OpenShift sandboxed containers 1.6

릴리스 노트

Last Updated: 2024-09-18

법적 공지

초록

릴리스 노트에는 새로운 기능 및 개선 사항, 주요 기술 변경 사항, 이전 버전의 주요 수정 사항 및 일반 가용성에 따라 알려진 버그가 요약되어 있습니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

RED HAT 문서에 관한 피드백 제공

피드백을 제공하거나 HCIDOCS 프로젝트에 대한 Jira 문제를 생성하여 피드백을 제공하거나 오류를 보고할 수 있습니다. 여기서 피드백의 진행 상황을 추적할 수 있습니다. Red Hat Jira 계정이 있어야 하며 로그인해야 합니다.

1. Create Issue 양식을 시작합니다.
2. **요약**,**설명** 및 **보고자** 필드를 완료합니다.
   설명 필드에 문서 URL, 장 또는 섹션 번호, 문제에 대한 자세한 설명을 포함합니다.
3. **생성**을 클릭합니다.

1장. 릴리스 정보

이 릴리스 노트에서는 Red Hat OpenShift Container Platform 4.15와 함께 OpenShift 샌드박스 컨테이너 1.6의 개발을 추적합니다.

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

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

2장. 새로운 기능 및 개선 사항

이 섹션에서는 OpenShift 샌드박스 컨테이너 1.6에 도입된 새로운 기능 및 개선 사항에 대해 설명합니다.

2.1. 퍼블릭 클라우드

새로운 Pod VM 이미지 생성 흐름을 통해 사용자 환경 개선

이번 릴리스에서는 **kata** 런타임을 설치한 후 Pod VM 이미지가 생성됩니다. 이미지가 생성되는 동안 상태 업데이트를 볼 수 있습니다.

Jira:KATA-2781

3장. 버그 수정

이 섹션에서는 OpenShift 샌드박스 컨테이너 1.6에서 수정된 버그에 대해 설명합니다.

3.1. 샌드박스 컨테이너

io.katacontainers.config.hypervisor.virtio_fs_extra_args 주석이 있는 Pod가 시작되지 않음

이전에는 **virtiofsd** 에서 **--thread-pool-size=16** 옵션을 허용하지 않았습니다. 이 문제는 OpenShift Container Platform 4.13.24 및 4.14.4에서 사용할 수 있는 **virtiofsd-1.5.0-1.el9_2.1** 에서 해결되었습니다.

Jira:KATA-2146

3.2. 성능 및 확장

RHEL 9 컴퓨팅 노드에서 심각한 데이터베이스 워크로드 성능 저하

RHEL(Red Hat Enterprise Linux) 9 컴퓨팅 노드에서 실행되는 데이터베이스 워크로드에서는 심각한 성능 저하가 관찰되었습니다. 이 문제는 OpenShift Container Platform 4.13, 4.14 및 4.15에서 해결되었습니다.

Jira:KATA-2247

과도한 메트릭 보고로 인해 Prometheus Pod가 실패합니다.

이전에는 **kata_shim_netdev** 메트릭에서 과도하게 많은 양의 메트릭을 보고하여 **메모리 부족** 오류로 인해 Prometheus Pod가 실패했습니다. 현재 릴리스에서는 이 문제가 해결되었습니다.

Jira:KATA-2639

controller-manager pod가 메모리 부족 오류와 함께 실패합니다.

이전 버전에서는 OpenShift 샌드박스 컨테이너 Operator가 OpenShift Container Platform 4.14.12를 실행하는 단일 노드 베어 메탈 클러스터에 배포되면 **controller-manager** Pod가 **메모리 부족** 오류로 실패했습니다. 현재 릴리스에서는 Pod의 리소스를 늘림으로써 문제가 해결되었습니다.

Jira:KATA-2790

4장. 확인된 문제

이 섹션에서는 OpenShift 샌드박스 컨테이너 1.6의 알려진 문제에 대해 설명합니다.

4.1. 보안

샌드박스 컨테이너는 SELinux 다중 범주 보안 레이블을 지원하지 않음

컨테이너의 보안 컨텍스트에서 SELinux MCS(Multi-Category Security) 레이블을 설정하면 Pod가 시작되지 않습니다. Pod 로그에 다음 오류가 표시됩니다.

```
Error: CreateContainer failed: EACCES: Permission denied: unknown
```

샌드박스 컨테이너가 생성될 때 런타임은 컨테이너의 보안 컨텍스트에 액세스할 수 없습니다. 즉 **virtiofsd** 는 적절한 SELinux 레이블로 실행되지 않으며 컨테이너의 호스트 파일에 액세스할 수 없습니다. 결과적으로 MCS 레이블을 사용하여 컨테이너별로 샌드박스 컨테이너의 파일을 격리할 수 없습니다. 즉, 모든 컨테이너가 샌드박스 컨테이너 내의 모든 파일에 액세스할 수 있습니다. 현재 이 문제에 대한 해결방법이 없습니다.

