 포인트를 반환하지 않았습니다. 이번 업데이트에서는 이 문제가 해결되어 이제 이러한 대시보드에 데이터가 예상대로 표시됩니다. (BZ#2037513)

- 이번 업데이트 이전에는 **prometheus-operator** 구성 요소에서 구성 맵에서 **ScrapeTimeout**의 시간 값을 허용했습니다. **ScrapeTimeout**을 **ScrapeInterval** 값보다 큰 값으로 설정하면 Prometheus는 구성 맵 설정 로드를 중지하고 모든 후속 구성 변경 사항을 적용하지 않습니다. 이번 업데이트를 통해 지정된 **ScrapeTimeout** 값이 **ScrapeInterval** 값보다 크면 시스템이 설정을 유효하지 않은 것으로 기록하지만 다른 구성 맵 설정을 계속 로드합니다. (BZ#2037762)

- 이번 업데이트 이전에는 OpenShift Container Platform 웹 콘솔의 **Kubernetes / Compute Resources / Cluster** 대시보드의 **CPU** 사용률 패널에서 노드의 CPU 사용률을 계산하는 데 사용되는 수식이 잘못된 음수 값을 잘못 표시할 수 있었습니다. 이번 업데이트를 통해 수식을 업데이트하고 **CPU 사용률** 패널에 올바른 값이 표시됩니다. (BZ#2040635)

- 이번 업데이트 이전에는 새 Pod를 사용할 수 있기 전에 업데이트 프로세스가 이전 Pod를 제거하기 때문에 15일마다 발생하는 자동 업데이트 중에 **prometheus-adapter** 구성 요소의 데이터에 액세스할 수 없었습니다. 이번 릴리스에서는 자동 업데이트 프로세스에서 새 Pod가 요청을 처리할 수 있는 경우에만 이전 Pod를 제거하여 업데이트 프로세스 중에 이전 Pod의 데이터를 계속 사용할 수 있습니다. (BZ#2048333)

- 이번 업데이트 이전에는 **kube-state-metrics:kube_pod_container_status_terminated_reason,kube_pod_init_container_status_terminated_reason** 및 **kube_pod_status_scheduled_time**에서 잘못된 메트릭이 누락되었습니다. 이번 릴리스에서는 **kube-state-metrics**가 이러한 지표를 올바르게 표시하여 사용할 수 있습니다. (BZ#2050120)

- 이번 업데이트 이전에는 **prometheus-operator** 구성 요소에 대해 유효하지 않은 쓰기 레이블 구성 맵 설정이 존재하는 경우 구성이 모든 후속 설정을 로드했습니다. 이번 릴리스에서는 구성 요소가 구성을 로드할 때 유효한 쓰기 레이블 설정을 확인합니다. 잘못된 설정이 있으면 오류가 기록되고 구성 로드 프로세스가 중단됩니다. (BZ#2051470)

- 이번 업데이트 이전에는 컨테이너의 리소스가 더 적더라도 Prometheus Pod의 **init-config-reloader** 컨테이너에서 CPU **100m** 및 **50Mi**의 메모리를 요청했습니다. 이번 업데이트를 통해 컨테이너는 **1m**의 CPU와 **10Mi**의 메모리를 요청합니다. 이러한 설정은 **config-reloader** 컨테이너 설정과 일치합니다. (BZ#2057025)

- 이번 업데이트 이전에는 관리자가 사용자 워크로드 모니터링을 활성화하면 **user-workload-monitoring-config** 구성 맵이 자동으로 생성되지 않았습니다. **user-workload-monitoring-config-edit** 역할의 관리자가 아닌 사용자는 구성 맵을 수동으로 생성할 수 있는 권한이 없으므로

관리자가 생성해야 했습니다. 이번 업데이트를 통해 관리자가 사용자 워크로드 모니터링을 활성화하고 적절한 역할의 사용자가 편집할 수 있는 경우 **user-workload-monitoring-config** 구성 맵이 자동으로 생성됩니다. (BZ#2065577)

- 이번 업데이트 이전에는 배포를 삭제한 후 CNO(Cluster Monitoring Operator)에서 삭제가 완료될 때까지 기다리지 않아 조정 오류가 발생했습니다. 이 업데이트에서는 CMO가 배포를 다시 만들기 전에 삭제될 때까지 대기하므로 이 문제가 해결됩니다. (BZ#2069068)

- 이번 업데이트 이전에는 사용자 워크로드 모니터링에 대해 Prometheus의 지표에 대한 외부 레이블을 구성한 경우 CMO에서 이러한 라벨을 Thanos Ruler에 올바르게 전파하지 않았습니다. Prometheus의 사용자 워크로드 모니터링 인스턴스에서 제공하지 않은 사용자 정의 프로젝트에 대한 외부 메트릭을 쿼리하는 경우 Prometheus를 추가하도록 Prometheus를 구성한 경우에도 이러한 지표의 외부 레이블이 표시되지 않는 경우가 있습니다. 이번 업데이트를 통해 이제 CMO에서 Prometheus에 구성한 외부 레이블을 Thanos Ruler로 적절히 전파하고, 외부 메트릭을 쿼리할 때 라벨을 볼 수 있습니다. 따라서 사용자 정의 프로젝트의 경우 Prometheus를 추가하도록 Prometheus를 구성한 경우에도 사용자 정의 프로젝트의 사용자 워크로드 모니터링 인스턴스에서 제공하지 않은 외부 지표를 쿼리하지 못하는 경우가 있었습니다. 이번 업데이트를 통해 이제 CMO에서 Prometheus에 구성한 외부 레이블을 Thanos Ruler로 적절히 전파하고, 외부 메트릭을 쿼리할 때 라벨을 볼 수 있습니다. (BZ#2073112)

- 이번 업데이트 이전에는 **tunbr** 인터페이스가 **NodeNetworkInterfaceFlapping** 경고를 잘못 트리거했습니다. 이번 업데이트를 통해 이제 **tunbr** 인터페이스가 경고가 무시되고 더 이상 경고가 잘못 트리거되지 않는 인터페이스 목록에 포함됩니다. (BZ#2090838)

- 이전에는 Prometheus Operator가 잘못된 레이블 재지정 구성을 허용했습니다. 이번 업데이트를 통해 Prometheus Operator에서 레이블이 다시 지정된 구성의 유효성을 검사합니다. (BZ#2051407)

네트워킹

- 이전에는 추가 네트워크 연결에 본딩 CNI 플러그인을 사용할 때 Multus와 호환되지 않았습니다. 네트워크 연결 정의에 대해 Whereabouts IPAM 플러그인과 함께 결합된 CNI 플러그인을 사용한 경우 할당된 IP 주소가 잘못 조정되었습니다. 이제 본딩 CNI 플러그인을 사용하는 네트워크 연결 정의가 IP 주소 할당을 위해 Whereabouts IPAM 플러그인과 올바르게 작동합니다. (BZ#2082360)

- 이전 버전에서는 기본 게이트웨이가 여러 개인 OVN-Kubernetes 클러스터 네트워크 공급자를 사용할 때 잘못된 게이트웨이가 선택되어 OVN-Kubernetes Pod가 예기치 않게 중지되었습니다. 이제 이러한 Pod가 더 이상 실패하지 않도록 올바른 기본 게이트웨이가 선택됩니다. (BZ#2040933)

- OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 클러스터의 경우 이전에 NetworkManager 서비스가 노드에서 다시 시작되면 해당 노드에서 네트워크 연결이 끊어졌습니다. 이제 네트워크 연결이 NetworkManager 서비스를 다시 시작할 수 있습니다. (BZ#2048352)

- 이전에는 캐시 업데이트를 처리하는 **goroutine**이 **mutex**를 보유하는 동안 버퍼링되지 않은 채널에 대한 쓰기를 중단할 수 있었습니다. 이번 업데이트를 통해 이러한 경합 조건이 해결되었습니다. (BZ#2052398)

- 이전 버전에서는 ovn-kubernetes의 경우 본딩 또는 팀 인터페이스로 부팅 시 **br-ex**를 설정하면 **br-ex**와 본딩 인터페이스 간의 미디어 액세스 제어(MAC) 주소가 일치하지 않았습니다. 그 결과 베어 메탈 또는 일부 가상 플랫폼에서는 예기치 않은 **br-ex** MAC 주소로 인해 네트워크 인터페이스 컨트롤러(NIC) 드라이버에서 트래픽이 삭제되어 모든 트래픽이 삭제되었습니다. 이번 업데이트를 통해 **br-ex** 및 본딩 인터페이스에서 동일한 MAC 주소를 사용하므로 트래픽이 삭제되지 않습니다. (BZ#2103080)

- 이전 버전에서는 **cluster-reader** 역할의 사용자는 **NodeNetworkConfigurationPolicy**와 같은

kubernetes-nmstate의 사용자 정의 리소스를 읽을 수 없었습니다. 이번 업데이트를 통해 **cluster-reader** 역할이 있는 사용자는 kubernetes-nmstate 사용자 정의 리소스를 읽을 수 있습니다. (BZ#2022745)

- 이전에는 서비스 엔드포인트가 제거되어 연결에 실패할 때 **LoadBalancer** IP의 contrack 항목이 제거되지 않았습니다. 이번 업데이트를 통해 contrack 항목은 연결이 실패하지 않습니다. (BZ#2061002)

- 이전 버전에서는 **jq package**가 누락되어 RHEL 노드가 있는 클러스터의 확장이 노드 배포에서 실패했습니다. 이번 업데이트를 통해 **jq 패키지가** 배포에 설치되고 RHEL 노드가 있는 클러스터 확장이 성공합니다. (BZ#2052393)

- 이전에는 OVN-Kubernetes가 서비스 구성이 변경 시 과도한 시간을 소비했습니다. 이로 인해 서비스 구성 변경으로 대기 시간이 눈에 띄게 발생했습니다. 이 업데이트를 통해 OVN-Kubernetes는 서비스 구성 변경의 대기 시간을 줄이기 위해 최적화되었습니다. (BZ#2070674)

- 이전에는 API 연결 문제로 인해 IPAM CNI에 대한 IP 조정 CronJob이 실패하여 CronJob이 간헐적으로 실패했습니다. 이번 업데이트를 통해 Whereabouts IPAM CNI에서 CronJob이 시작되었으며 이러한 연결 문제가 발생하지 않도록 api-internal 서버 주소와 연장된 API 시간 초과를 사용합니다. (BZ#2048575)

- 이번 업데이트를 통해 Kubernetes-NMstate가 설치된 OpenShift Container Platform 클러스터에 이제 **must-gathers** Kubernetes-NMstate 리소스에 포함됩니다. 이렇게 하면 **must-gathers**에 Kubernetes-NMstate의 리소스를 포함하여 문제 처리가 향상됩니다. (BZ#2062355)

- 현재 로드 밸런서 서비스가 클러스터 트래픽 정책으로 구성된 경우 호스트 경로에 알려진 문제가 있습니다. 결과적으로 로드 밸런서 서비스의 송신 트래픽이 기본 게이트웨이로 제공되며 호스트 라우팅 테이블에 있는 최상의 일치하는 경로로 전달되지 않습니다. 이 문제를 해결하려면 로드 밸런서 유형 서비스를 **Local** 트래픽 정책으로 설정합니다. (BZ#2060159)

- 이전 버전에서는 **PodDisruptionBudget** 사양이 단일 노드 OpenShift 클러스터에 적합하지 않아 일부 Pod를 제거할 수 없기 때문에 업그레이드 기능이 제한됩니다. 이번 업데이트를 통해 클러스터 토폴로지를 기반으로 **PodDisruptionBudget** 사양이 조정되어 Kubernetes-NMState Operator가 단일 노드 OpenShift 클러스터에서 업그레이드할 수 있습니다. (BZ#2075491)

- 이전 버전에서는 부팅 시 **br-ex** 브리지를 설정할 때 DHCP 클라이언트 ID 및 IPv6 주소 생성 모드가 제대로 작동하지 않아 **br-ex** 에서 예기치 않은 IP 주소가 발생했습니다. 이번 업데이트를 통해 이제 DHCP 클라이언트 ID 및 IPv6 생성 모드 구성이 **br-ex** 에 올바르게 설정됩니다. (BZ#2058030)

- 이전에는 CNI 정의의 **gateway** 필드에 대한 의존으로 인해 **egress-router-cni** Pod에 일부 클러스터 내부 경로가 없어 기본 경로를 삭제하고 자체 삽입했습니다. 이번 업데이트를 통해 **egress-router-cni** pod는 pod가 외부 및 내부 클러스터 대상에 도달하도록 올바른 라우팅 정보를 삽입합니다. (BZ#2075475)

- 이전에는 Pod 중단 예산을 사용하여 단일 노드 OpenShift에서 OVN raft 쿼럼을 생성했습니다. 이로 인해 단일 노드 OpenShift 클러스터에서 도움이 되지 않은 **PodDisruptionBudgetAtLimit** 경고가 발생했습니다. 이번 업데이트를 통해 이러한 클러스터에서 **PodDisruptionBudgetAtLimit** 경고가 더 이상 발생하지 않습니다. (BZ#2037721)

- 이전 버전에서는 **NetworkManager** 재시작의 경쟁 조건으로 인해 OVN-Kubernetes를 사용할 때 노드 부팅 시 DHCP에서 **br-ex** 브리지 설정을 성공적으로 완료할 수 있었습니다. 이번 업데이트를 통해 **br-ex**를 설정할 때 경쟁 조건이 제거되어 **NetworkManager**가 더 이상 재시작되지 않습니다. (BZ#2055433)

- 이전에는 **PtpConfigSlave** 소스 CR(사용자 정의 리소스)이 지원되지 않는 네트워크 전송 UDPv4로 설정되어 DU(Distributed Unit) 노드에 오류가 발생했습니다. 이번 수정에서는 UDPv4 대신 네

트워크 전송 L2를 사용하도록 **PtpConfigSlave** 소스 CR을 업데이트합니다. 결과적으로 DU 노드에 오류가 더 이상 표시되지 않습니다. (BZ#2060492)

- 이전에는 네트워크 정책을 업데이트할 때 모든 OpenShift Container Platform 정책 로깅 구성이 업데이트되었습니다. 이로 인해 일부 동시 또는 이후 네트워크 정책에서 대기 시간이 눈에 띄게 발생했습니다. 이번 업데이트를 통해 새 정책을 추가할 때 모든 네트워크 정책이 더 이상 업데이트되지 않으므로 대기 시간이 제거됩니다. (BZ#2089392)

네트워킹 성능 개선

- 이전 버전에서는 **systemd** 서비스에서 가상 장치를 제외하고 udev에서 표시되는 모든 네트워크 장치에 대해 예약된 CPU 목록에 따라 기본 Recieve Packet stering (RPS) 마스크를 설정했습니다. **crio** 후크 스크립트는 보장된 Pod에 대해 **/sys/devices** 에서 표시되는 모든 네트워크 장치의 RPS 마스크를 설정합니다. 이로 인해 네트워크 성능에 여러 영향을 미쳤습니다. 이번 업데이트에서는 **systemd** 서비스는 가상 인터페이스의 기본 RPS 마스크만 **/sys/devices/virtual** 아래에 설정합니다. 이제 **crio** 후크 스크립트에서 물리적 장치도 제외합니다. 이 구성에서는 프로세스 과부하, 폴링 간격, 대기 시간 급증과 같은 문제를 완화합니다. (BZ#2081852)

노드

- 이전에는 Pod 관리자가 Pod 시크릿 및 구성 맵의 등록 및 등록 해제를 처리했습니다. 이로 인해 Pod 보안이 Pod 내에 마운트되지 않는 경우가 있었습니다. 이번 수정으로 kubelet에서 등록된 Pod를 관리하는 데 사용하는 키에 Pod ID가 포함됩니다. 결과적으로 보안이 예상대로 올바르게 마운트됩니다. (BZ#1999325)

- 가비지 컬렉션 프로세스에서 메모리 누수로 인해 메모리 부족으로 인해 Pod가 노드에서 시작되지 않을 수 있습니다. 이번 수정으로 가비지 수집 프로세스에서 메모리가 유출되지 않고 노드가 예상대로 시작되어야 합니다. (BZ#2065749)

