Red Hat Ceph Storage 5

데이터 보안 및 강화 가이드

Red Hat Ceph Storage Data Security and Hardening Guide

Last Updated: 2023-03-18

Red Hat Ceph Storage 5 데이터 보안 및 강화 가이드

Red Hat Ceph Storage Data Security and Hardening Guide

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

법적 공지

초록

이 문서에서는 Ceph Storage 클러스터 및 해당 클라이언트에 대한 데이터 보안 및 강화 정보를 제공합니다. 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 메시지에서 참조하십시오.

차례

1장. 소개

보안은 중요한 문제이며 모든 Red Hat Ceph Storage 배포에 중점을 두고 있어야 합니다. 데이터 위반 및 다운타임은 비용이 많이 들고 관리하기 어렵습니다. 법률은 감사 및 규정 준수 프로세스를 통과해야 할 수 있으며 프로젝트에서 특정 수준의 데이터 개인 정보 보호 및 보안을 기대할 수 있습니다. 이 문서에서는 Red Hat Ceph Storage의 보안을 일반적으로 소개하고 시스템 보안을 지원하기 위한 Red Hat의 역할에 대해 설명합니다.

1.1. 머리말

이 문서에서는 Red Hat Ceph Storage 배포에 **cephadm** 을 사용하는 Ceph Orchestrator에 중점을 두고 Red Hat Ceph Storage의 보안 강화에 대한 조언과 모범 사례를 제공합니다. 이 가이드의 지침에 따라 사용자 환경의 보안을 강화할 수 있지만 이러한 권장 사항에 따라 보안 또는 규정 준수를 보장하지 않습니다.

1.2. RED HAT CEPH STORAGE 소개

RHCS(Red Hat Ceph Storage)는 확장성이 높고 안정적인 오브젝트 스토리지 솔루션으로, 일반적으로 OpenStack과 같은 클라우드 컴퓨팅 솔루션과 함께, 독립 실행형 스토리지 서비스로 또는 iSCSI와 같은 인터페이스를 사용하는 네트워크 연결 스토리지로 배포됩니다.

모든 RHCS 배포는 일반적으로 Ceph Storage 클러스터 또는 RADOS(Reliable Autonomous Distributed Object Store)라고 하는 스토리지 클러스터로 구성됩니다. 여기에는 다음 세 가지 유형의 데몬으로 구성됩니다.

- **Ceph 모니터(ceph-mon):** Ceph 모니터는 클러스터 상태에 대한 계약을 설정하고, OSD가 실행 및 실행 중인지와 같은 클러스터 상태 기록 유지, 클라이언트의 쓰기 및 읽기 및 클라이언트 및 Ceph Storage Cluster 데몬에 대한 인증과 같은 몇 가지 중요한 기능을 제공합니다.

- **Ceph Manager(ceph-mgr):** Ceph manager 데몬은 Ceph OSD 간에 배포된 배치 그룹의 사본, 배치 그룹 상태 기록, Ceph 클러스터에 대한 지표와 Ceph 클러스터 간의 피어링 상태를 추적합니다. 외부 모니터링 및 관리 시스템에 대한 인터페이스도 제공합니다.

- **Ceph OSD(ceph-osd):** Ceph Object Storage Daemon(OSD)은 클라이언트 데이터를 저장 및 제공하고, 클라이언트 데이터를 보조 Ceph OSD 데몬으로 복제하고, 주변 OSD 데몬에서 Ceph Monitor에 보고하며, 다른 기능 중에서 클러스터 크기가 중단될 때 데이터를 동적으로 복구하고, 데이터를 다시 입력합니다.

모든 RHCS 배포는 Ceph Storage 클러스터 또는 RADOS(Reliable Autonomous Distributed Object Store)에 최종 사용자 데이터를 저장합니다. 일반적으로 사용자는 **Ceph** Storage 클러스터와 직접 상호 작용하지 않고 Ceph 클라이언트와 상호 작용합니다.

다음 세 가지 기본 Ceph Storage 클러스터 클라이언트가 있습니다.

- **Ceph Object Gateway(radosgw):** RADOS 게이트웨이라고도 하는 Ceph 개체 게이트웨이, **radosgw** 또는 **rgw** 는 RESTful API를 사용하여 오브젝트 스토리지 서비스를 제공합니다. Ceph Object Gateway는 Ceph Storage Cluster 또는 RADOS에 클라이언트를 대신하여 데이터를 저장합니다.

- **Ceph 블록 장치(rbd):** Ceph 블록 장치는 쓰기가 copy-on-write, thin-provisioned 및 복제 가능한 가상 블록 장치를 커널 RBD(dpdkd)를 통해 Linux 커널에 제공하거나 **librbd** 를 통해 OpenStack과 같은 클라우드 컴퓨팅 솔루션에 사용할 수 있습니다.

- **Ceph 파일 시스템(cephfs): Ceph 파일 시스템은 하나 이상의 메타데이터 서버(mds)로 구성**

되며, 파일 시스템의 **inode** 부분을 **Ceph Storage** 클러스터의 오브젝트로 저장합니다. **Ceph** 파일 시스템은 커널 클라이언트, **FUSE** 클라이언트 또는 **OpenStack**과 같은 클라우드 컴퓨팅 솔루션의 **libcephfs** 라이브러리를 통해 마운트할 수 있습니다.

추가 클라이언트에는 개발자가 관리 목적으로 **Ceph Storage** 클러스터 및 명령줄 인터페이스 클라이언트와 상호 작용할 수 있는 사용자 지정 애플리케이션을 생성할 수 있는 **librados** 가 포함되어 있습니다.

1.3. 지원 소프트웨어

Red Hat Ceph Storage 보안의 중요한 측면은 보안 기능이 내장되어 있으며 시간이 지남에 따라 **Red Hat**이 지원하는 솔루션을 제공하는 것입니다. **Red Hat**에서 **Red Hat Ceph Storage**를 사용하는 구체적인 단계는 다음과 같습니다.

- 업스트림 관계 및 커뮤니티 참여를 유지하여 처음부터 보안에 중점을 둡니다.
- 보안 및 성능 추적 레코드를 기반으로 패키지 선택 및 구성.
- 관련 소스 코드에서 바이너리를 빌드합니다(업스트림 빌드를 수락하는 대신).
- 다양한 잠재적인 보안 문제 및 회귀 문제를 방지하기 위해 검사 및 품질 보장 툴 모음을 적용합니다.
- 릴리스된 모든 패키지에 디지털 서명하고 암호화 방식으로 인증된 배포 채널을 통해 배포합니다.
- 패치 및 업데이트 배포를 위한 통합된 단일 메커니즘 제공.

또한 **Red Hat**은 제품에 대한 위협 및 취약점을 분석하고 고객 포털을 통해 관련 권고 및 업데이트를 제공하는 전용 보안 팀을 유지합니다. 이 팀은 대부분 이론적인 문제와 달리 중요한 문제와 달리 중요한 문제를 결정합니다. **Red Hat** 제품 보안 팀은 전문 지식을 유지하고 서브스크립션 제품과 관련된 업스트림 커뮤니티에 광범위한 기여를 수행합니다. 이 프로세스의 핵심 부분인 **Red Hat Security Advisories**는 **Red Hat** 솔루션에 영향을 미치는 보안 결함에 대한 사전 예방 알림을 제공하며, 이러한 패치는 취약점이 처음 게시되는 날 자주 배포되는 패치와 함께 제공됩니다.

2장. 위협 및 취약점 관리

Red Hat Ceph Storage(RHCS)는 일반적으로 클라우드 컴퓨팅 솔루션과 함께 배포되므로 대규모 배포의 여러 구성 요소 중 하나로 추상화적으로 **Red Hat Ceph Storage** 배포를 생각하는 것이 도움이 될 수 있습니다. 이러한 배포에는 일반적으로 공유 보안 문제가 있으며, 이 안내서는 *보안 영역을* 나타냅니다. 위협 행위자 및 벡터는 자신의 동기 및 리소스에 대한 액세스를 기반으로 분류됩니다. 목표는 목표에 따라 각 영역에 대한 보안 문제를 감지하는 것입니다.

2.1. 위협 행위

위협 행위자는 보안을 시도할 수 있는 클래스를 나타내는 추상적인 방법입니다. 액터가 많을수록 공격 완화 및 예방에 필요한 보안 제어가 더욱 엄격합니다. 보안은 요구 사항에 따라 밸런싱 편의성, 보호 및 비용 문제입니다. 여기에 설명된 모든 위협 행위자에 대해 **Red Hat Ceph Storage** 배포를 보호할 수 없는 경우가 있습니다. **Red Hat Ceph Storage**를 배포할 때는 배포 및 사용량에 대한 균형을 결정해야 합니다.

