Backing Up, Restoring, and Downgrading the GSSM Database

This chapter describes how to back up and restore the primary GSSM database. It also describes how to downgrade to an earlier version of the GSS software on your GSSs and GSSMs and restore the software if you encounter problems with a GSS software upgrade.

It contains the following major sections:

- Backing Up the Primary GSSM
- Restoring a Primary GSSM Backup
- Downgrading Your GSS Devices

Backing Up the Primary GSSM

This section describes the procedure to perform a full backup of the primary GSSM database. It contains the following topics:

- Backup Overview
- Performing a Full Primary GSSM Backup

Backup Overview

The GSSM database maintains all network and device configuration information, as well the DNS rules used by the GSS devices to route DNS queries from users to available hosts.

> ✎
> **Note**   You should perform frequent backups of your primary GSSM and its database to ensure that if a sudden and unexpected power loss or media failure occurs, your GSSM configuration and database will survive, and your GSSM can be quickly restored.

We recommend that you perform a backup of your primary GSSM:

- Before you switch GSSM roles and before you make the standby GSSM the primary GSSM on your network
- Before you perform a GSS software upgrade
- After you make any changes in the device or network configuration of your GSSM

The GSS software performs a full backup of the GSSM network configuration settings as well as the GSSM database that contains global server load-balancing configuration information. A full backup of the primary GSSM allows you to pick and choose the specific GSSM configuration information that you want to later restore on the primary GSSM.

Whenever you execute a backup on your primary GSSM, the GSS software automatically creates a tar archive ("tarball") of the necessary files. A tar archive is a group of files collected together as a single file. This file has the .full extension.

When you execute a database restore on your primary GSSM, the archive file is automatically unpacked and the database is copied to the GSSM, overwriting the current GSSM database.

Backing up your GSSM database requires that you access the GSS CLI and then complete the following actions:

1. Determine the appropriate time to back up your GSSM

2. Perform the backup

3. Move the backup file to a secure location on your network

Performing a Full Primary GSSM Backup

You can perform a full primary GSSM backup at any time. Performing a backup requires access to the CLI of the primary GSSM.

To perform a full backup of your primary GSSM, perform the following steps:

1. Log in to the primary GSSM CLI and enable privileged EXEC mode.

    ```
    gssm1.example.com> enable
    gssm1.example.com#
    ```

2. Copy the current primary GSSM startup configuration to a file for use on other devices or for backup purposes by using the **copy startup-config disk** command. The *filename* argument specifies the name of the file containing the startup configuration settings.

    ```
    gssm1.example.com# copy startup-config disk newstartupconfig
    ```

Note The primary GSSM backup does not include user files that reside in the /home directory. If you have important files in the /home directory that you want to save, such as the startup-configuration file, use either the secure copy (**scp**) or **ftp** commands to copy those files to another device. Storing the startup-configuration file in a safe location can save time and reconfiguration issues in a recovery situation.

3. Create a full backup of your primary GSSM by using the **gssm backup full** command. The **gssm backup full** command performs a backup of both the database component of the GSSM and its network and device configuration information. Supply a filename for your backup.

Cisco Global Site Selector Administration Guide

```
gssm1.example.com# gssm backup full gssmfullbk
GSSM database backup succeeded [gssmfullbk.full]
```

4. After you receive confirmation that the primary GSSM successfully created your full backup, copy or move the backup file off the device to ensure that the backup is not lost if a problem occurs on your primary GSSM.

   Use either the secure copy (**scp**) or **ftp** command to copy or move your full backup to a remote host.

   ```
   gssm1.example.com# scp gssfullbk.full server.example.com:~/
   ```

Restoring a Primary GSSM Backup

This section describes how to restore a backup of the primary GSSM database. It contains the following topics:

- Restore Overview
- Restoring Your Primary GSSM from a Previous Backup

Restore Overview

You may need to restore a previous primary GSSM backup for the following reasons:

- You have replaced your primary GSSM with a new device and want to restore a previous backup to that primary GSSM.
- You are downgrading the GSS software to an earlier release.
- You have made a number of configuration changes to the primary GSSM and would like to return to the previous backup of the GSSM.

