Red Hat Ceph Storage 4

Using Keystone with the Ceph Object Gateway Guide

Configuring OpenStack and the Ceph Object Gateway to use Keystone for user authentication.

Last Updated: 2021-09-08

Red Hat Ceph Storage 4 Using Keystone with the Ceph Object Gateway Guide

Configuring OpenStack and the Ceph Object Gateway to use Keystone for user authentication.

Legal Notice

Abstract

This document describes how to configure OpenStack and the Ceph Object Gateway to use Keystone for user authentication. Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

Table of Contents

CHAPTER 1. KEYSTONE AUTHENTICATION AND THE CEPH OBJECT GATEWAY

Organizations using OpenStack Keystone to authenticate users can integrate Keystone with the Ceph Object Gateway. The Ceph Object Gateway enables the gateway to accept a Keystone token, authenticate the user and create a corresponding Ceph Object Gateway user. When Keystone validates a token, the gateway considers the user authenticated.

Benefits

- Managing users with Keystone
- Automatic User Creation in the Ceph Object Gateway
- The Ceph Object Gateway will query Keystone periodically for a list of revoked tokens.

CHAPTER 2. CONFIGURING OPENSTACK'S KEYSTONE FOR THE CEPH OBJECT GATEWAY

As a storage administrator, you can use OpenStack's Keystone authentication service to authenticate users through the Ceph Object Gateway. Before you can configure the Ceph Object Gateway, you must configure Keystone which will enable the Swift service and point to the Ceph Object Gateway.

2.1. PREREQUISITES

- A running Red Hat OpenStack Platform 13, 15, or 16 environment.
- A running Red Hat Ceph Storage environment.
- A running Ceph Object Gateway environment.

2.2. CREATING THE SWIFT SERVICE

Before configuring the Ceph Object Gateway, configure Keystone so that the Swift service is enabled and pointing to the Ceph Object Gateway.

Prerequisites

- A running Red Hat Ceph Storage cluster.
- Access to the Ceph software repository.
- Root-level access to OpenStack controller node.

Procedure

1. Create the Swift service:

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

Creating the service will echo the service settings.

Table 2.1. Example

Field	Value
description	Swift Service
enabled	True
id	37c4c0e79571404cb4644201a4a6e5ee
name	swift
type	object-store

2.3. SETTING THE CEPH OBJECT GATEWAY ENDPOINTS

After creating the Swift service, point the service to a Ceph Object Gateway.

Prerequisites

- A running Red Hat Ceph Storage cluster.
- Access to the Ceph software repository.
- A running Swift service on a Red Hat OpenStack Platform 13, 15, or 16 environment.

Procedure

1. Create the OpenStack endpoints pointing to the Ceph Object Gateway:

Syntax

```
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"
```

Replace *REGION_NAME* with the name of the gateway's zone group name or region name. Replace *URL* with URLs appropriate for the Ceph Object Gateway.

Example

```
[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"
```

Field	Value
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**

Field	Value
service_name	**swift**
service_type	**object-store**

Setting the endpoints will output the service endpoint settings.

2.4. VERIFYING OPENSTACK IS USING THE CEPH OBJECT GATEWAY ENDPOINTS

After creating the Swift service and setting the endpoints, show the endpoints to ensure that all settings are correct.

Prerequisites

- A running Red Hat Ceph Storage cluster.
- Access to the Ceph software repository.

Procedure

1. Verify settings in the configuration file:

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

Showing the endpoints will echo the endpoints settings, and the service settings.

Table 2.2. Example

Field	Value
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

Field	Value
service_type	object-store

CHAPTER 3. CONFIGURING THE CEPH OBJECT GATEWAY

As a storage administrator, you must configure the Ceph Object Gateway to accept authentication requests from the Keystone service.

3.1. PREREQUISITES

- A running Red Hat OpenStack Platform 13, 15, or 16 environment.
- A running Red Hat Ceph Storage environment.
- A running Ceph Object Gateway environment.

3.2. CONFIGURING THE CEPH OBJECT GATEWAY TO USE KEYSTONE SSL

Converting the OpenSSL certificates that Keystone uses configures the Ceph Object Gateway to work with Keystone. When the Ceph Object Gateway interacts with OpenStack's Keystone authentication, Keystone will terminate with a self-signed SSL certificate.

Prerequisites

- A running Red Hat Ceph Storage cluster.
- Access to the Ceph software repository.

