OpenShift Container Platform 4.8

릴리스 노트

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항

Last Updated: 2023-04-07

OpenShift Container Platform 4.8 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 4.8 릴리스 노트

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

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

1.1. 릴리스 정보

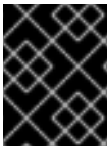
OpenShift Container Platform (RHSA-2021:2438)을 사용할 수 있습니다. 이 릴리스에서는 Kubernetes 1.21을 CRI-O 런타임과 함께 사용합니다. 이에는 OpenShift Container Platform 4.8과 관련된 새로운 기능, 변경 사항, 알려진 문제가 포함되어 있습니다.

Red Hat은 OpenShift Container Platform 4.8.0을 GA 버전으로 출시하지 않고, 대신 OpenShift Container Platform 4.8.2를 GA 버전으로 출시하고 있습니다.

OpenShift Container Platform 4.8 클러스터는 https://console.redhat.com/openshift 에서 사용할 수 있습니다. OpenShift Container Platform용 Red Hat OpenShift Cluster Manager 애플리케이션을 사용하면 온프레미스 또는 클라우드 환경에 OpenShift 클러스터를 배포할 수 있습니다.

OpenShift Container Platform 4.8은 Red Hat Enterprise Linux 7.9 이상과 RHCOS(Red Hat Enterprise Linux CoreOS) 4.8에서 지원됩니다.

컨트롤 플레인에는 RHCOS 머신을 사용해야 하며 컴퓨팅 머신에는 RHCOS 또는 Red Hat Enterprise Linux (RHEL) 7.9 이상을 사용할 수 있습니다.



중요

RHEL 7.9 이상 만 컴퓨팅 시스템에서 지원되므로 RHEL 컴퓨팅 시스템을 RHEL 8으로 업그레이드할 수 없습니다.

OpenShift Container Platform 4.8은 EUS (Extended Update Support) 릴리스입니다. Red Hat OpenShift EUS에 대한 자세한 내용은 OpenShift 라이프사이클 및 OpenShift EUS 개요에서 확인할 수 있습니다.

OpenShift Container Platform 4.8 버전이 릴리스되면서 4.5 버전의 지원이 종료되었습니다. 자세한 내용은 Red Hat OpenShift Container Platform 라이프 사이클 정책 을 참조하십시오.

1.2. 보다 포괄적인 오픈 소스 구현

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 교체하기 위해 최선을 다하고 있습니다.

이러한 노력의 일환으로 이번 릴리스에서는 다음과 같은 변경 사항이 적용되었습니다.

- OpenShift Docs GitHub 리포지토리 **master**의 이름이 **main**으로 변경되었습니다.
- "마스터"라는 용어를 "컨트롤 플레인"으로 점진적으로 대체하기 시작했습니다. 문서 전체에서 괄호 안에 "마스터"라고 기재하여 두 용어를 모두 사용합니다. 예: "... 컨트롤 플레인 노드(마스터 노드라고도 함)". 향후 릴리스에서는 이를 "컨트롤 플레인 노드"로 업데이트할 예정입니다.

1.3. 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.

1.4. 새로운 기능 및 개선 사항

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

1.4.1. RHCOS(Red Hat Enterprise Linux CoreOS)

1.4.1.1. RHCOS에서 RHEL 8.4 사용

RHCOS는 OpenShift Container Platform 4.8과 OpenShift Container Platform 4.7.24 이상에서 RHEL (Red Hat Enterprise Linux) 8.4 패키지를 사용합니다. 이를 통해 최신 수정 사항, 기능 및 향상된 기능은 물론 최신 하드웨어 지원 및 드라이버 업데이트를 받을 수 있습니다. OpenShift Container Platform 4.6은 전체 라이프사이클 동안 RHEL 8.2 EUS 패키지를 계속 사용하는 EUS (Extended Update Support) 릴리스입니다.

1.4.1.2. 부팅 이미지 자동화를 위해 스트림 메타데이터 사용

스트림 메타데이터는 OpenShift Container Platform을 설치하는 동안 클러스터에 메타데이터를 삽입하기 위한 표준화된 JSON 형식을 제공합니다. 자동화 기능 향상을 위해 새로운 **openshift-install coreos print-stream-json** 명령은 스크립팅 가능한 머신에서 읽을 수 있는 형식으로 스트림 메타데이터를 출력하는 방법을 제공합니다.

사용자 프로비저닝 설치의 경우 **openshift-install** 바이너리에는 AWS AMI와 같은 OpenShift Container Platform과 함께 사용하기 위해 테스트된 RHCOS 부팅 이미지에 대한 참조가 포함되어 있습니다. 이제 https://github.com/coreos/stream-metadata-go에서 공식 **stream-metadata-go** 라이브러리를 사용하여 Go 프로그램에서 스트림 메타데이터를 구문 분석할 수 있습니다.

자세한 내용은 스트림 메타데이터로 RHCOS AMI 액세스를 참조하십시오.

1.4.1.3. Butane config Transpiler를 통한 머신 구성 생성 간소화

OpenShift Container Platform에는 머신 구성을 생성하고 검증할 수 있도록 Butane config Transpiler가 포함되어 있습니다. 이제 Butane을 사용하여 LUKS 디스크 암호화, 부팅 디스크 미러링 및 사용자 지정 커널 모듈에 대한 머신 구성을 생성하는 것이 좋습니다.

자세한 내용은 Butane 을 사용하여 머신 구성 생성 을 참조하십시오.

1.4.1.4. 클라우드 플랫폼에서 사용자 지정 chrony.conf 기본값으로 변경

클라우드 관리자가 이미 사용자 지정 **/etc/chrony.conf** 구성을 설정한 경우 RHCOS는 더 이상 클라우드 플랫폼에서 기본값으로 **PEERNTP=no** 옵션을 설정하지 않습니다. 그렇지 않으면 **PEERNTP=no** 옵션이 기본값으로 계속 설정됩니다. 자세한 내용은 BZ#1924869에서 참조하십시오.

1.4.1.5. 베어 메탈 설치 시 다중 경로 활성화

베어 메탈 설치 중에 다중 경로를 활성화하는 것은 OpenShift Container Platform 4.8 이상에서 프로비저

닝된 노드에 지원됩니다. 설치된 시스템 자체에서 첫 번째 부팅부터 다중 경로를 사용하도록 커널 인수를 **coreos-installer install** 명령에 추가하여 다중 경로를 활성화할 수 있습니다. 시스템 구성을 통해 다중 경로를 활성화하면 설치 후 지원을 계속 사용할 수 있지만 OpenShift Container Platform 4.8부터 프로비저닝된 노드에는 설치 후 다중 경로를 활성화하는 것이 좋습니다.

자세한 내용은 RHCOS에서 커널 인수로 멀티패스 활성화 를 참조하십시오.

1.4.2. 설치 및 업그레이드

1.4.2.1. Azure의 빈 기존 리소스 그룹에 클러스터 설치

install-config.yaml 파일에서 **platform.azure.resourceGroupName** 필드를 정의하여 Azure에 클러스터를 설치할 기존 리소스 그룹을 정의할 수 있습니다. 이 리소스 그룹은 비어 있어야 하며 단일 클러스터에만 사용해야 합니다. 클러스터 구성 요소는 리소스 그룹의 모든 리소스에 대한 소유권을 가정합니다.

설치 프로그램의 서비스 주체 범위를 이 리소스 그룹으로 제한하는 경우 해당 환경에서 설치 프로그램에서 사용하는 기타 모든 리소스에 퍼블릭 DNS 영역 및 가상 네트워크와 같은 필수 권한이 있는지 확인해야 합니다. 설치 프로그램을 사용하여 클러스터를 삭제하면 사용자 지정 리소스 그룹이 삭제됩니다.

1.4.2.2. AWS에서 클러스터에 기존 IAM 역할 사용

install-config.yaml 파일에서 **compute.platform.aws.iamRole** 및 **controlPlane.platform.aws.iamRole** 필드를 설정하여 머신 인스턴스 프로파일에 기존 Amazon Web Services (AWS) IAM 역할을 정의할 수 있습니다. 이렇게 하면 IAM 역할에 대해 다음을 수행할 수 있습니다.

- 이름 지정 체계 일치
- 사전 정의된 사용 권한 경계 포함

1.4.2.3. AWS에서 기존 Route53 개인 호스트 영역 사용

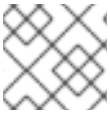
install-config.yaml 파일에서 **platform.aws.hostedZone** 필드를 설정하여 클러스터의 기존 Route 53 개인 호스트 영역을 정의할 수 있습니다. 자체 VPC를 제공하는 경우에만 기존 호스팅 영역을 사용할 수 있습니다.

1.4.2.4. 머신 CIDR 내에서 GCP 서브넷의 크기 늘리기

GCP(Google Cloud Platform)용 OpenShift Container Platform 설치 프로그램은 이제 머신 CIDR 내에서 최대한 큰 서브넷을 생성합니다. 이를 통해 클러스터는 적절한 크기의 머신 CIDR을 사용하여 클러스터의 노드 수를 수용할 수 있습니다.

1.4.2.5. 업그레이드 기간 개선

이번 릴리스에서는 모든 노드에 데몬 세트를 배포하는 클러스터 Operator의 업그레이드 기간이 크게 단축되었습니다. 예를 들어 250-노드 테스트 클러스터의 업그레이드 시간은 7.5시간에서 1.5시간으로 줄어들어 추가 노드당 1분 미만으로 업그레이드 시간이 단축되었습니다.



참고

이 변경 사항은 머신 구성 풀 롤아웃 시간에는 영향을 미치지 않습니다.

1.4.2.6. MCO는 업데이트를 보고하기 전에 모든 머신 구성 풀이 업데이트될 때까지 대기합니다.

업데이트 할 때 머신 구성 풀이 업데이트를 완료하지 않은 경우 MCO(Machine Config Operator)에서

Upgradeable=False 상태를 머신 구성 클러스터 Operator에 보고합니다. 이 상태는 향후 마이너 업데이트를 차단하지만 향후 패치 업데이트 또는 현재 업데이트를 차단하지 않습니다. 이전에는 작업자 풀이 업데이트를 수행하지 않은 경우에도 컨트롤 플레인 머신 구성 풀의 상태에 따라 MCO에서 **Upgradeable** 상태를 보고했습니다.

1.4.2.7. 베어 메탈 노드에 설치할 때 Fujitsu iRMC 사용

OpenShift Container Platform 4.8에서는 베어 메탈에 설치 관리자 프로비저닝 클러스터를 배포할 때 Fujitsu 하드웨어 및 Fujitsu iRMC 기본 보드 관리 컨트롤러 프로토콜을 사용할 수 있습니다. 현재 Fujitsu는 베어 메탈에 설치 관리자 프로비저닝 설치를 위해 iRMC S5 펌웨어 버전 **3.05P** 이상을 지원합니다. OpenShift Container Platform 4.8의 개선 사항 및 버그 수정 사항은 다음과 같습니다.

- iRMC 하드웨어에서 소프트 전원 끄기를 지원.
- 설치 프로그램이 베어 메탈 노드에 컨트롤 플레인을 배포하면 프로비저닝 서비스를 중지. 자세한 내용은 BZ#1949859에서 참조하십시오.
- 부트스트랩 **keepalived** 확인에 Ironic 상태 점검 추가. 자세한 내용은 BZ#1949859에서 참조하십시오.
- 컨트롤 플레인 노드에 유니캐스트 피어 목록이 비어 있지 않은지 확인. 자세한 내용은 BZ#1957708에서 참조하십시오.
- iRMC PowerInterface에 맞게 Bare Metal Operator가 업데이트됨. 자세한 내용은 BZ#1957869에서 참조하십시오.
- **pyghmi** 라이브러리 버전이 업데이트됨. 자세한 내용은 BZ#1920294에서 참조하십시오.
- 베어 메탈 Operator를 업데이트하여 누락된 IPMI 인증 정보 처리. 자세한 내용은 BZ#1965182에서 참조하십시오.
- **enabled_bios_interfaces**에서 iRMC 제거. 자세한 내용은 BZ#1969212에서 참조하십시오.
- 베어 메탈 pod 정의에 **ironicTlsMount** 및 **inspectorTlsMount** 추가. 자세한 내용은 BZ#1968701에서 참조하십시오.
- iRMC 서버의 RAID 기능 비활성화. 자세한 내용은 BZ#1969487에서 참조하십시오.
- 모든 드라이버에 대해 RAID 비활성화. 자세한 내용은 BZ#1969487에서 참조하십시오.

1.4.2.8. RHOSP에서 설치 관리자 프로비저닝 인프라를 사용하는 클러스터의 SR-IOV 네트워크 지원

이제 컴퓨팅 머신에 SR-IOV(Single-root I/O Virtualization) 네트워크를 사용하는 RHOSP에 클러스터를 배포할 수 있습니다.

자세한 내용은 SR-IOV 연결 컴퓨팅 머신을 지원하는 OpenStack에 클러스터 설치 를 참조하십시오.

1.4.2.9. VLAN 인터페이스에 대한 Ironic Python Agent 지원

이번 업데이트를 통해 Ironic Python Agent에서 세부 검사 중 인터페이스 목록에 VLAN 인터페이스를 보고합니다. 또한 IP 주소는 인터페이스에 포함되어 CSR을 올바르게 생성할 수 있습니다. 결과적으로 VLAN 인터페이스를 포함한 모든 인터페이스에 대해 CSR을 가져올 수 있습니다. 자세한 내용은 BZ#1888712을 참조하십시오.

1.4.2.10. OpenShift 업데이트 서비스를 통한 무선 업데이트

OSUS(OpenShift Update Service)는 Red Hat Enterprise Linux CoreOS(RHCOS)를 비롯한 OpenShift Container Platform에 대한 무선(OTA; Over-the-Air) 업데이트를 제공합니다. 이전에는 공용 API 뒤에 있는 Red Hat 호스팅 서비스로만 액세스할 수 있었지만 이제 로컬로 설치할 수 있습니다. OpenShift Update Service는 Operator 및 하나 이상의 애플리케이션 인스턴스로 구성되며 이제 OpenShift Container Platform 4.6 이상에서 일반적으로 사용할 수 있습니다.

자세한 내용은 OpenShift 업데이트 서비스 이해 를 참조하십시오.

1.4.3. 웹 콘솔

1.4.3.1. 사용자 지정 콘솔 경로에서 새로운 CustomDomains 클러스터 API 사용

console 및 **downloads**의 경우 새 **ingress** 구성 경로 구성 API **spec.componentRoutes**를 사용하도록 사용자 정의 경로 기능이 구현되었습니다. Console Operator 구성에 사용자 지정 경로 사용자 정의가 이미 포함되어 있지만 **console** 경로의 경우에만 사용됩니다. **console-operator** 구성을 통한 경로 구성은 더 이상 사용되지 않습니다. 따라서 **console** 사용자 정의 경로가 **ingress** 구성 및 **console-operator** 구성에 모두 설정된 경우 새 **ingress** 구성 사용자 정의 경로 구성이 우선합니다.

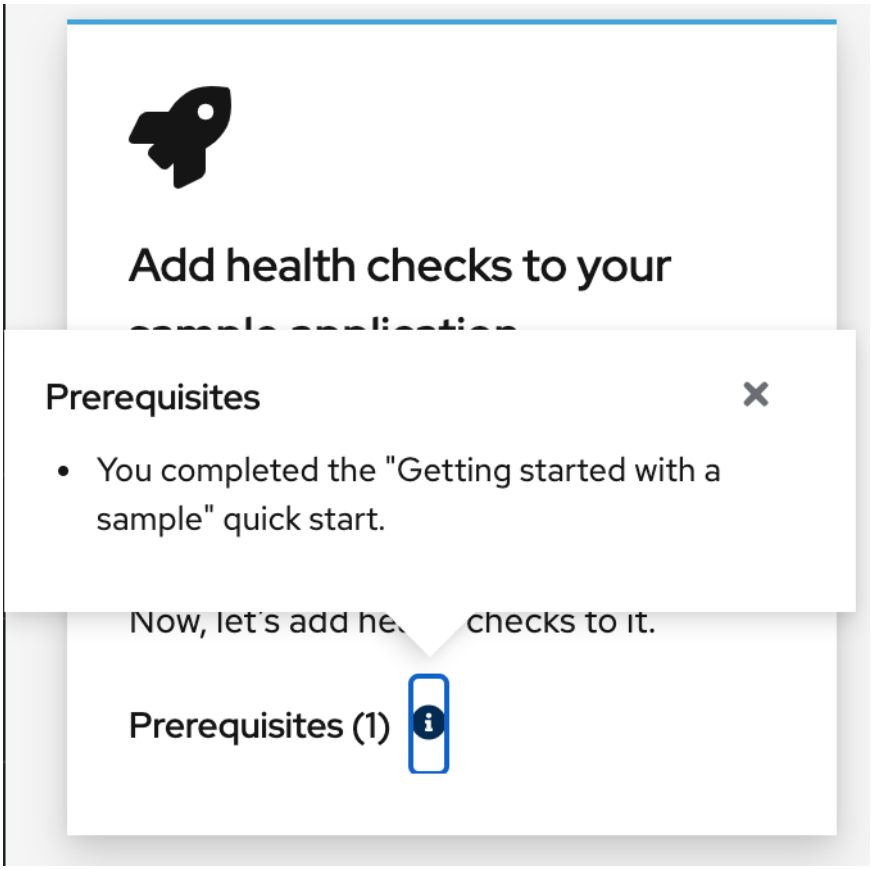
자세한 내용은 콘솔 경로 사용자 지정 을 참조하십시오.

1.4.3.2. 빠른 시작에서 코드 조각에 액세스

웹 콘솔에서 빠른 시작에 포함된 CLI 코드 조각을 실행할 수 있습니다. 이 기능을 사용하려면 Web Terminal Operator를 설치해야 합니다. Web Terminal Operator를 설치하지 않는 경우 웹 터미널에서 실행되는 웹 터미널 및 코드 조각 작업이 표시되지 않습니다. 또는 Web Terminal Operator가 설치되어 있는지 여부에 관계없이 코드 조각을 클립보드에 복사할 수 있습니다.

1.4.3.3. 빠른 시작 사전 요구 사항의 표시 개선

이전 버전에서는 빠른 시작 사전 요구 사항이 빠른 시작 카드의 목록 대신 결합된 텍스트로 표시되었습니다. 확장성을 염두에 두고 이제 사전 요구 사항이 카드가 아닌 팝업 메뉴에 표시됩니다.



1.4.3.4. 개발자 화면

이번 릴리스에서는 다음을 수행할 수 있습니다.

- 사용자 지정 파이프라인 템플릿을 사용하여 Git 리포지토리에서 애플리케이션을 생성하고 배포합니다. 이러한 템플릿은 OpenShift Pipelines 1.5 이상에서 제공하는 기본 파이프라인 템플릿을 재정의합니다.
- 인증 수준에 따라 Helm 차트를 필터링하고 **개발자 카탈로그** 의 모든 Helm 차트를 확인합니다.
- **Add(추가)** 페이지의 옵션을 사용하여 애플리케이션 및 관련 서비스를 생성하고 이러한 애플리케이션과 서비스를 OpenShift Container Platform에 배포합니다. **Add** page 옵션은 다음과 같습니다. **시작하기 리소스** 가져오기,**샘플을 사용하여 애플리케이션 생성**,**안내 문서로 빌드** 및 **새 개발자 기능 살펴보기**.
- 파이프라인 빌더에서 파이프라인을 생성할 때 작업 공간을 사용합니다. 작업을 사용하여 파이프라인의 작업 공간을 지원할 수 있도록 파이프라인에 트리거를 추가할 수도 있습니다.
- **개발자** 화면의 **토폴로지** 보기에서 JAR 파일을 사용하여 Java 애플리케이션을 배포합니다.
- OpenShift Container Platform에서 여러 이벤트 소스 유형을 생성하고 이러한 소스 유형을 싱크에 연결합니다. OpenShift Container Platform 클러스터에서 Knative 서비스로 배포된 기능을 가져와 싱크에 연결할 수 있습니다.
- 파이프라인의 **finally** 작업을 사용하여 명령을 병렬로 실행합니다.
- **Add Task(작업 추가)** 양식의 코드 지원을 사용하여 작업 매개변수 값에 액세스합니다. 파이프라인 매개변수와 해당 특정 파이프라인 매개변수를 참조하기 위한 올바른 구문을 보려면 해당 텍스트 필드로 이동합니다.

- 특정 조건이 충족된 후에만 **작업을** 실행합니다. **when** 필드를 사용하여 작업 실행을 구성하고 **when** 표현식에 대한 일련의 참조를 나열합니다.

1.4.4. IBM Z 및 LinuxONE

이번 릴리스에서 IBM Z 및 LinuxONE은 OpenShift Container Platform 4.8과 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 4.8을 사용하는 IBM Z 및 LinuxONE에서 지원되는 새로운 기능은 다음과 같습니다.

- RHEL 8.3 이상의 KVM은 IBM Z 및 Linux ONE에 OpenShift Container Platform 4.8을 사용자 프로비저닝 설치용 하이퍼바이저로 지원됩니다. 정적 IP 주소를 사용한 설치와 제한된 네트워크에서의 설치도 지원됩니다.
- etcd에 저장된 데이터 암호화
- 4K FCP 블록 장치
- 3-노드 클러스터 지원

지원되는 기능
다음 기능은 IBM Z 및 LinuxONE에서도 지원됩니다.

- 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
- OpenShift Container Platform 4.8 초기 설치가 포함된 OVN-Kubernetes
- SCSI 디스크의 z/VM Emulated FBA 장치

다음 기능은 4.8용 IBM Z의 OpenShift Container Platform에서만 사용할 수 있습니다.

- FICON의 ECKD 스토리지에 연결된 가상 머신에 대해 IBM Z/LinuxONE에서 HyperPAV 사용 가능

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

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

1.4.5. IBM Power Systems

이 릴리스에서 IBM Power Systems는 이제 OpenShift Container Platform 4.8과 호환됩니다. 설치 지침은 다음 설명서를 참조하십시오.

- IBM Power Systems에 클러스터 설치
- 네트워크가 제한된 환경에서 IBM Power System에 클러스터 설치

주요 개선 사항
OpenShift Container Platform 4.8을 사용하는 IBM Power Systems에서 다음과 같은 새로운 기능이 지원됩니다.

- etcd에 저장된 데이터 암호화
- 3-노드 클러스터 지원
- Multus SR-IOV

지원되는 기능
다음 기능은 IBM Power Systems에서도 지원됩니다.

- 현재 Operator 5개가 지원됩니다.
  - Cluster-Logging-Operator
  - Cluster-NFD-Operator
  - Elastic Search-Operator
  - Local Storage Operator
  - SR-IOV 네트워크 Operator
- 다중 경로
- iSCSI를 사용하는 영구 스토리지
- 로컬 볼륨을 사용하는 영구저장장치(Local Storage Operator)
- hostPath를 사용하는 영구 스토리지
- 파이버 채널을 사용하는 영구 스토리지
- Raw Block을 사용하는 영구 스토리지
- OpenShift Container Platform 4.8 초기 설치가 포함된 OVN-Kubernetes
- 4K 디스크 지원
- NVMe

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

- IBM Power Systems 용 OpenShift Container Platform에는 다음의 기술 프리뷰 기능이 포함되어 있지 않습니다.
  - PTP(Precision Time Protocol) 하드웨어
- 다음 OpenShift Container Platform 기능은 지원되지 않습니다 :
  - 시스템 상태 점검으로 손상된 시스템 자동 복구
  - CRC(CodeReady Containers)
  - 노드에서 오버 커밋 제어 및 컨테이너 밀도 관리
  - FIPS 암호화
  - Helm CLI(명령행 인터페이스) 도구
  - OpenShift Metering
  - OpenShift Virtualization
  - OpenShift Container Platform 배포 시 Tang 모드 디스크 암호화

- 작업자 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행해야 합니다.
- 영구 스토리지는 로컬 볼륨, NFS(Network File System), 또는 CSI(Container Storage Interface)를 사용하는 Filesystem 유형이어야 합니다.

1.4.6. 보안 및 컴플라이언스

1.4.6.1. OAuth 액세스 토큰 로그아웃 요청에 대한 감사 로깅

Default 감사 로그 정책에서는 OAuth 액세스 토큰 생성(로그인) 및 삭제(로그아웃) 요청에 대한 요청 본문을 기록합니다. 이전에는 삭제 요청 본문이 기록되지 않았습니다.

감사 로그 정책에 대한 자세한 내용은 노드 감사 로그 정책 구성 을 참조하십시오.

1.4.6.2. 헤드리스 서비스에 대한 서비스 제공 인증서의 와일드카드 제목

이제 헤드리스 서비스에 대한 서비스 제공 인증서를 생성하면 ***.<service.name>.<service.namespace>.svc** 형식으로 와일드카드 제목이 포함됩니다. 이렇게 하면 이러한 Pod에 대한 인증서를 수동으로 생성할 필요 없이 개별 상태 저장 세트 Pod에 TLS 보안 연결을 수행할 수 있습니다.

중요

생성된 인증서에는 헤드리스 서비스에 대한 와일드카드 제목이 포함되어 있으므로 클라이언트가 개별 Pod를 구분해야 하는 경우 서비스 CA를 사용하지 마십시오. 이 경우 다음을 수행합니다.

- 다른 CA를 사용하여 개별 TLS 인증서를 생성합니다.
- 개별 Pod로 전달되며 다른 Pod로 가장해서는 안 되는 연결에 대해 서비스 CA를 신뢰할 수 있는 CA로 수락하지 마십시오. 이러한 연결은 개별 TLS 인증서를 생성하는 데 사용된 CA를 신뢰하도록 구성해야 합니다.

자세한 내용은 서비스 인증서 추가 를 참조하십시오.

1.4.6.3. oc-compliance 플러그인 사용 가능

Compliance Operator는 OpenShift Container Platform 클러스터에 대한 많은 검사 및 업데이트 적용을 자동화합니다. 그러나 클러스터를 규정 준수 상태로 전환하려면 관리자가 Compliance Operator API 및 기타 구성 요소와 상호 작용해야 하는 경우가 많습니다. **oc-compliance** 플러그인을 사용할 수 있으며 프로세스를 더 쉽게 수행할 수 있습니다.

자세한 내용은 **oc-compliance** 플러그인 사용을 참조하십시오.

1.4.6.4. Kubernetes 컨트롤 플레인의 TLS 보안 프로파일

이제 Kubernetes API 서버 TLS 보안 프로파일 설정도 Kubernetes 스케줄러 및 Kubernetes 컨트롤러 관리자에서 지원됩니다.

자세한 내용은 TLS 보안 프로파일 설정 을 참조하십시오.

1.4.6.5. 서버로 사용되는 kubelet의 TLS 보안 프로파일

이제 Kubernetes API 서버의 HTTP 서버로 작동할 때 kubelet에 대한 TLS 보안 프로필을 설정할 수 있습니다.

자세한 내용은 TLS 보안 프로파일 설정 을 참조하십시오.

1.4.6.6. bcrypt 암호 해시 지원

이전에는 **oauth-proxy 명령에서** 인증에 사용되는 **htpasswd** 파일에서 SHA-1 해시 암호만 사용할 수 있었습니다. **oauth-proxy** 에는 **bcrypt** 암호 해시를 사용하는 **htpasswd** 항목이 지원됩니다. 자세한 내용은 BZ#1874322를 참조하십시오.

1.4.6.7. 설치 관리자 프로비저닝 클러스터를 사용하여 관리되는 Secure Boot 활성화

OpenShift Container Platform 4.8에서는 프로비저닝된 컨트롤 플레인 및 작업자 노드의 UEFI Secure Boot 모드를 자동으로 활성화하고 노드를 제거할 때 해제하는 기능을 지원합니다. 이 기능을 사용하려면 **install-config.yaml** 파일에서 노드의 **bootMode** 구성 설정을 **UEFISecureBoot**로 설정합니다. Red Hat은 펌웨어 버전 **2.75.75.75** 이상을 실행하는 10세대 HPE 하드웨어 또는 13세대 Dell 하드웨어에 대한 관리형 Secure Boot를 사용하는 설치 관리자 프로비저닝 설치를 지원합니다. 자세한 내용은 install-config.yaml 파일에서 관리형 Secure Boot 구성에서 참조하십시오.

1.4.7. 네트워킹

1.4.7.1. OVN-Kubernetes 클러스터 네트워크 공급자를 사용하여 설치 관리자가 프로비저닝한 베어 메탈 인프라에서 듀얼 스택 지원

베어 메탈 인프라에 설치된 클러스터에서 OVN-Kubernetes 클러스터 네트워크 공급자는 IPv4 및 IPv6 주소 제품군을 모두 지원합니다.

이전 버전의 OpenShift Container Platform에서 업그레이드하는 설치 관리자 프로비저닝 베어 메탈 클러스터의 경우 듀얼 스택 네트워킹을 지원하도록 클러스터를 변환해야 합니다. 자세한 내용은 IPv4/IPv6 듀얼 스택 네트워킹으로 변환을 참조하십시오.

1.4.7.2. 사용자 프로비저닝 인프라에서 OpenShift SDN에서 OVN-Kubernetes로 마이그레이션

사용자 프로비저닝 클러스터에 대해 OpenShift SDN 클러스터 네트워크 공급자를 OVN-Kubernetes 클러스터 네트워크 공급자로의 마이그레이션이 지원됩니다. 자세한 내용은 OpenShift SDN 클러스터 네트워크 공급자에서 마이그이션을 참조하십시오.

1.4.7.3. 노드 간에 OpenShift SDN 클러스터 네트워크 공급자 송신 IP 기능의 균형 조정

OpenShift SDN의 송신 IP 기능은 해당 네임스페이스에 여러 송신 IP 주소가 할당된 경우 지정된 네임스페이스의 노드 간에 네트워크 트래픽을 균등하게 조정합니다. 각 IP 주소는 다른 노드에 있어야 합니다. 자세한 내용은 OpenShift SDN에 대한 프로젝트의 송신 IP 구성 을 참조하십시오.

1.4.7.4. 네트워크 정책에서는 호스트 네트워크 Ingress 컨트롤러 선택 지원

OpenShift SDN 또는 OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 경우 Ingress 컨트롤러가 클러스터 네트워크 또는 호스트 네트워크에서 실행되는지 여부와 관계없이 네트워크 정책 규칙의 Ingress 컨트롤러에서 트래픽을 선택할 수 있습니다. 네트워크 정책 규칙에서 **policy-group.network.openshift.io/ingress: ""** 네임스페이스 선택기 레이블은 Ingress 컨트롤러의 트래픽과 일치합니다. **network.openshift.io/policy-group: ingress** 네임스페이스 선택기 레이블을 계속 사용할 수 있지만, 이는 향후 OpenShift Container Platform 릴리스에서 제거할 수 있는 레거시 레이블입니다.

OpenShift Container Platform의 이전 릴리스에서는 다음과 같은 제한 사항이 있었습니다.

- OpenShift SDN 클러스터 네트워크 공급자를 사용하는 클러스터는 **network.openshift.io/policy-group: ingress** 레이블을 **default** 네임스페이스에 적용하여 호스트 네트워크의 Ingress 컨트롤러에서 트래픽을 선택할 수 있었습니다.
- OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 클러스터는 호스트 네트워크의 Ingress 컨트롤러에서 트래픽을 선택할 수 없습니다.

자세한 내용은 네트워크 정책 정보를 참조하십시오.

1.4.7.5. 네트워크 정책에서 호스트 네트워크 트래픽 선택 지원

OVN-Kubernetes 클러스터 네트워크 공급자 또는 OpenShift SDN 클러스터 네트워크 공급자를 사용하는 경우 **policy-group.network.openshift.io/host-network: ""** 네임스페이스 선택기를 사용하여 네트워크 정책 규칙에서 호스트 네트워크 트래픽을 선택할 수 있습니다.

1.4.7.6. 네트워크 정책 감사 로그

OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 경우 네임스페이스에서 네트워크 정책에 대한 감사 로깅을 활성화할 수 있습니다. 로그는 syslog 호환 형식이며 로컬에 저장되거나 UDP 연결을 통해 전송되거나 UNIX 도메인 소켓으로 전송할 수 있습니다. 허용된 연결, 드롭된 연결 또는 두 연결을 모두 기록할지 여부를 지정할 수 있습니다. 자세한 내용은 네트워크 정책 이벤트 로깅 을 참조하십시오.

1.4.7.7. macvlan 추가 네트워크에 대한 네트워크 정책 지원

NetworkPolicy API를 구현하는 **MultiNetworkPolicy** API를 사용하여 macvlan 추가 네트워크에 적용되는 네트워크 정책을 생성할 수 있습니다. 자세한 내용은 다중 네트워크 정책 구성 을 참조하십시오.

1.4.7.8. SR-IOV에서 지원되는 하드웨어

OpenShift Container Platform 4.8에서는 추가 Intel 및 Mellanox 네트워크 인터페이스 컨트롤러를 지원합니다.

- Intel X710, XL710, and E810
- Mellanox ConnectX-5 Ex

자세한 내용은 지원되는 장치를 참조하십시오.

1.4.7.9. SR-IOV Network Operator 기능 개선

Operator와 함께 배포된 Network Resources Injector는 Downward API를 사용하여 대규모 페이지 요청 및 제한에 대한 정보를 노출하도록 기능이 개선되었습니다. Pod 사양에 대규모 페이지 요청 또는 제한이 포함되어 있으면 **/etc/podnetinfo** 경로에 정보가 노출됩니다.

자세한 내용은 Downward API 에 대한 대규모 페이지 리소스 주입 을 참조하십시오.

1.4.7.10. 네트워크 흐름 추적

OpenShift Container Platform 4.8에는 pod 네트워크의 네트워크 흐름에 대한 메타데이터를 네트워크 흐름 수집기로 보내는 기능이 추가되어 있습니다. 지원되는 프로토콜은 다음과 같습니다.

- NetFlow
- sFlow

- IPFIX

패킷 데이터는 네트워크 흐름 수집기로 전송되지 않습니다. 프로토콜, 소스 주소, 대상 주소, 포트 번호, 바이트 수, 기타 패킷 수준 정보 등의 패킷 수준 메타데이터가 네트워크 흐름 수집기로 전송됩니다.

자세한 내용은 네트워크 흐름 추적을 참조하십시오.

1.4.7.11. 노드 이름을 IP 주소로 확인하는데 더 이상 CoreDNS-mDNS가 사용되지 않음

OpenShift Container Platform 4.8 이상 릴리스에는 클러스터 멤버십 정보를 사용하여 A/AAAA 레코드를 생성하는 기능이 포함되어 있습니다. 이렇게 하면 노드 이름이 해당 IP 주소로 확인됩니다. 노드가 API에 등록되면 클러스터는 CoreDNS-mDNS를 사용하지 않고 노드 정보를 분산할 수 있습니다. 그러면 멀티캐스트 DNS와 연결된 네트워크 트래픽이 제거됩니다.

1.4.7.12. OpenShift Container Platform 4.8로 업그레이드를 지원하기 위해 HTTP 헤더 이름 변환

OpenShift Container Platform은 HAProxy 2.2로 업데이트되어 HTTP 헤더 이름을 **Host:xyz.com**에서 **host: xyz.com**과 같이 기본값으로 소문자로 변경합니다. 기존 애플리케이션이 HTTP 헤더 이름의 대문자에 민감한 경우 Ingress Controller **spec.httpHeaders.headerNameCaseAdjustments** API 필드를 사용하여 기존 애플리케이션을 수정할 때 까지 지원합니다. HAProxy 2.2를 사용 가능하면 OpenShift Container Platform을 업그레이드하기 전에 **spec.httpHeaders.headerNameCaseAdjustments**를 사용하여 필요한 구성을 추가하십시오.