위험 평가의 일환으로, 사용자가 저장하는 데이터 유형 및 액세스 가능한 리소스 유형도 고려해야 합니다. 이는 특정 행위자에게 영향을 미치기 때문입니다. 그러나 데이터가 위협 행위자에 반대하지 않더라도 단순히 컴퓨팅 리소스로 끌어들일 수 있습니다.

- 국가주권 행위자: 이것은 가장 잘 할 수 있는 광고입니다. 국내 주주 행위자는 대상에 대해 막대한 리소스를 가져올 수 있습니다. 그 이상의 다른 액추에이를 가지고 있습니다. 인간과 기술 모두 엄격한 통제없이 이러한 행위자를 보호하는 것은 어렵습니다.

- 심각한 **Crime:** 이 클래스는 높은 성능 및 재무적으로 구동되는 공격자 그룹을 설명합니다. 사내에서 개발 및 목표 조사를 통해 비용을 절감할 수 있습니다. 최근 몇 년 동안 대규모의 온라인 기업 기업인 러시아 비즈니스 네트워크와 같은 조직의 상승 추세가 사이버 공격이 상용이 된 것으로 입증되었습니다. **I industryespionage**는 심각한 조직된 범죄 그룹에 속합니다.

- 높은 기능 그룹: 일반적으로 상업적으로 청구되지 않은 **'Hacktivist'** 유형의 조직은 언급하지만 서비스 제공 업체 및 클라우드 운영자에게 심각한 위협을 초래할 수 있습니다.

- 동기가 있는 개인: 이 공격자는 악성인 또는 악의적인 직원, 불명한 고객 또는 소규모 산업 후원과 같은 많은 위장으로 나타납니다.

- **script Kiddies:** 이 공격자는 특정 조직을 대상으로 하지 않지만 자동 취약점 검사 및 악용을 실행합니다. 이러한 행위자 중 하나를 공격하는 것은 종종 부정 행위자이며, 조직의 명예에 대한 주요 위험입니다.

다음 사례는 위에서 확인한 몇 가지 위험을 완화하는 데 도움이 될 수 있습니다.

- 보안 업데이트: 네트워킹, 스토리지 및 서버 하드웨어를 포함한 기본 물리적 인프라의 엔드 투 엔드 보안 자세를 고려해야 합니다. 이러한 시스템에는 자체 보안 강화 사례가 필요합니다. **Red Hat Ceph Storage** 배포를 위해 보안 업데이트를 정기적으로 테스트하고 배포할 계획이 있어야 합니다.

- 제품 업데이트: **Red Hat**은 제품 업데이트를 사용할 수 있게 되는 것을 권장합니다. 업데이트는 일반적으로 **6**주 마다 릴리스되며 간혹 더 자주 릴리스됩니다. **Red Hat**은 추가 통합 테스트를 필요로 하지 않기 위해 주요 릴리스 내에서 포인트 릴리스와 **z-stream** 릴리스를 완전히 호환하려고 노력합니다.

- 액세스 관리: 액세스 관리에는 인증, 권한 부여 및 회계가 포함됩니다. 인증은 사용자 **ID**를 확인하는 프로세스입니다. 권한 부여는 인증된 사용자에게 권한을 부여하는 프로세스입니다. 회계는 어떤 사용자가 작업을 수행했는지 추적하는 프로세스입니다. 사용자에게 시스템 액세스 권한을 부여하는 경우 *최소 권한 원칙* 을 적용하고 사용자에게 실제로 필요한 세분화된 시스템 권한만 부여합니다. 이 방법은 시스템 관리자의 악의적인 행위자 및 오타 오류의 위험을 완화하는 데 도움이 될 수 있습니다.

- **pxe s** 관리: 역할 기반 액세스 제어(최소 필요 액세스)를 신중하게 할당하고 내부 인터페이스에서 암호화를 사용하고 인증/권한화 보안(예: 중앙 집중식 **ID** 관리)을 사용하여 악의적인 내부자의 위협을 완화할 수 있습니다. 작업 분리 및 불규칙한 작업 역할 회전과 같은 비기술적 옵션을 추가로 고려할 수도 있습니다.

2.2. 보안 영역

보안 영역은 시스템 내에서 공통 신뢰 요구 사항과 기대치를 공유하는 사용자, 애플리케이션, 서버 또는 네트워크로 구성됩니다. 일반적으로 동일한 인증, 권한 부여 요구 사항 및 사용자를 공유합니다. 이러한 영역 정의를 추가로 세분화할 수 있지만 이 안내서에서는 **4**개의 개별 보안 영역을 나타냅니다. 이 중 **3** 개는 보안이 강화된 **Red Hat Ceph Storage** 클러스터를 배포하는 데 필요한 베어 최소의 구성입니다. 이러한 보안 영역은 최소한 신뢰할 수 있는 보안 영역보다 아래에 나열되어 있습니다.

- 퍼블릭 보안 영역: 퍼블릭 보안 영역은 클라우드 인프라의 완전히 신뢰할 수 없는 영역입니다. 권한이 없는 **Red Hat OpenStack** 배포의 외부에 있는 네트워크 전체 또는 간단히 인터넷을 참조할 수 있습니다. 이 영역을 통과하는 기밀성 또는 무결성 요구 사항이 있는 모든 데이터는 암호화와 같은 배려 제어를 사용하여 보호해야 합니다. 공개 보안 영역 **SHOULD** 는 **RHCS**의 **public_network** 라고 하는 **Ceph Storage** 클러스터의 프런트 또는 클라이언트 측 네트워크와 혼동되지 않으며 일반적으로 퍼블릭 보안 영역 또는 **Ceph** 클라이언트 보안 영역의 일부가 아닙니다.

- **Ceph** 클라이언트 보안 영역: **RHCS**를 사용하면 **Ceph** 클라이언트 보안 영역은 **Ceph Object**

Gateway, Ceph Block Device, Ceph Filesystem 또는 librados 와 같은 Ceph 클라이언트에 액세스하는 네트워크를 나타냅니다. Ceph 클라이언트 보안 영역은 일반적으로 공개 보안 영역과 자체적으로 분리된 방화벽 뒤에 있습니다. 그러나 Ceph 클라이언트가 퍼블릭 보안 영역으로부터 항상 보호되는 것은 아닙니다. 퍼블릭 보안 영역에 Ceph Object Gateway의 S3 및 Swift API를 노출할 수 있습니다.

- 스토리지 액세스 보안 영역: 스토리지 액세스 보안 영역은 Ceph 클라이언트에 Ceph Storage 클러스터에 대한 액세스 권한을 제공하는 내부 네트워크를 나타냅니다. 이 문서가 OpenStack Platform Security 및 Hardening Guide에서 사용되는 용어와 일치하도록 "스토리지 액세스 보안 영역"을 사용합니다. 스토리지 액세스 보안 영역에는 RHCS의 public_network 라고 하는 Ceph Storage 클러스터의 프론트 또는 클라이언트 측 네트워크가 포함됩니다.

- Ceph 클러스터 보안 영역: Ceph 클러스터 보안 영역은 Ceph Storage 클러스터의 OSD 데몬에 복제, 하트비트, 백필링 및 복구를 위한 네트워크 통신을 제공하는 내부 네트워크를 나타냅니다. Ceph 클러스터 보안 영역에는 RHCS의 cluster_network 라고 하는 Ceph Storage Cluster의 백 측 네트워크가 포함되어 있습니다.

이러한 보안 영역은 별도로 매핑하거나 결합되어 지정된 RHCS 배포 내에서 가능한 신뢰 영역의 대부분을 나타낼 수 있습니다. 특정 RHCS 배포 토폴로지에 대해 보안 영역을 매핑해야 합니다. 영역 및 신뢰 요구 사항은 Red Hat Ceph Storage가 독립 실행형 용량에서 작동하는지 아니면 퍼블릭, 프라이빗 또는 하이브리드 클라우드를 제공하는지에 따라 달라집니다.

이러한 보안 영역을 시각적으로 표현하려면 보안 최적화 아키텍처를 참조하십시오.

추가 리소스

- 자세한 내용은 *Red Hat Ceph Storage Data Security 및 Hardening Guide* 의 *Network* communications 섹션을 참조하십시오.

