Performing Cisco IPICS Database Backup and Restore Operations

This chapter describes the procedures that you perform to back up your Cisco IPICS database and to restore your database from the backup location.

This chapter includes the following sections:

Overview of Cisco IPICS Database Backup and Restore Operations

As a best practice, Cisco recommends that you back up your Cisco IPICS database on a regular basis and maintain your backups in a secure location. This best practice ensures that you do not lose all system configuration if your Cisco IPICS server experiences a software or hardware failure.

Cisco IPICS performs regularly-scheduled database backups to preserve your data. For more information about scheduled database backups, including the default settings for the scheduled database backups and how to modify them, see the "Changing the Default Settings for a Scheduled Database Backup" section on page 11-6.

You can also perform a database backup at any time by manually executing the backup operation. For more information about manual backup procedures, see the "Restoring Data from a Database Backup" section on page 11-9.

A backup set contains all data in the Cisco IPICS server database, including radio descriptor files and IDC alert tones.

After you have backed up your data, you can restore your data by choosing from various options. By accessing the **Administration > Database Management** window, you can identify the backup that you want to restore. For more information regarding restore operations, see the "Restoring Data from a Database Backup" section on page 11-9.

Caution Database restores should only be done when there are no other users logging in to the system; otherwise, they may see errors or other strange behavior.

Backing up the Cisco IPICS Server Database

Cisco IPICS provides you with the following options to back up your database:

- Manual backups—You can perform a manual database backup to capture the current state of the Cisco IPICS database.
- Scheduled backups—By default, Cisco IPICS backs up the database every day at a predefined time and stores the backup in a predefined location. You can change the time, frequency, and/or location of the scheduled backup.

Note For optimum performance, Cisco recommends that you back up your database during periods of low activity or other off-peak hours. If you perform a backup during periods of high activity, the length of time that it takes to complete this operation can be significantly increased.

This section includes information about backing up the database and includes the following topics:

Managing Database Backups from the Database Management Window

To configure the parameters for backing up your database, and performing backup-related operations, navigate to the **Administration > Database Management** window.

The Database Management window includes the following tabs:

- Database Backup—From this tab, you can configure the options to back up your database. See the "Performing a Manual Database Backup" section on page 11-3 for more information about backing up your database.
- Restore From Backup—From this tab, you can restore your database backup. See the "Restoring Data from a Database Backup" section on page 11-9 for more information about restoring your database backup.
- Schedule Backup—From this tab, you can configure the options that apply to regularly-scheduled backups. You can specify the location of the backup and the length of time for which the backup is saved. In addition, you can specify when, and how often, Cisco IPICS performs the scheduled backups.

  See the "Changing the Default Settings for a Scheduled Database Backup" section on page 11-6 for more information about changing the settings for the scheduled database backups.

- Log—From this tab, you can view the database logs, which include backup and restore activity. The logs include status messages and information about any errors that might have occurred during a database backup or restore procedure. See the "Downloading and Viewing the Backup and Restore Logs" section on page 11-14 for more information about the database logs.

Performing a Manual Database Backup

To perform a manual database backup, navigate to the **Administration > Database Management > Database Backup** window.

The settings that you choose for a manual database backup, such as the location of the backup, can be different from the destination that you choose for the scheduled backups. (Settings for manual database backups do not affect or change the settings for scheduled database backups.)

To manually back up the database, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Database Backup** window.

Step 2 In the **Backup Destination** pane, choose one of the following destinations:

- **Default**—Click this radio button to place the backup in the default (**/idspri/backup**) directory.

  Cisco IPICS creates a subdirectory in the /idspri/backup directory for the database backup named **IDSB**_*yyyy-mm-dd_hh-mm-ss*. See the "Understanding Naming Conventions for Backup Directories" section on page 11-6 for more information about backup directory naming conventions.

- **Local Directory**—Click this radio button to specify a directory in the Cisco IPICS server to back up your database.

Note Cisco IPICS prepopulates the Local Directory field with the **/idspri/backup/cron** directory. You can remove the **/cron** subdirectory in the field to place your files in the **/idspri/backup** directory. However, if you back up your files to a local directory in the server, that directory must be a subdirectory of the **/idspri/backup** directory. Any directory within the **/idspri/backup** directory (for example, **/idspri/backup/mybackups**) is valid as a location for a database backup. If the directory that you specify does not exist, Cisco IPICS creates the directory for you.

Tip Make sure that you enter the path within the **/idspri/backup** directory in the Cisco IPICS server, and that you precede the destination path with a forward slash (/). If you do not specify a forward slash, Cisco IPICS displays a pop-up window with an error and does not perform the backup.

Remote Host—Click this radio button to back up your database to a remote location

Note Use the Remote Host option only if the remote host supports SSH and the Linux Secure Copy Protocol (SCP).

Remote back up is supported-on Linux based systems only. WS_FTP is not supported by Cisco IPICS for scheduled remote back ups.

When you click the Remote Host radio button, you must specify the following information:

- IP Address—Enter the IP address of the remote host.
- User Name—Enter a valid user name for access to the remote host.
- User Password—Enter a valid password for this user.
- Remote Directory—Enter the location of the full directory path on the remote host where you want the database to be stored. If the directory that you specify for the backup does not exist on the remote host, Cisco IPICS creates it for you.

  For more information, see the "Caveats for Remote Host Database Backups" section on page 11-8.

Step 3 Click **Backup Now**.

