Unified Backup and Restore for Nexus Dashboard and Services, Release 3.2.x

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
• ND release 3.2.1 • NDFC release 12.2.2 • NDI release 6.5.1 • NDO release 4.4.1	Unified backup and restore	Beginning with this release, with a few exceptions, backup and restore is no longer available at these individual service levels: • Nexus Dashboard Insights (NDI) • Nexus Dashboard Orchestrator (NDO) • Nexus Dashboard Fabric Controller (NDFC) Instead, a unified backup and restore is now available at the Nexus Dashboard (ND) level, where a backup and restore performed at the ND level backs up not only the configuration information for ND, but also for any services (such as NDI, NDO, or NDFC) running in that ND. This article describes this unified backup and restore process at the ND level, and replaces the individual backup and restore articles that were previously available at the NDI, NDO, and NDFC levels.

Understanding Backup and Restore Operations Before and After Unified Backup

In order to better understand how the unified backup and restore is implemented in ND release 3.2.1, it's helpful to understand how backup and restore was implemented in previous releases for for ND and the separate services.

How Backup and Restore Was Implemented Previously

ND Backup and Restore Prior to ND 3.2.1

Prior to ND 3.2.1, ND backup and restore had the following characteristics:

- Backup and restore was performed by navigating to **Admin > Backup & Restore** in the ND GUI.
- There was no remote backup option; you could only perform local backups.
- There was no backup scheduler available for ND backups.

NDFC Backup and Restore Prior to NDFC 12.2.2

Prior to NDFC 12.2.2, NDFC backup and restore was available for LAN and SAN fabrics.

For both types of fabrics:

- Backup and restore could be performed in the NDFC GUI for:
  - Individual fabrics within the NDFC by navigating to **Manage > Fabrics** and clicking **Actions > Configure Backup**, or
  - For the NDFC as a whole by navigating to **Admin > Backup and Restore**. You could also perform either a Config Only or a Full backup and restore for the NDFC as a whole.
- You could perform either local or remote backups.
- You could perform a manual backup, or use the Backup Scheduler to schedule:
  - The day when you want the scheduler to start.
  - The time of day when you want the scheduler to start.
  - How often the backup should be performed.

NDI Backup and Restore Prior to NDI 6.5.1

Prior to NDI 6.5.1, you would use the import and export of configurations process as the backup and restore for NDI deployments. Import and export was performed by navigating to **Admin > Configuration Import/Export** in the NDI GUI.

NDO Backup and Restore Prior to NDO 4.4.1

Prior to NDO 4.4.1, NDO backup and restore was available for ACI and NDFC fabrics.

For both types of fabrics:

- Backup and restore was performed by navigating to **Admin > Backup and Restore** in the NDO GUI.
- There was no local backup option; you could only perform remote backups.
- Using the Backup Scheduler, you could schedule:
  - The day when you want the scheduler to start.
  - The time of day when you want the scheduler to start.
  - How often the backup should be performed.

How Backup and Restore Is Implemented With the Unified ND 3.2.1 Release

With this ND 3.2.1 release, a unified backup and restore is available at the ND level that allows you to backup and restore configurations for ND and any services (such as NDFC, NDI, or NDO) that are running in that ND. Unified backup and restore is performed by navigating to **Admin > Backup and Restore** in the ND GUI.

- ND Backup and Restore Starting With ND 3.2.1
- NDFC Backup and Restore Starting With NDFC 12.2.2
- NDI Backup and Restore Starting With NDI 6.5.1
- NDO Backup and Restore Starting With NDO 4.4.1

ND Backup and Restore Starting With ND 3.2.1

With the unified backup and restore feature that is introduced in the ND 3.2.1 release, the ND backup and restore functionality, where only the ND configurations were backed up and restored, is no longer available. Instead, a backup and restore performed at the ND level backs up not only the configuration information for ND, but also for any services (such as NDI, NDO, or NDFC) running in that ND.

