OpenShift Container Platform 4.13

릴리스 노트

OpenShift Container Platform 릴리스의 새로운 기능 및 주요 변경 사항

Last Updated: 2024-07-25

OpenShift Container Platform 4.13 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 4.13 릴리스 노트

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

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

1.1. 릴리스 정보

OpenShift Container Platform (RHSA-2023:1326)을 사용할 수 있습니다. 이 릴리스에서는 Kubernetes 1.26 을 CRI-O 런타임과 함께 사용합니다. 이에는 OpenShift Container Platform 4.13와 관련된 새로운 기능, 변경 사항, 알려진 문제가 포함되어 있습니다.

OpenShift Container Platform 4.13 클러스터는 https://console.redhat.com/openshift 에서 사용할 수 있습니다. OpenShift Container Platform용 Red Hat OpenShift Cluster Manager 애플리케이션을 사용하면 온프레미스 또는 클라우드 환경에 OpenShift Container Platform 클러스터를 배포할 수 있습니다.

OpenShift Container Platform 4.13은 RHEL (Red Hat Enterprise Linux) 9.2를 기반으로 합니다. FIPS 검증을 위해 RHEL 9.2가 아직 제출되지 않았습니다. Red Hat은 RHEL 9.0 및 RHEL 9.2 모듈에 대한 FIPS 검증을 받기 위해 특정 기간 동안 커밋할 수는 없지만 RHEL 9.x의 마이너 릴리스도 필요할 것으로 예상합니다. 업데이트는 규정 준수 활동 및 정부 표준에서 사용할 수 있습니다 .

OpenShift Container Platform 4.13은 Red Hat Enterprise Linux 8.6, 8.7, 8.8과 RHCOS(Red Hat Enterprise Linux CoreOS) 4.13에서 지원됩니다.

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

1.2. OPENSHIFT CONTAINER PLATFORM 계층화된 종속 구성 요소 지원 및 호환성

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

1.3. 새로운 기능 및 개선 사항

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

1.3.1. RHCOS(Red Hat Enterprise Linux CoreOS)

1.3.1.1. RHCOS에서 RHEL 9.2 사용

RHCOS는 이제 OpenShift Container Platform 4.13에서 RHEL (Red Hat Enterprise Linux) 9.2 패키지를 사용합니다. 이를 통해 최신 수정 사항, 기능 및 향상된 기능은 물론 최신 하드웨어 지원 및 드라이버 업데이트를 받을 수 있습니다.

1.3.1.1.1. RHEL 9.2를 사용하여 OpenShift Container Platform으로 업그레이드하기 위한 고려 사항

이번 릴리스에서는 OpenShift Container Platform 4.13에서 RHEL 9.2 기반 RHCOS가 도입되었으며 업그레이드하기 전에 몇 가지 고려해야 할 사항이 있습니다.

- 일부 구성 요소 구성 옵션 및 서비스가 RHEL 8.6과 RHEL 9.2 간에 변경될 수 있으므로 기존 머신 구성 파일이 더 이상 유효하지 않을 수 있습니다.
- 기본 OpenSSH **/etc/ssh/sshd_config** 서버 구성 파일을 사용자 지정한 경우 이 Red Hat 지식베이스 문서에 따라 업데이트해야 합니다.
- RHEL 6 기본 이미지 컨테이너는 RHCOS 컨테이너 호스트에서는 지원되지 않지만 RHEL 8 작업자 노드에서 지원됩니다. 자세한 내용은 Red Hat Container Compatibility Matrix를 참조하십시오.
- 일부 장치 드라이버는 더 이상 사용되지 않습니다. 자세한 내용은 RHEL 설명서 를 참조하십시오.

1.3.1.2. 설치 관리자 프로비저닝 인프라를 사용하는 IBM Power Virtual Server (기술 프리뷰)

설치 관리자 프로비저닝 인프라(IPI)는 OpenShift Container Platform의 전체 스택 설치 및 설정을 제공합니다.

자세한 내용은 IBM Power Virtual Server에 설치 준비를 참조하십시오.

1.3.1.3. IBM Secure Execution on IBM Z and IBM (R) LinuxONE

이 기능은 OpenShift Container Platform 4.12에서 기술 프리뷰로 소개되었으며 현재 OpenShift Container Platform 4.13에서 일반적으로 사용할 수 있습니다. IBM Secure Execution은 KVM 게스트의 메모리 경계를 보호하는 하드웨어 기능 강화입니다. IBM Secure Execution은 클러스터 워크로드에 대해 최고 수준의 격리 및 보안을 제공하며 IBM Secure Execution-ready QCOW2 부팅 이미지를 사용하여 활성화할 수 있습니다.

IBM Secure Execution을 사용하려면 호스트 머신의 호스트 키가 있어야 하며 Ignition 구성 파일에 지정해야 합니다. IBM Secure Execution은 LUKS 암호화를 사용하여 부팅 볼륨을 자동으로 암호화합니다.

자세한 내용은 IBM 보안 실행을 사용하여 RHCOS 설치를 참조하십시오.

1.3.1.4. 지원 설치 관리자 SaaS는 IBM Power, IBM Z 및 IBM(R) LinuxONE에 대한 플랫폼 통합 지원을 제공합니다.

console.redhat.com 에서 지원되는 설치 관리자 SaaS는 지원 설치 관리자 사용자 인터페이스 또는 REST API를 사용하여 IBM Power, IBM Z 및 IBM® LinuxONE 플랫폼에 OpenShift Container Platform 설치를 지원합니다. 통합을 통해 사용자는 단일 인터페이스에서 인프라를 관리할 수 있습니다. IBM Power, IBM Z 및 IBM® LinuxONE과 지원 설치 관리자 SaaS와의 통합을 활성화하는 몇 가지 추가 설치 단계가 있습니다.

자세한 내용은 지원 설치 관리자를 사용하여 온프레미스 클러스터 설치를 참조하십시오.

1.3.1.5. RHCOS에 lsof 포함

OpenShift Container Platform 4.13에는 이제 RHCOS에 **lsof** 명령이 포함되어 있습니다.

1.3.2. 설치 및 업데이트

1.3.2.1. VMware vSphere 버전 8.0 지원

OpenShift Container Platform 4.13에서는 VMware vSphere 버전 8.0을 지원합니다. VMware vSphere 버전 7.0 업데이트 2에 OpenShift Container Platform 클러스터를 계속 설치할 수 있습니다.

1.3.2.2. VMware vSphere 리전 및 영역 활성화

OpenShift Container Platform 클러스터를 단일 VMware vCenter에서 실행되는 여러 vSphere 데이터 센터 또는 리전에 배포할 수 있습니다. 각 데이터 센터는 여러 클러스터 또는 영역을 실행할 수 있습니다. 이 설정을 사용하면 하드웨어 장애 또는 네트워크 중단으로 인해 클러스터가 실패할 위험이 줄어듭니다.

중요

이 기능에는 vSphere CSI(Container Storage Interface) 드라이버가 클러스터의 기본 스토리지 드라이버로 필요하므로 VMware vSphere 리전 및 영역 활성화 기능은 새로 설치된 클러스터에서만 사용할 수 있습니다.

이전 릴리스에서 업그레이드된 클러스터는 기본적으로 in-tree vSphere 드라이버를 사용합니다. 따라서 이 기능을 사용하려면 클러스터에 대해 CSI 자동 마이그레이션을 활성화해야 합니다. 그런 다음 업그레이드된 클러스터에 대해 여러 리전 및 영역을 구성할 수 있습니다.

자세한 내용은 VMware vSphere 리전 및 영역 사용을 참조하십시오 .

1.3.2.3. 기본 vSphere install-config.yaml 파일로 변경

vSphere에서 OpenShift Container Platform용 설치 프로그램을 실행한 후 이제 기본 **install-config.yaml** 파일에 **vcenters** 및 **failureDomains** 필드가 포함되어 클러스터의 여러 데이터 센터, 리전 및 영역 정보를 지정할 수 있습니다. VMware vCenter에서 실행되는 단일 데이터 센터로 구성된 vSphere 환경에 OpenShift Container Platform 클러스터를 설치하려는 경우 이러한 필드를 비워 둘 수 있습니다.

자세한 내용은 VMware vCenter의 리전 및 영역 구성을 참조하십시오.

1.3.2.4. 여러 vSphere 서브넷을 지원하는 외부 로드 밸런서

여러 서브넷을 지원하는 외부 로드 밸런서를 사용하도록 OpenShift Container Platform 클러스터를 구성할 수 있습니다. 여러 서브넷을 사용하는 경우 로드 밸런서 대상에서 사용하는 네트워크의 모든 IP 주소를 명시적으로 나열할 수 있습니다. 이 구성을 사용하면 로드 밸런서 대상을 재구성하지 않고 해당 네트워크 내에서 노드를 생성하고 삭제할 수 있으므로 유지 관리 오버헤드가 줄어들 수 있습니다.

자세한 내용은 외부 로드 밸런서 구성을 참조하십시오.

1.3.2.5. VMware vSphere에 클러스터를 설치하기 전에 VM 암호화 지원

OpenShift Container Platform 4.13의 경우 사용자 프로비저닝 인프라를 사용하여 VMware vSphere에 클러스터를 설치하기 전에 가상 머신을 암호화할 수 있습니다.

자세한 내용은 가상 머신 암호화를 위한 요구 사항을 참조하십시오.

1.3.2.6. 3-노드 클러스터 지원

OpenShift Container Platform 4.13부터 AWS(Amazon Web Services), Microsoft Azure, GCP(Google Cloud Platform) 및 VMware vSphere에서 3노드 클러스터 배포가 지원됩니다. 이 유형의 OpenShift Container Platform 클러스터는 컴퓨팅 머신 역할을 하는 세 개의 컨트롤 플레인 시스템으로 구성되므로 더 작고 리소스 효율이 높은 클러스터입니다.

자세한 내용은 AWS에 3-노드 클러스터 설치, Azure에 3-노드 클러스터 설치, GCP에 3-노드 클러스터 설치, vSphere에 3-노드 클러스터 설치를 참조하십시오.

1.3.2.7. IBM Cloud VPC 및 기존 VPC 리소스

기존 VPC(가상 프라이빗 클라우드)에 OpenShift Container Platform 클러스터를 배포하는 경우 **networkResourceGroupName** 매개변수를 사용하여 이러한 기존 리소스가 포함된 리소스 그룹의 이름을 지정할 수 있습니다. 이번 개선된 기능을 통해 기존 VPC 리소스 및 서브넷을 설치 프로그램이 프로비저닝하는 클러스터 리소스와 별도로 유지할 수 있습니다. 그런 다음 **resourceGroupName** 매개변수를 사용하여 설치 프로그램에서 프로비저닝한 모든 클러스터 리소스를 배포하는 데 사용할 수 있는 기존 리소스 그룹의 이름을 지정할 수 있습니다. **resourceGroupName** 이 정의되지 않은 경우 클러스터에 대한 새 리소스 그룹이 생성됩니다.

자세한 내용은 추가 IBM Cloud VPC 구성 매개변수를 참조하십시오.

1.3.2.8. OpenShift Container Platform 클러스터를 설치 및 삭제하는 데 GCP가 필요한 최소 권한

OpenShift Container Platform 4.13에서는 사전 정의된 역할을 사용하는 대신 OpenShift Container Platform 클러스터를 설치하고 삭제하는 데 필요한 최소 권한을 포함하도록 사용자 정의 역할을 정의할 수 있습니다. 이러한 권한은 설치 관리자 프로비저닝 인프라 및 사용자 프로비저닝 인프라에서 사용할 수 있습니다.

1.3.2.9. Azure에 대한 사용자 정의 태그

OpenShift Container Platform 4.13에서는 리소스를 그룹화하고 리소스 액세스 및 비용을 관리하기 위해 Azure에서 태그를 구성할 수 있습니다. 태그에 대한 지원은 Azure Public Cloud에서 생성된 리소스와 OpenShift Container Platform 4.13에서 TP(기술 프리뷰)로만 사용할 수 있습니다. OpenShift Container Platform 클러스터 생성 중에 **install-config.yaml** 파일에서 Azure 리소스에 태그를 정의할 수 있습니다.

1.3.2.10. 공유 VPC(Virtual Private Cloud)에 GCP의 OpenShift Container Platform 클러스터를 설치

OpenShift Container Platform 4.13에서는 GCP(Google Cloud Platform)의 공유 VPC(Virtual Private Cloud)에 클러스터를 설치할 수 있습니다. 이 설치 방법은 다른 GCP 프로젝트와 VPC를 공유하도록 클러스터를 구성합니다. 공유 VPC를 사용하면 조직에서 공통 VPC 네트워크를 통해 여러 프로젝트의 리소스를 연결할 수 있습니다. 일반적인 VPC 네트워크는 내부 IP 주소를 사용하여 조직의 통신의 보안과 효율성을 높일 수 있습니다.

자세한 내용은 공유 VPC에 GCP의 클러스터 설치를 참조하십시오.

1.3.2.11. 보호된 VM을 사용하여 GCP에 클러스터 설치

OpenShift Container Platform 4.13에서는 클러스터를 설치할 때 Shielded VMs를 사용할 수 있습니다. Shielded VM에는 보안 부팅, 펌웨어 및 무결성 모니터링, 루트킷 탐지 등 추가 보안 기능이 있습니다. 자세한 내용은 Enabling Shielded VMs and Google's documentation on Shielded VMs 에서 참조하십시오.

1.3.2.12. 기밀성 VM을 사용하여 GCP에 클러스터 설치

OpenShift Container Platform 4.13에서는 클러스터를 설치할 때 기밀성 VM을 사용할 수 있습니다. 기밀 VM은 처리되는 동안 데이터를 암호화합니다. 자세한 내용은 기밀 컴퓨팅에 대한 Google 문서를 참조하십시오. 서로 의존하지는 않지만 기밀 VM과 방패 VM을 동시에 활성화할 수 있습니다.

중요

OpenShift Container Platform 4.13 및 이전 버전에서 알려진 문제로 인해 GCP(Google Cloud Platform)에서 기밀 VM이 있는 클러스터에서 영구 볼륨 스토리지를 사용할 수 없습니다. 이 문제는 OpenShift Container Platform 4.13.4에서 해결되었습니다. 자세한 내용은 OCPBUGS-11768 에서 참조하십시오.

1.3.2.13. 기존 VPC(Virtual Private Cloud)에 AWS의 클러스터를 설치

OpenShift Container Platform 4.13에서는 AWS VPC를 사용하는 클러스터의 설치 프로세스가 간소화됩니다. 이 릴리스에서는 AWS Local Zones에 최적화된 머신 *풀인 엣지* 풀도 도입되었습니다.

자세한 내용은 AWS 로컬 영역을 사용하여 클러스터 설치를 참조하십시오.

1.3.2.14. OpenShift Container Platform 4.12에서 4.13으로 업그레이드할 때 관리자 승인 필요

OpenShift Container Platform 4.13에서는 더 이상 사용되지 않는 여러 API를 제거한 Kubernetes 1.26을 사용합니다.

클러스터 관리자는 클러스터를 OpenShift Container Platform 4.12에서 4.13로 업그레이드하기 전에 수동으로 승인을 제공해야 합니다. 이는 OpenShift Container Platform 4.13으로 업그레이드한 후에도 문제를 방지하기 위한 것입니다. 여기서 제거된 API는 클러스터에서 실행 중이거나 클러스터와 상호 작용하는 기타 구성 요소에서 여전히 사용 중입니다. 관리자는 제거될 모든 API에 대해 클러스터를 평가하고 영향을 받는 구성 요소를 마이그레이션하여 적절한 새 API 버전을 사용해야 합니다. 이 작업이 완료되면 관리자는 관리자 승인을 제공할 수 있습니다.

모든 OpenShift Container Platform 4.12 클러스터에는 OpenShift Container Platform 4.13으로 업그레이드하기 전에 이 관리자가 승인해야 합니다.

자세한 내용은 OpenShift Container Platform 4.13으로 업데이트 준비를 참조하십시오.

1.3.2.15. Microsoft Azure가 OpenShift Container Platform 클러스터를 설치 및 삭제하는 데 필요한 최소 권한

OpenShift Container Platform 4.13에서는 기본 제공 역할을 사용하는 대신 Microsoft Azure가 OpenShift Container Platform 클러스터를 설치하고 삭제하는 데 필요한 최소 권한을 포함하도록 사용자 정의 역할을 정의할 수 있습니다. 이러한 권한은 설치 관리자 프로비저닝 인프라 및 사용자 프로비저닝 인프라에서 사용할 수 있습니다.

1.3.2.16. 다중 아키텍처 페이로드 마이그레이션에 대한 단일 아키텍처

OpenShift Container Platform 4.13에서는 **oc adm upgrade --to-multi-arch** 명령을 도입하여 단일 아키텍처 컴퓨팅 머신이 있는 클러스터를 다중 아키텍처 컴퓨팅 머신이 있는 클러스터로 마이그레이션할 수 있습니다. 다중 아키텍처의 매니페스트 목록에 있는 페이로드로 업데이트하면 혼합 아키텍처 컴퓨팅 머신을 클러스터에 추가할 수 있습니다.

1.3.2.17. vSphere의 컨트롤 플레인에서 실행되도록 네트워크 구성 요소 구성

vSphere 설치의 컨트롤 플레인 노드에서 실행하려면 VIP 주소가 필요한 경우 컨트롤 플레인 노드에서 독점적으로 실행되도록 **ingressVIP** 주소를 구성해야 합니다. 기본적으로 OpenShift Container Platform에서는 작업자 머신 구성 풀의 모든 노드가 **ingressVIP** 주소를 호스팅할 수 있습니다. vSphere 환경은 컨트롤 플레인 노드와 별도의 서브넷에 작업자 노드를 배포하므로 컨트롤 플레인 노드에서 독점적으로 실행되도록 **ingressVIP** 주소를 구성하면 별도의 서브넷에 작업자 노드를 배포하여 문제가 발생하지 않습니다. 자세한 내용은 vSphere의 컨트롤 플레인에서 실행되도록 네트워크 구성 요소 구성을 참조하십시오.

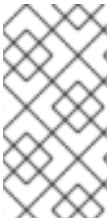
1.3.2.18. 단일 노드를 사용하여 AWS에 OpenShift Container Platform 클러스터 설치

OpenShift Container Platform 4.13에서는 AWS(Amazon Web Services)에 단일 노드로 클러스터를 설치할 수 있습니다. 단일 노드에 설치하면 노드의 리소스 요구 사항이 증가합니다. 자세한 내용은 단일 노드에 클러스터 설치를 참조하십시오.

1.3.2.19. Bare Metal Operator를 사용하여 사용자 프로비저닝 클러스터에서 베어 메탈 호스트를 확장

OpenShift Container Platform 4.13을 사용하면 Bare Metal Operator(BMO) 및 기타 메탈[3] 구성 요소를 사용하여 기존 사용자 프로비저닝 인프라 클러스터에서 베어 메탈 호스트를 확장할 수 있습니다. 사용자 프로비저닝 클러스터에서 Bare Metal Operator를 사용하면 호스트의 관리 및 스케일링을 단순화하고 자동화할 수 있습니다.

BMO를 사용하면 **BareMetalHost** 오브젝트를 구성하여 호스트를 추가하거나 제거할 수 있습니다. **BareMetalHost** 오브젝트 인벤토리에 external **Provisioned** 로 등록하여 기존 호스트를 추적할 수도 있습니다.



참고

베어 메탈 Operator를 사용하여 프로비저닝 네트워크를 사용하여 사용자 프로비저닝 인프라 클러스터를 확장할 수 없습니다. 이 워크플로는 프로비저닝 네트워크를 지원하지 않으므로 가상 미디어 네트워크 부팅을 지원하는 베어 메탈 호스트 드라이버만 사용할 수 있습니다(예: **redfish-virtualmedia** 및 **idrac-virtualmedia**).

BMO를 사용하여 사용자 프로비저닝 클러스터를 스케일링하는 방법에 대한 자세한 내용은 Bare Metal Operator가 있는 사용자 프로비저닝 클러스터 스케일링을 참조하십시오.

1.3.2.20. 64비트 ARM의 OpenShift Container Platform

OpenShift Container Platform 4.13은 이제 64비트 ARM 아키텍처 기반 Azure 사용자 프로비저닝 설치에서 지원됩니다. 에이전트 기반 설치 프로그램은 이제 64비트 ARM 시스템에서도 지원됩니다. 인스턴스 가용성 및 설치 설명서에 대한 자세한 내용은 다른 플랫폼에 대해 지원되는 설치 방법을 참조하십시오.

1.3.2.21. git-lfs 패키지 지원

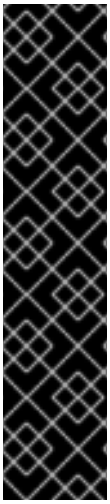
OpenShift Jenkins 이미지는 이제 **git-lfs** 패키지를 지원합니다. 이 패키지를 사용하면 OpenShift Jenkins 이미지에서 200MB(MB)보다 큰 아티팩트를 사용할 수 있습니다.

1.3.2.22. oc-mirror 플러그인을 사용하여 로컬 OCI Operator 카탈로그를 포함하는 기능을 일반적으로 사용할 수 있습니다.

oc-mirror 플러그인을 사용하여 디스크의 로컬 OCI Operator 카탈로그를 미러 레지스트리에 미러링할 수 있습니다. 이 기능은 이전에 OpenShift Container Platform 4.12에서 기술 프리뷰로 소개되었으며 현재 OpenShift Container Platform 4.13에서 일반적으로 사용할 수 있습니다.

이 릴리스에서는 로컬 OCI 카탈로그가 포함된 경우 다음 기능을 지원합니다.

- 대상 미러 레지스트리에서 이미지 정리
- 도구를 마지막으로 실행한 이후 변경된 항목만 미러링하려면 증분 미러링
- 대상 미러 레지스트리에 있는 카탈로그의 대체 이름의 네임스페이스 계층 구조



중요

- OpenShift Container Platform 4.12용 oc-mirror 플러그인에 기술 프리뷰 OCI 로컬 카탈로그 기능을 사용한 경우 oc-mirror 플러그인의 OCI 기능을 사용하여 로컬에서 카탈로그를 복사하고 OCI 형식으로 변환하여 완전히 연결이 끊긴 클러스터로 미러링할 수 있습니다.
- 로컬 OCI 카탈로그를 미러링할 때 로컬 OCI 형식의 카탈로그와 함께 미러링하려는 OpenShift Container Platform 릴리스 또는 추가 이미지를 레지스트리에서 가져와야 합니다. 디스크의 oc-mirror 이미지 세트 파일과 함께 OCI 카탈로그를 미러링할 수 없습니다.
- **--use-oci-feature** 플래그가 더 이상 사용되지 않습니다. 대신 **--include-local-oci-catalogs** 플래그를 사용하여 로컬 OCI 카탈로그 미러링을 활성화합니다.

자세한 내용은 로컬 OCI Operator 카탈로그 포함 을 참조하십시오.

1.3.2.23. RHOSP에서 장애 도메인을 사용하는 클러스터 배포 (기술 프리뷰)

RHOSP에서 여러 장애 도메인에 걸쳐 있는 클러스터를 배포할 수 있습니다. 대규모 배포의 경우 장애 도메인은 복원력과 성능을 향상시킵니다.

자세한 내용은 실패 도메인의 RHOSP 매개변수를 참조하십시오.

1.3.2.24. RHOSP에 사용자 관리 로드 밸런서를 사용하여 클러스터 배포 (기술 프리뷰)

이제 기본 내부 로드 밸런서가 아닌 사용자 관리 로드 밸런서를 사용하여 RHOSP에 클러스터를 배포할 수 있습니다.

자세한 내용은 사용자 관리 로드 밸런서를 사용하여 OpenStack에 클러스터 설치 구성을 참조하십시오.

1.3.2.25. Nutanix에 클러스터를 설치할 때 프로젝트 및 카테고리 사용

OpenShift Container Platform 4.13에서는 프로젝트 및 카테고리를 사용하여 Nutanix에 설치된 클러스터의 컴퓨팅 플레인 가상 머신을 구성할 수 있습니다. 프로젝트는 권한, 네트워크 및 기타 매개 변수를 관리하기 위한 사용자 역할의 논리 그룹을 정의합니다. 카테고리를 사용하여 공유 특성을 기반으로 가상 머신 그룹에 정책을 적용할 수 있습니다.

자세한 내용은 Nutanix에 클러스터 설치를 참조하십시오.

1.3.2.26. 에이전트 기반 설치 관리자에서 네트워크 연결 검사를 수행합니다.

에이전트 기반 설치 관리자를 사용하여 OpenShift Container Platform 4.13을 설치하는 경우 콘솔 애플리케이션(텍스트 사용자 인터페이스 포함)은 설치 프로세스 초기에 가져오기 검사를 수행하여 현재 호스트가 구성된 릴리스 이미지를 검색할 수 있는지 확인합니다. 콘솔 애플리케이션은 사용자가 네트워크 구성을 직접 수정할 수 있도록 하여 문제 해결 문제를 지원합니다.

자세한 내용은 현재 설치 호스트가 릴리스 이미지를 가져올 수 있는지 확인을 참조하십시오.

