



Backing Up Deployment Information

This chapter provides information on the following topics:

- [Overview, on page 1](#)
- [Identify Component IP Addresses, on page 1](#)
- [Backup Configuration Files, on page 4](#)
- [Backup UAS ConfD Databases, on page 5](#)
- [Collect Logs, on page 6](#)
- [Collect Charging Detail Records, on page 6](#)

Overview

Prior to performing a deployment deactivation (e.g. as part of an upgrade or downgrade process), it is highly recommended that you make backup copies of key information.

To backup this information:

1. [Identify Component IP Addresses, on page 1.](#)
2. [Backup Configuration Files, on page 4.](#)
3. [Backup UAS ConfD Databases, on page 5.](#)
4. [Collect Logs, on page 6](#)
5. [Collect Charging Detail Records, on page 6.](#)

Identify Component IP Addresses

To collect the HA-VIP, and floating IP addresses for UAS, ESC, UEM, and CF:

1. Log on to the server on which OSP-D is running.
2. Source the “stack_namerc-core” file.

```
source ~/<stack_name>rc-core
```
3. Obtain the floating IP for CF and UEM VMs.

```
neutron floatingip-list
```

Example command output:

id port_id	fixed_ip_address	floating_ip_address
22936d62-d086-4658-acfc-51b3d8952df6 a9489513-9bec-449b-af8-02487b9fb175	172.168.20.13	10.169.126.155
2fc42615-5254-44ec-af5a-a14440a36812 6a170e76-bb05-4cb9-b09e-e94b8e1ae99c 38a53400-346e-4e12-96b6-989fcad75ab3	172.168.20.5	10.169.126.145
70be87df-97db-4d53-b603-2efb7cfd4a6c		10.169.126.149
72205ae8-c905-4705-a67f-a99cf9078246 a088cc88-3e95-4751-a092-e2f6063d3886	172.168.20.101	10.169.126.154
780e652c-3ee7-47c3-ad25-f1cf17d0c9f6 f186730b-be55-4404-9a5a-84741a8d8032	172.16.182.6	10.169.126.144
871825f2-5d30-4a34-baec-3ba09cf93559 c416552e-5f41-4dbe-bbd1-6a9ef0a39e94	172.168.10.11	10.169.126.140
89c1784d-a8a5-4e91-835c-d4dbff47172e 78afdd69-5f86-48c7-84c0-a10dbff25ea57 89d6c6ac-bf12-45b9-ae52-7fd2a20a2838	172.168.10.13	10.169.126.143
a501bec3-d87f-47de-8e11-f5ce903ea1fe		10.169.126.147
f6ff9566-1514-4d55-b09d-800c19906d9e dde1fe31-e278-443f-bd5e-f434edefe14e	172.168.10.7	10.169.126.146
f8c131b5-a5d6-400e-8936-c407504208da aff0efca-cef0-4852-bdb4-9b1fa5ca373f	172.16.182.11	10.169.126.157
f963b405-3586-4ab2-8815-b76332832e64 2a3ab817-9939-45a9-8774-e062ea74387f	172.168.10.101	10.169.126.142

- Obtain the AutoDeploy address.

```
nova list | grep auto-deploy
```

- Log on to the AutoDeploy VM as the default user, *ubuntu*.

```
ssh ubuntu@<ad_vm_address>
```

- Switch to the *root* user.

```
sudo su
```

- Enter the ConfD CLI.

```
confd_cli -C -u admin
```

- Find the deployment details from AutoDeploy:

```
show service-deployment <deployment_name> siter autovnfr
```

Example command output:

```
siter LBUCS002
autovnfr LBPCF100-UAS
endpoint-info ip-address 10.169.126.141
endpoint-info port 2022
status alive
vnfmr LBPCF100-ESC
endpoint-info ip-address 172.168.10.7
endpoint-info port 830
```

```

status alive
vnfr LBPCF100-VNF
status alive
vnf-deploymenttr LBPCF100-DEPLOYMENT
  em-endpoint-info ip-address 172.168.10.11
  em-endpoint-info port 2022
autovnfr LBPGW100-UAS
endpoint-info ip-address 10.169.126.144
endpoint-info port 2022
status alive
vnfmr LBPGW100-ESC
endpoint-info ip-address 172.168.20.5
endpoint-info port 830
status alive
vnfr LBPGW100-VNF
status alive
vnf-deploymenttr LBPGW100-DEPLOYMENT
  em-endpoint-info ip-address 172.168.20.12

```

Record the UAS IP address for each VNF as highlighted in the command output example.

