Red Hat Ceph Storage 4

Ceph Object Gateway を使用した Keystone の使用ガイド

OpenStack と Ceph Object Gateway がユーザー認証に Keystone を使用するように設定

Last Updated: 2023-02-19

Red Hat Ceph Storage 4 Ceph Object Gateway を使用した Keystone の使用ガイド

OpenStack と Ceph Object Gateway がユーザー認証に Keystone を使用するように設定

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.

法律上の通知

概要

本書では、OpenStack および Ceph Object Gateway がユーザー認証に Keystone を使用するように設定する方法を説明します。 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、弊社の CTO、Chris Wright のメッセージを参照してください。

目次

第1章 KEYSTONE 認証および CEPH OBJECT GATEWAY

OpenStack Keystone を使用してユーザーを認証する組織では、Keystone と Ceph Object Gateway を統合することができます。Ceph Object Gateway は、ゲートウェイが Keystone トークンを受け入れ、ユーザーを認証して対応する Ceph Object Gateway ユーザーを作成できるようにします。Keystone がトークンを検証すると、ゲートウェイはユーザーが認証されたを見なします。

利点

- Keystone でユーザーの管理
- Ceph Object Gateway でのユーザーの自動作成
- Ceph Object Gateway は Keystone に対して、取り消されたトークンの一覧を定期的にクエリーします。

第2章 CEPH OBJECT GATEWAY 用 OPENSTACK の KEYSTONE の設定

ストレージ管理者は、OpenStack の Keystone 認証サービスを使用して、Ceph Object Gateway 経由でユーザーを認証することができます。Ceph Object Gateway を設定する前に、Swift サービスを有効にして Ceph Object Gateway を指定するように Keystone を設定する必要があります。

2.1. 前提条件

- 実行中の Red Hat OpenStack Platform 環境
- 稼働中の Red Hat Ceph Storage 環境
- 実行中の Ceph Object Gateway 環境。

2.2. SWIFT サービスの作成

Ceph Object Gateway を設定する前に、Swift サービスを有効にして Ceph Object Gateway を指定するように Keystone を設定します。

前提条件

- 稼働中の Red Hat Ceph Storage クラスター
- Ceph ソフトウェアリポジトリーへのアクセス
- OpenStack コントローラーノードへの root レベルのアクセス。

手順

1. Swift サービスを作成します。

```
[root@swift~]# openstack service create --name=swift --description="Swift Service" object-store
```

このサービスを作成すると、サービス設定がエコーされます。

表2.1 例

フィールド	値
description	Swift サービス
enabled	True
id	37c4c0e79571404cb4644201a4a6e5ee
name	swift
type	object-store

2.3. CEPH OBJECT GATEWAY エンドポイントの設定

Swift サービスを作成したら、サービスを Ceph Object Gateway に指定します。

前提条件

- 稼働中の Red Hat Ceph Storage クラスター
- Ceph ソフトウェアリポジトリーへのアクセス
- Red Hat OpenStack Platform 13、15、または 16 の環境で稼働している Swift サービス

手順

1. Ceph Object Gateway を指定する OpenStack エンドポイントを作成します。

   構文

   ```
   openstack endpoint create --region REGION_NAME swift admin "URL"
   openstack endpoint create --region REGION_NAME swift public "URL"
   openstack endpoint create --region REGION_NAME swift internal "URL"
   ```

   REGION_NAME は、ゲートウェイのゾーングループ名またはリージョン名に置き換えます。**URL** は、Ceph Object Gateway に適した URL に置き換えます。

   例

   ```
   [root@osp ~]# openstack endpoint create --region us-west swift admin
   "http://radosgw.example.com:8080/swift/v1"
   [root@osp ~]# openstack endpoint create --region us-west swift public
   "http://radosgw.example.com:8080/swift/v1"
   [root@osp ~]# openstack endpoint create --region us-west swift internal
   "http://radosgw.example.com:8080/swift/v1"
   ```

フィールド	値
adminurl	**http://radosgw.example.com:8080/swift/v1**
id	**e4249d2b60e44743a67b5e5b38c18dd3**
internalurl	**http://radosgw.example.com:8080/swift/v1**
publicurl	**http://radosgw.example.com:8080/swift/v1**
region	**us-west**
service_id	**37c4c0e79571404cb4644201a4a6e5ee**