- 업스트림 Kubernetes가 변경되었기 때문에 kubelet은 종료된 Pod에서 준비 상태 프로브를 실행하지 않았습니다. 결과적으로 로드 밸런서 또는 컨트롤러에서 종료 Pod에 더 천천히 반응하여 오류가 발생할 수 있었습니다. 이번 수정을 통해 Pod 종료 시 준비 상태 프로브가 다시 수행됩니다. (BZ#2089933)

- 버그로 인해 다른 Pod가 API에서 완료된 것으로 보고된 후 Pod가 빠르게 예약된 경우 kubelet에서 **OutOfCpu** 오류가 있는 Pod를 잘못 거부할 수 있었습니다. 이번 수정으로 kubelet은 이제 실행 중인 모든 컨테이너가 중지되고 새 컨테이너가 시작되지 않을 때까지 API의 터미널로 Pod의 단계를 보고합니다. 이 변경 후 성공 또는 실패를 보고하는 데 수명이 짧은 Pod가 약간 더 오래 걸릴 수 있습니다. (BZ#2022507)

- **prometheus-adapter** 의 최신 버전에서는 추가 Pod 지표를 전송하므로 VPA(Vertical Pod Autoscaler) 권장 사항은 많은 불필요한 반복적인 메시지를 생성하고 있습니다. 이번 수정으로 VPA는 추가 메트릭을 인식하고 무시합니다. 결과적으로 이러한 메시지가 더 이상 생성되지 않습니다. (BZ#2102947)

OpenShift CLI(oc)

- 이전 버전에서는 더 이상 사용되지 않는 이미지 버전이 소스로 사용된 경우 **oc** 카탈로그 미러링이 실패했습니다. 이제 이미지 매니페스트 버전이 자동으로 감지되고 미러링이 성공적으로 작동합니다. (BZ#2049133)

- 이전에는 대체 검사가 발생했을 때 로그에서 이해하기 어려웠습니다. 이를 보다 명확히 하기 위해 로그가 개선되었습니다. 결과적으로 **must-gather run** 출력이 훨씬 더 명확해졌습니다. (BZ#2035717)

- 이전 버전에서는 **must-gather** 를 잘못된 인수로 실행한 경우 오류가 지속적으로 보고되지 않았으며 대신 불가능한 경우에도 데이터 수집을 시도할 수 있었습니다. 이제 **must-gather**가 잘못된 옵션으로 호출되면 유용한 오류 출력을 제공합니다. (BZ#1999891)

- 이전 버전에서는 **oc adm catalog mirror** 명령에서 오류가 발생한 경우 계속되어 **0** 종료 코드를 반환했습니다. 오류가 있거나 0이 아닌 종료 코드로 인해 명령이 계속되어야 하는지 확인할 수 있는 **--continue-on-error** 플래그를 사용할 수 있습니다. (BZ#2088483)

- 이번 업데이트를 통해 **oc adm policy who-can** 명령에 **--subresource** 플래그가 추가되어 하위 리소스에서 지정된 작업을 수행할 수 있는 사람을 확인할 수 있습니다. (BZ#1905850)

- 이전에는 **oc project** 명령에 탭 완료를 사용할 수 없었습니다. 이제 **oc project** 이후 탭을 누르면 프로젝트를 올바르게 나열할 수 있습니다. (BZ#2080416)

- 이전 버전에서는 시작 프로브가 디버그 Pod에서 제거되지 않아 시작 프로브가 실패한 경우 디버그 Pod에 문제가 발생할 수 있었습니다. 기본적으로 **false**인 **--keep-startup** 플래그가 추가되었습니다. 즉, 기본적으로 디버그 pod에서 시작 프로브가 제거됩니다. (BZ#2056122)

- 이전 버전에서는 **oc debug node**를 호출한 후 시간 초과가 지정되지 않았으므로 사용자가 클러스터에서 로그인하지 않았습니다. 지정된 비활성 시간이 지나면 세션이 자동으로 종료되도록 **TMOUT** 환경 변수가 추가되었습니다. (BZ#2043314)

- 이번 업데이트를 통해 이제 사용자가 로그아웃한 경우에도 **oc login** 에 웹 콘솔의 URL이 표시됩니다. (BZ#1957668)

- 이전에는 컨테이너를 찾을 수 없는 경우 **oc rsync** 명령으로 잘못된 오류 출력이 표시되었습니다. 이번 릴리스에서는 특정 컨테이너가 실행되지 않을 때 **oc rsync** 명령이 올바른 오류 메시지를 표시합니다. (BZ#2057633)

- 이전에는 클러스터가 새로 추가된 경우 대용량 이미지를 정리할 수 없었습니다. 이로 인해 크기가 초과된 이미지를 필터링할 때 최근 이미지가 생략되었습니다. 이번 릴리스에서는 지정된 크기를 초과하는 이미지를 정리할 수 있습니다. (BZ#2083999)

- 이전에는 **gather** 스크립트에 오타가 있었습니다. 결과적으로 인사이트 데이터가 제대로 수집되지 않았습니다. 이번 릴리스에서는 오타가 수정되어 Insights 데이터가 이제 **must-gather**를 통해 올바르게 수집됩니다. (BZ#2106543)

- 이전에는 **oc** CLI를 통해 클러스터의 **EgressNetworkPolicy** 리소스 유형을 적용할 수 없었습니다. 이번 릴리스에서는 **EgressNetworkPolicy** 리소스를 생성, 업데이트 및 삭제할 수 있습니다. (BZ#2071614)

Kubernetes 컨트롤러 관리자

- 이전에는 Pod 종료자를 사용하여 작업을 추적하는 베타 기능이 기본적으로 활성화되어 있었습니다. 경우에 따라 종료자가 제거되지 않았기 때문에 Pod가 항상 제거되지 않는 경우가 있었습니다. 이번 업데이트를 통해 기능 게이트 **Job jenkinsfileingWithFinalizers** 는 기본적으로 비활성화되어 있습니다. 따라서 제거 중에 Pod를 그대로 두지 않아야 합니다. (BZ#2075621)

- 이전에는 CR 복제본 수가 0일 때마다 **PodDisruptionBudgetAtLimit** 경고가 발생했습니다. 이번 업데이트를 통해 중단 또는 복제본 수가 0인 경우 경고가 더 이상 실행되지 않습니다. (BZ#2053622)

OLM(Operator Lifecycle Manager)

- 이번 업데이트 이전에는 리소스 이름이 63자를 초과하면 유효하지 않은 서브스크립션 라벨이 생성되었습니다. 63자 제한을 초과하는 라벨을 자르면 문제가 해결되고 서브스크립션 리소스에서 더 이상 Kubernetes API를 거부하지 않습니다. (BZ#2016425)

- 이번 업데이트 이전에는 Marketplace Operator의 카탈로그 소스 Pod가 노드 드레이닝되지 않았습니다. 이로 인해 클러스터 자동 스케일러를 효과적으로 축소할 수 없었습니다. 이번 업데이트를 통해 카탈로그 소스 pod에 **cluster-autoscaler.kubernetes.io/safe-to-evict** 주석을 추가하고 클러스터 자동 스케일러를 효과적으로 축소할 수 있습니다. (BZ#2053343)

- 이번 업데이트 이전에는 Pod를 예약할 수 없는 경우와 같이 **collect-profiles** 작업을 완료하는 데 시간이 오래 걸릴 수 있었습니다. 이로 인해 작업이 충분하지만 실행할 수 없는 경우 예약된 작업 수가 Pod 할당량 제한을 초과했습니다. 이번 업데이트를 통해 한 번에 하나의 **collect-profiles** Pod만 존재하며, **collect-profiles** 작업은 Pod 할당량 제한을 초과하지 않습니다. (BZ#2055861)

- 이번 업데이트 이전에는 리더 선택 기간, 갱신 기한, 재시도 기간을 정의할 때 패키지 서버에서 Pod 토폴로지를 인식하지 못했습니다. 결과적으로 패키지 서버는 단일 노드 환경과 같은 리소스가 제한된 토폴로지를 충당했습니다. 이번 업데이트에서는 적절한 리스 기간, 갱신 기한 및 재시도 기간을 설정하는 **leaderElection** 패키지가 도입되었습니다. 이번 수정을 통해 리소스가 제한된 클러스터의 부담을 줄일 수 있습니다. (BZ#2048563)

- 이전 버전에서는 **openshift-marketplace** 네임스페이스에 잘못된 카탈로그 소스가 있었습니다. 이로 인해 모든 서브스크립션이 차단되었습니다. 이번 업데이트를 통해 **openshift-marketplace** 네임스페이스에 잘못된 카탈로그 소스가 있는 경우 사용자는 원래 주석이 있는 자체 네임스페이스의 품질 카탈로그 소스에서 Operator를 구독할 수 있습니다. 결과적으로 로컬 네임스페이스에 잘못된 카탈로그 소스가 있는 경우 사용자는 네임스페이스의 Operator에 가입할 수 없습니다. (BZ#2076323)

- 이전에는 **operator-marketplace** 프로젝트 폴링 중에 정보 수준 (info-level) 로그가 생성되어 로그 스팸이 발생했습니다. 이번 업데이트에서는 명령줄 플래그를 사용하여 로그 행을 디버그 수준으로 줄이며 사용자의 로그 수준을 더 많이 제어할 수 있습니다. 이로 인해 로그 스팸이 줄어듭니다. (BZ#2057558)

- 이전에는 CVO(Cluster Version Operator)에서 관리하는 각 구성 요소는 프로젝트의 리포지토리 루트의 **/manifest** 디렉터리에 정의된 YAML 파일로 구성됩니다. **/manifest** 디렉터리에서 YAML 파일을 제거할 때 **release.openshift.io/delete: "true"** 주석을 추가해야 합니다. 그렇지 않으면 CVO가 클러스터에서 리소스를 삭제하지 않습니다. 이번 업데이트에서는 **/manifest** 디렉터리에서 제거된 모든 리소스를 다시 사용하고 CVO가 리소스를 정리하도록 **release.openshift.io/delete: "true"** 주석을 추가합니다. 결과적으로 OLM 구성 요소에 더 이상 필요하지 않은 리소스가 클러스터에서 제거됩니다. (BZ#1975543)

- 이전에는 gRPC 카탈로그 소스에서 사용하는 **CheckRegistryServer** 기능이 카탈로그 소스와 연결된 서비스 계정이 있는지 확인하지 않았습니다. 이로 인해 서비스 계정이 없는 비정상 카탈로그 소스가 발생했습니다. 이번 업데이트를 통해 gRPC **CheckRegistryServer** 함수는 서비스 계정이 존재하는지 확인하고 없는 경우 서비스를 다시 생성합니다. 결과적으로 OLM은 gRPC 카탈로그 소스가 없는 경우 gRPC 카탈로그 소스가 소유한 서비스 계정을 다시 생성합니다. (BZ#2074612)

- 이전 버전에서는 사용자가 파일 기반 카탈로그 이미지에 대해 **opm index prune**을 실행할 때 발생한 오류 메시지에서 부정확한 언어로 인해 이 명령에서 해당 카탈로그 형식을 지원하지 않았습니다. 이번 업데이트에서는 사용자가 **opm index prune** 명령에서 SQLite 기반 이미지만 지원하도록 오류 메시지를 명확히 합니다. (BZ#2039135)

- 이전에는 Operator API 주위에 스레드 안전성이 손상되었습니다. 결과적으로 Operator 리소스가 올바르게 삭제되지 않았습니다. 이번 업데이트를 통해 Operator 리소스가 올바르게 삭제됩니다. (BZ#2015023)

- 이전 버전에서는 Pod 오류로 인해 인증서의 유효 기간이 인위적으로 연장되어 인증서가 잘못 교체되었습니다. 이번 업데이트를 통해 인증서 유효 기간이 올바르게 결정되고 인증서가 올바르게 순환됩니다. (BZ#2020484)

- OpenShift Container Platform 4.11에서 기본 클러스터 전체 Pod 보안 승인 정책은 모든 네임스페이스에 대해 **baseline**으로 설정되고 기본 경고 수준은 **restricted**로 설정됩니다. 이번 업데이트

이전에는 Operator Lifecycle Manager에서 **operator-marketplace** 네임스페이스에 Pod 보안 승인 경고가 표시되었습니다. 이번 수정을 통해 경고 수준을 **baseline**으로 낮추면 문제가 해결됩니다. (BZ#2088541)

Operator SDK

- 이번 업데이트 이전에는 Operator SDK에서 다운스트림이 지원되는 이미지가 아닌 업스트림 이미지를 사용하여 Hybrid Helm 기반 Operator를 스캐폴드했습니다. 이번 업데이트를 통해 Operator SDK는 지원되는 다운스트림 이미지를 사용하여 Hybrid Helm 기반 Operator를 스캐폴드합니다. (BZ#2039135)

- OpenShift Container Platform 4.11을 사용하면 Operator SDK를 사용하여 **arm64** Operator 이미지를 빌드할 수 있습니다. 결과적으로 Operator SDK는 이제 **arm64**를 대상으로 하는 Operator 이미지 빌드를 지원합니다. (BZ#2035899)

- 이전 버전에서는 Operator SDK와 함께 하이브리드 Helm Operator를 실행하는 {product-tile}에서 지원되는 다운스트림 이미지가 아닌 업스트림 이미지를 사용합니다. 이번 업데이트를 통해 하이브리드 Helm Operator를 스캐폴딩하면 다운스트림 이미지를 사용합니다. (BZ#2066615)

OpenShift API 서버

- 여러 Authentication Operator 컨트롤러가 동시에 동기화되었기 때문에 Authentication Operator가 구성에 반응하는 데 시간이 너무 오래 걸렸습니다. 이 기능은 Authentication Operator 컨트롤러가 리소스를 놓고 경쟁하지 않도록 일반 동기화 기간에 지터를 추가합니다. 따라서 Authentication Operator가 구성 변경에 반응하는 데 시간이 단축되었습니다. (BZ#1958198)

- OpenShift Container Platform 4.11에서 외부 ID 공급자의 인증 시도는 이제 감사 로그에 기록됩니다. 따라서 감사 로그의 외부 ID 공급자의 성공, 실패 및 오류가 발생한 로그인 시도를 볼 수 있습니다. (BZ#2086465)

RHCOS(Red Hat Enterprise Linux CoreOS)

- 이번 업데이트 이전에는 PXE를 통해 머신을 부팅하고 **BOOTIF** 인수가 커널 명령줄에 있는 경우 시스템은 단일 인터페이스에서만 DHCP가 활성화된 상태로 부팅됩니다. 이번 업데이트를 통해 **BOOTIF** 인수가 제공되는 경우에도 모든 인터페이스에서 DHCP가 활성화된 상태로 머신이 부팅됩니다. (BZ#2032717)

- 이전에는 VMware OVA 이미지에서 프로비저닝된 노드가 초기 프로비저닝 후 Ignition 구성을 삭제하지 않았습니다. 결과적으로 시크릿이 Ignition 구성 내에 저장될 때 보안 문제가 발생했습니다. 이번 업데이트를 통해 이제 새 노드에서 초기 프로비저닝 후 및 기존 노드의 이전 OpenShift Container Platform 릴리스에서 업그레이드할 때 VMware 하이퍼바이저에서 Ignition 구성이 삭제됩니다. (BZ#2082274)

- 이전에는 명령을 처음 호출할 때 **toolbox** 명령에 제공된 인수가 무시되었습니다. 이번 수정에서는 toolbox 스크립트를 업데이트하여 **podman container create** 명령 다음에 **podman start** 및 **podman exec** 명령을 시작합니다. 또한 여러 개의 인수 및 공백을 배열로 처리하기 위해 스크립트를 수정합니다. 결과적으로 **toolbox** 명령에 전달된 인수가 예상대로 실행됩니다. (BZ#2039589)

Performance Addon Operator

- 이전에는 CNF cyclictest 실행자에서 **--mainaffinity** 인수를 제공해야 했으며 이 인수는 바이너리를 실행해야 하는 스레드를 알려주었지만 cyclictest 실행자에 **--mainaffinity** 인수가 누락되었습니다. 이번 업데이트에서는 cyclictest 실행자에 **--mainaffinity** 인수를 추가하여 **cyclitest** 명령에 올바르게 전달됩니다. (BZ#2051540)

- 이전에는 **oslat** 컨테이너 사양에 **cpu-quota.crio.io: "disable"** 주석이 없어 대기 시간이 길어졌습니다. 그 결과 생성 중에 **cpu-quay.crio.io:"disable"** 주석이 Pod 정의에서 누락되었습니다. 이