1.3.3. 설치 후 구성

1.3.3.1. 다중 아키텍처 컴퓨팅 머신이 있는 OpenShift Container Platform 클러스터

다중 아키텍처 컴퓨팅 머신이 있는 OpenShift Container Platform 4.13 클러스터를 일반적으로 사용할 수

있습니다. Day 2 작업에서는 AWS 및 Azure 설치 관리자 프로비저닝 인프라에 다양한 아키텍처의 컴퓨팅 노드를 사용하여 클러스터를 생성할 수 있습니다. 베어 메탈에 사용자 프로비저닝 설치는 기술 프리뷰에 있습니다. 다중 아키텍처 컴퓨팅 머신을 사용하여 클러스터를 생성하는 방법에 대한 자세한 내용은 OpenShift Container Platform 클러스터에서 다중 아키텍처 컴퓨팅 머신 구성을 참조하십시오.

1.3.3.2. VSphere에서 클러스터의 여러 장애 도메인 지정

관리자는 VMware VSphere 인스턴스에서 실행되는 OpenShift Container Platform 클러스터에 대해 여러 장애 도메인을 지정할 수 있습니다. 즉, 데이터센터에 다양한 하드웨어 리소스 간에 주요 컨트롤 플레인과 워크로드 요소를 배포할 수 있습니다. 또한 여러 계층 2 네트워크 구성을 사용하도록 클러스터를 구성하여 노드 간 데이터 전송이 여러 네트워크에 걸쳐 확장될 수 있습니다.

자세한 내용은 VSphere에서 클러스터의 여러 장애 도메인 지정 을 참조하십시오.

1.3.4. 웹 콘솔

1.3.4.1. 개발자 화면

이번 릴리스에서는 웹 콘솔의 **개발자** 화면에서 다음 작업을 수행할 수 있습니다.

- **Git에서 가져오기** 흐름을 사용하여 **Serverless 함수** 를 생성합니다.
- **추가 페이지에서** 사용할 수 있는 **Serverless 함수 생성** 흐름을 사용하여 Serverless 함수를 생성합니다.
- **Git에서 가져오기 워크플로에서 pipeline-as-code 를 옵션으로 선택합니다.**
- **사용자 인터페이스에서 다음 위치에서 트래픽을 수신하는 Pod를 확인합니다.**
  - **토폴로지 보기의 측면 창**
  - **Pod의 세부 정보 보기**
  - **Pod 목록 보기**
- **웹 터미널 을 인스턴스화할 때 시간 초과 기간을 사용자 지정하거나 자체 이미지를 제공합니다.**
- **관리자로 기본 리소스를 모든 사용자의 개발자 화면 탐색에 미리 고정하도록 설정합니다.**

1.3.4.1.1. 파이프라인 페이지 개선 사항

OpenShift Container Platform 4.13에서는 Pipelines 페이지에서 다음과 같은 탐색 개선 사항이 표시됩니다.

- **이전에 선택한 탭은 Pipelines 페이지로 돌아갈 때 계속 표시됩니다.**
- **Repository details 페이지의 기본 탭은 이제 PipelinesRuns 이지만 Create Git Repository flow 를 따르면 기본 탭이 세부 정보입니다.**

1.3.4.1.2. Helm 페이지 개선 사항

OpenShift Container Platform 4.13에서 Helm 페이지에는 다음과 같은 새로운 기능 및 업데이트된 기능이 포함됩니다.

- **페이지에 사용되는 용어는 Helm 차트를 설치 및 제거하는 대신 Helm 릴리스 생성 및 삭제를 나타냅니다.**

- Helm 릴리스를 비동기식으로 생성 및 삭제하고 웹 콘솔에서 다음 작업을 수행하기 전에 작업이 완료될 때까지 기다리지 않을 수 있습니다.
- Helm 릴리스 목록에 상태 열이 포함됩니다.

1.3.5. OpenShift CLI(oc)

1.3.5.1. 지정된 네임스페이스에서 must-gather를 실행하기 위해 새 플래그 추가

OpenShift Container Platform 4.13에서 **oc adm must-gather** 명령에 **--run-namespace** 플래그를 사용할 수 있습니다. 이 플래그를 사용하여 must-gather 툴을 실행할 기존 네임스페이스를 지정할 수 있습니다.

자세한 내용은 must-gather 툴 정보를 참조하십시오.

1.3.5.2. OpenShift CLI(oc)를 사용하여 매니페스트 가져오기

OpenShift Container Platform 4.13에서는 새 **oc** CLI(명령줄 인터페이스) 플래그**--import-mode** 가 다음 **oc** 명령에 추가되었습니다.

- **oc import-image**
- **oc tag**

이 향상된 기능을 통해 사용자는 **oc import-image** 또는 **oc tag** 명령을 실행할 때 매니페스트 목록의 단일 하위 매니페스트 또는 모든 매니페스트를 가져오는 옵션을 제공하는 **--import-mode** 플래그를 **Legacy** 또는 **PreserveOriginal** 로 설정할 수 있습니다.

자세한 내용은 매니페스트 목록 작업을 참조하십시오.

1.3.5.3. 이미지의 os/arch 및 다이제스트 반환

OpenShift Container Platform 4.13에서 이미지에서 **oc describe** 를 실행하면 각 매니페스트의 os/arch 및 다이제스트가 반환됩니다.

1.3.6. IBM Z 및 IBM(R) LinuxONE

이번 릴리스에서 IBM Z 및 IBM® LinuxONE은 이제 OpenShift Container Platform 4.13과 호환됩니다. z/VM 또는 RHEL(Red Hat Enterprise Linux) KVM(커널 기반 가상 시스템)을 사용하여 설치할 수 있습니다. 설치 지침은 다음 설명서를 참조하십시오.

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

중요

컴퓨팅 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행

IBM Z 및 IBM (R) LinuxONE 주요 개선 사항

OpenShift Container Platform 4.13의 IBM Z 및 IBM® LinuxONE 릴리스에서는 OpenShift Container Platform 구성 요소 및 개념에 향상된 기능과 새로운 기능이 추가되었습니다.

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

- 지원되는 설치 관리자
- Cluster Resource Override Operator
- 송신 IP
- MetalLB Operator
- Network-Bound 디스크 암호화 - 외부 Tang 서버

IBM Secure Execution
OpenShift Container Platform은 IBM Z 및 IBM® LinuxONE(s390x 아키텍처)에서 IBM Secure Execution 용 RHCOS(Red Hat Enterprise Linux CoreOS) 노드 구성을 지원합니다.

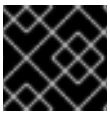
설치 지침은 다음 설명서를 참조하십시오.

- IBM Secure Execution을 사용하여 RHCOS 설치

1.3.7. IBM Power

이 릴리스에서 IBM Power는 이제 OpenShift Container Platform 4.13과 호환됩니다. 설치 지침은 다음 설명서를 참조하십시오.

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



중요

컴퓨팅 노드는 RHCOS(Red Hat Enterprise Linux CoreOS)를 실행

IBM Power 주요 기능 개선
OpenShift Container Platform 4.13의 IBM Power 릴리스에는 OpenShift Container Platform 구성 요소 및 개념에 대한 개선 사항 및 새로운 기능이 추가되었습니다.

이 릴리스에서는 IBM Power의 다음 기능을 지원합니다.

- 지원되는 설치 관리자
- Cluster Resource Override Operator
- IBM Power Virtual Server Block CSI Driver Operator (기술 프리뷰)
- 송신 IP
- 설치 관리자 프로비저닝 IBM Power Virtual Server용 인프라 활성화(기술 프리뷰)
- MetalLB Operator
- Network-Bound 디스크 암호화 - 외부 Tang 서버

IBM Power,IBM Z 및 IBM(R) LinuxONE 지원 매트릭스

표 1.1. OpenShift Container Platform 기능

기능	IBM Power	IBM Z 및 IBM® LinuxONE
대체 인증 공급자	지원됨	지원됨
지원되는 설치 관리자	지원됨	지원됨
로컬 스토리지 Operator를 통한 자동 장치 검색	지원되지 않음	지원됨
시스템 상태 점검으로 손상된 시스템 자동 복구	지원되지 않음	지원되지 않음
IBM Cloud용 클라우드 컨트롤러 관리자	지원됨	지원되지 않음
노드에서 오버 커밋 제어 및 컨테이너 밀도 관리	지원되지 않음	지원되지 않음
Cron 작업	지원됨	지원됨
Descheduler	지원됨	지원됨
송신 IP	지원됨	지원됨
etcd에 저장된 데이터 암호화	지원됨	지원됨
Helm	지원됨	지원됨
수평 Pod 자동 스케일링	지원됨	지원됨
IPv6	지원됨	지원됨
사용자 정의 프로젝트 모니터링	지원됨	지원됨
다중 경로	지원됨	지원됨
Network-Bound 디스크 암호화 - 외부 Tang 서버	지원됨	지원됨
비volatile 메모리 표현 드라이브(NVMe)	지원됨	지원되지 않음
OpenShift CLI(**oc**) 플러그인	지원됨	지원됨
Operator API	지원됨	지원됨
OpenShift Virtualization	지원되지 않음	지원되지 않음
IPsec 암호화를 포함한 OVN-Kubernetes	지원됨	지원됨

기능	IBM Power	IBM Z 및 IBM® LinuxONE
PodDisruptionBudget	지원됨	지원됨
PTP(Precision Time Protocol) 하드웨어	지원되지 않음	지원되지 않음
Red Hat OpenShift Local	지원되지 않음	지원되지 않음
스케줄러 프로파일	지원됨	지원됨
SCTP(스트림 제어 전송 프로토콜)	지원됨	지원됨
다중 네트워크 인터페이스 지원	지원됨	지원됨
3-노드 클러스터 지원	지원됨	지원됨
토폴로지 관리자	지원됨	지원되지 않음
SCSI 디스크의 z/VM Emulated FBA 장치	지원되지 않음	지원됨
4K FCP 블록 장치	지원됨	지원됨

표 1.2. 영구 스토리지 옵션

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

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

표 1.3. Operator

기능	IBM Power	IBM Z 및 IBM® LinuxONE
Cluster Logging Operator	지원됨	지원됨
Cluster Resource Override Operator	지원됨	지원됨
Compliance Operator	지원됨	지원됨
File Integrity Operator	지원됨	지원됨
Local Storage Operator	지원됨	지원됨
MetalLB Operator	지원됨	지원됨
NFD Operator	지원됨	지원됨
NMState Operator	지원됨	지원됨
OpenShift Elasticsearch Operator	지원됨	지원됨
Service Binding Operator	지원됨	지원됨
Vertical Pod Autoscaler Operator	지원됨	지원됨

표 1.4. Multus CNI 플러그인

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

표 1.5. CSI 볼륨

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

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

1.3.8. 이미지

1.3.8.1. 이미지 스트림에서 매니페스트 나열 이미지 지원

OpenShift Container Platform 4.13에서는 이제 이미지 스트림에 나열된 매니페스트 이미지에 대한 지원을 일반적으로 사용할 수 있습니다.

1.3.9. 보안 및 컴플라이언스

1.3.9.1. AES-GCM 암호화 지원

OpenShift Container Platform에서 etcd 암호화를 활성화할 때 AES-GCM 암호화 유형이 지원됩니다. AES-GCM 암호화 유형의 암호화 키는 매주 순환됩니다.

자세한 내용은 지원되는 암호화 유형을 참조하십시오.

1.3.10. 네트워킹

1.3.10.1. 네트워킹 지표 개선

1.3.10.1.1. egress_ips_rebalance_total

- 지표 이름: **ovnkube_master_egress_ips_rebalance_total**
- 도움말 메시지: 다른 노드로 이동하는 데 필요한 총 송신 **IP** 횟수입니다.

1.3.10.1.2. egress_ips_node_unreachable_total

- 메트릭 이름: **ovnkube_master_egress_ips_node_unreachable_total**
- 도움말 메시지:할당된 송신 **IP**에 할당된 총 횟수에 연결할 수 없었습니다.

1.3.10.1.3. egress_ips_unassign_latency_seconds

- 지표 이름: **ovnkube_master_egress_ips_unassign_latency_seconds**
- 도움말 메시지:**OVN northbound** 데이터베이스에서 송신 **IP** 할당 해제 대기 시간입니다.

1.3.10.1.4. interfaces_total

- 지표 이름: **ovs_vswitchd_interfaces_total**
- 도움말 메시지:포드 및 **Open vSwitch** 인터페이스에 대해 생성된 총 **Open vSwitch** 인터페이스 수를 사용할 수 있습니다.

1.3.10.1.5. interface_up_wait_seconds_total

- 지표 이름: **ovs_vswitchd_interface_up_wait_seconds_total**
- 도움말 메시지:포드를 대기하는 데 필요한 총 초 수와 **Open vSwitch** 인터페이스를 사용할 수 있을 때까지의 총 시간(초)입니다.

1.3.10.1.6. ovnkube_resource_retry_failures_total

- 메트릭 이름: **ovnkube_resource_retry_failures_total**
- 도움말 메시지:**Kubernetes** 리소스를 처리하는 총 횟수가 최대 재시도 제한에 도달하여 더 이상 처리되지 않았습니다.

1.3.10.2. 네트워킹 경고 기능 개선

- OVN Kubernetes는 클레임을 삭제하기 전에 최대 15번 재시도합니다. 이번 업데이트를 통해 이 오류가 발생하면 OpenShift Container Platform에서 클러스터 관리자에게 경고합니다. 각 경고에 대한 설명은 콘솔에서 볼 수 있습니다.

1.3.10.2.1. NoOvnMasterLeader

- 요약: ovn-kubernetes 마스터 리더가 없습니다.
- 콘솔의 설명:

> **Networking control plane is degraded. Networking configuration updates applied to the cluster will not be implemented while there is no OVN Kubernetes leader. Existing workloads should continue to have connectivity. OVN-Kubernetes control plane is not functional.**

1.3.10.2.2. OVNKubernetesNodeOVSOverflowUserspace

- 요약: OVS vSwitch 데몬은 버퍼 오버플로로 인해 패킷을 삭제합니다.
- 콘솔의 설명:

> **Netlink messages dropped by OVS vSwitch daemon due to netlink socket buffer overflow. This will result in packet loss.**

1.3.10.2.3. OVNKubernetesNodeOVSOverflowKernel

- 요약: OVS 커널 모듈은 버퍼 오버플로로 인해 패킷을 삭제합니다.
- 콘솔의 설명:

> **Netlink messages dropped by OVS kernel module due to netlink socket buffer overflow. This will result in packet loss.**

1.3.10.3. devfile IPAddressPool 리소스의 IP 주소를 특정 네임스페이스 및 서비스에 할당

이번 업데이트를 통해 CloudEvent **IPAddressPool** 리소스의 IP 주소를 서비스, 네임스페이스 또는 둘 다에 할당할 수 있습니다. 이 기능은 IP 주소 풀에서 특정 서비스 및 네임스페이스에 IP 주소를 고정하기 위해 CloudEvent가 필요한 muti 테넌트 베어 메탈 환경에서 유용합니다. 많은 IP 주소 풀의 IP 주소를 서비스 및

네임스페이스에 할당할 수 있습니다. 그런 다음 이러한 IP 주소 풀의 우선 순위를 정의할 수 있으므로 CloudEvent에서 더 높은 우선순위 IP 주소 풀부터 시작하는 IP 주소를 할당할 수 있습니다.

IP 주소 풀의 IP 주소를 서비스 및 네임스페이스에 할당하는 방법에 대한 자세한 내용은 CloudEvent 주소 풀 구성을 참조하십시오.

1.3.10.4. 이중 포트 NIC를 사용하여 노드에 OpenShift Container Platform 설치 지원 (기술 프리뷰)

이번 업데이트를 통해 다음 방법을 사용하여 두 개의 물리적 기능(PF)에서 2개의 VF(가상 기능)가 있는 본딩 인터페이스에 OpenShift Container Platform 클러스터를 배포할 수 있습니다.

- 에이전트 기반 설치
- 설치 프로그램에서 제공하는 인프라 설치
- 사용자 프로비저닝 인프라 설치

듀얼 포트 NIC가 있는 노드에 OpenShift Container Platform을 설치하는 방법에 대한 자세한 내용은 SR-IOV 장치의 NIC 파티셔닝을 참조하십시오.

1.3.10.5. BlueField-2 네트워크 장치를 DPDK(데이터 처리 장치) 모드에서 NIC(네트워크 인터페이스 컨트롤러) 모드로 전환하는 지원

이번 릴리스에서는 DPDK(데이터 처리 장치) 모드에서 NIC(네트워크 인터페이스 컨트롤러) 모드로 BlueField-2 네트워크 장치를 전환할 수 있습니다.

자세한 내용은 BlueField-2를 DPU에서 NIC로 전환을 참조하십시오.

1.3.10.6. 네트워크 카드의 MT2892 제품군의 하드웨어 오프로드 [ConnectX-6 Dx]는 GA입니다.

OpenShift Container Platform 4.13에서는 네트워크 카드의 MT2892 제품군 [ConnectX-6 Dx]에 대한 OvS Hardware Offload 지원이 추가되었습니다.

자세한 내용은 지원 장치를 참조하십시오.

1.3.10.7. OpenShift SDN 네트워크 플러그인으로 마이그레이션

OVN-Kubernetes 네트워크 플러그인을 사용하는 경우 OpenShift SDN 네트워크 플러그인으로 마이그레이션할 수 있습니다.

자세한 내용은 OpenShift SDN 네트워크 플러그인으로 마이그레이션을 참조하십시오.

1.3.10.8. CoreDNS 1.10.1로 업데이트

OpenShift Container Platform 4.13은 CoreDNS를 1.10.1로 업데이트합니다. CoreDNS는 이제 원래 클라이언트 쿼리에 지정된 DNSSEC DO Bit을 사용합니다. 클라이언트가 DNSSEC를 요청하지 않는 경우 DNS 응답 UDP 패킷 크기가 줄어듭니다. 결과적으로 작은 패킷 크기로 인해 TCP 연결 재시도 및 전체 DNS 대역폭에 의해 DNS 잘림이 저하될 가능성이 줄어듭니다.

1.3.10.9. 클러스터 네트워크 IP 주소 범위 확장

클러스터에 노드 추가를 지원하도록 클러스터 네트워크를 확장할 수 있습니다. 예를 들어 클러스터를 배포하고 **10.128.0.0/19** 를 클러스터 네트워크 범위와**23** 의 호스트 접두사로 지정한 경우 16개의 노드로 제한됩니다. 클러스터의 CIDR 마스크를 **/14** 로 변경하여 이를 510 노드로 확장할 수 있습니다. 자세한 내용은클러

스터 네트워크 범위 구성을 참조하십시오.

1.3.10.10. VMware vSphere 클러스터의 듀얼 스택 IPv4/IPv6

설치 관리자 프로비저닝 vSphere 클러스터에서는 IPv4가 있는 듀얼 스택 네트워킹을 기본 IP 제품군으로, IPv6를 보조 주소 제품군으로 사용할 수 있습니다. 자세한 내용은 네트워크 구성 매개변수를 참조하십시오.

1.3.10.11. 베어 메탈 듀얼 스택 클러스터에서 기본 IP 주소 제품군인 IPv6

베어 메탈에 클러스터를 설치하는 동안 듀얼 스택 클러스터에서 IPv6를 기본 IP 주소 제품군으로 구성할 수 있습니다. 새 클러스터를 설치할 때 이 기능을 활성화하려면 머신 네트워크, 클러스터 네트워크, 서비스 네트워크, API VIP 및 ingress VIP의 IPv4 주소 제품군 앞에 IPv6 주소 제품군을 지정합니다.

자세한 내용은 다음 소스를 참조하십시오.

- 설치 관리자 프로비저닝 인프라: 듀얼 스택 네트워킹으로 배포
- 사용자 프로비저닝 인프라: 네트워크 구성 매개변수

1.3.10.12. OVN-Kubernetes는 보조 네트워크로 사용 가능(기술 프리뷰)

이번 릴리스에서는 Red Hat OpenShift Networking OVN-Kubernetes 네트워크 플러그인을 통해 Pod에 대한 보조 네트워크 인터페이스를 구성할 수 있습니다. 보조 네트워크로 OVN-Kubernetes는 계층 2(스위스) 토폴로지 네트워크를 지원합니다. 이는 기술 프리뷰 기능으로 사용할 수 있습니다.

보조 네트워크로 OVN-Kubernetes에 대한 자세한 내용은 OVN-Kubernetes 추가 네트워크의 구성을 참조하십시오.

1.3.10.13. OVN-Kubernetes 네트워크 플러그인의 송신 방화벽에 노드 선택기 추가

OpenShift Container Platform 4.13에서 **nodeSelector** 가 OVN-Kubernetes 네트워크 플러그인의 송신 방화벽 대상 사양에 추가되었습니다. 이 기능을 사용하면 하나 이상의 노드에 레이블을 추가할 수 있으며 선택한 노드의 IP 주소가 관련 규칙에 포함됩니다. 자세한 내용은 EgressFirewall에 대한 nodeSelector 예제를 참조하십시오.

1.3.10.14. RHOSP에서 실행되는 클러스터의 OVN-Kubernetes 마이그레이션 절차 (기술 프리뷰)

이제 RHOSP에서 실행되고 Kuryr를 OVN-Kubernetes로 사용하는 클러스터를 마이그레이션할 수 있습니다.

자세한 내용은 Kuryr 네트워크 플러그인에서 OVN-Kubernetes 네트워크 플러그인으로 마이그레이션을 참조하십시오.

1.3.10.15. RHOSP에서 실행되는 클러스터에 대한 송신 IP 지원 개선

RHOSP에서 실행되고 OVN-Kubernetes를 사용하는 클러스터의 경우 예약 포트에 유동 IP 주소를 수동으로 다시 할당할 필요가 없습니다. 예약 포트가 한 노드에서 제거되고 다른 포트에서 다시 생성되는 경우 이제 재할당이 자동으로 수행됩니다.

1.3.10.16. SR-IOV에서 지원되는 하드웨어 (Single Root I/O Virtualization)

OpenShift Container Platform 4.13에서는 다음과 같은 SR-IOV 장치에 대한 지원이 추가되었습니다.

- Intel E810-XXVDA4T

- Intel X710 Base T

자세한 내용은 지원 장치를 참조하십시오.

1.3.11. 스토리지

1.3.11.1. KMS에서 재암호화에 대한 고객 관리 키 지원

이번 업데이트를 통해 AWS의 기본 인증 정보 요청이 수정되어 KMS(Key Management Service)에서 고객 관리 키를 다시 암호화할 수 있습니다. 수동 모드를 사용하도록 구성된 CCO(Cloud Credential Operator)가 있는 클러스터의 경우 관리자는 키 정책에 **kms:ReEncrypt*** 권한을 추가하여 이러한 변경 사항을 수동으로 적용해야 합니다. 다른 관리자는 이 변경의 영향을 받지 않습니다. (OCPBUGS-5410)

1.3.11.2. 논리 볼륨 관리자 스토리지(LVM Storage)에 대한 듀얼 스택 지원

OpenShift Container Platform 4.13에서는 IPv4 및 IPv6 네트워크 환경에서 LVM 스토리지가 이중 스택에서 지원됩니다. 자세한 내용은 듀얼 스택 클러스터 네트워크로 변환을 참조하십시오.

1.3.11.3. GitOps ZTP의 LVM 스토리지 지원

OpenShift Container Platform 4.13에서는 GitOps ZTP를 통해 LVM(Logical Volume Manager Storage)을 추가하고 구성할 수 있습니다. 자세한 내용은 PolicyGenTemplate CR 및 LVM Storage를 사용하여 LVM 스토리지 구성 을 참조하십시오.

1.3.11.4. 연결이 끊긴 환경의 LVM 스토리지 지원

OpenShift Container Platform 4.13에서는 연결이 끊긴 환경에 LVM 스토리지를 설치할 수 있습니다. 자세한 내용은 연결이 끊긴 환경에서 LVM 스토리지 설치를 참조하십시오.

1.3.11.5. 사용자 관리 암호화 사용 가능

사용자 관리 암호화 기능을 사용하면 설치 중에 OpenShift Container Platform 노드 루트 볼륨을 암호화하는 키를 제공하고 모든 관리 스토리지 클래스에서 이 키를 사용하여 프로비저닝된 스토리지 볼륨을 암호화할 수 있습니다. 이를 통해 플랫폼의 기본 계정 키가 아닌 선택한 키로 스토리지 볼륨을 암호화할 수 있습니다.

이 기능은 다음 스토리지 유형을 지원합니다.

- AWS(Amazon Web Services) Elastic Block Storage (EBS) (자세한 내용은 사용자 관리 암호화)를 참조하십시오.
- Microsoft Azure Disk 스토리지 (자세한 내용은 사용자 관리 암호화)
- GCP(Google Cloud Platform) PD(영구 디스크) 스토리지(자세한 내용은 사용자 관리 암호화)를 참조하십시오.

1.3.11.6. 비정상적인 노드 종료 후 CSI 볼륨 분리 (기술 프리뷰)

CSI(Container Storage Interface) 드라이버는 노드가 비정상적으로 중단될 때 볼륨을 자동으로 분리할 수 있습니다. 비정상적인 노드 종료가 발생하면 노드에 서비스 부족 테인트를 수동으로 추가하여 볼륨에서 자동으로 노드에서 분리할 수 있습니다. 이 기능은 기술 프리뷰 상태에서 지원됩니다.

자세한 내용은 비정상적인 노드 종료 후 CSI 볼륨분리를 참조하십시오.