When backing up a configuration from one ND cluster with the intent of restoring that configuration on a different ND cluster, both clusters must be running the same software version and have the same services enabled (also known as deployment mode).

NDFC Backup and Restore Starting With NDFC 12.2.2

With the unified backup and restore feature that is introduced in the ND 3.2.1 release, the backup and restore functionality for NDFC is essentially provided at the following levels:

- **At the lower-level fabric level**: For individual LAN and SAN fabrics within NDFC, the backup and restore functionality is still provided within the NDFC GUI, just as it was prior to the ND 3.2.1/NDFC 12.2.2 release. See Backing Up and Restoring LAN Operational Mode Setups and Backing Up and Restoring SAN Operational Mode Setups for more information.
- **At the upper-level NDFC level**: Beginning with the ND 3.2.1/NDFC 12.2.2 release, you no longer backup and restore at the NDFC level through the NDFC GUI, and you will backup and restore at this level using the unified backup and restore functionality through the ND GUI instead, as described in this article.

The following table provides more information on the key differences between the backup and restore behavior for NDFC prior to NDFC 12.2.2 and with the unified backup and restore available from NDFC 12.2.2 and later.

NDFC Backup/Restore Feature	Behavior Prior to 12.2.2	Behavior Starting With 12.2.2
Remote repositories	You enter the remote repository information through the NDFC GUI every time you perform a backup or restore.	You enter the remote location (repository) information only once in a central area in the ND GUI, under **Admin > System Settings**, prior to the initial unified backup and restore process. This remote location information is then referenced by any feature that uses remote location, including the unified backup and restore. See Configuring Remote Storage Locations for more information.
List of available backups	Not available; only a history of the operations performed is maintained, with links only for downloading local backups.	A list of available local or remote backups is maintained through the ND GUI.
Ability to restore from a list of available backups	Not supported. Even local backups must be downloaded and uploaded to restore from backup.	Supported. You simply select a backup from the list in the ND GUI to restore it.
History page	Supported through the NDFC GUI with limited information, such as the date, type, and name of the backup.	Supported through the ND GUI. It provides a list of all operations performed and their status.
Scheduled backups	Supported through the NDFC GUI; however, only one scheduled backup is supported.	Supported through the ND GUI. Two scheduled backups are supported.

NDFC Backup/Restore Feature	Behavior Prior to 12.2.2	Behavior Starting With 12.2.2
Fabric-level backup/restore	Available for all NDFC fabrics through the NDFC GUI.	Available for all NDFC fabrics through the NDFC GUI, including multi-cluster, Multi-Site (MSD), and standalone fabrics, except for the Fabric Groups fabric type, which is available through the ND GUI.
NDFC-level backup/restore	Available through the NDFC GUI.	Available through the ND GUI using the unified backup and restore feature.

NDI Backup and Restore Starting With NDI 6.5.1

Even though you will use the unified backup and restore feature that is introduced in the ND 3.2.1 release to back up and restore configurations at the ND level, the existing import and export of configurations process at the NDI level will continue to be available to back up and restore NDI deployments. This is necessary for situations where you might want to restore NDI backups from releases prior to NDI 6.5.1.

For example:

- If you backed up a configuration when you were running on NDI release 6.5.1 or later and you want to restore from that backup, you would use the new unified backup and restore functionality, as described in this document.
- However, if you backed up a configuration when you were running on an NDI release prior to 6.5.1 and you want to restore from that backup, you would use the existing import and export of configurations process at the NDI level to restore that backup.

NDO Backup and Restore Starting With NDO 4.4.1

With the unified backup and restore feature that is introduced in the ND 3.2.1 release, the NDO backup and restore functionality through the NDO GUI is no longer available. Instead, all NDO backup and restore functionality is performed at the ND level, which backs up not only the configuration information for ND, but also for any services (such as NDO) running in that ND.

