Red Hat Ceph Storage 3

Keystone を使用した認証 Ceph Object Gateway ユーザーの使用

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: 2021-09-15

Red Hat Ceph Storage 3 Keystone を使用した認証 Ceph Object Gateway ユーザーの使用

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。

目次

前書き

組織で OpenStack Keystone を使用してユーザーを認証する場合に、Keystone と Ceph Object Gateway を統合できます。これにより、ゲートウェイは Keystone トークンを受け入れてユーザーを認証し、対応する Ceph Object Gateway ユーザーを作成できます。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。

次の利点があります。

- Keystone でのユーザーの管理
- 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1章 OPENSTACK の設定

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。

1.1. SWIFT サービスの作成

OpenStack を使用して Swift ユーザーを検証するには、まず Swift サービスを作成します。

```
# 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。以下に例を示します。

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

1.2. エンドポイントの設定

Swift サービスを作成したら、Ceph Object Gateway を参照します。**{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。exemplary URL は、Ceph Object Gateway に適した URL に置き換えます。

```
# openstack endpoint create --region {region-name} \
    --publicurl   "http://radosgw.example.com:8080/swift/v1" \
    --adminurl    "http://radosgw.example.com:8080/swift/v1" \
    --internalurl "http://radosgw.example.com:8080/swift/v1" \
    swift
```

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処理されます。以下に例を示します。

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

フィールド	値
region	us-west
service_id	37c4c0e79571404cb4644201a4a6e5ee
service_name	swift
service_type	object-store

1.3. 設定の確認

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。

```
# 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。以下に例を示します。

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2章 CEPH OBJECT GATEWAY の設定

2.1. SSL の設定

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。

```
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"
openssl x509 -in /etc/keystone/ssl/certs/signing_cert.pem -pubkey | \
    certutil -A -d /var/ceph/nss -n signing_cert -t "P,P,P"
```

Ceph Object Gateway が Keystone と対話できるように、自己署名の SSL 証明書で OpenStack Keystone を終了することもできます。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するか、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。

2.2. CIVETWEB の設定

Ceph Object Gateway が Keystone を使用するように設定するには、管理ノードで Ceph 設定ファイルを開き、**[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に置き換えます。ゲートウェイインスタンスごとに、**rgw_s3_auth_use_keystone** の設定を **true** に設定し、NSS データベースが保存されるパスに **nss_db_path** を設定します。

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。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。詳細は、『Red Hat OpenStack Platform 13 の Users and Identity Management Guide』を参照してください。必要な設定オプションは以下のとおりです。

```
rgw_keystone_admin_user = {keystone service tenant user name}
rgw_keystone_admin_password = {keystone service tenant user password}
rgw_keystone_admin_tenant = {keystone service 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。

```
[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 service tenant user name}
rgw_keystone_admin_password = {keystone service tenant user password}
rgw_keystone_admin_tenant = {keystone service tenant name}
rgw_keystone_accepted_roles = {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}
```

変更を Ceph 設定ファイルに保存します。次に、更新した Ceph 設定ファイルを各 Ceph ノードにコピーします。以下に例を示します。

```
# scp /etc/ceph/ceph.conf <node-name>:/etc/ceph/
```

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。

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

2.3. CHIVETWEB の再起動

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。使用方法は、以下のいずれかでなければなりません。

```
# systemctl restart ceph-radosgw
# systemctl restart ceph-radosgw@rgw.`hostname -s`
```