Backup and Restore

- Backup and Restore Concepts, on page 1
- Set Up and Manage Repositories, on page 7
- Set Up Automatic Application Backups, on page 14
- Perform a Manual Backup, on page 16
- Restore Cisco EPN Manager Data, on page 17
- Manage Disk Space Issues During Backup and Restore, on page 20
- Migrate to Another Virtual Appliance Using Backup and Restore, on page 20

Backup and Restore Concepts

- Backup Types: Application and Appliance, on page 1
- Backup Scheduling, on page 2
- Backup Repositories, on page 3
- Backup Filenames, on page 3
- Backup Validation Process, on page 4
- Information That Is Backed Up, on page 4
- Information That Is Not Backed Up, on page 6

Backup Types: Application and Appliance

Cisco EPN Manager supports two types of backups:

- Application backups—Contain Cisco EPN Manager application data but do not include platform data (host-specific settings, such as the server hostname and IP address). Application backup should be used during Cisco EPN Manager upgrade, when you want to move only application data and not the platform/host specific configurations.
- Appliance backups—Contain all application data and platform data (host-specific settings, including the hostname, IP address, subnet mask, default gateway, and so on). Appliance backup should be used for disaster recovery (or to recover from platform hardware or software failures). For example, to recover from any disk or filesystem failure, the standard recovery process would be to re-install Cisco EPN Manager and then restore from the appliance backup in order to restore all data as well as platform-specific configurations. You would then need to manually reconstruct the HA configurations as they are not included in the appliance backup.

Note For details on what is considered application data and what is considered platform data, see Information That Is Backed Up, on page 4.

Note the following about application and appliance backups.

- Application and appliance backups can be restored to the same or a new host, as long as the new host has the same hardware and software configuration as the host from which the backup was taken.
- You can only restore an appliance backup to a host running the same version of the Cisco EPN Manager server software as the server from which the backup was taken.
- When upgrading to a later version of Cisco EPN Manager, application backup and restore can run across different releases, as long as the upgrade path is supported.
- You cannot restore an application backup using the appliance restore command, nor can you restore an appliance backup using the application restore command.

We recommend the following best practices:

- If you are *evaluating* Cisco EPN Manager, use the default automatic application backup to the local repository.
- If you are running Cisco EPN Manager *in a production environment* as a virtual appliance, take regular application backups to a remote backup server. You can use the application backups to restore your server for all failures except complete failure of the server hardware.

Backup Scheduling

Cisco EPN Manager performs automatic scheduled application backups. This feature is enabled by default and creates one application backup file every day in the default local backup repository.

You can change this schedule as needed. You can also take an automatic application backup at any time from the web GUI. Appliance backups can only be taken from the command line.

Automatic application backups can create storage space problems if the backup repository is local to the Cisco EPN Manager server. While this is usually acceptable in test implementations, it is not intended to substitute for routine scheduled backups to remote servers in a production environment.

We recommend the following for production environments:

- Set up remote repositories to store the backup files.
- Use the automatic schedule application backup to create backups on the remote repositories on a regular schedule.

Even if you are using scheduled backups, you can still use the command line to create application or appliance backups at any time.

Note By default, two minutes are added to the job execution time for job creation.

Backup Repositories

By default, automatic application backup feature stores backup files in the local backup repository **/localdisk/defaultRepo**. You can use the web GUI to create a new local backup repository and then choose it when you set up automatic application backups. You can also specify a remote repository but you must create the repository first as described in Set Up and Manage Repositories, on page 7.

When taking application or appliance backups using the command line, you must specify the local or remote repository you want the backup to be stored in. In a production environment, this is normally a remote repository that is accessed via NFS, SFTP, or FTP. We recommend you use NFS because it is typically much faster and more reliable than other protocols.

There is no difference between performing an application backup from the command line or performing it from the web GUI. Both actions create the same backup file.

Whenever you use NFS to take backups or restore data from a remote backup, make sure the mounted NFS server remains active throughout the backup or restore operation. If the NFS server shuts down at any point in the process, the backup or restore operation will hang without warning or an error message.

