Backup and Restore

About Backup and Restore

You can use the backup and restore functions to create backup files to restore to a different appliance (if required for your network configuration).

Backup

You can back up automation data only or both automation and Assurance data.

Automation data consists of Cisco DNA Center databases, credentials, file systems, and files. The automation backup is a full backup.

The Assurance data consists of network assurance and analytics data. The first backup of Assurance data is a full backup. After that, backups are incremental.

Important Do not modify the backup files. If you do, you might not be able to restore the backup files to Cisco DNA Center.

Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements, on page 3.

Only a single backup can be performed at a time. Performing multiple backups at once is not supported.

When a backup is being performed, you cannot delete the files that have been uploaded to the file service, and changes that you make to these files might not be captured by the backup process.

We recommend the following:

- Perform a daily backup to maintain a current version of your database and files.
- Perform a backup after making changes to your configuration, for example, when changing or creating a new policy on a device.
- Perform a backup only during a low-impact or maintenance period.

You can schedule weekly backups on a specific day of the week and time.

Restore

You can restore the backup files from the remote server using Cisco DNA Center.

When you restore the backup files, Cisco DNA Center removes and replaces the existing database and files with the backup database and files. While a restore is being performed, Cisco DNA Center is unavailable.

You cannot do a backup from one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You can only restore a backup to an appliance that is running the same Cisco DNA Center software release with the same first four digits and the same application versions as the appliance from which the backup was taken. To view the current applications and versions, choose **System** > **Software Management** and click **Currently Installed Applications**.

You can restore a backup to a Cisco DNA Center appliance with a different IP address. This situation could happen if the IP address is changed on Cisco DNA Center and you need to restore from an older system.

Important After a backup and restore of Cisco DNA Center, you need to access the **Integration Settings** window and update (if necessary) the **Callback URL Host Name** or **IP Address**. For more information, see Configure Integration Settings.

Backup and Restore Event Notifications

You can receive a notification whenever a backup or restore event takes place. To configure and subscribe to these notifications, complete the steps described in the "Work with Event Notifications" topic of the *Cisco DNA Center Platform User Guide*. When completing this procedure, ensure that you select and subscribe to the SYSTEM-BACKUP and SYSTEM-RESTORE events.

A notification is generated and sent whenever an event listed in the following table occurs:

Operation	Event
Backup	The process to create a backup file for your system has started.
	A backup file could not be created for your system. This event typically happens because: • The necessary disk space is not available on remote storage. • You are unable to fetch the status of your system's server, which is a precheck for the backup operation. • You encountered connectivity issues or latency while creating a backup file on your system.

Operation	Event
Restore	The process to restore a backup file has started.
	The restoration of a backup file failed. This event typically happens because: • The backup file has become corrupted. • You encountered connectivity issues or latency while creating a backup file from your system.

Backup Server Requirements

The backup server must run one of the following operating systems:

- RedHat Enterprise (or CentOS) 8 or later
- Ubuntu 16.04 (or Mint, etc) or later

Server Requirements for Automation Data Backup

To support automation data backups, the server must meet the following requirements:

- Must use SSH (port22)/remote sync (rsync). Cisco DNA Center does not support using FTP (port 21) when performing a backup.
- The Linux rsync utility must be installed.
- *(Not applicable to RedHat 7/CentOS 7)* The C.UTF-8 locale must be installed. To confirm whether C.UTF-8 is installed, enter:

```
# localectl  list-locales | grep -i c.utf
C.utf8
en_SC.utf8
```

- The backup user must own the destination folder for the backup or have read-write permissions for the user's group. For example, assuming the backup user is *backup* and the user's group is *staff*, the following sample outputs show the required permissions for the backup directory:
  - Example 1: Backup directory is owned by *backup* user:

```
$ ls -l  /srv/
drwxr-xr-x  4 backup     root  4096 Apr 10 15:57 acme
```

  - Example 2: *backup* user's group has required permissions:

```
$ ls -l  /srv/
drwxrwxr-x. 7 root   staff  4096 Jul 24  2017 acme
```

- SFTP subsystem must be enabled. The SFTP subsystem path depends on which Ubuntu release is installed. For the latest Ubuntu release, the following line must be uncommented and present in the SSHD configuration:

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

  The file where you need to uncomment the preceding line is usually located in `/etc/ssh/sshd_config`.