자세한 내용은 HTTP 헤더 대/소문자 변환을 참조하십시오.

1.4.7.13. OpenShift Container Platform 4.8에서 더 엄격한 HTTP 헤더 검증

OpenShift Container Platform이 HAProxy 2.2로 업데이트되어 HTTP 헤더에 대한 몇 가지 추가 제한이 적용됩니다. 이러한 제한 사항은 애플리케이션에서 발생할 수 있는 보안 약점을 완화하기 위한 것입니다. 특히 HTTP 요청 줄에서 호스트 이름을 지정하는 HTTP 클라이언트 요청은 요청 행과 요청의 HTTP **호스트** 헤더가 모두 지정되거나 포트 번호를 생략하지 않는 경우 거부됩니다. 예를 들어 헤더 **host: hostname** 을 사용하는 요청 **GET http://hostname:80/path** 는 **호스트** 헤더가 아닌 동안 요청 행이 포트 번호를 지정하므로 HTTP 400 "Bad 요청" 응답을 사용하여 거부됩니다. 이 제한의 목적은 요청 smuggling 공격을 완화하기 위한 것입니다.

HTTP/2가 활성화된 경우 이전 버전의 OpenShift Container Platform에서 이 엄격한 HTTP 헤더 검증이 활성화되었습니다. 즉, OpenShift Container Platform 4.7 클러스터에서 HTTP/2를 활성화하고 HTTP 400 오류를 확인하여 문제가 있는 클라이언트 요청을 테스트할 수 있습니다. HTTP/2를 활성화하는 방법에 대한 자세한 내용은 HTTP/2 Ingress 연결 활성화를 참조하십시오.

1.4.7.14. GCP에서 Ingress 컨트롤러에 대한 글로벌 액세스 구성

OpenShift Container Platform 4.8에서는 내부 로드 밸런서를 사용하여 GCP에서 생성된 Ingress 컨트롤러에 대한 글로벌 액세스 옵션을 추가로 지원합니다. 글로벌 액세스 옵션을 활성화하면 로드 밸런서와 동일한 VPC 네트워크 및 컴퓨팅 리전 내의 모든 리전의 클라이언트가 클러스터에서 실행되는 워크로드에 도달할 수 있습니다.

자세한 내용은 GCP에서 Ingress 컨트롤러에 대한 글로벌 액세스 구성 을 참조하십시오.

1.4.7.15. Ingress 컨트롤러 스레드 수 설정

OpenShift Container Platform 4.8에서는 클러스터에서 처리할 수 있는 들어오는 연결의 양을 늘리기 위해 스레드 수를 설정하는 기능을 추가 지원합니다.

자세한 내용은 Ingress 컨트롤러 스레드 수 설정 을 참조하십시오.

1.4.7.16. Ingress 컨트롤러에 대한 PROXY 프로토콜 구성

OpenShift Container Platform 4.8에서는 특히 **HostNetwork** 또는 **NodePortService** 엔드포인트 게시 전략 유형의 경우 클라우드가 아닌 플랫폼의 Ingress 컨트롤러에 대한 PROXY 프로토콜을 구성할 수 있도록 지원합니다.

자세한 내용은 Ingress 컨트롤러의 PROXY 프로토콜 구성 을 참조하십시오.

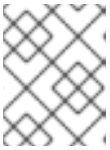
1.4.7.17. 컨트롤 플레인 노드의 NTP 서버

OpenShift Container Platform 4.8에서는 설치 관리자 프로비저닝 클러스터는 작업자 노드의 컨트롤 플레인 노드 및 NTP 클라이언트에 NTP(Network Time Protocol) 서버를 구성하고 배포할 수 있습니다. 이를 통해 작업자는 라우팅 가능한 네트워크에서 연결이 끊어진 경우에도 컨트롤 플레인 노드의 NTP 서버에서 날짜와 시간을 검색할 수 있습니다. 배포 후 NTP 서버 및 NTP 클라이언트를 구성하고 배포할 수도 있습니다.

1.4.7.18. Kuryr의 기본 API 로드 밸런서 관리로 변경

Kuryr-Kubernetes를 사용하는 RHOSP(Red Hat OpenStack Platform)에 OpenShift Container Platform 4.8 배포에서는 **default/kubernetes** 서비스의 API 로드 밸런서는 더 이상 CNO(Cluster Network Operator)에 의해 관리되지 않고 kuryr-controller 자체에서 대신 관리됩니다. 이는 다음을 의미합니다.

- OpenShift Container Platform 4.8로 업그레이드할 때 **default/kubernetes** 서비스에 다운타임이 발생합니다.



참고

OVN(Open Virtual Network) Octavia를 사용할 수 없는 배포에서는 다운타임이 늘어날 수 있습니다.

- Octavia Amphora 드라이버를 사용하는 데 더 이상 **default/kubernetes** 로드 밸런서가 필요하지 않습니다. 대신, OpenStack 클라우드에서 사용 가능한 경우 **default/kubernetes** 서비스를 구현하는 데 OVN Octavia가 사용됩니다.

1.4.7.19. 설치 후 프로비저닝 네트워크 활성화

베어 메탈 클러스터에 지원되는 설치 프로그램 및 설치 관리자 프로비저닝 설치는 **provisioning** 네트워크 없이 클러스터를 배포하는 기능을 제공합니다. OpenShift Container Platform 4.8 이상에서는 CBO(Cluster Baremetal Operator)를 사용하여 설치 후 **provisioning** 네트워크를 활성화할 수 있습니다.

1.4.7.20. 컨트롤 플레인에서 실행되도록 네트워크 구성 요소 구성

베어 메탈 설치의 컨트롤 플레인 노드에서 실행하려면 VIP 주소가 필요한 경우 컨트롤 플레인 노드에서 독점적으로 실행하도록 **apiVIP** 및 **ingressVIP** VIP 주소를 구성해야 합니다. 기본적으로 OpenShift Container Platform에서는 작업자 머신 구성 풀의 모든 노드가 **apiVIP** 및 **ingressVIP** VIP 주소를 호스팅할 수 있습니다. 베어 메탈 환경에서는 컨트롤 플레인 노드의 개별 서브넷에 작업자 노드를 배포하므로 **apiVIP** 및 **ingressVIP** 가상 IP 주소를 구성하여 컨트롤 플레인 노드에서 독점적으로 실행하도록 구성하면 별도의 서브넷에 작업자 노드를 배포하여 문제가 발생하지 않습니다. 보다 자세한 내용은 컨트롤 플레인에서 실행하기 위한 네트워크 구성 요소 설정에서 참조하십시오.

1.4.7.21. apiVIP 및 ingressVIP 트래픽에 대한 외부 로드 밸런서 구성

OpenShift Container Platform 4.8에서는 RHOSP(Red Hat OpenStack Platform) 및 베어 메탈 설치 관리자 프로비저닝 클러스터의 **apiVIP** 및 **ingressVIP** 트래픽을 처리하도록 외부 로드 밸런서를 구성할 수 있습니다. 외부 로드 밸런싱 서비스와 컨트롤 플레인 노드는 동일한 L2 네트워크에서 실행해야 하며 VLAN을 사용하여 로드 밸런싱 서비스와 컨트롤 플레인 노드 간에 트래픽을 라우팅할 때 동일한 VLAN에서 실행해야 합니다.

apiVIP 및 **ingressVIP** 트래픽을 처리하도록 로드 밸런서를 구성하는 것은 VMware 설치 관리자 프로비저닝 클러스터에 지원되지 않습니다.

1.4.7.22. 이중 스택 네트워킹에 대한 OVN-Kubernetes IPsec 지원

OpenShift Container Platform 4.8에는 이중 스택 네트워킹을 사용하도록 구성된 클러스터에 대한 OVN-Kubernetes IPsec 지원이 추가되었습니다.

1.4.7.23. OVN-Kubernetes의 송신 라우터 CNI

송신 라우터 CNI 플러그인을 일반적으로 사용할 수 있습니다. **EgressRouter** API 오브젝트를 지원하도록 Cluster Network Operator 기능이 개선되었습니다. OVN-Kubernetes를 사용하는 클러스터에 송신 라우터를 추가하는 프로세스가 간소화됩니다. 송신 라우터 오브젝트를 생성하면 Operator에서 네트워크 연결 정의 및 배포를 자동으로 추가합니다. 배포의 pod는 송신 라우터 역할을 합니다.

보다 자세한 내용은 송신 라우터 Pod 사용에 대한 고려 사항 을 참조하십시오.

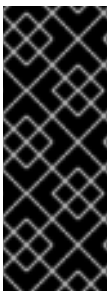
1.4.7.24. OpenShift Container Platform에서 IP 페일오버를 지원

베어 메탈 기반의 OpenShift Container Platform 클러스터에서 IP 페일오버가 지원됩니다. IP 페일오버는 **keepalived**를 사용하여 호스트 집합에서 외부 액세스가 가능한 VIP 주소 집합을 호스팅합니다. 각 VIP는 한 번에 하나의 호스트에서만 서비스를 제공합니다. **keepalived** 는 VRRP(Virtual Router Redundancy Protocol)를 사용하여 호스트 집합에서 VIP를 제공하는 서비스를 결정합니다. 호스트를 사용할 수 없게 되거나 **keepalived** 서비스가 응답하지 않는 경우 VIP가 세트의 다른 호스트로 전환됩니다. 즉, 호스트를 사용할 수 있는 한 VIP는 항상 서비스됩니다.

자세한 내용은 IP 페일오버 구성 을 참조하십시오.

1.4.7.25. DNS Pod 배치 제어

OpenShift Container Platform 4.8에서는 사용자 정의 노드 선택기 및 허용 오차를 사용하여 특정 노드에서 CoreDNS를 실행하거나 실행하지 않도록 데몬 세트를 구성할 수 있습니다.



중요

이전 버전의 OpenShift Container Platform에서는 모든 테인트에 대한 허용 오차를 사용하여 CoreDNS 데몬 세트를 구성하여 노드 테인트에 관계없이 DNS Pod가 클러스터의 모든 노드에서 실행되도록 했습니다. OpenShift Container Platform 4.8에서는 기본적으로 모든 테인트에 대해 이 허용 오차를 더 이상 구성하지 않습니다. 대신 기본값은 **node-role.kubernetes.io/master** taint를 허용하는 것입니다. DNS Pod를 다른 테인트가 있는 노드에서 실행하려면 사용자 정의 톨러레이션을 구성해야 합니다.

자세한 내용은 DNS pod 배치 제어 를 참조하십시오.

1.4.7.26. RHOSP에서 실행되는 클러스터를 지원하는 공급자 네트워크

RHOSP(Red Hat OpenStack Platform)의 OpenShift Container Platform 클러스터에서 이제 모든 배포 유형에 대해 공급자 네트워크를 지원합니다.

1.4.7.27. HAProxy에 대해 구성 가능한 tune.maxrewrite 및 tune.bufsize

클러스터 관리자는 이제 **headerBufferMaxRewriteByte** 및 **headerBufferBytes** Ingress 컨트롤러 튜닝 매개변수를 설정하여 Ingress 컨트롤러마다 **tune.maxrewrite** 및 **tune.bufsize** HAProxy 메모리 옵션을 구성할 수 있습니다.

보다 자세한 내용은 Ingress 컨트롤러 구성 매개변수 에서 참조하십시오.

1.4.8. 스토리지

1.4.8.1. GCP PD CSI 드라이버 Operator를 사용하는 영구 스토리지 사용 가능

GCP(Google Cloud Platform) PD(Persistent Disk) CSI(Container Storage Interface) 드라이버는 GCP 환경에서 자동으로 배포 및 관리되므로 드라이버를 수동으로 설치하지 않고도 이러한 볼륨을 동적으로 프로비저닝할 수 있습니다. 이 기능은 이전에 OpenShift Container Platform 4.7에서 기술 프리뷰 기능으로 소개되었으며 현재 OpenShift Container Platform 4.8에서 일반적으로 사용 가능하며 활성화되어 있습니다.

자세한 내용은 GCP PD CSI 드라이버 Operator 에서 참조하십시오.

1.4.8.2. Azure Disk CSI 드라이버 Operator를 사용한 영구 스토리지 (기술 프리뷰)

Azure Disk CSI Driver Operator는 PVC(영구 볼륨 클레임)를 생성하는 데 사용할 수 있는 기본 스토리지 클래스 오브젝트를 제공합니다. 이 드라이버를 관리하는 Azure Disk CSI Driver Operator는 기술 프리뷰로 사용할 수 있습니다.

자세한 내용은 Azure Disk CSI Driver Operator 에서 참조하십시오.

1.4.8.3. vSphere CSI Driver Operator를 사용한 영구 스토리지 (기술 프리뷰)

vSphere CSI Driver Operator는 PVC(영구 볼륨 클레임)를 생성하는 데 사용할 수 있는 기본 스토리지 클래스를 제공합니다. 이 드라이버를 관리하는 vSphere CSI Driver Operator는 기술 프리뷰로 사용할 수 있습니다.

자세한 내용은 vSphere CSI Driver Operator 에서 참조하십시오.

1.4.8.4. 자동 CSI 마이그레이션 (기술 프리뷰)

OpenShift Container Platform 4.8부터 동등한 CSI 드라이버로 다음 in-tree 볼륨 플러그인에 대한 자동 마이그레이션을 기술 프리뷰 기능으로 사용할 수 있습니다.

- AWS(Amazon Web Services) EBS(Elastic Block Storage)
- OpenStack Cinder

자세한 내용은 자동 CSI 마이그레이션 을 참조하십시오.

1.4.8.5. AWS EFS(기술 프리뷰) 기능의 외부 프로비저너가 제거됨

AWS(Amazon Web Services) Elastic File System (EFS) 기술 프리뷰 기능이 제거되어 더 이상 지원되지 않습니다.

1.4.8.6. RHOSP에서 실행되는 클러스터의 Cinder 볼륨 가용성 영역에 대한 제어 기능 강화

이제 설치 중에 Cinder 볼륨의 가용성 영역을 선택할 수 있습니다. 이미지 레지스트리의 특정 가용성 영역에서 Cinder 볼륨을 사용할 수도 있습니다.

1.4.9. 레지스트리

1.4.10. Operator 라이프사이클

1.4.10.1. 관리자의 오류 보고 기능 향상

OLM(Operator Lifecycle Manager)을 사용하여 Operator를 설치하는 클러스터 관리자는 현재 API 또는 하위 수준 API와 관련된 오류 조건에 직면할 수 있습니다. 이전에는 OLM이 Operator 설치 또는 업데이트 요청을 이행할 수 없는 이유에 대한 정보가 없었습니다. 이러한 오류는 오브젝트 속성의 오타 또는 누락된 RBAC와 같은 간단한 문제부터 메타데이터 구문 분석으로 인해 카탈로그에서 항목을 로드할 수 없는 더 복잡한 문제에 이르기까지 다양할 수 있습니다.

관리자에게 이러한 문제를 성공적으로 디버깅하기 위해 다양한 하위 수준 API 간의 상호 작용 프로세스 또는 OLM Pod 로그로의 액세스에 대한 이해를 요구하지 않기 때문에 OpenShift Container Platform 4.8에서는 OLM의 다음과 같은 개선 사항이 도입되어 관리자에게 보다 이해하기 쉬운 오류 보고 및 메시지를 제공합니다.

1.4.10.2. 설치 계획 재시도

InstallPlan 오브젝트에서 정의한 설치 계획에서 API 서버 가용성 또는 다른 작성자와의 충돌로 인해 일시적인 오류가 발생할 수 있습니다. 이전에는 이러한 오류로 인해 수동 정리가 필요한 부분적으로 적용된 설치 계획이 종료되었습니다. 이번 개선된 기능으로 Catalog Operator는 설치 계획 실행 중에 최대 1분 동안 오류를 다시 시도합니다. 새 **.status.message** 필드는 재시도가 발생할 때 사람이 읽을 수 있는 표시를 제공합니다.

1.4.10.3. 잘못된 Operator 그룹 표시

Operator 그룹 또는 여러 Operator 그룹이 없는 네임스페이스에 서브스크립션을 생성하면 이전에 설치 계획을 사용하여 Operator 설치가 중단되고 **phase=Installing**에 영구적으로 남아 있었습니다. 이번 개선된 기능을 통해 설치 계획이 **phase=Failed**로 즉시 전환되어 관리자가 잘못된 Operator 그룹을 수정한 다음 서브스크립션을 삭제하고 다시 생성할 수 있습니다.

1.4.10.4. 후보 Operator를 찾을 수 없는 경우 특정 보고

네임스페이스에서 종속성 확인이 실패할 때 생성되는 **ResolutionFailed** 이벤트는 이제 참조된 카탈로그 소스에 없는 패키지 또는 채널을 참조하는 서브스크립션이 포함된 경우 네임스페이스에 더 구체적인 텍스트를 제공합니다. 이전에는 이 메시지가 일반적이었습니다.

> no candidate operators found matching the spec of subscription '<name>'

이번 개선된 기능을 통해 메시지는 보다 구체화됩니다.

Operator가 존재하지 않습니다.

> no operators found in package <name> in the catalog referenced by subscription <name>

카탈로그가 존재하지 않습니다.

> no operators found from catalog <name> in namespace openshift-marketplace referenced by subscription <name>

-

채널이 존재하지 않습니다.

> no operators found in channel <name> of package <name> in the catalog referenced by subscription <name>

CSV(클러스터 서비스 버전)가 존재하지 않습니다.

> no operators found with name <name>.<version> in channel <name> of package <name> in the catalog referenced by subscription <name>

1.4.11. Operator 개발

1.4.11.1. 패키지 매니페스트 형식에서 번들 형식으로 Operator 프로젝트 마이그레이션

Operator에 대한 레거시 패키지 매니페스트 형식 지원은 OpenShift Container Platform 4.8 이상에서 제거됩니다. 번들 형식은 OpenShift Container Platform 4.6부터 OLM(Operator Lifecycle Manager)의 기본 Operator 패키징 형식입니다. 더 이상 사용되지 않는 패키지 매니페스트 형식으로 처음 생성된 Operator 프로젝트가 있는 경우 Operator SDK **pkgman-to-bundle** 명령을 사용하여 프로젝트를 번들 형식으로 마이그레이션할 수 있습니다.

자세한 내용은 번들 형식으로 패키지 매니페스트 프로젝트 마이그레이션 을 참조하십시오.

1.4.11.2. 번들 Operator가 포함된 카탈로그 게시

Operator를 설치하고 관리하려면 OLM(Operator Lifecycle Manager)이 클러스터의 카탈로그에서 참조하는 인덱스 이미지에 Operator 번들을 나열해야 합니다. Operator 작성자는 Operator SDK를 사용하여 Operator 및 모든 종속 항목에 대한 번들이 포함된 인덱스를 생성할 수 있습니다. 이 기능은 원격 클러스터에서 테스트하고 컨테이너 레지스트리에 게시하는 데 유용합니다.

자세한 내용은 번들 Operator가 포함된 카탈로그 게시 를 참조하십시오.

1.4.11.3. Operator 업그레이드 테스트 기능 개선

Operator SDK의 **run bundle-upgrade** 하위 명령은 최신 버전의 번들 이미지를 지정하여 설치된 Operator가 최신 버전으로 업그레이드되도록 트리거하는 작업을 자동화합니다. 이전에는 하위 명령은 **run bundle** 하위 명령을 사용하여 처음 설치한 Operator만 업그레이드할 수 있었습니다. 이번 개선된 기능을 통해 이제 기존 OLM(Operator Lifecycle Manager) 워크플로우와 함께 처음 설치된 Operator에서도 **run bundle-upgrade**가 작동합니다.

보다 자세한 내용은 Operator Lifecycle Manager에서 Operator 업그레이드 테스트 에서 참조하십시오.

1.4.11.4. OpenShift Container Platform 버전과 Operator 호환성 제어

OpenShift Container Platform 버전에서 API가 제거되면 제거된 API를 계속 사용하는 클러스터 버전에서 실행되는 Operator가 더 이상 제대로 작동하지 않게 됩니다. Operator 작성자는 Operator 사용자의 중단을 방지하기 위해 API 사용 중단 및 제거를 수용하도록 Operator 프로젝트를 업데이트해야 합니다.

자세한 내용은 OpenShift Container Platform 버전과 Operator 호환성 제어 를 참조하십시오.

빌드

1.4.11.5. 전략별 빌드 수에 대한 새 Telemetry 메트릭

Telemetry에는 새 **openshift:build_by_strategy:sum** 게이지 메트릭이 포함되어 있으며 이는 전략 유형별로 빌드 수를 Telemeter Client로 전송합니다. 이 메트릭을 사용하면 사이트 안정성 엔지니어(SRE)와 제품 관리자가 OpenShift Container Platform 클러스터에서 실행되는 빌드 종류를 확인할 수 있습니다.

1.4.11.6. 사용자 정의 PKI 인증 기관 마운트

이전 버전에서는 빌드에서 회사 아티팩트 리포지토리에 액세스하는 데 필요한 클러스터 PKI 인증 기관을 사용할 수 없었습니다. 이제 **mountTrustedCA**를 **true**로 설정하여 클러스터 사용자 정의 PKI 인증 기관을 마운트하도록 **BuildConfig** 오브젝트를 구성할 수 있습니다.

1.4.12. 이미지

1.4.13. 머신 API

1.4.13.1. 클러스터 자동 스케일러를 사용하여 vSphere에서 실행되는 머신을 0으로 스케일링

vSphere에서 머신을 실행할 때 **MachineAutoscaler** 리소스 정의에서 **minReplicas** 값을 **0**으로 설정할 수 있습니다. 이 값을 **0**으로 설정하면 클러스터 자동 스케일러는 시스템이 사용 중인지에 따라 0으로 시스템 집합을 스케일링합니다. 자세한 내용은 MachineAutoscaler 리소스 정의에서 참조하십시오.

1.4.13.2. kubelet-ca.crt 자동 순환에는 노드 드레이닝 또는 재부팅이 필요하지 않음

/etc/kubernetes/kubelet-ca.crt 인증 기관 (CA) 자동 순환에 더 이상 MCO(Machine Config Operator)가 노드를 드레이닝하거나 클러스터를 재부팅할 필요가 없습니다.

이번 변경의 일환으로 다음과 같은 수정 사항에 따라 MCO가 노드를 드레이닝할 필요가 없습니다.

- 머신 구성의 **spec.config.ignition.passwd.users.sshAuthorizedKeys** 매개변수에서 SSH 키 변경
- **openshift-config** 네임 스페이스에서 글로벌 풀 시크릿 또는 풀 시크릿 관련 변경 사항

MCO가 이러한 변경 사항을 감지하면 변경 사항을 적용한 다음 노드를 분리합니다.

자세한 내용은 Machine Config Operator 이해를 참조하십시오.

1.4.13.3. 머신 세트 정책 개선 사항

이전 버전에서는 머신 세트를 생성하려면 사용자가 CPU 고정 설정, NUMA 고정 설정, CPU 토폴로지 변경 등을 수동으로 구성해야 호스트에서 성능을 개선할 수 있었습니다. 이번 개선된 기능을 통해 사용자는 **MachineSet** 리소스에서 정책을 선택하여 설정을 자동으로 채울 수 있습니다. 자세한 내용은 BZ#1941334에서 참조하십시오.

1.4.13.4. 머신 세트 hugepage 기능 개선

이제 **MachineSet** 리소스에 **hugepages** 속성을 제공할 수 있습니다. 이번 개선된 기능으로 oVirt에서 사용자 지정 속성을 사용하여 **MachineSet** 리소스의 노드를 생성하고 이러한 노드에 하이퍼바이저의 **hugepages**를 사용하도록 지시합니다. 자세한 내용은 BZ#1948963에서 참조하십시오.

1.4.13.5. Machine Config Operator ImageContentSourcePolicy 오브젝트 기능 개선

OpenShift Container Platform 4.8은 선택한 **ImageContentSourcePolicy** 개체 변경에 대한 워크로드 중단을 방지할 수 있습니다. 이 기능을 사용하면 사용자와 팀이 워크로드 중단 없이 미러 및 레지스트리를 추가할 수 있습니다. 결과적으로 **/etc/containers/registries.conf** 파일에서 다음과 같은 변경에 대해 워크로

드 중단이 더 이상 발생하지 않습니다.

- **mirror-by-digest-only=true**인 레지스트리 추가
- **mirror-by-digest-only=true**인 레지스트리에 미러 추가
- **unqualified-search-registries** 목록에 항목 추가

/etc/containers/registries.conf 파일의 다른 변경 사항의 경우 Machine Config Operator는 기본적으로 노드를 드레이닝하여 변경 사항을 적용합니다. 자세한 내용은 BZ#1943315에서 참조하십시오.

1.4.14. 노드

1.4.14.1. Descheduler operator.openshift.io/v1 API 그룹 사용 가능

이제 Descheduler에 **operator.openshift.io/v1** API 그룹을 사용할 수 있습니다. Descheduler의 **operator.openshift.io/v1beta1** API 그룹에 대한 지원은 향후 릴리스에서 제거될 수 있습니다.

1.4.14.2. Descheduler에 대한 Prometheus 지표

Descheduler를 설치한 **openshift-kube-descheduler-operator** 네임스페이스에 **openshift.io/cluster-monitoring=true** 레이블을 추가하여 Descheduler에 대한 Prometheus 지표를 활성화할 수 있습니다.

다음 Descheduler 지표를 사용할 수 있습니다.

- **Descheduler_build_info** - Descheduler에 대한 빌드 정보를 제공합니다.
- **Descheduler_pods_evicted** - 전략, 네임스페이스, 결과의 조합에 대해 제거된 Pod 수를 제공합니다. 이 지표를 표시하려면 하나 이상의 제거된 Pod가 있어야 합니다.

1.4.14.3. Downward API를 사용하여 Huge Page 지원

이번 릴리스에서는 Pod 사양에서 Huge Page에 대한 요청 및 제한을 설정하면 Downward API를 사용하여 컨테이너 내에서 Pod 할당을 표시할 수 있습니다. 이러한 개선 사항은 **DownwardAPIHugePages** 기능 게이트를 사용합니다. OpenShift Container Platform 4.8에서는 기능 게이트를 활성화합니다.

자세한 내용은 Downward API를 사용하여 Huge Page 리소스 사용 을 참조하십시오.

1.4.14.4. Node Feature Discovery Operator의 새 레이블

NFD(노드 기능 검색) Operator는 OpenShift Container Platform 클러스터의 각 노드에서 사용 가능한 하드웨어 기능을 탐지합니다. 그런 다음 노드 레이블을 사용하여 노드 오브젝트를 수정합니다. 이를 통해 NFD Operator에서 특정 노드의 기능을 알릴 수 있습니다. OpenShift Container Platform 4.8에서는 NFD Operator에 대한 세 가지 추가 레이블을 지원합니다.

- **pstate intel-pstate**: Intel **pstate** 드라이버가 활성화되어 사용 중인 경우 **pstate intel-pstate** 레이블은 Intel **pstate** 드라이버의 상태를 반영합니다. 상태는 **active** 또는 **passive** 중 하나입니다.
- **pstate scaling_governor**: Intel **pstate** 드라이버 상태가 **활성** 상태이면 **pstate scaling_governor** 레이블은 scaling governor 알고리즘을 반영합니다. 알고리즘은 **powersave** 또는 **performance** 중 하나입니다.
- **Cstate 상태**: **intel_idle** 드라이버에 C-states 또는 idle 상태가 있는 경우 **cstate status** 레이블은 **true** 입니다. 그렇지 않은 경우는 **false**입니다.

1.4.14.5. Poison Pill Operator를 사용하여 비정상적인 노드 교정

Poison Pill Operator를 사용하여 비정상적인 노드를 자동으로 재부팅할 수 있습니다. 따라서 상태 저장 애플리케이션 및 RWO(ReadWriteOnce) 볼륨의 다운 타임을 최소화하고 일시적인 오류가 발생하면 컴퓨팅 용량을 복원합니다.

Poison Pill Operator는 모든 클러스터 및 하드웨어 유형에서 작동합니다.

자세한 내용은 Poison Pill Operator를 사용하여 노드 해결을 참조하십시오.

1.4.14.6. kubelet-ca.crt 자동 순환을 재부팅할 필요가 없음

/etc/kubernetes/kubelet-ca.crt 인증 기관 (CA) 자동 순환에 더 이상 MCO(Machine Config Operator)가 노드를 드레이닝하거나 클러스터를 재부팅할 필요가 없습니다.

이번 변경의 일환으로 다음과 같은 수정 사항에 따라 MCO가 노드를 드레이닝할 필요가 없습니다.

- 머신 구성의 **spec.config.ignition.passwd.users.sshAuthorizedKeys** 매개변수에서 SSH 키 변경
- **openshift-config** 네임 스페이스에서 글로벌 풀 시크릿 또는 풀 시크릿 관련 변경 사항

MCO가 이러한 변경 사항을 감지하면 변경 사항을 적용한 다음 노드를 분리합니다.

자세한 내용은 Machine Config Operator 이해 를 참조하십시오.

1.4.14.7. 일반적으로 수직 Pod 자동 스케일링 사용 가능

이제 OpenShift Container Platform VPA(Vertical Pod Autoscaler)를 일반적으로 사용할 수 있습니다. VPA는 Pod의 컨테이너 상태와 현재 CPU 및 메모리 리소스를 자동으로 확인하고 확인된 사용량에 따라 리소스 제한 및 요청을 업데이트할 수 있습니다.

아래 설명된 대로 **VerticalPodAutoscalerController** 오브젝트를 수정하여 하나의 복제본만 필요한 Pod와 함께 VPA를 사용할 수도 있습니다. 이전에는 VPA에서 두 개 이상의 복제본이 필요한 Pod에서만 작동했습니다.

보다 자세한 내용은 수직 Pod 자동 스케일러를 사용하여 Pod 리소스 수준 자동 조정 에서 참조하십시오.

1.4.14.8. 수직 Pod 자동 스케일링 최소값 구성

기본적으로 워크로드 오브젝트는 VPA가 Pod를 자동으로 업데이트할 수 있도록 최소 두 개의 복제본을 지정해야 합니다. 따라서 두 개 미만의 복제본을 지정하는 워크로드 오브젝트는 VPA에서 작동하지 않습니다. **minReplicas** 매개변수를 추가하도록 **VerticalPodAutoscalerController** 오브젝트를 수정하여 클러스터 전체 최소 값을 변경할 수 있습니다.

보다 자세한 내용은 수직 Pod 자동 스케일러를 사용하여 Pod 리소스 수준 자동 조정 에서 참조하십시오.

1.4.14.9. 노드의 CPU 및 메모리 리소스 자동 할당

OpenShift Container Platform은 노드가 시작될 때 **system-reserved** 설정의 최적의 크기 값을 자동으로 확인할 수 있습니다. 이전에는 **system-reserved** 설정의 CPU 및 메모리 할당이 수동으로 설정하는 데 필요한 고정된 제한사항이었습니다.

자동 리소스 할당이 활성화되면 각 노드의 스크립트가 노드에 설치된 CPU 및 메모리 용량을 기반으로 예약된 각각의 리소스에 최적 값이 계산됩니다.

자세한 내용은 노드의 리소스 자동 할당 을 참조하십시오.

1.4.14.10. 이미지 가져오기를 위해 특정 리포지토리 추가

이제 이미지 풀 및 푸시를 위해 허용되거나 차단된 레지스트리 목록을 생성할 때 레지스트리 내에서 별도의 리포지토리를 지정할 수 있습니다. 이전 버전에서는 레지스트리만 지정할 수 있었습니다.

자세한 내용은 특정 레지스트리 추가 및 특정 레지스트리 차단 을 참조하십시오.

1.4.14.11. Cron 작업 사용 가능

이제 cron 작업 사용자 정의 리소스를 일반적으로 사용할 수 있습니다. 이러한 변경의 일환으로 cron 작업의 성능을 크게 개선하는 새 컨트롤러가 구현되었습니다. cron 작업에 대한 자세한 내용은 작업 및 cron 작업 이해 를 참조하십시오.

1.4.15. Red Hat OpenShift Logging

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

1.4.16. 모니터링

1.4.16.1. 경고 규칙 변경

OpenShift Container Platform 4.8에는 다음 경고 규칙 변경 사항이 포함됩니다.

예 1.1. 경고 규칙 변경

- **ThanosSidecarPrometheusDown** 경고 심각도가 *중요*에서 *경고*로 업데이트되었습니다.
- **ThanosSidecarUnhealthy** 경고 심각도가 *중요*에서 *경고*로 업데이트되었습니다.
- **ThanosQueryHttpRequestQueryErrorRateHigh** 경고 심각도가 *중요*에서 *경고*로 업데이트되었습니다.
- **ThanosQueryHttpRequestQueryRangeErrorRateHigh** 경고 심각도가 *중요*에서 *경고*로 업데이트되었습니다.
- **ThanosQueryInstantLatencyHigh** 심각한 경고가 제거되었습니다. Thanos Querier가 즉각적 쿼리에 대한 대기 시간이 길면 이 경고가 실행됩니다.
- **ThanosQueryRangeLatencyHigh** 심각한 경고가 제거되었습니다. Thanos Querier가 범위 쿼리에 대한 대기 시간이 길면 이 경고가 실행됩니다.
- 모든 Thanos Querier 경고의 경우 **for** 시간이 1시간으로 증가되었습니다.
- 모든 Thanos 사이드카 경고의 경우 **for** 시간은 1시간으로 증가되었습니다.

참고

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

1.4.16.2. 향후 릴리스에서 제거될 사용 중인 API에 대한 경고 및 정보

OpenShift Container Platform 4.8에서는 다음 릴리스에서 제거될 API를 사용할 때 실행되는 두 개의 새 경고가 도입되었습니다.

- **APIRemovedInNextReleaseInUse** - OpenShift Container Platform의 다음 릴리스에서 제거될 API의 경우
- **APIRemovedInNextEUSReleaseInUse** - OpenShift Container Platform EUS (Extended Update Support)의 다음 릴리스에서 제거될 API의 경우

새 **APIRequestCount** API를 사용하여 더 이상 사용되지 않는 API를 사용하는 항목을 추적할 수 있습니다. 이를 통해 다음 릴리스로 업그레이드하기 위한 작업이 필요한지 여부를 계획할 수 있습니다.

1.4.16.3. 모니터링 스택 구성 요소 및 종속 항목에 대한 버전 업데이트

OpenShift Container Platform 4.8에는 다음과 같은 모니터링 스택 구성 요소 및 종속 항목에 대한 버전 업데이트가 포함되어 있습니다.

- Prometheus Operator는 이제 0.48.1 버전입니다.
- Prometheus는 이제 2.26.1 버전입니다.
- **node-exporter** 에이전트는 이제 버전 1.1.2입니다.
- Thanos는 이제 0.20.2 버전입니다.
- Grafana는 이제 7.5.5 버전입니다.

1.4.16.4. kube-state-metrics 가 버전 2.0.0으로 업그레이드되었습니다.

kube-state-metrics가 버전 2.0.0으로 업그레이드되었습니다. 다음 메트릭은 **kube-state-metrics** 버전 1.9에서 더 이상 사용되지 않으며 버전 2.0.0에서 제거됩니다.

- Pod의 일반적이지 않은 리소스 지표:
  - kube_pod_container_resource_requests_cpu_cores
  - kube_pod_container_resource_limits_cpu_cores
  - kube_pod_container_resource_requests_memory_bytes
  - kube_pod_container_resource_limits_memory_bytes
- 노드의 일반적이지 않은 리소스 지표:
  - kube_node_status_capacity_pods
  - kube_node_status_capacity_cpu_cores
  - kube_node_status_capacity_memory_bytes
  - kube_node_status_allocatable_pods
  - kube_node_status_allocatable_cpu_cores
  - kube_node_status_allocatable_memory_bytes

1.4.16.5. Grafana 및 Alertmanager UI 링크 제거

타사 Alertmanager UI에 대한 링크는 OpenShift Container Platform 웹 콘솔의 **모니터링 → 경고** 페이지에서 제거됩니다. 또한 타사 Grafana UI에 대한 링크는 **모니터링 → 대시보드** 페이지에서 제거됩니다. **openshift-monitoring** 프로젝트의 **네트워킹 → 경로** 페이지로 이동하여 **관리자** 화면의 웹 콘솔에서 Grafana 및 Alertmanager UI에 대한 경로에 계속 액세스할 수 있습니다.

