

IBM Power Systems Cloud Security Guide

Protect IT Infrastructure In All Layers

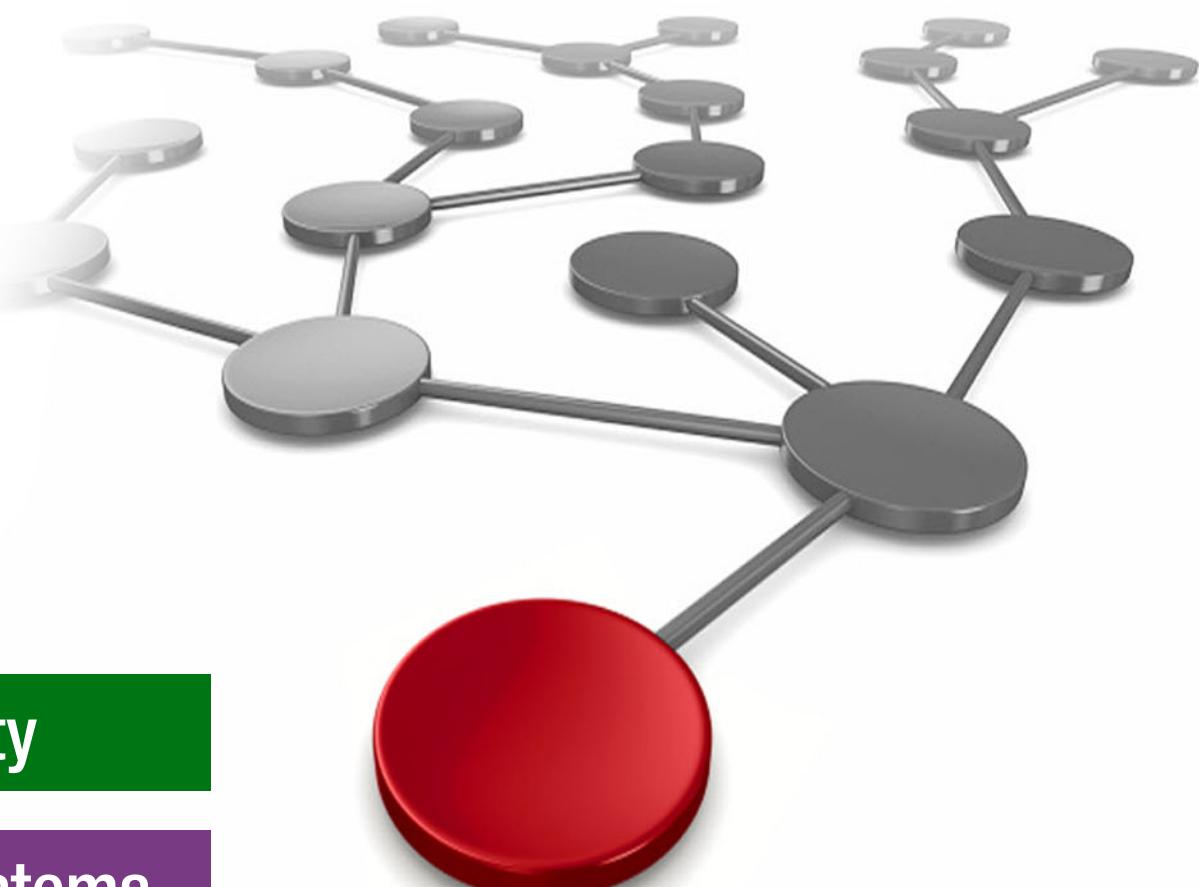
Dino Quintero

Faraz Ahmad

Behzad Koohi

Youssef Largou

Antony Steel



 **Security**

Power Systems

IBM
®

Redpaper



IBM Redbooks

IBM Power Systems Cloud Security Guide: Protect IT Infrastructure In All Layers

April 2022

Note: Before using this information and the product it supports, read the information in “Notices” on page ix.

First Edition (April 2022)

This edition applies to:

IBM PowerVC 2.0.1.

IBM PowerVM 3.1.3.

IBM PowerSC 2.0.

IBM AIX 7.2 Technology Level 5.

IBM i 7.4 Technology Refresh 5.

Red Hat Enterprise Linux release 8.4 for IBM POWER (little endian).

Red Hat Enterprise Linux 8.4.

Red Hat Enterprise Linux release 8.2 for IBM POWER (little endian).

IBM QRadar 7.3.3 FixPak 9.

IBM QRadar Community Edition 7.3.3.

IBM Security Guardium Key Lifecycle Manager 4.1.1.

IBM Guardium Data Encryption 3.0.

IBM Spectrum Protect 8.1.

Red Hat Ansible 2.9.

OpenSCAP Scanner 1.3.4.

This document was created or updated on April 14, 2022.

© Copyright International Business Machines Corporation 2022. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	ix
Trademarks	x
Preface	xi
Authors	xi
Now you can become a published author, too!	xii
Comments welcome	xiii
Stay connected to IBM Redbooks	xiii
Chapter 1. IBM Power Systems and IBM Power Systems Virtual Server security considerations	1
1.1 Introduction to security architecture	2
1.1.1 Aligning your security strategy	2
1.1.2 Protecting your assets	3
1.1.3 Managing your detection and response	5
1.2 Security considerations for cloud services and deployment models	9
1.2.1 Cloud services and security	9
1.2.2 Cloud deployment models and security considerations	12
1.3 IBM Power Systems security architecture	13
1.3.1 Hardware, firmware, and hypervisor	14
1.3.2 Operating system	15
1.3.3 Workloads, VMs, and containers	15
1.3.4 IBM PowerSC	16
1.3.5 IBM PowerSC Multi-factor Authentication	17
1.3.6 IBM Power10, protecting trust from core to the cloud	17
1.4 Paradigm shift for protecting IBM Power Systems	20
1.4.1 Zero Trust journey	21
1.4.2 Traditional threats	21
1.4.3 Threats to cloud and virtualized environments	22
1.4.4 Security between different LPARs	23
1.4.5 Protecting sensitive applications and data in containerized workloads	24
1.4.6 IBM Power Systems Virtual Server and General Data Protection Regulation ..	25
1.4.7 Emerging threats	25
1.5 Overview of cybersecurity landscape and threats for organizations	27
1.5.1 Top attack trends	27
1.5.2 X-Force recommendations for resilience	29
Chapter 2. IBM Power Systems and IBM Power Systems Virtual Server integrated security capabilities	31
2.1 PowerVM keystore	32
2.1.1 Platform KeyStore features	32
2.1.2 Configuring the Platform KeyStore	33
2.1.3 Platform KeyStore Storage Protection	34
2.1.4 Disaster recovery	35
2.1.5 Migrating a partition that uses the Platform KeyStore	35
2.2 IBM AIX security	37
2.2.1 Trusted Computing Base	37
2.2.2 AIX Secure Boot	37
2.2.3 AIX Trusted Execution	38

2.2.4 AIX Security Expert	39
2.2.5 Role-based access control	40
2.2.6 Encrypted file system	41
2.2.7 OpenSSH and Kerberos 5 support	41
2.2.8 Private boot with Network Installation Manager	42
2.2.9 Login control	42
2.2.10 Stack execution disable protection	42
2.2.11 Managing X11 and CDE concerns	43
2.2.12 List of setuid and setgid programs	43
2.2.13 AIX trusted installation and update	44
2.2.14 Network security	44
2.2.15 Network security for IBM Power Systems Virtual Server	45
2.2.16 Backing up and restoring encryption	45
2.3 IBM i security	47
2.3.1 Introduction to IBM i Security	47
2.3.2 IBM i security assessments	50
2.4 Linux security	51
2.4.1 Security best practices for Linux	51
2.4.2 OpenSSL enhancements	54
2.4.3 Blocking and allowing applications by using fapolicyd	54
2.4.4 Operating system boot security improvements	56
2.4.5 Cybersecurity profiles available with PowerSC GUI	56
2.4.6 SUSE Linux Enterprise Server Security Hardening Guide for the SAP HANA Platform	57
2.4.7 Red Hat Enterprise Linux Security Hardening Guide	57
2.5 NIST Security Content Automation Protocol SCAP	60
2.6 Linux Integrity Measurement Architecture	65
2.7 Compressed and encrypted Live Partition Mobility data	67
Chapter 3. IBM Power Systems and IBM Power Systems Virtual Server advanced security capabilities	69
3.1 IBM PowerSC and IBM PowerSC MFA	70
3.1.1 IBM PowerSC	70
3.1.2 IBM PowerSC Multi-Factor Authentication	70
3.2 Security and compliance for Red Hat OpenShift on IBM Power Systems and IBM Power Systems Virtual Server	71
3.2.1 Overview	71
3.2.2 Efficient cloud infrastructure scaling	72
3.2.3 Proven security and reliability	73
3.2.4 Red Hat OpenShift on IBM Power Systems Virtual Server	73
3.2.5 Containers security	73
3.3 Data in transit and at rest protection with IBM Security Guardium	76
3.3.1 IBM Security Guardium	76
3.3.2 IBM Security Guardium Data Encryption	77
3.3.3 IBM Security Guardium Key Lifecycle Manager	81
3.4 Detecting advanced threats, proving compliance, and securing cloud with IBM QRadar	90
3.4.1 Detecting advanced threats, proving compliance, and securing cloud with IBM QRadar	90
3.5 Modernizing security with IBM Cloud Pak for Security	108
Chapter 4. IBM Power Systems advanced security implementation scenarios	109
4.1 PowerSC for AIX	110
4.1.1 Prerequisites	110

4.1.2	Installing PowerSC on AIX systems	110
4.1.3	Installing PowerSC GUI AIX agent and server	111
4.1.4	Distributing the truststore security certificate to endpoints	112
4.1.5	Compliance checking	113
4.2	Security and compliance tools for IBM i	114
4.3	PowerSC for IBM i	123
4.3.1	PowerSC 2.0 supported features for IBM i	123
4.3.2	PowerSC for IBM i Agent prerequisites	123
4.3.3	PowerSC for installing IBM i Agent	123
4.3.4	Using the PowerSC GUI	124
4.3.5	Administering compliance levels and profiles	124
4.4	PowerSC for Linux	125
4.4.1	Prerequisites	125
4.4.2	Configuring Intrusion Detection Service on Red Hat Enterprise Linux	125
4.4.3	Distributing the truststore	126
4.4.4	Troubleshooting	126
4.5	Allowing and denying list management	127
4.5.1	On AIX (Trusted Execution)	127
4.5.2	Trusted Execution policies	131
4.5.3	Trusted execution logging on AIX (syslog and AIX auditing)	132
4.5.4	Allowing and denying list management on Linux (fapolicyd)	135
4.6	PowerSC MFA example configuration	137
4.6.1	Configuring the MFA Server	137
4.6.2	Configuring the timed-based one-time password authentication	142
4.6.3	Troubleshooting	148
4.6.4	Configuring AIX SSH client for MFA	148
4.6.5	Configuring Linux SSH Client for MFA	154
4.7	PowerSC MFA 2.0 high availability	155
4.7.1	Configuring the servers	156
4.7.2	Changing the PowerSC MFA clients	159
4.7.3	Switching the active IBM PowerSC MFA server	160
4.7.4	Administrative tasks	161
4.8	PowerSC MFA out-of-band authentication	162
4.9	PowerVC security services	162
4.9.1	Managing users, groups, and projects	162
4.9.2	Security management planning	166
4.9.3	Ports that are used by IBM PowerVC	166
4.9.4	Providing a certificate	166
Appendix A.	Use case for security compliance on IBM Power Systems through Red Hat Ansible	169
IBM Power Systems and the Red Hat Ansible Automation Platform	170	
Solution benefits	170	
Security and compliance with Red Hat Ansible for IBM AIX and Red Hat on Power Systems	171	
Basic Red Hat Ansible concepts	171	
Installing Red Hat Ansible Engine and AIX collection	172	
Running security and compliance playbook on Red Hat on IBM Power by using Red Hat Ansible and OpenSCAP	175	
Running security and compliance playbook on AIX using Red Hat Ansible and AIXpert	177	
Security and compliance with Red Hat Ansible for IBM i	179	
Overview	179	
Running a playbook for Secure Compliance for IBM i	180	

Related publications	213
IBM Redbooks	213
Other publications	213
Online resources	214
Help from IBM	214

Notices

This information was developed for products and services offered in the US. This material might 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, MD-NC119, Armonk, NY 10504-1785, US

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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

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 actual people or business enterprises 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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, 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 <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®	IBM Spectrum®	PowerVM®
Cognos®	IBM Z®	QRadar®
DB2®	Passport Advantage®	Redbooks®
Guardium®	PIN®	Redbooks (logo)  ®
IBM®	POWER®	Satellite™
IBM Cloud®	Power10™	Think®
IBM Cloud Pak®	POWER8®	WebSphere®
IBM Research®	POWER9™	X-Force®
IBM Security™	PowerHA®	

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Windows, and the Windows logo are trademarks of Microsoft Corporation 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.

Ansible, OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redpaper publication provides a security and compliance solution that is optimized for on-premises and cloud-virtualized environments on IBM Power Systems servers, running IBM AIX®, IBM i and Linux. Security control and compliance are some of the key components that are needed to defend the virtualized data center and cloud infrastructure against ever evolving threats.

The IBM business-driven approach to enterprise security that is used with solutions, such as IBM PowerSC, makes IBM a premier security vendor in the market today.

In this book, we explore, test, and document scenarios for managing security and compliance. These scenarios use IBM Power Systems architecture and software security solutions from IBM to help defend on-premises virtualized data center and cloud infrastructure against ever evolving threats.

This publication helps IT and Security managers, architects, and consultants to strengthen their security and compliance posture for an IT infrastructure in all layers.

Authors

This paper was produced by a team of specialists from around the world working at IBM Redbooks, Poughkeepsie Center.

Dino Quintero is a Systems Technology Architect with IBM Redbooks®. He has 28 years of experience with IBM Power Systems technologies and solutions. Dino shares his technical computing passion and expertise by leading teams in developing technical content in the areas of enterprise continuous availability, enterprise systems management, high-performance computing (HPC), cloud computing, artificial intelligence (including machine and deep learning), and cognitive solutions. He also is a Certified Open Group Distinguished IT Specialist. Dino holds a Master of Computing Information Systems degree and a Bachelor of Science degree in Computer Science from Marist College.