1.3.11.7. 일반적으로 VMware vSphere 암호화 지원 사용 가능

vSphere에서 실행되는 OpenShift Container Platform에서 VM(가상 머신) 및 영구 볼륨(PV)을 암호화할 수 있습니다.

자세한 내용은 vSphere 영구 디스크 암호화를 참조하십시오.

1.3.11.8. 여러 데이터센터에 대한 VMware vSphere CSI 토폴로지 지원 사용 가능

OpenShift Container Platform 4.12에는 다양한 영역 및 지역에 vSphere용 OpenShift Container Platform을 배포하는 기능이 도입되어 여러 컴퓨팅 클러스터에 배포할 수 있으므로 단일 장애 지점을 방지할 수 있습니다. OpenShift Container Platform 4.13에서는 여러 데이터센터를 통해 배포하고 설치 또는 설치 후 생성된 장애 도메인을 사용하여 토폴로지를 설정할 수 있도록 지원합니다.

자세한 내용은 vSphere CSI 토폴로지 에서 참조하십시오.

1.3.11.9. 일반적으로 사용 가능한 기본 스토리지 클래스를 두 개 이상 생성할 수 있습니다.

OpenShift Container Platform 4.13에서는 둘 이상의 기본 스토리지 클래스를 생성할 수 있습니다. 이 기능을 사용하면 기본값으로 정의된 두 번째 스토리지 클래스를 생성할 수 있으므로 기본 스토리지 클래스를 쉽게 변경할 수 있습니다. 그런 다음 이전 기본 스토리지 클래스에서 기본 상태를 제거하기 전에 두 개의 기본 스토리지 클래스가 일시적으로 있습니다. 짧은 시간 동안 기본 스토리지 클래스가 여러 개 있을 수 있지만 결국 하나의 기본 스토리지 클래스만 있는지 확인해야 합니다.

자세한 내용은 기본 스토리지 클래스 변경 및 다중 기본 스토리지 클래스 변경을참조하십시오.

1.3.11.10. 기본 스토리지 클래스 관리 사용 가능

OpenShift Container Platform 4.13에서는 **ClusterCSIDriver** 오브젝트에 **spec.storageClassState** 필드를 도입하여 OpenShift Container Platform에서 생성한 기본 스토리지 클래스를 관리하여 여러 가지 목표를 수행할 수 있습니다.

- 기본 스토리지 클래스가 있는 경우 스토리지 Operator가 초기 기본 스토리지 클래스를 다시 생성하지 못하도록 합니다.
- 기본 스토리지 클래스 이름 변경 또는 변경
- 동적 프로비저닝을 비활성화하여 정적 프로비저닝을 강제 적용합니다.

자세한 내용은 Managing the default storage class를 참조하십시오.

1.3.11.11. 소급 기본 StorageClass 할당 (기술 프리뷰)

이전 버전에서는 기본 스토리지 클래스가 없는 경우 기본 스토리지 클래스를 요청한 PVC(영구 볼륨 클레임)는 수동으로 삭제하고 다시 생성하지 않는 한 기본 스토리지 클래스를 무기한 보류 상태로 남아 있었습니다. OpenShift Container Platform은 이제 이러한 PVC에 기본 스토리지 클래스를 소급적으로 할당하여 해당 PVC가 보류 중 상태로 유지되지 않도록 할 수 있습니다. 이 기능을 활성화하면 기본 스토리지 클래스가 생성되거나 기존 스토리지 클래스 중 하나가 기본값으로 선언된 후 이전에 설정된 PVC가 기본 스토리지 클래스에 할당됩니다.

이 기능은 기술 프리뷰 상태에서 지원됩니다.

자세한 내용은 Absent 기본 스토리지 클래스를 참조하십시오.

1.3.11.12. IBM Power Virtual Server Block CSI Driver Operator (기술 프리뷰)

OpenShift Container Platform은 IBM Power Virtual Server Block Storage의 CSI(Container Storage Interface) 드라이버를 사용하여 PV(영구 볼륨)를 프로비저닝할 수 있습니다.

자세한 내용은 IBM Power Virtual Server Block CSI Driver Operator에서 참조하십시오.

1.3.11.13. CSI 인라인 임시 볼륨 사용 가능

CSI(Container Storage Interface) 인라인 임시 볼륨은 OpenShift Container Platform 4.5에서 기술 프리뷰 기능으로 도입되었으므로 pod가 배포되고 Pod가 제거될 때 인라인 임시 볼륨을 생성하는 Pod 사양을 정의할 수 있습니다. 이 기능은 이제 일반적으로 사용할 수 있습니다.

이 기능은 지원되는 CSI(Container Storage Interface) 드라이버에서만 사용할 수 있습니다.

이 기능에는 CSI 볼륨 승인 플러그인이 포함되어 있습니다. 이 플러그인은 Pod 승인 시 CSI 임시 볼륨을 프로비저닝할 수 있는 개별 CSI 드라이버를 사용할 수 있는 메커니즘을 제공합니다. 관리자 또는 배포는 **CSIDriver** 오브젝트에 **csi-ephemeral-volume-profile** 레이블을 추가할 수 있으며 레이블은 Admission 플러그인에 의해 검사되고 시행, 경고 및 감사 결정에 사용됩니다.

자세한 내용은 CSI 인라인 임시 볼륨을 참조하십시오.

1.3.11.14. Microsoft Azure File용 자동 CSI 마이그레이션 사용 가능

OpenShift Container Platform 4.8부터는 동등한 CSI(Container Storage Interface) 드라이버로 인트리 볼륨 플러그인에 대한 자동 마이그레이션을 기술 프리뷰 기능으로 사용할 수 있게 되었습니다. 이 기능은 OpenShift Container Platform 4.10에서 Azure File에 대한 지원이 제공되었습니다. OpenShift Container Platform 4.13에서는 이제 일반적으로 사용 가능한 Azure File에 대한 자동 마이그레이션을 지원합니다. Azure File의 CSI 마이그레이션은 기본적으로 활성화되어 있으며 관리자가 수행할 필요가 없습니다.

이 기능은 인트리 오브젝트를 해당 CSI 표현으로 자동 변환하므로 사용자에게 완전히 투명해야 합니다. 변환된 오브젝트는 디스크에 저장되지 않으며 사용자 데이터는 마이그레이션되지 않습니다.

in-tree 스토리지 플러그인을 참조하는 스토리지 클래스는 계속 작동하지만 기본 스토리지 클래스를 CSI 스토리지 클래스로 전환하는 것이 좋습니다.

자세한 내용은 CSI 자동 마이그레이션 을 참조하십시오.

1.3.11.15. VMware vSphere에 대한 자동 CSI 마이그레이션이 일반적으로 사용 가능

이 기능은 인트리 오브젝트를 해당 CSI 표현으로 자동 변환하므로 사용자에게 완전히 투명해야 합니다. in-tree 스토리지 플러그인을 참조하는 스토리지 클래스는 계속 작동하지만 기본 스토리지 클래스를 CSI 스토리지 클래스로 전환하는 것이 좋습니다.

OpenShift Container Platform 4.8부터는 동등한 CSI(Container Storage Interface) 드라이버로 인트리 볼륨 플러그인에 대한 자동 마이그레이션을 기술 프리뷰 기능으로 사용할 수 있게 되었습니다. vSphere에 대한 지원은 OpenShift Container Platform 4.10에서 이 기능을 통해 제공되었습니다. OpenShift Container Platform 4.13에서는 일반적으로 사용 가능한 vSphere에 대한 자동 마이그레이션을 지원합니다.

OpenShift Container Platform 4.13 이상을 새로 설치하는 경우 자동 마이그레이션이 기본적으로 활성화됩니다. 그러나 OpenShift Container Platform 4.12 또는 이전 버전에서 4.13으로 업데이트할 때 vSphere에 대한 자동 CSI 마이그레이션은 옵트인하는 경우에만 수행됩니다. 마이그레이션에 옵트인하기 전에 표시된 결과를 신중하게 검토합니다.

다음 조건이 모두 true인 경우 OpenShift Container Platform 4.12에서 4.13으로, 4.13에서 4.14로 업데이트가 차단됩니다.

- CSI 마이그레이션이 아직 활성화되지 않았습니다.
- OpenShift Container Platform은 vSphere 7.0u3L+ 또는 8.0u2 이상에서 실행되지 않습니다.
- vSphere in-tree PV(영구 볼륨)가 있습니다.

자세한 내용은 CSI 자동 마이그레이션 을 참조하십시오.

1.3.11.16. AWS EFS CSI 드라이버에 대한 교차 계정 지원 사용 가능

계정 간 지원을 통해 하나의 AWS(Amazon Web Services) 계정에 OpenShift Container Platform 클러스터를 사용하고 AWS EBS(Elastic File System) CSI(Container Storage Interface) 드라이버를 사용하여 다른 AWS 계정에 파일 시스템을 마운트할 수 있습니다.

자세한 내용은 AWS EFS CSI cross account support에서 참조하십시오.

1.3.11.17. Kubelet 대신 CSI Driver에 FSGroup 위임 사용 가능

이 기능을 사용하면 OpenShift Container Platform에서 볼륨이 마운트될 때 Pod의 FSGroup을 CSI(Container Storage Interface) 드라이버에 제공할 수 있습니다. Microsoft Azure File CSI 드라이버는 이 기능에 따라 다릅니다.

1.3.11.18. NFS를 지원하는 Azure File 사용 가능

OpenShift Container Platform 4.13은 일반적으로 사용 가능한 NFS(Network File System)를 사용하는 CSI(Azure File Container Storage Interface) Driver Operator를 지원합니다.

자세한 내용은 NFS 지원을 참조하십시오.

1.3.12. Operator 라이프사이클

1.3.12.1. OpenShift CLI를 사용하여 Operator 버전 찾기

OpenShift Container Platform 4.13에서는 다음 OpenShift CLI (oc) 명령을 실행하여 시스템에 설치할 수 있는 Operator 버전 및 채널을 찾을 수 있습니다.

oc describe 명령 구문의 예

```
$ oc describe packagemanifests <operator_name> -n <catalog_namespace>
```

다음 명령을 실행하여 Operator 버전 및 채널 정보의 출력 형식을 지정할 수 있습니다.

oc get 명령 구문의 예

```
$ oc get packagemanifests <operator_name> -n <catalog_namespace> -o <output_format>
```

자세한 내용은 특정 버전의 Operator 설치를 참조하십시오.

1.3.12.2. 다중 테넌트 클러스터의 Operator

OLM(Operator Lifecycle Manager)의 기본 동작은 Operator 설치 중에 단순화를 제공하는 것입니다. 그러나 이러한 동작으로 인해 특히 다중 테넌트 클러스터에서 유연성이 부족할 수 있습니다.

다중 테넌트 클러스터에서 Operator 관리에 대한 지침 및 권장 솔루션이 다음 주제를 사용하여 추가되었습니다.

- 다중 테넌트 클러스터의 Operator
- 다중 테넌트 클러스터에 대한 Operator의 여러 인스턴스 준비

1.3.12.3. 네임스페이스에 Operator 공동 배치

OLM(Operator Lifecycle Manager)은 동일한 네임스페이스에 설치된 OLM 관리 Operator를 처리합니다. 즉 서브스크립션 리소스는 관련 Operator와 동일한 네임스페이스에 배치됩니다. OLM은 실제로 관련이 없는 경우에도 버전 및 업데이트 정책과 같은 상태를 업데이트할 때 해당 상태를 고려합니다.

Operator 공동 배치 및 사용자 지정 네임스페이스를 사용하는 대체 절차에 대한 지침이 다음 주제와 함께 추가되었습니다.

- 네임스페이스에 Operator 공동 배치
- 사용자 지정 네임스페이스에 글로벌 Operator 설치

1.3.12.4. CSV 복사본 비활성화 시 업데이트된 웹 콘솔 동작

클러스터에서 CSV(클러스터 서비스 버전)가 비활성화되어 있는 경우 OpenShift Container Platform 웹 콘솔이 더 나은 Operator 검색을 제공하도록 업데이트되었습니다.

클러스터 관리자가 CSV를 복사할 수 없는 경우 CSV가 실제로 모든 네임스페이스에 복사되지 않더라도 일반 사용자를 위해 모든 네임스페이스의 **openshift** 네임스페이스에서 CSV 복사를 표시하도록 웹 콘솔을 수정합니다. 이를 통해 일반 사용자는 네임스페이스에서 이러한 Operator의 세부 정보를 확인하고 전역적으로 설치된 Operator가 제공하는 CR(사용자 정의 리소스)을 생성할 수 있습니다.

자세한 내용은 복사된 CSV 비활성화를 참조하십시오.

1.3.13. Operator 개발

1.3.13.1. 기본 노드 선택기로 제안된 네임스페이스 템플릿 설정

이번 릴리스에서는 Operator 작성자가 Operator가 실행되는 제안된 네임스페이스에 기본 노드 선택기를 설정할 수 있습니다. 제안된 네임스페이스는 CSV(**ClusterServiceVersion**)에 포함된 YAML의 네임스페이스 매니페스트를 사용하여 생성됩니다. OperatorHub를 사용하여 클러스터에 Operator를 추가하면 웹 콘솔은 설치 프로세스 중에 클러스터 관리자에게 제안된 네임스페이스를 자동으로 채웁니다.

자세한 내용은 기본 노드 선택기로 제안된 네임스페이스 설정을참조하십시오.

1.3.13.2. Node Tuning Operator

NodeTuning 클러스터 기능을 사용하여 NFD(Node Tuning Operator)를 활성화/비활성화할 수 있습니다. 클러스터 설치 시 비활성화된 경우 나중에 다시 활성화할 수 있습니다. 자세한 내용은 Node Tuning 기능을 참조하십시오.

1.3.14. 머신 API

1.3.14.1. 컨트롤 플레인 머신 세트에 대한 추가 플랫폼 지원

- 이번 릴리스에서는 Google Cloud Platform 클러스터에서 컨트롤 플레인 머신 세트가 지원됩니다.

- 이 릴리스에는 Microsoft Azure 클러스터에서 컨트롤 플레인 머신 세트의 사용자 환경에 대한 향상된 기능이 포함되어 있습니다. OpenShift Container Platform 버전 4.13과 함께 설치되거나 업그레이드된 Azure 클러스터의 경우 더 이상 컨트롤 플레인 머신 세트 사용자 정의 리소스(CR)를 생성할 필요가 없습니다.
  - 버전 4.13을 사용하여 설치된 클러스터에는 기본적으로 활성화된 컨트롤 플레인 머신 세트가 있습니다.
  - 버전 4.13으로 업그레이드된 클러스터의 경우 클러스터에 대해 비활성 CR이 생성되고 CR의 값이 컨트롤 플레인 시스템에 적합한지 확인한 후 활성화할 수 있습니다.

자세한 내용은 Control Plane Machine Set Operator 시작하기를참조하십시오.

1.3.15. Machine Config Operator

1.3.15.1. RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층 지정 사용 가능

이제 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층을 일반적으로 사용할 수 있습니다. 이 기능을 사용하면 추가 이미지를 기본 이미지에 계층화하여 기본 RHCOS 이미지의 기능을 확장할 수 있습니다.

자세한 내용은 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층 지정을참조하십시오.

1.3.15.2. RHCOS에 타사 및 사용자 정의 콘텐츠 추가 지원

RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층을 사용하여 RHEL(Red Hat Enterprise Linux) 및 타사 패키지를 클러스터 노드에 추가할 수 있습니다.

자세한 내용은 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층 지정을참조하십시오.

1.3.15.3. 코어 사용자 암호 설정 지원

이제 RHCOS 코어 사용자의 암호를 생성할 수 있습니다. SSH 또는**oc debug node** 명령을 사용하여 노드에 액세스할 수 없는 경우 이 암호를 사용하면 **core** 사용자를 사용하여 클라우드 공급자 직렬 콘솔 또는 베어 메탈 BMC(Baseboard Controller manager)를 통해 노드에 액세스할 수 있습니다.

자세한 내용은 노드 액세스의 코어 사용자 암호 변경을참조하십시오.

1.3.16. 노드

1.3.16.1. 태그를 통한 이미지 레지스트리 저장소 미러링

이제 다이제스트 사양 외에도 이미지 태그를 사용하여 미러링된 레지스트리에서 이미지를 가져올 수 있습니다. 이러한 변경을 수행하기 위해 **ImageContentSourcePolicy** (ICSP) 오브젝트가 더 이상 사용되지 않습니다. 이제 다이제스트 사양 또는 **ImageTagMirrorSet** (ITMS) 오브젝트를 사용하여 이미지 태그를 사용하여 이미지를 가져오도록 **ImageDigestMirrorSet** (IDMS) 오브젝트를 사용할 수 있습니다.

ICSP 오브젝트를 생성하는 데 사용한 기존 YAML 파일이 있는 경우 **oc adm migrate icsp** 명령을 사용하여 해당 파일을 IDMS YAML 파일로 변환할 수 있습니다.

이러한 새 오브젝트에 대한 자세한 내용은 이미지 레지스트리 저장소 미러링 구성을참조하십시오.

기존 ICSP YAML 파일을 IDMS YAML 파일로 변환하는 방법에 대한 자세한 내용은 이미지 레지스트리 저장소 미러링을 위한 ICSP (ICSP) 파일 변환을 참조하십시오.

1.3.16.2. crun 정식 출시일

이제 OpenShift Container Platform 4.13에서 crun 하위 수준 컨테이너 런타임을 일반적으로 사용할 수 있습니다. GA 버전에는 새로운 기능이 없습니다.

1.3.16.3. Linux Control Group 버전 2(cgroup v2) 정식 출시일

이제 OpenShift Container Platform 4.13에서 Linux Control Group 버전 2(cgroup v2)를 일반적으로 사용할 수 있습니다. GA 버전에는 새로운 기능이 없습니다.

1.3.16.4. Pod 중단 예산 (PDB) 비정상적인 Pod 제거 정책 (기술 프리뷰)

이번 릴리스에서는 PDB(Pod 중단 예산)에 대한 비정상적인 Pod 제거 정책을 기술 프리뷰 기능으로 지정할 수 있습니다. 이는 노드를 드레이닝하는 동안 애플리케이션의 오작동을 제거하는 데 도움이 될 수 있습니다.

이 기술 프리뷰 기능을 사용하려면 **TechPreviewNoUpgrade** 기능 세트를 활성화해야 합니다.

> **주의**
>
> 클러스터에서 **TechPreviewNoUpgrade** 기능 세트를 활성화하면 취소할 수 없으며 마이너 버전 업데이트를 방지할 수 없습니다. 프로덕션 클러스터에서 이 기능 세트를 활성화해서는 안 됩니다.

자세한 내용은 비정상 Pod에 대한 제거 정책 지정을참조하십시오.

1.3.16.5. Metal3 수정 지원

이전에는 Machine Health Checks가 자체 대응하거나 Self Node Remediation 공급자를 사용할 수 있었습니다. 이번 릴리스에서는 베어 메탈 클러스터에서 새 Metal3 수정 공급자도 지원됩니다.

자세한 내용은 베어 메탈의 전원 기반 업데이트 적용정보를 참조하십시오.

1.3.17. 모니터링

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

1.3.17.1. 모니터링 스택 구성 요소 및 종속 항목에 대한 업데이트

이 릴리스에는 스택 구성 요소 및 종속 항목을 모니터링하기 위한 다음 버전 업데이트가 포함되어 있습니다.

- Alertmanager에서 0.25.0으로
- kube-state-metrics to 2.8.1
- node-exporter를 1.5.0으로
- prom-label-proxy에서 0.6.0으로
- Prometheus를 2.42.0으로

- prometheus-operator to 0.63.0
- Thanos에서 0.30.2로

1.3.17.2. 경고 규칙 변경

참고

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

- **NodeFilesystemAlmostOutOfSpace** 경고는 설계에 의해 항상 가득 찬 특정**tmpfs** 마운트 지점에 대해 더 이상 발생하지 않습니다.

1.3.17.3. Alertmanager 설정에 보안을 추가하는 새로운 옵션

이번 릴리스에서는 코어 플랫폼 모니터링 및 사용자 정의 프로젝트의 Alertmanager 구성에 보안을 추가할 수 있습니다. Alertmanager가 경고를 보낼 수 있도록 수신자로 인증해야 하는 경우 수신자에 대한 인증 자격 증명이 포함된 보안을 사용하도록 Alertmanager를 구성할 수 있습니다.

1.3.17.4. node-exporter 컬렉터를 구성하는 새로운 옵션

이번 릴리스에서는 다음 node-exporter 수집기에 대해 CMO(Cluster Monitoring Operator) 구성 맵 설정을 사용자 지정할 수 있습니다. 다음 node-exporter 수집기는 선택 사항이며 활성화 또는 비활성화할 수 있습니다.

- **buddyinfo** 수집기
- **cpufreq** 수집기
- **netclass** 수집기
- **netdev** 수집기
- **netclass** 수집기의 **netlink** 백엔드
- **tcpstat** 수집기

1.3.17.5. 노드 역할별로 노드 관련 대시보드를 필터링하는 새로운 옵션

OpenShift Container Platform 웹 콘솔에서 노드 역할을 기반으로 노드 관련 모니터링 대시보드에서 데이터를 필터링할 수 있습니다. 작업자 노드와 같은 특정 역할의 노드에 대해서만 대시보드 데이터를 표시하려면 이 새 필터를 사용하여 관련 노드 역할을 빠르게 선택할 수 있습니다.

1.3.17.6. 메트릭 컬렉션 프로필을 활성화하는 새로운 옵션 (기술 프리뷰)

이 릴리스에서는 기본 플랫폼 모니터링에 대한 기술 프리뷰 기능을 도입하여 관리자가 기본 메트릭 데이터 또는 최소 양의 메트릭 데이터를 수집하도록 메트릭 수집 프로필을 설정할 수 있습니다. 최소 프로필을 활성화하면 경고와 같은 기본 모니터링 기능이 계속 작동하지만 Prometheus에 필요한 CPU 및 메모리 리소스가 감소합니다.

1.3.18. Network Observability Operator

Network Observability Operator는 OpenShift Container Platform 마이너 버전 릴리스 스트림과 별도로 업데이트를 릴리스합니다. 업데이트는 현재 지원되는 모든 OpenShift Container Platform 4 버전에서 지

원되는 단일 롤링 스트림을 통해 제공됩니다. Network Observability Operator의 새로운 기능, 개선 사항 및 버그 수정에 대한 정보는 Network Observability 릴리스 노트에서 확인할 수 있습니다.

1.3.19. 확장 및 성능

1.3.19.1. NUMA 리소스 Operator를 사용한 NUMA 인식 스케줄링 사용 가능

NUMA 리소스 Operator를 사용한 NUMA 인식 예약은 이전에 OpenShift Container Platform 4.10에서 기술 프리뷰로 도입되었으며 이제 OpenShift Container Platform 4.13에서 일반적으로 사용할 수 있습니다.

NUMA 리소스 Operator는 클러스터에서 사용 가능한 NUMA 영역에 대한 전체 이미지를 기반으로 워크로드에 대한 스케줄링을 결정하는 NUMA 인식 보조 스케줄러를 배포합니다. 이렇게 향상된 NUMA 인식 스케줄링을 통해 대기 시간에 민감한 워크로드를 단일 NUMA 영역에서 처리하여 효율성과 성능을 극대화합니다.

이번 업데이트에서는 다음 기능이 추가되었습니다.

- NUMA 리소스 보고서의 API 폴링 미세 조정.
- 노드 토폴로지 내보내기에 대한 노드 그룹 수준에서 구성 옵션입니다.

자세한 내용은 NUMA 인식 워크로드 스케줄링을 참조하십시오.

1.3.19.2. 3-노드 클러스터 및 표준 클러스터의 워크로드 파티셔닝 지원 (기술 프리뷰)

이번 업데이트 이전에는 단일 노드 OpenShift 클러스터에만 워크로드 파티셔닝이 지원되었습니다. 이제 3-노드 컴팩트 클러스터 및 표준 클러스터의 워크로드 파티셔닝을 구성할 수도 있습니다. 워크로드 파티셔닝을 사용하여 예약된 CPU 세트에서 실행되도록 OpenShift Container Platform 서비스, 클러스터 관리 워크로드 및 인프라 Pod를 분리합니다.

자세한 내용은 워크로드 파티셔닝을 참조하십시오.

1.3.19.3. GitOps ZTP를 사용하여 전원 상태 구성

OpenShift Container Platform 4.12에는 중요 및 중요하지 않은 워크로드의 전원 상태를 설정하는 기능이 도입되었습니다. OpenShift Container Platform 4.13에서는 GitOps ZTP를 사용하여 전원 상태를 구성할 수 있습니다.

기능에 대한 자세한 내용은 PolicyGenTemplates CR을 사용하여 전원 상태구성을 참조하십시오.

1.3.19.4. TALM 및 GitOps ZTP로 관리되는 클러스터의 컨테이너 이미지 사전 캐싱

이번 릴리스에서는 GitOps ZTP와 함께 사용할 수 있는 두 가지 새로운 토폴로지 라이프사이클 관리자(TALM) 기능이 추가되었습니다.

