



proNX Service Manager Installation and Administration Guide

Release

7.8



Modified: 2019-02-22

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

proNX Service Manager Installation and Administration Guide
7.8
Copyright © 2019 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Creating a Service Request with JTAC	xiii
Chapter 1	proNX Service Manager	15
	About PSM	15
	PSM Client	15
	PSM Dashboard	15
	PSM Server	15
	Red Hat (CentOS) Linux	16
	Support for RADIUS Server	16
	PSM Overview	16
	Running with Multiple Servers	17
	Overview	17
	Running Multiple Servers Without Server Replication	18
	Running Multiple Servers with Server Replication	18
	PSM Networking Considerations	19
	PSM Port Usage	20
Chapter 2	proNX Service Manager System Requirements	27
	PSM Server Requirements	27
	Software Requirements	27
	Hardware Requirements	27
	Network Element Limitations	28
	PSM Client Requirements	28
	Software Requirements	29
	Hardware Requirements	30
	Terminal Server Incremental Memory Requirements	30
Chapter 3	Installing the proNX Service Manager and Related Tasks	33
	Before You Install PSM Software	33
	About RPM	34
	Installing the PSM Server	34
	Upgrading the PSM Server	37
	Using Monit and Other Commands	40
	Installing the PSM Client Using the Wizard	41
	Installing the PSM Client Manually	43
	Upgrading the PSM Client	43

	Enabling Multiuser Access to the PSM Client on a Windows 2008 Server	44
	Configuring the PSM Server for a 32-bit Windows Client	44
	Starting the PSM Client	45
	Verifying PSM Client-server Connectivity	48
	Stopping the PSM Server	48
	Uninstalling the PSM Server	48
	Uninstalling the PSM Client	49
	Restoring the PSM Server Database from a Backup	49
	Reinitializing the PSM Server Database	51
Chapter 4	proNX Service Manager Administrator Tasks	53
	Changing the PSM Properties File	53
	Considerations When Adding an FTP or SFTP Server	54
	Updating the List Of Known Hosts on the PSM Server Machine	54
	Configuring Automated NE Database-backup Operations	55
	RADIUS on PSM	57
	Configuring PSM to Use a RADIUS Server	59
	Configuring Network Elements to Use the Local RADIUS Server	61
	Configuring Scheduled Historical PM Collection	64
	Configuring NE Log Collection	66
	Configuring PSM Alarm Severities	68
	Configuring PSM to E-mail NE Alarms	69
	Configuring Server Replication	70
	Stopping and Starting the PSM Server Application	72
	Configuring Automatic MIP Creation on the BTI810 Network Elements	72
	Configuring Ethernet Services Path Selection Through Non-ERPS Nodes	73
Chapter 5	Appendix	75
	Migrating the PSM Database to a New Server	75
	Example: Scheduling Using Quartz CronTrigger Format	76
	Using Git to Track override-common.properties	77
	Example: Using Fsck to Check and Repair a Filesystem	79
	Installing and Configuring Red Hat (CentOS) Linux	81
	Before You Install Red Hat (CentOS) Linux	81
	Running with a Proxy Server	82
	Installing and Configuring Red Hat (CentOS) Linux, 64-bit, for the PSM Server	82
	Time Zones	90

List of Figures

Chapter 1	proNX Service Manager	15
	Figure 1: PSM Managed Network	17
	Figure 2: Typical Network Deployment	19

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Chapter 1	proNX Service Manager	15
	Table 3: Port Usage in PSM Client to PSM Server Communications	21
	Table 4: Port Usage in PSM Server to PSM Server Communications	21
	Table 5: Port Usage in PSM Server to Network Element Communications	22
	Table 6: Port Usage in PSM Client to Network Element Communications (includes proNX 900 Running on the Client Machine)	23
	Table 7: Port Usage in PSM Server to Network Operations Center Communications	23
	Table 8: PSM Server to External RADIUS Server Communications	24
	Table 9: PSM Server to Other Hosts	24
	Table 10: BTI7800 Port Usage	24
Chapter 2	proNX Service Manager System Requirements	27
	Table 11: PSM Server Software Requirements	27
	Table 12: PSM Server Mandatory Specifications	28
	Table 13: PSM Server Typical Configurations	28
	Table 14: PSM Client Software Requirements	29
	Table 15: PSM Client Hardware Requirements	30

About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

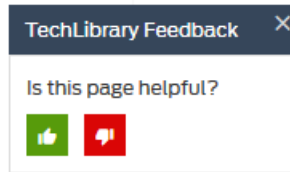
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

CHAPTER 1

proNX Service Manager

- [About PSM on page 15](#)
- [PSM Overview on page 16](#)
- [Running with Multiple Servers on page 17](#)
- [PSM Networking Considerations on page 19](#)

About PSM

The proNX Service Manager (PSM) provides comprehensive service provisioning, monitoring, and troubleshooting tools to allow you to efficiently manage network resources in a packet optical network. With its service-centric focus, PSM simplifies network operations and increases operational efficiency in tasks such as visualization and activation of services to troubleshooting and supporting end customers.

PSM is Java-based and uses a client-server architecture.

PSM Client

The PSM client is a Java-based GUI that communicates with the PSM server using an HTTPS-based protocol to provide the full functionality of the proNX Service Manager. The PSM client software runs on the desktop or laptop of the technician or NOC staff.

PSM Dashboard

The PSM Dashboard is a thin HTTPS Web-based client that is used to provide a quick view of the health of the managed network. It offers a subset of the functionality of the PSM client and runs on the desktop or laptop of the technician or NOC staff. The PSM Dashboard runs on supported browsers and does not require client software. For more information on the PSM Dashboard, see the *proNX Service Manager Dashboard User Guide*.

PSM Server

The PSM server communicates with network elements using SNMP or NETCONF and runs on Red Hat (CentOS) Linux on standard x86-64 servers. PSM clients and PSM Dashboard users connect to the PSM server to manage the network elements in the network.

The number of clients and nodes supported is determined by the hardware, and a calculator is available to determine the correct hardware for specific deployments.

The PSM server has the following components:

- One or more Java-based processes (depending on the performance requirements of the platform)
- MySQL database (automatically backed up daily)

Red Hat (CentOS) Linux

The PSM server is supported on Red Hat (CentOS) Linux. To facilitate configuration of the operating system, the PSM ISO includes a setup script that configures Red Hat (CentOS) Linux and installs the software packages required by the PSM server. For information on how to use this setup script to configure Red Hat (CentOS) Linux, see [“Installing and Configuring Red Hat \(CentOS\) Linux” on page 81](#).

Support for RADIUS Server

Included in the PSM server software package is a local instance of a RADIUS server implementation. When PSM is installed, the PSM server is configured by default to use this local RADIUS server to provide authentication and authorization mechanisms for access to PSM features.

PSM Overview

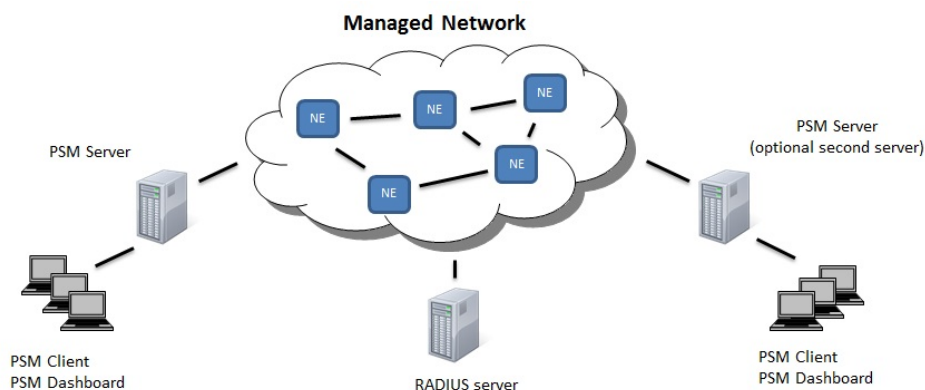
The PSM server manages network elements using SNMP and NETCONF. The PSM client and the PSM Dashboard provide you with the user interface to interact with the PSM server.

In the PSM paradigm, network element configuration data resides solely on the network elements themselves. The PSM server does not keep a separate network element configuration database. This absence of a centralized database allows PSM to achieve better scaling and better concurrency.

When management systems operate directly on configuration data stored on the network elements, there is added assurance that the data is accurate and up to date. Because there is only one set of data, issues with synchronizing an external copy of the data with the actual data on the network element do not exist. Furthermore, since the actual data is manipulated directly, it is a simple matter for the management software to detect and handle situations where multiple users attempt to make conflicting changes, regardless of whether the conflicting users are using the CLI, a separate nodal manager, or other PSM servers.

[Figure 1 on page 17](#) shows a network managed by two PSM servers and multiple clients, along with an external RADIUS server.

Figure 1: PSM Managed Network



When a server comes up, it registers itself as a trap listener on all network elements it is told to discover. It then receives traps from, and reports on, these network elements, and draws topology and discovers services based on configuration and operational data it reads from these network elements. This information is then made available to PSM clients that log in to this server. Clients logging in to a different server might see different network elements altogether, depending on what this other server is configured to discover.

Running with Multiple Servers

- [Overview on page 17](#)
- [Running Multiple Servers Without Server Replication on page 18](#)
- [Running Multiple Servers with Server Replication on page 18](#)

Overview

To provide a level of redundancy, PSM supports the use of multiple servers to manage a network.

In a multi-server configuration, each server receives traps from, and reports on, the network elements that it has discovered. The set of discovered network elements can be the same or can be different from server to server, depending purely on how you choose to divide your network for management. The servers can be geographically distinct for better disaster recovery or be part of a geographically-based management scheme.



NOTE: Some BTI Series network elements have limits on the number of PSM servers that can be used to manage them. See [“PSM Server Requirements” on page 27](#) for details.

Since the servers operate directly on configuration data stored on the network elements themselves, each server has the latest view, and is able to detect and recover from conflicts (in the unlikely event that two or more servers are changing the same set of attributes on the same network element).

While the PSM server does not store network element configuration data, it does store configuration data associated with the PSM server itself. This PSM configuration data relates to user interface interactions and the presentation of information, and includes the following:

- users for the server
- the list of network elements to discover and domain/group membership, which relate to what network elements to manage and how they are organized
- alarm assignment/acknowledgment and maintenance modes, which relate to management actions that a user can take
- customer details and association, which can be optionally defined and associated with services
- profiles, which are network-wide to provide consistency across network elements
- various options related to the display of data, the locations of tools, and other attributes specific to the server

The PSM server stores this set of information in the local MySQL database, which is set up and initialized during the PSM server installation process, and which persists through PSM server software upgrades.

How this data behaves when you run with multiple servers depends on whether you choose to run these servers independently (without server replication), or loosely coupled (with server replication).

Running Multiple Servers Without Server Replication

When you run multiple servers without server replication, each server is unaware of the other servers, and each has its own set of PSM configuration data.

The PSM configuration data that resides on the PSM server is not replicated nor synchronized with the PSM configuration data on the other servers.

For example, network element groups created on one server are not visible to the other servers, alarm assignment on one server is not visible to the other servers, and so forth.

With this approach, while you still achieve redundancy, you might have to recreate and/or reconcile your PSM configuration data when a server goes down.

Running Multiple Servers with Server Replication

When you run multiple servers with server replication, some of the PSM configuration data is synchronized among all servers within the same server replication cluster. This data subset is called the replicated data.

Updates to the replicated data on one server are automatically conveyed to all other servers in the same cluster. For example, a network element group created on one server automatically appears on the other servers, an alarm assignment on one server automatically appears on the other servers, and so forth. In this way, when a server goes down, you can simply log in to another server and continue working.

When enabling server replication on a server, you must explicitly specify the list of servers that belong to the same server replication cluster. A server replication cluster is a group of servers whose replicated data is synchronized among all its members. Not all servers in the network need to belong to the same server replication cluster. You can have more than one server replication cluster in the network.

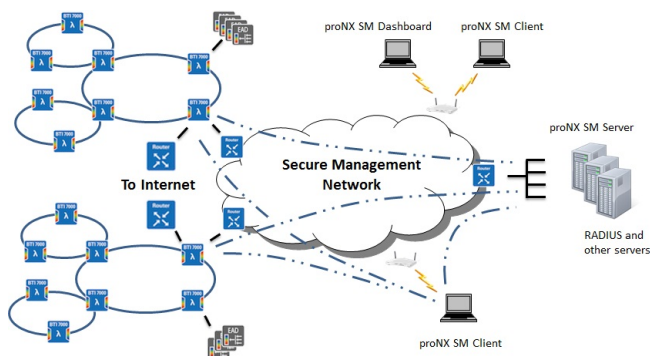
When a server configured for server replication comes up, it seeks out other members in the cluster and retrieves their replicated data. The server then overwrites its own replicated data with the retrieved replicated data. In other words, the first server that comes up is assumed to possess the correct replicated data. Servers that come up subsequently acquire and adopt this replicated data, which ultimately comes from the first server. Once all servers are up, the relationship between servers is peer-to-peer. Changes made on one server are automatically multicasted to the other servers. Each server will always have the up-to-date view.

For information on how to configure server replication, see [“Configuring Server Replication” on page 70](#).

PSM Networking Considerations

The PSM platform offers a set of services for visualizing and controlling network equipment. [Figure 2 on page 19](#) shows a typical network deployment with management traffic being separated onto a secure management network.

Figure 2: Typical Network Deployment



The network elements under management connect to the public Internet, but also maintain a separate and distinct connection to the management network. Traffic cannot cross from the public Internet to the management network. This can be enforced through physical segregation as shown above.

The PSM clients are connected to the management network. In some deployments, the clients might connect to the management network across the public Internet by using a VPN (not shown).

The PSM server (and other servers) are directly connected to the management network. Although the servers are shown as co-located, this is not necessary. If the servers are not co-located, the respective router/firewalls might need to be configured to allow proper communication between the servers (if necessary). These servers typically have public Internet connections as well, but through a separate physical interface. This is not shown.

The PSM platform requires communication paths between the following:

- the PSM clients and the PSM server
- the PSM server(s) and the PSM server(s)
- the PSM clients and the network elements under management
- the PSM server and the network elements under management
- the PSM server and the external RADIUS server (if applicable)
- the PSM server and other hosts, such as for backups, downloading of software images, etc. (not shown)

PSM Port Usage

The PSM platform provides services that are advertised on a set of protocol ports and leveraged by the PSM applications as well as by third party applications such as web browsers and servers running standard services.

If you are configuring a firewall to allow PSM traffic to pass through, you should be aware of the following communication paths in the PSM operating environment:

1. PSM client to/from PSM server
2. PSM server to/from PSM server
3. PSM server to/from a network element
4. PSM client to/from a network element
5. PSM server to/from a Network Operations Center (NOC), such as for HP Openview
6. PSM server to/from an external RADIUS server
7. PSM server to/from other hosts



NOTE: Communication between a PSM client and the PSM server assumes a secure, non-NATed network. Network address translation (NAT), which effectively hides the actual IP addresses, can cause connectivity problems between the client and the server.

Table 3 on page 21 through Table 9 on page 24 show the default port numbers that PSM and its attendant applications use on these different paths. Depending on the path, each endpoint can assume a client role or a server role or both roles. Since some of the applications support configurable port numbers, you will need to adjust the table entries accordingly if you change the port numbers from their defaults.