Cisco IPICS begins the database backup process. An information icon appears in the tab to inform you that the backup is in process, along with the following text:

```
Database backup in progress. Please wait...
```

Step 4 To view the activity for the backup, wait a few moments for the screen to refresh and view the Backup Log pane.

The Backup Log pane in the Database Backup window displays the log entries for the backup process. The screen refreshes periodically with log messages until the database backup completes.

Note To manually refresh the screen, click **Refresh**.

Step 5 To view the results of the backup operation, wait until the screen stops refreshing, then view the Backup Log pane.

Note The backup log pane can contain multiple pages of items. To view items in the list, use the navigation buttons as described in the "Navigating Item Lists" section on page 1-13.

If the backup operation was successful, you see a Status Text of **Available**.

Table 11-1 describes the fields in the Backup Log pane.

Table 11-1 Field Descriptions in the Backup Log Pane

Field	Description
ID	This field represents the internal ID of the database backup. Cisco IPICS assigns each backup operation a unique ID.
Backup Destination	This field represents the full directory path of the database backup, beginning with a forward slash (/). If the backup was a Remote Host backup, this field displays the full directory path on the remote server on which Cisco IPICS placed the Remote Host backup. **Note** Cisco IPICS creates a subdirectory inside the directory that you specify for each backup operation. Each directory is time-stamped with the date and time of the backup, as described in the "Understanding Naming Conventions for Backup Directories" section on page 11-6.

Table 11-1 Field Descriptions in the Backup Log Pane (continued)

Field	Description
IP Address	This field represents the IP address of the remote server, if the backup was a Remote Host backup. If Cisco IPICS performed a Default or Local Directory backup, this field is blank. If the backup operation was not successful, this field displays **none**.
Status	This field represents the status of the backup operation. The status field displays one of the following states: • **Initialized**—The backup process has begun the initial stages of the database backup. • **In Progress**—Cisco IPICS successfully completed the initial stages of the backup process and is performing the database backup. • **Available**—The database backup was successful and the specified backup is available for a restore operation. • **Not Available - Purged**—The specified database backup exceeded the retention period as specified by the **Backup Retention** list box and Cisco IPICS deleted the database backup. The date and time that the database was purged displays in the field. • **Canceled**—Cisco IPICS canceled the backup due to a known error (for example, a lack of hard disk space). • **Failed**—Cisco IPICS could not complete the database backup because of an unexpected error. If you see a **Canceled** or **Failed** error status, your database backup failed. You can find more information about the cause of the failure by navigating to the **Administration > Database Management > Log** window and viewing the contents of the backup log.
Size in Kb	This field represents the total size, in KB, of the specified database backup.
Backup Start Time	This field represents the time that Cisco IPICS started the specified database backup.
Backup End Time	This field represents the time that Cisco IPICS completed the specified database backup.
Purge Time	This field represents the time that Cisco IPICS deleted the specified database backup.

You can also view the database logs by navigating to the **Administration > Database Management > Log** window. To visually identify the type of status message that appears in the Database Logs pane, Cisco IPICS displays certain log entries in the following text colors:

- Green—Green messages indicate the completion of a script.

Note Carefully check the text of green messages to ensure that the script completed successfully with no errors. Green messages indicate that the script completed but they do not necessarily indicate that the script completed successfully.

- Black—Black messages are informational messages and indicate normal database backup processes.

- Blue—Blue messages are warning-level messages and indicate problems that are less severe than error-level messages, such as a backup operation that completed with errors. Occasionally, a warning-level error message can indicate a greater problem, such as a restore operation that did not complete successfully.
- Red—Red messages are error-level messages and indicate that a process did not complete successfully. Red messages usually indicate errors of a greater severity than warning-level (blue) messages.

For more information about troubleshooting problems that you might encounter, see the "Troubleshooting Cisco IPICS Backup and Restore Procedures" section on page 11-16.

Understanding Naming Conventions for Backup Directories

Cisco IPICS creates a subdirectory in the backup directory for each database backup. Cisco IPICS time-stamps each subdirectory with the date and time that Cisco IPICS performed the backup operation. The subdirectory name is in the following format:

IDSB_*yyyy-mm-dd_hh-mm-ss*

Where *yyyy-mm-dd_hh-mm-ss* represents the year, month, day, hour, minute and second, respectively, of the time that Cisco IPICS performed the database backup (for example, IDSB_2007-07-04_17-13-55).

Changing the Default Settings for a Scheduled Database Backup

Cisco IPICS is preconfigured with default settings for database backups. Table 11-2 shows the default settings for scheduled database backups:

Table 11-2 Default Settings for Scheduled Database Backups

Setting	Value
Frequency	Daily
Time of day	23:59 (11:59 p.m.)
Destination directory	The Cisco IPICS server **/idspri/backup/cron** directory. Cisco IPICS displays the **/idspri/backup** directory as part of the Local Directory option, and prepopulates the **/cron** subdirectory in the Local Directory field. **Note** If you choose the **Default** option, Cisco IPICS changes the default settings and stores database backups in the **/idspri/backup** directory.
Backup retention	8 days

You can modify any of the default settings that are displayed in Table 11-2. Your changes become effective only after you click **Save** and they become the default settings.

To modify the automated settings for a database backup, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Schedule Backup** window to access the Schedule Backup tab.