1.4.16.6. 웹 콘솔에서 대시보드 기능 확장 모니터링

OpenShift Container Platform 웹 콘솔의 **모니터링 → 대시보드** 페이지에서 새로운 확장 기능을 사용할 수 있습니다.

- 마우스로 영역을 선택하여 단일 그래프를 확대하면 다른 모든 그래프가 업데이트되어 동일한 시간 범위가 반영되도록 합니다.
- 대시보드 패널은 이제 그룹으로 분류되어 확장 및 축소할 수 있습니다.
- 이제 단일 값 패널에서 값에 따라 색상을 변경할 수 있습니다.
- 이제 대시보드 레이블을 **대시보드** 드롭다운 목록에 표시합니다.
- 이제 **시간 범위** 드롭다운 목록에서 **사용자 지정 시간 범위**를 선택하여 대시보드에 대한 사용자 지정 시간 범위를 지정할 수 있습니다.
- 해당하는 경우 대시보드 필터 드롭다운 메뉴에서 **모든** 옵션을 선택하여 해당 필터의 모든 옵션에 대한 데이터를 표시할 수 있습니다.

1.4.17. 미터링

Metering Operator는 OpenShift Container Platform 4.6부터 더 이상 사용되지 않으며 다음 OpenShift Container Platform 릴리스에서 제거될 예정입니다.

1.4.18. 스케일링

1.4.18.1. 단일 노드 클러스터에서 실행

단일 노드 클러스터에서 테스트를 실행하면 SR-IOV 및 SCTP 테스트를 포함하여 특정 테스트에 시간 초과가 발생하고 컨트롤 플레인 및 작업자 노드가 필요한 테스트를 건너뜁니다. 노드를 재부팅해야 하는 구성으로 인해 OpenShift 컨트롤 플레인을 비롯한 전체 환경이 재부팅되므로 완료하는 데 시간이 더 오래 걸립니다. 컨트롤 플레인 노드 및 작업자 노드가 필요한 모든 PTP 테스트는 건너뜁니다. 테스트를 시작할 때 노드 수를 확인하고 그에 따라 테스트 동작을 조정하기 때문에 추가 구성이 필요하지 않습니다.

검색 모드에서 PTP 테스트를 실행할 수 있습니다. 테스트에서는 클러스터 외부에서 구성된 PTP 컨트롤 플레인을 검색합니다. 다음 매개 변수가 필요합니다.

- **ROLE_WORKER_CNF=master** - 컨트롤 플레인 (**master**)은 노드가 속하게 될 유일한 시스템 풀이므로 필요합니다.
- **XT_U32TEST_HAS_NON_CNF_WORKERS=false** - 모듈이 로드된 노드만 있으므로 **xt_u32** 오류 검사를 건너뛰도록 지시하는데 필요합니다.
- **SCTPTEST_HAS_NON_CNF_WORKERS=false** - 모듈이 로드된 노드만 있으므로 SCTP 오류 검사를 건너뛰도록 지시하는데 필요합니다.

1.4.18.2. Performance Addon Operator를 사용하여 NIC를 단축

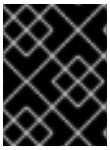
Performance Addon Operator를 사용하면 성능 프로필을 구성하여 각 네트워크 장치에 대한 NIC (Network Interface Card) 대기열 수를 조정할 수 있습니다. 장치 네트워크 대기열을 사용하면 패킷을 여러 물리적 대기열에 분산할 수 있으며 각 대기열은 패킷 처리를 위해 별도의 스레드를 가져옵니다.

DPDK(Data Plane Development Kit) 기반 워크로드의 경우 NIC 대기열을 예약된 CPU 또는 하우스키핑 CPU 수로 줄여 대기 시간을 단축하는 것이 중요합니다.

자세한 내용은 Performance Addon Operator를 사용하여 NIC 대기열 단축 을 참조하십시오.

1.4.18.3. 클러스터 최대값

OpenShift Container Platform 4.8의 클러스터 최대값 지침이 업데이트되었습니다.



중요

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

해당 환경의 클러스터 한도를 추정하려면 OpenShift Container Platform Limit Calculator 를 사용하십시오.

1.4.18.4. 성능 프로파일 작성

이제 PPC (Performance Profile Creator) 툴을 사용하여 성능 프로파일을 생성할 수 있습니다. 툴은 클러스터의 **must-gather** 데이터와 여러 사용자 지정 프로파일 인수를 소비하고, 이 정보를 사용하여 하드웨어 및 토폴로지에 적합한 성능 프로파일을 생성합니다.

자세한 내용은 성능 프로파일 생성 을 참조하십시오.

1.4.18.5. Node Feature Discovery Operator

이제 NFD(Node Feature Discovery) Operator 를 사용할 수 있습니다. 이를 사용하여 하드웨어 기능과 시스템 구성을 감지하기 위한 Kubernetes 애드온 기능인 NFD(Node Feature Discovery)을 오케스트레이션하여 노드 수준 정보를 노출합니다.

1.4.18.6. 드라이버 툴킷 (기술 프리뷰)

이제 Kubernetes에서 특수 소프트웨어 및 하드웨어 장치를 활성화할 수 있도록 드라이버 툴킷(Driver Toolkit)을 드라이버 컨테이너의 기본 이미지로 사용할 수 있습니다. 현재 기술 프리뷰 기능입니다.

1.4.19. 백업 및 복원

1.4.19.1. etcd 스냅샷 개선 사항

새로운 개선 사항에서는 백업 후와 복원 전에 etcd 스냅샷의 상태를 확인합니다. 이전 버전에서는 백업 프로세스가 스냅샷이 완료되었는지 확인하지 않았으며 복원 프로세스에서 복원된 스냅샷이 손상되지 않고 유효한지 확인하지 못했습니다. 이제 백업 또는 복원 중에 디스크가 손상되면 관리자에게 오류가 명확하게 보고됩니다. 자세한 내용은 BZ#1965024에서 참조하십시오.

1.4.20. Insights Operator

1.4.20.1. 제한된 네트워크 환경에서의 Insights Advisor 권장 사항

OpenShift Container Platform 4.8에서는 제한된 네트워크에서 작업하는 사용자가 Insights Operator 아카이브를 Insights Advisor에 수집하고 업로드하여 잠재적인 문제를 진단할 수 있습니다. 또한 사용자는 업로드하기 전에 Insights Operator 아카이브에 포함된 중요한 데이터를 읽을 수 있습니다.

자세한 내용은 네트워크가 제한된 환경에서 원격 상태 보고 사용 을 참조하십시오.

1.4.20.2. Insights Advisor 개선 사항

OpenShift Container Platform 웹 콘솔의 Insights Advisor에서 0개의 문제를 발견한 것으로 보고했던 것을 이제 올바르게 보고합니다. 이전에는 Insights Advisor는 정보를 제공하지 않았습니다.

1.4.20.3. Insights Operator 데이터 수집 기능 개선 사항

OpenShift Container Platform 4.8에서 Insights Operator는 다음과 같은 추가 정보를 수집합니다.

- 알려진 보안 문제 및 버전 문제를 찾기 위해 식별할 수 없는 클러스터 워크로드 정보
- **MachineHealthCheck** 및 **MachineAutoscaler** 정의
- **virt_platform** 및 **vsphere_node_hw_version_total** 지표
- SAP 스마트 데이터 통합 설치를 지원하기 위한 비정상적인 SAP pod에 대한 정보
- SAP 클러스터를 식별하기 위한 **datahubs.installers.datahub.sap.com** 리소스
- 네트워크 기능을 개선하기 위해 실패한 **PodNetworkConnectivityChecks**의 요약 정보
- **cluster-version** Operator 관련 문제를 디버깅하기 위해 **openshift-cluster-operator** 네임스페이스의 **cluster-version** Pod 및 이벤트에 대한 정보

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

1.4.20.4. 비정상적인 SAP Pod에 대한 Insights Operator 개선 사항

Insights Operator는 이제 비정상적인 SAP Pod에 대한 데이터를 수집할 수 있습니다. SDI 설치에 실패하면 초기화 Pod 중 실패한 항목을 확인하여 문제를 발견할 수 있습니다. 이제 Insights Operator에서 SAP/SDI 네임스페이스에서 실패한 Pod에 대한 정보를 수집할 수 있습니다. 자세한 내용은 BZ#1930393에서 참조하십시오.

1.4.20.5. SAP Pod 데이터 수집을 위한 Insights Operator 개선 사항

Insights Operator는 이제 SAP 클러스터에서 **Datahubs** 리소스를 수집할 수 있습니다. 이 데이터를 사용하면 SAP 클러스터에서만 수집된 모든 데이터가 누락되어 클러스터에 SDI 설치 여부를 확인할 수 없는 경우에도 SAP 클러스터를 Insights Operator 아카이브의 비SAP 클러스터와 구분할 수 있습니다. 자세한 내용은 BZ#1940432에서 참조하십시오.

1.4.21. 인증 및 권한 부여

1.4.21.1. 인증 정보인 AWS Security Token Service (STS)를 사용하여 OpenShift Container Platform을 실행 가능

Amazon Web Services Security Token Service (AWS STS)를 사용하도록 Cloud Credential Operator (CCO) 유틸리티 (**ccoctl**)를 설정할 수 있습니다. CCO가 STS를 사용하도록 구성되면 단기적이고 제한된 권한 보안 인증 정보를 제공하는 IAM 역할을 구성 요소에 할당합니다.

이 기능은 이전에 OpenShift Container Platform 4.7에서 기술 프리뷰 기능으로 소개되었으며 현재 OpenShift Container Platform 4.8에서 일반적으로 사용할 수 있습니다.

자세한 내용은 STS로 수동 모드 사용을 참조하십시오.

1.4.22. OpenShift 샌드박스 컨테이너

1.4.22.1. OpenShift Container Platform에서 OpenShift 샌드박스 컨테이너 지원(기술 프리뷰)

OpenShift 샌드박스 컨테이너 새 기능, 버그 수정, 알려진 문제 및 비동기 에라타 업데이트를 검토하려면 OpenShift 샌드박스 컨테이너 1.0 릴리스 노트 를 참조하십시오.

1.5. 주요 기술 변경 사항

OpenShift Container Platform 4.8에는 다음과 같은 주요 기술 변경 사항이 추가되었습니다.

Kuryr 서비스 서브넷 생성 변경 사항
Open Virtual Network를 사용하도록 구성된 Open Virtual Network를 사용하여 RHOSP(Red Hat OpenStack Platform)에 OpenShift Container Platform의 새 설치가 **networking.serviceCIDR**에서 요청된 크기의 두 배인 **services** 서브넷을 생성하지 않습니다. 생성된 서브넷이 요청된 크기와 동일합니다. 자세한 내용은 BZ#1955548에서 참조하십시오.

SHA-256 접두사가 없는 OAuth 토큰을 더 이상 사용할 수 없음
OpenShift Container Platform 4.6 이전에는 OAuth 액세스 및 권한 부여 토큰에 오브젝트 이름의 시크릿 정보가 사용되었습니다.

OpenShift Container Platform 4.6부터 OAuth 액세스 토큰 및 인증 토큰 오브젝트 이름은 SHA-256 접두사가 있는 중요하지 않은 오브젝트 이름으로 저장됩니다. 향후 OpenShift Container Platform 4.8에서는 SHA-256 접두사를 포함하지 않는 OAuth 토큰을 더 이상 사용하거나 생성할 수 없습니다.

FedRAMP (Federal Risk and Authorization Management Program)의 중간 수준의 제어
OpenShift Container Platform 4.8에서 **rhcos4-moderate** 프로파일이 완료되었습니다. **ocp4-moderate** 프로파일은 향후 릴리스에서 완료될 예정입니다.

Ingress 컨트롤러가 HAProxy 2.2.13으로 업그레이드
OpenShift Container Platform Ingress 컨트롤러가 HAProxy 버전 2.2.13으로 업그레이드되었습니다.

CoreDNS 버전 1.8.1로 업데이트
OpenShift Container Platform 4.8에서 CoreDNS는 여러 버그 수정, 이름 변경 메트릭 및 듀얼 스택 IPv6 활성화가 있는 버전 1.8.1을 사용합니다.

etcd에서 zap 로거 사용
OpenShift Container Platform 4.8에서 etcd는 이제 capnslog 대신 zap을 기본 로거로 사용합니다. zap은 시스템 사용 가능한 JSON 로그 메시지를 제공하는 구조화된 로거입니다. **jq**를 사용하여 이러한 로그 메시지를 쉽게 구문 분석할 수 있습니다.

capnslog 형식이 필요한 로그 소비자가 있는 경우 zap 로거 형식에 맞게 조정해야 할 수 있습니다.

capnslog 형식 예 (OpenShift Container Platform 4.7)

```
2021-06-03 22:40:16.984470 W | etcdserver: read-only range request
"key:\"/kubernetes.io/operator.openshift.io/clustercsidrivers/\"
range_end:\"/kubernetes.io/operator.openshift.io/clustercsidrivers0\" count_only:true " with result
"range_response_count:0 size:8" took too long (100.498102ms) to execute
```

zap 형식 예 (OpenShift Container Platform 4.8)

```
{"level":"warn","ts":"2021-06-14T13:13:23.243Z","caller":"etcdserver/util.go:163","msg":"apply request took too long","took":"163.262994ms","expected-duration":"100ms","prefix":"read-only range ","request":"key:\"/kubernetes.io/namespaces/default\" serializable:true keys_only:true ","response":"range_response_count:1 size:53"}
```

LSO에 대해 병합된 여러 데몬 세트
OpenShift Container Platform 4.8에서는 LSO(Local Storage Object)에 대해 여러 데몬 세트가 병합됩니다. 로컬 볼륨 사용자 지정 리소스를 생성하면 **daemonset.apps/diskmaker-manager**만 생성됩니다.

바인딩된 서비스 계정 토큰 볼륨이 활성화됨
이전에는 서비스 계정 토큰이 pod에 마운트된 시크릿이었습니다. OpenShift Container Platform 4.8부터 Projected 볼륨이 대신 사용됩니다. 이러한 변경으로 인해 서비스 계정 토큰에 더 이상 기본 시크릿이 포함되지 않습니다.

바인딩된 서비스 계정 토큰은 대상 바인딩 및 시간 바인딩입니다. 자세한 내용은 서비스 계정 토큰 바인딩 사용을 참조하십시오.

또한 kubelet은 토큰이 기간의 80%에 도달하면 토큰을 자동으로 업데이트하고, **client-go**는 토큰 변경 사항을 감시하고 자동으로 다시 로드합니다. 이러한 두 가지 동작의 조합은 바인딩된 토큰의 대부분의 사용이 만료되지 않는 기존 토큰의 사용과 다르지 않음을 의미합니다. **client-go** 외부의 비표준 사용으로 인해 문제가 발생할 수 있습니다.

Operator SDK v1.8.0
OpenShift Container Platform 4.8에서는 Operator SDK v1.8.0을 지원합니다. 이 최신 버전을 설치하거나 업데이트려면 Operator SDK CLI 설치를 참조하십시오.

참고

Operator SDK v1.8.0 은 Kubernetes 1.20을 지원합니다.

Operator SDK v1.3.0을 사용하여 이전에 생성되거나 유지 관리되는 Operator 프로젝트가 있는 경우 최신 Operator SDK 버전의 프로젝트 업그레이드를 참조하여 Operator SDK v1.8.0과의 호환성을 유지하도록 프로젝트를 업그레이드하십시오.

1.6. 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 4.8에서 더 이상 사용되지 않고 삭제된 주요 기능의 최신 목록은 아래 표를 참조하십시오. 더 이상 사용되지 않고 삭제된 기능에 대한 자세한 정보는 표 뒤에 나열되어 있습니다.

아래 표에서 기능은 다음과 같은 상태로 표시되어 있습니다.

- **GA**: *정식 출시일 (GA)*
- **TP**: *기술 프리뷰*
- **DEP**: *더 이상 사용되지 않음*
- **REM**: *삭제됨*

표 1.1. 사용되지 않거나 삭제된 기능 추적

기능	OCP 4.6	OCP 4.7	OCP 4.8
OperatorSource 개체	REM	REM	REM
패키지 매니페스트 형식(Operator Framework)	DEP	DEP	REM
oc adm catalog build	DEP	DEP	REM
oc adm catalog mirror의 **--filter-by-os** 플래그	GA	DEP	REM
v1beta1 CRDs	DEP	DEP	DEP
Docker Registry v1 API	DEP	DEP	DEP
Metering Operator	DEP	DEP	DEP
스케줄러 정책	GA	DEP	DEP
Cluster Samples Operator 의**ImageChangesInProgress** 상태	GA	DEP	DEP
Cluster Samples Operator의**MigrationInProgress** 상태	GA	DEP	DEP
OpenShift Container Platform 리소스의 **apiVersion**에서 **v1** 사용	GA	DEP	DEP
RHCOS(Red Hat Enterprise Linux CoreOS)에서 **dhclient** 사용	DEP	DEP	DEP
클러스터 로더	GA	GA	DEP
사용자의 RHEL 7 컴퓨팅 머신 가져오기	DEP	DEP	DEP
External provisioner for AWS EFS	REM	REM	REM
빌드 **BuildConfig** 사양의 **lastTriggeredImageID** 필드	GA	GA	DEP
Jenkins Operator	TP	TP	DEP
Prometheus 기반 HPA 사용자 정의 지표 어댑터	TP	TP	REM
RHV(Red Hat Virtualization)의 **instance_type_id** 설치 구성 매개 변수	GA	DEP	DEP

기능	OCP 4.6	OCP 4.7	OCP 4.8
Microsoft Azure 클러스터의 인증 정보 축소	GA	GA	REM

1.6.1. 더 이상 사용되지 않는 기능

1.6.1.1. Descheduler operator.openshift.io/v1beta1 API 그룹이 더 이상 사용되지 않음

Descheduler의 **operator.openshift.io/v1beta1** API 그룹은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 수 있습니다. 대신 **operator.openshift.io/v1** API 그룹을 사용합니다.

1.6.1.2. RHCOS(Red Hat Enterprise Linux CoreOS)에서 dhclient가 더 이상 사용되지 않음

OpenShift Container Platform 4.6부터 RHCOS(Red Hat Enterprise Linux CoreOS)는 **initramfs**에서 **NetworkManager**를 사용하여 초기 부팅 시 네트워킹을 구성하도록 전환되었습니다. 이러한 변경의 일환으로 DHCP에 대해 **dhclient** 바이너리 사용이 더 이상 지원되지 않습니다. 대신 네트워킹 구성에 **NetworkManager** 내부 DHCP 클라이언트를 사용합니다. **dhclient** 바이너리는 향후 릴리스에서 RHCOS(Red Hat Enterprise Linux CoreOS)에서 제거됩니다. 자세한 내용은 BZ#1908462에서 참조하십시오.

1.6.1.3. 클러스터 로더가 더 이상 사용되지 않음

클러스터 로더는 더 이상 사용되지 않으며 향후 릴리스에서 제거됩니다.

1.6.1.4. 빌드의 lastTriggeredImageID 매개변수는 더 이상 사용되지 않습니다.

이번 릴리스에서는 **BuildConfig** 사양에 설정할 수 있는 **BuildTriggerPolicy** 유형 중 하나인 **ImageChangeTrigger** 오브젝트에서 **lastTriggeredImageID**를 더 이상 사용하지 않습니다.

OpenShift Container Platform 다음 릴리스에서는 **lastTriggeredImageID** 에 대한 지원이 제거되고 무시됩니다. 그런 다음 이미지 변경 트리거는 **BuildConfig** 사양의 **lastTriggeredImageID** 필드에 대한 변경 사항을 기반으로 빌드를 시작하지 않습니다. 대신 빌드를 트리거하는 이미지 ID가 **BuildConfig** 오브젝트의 상태에 기록되며, 대부분의 사용자는 이를 변경할 수 없습니다.

따라서 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID**를 검사하는 스크립트 및 작업을 업데이트합니다. (BUILD-213)

1.6.1.5. Jenkins Operator(기술 프리뷰)는 더 이상 사용되지 않음

이번 릴리스에서는 기술 프리뷰 기능인 Jenkins Operator를 더 이상 사용하지 않습니다. 향후 OpenShift Container Platform 버전에서는 OpenShift Container Platform 웹 콘솔 인터페이스의 OperatorHub에서 Jenkins Operator를 제거합니다. 그런 다음 Jenkins Operator에 대한 업그레이드를 더 이상 사용할 수 없으며 Operator가 지원되지 않습니다.

고객은 Samples Operator에서 제공하는 템플릿을 사용하여 OpenShift Container Platform에 Jenkins를 계속 배포할 수 있습니다.

1.6.1.6. RHV(Red Hat Virtualization)의 instance_type_id 설치 구성 매개 변수

instance_type_id 설치 구성 매개 변수는 더 이상 사용되지 않으며 향후 릴리스에서 제거됩니다.

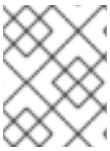
1.6.2. 삭제된 기능

1.6.2.1. Microsoft Azure에 대한 인증 정보 풀링 지원

OpenShift Container Platform 4.8.34부터 Microsoft Azure 클러스터의 mint 모드에서 CCO(Cloud Credential Operator) 사용에 대한 지원이 OpenShift Container Platform 4.8에서 제거되었습니다. 이러한 변경 사항은 2022년 6월 30일에 예정된 Microsoft Azure AD Graph API 사용 중지 로 인한 것이며 z-stream 업데이트에서 지원되는 모든 OpenShift Container Platform 버전으로 백포트되고 있습니다.

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

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



참고

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

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

Azure AD Graph API가 종료된 후 Mint 모드를 지원하지 않는 OpenShift Container Platform 버전으로 클러스터가 업그레이드되면 CCO는 연결된 **CredentialsRequest**에서 **OrphanedCloudResource** 조건을 설정하지만 오류를 치명적으로 처리하지는 않습니다. 조건에는 **unable to clean up App Registration / Service Principal: <app_registration_name>** 것과 유사한 메시지가 포함됩니다. Azure AD Graph API를 종료한 후에는 나머지 앱 등록 서비스 주체를 제거하기 위해 Azure CLI 도구 또는 Azure 웹 콘솔을 사용하여 수동 개입이 필요합니다.

리소스를 수동으로 정리하려면 영향을 받는 리소스를 찾아서 삭제해야 합니다.

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

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

출력 예

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

2. 다음 명령을 실행하여 앱 등록 서비스 주체를 삭제합니다.

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

참고

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

AWS EFS(기술 프리뷰) 기능의 외부 프로비저너가 제거됨

AWS(Amazon Web Services) Elastic File System (EFS) 기술 프리뷰 기능이 제거되어 더 이상 지원되지 않습니다.

1.6.2.2. 샘플 이미지 스트림에서 제거된 이미지

OpenShift Container Platform에서 제공되는 샘플 이미지 스트림에 더 이상 다음 이미지가 포함되지 않습니다.

```
registry.redhat.io/rhscl/nodejs-10-rhel7
registry.redhat.io/ubi7/nodejs-10
registry.redhat.io/rhscl/perl-526-rhel7
registry.redhat.io/rhscl/postgresql-10-rhel7
registry.redhat.io/rhscl/ruby-25-rhel7
registry.redhat.io/ubi7/ruby-25
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.9.0
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.9.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.9.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.9.0
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.9.0
```

1.6.2.3. Operator의 패키지 매니페스트 형식이 더 이상 지원되지 않음

Operator에 대한 레거시 패키지 매니페스트 형식 지원은 OpenShift Container Platform 4.8 이상에서 제거됩니다. 이러한 지원 제거에는 기존 형식으로 작성된 사용자 정의 카탈로그와 Operator SDK를 사용하여 처음 생성된 Operator 프로젝트가 포함되어 있습니다. 번들 형식은 OpenShift Container Platform 4.6부터 OLM(Operator Lifecycle Manager)의 기본 Operator 패키징 형식입니다.

번들 형식 사용에 대한 자세한 내용은 사용자 정의 카탈로그 관리 및 패키지 매니페스트 프로젝트를 번들 형식으로 마이그레이션을 참조하십시오.

또한 형식과 관련된 다음 명령이 OpenShift CLI (**oc**) 및 Operator SDK CLI에서 제거되었습니다.

- **oc adm catalog build**
- **operator-sdk generate packagemanifest**
- **operator-sdk run packagemanifest**

1.6.2.4. Prometheus 기반 HPA 사용자 지정 지표 어댑터 지원 제거

이 릴리스에서는 기술 프리뷰 기능인 Prometheus Adapter를 제거합니다.

1.6.2.5. 보안 토큰 스토리지 주석 인식이 제거됨

이제 클러스터의 감사 정책을 선택할 때 **authentication** 및 **openshift-apiserver** Operator에서 **oauth-apiserver.openshift.io/secure-token-storage** 주석을 무시합니다. 이제 감사 정책에서는 기본적으로 **secure-**를 사용합니다. 자세한 내용은 BZ#1879182에서 참조하십시오.

1.7. 버그 수정

assisted-installer

- 이전 버전에서 **Helped-service** 컨테이너는 **postgres** 가 시작되고 연결을 허용할 준비가 될 때까지 기다리지 않았습니다. **assisted-service** 컨테이너는 데이터베이스 연결을 설정 시도했지만 실패했으며 **assisted-service** 컨테이너가 실패하고 다시 시작되었습니다. 이 문제는 **assisted-service** 컨테이너에서 최대 10 초 동안 데이터베이스에 연결하려고 시도함으로써 해결되었습니다. **postgres**가 시작되고 10초 내에 연결을 허용할 준비가 되면 **assisted-service** 컨테이너가 오류 상태가 되지 않고 연결됩니다. **assisted-service** 컨테이너가 10초 이내에 **postgres**에 연결할 수 없는 경우 오류 상태가 되고 재시작 후 다시 시도합니다. (BZ#1941859)

베어 메탈 하드웨어 프로비저닝

- 이전에는 Ironic에서 기본적으로 HTTPS를 사용하고 올바른 인증서 번들을 사용할 수 없기 때문에 설치용 이미지를 다운로드하지 못했습니다. 이 문제는 이미지 다운로드를 **Insecure**로 설정하여 인증서 없이 전송을 요청하면 해결됩니다. (BZ#1953795)

- 이전에는 듀얼 스택 네트워킹을 사용할 때 작업자 노드 호스트 이름이 배포 전에 Ironic에서 검사한 호스트 이름과 일치하지 않는 경우가 있었습니다. 이로 인해 노드에 수동 승인이 필요했습니다. 이 문제는 해결되었습니다. (BZ#1955114)

- 이전에는 UEFI 모드에서 RHCOS 이미지를 다운로드한 후 **ironic-python-agent**가 UEFI 부트로더 항목을 생성했습니다. RHEL 8.4 기반의 RHCOS 이미지를 사용하는 경우 이 항목을 사용하여 이미지를 부팅하지 못할 수 있었습니다. 이미지를 부팅할 때 Ironic에서 설치한 항목을 사용하는 경우 부팅에 실패하고 BIOS 오류 화면이 출력될 수 있습니다. 이는 고정된 부팅 항목을 사용하는 대신 이미지에 있는 CSV 파일을 기반으로 부팅 항목을 구성하는 **ironic-python-agent**에 의해 해결됩니다. 이미지가 오류 없이 제대로 부팅됩니다. (BZ#1972213)

- 이전에는 노드가 시작 시 잘못된 IP 버전(IPv4 대신 IPv6 또는 그 반대)을 선택하는 경우가 있었습니다. 노드가 IP 주소를 수신하지 못했기 때문에 시작되지 않습니다. 이는 Cluster Bare Metal Operator가 IP 옵션을 다운로드자(**ip=dhcp** 또는 **ip=dhcp6**)에 전달하여 해결되므로 시작 시 올바르게 설정되고 노드가 예상대로 시작됩니다. (BZ#1946079)

- 이전에는 virtualmedial iso를 호스팅하는 HTTP 서버에 직접 연결을 활성화하고 로컬 스토리지 문제를 방지할 수 있도록 Ironic의 이미지 캐싱 메커니즘이 비활성화되어 있었습니다. 비표준 호환 HTTP 클라이언트 및 redfish 구현으로 인해 BMC 연결에 오류가 발생했습니다. 이 문제는 virtualmedia iso 가 캐시되어 Ironic 실행 노드에서 제공되는 기본 Ironic 동작으로 복구하여 해결되었습니다. 비표준 HTTP 클라이언트 및 redfish 구현으로 인한 문제가 해결되었습니다. (BZ#1962905)

- 이전에는 머신 인스턴스 **state** 주석이 설정되지 않았습니다. 그 결과 **STATE** 열이 비어 있었습니다. 이번 업데이트를 통해 이제 머신 인스턴스 **state** 주석이 설정되고 **STATE** 열의 정보가 자동으로 채워집니다. (BZ#1857008)

- 최신 ipmitool 패키지는 기본적으로 암호화 제품군 17을 사용하므로 암호 모음 17을 지원하지 않는 이전 하드웨어는 배포 중에 실패합니다. 하드웨어에서 암호화 제품군 17을 지원하지 않으면 Ironic에서 암호화 제품군 3을 사용하므로 ipmitool을 사용한 이전 하드웨어에 성공적으로 배포할 수 있습니다. (BZ#1897415)

- 이전에는 이미지 캐시를 채우기 전에 채택이 발생하여 영구적으로 채택이 실패하고 재시도를 시도하지 않은 경우도 있었습니다. 이로 인해 컨트롤 플레인 베어 메탈 호스트가 **adoption failed**를 보고했습니다. 이번 업데이트에서는 채택 실패 후 컨트롤 플레인 호스트가 올바르게 채택될 때까지 외부 프로비저닝 호스트를 자동으로 다시 시도합니다. (BZ#1905577)

- 이전에는 CR(사용자 정의 리소스)에 BMC(Baseboard Management Controller) 세부 정보가 필요했습니다. 그러나 지원 설치 프로그램에서 이 정보는 제공되지 않았습니다. 이번 업데이트를 통해 CR에서 노드를 생성하지 않는 경우 BMC 세부 정보를 건너뛸 수 있습니다. (BZ#1913112)

- 노드에 이미지를 프로비저닝할 때 qemu-image 가 1G의 RAM으로 제한되어 qemu-img가 충돌할 수 있었습니다. 이번 수정으로 제한이 2G로 증가하여 qemu-img가 프로비저닝을 안정적으로 완료합니다. (BZ#1917482)

- redfish/v1/SessionService URL에는 인증이 필요하므로 Ironic에서 사이트에 액세스할 때 인증 오류가 발생할 수 있었습니다. Ironic에서 이 오류 메시지를 보고할 때 기능적인 문제가 없기 때문에 해당 메시지가 제거되었습니다. (BZ#1924816)

- 일부 드라이브의 경우 파티션(예: **/dev/sda1**)에는 읽기 전용 파일이 없었습니다. 그러나 기본 장치(예: **/dev/sda**)에는 이 파일이 있습니다. 따라서 Ironic에서 파티션이 읽기 전용인지 확인할 수 없어 해당 드라이브에서 메타데이터 정리가 실패할 수 있었습니다. 이번 업데이트를 통해 파티션이 읽기 전용으로 감지되고 기본 장치에 대한 추가 검사가 포함됩니다. 결과적으로 읽기 전용 파티션에서 메타데이터 정리가 수행되지 않으며 메타데이터 정리가 더 이상 실패하지 않습니다. (BZ#1935419)

- 프록시가 구성된 상태에서 베어 메탈 IPI를 배포하면 내부 머신-os 이미지 다운로드가 프록시를 통해 전달되었습니다. 이로 인해 이미지가 손상되어 다운로드되지 않았습니다. 이번 업데이트에서는 이미지 다운로드가 더 이상 프록시를 사용하지 않도록 내부 이미지 트래픽이 **no_proxy**로 수정되었습니다. (BZ#1962592)

- 이전에는 Ironic과 RAM 디스크 간에 대용량 패킷을 전송하면 베어 메탈 배포에 실패했습니다. 이번 업데이트를 통해 Ironic은 RAM 디스크에서 연결 오류와 관련된 정보를 쿼리하여 배포가 성공할 수 있도록 합니다. (BZ#1957976)

빌드

- 이전에는 CVE-2021-3344가 수정된 후 빌드에서 OpenShift Container Platform 노드에 인타이틀먼트 키를 자동으로 마운트하지 않았습니다. 따라서 인타이틀먼트 인증서가 호스트 또는 노드에 저장된 경우 수정으로 사용 권한이 있는 빌드가 원활하게 작동하지 않습니다. 호스트 또는 노드에 저장된 인타이틀먼트 인증서를 가져오지 못한 경우 4.7.z의 BZ#1945692 및 4.6.z의 BZ#1946363에서 수정되었지만 이러한 수정으로 RHCOS(Red Hat Enterprise Linux CoreOS) 작업자 노드에서 실행되는 빌드에 대한 경고 메시지가 추가되었습니다. 현재 릴리스에서는 빌드가 RHEL 작업자 노드에서만 인타이틀먼트를 자동으로 마운트하고 RHCOS 작업자 노드에서 마운트 시도를 방지하여 이 문제를 해결합니다. 이제 RHCOS 노드에서 빌드를 실행할 때 인타이틀먼트 마운트에 대한 무단 경고가 발생하지 않습니다. (BZ#1951084)

- Docker Hub에서 이미지를 가져오는 일부 사용자는 다음 오류가 발생할 수 있습니다.

