Red Hat Ceph Storage 7

数据安全性和强化指南

Red Hat Ceph Storage 数据安全行和强化指南

Last Updated: 2024-06-14

Red Hat Ceph Storage 7 数据安全性和强化指南

Red Hat Ceph Storage 数据安全行和强化指南

法律通告

摘要

本文档为 Ceph Storage 集群及其客户端提供数据安全性和强化信息。 红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 信息

目录

第 1 章 数据安全简介

安全性是非常重要的，应该密切关注任何红帽 Ceph 存储部署的安全性。数据泄露和停机时间昂贵且难以管理，法律可能需要传递审计和合规性流程，并且项目预计其数据的某种程度和安全性。本文档介绍了红帽 Ceph 存储的安全性的一般介绍，以及红帽在支持系统的安全性方面发挥的作用。

1.1. 前言

本文档为强化 Red Hat Ceph Storage 安全性提供建议和良好的实践信息，重点在于使用 **cephadm** 进行 Red Hat Ceph Storage 部署。虽然遵循本指南中的说明将有助于增强您的环境的安全性，但我们不保证遵循这些建议的安全性或合规。

1.2. RED HAT CEPH STORAGE 简介

红帽 Ceph 存储(RHCS)是一种高度可扩展且可靠的对象存储解决方案，它通常与 OpenStack 等云计算解决方案进行部署，如单机存储服务或使用 iSCSI 等接口作为网络附加存储。

所有 RHCS 部署均由一个存储集群组成，通常被称为 Ceph 存储集群或 RADOS（可靠的分布式对象存储），它们由三种类型的守护进程组成：

- **Ceph Monitors(ceph-mon)：** Ceph 监视器提供一些关键功能，如建立关于集群状态的协议，以及维护集群状态的历史记录，如 OSD 是否启动并运行并在集群中，为其提供通过哪些客户端和读取数据提供池列表，以及为客户端和 Ceph 存储群集守护进程提供身份验证。

- **Ceph 管理器(ceph-mgr)：** Ceph 管理器守护进程跟踪 PG 在 Ceph OSD 之间分布的对等点、放置组状态的历史记录，以及 Ceph 集群的指标。它们也提供供外部监控和管理系统的接口。

- **Ceph OSD(ceph-osd)：** Ceph Object Storage Daemons(OSD)存储和提供客户端数据，将客户端数据复制到次要 Ceph OSD 守护进程，跟踪并报告 Ceph monitor 在邻居 OSD 的运行状况上，避免在集群大小更改时从故障和回填数据中恢复。

所有 RHCS 部署都会在 Ceph 存储集群或 RADOS（Reliable Autonomous Distributed Object Store）中存储最终用户数据。通常，用户**不**直接与 Ceph Storage 集群交互，而是与 Ceph 客户端交互。

主要 Ceph Storage 集群客户端有三个：

- **Ceph 对象网关(radosgw)** ：Ceph 对象网关-也称为 RADOS 网关、 **radosgw** 或 **rgw**-- 提供具有 RESTful API 的对象存储服务。Ceph 对象网关代表其客户端在 Ceph 存储集群或 RADOS 中存储数据。

- **Ceph 块设备(rbd)** ：Ceph 块设备通过内核 RBD(**krbd**)向 Linux 内核提供写时复制、精简配置且可克隆虚拟块设备，或者与 OpenStack 等云计算解决方案（通过 **librbd** ）提供 OpenStack。

- **Ceph 文件系统(cephfs)** ：Ceph 文件系统由一个或多个元数据服务器(**mds**)组成，它将 fileystem 作为对象存储在 Ceph Storage 集群中。Ceph 文件系统可通过内核客户端、FUSE 客户端或通过 **libcephfs** 库挂载，用于 OpenStack 等云计算解决方案。

其他客户端包括 **librados**，开发人员可以创建自定义应用与 Ceph 存储集群交互，以及命令行界面客户端，以供管理使用。

1.3. 支持软件

Red Hat Ceph Storage 安全性的一个重要方面是交付具有安全内置前期且红帽支持随时间的解决方案。红帽使用 Red Hat Ceph Storage 采取的具体步骤包括：

- 保持上游关系和社区参与，以帮助从一开始专注于安全性。
- 根据安全和性能跟踪记录选择和配置软件包。
- 从相关源代码构建二进制文件（而不是只接受上游构建）。
- 应用一系列检查和质量保证工具，以防止大量潜在安全问题和回归问题。
- 数字签名所有已发布的软件包，并通过经过加密验证的分发频道进行发布。
- 提供单一统一的补丁和更新分发机制。

此外，红帽还维护了一个专门的安全团队，针对我们的产品分析威胁和漏洞，并通过客户门户网站提供相关建议和更新。这个团队决定哪些问题很重要，而不是与大多数理论问题相关的问题。红帽产品安全团队在维护了专业技术方面，并对与订阅产品关联的上游社区做出了大量贡献。红帽安全公告 （红帽安全公告）的一个主要部分提供了影响红帽解决方案的安全缺陷通知 - 通常会在漏洞首次发布之日提供相关的补丁程序。

第 2 章 安全风险和漏洞管理

Red Hat Ceph Storage 通常与云计算解决方案一起部署，因此可以考虑 Red Hat Ceph Storage 部署作为一个大规模部署中的一个组件会很有帮助。这些部署通常具有共享的安全问题，在本指南称为*安全区（Security Zones）*。威胁者和向量会按照其动机和对资源的访问进行分类。目的是让您了解各个区域的安全顾虑，具体取决于您的目标。

2.1. 威胁者

威胁者是一个抽象的、用于指代您可能需要防御的一类行为的方式。能够使用更加强大的安全控制，这是成功攻击缓解和防止所需的安全控制。安全性是根据要求进行的平衡便利、防御和成本方面的问题。在某些情况下，可能无法确保 Red Hat Ceph Storage 部署免受此处描述的所有威胁行为。在部署 Red Hat Ceph Storage 时，您必须决定部署和使用余下的平衡。

作为风险评估的一部分，您还必须考虑您存储和任何可访问资源的数据类型，因为这将影响某些参与者。然而，即使您的数据对威胁威胁者没有吸引力，它们也可能很吸引于您的计算资源。

- **Nation-State Actors:** 这是最强大的攻击行为。Nation-state actors 可以使用巨大的资源来进行攻击。他们拥有超越其他任何参与者的功能。在没有严格控制（包括人工和技术）的情况下，很能防御此类的攻击。