Jira:KATA-1875

4.2. 성능 및 확장

CPU가 오프라인 상태인 경우 컨테이너 CPU 리소스 제한 증가

요청된 CPU가 오프라인 상태인 경우 컨테이너 CPU 리소스 제한을 사용하여 Pod에 사용 가능한 CPU 수를 늘리십시오. 기능을 사용할 수 있는 경우 **oc rsh <pod> 명령을 실행하여 Pod** 에 액세스한 다음 **lscpu** 명령을 실행하여 CPU 리소스 문제를 진단할 수 있습니다.

```
$ lscpu
```

출력 예:

```
CPU(s):                16
On-line CPU(s) list:   0-12,14,15
Off-line CPU(s) list:  13
```

오프라인 CPU 목록은 예측할 수 없으며 실행 시 실행으로 변경될 수 있습니다.

해결방법: 다음 예와 같이 Pod 주석을 사용하여 추가 CPU를 요청합니다.

```
metadata:
  annotations:
    io.katacontainers.config.hypervisor.default_vcpus: "16"
```

Jira:KATA-1376

sizeLimit 을 늘리면 임시 볼륨이 확장되지 않습니다.

볼륨 크기 기본값이 샌드박스 컨테이너에 할당된 메모리의 50%이므로 Pod 사양에서 **sizeLimit** 매개변수를 사용하여 임시 볼륨을 확장할 수 없습니다.

해결방법: 볼륨을 다시 마운트하여 크기를 변경합니다. 예를 들어 샌드박스 컨테이너에 할당된 메모리가 6GB이고 임시 볼륨이 **/var/lib/containers** 에 마운트된 경우 다음 명령을 실행하여 기본적으로 이 볼륨의 크기를 3GB 이상으로 늘릴 수 있습니다.

```
$ mount -o remount,size=4G /var/lib/containers
```

Jira:KATA-2579

리소스 요청 주석이 시스템 리소스와 일치하지 않으면 피어 Pod가 실패합니다.

io.katacontainers.config.hypervisor.default_vcpus 및 **io.katacontainers.config.hypervisor.default_memory** 주석의 값은 피어 Pod에 다음과 같은 제한 사항이 있는 QEMU의 의미 체계를 따릅니다.

- **io.katacontainers.config.hypervisor.default_memory** 를 **256** 미만으로 설정하면 다음 오류가 표시됩니다.

  ```
  Failed to create pod sandbox: rpc error: code = Unknown desc = CreateContainer failed: Memory specified in annotation io.katacontainers.config.hypervisor.default_memory is less than minimum required 256, please specify a larger value: unknown
  ```

- **io.katacontainers.config.hypervisor.default_memory** 를 **256** 으로, **io.katacontainers.config.hypervisor.default_vcpus** 를 **1** 로 설정하면 가장 작은 인스턴스 유형 또는 인스턴스 크기가 목록에서 시작됩니다.

- **io.katacontainers.config.hypervisor.default_vcpus** 를 **0** 으로 설정하면 모든 주석이 무시되고 기본 인스턴스가 시작됩니다.

해결방법: **io.katacontainers.config.hypervisor.machine_type** 을 구성 맵에 지정된 기본 AWS 인스턴스 유형 또는 구성 맵에 지정된 Azure 인스턴스 크기로 설정하여 유연한 Pod VM 크기를 활성화합니다.

Jira:KATA-2575, Jira:KATA-2578, Jira:KATA-2577

5장. 비동기 에라타 업데이트

OpenShift 샌드박스 컨테이너의 보안, 버그 수정 및 개선 사항 업데이트는 Red Hat Network를 통해 비동기 에라타로 릴리스됩니다.

Red Hat OpenShift Container Platform 4.15 에라타는 Red Hat Customer Portal 을 통해 제공됩니다.

비동기 에라타에 대한 자세한 내용은 OpenShift Container Platform 라이프 사이클 을 참조하십시오.

Red Hat 서브스크립션 관리 설정에서 에라타 이메일 알림을 활성화할 수 있습니다. 등록된 시스템 및 OpenShift Container Platform 인타이틀먼트가 있는 Red Hat 고객 포털 계정이 있어야 합니다.

이 섹션은 향후 OpenShift 샌드박스 컨테이너의 비동기 에라타 릴리스의 개선 사항 및 버그 수정에 대한 정보 제공을 위해 지속적으로 업데이트됩니다.

5.1. RHBA-2024:3964 - OPENSHIFT 샌드박스 컨테이너 1.6.0 이미지 릴리스, 버그 수정 및 개선 권고

출시 날짜: 2024-06-18

OpenShift 샌드박스 컨테이너 릴리스 1.6.0이 공개되었습니다. 이 권고에는 개선 사항 및 버그 수정이 포함된 OpenShift 샌드박스 컨테이너 업데이트를 포함합니다.

업데이트에 포함된 버그 수정 목록은 RHBA-2024:3964 권고에 설명되어 있습니다.

부록 A. 구성 요소별 티켓 목록

이 문서에는 Bugzilla 및 JIRA 티켓이 기재되어 있습니다. 링크는 티켓을 설명하는 이 문서의 릴리스 노트로 이어집니다.

Component	티켓
성능 / 확장	JIRA:KATA-1376,Jira:KATA-2579,Jira:KATA-2575,Jira:KATA-2247,Jira:KATA-2639,Jira:KATA-2790
퍼블릭 클라우드	Jira:KATA-2781
샌드박스 컨테이너	Jira:KATA-2146
보안	Jira:KATA-1875