CHAPTER 10

Archiving and Purging Data from the Database

These topics provide basic information about data purging and archiving and system stability:

- **Prime Network Database Schemas, page 10-1**, describes the schemas supported by the Prime Network database and the main tables in the Fault Database and Event Archive schemas.
- **Archiving and Purging Data, page 10-4**, describes how the Prime Network integrity service and other mechanisms maintain system stability by checking for and purging old data.

**Note**
If you have installed an embedded database, see Working With an Embedded Database, page 11-1 for additional information on how to administer it.

Prime Network Database Schemas

A Prime Network application operating system account is created when Prime Network is installed. When the database is created, it uses this operating system account name as the default for naming the schemas. **Table 10-1** lists the database schemas that are created by Prime Network. It also provides examples of what the schema names would be if `network-user` was defined as `network38` at installation time. You can also create the schemas manually, using different names, as described in the Cisco Prime Network 3.8 Installation Guide, but the purpose of each schema remains the same.

**Note**
Prime Network stores events in the database in Greenwich Mean Time (GMT). The Prime Network clients convert events to the time zone that is configured on the client’s workstation. As a best practice, use GMT (with 0 offset) on the gateway server.
### Table 10-1  Prime Network Database Schemas

<table>
<thead>
<tr>
<th>Default Schema Names</th>
<th>Description</th>
<th>Example Schema Name</th>
</tr>
</thead>
</table>
| network-user         | Prime Network main schema that contains most Prime Network data. This schema also contains the Fault Database (the tables that are related to the fault application):  
  - Network event tables—NETWORKEVENT, ALARM, and TICKET tables. Each of these tables contain an active partition and an archived partition, and the archived partitions are further divided into time-based subpartitions. Data in these three tables are never deleted; they are archived, either manually or automatically. When archived, the data is moved to an archive subpartition based on the object timestamp, and the data begins aging. When the archive exceeds its history size (14 days by default), the data is deleted.  
  - Non-network event tables—SYSTEMEVENT, AUDITEVENT, SECURITYEVENT, PROVISIONINGEVENT, NEWTRAPEVENT, NEWTRAPVALUE, MONITOR. Non-network tables contain only one time-based partition. Unlike tickets, they do not have lifecycle, so once created and saved, they begin aging. Like the network events tables, when the table exceeds its history size (14 days by default), the data is deleted.  
To change the settings that control when events are purged from the Fault Database, see **Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6**. A special process also purges tickets when the number of tickets exceeds its threshold; see **How Fault Data is Auto-Archived in the Database, page 10-9**. | network38 |
| network-user_ep      | Prime Network Event Archive (event persistence) schema that contains the following tables:  
  - HP_SYSLOG  
  - HP_TRAP  
The network-user_ep schema contains all raw events that are sent from devices to Prime Network. Specifically, these raw events are received by the Event Collector (on AVM 100) and persisted in the Event Archive. The data is arranged in time-based partitions. When a partition’s age exceeds its history size (14 days by default), the data is deleted. You can disable event archiving using the procedure in **Disabling and Re-Enabling Event Archiving, page 14-16**.  
To change the settings that control when events are purged from the Event Archive, see **Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6**. | network38_ep |
| network-user_dwe     | Prime Network Workflow Engine schema that contains all data (templates and workflows) related to the Workflow Engine. The Workflow Engine is described in **Workflow Administration Tasks, page 12-1**.  
Workflows are deleted according to the workflowEngine integrity test; see **Table 10-3 on page 10-6**. | network38_dwe |
Table 10-1  Prime Network Database Schemas (continued)

<table>
<thead>
<tr>
<th>Default Schema Names</th>
<th>Description</th>
<th>Example Schema Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-user_xmp</td>
<td>Prime Network Change and Configuration Management schema that contains all data related to the functions of Change and Configuration Management. This feature is optionally installed with Prime Network and is described in the Cisco Prime Network 3.8 Installation Guide. For more information on Change and Configuration Management, see the Cisco Prime Network 3.8 Change and Configuration Management User Guide.</td>
<td>network38_xmp</td>
</tr>
<tr>
<td>network-user_admin</td>
<td>User with database administrator permissions who can run maintenance tasks—such as gathering statistics—on the other Prime Network 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 database tables. This provides an automatic method for generating database statistics, which is recommended for better performance. For more information, see the Cisco Prime Network 3.8 Installation Guide.</td>
<td>network38_admin</td>
</tr>
</tbody>
</table>

Table 10-2 lists the main tables used by the network-user schema. They are listed here to aid in troubleshooting purposes (for example, if you see any missing statistics messages in the AVM 11 log (NETWORK_HOME/logs/11.out), they could be referring to tables that are no longer used by Prime Network).