- 새 검사를 통해 클러스터를 업데이트하기 전에 관리 클러스터 호스트에서 사용 가능한 디스크 공간이 충분한지 확인합니다. 이제 컨테이너 이미지 사전 캐싱 중에 TALM은 사용 가능한 호스트 디스크 공간을 예상 OpenShift Container Platform 이미지 크기와 비교하여 호스트에 디스크 공간이 충분한지 확인합니다.
- **ConfigMap** CR의 새로운**excludePrecachePatterns** 필드를 사용하면 업데이트 전에 이미지 TALM이 클러스터 호스트에 다운로드하는 사전 캐시를 제어하는 데 사용할 수 있습니다.

자세한 내용은 컨테이너 이미지 사전 캐시 필터 사용을참조하십시오.

1.3.19.5. HTTP 전송은 PTP 및 베어 메탈 이벤트용 AMQP 대체(기술 프리뷰)

HTTP는 이제 PTP 및 베어 메탈 이벤트 인프라에서 기본 전송입니다. AMQ Interconnect는 2024년 6월 30일부터 EOL(End of Life)입니다.

자세한 내용은 PTP 빠른 이벤트 알림 프레임워크정보를 참조하십시오.

1.3.19.6. Intel E810 웨스트 포트 채널 NIC를 PTP 회선 마스터 시계로 지원 (기술 프리뷰)

이제 PTP Operator를 사용하여 Intel E810 웨스트 포트 채널 NIC를 PTP 오브 마스터 시계로 구성할 수 있습니다. PTP 무지 마스터 시계는 시스템 클럭 및 네트워크 시간 동기화에 **ts2phc** (시간 스탬프 2 물리적 시계)를 사용합니다.

자세한 내용은 Configuring linuxptp services as a breakingmaster clock 에서참조하십시오.

1.3.19.7. GitOps ZTP에서 관리되는 클러스터의 기본 컨테이너 런타임으로 crun 구성

기본 컨테이너 런타임으로 crun을 구성하는 **ContainerRuntimeConfig** CR은 GitOps ZTP**ztp-site-generate** 컨테이너에 추가되었습니다.

GitOps ZTP를 사용하여 설치하는 클러스터에서 최적의 성능을 위해 단일 노드 OpenShift의 컨트롤 플레인 및 작업자 노드에 대해 crun을, 추가 Day 0 설치 매니페스트 CR과 함께 3노드 OpenShift 및 표준 클러스터에 대해 crun을 활성화합니다.

자세한 내용은 Configuring crun as the default container runtime에서 참조하십시오.

1.3.19.8. 문서 개선: etcd 개요 사용 가능

이제 OpenShift Container Platform 설명서에서 제공되는 이점 및 작동 방식 등 etcd에 대한 개요를 확인할 수 있습니다. Kubernetes의 기본 데이터 저장소인 etcd는 etcd Operator를 통해 OpenShift Container Platform의 클러스터 구성 및 관리에 대한 안정적인 접근 방식을 제공합니다. 자세한 내용은 etcd의 개요 를 참조하십시오.

1.3.20. Insights Operator

OpenShift Container Platform 4.13에서 Insights Operator는 이제 다음 정보를 수집합니다.

- **openshift_apps_deploymentconfigs_strategy_total** 지표 이 메트릭은 배포 구성에서 배포 전략 정보를 수집합니다.
- 머신이 실패하는 이유를 식별하는 추가 머신 리소스 정의
- Authentication Operator의 성능이 저하된 경우 Insights에 알리는 기본 **ingresscontroller.operator.openshift.io** 리소스입니다.

1.3.21. 호스트된 컨트롤 플레인(기술 프리뷰)

1.3.21.1. 호스트된 컨트롤 플레인 섹션 사용 가능

OpenShift Container Platform 설명서에는 호스트된 컨트롤 플레인 전용 섹션이 포함되어 있습니다. 이 섹션에는 호스팅된 클러스터 구성 및 관리에 대한 정보 및 기능 개요가 있습니다. 자세한 내용은 호스팅 컨트롤 플레인 을 참조하십시오.

1.3.21.2. 호스트된 컨트롤 플레인 업데이트

OpenShift Container Platform 설명서에 호스트 컨트롤 플레인 업데이트에 대한 정보가 포함되어 있습니다. 호스트된 컨트롤 플레인을 업데이트하려면 호스팅 클러스터 및 노드 풀을 업데이트해야 합니다. 자세한 내용은 호스팅된 컨트롤 플레인 업데이트를 참조하십시오.

1.3.22. 단일 노드에 OpenShift Container Platform을 설치하기 위한 요구사항

4.13에서는 **x86_64** 및 shut64 CPU 아키텍처를 지원합니다.

1.4. 주요 기술 변경 사항

OpenShift Container Platform 4.13에는 다음과 같은 주요 기술 변경 사항이 추가되었습니다.

추가 클라우드 공급자를 위한 클라우드 컨트롤러 관리자
Kubernetes 커뮤니티는 클라우드 컨트롤러 관리자를 사용하기 위해 Kubernetes 컨트롤러 관리자 사용을 사용 중단하여 기본 클라우드 플랫폼과 상호 작용할 계획입니다. 따라서 새 클라우드 플랫폼에 대한 Kubernetes 컨트롤러 관리자 지원을 추가할 계획이 없습니다.

이 OpenShift Container Platform 릴리스에 추가된 Nutanix 구현에서는 클라우드 컨트롤러 관리자를 사용합니다. 또한 이 릴리스에서는 VMware vSphere용 클라우드 컨트롤러 관리자를 사용할 수 있는 General Availability를 소개합니다.

클라우드 컨트롤러 관리자에 대한 자세한 내용은 Kubernetes Cloud Controller Manager 설명서를 참조하십시오.

클라우드 컨트롤러 관리자 및 클라우드 노드 관리자 배포 및 라이프사이클을 관리하려면 Cluster Cloud Controller Manager Operator를 사용합니다.

자세한 내용은 *Platform Operator 참조*의 Cluster Cloud Controller Manager Operator 항목을 참조하십시오.

MCD에서 일시 중지된 풀에서 kubelet CA 인증서를 동기화
이전에는 MCO(Machine Config Operator)에서 kubelet 클라이언트 인증 기관 (CA) 인증서 **/etc/kubernetes/kubelet-ca.crt** 를 일반 머신 구성 업데이트의 일부로 업데이트했습니다. OpenShift Container Platform 4.13부터 **kubelet-ca.crt** 가 일반 머신 구성 업데이트의 일부로 더 이상 업데이트되지 않습니다. 이러한 변경으로 인해 MCD(Machine Config Daemon)는 인증서 변경이 발생할 때마다 **kubelet-ca.crt** 를 최신 상태로 유지합니다.

또한 머신 구성 풀이 일시 중지된 경우 MCD에서 새로 순환된 인증서를 해당 노드로 푸시할 수 있습니다. 인증서 변경 사항이 포함된 새로 렌더링된 머신 구성이 이전 버전과 같이 풀에 대해 생성됩니다. 풀은 업데이트가 필요함을 나타냅니다. 이 조건은 이 제품의 향후 릴리스에서 제거됩니다. 그러나 인증서가 별도로 업데이트되므로 추가 업데이트가 없다고 가정하여 풀을 일시 정지 상태로 유지하는 것이 안전합니다.

또한 노드에 항상 최신 **kubelet-ca.crt** 가 있어야 하므로 **MachineConfigControllerPausedPoolKubeletCA** 경고가 제거되었습니다.

SSH 키 위치 변경
OpenShift Container Platform 4.13에서는 RHEL 9.2 기반 RHCOS가 도입되었습니다. 이번 업데이트 이전에는 RHCOS의 **/home/core/.ssh/authorized_keys** 에 SSH 키가 있었습니다. 이번 업데이트를 통해 RHEL 9.2 기반 RHCOS에서 SSH 키는 **/home/core/.ssh/authorized_keys.d/ignition** 에 있습니다.

기본 OpenSSH **/etc/ssh/sshd_config** 서버 구성 파일을 사용자 지정한 경우 이Red Hat 지식베이스 문서에 따라 업데이트해야 합니다.

Pod 보안 허용에 대한 향후 제한 적용
현재는 Pod 보안 위반이 감사 로그에 기록되어 경고로 표시되지만 Pod는 거부되지 않습니다.

Pod 보안 허용에 대한 글로벌 제한 적용은 현재 OpenShift Container Platform의 다음 마이너 릴리스에 대해 예정되어 있습니다. 이 제한 적용이 활성화되면 Pod 보안 위반이 있는 Pod가 거부됩니다.

향후 변경을 준비하려면 워크로드가 적용되는 Pod 보안 승인 프로필과 일치하는지 확인합니다. 전역 또는 네임스페이스 수준에서 정의된 시행된 보안 표준에 따라 구성되지 않은 워크로드는 거부됩니다. **restricted-v2** SCC는 제한된 Kubernetes 정의에 따라 워크로드를 허용합니다.
https://kubernetes.io/docs/concepts/security/pod-security-standards/#restricted

Pod 보안 위반을 수신하는 경우 다음 리소스를 참조하십시오.

- Pod 보안 위반을 유발하는 워크로드를 찾는 방법에 대한 정보는 Pod 보안 위반 식별을 참조하십시오.
- Pod 보안 승인 라벨 동기화가 수행되는 시기를 이해하려면 Pod 보안 표준과의 보안 컨텍스트 제약 조건 동기화를 참조하십시오. Pod 보안 허용 라벨은 다음과 같은 특정 상황에서 동기화되지 않습니다.
  - 워크로드는 **openshift-** 가 앞에 있는 시스템 생성 네임스페이스에서 실행됩니다.
  - 워크로드는 Pod 컨트롤러 없이 직접 생성된 Pod에서 실행됩니다.
- 필요한 경우 **pod-security.kubernetes.io/enforce** 라벨을 설정하여 네임스페이스 또는 Pod에서 사용자 정의 승인 프로필을 설정할 수 있습니다.

oc-mirror 플러그인에서 OpenShift API 끝점에서 그래프 데이터 컨테이너 이미지를 검색

oc-mirror OpenShift CLI(**oc**) 플러그인은 GitHub에서 전체 그래프 데이터 리포지토리를 다운로드하는 대신 OpenShift API 끝점에서 그래프 데이터 tarball을 다운로드합니다. 외부 공급업체가 아닌 Red Hat에서 이 데이터를 검색하는 것은 외부 콘텐츠에 대한 엄격한 보안 및 규정 준수 제한이 있는 사용자에게 더 적합합니다.

oc-mirror 플러그인이 다운로드한 데이터는 그래프 데이터 리포지토리에 있지만 OpenShift Update Service에는 필요하지 않은 콘텐츠를 제외합니다. 또한 컨테이너는 UBI 대신 UBI 마이크로를 기본 이미지로 사용하므로 이전보다 훨씬 작은 컨테이너 이미지를 생성합니다.

이러한 변경 사항은 oc-mirror 플러그인의 사용자 워크플로에 영향을 미치지 않습니다.

그래프 데이터 컨테이너 이미지의 Dockerfile이 OpenShift API 끝점에서 검색됨

Dockerfile을 사용하여 OpenShift Update Service의 그래프 데이터 컨테이너 이미지를 생성하는 경우 이제 그래프 데이터 tarball이 GitHub 대신 OpenShift API 끝점에서 다운로드됩니다.

자세한 내용은 OpenShift Update Service 그래프 데이터 컨테이너 이미지 생성을참조하십시오.

이제 vSphere 사용자 프로비저닝 인프라 클러스터에서 nodeip-configuration 서비스가 활성화됨

OpenShift Container Platform 4.13에서 이제 vSphere 사용자 프로비저닝 인프라 클러스터에서 **nodeip-configuration** 서비스가 활성화됩니다. 이 서비스는 OpenShift Container Platform에서 노드를 부팅할 때 Kubernetes API 서버와 통신하는 데 사용하는 NIC(네트워크 인터페이스 컨트롤러)를 결정합니다. 드문 경우지만 업그레이드 후 서비스가 잘못된 노드 IP를 선택할 수 있습니다. 이 경우 **NODEIP_HINT** 기능을 사용하여 원래 노드 IP를 복원할 수 있습니다. 네트워크 문제 해결을 참조하십시오.

Operator SDK 1.28

OpenShift Container Platform 4.13에서는 Operator SDK 1.28을 지원합니다. 이 최신 버전을 설치하거나 업데이트하려면 Operator SDK CLI 설치를 참조하십시오.

참고

Operator SDK 1.28에서는 Kubernetes 1.26을 지원합니다.

Operator SDK 1.25를 사용하여 이전에 생성되거나 유지 관리되는 Operator 프로젝트가 있는 경우 Operator SDK 1.28과의 호환성을 유지하도록 프로젝트를 업데이트합니다.

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

RHEL 9.2에 따른 RHCOS의 디스크 순서 동작 변경

OpenShift Container Platform 4.13에서는 RHEL 9.2 기반 RHCOS가 도입되었습니다. 이번 업데이트를 통해 심볼릭 디스크 이름 지정이 재부팅 시 변경될 수 있습니다. 이로 인해 설치 후 구성 파일을 적용하거나 서비스 생성을 위해 **/dev/sda** 와 같은 심볼릭 이름을 사용하는 디스크를 참조하는 노드를 프로비저닝하는 경우 문제가 발생할 수 있습니다. 이 문제의 영향은 구성 중인 구성 요소에 따라 다릅니다. **dev/disk/by-id** 와 같은 특정 디스크 참조를 포함하여 장치에 특정 이름 지정 체계를 사용하는 것이 좋습니다.

이러한 변경으로 인해 모니터링이 각 노드의 설치 장치에 대한 정보를 수집하는 경우 기존 자동화 워크플로우를 조정해야 할 수 있습니다.

자세한 내용은 RHEL 설명서 를 참조하십시오.

호스팅된 컨트롤 플레인의 백업, 복원 및 재해 복구에 대한 문서

OpenShift Container Platform 4.13 설명서에서 호스팅된 클러스터에서 etcd를 백업 및 복원하고 AWS 리전 내 호스팅 클러스터를 복원하는 절차가 "백업 및 복원" 섹션에서 "호스트 컨트롤 플레인" 섹션으로 이동되었습니다. 내용 자체는 변경되지 않았습니다.

1.5. 사용되지 않거나 삭제된 기능

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

더 이상 사용되지 않는 기능은 여전히 OpenShift Container Platform에 포함되어 있으며 계속 지원됩니다. 그러나 이 기능은 향후 릴리스에서 제거될 예정이므로 새로운 배포에는 사용하지 않는 것이 좋습니다. OpenShift Container Platform 4.13에서 더 이상 사용되지 않고 삭제된 주요 기능의 최신 목록은 아래 표를 참조하십시오. 더 이상 사용되지 않고 삭제된 기능에 대한 자세한 내용은 표 뒤에 나열되어 있습니다.

다음 표에서 기능은 다음 상태로 표시됩니다.

- *정식 출시일 (GA)*
- *더 이상 사용되지 않음*
- *Removed*

Operator에서 더 이상 사용되지 않는 기능 및 삭제된 기능

표 1.6. Operator가 더 이상 사용되지 않거나 삭제된 Operator

기능	4.11	4.12	4.13
Operator 카탈로그의 SQLite 데이터베이스 형식	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

이미지가 더 이상 사용되지 않거나 삭제된 기능

표 1.7. 더 이상 사용되지 않거나 삭제된 이미지

기능	4.11	4.12	4.13
Cluster Samples Operator의 **ImageChangesInProgress** 상태	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음
Cluster Samples Operator의 **MigrationInProgress** 상태	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

더 이상 사용되지 않는 기능 및 삭제된 기능

표 1.8. 더 이상 사용되지 않거나 제거된 추적기

기능	4.11	4.12	4.13
vSphere 7.0 업데이트 1 또는 이전	더 이상 사용되지 않음	더 이상 사용되지 않음	삭제됨 [1]
VMware ESXi 7.0 업데이트 1 이하	더 이상 사용되지 않음	더 이상 사용되지 않음	삭제됨 [1]
cluster.local 도메인에 대한 CoreDNS 와일드카드 쿼리	정식 출시일 (GA)	더 이상 사용되지 않음	더 이상 사용되지 않음
설치 관리자 프로비저닝 인프라 클러스터의 **install-config.yaml** 파일의 **ingressVIP** 및 **apiVIP** 설정	정식 출시일 (GA)	더 이상 사용되지 않음	더 이상 사용되지 않음

1. **OpenShift Container Platform 4.13의 경우 사용하는 구성 요소의 요구 사항을 충족하는 VMware vSphere 버전 8.0을 포함하여 VMware vSphere 버전 7.0 업데이트 2 이상 인스턴스에 OpenShift Container Platform 클러스터를 설치해야 합니다.**

더 이상 사용되지 않는 기능 및 삭제된 기능

표 1.9. 더 이상 사용되지 않거나 삭제된 추적기

기능	4.11	4.12	4.13
FlexVolume을 사용하는 영구 스토리지	더 이상 사용되지 않음	더 이상 사용되지 않음	더 이상 사용되지 않음

더 이상 사용되지 않거나 제거된 특수 하드웨어 및 드라이버 지원

표 1.10. 특수 하드웨어 및 드라이버 지원 사용 중단 및 제거된 추적기

기능	4.11	4.12	4.13
SRO(Special Resource Operator)	기술 프리뷰	Removed	Removed

다중 아키텍처 더 이상 사용되지 않는 기능

표 1.11. 다중 아키텍처 더 이상 사용되지 않는 추적기

기능	4.11	4.12	4.13
IBM Power8 모든 모델 (**ppc64le**)	정식 출시일 (GA)	더 이상 사용되지 않음	Removed
IBM Power AC922 (**ppc64le**)	정식 출시일 (GA)	더 이상 사용되지 않음	Removed
IBM Power IC922 (**ppc64le**)	정식 출시일 (GA)	더 이상 사용되지 않음	Removed
IBM Power LC922 (**ppc64le**)	정식 출시일 (GA)	더 이상 사용되지 않음	Removed
IBM z13 모든 모델 (**s390x**)	정식 출시일 (GA)	더 이상 사용되지 않음	Removed
IBM® LinuxONE emperor(**s390x**)	정식 출시일 (GA)	더 이상 사용되지 않음	Removed
IBM® LinuxONE Rockhopper (**s390x**)	정식 출시일 (GA)	더 이상 사용되지 않음	Removed
AMD64 (x86_64) v1 CPU	정식 출시일 (GA)	더 이상 사용되지 않음	Removed

더 이상 사용되지 않거나 삭제된 네트워킹

표 1.12. 더 이상 사용되지 않거나 삭제된 네트워킹

기능	4.11	4.12	4.13
RHOSP의 Kuryr	정식 출시일 (GA)	더 이상 사용되지 않음	더 이상 사용되지 않음

웹 콘솔 더 이상 사용되지 않거나 삭제된 기능

표 1.13. 웹 콘솔 사용 중단 및 제거된 추적기

기능	4.11	4.12	4.13
다중 클러스터 콘솔	기술 프리뷰	기술 프리뷰	Removed

노드 더 이상 사용되지 않으며 삭제된 기능

표 1.14. 더 이상 사용되지 않으며 삭제된 추적기

기능	4.11	4.12	4.13
ImageContentSourcePolicy (ICSP) 오브젝트	정식 출시일 (GA)	정식 출시일 (GA)	더 이상 사용되지 않음
Kubernetes 토폴로지 라벨 **failure-domain.beta.kubernetes.io/zone**	정식 출시일 (GA)	정식 출시일 (GA)	더 이상 사용되지 않음
Kubernetes 토폴로지 라벨 **failure-domain.beta.kubernetes.io/region**	정식 출시일 (GA)	정식 출시일 (GA)	더 이상 사용되지 않음

1.5.1. 더 이상 사용되지 않는 기능

1.5.1.1. RHV(Red Hat Virtualization) 사용 중단

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

1.5.1.2. cluster.local 도메인에 대한 와일드카드 DNS 쿼리는 더 이상 사용되지 않음

CoreDNS는 **cluster.local** 도메인 아래의 이름에 대한 와일드카드 DNS 쿼리 지원을 중지합니다. 이러한 쿼리는 이전 버전에서와 마찬가지로 OpenShift Container Platform 4.13에서 확인되지만 향후 OpenShift Container Platform 릴리스에서 지원은 제거됩니다.

1.5.1.3. RHOSP에서 실행되는 클러스터에 대한 Kuryr 지원

OpenShift Container Platform 4.12에서는 RHOSP에서 실행되는 클러스터에서 Kuryr에 대한 지원이 더 이상 사용되지 않습니다. OpenShift Container Platform 4.14 이전 버전에서는 지원이 제거됩니다.

1.5.1.4. ImageContentSourcePolicy 오브젝트

ImageContentSourcePolicy (ICSP) 오브젝트가 더 이상 사용되지 않습니다. 이제 다이제스트 사양 또는 **ImageTagMirrorSet** (ITMS) 오브젝트를 사용하여 이미지 태그를 사용하여 이미지를 가져오도록 **ImageDigestMirrorSet** (IDMS) 오브젝트를 사용할 수 있습니다.

이러한 새 오브젝트에 대한 자세한 내용은 이미지 레지스트리 저장소 미러링 구성을 참조하십시오.

기존 ICSP YAML 파일을 IDMS YAML 파일로 변환하는 방법에 대한 자세한 내용은 이미지 레지스트리 저장소 미러링을 위한 ICSP (ICSP) 파일 변환을 참조하십시오.

1.5.1.5. RHCOS에서 Toolbox가 더 이상 사용되지 않음

toolbox 스크립트는 더 이상 사용되지 않으며 향후 OpenShift Container Platform 릴리스에서 지원이 제거됩니다.

1.5.1.6. RHEL 9 드라이버 사용 중단

OpenShift Container Platform 4.13에서는 RHEL 9.2 기반 RHCOS가 도입되었습니다. 일부 커널 장치 드라이버는 RHEL 9에서 더 이상 사용되지 않습니다. 자세한 내용은 RHEL 설명서 를 참조하십시오.

1.5.1.7. VMware vSphere 구성 매개변수

OpenShift Container Platform 4.13에서는 다음 vSphere 구성 매개변수를 더 이상 사용하지 않습니다. 이러한 매개변수를 계속 사용할 수 있지만 설치 프로그램에서 **install-config.yaml** 파일에서 이러한 매개변수를 자동으로 지정하지는 않습니다.

- **platform.vsphere.vCenter**
- **platform.vsphere.username**
- **platform.vsphere.password**
- **platform.vsphere.datacenter**
- **platform.vsphere.defaultDatastore**
- **platform.vsphere.cluster**
- **platform.vsphere.folder**
- **platform.vsphere.resourcePool**
- **platform.vsphere.apiVIP**
- **platform.vsphere.ingressVIP**
- **platform.vsphere.network**

자세한 내용은 더 이상 사용되지 않는 VMware vSphere 구성 매개변수를참조하십시오.

1.5.1.8. Kubernetes 토폴로지 라벨

일반적으로 사용되는 Kubernetes 토폴로지 레이블 두 개가 교체됩니다. **failure-domain.beta.kubernetes.io/zone** 레이블이 **topology.kubernetes.io/zone** 로 교체됩니다. **failure-domain.beta.kubernetes.io/region** 레이블은 **topology.kubernetes.io/region** 로 교체됩니다. 대체 레이블은 Kubernetes 1.17 및 OpenShift Container Platform 버전 4.4부터 사용할 수 있습니다.

현재 더 이상 사용되지 않는 레이블과 대체 레이블이 모두 지원되지만 더 이상 사용되지 않는 라벨에 대한 지원은 향후 릴리스에서 제거될 예정입니다. 제거를 준비하기 위해 더 이상 사용되지 않는 라벨을 참조하는 리소스(예: 볼륨, 배포 또는 기타 워크로드)를 대신 사용하도록 수정할 수 있습니다.

1.5.2. 삭제된 기능

1.5.2.1. Kubernetes 1.26에서 베타 API 제거

Kubernetes 1.26에서는 다음 더 이상 사용되지 않는 API를 제거했으므로 적절한 API 버전을 사용하려면 매니페스트 및 API 클라이언트를 마이그레이션해야 합니다. 제거된 API 마이그레이션에 대한 자세한 내용은 Kubernetes 설명서 를 참조하십시오.

표 1.15. Kubernetes 1.26에서 제거된 API

리소스	제거된 API	마이그레이션 대상
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta1**	**flowcontrol.apiserver.k8s.io/v1beta3**
HorizontalPodAutoscaler	**autoscaling/v2beta2**	**autoscaling/v2**
PriorityLevelConfiguration	**flowcontrol.apiserver.k8s.io/v1beta1**	**flowcontrol.apiserver.k8s.io/v1beta3**

1.5.3. 향후 Kubernetes API 제거

OpenShift Container Platform의 다음 마이너 릴리스에서는 Kubernetes 1.27을 사용할 예정입니다. 현재 Kubernetes 1.27은 더 이상 사용되지 않는 API를 제거하도록 예약되어 있습니다.

계획된 Kubernetes API 제거 목록은 업스트림 Kubernetes 문서의 더 이상 사용되지 않는 API 마이그레이션 가이드를 참조하십시오.

제거를 위해 클러스터를 확인하는 방법에 대한 정보는 Kubernetes API 사용 중단 및제거 작업을 참조하십시오.

1.5.3.1. ppc64le, s390x, x86_64 v1 CPU 아키텍처의 특정 하드웨어 모델 제거

OpenShift Container Platform 4.13에서는 다음과 같은 더 이상 사용되지 않는 하드웨어 모델에 대해 RHCOS 기능에 대한 지원이 제거됩니다.