However, if you have a backup from a release prior to NDO 4.4.1 that you want to use in the restore process, a new **Configuration Import** feature is now available in NDO that allows you to restore backups from NDO release 3.7.2 to release 4.3.1. Refer to the *Nexus Dashboard Orchestrator Backups and Restore* articles for ACI and NDFC fabrics for those procedures.

For example:

- If you backed up a configuration when you were running on ND0 release 4.4.1 or later and you want to restore from that backup, you would use the new unified backup and restore functionality, as described in this document.
- However, if you backed up a configuration when you were running on an ND0 release 3.7.2 to release 4.3.1 and you want to restore from that backup, you would use the new **Configuration Import** feature in NDO as described in the *Nexus Dashboard Orchestrator Backups and Restore* article to restore that backup.

Configuring Remote Storage Locations

The remote storage location information is referenced by any feature that uses remote storage location, including the unified backup and restore.

1. In the ND GUI, navigate to **Admin > System Settings**, then click the **Remote Storage Locations** tab.
   - If you do not have any remote storage locations already created, you will see the message No Remote Locations Found displayed on the page.
   - If you have remote storage locations already created, you'll see those remote storage locations listed with the following values:

Field	Description
Name	The name of the remote storage location.
IP Address	The IP address of the remote storage location.
Protocol	The remote storage location type: ▪ NAS Storage ▪ SFTP
Status	The status of the remote storage location.
Used By	Provides information on who the remote host location is used by.
Username	The username for the remote host location.
Remote Path Filename	The absolute file path to the remote host location.
Allowed Apps	Shows which ND apps are allowed to use this remote location.

2. Create the remote store location.
   - If there are no remote storage locations created yet, click the **Add Remote Storage Location** button that is displayed.
   - If there are remote storage locations listed in this page, click the **Create Remote Storage Location** button that is displayed.

     The **Create Remote Storage Location** window appears.

3. Enter the necessary information to configure the remote storage location.

Field	Description
Name	Enter the name of the remote storage location.
Description	(Optional) Enter a description of the remote storage location.

Field	Description
Remote Storage Location Type	Choose **SFTP/SCP Server** as the remote storage location type.  As mentioned earlier, the remote storage location information is referenced by any feature that uses remote storage location, not just unified backup and restore. Even though **NAS Storage** is provided as an option in the **Create Remote Storage Location**, it is not supported with the unified backup and restore feature.

Use the information in the following table for the **SFTP/SCP Server** option in the **Remote Storage Location Type** field above:

Field	Description
Protocol	Choose the protocol to use for the remote storage location file transfer: • SFTP • SCP
Hostname or IP Address	Enter the hostname or IP address of the remote storage location.
Default Path	Enter the path to the directory where the backup file is to be saved on the remote server. The path must start with a slash character (/ or \) or must be an absolute path. For example: /backups/multisite Or: Users/backups/multisite
Remote Port	Enter the remote port for the remote host location. This field is pre-populated with a default value of 22.
Authorization Type	Choose the authorization type: • Password • SSH Public Types
Username	Enter the authorization username.
Password	Available if you chose **Password** in the **Authorization Type** field above. Enter the authorization password.

Field	Description
SSH Key	The **SSH Key** and **Passphrase** fields are available if you chose **SSH Public Types** in the **Authorization Type** field above. To use SSH keys, you must do the following: 1. Generate the private/public key pairs (with or without a passphrase). 2. Authorize the generated public key on the remote storage location. 3. Enter the private key in the **SSH Key** field. 4. Enter the passphrase (if used in step 1) in the **Passphrase** field.
Passphrase	

4. Click **Save**.

   You are returned to the **Remote Storage Locations** page with the newly-created remote storage location listed in the table.

   - To edit a remote storage location entry, click on the ellipsis (**...**) at the end of the row in the table for that remote storage location and click **Edit**.
   - To delete a remote storage location entry, click on the ellipsis (**...**) at the end of the row in the table for that remote storage location and click **Delete**.

