Red Hat Ceph Storage 7

データのセキュリティーおよび強化ガイド

Red Hat Ceph Storage データのセキュリティーおよび強化ガイド

Last Updated: 2024-03-28

Red Hat Ceph Storage 7 データのセキュリティーおよび強化ガイド

Red Hat Ceph Storage データのセキュリティーおよび強化ガイド

法律上の通知

概要

本書では、Ceph Storage クラスターおよびそのクライアントのデータセキュリティーと強化情報を提供します。 Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ を参照してください。

目次

第1章 データセキュリティーの概要

セキュリティーは重要な懸念事項であり、Red Hat Ceph Storage デプロイメントの重点を置く必要があります。データ侵害とダウンタイムはコストがかかり、管理が困難です。法律では監査とコンプライアンスプロセスに合格することが義務付けられている場合があり、プロジェクトではデータプライバシーとセキュリティーがある程度期待されています。本書では、Red Hat Ceph Storage のセキュリティーに関する全般的な概要と、システムのセキュリティーをサポートする Red Hat のロールについて説明します。

1.1. はじめに

本書では、Red Hat Ceph Storage のデプロイメントに **cephadm** を使用する Ceph Orchestrator に焦点を当てて、Red Hat Ceph Storage のセキュリティーを強化するためのアドバイスとグッドプラクティス情報を提供しています。本書の指示に従って、お使いの環境のセキュリティーを強化しますが、これらの推奨事項に従ってセキュリティーやコンプライアンスを保証しません。

1.2. RED HAT CEPH STORAGE の概要

Red Hat Ceph Storage (RHCS) はスケーラビリティーが高く、信頼性の高いオブジェクトストレージソリューションです。これは通常、OpenStack のようなクラウドコンピューティングソリューション (スタンドアロンストレージサービスとして、またはインターフェイスを使用したネットワーク接続ストレージ) とともにデプロイされます。

RHCS デプロイメントはすべて、通常 3 種類のデーモンで設定される Ceph Storage Cluster または RADOS (Reliable Autonomous Distributed Object Store) と呼ばれるストレージクラスターで設定されます。

- **Ceph Monitors (ceph-mon):** Ceph モニターは、クラスターの状態に関する合意の確率、OSD が稼働しているかどうかやクラスター内での履歴の維持、クライアントがデータの書き込みと読み取りを行うプールリストの提供、クライアントと Ceph Storage Cluster デーモンの認証の提供など、重要な機能を提供しています。

- **Ceph Manager (ceph-mgr):** Ceph Manager デーモンは、Ceph OSD 全体に分散される配置グループのコピー間のピアングのステータス、配置グループの状態履歴、Ceph クラスターに関するメトリックを追跡します。また、外部監視および管理システム用のインターフェイスも提供します。

- **Ceph OSD (ceph-osd):** Ceph Object Storage Daemons (OSD) は、クライアントデータの保存と提供、クライアントデータのセカンダリー Ceph OSD デーモンへのレプリケート、その健全性と隣接する OSD の健全性の追跡と Ceph Monitor への報告、障害からの動的リカバリー、クラスターサイズの変更時のデータのバックフィルなどの機能を備えています。

RHCS デプロイメントはすべて、Ceph Storage クラスターまたは RADOS (再利用可能な Autonomous Distributed Object Store) にエンドユーザーデータを保存します。通常、ユーザーは Ceph Storage Cluster と直接対話 **しません**。むしろ、Ceph クライアントと対話します。

Ceph Storage Cluster クライアントには、主に 3 つのクライアントがあります。

- **Ceph Object Gateway (radosgw):** Ceph Object Gateway (RADOS Gateway、 **radosgw** または **rgw** とも呼ばれる) は、RESTful API を備えたオブジェクトストレージサービスを提供します。Ceph Object Gateway は、クライアントの代わりに Ceph Storage クラスターまたは RADOS にデータを格納します。

- **Ceph Block Device (rbd):** Ceph ブロックデバイスは、Kernel RBD (**krbd**) を介して Linux カーネル、または **librbd** を介して OpenStack といったクラウドコンピューティングソリューショ

ンに、コピーオンライト、シンプロビジョニング、およびクローン可能な仮想ブロックデバイスを提供します。

- **Ceph File System (cephfs):** Ceph File System は、1 つ以上のメタデータサーバー (**mds**) で設定されており、このファイルシステムの inode の部分を Ceph Storage クラスターのオブジェクトとして格納します。Ceph ファイルシステムは、カーネルクライアント、FUSE クライアント、または OpenStack などのクラウドコンピューティングソリューション向けに **libcephfs** ライブラリーを介してマウントすることができます。

追加のクライアントには、開発者がカスタムアプリケーションを作成して Ceph Storage クラスターと対話できる **librados** や、管理目的でコマンドラインインターフェイスクライアントなどがあります。

1.3. ソフトウェアのサポート

Red Hat Ceph Storage のセキュリティーの重要な側面は、セキュリティーが事前に組み込まれ、Red Hat が長期にわたってサポートするソリューションを提供することです。Red Hat が Red Hat Ceph Storage を取得する特定の手順には、以下が含まれます。

- アップストリーム関係およびコミュニティーの連携を維持することで、最初からセキュリティーにフォーカスできるようにします。
- セキュリティーおよびパフォーマンス追跡レコードに基づいてパッケージを選択して設定します。
- (アップストリームビルドを受け入れる代わりに) 関連付けられたソースコードからバイナリーをビルドします。
- 検査および品質保証ツールのスイートを適用して、潜在的なセキュリティー問題やリグレッションを防ぎます。
- リリースされたすべてのパッケージにデジタル署名し、暗号化で認証されたディストリビューションチャンネルで配布します。
- パッチおよび更新を配信するための単一の統合メカニズムを提供します。

さらに、Red Hat は、製品に対して脅威と脆弱性を分析する専用のセキュリティーチームを維持し、カスタマーポータルから適切なアドバイスと更新を提供します。このチームは、ほとんどが理論上の問題である問題とは対照的に、どの問題が重要であるかを決定します。Red Hat Product Security チームは専門知識を維持し、Red Hat サブスクリプション製品に関連するアップストリームコミュニティーへの貢献をもたらします。プロセスの重要な部分である RedHat Security アドバイザリーは、脆弱性が最初に公開された日に頻繁に配布されるパッチとともに、Red Hat ソリューションに影響を与えるセキュリティーの欠陥を事前に通知します。

第2章 脅威および脆弱性管理

Red Hat Ceph Storage は通常、クラウドコンピューティングソリューションとともにデプロイされるため、Red Hat Ceph Storage のデプロイメントが大規模なデプロイメントの一連のコンポーネントの 1 つとして抽象化されていると考えると便利です。これらのデプロイメントには、通常セキュリティー上の懸念事項があります。これは本ガイドでは **セキュリティーゾーン** と呼ばれています。脅威のアクターとベクターは、その動機とリソースへのアクセスに基づいて分類されます。目的に応じて、各ゾーンのセキュリティー上の懸念を把握することを目的としています。

2.1. 脅威アクター

脅威アクターは、防御を試みる可能性のある敵のクラスを指す抽象的な方法です。アクターの能力が高いほど、攻撃の軽減と防止を成功させるために必要なセキュリティー制御が厳しくなります。セキュリティーは、要件に基づいて、利便性、防御、およびコストのバランスを取ることです。ここで説明するすべての脅威アクターに対して Red Hat Ceph Storage デプロイメントのセキュリティーを保護することができない場合があります。Red Hat Ceph Storage をデプロイする場合は、デプロイメントと使用方法のバランスを判断する必要があります。

