



Red Hat OpenStack Platform 13

director のアンダークラウドのバックアップと復元

director のアンダークラウドのバックアップと復元

Red Hat OpenStack Platform 13 director のアンダークラウドのバックアップと復元

director のアンダークラウドのバックアップと復元

OpenStack Team
rhos-docs@redhat.com

法律上の通知

Copyright © 2018 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

本ガイドでは、Red Hat OpenStack Platform director のアンダークラウドのバックアップと復元の方法について説明します。

目次

第1章 アンダークラウドのバックアップ	3
1.1. バックアップに関する留意事項	3
1.2. アンダークラウドノードの高可用性	3
1.3. アンダークラウドのバックアップ	3
1.4. 取得完了したバックアップの検証	5
第2章 アンダークラウドの復元	6
2.1. アンダークラウドの復元	6
2.2. 完了した復元の検証	9
2.2.1. Identity サービス (Keystone) の動作の確認	9

第1章 アンダークラウドのバックアップ

本ガイドでは、Red Hat OpenStack Platform director で使用するアンダークラウドのバックアップの方法を説明します。アンダークラウドとは、通常 OpenStack 環境のデプロイメントおよび管理に使用する単一の物理ノードのことを指します (ただし、仮想マシンで director を実行する、2 ノードタイプの pacemaker クラスタを使用した高可用性オプションも存在します)。

1.1. バックアップに関する留意事項

データ損失やシステムのダウンタイムを最小限に抑えるため、強力なバックアップおよびリカバリーポリシーを策定します。バックアップストラテジーを決定するにあたっては、以下の質問事項への回答を明確にしておく必要があります。

- **データ損失からどの程度迅速に復旧する必要がありますか。** データ損失が一切許容されない場合には、デプロイメントストラテジーとして、バックアップの使用に加えて、高可用性に焦点を当てるべきです。物理バックアップメディアを取得する際にかかる時間 (例: オフサイトの場所を利用している場合はそのサイトからのメディア) や復元の操作に利用可能なテープドライブがいくつあるかを考慮する必要があります。
- **保管する必要のあるバックアップの数はいくつですか。** データの保管年数に影響を与える法的かつ規制上の要件を考慮する必要があります。
- **バックアップはオフサイトに保管する必要がありますか。** バックアップメディアをオフサイトに保管すると、物理的な場所に降りかかる災害のリスクを軽減するのに役立ちます。
- **バックアップをテストする頻度はどの程度ですか。** 強力なバックアップストラテジーには、バックアップデータの定期的な復元テストが含まれます。これは、正しいデータが依然としてバックアップされており、バックアップや復元プロセス中にデータの破損が発生していないかを検証するのに役立ちます。これらのテストは、実際の災害復旧の条件下で実行するという前提で行われるべきです。
- **バックアップの対象は何ですか。** 以下のセクションでは、コンポーネントのデータベースとファイルシステムのバックアップと、バックアップの復旧について説明します。

1.2. アンダークラウドノードの高可用性

Red Hat は、アンダークラウドノードの高可用性 (HA) オプションに特定の要件を規定していないので、希望に応じて自由に検討することができます。たとえば、Red Hat Enterprise Virtualization (RHEV) 内の高可用性の仮想マシンとしてアンダークラウドノードを実行するように構成したり、必要なサービスを HA で提供する Pacemaker をインストールした物理ノードを使用したりする方法を検討することができます。

アンダークラウドノードの高可用性について検討する場合は、お使いの環境に最も有効であると判断したソリューションのドキュメントやグッドプラクティスを参照してください。

1.3. アンダークラウドのバックアップ

完全なアンダークラウドのバックアップには、以下のデータベースおよびファイルが含まれます。

- アンダークラウドノード上の MariaDB データベース
- (データベースを正確に復元できるように) アンダークラウド上の MariaDB 設定ファイル
- 設定データ: `/etc`