- **主要犯罪组织：** 这个类代表有强大能力和金融资源的攻击者。他们能够为攻击方法的开发和研究提供大量资金。近年来，一些兴起的组织（例如 Russian Business Network，它是一个大型网络犯罪组织），已证明网络攻击如何成为一种商品。工业间谍通常属于这类严重犯罪组织。

- **高能力组：** 这通常指"骇客组织"，它们可能并没有强大的资金支持，但会对服务提供商和云环境操作者员造成严重威胁。

- **有动力的个人：** 这些攻击者会包括不同的人员，例如恶意员工、受负面影响力的客户或小的工业间谍。

- **Script Kiddies:** 这些攻击者不针对特定的机构，而是运行自动化漏洞扫描和利用漏洞。它们通常看似微不足道，但可能会对一个机构构成声誉风险。

以下实践可帮助缓解上述发现的一些风险：

- **安全更新：** 您必须考虑底层物理基础架构的端到端安全，包括网络、存储和服务器硬件。这些系统需要自己的安全强化实践。对于 Red Hat Ceph Storage 部署，您应该有一个计划定期测试和部署安全更新。

- **产品更新：** 红帽建议在产品可用时运行产品更新。通常每 6 周发布更新（偶尔更频繁）。红帽努力在主版本内完全兼容点发行版本和 z-stream 版本，以便不需要额外的集成测试。

- **访问管理：** 访问权限管理包括身份验证、授权和核算。身份验证是验证用户身份的过程。授权是向经过身份验证的用户授予权限的过程。记帐(accounting)是跟踪用户执行操作的过程。当向用户授予系统访问权限时，请应用 *最小特权的原则*，仅授予用户实际需要的粒度系统特权。这种方法还可以帮助缓解系统管理员中恶意执行者和排字错误的风险。

- **管理内部：** 您可以通过应用谨慎分配基于角色的访问控制（最低访问权限）、在内部接口上使用加密以及使用身份验证/授权安全（如集中式身份管理）来缓解恶意人员的威胁。您还可以考虑额外的非技术选项，例如将职责分离和不定期的作业角色轮转。

2.2. 安全区

安全区由用户在系统中共享共同信任要求的用户、应用程序、服务器或网络组成。通常，它们共享相同的

身份验证和授权要求和用户。虽然您可以进一步重新定义这些区域定义，但本指南指的是四个不同的安全区，其中 3 个形成部署安全强化的 Red Hat Ceph Storage 集群所需的最小级别。这些安全区被列为从至少被信任到最受信任：

- **公共安全区：**公共安全区是云基础架构的一个完全不受信任的区域。它可以将互联网指代为整个或只是 Red Hat OpenStack 部署外部的网络。遍历此区域的任何具有保密性或完整性要求的数据都应使用成组控制（如加密）加以保护。**不应**将公共安全区与 Ceph Storage 集群前端或客户端网络混淆，该网络在 RHCS 中称为 **public_network**，通常 **不属于** 公共安全区或 Ceph 客户端安全区的一部分。

- **Ceph Client Security Zone：**通过 RHCS，Ceph 客户端安全区域指的是访问 Ceph 客户端的网络，如 Ceph 对象网关、Ceph 块设备、Ceph 文件系统或 **librados**。Ceph 客户端安全区通常位于防火墙后，将其与公共安全区分离。但是，Ceph 客户端并不总是受到公共安全区的保护。可以在公共安全区域中公开 Ceph 对象网关的 S3 和 Swift API。

- **Storage Access Security Zone：**存储访问安全区指的是为 Ceph 客户端提供 Ceph Storage 集群访问权限的内部网络。在这里，我们使用"存储访问安全区（storage access security zone）"，以便与 OpenStack 平台安全性和强化指南中使用的术语一致。存储访问安全区包括 Ceph Storage 集群的前端或客户端网络，它们被称为 RHCS 中的 **public_network**。

- **Ceph 集群安全性区域：**Ceph 集群安全区指的是内部网络，为 Ceph 存储集群的 OSD 守护进程提供复制、心跳、回填和恢复的网络通信。Ceph 集群安全区包含 Ceph Storage 集群的后端网络，该网络在 RHCS 中称为 **cluster_network**。

这些安全区可以单独映射，或者合并以代表给定 RHCS 部署中的大多数可能信任的区域。安全区应根据您的特定 RHCS 部署拓扑进行映射。区域及其信任要求会因 Red Hat Ceph Storage 在独立容量中运行，或为公共、私有或混合云提供。

有关这些安全区的可视化表示，请参阅 安全优化架构。

其它资源

- 如需了解更多详细信息，请参阅 *Red Hat Ceph Storage Data Security and Hardening Guide* 中的 *Network* communications 部分。

2.3. 连接安全区（CONNECTING SECURITY ZONES）

必须仔细配置跨多个安全区（具有不同信任级别或身份验证要求）的组件。这些连接通常是网络架构的弱点，并且应始终配置为满足所连接任何区域的最高信任级别。在很多情况下，连接的区的安全性控制应该是主要问题，因为攻击的可能性较高。区域满足对于攻击者向部署中更敏感的部分迁移或目标的攻击者提供了机会。