- IBM Power8 모든 모델 (**ppc64le**)
- IBM Power AC922 (**ppc64le**)
- IBM Power IC922 (**ppc64le**)
- IBM Power LC922 (**ppc64le**)
- IBM z13 모든 모델 (**s390x**)
- IBM® LinuxONE emperor(**s390x**)
- IBM® LinuxONE Rockhopper (**s390x**)
- AMD64 (**x86_64**) v1 CPU

1.6. 버그 수정

베어 메탈 하드웨어 프로비저닝

- 이전 버전에서는 iLO(Integrated Lights-Out) 관리 인터페이스 드라이버로 구성된 서버에 OpenShift Container Platform 클러스터 노드를 배포하려고 하면 노드의 프로비저닝이 실패했습

니다. ILO 드라이브의 **[ilo]/use_web_server_for_images** 구성 매개변수가 누락되어 드라이버에서 오브젝트 스토리지를 기본 스토리지 메커니즘으로 사용하려고 했기 때문에 오류가 발생했습니다. 제품에 오브젝트 스토리지가 없습니다. 이번 업데이트를 통해 OpenShift Container Platform 4.13 이상 버전에는 iLO 드라이버 구성에 **[ilo]/use_web_server_for_images** 가 포함되어 드라이버에서 **metal3** Pod에서 실행되는 웹 서버를 사용합니다. (OCPBUGS-5068)

클라우드 컴퓨팅

- 일부 Google Cloud Platform 클러스터 구성의 경우 내부 로드 밸런서는 설치 프로그램에서 생성한 인스턴스 그룹을 사용합니다. 이전에는 컨트롤 플레인 시스템이 수동으로 교체되면 새 컨트롤 플레인 노드가 컨트롤 플레인 인스턴스 그룹에 할당되지 않았습니다. 이로 인해 내부 로드 밸런서를 통해 노드에 연결할 수 없었습니다. 문제를 해결하기 위해 관리자는 Google Cloud 콘솔을 사용하여 컨트롤 플레인 시스템을 올바른 인스턴스 그룹으로 수동으로 이동해야 했습니다.
  이번 릴리스에서는 교체 컨트롤 플레인 노드가 올바른 인스턴스 그룹에 할당됩니다.
  (BZ#1970464, OCPCLOUD-1562)

- 이전에는 Google Cloud Platform의 컴퓨팅 머신 세트가 유효하지 않은 머신을 조정하려고 할 수 있었기 때문에 단계가 할당되지 않고 중단되었습니다. 이번 릴리스에서는 잘못된 구성이 있는 머신이 **Failed** 상태가 됩니다. (OCPBUGS-4574)

- 이전 버전에서는 연결된 노드에서 복제본이 준비된 것으로 간주되는 경우에도 백업 시스템이 **Running** 상태가 될 때 컨트롤 플레인 머신 세트 복제본이 준비되었다고 간주되었습니다. 이번 릴리스에서는 컨트롤 플레인 머신 세트 복제본이 준비된 것으로 간주되려면 노드와 해당 머신이 **Ready** 상태에 있어야 합니다. (OCPBUGS-8424)

- 이전에는 Microsoft Azure 클러스터에서 가속 네트워킹 기능에 대한 오류가 발생했을 때 **mapi_instance_create_failed** 경고 메트릭이 시작되지 않았습니다. 이번 릴리스에서는 Accelerated Networking이 활성화된 클러스터가 필요한 경우 경고를 생성할 수 있도록 누락된 경고가 추가되었습니다. (OCPBUGS-5235)

- 이전 버전에서는 머신이 **Running** 상태가 되면 노드 상태를 더 이상 확인하지 않았습니다. OCPBUGS-8424 의 이전 확인에는 노드와 해당 시스템이 컨트롤 플레인 시스템 세트 복제본이 준비된 것으로 간주되기 위한 **Ready** 상태가 되기 위한 요구 사항이 도입되었습니다. 결과적으로 노드와 시스템이 준비되었을 때 컨트롤 플레인 머신 세트가 단계를 누락하면 복제본이 준비되지 않았습니다. 이 동작으로 인해 컨트롤 플레인 머신 세트 Operator를 사용할 수 없어 업그레이드가 차단되었습니다. 이번 릴리스에서는 머신이 실행 중이지만 노드가 준비되지 않은 경우 노드가 준비될 때까지 정기적으로 노드를 확인합니다. 이번 수정을 통해 컨트롤 플레인 머신 세트 Operator를 사용할 수 없어 업그레이드가 차단됩니다. (OCPBUGS-10771)

- 이전 버전에서는 머신 상태 점검이 **maxUnhealthy** 임계값을 초과하여 경고를 생성할 때 클러스터가 머신 상태 점검을 성공적으로 조정할 수 있을 때 지표가 재설정되지 않았으며 경고가 계속되었습니다. 이번 릴리스에서는 경고를 트리거할 시기를 결정하는 논리가 개선되어 이제 클러스터가 정상일 때 경고가 지워집니다. (OCPBUGS-4725)

- OCPBUGS-5546 의 이전 확인으로 머신 구성 오브젝트에서**MachineConfig.Name** 의 **clusterName** 할당이 제거되었습니다. 그 결과 매개변수 값은 빈 문자열이었으며, IP 주소 이름을 생성하기 위해 **machineName** 값과 결합하면 잘못된 값이 생성되었습니다. 잘못된 값으로 인해 프로비저닝 중에 머신이 실패했습니다. 이번 릴리스에서는 유효한 IP 주소 이름을 생성하도록 **clusterName** 의 값이 인프라 오브젝트에서 가져옵니다. (OCPBUGS-7696)

- Kubernetes 1.26 릴리스에서는 노드가 라우팅 트래픽을 수신하지 못하도록 **NotReady** 상태가 있는 비정상 노드를 공용 로드 밸런서에서 제거하는 등 노드 인프라에 대한 변경 사항을 도입했습니다. 이러한 변경 사항은 Microsoft Azure의 클러스터 내부에서 실행된 노드에 영향을 미쳤습니다. 그 결과 노드가 **Ready** 상태를 복구하고 이후에 아웃바운드 연결을 설정할 수 없었습니다. 이번 업데이트를 통해 이제 공용 로드 밸런서에서 노드를 분리하지 않고도 **NotReady** 상태로 표시된 노드가 **kube-proxy** 상태 프로브에 의해 탐지됩니다. 즉, 노드는 이러한 단계 전반에서 아웃바운드 인터넷 연결을 유지할 수 있습니다. (OCPBUGS-7359)

Cloud Credential Operator

- Amazon Simple Storage Service(Amazon S3)는 Amazon S3 버킷 구성을 업데이트하여 AWS(Amazon Web Services) 리전에서 생성된 버킷에 S3 Block Public Access가 활성화되고 액세스 제어 제한(ACLs)이 기본적으로 비활성화되어 있습니다. 이 구성에서는 S3 버킷 리소스를 비공개 용도로 제한합니다. OpenShift Container Platform 4.13에서는 S3 버킷 리소스를 공개적으로 사용할 수 있도록 CCO 유틸리티(**ccoctl**) 및 기본 S3 버킷 구성을 고려하여 설치 프로그램을 업데이트합니다. (OCPBUGS-11706 및 OCPBUGS-11661)

개발자 콘솔

- 이전 버전에서는 OpenShift Container Platform에서 Knative Serving 및 Eventing에 API 버전 **v1alpha1** 을 사용했지만 버그로 인해 API 버전**v1beta1** 이 지원되지 않았습니다. 이번 수정으로 OpenShift Container Platform은 두 API 버전을 모두 지원합니다. (OCPBUGS-5164)

- 이전 버전에서는 OpenShift Container Platform 콘솔에서 파이프라인을 편집할 때 Pipeline builder 및 YAML 보기 구성 옵션에서 올바른 데이터가 렌더링되지 않았습니다. 이 문제로 인해 파이프라인 빌더 에서 파이프라인을 편집할 수 없었습니다. 이번 업데이트를 통해 데이터가 올바르게 구문 분석되고 빌더를 사용하여 파이프라인을 편집할 수 있습니다. (OCPBUGS-5016)

- 이전에는 토폴로지 사이드바에 업데이트된 정보가 표시되지 않았습니다. 토폴로지 사이드바에서 리소스를 직접 업데이트할 때 사이드바를 다시 열어서 변경 사항을 확인해야 했습니다. 이번 수정으로 업데이트된 리소스가 올바르게 표시됩니다. 결과적으로 토폴로지 사이드바에서 최신 변경 사항을 직접 확인할 수 있습니다. (OCPBUGS-4691)

- 이전에는 OpenShift Container Platform의 샘플 페이지에서 나열된 샘플 유형을 구분할 수 없었습니다. 이번 수정을 통해 샘플 페이지에 표시된 배지의 샘플을 확인할 수 있습니다. (OCPBUGS-10679)

문서
이전에는 OpenShift Container Platform 설명서에 "온-프레미스 베어 메탈 노드가 있는 클러스터 확장"이라는 하위 섹션이 포함되어 있었습니다. 그러나 이는 최신 문서를 정확하게 유지하기 위해 제거되었습니다.

etcd Cluster Operator

- 이전에는 컨트롤 플레인 머신 세트 Operator에서 클러스터 부트스트랩이 완료되기 전에 컨트롤 플레인 머신을 다시 생성하려고 했습니다. 이로 인해 etcd 클러스터 멤버십에서 부트스트랩 노드가 제거되어 etcd 쿼럼이 손실되고 클러스터가 오프라인 상태가 되었습니다. 이번 업데이트를 통해 컨트롤 플레인 Machine Set Operator는 etcd Cluster Operator가 부트스트랩 노드를 제거한 후에만 컨트롤 플레인 시스템을 다시 생성합니다. (OCPBUGS-10960)

호스트 컨트롤 플레인

- 이전에는 **HostedControlPlane** 오브젝트에서 **HostedCluster** 리소스에서 설정한 스케줄러 프로필의 변경 사항을 식별하지 않았습니다. 또한 **HostedControlPlane** 은 스케줄러에 변경 사항을 전파하지 않아 스케줄러에서 최신 스케줄러 프로필 변경 사항을 수신하기 위해 컨트롤 플레인 Pod를 재시작하지 않았습니다. 이번 업데이트를 통해 **HostedControlPlane** 은 이제 스케줄러 프로필 변경 사항을 인식한 다음 스케줄러를 동적으로 다시 시작하여 Pod에 프로필 변경 사항을 적용할 수 있습니다. (OCPBUGS-7091)

- 이전에는 호스팅된 클러스터에서 OIDC(OpenID Connect) 공급자인 **oidc** 를 고려하지 않아 **machine** 및 **machineset** 오브젝트가 오래된 것으로 삭제되었습니다. 이번 업데이트를 통해 호스트된 클러스터는 사용할 수 없는 **odic** 공급자의 상태를 감지할 수 있으므로 사용할 수 없는**oidc** 공급자로 인해 머신 및 머신 세트 오브젝트가 오래되지 않도록 할 수 있습니다. (OCPBUGS-10227)

- 이전에는 AWS(Amazon Web Services) 컴퓨팅 머신 세트의 **spec.metadata.annotations** 매개변수 값이 컴퓨팅 머신에서 해당 노드로 복사되지 않았습니다. 이로 인해 노드가 컴퓨팅 머신 세트에 지정된 주석이 누락되었습니다. 이번 릴리스에서는 노드에 주석이 올바르게 적용됩니다.

(OCPBUGS-4566)

설치 프로그램

- 이전에는 개인 클러스터를 제거할 때 설치 프로그램이 생성한 DNS 레코드가 제거되지 않았습니다. 이번 업데이트를 통해 이제 설치 프로그램에서 이러한 DNS 레코드를 올바르게 제거합니다. (OCPBUGS-7973)

- 이전에는 베어 메탈 설치 관리자 프로비저닝 인프라에서 BMC(Baseboard Management Controller) 및 배포 에이전트에 이미지를 제공하는 데 포트 80을 사용했습니다. 이 포트는 일반적으로 인터넷 통신용으로 선택되기 때문에 포트 80에서 보안 위험이 존재할 수 있습니다. 베어 메탈 설치 관리자 프로비저닝 인프라는 이제 배포된 클러스터에서 **metal3** Pod에서 사용하는 이미지를 제공하는 데 포트 6180을 사용합니다. (OCPBUGS-8511)

- 이전에는 bastion 호스트가 클러스터 노드와 동일한 VPC 네트워크에서 실행된 경우 부트스트랩 및 클러스터 노드에 대한 SSH 액세스가 실패했습니다. 또한 이 구성으로 인해 임시 부트스트랩 노드에서 클러스터 노드로의 SSH 액세스가 실패했습니다. 이러한 문제는 이제 임시 부트스트랩 노드와 클러스터 노드 간 SSH 트래픽을 지원하고 동일한 VPC 네트워크의 클러스터 노드로의 SSH 트래픽을 지원하도록 IBM Cloud 보안 그룹 규칙을 업데이트하여 해결되었습니다. 설치 관리자가 프로비저닝한 인프라 장애 시 분석을 위해 로그 및 디버그 정보를 정확하게 수집할 수 있습니다. (OCPBUGS-8035)

- 이전 버전에서는 **role** 매개변수가 **worker** 로 설정된 호스트의 IP 주소에 rendezvous IP를 구성하고 ISO 이미지를 생성한 경우 에이전트 기반 설치 프로그램이 클러스터를 설치하지 못했습니다. 이제 이 구성을 기반으로 ISO 이미지를 생성하려고 하면 검증 실패 메시지가 표시됩니다. 이 메시지를 받으면 **master** 역할이 있는 호스트의 IP를 사용하도록 **agent-config.yaml** 파일에서 **rendezvousIP** 필드를 업데이트해야 합니다. (OCPBUGS-2088)

- 이전에는 설치 프로그램에서 **aws-sdk-go** 라이브러리에 정의된 다음 새 리전을 허용하지 않았습니다. ap- **south-2,ap- southeast-4,eu-central-2,eu-south-2, me-central-1**. 설치 프로그램을 사용하여 설치 구성 파일을 만들 때 설치 프로그램은 이러한 새 리전을 나열하거나 이러한 지역에 대한 수동 항목을 허용하지 않습니다. 이번 업데이트를 통해 설치 프로그램은 이러한 리전을 지원하며 설치 구성 파일을 생성할 때 지정할 수 있습니다. (OCPBUGS-10213)

- 이전에는 **install-config.yaml** 파일의 **controlPlane.platform.openstack.failureDomain** 필드에 따라 **Machine.PrimaryNetwork** 를 설정하는 코드 베이스와 함께 문제가 발생했습니다. 이 문제는 컨트롤 플레인 시스템이 통신에 사용하는 RHOSP(Red Hat OpenStack Platform) 서브넷의 포트를 식별하는 데 Kuryr와 함께 실행되는 OpenShift Container Platform에 영향을 미칩니다. 이번 업데이트를 통해 **failureDomain** Technology Preview 구성 요소에서 **portTarget** 에 대한 **control-plane** 을 설정하면 설치 프로그램은 **Machine.PrimaryNetwork** 필드에 포트 정보를 설정하여 OpenShift Container Platform 클러스터가 Kuryr로 성공적으로 실행됩니다. (OCPBUGS-10658)

- 이전에는 **us-gov-west-1** 리전에 배포된 AWS 클러스터를 설치 제거하는 데 AWS 리소스가 지정되지 않은 경우 실패했습니다. 이로 인해 프로세스가 무한 루프로 전환되어 설치 프로그램이 리소스에 태그를 지정 해제하려고 했습니다. 이번 업데이트에서는 재시도를 수행하지 않습니다. 이로 인해 클러스터 설치 제거에 성공합니다. (BZ#2070744)

- 이전에는 GCP(Google Cloud Platform)에서 실행되는 프라이빗 OpenShift Container Platform 클러스터에 추가 방화벽 규칙이 수신되어 GCP가 내부 및 외부 로드 밸런서 모두에서 상태 검사를 수행할 수 있었습니다. 프라이빗 클러스터는 내부 로드 밸런서만 사용하므로 외부 로드 밸런서에 대한 상태 점검을 수행할 필요가 없습니다. 이번 업데이트를 통해 GCP에서 실행되는 프라이빗 클러스터는 외부 로드 밸런서의 상태 점검에서 제외된 이러한 추가 방화벽 규칙을 더 이상 수신하지 않습니다. (BZ#2110982)

Kubernetes 스케줄러

- 이전 버전에서는 **LifeCycleUtilization** 프로필이 테스트 네임스페이스 필터링으로 제외되면 Descheduler Operator 로그에 다음 오류가 기록되었습니다. **E0222 12:43:14.3318 1 target_config_reconciler.go:668]** 키가 실패했습니다. 결과적으로 Descheduler 클러스터 Pod가 시작되지 않았습니다. 이번 업데이트를 통해 이제 네임스페이스 제외가 **LifeCycleUtilization** 프로필에서 작동합니다. (OCPBUGS-7876)

관리 콘솔

- 이전에는 Create Pod 버튼을 렌더링할 때 사용자 권한이 확인되지 않았으며 권한이 없는 사용자에 대해 렌더링된 버튼이 있었습니다. 이번 업데이트를 통해 Create Pod 버튼을 렌더링할 때 사용자 권한이 확인되고 사용자에게 필요한 권한이 있는 사용자에게 렌더링됩니다. (BZ#2005232)

- 이전에는 **Pod** 리소스에 필요하지 않은 Pod 리소스 작업 메뉴에서**PDB** *추가*, *편집*, *삭제* 작업이 있었습니다. 이번 업데이트를 통해 작업이 제거됩니다. (BZ#2110565)

- 이전에는 세부 정보 페이지의 **PodDisruptionBudget** 필드에 잘못된 도움말 메시지가 표시되었습니다. 이번 업데이트를 통해 이제 도움말 메시지가 더 설명됩니다. (BZ#2084452)

- 이전 버전에서는 콘솔의 루트 경로로 이동할 때 메트릭이 비활성화되어 탐색 메뉴에 표시되지 않은 경우에도 URL이 Overview 페이지로 리디렉션되었습니다. 이번 업데이트를 통해 masthead 로고를 클릭하거나 콘솔의 루트 경로로 이동하면 메트릭이 비활성화된 경우 URL이 프로젝트 목록 페이지로 리디렉션됩니다. (OCPBUGS-3033)

- 이전에는 클러스터 드롭다운이 항상 표시되지 않아 보고 있는 클러스터를 명확하지 않았습니다. 이번 업데이트를 통해 이제 클러스터 드롭다운이 마스트 헤드에 있으므로 클러스터 드롭다운이 항상 표시되고 있는 클러스터를 확인할 수 있습니다. (OCPBUGS-7089)

- 이전 버전에서는 클러스터 버전이 **Failing**, UpdatingAndFailing ,**UpdatingAndFailing** 및 **Updating** 인 경우 노드 진행 표시줄이 표시되고 클러스터가 업데이트되지 않을 때 노드 진행률 표시줄이 표시되도록 설정되었습니다. 이번 업데이트를 통해 클러스터 버전이 **UpdatingAndFailing** 또는 **Updating** 인 경우에만 노드 진행률이 표시됩니다. (OCPBUGS-6049)

- 이전 버전에서는 ServiceAccount의 **kubeconfig** 파일을 다운로드할 때 오류가 표시되고 ServiceAccount 토큰에 연결할 수 없었습니다. 이 오류는 자동으로 생성된 보안이 제거되었기 때문입니다. 이번 업데이트를 통해 **kubeconfig** 다운로드 작업이 제거되어 더 이상 오류가 발생하지 않습니다. (OCPBUGS-7308)

- 이전에는 노드 세부 정보 페이지의 터미널 탭에 Pod 보안 조치로 인한 주석이 누락되어 오류가 표시되었습니다. 필수 주석이 없으면 노드 디버그 Pod를 시작할 수 없습니다. 이번 업데이트를 통해 OpenShift Container Platform에서 이러한 주석을 추가하므로 노드 디버그 Pod가 시작되고 터미널 탭이 오류 없이 로드됩니다. (OCPBUGS-4252)

- 이전 버전에서는 클러스터 관리자가 Operator를 제거할 때 **oc delete csv** 명령을 실행하려고 하면 Operator의 서브스크립션이 중단되었습니다. 서브스크립션과 충돌하여 관리자가 Operator를 다시 설치할 수 없었습니다. 이번 업데이트를 통해 관리자가 제거된 Operator를 다시 설치하려고 하면 자세한 오류 메시지가 표시됩니다. (OCPBUGS-3822)

- 이전 버전에서는 하나 이상의 기존 플러그인이 실패한 경우 웹 콘솔에 콘솔을 새로 고침하라는 toast 알림이 표시되지 않았습니다. Operator가 콘솔에 플러그인을 추가한 후 플러그인을 볼 수 있도록 이 작업이 필요합니다. 이번 업데이트를 통해 웹 콘솔은 Operator가 플러그인을 추가할 때 확인한 다음 이전에 실패한 플러그인에 관계없이 콘솔에 토스트 알림을 표시합니다. (OCPBUGS-10249)

- 이전 버전에서는 종료된 컨테이너가 **{{label}}** 및 **{{exitCode}}** 코드가 종료된 각 컨테이너에 대해 렌더링되었습니다. 이번 업데이트를 통해 읽을 수 있는 출력 메시지를 렌더링하도록 국제화 코드가 수정되었습니다. (OCPBUGS-4206)

- 이전에는 **clusterversion status.availableUpdates** 의 값이 **null** 및 **Upgradeable=False** 인 경우 클러스터 설정 페이지가 오류를 반환하도록 회귀가 도입되었습니다. 이번 업데이트를 통해 **status.availableUpdates** 가 **null** 값을 가질 수 있습니다. (OCPBUGS-6053)

모니터링

- 이전에는 Kubernetes 스케줄러에서 여러 재시작 작업을 수신한 노드의 특정 Pod 예약을 건너뛸 수 있었습니다. OpenShift Container Platform 4.13은 30분 이내에 예약할 수 없는 Pod에 대해 **KubePodNotScheduled** 경고를 포함하여 이 문제를 해결합니다. (OCPBUGS-2260)

- 이전 버전에서는 Thanos Ruler에 대해 두 개 이상의 레이블이 정의된 경우 **prometheus-operator** 에서 사용자 정의 리소스를 조정할 때마다 지정된 순서로 라벨을 추가하지 않았기 때문에 statefulset에서 레크리크레이션 루프에 들어갈 수 있었습니다. 이번 수정 후 **prometheus-operator** 는 이제 statefulset에 추가하기 전에 추가 라벨을 정렬합니다. (OCPBUGS-6055)

- 이번 릴리스에서는 특정 읽기 전용 **tmpfs** 인스턴스에 대해 **NodeFilesystemAlmostOutOfSpace** 가 더 이상 시작되지 않습니다. 이 변경으로 인해 설계에서 가득 찬 특정 **tmpfs** 마운트 지점에 경고가 실행되는 문제가 해결되었습니다. (OCPBUGS-6577)

네트워킹

- 이전에는 오류 메시지가 표시되어야 하는 경우 Ingress Operator에 **updateIngressClass** 함수 로그에 대한 성공 메시지가 표시되었습니다. 이번 업데이트를 통해 Ingress Operator의 로그 메시지가 정확합니다. (OCPBUGS-6700)

- 이전에는 Ingress Operator에서 **ingressClass.spec.parameters.scope** 를 지정하지 않았으며 Ingress 클래스 API 오브젝트는 기본적으로 유형 클러스터를 지정했습니다. 이로 인해 Operator가 시작될 때 모든 Ingress 클래스에 불필요한 업데이트가 발생했습니다. 이번 업데이트를 통해 Ingress Operator는 **cluster** 유형의 **ingressClass.spec.parameters.scope** 를 지정합니다. (OCPBUGS-6701)

- 이전에는 Ingress Operator에 **ensureNodePortService** 로그 메시지에 잘못된 서비스 이름이 있어 잘못된 정보가 기록되었습니다. 이번 업데이트를 통해 Ingress Operator는 **ensureNodePortService** 에 서비스를 정확하게 기록합니다. (OCPBUGS-6698)

- 이전 버전에서는 OpenShift Container Platform 4.7.0 및 4.6.20에서 Ingress Operator는 OpenShift Container Platform과 관련된 라우터 Pod에 주석을 사용했습니다. 버그 수정을 위해 활성 프로브의 유예 기간을 일시적으로 구성하는 방법입니다. 결과적으로 OpenShift Container Platform에서 수정 사항을 구현하기 위해 패치를 수행해야 했습니다. 이번 업데이트를 통해 Ingress Operator는 **terminationGracePeriodSeconds** API 필드를 사용하여 향후 릴리스에서 이전 패치를 분리합니다. (OCPBUGS-4703)

- 이전에는 CoreDNS가 기본 바이너리 및 이전 기본 이미지를 빌드하는 데 이전 툴체인을 사용하고 있었습니다. 이번 업데이트를 통해 OpenShift Container Platform은 빌드 툴체인 및 기본 이미지로 4.13을 사용하고 있습니다. (OCPBUGS-6228)

노드

- 이전에는 **LifecycleAndUtilization** descheduler 프로파일에 의해 활성화되는 **LowNodeUtilization** 전략에서 네임스페이스 제외를 지원하지 않았습니다. 이번 릴리스에서는 **LifecycleAndUtilization** Descheduler 프로파일이 설정된 경우 네임스페이스가 올바르게 제외됩니다. (OCPBUGS-513)