フィールド	値
service_name	**swift**
service_type	**object-store**

エンドポイントを設定すると、サービスエンドポイントの設定が出力されます。

2.4. OPENSTACK が CEPH OBJECT GATEWAY エンドポイントを使用していることを確認

Swift サービスを作成し、エンドポイントを設定したら、すべての設定が正しいことを確認します。

前提条件

- 稼働中の Red Hat Ceph Storage クラスター
- Ceph ソフトウェアリポジトリーへのアクセス

手順

1. 構成ファイルの設定を確認します。

```
[root@swift~]# openstack endpoint show object-store
```

エンドポイントを表示すると、エンドポイントの設定とサービス設定が表示されます。

表2.2 例

フィールド	値
adminurl	http://radosgw.example.com:8080/swift/v1
enabled	True
id	e4249d2b60e44743a67b5e5b38c18dd3
internalurl	http://radosgw.example.com:8080/swift/v1
publicurl	http://radosgw.example.com:8080/swift/v1
region	us-west
service_id	37c4c0e79571404cb4644201a4a6e5ee
service_name	swift
service_type	object-store

第3章 CEPH OBJECT GATEWAY の設定

ストレージ管理者は、Keystone サービスからの認証要求を受け入れるように Ceph Object Gateway を設定する必要があります。

3.1. 前提条件

- 実行中の Red Hat OpenStack Platform 環境
- 稼働中の Red Hat Ceph Storage 環境
- 実行中の Ceph Object Gateway 環境。

3.2. KEYSTONE SSL を使用するように CEPH OBJECT GATEWAY を設定

Keystone が使用する OpenSSL 証明書を変換すると、Ceph Object Gateway が Keystone と連携するように設定されます。Ceph Object Gateway が OpenStack の Keystone 認証と対話すると、Keystone は自己署名 SSL 証明書で終了します。

前提条件

- 稼働中の Red Hat Ceph Storage クラスター
- Ceph ソフトウェアリポジトリーへのアクセス

手順

1. OpenSSL 証明書を **nss db** 形式に変換します。

   例

   ```
   [root@osp ~]# mkdir /var/ceph/nss

   [root@osp ~]# mkdir /var/ceph/nss openssl x509 -in /etc/keystone/ssl/certs/ca.pem -pubkey |
   \
       certutil -d /var/ceph/nss -A -n ca -t "TCu,Cu,Tuw"
   [root@osp ~]# mkdir /var/ceph/nss openssl x509 -in /etc/keystone/ssl/certs/signing_cert.pem
   -pubkey | \
       certutil -A -d /var/ceph/nss -n signing_cert -t "P,P,P"
   ```

2. Ceph Object Gateway を実行しているノードに Keystone の SSL 証明書をインストールします。設定可能な **rgw_keystone_verify_ssl** の値を **false** に設定します。**rgw_keystone_verify_ssl** を **false** に設定すると、ゲートウェイは証明書の検証を試行しません。

3.3. KEYSTONE 認証を使用するように CEPH OBJECT GATEWAY を設定

OpenStack の Keystone 認証を使用するように Red Hat Ceph Storage を設定します。

前提条件

- 稼働中の Red Hat Ceph Storage クラスター

- Ceph ソフトウェアリポジトリーへのアクセス
- 実稼働環境への **admin** 権限

手順

1. 管理ノードの Ceph 設定ファイルを編集します。
2. **[client.radosgw.INSTANCE_NAME]** に移動します。ここで、**INSTANCE_NAME** は設定するゲートウェイインスタンスの名前です。
3. 各ゲートウェイインスタンスで以下を行います。
   a. **rgw_s3_auth_use_keystone** を **true** に設定します。
   b. **nss_db_path** 設定を、NSS データベースが保存されるパスに設定します。
4. 認証証明書を指定します。
   システム管理者が OpenStack サービスを設定する方法と同様に、OpenStack Identity API の v2.0 バージョン用の Keystone サービステナント、ユーザー、およびパスワードを設定することができます。ユーザー名とパスワードを指定することで、共有の秘密を **rgw_keystone_admin_token** 設定に提供するのを防ぎます。

重要

Red Hat は、実稼働環境で管理トークンによる認証を無効にすることを推奨します。サービステナントの認証情報には、**admin** 権限が必要です。

必要な設定オプションは以下のとおりです。

```
rgw_keystone_admin_user = KEYSTONE_TENANT_USER_NAME
rgw_keystone_admin_password = KEYSTONE_TENANT_USER_PASSWORD
rgw_keystone_admin_tenant = KEYSTONE_TENANT_NAME
```

Ceph Object Gateway ユーザーは Keystone の **tenant** にマッピングされます。Keystone ユーザーには、複数のテナントで異なるロールが割り当てられている可能性があります。Ceph Object Gateway がチケットを取得する際には、テナントと、そのチケットに割り当てられたユーザーロールを確認し、設定可能な **rgw_keystone_accepted_roles** に従って要求を受け入れるか拒否します。

