Maintaining the Cisco IPICS System

Cisco IPICS provides a centralized location for diagnostic and status information, in the Serviceability drawer in the Administration Console, that system administrators can use for troubleshooting Cisco IPICS issues. The Serviceability drawer allows access to windows that contain system status, diagnostics, and logging information for Cisco IPICS.

This section includes information about using the windows in the Serviceability drawer. See the "Cisco IPICS Serviceability" section on page 4-1.

Cisco IPICS Serviceability

From the Serviceability drawer in the Administration Console, you can monitor system status in the various windows.

The following sections provide an overview of some of the system status monitoring tasks that can be performed in the Serviceability drawer:

Viewing Real-Time System Status in the Dashboard Window

Cisco IPICS provides you with current, real-time information regarding the overall status of the system. You can access this information in the **Serviceability > Dashboard** window. This window lists the resources that are being used, such as CPU or processor load, or license resources, such as how many IP phone ports that remain on a Cisco IPICS license.

Note To refresh the real-time information in this window and obtain the latest information, click **Refresh** at the top of the window.

Viewing and Downloading Diagnostic Information

You can view diagnostic information for various Cisco IPICS components by accessing the **Serviceability > Diagnostics** window. When you access this window, Cisco IPICS runs a script to obtain diagnostic information, along with downloading the ipics.log file.

You can also download a diagnostic summary, along with the current system log information, to your PC. When you download the diagnostic summary, Cisco IPICS creates a tar file that contains the diagnostic summary and the most current ipics.log file.

Note The PC from which you access the Cisco IPICS Administration Console must have an application installed, such as Win Zip, that can open, and extract files from, a tar file archive.

You must also use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file does not display properly.

Viewing and Downloading the Cisco IPICS System Logs

The system logs that you view in the **Serviceability > System Logs** window contain messages of different severities, ranging from informational-level messages to messages that indicate a fatal error has occurred in Cisco IPICS.

To visually identify the type of status message that appears in this window, Cisco IPICS displays log entries of different severities in the following text colors:

- Red—Red messages indicate that an ERROR-level error has occurred.
- Blue—Blue messages indicate that a WARNING-level error has occurred.
- Black—Black messages indicate that an INFO-level error has occurred.

You can view the total number of ERROR, WARNING, and INFO messages in the Status Summary area, which is directly below the Recent System Logs pane.

Note By default, the TRACE and DEBUG messages are not captured in the system logs. You should not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Cisco IPICS displays the most current system log information in the System Logs window and allows you to download all the system logs.

Cisco IPICS records system log information in the ipics.log file and continues to add data to it until the file reaches approximately 5.2 MB. When that file size limit has been reached, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new ipics.log file to capture the most current log data. This process continues until there are 10 system log files that range from ipics.log.1 to ipics.log.10. Cisco IPICS automatically purges the oldest file when you have accumulated 10 files.

When the system logs are downloaded in the **Serviceability > System Logs** window, Cisco IPICS creates a zip file of all the ipics.log files. The system logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

Cisco IPICS Database Management

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 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. If you need to configure specific database parameters, you can do so in the **Administration > Database Management** window.

You can back up and restore data from a backed-up database, and then download and view the logs in the Database Management window in the Administration Console. You can also export and import the database using command line interface commands.

This section includes the following database management topics:

Backing Up the System

Cisco IPICS provides you with the following options for database backups:

- Manual backups—You can perform a manual database backup to capture the current state of the Cisco IPICS database.

Note Use the Remote Host option only if the remote host supports the Linux Secure Copy (scp) command. If you are using a remote host that does not support scp (for example, a Windows PC or server), click the **Local Directory** radio button. You must back up your data to the Cisco IPICS server, then use a secure file transfer protocol (SFTP) client software program, such as SSH Secure Shell Client software (or similar software), to copy the backup files to a remote host. Refer to the *Cisco IPICS Server Administration Guide* for detailed information about how to back up your files to a remote host that does not support scp.

- 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 define the time, frequency, and the location of the backed-up database. After you modify the default settings for a scheduled backup, you click **Save** and the new settings become the default settings, and remain in effect until you change them.

Note Cisco IPICS does not purge backups that are made to a remote host.

Caution Be sure to click **Save** after making any changes or your changes are not saved and the server reverts to the current default settings.