リスク評価の一環として、保存するデータの種類やアクセス可能なリソースも考慮する必要があります。これは、特定のアクターにも影響するためです。ただし、お使いのデータがアクターにさらせない場合でも、コンピューティングリソースに引き付けられる可能性があります。

- **ネーションステートアクター:** これは最も有能な敵です。国民国家の攻撃者は、ターゲットに対して莫大なリソースをもたらす可能性があります。彼らは他のどの攻撃者よりも優れた能力を持っています。人間と技術の両方で厳格な管理が行われていなければ、これらの攻撃者から身を守ることは困難です。

- **深刻な組織犯罪:** このクラスは、非常に有能で経済的に主導された攻撃者のグループを説明します。彼らは、社内のエクスプロイト開発とターゲット研究に資金を提供することができます。近年、大規模なサイバー犯罪企業である Russian Business Network などの組織の台頭により、サイバー攻撃がどのように商品になったかが実証されています。産業スパイは、深刻な組織犯罪グループに分類されます。

- **非常に有能なグループ:** 通常は商業的には資金提供されていないが、サービスプロバイダーやクラウドオペレーターに重大な脅威を招く可能性があるハクティビストタイプの組織を指します。

- **一人で行動するやる気のある個人:** この攻撃者は、不正または悪意のある従業員、不満を持った顧客、小規模な産業スパイなど、さまざまな形で登場します。

- **幼稚なクラッカー:** この攻撃者は特定の組織をターゲットとしませんが、自動化された脆弱性スキャンと不正使用を実行します。多くの場合、これらは厄介ですが、攻撃者の 1 人による侵害は、組織の評判に対する大きなリスクです。

次の方法は、上記で特定されたリスクの一部を軽減するのに役立ちます。

- **セキュリティー更新:** ネットワーク、ストレージ、サーバーハードウェアなど、基礎となる物理インフラストラクチャーのエンドツーエンドのセキュリティーポジションを考慮する必要があります。これらのシステムには、独自のセキュリティー強化プラクティスが必要です。Red Hat Ceph Storage のデプロイメントでは、定期的にテストしてセキュリティー更新をデプロイする計画を立てる必要があります。

- **製品更新:** Red Hat は、製品更新が利用可能になったら実行することを推奨します。更新は通常、6 週間ごとに (場合によってはもっと頻繁に) リリースされます。Red Hat は、追加の統合テストを必要としないように、メジャーリリース内でポイントリリースと z-stream リリースを完全に互換性のあるものにするよう努めています。

- **アクセス管理:** アクセス管理には、認証、認可、アカウンティングが含まれます。認証は、ユーザーのアイデンティティーを検証するプロセスです。承認は、パーミッションを認証ユーザーに付与するプロセスです。アカウンティングは、ユーザーがアクションを実行するユーザーを追跡するプロセスです。ユーザーにシステムアクセスを付与する場合は、**最小権限の原則** を適用し、実際に必要なシステム権限をユーザーにのみ付与します。このアプローチは、悪意のある攻撃者とシステム管理者の誤植の両方のリスクを軽減するのにも役立ちます。

- **インサイダーの管理:** ロールベースのアクセス制御 (最低限必要なアクセス) を慎重に割り当て、内部インターフェイスで暗号化を使用し、認証/認可セキュリティー (集中管理など) を使用することで、悪意のあるインサイダーの脅威を軽減できます。また、職務の分離や不規則な職務のローテーションなど、技術以外の追加オプションを検討することもできます。

2.2. セキュリティーゾーン

セキュリティーゾーンは、一般的な信頼要件とシステム内で期待するユーザー、アプリケーション、サーバー、またはネットワークで設定されます。通常、これらは同じ認証と承認の要件とユーザーを共有します。これらのゾーンの定義をさらに絞り込むことはできますが、本書では 4 つの異なるセキュリティーゾーンを指しています。これら 3 つは、セキュリティーが強化された Red Hat Ceph Storage クラスターのデプロイに必要な最小限のフォーマットの 3 つです。これらのセキュリティーゾーンは、少なくとも信頼されているものから順にリスト表示されます。

- **パブリックセキュリティーゾーン:** パブリックセキュリティーゾーンは、クラウドインフラストラクチャーの完全に信頼できない領域です。この環境は、インターネット全体として参照することも、認証局がない Red Hat OpenStack デプロイメント外部のネットワークにも言及することができます。このゾーンを経由する機密性または整合性要件があるデータはすべて、暗号化などの補正制御を使用して保護する必要があります。パブリックセキュリティーゾーンは、Ceph Storage クラスターのフロントエンドまたはクライアント側のネットワークと混同 **しないようにしてください**。これは RHCS の **public_network** と呼ばれ、パブリックセキュリティーゾーンまたは Ceph クライアントセキュリティーゾーンの一部 **ではありません**。

- **Ceph クライアントセキュリティーゾーン:** RHCS では、Ceph クライアントセキュリティーゾーンは、Ceph Object Gateway、Ceph Block Device、Ceph Filesystem、**librados** などの Ceph クライアントにアクセスするネットワークを指します。Ceph クライアントのセキュリティーゾーンは通常、ファイアウォールの背後で、パブリックのセキュリティーゾーンから自身を分離します。ただし、Ceph クライアントは常にパブリックのセキュリティーゾーンから保護される訳ではありません。パブリックのセキュリティーゾーンに、Ceph Object Gateway の S3 および Swift API を公開することができます。

- **ストレージアクセスセキュリティーゾーン:** ストレージアクセスセキュリティーゾーンは、Ceph Storage クラスターにアクセスできる Ceph クライアントを提供する内部ネットワークのことです。このドキュメントが OpenStack Platform セキュリティーおよび強化ガイドで使用されている用語と一致するように、ストレージアクセスセキュリティーゾーンというフレーズを使用します。ストレージアクセスセキュリティーゾーンには、Ceph Storage クラスターのフロントエンドまたはクライアント側のネットワーク (RHCS の **public_network** と呼ばれます) が含まれます。

- **Ceph クラスターセキュリティーゾーン:** Ceph クラスターセキュリティーゾーンは、レプリケーション、ハートビート、バックフィル、復旧のためのネットワーク通信で Ceph Storage クラスターの OSD デーモンを提供する内部ネットワークを指します。Ceph クラスターセキュリティーゾーンには、Ceph Storage クラスターのバックサイドネットワーク (RHCS の **cluster_network** と呼ばれます) が含まれます。

これらのセキュリティーゾーンは、個別にマッピングすることも、特定の RHCS デプロイメント内で信頼の可能な領域の大部分を表すこともできます。セキュリティーゾーンは、特定の RHCS デプロイメントトポロジーにマッピングする必要があります。ゾーンとその信頼要件は、Red Hat Ceph Storage が

スタンドアロン容量で動作しているか、パブリック、プライベート、またはハイブリッドクラウドを提供しているかによって異なります。

これらのセキュリティーゾーンを視覚的に表示するには、セキュリティーに最適化されたアーキテクチャー を参照してください。

関連情報

- 詳細は、**Red Hat Ceph Storage データのセキュリティーおよび強化ガイド**の **ネットワーク通信** セクションを参照してください。

2.3. セキュリティーゾーンの接続

異なる信頼レベルまたは認証要件のある複数のセキュリティーゾーンにまたがるコンポーネントは、慎重に設定する必要があります。このような接続は、ネットワークアーキテクチャーにおける弱いポイントであることが多く、接続しているゾーンの信頼レベルのセキュリティー要件を満たすように常に設定する必要があります。多くの場合、攻撃の可能性があるため、接続されたゾーンのセキュリティー制御が主要な懸念事項になります。ゾーンが出会うポイントは、攻撃者がデプロイメントのより機密性の高い部分に攻撃を移行または標的化する機会を提供します。