  > container image registry lookup failed...toomanyrequests: You have reached your pull rate limit

  이 오류는 **oc new-app**을 호출하는 데 사용한 **docker.io** 로그인에 **docker.io**의 유료 지원이 없기 때문에 발생합니다. 결과 애플리케이션에는 이미지 가져오기 제한의 대상이 되며 이로 인해 오류가 발생할 수 있습니다. 현재 릴리스에서는 **oc new-app** 도움말을 업데이트하여 이미지 레지스트리 및 리포지토리 사양에 대한 기본값이 작동하는 것을 사용자에게 알립니다. 따라서 사용자는 가능한 경우 기본값이 아닌 이미지 참조를 사용하여 유사한 오류를 방지할 수 있습니다. (BZ#1928850)

- 이전에는 빌드가 이미지 푸시에 실패했는지 오류 검사를 수행하지 않았습니다. 결과적으로 빌드는 항상 **Successfully push** 메시지를 기록했습니다. 이제 빌드에서 오류가 발생했는지 확인하고 이미지 푸시에 성공한 후에만 **Successfully push** 메시지를 기록합니다. (BZ#1947164)

- 이전에는 문서 및 **oc explain** 도움말 텍스트에서 **BuildConfig** 오브젝트의 **buildArgs** 필드가 기본 Kubernetes **EnvVar** 유형의 **valueFrom** 필드를 지원하지 않는 것을 전달하지 않았습니다. 그 결과 사용자들은 이것이 지원되는 것으로 믿고 이를 사용하려고 했습니다. 현재 릴리스에서는 문서 및 도움말 텍스트가 업데이트되므로 **BuildConfig** 오브젝트의 **buildArgs** 필드에서 **valueFrom** 필드를 지원하지 않는 것이 더 명확하게 되어 있습니다. (BZ#1956826)

- 빌드가 기본 이미지 가져오기와 같은 이미지 레지스트리와 상호 작용할 때 간헐적인 통신 문제로 인해 빌드 오류가 발생할 수 있습니다. 현재 릴리스에서는 이러한 상호 작용에 대한 재시도 횟수가 증가되어 있습니다. 이제 이미지 레지스트리와 간헐적인 통신 문제가 발생하면 OpenShift Container Platform 빌드의 복원력이 향상됩니다. (BZ#1937535)

클라우드 컴퓨팅

- 이전에는 **Cluster Image Registry Operator**가 **user_domain_name**을 변경할 수 없는 필드로 간주하여 설치 후 수정하지 않았습니다. 이로 인해 **user_domain_name**에 대한 변경 사항을 수락하지 않고 결과적으로 자격 증명이 발생했습니다. 이번 업데이트에서는 **user_domain_name**을 변경 가능한 것으로 표시하고 이미지 레지스트리 구성에 저장하지 않습니다. 이렇게 하면 설치 후 **user_domain_name** 및 기타 모든 **auth** 매개 변수를 수정할 수 있습니다. (BZ#1937464)

- 이전 버전에서는 프록시 업데이트로 인해 CI(Continuous Integration)가 실행되는 동안 API 서버 재시작을 포함하여 전체 클러스터 구성 업데이트가 발생했습니다. 결과적으로 Machine API Operator의 일부 클러스터가 예기치 않은 API 서버 중단으로 인해 시간 초과되었습니다. 이번 업데이트에서는 프록시 테스트를 분리하고 postconditions를 추가하여 CI 실행 중에 Machine API Operator의 클러스터가 다시 안정화됩니다. (BZ#1913341)

- 이전 버전에서는 다양한 vCenter 작업 유형이 구분되지 않았기 때문에 **Insufficient disk space on datastore** 상태의 머신을 삭제하는 데 예상보다 오랜 시간이 걸렸습니다. 이번 업데이트를 통해 머신 컨트롤러 삭제 절차에서 vCenter 작업 유형을 확인하고 더 이상 머신 컨트롤러의 삭제를 차단하지 않습니다. 결과적으로 머신 컨트롤러가 즉시 삭제됩니다. (BZ#1918101)

- 이전 버전에서는 인스턴스 유형이 누락된 경우에도 제로 주석에서 스케일링을 다시 큐에 추가했습니다. 그 결과 MachineSet 컨트롤러 로그에 지속적인 대기열 및 오류 공간 메시지가 표시되었습니다. 이번 업데이트를 통해 인스턴스 유형을 자동으로 확인하지 않으면 사용자가 주석을 수동으로 설정할 수 있습니다. 결과적으로 사용자가 주석을 수동으로 제공하면 알 수 없는 인스턴스 유형에 대해 0에서 부터 확장이 수행됩니다. (BZ#1918910)

- 이전에는 Machine API 종료 처리기에서 HTTP 응답이 올바르게 닫히지 않았습니다. 그 결과 **net.http** 읽기 및 쓰기 루프에 goroutine이 유출되어 메모리 사용량이 증가했습니다. 이번 업데이트를 통해 HTTP 응답이 항상 올바르게 닫힙니다. 결과적으로 메모리 사용량이 안정적이게 되었습니다. (BZ#1934021)

- 이전에는 MachineSet 컨트롤러 내부에 생성된 여러 클라이언트 세트로 인해 시작 시간이 지연되어 일부 대규모 클러스터에서 Pod가 준비 상태 검사에 실패했습니다. 결과적으로 MachineSet 컨트롤러가 무단 루프에 고정되었습니다. 이번 업데이트에서는 단일 클라이언트를 사용하도록 MachineSet 컨트롤러가 수정되었습니다. 결과적으로 MachineSet 컨트롤러가 예상대로 작동합니다. (BZ#1934216)

- 이전 버전에서는 첫 번째 부팅 시 Machine Config Daemon에서 업그레이드를 수행할 때 인스턴스를 부팅하는 데 시간이 오래 걸렸습니다. 그 결과 작업자 노드는 재시작 루프에 고착되어 MCH(시스템 상태 점검)가 제대로 시작되지 않았기 때문에 작업자 노드를 제거했습니다. 이번 업데이트를 통해 MHC는 제대로 시작되지 않은 노드를 더 이상 제거하지 않습니다. 대신 MHC는 명시적으로 요청된 경우에만 노드를 제거합니다. (BZ#1939054)

- 이전에는 CSR(인증서 서명 요청) 승인이 알 수 없는 이유로 지연되었습니다. 결과적으로 설치 중에 클러스터에 새 머신이 표시되고 클러스터 설치에 시간이 걸렸습니다. 초기 설치 단계에서 경우에 따라 사용할 수 없는 API 서버를 완화하기 위해 이번 업데이트에서는 캐시 재동기화 기간을 10시간에서 10분으로 변경합니다. 결과적으로 이제 컨트롤 플레인 머신이 보다 신속하게 승인되므로 클러스터 설치에 시간이 걸리지 않습니다. (BZ#1940972)

- 이전 버전에서는 기본 GCP(Google Cloud Platform) 이미지가 최신 Ignition 버전을 지원하지 않는 OpenShift Container Platform 4.6 릴리스의 버전을 참조했습니다. 결과적으로 기본 GCP 이미지를 사용하는 클러스터의 새 머신이 OpenShift Container Platform 4.7 이상을 부팅할 수 없었

습니다. 이번 업데이트에서는 릴리스 버전과 일치하도록 GCP 이미지가 업데이트되었습니다. 결과적으로 새 머신은 이제 기본 GCP 이미지로 부팅할 수 있습니다. (BZ#1954597)

- 이전 버전에서는 VM(가상 머신)의 ProvisioningState 값을 엄격하게 검사했기 때문에 존재 여부를 확인하는 동안 VM이 실패하는 경우가 있었습니다. 이번 업데이트에서는 존재 여부 확인 중에 삭제된 머신만 **Failed** 단계로 진행될 수 있도록 검사가 더 편리해졌습니다. (BZ#1957349)

- 이전에는 AWS 클러스터에서 **oc delete machine**을 사용하여 컨트롤 플레인 시스템을 삭제한 경우 해당 머신이 로드 밸런서에서 제거되지 않았습니다. 결과적으로 로드 밸런서는 제거된 컨트롤 플레인 시스템에 대한 요청을 계속 처리했습니다. 이번 수정으로 컨트롤 플레인 시스템을 제거해도 로드 밸런서에서 더 이상 시스템에 대한 요청을 처리하지 않습니다. (BZ#1880757)

- 이전 버전에서는 연결할 수 없는 머신을 삭제할 때 영구 볼륨에 생성된 노드에 연결된 vSphere VMDK(가상 머신 디스크)가 잘못 삭제되었습니다. 그 결과 VMDK의 데이터를 복구할 수 없었습니다. 이번 수정에서는 kubelet에 연결할 수 없는 경우 vSphere 클라우드 공급자가 노드에서 이러한 디스크를 확인하고 분리합니다. 결과적으로 VMDK를 손실하지 않고 연결할 수 없는 시스템을 삭제할 수 있습니다. (BZ#1883993)

- 이전에는 성된 AWS 인스턴스 유형 목록이 최신 버전이 아니었기 때문에 복제본이 0인 Cluster Autoscaler Operator 및 머신 세트를 사용할 때 일부 최신 AWS(Amazon Web Services) 인스턴스 유형을 0에서 확장할 수 없었습니다. 이제 최신 인스턴스 유형을 포함하도록 AWS 인스턴스 유형 목록이 업데이트되었습니다. 이번 수정을 통해 클러스터 자동 스케일러 Operator에서 복제본이 없는 경우 더 많은 인스턴스 유형을 사용할 수 있습니다. (BZ#1896321)

- 이전에는 Pod 중단 예산에서 업스트림 제거 API 기능이 누락되어 연결할 수 없는 노드에서 Pod를 배출할 수 없었습니다. 결과적으로 연결할 수 없는 노드의 시스템은 삭제 후 제거되는 데 과도한 시간이 걸릴 수 있었습니다. 이제 연결할 수 없는 노드에서 머신을 삭제할 때 유예 기간 제한 시간이 1초로 변경되었습니다. 이번 수정으로 Machine API에서 연결할 수 없는 노드를 성공적으로 배출 및 삭제할 수 있습니다. (BZ#1905709)

Cloud Credential Operator

- 이전에는 Cloud Credential Operator가 **지원되지 않는 플랫폼 유형을 반복했습니다. 베어 메탈 플랫폼에서 baremetal** 경고. 이번 업데이트를 통해 베어 메탈 플랫폼은 더 이상 알 수 없는 플랫폼으로 취급되지 않습니다. 따라서 잘못된 로깅 메시지가 줄어듭니다. (BZ#1864116)

- 이전 버전에서는 Cloud Credential Operator의 **credentialsRequest** CR(사용자 정의 리소스)에 저장된 반복적인 오류 메시지 표시로 인해 과도한 CPU 사용량이 발생하고 AWS(Amazon Web Services) 속도 제한과 같은 일부 오류 시나리오에 로깅되었습니다. 이번 업데이트에서는 사용자가 더 쉽게 찾을 수 있는 조건에 오류 메시지가 저장되도록 클라우드 공급자에서 반환되는 요청 ID를 제거하고 **CredentialRequest** CR에서 반복되는 오류 메시지를 제거합니다. (BZ#1910396)

- 이전에는 CCO 배포가 비정상적인지 여부를 CCO(Cloud Credential Operator)와 CVO(Cluster Version Operator) 모두 보고했습니다. 이로 인해 문제가 발생한 경우 이중 보고가 발생했습니다. 이번 릴리스를 통해 CCO에서는 배포가 비정상적인지 여부를 더이상 보고하지 않습니다. (BZ#1957424)

Cluster Version Operator

- 이전 버전에서는 Cluster Version Operator가 **cluster_operator_up** 메트릭을 설정할 때 **Available** 및 **Degraded** 매개변수를 모두 평가하여 **Available=True**가 "has not been available"의 경고 설명과 일치하지 않더라도 **Available=True** 또는 **Degraded=True**를 사용하여 Operator에 대해 **ClusterOperatorDown** 경고가 표시되었습니다. 이번 수정으로 Cluster Version Operator는 이제 **cluster_operator_up** 메트릭을 설정할 때 **Degraded** 매개변수를 무시합니다. (BZ#1834551)

- 이전 버전에서는 Prometheus가 클러스터에 설치될 때 중요한 플랫폼 토폴로지 메트릭을 사용할

수 없었으며 호출자로 생성된 설치 프로그램 메트릭을 ""로 설정하면 CI 오류가 발생했습니다. 오류를 유발하는 메트릭이 제공되기 전에 정보를 동기화하지 않은 경우 가능한 경합 조건이 수정되었습니다. (BZ#1871303)

- 이전 버전에서는 Cluster Version Operator의 자체 배포와 같이 동일한 키에 대한 허용 오차가 있는 여러 매니페스트에서 마지막 항목 읽기 및 이전 항목 덮어쓰기만 허용했습니다. 이로 인해 **in-cluster tolerations**이 매니페스트의 나열된 허용 오차와 달랐습니다. 이번 업데이트를 통해 이제 Cluster Version Operator가 완전히 동일한 경우 허용 오차가 일치하는 것으로 간주합니다. 이를 통해 Cluster Version Operator는 **in-cluster resource**의 매니페스트에 모든 허용 오차를 표시할 수 있습니다. (BZ#1941901)

- 이전에는 Cluster Version Operator가 이러한 속성을 설정하지 않은 매니페스트에 대해 **env** 및 **envFrom**을 조정하지 않았습니다. 이는 Cluster Version Operator가 컨테이너 환경을 제대로 관리하지 못했음을 의미합니다. 이번 업데이트에서는 Cluster Version Operator가 개선되어 이제 매니페스트에 설정되지 않은 경우 **env** 및 **envFrom**을 지웁니다. 이를 통해 클러스터는 잘못된 **cluster-admin** 변경 사항에서 이러한 속성을 자동으로 복구할 수 있습니다. (BZ#1951339)

- 이전 버전에서는 **cluster-version-operator** 배포 오브젝트와 같이 동일한 키에 대한 허용 오차가 있는 여러 매니페스트에서 마지막 항목 읽기 및 이전 항목 덮어쓰기만 허용했습니다. 이로 인해 클러스터내 허용 오차가 매니페스트의 나열된 허용 오차와 달랐습니다. 이번 업데이트를 통해 이제 Cluster Version Operator는 허용 오차가 동일할 때 일치하는 것으로 간주합니다. 이를 통해 Cluster Version Operator는 클러스터내 리소스의 매니페스트에 모든 허용 오차를 표시할 수 있습니다. (BZ#1941901)

- 이전에는 **ClusterOperator** 리소스가 10분 동안 성능이 저하될 때 Cluster Version Operator에서 **ClusterOperatorDegraded** 경고를 보고했습니다. 이는 리소스가 아직 생성되고 있기 때문에 설치 중에 이 경고가 중간에 발생되는 경우가 있었습니다. 이번 업데이트에서는 10분 기간을 30분으로 변경하여 조기 **ClusterOperatorDegraded** 경고 없이 설치가 진행될 수 있는 충분한 시간이 제공됩니다. (BZ#1957991)

Compliance Operator

- 이전 버전에서는 사용자가 규정 준수 확인을 실행할 때 **NON-COMPLIANT** 결과가 제공되었지만 사용자가 조치를 취해야 하는 해결 단계는 표시되지 않았습니다. 이번 릴리스에서는 사용자가 규칙을 확인하는 데 필요한 단계를 검토할 수 있는 **instructions** 키를 제공합니다. 이를 통해 사용자와 감사자는 Operator가 올바른 값을 확인하고 있는지 확인할 수 있습니다. (BZ#1919367)

콘솔 Kubevirt 플러그인

- 이전 버전에서는 사용자가 가상화 템플릿에 부팅 소스를 추가할 수 있는 웹 콘솔 양식에서 설명 텍스트는 템플릿이 사용된 운영 체제와 관계없이 Fedora에 대한 정보를 제공했습니다. 이번 업데이트에서는 템플릿의 운영 체제와 관련된 예를 제공하는 수정 사항을 추가하여 사용자에게 관련 지침을 제공합니다. (BZ#1908169)

- 이전 버전에서는 사용자가 가상 머신 템플릿을 생성하는 데 도움이 되는 웹 콘솔 마법사에서 부정확한 언어로 인해 작업이 템플릿에 적용되었는지 또는 가상 머신에 적용되었는지 알 수 없었습니다. 이번 수정에서는 사용자가 정보에 입각한 결정을 내릴 수 있도록 명확하게 설명합니다. (BZ#1922063)

- 이전에는 웹 콘솔의 모호한 오류 메시지로 인해 템플릿에서 생성 중인 가상 머신에 네트워크 인터페이스를 추가하려는 일부 사용자에게 불필요한 혼동이 발생했습니다. 이번 업데이트에서는 오류 메시지에 세부 정보를 추가하여 사용자가 오류 문제를 보다 쉽게 해결할 수 있도록 합니다. (BZ#1924788)

- 이전에는 웹 콘솔의 RHEL(Red Hat Enterprise Linux) 6 템플릿에서 가상 머신을 생성하려고 하면 RHEL 6을 통해 지원 수준을 정의하는 방법에 대한 정보가 팝업 창에 표시되었습니다. 이번 수정을 통해 이 창의 텍스트가 변경되어 RHEL 6이 지원되지 않습니다. (BZ#1926776)

- 이전에는 웹 콘솔의 드롭다운 목록이 버튼 요소에 의해 가려져 사용자가 가상 시스템을 생성할 때 특정 운영 체제를 선택할 수 없었습니다. 이번 수정에는 오류를 수정하고 사용자가 사용 가능한 운영 체제를 선택할 수 있는 버튼 요소의 **z-index** 값을 조정하는 작업이 포함되어 있습니다. (BZ#1930015)

- 이전에는 스토리지 클래스가 정의되지 않은 클러스터에서 웹 콘솔의 새 가상 시스템 마법사를 사용한 경우 웹 콘솔이 무한 루프에 묶여 충돌했습니다. 이번 수정을 통해 스토리지 클래스가 정의되지 않은 인스턴스의 스토리지 클래스 드롭다운 목록이 제거됩니다. 결과적으로 웹 콘솔이 충돌하지 않습니다. (BZ#1930064)

- 이전에는 버튼 요소의 텍스트가 즐겨찾기 목록에서 VM 템플릿을 제거하는 버튼의 기능을 명확하게 설명하지 않았습니다. 이번 수정을 통해 버튼의 기능을 명확히 설명하는 텍스트가 업데이트되었습니다. (BZ#1937941)

- 이전에는 **RerunOnFailure** 실행 전략이 있는 가상 시스템의 경우 가상 시스템을 중지하면 여러 UI 요소가 응답하지 않아 사용자가 상태 정보를 읽거나 가상 시스템을 다시 시작할 수 없었습니다. 이번 업데이트에서는 사용자가 이러한 기능을 사용할 수 있도록 응답하지 않는 요소가 수정되었습니다. (BZ#1951209)

- 이전 버전에서는 별도의 **/var** 파티션을 포함하도록 구성된 클러스터의 경우 파일 시스템을 쿼리하는 경우 **/var** 파티션 크기를 제외하고 루트 디렉터리에 마운트된 디스크 크기만 반환했습니다. 이번 수정으로 쿼리 실행 방식이 변경되어 사용자가 클러스터에서 파일 시스템의 총 크기를 확인할 수 있습니다. (BZ#1960612)

콘솔 스토리지 플러그인

- 이전 버전에서는 올바른 스토리지 클래스를 사용할 수 없는 경우 OpenShift Container Storage Operator에 오류 메시지가 표시되었습니다. 이번 업데이트에서는 오류 메시지를 제거하고 올바른 스토리지 클래스를 사용할 수 있을 때까지 **다음** 버튼을 비활성화합니다. (BZ#1924641)

- 이전 버전에서는 사용자가 내부 연결 스토리지 클러스터를 생성하는 동안 브라우저의 뒤로 버튼을 클릭하면 설치 마법사에서 프로세스가 다시 시작되었습니다. 이번 업데이트에서는 문제가 해결되었습니다. (BZ#1928008)

- 로컬 볼륨 검색에 노드를 추가하면 기존 노드 목록이 표시되므로 불필요한 탐색이 줄어듭니다. (BZ#1947311)

- 이전에는 **스토리지 클러스터 생성** 마법사를 통해 정의되지 않은 값이 있는 중재자 영역을 활성화할 수 있었습니다. 이번 업데이트에서는 정의되지 않은 값을 필터링하므로 중재자 영역을 정의된 값으로만 만들 수 있습니다. (BZ#1926798)

- 이전 버전에서는 제품 제목의 철자와 등록된 상표 기호의 사용 방법이 일치하지 않아 웹 콘솔에웹 콘솔에 퀵 스타트 카드가 잘못 표시되었습니다. 이번 업데이트에서는 제품 이름이 올바르게 지정되어 있으며 등록된 상표 기호가 첫 번째 카드에만 일관되게 표시됩니다. (BZ#1931760)

DNS

- 이전 버전에서는 BZ#1936587에서 글로벌 CoreDNS 캐시 최대 TTL을 900초로 설정했습니다. 그 결과 업스트림 리졸버에서 수신된 NXDOMAIN 레코드가 900초 동안 캐시되었습니다. 이번 업데이트를 통해 최대 30초 동안 음수 DNS 응답 레코드를 명시적으로 캐시합니다. 결과적으로 NXDOMAINs가 더 이상 900초 동안 캐시하지 않습니다. (BZ#1943578)

- BZ#1953097 의 수정으로 CoreDNS **bufsize** 플러그인이 1232바이트인 CoreDNS bufsize 플러그인을 활성화했습니다. 일부 기본 DNS 확인자는 UDP에서 512바이트를 초과하는 DNS 응답 메시지를 수신할 수 없습니다. 결과적으로 Go의 내부 DNS 라이브러리와 같은 일부 DNS 확인자는

DNS Operator에서 자세한 DNS 응답을 받을 수 없습니다. 이번 업데이트에서는 모든 서버에 대해 CoreDNS **bufsize**를 512바이트로 설정합니다. 그 결과 UDP DNS 메시지가 올바르게 수신됩니다. (BZ#1966116)

- 이전 버전에서는 클러스터 업스트림 리졸버에서 UDP를 통해 512 바이트를 초과하는 DNS 응답을 반환했습니다. 그 결과 coreDNS에서 **SERVFAIL** 또는 기타 오류 메시지를 반환하고 클라이언트가 TCP를 다시 시도하도록 했습니다. 이번 업데이트에서는 UDP 버퍼 크기가 1232바이트인 coreDNS bufisze 플러그인을 활성화했습니다. (BZ#1949361)

etcd

- 이전에는 etcd Operator에 전송 누수가 발생하여 시간이 지남에 따라 메모리 사용량이 증가했습니다. 메모리 누수가 수정되었습니다. (BZ#1925586)

- 이전에는 **etcdInsufficientMembers** 경고가 잘못 실행되었습니다. 이번 릴리스에서는 인스턴스 레이블 외에도 pod 레이블을 포함하도록 경고가 업데이트되어 쿼럼이 유실된 경우에만 경고가 실행됩니다. (BZ#1929944)

- 이전 버전에서는 SO_REUSEADDR 소켓 옵션이 도입되어 준비 상태 프로브가 올바른 준비 상태를 보고하지 않아 etcd Pod가 etcd-quorum-guard에 실패하더라도 etcd pod가 준비 상태로 표시되었습니다. 이러한 옵션을 고려하여 준비 상태 프로브 검사가 업데이트되었으며 etcd 준비 상태 프로브가 이제 피연산자의 준비 상태를 올바르게 반영합니다. (BZ#1946607)

- 이전에는 **spec.loglevel** 필드에서 etcd 피연산자에 **log-level** 플래그를 설정하지 않았으므로 사용자가 etcd 로그 수준을 변경할 수 없었습니다. 이제 사용자는 다음과 같이 로그 수준을 설정할 수 있습니다.

  - **Debug**, **Trace**, **TraceAll** 로그 수준이 etcd **debug** 로그 수준에 매핑됩니다.
  - **default** 또는 **Normal** 로그 수준은 etcd **info** 로그 수준에 매핑됩니다.

  자세한 내용은 BZ#1948553에서 참조하십시오.

- 이전 버전에서는 etcd 프로세스에 따라 관련 포트가 릴리스될 때까지 다음 프로세스가 시작되지 않았습니다. 이 프로세스에 **SO_REUSEADDR**을 추가하면 포트를 즉시 재사용할 수 있습니다. 자세한 내용은 BZ#1927942에서 참조하십시오.

- 이전 버전에서는 **network.Status.ServiceNetwork** 필드가 채워지지 않은 경우 etcd-endpoint의 ConfigMap이 비어 있었습니다. 이로 인해 etcd Operator를 확장할 수 없었습니다. OpenShift Container Platform 4.8의 새로운 기능을 사용하면 **network.Status.ServiceNetwork** 필드가 채워지지 않을 때 etcd Operator를 확장할 수 있습니다. (BZ#1902247)

이미지 레지스트리

- 이전에는 이미지를 삭제하지 못할 때 이미지 정리기가 중지되었습니다. 결과적으로 두 이미지 정리기가 동시에 이미지를 삭제하려고 하면 둘 중 하나가 **not found** 오류로 실패했습니다. 이번 업데이트를 통해 **not found** 오류가 무시되어 이미지 정리기가 동시 삭제를 허용할 수 있습니다. (BZ#1890828)

- 이전 버전에서는 Image Registry Operator 상태 평가 중에 경로 상태 포함 부족으로 인해 성능이 **degraded** 상태의 경로가 있더라도 Image Registry Operator의 성능이 저하되지 않았습니다. 이번 수정을 통해 이미지 레지스트리 Operator에서 구성된 모든 경로를 가져와서 자체 상태를 평가할 때 해당 상태를 평가합니다. 이번 업데이트를 통해 **degraded** 경로가 있는 경우 이미지 레지스트리 Operator는 오류 메시지와 함께 **degraded**로 보고합니다. (BZ#1902076)

- 이전에는 자동으로 생성된 Docker 구성 보안에 통합된 내부 레지스트리 경로에 대한 인증 정보가 포함되지 않았습니다. 경로를 통해 레지스트리에 액세스하는 데 필요한 인증 정보가 없기 때문에

pod는 인증 부족으로 인해 레지스트리에 연결하지 못했습니다. 이번 수정 사항에는 기본 Docker 인증 정보 시크릿에 구성된 모든 레지스트리 경로가 포함됩니다. 이제 인증 정보에 각 경로에 대한 항목이 포함되어 있으므로 pod는 모든 경로에서 통합 레지스트리에 연결할 수 있습니다. (BZ#1911470)

- 이전에는 이미지 레지스트리가 클러스터 전체 ICSP(**ImageContentSourcePolicy**) 규칙을 무시했습니다. pull-through 중에 이미지 미러가 무시되어 연결이 끊긴 클러스터에서 풀링 오류가 발생했습니다. 이번 업데이트를 통해 대상 저장소에 ICSP 규칙이 있는 경우 레지스트리에서 미러를 가져옵니다. 결과적으로 구성된 미러에서 이미지를 가져오는 데 실패하지 않습니다. (BZ#1918376)

- 이전에는 Image Registry Operator가 구성 리소스의 **.status.readyReplicas** 필드를 업데이트하지 않았으므로 해당 값은 항상 **0** 이었습니다. 이번 수정으로 Image Registry Operator는 배포의 준비된 이미지 레지스트리 복제본 수를 구성에 기록합니다. 이제 이 필드에 준비된 이미지 레지스트리 복제본 수가 표시됩니다. (BZ#1923811)

- Azure는 사용자가 **v1** 대신 Storage Accounts **v2**를 사용하는 것을 권장합니다. 특정 보안 프로필에서 관리자는 Azure가 **v1** 스토리지 계정 생성을 수락하지 않도록 할 수 있습니다. 이미지 레지스트리는 **v1** 스토리지 계정에 따라 다르기 때문에 이러한 환경에서 클러스터 설치에 실패합니다. 이번 수정으로 클러스터 부트스트랩 중에 Image Registry Operator에서 **V2** 스토리지 계정을 생성하고 사용하려고 시도합니다. **v1**에서 실행되는 클러스터는 계속해서 **V1** 스토리지 계정을 사용합니다. 설치에 성공하고 Image Registry Operator에서 **Available**을 보고합니다. (BZ#1929654)

ImageStreams

- 이전에는 스트림에서 여러 이미지를 가져올 때 성능이 저하된 경우가 있었습니다. 이번 릴리스에서는 이미지 레지스트리에 대한 동시 요청 수가 5개에서 50개로 증가하여 성능이 향상됩니다. (BZ#1954715)

Insights Operator

- 이전에는 Insights Operator에서 **openshift-cluster-version** 네임스페이스에서 CVO(Cluster Version Operator) Pod 또는 이벤트를 수집하지 않았습니다. 그 결과 Insights Operator는 CVO가 경험할 수 있는 문제에 대한 정보를 표시하지 않았으며 사용자가 CVO에 대한 진단 정보를 가져올 수 없었습니다. 이제 Insights Operator가 CVO pod 및 이벤트를 **openshift-cluster-operator** 네임스페이스에서 수집하여 CVO 관련 문제를 보고하도록 업데이트되었습니다. (BZ#1942271)

설치 프로그램

- 이전에는 IPv6 네트워크가 /64가 아닌 경우 접두사 길이를 DNSmasq로 지정해야 했습니다. 이로 인해 컨트롤 플레인 호스트가 PXE 부팅에 실패했습니다. 이번 업데이트에는 DNSmasq 구성의 서브넷 접두사 길이가 포함됩니다. 결과적으로 컨트롤 플레인 호스트는 접두사 길이의 IPv6 네트워크에서 DHCP 및 PXE 부팅됩니다. (BZ#1927068)

- vSphere에 설치할 때 부트스트랩 머신이 **/etc/resolv.conf** 파일의 이름 서버를 올바르게 업데이트하지 않은 경우가 있었습니다. 이로 인해 부트스트랩 시스템이 임시 컨트롤 플레인에 액세스할 수 없어 설치에 실패했습니다. 이번 수정에서는 보다 안정적인 업데이트를 위한 올바른 행을 찾는 데 필요한 변경 사항이 포함되어 있습니다. 이제 부트스트랩 관리자가 임시 컨트롤 플레인에 액세스할 수 있으므로 설치에 성공할 수 있습니다. (BZ#1967355)

- 이전에는 설치 프로그램에서 URL을 생성할 때 부트스트랩 Ignition 구성이 있어야 하는 리전을 고려하지 않았습니다. 결과적으로 부트스트랩 머신이 올바르지 않았기 때문에 제공된 URL에서 구성을 가져올 수 없었습니다. 이번 업데이트에서는 URL을 생성할 때 사용자의 리전을 고려하여 올바른 공용 엔드포인트를 선택합니다. 결과적으로 설치 프로그램에서 항상 올바른 부트스트랩 Ignition URL을 생성합니다. (BZ#1934123)

- 이전 버전에서는 스토리지 계정을 만들 때 Azure의 최소 TLS의 기본 버전이 1.0이었습니다. 그 결

과 정책 검사에 실패했습니다. 이번 업데이트에서는 스토리지 계정을 생성할 때 Minimum TLS 버전을 1.2로 설정하도록 openshift-installer Azure 클라이언트를 구성합니다. 결과적으로 정책 검사를 통과합니다. (BZ#1943157)

- 이전에는 Azure에서 IPI를 사용하여 배포된 프라이빗 클러스터에 부트스트랩 노드에 SSH를 허용하는 인바운드 NSG 규칙이 있었습니다. 이 허용으로 Azure의 보안 정책을 트리거할 수 있습니다. 이번 업데이트를 통해 NSG 규칙이 제거되었습니다. (BZ#1943219)

- 이전에는 설치 프로그램이 **ap-northeast-3** AWS 리전을 인식하지 못했습니다. 이번 업데이트를 통해 설치 프로그램에서 알려진 파티션의 패턴에 맞는 알 수 없는 지역에 설치할 수 있으므로 사용자가 **ap-northeast-3** AWS 리전에 인프라를 생성할 수 있습니다. (BZ#1944268)

- 이전 버전에서는 온프레미스 플랫폼에 내부 로드 밸런서 장치를 만들 수 있는 기능이 없었습니다. 이번 업데이트를 통해 사용자가 매니페스트를 생성할 때 이 전략이 AWS, Azure 및 GCP와 같은 클라우드 플랫폼에서만 사용되는지 확인하는 검사가 추가되었습니다. (BZ#1953035)

- 이전 버전에서는 Google Cloud Platform 리소스의 이름을 지정할 때 필터로 인해 **Google**이라는 단어를 사용하는 특정 이름을 사용할 수 없었습니다. 이번 업데이트에서는 클러스터 이름에 설치 프로그램에 추가되어 이름을 설정할 때 Google이라는 단어의 일부 변형을 사용할 수 있습니다. (BZ#1955336)

- 이전에는 설치 관리자 프로비저닝 인프라가 있는 베어 메탈 설치에서 설치 프로그램 프로세스가 프로비저닝 네트워크와 통신할 수 있어야 했습니다. 이제 설치 프로그램 프로세스에서 API 서버의 가상 IP와 통신할 수 있습니다. 이번 변경으로 인해 프로비저닝 네트워크가 라우팅할 수 없고 설치 프로그램 프로세스가 RHOSP(Red Hat OpenStack Platform) 또는 Red Hat Advanced Cluster Management와 같은 원격 위치에서 실행될 수 있습니다. API 서버의 가상 IP에서 TCP 포트 **6385** 및 **5050**과 통신할 수 있도록 방화벽 규칙을 조정해야 할 수도 있습니다. (BZ#1932799)

- 이전에는 RHOSP(Red Hat OpenStack Platform)에 설치할 때 **platform.openstack.machinesSubnet** 필드에 없는 서브넷 ID가 제공되면 **openshift-install** 명령에서 SIGSEGV 및 역추적이 생성되었습니다. 이제 다음 메시지와 같은 오류가 생성되도록 **openshift-install** 명령이 수정되었습니다.

  ```
  FATAL failed to fetch Metadata: failed to load asset "Install Config":
  platform.openstack.machinesSubnet: Not found: "<network-ID>"
  ```

  (BZ#1957809)

- 이전에는 RHOSP HTTPS 인증서를 호스팅 장치로 가져오지 않은 한 RHOSP(Red Hat OpenStack Platform)의 설치에 실패했습니다. 이제 **cloud.yaml**의 **cacert** 값이 RHOSP HTTPS 인증서로 설정된 경우 설치가 성공적으로 수행됩니다. 더 이상 인증서를 호스트에 가져올 필요가 없습니다. (BZ#1786314)

- 이전에는 **proxy.config.openshift.io**의 외부 네트워크 항목이 부정확하여 설치에 실패할 수 있었습니다. 이제 유효성 검사를 통해 수정을 활성화하기 위한 부정확한 정보가 식별됩니다. (BZ#1873649)

- 이전에는 모호하거나 혼란스러웠던 Terraform 구성 요소에 대한 설명이 이제는 더 명확한 정보로 대체되었습니다. (BZ#1880758)

- 이전 gophercloud/utils 변경에 자체 서명된 인증서를 사용하는 사용자 지정 HTTP 클라이언트가 도입되었습니다. 이러한 변경으로 프록시 환경 변수에 대한 설정을 포함하여 **DefaultTransport**에서 제거된 설정으로 인해 자체 서명 인증서와 프록시를 모두 사용한 설치에 오류가 발생했습니다. 이번 업데이트에서는 사용자 정의 HTTP 클라이언트가 **DefaultTransport**의 설정을 상속하므로 이제 자체 서명된 인증서 및 프록시를 사용하여 OpenShift Container Platform을 설치할 수 있습니다. (BZ#1925216)

- 이전 버전에서는 설치 프로그램이 검증 중에 설치 구성의 **defaultMachineSet** 값을 고려하지 않아 설치 프로그램이 실패했습니다. 이번 업데이트에서는 기본값을 설치 구성에 적용하고 빈 필드의 유효성을 검사하기 시작합니다. (BZ#1903055)

- 이전에는 **soft-anti-affinity**에 클라이언트에서 최소 Nova 마이크로버전을 설정해야 했습니다. 대부분의 Ansible OS 서버 모듈 버전에서는 클라이언트가 최소 값을 자동으로 설정하지 않아도 되었습니다. 결과적으로 soft-anti-affinity 명령이 실패할 가능성이 있었습니다. 이번 업데이트에서는 소프트 방지를 처리할 때 Python OpenStack 클라이언트를 사용하여 Nova 마이크로버전을 설정하는 작업이 수정되었습니다. (BZ#1910067)

- 이전에는 OpenStack UPI 플레이북에서 생성된 모든 리소스에 태그를 지정하지 않았습니다. 그 결과 **openshift-install destroy** 명령이 모든 클러스터 리소스를 올바르게 식별하지 못하고 시간 초과에 도달할 때까지 리소스 삭제를 반복하여 리소스가 남아 있게 되었습니다. 이번 업데이트에서는 OpenStack UPI 플레이북에 누락된 태그 지침이 추가되었습니다. (BZ#1916593)

- 이전에 **e2e-gcp-upi** Python 패키지 오류로 인해 실패했습니다. 이번 업데이트를 통해 gsutil에 대해 올바른 Python 버전, pip 버전 및 **CLOUDSDK_PYTHON**을 설정하여 패키지 오류를 해결할 수 있습니다. (BZ#1917931)

- 이전 버전에서는 pip 버전 21이 설치된 Python 버전 2를 지원하지 않았습니다. 이로 인해 컨테이너 설정에 필요한 모든 종속 패키지를 확인하는 중에 오류가 발생했습니다. 이번 업데이트에서는 문제를 피하기 위해 pip 버전이 21보다 작은 값으로 수정되었습니다. (BZ#1922235)

