



Red Hat OpenStack Platform

10

オーバークラウドへの **Fernet** のデプロイ

Red Hat OpenStack Platform director オーバークラウドへの Fernet のデプロイ

OpenStack Team

Red Hat OpenStack Platform 10 オーバークラウドへの Fernet のデプロイ

Red Hat OpenStack Platform director オーバークラウドへの Fernet のデプロイ

OpenStack Team
rhos-docs@redhat.com

法律上の通知

Copyright © 2017 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.

概要

Red Hat OpenStack Platform director オーバークラウドに Fernet をデプロイします。

目次

第1章 オーバークラウドへの FERNET のデプロイ	3
1.1. FERNET 鍵の準備	3
1.2. オーバークラウドで FERNET を使用するための設定	3
1.3. FERNET デプロイメントの確認	4

第1章 オーバークラウドへの FERNET のデプロイ

本章では、Fernet トークンプロバイダーを使用するためのオーバークラウドの設定方法について説明します。

- ※ **鍵管理**: この例には、**keystone-manage** を使用してオーバークラウドの Fernet 鍵をアンダー上に生成します。これらの鍵は、デフォルトでは UUID トークン形式を使用するように設定されているため、アンダークラウドでは実際には使用されません。本書に記載の手順を実行した後にアンダークラウドが Fernet トークン形式を使用するように設定する場合には、オーバークラウドと同じ鍵を使用することになります (これは、望ましくない場合があります)。
- ※ **Swift アーチファクト**: この実装には、Heat swift アーチファクトを使用します。これは、Fernet 鍵ディレクトリーのコピーをコントローラーノードのみではなく、デプロイメント内の全ノードに配置します。この結果がデプロイメントの要件を満たすかどうかを検討する必要があります。

1.1. FERNET 鍵の準備

本項では、アンダークラウドで Fernet 鍵を生成して swift にアップロードします。

1. アンダークラウドノードで、**keystone_manage** を使用して Fernet 鍵を生成します。

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

2. Fernet 鍵が含まれた tar ファイルを作成します。

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

注記

コントローラーノード内の鍵は手動で変更すべきではありません。全コントローラーノードに全く同じセットの Fernet 鍵がある必要があります。そうでない場合には、1 台のコントローラーで生成されたトークンが別のコントローラーでは受け入れられなくなります。

3. Fernet 鍵を swift のアーチファクトとしてアップロードします。

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

1.2. オーバークラウドで FERNET を使用するための設定

本項では、keystone が **fernet** をトークンプロバイダーとして使用するよう設定する YAML ファイルを作成します。この設定は、後のステップで既存のオーバークラウドに適用します。

1. 必要な設定を記載した **fernet.yaml** という名前のファイルを作成します。

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

2. 前のステップで作成した **fernet.yaml** ファイルを指定してオーバークラウドをデプロイします。以下に例を示します。

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



注記

将来にオーバークラウドを再デプロイする場合にも、必ず **fernet.yaml** を指定してください。トークンプロバイダーが異なる形式を使用するように再構成されるのを防ぐ必要があります。

このプロセスが完了するには、多少時間がかかる場合があります。

1.3. FERNET デプロイメントの確認

オーバークラウドコントローラーの設定をチェックして、プロセスが成功したことを確認します。

1. コントローラーノードの IP アドレスを取得します。

```
$ 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. コントローラーに SSH 接続します。

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

3. トークンドライバーの値とプロバイダーの設定を取得します。

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

4. Fernet プロバイダーをテストします。

```
$ 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 |
+-----+-----+
-----+

```

結果には、Fernet の長いトークンが含まれているはずです。このトークンは、PKI トークンよりも短くなります。



注記

トークンの署名に使用される鍵がアンダークラウドの swift で使用できるようになりました。この鍵は、新規インストーラーをデプロイする必要がある場合のために swift 内に維持すべきですが、必要な場合には **swift** コマンドで削除することができます。

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