Step 2 In the **Schedule Destination** pane, choose from one of the following destinations for your database backup:

- **Default**—Click this radio button to place the database backup in the **/idspri/backup** directory.
- **Local Directory**—Click this radio button to specify a subdirectory of the **/idspri/backup** directory on the local server to back up your database. If you back up your files to a local directory on the server, that directory must be a subdirectory of the **/idspri/backup** directory. If the directory does not exist, Cisco IPICS creates the directory for you.

Note Make sure that you precede the destination path with a forward slash (/). If you do not specify a forward slash, Cisco IPICS displays an error message in the **Administration > Database Management > Log** window and does not perform the database backup.

- **Remote Host**—Click this radio button to back up your database to a remote location. When you choose this option, you must specify the following information:
  - IP Address—Enter the IP address of the remote host.
  - User Name—Enter a valid user name for access to the remote host.
  - User Password—Enter a valid password for this user.
  - Remote Directory—Enter the location of the full directory path on the remote host where you want the backup files to be stored.

Note Cisco IPICS does not purge Remote Host backups.

Remote back up is supported-on Linux based systems only. WS_FTP is not supported by Cisco IPICS for scheduled remote back ups.

See the "Guidelines for Choosing a Destination for Database Backups" section on page 11-8 for more information about choosing a destination, user name, and password for your backup.

Step 3 To change the retention settings for the database backup, click the **Backup Retention** drop-down list to choose the number of days that you want the backup files to be stored.

Cisco IPICS deletes any backup files that are older than the backup retention setting whenever it performs a scheduled or manual backup.

Step 4 In the **Schedule Time** pane, view the default time and day values for the scheduled backup and, if required, modify the values by performing the following steps:

a. To modify the time of day for the scheduled backup to begin, click the **Start Time** drop-down lists and choose the appropriate values.

b. Under **Repeat Every**, modify the frequency of the scheduled backups by clicking the radio button that corresponds to one of the following options:
   - **Day**—This option schedules a daily backup. Click this radio button to configure daily database backups.

– **Specific Days**—This option activates the check boxes for individual days of the week. Click this radio button and check the appropriate days of the week to perform a database backup on the days of the week that you select.

Step 5 Click **Save** to apply and save your changes.

To discard your changes and return to the current default settings, click the **Cancel** button.

Caution If you do not click **Save**, your changes are not saved and the server reverts to the current settings.

Guidelines for Choosing a Destination for Database Backups

Be aware of the following guidelines when you choose a destination for your Cisco IPICS backups:

- Cisco recommends that you choose the remote host option when you back up your database. Using the remote host option ensures that you have a location for your database backups that will not be affected by Cisco IPICS server hardware or software failures.
- As an extra safeguard, you can also copy or move a database backup from one remote host to another for redundancy purposes.
- Manually perform a database backup to a remote host destination before you uninstall, reinstall, or upgrade the Cisco IPICS server software to preserve your most recent data.
- When you reinstall the Cisco IPICS operating system software on your server, the installation process formats the hard drive and removes all data from your server. To prevent the loss of your backup data, make sure that you have available another Linux-based server.
- Choose the remote host option only if the remote host supports SSH and the Linux Secure Copy Protocol (SCP), such as a Linux server.

Caveats for Remote Host Database Backups

When you specify the Remote Host option, be aware of the following caveats:

- Remote back up is supported-on Linux based systems only. WS_FTP is not supported by Cisco IPICS for scheduled remote back ups.
- The remote host must be a Unix-based system that supports standard ssh login.
- You must know the IP address of the remote host.
- You must use a valid user name and password on the remote host.
- To help ensure the security of your data, Cisco IPICS does not support the use of different user IDs for remote backup and restore operations that you perform on the same data set. Therefore, when you restore your data, make sure that you specify the same user ID as the one that you used to back up your data. If you specify a different user ID, the restore procedure does not succeed because of file accessibility issues; in this situation, Cisco IPICS displays “permission denied” error messages in the db-maintenance.log. As a best practice, Cisco recommends that you designate a specific user ID that you can use for all of your remote backup and restore activities.
- The remote host that you specify must be capable of running the scp command. If there are no remote hosts on your network that support scp (for example, a Windows PC or server), use the Local Directory option to back up your data, then use an SFTP client program, such as SSH Secure Shell

Client software (or similar software), to copy the backup files to a remote host. Follow the procedure in the "Backing Up Data to a Remote Host Without scp Support" section on page 11-16 to back up your data to a remote host that does not support scp.

- If the directory that you specify for the backup does not exist on the remote host, Cisco IPICS creates it for you.
- You must be the owner of the directory or have full access to the directory that you are using for the backup. The directory cannot have the group or others writable permission.
- Do not save backups in Unix system directories (for example, /, /var, /opt, /tmp, /etc) or in reserved Cisco IPICS system directories (/opt/cisco, /documents, /idspri/backup).

Restoring Data from a Database Backup

When you perform a restore operation, you retrieve data from a database backup, and restore the Cisco IPICS database to the state that it was in at the time that Cisco IPICS performed the backup.

Caution Database restores should only be done when there are no other users logging in to the system; otherwise, they may see errors or other strange behavior.

Note You cannot restore data from a database backup if high availability is running. In this case, you must temporarily unconfigure high availability before performing the restore. For instructions, see the "Unconfiguring HA" section on page 10-6.

You may need to restore your database if you encounter one or more of the following situations:

- You have to reinstall the server software and you need to restore the database to the state that it was in before you reinstalled the software.
- Server data, such as channels, channel groups or VTGs, were deleted from the database in error and you need to retrieve them.
- You need to copy a database from one Cisco IPICS server to another Cisco IPICS server. You copy the database by performing a database backup from one server, and restoring the database from that backup to another server.