Faraz Ahmad is a an IBM Power Systems solution architect working in IBM Lab Services, India. Faraz has over 16 years of experience in various areas of IT, including software development, solution designing, and IT consulting. He specializes in cybersecurity and in his current role, he designs security solutions for IBM customers. He is also a geography lead and mentors security consultants in the Central and Eastern Europe, Middle East, and Africa regions. His other areas of expertise includes IBM PowerHA®, AIX, Linux, Networking, and virtualization. He is the author of multiple patents and recognized as an Invention Plateau holder. He has a degree in Computer Science from Birla Institute of Technology, Ranchi, India.

Behzad Koohi is an IT Architect working in IBM Canada. He is responsible for Power and Storage infrastructure design and professional services that are required for solution implementation for Ontario and has been Advisory IT Specialist. He has 27 years experience in the IBM POWER®, Storage, SAN, and backup fields. He holds a Bachelor degree in Computer Science from York University Toronto, Canada.

Youssef Largou is the founding director at PowerM, a platinum IBM Business Partner in Morocco. He has 20 years of experience in Systems, HPC, middleware, and hybrid cloud, including IBM Power Systems, IBM Storage, IBM Spectrum, IBM WebSphere®, IBM DB2®, IBM Cognos®, Portal, IBM MQ, ESB, Cloud Paks, and Red Hat OpenShift. He has been working within numerous industries with a wide range of technologies. Youssef is also an IBM Champion 2020, 2021, and 2022 and has designed many reference architectures. He was awarded five times as an IBM Beacon Award Finalist in Storage, Software Defined Storage, and LinuxONE. He holds an engineer degree in Computer Science from the Ecole Nationale Supérieure des Mines de Rabat and Excecutif MBA from EMLyon.

Antony Steel is the founding director and the Chief Technology Officer at Belisama. A research chemist by training, Antony brings a unique experience and perspective with over 30 years of experience in the IT industry. Before devoting himself full time to Belisama, Antony was involved as a user, administrator, developer, and key technical adviser with an IBM Business Partner and then almost 20 years in IBM in various roles with the most recent being a Senior Managing Consultant/Advanced Technical Support. Antony's clients include users, senior management, and other key stakeholders in a range of industries, including some of the largest financial and business institutions and government departments in Australia, New Zealand, and the Asia Pacific region. He holds an honors degree in Theoretical Chemistry from the University of Sydney.

Thanks to the following people for their contributions to this project:

Wade Wallace
IBM Redbooks, Poughkeepsie Center

Marcelo Avalos del Carpio
Kyndryl

Hrithik Govardhan
Lead Software Developer
Rocket Software

Tim Hill
VP Software Engineering
Rocket Software

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:
ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:
ibm.com/redbooks
- ▶ Send your comments in an email to:
redbooks@us.ibm.com
- ▶ Mail your comments to:
IBM Corporation, IBM Redbooks
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- ▶ Find us on LinkedIn:
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>



IBM Power Systems and IBM Power Systems Virtual Server security considerations

Reducing the risk of a cyberattack is one of the most difficult tasks in the computer industry. By overcoming computer security, cyberthieves are continually discovering new strategies and attacking businesses.

Using a “defense in depth” or multi-layered strategy to cybersecurity risk reduction is critical. Security for the hardware, operating system, firmware, hypervisor, and security tooling, such as IBM PowerSC, is provided by IBM Power Systems and the POWER9™ and POWER10 processors. Business must adopt a zero trust approach to wrap security around every user, device, and connection every time and to unify and integrate all security tools to protect their most valuable assets and proactively manage threats.

This chapter includes the following topics:

- ▶ 1.1, “Introduction to security architecture” on page 2
- ▶ 1.2, “Security considerations for cloud services and deployment models” on page 9
- ▶ 1.3, “IBM Power Systems security architecture” on page 13
- ▶ 1.4, “Paradigm shift for protecting IBM Power Systems” on page 20
- ▶ 1.5, “Overview of cybersecurity landscape and threats for organizations” on page 27

1.1 Introduction to security architecture¹

Before you review this architecture, inventory all cloud use in your organization. Be sure to include the service and deployment models that are used and the components within each cloud. Have a good understanding of where applications and data are located and how they support their business areas. Also, be sure to include an understanding of your on-premises environment and the points where your on-premises systems must interact with your cloud environment.

1.1.1 Aligning your security strategy

Businesses must take risks to harvest market opportunities and generate profit. Do you know what your cyberrisk is? The most recent IBM Security™ X-Force® Intelligence report included the following facts:

- ▶ Ransomware is now the most prevalent form of attack, comprising 23% of all incidents.
- ▶ The Sodinokibi (also known as REvil) ransomware actors alone scammed an estimated US\$123M from a single ransomware campaign.
- ▶ Over 100 executives were targeted in customized phishing campaigns.

The FBI reported a record number (over 790,000) of cybercomplaints that caused a total of more than US\$4.2B in damages². You must know where your industry ranks in terms of most targeted industries and how vulnerable your cloud investment makes you to cyberattacks. Be aware of your cost when threat actors turn their attention to you (see Figure 1-1).

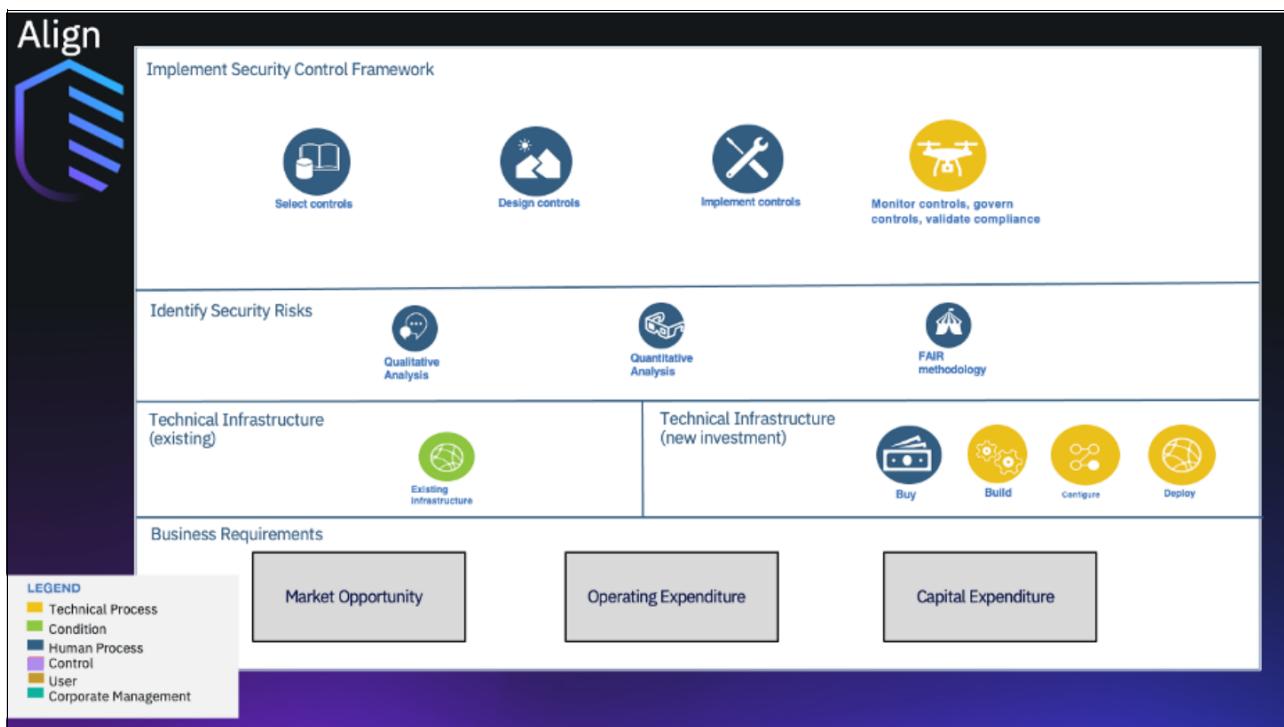


Figure 1-1 Aligning security strategy

¹ Security architecture for cloud applications:
<https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/referenc e-architecture>

² Amer Owaida. "FBI: Cybercrime losses topped US\$4.2 billion in 2020", We Live Security (ESET), March 18, 2021:
<https://www.welivesecurity.com/2021/03/18/fbi-cybercrime-losses-topped-us42billion-2020/>

The best way to be prepared is to perform a cyberrisk assessment. Organizations with a risk management capability might want to assess themselves; others might opt to use industry experts to perform the risk assessment for them.

For more information, see this [IBM Security web page](#).

The results of a risk assessment include a recommended set of controls to mitigate the identified risk and at the same time optimize your investments in security technology. A cloud security architect defines how to govern controls to ensure their effectiveness. Finally, your organization must have a roadmap and implementation plan for the controls.

1.1.2 Protecting your assets

All organizations must harden their environments in anticipation of an attack. This process typically involves locking down access; increasing behavior monitoring for users, endpoints, and servers; and protecting important business assets, such as data and applications.

Hardening your environment is even more critical for cloud environments. Cloud computing risks include broad network access to cloud platforms, on-demand self-service, and a loss of control and visibility. Because of these risks, cloud security can be more difficult than for on-premises (see Figure 1-2).

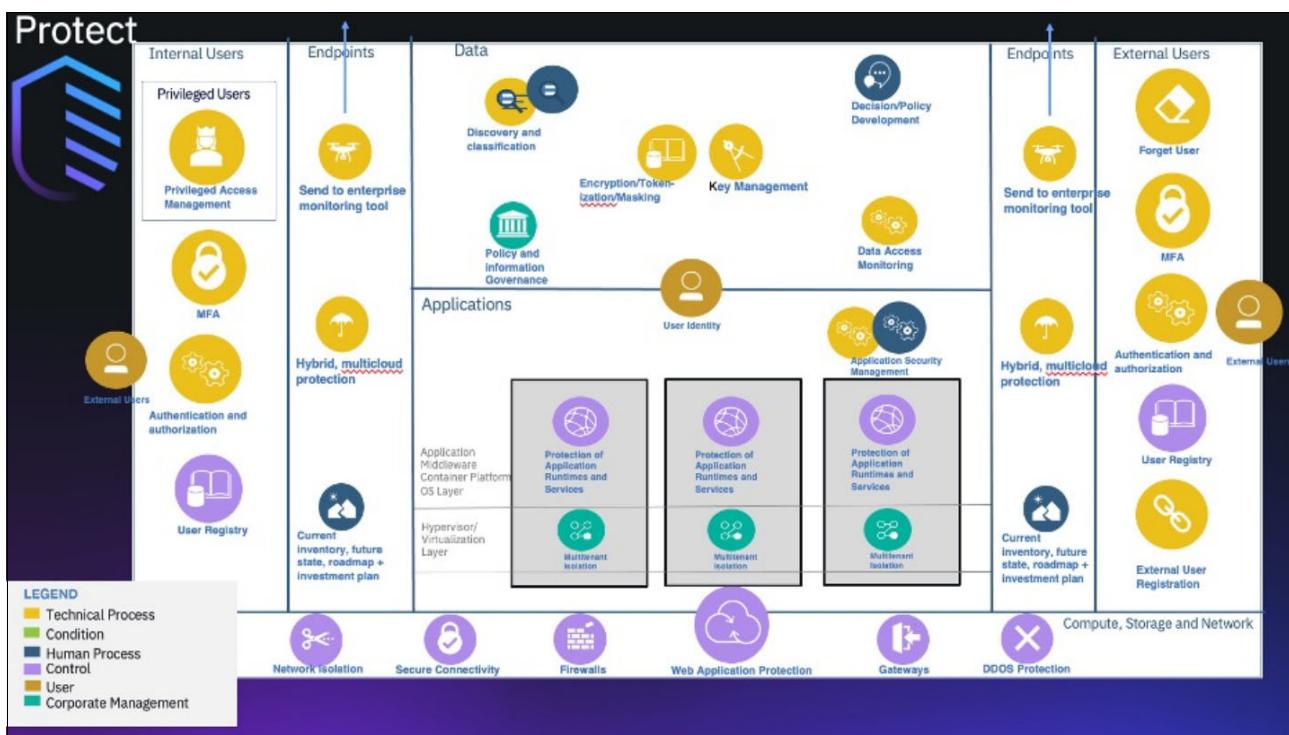


Figure 1-2 Protecting assets

To approach this challenge, understand what needs protection and apply a set of controls that permits least-privileged access. A zero trust architecture (ZTA) uses the zero trust (ZT) concepts, which are designed to reduce the uncertainty in making access decisions in IT infrastructures. ZT was developed to provide greater security in diverse and distributed environments.

Data

Imagine receiving the following email when you get to work:

All of your data is backed up. You must pay 0.015 BTC to [REDACTED] in 48 hours for recover it. After 48 hours, we will leak and expose all your data. In case of refusal to pay, we will contact the General Data Protection Regulation, GDPR, and notify them that you store user data in an open form and is not safe. Under the rules of the law, you face a heavy fine or arrest and your base dump will be dropped from our server.

That is what happened to over 22,000 organizations who had exposed MongoDB databases on their cloud platforms. According to a July 2020 article by Alina Bizga, Hot for Security (Bitdefender³), nearly 47% of all existing MongoDB NoSQL databases are accessible online.

You must think carefully about protecting your data when moving to cloud. Consider the following questions:

- ▶ What data do you have and where is it?
- ▶ What level of protection meets compliance and privacy requirements for the data that you control?
- ▶ Who else shares the responsibility for control of the data?

After you know what data you have and where it is stored, you can establish policies for protecting data and implementing governance to ensure that they remain effective.

Users

Your users are actively targeted by internet bots. In August 2020, Cyware published an article about the TeamTNT botnet stealing the credentials of AWS accounts⁴. Apparently, TeamTNT was actively working to “improve” their malware, including what was the first known botnet to scan and steal AWS credentials.

Consider the following questions to protect your cloud users:

- ▶ What kinds of users do you have (customers, employees, developers, users, executives, suppliers, or privileged users)?
- ▶ What is the least privilege that is needed for each role?
- ▶ How can you create policies that allow the least privilege you define?

Design an architecture with suitable access controls. Look to see which of your tools can extend to cloud. Analyze the gaps to design the remaining controls that are needed to provide protection for your users.

By using cloud, you might have more external customers than before who might have more requirements, such as the ability to sign up for an account and the right to be forgotten.