2.3. 보안 영역 연결

신뢰 수준 또는 인증 요구 사항이 다른 여러 보안 영역에 걸쳐 있는 모든 구성 요소를 신중하게 구성해야 합니다. 이러한 연결은 네트워크 아키텍처의 약한 지점이며 항상 연결되어 있는 영역 중 가장 높은 신뢰 수준의 보안 요구 사항을 충족하도록 구성해야 합니다. 대부분의 경우 연결된 영역의 보안 제어는 공격 가능성으로 인해 주요 우려가 되어야 합니다. 영역이 충족되는 포인트는 공격자가 배포의 더 중요한 부분으로 공격을 마이그레이션하거나 대상으로 지정할 수 있는 기회를 제공합니다.

경우에 따라 Red Hat Ceph Storage 관리자는 통합 지점이 상주하는 영역보다 높은 표준의 통합 지점을 보호하는 것을 고려할 수 있습니다. 예를 들어, Ceph Cluster Security Zone은 다른 보안 영역에 쉽게 연결할 이유가 없기 때문에 다른 보안 영역과 쉽게 분리할 수 있습니다. 반면 Storage Access Security Zone은 Ceph 모니터 노드의 포트 6789 와 Ceph OSD 노드의 포트 6800-7300 에 대한 액세스를 제공해야 합니다. 그러나 포트 3000 은 Ceph 관리자에게만 노출되어야 하는 Ceph Grafana 모니터링 정보에 대

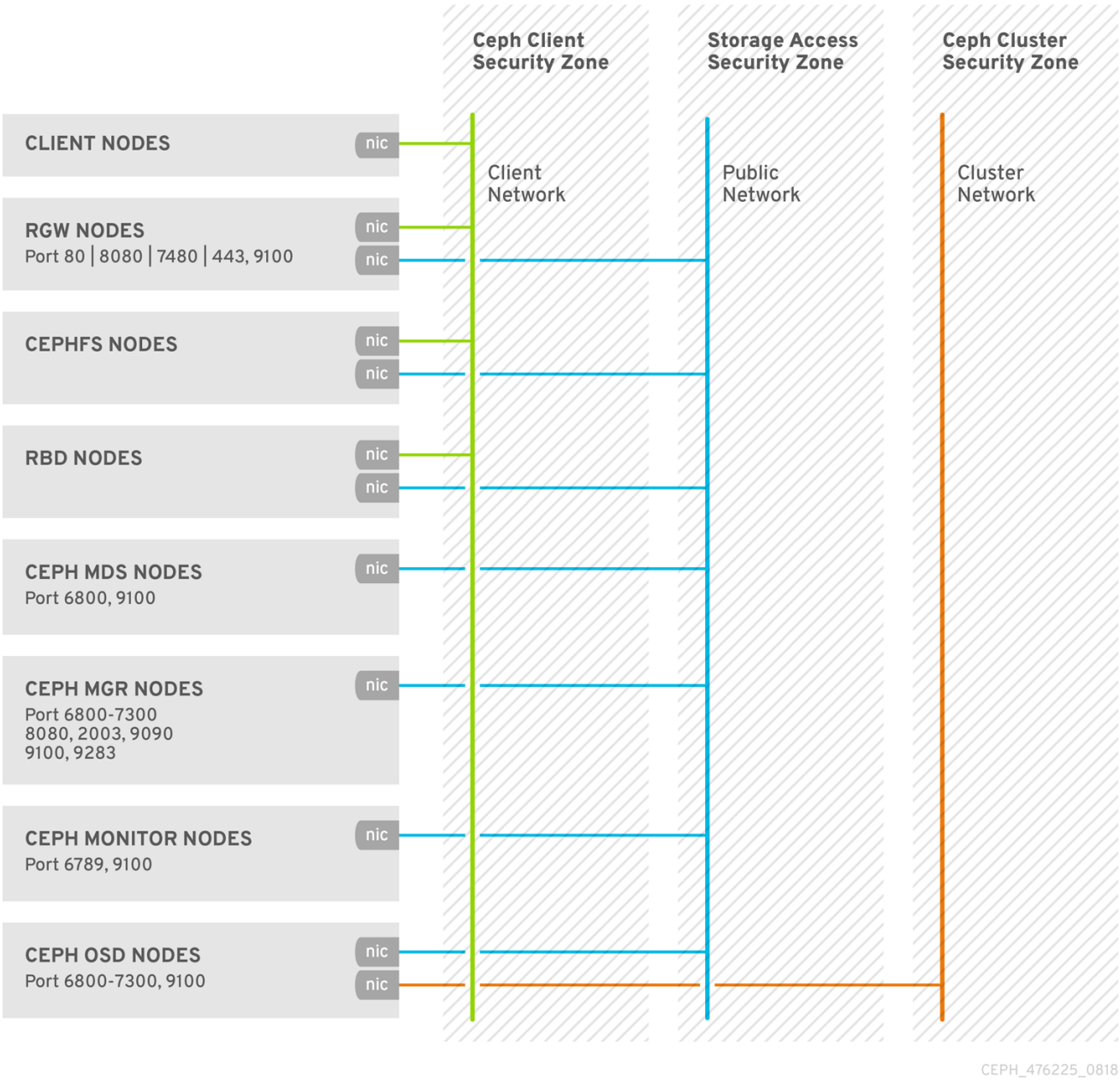
한 액세스를 제공하기 때문에 스토리지 액세스 보안 영역에만 독점적이어야 합니다. Ceph 클라이언트 보안 영역의 Ceph Object Gateway는 Ceph Cluster Security Zone의 모니터(포트 6789) 및 OSD(포트 6800-7300)에 액세스해야 하며, S3 및 Swift API를 HTTP 포트 80 또는 HTTPS 포트 443 과 같은 공용 보안 영역에 노출해야 하지만, 관리 API로 액세스를 제한해야 할 수 있습니다.

Red Hat Ceph Storage의 설계는 보안 영역을 분리하기 어렵습니다. 핵심 서비스는 일반적으로 두 개 이상의 영역에 걸쳐 있으므로 보안 제어를 적용할 때 특수 고려해야 합니다.

2.4. SECURITY-OPTIMIZED ARCHITECTURE

Red Hat Ceph Storage 클러스터의 데몬은 일반적으로 서브넷이 분리되어 방화벽 뒤에서 실행되는 노드에서 실행되므로 RHCS 클러스터의 보안을 비교적 간단하게 수행할 수 있습니다.

반면 Ceph 블록 장치(rbd), Ceph Filesystem(cephfs), Ceph Object Gateway(rgw)와 같은 Red Hat Ceph Storage 클라이언트는 RHCS 스토리지 클러스터에 액세스하지만 해당 서비스를 다른 클라우드 컴퓨팅 플랫폼에 노출합니다.


Ceph Client Security Zone
Storage Access Security Zone
Ceph Cluster Security Zone
CLIENT NODES
nic
RGW NODES
Port 80 | 8080 | 7480 | 443, 9100
nic
nic
CEPHFS NODES
nic
nic
RBD NODES
nic
nic
CEPH MDS NODES
Port 6800, 9100
nic
CEPH MGR NODES
Port 6800-7300
8080, 2003, 9090
9100, 9283
nic
CEPH MONITOR NODES
Port 6789, 9100
nic
CEPH OSD NODES
Port 6800-7300, 9100
nic
nic
Client Network
Public Network
Cluster Network
CEPH_476225_0818

3장. 암호화 및 키 관리

Red Hat Ceph Storage 클러스터는 일반적으로 프라이빗 스토리지 클러스터 네트워크를 사용하는 경우 일반적으로 자체 네트워크 보안 영역에 있습니다.

중요

공격자가 공용 네트워크에서 **Ceph** 클라이언트에 액세스할 수 있는 경우 보안 영역 분리가 충분하지 않을 수 있습니다.

네트워크 트래픽의 기밀성 또는 무결성을 보장하고 **Red Hat Ceph Storage**가 암호화 및 키 관리를 사용하는 경우 다음과 같은 보안 요구 사항이 있는 경우가 있습니다.

- **SSH**
- **SSL** 종료
- **Transit**의 암호화
- **Rest**의 암호화

3.1. SSH

Red Hat Ceph Storage 클러스터의 모든 노드는 클러스터 배포의 일부로 **SSH**를 사용합니다. 즉, 각 노드에서 다음을 수행합니다.

- 암호가 없는 **root** 권한이 있는 **cephadm** 사용자가 있습니다.
- **SSH** 서비스가 활성화되어 있고 확장 포트 **22**가 열려 있습니다.
- **cephadm** 사용자의 공용 **SSH** 키 사본을 사용할 수 있습니다.

중요

확장 기능을 통해 **cephadm** 사용자에 액세스할 수 있는 모든 사용자는 **Red Hat Ceph Storage** 클러스터의 모든 노드에서 **root** 로 명령을 실행할 수 있는 권한이 있습니다.