When you execute a database restore on your primary GSSM, the archive file is automatically unpacked and the database is copied to the GSSM, overwriting the current GSSM database. See the "Backing Up the Primary GSSM" section for details about performing a database backup of the GSSM.

The GSS database may change between software versions. When you downgrade to an earlier version of the GSSM database, any configuration changes, device configuration information, and DNS rules entered through the primary GSSM (subsequent to your last software upgrade) will be lost.

Restoring Your Primary GSSM from a Previous Backup

When restoring the primary GSSM from a previous backup, use the last backup to restore the GSS device network configuration settings as well as the encryption keys used to communicate with other GSS devices. Restoring the primary GSSM from a backup returns the device to its exact configuration as of the last backup.

To restore an earlier version of the primary GSSM from a previous backup, perform the following steps:

1. Log in to the primary GSSM CLI and enable privileged EXEC mode.

   ```
   gssm1.example.com> enable
   gssm1.example.com#
   ```

2. Verify that your previous backup of the primary GSSM is in a location that is accessible from the GSSM being restored. Previous backups have a .full file extension. For details about locating files in a GSS directory, see the "Managing GSS Files"section in Chapter 2, Managing the GSS from the CLI.

1. Stop the GSS software on the primary GSSM, and then use the **gss status** command to confirm that the primary GSSM has stopped.

   ```
   atcr1.cisco.com# gss stop
   atcr1.cisco.com# gss status
   Cisco GSS - 1.3(1.0.0) - [Wed Feb 15 11:33:47 UTC 2006]

   gss is not running.
   ```

2. After the GSSM software stops, restore the GSSM from the backup file by using the **gssm restore** command. For example, to restore the file *gssmfullbk.full*, enter:

   ```
   gss1.example.com# gssm restore gssmfullbk.full
   ```

3. Confirm your decision to overwrite existing GSS system configuration information on the GSSM and restart the GSSM device. Enter **y** for yes (or **n** to stop the restore process).

   ```
   % WARNING WARNING WARNING
   You will be asked which portion(s) of the system configuration to
   overwrite. You may want to create a database backup before
   proceeding.

   Are you sure you wish to continue? (y/n): y
   Backup file is valid. Timestamp = 2003-Sep-15-14:01:53
   ```

4. Confirm your decision to restore primary GSSM platform information or only the GSS database by performing one of the following actions:

- Type **y** to restore GSSM platform information.

> ![Note icon]
>
> **Note**   Restoring platform information requires a reboot of the GSS at the end of the restore procedure.

- Type **n** to restore only the primary GSSM database and not the GSSM platform information. If you choose not to restore GSSM platform information, reconfigure the GSSM platform information from the CLI. See the *Cisco Global Site Selector Getting Started Guide* for details.

```
This backup contains a backup of the platform configuration.
'n' restores just the database. Restoring platform files requires
a reboot.
Restore Platform files? [y/n]: y
```

Your selection enables you to return the primary GSSM to its original state prior to the database backup. Platform information includes all configuration parameters set at the CLI, including: interface configuration, hostname, service settings (NTP, SSH, Telnet, FTP, and SNMP), time zone, logging levels, web certificates, inter-GSS communication certificates, access lists and access groups, CLI user information, GUI user information, and property-set CLI commands.

5. Confirm your decision to restore the GSS network information for remote devices activated from the primary GSSM by performing one of the following actions:

- Type **y** to restore the GSS network information.

Network information includes registered GSS devices, GSS device status, node information, and IP addresses. This network information is displayed in the GSS list table in the Resources tab. GSS network information does not include DNS rules, answers, and keepalives. Those configuration elements are automatically restored as part of the database restore process.

