

IBM PowerSC

Standard Edition

Version 1.1.0, 1.1.1, and 1.1.2

PowerSC Standard Edition

IBM

IBM PowerSC

Standard Edition

Version 1.1.0, 1.1.1, and 1.1.2

PowerSC Standard Edition

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 37.

This edition applies to IBM PowerSC Version 1.1.2.0, or earlier, and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2013, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	v	Detecting virtual log devices.	23
What's new in PowerSC Standard Edition 1.1.2, or earlier	1	Configuring Trusted Logging	24
PowerSC Standard Edition Release Notes Versions 1.1.2, or earlier	3	Configuring the AIX Audit subsystem	24
PowerSC Standard Edition 1.1.2, or earlier, concepts	5	Configuring syslog	25
Installing PowerSC Standard Edition 1.1.2, or earlier	7	Writing data to virtual log devices.	25
Trusted Boot	9	Trusted Network Connect and Patch management	27
Trusted Boot concepts	9	Trusted Network Connect concepts	27
Planning for Trusted Boot	9	Trusted Network Connect components	27
Trusted Boot prerequisites	10	Trusted Network Connect secure communication	28
Preparing for remediation	10	Trusted Network Connect protocol	28
Migration considerations	10	IMC and IMV modules	28
Installing Trusted Boot.	11	Installing Trusted Network Connect	29
Installing the collector	11	Configuring Trusted Network Connect and Patch management	30
Installing the verifier	11	Configuring Trusted Network Connect server	30
Configuring Trusted Boot.	11	Configuring Trusted Network Connect client	30
Enrolling a system	11	Configuring the patch management server	30
Attesting a system	12	Configuring Trusted Network Connect server email notification	31
Managing Trusted Boot	12	Configuring IP referrer on VIOS	32
Interpreting attestation results	12	Managing Trusted Network Connect and Patch management	32
Deleting systems	13	Viewing the Trusted Network Connect server logs	32
Troubleshooting Trusted Boot	13	Creating policies for the Trusted Network Connect client	33
Trusted Firewall	15	Starting verification for the Trusted Network Connect client	34
Trusted Firewall concepts.	15	Viewing the verification results of the Trusted Network Connect	34
Installing Trusted Firewall	17	Updating the Trusted Network Connect client	34
Configuring Trusted Firewall	18	Managing patch management policies	35
Multiple Shared Ethernet Adapters	18	Importing Trusted Network Connect certificates	35
Removing Shared Ethernet Adapters	19	Troubleshooting Trusted Network Connect and Patch management	35
Creating rules	20	Notices	37
Deactivating rules	21	Privacy policy considerations	39
Trusted Logging	23	Trademarks	39
Virtual logs	23	Index	41

About this document

This document provides system administrators with complete information about file, system, and network security.

Highlighting

The following highlighting conventions are used in this document:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
<i>Italics</i>	Identifies parameters whose actual names or values are to be supplied by the user.
Monospace	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

Case-sensitivity in AIX®

Everything in the AIX operating system is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type **LS**, the system responds that the command is not found. Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

What's new in PowerSC Standard Edition 1.1.2, or earlier

Read about new or significantly changed information for the PowerSC™ Standard Edition 1.1.2, or earlier, topic collection.

In this PDF file, you might see revision bars (|) in the left margin that identifies new and changed information.

November 2012

Updated the information in the “Trusted Network Connect and Patch management” on page 27 topic.

May 2012

Added the documentation for the new feature for “Trusted Firewall” on page 15.

PowerSC Standard Edition Release Notes Versions 1.1.2, or earlier

The release notes contain information about changes to PowerSC Standard Edition Versions 1.1.2, or earlier, that were identified after the documentation was completed.

What's new

Trusted Firewall for PowerSC Standard Edition provides virtualization-layer security that improves performance and resource efficiency when communicating across virtual local area networks (VLAN) on the same Virtual I/O Server (VIOS). By defining which types of communication to allow across selected VLANs, you can shorten the path of the communication. For more information about Trusted Firewall, see “Trusted Firewall” on page 15.

Read this before installation

To view the most current version of the Release Notes, go to the online Release Notes in the Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSTQK9_1.1.2/com.ibm.powersc112.se/powersc_se_rn.htm).

PowerSC Standard Edition is a licensed program, and is not included with the AIX operating system.

Note: This software might contain errors that could result in a critical business impact. Install the latest available fixes prior to using this software. To learn more about installing the PowerSC Standard Edition software, see “Installing PowerSC Standard Edition 1.1.2, or earlier” on page 7.

System requirements

The PowerSC Trusted Boot technology requires a minimum firmware level of eFW7.4 and either IBM® AIX Version 6 with Technology Level 7 or IBM AIX Version 7 with Technology Level 1. The OpenPTS Verifier component of Trusted Boot runs on the AIX operating system and other platforms. The AIX version can be installed from the AIX Expansion Pack. The OpenPTS Verifier for other platforms can be downloaded from Download Linux OpenPTS Verifier For Use With AIX Trusted Boot (<https://www.ibm.com/services/forms/preLogin.do?source=swg-openpts>).

PowerSC Trusted Boot is part of the PowerSC Standard Edition and does not apply to the PowerSC Express Edition.

The PowerSC Trusted Logging and the Trusted Network Connect and Patch Management offerings require Virtual I/O Server 2.2.1.0, or later.

The Trusted Network Connect client requires AIX Version 6.1 with the 6100-06 Technology Level, or higher, or the AIX Version 7.1 Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management.

Installation, migration, upgrade, and configuration information

For information about installing PowerSC Standard Edition, see “Installing PowerSC Standard Edition 1.1.2, or earlier” on page 7.

Limitations and restrictions

When you perform a complete reinstallation of the AIX operating system, the Trusted Boot feature requires that you back up the `/var/tss/lib/tpm/system.data` file and replace it in the same location after reinstallation is complete. Otherwise, you are required to remove and reinstall the virtualized Trusted Platform Module (vTPM) to the partition from the management console.

PowerSC Standard Edition 1.1.2, or earlier, concepts

This overview of PowerSC Standard Edition explains the features, components, and the hardware support related to the PowerSC Standard Edition feature.

PowerSC Standard Edition provides security and control of the systems operating within a cloud or in virtualized data centers, and provides an enterprise view and management capabilities. PowerSC Standard Edition is a suite of features that includes Security and Compliance Automation, Trusted Boot, Trusted Firewall, Trusted Logging, and Trusted Network Connect and Patch management. The security technology that is placed within the virtualization layer provides additional security to stand-alone systems.

The following table provides details about the editions, the features included in the editions, the components, and the processor-based hardware on which each component is available.

Table 1. PowerSC Standard Edition components, description, operating system support, and hardware support

Components	Description	Operating system supported	Hardware supported
Security and Compliance Automation	Automates the setting, monitoring, and auditing of security and compliance configuration for the following standards: <ul style="list-style-type: none"> • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA) 	<ul style="list-style-type: none"> • AIX 5.3 • AIX 6.1 • AIX 7.1 	<ul style="list-style-type: none"> • POWER5 • POWER6® • POWER7®
Trusted Boot	Measures the boot image, operating system, and applications, and attests their trust by using the virtual trusted platform module (TPM) technology.	AIX 7.1	POWER7 firmware eFW7.4, or later
Trusted Firewall	Saves time and resources by enabling direct routing across specified virtual LANs (VLANs) that are controlled by the same Virtual I/O Server.	<ul style="list-style-type: none"> • AIX 6.1 • AIX 7.1 • VIOS Version 2.2.1.4, or later 	<ul style="list-style-type: none"> • POWER6 • POWER7 • Virtual I/O Server Version 6.1S, or later
Trusted Logging	The logs of AIX are centrally located on the Virtual I/O Server (VIOS) in real time. This feature provides tamperproof logging and convenient log backup and management.	<ul style="list-style-type: none"> • AIX 5.3 • AIX 6.1 • AIX 7.1 	<ul style="list-style-type: none"> • POWER5 • POWER6 • POWER7

| *Table 1. PowerSC Standard Edition components, description, operating system support, and hardware support (continued)*

Components	Description	Operating system supported	Hardware supported
Trusted Network Connect and patch management	Verifies that all AIX systems in the virtual environment are at the specified software and patch level and provides management tools to ensure that all AIX systems are at the specified software level. Provides alerts if a down-level virtual system is added to the network or if a security patch is issued that affects the systems.	<ul style="list-style-type: none"> • AIX 5.3 • AIX 6.1 • AIX 7.1 	<ul style="list-style-type: none"> • POWER5 • POWER6 • POWER7

Installing PowerSC Standard Edition 1.1.2, or earlier

You must install a fileset for each specific function of PowerSC Standard Edition.