추가 리소스

- 자세한 내용은 ***Red Hat Ceph Storage*** *설치 가이드* 의 ***How cephadm*** *작동* 섹션을 참조하십시오.

3.2. SSL 종료

Ceph Object Gateway는 **HAProxy**와 함께 배포될 수 있으며 로드 밸런싱 및 페일오버를 위해 **keepalived** 를 배포할 수 있습니다. 오브젝트 게이트웨이 **Red Hat Ceph Storage** 버전 **2** 및 **3**에서는 **Civetweb**을 사용합니다. 이전 버전의 **Civetweb**에서는 **SSL**을 지원하지 않으며 일부 성능 제한으로 **SSL**을 지원합니다.

Red Hat Ceph Storage 버전 **5**에서 오브젝트 게이트웨이는 **Beast**를 사용합니다. **OpenSSL** 라이브러리를 사용하여 **TLS(Transport Layer Security)**를 제공하도록 **Beast** 프런트 엔드 웹 서버를 구성할 수 있습니다.

HAProxy를 사용하고 **keepalived** 를 사용하여 **SSL** 연결을 종료하는 경우 **HAProxy** 및 **keepalived** 구성 요소는 암호화 키를 사용합니다.

HAProxy를 사용하고 **keepalived** 를 사용하여 **SSL**을 종료하는 경우 로드 밸런서와 **Ceph Object Gateway** 간의 연결은 암호화 되지 않습니다.

자세한 내용은 ***Configuring SSL for Beast*** 및 ***HAProxy 및 keepalived*** 를 참조하십시오.

3.3. ECDHE V2 프로토콜

Ceph의 유선 프로토콜인 **msgr2** 의 두 번째 버전에는 다음과 같은 기능이 있습니다.

- 네트워크를 통해 이동하는 모든 데이터를 암호화하는 보안 모드입니다.

- 인증 페이로드의 캡슐화를 개선하여 새로운 인증 모드를 향후 통합할 수 있습니다.

- 광고 및 협상의 기능 개선

Ceph 데몬은 레거시 v1- 호환 및 새로운 v2 호환 Ceph 클라이언트를 허용하는 여러 포트에 바인딩되어 동일한 스토리지 클러스터에 연결합니다. Ceph Monitor 데몬에 연결하는 Ceph 클라이언트 또는 기타 Ceph 데몬에서는 먼저 v2 프로토콜을 사용하지만 가능하면 레거시 v1 프로토콜을 사용합니다. 기본적으로 v1 및 v2 프로토콜 모두 사용됩니다. 새로운 v2 포트는 3300이며, 레거시 v1 포트는 기본적으로 6789입니다.

동작 v2 프로토콜에는 v1 또는 v2 프로토콜 사용 여부를 제어하는 두 가지 구성 옵션이 있습니다.

- ms_bind_msgr1 - 이 옵션은 데몬이 v1 프로토콜이라는 포트에 바인딩하는지 여부를 제어합니다. 기본적으로 마찬가지입니다.

- ms_bind_msgr2 - 이 옵션은 데몬이 v2 프로토콜이라는 포트에 바인딩하는지 여부를 제어합니다. 기본적으로 마찬가지입니다.

마찬가지로, 사용된 IPv4 및 IPv6 주소를 기반으로 두 가지 옵션을 제어합니다.

- ms_bind_ipv4 - 이 옵션은 데몬이 IPv4 주소에 바인딩하는지 여부를 제어합니다. 기본적으로 true 입니다.

- ms_bind_ipv6 - 이 옵션은 데몬이 IPv6 주소에 바인딩하는지 여부를 제어합니다. 기본적으로 true 입니다.

참고

여러 포트에 바인딩할 수 있는 기능은 듀얼 스택 IPv4 및 IPv6 지원을 제공합니다.

msgr2 프로토콜은 다음 두 가지 연결 모드를 지원합니다.

- crc
  - Gradle 에 대한 연결이 설정된 경우 강력한 초기 인증을 제공합니다.
  - 비트 플립을 보호하기 위해 crc32c 무결성 검사를 제공합니다.
  - 악성 메시지 가로채기(man-in-the-middle) 공격에 대한 보호를 제공하지 않습니다.
  - eavesdropper가 모든 인증 후 트래픽을 보는 것을 방지하지 않습니다.
- 보안
  - Gradle 에 대한 연결이 설정된 경우 강력한 초기 인증을 제공합니다.
  - 모든 인증 후 트래픽의 전체 암호화를 제공합니다.
  - 암호화 무결성 검사를 제공합니다.

기본 모드는 crc 입니다.

Ceph Object Gateway 암호화

또한 Ceph Object Gateway는 S3 API를 사용하여 고객 제공 키로 암호화를 지원합니다.

중요

관리자는 전송 시 엄격한 암호화가 필요한 규정 준수 표준을 준수하기 위해 클라이언트 측 암호화를 사용하여 Ceph Object Gateway를 배포 해야 합니다.

Ceph 블록 장치 암호화

Red Hat OpenStack Platform 13의 백엔드로 Ceph를 통합하는 시스템 관리자는 RBD Cinder에 대

해 **dm_crypt** 를 사용하여 **Ceph** 블록 장치 볼륨을 암호화하여 **Ceph** 스토리지 클러스터 내에서 유선 암호화를 보장합니다.

중요

시스템 관리자는 전송 시 엄격한 암호화가 필요한 규제 준수 표준을 준수하기 위해 **RBD Cinder**에 **dmcrypt** 를 사용하여 **Ceph** 스토리지 클러스터 내에서 유선 암호화를 확인해야 합니다.

추가 리소스

- 자세한 내용은 ***Red Hat Ceph Storage Configuration Guide*** 의 *연결 모드 구성 옵션을* 참조하십시오.

3.4. 전송 중 암호화

Red Hat Ceph Storage 5 이상부터 네트워크를 통한 모든 **Ceph** 트래픽에 대한 암호화는 기본적으로 활성화되어 있으며, 이는 지저 버전 **2** 프로토콜을 도입하여 기본적으로 활성화됩니다. **v2**의 보안 모드 설정은 **Ceph** 데몬과 **Ceph** 클라이언트 간의 통신을 암호화하여 엔드 투 엔드 암호화를 제공합니다.

ceph config dump 명령, **netstat -lp | grep ceph-osd** 명령을 사용하여 지저 **v2** 프로토콜의 암호화를 확인하거나 **v2** 포트에서 **Ceph** 데몬을 확인할 수 있습니다.

추가 리소스

- ***SSL 종료*** 에 대한 자세한 내용은 **SSL** 종료를 참조하십시오.
- ***S3 API 암호화에 대한 자세한 내용은 S3 서버 측*** 암호화를 참조하십시오.

3.5. REST의 암호화

Red Hat Ceph Storage는 다음과 같은 몇 가지 시나리오에서 암호화를 지원합니다.

1. **Ceph Storage Cluster: Ceph Storage Cluster**는 **Ceph OSD**의 **Linux Unified Key Setup** 또는 **LUKS** 암호화와 해당 저널, 미리 쓰기 로그, 메타데이터 데이터베이스를 지원합니다. 이 시나리오에서 **Ceph**는 클라이언트가 **Ceph** 블록 장치, **Ceph** 파일 시스템 또는 **librados** 에 구축된 사용자 지정 애플리케이션인지와 관계없이 모든 데이터를 암호화합니다.

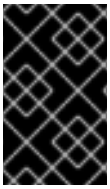
2. **Ceph Object Gateway: Ceph** 스토리지 클러스터는 클라이언트 오브젝트 암호화를 지원합니다. **Ceph Object Gateway**가 개체를 암호화하면 **Red Hat Ceph Storage** 클러스터와 독립적으로 암호화됩니다. 또한 전송된 데이터는 **Ceph Object Gateway**와 **Ceph Storage Cluster** 간의 암호화된 형식입니다.

Ceph Storage 클러스터 암호화

Ceph 스토리지 클러스터는 **Ceph OSD**에 저장된 데이터 암호화를 지원합니다. **Red Hat Ceph Storage**는 **dmcrypt** 를 지정하여 논리 볼륨을 암호화할 수 있습니다. 즉, **ceph-volume** 에 의해 호출되는 **lvm ;** 즉, 물리적 볼륨이 아닌 **OSD**의 논리 볼륨을 암호화합니다. 동일한 **OSD** 키를 사용하여 파티션과 같은 비**LVM** 장치를 암호화할 수 있습니다. 논리 볼륨을 암호화하면 구성 유연성이 향상됩니다.

