Red Hat OpenStack Platform 16.2

オーバークラウドへの Fernet のデプロイ

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

Last Updated: 2022-03-26

Red Hat OpenStack Platform 16.2 オーバークラウドへの Fernet のデプロイ

Red Hat OpenStack Platform 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

概要

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

目次

前書き

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、弊社 の CTO、Chris Wright のメッセージ を参照してください。

RED HAT ドキュメントへのフィードバック (英語のみ)

弊社ドキュメントに対するご意見をお聞かせください。ドキュメントの改善点があればお知らせください。

ドキュメントへのダイレクトフィードバック (DDF) 機能の使用 (英語版のみ)

特定の文章、段落、またはコードブロックに対して直接コメントを送付するには、DDF の **Add Feedback** 機能を使用してください。なお、この機能は英語版のドキュメントでのみご利用いただけます。

1. **Multi-page HTML** 形式でドキュメントを表示します。
2. ドキュメントの右上隅に **Feedback** ボタンが表示されていることを確認してください。
3. コメントするテキスト部分をハイライト表示します。
4. **Add Feedback** をクリックします。
5. **Add Feedback** フィールドにコメントを入力します。
6. (オプション) ドキュメントチームが連絡を取り問題についてお伺いできるように、ご自分のメールアドレスを追加します。
7. **Submit** をクリックします。

第1章 オーバークラウドでの暗号化に FERNET キーの使用

Fernet はデフォルトのトークンプロバイダーであり、**uuid** に置き換わるものです。Fernet デプロイメントを確認して、Fernet キーをローテーションできます。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。最も数値の高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するプライマリーキーが含まれます。

Fernet キーのローテーションでは、以下のプロセスを使用します。

1. プライマリーキーはセカンダリーキーになります。
2. <system> は新しいプライマリーキーを発行します。送信プライマリーキーは無効になりました。セカンダリーキーを使用して、以前のプライマリーキーに関連付けられたトークンを復号できますが、新しいトークンを発行することはできません。

Fernet 鍵のローテーションサイクルの長さを決定する際には、組織のセキュリティー体制に従います。組織にガイダンスがない場合は、セキュリティー上の理由から、毎月のローテーションサイクルが推奨されます。

1.1. FERNET デプロイメントの確認

Fernet トークンが適切に機能していることを確認するには、コントローラーノードの IP アドレスを取得し、コントローラーノードに対して SSH を実行し、トークンドライバーおよびプロバイダーの設定を確認します。

手順

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. コントローラーノードに対して 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 | gAAAAABX4LppE8vaiFZ992eah2i3edpO1aDFxlKZq6a_RJzxUx56QVKORrmW0-oZK3-
Xuu2wcnpYq_eek2SGLz250eLpZOzxKBR0GsoMfxJU8mEFF8NzfLNcbuS-iz7SV-
N1re3XEywSDG90JcgwjQfXW-8jtCm-n3LL5IaZexAYIw059T_-cd8 |
| project_id | 26156621d0d54fc39bf3adb98e63b63d |
| user_id | 397daf32cadd490a8f3ac23a626ac06c |
------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------+
```

結果には長い Fernet トークンが含まれます。

1.2. WORKFLOW サービスの使用による FERNET キーのローテーション

スタックの更新後も Fernet キーが維持されるようにするには、Workflow サービス (mistral) でキーをローテーションします。デフォルトでは、director は **ManageKeystoneFernetKeys** パラメーターを使用して、環境ファイルのオーバークラウドの Fernet キーを管理します。Fernet キーは、**KeystoneFernetKeys** セクションのワークフローサービスに保存されます。

手順

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。heat-admin ユーザーとしてコントローラーノードにログインし、**crudini** コマンドを使用して Fernet キーをクエリーします。

    ```
    [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
    ```

    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 Fernet キーディレクトリーを検査します。

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

    - **0**: ステージドキーが含まれます。これは次のプライマリーキーになり、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、キーのローテーションが行われるたびに増えます。最大の数字が、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 **max_active_keys** プロパティーで設定されます。デフォルトは 5 つのキーです。
- 鍵は、すべてのコントローラーノードに伝播します。

2. **workflow** コマンドを使用して 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                  |
+-------------------+--------------------------------------+
```

検証

1. ID を取得し、ワークフローが成功し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                  |
+-------------------+--------------------------------------+
```

2. 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**: ステージキーが含まれ、常に番号が **0** になるようにします。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なります。
- **1 および 2** - セカンダリーキーを取得します。
- **3** - プライマリーキーが含まれます。この数は、キーのローテーションが行われるたびに増えます。最大の数字が、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 **max_active_keys** プロパティーで設定されます。デフォルトは 5 つのキーです。
- 鍵は、すべてのコントローラーノードに伝播します。