Chapter 13

Configuring the JPS on a Solaris Platform

This chapter describes how to configure the Juniper Policy Server (JPS), a component of the SRC software that acts as a policy server in the PacketCable Multimedia Specification (PCMM) environment, on a Solaris platform using the SRC configuration applications that run only on Solaris platforms.

You can also use the CLI that runs on Solaris platforms and the C-series platforms to configure the JPS. See *Chapter 12, Configuring the JPS with the SRC CLI*.

This chapter contains the following topics:

For more information about the JPS, see *Chapter 11, Using PCMM Policy Servers*.

Installing the JPS

Before you use the JPS for the first time:

1. Deploy an SRC-managed PCMM network.

   For more information about PCMM and the SRC software, see *Chapter 4, Providing Premium Services in a PCMM Environment*.

2. Install the UMCjps package.

   pkgadd -d /cdrom/cdrom0/solaris UMCjps

   For information about installing Solaris packages, see *SRC-PE Getting Started Guide, Chapter 28, Installing the SRC Software on a Solaris Platform*.

3. Apply the local configuration on the host.

   /opt/UMC/jps/etc/config -a

   This command examines the local machine environment, customizes the *etc/jps.in* and *etc/jpsroot.in* files, and installs the customized files as the *etc/jps* and *etc/jpsroot* files.

NOTE: You must apply the local configuration once after installing the JPS.

If you want to configure the JPS to send time change events to the RKS, apply the local configuration using the command described in *Configuring the JPS for Time Change Event Notification* on page 134.

Configuring the JPS for Time Change Event Notification

PCMM-compliant policy servers send time change events to the RKS. You can configure the JPS to send time change events to the RKS by using the Network Time Protocol (NTP) to synchronize time with the local clock.

NOTE: Configuring NTP on the system may interfere with all other time-sensitive components on the system. We recommend that you configure NTP only if the JPS is running on the system by itself.

To configure the JPS to send time change events to the RKS:

1. On the JPS host, log in as `root`.

2. Configure the NTP servers.

   /opt/UMC/jps/etc/config -a -t <ntpServer>,<ntpServer>

   where ntpServer is the DNS name or IP address of an NTP server accessible from the JPS host. Use a comma to separate each NTP server if you specify more than one.

   This command schedules an NTP cron job every 10 minutes to synchronize the local clock for the JPS with the NTP servers. The JPS sends the time change event to the RKS if the local clock changes during synchronization.

Modifying the Local Clock

If you have configured NTP servers for the JPS by using the procedure described in *Configuring the JPS for Time Change Event Notification* on page 134, do not modify the time for the local clock by using the standard **date** command.

To modify the local clock:

1. On the JPS host, log in as `root`.
2. Modify the time for the local clock.

   /opt/UMC/jps/etc/jpsDate [<MMDDhhmm>[[<CC>]<YY>][.<ss>]]

   where MM indicates the month, DD indicates the day, hh indicates the hour, mm indicates the minute, CC indicates the century minus one, YY indicates the last 2 digits of the year, and ss indicates the second.

   The month, day, year, and century may be omitted; the current values are applied as defaults.

   For example, the following entry sets the date to Oct 8, 12:45 AM:

   /opt/UMC/jps/etc/jpsDate 10080045

   The current year is the default because no year is supplied.

Starting and Managing the JPS

After you have installed the JPS and applied the local configuration of the JPS, you can perform these tasks:

- Starting the JPS on page 135
- Restarting the JPS on page 136
- Stopping the JPS on page 136
- Displaying JPS Status on page 136

To modify the JPS configuration, see *Configuring the JPS* on page 137. To monitor the JPS configuration, see *Monitoring the JPS* on page 145.

Starting the JPS

You must start the JPS when you install the JPS without rebooting the JPS host.

To start the JPS:

1. On the JPS host, log in as `root` or as an authorized nonroot admin user.
2. Start the JPS from its installation directory.

   For root user: **/opt/UMC/jps/etc/jps start**

   For nonroot user: **/opt/UMC/jps/etc/jpsroot start**

   The system responds with a start message. If the JPS is already running, the system responds with a warning message.