Procedure

1. Convert the OpenSSL certificate to the **nss db** format:

   #### Example

   ```
   [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. Install Keystone's SSL certificate in the node running the Ceph Object Gateway. Alternatively set the value of the configurable **rgw_keystone_verify_ssl** setting to **false**.
   Setting **rgw_keystone_verify_ssl** to **false** means that the gateway won't attempt to verify the certificate.

3.3. CONFIGURING THE CEPH OBJECT GATEWAY TO USE KEYSTONE AUTHENTICATION

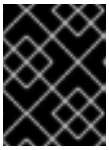
Configure the Red Hat Ceph Storage to use OpenStack's Keystone authentication.

Prerequisites

- A running Red Hat Ceph Storage cluster.
- Access to the Ceph software repository.
- **admin** privileges to the production environment.

Procedure

1. Edit the Ceph configuration file on the admin node.
2. Navigate to the **[client.radosgw.*INSTANCE_NAME*]**, where *INSTANCE_NAME* is the name of the Gateway instance to configure.
3. Do the following for each gateway instance:
   a. Set the **rgw_s3_auth_use_keystone** setting to **true**.
   b. Set the **nss_db_path** setting to the path where the NSS database is stored.
4. Provide authentication credentials:
   It is possible to configure a Keystone service tenant, user and password for keystone for v2.0 version of the OpenStack Identity API, similar to the way system administrators tend to configure OpenStack services. Providing a username and password avoids providing the shared secret to the **rgw_keystone_admin_token** setting.



IMPORTANT

Red Hat recommends disabling authentication by admin token in production environments. The service tenant credentials should have **admin** privileges.

The necessary configuration options are:

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

A Ceph Object Gateway user is mapped into a Keystone **tenant**. A Keystone user has different roles assigned to it on possibly more than a single tenant. When the Ceph Object Gateway gets the ticket, it looks at the tenant, and the user roles that are assigned to that ticket, and accepts or rejects the request according to the **rgw_keystone_accepted_roles** configurable.

A typical configuration might have the following settings:

Example

```
[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_
```

Additional Resources

- *Users and Identity Management Guide* for Red Hat OpenStack Platform 13.
- *Users and Identity Management Guide* for Red Hat OpenStack Platform 15.
- *Users and Identity Management Guide* for Red Hat OpenStack Platform 16.

3.4. RESTARTING THE CEPH OBJECT GATEWAY DAEMON

Restarting the Ceph Object Gateway must be done to active configuration changes.

Prerequisites

- A running Red Hat Ceph Storage cluster.
- Access to the Ceph software repository.
- **admin** privileges to the production environment.

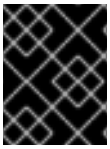
Procedure

1. Once you have saved the Ceph configuration file and distributed it to each Ceph node, restart the Ceph Object Gateway instances:

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

APPENDIX A. KEYSTONE INTEGRATION CONFIGURATION OPTIONS

You can integrate your configuration options into Keystone. See below for a detailed description of the available Keystone integration configuration options:



IMPORTANT

After updating the Ceph configuration file, you must copy the new Ceph configuration file to all Ceph nodes in the storage cluster.

rgw_s3_auth_use_keystone

Description

If set to **true**, the Ceph Object Gateway will authenticate users using Keystone.

Type

Boolean

Default

false

nss_db_path

Description

The path to the NSS database.

Type

String

Default

""

rgw_keystone_url

Description

The URL for the administrative RESTful API on the Keystone server.

Type

String

Default

""

rgw_keystone_admin_token

Description

The token or shared secret that is configured internally in Keystone for administrative requests.

Type

String

Default

""

rgw_keystone_admin_user

Description

The keystone admin user name.

Type

String

Default

""

rgw_keystone_admin_password

Description

The keystone admin user password.

Type

String

Default

""

rgw_keystone_admin_tenant

Description

The Keystone admin user tenant for keystone v2.0.

Type

String

Default

""

rgw_keystone_admin_project

Description

The Keystone admin user project for keystone v3.

Type

String

Default

""

rgw_keystone_admin_domain

Description

The Keystone admin user domain.

Type

String

Default

""

rgw_keystone_api_version

Description

The version of the Keystone API to use. Valid options are **2** or **3**.

Type

Integer

Default

2

rgw_keystone_accepted_roles

Description

The roles required to serve requests.

Type

String

Default

"Member, admin"

rgw_keystone_accepted_admin_roles

Description

The list of roles allowing a user to gain administrative privileges.

Type

String

Default

""

rgw_keystone_token_cache_size

Description

The maximum number of entries in the Keystone token cache.

Type

Integer

Default

10000

rgw_keystone_revocation_interval

Description

The number seconds between tokens revocation check.

Type

Integer

Default

15 * 60

rgw_keystone_verify_ssl

Description

If **true** Ceph will try to verify Keystone's SSL certificate.

Type

Boolean

Default

true

rgw_keystone_implicit_tenants

Description

Create new users in their own tenants of the same name. Set this to **true** or **false** under most circumstances. For compatibility with previous versions of Red Hat Ceph Storage, it is also possible to set this to **s3** or **swift**. This has the effect of splitting the identity space such that only the indicated protocol will use implicit tenants. Some older versions of Red Hat Ceph Storage only supported implicit tenants with Swift.

Type

String

Default

false