번 업데이트를 통해 Pod 생성 중에 **cpu-quota.crio.io:"disable"** 주석이 추가되고 결과적으로 **oslat** Pod의 **specification** 필드에 표시됩니다. (BZ#2061676)

라우팅

- 이전에는 Ingress Operator에서 OpenShift Ingress 네임스페이스의 Kubernetes 서비스 오브젝트가 조정하려는 Ingress 컨트롤러가 생성되었는지 확인하지 않았습니다. 따라서 Ingress Operator는 소유권에 관계없이 동일한 이름과 네임스페이스가 있는 Kubernetes 서비스를 수정하거나 제거하므로 예기치 않은 동작이 발생합니다. 이번 업데이트를 통해 Ingress Operator는 이제 서비스를 수정하거나 제거하기 전에 기존 Kubernetes 서비스의 소유권을 확인할 수 있습니다. 소유권이 일치하지 않으면 Ingress Operator에 오류가 표시되고 작업을 수행하지 않습니다. 결과적으로 Ingress Operator는 수정 또는 제거하려는 OpenShift Ingress 네임스페이스와 동일한 이름으로 사용자 정의 Kubernetes 서비스를 수정하거나 삭제할 수 없습니다. (BZ#2054200)

- 이전에는 OpenShift Container Platform 4.8에서 플랫폼 경로를 사용자 정의하는 API를 추가했습니다. 이 API에는 사용자 지정 가능한 경로의 현재 호스트 이름과 이러한 경로에 대한 사용자의 원하는 호스트 이름을 각각 보고하는 클러스터 수신 구성에 상태 및 사양 필드가 포함되어 있습니다. API는 이러한 값에 대한 제약 조건도 정의했습니다. 이러한 제약 조건은 제한적이며 유효한 잠재적인 일부 호스트 이름을 제외했습니다. 결과적으로 API에 대한 제한적인 검증으로 인해 사용자가 허용되어야 하는 사용자 정의 호스트 이름을 지정할 수 없게 되었고, 허용된 도메인이 있는 사용자가 클러스터를 설치할 수 없게 되었습니다. 이번 업데이트를 통해 경로 및 OpenShift Container Platform에 유효한 모든 호스트 이름을 허용하도록 호스트 이름에 대한 제약 조건이 완화되었습니다. OpenShift Container Platform을 사용하면 사용자가 10진수가 포함된 gcc로 클러스터 도메인을 사용할 수 있습니다. (BZ#2039256)

- 이전에는 Ingress Operator에서 클러스터 **spec.domain** 매개변수로 구성된 Ingress 컨트롤러가 **spec.baseDomain** 매개변수와 일치하는지 확인하지 않았습니다. 이로 인해 Operator에서 DNS 레코드를 생성하고 **DNSManaged** 조건을 **false**로 설정했습니다. 이번 수정으로 Ingress Operator에서 **spec.domain** 매개변수가 클러스터 **spec.baseDomain**과 일치하는지 확인합니다. 결과적으로 사용자 정의 Ingress 컨트롤러의 경우 Ingress Operator는 DNS 레코드를 생성하지 않고 **DNSManaged** 조건을 false로 설정합니다. (BZ#2041616)

- 이전에는 OpenShift Container Platform 4.10에서 HAProxy must-gather 함수가 실행하는 데 최대 1시간이 걸릴 수 있었습니다. 이는 종료 상태의 라우터가 **oc cp** 명령을 지연할 때 발생할 수 있습니다. 지연은 Pod가 종료될 때까지 지속됩니다. 새 릴리스에서는 **oc op** 명령의 10분 제한이 더 이상 지연되지 않습니다. (BZ#2104701)

- 이전에는 Ingress 컨트롤러가 삭제될 때 Ingress Operator에서 경로 상태를 지우지 않아 삭제 후 경로가 여전히 Operator에 표시되었습니다. 이번 수정에서는 Ingress 컨트롤러가 삭제될 때 경로 상태가 지워 삭제 후 Operator에서 경로가 지워집니다. (BZ#1944851)

- 이전에는 **oc explain router.status.ingress.conditions** 명령의 출력에 API(애플리케이션 프로그래밍 인터페이스)에서 잘못된 표현으로 인해 **Admitted**가 아닌 **Currently only Ready**만 표시되었습니다. 이번 수정으로 API의 단어가 수정되었습니다. 결과적으로 명령 출력이 올바르게 표시됩니다. (BZ#2041133)

- 이전에는 Ingress Operator에서 사용자가 **LoadBalancer-type** 서비스에서 관리하는 주석을 수정했음을 감지했습니다. 결과적으로 Operator는 업그레이드를 차단하기 위해 Ingress Cluster Operator의 **Upgradeable** 상태 조건을 **False**로 설정하고 Ingress Operator에서 **Upgradeable** 상태 조건을 **False**로 설정하여 서비스에 주석이 없는 경우 업그레이드를 차단했습니다. 이제 서비스의 주석을 확인하는 논리에서 빈 주석을 올바르게 처리하고 Ingress Operator에서 더 이상 업그레이드를 잘못 차단하지 않습니다. (BZ#2097555)

- 이전에는 Ingress Operator에서 Operator가 이전 버전의 OpenShift Container Platform에서 **LoadBalancer-type** 서비스에 추가한 종료자를 제거했습니다. 이번 업데이트를 통해 Ingress Operator는 더 이상 종료자를 제거하지 않습니다. (BZ#2069457)

- Ingress Operator는 Ingress canary 경로에 대해 상태 점검을 수행합니다. 이번 업데이트 이전에는 연결에 **keepalive** 데몬이 활성화되어 있기 때문에 상태 점검이 완료된 후 Ingress Operator가 로드 밸런서(LB)에 대한 TCP 연결을 종료하지 않습니다. 기존 연결을 사용하는 대신 다음 상태 점검을 위해 새 연결이 생성되었습니다. 그 결과, 연결은 로드 밸런서에 빌드되고 로드 밸런서에 너무 많은 연결을 생성합니다. 이번 업데이트를 통해 canary 경로에 연결할 때 **keepalive** 데몬이 비활성화되고 canary 프로브가 실행될 때마다 새 연결이 생성되어 종료됩니다. (BZ#2037447)

- 이전에는 Ingress 컨트롤러에서 라우터 배포에서 **allowPrivilegeEscalation** 값을 false로 설정하지 않아 라우터 Pod가 잘못된 SCC(Security Context Constraint)로 선택되고 사용자 정의 SCC와 충돌했습니다. 이번 수정에서는 **allowPrivilegeEscalation** 값을 **true**로 설정하여 라우터 Pod가 올바른 SCC로 선택되어 사용자 지정 SCC와의 충돌을 방지합니다. (BZ#2007246)

- 이전에는 canary 경로가 Ingress 컨트롤러에 허용되지 않은 경우 Ingress Operator 상태 조건이 **degraded** 로 표시되지 않았습니다. 결과적으로 상태 조건이 **not admitted**로 표시되는 경우 canary 경로가 **valid**로 표시될 수 있었습니다. 이번 업데이트를 통해 Ingress Operator 상태가 canary 컨트롤러의 상태를 보다 정확하게 반영합니다. (BZ#2021446)

- 이전에는 **openshift-router** 프로세스에서 **SIGTERM** 종료 신호를 간단히 무시했습니다. 이로 인해 컨테이너가 Kubernetes 종료 요청을 무시하여 1시간 동안 종료되었습니다. 이번 업데이트를 통해 라우터는 이제 **SIGTERM** 신호에 응답합니다. (BZ#2076297)

- 이전 버전에서는 승인 경로에 대한 Ingress 컨트롤러가 삭제되거나 샤딩 구성이 추가되면 잘못된 **허용** 상태가 지정되었습니다. 이번 업데이트를 통해 Ingress 컨트롤러에서 바인딩 **되지 않은** 경로의 상태를 지우고 잘못된 상태 시나리오를 방지합니다. (BZ#1944851)

- 이전 버전에서는 4.7 또는 이전 버전을 사용하여 설치한 OpenShift Container Platform 클러스터에서 **0.0.0.0/0** 의 **service.beta.kubernetes.io/aws-load-balancer-internal** 주석 값을 유지했습니다. 4.8 이상을 사용하여 설치한 클러스터에는 주석 값이 **true** 가 있습니다. 주석 값 **true** 를 확인하는 AWS 클라우드 공급자 구현에서는 값이 **0.0.0.0/0** 인 경우 잘못된 결과를 반환합니다. 이로 인해 4.10으로 클러스터 업그레이드가 완료되지 않았습니다. 이번 업데이트를 통해 클러스터 업그레이드가 완료될 수 있도록 주석 값이 **true** 로 정규화됩니다. (BZ#2055470)

확장 및 성능

- 이번 업데이트 이전에는 NFD가 이미 설치되어 있는지 여부와 관계없이 SRO가 기본적으로 NFD(Node Feature Discovery)를 설치했습니다. NFD가 설치된 경우 이로 인해 SRO 배포가 실패합니다. SRO는 기본적으로 NFD를 더 이상 배포하지 않습니다.

스토리지

- 이전 버전에서는 사용자가 PVC(영구 볼륨 클레임)를 생성한 경우 OpenShift Container Platform과 함께 제공된 Alibaba Container Storage Interface(CS) 드라이버에서 20GiB 미만의 PVC(영구 볼륨 클레임)를 생성할 때 오류가 반환되었습니다. Alibaba Cloud는 20GiB보다 큰 볼륨만 지원하기 때문입니다. 이번 업데이트를 통해 Alibaba CSI 드라이버는 모든 볼륨 크기를 20GiB 이상으로 자동으로 증가하며 작은 PVC가 동적으로 프로비저닝됩니다. 이로 인해 비용이 증가할 수 있습니다. 관리자는 제한된 환경의 각 네임스페이스에 대해 PVC 수에 대한 할당량을 사용하여 비용을 제한할 수 있습니다. (BZ#2057495)

- 이전 버전에서는 LSO(Local Storage Operator)에서 생성된 PV(영구 볼륨)에 소유자 참조가 추가되어 노드를 삭제하면 PV에 삭제 요청도 실행됩니다. 이로 인해 Pod에 연결된 상태에서 PV가 **Terminating** 상태로 유지될 수 있습니다. LSO는 더 이상 OwnerReference를 생성하지 않으므로 클러스터에서 노드를 제거한 후 클러스터 관리자가 사용되지 않은 PV를 삭제해야 합니다. (BZ#2061447) 자세한 내용은 로컬 볼륨을 사용한 영구 저장장치 를 참조하십시오.

- 이번 수정을 통해 GCP CSI Driver에서 읽기 전용으로 많은 볼륨을 적절하게 프로비저닝할 수 있습니다. (BZ#1968253)

- OpenShift Container Platform을 사용하면 업스트림 커뮤니티 또는 VMware에서 제공하는 vSphere CSI 드라이버를 설치할 수 있습니다. Red Hat은 이 드라이버를 지원하지 않지만, Red Hat에서 제공하는 vSphere CSI 드라이버보다 기능이 더 많이 포함되어 있기 때문에 클러스터 관리자는 계속 설치하고 사용할 수 있습니다. OpenShift Container Platform은 업스트림 및 VMware vSphere CSI 드라이버를 사용하여 4.11로 업그레이드할 수 있지만 타사 CSI 드라이버가 있는지에 대해 경고합니다. 자세한 내용은 (BZ#2089419) 및 (BZ#2052071)를 참조하십시오.

- 이번 업데이트를 통해 AWS(Amazon Web Services)에 대한 기본 인증 정보 요청이 변경되어 KMS(Key Managment Service)의 고객 관리 키를 사용하여 암호화된 볼륨을 마운트할 수 있습니다. CCO(Cloud creditial Operator)를 사용하여 수동 모드에서 인증 정보 요청을 생성한 관리자는 AWS에서 고객 관리 키를 사용하여 암호화된 볼륨을 마운트하려는 경우 이러한 변경 사항을 수동으로 적용해야 합니다. 다른 관리자는 이 변경 사항의 영향을 받지 않아야 합니다. (BZ#2049872)

- 이전에는 IBM Cloud에 배포된 OpenShift Container Platform 클러스터를 삭제한 후 백엔드 스토리지 볼륨이 삭제되지 않았습니다. 이로 인해 클러스터 리소스가 완전히 제거되지 않았습니다. 이번 수정에서는 설치 프로그램과 CSI(Container Storage Interface) 드라이버에 지원이 추가되어 클러스터가 제거된 후 백엔드 볼륨 삭제가 발생합니다. (BZ#2047732)

웹 콘솔 (개발자 화면)

- 이번 업데이트 이전에는 유효하지 않은 devfile 리포지토리(devfile v2.2 미만)를 입력할 때 **Git 가져오기** 양식에 오류 메시지가 표시되었습니다. 이번 업데이트에서는 v2.2보다 오래된 devfiles가 지원되지 않는다는 오류 메시지가 표시됩니다. (BZ#2046435)

- 이번 업데이트 이전에는 클러스터에서 **ConsoleLink CR** (openshift-blog)을 사용할 수 없는 경우 블로그 링크가 정의되지 않았습니다. 블로그 링크를 클릭하면 OpenShift 블로그로 리디렉션되지 않았습니다. 이번 업데이트를 통해 **ConsoleLink CR** (openshift-blog)이 클러스터에 없는 경우에도 https://developers.redhat.com/products/openshift/whats-new에 대한 대체 링크가 추가됩니다. (BZ#2050637)

- 이번 업데이트 이전에는 kafka CR의 API 버전이 업데이트되었습니다. 이 버전은 이전 버전을 지원하지 않았으므로 생성된 경우에도 **Create Event Source - KafkaSource**에 빈 **부트스트랩 서버**가 표시되었습니다. 이번 업데이트를 통해 Kafka CR의 업데이트된 API는 이전 버전을 지원하고 **Create Event Source - KafkaSource**양식에서 **부트르스랩 서버** 목록을 렌더링합니다. (BZ#2058623)

- 이번 업데이트 이전에는 **Git에서 가져오기**를 사용하여 프라이빗 Git 리포지토리를 가져올 때 프라이빗 리포지토리 세부 정보를 가져오는 시크릿이 디코딩되지 않았기 때문에 올바른 가져오기 유형과 빌더 이미지가 확인되지 않았습니다. 이번 업데이트를 통해 **Git에서 가져오기** 양식에서 시크릿을 디코딩하여 개인 리포지토리 세부 정보를 가져옵니다. (BZ#2053501)

- 이번 업데이트 이전에는 개발자 화면에서 **토폴로지** 보기에서 선택한 작업이 아닌 가장 최근에 확인한 워크로드에 대해 **Observe** 대시보드를 열었습니다. 이 문제는 세션이 URL의 쿼리 매개변수 대신 redux 저장소를 선호하기 때문에 발생합니다. 이번 업데이트를 통해 **Observe** 대시보드는 URL의 쿼리 매개변수를 기반으로 구성 요소를 렌더링합니다. (BZ#2052953)

- 이번 업데이트 이전에는 클러스터에 없는 경우에도 하드 코딩된 값 **gp2**로 시작하는 데 사용된 **Pipeline**이 기본 스토리지 클래스로 시작합니다. 이번 업데이트를 통해 하드 코딩된 값 대신 기본 지정된 스토리지 클래스 이름을 사용할 수 있습니다. (BZ#2084635)

- 이번 업데이트 이전에는 대용량 파이프라인 로그를 실행하는 동안 자동 스크롤 기능이 작동하지 않고 로그에 이전 메시지가 표시됩니다. 대용량 파이프라인 로그를 실행하면 **scrollIntoView** 메서드에 대한 많은 호출이 생성됩니다. 이번 업데이트를 통해 대용량 파이프라인 로그가 **scrollIntoView** 메서드에 대한 호출을 생성하지 않고 원활한 자동 스크롤 기능을 제공합니다. (BZ#2014161)

- 이번 업데이트 이전에는 **Create RoleBinding** 양식을 사용하여 **RoleBinding**을 생성할 때 제목 이름이 필수입니다. 누락된 제목 이름이 **Project Access** 탭을 로드하지 못합니다. 이번 업데이트를 통해 **주체 이름** 속성이 없는 **RoleBinding**이 **Project Access** 탭에 나열되지 않습니다. (BZ#2051558)

