



Disaster Recovery (Backup and Restore)

This chapter contains the following sections:



Note This section is applicable only for Cisco DCNM OVA/ISO installations.

- [Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup, on page 1](#)
- [Backup and Restore Cisco DCNM on a Cluster Setup, on page 2](#)

Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.



Note In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(1), the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

Perform the following task to take a backup of Cisco DCNM and Application data.

Procedure

Step 1 Logon to the Cisco DCNM appliance using SSH.

Step 2 Take a backup of the application data using the **appmgr backup** command.

```
dcnm# appmgr backup
```

From Release 11.4(1), Cisco DCNM allows you to configure a cron job that allows saves the backup to a remote scp server. Use **appmgr backup schedule** command to configure a scheduled backup.

```
dcnm# appmgr backup schedule [day] <hh<hh>:<mm>
[destination <user>@<host>:[<dir>]]
```

Copy the backup file to a safe location and shut down the DCNM Appliance.

Step 3 Right click on the installed VM and select **Power > Power Off**.

Step 4 Deploy the new DCNM appliance.

Step 5 After the VM is powered on, click on **Console** tab.

A message indicating that the DCNM appliance is configuring appears on the screen.

Copy and paste the URL to the browser to continue with restore process.

Step 6 On the DCNM Web Installer UI, click **Get Started**.

Step 7 On the Cisco DCNM Installer screen, select radio button.

Select the backup file that was generated in [Step 2, on page 1](#).

Continue to deploy the DCNM.

Step 8 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

Step 9 After the data is restored, check the status using the **appmgr status all** command.

Backup and Restore Cisco DCNM on a Cluster Setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.

Perform the following task to take perform backup and restore of data in a Cisco DCNM Cluster setup.

Before you begin

Check and ensure that the Active and Standby servers are operational, using the `appmgr show ha-role` command.

Example:

On the Active node:

```
dcnm-active# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node:

```
dcnm2-standby# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Procedure

- Step 1** Log on to the Cisco DCNM appliance using SSH.
- Step 2** Take a backup of the application data using the **appmgr backup** command on both Active, Standby appliances, and on all Compute nodes.

```
dcnm-active# appmgr backup
dcnm-standby# appmgr backup
dcnm-compute1# appmgr backup
dcnm-compute2# appmgr backup
dcnm-compute3# appmgr backup
```

Copy the backup files of all nodes to a safe location and shut down the DCNM Appliance.

- Step 3** Right click on the installed VM and select **Power > Power Off**.
- Step 4** Install two Cisco DCNM Release 11.5(1) appliances.

Note Ensure that the Hostnames match the earlier Active and Standby appliances.

For instructions, see [Installing the Cisco DCNM](#).

- Step 5** Install three Cisco DCNM Compute nodes.

Note Ensure that the Hostnames match the earlier Compute nodes.

For instructions, see [Installing Cisco DCNM Compute Node](#).

- Step 6** Provide access to the `/root` directory on all nodes using the following command.

```
dcnm# appmgr root-access permit
```

- Step 7** Stop telemetry on Active and Standby nodes using the following command:

```
dcnm-active# systemctl stop pmn-telemetry
dcnm-standby# systemctl stop pmn-telemetry
```

- Step 8** Set the environment variable to allow restore process using CLI and restore the node with the same hostname as respective Active and Standby backup files, using the following command:

Note Ensure that you perform the restore in the same order—Active, Standby, Compute1, Compute2, and Compute3.

```
dcnm-active# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm1-backup-file>
dcnm-standby# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm2-backup-file>
dcnm-compute1# APPMGR_ALLOW_RESTORE=1 appmgr restore <compute1-backup-file>
dcnm-compute2# APPMGR_ALLOW_RESTORE=1 appmgr restore <compute2-backup-file>
dcnm-compute3# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm2-backup-file>
```

- Step 9** After the data is restored, check the status using the **appmgr status all** command.
-

What to do next

Log on to the DCNM Web UI with appropriate credentials.

The Applications tab displays all the services running on the DCNM deployment that you have installed. Click Compute tab to view the new Compute in Discovered state on the Cisco DCNM Web UI.

To add the compute nodes to a cluster, see [Adding Computes to a Cluster Node](#) in your deployment-specific *Cisco DCNM Configuration Guide* for more information.



Note If you didn't enable clustered mode while installing DCNM, use the **appmgr afw config-cluster** command to enable the compute cluster. For instructions, refer to [Enabling the Compute Cluster](#) in the Cisco DCNM LAN Fabric Configuration Guide.

When a compute node goes through an unscheduled powercycle and restarts, the Elasticsearch container won't start. It's possible that some filesystems are corrupted. To resolve this issue, reboot the Compute node in safe mode by using **fsck -y** command.