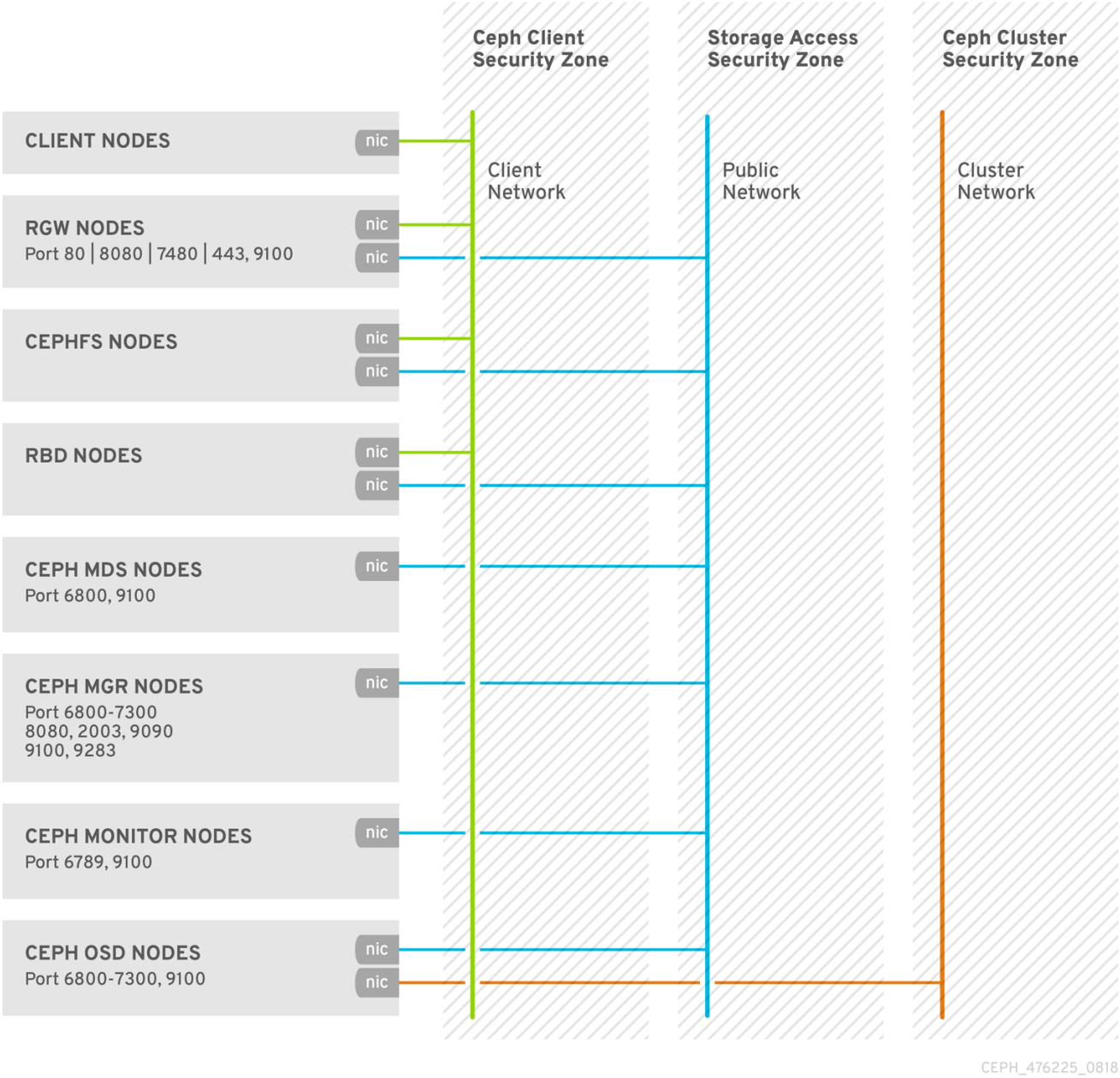
在某些情况下，Red Hat Ceph Storage 管理员可能需要考虑在比集成点所在的任何区域以外的标准安全集成点。例如，Ceph Cluster Security Zone 可以轻松地与其他安全区隔离，因为没有理由将它连接到其他安全区。相反，Storage Access Security Zone 必须提供对 Ceph 监控节点上的 **6789** 端口的访问，并在 Ceph OSD 节点上提供端口 **6800-7300**。但是，端口 **3000** 应该专用于 Storage Access Security 区域，因为它提供了对 Ceph 管理员公开的 Ceph Grafana 监控信息的访问。Ceph 客户端安全区中的 Ceph 对象网关需要访问 Ceph 集群安全性区的监控器（端口 **6789**）和 OSD（端口 **6800-7**300），并且可能会将其 S3 和 Swift API 公开给公共安全区，如通过 HTTP 端口 **80** 或 HTTPS 端口 **443** ；但是，它可能需要限制访问 admin API 的访问。

因为 Red Hat Ceph Storage 的设计，分离安全区比较困难。由于核心服务通常至少跨越两个区域，因此在将安全控制应用到它们时，必须考虑特殊考虑。

2.4. 安全优化架构

Red Hat Ceph Storage 集群的守护进程通常在防火墙后被隔离的节点上运行，这使其比较简单来保护 RHCS 集群。

与之相反，Red Hat Ceph Storage 客户端（如 Ceph 块设备(**rbd**)、Ceph Filesystem(**cephfs**)和 Ceph 对象网关(**rgw**)访问 RHCS 存储集群，但将其服务公开给其他云计算平台。



第 3 章 加密和密钥管理

Red Hat Ceph Storage 集群通常位于自己的网络安全区中，特别是在使用私有存储集群网络时使用。

重要

如果攻击者获得公共网络上的 Ceph 客户端访问权限，则安全区分离可能不足以实现保护目的。

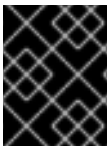
有些情况下，需要确保网络流量的保密性或完整性，Red Hat Ceph Storage 使用加密和密钥管理，包括：

- SSH
- SSL 终止
- Messenger v2 协议
- Transit 中的加密
- 静止加密（Encryption at Rest）
- 密钥轮转

3.1. SSH

Red Hat Ceph Storage 集群中的所有节点都使用 SSH 作为部署集群的一部分。这意味着每个节点：

- **cephadm** 用户具有无密码的 root 特权。
- SSH 服务已启用，并使端口 22 处于打开状态。
- **cephadm** 用户的公共 SSH 密钥的一个副本。



重要

任何有权访问 **cephadm** 用户的人都可以扩展，可以在 Red Hat Ceph Storage 集群内的任何节点上以 **root** 身份运行命令。

其它资源

- 如需更多信息，请参阅 *Red Hat Ceph Storage 安装指南中的 **cephadm** 如何工作* 部分。

3.2. SSL 终止

Ceph 对象网关可以和 HAProxy 和 **keepalived** 一起部署，以实现负载平衡和故障转移。对象网关 Red Hat Ceph Storage 版本 2 和 3 使用 Civetweb。Civetweb 的早期版本不支持 SSL 及更新的版本，但有一些性能限制。

Red Hat Ceph Storage 版本 5 使用 Beast。您可以将 Beast 前端 web 服务器配置为使用 OpenSSL 库来提供传输层安全性(TLS)。

