Red Hat OpenStack Platform 16.1

오버클라우드에 Fernet 배포

Red Hat OpenStack Platform 오버클라우드에 Fernet 배포

Last Updated: 2023-03-25

Red Hat OpenStack Platform 16.1 오버클라우드에 Fernet 배포

Red Hat OpenStack Platform 오버클라우드에 Fernet 배포

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.

법적 공지

초록

Red Hat OpenStack Platform 오버클라우드에 Fernet을 배포합니다.

차례

PREFACE

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견을 보내 주십시오. Red Hat이 어떻게 이를 개선하는지 알려주십시오.

DDF(직접 문서 피드백) 기능 사용

특정 문장, 단락 또는 코드 블록에 대한 직접 주석은 **피드백 추가** DDF 기능을 사용하십시오.

1. *다중 페이지 HTML* 형식으로 설명서를 봅니다.
2. 문서 오른쪽 상단에 **Feedback** (피드백) 버튼이 표시되는지 확인합니다.
3. 주석 처리하려는 텍스트 부분을 강조 표시합니다.
4. **피드백 추가**를 클릭합니다.
5. 주석을 사용하여 **Add Feedback** (피드백 추가) 필드를 작성합니다.
6. 선택 사항: 설명서 팀이 문제에 대한 자세한 내용을 문의할 수 있도록 이메일 주소를 추가하십시오.
7. **Submit(제출)**을 클릭합니다.

1장. 오버클라우드에서 암호화에 FERNET 키 사용

Fernet은 기본 토큰 프로바이더로, **uuid** 를 대체합니다. Fernet 배포를 검토하고 Fernet 키를 순환할 수 있습니다.

1.1. FERNET 배포 검토

구성을 검토하여 Fernet 토큰이 올바르게 작동하는지 확인합니다.

절차

1. 컨트롤러 노드의 IP 주소를 검색합니다.

```
[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. 컨트롤러 노드에 SSH로 연결합니다.

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

3. 토큰 드라이버 및 공급자 설정 값을 검색합니다.

```
[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 공급자를 테스트합니다.

```
[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 |
----------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------+
```

결과에 긴 Fernet 토큰이 포함됩니다.

1.2. FERNET 키 순환 주기

Fernet 키 순환 주기의 길이를 결정할 때 조직의 보안 포스처를 따르십시오. 조직에 지침이 없는 경우 보안상의 이유로 월별 회전 주기가 좋은 방법입니다.

Fernet은 **/var/lib/config-data/puppet-generated/keystone/etc/keystone/fernet-keys** 에 저장되는 세 가지 유형의 키를 사용합니다. 가장 많이 사용되는 디렉터리에는 새 토큰을 생성하고 기존 토큰을 해독하는 기본 키가 포함되어 있습니다.

Fernet 키 순환은 다음 프로세스를 사용합니다. . 기본 키는 보조 키가 됩니다. . <system>은 새 기본 키를 발행합니다. 나가는 기본 키가 더 이상 유효하지 않습니다. 보조 키를 사용하여 이전 기본 키와 연결된 토큰을 해독할 수 있지만 새 토큰을 발행할 수 없습니다.

1.3. WORKFLOW 서비스를 사용하여 FERNET 키 순환

기본적으로 director는 오버클라우드 Fernet 키를 관리합니다. 이 설정은 **ManageKeystoneFernetKeys** 를 사용하여 환경 파일에서 관리됩니다. 결과적으로 Fernet 키는 **KeystoneFernetKeys** 섹션의 Workflow 서비스(mistral)에 저장됩니다. 이 접근 방식은 워크플로 서비스를 사용하여 Fernet 키를 회전하고 스택 업데이트 후에도 키가 지속됨을 의미합니다.

절차

1. 기존 Fernet 키를 검토합니다.

   a. Fernet 키 위치를 식별합니다. 컨트롤러 노드에 heat-admin 사용자로 로그인하고 **crudini 명령을 사용하여** Fernet 키를 쿼리합니다.

   ```
   [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
   ```

   

   참고

   /etc/keystone/ 디렉터리는 컨테이너 파일 시스템 경로를 나타냅니다.

   b. 현재 Fernet 키 디렉토리를 검사합니다.

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

   - **0** - 다음 기본 키가 되고 항상 **0** 에 번호가 매겨진 준비 키가 들어 있습니다.
   - **1** - 보조 키를 포함합니다.
   - **2** - 기본 키를 포함합니다. 이 숫자는 키가 순환될 때마다 증가합니다. 가장 많은 숫자는 항상 기본 키로 사용됩니다.

참고

- 최대 키 수는 **max_active_keys** 속성으로 설정됩니다. 기본값은 5개 키입니다.
- 키는 모든 컨트롤러 노드에 전파됩니다.

2. **workflow** 명령을 사용하여 Fernet 키를 순환합니다.

```
[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                  |
+-------------------+--------------------------------------+
```

검증

1. ID를 검색하고 워크플로가 성공했는지 확인합니다.

```
[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. 컨트롤러 노드에서 Fernet 키 수를 검토하고 이전 결과와 비교합니다.

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

- **0** - 준비 된 키를 포함 하 고 항상 번호 **0**. 이 키는 다음 순환 중에 기본 키가 됩니다.
- **1 & 2** - 보조 키를 유지합니다.

- **3** - 기본 키를 포함합니다. 이 숫자는 키를 회전할 때마다 증가합니다. 가장 많은 숫자는 항상 기본 키로 사용됩니다.

참고

- 최대 키 수는 **max_active_keys** 속성으로 설정됩니다. 기본값은 5개 키입니다.
- 키는 모든 컨트롤러 노드에 전파됩니다.