- ログデータ: `/var/log`
- イメージデータ: `/var/lib/glance`
- 証明書生成データ (SSL を使用している場合): `/var/lib/certmonger`
- コンテナイメージデータ: `/var/lib/docker`、`/var/lib/registry`
- swift の全データ: `/srv/node`
- stack ユーザーのホームディレクトリー内の全データ: `/home/stack`



注記

バックアッププロセスを実行する前に、アンダークラウドに利用可能なディスク容量が十分であることを確認します。アーカイブファイルは、少なくとも 3.5 GB となることが予想され、それ以上になる可能性があります。

手順

1. アンダークラウドに **root** ユーザーとしてログインします。
2. Create a **backup** ディレクトリーを作成して、そのディレクトリーを所有するユーザーを **stack** に変更します。

```
[root@director ~]# mkdir /backup
[root@director ~]# chown stack: /backup
```

3. **backup** ディレクトリーからデータベースをバックアップします。

```
[root@director ~]# cd /backup
[root@director ~]# mysqldump --opt --all-databases >
/root/undercloud-all-databases.sql
```

4. データベースのバックアップと設定ファイルをアーカイブします。

```
[root@director ~]# tar --xattrs --ignore-failed-read -cf \
undercloud-backup-`date +%F`.tar \
/root/undercloud-all-databases.sql \
/etc \
/var/log \
/var/lib/glance \
/var/lib/certmonger \
/var/lib/docker \
/var/lib/registry \
/srv/node \
/root \
/home/stack
```

- **--ignore-failed-read** オプションを指定すると、アンダークラウドには適用しないディレクトリーはスキップされます。
- **--xattrs** オプションには、Object Storage (swift) のメタデータを保管するのに必要な拡張属性が含まれます。

これで、**undercloud-backup-`<date>`.tar.gz** という名前のファイルが作成されます。**<date>** はシステムの日付です。この **tar** ファイルをセキュアな場所にコピーします。

1.4. 取得完了したバックアップの検証

復元プロセスを実行/検証することでバックアッププロセスが正常に完了したことを検証できます。バックアップからの復元の詳しい情報は、次の項を参照してください。

第2章 アンダークラウドの復元

本項では、Red Hat OpenStack Platform director で使用するアンダークラウドの復元方法を説明します。

2.1. アンダークラウドの復元

以下の復元プロセスは、アンダークラウドノードでエラーが発生して、回復不可能な状態であることを前提としています。この手順では、新規インストール環境でデータベースおよびクリティカルなファイルシステムの復元を行う必要があります。以下が前提条件です。

- Red Hat Enterprise Linux 7 の最新版を再インストール済みであること
- ハードウェアレイアウトが同じであること
- マシンのホスト名とアンダークラウドの設定が同じであること
- バックアップアーカイブが **root** ディレクトリーにコピー済みであること

手順

1. アンダークラウドに **root** ユーザーとしてログインします。
2. **stack** ユーザーを作成します。

```
[root@director ~]# useradd stack
```

3. そのユーザーのパスワードを設定します。

```
[root@director ~]# passwd stack
```

4. **sudo** を使用する場合にパスワードを要求されないようにします。

```
[root@director ~]# echo "stack ALL=(root) NOPASSWD:ALL" | tee -a  
/etc/sudoers.d/stack  
[root@director ~]# chmod 0440 /etc/sudoers.d/stack
```

5. コンテンツ配信ネットワークにシステムを登録します。プロンプトが表示されたら、カスタマーポータルユーザー名とパスワードを入力します。

```
[root@director ~]# subscription-manager register
```

6. Red Hat OpenStack Platform のエンタイトルメントをアタッチします。

```
[root@director ~]# subscription-manager attach --pool=Valid-Pool-  
Number-123456
```

