

IBM PowerSC

Standard Edition

Version 1.1.3

PowerSC Standard Edition

IBM

IBM PowerSC

Standard Edition

Version 1.1.3

PowerSC Standard Edition

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 71.

This edition applies to IBM PowerSC Standard Edition Version 1.1.3 and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2012, 2014.**

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

Contents

About this document	v	Configuring the AIX Audit subsystem	40
What's new in PowerSC Standard Edition 1.1.3	1	Configuring syslog	41
PowerSC Standard Edition Release Notes Version 1.1.3	3	Writing data to virtual log devices.	41
PowerSC Standard Edition 1.1.3 concepts	5	Trusted Network Connect and Patch management	43
Installing PowerSC Standard Edition 1.1.3	7	Trusted Network Connect concepts	43
Security and Compliance Automation	9	Trusted Network Connect components	43
Security and Compliance Automation concepts	9	Trusted Network Connect secure communication	44
Payment Card Industry - Data Security Standard compliance	10	Trusted Network Connect protocol	44
Trusted Boot	25	IMC and IMV modules	44
Trusted Boot concepts	25	Installing Trusted Network Connect	45
Planning for Trusted Boot	25	Configuring Trusted Network Connect and Patch management	46
Trusted Boot prerequisites	26	Configuring Trusted Network Connect server	46
Preparing for remediation	26	Configuring Trusted Network Connect client	46
Migration considerations	27	Configuring the patch management server	46
Installing Trusted Boot.	27	Configuring Trusted Network Connect server email notification	48
Installing the collector	27	Configuring IP referrer on VIOS	48
Installing the verifier	27	Managing Trusted Network Connect and Patch management	49
Configuring Trusted Boot.	27	Viewing the Trusted Network Connect server logs	49
Enrolling a system	27	Creating policies for the Trusted Network Connect client	49
Attesting a system	28	Starting verification for the Trusted Network Connect client	50
Managing Trusted Boot	28	Viewing the verification results of the Trusted Network Connect	50
Interpreting attestation results	28	Updating the Trusted Network Connect client.	51
Deleting systems	29	Managing patch management policies	51
Troubleshooting Trusted Boot	29	Importing Trusted Network Connect certificates	51
Trusted Firewall	31	TNC server reporting	52
Trusted Firewall concepts.	31	Troubleshooting Trusted Network Connect and Patch management	52
Installing Trusted Firewall	33	PowerSC Standard Edition commands 55	
Configuring Trusted Firewall	34	chvfilt command	55
Trusted Firewall Advisor	34	genvfilt command	56
Trusted Firewall logging	34	lsvfilt command	57
Multiple Shared Ethernet Adapters	35	mkvfilt command	58
Removing Shared Ethernet Adapters	36	pmconf command	59
Creating rules	36	psconf command	62
Deactivating rules	37	rmvfilt command	67
Trusted Logging	39	vlanlfw command	68
Virtual logs	39	Notices	71
Detecting virtual log devices.	39	Privacy policy considerations	73
Installing Trusted Logging	40	Trademarks	73
Configuring Trusted Logging	40	Index	75

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 1.1.3

Read about new or significantly changed information for the PowerSC™ Standard Edition Version 1.1.3 topic collection.

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

December 2014

- Added information about the `powerscExp.ice.cmds.1.1.3.2` fileset to the list of files that are required in “Installing PowerSC Standard Edition 1.1.3” on page 7.
- Added the topic set “Security and Compliance Automation” on page 9.
- Added information about the Payment Card Industry version 3 standards in “Payment Card Industry - Data Security Standard compliance” on page 10.
- Removed or updated obsolete information in various topics.

April 2014

- Removed or updated obsolete information in various topics.

December 2013

- Updated the system requirements in “PowerSC Standard Edition 1.1.3 concepts” on page 5.
- Identified a required Trusted Boot file replacement when you reinstall the AIX operating system in “Trusted Boot prerequisites” on page 26.
- Added information about the Trusted Firewall Advisor function in “Trusted Firewall Advisor” on page 34.
- Added information about the Trusted Firewall logging function in “Trusted Firewall logging” on page 34.
- Added a note about requirements to start and stop Trusted Firewall logging in “Trusted Firewall logging” on page 34.
- Renamed the Trusted Firewall Monitoring feature to the Trusted Firewall Advisor feature in “Trusted Firewall logging” on page 34 and in “Trusted Firewall Advisor” on page 34.
- Added the topic “Installing Trusted Logging” on page 40.
- Added information about interim fix updates for Trusted Network Connect in “Configuring the patch management server” on page 46.
- Added information about Trusted Network Connect server reporting in “TNC server reporting” on page 52.
- Added information about installing the Trusted Network Connect verifier in “Installing the verifier” on page 27.
- Added the Trusted Firewall commands in “PowerSC Standard Edition commands” on page 55.
- Renamed the `tscpmconsole` command to the `pmconf` command, and added its information in “pmconf command” on page 59.
- Renamed the `tsconsole` command to the `psconf` command, and added its information in “psconf command” on page 62.
- Updated information about options for the `vlantfw` command in “vlantfw command” on page 68.
- Removed or updated obsolete information in various topics.

November 2012

Updated the information in the “Trusted Network Connect and Patch management” on page 43 topic.

May 2012

Added the documentation for the new feature for “Trusted Firewall” on page 31.

PowerSC Standard Edition Release Notes Version 1.1.3

The release notes contain information about changes to PowerSC Standard Edition Versions 1.1.3 that were identified after the documentation was completed.

What's new

Read about new or changed information in the PowerSC Standard Edition release notes topic collection.

December 2013

The following information describes new or changed items that were identified after the IBM® PowerSC Standard Edition information center content was finalized:

- Identified additional filesets that are required for running Trusted Network Connect version 1.1.3 in "Additional fileset requirement for running Trusted Network Connect."
- Corrected documentation error in "Corrections to items in the IBM PowerSC Standard Edition "What's new" topic."
- Restructured the information for IBM PowerSC documentation.

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_1.1.3/com.ibm.powersc113.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 Version 1.1.3*.

Additional fileset requirement for running Trusted Network Connect

To run the version 1.1.3 version of Trusted Network Connect, you must install the `powerscStd.tnc_command` fileset that is available on your IBM PowerSC Standard Edition DVD. Install the fileset on your AIX system by using the **installp** command. This fileset provides the function of the **psconf** and **pmconf** commands.

Note: If you are using the IP Referrer function of Trusted Network Connect, you must also install the `powerscStd.tnc_command` fileset on your VIOS system.

Installation, migration, upgrade, and configuration information

For information about installing PowerSC Standard Edition, see *Installing PowerSC Standard Edition Version 1.1.3*.

Corrections to items in the IBM PowerSC Standard Edition "What's new" topic

The two list items that refer to the replaced commands should read:

- Renamed the **tncpmconsole** command to the **pmconf** command, and added its information in **pmconf** command.

- Renamed the **tnconso** command to the **psconf** command, and added its information in **psconf** command.

PowerSC Standard Edition 1.1.3 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.	<ul style="list-style-type: none"> • AIX 6 with 6100-07, or later • AIX 7 with 7100-01, or later 	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 <p>The Trusted Network Connect client requires one of the following components:</p> <ul style="list-style-type: none"> • AIX 6.1 with 6100-06, or later • AIX version 7.1 Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management 	<ul style="list-style-type: none"> • POWER5 • POWER6 • POWER7

Installing PowerSC Standard Edition 1.1.3

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.
- `powerscExp.ice.cmds.1.1.3.2`: 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 the 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 1.1.3 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 27

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

“Installing Trusted Network Connect” on page 45

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

Related tasks:

“Installing Trusted Firewall” on page 33

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

“Installing Trusted Logging” on page 40

You can install the PowerSC Trusted Logging feature by using the command line interface or the SMIT tool.

Security and Compliance Automation

AIX Profile Manager manages predefined profiles for security and compliance. The PowerSC Real Time Compliance continuously monitors enabled AIX systems to ensure that they are configured consistently and securely.

The XML profiles automate the recommended AIX system configuration of IBM to be consistent with the Payment Card Data Security Standard, the Sarbanes-Oxley Act, or the U.S. Department of Defense UNIX Security Technical Implementation Guide and Health Insurance Portability and Accountability Act (HIPAA). The organizations that comply with the security standards must use the predefined system security settings.

The AIX Profile Manager operates as an IBM Systems Director plug-in that simplifies applying security settings, monitoring security settings, and auditing security settings for both the AIX operating system and Virtual I/O Server (VIOS) systems. To use the security compliance feature, the PowerSC application must be installed on the AIX managed systems that conform to the compliance standards. The Security and Compliance Automation feature is included in the PowerSC Express Edition, and the PowerSC Standard Edition.

The PowerSC Express Edition installation package, 5765-G82, must be installed on AIX managed systems. The installation package installs the powerscExp.ice fileset and the powerscStd.ice fileset that can be implemented on the system by using the AIX Profile Manager or the **pscxpert** command. PowerSC with IBM Compliance Expert Express (ICEE) compliance is enabled to manage and improve the XML profiles. The XML profiles are managed by the AIX Profile Manager.

Note: Install all applications on the system before you apply a security profile.

Security and Compliance Automation concepts

The PowerSC security and compliance feature is an automated method to configure and audit AIX systems in accordance with the U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG), the Payment Card Industry (PCI) data security standard (DSS), the Sarbanes-Oxley act, COBIT compliance (SOX/COBIT), and the Health Insurance Portability and Accountability Act (HIPAA).

PowerSC helps to automate the configuration and monitoring of systems that must be compliant with the Payment Card Industry (PCI) data security standard (DSS) version 1.2, 2.0, or 3.0. Therefore, PowerSC security and compliance feature is an accurate and complete method of security configuration automation that is used to meet the IT compliance requirements of the DoD UNIX STIG, the PCI DSS, the Sarbanes-Oxley act, COBIT compliance (SOX/COBIT), and the Health Insurance Portability and Accountability Act (HIPAA).

Note: PowerSC security and compliance updates the existing xml profiles that are used by IBM Compliance Expert express (ICEE) edition. The PowerSC Express Edition and the PowerSC Standard Edition XML profiles can be used with the **pscxpert** command, similar to ICEE.