Note You cannot use an NFS-mounted directory as the Cisco DNA Center backup server directory. A cascaded NFS mount adds a layer of latency and is therefore not supported.

Server Requirements for Assurance Backup

To support Assurance data backups, the server must be a Linux-based NFS server that meets the following requirements:

- Support NFS v4 and NFS v3. (To verify this support, from the server, enter **nfsstat -s**.)
- Have read and write permissions on the NFS export directory.
- Have a stable network connection between Cisco DNA Center and the NFS server.
- Have sufficient network speed between Cisco DNA Center and the NFS server.
- Have the C.UTF-8 locale installed. To confirm whether C.UTF-8 is installed, enter:

```
# localectl  list-locales | grep -i c.utf
C.utf8
en_SC.utf8
```

Note You cannot use an NFS-mounted directory as the Cisco DNA Center backup server directory. A cascaded NFS mount adds a layer of latency and is therefore not supported.

Requirements for Multiple Cisco DNA Center Deployments

If your network includes multiple Cisco DNA Center clusters, you cannot use the same backup location for automation and Assurance backups. For multiple Cisco DNA Center deployments, the best practice is to separate the backup directory structure for each Cisco DNA Center cluster. The following example configuration shows how to separate your backup directory structure.

Resource	Example Configuration
Cisco DNA Center clusters	**1.** *cluster1* **2.** *cluster2*
Backup server hosting automation and Assurance backups	The example directory is `/data/`, which has ample space to host both types of backups.
Directory ownership and permissions	Earlier in this section, see "Server Requirements for Automation Data Backup."
Directory ownership and permissions	Earlier in this section, see "Server Requirements for Assurance Backup."

NFS export configuration	The content of the `/etc/exports` file:
	`/data/assurance/cluster1 *(rw,sync,no_subtree_check,all_squash)`
	`/data/assurance/cluster2 *(rw,sync,no_subtree_check,all_squash)`

Requirements When Migrating to New Cisco DNA Center Hardware

If you upgrade your Cisco DNA Center cluster to new hardware or you replace your existing cluster hardware as part of the return materials authorization (RMA) process, use a different directory structure for the backup after restoring from the existing backup location.

Note If you replace one or two nodes from an existing three-node cluster, there is no need to change the backup directory structure.

Backup Server Directory Layout

To simplify backups, we recommend that you use the following directory layout for your backup server:

Single Cisco DNA Center Cluster Deployment

- Full backup (Automation and Assurance):
  - cluster1: /data/automation/cluster1
  - cluster1: /data/assurance/cluster1
- Automation-only backup:

  cluster1: /data/automation/cluster1

Multiple Cisco DNA Center Cluster Deployment

- Full backup (Automation and Assurance):
  - cluster1: /data/automation/cluster1
  - cluster1: /data/assurance/cluster1
  - cluster2: /data/automation/cluster2
  - cluster2: /data/assurance/cluster2
- Automation-only backup:
  - cluster1: /data/automation/cluster1
  - cluster2: /data/automation/cluster2

Backup Storage Requirements

Cisco DNA Center stores backup copies of Assurance data on an external NFS device and automation data on an external remote sync (rsync) target location. You must allocate enough external storage for your backups to cover the required retention. We recommend the following storage.