7. デフォルトのリポジトリをすべて無効にしてから、必要な Red Hat Enterprise Linux リポジトリを有効にします。

```
[root@director ~]# subscription-manager repos --disable=*  
[root@director ~]# subscription-manager repos --enable=rhel-7-  
server-rpms --enable=rhel-7-server-extras-rpms --enable=rhel-7-
```

```
server-rh-common-rpms --enable=rhel-ha-for-rhel-7-server-rpms --
enable=rhel-7-server-openstack-13-rpms
```

8. システムで更新を実行して、ベースシステムパッケージを最新の状態にします。

```
[root@director ~]# yum update -y
[root@director ~]# reboot
```

9. アンダークラウドの時刻が同期されていることを確認します。以下に例を示します。

```
[root@director ~]# yum install -y ntp
[root@director ~]# systemctl start ntpd
[root@director ~]# systemctl enable ntpd
[root@director ~]# ntpdate pool.ntp.org
[root@director ~]# systemctl restart ntpd
```

10. バックアップ用に一時ディレクトリを作成します。

```
[root@director ~]# mkdir /var/tmp/undercloud_backup
```

11. ファイルシステムのバックアップアーカイブを一時ディレクトリに抽出します。

```
[root@director ~]# tar -xvf /root/undercloud-backup-[timestamp].tar
-C /var/tmp/undercloud_backup --xattrs || true
```

12. **rsync** をインストールします。

```
[root@director ~]# yum -y install rsync
```

13. 以下のディレクトリをバックアップのコンテンツと同期します。

```
[root@director ~]# rsync -a -X
/var/tmp/undercloud_backup/home/stack/ /home/stack
[root@director ~]# rsync -a -X
/var/tmp/undercloud_backup/etc/haproxy/ /etc/haproxy/
[root@director ~]# rsync -a -X
/var/tmp/undercloud_backup/etc/pki/instack-certs/ /etc/pki/instack-
certs/
[root@director ~]# mkdir -p /etc/puppet/hieradata/
[root@director ~]# rsync -a -X
/var/tmp/undercloud_backup/etc/puppet/hieradata/
/etc/puppet/hieradata/
[root@director ~]# rsync -a -X /var/tmp/undercloud_backup/srv/node/
/srv/node/
[root@director ~]# rsync -a -X
/var/tmp/undercloud_backup/var/lib/glance/ /var/lib/glance/
```

14. **openstack-keystone** パッケージをインストールして、その設定データを同期します。

```
[root@director ~]# yum -y install openstack-keystone
[root@director ~]# rsync -a /var/tmp/undercloud_backup/etc/keystone/
/etc/keystone/
```

15. **polycoreutils-python** パッケージをインストールします。

```
[root@director ~]# yum -y install polycoreutils-python
```

16. アンダークラウドで SSL を使用している場合には、CA 証明書をリフレッシュします。

```
[root@director ~]# semanage fcontext -a -t etc_t "/etc/pki/instack-
certs(/.*)"?"
[root@director ~]# restorecon -R /etc/pki/instack-certs
[root@director ~]# update-ca-trust extract
```

17. データベースサーバーとクライアントツールをインストールします。

```
[root@director ~]# yum install -y mariadb mariadb-server python-
tripleoclient
```

18. データベースを起動します。

```
[root@director ~]# systemctl start mariadb
[root@director ~]# systemctl enable mariadb
```

19. データベースのバックアップのサイズに対応するように、許可されるパケット数を増やします。

```
[root@director ~]# mysql -uroot -e"set global max_allowed_packet =
1073741824;"
```

20. データベースのバックアップを復元します。

```
[root@director ~]# mysql -u root <
/var/tmp/undercloud_backup/root/undercloud-all-databases.sql
```

21. Mariadb を再起動して、バックアップファイルからパーミッションをリフレッシュします。

```
[root@director ~]# systemctl restart mariadb
```

1. 古いユーザーパーミッションの一覧を取得します。

```
[root@director ~]# mysql -e 'select host, user, password from
mysql.user;'
```