Restarting the JPS

To restart the JPS:

1. On the JPS host, log in as `root` or as an authorized nonroot admin user.
2. Restart the JPS from its installation directory.

   For root user: **/opt/UMC/jps/etc/jps restart**

   For nonroot user: **/opt/UMC/jps/etc/jpsroot restart**

   The system responds with a start message. If the JPS is already running, the system responds with a shutdown message and then a start message.

Stopping the JPS

To stop the JPS:

1. On the JPS host, log in as `root` or as an authorized nonroot admin user.
2. Stop the JPS from its installation directory.

   For root user: **/opt/UMC/jps/etc/jps stop**

   For nonroot user: **/opt/UMC/jps/etc/jpsroot stop**

   The system responds with a shutdown message. If the JPS is not running when you issue the command, the system responds with the command prompt.

To start the JPS, see *Starting the JPS* on page 135.

Displaying JPS Status

To display the JPS status:

1. On the JPS host, log in as `root` or as an authorized nonroot admin user.
2. Display the status from the JPS installation directory.

   For root user: **/opt/UMC/jps/etc/jps status**

   For nonroot user: **/opt/UMC/jps/etc/jpsroot status**

   The system responds with a status message.

Configuring the JPS

You can configure and manage the JPS by using the SRC CLI that runs on Solaris platforms and the C-series platforms. See *Chapter 12, Configuring the JPS with the SRC CLI*.

The tasks to configure the JPS for a cable network environment are:

1. Configuring the JPS on page 111
2. Modifying the Subscriber Configuration on page 124

In addition to configuring the JPS, you might need to perform these tasks:

1. Configuring the SAE to Interact with the JPS on page 125

   You can also use SRC configuration applications to perform this task. See Configuring the SAE to Interact with the JPS on Solaris Platforms on page 137.

2. Using the NIC Resolver on page 130

Configuring the SAE to Interact with the JPS on Solaris Platforms

You must configure the SAE as an application manager to allow it to interact with PCMM-compliant policy servers. The policy server acts as a policy decision point that manages the relationships between application managers and CMTS devices. Policy servers that manage the same group of CMTS devices are grouped together and are simultaneously active. The policy server group provides a way for the SAE to communicate with any CMTS device that is managed by a policy server in the policy server group. To provide redundancy, the SAEs are grouped in an SAE community that connects to a policy server group. Only one of the SAEs in the SAE community is active. The active SAE establishes connections to all the policy servers in the policy server group. The active SAE will fail over to a redundant SAE only when it loses the connection to all the policy servers in the policy server group. State synchronization enables the SAE to synchronize its state with all the CMTS devices connected to a policy server group.

The tasks to configure the SAE as an application manager are:

- Specifying Application Managers for the Policy Server on page 138
- Specifying Application Manager Identifiers for Policy Servers on page 141
- Adding Objects for Policy Servers to the Directory on page 142
- Configuring Initialization Scripts on page 143
- Enabling State Synchronization on page 144

Specifying Application Managers for the Policy Server

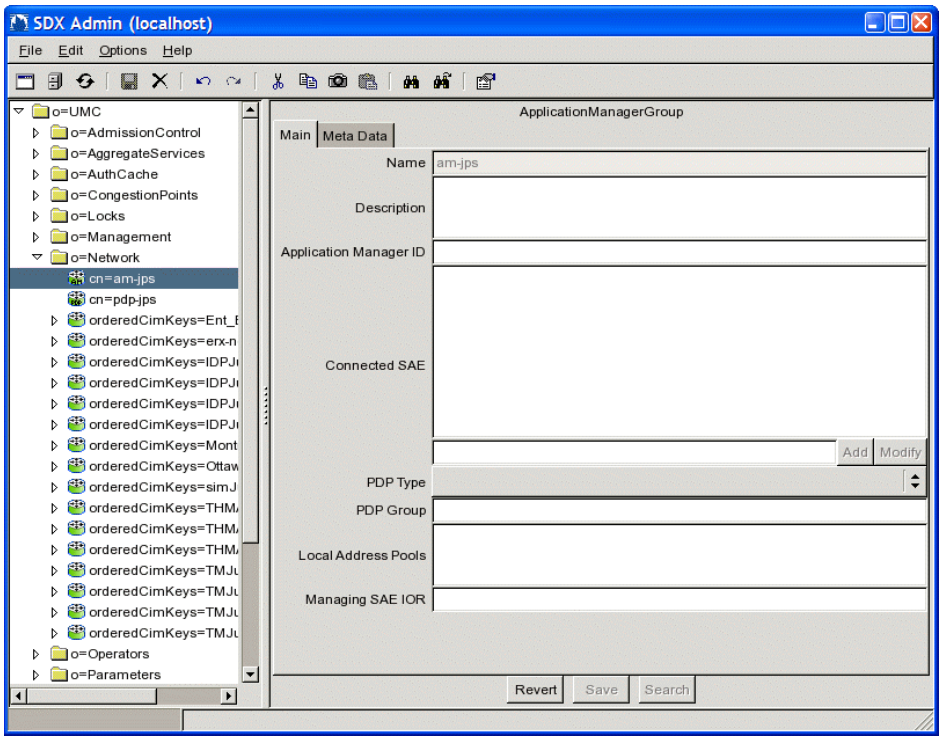
To specify the SAE community that connects to a policy server group, you need to add an application manager group object to the directory.

