Backup and Restore

You can take a backup manually anytime. You can also configure a scheduler to backup all fabric configurations and intents.

You can backup and restore using any of the following formats:

- **Config only**: A Config only backup is smaller. It contains the intent, dependent data, discovery information, credentials, and policies. A restore from this backup has functional fabrics, switch discovery, expected configurations, and other settings.
- **Full**: A Full backup is large. It contains current data, historical data, alarms, host information, and everything in a Config only backup. A restore from this backup has functional historical reports, metrics charts, and all base functionality.

You can restore a config-only backup or a full backup.

When restoring a backup, you can choose to do a config only restore or a full restore. A config only restore will restore only the configuration (intent, discovery information, credentials, and policies) and can be done using both config only backups and full backups. A full restore will restore the configuration and any current and historical data, charts, etc. and can be done using only full backups.

Note Wait for minimum of 20 minutes after fresh installation before restoring the backup data. Some applications may not be operational if the backup is restored immediately in the freshly installed setup.

NDFC Backup and Restore Behavior in Release 12.1.2e

This table provides information about NDFC backup and restore behavior in release 12.1.2e. Anything not mentioned is assumed to be fully supported.

Table 1: NDFC Backup and Restore Behavior

Feature	Config Data Backup and Restore	Operational Data Backup and Restore
LAN		
Fabric backups	Supported (Schedules)	Not supported (Backups)
Reports	Not supported (Report Definitions)	Not supported (Reports)

Feature	Config Data Backup and Restore	Operational Data Backup and Restore
Image management	Not supported (Policies, Images)	Not supported (History, etc)
EPL	Supported	Supported (Historical Endpoint Search) up to 1 million records. Not supported (Dashboard, Endpoint Life, Endpoint History).
ALL		
Alarm	Supported	Not Supported
PM	Supported	Supported for 90 days data

This section includes the following:

Scheduler

The purpose of the scheduler is to take backups of the system, if a system needs to be restored. You must backup to a remote location.

To schedule a backups of application and configuration data from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin

If there are no scheduled backup jobs, **No Schedule set** is displayed.

Procedure

Step 1 Click on **No Schedule set**.

The **Scheduler** window appears.

Step 2 Check the **Enable scheduled backups** check box.

Step 3 Under **Type**, select your desired format to restore.

- Choose **Config only** or **Full**.

Step 4 In the **Destination** field, click and choose **Export to SCP Server** or **Export to SFTP Server** from the drop-down list.

Step 5 In the **Server** field, provide the Server IP Address.

Step 6 In the **File Path** field, provide the absolute path of the directory to store the backup file.

Step 7 Enter **Username** and **Password** to the backup directory.

Step 8 Enter the **Encryption Key** to the backup file.

You must have an Encryption Key in order to restore from the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

Step 9 In the **Run on days** field, select the check box to schedule the backup job on one or more days.

Step 10 In the **Start at** field, use the time picker to schedule the backup at a particular time.

The time picker is a 12-hour clock.

Step 11 Click **Schedule backup** to run the backup job as per schedule.

Restore

Note Wait for minimum of 20 minutes after fresh installation before restoring the backup data. Some applications may not be operational if the backup is restored immediately in the freshly installed setup.

From Cisco NDFC Release 12.1.2e, you can restore on a freshly installed Nexus Dashboard Fabric Controller system with no feature enabled as well as on an existing system where features have already enabled.

If the restore is done on a system with features enabled, note the following:

- You cannot restore a SAN Controller backup on a LAN Controller (and vice versa).
- You can perform only config only restore. Whether the original backup is a config only backup or a full backup, only config (non operational) data will be restored. All operational data (statistics and historical data) will be lost.

Guidelines

When you migrate from L2 HA to L3 HA, check the Ignore External Service IP Configuration check box to ensure that the persistent IPs in the backup are ignored and it selects new ones during the restore. Rest of the data will be restored.

Note During disaster recovery, NDFC allows you to restore only on the same version on which the backup was taken.

To restore application and configuration data from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Click **Restore**.

The **Restore now** window appears.

Step 2 Under **Type**, select your desired format to restore.

- Choose **Config only** or **Full**.

Step 3 In the **Source** field, click and choose the appropriate source where you have stored the backup file.

- Choose **Upload File** if the file is stored in a local directory.
  a. Open the directory where you've saved the backup file.
  b. Drag and drop the backup file to the **Restore now** window.

  or

  Click Browse. Navigate to the directory where you've saved the backup file. Select the backup file and click Open.
  c. Enter the **Encryption Key** to the backup file.

  Note You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

- Choose **Import from SCP Server** or **Import from SFTP Server** if the backup file is stored in a remote directory.
  a. In the **Server** field, provide the Server IP Address.
  b. In the **File Path** field, provide the relative file path to the backup file.
  c. In the **Username** and **Password** fields, enter appropriate details.
  d. In the **Encryption Key** field, enter the Encryption Key to the backup file.

  Note You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

Step 4 (Optional) Check the **Ignore External Service IP Configuration** check box.

If the **Ignore External Service IP Configuration** check box is selected, then the external service IP configuration is ignored. This selection allows you to take a backup on a system and restore it on a different system, with different management and/or data subnets.

This option does not have any impact during an upgrade from Cisco DCNM 11.5(x) to Cisco NDFC.

Step 5 Click **Restore**.

The backup file appears in the table on the Backup & Restore window. The time required to restore depends on the data in the backup file.

Backup Now

To take a backup of application and configuration data from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Click **Backup now**.

Step 2 Under **Type**, select your desired format to restore.

- Choose **Config only** or **Full**.

Step 3 In the **Destination** field, click and choose the appropriate destination to store the backup file.

- Choose **Local Download** to store the backup in a local directory.
  1. Enter the **Encryption Key** to the backup file.

     Note You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

  2. Click **Backup**.

     After the backup is complete, the backup file available for download from the **Backup & Restore** screen.

  3. In the Actions column, you can click on Download icon to save the backup to a local directory.

     Click on **Delete** icon to delete the backup.

     Note You must delete the backups that are taken with **Local Download** options as soon as possible due to the limited amount of allocated disk space.

- Choose **Export to SCP Server** or **Export to SFTP Server** to store the backup file in a remote directory.

  You must specify the file name if you choose the **Export to SFTP Server** option for backup. You do not need to specify the file name for the **Export to SCP Server** option. The file name should contain *path/filename.tar.gz*.

  1. In the **Server** field, provide the Server IP Address.
  2. In the **File Path** field, provide the relative file path to the backup file.
  3. In the **Username** and **Password** fields, enter appropriate details.
  4. In the **Encryption Key** field, enter the Encryption Key to the backup file.

     Note You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

  5. Click **Backup**.

     After the backup is complete, the backup file is saved in the remote directory.