当使用 HAProxy 和 **keepalived** 终止 SSL 连接时，HAProxy 和 **keepalived** 组件使用加密密钥。

当使用 HAProxy 和 **keepalived** 终止 SSL 时，负载均衡器和 Ceph 对象网关之间的连接 **不会**加密。

详情请参阅 *为 Beast 配置 SSL 和 HAProxy 和 keepalived*。

3.3. MESSENGER V2 协议

Ceph 的 on-wire 协议 **msgr2** 的第二个版本具有以下功能：

- 安全模式通过网络加密所有数据。
- 身份验证有效负载的封装改进，支持以后集成新的身份验证模式。
- 功能公告和协商的改进。

Ceph 守护进程绑定到多个端口，允许旧旧 v1- 兼容新的 v2 兼容 Ceph 客户端，以连接同一存储集群。Ceph 客户端或其他 Ceph 守护进程连接到 Ceph Monitor 守护进程将先尝试使用 **v2** 协议（如果可能），但若不可能，则使用旧的 **v1** 协议。默认情况下，启用 messenger 协议 **v1** 和 **v2**。新的 v2 端口为 3300，旧的 v1 端口默认为 6789。

messenger v2 协议有两个配置选项，用于控制是否使用 v1 还是 v2 协议：

- **ms_bind_msgr1** - 这个选项控制守护进程是否绑定到 v1 协议的端口，默认为 **true**。
- **ms_bind_msgr2** - 这个选项控制守护进程是否绑定到 v2 协议的端口，默认为 **true**。

同样，两个选项根据使用的 IPv4 和 IPv6 地址进行控制：

- **ms_bind_ipv4** - 此选项控制守护进程是否绑定到 IPv4 地址；默认为 **true**。
- **ms_bind_ipv6** - 这个选项控制守护进程是否绑定到 IPv6 地址，默认为 **true**。

注意

绑定到多个端口的功能已缩减了双栈 IPv4 和 IPv6 支持的方法。

msgr2 协议支持两种连接模式：

- **crc**
  - 当使用 **cephx** 建立连接时，提供强大的初始身份验证。
  - 提供 **crc32c** 完整性检查，以防止比特反转（bit flipping）攻击。
  - 不能提供对恶意的中间人攻击提供保护。
  - 不能阻止对认证后的网络流量进行窃听。
- **secure**
  - 当使用 **cephx** 建立连接时，提供强大的初始身份验证。
  - 提供所有认证后的网络流量的完全加密。
  - 提供加密完整性检查。

默认模式是 **crc**。

Ceph 对象网关加密

另外，Ceph 对象网关支持使用其 S3 API 与客户提供的密钥进行加密。

重要

为了遵守法规合规性标准要求传输严格的加密，管理员**必须**通过客户端侧加密部署 Ceph 对象网关。

Ceph 块设备加密

系统管理员使用 **dm_crypt** 将 Ceph 块设备卷集成为 Red Hat OpenStack Platform 13 **必须** 加密 Ceph 块设备卷，以确保 Ceph 存储集群中的在线加密。

重要

为了遵守法规合规性标准要求传输严格的加密，系统管理员**必须**使用 **dmcrypt** 用于 RBD Cinder，以确保 Ceph 存储集群中的在线加密。

其他资源

- 如需了解更多详细信息，*请参阅 Red Hat Ceph Storage 配置指南中的 连接模式配置选项*。

3.4. 传输中加密（ENCRYPTION IN TRANSIT）

从 Red Hat Ceph Storage 5 及之后的版本开始，默认启用通过网络的所有 Ceph 流量加密，并引入 messenger 版本 2 协议。mesenger v2 的**安全**模式设置加密 Ceph 守护进程和 Ceph 客户端之间的通信，从而为您提供端到端加密。

您可以使用 **ceph config dump** 命令（**netstat -lp | grep ceph-osd** 命令）检查 messenger v2 协议的加密，或者在 v2 端口上验证 Ceph 守护进程。

其他资源

- 有关 *SSL 终止* 的详情，请查看 SSL 终止。
- 有关 *S3 API 加密的详情，请查看 S3 服务器端加密*。

3.5. MESSENGER V2 协议的压缩模式

messenger v2 协议支持压缩功能。默认情况下不启用压缩。

建议不要压缩和加密相同的消息，因为对等点之间的消息级别会减少。如果启用了加密，将忽略启用压缩的请求，直到配置选项 **ms_osd_compress_mode** 设为 **true**。

它支持两种压缩模式：

- **force**
  - 在多可用区部署中，在 OSD 之间压缩复制消息会节省延迟。
  - 在公有云中，将消息大小最小化，从而降低云提供商的网络成本。
  - 带有 NVMe 的公有云上的实例提供与设备带宽相关的低网络带宽。不能提供对恶意的中间人攻击提供保护。

- **none**
  - 在不压缩的情况下传输消息。

若要确保启用消息的压缩，请运行 **debug_ms** 命令并检查连接的一些调试条目。另外，您可以运行 **ceph config get** 命令，获取网络信息的不同配置选项的详细信息。

其他资源

- 如需了解更多详细信息，请参阅 *Red Hat Ceph Storage 配置指南中的 压缩模式配置选项*。

3.6. 静止加密（ENCRYPTION AT REST）

Red Hat Ceph Storage 在一些情况下支持对静止数据（data at rest）进行加密：

1. **Ceph Storage Cluster：** Ceph Storage 集群支持对 Ceph OSD 的 Linux 统一密钥设置或 LUKS 加密，以及对应的日志、write-ahead 日志和元数据数据库。在这种情况下，Ceph 会加密所有客户端是否是 Ceph 块设备、Ceph Filesystem 还是在 **librados** 上构建的自定义应用的数据。

2. **Ceph 对象网关：** Ceph 存储集群支持客户端对象加密。当 Ceph 对象网关加密对象时，它们独立于 Red Hat Ceph Storage 集群进行加密。此外，传输的数据也以加密的形式在 Ceph 对象网关和 Ceph 存储集群之间。

Ceph Storage 集群加密

Ceph 存储集群支持加密 Ceph OSD 中存储的数据。Red Hat Ceph Storage 可通过指定 **dmcrypt** 来加密带有 **lvm** 的逻辑卷。这时由 **ceph-volume** 调用的 **lvm**，加密 OSD 的逻辑卷而不是它的物理卷。它可以像使用相同 OSD 密钥的分区一样对非 LVM 设备进行加密。加密逻辑卷可以实现更大的灵活性。

Ceph 使用 LUKS v1 而不是 LUKS v2，因为 LUKS v1 在 Linux 发行版之间拥有广泛的支持。

在创建 OSD 时，**LVM** 将生成一个 secret 密钥，并通过 **stdin** 在 JSON 有效负载中安全地将密钥传递给 Ceph Monitor。加密密钥的属性名称为 **dmcrypt_key**。