To add an application manager group with SDX Admin:

1. In the navigation pane, highlight *o = Network*, and right-click.
2. Select **New > ApplicationManagerGroup**.

   The New ApplicationManagerGroup dialog box appears.
3. In the New ApplicationManagerGroup dialog box, enter the name of the application manager group, and click **OK**.

   The name of the group appears in the navigation pane, and information about the group appears in the ApplicationManagerGroup pane.



4. Configure the parameters in the Main tab.
5. Click **Save** in the ApplicationManagerGroup pane.

Description

- Specifies information about the SAE community; keywords that the SDX Admin find utility uses.
- Value—Text string
- Default—No value

Application Manager Tag

- Unique identifier within the domain of the service provider for the application manager that handles the service session; used to specify the application manager identifier (AMID) that is included in all messages sent to and from the policy server.
- Value—2-byte unsigned integer
- Guidelines—This property is required.

  The SAE constructs the AMID value by concatenating two fields: Application Manager Tag and Application Type. The Application Type value is obtained from a service during activation. For more information about the Application Type field, see *Specifying Application Manager Identifiers for Policy Servers* on page 141.

- Default—No value

Connected SAE

- SAEs that are connected to the specified policy server group (PDP Group). This list becomes the community of SAEs.
- Value—IP address or hostname
- Guidelines—This property is required. When you modify a community, wait for passive session stores of the new community members to be updated before you shut down the current active SAE. Otherwise, a failover from the current active SAE to the new member is triggered immediately, and the new member's session store may not have received all data from the active SAE's session store.
- Default—No value

PDP Type

- Type of device that this directory object will be used to manage.
- Value—For the JPS, enter the value PCMM.

  If you do not fill in this field, the device driver ignores this application manager group.

- Default—No value

PDP Group

- Name of the policy server group associated with this SAE community.
- Value—Text string
- Guidelines—This property is required.
- Default—No value

Local Address Pools

- List of IP address pools that the specified PDP group currently manages and stores. You must configure a local address pool if you are using the NIC so that the NIC can resolve the IP-to-SAE mapping. See *Using the NIC Resolver* on page 130.
- Value—List of IP address pools. You can specify an unlimited number of IP address pools. You can specify either the first and last addresses in a range, or you can specify a subnet address, a subnet mask, and a list of addresses to exclude from the subnet.

  The IP pool syntax has the following format:

  ([< ipAddressStart > < ipAddressEnd >] |
  { < ipBaseAddress > /(< mask > | < digitNumber >)(, < ipAddressExclude >)* })

  - < ipAddressStart > —First IP address (version 4 or 6) in a range
  - < ipAddressEnd > —Last IP address (version 4 or 6) in a range
  - < ipBaseAddress > —Network base address
  - < mask > —Subnet mask
  - < digitNumber > —Integer specifying the length of the subnet mask
  - < ipAddressExclude > —List of IP addresses to be excluded from the subnet
  - |—Choice of expression; choose either the expression to the left or the expression to the right of this symbol
  - *—Zero or more instances of the preceding group