Appliance	NFS Storage (14 Days Incremental)	Rsync Storage (Daily Full)
DN2-HW-APL	1.7 TB	50 GB
DN2-HW-APL-L	3 TB	100 GB
DN2-HW-APL-XL	8.4 TB	300 GB

Additional notes:

- The preceding table assumes fully loaded appliance configurations that support the maximum number of access points and network devices for each appliance.
- Only unique data is backed up to NFS. Therefore, single- and three-node HA configurations create backups of approximately equal sizes.
- NFS storage is the only available destination type for Assurance data backups.
- NFS backups are incremental after the first full backup. The preceding table assumes that the first day you run an Assurance data backup, a full backup is generated. Then, each subsequent day generates an incremental backup.
- Rsync storage is the only available destination type for automation data backups.
- The rsync backup sizing is estimated for one daily backup. If you want to retain backups for additional days, multiply the required storage by the additional number of days. For example, if you have a DN2-HW-APL appliance and you want to store five copies of automation data backups generated once each day, the total storage required is 5 * 50 GB = 250 GB.
- The total backup time varies depending on your daily data load and the amount of historical data that you want to retain.
- The write path to Cisco DNA Center depends on the network throughput from Cisco DNA Center to the NFS server. The NFS server must have a throughput of at least 100 MB/sec.
- As with any other IT service, monitoring NFS performance is required to ensure optimal performance.

Example of NFS Server Configuration—Ubuntu

The remote share for backing up an Assurance database (NDP) must be an NFS share. If you need to configure an NFS server, use the following procedure (Ubuntu distribution) as an example.

Step 1 Enter the **sudo apt-get update** command to access and update the advanced packaging tool (APT) for the NFS server.

For example, enter a command similar to the following:

```
$ sudo apt-get update
```

Step 2 Enter the **sudo apt-get install** command to install the advanced packaging tool for NFS.

For example, enter a command similar to the following:

```
$ sudo apt-get install -y nfs-kernel-server
```

Step 3 Enter the **sudo mkdir -p** command to create nested directories for the NFS server.

For example, enter a command similar to the following:

```
$ sudo mkdir -p /var/nfsshare/
```

Step 4 Enter the **sudo chown nobody:nogroup** command to change the ownership of the group to nobody and nogroup.

For example, enter a command similar to the following:

```
$ sudo chown nobody:nogroup /var/nfsshare
```

Step 5 Enter the **sudo vi /etc/exports** command to add the following line to the end of `/etc/exports`:

```
$ sudo vi /etc/exports
/var/nfsshare *(rw,all_squash,sync,no_subtree_check)
```

Step 6 Enter the **sudo exportfs -a** command to export the file systems for the NFS server.

For example, enter a command similar to the following:

```
$ sudo exportfs -a
```

Step 7 Enter the **sudo systemctl start nfs-server** command to restart the NFS server.

For example, enter a command similar to the following:

```
$ sudo systemctl start nfs-server
```

Example of NFS Server Configuration—CentOS

The following procedure shows an example NFS server configuration for CentOS.

Step 1 Enter the **sudo yum check-update** command to access and update the Yellowdog Updater Modified (YUM) for the NFS server.

For example, enter a command similar to the following:

```
$ sudo yum check-update
```

Step 2 Enter the **sudo apt-get install** command to install the advanced packaging tool for NFS.

For example, enter a command similar to the following:

```
$ sudo yum install -y nfs-utils
```

Step 3 Enable and start the NFS server.

```
$ sudo systemctl enable nfs-server
$ sudo systemctl start nfs-server
```

Step 4 Enter the **sudo mkdir -p** command to create nested directories for the NFS server.

For example, enter a command similar to the following:

```
$ sudo mkdir -p <your_NFS_directory>
```

Step 5 Enter the **sudo chown nfsnobody** command to change the ownership of the group.

For example, enter a command similar to the following:

```
$ sudo chown nfsnobody:nfsnobody /var/nfsshare
```

Step 6 Enter the **sudo vi /etc/exports** command to add the following line to the end of /etc/exports:

```
$ sudo vi /etc/exports
/var/nfsshare *(rw,all_squash,sync,no_subtree_check)
```

Step 7 Enter the **sudo exportfs -a** command to export the file systems for the NFS server.

For example, enter a command similar to the following:

```
$ sudo exportfs -a
```

Step 8 Enter the **sudo systemctl start nfs-server** command to restart the NFS server.

For example, enter a command similar to the following:

```
$ sudo systemctl start nfs-server
```

Configure Firewall Rules to Allow NFS

By default, the firewall is disabled on Debian/Ubuntu distributions but enabled on RedHat/CentOS distributions. Check whether firewall is enabled on Debian/Ubuntu distributions and if it is, add firewall rules.