- 이전 버전에서는 동작의 회귀 문제로 인해 Machine Config Operator (MCO)가 **kubeletconfig** 또는 **containerruntimeconfig** CR(사용자 정의 리소스)에 중복 **MachineConfig** 오브젝트를 생성했습니다. 중복된 오브젝트가 성능 저하되고 클러스터를 업그레이드할 수 없습니다. 이번 업데이트를

통해 **kubeletconfig** 및 **containerruntimeconfig** 컨트롤러에서 중복 오브젝트를 탐지한 다음 삭제할 수 있습니다. 이 작업을 수행하면 성능이 저하된 **MachineConfig** 개체 오류가 제거되고 클러스터 업그레이드 작업에 영향을 미치지 않습니다. (OCPBUGS-7719)

Node Tuning Operator (NTO)

- 이전 버전에서는 CNF 지원 OpenShift Container Platform 클러스터에서 대기 시간 테스트를 실행하는 데 CNF(클라우드 네이티브 기능)에서 이미지에서 사용하는 **hwlatdetect** 툴이 감지 기간이 10초로 구성되었습니다. 이 구성을 감지 너비 구성의 0.95의 두 번째 설정으로 인해 **hwlatdetect** 의 대기 시간 급증이 누락될 가능성이 높아졌습니다. 이 도구는 할당된 감지 기간 동안 노드를 약 9.5% 정도 모니터링하므로 대기 시간 급증이 누락될 가능성이 높아졌습니다. 이번 업데이트를 통해 탐지 기간이 1초로 설정되어 이제 도구는 할당된 감지 기간 동안 노드의 약 95%를 모니터링할 수 있습니다. 나머지 5%의 모니터링 시간은 커널이 시스템 작업을 수행할 수 있도록 할당되지 않은 채 남아 있습니다. (OCPBUGS-12433)

OpenShift CLI(oc)

- 이전에는 **oc adm upgrade** 명령에서 ClusterVersion에서 **Failing=True** 상태를 읽지 않았습니다. 이번 업데이트를 통해 클러스터 상태를 요약할 때 **oc adm upgrade** 에 **Failing=True** 조건 정보가 포함됩니다. 이렇게 하면 **ClusterOperators** 의 **Degraded=True** 상태 및 현재 클러스터 또는 향후 업데이트의 동작에 영향을 줄 수 있는 기타 문제가 표시됩니다. (OCPBUGS-3714)

- 이전 버전에서는 **oc-mirror** 명령에서 OCI 및 FBC Operator용 카탈로그 콘텐츠를 미러링된 디스크 이미지에서 빌드했습니다. 결과적으로 카탈로그의 모든 콘텐츠가 미러링되지 않아 카탈로그에서 일부 콘텐츠가 누락되었습니다. 이번 업데이트를 통해 대상 레지스트리로 푸시하기 전에 미러링된 콘텐츠를 반영하도록 카탈로그 이미지가 빌드되어 카탈로그가 보다 완전한 카탈로그를 생성합니다. (OCPBUGS-5805)

- 이전에는 oc-mirror OpenShift CLI(**oc**) 플러그인에서 **ImageContentSourcePolicy** 리소스의 항목으로 Operator 카탈로그를 추가했습니다. Operator 카탈로그가 **CatalogSource** 리소스의 대상 레지스트리에서 직접 사용되므로 이 리소스는 이 항목이 필요하지 않습니다. 이 문제로 인해 **ImageContentSourcePolicy** 리소스의 예기치 않은 항목으로 인해 클러스터가 릴리스 이미지 서명 리소스를 수신하지 못했습니다. 이번 업데이트를 통해 oc-mirror 플러그인은 **ImageContentSourcePolicy** 리소스에서 Operator 카탈로그 항목을 제거하여 클러스터가 **CatalogSource** 리소스의 Operator 카탈로그에서 서명 리소스를 수신하도록 합니다. (OCPBUGS-10320)

OLM(Operator Lifecycle Manager)

- Operator의 CR(사용자 정의 리소스) 상태에는 Operator가 보유한 구성 요소 목록이 포함됩니다. 이 목록은 GVK(그룹/버전/종류)에 따라 정렬되지만 동일한 GVK가 있는 오브젝트의 순서가 변경될 수 있습니다. Operator가 동일한 GVK가 있는 여러 구성 요소를 보유하는 경우 구성 요소의 순서가 변경되었기 때문에 OLM(Operator Lifecycle Manager)이 Operator CR의 상태를 지속적으로 업데이트할 수 있습니다. 이 버그 수정에서는 Operator 구성 요소 참조가 결정적이 되도록 OLM을 업데이트합니다. 결과적으로 구성 요소 목록이 일정하게 유지되면 OLM에서 더 이상 CR을 반복적으로 업데이트하지 않습니다. (OCPBUGS-2556)

- OLM(Operator Lifecycle Manager)은 Operator를 검색하고 설치할 수 있는 **CatalogSource** 오브젝트 세트를 관리합니다. 이러한 카탈로그 소스는 이 작업의 기본 소스이며 Red Hat에서 관리합니다. 그러나 OLM 시스템에서 알 수 없는 방식으로 이러한 기본 카탈로그 소스를 변경할 수 있었습니다. 작동하지 않는 방식으로 기본 카탈로그 소스를 수정하면 사용자가 클러스터에 기존 Operator를 새로 설치하거나 업그레이드하지 못할 수 있는 OLM을 통해 계단식 문제가 발생할 수 있습니다. 이번 버그 수정을 통해 기본 카탈로그 소스를 관리하는 **catalog-operator** 런타임이 **CatalogSource** 사양에 대한 다른 변경 사항을 인식합니다. 결과적으로 기본 카탈로그 소스를 변경하면 OLM에서 변경 사항을 탐지하여 기본값으로 재설정합니다. (OCPBUGS-5466)

RHCOS(Red Hat Enterprise Linux CoreOS)

- 이전 버전에서는 Azure에서 SR-IOV 인터페이스가 부팅 중에 NetworkManager에 의해 구성되었습니다. **NM_UNMANAGED** 로 표시하는 udev 규칙이**initramfs** 파일에 없었습니다. 이번 업데이트를 통해 udev 규칙이 **initramfs** 파일에 있으며 SR-IOV 인터페이스는 항상 NetworkManager에 의해 관리되지 않아야 합니다. (OCPBUGS-7173)

Security Profiles Operator

- 이전 버전에서는 SPO(Security Profiles Operator) SELinux 정책에서 **net_container** 와 같은 다른 템플릿을 선택한 경우 컨테이너 템플릿에서 하위 수준 정책 정의를 상속하지 않았습니다. 이 정책은 컨테이너 템플릿에만 존재하는 하위 수준 정책 정의가 필요하기 때문에 작동하지 않습니다. 이 문제는 SPO SELinux 정책에서 SELinux 정책을 SPO 사용자 지정 형식에서 CIL(Common Intermediate Language) 형식으로 변환할 때 발생했습니다. 이번 업데이트를 통해 컨테이너 템플릿은 SPO에서 CIL으로 변환해야 하는 SELinux 정책에 추가됩니다. 또한 SPO SELinux 정책은 지원되는 모든 정책 템플릿에서 하위 수준 정책 정의를 상속할 수 있습니다. (OCPBUGS-12879)

확장 및 성능

- 이전 버전에서는 성능 프로필이 생성될 때 생성된 CRI-O 런타임 파일이 CRI-O 런타임으로 **runc** 를 사용하도록 자동 구성되었습니다.
  이제 성능 프로필이 생성될 때 **crun** 을 컨테이너 런타임으로 설정하면 일반적으로 생성된 런타임 CRI-O 파일이 **ContainerRuntimeConfig** CR에 구성된**defaultRuntime** 과 일치합니다.**crun** 또는 **runc** 중 하나일 수 있습니다. 기본값은**runc** 입니다. (OCPBUGS-11813)

스토리지

- 이전에는 **openshift-manila-csi-driver** 네임스페이스에 워크로드 파티셔닝 관리에 필요한 라벨이 포함되지 않았습니다. 이러한 누락된 라벨은 선택한 CPU 세트에서 실행되도록 Manila CSI Pod를 제한하는 작업에 영향을 미쳤습니다. 이번 업데이트를 통해 **openshift-manila-csi-driver** 네임스페이스에 이제 **workload.openshift.io/allowed** 라벨이 포함됩니다. (OCPBUGS-11341)

Windows 컨테이너

- 이전에는 Windows 노드 업그레이드 프로세스 중에 Microsoft Windows 컨테이너 워크로드가 완전히 중단되지 않았습니다. 이로 인해 워크로드가 업그레이드 중인 노드에 남아 있기 때문에 서비스가 중단되었습니다. 이번 업데이트를 통해 WMCO(Windows Machine Config Operator)는 워크로드를 드레이닝한 다음 노드 업그레이드가 완료될 때까지 노드를 차단합니다. 이 작업을 수행하면 Microsoft Windows 인스턴스를 원활하게 업그레이드할 수 있습니다. (OCPBUGS-5732)

- 이전에는 WMCO(Windows Machine Config Operator)에서 **DaemonSet** 워크로드를 드레이닝할 수 없었습니다. 이 문제로 인해 Windows **DaemonSet** Pod가 WMCO가 제거 또는 업그레이드하려고 시도한 Windows 노드를 차단했습니다. 이번 업데이트를 통해 WMCO에는 WMCO가 **DaemonSet** 워크로드를 제거할 수 있도록 추가 RBAC(역할 기반 액세스 제어) 권한이 포함되어 있습니다. WMCO는 **containerd** shim을 사용하여 생성된 모든 프로세스를 삭제할 수도 있으므로 WMCO가 클러스터에서 노드를 제거한 후 **DaemonSet** 컨테이너가 Windows 인스턴스에 존재하지 않습니다. (OCPBUGS-5354)

- 이전 버전에서는 리포지토리 태그가 빌드 시스템으로 전달되지 않았기 때문에 컨테이너 컨테이너 런타임에서 각 Windows 노드에서 잘못된 버전을 보고했습니다. 이로 인해 컨테이너에서 **Go** 빌드 버전을 각 **Windows** 노드의 버전으로 보고했습니다. 이번 업데이트를 통해 컨테이너 가 각 **Windows** 노드의 올바른 버전을 보고하도록 빌드 중에 올바른 버전이 바이너리에 삽입됩니다. (OCPBUGS-5378)

1.7. 기술 프리뷰 기능

이 릴리스의 일부 기능은 현재 기술 프리뷰 단계에 있습니다. 이러한 실험적 기능은 프로덕션용이 아닙

니다. 해당 기능은 **Red Hat Customer Portal**의 지원 범위를 참조하십시오.

기술 프리뷰 기능 지원 범위

다음 표에서 기능은 다음 상태로 표시됩니다.

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

네트워킹 기술 프리뷰 기능

표 1.16. 네트워킹 기술 프리뷰

기능	4.11	4.12	4.13
PTP 듀얼 NIC 하드웨어가 경계 클럭으로 구성	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
Ingress Node Firewall Operator	사용할 수 없음	기술 프리뷰	기술 프리뷰
특정 IP 주소 풀을 사용하여 BGP 모드를 사용하여 MetalLB 서비스를 노드 서브 세트에서 알림	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
특정 IP 주소 풀을 사용하여 노드 서브 세트에서 MetalLB 서비스를 L2 모드를 사용하여 알립니다.	기술 프리뷰	기술 프리뷰	기술 프리뷰
SR-IOV 네트워크에 대한 다중 네트워크 정책	사용할 수 없음	기술 프리뷰	기술 프리뷰
OVN-Kubernetes 네트워크 플러그인의 보조 네트워크	사용할 수 없음	사용할 수 없음	기술 프리뷰
인터페이스별 안전한 sysctl 목록 업데이트	사용할 수 없음	기술 프리뷰	기술 프리뷰

기능	4.11	4.12	4.13
MT2892 제품군 [ConnectX-6 Dx] SR-IOV 지원	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
MT2894 제품군 [ConnectX-6 Lx] SR-IOV 지원	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
MT42822 ConnectX-6 NIC 모드 SR-IOV 지원의 BlueField-2	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
Silicom STS Family SR-IOV 지원	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
MT2892 제품군 [ConnectX-6 Dx] OvS 하드웨어 오프로드 지원	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
MT2894 제품군 [ConnectX-6 Lx] OvS 하드웨어 오프로드 지원	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
MT42822 ConnectX-6 NIC 모드 OvS Hardware Offload 지원의 BlueField-2	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
Bluefield-2를 DPU에서 NIC로 전환	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
Intel E810-XXVDA4T	사용할 수 없음	사용할 수 없음	정식 출시일 (GA)

스토리지 기술 프리뷰 기능

표 1.17. 스토리지 기술 프리뷰

기능	4.11	4.12	4.13
OpenShift 빌드에서 공유 리소스 CSI 드라이버 및 빌드 CSI 볼륨 빌드	기술 프리뷰	기술 프리뷰	기술 프리뷰
CSI 볼륨 확장	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
CSI Azure File Driver Operator	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
CSI Google Filestore Driver Operator	사용할 수 없음	기술 프리뷰	기술 프리뷰

기능	4.11	4.12	4.13
CSI 자동 마이그레이션 (Azure file, VMware vSphere)	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
CSI 자동 마이그레이션 (Azure Disk, OpenStack Cinder)	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
CSI 자동 마이그레이션 (AWS EBS, GCP 디스크)	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
CSI 인라인 임시 볼륨	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
CSI 일반 임시 볼륨	사용할 수 없음	정식 출시일 (GA)	정식 출시일 (GA)
IBM Power Virtual Server Block CSI Driver Operator	사용할 수 없음	사용할 수 없음	기술 프리뷰
Local Storage Operator를 통한 자동 장치 검색 및 프로비저닝	기술 프리뷰	기술 프리뷰	기술 프리뷰
Azure File CSI Operator 드라이버에 대한 NFS 지원	사용할 수 없음	일반적으로 사용 가능	일반적으로 사용 가능

설치 기술 프리뷰 기능

표 1.18. 설치 기술 프리뷰

기능	4.11	4.12	4.13
kvc로 노드에 커널 모듈 추가	기술 프리뷰	기술 프리뷰	기술 프리뷰
IBM Cloud VPC 클러스터 (x86_64)	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
선택 가능한 Cluster Inventory	기술 프리뷰	기술 프리뷰	기술 프리뷰
다중 아키텍처 컴퓨팅 시스템	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
RHEL의 BuildConfig에 공유 인타이틀먼트 마운트	기술 프리뷰	기술 프리뷰	기술 프리뷰
에이전트 기반 OpenShift Container Platform 설치 프로그램	사용할 수 없음	정식 출시일 (GA)	정식 출시일 (GA)
AWS Outposts 플랫폼	사용할 수 없음	기술 프리뷰	기술 프리뷰

기능	4.11	4.12	4.13
SR-IOV 장치의 NIC 파티셔닝 활성화	사용할 수 없음	사용할 수 없음	기술 프리뷰
Azure Tagging	사용할 수 없음	사용할 수 없음	기술 프리뷰
GCP 기밀 VM	사용할 수 없음	사용할 수 없음	기술 프리뷰
설치 관리자 프로비저닝 인프라를 사용하여 Alibaba Cloud에 클러스터 설치	기술 프리뷰	기술 프리뷰	기술 프리뷰

노드 기술 프리뷰 기능

표 1.19. 노드 기술 프리뷰 추적기

기능	4.11	4.12	4.13
선점되지 않은 우선 순위 클래스	정식 출시일 (GA)	정식 출시일 (GA)	정식 출시일 (GA)
Linux Control Group 버전 2 (cgroup v2)	개발자 프리뷰	기술 프리뷰	정식 출시일 (GA)
crun 컨테이너 런타임	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)
Cron 작업 시간대	사용할 수 없음	기술 프리뷰	기술 프리뷰

Multi-Architecture 기술 프리뷰 기능

표 1.20. Multi-Architecture 기술 프리뷰 추적기

기능	4.11	4.12	4.13
arm64 아키텍처의 **kdump**	사용할 수 없음	기술 프리뷰	기술 프리뷰
s390x 아키텍처의 **kdump**	기술 프리뷰	기술 프리뷰	기술 프리뷰
ppc64le 아키텍처의 **kdump**	기술 프리뷰	기술 프리뷰	기술 프리뷰
IBM Secure Execution on IBM Z 및 IBM® LinuxONE	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)

기능	4.11	4.12	4.13
설치 관리자 프로비저닝 인프라를 사용하는 IBM Power Virtual Server	사용할 수 없음	사용할 수 없음	기술 프리뷰

전문 하드웨어 및 드라이버 지원 기술 프리뷰 기능

표 1.21. 전문 하드웨어 및 드라이버 지원 기술 프리뷰 추적기

기능	4.11	4.12	4.13
드라이버 툴킷	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
SRO(Special Resource Operator)	기술 프리뷰	기술 프리뷰	사용할 수 없음
Hub 및 spoke 클러스터 지원	사용할 수 없음	사용할 수 없음	기술 프리뷰

웹 콘솔 기술 프리뷰 기능

표 1.22. 웹 콘솔 기술 프리뷰 추적기

기능	4.11	4.12	4.13
동적 플러그인	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)

확장성 및 성능 기술 프리뷰 기능

표 1.23. 확장성 및 성능 기술 프리뷰 추적기

기능	4.11	4.12	4.13
하이퍼 스레딩 인식 CPU 관리자 정책	기술 프리뷰	기술 프리뷰	기술 프리뷰
Node Observability Operator	사용할 수 없음	기술 프리뷰	기술 프리뷰
construction-precaching-cli 툴	사용할 수 없음	사용할 수 없음	기술 프리뷰
작업자 노드를 사용한 단일 노드 OpenShift 클러스터 확장	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)

기능	4.11	4.12	4.13
토폴로지 Aware Lifecycle Manager (TALM)	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
마운트 네임스페이스 캡슐화	사용할 수 없음	사용할 수 없음	기술 프리뷰
NUMA 리소스 Operator를 사용한 NUMA 인식 스케줄링	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)
HTTP 전송은 PTP 및 베어 메탈 이벤트의 AMQP 대체	사용할 수 없음	사용할 수 없음	기술 프리뷰
Intel E810 웨스트 포트 채널 NIC를 PTP 다이브 마스터 시계	사용할 수 없음	사용할 수 없음	기술 프리뷰
3-노드 클러스터 및 표준 클러스터의 워크로드 파티셔닝	사용할 수 없음	사용할 수 없음	기술 프리뷰

Operator 기술 프리뷰 기능

표 1.24. Operator 기술 프리뷰 추적기

기능	4.11	4.12	4.13
Hybrid Helm Operator	기술 프리뷰	기술 프리뷰	기술 프리뷰
Java 기반 Operator	사용할 수 없음	기술 프리뷰	기술 프리뷰
Node Observability Operator	사용할 수 없음	사용할 수 없음	기술 프리뷰
Network Observability Operator	사용할 수 없음	정식 출시일 (GA)	정식 출시일 (GA)
플랫폼 Operator	사용할 수 없음	기술 프리뷰	기술 프리뷰
RukPak	사용할 수 없음	사용할 수 없음	기술 프리뷰
cert-manager Operator	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)

기술 프리뷰 기능 모니터링

표 1.25. 모니터링 기술 프리뷰 추적기

기능	4.11	4.12	4.13
사용자 정의 프로젝트 모니터링에 대한 경고 라우팅	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
플랫폼 모니터링 메트릭을 기반으로 하는 경고 규칙	사용할 수 없음	기술 프리뷰	기술 프리뷰
지표 컬렉션 프로필	사용할 수 없음	사용할 수 없음	기술 프리뷰

RHOSP(Red Hat OpenStack Platform) 기술 프리뷰 기능

표 1.26. RHOSP 기술 프리뷰

기능	4.11	4.12	4.13
RHOSP DCN 지원	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
RHOSP에서 클러스터용 외부 클라우드 공급자 지원	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)

아키텍처 기술 프리뷰 기능

표 1.27. 아키텍처 기술 프리뷰 추적기

기능	4.11	4.12	4.13
베어 메탈에서 OpenShift Container Platform의 호스트 컨트롤 플레인	사용할 수 없음	기술 프리뷰	기술 프리뷰
AWS(Amazon Web Services)에서 OpenShift Container Platform의 호스트 컨트롤 플레인	기술 프리뷰	기술 프리뷰	기술 프리뷰
OpenShift Virtualization에서 OpenShift Container Platform의 호스트 컨트롤 플레인	사용할 수 없음	사용할 수 없음	기술 프리뷰

머신 관리 기술 프리뷰 기능

표 1.28. 머신 관리 기술 프리뷰 추적기

기능	4.11	4.12	4.13
클러스터 API를 사용하여 머신 관리	기술 프리뷰	기술 프리뷰	기술 프리뷰
vGPU Cloud의 클라우드 컨트롤러 관리자	기술 프리뷰	기술 프리뷰	기술 프리뷰

기능	4.11	4.12	4.13
Amazon Web Services용 클라우드 컨트롤러 관리자	기술 프리뷰	기술 프리뷰	기술 프리뷰
Google Cloud Platform용 클라우드 컨트롤러 관리자	기술 프리뷰	기술 프리뷰	기술 프리뷰
IBM Cloud용 클라우드 컨트롤러 관리자	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
IBM Cloud Power VS용 클라우드 컨트롤러 관리자	사용할 수 없음	사용할 수 없음	기술 프리뷰
Microsoft Azure용 클라우드 컨트롤러 관리자	기술 프리뷰	기술 프리뷰	기술 프리뷰
Nutanix의 클라우드 컨트롤러 관리자	사용할 수 없음	사용할 수 없음	정식 출시일 (GA)
RHOSP(Red Hat OpenStack Platform)의 클라우드 컨트롤러 관리자	기술 프리뷰	정식 출시일 (GA)	정식 출시일 (GA)
VMware vSphere용 클라우드 컨트롤러 관리자	기술 프리뷰	기술 프리뷰	정식 출시일 (GA)

인증 및 권한 부여 기술 프리뷰 기능

표 1.29. 인증 및 권한 부여 기술 프리뷰

기능	4.11	4.12	4.13
Pod 보안 승인 제한 적용	사용할 수 없음	기술 프리뷰	기술 프리뷰

Machine Config Operator 기술 프리뷰 기능

표 1.30. Machine Config Operator 기술 프리뷰

기능	4.11	4.12	4.13
RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 계층화	사용할 수 없음	기술 프리뷰	정식 출시일 (GA)

1.8. 확인된 문제

- **OpenShift Container Platform 4.1에서는 익명 사용자가 검색 엔드 포인트에 액세스할 수 있었습니다. 이후 릴리스에서는 일부 검색 끝점이 통합된 API 서버로 전달되기 때문에 보안 악용에**

대한 가능성을 줄이기 위해 이 액세스를 취소했습니다. 그러나 인증되지 않은 액세스는 기존 사용 사례가 손상되지 않도록 업그레이드된 클러스터에 보존됩니다.

OpenShift Container Platform 4.1에서 **4.13**으로 업그레이드된 클러스터의 클러스터 관리자인 경우 인증되지 않은 액세스를 취소하거나 계속 허용할 수 있습니다. 인증되지 않은 액세스가 필요하지 않은 경우 해당 액세스를 취소해야 합니다. 인증되지 않은 액세스를 계속 허용하는 경우 이에 따라 보안 위험이 증가될 수 있다는 점에 유의하십시오.

주의

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

다음 스크립트를 사용하여 감지 끝점에 대한 인증되지 않은 액세스를 취소하십시오.

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

이 스크립트는 인증되지 않은 주제를 다음 클러스터 역할 바인딩에서 제거합니다.

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

- system:discovery
- system:openshift:discovery

(BZ#1821771)

- 명령이 주석 이름과 값 간의 구분 기호로 등호(=)를 포함하는 LDAP 그룹 이름에 대해 oc annotate 명령은 작동하지 않습니다. 이 문제를 해결하려면 oc patch 또는 oc edit를 사용하여 주석을 추가합니다. (BZ#1917280)

- Git 리포지토리를 추가하고 GitLab 및 Bitbucket pipeline-as-code 리포지토리로 구성하면 잘못된 리포지토리 리소스가 생성됩니다. 결과적으로 GitLab 및 Bitbucket 공급자에 대해 spec.git_provider.url Git 공급자 URL이 제거됩니다.