The following filesets are available for PowerSC Standard Edition:

- `powerscExp.ice`: Installed on AIX systems that require the Security and Compliance Automation feature of PowerSC Standard Edition.
- `powerscStd.vtpm`: Installed on AIX systems that require the Trusted Boot feature of PowerSC Standard Edition.
- `powerscStd.vlog`: Installed on AIX systems that require the Trusted Logging feature of PowerSC Standard Edition.
- `powerscStd.tnc_pm`: Installed on the AIX Version 6.1 with the 6100-06 Technology Level, or higher, or on the AIX Version 7.1 Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management.
- `powerscStd.svm`: Installed on AIX systems that might benefit from the routing feature of PowerSC Standard Edition.

Install PowerSC Standard Edition by using one of the following interfaces:

- The **installp** command from the command-line interface (CLI)
- The SMIT interface

To install PowerSC Standard Edition by using the SMIT interface, complete the following steps:

1. Run the following command:

```
% smitty installp
```
2. Select the **Install Software** option.
3. Select the input device or directory for the software to specify the location and the installation file of the IBM Compliance Expert installation image. For example, if the installation image has the directory path and file name `/usr/sys/inst.images/powerscStd.vtpm`, you must specify the file path in the **INPUT** field.
4. View and accept the license agreement. Accept the license agreement by using the down arrow to select **ACCEPT new license agreements**, and press the tab key to change the value to **Yes**.
5. Press **Enter** to start the installation.
6. Verify that the command status is **OK** after the installation is complete.

Viewing software license

The software license can be viewed in the CLI by using the following command:

```
% installp -lE -d path/filename
```

Where *path/filename* specifies the PowerSC Standard Edition installation image.

For example, you can enter the following command using the CLI to specify the license information related to the PowerSC Standard Edition:

```
% installp -lE -d /usr/sys/inst.images/powerscStd.vtpm
```

Related concepts:

“PowerSC Standard Edition 1.1.2, or earlier, concepts” on page 5

This overview of PowerSC Standard Edition explains the features, components, and the hardware support related to the PowerSC Standard Edition feature.

“Installing Trusted Boot” on page 11

There are some required hardware and software configurations that are required to install Trusted Boot.

“Installing Trusted Network Connect” on page 29

Installing the components of Trusted Network Connect (TNC) requires you to complete certain steps.

Related tasks:

“Installing Trusted Firewall” on page 17

Installing the PowerSC Trusted Firewall is similar to installing other PowerSC features.

Trusted Boot

The Trusted Boot feature uses the Virtual Trusted Platform Module (VTPM), which is a virtual instance of the Trusted Computing Group's TPM. The VTPM is used to securely store measurements of the system boot for future verification.

Trusted Boot concepts

It is important to understand the integrity of the boot process and how to classify the boot as a trusted boot or a nontrusted boot.

You can configure a maximum of 60 VTPM-enabled logical partitions (LPAR) for each physical system by using the Hardware Management Console (HMC). When configured, the VTPM is unique to each LPAR. When used with the AIX Trusted Execution technology, the VTPM provides security and assurance to the following partitions:

- The boot image on the disk
- The entire operating system
- The application layers

An administrator can view trusted and nontrusted systems from a central console that is installed with the **openpts** verifier that is available on the AIX expansion pack. The **openpts** console manages one or more Power Systems™ servers, and monitors or attests the trusted state of AIX systems throughout the data center. Attestation is the process where the verifier determines (or attests) if a collector has performed a trusted boot.

Trusted boot status

A partition is said to be trusted if the verifier successfully attests the integrity of the collector. The verifier is the remote partition that determines if a collector has performed a trusted boot. The collector is the AIX partition that has a Virtual Trusted Platform Module (VTPM) attached and the Trusted Software Stack (TSS) installed. It indicates that the measurements that are recorded within the VTPM match a reference set held by the verifier. A trusted boot state indicates whether the partition booted in a trusted manner. This statement is about the integrity of the system boot process and does not indicate the current or ongoing level of the security of the system.

Nontrusted boot status

A partition enters a nontrusted state if the verifier cannot successfully attest the integrity of the boot process. The nontrusted state indicates that some aspect of the boot process is inconsistent with the reference information held by the verifier. The possible causes for a failed attestation include booting from a different boot device, booting a different kernel image, and changing the existing boot image.

Related concepts:

“Troubleshooting Trusted Boot” on page 13

There are some of the common scenarios and remedial steps that are required to help identify the reason for attestation failure when using Trusted Boot.

Planning for Trusted Boot

Learn about the hardware and software configurations that are required to install Trusted Boot.

Trusted Boot prerequisites

The installation of Trusted Boot involves configuring the collector and the verifier.

Collector

The configuration requirements to install a collector involves the following prerequisites:

- POWER7 hardware that is running on a 740 firmware release.
- Install IBM AIX 6 with Technology Level 7 or install IBM AIX 7 with Technology Level 1.
- Install Hardware Management Console (HMC) version 7.4 or later.
- Configure the partition with the VTPM and a minimum of 1 GB memory.
- Install Secure Shell (SSH), specifically OpenSSH or equivalent.

Verifier

The **openpts** verifier can be accessed from the command-line interface and the graphical user interface that is designed to run on a range of platforms. The AIX version of the OpenPTS verifier is available on the AIX expansion pack. The versions of OpenPTS verifier for Linux and other platforms are available through a web download. The configuration requirements include the following prerequisites:

- Install SSH, specifically OpenSSH or equivalent.
- Establish network connectivity (through SSH) to the collector.
- Install Java™ 1.6 or later to access the **openpts** console from the graphical interface.

Preparing for remediation

The Trusted Boot information that is described here serves as a guide to identifying situations that might require remediation. It does not affect the boot process.

There are many circumstances that can cause an attestation to fail, and it is difficult to predict the circumstance you might encounter. You must decide on the appropriate action depending on the circumstance. However, it is good practice to prepare for some of the severe scenarios and have a policy or a workflow to help you to handle such incidents. Remediation is the corrective action that must be taken when attestation reports one or more collectors are not trusted.

For example, if an attestation failure occurred due to the boot image differing from the verifier's reference, consider having answers to the following questions:

- How can you verify that the threat is credible?
- Was there any planned maintenance that was carried out, an AIX upgrade, or new hardware that was recently installed?
- Can you contact the administrator who has access to this information?
- When was the system last booted in a trusted state?
- If the security threat looks legitimate, what action must you take? (Suggestions include collecting audit logs, disconnecting the system from the network, powering the system down, and alerting users).
- Were there any other systems compromised that must be checked?

Related concepts:

“Troubleshooting Trusted Boot” on page 13

There are some of the common scenarios and remedial steps that are required to help identify the reason for attestation failure when using Trusted Boot.

Migration considerations

Consider these prerequisites before you migrate a partition enables for virtual trusted platform module (VTPM).

An advantage of a VTPM over a physical TPM is that it allows the partition to move between systems while retaining the VTPM. To securely migrate the logical partition, the firmware encrypts the VTPM data before transmission. To ensure a secure migration, the following security measures must be implemented before migration:

- Enable IPSEC between the Virtual I/O Server (VIOS) that is performing the migration.
- Set the trusted system key through the Hardware Management Console (HMC) to control the managed systems that are capable of decrypting the VTPM data after migration. The migration destination system must have the same key as that of the source system to successfully migrate the data.

Related information:

 [Using HMC](#)

 [VIOS migration](#)

Installing Trusted Boot

There are some required hardware and software configurations that are required to install Trusted Boot.

Related information:

“Installing PowerSC Standard Edition 1.1.2, or earlier” on page 7

You must install a fileset for each specific function of PowerSC Standard Edition.

Installing the collector

You must install the collector by using the fileset from the AIX base CD.

To install the collector, install the `powerscStd.vtpm` and `openpts.collector` packages which are on the base CD, by using the `smit` or `installp` command.

Installing the verifier

The verifier can be installed from the fileset by using the expansion pack.

To install the verifier on the AIX operating system, install the `openpts.verifier` package from the AIX expansion pack by using the `smit` or `installp` command. This installs both the command line and graphical interface versions of the verifier.

Configuring Trusted Boot

Learn the procedure to enroll a system and to attest a system for Trusted Boot.

Enrolling a system

Learn the procedure to enroll a system with the verifier.

Enrolling a system is the process of providing an initial set of measurements to the verifier, which forms the basis for subsequent attestation requests. To enroll a system from the command line, use the following command from the verifier:

```
openpts -i <hostname>
```

Information about the enrolled partition is located in the `$HOME/.openpts` directory. Each new partition is assigned with a unique identifier during the enrollment process and information related to the enrolled partitions is stored in the directory corresponding to the unique ID.

To enroll a system from the graphical interface, complete the following steps:

1. Launch the graphical interface by using `/opt/ibm/openpts_gui/openpts_GUI.sh` command.
2. Select **Enroll** from the navigation menu.