Additionally, network elements might have their own networking requirements outside of PSM connectivity. Table 10 on page 24 shows the BTI7800 networking port numbers.

The tables in this section provide information on the typical operating environment and cannot cover all possible scenarios in your network. For this reason, use the information in these tables to complement your own network implementation.



NOTE: To ensure there are no issues with the PSM operating environment, we recommend that the full ephemeral port range defined by IANA be open for client ports, that is, TCP ports 1023:65535.

Table 3: Port Usage in PSM Client to PSM Server Communications

Application	Description	PSM client port numbers	PSM server port numbers
		Protocol Role: client	Protocol Role: server
FTP	For file transfer between a PSM client and PSM server.	TCP:ephemeral	TCP:20,21
SSH, SCP, SFTP	For secure connectivity, server administration, and secure file transfers.	TCP:ephemeral	TCP:22
Monit Web GUI	For monitoring the PSM server using a Web GUI.	TCP:ephemeral	TCP:2812
MySQL (support)	For troubleshooting.	TCP:ephemeral	TCP:3306
Graphite web interface	For historical PMs.	TCP:ephemeral	TCP:8080
proNX Service Manager Dashboard	For proNX Service Manager Dashboard connectivity.	TCP:ephemeral	TCP:9000
JMX (support)	For troubleshooting.	TCP:ephemeral	TCP:9520
PSM REST WS	Representational state transfer web service, for normal HTTPS communication between a PSM client and the PSM server.	TCP:ephemeral	TCP:9998
		Protocol Role: server	Protocol Role: client
PSM REST Notification WS	Representational state transfer web service, for notifications from the PSM server.	TCP:9999-10100	TCP:ephemeral

Table 4: Port Usage in PSM Server to PSM Server Communications

Application	Description	PSM server port numbers	PSM server port numbers
		Protocol Role: client	Protocol Role: server
Server Replication	For server replication messages between servers.	TCP:ephemeral	TCP:9999-10100

Table 5: Port Usage in PSM Server to Network Element Communications

Application	Description	PSM server port numbers	Network element port numbers
		Protocol Role: client	Protocol Role: server
ICMP	Ping utility, used by the PSM server to check connectivity to the NEs.	port numbers not applicable	port numbers not applicable
NETCONF	For normal communication between the PSM server and the NE.	TCP:ephemeral	BT17800: TCP:2022 Juniper Networks MX Series router: TCP:830
CLI	For access to the CLI, normally executed from a PSM client, but can be run from the PSM server, as applicable.	TCP:ephemeral	See Table 6 on page 23 .
TL1	For access to TL1, normally executed from a PSM client, but can be run from the PSM server, as applicable.	TCP:ephemeral	See Table 6 on page 23 .
SNMP	For normal communication between the PSM server and the NE.	UDP:ephemeral	UDP:161
		Protocol Role: server	Protocol Role: client
FTP	For NE backup, restore, and software upgrades. This is only required if the FTP server on the PSM server is used. If an external FTP server is used, then the NEs will need access to those ports on the external FTP server.	TCP:20,21	TCP:ephemeral
SFTP	For NE backup, restore, and software upgrades. This is only required if the SFTP server on the PSM server is used. If an external SFTP server is used, then the NEs will need access to those ports on the external SFTP server.	TCP:22	TCP:ephemeral
NTP	For the NTP time synchronization service provided to the NEs. This is only required if the NTP (server-side) service on the PSM server is used.	UDP:123	UDP:ephemeral
SNMP	For notifications from the NEs.	UDP:162,1620	UDP:ephemeral
RADIUS	For authentication when logging in to the NEs. This is only required if the RADIUS server on the PSM server is used.	UDP:1812,1813	UDP:ephemeral

Table 6: Port Usage in PSM Client to Network Element Communications (includes proNX 900 Running on the Client Machine)

Application	Description	PSM client port numbers	Network element port numbers
		Protocol Role: client	Protocol Role: server
ICMP	Ping utility, used by the proNX 900 on the PSM client machine to check connectivity to the NEs.	port numbers not applicable	port numbers not applicable
SNMP	For normal proNX 900 communication with the NE.	UDP:ephemeral	UDP:161
CLI	For access to the CLI on the NE.	TCP:ephemeral	TCP: 22 (SSH to BT17800 Series NEs and MX Series routers), 23 (telnet to BT1700 Series and BT1800 Series NEs), 3084 (telnet to BT17000 Series NEs), 8022 (SSH to BT17000 Series NEs)
TL1	For access to TL1 on the NE.	TCP:ephemeral	TCP: 3021 (SSH used by proNX 900), 3022 (SSH), 3082 (telnet used by proNX 900), 3083 (telnet)
Shell	For access to the BT17800 operating system shell.	TCP:ephemeral	TCP:2024
		Protocol Role: server	Protocol Role: client
FTP	For NE backup, restore, and software upgrades. This is only required if the FTP server on a PSM client is used. If an external FTP server is used, then the NEs will need access to those ports on the external FTP server.	TCP:20,21	TCP:ephemeral
SFTP	For NE backup, restore, and software upgrades. This is only required if the SFTP server on a PSM client is used. If an external SFTP server is used, then the NEs will need access to those ports on the external SFTP server.	TCP:22	TCP:ephemeral

Table 7: Port Usage in PSM Server to Network Operations Center Communications

Application	Description	PSM server port numbers	Network Operations Center (NOC) port numbers
		Protocol Role: client	Protocol Role: server

Table 7: Port Usage in PSM Server to Network Operations Center Communications (continued)

Application	Description	PSM server port numbers	Network Operations Center (NOC) port numbers
SNMP	For northbound traps to the NOC (for example, to HP Openview)	UDP:ephemeral	UDP:162

Table 8: PSM Server to External RADIUS Server Communications

Application	Description	PSM server port numbers	External RADIUS server port numbers
		Protocol Role: client	Protocol Role: server
RADIUS	For authentication when logging in to the PSM server. This is only required if an external RADIUS server is used.	UDP:ephemeral	UDP:1812,1813

Table 9: PSM Server to Other Hosts

Application	Description	PSM server port numbers	Remote server/host port numbers
		Protocol Role: client	Protocol Role: server
FTP	For NE backup, restore, and software upgrades. This is only required if an external FTP server is used.	TCP:ephemeral	TCP:20,21
SFTP	For NE backup, restore, and software upgrades. This is only required if an external SFTP server is used.	TCP:ephemeral	TCP:22
DNS	For domain name lookups of hosts under management.	UDP:ephemeral	UDP:53
HTTP	For communication with web services.	TCP:ephemeral	TCP:80
NTP	For synchronization when using the NTP servers.	UDP:ephemeral	UDP:123

Table 10: BTI7800 Port Usage

Application	Description	BTI7800 port numbers	Remote server/host port numbers
		Protocol Role: client	Protocol Role: server
FTP	For NE software upgrades, log file rotation, and other file transfer applications.	TCP:ephemeral	TCP:20,21

Table 10: BTI7800 Port Usage (continued)

Application	Description	BTI7800 port numbers	Remote server/host port numbers
SFTP, SCP	For NE software upgrades, log file rotation, and other file transfer applications.	TCP:ephemeral	TCP:22
DNS	Domain name service, used by the BTI7800 to resolve domain names.	UDP:ephemeral	UDP:53
NTP	For NTP time synchronization.	UDP:123	UDP:123
SNMP	For SNMP traps to management systems.	UDP:ephemeral	UDP:162
SYSLOG	For access to the syslog server.	UDP:ephemeral	UDP:514
RADIUS	For authentication and authorization when logging in to the BTI7800. This is only required if a RADIUS server is used.	UDP:ephemeral	UDP:1812
TACACS+	For authentication and authorization when logging in to the BTI7800. This is only required if a TACACS+ server is used.	TCP:ephemeral	TCP:49
		Protocol Role: server	Protocol Role: client
CLI over SSH	For access to the CLI.	TCP:22	TCP:ephemeral
NETCONF	For NETCONF access from management systems.	TCP:2022	TCP:ephemeral
SSH	For direct access to the NE shell.	TCP:2024	TCP:ephemeral
TL1 over Telnet	For access to TL1.	TCP:3083	TCP:ephemeral
SNMP	For SNMP access from management systems.	UDP:161	UDP:ephemeral
Traceroute	For traceroute messages.	UDP:33434-33436	UDP:ephemeral

CHAPTER 2

proNX Service Manager System Requirements

- [PSM Server Requirements on page 27](#)
- [PSM Client Requirements on page 28](#)

PSM Server Requirements

The following tables list the recommended minimum software and typical hardware requirements for a PSM server.

The PSM server supports a maximum of 10 clients (any combination of PSM clients and proNX Service Manager Dashboard clients).

Software Requirements

Table 11: PSM Server Software Requirements

Software	Minimum Requirement
Operating system	Red Hat (CentOS) Linux, 64-bit, RHEL/CentOS 6 (6.3 or later), or RHEL/CentOS 7 (7.1 or later) Juniper Networks provides a setup script to help configure the OS and the installed packages to support the PSM server application. This script is included in the PSM ISO image.
Java Development Kit	OpenJDK Version 8 latest update

Hardware Requirements

PSM server hardware requirements depend on the number of clients, the number and type of network elements supported, and any special requirements imposed by enabled features (for example, historical PMs). [Table 12 on page 28](#) shows the specifications that all PSM servers must have. [Table 13 on page 28](#) shows the typical PSM server configurations.

Table 12: PSM Server Mandatory Specifications

Hardware	Requirement
Processor	Intel 64-bit
RAM	DDR3, 1066MHz or faster
Hard Disk	SAS, 7k or faster
Network Interface Cards	Dedicated 1GbE PCIe Cards (Intel preferred) + 1GbE port on motherboard
RAID	1 x hardware-based RAID 1 card with a battery-backed write cache
Integrated Lights Out Management	1 x dedicated IPMI 2.0 compatible BMC
Media Installation	1 x DVD +/- RW Drive

Table 13: PSM Server Typical Configurations

Number of cores	Amount of RAM	Hard disk capacity	Ethernet (PCIe)
6	12GB	2 x 1TB	2 x 10/100/1000 Ethernet
12	16GB	4 x 1TB	2 x 10/100/1000 Ethernet
16	24GB	8 x 1TB	4 x 10/100/1000 Ethernet
32	32GB	16 x 1TB	4 x 10/100/1000 Ethernet

In general, any server that is sized to meet your requirements can be used. Contact your Juniper Networks representative to confirm the server hardware requirements that will satisfy your particular needs.

Network Element Limitations

The BT17800 Series network element can be managed by a maximum of two PSM servers only.

PSM Client Requirements

The following tables list the recommended software and hardware requirements for the proNX Service Manager client and the proNX Service Manager Dashboard client.

A maximum of 10 clients (any combination of PSM clients and proNX Service Manager Dashboard clients) is supported.

Software Requirements

Table 14: PSM Client Software Requirements

Software	Requirement
Operating system	Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 10, latest updates applied.
	Supported on 32 and 64 bit versions
	Linux
	OS X, latest updates applied. Apple OS X Leopard +
Java Runtime Environment	Oracle JRE Version 8 latest update (recommended) ¹ , or
	OpenJDK Version 8 latest update ²
Browser	
NOTE: The proNX Service Manager Dashboard client requires JSON/XML view plug-ins to be installed if you wish to view the raw Representational State Transfer (REST) data in your browser.	
Microsoft Windows	Microsoft® Internet Explorer®, latest updates applied (not supported for the proNX Service Manager Dashboard client)
	Mozilla Firefox, latest updates applied
	Google Chrome, latest updates applied
OSX	Apple Safari, latest updates applied
	Mozilla Firefox, latest updates applied
	Google Chrome, latest updates applied

Table 14: PSM Client Software Requirements (continued)

Software	Requirement
----------	-------------

¹ Download the latest Oracle Java Runtime Environment Version 8 from www.oracle.com.

² Download the latest OpenJDK Version 8 from various vendors such as Red Hat.

NOTE: By default, the PSM client uses the default Java version on your system. You can change the Java version that the PSM client uses by modifying the `jdkhome` variable in the `<psm-install-dir>\etc\psmclient.conf` file to point to the installation directory of the Java version that you want to use. You may need to do this under the following situations:

- if the Java version you are installing is not automatically set up as the default by the installer
- if you are installing Java directly without an installer, such as installing through a zip file
- if you are installing OpenJDK
- if you have multiple Java versions installed and you want to select a non-default version

For example:

```
jdkhome="C:\Program Files\Java\java-1.8.0-openjdk-1.8.0.191-1.b12.redhat.windows.x86_64"
```

where `C:\Program Files\Java\java-1.8.0-openjdk-1.8.0.191-1.b12.redhat.windows.x86_64` is the directory of the Java installation you want the PSM client to use.

Hardware Requirements

Table 15 on page 30 lists the minimum hardware requirements for a PSM client managing a simple network. The actual hardware required is dependent on the size of the managed network. Contact Juniper Networks Support to determine whether your PSM client hardware is suitable for your network installation.

Table 15: PSM Client Hardware Requirements

Hardware	Requirement
Processor	Intel Pentium Dual-Core Processor E5300 or equivalent
RAM	4GB single channel DDR3 1600MHz
Hard disk space	73 GB
Video card	512MB Dedicated graphics card
Network Interface Card	1 x 1GbE
Media Installation	DVD +/- RW Drive

Terminal Server Incremental Memory Requirements

When running the proNX Service Manager client application in a terminal server deployment, the memory required on the Windows or Linux server is proportional to the number of clients served. Each client requires 2 GB of RAM. This is in addition to the base memory requirements for the server.

For example, assuming the base memory requirements for a Windows server is 4 GB, the following memory is required to support 10 proNX Service Manager clients:

```
Total memory required = base_memory + (#_of_clients x 2 GB)
                      = 4 GB + 10 x 2 GB
                      = 24 GB
```



NOTE: These calculations do not apply to the proNX Service Manager Dashboard client. The proNX Service Manager Dashboard client runs in a web browser whose memory requirements are accounted for in the operating system.

CHAPTER 3

Installing the proNX Service Manager and Related Tasks

- [Before You Install PSM Software on page 33](#)
- [About RPM on page 34](#)
- [Installing the PSM Server on page 34](#)
- [Upgrading the PSM Server on page 37](#)
- [Using Monit and Other Commands on page 40](#)
- [Installing the PSM Client Using the Wizard on page 41](#)
- [Installing the PSM Client Manually on page 43](#)
- [Upgrading the PSM Client on page 43](#)
- [Enabling Multiuser Access to the PSM Client on a Windows 2008 Server on page 44](#)
- [Configuring the PSM Server for a 32-bit Windows Client on page 44](#)
- [Starting the PSM Client on page 45](#)
- [Verifying PSM Client-server Connectivity on page 48](#)
- [Stopping the PSM Server on page 48](#)
- [Uninstalling the PSM Server on page 48](#)
- [Uninstalling the PSM Client on page 49](#)
- [Restoring the PSM Server Database from a Backup on page 49](#)
- [Reinitializing the PSM Server Database on page 51](#)

Before You Install PSM Software

Review the following checklist before installing proNX Service Manager software:

- Obtain the proNX Service Manager software DVD.
- Obtain the IP address of the server workstation on which PSM server is being installed. This IP address must be reachable from the managed network elements.