9. Log on to the master AutoVNF VM as the default user, *ubuntu*.

```
ssh ubuntu@<ad_vm_address>
```

10. Switch to the *root* user.

```
sudo su
```

11. Enter the ConfD CLI.

```
confd_cli -C -u admin
```

12. Collect the VIP address for ESC.

In releases prior to 6.0:

```
show autovnf-oper:vnfm
```

Example output:

```

autovnf-oper:vnfm vnfmd
state alive
version 3.1.0.94
transaction-id 1507961257-916914
ha-vip 30.30.62.7
vnfc-instance vnfmd-ESC
compute-host tblano-compute-7.localdomain
interfaces autovnfd-uas-management
ip-address 30.30.61.17
mac-address fa:16:3e:3d:be:31
interfaces autovnfd-uas-orchestration
ip-address 30.30.62.7
mac-address fa:16:3e:68:8e:15

```

In 6.0 and later releases:

```
show vnfr
```

For an example output, see the [Example show vnfr Command Output](#).

13. Collect the VIP address for the UEM and CF.

```
show autovnf-oper:vip-port
```

Example output:

```

vip-port vnf-dvdeployment vnf-deployment
transaction-id 1508009048-329005
port autovnf-dv-uas-management-30.30.61.103
network autovnf-dv-uas-management
ha-vip 30.30.61.103
vdu-ref element-manager
port autovnf-dv-uas-management-30.30.61.104
network autovnf-dv-uas-management
ha-vip 30.30.61.104
vdu-ref control-function
vip-port vnfmd vnfmd-deployment
transaction-id 1507961257-916914
port vnfmd-ESC-vip
network autovnf-dv-uas-management
ha-vip 30.30.62.7
vdu-ref esc

```

In 6.0 and later releases:

show vnfr

For an example output, see the [Example show vnfr Command Output](#).

- Repeat [13, on page 3](#) for each VNF-UAS.

Backup Configuration Files

Backing up configuration files involves using SFTP to download copies of these files to a backup directory on a remote server.



Important

If SFTP to any of the VMs fails, then remove the respective entry from the *known_hosts* file under *.ssh* directory and retry.

To backup the configuration files:

- Create a backup directory, if one does not already exist.
- SFTP the Day 0 configuration called *system.cfg* from each UGP-based VNF to the backup directory.
- SFTP the latest Day N configuration file from each UGP-based VNF to the backup directory.

The Day N configuration file specifies the configuration of the various gateway and services deployed on the UGP.



Important

UGP-based VNF Day N configuration can also be obtained by logging in to the CF and logging the output of the **show configuration** command. In addition, password information saved in this file is encrypted. Prior to re-applying this configuration to the upgraded/redeployed VNF, you'll need to manually reconfigure the unencrypted passwords in the configuration file.

- Collect the output of the **show support details** command for each VNF.
- SFTP the latest AutoDeploy configuration file from the AutoDeploy VM to the backup directory.



Important You'll need to log in to the AutoDeploy VM using the credentials for the user *ubuntu*.

6. SFTP the latest AutoVNF configuration file from the master AutoVNF VM to the backup directory.



Important You'll need to log in to the AutoVNF VM using the credentials for the user *ubuntu*.

7. SFTP the latest VIM Orchestrator configuration file from the AutoDeploy VM to the backup directory.
8. SFTP the latest VIM configuration file from the AutoDeploy VM to the backup directory.

Backup UAS ConfD Databases

Backing up ConfD databases (CDBs) is done on the UAS software role VMs and involves copying the databased files to a secure location.

