Backup and Restore

About Backup and Restore

Use the backup and restore functions in Catalyst Center VA to create backup files. You can restore the backup files to the same appliance (in case your Catalyst Center becomes unusable) or use them to migrate your Catalyst Center to a different appliance, for example:

- Back up data from a Catalyst Center hardware appliance and restore the data to a Catalyst Center VA.
- Back up data from one Catalyst Center VA and restore the data to another Catalyst Center VA

Before you can create a backup on an NFS server, you need to configure the backup server so that the Catalyst Center Maglev user can access it. For Catalyst Center on AWS, see Configure an NFS Server, on page 1 in this guide. For all other information about backup and restore, see the *Cisco DNA Center Administrator Guide, Release 2.3.5*.

Configure an NFS Server

Before you can create a backup of a Catalyst Center VA, you need to configure your NFS server so that the Maglev user can access it.

Before you begin

- Have the Cisco DNA Center VA IP address and key.pem file on hand. These were provided to you during the deployment.
- Verfiy that the key.pem file has 400 permissions.

For more information, see "Guidelines for Accessing the Cisco DNA Center CLI" in the *Cisco DNA Center 2.3.5 on AWS Deployment Guide*.

Step 1 Use SSH to connect to the Catalyst Center VA and its Maglev restricted shell using the key.pem file that you downloaded during the deployment:

```
$ ssh -i key.pem maglev@catalyst_center_ip_address -p 2222
```

Note Access to the backup server is allowed only through the security group ports that are enabled on AWS. For this reason, you must log in to the Maglev restricted shell first and then access the backup server.

Step 2 Make sure that the key.pem file has the necessary permissions to log in to the backup server.

```
$ ls -ltr
```

The key.pem file has read permissions, as shown in the following example:

```
-r-------- 1 maglev maglev 1674 Feb  5 19:57 A-1-1707161965011.pem
```

Step 3 Log in to the backup server and become the root user.

a) Use SSH to connect to the backup server and log in as the **ec2-user** using the key.pem file that you downloaded during the deployment:

```
$ ssh -i key.pem ec2-user@backup_server_ip_address
```

b) At the **Are you sure you want to continue connecting (yes/no)?** prompt, type **yes** and press the **Return** key.

c) Switch to the root user:

```
$ sudo su
```

Step 4 Add the **maglev** user to the `sudoers` file.

a) Edit the `sudoers` file using the **vi** editor:

```
$ sudo vi /etc/sudoers.d/90-cloud-init-users
```

b) Add the following line at the end of the file:

```
$ maglev ALL=(ALL) NOPASSWD:ALL
```

c) Save and exit the **vi** editor.

Step 5 Create an NFS share directory for the NFS configuration and set permissions.

Note The directory is not automatically created in Cisco Global Launchpad, Release 1.8. Create the folder as required for configuring the backup.

a) Navigate to the `/var` directory:

```
$ cd /var
```

b) Create an NFS share directory. In the following example and throughout this procedure, the directory is named "nfsshare":

```
$ mkdir nfsshare
```

Note Make a note of the directory name you choose, as you need to provide this name when you configure the NFS server in Cisco DNA Center VA.

c) Set read, write, and execute permissions for the NFS share directory:

```
$ chmod -R 777 /var/nfsshare/
$ chmod -R o+w /var/nfsshare/
```

Step 6 Create a directory for rsync configuration and set permissions.

Note The directory is not automatically created in Cisco Global Launchpad, Release 1.8. Create the folder as required for configuring the backup.

a) Navigate to the `/var` directory:

```
$ cd /var
```

b) Create a directory named "catalyst-backup":

```
$ mkdir catalyst-backup
```

c) Set read, write, and execute permissions for the directory:

```
$ chmod -R 777 /var/catalyst-backup/
$ chmod -R o+w /var/catalyst-backup/
```

Step 7 List the block devices that are attached to the system and identify a partition that has 500-GB and is using the ext4 filesystem:

```
$ lsblk
```

The output is similar to the following example:

```
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1    259:0   0 500G  0 disk /var/catalyst-NFSbackup
nvme0n1    259:1   0   8G  0 disk
1-nvme0n1p1   259:2   0   8G  0 part /
```