Handling Encryption Keys

At certain points in the backup process, you will be asked to provide an encryption key, which is used to encrypt the backup file. You will then use that same encryption key later on to restore that backup.

When you enter an encryption key as part of the backup process, you must ensure that you do not lose that encryption key information. If the encryption key is lost, the backup is useless because you will not be able to restore the backup without that encryption key.

Backing Up and Restoring ND and Services Configurations

The following sections describe how to back up and restore ND and services configurations.

Guidelines

Following are the guidelines on backing up and restoring ND and services configurations.

- The following guidelines apply specifically for the unified backup and restore functionality that is introduced in this release:
  - The ND unified backup and restore feature is supported only between the same versions of ND. You cannot perform a backup on version X of ND and then restore on version Y of ND.
  - After restoring a backup, the password might change to an older password where the backup was collected. For example, assume you have a cluster that is running with password-1, and you then take a backup and change the password to password-2. When you then go through the backup restore process, after the restore process is finished, the password will be changed back to the older password-1 password.
  - When you perform a backup, all services that are part of the Nexus Dashboard at that time (any services listed in the **Current Deployment Mode**, as described in Backing Up ND and Services Configurations) are backed up. If you perform a restore from that particular backup, you will restore everything from all deployments from that backup.

    For example, assume you have Insights and Orchestrator as the services listed in the **Current Deployment Mode** when you perform a backup. If you were to perform a restore process at a later date using this particular backup, it will restore the configurations for both of those services that were part of that backup.

  - For scheduled backups as described in Configuring Scheduled Backups, a maximum of two scheduled backups is supported.
- The following guidelines apply when backing up and restoring NDFC configurations:
  - Check the **Ignore External Service IP Configuration** check box, as described in Restoring ND and Services Configurations, whenever you take a backup on one system and restore it on a different system, with different management and/or data subnets.
  - NDFC has two backup and restore options: **Config-only** and **Full**. When performing a restore from a backup:
    - You can perform a **Config-only** restore on existing NDFC deployments where features are enabled and other states exist.
    - You can perform a **Full** restore only on a freshly installed cluster, or you must perform an acs reboot clean on the cluster before you can perform a **Full** restore, as described in Nexus Dashboard Troubleshooting.

Backing Up ND and Services Configurations

The following sections describe how to back up ND services and configurations:

- Manually Backing Up ND and Services Configurations
- Configuring Scheduled Backups
- Viewing Backup History

Manually Backing Up ND and Services Configurations

1. Navigate to the unified backup and restore page in the Admin Console GUI:

   Admin > Backup & Restore

   Backups that are already configured are listed in the **Backups** page.

2. Click **Create Backup**.

   The **Create Backup** slider appears.

3. Review the information provided in the **Current Deployment Mode** area.

   This area shows the services that are currently running in this Nexus Dashboard. Note that the unified backup and restore backs up all the services that are shown in this area; you cannot select individual services within the Nexus Dashboard to back up.

4. In the **Name** field, enter a name for this backup.
5. In the **Type** field, determine whether you want a Config-Only or a Full backup.

   

   The Full backup type is not supported for NDI. If you select the Full backup type when backing up an NDI system, a Config-Only backup will actually be performed instead.

   - **Config-Only**: A Config-Only backup is smaller than a Full backup, which is described below. It contains the following configuration data, depending on the services that are being backed up:
     - Insights: Compliance rules, settings, and other configured parameters
     - Orchestrator: Templates, settings, and other configured parameters
     - Fabric Controller: Schedules, templates, policies, and other configured parameters
   - **Full**: A Full backup is large. In addition to everything in a Config-Only backup, a Full backup also contains operational data, such as statistics, counters, and so on. Operational data is only applicable for Fabric Controller; other services will only have configuration backed up.

     When restoring a backup that was saved using the Full backup type, you can perform either a config-only restore or a full restore. Note that you cannot perform a full restore on a cluster that has an existing configuration; the backup must be restored on a new cluster with no existing configuration in this case.