- 이번 업데이트 이전에는 독립 실행형 또는 **k-native service**, **Broker**, **KameletBinding**을 지원하는 일부 경우에도 이벤트 소스에 대한 싱크 및 트리거에 모든 리소스를 표시했습니다. 싱크 드롭다운 목록에 표시되는 데 사용되는 주소 지정 리소스입니다. 이번 업데이트를 통해 독립 실행형 리소스만 싱크로 표시하도록 필터가 추가되었습니다. (BZ#2054285)

- 이번 업데이트 이전에는 렌더링 전에 토폴로지 뷰의 사이드바에 있는 빈 탭을 필터링하지 않았습니다. 토폴로지 보기에 **워크로드**에 대한 잘못된 탭이 표시됩니다. 이번 업데이트를 통해 빈 탭이 올바르게 필터링됩니다. (BZ#2049483)

- 이번 업데이트 이전에는 **마지막 실행 시작** 버튼을 사용하여 파이프라인을 시작할 때 생성된 **PipelineRun**의 **startedby** 주석이 올바른 사용자 이름으로 업데이트되지 않아 섹션에 의해 트리거된 섹션에 올바른 사용자 이름이 표시되지 않았습니다. 이번 업데이트를 통해 **started-by** 주석 값이 올바른 사용자 이름으로 업데이트되고 섹션은 파이프라인을 시작한 올바른 사용자의 사용자 이름을 보여줍니다. (BZ#2046618)

- 이번 업데이트 이전에는 **ProjectHelmChartRepository** CR이 클러스터에 표시되지 않습니다. 결과적으로 이 CR의 API 스키마가 아직 클러스터에서 초기화되지 않았습니다. 이번 업데이트를 통해 **ProjectHelmChartRepository**가 클러스터에 표시됩니다. (BZ#2054197)

- 이번 업데이트 이전에는 토폴로지에서 키보드를 사용하여 탐색할 때 선택한 항목이 강조 표시되지 않았습니다. 이 업데이트에서는 키보드를 사용한 탐색이 선택한 항목을 강조 표시하고 스타일을 업데이트합니다. (BZ#2039277)

- 이번 업데이트 이전에는 웹 터미널 레이아웃이 기본 보기 외부에서 열리며 크기를 조정할 수 없었습니다. 이번 업데이트를 통해 기본 보기 내에 웹 터미널이 열리고 올바르게 크기 조정됩니다. (BZ#2022253)

- 이번 업데이트 이전에는 일부 사이드바 항목에 네임스페이스 컨텍스트가 포함되지 않았습니다. 결과적으로 다른 브라우저에서 링크를 열거나 다른 활성 네임스페이스에서 링크를 열면 웹 콘솔이 올바른 네임스페이스로 전환되지 않습니다. 이번 업데이트를 통해 URL을 열 때 올바른 네임스페이스가 선택됩니다. (BZ#2039647)

- 이전 버전에서는 콘솔을 사용하여 템플릿을 인스턴스화할 때 해당 매개변수가 시크릿 리소스로 저장되었습니다. 템플릿이 제거되면 시크릿이 그대로 유지됩니다. 이로 인해 불필요한 빌드가 클러스터에 생성되었습니다. 이번 업데이트를 통해 템플릿 인스턴스에 매핑되는 시크릿에 소유권 참조가 추가됩니다. 이제 템플릿 인스턴스가 제거되면 시크릿도 제거됩니다. (BZ#2015042)

- 이번 업데이트를 통해 **jsonData** 속성이 더 이상 사용되지 않고 **ping** 소스의 **데이터로** 교체되었습니다. (BZ#2084438)

- 이전에는 OpenShift Container Platform 웹 콘솔의 토폴로지 보기가 실패했거나 노드가 100개 이상인 클러스터의 경우 지연되었습니다. 이번 업데이트를 통해 토폴로지 보기에 노드가 100개 이상인 클러스터의 **LimitExceeded** 상태가 표시됩니다. 대신 **검색** 페이지를 사용하여 리소스를 볼 수 있는 옵션이 제공됩니다. 또는 토폴로지 보기를 계속 로드 **하려면 토폴로지 표시를** 클릭할 수 있습니다. (BZ#2060329)

- 이전 버전에서는 서비스가 여러 서비스 포트를 노출하고 경로 대상 포트가 **8080** 인 경우 대상 포트를 변경하려고 하면 다른 서비스 포트가 포트 **8080** 서비스 포트 대신 업데이트됩니다. 이번 업데이트를 통해 새 대상 포트가 설정되면 활성 대상 포트에 해당하는 서비스 포트가 교체됩니다. (BZ#2077943)

- 이전에는 리포지토리 정보를 가져오기 위해 인스턴스 API를 관리하는 데 사용된 **git** 탐지가 자체 호스팅 GitHub 및 Bitbucket의 리포지토리에 작동하지 않았습니다. 이번 업데이트를 통해 자체 호스팅 GitHub 및 Bitbucket 인스턴스 리포지토리에 대한 검색이 작동합니다. (BZ#2038244)

- 이전에는 **apiVersion** 이 **EventSource** 생성 양식의 **리소스** 드롭다운 메뉴에 올바른 형식으로 전달되지 않았습니다. 이로 인해 **InContext** 가 **EventSource** 생성에서 선택되지 않아 **리소스** 드롭다운 메뉴에서 제외되었습니다. 이번 업데이트를 통해 **리소스** 드롭다운 메뉴에 **InContext** 의 리소스가 포함됩니다. **(BZ#2070020)**

- **이전에는 Pipeline 지표 페이지에 메트릭 쿼리에 대한 모든 API 호출이 표시되고 404 오류로 실패했습니다. 이번 업데이트를 통해 prometheus-tenancy API를 사용하여 파이프라인의 메트릭 데이터를 가져옵니다. 이제 파이프라인 지표 페이지에 적어도 네임스페이스에 대한 액세스 권한이 있는 관리자가 아닌 사용자에게 모든 데이터와 그래프가 표시됩니다. (BZ#2041769)**

- **이전에는 빠른 검색에 액세스하여 Crtl+space 키보드 바로 가기를 사용하여 모달을 추가할 수 있었지만 동일한 키보드 바로 가기를 사용하여 닫을 수 없었습니다. 이번 업데이트를 통해 빠른 검색을 닫고 Ctrl+space 키보드 바로 가기를 사용하여 모달을 추가할 수 있습니다. (BZ#2093586)**

- **이전에는 사용자가 삭제된 경우 사용자 설정에 대해 생성된 리소스가 제거되지 않았습니다. 결과적으로 openshift-console-user-settings 네임스페이스에서 생성된 리소스가 제거되지 않았습니다. 이번 업데이트를 통해 ownerReference 가 생성 시 메타데이터에 추가됩니다. 이렇게 하면 사용자가 더 이상 존재하지 않을 때 리소스를 자동으로 제거할 수 있습니다. (BZ#2019564)**

1.7. 기술 프리뷰 기능

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

기술 프리뷰 기능 지원 범위

아래 표에서 기능은 다음 상태로 표시됩니다.

- **TP:** *기술 프리뷰*

- **GA:** *상용 버전*

- **-:** *사용할 수 없음*
- **DEP:** *더 이상 사용되지 않음*

표 1.2. 기술 프리뷰

기능	OCP 4.9	OCP 4.10	OCP 4.11
경계 클럭으로 구성된 PTP 단일 NIC 하드웨어	-	TP	GA
PTP 듀얼 NIC 하드웨어가 경계 클럭으로 구성	-	-	TP
일반 클럭을 사용하는 PTP 이벤트	TP	GA	GA
경계 클럭이 있는 PTP 이벤트	-	TP	GA
OpenShift 빌드에서 공유 리소스 CSI 드라이버 및 빌드 CSI 볼륨 빌드	-	TP	TP
서비스 바인딩	TP	GA	GA
CSI 볼륨 확장	TP	TP	GA
CSI AliCloud Disk Driver Operator	-	GA	GA
CSI Azure Disk Driver Operator	TP	GA	GA
CSI Azure File Driver Operator	-	TP	GA
CSI Azure Stack Hub Driver Operator	GA	GA	GA
CSI GCP PD Driver Operator	GA	GA	GA
CSI IBM VPC Block Driver Operator	-	GA	GA
CSI AWS EFS Driver Operator	TP	GA	GA
CSI vSphere Driver Operator	TP	GA	GA
CSI 자동 마이그레이션 (AWS EBS, Azure 파일, GCP 디스크, VMware vSphere)	TP	TP	TP
CSI 자동 마이그레이션 (Azure Disk, OpenStack Cinder)	TP	TP	GA
CSI 인라인 임시 볼륨	TP	TP	TP

기능	OCP 4.9	OCP 4.10	OCP 4.11
CSI 일반 임시 볼륨	-	-	GA
공유 리소스 CSI 드라이버	-	TP	TP
Local Storage Operator를 통한 자동 장치 검색 및 프로비저닝	TP	TP	TP
OpenShift Pipelines	GA	GA	GA
OpenShift GitOps	GA	GA	GA
OpenShift 샌드박스 컨테이너	TP	GA	GA
kvc로 노드에 커널 모듈 추가	TP	TP	TP
선점되지 않은 우선 순위 클래스	TP	TP	GA
Kubernetes NMState Operator	TP	GA	GA
지원되는 설치 관리자	TP	GA	GA
x86_64 아키텍처의 **kdump**	TP	TP	GA
arm64 아키텍처의 **kdump**	-	-	TP
s390x 아키텍처의 **kdump**	TP	TP	TP
ppc64le 아키텍처의 **kdump**	TP	TP	TP
ARM 플랫폼의 OpenShift	-	GA	GA
서버리스 기능	TP	TP	TP
메모리 관리자	GA	GA	GA
vGPU Cloud의 클라우드 컨트롤러 관리자	-	TP	TP
Amazon Web Services용 클라우드 컨트롤러 관리자	TP	TP	TP
Google Cloud Platform용 클라우드 컨트롤러 관리자	-	TP	TP
IBM Cloud용 클라우드 컨트롤러 관리자	-	TP	TP
Microsoft Azure용 클라우드 컨트롤러 관리자	TP	TP	TP

기능	OCP 4.9	OCP 4.10	OCP 4.11
RHOSP(Red Hat OpenStack Platform)의 클라우드 컨트롤러 관리자	TP	TP	TP
VMware vSphere용 클라우드 컨트롤러 관리자	-	TP	TP
드라이버 툴킷	TP	TP	TP
SRO(Special Resource Operator)	TP	TP	TP
간단한 컨텐츠 액세스	TP	GA	GA
Node Health Check Operator	TP	TP	GA
보조 네트워크에 대한 Pod 수준 본딩	-	GA	GA
IPv6 듀얼 스택	GA	GA	GA
선택 가능한 Cluster Inventory	-	TP	TP
이기종 클러스터	-	-	TP
하이퍼 스레딩 인식 CPU 관리자 정책	-	TP	
이기종 클러스터	-	-	TP
Dynamic Plugins	-	TP	TP
Hybrid Helm Operator	-	TP	TP
사용자 정의 프로젝트 모니터링에 대한 경고 라우팅	-	TP	GA
oc-mirror CLI 플러그인을 사용하여 연결 해제된 미러링	-	TP	GA
RHEL의 BuildConfig에 공유 인타이틀먼트 마운트	-	TP	TP
RHEL에서 공유 시크릿 마운트	-	GA	GA
RHOSP DCN 지원	-	TP	TP
RHOSP에서 클러스터용 외부 클라우드 공급자 지원	-	TP	TP
RHOSP에서 클러스터의 OVS 하드웨어 오프로드	-	TP	GA
외부 DNS Operator	-	GA	GA

기능	OCP 4.9	OCP 4.10	OCP 4.11
Web Terminal Operator	TP	GA	GA
플랫폼 모니터링 메트릭을 기반으로 하는 경고 규칙	-	-	TP
AWS Load Balancer Operator	-	-	TP
Node Observability Operator	-	-	TP
Java 기반 Operator	-	-	TP
OpenShift Container Platform에서 호스팅되는 컨트롤 플레인	-	-	TP
클러스터 API를 사용하여 머신 관리	-	-	TP
토폴로지 인식 라이프 사이클 관리자	-	TP	TP
설치 관리자 프로비저닝 인프라를 사용하여 Alibaba Cloud에 클러스터 설치	-	TP	TP

1.8. 확인된 문제

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

  OpenShift Container Platform 4.1에서 **4.11**로 업그레이드된 클러스터의 클러스터 관리자인 경우 인증되지 않은 액세스를 취소하거나 계속 허용할 수 있습니다. 인증되지 않은 액세스가 필요하지 않은 경우 해당 액세스를 취소해야 합니다. 인증되지 않은 액세스를 계속 허용하는 경우 이에 따라 보안 위험이 증가될 수 있다는 점에 유의하십시오.

  주의

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

다음 스크립트를 사용하여 감지 끝점에 대한 인증되지 않은 액세스를 취소하십시오.

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

이 스크립트는 인증되지 않은 주제를 다음 클러스터 역할 바인딩에서 제거합니다.

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

(BZ#1821771)

- 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 edit를 사용하여 주석을 추가합니다. (BZ#1917280)

- 모니터링 스택에서 사용자 정의 경고에 대한 전용 Alertmanager 인스턴스를 활성화 및 배포한 경우 OpenShift Container Platform 웹 콘솔의 개발자 화면에서 경고를 음소거할 수 없습니다. 이 문제는 4.11.8에서 해결되었습니다. (BZ#2100860)

- 새로 설치된 OpenShift Container Platform 4.11 클러스터에서 플랫폼 모니터링 경고에는 openshift_io_alert_source="platform" 레이블이 없습니다. 이 문제는 이전 마이너 버전에서 업그레이드된 클러스터에는 영향을 미치지 않습니다. 현재 이 문제에 대한 해결방법이 없습니다. (BZ#2103127)

- RHOSP(Red Hat OpenStack Platform)에서 포트 풀이 다양한 대량 포트 생성 요청을 동시에 채울 때 Kuryr에 잠재적인 문제가 영향을 미칠 수 있습니다. 이러한 대량 요청 중에 IP 주소 중 하나에 대한 IP 할당이 실패하면 Neutron에서 모든 포트에 대해 작업을 다시 시도합니다. 이 문제는 이전 에라타에서 해결되었지만 대규모 포트 생성 요청을 방지하기 위해 포트 풀 배치에 대해 작은 값을 설정할 수 있습니다. (BZ#2024690)

- oc-mirror CLI 플러그인은 버전 4.9 이전의 OpenShift Container Platform 카탈로그를 미러링할 수 없습니다. (BZ#2097210)

- 이미지 세트 구성의 archiveSize 값이 컨테이너 이미지 크기보다 작으면 oc-mirror CLI 플러그인은 대상 미러 레지스트리에 이미지 세트를 업로드하지 못할 수 있습니다. 이로 인해 카탈로그 디렉터리가 여러 아카이브에 걸쳐 있을 수 있습니다. (BZ#2106461)

- OpenShift Container Platform 4.11에서 MetalLB Operator 범위가 네임스페이스에서 클러스터로 변경되었으며 이로 인해 이전 버전에서 업그레이드가 실패했습니다.

  이 문제를 해결하려면 이전 버전의 MetalLB Operator를 제거하십시오. MetalLB 사용자 정의 리소스의 네임스페이스 또는 인스턴스를 삭제하지 말고 새 Operator 버전을 배포합니다. 이렇게 하면 MetalLB가 실행되고 구성됩니다.

