



Red Hat OpenStack Platform 10

Deploy Fernet on the Overcloud

Deploy Fernet on the Red Hat OpenStack Platform director overcloud

Red Hat OpenStack Platform 10 Deploy Fernet on the Overcloud

Deploy Fernet on the Red Hat OpenStack Platform director overcloud

OpenStack Team
rhos-docs@redhat.com

Legal Notice

Copyright © 2018 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Deploy Fernet on the Red Hat OpenStack Platform director overcloud.

Table of Contents

CHAPTER 1. DEPLOY FERNET ON THE OVERCLOUD	3
1.1. PREPARE THE FERNET KEYS	3
1.2. CONFIGURE THE OVERCLOUD TO USE FERNET	3
1.3. REVIEW THE FERNET DEPLOYMENT	4

CHAPTER 1. DEPLOY FERNET ON THE OVERCLOUD

This chapter describes how to configure your Overcloud to use the Fernet token provider.

- **Key Management** - This example uses *keystone-manage* to generate the overcloud Fernet keys on the undercloud. These keys will not actually be used by the Undercloud since it is configured to use the UUID token format by default. If you do configure the undercloud to use the Fernet token format after following the procedure in this document, it will use the same keys as the overcloud (which may not be desirable).
- **Swift Artifacts** - This implementation uses Heat swift artifacts, which puts a copy of the Fernet key directory on every node in your deployment (not just the Controller node). You will need to consider whether this outcome is acceptable for your deployment requirements.

1.1. PREPARE THE FERNET KEYS

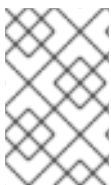
This section generates the Fernet keys on the undercloud, and uploads them into swift.

1. On the undercloud node, use **keystone_manage** to generate Fernet keys:

```
$ . ~/stackrc
$ sudo keystone-manage fernet_setup --keystone-user keystone --keystone-group keystone
```

2. Create a tar file containing the Fernet keys:

```
$ sudo tar -zcf keystone-fernet-keys.tar.gz /etc/keystone/fernet-keys
```



NOTE

the keys in the controller nodes should not be changed manually. All controller nodes should have the exact same set of Fernet keys, otherwise a token generated by one controller won't be accepted by the others.

3. Upload the Fernet keys as swift artifacts:

```
$ upload-swift-artifacts -f keystone-fernet-keys.tar.gz
```

1.2. CONFIGURE THE OVERCLOUD TO USE FERNET

This section creates a YAML file that configures keystone to use **fernet** as the token provider. This setting is then applied to your existing overcloud in a later step.

1. Create a file named **fernet.yaml** that contains the required **token_provider** setting:

```
parameter_defaults:
  controllerExtraConfig:
    keystone::token_provider: 'fernet'
```

2. Deploy the overcloud, including the *fernet.yaml* file that was created in the previous step. For example:

■

```
openstack overcloud deploy --templates -e fernet.yaml
```



NOTE

If re-deploying the overcloud in the future, you will need to ensure that you still include *fernet.yaml*, to prevent the token provider from being re-configured to use a different format.

The process may take some time to complete.

1.3. REVIEW THE FERNET DEPLOYMENT

Review the overcloud controller configuration to confirm that the process was successful:

1. Retrieve the IP address of the controller node:

```
$ openstack server list
+-----+-----+-----+-----+
| ID                                     | Name                                     |
+-----+-----+-----+-----+
| 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 to the controller:

```
$ ssh heat-admin@192.0.2.16
Last login: Tue Sep  6 00:09:59 2016 from 192.0.2.1
```

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

```
$ sudo crudini --get /etc/keystone/keystone.conf token driver
sql
$ sudo crudini --get /etc/keystone/keystone.conf token provider
fernet
```

4. Test the Fernet provider:

```
$ openstack token issue
WARNING: openstackclient.common.utils is deprecated and will be removed
after Jun 2017. Please use osc_lib.utils
+-----+-----+-----+-----+
| Field | Value |
+-----+-----+-----+-----+
```



```

-----+
| expires | 2016-09-20 05:26:17+00:00 |
| id | gAAAAABX4LppE8vaiFZ992eah2i3edp01aDFx1KZq6a_RJzxUx56QVKORrmW0-oZK3-
Xuu2wcnpyq_eeK2SGLz250eLpZ0zxKBR0GsoMfxJU8mEFF8NzfLNcbuS-iz7SV-
N1re3XEywSDG90JcgwjQfXW-8jtcM-n3LL5IaZexAYIw059T_-cd8 |
| project_id | 26156621d0d54fc39bf3adb98e63b63d |
| user_id | 397daf32cadd490a8f3ac23a626ac06c |
+-----+
-----+
-----+
-----+

```

The result should include the long Fernet token. This token will still be shorter in length than the PKI token.



NOTE

The keys used to sign tokens are now available in the undercloud's swift. The keys should remain in swift in case you need to deploy a new controller, however, you can delete them using the **swift** command, if needed:

```
swift delete overcloud-artifacts keystone-fernet-keys.tar.gz
```