- 이전에는 설치 프로그램이 클라우드에 대한 정보를 두 번 수집했습니다. 그 결과 OpenStack API에 대한 요청 수가 두 배로 늘어났습니다. 이로 인해 클라우드에 추가 로드가 발생하고 설치 시간이 늘어났습니다. 이번 업데이트에서는 할당량을 확인하기 전에 클라우드에 대한 정보를 수집하여 문제를 해결한 다음 검증을 위해 동일한 정보를 재사용합니다. (BZ#1923038)

- 이전 버전에서는 /64 이외의 서브넷을 사용하여 IPv6 프로비저닝 네트워크를 배포할 때 DNSmasq는 접두사 길이를 지정해야 했습니다. 따라서/64 이외의 네트워크를 사용할 때 호스트가 PXE 부팅에 실패했습니다. 이번 업데이트에는 DNSmasq 구성의 접두사 길이가 포함됩니다. 결과적으로 호스트는 접두사 길이의 IPv6 네트워크에서 DHCP 및 PXE 부팅에 성공합니다. (BZ#1925291)

- 이전 버전에서는 로깅이 제거되었다고 표시했지만 OpenShift Container Platform 설치 프로그램에서 **Shared Subnet** 태그를 제거할 때 IAM 권한 문제를 보고하지 않았습니다. 이번 업데이트에서는 결과에 태그 해제 및 로깅 오류가 있는지 확인합니다. 이제 로그에 공유 리소스 태그 해제의 상태가 표시됩니다. (BZ#1926547)

- 이전에는 Premium_LRS 디스크 유형을 사용하여 Azure 클러스터가 생성되었으며 PremiumIO 기능을 지원하지 않는 인스턴스 유형으로 클러스터가 실패했습니다. 이번 업데이트에서는 선택한 인스턴스 유형에 디스크 유형이 기본 디스크 유형인 Premium_LRS인 PremiumIO 기능이 있는지 확인합니다. 코드는 Azure 서브스크립션 및 리전을 쿼리하여 필요한 정보를 가져오고 조건이 충족되지 않는 경우 오류를 반환합니다. (BZ#1931115)

- 이전에는 API 서버가 다시 시작될 때 부트스트랩에서 API VIP를 사용할 수 없게 되어 프로비저닝 서비스를 사용할 수 없게 되고 프로비저닝에 실패했습니다. 이제 프로비저닝 서비스(Ironic)가 VIP 상태 점검에 포함되고, API VIP를 계속 사용할 수 있습니다. (BZ#1949859)

kube-apiserver

- 이전에는 GCP(Google Cloud Platform) 로드 밸런서 상태 검사기에서 호스트의 오래된 conntrack 항목을 남겨 두었으며 이로 인해 GCP 로드 밸런서를 사용하는 API 서버 트래픽에 대한 네트워크 중단이 발생했습니다. 상태 검사 트래픽이 호스트를 통해 더 이상 반복되지 않으므로 API 서버에 대한 네트워크 중단이 더 이상 발생하지 않습니다. (BZ#1925698)

Machine Config Operator

- 이전에는 **drain timeout** 및 풀 성능저하 기간이 너무 짧고 더 많은 시간이 필요한 일반 클러스터에서 경고가 조기에 발생할 수 있었습니다. 이번 업데이트를 통해 시간 초과가 오류를 보고하는 데 필요한 시간이 연장됩니다. 이를 통해 일반 클러스터의 성능이 저하되지 않고 Cluster Operator에게 더 실용적이고 유용한 경고가 제공됩니다. (BZ#1968019)

- 이전에는 IPI(OpenShift Installer Provisioned Infrastructure)를 사용하여 VMware vSphere에서 새 가상 시스템을 생성하는 동안 노드가 클러스터에 참여하지 못했습니다. 이러한 문제는 DHCP(Dynamic Host Configuration Protocol)가 IDI에서 제공하는 이름 대신 호스트 이름을 입력할 때 발생했습니다. 이 문제가 해결되었습니다. (BZ#1920807)

- 이전에는 호스트 이름을 설정하기 전에 네트워크를 활성화하면 설치에 실패할 수 있었습니다. 이로 인해 노드가 클러스터에 참여하지 못하고 다른 시도를 수행하기 전에 5분 정도 지연되었습니다. 이제 이 문제가 해결되고 노드가 첫 번째 시도 중에 클러스터에 자동으로 참여합니다. (BZ#1899187)

- 이전에는 키가 남아 있어도 코어 사용자 및 관련 SSH 키를 삭제할 수 있었습니다. 이번 업데이트를 통해 사용자는 코어 사용자를 삭제할 수 없습니다. (BZ#1885186)

- 4.6에서 4.7로 업그레이드할 때 **vsphere-hostname** 서비스에서 설정한 호스트 이름은 노드가 설치된 경우에만 적용되었습니다. 업그레이드하기 전에 호스트 이름이 정적으로 설정되지 않은 경우 호스트 이름이 손실되었을 수 있습니다. 이번 업데이트에서는 노드가 설치된 경우에만 **vsphere-hostname** 서비스가 실행될 수 있는 조건을 제거합니다. 따라서 업그레이드 시 vSphere 호스트 이름이 손실되지 않습니다. (BZ#1942207)

- **keepalived** 2.0.10 버그로 인해 활성 프로브에서 **keepalived** 컨테이너가 삭제된 경우 시스템에 할당된 모든 가상 IP 주소(VIP)는 그대로 유지되고 **keepalived**가 다시 시작할 때 정리되지 않았습니다. 이로 인해 여러 노드가 동일한 VIP를 보유할 수 있었습니다. 이제 **keepalived**가 시작될 때 VIP가 제거됩니다. 결과적으로 VIP는 단일 노드에 의해 보유됩니다. (BZ#1931505)

- 이전에는 RHCOS(Red Hat Enterprise Linux CoreOS)와 같은 비CoreOS 노드에서 rpm-ostree 관련 작업이 제대로 처리되지 않았습니다. 결과적으로 커널 전환과 같은 작업이 RHEL 노드를 포함하는 풀에 적용되면 RHEL 노드 성능이 저하되었습니다. 이번 업데이트를 통해 Machine Config Daemon은CoreOS 노드에서 지원되지 않는 작업이 수행될 때마다 메시지를 로깅합니다. 메시지를 기록한 후 오류 대신 nil을 반환합니다. 이제 풀의 RHEL 노드는 머신 구성 데몬에서 지원되지 않는 작업을 수행할 때 예상대로 진행됩니다. (BZ#1952368)

- 이전에는 비어 있는 정적 pod 파일이 **/etc/kubernetes/manifests** 디렉터리에 작성되었습니다. 이로 인해 kubelet 로그에서 일부 사용자와 혼동을 일으킬 수 있는 오류를 보고했습니다. 빈 매니페스트는 이제 필요하지 않은 경우 다른 위치로 이동합니다. 이로 인해 kubelet 로그에 오류가 표시되지 않습니다. (BZ#1927042)

Metering Operator

- 이전 버전에서는 Reporting Operator에서 이벤트 조정 시 사용자 제공 보존 기간이 포함된 **Report** CR(사용자 정의 리소스)을 잘못 처리했습니다. 결과적으로 영향을 받는 사용자 정의 리소스가 무기한 다시 큐에 추가되므로 만료된 **Report** CR로 인해 Reporting Operator가 계속 반복됩니다. 이번 업데이트에서는 보존 기간을 지정한 만료된 **Report** CR을 다시 큐에 추가하지 않습니다. 결과적으로 Reporting Operator는 만료된 **Report** CR에 대한 이벤트를 올바르게 처리합니다. (BZ#1926984)

모니터링

- 이전에는 **node-exporter** daemontset의 **mountstats** 수집기로 인해 NFS 마운트 지점이 있는 노드에서 메모리 사용량이 증가했습니다. 이번 업데이트를 통해 이제 사용자가 **mountstats** 수집기를 비활성화하여 메모리 사용량을 줄일 수 있습니다. (BZ#1955467)

네트워킹

- 이전 버전에서는 잘못된 **keepalived** 설정으로 인해 VIP가 잘못된 시스템으로 종료되어 올바른 시스템으로 다시 이동할 수 없었습니다. 이번 업데이트를 통해 VIP가 올바른 시스템에 종료되도록 잘못된 **keepalived** 설정이 제거됩니다. (BZ#1916890)

- iptables 재작성 규칙으로 인해 서비스 IP와 pod IP를 통해 고정 소스 포트를 사용하여 서비스에 연결하는 클라이언트가 포트 충돌과 관련된 문제가 발생할 수 있습니다. 이번 업데이트를 통해 추가 OVS 규칙을 삽입하여 포트 충돌이 발생하는 시점을 파악하고 추가 SNAT을 수행하여 해당 충돌을 방지합니다. 따라서 서비스에 연결할 때 더 이상 포트 충돌이 발생하지 않습니다. (BZ#1910378)

- 이전 버전에서는 컨트롤 플레인 노드와 송신 할당 노드 간의 IP 포트 9가 내부 방화벽에 의해 차단되었습니다. 이로 인해 IP 주소가 할당되지 않아 송신 노드가 실패했습니다. 이번 업데이트에서는 IP 포트 9를 통해 컨트롤 플레인 노드와 송신 노드 간 액세스를 활성화합니다. 결과적으로 송신 노드에 IP 주소 할당이 성공적으로 허용됩니다. (BZ#1942856)

- 이전에는 더 이상 유효하지 않은 연결 추적 항목으로 인해 UDP 서비스 트래픽이 차단될 수 있었습니다. **NodePort** 서비스에 대해 서버 pod가 사이클링된 후 pod에 대한 액세스가 제한되었습니다. 이번 업데이트를 통해 **NodePort** 서비스 사이클링의 경우 연결 추적 항목이 제거되어 새 네트워크 트래픽이 사이클된 엔드포인트에 도달할 수 있습니다. (BZ#1949063)

- 이전에는 OVN-Kubernetes 네트워크 공급자가 여러 **ipBlocks**가 있는 네트워크 정책을 무시했습니다. 첫 번째 항목을 무시한 후 모든 ipBlock을 수행하면 Pod가 구성된 모든 IP 주소에 연결할 수 없습니다. Kubernetes 네트워크 정책에서 OVN ACL을 생성하는 코드가 수정되었습니다. 결과적으로 여러 **ipBlocks**이 있는 네트워크 정책이 올바르게 작동합니다. (BZ#1953680)

- 이전에는 OVN-Kubernetes 클러스터 네트워크 공급자를 사용할 때 엔드포인트가 없는 Kubernetes 서비스가 잘못된 연결을 수락했습니다. 이번 업데이트를 통해 엔드포인트가 없는 서비스에 대해 더 이상 로드 밸런서가 생성되지 않으므로 트래픽이 더 이상 허용되지 않습니다. (BZ#1918442)

- 이전에는 Multus의 CNI(Container Network Interface) 플러그인이 0으로 시작된 IPv6 주소를 인식하지 못했습니다. 이번 업데이트를 통해 CNI 플러그인은 0보다 큰 값으로 시작하는 IPv6에서 작동합니다. (BZ#1919048)

- 이전에는 머신 구성 정책 변경에 의해 재부팅이 트리거될 때 SR-IOV Network Operator가 재부팅을 시작하면 경쟁 조건이 트리거될 수 있었습니다. 이 경우 노드가 결정되지 않은 상태로 남아 있었습니다. 이번 업데이트를 통해 이러한 상황을 피할 수 있습니다. (BZ#1921321)

- 이전에는 Kuryr 클러스터 네트워크 공급자를 사용하여 새 사용자 프로비저닝 클러스터를 생성할 때 클러스터 노드에서 사용하는 OpenStack 하위 집합이 검출되지 않아 클러스터 설치 시간이 초과될 수 있었습니다. 이번 업데이트를 통해 서브넷이 올바르게 감지되고 사용자가 프로비저닝한 설치가 성공적으로 수행됩니다. (BZ#1927244)

- 이전 버전에서는 OpenShift Container Platform 4.6에서 OpenShift Container Platform 4.7으로 업그레이드할 때 CNO(Cluster Network Operator)가 다음 버전으로 업그레이드를 완료한 것으로 잘못 표시되었습니다. 이후 업그레이드에 실패한 경우 CNO는 자체적으로 **degraded**으로 보고되었지만 버전 4.7로 잘못 보고되었습니다. 이번 업데이트를 통해 CNO는 클러스터 네트워크 제공자 이미지가 성공적으로 업그레이드될 때까지 기다린 후 CNO 업그레이드를 성공한 것으로 보고합니다. (BZ#1928157)

- 이전 버전에서는 OVN-Kubernetes 클러스터 네트워크 공급자를 사용하는 경우 Kubernetes 버전에 영숫자가 아닌 마이너 버전이 포함된 경우 엔드포인트 슬라이스 컨트롤러가 실행되지 않을 수 있었습니다. 이 업데이트를 설치하면 엔드포인트 슬라이스 컨트롤러가 기본적으로 활성화됩니다. (BZ#1929314)

- Kuryr 클러스터 네트워크 공급자를 사용하는 경우 설치 후 생성된 Neutron 포트의 이름은 설치 중에 생성된 Neutron 포트와 다른 패턴으로 이름이 지정되었습니다. 결과적으로 설치 후 생성된

Neutron 포트가 기본 로드 밸런서에 추가되지 않았습니다. 이번 업데이트를 통해 Kuryr는 두 명명 규칙을 사용하여 생성된 Neutron 포트를 탐지합니다. (BZ#1933269)

- 이전에는 OVN(Open Virtual Network)에서 Hairpin 트래픽 패킷의 소스 IP 주소를 로드 밸런서의 IP 주소로 변경하여 네트워크 정책을 사용 중일 때 트래픽이 차단되었습니다. 이번 업데이트를 통해 Kuryr는 네트워크 정책의 네임스페이스에서 모든 서비스의 IP 주소로 트래픽을 열고 헤어핀 트래픽이 차단되지 않습니다. (BZ#1920532)

- 이전에는 IPv4 주소가 있는 노드에서 단일 스택 IPv6 클러스터를 시작할 때 kubelet에서 노드 IP에 IPv6 IP 대신 IPv4 IP를 사용할 수 있었습니다. 결과적으로 호스트 네트워크 pod에는 IPv6 IP 대신 IPv4 IP가 있어 IPv6 전용 pod에서 연결할 수 없게 되었습니다. 이번 업데이트에서는 node-IP-picking 코드가 수정되어 IPv6 IP를 사용하는 kubelet이 생성됩니다. (BZ#1939740)

- 이전에는 알 수 없는 이유로 kubelet이 노드에 잘못된 IP 주소를 등록할 수 있었습니다. 그 결과 노드가 재부팅될 때까지 **NotReady** 상태가 됩니다. 이제 systemd 관리자 구성이 유효한 IP 주소를 환경 변수로 다시 로드됩니다. 즉, kubelet이 잘못된 IP 주소를 등록했기 때문에 노드가 더 이상 **NotReady** 상태를 입력하지 않습니다. (BZ#1940939)

- 이전에는 shadowed 변수에 대한 리팩토링으로 인해 체크포인트 파일 사용과 관련된 회귀 문제가 발생했으며 SR-IOV Pod 샌드박스가 시작되지 않았습니다. 리팩토링 중 kubelet 소켓 경로에 대한 검사가 올바르게 처리되지 않았습니다. 수정을 통해 kubelet 소켓 경로에 대한 검사를 올바르게 복원하고 이제 SR-IOV Pod 샌드박스가 제대로 생성됩니다. (BZ#1968625)

노드

- 이전에는 RADOS(Reliable Autonomic Distributed Object Store) 블록 장치(RBD)가 **lsblk**를 실행하는 권한이 없는 컨테이너 pod에 표시되었습니다. 이 문제는 수정되었으며 RBD는 **lsblk**를 실행하는 권한이 없는 컨테이너 pod에 더 이상 표시되지 않습니다. (BZ#1772993).

- 이전 버전에서는 클러스터를 업그레이드하는 동안 **/etc/hostname** 파일이 CRI-O로 변경되었습니다. 이로 인해 노드가 실패하고 재부팅 시 반환되었습니다. 이번 업데이트에서는 업그레이드 중에 **/etc/hosts** 파일을 그대로 유지하도록 CRI-O에 특수 처리가 추가되어 업그레이드된 노드가 문제없이 부팅됩니다. (BZ#1921937)

- 이전 버전에서는 CRI-O가 네트워크를 프로비저닝한 후 pod를 생성하는 데 시간이 너무 오래 걸렸습니다. 이렇게 되면 네트워크 정리 코드에 버그가 발생하여 네트워크 리소스가 프로비저닝된 후 네트워크 리소스가 제대로 정리되지 않습니다. 이번 업데이트에서는 명령이 시간 초과되어도 네트워킹 리소스를 올바르게 정리하도록 코드가 변경되었습니다. 이렇게 하면 Pod 생성에 시간이 너무 오래 걸리는 경우에도 클러스터가 정상적인 네트워크 작업을 계속할 수 있습니다. (BZ#1957224)

- 이전에는 **CNI** 플러그인을 사용하여 노드가 재부팅되지 않았습니다. CRI-O는 재부팅하기 전에 실행 중인 모든 컨테이너에서 **CNI DEL**을 호출하도록 수정되었습니다. 이번 업데이트에서는 **CNI** 리소스를 정리하고 성공적으로 재부팅할 수 있습니다. (BZ#1948137)

- 이전에는 **CNI** 정리 작업에서 클린업 실패를 확인하지 않았기 때문에 실패한 경우 **CNI DEL** 요청을 호출하지 않았습니다. 이제 CRI-O에서 **CNI DEL** 요청을 호출하여 **CNI** 리소스를 올바르게 정리합니다. (BZ#1948047)

- 이전 버전에서는 컨테이너 또는 이미지에 대한 재부팅 요청으로 인해 컨테이너 또는 이미지가 디스크에 커밋되는 동안 재부팅이 발생한 경우 오류가 발생할 수 있었습니다. 이로 인해 컨테이너에 대한 스토리지가 손상되어 이미지를 가져오거나 이미지에서 컨테이너를 다시 생성할 수 없었습니다. 이번 업데이트에서는 노드가 재부팅될 시기를 감지하고 true 인 경우 컨테이너 스토리지를 지웁니다. (BZ#1942536)

- 이전에는 **runc**에서 해당 권한을 실행한 엔터티의 권한을 사용했습니다. 그러나 **workdir**에 대한 권한은 **container** 사용자가 설정합니다. 이러한 권한이 다르면 컨테이너 생성 오류가 발생하여 컨

테이너 시작에 오류가 발생했습니다. 이 패치는 한 번만 실패할 경우 **workdir**에 **runc**를 **chdir**로 여러 번 업데이트합니다. 이렇게 하면 컨테이너가 성공적으로 생성됩니다. (BZ#1934177)

- 이전에는 CRI-O 로그에 이미지를 가져온 소스에 대한 정보가 없었습니다. 이번 수정을 통해 CRI-O 로그의 정보 수준에 로그 풀 소스가 추가됩니다. (BZ#1881694)

- 이전 버전에서는 Pod를 빠르게 생성 및 삭제할 때 Pod가 삭제되기 전에 Pod 샌드박스 생성을 완료하는 데 시간이 부족할 수 있었습니다. 결과적으로 'ErrCreatePodSandbox'error를 사용하여 Pod 삭제가 실패할 수 있었습니다. 이제 Pod가 종료되면 이 오류가 무시됩니다. 결과적으로 Pod가 Pod 샌드박스 생성을 완료하지 못한 경우 Pod 종료가 더 이상 실패하지 않습니다. (BZ#1908378)

- 이전에는 MCO (Machine Config Operator)에서 **추적**을 유효한 로그 수준으로 허용하지 않았습니다. 결과적으로 MCO는 CRI-O에서 지원하는 경우에도 추적 수준 로깅을 활성화하는 방법을 제공할 수 없었습니다. **추적** 로그 수준을 지원하도록 MCO가 업데이트되었습니다. 결과적으로 MCO 구성을 통해 추적 로그 수준을 볼 수 있습니다. (BZ#1930620)

- 이전에는 kubelet에서 완전히 가져오지 않은 이미지 상태를 가져오려고 했습니다. 결과적으로 **crictl**에서 이러한 이미지에 대한 **error locating item named "manifest"** 오류를 보고합니다. 매니페스트가 없는 이미지를 나열하지 않도록 CRI-O가 업데이트되었습니다. 결과적으로 **crictl**에서 더 이상 이러한 오류를 보고하지 않습니다. (BZ#1942608)

- 이전에는 오래된 상태 메시지가 제거되지 않았습니다. 이로 인해 MCO(Machine Config Operator)가 적절한 머신 구성 풀을 찾을 수 없는 경우가 있었습니다. 이번 릴리스에서는 상태 수를 제한하기 위해 정리 기능이 추가되었습니다. 결과적으로 MCO는 최대 3개의 다른 kubeletConfig 상태를 유지합니다. (BZ#1950133)

- 이전 버전에서는 OpenShift Container Platform 버전 4.6.25에서 업그레이드할 때 **kubeletconfig** CR 또는 **ContainerRuntimeConfig** CR이 두 개 이상 있는 클러스터에서 MCO(Machine Config Operator)가 동일한 구성에 대한 중복 머신 구성을 생성할 수 있었습니다. 그 결과 MCO에서 이전 컨트롤러 버전(IGNITION 3.1.0)을 사용하므로 업그레이드에 실패했습니다. 이번 업데이트에서는 오래된 중복 머신 구성을 정리하고 버전 4.6.25에서 올바르게 업그레이드할 수 있습니다. (BZ#1955517)

oauth-apiserver

- 이전 버전에서는 일부 OAuth 서버 지표가 제대로 초기화되지 않았으며 Prometheus UI의 검색에 표시되지 않았습니다. 이제 누락된 OAuth 서버 지표가 올바르게 초기화되고 Prometheus UI 지표 검색에 표시됩니다. (BZ#1892642)

- 이전에는 사용자 정의 보안 컨텍스트 제약 조건(SCC)에 **defaultAllowPrivilegeEscalation: false** 및 **allowPrivilegedContainer : true** 필드가 포함된 경우 보안 컨텍스트 변경이 API 검증에 실패한 상태로 권한 있는 **openshift -apiserver** 및 **oauth-apiserver** Pod를 변경했습니다. 이로 인해 pod를 시작하지 못해 OpenShift API 중단이 발생하는 경우가 있었습니다. 보안 컨텍스트 변경기에서 이미 권한이 있는 컨테이너의 **defaultAllowPrivilegeEscalation** 필드를 무시하고 해당 필드를 포함하는 사용자 지정 SCC에서는 pod가 시작되지 않습니다. (BZ#1934400)

oc

- 이전 버전에서는 **oc explain** 명령을 실행할 때 리소스 문자열의 일부로 제공된 경우 리소스 그룹 이름이 자동으로 탐지되지 않았습니다. 다른 그룹의 두 리소스에 동일한 리소스 이름이 있는 경우 **--api-version** 매개 변수를 통해 그룹을 지정하지 않는 한 가장 높은 우선 순위 정의가 반환되었습니다. 이제 **--api-version** 매개 변수가 포함되어 있지 않으면 그룹 이름을 감지하기 위해 리소스 문자열에 대해 접두사 확인이 실행됩니다. 명령에서 반환되는 설명은 명시된 그룹의 일치하는 리소스와 관련이 있습니다. (BZ#1725981)

- 이전에는 **oc image extract** 명령에서 이미지의 루트 디렉터리에서 파일을 추출하지 않았습니다. 명령이 업데이트되었으며 이제 이미지 루트 디렉터리에서 파일을 추출하는 데 사용할 수 있습니다. (BZ#1919032)

- 이전에는 **oc apply** 명령이 각 호출에 대해 OpenAPI 사양을 가져옵니다. 이제 명령을 처음 실행하면 OpenAPI 사양이 캐시됩니다. **oc apply** 명령이 여러 번 실행되고 네트워크 로드가 감소하면 캐시된 OpenAPI 사양이 재사용됩니다. (BZ#1921885)

- 이전에는 이미지 미러링 중에 생성된 권한 부여 헤더가 일부 레지스트리의 헤더 크기 제한을 초과할 수 있었습니다. 이로 인해 미러링 작업 중에 오류가 발생했습니다. 이제 인증 헤더가 헤더 크기 제한을 초과하지 않도록 **oc adm catalog mirror** 명령에 **--skip-multiple-scopes** 옵션이 **true**로 설정됩니다. (BZ#1946839)

- 이전에는 **oc volume set** 명령에 **--claim-class** 옵션이 포함된 경우 **storageClassName** 속성이 **PersistentVolumeClaim** 오브젝트에 추가되지 않았습니다. 대신 **--claim-class** 옵션 값이 **volume.beta.kubernetes.io/storage-class** 주석에 추가되었습니다. 이로 인해 **storageClassName** 속성에 종속되어 볼륨의 스냅샷이 실패할 수 있었습니다. 이제 **oc volume set** 명령에서 **--claim-class** 옵션의 값을 **PersistentVolumeClaim** 오브젝트의 **storageClassName** 속성에 적용하고 볼륨 스냅샷은 특성 값을 참조할 수 있습니다. (BZ#1954124)

- 이전 버전에서는 **oc adm top --help**의 출력에서 **oc adm top** 명령이 pod 및 노드의 CPU, 메모리 및 스토리지 리소스 사용량을 표시할 수 있다고 설명했습니다. **oc adm top** 명령은 스토리지 리소스 사용량을 표시하지 않습니다. 이제 스토리지 참조가 **oc adm top --help** 출력에 포함되어 있지 않습니다. (BZ#1959648)

OLM(Operator Lifecycle Manager)

- 이전 버전에서는 Operator 설치의 일부로 적용된 CRD(**CustomResourceDefinition**) 오브젝트가 동일한 Operator의 최신 버전의 설치 요구 사항을 충족할 수 있었습니다. 결과적으로 Operator 업그레이드 중에 교체되는 버전이 조기 제거될 수 있었습니다. 경우에 따라 업그레이드가 중지되는 경우도 있습니다. 이번 업데이트를 통해 Operator 번들 설치의 일부로 생성되거나 업데이트된 CRD에 원본 번들을 나타내는 주석이 추가됩니다. 이러한 주석은 **CSV(ClusterServiceVersion**) 오브젝트에서 기존 CRD와 동일한 번들 CRD를 구분하는 데 사용됩니다. 결과적으로 현재 버전의 CRD를 적용할 때까지 업그레이드가 완료되지 않습니다. (BZ#1947946)

- 이전에는 **CatalogSource** 오브젝트에서 참조하는 인덱스를 실행한 Pod에 **securityContext** 필드에 명시적으로 설정된 **readOnlyRootFileSystem: false**가 없었습니다. 결과적으로 **readOnlyRootFileSystem: true**를 강제 적용하고 해당 pod의 **securityContext**와 일치하는 SCC(보안 컨텍스트 제약 조건) 가 있는 경우 해당 pod에 할당되어 반복적으로 장애가 발생하게 됩니다. 이번 업데이트에서는 **securityContext** 필드에 **readOnlyRootFileSystem: false**를 명시적으로 설정합니다. 결과적으로 **CatalogSource** 오브젝트에서 참조하는 Pod는 읽기 전용 루트 파일 시스템을 적용하는 SCC와 더 이상 일치하지 않으며 더 이상 장애가 발생하지 않습니다. (BZ#1961472)

- 이전 버전에서는 OLM(Operator Lifecycle Manager)에서 처음 설치하는 동안 버전이 **startingCSV** 필드에 지정된 경우 건너뛴 버전의 설치를 허용하지 않았습니다. 이로 인해 사용자가 생략한 이유와 관계없이 설치를 원하더라도 건너뛴 버전을 설치할 수 없게 되었습니다. 이번 수정에서는 사용자가 **Subscription** 오브젝트에 **startCSV** 사양을 사용하여 초기 설치 중에만 건너뛴 버전을 설치할 수 있도록 OLM을 업데이트합니다. 사용자는 예상대로 건너뛰기된 버전으로 업그레이드할 수 없습니다. (BZ#1906056)

- **k8s.io/apiserver**가 웹 후크 작성자의 컨텍스트 오류를 처리하지 않았기 때문에 시간 초과와 같은 컨텍스트 오류로 인해 작성자가 패닉 상태가 발생했습니다. 이번 수정을 통해 문제에 대한 업스트림 수정을 포함하도록 API 서버 버전이 증가하므로 작성자가 컨텍스트 오류를 정상적으로 처리할 수 있습니다. (BZ#1913525)

- 이전에는 **oc adm catalog mirror** 명령을 Air-Gapped 환경에서 Operator 카탈로그를 미러링하는 데 쉽게 사용할 수 없었습니다. 이 향상된 기능을 통해 카탈로그의 콘텐츠를 파일 시스템에 미러링하고 이동식 미디어에 배치한 다음 파일 시스템에서 아울러 클러스터에서 사용할 레지스트리로 미러링할 수 있습니다. (BZ#1919168)

- 이전에 Catalog Operator가 생성한 번들은 시간 제한을 설정하지 않고 설치 계획에 대한 번들 압축 풀기 작업을 만들었습니다. 번들 이미지가 없거나 삭제된 경우 작업이 영구적으로 실행되었으며 설치 계획이 **Installing** 단계에 머물러 작업 pod가 이미지를 확인하지 못했습니다. 이번 수정으로 Catalog Operator는 **--bundle-unpack-timeout** 플래그를 사용하여 구성할 수 있는 번들 압축 해제 작업에 기본 **10m** 시간 초과를 설정합니다. 결과적으로 구성된 시간 초과 후 번들의 압축 풀기 작업이 실패하고 설치는 **status.conditions** 및 **status.bundleLookups.conditions** 속성에 이유가 표시되며 **Failed** 단계로 전환됩니다. (BZ#1921264)

- OpenShift Container Platform 4.6 이전의 클러스터에 설치된 Operator는 종속성 확인 및 업그레이드 선택을 위해 지정된 Operator 패키지에서 가져온 것으로 확인되지 않았습니다. 이로 인해 기존 Operator 설치가 자체 서브스크립션 기준과 충돌하여 네임스페이스 내에서 업그레이드 및 종속성 확인이 차단되었습니다. 이번 수정에서는 서브스크립션에서 참조하는 Operator의 패키지 이름과 버전을 추측하도록 OLM이 업데이트되었습니다. 그 결과 업그레이드 및 종속성 확인이 예상대로 진행됩니다. (BZ#1921953)

- 일시적인 오류에 사용되는 **Info** 로그 수준으로 인해 기본 구성에 대한 OLM Operator 로그가 상세하게 표시되었습니다. 이번 수정을 통해 일시적인 오류 로그 수준을 **debug**로 변경합니다. 결과적으로 **debug** 구성에 대해 볼 수 있는 중요하지 않은 로그 수가 줄어듭니다. (BZ#1925614)

- 이전에는 **Subscription** 오브젝트의 **spec.config.resources** 섹션이 설정되지 않았거나 비어 있는 경우에도 설치된 배포에 항상 적용되었습니다. 이로 인해 CSV(클러스터 서비스 버전)에 정의된 리소스가 무시되고 **Subscription** 오브젝트의 **spec.config.resources** 섹션에 정의된 리소스만 사용되었습니다. 이번 수정에서는 **spec.config.resources** 섹션이 nil 또는 비어 있지 않은 값으로 설정된 경우에만 배포 관련 리소스를 재정의하도록 OLM을 업데이트합니다. (BZ#1926893)

- 종속성 및 업그레이드 확인 중에 서브스크립션 고유성은 이전에 서브스크립션된 패키지 이름을 기반으로 했습니다. 네임스페이스의 두 서브스크립션이 동일한 패키지를 구독하면 내부적으로 단일 서브스크립션으로 처리되므로 예기치 않은 동작이 발생합니다. 이번 수정을 통해 이제 **.spec.name** 대신 **.metadata.name**을 통해 네임스페이스 내에서 내부적으로 서브스크립션을 고유하게 식별할 수 있습니다. 결과적으로 동일한 **.spec.name.**이 포함된 여러 **Subscription** 오브젝트가 포함된 네임스페이스에 업그레이드 및 종속성 확인 동작이 일관되게 유지됩니다. (BZ#1932001)

- 예정된 카탈로그 업데이트 폴링 시도가 1분 이내로 남아 있는 경우 간격 지터 기능은 재동기화 간격을 0으로 줄입니다. 이로 인해 Operator Catalog가 핫 루프에 진입하여 CPU 사이클이 낭비되었습니다. 이번 수정을 통해 재동기화 지연을 계산하는 데 사용되는 지터 기능의 정확도가 높아졌습니다. 결과적으로 Catalog Operator는 다음 카탈로그 업데이트 폴링까지 대부분 유휴 상태로 유지됩니다. (BZ#1932182)

- Operator 업그레이드 중에 관련 **ServiceAccount** 오브젝트의 소유자 참조가 이전이 아닌 새로운 CSV(**ClusterServiceVersion**) 오브젝트를 가리키도록 업데이트되었습니다. 이로 인해 CSV를 조정하는 OLM Operator와 Catalog Operator 간에 경쟁 조건이 발생하여 서비스 계정 소유권 변경으로 **Pending**/**RequirementsNotMet**로 표시하는 설치 계획을 실행할 수 있습니다. 이로 인해 새 CSV가 이전 CSV가 정상 상태를 나타낼 때까지 무기한 기다리는 동안 업그레이드 완료를 차단했습니다. 이번 수정으로 한 단계에서 소유자 참조를 업데이트하는 대신 두 번째 소유자가 기존 소유자에 추가됩니다. 따라서 동일한 서비스 계정이 이전 CSV와 새 CSV에 대한 요구 사항을 충족할 수 있습니다. (BZ#1934080)

- 이전에 CSV(클러스터 서비스 버전)에는 **ownerReferences** 값이 설정되지 않았거나 관련 CSV로 설정된 **ownerReferences** 값을 설정하지 않았습니다. 이로 인해 **metadata.ownerReferences** 필드가 비어 있지 않은 경우 Operator 설치의 일부로 **default** 서비스 계정이 생성되지 않았습니

다. 이번 수정으로 CSV에는 CSV로 설정된 **ownerReferences** 값이 없거나 **ownerReference** 값을 관련 CSV로 설정하기 위해 CSV에 연결된 서비스 계정이 있어야 합니다. 결과적으로 CSV가 아닌 **ownerReferences** 값만 있는 서비스 계정은 모든 CSV의 요구 사항을 충족할 수 있습니다. (BZ#1935909)

- OpenShift Container Platform 4.5 이전에는 **openshift-marketplace** 네임스페이스의 Marketplace Operator에서 배포 및 관리하는 기본 카탈로그가 Marketplace Operator에서 노출한 API인 **OperatorSource** 개체에 의해 생성되었습니다. Operator 소스에서 발생하는 오류를 나타내기 위해 적절한 메트릭 및 경가 작성되었습니다. OpenShift Container Platform 4.6에서는 여러 릴리스에서 더 이상 사용되지 않는 **OperatorSource** 리소스가 제거되었으며 Marketplace Operator가 대신 OLM의 **CatalogSource** 리소스를 직접 생성했습니다. 그러나 **openshift-marketplace** 네임스페이스에 배포된 카탈로그 소스에는 동일한 메트릭 및 경고 계측이 수행되지 않았습니다. 따라서 기본 카탈로그 소스에서 발생한 오류가 Prometheus 경고로 강조 표시되지 않았습니다. 이번 수정에서는 OLM의 새 **catalogsource_ready** 메트릭이 도입되었습니다. 이 메트릭은 기본 카탈로그 소스에 대한 메트릭에 카탈로그 소스가 준비되지 않음을 나타낼 때마다 Marketplace Operator에서 경고를 발생시키는 데 사용됩니다. 결과적으로 **openshift-marketplace** 네임스페이스에 준비되지 않은 기본 카탈로그 소스에 대해 Prometheus 경고가 제공됩니다. (BZ#1936585)