6. In the **Destination** field, determine whether you want a local or remote backup.
   - **Local Download**: The backup data is stored on the local cluster.

You are limited to only one local backup at any time.

a. In the **Encryption Key** field, enter the encryption key to the backup file.

   You must have an encryption key in order to restore from the backup. See Handling Encryption Keys for more information.

- **Remote Location**: The backup data is stored in a remote location.

  a. In the **Remote Location** field, select an already-configured remote location from the list, if available, or click **Create Remote Location**.

     If you click **Create Remote Location**, follow the procedures provided in Configuring Remote Storage Locations, then return here.

  b. In the **Remote Path** field, enter the remote path for the remote backup.

  c. In the **Encryption Key** field, enter the encryption key to the backup file.

     You must have an encryption key in order to restore from the backup. See Handling Encryption Keys for more information.

7. Click **Backup Now**.

   You are returned to the main **Backups** page, with the backup that you just configured now listed.

8. Use the information provided in the **Status** column to monitor the status of your backup.

   You should initially see **In Progress** as the status for your backup as the backup is progressing. Click **View Details** to see additional details on the areas that are being backed up and the progress of those backups.

   After a period of time, the Status should first change to 100%, then will change to **Success**.

9. Click the link in the **Name** column to display additional information on that backup, such as the services that are included with this particular backup and the type of backup that was performed (Config-Only or Full).

   You can also perform the following actions from this window by clicking the **Actions** dropdown:

   - **Delete**: Choose this option to delete the backup.
   - **Download**: Choose this option to download the backup to a local folder.
   - **Restore**: Choose this option to restore a backed up configuration. See Restoring ND and Services Configurations for more information.

In the main **Backups** page, you can also click the ellipsis (...) on any of the backups listed to perform those same actions on any backup.

Configuring Scheduled Backups

1. Navigate to the unified backup and restore page in the Admin Console GUI:

   Admin > Backup & Restore

Backups that are already configured are listed in the **Backups** page.

2. Click the **Backup Schedules** tab.

   Already-configured scheduled backups are listed.

3. Click **Create Backup Schedule**.

   The **Create Backup Schedule** slider appears.

4. Review the information provided in the **Current Deployment Mode** area.

   This area shows the services that are currently running in this Nexus Dashboard. Note that the unified backup and restore backs up all the services that are shown in this area; you cannot select individual services within the Nexus Dashboard to back up.

5. In the **Name** field, enter a name for this backup.
6. In the **Type** field, determine whether you want a Config-Only or a Full backup.
   - **Config-Only**: A Config-Only backup is smaller than a Full backup, which is described below. It contains the following configuration data, depending on the services that are being backed up:
     - Insights: Compliance rules, settings, and other configured parameters
     - Orchestrator: Templates, settings, and other configured parameters
     - Fabric Controller: Schedules, templates, policies, and other configured parameters
   - **Full**: A Full backup is large. In addition to everything in a Config-Only backup, a Full backup also contains operational data, such as statistics, counters, and so on. Operational data is only applicable for Fabric Controller; other services will only have configuration backed up.

     When restoring a backup that was saved using the Full backup type, you can perform either a config-only restore or a full restore. Note that you cannot perform a full restore on a cluster that has an existing configuration; the backup must be restored on a new cluster with no existing configuration in this case.

7. In the **Remote Location** field, select an already-configured remote location from the list, if available, or click **Create Remote Location**.

   If you click **Create Remote Location**, follow the procedures provided in Configuring Remote Storage Locations, then return here.

8. In the **Remote Path Filename** field, enter the remote path for the remote backup.
9. In the **Encryption Key** field, enter the encryption key to the backup file.

   You must have an encryption key in order to restore from the backup. See Handling Encryption Keys for more information.

