Backing Up and Restoring Your Nexus Dashboard, Release 4.2.1

Table of Contents

New and changed information

This 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
Nexus Dashboard 4.2.1	Backup and restore of telemetry operational data	Beginning with Nexus Dashboard 4.2.1, you can now back up and restore telemetry operational data. See Backing up and restoring telemetry operational data for more information.

Understanding backup and restore operations before and after the unified system

In order to better understand how the unified backup and restore is implemented in release 4.2.1, it is helpful to understand how backup and restore was implemented in previous releases.

- How backup and restore operations were implemented before unified backup (prior to Nexus Dashboard release 3.2.1)
- How backup and restore operations were implemented with unified backup in Nexus Dashboard release 3.2.1
- How backup and restore operation is implemented with the unified system in Nexus Dashboard release 4.1.1 and later

How backup and restore operations were implemented before unified backup (prior to Nexus Dashboard release 3.2.1)

Prior to Nexus Dashboard release 3.2.1, backup and restore operations were performed at the Nexus Dashboard level, as well as at the individual services levels that were running in that Nexus Dashboard (Nexus Dashboard Fabric Controller, Nexus Dashboard Insights, and Nexus Dashboard Orchestrator). Refer to Unified Backup and Restore for Nexus Dashboard and Services for more information.

How backup and restore operations were implemented with unified backup in Nexus Dashboard release 3.2.1

With the Nexus Dashboard 3.2.1 release, a unified backup and restore operation became available at the Nexus Dashboard level that allowed you to back up and restore configurations for Nexus Dashboard and any services (Nexus Dashboard Fabric Controller, Nexus Dashboard Insights, and Nexus Dashboard Orchestrator) running in that Nexus Dashboard. Refer to Unified Backup and Restore for Nexus Dashboard and Services for more information.

How backup and restore operation is implemented with the unified system in Nexus Dashboard release 4.1.1 and later

With the unified system that is part of Nexus Dashboard release 4.1.1, there are no longer any individual services (Nexus Dashboard Fabric Controller, Nexus Dashboard Insights, and Nexus Dashboard Orchestrator) running separately beneath the upper level Nexus Dashboard; instead, all the individual services are bundled together with Nexus Dashboard as a single, unified system.

The unified backup and restore feature introduced in the Nexus Dashboard 3.2.1 release is essentially unchanged in release 4.1.1.

Backing up and restoring Nexus Dashboard configurations

These sections describe how to back up and restore Nexus Dashboard configurations.

- Guidelines and limitations for backing up and restoring Nexus Dashboard configurations
- Handling encryption keys
- Back up Nexus Dashboard configurations
- Restore Nexus Dashboard configurations

Guidelines and limitations for backing up and restoring Nexus Dashboard configurations

These sections provide the guidelines for backing up and restoring Nexus Dashboard configurations.

- General guidelines and limitations for backing up and restoring Nexus Dashboard configurations
- Guidelines and limitations: Backing up and restoring telemetry operational data

General guidelines and limitations for backing up and restoring Nexus Dashboard configurations

These general guidelines apply for backing up and restoring Nexus Dashboard configurations.

- The Nexus Dashboard unified backup and restore feature is supported only between the same versions of Nexus Dashboard. You cannot perform a backup on version X of Nexus Dashboard and then restore on version Y of Nexus Dashboard.
- You can only restore a multi-node backup on the a system with the same or greater number of nodes in the cluster. For example, if you backed up a 3-node physical cluster configuration, you can only restore that backup on a system with a 3-node or greater physical cluster. However, backing up a configuration from 5-node virtual cluster and restoring the configuration on 3-node virtual cluster is supported.
- If a backup is taken from a federated cluster, then the cluster where you are restoring must have the same cluster name; otherwise, the restore will fail.
- Restoring a backup on a cluster that supports a fewer number of Apps as compared to the cluster from where the backup was taken is not supported.
- After restoring a backup on a freshly-installed cluster, the credentials of the freshly-installed cluster are retained. This is different from the behavior in releases prior to Nexus Dashboard release 4.1.1, where the credentials of the source cluster where the backup was collected are applied on the restored cluster. We recommend that you update the credentials of the cluster after the restore operation as per your requirements.
- After performing a restore operation, all anomalies and advisories (including Active Bug anomalies and Best Practices advisories) are cleared. Nexus Dashboard retains the last run time of bug scan and best practices jobs after a restore operation, which are displayed in **Admin > System Status > Telemetry > Switches**. Nexus Dashboard then waits for 7 days to elapse for the devices' last run time before scheduling the next bug scan and best practices jobs, so you will start getting

fresh bug anomalies and best practices advisories only after the next job has completed.