LUKS v1은 **LUKS v2** 대신 **LUKS v1**을 사용합니다. **LUKS v1**은 **Linux** 배포판 간에 가장 광범위한 지원을 받기 때문입니다.

OSD를 생성할 때 **lvm** 은 시크릿 키를 생성하고 **stdin** 을 통해 **JSON** 페이로드에서 안전하게 **Ceph Monitor**에 키를 전달합니다. 암호화 키의 속성 이름은 **dmcrypt_key** 입니다.



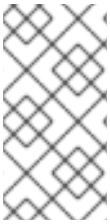
중요

시스템 관리자는 암호화를 명시적으로 활성화해야 합니다.

기본적으로 **Ceph**는 **Ceph OSD**에 저장된 데이터를 암호화하지 않습니다. 시스템 관리자는 **dmcrypt** 를 사용하여 **Ceph OSD**에 저장된 데이터를 암호화해야 합니다. **Ceph OSD**를 스토리지 클러스터에 추가하는 데 **Ceph Orchestrator** 서비스 사양 파일을 사용하는 경우 파일에서 다음 옵션을 설정하여 **Ceph OSD**를 암호화합니다.

예제

```
...
encrypted: true
...
```



참고

LUKS 및 **dmcrypt** 는 전송 중 데이터 암호화가 아닌 미사용 데이터의 암호화만 처리합니다.

Ceph Object Gateway 암호화

Ceph Object Gateway는 **S3 API**를 사용하여 고객 제공 키로 암호화를 지원합니다. 고객 제공 키를 사용하는 경우 **S3** 클라이언트는 암호화된 데이터를 읽거나 쓰는 각 요청과 함께 암호화 키를 전달합니다. 이러한 키를 관리하는 것은 고객의 책임입니다. 고객은 각 오브젝트를 암호화하는 데 사용되는 **Ceph Object Gateway**의 키를 알아야 합니다.

추가 리소스

- 자세한 내용은 ***Red Hat Ceph Storage*** *개발자 가이드에서* **S3 API** 서버 쪽 암호화 를 참조하십시오.

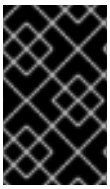
4장. ID 및 액세스 관리

Red Hat Ceph Storage는 다음을 위해 ID 및 액세스 관리를 제공합니다.

- Ceph Storage 클러스터 사용자 액세스
- Ceph Object Gateway 사용자 액세스
- Ceph Object Gateway LDAP/AD 인증
- Ceph Object Gateway OpenStack Keystone 인증

4.1. CEPH STORAGE 클러스터 사용자 액세스

사용자를 식별하고 메시지 가로채기(man-in-the-middle) 공격으로부터 보호하기 위해 Ceph는 사용자 및 데몬을 인증하는 nfsnobody 인증 시스템을 제공합니다. Gradle 에 대한 자세한 내용은 *Ceph 사용자 관리를* 참조하십시오.

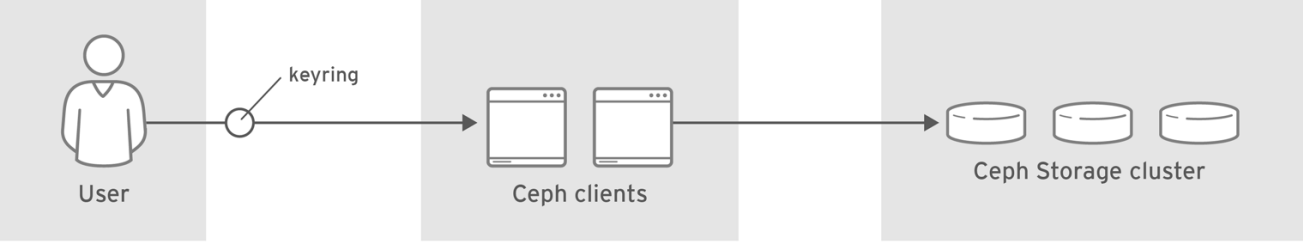


중요

Runtime Class 프로토콜은 전송 또는 암호화의 데이터 암호화를 처리하지 않습니다.

ImageCon는 인증을 위해 공유 비밀 키를 사용합니다. 즉, 클라이언트와 모니터 클러스터 모두 클라이언트의 시크릿 키 사본이 있습니다. 인증 프로토콜은 따라서 양 당사자가 실제로 공개하지 않고 키 사본을 가지고 있음을 증명할 수 있습니다. 이는 상호 인증을 제공합니다. 즉, 클러스터가 비밀 키를 소유하고, 사용자는 클러스터에 시크릿 키 사본이 있는지 확인합니다.

사용자는 Ceph 클라이언트를 사용하여 Red Hat Ceph Storage 클러스터 데몬과 상호 작용하는 애플리케이션과 같은 개인 또는 시스템 행위자입니다.



Ceph는 기본적으로 활성화되어 있는 인증 및 권한 부여로 실행됩니다. **Ceph** 클라이언트는 일반적으로 명령줄을 사용하여 지정된 사용자의 시크릿 키가 포함된 사용자 이름과 인증 키를 지정할 수 있습니다. 사용자 및 인증 키를 인수로 제공하지 않으면 **Ceph**에서 **client.admin** 관리 사용자를 기본값으로 사용합니다. 인증 키를 지정하지 않으면 **Ceph** 구성에서 인증 키 설정을 사용하여 인증 키를 찾습니다.

중요

Ceph 클러스터를 강화하기 위해 인증 키는 현재 사용자 및 루트에 대한 읽기 및 쓰기 권한만 갖습니다. **client.admin** 관리자 키가 포함된 인증 키는 **root** 사용자로 제한해야 합니다.

인증을 사용하도록 **Red Hat Ceph Storage** 클러스터를 구성하는 방법에 대한 자세한 내용은 **Red Hat Ceph Storage 5**의 *구성 가이드* 를 참조하십시오. 보다 구체적으로는 ***Ceph** 인증 구성을* 참조하십시오.

4.2. CEPH OBJECT GATEWAY 사용자 액세스

Ceph Object Gateway는 **RESTful** 애플리케이션 프로그래밍 인터페이스(**API**) 서비스에 사용자 데이터를 포함하는 **S3** 및 **Swift API**에 액세스하도록 인증하고 권한을 부여하는 자체 사용자 관리를 제공합니다. 인증은 다음으로 구성됩니다.

- **S3** 사용자: **S3 API** 사용자의 액세스 키 및 시크릿입니다.
- **Swift** 사용자: **Swift API** 사용자의 액세스 키 및 시크릿입니다. **Swift** 사용자는 **S3** 사용자의 하위 사용자입니다. **S3 'parent'** 사용자를 삭제하면 **Swift** 사용자가 삭제됩니다.
- 관리자 사용자: 관리 **API** 사용자에 대한 액세스 키 및 시크릿입니다. 관리자 사용자는 **Ceph Admin API**에 액세스하고 사용자 생성과 같은 기능을 실행하고 버킷 또는 컨테이너 및 해당 개체에 액세스할 수 있는 권한을 부여할 수 있으므로 관리자 사용자는 별도로 생성해야 합니다.

Ceph Object Gateway는 모든 사용자 인증 정보를 **Ceph Storage** 클러스터 풀에 저장합니다. 이름, 이메일 주소, 할당량 및 사용을 포함한 사용자에 대한 추가 정보를 저장할 수 있습니다.

자세한 내용은 사용자 관리 및 관리자 사용자 생성을 참조하십시오.

4.3. CEPH OBJECT GATEWAY LDAP 또는 AD 인증

Red Hat Ceph Storage는 Ceph Object Gateway 사용자를 인증하기 위해 Light-weight Directory Access Protocol(LDAP) 서버를 지원합니다. LDAP 또는 AD(Active Directory)를 사용하도록 구성하면 Ceph Object Gateway가 LDAP 서버로 지연되어 Ceph Object Gateway 사용자를 인증합니다.

Ceph Object Gateway는 LDAP 사용 여부를 제어합니다. 그러나 구성되면 사용자를 인증하는 LDAP 서버입니다.

Ceph Object Gateway와 LDAP 서버 간 통신을 보호하려면 LDAP Secure 또는 LDAPS를 사용하여 구성을 배포하는 것이 좋습니다.

중요

LDAP를 사용하는 경우 rgw_ldap_secret = *PATH_TO_SECRET_FILE* 시크릿 파일에 대한 액세스가 안전한지 확인합니다.