- Make sure the server and client workstations meet the system requirements described in [“PSM Server Requirements” on page 27](#) and [“PSM Client Requirements” on page 28](#).
- Make sure the operating system and required packages are installed. See [“Installing and Configuring Red Hat \(CentOS\) Linux” on page 81](#).

The installation order is:

1. Install the proNX Service Manager server software. See [“Installing the PSM Server” on page 34](#).
2. Install proNX Service Manager client software. See [“Installing the PSM Client Using the Wizard” on page 41](#) or [“Installing the PSM Client Manually” on page 43](#).



NOTE: Before installing any software, consult the *proNX Service Manager Release Notes* for this release. The *proNX Service Manager Release Notes* contains important information relating to installing and upgrading software for this release and might require you to take additional steps prior to or after executing the procedures in this section.

About RPM

RPM Package Manager (RPM) is an automated, non-interactive software installation package management system that is used for some Linux distributions. The acronym RPM refers to the actual package manager, and to the software that is packaged in the .rpm file.

The PSM server is installed from a .rpm file included in the PSM DVD and ISO image.

Installing the PSM Server

This procedure describes how to install the PSM server from an installation DVD or ISO image.

- Obtain the PSM DVD or ISO image.



NOTE: Before starting this procedure, consult the *proNX Service Manager Release Notes* for this release. The *proNX Service Manager Release Notes* contains important information relating to installing and upgrading software for this release, and might require you to take additional steps prior to or after executing this procedure.

1. Log in to the PSM server.
2. Insert the PSM DVD into the DVD drive of the server or copy the PSM ISO image onto the server.

3. Mount the DVD or the ISO. The mount directory (**/media**) in the following commands can be changed.

To mount the DVD:

```
mount -t iso9660 /dev/cdrom /media
```

To mount the ISO:

```
mount -t iso9660 -o loop PSM-xxx.iso /media
```

where **PSM-xxx.iso** is the name of the ISO file (for example, **PSM-7.8.0.iso**).

4. Copy the RPM file from the mounted DVD or ISO to any location on the server workstation. For example:

```
cp /media/ems9001-7.8-0.x86_64.rpm /usr/local
```

5. Install the new PSM server.

- a. To reduce the risk of database corruption while installing, execute the installation within the Linux screen terminal. Commands launched within the screen terminal continue to run even if your connection to the server is lost.

```
screen
```

The screen terminal is launched.

- b. In the screen terminal, navigate to the location where the RPM file was copied, and start the installation. For example:

```
cd /usr/local
rpm -ivh ems9001-7.8-0.x86_64.rpm
```



NOTE: If your connection to the server is lost during this step, log back in from any machine and type **screen -r** to reattach the screen.

The following is an example of the installation output. Your output might differ depending on release and configuration:

```
# rpm -ivh ems9001-7.8-0.x86_64.rpm
Preparing... #####
[100%]
Updating / installing...
 1:ems9001-7.8.0 #####
[100%]
Configuring iptables rules
Removing databases
Synchronising database schema
Checking database schema
Initialising database
Configuring radius
```

```

Configuring existing radius account
Configuring crontab entries
Configuring performance monitoring/graphing
Configuring process supervision
Configuring scripts
>>> Install Successful <<<

```

The output indicates that the following main events occurred:

- The new RPM package is expanded.
- The operating system firewall is updated with new rules for PSM.
- MySQL starts and the database is dropped and reinitialized with new schemas. As part of the installation, the MySQL database is configured with a default user and password. Contact Juniper Networks Support if you do not know the default user and password.
- The local RADIUS server is configured.
- The performance monitoring and graphing infrastructure is set up.
- The process manager is re-initialized to start managing PSM

The following directory is created:

```
/usr/local/ems9001-7.8
```



NOTE: The proNX Service Manager files are installed in the above directory. A softlink is created to this directory at:

```
/usr/local/ems9001
```

- c. Exit the screen terminal.

```
exit
```

This closes the Linux screen terminal and returns you to the original shell.

6. Unmount the DVD or ISO. Enter:

```
umount /media
```

7. Reboot the server.

```
reboot
```

8. After the server machine has rebooted, log back in and confirm that the PSM server is up and running.

```
[user ~]# psm-status
```

```
Every 2.0s: monit summary
```

```
Tue Jun 21 15:51:22 2016
```

```
The Monit daemon 5.14 uptime: 14d 2h 57m
```

Process 'SSH'	Running
Process 'radiusd'	Running
Process 'SNMPD'	Running
Process 'MySQL'	Running
Process 'proftpd'	Running
Filesystem 'rootfs'	Accessible
Filesystem 'logfs'	Accessible
Filesystem 'varfs'	Accessible
Filesystem 'pmsfs'	Accessible
Process 'Ems-Server-Masters'	Running
Process 'Ems-Server-Workers'	Running
Process 'Ems-Server-Discovery'	Running
Process 'Ems-Dashboard'	Running
Process 'CROND'	Running
Process 'carbon'	Running
System 'psm.example.com'	Running

The 'Ems-' processes should all be in the running state. You might need to wait a few minutes before the 'Ems-' processes all change to the running state. Type **<ctrl> c** to exit the Linux watch command window.

- To confirm that the new version of the server is installed, check the version information:

```
[user ~]# rpm -q ems9001
ems9001-7.8-0.x86_64
```

Look for the 'ems9001-' entry and confirm that the version is indeed the correct release.

You have successfully installed the PSM server.

Upgrading the PSM Server

This procedure describes how to upgrade the PSM server to Release 7.8.

- Obtain the PSM DVD or ISO image for Release 7.8.



NOTE: Before starting this procedure, consult the *proNX Service Manager Release Notes* for this release. The *proNX Service Manager Release Notes* contains important information relating to installing and upgrading software for this release, and may require you to take additional steps prior to or after executing this procedure.



NOTE: The *proNX Service Manager Release Notes* specifies the allowed upgrade paths for this release. Contact Juniper Networks Support when upgrading from releases that are not explicitly specified.

1. Log in to the PSM server.
2. Ensure the current PSM server version is one of the releases from which upgrade to this release is supported. For example:

```
[user ~]# rpm -q ems9001
ems9001-6.3-0.x86_64
```

3. Optionally, save any configuration that will be overwritten.
 - a. If you have made any changes to the property values in the **workers.xml** file, save that file so that they do not get overwritten during the server upgrade.

Locate the **workers.xml** file in directory **/usr/local/ems9001/resources/serverConfigurations/** and copy it to a location where it will not be overwritten during the server upgrade, preferably onto another machine.
 - b. If you have developed any custom server scripts, save those files so that they do not get overwritten during the server upgrade.

Locate the scripts in the directory **/usr/local/ems9001/conf/serverScripts** and copy them to a location in which they will not be overwritten during the server upgrade, preferably onto another machine.
 - c. Scheduled discoveries are also lost during the upgrade. If you have any scheduled discoveries, ensure you have the information to reschedule those discoveries so that you can restore them when you launch the new client.
4. Generate a backup of the existing PSM server database as follows:
 - a. Stop the server by entering the following command:

```
psm-stop
```

The stop command is successful when the 'Ems-' processes all change to 'not monitored' state. Type **<ctrl> c** to exit the Linux watch command window.

- b. Export the PSM server database. For example:

```
cd /tmp
mysqldump -u<user> -p --databases ems emsquartz > dbbackup.sql
```

The database backup file is stored in the **/tmp** directory.



NOTE: If a problem occurs during the upgrade that prevents the database from being automatically imported, import the database manually after you have finished upgrading. For example:

```
mysql -u<user> -p < dbbackup.sql
```

For information on how to restore the database from a backup, see [“Restoring the PSM Server Database from a Backup” on page 49](#).

5. Uninstall the current PSM server by entering the following command:

```
rpm -e ems9001
```

6. If you are upgrading from release 7.7 or lower to release 7.8 or higher, then you are required to install OpenJDK.

For information on how to do this, follow steps 11 through 14 in [“Installing and Configuring Red Hat \(CentOS\) Linux” on page 81](#).

7. Follow the steps in [“Installing the PSM Server” on page 34](#) to install the new PSM server.

If you do not have any configuration you need to restore from step 3, then you have completed the server installation. Otherwise, proceed to the next step.

8. If you have to restore changes to the property values in the **workers.xml** file, do the following:

Reapply the changes from the old **workers.xml** file that you saved in step 3. Do not simply overwrite the new file with the old ones, as there might be new properties defined in the new file that are required in the new software release. Instead, edit the file, identify the changes in the old file that you want to keep, and make those changes in the new **workers.xml** file. When you are done, save and close the new **workers.xml** file.

9. If you have to restore custom server scripts, copy the scripts back to the **/usr/local/ems9001/conf/serverScripts** directory.

10. To activate these changes, restart the PSM server.

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to the running state. Type **<ctrl> c** to exit the Linux watch command window.

You have successfully upgraded the PSM server.

Using Monit and Other Commands

Process management is performed by Monit, an open source utility for managing and monitoring processes, files, directories, and file systems. During the installation of PSM, the configuration files for monit are updated to monitor the PSM server process. The monit configuration can be re-read after installing the PSM by entering the command “monit reload”, or by rebooting the machine.

You can obtain the status of the PSM and other important services via the monit web interface at [http:// <server ip address>:2812](http://<server ip address>:2812) or on the command line.

When using the command line, you have access to a number of monit commands but it is recommended that you use the supplied aliases instead of invoking the monit commands directly. Some aliases are provided for convenience while others issue the monit command coupled with a 'monit summary' under the Linux watch command. You can then watch the command progress and complete before proceeding. In many situations, you should not proceed until the command has completed successfully. To exit from the Linux watch command window, type **<ctrl> c**.

- **psm-start** - Starts the OS processes needed for the PSM server application and displays the monit status summary within the Linux watch command.
- **psm-stop** - Stops the OS processes needed for the PSM server application and displays the monit status summary within the Linux watch command.
- **psm-restart** - Restarts the OS processes needed for the PSM server application and displays the monit status summary within the Linux watch command.
- **psm-status** - Displays the monit status summary within the Linux watch command. The PSM server processes are identified by the 'Ems-' prefix. The processes are in the "Running" state when the server is up and running, and in the "Not monitored" state when the server is stopped. For example:

```
[user ~]# psm-status

Every 2.0s: monit summary

                        Tue Jun 21 15:51:22 2016

The Monit daemon 5.14 uptime: 14d 2h 57m

Process 'SSH'                Running
Process 'radiusd'            Running
Process 'SNMPD'              Running
Process 'MySQL'              Running
Process 'proftpd'            Running
Filesystem 'rootfs'          Accessible
Filesystem 'logfs'           Accessible
Filesystem 'varfs'           Accessible
Filesystem 'pmsfs'           Accessible
Process 'Ems-Server-Masters' Running
Process 'Ems-Server-Workers' Running
Process 'Ems-Server-Discovery' Running
Process 'Ems-Dashboard'      Running
```


Process 'CROND'	Running
Process 'carbon'	Running
System 'psm.example.com'	Running

- psm-cd - Changes directory to `/usr/local/ems9001`.
- psm-cd-bin - Changes directory to `/usr/local/ems9001/bin`.
- psm-cd-conf - Changes directory to `/usr/local/ems9001/conf`.
- psm-cd-logs - Changes directory to `/usr/local/ems9001/logs`.
- psm-tail-audit - Performs the Linux 'tail' command on the **audit.log** file.
- psm-tail-discovery - Performs the Linux 'tail' command on the **EMS_SERVER-discovery.log** file.
- psm-tail-ems - Performs the Linux 'tail' command on both the **EMS_SERVER-masters.log** and the **EMS_SERVER-workers.log** files.
- psm-tail-masters - Performs the Linux 'tail' command on the **EMS_SERVER-masters.log** file.
- psm-tail-workers - Performs the Linux 'tail' command on the **EMS_SERVER-workers.log** file.
- getVersionInfo - Displays version information on the Linux kernel and operating system.

Installing the PSM Client Using the Wizard

Use this procedure to install the PSM client on Windows (32-bit or 64-bit), Linux, or MAC OS X. A user must have administrator privileges to install the PSM client, but does not need administrator privileges to run the client.

- See “PSM Client Requirements” on page 28.
 - On Linux, ensure the package **libgnome2.0** is installed. This package is required even if you are not running a Gnome desktop.
 - On MAC OS X, ensure you can install applications from all sources. Go to **System Preferences > Security & Privacy** and select the **General** tab. Set **Allow applications downloaded from:** to **Anywhere**. You might have to unlock the **Security & Privacy** window to make the change.
1. The PSM client wizard installer consists of a file for each operating system. The installer is included in the installation DVD, and can also be downloaded directly from the PSM server. In your web browser, go to **https://<server>:9998/client**, where **<server>** is the IP address of the workstation on which PSM server is installed. For example:

```
https://10.10.1.100:9998/client
```

Enter your username and password if prompted.

The installer files are as follows:

- Windows - **psmclient-xxx-windows.exe**

- OS X - `psmclient-xxx-macosx.tgz`
- Linux - `psmclient-xxx-linux.sh`

where `xxx` is the release number.

2. Click the appropriate PSM client installer and save it to the local machine.
3. Launch and run the installer. If a user account control dialog appears, click to allow the installer to run.

The client installer splash screen is displayed.



NOTE: In certain versions of MAC OS X, if you use a non-Safari browser (for example, Chrome or Firefox) to unpack the archive, this step might fail with an "Unable to unarchive psmclient-xxx-macosx.tgz into Downloads" error message. If you encounter this error, use Safari to launch the installer, or open a terminal shell and manually uncompress and unarchive the installer files:

```
tar -xzf psmclient-xxx-macosx.tgz
```

4. Click **Next**.
5. Read the EULA and select the **I accept the terms in the license agreement** check box if you agree.
6. Accept the default install path, or specify the path where you want to install the PSM client and click **Next**.
7. Click **Install**.

The wizard installs the PSM client.

8. When the wizard is complete, click **Finish**.

Shortcut icons are placed on the desktop as well as in the Start menu.



NOTE: If you are installing the client on a Windows 32-bit operating system, see [“Configuring the PSM Server for a 32-bit Windows Client” on page 44](#).

To launch the client, see [“Starting the PSM Client” on page 45](#).

This procedure is complete.

Installing the PSM Client Manually

Use this procedure to install the PSM client on Windows (32-bit or 64-bit), Linux, or MAC OS X. A user must have administrator privileges to install the PSM client, but does not need administrator privileges to run the client.

- See “PSM Client Requirements” on page 28.
 - On Linux, ensure the package **libgnome2.0** is installed. This package is required even if you are not running a Gnome desktop.
 - On MAC OS X, ensure you can install applications from all sources. Go to **System Preferences > Security & Privacy** and select the **General** tab. Set **Allow applications downloaded from:** to **Anywhere**. You might have to unlock the **Security & Privacy** window to make the change.
1. The PSM client is in a compressed file that is included on the PSM DVD. It can also be downloaded directly from the PSM server. In your web browser, go to **https://<server>:9998/client**, where **<server>** is the IP address of the workstation on which PSM server is installed. For example:

```
https://10.10.1.1:9998/client
```

Enter your username and password if prompted.

There is one compressed file for all supported operating systems: **psmclient-xxx.zip**, where **xxx** is the release number.

