Red Hat OpenStack Platform 15

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デプロイ

Last Updated: 2022-09-15

Red Hat OpenStack Platform 15 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

概要

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

目次

第1章 オーバークラウドでのブリックトークンの使用

uuid はデフォルトのトークンプロバイダーとなり、**uuid** を置き換えます。このガイドでは、デプロイメントを確認する方法と、faclキーをローテーションする方法を説明します。

1.1. PIDGIN デプロイメントの確認

この手順では、設定を見直して、pidc トークンが正しく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           |
+--------------------------------------+------------------------+--------+--------------------+
| 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. pidgin 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 | gAAAAABX4LppE8vaiFZ992eah2i3edpO1aDFxlKZq6a_RJzxUx56QVKORrmW0-oZK3-
Xuu2wcnpYq_eek2SGLz250eLpZOzxKBR0GsoMfxJU8mEFF8NzfLNcbuS-iz7SV-
N1re3XEywSDG90JcgwjQfXW-8jtCm-n3LL5IaZexAYIw059T_-cd8 |
| project_id | 26156621d0d54fc39bf3adb98e63b63d |
| user_id | 397daf32cadd490a8f3ac23a626ac06c |
+------------+----------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------+
```

結果には、長いpid トークンが含まれるはずです。

1.2. PIDGIN 鍵のローテーション

Red Hat は、ローテーションサイクルの長さを考慮する際にセキュリティーの途中で誤解を生じさせることを推奨します。これは、ローテーションプロセスを比較的簡単で行うことができるためです。セキュリティーポジションからのガイダンスがない場合には、月次ローテーションサイクルを開始することが推奨されます。

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。最高番号の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。

キーのローテーションプロセス中に、プライマリーキーはセカンダリーキーのステータスに再度設定され、新しいプライマリーキーが発行され、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され、新規キーを発行することはできません。

1.2.1. Mistral を使用したブリックキーのローテーション

デフォルトでは、director はオーバークラウドの中の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、Mistral（**KeystoneFernetKeys**下）に保管されます。このアプローチでは、Mistral でキーを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. 既存のブリックキーを確認します。

   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、コンテナーのファイルシステムのパスを参照します。

   b. 現在のブリック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** キー（次のプライマリーキー）が含まれ、常に **0** の番号が付けられます。
   - **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、数字が最も高い数値が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 プロパティーによって決定されます。
- キーはすべてのコントローラーに伝播されます。

2. Mistral ワークフローを使用してブリック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. コントローラーで、pidgin キーの数を確認し、以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** キーが含まれ、常に **0** の番号が付けられます。このキーは、次回のローテーション時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、数字が最も高い数値が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 プロパティーによって決定されます。
- キーはすべてのコントローラーに伝播されます。