CHAPTER 19

Maintaining System Health

This chapter contains the following sections:

Monitoring System Health

To view the system health dashboards, choose **Administration > Admin Dashboard**. Table 19-1 describes the information displayed on the dashboards.

Table 19-1 **Administration > Admin Dashboard Information**

Health Information Displayed	Description
System Health	Displays memory and CPU health information over a period of time.
System Events	Displays a list of events, time the event occurred, and the severity of the event.
System Information	Displays general system health information such as the server name, number of jobs scheduled and running, the number of supported MIB variables, number of users logged in, etc.

Using System Logs

Prime AM logs all error, informational, and trace messages generated by all devices that are managed by Prime AM.

Prime AM also logs all SNMP messages and Syslogs it receives.

You can download and email the logs to use for troubleshooting Prime AM.

Step 1 Choose **Administration > Logging**. The General Logging Options Screen appears.

Step 2 Choose a Message Level:

- Error
- Information
- Trace

Step 3 Check the check boxes within the Enable Log Module option to enable various administration modules. Check the **Log Modules** option to select all modules.

Step 4 In the Log File Settings portion, enter the following settings. These settings will be effective after restarting Prime AM.

- Maximum file size—Maximum number of MBs allowed per log file.
- Number of files—Maximum number of log files allowed.
- File prefix—Log file prefix, which can include the characters “%g” to sequentially number of files.

Step 5 Click the Download button to download the log file to your local machine.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

Step 6 Enter the Email ID or Email IDs separated by commas to send the log file.

Note To send the log file in a mail you must have Email Server Configured.

Step 7 Click **Submit**.

Changing SNMP Logging Options

Step 1 Choose **Administration > Logging**, then click SNMP Logging Options.

Step 2 Check the **Enable SNMP Trace** check box to enable sending SNMP messages (along with traps) between devices and Prime AM.

Step 3 Check the **Display Values** check box to see the SNMP message values.

Step 4 Configure the IP address or IP addresses to trace the SNMP traps. You can add up to a maximum of 10 IP addresses in the text box.

Step 5 Specify the maximum SNMP file size and the number of SNMP files.

Step 6 Click **Save**.

Changing Syslog Logging Options

Step 1 Choose **Administration > Logging**, then click Syslog Logging Options.

Step 2 Check the **Enable Syslog** check box to enable collecting and processing system logs.

Step 3 Enter the Syslog Host IP address of the interface from which the message is to be transmitted.

Step 4 Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.

Step 5 Click **Save**.

Using Logging Options to Enhance Troubleshooting

The logging screen allows you to customize the amount of data Prime AM collects in order to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC. These steps may create a smoother troubleshooting session:

Step 1 Choose **Administration > Logging**.

Step 2 From the Message Level drop-down list, choose **Trace**.

Step 3 Check each check box to enable all log modules.

Step 4 Reproduce the current problem.

Step 5 Return to the Logging Options page.

Step 6 Click **Download** from the Download Log File section.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

Step 7 After you have retrieved the logs, choose **Information** from the Message Level drop-down list.

Note Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

Changing Settings

When you choose **Administration > System**, you can change the Prime AM settings described in Table 19-2.

Table 19-2 Prime AM Settings

Click this Setting ...	To Specify ...
Alarms and events	Which alarms should be deleted, define which alarm types are displayed, specify alarm email options. **Note** Data cleanup tasks run nightly to delete old alarms. In addition to the data cleanup task, Prime AM has an hourly task to check alarm table size. When the alarm table size exceeds 300 K, the task deletes the oldest cleared alarms until the alarm table size is within 300 K. The Alarm Display Options apply to the Alarm Summary page only. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state. E-mails are not generated for acknowledged alarms regardless of severity change.
Data retention	How long to retain data for the different data types. **Note** For the best interactive graph data views, change the default settings to the maximum possible: 90 days for daily aggregated data and 54 weeks for weekly aggregated data. You must also make the appropriate measures to increase RAM and CPU capacity to compensate for these adjustments.
Login disclaimer	The disclaimer text that is displayed at the bottom of the login page for all users.
Mail server configuration	Global e-mail parameters for sending e-mails from Prime AM reports and alarm notifications. You can set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail addresses. Click the "Configure email notification for individual alarm categories" link to specify the alarm categories and severity levels you want to enable. Email notifications are sent when an alarm occurs that matches categories and the severity levels you select.
Notification receivers	Receivers who will receive notifications from Prime AM. Alerts and events are sent as SNMPv2 notifications to configured notification receivers. **Note** If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is configured. By default only INFO level events are processed for the selected category. Only SNMPV2 traps are considered for northbound notification.
Report	The path where reports are stored and for how long the reports are retained.
Server settings	Whether to enable or disable server ports.
Severity Configuration	The severity level of the alarms.
SNMP Settings	Global SNMP settings such as trace display values such as reachability parameters and backoff algorithm. If you select Exponential (the default value) for the Backoff Algorithm, each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time. If you select to use reachability parameters, the Prime AM defaults to the global Reachability Retries and Timeout that you configure. If unchecked, Prime AM always uses the timeout and retries specified. The default is selected.
Image Management	Preference parameters for downloading, distributing, and recommending software Images.