  자세한 내용은 MetalLB Operator 업그레이드를 참조하십시오. (BZ#2100180)

- BFD(Bidirectional forwarding detection) 프로필을 삭제하고 BGP(Border Gateway Protocol) 피어 리소스에 추가된 bfdProfile 을 제거하면 BFD가 비활성화되지 않습니다. 대신 BGP 피어는 기본 BFD 프로필 사용을 시작합니다. BGP 피어 리소스에서 BFD를 비활성화하려면 BGP 피어 구성을 삭제하고 BFD 프로필없이 다시 생성합니다. (BZ#2050824)

- OpenShift Container Platform 4.11용 OpenShift CLI(oc)는 Go 1.18 라이브러리에서 신뢰할 수 없는 인증서의 오류 처리 오류로 인해 macOS에서 제대로 작동하지 않습니다. 이 변경으로 인해 macOS에서 실행할 때 더 이상 진행하지 않고 certificate is not trusted 오류와 함께 oc login 및 기타 oc명령이 실패할 수 있습니다. Go 1.18에서 오류 처리가 올바르게 수정될 때까지(Go issue #52010에 의해 추적됨) 대신 OpenShift Container Platform 4.10 oc CLI를 사용하는 것이 좋습니다. OpenShift Container Platform 4.10 oc CLI를 OpenShift Container Platform 4.11 클러스터와 함께 사용할 때 oc serviceaccounts get-token <service_account> 명령을 사용하여 토큰을 가져올 수 없습니다. (BZ#2097830) (BZ#2109799)

- 현재 Helm 차트 리포지토리 추가 양식에 프로젝트의 개발자 카탈로그를 확장하는 알려진 문제가 있습니다. 빠른 시작 가이드는 원하는 네임스페이스에 ProjectHelmChartRepository CR을 추가할 수 있는 반면 kubeadmin의 권한이 필요한 것은 아닙니다. (BZ#2054197)

- 현재 알려진 문제가 있습니다. TLS 확인을 사용하는 ProjectHelmChartRepository CR(사용자 정의 리소스) 인스턴스를 생성하는 경우 리포지터리를 나열하고 Helm 관련 작업을 수행할 수 없습니다. 현재 이 문제에 대한 해결방법이 없습니다. (HELM-343)

- 베어 메탈 IBM Power에서 OpenShift Container Platform을 실행할 때 Petitboot 부트로더가 일부 RHCOS 라이브 이미지의 부팅 구성을 채울 수 없는 알려진 문제가 있습니다. 이러한 경우 PXE로 노드를 부팅하여 RHCOS를 설치하면 예상되는 라이브 이미지 디스크 구성이 표시되지 않을 수 있습니다.

  이 문제를 해결하려면 Petitboot 셸에서 kexec를 사용하여 수동으로 부팅할 수 있습니다.

  라이브 이미지를 보유한 디스크를 확인합니다(이 예제에서는 nvme0n1p3)를 실행하고 다음 명령을 실행합니다.

  ```
  # cd /var/petitboot/mnt/dev/nvme0n1p3/ostree/rhcos-*/
  # kexec -l vmlinuz-*.ppc64le -i initramfs-*.img -c "ignition.firstboot rd.neednet=1
  ip=dhcp $(grep options /var/petitboot/mnt/dev/nvme0n1p3/loader/entries/ostree-1-
  rhcos.conf | sed 's,^options ,,')" && kexec -e
  ```

  (BZ#2107674)

- 연결이 끊긴 환경에서 SRO는 기본 레지스트리에서 DTK를 가져오지 않습니다. 대신 미러 레지스트리에서 가져옵니다. (BZ#2102724)

- 프로세스 카운터는 phc2sys가 실행되고 있지 않은 인터페이스에서 phc2sys 프로세스에 대한 잘못된 정보를 표시합니다. 현재 이 문제에 대한 해결방법이 없습니다. (OCPBUGSM-46005)

- 듀얼 NIC PTP 구성이 있는 노드의 NIC(네트워크 인터페이스 컨트롤러)가 종료되면 두 PTP 인터페이스에 결함이 있는 이벤트가 생성됩니다. 현재 이 문제에 대한 해결방법이 없습니다. (OCPBUGSM-46004)

- 저 대역폭 시스템에서, 시스템 클럭이 몇 시간 동안 연결이 끊어지고 복구된 후 시스템 클럭이 PTP 일반 클럭과 동기화되지 않습니다. 현재 이 문제에 대한 해결방법이 없습니다.

(OCPBUGSM-45173)

- 이전 버전에서는 OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 경우 type=LoadBalancer 가 있는 서비스가 internalTrafficPolicy=cluster 설정으로 구성된 경우 호스트 라우팅 테이블에 더 나은 경로가 포함되어 있어도 모든 트래픽이 기본 게이트웨이로 라우팅되었습니다. 이제 항상 기본 게이트웨이를 사용하는 대신 최상의 경로가 사용됩니다. (BZ#2060159)

- OVN 클러스터에 작업자 노드가 75개 이상인 경우 2000개 이상의 서비스와 라우팅 오브젝트를 동시에 생성하면 생성된 Pod가 ContainerCreating 상태로 중단될 수 있습니다. 이 문제가 발생하면 oc describe pod <podname> 명령을 입력하면 다음과 같은 경고가 표시됩니다. FailedCreatePodSandBox…failed to configure pod interface: timed out waiting for OVS port binding (ovn- installed) . 현재 이 문제에 대한 해결방법이 없습니다. (BZ#2084062)

- 현재 OVN-Kubernetes에는 NetworkManager 서비스가 노드를 재시작할 때마다 네트워크 연결이 끊어지고 복구되어야 하는 알려진 문제가 있습니다. (BZ#2074009)

- 기본 SCC(보안 컨텍스트 제약 조건)로 인해 일반 임시 볼륨을 사용하는 Pod가 Pending 상태로 유지될 수 있습니다. 이 문제를 해결하려면 사용자 지정 SCC를 생성할 수 있습니다. 자세한 내용은 SCC 오류로 인해 일반 임시 볼륨이 있는 Pod를 참조하십시오. 해결방법은 일반 임시 볼륨 사용 허용을 참조하십시오. (BZ#2100429)

- OpenShift 샌드박스 컨테이너가 있는 경우 클러스터를 업그레이드할 때 MCO(Machine Config Operator) Pod가 CrashLoopBackOff 상태로 변경되고 Pod의 openshift.io/scc 주석이 기본 hostmount-anyuid 값 대신 sandboxed-containers-operator-scc 가 표시되는 문제가 발생할 수 있습니다.

  이 경우, sandboxed-containers-operator-scc SCC의 seLinuxOptions 전략을 덜 제한적인 RunAsAny 로 일시적으로 변경하여 허용 프로세스가 hostmount-anyuid SCC보다 우선하지 않도록 합니다.

  1. 다음 명령을 실행하여 seLinuxOptions 전략을 변경합니다.

     ```
     $ oc patch scc sandboxed-containers-operator-scc --type=merge --patch
     '{"seLinuxContext":{"type": "RunAsAny"}}'
     ```

  2. 다음 명령을 실행하여 MCO Pod를 다시 시작합니다.

     ```
     $ oc scale deployments/machine-config-operator -n openshift-machine-config-
     operator --replicas=0
     ```

```
$ oc scale deployments/machine-config-operator -n openshift-machine-config-
operator --replicas=1
```

3. 다음 명령을 실행하여 **sandboxed-containers-operator-scc** 의 **seLinuxOptions** 전략을 원래 **MustRunAs** 값으로 되돌립니다.

```
$ oc patch scc sandboxed-containers-operator-scc --type=merge --patch
'{"seLinuxContext":{"type": "MustRunAs"}}'
```

4. 다음 명령을 실행하여 **hostmount-anyuid SCC**가 **MCO Pod**에 적용되었는지 확인합니다.

```
$ oc get pods -n openshift-machine-config-operator -l k8s-app=machine-config-
operator -o yaml | grep scc
openshift.io/scc: hostmount-anyuid
```

(KATA-1373)

- 파이프라인 메트릭 **API**는 **RHOSP 1.6** 이상의 필수 **pipelinerun/taskrun histogram** 값을 지원하지 않습니다. 결과적으로 잘못된 값을 표시하는 대신 **Pipeline → Details** 페이지의 지표 탭이 제거됩니다. 현재 이 문제에 대한 해결방법이 없습니다. (link: BZ#2074767)

- 일부 **Alibabacloud** 서비스는 클러스터의 모든 리소스를 지정된 리소스 그룹에 배치하지 않습니다. 결과적으로 **OpenShift Container Platform** 설치 프로그램에서 생성된 일부 리소스는 기본 리소스 그룹에 배치됩니다. 현재 이 문제에 대한 해결방법이 없습니다. (BZ#2096692)

- 각 클러스터 노드를 재부팅한 후 클러스터 **Operator** 네트워크 및 **kube-apiserver** 가 클러스터의 각 노드를 재부팅한 후 성능이 저하되고 클러스터가 비정상 상태가 됩니다. 현재 이 문제에 대한 해결방법이 없습니다. (BZ#2102011)

- **install-config.yaml** 에 **resourceGroupID** 를 지정하면 부트스트랩 리소스를 삭제할 때 오류가 표시되고 **OpenShift Container Platform** 설치가 실패합니다. 이 문제에 대한 해결 방법으로 **install-config.yaml** 에 **resourceGroupID** 를 지정하지 마십시오. (BZ#2100746)

- **RHEL** 컴퓨팅 노드의 스케일 업과 관련하여 알려진 문제가 있습니다. 새 노드가 **Ready** 로 변경될 수 있지만 **Ingress Pod**는 이러한 노드에서 실행 중으로 전환할 수 없으며 확장에 성공할 수 없습니다. 해결 방법으로 **RHCOS** 노드를 사용한 확장 기능이 작동합니다. (BZ#2056387)

-

GCP(Google Cloud Platform)에 머신 세트를 생성한 후 capg-controller-manager 시스템이 프로비저닝에 남아 있습니다. 현재 이 문제에 대한 해결방법이 없습니다. (BZ#2107999)

- 클러스터에서 생성한 PV(영구 볼륨)가 destroy cluster 명령으로 정리되지 않는 Nutanix에 알려진 문제가 있습니다. 이 문제에 대한 해결 방법으로 PV를 수동으로 정리해야 합니다. (BZ#2108700)

- Nutanix 설치에는 Prism Central 2022.x에서 4096비트 인증서를 사용하는 경우 설치에 실패하는 알려진 문제가 있습니다. 대신 2048비트 인증서를 사용합니다. (KCS)

- 현재 잘못된 구문 또는 값이 성공으로 egressqos 를 생성하고 편집할 때 알려진 문제가 있습니다. egressqos 의 잘못된 값이 성공적으로 생성되지 않아야 합니다. 현재 이 문제에 대한 해결 방법이 없습니다. (BZ#2097579)

- 일부 이미지 인덱스에 이전 이미지가 포함되므로 oc adm catalog mirror 및 oc image mirror 를 실행하면 소스 이미지를 검색할 수 없습니다. error: unable to retrieve source image. 임시 해결 방법으로 --skip-missing 옵션을 사용하여 오류를 무시하고 이미지 인덱스를 계속 다운로드할 수 있습니다. 자세한 내용은 Service Mesh Operator 미러링 실패 에서 참조하십시오.

- VF(가상 기능)가 이미 존재하는 경우 물리적 기능(PF)에 macvlan을 생성할 수 없습니다. 이 문제는 Intel E810 NIC에 영향을 미칩니다. (BZ#2120585)

- ZTP를 통해 배포된 클러스터에 호환되지 않는 정책이 있고 ClusterGroupUpdates 오브젝트가 없는 경우 TALM Pod를 다시 시작해야 합니다. TALM을 다시 시작하면 적절한 ClusterGroupUpdates 오브젝트가 생성되어 정책 준수를 적용합니다. (OCPBUGS-4065)

- 현재 x509: 인증서로 특히 출력되는 인증서 컴플라이언스 문제는 VMware vSphere에 OpenShift Container Platform 클러스터를 설치하기 위해 macOS에서 설치 프로그램을 실행할 때 존재합니다. 이 문제는 컴파일러가 새로 지원되는 macOS 인증서 표준을 인식하지 못하는 golang 컴파일러의 알려진 문제와 관련이 있습니다. 이 문제에 대한 해결방법이 없습니다. (OSDOCS-5694)

- 현재 매우 많은 수의 파일이 포함된 PV(영구 볼륨)를 사용하는 경우 Pod가 시작되지 않거나 시작하는 데 과도한 시간이 걸릴 수 있습니다. 자세한 내용은 기술 자료 문서를 참조하십시오. (BZ1987112)

1.9. 비동기 에라타 업데이트

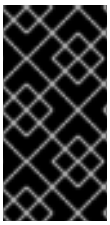
OpenShift Container Platform 4.11의 보안, 버그 수정 및 개선 사항 업데이트는 Red Hat Network를 통해 비동기 에라타로 릴리스됩니다. 모든 OpenShift Container Platform 4.11 에라타는 Red Hat Customer Portal을 통해 제공됩니다. 비동기 에라타에 대한 자세한 내용은 OpenShift Container Platform 라이프 사이클에서 참조하십시오.

Red Hat Customer Portal 사용자는 Red Hat 서브스크립션 관리(RHSM) 계정 설정에서 에라타 통지를 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 Platform에서 에라타 통지 이메일을 생성하기 위해 OpenShift Container Platform을 사용할 수 있는 등록된 시스템 및 권한이 필요합니다.

이 섹션은 향후 OpenShift Container Platform 4.11의 비동기 에라타 릴리스의 개선 사항 및 버그 수정에 대한 정보 제공을 위해 지속적으로 업데이트됩니다. OpenShift Container Platform 4.11.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 확인하십시오.

1.9.1. RHSA-2022:5069 - OpenShift Container Platform 4.11.0 이미지 릴리스, 버그 수정 및 보안 업데이트 권고

출시 날짜: 2022-08-10

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.10.0을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:5069 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:5068 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.0 --pullspecs
```

1.9.2. RHSA-2022:6103 - OpenShift Container Platform 4.11.1 버그 수정 및 보안 업데이트

출시 날짜: 2022-08-23

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.1을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:6103 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:6102 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.1 --pullspecs
```

1.9.2.1. 기능

1.9.2.1.1. 보조 네트워크에 대한 Pod 수준 본딩의 일반 가용성

이번 업데이트를 통해 이제 Pod 수준 본딩 을 일반적으로 사용할 수 있습니다.

1.9.2.2. 버그 수정

- 이전에는 Bond-CNI의 기능이 active-backup 모드로만 제한되었습니다. 이번 업데이트에서는 지원되는 본딩 모드는 다음과 같습니다.
  - balance-rr - 0
  - active-backup - 1
  - balance-xor - 2

  (BZ#2102047)

1.9.2.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.3. RHBA-2022:6143 - OpenShift Container Platform 4.11.2 버그 수정 업데이트

출시 날짜: 2022-08-29

OpenShift Container Platform 릴리스 4.11.2가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6143 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:6142 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.2 --pullspecs
```

1.9.3.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.4. RHSA-2022:6287 - OpenShift Container Platform 4.11.3 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2022-09-06

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.3을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:6287 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:6286 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.3 --pullspecs
```

1.9.4.1. 기능

1.9.5. 확장 및 성능

OpenShift Container Platform 4.11.3부터는 더 이상 agent_service_config.yaml 파일에서 루트 FS 이미지 URL(rootFSUrl)을 설정할 필요가 없습니다. 이제 rootFSUrl 이 자동으로 처리됩니다.

1.9.5.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.6. RHBA-2022:6376 - OpenShift Container Platform 4.11.4 버그 수정 업데이트

출시 날짜: 2022-09-12

OpenShift Container Platform 릴리스 4.11.4가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6376 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:6375 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.4 --pullspecs
```

1.9.6.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.7. RHSA-2022:6536 - OpenShift Container Platform 4.11.5 버그 수정 및 보안 업데이트

출시 날짜: 2022-09-20

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.5를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:6536 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:6535 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.5 --pullspecs
```

1.9.7.1. 확인된 문제

-

기본 Ingress 컨트롤러를 분할하면 카나리아 oauth,oauth, 콘솔 과 같은 OpenShift Container Platform 오타리 경로가 중단됩니다. 이 문제를 해결하려면 일치하는 라벨과 표현식을 경로에 수동으로 추가할 수 있습니다. (BZ#2024946)

1.9.7.2. 버그 수정

- 이전 버전에서는 routeSelector 업데이트에서 라우터 배포 전에 Ingress 컨트롤러의 경로 상태를 제거했습니다. 그 결과 경로 상태가 잘못 입력되었습니다. 이번 업데이트를 통해 routeSelector 업데이트를 통해 경로 상태가 지워집니다. (BZ#2110528)

1.9.7.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.8. RHBA-2022:6659 - OpenShift Container Platform 4.11.6 버그 수정 업데이트

출시 날짜: 2022-09-28

OpenShift Container Platform 릴리스 4.11.6이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6659 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:6658 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.6 --pullspecs
```

1.9.8.1. OpenShift Container Platform 4.11 RAN 새로운 기능

1.9.8.1.1. 업데이트 실패 후 클러스터 복구

단일 노드 OpenShift의 경우 OpenShift Container Platform 버전 업데이트 전에 Topology Aware Lifecycle Manager (TALM) Operator를 사용하여 현재 배포 백업을 생성할 수 있습니다. 업데이트에 실패하면 백업을 사용하여 클러스터를 업데이트 전 상태로 반환합니다. 자세한 내용은 업그레이드하기 전에 클러스터 리소스의 백업 생성 을 참조하십시오.

1.9.8.1.2. PolicyGenTemplate 사용자 정의 리소스(CR)에서 chronyd 비활성화

이전 버전에서 OpenShift Container Platform 4.11로 업데이트하는 경우 chronyd 를 비활성화해야

합니다. chronyd 를 비활성화하려면 TunedPerformancePatch.yaml 파일의 .spec.profile.data 아래의 [service] 섹션에 다음 행을 추가합니다. TunedPerformancePatch.yaml 파일은 PolicyGenTemplate CR 그룹에서 참조됩니다.