AutoDeploy CDB:

Copy the contents of the `/opt/cisco/usp/uas/confd-6.3.1/var/confd/cdb` directory.

Example directory contents:

```
total 1100
drwxr-xr-x 2 root root 4096 Sep 27 22:27 ./
drwxr-xr-x 8 root root 4096 Sep 27 18:48 ../
-rw-r--r-- 1 root root 10332 Sep 27 22:10 aaa_init.xml
-rw-r--r-- 1 root root 10261 Oct 2 20:20 A.cdb
-rw-r--r-- 1 root root 1086629 Sep 27 22:10 C.cdb
-rw-r--r-- 1 root root 804 Sep 27 22:27 O.cdb
```

AutoIT CDB

Copy the contents of the `/opt/cisco/usp/uas/confd-6.3.1/var/confd/cdb` directory.

Example directory contents:

```
total 884
drwxr-xr-x 2 root root 4096 Sep 14 18:55 ./
drwxr-xr-x 8 root root 4096 Sep 11 21:56 ../
-rw-r--r-- 1 root root 10234 Sep 12 18:34 aaa_init.xml
-rw-r--r-- 1 root root 7092 Sep 14 18:56 A.cdb
-rw-r--r-- 1 root root 857637 Sep 12 18:34 C.cdb
-rw-r--r-- 1 root root 16363 Sep 14 18:56 O.cdb
```

AutoVNF

Copy the contents of the `/opt/cisco/usp/uas/confd-6.3.1/var/confd/cdb` directory.

Example directory contents:

```
total 1232
drwxr-xr-x 2 root root 4096 Oct 4 05:39 ./
drwxr-xr-x 8 root root 4096 Sep 27 18:48 ../
-rw-r--r-- 1 root root 10218 Sep 27 22:22 aaa_init.xml
```

```
-rw-r--r-- 1 root root      3789 Sep 27 22:22 A.cdb
-rw-r--r-- 1 root root 1223594 Sep 27 22:22 C.cdb
-rw-r--r-- 1 root root      277 Sep 27 18:48 gilán.xml
-rw-r--r-- 1 root root      2216 Oct  4 05:39 O.cdb
-rw-r--r-- 1 root root      271 Sep 27 18:48 vpc.xml
```

Collect Logs

Prior to deactivating any part of the deployment, it is recommended that you collect logs from the different components that comprise the USP-based VNF and transfer them to a remote backup server.

- **AutoDeploy Logs:** Refer to [Viewing AutoDeploy Logs](#) for information on the logs to collect and their locations.

It is recommended that you copy autodeploy.log to autodeply_beforedeactivation.log and then collect logs during de-activation.

- **AutoIT Logs:** Refer to [Viewing AutoIT Logs](#) for information on the logs to collect and their locations.

It is recommended that you copy autoit.log to autoit_beforedeactivation.log and then collect logs during de-activation.

- **AutoVNF Logs:** Refer to [Viewing AutoVNF Logs](#) for information on the logs to collect and their locations.

It is recommended that you copy autovnf.log to autovnf_beforedeactivation.log and then collect logs during de-activation.

- **VNFM (ESC) Logs:** Refer to [Viewing ESC Logs](#) for information on the logs to collect and their locations.

- **UEM Logs:** Refer to [Viewing UEM Logs](#) for information on the logs to collect and their locations.

Collect Charging Detail Records

Prior to performing an upgrade or redeployment, it is strongly recommended that you collect or backup copies of all charging detail records (CDRs).

The UGP-based VNF supports the ability to push locally-stored CDRs to a configured collection server based on user-defined intervals or criteria. Refer to the “Configuring CDR Push” section within the “HDD Storage” chapter of the GTPP Interface Administration and Reference. Select the document pertaining to your software version from those available here: <https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html>

Prior to initiating the VNF upgrade or redeployment, collect or backup copies of all CDRs using one of these two methods:

- Initiate a manual push of specified CDR files to the configured collection server, OR
- Retrieve CDRs via SFTP

Instructions for using these methods is provided in the GTPP Interface Administration and Reference. Note that additional configuration may be required in order to use these methods.