Red Hat OpenStack Platform 16.2

Deploy Fernet on the Overcloud

Deploy Fernet on the Red Hat OpenStack Platform overcloud

Last Updated: 2023-11-09

Red Hat OpenStack Platform 16.2 Deploy Fernet on the Overcloud

Deploy Fernet on the Red Hat OpenStack Platform overcloud

OpenStack Team
rhos-docs@redhat.com

Legal Notice

Abstract

Deploy Fernet on the Red Hat OpenStack Platform overcloud.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

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 .

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Tell us how we can make it better.

Providing documentation feedback in Jira

Use the Create Issue form to provide feedback on the documentation. The Jira issue will be created in the Red Hat OpenStack Platform Jira project, where you can track the progress of your feedback.

1. Ensure that you are logged in to Jira. If you do not have a Jira account, create an account to submit feedback.

2. Click the following link to open a the **Create Issue** page: Create Issue

3. Complete the **Summary** and **Description** fields. In the **Description** field, include the documentation URL, chapter or section number, and a detailed description of the issue. Do not modify any other fields in the form.

4. Click **Create**.

CHAPTER 1. USING FERNET KEYS FOR ENCRYPTION IN THE OVERCLOUD

Fernet is the default token provider, that replaces **uuid**. You can review your Fernet deployment and rotate the Fernet keys. Fernet uses three types of keys, which are stored in **/var/lib/config-data/puppet-generated/keystone/etc/keystone/fernet-keys**. The highest-numbered directory contains the primary key, which generates new tokens and decrypts existing tokens.

Fernet key rotation uses the following process:

1. The primary key becomes the secondary key.
2. The <system> issues a new primary key. The outgoing primary key is no longer valid. You can use secondary keys to decrypt tokens that were associated with previous primary keys, but you cannot issue new tokens.

When you decide the length of Fernet key rotation cycles, follow the security posture of your organization. If your organization does not have guidance, a monthly rotation cycle is good practice for security reasons.

1.1. REVIEWING THE FERNET DEPLOYMENT

To test that Fernet tokens are working correctly, retrieve the IP address of the Controller node, SSH into the Controller node, and review the settings of the token driver and provider.

Procedure

1. Retrieve the IP address of the Controller node:

```
[stack@director ~]$ source ~/stackrc
[stack@director ~]$ openstack server list
--------------------------------------------------------------------------------------+
| ID                                   | Name                    | Status | Networks            |
--------------------------------------------------------------------------------------+
| 756fbd73-e47b-46e6-959c-e24d7fb71328 | overcloud-controller-0  | ACTIVE |
ctlplane=192.0.2.16 |
| 62b869df-1203-4d58-8e45-fac6cd4cfbee | overcloud-novacompute-0 | ACTIVE |
ctlplane=192.0.2.8  |
--------------------------------------------------------------------------------------+
```

2. SSH into the Controller node:

```
[heat-admin@overcloud-controller-0 ~]$ ssh heat-admin@192.0.2.16
```

3. Retrieve the values of the token driver and provider settings:

```
[heat-admin@overcloud-controller-0 ~]$ sudo crudini --get /var/lib/config-data/puppet-
generated/keystone/etc/keystone/keystone.conf token driver
sql
[heat-admin@overcloud-controller-0 ~]$ sudo crudini --get /var/lib/config-data/puppet-
generated/keystone/etc/keystone/keystone.conf token provider
fernet
```

4. Test the Fernet provider:

```
[heat-admin@overcloud-controller-0 ~]$ exit
[stack@director ~]$ source ~/overcloudrc
[stack@director ~]$ openstack token issue
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------+
| Field | Value |
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------+
| expires | 2016-09-20 05:26:17+00:00 |
| id | gAAAAABX4LppE8vaiFZ992eah2i3edpO1aDFxlKZq6a_RJzxUx56QVKORrmW0-oZK3-
Xuu2wcnpYq_eek2SGLz250eLpZOzxKBR0GsoMfxJU8mEFF8NzfLNcbuS-iz7SV-
N1re3XEywSDG90JcgwjQfXW-8jtCm-n3LL5IaZexAYIw059T_-cd8 |
| project_id | 26156621d0d54fc39bf3adb98e63b63d |
| user_id | 397daf32cadd490a8f3ac23a626ac06c |
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------+
```

The result includes the long Fernet token.