  해결방법: Bitbucket에 대한 필수 spec.git_provider.user 필드를 추가합니다. 또한 Git 액세스 토큰 또는 Git 액세스 토큰 시크릿 을 선택하여 Git 리포지토리를 계속 추가합니다. (OCPBUGS-7036)

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

- ControlPlaneMachineSet 정의에 세 개 이상의 실패 도메인을 포함하는 경우 로드 밸런싱 알고리즘은 기존 컨트롤 플레인 시스템에 우선 순위를 지정하지 않습니다. 기존 세 가지 실패 도메인보다 우선 순위가 알파벳순으로 높은 네 번째 실패 도메인을 추가하는 경우 네 번째 실패 도메인은 기존 실패 도메인보다 우선합니다. 이 동작은 롤링 업데이트를 컨트롤 플레인 시스템에 적용할 수 있습니다. 기존의 사용 중인 장애 도메인을 신규 및 사용되지 않는 장애 도메인보다 우선 순위가 높으면 이 문제를 방지할 수 있습니다. 이 작업은 정의에 세 개 이상의 실패 도메인을 추가하는 동안 각 컨트롤 플레인 시스템을 안정화합니다. (OCPBUGS-11968)

- 단일 노드 OpenShift 인스턴스에서 실행 중인 모든 포드를 제거하기 위해 노드를 드레이닝하지 않고 재부팅하면 워크로드 컨테이너 복구에 문제가 발생할 수 있습니다. 재부팅 후 모든 장치 플러그인이 준비되기 전에 워크로드가 다시 시작되어 리소스를 사용할 수 없거나 잘못된 NUMA 노드에서 실행되는 워크로드가 발생합니다. 해결방법은 재부팅 복구 절차 중에 모든 장치 플러그인이 자체적으로 다시 등록되면 워크로드 Pod를 다시 시작하는 것입니다. (OCPBUGS-2180)

- SR-IOV netdevice를 사용하는 Pod를 삭제할 때 오류가 발생할 수 있습니다. 이 오류는

RHEL 9의 변경으로 인해 이름이 변경될 때 네트워크 인터페이스의 이전 이름이 대체 이름 목록에 추가됩니다. 결과적으로 SR-IOV 가상 기능(VF)에 연결된 Pod가 삭제되면 VF는 원래 이름(예: ensf0v 2)이 아닌 새로운 예기치 않은 이름(예: dev69) 이 있는 풀로 돌아갑니다. 이 오류는 치명적이지 않지만 Multus 및 SR-IOV 로그에 시스템이 자체적으로 복구하는 동안 오류가 표시될 수 있습니다. 이 오류로 인해 Pod를 삭제하는 데 몇 초가 걸릴 수 있습니다. (OCPBUGS-11281)

- 인터페이스별 안전한 sysctl을 업데이트하는 데몬 세트의 YAML 정의에서 잘못된 우선순위 클래스 이름과 구문 오류로 인해 openshift-multus 네임스페이스에서 cni-sysctl-allowlist 구성 맵을 사용하여 인터페이스의 안전한 sysctl 목록을 수정하지 않습니다.

  해결방법: 데몬 세트를 수동으로 또는 사용하여 이 문제를 해결하기 위해 노드의 /etc/cni/tuning/allowlist.conf 파일을 수정합니다. (OCPBUGS-11046)

- UDP GRO를 활성화하는 OpenShift Container Platform 4.12에 도입된 새로운 기능으로 인해 모든 veth 장치에 사용 가능한 CPU당 하나의 RX 대기열이 있습니다(이전에는 각 veth에 대기열이 있습니다). 이러한 대기열은 Open Virtual Network에 의해 동적으로 구성되며 대기 시간 튜닝과 이 큐 생성 사이에 동기화가 없습니다. 대기 시간 튜닝 논리는 veth NIC 생성 이벤트를 모니터링하고 모든 대기열이 올바르게 생성되기 전에 RPS 대기열 CPU 마스크 구성을 시작합니다. 이는 일부 RPS 대기열 마스크가 구성되지 않았음을 의미합니다. 모든 NIC 큐가 올바르게 구성되지 않았기 때문에 타이밍에 민감한 CPU를 사용하는 실시간 애플리케이션에서 대기 시간이 급증하여 다른 컨테이너의 서비스와 통신할 수 있습니다. 커널 네트워킹 스택을 사용하지 않는 애플리케이션은 영향을 받지 않습니다. (OCPBUGS-4194)

- CNO(Cluster Network Operator) 컨트롤러에서는 필요한 것보다 더 많은 리소스를 모니터링합니다. 결과적으로 조정 프로그램이 너무 자주 트리거되어 필요한 것보다 훨씬 더 많은 API 요청이 발생합니다. 1초마다 약 1개의 구성 맵 액세스 요청이 수행됩니다. 이렇게 하면 CNO 및 kube-apiserver 모두에서 부하가 증가합니다. (OCPBUGS-11565)

- OpenShift Container Platform 4.13의 경우 Driver Toolkit (DTK) 컨테이너 이미지에는 드라이버 컨테이너를 빌드하기 위한 소프트웨어 스택의 두 번째 계층으로 ubi9 이미지가 필요합니다. 소프트웨어 스택의 두 번째 계층으로 ubi8 이미지를 사용하려는 경우 빌드 오류가 발생합니다. (OCPBUGS-11120)

- CSI 드라이버를 사용할 때 vSphere 플랫폼에 일부 OpenShift Container Platform 설치에서는 시작 중에 vCenter에서 노드에 대한 정보를 검색하지 못하여 CSI 드라이버가 재시도하지 않기 때문에 vSphere CSI 드라이버가 제대로 작동하지 않을 수 있습니다.

  해결방법: SSH를 사용하여 vsphere-syncer 프로세스의 현재 리더인 노드에 연결하고 vsphere-syncer 컨테이너를 다시 시작하여 (crictl 사용) 이 문제를 완화하고 드라이버가 성공적으로 발생할 수 있습니다. (OCPBUGS-13385)

- OpenShift Container Platform 4.13의 경우 baremetal 작업자와 함께 RHOSP(Red Hat

OpenStack Platform) 16.2 상단에 버전 4.13을 설치하는 데 baremetal 작업자가 OpenShift 4.13과 함께 제공되는 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지에서 부팅할 수 없기 때문에 실패합니다. 근본적인 문제는 RHCOS 이미지에 바이트 순서 표시가 없다는 것입니다. 이러한 수정 사항은 다음 16.2 빌드에 대해 계획되어 있습니다. (OCPBUGS-13395)

- RHEL 9.2에서 알려진 문제로 인해 기밀 VM이 있는 GCP 클러스터에서 영구 볼륨을 사용할 수 없습니다. (OCPBUGS-7582)

- OpenShift Container Platform 4.13으로 업그레이드할 때 openvswitch2.15 가 설치된 OpenShift Container Platform 4.12 클러스터에서 실행 중인 RHEL(Red Hat Enterprise Linux) 작업자는 실패합니다. upgrade.yml Playbook은 openvswitch2.17-2.17.0-88.el8fdp86_64와 openvswitch2.15-2.15.0-136.el8fdp.x86_64 오류 메시지와 함께 실패합니다.

  이 문제를 해결하려면 OpenShift Container Platform 4.13으로 업데이트하기 전에 openvswitch2.15 패키지를 수동으로 제거하고 openvswitch2.17 패키지를 설치합니다. 그런 다음 upgrade.yml 플레이북을 실행하여 RHEL 작업자를 업데이트하고 업데이트 프로세스를 완료합니다. (OCPBUGS-11677)

- 스토리지를 워크로드에 연결할 때 디스크 검색 지연이 있습니다. (OCPBUGS-11149)

- OpenShift Container Platform 4.12에서 4.13으로 업데이트하는 경우 Mellanox NIC는 ens7f0 과 같은 SR-IOV 네트워크 노드 정책의 이름을 ens7f0np0 로 변경합니다. 이 이름은 RHEL 9 커널 업데이트로 인해 발생합니다. 결과적으로 인터페이스를 찾을 수 없기 때문에 VF(가상 기능)를 생성할 수 없습니다. SR-IOV 네트워크 노드 정책에서 이 변경 사항을 고려해야 합니다. 예를 들어, policy에서 ens7f0 이 참조되는 경우 업데이트하기 전에 ens7f0np0 을 정책에 추가합니다.

  이 문제를 해결하려면 OpenShift Container Platform 4.13으로 업데이트하기 전에 SriovNetworkNodePolicy CR(사용자 정의 리소스)을 수동으로 편집하여 ens7f0np0 을 추가해야 합니다. (OCPBUGS-13186) 다음 코드는 호환성을 보장하기 위해 SriovNetworkNodePolicy 에 추가되는 두 이름과 정책 업데이트의 예를 제공합니다.

```
# ...
deviceType: netdevice
nicSelector:
  deviceID: "101d"
  pfNames:
    - ens7f0
    - ens7f0np0
  vendor: '15b3'
nodeSelector:
  feature.node.kubernetes.io/sriov-capable: 'true'
numVfs: 4
# ...
```

- Pod를 삭제할 때 SR-IOV VF(가상 기능)에서 MAC 주소를 재설정하지 않으면 Intel E810 NIC에는 실패할 수 있습니다. 따라서 SR-IOV VF를 사용하여 Pod를 생성하는 데 Intel E810 NIC 카드에서 최대 2분이 걸릴 수 있습니다. (OCPBUGS-5892)

- 클러스터 업그레이드를 수행하는 데 사용하는 서브스크립션 정책에 유효하지 않은 서브스크립션 채널을 지정하면 Subscription 리소스가 AtLatestKnown 상태로 유지되므로 TALM(Topology Aware Lifecycle Manager)에서 TALM이 정책을 적용한 직후 업그레이드가 성공했음을 나타냅니다. (OCPBUGS-9239)

- 시스템 충돌 후 kdump 는 Intel E810 NIC 및 Ice driver가 설치된 HPE Edgeline e920t 및 HPEECDHE DL110 Gen10 서버에서 vmcore 크래시 덤프 파일을 생성하지 못합니다. (RHELPLAN-138236)

- GitOps ZTP에서 SiteConfig CR을 사용하여 단일 노드를 포함하는 관리형 클러스터를 프로비저닝할 때 하나 이상의 노드에 siteConfig CR에 구성된 disk ECDHE 리소스가 있으면 디스크 파티션이 실패합니다. (OCPBUGS-9272)

- PTP 경계 클럭(T-BC) 및 배포된 DU 애플리케이션으로 구성된 클러스터에서는 최대 40초 동안 vDU 호스트의 후속 인터페이스에서 메시지가 간헐적으로 전송되지 않습니다. 로그의 오류 비율은 다를 수 있습니다. 오류 로그 예는 다음과 같습니다.

  출력 예

  ```
  2023-01-15T19:26:33.017221334+00:00 stdout F phc2sys[359186.957]: [ptp4l.0.config] nothing to synchronize
  ```

  (RHELPLAN-145492)

- GitOps ZTP를 사용하여 단일 노드 OpenShift 클러스터를 설치하고 HTTP 전송으로 PTP 및 베어 메탈 이벤트를 구성하면 linuxptp-daemon 데몬 Pod를 간헐적으로 배포하지 못합니다. 필수 PersistentVolumeClaim (PVC) 리소스는 생성되지만 Pod에 마운트되지 않습니다. 다음과 같은 볼륨 마운트 오류가 보고됩니다.

  출력 예

> **mount: /var/lib/kubelet/plugins/kubernetes.io/local-volume/mounts/local-pv-bc42d358: mount(2) system call failed: Structure needs cleaning.**

이 문제를 해결하려면 **cloud-event-proxy-store-storage-class-http-events PVC CR**을 삭제하고 **PTP Operator**를 다시 배포합니다. (OCPBUGS-12358)

- **site Config CR**에서 보안 부팅이 활성화된 단일 노드 **OpenShift** 관리 클러스터의**ZTP(ZTP)** 프로비저닝 중에 호스트 프로비저닝 중에 **BareMetalHost CR**에 대해 여러 **ProvisioningError** 오류가 보고됩니다. 이 오류는 **BMC(Baseboard Management Controller)**에 보안 부팅 설정이 성공적으로 적용되었지만 **BareMetalHost CR**을 적용한 후에는 호스트의 전원이 켜지지 않음을 나타냅니다. 이 문제를 해결하려면 다음 단계를 수행하십시오.

  1. 호스트를 재부팅합니다. 이렇게 하면 **GitOps ZTP** 파이프라인이 보안 부팅 설정을 적용할 수 있습니다.

  2. 동일한 구성으로 클러스터의 **GitOps ZTP** 프로비저닝을 다시 시작합니다.

  (OCPBUGS-8434)

- 듀얼 스택 **GitOps ZTP** 허브 클러스터를 설치한 후 이중 스택 가상 **IP** 주소(VIP)를 활성화하고 프로비저닝 **CR**에서 **virtualMediaViaExternalNetwork** 플래그를 활성화하면 **IRONIC_EXTERNAL_URL_V6** 환경 변수가 **IPv4** 주소를 잘못 할당합니다. (OCPBUGS-4248)

- **ZT** 서버에는 **bio sRegistry** 언어가 **en-US** 대신 **en -US**로 설정되어 있습니다. 이로 인해 관리 클러스터 호스트의 **GitOps ZTP** 프로비저닝 중에 문제가 발생합니다. **ZT** 서버에 대해 생성된 **FirmwareSchema CR**에는 **allowable_values,attribute_type** 및 **read_only** 필드가 채워지지 않습니다. (OCPBUGS-4388)

- **OpenShift Container Platform** 버전 **4.13.0**에서는 에이전트 기반 설치 프로그램을 사용하여 클러스터를 설치하려고 할 때 오류가 발생합니다. 읽기 디스크 단계를 수행하면 오류가 반환되고 클러스터 설치가 중단됩니다. 이 오류는 **HPE Cryostat Cryostat10** 서버에서 발견되었습니다. (OCPBUGS-13138)

-

RFC2544 성능 테스트에서는 패킷을 통과하는 패킷의 최대 지연 값이 최소 임계값을 초과함을 보여줍니다. 이 회귀 문제는 Telco RAN DU 프로필을 실행하는 OpenShift Container Platform 4.13 클러스터에서 찾을 수 있습니다. (OCPBUGS-13224)

- OpenShift Container Platform 4.13이 설치된 단일 노드 OpenShift 클러스터에서 성능 테스트는 최대 대기 시간이 20마이크로초를 초과한 결과를 보여줍니다. (RHELPLAN-155443)

- OpenShift Container Platform 4.13이 설치된 단일 노드 OpenShift 클러스터에서 성능 테스트는 cyclictest 최대 대기 시간 결과가 20마이크로초보다 큰 결과를 보여줍니다. (RHELPLAN-155460)

- DPDK의 CPU 로드 밸런싱 비활성화에 설명된 짧은 대기 시간 튜닝과 관련된 cpu-load-balancing.crio.io: "disable" 주석은 워크로드 파티셔닝이 구성되지 않은 시스템에서 작동하지 않습니다. 보다 구체적으로, 이는 인프라가 cpu 10.0.0.1ingMode 를 워크로드 파티셔닝 에 설명된 대로 AllNodes 값으로 설정하지 않는 클러스터에 영향을 미칩니다.

  이는 이러한 클러스터의 실현 가능한 대기 시간에 영향을 미치며 대기 시간이 짧은 워크로드가 올바르게 작동하지 않을 수 있습니다. (OCPBUGS-13163)

- Nutanix 플랫폼의 OpenShift Container Platform 4.12 클러스터에는 Nutanix Cloud Control Manager(CCM)에 필요한 구성이 누락된 경우 Upgradeable=False 조건이 있을 수 있습니다. 이 조건을 해결하려면 Nutanix를 플랫폼으로 사용할 때 OpenShift 4.13으로 업그레이드하는 데 필요한 ConfigMap 및 보안을 생성하는 방법을 참조하십시오.

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

- 컨트롤 플레인 노드에 예약된 Azure File NFS 볼륨을 사용하여 Pod를 생성하면 마운트가 거부됩니다. (OCPBUGS-18581)

  이 문제를 해결하려면 컨트롤 플레인 노드를 예약할 수 있고 작업자 노드에서 Pod를 실행할 수 있는 경우 nodeSelector 또는 Affinity를 사용하여 작업자 노드에서 Pod를 예약합니다.

- 노드 테인트를 제거하지 못하여 vSphere의 에이전트 기반 설치가 실패하여 설치가 보류 중 상태가 됩니다. 단일 노드 OpenShift 클러스터는 영향을 받지 않습니다. 다음 명령을 실행하여 노드 테인트를 수동으로 삭제하여 이 문제를 해결할 수 있습니다.

```
$ oc adm taint nodes <node_name>
node.cloudprovider.kubernetes.io/uninitialized:NoSchedule-
```

(OCPBUGS-20049)

1.9. 비동기 에라타 업데이트

OpenShift Container Platform 4.13의 보안, 버그 수정 및 개선 사항 업데이트는 Red Hat Network를 통해 비동기 에라타로 릴리스됩니다. 모든 OpenShift Container Platform 4.13 에라타는 Red Hat 고객 포털에서 사용할 수 있습니다. 비동기 에라타에 대한 자세한 내용은 OpenShift Container Platform 라이프 사이클에서 참조하십시오.

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

참고

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

이 섹션은 향후 OpenShift Container Platform 4.13과 관련된 비동기 에라타 릴리스의 개선 사항 및 버그 수정에 대한 정보 제공을 위해 지속적으로 업데이트됩니다. OpenShift Container Platform 4.13.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 클러스터 업데이트 관련 지침을 항상 확인하십시오.

1.9.1. RHSA-2023:1326 - OpenShift Container Platform 4.13.0 이미지 릴리스, 버그 수정 및 보안 업데이트 권고

출시 날짜: 2023-05-17

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.0을 사용할 수 있습니다. 업데이

트에 포함된 버그 수정 목록은 RHSA-2023:1326 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:1325 권고를 통해 제공됩니다. 업데이트에 포함된 보안 업데이트 목록은 RHSA-2023:2138 권고에 설명되어 있습니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.0 --pullspecs
```

1.9.2. RHSA-2023:3304 - OpenShift Container Platform 4.13.1 버그 수정 및 보안 업데이트

출시 날짜: 2023-05-30

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.1을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:3304 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:3303 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.1 --pullspecs
```

1.9.2.1. 버그 수정

- 이전에는 지원 설치에 일시적인 오류가 발생할 수 있었습니다. 이 오류가 발생한 경우 설치를 복구하지 못했습니다. 이번 업데이트를 통해 일시적인 오류가 올바르게 다시 시도됩니다. (OCPBUGS-13138)

- 이전 버전에서는 중첩된 경로가 예상 최대 path-components를 초과하면 일부 레지스트리에 대해oc-mirror OpenShift CLI(oc CLI) 플러그인이 일부 레지스트리에 대해 401 무단 오류로 실패했습니다. 이번 업데이트를 통해 --max-nested-paths 플래그의 기본 정수가 0(제한 없음)으로 설정됩니다. 결과적으로 생성된 ImageContentSourcePolicy 에는 기본적으로 사용되는 네임스페이스 수준과 달리 저장소 수준에 대한 소스 및 미러 참조가 포함됩니다. (OCPBUGS-13591)

1.9.2.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.3. RHSA-2023:3367 - OpenShift Container Platform 4.13.2 버그 수정 및 보안 업데이트

출시 날짜: 2023-06-07

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.2를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:3367 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:3366 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.2 --pullspecs
```

1.9.3.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.4. RHSA-2023:3537 - OpenShift Container Platform 4.13.3 버그 수정 및 보안 업데이트

출시 날짜: 2023-06-13

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.3을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:3537 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:3536 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

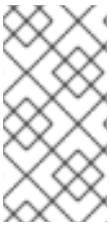
다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.3 --pullspecs
```

1.9.4.1. 기능

1.9.4.1.1. ZTP를 사용한 iPXE 네트워크 부팅 지원

ZTP(ZTP)는 Bare Metal Operator(BMO)를 사용하여 대상 호스트에서 RHCOS(Red Hat Enterprise Linux CoreOS)를 통신 클러스터 배포의 일부로 부팅합니다. 이번 업데이트를 통해 GitOps ZTP는 이러한 RHCOS 설치를 위해 사전 부팅 실행 환경(iPXE) 네트워크 부팅 옵션을 추가하여 BMO의 기능을 활용합니다.



참고

iPXE 네트워크 부팅을 사용하려면 RHACM(Red Hat Advanced Cluster Management) 2.8 이상을 사용해야 합니다.

자세한 내용은 site Config 및 GitOps ZTP를 사용하여 관리되는 클러스터 배포를 참조하십시오.

1.9.4.2. 버그 수정

- 이전에는 단일 노드 OpenShift에서 노드 재부팅의 경우 장치가 비정상이거나 할당할 수 없는 경우에도 노드에서 애플리케이션 Pod를 요청할 수 있는 경합 조건이 있었습니다. 이로 인해 애플리케이션이 장치에 액세스하려고 하면 런타임 오류가 발생했습니다. 이번 업데이트를 통해 장치 플러그인이 kubelet에 등록되어 있고 정상적인 장치가 할당될 노드에 있는 경우에만 Pod에서 요청하는 리소스가 할당됩니다.

  이러한 조건이 충족되지 않으면 예상되는 동작인 UnexpectedAdmissionError 오류로 인해 Pod가 허용될 수 있습니다. 애플리케이션 포드가 배포의 일부인 경우, 장애 발생 시 후속 Pod가 급증하고 궁극적으로 장치를 할당하는 데 적합한 경우 성공적으로 실행됩니다. (OCPBUGS-14438)

- 이전에는 클라이언트 TLS(mTLS)가 Ingress 컨트롤러에 구성되었으며 클라이언트 CA 번들의 인증 기관(CA)을 다운로드하려면 1MB 이상의 인증서 해지 목록(CRL)이 필요했습니다. CRL ConfigMap 오브젝트 크기 제한으로 인해 업데이트가 수행되지 않았습니다. CRL이 누락된 결과 유효한 클라이언트 인증서가 있는 연결이 알 수 없는 ca 오류와 함께 거부되었을 수 있습니다. 이번 업데이트를 통해 각 Ingress 컨트롤러의 CRL ConfigMap 이 더 이상 존재하지 않습니다. 대신 각 라우터 Pod가 CRL을 직접 다운로드하여 유효한 클라이언트 인증서와의 연결이 더 이상 거부되지 않습니다. (OCPBUGS-13967)

- 이전 버전에서는 클라이언트 TLS(mTLS)가 Ingress 컨트롤러에 구성되었기 때문에 배포 CA(인증 기관)와 발행 CA 간에 일치하지 않아 잘못된 CRL(인증서 취소 목록)이 다운로드되었습니다. 결과적으로 올바른 CRL 대신 잘못된 CRL을 다운로드하여 알 수 없는 오류 메시지와 함께

유효한 클라이언트 인증서 연결이 거부되었습니다. 이번 업데이트를 통해 다운로드한 CRL은 이제 이를 배포하는 CA에서 추적할 수 있습니다. 이렇게 하면 유효한 클라이언트 인증서가 더 이상 거부되지 않습니다. (OCPBUGS-13964)

1.9.4.3. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.5. RHSA-2023:3614 - OpenShift Container Platform 4.13.4 버그 수정 및 보안 업데이트

출시 날짜: 2023-06-23

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.4를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:3614 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:3612 권고를 통해 제공됩니다. 업데이트에 포함된 보안 업데이트 목록은 RHSA-2023:3342 권고에 설명되어 있습니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.4 --pullspecs
```

1.9.5.1. 버그 수정

- 이전에는 GCP(Google Cloud Platform)에서 기밀성 VM(가상 머신)이 있는 클러스터에서 영구 볼륨 스토리지를 사용할 수 없었습니다. 이 문제는 OpenShift Container Platform 4.13.3 및 이전 버전에서 유지됩니다. OpenShift Container Platform 4.13.4 이상 버전에서는 GCP에서 기밀 VM이 있는 클러스터에서 영구 볼륨 스토리지를 사용할 수 있습니다. (OCPBUGS-11768)

- 이전에는 AWS IAM ID 및 역할을 검증하기 위해 Vault에서 사용하는 값이 조작되고 인증을 우회할 수 있는 Vault 및 Vault Enterprise에 결함이 있었습니다. (BZ#2167337)

- 이전에는 GitOps ZTP에서 siteConfig CR을 사용하여 단일 노드를 포함하는 관리 클러스터를 프로비저닝하면 하나 이상의 노드에 site Config CR에 구성된 디스크 Cryostat 리소스가 있을 때 디스크 파티션이 실패했습니다. (OCPBUGS-13161)

- 이전 버전에서는 모든 클러스터가 이미 호환되는 경우CGU(ClusterGroupUpgrade) CR에 잘못된 백업 상태가 보고되었습니다. (OCPBUGS-13700)

- 이전 버전에서는 여러 클러스터를 확장하는 동안 클러스터 업그레이드 CGU CR이 BackupTimeout 오류로 업그레이드할 수 없었습니다. (OCPBUGS-7422)

1.9.5.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.6. RHSA-2023:4091 - OpenShift Container Platform 4.13.5 버그 수정 및 보안 업데이트

출시 날짜: 2023-07-20

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.5를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:4091 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:4093 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.5 --pullspecs
```

1.9.6.1. 버그 수정

- 이전에는 Gateway API 기능이 게이트웨이 도메인의 후행 점이 있는 DNS 레코드를 제공하지 않았습니다. 이로 인해 GCP 플랫폼에서 DNS 레코드의 상태를 사용할 수 없었습니다. 이번 업데이트를 통해 게이트웨이 API 게이트웨이의 DNS 레코드가 올바르게 프로비저닝되고 게이트웨이 API 기능이 GCP에서 작동하므로 게이트웨이 서비스 dns 컨트롤러에서 이제 도메인에 누락된 경우 후행 점을 추가하기 때문입니다. (OCPBUGS-15434)

- 이전 버전에서는 개발자 콘솔의 파이프라인 페이지를 사용하여 리포지토리를 추가하고 Git Repo URL 로서 GitLab 또는 Bitbucket Pipeline을 코드 리포지토리 URL로 입력한 경우 생성된 Repository 리소스가 유효하지 않습니다. 이는 이제 git_provider.url 사양에서 누락된 스키마 문제로 인해 발생했습니다. (OCPBUGS-15410)