Note You can restore data from one server to another only if both servers are running the same version of Cisco IPICS software. If the software versions of the two servers differ, the database schema might not be the same. In this case, the restore operation could fail, or you could encounter unpredictable errors when you perform tasks in the Administration Console.

This section contains information about restoring your data and includes the following topics:

Options for Using the Restore Procedure

To configure the restore parameters and perform all restore operations, access the **Administration > Database Management > Restore from Backup** window.

Caution A restore operation logs all users out of the Cisco IPICS database and users cannot log in to Cisco IPICS until the restore operation completes. To minimize any disruption that the restore procedure may cause to users, Cisco recommends that you perform a restore operation during a maintenance window or other off-peak hours.

You can restore your data from the default location, from another local directory that you specify, or from a remote host.

Note Before you restore your database, be aware that any configuration changes that you make after Cisco IPICS performs the database backup will not be restored.

Performing the Restore Procedure

To restore your data, perform the following procedure:

Before you begin

Ensure that no other users are logged in to the system.

Procedure

Step 1 Navigate to the **Administration > Database Management > Restore from Backup** window.

Step 2 In the **Restore Destination** pane, choose from the following options to restore your data:

- **Default**—Click this radio button to restore your data from the default location, which is **/idspri/backup**. If you backed up your database in the default location, choose this option. If there is more than one database backup in the default directory (for example, regularly scheduled database backups), Cisco IPICS uses the most recent backup for the restore operation.
- **Local Directory (requires full path)**—Click this radio button to restore your data from the local directory that you specify.

  When you specify a local directory or remote host for your restore operation, make sure that you specify the entire directory path and that you include the following directories in the directory path:

  - The **/idspri/backup** directory—Cisco IPICS stores every backup to a local directory in the **/idspri/backup** directory.
  - The **IDSB**_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss* directory that Cisco IPICS created when it performed the database backup.

Note You also specify the Local Directory option if you backed up your data to a remote host that does not support SCP. If you backed up your files to a remote host that does not support scp, follow the procedure in the "Restoring Data from a Remote Host Without scp Support" section on page 11-17 to move the backed-up files from the remote host to a local directory. Then, continue with this procedure.

- **Remote Host**—Click this radio button to restore your data from a remote host, in the directory location that you specify.

  When you click the Remote Host radio button, you must specify the following information:

  - IP Address—Enter the IP address of the remote host.
  - User Name—Enter a valid user name for access to the remote host.

    The user name to restore the database must be the same user name that you used to back up the database. If you specify a different user name, the restore procedure does not succeed because the user does not have the correct permissions to access the database backup.
  - User Password—Enter a valid password for this user.
  - Remote Directory—Enter the directory path for the remote host from which you want the database to be restored. Enter the full directory path, including the directory that was generated by Cisco IPICS for the database backup; for example: **/mybackups/IDSB_2006-08-25_17-13-55**.

Note Be sure to enter the correct user name, password, and remote directory; otherwise, the scp process fails. If the scp process fails, you can determine the cause of the failure by checking the logs in the **Administration > Database Management > Log** window.

Step 3 Click **Restore Now**.

A pop-up window displays to confirm the restore process.

Note When you perform a restore operation, all of the data that has been saved since the last time that your data was backed up, is lost. If you want to cancel the restore process and retain the data that has been saved since the last backup, click **Cancel**.

Step 4 Click **OK**.

Cisco IPICS begins the restore process and logs all users out of the Administration Console.

Note Unlike a database backup operation, you cannot view the log details of the restore operation in the Administration Console until the restore operation completes. The Tomcat service restarts during the restore operation and automatically logs all users out of Cisco IPICS.

Tip You can check the status of the restore operation before it completes by viewing the **/opt/cisco/ipics/database/logs/db-maintenance.log** file on the Cisco IPICS server. For more information, see the "Checking the Restore Status in the Database Log" section on page 11-13.

Step 5 To see the status of the restore operation, perform one of the following actions:

- To view the status of the restore operation by using CLI commands, see the "Checking the Restore Status in the Database Log" section on page 11-13.
- To view the final status of the restore operation, perform the following procedure:
  a. Wait about 10 to 15 minutes, then log in to the Administration Console by using the ipics user ID.

     If you attempt to log in to the Administration Console before the restore process completes, Cisco IPICS displays a message that is similar to the following example:

     ```
     You entered an invalid user name or password, or your browser was unable to
     recognize your entries.
     Please enter your user name and password again.
     If this problem persists, the database may be unavailable. Contact your System
     Administrator for help.
     ```

     If you receive the preceding message, you can check the progress of the restore operation by opening a terminal window and checking the log as described in the "Checking the Restore Status in the Database Log" section on page 11-13. If you still cannot log in to check this status, follow the troubleshooting procedures in the "Unable to Log In to the Administration Console After Restoring Data" section on page 11-18 to attempt to fix the problem.
  b. Navigate to the **Administration > Database Management > Log** window.
  c. Check the Database Logs pane to view the most recent status messages that pertain to the restore procedure.

Note Click **Refresh** to refresh the log window and view new messages.

Step 6 To view the entire database log file, perform the following procedure:

a. Wait approximately 20 minutes and then log in to the Administration Console.
b. Navigate to the **Administration > Database Management > Log** window.
c. Click **Download**.
d. Perform the actions that are listed in Step 3 in the "Downloading and Viewing the Backup and Restore Logs" section on page 11-14 to unzip the .zip file and view or download the db-maintenance.log file.