- Nexus Dashboard stores local users with their passwords in the backup. When restoring from a backup, local users with their original passwords are created from the backup. However, if an existing local user has the same username as one from the backup, the existing user's password is not be replaced.

- These are the guidelines for the maximum number of backups:

  - For scheduled backups as described in Configure scheduled backups, a maximum of two scheduled backups is supported.
  - For manual backups, a default value of two backups is configured in the **Maximum Backups per Fabric** field under **Admin > System Settings > Fabric management > LAN-Fabric**; however, you can change the maximum number of backups in that field.

  When new backups take place, the oldest backup over the maximum number gets removed automatically.

- Put a check in the **Ignore External Service IP Configuration** check box, as described in Restore Nexus Dashboard configurations, whenever you take a backup on one system and restore it on a different system with different management or data subnets.

- Backup or restore operations do not impact Device Connector sessions, because the Device Connector does not include specific backup or restore functionality and continues to operate as configured following a restore operation. However, the Device Connector relies on Nexus Dashboard proxy settings to connect to Cisco Intersight. If these proxy settings are changed during a restore operation, the connection to Intersight may be interrupted. For more information, see Configure Device Connector settings.
- Nexus Dashboard 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 Nexus Dashboard deployments where features are enabled and other states exist.
  - You can perform a **Full** restore on a freshly installed cluster or on an existing cluster after you performed an acs reboot clean on the cluster before you can perform a **Full** restore, as described in Cisco Nexus Dashboard Troubleshooting.
- If you are migrating from a config-profile to CLI overlay mode, restoring a Nexus Dashboard configuration to a pre-migration state is not supported. Best practice is to take a Nexus Dashboard backup before and after the migration.

Guidelines and limitations: Backing up and restoring telemetry operational data

This section provides the guidelines and limitations when backing up and restoring telemetry operational data, as described in Backing up and restoring telemetry operational data.

- A **Full** backup of telemetry operational data is performed only when you have met these conditions:

  - In the **Create Backup** page, you choose a **Full** backup as the backup **Type** and you check the box in the **Include telemetry operational data** field. See Manually back up Nexus Dashboard configurations for more information.

    - You have a remote storage location created for the backup. In addition, you must use **NAS Storage** as the **Remote Storage Location Type**. See Create a remote storage location for more information.

- You must ensure that there is sufficient storage available on the NAS storage for the **Full** backup of telemetry operational data. You will need around 275GB for 1000 switches, which is the maximum number of switches that are supported across any form factors. Nexus Dashboard displays the size of the backup during the backup process.

  In addition, we recommend the following for the NAS storage:

    - A 10GB link between the Nexus Dashboard and the NAS storage
    - SSDs as the storage devices in the NAS storage
- The telemetry operational data that is backed up is not encrypted on the NAS storage; it is your responsibility to make sure that the disk is encrypted to protect your data. However, the configuration backup that gets collected as part of the telemetry operational backup is encrypted, just as it was in previous releases.
- After a backup of telemetry operational data is complete, the NAS storage will contain a directory with the name of the backup, based on the value that you provided in the **Name** field when you created the backup. This directory contains:
    - A tar.gz file that contains all the configurations on the Nexus Dashboard and its Apps.
    - A directory where the telemetry operational data is backed up.
- You can perform manual or scheduled **Full** backups of telemetry operational data. However, only one schedule for a **Full** backup of telemetry operational data on NAS storage is supported.
- If you delete backups from Nexus Dashboard, this only clears out the local metadata on the Nexus Dashboard. If you want to delete the remote backup from the NAS storage, you must manually delete those backups on the NAS storage.
- Nexus Dashboard backs up one month worth of operational, historical, and telemetry configuration data. For historical data, the granularity is either 5 minutes or 3 hours, depending on the point in the one-month cycle (historical data for the past week has 5-minute granularity, and any beyond has 3-hour granularity). After a restore, all historical data is provided at 3-hour granularity.
- A Full restore operation is only supported on a fresh installation of Nexus Dashboard.
- Telemetry data can be extremely large, so backing up and restoring telemetry operational data might take a long period of time. In addition, the backup and restore time is affected by the network speed between the Nexus Dashboard system and the NAS system. As an example, a 600GB backup and restore, with a 1GB link between the Nexus Dashboard system and the NAS system, might take around 2.5 hours.