³ Alina Bizga. "Bad Actors Target MongoDB Databases, Threatening to Contact GDPR Legislators Unless Ransom is Paid", Hot for Security (Bitdefender), July 3, 2020:

<https://securityboulevard.com/2020/07/bad-actors-target-mongodb-databases-threatening-to-contact-gdp-r-legislators-unless-ransom-is-paid/>

⁴ "TeamTNT Botnet Steals AWS Credentials From Compromised Servers", Cyware, August 20, 2020:

<https://cyware.com/news/teamtnt-botnet-steals-aws-credentials-from-compromised-servers-e7a2d2d9>

Applications

For more information about malicious application examples, see the following web pages:

- ▶ [Malicious npm package opens backdoors on programmers' computers](#)
- ▶ [Mercedes-Benz onboard logic unit \(OLU\) source code leaks online](#)
- ▶ [MAGMI Magento plug-in flaw allows remote code execution on a vulnerable site](#)

These reports are from some of the 2020 headlines in cybersecurity news that show typical application security issues. They discuss vulnerabilities in shared and open source code, the failure to protect code registries, and cross-site request forgeries.

To avoid these kinds of application security flaws, use a DevSecOps process. DevSecOps is a combination of tools, processes, and culture. For example, some of the tools might include code scanners, private registries, and CI/CD pipelines. Some of the processes include feedback loops from vulnerability scans back to development for fixes.

To make the most effective use of the DevSecOps tools and processes, your organization must also embrace the culture of DevSecOps. Changing culture and processes can be challenging. Organizations that want to adopt or improve their processes and training can use IBM services to help you adopt DevSecOps.

Infrastructure and endpoints

Protecting infrastructure and endpoints requires patching vulnerabilities and keeping up with the latest software releases for your tools, operating systems, and devices. A good vulnerability management program is essential.

Assess your current state of patching that is within your responsibility and request due diligence statements from your providers for their areas of responsibility. Determine the future maturity that you want from your team and vendors. Build an actionable roadmap and investment plan to get there.

Ensure that monitoring and response from your security operations team includes the components within your current and future states.

Network

In June of 2020, Akamai detected and mitigated the largest ever recorded distributed denial-of-service (DDoS) attack on the Akamai platform. The attackers spewed 809,000,000 packets per second at a major European bank.⁵

The scale of this DDoS attack emphasizes the importance of network security. Network security remains a critical security control, even in the cloud. It can be particularly challenging without clearly defined network perimeters. When thinking about your cloud network security architecture, carefully consider the following aspects:

- ▶ Network isolation
- ▶ Secure customer connectivity
- ▶ Firewalls
- ▶ DDoS protection

⁵ <https://www.akamai.com/blog/news/largest-ever-recorded-packet-per-second-based-ddos-attack-mitigated-by-akamai>

1.1.3 Managing your detection and response

The shared responsibility model plays a critical role in defining your cloud incident management and response strategy. Many incidents are multi-stage attacks that involve lateral movement through an organization's infrastructure. Security incidents might cross from on-premises to cloud and then, across multiple clouds.

Enterprise cloud services are not immune to phishing and spam schemes. Investigation and response to these types of incidents can require coordination between multiple cloud vendors and their customers.

The key is to ensure that the correct architecture is in place to support visibility, detection, investigation, and response across the shared-responsibility model (see Figure 1-3).



Figure 1-3 Managing detection and response

Visibility

Visibility depends on the information that the provider can make available to the customer, which in turn often depends on the service model and platform that are used. Because most cloud-based activity, such as provisioning storage or creating users, uses API calls, it is critical to capture logs of those calls.

Other activity logs, such as logins, are also important. Network flow information is increasingly recognized as critical data for security operations; therefore, many cloud providers make this data available to customers.

The client's cloud security architecture must use a tool to capture the activity that is made available, stage the data for processing, and interpret meaning of the events.

Detection

Detection depends on the following capabilities:

- ▶ Capture activity and interpret what it means,
- ▶ Recognize the new threat vectors that were introduced by cloud and how to use the captured data to detect them.

Another important information source is a threat intelligence feed that helps organizations to know what the latest threats look like and what it takes to detect them. It can also be useful to have stateful information, such as current configuration information, about the cloud assets being monitored.

Finally, it is imperative that the detection systems have the algorithms that are needed to recognize the new cloud-based threat vectors.

Investigation

Tooling for investigation must support the security operations center workflow processes.

Typical workflows include the following components:

- ▶ An alert that something was detected.
- ▶ Presenting the captured data in a form that provides the best information possible about the incident.
- ▶ The use of AI-based research tools to uncover threat actors, methods, and indicators of compromise that is related to the incident.

Response

The critical components for response are a playbook and an orchestration tool that bring together the technical information about the incident with the people who must complete the steps. Knowing what to do and automating the process are the most important factors in shortening response time.

Responses include not only the technical work that is needed to stop the attack and determine the extent of the damage, but also nontechnical tasks, such as handling public relations, informing affected individuals, and knowing the precise effect on privacy and regulatory compliance.

Modernize your security program

IBM Cloud® Pak for Security (see Figure 1-4) enables you to use the rapid, agile capabilities that come from running cloud-native tools. It more quickly integrates security tools and generates deeper insights into threats across hybrid, multi-cloud environments.

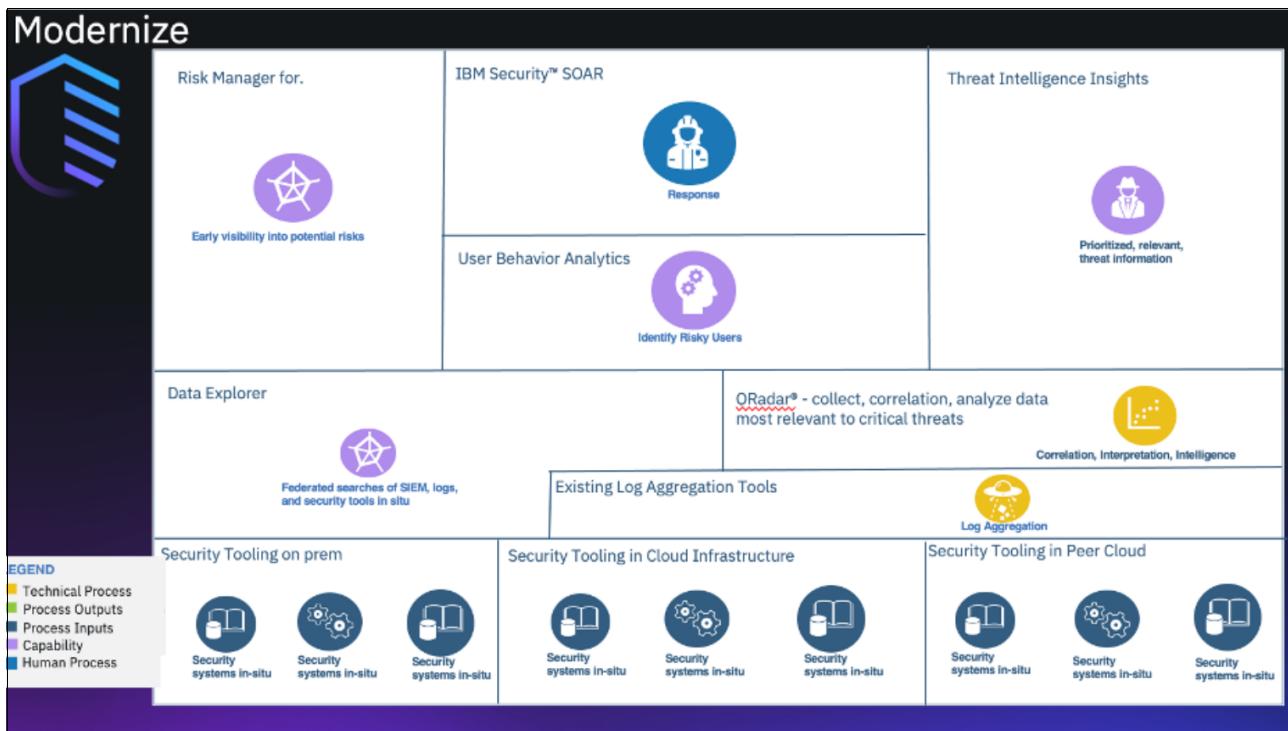


Figure 1-4 Modernizing security program

Most importantly, it uses an infrastructure-independent, common operating environment that runs anywhere. You can quickly search for threats, orchestrate actions, and automate responses without moving your data.

You can compose your security platform by subscribing to services that include the capabilities that you need. This ability allows you to scale up during busy periods and scale down to a more economic platform during slower periods.

IBM Cloud Pak® for Security provides the following tools:

- Data Explorer enables federated search for investigation without moving data.
- Threat Intelligence Insights delivers prioritized, relevant threat information and enables you to scan for threats in your environment.
- IBM Security SOAR delivers security orchestration, automation, and response.
- IBM QRadar® collects, analyzes, and correlates data from many sources to detect and prioritize the most critical threats that require investigation.
- User Behavior Analytics quickly identifies risky users that are associated across three vectors (compromised or stolen credentials, careless or malicious insiders, and malware takeover of user accounts or devices).
- Risk Manager provides early visibility into potential security risks by correlating insights across risk domains.

1.2 Security considerations for cloud services and deployment models

In cloud computing, the cloud service provider owns, implements, manages, and maintains the resources. Then, the customer uses those resources by way of a mobile application, API, or a web browser, and pays for them on a pay-as-you-go basis.

One of the rising cloud-computing adoption challenges is increased security vulnerabilities. The remote use of cloud resources requires an expansion of your trust boundaries to incorporate an external cloud.

1.2.1 Cloud services and security

Unless your cloud provider implements the same or compatible security technologies and frameworks you use, it can be difficult to establish a security architecture that spans the trust boundary without introducing vulnerabilities (see Table 1-5).

Table 1-1 Top security challenges of cloud computing services

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Serverless computing	Software as a Service (SaaS)
Unencrypted data	Data security requirements	Security visibility	Shadow services and compromised accounts
Configuration mistakes	Threat modeling	Number of protocols and attack points	Identity and Access Management
Shadow services	Inherited software vulnerabilities	Number of permissions to manage	Encrypt cloud data
User role-based permissions	Role-based access controls	View of the entire serverless system	Provider security

Figure 1-5 shows the administrative responsibilities that are shared between the cloud consumer and the cloud provider.

	Traditional IT	IaaS	PaaS	Serverless	SaaS
Applications					
Data					
Runtime					
Middleware					
Operating system					
Virtualization					
Servers					
Storage					
Networking					
			Cloud consumer	Cloud provider	

Figure 1-5 Administrative responsibilities between cloud consumer and cloud provider

Infrastructure as a Service security

IaaS provides foundational computing resources (physical or virtual servers, operating system, storage, and networking infrastructure) that you use over an internet connection on a pay-as-you-use basis. IaaS allows you to rent physical IT infrastructure for building your own remote data center on the cloud, rather than building the infrastructure on-premises.

With the IaaS delivery model, the cloud provider often has full administrative control over the hardware, network, storage, and virtualization platforms.

The cloud consumer often has a full or partial administrative control over virtual machine (VM)/logical partition (LPAR), databases, runtimes, and security settings.

As an IaaS customer, you are in charge of securing everything from applications, data, user access, operating systems, and virtual network.

The following challenges rise significantly when IaaS is used:

- ▶ Unencrypted data

In public, hybrid, and multi-cloud environments, data moves between on-premises and cloud-based resources, and between different cloud applications. Encryption is important to protect the data from unauthorized access.

You can encrypt data on-premises, before it goes to the cloud, or in the cloud. You can use your own encryption keys or IaaS-provider encryption. Your IT department might also want to encrypt data in transit.

- ▶ Configuration mistakes

A typical cause of cloud security incidents is misconfiguration of cloud resources (mis-configured inbound or outbound ports, complex authentication that is not activated, and data and applications encryption turned off).

- ▶ Shadow services

After you provision an application or cloud resource, you can use a cloud provider without informing your IT department. To secure data and application in these services, IT first identifies the services and users through an audit.

- ▶ User role-based permissions

It is a best practice to safeguard access to cloud infrastructure by ensuring that users have only the correct permissions they need to accomplish their tasks.

Platform as a Service security

PaaS provides a comprehensive cloud-based platform for developing, running, and managing applications without the challenges of cost, complexity, and inflexibility of building and maintaining that platform on premises. The PaaS provider manages servers, networks, storage, virtualization software, middleware, and runtime. Development teams can use all of it for a monthly fee based on usage, and might purchase more resources on demand, as needed.

With the PaaS delivery model, the cloud provider often has full administrative control over all items that are listed under IaaS plus VM/LDAP, databases, and runtimes.

The cloud consumer's administrative control is limited to the ready-made environment.

In the cloud, security responsibility also is shared between the cloud provider and therefore, the customer. As a PaaS customer, you are in charge of securing your applications, data, and user access. The PaaS provider secures the underlying hardware, network, middleware, and runtime.

The following security best practices can be considered when PaaS is used:

- ▶ Ensures that the provider's security meet with the compliance and security requirements.
- ▶ Uses threat modeling as an efficient technique and methodology to improve the security and compliance of your software within the earlier stages of development. It also provides a structured method for identifying weaknesses and security improvements in your application design.
- ▶ Checks for inherited software vulnerabilities.
- ▶ Implements role-based access controls.

Serverless computing security

Serverless computing can be defined as a hyper-efficient PaaS, which differs from conventional PaaS in the following ways:

- ▶ Serverless discharges all responsibility for infrastructure management tasks to the cloud provider, which allows you to focus all your time and energy on developing code and applications.
- ▶ Serverless runs code only on-demand; that is, when requested by the application, which enables the cloud provider to charge a customer for compute resources only when their code is running.
- ▶ The following challenges rise significantly when Serverless computing is used:
 - The total amount of information and number of resources increases significantly. This increase challenges your ability to analyze and investigate all of the data.
 - Protocols and attack points are multiplied to each function.
 - Serverless uses more resources, which implies more permissions to manage.

- Serverless applications use different cloud services from various cloud providers across multiple technologies, regions, and patterns, which results in more complexity to set up and maintain a security-focused view.

Software as a Service security

SaaS is application software that runs within the cloud that customers use by way of an internet connection. This connection often is made by using a mobile application or web access, typically for a monthly or annual fee.

With the SaaS delivery model, the cloud provider often has full administrative control over all items that are listed under IaaS plus VM/LDAP, databases, runtimes, and the services implementation.

The cloud consumer's administrative control is limited to the service implementation, which can be configured by way of a custom front-end.

The SaaS provider is in charge of securing network, servers, storage, virtualization, operating systems, middleware, runtimes, applications, and data. However, providers are not responsible for securing your data or user access to it. To avoid security breaches, you can implement improved security practices and technologies.