As a best practice, make sure that you adhere to the following guidelines when you perform Cisco IPICS backup and restore procedures:

- To ensure data integrity in the event of a system failure, Cisco recommends that you back up your files to a remote host location.
- 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.
  - To view the backup log, navigate to the **Administration > Database Management > Database Backup** window. Log entries display in the Backup Log pane.
  - To view and/or download the database logs, navigate to the **Administration > Database Management > Log** window.
- 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.

Choosing the Destination for a Backup

When you specify the options for a scheduled backup, or when you perform a manual backup, you should determine the best location to store the backup. The location for the database backup can be to the default directory of the local Cisco IPICS server, to another directory of the local server, or to a remote host.

You can choose from the following types of locations for your database backup:

- Default directory—This is the default location that Cisco IPICS uses. When you choose this location, the backups are stored in the **/idspri/backup** directory.
- Local directory—Using this option, you can specify a directory for the backup. 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 that you specify does not exist, Cisco IPICS creates the directory for you.

Note Make sure that you preceded 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—Choose this option to back up your database to a remote location. When you choose this option, you must specify the following information:
  - Remote Host 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.

Note When choosing a remote host for the backup, be aware that the user name for the remote host is not encrypted in the Cisco IPICS server and is stored as clear text; therefore, Cisco recommends that you create a special user name that has restricted access to the remote host, has scp access, and only has write access to the directory where you saved the database backup.

  - 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 FTP client program to copy the backup files to a remote host. Refer to the *Cisco IPICS Server Administration Guide* for detailed information about how to back up your files to a remote host that does not support scp.
  - If the directory that you specify does not exist on the remote host, Cisco IPICS creates it for you.

Cisco recommends that you use the following guidelines when choosing a destination for your Cisco IPICS database backups:

- Choose a remote host location when you back up your database. Using the remote host option ensures that you have a location for your backups that cannot be affected by any hardware or software failures that might occur with the Cisco IPICS server.
- For 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 before you uninstall, reinstall, or upgrade the Cisco IPICS server software to ensure that you have a copy of the most recent data.
- The Cisco IPICS software requires the Cisco IPICS operating system to operate. If 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 all of your backups, you should back up your database to a remote location prior to installing the Cisco IPICS operating system.

– For this backup, choose the remote host option only if the remote host supports the scp command, such as a Linux server. To back up your data to a remote host that does not support scp, such as a Windows-based PC or server, choose the local directory option.

  To back up your files to a Linux-based server, use the remote host option before you install the new Cisco IPICS operating system.

  To back up your files to a Windows-based machine, use the local directory option; then, use the SSH Secure Shell Client software, or similar software, to perform a secure copy (scp) to the Windows-based machine.

Restoring the System

You may need to restore your database if you encounter any 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 VTG templates, were deleted from the database mistakenly and you need to retrieve them.
- You need to copy a database from one Cisco IPICS server to another. 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 using the same version of Cisco IPICS software. If the software versions of the server being backed up and the server being restored are not the same, the database schema might be different and the restore operation fails.

Caution Be aware that 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 operation may cause to users, Cisco recommends that you perform a restore procedure during maintenance operations or other off-peak hours.

You can choose from the following options to restore your data:

- Default—Choose this option 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, if you perform regularly scheduled database backups), Cisco IPICS uses the most recent backup for the restore operation.
- Local Directory (requires full path)—Choose this option 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. Make sure that you include the following directories in the directory path:

  - The **/idspri/backup** directory. Cisco IPICS places 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.
- Remote Host—Choose this option to restore your data from a remote host, in the directory location that you specify.

  When you choose to restore your data from a remote host, you must specify the following information:

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

    Your data is more secure if the same user performs both the backup and restore operations; therefore, the user name to restore the data 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 backed-up database.
  - 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.

A restore operation does not allow you to view the log details of the operation while it is in progress. The Tomcat service restarts during the restore operation and automatically logs all users out of Cisco IPICS. You must wait for the restore process to complete before you can log in again.

Tip You can check the status of the restore process in the **/opt/cisco/ipics/database/logs/db-maintenance.log** file on the Cisco IPICS server. For more information, refer to the *Cisco IPICS Server Administration Guide*.