Backing up and restoring telemetry operational data

Prior to Nexus Dashboard release 4.2.1, support was available for backing up and restoring configurations using either **Config-Only** or **Full** type backups and restores. However, if you chose a **Full** backup, Nexus Dashboard did not support the backup and restore of operational or specific historical telemetry data and would only back up the telemetry configuration.

Beginning with Nexus Dashboard release 4.2.1, support is now available for performing a **Full** backup

and restore on telemetry data, where telemetry operational data is backed up and restored, along with telemetry configuration data.

See Guidelines and limitations: Backing up and restoring telemetry operational data for guidelines and limitations when backing up and restoring telemetry operational data.

- Data that is and is not backed up
- Post restore tasks

Data that is and is not backed up

These sections list the data that is and is not backed up as part of this feature.

- Data that is backed up
- Data that is not backed up

Data that is backed up

For the granularity of the data backup, see Guidelines and limitations: Backing up and restoring telemetry operational data.l

- Interface stats/operational data
- Environmental data (CPU/memory/temperature, and so on)
- Capacity data
- Endpoints
- Layer 3 neighbors
- Routes (only history)
- Cleared anomalies (both system and fabric)

Data that is not backed up

- Active anomalies
- Software telemetry 5-minute granular statistics
- Auditing routing information
- Flows (FT/TA), anomalies raised by Flow pipeline
- MongoDB data. These features will not have historical data after restore:
  - Assurance
  - Compliance
  - Delta Analysis
  - PolicyCAM
  - Orchestrator Assurance
- Metadata

- Advisories
- Tech Supports for switches
- Kafka messages

Post restore tasks

All fabrics will be in the out-of-sync state after a restore and are not usable in this state. After you have performed a restore from this type of backup, you will have to perform a Reconfigure operation to bring the fabrics back in sync. See Telemetry tasks in the Tasks after you have restored a configuration using unified backup section for more information.

Create a remote storage location

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

1. In the Nexus Dashboard GUI, navigate to **Admin > System Settings**.

   The **General** tab is chosen by default.

2. Locate the **Remote storage** area in **General**.
   - If you do not have any remote storage locations already created, you will see the message No remote storage added 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.
Description	A description of the remote storage location, if necessary.
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.

3. If there are no remote storage locations created yet, click **Edit** in the **Remote storage** area.

   The **Remote storage** page appears.

4. Click **+ Add remote storage locations** to create a remote storage location.

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

5. In the **Create Remote Storage Location** window, 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.
Remote Storage Location Type	Choose the remote storage location type: • SFTP/SCP Server • NAS Storage

6. Enter the necessary information to configure the remote storage location.
   - If you chose the **NAS Storage** option in the **Remote Storage Location Type** field, enter the necessary information in these fields.

Field	Description
Type	Choose the type of configuration for the NAS storage: • **Read Write**: Data can be read from and written to the NAS mount point by Nexus Dashboard hosts. • **Read Only**: Data can only be read from the NAS mount point by Nexus Dashboard hosts.
Hostname/IP	Enter the hostname or IP address of the remote storage location.
Port	Enter the port for the NAS storage. This field is pre-populated with a default value of 2049.
Export path	Enter the path to the directory where the backup file is to be saved on the remote server. • The path can be an absolute path, which would start with a slash character (/), such as: /backups/multisite • Or the path can be a path relative to your home directory, such as: Users/backups/multisite
Alert threshold	Enter the alert threshold. When the NAS volume usage exceeds this percentage value, a fault will be raised. This field is pre-populated with a default value of 80.
Limit (MB/GB)	Enter the limit value, in MB or GB, if necessary. If set, this is the total size that should not be exceeded by Nexus Dashboard when allocating storage on this NAS volume. For example: 500MB, 1GB.