The following security best practices can be considered when PaaS is used:

- ▶ Detect shadow services and compromised accounts by using tools to audit networks for unauthorized cloud services and compromised accounts.
- ▶ Apply identity and access management (IAM).
- ▶ Encrypt cloud data. Data encryption protects data at-rest and data in-transit between the cloud user and the cloud provider or between different cloud resources.
- ▶ Ensure that the provider's security meet with the compliance and security requirements.

1.2.2 Cloud deployment models and security considerations

The cloud deployment model represents a specific type of cloud environment that is defined by ownership, boundaries, size, and use cases.

Security in the cloud is an enabling technology that helps you accelerate your journey to the cloud. To avoid cloud computing risks, a cloud provider must incorporate built-in security layers at every level delivering a fully configured solution with a proven industry-leading security and regular vulnerability scans.

Private cloud security

A private cloud is cloud infrastructure that is operated for one company. It is managed by the company or a third party. It is hosted primarily on-premises, but also can be hosted on dedicated cloud-provider or third-party infrastructure.

Private cloud enables you to take advantage of cloud efficiencies while providing greater administrative control over your resources, data security, and regulatory compliance. It avoids the potential introduction of vulnerabilities by extending the trust boundaries.

Public cloud security

Unlike single-tenant private cloud infrastructure, public cloud environments are multitenant and accessible by way of the internet. Therefore, public and private clouds must have different approaches when dealing with cloud security.

With a public cloud infrastructure, physical security in IaaS, middleware security in PaaS, encryption of data at rest, and authentication services in SaaS are abstracted away.

Hybrid cloud security

Hybrid cloud integrates private and public clouds by using technologies, management tools, frameworks, and patterns that allow workloads to move seamlessly between both as needed for optimal performance, ability, security, compliance, and cost-effectiveness.

Security and monitoring solutions often work with public cloud infrastructure or on-premises resources, but generally not both. This constraint leads to a challenging patchwork of security mechanisms that needs a consequent amount of IT's time to manage and maintain.

1.3 IBM Power Systems security architecture

Building security into every level of your stack is achievable by implementing various third-party vendor security solutions. However, that approach compounds the complexity that exists, and introduces even more vulnerabilities and points of exposure into your network. Your best recourse is to take a multi-layered, holistic approach, one that secures all of your organization's data and systems while also minimizing complexity.

With IBM Power Systems, you get comprehensive, end-to-end security that tightly integrates across the entire stack, from processor and firmware to operating system and hypervisors, to apps and network resources, all the way to security system management (see Figure 1-6).

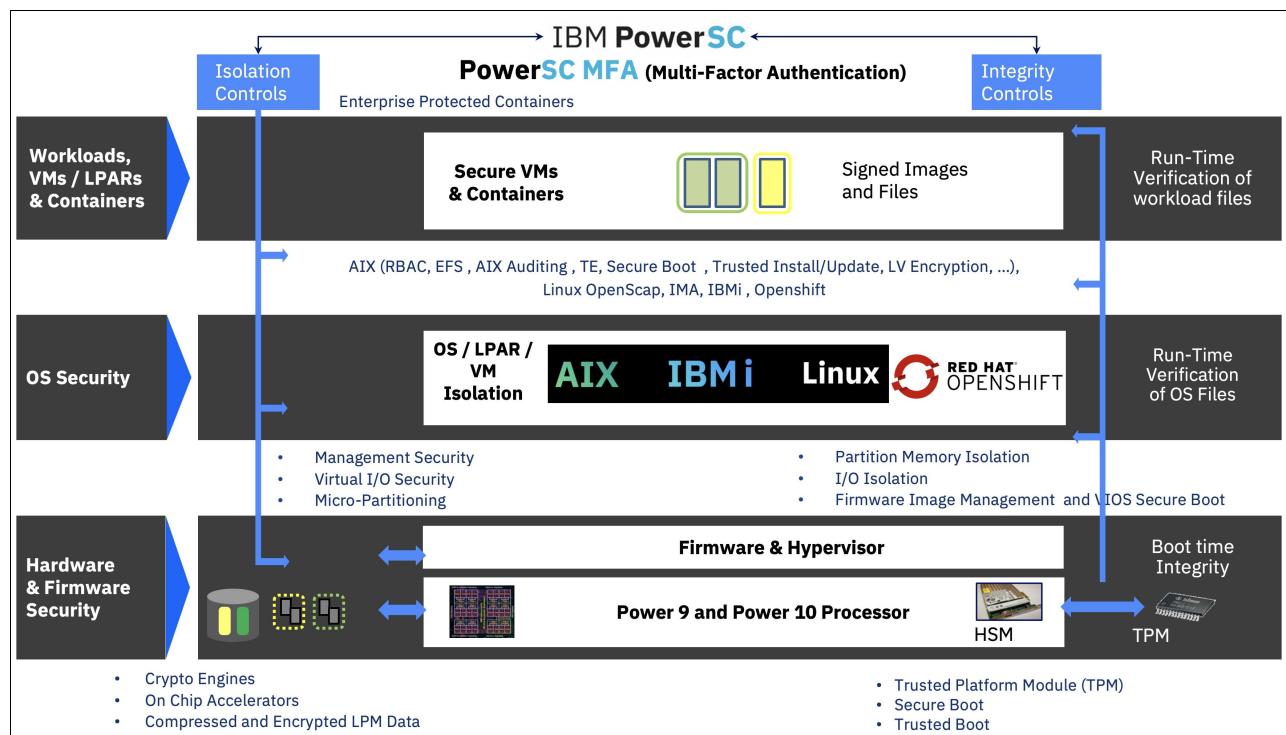


Figure 1-6 IBM Power Systems security architecture

1.3.1 Hardware, firmware, and hypervisor

Systems can be easily configured to boot a compromised operating system kernel if no measures are taken to ensure kernels. Also, poorly performing cryptography can be an impediment to the protection of sensitive data that is in transit and at rest.

IBM Power Systems provides proven security features for the hardware, firmware, and hypervisor that helps address IT security challenges with a comprehensive (yet simplified) approach to security and compliance across the entire stack.

Cryptographic engines

IBM Power10™ systems protect sensitive data by using the latest pervasive encryption capabilities across hybrid cloud deployments. The Power10 processor introduces full memory encryption at scale, ready to use. Transparent memory encryption is designed to simplify encryption and support end-to-end security without affecting performance by using hardware features for a seamless user experience.

Also, workloads on Power10 benefit from cryptographic algorithm acceleration (with 4x the number of cryptographic engines), which allows algorithms (such as AES, SHA2, and SHA3) to run significantly faster on Power10 than they did on POWER9-based systems (on a per-core basis). This performance acceleration allows features, such as AIX Logical Volume Encryption to be turned on with low performance overhead.

To be prepared for the Quantum Era, Power10 Systems are built to efficiently support upcoming cryptography techniques, such as Quantum-safe Cryptography and Fully Homomorphic Encryption (FHE).

Quantum-safe Cryptography refers to the efforts to identify algorithms that are resistant to attacks by classic and quantum computers in preparation for the time when large-scale quantum computers are built.

Homomorphic encryption refers to encryption techniques that permit systems to perform computations on encrypted data without decrypting the data first. The software libraries for these solutions are optimized for the IBM POWER Instruction Set Architecture (ISA), which today are (or soon are to be available) from their respective Open Source communities.

On-chip accelerators

POWER9 boasts on-chip accelerators that compress and decompress GZIP files much faster than software. You can quickly compress and encrypt entire VMs and securely move them across the network.

Secure boot on Power

Secure boot protects system integrity by verifying and validating all firmware components by way of digital signatures. All firmware that is released by IBM is digitally signed and verifiable. You can also install your own firmware and replace the hierarchy of public keys that are needed for verification.

Trusted boot and Trusted Platform Module

The trusted boot feature in POWER allows for the inspection and remote verification (attestation) of all firmware components on your server. The trusted boot feature uses the TPM, which serves as the Root of Trust (RoT) for measuring the software stack. Verification is signed by the TPM, so you know that the firmware was not tampered within any way.

PowerVM Enterprise Hypervisor

IBM PowerVM® has an excellent security track record when compared against major competitors, so you can confidently secure your VMs and cloud environments.

1.3.2 Operating system

IBM Power Systems offers leading security capabilities for a wide range of operating systems, such as IBM AIX, IBM i, and Linux. Features vary depending on the operating system, but examples of these capabilities include being able to complete the following tasks:

- ▶ Assign administrative functions that often are reserved for the root user without compromising security.
- ▶ Encrypt file-level data through individual keystores.
- ▶ Gain greater control over the commands and functions that are available to users, along with control over what objects they can access.
- ▶ Log access to an object in the security audit journal by using system values and the object-auditing values for users and objects.
- ▶ Carry encryption across an entire drive; first, encrypting an object and then, writing out in the encrypted form.
- ▶ Measure and verify every file before it runs or opens for the requesting user.

1.3.3 Workloads, VMs, and containers

Workloads are no longer restricted to on-premises data centers; they are continually moving to virtualized and cloud environments. This means that many organizations are adopting containers to deploy new and existing applications across hybrid infrastructures. These increasingly dynamic environments and workloads require equally versatile security capabilities.

Live Partition Mobility

By using IBM Power Systems, you can secure data in motion. LPM protects VMs through encryption when you must migrate from one system to another. This capability is critical if you have virtualized on-premises data centers and hybrid cloud environments.

Protected Execution Facility

The Protected Execution Facility is one example of how IBM Power Systems protects this level of the stack. It is a POWER feature that encrypts and runs your VMs in secure memory; that is, a compromised hypervisor does not have access.

Also, in a cloud environment, malicious insiders or administrators with access to the VM do not have access to the workloads running in the secure memory. The decryption process occurs only on a verified system.

Confidential computing

POWER offers the most secure workload isolation in cloud deployments, with integrity engineered into every layer of the system. All components of the stack are fully integrated and co-optimized, and are provided by IBM as a single vendor, which makes it much more secure (see Figure 1-7).

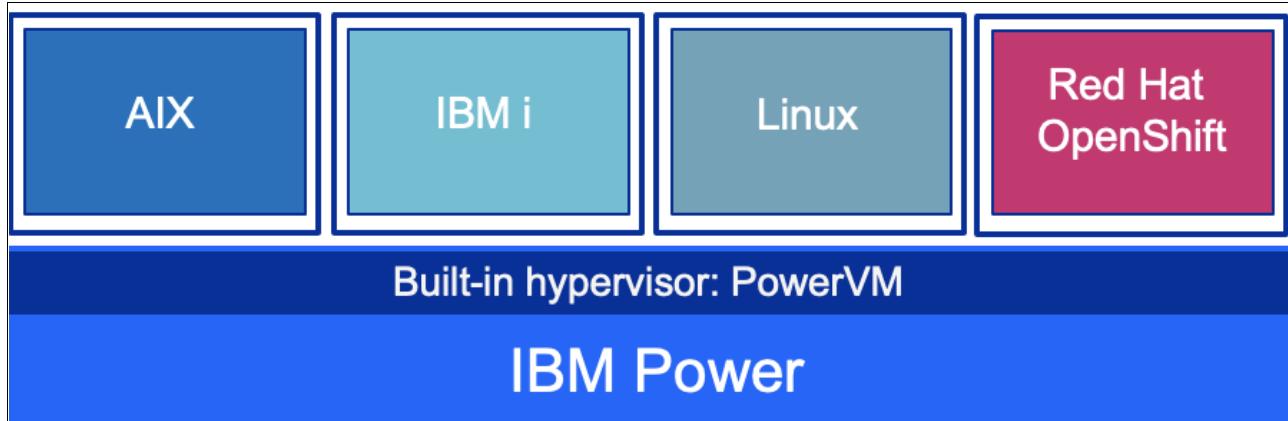


Figure 1-7 IBM Power Systems Security architecture

PowerVM, the built-in hypervisor, has an outstanding track record, with orders of magnitude fewer vulnerabilities than competitive x86 hypervisors. Power10 systems feature advanced firmware integrity with extra measures to isolate the CPU from service processors for better defense against attacks on management systems.

Power10 introduces innovations to address emerging threats, specifically with more features and enhancements to defend against application domain vulnerabilities, such as return-oriented programming (ROP) attacks (a security exploit technique that is used by attackers to run code on a target system). This capability uses a new in-core hardware architecture that imparts minimal performance overhead.

1.3.4 IBM PowerSC

IBM PowerSC is an integrated portfolio offering for enterprise security and compliance in cloud and virtual environments. It is on top of your stack while providing a web-based UI for managing the security features of IBM Power Systems that are from the lowest level up.

With its simplification and automation capabilities, IBM PowerSC helps to save time and cut costs by streamlining compliance and audit processes. It also reduces security risks by increasing visibility across the stack.

IBM PowerSC includes the following features:

- ▶ Assign administrative functions that often reserved for the root user without compromising security.
- ▶ Compliance automation IBM PowerSC includes pre-built profiles that support many industry standards. You can customize these profiles and merge them with enterprise rules without having to touch XML.
- ▶ Real-time compliance detects and alerts you when someone opens or interacts with security-critical files.
- ▶ Trusted Network Connect (TNC) alerts you when a VM is not at the prescribed patch level. It also notifies you when fixes become available.

- ▶ Trusted boot allows for the inspection and remote verification of all firmware components that are running on your server.
- ▶ Trusted firewall protects and routes internal network traffic between the AIX, IBM i, and Linux operating systems.
- ▶ Trusted logging creates centralized audit logs, which are easy to back up, archive, and manage.
- ▶ Preconfigured reporting and interactive timeline. The IBM PowerSC Standard Edition supports auditing with different preconfigured reports.

1.3.5 IBM PowerSC Multi-factor Authentication

Multi-factor authentication allows you to use at least two of the following categories to confirm separate pieces of evidence to grant access to a system:

- ▶ Something that you know: A password and PIN Code.
- ▶ Something that you have: ID badge or a cryptographic key.
- ▶ Something that you are: Fingerprint or other biometric data.

IBM PowerSC Multi-Factor Authentication (MFA) provides alternative authentication mechanisms for systems that are used with RSA SecurID-based authentication systems, and certificate authentication options, such as Common Access Card (CAC) and Personal Identification Verification (PIV) cards. IBM PowerSC MFA allows the use of alternative authentication mechanisms instead of the standard password.

1.3.6 IBM Power10, protecting trust from core to the cloud

Although enforcing a data encryption policy is a great way to minimize the risk of a data breach that, in turn, minimizes costs, at the time of this writing, only 17% of enterprises surveyed indicated that they protected more than 50% of their sensitive data in cloud with encryption⁶.