10. In the **Scheduler** area, select the date and time that you want to use for the backup schedule.
11. In the **Frequency** area, set the frequency that you want for the scheduled backups:
    - Every day
    - Every 7 days
    - Every 30 days

12. Click **Create**.

    You are returned to the **Backup Schedules** page with the newly-created backup schedules listed in the table.

You can view the details of the scheduled backup by clicking on the entry in the **Name** column. You can also view remote location details by clicking on the entry in the **Destination** column.

- To edit a backup schedule entry, click on the ellipsis (**...**) at the end of the row in the table for that backup schedule entry and click **Edit**.
- To delete a backup schedule entry, click on the ellipsis (**...**) at the end of the row in the table for that backup schedule entry and click **Delete**.

Viewing Backup History

1. Navigate to the unified backup and restore page in the Admin Console GUI:

   Admin > Backup & Restore

   Backups that are already configured are listed in the **Backups** page.

2. Click the **History** tab.

   A history of the backups is listed, with the following information:

   - **Name**: The name of the backup.
   - **Date**: The date when an action was taken with regards to a backup.
   - **Action**: The action that was taken on a backup, such as **Created**, **Deleted**, **Downloaded**, **Restored**, and **Updated**.
   - **Type**: The type of backup (**Config-Only** or **Full**).
   - **Details**: Additional detail on a particular backup.
   - **User**: The user associated with a particular backup.
   - **Status**: The status of a backup, such as **Success**, **In Progress**, or **Failure**.

Restoring ND and Services Configurations

1. Determine if you have to on-board NDO fabrics prior to restoring from a backup.

   In these procedures, you will be restoring from a unified backup that you took previously. If NDO services were part of the ND when that unified backup was taken, then you must on-board the NDO fabrics before you begin these restore processes.

2. Navigate to the unified backup and restore page in the Admin Console GUI:

   Admin > Backup & Restore

   Backups that are already configured are listed in the **Backups** page.

3. Access the **Restore** slider page using either of the following methods:

- Click the ellipsis (...) on any backup that you want to restore and choose **Restore**, or
- Click **Restore** in the upper right corner of the main **Backup and Restore** page.

  The **Restore** slide page appears.

4. In the **Source** field, determine where the backup is that you want to restore, if applicable.

   

   If you are restoring a backup by clicking the ellipsis (...) on a specific backup, then this field is not editable.

   - **Upload Configuration Backup Table**: The Backup File area appears, where you can either drag and drop a local backup file to restore or you can navigate to the local area on your system to select a backup file to restore.
   - **Remote Location**:
     a. In the **Remote Location** field, select an already-configured remote location from the list, if available, or click **Create Remote Location**.

        If you click **Create Remote Location**, follow the procedures provided in Configuring Remote Storage Locations, then return here. Even though you should have configured a remote location as part of the remote backup process, you might also have to configure a remote location as part of the restore process if you're in a different cluster from the one where you configured the remote backup. In this case, you would be configuring the remote location again at this point so that the system can find the remote backup that you configured in the other cluster.

     b. In the **Remote Path** field, enter the remote path where the remote backup resides.
5. In the **Encryption Key** field, enter the encryption key that you used when you backed up the file.

   See Handling Encryption Keys for more information.

6. In the Validation area, on the row with your backup, click **Validate and Upload**.

   

   If you entered an incorrect encryption key, an error message will display saying that there was an error during the validation process. Click the trashcan in the line that shows the backup file name to delete the validation attempt and try again.

7. When the Progress bar shows 100% for the validation, the **Next** button becomes active. Click **Next**.

   The Restore window appears, displaying the following information:

   - The current deployment mode
   - The deployment mode of the backup file, which will be the sytem's deployment mode after the restore process is completed
   - The type of backup that was used when the backup file was originally configured (Full or Config-Only)
8. (Optional) Check the **Ignore External Service IP Configuration** check box, if necessary.

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.