   - If you chose the **SFTP/SCP Server** option in the **Remote Storage Location Type** field, enter the necessary information in these fields.

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 can be an absolute path, which would start with a slash character (/), such as: /backups/multisite • Or the path can be a path relative to your home directory, such as: 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 • CyberArk
Username	Enter the authorization username.
Password	Available if you chose **Password** in the **Authorization Type** field above. Enter the authorization password.
SSH Key	The **SSH Key** and **Passphrase** fields are available if you chose **SSH Public Types** in the **Authorization Type** field. To use SSH keys, follow these steps: 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. If you used a passphrase in step 1, enter the passphrase in the **Passphrase** field.
Passphrase	

Field	Description
Credential Store key	The **Credential Store key** field is available if you choose **CyberArk** in the **Authorization Type** field. You will see the **CyberArk** tab only if you configured system certificate and mapped to CyberArk feature. For more information on CA certificates and credential store, see Managing Certificates in your Nexus Dashboard and Configuring Users, Roles, and Security.

7. Click **Save**.

   You are returned to the **Remote storage** 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**.

8. Click Save in the **Remote storage** page.

   You are returned to the **System Settings/General** page.

Handling encryption keys

At certain points in the backup process, the process prompts you to provide an encryption key to encrypt the backup file. You will use the same encryption key later to restore the backup.

When you enter an encryption key as part of the backup process, do not lose the encryption key information. If you lose the encryption key, the backup is useless because you cannot restore the backup without the encryption key. Cisco is also not able to restore a backup if you lose the encryption key information.

Back up Nexus Dashboard configurations

These sections describe how to back up ND services and configurations.

- Manually back up Nexus Dashboard configurations
- Configure scheduled backups
- View backup history

Manually back up Nexus Dashboard configurations

1. Navigate to the unified backup and restore page in the Nexus Dashboard GUI:

   Admin > Backup and Restore

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

2. Click **Create backup**.

   The **Create backup** page appears.

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

   

   If you choose **Full** backup, Nexus Dashboard now supports the backup and restore of telemetry operational data, along with the telemetry configuration. See Backing up and restoring telemetry operational data for more information.

   - **Config-Only**: A Config-Only backup is smaller than a Full backup. It contains configuration data that depends 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 and counters. Operational data is only applicable for Fabric Controller; other services only have configuration data 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.

     

     You cannot perform a Full restore on a cluster that has an existing configuration; you must restore the backup on a new cluster with no existing configuration.

5. Determine if you want to back up and restore telemetry operational data, now supported in Nexus Dashboard release 4.2.1.

   See Backing up and restoring telemetry operational data for more information.

   If you want to back up and restore telemetry operational data, along with the telemetry configuration:

   a. Verify that you chose **Full** as the backup **Type**.
   b. After choosing **Full** as the backup **Type**, check the box in the **Include telemetry operational data** field.
      - The **Include telemetry operational data** field only appears if you choose **Full** as the backup **Type**.
      - In addition, the **Destination** field is grayed out because you can only perform a remote backup in this case. Enter the necessary information for the remote storage using the **Remote storage location** information provided in the next step.

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 to restore from the backup. See Handling encryption keys for more information.

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

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

     If you click **Create remote storage location**, follow the steps provided in Create a remote storage location, then return here.

  b. In the **Remote path** field, review the remote path that is being used for the remote backup.

     When taking backups, the **Remote path** field is not editable; it shows the path that was configured when you created the remote storage using the procedures provided in Create a remote storage location. The backup will be created in that location.

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

     You must have an encryption key 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 progresses. 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 changes to **100%**, then changes to **Success**.

   

   Sometimes, even if the overall progress appears green, there might be some warnings or errors. You need to review the sub-tasks to check for these warnings or errors.

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 these actions from this window by clicking the **Actions** dropdown:

   - **Delete**: Deletes the backup.
   - **Download**: Downloads the backup to a local folder.
   - **Restore**: Restores a backed up configuration. See Restore Nexus Dashboard 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.