Step 8 Format the partition that you've chosen to use:

```
$ mkfs.ext4 /dev/nvme1n1
```

Step 9 Mount the formatted partition to the NFS share directory you created in Step 5, on page 2:

```
$ mount /dev/nvme1n1 /var/nfsshare/|
```

Step 10 Configure the exports file to allow NFS exports.

a) Edit the exports file using the **vi** editor:

```
$ vi /etc/exports
```

b) Allow NFS exports by adding the NFS share directory that was created in Step 5, on page 2:

```
$ /var/nfsshare/ *(rw,all_squash,sync,no_subtree_check)
```

c) Save and close the editor.

d) Apply the changes:

```
exportfs -a
```

Step 11 Validate the NFS export settings and confirm that the NFS share directory is exported with the appropriate permissions.

```
exportfs -v
```

What to do next

Log into the Catalyst Center GUI, configure the backup settings based on your preferences, and initiate a backup. For more information about backup and restore, see the *Cisco DNA Center Administrator Guide, Release 2.3.5*.

Backup and Restore—Hardware Appliance to VA

This procedure provides a high-level overview of how you can back up the data from a Catalyst Center hardware appliance and restore it to a Catalyst Center VA. For detailed instructions, see the "Backup and Restore" chapter in the *Cisco DNA Center Administrator Guide, Release 2.3.5*.

Before you begin

- Make sure that the hardware appliance used for the backup is a 44-core Catalyst Center appliance.
- If you're using a Cloud backup (NFS) server, you'll need to know the backup password in order to log into the server.

  Your backup server password is dynamically created. The password is composed of the first four characters of the VA pod name and the backup server's IP address without the periods. For example, if the VA pod name is DNAC-SJC and the backup server's IP address is 10.0.0.1, the backup server password is DNAC10001.

Note You can find the VA pod name on the **Dashboard** pane after you choose the region that it's deployed in.

You can find the backup server's IP address in the **View Catalyst Center** pane.

Step 1 Back up the data from the Catalyst Center hardware appliance.

Make sure that the backup server is connected to Catalyst Center through a VPN.

Step 2 Create a Catalyst Center VA. For more information, see "Create a New Catalyst Center VA" in the *Cisco DNA Center on AWS Deployment Guide*.

Make sure the Catalyst Center VA is up and running.

Step 3 Connect the Catalyst Center VA to the backup server from Step 1.

Make sure that the backup server is reachable from the Catalyst Center VA.

Step 4 Configure the backup server on the Catalyst Center VA.

Step 5 Restore the data on to the Catalyst Center VA.

Backup and Restore—VA to VA

This procedure provides a high-level overview of how you can back up the data from one (source) Catalyst Center VA and restore it to another (target) Catalyst Center VA. For detailed instructions, see the "Backup and Restore" chapter in the *Cisco DNA Center Administrator Guide, Release 2.3.5*.

Before you begin

- Make sure that you successfully deployed two Catalyst Center VAs with Cisco Global Launchpad, AWS CloudFormation, or AWS Marketplace. For more information, see *Cisco DNA Center on AWS Deployment Guide*.
- Make sure that both Catalyst Center VAs are up and running.
- Make sure that the backup server is connected to the source Catalyst Center VA through a VPN.
- Make sure that the backup server is reachable from the target Catalyst Center VA.
- If you're using a Cloud backup (NFS) server, you'll need to know the backup password in order to log into the server.

  Your backup server password is dynamically created. The password is composed of the first four characters of the VA pod name and the backup server's IP address without the periods. For example, if the VA pod name is DNAC-SJC and the backup server's IP address is 10.0.0.1, the backup server password is DNAC10001.

Note You can find the VA pod name on the **Dashboard** pane after you choose the region that it's deployed in.

You can find the backup server's IP address in the **View Catalyst Center** pane.

Step 1 Back up the data from the source Catalyst Center VA to a backup server.

Step 2 Bring up the target Catalyst Center VA that you want to restore the data to.

Step 3 Connect the target Catalyst Center VA to the backup server. (See Step 1.)

Step 4 Configure the backup server on the target Catalyst Center VA.

Step 5 Restore the data to the target Catalyst Center VA.