

PowerSC

An introduction to PowerSC 2.1.0.4 with ClamAV

Stephen Dominguez – sdoming@us.ibm.com – <https://www.securitysteve.net>

Agenda

PowerSC Topics

Introduction

Security and Compliance

AIX Patch Management

Multi-Factor Authentication

Malware Prevention on AIX (Including ClamAV)



Introduction

The History of PowerSC

- Dec 2011 – Release 1.0.0.0 – AIX Development
- 2016 – Rocket Software becomes the PowerSC Development Partner with IBM
- Dec 2017 – Release 1.1.5.0 PowerSC GUI and initial PMFA release
- Dec 2018 – Release 1.2.0.0
- Dec 2019 – Release 1.3.0.0
- Sept 2021 – Release 2.0.0.0 – Standard Edition and PMFA merge under 2.0.0.0
- Dec 2022 – Release 2.1.0.4 – ClamAV support for AIX added



PowerSC Licensing & Support

- Licensing is based on a per-core basis
- PowerSC 2.0 consists of "PowerSC Standard Edition" and "PowerSC MFA"
- PowerSC Standalone Licensing – the least expensive but not necessarily the best value, because the higher tiers are software bundles
- Once the proper licensing is paid for, the customer may download PowerSC from Entitled Systems Support (ESS)
- Work with your IBM Seller or Business Partner to obtain proper licensing



PowerSC 2.0 Licensing Matrix

	AIX Standard Edition	PowerSC Standalone	AIX Enterprise Edition	Enterprise Cloud Edition with AIX	Enterprise Cloud Edition
AIX	No	yes	Yes	Yes	Yes
LoP	No	yes	No	No	Yes
IBM i	No	yes	No	No	Yes

90 Day Trial

- IBM Seller or Business Partner is responsible for managing the trial
- After 90 days, must be removed if no license was acquired
- This is only for evaluation; it can't be used on production systems
- Trial download link:
<https://epwt-www.mybluemix.net/software/support/trial/cst/programwebsite.wss?siteId=1287&h=null&p=null>



PowerSC 2.0

Standard Edition	Multi-Factor Authentication
GUI Server	MFA Server & Clients
GUI Agent	
Security & Compliance Automation	
Real Time Compliance	
Trusted Network Connect & Patch Management	
Trusted Logging	
Trusted Boot	
Trusted Firewall	



PowerSC Standard Edition requirements - AIX

Table 1. AIX JRE prerequisites

Component	Operating System	Minimum Java JRE version
PowerSC GUI server	AIX	Java 8, 64-bit
PowerSC GUI agent	AIX	Java 8, 64-bit

PowerSC GUI server

- AIX 7.1 , or later

PowerSC GUI agent

- 7200-04, 7200-05, AIX 7.3
- Minimum required level for 7100 is 7100-05-05



PowerSC Standard Edition requirements - Linux

PowerSC GUI server

PowerSC GUI agent

Power Servers

- Linux on Power® servers running SUSE Linux Enterprise Server 15, or later on IBM® Power systems
- Linux on Power servers running SUSE Linux Enterprise Server for SAP Applications 15, or later on IBM Power systems
- Linux on Power servers running Red Hat Enterprise Linux Server 8.3, or later on IBM Power systems

- Linux on Power servers running SUSE Linux Enterprise Server 15, or later on IBM Power systems
- Linux on Power servers running SUSE Linux Enterprise Server for SAP Applications 15, or later on IBM Power systems
- Linux on Power servers running Red Hat Enterprise Linux Server 8.3, or later on IBM Power systems

Intel Systems

- Linux on Intel systems running SUSE Linux Enterprise Server 15, or later
- Linux on Intel systems running SUSE Linux Enterprise Server for SAP Applications 15, or later
- Linux on Intel systems running Red Hat Enterprise Linux Server 8.3, or later

- Linux on Intel systems running SUSE Linux Enterprise Server 15, or later
- Linux on Intel systems running SUSE Linux Enterprise Server for SAP Applications 15, or later
- Linux on Intel systems running Red Hat Enterprise Linux Server 8.3, or later



PowerSC Standard Edition requirements – IBM i

Table 7. IBM i operating system requirements

PowerSC GUI agent

- IBM i V7R2M0, or later

Table 1. IBM i JRE prerequisites

Component	Operating System	Minimum Java JRE version
PowerSC GUI agent	IBM i	Java 8, 64-bit or Java 8, 32-bit

PowerSC Standard Edition Requirements - HMC

- HMC V10 R2 M1030 and above
- HMC Hardening

IBM i Features with PowerSC

Name	Description
Compliance	IBM i Best Practices profile provided. Provides security hardening measures for the categories of “System-wide access control”, “Password policies”, “System security”, “Login controls”, “System auditing”, “Secure connections”, “User profile security”, “Network services”, “Group PTF currency status”, “Patch status individual PTFs”, and “Default passwords”. See PowerSC documentation for full details.
File Integrity Management (FIM)	IBM i Audit File list supported using options: OBJAUD, SUBTREE, and CRTOBJAUD. See PowerSC documentation for full details.
Security Patches	Function for verifying security patches on endpoint
Host Intrusion	Provides protection against brute force attacks



IBM i Features with PowerSC

Name	Description
Enhanced Detection and Response (EDR)	EDR supported for IBM i: Compliance, FIM, and Host Intrusion
Multi-Factor Authentication	When you authenticate an IBM i user through IBM PowerSC MFA authentication, the IBM i user no longer uses their password to log in. Instead, they use the out-of-band workflow to generate a cache token credential (CTC) and use that CTC as their password.



