



Red Hat OpenStack Platform 13

Back Up and Restore the Director Undercloud

Back up and restore the director undercloud

Red Hat OpenStack Platform 13 Back Up and Restore the Director Undercloud

Back up and restore the director undercloud

OpenStack Team
rhos-docs@redhat.com

Legal Notice

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.

Abstract

A guide to backing up and restoring the undercloud in Red Hat OpenStack Platform director.

Table of Contents

CHAPTER 1. BACK UP THE UNDERCLOUD	3
1.1. BACKUP CONSIDERATIONS	3
1.2. HIGH AVAILABILITY OF THE UNDERCLOUD NODE	3
1.3. BACKING UP THE UNDERCLOUD	3
1.4. VALIDATE THE COMPLETED BACKUP	4
CHAPTER 2. RESTORE THE UNDERCLOUD	5
2.1. RESTORING THE UNDERCLOUD	5
2.2. VALIDATE THE COMPLETED RESTORE	8
2.2.1. Check Identity Service (Keystone) Operation	8

CHAPTER 1. BACK UP THE UNDERCLOUD

This guide describes how to back up the undercloud used in the Red Hat OpenStack Platform director. The undercloud is usually a single physical node (although high availability options exist using a two-node pacemaker cluster that runs director in a VM) that is used to deploy and manage your OpenStack environment.

1.1. BACKUP CONSIDERATIONS

Formulate a robust back up and recovery policy in order to minimize data loss and system downtime. When determining your back up strategy, you will need to answer the following questions:

- *How quickly will you need to recover from data loss?* If you cannot have data loss at all, you should include high availability in your deployment strategy, in addition to using backups. You'll need to consider how long it will take to obtain the physical backup media (including from an offsite location, if used), and how many tape drives are available for restore operations.
- *How many backups should you keep?* You will need to consider legal and regulatory requirements that affect how long you are expected to store data.
- *Should your backups be kept off-site?* Storing your backup media offsite will help mitigate the risk of catastrophe befalling your physical location.
- *How often should backups be tested?* A robust back up strategy will include regular restoration tests of backed up data. This can help validate that the correct data is still being backed up, and that no corruption is being introduced during the back up or restoration processes. These drills should assume that they are being performed under actual disaster recovery conditions.
- *What will be backed up?* The following sections describe database and file-system backups for components, as well as information on recovering backups.

1.2. HIGH AVAILABILITY OF THE UNDERCLOUD NODE

You are free to consider your preferred high availability (HA) options for the Undercloud node; Red Hat does not prescribe any particular requirements for this. For example, you might consider running your Undercloud node as a highly available virtual machine within Red Hat Enterprise Virtualization (RHEV). You might also consider using physical nodes with Pacemaker providing HA for the required services.

When approaching high availability for your Undercloud node, you should consult the documentation and good practices of the solution you decide works best for your environment.

1.3. BACKING UP THE UNDERCLOUD

A full undercloud backup includes the following databases and files:

- All MariaDB databases on the undercloud node
- MariaDB configuration file on the undercloud (so that you can accurately restore databases)
- The configuration data: `/etc`
- Log data: `/var/log`
- Image data: `/var/lib/glance`

- Certificate generation data if using SSL: `/var/lib/certmonger`
- Any container image data: `/var/lib/docker` and `/var/lib/registry`
- All swift data: `/srv/node`
- All data in the stack user home directory: `/home/stack`



NOTE

Confirm that you have sufficient disk space available on the undercloud before performing the backup process. Expect the archive file to be at least 3.5 GB, if not larger.

Procedure

1. Log into the undercloud as the `root` user.
2. Back up the database:

```
# mysqldump --opt --all-databases > /root/undercloud-all-databases.sql
```

3. Archive the database backup and the configuration files:

```
# sudo 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
```

- The `--ignore-failed-read` option skips any directory that does not apply to your undercloud.
- The `--xattrs` option includes extended attributed, which are required to store metadata for Object Storage (swift).

This creates a file named `undercloud-backup-<date>.tar.gz`, where `<date>` is the system date. Copy this tar file to a secure location.

1.4. VALIDATE THE COMPLETED BACKUP

You can validate the success of the completed back up process by running and validating the restore process. See the next section for further details on restoring from backup.

CHAPTER 2. RESTORE THE UNDERCLOUD

This section describes how to restore the undercloud used in the Red Hat OpenStack Platform Director.

2.1. RESTORING THE UNDERCLOUD

The following restore procedure assumes your undercloud node has failed and is in an unrecoverable state. This procedure involves restoring the database and critical filesystems on a fresh installation. It assumes the following:

- You have re-installed the latest version of Red Hat Enterprise Linux 7.
- The hardware layout is the same.
- The hostname and undercloud settings of the machine are the same.
- The backup archive has been copied to the **root** directory.

Procedure

1. Log into your undercloud as the **root** user.

2. Create the **stack** user:

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

3. Set a password for the user:

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

4. Disable password requirements when using **sudo**:

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

5. Register your system with the Content Delivery Network, entering your Customer Portal user name and password when prompted:

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

6. Attach the Red Hat OpenStack Platform entitlement:

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

7. Disable all default repositories, and then enable the required Red Hat Enterprise Linux repositories:

```
[root@director ~]# sudo subscription-manager repos --disable=*
[root@director ~]# sudo 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. Perform an update on your system to make sure you have the latest base system packages:

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

9. Ensure the time on your undercloud is synchronized. For example:

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

10. Create a temporary directory for the backup

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

11. Extract the filesystem backup archive into the temporary directory:

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

12. Install **rsync**:

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

13. Synchronize the following directories with backup content:

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

14. Install the **openstack-keystone** package and synchronize its configuration data:

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

15. Install the **polycoreutils-python** package:

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

16. If using SSL in the undercloud, refresh the CA certificates:

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

17. Install the database server and client tools:

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

18. Start the database:

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

19. Increase the allowed packets to accommodate the size of our database backup:

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

20. Restore the database backup:

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

21. Restart Mariadb to refresh the permissions from the backup file:

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

1. Get a list of old user permissions:

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

2. Remove the old user permissions for each host listed. For example:

```
[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. Install the **openstack-glance** package and restore its file permissions:

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

4. Install the `openstack-swift` packages and restore its file permissions:

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

5. Switch to the new stack user:

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

6. Run the undercloud installation command. Ensure to run it in the `stack` user's home directory:

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

7. Wait until the install completes. The undercloud automatically restores its connection to the overcloud. The nodes will continue to poll OpenStack Orchestration (heat) for pending tasks.

8. Synchronize the container data with backup content:

```
[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. VALIDATE THE COMPLETED RESTORE

Use the following commands to perform a healthcheck of your newly restored environment:

2.2.1. Check Identity Service (Keystone) Operation

This step validates Identity Service operations by querying for a list of users.

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

When run from the controller, the output of this command should include a list of users created in your environment. This action demonstrates that keystone is running and successfully authenticating user requests. For example:

```
# 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 |
+-----+-----+-----+-----+
-----+

```