Managing the Oracle Database and System Data

These topics explain how to manage the data that is used by Prime Network so that it is properly stored, and how to respond to system instability and event floods.

To change Oracle database passwords, see Changing Password for Oracle Database Schemas, page 11-10.

For more information on the flow of events through Prime Network, see How Prime Network Handles Incoming Events, page 9-1. For information on the Infobright database and Operations Reports, refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

Overview of the Prime Network Oracle Database and Schemas

The Oracle database can be embedded or external. Both types of Oracle databases can be installed on the gateway server or on a separate server. An *embedded* Oracle database is fully integrated with Prime Network; you can use native tools to manage and monitor an embedded database. An embedded Oracle database is automatically backed up by Prime Network. An *external* Oracle database is managed separately from Prime Network using the tools provided by Oracle; it is not backed up by Prime Network.

Oracle Database Schemas

A Prime Network application operating system account is created when Prime Network is installed. When Prime Network creates the Oracle database schemas, it uses this operating system account name as the default for naming all schemas.

Table 8-1 lists the Oracle database schemas that are created by Prime Network. It also provides examples of what the schema names would be if *pnuser* (the operating system account for the Prime Network application) was defined as **pn41** at installation time. You can also create the schemas manually, using different names, as described in the *Cisco Prime Network 4.2 Installation Guide*, but the purpose of each schema remains the same.

Table 8-1 Prime Network External and Embedded Oracle Database Schemas

Default Schema Names	Description	Example Schema Name
pnuser	Prime Network main schema that contains most Prime Network data. It also contains the Fault Database, which are the tables related to the fault subsystem: • Network fault and event tables—NETWORKEVENT, ALARM, TICKET, GENERICEVENT, GENERICTRAPEVENT, GENERICTRAPVALUE, NEWTRAPEVENT, and NEWTRAPVALUE tables. Each of these tables contain one active partition and several archive partitions (1 partition per hour). Tickets can be manually or automatically archived. When data is archived, it is moved to an archive partition based on the object timestamp. Archive partitions which exceeds the history size (14 days by default) are deleted. • Non-network fault and event tables—SYSTEMEVENT, AUDITEVENT, SECURITYEVENT, PROVISIONINGEVENT tables are partitioned according to time. Partitions that exceed the history size are deleted. Data is deleted from the Fault Database according to the settings in **Global Settings > Event Management Settings**.	**pn41**
*pnuser*_**ep**	Legacy Event Archive schema that is no longer used. (The tables are still created but they are empty.)	**pn41_ep**
*pnuser*_**rep**	Prime Network reports schema that contains synonyms based on the *pnuser* schema tables; it is used by the reports mechanism. Reports are deleted according to the settings in **Global Settings > Report Settings**; see Purging Reports, page 8-12.	**pn41_rep**
*pnuser*_**ep_rep**	Prime Network reports schema that contains synonyms based on the *pnuser*_**ep** schema tables; it used by the reports mechanism. Reports are deleted according to the settings in **Global Settings > Report Settings**; see Purging Reports, page 8-12.	**pn41_ep_rep**
*pnuser*_**xmp**	Prime Network Change and Configuration Management, Compliance Manager, and Command Manager schema that contains data related to these features. For more information on Change and Configuration Management, see Purging Configuration Archives and Software Images, page 8-11.	**pn41_xmp**
*pnuser*_**admin**	User with Oracle database administrator permissions who can run maintenance tasks—such as gathering statistics—on the other Prime Network Oracle database schemas. If this user is created with the proper permissions (as described in the installation guide), Prime Network will run a cron job called **every_24_hours.cmd** that gathers statistics on other Oracle database tables. This provides an automatic method for generating Oracle database statistics, which is recommended for better performance. For more information, refer to the *Cisco Prime Network 4.2 Installation Guide*.	**pn41_admin**

For information on the Infobright database used by Operations Reports, refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

Controlling How Data is Saved, Archived, and Purged

The Prime Network defaults for saving and deleting data ensure that current data remains available, while not impacting system performance. Table 8-2 lists the defaults for purging (permanently deleting) data from the database or gateway directories. You can adjust these settings according to the needs of your deployment. These mechanisms are described in the following topics:

Note For information on Operations Reports data and the Infobright database, refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

The following table lists the default settings for purging data from Prime Network.

Table 8-2 Default Settings for Purging Data

Data	Purged After (Default):
Oracle Fault Database[1]	14 days
Jobs	Never purged
Reports—Prime Network standard reports	90 days
Backups of gateway data for systems with external Oracle database	5 backups
Backups of gateway data for systems with embedded Oracle database	16 backups
Backups of database for systems with embedded Oracle database[2]	8 days
Diagnostics (Graphs) tool	29 days
Configuration Archive files and change logs	30 days
Software Images	n/a (manual deletions only)

1. Tickets are deleted 14 days after they are moved to an archive partition in the Fault Database. For more information, see Clearing, Archiving, and Purging Fault Data, page 8-5.
2. See Managing an Embedded Oracle Database, page 8-14 for information on additional checks that are performed by Prime Network.

How the Data Purging Mechanism Works

Prime Network maintains system stability by running cron jobs to maintain the Oracle database and eliminate clutter in the system, especially fault management data. Some jobs are run every 12 hours, while others are run every hour.

Different cron jobs are run on different schedules. To check the current schedules, use this procedure.

Step 1 Using an SSH session, log into the Prime Network gateway as *pnuser*.

Step 2 Use the following command to list the contents of the crontab file for user *pnuser*. The local/cron directories listed below are all located in *NETWORKHOME*.

```
# crontab -l
# Cisco Prime Network crontab file
# contains scheduled tasks for user prime-network
* * * * * if [ -f local/cron/every_1_minute.cmd ]; then local/cron/every_1_minute.cmd >
/dev/null 2>&1; fi
* * * * * /var/adm/cisco/prime-network/scripts/keep_alive_port_watchdog.pl > /dev/null
2>&1
0 * * * * if [ -f local/cron/every_1_hour.cmd ]; then local/cron/every_1_hour.cmd >
/dev/null 2>&1; fi
0 4,16 * * * if [ -f local/cron/every_12_hours.cmd ]; then local/cron/every_12_hours.cmd
> /dev/null 2>&1; fi
0 23 * * * if [ -f local/cron/every_24_hours.cmd ]; then local/cron/every_24_hours.cmd >
/dev/null 2>&1; fi
0,10,20,30,40,50 * * * *  if [ -f local/cron/every_10_minutes.cmd ]; then
local/cron/every_10_minutes.cmd > /dev/null 2>&1; fi
0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57 * * * *  if [ -f
local/cron/every_3_minutes.cmd ]; then local/cron/every_3_minutes.cmd > /dev/null 2>&1;
fi
```

(The port watchdog script is part of the AVM protection mechanism and is described in AVM 100 and Unit Server High Availability, page 5-3.)