Table 10-2  Database Tables in the network-user Schema

<table>
<thead>
<tr>
<th>Primary Tables (Tables with More Traffic)</th>
<th>ALARM</th>
<th>NEWTRAPEVENT</th>
<th>SECURITYEVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AUDITEVENT</td>
<td>NEWTRAPVALUE</td>
<td>SEVERITYASPECT</td>
</tr>
<tr>
<td></td>
<td>NETWORKEVENT</td>
<td>NOTIFICATION</td>
<td>SYSTEMEVENT</td>
</tr>
<tr>
<td></td>
<td>NEWAFFECTEDSNC</td>
<td>PROVISIONINGEVENT</td>
<td>TICKET</td>
</tr>
</tbody>
</table>
Archiving and Purging Data

The Prime Network integrity service and several other mechanisms control how long data is saved and eventually purged (deleted) from the system. For fault data, there is an extra archiving mechanism for saving and tracking older data. These mechanisms are described in the following topics:

- How Data Purging Works, page 10-5
- Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6
- Customizing Purge Settings for Reports, page 10-8
- How Fault Data is Auto-Archived in the Database, page 10-9

If you have installed an embedded database, see Working With an Embedded Database, page 11-1 for information on additional checks that are performed by Prime Network. Data gathered by the Prime Network Monitoring tool is purged after 28 days as described in When Prime Network Monitoring Data is Purged, page 9-18.

**Table 10-2 Database Tables in the network-user Schema (continued)**

<table>
<thead>
<tr>
<th>Tables with Less Traffic</th>
<th>Tables with More Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOSRESULTS</td>
<td>MAP</td>
</tr>
<tr>
<td>BOSUSER</td>
<td>MAPASPECT</td>
</tr>
<tr>
<td>BUSINESSOBJECT</td>
<td>MAPDATAASPECT</td>
</tr>
<tr>
<td>CLIENTREGISTRY</td>
<td>MARTINITUNNELPEER</td>
</tr>
<tr>
<td>CONNECTIONTP</td>
<td>NETWORKPSEUDOWIRE</td>
</tr>
<tr>
<td>CUSTOMER</td>
<td>NETWORKVLAN</td>
</tr>
<tr>
<td>EFPCROSSCONNECT</td>
<td>NOTE</td>
</tr>
<tr>
<td>ETHERNETFLOWDOMAIN</td>
<td>OIDARRAYS</td>
</tr>
<tr>
<td>ETHERNETSERVICE</td>
<td>PASSWORDHISTORYENTRY</td>
</tr>
<tr>
<td>ETHFLOWPOINT</td>
<td>PERMISSION</td>
</tr>
<tr>
<td>EVC</td>
<td>PSEUDOWIREEDGE</td>
</tr>
<tr>
<td>HIERARCHYNODE</td>
<td>PWSWITCHINGENTITY</td>
</tr>
<tr>
<td>LCA</td>
<td>RECONCILIATIONASPECT</td>
</tr>
<tr>
<td></td>
<td>REPORT</td>
</tr>
<tr>
<td></td>
<td>REPORTDATA</td>
</tr>
<tr>
<td></td>
<td>SCOPE</td>
</tr>
<tr>
<td></td>
<td>SERVICE</td>
</tr>
<tr>
<td></td>
<td>SITE</td>
</tr>
<tr>
<td></td>
<td>SWITCHINGENTITY</td>
</tr>
<tr>
<td></td>
<td>VIRTUALROUTER</td>
</tr>
<tr>
<td></td>
<td>VLANPERSISTEDLINK</td>
</tr>
<tr>
<td></td>
<td>VPLSFORWARD</td>
</tr>
<tr>
<td></td>
<td>VPLSINSTANCE</td>
</tr>
<tr>
<td></td>
<td>VPN</td>
</tr>
</tbody>
</table>

For more information on the Event Archive and Fault Database and the flow of events through Prime Network, see Managing the Event Collector (AVM 100), page 14-1. For information on how to change database passwords, see Changing Passwords: Prime Network Database Schemas, page 15-1.
How Data Purging Works

Prime Network maintains system stability by running cron jobs to maintain the 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 network-user. (network-user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network38.)