重要

系统管理员必须明确启用加密。

默认情况下，Ceph 不会加密 Ceph OSD 中存储的数据。系统管理员必须启用 **dmcrypt** 来加密 Ceph OSD 中存储的数据。使用 Ceph 编排器服务规格文件将 Ceph OSD 添加到存储集群时，在 文件中设置以下选项以加密 Ceph OSD：

示例

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

注意

LUKS 和 **dmcrypt** 仅针对静态数据的地址加密，而不是对传输中的数据进行加密。

Ceph 对象网关加密

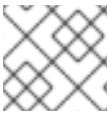
Ceph 对象网关支持使用其 S3 API 与客户提供的密钥进行加密。在使用客户提供的密钥时，S3 客户端会传递加密密钥以及每个请求来读取或写入加密数据。客户负责管理这些密钥。客户必须记住用于加密每个对象的 Ceph 对象网关的关键是什么。

其它资源

- 详情请参阅 *Red Hat Ceph Storage Developer Guide* 中的 S3 API 服务器端加密。

3.7. 启用密钥轮转

Ceph 集群中的 Ceph 和 Ceph 对象网关守护进程具有 secret 密钥。此密钥用于连接到集群并与集群进行身份验证。您可以使用密钥轮转功能，在活跃的 Ceph 集群中更新活跃的安全密钥，从而尽量减少服务中断。



注意

活跃的 Ceph 集群包括 Ceph 客户端角色中的节点，以及并行密钥更改。

密钥轮转有助于确保满足当前行业和安全合规要求。

先决条件

- 一个正在运行的 Red Hat Ceph Storage 集群。
- 具有 **admin** 特权的用户。

步骤

1. 轮转密钥：

   语法

   ```
   ceph orch daemon rotate-key NAME
   ```

   示例

   ```
   [ceph: root@host01 /]# ceph orch daemon rotate-key mgr.ceph-key-host01
   Scheduled to rotate-key mgr.ceph-key-host01 on host 'my-host-host01-installer'
   ```

2. 如果使用 MDS、OSD 或 MGR 以外的守护进程，重启守护进程以切换到新密钥。MDS、OSD 和 MGR 守护进程不需要守护进程重启。

   语法

   ```
   ceph orch restart SERVICE_TYPE
   ```

   示例

   ```
   [ceph: root@host01 /]# ceph orch restart rgw
   ```

第 4 章 身份和访问权限管理

Red Hat Ceph Storage 提供身份和访问管理：

- Ceph Storage 集群用户访问
- Ceph 对象网关用户访问
- Ceph 对象网关 LDAP/AD 身份验证
- Ceph 对象网关 OpenStack Keystone 身份验证

4.1. CEPH STORAGE 集群用户访问

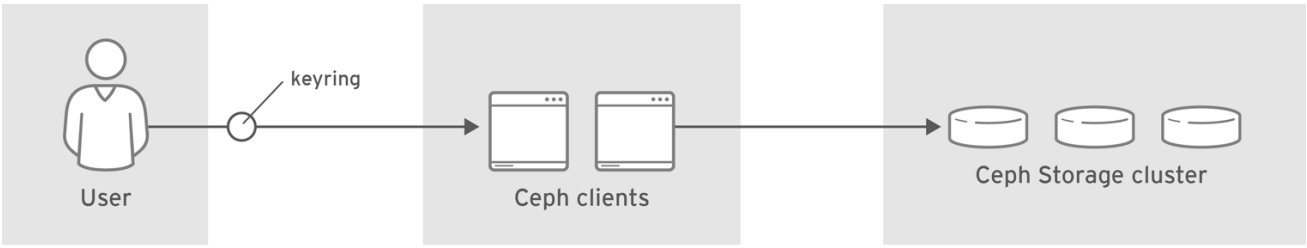
为了识别用户和防止中间人攻击，Ceph 提供其 **cephx** 身份验证系统来验证用户和守护进程。有关 **cephx** 的更多详细信息，请参阅 *Ceph 用户管理*。

重要

cephx 协议**不会考虑**传输中加密或静止加密。

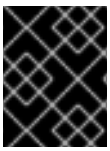
cephx 使用共享密钥来进行身份验证，这意味着客户端和服务器均有客户端的机密密钥的副本。身份验证协议使得双方能够为每个方证明其各自具有密钥副本，而无需实际发现。这提供了 mutual 身份验证，这意味着集群是确保用户具有 secret 密钥，用户则确保集群具有 secret 密钥的副本。

用户是个人或系统参与者，如使用 Ceph 客户端与红帽 Ceph Storage 集群守护进程交互的应用程序。



CEPH_459704_1017

Ceph 使用默认启用的身份验证和授权运行。Ceph 客户端可以指定用户名和包含指定用户密钥的密钥环，通常是使用命令行。如果未提供用户和密钥环作为参数，Ceph 将使用 **client.admin** 管理用户作为默认值。如果未指定密钥环，Ceph 将使用 Ceph 配置中的 **keyring** 设置查找密钥环。



重要

要强化 Ceph 集群，密钥环**只应该**使当前用户和 **root** 具有读写权限。包含 **client.admin** 管理用户的密钥环必须仅限于 **root** 用户。

有关配置 Red Hat Ceph Storage 集群以使用身份验证的详情，请参阅 Red Hat Ceph Storage 7 的 *配置指南*。更具体地说，请参阅 *Ceph 身份验证配置*。

4.2. CEPH 对象网关用户访问

Ceph 对象网关提供 RESTful 应用程序编程接口(API)服务，提供自己的用户管理，以进行身份验证并授权用户访问包含用户数据的 S3 和 Swift API。身份验证包括：

- **S3 User：** S3 API 用户的用户的访问密钥和 secret。
- **Swift 用户：** Swift API 用户访问密钥和 secret。Swift 用户是 S3 用户的子用户。删除 S3 'parent' 用户将删除 Swift 用户。
- **管理用户：** 管理 API 用户的访问密钥和 secret。应创建管理用户，因为管理用户将能够访问 Ceph 管理员 API 并执行其功能，如创建用户，并为他们授予他们访问 bucket 或容器及其对象的权限。