  You can use spaces in the syntax only to separate the first and last explicit IP addresses in a range.
- Default—No value
- Example—([10.10.10.5 10.10.10.250] {10.20.20.0/24})

Managing SAE IOR

- Common Object Request Broker Architecture (CORBA) reference for the SAE managing this policy server group.
- Value—One of the following items:
  - The actual CORBA reference for the SAE
  - The absolute path to the interoperable object reference (IOR) file
  - A corbaloc URL in the form corbaloc:: < host > :8801/SAE
    - < host > —Name or IP address of the SAE host

- Guidelines—The **amIorPublisher** script provides this information when the SAE connects to the policy server. If you do not select this script when configuring initialization scripts, enter a value in this field. For information about configuring initialization scripts, see *Configuring Initialization Scripts* on page 143.
- Default—No value
- Example—One of the following items:
  - Absolute path— */opt/UMC/sae/var/run/sae.ior*
  - corbaloc URL—boston:8801/sae
  - Actual IOR—IOR:000000000000002438444C3A736D67742E6A756E697...

Specifying Application Manager Identifiers for Policy Servers

To configure the AMID so that the application manager (such as the SAE) can be identified in messages sent to and from the policy server, the SAE constructs the AMID value by concatenating two fields: Application Manager Tag and Application Type. The Application Manager Tag value is obtained from the specification of application managers for policy servers. The Application Type value is obtained during service activation from the specification of the PCMM Application Type value when you configure normal services. For more information about configuring services, see *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

PCMM Application Type

- Unique identifier within the domain of the service provider for the application associated with a gate; used to specify the AMID that is included in all messages sent to and from the policy server.
- Value—2-byte unsigned integer
  - 0—No defined application association
  - Other values—Application Type
- Guidelines—This property is required.

  The SAE constructs the AMID value by concatenating two fields: Application Manager Tag and PCMM Application Type. For more information about the Application Manager Tag field, see *Specifying Application Managers for the Policy Server* on page 138.
- Default—No value

Adding Objects for Policy Servers to the Directory

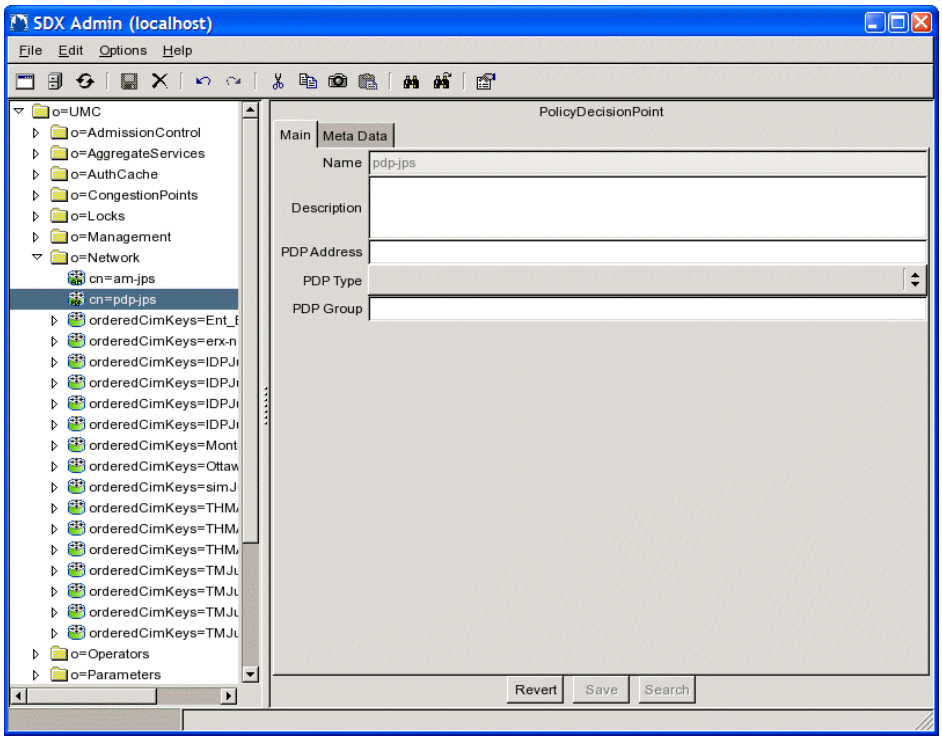
To communicate with policy servers, the SAE creates and manages pseudointerfaces that it associates with a policy decision point object in the directory. Each policy server in the SRC network must appear in the directory as a policy decision point object.