추가 리소스

- 자세한 내용은 *Red Hat Ceph Storage Object Gateway 가이드의 LDAP 및 Ceph Object Gateway구성* 섹션을 참조하십시오.
- 자세한 내용은 *Red Hat Ceph Storage Object Gateway 가이드의 Active Directory 및 Ceph Object Gateway구성* 섹션을 참조하십시오.

4.4. CEPH OBJECT GATEWAY OPENSTACK KEYSTONE 인증

Red Hat Ceph Storage는 OpenStack Keystone을 사용하여 Ceph Object Gateway Swift API 사용자를 인증하도록 지원합니다. Ceph Object Gateway는 Keystone 토큰을 수락하고 사용자를 인증하고 해당 Ceph Object Gateway 사용자를 만들 수 있습니다. Keystone에서 토큰을 검증할 때 Ceph Object Gateway는 인증된 사용자를 고려합니다.

Ceph Object Gateway는 인증에 OpenStack Keystone을 사용할지 여부를 제어합니다. 그러나 구성

되면 사용자를 인증하는 **OpenStack Keystone** 서비스입니다.

Keystone에서 작동하도록 **Ceph Object Gateway**를 구성하려면 **Keystone**에서 **nss db** 형식으로 요청을 생성하는 데 사용하는 **OpenSSL** 인증서를 변환해야 합니다.

추가 리소스

- 자세한 내용은 ***Red Hat Ceph Storage Object Gateway 가이드의 Ceph Object Gateway 및 OpenStack Keystone*** 섹션을 참조하십시오.

5장. 인프라 보안

이 가이드의 범위는 **Red Hat Ceph Storage**입니다. 그러나 적절한 **Red Hat Ceph Storage** 보안 계획에는 다음과 같은 사전 요구 사항을 고려해야 합니다.

5.1. 사전 요구 사항

- *Red Hat Enterprise Linux 8 Security Hardening Guide*.
- *SELinux 가이드를 사용하여 Red Hat Enterprise Linux 8*을 검토합니다.

5.2. 관리

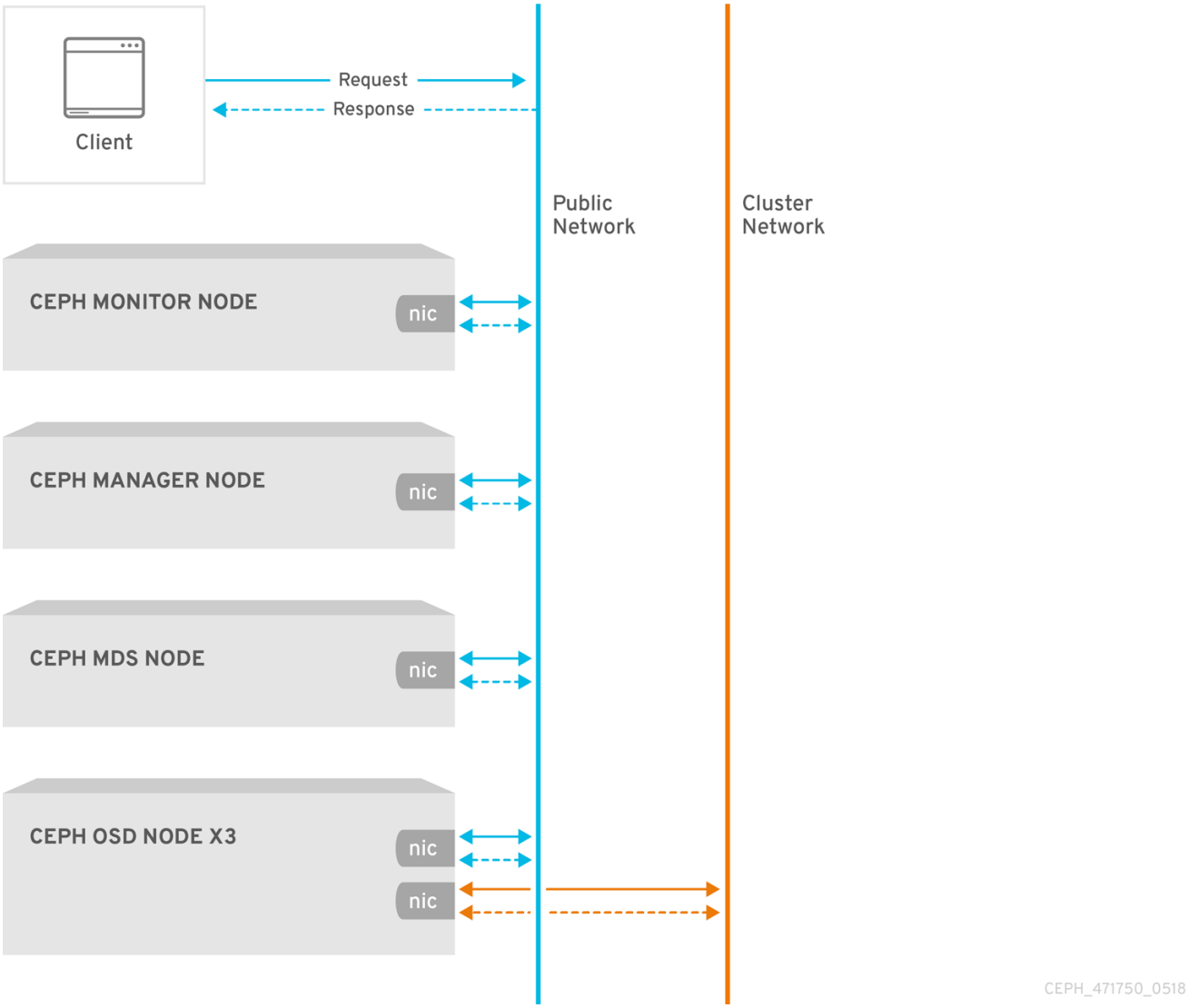
Red Hat Ceph Storage 클러스터 관리에는 명령줄 툴을 사용해야 합니다. **CLI** 툴에는 클러스터에 대한 관리자 액세스 권한에 대한 관리자 키가 필요합니다. 기본적으로 **Ceph**는 관리자 키를 **/etc/ceph** 디렉터리에 저장합니다. 기본 파일 이름은 **ceph.client.admin.keyring** 입니다. 클러스터에 대한 관리자 권한이 있는 사용자만 인증 키에 액세스할 수 있도록 인증 키를 보호하는 단계를 수행합니다.

5.3. 네트워크 통신

Red Hat Ceph Storage는 다음 두 가지 네트워크를 제공합니다.

- 공용 네트워크입니다.
- 클러스터 네트워크입니다.

모든 **Ceph** 데몬 및 **Ceph** 클라이언트에는 *스토리지 액세스 보안 영역의 일부인 공용 네트워크에 액세스해야 합니다*. 반면 **OSD** 데몬만 ***Ceph*** *클러스터 보안 영역의 일부인 클러스터 네트워크에 액세스해야 합니다*.



Ceph 구성에는 **public_network** 및 **cluster_network** 설정이 포함됩니다. 강화를 위해 **CIDR** 표기법을 사용하여 **IP** 주소와 넷마스크를 지정합니다. 클러스터에 여러 서브넷이 있는 경우 쉼표로 구분된 **IP** 주소 및 넷마스크 항목을 여러 개 지정합니다.

```
public_network = <public-network/netmask>[,<public-network/netmask>]
cluster_network = <cluster-network/netmask>[,<cluster-network/netmask>]
```

자세한 내용은 ***Red Hat Ceph Storage** 구성 가이드의 **Ceph** 네트워크 구성* 섹션을 참조하십시오.

5.4. 네트워크 서비스 강화

시스템 관리자는 **Red Hat Enterprise Linux 8 Server**에 **Red Hat Ceph Storage** 클러스터를 배포합니다. **SELinux**는 기본적으로 활성화되어 있으며 방화벽은 **SSH** 서비스 포트 **22** 를 제외한 모든 인바운드 트래픽을 차단하지만 다른 인증되지 않은 포트가 열려 있거나 불필요한 서비스를 사용하도록 해야 합니다.

각 서버 노드에서 다음을 실행합니다.