Configure scheduled backups

1. Navigate to the unified backup and restore page in the Nexus Dashboard GUI:

   Admin > Backup and Restore

   The **Backups** page lists backups that are already configured.

2. Click **Backup Schedules**.

   This tab lists already-configured scheduled backups.

3. Click **Create backup schedule**.

   The **Create backup schedule** drawer appears.

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.

   

   If you choose **Full** backup, Nexus Dashboard does not support the backup and restore of operational or historical telemetry data and will only back up the telemetry configuration.

   - **Config-Only**: A Config-Only backup is smaller than a Full backup. It contains configuration data that depends on the services that are being backed up:
     - Insights: Compliance rules, settings, and other configured parameters
     - Orchestrator: Templates, settings, 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 and counters. Operational data is only applicable for Fabric Controller; other services 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.

     

     You cannot perform a Full restore on a cluster that has an existing configuration; you must restore the backup on a new cluster with no existing configuration in this case.

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

   If you click **Create Remote Location**, follow the steps provided in Create a remote storage location, then return here.

7. In the **Remote path** field, review the remote path that is being used for the remote backup.

   When taking backups, the **Remote path** field is not editable; it shows the path that was configured when you created the remote storage using the procedures provided in Create a remote storage location. The backup will be created in that location.

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

You must have an encryption key to restore from the backup. See Handling encryption keys for more information.

9. Enter the necessary information in the **Scheduler** area.
   a. In the **Starting Date and Time** field, choose the date and time that you want to use for the backup schedule, then click OK.
   b. In the **Frequency** area, set the frequency that you want for the scheduled backups.

      When scheduling backups for telemetry operational data, only 7 days cadence is supported.

      - Every 24 hours
      - Every 7 days
      - Every 30 days
10. Click **Create**.

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

    - To view the details of the scheduled backup, click on the entry in the **Name** column. You can also edit or delete the scheduled backup configuration in this page.
    - To view remote location details, click 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**.

The created scheduled backups will also be listed under the **Backups** tab. In **Backups**, click the entries in the **Destination** or **Schedule** columns to view details related to those areas.

View backup history

1. Navigate to the unified backup and restore page in the Nexus Dashboard GUI:

   Admin > Backup and Restore

   The **Backups** page lists backups that are already configured.

2. Click **History**.

   The **History** tab lists a history of the backups, with the following information:

   - **Start Time**: The start time when an action was taken for a backup.
   - **End Time**: The end time when an action was taken for 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**.

Restore Nexus Dashboard configurations

1. Navigate to the unified backup and restore page in the Nexus Dashboard GUI:

   Admin > Backup and Restore

   The **Backups** page lists already-configured backups.

2. Access the **Restore** page page by
   - choosing the entry in the list of backups shown in the **Backups** page, then clicking **Actions > Restore**, or
   - clicking **Restore** in the upper right corner of the main **Backup and Restore** page.

     The **Restore** page appears.

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

   

   If you are restoring a backup by choosing the a specific backup in the list of backups shown in the **Backups** page, then this field is not editable.

   - **Backup File**: Either drag and drop a local backup file to restore or you can navigate to the local area on your system to choose a backup file to restore.
   - **Remote Storage Location**:
     a. In the **Remote Storage Location** field, choose an already-configured remote location from the list, if available, or click **Create remote storage location**.

        If you click **Create Remote Storage Location**, follow the steps provided in Create a remote storage location, 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 **File name** field, provide a path to the backup file that you want to restore.

        The path can be
        - absolute, where it starts with a slash (/) (for example, /remote/storage/mybackup.tar.gz), or
        - relative to the path specified in **Remote Storage Location** (for example, mybackup.tar.gz or backups/mybackup.tar.gz)

4. 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.

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

   If you entered an incorrect encryption key, an error message displays 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.

6. After the Progress bar shows 100% for the validation, click **Next**.

   The Restore page appears, displaying this 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)

7. (Optional) Put a check in the **Ignore External Service IP Configuration** check box, if necessary.

   If you put a check in the **Ignore External Service IP Configuration** check box, 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 or data subnets.