Security and Compliance

Subset excluding TNC. Malware Prevention and MFA

Cybersecurity Context - CIS v8

4.6 Securely Manage Enterprise Assets and Software

Network

Protect



Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

8.9 Centralize Audit Logs

Network

Detect



Centralize, to the extent possible, audit log collection and retention across enterprise assets.

8.12 Collect Service Provider Logs

Data

Detect



Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.



Cybersecurity Context - CIS v8

13.1 Centralize Security Event Alerting

Network

Detect



Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

13.2 Deploy a Host-Based Intrusion Detection Solution

Devices

Detect



Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

13.7 Deploy a Host-Based Intrusion Prevention Solution

Devices

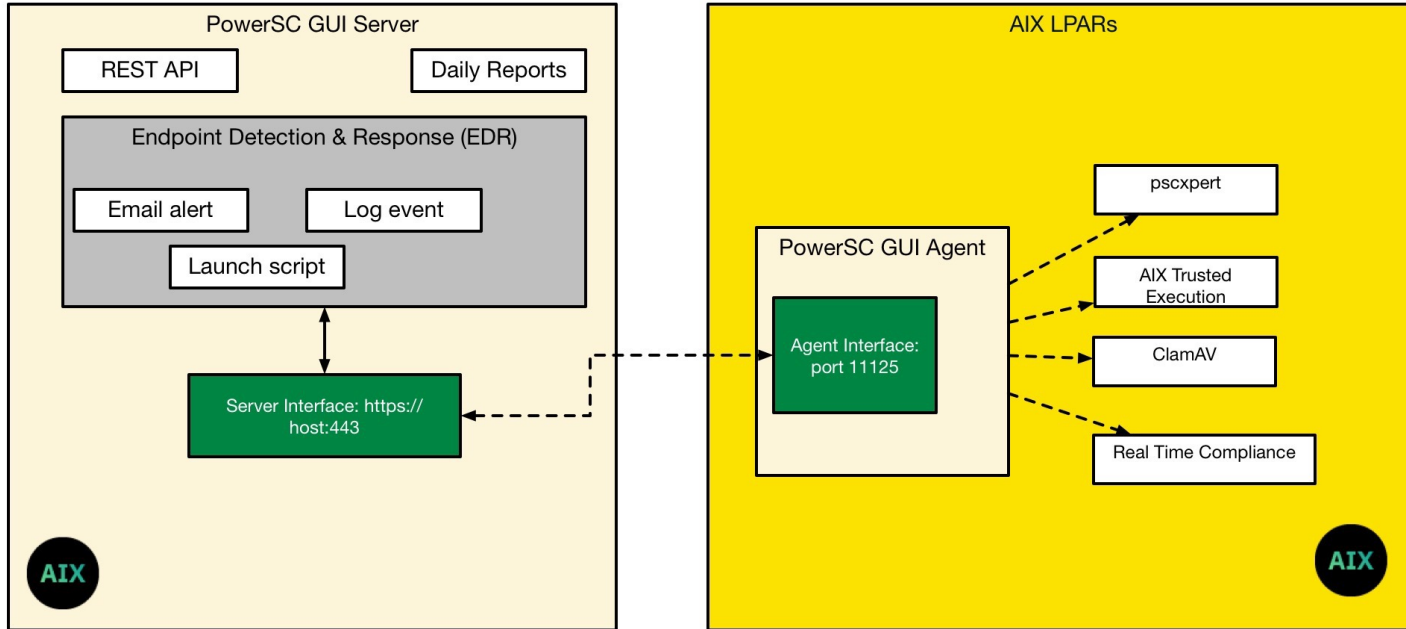
Protect



Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.



PowerSC GUI Topology - AIX



Security Measures – PowerSC GUI server

Security Measure	AIX	Linux	IBM i
Compliance	pscxpert	pscxpert	pscxpert
File Integrity Management	Real Time Compliance	Auditd	IBM i audit
	AIX Trusted Execution		
Blocklisting	Yes	Yes	Yes
Allowlisting	AIX Trusted Execution	fapolicyd	No
Traditional Endpoint Malware Detection & Prevention	ClamAV	ClamAV	No
Intrusion Detection Service	Real Time Compliance	psad	Brute force password
Security Patching	Trusted Network Connect & Patch Management	yum or zypper	yes
Enhanced Detection & Response	Yes	Yes	Yes
Security Forensics	Event Analysis Tool	Event Analysis Tool	Event Analysis Tool



Centralized Security Management

- Organize PowerSC GUI Agents with user-defined and automated PowerSC groups
- Provides separation of duties via administrative access control
- Provides highly granular configuration options to handle simple to extremely complex AIX environments
- Copy the configuration and security from one endpoint to any group of endpoints
- Extensive reporting options
- Support for automation via REST API