2. Uncompress the file and extract the contents into an applications folder.

For example:

- On Windows: **C:\Program Files\psmclient-xxx**
- On OS X: **/Applications/psmclient-xxx**
- On Linux, install the psmclient where you install other applications.



NOTE: If you are installing the client on a Windows 32-bit operating system, see “Configuring the PSM Server for a 32-bit Windows Client” on page 44.

To launch the client, see *Launching the PSM Client*.

This procedure is complete.

Upgrading the PSM Client

This procedure describes how to upgrade the PSM client.

- The user must have administrator privileges
1. Uninstall PSM client as instructed in [“Uninstalling the PSM Client”](#) on page 49.
 2. Install and start the PSM client as instructed in [“Installing the PSM Client Using the Wizard”](#) on page 41 or [“Installing the PSM Client Manually”](#) on page 43.

Enabling Multiuser Access to the PSM Client on a Windows 2008 Server

Use this procedure to enable multiple users to access the PSM client on a Windows 2008 server.

1. Install the PSM client on the Windows 2008 server. See [“Installing the PSM Client Using the Wizard”](#) on page 41.
2. Navigate to the client executable file in the installation directory and specify its permissions such that it is accessible to all users.
3. Open dedicated ports on the server for each client.
Edit the **ems.properties** file in directory `<installation directory>\psmclient`. Client ports are specified in the following (default) line:

```
ems.client.port = 9999-10100
```

Change the ports listed to suit your needs.
4. Save and close the **ems.properties** file.
5. Open the ports specified in the **ems.client.port** attribute of the **ems.properties** file on all intermediary firewalls so that users have access to the server.
6. Access the PSM client on the Windows 2008 server machine by launching a remote desktop session on the client machine, and logging in to the Windows server.

This procedure is complete.

Configuring the PSM Server for a 32-bit Windows Client

If you are installing at least one PSM client on a Windows 32-bit operating system, you must change the minimum RAM size that the PSM server expects each PSM client to have.

- The PSM server must be installed.

1. Log in to the PSM server.
2. Edit the `/var/local/ems9001/conf/override-common.properties` file as follows:

```
client.minimumRAMSizeMb=2000
```

3. Save and close the file.
4. Track changes to the `/var/local/ems9001/conf/override-common.properties` file with Git by committing this update to the Git repository.

For example:

```
[user conf]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Changed minimum RAM size. By user@example.org."
override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

5. Restart the PSM server for the change to take effect.

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to 'running' state. Type **<ctrl> c** to exit the Linux watch command window.

You have successfully configured the PSM server to handle 32-bit Windows clients.

Starting the PSM Client

Use this procedure to start the PSM client on Windows, Linux, or OS X.

Before you can perform this procedure, you must install the client software. Refer to [“Installing the PSM Client Using the Wizard” on page 41](#) or [“Installing the PSM Client Manually” on page 43](#) for instructions on installing the client.

1. Launch the **psmclient** executable file as follows:

- Windows: navigate to the **bin** folder within the PSM client installation folder and double-click the **psmclient.exe** file. Alternatively launch the client from the Desktop icon or Start menu entry created by the PSM client installer.
- OS X or Linux: open a terminal window, navigate to the PSM client installation directory and launch from the command line: **bin/psmclient**. Alternatively launch the client from the Desktop icon created by the PSM client installer.

The PSM installation starts by displaying the splash screen.

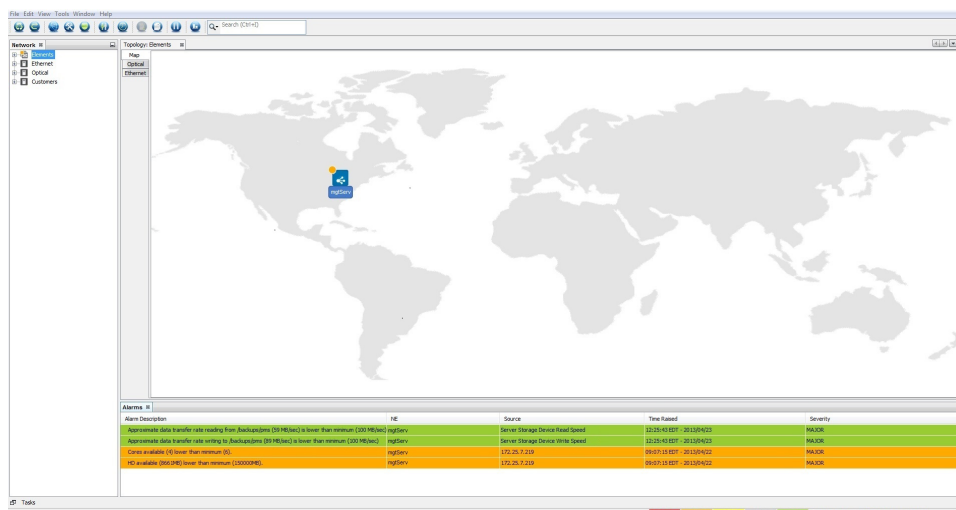


Then PSM displays the login screen.



2. In the **Server** field, enter the IP address for the PSM server, or choose a previously used server from the drop-down menu.
3. Enter the **Username** and **Password**.
4. Click **Login**.

After successful login, the PSM client navigation window is displayed. The following screen shows a newly installed server with no pre-discovered network elements.

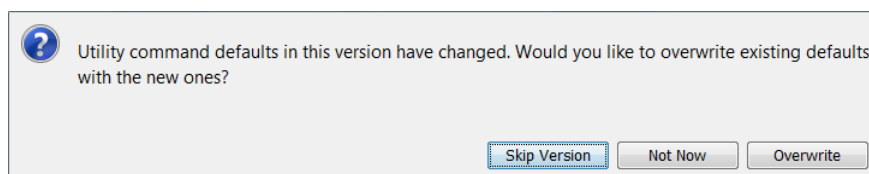


A "Connected to Server" indication is displayed in the lower right corner of the window. If connectivity to the server is lost, this changes to a "Connection to Server Lost" indication.



NOTE: Depending on the frequency with which the client and server check the path, it might take several minutes for a loss of connectivity to be detected and displayed.

If Juniper Networks has updated the utility software, you might see the following dialog in certain situations:



The utility software is the software defined in **Tools > Options > Utilities**. Choose:

- **Overwrite** if you have not changed any of the Type or Version **Default** settings. Choosing this option only overwrites the **Default** settings, and does not affect or overwrite the Type or Version-specific settings.
- **Not Now** if you have changed the **Default** settings and you want to save them before you overwrite them. To save the current **Default** settings, select **Tools > Options > Utilities** and click **Export** to save the settings (including the **Default** settings) to a zipped file. The **Default** settings can be found in `config\Preferences\com\btisystems\pronx\ems\client\preferences.properties` in the exported file. After you save the **Default** settings, re-launch the PSM client and choose **Overwrite** in the dialog.
- **Skip Versions** only if instructed to do so by Juniper Networks Support.

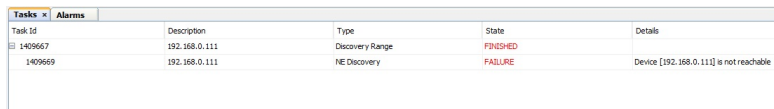
This procedure is complete.

Verifying PSM Client-server Connectivity

Use this procedure after installation or at any other time to verify that the PSM client is receiving asynchronous events from the PSM server.

1. Click **Tools > Network Element Discovery**.
2. In the **Device Discovery** window, enter a non-existent IP address in the **Discovery Criteria** box.
3. Click **OK**.

Look in the Tasks window and make sure you see the NE Discovery task for the non-existent IP address being launched and subsequently failing. If you do not see this task failing, check and fix your firewall settings and repeat this procedure.



Task Id	Description	Type	State	Details
1409667	192.168.0.111	Discovery Range	FINISHED	
1409669	192.168.0.111	NE Discovery	FAILURE	Device [192.168.0.111] is not reachable

Stopping the PSM Server

Use this procedure to stop the PSM server.

1. Determine the status of the PSM server by entering the following command.

```
psm-status
```

Type **<ctrl> c** to exit the Linux watch command window.

2. Stop the PSM server by entering the following command.

```
psm-stop
```

The stop command is successful when the 'Ems-' processes all change to 'not monitored' state. Type **<ctrl> c** to exit the Linux watch command window.

Uninstalling the PSM Server

Use this procedure to uninstall the PSM server.

- Close all PSM client sessions.
 - You must have administrator privileges.
1. Stop the PSM server by entering the following command.

```
psm-stop
```


The stop command is successful when the 'Ems-' processes all change to 'not monitored' state. Type **<ctrl> c** to exit the Linux watch command window.

2. Uninstall the PSM server.

```
rpm -e ems9001
```

The following output appears:

```
Stopping Server(all) ...Done
Stopping dashboard... Done
Removing PSM iptables rules
Delete crontab entries
Reinitializing monit daemon
```

The PSM (ems9001) processes are stopped, the software is removed, and monit is reinitialized.

This procedure is complete.

Uninstalling the PSM Client

Use this procedure to uninstall the PSM client on Windows, Linux, or OS X.

- You must have administrator privileges.

1. Exit the PSM client.

2. There are two ways to uninstall the PSM client.

- Manually - If the PSM client was installed manually, navigate to the folder where you installed the PSM client, and delete the installation folder.
- Using the wizard - If the PSM client was installed on Windows using the installation wizard, then you can uninstall it by using the Uninstall option in the Start menu or through the standard Windows Control Panel program uninstallation procedure.

This procedure is complete.

Restoring the PSM Server Database from a Backup

Use this procedure to restore the PSM server database from a backup.

The PSM server database is automatically backed up daily as a cron job (**/etc/cron.daily/mysqlbackup**). By default, the backup is run every morning between 3:00 and 4:00 AM. The backups are stored in **/backups/daily/ems**.

The backups are gzipped and stored using the following naming convention:

```
daily_ems_date_time.day_of_week.sql.gz
```

For example:

```
daily_ems_2016-12-06_03h11m_Tuesday.sql.gz
```

1. Stop the PSM server.

```
psm-stop
```

2. Uninstall the PSM server.

```
rpm -e ems9001
```

3. Drop the ems database. For example:

```
mysql -u<user> -p -e "DROP DATABASE ems"
```

4. Change directory to where the backups are stored.

```
cd /backups/daily/ems
```

5. Unzip the desired backup.

For example:

```
gunzip daily_ems_2016-12-06_03h11m_Tuesday.sql.gz
```

The backup file is unzipped into the local directory. For example:

```
[user ems]# ls  
daily_ems_2016-12-06_03h11m_Tuesday.sql
```

6. Restore the backup.

For example:

```
mysql -u<user> -p -e "create schema ems"  
mysql -u<user> -p ems < daily_ems_2016-12-06_03h11m_Tuesday.sql
```

7. Reinstall the PSM server.

For example:

```
[user ~]# cd /usr/local  
[user local]# ls ems*  
ems9001-7.8-0.x86_64.rpm  
[user local]# rpm -ivh ems9001-7.8-0.x86_64.rpm
```

8. Reboot the server.

```
reboot
```

The backup is restored.

Reinitializing the PSM Server Database

Use this procedure to reinitialize the PSM server database to factory defaults.

1. Stop the PSM server by entering the following command.

```
psm-stop
```

The stop command is successful when the 'Ems-' processes all change to 'not monitored' state. Type **<ctrl> c** to exit the Linux watch command window.

2. Drop the databases.

```
# cd /usr/local/ems9001/bin  
# ./emsdropdb.sh -a
```

3. Uninstall the PSM server.

```
rpm -e ems9001
```

4. Follow the steps in [“Installing the PSM Server” on page 34](#) to reinstall the PSM server.

CHAPTER 4

proNX Service Manager Administrator Tasks

- [Changing the PSM Properties File on page 53](#)
- [Considerations When Adding an FTP or SFTP Server on page 54](#)
- [Configuring Automated NE Database-backup Operations on page 55](#)
- [RADIUS on PSM on page 57](#)
- [Configuring Scheduled Historical PM Collection on page 64](#)
- [Configuring NE Log Collection on page 66](#)
- [Configuring PSM Alarm Severities on page 68](#)
- [Configuring PSM to E-mail NE Alarms on page 69](#)
- [Configuring Server Replication on page 70](#)
- [Stopping and Starting the PSM Server Application on page 72](#)
- [Configuring Automatic MIP Creation on the BTI810 Network Elements on page 72](#)
- [Configuring Ethernet Services Path Selection Through Non-ERPS Nodes on page 73](#)

Changing the PSM Properties File

The `/usr/local/ems9001/conf/common.properties` file is read on startup and contains parameters that control certain aspects of the PSM server behavior. This file is read-only and should not be modified by the user.

To make changes to the parameters specified in this file, modify the `/var/local/ems9001/conf/override-common.properties` file instead. As the name suggests, the `override-common.properties` file overrides the settings in the `common.properties` file. On startup, the PSM server reads the `common.properties` first, and then the `override-common.properties` file.

The `override-common.properties` file typically contains only parameters that have different values from their equivalents in the `common.properties` file. If a parameter appears in both files, the parameter value in the `override-common.properties` file takes effect.



NOTE: The `/var/local/ems9001/conf/override-common.properties` file survives PSM server software upgrades. You do not need to manually reinstate the property changes after the upgrade.

The `common.properties` file and, by correlation, the `override-common.properties` file may contain both user-settable and system-level parameters that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

All changes to the `/var/local/ems9001/conf/override-common.properties` file should be tracked with Git. See [“Using Git to Track `override-common.properties`” on page 77](#) for information on how to do this.

Considerations When Adding an FTP or SFTP Server

FTP or SFTP servers are used for network element database backup and restore functions, and network element system software upgrades. The PSM server installation includes a local (S)FTP server that is compatible with PSM and BTI Series network elements.

You may choose to use an external (S)FTP server. The following third party (S)FTP servers have been verified to be compatible with PSM and BTI Series network elements:

- FileZilla FTP server
- WinSSHD server
- VSFTPD server
- Cerberus FTP server



NOTE: Some free open source (S)FTP servers may not work properly due to incompatibilities with PSM and BTI Series network elements. For best results, choose a server from the list above.



NOTE: To use SFTP, the OpenSSH environment must be configured on the machine on which the PSM client is installed, and shell access must be enabled on the machine where the SFTP server is installed.

- [Updating the List Of Known Hosts on the PSM Server Machine on page 54](#)

Updating the List Of Known Hosts on the PSM Server Machine

Use the following procedure to add the (S)FTP server to the list of known hosts on the PSM server machine.



NOTE: You must perform this procedure even if you are using the included PSM (S)FTP server. The included PSM (S)FTP server is not added to the list of known hosts by default. It must be explicitly added.

1. At the command line on the PSM server machine, enter the following command:

```
ssh <username>@<hostname>
```

where *hostname* is the IP address of the (S)FTP server and *username* is the username to connect with.

The systems responds with:

The authenticity of host 'hostname (hostname)' can't be established. DSA key fingerprint is xxxxxx. Are you sure you want to continue connecting (yes/no)?

2. Enter **yes**.

The systems responds with:

Warning: Permanently added 'hostname' (DSA) to the list of known hosts.

3. Log off of the (S)FTP server by typing **exit** at the command prompt.

You have successfully completed this procedure.

Configuring Automated NE Database-backup Operations

The PSM server automatically backs up all discovered NEs on a daily basis. The backups are scheduled to run at 4:15 AM by default but this can be changed. PSM automatically uses the (S)FTP server installed on the PSM server and places the backup files in the default **/home/ftpadmin/NeDbBackups** directory. If an alternative location is desired then the (S)FTP server and subdirectory can be changed using the procedure in this section.

PSM uses the following format when naming backup files:

```
IP_address_BTIVersionnumber_Date_Time
```

For example:

```
10.1.202.1_BTIV000v6.2.0_20120108_041607.487
```

There is no indication on the PSM client that the scheduled backups have run, unless one fails. If a database backup operation fails for a particular network element, an alarm, which must be cleared manually, is raised to PSM server.

Only one attempt at a database backup operation is made on each network element during each schedule. The PSM server does not send additional database backup requests

after an operation fails. However, if the backup operation is set to run regularly, it sends a database backup request at the next scheduled backup time.

1. On the workstation where the PSM server is installed, open the file `/var/local/ems9001/conf/override-common.properties`.



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes might have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

2. **Specify the backup time and frequency.** In the `/var/local/ems9001/conf/override-common.properties` file, set the property `schedule.neDbBackup.cron` to specify the time at which the PSM server will send a database-backup request to each network element it manages. See [“Example: Scheduling Using Quartz CronTrigger Format” on page 76](#) for examples on how to specify the schedule.
3. **Specify the destination FTP server and subdirectory.** In the `/var/local/ems9001/conf/override-common.properties` file, set the properties `neDbBackup.ftpServerId` or `neDbBackup.sftpServerId` to specify the FTP or SFTP server to which the database is to be backed up. The format is `<ip address>:<port>:<user>:<subdirectory>`.
 - `<ip address>` is the IP address of the (S)FTP server.
 - `<port>` is the port number on which the (S)FTP server is listening.
 - `<user>` is a username that is allowed to log in to the (S)FTP server.
 - `<subdirectory>` is the name of the subdirectory where the backup files are to be placed (specified with a path relative to the FTP root directory). If you do not specify the subdirectory explicitly, the backup files are placed in the FTP root directory.



NOTE: The specified server with the above parameters (including the subdirectory if present) must exist in the PSM (S)FTP server list. See the *proNX Service Manager User Guide* for information on how to add servers to the PSM (S)FTP server list. If the (S)FTP server with the above parameters does not exist in the PSM (S)FTP server list, backups will not take place.



NOTE: You must manually create the specified subdirectory on the (S)FTP server.



NOTE: If you do not specify an (S)FTP server, the database is backed up to the default `/home/ftpadmin/NeDbBackups` directory on the local (S)FTP server included as part of the PSM server installation.

4. Save and close the `/var/local/ems9001/conf/override-common.properties` file.
5. Track changes to the `/var/local/ems9001/conf/override-common.properties` file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured automated NE backups. By
user@example.org." override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

6. To activate changes made to the `override-common.properties` file, restart the PSM server.

```
psm-restart
```



NOTE: NE database backup related alarms do not automatically clear themselves once the problem has been resolved. Any NE database backup alarms that occur must be manually cleared.

The restart command successfully completes when the 'Ems-' processes all change to 'running' state. Type `<ctrl> c` to exit the Linux watch command window.

RADIUS on PSM

The PSM server software includes a pre-packaged FreeRADIUS server that can be used to authenticate users in PSM and users in the network. This local RADIUS server stores user credentials in a SQL database (also included).

RADIUS facilitates the exchange of user credentials between the client and the server. The credentials are encrypted using a shared secret that is known to both the client and the server. The RADIUS protocol is UDP-based.

When a user launches the PSM client or the proNX Service Manager Dashboard and attempts to log in, or when a user attempts to log in to a network element directly, the PSM server acts as a RADIUS client, providing encrypted user credentials to a RADIUS server. The RADIUS server determines the access service that an authenticated user is authorized to use, and provides information to the network access server to allow the specific access service to be used.

The RADIUS authentication exchange happens at user login. The status of the client login is maintained and subsequent authentication exchanges take place at an interval that is configurable. This means that the current login session is impacted by changes in server availability or configuration.

The PSM RADIUS client does not support session accounting.

If firewall traversal is required, then the firewall must be configured to allow RADIUS traffic. The default ports for RADIUS traffic are 1812 and 1813.

The following table lists the supported RADIUS attributes:

Packet type	Attribute	Description
ACCESS-REQUEST - PSM server to RADIUS server. Sent by PSM to request a PSM client user be remotely authenticated.	User-Name	User's login userid.
	User-Password	User's login password.
	Called-Station-Id	Called station identifier.
	Message-Authenticator	RFC 2869 message authenticator.
ACCESS-ACCEPT - RADIUS server to PSM server. This response message must be received by PSM to allow the PSM client user login.	Reply-Message	The Reply-Message attribute must be present and determines the privilege level of the user. Contains "Administrator" or "Service Provider" or "NOC".
ACCESS-REJECT	All attributes ignored.	RADIUS server to PSM server. The receipt of this message causes the login to fail.
ACCESS-CHALLENGE	All attributes ignored.	RADIUS server to PSM server. This response message is treated as if an ACCESS-REJECT response was received.

The following table lists some of the attributes that can be provisioned on the PSM server. See the **common.properties** file in **/usr/local/ems9001/conf** for the default values.

Attribute	Description
RADIUS server IP address	Address of RADIUS server.
RADIUS server port (Authentication)	Typically 1812.
RADIUS server port (Accounting)	Typically 1813.
RADIUS authentication timeout	This is the time period in seconds that the RADIUS client waits for a response to ACCESS-REQUEST before considering the attempt a failure.
RADIUS authentication retry count	This is the number of times that authentication is attempted in the case of failure to reach the server.

Attribute	Description
Server authentication key (shared secret)	This consists of 6 to 256 case-sensitive alphanumeric characters and the following special characters: ! @ # \$ % ^ & * () _ + - = { } [] ' < > . / ~
Called-Station-Id	This is the called station identifier that is used in ACCESS-REQUEST messages.

The following table lists the attributes that must be provisioned in the authentication database to authenticate a client. A PSM-specific policy on the RADIUS server can be based on receiving a called-station-id attribute that matches the configured value.

RADIUS Attribute	Origin	Content
User-Name	RFC 2865	User id of the user described by the entry.
User-Password	RFC 2865	Password of the user described by the entry.
Reply-Message	RFC 2865	Authorization level (must contain "Administrator" or "Service Provider" or "NOC").

- [Configuring PSM to Use a RADIUS Server on page 59](#)
- [Configuring Network Elements to Use the Local RADIUS Server on page 61](#)

Configuring PSM to Use a RADIUS Server

Use this procedure to configure PSM to use a RADIUS server.

There is no limit to the number of RADIUS servers that can be specified. PSM cycles through the defined RADIUS servers and tries each server in turn until a response is received.

1. Add the PSM server to the list of allowable RADIUS clients.
 - a. Change to the RADIUS **raddb** directory.

```
cd /etc/raddb
```

- b. Edit the **clients.conf** file and add the IP address of the PSM server to the list of allowable RADIUS clients.

This file contains entries for each set of clients, with each entry indicating the IP address (or range) and the shared secret to use when connecting to the RADIUS server. For example:

```
client 10.64.6.24 {
    secret      = testing123
}
```

2. Restart the RADIUS server daemon for the changes to take effect.

```
service radiusd restart
```

The RADIUS server is now configured to accept authentication requests from the specified PSM server.



NOTE: By default, the local RADIUS server listens on port 1812 for authentication requests.

3. Configure the PSM server to use the RADIUS server.

Edit the following file: `/var/local/ems9001/conf/override-common.properties`



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

4. Configure the `auth.radius.server.1` attribute as follows:

- To specify that the local RADIUS server on the PSM machine is to be used, set the value to **localhost**.
- To specify that an external RADIUS server is to be used, set the value to the IP address of the external RADIUS server.

For example:

```
auth.radius.server.1=192.168.101.8
```



NOTE: The PSM server is initially configured to use the local, pre-packaged RADIUS server.

5. Configure the port numbers used by RADIUS. The typical values are shown below:

```
auth.radius.port.authentication.1=1812
auth.radius.port.accounting.1=1813
```

6. Configure the shared secret. This must match the shared secret configured on the RADIUS server.

For example:

```
auth.radius.secret.1=testing123
```

7. Configure other RADIUS attributes as needed. For the list of attributes that you can configure, look for **auth.radius** in the **common.properties** file.

Remember to modify the **/var/local/ems9001/conf/override-common.properties** file and not the **/usr/local/ems9001/conf/common.properties** file.

8. To specify additional RADIUS servers, create a set of attributes similar to the ones in the previous steps, but append the next number to each attribute, as shown in the following example:

```
auth.radius.server.2
auth.radius.port.authentication.2
auth.radius.port.accounting.2
auth.radius.secret.2
auth.radius.xxx.2
```

```
auth.radius.server.3
auth.radius.port.authentication.3
auth.radius.port.accounting.3
auth.radius.secret.3
auth.radius.xxx.3
```

9. Save and close the file.
10. Track changes to the **/var/local/ems9001/conf/override-common.properties** file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured RADIUS server. By user@example.org."
override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

11. Changes made to the **override-common.properties** file do not take effect until the PSM is restarted. To restart the server, enter the following command:

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to 'running' state. Type **<ctrl> c** to exit the Linux watch command window.

Configuring Network Elements to Use the Local RADIUS Server

Use this procedure to configure network elements to use the local, pre-packaged RADIUS server.

The PSM server software includes a pre-packaged FreeRADIUS server that can be used to authenticate users in the network. This RADIUS server is initially configured to allow

clients from the local host only. To allow network elements to use this RADIUS server, you need to configure this RADIUS server to allow those NE clients, and you need to configure those NE clients to use this RADIUS server.

1. Add the list of allowable NE clients to the RADIUS configuration file.
 - a. Change to the RADIUS **raddb** directory.

```
cd /etc/raddb
```

- b. Edit the **clients.conf** file and add the IP addresses of the NEs that will be making use of this RADIUS server.

This file contains entries for each set of clients, with each entry indicating the IP address (or range) and the shared secret for those NEs to use when connecting to the RADIUS server. For example:

```
client 10.1.203.0/24 {  
    secret      = testing123  
}
```

2. Restart the RADIUS server daemon for the changes to take effect.

```
service radiusd restart
```

The RADIUS server is now configured to accept authentication requests from the specified network elements.



NOTE: By default, the local RADIUS server listens on port 1812 for authentication requests.

3. Use PSM to add users to the RADIUS server database.

It is good practice to add users to the database before configuring the NE to use the RADIUS server.

- a. Ensure PSM is configured to use the included RADIUS server. For example, in the **/var/local/ems9001/conf/override-common.properties** file:

```
auth.radius.server.1=localhost  
auth.radius.port.authentication.1=1812  
auth.radius.port.accounting.1=1813  
auth.radius.timeout.1=2  
auth.radius.retryCount.1=2  
auth.radius.secret.1=testing123
```



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

- b. If you make any changes to the `/var/local/ems9001/conf/override-common.properties` file, track your changes with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured RADIUS server. By
user@example.org." override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track `override-common.properties`” on page 77](#).

- c. If you make any changes to the `override-common.properties` file, restart the PSM server in order for the changes to take effect.

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to 'running' state. Type **<ctrl> c** to exit the Linux watch command window.

- d. Add users to the RADIUS database by using the user management capability in PSM.

For information on how to do this, see the *proNX Service Manager User Guide*.

4. Configure network elements to use this RADIUS server.

For each network element, use the CLI, the proNX 900, or PSM to configure the following parameters:

RADIUS configuration parameters on the NEs	Example values	Description
RADIUS server IP address	10.10.1.100	Specifies 10.10.1.100 as the IP address of the RADIUS server to use.
RADIUS server role	primary	Specifies that this is the primary RADIUS server.
RADIUS server port	1812	Specifies the port on which to make the authentication request.
RADIUS server key	testing123	Specifies the shared secret configured on the RADIUS server for this network element.

RADIUS configuration parameters on the NEs	Example values	Description
RADIUS server priority	remote	Specifies that the NE authenticates with the RADIUS server first before authenticating with the local database.

For information on how to use PSM to configure these parameters on the NEs, see the *proNX Service Manager User Guide*.

The NEs can now connect to the local RADIUS server as clients.

Configuring Scheduled Historical PM Collection

Use this procedure to enable scheduled historical PM collection and to configure the collection schedule.

The PSM server can be configured to automatically collect historical PMs from all managed network elements. The amount of memory required to store these PMs is dependent on the number of metrics (PM points) collected, the frequency of collection, and the number of network elements.



NOTE: Before you enable scheduled historical PM collection, ensure you have sufficient disk storage space.

Each data point in the database is 12 bytes in size. To calculate the amount of storage required for a particular scenario, determine the number of data points stored and multiply by 12. This provides a good approximation of the storage required. Minor fixed storage costs are not included in this calculation.

For example, for a BT17200 NE fully loaded with 19 MXP cards with 12 ports per card and 12 supported PM points per port:

```
memory storage required per month (15-minute and 1-day PMs)
= number of cards per NE
  * number of ports per card
  * number of supported PM points per port
  * number of 15-minute and 1-day PM bins per day
  * 30 days per month
  * 12 bytes per point
= 19 * 12 * 12 * (96 + 1) * 30 * 12
= approximately 96 MB per NE
```

The historical PM database is located in the **/backups** partition, which is sized at 15% of the total disk space. The PSM server stores PMs in the database for 30 days. PM data points older than 30 days are purged from the database.

Scheduled historical PM collection scheduling is performed by specifying the values of the following properties in the **/var/local/ems9001/conf/override-common.properties** file:


```
// Switch for turning on/off the scheduled historical PM collection. Controls
all NEs.
pm.historical.collectionEnabled=false
// Switch for turning on/off the scheduled historical PM collection for 7800
type NEs.
pm.historical.7800CollectionEnabled=false
// Switch for turning on/off the scheduled historical PM collection for 800
type NEs.
pm.historical.800CollectionEnabled=false
// Schedule for Historical PM collection for 7000 type NEs.
// Every 12 hours.
schedule.historicalPmCollection.cron=0 0 0/12 * * ?
```

By default, the PSM server retrieves historical PMs every 12 hours, which allows time to correct any retrieval failures for the 1-day bin while minimizing unnecessary processing. If you want to view historical PMs that have not yet been retrieved, you can use the manual PM retrieval function that allows you to retrieve historical PMs on demand. See the *proNX Service Manager User Guide* for details.



NOTE: Be careful not to set the retrieval frequency such that a new retrieval is initiated before the current retrieval has completed. The prospect of this occurring increases as the network element becomes more populated. Some fully-populated network elements may require up to 30 minutes or more for the PM retrieval process to complete.

1. On the workstation where the PSM server is installed, open the `/var/local/ems9001/conf/override-common.properties` file.



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

2. Enable or disable historical PM collection as desired.
 - To enable historical PM collection for the BT17000 Series NEs, set `pm.historical.collectionEnabled=true`.
 - To enable historical PM collection for the BT17800 Series NEs, set `pm.historical.collectionEnabled=true` and `pm.historical.7800CollectionEnabled=true`.
 - To enable historical PM collection for the BT1800 Series NEs, set `pm.historical.collectionEnabled=true` and `pm.historical.800CollectionEnabled=true`.
 - To disable historical PM collection for all NEs, set `pm.historical.collectionEnabled=false`.

- To disable historical PM collection for the BTI7800 Series NEs only, set **pm.historical.7800CollectionEnabled=false**.
 - To disable historical PM collection for the BTI800 Series NEs only, set **pm.historical.800CollectionEnabled=false**.
3. Set the collection schedule by changing the **schedule.historicalPmCollection.cron** setting.

For information on how to set this value, see [“Example: Scheduling Using Quartz CronTrigger Format” on page 76](#).
 4. Save and close the **/var/local/ems9001/conf/override-common.properties** file.
 5. Track changes to the **/var/local/ems9001/conf/override-common.properties** file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured historical PMs. By user@example.org."
override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

6. To activate changes made to the **override-common.properties** file, restart the PSM server.

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to 'running' state. Type **<ctrl> c** to exit the Linux watch command window.

Configuring NE Log Collection

Use this procedure to configure network element log collection.

The PSM server can retrieve NE logs on a collection schedule as well as on demand. To retrieve logs, PSM logs in to the NE or router and transfers the specified log file from the NE or router to the PSM server machine using FTP. PSM then parses and stores the logs into its database and makes the logs available for the user to query. Once the logs are in the database, the retrieved log file is no longer needed and is removed automatically. For information on how to view NE logs, see the *proNX Service Manager User Guide*.

1. Log in to the PSM server machine and open the `/var/local/ems9001/conf/override-common.properties` file.



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences and must only be performed under the guidance of Juniper Networks Support.

2. Configure log collection parameters.

PSM logs in to the network element or router and transfers the specified log files to the PSM server machine using FTP.



NOTE: `<ne>` is 7800 for BT17800 Series network elements and `junos` for supported Juniper Networks routers.

- To set the FTP username, set `logCollection.<ne>.ftp.username=<username>`, where `<username>` is the username of the FTP user configured on the PSM server machine. If you leave this blank, the default FTP user is used. The default FTP user is set up as part of PSM server software installation.
 - To set the FTP password, set `logCollection.<ne>.ftp.password=<password>`, where `<password>` is the FTP password for the specified username. If you leave this blank, the default FTP password is used.
 - To set the destination file path where the log file is to be transferred, set `logCollection.<ne>.ftp.absolutePath=<filepath>`, where `<filepath>` is the absolute path of the directory where you want to place the log file. If you leave this blank, the log files are placed in `/home/ftpadmin`.
 - To specify the log file(s) that you want to retrieve, set `logCollection.<ne>.ftp.fileList=<files>`, where `<files>` is a comma-separated list of log files you want to retrieve. If you leave this blank, the `system.log` file is retrieved for BT17800 Series network elements and the `messages` file is retrieved for supported Juniper Networks routers.
 - To specify the FTP timeout value, set `logCollection.<ne>.ftp.readTimeout=<timeout>`, where `<timeout>` is the number of milliseconds to wait for FTP to complete. If the timeout expires, PSM assumes the FTP has failed.
 - To specify the (source) directory on supported Juniper Networks routers, set `logCollection.junos.ftp.directory=<directory>`, where `<directory>` is the directory where the log files are stored on the router.
3. If you want PSM to collect logs automatically, set the collection schedule by changing the `schedule.logCollection.cron` setting.

For information on how to set this value, see [“Example: Scheduling Using Quartz CronTrigger Format”](#) on page 76.



NOTE: Different network elements might support different strategies for log rotation. Log rotation refers to closing and saving the current log file and creating a new log file for subsequent logs. In order to minimize the risk of PSM missing a log file, ensure that the log rotation frequency on the network element or router aligns with the log collection frequency on PSM.

4. Save and close the `/var/local/ems9001/conf/override-common.properties` file.
5. Track changes to the `/var/local/ems9001/conf/override-common.properties` file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured log collection. By user@example.org."
override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

6. To activate changes made to the `override-common.properties` file, restart the PSM server.

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to 'running' state. Type `<ctrl> c` to exit the Linux watch command window.

Configuring PSM Alarm Severities

Use this procedure to configure the severities of PSM-generated alarms.



NOTE: The updated alarm severity appears in subsequent alarms generated by PSM. Severities of existing PSM alarms are not affected by this procedure.

1. Edit the `/usr/local/ems9001/resources/deviceMetadata/alarm-meta-psm.xml` file.
2. Find the alarm you want to change and edit the severity.

For example, to set the `NE_BACKUP` alarm severity to `CRITICAL`, change the alarm as follows:

```
<alarm-definition name="NE_BACKUP" service-affecting="false"
severity="CRITICAL"/>
```

3. Save and close the file.
4. Track changes to the **alarm-meta-psm.xml** file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /usr/local/ems9001/resources/deviceMetadata
[user deviceMetadata]# git commit -m "Set NE_BACKUP alarm severity to
CRITICAL. By user@example.org." alarm-meta-psm.xml
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

5. Changes made to the **alarm-meta-psm.xml** file do not take effect until the PSM server is restarted. To restart the server, enter the following command:

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to the running state. Type **<ctrl> c** to exit the Linux watch command window.

Configuring PSM to E-mail NE Alarms

The PSM can be configured to automatically e-mail NE alarm notifications to specified e-mail addresses. The severity of alarms for which e-mails are sent is configurable, and e-mails are sent for RAISE, CLEAR, and ACKNOWLEDGED alarm state changes.

Alarm/e-mail configuration is done by specifying the values of the following properties in the **/var/local/ems9001/conf/override-common.properties** file:

```
event.dispatch.email.host // Email host. If left blank, disables email/alarm
// notification.
event.dispatch.email.username // SMTP user name
event.dispatch.email.password // SMTP password
event.dispatch.email.port // SMTP port
event.dispatch.email.from // From address
event.dispatch.email.to // Comma-separated list of recipients
event.dispatch.email.severity // specifies severity threshold. Emails are
// sent if the alarm severity is equal to, or more severe than, the configured
// threshold.
```

1. On the workstation where the PSM server is installed, open the `/var/local/ems9001/conf/override-common.properties` file.



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

2. Specify the values for the properties in the file as desired.
3. Save and close the `/var/local/ems9001/conf/override-common.properties` file.
4. Track changes to the `/var/local/ems9001/conf/override-common.properties` file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured email alarm notifications. By
user@example.org." override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

5. To activate changes made to the `override-common.properties` file, restart the PSM server.

```
psm-restart
```



NOTE: Existing alarms that have already been processed by PSM for discovered NEs are not sent to the e-mail server. Only new alarms are sent.

The restart command successfully completes when the 'Ems-' processes all change to the running state. Type `<ctrl> c` to exit the Linux watch command window.

Configuring Server Replication

Use this procedure to configure server replication.

Server replication allows servers in a replication cluster to synchronize their replicated data.

1. Edit the `/var/local/ems9001/conf/override-common.properties` file.



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behavior of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

2. Set the `replication.enabled` attribute as follows:

- To enable server replication, set the value to **true**.
- To disable server replication, set the value to **false**.

For example, to enable server replication:

```
replication.enabled=true
```



NOTE: By default, server replication is disabled.

3. Configure the IP addresses of the other servers in the cluster.

The list of IP addresses is a comma-separated list. For example:

```
replication.cluster=10.64.6.24,10.64.6.25
```

4. Save and close the file.
5. Track changes to the `/var/local/ems9001/conf/override-common.properties` file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured server replication. By
user@example.org." override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

6. Changes made to the `override-common.properties` file do not take effect until the PSM server is restarted. To restart the server, enter the following command:

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to the running state. Type **<ctrl> c** to exit the Linux watch command window.

Stopping and Starting the PSM Server Application

Use this procedure to stop or start the PSM server application.

1. To stop the PSM server application:

```
psm-stop
```

This command is executed under the Linux watch command where you can watch the command progress and complete.

This command is completed when all the 'Ems-' processes change to the "Not monitored" state.

To exit from the Linux watch command window, type **<ctrl> c**.

2. To start the PSM server application:

```
psm-start
```

This command is executed under the Linux watch command where you can watch the command progress and complete.

This command is completed when all the 'Ems-' processes change to the running state.

To exit from the Linux watch command window, type **<ctrl> c**.

Configuring Automatic MIP Creation on the BTI810 Network Elements

When configuring connectivity fault management (CFM) for Ethernet services on BTI810 network elements, you may need to enable automatic MIP creation. MIPs are required for the link trace and loopback capabilities. If you do not plan on using link trace or loopback, then you should not enable automatic MIP creation. There are limits to the number of MIPs that can be created on BTI810 network elements. See the *BTI800 Series Technical Product Guide* for details.

1. Edit the `/var/local/ems9001/conf/override-common.properties` file.



.....

NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behaviour of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

.....

2. Set the `ethernetActivation.bti800.autoCreateMips` attribute as follows:

- To enable automatic MIP creation, set the value to **true**.
- To disable automatic MIP creation, set the value to **false**.

For example, to enable automatic MIP creation:

```
ethernetActivation.bti800.autoCreateMips=true
```



NOTE: By default, automatic MIP creation is disabled.

3. Save and close the file.
4. Track changes to the `/var/local/ems9001/conf/override-common.properties` file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured automatic MIP creation. By
user@example.org." override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

5. Changes made to the `override-common.properties` file do not take effect until the PSM server is restarted. To restart the server, enter the following command:

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to the running state. Type `<ctrl> c` to exit the Linux watch command window.

Configuring Ethernet Services Path Selection Through Non-ERPS Nodes

Use this procedure to configure Ethernet services path selection through non-ERPS nodes when PSM auto-provisions NNIs.

When using the **Auto-Provision NNIs** feature, PSM can be configured to use a more restrictive or a more liberal set of selection criteria for selecting internal NNIs.

1. Edit the `/var/local/ems9001/conf/override-common.properties` file.



NOTE: The `/var/local/ems9001/conf/override-common.properties` file contains many settings that affect the behaviour of the PSM server. Only those attributes explicitly described in this guide should be changed. Changing any other attributes may have unintended consequences, and must only be performed under the guidance of Juniper Networks Support.

2. Set the `ethernetServices.autoRouting.nonErpsSegments.singlePath` attribute as follows:

- To force PSM to select a single linear path through non-ERPS nodes, set the value to **true**. Make this selection only if there is a single path through non-ERPS nodes to the endpoint.
- To let PSM make a more liberal NNI selection through non-ERPS nodes, set the value to **false**. This may cause PSM to select more NNIs than is necessary. This is the default setting.

For example, to force the selection of a single linear path:

```
ethernetServices.autoRouting.nonErpsSegments.singlePath=true
```

3. Save and close the file.
4. Track changes to the `/var/local/ems9001/conf/override-common.properties` file with Git by committing this update to the Git repository.

For example:

```
[user ~]# cd /var/local/ems9001/conf
[user conf]# git commit -m "Configured single path selection for non-ERPS
nodes. By user@example.org." override-common.properties
```

This update can now be seen in the Git log. For more information on Git, see [“Using Git to Track override-common.properties” on page 77](#).

5. Changes made to the `override-common.properties` file do not take effect until the PSM server is restarted. To restart the server, enter the following command:

```
psm-restart
```

The restart command successfully completes when the 'Ems-' processes all change to the running state. Type `<ctrl> c` to exit the Linux watch command window.

CHAPTER 5

Appendix

- [Migrating the PSM Database to a New Server on page 75](#)
- [Example: Scheduling Using Quartz CronTrigger Format on page 76](#)
- [Using Git to Track override-common.properties on page 77](#)
- [Example: Using Fsck to Check and Repair a Filesystem on page 79](#)
- [Installing and Configuring Red Hat \(CentOS\) Linux on page 81](#)
- [Time Zones on page 90](#)

Migrating the PSM Database to a New Server

Use this procedure to migrate the PSM database to a new server.

1. Stop the PSM server.

```
psm-stop
```

The stop command successfully completes when the 'Ems-' processes all change to "Not monitored" state. Type **<ctrl> c** to exit the Linux watch command window.

2. Export the whole MySQL database from the source machine. At the shell prompt on the OS, run the following command:

```
mysqldump -u<user> -p --all-databases > dumpdb.sql
```

This command exports the entire MySQL database.

Alternatively, specify each PSM schema separately and take the backup file. For example, from the shell prompt on the OS, run the following command:

```
mysqldump -u<user> -p --databases ems emsquartz radius net_snmp hoard  
bti7xx_14 bti701_v107 bti7000_720 bti7000_920 bti2060_620 axn xxx.sql ...  
> dumpdb.sql
```

3. Copy the PSM database from the server to a temporary location.
4. Install the operating system on the new server.
5. Start MySQL.

```
service mysqld start
```

6. Import the PSM database from the temporary location.

```
mysql -u<user> -p < dumpdb.sql
```

7. Log in to MySQL.

```
mysql -u<user> -p
```

8. Flush the database settings. At the MySQL prompt, enter:

```
flush privileges;
```

9. Exit MySQL.

10. Install the PSM server.

Example: Scheduling Using Quartz CronTrigger Format

The PSM server uses the Quartz scheduler CronTrigger format to specify schedules for automated backups, logs, and other tasks. Schedules can be specified in the `/var/local/ems9001/conf/override-common.properties` file.

The scheduler entries take the following form:

```
schedule=<seconds> <minutes> <hours> <day_of_month> <month> <day_of_week>  
[<year>]
```

To aid in the creation of more complex schedules, the CronTrigger format supports a set of special characters, including the following:

- "*" means "every" unit for units in that position. For example, a "*" in the <hours> position means every hour.
- "?" means "don't care" for that position. For example, a "?" in the day_of_week position means that the day of week is irrelevant to the schedule.
- "/" is used to specify increments. For example, "0/15" in the seconds position means 0, 15, 30, 45.

Here is an expression scheduling the running of an NE backup everyday at 4:15 AM:

```
schedule.neDbBackup.cron=0 15 4 * * ?
```

To specify an NE backup to run every Sunday at 3:00 AM:

```
schedule.neDbBackup.cron=0 0 3 ? * SUN
```

For more information on the Quartz scheduler CronTrigger syntax, see <http://www.quartz-scheduler.org/documentation/quartz-1.x/tutorials/crontrigger>.

Using Git to Track `override-common.properties`

Git is a free and open source distributed version control system. The PSM server installation automatically creates a Git repository for `/var/local/ems9001/conf` and automatically adds the `override-common.properties` file to that repository. This allows you to track all updates to that file.

Every time you update the `override-common.properties` file, issue a `git commit` command and indicate the reason for the update. For example:

```
[user conf]# git commit -m "Changed automated NE backup time. By
user@example.org." override-common.properties
```

The text in quotations is freeform, and is used to specify the reason for the update and to identify the user who is making the change.

Here is a sample output of the `git commit` command:

```
[master a80a2f3] Changed automated NE backup time. By user@example.org.
Committer: user <user@example.org>
Your name and email address were configured automatically based
on your username and hostname. Please check that they are accurate.
You can suppress this message by setting them explicitly:

    git config --global user.name "Your Name"
    git config --global user.email you@example.com

After doing this, you may fix the identity used for this commit with:

    git commit --amend --reset-author

1 files changed, 1 insertions(+), 1 deletions(-)
[user conf]#
```

To view the log of changes, use the `git log` command. For example:

```
[user conf]# git log override-common.properties
```

This produces a log of all the changes made to the file, with the most recent change listed first:

```
commit a80a2f33cdbf27e1b7973f93360a82471f1249f2
Author: user <user@example.org>
Date: Thu May 30 14:22:56 2013 -0400

    Changed automated NE backup time. By user@example.org.

commit 187bf1786d7da5153a04c30611ed44d49ebf6974
Author: user <user@example.org>
Date: Thu May 30 14:20:25 2013 -0400

    Enabled historical PM collection. By user@example.org.

commit 6835ba91cce1b8a8f2c5414315fc035b6e7545c8
```

```
Author: user <user@example.org>
Date:   Thu May 30 14:13:50 2013 -0400

    conf initial configuration
[user conf]#
```

To view the log of changes and their differences, use the **git log -u <start>..<end>** command. If **<end>** is omitted, the log will include all changes from **<start>** up to the most recent update. In this example, to view a log of all changes after installation:

```
[user conf]# git log -u 6835ba91cce1b8a8f2c5414315fc035b6e7545c8..
override-common.properties
```

This command shows the log of changes and their differences starting from the commit identifier **6835ba91cce1b8a8f2c5414315fc035b6e7545c8**, which in this example is immediately after installation. The output is as follows:

```
commit a80a2f33cdbf27e1b7973f93360a82471f1249f2
Author: user <user@example.org>
Date:   Thu May 30 14:22:56 2013 -0400

    Changed automated NE backup time. By user@example.org.

diff --git a/override-common.properties b/override-common.properties
index 8aa0651..3e77f16 100644
--- a/override-common.properties
+++ b/override-common.properties
@@ -268,7 +268,7 @@ schedule.watchdog.cron=0 0/2 * * * ?
 // Schedule for generating NE database backups for the subset of all known
 devices. (Note: Number of parallel backups is defined implicitly by workers'
 pool task configuration)
 // Every day at 4:15 a.m.
 // Note: Problems were observed when full backups are run every 20sec's
 because parallel backups were running.
-schedule.neDbBackup.cron=0 15 4 * * ?
+schedule.neDbBackup.cron=0 15 3 * * ?