8. Click **Restore**.

   A warning appears that prompts you to verify that you want to begin the restore process.

   You will not be able to access any Nexus Dashboard functionality while the restore process runs, which could take several minutes.

9. Click **Restore** in the warning page to proceed with the restore process.

   Another page 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.

10. After the Progress bar shows 100% for the restore process, click **View History** to navigate to the **History** area in the **Backup and Restore**.

    The page displays **Success** in the **Status** column for the restore process.

Tasks after you have restored a configuration using unified backup

- Nexus Dashboard tasks
- Orchestration tasks
- Telemetry tasks

Nexus Dashboard tasks

If you configured connectivity between multiple Nexus Dashboard clusters, you will have to re-register the clusters after you have completed the restore process.

These are the overall steps for this process:

1. Bring up the clusters and establish multi-cluster connectivity.

   See Connecting Clusters.

2. Create a backup on the primary cluster.

   See Back up Nexus Dashboard configurations.

3. Perform a clean reboot on the primary cluster.

   See Connecting Clusters.

4. Restore the backup on the primary cluster.

   See Restore Nexus Dashboard configurations.

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

   See Connecting Clusters.

Orchestration tasks

If you had the Orchestration feature enabled when you performed a Nexus Dashboard backup, after you re-register the ACI fabrics, it takes about 2-3 minutes to trigger the post-restore Orchestration tasks. You can track the progress of this update by navigating to the **Orchestration** page in Nexus Dashboard (**Manage > Orchestration**).

Telemetry tasks

Nexus Dashboard has a reconfigure workflow that brings the telemetry-enabled fabrics status back in sync. You must perform certain reconfigure tasks after restoring a configuration.

After you have restored a configuration that was backed up, the state of the telemetry-enabled fabrics shown at the Nexus Dashboard level could show as Out of Sync, which indicates that those fabrics are out of sync with the true state of the telemetry-enabled fabrics and telemetry streaming is not functional. When telemetry-enabled fabrics are out of sync in this fashion, the status of individual features (such as software telemetry, flow collection, and switch status) are not valid and should be ignored.

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 create 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. Afterward, the Nexus Dashboard configuration will show software telemetry as enabled but the fabric does not have that same status.

To bring the telemetry-enabled fabrics status back in sync and reapply telemetry configurations to the fabric:

1. Verify the switches are in the proper state.

Before performing a reconfigure operation in the Nexus Dashboard GUI, all switches belonging to NX-OS fabrics must be in one of these states:

- InSync
- OutOfSync
- Pending

If not, the reconfigure operation fails for the entire fabric, with a message that the fabric is not ready, if there is a single switch that is not in one of those states. You must bring the switches to one of these states before continuing with the reconfigure operation.

2. Perform the reconfigure operation.

   You can perform a reconfigure operation:

   - Either on each fabric, by clicking on that fabric in **Manage > Fabrics** to navigate to that fabric's **Overview** page and clicking **Actions > Telemetry > Reconfigure**, or
   - Across all fabrics, by navigating to **Admin > System Status > Telemetry** and clicking on **Reconfigure All**, then clicking **Confirm** in the confirmation pop-up.

   This cleans up any existing configurations on the telemetry-enabled fabrics and pushes all new configurations from Nexus Dashboard to the fabrics.

3. Verify that the individual features are reflecting the proper status.

   After the operation completes, the individual feature statuses will be:

   - Enabled if the configuration push is successful for all switches,
   - Enable Fail if it fails for any switch, or
   - Enable Pending if change control mode is enabled.

   The cumulative **Telemetry Configuration Status** will then display as:

   - OK if the configuration is successful for all switches,
   - Not OK if it fails or is pending in change control mode for all switches, or
   - Partial OK if it succeeds for some switches and fails or is pending in change control mode for others.

4. Perform any post-reconfiguration operations, if necessary.

   If you have Netflow configured on Nexus Dashboard, during the restore process, if the intent is wiped out from Nexus Dashboard, triggering a reconfigure will wipe out these Netflow configurations from the switches. You must add your intents back to Nexus Dashboard accordingly to restore your configurations.

Backing up and restoring fabric configurations

These sections describe how to back up and restore fabric configurations.