Scalability

- Scalability is EXCELLENT
- Excellent performance for up to 500 endpoints
- Performance possible with 1000 endpoints when using small groups
- Subsequent releases are providing performance improvements



What PowerSC is NOT

- SIEM
- Data Encryption
- Centralized User & Group Management



AIX XMLs – Rocket Software

Name	Description
CISv1.xml	1 st generally recommended; Dec 2019
DoDv7.xml	Dec 2019
GDPRv1.xml	June 2018
PCIv3.xml	Dec 2017
NERCv5.xml	April 2017

Linux XMLs – Rocket Software

Name	Description
Linux_CISv1.xml	March 2021
Linux_SAPHANAv1.xml	April 2020
Linux_GDPRv1.xml	Updated April 2019
Linux_PCIV3.xml	Updated April 2019



System i

Name	Description
IBMi_best_practices.xml	Dec 2019



VIOS XMLs – Rocket Software

Name	Description
VIOS_PCIv3.xml	Nov 2020
VIOS_CISv1.xml	Nov 2020





HMC

Name	Description
Linux_HMCv1.xml	2022



What Does it Look Like?


IBM PowerSC **Compliance** Configuration  root 

All Systems 4 Systems


System Passes and Failures






100% 4 Passes 0 Failures 0%

Total Rules Checked

12 

Specific Rules Failed

0 

 Apply Profiles  Undo  Check  Refresh Table  Refresh Interval

<input type="checkbox"/>	System Name	Compliance Rule Type	Applied Timestamp	Checked Timestamp	Compliance Status	#Failed Rules	#Passed Rules
<input type="checkbox"/>	lbsaix1.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 2:27:24 PM	1/27/2017, 12:27:17 PM	Passed	0	3
<input type="checkbox"/>	lbsaix7.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 2:27:31 PM	1/19/2017, 2:27:56 PM	Passed	0	3
<input type="checkbox"/>	lbspta1.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 2:27:30 PM	1/19/2017, 2:27:55 PM	Passed	0	3
<input type="checkbox"/>	lbtnc1.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 1:37:06 PM	1/19/2017, 2:28:37 PM	Passed	0	3



Compliance Failure

All Systems 4 Systems

System Passes and Failures




Total Rules Checked


12 


Specific Rules Failed

1 

Apply Profiles Undo Check Refresh Table Refresh Interval

Filtering by text 

<input type="checkbox"/>	System Name	Compliance Rule Type	Applied Timestamp	Checked Timestamp	Compliance Status	#Failed Rules	#Passed Rules
<input type="checkbox"/>	lbsaix1.aus.stglabs.ibm.com	PClv3_Custom	1/19/2017, 2:27:24 PM	1/30/2017, 3:44:13 PM	Passed	0	3
<input checked="" type="checkbox"/>	lbsaix7.aus.stglabs.ibm.com	PClv3_Custom	1/19/2017, 2:27:31 PM	1/30/2017, 3:44:20 PM	Failed	1	2
	1/30/2017, 3:44:20 PM pciv3_minlen_AF857627: User attribute minlen for Ip should have value 7 but it is 0 now						
<input type="checkbox"/>	lbspta1.aus.stglabs.ibm.com	PClv3_Custom	1/19/2017, 2:27:30 PM	1/30/2017, 3:44:19 PM	Passed	0	3
<input type="checkbox"/>	lbtnc1.aus.stglabs.ibm.com	PClv3_Custom	1/19/2017, 1:37:06 PM	1/30/2017, 3:45:06 PM	Passed	0	3



Profile Editor

Group Editor

Profile Editor

Endpoint Admin

PCIV3.xml



Save



Delete Profile



Save as New Custom Profile



Copy Profile to Group Members

Filtering by text



NERC_to_AIXDefault.xml

NERCv5.xml

NERCv5_to_AIXDefault.xml

PCI.xml

PCI_to_AIXDefault.xml

PCIV3.xml

PCIV3_to_AIXDefault.xml

SOX-COBIT.xml

Custom

<input checked="" type="checkbox"/>	Rule Name	Type	Description
<input checked="" type="checkbox"/>	prereqrl	Prereq	Prereq rule for remote root login: Checks whether any non-root user exists with privileges to login remotely.
<input checked="" type="checkbox"/>	prereqsed	Prereq	Prereq rule for SED: Checks whether the machine has 64 bit kernel support or not.
<input checked="" type="checkbox"/>	prereqnon tcb	Prereq	Prereq rule for non-TCB: Checks whether the system is non-TCB or not.
<input checked="" type="checkbox"/>	prereqda	Prereq	Prereq rule for disableacct: Adds /bin/false to shells in login.cfg, if it does not exist.
<input checked="" type="checkbox"/>	prereqTE	Prereq	Prereq rule for Trusted Execution: Checks whether the system has Trusted Execution feature on or not.
<input checked="" type="checkbox"/>	pciv3_minage	PCIV3	Implements PCI section 2.1: Always change vendor-supplied defaults before installing a system on the network - eg: include passwords, simple network management protocol(snmp) community strings and elimination of unnecessary accounts.
<input checked="" type="checkbox"/>	pciv3_maxage	PCIV3	Implements PCI Section 8.2.4: Maximum age for password: Specifies the maximum number of weeks (13 weeks at least 90 days) that a password is valid.
<input checked="" type="checkbox"/>	pciv3_maxexpired	PCIV3	Implements PCI section 2.1: Always change vendor-supplied defaults before installing a system on the network - eg: include passwords, simple network management protocol(snmp) community strings and elimination of unnecessary accounts.