Backup Filenames

Application backups launched from the web GUI—either automatically or manually—are assigned a filename with the following format:

*host-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

Application backups launched from the CLI use the same format, except that the file starts with the user-specified filename rather than the server name.

filename*-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

Appliance backups launched from the CLI have files that also start with the user-specified filename, but the type is indicated as SYS, not APP.

filename*-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_**SYS**_CK*checksum*.tar.gpg

The following table describes the variables used by the backup files.

Variable	Description
host	Host name of the server from which the backup was taken (for application backups launched from web GUI).
filename	Filename specified by user in command line (for application backups launched from CLI, and for appliance backups)
yymmdd-hhmm	Date and time the backup was taken
ver	Internal version.
size	Total size of the backup
cpus	Total number of CPUs in the server from which the backup was taken
target	Total amount of system memory in the server from which the backup was taken
ram	Total amount of RAM in the server from which the backup was taken

swap	Total size of the swap disk on the server from which the backup was taken
checksum	Backup file checksum

Backup Validation Process

Cisco EPN Manager performs the following steps to validate the backup files:

1. Before starting the backup process, validates disk size, fast-recovery area, and control files.
2. Validates the created backup database to ensure that it can be restored.
3. Validates the zipped application data against the files that were backed up.
4. Validates the TAR file to make sure it is correct and complete.
5. Validates the GPG file to ensure that it is correct.

If you manually transfer the backup file, or if you want to verify that the backup file transfer is completed, view the file's md5CheckSum and file size.

Another best practice for validating a backup is to restore it to a standalone "test" installation of Cisco EPN Manager.

Information That Is Backed Up

The following table describes the information that is contained in backup files. This information is restored to the server from backups.

See Information That Is Not Backed Up, on page 6 for details about data that is not saved by the backup mechanism.

Note The /opt/CSCOlumos/conf/Migration.xml file contains all configuration files and reports that are backed up. This file is included in the backup and is restored.

Data Type	Feature	Information Saved and Restored

Application Data	Background job settings	Data in the database
	Configuration archive (device configuration files)	Data in the database

	Configuration templates	• Files in /opt/CSCOlumos:
		  • /conf/ootb
		  • /xmp_inventory/dar/customized-feature-parts/CONFIGURATION
		• Data in the database

	Credentials	Data in the database
	Device inventory data	Data in the database
	Licenses	Files in /opt/CSCOlumos/licenses
	Maps	• Files in /opt/CSCOlumos/domainmaps • Data in the database

	Reports	• Files in /localdisk/ftp:
		  • /reports
		  • /reportsOnDemand
		• Data in the database

	Managed device software image files	Data in the database
	System settings	Data in the database
	User preferences	• Files in /opt/CSCOlumos/conf/wap/datastore/webacs/xml/prefs • Data in the database
	Cisco EPN Manager users, groups, and roles	Data in the database
	Virtual domains	Data in the database

Platform Data	CLI settings	All CLI information and settings are preserved. This includes the list of backup repositories, the FTP user name, users created using the CLI, AAA information specified via the CLI, and other CLI settings (such as the terminal timeout).
	Credentials	Linux OS credentials file
	Network settings	Files in /opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml
	Linux user preferences	Linux data structure
	Linux users, groups, and roles	Linux data structure

Information That Is Not Backed Up

Before performing a backup, make sure that you manually note the following information because it is not saved as a part of the backup process. You must reconfigure these settings after the data has been restored.

- High availability configurations
- Local customization (for example, report heap size)
- Patch history information
- Certificates

  If you have configured a server with a web certificate and set it up to authenticate clients with client certificates, you must repeat the same configuration on the new server again after you have completed the backup and restore procedure.

For a list of information that is backed up, see Information That Is Backed Up, on page 4.

How to Resolve Chrony User/Group Configuration Issues After Cisco EPN Manager Upgrade

After upgrading the Cisco EPN Manager, the *chrony* user and group configuration may be overwritten by restoring the database as a part of the upgrade process. If you are using Red Hat Enterprise Linux 8, `chronyd` is the recommended NTP service instead of `ntpd`.