1. **firewalld** 서비스를 시작하고 부팅 시 실행되도록 활성화한 다음 실행 중인지 확인합니다.

```
# systemctl enable firewalld
# systemctl start firewalld
# systemctl status firewalld
```

2. 열려 있는 모든 포트의 인벤토리를 가져옵니다.

```
# firewall-cmd --list-all
```

새 설치에서 **sources:** 섹션은 특별히 열려 있는 포트가 없음을 나타내는 비어 있어야 합니다. **services** 섹션에는 **SSH** 서비스(및 포트 **22**)및 **dhcpv6-client** 가 활성화되었음을 나타내는 **ssh** 가 표시되어야 합니다.

```
sources:
services: ssh dhcpv6-client
```

3. **SELinux**가 실행 중이고 강제 작동하는지 확인합니다.

```
# getenforce
Enforcing
```

SELinux가 허용 인 경우 이를 **Enforcing** 으로 설정합니다.

```
# setenforce 1
```

SELinux가 실행 중이 아닌 경우 활성화합니다. 자세한 내용은 *Red Hat Enterprise Linux 8 Using SELinux Guide* 를 참조하십시오.

각 **Ceph** 데몬은 하나 이상의 포트를 사용하여 **Red Hat Ceph Storage** 클러스터의 다른 데몬과 통신합니다. 경우에 따라 기본 포트 설정을 변경할 수 있습니다. 일반적으로 관리자는 **Ceph Object Gateway** 또는 **ceph-radosgw** 데몬으로 기본 포트만 변경합니다.

표 **5.1. Ceph** 포트

TCP/UDP Port	데몬	설정 옵션
6789, 3300	**ceph-mon**	해당 없음
6800-7300	**ceph-osd**	**ms_bind_port_min** to **ms_bind_port_max**
6800-7300	**ceph-mgr**	**ms_bind_port_min** to **ms_bind_port_max**
6800	**ceph-mds**	해당 없음
8080	**ceph-radosgw**	**rgw_frontends**

Ceph Storage Cluster 데몬에는 **ceph-mon,ceph-mgr, ceph-osd** 가 포함됩니다. 이러한 데몬 및 해당 호스트는 **Ceph** 클러스터 보안 영역을 구성합니다. 이 영역은 강화 목적으로 자체 서브넷을 사용해야 합니다.

Ceph 클라이언트에는 **ceph-radosgw,ceph-mds,ceph-fuse,libcephfs,rbd,librbd, librados** 가 포함됩니다. 이러한 데몬 및 해당 호스트는 스토리지 액세스 보안 영역을 구성합니다. 이 영역은 강화 목적으로 자체 서브넷을 사용해야 합니다.

Ceph Storage Cluster 영역의 호스트에서 **Ceph** 클라이언트를 실행하는 호스트만 활성화하여 **Ceph Storage Cluster** 데몬에 연결하는 것이 좋습니다. 예를 들어 다음과 같습니다.

```
# firewall-cmd --zone=<zone-name> --add-rich-rule="rule family="ipv4" \
source address="<ip-address>/<netmask>" port protocol="tcp" \
port="<port-number>" accept"
```

< zone-name >을 영역 이름으로, **< ipaddress >**를 **IP** 주소로, **< netmask >**을 **CIDR** 표기법의 서브넷 마스크로, **< port-number >**를 포트 번호 또는 범위로 바꿉니다. 재부팅 후 변경 사항이 유지되도록 **--permanent** 플래그를 사용하여 프로세스를 반복합니다. 예를 들어 다음과 같습니다.

```
# firewall-cmd --zone=<zone-name> --add-rich-rule="rule family="ipv4" \
source address="<ip-address>/<netmask>" port protocol="tcp" \
port="<port-number>" accept" --permanent
```

5.5. REPORTING

Red Hat Ceph Storage는 **ceph-mgr** 데몬 플러그인, 즉 **RESTful API,** 대시보드 및 **Prometheus** 및

NetNamespace와 같은 기타 플러그인과 함께 기본 시스템 모니터링 및 보고를 제공합니다. Ceph는 collectd 및 소켓을 사용하여 설정, 구성 세부 정보 및 통계 정보를 검색하는 데 이 정보를 수집합니다.

시스템 관리자는 기본 시스템 동작 외에도 열려 있는 포트 및 연결을 각각 추적하도록 IP-Tables 또는 Conn NetNamespace 플러그인 구성 등 보안 문제에 대해 collectd 를 보고하도록 구성할 수 있습니다.

시스템 관리자는 런타임 시 구성 설정을 검색할 수도 있습니다. *런타임 시 Ceph 구성* 보기를 참조하십시오.

5.6. 감사 관리자 작업

시스템 보안의 중요한 측면은 클러스터에서 관리자 작업을 주기적으로 감사하는 것입니다. Red Hat Ceph Storage는 /var/log/ceph/ceph.audit.log 파일에 관리자 작업 내역을 저장합니다.

각 항목에는 다음이 포함됩니다.

- **timestamp:** 명령이 실행된 시기를 나타냅니다.
- 모니터 주소: 수정된 모니터를 식별합니다.
- 클라이언트 노드: 변경을 시작하는 클라이언트 노드를 식별합니다.
- 엔터티: 변경을 수행하는 사용자를 식별합니다.
- **command:** 실행된 명령을 식별합니다.

예를 들어 시스템 관리자가 nodown 플래그를 설정하고 설정 해제하면 감사 로그에 다음이 표시됩니다.

```
2021-08-13 21:50:28.723876 mon.reesi003 mon.2 172.21.2.203:6789/0 2404194 : audit [INF]
from='client.? 172.21.6.108:0/4077431892' entity='client.admin' cmd=[{"prefix": "osd set", "key":
"nodown"}]: dispatch
2021-08-13 21:50:28.727176 mon.reesi001 mon.0 172.21.2.201:6789/0 2097902 : audit [INF]
from='client.348389421 -' entity='client.admin' cmd=[{"prefix": "osd set", "key": "nodown"}]: dispatch
2021-08-13 21:50:28.872992 mon.reesi001 mon.0 172.21.2.201:6789/0 2097904 : audit [INF]
```

```
from='client.348389421 -' entity='client.admin' cmd='[{"prefix": "osd set", "key": "nodown"}]': finished
2021-08-13 21:50:31.197036 mon.mira070 mon.5 172.21.6.108:6789/0 413980 : audit [INF]
from='client.? 172.21.6.108:0/675792299' entity='client.admin' cmd=[{"prefix": "osd unset", "key":
"nodown"}]: dispatch
2021-08-13 21:50:31.252225 mon.reesi001 mon.0 172.21.2.201:6789/0 2097906 : audit [INF]
from='client.347227865 -' entity='client.admin' cmd=[{"prefix": "osd unset", "key": "nodown"}]: dispatch
2021-08-13 21:50:31.887555 mon.reesi001 mon.0 172.21.2.201:6789/0 2097909 : audit [INF]
from='client.347227865 -' entity='client.admin' cmd='[{"prefix": "osd unset", "key": "nodown"}]': finished
```

Ceph와 같은 분산 시스템에서는 한 인스턴스에서 작업을 시작하고 클러스터의 다른 노드로 전파될 수 있습니다. 작업이 시작되면 로그는 디스패치 임을 나타냅니다. 작업이 종료되면 로그는 완료된 것으로 표시됩니다.

예: entity='client.admin' 은 사용자가 **admin** 사용자임을 나타냅니다. **cmd=[{"prefix": "osd set": "key": "nodown"}]** 명령은 **admin** 사용자가 **ceph osd set nodown** 을 실행했음을 나타냅니다.

6장. 데이터 보존

Red Hat Ceph Storage는 사용자 데이터를 저장하지만 일반적으로 간접적인 방식으로 저장합니다. 고객 데이터 보존에는 Red Hat OpenStack Platform과 같은 다른 애플리케이션이 포함될 수 있습니다.

6.1. CEPH STORAGE 클러스터

신뢰할 수 있는 Autonomic Distributed Object Store 또는 RADOS라고 하는 Ceph Storage Cluster는 데이터를 풀 내 개체로 저장합니다. 대부분의 경우 이러한 오브젝트는 Ceph Block Device 이미지, Ceph Object Gateway 개체 또는 Ceph Filesystem 파일과 같은 클라이언트 데이터를 나타내는 원자 단위입니다. 그러나 librados 위에 빌드된 사용자 지정 애플리케이션은 풀에 바인딩되고 데이터도 저장할 수 있습니다.

organizations는 오브젝트 데이터를 저장하는 풀에 대한 액세스를 제어합니다. 그러나 Ceph Storage Cluster 사용자는 일반적으로 사용자가 아닌 Ceph 클라이언트입니다. 따라서 일반적으로 사용자는 Ceph Storage 클러스터 풀에서 직접 오브젝트를 작성, 읽기 또는 삭제할 수 없습니다.

