Backing Up and Restoring SAN Operational Mode Setups, Release 12.1.3

Table of Contents

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
NDFC release 12.1.3	Reorganized content	Content within this document was originally provided in the *Cisco NDFC-Fabric Controller Configuration Guide* or the *Cisco NDFC-SAN Controller Configuration Guide*. Beginning with release 12.1.3, this content is now provided solely in this document and is no longer provided in those documents.

Backing Up and Restoring SAN Fabrics

The following sections describe how to back up and restore SAN fabrics.

Guidelines: SAN Fabrics

Following are the guidelines on backing up and restoring SAN fabrics:

- If you add or remove devices to the fabric, you can't restore a fabric from a current date to an earlier date.
- The backup and restore procedures described in this document apply only for NDFC 12.x systems.
- If a SAN switch was backed up previously and a new SAN fabric backup is initiated, NDFC will compare the current running SAN switch configuration with the previously backed up SAN switch configuration. If NDFC determines that there are no changes between the current running SAN switch configuration and the previous SAN switch configuration, NDFC will skip creating a new backup for a SAN switch configuration that hasn't changed.

Backing Up a SAN Fabric

You can back up all fabric configurations and intents automatically or manually. You can save configurations in Cisco NDFC, which are the intents. The intent may or may not be pushed out to the switches.

The backup has the information related to intent and fabric configurations in addition to the associated state of the resource manager in terms of used resources on the fabrics. Cisco NDFC backs up only when there is a configuration push.

The following sections describe the necessary steps to back up a fabric:

Enabling an Automatic (Scheduled) Fabric Backup

Cisco NDFC triggers an automatic backup only if you did not trigger any manual backup after the last configuration push.

To enable an automatic (scheduled) backup for fabric configurations and intents:

1. Navigate to the Fabrics window:

   SAN > Fabric

2. Select a fabric from the list of configured fabrics, then click **Actions > Configure Backup**.

   The **Configure Backup** window appears.

   

   You can also navigate to this **Configure Backup** window for a fabric by double-clicking on a fabric in the **Fabrics** window, then clicking **Actions > Configure Backup**.

3. Check the box next **Enable scheduled archive** to enable an automatic (scheduled) backup of this fabric.

   The remaining fields in this window become editable.

4. In the **Frequency** field, set the desired frequency of the fabric backup.
   - **Daily**: Backs up the fabric on a daily basis.
   - **Weekly**: Choose one or more days when you want to have the fabric backed up every week.
   - **Monthly**: Choose the day of the month when you want to have the fabric backed up every month.
   - **Custom**: Choose one of the following custom periods when you want to have the fabric backed up.

     Run every:

     - 5 days
     - 10 days
     - 15 days
     - 20 days
     - 25 days
5. Choose the time of the day (UTC) when you want to have the fabrics automatically backed up:
   - Hour
   - Minute
   - am/pm
6. Click **Save** when you have completed the configurations in this window.

Enabling a Manual Fabric Backup

To enable a manual backup for fabric configurations and intents:

1. Navigate to the **Fabrics** window:

   SAN > Fabric

2. Double-click on a configured fabric to bring up the **Overview** window for that fabric.
3. Click the **Backup** tab.
4. Click **Actions > Backup Now**.
5. Enter a name (tag) for the manual fabric backup.

6. Determine if you want to mark the backup as golden.

   Click the box next to **Mark backup as golden** to mark this backup as golden. See Marking a Backup as Golden for more information about golden backups.

7. Click **Ok**.

Marking a Backup as Golden

Once you have a fabric backup configured (either a manual or an automatic backup), you can mark that fabric backup as *golden*, indicating that you don't want to delete that backup even after you reach the archiving limit. Golden backups will not be removed automatically to make space for new backups.

Note the following guidelines with golden backups:

- NDFC archives only up to ten golden backups.
- You can't delete golden backups of fabrics. However, you can remove the golden backup designation on a particular backup as described below, which would then allow you to delete that backup, if necessary.