Only a few enterprises at the worldwide level have an encryption strategy that is applied consistently across the entire organization, largely because it adds complexity, costs, and negatively affects performance, which means missed SLAs to the business.

The rapidly evolving cyberthreat landscape requires focus on cyber-resilience. Persistent and end-to-end security is the only way to reduce exposure to threats. Power processor-based platforms always offered the most secure and reliable servers in its class.

The Power E1080 further extends the industry-leading security and reliability of the Power processor-based platform, with focus on protecting applications and data across all the hybrid cloud environments. It introduces significant innovations along the following major dimensions:

- ▶ Advanced Data Protection offers simple to use and efficient capabilities to protect sensitive data through mechanisms such as encryption and multi-factor authentication.
- ▶ Platform Security ensures that the server is hardened against tampering, continuously protects its integrity, and ensures strong isolation among multi-tenant workloads. Without strong platform security, all other system security measures are at risk.
- ▶ Security Innovation for Modern Threats provides stays ahead of new types of cybersecurity threats by using emerging technology.

⁶ Thales Data Threat Report - Global Edition:
<https://cpl.thalesgroup.com/resources/encryption/2021/data-threat-report>

- ▶ Integrated Security Management addresses the key challenge of ensuring correct configuration of the many security features across the stack, monitoring them, and reacting if unexpected changes are detected.

The Power E1080 is enhanced to simplify and integrate security management across the stack, which reduces the likelihood of administrator errors.

In the Power E1080, all data is protected by a greatly simplified end-to-end encryption that extends across the hybrid cloud without detectable performance effect and prepares for future cyberthreats.

Power10 processor-core technology features built-in security integration:

- ▶ Stay ahead of current and future data threats with better cryptographic performance and support for quantum-safe cryptography and fully homomorphic encryption (FHE).
- ▶ Enhance the security of applications with more hardened defense against return-oriented programming (ROP) attacks.
- ▶ Simplified single-interface hybrid cloud security management without any required setup.
- ▶ Protect your applications and data with the most secure VM isolation in the industry with orders of magnitude lower Common Vulnerability Exposures (CVEs) than hypervisors that are related to x86 processor-based servers.

Also, workloads on the Power E1080 benefit from cryptographic algorithm acceleration, which allows algorithms, such as AES, SHA2, and SHA3, to run significantly faster than POWER9 processor-based servers on a per-core basis. This performance acceleration allows features, such as AIX Logical Volume Encryption, to be enabled with less performance overhead.

Crypto engines and transparent memory encryption

Power10 processor technology is engineered to achieve significantly faster encryption performance with quadruple the number of advanced encryption standard (AES) encryption engines.

Compared to IBM POWER9 processor-based servers, Power E1080 is updated for today's most demanding standards and anticipated future cryptographic standards, such as post-quantum and fully homomorphic encryption (FHE), and brings new enhancements to container security.

Transparent memory encryption is designed to simplify encryption and support end-to-end security without affecting performance by using hardware features for a seamless user experience.

Figure 1-8 shows the protection that is introduced in all layers of an infrastructure.

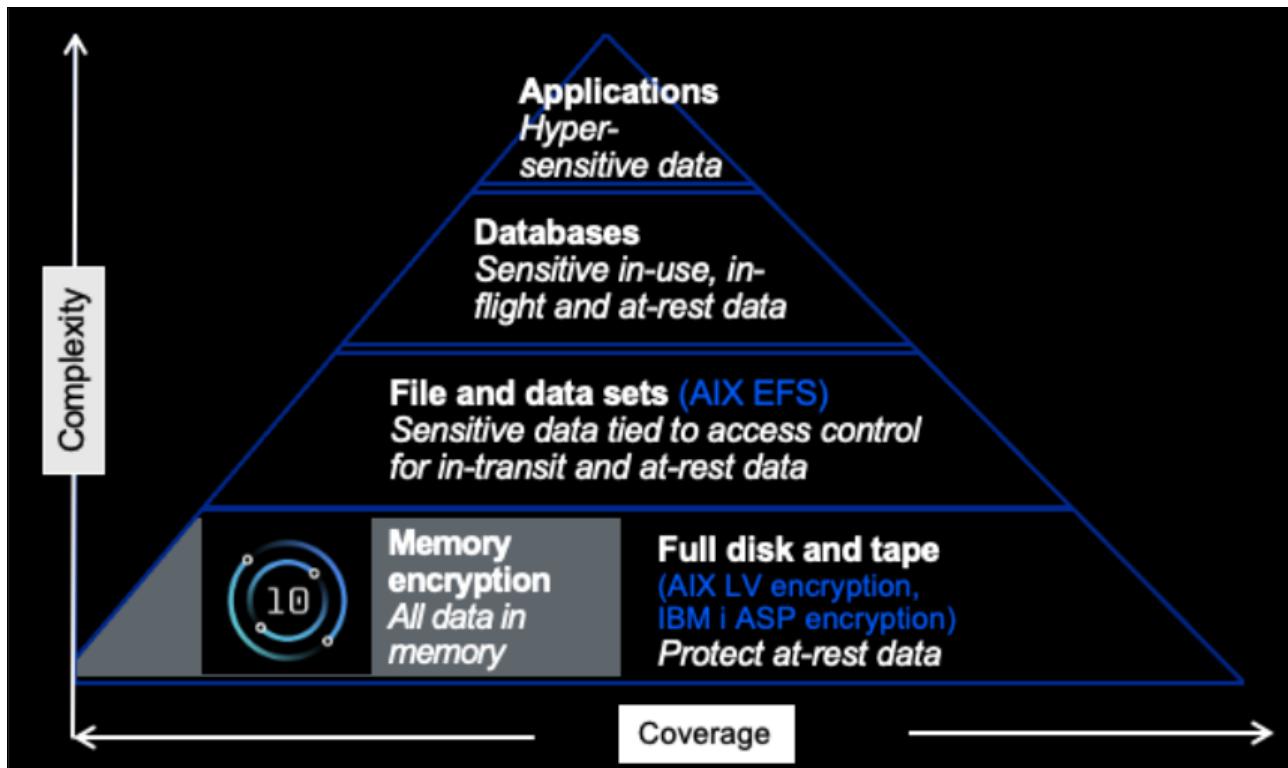


Figure 1-8 Protect data in memory with transparent memory encryption

Quantum-safe cryptography support

To be prepared for the Quantum era, the Power E1080 is built to efficiently support future cryptography, such as Quantum-safe cryptography and Fully Homomorphic Encryption (FHE). The software libraries for these solutions are optimized for the Power10 processor-chip instruction set architecture (ISA) and are or will be available in the respective open source communities.

IBM PowerSC support

The Power E1080 benefits from the integrated security management capabilities that are offered by IBM PowerSC, which is the IBM Power Systems software portfolio for managing security and compliance on every Power processor-based platform that is running AIX, IBM i, or the supported distributions and versions of Linux.

PowerSC is introducing more features to help customers manage security end to end across the stack to stay ahead of various threats. Specifically, PowerSC 2.0 adds support for Endpoint Detection and Response (EDR), host-based intrusion detection, block listing, and more Linux support.

1.4 Paradigm shift for protecting IBM Power Systems

Forward-leaning companies are embracing change at an accelerated pace. Business priorities are driving digital transformation:

- ▶ Users and Endpoints: Accessing from anywhere by using any device.
- ▶ Data and Apps: Data is a shared resource for users and applications.
- ▶ Infrastructure: Servers and networks distributed across hybrid cloud environments.

Security must safeguard these key transformations; unfortunately, traditional cybersecurity programs are built to handle this level of transformation. You must overcome those challenges by putting zero trust into action with a modern, open approach to security that aligns with business priorities.

Cognitive security combines the strengths of AI and human intelligence to proactively detect and analyze threats. This combination provides actionable insights to administrators and security officials for making informed decisions with speed and accuracy.

This paradigm shift is game changing for security analysts and cyberattackers. For example, quantum computing and the increased adoption of containerized workloads requires a paradigm shift in cryptography and mechanisms that are used to protect containers in every layer. Figure 1-9 highlights some of traditional and emerging threats at the hardware, firmware, hypervisor, operating system, and applications layers that are mapped with IBM Power Systems security architecture.

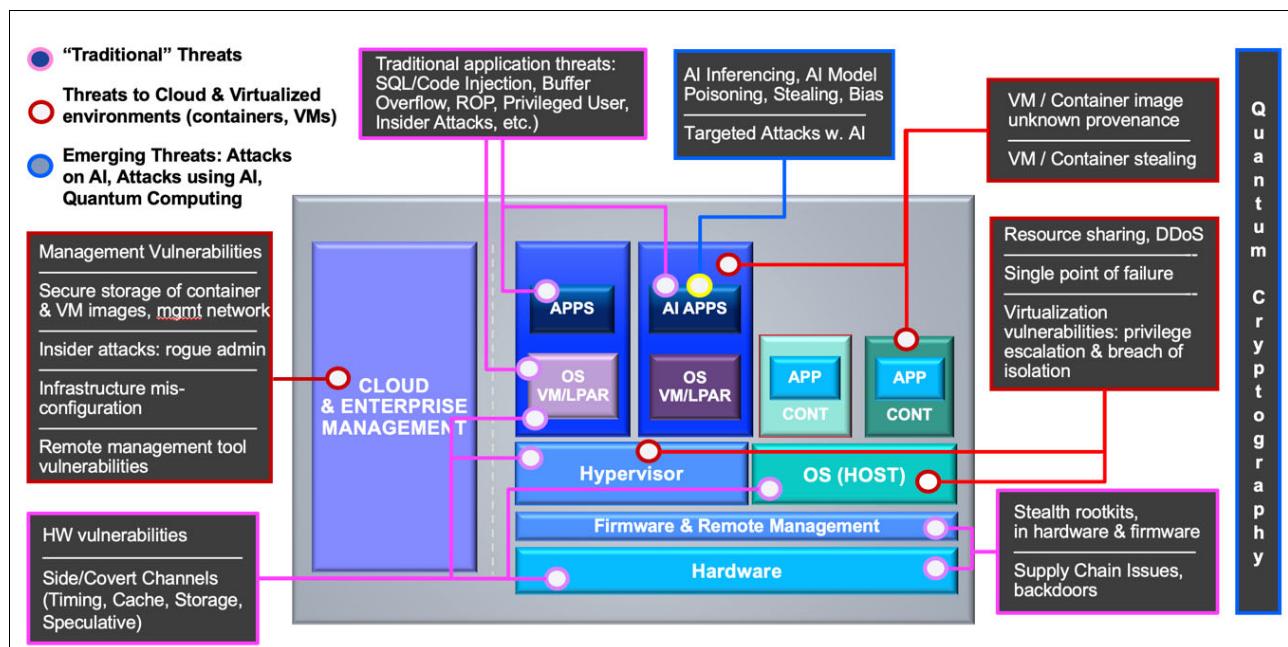


Figure 1-9 Traditional threats, threats to cloud and virtualized environment and emerging threats

1.4.1 Zero Trust journey

Zero Trust is a project that takes a long time to complete. Zero Trust's primary goal is to understand and regulate how users, processes, and devices interact with data.

To build a realistic picture of network activity, verify its validity, and prevent lateral movement by a threat actor, multiple data points are required. The system can take advantage of user and device data, and security-relevant information (such as location, time, and logged behavior) to allow or deny access to specific assets, with the choice being logged for future suspicious activity analyses. This procedure applies to every request for access to a sensitive resource.

Building a mature zero trust environment is a slow process that often necessitates extra capabilities because it does not address (at an early stage) new attacks technologies, tactics, or strategies.

The shift can be made gradually, which reduces risk at each stage and, over time, dramatically boosts visibility and automatic reactions.

Figure 1-10 shows how you can start now and improve over time by adding the fundamental capabilities first and then, refining them and adding integration over time until you add the analytics and orchestration to create the automated and real-time feedback.

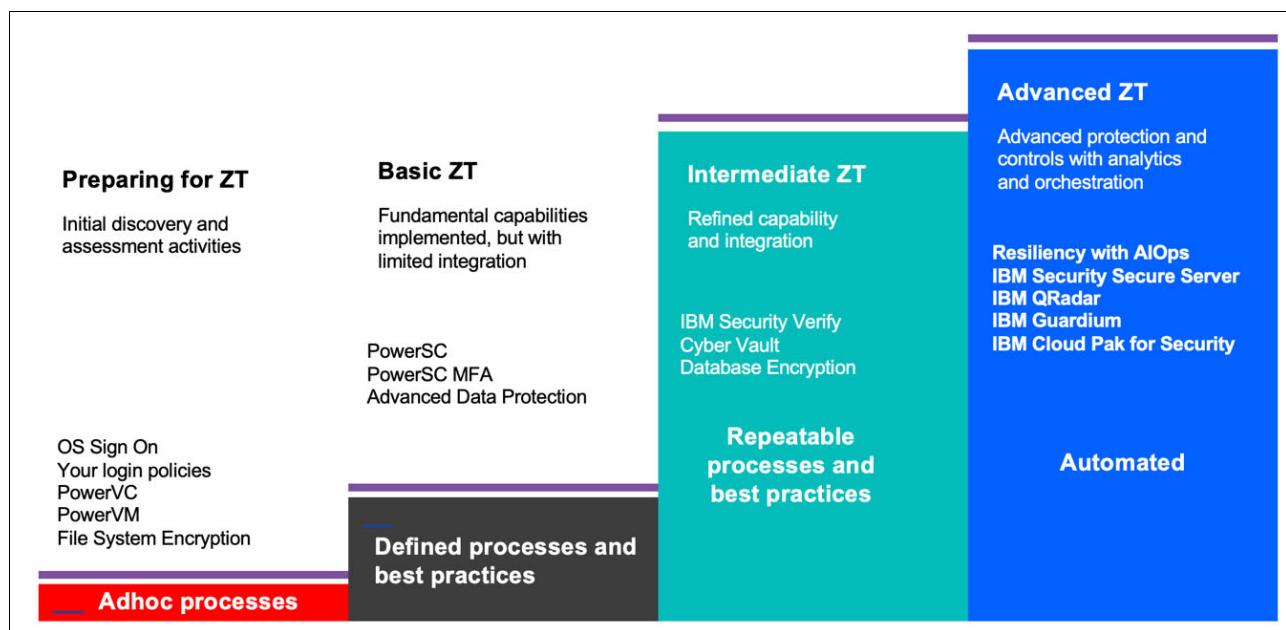


Figure 1-10 Zero Trust journey for IBM Power Systems

1.4.2 Traditional threats

A traditional vulnerability represents a popular or known exploitable weakness in the server that enables attack through remote or physical access to system hardware, middleware, or applications. Top traditional threats include the following examples:

- ▶ CPU side channel attacks
- ▶ Timing attacks
- ▶ DRAM memory Rowhammer attacks
- ▶ Broken access control
- ▶ Cryptographic failures

- ▶ SQL injection or code injection
- ▶ Security misconfiguration
- ▶ Vulnerable and outdated components
- ▶ Identification and authentication failures
- ▶ Software and data integrity failures
- ▶ Rootkits
- ▶ Supply chain backdoors

IBM Power Systems Security solutions that are powered by IBM Security portfolio address the most of traditional threats, as listed in Table 1-2.