```
[service]
service.chronyd=stop,disable
```

자세한 내용은 권장 클러스터 커널 구성 을 참조하십시오.

1.9.8.2. OpenShift Container Platform 4.11 RAN 알려진 문제

- RAN DU 프로필을 사용하여 단일 노드 OpenShift 클러스터를 배포한 후 openvswitch 오류: 핸들러 스레드와의 cpu_id 불일치 가 Open vSwitch 커널 로그에 지속적으로 생성됩니다. (OCPBUGSM-46165)

- 보안 부팅이 현재 비활성화되어 있고 ZTP를 사용하여 활성화하려고 하면 클러스터 설치가 시작되지 않습니다. ZTP를 통해 보안 부팅을 활성화하면 가상 CD를 연결하기 전에 부팅 옵션이 구성됩니다. 따라서 기존 하드 디스크에서 첫 번째 부팅 시 보안 부팅이 설정되어 있습니다. CD에서 시스템이 부팅되지 않기 때문에 클러스터 설치가 중지됩니다. (OCPBUGSM-45085)

- 클러스터 업그레이드를 수행하는 데 사용되는 서브스크립션 정책에 유효하지 않은 서브스크립션 채널이 지정된 경우, Subscription 상태가 AtLatestKnown 이므로 정책 적용 직후 Topology Aware Lifecycle Manager가 성공적으로 업그레이드되었음을 나타냅니다. (OCPBUGSM-43618)

- SRIOV-FEC Operator가 별도의 정책을 통해 설치되고 CatalogSource 에서 기본 카탈로그 소스의 이름을 재사용하는 경우 기본 카탈로그 소스 관리와 충돌하여 Operator 설치에 실패할 수 있습니다. 이 문제를 방지하려면 SRIOV-FEC CatalogSource CR을 common-config-policy 에 추가해야 하며 Operator 서브스크립션을 common-subscriptions-policy 에 추가해야 합니다. 별도의 정책을 사용하여 SRIOV-FEC Operator를 설치하는 경우 이 Operator의 CatalogSource 이름을 고유하게 지정해야 합니다. (OCPBUGSM-39859)

- 클러스터 의 여러 노드에 적용되는 경우 siteConfig 디스크 파티션 정의가 실패합니다. site Config CR을 사용하여 컴팩트 클러스터를 프로비저닝하는 경우 Kustomize 플러그인 오류로 여러 노드에서 유효한 디스크 파티션 구성을 생성할 수 없습니다. (OCPBUGSM-44403)

- ZTP 컨테이너를 사용하여 ArgoCD 리소스를 패치하면 패치는 해당 릴리스 버전의 최신 컨테이너 버전을 따르는 태그를 가리킵니다. ZTP 컨테이너를 릴리스 내의 특정 버전에 고정하려면 패치 파일 argocd-openshift-gitops-patch.json 을 특정 버전을 가리키도록 업데이트해야 합니다. (OCPBUGSM-44261)

- BMCEventSubscription CR을 적용하지 못하여 Redfish 이벤트 서브스크립션을 생성하지 못합니다. 서브스크립션 YAML 파일이 생성되고 적용되면 활성 Redfish 서브스크립션이 표시되지 않습니다. 이 문제를 해결하려면 API를 직접 호출하고 서브스크립션을 생성합니다. 예를 들면 다음과 같습니다.

  1. 다음 명령을 실행하여 인증 토큰을 가져옵니다.

```
$ curl -i --insecure --request POST --header "OData-Version: 4.0" \
--header "Content-Type: application/json" -d '{"UserName": <BMC_USERNAME>, \
"Password": <BMC_PASSWORD>}'
https://<BMC_IP>/redfish/v1/SessionService/Sessions/ |grep 'X-Auth-Token'
```

  출력 예

```
X-Auth-Token: 1234abcd5678efgh9012ijkl3456mnop
```

  2. 인증 토큰을 사용하여 Redfish 이벤트 서브스크립션을 생성합니다.

```
$ curl -X POST -i --insecure --header "X-Auth-Token:
1234abcd5678efgh9012ijkl3456mnop" \
-H 'Content-Type: application/json' --data-raw '{"Protocol": "Redfish", "Context": \
"Public", "Destination": "https://hw-event-proxy-openshift-hw-
events.apps.example.com/webhook", \
"EventTypes": ["Alert"]}' https://<BMC_IP>/redfish/v1/EventService/Subscriptions
```

  Redfish 이벤트 서브스크립션이 성공적으로 생성되었음을 나타내는 Location: https://<BMC_IP>/redfish/v1/EventService/Subscriptions/35 인 헤더와 201 Created 응답이 표시되어야 합니다. (OCPBUGSM-43707)

- GitOps ZTP 파이프라인을 사용하여 연결이 끊긴 환경에 단일 노드 OpenShift 클러스터를 설치하는 경우 클러스터에 적용되는 두 개의 CatalogSource CR이 있어야 합니다. CatalogSource CR 중 하나가 여러 노드를 재부팅한 후 삭제됩니다. 이 문제를 해결하려면 카탈로그 소스의 certified-operators 및 redhat-operators 와 같은 기본 이름을 변경할 수 있습니다. (OCPBUGSM-46245)

- 확장 테스트 중에 여러 클러스터를 업데이트하지 못했습니다. Telecom vDU 구성이 적용된 OpenShift Container Platform 4.9.26 업데이트를 시작한 후 ClusterVersion CR을 사용하여 시

작된 4.10.13으로 클러스터 업데이트가 실패하고 클러스터 Operator가 대상 버전으로 업데이트 될 때까지 기다립니다. (OCPBUGSM-44655)

- ZTP GitOps 파이프라인 단일 노드 OpenShift 설치 중에 Operator Lifecycle Manager registry-server 컨테이너가 READY 상태에 도달하지 못하는 경우가 있습니다. 새 CatalogSource 를 사용하여 서브스크립션을 생성할 때 CatalogSource 는 TRANSIENT_FAILURE 상태로 유지됩니다. (OCPBUGSM-44041)

- Pod에 tuned 덮어쓰기를 적용하고 tuned Pod를 삭제하여 다시 시작할 때 Pod를 다시 시작해야 하며 시스템이 정상적으로 실행되어야 합니다. 대신 systemd 중단이 발생하여 시스템이 응답하지 않을 수 있습니다. (RHELPLAN-131021)

- 정적 IPv6 주소 구성이 있는 라이브 ISO에서 ZT Systems 시스템을 부팅할 때 NetworkManager 는 인터페이스 링크가 준비되기 전에 성공적으로 종료됩니다. 그러면 네트워크 인터페이스가 구성 없이 유지됩니다. 이 문제를 해결하려면 AgentServiceConfig CR에서 참조하는 RHCOS ISO를 편집하여 grub.cfg 파일의 커널 매개변수에 rd.net.timeout.carrier 를 추가합니다.

  1. 설치 중인 릴리스의 rhcos-live ISO 이미지를 가져옵니다. 다음 명령을 실행하여 hub 클러스터의 AgentServiceConfig CR에서 URL을 검색할 수 있습니다.

     ```
     $ oc get AgentServiceConfig agent -o yaml
     ```

  2. /mnt/iso/ 디렉터리에 이미지를 마운트합니다.

     ```
     $ mount rhcos-live.x86_64.iso /mnt/iso/
     ```

  3. iso-grub-cfg/ 디렉터리를 생성하고 디렉터리로 변경합니다.

     ```
     $ mkdir iso-grub-cfg/; pushd iso-grub-cfg/
     ```

  4. /mnt/iso/ 디렉터리의 콘텐츠를 작업 디렉터리에 복사합니다.

     ```
     $ rsync -avH /mnt/iso/* .
     ```

  5. GRUB 설정 파일을 엽니다.

     ```
     $ vim EFI/redhat/grub.cfg
     ```

-

a. linux 부팅 줄에 rd.net.timeout.carrier=20 문자열을 추가합니다.

6. 다음 명령을 실행하여 초기 작업 디렉터리로 돌아갑니다.

```
$ popd
```

7. iso-grub-cfg 디렉토리에서 ISO 파일을 생성합니다.

```
$ mkisofs -JR -graft-points -o rhcos-carrier-timeout.iso iso-grub-cfg
```

8. 업데이트된 ISO 이미지를 hub 클러스터에서 액세스할 수 있는 서버로 푸시합니다.

9. hub 클러스터에서 업데이트된 ISO 이미지를 가리키도록 설치 릴리스의 AgentServiceConfig CR의 osImages 항목을 업데이트합니다.

```
$ oc edit AgentServiceConfig agent
```

10. 업데이트된 ISO 이미지의 URL을 참조하도록 url 필드를 업데이트합니다.

(OCPBUGSM-46336)

- 커널 오류는 DU 프로필 및 워크로드 테스트 애플리케이션을 사용하여 베어 메탈 SNO를 재부팅한 후 발생합니다. 이 문제를 해결하려면 성능 프로필에 추가 커널 매개변수를 추가할 수 있습니다.

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
spec:
  additionalKernelArgs:
  - rcutree.kthread_prio=11
```

(RHELPLAN-123262)

- ZTP 클러스터 배포 중에 HTTP 412 오류 코드를 참조하는 오류로 인해 베어 메탈 호스트 이미지 프로비저닝이 실패할 수 있습니다.

> **Deploy step deploy.deploy failed with HTTPError: HTTP PATCH https://10.16.230.34/redfish/v1/Managers/1/VirtualMedia/EXT1 returned code 412. Base.1.8.GeneralError: A general error has occurred. See ExtendedInfo for more information. Extended information: [**
>
> **{'MessageSeverity': 'Critical', 'MessageArgs': [], 'MessageId': 'Base.1.8.PreconditionFailed', 'Resolution': 'Try the operation again using the appropriate ETag.', '@odata.type': '#Message.v1_1_0.Message', 'Message': 'The ETag supplied did not match the ETag required to change this resource.'}]**

이 문제는 이전 펌웨어를 실행하는**ECDHE8 HP** 시스템 및 **FlexVolume9** 시스템을 포함한 다양한 서버 모델에 영향을 미칠 수 있습니다. **ECDHE9 HP** 시스템의 경우 최신 **iLO** 펌웨어로 업그레이드하면 이 문제가 해결될 수 있습니다. **FlexVolume8 HP** 및 기타 시스템의 경우 현재 이 문제에 대한 해결방법이 없습니다. (**OCPBUGS-1246**)

- 특정**ECDHE** 모델의 경우, 예를 들어 **ZTP** 클러스터 배포 중 베어 메탈 호스트 이미지 프로비저닝이 **HTTP 400** 상태 코드와 **PropertyNotWriteable** 오류로 실패할 수 있습니다.

> **HTTP response for PATCH https://192.168.26.178/redfish/v1/Systems/1/Pending: status code: 400, error: Base.1.8.GeneralError: A general error has occurred. See ExtendedInfo for more information., extended: [{'MessageArgs': ['BootSourceOverrideEnabled'], 'Resolution': 'Remove the property from the request body and resubmit the request if the operation failed.', MessageId': 'Base.1.8.PropertyNotWritable', 'Message': 'The property BootSourceOverrideEnabled is a read only property and cannot be assigned a value.', '@odata.type': '#Message.v1_1_0.Message', 'MessageSeverity': 'Warning'}]**

현재 이 문제에 대한 해결방법이 없습니다. (**OCPBUGSM-46305**)

- 베어 메탈 클러스터에서 기본 노드 교체 중에 새 기본 호스트가 프로비저닝 상태로 유지되지만 노드는 클러스터에 **Ready** 로 보고합니다. (**OCPBUGSM-45772**)

- **RHACM(Red Hat Advanced Cluster Management)**을 사용하면 가상 미디어가 디스크에 이미지를 작성한 후 **iDRAC** 콘솔에서 **ISO**의 연결을 끊지 않으면 **Dell PowerEdge R640** 서버에서 클러스터 배포가 차단됩니다. 이 문제를 해결하려면 **iDRAC** 콘솔의 가상 미디어 탭을 통해 **ISO**를 수동으로 연결을 끊습니다. (**OCPBUGSM-45884**)

- 듀얼 스택 네트워킹 환경에서 장치 및 연결은 **nm-initrd-generator** 유틸리티에서 생성된 기본 **dhcp6** 프로필로 **ip-check** 상태로 유지됩니다. 이 문제로 인해 **/etc/resolve.conf** 파일이 생성되지 않습니다. 해결 방법으로 **NetworkManager** 서비스를 다시 시작합니다. 그러면 누락된 **/etc/resolve.conf** 파일이 생성되고 설치를 계속할 수 있습니다. (**RHELPLAN-127788**, **OCPBUGS-70**)

- Dell 하드웨어에서 NVIDIA 브랜드 Mellanox NIC를 사용하는 경우 사전 설정된 F5 애플리케이션 수신 버퍼보다 큰 들어오는 패킷이 잘못된 VLAN 태그를 사용하여 도착합니다. 이로 인해 NIC에서 예기치 않게 잘린 패킷이 제공됩니다. (RHELPLAN-123058)

- 고정 IP로 구성되어 GitOps ZTP 파이프라인을 사용하여 배포된 단일 노드 OpenShift 노드는 2일차 Operator 구성 중에 연결할 수 없습니다. OpenShift Container Platform 클러스터 설치가 성공적으로 완료되고 클러스터가 정상입니다. 재부팅하면 네트워크 인터페이스를 사용하여 노드에 연결할 수 없습니다. (OCPBUGSM-46688)

- Git 리포지토리에서 SriovNetworkNodePolicy 정책을 제거한 후 삭제된 정책에서 관리하는 SriovNetworkNodePolicy 리소스는 스포크 클러스터에 남아 있습니다. (OCPBUGSM-34614)

- PTP Operator를 4.10에서 4.11로 업그레이드하는 경우 OpenShift 서브스크립션에서 "ptp-operator" 의 채널 "stable" 에 있는 다른 항목으로 대체되지 않는 채널 헤드 (entries notries) 오류를 보고합니다. 그러나 Operator 업그레이드가 성공적으로 수행됩니다. (OCPBUGSM-46114)

- 현재 ZTP 소스 CR의 모든 PtpConfig CR에는 phc2sysOpts 옵션이 포함되어 있습니다. 따라서 사용자가 사용자 PolicyGenTemplate CR에 phc2sysOpts 를 포함하지 않는 경우에도 phc2sysOpts 옵션이 설명된 PTP 구성에 추가됩니다. 듀얼 NIC가 있는 PTP가 ZTP를 통해 구성된 경우 ZTP가 완료된 후 phc2sysOpts 옵션을 제거하려면 사용자가 하나의 PtpConfig CR을 업데이트해야 합니다. (OCPBUGSM-47798)

- 보안 부팅이 활성화된 경우 /sys/kernel/debug/sched_features 파일을 열 수 없기 때문에 서비스가 시작되지 않습니다. (OCPBUGSM-1466)

- 보안 부팅이 활성화되면 kdump 서비스가 kexec: kdump 커널 오류를 로드하지 못할 수 있습니다. 이 문제를 해결하려면 커널 인수에 efi=runtime 을 추가합니다. (OCPBUGSM-97)

- SNO 클러스터가 OCP 4.10에서 OCP 4.11로 업그레이드된 경우 업그레이드 프로세스 중에 SNO 클러스터가 3번 재부팅될 수 있습니다. (OCPBUGSM-46704)

- ZTP를 통해 Supermicro 서버를 배포하면 잘못된 부팅 장치를 선택하여 설치가 시작되지 않을 수 있습니다. (OCPBUGSM-369)