Group Editor

IBM PowerSC

Compliance Configuration

Groups

+ ADD NEW GROUP

All Systems 4 Systems

test group 1 System

Test group 2 2 Systems

test group 3 3 Systems

Group Editor Profile Editor Endpoint Admin

All Systems 4 Systems

Save Delete Group Create New Group Add Systems to Group

<input checked="" type="checkbox"/>	System Name	Compliance Rule Type	Applied Timestamp	Check Timestamp
<input checked="" type="checkbox"/>	lbsaix1.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 2:27:24 PM	1/30/201
<input checked="" type="checkbox"/>	lbsaix7.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 2:27:31 PM	1/30/201
<input checked="" type="checkbox"/>	lbspta1.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 2:27:30 PM	1/30/201
<input checked="" type="checkbox"/>	lbstnc1.aus.stglabs.ibm.com	PCiv3_Custom	1/19/2017, 1:37:06 PM	1/30/201



Dashboard

Total Systems 3 0 with RTC Running 1 with TE Running	Compliance Failures 0 in 0 Systems in 0 Groups	Total RTC Events 0 in 0 Files in 0 Systems	Total TE Events 74 in 36 Files in 2 Systems
---	---	---	--

Compliance Info

System Passes and Failures

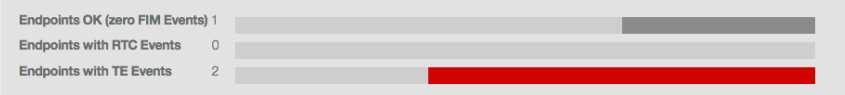


Total Rules Checked 3	Specific Rules Failed 0	No Applied Profile Systems 0	Groups With Rules Failed 0
--	--	---	---

Groups With Compliance Failures

Group Name	Failures
NO SYSTEMS HAVE BEEN ADDED	

Security/File Integrity Monitoring



Groups With FIM Events

Group Name	Events
All Systems	74 in 2 Systems



Techopedia EDR Definition

What Does Endpoint Detection and Response (EDR) Mean?

Endpoint detection and response (EDR) is a specific type of security focusing on endpoint devices. It is often described as the use of a central data repository to observe and analyze endpoint vulnerabilities and work toward stronger endpoint threat response.



EDR Event Types

EDR Subset	AIX	RHEL	SLES	IBM i	HMC
RTC configuration change was requested	✓				
TE configuration change was requested	✓				
Auditd configuration change was requested		✓	✓		
FIM - Content Change	✓	✓	✓	✓	
FIM - Access Change	✓	✓	✓	✓	
FIM - Directory Change	✓	✓	✓	✓	
Allowlisting - Hash Mismatch	✓	✓	✓		
Allowlisting – Meta-data Mismatch		✓	✓		
Compliance Profile Apply	✓	✓	✓	✓	✓
Compliance Profile Undo	✓	✓	✓	✓	✓
Compliance check	✓	✓	✓	✓	✓



EDR Event Types



EDR Subset	AIX	RHEL	SLES	IBM i	HMC
Host Intrusion - Too many password failures	✓	✓	✓		
Host Intrusion - Port scan		✓	✓		
Host Intrusion - Agent Connectivity	✓	✓	✓	✓	✓
Host Intrusion – Malware event	✓	✓	✓	✓	



Host-based EDR Alert Configuration

Configure Alerts

Event Category	Event Type	Urgency	Responses
> Configuration Changed	RTC configuration change was requested	Low	None
> Configuration Changed	TE configuration change was requested	Low	None
> Configuration Changed	AUDITD configuration change was requested	Medium	None
> File Integrity Monitoring	Content Change	High	None
> File Integrity Monitoring	Access Change	Low	Email, Syslog
> File Integrity Monitoring	Directory Change	Low	None
> Allow Listing	Hash Mismatch	High	Email, Syslog
> Allow Listing	Meta-data Mismatch	Low	None
> Compliance	Profile Apply	Low	None

 Save  Cancel



Host-based EDR Event Analysis Tool

IBM PowerSC

Event Analysis for sdaixc2

Urgency Event category Show Timestamp

 FIM Active alerts only From 02 / 14 / 2022 To 02 / 14 / 2022

Filter by text

foo.txt



7 total alerts

<input type="checkbox"/>	Urgency ▾	Event Category ▾	Event Type ▾	Timestamp ▾
>	<input type="checkbox"/> Low	File Integrity Monitoring	Attributes changed on file /tmp/foo.txt	2022-02-14T20:51:02Z
>	<input type="checkbox"/> Low	File Integrity Monitoring	Attributes changed on file /tmp/foo.txt	2022-02-14T20:49:39Z
>	<input type="checkbox"/> Low	File Integrity Monitoring	Attributes changed on file /tmp/foo.txt	2022-02-14T20:38:00Z
>	<input type="checkbox"/> Low	File Integrity Monitoring	Attributes changed on file /tmp/foo.txt	2022-02-14T20:35:18Z
>	<input type="checkbox"/> Low	File Integrity Monitoring	Attributes changed on file /tmp/foo.txt	2022-02-14T20:27:39Z
>	<input type="checkbox"/> Low	File Integrity Monitoring	Attributes changed on file /tmp/foo.txt	2022-02-14T20:23:04Z