The preconfigured compliance profiles delivered with the PowerSC Express Edition and the PowerSC Standard Edition reduce the administrative workload of interpreting compliance documentation and implementing the standards as specific system configuration parameters. This technology reduces the cost of compliance configuration and auditing by automating the processes. IBM PowerSC Express Edition and IBM PowerSC Standard Edition is designed to help effectively manage the system requirement associated with external standard compliance that can potentially reduce costs and improve compliance.

| **Payment Card Industry - Data Security Standard compliance**

| The Payment Card Industry - Data Security Standard (PCI - DSS) categorizes IT security into 12 sections that are called the 12 requirements and security assessment procedures.

| The 12 requirements and security assessment procedures of IT security that are defined by PCI - DSS include the following items:

| **Requirement 1: Install and maintain a firewall configuration to protect the data of the cardholder.**

| Documented list of services and ports necessary for business. This requirement is implemented by disabling unnecessary and insecure services.

| **Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.**

| Always change vendor-supplied defaults before you install a system on the network. This requirement is implemented by disabling the Simple Network Management Protocol (SNMP) daemon.

| **Requirement 3: Protect the stored data of the cardholder.**

| This requirement is implemented by enabling the Encrypted File System (EFS) feature that is provided with the AIX operating system.

| **Requirement 4: Encrypt the data of the cardholder when you transmit the data across open public networks.**

| This requirement is implemented by enabling the IP Security (IPSEC) feature that is provided with the AIX operating system.

| **Requirement 5: Use and regularly update anti-virus software programs.**

| This requirement is implemented by using the Trusted Execution policy program. Trusted Execution is the recommended anti-virus software, and it is native to the AIX operating system. PCI requires that you capture the logs from the Trusted Execution program by enabling security information and event management (SIEM) to monitor the alerts. By running the Trusted Execution program in log-only mode, it does not stop the checks when an error is caused by a hash mismatch.

| **Requirement 6: Develop and maintain secure systems and applications.**

| To implement this requirement, you must install the required patches to your system manually. If you purchased PowerSC Standard Edition, you can use the Trusted Network Connect (TNC) feature.

| **Requirement 7: Restrict access to the cardholder data, by business need to know.**

| You can implement strong access control measures by using the RBAC feature to enable rules and roles. RBAC cannot be automated because it requires the input of an administrator to be enabled.

| The RbacEnablement checks the system to determine whether the isso, so, and sa properties for the roles exist on the system. If these properties do not exist, the script creates them. This script is also run as part of the pscxpert checks that it completes when it is running commands, such as the pscxpert -c command.

| **Requirement 8: Assign a unique ID to each person who has access to the computer.**

| You can implement this requirement by enabling PCI profiles. The following rules apply to PCI profile:

- | • Change user passwords at least every 90 days.
- | • Require a minimum password length of 7 characters.
- | • Use a password that contains both numerals and alphabetic characters.
- | • Do not allow an individual to submit a new password that is the same as the previous four passwords that were used.
- | • Limit repeated access attempts by locking out the user ID after six unsuccessful attempts.
- | • Set the lockout duration to 30 minutes, or until an administrator re-enables the user ID.

- Require a user to reenter a password to reactivate a terminal after it is idle for 15 minutes or longer.

Requirement 9: Restrict physical access to the data of the cardholder.

Store repositories that contain sensitive cardholder data in an access-restricted room.

Requirement 10: Track and monitor all access to network resources and to the cardholder data.

This requirement is implemented by logging access to the system components by enabling the automatic logs on the system components.

Requirement 11: Regularly test the security systems and processes.

This requirement is implemented by using the Real-Time Compliance feature.

Requirement 12: Maintain a security policy that includes information security for employees and contractors.

Activation of modems for vendors only when needed by vendors with immediate deactivation after use. This requirement is implemented by disabling remote root login, activating on a needed basis by a system administrator, and then deactivating when it is no longer needed.

PowerSC Standard Edition (for version 3) and PowerSC Express Edition (for version 2) reduce the configuration management that is required to meet the guidelines that are defined by PCI DSS. However, the entire process cannot be automated.

For example, restricting access to the data of the cardholder based on the business requirement cannot be automated. The AIX operating system provides strong security technologies, such as Role Based Access Control (RBAC); however, PowerSC Standard Edition cannot automate this configuration because it cannot determine the individuals who require access and the individuals who do not. IBM Compliance Expert can automate the configuration of other security settings that are consistent with the PCI requirements.

When the PCI profile is applied to a database environment, several TCP and UDP ports that are used by the software stack are disabled by restrictions. You must enable these ports and disable the Trusted Execution function to run the application and workload. Run the following commands to remove the restrictions on the ports and disable the Trusted Execution function:

```
trustchk -p TE=OFF
tcptr -delete 9091 65535
tcptr -delete 9090 9090
tcptr -delete 112 9089
tcptr -add 9091 65535 1024 1
```

Note: All of the custom script files that are provided to maintain PCI - DSS compliance are in the /etc/security/psceexpert/bin directory.

The following table shows how PowerSC Express Edition and PowerSC Standard Edition address the requirements of the PCI DSS standard by using the functions of the AIX Security Expert utility:

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
2.1	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the minimum number of weeks that must pass before you can change a password to 0 weeks by setting the minage parameter to a value of 0.	/etc/security/psceexpert/bin/chusrattr

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
<p>PCI version 2 8.5.9</p> <p>PCI version 3 8.2.4</p>	Change user passwords at least every 90 days.	Sets the maximum number of weeks that a password is valid to 13 weeks by setting the maxage parameter to a value of 13.	/etc/security/psccexpert/bin/chusrattr
2.1	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the number of weeks that an account with an expired password remains in the system to 8 weeks by setting the maxexpired parameter to a value of 8.	/etc/security/psccexpert/bin/chusrattr
<p>PCI version 2 8.5.10</p> <p>PCI version 3 8.2.3</p>	Require a minimum password length of at least 7 characters.	Sets the minimum password length to 7 characters by setting the minlen parameter to a value of 7.	/etc/security/psccexpert/bin/chusrattr
<p>PCI version 2 8.5.11</p> <p>PCI version 3 8.2.3</p>	Use passwords that contain both numeric and alphabetic characters.	Sets the minimum number of alphabetic characters that are required in a password to 1. This setting ensures that the password contains alphabetic characters by setting the minalpha parameter to a value of 1.	/etc/security/psccexpert/bin/chusrattr
<p>PCI version 2 8.5.11</p> <p>PCI version 3 8.2.3</p>	Use passwords that contain both numeric and alphabetic characters.	Sets the minimum number of non-alphabetic characters that are required in a password to 1. This setting ensures that the password contains nonalphabetic characters by setting the minother parameter to a value of 1.	/etc/security/psccexpert/bin/chusrattr
<p>PCI version 2 2.1</p> <p>PCI version 3 8.2.2</p>	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the maximum number of times that a character can be repeated in a password to 8 by setting the maxrepeats parameter to a value of 8. This setting indicates that a character in a password can be repeated an unlimited number of times when it conforms to the other password limitations.	/etc/security/psccexpert/bin/chusrattr
<p>PCI version 2 8.5.12</p> <p>PCI version 3 8.2.5</p>	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	Sets the number of weeks before a password can be reused to 52 by setting the histexpire parameter to a value of 52.	/etc/security/psccexpert/bin/chusrattr
<p>PCI version 2 8.5.12</p> <p>PCI version 3 8.2.5</p>	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	Sets the number of previous passwords that you cannot reuse to 4 by setting the histsize parameter to a value of 4.	/etc/security/psccexpert/bin/chusrattr

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 8.5.13 PCI version 3 10.2.4	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Sets the number of consecutive unsuccessful login attempts that disables an account to 6 attempts for each non-root account by setting the loginentries parameter to a value of 6.	/etc/security/psceexpert/bin/chusrattr
PCI version 2 8.5.13 PCI version 3 10.2.4	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Sets the number of consecutive unsuccessful login attempts that disables a port to 6 attempts by setting the logindisable parameter to a value of 6.	<ul style="list-style-type: none"> • /etc/security/psceexpert/bin/chdefstanza • /etc/security/login.cfg
PCI version 2 8.5.14 PCI version 3 10.2.4	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	Sets the duration of time that a port is locked after it is disabled by the <i>logindisable</i> attribute to 30 minutes by setting the loginreenable parameter to a value of 30.	<ul style="list-style-type: none"> • /etc/security/psceexpert/bin/chdefstanza • /etc/security/login.cfg
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	Disables the remote root login function by setting its value to false. The system administrator can activate the remote login function as needed, and then deactivate it when the task is complete.	<ul style="list-style-type: none"> • /etc/security/psceexpert/bin/chuserstanza • /etc/security/user
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Enables the function that ensures that all users have a unique user name before they can access system components or card holder data by setting that function to a value of true.	<ul style="list-style-type: none"> • /etc/security/psceexpert/bin/chuserstanza • /etc/security/user
10.2	Enable auditing on the system.	Enables auditing of the binary files on the system.	/etc/security/psceexpert/bin/pciaudit
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the lpd daemon.	Stops the lpd daemon and comments out the corresponding entry in the /etc/inittab file that automatically starts the daemon.	/etc/security/psceexpert/bin/comntrows
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the Common Desktop Environment (CDE).	Disables the CDE function when the layer four traceroute (LFT) is not configured.	/etc/security/psceexpert/bin/comntrows
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the timed daemon.	Stops the timed daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/psceexpert/bin/rctcpip

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the NTP daemon.	Stops the NTP daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscxpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rwhod daemon.	Stops the rwhod daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscxpert/bin/rctcpip
PCI version 2 2.1 PCI version 3 2.1.1	Change the vendor-supplied defaults before installing a system on the network, which includes disabling the SNMP daemon.	Stops the SNMP daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscxpert/bin/rctcpip
PCI version 2 2.1 PCI version 3 2.1.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the SNMPMIBD daemon.	Disables the SNMPMIBD daemon by commenting out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscxpert/bin/rctcpip
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the AIXMIBD daemon.	Disables the AIXMIBD daemon by commenting out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscxpert/bin/rctcpip
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the HOSTMIBD daemon.	Disables the HOSTMIBD daemon by commenting out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscxpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the DPID2 daemon.	Stops the DPID2 daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscxpert/bin/rctcpip
PCI version 2 2.1 PCI version 3 2.2.2	Change vendor-supplied defaults before installing a system on the network, which includes stopping the DHCP server.	Disables the DHCP server.	/etc/security/pscxpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the DHCP agent.	Stops and disables the DHCP relay agent and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the agent.	/etc/security/pscxpert/bin/rctcpip

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rshd daemon.	Stops and disables all instances of the rshd daemon and the shell service, and comments out the corresponding entries in the /etc/inetd.conf file that automatically start the instances.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rlogind daemon.	Stops and disables all instances of the rlogind daemon and rlogin service. The AIX Security Expert utility also comments out the corresponding entries in the /etc/inetd.conf file that automatically start the instances.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rexecd daemon.	Stops and disables all instances of the rexecd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the comsat daemon.	Stops and disables all instances of the comsat daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the fingerd daemon.	Stops and disables all instances of the fingerd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the systat daemon.	Stops and disables all instances of the systat daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/psccexpert/bin/cominetdconf
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the netstat command.	Disables the netstat command by commenting out the corresponding entry in the /etc/inetd.conf file.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.3	Disable unnecessary and insecure services, which include the tftpd daemon.	Stops and disables all instances of the tftpd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/psccexpert/bin/cominetdconf