Table 19-2 Prime AM Settings

Click this Setting ...	To Specify ...
Configuration	Whether to backup the running configuration, to rollback the configuration, or to get show commands output from cache.
Configuration Archive	Basic configuration archive settings such as protocol, timeout value, number of configuration versions to store, etc.
Audit	Audit log purge settings and where to send purged logs.
Monitoring Settings	Auto monitoring for device and interface health collection and enable deduplication for server heath collections.

Checking the Status of Prime AM

To check the status of Prime AM at any time, follow these steps:

Step 1 Log into the system as **root**.

Step 2 Using the Linux CLI, perform one of the following:

- Navigate to the installation directory (such as /opt/NCS1.0.X.X) and enter **./NCSStatus**.
- Navigate to the installation directory (such as /opt/NCS1.0.X.X) and enter **NCSAdmin status**.

The CLI displays messages indicating the status of Prime AM.

Stopping Prime AM

You can stop Prime AM at any time by following these steps:

Note If any users are logged in when you stop Prime AM, their sessions stop functioning.

Step 1 Log into the system as root.

Note To see which version of Prime AM you currently have installed, enter **nmsadmin.sh version**.

Step 2 Using the Linux CLI, perform one of the following:

- Navigate to the shortcut location (defaulted to /opt/NCSA.B.C.D) and enter **./StopNCS**.
- Navigate to the installation bin directory (defaulted to /opt/NCSA.B.C.D/bin) and enter **StopNCS**.

The CLI displays messages indicating that Prime AM is stopping.

Backing Up the Database

This section provides instructions for backing up the Prime AM database. You can schedule regular backups through the Prime AM user interface or manually initiate a backup.

Note Machine specific settings (such as FTP enable and disable, FTP port, FTP root directory, TFTP enable and disable, TFTP port, TFTP root directory, HTTP forward enable and disable, HTTP port, HTTPS port, report repository directory, and all high availability settings) are not included in the backup and restore function if the backup is restored to a different device.

This section contains the following topics:

- Scheduling Automatic Backups
- Performing a Manual Backup

Scheduling Automatic Backups

To schedule automatic backups of the Prime AM database, follow these steps:

Step 1 Log into the Prime AM user interface.

Step 2 Click **Tools > Task Manager > Background Tasks** to display the Scheduled Tasks page.

Step 3 Click the **NCS Server Backup** task to display the **NCS Server Backup** page.

Step 4 Check the **Enabled** check box.

Step 5 At the **Backup Repository** parameter, Choose an existing backup repository or click create button to create a new repository.

Step 6 If you are backing up in remote location, select the FTP Repository check box. You need to enter the FTP location, Username and Password of the remote machine.

Step 7 In the Interval (Days) text box, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 8 In the Time of Day text box, enter the time when you want the backup to start. It must be in this format: *hh*:*mm* AM/PM (for example: 03:00 AM).

Note Backing up a large database affects the performance of the Prime AM server. Therefore, we recommend that you schedule backups to run when the Prime AM server is idle (for example, in the middle of the night).

Step 9 Click **Submit** to save your settings. The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/root/NCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-11_11-11-11.zip).

Performing a Manual Backup

To back up the Prime AM database on a Linux server, follow these steps:

Note you do not need to shutdown Oracle or the platform to do a backup.

Step 1 Log into the system as root.

Step 2 Create a local or remote backup directory for the Prime AM database with no spaces in the name (for example, mkdir **NCS1.0.X.X_Backup**).

Note Make sure that the directory name does not contain spaces. Spaces can generate errors.

Note If it is a remote backup location, you MUST specify the correct ftp location (For example, ftp://hostname/location) and user credentials.

Step 3 You can do a backup either through Command Line

Step 4 Perform one of the following:

- Backup the appliance and application to the repository (local or remote).

  backup *testbackup* **repository** *backup_repo*

- Backup the application only to the repository (local or remote).

  backup *testbackup* **repository** *backup_repo* **application** *NCS*

The CLI displays messages indicating the status of the backup.

Restoring the Database

To restore the Prime AM database from a backup file. follow these steps:

Step 1 To view all local repository backups, use the below command:

show repository backup_repo

Note If possible, stop all Prime AM user interfaces to stabilize the database.