AIX Patch Management

PowerSC's Trusted Network Connect and Patch Management

TNC - Cybersecurity Context - CIS 7.1

7.3 Perform Automated Operating System Patch Management

Applications

Protect



Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

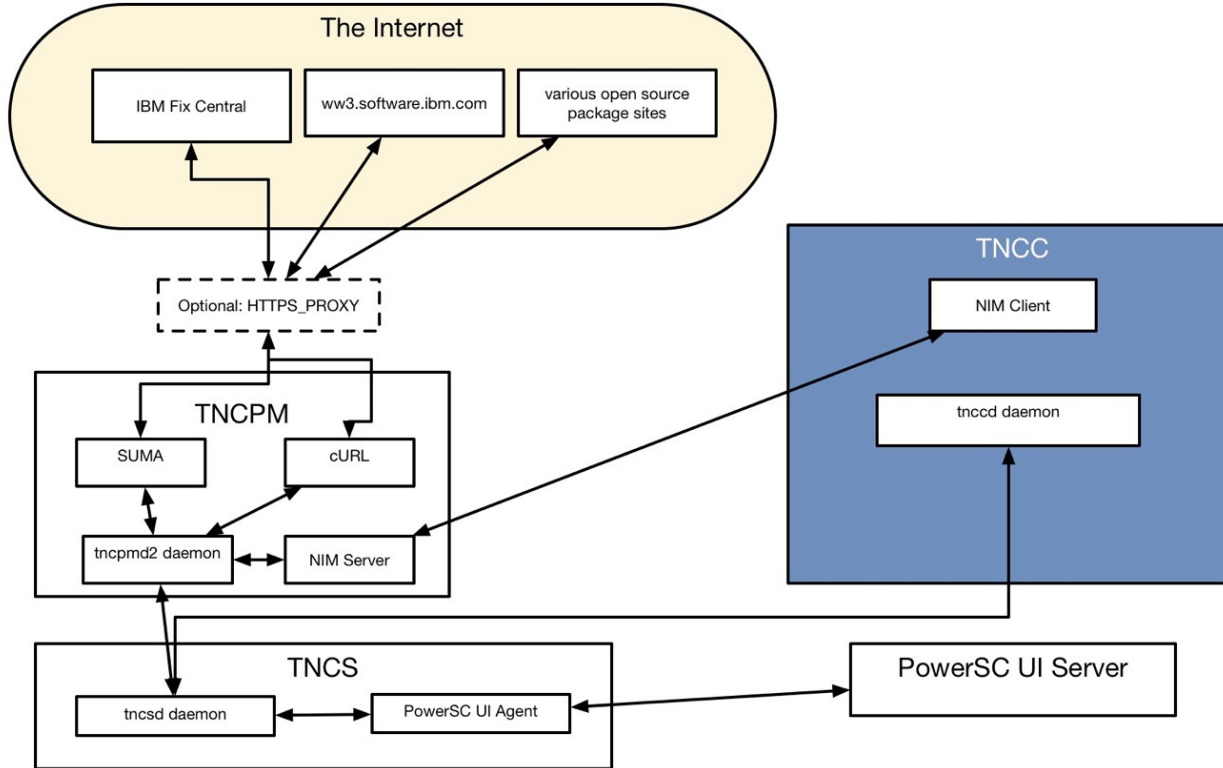


TNC Overview

- One of the most fundamental and important cyber defenses is Vulnerability Management. PowerSC has provided Trusted Network Connect and Patch Management (TNC) as a key solution to use when implementing your Vulnerability Management cyber defenses. TNC is the AIX/VIOS patching component of PowerSC that allows you to automate and reduce the effort needed to properly update AIX and VIOS systems with security ifixes, service packs and technology levels.



PowerSC TNC Topology - 1.2.0.1



Key Features of TNC

- Point and click management support via the PowerSC Graphical User Interface
- Patch Repository is automatically updated with new SPs and ifixes
- TNC provides flexible and granular options for defining patch policy
- Patch recommendations made upon the actual filesets installed on AIX or VIOS endpoints
- Extensive install support, including open-source packages in rpm & installp format
- Light-weight component architecture that provides excellent performance
- Automatic updating of patch repository for ifixes having superseding versions
- Flexible command line functions that facilitate automation
- TNC supports alt_disk updates for ifixes, service packs and technology levels



Multi-Factor Authentication

An essential cyber defense

Cybersecurity Context – CIV v8

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
6.4	Require MFA for Remote Network Access Require MFA for remote network access.	Users	Protect	●	●	●
6.5	Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Users	Protect	●	●	●