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the talkd daemon.	Stops and disables all instances of the talkd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rquotad daemon.	Stops and disables all instances of the rquotad daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rstatd daemon.	Stops and disables all instances of the rstatd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rusersd daemon.	Stops and disables all instances of the rusersd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the rwalld daemon.	Stops and disables all instances of the rwalld daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the sprayd daemon.	Stops and disables all instances of the sprayd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the pcnfsd daemon.	Stops and disables all instances of the pcnfsd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the TCP echo service.	Stops and disables all instances of the echo(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the TCP discard service.	Stops and disables all instances of the discard(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the TCP chargen service.	Stops and disables all instances of the chargen(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the TCP daytime service.	Stops and disables all instances of the daytime(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the TCP time service.	Stops and disables all instances of the timed(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the UDP echo service.	Stops and disables all instances of the echo(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the UDP discard service.	Stops and disables all instances of the discard(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the UDP chargen service.	Stops and disables all instances of the chargen(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/psccexpert/bin/cominetdconf

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the UDP daytime service.	Stops and disables all instances of the daytime(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the UDP time service.	Stops and disables all instances of the timed(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.3	Disable unnecessary and insecure services, which include the FTP service.	Stops and disables all instances of the ftpd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.3	Disable unnecessary and insecure services, which include the telnet service.	Stops and disables all instances of the telnetd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include dtspc.	Stops and disables all instances of the dtspc daemon. The AIX Security Expert also comments out the corresponding entry in the /etc/inittab file that automatically starts the daemon when the LFT is not configured and the CDE is disabled in the /etc/inittab file.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the ttldbserver service.	Stops and disables all instances of the ttldbserver service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 PCI version 3 2.2.2	Disable unnecessary and insecure services, which include the cmsd service.	Stops and disables all instances of the cmsd service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/pscxpert/bin/cominetdconf
PCI version 2 2.2.3 PCI version 3 2.2.4	Configure system security parameters to prevent misuse.	Removes the Set User ID (SUID) commands by commenting out the corresponding entry in the /etc/inetd.conf file that automatically enables the commands.	/etc/security/pscxpert/bin/rmsuidfrmcmds

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
<p>PCI version 2 2.2.3</p> <p>PCI version 3 2.2.4</p>	Configure system security parameters to prevent misuse.	Enables the lowest security level for the File Permissions Manager.	/etc/security/psceexpert/bin/filepermgr
<p>PCI version 2 2.2.3</p> <p>PCI version 3 2.2.4</p>	Configure system security parameters to prevent misuse.	Modifies the Network File System protocol with restricted settings that conform to the PCI security requirements. These restricted settings include disabling remote root access and anonymous UID and GID access.	/etc/security/psceexpert/bin/nfsconfig
<p>PCI version 2 2.2.2</p> <p>PCI version 3 2.2.3</p>	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the rlogind, rshd, and tftpd daemons, which are not secure.	/etc/security/psceexpert/bin/dismrtdmns
<p>PCI version 2 2.2.2</p> <p>PCI version 3 2.2.3</p>	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the rlogind, rshd, and tftpd daemons, which are not secure.	/etc/security/psceexpert/bin/rmrhostsnetr
<p>PCI version 2 2.2.2</p> <p>PCI version 3 2.2.3</p>	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the logind, rshd, and tftpdpci_rmetchostsequiv daemons, which are not secure.	/etc/security/psceexpert/bin/rmetchostsequiv
<p>PCI version 2 1.3.6</p> <p>PCI version 3 2.2.3</p>	Implement stateful inspection, or packet filtering, in which only established connections are allowed on the network.	Enables the network clean_partial_conns option by setting its value to 1.	/etc/security/psceexpert/bin/ntwkopts
<p>PCI version 2 2.2.2</p> <p>PCI version 3 2.2.3</p>	Implement stateful inspection, or packet filtering, in which only established connections are allowed on the network.	Enables TCP security by setting the network tcp_tcpsecure option to a value of 7. This setting provides protection against data, reset (RST), and TCP connection request (SYN) attacks.	/etc/security/psceexpert/bin/ntwkopts

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
1.2	Protect unauthorized access to unused ports.	Configures the system to shun the hosts for 5 minutes to prevent other systems from accessing unused ports.	/etc/security/psceexpert/bin/ipsecshunhosthls Note: You can enter additional filter rules in the /etc/security/aixpert/bin/filter.txt file. These rules are integrated by the ipsecshunhosthls.sh script when you apply the profile. The entries should be in the following format: <i>port_number:ip_address: action</i> where the possible values for <i>action</i> are Allow or Deny.
1.2	Protect the host from port scans.	Configures the system to shun vulnerable ports for 5 minutes, which prevents port scans.	/etc/security/psceexpert/bin/ipsecshunports Note: You can enter additional filter rules in the /etc/security/aixpert/bin/filter.txt file. These rules are integrated by the ipsecshunhosthls.sh script when you apply the profile. The entries should be in the following format: <i>port_number:ip_address: action</i> where the possible values for <i>action</i> are Allow or Deny.
1.2	Limit object creation permissions.	Sets the default object creation permissions to 22 by setting the umask parameter to a value of 22.	/etc/security/psceexpert/bin/chusrattr
1.2	Limit system access.	Ensures that the root ID the only one that is listed in the cron.allow file and removes the cron.deny file from the system.	/etc/security/psceexpert/bin/limitsysacc
6.5.8	Remove dot from the path root.	Removes the dots from the PATH environment variable in the following files that are located in the root home directory: <ul style="list-style-type: none"> • .cshrc • .kshrc • .login • .profile 	/etc/security/psceexpert/bin/rmdotfrmpathroot
6.5.8	Remove dot from the non-root path:	Removes the dots from <i>PATH</i> environment variable in the following files that are in the user home directory: <ul style="list-style-type: none"> • .cshrc • .kshrc • .login • .profile 	/etc/security/psceexpert/bin/rmdotfrmpathroot
2.2.3	Limit system access.	Adds the root user capability and user name in the /etc/ftpusers file.	/etc/security/psceexpert/bin/chetcftpusers
2.1	Remove the guest account.	Removes the guest account and its files.	/etc/security/psceexpert/bin/execcmds

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
6.5.2	Prevent launching programs in content space.	Enables the stack execution disable (SED) feature.	/etc/security/pscexpert/bin/sedconfig
8.2	Ensure that the password for root is not weak.	Starts a root password integrity check against the root password, thereby ensuring a strong root password.	/etc/security/pscexpert/bin/chuserstanza
PCI version 2 8.5.15 PCI version 3 8.1.8	Limit access to the system by setting the session idle time.	Sets the idle time limit to 15 minutes. If the session is idle for longer than 15 minutes, you must reenter the password.	/etc/security/pscexpert/bin/autologoff
1.3.5	Limit traffic access to cardholder information.	Sets the TCP traffic regulation to its high setting, which enforces denial-of-service mitigation on ports.	/etc/security/pscexpert/bin/tcptr_pscexpert
1.3.5	Maintain a secure connection when migrating data.	Enables automated IP Security (IPSec) tunnel creation between Virtual I/O Servers during live partition migration.	/etc/security/pscexpert/bin/cfgsecmig
1.3.5	Limit packets from unknown sources.	Allows the packets from the Hardware Management Console.	/etc/security/pscexpert/bin/ipsecpermithostorport
5.1.1	Maintain antivirus software.	Maintains the system integrity by detecting, removing, and protecting against known types of malicious software.	/etc/security/pscexpert/bin/manageITsecurity
PCI version 2 Section 7 PCI version 3 Section 7	Maintain access on an as needed basis.	Enable role-based access control (RBAC) by creating system operator, system administrator, and information system security officer user roles with the required permissions.	/etc/security/pscexpert/bin/EnableRbac
PCI version 2 Not included in version 2 profile, added in version 3. PCI version 3 2.3	Implement more security features for any required services, protocols, or daemons that are considered to be insecure.	Uses secured technologies such as Secure Shell (SSH), SSH File Transfer Protocol (S-FTP), Secure Sockets Layer (SSL), or Internet Protocol Security Virtual Private Network (IPsec VPN) to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP. It also configures the SSH daemon to use only the SSHv2 protocol.	/etc/security/pscexpert/bin/sshPCIconfig
PCI version 2 Not included in version 2 profile, added in version 3. PCI version 3 2.3	The SSH Client must be configured to use only the SSHv2 protocol.	Configures the SSH client to use the SSHv2 protocol.	/etc/security/pscexpert/bin/sshPCIconfig

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The SSH daemon must listen only on management network addresses unless it is authorized for uses other than management.	Ensures that the SSH daemon is set up only to listen.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The SSH daemon must be configured to use only FIPS 140-2 approved ciphers	Ensures that the SSH daemon uses only the FIPS 140-2 ciphers.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The SSH daemon must be configured to use only Message Authentication Codes (MACs) that employ FIPS 140-2 approved cryptographic hash algorithms.	Ensures that the MACs are running the approved algorithms.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The SSH daemon must restrict login ability to specific users or groups.	Restricts login on the system to specific users and groups.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The system must display the date and time of the last successful account login upon login.	Maintains the information from the last successful login, and displays it after the next successful login.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The SSH daemon must complete strict mode checking of home directory configuration files.	Ensures that the home directory configuration files are set to the correct modes.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The SSH daemon must use privilege separation.	Ensures that the SSH daemon has the correct amount of separation of its privileges.	/etc/security/psccexpert/bin/sshPCIconfig

Table 2. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	The SSH daemon must not allow rhosts to have RSA authentication.	Disables RSA authentication for rhosts when you are using the SSH daemon.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 2.3</p>	Restrict maximum number of login sessions to 2 per user.	Sets the maximum number of login sessions to 2 per user.	/etc/security/psccexpert/bin/sshPCIconfig
<p>PCI version 2 1.1.5 2.2.2</p> <p>PCI version 3 10.4</p>	Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	Enables the ntp daemon.	/etc/security/psccexpert/bin/rctcpip
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 8.1.5</p>	Disable a user account when not in use.	Disables user accounts after 35 days of inactivity.	/etc/security/psccexpert/bin/disableacctpci
<p>PCI version 2 Not included in version 2 profile, added in version 3.</p> <p>PCI version 3 8.2</p>	Restrict maximum number of login sessions to 2 per user.	Sets the maximum number of active sessions for the user set to 2 by setting the maxulogs parameter to a value of 2.	/etc/security/psccexpert/bin/chusrattr

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 29

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.