- 이번 릴리스에서는 **Pipeline**에 대해 **Code Repository** 오브젝트로 **git_provider.user** 사양이 추가되었습니다. 이 사양을 사용하려면 **Git** 공급자가 **Bitbucket**인 경우 사용자 이름을 제공해야 합니다. (OCPBUGS-15410)

- 이번 릴리스에서는 **Pipelines** → **Create** → **Add Git Repository** 페이지의 **Secret** 필드가 필수입니다. 구성 옵션 표시를 클릭한 다음 리포지토리에 대한 **Git** 액세스 토큰 또는 **Git** 액세스 토큰 시크릿을 구성해야 합니다. (OCPBUGS-15410)

- 이전 버전에서는 **Helm** 콘솔의 **Helm** 차트 리포지터리를 편집하려고 하면 리포지토리 탭을 클릭한 다음 **Helm** 차트 리포지터리의 **kebab** 메뉴를 통해 **HelmChartRepository** 편집을 선택하면 **404: Page Not Found** 오류가 표시되는 오류 페이지가 표시되었습니다. 이는 최신 상태가 아닌 구성 요소 경로로 인해 발생했습니다. 이제 이 문제가 해결되었습니다. (OCPBUGS-15130)

1.9.6.2. 업데이트

기존 **OpenShift Container Platform 4.13** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.7. RHSA-2023:4226 - OpenShift Container Platform 4.13.6 버그 수정 및 보안 업데이트

출시 날짜: **2023-07-27**

보안 업데이트가 포함된 **OpenShift Container Platform** 릴리스 **4.13.6**을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:4226 권고에 설명되어 있습니다. 업데이트에 포함된 **RPM** 패키지는 RHBA-2023:4229 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.6 --pullspecs
```

1.9.7.1. 업데이트

기존 **OpenShift Container Platform 4.13** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.8. RHSA-2023:4456 - OpenShift Container Platform 4.13.8 버그 수정 및 보안 업데이트

출시 날짜: 2023-08-08

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.8을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:4456 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:4459 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.8 --pullspecs
```

1.9.8.1. 버그 수정

- 이전에는 RHOSP(Red Hat OpenStack Platform)의 실제 로드 밸런서 주소가 표시되지 않았습니다. 이번 업데이트를 통해 실제 로드 밸런서 주소가 추가되어 RHOSP 로드 밸런서 오브젝트 주석에 표시됩니다. (OCPBUGS-15973)

1.9.8.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.9. RHSA-2023:4603 - OpenShift Container Platform 4.13.9 버그 수정 및 보안 업데이트

출시 날짜: 2023-08-16

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.9를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:4603 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:4606 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.9 --pullspecs
```

1.9.9.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.10. RHSA-2023:4731 - OpenShift Container Platform 4.13.10 버그 수정 및 보안 업데이트

출시 날짜: 2023-08-30

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.10을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:4731 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:4734 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.10 --pullspecs
```

1.9.10.1. 버그 수정

- 이전에는 Mint 모드를 사용하는 클러스터에서 루트 시크릿을 제거했으며 4.13.8에서 4.13.9로 업그레이드하는 동안 문제가 발생했습니다. 이는 4.13.9로 백포트된 Ingress Operator의 인증 정보 요청의 수정으로 인해 발생했습니다. 이번 업데이트를 통해 이러한 클러스터는 4.13.9 이상으로 업데이트할 수 없습니다. (OCPBUGS-17733)

1.9.10.2. 알려진 문제

- UDP 일반 수신 오프로드(GRO)를 활성화하는 OpenShift Container Platform 4.12에 새 기능을 추가하면 모든 가상 이더넷 쌍(veth) 장치에 사용 가능한 CPU당 하나의 RX 큐가 있습니다. 이전에는 각 veth에 하나의 큐가 있었습니다. 이러한 대기열은 OVN(Open Virtual Network)에 의해 동적으로 구성되며 대기 시간 튜닝과 이 큐 생성 사이에 동기화되지 않습니다.

  대기 시간 튜닝 논리는 모든 대기열이 올바르게 생성되기 전에 veth NIC 생성 이벤트를 모니

터링하고RPS(Receive Packet Steering) 대기열 CPU 마스크 구성을 시작합니다. 이는 일부 RPS 대기열 마스크가 구성되지 않았음을 의미합니다. 모든 NIC 큐가 올바르게 구성되지 않았으므로 다른 컨테이너의 서비스와 통신하기 위해 타이밍 민감한 CPU를 사용하는 실시간 애플리케이션에서 대기 시간이 급증할 가능성이 있습니다. 커널 네트워킹 스택을 사용하지 않는 애플리케이션은 영향을 받지 않습니다. (OCPBUGS-17794)

1.9.10.3. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.11. RHBA-2023:4905 - OpenShift Container Platform 4.13.11 버그 수정

출시 날짜: 2023-09-05

OpenShift Container Platform 릴리스 4.13.11이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:4905 권고에 설명되어 있습니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.11 --pullspecs
```

1.9.11.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.12. RHBA-2023:5011 - OpenShift Container Platform 4.13.12 버그 수정

출시 날짜: 2023-09-12

OpenShift Container Platform 릴리스 4.13.12가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:5011 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:5014 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.12 --pullspecs
```

1.9.12.1. 기능

1.9.12.1.1. NUMA 인식 스케줄링의 SR-IOV 네트워크 토폴로지 제외

이번 릴리스에서는 SR-IOV 네트워크의 NUMA(Non-Uniform Memory Access) 노드를 토폴로지 관리자에게 알리는 것을 제외할 수 있습니다. SR-IOV 네트워크의 NUMA 노드를 알리지 않으면 NUMA 인식 Pod 예약 중에 더 유연한 SR-IOV 네트워크 배포를 허용할 수 있습니다.

예를 들어 일부 시나리오에서는 단일 NUMA 노드에서 Pod의 CPU 및 메모리 리소스를 최대화하는 것이 우선 순위입니다. 토폴로지 관리자는 Pod의 SR-IOV 네트워크 리소스에 대한 NUMA 노드에 대한 힌트를 제공하지 않기 때문에 토폴로지 관리자는 SR-IOV 네트워크 리소스 및 Pod CPU 및 메모리 리소스를 다른 NUMA 노드에 배포할 수 있습니다. 이전 OpenShift Container Platform 릴리스에서는 토폴로지 관리자가 동일한 NUMA 노드에만 모든 리소스를 배치하려고 했습니다.

NUMA 인식 Pod 예약 중에 보다 유연한 SR-IOV 네트워크 배포에 대한 자세한 내용은 NUMA 인식 스케줄링 의 SR-IOV 네트워크 토폴로지 제외 를 참조하십시오.

1.9.12.1.2. Google Cloud Provider 클러스터에 사용자 정의 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지 사용

기본적으로 설치 프로그램은 컨트롤 플레인 및 컴퓨팅 머신을 시작하는 데 사용되는 RHCOS(Red Hat Enterprise Linux CoreOS) 이미지를 다운로드하여 설치합니다. 이번 개선된 기능을 통해 설치 구성 파일(install-config.yaml)을 수정하여 사용자 정의 RHCOS 이미지를 지정하여 기본 동작을 덮어쓸 수 있습니다. 클러스터를 배포하기 전에 다음 설치 매개변수를 수정할 수 있습니다.

- controlPlane.platform.gcp.osImage.project
- controlPlane.platform.gcp.osImage.name
- compute.platform.gcp.osImage.project

- compute.platform.gcp.osImage.name
- platform.gcp.defaultMachinePlatform.osImage.project
- platform.gcp.defaultMachinePlatform.osImage.name

이러한 매개변수에 대한 자세한 내용은 추가 Google Cloud Platform 구성 매개변수를 참조하십시오.

1.9.12.1.3. Network API의 Service 오브젝트에서 allocateLoadBalancerNodePorts 지원

Service 오브젝트의 Network API의 ServiceSpec 구성 요소는 사용자가 서비스에 생성하는 특성을 설명합니다. ServiceSpec 구성 요소 내의 allocateLoadBalancerNodePorts 속성이 OpenShift Container Platform 4.13에서 지원됩니다. allocateLoadBalancer NodePorts 속성은 LoadBalancer 유형의 서비스에 NodePort가 자동으로 할당될지 여부를 정의합니다.

1.9.12.2. 버그 수정

- 이전에는 OpenShift Container Platform 라우터가 백엔드가 하나뿐인 경우 가중치가 0인 경로로 트래픽을 리디렉션했습니다. 이번 업데이트를 통해 라우터는 가중치가 0인 단일 백엔드가 있는 경로로 트래픽을 보내지 않습니다. (OCPBUGS-17107)

1.9.12.3. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.13. RHSA-2023:5155 - OpenShift Container Platform 4.13.13 버그 수정 및 보안 업데이트

출시 날짜: 2023-09-20

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.13을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:5155 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:5158 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.13 --pullspecs
```

1.9.13.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.14. RHBA-2023:5382 - OpenShift Container Platform 4.13.14 버그 수정

출시 날짜: 2023-10-05

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.14를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2023:5382 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:5388 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.14 --pullspecs
```

1.9.14.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.15. RHBA-2023:5467 - OpenShift Container Platform 4.13.15 버그 수정

출시 날짜: 2023-10-10

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.15를 사용할 수 있습니다. 업데

이트에 포함된 버그 수정 목록은 RHBA-2023:5467 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:5470 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.15 --pullspecs
```

1.9.15.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.16. RHSA-2023:5672 - OpenShift Container Platform 4.13.17 버그 수정 및 보안 업데이트

출시 날짜: 2023-10-17

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.17을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:5672 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:5675 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.17 --pullspecs
```

1.9.16.1. 버그 수정

- 이전에는 사용자가 포트 번호 없이 EndpointSlice 포트를 생성한 경우 CoreDNS가 예기치 않게 종료되었습니다. 이번 업데이트를 통해 CoreDNS에 검증이 추가되어 예기치 않은 종료가 발생하지 않습니다. (OCPBUGS-19985)

1.9.16.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.17. RHSA-2023:5902 - OpenShift Container Platform 4.13.18 버그 수정 및 보안 업데이트

출시 날짜: 2023-10-24

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.18을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:5902 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:5905 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.18 --pullspecs
```

1.9.17.1. 버그 수정

- etcdctl 바이너리는 로컬 시스템에 무기한 캐시되어 업데이트를 수행할 수 없었습니다. 이제 cluster-backup.sh 스크립트의 모든 호출에서 바이너리를 가져옵니다. (OCPBUGS-20488)

1.9.17.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.18. RHSA-2023:6130 - OpenShift Container Platform 4.13.19 버그 수정 및 보안 업데이트

출시 날짜: 2023-10-31

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.19를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:6130 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:6133 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.19 --pullspecs
```

1.9.18.1. 기능

1.9.18.1.1. 이제 Insights Operator에서 apiserver.config.openshift.io를 추적합니다.

Insights Operator를 실행한 후 이제 APIServer.config.openshift.io 의 감사 프로필에 대한 정보와 함께 경로 config/apiserver.json 의 아카이브에 새 파일을 사용할 수 있습니다.

감사 프로필에 대한 액세스는 일반적인 감사 정책, 가장 일반적으로 사용되는 프로필, 산업 간 차이점이 무엇이고, 어떤 종류의 사용자 지정이 적용되는지 이해하는 데 도움이 됩니다.

1.9.18.2. 버그 수정

- 이전에는 CVO(Cluster Version Operator)에서 SCC(SecurityContextConstraints) 리소스를 예상대로 조정하지 않았습니다. CVO는 SCC 리소스의 Volumes 필드를 릴리스 이미지에 정의된 상태로 적절하게 조정합니다. 시스템 SCC 리소스에 대한 사용자 수정이 허용됩니다.

  향후 OpenShift Container Platform 버전은 시스템 SCC 리소스의 사용자 수정을 허용하지 않으므로 이제 사용자 수정 SCC를 감지할 때 CVO는 마이너 버전 업데이트 게이트를 적용합니다. 사용자는 향후 마이너 OpenShift Container Platform 버전으로 업데이트하기 전에 수정되지 않은 시스템 SCC 리소스를 준수하는 워크로드를 수행해야 합니다. 자세한 내용은 4.14로 업그레이드하기 전에 "Detected modified SecurityContextConstraints" 업데이트 게이트 를 참조하십시오. (OCPBUGS-19472)

1.9.18.3. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.19. RHSA-2023:6257 - OpenShift Container Platform 4.13.21 버그 수정 및 보안 업데이트

출시 날짜: 2023-11-8

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.21을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:6257 권고에 설명되어 있습니다. 이 릴리스에는 RPM 패키지가 없습니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.21 --pullspecs
```

1.9.19.1. 버그 수정

- 이전에는 Azure 프라이빗 클러스터의 송신 노드에 송신 IP를 적용할 수 없었습니다. 이 패치는 아웃 바운드 규칙을 사용하여 아웃 바운드 연결을 수행하는 Azure 설정에 송신 IP를 활성화합니다. Azure의 아키텍처 제약 조건은 송신 IP 역할을 하는 보조 IP가 이러한 설정에서 아웃바운드 연결을 수행하지 못하도록 합니다. 이번 릴리스에서는 일치하는 Pod에 인터넷에 대한 아웃바운드 연결이 없지만 인프라 네트워크의 외부 서버에 연결할 수 있습니다. (OCPBUGS-22299)

1.9.19.2. 알려진 문제

- ClusterGroupUpdate CR이 시작될 때 선택한 모든 클러스터가 호환되는 경우 TALM은 정책 수정을 건너뜁니다. 동일한 ClusterGroupUpdate CR의 수정된 카탈로그 소스 정책 및 서브스크립션 정책이 있는 Operator 업데이트가 완료되지 않습니다. 카탈로그 소스 변경 사항이 적용될 때까지 계속 준수되므로 서브스크립션 정책을 건너뜁니다.

  이 문제를 해결하려면 common-subscription 정책의 하나의 CR에 간단한 변경 사항을 추가합니다(예: metadata.annotations.upgrade: "1"). 이렇게 하면 ClusterGroupUpdate CR을 시작하기 전에 정책을 준수하지 않습니다. (OCPBUGS-2812)

1.9.19.3. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.20. RHSA-2023:6846 - OpenShift Container Platform 4.13.22 버그 수정 및 보안 업데이트

출시 날짜: 2023-11-15

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.22를 사용할 수 있습니다. 업데

이트에 포함된 버그 수정 목록은 RHSA-2023:6846 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:6848 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.22 --pullspecs
```

1.9.20.1. 버그 수정

- 이전에는 copy 명령에 -p 플래그 옵션이 누락되었습니다. 이제 명령은 타임스탬프를 보존하도록 -p 플래그를 지원합니다. (OCPBUGS-23021)

- 이전에는 Burstable 컨테이너가 성능 프로필로 구성된 노드의 예약된 CPU에서만 실행될 수 있었습니다. 이로 인해 RHEL(Red Hat Enterprise Linux) 9가 CPU 선호도 및 cpuset 구성 요소의 동작을 변경하여 cpuset 이 변경되면 CPU 선호도가 재설정되지 않았습니다. 이제 새로 실행 중인 컨테이너의 cpuset 구성 요소와 상호 작용하는 모든 구성 요소에 CPU 선호도가 재설정됩니다. 즉, Burstable 컨테이너는 현재 Guaranteed 컨테이너에 할당되지 않은 모든 CPU에 액세스할 수 있습니다. (OCPBUGS-20365)

1.9.20.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.21. RHSA-2023:7323 - OpenShift Container Platform 4.13.23 버그 수정 및 보안 업데이트

출시 날짜: 2023-11-21

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.23을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:7323 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:7325 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.23 --pullspecs
```

1.9.21.1. 기능

1.9.21.1.1. 웹 브라우저를 사용하여 CLI에 로그인

이번 릴리스에서는 **oc login** 명령에 새로운 **oc CLI**(명령줄 인터페이스) 플래그인 **--web** 을 사용할 수 있습니다.

이번 개선된 기능을 통해 웹 브라우저를 사용하여 로그인할 수 있으므로 명령줄에 액세스 토큰을 삽입하지 못할 수 있습니다.

자세한 내용은 웹 브라우저를 사용하여 OpenShift CLI에 로깅을 참조하십시오.

1.9.21.2. 버그 수정

- 이전에는 일부 **Redfish** 가상 미디어 장치가 하드웨어를 프로비저닝하는 데 사용할 수 없기 때문에 **Ironic**에서 **Cisco UCS** 하드웨어를 새 **baremetalhost**로 프로비저닝할 수 없었습니다. 이번 릴리스에서는 **Ironic**에서 하드웨어를 프로비저닝할 수 있는 모든 장치를 확인하여 **Redfish Virtual Media**를 사용하여 **Cisco UCS Hardware**를 프로비저닝할 수 있습니다. (OCPBUGS-19078)

- 이전에는 **IP**가 할당되고 할당되지 않은 **LB** 서비스가 있는 동안 **metallb**의 컨트롤러가 다시 시작되었습니다. 이로 인해 **metallb**의 컨트롤러에서 이미 할당된 **IP**를 다른 **LB** 서비스로 이동하여 워크로드가 손상되었습니다. 이번 릴리스에서는 **metallb**의 컨트롤러가 이미 **IP**가 할당된 서비스를 처리합니다. (OCPBUGS-23160)

1.9.21.3. 업데이트

기존 **OpenShift Container Platform 4.13** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.22. RHSA-2023:7475 - OpenShift Container Platform 4.13.24 버그 수정 및 보안 업데이트

출시 날짜: **2023-11-29**

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.24를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:7475 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:7477 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.24 --pullspecs
```

1.9.22.1. 버그 수정

- 이전에는 CSI 스토리지가 있는 노드에서 클러스터 자동 스케일러를 사용하면 CrashBackoff 루프가 발생할 수 있었습니다. 이번 릴리스에서는 오류 처리를 개선하기 위해 종속 항목이 업데이트되어 CrashBackoff 루프가 발생하지 않습니다. (OCPBUGS-23272)

1.9.22.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.23. RHSA-2023:7604 - OpenShift Container Platform 4.13.25 버그 수정 및 보안 업데이트

출시 날짜: 2023-12-06

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.25를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:7604 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2023:7606 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.25 --pullspecs
```

1.9.23.1. 버그 수정

- 이전에는 Image Registry Operator에서 액세스 키를 5분마다 가져오는 과정의 일부로 스토리지 계정 목록 끝점에 대한 API 호출을 수행했습니다. 많은 OpenShift Container Platform 클러스터가 있는 프로젝트에서 이로 인해 새 클러스터를 생성하려고 할 때 API 제한으로 인해 429 오류가 발생할 수 있습니다. 이번 릴리스에서는 호출 간 시간이 5분에서 20분으로 증가합니다. (OCPBUGS-22126)

1.9.23.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.24. RHSA-2023:7687 - OpenShift Container Platform 4.13.26 버그 수정 및 보안 업데이트

출시 날짜: 2023-12-13

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.26을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2023:7687 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:7689 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.26 --pullspecs
```

1.9.24.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.25. RHSA-2023:7827 - OpenShift Container Platform 4.13.27 버그 수정 및 보안 업데이트

출시 날짜: 2024-01-04

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.27을 사용할 수 있습니다. 업데

이트에 포함된 버그 수정 목록은 RHSA-2023:7827 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2023:7829 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.27 --pullspecs
```

1.9.25.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.26. RHBA-2024:0055 - OpenShift Container Platform 4.13.28 버그 수정 및 보안 업데이트

출시 날짜: 2024-01-10

OpenShift Container Platform 릴리스 4.13.28이 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2024:0055 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:0057 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.28 --pullspecs
```

1.9.26.1. 버그 수정

- 이전에는 다른 DNS 접미사로 인해 ccoctl 이 중국에서 AWS STS(보안 토큰 서비스) 리소스를 생성하지 못했습니다. 이번 릴리스에서는 ccoctl 을 사용하여 중국 리전에서 STS 리소스를 생성할 수 있으며 클러스터를 성공적으로 설치할 수 있습니다. (OCPBUGS-25369)

1.9.26.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.27. RHSA-2024:0193 - OpenShift Container Platform 4.13.29 버그 수정 및 보안 업데이트

출시 날짜: 2024-01-17

OpenShift Container Platform 릴리스 4.13.29가 공개되었습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:0193 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:0195 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.29 --pullspecs
```

1.9.27.1. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.28. RHBA-2024:0286 - OpenShift Container Platform 4.13.30 버그 수정 및 보안 업데이트

출시 날짜: 2024-01-24

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.30을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHBA-2024:0286 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHSA-2024:0288 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.30 --pullspecs
```

1.9.28.1. 버그 수정

- 이전 버전에서는 미러링 릴리스에 **EUS** 채널을 사용하면 **oc-mirror** 명령을 사용하여 미러링에 실패했습니다. 이 문제는 **oc-mirror** 에서 **EUS** 채널이 짝수 릴리스에만 해당한다는 것을 인식하지 못했기 때문에 발생했습니다. 이번 릴리스에서는 **oc-mirror** 명령 사용자가 **EUS** 채널을 사용하여 릴리스 미러링을 수행할 수 있습니다. (OCPBUGS-26595)

1.9.28.2. 업데이트

기존 **OpenShift Container Platform 4.13** 클러스터를 최신 릴리스로 업데이트하려면 **CLI**를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.29. RHSA-2024:0484 - OpenShift Container Platform 4.13.31 버그 수정 및 보안 업데이트

출시 날짜: 2024-02-01

보안 업데이트가 포함된 **OpenShift Container Platform** 릴리스 **4.13.31**을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:0484 권고에 설명되어 있습니다. 업데이트에 포함된 **RPM** 패키지는 RHBA-2024:0488 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.31 --pullspecs
```

1.9.29.1. 버그 수정

- 이전에는 **Whereabouts CNI** 플러그인으로 생성된 풀의 **IP**가 노드 강제 재부팅 후 **ContainerCreating** 상태로 중단되었습니다. 이번 릴리스에서는 노드 강제 재부팅이 해결된 후 **IP** 할당과 관련된 **Whereabouts CNI** 플러그인 문제가 해결되었습니다. (OCPBUGS-27367)

- 이전에는 기본적으로 **container_t SELinux** 컨텍스트가 **DRI** 장치에 대한 액세스를 제공하는 **dri_device_t** 오브젝트에 액세스할 수 없었습니다. 이제 새 컨테이너 정책 **container-selinux**를 사용하면 **pod**에서 장치 플러그인을 사용하여 **dri_device_t** 오브젝트에 액세스할 수 있습니다. (OCPBUGS-27416)

1.9.29.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.30. RHSA-2024:0660 - OpenShift Container Platform 4.13.32 버그 수정 및 보안 업데이트

출시 날짜: 2024-02-07

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.32를 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:0660 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:0662 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.32 --pullspecs
```

1.9.30.1. 기능

다음 기능은 이 z-stream 릴리스에 포함되어 있습니다.

1.9.30.1.1. Whereabouts cron 일정 구성 활성화

- Whereabouts 조정 일정은 하루에 한 번 실행되도록 하드 코딩되었으며 재구성할 수 없습니다. 이번 릴리스에서는 ConfigMap 리소스에서 whereabouts cron 스케줄의 구성을 활성화했습니다. 자세한 내용은 Whereabouts IP reconciler 일정 구성을 참조하십시오.

1.9.30.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.

1.9.31. RHSA-2024:0741 - OpenShift Container Platform 4.13.33 버그 수정 및 보안 업데이트

출시 날짜: 2024-02-14

보안 업데이트가 포함된 OpenShift Container Platform 릴리스 4.13.33을 사용할 수 있습니다. 업데이트에 포함된 버그 수정 목록은 RHSA-2024:0741 권고에 설명되어 있습니다. 업데이트에 포함된 RPM 패키지는 RHBA-2024:0743 권고를 통해 제공됩니다.

권고에 이 릴리스의 모든 컨테이너 이미지에 대한 설명은 제외되어 있습니다.

다음 명령을 실행하여 이 릴리스의 컨테이너 이미지를 볼 수 있습니다.

```
$ oc adm release info 4.13.33 --pullspecs
```

1.9.31.1. 버그 수정

- 이전 버전에서는 OpenShift Container Platform을 업그레이드하면 업스트림에서 CoreDNS 1.10.1을 사용하여 EDNS 이외의 쿼리의 페이로드보다 큰 페이로드가 반환되어 DNS 쿼리가 실패할 수 있었습니다. 이번 릴리스에서는 비호환 업스트림이 있는 클러스터에서 오버플로 오류 시 TCP로 재시도하여 업그레이드 시 기능이 중단되는 것을 방지할 수 있습니다. (OCPBUGS-28205)

- 이전에는 Amazon EBS(Elastic File System) CSI(Container Storage Interface) 드라이버 컨테이너에 적용된 CPU 제한으로 인해 I/O 작업의 성능 저하 문제가 EFS 볼륨에 발생했습니다. 이제 EFS CSI 드라이버의 CPU 제한이 제거되어 성능 저하 문제가 더 이상 존재하지 않습니다. (OCPBUGS-28979)

1.9.31.2. 업데이트

기존 OpenShift Container Platform 4.13 클러스터를 최신 릴리스로 업데이트하려면 CLI를 사용하여 클러스터 업데이트를 참조하십시오.