To resolve this, follow the steps that are given below:

1. **Verify Chrony User:** Check if the `chrony` user exists in the `/etc/passwd` file. If the `chrony` user is not found, add it with the following command:

   ```
   echo"chrony:x:997:994::/var/lib/chrony:/sbin/nologin" | sudo tee -a /etc/passwd >/dev/null
   ```

2. **Enable and Start Chronyd Service:** To enable the `chronyd` service, follow the steps given below: to start at boot:

   - Enable the *chrony* service to Start at Boot:

     ```
     systemctl enable chronyd
     ```

   - Start the `chronyd` service:

     ```
     systemctl start chronyd
     ```

- Verify the service status:

```
systemctl status chronyd
```

By following these instructions, you can enable and start the `chronyd` service, which will provide NTP synchronization for your system.

- To can check the status of the NTP service after enabling and starting the service, use the command *`chronyc tracking`*. This command provides detailed information about the NTP synchronization status.
- To synchronize with the NTP server, use the command: *`chronyc makestep`*
- If you must stop or disable the service, you can use the commands `systemctl stop chronyd` and *`systemctl disable chronyd`*, respectively.

Ensuring that `chronyd` is properly configured and running is crucial for maintaining accurate time synchronization.

Set Up and Manage Repositories

Cisco EPN Manager supports the following repository types:

- Remote repositories—NFS, FTP, SFTP, and TFTP.

See the following topics for information on how to set up and manage these different types of repositories.

Create a Local Backup Repository

Cisco EPN Manager stores automatic backup files in the default local backup repository **/localdisk/defaultRepo**. You can create a different local backup repository and use it if you prefer.

Procedure

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the Jobs list, check the **Server Backup** check box.

Step 4 Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.

Step 5 Create the new local repository using the Edit Job properties dialog box.

a. Click **Create**. The Create Backup Repository dialog box opens.

b. Enter the name of the local repository you want to create.

c. Enter the password if you want to make the backup password secured.

Note
Make sure you remember the password to restore the backup.

d. If it is an FTP repository, check the **FTP** check box and enter the location and credentials.

e. Click **Submit**. The new repository is added to the Backup Repository drop-down list in the Edit Job Properties dialog box.

Step 6 Click **Save**.

Step 7 If you want to use the repository for future automatic application backups, specify it as described in Specify the Backup Repository for Automatic Backups, on page 15.

Use a Remote Backup Repository

In production environments, we recommend that you use remote repositories for backups so that your network management data is protected from hardware and site failures. In most cases, this means you will need to:

1. Create one or more remote repositories to hold Cisco EPN Manager backup files. You will need to set these up yourself if your organization does not already have remote backup servers.
2. Specify the remote repository as the destination for automatic application backups.
3. If needed, specify the interval between automatic application backups and time of day to take them. You will need to monitor and manually archive automatic application backups stored on remote repositories (because the **Max backups to keep** setting does not apply to remote repositories).
4. Specify the remote repository as the backup destination when taking an application or appliance backup using the CLI backup commands.

As with any resource that you plan to access remotely, specifying the correct server IP address and login credentials during setup are a requirement for successful use of remote backup repositories with Cisco EPN Manager.

Use Remote NFS Backup Repositories

To use NFS-based remote backup repositories, you need an NFS file server (which exports the designated folders in its file system to its client) and Cisco EPN Manager (which acts as the server's client). The Cisco EPN Manager system mounts the exported folders and makes them, along with other local folders, available to the Cisco EPN Manager server. To set this up, complete the following three tasks:

1. Specify the paths for the two folders on the NFS server that will stage and store backups, then configure the NFS server to export these paths. Since this falls outside of the scope of Cisco EPN Manager setup, this task should be completed by the NFS server’s system admin.
2. Set up Cisco EPN Manager to use the staging and storing folders you specified. This should be completed by a Cisco EPN Manager admin.
3. Secure communication between the NFS server and Cisco EPN Manager, which is very important because NFS is not secure on its own. This should be completed by a Linux admin who has a solid understanding of the security issues that NFS and its installation entails. For tips on hardening NFS, see Harden NFS-Based Storage.