Step 7 If you are restoring the system to replace an existing server that failed or to re-create an existing Cisco IPICS system and its data on a new server, and the server on which you are restoring will have the same name as the old server, take these actions to restore trust certificates from the old server to the new server:

a. Use an SSH client to access the server on which the Cisco IPICS backup is located, log in as the root user, and enter these commands to extract the security tar file to a /tmp directory:

   # cd /tmp

   To extract the files for the primary Cisco IPICS server, where *path* is the full backup directory path and *ip_address* is the IP address of the primary Cisco IPICS server:

   # tar xvf *path***/security.pri.**_ip_address_**.tar**

   To extract the files for the secondary Cisco IPICS server, (in a high availability deployment only), where *path* is the full backup directory path and *ip_address* is the IP address of the primary Cisco IPICS server:

   # tar xvf *path***/security.sec.**_ip_address_**.tar**

b. Log in as the root user to the Cisco IPICS server on which the security directory is to be manually restored and enter these commands to back up the current security directory:

 # cd /opt/cisco/ipics

 # tar cvf security.tar.save security

c. Enter this command to replace the trust certificate files with the files that you extracted earlier in this step:

 # /bin/cp -rp /tmp/security/* /opt/cisco/security

d. Enter this command to restart Cisco IPICS:

 # service ipics restart

Checking the Restore Status in the Database Log

When the restore process begins, Cisco IPICS logs out all users from the Cisco IPICS Administration Console when the restore process begins. You cannot log in to the Administration Console until the process completes. To check the status of the restore procedure before it completes, log in to the Cisco IPICS server and view the contents of the db-maintenance.log file.

The db-maintenance.log file is located in the following directory on the server: **/opt/cisco/ipics/database/logs**.

For more information about the db-maintenance.log file, and other log files in Cisco IPICS, see the "Downloading and Viewing the Backup and Restore Logs" section on page 11-14.

To manually access the database log and check the status of the restore operation, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the ipicsadmin or root user ID.

A terminal window displays.

Note The ipicsadmin user has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. The root user has access to all files in the Cisco IPICS server.

Step 2 Enter the following command to see the last 25 lines of text in the db-maintenance.log file:

[ipicsadmin]# **tail -25 /opt/cisco/ipics/database/logs/db-maintenance.log**

Step 3 Check the last lines of this output to see whether the restore process completed successfully.

Step 4 To check the status of the restore operation, perform one or more of the following actions, depending on the output in the db-maintenance.log file:

- If you see the "Restore ended without errors" log entry, the restore process completed successfully and no further action is required.
- If you do not see the "Restore process ended without errors" log entry, or if you do not see any other message that indicates that the restore process has completed, wait several minutes and then repeat Step 2.

- If you see an error message indicating that the restore process ended but was not successful, check the log files by performing the following procedure:
  a. Enter the following command:

     [ipicsadmin]# **more /opt/cisco/ipics/database/logs/db-maintenance.log**

     Press the Spacebar to see additional lines of text, if necessary.
  b. View and evaluate the log file entries.

     The log file should provide you with information that indicates why the restore process did not complete successfully; for example, a remote restore operation could not complete because you entered an incorrect password for the remote host.
  c. Note the failure that occurred.
  d. Perform any actions as indicated by the failure to fix the problem. If you require further assistance, see the "Troubleshooting Cisco IPICS Backup and Restore Procedures" section on page 11-16 to attempt to fix the problem.
  e. Retry the restore operation by following the procedure in the "Performing the Restore Procedure" section on page 11-10.

Downloading and Viewing the Backup and Restore Logs

Cisco IPICS stores the logging details of backup and restore activity in two files, db-maintenance.log and dbm_log_archive.log.gz.

- The db-maintenance.log file captures the logging information that Cisco IPICS generates for backup or restore operations in a single day.

  You can view the contents of the db-maintenance.log file in the **Administration > Database Management > Log** window.

Note The db-maintenance.log file does not exist on the server until you perform a database backup or restore operation for the first time.

- The dbm_log_archive.log.gz file is a compressed file that contains archived data from previous db-maintenance.log daily log files.

  Whenever you perform a backup or restore operation, Cisco IPICS checks the db-maintenance.log file to see if it contains log data for that day. If the db-maintenance.log file contains data for a previous day, Cisco IPICS moves the information in the db-maintenance.log file to the dbm_log_archive.log.gz file. Cisco IPICS then saves the log data from the current backup or restore operation to the db-maintenance.log file.

  The default maximum allowable size of the dbm_log_archive.log.gz file is 5 MB. When the file reaches the maximum size, Cisco IPICS removes 5 percent of the oldest information in the dbm_log_archive.log.gz file until the file is smaller than the configured maximum size.

You can download the dbm_log_archive.log.gz file, along with the db-maintenance.log file, and save it to your PC by clicking the **Download** button in the **Administration > Database Management > Log** window. After you download the files to your PC, you can view them as a text file.

Cisco recommends that you regularly check the database logs for status messages and/or error information that may be pertinent to recent backup and recovery activity.

Note The downloaded files are joined and compressed into a single zipped file. The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files.

To download the db-maintenance.log and the database archive file from the Administration Console, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Log** window to access the Log tab.

Step 2 Click **Download** to open the Download dialog box.

The Download dialog box displays.