Configure Firewall Rules—Debian/Ubuntu

For **Debian/Ubuntu**, do the following:

Step 1 Enter the following command to check whether the firewall is enabled or disabled:

```
$ sudo ufw status
```

If the firewall is disabled, the output shows:

```
Status: inactive
```

If the firewall is enabled, the output shows:

```
Status: active
```

Step 2 If the firewall is enabled, set the static port for the mountd process to allow for easy firewall rule creation. To set the static port for mountd, change the following line to add `--port 32767` to /etc/default/nfs-kernel-server:

```
RPCMOUNTDOPTS="--manage-gids  --port 32767"
```

Step 3 Enter the following commands to add firewall rules to allow NFS:

```
sudo ufw allow portmapper
sudo ufw allow nfs
sudo ufw allow mountd
```

Configure Firewall Rules—RedHat/CentOS

For **RedHat/CentOS**, do the following:

Step 1 Add the mountd port to services and to nfs.conf.

Note RedHat/CentOS-based distributions use a different port for mountd than Debian-based distributions. RedHat/CentOS distributions use port **20048** for mountd in the /etc/service file.

Add the following lines to /etc/nfs.conf if they don't exist:

```
[mountd]
manage-gids = 1
port = 20048
```

Step 2 Enter the following command to restart the NFS services and firewall:

```
sudo systemctl restart nfs-server rpcbind nfs-mountd
```

Step 3 Enter the following commands to add firewall rules to allow NFS:

```
sudo firewall-cmd --permanent --add-service={nfs,rpc-bind,mountd}
sudo firewall-cmd --reload
```

Configure Backup Servers

If you plan to back up automation data only, you need to configure the Cisco DNA Center automation backup server. If you plan to back up both automation and Assurance data, you need to configure the Cisco DNA Center automation backup server and the NFS backup server.

This procedure shows you how to set up both servers.

Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.
- The server that you plan to use for data backups must meet the requirements described in Backup Server Requirements, on page 3.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore** > **Configure**.

Step 2 To configure the automation backup server, do the following:

a) Define the following settings:

Field	Description
SSH IP Address	IP address of the remote server that you can SSH into.
SSH Port	Port address of the remote server that you can SSH into.

Field	Description
Server Path	Path to the folder on the server where the backup files are saved.
Username	Username used to protect the encrypted backup.
Password	Password used to protect the encrypted backup.
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This passphrase is required and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored.

b) Click **Apply**.

Step 3 To configure the NFS backup server, click the **NFS** tab and do the following:

a) Define the following settings:

Field	Description
Host	IP address or host name of the remote server that you can SSH into.
Server Path	Path to the folder on the server where the backup files are saved.

b) Click **Apply**.

Back Up Data Now

You can choose to back up one of the following data sets:

- Automation data only
- Both automation and Assurance data

When you perform a backup, Cisco DNA Center copies and exports the data to the location on the remote server that you configured.

Note Data is backed up using SSH/rsync. Cisco DNA Center does not support using FTP (port 21) when performing a backup.

Before you begin

Make sure that the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.
- Backup servers meet the requirements described in Backup Server Requirements, on page 3.

- Backup servers have been configured in Cisco DNA Center. For information, see Configure Backup Servers, on page 9.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore** > **Backups**.

Note If you have not yet configured a backup server, Cisco DNA Center requires that you configure one before proceeding. Click **Configure Settings** and see Configure Backup Servers, on page 9.

Step 2 Click **Add**.

The **Create Backup** pane opens.

Step 3 In the **Backup Name** field, enter a unique name for the backup.

Step 4 Click **Create now** to perform the backup immediately.

Step 5 Define the scope of the backup:

- Click **Cisco DNA Center (All data)** to back up automation and Assurance data.
- Click **Cisco DNA Center (without Assurance data)** to back up only automation data.

Step 6 Click **Create**.

Note You can view the current backup status and the history of previous backups in the **Activity** tab.