3. Enter the host name and the SSH credentials of the system.
4. Click **Enroll**.

Related concepts:

“Attesting a system”

Learn the procedure to attest a system from the command-line and by using the graphical interface.

Attesting a system

Learn the procedure to attest a system from the command-line and by using the graphical interface.

To query the integrity of a system boot, use the following command from the verifier:

```
openpts <hostname>
```

To attest a system from the graphical interface, complete the following steps:

1. Select a category from the navigation menu.
2. Select one or more systems to attest.
3. Click **Attest**.

Enrolling and attesting a system without a password

The attestation request is sent through the Secure Shell (SSH). Install the verifier’s certificate on the collector to permit SSH connections without a password.

To set up the verifier's certificate on the collector’s system, complete the following steps :

- On the verifier, run the following commands:

```
ssh-keygen # No passphrase  
scp ~/.ssh/id_rsa.pub <collector>:/tmp
```

- On the collector, run the following command:

```
cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys
```

Managing Trusted Boot

Learn the procedure to manage the attestation results of Trusted Boot.

Interpreting attestation results

Learn the procedure to view and understand the attestation results.

An attestation can result in one of following states:

1. Attestation request failed: The attestation request did not complete successfully. See the Troubleshooting section to understand the possible causes for the failure.
2. System integrity valid: The attestation completed successfully, and the system boot matches the reference information that is held by the verifier. This indicates a successful Trusted Boot.
3. System integrity invalid: The attestation request completed, but a discrepancy was detected between the information that is collected during system boot and the reference information that is held by the verifier. This indicates a nontrusted boot.

The attestation also reports whether an update was applied to the collector by using the following message:

System update available: This message indicates that an update was applied on the collector and a set of updated reference information is available that is effective for the next boot. The user is prompted on the verifier to accept or reject the updates. For example, the user can choose to accept these updates if the user is aware of the maintenance occurring on the collector.

To investigate an attestation failure by using the graphical interface, complete the following steps:

1. Select a category from the navigation menu.
2. Select a system to investigate.
3. Double-click the entry corresponding to the system. A properties window is displayed. This window contains log information about the failed attestation.

Deleting systems

Learn the procedure to delete a system from the verifier's database.

To remove a system from the database of the verifier, run the following command:

```
openpts -r <hostname>
```

Troubleshooting Trusted Boot

There are some of the common scenarios and remedial steps that are required to help identify the reason for attestation failure when using Trusted Boot.

The **openpts** command declares a system as invalid if the current boot state of the system does not match the reference information that is held on the verifier. The **openpts** command determines the possible reason for the integrity to be invalid. There are several variables in a full AIX boot, and a failed attestation requires analysis to determine the cause of the failure.

The following table lists some of the common scenarios and remedial steps to identify the reason for the failure:

Table 2. Troubleshooting some of the common scenarios for failure

Reason for failure	Possible causes of failure	Suggested remediation
Attestation did not complete.	<ul style="list-style-type: none"> • Incorrect host name. • No network route between the source and destination. • Incorrect security credentials. 	<p>Check the Secure Shell (SSH) connection using the following command:</p> <pre>ssh ptsc@hostname</pre> <p>If the SSH connection is successful, then check for the following reasons for attestation failure:</p> <ul style="list-style-type: none"> • The system that is being attested is not running the tcsd daemon. • The system that is being attested was not initialized by the ptsc command. This process should occur automatically during the system startup but check for the presence of a <code>/var/ptsc/</code> directory on the collector. If the <code>/var/ptsc/</code> directory does not exist, run the following command on the collector: <pre>ptsc -i</pre>
The CEC firmware was changed.	<ul style="list-style-type: none"> • A firmware upgrade was applied. • The LPAR was migrated to a system that was running a different version of the firmware. 	Check the firmware level of the system that is hosting the LPAR.
The resources allocated to the LPAR changed.	The CPU or memory allocated to the LPAR changed.	Check the partition profile in the HMC.
The firmware changed for the adapters that are available in the LPAR.	A hardware device was added or removed from the LPAR.	Check the partition profile in the HMC.

Table 2. Troubleshooting some of the common scenarios for failure (continued)

Reason for failure	Possible causes of failure	Suggested remediation
The list of devices attached to the LPAR was changed.	A hardware device was added or removed from the LPAR.	Check the partition profile in the HMC.
The boot image changed, which includes the operating system kernel.	<ul style="list-style-type: none"> An AIX update was applied and the verifier was unaware of the update. The bosboot command was run. 	<ul style="list-style-type: none"> Confirm with the administrator of the collector whether any maintenance was performed before the latest reboot operation. Check the logs on the collector for maintenance activity.
The LPAR is booted from a different device.	<ul style="list-style-type: none"> Enrollment was carried out immediately after network installation. The system is booted from a maintenance device. 	The boot device and flags can be checked by using the bootinfo command. If enrollment was carried out immediately after Network Installation Management (NIM) installation and before the reboot operation, the enrolled details pertain to the network installation and not to the next disk boot. This enrollment can be repaired by removing the enrollment and re-enrolling the logical partition.
The interactive System Management Services (SMS) boot menu was called.		The boot process must run uninterrupted without user interaction for a system to be trusted. Entering the SMS boot menu causes the boot to be invalid.
The trusted execution (TE) database was altered.	<ul style="list-style-type: none"> Binary files were added or removed from the TE database. Binary files in the database were updated. 	Run the trustchk command to verify the database.

Related concepts:

“Preparing for remediation” on page 10

The Trusted Boot information that is described here serves as a guide to identifying situations that might require remediation. It does not affect the boot process.

“Trusted Boot concepts” on page 9

It is important to understand the integrity of the boot process and how to classify the boot as a trusted boot or a nontrusted boot.

Related information:

 Using HMC

Trusted Firewall

The Trusted Firewall feature provides virtualization-layer security that improves performance and resource efficiency when communicating between different virtual LAN (VLAN) security zones on the same Power Systems server. Trusted Firewall decreases the load on the external network by moving the filtering capability of firewall packets meeting specified rules to the virtualization layer. This filtering capability is controlled by easily defined network filter rules, which allow trusted network traffic to cross between VLAN security zones without leaving the virtual environment. Trusted Firewall protects and routes internal network traffic between the AIX, IBM i, and Linux operating systems.

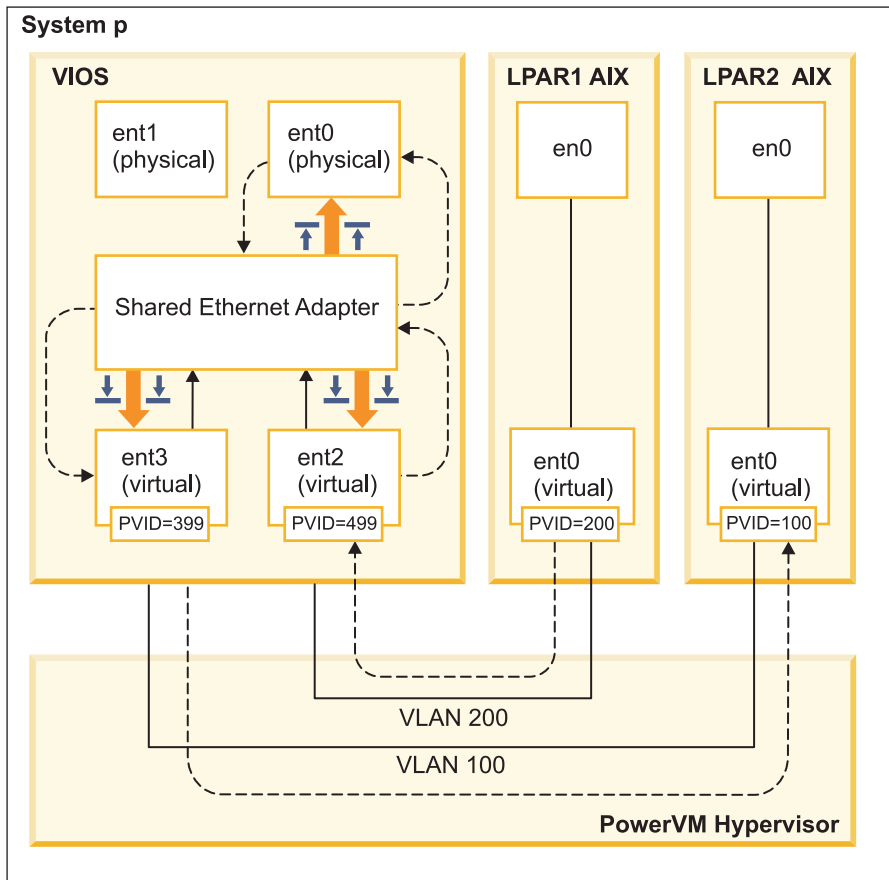
Trusted Firewall concepts

There are some basic concepts to understand when using Trusted Firewall.