To mark a specific backup as golden:

1. Navigate to the **Fabrics** window:

   SAN > Fabric

2. Double-click on a configured fabric to bring up the **Overview** window for that fabric.
3. Click the **Backup** tab.
4. Select the backup that you want to mark as golden.

   You can mark either an automatic or a manual backup as golden. You can distinguish between automatic or manual backups through their names:

   - Automatic backups have only the versions in their names.
   - Manual backups have tag names, which you provided when you initiated a manual backup, along with the version in the backup name.

     Hover over a backup to see the name.

5. Click **Actions > Mark as golden**.

   If you want to remove a golden mark on a particular backup, select that backup in this window and click **Actions > Remove as golden**.

Working With Backup Files

After you have backed up the SAN fabric using the procedures provided in Backing Up a SAN Fabric, you can then navigate to the appropriate area to work with those backup files. The following sections provide the necessary information when working with backup files:

- Navigate to the Backup Window
- Copy Backup to Bootflash
- Compare Configuration Files
- Export Configuration

Navigate to the Backup Window

You can navigate to the **Backup** window using either of these paths:

- At the fabric level:
  1. Navigate to the **Fabrics** window:

     SAN > Fabric

  2. Double-click on a SAN fabric that was backed up.
  3. In the **Fabric Overview** page for that SAN fabric, click the **Backup** tab.
- At the switch level:
  1. Navigate to the **Switches** window:

     SAN > Switches

  2. Double-click on a switch that was backed up.
  3. In the **Switch Overview** page for that switch, click the **Backup** tab.

The following information is displayed on the **Backup** tab at either the fabric or the switch level:

Field	Description
Switch	Displays the switch name.
Backup Date	Displays the backup date.
Backup Tag	Displays the backup tag name.
Backup Type	Displays the type of backup.
Configuration File	Displays the configuration files that are archived for that device.

You can use **Filter by attribute** to view required information.

Click the **Refresh** icon to refresh the table.

The following table describes the actions you can perform in this tab:

Action	Description
Backup now	Available only in the fabric level **Backup** window. See Enabling a Manual Fabric Backup for more information.
Copy to bootflash	See Copy Backup to Bootflash for more information.
Compare	See Compare Configuration Files for more information.
Export	See Export Configuration for more information.

Action	Description
Edit tag	Used to edit a tag of a switch. Click the check box for a required switch, then click **Actions > Edit tag** and click **OK**.
Mark as golden	Used to mark a backup as a golden backup. See Marking a Backup as Golden for more information.
Remove as golden	Used to remove the golden backup designation on a backup. Click the check box for a required switch, then click **Actions > Remove as golden**. Click **Confirm** in the confirmation window.
Delete	Used to delete a switch from a backup. Click the check box for a required switch, then click **Actions > Delete**. Click **Confirm** in the confirmation window.

Copy Backup to Bootflash

To copy a backup to bootflash:

1. Navigate to the appropriate **Backup** window.

   See Navigate to the Backup Window.

2. Click the checkbox next to the backup that you want to copy to bootflash.
3. Click **Actions> Copy to bootflash**.

   After several moments, a **Success** window appears.

4. Click **Ok**.

Compare Configuration Files

This feature allows you to compare two different configuration files.

To compare configuration files:

1. Navigate to the appropriate **Backup** window.

   See Navigate to the Backup Window.

2. Click the check boxes next to two different configuration files to select those files to compare.

   The first file that you select is designated as the Source file and the second configuration file is designated as the Target file.

3. Click **Actions > Compare**.

   The **View Config Diff** page appears, displaying the difference between the two configuration files.

   The content in the Source and Target configuration files is displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration. You can also choose **Changed** to view the configuration differences of the configuration files.

   The differences in the configuration file are shown in the table, with these legends:

- **Red**: Diff configuration details.
- **Green**: New added configuration.
- **Blue**: Modified configuration details.