Table 1-2 Traditional threat versus IBM POWER Architecture and IBM Security solutions

Layer	Hardware vulnerabilities	Application threats	Stealth rootkits	Supply chain backdoors	IBM Security solution
Hardware	X		X	X	▶ IBMPowerVM ▶ IBM PowerSC
Firmware			X	X	
Hypervisor	X				
Operating system	X				▶ IBM PowerSC ▶ File system encryption
VM/LPAR		X			IBM PowerSC
Application		X			▶ IBM QRadar ▶ IBM Guardium® ▶ IBM Cloud Pak for Security ▶ Database Encryption

1.4.3 Threats to cloud and virtualized environments

VMs and containers often are where the applications and workloads run. They must be secured to ensure the security of the system.

One of the most important tasks that the system must do is to verify the VM or container *before* allowing it to run so that the system knows that it was not attacked and altered for malicious purposes. When the VM or container is running, the hypervisor or operating system must ensure that they remain isolated.

Top traditional threats include the following examples:

- ▶ Management vulnerabilities
- ▶ Secure storage of container and VM images; management network
- ▶ Insider attacks; that is, rogue administrator
- ▶ Infrastructure misconfiguration
- ▶ Remote management tool vulnerabilities
- ▶ Resource sharing, DDoS
- ▶ Single point of failure
- ▶ Virtualization vulnerabilities: privilege escalation and breach of isolation
- ▶ VM or container image unknown provenance
- ▶ VM or container stealing

1.4.4 Security between different LPARs

PowerVM is a high-performance virtualization solution for IBM Power Systems servers that are running IBM AIX, IBM i, and Linux workloads. PowerVM represents the state of the art in enterprise virtualization and is based on more than a decade of evolution and innovation. It is widely deployed in production environments globally by most Power Systems customers.

The Power Systems scale-out and scale-up server family includes proven workload consolidation platforms that help clients save costs while enhancing overall performance, availability, and energy efficiency.

An enterprise can combine large numbers of applications and servers, fully virtualize its system resources, and create a more flexible, dynamic IT infrastructure with these servers and PowerVM virtualization technologies (see Figure 1-11).

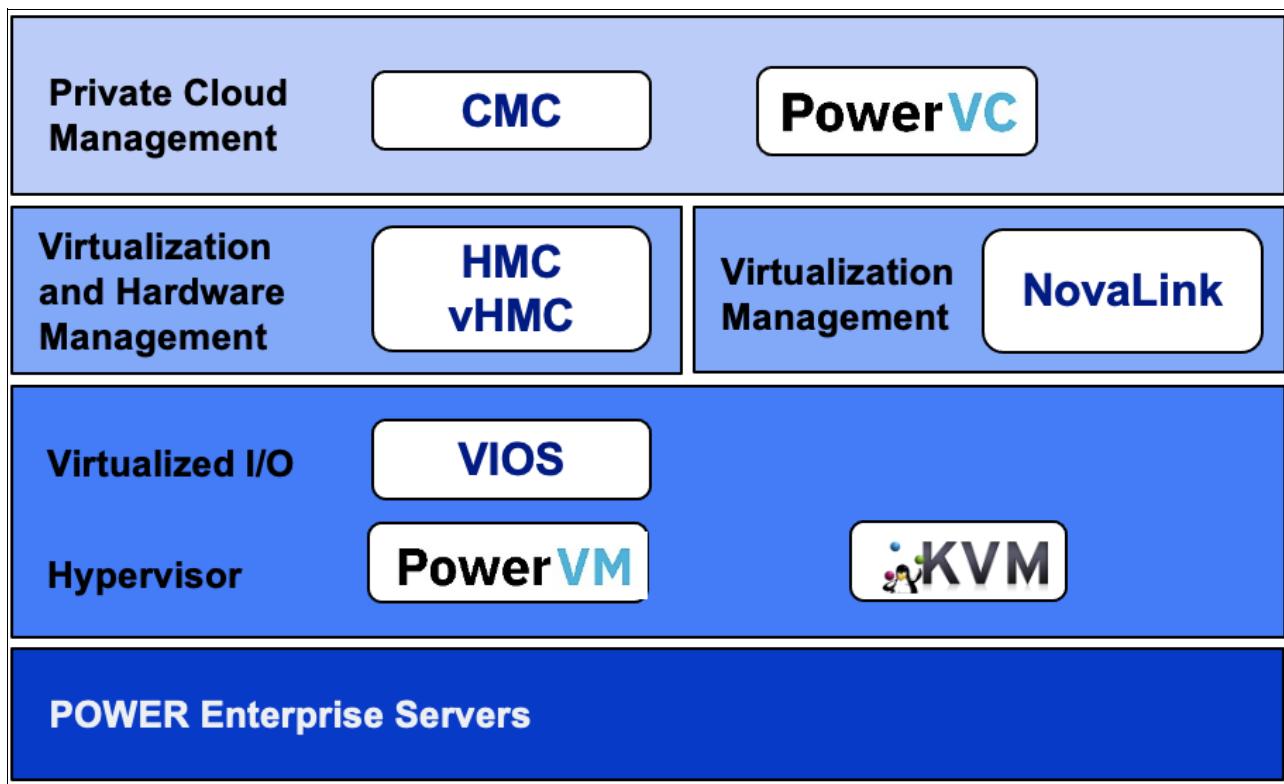


Figure 1-11 End to end virtualization and security

The following security solutions are available for hypervisor, memory, process, and I/O:

- ▶ PowerVM Hypervisor

PowerVM takes advantage of the Power hardware to provide high levels of security. Hypervisor domain, Kernel domain, and Application domain are the three separate protection domains that are built into the hardware. The hardware restricts the number of instructions that can be performed, depending on the current protection domain. It also provides particular access points for changing domains.

- ▶ Memory security

Only the hypervisor can access memory by using a physical actual address because of the hardware's design. Code in partitions accesses memory by way of a layer of indirection, with the partitions' addresses serving as aliases for the physical real memory.

This capability is used not only for partition isolation, but also for the server's other virtualized functions.

- ▶ Processor security

Because retrieving data from DIMMs takes time, processors provide several levels of data and instruction caches to speed up instruction execution. The caches on Power servers are accessed by the hardware that uses physical real addresses.

Because the hypervisor is in charge of configuring the HPT, which has this physical address, no security risk exists in leaving data in the caches when the partitions are switched on hardware threads.

- ▶ I/O security

I/O is protected by way of a structure that is called the Translation Control Entry Table, which is similar to how memory is protected with Hardware Page Tables (TCEs). The I/O request must involve the hypervisor because the partition cannot issue the instructions to start an I/O request or update the TCEs that are maintained in physical real memory.

1.4.5 Protecting sensitive applications and data in containerized workloads

The concept of containerizing applications has been around for decades, but adoption recently accelerated as new container technology collides with the growing need for businesses to transform their operations and infrastructure. For more flexibility and speed to market, they are increasingly turning to cloud-native development and hybrid, multicloud computing environments.

Microservices-based applications that are deployed in containers by using technologies, such as Kubernetes, provide that necessary flexibility and speed. Containers are suitable for modern systems because they enable portability by combining code, configuration files, libraries, and other dependencies into a lightweight, platform-neutral executable software bundle.

However, containers present more security challenges, including the following examples:

- ▶ The possibility of “escape attacks” to gain access to shared host were demonstrated by security Researchers.
- ▶ Raising concerns about the strength of isolation for highly sensitive workloads.
- ▶ Isolation of shared Linux kernel in “standard” containers are not as strong as hypervisors and more difficult to configure.
- ▶ IBM Enterprise Protected Containers offers isolated, confidentiality, and integrity protected Red Hat OpenShift containers that offer the same level of security as LPARs:
 - Provide the same strength of isolation to containers as that afforded by VMs or LPARs.
 - Run EPC containers as lightweight VMs, which use hybrid virtualization that is co-optimized in Power10 and PowerVM.
 - End-to-end protection of code and data, including when in use (confidential computing).
 - Simplify workload regulatory compliance, especially in multi-tenant environments.
 - PowerVM has no CVEs currently and orders of magnitude lower number of CVEs than competitive hypervisors.

1.4.6 IBM Power Systems Virtual Server and General Data Protection Regulation

IBM Power Systems Virtual Server is a Power Systems offering. Power Systems Virtual Servers are in the IBM data centers, which are distinct from the IBM Cloud servers with separate networks and direct-attached storage.

You can use the Power Systems Virtual Servers to deploy a virtual server, also known as an LPAR, in a matter of minutes. IBM Power Systems clients who often relied upon on-premises-only infrastructure can now quickly and economically extend their Power IT resources off-premises.

Avoid the large capital expense or added risk when migrating your essential workloads and get started with Power Systems Virtual Servers today.

In the data centers, the Power Systems Virtual Servers are separated from the rest of the IBM Cloud servers with separate networks and direct-attached storage. The internal networks are fenced but offer connectivity options to IBM Cloud infrastructure or on-premises environments. This infrastructure design enables Power Systems Virtual Servers to maintain key enterprise software certification and support because the Power Systems Virtual Server architecture is identical to certified on-premises infrastructure.

The General Data Protection Regulation seeks to create a harmonized data protection law framework across the European Union (EU) and aims to return to citizens the control of their personal data. The GDPR imposes strict rules on anyone that is hosting and processing personal data anywhere in the world. Also, this regulation introduces rules that relate to the free movement of personal data within and outside of the EU.

With the GDPR, IBM Power Systems Virtual Server clients can rely on the Power Systems Virtual Server team's understanding and compliance with emerging data privacy standards and legislation. Power Systems Virtual Server clients also can rely on IBM's wider ability to provide a comprehensive suite of solutions to assist businesses of all sizes with their own internal data governance requirements.⁷

1.4.7 Emerging threats

Potential cyberisks rise in tandem with technological advancements. Although this idea is not new, the present rate of innovation makes it more vital than ever to assess the ramifications of these advancements on IBM Power Systems cybersecurity capabilities, especially as hackers become more skilled and adept at using growing weak spots.

Quantum Computing

Quantum computing is based on quantum mechanics, which governs how nature works at the smallest scales. At the same time, it delivers an expanding advantage for specific classes of problems, such as factoring large numbers, with deep implications for cybersecurity.

For decades, cryptography relied mostly on the hardness of factorization problem:

- ▶ Quantum computers significantly reduce the hardness of this problem, thus requiring a new paradigm for cryptography.
- ▶ Well-known examples are Shor's algorithms for factoring and discrete logarithms.
- ▶ Most asymmetric (Public-Private Key) Cryptographic algorithms are vulnerable, including RSA, DH, and ECDSA.

⁷ <https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-data-protection>

The most contentious use of Quantum computing is its ability to break public-key encryption, notably the RSA scheme. RSA is based on the fact that factoring the product of two prime numbers is computationally difficult. It takes a billion of years for a traditional computer to crack RSA encryption. RSA might be defeated in seconds by a quantum computer with about 4,000 stable qubits.

NIST, in collaboration with outside technologists such IBM, is developing an open cryptography stack, which is robust against attacks from quantum computers.

The goal of post-quantum cryptography (also known as quantum-resistant cryptography) is to develop cryptographic systems that are secure against quantum and conventional computers while also allowing them to communicate with existing protocols and networks.

IBM Research® is extensively involved with NIST in this collaboration. IBM Power Systems efficiently supports this stack:

- ▶ Software stack enhancements in IBM POWER8® and POWER9 with the use of POWER ISA crypto assist instructions.
- ▶ Power10 processor HW enhancements.

The IBM Power 10 processor is designed to deliver much faster encryption performance for today's most demanding cryptographic standards, predicted future cryptographic standards (such as quantum-safe cryptography), and fully homomorphic encryption.

Artificial Intelligence

As Artificial Intelligence (AI) becomes a prevalent tool in the IT landscape, cybersecurity is becoming a battleground for AI. AI is being used to avoid traditional security protections and counter adversary responses.

The cat and mouse game between attacker and defender is evolving to a new level where artificial intelligence enhancing the human aspect. AI versus AI most likely is the future of cybersecurity.

Attackers might use AI to conceal the attack. One goal of IBM Research's security AI effort is to anticipate potential assaults and develop defensive solutions before black hats (criminals) begin an attack.

The Adversarial Robust Toolbox (ART)⁸, an Open Source tool for use by the AI and software communities for this type of study, was one of IBM's creations. For the first time, ART v1.4 allows developers and researchers to use a single unified library to evaluate and defend machine learning models and applications against the adversarial threats of evasion, poisoning, extraction, and inference.

IBM donated ART to the Linux Foundation, which received ART with the simple goal of accelerating the development of responsible AI-powered technologies. It also encouraged the AI and Security communities to collaborate and co-create these tools to ensure that they work for everyone as intended in various real-world AI deployments. IBM recently integrated ART to its IBM Cloud Pak for Data as part of its Open-Source Management service, making it easier and more secure for developers to access ART.

For more information, see this [IBM Developer web page](#).

⁸ <https://developer.ibm.com/articles/applying-the-adversarial-robustness-toolbox/>

1.5 Overview of cybersecurity landscape and threats for organizations

Understanding the attack landscape can assist security teams in prioritizing resources, drilling for the most likely scenarios, and identifying shifts in attacker techniques.

In this section, we provide insights about the top attack trends: ransomware is undeniably the top attack type, followed by data theft and server access attacks. In terms of initial attack vectors, scan and exploit are the most used, followed by phishing and credential theft.

Note: The X-Force Threat Intelligence Index gives insights into the major cybersecurity threats that organizations all over the world face today. For more information, see [IBM X-Force Threat Intelligence Index 2021](#).

1.5.1 Top attack trends

IBM Security X-Force⁹ drew on billions of data points that were collected from our customers and public sources January - December 2020 to analyze attack types, infection vectors, and global and industry comparisons. Some of the top findings that are presented in the X-Force Threat Intelligence Index are discussed in this section.