Power Systems hardware can be configured with multiple virtual LAN (VLAN) security zones. A user-configured policy, created as a Trusted Firewall filter rule, permits some trusted network traffic to cross VLAN security zones and remain internal to the virtualization layer. This is similar to introducing a network-attached physical firewall into the virtualized environment, which provides a more performance-efficient method of implementing firewall capabilities for virtualized data centers.

With Trusted Firewall, you can configure rules to allow certain types of traffic to transfer directly from one VLAN on a Virtual I/O Server (VIOS) to another VLAN on the same VIOS, while still maintaining a high level of security by limiting other types of traffic. It is a configurable firewall within the virtualization layer of Power Systems servers.

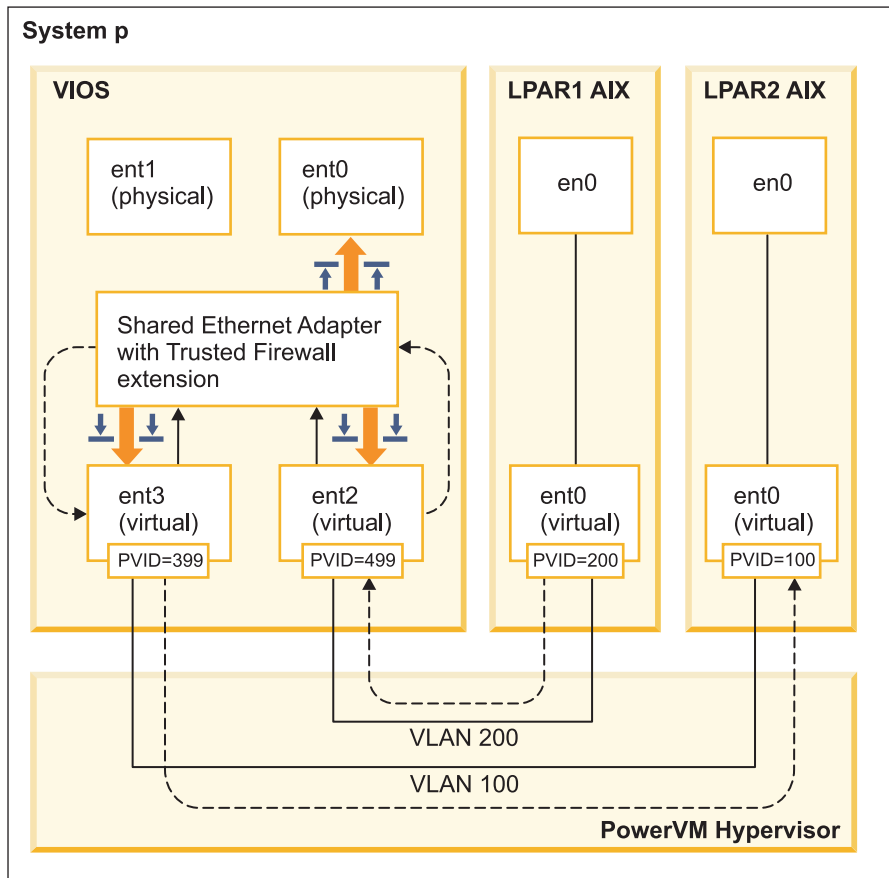
Using the example in Figure 1 on page 16, the goal is to be able to transfer information securely and efficiently from LPAR1 on VLAN 200 and from LPAR2 on VLAN 100. Without Trusted Firewall, information targeted for LPAR2 from LPAR1 is sent out of the internal network to the router, which routes the information back to LPAR2.



TFW502-3

Figure 1. Example of cross-VLAN information transfer without Trusted Firewall

Using Trusted Firewall, you can configure rules to allow the information to pass from LPAR1 to LPAR2 without leaving the internal network. This path is shown in Figure 2 on page 17.



TFW503-4

Figure 2. Example of cross-VLAN information transfer with Trusted Firewall

Configuration rules that allow certain information to pass securely across VLANs shorten the path to its destination. The Trusted Firewall uses the Shared Ethernet Adapter (SEA) and the Security Virtual Machine (SVM) kernel extension to enable the communication.

Shared Ethernet Adapter

The SEA is where the routing begins and ends. When the SVM is registered, the SEA receives the packets and forwards them to the SVM. If the SVM determines that the packet is for an LPAR on the same Power Systems server, it updates the packet's layer 2 header. The packet is returned to the SEA for forwarding to the final destination either within the system or on the external network.

Security Virtual Machine

The SVM is where the filtering rules are applied. The filtering rules are necessary to maintain security on the internal network. After registering the SVM with the SEA, the packets are forwarded to the SVM before being sent to the external network. Based on the active filter rules, the SVM determines whether a packet stays in the internal network or moves to the external network.

Installing Trusted Firewall

Installing the PowerSC Trusted Firewall is similar to installing other PowerSC features.

Prerequisites:

- PowerSC versions prior to 1.1.1.0 did not have the required fileset to install Trusted Firewall. Ensure that you have the PowerSC installation CD for version 1.1.1.0, or later.

- To take advantage of Trusted Firewall, you must have already used the Hardware Management Console (HMC) or Virtual I/O Server (VIOS) to configure your Virtual LANs (VLANs).

Trusted Firewall is provided as an additional fileset on the PowerSC Standard Edition installation CD. The file name is `powerscStd.svm.rte`. You can add the Trusted Firewall to an existing instance of PowerSC Version 1.1.0.0, or later, or install it as part of a new installation of PowerSC Version 1.1.1.0, or later.

To add the Trusted Firewall function to an existing PowerSC instance:

1. Ensure that you are running VIOS Version 2.2.1.4, or later.
2. Insert the PowerSC installation CD for version 1.1.1.0 or download the image of the installation CD.
3. Use the `oem_setup_env` command for root access.
4. Use the `installp` command or the SMIT tool to install the `PowerscStd.svm.rte` fileset.

Related information:

“Installing PowerSC Standard Edition 1.1.2, or earlier” on page 7

You must install a fileset for each specific function of PowerSC Standard Edition.

Configuring Trusted Firewall

Additional configuration settings are required for the Trusted Firewall feature after it is installed.

Multiple Shared Ethernet Adapters

You can configure Trusted Firewall on systems that use multiple Shared Ethernet Adapters.

Some configurations use multiple Shared Ethernet Adapters (SEAs) on the same Virtual I/O Server (VIOS). Multiple SEAs can provide benefits of failover protection and resource leveling. Trusted Firewall supports routing across multiple SEAs, provided they are on the same VIOS.

Figure 3 on page 19 shows an environment using multiple SEAs.

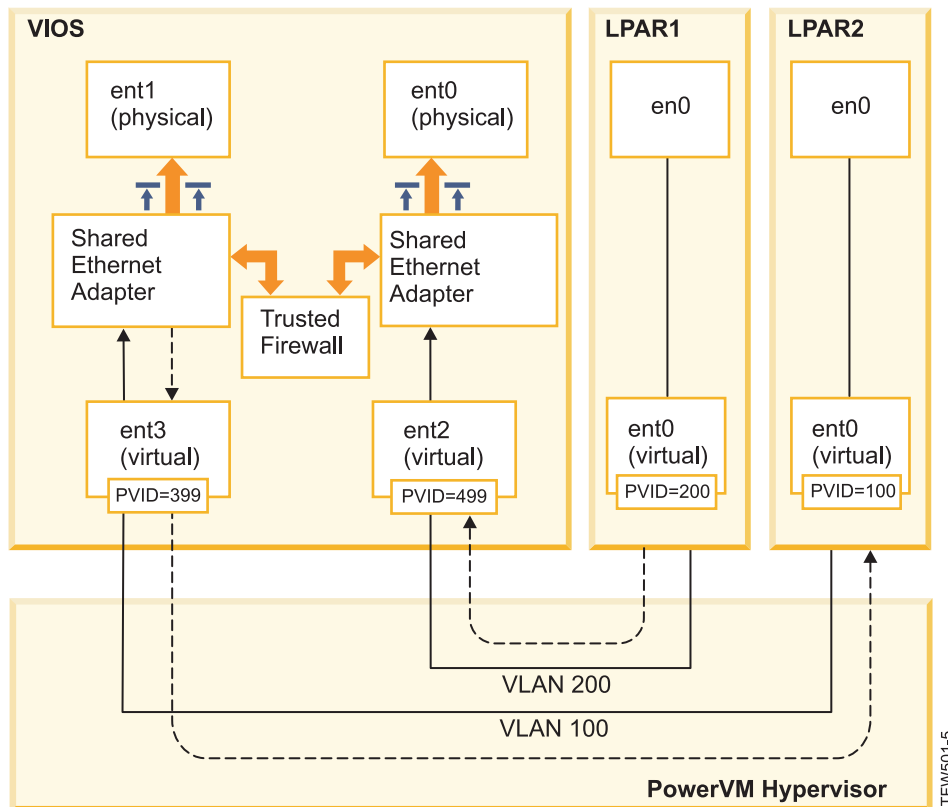


Figure 3. Configuration using multiple Shared Ethernet Adapters on a single VIOS

The following are examples of multiple SEA configurations that are supported by Trusted Firewall:

- The SEAs are configured with trunk adapters on the same Power® hypervisor virtual switch. This configuration is supported because each SEA receives network traffic with different VLAN IDs.
- The SEAs are configured with trunk adapters on different Power hypervisor virtual switches, and each trunk adapter is on a different VLAN ID. In this configuration, each SEA still receives network traffic by using different VLAN IDs.
- The SEAs are configured with trunk adapters on different Power hypervisor virtual switches, and the same VLAN IDs are reused on the virtual switches. In this case, the traffic for both SEAs has the same VLAN IDs.