4. Click **Copy to Target** to copy the source configuration to the target configuration file, or click **Cancel** to revert to the configuration details page.

   The **Copy Configuration** window displays the source configuration preview and the target device of the destination configuration. The selected devices area shows the following fields:

   - **Device Name**: Specifies the target device name to which the source configuration is copied.
   - **IP Address**: Specifies the IP Address of the destination device.
   - **Group**: Specifies the group to which the device belongs.
   - **Golden Config**: Specifies the version of the destination configuration.
   - **Status**: Specifies the status of the device.

5. Click **Yes** to copy the configuration to the destination device configuration.

Export Configuration

To export a backup configuration file:

1. Navigate to the appropriate **Backup** window.

   See Navigate to the Backup Window.

2. Click the checkbox next to the backups that you want to export.
3. Click **Actions > Export**.

   The files are downloaded in your local system. You can then use third-party file transfer tools to transfer these files to an external server.

Backing Up and Restoring NDFC Configurations

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

Understanding NDFC Backup Formats

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

- **Config Only**: A Config Only backup is smaller than a Full backup, which is described below. 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. In addition to everything in a Config Only backup, a Full backup contains current data, historical data, alarms, and host information. 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 either a Config Only backup or a Full backup.
- A Full restore will restore the configuration and any current and historical data, charts, and so on, and can be done using only Full backups.

Wait for a minimum of 20 minutes after a 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

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

In the following table:

- A Config Only backup and restore includes only the features listed in the **Configuration Data Backup and Restore** column.

- A Full backup and restore includes the features listed in both the **Configuration Data Backup and Restore** and the **Operational Data Backup and Restore** columns.

Table 1. NDFC Backup and Restore Behavior

Feature	Configuration Data Backup and Restore	Operational Data Backup and Restore
SAN		
SAN archives	Supported (Schedules)	Not supported (Backups)
Reports	Not supported (Report Definitions)	Not supported (Reports)
Image management	Not supported (Policies, Images)	Not supported (History, etc)
ALL		
Alarm	Supported	Not Supported
Performance Monitoring (PM)	Supported	Supported for 90 days data

Guidelines: NDFC Configurations

Following are the guidelines on backing up and restoring NDFC configurations:

- During disaster recovery, NDFC allows you to restore only on the same version on which the backup was taken.
- The backup and restore procedures described in this document apply only for NDFC 12.x systems.

Backing Up NDFC Configurations

The following sections describe the necessary steps to back up an NDFC configuration:

- Enabling an Automatic (Scheduled) Backup of NDFC Configurations
- Enabling a Manual Backup of NDFC Configurations

Enabling an Automatic (Scheduled) Backup of NDFC Configurations

You can create automatic (scheduled) backups of the NDFC configurations and restore those NDFC configurations at a later date, if necessary. Scheduled NDFC configurations backups must be backed up to a remote location.

To enable automatic (scheduled) backups of the NDFC configurations:

1. Navigate to the **Backup and Restore** window:

   Operations > Backup and Restore

2. Review the scheduled backup jobs in this window.

   If there are no backup jobs scheduled yet, **No Schedule set** is displayed in the upper right corner of the window.

3. Click on **No Schedule set**.

   The **Scheduler** window appears.

4. Check the **Enable scheduled backups** check box.
5. Under **Type**, select your desired format to back up (**Config only** or **Full**).

   See Understanding NDFC Backup Formats for more information.

6. In the **Destination** field, click and choose **Export to SCP Server** or **Export to SFTP Server** from the drop-down list.
7. In the **Server** field, provide the server IP address.
8. In the **Directory Path** field, provide the absolute path of the directory to store the backup file.
9. Enter the necessary information in the **Username** and **Password** fields.
10. 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.

11. In the **Run on days** field, select the check box to schedule the backup job on one or more days.
12. In the **Start at** field, use the time picker to schedule the backup at a particular time.