To add a policy server to the directory with SDX Admin:

1. In the navigation pane, select *o = Network*, and right-click.
2. Select **New > PolicyDecisionPoint**.

   The New PolicyDecisionPoint dialog box appears.
3. In the New PolicyDecisionPoint dialog box, enter the name of the policy server, and click **OK**.

   The name of the policy server appears in the navigation pane, and information about the policy server appears in the PolicyDecisionPoint pane.



4. Set the parameters in the Main tab of the PolicyDecisionPoint pane.
5. Click **Save** in the PolicyDecisionPoint pane.
6. Create an SAE community for the policy servers. See *Specifying Application Managers for the Policy Server* on page 138.

Description

- Information about this policy server; keywords that the SDX Admin find utility uses.
- Value—Text string
- Default—No value

PDP Address

- IP address of the policy server. The SAE uses this address to establish a COPS connection with the policy server.
- Value—IP address
- Guidelines—This property is required.
- Default—No value

PDP Type

- Type of device that this directory object will be used to manage.
- Value—For the JPS, enter the value PCMM.

  If you do not fill in this field, the device driver ignores this policy server.
- Default—No value

PDP Group

- Name of the policy server group.
- Value—Text string
- Guidelines—This property is required.
- Default—No value

Configuring Initialization Scripts

When the SAE establishes a connection with a policy server, it runs an initialization script to customize the setup of the connection.

To use SDX Configuration Editor to configure initialization scripts for the SAE:

1. In the navigation pane, select the SAE object for which you want to configure an initialization script.
2. Select the Router tab.

   The Router pane appears.
3. In the Router Scripts area of the Router pane, enter the name of the initialization script in the PCMM Script property.

PCMM Script

- Initialization script for a PCMM environment. The script is run when the connection between a policy server and the SAE is established and again when the connection is dropped.
- Value—Name of a script
- Default—amIorPublisher
- Property name—Router.script.pcmm

Enabling State Synchronization

State synchronization is achieved when the SAE is required to communicate with the policy server over the COPS connection. To enable state synchronization with policy servers, you can specify these properties for the PCMM device driver in the Router tab of SDX Configuration Editor.

Disable Full Sync

- When the SAE is deployed with PCMM policy servers, specifies whether state synchronization with the PCMM policy servers is enabled or disabled.
- Value
  - true—Disables state synchronization
  - false—Enables state synchronization
- Guidelines—When using other PCMM-compliant policy servers (instead of the JPS), we recommend setting this value to true.
- Default—false
- Property name—Router.pcmm.disableStateSync

Disable I03 Policy

- When the SAE is deployed with pre-PCMM I03 CMTS devices, disable the PCMM I03 policies by setting this property to true.
- Value
  - true—Disables PCMM I03-compliant policy
  - false—Enables PCMM I03-compliant policy
- Guidelines—When there are pre-PCMM I03 CMTS devices in the network, you must set this value to true.
- Default—true
- Property name—Router.pcmm.disableI03policy

Session Recovery Retry Interval

- Time interval between attempts by the SAE to restore service sessions that are still being recovered in the background when state synchronization completes with a state-data-incomplete error. The SAE attempts to restore a service session if it receives a service modification or deactivation request for an unrecovered service session before the next interval.
- Value—Number of milliseconds in the range 0–2147483647

- Guidelines—We recommend setting this value to 3600000 (1 hour) or longer.
- Default—3600000
- Property name—Router.pcmm.backgroundSessionRecovery.retryInterval

Monitoring the JPS

You can use the SRC CLI or the C-Web interface to monitor:

- The basic health indicators for the server process
- The current state of the JPS, such as the current network connections or recent performance statistics

For information about using the SRC CLI to monitor the JPS, see *Chapter 14, Monitoring the JPS with the SRC CLI*.

For information about using the C-Web interface to monitor the JPS, see *Chapter 15, Monitoring the JPS with the C-Web Interface*.