**Step 2** Use the following command to list the contents of the crontab file for user network-user. 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
```

(The port watchdog script is part of the AVM protection mechanism and is described in AVM 100 and Unit Server High Availability, page 16-3.)

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 10-3 lists the integrity service checks that run on a regular basis to ensure system stability and purge old data. Prime Network performs archives and purges fault data according to the settings described in Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6.

If you have an embedded database, additional purging checks are performed as described in Purging Data and Checking Space on an Embedded Database, page 11-8. These settings are defined in the registry unless otherwise noted.
Chapter 10  Archiving and Purging Data from the Database

Table 10-3  Integrity Tests

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analyze</td>
<td>Generates a System event if the period between the current date and the date each database table was analyzed is larger than the analyze-Period setting. Tables are analyzed every 30 days and includes all database tables. Archiving database logs is also enabled, and Prime Network saves a maximum of 10 database logs.</td>
</tr>
<tr>
<td>backup</td>
<td>Backs up the registry, encryption keys, and crontab files. By default, backups are saved to \textit{NETWORKHOME}/backup. Backups are performed every 12 hours at 4:00 a.m. and 4:00 p.m. (Registry backup settings are described in Backup and Restore, page 8-1.)</td>
</tr>
<tr>
<td>businessObject</td>
<td>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.</td>
</tr>
<tr>
<td>capacity</td>
<td>Checks the disk space capacity and sends alarms. Alarms are sent when the disk capacity reaches 80% and 90%.</td>
</tr>
<tr>
<td>checkDbClock</td>
<td>Ensures that database clock is synchronized with the NTP server.</td>
</tr>
<tr>
<td>mapAspect</td>
<td>Removes mapAspect OIDs which are not connected to any hierarchy.</td>
</tr>
<tr>
<td>oidArrays</td>
<td>Removes OIDs which exist in the OidArrays table, but not in a parent table.</td>
</tr>
<tr>
<td>reports</td>
<td>Deletes reports after 90 days. (This setting is controlled in the Prime Network Administration GUI client; see Customizing Purge Settings for Reports, page 10-8).</td>
</tr>
<tr>
<td>unusableIndexes</td>
<td>Checks for unusable table indexes and, if found, rebuilds them.</td>
</tr>
<tr>
<td>workflowEngine</td>
<td>Deletes all complete workflows after 7 days. For information on Prime Network Activation workflows and when they are deleted, see the \textit{Cisco Prime Network 3.8 Activation User Guide}.</td>
</tr>
</tbody>
</table>

Customizing Archive and Purge Settings for the Fault Database and Event Archive

The Event Management Settings window controls the following settings for both the Fault Database and the Event Archive:

- When archived data is deleted (purged)
- When database partitions are split

Every hour Prime Network monitors the size of tables in the Fault Database, deleting old data and splitting the partitions. These settings are controlled using Global Settings > Event Management Settings.

All database tables contain an active partition and an archived partition. Archived partitions are further divided into time-based subpartitions. When data is archived, it is moved to an archive subpartition. The archive partitioning and data purging is controlled by the settings in this window.

Note To disable saving any raw events to the Event Archive, use the procedure in Disabling and Re-Enabling Event Archiving, page 14-16.

In addition the Inventory Event Viewer settings control when network and provisioning events are removed from the inventory event display Prime Network Vision. This display is launched when a user views a device’s inventory in Prime Network Vision, thus allowing users to see network and provisioning events (and tickets) on devices within their scope. By default, network and provisioning events are
Archiving and Purging Data from the Database

removed from the display after 6 hours, and no more than 15,000 events are displayed. Users can also adjust this setting from their Prime Network Vision GUI client (using Tools > Options in their client). Changes made from the client will override the settings controlled from Prime Network Administration.

<table>
<thead>
<tr>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing these settings can result in immediate and permanent removal of fault data.</td>
</tr>
</tbody>
</table>

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

**Step 2**
Make your desired changes to the following settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault Database</td>
<td>Remove events from database after ____ days</td>
</tr>
<tr>
<td></td>
<td>Number of days after which archived events will be deleted from each archived database partition. The default is 14.</td>
</tr>
<tr>
<td>Database partition size (in hours)</td>
<td>Number of hours after which each database partition will be split. The default is 1 hour. (For database sizing guidelines and other capacity planning information, contact your Cisco account representative.)</td>
</tr>
<tr>
<td>Event Archive</td>
<td>Remove events from database after ____ days</td>
</tr>
<tr>
<td></td>
<td>Number of days after which archived events will be deleted from each archived database partition. The default is 14. To disable saving any raw events to the Event Archive, set this to 0 days.</td>
</tr>
<tr>
<td>Database partition size (in hours)</td>
<td>Number of hours after which each database partition will be split. The default is 1 hour. (For database sizing guidelines and other capacity planning information, contact your Cisco account representative.)</td>
</tr>
<tr>
<td>Inventory Event Viewer</td>
<td>Maximum history size (in hours)</td>
</tr>
<tr>
<td></td>
<td>Number of hours after which network and provisioning events are removed from the inventory event viewer in Prime Network Vision. The default is 6 hours. These settings are overridden if a user makes local changes to their Prime Network Vision GUI client (using Tools &gt; Options in their client).</td>
</tr>
</tbody>
</table>

**Step 3**
Click **Apply**. The changes will take effect in the next partitioning process execution (which is done once an hour).

For information about the main menu that is displayed in the Prime Network window, see Event Management Settings Window, page 1-18.
Customizing Purge Settings for Reports

You can run different types of reports from the Prime Network window using the Reports main menu. This feature is described in the Cisco Prime Network 3.8 User Guide. The Report Settings page in the Global Settings drawer controls:

- When reports should be purged. Reports are saved 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge Report After</td>
<td>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.</td>
</tr>
<tr>
<td>Store Reports Up to</td>
<td>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.</td>
</tr>
</tbody>
</table>

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**
Check or uncheck the Enable Shared Reports check box to specify 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.

For information about the main menu that is displayed in the Prime Network window, see Report Settings Window, page 1-24.

How Fault Data is Auto-Archived in the Database

The NETWORKEVENT, ALARM, and TICKET database tables—that is, the tables that contain the events, alarms, and tickets that are in the Fault Database—each contain an active partition and an archived partition. The archived partitions further divided into time-based subpartitions. The archive operation moves data to an archive subpartition. Archived data is purged after 14 days, according to the setting in Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6.

Auto-Archiving of Cleared Tickets

Prime Network automatically archives cleared tickets which have not changed in the last hour. This setting is controlled in the registry.

Note All changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoArchivingTimeout</td>
<td>Remove Cleared tickets that have not changed in this period of time (in milliseconds).</td>
<td>3600000 (1 hour)</td>
</tr>
</tbody>
</table>

Step 1 Log into the gateway as network-user and change to the Main directory by entering the following command. (network-user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network38.)