Ceph 对象网关在 Ceph 存储集群池中存储所有用户身份验证信息。更多信息可以存储关于用户的信息，包括名称、电子邮件地址、配额和使用。

如需了解更多详细信息，请参阅 用户管理和创建用户 。

4.3. CEPH 对象网关 LDAP 或 AD 身份验证

红帽 Ceph 存储支持使用轻量级目录访问协议(LDAP)服务器来验证 Ceph 对象网关用户。当配置为使用 LDAP 或 Active Directory(AD)时，Ceph Object Gateway defers 到 LDAP 服务器，以验证 Ceph 对象网关的用户。

Ceph 对象网关控制是否使用 LDAP。但是，配置完成后，它是负责验证用户的 LDAP 服务器。

为了保护 Ceph 对象网关和 LDAP 服务器之间的通信，红帽建议使用 LDAP 安全或 LDAPS 部署配置。

重要

在使用 LDAP 时，请确保对 **rgw_ldap_secret = *PATH_TO_SECRET_FILE*** secret 文件的访问是安全的。

4.4. CEPH 对象网关 OPENSTACK KEYSTONE 身份验证

红帽 Ceph 存储支持使用 OpenStack Keystone 验证 Ceph 对象网关 Swift API 用户。Ceph 对象网关可以接受 Keystone 令牌，对用户进行身份验证并创建对应的 Ceph 对象网关用户。当 Keystone 验证令牌时，Ceph 对象网关会认为用户通过身份验证。

Ceph 对象网关控制是否使用 OpenStack Keystone 进行身份验证。但是，配置完成后，它是负责对用户进行身份验证的 OpenStack Keystone 服务。

配置 Ceph 对象网关以搭配 Keystone 使用时，需要将 Keystone 用于创建请求的 OpenSSL 证书转换为 **nss db** 格式。

其它资源

- 如需更多信息，请参阅 *Red Hat Ceph Storage 对象网关指南中的 Ceph 对象网关和 OpenStack Keystone* 部分。

第 5 章 基础架构安全性

本指南范围是 Red Hat Ceph Storage。但是，正确的红帽 Ceph 存储安全计划需要考虑以下先决条件：

先决条件

- 请参阅红帽客户门户网站中的 Red Hat Enterprise Linux 产品文档中的 *使用 SELinux 指南*。
- 请参阅红帽客户门户网站中的 Red Hat Enterprise Linux 产品文档中的 *安全强化指南*。

5.1. 管理

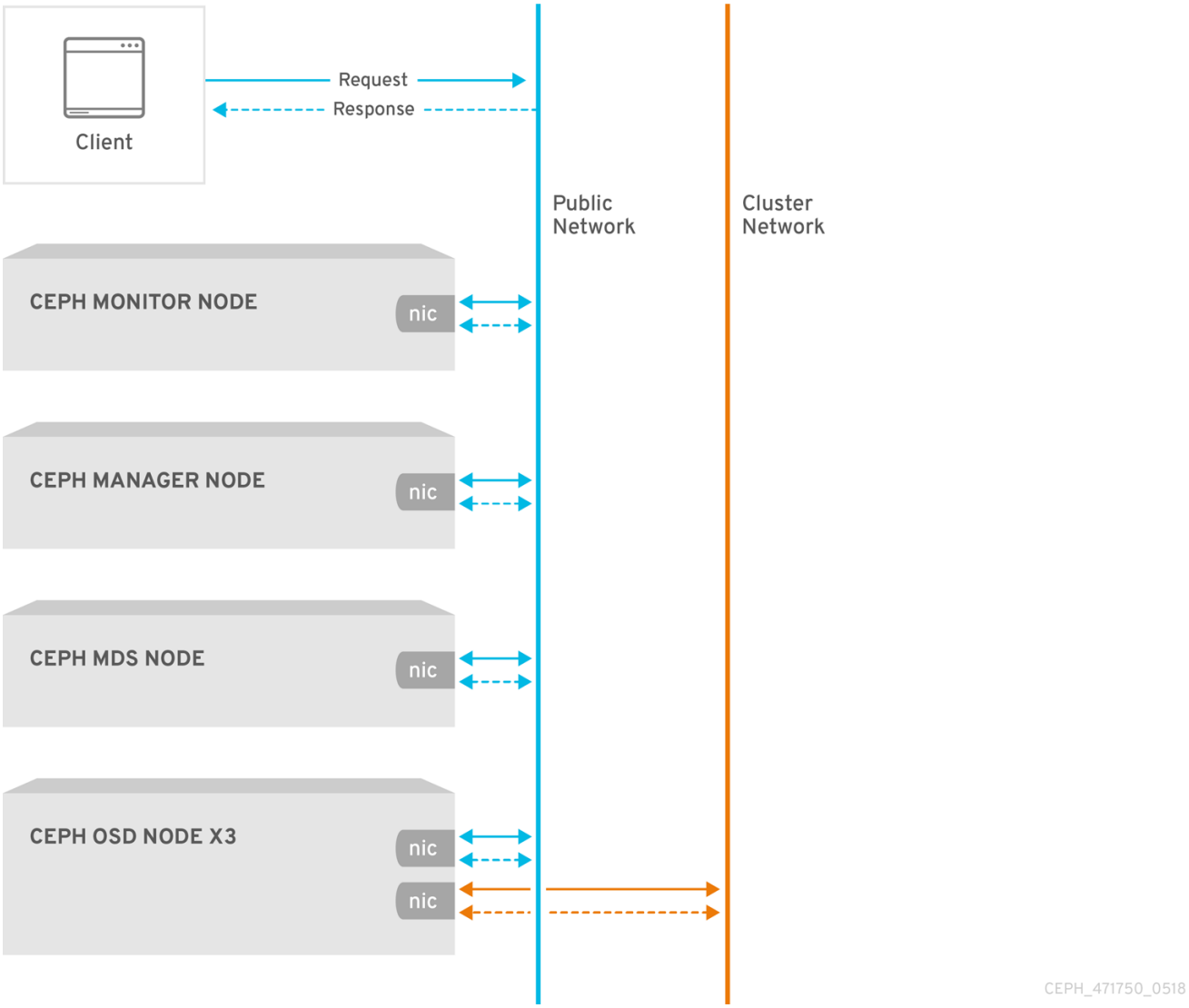
管理红帽 Ceph 存储集群涉及使用命令行工具。CLI 工具需要管理员密钥才能获得集群的访问权限。默认情况下，Ceph 将管理员密钥存储在 **/etc/ceph** 目录中。默认文件名是 **ceph.client.admin.keyring**。采取步骤来保护密钥环，以便只有具有管理特权的用户才能访问密钥环。

