Red Hat Ceph Storage 4

将 Keystone 与 Ceph 对象网关使用指南

配置 OpenStack 和 Ceph 对象网关，以使用 Keystone 进行用户身份验证。

Last Updated: 2021-09-16

Red Hat Ceph Storage 4 将 Keystone 与 Ceph 对象网关使用指南

配置 OpenStack 和 Ceph 对象网关，以使用 Keystone 进行用户身份验证。

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.

法律通告

摘要

本文档介绍如何配置 OpenStack 和 Ceph 对象网关，以使用 Keystone 进行用户身份验证。 红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。详情请查看 CTO Chris Wright 信息。

目录

第 1 章 KEYSTONE 身份验证和 CEPH 对象网关 3

第 2 章 为 CEPH 对象网关配置 OPENSTACK KEYSTONE 4
2.1. 先决条件 4
2.2. 创建 SWIFT 服务 4
2.3. 设置 CEPH 对象网关端点 4
2.4. 验证 OPENSTACK 使用 CEPH 对象网关端点 6

第 3 章 配置 CEPH 对象网关 7
3.1. 先决条件 7
3.2. 配置 CEPH 对象网关以使用 KEYSTONE SSL 7
3.3. 配置 CEPH 对象网关以使用 KEYSTONE 身份验证 7
3.4. 重启 CEPH 对象网关守护进程 9

附录 A. KEYSTONE 集成配置选项 10

第 1 章 KEYSTONE 身份验证和 CEPH 对象网关

使用 OpenStack Keystone 验证用户身份的组织可以将 Keystone 与 Ceph 对象网关集成。Ceph 对象网关使得网关能够接受 Keystone 令牌，对用户进行身份验证，并且创建对应的 Ceph 对象网关用户。当 Keystone 验证令牌时，网关将考虑用户经过身份验证。

优点

- 使用 Keystone 管理用户
- 在 Ceph 对象网关中自动创建用户
- Ceph 对象网关将定期查询 Keystone，以获取已撤销令牌的列表。

第 2 章 为 CEPH 对象网关配置 OPENSTACK KEYSTONE

作为存储管理员，您可以使用 OpenStack 的 Keystone 身份验证服务通过 Ceph 对象网关对用户进行身份验证。在您配置 Ceph 对象网关之前，您必须配置 Keystone，以启用 Swift 服务并指向 Ceph 对象网关。

2.1. 先决条件

- 正在运行的红帽 OpenStack 平台 13、15 或 16 环境。
- 正在运行的红帽 Ceph 存储环境。
- 正在运行的 Ceph 对象网关环境。

2.2. 创建 SWIFT 服务

在配置 Ceph 对象网关之前，请配置 Keystone，使 Swift 服务已启用并指向 Ceph 对象网关。

先决条件

- 一个正在运行的 Red Hat Ceph Storage 集群。
- 访问 Ceph 软件存储库。
- OpenStack 控制器节点的根级别访问权限.

流程

1. 创建 Swift 服务：

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

创建服务将回显服务设置。

表 2.1. 示例

字段	值
description	Swift 服务
enabled	True
id	37c4c0e79571404cb4644201a4a6e5ee
name	swift
type	object-store

2.3. 设置 CEPH 对象网关端点

在创建了 Swift 服务后，将服务指向 Ceph 对象网关。

先决条件

- 一个正在运行的 Red Hat Ceph Storage 集群。
- 访问 Ceph 软件存储库。
- 在红帽 OpenStack 平台 13、15 或 16 环境上运行 Swift 服务。

流程

1. 创建指向 Ceph 对象网关的 OpenStack 端点：

   语法

   ```
   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"
   ```

   将 *REGION_NAME* 替换为网关的 zone group name 或 region 名称的名称。使用适合 Ceph 对象网关的 *URL* 替换 URL。

   示例

   ```
   [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"
   ```

字段	值
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**
service_name	**swift**
service_type	**object-store**

设置端点将输出服务端点设置。

2.4. 验证 OPENSTACK 使用 CEPH 对象网关端点

创建 Swift 服务并设置端点后，请显示端点以确保所有设置都正确。

先决条件

- 一个正在运行的 Red Hat Ceph Storage 集群。
- 访问 Ceph 软件存储库。

流程

1. 验证配置文件中的设置：

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

显示端点将回显端点设置和服务设置。

表 2.2. 示例

字段	值
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 配置 CEPH 对象网关

作为存储管理员，您必须配置 Ceph 对象网关，以接受来自 Keystone 服务的身份验证请求。

3.1. 先决条件

- 正在运行的红帽 OpenStack 平台 13、15 或 16 环境。
- 正在运行的红帽 Ceph 存储环境。
- 正在运行的 Ceph 对象网关环境。

3.2. 配置 CEPH 对象网关以使用 KEYSTONE SSL

转换 Keystone 使用的 OpenSSL 证书，配置 Ceph 对象网关以搭配 Keystone 使用。当 Ceph 对象网关与 OpenStack 的 Keystone 身份验证交互时，Keystone 将终止自签名 SSL 证书。