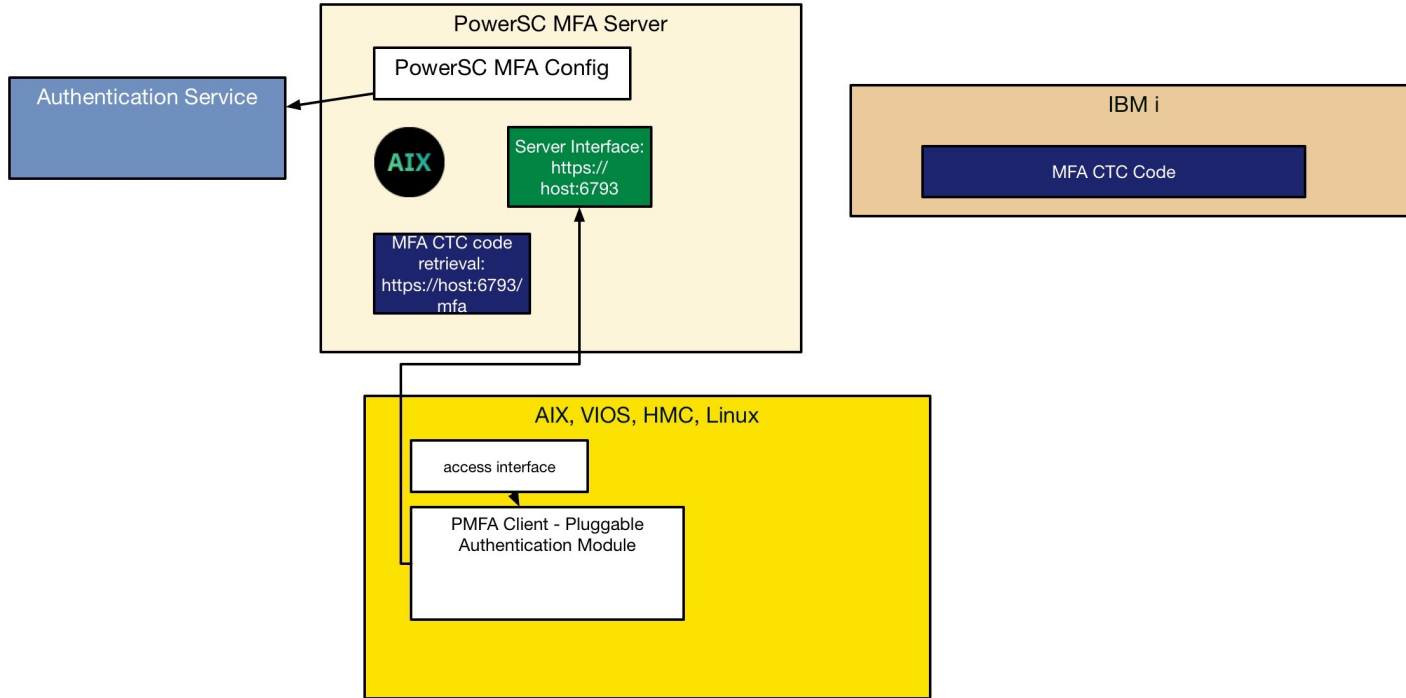


What is Multi-Factor Authentication (MFA)

- There are 3 types of authentication factors:
 - Something you know (password)
 - Something you have (RSA key fob device)
 - Something you are (Retinal scan)
- Traditional AIX/Linux authentication is one factor (something you know). MFA requires 2 or more different factors



PowerSC MFA Topology



Minimum Software Level Requirements

- For the PowerSC MFA server:
 - AIX 7.1 TL 5
 - AIX 7.2 TL 2

- For the following platforms:
 - AIX 6.1.9.8
 - AIX 7.1.4.3
 - AIX 7.2.1.1
 - VIOS 2.2.5.20
 - RHEL 8.x
 - SUSE 15
 - HMC V9.1.920.0
 - Virtual HMC V9.1.940
 - PowerSC GUI Server 1.2.0.2



PowerSC MFA Authentication Methods

- RSA SecureID
- Certificate Authentication
- RADIUS
 - “generic” RADIUS
 - Gemalto SafeNet RADIUS
 - RSA SecurID RADIUS
- Timed One-time Password (TOTP)
 - Generic TOTP
 - IBM TouchToken
- Ubikey
- IBM Security Access Manager



Malware Prevention with PowerSC

Cybersecurity Context - CIS v8

2.5 Allowlist Authorized Software

Applications

Protect



Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

2.6 Allowlist Authorized Libraries

Applications

Protect



Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

2.7 Allowlist Authorized Scripts

Applications

Protect



Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.



Cybersecurity Context - CIS v8

10.1 Deploy and Maintain Anti-Malware Software

Devices

Protect



Deploy and maintain anti-malware software on all enterprise assets.

10.2 Configure Automatic Anti-Malware Signature Updates

Devices

Protect



Configure automatic updates for anti-malware signature files on all enterprise assets.

10.6 Centrally Manage Anti-Malware Software

Devices

Protect



Centrally manage anti-malware software.



Malware Definition

- Malware is a general term for software intended to cause harm, disrupt, or gain unauthorized access to a computer system. Trojans, worms, miners, rootkits, viruses, keyloggers, and ransomware are all examples of different types of malware.