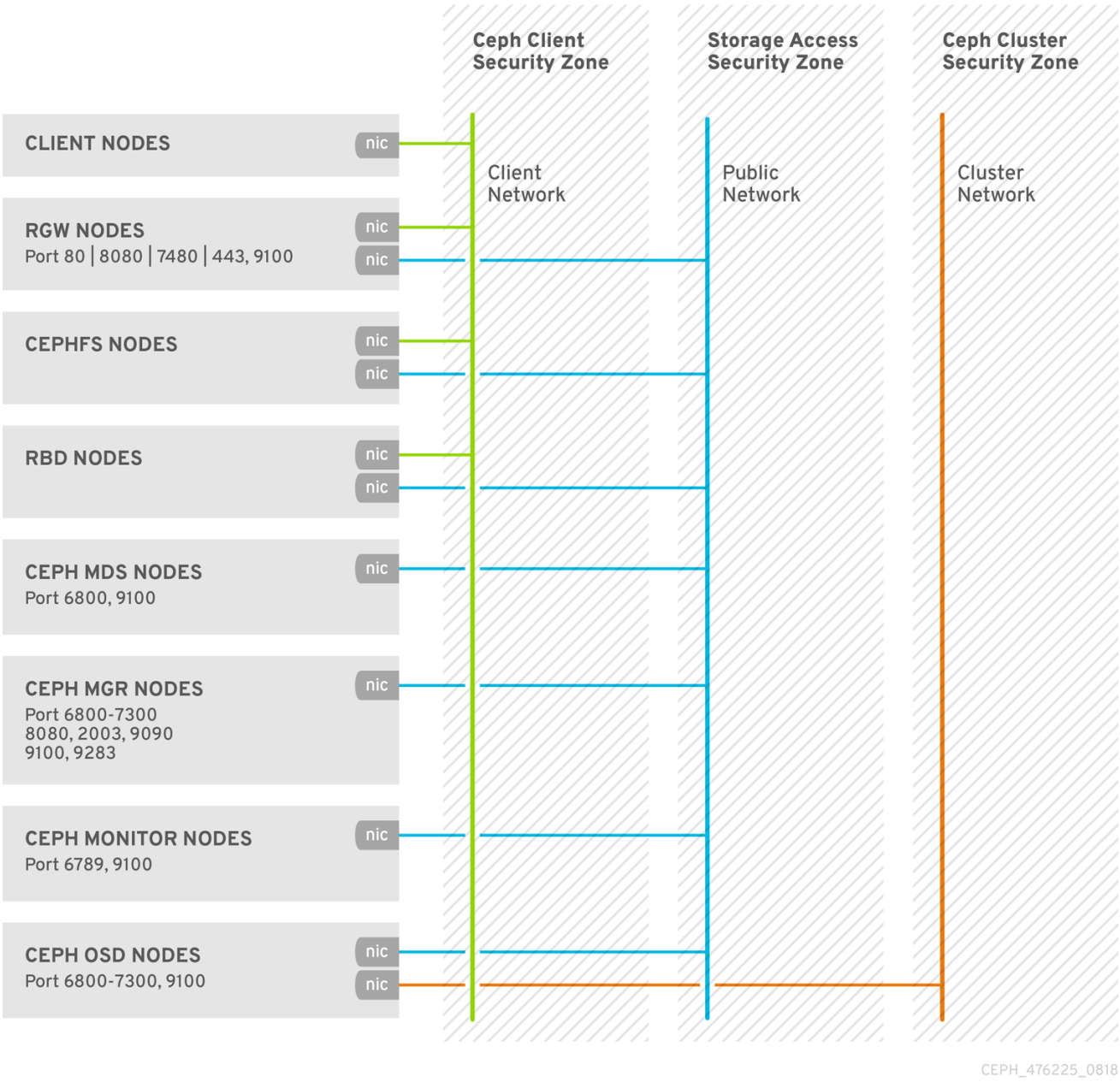
場合によっては、Red Hat Ceph Storage の管理者は、統合ポイントが存在するどのゾーンよりも高い基準で統合ポイントを保護することを検討したい場合があります。たとえば、他のセキュリティーゾーンに接続する理由がないため、Ceph Cluster Security Zone は他のセキュリティーゾーンから簡単に分離できます。一方、Storage Access Security Zone は、Ceph モニターノードのポート **6789** へのアクセスを提供し、Ceph OSD ノード上のポート **6800-7300** を提供する必要があります。ただし、Ceph 管理者にのみ公開される必要がある Ceph Grafana 監視情報へのアクセスを提供するため、ポート **3000** は Storage Access Security Zone のみに限定する必要があります。Ceph クライアントセキュリティーゾーンの Ceph Object Gateway は、Ceph クラスターセキュリティーゾーンのモニター (ポート **6789**) および OSD (ポート **6800-7300**) にアクセスし、その S3 および Swift API を HTTP ポート **80** や HTTPS ポート **443** 経由などのパブリックセキュリティーゾーンに公開する場合がありますが、引き続き管理 API へのアクセスを制限しないといけない場合があります。

Red Hat Ceph Storage の設計では、セキュリティーゾーンの分離が困難になります。通常、コアサービスは少なくとも 2 つのゾーンにまたがるため、セキュリティーコントロールを適用する際に特別な考慮を指定する必要があります。

2.4. セキュリティーに最適化されたアーキテクチャー

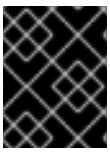
Red Hat Ceph Storage クラスターのデーモンは、通常サブネットを分離しているノードで稼働するため、RHCS クラスターのセキュリティーは比較的簡単です。

一方、Ceph ブロックデバイス (**rbd**)、Ceph ファイルシステム (**cephfs**)、Ceph オブジェクトゲートウェイ (**rgw**) などの Red Hat Ceph Storage クライアントは RHCS ストレージクラスターにアクセスしますが、サービスを他のクラウドコンピューティングプラットフォームに公開します。


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

第3章 暗号化および鍵管理

Red Hat Ceph Storage クラスターは、通常、プライベートストレージクラスターネットワークを使用する場合に、独自のネットワークセキュリティーゾーンにあります。



重要

攻撃者がパブリックネットワーク上の Ceph クライアントにアクセスできる場合は、セキュリティーゾーンの分離が不十分である可能性があります。

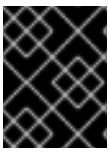
ネットワークトラフィックの機密性または整合性を保証するためのセキュリティー要件があり、Red Hat Ceph Storage が暗号化とキー管理を使用する状況があります。

- SSH
- SSL ターミネーション
- メッセンジャー v2 プロトコル
- 転送中での暗号化
- REST での暗号化
- キーのローテーション

3.1. SSH

Red Hat Ceph Storage クラスターのすべてのノードは、クラスターのデプロイの一部として SSH を使用します。これは、各ノードで以下のことを意味します。

- パスワードなしの root 権限を持つ **cephadm** ユーザーが存在します。
- SSH サービスが有効になり、拡張ポート 22 が開いています。
- **cephadm** ユーザーの公開 SSH キーのコピーが利用可能です。



重要

拡張機能によって **cephadm** ユーザーにアクセスできるユーザーには、Red Hat Ceph Storage クラスターの任意のノードで **root** としてコマンドを実行する権限があります。