 // Schedule for retrieving the current FTP server status.
 // Every 5 minutes ...

commit 187bf1786d7da5153a04c30611ed44d49ebf6974
Author: user <user@example.org>
Date:   Thu May 30 14:20:25 2013 -0400

    Enabled historical PM collection. By user@example.org.

diff --git a/override-common.properties b/override-common.properties
index 205c6d7..8aa0651 100644
--- a/override-common.properties
+++ b/override-common.properties
@@ -384,7 +384,7 @@ carbon.host=localhost
 carbon.linePort=2003

 // Switch for turning on/off the scheduled historical PM collection.
-pm.historical.collectionEnabled=false
+pm.historical.collectionEnabled=true
```

```
// Mappings of PSM roles to comma-separated list of RADIUS roles.
[user conf]#
```

In the above example, at 14:20:25, user@example.org changed **pm.historical.collectionEnabled** to **true**, and at 14:22:56, user@example.org changed **schedule.neDbBackup.cron** to be at 3:15 every morning.

If you have forgotten whether you have performed a **git commit** or not, use the **git status** command to check the status. For example:

```
[user conf]# git status
# On branch master
# Changes not staged for commit:
#   (use "git add <file>..." to update what will be committed)
#   (use "git checkout -- <file>..." to discard changes in working directory)
#
#       modified:   override-common.properties
#
no changes added to commit (use "git add" and/or "git commit -a")
[user conf]#
```

The above output tells you that the **override-common.properties** file has been modified but not committed.

For more information on Git, see <http://git-scm.com/>.

Example: Using Fsck to Check and Repair a Filesystem

This procedure provides a basic example on how to use fsck and other Linux commands to check and repair a filesystem.

Pre-requisites:

- You must be locally connected to the PSM server (rather than remotely using telnet or ssh).

The Linux fsck command can be used to check and repair a corrupted filesystem under some situations. This section contains one example of how to accomplish this for a non-root partition. Methods using other commands exist. Consult the Linux man pages for more complete coverage of the commands used in this example.

1. Change to single user mode.

```
telinit 1
```

2. List the mount points on your system.

For example:

```
[user ~]# df -T
Filesystem      Type      1K-blocks      Used Available Use% Mounted on
/dev/mapper/vg-lv_root
ext4           55316552    6082732   46426180   12% /
```

```

tmpfs      tmpfs      3848252      0      3848252      0% /dev/shm
/dev/mapper/vg-lv_backups
/dev/sda1   ext4      16094652     6680620     8596472      44% /backups
/dev/mapper/vg-lv_home
/dev/mapper/vg-lv_tmp
/dev/mapper/vg-lv_var
/dev/mapper/vg-lv_log
ext4      1032088      54272      925388      6% /boot
ext4      20223240     10190760     9006896      54% /home
ext4      10740304     158644     10036076      2% /tmp
ext4      67702420     15364244     48901456      24% /var
ext4      32189320     290212     30263988      1% /var/log

```

3. Unmount all filesystems from `/etc/fstab`.

```
[user ~]# umount -a
```



CAUTION: To prevent data corruption, ensure that you unmount before running the `fsck` command on any filesystem.



NOTE: Not all filesystems can be unmounted. You should not run `fsck` on any mounted filesystem.

4. Find the logical volumes.

For example:

```

[root@mgtServ3 ~]# lvscan
ACTIVE          '/dev/vg/lv_var' [65.59 GiB] inherit
ACTIVE          '/dev/vg/lv_log' [31.19 GiB] inherit
ACTIVE          '/dev/vg/lv_tmp' [10.41 GiB] inherit
ACTIVE          '/dev/vg/lv_backups' [15.59 GiB] inherit
ACTIVE          '/dev/vg/lv_home' [19.59 GiB] inherit
ACTIVE          '/dev/vg/lv_root' [53.59 GiB] inherit

```

5. Check and repair the filesystem.

For example, to check and repair the `/home` partition:

```

[user ~]# fsck -yvfM /dev/vg/lv_home
fsck from util-linux-ng 2.18
e2fsck 1.41.12 (17-May-2010)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information

      449 inodes used (0.04%)

```



```

    10 non-contiguous files (2.2%)
    1 non-contiguous directory (0.2%)
    # of inodes with ind/dind/tind blocks: 0/0/0
    Extent depth histogram: 439
242020 blocks used (5.92%)
    0 bad blocks
    1 large file

    423 regular files
    17 directories
    0 character device files
    0 block device files
    0 fifos
    0 links
    0 symbolic links (0 fast symbolic links)
    0 sockets
-----
    440 files

```

In the above output, there are no errors in the **/home** partition.

6. Continue to check and repair other partitions. After you finish the repairs, reboot the PSM server.

```
reboot
```

Installing and Configuring Red Hat (CentOS) Linux

This section provides information about installing and configuring Red Hat (CentOS) Linux for the PSM server.

- [Before You Install Red Hat \(CentOS\) Linux on page 81](#)
- [Installing and Configuring Red Hat \(CentOS\) Linux, 64-bit, for the PSM Server on page 82](#)

Before You Install Red Hat (CentOS) Linux

Obtain the following information from your IT department before installing Red Hat (CentOS) Linux.

- the IP address for the server where the operating system will be installed
- the system name
- the domain name
- the subnet mask
- the gateway
- the DNS server
- the proxy server if applicable (see below)



NOTE: Before installing any software, consult the *proNX Service Manager Release Notes* for this release. The *proNX Service Manager Release Notes* contains important information relating to installing and upgrading software for this release, and may require you to take additional steps prior to or after executing the procedures in this section.

Running with a Proxy Server

If the machine that you're installing the PSM server on is located behind a proxy, you must make changes to the following configuration files in order for the installation to proceed properly:

- **wgetrc** - The `wget` command is used by the installation script supplied by Juniper Networks to download files. The `wget` command needs to know that it's running behind a proxy. The recommended approach is to modify the `wget` configuration file, `/etc/wgetrc` for the system or `~/.wgetrc` for an individual user, by adding the following lines:

```
use_proxy=on
http_proxy=proxy_host_or_ip:proxy_port
proxy_user=username
proxy_password=password
```

- **curlrc** - The `curl` command is used by the installation script supplied by Juniper Networks to download files. The `curl` command needs to know that it's running behind a proxy. The recommended approach is to modify the `curl` configuration file, `~/.curlrc`, by adding the following line:

```
proxy=http://username:password@proxy_host_or_ip:proxy_port
```

Installing and Configuring Red Hat (CentOS) Linux, 64-bit, for the PSM Server

Use this procedure to install and configure Red Hat (CentOS) Linux, 64-bit, from an installation DVD.

- See [“PSM Server Requirements” on page 27](#).
- Obtain the installation DVD for Red Hat (CentOS) Linux.
- Obtain the PSM DVD or ISO image.
- Obtain the information specified in [“Before You Install Red Hat \(CentOS\) Linux” on page 81](#).
- Ensure the server machine is physically connected to a LAN and is able to access the Internet.
- Ensure the system is bootable from the DVD drive.
- Ensure the SATA mode in the BIOS is set to support AHCI instead of legacy. For some BIOSs, this may be called "Enable SATA AHCI Support".



NOTE: Before starting this procedure, consult the *proNX Service Manager Release Notes* for this release. The *proNX Service Manager Release Notes* contains important information relating to installing and upgrading software for this release, and may require you to take additional steps prior to or after executing this procedure.



NOTE: This procedure provides supplementary installation information on how to configure the operating system and/or software packages in order to run the PSM server application, and is not intended to replace the procedures provided by the operating system and/or software package suppliers.



NOTE: This section uses examples to illustrate the installation procedure. The examples refer to IP addresses and software version numbers that may not match your particular network configuration or the current software release. Consequently, the output that you see may differ from what is shown in the examples.

1. Insert the Red Hat (CentOS) Linux installation DVD and follow the on-screen instructions.

Select the following options during the installation:

- If the server has an existing Linux installation, specify that you want to perform a fresh installation. In some installations, this may appear as the **Fresh Installation** option.
- Provision the network settings. In some installations, this may appear as the **Network Configuration** option. Specify a static IP address, netmask, hostname, default gateway, and DNS server. Ensure the **Connect automatically** option is selected and that the server machine is physically connected to the network.
- Select the option to make use of all the disk space for the new installation. In some installations, this may appear as the **Use All Space** option. See NOTE below.
- Select the minimal server installation option. In some installations, this may appear as the **Minimal** installation option.



NOTE: It is recommended that you partition the disk such that the /home partition takes up only 15% of the total disk space. You should configure the / partition to take up the rest of the partitionable space. For RHEL (CentOS) 6, you can configure the partitioning by selecting **Review and modify partitioning layout**. For RHEL (CentOS) 7, you can configure the partitioning by selecting **I will configure partitioning** in the **INSTALLATION DESTINATION** window.

For all other options, follow the on-screen instructions and/or use the defaults.

2. Reboot the server and log in as **root** using the credentials you specified during the OS installation.
3. Confirm that your network settings are correct.
 - a. Check your network connectivity.

Ping a known IP address in your network. For example:

```
[root@psmdemo ~]# ping -c2 10.64.0.1
PING 10.64.0.1 (10.64.0.1) 56(84) bytes of data.
64 bytes from 10.64.0.1: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 10.64.0.1: icmp_seq=2 ttl=64 time=1.03 ms

--- 10.64.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.037/1.049/1.062/0.034 ms
```

- b. Confirm your DNS server is working properly.

Ping a well-known site to ensure the site name is resolved. For example:

```
[root@psmdemo ~]# ping -c2 www.google.com
PING www.google.com (173.194.43.113) 56(84) bytes of data.
64 bytes from yyz08s10-in-f17.1e100.net (173.194.43.113): icmp_seq=1
ttl=57 time=7.73 ms
64 bytes from yyz08s10-in-f17.1e100.net (173.194.43.113): icmp_seq=2
ttl=57 time=7.93 ms

--- www.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 7.736/7.833/7.930/0.097 ms
```

If either of these steps fails, fix your network settings before proceeding.

4. If you are installing Red Hat, you must register your computer, attach a subscription, and subscribe to the necessary channels before you can update your server machine from the Red Hat repositories. If you are installing CentOS, skip to 5.
 - a. Register your subscription by using the **subscription-manager register** command and entering your Red Hat subscription username and password.
 - b. Attach the subscription by using the **subscription-manager attach --auto** command.
 - c. Subscribe to the options channel.

- For Red Hat 6, use the following command:

```
subscription-manager repos --enable=rhel-6-server-optional-rpms
```

- For Red Hat 7, use the following command:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

- d. Additionally, for Red Hat 7, you must subscribe to the extras channel by using the following command.

```
subscription-manager repos --enable=rhel-7-server-extras-rpms
```

5. Update the system packages.

```
[root@psmdemo ~]# yum -y update
```

6. Reboot the server and log back in as **root**.

7. Add the server to the hosts file.

Look in the **/etc/hosts** file and add the name of the server, the domain, and the IP address as one of the entries.

For example, for a server named **psmdemo**:

```
[root@psmdemo ~]# vi /etc/hosts
[root@psmdemo ~]# cat /etc/hosts | grep psmdemo
10.64.8.155 psmdemo.example.org psmdemo
[root@psmdemo ~]#
```

8. Ensure the date and time are set correctly.

To verify the date, for example:

```
[root@psmdemo ~]# date
Mon Jan 13 09:28:54 EST 2014
```

If the date and time are not set correctly, manually set the date and time. For example:

```
[root@psmdemo ~]# date -s "Jan 21 14:38:00 2014 EST"
```



NOTE: Alternatively, if NTP has been set up, you can use the `ntpdate` command to manually synchronize the time with an NTP server (for example, `ntpdate us.pool.ntp.org`). The `ntpdate` command can only be performed if you do not have an `ntpd` service running. If you do, then stop the service first by issuing the `service ntpd stop` command. In a new installation, NTP will not have been set up yet. NTP is set up as part of the `psm-xxxxx.run` script.

Proceed to the next step only after the date and time are correct.

9. Install an SSH client, such as openSSH.

```
yum install openssh-clients
```

This installs openSSH and its dependencies.

10. Install the Extra Packages for Enterprise Linux (EPEL). EPEL contains packages that are required by the PSM server.

- a. For CentOS:

The EPEL package is available through YUM.

