



# Red Hat OpenStack Platform 13

## 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



# Red Hat OpenStack Platform 13 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

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.

## 法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Deploy\_Fernet\_on\_the\_Overcloud.ent file |.

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

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

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

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

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

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

The OpenStack<sup>®</sup> 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 オーバークラウドでの FERNET トークンの使用 .....	3
1.1. FERNET デプロイメントの確認	3
1.2. FERNET 鍵のローテーション	4
1.2.1. Mistral を使用した Fernet 鍵のローテーション	4



## 第1章 オーバークラウドでの FERNET トークンの使用

Fernet は、**uuid** に代わるデフォルトのトークンプロバイダーです。本ガイドでは、Fernet デプロイメントを確認する方法と、Fernet キーをローテーションする方法を説明します。

### 1.1. FERNET デプロイメントの確認

この手順では、設定を確認し、Fernet トークンが正常に機能していることを確認します。

1. コントローラーノードの IP アドレスを取得します。

```
[stack@director ~]$ source ~/stackrc
[stack@director ~]$ openstack server list
+-----+-----+-----+-----+
| ID                | Name                | Status | Networks          |
+-----+-----+-----+-----+
| 756bd73-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. コントローラーに対して SSH を実行します。

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

3. トークンドライバーおよびプロバイダー設定の値を取得します。

```
[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. Fernet プロバイダーをテストします。

```
[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 | gAAAAABX4LppE8vaiFZ992eah2i3edpO1aDFxIKZq6a_RJzxUx56QVKORrmW0-oZK3-
Xuu2wcnpYq_eek2SGLz250eLpZOzxKBR0GsoMfxJU8mEFF8NzfLNcbuS-iz7SV-
N1re3XEywSDG90JcgwjQfXW-8jtCm-n3LL5laZexAYlw059T_-cd8 |
| project_id | 26156621d0d54fc39bf3adb98e63b63d |
| user_id | 397daf32cadd490a8f3ac23a626ac06c |
+-----+-----+-----+-----+
```

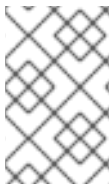
結果には長い Fernet トークンが含まれている必要があります。

## 1.2. FERNET 鍵のローテーション

ローテーションプロセスは比較的簡単に実行できるため、ローテーションサイクルの長さを考慮すると、Red Hat はセキュリティ側で警告することを推奨します。セキュリティ体制からのガイダンスがない場合は、毎月のローテーションサイクルが適切な開始地点となります。

Fernet は、`/var/lib/config-data/puppet-generated/keystone/etc/keystone/fernet-keys` に保存されている 3 種類のキーを使用します。最も番号の大きいディレクトリーには、新しいトークンを生成し、既存のトークンを復号化するために使用されるプライマリーキーが含まれます。

キーローテーションプロセスで、プライマリーキーはセカンダリーキーのステータスに委任され、新しいプライマリーキーが発行されるため、危険にさらされたプライマリーキーの値が減少します。セカンダリーキーは、以前のプライマリーキーで作成されたトークンを復号化するためにのみ使用でき、新しいキーを発行できません。



### 注記

Fernet キーのローテーションを実行する前に、すべてのオープンクラウドノードがオンラインであることを確認します。そうしないと、`deploy_ssh_key` タスクでプロセスが失敗します。

### 1.2.1. Mistral を使用した Fernet 鍵のローテーション

デフォルトでは、director はオープンクラウドの Fernet キーを管理するように設定されています。この設定は、`ManageKeystoneFernetKeys` を使用して環境ファイルで管理されます。その結果、Fernet キーは Mistral (`KeystoneFernetKeys` 下) に保存されます。この方法では、Fernet キーを Mistral でローテーションでき、スタックの更新後も維持されます。

1. 既存の Fernet キーを確認します。
  - a. Fernet キーの場所を特定します。

```
# SSH back to the controller
[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
```



### 注記

`/etc/keystone/` ディレクトリーは、コンテナのファイルシステムのパスを参照します。

- b. 現在の Fernet キーディレクトリーを確認します。

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

- **0** - ステージングされた キー（次のプライマリーキーになる）が含まれ、番号は常に **0** になります。
- **1** - セカンダリー キーが含まれます。



- **2- プライマリー キー** が含まれます。この数はキーがローテーションされるたびに増分し、最大数は常にプライマリーキーとして機能します。



### 注記

- キーの最大数は、デフォルトで5つのキーである `max_active_keys` プロパティによって決定されます。
- キーはすべてのコントローラーで伝播されます。

2. Mistral ワークフローを使用して Fernet キーをローテーションします。

```
[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

3. ID を取得し、ワークフローが正常に実行されたことを確認します。

```
[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

4. コントローラーノードで Fernet キーの数を確認し、前の結果と比較します。

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

- **0**: ステージングされた キーが含まれ、番号は常に **0** になります。このキーは、次のローテーション中にプライマリーキーにプロモートされます。
- **1 & 2** - セカンダリー キーが含まれます。
- **3** - プライマリー キーが含まれます。この数はキーがローテーションされるたびに増分し、最大数は常にプライマリーキーとして機能します。



### 注記

- キーの最大数は、デフォルトで5つのキーである `max_active_keys` プロパティによって決定されます。
- キーはすべてのコントローラーで伝播されます。