Before You Set Up the NFS Backup Configuration

Before you begin, make sure:

- You know the IP address of the NFS server on which you want to stage and store backups. The staging and storage folders can be on the same NFS server, or on separate NFS servers. If you plan to stage and store on separate NFS servers, you will need IP addresses for both servers.
- You know the path names of the staging and storage folders on the NFS server. If you choose to stage and store on the same NFS server, the staging and storage folders *must* have different names.
- You have an administrator user ID with root privileges on the Cisco EPN Manager server.
- You have selected a repository name on the Cisco EPN Manager server, which will point to the NFS server storage folder.

Set Up NFS-Based Remote Repositories

Complete the following procedure to set up the NFS-based remote repositories that Cisco EPN Manager use for backups.

Procedure

Step 1 Log in to the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Set up the NFS remote repositories that stage the temporary files that are created during backup processing and store completed backup files:

```
config# backup-staging-url nfs://Staging_Server_IP_Address:/Staging_Server_Path
config# repository repositoryName
config-Repository# url nfs://Storage_Server_IP_Address:/Storage_Server_Path
```

Where:

- *Staging_cdg_Server_IP_Address* is the IP address of the NFS server on which the staging repository is located.
- *Staging_Server_Path* is the full path of the staging repository on its host NFS server.
- *repositoryName* is the name of the remote repository that will store completed backup files.
- *Storage_cdg_Server_IP_Address* is the IP address of the NFS server on which the storage repository is located.
- *Storage_Server_Path* is the full path of the storage repository on its host NFS server.

Caution
We recommend that you only enter an IP address for *Staging_cdg_Server_IP_Address* and *Storage_cdg_Server_IP_Address*. If the DNS service has been compromised and you enter a URL instead, this can result in the redirection of traffic to a malicious NFS server. That said, if you still prefer to specify a URL, we suggest you configure Cisco EPN Manager to use local name resolution (instead of relying on the DNS service). This can be done by entering the NFS server's name and IP address in the **/etc/hosts** file. Doing so can improve system security.

Step 4 Exit configuration mode:

```
config-Repository# exit
config# exit
```

Use Remote FTP Backup Repositories

Note We recommend using remote NFS repositories.

You can create backup repositories on a remote FTP server and configure the Cisco EPN Manager server to use them.

The FTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user (FTP user) with write access to the FTP server disk.
- Has a local subdirectory that matches the repository name you specify on the Cisco EPN Manager server.
- Has a password of 16 characters or less.

Other than these requirements, no other configuration is needed on the FTP backup server.

For the SFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the FTP server using the CLI. You can configure the FTP server only using the CLI.

Procedure

Step 1 Log into the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Configure a symbolic link to the remote FTP server, then exit configuration mode:

```
config# repository repositoryName
config-Repository# url ftp://RemoteServerIP//sharedFolder
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

Where:

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).
- *RemoteServerIP* is the IP address of the FTP server hosting the shared backup folder.
- *sharedFolder* is the name of the shared backup folder on the FTP server.
- *userName* is the name of the user with write privileges to the repository on the FTP server.
- *userPassword* is the corresponding password for that user. The password must be 16 characters or less.

Step 4 Verify the creation of the symbolic link:

```
show repository repositoryName
```

What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see Specify the Backup Repository for Automatic Backups, on page 15.

Use Remote SFTP Backup Repositories

Note We recommend using remote NFS repositories.

You can create backup repositories on a remote SFTP server and configure the Cisco EPN Manager server to use them.

The SFTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user with write access to the SFTP server disk.
- Has a local shared folder where the backups will be stored.

Other than these requirements, no other configuration is needed on the SFTP backup server.

For the SFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the SFTP server using the CLI. You can configure the SFTP server only using the CLI.

Procedure

Step 1 Log into the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Configure a symbolic link to the remote SFTP server, then exit configuration mode:

```
config# repository repositoryName
config-Repository# url sftp://RemoteServerIP//sharedFolder
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

Where:

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).
- *RemoteServerIP* is the IP address of the SFTP server hosting the shared backup folder. Note that the example above specifies an absolute path to the shared folder. To specify a relative path to the shared folder, use only one slash in the URL (for example, **url sftp://***RemoteServerIP/sharedfolder*).
- *sharedFolder* is the name of the shared backup folder on the SFTP server.
- *userName* is the name of the user with write privileges to the repository on the SFTP server.
- *userPassword* is the corresponding password for that user.