If desired, you can modify when the jobs run by editing the crontab file. For example, the following line in the crontab file runs the file every_12_hours.cmd at 4:00 a.m. and 4:00 p.m.:

```
0 4,16 * * * local/cron/every_12_hours.cmd > /dev/null 2>&1
```

Table 8-3 lists some of the integrity tests performed by Prime Network. These tests run on a regular basis to ensure system stability and purge old data. Prime Network archives and purges fault data according to the settings described in Clearing, Archiving, and Purging Fault Data, page 8-5.

If you have an embedded Oracle database, additional purging checks are performed as described in Managing an Embedded Oracle Database, page 8-14. These settings are defined in the registry unless otherwise noted.

Table 8-3 Integrity Tests

Test Name	Description
analyze	Generates a System event if the period between the current date and the date each Oracle database table was analyzed is larger than the analyze-Period setting.
backup	Backs up the registry, encryption keys, and crontab files. By default, backups are saved to *NETWORKHOME*/backup. Backups are performed every 12 hours at 4:00 a.m. and 4:00 p.m. (Registry backup settings are described in Backing Up and Restoring Data Stored on the Gateway, page 2-7.)
businessObject	Checks for invalid OIDs in business objects. If more than two invalid business tags are found, Prime Network generates an event containing the list of OIDs.
capacity	Checks the disk space capacity and sends alarms. Alarms are sent when the disk capacity reaches 80% and 90%.
checkDbClock	Ensures that Oracle database clock is synchronized with the NTP server.
jobSchedulerPruning	Ensures that jobs have been deleted according to the system settings. (This setting is controlled in the Prime Network Administration GUI client; see Purging Jobs, page 8-12).
mapAspect	Removes mapAspect OIDs which are not connected to any hierarchy.
oidArrays	Removes OIDs which exist in the OidArrays table, but not in a parent table.
reports	Deletes reports after 90 days. (This setting is controlled in the Prime Network Administration GUI client; see Purging Reports, page 8-12).
unusableIndexes	Checks for unusable table indexes and, if found, rebuilds them.

Clearing, Archiving, and Purging Fault Data

These topics explain how fault data is saved, cleared, archived, and deleted, along with their configurable points:

- How is Fault Data Cleared, Archived, and Purged?, page 8-5
- Adjusting the Ticket Locking and Auto-Clearing Mechanisms, page 8-7
- Adjusting the Ticket Auto-Archiving Settings, page 8-8
- Adjusting the Fault Database Purging Settings, page 8-11
- Purging Configuration Archives and Software Images, page 8-11

For information on changing purging settings for Operations Reports and the Infobright database, refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

How is Fault Data Cleared, Archived, and Purged?

The following topics explain the difference between clearing, archiving, and purging fault data, along with the automatic and manual mechanism you can use.

Note In some cases a distinction is drawn between *network events* and *non-network events*. Network events are Service, Trap, and Syslog events. Non-network events are System, Security, and Provisioning events.

Clearing Fault Data

When an event, alarm, or ticket is *cleared*, it means it is no longer a problem. For a ticket, this means its root cause and all of its associated events have cleared. When an item is cleared, its severity icon changes to a green check mark, providing a visual indication that the problem has been addressed. (Acknowledging an event is different. Acknowledging indicates that someone is *aware* of the issue. Acknowledging does not change the severity icon; it just changes its Acknowledged value to **True**.)

Because a new event could still associate to the ticket (for example, if the root cause recurs), a cleared ticket is still considered *active*.

Every 60 seconds, a special mechanism checks to see if uncleared tickets can be cleared. The mechanism looks for the following:

- If the ticket's events are cleared, or
- If the ticket's root cause is cleared, and its other events are configured for auto-clearing.

If either of these cases is true and the ticket has not been modified in the last 4 minutes, Prime Network clears the ticket.

The clearing mechanism is important because a ticket is not considered cleared until its root cause and all of its events are cleared. But situations can occur in which a ticket's root cause is cleared, but an associated event has not cleared due to a missed syslog or a reachability problem. If the event is set to auto-clear, and the ticket's root cause is cleared, the auto-clear mechanism will clear the event, resulting in the entire ticket being cleared. Whether an event can be auto-cleared is controlled by its auto-cleared registry setting.

Note Auto-clear does not clear a ticket if the root cause event is not cleared.

When an event is auto-cleared, the Vision client displays an event description with "Auto Cleared" in the text—for example, **Auto Cleared - Link Down due to Admin Down**. All syslogs and traps are configured to clear automatically, except:

- Syslogs and traps that are ticketable.
- A few important syslogs and traps that do not have a corresponding Service events. For example, a device that suddenly loses power does not send a Down event. Instead, it sends a cold start trap when it subsequently recovers, and this trap is not cleared automatically because no corresponding Down event exists, if the cold start trap were automatically cleared, the device-recovery notification would be lost.

You can customize the following criteria, which are disabled by default (see Adjusting the Ticket Locking and Auto-Clearing Mechanisms, page 8-7):

- Clear a ticket based on its severity and the number of days since it was last modified. (In this case, the ticket description will say **Cleared due to time expiration**.)
- Adjust when a cleared ticket is locked and no new events can associate to it. If the ticket remains unchanged for 1 hour (by default), it is archived; see Archiving Fault Data, page 8-6 for more information on archiving.

Archiving Fault Data

When a ticket or event is *archived, it* means the ticket or event is no longer active. Archived data is moved to an archive partition in the Fault Database.

Some data is immediately archived in the Fault Database—standard events, new alarms and upgraded events that are not ticketable, and (if enabled) events from unmanaged devices. (Standard and upgraded events are described in Upgraded Events and Standard Events, page 9-1.)

To protect system performance and stability, Prime Network has an auto-archive mechanism runs every 60 seconds and archives tickets (and their associated events). Cleared tickets are archived if they are unchanged for a specified period of time (1 hour by default). Cleared and uncleared tickets may be archived if their number or size maybe affect system stability. The auto-archive criteria are listed in the following table (see Adjusting the Ticket Auto-Archiving Settings, page 8-8).

Archive criteria	Archive ticket if:
Length of time ticket has been clear	No new events were associated to the cleared ticket in past 1 hour (by default).
Size of ticket (cleared or uncleared)	A cleared or uncleared ticket has more than 150 events associated with one of its alarms. (Prime Network also generates a System event 15 minutes before it archives the ticket.)
Number of large tickets (cleared or uncleared) in Fault Database	The database has 1500 large cleared and/or uncleared tickets in its active partition. (Prime Network also generates a System event as it approaches this number.)
Total number of tickets (cleared or uncleared) in Fault Database	The database has over 16,000 cleared and/or uncleared tickets in its active partition.

Purging Fault Data from the Fault Database

When data is purged, it is permanently removed from the Fault Database. By default, Prime Network purges event data from the Fault Database after 14 days—that is, 14 days from the event's creation time. However, events that are associated with uncleared tickets are never purged, regardless of their age. Once the ticket clears, if any of its events are 14 days old, they are immediately purged.

Adjusting the Ticket Locking and Auto-Clearing Mechanisms

This topic describes how you can customize the auto-clearing mechanism.