Figure 1-12 shows the breakdown of attack as a percentage of total attacks that were observed according to IBM Security X-Force Report 2021.

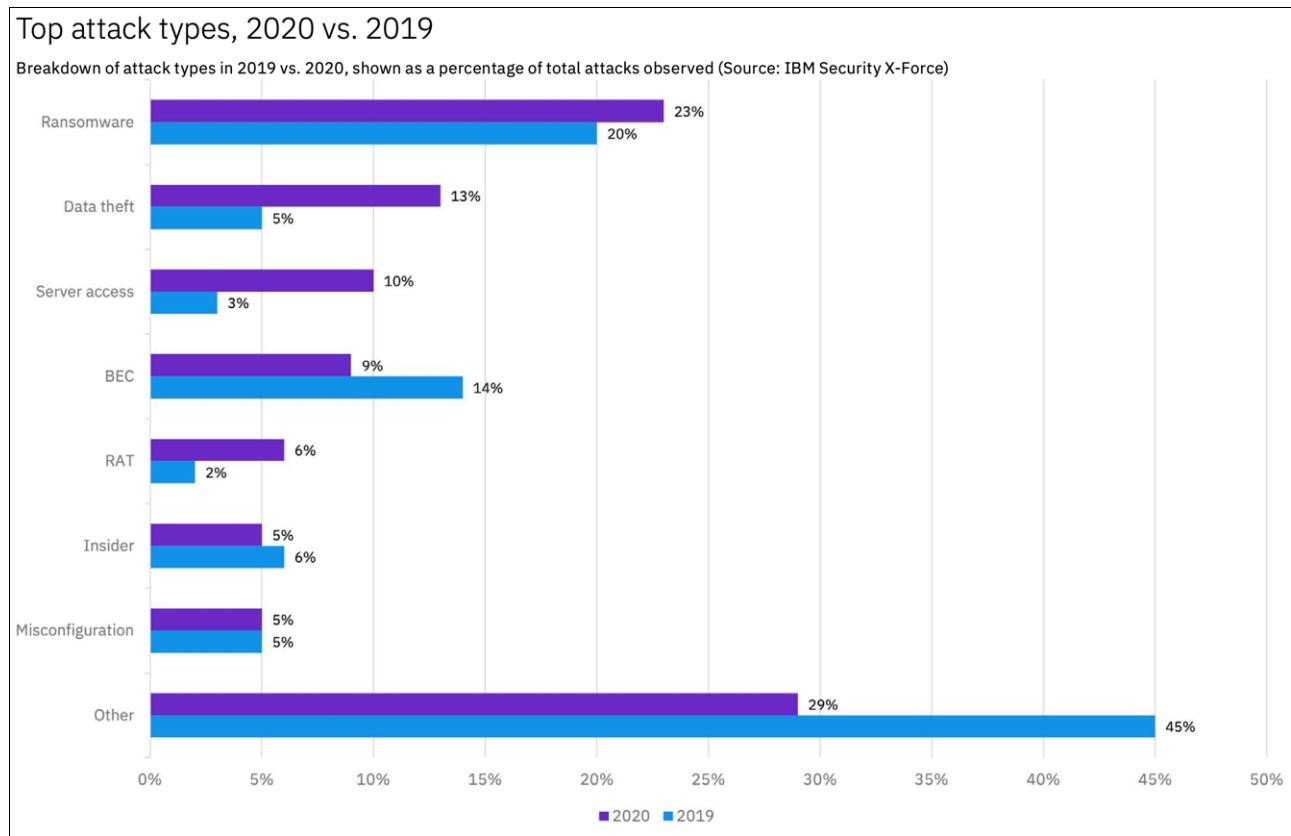


Figure 1-12 Breakdown of attack type in 2019 versus 2020

⁹ <https://www.ibm.com/downloads/cas/M1X3B7QG>

Ransomware attack

Ransomware is malware that is used to blackmail victims by threatening to publish sensitive information or lock users out until a ransom is paid (often in crypto currency, such as Bitcoin).

Ransomware attacks are disruptive. They affect your business and your servers, and potentially spread to your customers. Like all cyberattacks, they not only result in massive data and financial loss, but also in:

- ▶ Damage to brand and reputation
- ▶ Erosion of customer loyalty
- ▶ Theft of intellectual property
- ▶ Loss of business
- ▶ Regulatory penalties
- ▶ Impaired security for your business or governments and states
- ▶ Increased potential for future attacks

Data theft

Data theft occurs when any data that was not intended to be shared is obtained, normally in a malicious or illegal way. Data theft increased in recent years largely because of the growing number of people and employees with access to data.

Server access

A server access attack involves a threat actor gaining unauthorized access to a victim's server, either by using stolen server credentials, a vulnerability, or other means.

Denial-of-service

Denial-of-Service (DoS) and DDoS attacks flood a system's resources, which overwhelms them and prevents responses to service requests. These attacks reduce the system's ability to perform. Often, this attack is a setup for another attack.

Malware

Malware is malicious software that can render infected systems inoperable. Most malware variants destroy data by deleting or wiping files that are critical to the operating system's ability to run.

Phishing

Phishing scams attempt to steal users' credentials or sensitive data, such as credit card numbers. In this case, scammers send users emails or text messages that are designed to look as though they are coming from a legitimate source by using fake hyperlinks.

Top infections vectors

Attack vector is a method of achieving unauthorized network access to start a cyberattack. Attack vectors allow cybercriminals to use system vulnerabilities to gain access to sensitive data, personally identifiable information, and other valuable information that is accessible after a data breach.

Driven by the heavy use of different vulnerabilities, scanning and exploiting represents the most common initial infection vector that is used by threat actors. Scan and exploit attacks generally require few resources and can be automated and scaled to target various victims, which can account for why this vector saw such a high volume in 2020.

Phishing is the second most commonly used infection vector, followed by credential theft.

Figure 1-13 shows a percentage breakdown of seven initial attack vectors that were observed by IBM Security X-Force Incident Response in 2020, according to IBM Security X-Force Report 2021.

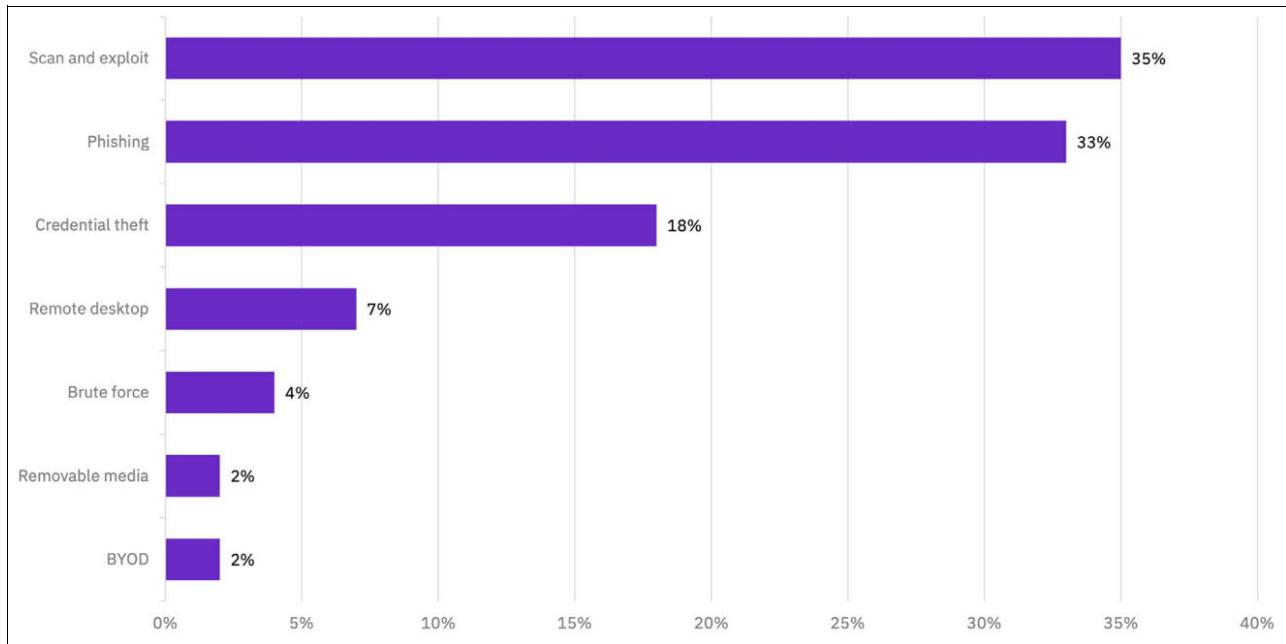


Figure 1-13 Percentage breakdown of seven initial attack vectors observed by IBM Security X-Force

1.5.2 X-Force recommendations for resilience

Based on IBM Security X-Force findings, keeping up with threat intelligence and building strong response capabilities are effective ways to help mitigate threats in the evolving landscape, regardless of in which industry or country one operates.

Table 1-3 lists the X-Force recommendations that organizations can take to better prepare for cyberthreats in 2022.

Table 1-3 Top X-Force recommendations for resilience (Source: IBM Security X-Force Report 2021)

Recommendation	Explanation	IBM Power Systems coverage
Get in front of the threat rather than react to it.	Use threat intelligence to better understand threat actor motivations and tactics to prioritize security resources.	▶ PowerSC Compliance Automation ▶ PowerSC Real Time Compliance (RTC)
Preparation is key for a response to ransomware.	Planning for a ransomware attack (including a plan that addresses blended ransomware and data theft extortion techniques) and regularly drilling this plan can make all the difference in how your organization responds in the critical moment.	

Recommendation	Explanation	IBM Power Systems coverage
Double check your organization's patch management structure.	With scanning and exploiting being the most common infection vector last year, harden your infrastructure and reinvigorate internal detections to find and stop automated exploitation attempts quickly and effectively.	<ul style="list-style-type: none"> ▶ Patch Management with Red Hat Ansible ▶ Trusted Network Connect and Patch Management ▶ PowerSC Trusted Logging ▶ PowerSC Trusted Boot ▶ PowerSC Trusted Firewall
Protect against insider threats.	Use data loss prevention (DLP) solutions, training, and monitoring to prevent inadvertent or malicious insiders from breaching your organization.	<ul style="list-style-type: none"> ▶ IBM PowerSC ▶ AIX Trusted Execution ▶ Real-time Malware Detection ▶ PowerSC Trusted Logging ▶ PowerSC Trusted Boot ▶ PowerSC Trusted Firewall
Build and train an incident response team within your organization.	If this recommendation is not a possibility, engage an effective incident response capability for prompt response to high-impact incidents.	<ul style="list-style-type: none"> ▶ PowerSC Compliance Automation ▶ PowerSC Real Time Compliance (RTC)
Stress test your organization's incident response plan to develop muscle memory.	Tabletop exercises or cyberrange experiences can provide your team with critical experience to improve reaction time, reduce downtime, and ultimately save money in the case of a breach.	PowerSC Compliance Automation
Implement multifactor authentication (MFA).	Adding layers of protection to accounts continues to be one of the most efficient security priorities for organization.	IBM PowerSC Multi-Factor Authentication on Power
Have backups, test backups, and store backups offline.	Not only ensuring the presence of backups but also their effectiveness through real-world testing makes a critical difference in the organization's security.	Secure backup or restore



IBM Power Systems and IBM Power Systems Virtual Server integrated security capabilities

This chapter describes the integrated security capabilities that are provided by IBM Power Systems and Power Virtual Server.

This chapter includes the following topics:

- ▶ 2.1, “PowerVM keystore” on page 32
- ▶ 2.2, “IBM AIX security” on page 37
- ▶ 2.3, “IBM i security” on page 47
- ▶ 2.4, “Linux security” on page 51
- ▶ 2.5, “NIST Security Content Automation Protocol SCAP” on page 60
- ▶ 2.6, “Linux Integrity Measurement Architecture” on page 65
- ▶ 2.7, “Compressed and encrypted Live Partition Mobility data” on page 67

2.1 PowerVM keystore

Starting with system firmware FW950 and HMC 9.2.950, the Platform KeyStore (PKS) feature creates an encrypted nonvolatile store. This store provides logical partitions with more capabilities to protect sensitive information.

PowerVM provides an isolated PKS storage allocation for each partition with individually managed access controls. A new set of hypervisor calls also was created to allow the partitions to access their PKS storage.

Some possible use cases of this feature include the following examples:

- ▶ Boot device encryption.
- ▶ Self-encrypting drives.
- ▶ Unlocking encrypted logical volumes without requiring a passphrase.
- ▶ Public key and certificate protection.

Secure boot public keys can be maintained by the boot loader and protected from manipulation by the kernel.

- ▶ Provide a lockable flash that is accessible during early IPL of the partition and is then locked down from further access.

Note: At the time of this writing, PKS is not available on IBM Power Virtual Server. PKS is available only on-premises as enterprise capability.

2.1.1 Platform KeyStore features

PKS includes the following features:

- ▶ AES-256 GCM encrypted KeyStore in nonvolatile flash on the service processor
Every POWER9 system generates a unique PKS root key, which is maintained and protected by PowerVM. This key is accessible to PowerVM only and cannot be extracted by a system administrator or service provider.

For more information, see 2.1.3, “Platform KeyStore Storage Protection” on page 34.

- ▶ Redundant copy of PKS maintained on the hardware management console (HMC) to support hardware failure and partition migration. For more information, see 2.1.4, “Disaster recovery” on page 35, and 2.1.5, “Migrating a partition that uses the Platform KeyStore” on page 35.
- ▶ Unique consumers are provided to support the separation of partition firmware, boot loader, and kernel. Consider the following points:
 - Each consumer maintains its own access controls.
 - Every object that is stored in PKS is associated to a consumer.
- ▶ Consumer access is controlled by way of an ephemeral password.

On every IPL of the partition, PowerVM resets all consumer passwords to a NULL or unset value. Until this password is set, access to any objects that are owned by the consumer are acquired by using a NULL password.

To protect their objects, the consumer must generate and set a password and provide that information to PKS. The consumer then uses this password for all future accesses. This behavior allows the consumer to maintain the password in protected volatile memory but the consumer is not required to persist it.

- ▶ Object access policies enable the consumer to define optional policies that must be met to allow future access to the object. These policies are enforced by PowerVM on every attempt to read, write, or remove an object in PKS. Policies include the following examples:
 - Operating system-secure boot must be enabled.
 - World readable: Object can be read by any consumer, but written or removed only by the owner.
 - Write once/immutable: After it is written, it cannot be overwritten or removed.