5.2. 网络通信

Red Hat Ceph Storage 提供两个网络：

- 公共网络。
- 一个集群网络。

所有 Ceph 守护进程和 Ceph 客户端都需要访问公共网络，该网络是*存储访问安全区*的一部分。相反，仅 OSD 守护进程需要访问集群网络（这是 *Ceph 集群安全区*的一部分）。



Ceph 配置包含 **public_network** 和 **cluster_network** 设置。为了强化目的，使用 CIDR 标记指定 IP 地址和子网掩码。如果集群有多个子网，请指定多个以逗号分隔的 IP 地址和子网掩码条目。

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

详情请参阅 *Red Hat Ceph Storage 配置指南中的 Ceph 网络配置* 部分。

5.3. 强化网络服务

系统管理员在 Red Hat Enterprise Linux 8 服务器上部署红帽 Ceph 存储集群。SELinux 默认是开启的，防火墙会阻止除 SSH 服务端口 **22** 之外的所有入站流量；但是，您**需要**确定系统确实是这样配置的，以确定没有打开未验证的端口或没有启用不需要的服务。

在每个服务器节点上，执行以下操作：

1. 启动 **firewalld** 服务，启用它在引导时运行并确保它正在运行：

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

2. 获取所有开放端口的清单。

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

在新安装中，**sources:** 部分应为空，表示没有打开任何端口。**services** 部分应指示 **ssh** 表示 SSH 服务（以及端口 **22**）和 **dhcpv6-client** 已启用。

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

3. 确保 SELinux 正在运行并设置为 **Enforcing**。

```
# getenforce
Enforcing
```

如果 SELinux 为 **Permissive**，则将其设置为 **Enforcing** 模式。

```
# setenforce 1
```

如果 SELinux 没有运行，请启用它。请参阅红帽客户门户网站中的 为 Red Hat Enterprise Linux 产品文档中的 *配置基本系统设置指南中的 使用 SELinux 指南*。

*每个 Ceph 守护进程使用一个或多个端口与 Red Hat Ceph Storage 集群中的其他守护进程通信。在某些情况下，您可以更改默认端口设置。管理员通常仅更改使用 Ceph 对象网关或 **ceph-radosgw** 守护进程的默认端口。*

表 5.1. Ceph 端口

TCP/UDP 端口	Daemon	配置选项
6789, 3300	**ceph-mon**	N/A
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**	N/A
8080	**ceph-radosgw**	**rgw_frontends**

*Ceph Storage 集群守护进程包括 **ceph-mon**、**ceph-mgr** 和 **ceph-osd**。这些守护进程及其主机组成了 Ceph 集群安全区，该区域应使用自己的子网来强化目的。*

*Ceph 客户端包括 **ceph-radosgw**、**ceph-mds**、**ceph-fuse**、**libcephfs**、**rbd**、**librbd** 和 **librados**。这些守护进程及其主机组成存储访问安全区，该区应使用自己的子网来强化目的。*

在 Ceph Storage Cluster zone 主机上，请考虑仅启用运行 Ceph 客户端的主机来连接 Ceph Storage Cluster 守护进程。例如：

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

将 **<zone-name>** 替换为区名称，**<ipaddress>** 替换为 IP 地址，**<netmask>** 替换为 CIDR 标记中的子网掩码，将 **<port-number>** 替换为端口号或范围。使用 **--permanent** 标志重复该过程，以便更改在重新引导后仍然有效。例如：

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

5.4. 报告

Red Hat Ceph Storage 提供基本的系统监控和报告 **ceph-mgr** 守护进程插件；即 RESTful API、仪表板和 **Prometheus** 和 **Zabbix** 等其他插件。Ceph 使用 **collectd** 和 socket 收集此信息，以检索设置、配置详细信息和统计信息。

除了默认的系统行为外，系统管理员还可以配置 **collectd** 以报告安全性问题，例如配置 **IP Tables** 或 **ConnTrack** 插件，以分别跟踪开放端口和连接。

系统管理员也可以在运行时检索配置设置。请参阅 *在运行时查看 Ceph 配置*。

5.5. 审计管理员操作

系统安全的一个重要方面是定期审核集群的管理员操作。Red Hat Ceph Storage 在 **/var/log/ceph/CLUSTER_FSID/ceph.audit.log** 文件中存储管理员操作的历史记录。在监控主机上运行以下命令：

示例

```
[root@host04 ~]# cat /var/log/ceph/6c58dfb8-4342-11ee-a953-fa163e843234/ceph.audit.log
```

每个条目都将包含：

- **Timestamp**：代表执行命令的时间。
- **monitor Address**：标识修改的 monitor。
- **Client Node:** 标识发起更改的客户端节点。
- **Entity:** 标识进行更改的用户。
- **Command:** 标识要执行的命令。

以下是 Ceph 审计日志的输出：

```
2023-09-01T10:20:21.445990+0000 mon.host01 (mon.0) 122301 : audit [DBG] from='mgr.14189
10.0.210.22:0/1157748332' entity='mgr.host01.mcadea' cmd=[{"prefix": "config generate-minimal-
conf"}]: dispatch
2023-09-01T10:20:21.446972+0000 mon.host01 (mon.0) 122302 : audit [INF] from='mgr.14189
10.0.210.22:0/1157748332' entity='mgr.host01.mcadea' cmd=[{"prefix": "auth get", "entity":
"client.admin"}]: dispatch
2023-09-01T10:20:21.453790+0000 mon.host01 (mon.0) 122303 : audit [INF] from='mgr.14189
```

> *10.0.210.22:0/1157748332' entity='mgr.host01.mcadea'*
> *2023-09-01T10:20:21.457119+0000 mon.host01 (mon.0) 122304 : audit [DBG] from='mgr.14189*
> *10.0.210.22:0/1157748332' entity='mgr.host01.mcadea' cmd=[{"prefix": "osd tree", "states":*
> *["destroyed"], "format": "json"}]: dispatch*
> *2023-09-01T10:20:30.671816+0000 mon.host01 (mon.0) 122305 : audit [DBG] from='mgr.14189*
> *10.0.210.22:0/1157748332' entity='mgr.host01.mcadea' cmd=[{"prefix": "osd blocklist ls", "format":*
> *"json"}]: dispatch*

在 Ceph 等分布式系统中，操作可能在一个实例上开始，并可传播到集群中的其他节点。当操作开始时，日志表示 ***dispatch****。当操作结束时，日志表示* ***finished****。*