```
# 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 AVM 11 using networkctl.

Auto-Archiving Fault Data Based on the Number of Tickets

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

- When the total number of tickets in the Fault Database exceeds 12,800, it generates a System event.
- When the total number of tickets in the Fault Database exceeds 16,000, it archives tickets in groups of 400.
Archiving and Purging Data

Table 10-5 shows the registry parameters that control this type of Fault Database purging.

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ticketRedThresholdAmount</td>
<td>When the number of open tickets surpasses this amount, archive the number of tickets specified by ticketArchivingBulk.</td>
<td>16000</td>
</tr>
<tr>
<td>ticketYellowThresholdPercentage</td>
<td>When the number of open tickets surpasses this percentage of ticketRedThresholdAmount, generate a system message.</td>
<td>80</td>
</tr>
<tr>
<td>wakeUpMessageInterval</td>
<td>Interval for checking the number of open tickets (in milliseconds).</td>
<td>60000 (1 minute)</td>
</tr>
<tr>
<td>ticketArchivingBulk</td>
<td>Alarm is generated once it crosses upper threshold after this many polling cycles.</td>
<td>400</td>
</tr>
</tbody>
</table>

If you have installed an embedded database, see the additional topics in Working With an Embedded Database, page 11-1.

Auto-Archiving Fault Data Based on the Size of Tickets

Every five minutes, Prime Network checks the Fault Database to see if it contains any large tickets that should be archived. A ticket is considered large if it has more than 150 events associated with an alarm. 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 the agent finds more than 1500 large tickets then it will also send a system event notifying about it.

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

Table 10-6 shows the registry parameters that control this type of Fault Database purging.

Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

For information on the format of the runRegTool.sh script, see Changing Registry Settings Using runRegTool.sh, page C-2.
Table 10-6    Registry Settings for Purging Large Tickets From the Fault Database

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>findLargeTicketsMessageInterval</td>
<td>Interval for searching for large tickets (in minutes).</td>
<td>5</td>
</tr>
<tr>
<td>maxTicketSize</td>
<td>When the number of events associated with an alarm surpasses this number, consider it a large ticket and generate a System event.</td>
<td>150</td>
</tr>
<tr>
<td>autoRemoveTimeInterval</td>
<td>Interval at which to archive a large ticket (in minutes) after sending System event.</td>
<td>15</td>
</tr>
<tr>
<td>oversizedTicketAmountLimit</td>
<td>When the number of large tickets surpasses this number, generate a System event.</td>
<td>1500</td>
</tr>
</tbody>
</table>

If you have installed an embedded database, see the additional topics in Working With an Embedded Database, page 11-1.