- Back up fabric configurations
- Restore fabric configurations

General guidelines for backing up and restoring fabric configurations

These general guidelines apply for backing up and restoring fabric configurations.

- When you perform a fabric-level backup in release 4.2.1, any settings that you have configured in the **General** and **Telemetry** tabs at the fabric level will be backed up, and those settings will be restored when you perform a restore operation from that backup.
- You cannot perform a fabric-level backup and restore operation on ACI fabrics in Nexus Dashboard.
- Nexus Dashboard 4.2.1, unified backup feature includes new fields in **General** under **Edit Fabric Settings**.

Field	Description
Name	The name of the fabric.
Type	The description of the fabric type.
Location	The location the fabric is deployed.
Overlay routing protocol	The overlay fabric connectivity option.
BGP ASN for spines	The BGP AS number associated with the fabric.
License tier for fabric	The license type of the fabric.
Enabled features	The telemetry support option.
Security domain	The access privileges for the users.

Back up fabric configurations

These sections describe how to back up fabric configurations.

- Manually back up fabric configurations
- Configure scheduled fabric backups

Manually back up fabric configurations

1. Navigate to the fabric backup and restore page in the Nexus Dashboard GUI:
   a. Navigate to the main Fabrics page:

      Manage > Fabrics

b. Click on a fabric that you want to back up.

   The **Overview** page for that fabric appears.

c. Click **Actions > Maintenance > Backup Now**.

   The **Create Fabric Backup** page appears.

d. Enter the name of the **Backup Tag** and click **Create Backup**.

   The backup is initiated.

Configure scheduled fabric backups

1. Navigate to the fabric backup and restore page in the Nexus Dashboard GUI:
   a. Navigate to the main Fabrics page:

      Manage > Fabrics

   b. Click on a fabric that you want to back up.

      The **Overview** page for that fabric appears.

   c. Click **Actions > Maintenance > Backup Now**.

      The **Create Fabric Backup** page appears.

   d. Enter the name of the **Backup Tag** and click **Create Backup**.

      The backup is initiated.

Restore fabric configurations

1. Navigate to the fabric backup and restore page in the Nexus Dashboard GUI:
   a. Navigate to the main Fabrics page:

      Manage > Fabrics

   b. Click on a fabric that you want to back up.

      The **Overview** page for that fabric appears.

   c. Click **Actions > Maintenance > Restore Fabric**.

      The **Restore Fabric** page appears.

   d. Select a backup from the list and click **Next**.

      The **Restore Preview** page appears.

   e. Review the content for the configuration changes and click **Restore Intent**.

      The restore is initiated.

Tasks after you have restored a fabric configuration using unified backup

Telemetry tasks

Nexus Dashboard has a reconfigure workflow that brings the telemetry-enabled fabrics status back in sync. You must perform certain reconfigure tasks after restoring a fabric configuration.

After you have restored a fabric configuration that was backed up, the state of the telemetry-enabled fabrics shown at the Nexus Dashboard level could show as Out of Sync, which indicates that those fabrics are out of sync with the true state of the telemetry-enabled fabrics and telemetry streaming is not functional. When telemetry-enabled fabrics are out of sync in this fashion, the status of individual features (such as software telemetry, flow collection, and switch status) are not valid and should be ignored.

To bring the telemetry-enabled fabrics status back in sync and reapply telemetry configurations to the fabric:

1. Verify the switches are in the proper state.

   Before performing a reconfigure operation in the Nexus Dashboard GUI, all switches belonging to NX-OS fabrics must be in one of these states:

   - InSync
   - OutOfSync
   - Pending

   If not, the reconfigure operation fails for the entire fabric, with a message that the fabric is not ready, if there is a single switch that is not in one of those states. You must bring the switches to one of these states before continuing with the reconfigure operation.

2. Perform the reconfigure operation by clicking on that fabric in **Manage > Fabrics** to navigate to that fabric's **Overview** page and clicking **Actions > Telemetry > Reconfigure**.

   This cleans up any existing configurations on the telemetry-enabled fabrics and pushes all new configurations from Nexus Dashboard to the fabrics.

Copyright

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883