An example of this configuration is having LPAR2 on VLAN200 with virtual switch 10 and LPAR3 on VLAN200 with virtual switch 20. Because both LPARs and their corresponding SEAs use the same VLAN ID (VLAN200), both of the SEAs have access to the packets with that VLAN ID.

You cannot enable bridging on more than one VIOS. For this reason, the following multiple SEA configurations are not supported by Trusted Firewall:

- Multiple VIOS and multiple SEA drivers.
- Redundant SEA load sharing: Trunk adapters that are configured for inter-VLAN routing cannot be split between VIOS servers.

Removing Shared Ethernet Adapters

The steps to remove Shared Ethernet Adapter devices from the system must be performed in a specific order.

To remove a Shared Ethernet Adapter (SEA) from your system, complete the following steps:

1. Remove the Security Virtual Machine that is associated with the SEA by entering the following command:

```
rmdev -dev svm
```
2. Remove the SEA by entering the following command:

```
rmdev -dev shared ethernet adapter ID
```

Note: Removing the SEA before removing the SVM can result in system failure.

Creating rules

You can create rules to enable Trusted Firewall cross-VLAN routing.

To enable the routing features of Trusted Firewall, you must create rules specifying which communications are allowed. For enhanced security, there is no single rule that allows communication between all of the VLANs on the system. Each allowed connection requires its own rule, though each rule that is activated allows communication in both directions for its specified endpoints.

Because the rule creation is created in the Virtual I/O Server (VIOS) interface, additional information about the commands is available in the VIOS topic collection in the Power Systems Hardware Information Center.

To create a rule, complete the following steps:

1. Open the VIOS command-line interface.
2. Initialize the SVM driver by entering the following command:

```
mksvm
```
3. Start Trusted Firewall by entering the start command:

```
vlantfw -s
```
4. To display all known LPAR IP and MAC addresses, enter the following command:

```
vlantfw -d
```

You will need the IP and MAC addresses of the logical partitions (LPARs) for which you are creating rules.

5. Create the filter rule to allow communication between the two LPARs (LPAR1 and LPAR2) by entering one of the following commands:
 - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]`
 - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]-o any -p 0 -0 gt -P 23`

Note: One filter rule allows communication in both directions by default, depending on port and protocol entries. For example, you can enable Telnet for LPAR1 to LPAR2 by running the following command:

```
genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress] -o any -p 0 -0 eq -P 23
```

6. Activate all of the filter rules in the kernel by entering the following command:

```
mkvfilt -u
```

Note: This procedure activates this rule and any other filtering rules that exist on the system.

Additional examples

The following examples show some other filter rules that you can create by using Trusted Firewall.

- To allow Secure Shell communication from the LPAR on VLAN 100 to the LPAR on VLAN 200, enter the following command:

```
genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -0 eq -P 22 -c tcp
```

- To allow traffic between all of the ports 0 - 499, enter the following command:

```
genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -0 lt -P 500 -c tcp
```

- To allow all TCP traffic between the LPARs, enter the following command:

```
genvfilt -v4 -a P -z 100 -Z 200 -c tcp
```

If you do not specify any ports or port operations, the traffic can use all ports.

- To allow Internet Control Message Protocol messaging between LPARs, enter the following command:

```
genvfilt -v4 -a P -z 100 -Z 200 -c icmp
```

Related concepts:

“Deactivating rules”

You can deactivate rules that enable cross-VLAN routing in the Trusted Firewall feature.

Related information:

Virtual I/O Server

genvfilt command

mkvfilt command

vlantfw command

Deactivating rules

You can deactivate rules that enable cross-VLAN routing in the Trusted Firewall feature.

Because the rules are deactivated in the Virtual I/O Server (VIOS) interface, additional information about the commands and process are available in the VIOS topic collection in the Power Systems Hardware Information Center.

To deactivate a rule, complete the following steps:

1. Open the VIOS command-line interface.
2. To display all active filter rules, enter the following command:

```
lsvfilt -a
```

You can omit the **-a** flag to display all of the filter rules stored in the Object Data Manager.

3. Note the identification number for the filter rule that you are deactivating. For this example, the identification number of the filter rule is 23.
4. Deactivate filter rule 23 when it is active in the kernel by entering the following command:

```
rmvfilt -n 23
```

To deactivate all of the filter rules in the kernel, enter the following command:

```
rmvfilt -n all
```

Related concepts:

“Creating rules” on page 20

You can create rules to enable Trusted Firewall cross-VLAN routing.

Related information:

lsvfilt command

rmvfilt command

Trusted Logging

PowerVM® Trusted Logging lets AIX LPARs write to log files that are stored on an attached Virtual I/O Server (VIOS). Data is transmitted to the VIOS directly through the hypervisor, and network connectivity is not required between the client LPAR and the VIOS.

The prerequisites for installing Trusted Logging are VIOS 2.2.1.0 and IBM AIX 6 with Technology Level 7 or IBM AIX 7 with Technology Level 1.

Virtual logs

The Virtual I/O Server (VIOS) administrator creates and manages the log files, and they are presented to the AIX operating system as virtual log devices in the /dev directory, similar to the virtual disks or virtual optical media.

Storing log files as virtual logs increases the level of trust in the records because they cannot be changed by a user with root privileges on the client LPAR where they were generated. Multiple virtual log devices can be attached to the same client LPAR and each log is a different file in the /dev directory.

Trusted Logging lets log data from multiple client LPARs be consolidated into a single file system, which is accessible from the VIOS. Therefore, the VIOS provides a single location on the system for log analysis and archival. The client LPAR administrator can configure applications and the AIX operating system to write data to the virtual log devices, which is similar to writing data to the local files. The AIX Audit subsystem can be configured to direct the audit records to virtual logs, and other AIX services, such as syslog, work with their existing configuration to direct data to virtual logs.


To configure the virtual log, the VIOS administrator must specify a name for the virtual log, which has the following separate components:

- Client name
- Log name

The names of the two components can be set by the VIOS administrator to any value, but the client name is typically the same for all virtual logs that are attached to a given LPAR (for example, the LPAR's host name). The log name is used to identify the purpose of the log (for example, audit or syslog).

On an AIX LPAR, each virtual log device is present as two functionally equivalent files in the /dev file system. The first file is named after the device, for example, /dev/vlog0, and the second file is named by concatenating a vl prefix with the log name and the device number. For example, if the virtual log device vlog0 has audit as the log name, it is present in the /dev file system as both vlog0 and vlaudit0.

Related information:

 [Creating virtual logs](#)

Detecting virtual log devices

After a VIOS administrator has created virtual log devices and attached them to a client LPAR, the client LPAR device configuration must be refreshed for the devices to be visible.

The client LPAR administrator refreshes the settings by using one of the following methods:

- Rebooting the client LPAR
- Running the **cfgmgr** command

Run the **lsdev** command to display the virtual log devices. The devices are prefixed with **vlog** by default. An example of the **lsdev** command output on an AIX LPAR on which two virtual logs devices are present is as follows:

```
lsdev
vlog0 Virtual Log Device
vlog1 Virtual Log Device
```

Inspect the properties of an individual virtual log device by using the **lsattr -El <device name>** command, which produces output that is similar to the following :

```
lsattr -El vlog0
PCM                Path Control Module          False
client_name        dev-lpar-05 Client Name                   False
device_name        vlsyslog0 Device Name                    False
log_name           syslog Log Name                       False
max_log_size       4194304 Maximum Size of Log Data File  False
max_state_size     2097152 Maximum Size of Log State File False
pvid               none Physical Volume Identifier  False
```

This output displays the client name, device name, and the amount of log data that VIOS can store.