    The time picker uses a 12-hour clock.

13. Click **Save** to run the backup job based on the configured schedule.

Enabling a Manual Backup of NDFC Configurations

To enable a manual backup of application and configuration data of an Nexus Dashboard Fabric Controller backup:

1. Navigate to the **Backup and Restore** window:

   Operations > Backup and Restore

2. Click **Backup now**.
3. Under **Name**, enter a name for the manual backup.
4. Under **Type**, select your desired format to back up (**Config only** or **Full**).

   See Understanding NDFC Backup Formats for more information.

5. Determine if you are configuring a local backup or a remote backup.

   

   We do not recommend local backups when backing up NDFC configurations because they are not persistent. We strongly recommend that you configure a remote backup instead.

   - If you are configuring a remote backup:
     a. In the **Destination** field, choose **Export to SCP Server** or **Export to SFTP Server** to store the backup file in a remote directory.

b. In the **Server** field, provide the server IP address.

c. In the **File Path** field, provide the absolute file path to the backup file.

- You must specify the file name in the file path if you choose the **Export to SFTP Server** option for backup (for example, *path/filename.tar.gz*).
- You do not have to specify the file name in the file path for the **Export to SCP Server** option.

d. Enter the necessary information in the **Username** and **Password** fields.

e. Enter the **Encryption Key** to the backup file.

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.

f. Click **Backup**.

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

- If you are configuring a local backup:

a. In the **Destination** field, choose **Local Download**.

b. Enter the **Encryption Key** to the backup file.

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.

c. Click **Backup**.

After the backup is complete, the backup file is available for download from the **Backup and Restore** window.

d. In the **Backup and Restore** window, in the **Actions** column, you can click on the Download icon to save the backup to a local directory.

If you want to delete the manual backup for any reason, click the **Delete** icon to delete the backup.

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

Restoring NDFC Configurations

You can perform a full restore from a full backup, or you can perform a config-only restore from either a full or config-only backup.

You can perform a config-only inline restore on an existing NDFC system using a prior backup. When performing a config-only restore from a full backup, only the non-operational data is restored. All operational data (statistics and historical data) will be lost.

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 features enabled as well as on an existing system where features have already been 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 a Config Only restore. Whether the original backup is a Config Only backup or a Full backup, only configuration (non-operational) data will be restored. All operational data (statistics and historical data) will be lost.

To restore application and configuration data from a Nexus Dashboard Fabric Controller backup:

1. Navigate to the **Backup and Restore** window:

   Operations > Backup and Restore

2. Click **Restore**.

   The **Restore now** window appears.

3. Under **Type**, select your desired format to restore (**Config only** or **Full**).

   See Understanding NDFC Backup Formats for more information.

4. Determine if you are restoring from a local backup or from a remote backup.
   - If you are restoring from a local backup:
     a. In the **Source** field, choose **Upload File**.
     b. Navigate to the local directory where you backed up the NDFC configuration, then drag and drop the backup into the **Restore now** area, or click **Browse** to navigage to the local directory where you backed up the NDFC configuration and select the backup.
     c. Go to Step 5.
   - If you are restoring from a remote backup:
     a. In the **Source** field, choose **Import from SCP Server** or **Import from SFTP Server** if the backup file is stored in a remote directory.
     b. In the **Server** field, provide the server IP address.
     c. In the **File Path** field, provide the absolute file path to the backup file.
     d. Enter the necessary information in the **Username** and **Password** fields.
5. Enter the **Encryption Key** to the backup file.

   

   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.

6. (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.

7. Click **Next**.
8. Verify the information in the **Summary** page, then click **Restore**.

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

After a restore operation, the performance monitoring (PM) feature is disabled on each fabric. You must manually enable PM on each fabric after the restore. Up to 90 days of historical PM data may be present in the backup and will then appear in the History.

Copyright