



Backing Up and Restoring the Director

This chapter provides you with the steps you have to take to restore the Director node from an automatic or manual backup, as well as how to force a Director backup.

This chapter is organized as follows:

- [How It Works, page 2-1](#)
- [Manually Running a Director Backup, page 2-1](#)
- [Restoring the Director, page 2-2](#)

How It Works

Due to its importance the Director node has a redundant backing up facility that comes in addition to the snapshot-based backups. This facility does not replace the snapshot-based backups. It allows you to restore the Director only if you need to.

Director backups are created by a script that runs on the node itself on an hourly schedule. The script can also be run manually if needed (see [Manually Running a Director Backup](#)).

Backup data is sent to NFS to *exported_directory/backup*. The five most current backups are kept at any given time, older are deleted. Keep in mind that not every run of the backup script produces a backup. This only happens when the scripts detects that the filesystem has changed since the last run.

The backup naming convention is *director-YYYYMMDD_HHmm.tar.gz*.

Because the backup only contains important configuration and database files, its size is kept to the minimum. Size-wise, all current backups should not take more than a few megabytes. This also means that when restoring the Director you first need to redeploy the node from scratch and then apply the backup to the restored node. See [Restoring the Director](#) for details.

Manually Running a Director Backup

If you ever need to run the `backup-director.sh` script manually you can do so by completing these steps:

-
- Step 1** Log in to the Director node using the admin user.
 - Step 2** Select **Drop to Shell** from the menu.
 - Step 3** Run this command:

```
sudo /opt/cisco/sbin/backup-director.sh
```

Restoring the Director

Before you start the restore procedure (as described below), do the following:

- Ensure that there are valid backups on your NFS in *exported_directory/backup*—select one and check that its size is greater than zero and that the tarball is not corrupted
- Secure all Cisco WebEx Social installation images starting from the release you are running all the way down the supported upgrade path to the base release. So for example if you are running release N.M SR2, secure the installation images for releases N.M, N.M SR1, and N.M SR2. Place all the images on a location where they can be accessed using HTTP or SCP.

When you are ready, complete these steps to restore the director from the backup:

- Step 1** Power off the Director node.
- Step 2** Start deploying a new Director VM (see the *Cisco WebEx Social Installation and Upgrade Guide* for details).
- Step 3** Wait for the Director UI to become available.
- Step 4** Sign in to the Director UI using the default password (See the *Cisco WebEx Social Installation and Upgrade Guide* for details).
- Step 5** Reset your Unified Access Password when prompted. You can type a new password or use your current password.
- Step 6** Go to **System > Configuration > NFS** and set up NFS so that you can access your Director backups.
- Step 7** Click **Apply Config**.
- Step 8** If you are running a Service Release, upload the Cisco WebEx Social installation image using the **System > Software** tab and upgrade to it. Repeat if the supported upgrade path requires multiple upgrades.
- Step 9** Log in to the Director console using user admin.
- Step 10** Select **Drop to Shell**.
- Step 11** Run this command:

```
sudo service puppet debug
```
- Step 12** Ensure that there are no errors in the output before continuing with the next step.
- Step 13** Run this command to trigger automounting of the NFS share:

```
cd /mnt/auto/backup; ls /mnt/auto/backup
```
- Step 14** Go to the `/opt/cisco/sbin` directory:

```
cd /opt/cisco/sbin
```
- Step 15** Restore your backup:

```
sudo ./backup-director.sh -r /mnt/auto/backup/director-YYYYMMDD_HHmm.tar.gz
```

where `director-YYYYMMDD_HHmm.tar.gz` is the filename of the backup you want to restore.
- Step 16** After the script finishes, your ssh session ends. Log back in and run this command:

sudo service puppet debug

- Step 17** Sign in to the Director UI using the *Unified Access Password* that you used to employ before you started this procedure.
- Step 18** Go to **System > Configuration > Unified Access** and once again reset your Unified Access Password to ensure it is correctly set on all selected features (indicated by the `chk` boxes).
- Step 19** Click **Apply Config**.
- Step 20** *Optional—proceed with this step if you don't want to wait for the first scheduled backup run.* Go back to the Director console and manually run a backup of the restored Director node:

sudo /opt/cisco/sbin/backup-director.sh



Note

In case the first scheduled backup run happens before you run the manual backup step, you see this output: “Nothing changed - nothing to backup.”. This is normal because the initial backup is already created.