Table 13. Endpoint Actions by Operating System Type (continued)

Action Category	AIX	Linux	IBM i
Blocklisting	<p>Configure Blocklisting See “Configuring the blocklist” on page 70 for more information.</p> <p>Copy Blocklisting Configuration See “Copying the blocklist configuration” on page 70 for more information.</p> <p>Run Blocklist Scan See “Running the blocklist scan” on page 70 for more information.</p>		



Action Category	AIX	Linux	IBM i
Allow List	<p>Configure TE See “Configuring Trusted Execution (TE)” on page 58 for more information.</p> <p>Copy TE Configuration See “Copying Trusted Execution (TE) options to other groups” on page 58 for more information.</p> <p>Edit TE file List See “Editing the Trusted Execution (TE) file list” on page 59 for more information.</p> <p>Copy TE File List See “Copying Trusted Execution (TE) file list monitoring options to other groups” on page 59 for more information.</p> <p>Run TSD Scan See “Running a Trusted Signature Database (TSD) scan” on page 59 for more information.</p> <p>TSD Maintenance See “Running a Trusted Signature Database (TSD) scan” on page 59 for more information.</p>	<p>Configure fapolicyd See “Configuring the allow list” on page 60 for more information.</p> <p>Copy fapolicyd Configuration See “Copying the configuration” on page 62 for more information.</p> <p>Copy fapolicyd File List See “Copying the file list” on page 63 for more information.</p> <p>Edit fapolicyd File List See “Editing the file list” on page 63 for more information.</p>	NA



ClamAV with PowerSC

Traditional endpoint malware countermeasure

Description

- open source (GPLv2) anti-virus toolkit
- ClamAV is provided by Cisco Systems, Inc



Features

- Designed to scan files quickly
- Detects millions of viruses, worms, trojans and other malware
- Signed signature databases ensure that ClamAV will only execute trusted signature definitions
- Scans within archives and compressed files but also protects against archive bombs



System Requirements

- Minimum RAM: 4GB
- Minimum Disk: 6GB



FreshClam Definition

- Signature database (cvd) command line update tool
- freshclam is used to download and update ClamAV's official virus signature databases.



Database Update Options

- Directly from internet
- Indirectly through a https Proxy Server
- Indirectly using a private mirror, local webserver using cvdupdate tool
- Indirectly using a private mirror, local webserver using freshclam



ClamScan Definition

- Command line program to scan files and directories that does not require the clamd daemon.

PowerSC GUI server ClamAV Functionality

- Modify the configuration of ClamAV on endpoints running the PowerSC GUI agent
- Copy the ClamAV configuration of a single endpoint to a group of endpoints
- Issue automated and manual scans by using the PowerSC GUI server
- Configure scheduled scans to search specific directories on an endpoint
- Extensive email reporting options provided by using the PowerSC GUI server
- Perform automated scans and virus database updates by using the PowerSC GUI server's REST API



EDR Email Notifications for Malware

Focused Other

Today

- root@sdpscgui.rchland.ibm.com**
PowerSC UI Server Report 1:05 PM
Compliance Overview for all systems This report is generated at Mon Apr 03 13:00:00 CDT 2...
- root@sdpscgui.rchland.ibm.com**
Malware Win.Test.EICAR_HDB-1 detected on sdaixc2.rchland.ibm.com. - Pow... 12:48 PM
File name: /tmp/1680030847552-foo.ksh Malware: Win.Test.EICAR_HDB-1 --- https://sdpscgui...
- root@sdpscgui.rchland.ibm.com**
Malware file quarantined on sdaixc2.rchland.ibm.com. - PowerSC - sdpscgui.r... 12:48 PM
File name: /tmp/1680030847552-foo.ksh --- https://sdpscgui.rchland.ibm.com/webclient/
- root@sdpscgui.rchland.ibm.com**
Malware scan completed on sdaixc2.rchland.ibm.com. - PowerSC - sdpscgui... 12:48 PM
A completely generic (and thus meaningless) event has been received. --- https://sdpscgui.r...
- root@sdpscgui.rchland.ibm.com**
Malware scan started on sdaixc2.rchland.ibm.com. - PowerSC - sdpscgui.rchl... 12:47 PM
A completely generic (and thus meaningless) event has been received. --- https://sdpscgui.r...

Malware Win.Test.EICAR_HDB-1 detected on sdaixc2.rchland.ibm.com. - PowerSC - sdpscgui.rchland.ibm.com

R **root@sdpscgui.rchland.ibm.com** <root@sdpscgui.rchland.ibm.com>
To: Stephen Dominguez

File name: /tmp/1680030847552-foo.ksh
Malware: Win.Test.EICAR_HDB-1

<https://sdpscgui.rchland.ibm.com/webclient/>



ClamAV Scan

The image shows a 'Details' dialog box for a ClamAV scan. The dialog box is white with a dark border and contains the following information:

- 3/2/2023, 11:54:16 AM**
- File Name:** /tmp/1677696014086-1677693350758-eicar.com
- SECURITY_TABLE.VARIABLES.malware:** Win.Test.EICAR_HDB-1

At the bottom of the dialog box, there are two buttons: 'Cancel' (dark grey) and 'Hide events' (blue).