関連情報

- 詳細は、**Red Hat Ceph Storage インストールガイド**の **cephadm の仕組み** セクションを参照してください。

3.2. SSL ターミネーション

Ceph Object Gateway は HAProxy と併用してデプロイでき、負荷分散とフェイルオーバーのために **keepalived** を使用することができます。オブジェクトゲートウェイ Red Hat Ceph Storage バージョン 2 および 3 は Civetweb を使用します。Civetweb の以前のバージョンは SSL をサポートしておらず、新しいバージョンは SSL をサポートしていますが、パフォーマンスに制限があります。

オブジェクトゲートウェイ Red Hat Ceph Storage バージョン 5 は Beast を使用します。Beast フロントエンド Web サーバーが OpenSSL ライブラリーを使用して Transport Layer Security (TLS) を提供するように設定できます。

HAProxy と **keepalived** を使用して SSL 接続を終了する場合は、HAProxy および **keepalived** コンポーネントは暗号化キーを使用します。

HAProxy と **keepalived** を使用して SSL を終端する場合、ロードバランサーと Ceph Object Gateway 間の接続は暗号化 **されません**。

詳細は、**Beast の SSL の設定** および **HAProxy および keepalived** を参照してください。

3.3. メッセンジャー V2 プロトコル

Ceph のオンワイヤプロトコル **msgr2** の 2 番目のバージョンには、以下の機能があります。

- 安全なモードは、ネットワークを介したすべてのデータの移動を暗号化します。
- 認証ペイロードのカプセル化を改善し、新しい認証モードの今後の統合を可能にします。
- 機能のアドバタイズおよびネゴシエーションの改善。

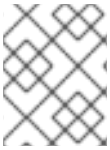
Ceph デーモンは、レガシー、v1 互換、および新しい v2 互換の Ceph クライアントを同じストレージクラスターに接続することができるように、複数のポートにバインドします。Ceph Monitor デーモンに接続する Ceph クライアントまたはその他の Ceph デーモンは、まず **v2** プロトコルを使用しますが、可能な場合は古い **v1** プロトコルが使用されます。デフォルトでは、メッセンジャープロトコル **v1** と **v2** の両方が有効です。新規の v2 ポートは 3300 で、レガシー v1 ポートはデフォルトで 6789 になります。

messenger v2 プロトコルには、v1 プロトコルまたは v2 プロトコルを使用するかどうかを制御する 2 つの設定オプションがあります。

- **ms_bind_msgr1** - このオプションは、デーモンが v1 プロトコルと通信するポートにバインドするかどうかを制御します。デフォルトでは **true** です。
- **ms_bind_msgr2** - このオプションは、デーモンが v2 プロトコルと通信するポートにバインドするかどうかを制御します。デフォルトでは **true** です。

同様に、使用する IPv4 アドレスと IPv6 アドレスに基づいて 2 つのオプションを制御します。

- **ms_bind_ipv4** - このオプションは、デーモンが IPv4 アドレスにバインドするかどうかを制御します。デフォルトでは **true** です。
- **ms_bind_ipv6** - このオプションは、デーモンが IPv6 アドレスにバインドするかどうかを制御します。デフォルトでは **true** です。



注記

複数のポートにバインドする機能は、デュアルスタック IPv4 および IPv6 サポートの方法になります。

msgr2 プロトコルは、以下の 2 つの接続モードをサポートします。

- **crc**
  - **cephx** で接続を確立すると、強固な初期認証を提供します。

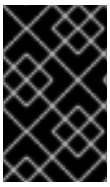
- ビットフリップから保護する **crc32c** 整合性チェックを提供します。
- 悪意のある中間者攻撃に対する保護を提供しません。
- 盗聴者がすべての認証後のトラフィックを見るのを妨げません。

- **secure**
  - **cephx** で接続を確立すると、強固な初期認証を提供します。
  - 認証後トラフィックをすべて完全に暗号化します。
  - 暗号化整合性チェックを提供します。

デフォルトのモードは **crc** です。

Ceph Object Gateway 暗号化

また、Ceph Object Gateway は S3 API を使用したお客様によって提供されるキーによる暗号化をサポートします。

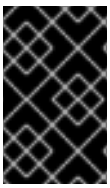


重要

転送において厳密な暗号化を必要とする規制コンプライアンス標準に準拠するために、管理者はクライアント側の暗号化で Ceph Object Gateway をデプロイ **する必要があります**。

Ceph ブロックデバイスの暗号化

システム管理者は、Ceph を Red Hat OpenStack Platform 13 暗号化のバックエンドとして統合し、RBD Cinder に **dm_crypt** を使用して Ceph ブロックデバイスボリュームを Ceph Storage クラスター内で有線暗号化できるようにする **必要があります**。



重要

転送で厳密な暗号化を必要とする規制コンプライアンス標準に準拠するために、システム管理者は、RBD Cinder に **dmcrypt** を使用して、Ceph ストレージクラスター内で有線暗号化を行う **必要があります**。

関連情報

- 詳細は、**Red Hat Ceph Storage 設定ガイド**の **接続モードの設定オプション** を参照してください。

3.4. 転送中での暗号化

Red Hat Ceph Storage 5 以降、メッセンジャーバージョン 2 プロトコルの導入により、ネットワーク上のすべての Ceph トラフィックの暗号化がデフォルトで有効になっています。messenger v2 の **secure mode** 設定は、Ceph デーモンと Ceph クライアント間の通信を暗号化するため、エンドツーエンドの暗号化を提供します。

ceph config dump コマンド、**netstat -lp | grep ceph-osd** コマンドを使用して messenger v2 プロトコルの暗号化を確認するか、v2 ポートで Ceph デーモンを確認できます。

関連情報

- SSL ターミネーションの詳細は、**SSL ターミネーション** を参照してください。
- S3 API 暗号化の詳細は、**S3 サーバー側の暗号化** を参照してください。

3.5. MESSENGER V2 プロトコルの圧縮モード

Red Hat Ceph Storage 6 以降では、messenger v2 プロトコルが圧縮機能をサポートしています。

この機能は、デフォルトでは有効になっていません。ピア間のメッセージのセキュリティーレベルが低下するため、同じメッセージを圧縮して暗号化することは推奨しません。暗号化が有効になっている場合、設定オプション **ms_osd_compress_mode** が **true** に設定されるまで、圧縮を有効にする要求は無視されます。

次の 2 つの圧縮モードをサポートしています。

- **force**
  - マルチアベイラビリティゾーンのデプロイメントでは、OSD 間のレプリケーションメッセージを圧縮して遅延を節約します。
  - パブリッククラウドでは、メッセージサイズが最小化されるため、クラウドプロバイダーのネットワークコストが削減されます。
  - NVMe を使用するパブリッククラウド上のインスタンスは、デバイスの帯域幅に比べて低いネットワーク帯域幅を提供します。悪意のある中間者攻撃に対する保護を提供しません。
- **none**
  - メッセージは圧縮せずに送信されます。

メッセージの圧縮が有効になっていることを確認するには、**debug_ms** コマンドを実行し、接続のいくつかのデバッグエントリーを確認します。また、**ceph config get** コマンドを実行して、ネットワークメッセージのさまざまな設定オプションに関する詳細を取得できます。