通常の設定には、以下の設定があります。

例

```
[client.radosgw.gateway]
rgw_keystone_url = {keystone server url:keystone server admin port}
##Authentication using an admin token. Not preferred.
#rgw_keystone_admin_token = {keystone admin token}
##Authentication using username, password and tenant. Preferred.
rgw_keystone_admin_user = _KEYSTONE_TENANT_USER_NAME_
rgw_keystone_admin_password =  _KEYSTONE_TENANT_USER_PASSWORD_
rgw_keystone_admin_tenant =  _KEYSTONE_TENANT_NAME_
rgw_keystone_accepted_roles = _KEYSTONE_ACCEPTED_USER_ROLES_
##
rgw_keystone_token_cache_size = _NUMBER_OF_TOKENS_TO_CACHE_
```

```
rgw_keystone_revocation_interval =
_NUMBER_OF_SECONDS_BEFORE_CHECKING_REVOKED_TICKETS_
rgw_keystone_make_new_tenants =
_TRUE_FOR_PRIVATE_TENANT_FOR_EACH_NEW_USER_
rgw_s3_auth_use_keystone = true
nss_db_path = _PATH_TO_NSS_DB_
```

関連情報

- Red Hat OpenStack Platform 13 の**『ユーザーおよびアイデンティティー管理ガイド』**

3.4. CEPH OBJECT GATEWAY デーモンの再起動

Ceph Object Gateway を再起動すると、アクティブな設定変更を行う必要があります。

前提条件

- 稼働中の Red Hat Ceph Storage クラスター
- Ceph ソフトウェアリポジトリーへのアクセス
- 実稼働環境への **admin** 権限

手順

1. Ceph 設定ファイルを保存して各 Ceph ノードに分散したら、Ceph Object Gateway インスタンスを再起動します。

```
[root@ceph~]# systemctl restart ceph-radosgw
[root@ceph~]# systemctl restart ceph-radosgw@rgw.`hostname -s`
```

付録A KEYSTONE の統合設定オプション

設定オプションは Keystone に統合できます。利用可能な Keystone 統合設定オプションの詳細は、以下を参照してください。

重要

Ceph 設定ファイルを更新したら、新しい Ceph 設定ファイルをストレージクラスター内の全 Ceph ノードにコピーする必要があります。

rgw_s3_auth_use_keystone

詳細

true に設定すると、Ceph Object Gateway は Keystone を使用してユーザーを認証します。

型

ブール値

デフォルト

false

nss_db_path

詳細

NSS データベースへのパス。

型

文字列

デフォルト

""

rgw_keystone_url

詳細

Keystone サーバーの管理 RESTful API の URL。

型

文字列

デフォルト

""

rgw_keystone_admin_token

詳細

管理リクエストのために Keystone の内部に設定されるトークンまたは共有シークレット。

型

文字列

デフォルト

""

rgw_keystone_admin_user

詳細

keystone 管理ユーザー名

型

文字列

デフォルト

""

rgw_keystone_admin_password

詳細

keystone 管理ユーザーのパスワード。

型

文字列

デフォルト

""

rgw_keystone_admin_tenant

詳細

keystone v2.0 用の Keystone 管理ユーザーテナント。

型

文字列

デフォルト

""

rgw_keystone_admin_project

詳細

keystone v3 の Keystone 管理ユーザープロジェクト。

型

文字列

デフォルト

""

rgw_keystone_admin_domain

詳細

Keystone 管理ユーザードメイン。

型

文字列

デフォルト

""

rgw_keystone_api_version

詳細

使用する Keystone API のバージョン。有効なオプションは **2** または **3** です。

型

整数

デフォルト

2

rgw_keystone_accepted_roles

詳細

要求を提供するのに必要なロール。

型

文字列

デフォルト

"Member, admin"

rgw_keystone_accepted_admin_roles

詳細

ユーザーが管理者権限を取得できるようにするロールの一覧。

型

文字列

デフォルト

""

rgw_keystone_token_cache_size

詳細

Keystone トークンキャッシュのエントリーの最大数。

型

整数

デフォルト

10000

rgw_keystone_revocation_interval

詳細

トークン失効チェックの間隔 (秒単位)。

型

整数

デフォルト

15 * 60

rgw_keystone_verify_ssl

詳細

true の場合、Ceph は Keystone の SSL 証明書を確認します。

型

ブール値

デフォルト

true

rgw_keystone_implicit_tenants

詳細

同じ名前の独自のテナントに新しいユーザーを作成します。ほとんどの場合は、**true** または **false** に設定します。以前のバージョンの Red Hat Ceph Storage との互換性を確保するには、これを **s3** または **swift** に設定することもできます。これにより、ID 領域を分割し、指定されたプロトコルのみが暗黙的なテナントを使用します。Red Hat Ceph Storage の古いバージョンの一部は、Swift を使用する暗黙的なテナントのみをサポートします。

型

文字列

デフォルト

false