第 6 章 数据保留

Red Hat Ceph Storage 存储存储用户数据，但通常采用间接方式。客户数据保留可能涉及其他应用程序，如 Red Hat OpenStack Platform。

6.1. CEPH STORAGE 集群

Ceph Storage Cluster- 通常被称为可靠的自主分布式对象存储或 RADOS- 存储作为池中的对象。在大多数情况下，这些对象是代表客户端数据的原子单元，如 Ceph 块设备镜像、Ceph 对象网关对象或 Ceph Filesystem 文件。但是，在 **librados** 基础上构建的自定义应用可以绑定到池，也可以存储数据。

cephx 控制对存储对象数据的池的访问。但是，Ceph Storage Cluster 用户通常是 Ceph 客户端，而不是用户。因此，用户 **通常不会** 直接在 Ceph Storage Cluster 池中写入、读取或写入对象。

6.2. CEPH 块设备

红帽 Ceph 存储的最常见用途是 Ceph 块设备接口，也称为 RADOS 块设备或 RBD，创建虚拟卷、镜像和计算实例，并将它们存储为池中的一系列对象。Ceph 将这些对象分配到 PG，并将它们伪随机放在整个集群的 OSD 中。

根据应用程序使用的 Ceph Block Device 接口（通常为 Red Hat OpenStack Platform），用户可以创建、修改和删除卷和镜像。Ceph 处理各个对象的创建、检索、更新和删除操作。

删除卷和镜像会以无法恢复的方式销毁对应的对象。但是，重新隐藏的数据工件可能会继续驻留在存储介质上，直到被覆盖为止。数据也可能保留在备份存档中。

6.3. CEPH 文件系统

Ceph 文件系统接口创建虚拟文件系统，并将它们作为池中一系列对象来存储它们。Ceph 将这些对象分配到 PG，并将它们伪随机放在整个集群的 OSD 中。

通常，Ceph 文件系统使用两个池：

- **元数据：** 元数据池存储 Ceph 元数据服务器(MDS)的数据，它们通常由索引节点组成，即文件所有权、权限、创建日期和时间、上次修改或访问日期和时间、父目录等。
- **Data：** 数据池存储文件数据。Ceph 可以将文件存储为一个或多个对象，通常代表区块较小的文件数据，如扩展。

根据应用程序使用的 Ceph System 接口（通常为 Red Hat OpenStack Platform），用户可以在 Ceph 文件系统中创建、修改和删除文件。Ceph 处理代表该文件的每个对象的创建、检索、更新和删除操作。

删除文件会以无法恢复的方式销毁对应的对象。但是，重新隐藏的数据工件可能会继续驻留在存储介质上，直到被覆盖为止。数据也可能保留在备份存档中。

6.4. CEPH 对象网关

从数据安全性和保留角度看，Ceph 对象网关接口与 Ceph 块设备和 Ceph 文件系统接口相比有一些重要的区别。Ceph 对象网关向用户提供服务。Ceph 对象网关可能会存储：

- **用户身份验证信息：** 用户身份验证信息通常由用户 ID、用户访问密钥和用户 secret 组成。如果提供，它也可能包含用户的名称和电子邮件地址。Ceph 对象网关将保留用户身份验证数据，除非用户从系统明确删除。

- ***用户数据：*** *用户数据通常包含用户或管理员创建的存储桶或容器，以及用户创建的 S3 或 Swift 对象。Ceph 对象网关接口为每个 S3 或 Swift 对象创建一个或多个 Ceph 存储集群对象，并将对应的 Ceph Storage 集群对象存储在数据池中。Ceph 将 Ceph 存储集群对象分配到 PG，并在整个集群的 OSD 中进行伪随机放置。Ceph 对象网关还可以存储存储桶或索引中包含的对象的索引，以启用服务，如列出 S3 存储桶或 Swift 容器的内容。此外，在实施多部分上传时，Ceph 对象网关可以暂时存储 S3 或 Swift 对象的部分上传。*
  用户可以创建、修改和删除存储桶或容器，以及它们在 Ceph 对象网关中包含的对象。Ceph 处理代表 S3 或 Swift 对象的创建、检索、更新和删除操作。

  删除 S3 或 Swift 对象会以无法恢复的方式销毁对应的 Ceph Storage 集群对象。但是，重新隐藏的数据工件可能会继续驻留在存储介质上，直到被覆盖为止。数据也可能保留在备份存档中。

- ***日志记录 ：****Ceph 对象网关也存储用户计划要执行的操作日志，从而完成和执行的操作。此数据提供有关创建、修改或删除存储桶或容器或位于 S3 存储桶或 Swift 容器的 S3 或 Swift 对象的可追溯性。当用户删除其数据时，日志信息不会生效，并在由系统管理员删除或根据过期策略自动删除前保留存储。*

Bucket 生命周期

Ceph 对象网关也支持 bucket 生命周期功能，包括对象到期。与 General Data Protection Regulation 等数据保留法规可能需要管理员设置对象过期策略，并将其披露给用户以及其他合规因素。

多站点

Ceph 对象网关通常部署到多站点环境中，让用户在一个站点存储对象，Ceph 对象网关在另一个集群中创建对象的副本，可能位于其他地理位置。例如，如果主集群失败，二级集群可能会恢复操作。在另一个示例中，次要集群可能位于不同的地理位置，如边缘网络或内容交付网络，因此客户端可以访问最接近的集群以提高响应时间、吞吐量和其他性能特性。在多站点场景中，管理员必须确保每个站点都实施了安全措施。另外，如果在多站点场景中发生数据地理分布，管理员必须了解数据跨策略边界时的任何法规影响。

第 7 章 联邦信息处理标准(FIPS)

在最新认证的 Red Hat Enterprise Linux 版本中运行时，Red Hat Ceph Storage 使用 FIPS 验证加密模块。

- 在 Red Hat Enterprise Linux 在安装过程中或之后启用 FIPS 模式。
  - 对于容器部署，请按照 Red Hat Enterprise Linux 9 安全强化指南 中的说明进行操作。

其它资源

- 请参阅美国政府标准以了解 FIPS 验证的最新信息。
- 请参阅 Red Hat Ceph Storage 兼容性指南 。

第 8 章 概述

本文档仅介绍了 Red Hat Ceph Storage 的安全性。联系红帽 Ceph 存储咨询团队以获取更多帮助。