関連情報

- 詳細は、**Red Hat Ceph Storage 設定ガイド** の **圧縮モードの設定オプション** を参照してください。

3.6. REST での暗号化

Red Hat Ceph Storage は、いくつかのシナリオでは、残りの暗号化をサポートします。

1. **Ceph Storage Cluster:** Ceph Storage クラスターは、Ceph OSD の Linux Unified Key Setup または LUKS 暗号化と、それに対応するジャーナル、ライトアヘッドログ、メタデータデータベースをサポートします。このシナリオでは、クライアントが Ceph Block Device、Ceph Filesystem、または **librados** 上に構築されたカスタムアプリケーションであるかどうかにかかわらず、Ceph は静止状態のすべてのデータを暗号化します。
2. **Ceph Object Gateway:** Ceph ストレージクラスターは、クライアントオブジェクトの暗号化をサポートしています。Ceph Object Gateway がオブジェクトを暗号化する際に、それらは Red Hat Ceph Storage クラスターとは独立して暗号化されます。また、送信されるデータは、Ceph Object Gateway と Ceph Storage Cluster の間で暗号化された形式になります。

Ceph Storage クラスターの暗号化

Ceph Storage クラスターは、Ceph OSD に保存されているデータの暗号化をサポートします。Red Hat Ceph Storage は、**dmcrypt** を指定して **lvm** で論理ボリュームを暗号化できます。つまり、**ceph-volume** によって呼び出される **lvm** は、OSD の物理ボリュームではなく論理ボリュームを暗号化します。同じ OSD キーを使用してパーティションなどの LVM 以外のデバイスを暗号化できます。論理ボリュームを暗号化することで、より多くの設定の柔軟性が可能になります。

LUKS v1 は、Linux ディストリビューション間で最も幅広いサポートを持つため、Ceph は LUKS v2 ではなく LUKS v1 を使用します。

OSD を作成する際、**lvm** は秘密鍵を生成し、その鍵を **stdin** 経由で JSON ペイロードで Ceph Monitors に安全に渡します。暗号化キーの属性名は **dmcrypt_key** です。

重要

システム管理者は、暗号化を明示的に有効にする必要があります。

デフォルトでは、Ceph は Ceph OSD に保存されたデータを暗号化しません。システム管理者は、Ceph OSD に保存されているデータを暗号化するために **dmcrypt** を有効にする必要があります。Ceph OSD をストレージクラスターに追加するために Ceph Orchestrator サービス仕様ファイルを使用する場合は、ファイルに次のオプションを設定して Ceph OSD を暗号化します。

例

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

注記

LUKS および **dmcrypt** は、保存データの暗号化のみに対応し、移動中のデータの暗号化には対応しません。

Ceph Object Gateway 暗号化

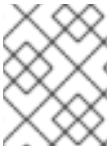
Ceph Object Gateway は、S3 API を使用したお客様によって提供されるキーによる暗号化をサポートします。お客様が提供する鍵を使用する場合、S3 クライアントは暗号鍵を各リクエストと共に渡して、暗号化されたデータの読み取りまたは書き込みを行います。これらのキーを管理するのは、お客様の責任です。各オブジェクトの暗号化に使用する Ceph Object Gateway の鍵を覚えておく必要があります。

関連情報

- 詳細は、**Red Hat Ceph Storage 開発者ガイド**の S3 API サーバー側の暗号化 を参照してください。

3.7. キーローテーションを有効にする

Ceph クラスター内の Ceph および Ceph Object Gateway デーモンには秘密鍵があります。このキーは、クラスターへの接続とクラスターでの認証に使用されます。キーのローテーション機能を使用すると、サービスの中断を最小限に抑えて、アクティブな Ceph クラスター内のアクティブなセキュリティーキーを更新できます。



注記

アクティブな Ceph クラスターには、並行してキーを変更する Ceph クライアントロール内のノードが含まれます。

キーのローテーションは、現在の業界およびセキュリティーのコンプライアンス要件を確実に満たすのに役立ちます。

前提条件

- 稼働中の Red Hat Ceph Storage クラスターがある。
- **admin** 権限を持つユーザー。

手順

1. キーを回転します。

   構文

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

   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. MDS、OSD、MGR 以外のデーモンを使用している場合は、デーモンを再起動して新しいキーに切り替えます。MDS、OSD、および MGR デーモンでは、デーモンを再起動する必要はありません。

   構文

   ```
   ceph orch restart SERVICE_TYPE
   ```

   例

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

第4章 IDENTITY AND ACCESS MANAGEMENT

Red Hat Ceph Storage は、以下の ID およびアクセス管理を提供します。

- Ceph Storage クラスターのユーザーアクセス
- Ceph Object Gateway ユーザーアクセス
- Ceph Object Gateway LDAP/AD 認証
- Ceph Object Gateway OpenStack Keystone 認証

4.1. CEPH STORAGE クラスターのユーザーアクセス

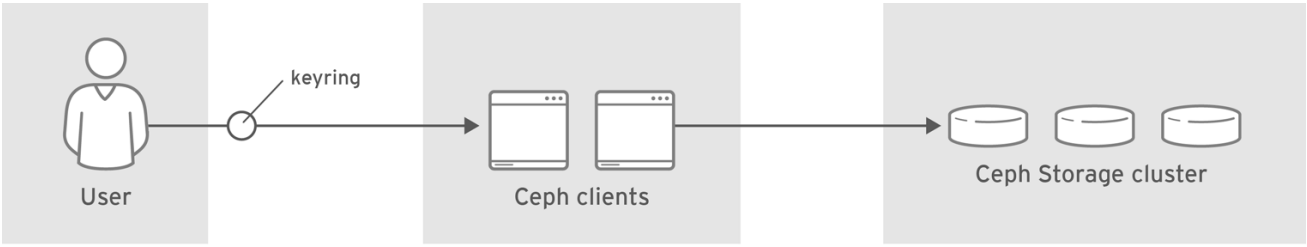
ユーザーを特定し、中間者攻撃から保護するために、Ceph は **cephx** 認証システムを提供し、ユーザーおよびデーモンを認証します。**cephx** の詳細は、Ceph ユーザー管理 を参照してください。

重要

cephx プロトコルは、転送時のデータ暗号化または保存時の暗号化には対応 **していません**。

Cephx は共有シークレットキーを使用して認証を行います。つまり、クライアントとモニタークラスターの両方にはクライアントの秘密鍵のコピーがあります。認証プロトコルは、実際にキーを公開することなく、両方の当事者がキーのコピーを持っていることをお互いに証明できるようなものです。これは相互認証を提供します。つまり、ユーザーがシークレットキーを所有し、ユーザーにはシークレットキーのコピーがあることを確認します。

ユーザーは、Ceph クライアントを使用して Red Hat Ceph Storage クラスターデーモンと対話する個人またはアプリケーションなどのシステムアクターです。



CEPH_459704_1017

Ceph は、デフォルトで有効になっている認証および認可で実行されます。Ceph クライアントは、通常コマンドラインを使用して、指定したユーザーの秘密鍵を含むユーザー名とキーリングを指定できます。ユーザーとキーリングが引数として提供されていない場合、Ceph は **client.admin** 管理ユーザーをデフォルトとして使用します。キーリングが指定されていない場合は、Ceph が Ceph 設定の **keyring** 設定を使用してキーリングを探します。

重要

Ceph クラスターを強化するには、キーリングは、現在のユーザーおよび **root** に ***のみ*** 読み取り/書き込み権限を付与します。**client.admin** 管理ユーザーキーを含むキーリングは **root** ユーザーに制限する必要があります。

認証を使用するように Red Hat Ceph Storage クラスターを設定するための詳細は、Red Hat Ceph Storage 7 の **設定ガイド** を参照してください。具体的には、**Ceph の認証設定** を参照してください。