- 이전 버전에서는 기본 채널과 비기본 채널에서 Operator 종속성을 사용할 수 있는 경우 OLM(Operator Lifecycle Manager)에서 두 채널 중 하나를 임의로 지정하는 서브스크립션을 생성할 수 있었습니다. 이제 Operator 종속성은 먼저 기본 채널의 후보자에 의해 충족되고 그 다음에는 다른 채널의 후보자에 의해 충족됩니다. (BZ#1945261)

- 이전에는 CSV(클러스터 서비스 버전)가 여러 Operator의 구성 요소로 복사될 수 있었습니다. 이는 Operator를 설치한 후 Operator 그룹에 네임스페이스가 추가된 경우 발생할 수 있습니다. 이 동작은 메모리 사용 및 CPU 로드에 영향을 미쳤습니다. 이제 CSV가 **Copied** 이유와 함께 Operator의 **status.components** 필드에 표시되지 않으며 성능에도 영향을 주지 않습니다. (BZ#1946838)

Operator SDK

- 이전에는 조정 중에 **ManagedFields**가 처리되었기 때문에 일부 리소스가 무한 루프로 포착되었습니다. 이번 수정에서는 **ManagedFields**를 무시하도록 **operator-lib**를 업데이트하여 루프를 일관되게 조정합니다. (BZ#1856714)

- **--help** 가 CLI(명령줄 인터페이스)에서 전달되었을 때 기본 플러그인이 호출되지 않았기 때문에 Operator SDK에 최소 도움말 메시지가 출력되었습니다. 이번 수정에서는 사용자가 **operator-sdk init --help** 명령을 실행할 때 기본 플러그인을 호출하고 더 유용한 도움말 메시지를 출력합니다. (BZ#166222)

- 이전 버전에서는 선택적 검증기가 누락된 경우 문제 경고 대신 **operator-sdk bundle**이 실패했습니다. 이 문제가 해결되었습니다. (BZ#1921727)

openshift-apiserver

- 이전에는 사용자 정의 보안 컨텍스트 제약 조건(SCC)의 기본 집합보다 우선 순위가 더 높을 수 있었습니다. 그 결과 해당 SSC가 **openshift-apiserver** pod와 일치하는 경우가 있어 루트 파일 시스템에 쓸 수 있는 기능이 손상되었습니다. 또한 이 버그로 인해 일부 OpenShift API가 중단되었습니다. 이번 수정에서는 **openshift-apiserver** pod에 루트 파일 시스템에 쓰기 가능하도록 명시적으로 표시되어 있습니다. 따라서 사용자 정의 SCC가 **openshift-apiserver** Pod의 실행을 저지할 수 없습니다. (BZ#1942725)

Performance Addon Operator

- 이전 버전에서는 대기 시간이 짧은 응답을 제공하도록 컨테이너를 구성할 때 CRI-O를 사용한 동적 인터럽트 마스크가 **irqbalance** 시스템 서비스에 설정된 인터럽트 마스크와 일치하지 않았습

니다. 각각 다른 마스크를 설정하고 컨테이너 지연 시간이 손상되었습니다. 이번 업데이트에서는 **irqbalance** 시스템 서비스와 일치하도록 CRI-O를 설정하여 설정된 인터럽트 마스크세트를 변경합니다. 그 결과 동적 인터럽트 마스크 처리가 예상대로 작동합니다. (BZ#1934630)

RHCOS

- 이전에는 부팅 프로세스에서 다중 경로가 너무 늦게 활성화되었습니다. 결과적으로 RHCOS(Red Hat Enterprise Linux CoreOS)는 일부 다중 경로 환경에서 I/O 오류를 반환합니다. 이번 업데이트를 통해 이제 부팅 프로세스 초기에 다중 경로가 활성화됩니다. 따라서 RHCOS는 일부 다중 경로 환경에서 더 이상 I/O 오류를 반환하지 않습니다. (BZ#1954025)

- 이전 버전에서는 잠재적인 경쟁 조건으로 인해 일부 환경에서 RHCOS(Red Hat Enterprise Linux CoreOS) PXE 배포에서 rootfs를 가져오지 못할 수 있었습니다. 이번 수정을 통해 rootfs를 가져오려고 시도하기 전에 연결을 다시 시도하여 경우에 따라 **coreos-livepxe-rootfs** 스크립트가 실패하는 시점을 계속 진행하기 전에 원격 서버에 대한 액세스를 확인하고 rootfs 파일을 확인합니다. (BZ#1871303)

- 이전에는 **MachineConfig**의 사용자 사전 설정이 무시되었습니다. 이로 인해 사용자가 **kdump.service**의 설정을 변경할 수 없었습니다. 이제 기본 사전 설정의 우선 순위 수준이 사용자 구성 기본값보다 낮으므로 사용자 구성이 벤더 구성을 적절하게 재정의할 수 있습니다. (BZ#1969208)

- 이전에는 **coreos-installer**가 손상된 GUID 파티션 테이블(GPT)이 있는 디스크에 설치를 거부했습니다. 설치 이미지로 작성하기 전에 대상 디스크의 GPT를 읽으려고 했기 때문입니다. 이번 수정으로 **coreos-installer**는 기존 파티션을 보존하라는 지침이 있을 때 대상 디스크의 GPT만 읽고 손상된 GPT가 있는 디스크에 성공적으로 설치됩니다. (BZ#1914976)

- 이전에는 포맷되지 않은 직접 액세스 스토리지 장치(DASD)에 클러스터를 설치하면 **coreos-installer**에서 잘못 작성된 디스크 섹터가 생성되었습니다. 이제 **coreos-installer**는 포맷되지 않은 새로운 DASD 드라이브를 4096바이트 섹터로 올바르게 포맷합니다. 이렇게 하면 **coreos-installer**가 디스크 드라이브에 OS 이미지의 설치를 완료할 수 있습니다. (BZ#1905159)

- 이전에는 s390x z15 시스템에서 하드웨어 지원 **zlib** 압축을 해제하면 RHEL rootfs 이미지 마운트에 실패하여 RHEL 8.3 커널을 사용하는 REHL s390x z15 노드의 부팅이 실패했습니다. 하드웨어 지원 **zlib** 압축을 사용할 수 있을 때 커널이 **zlib**에서 압축된 squashfs 파일을 올바르게 처리하도록 업데이트되었습니다. (BZ#1903383)

- 이전에는 **zipl** 명령은 512바이트의 섹터 크기를 가정하여 디스크를 구성했습니다. 그 결과 4k 섹터가 있는 SCSI 디스크에서 **zipl** 부트로더 구성에 잘못된 오프셋이 포함되어 zVM을 부팅할 수 없었습니다. 이번 수정으로 **zipl**은 이제 디스크 섹터 크기를 고려하여 zVM이 성공적으로 부팅됩니다. (BZ#1918723)

- 이전 버전에서는 **chrony.config**가 자동으로 여러 번 실행되어 첫 번째 실행에 실패할 수 있었습니다. 이로 인해 **chrony.config** 구성이 초기 실행 중에 설정되고 변경할 수 없기 때문에 문제가 발생했습니다. 이제 **chrony.config**가 처음 실행되는 경우 구성 설정 프로세스를 제한하여 이러한 오류를 방지할 수 있습니다. (BZ#1924869)

- 이전에는 노드가 비정상으로 표시되었으며 워크로드가 많은 기간에는 예상대로 작동하지 않았습니다. 이는 메모리를 사용하는 워크로드가 메모리 회수 속도보다 더 빠르기 때문에 발생했습니다. 이번 업데이트를 통해 메모리 재요청 및 메모리 부족 상황이 해결되었으며 워크로드가 많은 상황에서는 이러한 상태가 더 이상 발생하지 않습니다. (BZ#1931467)

- 이전에는 Kerberos 인수를 사용하는 본딩 인터페이스의 최대 전송 단위(MTU) 사양이 제대로 할당되지 않았습니다. 이 문제가 해결되었습니다. (BZ#1932502)

- 이전에는 **clevis-luks-askpass.path** 장치가 기본적으로 활성화되지 않았습니다. 이로 인해 루트가 아닌 **LUKS Clevis** 장치가 재부팅 시 자동으로 잠금 해제되지 않았습니다. 이번 업데이트를 통

해 기본적으로 **clevis-luks-askpass.path** 장치를 활성화하고 루트가 아닌 **LUKS Clevis** 장치가 재부팅 시 자동으로 잠금 해제할 수 있습니다. (BZ#1947490)

- 이전 버전에서는 systemd가 **mountinfo**를 과도하게 읽고 CPU 리소스를 과도하게 소비하여 이로 인해 컨테이너가 시작되지 않았습니다. 이번 업데이트를 통해 **systemd**에서 **mountinfo**를 읽을 때 제한을 활성화하여 컨테이너가 성공적으로 시작될 수 있습니다. (BZ#1957726)

- 이전 버전에서는 MCO (Machine Config Operator)에서 Ignition 버전을 점검하기 위해 Ignition을 호출하면 Ignition이 충돌했습니다. 결과적으로 MCO가 시작되지 않았습니다. 이번 업데이트를 통해 MCO가 더 이상 Ignition 버전을 쿼리하지 않고 MCO가 성공적으로 시작됩니다. (BZ#1927731)

라우팅

- 이전에는 HAProxyDown 경고 메시지가 모호했습니다. 결과적으로 최종 사용자는 이 경고가 HAProxy pod가 아닌 라우터 pod를 사용할 수 없음을 의미한다고 생각했습니다. 이번 업데이트로 HAProxyDown 경고 메시지가 더 명확해졌습니다. (BZ#1941592)

- 이전에는 허용 목록 IP에 대한 파일을 생성하는 HAProxy의 도우미 기능 템플릿에서 잘못된 인수 유형이 예상되었습니다. 결과적으로 긴 IP 목록의 백엔드에 대해 허용 목록 ACL이 적용되지 않았습니다. 이번 업데이트를 통해 허용 목록 ACL이 긴 IP 목록 백엔드에 적용되도록 도우미 기능 템플릿의 인수 유형이 변경됩니다. (BZ#1964486)

- 이전에는 사용자 정의 도메인을 사용하여 Ingress를 생성할 때 OpenShift Container Platform Ingress 컨트롤러에서 라우터 표준 호스트 이름으로 업데이트하고 **external-dns**를 사용하여 Route 53과 동기화했습니다. 문제는 정식 라우터 호스트 이름이 DNS에 존재하지 않았으며 OpenShift Container Platform에서 생성되지 않았다는 것입니다. OpenShift Container Platform은 **apps.<cluster_name>.<base_domain>** DNS 레코드가 아닌 ***.apps.<cluster_name>.<base_domain>** DNS 레코드를 생성합니다. 따라서 정식 라우터 호스트 이름이 올바르지 않았습니다. 이번 수정에서는 정식 라우터 호스트 이름을 **router-default.apps.<cluster_name>.<base_domain>**으로 설정합니다. 정식 호스트 이름을 사용하고 와일드카드 또는 하위 도메인 앞에 자동화가 있는 클러스터 관리자는 정식 Ingress 호스트 이름이 **<ingress-controller-name>.apps.<cluster_name>.<base_domain>**으로 설정되어 있음을 인지하고 있어야 합니다. (BZ#1901648)

- 이전에는 BZ#1932401에 대한 수정 사항이 기본 Go HTTP 클라이언트 전송을 덮어썼습니다. 이로 인해 클러스터 전체 프록시 설정이 Ingress Operator Pod에 연결되어 있지 않아 클러스터 전체 송신 프록시가 있는 클러스터에서 카나리아 검사를 수행하지 못했습니다. 이번 업데이트에서는 카나리아 클라이언트의 HTTP 전송에서 프록시 설정을 명시적으로 설정합니다. 결과적으로 카나리아 검사는 모든 클러스터 전체 프록시에서 작동합니다. (BZ#1935528)

- 이전에는 카나리아 DaemonSet에서 노드 선택기를 지정하지 않아 카나리아 네임스페이스의 기본 노드 선택기를 사용했습니다. 결과적으로 카나리아 DaemonSet은 인프라 노드에 예약할 수 없으며 경우에 따라 경고가 발생했습니다. 이번 업데이트에서는 인프라 노드에 카나리아 DaemonSet을 명시적으로 예약하고 테인트된 인프라 노드를 허용합니다. 이를 통해 카나리아 DaemonSet은 문제나 경고 없이 작업자 및 인프라 노드에 안전하게 롤아웃할 수 있습니다. (BZ#1933102)

- 이전 버전에서는 유휴 워크로드가 있는 이전 버전에서 클러스터를 업그레이드할 때 **oc idle** 기능 수정 및 재작업으로 인해 OpenShift Container Platform 4.6 또는 4.7으로 업그레이드된 HTTP 요청에서 유휴 상태의 워크로드가 발생하지 않았습니다. 이번 업데이트를 통해 유휴 변경 사항이 Ingress Operator 시작 시 엔드포인트에서 서비스로 미러링됩니다. 따라서 업그레이드 후 워크로드를 유휴 상태로 해제하면 예상대로 작동합니다. (BZ#1925245)

- 이전에는 모든 HTTP 트래픽을 HTTPS로 리디렉션하는 외부 로드 밸런서를 통해 기본 Ingress 컨트롤러를 노출하면 Ingress Operator에서 수행한 Ingress Canary 엔드포인트 검사가 실패하여 Ingress Operator가 **degraded**되었습니다. 이번 수정을 통해 일반 텍스트 카나리아 경로를 에지

암호화된 경로로 변환합니다. 이제 카나리아 경로는 안전하지 않은 트래픽이 로드 밸런서에 의해 리디렉션되는 경우에만 HTTPS 로드 밸런서를 통해 작동합니다. (BZ#1932401)

- 이전에는 Ingress Operator Canary Check Client에서 HTTP 트래픽을 삭제한 로드 밸런서에 HTTP를 통해 카나리아 요청을 전송했습니다. 이로 인해 카나리아 검사에 실패한 후 Ingress Operator의 성능이 **degraded**되었습니다. 이번 수정으로 라우터의 리디렉션을 사용하는 대신 Ingress Operator Canary Check Client는 처음부터 HTTPS를 통해 카나리아 점검 요청을 보냅니다. 이제 비보안 HTTP 트래픽을 삭제하는 로드 밸런서를 통해 기본 Ingress 컨트롤러를 노출하는 클러스터에 대해 카나리아 검사가 작동합니다. (BZ#1934773)

- 이전 버전에서는 **openshift-router**에서 사용한 HAProxy 템플릿이 **firstMatch()** 함수에 대해 반복적으로 호출했습니다. 이 함수는 매번 정규 표현식을 구문 분석하고 다시 컴파일합니다. **firstMatch()**로 호출할 때 마다 정규식을 구문 분석하고 다시 컴파일하는 것은 특히 경로가 수천 개인 구성의 경우 비용이 많이 듭니다. 이번 수정을 통해 **firstMatch()** 호출의 정규 표현식이 이미 표시된 경우 이미 컴파일된 버전이 다시 사용되고 캐시됩니다. 이제 **haproxy-config.template**을 구문 분석하고 평가할 때 실행 시간이 60% 단축되었습니다. (BZ#1937972)

- 이전에는 재정의 주석을 사용하여 잘못된 호스트 이름으로 경로 이름을 지정할 수 있었습니다. 이번 업데이트에서는 이 문제가 해결되었습니다. (BZ#1925697)

- 이전 버전에서는 경로를 통해 노출된 서비스에서 **선택기를** 제거하면 서비스 포드에 대해 **생성되는** 끝점 라이센스가 복제되어 중복 서버 항목으로 인해 HAProxy 재로드 오류가 발생했습니다. 이번 업데이트에서는 HAProxy 구성 파일을 작성할 때 실수로 중복된 서버 행을 필터링하여 서비스에서 선택기를 삭제해도 더 이상 라우터가 실패하지 않습니다. (BZ#1961550)

Samples

- 이전에는 Cluster Samples Operator에서 모니터링 중인 개체에 대한 컨트롤러 캐시를 변경할 수 있었기 때문에 Kubernetes에서 컨트롤러 캐시를 관리할 때 오류가 발생했습니다. 이번 업데이트에서는 Cluster Samples Operator가 컨트롤러 캐시의 정보를 사용하는 방법이 수정되었습니다. 결과적으로 Cluster Samples Operator에서 컨트롤러 캐시를 수정하여 오류가 발생하지 않습니다. (BZ#1949481)

service-ca

- OpenShift Container Platform 4.8을 사용하면 조직의 요구에 맞게 루트가 아닌 사용자로 **service-ca-operator** Pod를 실행할 수 있습니다. 루트가 아닌 사용자로 실행하는 경우 **service-ca-operator**는 다음 UID 및 GID 로 실행됩니다.

  ```
  uid=1001(1001) gid=1001 groups=1001
  ```

  (BZ#1914446)

스토리지

- 이전 버전에서는 **capacity breakdown**을 요청할 때 **block type PVC** 파일 시스템에 대한 지표가 보고되지 않았습니다. 즉, 사용자는 모든 파일 시스템에서 지표에 대한 부정확한 보고를 받았습니다. 이번 업데이트를 통해 Kubelet에서 요청할 때 **block type PVC**가 포함됩니다. 이는 모든 파일 시스템 지표에 대한 정확한 보고를 제공합니다. (BZ#1927359)

- 이전에는 **/var/lib/kubelet**이 **Cinder CSI Node Controller** 컨테이너에 두 번 마운트되었습니다. 이로 인해 **/var/lib/kubelet/pods**가 공간이 부족함을 나타내는 오류로 인해 **CSI Node Controller**가 시작하지 못했습니다. 수정을 통해 **CSI Node Controller**를 성공적으로 실행할 수 있는 **/var/lib/kubelet** 및 **/var/lib/kubelet/pods**의 중복 마운트가 제거됩니다. (BZ#1952211)

- 이전 버전에서는 Cinder CSI 드라이버의 PV(영구 볼륨) 재조정 중에 **findmnt** 명령이 여러 볼륨 마운트를 수신하여 올바른 볼륨을 선택할 수 없어 크기 조정이 중지되었습니다. 결과적으로 사용자

가 파일 시스템을 수동으로 확장해야 했습니다. 이 수정을 통해 이제 명령에서 첫 번째 마운트를 사용하므로 파일 시스템의 크기를 PV와 함께 조정할 수 있습니다. (BZ#1919291)

- Cinder CSI Driver Operator는 이제 **VolumeSnapshotClass** 오브젝트를 수동으로 생성하지 않고 기본 스토리지 클래스를 생성할 때 Cinder CSI용 기본 **VolumeSnapshotClass** 오브젝트를 자동으로 프로비저닝합니다. (BZ#1905849)

- 이전에는 recycler-pod 템플릿이 kubelet 정적 매니페스트 디렉터리에 잘못 배치되었습니다. 이 잘못된 위치에서는 recycler의 정적 pod 시작 실패를 나타내는 정적 pod 로그 메시지가 생성되었습니다. 이번 업데이트를 통해 정적 Pod 매니페스트 디렉터리에서 잘못 배치된 recycler-pod 템플릿이 제거되었습니다. 결과적으로 오류 메시지가 더 이상 표시되지 않습니다. (BZ#1896226)

- 이전에는 사용 중인 디스크가 사용 가능한 디스크로 잘못 감지되었기 때문에 LSO(Local Storage Operator)에서 다른 프로비저너에 속하는 디스크를 클레임할 수 있었습니다. 이제 LSO에서 해당 디스크를 클레임할 수 없도록 디스크의 바인딩 마운트가 확인됩니다. (BZ#1929175)

- 이전 버전에서는 장치 ID에 다음과 같은 지원되지 않는 문자 (예: **:**)가 포함되어 있기 때문에 LSO(Local Storage Operator)에서 잘못된 레이블 값으로 PV(영구 볼륨)를 생성하려고 했습니다. 이 문제는 장치 정보를 레이블에서 주석으로 이동하여 수정되었습니다. (BZ#1933630)

- 이전 버전에서는 삭제 프로그램이 올바르게 등록되지 않았기 때문에 LSO(Local Storage Operator)에서 PV(영구 볼륨)를 정리하지 않았습니다. 이로 인해 PV가 **released** 상태로 유지됩니다. 이제 PV가 올바르게 큐에 추가되어 올바르게 삭제됩니다. (BZ#1937145)

- 이전 버전에서는 Pod가 삭제될 때 파이버 채널 볼륨이 노드에서 제대로 마운트 해제되지 않았습니다. 이 문제는 노드의 kubelet이 실행되지 않은 경우 API 서버에서 볼륨을 사용한 다른 Pod가 삭제될 때 발생했습니다. 이번 업데이트를 통해 새 kubelet이 시작될 때 파이버 채널 볼륨이 올바르게 마운트 해제됩니다. 또한 새 kubelet이 완전히 시작되고 볼륨을 마운트 해제하는 조합이 생성되어 파이버 채널 볼륨이 손상되지 않을 때까지 볼륨을 여러 노드에 마운트할 수 없습니다. (BZ#1954509)

웹 콘솔(관리자 화면)

- 이전 버전에서는 개발자 모드에서 콘솔 UI의 CNV 네임스페이스 내에서 사용자 정의 리소스를 삭제하려고 할 때 **삭제** 버튼을 클릭하면 **삭제** 버튼이 고착 상태로 표시되었습니다. 또한 CLI에서 동일한 작업을 수행할 때 표시되는 오류 메시지가 표시되지 않았습니다. 이번 업데이트를 통해 오류 메시지가 예상대로 표시되고 **D삭제** 버튼이 고착되지 않습니다. (BZ#1939753)

- 이전에는 OperatorHub 공급자 유형 **filter** 속성에 **CatalogSource**와의 관계가 명확하게 표시되지 않았습니다. 이 문제로 인해 사용자는 **filter** 기준을 구분할 수 없었습니다. 이 패치는 공급자 유형 **filter**를 **Source**로 업데이트합니다. 이를 통해 **filter**와 **CatalogSource** 간의 관계가 보다 명확하게 표시됩니다. (BZ#1919406)

- 이전에는 **리소스** 메뉴의 **리소스 목록 드롭다운** 구성 요소가 일부 언어에 대해 국제화되지 않았습니다. 이번 업데이트를 통해 영어 이외의 사용자의 환경을 개선하도록 **리소스** 메뉴가 업데이트되었습니다. (BZ#1921267)

- 이전에는 **영구 볼륨 클레임 삭제**와 같은 일부 메뉴 항목이 올바르게 국제화되지 않았습니다. 이제 더 많은 메뉴 항목이 올바르게 국제화되었습니다. (BZ#1926126)

- 이전에는 **HorizontalPodAutoscaler 추가** 페이지의 일부 텍스트 및 경고 메시지가 국제화되지 않았습니다. 텍스트는 이제 국제화되었습니다. (BZ#1926131)

- 이전 버전에서는 사용자가 Operator SDK를 사용하여 Operator를 생성하고 **xDescriptors={"urn:alm:<...와 같은 주석을 지정할 때>:hidden"}** Operator 인스턴스 생성 페이지에서 필드를 숨기는 경우 해당 필드가 여전히 페이지에 표시될 수 있습니다. 이제 Operator 인스턴스 생성 페이지에서 숨겨진 필드가 생략됩니다. (BZ#1966077)

- 이전에는 모바일 장치에 테이블이 잘못 표시되었습니다. 이번 업데이트를 통해 이제 테이블이 올바르게 표시됩니다. (BZ#1927013)

- 이전에는 OpenShift Container Platform 웹 콘솔의 실행 속도가 느릴 수 있었습니다. 이번 업데이트를 통해 웹 콘솔이 더 빠르게 시작됩니다. (BZ#1927310)

- 이전 버전에서는 OpenShift Container Platform 관리자에게 보내는 국제화된 알림 부족이 사용자 환경에 영향을 주었습니다. 이제 국제화가 가능합니다. (BZ#1927898)

- 이전 버전에서는 **클러스터 사용량** 대시보드의 국제화 지속 시간이 부족하여 사용자 환경에 영향을 주었습니다. 이제 국제화가 가능합니다. (BZ#1927902)

- 이전 버전에서는 OpenShift Container Platform 웹 콘솔의 OLM(Operator Lifecycle Manager) 상태 설명자가 호환되지 않는 데이터 유형이 할당되면 오류가 발생했습니다. 검증이 추가되어 처리에서 호환되지 않는 데이터 유형이 제거되어 오류가 발생하지 않습니다. 로깅된 경고는 호환되지 않는 상태 유형도 식별합니다. (BZ#1927941)

- 다음 OpenShift Container Platform 웹 콘솔 보기에서 다중 필터링을 지원합니다.

  - **홈 → 검색** (**리소스** 탭)
  - **홈 → 이벤트** (**리소스** 탭)
  - **워크로드** > **Pod** (**필터** 탭)

  자세한 내용은 BZ#1930007에서 참조하십시오.

- 다음 버그 수정에서는 OpenShift Container Platform 웹 콘솔의 다양한 변환 문제를 해결합니다.

  - BZ#1921780
  - BZ#1921781
  - BZ#1922992
  - BZ#1924585
  - BZ#1924747
  - BZ#1925083

- 이전에는 웹 콘솔이 채널 모달 드롭다운을 채우기 위해 하드 코딩된 채널 문자열에 의존했습니다. 결과적으로 사용자는 현재 버전에 대해 올바르지 않을 수 있는 채널 값을 볼 수 있었습니다. 이제 Cluster Version Operator가 지정된 버전에 올바른 채널을 제공하지 않으면 채널 모달 드롭다운이 텍스트 입력 필드로 변경되고 사용자에게 채널 및 도움말 텍스트를 제안합니다. 콘솔은 더 이상 하드 코딩된 채널 문자열에 의존하지 않습니다. (BZ#1932281)

- 이전에는 중국어 또는 일본어에 대한 타임스탬프 형식이 올바르지 않았습니다. 결과적으로 타임스탬프를 읽기가 어려웠고 이로 인해 사용자 환경이 저하되었습니다. 이번 업데이트를 통해 사용자 환경 개선을 위해 **Moment.js**로 중국어 및 일본어에 기본 타임스탬프 형식을 사용합니다. (BZ#1932453)

- 이전에는 FilterToolbar 구성 요소의 **rowFilters** 속성에서 **null** 값을 허용하지 않았습니다. 따라서 **rowFilters** 속성이 정의되지 않은 경우 무의미한 예외가 발생했습니다. 이제 FilterToolbar 구성 요소에서 **rowFilters** 속성이 참조되면 **null** 값이 허용됩니다. 결과적으로 **rowFilters** 속성이 정의되지 않은 경우 FilterToolbar 에서 예외가 발생하지 않습니다. (BZ#1937018)

- 이전에는 필드 수준 도움말 인스턴스에 잘못된 스타일의 도움말 텍스트가 적용되었습니다. 이제 필드 수준 도움말 인스턴스에 대해 도움말 텍스트의 올바른 스타일이 표시되고 콘솔 전체에 일관되게 적용됩니다. (BZ#1942749).

- 이전 버전에서는 OLM(Operator Lifecycle Manamgent) 상태 조건 설명자가 리소스 세부 정보 페이지에서 일반 세부 정보 항목으로 렌더링되었습니다. 그 결과 **Condition** 테이블이 절반 너비로 렌더링되었습니다. 이번 업데이트를 통해 조건 설명자는 **Operand** 세부 정보 페이지의 일반 **Conditions** 테이블 아래에 전체 범위 테이블로 렌더링됩니다. (BZ#1943238)

- 이전에는 "Ingresses"라는 단어가 중국 사용자를 위해 번역되었지만 사용자 환경에 맞지 않았습니다. 이제 "Ingress"라는 단어가 번역되지 않습니다. (BZ#1945816)

- 이전에는 "Operators"라는 단어가 중국어 사용자에 대해 번역되었지만 복수의 번역으로 인해 사용자 환경이 저하되었습니다. 이제 "Operators"라는 단어가 번역되지 않습니다. (BZ#1945818)

- 이전에는 잘못된 코드로 인해 **User** 및 **Group** 세부 정보에 관련이 없는 제목이 표시되었습니다. 이제 **User** 또는 **Group**을 필터링하기 위해 코드가 추가되어 **User** 및 **Group** 세부 정보에 관련 제목이 표시됩니다. (BZ#1951212)

- 이전에는 Pod Containers 텍스트가 국제화되지 않았으므로 사용자 환경이 좋지 않았습니다. 이제 Pod Containers 텍스트가 국제화되어 사용자 환경이 개선되었습니다. (BZ#1937102)

- 이전 버전에서는 **PackageManifest** 목록 페이지 항목이 세부 정보 페이지에 연결되지 않아 사용자가 목록 페이지에서 개별 **PackageManifest** 항목을 쉽게 탐색할 수 없었습니다. 이제 각 **PackageManifest** 항목이 다른 목록 페이지의 규칙과 일치하는 세부 정보 페이지에 연결됩니다. 사용자는 목록 페이지에서 PackageManifest 세부 정보 페이지에 쉽게 액세스할 수 있습니다. (BZ#1938321)

- **작업** 테이블의 **완료** 열은 **성공된** 완료 수 대신 **원하는** 완료 수를 기준으로 정렬되었습니다. 데이터는 **# Succeeded of # Desireded**로 표시되므로 해당 열을 기준으로 정렬할 때 두 번째 숫자를 기준으로 정렬되었기 때문에 결과가 혼동되었습니다. 이제 **작업 완료** 열이 **# Succeeded**에서 정렬되어 보다 잘 이해할 수 있습니다. (BZ#1902003)

- **Manage Columns** 모달의 입력 레이블은 클릭할 수 없으므로 해당 레이블을 클릭하여 열을 관리할 수 없었습니다. 이번 버그 수정을 통해 이제 열 관리에 사용할 수 있는 레이블을 클릭할 수 있습니다. (BZ#1908343)

- Google Cloud Platform에서 스토리지 클래스를 생성할 때 CSI 프로비전 프로그램이 나열되지 않았습니다. 이번 버그 수정으로 문제가 해결되었습니다. (BZ#1910500)

- 이전에는 사용자가 **사용자 관리 → 역할** 목록 보기에서 **클러스터** 역할을 클릭한 경우 세부 정보 페이지의 백 링크는 **클러스터 역할**에 대한 일반 목록 보기를 제공하는 **클러스터 역할**입니다. 이로 인해 이전 웹 콘솔 탐색이 잘못된 페이지로 리디렉션되었습니다. 이번 릴리스에서는 백 링크가**클러스터 역할/역할 바인딩**세부 정보 페이지에서 **역할/바인딩** 목록 보기로 사용자를 안내합니다. 이를 통해 사용자는 웹 콘솔에서 뒤로 올바르게 이동할 수 있습니다. (BZ#1915971)

- 이전에는 **생성된 날짜 시간이** 읽기 쉬운 형식으로 표시되지 않아 UTC에 표시된 시간을 이해하고 사용하기 어려웠습니다. 이번 릴리스에서는 UTC를 읽고 이해할 수 있도록 표시 시간이 다시 포맷됩니다. (BZ#1917241)

- 이전에는 웹 콘솔의 Pod 요청 및 제한 계산이 올바르지 않았습니다. 이는 완료된 Pod 또는 init 컨테이너를 제외하지 않은 결과입니다. 이번 릴리스에서는 계산에 필요하지 않은 Pod가 제외되어 pod 요청에 대한 웹 콘솔 계산 결과의 정확성이 향상됩니다. (BZ#1918785)

- 이전에는 정의되지 않은 값을 구문 분석하면 숫자(NaN) 예외가 발생하지 않았으며 **차트** 툴팁에 값이 없는 상자가 표시되었습니다. 이번 릴리스에서는 **차트** 도구에 올바른 값을 표시하도록 데이터를 가져올 때 시작 날짜가 지정됩니다. 이번 변경으로 결과가 동기화되고 정의되지 않은 값이

구문 분석되지 않습니다. (BZ#1906304)

- 이전 버그 수정 중에 Pod 로그에 대한 다운로드 링크가 빈 다운로드 속성이 포함된 표준 HTML 앵커 요소로 변경되었습니다. 결과적으로 다운로드 파일은 기본 파일 이름 형식을 찾을 수 없었습니다. 이번 업데이트에서는 앵커 요소 다운로드 속성에 파일 이름을 추가하여 pod 로그를 다운로드할 때 **<pod-name>-<container-name>.log** 형식으로 기본 파일 이름이 사용되도록 합니다. (BZ#1945630)

- 이전 버전에서는 사용자가 리소스를 생성할 수 있지만 편집 권한이 없는 경우 웹 콘솔 YAML 편집기가 읽기 전용 모드로 잘못 설정되었습니다. 이제 리소스에 대한 액세스 권한이 있는 사용자가 편집기 콘텐츠를 편집할 수 있습니다. (BZ#1824911)

- 이전에는 웹 콘솔이 대부분의 장소에 12시간 형식으로 표시했으며 경우에 따라 24시간 형식으로 표시되었습니다. 또한 1년 이상 지난 날짜에 대해서는 연도가 표시되지 않았습니다. 이번 릴리스에서는 날짜 및 시간이 일관되게 포맷되고 사용자 로케일 및 언어 기본 설정과 일치하며 1년 이상 지난 날짜에 대해서도 연도가 표시됩니다. (BZ#1862084)

- 이전에는 웹 콘솔에서 해당 이벤트를 볼 권한이 없는 사용자에 대해 **ClusterVersion** 리소스를 폴링하고 있었습니다. 이렇게 하면 콘솔 pod 로그에 많은 수의 오류가 출력됩니다. 이 문제를 방지하려면 리소스를 폴링하기 전에 사용자의 권한을 확인해야 합니다. 따라서 콘솔 Pod 로그에서 불필요한 오류가 제거됩니다. (BZ#1848151)

- 이전에는 YAML 편집기의 키보드 사용자가 편집기를 종료할 수 없었습니다. 편집기 외부에서 **view shortcuts** 팝업을 사용하여 편집기에서 사용자가 액세스할 수 없었습니다. 이번 업데이트를 통해 사용자는 **opt + F1** 키 입력을 사용하여 편집기 위에 **Accessibility help**를 표시할 수 있습니다. 이러한 변경으로 YAML 편집기의 키보드 사용자는 올바른 키 입력을 사용하여 편집기를 종료할 수 있습니다. (BZ#1874931)

- OCP(OpenShift Container Platform)의 4.x 릴리스 후 OCP 4 웹 콘솔에 업로드된 바이너리 시크릿 파일이 로드되지 않았습니다. 이로 인해 설치에 실패했습니다. OpenShift Container Platform 4.8에서는 이 기능이 OCP 4 웹 콘솔로 복원되었습니다. 이제 바이너리 파일 형식을 사용하여 필수 시크릿의 입력을 수행할 수 있습니다. (BZ#1879638)

- 이전에는 역할 바인딩 링크를 적절히 생성하도록 BZ#1871996이 수정되어 네임스페이스를 선택할 때 바인딩 유형을 일관되게 선택할 수 없었습니다. 따라서 활성 네임스페이스가 있는 사용자는 활성 네임스페이스를 **All namespaces**로 변경하지 않고 클러스터 역할 바인딩을 생성할 수 없었습니다. 이번 업데이트에서는 BZ#1871996 변경 사항의 일부를 되돌려서 사용자가 활성 네임스페이스와 관계없이 클러스터 역할 바인딩을 생성할 수 있도록 합니다. (BZ#1927882)

웹 콘솔 (개발자 화면)