- 기본 dns-default Pod에는 "target.workload.openshift.io/management:" 주석이 없습니다. 결과적으로 SNO에서 워크로드 파티션 기능이 활성화되면 Pod 리소스가 변경되어 예약된

CPU 세트에 고정되지 않습니다. 이 문제를 해결하려면 클러스터 관리자가 다음 명령을 사용하여 주석을 수동으로 추가할 수 있습니다.

```
$ oc annotate pod dns-default
target.workload.openshift.io/management='{"effect":"PreferredDuringScheduling"}' -n
openshift-dns
```

(OCPBUGSM-753)

1.9.8.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.9. RHSA-2022:6732 - OpenShift Container Platform 4.11.7 버그 수정 업데이트

출시 날짜: 2022-10-03

OpenShift Container Platform 릴리스 4.11.7이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6732 권고에 설명되어 있습니다. 이 업데이트를 위한 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.7 --pullspecs
```

1.9.9.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.10. RHBA-2022:6809 - OpenShift Container Platform 4.11.8 버그 수정 업데이트

출시 날짜: 2022-10-12

OpenShift Container Platform 릴리스 4.11.8이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6809 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:6808 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.8 --pullspecs
```

1.9.10.1. 버그 수정

- 이전에는 모니터링 스택에서 사용자 정의 경고에 전용 **Alertmanager** 인스턴스를 활성화 및 배포한 경우 **OpenShift Container Platform** 웹 콘솔의 개발자 화면에서 경고를 음소거할 수 없습니다. 이번 업데이트를 통해 개발자 관점에서 사용자 정의 경고를 음소거할 수 있습니다. (OCPBUGS-1790)

1.9.10.2. 업데이트

기존 **OpenShift Container Platform 4.11** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.11. RHBA-2022:6897 - OpenShift Container Platform 4.11.9 버그 수정 업데이트

출시 날짜: 2022-10-17

OpenShift Container Platform 릴리스 **4.11.9**가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6897 권고에 설명되어 있습니다. 업데이트에 포함된 **RPM** 패키지는 RHBA-2022:6896 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.9 --pullspecs
```

1.9.11.1. 업데이트

기존 **OpenShift Container Platform 4.11** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.12. RHSA-2022:7201 - OpenShift Container Platform 4.11.12 버그 수정 및 보안 업데이트

출시 날짜: 2022-11-02

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.12를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:7201 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:7200 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.12 --pullspecs
```

1.9.12.1. 확인된 문제

- 클러스터가 4.9 이하 버전에서 점진적으로 업데이트되는 경우 openshift-dns 네임스페이스에 향후 버전 업데이트에 필요한 pod-security 라벨이 포함되어 있지 않을 수 있습니다. (OCPBUGS-1549)

1.9.12.2. 주요 기술 변경 사항

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

자세한 내용은 볼륨 프로젝션을 사용하여 서비스 계정 토큰 구성 을 참조하십시오.

1.9.12.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.13. RHBA-2022:7201 - OpenShift Container Platform 4.11.13 버그 수정 업데이트

출시 날짜: 2022-11-09

OpenShift Container Platform 릴리스 4.11.13이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:7290 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:7289 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.13 --pullspecs
```

1.9.13.1. 주요 기술 변경 사항

- 이제 Cloud Credential Operator 유틸리티(ccoctl)에서 AWS STS(AWS Security Token Service) 에 리전 끝점을 사용하는 시크릿을 생성합니다. 이 접근 방식은 AWS 권장 모범 사례와 일치합니다.

1.9.13.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.14. RHSA-2022:8535 - OpenShift Container Platform 4.11.16 버그 수정 및 보안 업데이트

출시 날짜: 2022-11-24

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.16을 사용할 수 있습니다. 이 릴리스에 대한 IBM Powerbuild가 없습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:8535 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:8534 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.16 --pullspecs
```

1.9.14.1. 주요 기술 변경 사항

- 이번 릴리스에서는 Cloud Credential Operator 유틸리티를 사용하여 GCP 리소스를 삭제할 때 구성 요소 CredentialsRequest 오브젝트에 대한 파일이 포함된 디렉터리를 지정해야 합니다.

1.9.14.2. 버그 수정

- 이전에는 DES(Azure Disk Encryption Set) 또는 RG(Resource Group) 이름을 지정할 때 대문자를 사용한 경우 검증에 실패했습니다. 이 릴리스에서는 이제 DES 및 RG 이름의 대문자와 소문자를 사용할 수 있습니다. (OCPBUGS#4826)

1.9.14.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.15. RHBA-2022:8627 - OpenShift Container Platform 4.11.17 버그 수정 및 보안 업데이트

출시 날짜: 2022-11-28

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.17을 사용할 수 있습니다. 이 릴리스에 대한 IBM Powerbuild가 없습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:8627 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:8626 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.17 --pullspecs
```

1.9.15.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.16. RHBA-2022:8698 - OpenShift Container Platform 4.11.18 버그 수정 업데이트

출시 날짜: 2022-12-05

OpenShift Container Platform 릴리스 4.11.18이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:8698 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:8697 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.18 --pullspecs
```

1.9.16.1. 기능 개선

- IPv6 원하지 않는 서블러 알림 및 IPv4 불필요한 주소 확인 프로토콜이 SR-IOV CNI 플러그인에서 기본값으로 설정되어 있습니다. SR-IOV(Single Root I/O Virtualization) CNI 플러그인으

로 생성된 Pod는 IP 주소 관리 CNI 플러그인이 IP를 할당하여 이제 IPv6 비호주 서블러 알림 및/또는 IPv4 비정상적인 주소 확인 프로토콜을 기본적으로 네트워크에 보냅니다. 이번 개선된 기능을 통해 특정 IP의 새 Pod MAC 주소 호스트에 올바른 정보로 ARP/NDP 캐시를 새로 고치도록 알립니다. 자세한 내용은 지원되는 장치를 참조하십시오.

1.9.16.2. 주요 기술 변경 사항

- 이전에는 이름이 다른 이기종 클러스터가 OpenShift Container Platform 설명서에서 다중 아키텍처라고 합니다. 자세한 내용은 다중 아키텍처 클러스터 구성을참조하십시오.

1.9.16.3. 버그 수정

- 이전에는 일부 오브젝트 스토리지 인스턴스가 표시되지 않는 콘텐츠가 없는 경우 204 No Content 로 응답했습니다. OpenShift Container Platform에 사용된 RHOSP(Red Hat OpenStack Platform) SDK는 204를 올바르게 처리하지 못했습니다. 이번 업데이트를 통해 나열할 항목이 없는 경우 설치 프로그램이 문제를 해결합니다. (OCPBUGS-4081)

- 이전 버전에서는 로드된 클러스터의 kube-apiserver 의 롤아웃 시간이 느리고 종종 5분 롤아웃 타임아웃을 초과했습니다. 이번 업데이트를 통해 롤아웃 시간이 짧고 5분 임계값 내에 있습니다. (OCPBUGS-3182)

1.9.16.4. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.17. RHSA-2022:8893 - OpenShift Container Platform 4.11.20 버그 수정 및 보안 업데이트

출시 날짜: 2022-12-15

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.20을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:8893 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:8892 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.20 --pullspecs
```

1.9.17.1. 버그 수정

- 이전에는 OpenShift Container Platform 설치 프로그램에서 GCP(Google Cloud Platform)에 클러스터를 설치할 때 사용자에게 불완전한 리전 목록을 제공했습니다. 이번 업데이트를 통해 설치 프로그램에 지원되는 모든 영역이 포함됩니다. (OCPBUGS-3023)

1.9.17.2. 확인된 문제

- spec.endpointPublishingStrategy.loadBalancer.scope 필드를 설정하여 기본 Ingress 컨트롤러의 라우터 범위를 전환하면 성능이 저하된 Ingress Operator가 생성됩니다. 결과적으로 웹 콘솔 URL과 같이 해당 끝점을 사용하는 경로에 액세스할 수 없게 됩니다. 이 문제를 해결하려면 라우터 pod 중 하나를 다시 시작하면 로드 밸런서의 여러 인스턴스를 inService 상태로 다시 가져옵니다. (OCPBUGS-2554)

1.9.17.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.18. RHSA-2022:9107 - OpenShift Container Platform 4.11.21 버그 수정 및 보안 업데이트

출시 날짜: 2023-01-04

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.21을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:9107 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.21 --pullspecs
```

1.9.18.1. 버그 수정

- 이전 버전에서는 RHOSP(Red Hat OpenStack Platform) 인증 정보를 순환한 후 Cinder CSI 드라이버는 번개기에서 다시 시작할 때까지 이전 인증 정보를 계속 사용했습니다. 이전 인증 정보가 더 이상 유효하지 않으면 모든 볼륨 작업이 실패합니다. 이번 업데이트를 통해 RHOSP 인증 정보가 순환되면 Cinder CSI 드라이버가 자동으로 업데이트됩니다. (OCPBUGS-4103)

- 이전에는 CoreDNS v1.7.1에서 모든 업스트림 캐시가 DNSSEC를 새로 고침했습니다. bufsize는 업스트림 쿼리를 위해 2048바이트로 하드 코딩되어 네트워킹 인프라 내에 UDP Payload 제한이 있을 때 일부 DNS 업스트림 쿼리가 중단되었습니다. 이번 업데이트를 통해

OpenShift Container Platform은 항상 업스트림 캐시 요청에 bufsize 512를 사용합니다. 이는 Corefile에 지정된 bufsize입니다. 업스트림 DNS 요청에 대해 bufsize 2048의 잘못된 기능에 의존하는 경우 고객은 영향을 받을 수 있습니다. (OCPBUGS-2901)

- 이전에는 영역이 있는 리전에서 vmSize 가 유효하지 않을 때 가용성 세트가 생성되었습니다. 그러나 가용성 세트는 영역이 없는 지역에서만 생성해야 합니다. 이번 업데이트를 통해 올바른 vmSize 가 제공되며 머신 세트에 대해 가용성 세트가 더 이상 제공되지 않습니다. (OCPBUGS-2123)

1.9.18.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.19. RHBA-2023:0027 - OpenShift Container Platform 4.11.22 버그 수정 업데이트

출시 날짜: 2023-01-09

OpenShift Container Platform 릴리스 4.11.22가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:0027 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.22 --pullspecs
```

1.9.19.1. 버그 수정

- OpenShift Container Platform 4.11 릴리스에서는 install-config.yaml 파일을 업데이트하여 이제 me-west1, (Tel Aviv, 이스라엘) 리전을 나열합니다. openshift-install 바이너리를 실행하여 OpenShift Container Platform을 설치한 후 선택한 클러스터에 대해 me-west1 리전을 선택할 수 있습니다. (OCPBUGS-4720)

- 이전에는 일부 오브젝트 스토리지 인스턴스가 콘텐츠가 표시될 때 204 No Content 오류 메시지로 응답했습니다. OpenShift Container Platform에 사용된 RHOSP(Red Hat OpenStack Platform) SDK는 204를 올바르게 처리하지 않습니다. 이번 업데이트를 통해 Swift 컨테이너에 나열할 개체가 없는 경우 설치 프로그램이 문제를 해결합니다. (OCPBUGS-5078)

- 이전 버전에서는 OpenShift Container Platform 4.11.ec4 빌드 배포가 최신 RHCOS 이미지 412.86.202210072120-0 및 rhel-86 이미지로 실패했습니다. 결과적으로 RHCOS(Red Hat

Enterprise Linux CoreOS) 노드가 부팅 중입니다. 이번 업데이트를 통해 배포가 성공적으로 완료됩니다. (OCPBUGS-2321)

1.9.19.2. 확인된 문제

- 노드에 대해 약 470개 이상의 컨테이너가 있는 4.11 이상 am 64 클러스터로 인해 다음 오류로 인해 추가 Pod 생성이 실패할 수 있습니다.

```
runc create failed: unable to start container process: unable to init seccomp: error loading seccomp filter into kernel: error loading seccomp filter: errno 524"
```

이는 작업자 노드에서 생성할 수 있는 seccomp 프로필 수의 CoreOS 제한 때문입니다. 이는 업그레이드, 작업자 노드 오류 또는 Pod 확장 중에 Pod당 여러 컨테이너가 있는 클러스터에서 발생합니다. 이는 이후 버전의 OpenShift Container Platform에서 수정될 예정입니다. (OCPBUGS-2637)

1.9.19.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.20. RHSA-2023:0069 - OpenShift Container Platform 4.11.24 버그 수정 및 보안 업데이트

출시 날짜: 2023-01-19

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.24를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:0069 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:0068 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.24 --pullspecs
```

1.9.20.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.21. RHSA-2023:0245 - OpenShift Container Platform 4.11.25 버그 수정 및 보안 업데이트

출시 날짜: 2023-01-23

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.25를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:0245 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:0244 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.25 --pullspecs
```

1.9.21.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.22. RHSA-2023:0565 - OpenShift Container Platform 4.11.26 버그 수정 및 보안 업데이트

출시 날짜: 2023-02-07

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.26을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:0565 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:0564 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.26 --pullspecs
```

1.9.22.1. 확인된 문제

- 이번 릴리스에서는 Pod에 연결된 정적 MAC 주소로 구성된 SR-IOV 보조 네트워크 인터페이스가 완전한 네트워크 연결을 제공하지 않는 기능 이 문제는 Intel Ethernet Network Adapter X710 제품(i40e/iavf Linux 커널 드라이버)을 기반으로 하는 SR-IOV 가상 기능에만 영향을 미칩니다. 자세한 내용은 OCPBUGS-5139 에서 참조하십시오.

1.9.22.2. 버그 수정

- 이전 버전에서는 **cluster-image-registry-operator** 가 **Swift**에 도달하지 못하면 **PVC**(영구 볼륨 클레임)를 사용하도록 기본 설정되었습니다. 이번 업데이트를 통해 **RHOSP**(Red Hat OpenStack Platform) **API** 또는 기타 부수적인 실패로 인해 **cluster-image-registry-operator** 가 프로브를 다시 시도합니다. 재시도하는 동안 기본값은 **RHOSP** 카탈로그가 올바르게 발견되고 오브젝트 스토리지를 포함하지 않는 경우에만 발생하거나 **RHOSP** 카탈로그가 있고 현재 사용자에게 컨테이너를 나열할 수 있는 권한이 없는 경우에만 발생합니다. (OCPBUGS-5578)

- 이전 버전에서는 **spec.provider** 에 대한 정의가 누락되어 **ClusterServiceVersion** 을 표시하려고 할 때 **Operator** 세부 정보 페이지에 실패했습니다. 이번 업데이트를 통해 **spec.provider** 없이 사용자 인터페이스가 작동하며 **Operator** 세부 정보 페이지가 실패하지 않습니다. (OCPBUGS-6689)

1.9.22.3. 업데이트

기존 **OpenShift Container Platform 4.11** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.23. RHSA-2023:0651 - OpenShift Container Platform 4.11.27 버그 수정 및 보안 업데이트

출시 날짜: **2023-02-15**

보안 업데이트가 포함된 **OpenShift Container Platform** 릴리스 **4.11.27**을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:0651 권고에 설명되어 있습니다. 업데이트에 포함된 **RPM** 패키지는 RHBA-2023:0650 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.27 --pullspecs
```

1.9.23.1. 버그 수정

- 이전에는 토폴로지 사이드바에 업데이트된 정보가 표시되지 않았습니다. 토폴로지 사이드바에서 직접 리소스를 업데이트했을 때 사이드바를 다시 열어 변경 사항을 확인해야 했습니다. 이번 수정으로 업데이트된 리소스가 올바르게 표시됩니다. (OCPBUGS-5459)

1.9.23.2. 업데이트

기존 **OpenShift Container Platform 4.11** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.24. RHSA-2023:0774 - OpenShift Container Platform 4.11.28 버그 수정 및 보안 업데이트

출시 날짜: 2023-02-21

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.28을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:0774 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:0773 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.28 --pullspecs
```

1.9.24.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.25. RHSA-2023:0895 - OpenShift Container Platform 4.11.29 버그 수정 및 보안 업데이트

출시 날짜: 2023-02-28

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.29를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:0895 권고에 설명되어 있습니다. 이 업데이트를 위한 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.29 --pullspecs
```

1.9.25.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.26. RHSA-2023:1030 - OpenShift Container Platform 4.11.30 버그 수정 및 보안 업데이트

출시 날짜: 2023-03-07

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.30을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:1030 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:1029 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.30 --pullspecs
```