- | When you prepare to reinstall the AIX operating system on a system with Trusted Boot already installed,
- | you must copy the `/var/tss/lib/tpm/system.data` file and use it to overwrite the file in the same
- | location after the reinstallation completes. If you do not copy this file, you must remove the virtualized
- | Trusted Platform Module from the management console and reinstall it on the partition.

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 off, and alerting users).
- Were there any other systems compromised that must be checked?

Related concepts:

“Troubleshooting Trusted Boot” on page 29

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 that is enabled 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 1.1.3” 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 OpenPTS verifier component runs on the AIX operating system and on other platforms.

| The AIX version of the verifier can be installed from the fileset by using the AIX 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.

| The OpenPTS verifier for other operating systems can be downloaded from Download Linux OpenPTS
| Verifier For Use With AIX Trusted Boot.

Related information:

[Download Linux OpenPTS Verifier For Use With AIX Trusted Boot](#)

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 3. 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 tcscd 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>

Table 3. Troubleshooting some of the common scenarios for failure (continued)

Reason for failure	Possible causes of failure	Suggested remediation
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.
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 26

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 25

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 32, 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.

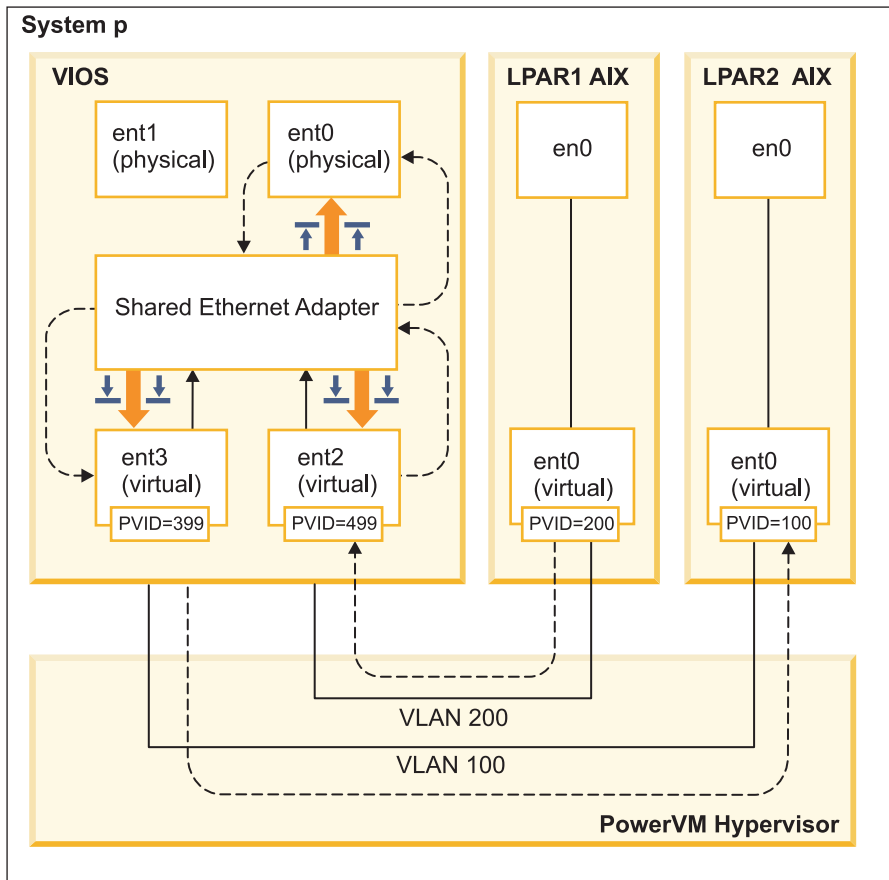


Figure 1. Example of cross-VLAN information transfer without Trusted Firewall

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 33.

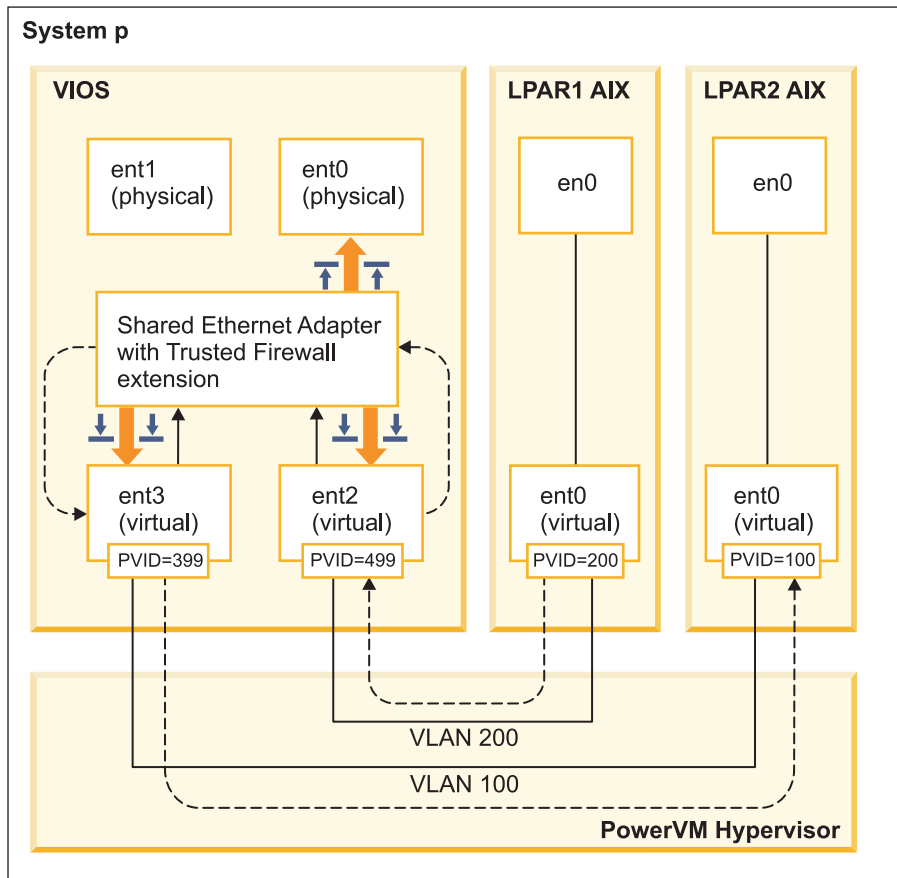


Figure 2. Example of cross-VLAN information transfer with Trusted Firewall

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 1.1.3” 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.

Trusted Firewall Advisor

Trusted Firewall Advisor analyzes system traffic from different logical partitions (LPARs) to provide information for determining whether running Trusted Firewall improves system performance.

If the Trusted Firewall Advisor function records a significant amount of traffic from different virtual LANs (VLANs) that are on the same central electronics complex, enabling Trusted Firewall should benefit your system.

To enable Trusted Firewall Advisor, enter the following command:

```
vlantfw -m
```

To display the results of Trusted Firewall Advisor, enter the following command:

```
vlantfw -D
```

To disable Trusted Firewall Advisor, enter the following command:

```
vlantfw -M
```

Trusted Firewall logging

Trusted Firewall logging compiles a list of network traffic paths within the central electronics complex. The list shows the filters that Trusted Firewall uses to route traffic.

When Trusted Firewall Advisor determines that routing the traffic internally improves efficiency, Trusted Firewall logging maintains a list of paths in the `svm.log` file. The size of the `svm.log` file is limited to 16 MB. If the entries exceed the 16 MB limit, the oldest entries are removed from the log file.

To start Trusted Firewall logging, enter the following command:

```
vlantfw -l
```

To stop Trusted Firewall logging, enter the following command:

```
vlantfw -L
```

| You can view the log file at the following location: /home/padmin/svm/svm.log.

| **Note:** You can run the commands to start and stop Trusted Firewall logging only when you are
| authenticated as a root user.

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 shows an environment using multiple SEAs.

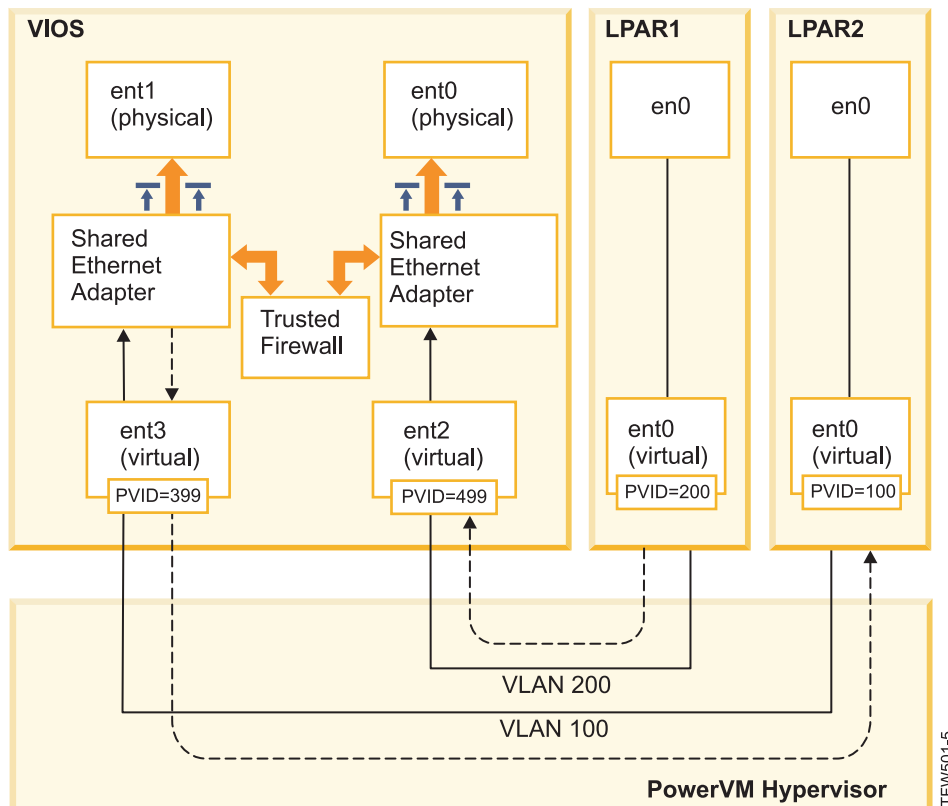


Figure 3. Configuration using multiple Shared Ethernet Adapters on a single VIOS

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:

```
vlanfw -s
```

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

```
vlanfw -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 reference:

“genvfilt command” on page 56

“mkvfilt command” on page 58

“vlantfw command” on page 68

Related information:

 [Virtual I/O Server \(VIOS\)](#)

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 36

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

Related reference:

“lsvfilt command” on page 57

“rmvfilt command” on page 67

Trusted Logging

PowerVM® Trusted Logging lets AIX logical partitions (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.

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 host name of the LPAR). 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.

Installing Trusted Logging

- | You can install the PowerSC Trusted Logging feature by using the command line interface or the SMIT tool.
- | The prerequisites for installing Trusted Logging are VIOS 2.2.1.0, or later, and IBM AIX 6 with Technology Level 7 or IBM AIX 7 with Technology Level 1.
- | The file name for installing the Trusted Logging feature is `powerscStd.vlog`, which is included on the PowerSC Standard Edition installation CD.
- | To install the Trusted Logging function:
 1. Ensure that you are running VIOS Version 2.2.1.0, or later.
 2. Insert the PowerSC installation CD or download the image of the installation CD.
 3. Use the **installp** command or the SMIT tool to install the `powerscStd.vlog` fileset.
- | **Related information:**
 - | “Installing PowerSC Standard Edition 1.1.3” on page 7
 - | You must install a fileset for each specific function of PowerSC Standard Edition.

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 39.

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 39.

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, the certificate of the client must be imported into the database of the server. The certificate is marked as untrusted initially, and then the administrator uses the **psconf** command to view and mark the certificates as trusted by entering the following command:

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

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

| To import the certificate from the server, enter the following command:

```
| psconf import -S -k<key filename> -f<key filename>
```

| To import the certificate from the client, enter the following command:

```
| psconf 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 following command:

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

Related reference:

“psconf command” on page 62

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 websites. To download the updates, the system must be connected to the Internet. Enter the following command to configure the TNCPM server:

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

For example:

```
pmconf 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 “Creating policies for the Trusted Network Connect client” on page 49.

5. Configure the TNC IP referrer on VIOS. This configuration on VIOS triggers the verification on the clients that are connecting to the network. Enter the following command to configure the referrer:

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

For example:

```
psconf 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:

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

For example:

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

Related reference:

“psconf command” on page 62

Related information:

“Installing PowerSC Standard Edition 1.1.3” on page 7

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

Installing with NIM

 [IBM Fix Central](#)

 [Passport Advantage Online Help Center](#)

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:

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

| For example:

```
| psconf 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 of 42830 minutes is used for the `tncport` port, and the default value of 38240 minutes is used for the `pmserver` port.

Related reference:

“psconf command” on page 62

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:

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

For example:

```
psconf 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 reference:

“psconf command” on page 62

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 fix repositories for TNC patch management, enter the following command:
| `pmconf init -i <download interval> -l <TL list> [-A] [-P <download path>][-x <ifix interval>]
| [-K <ifix key>]`

| An example of the **pmconf** command follows:

| `pmconf 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 enable automatic IBM Security Advisory and interim fix downloads, you can specify an interim fix interval. This feature provides automatic notification of newly-published security interim fixes and associated Common Vulnerabilities and Exposures (CVE) identifiers. All security advisories and interim fixes are verified prior to registration with the TNC. The IBM AIX vulnerability public key, which is required to download interim fixes automatically, is available at the IBM AIX Security website. Automatic service pack and interim fix downloads are disabled by setting both the download interval and interim fix interval to 0.

You can also update service pack and interim fix registration manually. To manually register an IBM Security Advisory along with its corresponding interim fixes, enter the following command:

`pmconf add -y <advisory file> -v <signature file> -e <ifix tar file>`

| To manually register a stand-alone interim fix, enter the following command:

| `pmconf add -p <SP> -e <ifix file>`

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

`pmconf 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:

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

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

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

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

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

An example of this command follows:

`pmconf 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:

`pmconf 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 reference:

“psconf command” on page 62

Related information:

 IBM AIX Security

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, enter the following command:

```
| psconf add -e <email_id>[ipgroup=[±]G1, G2 ..]
```

| For example:

```
| psconf 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 an email to a global email address for the IP group that does not have an email address assigned to it, enter the following command:

```
| psconf add -e <mailaddress>
```

| For example:

```
| psconf 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 reference:

“psconf command” on page 62

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/tncs.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:

```
| psconf mkipref tncport=<port> tncserver=<ip:port>
```

| For example:

```
| psconf 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 reference:

“psconf command” on page 62

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 **psconf** command:

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

| **Related reference:**

“psconf command” on page 62

Creating policies for the Trusted Network Connect client

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

| The psconf 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:

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

| For example:

```
| psconf 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:

```
| psconf add -F <fspolicname> <rel100-TL-SP>
```

| For example:

```
| psconf 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 to assign an IP group, enter the following command:

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

| For example:

```
| psconf add -P mypol ipgroup=myipgrp,myipgrp1
```

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

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

For example:

```
psconf 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 reference:

“psconf command” on page 62

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/tncs.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:

```
tnconsole 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 reference:

“psconf command” on page 62

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, enter the following command:

```
| psconf list -s ALL -i ALL
```

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

| • **IGNORED:** The client IP is ignored in the IP list (that is, the client can be exempt from verification).

- | • **COMPLIANT**: 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 determine the reason for the failure, run the **psconf** command with the client IP that has failed:

| `psconf list -s ALL -i <ip>`

Related reference:

“psconf command” on page 62

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:

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

| For example:

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

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

Related reference:

“psconf command” on page 62

Managing patch management policies

| The **pmconf** 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:

| `pmconf mktncpm [pmport=<port>] tncserver=<host:port>`

| For example:

`pmconf mktncpm pmport=2000 tncserver=10.1.1.1:1000`

Note: The `pmport` and the `tncserver` ports must be different.

Related reference:

“pmconf command” on page 59

Importing Trusted Network Connect certificates

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

| The Trusted Network Connect (TNC) daemons communicate over the encrypted channels enabled by using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol. This daemon ensures that the data and commands that are transported on 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 **psconf** command to view and to mark the certificates as trusted by entering the following command:

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

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

| To import the certificate from a server, enter the following command:

| `psconf import -S -k <key filename> -f <filename>`

| To import the certificate from a client, enter the following command:

| `psconf import -C -k <key filename> -f <filename>`

Related reference:

“psconf command” on page 62

| TNC server reporting

| The Trusted Network Connect (TNC) server supports both the comma-separated values (CSV) format and the text output format for its common vulnerabilities and exposures (CVE), IBM Security Advisory, TNC server policies, TNC client security fix, and registered service packs and interim fix reports.

| The CVE report displays all of the common exposures and vulnerabilities for the registered service packs.

| To display the results of this report, enter the following command:

| `psconf report -v {CVEid|ALL} -o {TEXT|CSV}`

| The IBM Security Advisory report displays the known security vulnerabilities on the installed IBM software. To display the results of this report, enter the following command:

| `psconf report -A <advisoryname>`

| The TNC server policies report displays the security policies that are enforced on the TNC server. To display the results of this report, enter the following command:

| `psconf report -P {policyname|ALL} -o {TEXT|CSV}`

| The TNC client fix report displays the installed and missing interim fixes for the TNC client. To display the results of this report, enter the following command:

| `psconf report -i {ip|ALL} -o {TEXT|CSV}`

| You can also run a report that generates a list of registered service packs and the related authorized program analysis reports (APARs) and interim fixes. To display the results of this report, enter the following command:

| `psconf report -B {buildinfo|ALL} -o {TEXT|CSV}`

Related reference:

“psconf command” on page 62

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 4. Troubleshooting the configuration settings for the TNC and Patch management systems

Problem	Solution
TNC server is not starting or responding	<p>Complete the following procedure:</p> <ol style="list-style-type: none"> 1. Determine whether the TNC server daemon is running by entering the command: <code>ps -eaf grep tnccsd</code> 2. If it is not running, delete the <code>/var/tnc/.tncsock</code> file. 3. Restart the server. <p>If that does not solve the problem, check the <code>/etc/tnccs.conf</code> configuration file for the component = SERVER entry on the TNC server.</p>
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: <code>ps -eaf grep tncpmd</code> • Check the <code>/etc/tnccs.conf</code> 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"> • Determine whether the TNC client daemon is running by entering the following command: <code>ps -eaf grep tnccsd</code> • Check the <code>/etc/tnccs.conf</code> 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: <code>ps -eaf grep tnccsd</code> • Check the <code>/etc/tnccs.conf</code> 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 <code>level=info</code> log in the <code>/etc/tnccs.conf</code> file. You can analyze the log messages.

PowerSC Standard Edition commands

PowerSC Standard Edition provides commands that enable communication with the Trusted Firewall component and the Trusted Network Connect component by using the command line.

chvfilter command

Purpose

Changes the values for the existing virtual LAN-crossing filter rule.

Syntax

```
chvfilter [ -v <4|6> ] -n fid [ -a <D|P> ] [ -z <svlan> ] [ -Z <dvlan> ] [ -s <s_addr> ] [ -d <d_addr> ] [ -o <src_port_op> ] [ -p <src_port> ] [ -O <dst_port_op> ] [ -P <dst_port> ] [ -c <protocol> ]
```

Description

The **chvfilter** command is used to change the definition of a virtual LAN-crossing filter rule in the filter rule table.

Flags

- a Specifies the action. Valid values follow:
 - D (Deny): Blocks traffic
 - P (Permit): Allows traffic
- c Specifies different protocols to which the filter rule is applicable. Valid values follow:
 - udp
 - icmp
 - icmpv6
 - tcp
 - any
- d Specifies the destination address in IPv4 or IPv6 format.
- m Specifies the source address mask.
- M Specifies the destination address mask.
- n Specifies the filter ID of the filter rule that should be modified.
- o Specifies the source port or the Internet Control Message Protocol (ICMP) type operation. Valid values follow:
 - lt
 - gt
 - eq
 - any
- O Specifies the destination port or the ICMP code operation. Valid values follow:
 - lt
 - gt
 - eq

- any
- p Specifies the source port or the ICMP type.
- P Specifies the destination port or the ICMP code.
- s Specifies the source address in v4 or v6 format.
- v Specifies the IP version of the filter rule table. Valid values are 4 and 6.
- z Specifies the virtual LAN ID of the source logical partition.
- Z Specifies the virtual LAN ID of the destination logical partition.

Exit Status

This command returns the following exit values:

- 0 Successful completion.
- >0 An error occurred.

Examples

- To change a valid filter rule that exists in the kernel, type the command as follows:

```
chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -0 lt -P 345 -c tcp
```

- When a filter rule (n=2) does not exist in the kernel, the output is as follows:

```
chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -0 lt -P 345 -c tcp
```

The system displays the output as follows:

```
ioctl(QUERY_FILTER) failed no filter rule err=2
Cannot Change the filter rule.
```

genvfilt command

Purpose

Adds a filter rule for the virtual LAN (VLAN) crossing between logical partitions on the same IBM Power Systems server.

Syntax