- 이전에는 개발자 콘솔에서 서비스 클러스터를 로컬로 만들기 위해 레이블을 변경하면 사용자가 Knative 서비스를 생성할 수 없었습니다. 이번 업데이트에서는 사용자가 개발자 콘솔에서 Knative 서비스를 **cluster-local**로 생성할 수 있도록 cluster-local에 대해 지원되는 최신 레이블을 사용합니다. (BZ#1969951)

- 이전에는 IMV(Image Manifest Vulnerabilities)의 **낮음** 및 **중간** 수준의 심각도 문제에 대한 색상이 (Quay.io) 인터페이스에 표시된 색상과 일치하지 않았습니다. 결과적으로 사용자가 취약점의 심각도 순서를 **높음**으로 변경한 경우 IMV가 문제를 잘못 정렬했습니다. 이로 인해 IMV를 검토할 때 혼동이 발생했습니다. 현재 릴리스에서는 이 문제가 해결되었습니다. (BZ#1942716)

- 이전에는 Samples Operator가 설치되지 않았기 때문에 OpenShift 네임스페이스 템플릿을 사용할 수 없는 경우 개발자 화면의 **토폴로지** 보기가 로드되지 않았습니다. 이번 업데이트에서는 이 문제가 해결되었습니다. (BZ#1949810)

- 이전 버전에서는 devfile을 가져올 때 웹 콘솔이 환경 변수, 포트 및 제한에 대한 구성을 제공하는 **buildguidanceimage-placeholder** 컨테이너를 무시했습니다. 새로운 배포에 자리 표시자 이미

지를 가져올 수 없고 필요한 구성이 누락되어 새 배포에 두 번째 컨테이너를 시작할 수 없었습니다. 이제 **build guidance** 컨테이너가 새 배포에서 삭제되고 컨테이너는 환경 변수, 포트 및 제한 구성을 추가합니다. (BZ#1952214)

- 이전에는 다른 탭에서 **개발자** 화면을 전환하고 프로젝트 세부 정보를 다시 로드할 때 화면에 연결된 경로가 렌더링되지 않아 **404** 오류가 발생했습니다. 이번 업데이트에서는 모든 비활성 경로를 로드하고 올바른 화면으로 전환합니다. (BZ#1929769)

- 이전 버전에서는 사용자에게 네임스페이스에 필요한 액세스 권한이 없어 오류가 발생하면 **모니터링** 대시보드 페이지의 **워크로드** 드롭다운 메뉴에 진행 중인 로드 아이콘이 계속 표시되었습니다. 현재 릴리스에서는 이 문제가 해결되었습니다. 이제 **모니터링** 대시보드 페이지에 **Forbidden** 오류가 있음을 나타내는 메시지가 표시됩니다. (BZ#1930546)

- 이전 버전에서는 API 서버에서 **resource quota** 리소스를 업데이트하는 충돌이 있을 때 409 상태 코드를 반환하는 리소스를 생성할 수 없었습니다. 결과적으로 리소스를 만들지 못했으므로 API 요청을 다시 시도해야 할 수 있었습니다. 이번 업데이트를 통해 **OpenShift Console** 웹 애플리케이션은 409 상태 코드를 수신할 때 요청을 3번 재시도하려고 시도하므로 요청을 완료하기에 충분한 경우가 많습니다. 409 상태 코드가 계속 발생하는 경우 콘솔에 오류가 표시됩니다. (BZ#1920699)

- 이전에는 **YAML** 탭을 선택할 때 **metadata.managedFields** 섹션이 즉시 축소되지 않았습니다. 이는 **Pipeline Builder** 및 **Edit HorizontalPodAutoscaler** (HPA)와 같은 페이지의 **Form** 또는 **YAML** 전환기와 관련된 문제로 인해 발생했습니다. 그 결과 입력하려고 했던 문서 부분이 축소되었습니다. **metadata.managedFields** 섹션은 그대로 유지되었으며 커서는 **YAML** 편집기의 왼쪽 맨 위의 시작 위치로 재설정되었습니다. 현재 릴리스에서는 이 문제가 해결되었습니다. 이제 **YAML**을 로드할 때 **metadata.managedFields** 섹션이 즉시 축소됩니다. (BZ#1932472)

- 이전에는 프라이빗 리포지토리에 대한 **Git 가져오기** 흐름에서 생성된 파이프라인을 실행하지 못했습니다. 이는 pipeline **ServiceAccount** 오브젝트가 개인 Git 리포지토리에 대해 **Git 가져오기** 흐름에 의해 생성된 시크릿을 사용하지 않았기 때문에 발생했습니다. 이번 업데이트를 통해 pipeline **ServiceAccount** 오브젝트의 주석에 시크릿 이름을 추가하고 제공된 시크릿에 파이프라인별 주석을 추가할 수 있습니다. 결과적으로 프라이빗 Git 리포지토리의 파이프라인이 성공적으로 실행됩니다. (BZ#1970470)

- 이전에는 사용자가 **YAML** 편집기에 포맷된 **YAML** 스니펫을 삽입할 때 새 선택 사항이 스니펫의 새 콘텐츠와 일치하지 않았습니다. 들여쓰기가 제거되었으며 선택 항목에 임의의 글자가 표시됩니다. 현재 릴리스에서는 이 문제가 해결되었습니다. 이제 커서가 시작된 위치에 남아 있으며 커서 끝 위치에 누락된 들여쓰기가 추가됩니다. **YAML** 스니펫을 삽입한 후 새 선택 항목이 새 콘텐츠와 일치합니다. (BZ#1952545)

- 이전 버전에서는 Knative 서비스의 사양과 메타데이터에 주석이 전달되었습니다. 그 결과 **토폴로지**에서 Knative 서비스의 관련 개정을 위해 데코레이터가 표시되었습니다. 이번 릴리스에서는 주석을 Knative 서비스 메타데이터에만 전달하여 이 문제를 해결했습니다. 이제 데코레이터는 **토폴로지**의 Knative 서비스에만 표시되고 관련 수정 사항은 표시되지 않습니다. (BZ#1954959)

- 이전에는 매개 변수가 비어 있는 파이프라인을 생성한 경우 (예: ”) OpenShift Container Platform 웹 콘솔의 필드에서 빈 문자열을 허용하지 않았습니다. 현재 릴리스에서는 이 문제가 해결되었습니다. 이제 ”는 매개 변수 섹션에서 유효한 기본 속성으로 지원됩니다. (BZ#1951043)

- 이전에는 **개발자** 관점에서 Knative 서비스를 개인 서비스로 생성할 수 없었습니다. 이 문제는 **'networking.knative.dev/visibility': 'cluster-local'** 레이블을 업데이트하여 해결되었습니다. (BZ#1970796)

- 이전에는 유형 소스와 함께 이벤트 소스의 카탈로그에 싱크 유형 Kamelets가 표시되었습니다. 이 문제는 Kamelets 리소스를 필터링하여 소스 유형만 나열하여 해결되었습니다. (BZ#1972258)

Windows 컨테이너

- 이전에는 사용자가 추가 Windows 노드를 확장할 때 로드 밸런서 서비스가 불안정해졌습니다. 이번 업데이트를 통해 로드 밸런서 서비스를 안정화하여 사용자가 잘못된 성능 없이 여러 개의 Windows 노드를 추가할 수 있습니다. (BZ#1905950)
- 이전에는 Windows Pod가 실행된 후 생성된 경우 로드 밸런서가 생성된 후 **kube-proxy** 서비스가 예기치 않게 충돌했습니다. 이번 업데이트를 통해 로드 밸런서 서비스를 다시 생성할 때 kube-proxy 서비스가 충돌하지 않습니다. (BZ#1939968)
- 이전에는 로드 밸런서의 Ingress에 있는 빈 IP 주소 값이 데이터 경로를 중단했습니다. 그 결과 Windows 서비스에 연결할 수 없었습니다. 이번 업데이트를 통해 IP 주소 값이 비어 있어도 Windows 서비스에 연결할 수 있습니다. (BZ#1952914)
- 이전 버전에서는 사용자가 예상 볼륨이 있는 Windows Pod를 생성할 때 Pod가 **ContainerCreating** 단계에 남아 있었습니다. 이번 업데이트를 통해 Windows Pod 생성이 **Running** 단계로 진행됩니다. (BZ#1973580)

1.8. 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**: *정식 출시일 (GA)*
- **-**: *사용할 수 없음*
- **DEP**: *더 이상 사용되지 않음*

표 1.2. 기술 프리뷰

기능	OCP 4.6	OCP 4.7	OCP 4.8
일반 시계가 있는 PTP(Precision Time Protocol) 하드웨어	TP	TP	GA
oc CLI 플러그인	TP	TP	GA
Descheduler	TP	GA	GA
OVN-쿠버네티스 포드 네트워크 공급자	GA	GA	GA
메모리 활용을 위한 HPA	TP	GA	GA
서비스 바인딩	TP	TP	TP
로그 전송	GA	GA	GA
사용자 정의 프로젝트 모니터링	GA	GA	GA

기능	OCP 4.6	OCP 4.7	OCP 4.8
Cinder 포함 원시 블록	TP	TP	GA
CSI 볼륨 스냅샷	TP	GA	GA
CSI 볼륨 복제	GA	GA	GA
CSI 볼륨 확장	TP	TP	TP
vSphere Problem Detector Operator	-	GA	GA
CSI Azure Disk Driver Operator	-	-	TP
CSI GCP PD Driver Operator	-	TP	GA
CSI OpenStack Cinder Driver Operator	-	GA	GA
CSI AWS EBS Driver Operator	TP	TP	TP
CSI 자동 마이그레이션	-	-	TP
Red Hat Virtualization(oVirt) CSI Driver Operator	GA	GA	GA
CSI 인라인 임시 볼륨	TP	TP	TP
CSI vSphere Driver Operator	-	-	TP
Local Storage Operator를 통한 자동 장치 검색 및 프로비저닝	TP	TP	TP
OpenShift Pipelines	TP	GA	GA
OpenShift GitOps	TP	GA	GA
OpenShift 샌드박스 컨테이너	-	-	TP
Vertical Pod Autoscaler	TP	TP	GA
Cron 작업	TP	TP	GA
PodDisruptionBudget	TP	TP	GA
Operator API	GA	GA	GA
kvc로 노드에 커널 모듈 추가	TP	TP	TP

기능	OCP 4.6	OCP 4.7	OCP 4.8
egress 라우터 CNI 플러그인	-	TP	GA
스케줄러 프로파일	-	TP	TP
선점되지 않은 우선 순위 클래스	-	TP	TP
Kubernetes NMState Operator	-	TP	TP
지원되는 설치 관리자	-	TP	TP
AWS STS(보안 토큰 서비스)	-	TP	GA
Kdump	-	TP	TP
OpenShift Serverless	-	-	GA
서버리스 기능	-	-	TP
Jenkins Operator	TP	TP	DEP
CPU 관리자	GA	GA	GA
드라이버 툴킷	-	-	TP

1.9. 확인된 문제

- OpenShift Container Platform 4.1에서는 익명 사용자가 검색 엔드 포인트에 액세스할 수 있었습니다. 이후 릴리스에서는 일부 검색 끝점이 통합된 API 서버로 전달되기 때문에 보안 악용에 대한 가능성을 줄이기 위해 이 액세스를 취소했습니다. 그러나 인증되지 않은 액세스는 기존 사용 사례가 손상되지 않도록 업그레이드된 클러스터에 보존됩니다.
  OpenShift Container Platform 4.1에서 4.8로 업그레이드된 클러스터의 클러스터 관리자인 경우 인증되지 않은 액세스를 취소하거나 계속 허용할 수 있습니다. 특별히 필요한 경우가 아니면 인증되지 않은 액세스를 취소하는 것이 좋습니다. 인증되지 않은 액세스를 계속 허용하는 경우 이에 따라 보안 위험이 증가될 수 있다는 점에 유의하십시오.

  주의

  인증되지 않은 액세스에 의존하는 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 edit**를 사용하여 주석을 추가합니다. (BZ#1917280)

- 사용자 프로비저닝 인프라를 사용하여 vSphere의 가상 머신의 전원을 켜는 경우 노드를 확장하는 프로세스가 예상대로 작동하지 않을 수 있습니다. 하이퍼바이저 구성에서 알려진 문제로 인해 시스템이 하이퍼바이저 내에 생성되지만 전원이 켜지지 않습니다. 머신 세트를 확장한 후 노드가 **Provisioning** 상태에 있는 것으로 표시되면 vSphere 인스턴스 자체에서 가상 머신의 상태를 조사할 수 있습니다. VMware 명령 **govc tasks** 및 **govc events** 이벤트를 사용하여 가상 시스템의 상태를 확인합니다. 다음과 유사한 오류 메시지가 있는지 확인합니다.

  ```
  Invalid memory setting: memory reservation (sched.mem.min) should be equal to
  memsize(8192).
  ```

  이 VMware KBase 문서의 지침에 따라 문제를 해결할 수 있습니다. 자세한 내용은 Red Hat Knowledgebase 솔루션 [UPI vSphere] 노드 확장이 예상대로 작동하지 않음 을 참조하십시오. (BZ#1918383)

- ECKD 유형 DASD를 VirtIO 블록 장치로 사용하면 IBM Z에서 RHEL KVM 설치에 RHCOS를 설치 실패합니다. (BZ#1960485)

- OVN(Open Virtual Network) 버그로 인해 Octavia 로드 밸런서에 지속적으로 연결 문제가 발생합니다. Octavia 로드 밸런서가 생성되면 OVN을 일부 Neutron 서브넷에 연결하지 못할 수 있습니다. 이러한 로드 밸런서는 일부 Neutron 서브넷에 연결할 수 없습니다. 이 문제는 Kuryr가 설정될 때 각 OpenShift 네임스페이스에 대해 임의로 생성되는 Neutron 서브넷에 영향을 미칩니다. 결과적으로 이 문제가 발생하면 OpenShift **Service** 오브젝트를 구현하는 로드 밸런서가 문제의 영향을 받는 OpenShift 네임스페이스에서 연결할 수 없습니다. 이 버그로 인해 버그가 수정될 때까지 OVN 및 OVN Octavia가 구성된 RHOSP(Red Hat OpenStack Platform) 16.1에서는 Kuryr SDN을 사용하는 OpenShift Container Platform 4.8 배포가 권장되지 않습니다. (BZ#1937392)

- Console Operator는 콘솔 경로(**console** 또는 **downloads**) 중 하나에 대해 **componentRoutes** 조건으로 **Ingress** 리소스를 올바르게 업데이트하지 않습니다. (BZ#1954148)

- OVN-Kubernetes 네트워크 공급자는 **NodePort**- 및 **LoadBalancer**-유형 서비스에 대한 **externalTrafficPolicy** 기능을 지원하지 않습니다. **service.spec.externalTrafficPolicy** 필드는 서비스의 트래픽이 노드-로컬 또는 클러스터 전체 엔드포인트로 라우팅되는지 여부를 결정합니다. 현재 이러한 트래픽은 기본적으로 클러스터 전체 엔드포인트로 라우팅되며 노드 로컬 엔드포인트로 트래픽을 제한할 수 없습니다. 이 문제는 향후 릴리스에서 해결될 예정입니다. (BZ#1903408)

- 현재 Kubernetes 포트 충돌 문제로 인해 Pod가 재배포된 후에도 Pod 간 통신이 중단될 수 있습니다. 자세한 내용과 해결 방법은 Red Hat 지식 베이스 솔루션 Port collisions between pod and cluster IPs on OpenShift 4 with OVN-Kubernetes에서 참조하십시오. (BZ#1939676, BZ#1939045)

- OVN-Kubernetes 네트워크 공급자를 사용하고 컴퓨팅 노드가 RHEL 7.9를 실행하는 클러스터의 경우 OpenShift Container Platform 4.7에서 OpenShift Container Platform 4.8으로 업그레이드가 BZ#1976232에 의해 차단됩니다. 릴리즈 4.8로 업그레이드하려면 이 버그의 수정 사항이 포함된 4.8 패치를 기다려야 합니다. (BZ#1976232)

- OVN-Kubernetes 네트워크 공급자를 사용하고 OpenShift Container Platform 4.7에서 OpenShift Container Platform 4.8로 업그레이드하는 클러스터의 경우 OVN-Kubernetes의 버그로 인해 pod IP 주소가 오래될 수 있습니다. 그 버그는 거의 경험되지 않은 경합 조건입니다. 결과적으로 4.8 릴리스로 업그레이드하는 동안 노드가 드레이닝되지 않고 일부 Operator에서 **Degraded** 상태를 보고합니다. 해결 방법으로 **CrashLoopBackOff** 상태에 있고 업그레이드를 완료하지 않은 Pod를 식별합니다. **oc delete <pod-name>** 명령을 사용하여 각 pod를 삭제합니다. (BZ#1974403)

- **kubeletconfig** 리소스의 **tlsSecurityProfile** 필드에 대한 설명 (예: **oc explain** 명령을 사용하는 경우)은 TLS 보안 프로필에 대한 올바른 암호를 나열하지 않습니다. 이 문제를 해결하려면 영향을 받는 노드의 **/etc/kubernetes/kubelet.conf** 파일에서 암호 목록을 확인하십시오. (BZ#1971899)

- 단일 노드에서 CNF 테스트를 정규 모드로 실행할 때 클러스터 준비 여부를 파악하는 논리에 세부 정보가 누락되어 있습니다. 특히 SR-IOV 네트워크를 생성하면 1분 이상의 시간이 경과할 때까지 네트워크 연결 정의가 생성되지 않습니다. 모든 DPDK 테스트는 계단식으로 실패합니다. **-ginkgo.skip** 매개변수를 사용하여 단일 노드에서 설치에 대해 실행할 때 DPDK 기능을 건너뛰는 일반 모드에서 CNF 테스트를 실행합니다. 검색 모드에서 CNF 테스트를 실행하여 단일 노드에 대한 설치에 대해 테스트를 실행합니다. (BZ#1970409)

- 현재 CNF-tests는 SR-IOV 및 DPDK 테스트용 MLX NIC로 보안 부팅을 지원하지 않습니다. **-ginkgo.skip** 매개변수를 사용하여 보안 부팅이 활성화된 환경에 대해 실행할 때 CNF 테스트를 실행할 수 있습니다. 검색 모드에서 실행하면 MLX 카드로 보안 부팅이 활성화된 환경에 대해 테스트를 실행하는 것이 좋습니다. 이 문제는 향후 릴리스에서 해결될 예정입니다. (BZ#1975708)

- **ArgoCD** Operator를 등록하고 ArgoCD 및 AppProject가 시작되면 이미지가 더 제한적인 OpenShift Container Platform 환경에서 작동하지 않기 때문에 **guestbook**이라는 예제 애플리케이션을 시작할 수 없습니다. 임시 해결 방법으로 다음 예제를 배포하여 **ArgoCD** Operator가 제대로 작동하는지 확인할 수 있습니다.

```
PROJ=younamespace
cat > $PROJ-app.yaml <<EOF
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: simple-restricted-webserver
  namespace: $PROJ
spec:
```

```
  destination:
    namespace: $PROJ
    server: https://kubernetes.default.svc
  project: default
  source:
    path: basic-nginx
    repoURL: 'https://github.com/opdev/argocd-example-restricted-apps.git'
    targetRevision: HEAD
EOF
oc create -f $PROJ-app.yaml
```

자세한 내용은 BZ#1812212을 참조하십시오.

- 사용자가 여러 탭에 콘솔을 열고 있는 경우 **개발자** 화면의 일부 사이드바 링크가 프로젝트에 직접 연결되지 않으며 선택한 프로젝트에서 예기치 않은 변경 사항이 발생합니다. 이 문제는 향후 릴리스에서 해결될 예정입니다. (BZ#1839101)

- **pathType을 사용하는 경우 Ingress를 사용하여 패스스루 경로를 생성할 수 없습니다. prefix**. 대신 **pathType**을 **ImplementationSpecific**으로 설정하고 **path**를 ''로 설정하여 패스스루 경로를 생성할 수 있습니다.

  Ingress YAML 파일 샘플

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress7
  namespace: test-ingress
  annotations:
    route.openshift.io/termination: passthrough
spec:
  rules:
  - host: <ingress-psql-example-test-ingress.apps>
    http:
      paths:
      - path: ''
        pathType: ImplementationSpecific
        backend:
          service:
            name: <ingress-psql-example>
            port:
              number: 8080
```

자세한 내용은 BZ#1878685을 참조하십시오.

- 현재 **검색** 페이지에서 **이름** 필터를 적용하거나 제거한 후 **Pipeline** 리소스 테이블이 즉시 업데이트되지 않습니다. 그러나 페이지를 새로 고치거나 Pipeline을 닫고 **Pipelines** 섹션을 확장하면 **이름** 필터가 적용됩니다. **Name** 필터를 삭제할 때도 동일한 동작이 표시됩니다. 이 문제는 향후 릴리스에서 해결될 예정입니다. (BZ#1901207).

- 이제 문서에는 **Provisioning** 사용자 정의 리소스의 **ProvisioningNetworkCIDR** 값이 설명되어 있습니다. 이렇게 하면 IPv6 프로비저닝 네트워크가 **dnsmasq**로 인해 /64 제한값으로 제한됩니다. (BZ#1947293)

- 문제 해결을 지원하기 위해 설치 프로그램에서 boostratp 실패에서 수집된 로그에 컨트롤 플레인 및 부트스트랩 호스트의 IP 주소 및 경로가 포함됩니다. (BZ#1956079)

- 자체 서명된 Amazon Commercial Cloud Services 클러스터를 사용하는 경우 내부 이미지 레지스트리에서 가져오거나 푸시할 수 없습니다. 이 문제를 해결하려면 **configs.imageregistry/cluster** 리소스에 **spec.disableRedirect**를 **true**로 설정해야 합니다. 따라서 S3 저장소에서 직접 가져오지 않고 이미지 레지스트리에서 이미지 레이어를 가져올 수 있습니다. (BZ#1924568)

- 이전에는 OpenShift Container Platform 웹 콘솔에서 Bitbucket 리포지토리를 사용하여 배포에 생성된 토폴로지 URL에 슬래시 문자가 포함된 분기 이름이 포함된 경우 작동하지 않았습니다. 이는 Bitbucket API (BCLOUD-9969)와 관련된 문제로 인해 발생했습니다. 현재 릴리스에서는 이 문제가 완화되었습니다. 분기 이름에 슬래시가 포함된 경우 토폴로지 URL은 리포지토리의 기본 분기 페이지를 가리킵니다. 이는 향후 OpenShift Container Platform 릴리스에서 제거될 예정입니다. (BZ#1969535).

- RHV(Red Hat Virtualization)에 OCP(OpenShift Container Platform) 버전 4.6을 설치하려면 RHV 버전 4.4가 필요합니다. RHV 4.3에서 이전 버전의 OCP를 실행하는 경우 OCP 버전 4.6으로 업데이트하지 마십시오. Red Hat은 RHV 버전 4.3에서 OCP 버전 4.6 실행을 테스트하지 않았으며 이 조합을 지원하지 않습니다. 테스트된 통합에 대한 자세한 내용은 OpenShift Container Platform 4.x Tested Integrations (x86_x64 용)에서 참조하십시오.

- **operator-sdk pkgman-to-bundle** 명령은 **--build-cmd** 플래그를 사용하여 실행하면 오류로 종료됩니다. 자세한 내용은 (BZ#1967369)을 참조하십시오.

- 현재 웹 콘솔 퀵스타트 카드의 사전 요구 사항이 목록 대신 단락으로 표시됩니다. 이 문제는 향후 릴리스에서 해결될 예정입니다. (BZ#1905147)

- OpenShift Container Platform 단일 노드 구성에서 비실시간 커널을 사용할 때보다 실시간 커널(커널-rt)을 사용할 때 Pod 생성 시간이 2배 이상 느립니다. kernel-rt를 사용하는 경우 노드 재부팅 후 복구 시간이 영향을 받기 때문에 생성 속도가 느린 경우 최대 Pod 수에 영향을 미칩니다. kernel-rt를 사용하는 경우 **rcupdate.rcu_normal_after_boot=0 커널 인수를 사용하여 부팅하여 영향을 받은 복구 시간을 개선할 수 있습니다.** 이 인수에는 실시간 커널 버전 **kernel-rt-4.18.0-305.16.1.rt7.88.el8_4** 이상이 필요합니다. 이 알려진 문제는 OpenShift Container Platform 버전 4.8.15 이상에 적용됩니다. (BZ#1975356)

- OpenShift Container Platform 단일 노드 재부팅 후 모든 Pod가 다시 시작되어 일반 Pod 생성 시간보다 오래 걸립니다. 이 문제는 CNI(컨테이너 네트워크 인터페이스)에서 **pod add** 이벤트를 충분히 신속하게 처리할 수 없기 때문에 발생합니다. **timed out waiting for OVS port binding**이라는 오류 메시지가 표시됩니다. OpenShift Container Platform 단일 노드 인스턴스는 결국 복구되지만 예상보다 느리게 복구됩니다. 이 알려진 문제는 OpenShift Container Platform 버전 4.8.15 이상에 적용됩니다. (BZ#1986216)

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

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

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

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

(BZ#2017708)

- RHCOS 및 MCO (Machine Config Operator)의 이미지가 OpenShift Container Platform 4.8.z 릴리스에서 이후 4.8.z 릴리스로 업그레이드하는 동안 변경되지 않으면 컨트롤 플레인 노드가 업그레이드를 완료하기 전에 업그레이드가 완료로 표시됩니다. 이렇게 하면 업그레이드가 실제로 완료되기 전에 클러스터에서 작업을 수행하면 업그레이드가 실패할 수 있습니다. 이 문제를 해결하려면 클러스터에서 추가 작업을 수행하기 전에 컨트롤 플레인 노드에서 업데이트가 완료되었는지 확인합니다. **oc get mcp/master** 명령을 사용하여 각 풀의 클러스터에서 사용할 수 있는 MCO 관리 노드의 상태를 검토할 수 있습니다. (BZ#2025396)

- 4.7 OpenShift Container Platform 클러스터에서 4.8로 업그레이드한 후 OpenShift Container Platform 노드의 보조 NIC(네트워크 인터페이스 컨트롤러)를 통해 내부 네트워크에서 외부 네트워크 Pod로의 라우팅 경로가 기본적으로 비활성화됩니다. 이는 4.8부터 시작하는 OVN(Open Virtual Network) 설계에서 공유 게이트웨이가 기본 게이트웨이 모드이기 때문입니다. 해당 라우팅 경로가 필요한 경우 업그레이드 전이나 후에 해결 방법으로 **openshift-network-operator** 네임스페이스에 **gateway-mode-config** 구성 맵을 생성하여 OVN Gateway 모드를 로컬로 강제 적용합니다.
  다음 명령을 입력하여 **openshift-network-operator** 네임스페이스에 **gateway-mode-config** 를 생성합니다.

```
$ cat localGW.yml
```

```
apiVersion: v1
kind: ConfigMap
metadata:
   name: gateway-mode-config
   namespace: openshift-network-operator
data:
   mode: "local"
immutable: true
```

```
$ oc apply -f localGW.yml
```

```
configmap/gateway-mode-config created
```

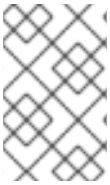
  추가 지침은 (KCS) 및 (BZ#2089389)를 참조하십시오. 이 설정은 향후 릴리스에서 더 자세히 다룹니다.

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

1.10. 비동기 에라타 업데이트

OpenShift Container Platform 4.8의 보안, 버그 수정 및 개선 사항 업데이트는 Red Hat Network를 통해 비동기 에라타로 릴리스됩니다. 모든 OpenShift Container Platform 4.8 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 통지가 활성화되면 사용자는 등록된 시스템과 관련된 새 에라타가 릴리스될 때마다 이메일을 통해 통지를 받습니다.



참고

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

이 섹션은 향후 OpenShift Container Platform 4.8과 관련된 비동기 에라타 릴리스의 개선 사항 및 버그 수정에 대한 정보 제공을 위해 지속적으로 업데이트됩니다. OpenShift Container Platform 4.8.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.

1.10.1. RHSA-2021:2438 - OpenShift Container Platform 4.8.2 이미지 릴리스, 버그 수정 및 보안 업데이트 권고

출시 날짜: 2021-07-27

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.2를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2021:2438 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:2437 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.2 --pullspecs
```

1.10.2. RHBA-2021:2896 - OpenShift Container Platform 4.8.3 버그 수정 업데이트

출시 날짜: 2021-08-02

OpenShift Container Platform 릴리스 4.8.3이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2021:2896 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:2899 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.3 --pullspecs
```

1.10.2.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.3. RHSA-2021:2983 - OpenShift Container Platform 4.8.4 보안 및 버그 수정 업데이트

출시 날짜: 2021-08-09

OpenShift Container Platform 릴리스 4.8.4가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2021:2983 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:2984 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.4 --pullspecs
```

1.10.3.1. 버그 수정

- 이전 버전에서는 BZ#1954309 및 BZ#1960446이 OpenShift Container Platform 4.8.3 릴리스 노트에서 수정된 버그 목록에 있었지만 버전 4.8.3 릴리스에서 생략되었습니다. 이번 릴리스에서는 **BZ#1960446**의 버그 수정 요약이 OpenShift Container Platform 4.8.4 릴리스 노트의 "버그 수정" 섹션으로 이동되고 **BZ#1954309**의 버그 수정 요약이 제거됩니다.

- 이전에는 **nmstate-handler** Pod에 잘못된 허용 오차 설정이 있어서 **nmstate** Operator가 있는 노드에서 네트워크 구성을 수행하지 못했습니다. 이번 업데이트를 통해 처리기 Pod는 모든 노드에서 허용됩니다. (BZ#1960446)

- 이전에는 웹 콘솔에서 실패한 **ClusterServiceVersion** 오브젝트 (CSV)에 대해 **The operator is running in openshift-operators but is managing this namespace**라고 표시되었습니다. 이 메시지는 구체적으로 설명되지 않았으며 사용자가 실패한 CSV의 문제를 해결하는 데 도움이 되지 않았습니다. 이번 릴리스에서는 복사된 CSV에 대한 메시지가 사용자를 원본 CSV로 전달하여 실패의 원인을 찾고 원본 CSV에 대한 링크를 제공합니다. (BZ#1972478)

- 이전 버전에서 Operator는 레지스트리에서 **spec.tolerations** 대신 사용자 정의 허용 오차가 검사된 **spec.nodeSelector**를 사용해야 하는지 확인했지만 **spec.tolerations**의 사용자 정의 허용 오차는 **spec.nodeSelector**가 설정된 경우에만 적용됩니다. 이번 릴리스에서는 **spec.tolerations**가 확인되고 **spec.tolerations**가 설정된 경우 Operator에서 사용자 정의 허용 오차를 사용합니다. (BZ#1973662)

- 이전 버전에서는 이미지 스트림없이 배포가 생성되었으며 **image.openshift.io/triggers** 주석이 없이 배포가 생성된 경우 배포 컨트롤러에서 복제본 세트를 무한 루프로 생성했습니다. 이번 릴리스에서 이 문제가 해결되었습니다. (BZ#1981770)

- 이번 릴리스에서는 **must-gather** 로드에 Manila CSI 로그가 추가됩니다. (BZ#1986026)

- 이전에는 VM에 대한 자동 고정을 사용할 때 속성 이름이 **disabled**, **existing**, 또는 **adjust**이었습니다. 이번 릴리스에서는 이름은 각 정책을 더 잘 설명하고 oVirt에서 차단되었기 때문에 **existing** 이름이 제거되었습니다. 새 속성 이름은 **none**이고 **resize_and_pin**은 oVirt 사용자 인터페이스와 일치합니다. (BZ#1987182)

1.10.3.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.4. RHBA-2021:3121 - OpenShift Container Platform 4.8.5 버그 수정 업데이트

출시 날짜: 2021-08-16

OpenShift Container Platform 릴리스 4.8.5가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2021:3121 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:3122 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.5 --pullspecs
```

1.10.4.1. 기능

1.10.4.1.1. 송신 IP 개선 사항

새로운 개선 사항은 OpenShift Container Platform 4.8 Anonymizer에 송신 IP 주소 지원을 추가합니다. 자세한 내용은 (BZ#1974877)을 참조하십시오.

1.10.4.2. 버그 수정

- 이전에는 **JenkinsPipelineStrategy**가 정의된 **BuildConfig** 오브젝트에 **oc logs**가 작동하지 않았습니다. 이번 업데이트를 통해 **oc logs**가 이제 파이프라인 빌드에서 작동합니다. (BZ#1974267)
- 이전 버전에서는 VIP(가상 IP)를 보유한 **Keepalived** 컨테이너가 **SIGTERMed**로 표시되면 VRRP 사전 조치 메시지가 전송되지 않았습니다. 결과적으로 VIP가 시간 초과 후 다른 노드로 마이그레이션되었습니다. 이번 업데이트를 통해 **SIGTERMed**로 표시된 VIP를 보유한 **Keepalived** 컨테이너가 **VRRP priority 0** 광고 메시지를 보냅니다. 결과적으로 이제 더 빠른 VIP 마이그레이션이 가능합니다. (BZ#1920670)
- 이전에는 **Kameletbinding**을 사용하여 **action** 및 **sink** Kamelets를 생성할 수 있었지만 **source** 유형의 Kamelet만 나열되어야 했습니다. 이번 업데이트에서는 **sink** 및 **action** 유형 Kamelets를 선택하는 옵션이 제거됩니다. 결과적으로 **source** Kamelets가 이벤트 소스에 대해 카탈로그에 표시되는 유일한 유형입니다. (BZ#1972258)

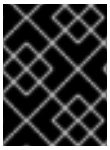
1.10.4.3. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.5. RHBA-2021:3247 - OpenShift Container Platform 4.8.9 보안 및 버그 수정 업데이트

출시 날짜: 2021-08-31

OpenShift Container Platform 릴리스 4.8.9가 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3247 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:3248 권고를 통해 제공됩니다.



중요

RHBA-2021:3247 권고의 SHA-256 이미지 다이제스트 정보가 잘못되었습니다. 올바른 정보는 다음과 같습니다.

릴리스 이미지 메타데이터를 검사하려면 **oc** 툴을 다운로드하고 다음 명령을 실행합니다.

- x86_64 아키텍처의 경우:
  -

```
$ oc adm release info quay.io/openshift-release-dev/ocp-release:4.8.9-x86_64
```

이미지 다이제스트는 **sha256:5fb4b4225498912357294785b96cde6b185eaed20bbf7a4d008c462134a4edfd**입니다.

- s390x 아키텍처의 경우:

```
$ oc adm release info quay.io/openshift-release-dev/ocp-release:4.8.9-s390x
```

이미지 다이제스트는 **sha256:2665d✓917890b3d06c339bb03dac65b84485fef36c90f219f2773393ba291d**입니다.

- ppc64le 아키텍처의 경우:

```
$ oc adm release info quay.io/openshift-release-dev/ocp-release:4.8.9-ppc64le
```

이미지 다이제스트는 **sha256:ded5e8d61915f74d938668cf58cdc9f37eb4172bc24e80c16c7fe1a6f84eff43**입니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.9 --pullspecs
```

1.10.5.1. 버그 수정

- 이 릴리스에는 중국어, 일본어, 한국어로 로컬라이제이션된 컨텐츠가 추가되었습니다. (BZ#1972987)
- OpenShift Container Platform 4.5용 OVN-Kubernetes에 사용된 주소 집합 명명 규칙은 OpenShift Container Platform 4.6에서 변경되었지만 기존 주소 세트를 새 명명 규칙으로 마이그레이션하는 것은 업그레이드의 일부로 처리되지 않았습니다. 수신 또는 송신 섹션에 대한 네임스페이스 선택기 기준이 지정된 버전 4.5에서 생성된 네트워크 정책은 해당 네임스페이스 내의 Pod IP 주소로 최신 상태로 유지되지 않은 이전 주소 집합과 일치합니다. 이러한 정책은 4.6 이상 릴리스에서 제대로 작동하지 않을 수 있으며 예기치 않은 트래픽을 허용하거나 삭제할 수 있습니다. 이전에는 이러한 정책을 제거하고 다시 만드는 해결방법이 있었습니다. 이번 릴리스에서는 이전 명명 규칙이 있는 주소 세트가 제거되고 이전 주소 집합을 참조하는 정책 ACL이 OVN-Kubernetes 업그레이드 중에 새 명명 규칙에 따라 주소 집합을 참조하도록 업데이트됩니다. 버전 4.5에서 생성된 영향을 받는 네트워크 정책이 업그레이드 후 올바르게 작동합니다. (BZ#1976241)

1.10.5.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.6. RHBA-2021:3299 - OpenShift Container Platform 4.8.10 버그 수정 업데이트

출시 날짜: 2021-09-06

OpenShift Container Platform 릴리스 4.8.10이 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3299 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:3300 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.10 --pullspecs
```

1.10.6.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.7. RHBA-2021:3429 - OpenShift Container Platform 4.8.11 버그 수정 업데이트

출시 날짜: 2021-09-14

OpenShift Container Platform 릴리스 4.8.11이 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3429 권고에 나열되어 있습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.11 --pullspecs
```

1.10.7.1. 버그 수정

- 이전에는 **이벤트 소스를 개발자 카탈로그 그룹에서** 찾을 수 있었습니다. 이번 업데이트를 통해 **Serverless** add 그룹의 이름이 **Eventing** 으로 바뀌었으며 **Eventing** add 그룹에서 **이벤트 소스**를 확인할 수 있습니다. (BZ#1999931)

1.10.7.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.8. RHBA-2021:3511 - OpenShift Container Platform 4.8.12 버그 수정 업데이트

출시 날짜: 2021-09-21

OpenShift Container Platform 릴리스 4.8.12가 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3511 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:3512 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.12 --pullspecs
```

1.10.8.1. 기능

1.10.8.1.1. 클러스터에 대한 새로운 최소 스토리지 요구 사항

OpenShift Container Platform 클러스터를 설치하는 데 필요한 최소 스토리지가 120GB에서 100GB로 감소했습니다. 이 업데이트는 지원되는 모든 플랫폼에 적용됩니다.

1.10.8.2. 버그 수정

- 이전에는 **oc** 툴에서 일부 레지스트리에 비해 너무 큰 헤더를 전송하여 해당 레지스트리에서 대규모 미러링 요청을 거부했습니다. 이번 업데이트에서는 **oc adm catalog mirror** 명령의 헤더 크기에 제한을 두어 미러링이 예상대로 작동합니다. (BZ#1874106)

- 이번 업데이트 이전에는 클러스터 자동 확장기에서 the **csidrivers.storage.k8s.io** or **csistoragecapacities.storage.k8s.io** 리소스에 액세스할 수 없어 권한 오류가 발생했습니다. 이번 수정을 통해 클러스터 자동 스케일러에 할당된 역할이 업데이트되어 해당 리소스에 대한 권한이 포함됩니다. (BZ#1995595)

1.10.8.3. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.9. RHBA-2021:3632 - OpenShift Container Platform 4.8.13 버그 수정 및 보안 업데이트

출시 날짜: 2021-09-27

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.13을 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3632 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:3631 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.13 --pullspecs
```

1.10.9.1. 기능

1.10.9.1.1. Kubernetes 1.21.4의 업데이트

이 업데이트에는 Kubernetes 1.21.4의 변경 사항이 포함되어 있습니다. 자세한 내용은 다음 변경 로그에서 확인할 수 있습니다. 1.21.4,1.21.3, 1.21.2.