The locking mechanism that allows you to specify *when* a cleared ticket will be locked, meaning no new events can associate to it. This period is 1 hour by default, but this mechanism allows you to specify a shorter period. The locking setting does not override when the ticket is archived (1 hour). For example, if the ticket locking mechanism was set to 20 minutes, the following would happen to an event that cleared at 1:10:

1. If no new events associate to the ticket for 20 minutes, the ticket would be locked at 1:30.
2. The ticket would be archived at 2:10.

Even if an associated event occurred at 1:35, the locked ticket would *not* be reopened (uncleared). Instead, Prime Network would create a new ticket.

The second mechanism lets you control when to force-clear a ticket according to its severity and how long it has remained unchanged. This helps you rid the system of less serious tickets that remain uncleared for a long period of time.

Step 1 Select **Global Settings > Event Management Settings** from Prime Network Administration.

Step 2 Make your desired changes to the following settings in the Tickets area.

Description		Default
Lock cleared tickets after ____ minutes	If specified, determines when a cleared ticket can no longer be reopened (uncleared) and new events cannot be added to it. If not specified, the default is used (1 hour of idle time). This does not change the default archive time of 1 hour. (See the example earlier in this topic.)	Disabled
Automatically clear tickets	System clears the tickets that are older than a predefined time and severity.	Disabled
	Severity—Severity of the tickets (Critical, Major, Minor, Warning) that should be cleared.	Disabled
	Days since last modification—Clears the ticket if the ticket was not modified for the specified number of days.	Disabled

Step 3 Click **Apply**. The changes will take effect in the next partitioning process execution (which is done once an hour). You can restore the default settings at any time by clicking **Restore**.

Adjusting the Ticket Auto-Archiving Settings

Caution Consult with your Cisco account representative before changing these settings. Making the settings smaller could result in immediate and permanent removal of fault data. Making the settings larger could result in slow data retrieval performance; the system might require additional storage and some database tuning; and backups might require more time.

Cleared tickets are auto-archived if they have not changed in the past 1 hour. This setting is controlled in the registry.

Table 8-4 Registry Settings for Automatic Archiving of Cleared Tickets

Registry Entry	Description	Default Value
autoArchivingTimeout	Archive cleared tickets that have not changed in this period of time (in milliseconds). This timeout is not affected by the locking mechanism described in Adjusting the Ticket Locking and Auto-Clearing Mechanisms, page 8-7.)	3600000 (1 hour)

Step 1 Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

Step 2 To change the autoArchivingTimeout setting to 90 minutes:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/plugin/AlarmPlugin/autoArchivingTimeout" 5400000
```

Step 3 Restart the gateway for your changes to take effect. See Stopping and Restarting Prime Network Components, page 3-16.

Adjusting Ticket Auto-Archiving Based on Total Number of Tickets (Oracle Fault Database)

Prime Network checks how many cleared and uncleared tickets are saved in the Oracle Fault Database to see if they should be archived, as follows:

- When the total number of tickets (cleared and uncleared) in the Fault Database exceeds 12,800, it generates a System event.
- When the total number of tickets (cleared and uncleared) in the Fault Database exceeds 16,000, it archives tickets in groups of 400.

Use the Registry Controller to adjust these settings.

Caution Consult with your Cisco account representative before changing these settings. Making the settings smaller could result in immediate and permanent removal of fault data. Making the settings larger could result in slow data retrieval performance; the system might require additional storage and some database tuning; and backups might require more time.

Step 1 Choose **Tools > Registry Controller > Database** from the main menu of the Administration GUI client.

Step 2 Adjust the settings as needed.

Settings for Archiving Based on Total Number of Tickets	What the Setting Controls	Default
Ticket Red Threshold Amount	When the number of cleared or uncleared tickets exceeds this number, Prime Network should archive the amount of tickets specified by *Ticket Archiving Bulk*	16000
Ticket Yellow Threshold Percentage	When this percentage of *Ticket Red Threshold Amount* is exceeded, Prime Network should generate a System event	80
Wake Up Message Interval	How often Prime Network should check the amount of cleared and uncleared tickets (in milliseconds).	60000 (1 minute)
Ticket Archiving Bulk	Amount of cleared or uncleared tickets Prime Network should archive when *Ticket Red Threshold Amount* is exceeded. After the *Wake Up Message Interval* has passed, if the total is still above the *Ticket Red Threshold Amount*, it will archive this number of tickets again.	10

Step 3 Verify your changes to ensure you want to overwrite the current registry settings because after you click Apply, you cannot retrieve your settings using the Restore button.

Step 4 Click **Apply**.

If you have installed an embedded Oracle database, see the additional management topics in Managing an Embedded Oracle Database, page 8-14.

Adjusting Ticket Auto-Archiving Based on the Size of Tickets (Oracle Database)

Every five minutes, Prime Network checks the Oracle database to see if it contains any large tickets (cleared or uncleared) that should be archived. A ticket is considered large if it has more than 150 events associated with an alarm. To protect system performance, Prime Network does the following:

- If a large ticket is found, it generates a System event similar to the following:

  ```
  The system contains the following XXX ticket(s) with more than 150 events per alarm.
  You can manually archive these tickets or the system will automatically archive them
  in: 15 minutes
  ```

  If the user does not respond within 15 minutes, Prime Network archives the tickets.

- If more than 1500 large tickets are found, it will send this System event:

  ```
  There are more than XXX excessively large tickets in the system (tickets with more
  than 150 events per alarm).
  ```

Use the Registry Controller to adjust these settings.

Caution Consult with your Cisco account representative before changing these settings. Making the settings smaller could result in immediate and permanent removal of fault data. Making the settings larger could result in slow data retrieval performance; the system might require additional storage and some database tuning; and backups might require more time.

Step 1 Choose **Tools > Registry Controller > Database** from the main menu of the Administration GUI client.

Step 2 Adjust the settings as needed.

Settings for Archiving Based on Ticket Size	What the Setting Controls	Default
Find Large Tickets Message Interval	Interval for searching for large cleared or uncleared tickets (in minutes).	5
Max Ticket Size	When the number of events associated with an alarm surpasses this number, consider it a large ticket and generate a System event.	150
Auto Remove Time Interval	Interval at which to archive large cleared or uncleared tickets (in minutes) after sending System event.	15
Oversized Ticket Amount Limit	When the number of large cleared or uncleared tickets surpasses this number, generate a System event.	1500

Step 3 Verify your changes to ensure you want to overwrite the current registry settings because after you click Apply, you cannot retrieve your settings using the Restore button.

Step 4 Click **Apply**.

If you have installed an embedded Oracle database, see the additional topics in Managing an Embedded Oracle Database, page 8-14.

Adjusting the Fault Database Purging Settings

These settings control when fault data is permanently deleted from the Oracle Fault Database.

Caution Consult with your Cisco account representative before changing these settings. Making the settings smaller could result in immediate and permanent removal of fault data. Making the settings larger could result in slow data retrieval performance; the system might require additional storage and some database tuning; and backups might require more time.

Step 1 Select **Global Settings > Event Management Settings** from Prime Network Administration.

Step 2 Make your desired changes to the following settings.

Field		Description	Default
Fault Database	Remove events from database after ____ days	Number of days after which archived data will be deleted from Oracle Fault Database partitions.	14
	Database partition size (in hours)	Number of hours after which each Oracle Fault Database partition will be split. (For database sizing guidelines and other capacity planning information, contact your Cisco account representative.)	1
Event Archive	Remove events from database after ____ days	**Note** The Event Archive is no longer used in Prime Network (it is still created but is empty). Do not change this setting.	14
	Database partition size (in hours)		1

Step 3 Click **Apply**. The changes will take effect in the next partitioning process execution (which is done once an hour). You can restore the default settings at any time by clicking **Restore**.

Purging Configuration Archives and Software Images

Prime Network Change and Configuration Management data is deleted according to these settings:

- Device configuration files and change logs are saved for 30 days by default. After that, they are deleted from the archive.
- Software image files are not deleted; they can only be manually removed using the Change and Configuration Management GUI client.

For more information, refer to the *Cisco Prime Network 4.2 User Guide*.

Purging Jobs

The retention policy for job runs can be configured using the Job Manager Settings page. This includes jobs for CCM, Compliance Audit, Command Manager, and Transaction Manager. Old job runs which do not comply to the configured policy will be automatically purged. By default, no jobs are purged.

To set up or change Job Manager purge settings:

Step 1 Choose **Global Settings > Job Manager Settings**.

Step 2 Configure the settings that control when job runs will be purged from Prime Network.

Field	Description
Purge Job Runs After	Specifies how long to save a job run. The time is measured from when the job run is created (in days).
Store Up to	Specifies the maximum number of job runs, after which job runs should be purged. When this number is exceeded, Prime Network deletes the oldest job runs (first in, first out). Prime Network runs a purge by size check every time a new job runs is created or a user changes the settings on this page. This feature is disabled by default.

If these settings are changed to lower values, after the changes are applied, Prime Network immediately deletes all job runs that exceed the thresholds.

Step 3 Click **Apply** to immediately apply your settings.

Purging Reports

The Report Settings page in the Global Settings drawer controls:

- When reports should be purged. Reports are saved in the Oracle database and in a gateway file system (in an intermediate format that is rendered to HTML or PDF when viewed). By default, they are purged after 90 days. This page also shows you how much space reports are currently consuming.
- Whether users can share reports (create public reports). If a report is public, all users can view the report; public reports are *not* filtered according to scopes or security privileges.

The settings do not affect user permissions for report actions such as adding, deleting, canceling, and so forth. Users can still perform all actions on reports they create; they can view other reports only if the reports are public. Administrators are the only users who can perform all actions on all reports.

Note We recommend that you use these default settings in order to reduce system clutter. Allowing report data to accumulate could affect system performance.

To set up or change global report settings:

Step 1 Choose **Global Settings > Report Settings**.

Step 2 Configure the settings that control when reports will be purged from Prime Network, using dates, size, or both.

Field	Description
Purge report after: ___ days	Specifies how long to save a report. The time is measured from when the report is created. If you do not check this box, Prime Network defaults to 90 days. The Prime Network integrity service runs a job every 12 hours to purge all reports that exceed this age.
Store reports up to: ___ MB	Specifies the maximum disk size, in MB, at which reports should be purged. When this space setting is exceeded, Prime Network deletes the oldest reports (first in, first out). Prime Network runs a purge by size check every time a new report is created or a user changes the settings on this page. This feature is disabled by default.

If these settings are changed to lower values, after the changes are applied, Prime Network immediately deletes all reports that exceed the thresholds.

Step 3 The Enable Shared Reports check box specifies whether users can create public reports. When a report is public, all users can view the contents; reports are *not* filtered according to scopes or security privileges. Changes to this setting are applied to all subsequent new reports.

- If not selected, no users will be able to create public reports. Users will only be able to view their own reports.
- If selected, users have the option to create public reports and share them with other users.

Step 4 Click **Apply** to immediately apply your settings.

After you click **Apply**, the report settings are applied to all existing and new reports. You can restore the Prime Network default settings at any time by clicking **Restore** and **Apply**.

Purging Monitoring (Graphs) Tool Data

Data gathered by the Prime Network Monitoring tool is purged after 28 days as described in Checking Overall System Health with the Monitoring (Graphs) Tool, page 3-34.

Purging Backups

Prime Network performs backups on a regular basis for Prime Network gateway data and the embedded Oracle database. For more information, see Backing Up and Restoring Data, page 2-5. For information on Infobright database backups, refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

Note You should save backups to tape on a regular basis.

This table lists the default backup settings.

Data Type	Backups Purged After:
Prime Network gateway data (system with external Oracle database)	5 backups
Prime Network gateway data (system with embedded Oracle database)	16 backups
Embedded Oracle database	8 days

We do not recommend changing the backup settings for the gateway or embedded Oracle data.

Managing an Embedded Oracle Database

Prime Network performs regular checks to ensure the health of the embedded Oracle database. Prime Network also provides native utilities for adding storage, collecting database logs and reports, and other maintenance tasks. These are all described in the following topics:

- Overview: How Prime Network Monitors an Embedded Oracle Database, page 8-14
- Embedded Oracle Database Events and Errors, page 8-15
- Stopping, Starting, and Changing Oracle Embedded Database Settings (emdbctl Utility), page 8-17
- Retrieving Your Embedded Oracle Database Profile Setting from the Registry, page 8-19
- Changing the SMTP Server for Embedded Oracle Database Notifications, page 8-22

Overview: How Prime Network Monitors an Embedded Oracle Database