```
genvfilt -v <4|6> -a <D|P> -z <svlan> -Z <dvlan> [-s <s_addr> ] [-d <d_addr> ] [-o <src_port_op> ] [-p <src_port> ] [-O <dst_port_op> ] [-P <dst_port> ] [-c <protocol> ]
```

Description

The **genvfilt** command adds a filter rule for the virtual LAN (VLAN) crossing between logical partitions (LPARs) on the same IBM Power Systems server.

Flags

- a Specifies the action. Valid values follow:
 - D (Deny): Blocks traffic
 - P (Permit): Allows traffic
- c Specifies different protocols to which the filter rule is applicable. Valid values follow:
 - udp
 - icmp
 - icmpv6

- tcp
 - any
- d Specifies the destination address in v4 or v6 format.
 - m Specifies the source address mask
 - M Specifies the destination address mask.
 - o Specifies the source port or the Internet Control Message Protocol (ICMP) type operation. Valid values follow:
 - lt
 - gt
 - eq
 - any
 - O Specifies the destination port or the ICMP code operation. Valid values follow:
 - lt
 - gt
 - eq
 - any
 - p Specifies the source port or the ICMP type.
 - P Specifies the destination port or the ICMP code.
 - s Specifies the source address in IPv4 or IPv6 format.
 - v Specifies the IP version of the filter rule table. Valid values are 4 and 6.
 - | -z Specifies the virtual LAN ID of the source LPAR. The virtual LAN ID must be in the range of 1 - 4096.
 - | -Z Specifies the virtual LAN ID of the destination LPAR. The virtual LAN ID must be in the range of 1 - 4096.

Exit Status

This command returns the following exit values:

- 0 Successful completion.
- >0 An error occurred.

Examples

1. To add a filter rule to permit TCP data from a source VLAN ID of 100 to a destination VLAN ID of 200 on specific ports, type the command as follows:

```
genvfilt -v4 -a P -z 100 -Z 200 -o lt -p 345 -O lt -P 345 -c tcp
```

Related reference:

- “mkvfilt command” on page 58
- “vlantfw command” on page 68

lsvfilt command

Purpose

Lists virtual LAN-crossing filter rules from the filter table.

Syntax

lsvfilt [-a]

Description

The **lsvfilt** command is used to list the virtual LAN-crossing filter rules and their status.

Flags

-a Lists only the active filter rules.

Exit Status

This command returns the following exit values:

- 0** Successful completion.
- >0** An error occurred.

Examples

1. To list all the active filter rules in the kernel, type the command as follows:

```
lsvfilt -a
```

Related concepts:

“Deactivating rules” on page 37

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

mkvfilt command

Purpose

Activates the virtual LAN-crossing filter rules defined by the **genvfilt** command.

Syntax

mkvfilt -u

Description

The **mkvfilt** command activates the virtual LAN-crossing filter rules defined by the **genvfilt** command.

Flags

-u Activates the filter rules in the filter rule table.

Exit Status

This command returns the following exit values:

- 0** Successful completion.
- >0** An error occurred.

Examples

1. To activate the filter rules in the kernel, type the command as follows:

```
mkvfilt -u
```

Related reference:

pmconf command

Purpose

Reports and manages the trusted network connect patch management (TNCPM) server by registering technology levels and TNC servers for latest fixes and generating reports on TNCPM status.

Note: The TNCPM server must be run only on AIX Version 7.1 with the 7100-02 Technology Level to allow the download of the service pack metadata.

Syntax

pmconf mktncpm [**pmport**=<port>] **tncserver**=ip | hostname : port

pmconf rmtncpm

pmconf start

pmconf stop

| **pmconf init** -i <download interval> -l <TL List> -A [-P <download path>] [-x <ifix interval>] [-K <ifix
| key>]

pmconf add -l TL_list

pmconf add -p <SP List> [-U <user-defined SP path>]

| **pmconf add** -p <SP> -e <ifix file>

| **pmconf add** -y <advisory file> -v <signature file> -e <ifix tar file>

pmconf delete -l TL_list

pmconf delete -p <SP List>

| **pmconf delete** -p <SP>-e ifix file

pmconf list -s [-c] [-q]

pmconf list -l SP

pmconf list -C

pmconf list -a SP

pmconf hist -u

pmconf hist -d

pmconf import -f cert_filename -k key_filename

pmconf export -f filename

pmconf modify -i < download interval>

pmconf modify -P <download path>

pmconf modify -g <yes or no to accept all licenses>

pmconf modify -t <APAR type list>

| **pmconf modify -x** <ifix interval>

| **pmconf modify -K** <ifix key>

pmconf delete -l <TL list>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = value

Description

The functions of the **pmconf** command are as follows:

Fix repository management

Registers or unregisters technology levels; unregisters TNC servers. TNCPM creates a fix repository for each technology level that contains the latest fixes, **lspp** information (for example, information about installed file sets or file set updates), and security fix information for that technology level.

Reporting

Generates reports on the status of TNCPM.

The following operations can be performed by using the **pmconf** command:

Item	Description
add	Registers a new technology level by using TNCPM.
chtncpm	Changes the attributes in the tncs.conf file. An explicit start command is required for the changes to take effect in the TNCPM server.
delete	Unregisters a technology level by using TNCPM.
history	Displays update and download history.
list	Displays the information about TNCPM.
log	Sets the log level for the TNC components.
mktnrpm	Creates the TNCPM server.
modify	Modifies the tncpm.conf attributes.
rmtncpm	Removes the TNCPM server.
start	Starts the TNCPM server.
stop	Stops the TNCPM server.

Flags

Item	Description
-A	Accepts all license agreements when performing client updates.
-a <advisory file>	Specifies the advisory file that corresponds to the ifix parameter. If the advisory file is not provided, the ifix parameter is not viewed as a common vulnerabilities and exposures (CVE) address of the interim fix.
-e <ifix file>	Specifies the interim fixes that are added to the TNCPM.
-i <download_interval>	Specifies the interval that TNCPM checks for a new service pack for the registered technology levels. The interval is an integer value that represents minutes or in the following format: d (no of days): h (hours): m (minutes).
-K <ifix key>	Specifies the public key of IBM AIX Product Security Incident Response Tool (PSIRT) that is used to authenticate the downloaded advisories and interim fixes. This public key can be downloaded from a PGP public key server by using the 0x28BFAA12 ID.
-p <SP_list>	Specifies a list of service packs to be downloaded. The list is a comma-separated list in the format, REL00-TL-SP (for example, 6100-01-04 represents the service pack 04 for technology level 01 and version 6.1). When you use the -U flag, specify only one SP.
-t <APAR_type_list>	Specifies the APAR types that the TNCPM supports for the client update and TNC server listing. Security APARs are always supported. APAR_type_list is a comma-separated list of the following types: HIPER, FileNet® Process Engine, Enhancement.
-P <fix_repository_path>	Specifies the download directory for the fix repositories that will be download by TNCPM. The default directory is /var/tnc/tncpm/fix_repository .
-U <user_defined_fix_repository>	Specifies the path to the user-defined fix repository. Specify the release, the technology level, and the service pack that are associated with the fix repository that is used for verification and updates of clients.
-s	Generates a report of registered service packs.
-l <SP>	Generates a report of lspp information for the service pack. <i>SP</i> is in the format, REL00-TL-SP (for example, 6100-01-04 represents the service pack 04 for technology level 01 and version 6.1).
-u	Generates a report of the client update history.
-d	Generates a report of the service pack download history.
-C	Generates a report for the server certificate.
-a <SP>	Generates a report of security authorized program analysis report (APAR) information for the service pack. <i>SP</i> is in the format, REL00-TL-SP (for example, 6100-01-04 represents the service pack 04 for technology level 01 and version 6.1).
-f <filename>	Specifies the certificate file name.
-k <key_filename>	Specifies the file from which the certificate key must be read in case of an import operation.
-c	Displays the user attributes in colon-separated records, as follows: # name: <i>attribute1: attribute2: ...</i> policy: <i>value1: value2: ...</i>
-v <signature file>	Specifies the signature file for the IBM AIX vulnerability advisory.
-y <advisory file>	Specifies an IBM AIX vulnerability advisory file.
-q	Suppresses the header information.
-x <ifix interval>	Specifies the interval in minutes to check for and download new interim fixes. If this value is set to 0, the automatic interim fix download and notification is disabled. The default interval is every 24 hours.

Exit Status

This command returns the following exit values:

Item	Description
0	The command ran successfully, and all the requested changes are made.
>0	An error occurred. The printed error message includes more details about the type of failure.

Examples

- To initialize TNCPM, enter the following command:
pmconf init -f 10080 -l 5300-11,6100-00
- To create the TNCPM daemon, enter the following command:
mktncpm pmport=55777 tncserver=11.11.11.11:77555
- To start the server, enter the following command:
pmconf start
- To stop the server, enter the following command:
pmconf stop
- To register a new technology level by using TNCPM, enter the following command:

- ```
pmconf add -l 6100-01
```
6. To unregister a technology level from TNCPM, enter the following command:
 

```
pmconf delete -l 6100-01
```
  7. To unregister a TNC server that has an IP address of 11.11.11.11 from TNCPM, enter the following command:
 

```
pmconf delete -t 11.11.11.11
```
  8. To register a newer version of an earlier service pack to TNCPM, enter the following command:
 

```
pmconf add -s 6100-01-04
```
  9. To unregister an earlier service pack from TNCPM, enter the following command:
 

```
pmconf delete -s 6100-01-04
```
  10. To generate a report of fix repositories for each registered technology level, enter the following command:
 

```
pmconf list -s
```
  11. To generate a report of a registered technology level **lslpp** information, enter the following command:
 

```
pmconf list -l 6100-01-02
```
  12. To generate a report from the update history, enter the following command:
 

```
pmconf hist -u
```
  13. To generate a report from the download history, enter the following command:
 

```
pmconf hist -d
```
  14. To generate a report of the server certificate, enter the following command:
 

```
pmconf list -C
```
  15. To generate a report of a service pack security APAR information, enter the following command:
 

```
pmconf list -a 6100-01-02
```
  16. To import a server certificate, enter the following command:
 

```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```
  17. To export the server certificate, enter the following command:
 

```
pmconf export -f /tmp/server.txt
```

---

## psconf command

### Purpose

Reports and manages the Trusted Network Connect (TNC) server, the TNC client, the TNC IP Referrer (IPRef), and Service Update Management Assistant (SUMA). It manages fileset and patch management policies regarding endpoint (server and client) integrity at or after network connection to protect the network from threats and attacks.