1.9.26.1. 버그 수정

- 이전에는 Secret 을 생성할 때 Start Pipeline 모델에서 잘못된 JSON 값을 생성했습니다. 그 결과 시크릿 을 사용할 수 없어 PipelineRun 이 실패할 수 있었습니다. 이번 수정으로 Start Pipeline 모델에서 보안에 유효한 JSON 값을 생성합니다. 이제 파이프라인을 시작하는 동안 유효한 시크릿을 생성할 수 있습니다. (OCPBUGS-7494)

1.9.26.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.27. RHSA-2023:1158 - OpenShift Container Platform 4.11.31 버그 수정 및 보안 업데이트

출시 날짜: 2023-03-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.31을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:1158 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:1157 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.31 --pullspecs
```

1.9.27.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하

여 클러스터 업데이트를 참조하십시오.

1.9.28. RHBA-2023:1296 - OpenShift Container Platform 4.11.32 버그 수정 및 보안 업데이트

출시 날짜: 2023-03-22

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.32를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:1296 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:1295 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.32 --pullspecs
```

1.9.28.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.29. RHBA-2023:1396 - OpenShift Container Platform 4.11.33 버그 수정

출시 날짜: 2023-03-28

OpenShift Container Platform 릴리스 4.11.33이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:1396 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:1395 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.33 --pullspecs
```

1.9.29.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.30. RHSA-2023:1504 - OpenShift Container Platform 4.11.34 버그 수정 및 보안 업데이트

출시 날짜: 2023-04-04

OpenShift Container Platform 릴리스 4.11.34가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:1504 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:1503 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.34 --pullspecs
```

1.9.30.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.31. RHBA-2023:1650 - OpenShift Container Platform 4.11.35 버그 수정

출시 날짜: 2023-04-12

OpenShift Container Platform 릴리스 4.11.35가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:1650 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:1649 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.35 --pullspecs
```

1.9.31.1. 버그 수정

- 이전에는 OpenStack clouds.yaml 파일이 순환된 경우 새 클라우드 인증 정보를 가져오기 위해 machine-api-provider-openstack 을 다시 시작해야 했습니다. 그 결과 MachineSet 을 0으로 확장할 수 있습니다. 이러한 변경으로 클라우드 인증 정보는 더 이상 캐시되지 않으며 필요한 경우 machine-api-provider-openstack 이 해당 시크릿을 읽습니다. (OCPBUGS-10954)

1.9.31.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.32. RHBA-2023:1733 - OpenShift Container Platform 4.11.36 버그 수정

출시 날짜: 2023-04-13

OpenShift Container Platform 릴리스 4.11.36이 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2023:1733 권고에 설명되어 있습니다. 이 업데이트를 위한 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.36 --pullspecs
```

1.9.32.1. 업데이트

모든 OpenShift Container Platform 4.11 사용자는 이 릴리스에서 수정된 유일한 결함은 설치 시간으로 제한되므로 이전에 설치한 클러스터를 이 버전으로 업데이트할 필요가 없습니다.

1.9.33. RHBA-2023:1760 - OpenShift Container Platform 4.11.37 버그 수정

출시 날짜: 2023-04-19

OpenShift Container Platform 릴리스 4.11.37이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:1760 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:1759 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.37 --pullspecs
```

1.9.33.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.34. RHBA-2023:1863 - OpenShift Container Platform 4.11.38 버그 수정 업데이트

출시 날짜: 2023-04-26

OpenShift Container Platform 릴리스 4.11.38이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:1863 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:1862 권고에서 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.38 --pullspecs
```

1.9.34.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.35. RHSA-2023:2014 - OpenShift Container Platform 4.11.39 버그 수정 및 보안 업데이트

출시 날짜: 2023-05-02

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.39를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:2014 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:2056 권고에서 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.39 --pullspecs
```

1.9.35.1. 버그 수정

- 이전에는 Ingress Operator에서 시크릿 크기 제한 1MB로 인해 Ingress 컨트롤러 수가 많은 클러스터에 router-certs 시크릿을 게시하지 못했습니다. 결과적으로 router-certs 보안을 사용하여 클러스터 Ingress 도메인에 액세스하는 Authentication Operator에 OAuth 목적으로 사용할 최신 인증서가 없었습니다. 이번 업데이트를 통해 Ingress Operator는 클러스터 Ingress 도메인을 보유한 Ingress 컨트롤러에 대해서만 인증서와 키를 게시하므로 시크릿이 크기 제한을 초과하지 않습니다. 이번 업데이트를 통해 Authentication Operator가 OAuth 인증을 위해 최신 인증서를 읽고 사용할 수 있습니다. (OCPBUGS-8000)

1.9.35.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.36. RHBA-2023:2694 - OpenShift Container Platform 4.11.40 버그 수정 업데이트

출시 날짜: 2023-05-18

OpenShift Container Platform 릴리스 4.11.40이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:2694 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:2693 권고에서 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.40 --pullspecs
```

1.9.36.1. 버그 수정

- 이전 버전에서는 OpenShift 웹 콘솔에서 Knative(kn) 서비스를 삭제할 때 연결된 < kn-service-name>-github-webhook-secret Webhook가 삭제되지 않았습니다. 원래 서비스와 동일한 이름을 유지하면서 Knative 서비스를 다시 생성하려고 하면 작업이 실패했습니다. 이번 업데이트를 통해 OpenShift 웹 콘솔에서 Knative(kn) 서비스를 삭제하면 관련 Webhook가 서비스와 동시에 삭제됩니다. 이제 작업이 실패하지 않고 삭제된 서비스와 동일한 이름으로 Knative 서비스를 다시 생성할 수 있습니다. (OCPBUGS-7949)

1.9.36.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.37. RHBA-2023:3213 - OpenShift Container Platform 4.11.41 버그 수정 업데이트

출시 날짜: 2023-05-24

OpenShift Container Platform 릴리스 4.11.41이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:3213 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:3212 권고에서 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.41 --pullspecs
```

1.9.37.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.38. RHSA-2023:3309 - OpenShift Container Platform 4.11.42 버그 수정 및 보안 업데이트

출시 날짜: 2023-05-31

OpenShift Container Platform 릴리스 4.11.42가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:3309 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:3308 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.42 --pullspecs
```

1.9.38.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.39. RHSA-2023:3542 OpenShift Container Platform 4.11.43 버그 수정 및 보안 업데이트

출시 날짜: 2023-06-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.43을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:3542 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:3541 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.43 --pullspecs
```

1.9.39.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.40. RHSA-2023:3915 - OpenShift Container Platform 4.11.44 버그 수정 및 보안 업데이트

출시 날짜: 2023-07-06

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.44를 사용할 수 있습니다. 이번 업데이트에는 FIPS 모드에서 OpenShift Container Platform을 실행하는 고객을 위한 Red Hat 보안 공지가 포함되어 있습니다. 자세한 내용은 RHSB-2023:001 을 참조하십시오.

업데이트에 포함된 버그 수정 목록은 RHSA-2023:3915 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:3914 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.44 --pullspecs
```

1.9.40.1. 버그 수정

- 이전 버전에서는 클라이언트 TLS(mTLS)가 Ingress 컨트롤러에 구성되었으며 클라이언트 CA 번들의 CA(인증 기관)에 다운로드해야 하는 인증서 취소 목록(CRL)을 다운로드해야 하므로 ConfigMap 오브젝트의 크기 제한으로 인해 CRL ConfigMap 오브젝트를 업데이트할 수 없었습니다. CRL이 누락되어 있는 경우 알 수 없는 ca 오류와 함께 유효한 클라이언트 인증서 연결이 거부되었을 수 있었습니다. 이번 업데이트를 통해 각 수신 컨트롤러의 CRL ConfigMap 오브젝트가 더 이상 존재하지 않습니다. 대신 CRL ConfigMap 오브젝트가 각 라우터 Pod에서 직접 다운로드되어 유효한 클라이언트 인증서와 연결이 더 이상 거부되지 않습니다. (OCPBUGS-14456)

- 이전 버전에서는 클라이언트 TLS(mTLS)가 수신 컨트롤러에 구성되었기 때문에 배포 CA(인증 기관)와 발행 CA 간의 불일치로 인해 잘못된 CRL(인증서 취소 목록)이 다운로드되었습니다. 결과적으로 잘못된 CRL이 올바른 CRL 대신 다운로드되어 알 수 없는 ca 오류 메시지와 함께 유효한 클라이언트 인증서 연결이 거부됩니다. 이번 업데이트를 통해 다운로드한 CRL은 이제 이를 배포하는 CA에서 추적할 수 있습니다. 이렇게 하면 유효한 클라이언트 인증서가 더 이상 거부되지 않습니다. (OCPBUGS-14457)

1.9.40.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.41. RHSA-2023:4053 OpenShift Container Platform 4.11.45 버그 수정 및 보안 업데이트

출시 날짜: 2023-07-19

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.45를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:4053 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:4052 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.45 --pullspecs
```

1.9.41.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.42. RHSA-2023:4310 OpenShift Container Platform 4.11.46 버그 수정 및 보안 업데이트

출시 날짜: 2023-08-02

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.46을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:4310 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:4312 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.46 --pullspecs
```

1.9.42.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.43. RHBA-2023:4614 OpenShift Container Platform 4.11.47 버그 수정 업데이트

출시 날짜: 2023-08-16

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.47을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:4614 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:4616 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.47 --pullspecs
```

1.9.43.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.44. RHBA-2023:4752 OpenShift Container Platform 4.11.48 버그 수정 업데이트

출시 날짜: 2023-08-31

OpenShift Container Platform 릴리스 4.11.48이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:4752 권고에 설명되어 있습니다. 이번 업데이트에는 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.48 --pullspecs
```

1.9.44.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.45. RHSA-2023:5001 OpenShift Container Platform 4.11.49 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2023-09-13

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.49를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:5001 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:5003 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.49 --pullspecs
```

1.9.45.1. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.46. RHBA-2023:5350 OpenShift Container Platform 4.11.50 버그 수정 업데이트

출시 날짜: 2023-10-04

OpenShift Container Platform 릴리스 4.11.50이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:5350 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:5352 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.50 --pullspecs
```

1.9.46.1. 기능

1.9.46.1.1. Google Cloud Provider 클러스터에 사용자 정의 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 사용

기본적으로 설치 프로그램은 컨트롤 플레인 및 컴퓨팅 머신을 시작하는 데 사용되는 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지를 다운로드하여 설치합니다. 이번 개선된 기능을 통해 설치 구성

파일(**install-config.yaml**)을 수정하여 사용자 정의 **RHCOS** 이미지를 지정하여 기본 동작을 덮어쓸 수 있습니다. 클러스터를 배포하기 전에 다음 설치 매개변수를 수정할 수 있습니다.

- **controlPlane.platform.gcp.osImage.project**
- **controlPlane.platform.gcp.osImage.name**
- **compute.platform.gcp.osImage.project**
- **compute.platform.gcp.osImage.name**
- **platform.gcp.defaultMachinePlatform.osImage.project**
- **platform.gcp.defaultMachinePlatform.osImage.name**

이러한 매개변수에 대한 자세한 내용은 추가 **Google Cloud Platform** 구성 매개변수를 참조하십시오.

1.9.46.2. 버그 수정

- 이전에는 **Manila CSI Driver Operator**에 사용된 클라우드 인증 정보가 캐시되어 이러한 인증 정보가 순환된 경우 인증 문제가 발생했습니다. 이번 업데이트를 통해 이 문제가 해결되었습니다. (**OCPBUGS-18782**)

1.9.46.3. 업데이트

기존 **OpenShift Container Platform 4.11** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.47. RHSA-2023:5697 OpenShift Container Platform 4.11.52 버그 수정 업데이트 및 보안 업데이트

출시 날짜: **2023-10-18**

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.52를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:5697 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:5717 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.52 --pullspecs
```

1.9.47.1. 확인된 문제

Python에 대한 최신 보안 업데이트로 인해 베어 메탈 플랫폼의 호스트 프로비저닝이 실패했습니다. 이 문제가 해결될 때까지 OpenShift Container Platform 클러스터를 베어 메탈 플랫폼의 버전 4.11.52로 업그레이드하지 마십시오. 이 버전으로 업그레이드하고 문제가 해결되지 않으면 노드를 확장할 수 없습니다. (OCPBUGS-20486)

1.9.47.2. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.48. RHSA-2023:6272 OpenShift Container Platform 4.11.53 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2023-11-08

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.53을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:6272 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:6274 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.53 --pullspecs
```

1.9.48.1. 버그 수정

- 이전에는 EndpointSlice 포트가 포트 번호 없이 생성된 경우 CoreDNS 가 충돌했습니다. 이번 업데이트를 통해 CoreDNS 에 검증이 추가되어 이 상황에서 서버가 더 이상 충돌하지 않습니다. (OCPBUGS-20359)

1.9.48.2. 확인된 문제

- Python에 대한 최신 보안 업데이트로 인해 베어 메탈 플랫폼의 호스트 프로비저닝이 실패했습니다. 이 문제가 해결될 때까지 OpenShift Container Platform 클러스터를 베어 메탈 플랫폼의 버전 4.11.53으로 업그레이드하지 마십시오. 이 버전으로 업그레이드하고 문제가 해결되지 않으면 노드를 확장할 수 없습니다. (OCPBUGS-20486)

1.9.48.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.49. RHSA-2023:7479 OpenShift Container Platform 4.11.54 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2023-11-29

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.54를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:7479 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:7481 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.54 --pullspecs
```

1.9.49.1. 기능

1.9.49.1.1. 이제 Insights Operator에서 apiserver.config.openshift.io를 추적합니다.

Insights Operator를 실행한 후 이제 APIServer.config.openshift.io 의 감사 프로필에 대한 정보와 함께 경로 config/apiserver.json 의 아카이브에 새 파일을 사용할 수 있습니다.

감사 프로필에 대한 액세스는 일반적인 감사 정책, 가장 일반적으로 사용되는 프로필, 산업 간 차이점이 무엇이고, 어떤 종류의 사용자 지정이 적용되는지 이해하는 데 도움이 됩니다.

1.9.49.2. 버그 수정

- 이전에는 사용자가 컨테이너 간에 파일을 복사할 때 타임스탬프가 보존되지 않았습니다. 이번 릴리스에서는 컨테이너 간에 파일을 복사할 때 타임스탬프를 유지하기 위해 -p 플래그가 추가

됩니다. (OCPBUGS-23041)

1.9.49.3. 업데이트

기존 OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.50. RHSA-2023:7691 OpenShift Container Platform 4.11.55 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2023-12-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.55를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:7691 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:7693 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.55 --pullspecs
```

1.9.50.1. 버그 수정

- 이전에는 마스터 노드가 추가 네트워크에 연결된 경우 OpenStack 플랫폼에서 4.12로 업그레이드할 수 없었습니다. 업그레이드하는 동안 두 공급자 모두 단기간에 동시에 활성화되어 있으며 다른 노드 IP를 보고할 수 있습니다. 이 동작은 in-tree 클라우드 공급자에서 외부 클라우드 공급자로 전환할 때 알려진 경쟁 조건으로 인해 발생합니다. 이번 릴리스에서는 두 공급자 모두 동일한 기본 노드 IP를 보고하도록 하는 주석이 추가되어 노드 IP가 표시되지 않습니다. (OCPBUGS-20122)

1.9.50.2. 업데이트

OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.51. RHSA-2024:0059 OpenShift Container Platform 4.11.56 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2024-01-10

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.56을 사용할 수 있습니다. 업데

이트에 포함된 버그 수정 목록은 RHSA-2024:0059 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:0061 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.56 --pullspecs
```

1.9.51.1. 업데이트

OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.52. RHSA-2024:0306 OpenShift Container Platform 4.11.57 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2024-01-25

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.57을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:0306 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:0308 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.57 --pullspecs
```

1.9.52.1. 업데이트

OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.53. RHSA-2024:0682 OpenShift Container Platform 4.11.58 버그 수정 업데이트 및 보안 업데이트

출시 날짜: 2024-02-08

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.11.58를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:0682 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:0684 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.11.58 --pullspecs
```

1.9.53.1. 업데이트

OpenShift Container Platform 4.11 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.