先决条件

- 一个正在运行的 Red Hat Ceph Storage 集群。
- 访问 Ceph 软件存储库。

流程

1. 将 OpenSSL 证书转换为 **db** 格式：

   示例

   ```
   [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. 在运行 Ceph 对象网关的节点中安装 Keystone 的 SSL 证书。或者，将可配置的 **rgw_keystone_verify_ssl** 设置的值设置为 **false**。
   将 **rgw_keystone_verify_ssl** 设置为 **false** 表示网关不会尝试验证证书。

3.3. 配置 CEPH 对象网关以使用 KEYSTONE 身份验证

配置红帽 Ceph 存储，以使用 OpenStack 的 Keystone 身份验证。

先决条件

- 一个正在运行的 Red Hat Ceph Storage 集群。
- 访问 Ceph 软件存储库。
- 生产环境的管理 **特权**。

流程

1. 编辑管理节点上的 Ceph 配置文件。
2. 导航到 **[client.radosgw.*INSTANCE_NAME*],** 其中 *INSTANCE_NAME* 是要配置的网关实例的名称。
3. 为每个网关实例执行以下操作：
   a. 将 **rgw_s3_auth_use_keystone** 设置设置为 **true**。
   b. 将 **thenss_db_path** 设置设置为 NSS 数据库存储的路径。
4. 提供身份验证凭证：
   可以配置 Keystone 服务租户、适用于 OpenStack 身份 API 的 v2.0 版本的 Keystone 用户和密码，这与系统管理员倾向于配置 OpenStack 服务的方式类似。提供用户名和密码可避免向 **rgw_keystone_admin_token** 设置提供共享 secret。

重要

红帽建议在生产环境中通过 admin 令牌禁用身份验证。服务租户凭据应当具有 **admin** 特权。

所需的配置选项有：

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

Ceph 对象网关用户映射到 Keystone **租户**。Keystone 用户在 上分配有不同的角色，可能有多个租户。当 Ceph 对象网关获取票据时，它将查看租户，以及分配给该票据的用户角色，并且根据可配置的 **rgw_keystone_accepted_roles** 接受或拒绝请求。

典型的配置可能具有以下设置：

示例

```
[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_
```

其它资源

- 红帽 OpenStack 平台 13 *的用户和身份管理指南*.
- 红帽 OpenStack 平台 15 *用户和身份管理指南*.
- 红帽 OpenStack 平台 16 *的用户和身份管理指南*.

3.4. 重启 CEPH 对象网关守护进程

必须重新启动 Ceph 对象网关才能激活配置更改。

先决条件

- 一个正在运行的 Red Hat Ceph Storage 集群。
- 访问 Ceph 软件存储库。
- 生产环境的管理 **特权**。

流程

1. 保存 Ceph 配置文件并将其分发到每个 Ceph 节点后，重启 Ceph 对象网关实例：

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

附录 A. KEYSTONE 集成配置选项

您可以将您的配置选项集成到 Keystone 中。有关可用 Keystone 集成配置选项的详细信息，请参见以下：

重要

在更新 Ceph 配置文件后，您必须将新的 Ceph 配置文件复制到存储集群中的所有 Ceph 节点。

rgw_s3_auth_use_keystone

描述

如果设为 **true**，Ceph 对象网关将使用 Keystone 验证用户的身份。

类型

布尔值

默认

false

nss_db_path

描述

NSS 数据库的路径。

类型

字符串

默认

""

rgw_keystone_url

描述

Keystone 服务器上管理 RESTful API 的 URL。

类型

字符串

默认

""

rgw_keystone_admin_token

描述

Keystone 中为管理请求配置令牌或共享机密。

类型

字符串

默认

""

rgw_keystone_admin_user

描述

keystone admin 用户名。

类型

字符串

默认

""

rgw_keystone_admin_password

描述

keystone admin 用户密码.

类型

字符串

默认

""

rgw_keystone_admin_tenant

描述

keystone v2.0 的 Keystone admin 用户租户。

类型

字符串

默认

""

rgw_keystone_admin_project

描述

keystone v3 的 Keystone admin 用户项目。

类型

字符串

默认

""

rgw_keystone_admin_domain

描述

Keystone admin 用户域。

类型

字符串

默认

""

rgw_keystone_api_version

描述

要使用的 Keystone API 版本。有效选项为 **2** 或 **3**。

类型

整数

默认

2

rgw_keystone_accepted_roles

描述

为请求提供服务所需的角色。

类型

字符串

默认

"Member、admin"

rgw_keystone_accepted_admin_roles

描述

角色列表，允许用户获取管理特权。

类型

字符串

默认

""

rgw_keystone_token_cache_size

描述

Keystone 令牌缓存中条目的最大数量。

类型

整数

默认

10000

rgw_keystone_revocation_interval

描述

令牌撤销检查之间的秒数。

类型

整数

默认

15 * 60

rgw_keystone_verify_ssl

描述

如果为 **true**，Ceph 将尝试验证 Keystone 的 SSL 证书。

类型

布尔值

默认

true

rgw_keystone_implicit_tenants

描述

在自己的租户中创建新用户，它们的名称相同。在大多数情况下，**将它设置为 true** 或 **false**。若要与以前版本的红帽 Ceph 存储兼容，也可以将它设置为 **s3** 或 **swift**。这意味着拆分身份空间，使得只有指定的协议才会使用隐式租户。些较早版本的红帽 Ceph 存储仅支持 Swift 的隐式租户。

类型

字符串

默认

false