### Syntax

TNC server operations:

```
| psconf mkserver [tncport=<port>] pmserver=<host:port> [tsserver=<host>] [
```

```
| recheck_interval=<time_in_minutes> | d (days) : h (hours) : m (minutes)] [dbpath = <user-defined
```

```
| directory>]
```

```
psconf { rmserver | status }
```

```
psconf { start | stop | restart } server
```

```
psconf chserver attribute = value
```

```

| psconf add -F <FSPolicyname> -r <buildinfo> [apargrp= [±]<apargrp1, apargrp2.. >] [ifixgrp=[+|-
| <ifixgrp1,ifixgrp2...>]

| psconf add { -G <ipgroupname> ip=[±]<host1, host2...> | -A<apargrp> [aparlist=[±]apar1, apar2... | -V
| <ifixgrp> [ifixlist=[+|-]ifix1,ifix2...]}

psconf add -P <policyname> { fspolicy=[±]<f1,f2...> | ipgroup=[±]<g1,g2...> }

psconf add -e emailid [-E FAIL | COMPLIANT | ALL] [ipgroup= [±]<g1,g2...>]

psconf add -I ip= [±]<host1, host2...>

| psconf delete { -F <FSPolicyname> | -G <ipgroupname> | -P <policyname> | -A <apargrp> | -V <ifixgrp>}

psconf delete -H -i <host | ALL> -D <yyyy-mm-dd>

psconf certadd -i <host> -t <TRUSTED | UNTRUSTED>

psconf certdel -i <host>

psconf verify -i <host> | -G <ipgroup>

| psconf update [-p] {-i <host >| -G <ipgroup> [-r <buildinfo> | -a <apar1, apar2...> | [-u] -v <ifix1, ifix2,...>}

psconf log loglevel=<info | error | none>

psconf import -C -i <host> -f <filename> | -d <import database filename>

psconf { import -k <key_filename> | export} -S -f <filename>

| psconf list { -S | -G < ipgroupname | ALL > | -F < FSPolicyname | ALL > | -P < policyname | ALL > | -r
| < buildinfo | ALL > | -I -i < ip | ALL > | -A < apargrp | ALL > | -V < ifixgrp>} [-c] [-q]

psconf list { -H | -s <COMPLIANT | IGNORE | FAILED | ALL> } -i <host | ALL> [-c] [-q]

psconf export -d <path to export directory>

| psconf report -v <CVEid|ALL> -o <TEXT|CSV>

| psconf report -A <advisoryname>

| psconf report -P <policyname|ALL> -o <TEXT|CSV>

| psconf report -i <ip|ALL> -o <TEXT|CSV>

| psconf report -B <buildinfo|ALL> -o <TEXT|CSV>

TNC client operations:

| psconf mkclient [tncport=<port>] tncserver=<host:port>

| psconf mkclient tncport=<port> -T

psconf { rmclient | status }

psconf {start | stop | restart } client

```

**psconf chclient** attribute = *value*

**psconf list** { **-C** | **-S** }

**psconf export** { **-C** | **-S** } **-f** <filename>

**psconf import** { **-S** | **-C -k** <key\_filename> } **-f** <filename>

TNC IPRef operations:

**psconf mkipref** [ **tncport**=<port> ] **tncserver**=<host:port>

**psconf** { **rmipref** | **status**}

**psconf** { **start** | **stop** | **restart**} ipref

**psconf chipref** attribute = *value*

**psconf** { **import -k** <key\_filename> | **export** } **-R -f** <filename>

**psconf list -R**

## Description

The TNC technology is an open standard-based architecture for endpoint authentication, platform integrity measurement, and integrating security systems. The TNC architecture inspects endpoints (network clients and servers) for compliance with security policies before allowing them on the protected network. The TNC IPRef notifies the TNC server about any new IPs that are detected on the virtual I/O server (VIOS).

SUMA helps move system administrators away from the task of manually retrieving maintenance updates from the web. It offers flexible options that enable the system administrator to set up an automated interface to download fixes from a fix distribution website to their systems.

The **psconf** command manages the network server and clients by adding or deleting security policies, validating clients as trusted or untrusted, generating reports, and updating the server and the client.

The following operations can be performed by using the **psconf** command:

| Item            | Description                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>add</b>      | Adds a policy, a client, or the email information on the TNC server.                                                                                                                                                                                                                                                                                                                     |
| <b>apargrp</b>  | Specifies the APAR group names as part of the fileset policy that are used for verification of TNC clients.                                                                                                                                                                                                                                                                              |
| <b>aparlist</b> | Specifies the list of APARs that are part of the APAR group.                                                                                                                                                                                                                                                                                                                             |
| <b>certadd</b>  | Marks the certificate as trusted or untrusted.                                                                                                                                                                                                                                                                                                                                           |
| <b>certdel</b>  | Deletes the client information.                                                                                                                                                                                                                                                                                                                                                          |
| <b>chclient</b> | Changes the attributes in the <code>tnccs.conf</code> file. An explicit <b>start</b> command is required for the changes to take effect in the TNC client. The syntax of attribute=value will be same as that of <b>mkclient</b> .                                                                                                                                                       |
| <b>chipref</b>  | Changes the attributes in the <code>tnccs.conf</code> file. An explicit <b>start</b> command is required for the changes to take effect in IPRef. The syntax of attribute=value is the same as that of the <b>mkipref</b> .                                                                                                                                                              |
| <b>chserver</b> | Changes the attributes in the <code>tnccs.conf</code> file. An explicit <b>start</b> command is required for the changes to take effect in the TNC server. The syntax of attribute=value is same as that of <b>mkserver</b> .<br><b>Note:</b> The <b>dbpath</b> attribute cannot be changed by using the <b>chserver</b> command. It can be set only while running the <b>mkserver</b> . |
| <b>dbpath</b>   | Specifies the TNC database location. The default value is <code>/var/tnc</code> .                                                                                                                                                                                                                                                                                                        |
| <b>delete</b>   | Deletes a policy or the client information.                                                                                                                                                                                                                                                                                                                                              |
| <b>export</b>   | Exports the client or server certificate , or database on TNC server.                                                                                                                                                                                                                                                                                                                    |



| Item                    | Description                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>fspolicy</b>         | Specifies the fileset policy of the release, technology level and service pack that are used for verification of TNC Clients.                                                                                                                                                                                                                                                                               |
| <b>import</b>           | Imports a certificate on client or server, or database on TNC server.                                                                                                                                                                                                                                                                                                                                       |
| <b>ipgroup</b>          | Specifies the Internet Protocol (IP) group that contains multiple client IP addresses or host names.                                                                                                                                                                                                                                                                                                        |
| <b>list</b>             | Displays information about the TNC server, the TNC client, or the SUMA.                                                                                                                                                                                                                                                                                                                                     |
| <b>log</b>              | Sets the log level for the TNC components.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>mkclient</b>         | Configures the TNC client.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>mkipref</b>          | Configures the TNC IPRef.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>mkserver</b>         | Configures the TNC server.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>pmport</b>           | Specifies the port number on which the <b>pmserver</b> listens to. The default value is 38240.                                                                                                                                                                                                                                                                                                              |
| <b>pmserver</b>         | Specifies the host name or IP address of the <b>suma</b> command that downloads the latest service packs and security fixes available in the IBM® ECC website and the IBM Fix Central website.                                                                                                                                                                                                              |
| <b>recheck_interval</b> | Specifies the interval in minutes or d (days) : h (hours) : m (minutes) format for the TNC server to verify the TNC clients.<br><b>Note:</b> A value of <b>recheck_interval=0</b> means that the scheduler does not initiate verification of the clients at regular intervals and the registered clients are automatically verified during the startup. In such cases, the client can be manually verified. |
| <b>report</b>           | Generates a report that has a .txt or .csv file extension.                                                                                                                                                                                                                                                                                                                                                  |
| <b>restart</b>          | Restarts the TNC client, the TNC server, or the TNC IPRef.                                                                                                                                                                                                                                                                                                                                                  |
| <b>rmclient</b>         | Unconfigures the TNC client.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>rmipref</b>          | Unconfigures the TNC IPRef.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>rmserver</b>         | Unconfigures the TNC server.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>start</b>            | Starts the TNC client, the TNC server, or the TNC IPRef.                                                                                                                                                                                                                                                                                                                                                    |
| <b>status</b>           | Shows the status of the TNC configuration.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>stop</b>             | Stops the TNC client, the TNC server, or the TNC IPRef.                                                                                                                                                                                                                                                                                                                                                     |
| <b>tncport</b>          | Specifies the port number on which the TNC server listens to. The default value is 42830.                                                                                                                                                                                                                                                                                                                   |
| <b>tncserver</b>        | Specifies the TNC server that verifies or updates the TNC clients.                                                                                                                                                                                                                                                                                                                                          |
| <b>tsserver</b>         | Specifies the IP or host name of the Trusted Surveyor server.                                                                                                                                                                                                                                                                                                                                               |
| <b>update</b>           | Installs patches on the client.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>verify</b>           | Initiates a manual verification of the client.                                                                                                                                                                                                                                                                                                                                                              |

## Flags

| Item                                                  | Description                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-A &lt;advisoryName&gt;</b>                        | Specifies the advisory name for the report.                                                                                                                                                                                                                                                                                       |
| <b>-B &lt;buildinfo&gt;</b>                           | Specifies the build information to prepare a patch report.                                                                                                                                                                                                                                                                        |
| <b>-c</b>                                             | Displays the user attributes in colon-separated records as follows:<br><i># name: attribute1: attribute2: ...</i><br><i>policy: value1: value2: ...</i>                                                                                                                                                                           |
| <b>-C</b>                                             | Specifies that the operation is for client component.                                                                                                                                                                                                                                                                             |
| <b>-d database file location/dir path of database</b> | Specifies the file path location for import of the database/specifies the directory path location for export of the database.                                                                                                                                                                                                     |
| <b>-D yyyy-mm-dd</b>                                  | Specifies the date for a particular client entry in the log history, where <i>yyyy</i> is the year, <i>mm</i> in the month, and <i>dd</i> is the day.                                                                                                                                                                             |
| <b>-e emailid ipgroup=[±]g1, g2...</b>                | Specifies the email ID followed by a comma separated IP group name list.                                                                                                                                                                                                                                                          |
| <b>-E   FAIL   COMPLIANT   ALL  </b>                  | Specifies the event for which the emails need to be sent to the configured email id.<br>FAIL- Mails are sent when the verification status of the client is FAILED.<br>COMPLIANT- Mails are sent when the verification status of the client is COMPLIANT.<br>ALL - Mails are sent for all the statuses of the client verification. |
| <b>-f filename</b>                                    | Specifies the file from which the certificate must be read in case of an import operation, or specifies the location to which the certificate must be written in case of an export operation.                                                                                                                                     |
| <b>-F fspolicy buildinfo</b>                          | Specifies the file system policy name, followed by the build information. The build information can be provided in the following format:<br>6100-04-01, where 6100 represents version 6.1, 04 is the maintenance level, and 01 is the service pack.                                                                               |