The background shows a security event log with the following entries:

- 1 SECURITY_TABLE.CATEGORIES.MALWARE_SCAN_STARTED
- 1 SECURITY_TABLE.CATEGORIES.MALWARE_SCAN_COMPLETED
- 1 SECURITY_TABLE.CATEGORIES.MALWARE_DETECTED
- 1 SECURITY_TABLE.CATEGORIES.MALWARE_FILE_QUARANTINED



Closing

<https://ibm.biz/aix-linux-security>

AIX, Linux, and Red Hat OpenShift Security Services

This support page provides a top-down approach for describing the standard AIX, Linux, and Red Hat OpenShift Security Services provided by IBM Technology Expert Labs.

If you would like to make a request for a professional security service not listed on this site, forward your request to your local IBM Technology Expert Labs team.

– Security Assessment Services

- + AIX Security Assessment
- + Linux Security Assessment
- + OpenShift Security Assessment

– PowerSC Implementation Services

- + Security and Compliance with PowerSC
- + [AIX Patch Management with PowerSC](#)
- + ClamAV with PowerSC
- + Multi-Factor Authentication with PowerSC

– Centralized Authentication and Identity Management Services

- + AIX or Linux LDAP Integration with Microsoft Active Directory
- + AIX or Linux LDAP integration with IBM Security Directory Server
- + LDAP Login Control Automation

– AIX Security Implementation Services

- + AIX Malware Prevention
- + Enhanced Role Based Access Control
- + AIX Auditing

All Services [PDF \(1.7MB\)](#)

Contact us at technologyservices@ibm.com or your local IBM Technology Expert Labs team



Additional References

- PowerSC Documentation
<https://www.ibm.com/docs/en/powersc-standard>
- For more PowerSC MFA information:
<https://www.ibm.com/docs/en/powersc-mfa>
- PowerSC Redbook
<http://www.redbooks.ibm.com/abstracts/sg248082.html?Open>
- Center for Internet Security Controls
<https://www.cisecurity.org/controls/cis-controls-list/>



Thank You!

- Feel free to contact me in the future:
Stephen Dominguez
email: sdoming@us.ibm.com
blog: <https://www.securitysteve.net>
- You can find full descriptions of our services at:
<https://ibm.biz/aix-linux-security>



The screenshot displays the 'Security Steve' website, which is Stephen Dominguez's Power Security Blog for AIX & Linux. The page features a navigation menu with links to Home, Questions?, Coming to AIX Security, Steve's AIX Top Ten, About Security Steve, Posts, and Comments. Below the navigation, there are sections for 'Steve's AIX Top Ten' and 'Follow me on Twitter'. The 'Steve's AIX Top Ten' section includes the title 'Security Steve's Top Ten AIX Security Tools' and a detailed introduction. It lists 10 security tools for evaluation, such as AIX Role Based Access Control (RBAC), AIX Trusted Execution (TE), and PowerSC Security and Compliance Automation. A tweet from @SecuritySteve is also visible, mentioning a data breach at Forever 21.

Security Steve
Stephen Dominguez's Power Security Blog for AIX & Linux

HOME QUESTIONS? COMING TO AIX SECURITY STEVE'S AIX TOP TEN ABOUT SECURITY STEVE POSTS COMMENTS

LINKS CONSULTING SERVICES THE SECURITY STEVE NEWSLETTER LINUX LINKS SECURITY TERMS

Steve's AIX Top Ten

Security Steve's Top Ten AIX Security Tools

In no particular order, the following is my general recommendation for the 10 most important security tools that you should be using in your AIX environment. Each tool provides important and unique capabilities that are essential to achieving a Defense in Depth security strategy for your AIX environment. Teri Radichel states in her case study of the Target's 2013 Data Breach, "Case Study: Critical Controls that Could Have Prevented Target Breach", the following:

"Businesses should not rely on a single security tool or process to prevent data loss or harm to the business. Layers of defenses including preventative and detective measures should be employed. Due to the complex nature of security and the persistence of the adversary, detection is crucial. A detailed understanding of networks, hardware, software and processes is required to create a comprehensive plan. Using the Critical Controls (the 20 Center for Internet Security Critical Controls) to implement layers of security helps thwart attacks by guarding against the many different ways attackers gain access to systems."

These are the 10 most important AIX security tools that should be evaluated for use by all organizations using AIX:

1. AIX Role Based Access Control (RBAC)
2. AIX Trusted Execution (TE)
3. PowerSC Security and Compliance Automation
4. PowerSC Real Time Compliance (RTC)
5. PowerSC Graphical User Interface
6. File Permission Manager – (FPM)
7. LDAP Services using IBM Tivoli Directory Server with Pass-through Authentication
8. Multi-factor Authentication at the Network
9. AIX Auditing
10. AIX Stack Execution Disable (SED)

The Most Important Tool?

You may ask, "What's the most important tool?". Well to be perfectly honest, the most important "tool" isn't even on my

Follow me on Twitter

Tweets by @SecuritySteve

Security Steve
@SecuritySteve

Forever 21 now breached:

RETAIL CHAIN FOREVER 21 WARNS OF DATA BREACH

By Alissa M. Stauden

Embed View on Twitter