```
yum -y install epel-release
```

- b. For Red Hat:

EPEL is part of the Fedora project, and can be installed as follows:

```
rpm -ivh
http://dl.fedoraproject.org/pub/epel/epel-release-latest-n.noarch.rpm
```

where *n* is 6 for Red Hat 6, and 7 for Red Hat 7.

Confirm by checking for the repository. For example:

```
[root@psmdemo ~]# ls /etc/yum.repos.d/epel*
epel.repo    epel-testing.repo
```

11. Install the OpenJDK Java Runtime Environment (JRE) on the server machine. The server machine must have Internet access.

For example:

```
[root@psmdemo ~]# yum install java-1.8.0-openjdk
Loaded plugins: fastestmirror

<trimmed>

Installed:
  java-1.8.0-openjdk.x86_64 1:1.8.0.191.b12-1.e17_6

Dependency Installed:
  copy-jdk-configs.noarch 0:3.3-10.e17_5      giflib.x86_64 0:4.1.6-9.e17
  java-1.8.0-openjdk-headless.x86_64 1:1.8.0.191.b12-1.e17_6
  javapackages-tools.noarch 0:3.4.1-11.e17
  libXcomposite.x86_64 0:0.4.4-4.1.e17      libXi.x86_64 0:1.7.9-1.e17
  libXtst.x86_64 0:1.2.3-1.e17
  libjpeg-turbo.x86_64 0:1.2.90-6.e17
  lksctp-tools.x86_64 0:1.0.17-2.e17      nss-pem.x86_64 0:1.0.3-5.e17
  python-javapackages.noarch 0:3.4.1-11.e17
  python-lxml.x86_64 0:3.2.1-4.e17
  ttmkfsdir.x86_64 0:3.0.9-42.e17      tzdata-java.noarch
  0:2018i-1.e17      xorg-x11-fonts-Type1.noarch 0:7.5-9.e17

Dependency Updated:
  chkconfig.x86_64 0:1.7.4-1.e17      nspr.x86_64 0:4.19.0-1.e17_5
  nspr-devel.x86_64 0:4.19.0-1.e17_5  nss.x86_64 0:3.36.0-7.e17_5
  nss-softokn.x86_64 0:3.36.0-5.e17_5
  nss-softokn-freebl.x86_64 0:3.36.0-5.e17_5  nss-sysinit.x86_64
  0:3.36.0-7.e17_5  nss-tools.x86_64 0:3.36.0-7.e17_5  nss-util.x86_64
  0:3.36.0-1.e17_5

Complete!
```

Check that OpenJDK has been installed.

For example:

```
[root@psmdemo ~]# ls /usr/lib/jvm
java-1.8.0-openjdk-1.8.0.191.b12-1.e17_6.x86_64
jre
jre-1.8.0
jre-1.8.0-openjdk
jre-1.8.0-openjdk-1.8.0.191.b12-1.e17_6.x86_64
jre-openjdk
```

For more information on installing OpenJDK, see <https://openjdk.java.net/install/>.

12. Run the **psm-xxxxx.run** script provided by Juniper Networks in the PSM ISO image. This script requires Internet access, and configures the operating system and installs the software packages required by the PSM server.



NOTE: If you are installing the PSM server on a machine that is behind a proxy, ensure you have modified the appropriate configuration files as described in “Before You Install Red Hat (CentOS) Linux” on page 81.

- a. Insert the PSM DVD into the DVD drive of the server or copy the PSM ISO image onto the server.

To copy the ISO image onto the server, you can use **scp** if transferring from a Linux machine, or you can use a Windows SCP application (for example, WinSCP) if transferring from a Windows machine.

- b. Create the mount directory on the server if it is not already created.

For example:

```
mkdir /media
```

- c. Mount the DVD or the ISO.

To mount the DVD:

```
mount -t iso9660 /dev/cdrom /media
```

To mount the ISO:

```
mount -t iso9660 -o loop xxx.iso /media
```

where **xxx.iso** is the name of the ISO file (for example, **PSM-7.8.0.iso**).

- d. In the mount directory, look for the **psm-xxxxx.run** script and copy that file into the **/root** directory. **xxxxx** is the update version number, which varies from release to release.

For example:

```
[root@psmdemo ~]# cp /media/psm-xxxxx.run .
```

- e. If necessary, change permissions on the script to allow it to be run.

For example:

```
[root@psmdemo ~]# chmod +x psm-xxxxx.run
```

- f. Run the script.

For example:

```
[root@psmdemo ~]# ./psm-xxxxx.run
```

Here is sample output from one version of the script:

```
By accepting this license in any manner, you represent that you have
read, understood and agree to be bound by and comply with the terms and
conditions of the End-User Software License Agreement found at
http://www.juniper.net/support/eula/ (this License or "EULA"). This
License defines what you may do with the Licensed Software and may contain
limitations on warranties and/or remedies. If you do not agree with or
accept these terms and conditions then you are not granted a license
and are not authorized to access, download, install or use the Licensed
Software.
Please type y to accept, n otherwise: y
Verifying archive integrity... All good.
```



```

Uncompressing PSM Server Setup .. 100%

Confirming script running as root:                [ OK ]
Confirming distro is Red Hat RPM-based:            [ OK ]
Confirming architecture is x86_64:                [ OK ]
Confirming yum is available:                      [ OK ]
Confirming hostname not set to localhost:          [ OK ]
Confirming hostname is configured and pingable:    [ OK ]
Confirming Internet connectivity (install only):    [ OK ]
Confirming EPEL repo is provisioned:               [ OK ]
Validating OpenJDK Java 8 JDK installation:         [ OK ]
Installing base dependencies (be patient):          [ OK ]
Installing EPEL dependencies (be patient):          [ OK ]
Generating unique machine-uuid:                   [ OK ]
Installing scripts and configuration files:         [ OK ]
Installing daily database backup:                  [ OK ]
Installing resty and friends:                     [ OK ]
Installing PM graph dependencies (be patient):      [ OK ]
Verifying PM graph framework:                     [ OK ]
Verifying PM tagging:                             [ OK ]
Verifying PM graph database:                      [ OK ]
Verifying PM graph storage:                       [ OK ]
Verifying PM graphing:                           [ OK ]
Initializing PM graphing database:                 [ OK ]
Configuring SNMP daemon:                          [ OK ]
Configuring NTP daemon:                           [ OK ]
Configuring OS:                                   [ OK ]
Configuring process supervision:                  [ OK ]
Generating file uninstall list                    [ OK ]

Script completed successfully

```



NOTE: All RPMs installed by the script, and all files created or updated by the script, are logged in `/root/uninstall.log`. The log is provided in case you want to manually uninstall the packages and/or remove the files that the script has installed. Because these packages and files are required for proper operation of the PSM server, you should only do this if you are no longer using this machine as a PSM server.

13. Reboot the server.

The reboot is necessary to ensure the path variables are set up properly.

14. After the server reboots, log back in and verify that the `$JAVA_HOME` variable is correctly set to reference the newly installed Java directory.

For example:

```
[root@psmdemo /]# echo $JAVA_HOME
/usr/lib/jvm/jre-openjdk
```

You have successfully installed and configured Red Hat (CentOS) Linux and all necessary packages for the PSM server.

Time Zones

/usr/share/zoneinfo/

Africa	Israel
America	Jamaica
Antarctica	Japan
Arctic	Kwajalein
Asia	Libya
Atlantic	MET
Australia	Mexico
Brazil	Mideast
Canada	MST
CET	MST7MDT
Chile	Navajo
CST6CDT	NZ
Cuba	NZ-CHAT
EET	Pacific
Egypt	Poland
Eire	Portugal
EST	posix
EST5EDT	posixrules
Etc	PRC
Europe	PST8PDT
Factory	right
GB	ROC
GB-Eire	ROK
GMT	Singapore
GMT0	Turkey
GMT-0	UCT
GMT+0	Universal
Greenwich	US
Hongkong	UTC
HST	WET
Iceland	W-SU
Indian	zone.tab

Iran

Zulu

iso3166.tab

/usr/share/zoneinfo/Africa:

Abidjan

Kampala

Accra

Khartoum

Addis_Ababa

Kigali

Algiers

Kinshasa

Asmara

Lagos

Asmera

Libreville

Bamako

Lome

Bangui

Luanda

Banjul

Lubumbashi

Bissau

Lusaka

Blantyre

Malabo

Brazzaville

Maputo

Bujumbura

Maseru

Cairo

Mbabane

Casablanca

Mogadishu

Ceuta

Monrovia

Conakry

Nairobi

Dakar

Ndamena

Dar_es_Salaam

Niamey

Djibouti

Nouakchott

Douala

Ouagadougou

EL_Aaiun

Porto-Novo

Freetown

Sao_Tome

Gaborone

Timbuktu

Harare

Tripoli

Johannesburg

Tunis

Windhoek

/usr/share/zoneinfo/America:

Anchorage	Lima
Anguilla	Los_Angeles
Antigua	Louisville
Araguaina	Maceio
Argentina	Managua
Aruba	Manaus
Asuncion	Marigot
Atikokan	Martinique
Atka	Mazatlan
Bahia	Mendoza
Barbados	Menominee
Belem	Merida
Belize	Mexico_City
Blanc-Sablon	Miquelon
Boa_Vista	Moncton
Bogota	Monterrey
Boise	Montevideo
Buenos_Aires	Montreal
Cambridge_Bay	Montserrat
Campo_Grande	Nassau
Cancun	New_York
Caracas	Nipigon
Catamarca	Nome
Cayenne	Noronha
Cayman	North_Dakota
Chicago	Panama
Chihuahua	Pangnirtung
Coral_Harbour	Paramaribo
Cordoba	Phoenix
Costa_Rica	Port-au-Prince
Cuiaba	Porto_Acre
Curacao	Port_of_Spain

Danmarkshavn	Porto_Velho
Dawson	Puerto_Rico
Dawson_Creek	Rainy_River
Denver	Rankin_Inlet
Detroit	Recife
Dominica	Regina
Edmonton	Resolute
Eirunepe	Rio_Branco
EL_Salvador	Rosario
Ensenada	Santarem
Fortaleza	Santiago
Fort_Wayne	Santo_Domingo
Glace_Bay	Sao_Paulo
Godthab	Scoresbysund
Goose_Bay	Shiprock
Grand_Turk	St_Barthelemy
Grenada	St_Johns
Guadeloupe	St_Kitts
Guatemala	St_Lucia
Guayaquil	St_Thomas
Guyana	St_Vincent
Halifax	Swift_Current
Havana	Tegucigalpa
Hermosillo	Thule
Indiana	Thunder_Bay
Indianapolis	Tijuana
Inuvik	Toronto
Iqaluit	Tortola
Jamaica	Vancouver
Jujuy	Virgin
Juneau	Whitehorse
Kentucky	Winnipeg

Knox_IN	Yakutat
La_Paz	Yellowknife

/usr/share/zoneinfo/America/Argentina:

Buenos_Aires	Rio_Gallegos
Catamarca	Salta
ComodRivadavia	San_Juan
Cordoba	San_Luis
Jujuy	Tucuman
La_Rioja	Ushuaia
Mendoza	

/usr/share/zoneinfo/America/Indiana:

Indianapolis	Tell_City
Knox	Vevay
Marengo	Vincennes
Petersburg	Winamac

/usr/share/zoneinfo/America/Kentucky:

Louisville	Monticello
------------	------------

/usr/share/zoneinfo/America/North_Dakota:

Center	New_Salem
--------	-----------

/usr/share/zoneinfo/Antarctica:

Casey	Palmer
Davis	Rothera
DumontDURville	South_Pole
Mawson	Syowa
McMurdo	Vostok

/usr/share/zoneinfo/Arctic:

Longyearbyen

/usr/share/zoneinfo/Asia:

Aden	Kuching
Almaty	Kuwait
Amman	Macao
Anadyr	Macau
Aqtau	Magadan
Aqtobe	Makassar
Ashgabat	Manila
Ashkhabad	Muscat
Baghdad	Nicosia
Bahrain	Novosibirsk
Baku	Omsk
Bangkok	Oral
Beirut	Phnom_Penh
Bishkek	Pontianak
Brunei	Pyongyang
Calcutta	Qatar
Choibalsan	Qyzylorda
Chongqing	Rangoon
Chungking	Riyadh
Colombo	Riyadh87
Dacca	Riyadh88
Damascus	Riyadh89
Dhaka	Saigon
Dili	Sakhalin
Dubai	Samarkand
Dushanbe	Seoul
Gaza	Shanghai
Harbin	Singapore
Ho_Chi_Minh	Taipei
Hong_Kong	Tashkent
Hovd	Tbilisi
Irkutsk	Tehran

Istanbul	Tel_Aviv
Jakarta	Thimbu
Jayapura	Thimphu
Jerusalem	Tokyo
Kabul	Ujung_Pandang
Kamchatka	Ulaanbaatar
Karachi	Ulan_Bator
Kashgar	Urumqi
Kathmandu	Vientiane
Katmandu	Vladivostok
Kolkata	Yakutsk
Krasnoyarsk	Yekaterinburg
Kuala_Lumpur	Yerevan

/usr/share/zoneinfo/Atlantic:

Azores	Jan_Mayen
Bermuda	Madeira
Canary	Reykjavik
Cape_Verde	South_Georgia
Faeroe	Stanley
Faroe	St_Helena

/usr/share/zoneinfo/Australia:

ACT	Melbourne
Adelaide	North
Brisbane	NSW
Broken_Hill	Perth
Canberra	Queensland
Currie	South
Darwin	Sydney
Eucla	Tasmania
Hobart	Victoria
LHI	West
Lindeman	Yancowinna
Lord_Howe	

/usr/share/zoneinfo/Brazil:

Acre	East
DeNoronha	West

/usr/share/zoneinfo/Canada:

Atlantic	Mountain
Central	Newfoundland
Eastern	Pacific
East-Saskatchewan	Saskatchewan
	Yukon

/usr/share/zoneinfo/Chile:

Continental	EasterIsland
-------------	--------------

/usr/share/zoneinfo/etc:

GMT	GMT-4
GMT0	GMT+4
GMT-0	GMT-5
GMT+0	GMT+5
GMT-1	GMT-6
GMT+1	GMT+6
GMT-10	GMT-7
GMT+10	GMT+7
GMT-11	GMT-8
GMT+11	GMT+8
GMT-12	GMT-9
GMT+12	GMT+9
GMT-13	Greenwich
GMT-14	UCT
GMT-2	Universal
GMT+2	UTC
GMT-3	Zulu
GMT+3	

/usr/share/zoneinfo/Europe:

Amsterdam	Monaco
Andorra	Moscow
Athens	Nicosia
Belfast	Oslo
Belgrade	Paris
Berlin	Podgorica
Bratislava	Prague
Brussels	Riga
Bucharest	Rome
Budapest	Samara
Chisinau	San_Marino
Copenhagen	Sarajevo
Dublin	Simferopol
Gibraltar	Skopje
Guernsey	Sofia
Helsinki	Stockholm
Isle_of_Man	Tallinn
Istanbul	Tirane
Jersey	Tiraspol
Kaliningrad	Uzhgorod
Kiev	Vaduz
Lisbon	Vatican
Ljubljana	Vienna
London	Vilnius
Luxembourg	Volgograd
Madrid	Warsaw
Malta	Zagreb
Mariehamn	Zaporozhye
Minsk	Zurich

/usr/share/zoneinfo/Indian:

Antananarivo	Mahe
Chagos	Maldives
Christmas	Mauritius
Cocos	Mayotte
Comoro	Reunion
Kerguelen	

/usr/share/zoneinfo/Mexico:

BajaNorte	General
BajaSur	

/usr/share/zoneinfo/Mideast:

Riyadh87	Riyadh89
Riyadh88	

/usr/share/zoneinfo/Pacific:

Apia	Midway
Auckland	Nauru
Chatham	Niue
Easter	Norfolk
Efate	Noumea
Enderbury	Pago_Pago
Fakaofu	Palau
Fiji	Ponape
Funafuti	Pitcairn
Galapagos	Port_Moresby
Gambier	Rarotonga
Guadalcanal	Saipan
Guam	Samoa
Honolulu	Tahiti
Johnston	Tarawa
Kiritimati	Tongatapu
Kosrae	Truk
Kwajalein	Wake
Majuro	Wallis
Marquesas	Yap