1.2. ROTATING THE FERNET KEYS BY USING THE WORKFLOW SERVICE

To ensure that the Fernet keys persist after stack updates, rotate the keys with the Workflow service (mistral). By default, director manages the overcloud Fernet keys in an environment file with the **ManageKeystoneFernetKeys** parameter. The Fernet keys are stored in the Workflow service, in the **KeystoneFernetKeys** section.

Procedure

1. Review the existing Fernet keys:

   a. Identify the Fernet key location. Log in to a Controller node as the heat-admin user and use the **crudini** command to query the Fernet keys:

   ```
   [stack@<undercloud_host> ~]$ ssh heat-admin@overcloud-controller-o
   [heat-admin@overcloud-controller-0 ~]$ sudo crudini --get /var/lib/config-data/puppet-generated/keystone/etc/keystone/keystone.conf fernet_tokens key_repository
   /etc/keystone/fernet-keys
   ```

   NOTE

   The **/etc/keystone/** directory refers to the container file system path.

   b. Inspect the current Fernet key directories:

   ```
   [heat-admin@overcloud-controller-0 ~]$ sudo ls /var/lib/config-data/puppet-generated/keystone/etc/keystone/fernet-keys
   0  1  2
   ```

   - **0** - Contains the staged key, which becomes the next primary key and is always numbered **0**.

- **1** - Contains the secondary key.
- **2** - Contains the primary key. This number increments each time that the keys rotate. The highest number always serves as the primary key.

NOTE

- The maximum number of keys is set with **max_active_keys** property. The default is 5 keys.
- The keys propagate across all Controller nodes.

2. Rotate the Fernet keys by using the **workflow** command:

```
[stack@director ~]$ source ~/stackrc
[stack@director ~]$ openstack workflow execution create
tripleo.fernet_keys.v1.rotate_fernet_keys {"container": "overcloud"}
------------------------------------------------------------+
| Field             | Value                                 |
------------------------------------------------------------+
| ID                | 58c9c664-b966-4f82-b368-af5ed8de5b47  |
| Workflow ID       | 78f0990a-3d34-4bf2-a127-10c149bb275c  |
| Workflow name     | tripleo.fernet_keys.v1.rotate_fernet_keys |
| Description       |                                       |
| Task Execution ID | <none>                                |
| State             | RUNNING                               |
| State info        | None                                  |
| Created at        | 2017-12-20 11:13:50                   |
| Updated at        | 2017-12-20 11:13:50                   |
------------------------------------------------------------+
```

Verification

1. Retrieve the ID and ensure that the workflow is successful.

```
[stack@director ~]$ openstack workflow execution show 58c9c664-b966-4f82-b368-
af5ed8de5b47
------------------------------------------------------------+
| Field             | Value                                 |
------------------------------------------------------------+
| ID                | 58c9c664-b966-4f82-b368-af5ed8de5b47  |
| Workflow ID       | 78f0990a-3d34-4bf2-a127-10c149bb275c  |
| Workflow name     | tripleo.fernet_keys.v1.rotate_fernet_keys |
| Description       |                                       |
| Task Execution ID | <none>                                |
| State             | SUCCESS                               |
| State info        | None                                  |
| Created at        | 2017-12-20 11:13:50                   |
| Updated at        | 2017-12-20 11:15:00                   |
------------------------------------------------------------+
```

2. On the Controller node, review the number of Fernet keys, and compare with the previous result.

```
[heat-admin@overcloud-controller-0 ~]$ sudo ls /var/lib/config-data/puppet-
generated/keystone/etc/keystone/fernet-keys
0  1  2  3
```

- **0** - Contains the staged key and always be numbered **0**. This key becomes a primary key during the next rotation.
- **1 & 2** - Contain the secondary keys.
- **3** - Contains the primary key. This number increments each time the keys rotate. The highest number always serves as the primary key.

NOTE

- The maximum number of keys is set with the **max_active_keys** property. The default is 5 keys.
- The keys propagate across all Controller nodes.