2. リストされた各ホストの古いユーザーパーミッションを削除します。以下に例を示します。

```
[root@director ~]# HOST="192.0.2.1"
[root@director ~]# USERS=$(mysql -Nse "select user from mysql.user
WHERE user != \"root\" and host = \"\$HOST\";" | uniq | xargs)
[root@director ~]# for USER in $USERS ; do mysql -e "drop user
\"$USER\"@\"$HOST\"" || true ;done
[root@director ~]# mysql -e 'flush privileges'
```

3. **openstack-glance** パッケージをインストールして、そのファイルパーミッションを復元します。

```
[root@director ~]# yum install -y openstack-glance
[root@director ~]# chown -R glance: /var/lib/glance/images
```

4. **openstack-swift** パッケージをインストールして、そのファイルパーミッションを復元します。

```
[root@director ~]# yum install -y openstack-swift
[root@director ~]# chown -R swift: /srv/node
```

5. 新規作成した **stack** ユーザーに切り替えます。

```
[root@director ~]# su - stack
[stack@director ~]$
```

6. アンダークラウドのインストールコマンドを実行します。このコマンドは、**stack** ユーザーのホームディレクトリーから実行するようにしてください。

```
[stack@director ~]$ openstack undercloud install
```

7. インストールが完了するまで待ちます。アンダークラウドは、オーバークラウドへの接続を自動的に復元します。ノードは、保留中のタスクに対して、OpenStack Orchestration (heat) のポーリングを続けます。

8. コンテナのデータをバックアップのコンテンツと同期します。

```
[root@director ~]$ sudo rsync -a -X
/var/tmp/undercloud_backup/var/lib/docker/ /var/lib/docker/
[root@director ~]$ sudo rsync -a -X
/var/tmp/undercloud_backup/var/lib/registry/ /var/lib/registry/
[root@director ~]$ sudo rsync -a -X
/var/tmp/undercloud_backup/etc/docker/ /etc/docker/
[root@director ~]$ sudo rsync -a -X
/var/tmp/undercloud_backup/etc/docker-distribution/ /etc/docker-
distribution/
[root@director ~]$ sudo cp
/var/tmp/undercloud_backup/etc/sysconfig/docker* /etc/sysconfig/.
[root@director ~]$ sudo systemctl restart docker docker-distribution
```

2.2. 完了した復元の検証

以下のコマンドを使用して、新しく復元した環境のヘルスチェックを実行します。

2.2.1. Identity サービス (Keystone) の動作の確認

このステップでは、ユーザーの一覧をクエリーで取得して、Identity サービスの動作を検証します。

```
# source overcloudrc
# openstack user list
```

コントローラーから実行する場合は、このコマンドの出力には、この環境で作成されたユーザーの一覧が含まれているはずです。このアクションでは、keystone が実行中でユーザーの要求を正常に認証していることが分かります。以下に例を示します。

```
# openstack user list
```

```
+-----+-----+-----+-----+
|          id          |    name    | enabled |          email          |
+-----+-----+-----+-----+
| 9e47bb53bb40453094e32eccce996828 |    admin   |    True | root@localhost          |
| 9fe2466f88cc4fa0ba69e59b47898829 | ceilometer |    True | ceilometer@localhost    |
| 7a40d944e55d422fa4e85daf47e47c42 |    cinder  |    True | cinder@localhost        |
| 3d2ed97538064f258f67c98d1912132e |    demo    |    True |                          |
| 756e73a5115d4e9a947d8aad6f5ac22 |    glance  |    True | glance@localhost        |
| f0d1fcee8f9b4da39556b78b72fdafb1 |    neutron |    True | neutron@localhost       |
| e9025f3faeee4d6bb7a057523576ea19 |    nova    |    True | nova@localhost          |
| 65c60b1278a0498980b2dc46c7dcf4b7 |    swift   |    True | swift@localhost         |
+-----+-----+-----+-----+
|          id          |    name    | enabled |          email          |
```