6.2. CEPH 블록 장치

RADOS 블록 장치 또는 RBD라고도 하는 Ceph 블록 장치 인터페이스인 Red Hat Ceph Storage를 가장 많이 사용하며 가상 볼륨, 이미지 및 컴퓨팅 인스턴스를 생성하여 풀 내에 일련의 오브젝트로 저장합니다. Ceph는 이러한 오브젝트를 배치 그룹에 할당하고 클러스터 전체에서 OSD에 의사 무작위로 배포 또는 배치합니다.

Ceph 블록 장치 인터페이스를 사용하는 애플리케이션에 따라 일반적으로 Red Hat OpenStack Platform은 볼륨 및 이미지를 생성, 수정, 삭제할 수 있습니다. Ceph는 개별 오브젝트의 생성, 검색, 업데이트 및 삭제 작업을 처리합니다.

볼륨 및 이미지를 삭제하면 복구할 수 없는 방식으로 해당 오브젝트가 삭제됩니다. 그러나 복원 데이터 아티팩트는 덮어 쓰기 전까지 스토리지 미디어에 계속 상주할 수 있습니다. 또한 데이터는 백업 파일에 남아 있을 수 있습니다.

6.3. CEPH 파일 시스템

Ceph File System 인터페이스는 가상 파일 시스템을 생성하여 풀 내에 일련의 오브젝트로 저장합니다. Ceph는 이러한 오브젝트를 배치 그룹에 할당하고 클러스터 전체에서 OSD에 의사 무작위로 배포 또는 배치합니다.

일반적으로 **Ceph** 파일 시스템은 다음 두 개의 풀을 사용합니다.

- **metadata :** 메타데이터 풀은 일반적으로 **inode**로 구성된 **Ceph** 메타데이터 서버**(MDS)**의 데이터를 저장합니다. 즉, 파일 소유권, 권한, 생성 날짜 및 시간, 마지막으로 수정한 날짜 및 시간, 상위 디렉터리 등이 있습니다.

- **data:** 데이터 풀은 파일 데이터를 저장합니다. **Ceph**는 파일을 하나 이상의 오브젝트로 저장할 수 있으며 일반적으로 **Extent**와 같은 더 작은 파일 데이터 청크를 나타냅니다.

Ceph 파일 시스템 인터페이스(일반적으로 **Red Hat OpenStack Platform**)를 사용하는 애플리케이션에 따라 **Ceph** 파일 시스템에서 파일을 생성, 수정 및 삭제할 수 있습니다. **Ceph**는 파일을 나타내는 개별 오브젝트의 생성, 검색, 업데이트 및 삭제 작업을 처리합니다.

파일을 삭제하면 복구할 수 없는 방식으로 해당 오브젝트가 삭제됩니다. 그러나 복원 데이터 아티팩트는 덮어 쓰기 전까지 스토리지 미디어에 계속 상주할 수 있습니다. 또한 데이터는 백업 파일에 남아 있을 수 있습니다.

6.4. CEPH OBJECT GATEWAY

데이터 보안 및 보존 관점에서 **Ceph Object Gateway** 인터페이스는 **Ceph** 블록 장치 및 **Ceph Filesystem** 인터페이스와 비교할 때 몇 가지 중요한 차이점이 있습니다. **Ceph Object Gateway**는 사용자에게 서비스를 제공합니다. **Ceph Object Gateway**는 다음을 저장할 수 있습니다.

- 사용자 인증 정보**:** 일반적으로 사용자 인증 정보는 사용자 **ID**, 사용자 액세스 키 및 사용자 시크릿으로 구성됩니다. 또한, 제공된 경우 사용자의 이름과 이메일 주소를 포함할 수 있습니다. **Ceph Object Gateway**는 사용자가 시스템에서 명시적으로 삭제되지 않는 한 사용자 인증 데이터를 유지합니다.

- 사용자 데이터**:** 사용자 데이터는 일반적으로 사용자 또는 관리자가 생성한 버킷이나 컨테이너와 여기에 포함된 사용자 생성 **S3** 또는 **Swift** 오브젝트로 구성됩니다. **Ceph Object Gateway** 인터페이스는 각 **S3** 또는 **Swift** 오브젝트에 대해 하나 이상의 **Ceph Storage** 클러스터 오브젝트를 생성하고 해당 **Ceph Storage** 클러스터 오브젝트를 데이터 풀에 저장합니다. **Ceph**는 **Ceph Storage** 클러스터 개체를 할당하여 그룹을 배치하고 클러스터 전체에서 **OSD**에 의사 무작위로 배포 또는 배치합니다. **Ceph Object Gateway**는 버킷 또는 인덱스에 포함된 오브젝트의 인덱스를 저장하여 **S3** 버킷 또는 **Swift** 컨테이너의 콘텐츠 나열과 같은 서비스를 활성화할 수 있습니다. 또한 다중 파트 업로드를 구현할 때 **Ceph Object Gateway**는 **S3** 또는 **Swift** 오브젝트의 부분 업로드를 일시적으로 저장할 수 있습니다.

  사용자는 버킷 또는 컨테이너를 생성, 수정, 삭제하고, **Ceph Object Gateway**에 포함된 오브젝트를 삭제할 수 있습니다. **Ceph**는 **S3** 또는 **Swift** 오브젝트를 나타내는 개별 **Ceph Storage** 클

러스터 오브젝트의 생성, 검색, 업데이트 및 삭제 작업을 처리합니다.

S3 또는 **Swift** 오브젝트를 삭제하면 복구할 수 없는 방식으로 해당 **Ceph Storage** 클러스터 오브젝트가 삭제됩니다. 그러나 복원 데이터 아티팩트는 덮어 쓰기 전까지 스토리지 미디어에 계속 상주할 수 있습니다. 또한 데이터는 백업 파일에 남아 있을 수 있습니다.

- **logging: Ceph Object Gateway**는 사용자가 수행하려는 사용자 작업 및 실행된 작업 로그도 저장합니다. 이 데이터는 버킷 또는 컨테이너를 생성, 수정 또는 삭제한 사용자 또는 **S3** 버킷 또는 **Swift** 컨테이너에 있는 **S3** 또는 **Swift** 오브젝트에 대한 추적 기능을 제공합니다. 사용자가 데이터를 삭제하면 로깅 정보는 영향을 받지 않으며 시스템 관리자가 삭제하거나 만료 정책에 의해 자동으로 제거될 때까지 스토리지에 남아 있습니다.

버킷 라이프사이클

Ceph Object Gateway는 오브젝트 만료를 포함하여 버킷 라이프사이클 기능도 지원합니다. 일반 데이터 보호 규정과 같은 데이터 보존 규정은 관리자가 객체 만료 정책을 설정하고 다른 규정 준수 요인에 대해 사용자에게 공개하도록 요청할 수 있습니다.

다중 사이트

Ceph Object Gateway는 종종 다중 사이트 컨텍스트에 배포되며, 사용자가 한 사이트에 개체를 저장하고 **Ceph Object Gateway**는 다른 지리적 위치에서 오브젝트 복제본을 만들 수 있습니다. 예를 들어 주 클러스터가 실패하면 보조 클러스터가 작업을 다시 시작할 수 있습니다. 다른 예에서, 보조 클러스터는 에지 네트워크 또는 콘텐츠-배달 네트워크와 같은 다른 지리적 위치에 있을 수 있으므로 클라이언트는 응답 시간, 처리량 및 기타 성능 특성을 개선하기 위해 가장 가까운 클러스터에 액세스할 수 있습니다. 다중 사이트 시나리오에서는 관리자가 각 사이트에 보안 조치를 구현했는지 확인해야 합니다. 또한 데이터의 지리적 배포가 다중 사이트 시나리오에서 발생하는 경우 관리자는 데이터가 기술적 경계를 넘는 경우 규정적인 영향을 알고 있어야 합니다.

7장. 연방 정보 처리 표준 (FIPS)

Red Hat Ceph Storage는 Red Hat Enterprise Linux 7.6 또는 Red Hat Enterprise Linux 8.1 또는 Red Hat Enterprise Linux 8.2에서 실행할 때 FIPS 검증 암호화 모듈을 사용합니다.

- **Red Hat Enterprise Linux 시스템 설치 중 또는 그 이후에 FIPS 모드를 활성화합니다.**
  - 컨테이너 배포의 경우 *Red Hat Enterprise Linux 8 Security Hardening Guide* 의 지침을 따르십시오.

추가 리소스

- **FIPS 검증에 대한 최신 정보를 확인하려면 *미국 정부 표준을* 참조하십시오.**

8장. 요약

이 문서에서는 **Red Hat Ceph Storage**의 보안을 일반적으로 소개합니다. 추가 지원을 받으려면 **Red Hat Ceph Storage** 컨설팅 팀에 문의하십시오.