4.2. CEPH OBJECT GATEWAY ユーザーアクセス

Ceph Object Gateway は、ユーザーがユーザーデータを含む S3 および Swift API にアクセスすることを認証および承認する、独自のユーザー管理を備えた RESTful アプリケーションプログラミングインターフェイス (API) サービスを提供します。認証は以下で設定されます。

- **S3 User:** S3 API のユーザーのアクセスキーおよびシークレット。
- **Swift ユーザー:** Swift API のユーザー向けのアクセスキーおよびシークレットSwift ユーザーは、S3 ユーザーのサブユーザーです。S3 の parent ユーザーを削除すると、Swift ユーザーが削除されます。
- **管理ユーザー:** 管理 API のユーザーのアクセスキーおよびシークレット。管理ユーザーは Ceph Admin API にアクセスして、ユーザーの作成やバケットやコンテナー、およびそれらのオブジェクトへのアクセス許可などの機能を実行できるため、管理ユーザーは慎重に作成する必要があります。

Ceph Object Gateway は、すべてのユーザー認証情報を Ceph Storage クラスタープールに保存します。名前、メールアドレス、クォータ、使用方法などのユーザーに関する追加情報を保存できます。

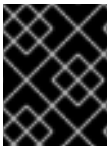
詳細は、ユーザー管理 および 管理ユーザーの作成 を参照してください。

4.3. CEPH OBJECT GATEWAY LDAP または AD 認証

Red Hat Ceph Storage は、Ceph Object Gateway ユーザーを認証するために、LDAP (Light-weight Directory Access Protocol) サーバーをサポートします。LDAP または Active Directory (AD) を使用するように設定されている場合、Ceph Object Gateway は LDAP サーバーに対して定義し、Ceph Object Gateway のユーザーを認証します。

Ceph Object Gateway は、LDAP を使用するかどうかを制御します。ただし、一度設定すると、ユーザーの認証を担当するのは LDAP サーバーです。

Ceph Object Gateway と LDAP サーバー間の通信をセキュアにするため、Red Hat は LDAP Secure または LDAPS で設定をデプロイすることを推奨します。



重要

LDAP を使用する場合は、**rgw_ldap_secret = PATH_TO_SECRET_FILE** シークレットファイルへのアクセスが安全であることを確認してください。

4.4. CEPH OBJECT GATEWAY OPENSTACK KEYSTONE 認証

Red Hat Ceph Storage は、OpenStack Keystone を使用して Ceph Object Gateway Swift API ユーザーの認証をサポートします。Ceph Object Gateway は Keystone トークンを受け入れ、ユーザーを認証し、対応する Ceph Object Gateway ユーザーを作成します。Keystone がトークンを検証すると、Ceph Object Gateway はユーザーが認証されているとみなします。

Ceph Object Gateway は、認証に OpenStack Keystone を使用するかどうかを制御します。ただし、設定が完了すると、ユーザーの認証を担当するのは OpenStack Keystone サービスです。

Keystone と連携するように Ceph Object Gateway を設定するには、**nss db** 形式への要求の作成に Keystone が使用する OpenSSL 証明書を変換する必要があります。

関連情報

- 詳細は、**Red Hat Ceph Storage Object Gateway ガイド** の Ceph Object Gateway および OpenStack Keystone セクションを参照してください。

第5章 インフラストラクチャーセキュリティー

本ガイドのスコープは Red Hat Ceph Storage です。ただし、適切な Red Hat Ceph Storage のセキュリティー計画では、以下の前提条件を考慮する必要があります。

前提条件

- Red Hat Customer Portal にある、ご使用の OS バージョンの Red Hat Enterprise Linux の製品ドキュメント 内の **SELinux の使用ガイド** を参照してください。
- Red Hat Customer Portal にある、ご使用の OS バージョンの Red Hat Enterprise Linux の製品ドキュメント 内の **セキュリティー強化ガイド** を確認してください。

5.1. 管理

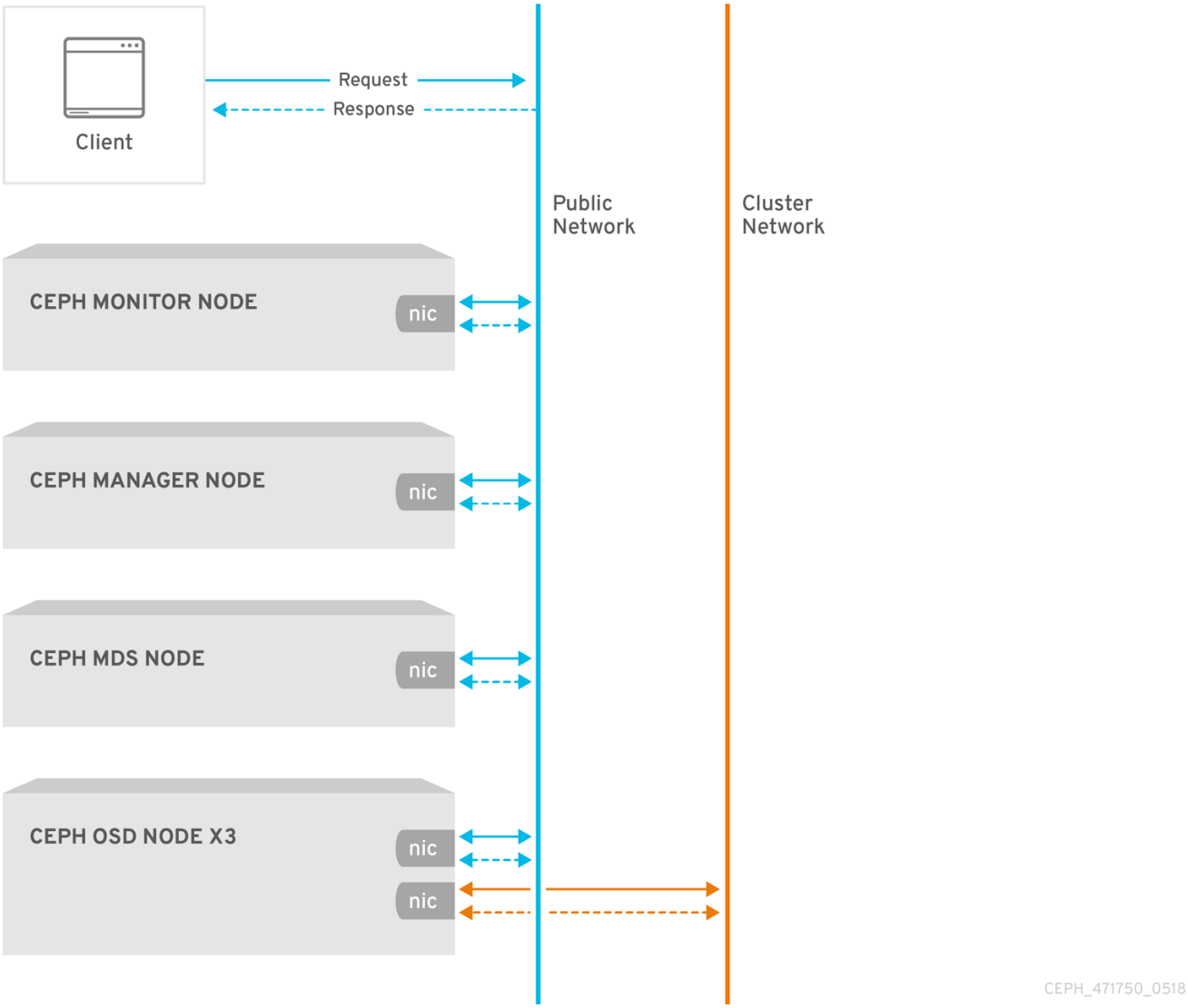
Red Hat Ceph Storage クラスターの管理には、コマンドラインツールを使用する必要があります。CLI ツールには、クラスターへの管理者アクセス権限を付与するための管理者キーが必要です。デフォルトでは、Ceph は管理者キーを **/etc/ceph** ディレクトリーに保存します。デフォルトのファイル名は **ceph.client.admin.keyring** です。クラスターに対する管理者権限を持つユーザーのみがキーリングにアクセスできるよう、キーリングのセキュリティーを保護する手順を説明します。