Step 2 Manually shutdown the platform as root.

Step 3 Using the CLI, perform one of the following:

- restore the appliance and application backup.

  restore *testbackup-yymmdd-xxxx.tar.gpg* **repository** *backup_repo*

- restore the appliance only backup.

  restore *testbackup-yymmdd-xxxx.tar.gpg* **repository** *backup_repo* **application** *NCS*

Step 4 Click **Yes** if a message appears indicating that Prime AM is running and needs to be shut down.

Note If the restore process shuts down Prime AM, a restart is attempted after a successful restore. The appliance will then restart and you will have to again login and restart the dbserver, and the platform manually as root (make sure you do not start with dbclean, else you will loose your recently restored data).

The CLI displays messages indicating that the Prime AM database is being restored.

Uninstalling

You can uninstall Prime AM at any time, even while Prime AM is running.

To uninstall Prime AM on a Linux server, follow these steps:

Step 1 Stop Prime AM.

Step 2 Log into the system as root through an X terminal session.

Step 3 Using the Linux CLI, navigate to the /opt/NCS1.0.X.X directory (or the directory chosen during installation).

Step 4 Enter **./UninstallNCS**.

Step 5 Click **Yes** to continue the uninstall process.

Step 6 Click **Finish** when the uninstall process is complete.

Note If any part of the /opt/NCS1.0.X.X directory remains on the hard drive, manually delete the directory and all of its contents. If you fail to delete the previous Prime AM installation, this error message appears when you attempt to reinstall Prime AM: "**Cisco Prime AM is already installed. Please uninstall the older version before installing this version.**"

Recovering the Prime AM Password

You can change the Prime AM application root user or FTP user password. This option provides a safeguard if you lose the root password. An executable was added to the installer /bin directory (passwd.bat for Windows and passwd.sh for Linux). To recover the passwords and regain access to Prime AM, follow these steps:

Note If you are a Linux user, you must be the root user to run the command.

Note In Linux, use the ***passwd.sh*** to change the Prime AM password. The ***passwd*** is a built-in Linux command to change the OS password.

Step 1 Change to the Prime AM bin folder.

Step 2 For Linux, use the following command:

Enter **passwd.sh root-user** ***newpassword*** to change the Prime AM root password. The new password is the root login password you choose.
or
Enter **passwd.sh location-ftp-user** ***newuser newpassword*** to change the FTP user and password. The newuser and newpassword are the MSE or Location server user and password.

Step 3 The following options are available with these commands:

- -q — to quiet the output
- -pause — to pause before exiting-gui — to switch to the graphical user interface
- -force — to skip prompting for configuration

Step 4 Start Prime AM.

Managing and Updating Product Licenses

Prime AM licensing is based on the number of Netflow interfaces which you want to use Prime AM to manage. An Prime AM device license provides full access to all Prime AM features in order to manage a set number of such interfaces. You purchase a single base license and then purchase additional add-on licenses as necessary to accommodate additional devices.

Prime AM is deployed through physical or virtual appliances. You use the standard License Center Graphical User Interface to add new licenses, which are locked by the standard Cisco Unique Device Identifier (UDI). When Prime AM is deployed on a virtual appliance, the licensing is similar to that on a physical appliance, except instead of using a UDI, you use a Virtual Unique Device Identifier (VUDI).

Note To move licenses from one physical appliance to another, you need to call the Licensing TAC and rehost the licenses to a new UDI.

The Prime AM License is recognized by the SKU, which is usually attached to every purchase order to clearly identify which software or package is purchased by a customer.

Note If you are using an evaluation license, it is recommended that you add a base license before your evaluation license expires.

You can view license information by clicking **Help > About Prime AM**.

Caution Do not modify your license file; If you make any modifications, your license file will be corrupted.

Viewing License Details

To view the license type you currently have, the device and interface limits, and the percentage used and remaining on the license:

Step 1 Choose **Administration > Licenses**.

Step 2 Rest your cursor on the icon that appears next to Licenses to view licensing ordering help.

Adding Licenses

To add a new license:

Step 1 Choose **Administration > Licenses**.

Step 2 Under the Summary folder, click Files.

Step 3 Click **License Files**.

Step 4 Click **Add**.

Step 5 Browse to the location of the license file, then click **OK**.

Note Make sure the license file does not have a .txt extension.

Deleting Licenses

You might need to delete a license when:

- You are currently using an evaluation license and want to apply a base license.
- You are currently using an add-on license and want to apply a new license to accomodate additional devices.

Step 1 Choose **Administration > Licenses**.

Step 2 Under the Summary folder, click Files.

Step 3 Click **License Files**.

Step 4 Select the license file you want to delete, then click **Delete**.