If you type **y** to restore the GSS network information and your configuration includes a standby GSSM, you must reenable the standby GSSM and then reregister it with the primary GSSM. See the *Cisco Global Site Selector Getting Started Guide* for details.

- Type **n** to instruct the software not to restore GSS network information to the GSSM. If you choose not to restore the GSS network information, you must reenable each device, then reregister the device with the primary GSSM. See the *Cisco Global Site Selector Getting Started Guide* for details.

Note Disabling and enabling each device, then reregistering the device with the primary GSSM, may result in a temporary network service outage.

```
Do you want to replace your current GSS network configuration with
the one specified in the backup file? (y/n): y
```

The GSSM continues with the restore process.

```
Deleting existing database...
Creating empty database for restore...
Restoring the database...
Using GSS network information present in backup file...
Restoring platform backup files.
Database restored successfully.
Reboot Device now? (y/n): y
```

If you choose to reboot the device, the primary GSSM reboots.

6. Confirm that the primary GSSM is up and running in normal operation mode (runmode = 5), by using the **gss status** command.

After you restore a backup file in which you did not preserve the GSS network information, note the following configuration changes in the primary GSSM GUI:

- All previous associations established between a GSS device and a location are removed. When you access the Modifying GSS details page (Resources tab) of the primary GSSM GUI, each GSS location is set to Unspecified. If necessary, reestablish the association between a GSS device and location on the Modifying GSS details page as described in the *Cisco Global Site Selector Administration Guide*.

- For a DNS sticky configuration, all favored peer associations established between a local GSS node and a remote GSS peer are removed. When you access the Global Sticky Configuration details page (Traffic Mgmt tab) of the primary GSSM GUI, each local GSS node favored peer is set to Unspecified. If necessary, reestablish the association between each local GSS node and its favored peer as described in the *Cisco Global Site Selector Global Server Load-Balancing Configuration Guide*.

Downgrading Your GSS Devices

If you encounter problems with a GSS software upgrade, restore an earlier version of the GSS software on your GSSs and GSSMs. To restore an earlier version of your software, you must have a previous backup of the primary GSSM database that corresponds to the current version of the GSS software. For example, if you want to downgrade from GSS software Release 1.2 to GSS software Release 1.1, you must have a GSS software Release 1.1 database backup that you can restore. Your GSS software Release 1.2 database cannot run on the Release 1.1 platform because of changes in the database schema between releases.

When downgrading the GSS software, use the following order of operations to protect your critical GSS data and properly restore your GSSM database:

1. Verify the GSSM role in the GSS network.

2. Perform a backup of your primary GSSM that contains the more recent version of the GSS software.

3. Obtain an earlier software (.upg) file.

4. Downgrade your GSS device.

5. Restore your GSSM database backup that corresponds to the downgraded version of the GSS software.

Do not attempt to restore an earlier version of the GSS software than the earliest GSSM database backup that you have available. For example, if the earliest version of the GSS software in your possession is Release 1.1, and your earliest GSSM database backup is for Release 1.1, do not downgrade to a release of GSS software earlier than Release 1.1.

To restore an earlier version of your GSS software, perform the following steps:

1. Verify that the roles of the designated primary and standby GSSMs have not changed. The changing of roles between the designated primary GSSM and the standby GSSM is intended to be a temporary GSS network configuration until the original primary GSSM is back online. See the "Verifying the GSSM Role in the GSS Network" section of Appendix A, Upgrading the GSS Software.

2. Perform a backup of your primary GSSM as described in the "Performing a Full Primary GSSM Backup" section.

3. Obtain an earlier software version as described in the "Obtaining the Software Upgrade" section of Appendix A, Upgrading the GSS Software.

4. Install the earlier software version as described in the "Upgrading Your GSS Devices" section of Appendix A, Upgrading the GSS Software.

5. After you downgrade the software on your primary GSSM,see the "Restoring Your Primary GSSM from a Previous Backup" section. Restore the GSSM database backup that was previously saved from the downgraded GSS software release.

Downgrading Your GSS Devices