5.2. ネットワーク通信

Red Hat Ceph Storage は 2 つのネットワークを提供します。

- パブリックネットワーク。
- クラスターネットワーク

すべての Ceph デーモンおよび Ceph クライアントでは、**ストレージアクセスセキュリティーゾーン** の一部であるパブリックネットワークへのアクセスが必要です。一方、OSD デーモン **のみ** が **Ceph クラスターセキュリティーゾーン** の一部であるクラスターネットワークへのアクセスを必要とします。



Ceph の設定には、**public_network** および **cluster_network** の設定が含まれます。強化の目的で、CIDR 表記を使用して IP アドレスとネットマスクを指定します。クラスターに複数のサブネットがある場合は、複数のコンマ区切りの IP アドレスおよびネットマスクエントリーを指定します。

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

詳細は、**Red Hat Ceph Storage 設定ガイド**の Ceph ネットワーク設定 セクションを参照してください。

5.3. ネットワークサービスの強化

システム管理者は、Red Hat Enterprise Linux 8 Server に Red Hat Ceph Storage クラスターをデプロイします。SELinux はデフォルトでオンになっており、ファイアウォールは SSH サービスポート **22** 以外の受信トラフィックをすべてブロックします。ただし、その他の承認されていないポートが開いたり不要なサービスが有効にならないようにするため、これが当てはまるようにする **必要** があります。

各サーバーノードで、以下を実行します。

1. **firewalld** サービスを起動し、システムの起動時に実行できるようにし、実行していることを確認します。

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

2. 開いているすべてのポートのインベントリーを取得します。

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

新規インストールでは、**sources:** セクションを空白にし、ポートが特別に開いていないことを示します。**services** セクションは、**SSH** サービス (およびポート **22**) および **dhcpv6-client** が有効になっていることを示します。

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

3. SELinux が実行され、**Enforcing** であることを確認します。

```
# getenforce
Enforcing
```

SELinux が **Permissive** の場合は、**Enforcing** に設定します。

```
# setenforce 1
```

SELinux が実行されていない場合は有効にします。Red Hat Customer Portal にある、ご使用の OS バージョンの Red Hat Enterprise Linux の製品ドキュメント 内の **基本システム設定の設定** ガイド内の **セキュリティー強化ガイド** 内の **SELinux の使用ガイド** を参照してください。

各 Ceph デーモンは 1 つ以上のポートを使用して、Red Hat Ceph Storage クラスターの他のデーモンと通信します。場合によっては、デフォルトのポート設定を変更することができます。通常、管理者は Ceph Object Gateway または **ceph-radosgw** デーモンのデフォルトのポートのみを変更します。

表5.1 Ceph ポート

TCP/UDP ポート	デーモン	設定オプション
6789、3300	**ceph-mon**	該当なし
6800-7300	**ceph-osd**	**ms_bind_port_min** から **ms_bind_port_max**
6800-7300	**ceph-mgr**	**ms_bind_port_min** から **ms_bind_port_max**
6800	**ceph-mds**	該当なし
8080	**ceph-radosgw**	**rgw_frontends**

Ceph Storage クラスターのデーモンには、**ceph-mon**、**ceph-mgr**、および **ceph-osd** が含まれます。これらのデーモンとそのホストは、Ceph クラスターのセキュリティーゾーンで設定されます。このゾーンは、強化目的で独自のサブネットを使用する必要があります。

Ceph クライアントには、**ceph-radosgw**、**ceph-mds**、**ceph-fuse**、**libcephfs**、**rbd**、**librbd**、および **librados** が含まれます。これらのデーモンとそのホストは、強化目的で独自のサブネットを使用するストレージアクセスのセキュリティーゾーンで設定されます。

Ceph Storage Cluster ゾーンのホストでは、Ceph クライアントを実行しているホストのみが Ceph Storage Cluster デーモンに接続できるようにすることを検討してください。以下に例を示します。

```
# 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> をゾーン名に、**<ipaddress>** を IP アドレスに、**<netmask>** を CIDR 表記のサブネットマスクに、**<port-number>** をポート番号または範囲に置き換えます。**--permanent** フラグを使用してプロセスを繰り返し、再起動後も変更が維持されるようにします。以下に例を示します。

```
# 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. REPORTING

Red Hat Ceph Storage は、基本的なシステム監視を提供し、**ceph-mgr** デーモンプラグイン (RESTful API、ダッシュボード、その他のプラグイン (**Prometheus** や **Zendix** など)) と共にレポートします。Ceph は、設定、設定の詳細、および統計情報を取得する **collectd** およびソケットを使用してこの情報を収集を取得します。

システム管理者は、デフォルトのシステム動作以外に、**IP-Tables** プラグインまたは **ConnTrack** プラグインを、オープンポートと接続を追跡するように、セキュリティー上の問題について報告するように **collectd** を設定することもできます。

システム管理者は、ランタイム時に設定を取得することもできます。**ランタイム時の Ceph 設定の表示** を参照してください。

5.5. 管理者アクションの監査

システムセキュリティーの重要な要素として、クラスター上で管理者のアクションを定期的に監査することが挙げられます。Red Hat Ceph Storage は、管理者アクションの履歴を **/var/log/ceph/CLUSTER_FSID/ceph.audit.log** ファイルに保存します。モニターホスト上で次のコマンドを実行します。

例

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

各エントリーには以下が含まれます。

- **タイムスタンプ**: コマンドが実行されるタイミングを示します。
- **監視アドレス**: 変更したモニターを識別します。

- **クライアント:** 変更を開始するクライアントノードを特定します。
- **エンティティー:** 変更を行うユーザーを識別します。
- **コマンド:** 実行したコマンドを特定します。

以下は Ceph 監査ログの出力です。

```
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
```

Ceph などの分散システムでは、アクションが 1 つのインスタンスで開始し、クラスター内の他のノードに伝播される可能性があります。アクションが開始すると、ログは **dispatch** を示します。アクションが終了すると、ログは **finished** したことを示します。

第6章 データの保持

Red Hat Ceph Storage はユーザーデータを保存しますが、通常は間接的な方法になります。顧客データの保持には、Red Hat OpenStack Platform などのその他のアプリケーションが必要になる場合があります。

6.1. CEPH STORAGE CLUSTER

Ceph Storage Cluster (Reliable Autonomic Distributed Object Store または RADOS と呼ばれることもあります) は、データをオブジェクトとしてプール内に保存します。ほとんどの場合、これらのオブジェクトは Ceph Block Device イメージ、Ceph Object Gateway オブジェクト、Ceph ファイルシステムファイルなどのクライアントデータを表すアトミック単位です。ただし、**librados** 上に構築されたカスタムアプリケーションは、プールにバインドされ、データも保存される可能性があります。