You can create a new backup only when there is no backup job in progress.

You can view the successfully completed backup jobs in the **Backup** tab.

During the backup process, Cisco DNA Center creates the backup database and files. The backup files are saved to the specified location on the remote server. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. You receive a **Backup done!** notification when the process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. Cisco DNA Center displays an error message stating the cause of the backup failure. The most common reason for a failed backup is insufficient disk space. If your backup process fails, make sure that there is sufficient disk space on the remote server and attempt another backup.

Schedule Data Backups

You can schedule recurring backups and define the day of the week and the time of day when they will occur.

Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.
- Backup servers meet the requirements described in Backup Server Requirements, on page 3.

- Backup servers have been configured in Cisco DNA Center. For information, see Configure Backup Servers, on page 9.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore** > **Schedule**.

Step 2 Click **Add**.

Step 3 In the **Backup Name** field, enter a unique name for the backup.

Step 4 Click **Schedule weekly**.

Choose the days and time for scheduling the backup.

Step 5 Define the scope of the backup:

- Click **Cisco DNA Center (All data)** to back up automation and Assurance data.
- Click **Cisco DNA Center (without Assurance data)** to back up automation data only.

Step 6 Click **Schedule**.

Note You can view the scheduled backup jobs in the **Schedule** tab. After the backup starts, you can view backup status in the **Activity** tab.

You can create a new backup only when there is no backup job in progress.

You can view the successfully completed backup jobs in the **Backup** tab.

During the backup process, Cisco DNA Center creates the backup database and files. The backup files are saved to the specified location on the remote server. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. You receive a **Backup done!** notification when the process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. Cisco DNA Center displays an error message stating the cause of the backup failure. The most common reason for a failed backup is insufficient disk space. If your backup process fails, make sure that there is sufficient disk space on the remote server and attempt another backup.

Restore Data from Backups

When you restore data from a backup file, Cisco DNA Center removes and replaces the existing database and files with the backup database and files. The data that is restored depends on what is on the backup:

- Automation data backup: Cisco DNA Center restores the full automation data.
- Automation and Assurance data backup: Cisco DNA Center restores the full automation data and the Assurance data as far back as the date that you choose.

Caution The Cisco DNA Center restore process only restores the database and files. The restore process does not restore your network state and any changes made since the last backup, including any new or updated network policies, passwords, certificates, or trusted certificates bundle.

Note

- You cannot do a backup from one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You can only restore a backup to an appliance that is running the same Cisco DNA Center software release with the same first four digits and the same application versions as the appliance from which the backup was taken. To view the current applications and versions, choose **System** > **Software Management** and click **Currently Installed Applications**.
- If multiple clusters share the same Cisco AI Network Analytics configuration and are active at the same time, restoring a backup that includes the AI Network Analytics configuration on a different Cisco DNA Center cluster might result in data inconsistency and service disruption.

  Therefore, the AI Network Analytics configuration must be active on a single cluster. To uninstall the AI Network Analytics package from any inactive cluster, choose **System** > **Software Management** > **Currently Installed Applications** > **AI Network Analytics** > **Uninstall**.

Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.
- You have backups from which to restore data.

When you restore data, Cisco DNA Center enters maintenance mode and is unavailable until the restore process is done. Make sure you restore data at a time when Cisco DNA Center can be unavailable.

If you restore from a backup (on either the Cisco ISE or Cisco DNA Center side), Group-Based Access Control policy data does not synchronize automatically. You must run the policy migration operation manually to ensure that Cisco ISE and Cisco DNA Center are synchronized.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore**.

The **Backup & Restore** window displays the following tabs: **Backups**, **Schedule**, **Activity**, and **Configure**.

If you already successfully created a backup on a remote server, it appears in the **Backups** tab.

Step 2 In the **Backup Name** column, locate the backup that you want to restore.

Step 3 In the **Actions** column, choose **Restore**.

During the restore process, Cisco DNA Center goes into maintenance mode. Wait until Cisco DNA Center exits maintenance mode before proceeding.

Step 4 Click the **Backups** tab to view the results of a successful restore.