The virtual log stores two types of log data, which are:

- Log data: The raw log data generated by applications on the AIX LPAR.
- State data: Information about when the devices were configured, opened, closed, and other operations that are used to analyze log activity.

The VIOS administrator specifies the amount of **log data** and **state data** that can be stored for each virtual log, and the amount is indicated by the **max_log_size**, and **max_state_size** attributes. When the amount of stored data exceeds the specified limit, the earliest log data is overwritten. The VIOS administrator must ensure that the log data is collected and archived frequently to preserve the logs.

Configuring Trusted Logging

Learn the procedure to configure Trusted Logging on the AIX Audit subsystem, and syslog.

Configuring the AIX Audit subsystem

The AIX Audit subsystem can be configured to write binary data to a virtual log device in addition to writing logs to the local file system.

Note: Before you configure the AIX Audit subsystem, you must complete the procedure in “Detecting virtual log devices” on page 23.

To configure the AIX Audit subsystem, complete the following steps:

1. Configure the AIX Audit subsystem to log data in binary (**auditbin**) mode.
2. Activate Trusted Logging for AIX auditing by editing the **/etc/security/audit/config** configuration file.
3. Add a **virtual_log = /dev/vlog0** parameter to **bin:** stanza.

Note: The instruction is valid if the LPAR administrator wants **auditbin** data to be written to the **/dev/vlog0**.

4. Restart the AIX Audit subsystem in the following sequence:

```
audit shutdown
audit start
```


The audit records are written to Virtual I/O Server (VIOS) through the specified virtual log device in addition to writing logs to the local file system. The logs are stored under control of the existing `bin1` and `bin2` parameters in the `bin:` stanza of the `/etc/security/audit/config` configuration file.

Related information:

Auditing subsystem

Configuring syslog

Syslog can be configured to write messages to virtual logs by adding rules to the `/etc/syslog.conf` file.

Note: Before you configure the `/etc/syslog.conf` file, you must complete the procedure in “Detecting virtual log devices” on page 23.

You can edit the `/etc/syslog.conf` file to match the log messages, which are based on the following criteria:

- Facility
- Priority level

To use the virtual logs for syslog messages, the `/etc/syslog.conf` file must be configured with rules to write the desired messages to the appropriate virtual log in the `/dev` directory.

For example, to send debug-level messages that are generated by any facility to the `vlog0` virtual log, add the following line to the `/etc/syslog.conf` file:

```
*.debug /dev/vlog0
```

Note: Do not use the log rotation facilities that are available in the `syslogd` daemon for any command that writes data to virtual logs. The files in the `/dev` file system are not regular files and they cannot be renamed and moved. The VIOS administrator must configure virtual log rotation within the VIOS.

The `syslogd` daemon must be restarted after the configuration by using the following command:

```
refresh -s syslogd
```

Related information:

`syslogd` Daemon

Writing data to virtual log devices

Arbitrary data is written to a virtual log device by opening the appropriate file in the `/dev` directory and writing data to the file. A virtual log can be opened by one process at a time.

For example:

To write messages to the virtual log devices by using the `echo` command, enter the following command:

```
echo "Log Message" > /dev/vlog0
```

To store files to the virtual log devices by using the `cat` command, enter the following command:

```
cat /etc/passwd > /dev/vlog0
```

The maximum individual write size is limited to 32 KB, and programs that attempt to write more data in a single write operation receive an I/O (EIO) error. The command-line interface (CLI) utilities, such as the `cat` command, automatically break up the transfers into 32 KB write operations.

Trusted Network Connect and Patch management

Trusted Network Connect (TNC) is part of the trusted computing group (TCG) that provides specifications to verify the end-point integrity. TNC has defined open solution architecture that helps administrators enforce policies to effectively control access to the network infrastructure.

Trusted Network Connect concepts

Learn about the components, configuring secure communication, and the patch management system of the Trusted Network Connect (TNC).

Trusted Network Connect components

Learn about the components of the Trusted Network Connect (TNC) framework.

The TNC model consists of the following components:

Trusted Network Connect server

The Trusted Network Connect (TNC) server identifies the clients that are added to the network and initiates a verification on them.

The TNC client provides the required fileset level information to the server for verification. The server determines whether the client is at the level that is configured by the administrator. If the client is not compliant, the TNC server notifies the administrator about the remediation that is required.

The TNC server initiates verifications on the clients that are trying to access the network. The TNC server loads a set of integrity measurement verifiers (IMVs) that can request the integrity measurements from clients and verify them. AIX has a default IMV, which verifies the fileset and security patch level of the systems. The TNC server is a framework which loads and manages multiple IMV modules. For verifying a client, it relies on the IMVs to request information from clients and verifies the clients.

Patch management

The Trusted Network Connect (TNC) server integrates with the SUMA to provide a patch management solution.

The AIX SUMA downloads the latest service packs and security fixes available in the IBM ECC and Fix Central. The TNC and patch management daemon pushes the latest updated information to the TNC server, which serves as a baseline fileset to verify the clients.

The **tncpmd** daemon must be configured to manage Service Update Management Assistant (SUMA) downloads and to push fileset information to the TNC server. This daemon must be hosted on a system that is connected to the Internet to be able to download the updates automatically. To use the TNC patch management server without connecting it to the Internet, you can register a user-defined fix repository with the TNC patch management server.

Note: The TNC server and the **tncpmd** daemon can be hosted on the same system.

Trusted Network Connect client

The Trusted Network Connect (TNC) client provides the information that is required by the TNC server for verification.

The server determines whether the client is at the level configured by the administrator. If the client is not compliant, the TNC server notifies the administrator about the updates that are required.

The TNC client loads the IMCs on startup and uses the IMCs to gather the required information.

Trusted Network Connect IP referrer

The Trusted Network Connect (TNC) server can automatically initiate the verification on clients that are part of the network. The IP referrer running on Virtual I/O Server (VIOS) partition detects the new clients that are serviced by the VIOS and sends their IP addresses to the TNC server. The TNC server verifies the client regarding the policy that is defined.

Trusted Network Connect secure communication

The Trusted Network Connect (TNC) daemons communicate over the encrypted channels that are enabled by Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

The secure communication is to ensure that the data and commands that flow in the network are authenticated and secure. Each system must have its own key and certificate, which are generated when the initialization command for the components is run. This process is completely transparent to the administrator and requires less involvement from the administrator.

To verify a new client, its certificate is imported into the database of the server. The certificate is marked as untrusted initially, and then the administrator uses the **tnconconsole** command to view and mark the certificates as trusted by entering the following command:

```
tnconconsole certadd -i<ip> -t<TRUSTED|UNTRUSTED>
```

To use a different key and certificate, the **tnconconsole** command provides the option to import the certificate.

To import the certificate on the server, enter the following command:

```
tnconconsole import -S -k<key filename> -f<key filename>
```

To import the certificate on the client, enter the following command:

```
tnconconsole import -C -k<key filename> -f<key filename>
```

Trusted Network Connect protocol

The Trusted Network Connect (TNC) protocol is used with the TNC framework to maintain network integrity.

TNC provides specifications to verify the end-point integrity. The end-points that request access are assessed based on the integrity measurements of critical components that can affect its operational environment. The TNC framework enables administrators to monitor the integrity of the systems in the network. The TNC is integrated with the AIX patch distribution infrastructure to build a complete patch management solution.

TNC specifications must satisfy the requirements of AIX and POWER® family system architecture. The components of TNC are designed to provide a complete patch management solution on the AIX operating system. This configuration enables administrators to efficiently manage the software configuration on AIX deployments. It provides tools to verify the patch levels of the systems and generate a report on the clients that are not compliant. Additionally, patch management simplifies the process of downloading the patches and installing them.

IMC and IMV modules

The Trusted Network Connect (TNC) server or client internally use the integrity measurement collector (IMC) and integrity measurement verifier (IMV) modules for server verification.

This framework allows loading of multiple IMC and IMV modules into the server and clients. The module that performs the operating system (OS) and fileset level verification is shipped with the AIX operating system by default. To access the modules that are shipped with the AIX operating system, use one of the following paths:

- `/usr/lib/security/tnc/libfileset_imc.a`: Collects the OS level and information about the fileset that is installed from the client system and sends it to the IMV (TNC server) for verification.
- `/usr/lib/security/tnc/libfileset_imv.a`: Requests the OS level and fileset information from the client and compares it with the baseline information. It also updates the status of the client into the database of the TNC server. To view the status, enter the `tnconconsole` command:

```
tnconconsole list -s<COMPLIANT|IGNORE|FAILED|ALL>-i<ip|ALL> [-c] [-q]
```

Related information:

`tnconconsole` command

Installing Trusted Network Connect

Installing the components of Trusted Network Connect (TNC) requires you to complete certain steps.