Step 3 Click **Save** to save the compressed file to your PC.

The **Save As** dialog box opens.

Step 4 Navigate to the directory location where you want to save the file; then, click **Save**.

The download program saves the .zip file to the location that you specified.

Step 5 Navigate to the directory location where you saved the .zip file.

Step 6 Double-click the .zip file to open it.

The .zip file opens and displays the db-maintenance.log and dbm_log_archive.log.gz files.

Step 7 Click the db-maintenance.log file to select it.

Step 8 Click **Extract**.

The Extract window opens.

Step 9 Navigate to the location of the directory where you want to save the db-maintenance.log file.

Step 10 Click **Extract**.

The extract program saves the db-maintenance.log file to the location that you specified on your PC.

Step 11 Double-click the dbm_log_archive.log.gz file to open it.

The .gz file opens and displays the dbm_log_archive.log file in a separate window.

Step 12 Click the dbm_log_archive.log file to select it.

Step 13 Click **Extract**.

The Extract window opens.

Step 14 Navigate to the location of the directory where you want to save the dbm_log_archive.log file.

Step 15 Click **Extract**.

The extract program saves the dbm_log_archive.log file to the location that you specified on your PC.

Step 16 To view the content of the log files, open the files with any software program, such as Notepad, that allows you to view text files.

Troubleshooting Cisco IPICS Backup and Restore Procedures

This section describes how to troubleshoot backup and/or restore activity.

The procedures that are described in this section require that you have access to one or more of the following user IDs:

- root
- informix
- ipicsadmin

This section includes the following topics:

Backing Up Data to a Remote Host Without scp Support

Problem The remote host to which you want to back up your data does not support the scp command (for example, the remote host is a Windows PC or server).

Solution Choose the Local Directory option when you back up your files; then, use a Secure File Transfer Protocol (SFTP) client software program to copy your backup data to a remote host.

To back up your data to a remote host that does not support scp, perform the following procedure:

Procedure

Step 1 Back up your files to a local directory by following the procedure in the "Performing a Manual Database Backup" section on page 11-3.

Step 2 Open a program that can act as an SFTP program, such as SSH Secure Shell Secure File Transfer Client or similar software. If you use SSH Secure Shell File Transfer Client, choose **Start > Programs > SSH Secure Shell > Secure File Transfer Client** to connect remotely to the Cisco IPICS server from your PC.

The SSH Secure Shell File Transfer Client window displays. The desktop of your PC displays in the left pane.

Step 3 Click **Quick Connect** to connect to the server.

The Connect to Remote Host window displays.

Step 4 In the Host field, enter the DNS host name or the IP address for your server; then, press the **Tab** key.

Step 5 In the User Name field, enter **root**.

Step 6 Click **Connect**.

The Enter Password window displays.

Step 7 Enter the password for the root user and click **OK**.

The SSH Secure Shell File Transfer Client connects to the server and displays the contents of the **/root** directory in the right pane of the window.

Step 8 Choose **Operation > Go to Folder** from the SSH Secure Shell menu bar.

The **Go to Folder** pop-up window displays.

Step 9 In the **Enter Folder Name** field, enter the name of the folder where you backed up your files (for example, **/idspri/backup/mybackup**).

The right pane of the window displays the contents of the folder. The folder contains a directory that is timestamped with the date and time that the local directory backup was performed, for example **IDSB_2006-11-02_14-04-52**. This directory contains your backup files.

Step 10 In the left pane of the window, navigate to the folder on your PC where you want to copy the backup files.

Step 11 Click the timestamped **IDSB***yyyy-mm-dd_hh-mm-ss* folder in the right pane of the window.

Step 12 Drag the folder from the right pane of the window to the left pane to initiate the copy procedure.

A progress window displays while the SSH Secure Shell program copies the backup folder and its contents to the folder that you specified on your PC. After the copy operation completes, the backup folder displays in the left pane.

Step 13 Close the SSH Secure Shell File Transfer Client.

Restoring Data from a Remote Host Without scp Support

Problem You backed up your data to a remote host that does not support scp (for example, a Windows PC or server), and you need to retrieve the backup files from the remote host.

Solution Use an SFTP client software program to move the backup files from the remote host to the server; then, restore your data from the local directory to which you moved the backed-up data.

To restore your data from a remote host that does not support scp, perform the following procedure:

Procedure

Step 1 Access the remote host where you backed up your data.

Step 2 Open a program that can act as an SFTP program, such as SSH Secure Shell Secure File Transfer Client or similar software. If you use SSH Secure Shell File Transfer Client, choose **Start > Programs > SSH Secure Shell > Secure File Transfer Client** to connect remotely to the Cisco IPICS server from your PC.

The SSH Secure Shell File Transfer Client window displays. The desktop of your PC displays in the left pane.

Step 3 Click **Quick Connect** to connect to the server.

The Connect to Remote Host window displays.

Step 4 In the Host field, enter the DNS host name or the IP address for your server; then, press the **Tab** key.

Step 5 In the User Name field, enter **root**.

Step 6 Click **Connect**.

The Enter Password window displays.

Step 7 Enter the password for the root user and click **OK**.

The SSH Secure Shell File Transfer Client connects to the Cisco IPICS server and displays the contents of the **/root** directory in the right pane of the window.

Step 8 In the left pane of the window, navigate to the folder location on your remote host where you stored the backup files, for example, **C:\My Documents\IDSB_2006-11-02_14-04-52**.