Step 4 Verify the creation of the symbolic link:

```
show repository repositoryName
```

What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see Specify the Backup Repository for Automatic Backups, on page 15.

Use Remote TFTP Backup Repositories

Note We recommend using remote TFTP repositories.

You can create backup repositories on a remote TFTP server and configure the Cisco EPN Manager server to use them.

The TFTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user with the *write* access to the TFTP server disk.
- Has a local shared folder where the backups are stored.
- Has a remote TFTP server that is up and running.

Other than these requirements, no other configuration is needed on the TFTP backup server.

For the TFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the TFTP server using the CLI. You can configure the TFTP server only using the CLI.

Procedure

Step 1 Log in to the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server.

Step 2 Enter the configuration mode.

Step 3 Configure a symbolic link to the remote TFTP server, then exit the configuration mode:

```
config# repository repositoryName
config-Repository# url tftp://RemoteTFTPServerIP/sharedFolder
config-Repository# exit
config# write memory
config# exit
```

Where,

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).
- *RemoteTFTPServerIP* is the IP address of the TFTP server hosting the shared backup folder.

  Note
  The example above specifies an absolute path to the shared folder. To specify a relative path to the shared folder, use only one slash in URL (for example, url tftp://RemoteServerIP/sharedfolder).

- *sharedFolder* is the name of the shared backup folder on the TFTP server.
- *write memory* is the command that is used to save configuration.

Step 4 Verify the creation of the symbolic link:

```
show repository repositoryName
```

What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see Specify the Backup Repository for Automatic Backups, on page 15.

Delete a Local Backup Repository

Use the following procedure to delete a local backup repository. This procedure ensures that the admin interface has the updated information.

Procedure

Step 1 Log into the server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server).

Step 2 List the local application backup repositories and identify the one that you want to delete:

```
show running-config | begin repository
```

Step 3 Enter configuration mode and delete the repository:

```
configure terminal
(config)# no repository repositoryName
```

Step 4 Repeat step 2 to verify that the repository was deleted.

Set Up Automatic Application Backups

Automatic application backups are enabled by default after installation. You can customize the schedule, specify a different backup repository, or adjust the number of backups that are saved.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- Information That Is Backed Up, on page 4
- Information That Is Not Backed Up, on page 6

Schedule Automatic Application Backups

Automatic application backups are enabled by default but you can adjust the day and interval at which these backups are performed. Performing a backup is resource-intensive and affects Cisco EPN Manager server performance. Avoid scheduling automatic backups to occur at peak traffic times.

If an automatic application backup fails, Cisco EPN Manager generates a Backup Failure alarm (with major severity). You can view these alarms just as you do other alarms (see Find and View Alarms).

Note After an automatic application backup fails, a pop-up message is displayed before every subsequent login attempt. This message continues to appear until you acknowledge the corresponding alarm.

Procedure

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the Jobs list, check the **Server Backup** check box, then click **Edit Schedule**. The Schedule dialog box opens.

Step 4 In the Schedule dialog box, select a start date, recurrence interval, and optional end time.

Step 5 Click **Submit**. These settings will now be used for future automatic application backups.

Note
When setting a scheduled backup, an additional margin of two minutes is automatically added to the specified backup time. For instance, if the backup is set for time T, scheduled backup starts at T+2 minutes. This margin accounts for potential delays and ensures that the backup job is not skipped if the current time and scheduled time are close.

Specify the Backup Repository for Automatic Backups

You can use the Cisco EPN Manager interface to specify a different backup repository for automatic application backups. The backup repository can be local or remote. You can also use the interface to create a new local backup repository if it does not already exist.

Before you begin

If you want to use a remote repository for automatic backups, you must create the repository first. Only local repositories can be created using this procedure. See Set Up and Manage Repositories, on page 7.

