Nexus Dashboard Orchestrator Backups and Restore for NDFC Fabrics, Release 4.4.x

Table of Contents

Updates to Backup and Restore in Nexus Dashboard Orchestrator Release 4.4.1

Beginning with Nexus Dashboard Orchestrator release 4.4.1, backup and restore is no longer available at the Nexus Dashboard Orchestrator (NDO) service level. 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 NDO, running in that ND, as described in Unified Backup and Restore for Nexus Dashboard and Services.

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.

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 Unified Backup and Restore for Nexus Dashboard and Services.
- 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 to restore that backup, as described below.

Restoring a Backup Using Configuration Import

1. Log in to your Cisco Nexus Dashboard Orchestrator.
2. Navigate to **Admin > Configuration Import**.
3. Click **Import Backup File.**

   The **Import Backup File** popup appears.

4. Choose the location where the backup file is stored and provide the necessary information:
   - **Remote**: Provide the URL to the backup file stored in the remote location, using this format:

     ```
     http[s]://IP:[:port]/path/filename
     ```

     Note that this remote URL must be publicly accessible within the network. It must not request for authentication.

   - **Local**: Navigate to the local folder where you have the backup file stored, then drag and drop the file into the area in the window, or click **Browse** to navigate to the local folder where you have the backup file stored and select that file.
   - **SCP**: Enter the necessary information to restore a remote file using SCP:
     - **Hostname/IP Address**: Provide the host name or IP address of the remote server where you saved the backup.
     - **Port**: Specify the port used to connect to the remote server.

For example, 22.

- **File Path**: Provide the full path to a directory on the remote server where you saved the backup.

  The path must start with a slash (/) characters and must not contain periods (.) or backslashes (\). For example, */backups/multifabric*.

  > The directory must exist on the remote server.

- **Username**: Provide the username that is used to sign in to the remote server.
- **Authentication Type**: Specify the authentication type used when connecting to the remote server.
  - **Password**: Provide the password that is used to sign in to the remote server.
  - **SSH Public/Private Files**: Provide the SSH Key/Passphrase pair that is used to sign in to the remote server.

5. Click **Restore**.

First Published: 2024-03-11
Last Modified: 2024-07-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883