Step 9 Choose **Operation > Go to Folder** from the SSH Secure Shell menu bar.

The **Go to Folder** pop-up window displays.

Step 10 In the **Enter Folder Name** field, enter **/idspri/backup**.

The right pane of the window displays the contents of the **/idspri/backup** folder.

Step 11 Drag the backup folder on your PC from the left pane of the window to the right pane to initiate the copy procedure.

A progress window displays while the SSH Secure Shell program copies the backup folder and its contents from your PC to the **/idspri/backup** directory. After the copy operation completes, the backup folder displays in the right pane.

Step 12 Click the **New Terminal Window** icon or choose **Window > New Terminal** from the menu bar to open a terminal window session.

Step 13 Enter the following command to change the ownership of the backup folder and files from the root user and group to the informix user and ipics group:

[root]# **chown -R informix:ipics /idspri/backup/IDSB***

Step 14 Enter the following command to enable Cisco IPICS to read from and write to the backup folder and files:

[root]# **chmod -R 550 /idspri/backup/IDSB***

Step 15 To close the SSH Secure Shell terminal window, click **Close**.

Step 16 To close the SSH Secure Shell File Transfer Client, click **Close**.

Step 17 Restore your files from the local directory by following the procedure in the "Performing the Restore Procedure" section on page 11-10. Be sure to specify the full directory path of the backed-up database when you perform the local restore operation.

Unable to Log In to the Administration Console After Restoring Data

If you cannot log in to the Administration Console after you restore your data, note any errors that you receive in your browser and compare the error against the problem descriptions that follow. Then, perform the procedure that is listed in the corresponding solution to attempt to fix your problem.

Problem After checking the status of the restore operation as described in the "Checking the Restore Status in the Database Log" section on page 11-13, you determine that the restore process has completed successfully. However, when you attempt to log in to the Cisco IPICS console, you receive a **Cannot find server or DNS Error** error message in your browser and you cannot access the Administration Console.

Solution The Tomcat service may not have restarted after the restore operation. To restart the Tomcat service, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the root user ID.

Step 2 To restart the Cisco IPICS processes including the Tomcat service, enter the following command:

[root]# **service ipics restart**

Note Be aware that this command also restarts the policy engine, which cancels any active dial-in or dial-out calls.

Cisco IPICS displays the `[OK]` message after the Tomcat process and other Cisco IPICS processes have stopped, and again after they have successfully restarted.

Step 3 Log in to the Administration Console.

Problem After checking the status of the restore operation as described in the "Checking the Restore Status in the Database Log" section on page 11-13, you determine that the restore process has completed successfully. However, when you attempt to log in to the Cisco IPICS Administration Console, the system displays the following pop-up window:

```
You entered an invalid name or password.
Please try again.
If this problem persists, the database may be unavailable. Contact your system
administrator for help.
```

Solution In this case, the Cisco IPICS database might not have restarted after the restore operation. To restart the database, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the root user ID.

Step 2 To check the status of the database, enter the following command:

[root]# **onstat -**

Note This command displays the current status of the database.

If the database is online and running, the command displays the following response.

```
IBM Informix Dynamic Server Version 10.00.UC8W4   -- On-Line -- Up 15:54:28 -- 505836
Kbytes
```

If the database is not running, the command displays the following response:

```
shared memory not initialized for INFORMIXSERVER 'IPICSDBServer'
```

Step 3 If the database is not running, manually start the Informix database by entering the following command:

[root]# **service ipics_db start**

Step 4 Log in to the Administration Console.

Unable to Retrieve a Database Backup from a Remote Host After Reinstalling Cisco IPICS

Problem After reinstalling the Cisco IPICS operating system, you attempt to restore your data from a remote host. The restore operation failed.

Solution When you reinstall the Cisco IPICS operating system, the host keys that the scp process uses are deleted from the Cisco IPICS system. These host keys are used by the remote system for authentication purposes. In this case, the host keys that are used by the remote system to authenticate the Cisco IPICS system no longer match the host keys for the newly-installed Cisco IPICS system.

To configure the remote host so that the new host keys are recognized, perform the following steps:

Procedure

Step 1 Open a terminal window to the remote host by using SSH Secure Shell Client software or similar software.

Step 2 Log in to the remote host by using the same user name that you used for the database backup to the remote host.

Step 3 Open a secure shell terminal to the Cisco IPICS server by entering the following command:

ssh <*ip_address*> | <*dnsname*>

where:

<*ip_address*> or <*dnsname*> represents the IP address or DNS host name of the server.