Cephx は、オブジェクトデータを格納しているプールへのアクセスを制御します。ただし、Ceph Storage Cluster ユーザーは、通常 Ceph クライアントであり、ユーザーではありません。そのため、通常、ユーザーは Ceph Storage クラスタープールでオブジェクトを直接書き込み、読み取り、または削除する機能が**ありません**。

6.2. CEPH ブロックデバイス

Red Hat Ceph Storage の最もよく使われる Ceph Block Device インターフェイス (RADOS Block Device または RBD とも呼ばれる) は、仮想ボリューム、イメージ、コンピュートインスタンスを作成し、プール内に一連のオブジェクトとして保存します。Ceph は、これらのオブジェクトを配置グループに割り当て、クラスター全体の OSD に疑似ランダムに分散または配置します。

Ceph Block Device インターフェイスを使用するアプリケーションによっては、通常 Red Hat OpenStack Platform のユーザーがボリュームとイメージを作成、変更、および削除することができます。Ceph は、個々のオブジェクトの作成、取得、更新、および削除の操作を処理します。

ボリュームとイメージを削除すると、回復不能な方法で対応するオブジェクトを破棄します。ただし、上書きされるまで、データアーティファクトはストレージメディアに引き続き存在する可能性があります。データはバックアップアーカイブのままになる可能性があります。

6.3. CEPH ファイルシステム

Ceph File System インターフェイスは仮想ファイルシステムを作成し、プール内の一連のオブジェクトとして保存します。Ceph は、これらのオブジェクトを配置グループに割り当て、クラスター全体の OSD に疑似ランダムに分散または配置します。

通常、Ceph File System は 2 つのプールを使用します。

- **メタデータ:** メタデータプールには、Ceph Metadata Server (MDS) のデータが格納されます。MDS は通常、i ノードで設定されます。つまり、ファイルの所有権、アクセス許可、作成日時、最終更新日またはアクセス日時、親ディレクトリーなどです。

- **data:** データプールはファイルデータを保存します。Ceph はファイルを 1 つまたは複数のオブジェクトとして保存し、通常はエクステントなどのファイルデータのチャンクを表すことができます。

Ceph ファイルシステムインターフェイス (通常は Red Hat OpenStack Platform) を使用するアプリケーションに応じて、ユーザーは Ceph ファイルシステムでファイルを作成、変更、および削除できます。Ceph は、ファイルを表す個々のオブジェクトの作成、取得、更新、および削除の操作を処理します。

ファイルを削除すると、回復できない方法で対応するオブジェクトが削除されます。ただし、上書きされるまで、データアーティファクトはストレージメディアに引き続き存在する可能性があります。データはバックアップアーカイブのままになる可能性があります。

6.4. CEPH OBJECT GATEWAY

データセキュリティーおよび保持の観点から、Ceph Object Gateway インターフェイスには Ceph Block Device および Ceph Filesystem インターフェイスと比較すると、いくつかの重要な違いがあります。Ceph Object Gateway はユーザーにサービスを提供します。Ceph Object Gateway は以下を保存できます。

- **ユーザー認証情報:** ユーザー認証情報は通常、ユーザー ID、ユーザーアクセスキー、およびユーザーシークレットで設定されます。また、提供された場合は、ユーザー名とメールアドレスを設定することもできます。Ceph Object Gateway は、ユーザーが明示的にシステムから削除しない限り、ユーザー認証データを保持します。

- **ユーザーデータ:** ユーザーデータは通常、ユーザーまたは管理者が作成したバケットまたはコンテナーと、内部にユーザーが作成した S3 または Swift オブジェクトで設定されます。Ceph Object Gateway インターフェイスは、各 S3 または Swift オブジェクトに 1 つ以上の Ceph Storage クラスターオブジェクトを作成し、対応する Ceph Storage クラスターオブジェクトをデータプールに保存します。Ceph は、Ceph Storage クラスターオブジェクトを配置グループに割り当て、クラスター全体の OSD に疑似ランダムに分散または配置します。Ceph Object Gateway は、バケットまたはインデックスに含まれるオブジェクトのインデックスも保存し、S3 バケットまたは Swift コンテナーの内容のリスト表示などのサービスを有効にします。また、マルチパートアップロードを実装する際に、Ceph Object Gateway は S3 または Swift オブジェクトの部分的なアップロードを一時的に保存する可能性があります。
  ユーザーは、バケットまたはコンテナー、およびそれらに含まれるオブジェクトを Ceph Object Gateway で作成、変更、および削除できます。Ceph は、S3 または Swift オブジェクトを表す各 Ceph Storage クラスターオブジェクトの作成、取得、更新、削除の操作を処理します。

  S3 または Swift オブジェクトを削除すると、回復不能な方法で対応する Ceph Storage クラスターオブジェクトが破棄されます。ただし、上書きされるまで、データアーティファクトはストレージメディアに引き続き存在する可能性があります。データはバックアップアーカイブのままになる可能性があります。

- **ログ:** Ceph Object Gateway は、ユーザーが実行しようとしているユーザー操作と実行された操作のログも保存します。このデータは、バケットまたはコンテナー、あるいは S3 バケットまたは Swift コンテナーに存在する S3 または Swift オブジェクトを誰が作成、変更、または削除したかについてのトレーサビリティーを提供します。ユーザーがデータを削除する際、ロギング情報は影響を受けず、システム管理者によって削除されるか、期限切れのポリシーによって自動的に削除されるまでストレージが保持されます。

バケットライフサイクル

Ceph Object Gateway は、オブジェクトの有効期限を含むバケットライフサイクル機能もサポートします。General Data Protection Regulation のようなデータの保持規制により、管理者はオブジェクトの有効期限ポリシーを設定し、その他のコンプライアンス要素間でユーザーに開示することが必要になる場合があります。

マルチサイト

Ceph Object Gateway は、多くの場合、マルチサイトコンテキストにデプロイされます。これにより、ユーザーは 1 つのサイトにオブジェクトを格納し、Ceph Object Gateway は、別の地理的な場所にある別のクラスターにオブジェクトのレプリカを作成します。たとえば、プライマリークラスターが失敗した場合、セカンダリークラスターは操作を再開できます。別の例では、セカンダリークラスターは、エッジネットワークやコンテンツ再配信ネットワークなど、異なる地理的な位置にある場合がありま

す。たとえば、クライアントが最も近いクラスターにアクセスして、応答時間、スループット、およびその他のパフォーマンスの特性を改善することができます。マルチサイトのシナリオでは、管理者は各サイトがセキュリティー対策を実装することを確認する必要があります。また、マルチサイトのシナリオでデータの地理的な配布が発生する場合、管理者はデータ間の境界線上にある場合に規制上の影響について認識する必要があります。

第7章 FIPS (FEDERAL INFORMATION PROCESSING STANDARD)

Red Hat Ceph Storage は、最新の認定済み Red Hat Enterprise Linux バージョンで実行する場合、FIPS 検証済みの暗号化モジュールを使用します。

- システムのインストール時またはインストール後に、Red Hat Enterprise Linux で FIPS モードを有効にします。
  - コンテナーのデプロイメントについては、**Red Hat Enterprise Linux 9 セキュリティーおよび強化機能ガイド** の説明に従ってください。

関連情報

- **米国の各種の標準仕様** を参照し、FIPS 検証に関する最新情報を確認してください。
- **Red Hat Ceph Storage 互換性ガイド** を参照してください。

第8章 概要

本書は、Red Hat Ceph Storage のセキュリティーに関する一般的な概要のみを提供しています。さらにヘルプが必要な場合は、Red Hat Ceph Storage コンサルティングチームにお問い合わせください。