1.10.9.2. 버그 수정

- 이전에는 **--max 구성 요소** 인수를 사용할 때 슬라이스에서 선택되지 않은 인덱스 작업이 있었습니다. 그 결과 **oc** 클라이언트에서 패닉 오류를 반환하고 충돌했습니다. 이번 업데이트에서는 범위가 아닌 인덱스에 대해 값이 요청되지 않도록 검사를 추가합니다. 결과적으로 max **-components** 인수를 사용할 때 **oc** 클라이언트가 더 이상 충돌하지 않습니다. (BZ#2004193)

1.10.9.3. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.10. RHBA-2021:3682 - OpenShift Container Platform 4.8.14 버그 수정 업데이트

출시 날짜: 2021-10-11

OpenShift Container Platform 릴리스 4.8.14가 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3682 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:3865 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.14 --pullspecs
```

1.10.10.1. 다음 OpenShift Container Platform 릴리스로 업그레이드 준비

OpenShift Container Platform 4.8.14에서는 현재 OpenShift Container Platform 4.9로 계획된 다음 OpenShift Container Platform 릴리스로의 업그레이드에 영향을 미치는 점검이 도입되었습니다. 이는 OpenShift Container Platform 4.9를 사용할 것으로 예상되는 Kubernetes 1.22가 더 이상 사용되지 않는 **v1beta1** API가 많이 제거되었기 때문입니다.

이 검사를 수행하려면 OpenShift Container Platform 4.8에서 4.9로 클러스터를 업그레이드하려면 관리자가 수동 승인을 제공해야 합니다. 이는 OpenShift Container Platform 4.9로 업그레이드한 후에도 문제를 방지하기 위한 것입니다. 여기서 제거된 API는 클러스터에서 계속 사용됩니다. 적절한 새 API 버전을 사용하려면 제거된 API에 대해 클러스터를 평가하고 마이그레이션해야 합니다. 이 평가 및 마이그레이션이 완료되면 관리자는 승인을 제공할 수 있습니다.

OpenShift Container Platform 4.9로 업그레이드하려면 모든 클러스터에 이 관리자의 승인이 필요합니다.

제거된 Kubernetes API 목록, 삭제된 API를 사용하여 클러스터를 평가하는 방법에 대한 팁 및 관리자 확인을 제공하는 방법에 대한 자세한 내용은 OpenShift Container Platform 4.9로 업그레이드 준비를 참조하십시오.

1.10.10.2. 버그 수정

- 이전 버전에서는 **provisioningHostIP** 를 설정할 때 provisioning 네트워크가 비활성화된 경우에도 Metal3 Pod에 할당되었습니다. 더 이상 이러한 일이 발생하지 않습니다. (BZ#1975711)

- 이전에는 IPv6 DHCP를 사용할 때 노드 인터페이스 주소가 **/128** 접두사로 임대될 수 있었습니다. 결과적으로 OVN-Kubernetes는 동일한 접두사를 사용하여 노드의 네트워크를 유추하고 게이트웨이를 통해 다른 클러스터 노드에 대한 트래픽을 포함한 다른 주소 트래픽을 라우팅합니다. 이번 업데이트를 통해 OVN-Kubernetes는 노드의 라우팅 테이블을 검사하고 노드의 인터페이스 주소에 대한 광범위한 라우팅 항목을 확인하여 해당 접두사를 사용하여 노드의 네트워크를 유추합니다. 결과적으로 다른 클러스터 노드로의 트래픽이 더 이상 게이트웨이를 통해 라우팅되지 않습니다. (BZ#1994624)

1.10.10.3. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.11. RHBA-2021:3821 - OpenShift Container Platform 4.8.15 버그 수정 및 보안 업데이트

출시 날짜: 2021-10-19

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.15를 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3821 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:3820 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.15 --pullspecs
```

1.10.11.1. 확인된 문제

- OpenShift Container Platform 단일 노드 구성에서 비실시간 커널을 사용할 때보다 실시간 커널(커널-rt)을 사용할 때 Pod 생성 시간이 2배 이상 느립니다. kernel-rt를 사용하는 경우 노드 재부팅 후 복구 시간이 영향을 받기 때문에 생성 속도가 느린 경우 최대 Pod 수에 영향을 미칩니다. kernel-rt를 사용하는 경우 **rcupdate.rcu_normal_after_boot=0 커널 인수를 사용하여 부팅하여 영향을 받은 복구 시간을 개선할 수 있습니다.** 이 인수에는 실시간 커널 버전 **kernel-rt-4.18.0-305.16.1.rt7.88.el8_4** 이상이 필요합니다. 이 알려진 문제는 OpenShift Container Platform 버전 4.8.15 이상에 적용됩니다. (BZ#1975356)

- OpenShift Container Platform 단일 노드 재부팅 후 모든 Pod가 다시 시작되어 일반 Pod 생성 시간보다 오래 걸립니다. 이 문제는 CNI(컨테이너 네트워크 인터페이스)에서 **pod add** 이벤트를 충분히 신속하게 처리할 수 없기 때문에 발생합니다. **timed out waiting for OVS port binding**이라는 오류 메시지가 표시됩니다. OpenShift Container Platform 단일 노드 인스턴스는 결국 복구되지만 예상보다 느리게 복구됩니다. 이 알려진 문제는 OpenShift Container Platform 버전 4.8.15 이상에 적용됩니다. (BZ#1986216)

1.10.11.2. 버그 수정

- 이전 버전에서는 Local Storage Operator에서 분리된 PV(영구 볼륨)를 삭제하는 경우 PV를 삭제한 다음 10초 동안 기다린 후 다음 볼륨을 삭제했습니다. 많은 PV를 삭제해야 하는 환경에서는 10초의 대기 기간이 발생하여 불필요한 지연이 발생하고 새 영구 볼륨 클레임이 너무 오래 걸렸습니다. 이 버그 수정을 통해 대기 기간이 10초 제거됩니다. 새 영구 볼륨 클레임이 적시에 처리됩니다. (BZ#2008088)

- 이전에는 provisioning **Network** 가 비활성화된 경우에도 베어 메탈 배포의 구성 설정에 **provisioningHostIP** 의 값이 포함된 경우 Metal3 Pod가 유지 관리되지 않은 프로비저닝 IP 주소로 시작되었습니다. Ironic은 시작될 때 이 프로비저닝 IP 주소를 사용했으며 주소가 작동을 중지하면 실패했습니다. 이 버그 수정으로 provisioning **Network** 가 비활성화되면 시스템은 **provisioningHostIP** 를 무시합니다. Ironic은 올바르게 구성된 외부 IP 주소로 시작합니다. (BZ#1975711)

1.10.11.3. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.12. RHBA-2021:3927 - OpenShift Container Platform 4.8.17 버그 수정 및 보안 업데이트

출시 날짜: 2021-10-27

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.17을 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:3927 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:3926 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.17 --pullspecs
```

1.10.12.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.13. RHBA-2021:4020 - OpenShift Container Platform 4.8.18 버그 수정 업데이트

출시 날짜: 2021-11-02

OpenShift Container Platform 릴리스 4.8.18이 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:4020 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:4019 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.18 --pullspecs
```

1.10.13.1. 버그 수정

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

1.10.13.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.14. RHBA-2021:4109 - OpenShift Container Platform 4.8.19 버그 수정 업데이트

출시 날짜: 2021-11-11

OpenShift Container Platform 릴리스 4.8.19가 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:4109 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:4108 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.19 --pullspecs
```

1.10.14.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.15. RHBA-2021:4574 - OpenShift Container Platform 4.8.20 버그 수정 업데이트

출시 날짜: 2021-11-16

OpenShift Container Platform 릴리스 4.8.20이 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:4574 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:4571 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.20 --pullspecs
```

1.10.15.1. 확인된 문제

- **hostsubnets.network.openshift.io** 는 현재 OVN 클러스터에 있지 않으므로 현재 옵트인 난독화는 OVN이 있는 클러스터에서 작동하지 않습니다. (BZ#2009322)

1.10.15.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.16. RHBA-2021:4716 - OpenShift Container Platform 4.8.21 버그 수정 업데이트

출시 날짜: 2021-11-23

OpenShift Container Platform 릴리스 4.8.21이 공개되었습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:4716 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:4715 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.21 --pullspecs
```

1.10.16.1. 기능

1.10.16.1.1. Kubernetes 1.21.5의 업데이트

이 업데이트에는 Kubernetes 1.21.5의 변경 사항이 포함되어 있습니다. 자세한 내용은 다음 변경 로그에서 확인할 수 있습니다. 1.21.5.

1.10.16.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.17. RHBA-2021:4830 - OpenShift Container Platform 4.8.22 버그 수정 및 보안 업데이트

출시 날짜: 2021-11-30

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.22를 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:4830 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:4829 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.22 --pullspecs
```

1.10.17.1. 기능

1.10.17.1.1. Kubernetes 1.21.6의 업데이트

이 업데이트에는 Kubernetes 1.21.6의 변경 사항이 포함되어 있습니다. 자세한 내용은 다음 변경 로그에서 확인할 수 있습니다. 1.21.6.

1.10.17.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.18. RHBA-2021:4881 - OpenShift Container Platform 4.8.23 버그 수정 업데이트

출시 날짜: 2021-12-07

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.23을 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:4881 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:4880 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.23 --pullspecs
```

1.10.18.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.19. RHBA-2021:4999 - OpenShift Container Platform 4.8.24 버그 수정 및 보안 업데이트

출시 날짜: 2021-12-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.24를 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:4999 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2021:4998 권고를 통해 제공됩니다.

이 릴리스에는 CVE-2021-44228, CVE-2021 -45046, CVE-2021 -4104 및 CVE-2021 -4125 에 대한 중요한 보안 업데이트가 포함되어 있으며, 이 모든 것이 Apache Log4j 유틸리티와 관련이 있습니다. 이러한 보안 취약점에 대한 수정 사항은 RHSA-2021:5108,RHSA-2021:5148 및 RHSA-2021:5183 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.24 --pullspecs
```

1.10.19.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.20. RHBA-2021:5209 - OpenShift Container Platform 4.8.25 버그 수정 및 보안 업데이트

출시 날짜: 2022-01-05

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.25를 사용할 수 있습니다. 업데이트에 포함된 버그 수정은 RHBA-2021:5209 권고에 나열되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2021:5208 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.25 --pullspecs
```

1.10.20.1. 버그 수정

- 이전에는 구성 파일에 알 수 없는 필드 또는 섹션이 있는 경우 **ovnkube-node 및 ovnkube-master** Pod가 시작되지 않았습니다. 결과적으로 OVN-Kubernetes가 업데이트되지 않았습니다. 이번 업데이트를 통해 알 수 없는 필드가 구성 파일에 있는 경우 OVN-Kubernetes가 더 이상 종료되지 않습니다. 대신 경고가 기록됩니다. 결과적으로 구성 파일에 알 수 없는 필드 또는 섹션이 포함되어 있으면 OVN-Kubernetes가 더 이상 실패하지 않습니다. (BZ#2030465)

- 이전에는 숫자 문자로 시작한 vCenter 호스트 이름이 **openshift-install** 명령을 실행할 수 없었습니다. 결과적으로 설치 프로그램에서 **잘못된 것으로 레이블이 지정되었습니다**. 이번 업데이트에서는 숫자 문자에 대한 유효성 검사가 추가되었습니다. 결과적으로 숫자 문자가 있는 vCenter 호스트를 만들 수 있습니다. (BZ#2022171)

- 이전에는 RHOSP(Red Hat OpenStack Platform) 다운로드 관리자 컨테이너의 'curl'에서 **install-config.yaml** 파일의 'noProxy' 값에 있는 네트워크 CIDR을 인식하지 못했습니다. 대신 쉼표로 구분된 IP 주소 목록만 인식합니다. 이번 업데이트를 통해 사용자는 'noProxy' 값에 네트워크 CIDR을 포함할 수 있습니다. (BZ#2005805)

1.10.20.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.21. RHBA-2022:0021 - OpenShift Container Platform 4.8.26 버그 수정 업데이트

출시 날짜: 2022-01-11

OpenShift Container Platform 릴리스 4.8.26이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0021 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:0020 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.26 --pullspecs
```

1.10.21.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.22. RHBA-2022:0113 - OpenShift Container Platform 4.8.27 버그 수정 업데이트

출시 날짜: 2022-01-18

OpenShift Container Platform 릴리스 4.8.27이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0113 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:0111 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.27 --pullspecs
```

1.10.22.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.23. RHBA-2022:0172 - OpenShift Container Platform 4.8.28 버그 수정 업데이트

출시 날짜: 2022-01-25

OpenShift Container Platform 릴리스 4.8.28이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0172 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:0171 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.28 --pullspecs
```

1.10.23.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.24. RHBA-2022:0278 - OpenShift Container Platform 4.8.29 버그 수정 업데이트

출시 날짜: 2022-02-01

OpenShift Container Platform 릴리스 4.8.29가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0278 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:0277 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.29 --pullspecs
```

1.10.24.1. 버그 수정

- 업데이트된 Jenkins 플러그인인 OpenShift 동기화 1.0.48은 Jenkins의 Kubernetes 플러그인의 Pod 템플릿에 적용되는 ConfigMap 및 ImageStream 레이블이 잘못 지정되었습니다. 결과적으로 OpenShift Sync는 'jenkins-agent' 레이블이 있는 구성 맵과 이미지 스트림에서 Pod 템플릿 가져오기를 중지했습니다. 이번 업데이트에서는 레이블 사양이 수정되고 Pod 템플릿을 예상대로 가져옵니다. (**BZ#2038960**)

- 이전에는 Local Storage Operator에서 5초마다 새로 추가된 블록 장치를 검색하여 CPU 사용량이 증가했습니다. 이번 업데이트에서는 간격을 60초로 늘려 CPU 사용량을 줄입니다. (**BZ#2006698**)

1.10.24.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.25. RHBA-2022:0484 - OpenShift Container Platform 4.8.31 버그 수정 및 보안 업데이트

출시 날짜: 2022-02-15

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.31을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0484 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:0483 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.31 --pullspecs
```

1.10.25.1. 기능

1.10.25.1.1. Whereabouts CNI 플러그인의 IP 조정

Whereabouts CNI 플러그인에 대한 새로운 개선 사항은 Kubernetes cronjob으로 실행되는 IP 조정 작업인 **ip-reconciler** 를 추가합니다. 이전에는 Pod에 대해 **CNI DEL** 요청이 완료되지 않은 경우 사용되지 않은 경우에도 Pod의 IP 주소가 계속 할당되어 있었습니다. 이제 이러한 IP 주소가 정기적으로 수집되어 다시 할당할 수 있습니다. (BZ#2028966)

1.10.25.2. 버그 수정

- 이전에는 경쟁 조건으로 인해 OpenStack 클라우드 공급자가 OpenStack 자격 증명을 사용하여 프로비저닝되지 않았습니다. 이로 인해 Octavia를 사용하여 로드 밸런싱 서비스를 만들 수 없었습니다. 이번 업데이트에서는 이러한 인증 정보를 반복적으로 가져옵니다. 구성 요소가 성공적으로 초기화되고 **LoadBalancer**-type 서비스를 생성할 수 있습니다. (BZ#2039377)

- 이전에는 **standard-csi** 스토리지 클래스에 **reclaimPolicy** 필드의 값이 포함되지 않았습니다. 그 결과 OpenStack Cinder CSI Driver Operator가 로그에 **StorageClassUpdated** 이벤트를 지속적으로 인쇄했습니다. 이번 업데이트에서는 **reclaimPolicy** 필드에 기본값을 제공합니다. Operator는 더 이상 로그에 과도한 업데이트 이벤트를 출력하지 않습니다. (*BZ#2049088)

- 이번 업데이트 이전에는 **oc set** 명령의 여러 하위 명령이 **--dry-run** 옵션으로 올바르게 작동하지 않았습니다. **dry-run=server** 옵션을 사용하는 명령에서 리소스를 업데이트합니다. 이번 업데이트에서는 **oc set** 하위 명령이 예상대로 작동하도록 **--dry-run** 옵션이 수정되었습니다. (BZ#2038931)

- 이전에는 웹 콘솔에서 **ServiceBinding**-type 리소스에 대한 **리소스** 속성을 읽지 않았습니다. 결과적으로 토폴로지 보기에 서비스 바인딩 커넥터가 표시되지 않았습니다. 이번 업데이트에서는 이 문제가 해결되었습니다. 웹 콘솔에서 **리소스** 속성을 읽고 서비스 바인딩 커넥터를 올바르게 표시합니다. (BZ#2019301)

1.10.25.3. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.26. RHBA-2022:0559 - OpenShift Container Platform 4.8.32 버그 수정 업데이트

출시 날짜: 2022-02-23

OpenShift Container Platform 릴리스 4.8.32가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0559 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:0558 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.32 --pullspecs
```

1.10.26.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.27. RHBA-2022:0651 - OpenShift Container Platform 4.8.33 bug fix update

출시 날짜: 2022-03-01

OpenShift Container Platform 릴리스 4.8.33이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0651 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:0650 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.33 --pullspecs
```

1.10.27.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.28. RHBA-2022:0795 - OpenShift Container Platform 4.8.34 버그 수정 업데이트

출시 날짜: 2022-03-16

OpenShift Container Platform 릴리스 4.8.34가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0795 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:0793 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.34 --pullspecs
```

1.10.28.1. 기능

1.10.28.1.1. Kubernetes 1.21.8의 업데이트

이번 업데이트에는 Kubernetes 1.21.6의 변경 사항이 1.21.8까지 포함되어 있습니다. 자세한 내용은 다음 변경 로그에서 확인할 수 있습니다. 1.21.7 및 1.21.8.

1.10.28.2. 삭제된 기능

OpenShift Container Platform 4.8.34부터 Microsoft Azure 클러스터의 mint 모드에서 CCO(Cloud Credential Operator) 사용에 대한 지원이 OpenShift Container Platform 4.8에서 제거되었습니다. 이러한 변경 사항은 2022년 6월 30일에 예정된 Microsoft Azure AD Graph API 사용 중지 로 인한 것이며 z-stream 업데이트에서 지원되는 모든 OpenShift Container Platform 버전으로 백포트되고 있습니다. 자세한 내용은 Microsoft Azure에 대한 자격 증명 추출 지원을 참조하십시오.

1.10.28.3. 확인된 문제

- 현재 OpenShift Container Platform 4.8.20에서 4.8.21로 업그레이드할 때 RHCOS(Red Hat Enterprise Linux CoreOS) 또는 Machine Config Operator 이미지가 버전 충돌에서 변경되지 않습니다. 결과적으로 컨트롤 플레인 노드가 여전히 **업데이트** 상태에 있을 때 업그레이드가 **완료된** 것으로 표시됩니다. **업그레이드** 로 표시된 경우 업데이트를 중단할 수 있으므로 사용자는 다른 절차를 수행할 수 없습니다. 임시 해결 방법으로 사용자는 다른 절차를 수행하기 전에 컨트롤 플레인 노드에서 업데이트를 완료할 때까지 기다려야 합니다. (BZ#2025396)

1.10.28.4. 버그 수정

- 이전에는 Prometheus QL을 사용한 **SystemMemoryExceedsReservation** 경고에서 **hugepages** 메모리 사용을 사용했습니다. 그 결과 OpenShift Container Platform 4.8의 클러스터에서 불필요하게 경고가 트리거되었습니다. 이번 업데이트를 통해 시스템 메모리 순환에서 Linux **hugepages** 가 제거되었으며 경고가 더 이상 불필요하게 트리거되지 않습니다. (BZ#2028854)

- 이전 버전에서는 OVN-Kubernetes가 있는 OpenShift Container Platform에서 ExternalIP를 통해 서비스에 대한 수신 액세스를 관리했습니다. 4.8.33에서 4.8.34로 업그레이드할 때 액세스 **ExternalIP** 는 "경로에서 호스트 없음"과 같은 문제로 작업을 중지합니다. 이번 업데이트를 통해 관리자는 이제 externalIPs에서 클러스터로 트래픽을 전달해야 합니다. 지침은 (KCS*) 및 (Kubernetes 외부 IP) (BZ#2076662)를 참조하십시오.

1.10.28.5. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.29. RHBA-2022:0872 - OpenShift Container Platform 4.8.35 버그 수정 및 보안 업데이트

출시 날짜: 2022-03-22

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.35를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:0872 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:0871 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.35 --pullspecs
```

1.10.29.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 마이너 버전에서 클러스터 업데이트를 참조하십시오.

1.10.30. RHSA-2022:1154 - OpenShift Container Platform 4.8.36 버그 수정 및 보안 업데이트

출시 날짜: 2022-04-11

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.36을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:1154 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:1153 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.36 --pullspecs
```

1.10.30.1. 버그 수정

- 이전에는 Ingress Operator에서 Ingress 카나리아 경로에 대한 상태 점검을 수행했습니다. 상태 점검이 완료되면 연결에서 **keepalive** 패킷이 활성화되었기 때문에 Ingress Operator에서 **LoadBalancer** 서비스에 대한 TCP 연결을 종료하지 않았습니다. 다음 상태 점검을 수행하는 동안 기존 연결을 사용하는 대신 **LoadBalancer** 서비스에 새 연결이 설정되었습니다. 이로 인해 **LoadBalancer** 서비스에 대한 연결이 누적되었습니다. 시간이 지남에 따라 **LoadBalancer** 서비스에서 연결 수가 소모되었습니다. 이번 업데이트를 통해 Ingress 카나리아 경로에 연결할 때 Keepalive가 비활성화됩니다. 결과적으로 카나리아 프로브가 실행될 때마다 새 연결이 생성되고 닫힙니다. Keepalive가 비활성화되어 있지만 설정된 연결의 누적은 더 이상 존재하지 않습니다. (BZ#2066302)

- 이전 버전에서는 RHOSP(Red Hat OpenStack Platform)-16에서 사용할 수 있는 Cisco ACI Neutron 구현의 서브넷 쿼리로 인해 지정된 네트워크에 대한 예기치 않은 결과가 발생했습니다. 그 결과 RHOSP **cluster-api-provider** 에서 중복된 포트가 있는 인스턴스를 동일한 서브넷에 프로비저닝하려고 할 수 있었기 때문에 프로비저닝에 실패했습니다. 이번 업데이트를 통해 RHOSP **cluster-api-provider** 에 추가 필터가 추가되어 서브넷당 포트가 하나만 있는지 확인합니다. 결과적으로 Cisco ACI를 사용하여 RHOSP-16에 OpenShift Container Platform을 배포할 수 있습니다. (BZ#2064634)

- 이전에는 **oc debug node** 명령의 시간 초과가 유휴 상태에 지정되지 않았습니다. 결과적으로 사용자가 클러스터에서 로그아웃되지 않았습니다. 이번 업데이트를 통해 디버그 Pod의 **TMOUT** 환경 변수가 비활성 타임아웃에 추가되었습니다. 결과적으로 **TMOUT** 비활성 후에 세션이 자동으로 종료됩니다. (BZ#2066760)

1.10.30.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.31. RHBA-2022:1369 - OpenShift Container Platform 4.8.37 버그 수정 업데이트

출시 날짜: 2022-04-21

OpenShift Container Platform 릴리스 4.8.37이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:1369 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.37 --pullspecs
```

1.10.31.1. 버그 수정

- 이전에는 노드를 삭제할 때 Local Storage Operator에서 PV(영구 볼륨)를 삭제하기 위한 요청을 발행하고 Pod에 연결된 동안 PV를 종료 상태로 유지합니다. 이번 업데이트에서는 PV의 소유자 참조가 제거되고 노드를 삭제할 때 종료 상태가 되지 않습니다. (**BZ#2072573**)

1.10.31.2. Upgdating

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 마이너 버전에서 클러스터 업데이트를 참조하십시오.

1.10.32. RHBA-2022:1427 - OpenShift Container Platform 4.8.39 버그 수정 업데이트

출시 날짜: 2022-04-27

OpenShift Container Platform 릴리스 4.8.39가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:1427 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:1423 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.39 --pullspecs
```

1.10.32.1. 알려진 문제

- 현재 4.8에서 4.9로 업그레이드할 수 없습니다. OpenShift Container Platform 사용자는 해당 릴리스 채널에서 사용 가능한 경우 다음 버전으로 업그레이드하는 것이 좋습니다. (**BZ#2068601**)

1.10.32.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 마이너 버전에서 클러스터 업데이트를 참조하십시오.

1.10.33. RHSA-2022:2272 - OpenShift Container Platform 4.8.41 버그 수정 및 보안 업데이트

출시 날짜: 2022-05-25

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.41을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:2272 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:270 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.41 --pullspecs
```

1.10.33.1. 기능

1.10.33.1.1. Kubernetes 1.21.11의 업데이트

이번 업데이트에는 Kubernetes 1.21.9부터 1.21.11까지의 변경 사항이 포함되어 있습니다. 자세한 내용은 다음 변경 로그에서 확인할 수 있습니다. 1.21.9,1.21.10 및 1.21.11.

1.10.33.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.34. RHBA-2022:4737 - OpenShift Container Platform 4.8.42 버그 수정 업데이트

출시 날짜: 2022-06-01

OpenShift Container Platform 릴리스 4.8.42가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:4737 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:4736 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.42 --pullspecs
```

1.10.34.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.35. RHBA-2022:4952 - OpenShift Container Platform 4.8.43 버그 수정 및 보안 업데이트

출시 날짜: 2022-06-16

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.43을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:4952 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2022:4951 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.43 --pullspecs
```

1.10.35.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.36. RHBA-2022:5032 - OpenShift Container Platform 4.8.44 버그 수정 업데이트

출시 날짜: 2022-06-22

OpenShift Container Platform 릴리스 4.8.44가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:5032 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:5031 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.44 --pullspecs
```

1.10.36.1. 버그 수정

- 이전 버전에서는 OpenShift Container Platform 4.8의 사용자 정의 플랫폼 경로의 API에서 10진수로 사용자 정의 호스트 이름 및 클러스터 도메인을 제외하는 사양 및 상태에 대한 제한이 생성되었습니다. 이로 인해 사용자가 호스트 이름을 지정하고 10진수가 포함된 클러스터 도메인을 설치할 수 없었습니다. 이번 수정으로 API 제한 사항이 없어 사용자가 모든 호스트 이름을 지정하고 모든 클러스터 도메인을 설치할 수 있습니다. (BZ#2081457)

1.10.36.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 마이너 버전에서 클러스터 업데이트를 참조하십시오.

1.10.37. RHBA-2022:5167 - OpenShift Container Platform 4.8.45 버그 수정 업데이트

출시 날짜: 2022-06-30

OpenShift Container Platform 릴리스 4.8.45가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:5167 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:5166 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.45 --pullspecs
```

1.10.37.1. 버그 수정

- 이전 버전에서는 **NetworkManager-wait-online.service** 시간이 초과되어 Ignition 구성 파일을 가져오기 전에 **coreos-installer** 에 연결할 수 없었습니다. 이번 업데이트를 통해 **NetworkManager-wait-online.service** 는 **coreos-installer** 가 Ignition 구성 파일을 가져올 수 있도록 더 많은 시간을 로드할 수 있습니다. (BZ#1983773)

1.10.37.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 마이너 버전에서 클러스터 업데이트를 참조하십시오.

1.10.38. RHBA-2022:5424 - OpenShift Container Platform 4.8.46 버그 수정 업데이트

출시 날짜: 2022-07-06

OpenShift Container Platform 릴리스 4.8.46이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:5424 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:5423 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.46 --pullspecs
```

1.10.38.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.39. RHBA-2022:5889 - OpenShift Container Platform 4.8.47 버그 수정 업데이트

출시 날짜: 2022-08-09

OpenShift Container Platform 릴리스 4.8.46이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:5889 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:5888 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.47 --pullspecs
```

1.10.39.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.40. RHBA-2022:6099 - OpenShift Container Platform 4.8.48 버그 수정 업데이트

출시 날짜: 2022-08-25

OpenShift Container Platform 릴리스 4.8.48이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6099 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:6098 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.48 --pullspecs
```

1.10.40.1. 버그 수정

- 이전 버전에서는 설치 프로그램에서 역할에 관계없이 **install-config.yaml** 의 **platform.baremetal.hosts** 섹션에 나열된 첫 번째 호스트를 컨트롤 플레인 시스템으로 사용했습니다. 이번 업데이트를 통해 역할이 있는 경우 적용됩니다. (**BZ#2025901**)

1.10.40.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.41. RHSA-2022:6308 - OpenShift Container Platform 4.8.49 버그 수정 및 보안 업데이트

출시 날짜: 2022-09-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.49를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:6308 권고에 설명되어 있습니다. 이 업데이트가 포함된 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.49 --pullspecs
```

1.10.41.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.42. RHBA-2022:6511 - OpenShift Container Platform 4.8.50 버그 수정 업데이트

출시 날짜: 2022-09-21

OpenShift Container Platform 릴리스 4.8.50이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:6511 권고에 설명되어 있습니다. 이 업데이트가 포함된 RPM 패키지가 없습니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.50 --pullspecs
```

1.10.42.1. 버그 수정

- 이전에는 Operator에서 IngressController를 삭제하고 다시 생성하여 클러스터의 PROXY 프로토콜을 4.8로 업데이트해야 했습니다. 이번 업데이트를 통해 IngressController API 상태 필드를 **spec.endpointPublishingStrategy.hostNetwork.protocol** 또는 **spec.endpointPublishingStrategy.nodePort.protocol** 을 **PROXY** 로 설정하면 업그레이드된 클러스터의 필드가 업데이트됩니다. (**BZ#2084337**)

1.10.42.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.43. RHSA-2022:6801 - OpenShift Container Platform 4.8.51 버그 수정 및 보안 업데이트

출시 날짜: 2022-10-13

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.51을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:6801 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:6800 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.51 --pullspecs
```

1.10.43.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.44. RHBA-2022:7034 - OpenShift Container Platform 4.8.52 버그 수정 업데이트

출시 날짜: 2022-10-26

OpenShift Container Platform 릴리스 4.8.52가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:7034 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:7032 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.52 --pullspecs
```

1.10.44.1. 버그 수정

- 이전에는 1초 후에 활성 상태 프로브가 시간 초과되어 kuryr-controller가 다시 시작되었습니다. 이번 수정을 통해 기본 시간 제한이 증가하여 kuryr-controller가 더 오래 실행됩니다. (**OCPBUGS-216**)

1.10.44.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.45. RHSA-2022:7874 - OpenShift Container Platform 4.8.53 버그 수정 및 보안 업데이트

출시 날짜: 2022-11-18

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.53을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2022:7874 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:7873 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.53 --pullspecs
```

1.10.45.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.46. RHBA-2022:8619 - OpenShift Container Platform 4.8.54 버그 수정 업데이트

출시 날짜: 2022-11-30

OpenShift Container Platform 릴리스 4.8.54가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:8619 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:8618 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.54 --pullspecs
```

1.10.46.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.47. RHBA-2022:8927 - OpenShift Container Platform 4.8.55 버그 수정 업데이트

출시 날짜: 2022-12-16

OpenShift Container Platform 릴리스 4.8.55가 공개되었습니다. 이번 릴리스에서는 s390x 아키텍처가 없습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2022:8927 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2022:8926 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.55 --pullspecs
```

1.10.47.1. Kubernetes 1.21.14 업데이트

이번 업데이트에는 Kubernetes 1.21.12의 변경 사항이 1.21.14까지 포함되어 있습니다. 자세한 내용은 다음 변경 로그에서 확인할 수 있습니다. 1.21.12,1.21.13, 1.21.14.

1.10.47.2. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.48. RHBA-2023:0018 - OpenShift Container Platform 4.8.56 버그 수정 및 보안 업데이트

출시 날짜: 2023-01-12

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.56을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:0018 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:0017 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.56 --pullspecs
```

1.10.48.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.

1.10.49. RHSA-2023:0237 - OpenShift Container Platform 4.8.57 버그 수정 및 보안 업데이트

출시 날짜: 2023-01-25

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.8.57을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:0237 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:0236 권고를 통해 제공됩니다.

다음 명령을 실행하여 이 릴리스에서 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.8.57 --pullspecs
```

1.10.49.1. update

기존 OpenShift Container Platform 4.8 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트에서 참조하십시오.