To configure the setup for using the components of TNC, complete the following steps:

1. Identify the IP addresses of the systems to setup the TNC server, the Trusted Network Connect and Patch Management (TNCPM) server, and the TNC IP referrer for the Virtual I/O Server (VIOS).

Note: The TNC server cannot be configured as a TNC client.

2. Set up the network installation management (NIM) server. The system that is configured as a server is the NIM master, and the `sets:bos.sysmgt.nim.master` filesets must be installed on the client system.
3. Configure the TNCPM server. This configuration can be set up on the NIM system. The TNCPM server uses the SUMA to download the patches from IBM Fix Central and ECC sites. Therefore, the system must be connected to Internet to be able to download the updates.

```
tncpmconsole mktncpm [pmpport=<port>] tncserver=<host:port>
```

For example:

```
tncpmconsole mktncpm pmpport=20000 tncserver=1.1.1.1:10000
```

4. Configure the policies on the TNC server. To create the policies for verifying the clients, see the client policies section of the document.
5. Configure the TNC IP referrer on VIOS. This configuration is required to use VIOS to trigger the verification on the clients that are connecting to network. Enter the following command to configure the referrer:

```
tnconconsole mkipref tncport=<port> tncserver=<ip:port>
```

For example:

```
tnconconsole mkipref tncport=10000 tncserver=1.1.1.1:10000
```

Note: The value of the server port and the TNC port, which is a client port must be the same.

6. Configure the clients by using the following command:

```
tnconconsole mkclient tncport=<port> tncserver=<serverip>:<port>
```

For example:

```
tnconconsole mkclient tncport=10000 tncserver=10.1.1.1:10000
```

Related information:

`tnconconsole` command

“Installing PowerSC Standard Edition 1.1.2, or earlier” on page 7

You must install a fileset for each specific function of PowerSC Standard Edition.

Configuring Trusted Network Connect and Patch management

You must configure Trusted Network Connect (TNC) as a patch management daemon. The TNC server integrates with the SUMA to provide a comprehensive patch management solution.

Configuring Trusted Network Connect server

Learn the steps to configure the TNC server.

To configure the TNC server, the `/etc/tncs.conf` file must have a value similar to the following:

```
component = SERVER
```

To configure a system as a server, enter the following command:

```
tnconsolet mkserver tncport=<port> pmserver=<ip|hostname[,ip2|hostname2..]:port>
[recheck_interval=<time in mins>]
```

For example:

```
tnconsolet mkserver tncport=10000 pmserver=2.2.2.2:20000 recheck_interval=20
```

Note: The `tncport` port and the `pmserver` port must be set to different values, and if the value of the `recheck_interval` parameter is not provided, a default value of 1440 minutes is used.

The default port value used for the `tncport` is 42830, and the default value for the `pmserver` port is 38240.

Related information:

tnconsolet command

Configuring Trusted Network Connect client

Learn the steps to configure the Trusted Network Connect (TNC) client and the configuration settings that are required for the setup.

To configure the TNC client, the `/etc/tncs.conf` file must have a value similar to the following :

```
component = CLIENT
```

To configure a system as a client, enter the following command:

```
tnconsolet mkclient tncport=<port> tncserver=<ip:port>
```

For example:

```
tnconsolet mkclient tncport=10000 tncserver=1.1.1.1:10000
```

Note: The value of the server port and the `tncport`, which is a client port must be the same.

Related information:

tnconsolet command

Configuring the patch management server

Learn the steps to configure a system as a patch management server.

The Trusted Network Connect (TNC) patch management server must be configured on the Network Installation Management (NIM) server so the TNC clients can be updated.

To initialize the TNC patch management fix repositories, enter the following command:

```
tncpmconsolet init -i <download interval> -l <TL list> [-A] [-P <fix_repository_path>]
```

An example of this command follows:

```
tncpmconsole init -i 1440 -l 6100-07,7100-01
```

The **init** command downloads the latest service pack for each technology level, and makes it available for the TNC server. The updated service packs enable the TNC server to run a baseline TNC client verification, and for the TNC patch management server to install the TNC client updates. Specify the **-A** flag to accept all license agreements when running the client updates. By default, the fix repositories that are downloaded by the TNC patch management server are in the `/var/tnc/tncpm/fix_repository` file. Use the **-P** flag to specify a different directory.

To register a new technology level and to download its latest service pack, enter the following command:

```
tncpmconsole add -l <TL list>
```

To download a service pack that is not the most current version, or to download a technology level to be used for verification and client updates, enter the following command:

```
tncpmconsole add -l <TL list> -d  
tncpmconsole add -s <SP List>
```

To register a service pack or technology level fix repository that exists on the system, enter the following command:

```
tncpmconsole add -s <SP> -p <user_defined_fix_repository>  
tncpmconsole add -l <TL> -p <user_defined_fix_repository>
```

To configure a system to serve as a patch management server, enter the following command:

```
tncpmconsole mktncpm [pmpport=<port>] tncserver=ip_list[:port]
```

An example of this command follows:

```
tncpmconsole mktncpm pmpport=20000 tncserver=1.1.1.1:100000
```

The TNC patch management server always supports the management of security Authorized Problem Analysis Reports (APARs). Enter the following command to configure the TNC patch management to manage other types of APARs:

```
tncpmconsole add -t <APAR_type_list>
```

In the previous example, `<APAR_type_list>` is a comma-separated list that contains the following types of APARs:

- HIPER
- PE
- Enhancement

The TNC patch management server supports **syslog** for downloading service pack, technology level, and client updates. The facility is user and priority is info. An example of this is `user.info`.

The TNC patch management server also maintains a log with all of the client updates in the `/var/tnc/tncpm/log/update/<ip>/<timestamp>` directory.

Related information:

tncconsole command

tncpmconsole command

Configuring Trusted Network Connect server email notification

Learn the procedure to configure email notification for the Trusted Network Connect (TNC) server.

The TNC server views the patch level of the client and if the TNC server finds that the client is not compliant, it sends an email to the administrator with the result and the required remediation.

To configure the email address of the administrator, use the following command:

```
tnconsole add -e <mailed>[ipgroup=[±]G1, G2 ..]
```

For example:

```
tnconsole add -e abc@ibm.com ipgroup=vayugrp1,vayugrp2
```

In the preceding example, the email for IP group *vayugrp1* and *vayugrp2* is sent to the abc@ibm.com email address.

To send the mail to a global email address for the IP group that does not have an email address assigned to it, use the following command:

```
tnconsole add -e <mailaddress>
```

For example:

```
tnconsole add -e abc@ibm.com
```

In the preceding example, if an IP group does not have an email address assigned to it, the mail is sent to the abc@ibm.com email address. It acts as a global email address.

Related information:

tnconsole command

Configuring IP referrer on VIOS

Learn how to configure the IP referrer on Virtual I/O Server (VIOS) to automatically initiate verification.

Note: You must configure the SVM kernel extension on the Virtual I/O Server (VIOS) before configuring the IP referrer.

To configure the TNC IP Referrer, the `/etc/tnccs.conf` configuration file must have a setting similar to the following component = IPREF.

You can configure a system as a client by entering the following command:

```
tnconsole mkipref tncport=<port> tncserver=<ip:port>
```

For example:

```
tnconsole mkipref tncport=10000 tncserver=1.1.1.1:10000
```

The value of the tncserver port and the tncport, which is the client port must be the same.

Related information:

tnconsole command

Managing Trusted Network Connect and Patch management

Learn how to manage Trusted Network Connect (TNC) to implement tasks, such as adding the clients, policies, logs, verification results, updating clients, and certificates related to TNC.

Viewing the Trusted Network Connect server logs

Learn how to view the logs of the Trusted Network Connect (TNC) server.

The TNC server logs the verification results of all the clients. To view the log, run the **tnconsole** command:


```
tnconconsole list -H -i <ip |ALL>
```

Related information:

tnconconsole command

Creating policies for the Trusted Network Connect client

Learn how to set up policies related to Trusted Network Connect (TNC) client.

The tnconconsole console provides the interface that is required to manage the TNC policies. Each client or a group of clients can be associated with a policy.

The following policies can be created:

- An Internet Protocol (IP) group contains multiple client IP addresses.
- Each client IP can belong to only one group.
- The IP group is associated with a policy group.
- A policy group contains different kinds of policies. For example, the fileset policy that specifies what must be the client's operating system level (that is, release, technology level, and service pack). There can be multiple fileset policies in a policy group and the client that refers to this policy must be at the level specified by one of the fileset policies.

The following commands show how to create an IP group, policy group, and fileset policies.

To create an IP group, enter the following command:

```
tnconconsole add -G <ipgrpname> ip=[±]<ip1,ip2,ip3 ...>
```

For example:

```
tnconconsole add -G myipgrp ip=1.1.1.1,2.2.2.2
```

Note: For a group, at least one IP must be provided. Multiple IPs must be separated by a comma.