9. Click **Restore**.

   A warning window appears to verify that you want to begin the restore process. Note that you will not be able to access any Nexus Dashboard functionality while the restore process runs, which could take several minutes.

10. Click **Restore** in the warning window to proceed with the restore process.

    Another window appears, showing the progress of the restore process. Click the arrow next to the entry in the **Type** column to get more details of the restore process.

11. If the restore process is successful, you will see 100% as the Progress, and the **View History** button becomes active.

    Click **View History** to navigate to the **History** area in the **Backup and Restore** window, with the restore process displayed and **Success** shown in the **Status** column.

Tasks After You Have Restored a Configuration Using Unified Backup

- ND Tasks
- NDI Tasks
- NDFC Tasks

ND Tasks

If you configured connectivity between multiple Nexus Dashboard clusters (also known as "federation," as described in "Multi-Cluster Connectivity" in Nexus Dashboard Infrastructure Management), you will have to re-register the clusters after you have completed the restore process.

The overall steps for this is as follows:

1. Bring up the clusters and add them to the federation.

   See "Connecting Multiple Clusters" in Nexus Dashboard Infrastructure Management.

2. Take a backup on the primary cluster.

   See Backing Up ND and Services Configurations.

3. Perform a clean reboot on the primary cluster.

   See Nexus Dashboard Infrastructure Management.

4. Restore the backup on the primary cluster.

   See Restoring ND and Services Configurations.

5. Re-register all the clusters on the primary cluster after the restore.

   See Nexus Dashboard Infrastructure Management.

NDI Tasks

As part of the new unified backup and restore feature, a new resync workflow is introduced at the NDI level to bring the NDI fabrics status back in sync. You must perform certain resync tasks after restoring a configuration using the new unified backup and restore.

After you have restored a configuration that was backed up using the new ND unified backup and restore feature, the state of the NDI fabrics shown at the ND level could be out of sync with the true state of the NDI fabrics. As an example, assume the following scenario:

1. You have software telemetry enabled on a fabric and the telemetry configurations are pushed to the fabric.
2. You then take a backup using the new unified backup process.
3. Afterward, assume you then disable telemetry, which removes the configurations from the fabrics.
4. You then go through the backup restore process, as described in this article. Afterwards, the NDI configuration will show software telemetry as enabled but the fabric does not have that same status.

   To bring the NDI fabrics status back in sync, go to the NDI GUI and perform a resync operation there, either on each NDI fabric or across all NDI fabrics, using the new NDI resync operation introduced in the NDI 6.5.1 release. This will clean up any existing configurations on the NDI fabrics and will push all of the new configurations from NDI to the fabrics.

Before performing a resync operation in the NDI GUI, all switches belonging to NX-OS fabrics in NDFC must be in one of these states:

- InSync
- OutOfSync
- Pending

If not, the resync operation will fail with a message that the fabric is not ready. You must bring the switches to these states before continuing with the resync operation.

In a co-location scenario, where the first cluster is hosting NDFC and the second cluster is hosting NDI, if the first cluster (which is running on NDFC release 12.2.2 or later) is restored, all of the fabrics remotely onboarded on the remote NDI cluster will move to an OutOfSync state. You must then perform the resync operation to get the fabrics back in sync with NDI in this case. Note that this prerequisite does not apply if the first cluster is on a release earlier than NDFC 12.2.2.

If you have Netflow configured on your NDI, during the restore process of NDI or NDFC, if the intent is wiped out from NDFC, triggering a resync will wipe out these Netflow configurations from the switches. You will have to add your intents back to NDFC accordingly to restore your configurations.

NDFC Tasks

Similarly, for NDFC, after you have restored a configuration that was backed up using the new ND unified backup and restore feature, the state of the NDFC fabrics shown at the ND level might be out of sync with the true state of the NDFC fabrics. To bring the NDFC fabrics status back in sync, in the **Fabric Overview** page, click **Actions** at the top of the page and select **Recalculate and Deploy**.

SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)