You should receive a message similar to the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@        WARNING: HOST IDENTIFICATION HAS CHANGED!        @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
Add correct host key in /yoursystem/ssh/known_hosts to get rid of this message.
Agent forwarding is disabled to avoid attacks by corrupted servers.
X11 forwarding is disabled to avoid attacks by corrupted servers.
Are you sure you want to continue connecting (yes/no)?
```

Step 4 To accept the new public host key for the Cisco IPICS server, enter **Yes**.

Step 5 Enter **exit** to log out of the Cisco IPICS server.

Step 6 Enter **exit** to log out of the remote host.

Step 7 Retry the restore operation from the Cisco IPICS Administration Console as described in the "Restoring Data from a Database Backup" section on page 11-9.

Cannot Access the Administration Console to Back Up and Restore the Cisco IPICS Database

Problem You cannot access the Administration Console, so you are unable to perform backup and restore operations.

Solution For situations where you cannot access the Administration Console, you can use the command-line interface (CLI) to perform backup and restore procedures.

Note Cisco recommends that you use the Administration Console for normal backup and restore procedures. Use these CLI commands only in those situations where you cannot access the Administration Console.

To back up and restore your data by using CLI, perform the procedures that are documented in the following sections:

- Using CLI to Manually Back Up the Cisco IPICS Database, page 11-21
- Using CLI to Manually Restore the Cisco IPICS Database, page 11-22

Using CLI to Manually Back Up the Cisco IPICS Database

To manually back up your database by using CLI, use the **backup_ipics_ids** script. This script backs up your database, either to the default backup location or to a location that you specify. Use the arguments in the script to specify the location of the backup. You can back up your database files to the local server or to a remote server that supports the **scp** command.

To manually back up your database files, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the informix user ID.

If you cannot log in directly as the informix user (for example, if you do not know the password for the informix user ID), you can log in as the root user; then, access the informix user ID by using one of the following methods:

- Log in with the informix user ID by entering the following command:

  [root]# **su - informix**

- Reset the password for the informix user ID by entering the following command:

  [root]# **reset_pw -u informix**

  For more information about using the **reset_pw** command, see the "Troubleshooting the Cisco IPICS Server" chapter of the *Cisco IPICS Troubleshooting Guide*.

  A terminal window displays.

Step 2 To back up your database files, enter the following command:

[informix]$ **backup_ipics_ids** [**cp** <*localdirectory*>] [**scp** <*remotedirectory*> <*remoteip*> <*remoteuserid*> <*remotepassword*>]

where:

<*localdirectory*> specifies a subdirectory of the **/idspri/backup** directory where you want to store the database backup. If this directory does not exist, Cisco IPICS creates it for you as **/idspri/backup/***localdirectory*. For example, if you specify a directory of **mybackups** and that directory does not exist, Cisco IPICS creates a directory named **/idspri/backup/mybackups** and places the backup in that directory.

<*remotedirectory*> specifies the full directory path on the remote host where you want to store the database backup. This directory must exist; otherwise, the backup operation fails.

<*remoteip*> specifies the remote host IP address.

<*remoteuserid*> specifies the remote host user ID.

<*remotepassword*> specifies the password for the remote host user ID.

By default, if you do not specify any arguments with the **backup_ipics_ids** command, Cisco IPICS stores the database backup in the following directory:

/idspri/backup/IDSB_*yyyy-mm-dd_hh-mm-ss*

where:

yyyy-mm-dd_hh-mm-ss specifies the year, month, day, hour, minute, and second, respectively, that Cisco IPICS performed the backup procedure.

After you enter the **backup_ipics_ids** command, Cisco IPICS backs up the database files, creates the **IDSB_***yyyy-mm-dd_hh-mm-ss* subdirectory, and stores the backup in the specified subdirectory.

Using CLI to Manually Restore the Cisco IPICS Database

You can use the **restore_ipics_ids** script to restore your database from a backup file that you obtained from a backup operation. You can restore your database from a backup file on the local Cisco IPICS server or from a file on a remote server.

When you restore your files, you specify the full directory path where the backup file resides. The backup file has a file extension of .ota. An example of a full directory path is as follows:

/idspri/backup/IDSB_2007-05-01_17-11-47

By default, Cisco IPICS stores scheduled backup files in the **/idspri/backup/cron** directory. To restore your database from a scheduled backup that uses the default values, specify an .ota file from the **/idspri/backup/cron/** directory.

To manually restore your database from an existing backup, perform the following procedure. If high availability is running, you must temporarily unconfigure high availability before performing this procedure. For instructions, see the "Unconfiguring HA" section on page 10-6.

Procedure

Step 1 Open a terminal window and log in to the server by using the informix user ID.

A terminal window displays.

Step 2 If you already know the name of the backup file to use for the restore procedure, continue to Step 3. Otherwise, find the .ota file to use for the restore procedure by performing the following tasks:

- To find an .ota file on the local server, perform the following steps:
  - **a.** To list all of the .ota files on your server, enter the following command:

    [root]# **find / -name *.ota | more**

The name and full directory path of all .ota files that are on the server displays.

Note If many .ota files exist on your server, the list of files displays in multiple screens. Press the **Spacebar** to continue to the next screen.

b. Make a note of the full directory path and name of the .ota file that you want to use for the restore procedure.

- To find an .ota file on a remote host, log in to the remote host and perform Steps a and b.

Note When Cisco IPICS performs a remote backup, it creates a copy of each remote backup and stores it in the **/idspri/backup** directory on the local server; therefore, you can also find the list of remote backups in the **/idspri/backup** directory on the local server.

Step 3 To restore your database files, enter the following command:

[informix]$ **restore_ipics_ids** [**L**] [**L A** <*localdirectory*>] [**L A R** <*remoteuserid*> <*remotepassword*> <*remoteip*> <*remotedirectory*>]

where:

<*localdirectory*> specifies the full directory path on the local server where the .ota file is located.

<*localfilename*>**.ota** specifies the name of the backup file on the local server to use for the restore procedure.

<*remoteuserid*> specifies the remote host user ID.

<*remotepassword*> specifies the password of the remote host user ID. If backup files are not on the same server to which you are restoring, precede any special characters in the password with a backslash (\).

<*remoteip*> specifies the remote host IP address.

<*remotedirectory*> specifies the full directory path on the remote host where the .ota file is located.

Cisco IPICS restores the database from the .ota file that you specify.