To create a fileset policy, enter the following command:

```
tnconconsole add -F <fspolicyname> <rel00-TL-SP>
```

For example:

```
tnconconsole add -F myfspol 6100-02-03 aparlist=IY0001,IY0002
```

Note: The build information must be in the <rel00-TL-sp> format.

To create a policy and assign an IP group, enter the following command:

```
tnconconsole add -P <policyname> ipgroup=[±] <ipgrp1, ipgrp2 ...>
```

For example:

```
tnconconsole add -P mypol ipgroup=myipgrp,myipgrp1
```

To assign fileset policy to a policy, enter the following command:

```
tnconconsole add -P <policyname> fspolicy=[±]<fspol1, fspol2 ...>
```

For example:

```
tnconconsole add -P mypol fspolicy=myfspol,myfspol1
```

Note: If multiple fileset policies are provided, the system enforces the best matching policy on the client. For example, if the client is on 6100-02-01 and you mention the fileset policy as 7100-03-04 and 6100-02-03, then 6100-02-03 is enforced on the client.

Related information:

tnconconsole command

Starting verification for the Trusted Network Connect client

Learn how to verify the Trusted Network Connect (TNC) client.

Use one of the following methods for client verification:

- The IP referrer daemon on the Virtual I/O Server (VIOS) forwards the client IP to the TNC server: The client LPAR acquires the IP and tries to access the network. The IP referrer daemon on VIOS detects the new IP address and forwards it to the TNC server: The TNC server initiates verification on receiving the new IP address.
- The TNC server verifies the client periodically: The administrator can add the client IPs that are to be verified in the TNC policy database. The TNC server verifies the clients that are in the database. The reverification happens automatically at regular intervals with reference to the `recheck_interval` attribute value that is specified in the `/etc/tnccs.conf` configuration file.
- The administrator initiates the client verification manually: The administrator can initiate the verification manually to verify whether a client is added to the network by running the following command:

```
tnconconsole verify -i <ip>
```

Note: For resources that are not connected to a VIOS, the clients can be verified and updated when they are added manually to the TNC server.

Related information:

tnconconsole command

Viewing the verification results of the Trusted Network Connect

Learn the procedure to view the verification results of the Trusted Network Connect (TNC) client.

To view the verification results of the clients in the network, run the following command:

```
tnconconsole list -s ALL -i ALL
```

This command displays all clients that have a **IGNORED**, **COMPLAINT**, or **FAILED** status.

- **IGNORED:** The client IP is ignored in the IP list (that is, the client can be exempt from verification).
- **COMPLAINT:** The client passed the verification (that is, the client is compliant with the policy).
- **FAILED:** The client failed verification (that is, the client is not compliant with the policy, and administration action is required).

To know the reason for the failure, run the **tnconconsole** command with the client IP that has failed:

```
tnconconsole list -s ALL -i <ip>
```

Related information:

tnconconsole command

Updating the Trusted Network Connect client

The Trusted Network Connect (TNC) server verifies a client and updates the database with the status of the client and the result of verification. The administrator can view the results and take action to update the client.

To update a client that is at a previous level, enter the following command:

```
tnconconsole update -i <ip> -r <buildinfo> [-a apar1,apar2...]
```

For example:

```
tnconconsole update -i 4.4.4.4 -r 6100-02-03 -a IY0004
```

The **tnconconsole** command updates the client with the build and the APAR installations if they are not installed.

Managing patch management policies

The **tncpmconsole** command is used to configure the patch management policies.

The patch management policies provide information, such as the TNC server IP address and the time interval to initiate a SUMA update.

To manage the patch management policy, enter the following command:

```
tncpmconsole mktncpm [pmpport=<port>] tncserver=<host:port>
```

For example:

```
tncpmconsole mktncpm pmpport=2000 tncserver=10.1.1.1:1000
```

Note: The pmpport and the tncserver ports must be different.

Importing Trusted Network Connect certificates

Learn the procedure to import a certificate and to securely transmit data in the network.

The TNC daemons communicate over the encrypted channels enabled by Transport Layer Security (TLS) or Secure Sockets Layer (SSL). This daemon ensures that the data and commands that flow in the network are authenticated and secure. Each system has its own key and certificate, which are generated when the initialization command for the components is run. This process is transparent to the administrator and requires less involvement from the administrator. When a client is being verified for the first time, its certificate is imported into the database of the server. The certificate is marked as untrusted initially, and the administrator uses the **tnconconsole** command to view, and mark the certificates as trusted by entering the following command:

```
tnconconsole certadd -i <ip> -t <TRUSTED|UNTRUSTED>
```

If the administrator wants to use a different key, and certificate, the **tnconconsole** command provides the feature to import them.

To import the certificate on server, enter the following command:

```
tnconconsole import -S -k <key filename> -f <filename>
```

To import the certificate on client, enter the following command:

```
tnconconsole import -C -k <key filename> -f <filename>
```

Troubleshooting Trusted Network Connect and Patch management

Learn the possible causes for failure and the steps to troubleshoot the TNC and the patch management system.

To troubleshoot the TNC and the patch management system, verify the configuration settings that are listed in the following table.

Table 3. Troubleshooting the configuration settings for the TNC and Patch management systems

Problem	Solution
TNC server is not starting or responding	<ul style="list-style-type: none"> • Determine whether the TNC server daemon is running by entering the command: ps -eaf grep "tnccsd" • Check the /etc/tnccs.conf configuration file for the component = SERVER entry on the TNC server.
The TNC patch management server is not starting or responding	<ul style="list-style-type: none"> • Determine whether the TNC patch management server daemon is running by entering the following command: ps -eaf grep tncpmd • Check the /etc/tnccs.conf configuration file for the component = TNCPM entry on the TNC patch management server.
TNC client is not starting or responding	<ul style="list-style-type: none"> • Check if the TNC client daemon is running, enter the following command: ps -eaf grep tnccsd • Check the /etc/tnccs.conf configuration file for the component = CLIENT entry on the TNC client.
TNC IP referrer is not running on Virtual I/O Server (VIOS)	<ul style="list-style-type: none"> • Determine whether the TNC IP referrer daemon is running by entering the following command: ps -eaf grep tnccsd • Check the /etc/tnccs.conf configuration file for the component = IPREF entry on VIOS.
Unable to configure a system as both a TNC server and client	The TNC server and client cannot run simultaneously on the same system.
Daemons are running but verification does not happen	Enable the log messages for the daemons. Set the level=info log in the /etc/tnccs.conf file. You can analyze the log messages.

Notices

This information was developed for products and services offered in the U.S.A. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as the customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at <http://www.ibm.com/software/info/product-privacy>.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Index

A

AIX Audit subsystem 24
AIX syslog 25
Attesting a system 12

C

Client Policies 33
Client verification 34
Components 27
 concepts 27
 Configuring 30
 Configuring client 30
 Configuring patch management server 30
 Configuring server 30
 Configuring the trusted logging 24
 Configuring Trusted Boot 11
 Configuring Trusted Logging 24, 25

D

Deleting systems 13

E

email notification 32
enrolling a system 11

H

hardware and software requirements 5

I

IMC and IMV modules 29
import certificates 28
Import certificates 35
Installing 7, 29
 Installing PowerSC Standard Edition 7
 Installing the collector 11
 Installing the verifier 11
 Installing Trusted Boot 11
 Interpreting attestation results 12
 IP Referrer 28
 IP Referrer on VIOS 32

M

Managing policies 35
Managing TNC and Patch management 32
Managing Trusted Boot 12
Migration considerations 11

O

overview 5, 27

P

Patch management 27
Planning 10
PowerSC
 Trusted Firewall
 configuring 18
 configuring with multiple SEAs 18
 creating rules 20
 deactivating rules 21
 installing 17
 removing SEAs 19
PowerSC Standard Edition 5, 7
Preparing for remediation 10
Prerequisites 10
Protocol 28

S

secure communication 28
Server 27
SUMA 27

T

TNC 35
TNC client 27
troubleshooting 13
Troubleshooting TNC and Patch management 35
Trusted Boot 9, 10, 11, 12, 13
Trusted Boot concepts 9
Trusted Firewall 15
 configuring 18
 multiple SEAs 18
 creating rules 20
 deactivating rules 21
 installing 17
 removing SEAs 19
Trusted Firewall concepts 15
Trusted Logging 23, 25
Trusted Logging overview 23
Trusted network connect 30, 34, 35
Trusted Network Connect 27, 28, 29, 30, 32, 33, 34
Trusted Network Connect and Patch management 27
Trusted Network Connect server 32

U

Updating TNC client 34

V

Viewing logs 32
Viewing verification results 34
Viewing virtual log devices 23
virtual logs 23

W

Writing data to virtual log devices 25



Printed in USA