Procedure

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.
Step 2 Choose **System Jobs** > **Infrastructure**.
Step 3 In the list of jobs, check the **Server Backup** check box.
Step 4 Click **Edit** (the pencil icon). The Edit Job Properties dialog box opens.
Step 5 Select a repository from the Backup Repository drop-down list, then click **Save**. Cisco EPN Manager will use the new repository when it performs the next automatic application backup.

Change the Number of Automatic Application Backups That Are Saved

Follow this procedure to adjust the number of automatic application backups that are saved on a local repository. When a backup exceeds the number you specify here, Cisco EPN Manager deletes the oldest backup from the repository.

The **Max UI backups to keep** setting does not apply if you are using remote repositories for automatic application backups. You must monitor and archive or delete old backups on remote repositories using your own methods.

Procedure

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.
Step 2 Choose **System Jobs** > **Infrastructure**.
Step 3 In the Jobs list, check the **Server Backup** check box.

Step 4 Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.

Step 5 Enter a value in the **Max UI backups to keep** field, then click **Save**. Cisco EPN Manager will enforce this setting at the next backup.

Perform a Manual Backup

The topics in this section explain how to perform manual application or appliance backups.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- Information That Is Backed Up, on page 4
- Information That Is Not Backed Up, on page 6

Perform an Immediate Application Backup

Cisco EPN Manager performs automatic application backups as described in Backup Scheduling, on page 2. If needed, you can manually trigger an application backup as described in the following topics.

Perform an Immediate Application Backup Using the Web GUI

Use this procedure to trigger an immediate application backup using the web GUI.

Procedure

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the Jobs list, check the **Server Backup** check box, then click **Run**.

Step 4 To view the backup status, scroll to the top of the table to locate the new job, then check its status and results.

Perform an Immediate Application Backup Using the CLI

Use this procedure to trigger an immediate application backup using the CLI.

Procedure

Step 1 Log into the server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server).

Step 2 Display the list of backups, where *repositoryName* is the backup repository:

```
show repository repositoryName
```

Step 3 Start the remote backup.

```
backup filename repository repositoryName application NCS
```

where, *filename* is the name that you want to give the application backup file (for example, myBackup). The character length of the file name is 26. Other information is appended to the filename automatically, as explained in Backup Filenames, on page 3.

Perform a Manual Appliance Backup

Use this procedure to perform an appliance backup to a remote repository. Be sure you have configured the remote repository as described in Set Up NFS-Based Remote Repositories, on page 9.

Procedure

Step 1 Make sure the remote host is available.

Step 2 Log into the Cisco EPN Manager server as admin (see Establish an SSH Session With the Cisco EPN Manager Server).

Step 3 Start the remote backup:

```
(admin)# backup filename repository repositoryName
```

Step 4 To verify that the backup transfer is complete, view the md5CheckSum and file size.

Restore Cisco EPN Manager Data

All restore operations are performed using the CLI. Data can be restored to the host where the backup is executed (local host), or to a remote host. Backups can only be restored in their entirety; you cannot restore only parts of a backup.

For more information, see the following topics.

- Restore an Application Backup, on page 17
- Restore an Appliance Backup, on page 18

Restore an Application Backup

When you restore an application backup, make sure it is being restored to an OVA installation of the same size or larger. If the OVA installation is smaller, the restore fails.

To restore an *appliance* backup, use the procedure in Restore an Appliance Backup, on page 18.

Before you begin

If you are using high availability, read the guidelines in Remove HA During Restore before restoring your data.

Procedure

Step 1 Access the ESXi console. Once you are in the ESXi console, restoration process can be initiated.

Step 2 If a previous restoration attempt failed, the database may have been corrupted. Run this command to recreate the database:

```
ncs run reset db
```

Note
High Availability (if enabled) must be removed before running this command.

Running the **ncs run reset db** command deletes the existing data in database (network data) and resets the database to default factory settings.

Step 3 List the saved application backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.

```
show repository repositoryName
```

Step 4 To restore the previously backed-up application data:

```
restore backupFileName repository repositoryName application NCS
```

Step 5 If you are using Cisco Smart Licensing, reregister Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. See Register Cisco EPN Manager with the Cisco Smart Software Manager.

Restore an Appliance Backup

When you restore an appliance backup, make sure it is being restored to an OVA installation of the same size or larger. If the OVA installation is smaller, the restore fails.