| Item                                      | Description                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -G <i>ipgroupname</i> ip=[±]ip1, ip2...   | Specifies the IP group name followed by a comma-separated IP list.                                                                                                                                                                                                                                                                                                       |
| -H                                        | Lists the history log.                                                                                                                                                                                                                                                                                                                                                   |
| -i <i>host</i>                            | Specifies the IP address or host name.                                                                                                                                                                                                                                                                                                                                   |
| -I ip=[±]ip1, ip2...   [±] host1,host2... | Specifies the IP/host name that must be ignored during verification.                                                                                                                                                                                                                                                                                                     |
| -k <i>filename</i>                        | Specifies the file from which the certificate key must be read in case of an import operation.                                                                                                                                                                                                                                                                           |
| -p                                        | Previews the TNC client update.                                                                                                                                                                                                                                                                                                                                          |
| -P <policyName>                           | Specifies the policy name to prepare a client policy report.                                                                                                                                                                                                                                                                                                             |
| -q                                        | Suppresses the header information.                                                                                                                                                                                                                                                                                                                                       |
| -r <i>buildinfo</i>                       | Generates the report based on the build information. The build information can be provided in the following format:<br><br>6100-04-01, where 6100 represents version 6.1, 04 is the maintenance level, and 01 is the service pack.                                                                                                                                       |
| -R                                        | Specifies that the operation is for IPRef component.                                                                                                                                                                                                                                                                                                                     |
| -s COMPLIANT   IGNORE   FAILED   ALL      | Displays the client by status as follows:<br><br><b>COMPLIANT</b><br>Displays the active clients.<br><br><b>IGNORE</b><br>Displays the clients that are excluded from any verification.<br><br><b>FAILED</b> Displays the clients that have failed verification as per the configured policy.<br><br><b>ALL</b> Displays all the clients irrespective of their statuses. |
| -S <host>                                 | Specifies the host name to prepare a client security fix report.                                                                                                                                                                                                                                                                                                         |
| -t TRUSTED   UNTRUSTED                    | Marks the specified client as trusted or untrusted.<br><b>Note:</b> Only system administrators can verify the server or client as trusted or untrusted.                                                                                                                                                                                                                  |
| -T                                        | Specifies that the client can accept request from any TS server that has a valid certificate.                                                                                                                                                                                                                                                                            |
| -u                                        | Uninstalls an interim fix that is installed on a TNC client.                                                                                                                                                                                                                                                                                                             |
| -v                                        | Specifies a comma-separated interim fix list.                                                                                                                                                                                                                                                                                                                            |
| -V                                        | Specifies the interim fix group name.                                                                                                                                                                                                                                                                                                                                    |

## Exit Status

This command returns the following exit values:

| Item | Description                                                                                   |
|------|-----------------------------------------------------------------------------------------------|
| 0    | The command ran successfully, and all the requested changes are made.                         |
| >0   | An error occurred. The printed error message includes more details about the type of failure. |

## Examples

- To start the TNC server, enter the following command:  
psconf start server
- To add a file system policy named 71D\_latest for the build 7100-04-02, enter the following command:  
psconf add -F 71D\_latest 7100-04-02
- To delete a file system policy named 71D\_old, enter the following command:  
psconf delete -F 71D\_old
- To validate that the client that has an IP address of 11.11.11.11 is **trusted**, enter the following command:  
psconf certadd -i 11.11.11.11 -t TRUSTED
- To delete the client that has an IP address of 11.11.11.11 from the server, enter the following command:  
psconf certdel -i 11.11.11.11
- To verify the client information that has an IP address of 11.11.11.11, enter the following command:

- ```
psconf verify -i 11.11.11.11
```
7. To display the client information that has an IP address of 11.11.11.11, enter the following command:

```
psconf list -i 11.11.11.11
```
 8. To generate the report for clients that are in **COMPLAINT** status, enter the following command:

```
psconf list -s COMPLAINT -i ALL
```
 9. To generate the report for the build 7100-04-02, enter the following command:

```
psconf list -r 7100-04-02
```
 10. To display the connection history of a client that has an IP address of 11.11.11.11, enter the following command:

```
psconf list -H -i 11.11.11.11
```
 11. To delete the entry of a client that has an IP address of 11.11.11.11 from the log history older or equal to 1 February, 2009, enter the following command:

```
psconf delete -H -i 11.11.11.11 -D 2009-02-01
```
 12. To import the client certificate of a client that has an IP address of 11.11.11.11 from the server, enter the following command:

```
psconf import -C -i 11.11.11.11 -f /tmp/client.txt
```
 13. To export the server certificate from a client, enter the following command:

```
psconf export -S -f /tmp/server.txt
```
 14. To update the client that has an IP address of 11.11.11.11 to an appropriate level from the server, enter the following command:

```
psconf update -i 11.11.11.11
```
 15. To display the client statuses, enter the following command:

```
psconf status
```
 16. To display the client certificate, enter the following command:

```
psconf list -C
```
 17. To start the client, enter the following command:

```
psconf start client
```

Security

Attention RBAC users and Trusted AIX users:

This command can perform privileged operations. Only privileged users can run privileged operations. For more information about authorizations and privileges, see Privileged Command Database in Security. For a list of privileges and the authorizations associated with this command, see the **lssecattr** command or the **getcmdattr** subcommand

rmvfilt command

Purpose

Removes the virtual LAN-crossing filter rules from the filter table.

Syntax

```
rmvfilt -n [fid|all> ]
```

Description

The **rmvfilt** command is used to remove the virtual LAN-crossing filter rules from the filter table.

Flags

-n Specifies the ID of the filter rule that will be removed. The **all** option is used to remove all the filter rules.

Exit Status

This command returns the following exit values:

0 Successful completion.

>0 An error occurred.

Examples

1. To remove all the filter rules or to deactivate all the filter rules in the kernel, type the command as follows:

```
rmvfilt -n all
```

Related concepts:

“Deactivating rules” on page 37

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

vlanfw command

Purpose

Displays or clears the IP and Media Access Control (MAC) mapping information, and controls the logging function.

Syntax

vlanfw -h | -s | -t | -d | -f | -G | -q | -D | -E | -F | -i | -I | -L | -m | -M | -N *integer*

Description

The **vlanfw** command displays or clears the IP and MAC mapping entries. It also provides the ability to start or stop the Trusted Firewall logging facility.

Flags

-d Displays all the IP mapping information.

-D Displays the collected connection data.

-E Displays the connection data between logical partitions (LPARs) on different central processor complexes.

-f Removes all the IP mapping information.

-F Clears the connection data cache.

-G Displays the filter rules that can be configured to route the traffic internally by using Trusted Firewall.

-I Displays the connection data between LPARs that are associated with different VLAN IDs, but share the same central processor complexes.

-l Starts the Trusted Firewall logging facility.

-L Stops the Trusted Firewall logging facility and redirects the trace file contents to the `/home/padmin/svm/svm.log` file.

- | **-m** Enables Trusted Firewall monitoring.
- | **-M** Disables Trusted Firewall monitoring.
- | **-q** Queries the secure virtual machine status.
- | **-s** Starts the Trusted Firewall.
- | **-t** Stops the Trusted Firewall.

| **Parameters**

- | **-N** *integer*
- | Displays the filter rule that corresponds to the integer that is specified.

Exit Status

This command returns the following exit values:

- 0** Successful completion.
- >0** An error occurred.

Examples

1. To display all the IP mappings, type the command as follows:
vlantfw -d
2. To remove all the IP mappings, type the command as follows:
vlantfw -f
- | 3. To start the Trusted Firewall logging function, type the command as follows:
| vlantfw -l
4. To check the status of a secure virtual machine, type the command as follows:
vlantfw -q
5. To start trusted firewall, type the command as follows:
vlantfw -s
6. To stop trusted firewall, type the command as follows:
vlantfw -t
- | 7. To display the corresponding rules that can be used to generate filters that route traffic within the
| central processor complex, type the command as follows:
| vlantfw -G

Related reference:

“genvfilt command” on page 56

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 41
AIX syslog 41
Attesting a system 28

C

chvfilt command 55
Client Policies 49
Client verification 50
Commands
 chvfilt 55
 genvfilt 56
 lsvfilt 57
 mkvfilt 58
 rmvfilt 67
 vlantfw 68
Components 43
concepts 43
Configuring 46
Configuring client 46
Configuring patch management server 47
Configuring server 46
Configuring the trusted logging 41
Configuring Trusted Boot 27
Configuring Trusted Logging 40, 41

D

Deleting systems 29

E

email notification 48
enrolling a system 28

G

genvfilt command 56

H

hardware and software requirements 5

I

IMC and IMV modules 45
import certificates 44
Import certificates 51
Installing 7, 45
Installing PowerSC Standard Edition 7
Installing the collector 27
Installing the verifier 27
Installing Trusted Boot 27
Interpreting attestation results 28
IP Referrer 44
IP Referrer on VIOS 48

L

lsvfilt command 57

M

Managing policies 51
Managing TNC and Patch management 49
Managing Trusted Boot 28
Migration considerations 27
mkvfilt command 58

O

overview 5, 43

P

Patch management 43
Payment Card Industry - DSS compliance 10
Planning 26
pmconf command 59
PowerSC 10
 Trusted Firewall
 configuring 34
 configuring with multiple SEAs 35
 creating rules 36
 deactivating rules 37
 installing 33
 removing SEAs 36
 Trusted Logging
 installing 40
PowerSC Standard Edition 5, 7
Preparing for remediation 26
Prerequisites 26
Protocol 44
psconf command 62

R

Reporting and management tool for TNC, SUMA
 using psconf command 62
Reporting and management tool for TNC/CPM
 using pmconf command 59
rmvfilt command 67

S

secure communication 44
Server 43
SUMA 43

T

TNC 52
TNC client 43
troubleshooting 29
Troubleshooting TNC and Patch management 52
Trusted Boot 25, 26, 27, 28, 29

- Trusted Boot concepts 25
- Trusted Firewall 31
 - configuring 34
 - multiple SEAs 35
 - creating rules 36
 - deactivating rules 37
 - installing 33
 - removing
 - SEAs 36
- Trusted Firewall concepts 31
- Trusted Logging 39, 42
 - installing 40
- Trusted Logging overview 39
- Trusted network connect 46, 50, 51
- Trusted Network Connect 43, 44, 45, 46, 47, 48, 49, 50, 51
- Trusted Network Connect and Patch management 43
- Trusted Network Connect server 48, 49

U

- Updating TNC client 51

V

- Viewing logs 49
- Viewing verification results 50
- Viewing virtual log devices 39
- virtual logs 39
- vlanfw command 68

W

- Writing data to virtual log devices 42



Printed in USA