Prime Network performs regular maintenance checks and backups for embedded Oracle databases. Backups are enabled as part of the installation process. If you did not enable backups, you can do so using the procedure in Backing Up and Restoring Data, page 2-5. That topic also provides information on backup schedules, how many backups are saved, and the backup location.

Table 8-5 lists the regular maintenance checks performed by Prime Network.

Table 8-5 Cron Jobs for Maintaining the Embedded Oracle Database

Cron Job Task	Description
Monitor disk usage on Oracle database server	Hourly job that checks Oracle database disk usage (on server host) for data files, redo logs, backup files, and so on. If any directory exceeds a threshold, an e-mail and System event is sent. Event severity depends on threshold: • 50-70%—Warning event • 70-80%—Minor event • 80% and above—Major event See Oracle database Disk Usage Alerts, page 8-15, for additional information about this problem.
Check available space in tablespaces	Hourly job that checks whether tablespaces listed in *NETWORKHOME*/Main/scripts/embedded_db/cron/TS_ALERTS.prm. If threshold is exceeded, a new data file is added to tablespace, and an e-mail and System event is sent. Event severity depends on threshold: • 80-90%—Minor event • 90% and above—Major event See Oracle database Tablespace Usage Alerts, page 8-16, for additional information about this problem.
Check Oracle database backup log for errors	Daily job that checks backup logs for errors. Removes logs over 14 days old.
Clean Oracle database log and trace files	Hourly job that removes Oracle database log and trace files more than 31 days old.

Embedded Oracle Database Events and Errors

Prime Network monitors the embedded Oracle database and generates System events when necessary.

Oracle database Disk Usage Alerts

Prime Network will continue to generate events (one hour later, at the next cron job) if the same directory's disk usage surpasses the *next* threshold, or a different directory's disk usage surpasses any threshold. If the disk space is unchanged, no new System events are generated.

If the problem continues:

1. Ask your system administrator to add disk space to the relevant file systems.
2. If more disk space cannot be added, contact the Cisco Technical Assistance Center for information on how to reduce history size. This will not change the disk usage, but will eliminate the need to add disk space.

Oracle database Tablespace Usage Alerts

Note You can change the thresholds by editing the TS_ALERTS.prm file. Prime Network will use the new threshold numbers when it performs the next hourly cron job.

If a tablespace exceeds its capacity, Prime Network will add a new data file to the tablespace. Prime Network will generate an hourly system event until the problem is fixed. If the problem continues, do the following:

1. If you have the required disk space, add data files using the **add_storage_for_tablespace.pl** utility. See Adding Database Files to a Specific Tablespace (add_storage_for_tablespace.pl), page 8-21.
2. Contact the Cisco Technical Assistance Center.

Oracle Errors Monitored by Prime Network

Table 8-6 lists the Oracle errors that are monitored by Prime Network. If you receive any of the following errors, contact the Cisco Technical Assistance Center (TAC).

Table 8-6 Oracle Database Function Error Messages

Error Code and Message	Possible Reason
ORA-00600: internal error code, arguments: [*string*], [*string*], [*string*], [*string*], [*string*], [*string*], [*string*], [*string*]	This is the generic internal error number for Oracle program exceptions. This indicates that a process has encountered an exceptional condition.
ORA-00604: error occurred at recursive SQL level *string*	An error occurred while processing a recursive SQL statement (a statement applying to internal dictionary tables).
ORA-00050: operating system error occurred while obtaining an enqueue	Could not obtain the operating system resources necessary to cover an oracle enqueue. This is normally the result of an operating system user quota that is too low.
ORA-00052: maximum number of enqueue resources (string) *exceeded*	Ran out of enqueue resources.
ORA-00053: maximum number of enqueues exceeded	Ran out of enqueue state objects.
ORA-00055: maximum number of DML locks exceeded	Ran out of DML lock state objects.
ORA-00059: maximum number of DB_FILES exceeded	The value of the DB_FILES initialization parameter was exceeded.
ORA-00060: deadlock detected while waiting for resource	Transactions deadlocked one another while waiting for resources.
ORA-00250: archiver not started	An attempt was made to stop automatic archiving, but the archive process was not running.
ORA-00255: error archiving log string of thread *string*, sequence # *string*	An error occurred during archiving.
ORA-00257: archiver error. Connect internal only, until freed	The archiver process received an error while trying to archive a redo log. If the problem is not resolved soon, the database will stop executing transactions. The most likely cause of this message is the destination device is out of space to store the redo log file.
ORA-01033: ORACLE initialization or shutdown in progress	An attempt was made to log on while Oracle is being started up or shut down.
ORA-01035: ORACLE only available to users with RESTRICTED SESSION privilege	Logins are disallowed because an instance started in restricted mode. Only users with RESTRICTED SESSION system privilege can log on.

Table 8-6 Oracle Database Function Error Messages (continued)

Error Code and Message	Possible Reason
ORA-01110: data file string: (*string*)	Reports the file name. This error accompanies other errors that explain the problem associated with this file.
ORA-01116: error in opening database file (*string*)	At attempt to open a database file failed. Most likely the file is inaccessible. Accompanying errors will provide the file name.
ORA-01520: number of data files to add (*string*) exceeds limit of string	CREATE TABLESPACE statement specifies more files than is permitted for this database.
ORA-01536: space quota exceeded for tablespace '*string*'	The space quota for the segment owner in the tablespace has been exhausted and the operation attempted the creation of a new segment extent in the tablespace.
ORA-01652: unable to extend temp segment by *num* in tablespace *name*	Most likely due to failing to allocate an extent for the temporary segment in the tablespace.
ORA-01659: unable to allocate MINEXTENTS beyond *string* in tablespace *string*	Failed to find sufficient contiguous space to allocate MINEXTENTS for the segment being created.
ORA-27041: Unable to open *file*	An attempt to open a file failed. Check the accompanying error messages for the file name.
ORA-27100: shared memory realm already exists	Tried to start duplicate instances, or tried to restart an instance that had not been properly shut down.
ORA-27102: out of memory	—
ORA-27103: internal error	—
ORA-27146: post/wait initialization failed	OS system call failed.

Stopping, Starting, and Changing Oracle Embedded Database Settings (emdbctl Utility)

Note If you are using gateway server high availability, freeze the cluster services *before* using **emdbctl** with the **stop**, **start**, **restore**, **restore_db**, or **enable_backup** options. These options will stop and restart the cluster services. If the cluster is running and detects that the services are down, it may attempt to restart them. When used with Oracle ADG, reconfigure the Oracle database replication after restoring the primary DB. For more information on replication process, refer to the *Cisco Prime Network 4.2 Gateway High Availability Guide*.

Use the **emdbctl** command to perform embedded Oracle database backup and restore operations, collect logs and reports, and other administrative actions. The **emdbctl** command is located in *NETWORKHOME*/Main/scripts/embedded_db. It takes the following options:

Option	Description	See:
--stop	Stops Prime Network on the gateway and units, and stops the embedded Oracle database services and listener.	This topic for examples.
--start	Starts the embedded Oracle database services and listener, and starts Prime Network on the gateway and units (if the units are down).	
--enable_backup	Enables the automatic backup mechanism.	Enabling Embedded Oracle Database Backups, page 2-11
--backup	Backs up the embedded Oracle database and Prime Network, including the registry.	Backing Up and Restoring Data, page 2-5
--restore	Restores the embedded Oracle database *and* Prime Network, including the registry using valid backup files.	Backing Up and Restoring Data, page 2-5
--restore_db	Restores the embedded Oracle database only.	
--collect	Collects embedded Oracle database logs and reports. It collects logs and trace files from the Oracle database server, runs a diagnostic tool, zips the output together, and copies it to the gateway at *NETWORKHOME*/Main/logs/emdb/ana_collector.zip. It can be run alone or as part of the artifacts of the Profiler Tool (available from the Cisco Developer Network).	n/a
--change_backup_time	Changes the Oracle database backup time.	Changing the Embedded Oracle Database Backup Schedule, page 2-12
--set_smtp_server	Changes the SMTP server for e-mail notifications from the Oracle database.	Changing the SMTP Server for Embedded Oracle Database Notifications, page 8-22
--set_email	Sets the e-mail address for receiving e-mail notifications. Use the following format: **--set_email** *name@domain,name@domain...*	n/a

You must be logged in as *pnuser* to use this command.

The following illustrates how to use the start and stop options:

```
# emdbctl --stop
Stopping Prime Network
Stopping NCCM DM Server...
- DM server is up, about to shut it down
- Sent graceful shutdown command to the dm Server (pid 25499), waiting for 2 seconds
- Checking if DM server is still up (1st)
- The DM Server is down
AVM unregistered successfully
Stopping AVMs.....Done.
Stopping the database and listener
#
# emdbctl --start
```

```
- Starting the database and listener
- Starting MVM.....................................................Done.
- Starting Gateway ...............................................................Done.
```

Retrieving Your Embedded Oracle Database Profile Setting from the Registry

The embedded database represents your deployment's estimated database usage patterns and load. Prime Network uses this information to calculate the maximum size of the Oracle database, data files, temp files, redo logs, and so forth. The following table lists the supported profiles (which are described in detail in the *Cisco Prime Network 4.2 Installation Guide*).

Profile Number	Description
1	1 actionable events per second (POC/LAB deployment)
2	Up to 5 actionable events per second
3	Up to 20 actionable events per second
4	Up to 50 actionable events per second
5	Up to 100 actionable events per second
6	Up to 200 actionable events per second
7	Up to 250 actionable events per second

If you cannot remember what database profile you are using, use this procedure to retrieve the value from the registry.

Step 1 Log into the Prime Network gateway as *pnuser*.

Step 2 Change directories to *NETWORKHOME*/Main and enter the following commands. The first command returns the profile set during installation. The second command will return a value only if you used added disk space using **add_emdb_storage.pl**. If the commands return different database profiles, use the value returned by the first command (the profile you specified during installation).

runRegTool.sh -gs localhost get 127.0.0.1 avm11/services/persistency/general/EmbeddedDataProfile

runRegTool.sh -gs localhost get 127.0.0.1 avm11/services/persistency/general/EmbeddedMemoryProfile

For example:

```
# runRegTool.sh -gs localhost get 127.0.0.1
avm11/services/persistency/general/EmbeddedMemoryProfile
2
# runRegTool.sh -gs localhost get 127.0.0.1
avm11/services/persistency/general/EmbeddedDataProfile
null
```

In this example, the database profile being used is 2 (up to 5 actionable events per second).

Adding Storage to an Embedded Oracle Database

Prime Network provides two utilities for adding additional storage to an embedded Oracle database:

- To add storage to the entire Oracle database, see Adding Database Files to the Embedded Oracle Database (add_emdb_storage.pl), page 8-20.
- To add storage to a specific tablespace, see Adding Database Files to a Specific Tablespace (add_storage_for_tablespace.pl), page 8-21.

Adding Database Files to the Embedded Oracle Database (add_emdb_storage.pl)

Use the **add_emdb_storage.pl** script to add Oracle database files according to the database size you estimate you will need. When you use these scripts you will be prompted to enter your database profile (the estimated database capacity) and the history size for events and workflows. This enables the script to calculate the maximum size of the Oracle database, and to create the data files, temp files, and redo logs.

If you need assistance estimating the Oracle database size, contact your Cisco representative.

Step 1 Log into the Prime Network gateway as *pnuser*.

Step 2 Change directories to *NETWORKHOME*/Main/scripts/embedded_db and enter the following command:

```
# ./add_emdb_storage.pl
```

Step 3 Enter the appropriate response at the prompts:

```
- writing log to /export/home/pn41/Main/logs/emdb/add-storage-1369796303.log
- Retrieving registry information & initializing connection
- The profile used for setting the database is 1 (1 actionable events per
second (POC/LAB deployment)). Do you wish to proceed with this
profile?  (yes,no) [default yes] no
- Select a DB profile
---------------------
1) 1 actionable events per second (POC/LAB deployment)
2) Up to 5 actionable events per second
3) Up to 20 actionable events per second
4) Up to 50 actionable events per second
5) Up to 100 actionable events per second
6) Up to 200 actionable events per second
7) Up to 250 actionable events per second
(1 - 7) [default 1]
- Insert the event archiving size in days. Prime Network default archive is 14 days:
[default 14]
- Required storage for pn41 tablespace: 7168 MB
- Adding 5632 MB for pn41 on /export/home/ana-oracle/oradata/anadb/. This might take a
while
```

Note If you enter incorrect values—such as the wrong Oracle database profile estimate—you can rerun the script with different inputs.

If you encounter any errors, messages similar to the following examples are displayed.

- If there is not enough disk space to create the additional Oracle database files or redo logs:

```
- There isn't enough space on the current disks to create an additional of
        6144 MB.   Please enter a new location for creating the remaining
        DB files. Before you continue:
```

```
        1. Verify user <os-db-user> has writing permissions on the new location
        or run the following command as the OS root user:
        chown -R <os-db-user>:oinstall <path>
        2. Verify the new location is mounted as UFS with 'forcedirectio'
        option

New location:
```

Enter another location.

- If the files or redo logs cannot be created for any reason, you will see an error message and the following prompt:

```
- How would you like to continue?
---------------------------------
1) Retry
2) Skip (move to the next in list)
3) Abort
(1 - 3) [default 1]
```

For example, if the correct permissions were not set, you would see the following.

```
Failed to add datafile for pn41:
-1119: ORA-01119: error in creating database file '/2del/pn41_DATA11.dbf'
ORA-27040: file create error, unable to create file
Linux-x86_64 Error: 13: Permission denied
```

The menu choices provide you with an opportunity to fix the permissions and retry creating the file or log.

The log file is located in *NETWORKHOME*/Main/logs/emdb/add-storage-*time-stamp*.log.

Adding Database Files to a Specific Tablespace (add_storage_for_tablespace.pl)

Use the **add_storage_for_tablespace.pl** script to add Oracle database files to a specific tablespace. If a tablespace exceeds its capacity, Prime Network will add a new data file to the tablespace and generate an hourly system event until the problem is fixed.

The command is located in *NETWORKHOME*/Main/scripts/embedded_db. It takes the following arguments:

add_storage_for_tablespace.pl --tablespace *tablespace_name* **--space** *additional_space_required (MB)* **--location** *location_for_new_files*

The log file is located in *NETWORKHOME*/Main/logs/emdb/add-storage-to_tbs-*timestamp*.log.

Before You Begin

You will need the following information to use this script:

- The name of the tablespace that requires more database files.
- Additional space required for the above tablespace.
- The full directory name where the new database files will be created.

The following examples add 100 MB to the pn41 tablespace located in /export/home/oracle/oradata/anadb. This command performs the operation in one command line:

```
# ./add_storage_for_tablespace.pl --tablespace pn41 --space 100 --location
/export/home/oracle/oradata/anadb/
```

This procedure adds the tablespace using interactive mode:

Step 1 Log into the Prime Network gateway as *pnuser*.

Step 2 Change directories to *NETWORKHOME*/Main/scripts/embedded_db and enter the following command:

```
# ./add_storage_for_tablespace.pl
```

Step 3 Enter the appropriate response at the prompts:

```
This script will add an additional datafile for a certain tablespace in the DB
--------------------------------------------------------------------------------

+Retrieving registry information & initializing connection
+Choose one of the following Prime Network tablespaces to add datafiles to:

TABLESPACE_NAME                FREE_SPACE_MB
-----------------------------  -------------
UNDOTBS1                       1992.25
pn41_XMP                       1009.625
pn41_EP                         928.6875
pn41                            271.8125
pn41_ADMIN                       98.375
SYSAX                            37.375
SYSTEM                            6.75
USERS                             3.6875

- Enter tablespace name: pn41

+Choose one of the following locations for the new datafile/s to be created at:
/export/home/oracle/oradata/anadb/
- Enter location: /export/home/oracle/oradata/anadb/

- Enter the required size in MB (For Example: 1000): 100

+About to add 100 MB to pn41 on /export/home/oracle/oradata/anadb/
Successfully added 100 M on /export/home/oracle/oradata/anadb/ to pn41
```

Changing the SMTP Server for Embedded Oracle Database Notifications

If necessary, you can change the SMTP server for e-mail notifications from the embedded Oracle database using the **emdbctl** command, as shown in this example.

```
# emdbctl --set_smtp_server
Enter your SMTP server IP/Hostname: 1.1.1.1
Verifying connectivity to 1.1.1.1
             Failed to connect to 1.1.1.1 on port 25. Please try again
Enter your SMTP server IP/Hostname: outbound.cisco.com
Verifying connectivity to outbound.cisco.com
Reading Prime Network registry
Updating the SMTP server parameter in the database
Done
```

Responding to Event Floods and Poor System Performance

Prime Network provides two methods for responding to system instability or event floods:

Filter	Description	Default Setting	For more information, see:
Global Event Filter	Controls traps and syslogs that Prime Network drops at different system load levels. (Dropped means they are not forwarded by VNEs for processing.) Raw events are still saved to the Oracle Fault Database.	Enabled (and customizable)	Using the Automatic Overload Prevention Mechanism (Safe Mode) and the Global Event Filter, page 8-23
Cisco Configuration Management Trap Filter	Filters out ciscoConfigManEvent traps using the Noise Filter. These traps are ignored and are not saved to the Oracle Fault Database.	Disabled	Filtering Out ”Pure Noise“ Traps Using the ciscoConfigManEvent Trap Filter, page 8-27

For information on creating other customized noise filters, refer to the Cisco Developer Network.

Using the Automatic Overload Prevention Mechanism (Safe Mode) and the Global Event Filter

Prime Network uses a software mechanism called Automatic Overload Prevention (AOP) to detect and prevent system overload. The AOP service monitors the load produced by components in Prime Network. Similar components, such as those that control fault management, are grouped together into an AOP subsystem. When a subsystem’s processing load becomes heavy, the whole system moves into *safe mode*. Other subsystems respond by adjusting their processing in order to prevent system overload. When this happens, a System event is generated and can be viewed in Prime Network EventVision.

If the subsystem continues to be overloaded, the components will take other measures to lessen the system load (if those measures are configured). As soon as the problematic subsystem returns to a normal load, all other components revert to normal.

The AOP mechanism is currently used by the following subsystems, due to the very large amount of data they process:

- Reporting subsystem.
- Fault subsystem, which includes the Alarm Plugin, Global Event Filter Agent, Event Integrity Agent, and Ticket Agent.

Loads and Running Levels

The AOP service maintains the following information about each component in a subsystem.

Load Indicator	Definition
Current Load	Current processing load. When a component's Current Load changes, other components may respond by changing their Current Loads and/or Running Levels. Supported Current Loads are: • **NORMAL** • **LOAD*x* (safe mode), where *x* is 1-6**
Running Level	The state in which a component is running. Running Levels can change in response to Current Load and/or Running Level changes in other components. Supported Running Levels are: • **NORMAL**, also called Running Level 0. • **AOP***x* or safe mode, where *x* is Running Levels 1-6.

When a problem occurs and a component's load increases, the following can occur, depending on your system configuration:

- The reporting subsystem disabled reports (at AOP 6, by default).
- The Alarm Plugin stops auto-clearing events (at AOP 6, by default).
- The Global Event Filter drops some syslogs and traps (it does this at all AOP levels, and at AOP 6, it drops *all* syslogs and traps).

To specify which events the fault subsystem drops at different running levels, see Configuring the AOP Global Event Filter, page 8-25.

Note Dropping syslogs and traps in this context means that syslogs and traps are not correlated and forwarded to the Fault Agent (AVM 25); syslogs and traps are still sent to the Oracle Fault Database. Also note that *only* syslogs and traps are dropped; Service events and non-network events (Audit, Security, System, and Provisioning events) are *never* dropped by the AOP mechanism.

As soon as the load returns to normal on the problematic component, all components respond by returning to normal and the system moves out of safe mode.

Displaying Current AOP Loads and Running Levels

To display the status of all components that are using AOP:

Step 1 Open an SSH session to the Prime Network gateway server and log in as *pnuser*.

Step 2 Enter the following:

```
# telnet 0 2011
Connected to 0.
Sheer BOS AVM management
AVM11#/>cd aop
AVM11#aop>getAOPStatus
```

```
-------------------------------------------------------------------------------------
---
Subsystem  ComponentId                Load     Running Level  Last Modification Time
-------------------------------------------------------------------------------------
---
FAULT      ALARM_PLUGIN               NORMAL   AOP6           Thu Oct 21 13:20:20 PST
2013
FAULT      EVENT_GLOBAL_FILTER_AGENT  NORMAL   AOP1           Thu Oct 21 13:20:20 PST
2013
FAULT      EVENTINTEGRITY_AGENT       NORMAL   AOP1           Thu Oct 21 13:20:20 PST
2013
FAULT      TICKET_AGENT               LOAD1    NORMAL         Thu Oct 21 13:20:20 PST
2013
REPORTS    REPORTS_AGENT              NORMAL   AOP6           Thu Oct 21 13:20:17 PST
2013
-------------------------------------------------------------------------------------
---
total rows in report: 5
```

Configuring the AOP Global Event Filter

The Event Global Filter has two flavors:

- Filtering when the system is running in NORMAL mode (Running Level 0)
- Filtering when the system is in AOP mode (Running Levels AOP 1-6)

You can define filters for Running Levels 0-5—that is, for NORMAL mode, and for AOP 1-5. At Running Level 6, all traps and syslogs are dropped so no further filtering is useful.

The filter contains a list of rules that define what events should be excluded. Events are assigned a number (1-6), corresponding to the AOP running levels. When the AOP running level is *x*, all events with a number equal to or lesser than *x* are dropped. Note that this is done after events are saved to the Oracle Fault Database.

Use the following procedure to create a new filter. In this procedure you will specify:

- Running level at which to drop the events that match the filter.
- The event information. When matched, the event will be dropped.

To create a new filter, use this procedure. For information on the properties described in the procedure, contact your Cisco customer service representative.

Step 1 Log into the Prime Network gateway server as *pnuser*.

Step 2 Add the new filter information to the registry using the following command.

ID is the AOP running level at which to drop events if they match the filter criteria, and *propertyName* is the event attribute to be checked by the filter:

```
# ./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0
site/event-global-filter/runningLevelID/propertyName
```

propertyName can be any of the following:

Attribute	Description and Supported Values
SeverityEnum	An integer that represents the severity. Supported SeverityEnums are: 1—INFO 2—CLEARED 3—WARNING 4—MINOR 5—MAJOR 6—CRITICAL
Name	An integer that represents the alarm as defined in the alarm-types.xml registry file. For example, 1 represents “Link Down.”
State	Short description of the event, such as “Port down due to card down.”
DetectionType	An integer that represents the event protocol type. Supported DetectionTypes are: 0—Service Event 1—Syslog Event 2—V1 Trap 3—V2 Trap 4—V3 Trap

This command adds a SeverityEnum property value to AOP 1:

```
# ./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0
site/event-global-filter/runningLevel1/SeverityEnum
```

Step 3 Set a value for the event property. Events will be dropped when the property has that value.

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/event-global-filter/runningLevelID/propertyName/propertyValue “”
```

This command sets the SeverityEnum value to 1 in the Global Event Filter:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/event-global-filter/runningLevel1/SeverityEnum/1 “”
```

To remove a filter, use this procedure.

Step 1 Log into the Prime Network gateway server as *pnuser*.

Step 2 Remove the filter from the registry using the following command.

ID is the AOP running level at which to drop events if they match the filter criteria, and *propertyName* is the event attribute to be checked by the filter:

```
# ./runRegTool.sh -gs 127.0.0.1 remove 0.0.0.0
site/event-global-filter/runningLevelID/propertyName “”
```

This command removes the filter created in the previous procedure:

```
# ./runRegTool.sh -gs 127.0.0.1 remove 0.0.0.0
site/event-global-filter/runningLevel1/SeverityEnum ""
```

Filtering Out "Pure Noise" Traps Using the ciscoConfigManEvent Trap Filter

If the system is flooded with ciscoConfigManEvent traps, you can enable a filter that will drop these traps when they are received by Prime Network. This flooding happen if Prime Network repeatedly requests configuration information from devices (for example, by sending **show running config** and **show startup config** commands). When you enable the filter, these traps are completely ignored and are not saved to the Oracle Fault Database.

You can also make a customized noise filter. For information, refer to the Cisco Prime Network Technology Center at https://developer.cisco.com/site/prime-network/.

Caution If you enable the ciscoConfigManEvent Trap Filter, ciscoConfigManEvent traps will *not* be saved to the Oracle Fault Database and will therefore not available for reports.

The basic steps of this procedure are:

1. Check the registry for the location of the first two snmp-processor entries. You will need this information in order to assign the ciscoConfigManEvent Trap Filter a position that will not overwrite any existing entries.
2. Configure the ciscoConfigManEvent Trap Filter processing position. This ensures that after raw events are received and processed by the RawAgentIpSnmpEventProcessor, they are immediately sent to the ciscoConfigManEvent Trap Filter.
3. Enable the ciscoConfigManEvent Trap Filter.
4. Restart the Event Collector AVM (AVM 100).

To configure and enable the Noise Filter:

Step 1 Check the registry position of the first two processors to identify a position for the new filter that will not overwrite an existing entry.

a. Change to the Main directory and run the following commands. The first command checks for any custom changes that have been made, and the second command checks the location for the default settings.

runRegTool.sh localhost get site/trap/agents/trap/processors/snmp-processors| grep position

runRegTool.sh localhost get trap/agents/trap/processors/snmp-processors| grep position

You will see output similar to the following:

```
<entry name="position">10</entry>
<entry name="position">20</entry>
<entry name="position">70</entry>
<entry name="position">60</entry>
<entry name="position">4000</entry>
<entry name="position">40</entry>
<entry name="position">30</entry>
```

```
                    <entry name="position">50</entry>
                    <entry name="position">45</entry>
```

In this example, we would like to put the new filter between 10 and 20, assuming 10 is the RawAgent IpSnmpEventProcessor.

b. Verify which position is assigned to the RawAgentIpSnmpEventProcessor; it is normally position 10 but must be verified.

runRegTool.sh localhost get trap/agents/trap/processors/snmp-processors | more

Continue to hit Return until you reach the entry with position 10. In this example, the RawAgentIpSnmpEventProcessor is in position 10.

```
<key name="processors">
          <key name="snmp-processors">
              <key name="snmp-processor1">
                    <entry
name="class">com.sheer.metrocentral.framework.instrumentation.trap.processor.RawAge
ntIpSnmpEventProcessor</entry>
                           <entry name="description">Extract the IP from the
packet</entry>
                                 <entry name="enable">true</entry>
                                 <entry name="position">10</entry>
                                 <entry name="initial-processor-label">snmp</entry>
                                 <key name="matcher">
                                       <entry
name="class">com.sheer.metrocentral.framework.instrumentation.trap.matcher.IncludeA
llMatcher</entry>
              </key>
           </key>
```

c. If you did not find the RawAgentSnmpEventProcessor, follow the same procedure on the **site** hive:

runRegTool.sh localhost get site/trap/agents/trap/processors/snmp-processors | more

- If the RawAgentSnmpEventProcessor is in position 10, and no other filter configured between position 10 and position 20, assign the ciscoConfigManEvent Trap Filter a position between 11-19.
- If the RawAgentSnmpEventProcessor was moved to a different position, note its location, and assign the ciscoConfigManEvent Trap Filter to the next available position (that follows the RawAgentSnmpEventProcessor).

Step 2 Set the ciscoConfigManEvent Trap Filter location:

runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/trap/agents/trap/processors/snmp-processors/snmp-processor-config-man-filter/position *n*

Using the information from Step 1, the position can be any number from 11-19. This command sets the location to **15**:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/trap/agents/trap/processors/snmp-processors/snmp-processor-config-man-filter/posit
ion 15
```

Step 3 Enable the ciscoConfigManEvent Trap Filter:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/trap/agents/trap/processors/snmp-processors/snmp-processor-config-man-filter/enabl
e true
```

Step 4 Restart the Event Collector AVM (AVM 100).

Tracking Oracle Database and System Integrity Events

The following predefined reports can provide you with important Oracle database statistics for a period of time that you specify. To run any of these reports, select **Reports** from the main menu.

For historical events related to:	See:
Total number of events that occurred during a specified period of time	Fault Database Statistics report (**Reports > Run Report > Events Reports > Fault Database Statistics**)
Number of active and archived events, large tickets, notifications	Database Monitoring report (**Reports > Run Report > Events Reports > Database Monitoring**)
Ticket archiving, dropped events, tablespace problems	Database log files (see Log Files Reference, page C-3) Detailed System Events report (**Reports > Run Report > Events Reports > Detailed Non-Network Events > Detailed System Events**).