To restore an *application* backup, use the procedure in Restore an Application Backup, on page 17.

Cisco recommends that you change the restored server's IP address, subnet mask, and default gateway if:

- The restored host is on the same subnet as the old host, and the old host is still active.
- The restored host is on a different subnet from the old host.

Before you begin

If you are using high availability, read the information in Remove HA During Restore before restoring your data.

Procedure

Step 1 Access the ESXi console. Once you are in the ESXi console, restoration process can be initiated.

Step 2 If a previous restoration attempt failed, the database may have been corrupted. With the backup stored in an external repository, reinstall the setup using the same release and then retry the restore.

Step 3 List the saved appliance backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.

```
show repository repositoryName
```

Step 4 To restore the previously backed-up application data:

```
restore backupFileName repository repositoryName
```

Step 5 Determine whether you should change the IP address, subnet mask, and default gateway.

a) Check if your installation meets the following criteria:

- The restored host is on the same subnet as the old host, and the old host is still active.
- The restored host is on a different subnet from the old host.

If it does, perform the next step.

b) Change the IP address, subnet mask, default gateway and (optionally) the host name on the restored server.

c) Write the changes to the server's running configuration and restart Cisco EPN Manager services. For example:

```
configure terminal
(config)# int GigabitEthernet 0
(config-GigabitEthernet)# ip address IPAddress subnetMask
(config-GigabitEthernet)# exit
(config)# ip default-gateway gatewayIP
(config)# hostname hostname
(config)# exit
(admin)# write mem
(admin)# ncs stop
(admin)# ncs start
(admin)# exit
```

Step 6 If you are using Cisco Smart Licensing, reregister Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. See Register Cisco EPN Manager with the Cisco Smart Software Manager.

Recover from Failed Restores

You may sometimes find that a restore does not complete, or reports a failure. Whenever a restore fails, you run the risk of database corruption, which can prevent the further restoration or re-installation. Perform the following steps to restore a corrupted database before attempting another restore or re-installation.

Procedure

Step 1 Open a CLI session with the Cisco EPN Manager server (see Establish an SSH Session With the Cisco EPN Manager Server).

Step 2 Enter the following command to reset the corrupted database:

```
ncs run reset db
```

Manage Disk Space Issues During Backup and Restore

If you are experiencing disk issues *during* a backup or restore, move your installation to a server with adequate disk space by following the procedure in Migrate to Another Virtual Appliance Using Backup and Restore, on page 20.

If you are unable to create a backup *after* a restore of your existing system, follow the steps explained in Compact the Database to free disk space and create a successful backup. If you are still unable to create a backup after using the **ncs cleanup** command, set up and use a remote repository (using NFS, FTP, or SFTP) for your backups, as explained in Use a Remote Backup Repository, on page 8.

Migrate to Another Virtual Appliance Using Backup and Restore

You will need to migrate your Cisco EPN Manager data from an existing virtual appliance (OVA server installation) to a new one whenever you want to:

- Replace the old server entirely, such as after a catastrophic hardware failure. In this case, you can use your old installation media to re-create the new host on a replacement server, then migrate your application data from the old host to the new host.
- Migrate to a larger or more powerful server, so you can use Cisco EPN Manager to manage more of your network. In this case, you will want to ensure that you have the OVA installation file and install it on the new server using the larger installation option before retiring the older, smaller one. You can then migrate your application data from the old host.

In both cases, it is relatively easy to migrate your old data to the new virtual appliance by restoring to the new host an appliance or application backup taken from the old host.

Procedure

Step 1 If you have not already done so, set up a remote backup repository for the old host, as explained in Use a Remote Backup Repository, on page 8.

Step 2 Perform an application backup of the old host and save it to the remote repository (see Perform an Immediate Application Backup Using the CLI, on page 16).

Step 3 Install the new host (installation steps are in the Cisco Evolved Programmable Network Manager Installation Guide).

Step 4 Configure the new host to use the same remote backup repository as the old host (see Use a Remote Backup Repository, on page 8).

Step 5 Restore the application backup on the remote repository to the new host (see Restore an Application Backup, on page 17).