2.1.2 Configuring the Platform KeyStore

The PKS is configured by way of the management console. It is disabled by default when creating partitions, but can be enabled during creation or added to existing partitions. The total per partition size of PKS available can be configured 4 K - 64 K bytes in increments of 1 K.

Changes to the PKS configuration can be made after creation but consider the following limitations:

- ▶ This size of PKS can be increased to the maximum allowed while the partition is powered off, but reducing the size is not allowed.
- ▶ To disable PKS on a partition, the requested size is set to 0. This operation is blocked by PowerVM if it detects objects in storage. PKS can be disabled while the partition is running but it cannot be re-enabled.

Note: Consider the following points:

- ▶ When planning to migrate a partition with PKS enabled, see the 2.1.5, “Migrating a partition that uses the Platform KeyStore” on page 35 to complete any necessary configuration.
- ▶ FW950 supports a maximum of 1 MB of PKS storage per system, which is available to be assigned to the partitions.

For more information about configuring PKS from the management console, see the following IBM Support web pages:

- ▶ [Enabling and disabling Platform Keystore for Partitions](#)
- ▶ [Enabling Platform Keystore capability for Partitions](#)

2.1.3 Platform KeyStore Storage Protection

The PKS for each partition is stored in the nonvolatile RAM on the service processor (SP). Before storing this data on the service processor, it is encrypted by keys that are accessible to PowerVM only.

Figure 2-1 shows how PowerVM can decrypt and protect PKS.

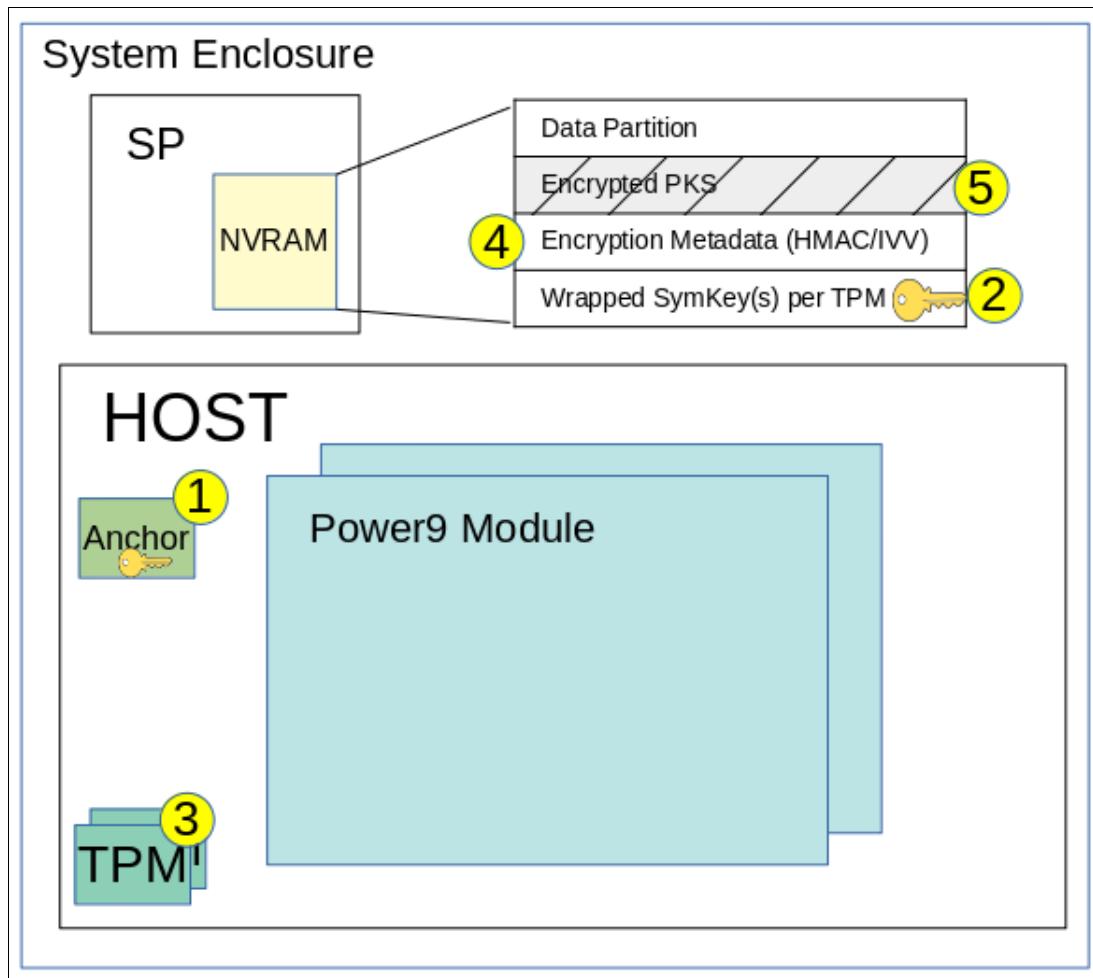


Figure 2-1 PowerVM with PKS

PowerVM accesses PKS on POWER9 systems by using the following procedure:

1. The PKS root key is read from the protected anchor card (1 in Figure 2-1).
2. The wrapped PKS root key is read from SP NVRAM (2 in Figure 2-1).
3. The Trusted Platform Modules (TPM) (3 in Figure 2-1) are used to unwrap the PKS root key.
4. PowerVM compares all copies of the PKS root key to ensure they match in all locations and restores any missing copies. For more information, see 2.1.4, “Disaster recovery” on page 35.
5. PowerVM reads the encryption metadata (4 in Figure 2-1) and the encrypted PKS (5 in Figure 2-1) from SP NVRAM.

6. PowerVM derives a unique partition AES-256 encryption key from the PKS root key and decrypts the partition's PKS by using AES-GCM mode in the POWER processor's NX accelerator unit.

PKS is now ready for the partitions to use.

7. When the partition modifies the PKS contents, PowerVM encrypts it and stores it to SP NVRAM.

Note: The encryption and storage to SP NVRAM is handled asynchronously. A separate h-call interface is provided to the partition to confirm that the object was flushed to SP NVRAM.

8. PowerVM periodically encrypts PKS storage and stores a copy on the management console. For more information, see the next section.

2.1.4 Disaster recovery

The PowerVM Platform KeyStore is resilient to hardware failure and part replacement.

The PKS root key that protect PKS is stored on multiple components throughout the platform. When PowerVM detects that a component was replaced, it restores the necessary information to the component during the next boot of the system to regain redundancy.

The partitions PKS data is encrypted and stored on the service processor. If the service processor is replaced or a Reset server firmware settings operation is performed on it, all of the PKS data is cleared. For this reason, PowerVM encrypts a copy of PKS for every partition and that backup copy is periodically stored on the management console. When the HMC detects that the service processor is cleared, it restores PKS as part of the recovery procedure.

2.1.5 Migrating a partition that uses the Platform KeyStore

PowerVM supports automatic encrypted migration of the PKS.

Note: If PKS was enabled for a partition, the management console blocks migration of that partition to a target system that does not support PKS. If nothing was stored in PKS, PKS can be disabled for the partition by setting the PKS size to 0 on the management console. If PowerVM determines that PKS is empty, it disables PKS and the migration can be reattempted; however, if PKS is not empty, the resize operation is blocked.

Migration by way of the active Live Partition Mobility

PowerVM introduced encryption of all data during LPM. For information, see this [IBM Power Community web page](#). PowerVM uses the same LPM encryption technique to transfer PKS from the source to the target destination.

Migration by way of Simplified Remote Restart or Inactive LPM

To support Simplified Remote Restart (SRR) of PKS or Inactive LPM, you must set up a matching trusted system key on the source *and* target system. The trusted system key is used by PowerVM to generate encryption keys to encrypt the backup copy of PKS that is off-loaded to the HMC. This backup copy is used by the management console to migrate PKS to the target system during the SRR procedure.

Warning: The trusted system key must be set up on both systems in advance to ensure that a successful SRR can be performed, even if the source system is unavailable.

For more information about how to change the trusted system key, see the following IBM Documentation web pages:

- ▶ [Changing the trusted system key](#)
- ▶ [Listing the trusted system key](#)

Securely erasing the Platform KeyStore

The ASMI Secure Storage Policy menu is provided to clear sensitive data from the system for the following tasks:

- ▶ Return the system to IBM Global Asset Recovery Services (GARS)
- ▶ Resale the system

You must clear sensitive data when changes occur in the customer workloads, such as moving a system from a development environment to production environment, and vice versa.

This procedure requires physical access to the system to authorize the operation. This access ensures it cannot be used to remotely perform a DoS attack.

Warning: Performing this procedure destroys any data that is maintained by the PKS for all partitions on the system with no way to recover. Any partitions to be maintained *must* be migrated off the system before proceeding.

Complete the following steps to securely erase the PKS:

1. Migrate all partitions to be kept to another system and delete the partitions that are not to be maintained.
2. Power off the system if necessary.
3. Perform a Clear All operation to clear and generate a PKS root key.
4. After completing step 3, power off the system.
5. Perform a Reset server firmware to wipe all encrypted PKS data from SP NVRAM.

Now, all persistent data that is maintained by the server firmware in the platform is cleared.

2.2 IBM AIX security

The AIX operating system allows you to perform tasks, such as hardening a system, changing permissions, setting up authentication methods, and configuring the Common Criteria Security Evaluation features.

Securing the base operating system provides information about how to protect the system regardless of network connectivity.

2.2.1 Trusted Computing Base

The system administrator must determine how much trust can be given to a specific program. This determination includes considering the value of the information resources on the system in deciding how much trust is required for a program to be installed with privilege.

The Trusted Computing Base (TCB) is the part of the system that is responsible for enforcing system-wide information security policies. By installing and using the TCB, you can define user access to the trusted communication path, which permits secure communication between users and the TCB.

TCB features can be enabled only when the operating system is installed. To install TCB on an installed machine, you must perform a Preservation installation. Enabling TCB permits you to access the trusted shell, trusted processes, and the Secure Attention Key (SAK).

For more information, see this [IBM Documentation web page](#).

2.2.2 AIX Secure Boot

The AIX Secure boot feature is used to verify the authenticity of the boot process.

You can use the secure boot technology to verify the integrity of PowerVM firmware, including hostboot, POWER Hypervisor (PHYP), and partition firmware (PFW) through digital signature in POWER9 systems, or later, and PowerVM systems. The firmware that runs on the POWER9 processor can be trusted when you use the firmware-secure boot feature.

The AIX Secure boot feature extends the chain of trust to the AIX logical partition (LPAR) by digitally verifying the following AIX and PFW codes:

- ▶ Operating system boot loader
- ▶ Kernel
- ▶ Runtime environment
- ▶ Device drivers, including boot device drivers
- ▶ Kernel extensions
- ▶ Applications
- ▶ Libraries

The AIX Secure boot feature includes the following enhancements:

- ▶ The AIX Secure boot feature starts validating code integrity before the Trusted Execution (TE) feature. When The AIX Secure boot feature is enabled, the TSD is loaded earlier in the boot process. The TSD is loaded before the kernel loads the first application.
- ▶ The AIX Secure boot feature verifies the digital signatures of the codes that must be run. At run time, the TE feature verifies the cryptographic hashes of the boot and initialization codes.

To list the secure boot policy from the LPAR, run the command that is shown in Example 2-1.

Example 2-1 Listing the secure boot policy from the LPAR

```
$ lsattr -E -l sys0 -a secure_boot
```

In IBM Cloud, **secure_boot** is turned off by default.

2.2.3 AIX Trusted Execution

The AIX security feature of the TE environment protects the installed components and software applications.

TE refers to a collection of features that are used to verify the integrity of the system and implement advance security policies, which together can be used to enhance the trust level of the complete system.

This security feature is achieved by maintaining and validating integrity of each component of the system and installed supported applications. The kernel trusts and starts only those objects that the kernel can validate the integrity successfully.

Any untrusted object is denied permission to run.

The TE feature of AIX protects the system against malware that might gain access to the system and infect legitimate system or application components. Such access causes unauthorized execution of the malware code along with the legitimate application.

Security Profile Evaluation Assurance Level 4+ is required and labeled AIX Security and Evaluation Assurance Level 4+.

System administrators can install a system with the Base AIX Security (BAS) and Evaluation Assurance Level 4+ (EAL4+) option or Labeled AIX Security (LAS) and Evaluation Assurance Level 4+ (EAL4+) during a base operating system (BOS) installation. A system with these options includes restrictions on the software that is installed during BOS installation, plus network access is restricted.

TE replaces Trusted Computing Base (TCB) with a superior capability. The database for TE is called *Trusted Signature Database* (TSD) and is in the /etc/securitytsd/tsd.dat file.

According to the TE security architecture, a *trusted file* is a file that is critical from the security perspective of the system. If compromised, this file can jeopardize the security of the entire system. Typically, the following files match this description:

- ▶ Kernel (operating system)
- ▶ All setuid root programs
- ▶ All setgid root programs
- ▶ Any program that is exclusively run by the root user or by a member of the system group
- ▶ Any program that must be run by the administrator while on the trusted communication path (for example, the **ls** command)
- ▶ The configuration files that control system operation
- ▶ Any program that is run with the privilege or access rights to alter the kernel or the system configuration files

A file can be marked as trusted by adding its definition in the TSD by using the **trustchk** command. The **trustchk** command can be used to add, delete, or list entries from the TSD.

To enable TSD protection, run the commands as shown in Example 2-2.

Example 2-2 Enabling TSD

```
$ .trustchk -p tsd_lock=on  
$ trustchk -p te=on
```

Perform a system check comparison with the TSD and report errors as shown in Example 2-3.

Example 2-3 Checking comparison with the TSD

```
$ .trustchk -n ALL
```

For more information about Trusted Execution support, see this [IBM Support web page](#).

2.2.4 AIX Security Expert

AIX Security Expert provides a center for all security settings (TCP, NET, IPSEC, system, and auditing).

AIX Security Expert is a system security hardening tool. It is part of the `bos.aixpert` file set. AIX Security Expert provides simple menu settings for high-level security, medium-level security, low-level security, and AIX Standard Settings security that integrate over 300 security configuration settings while still providing control over each security element for advanced administrators.

AIX Security Expert can be used to implement the suitable level of security without the necessity of reading many papers about security hardening and then, individually implementing each security element.

AIX Security Expert can be used to take a security configuration snapshot. This snapshot can be used to set up the same security configuration on other systems. This feature saves time and ensures that all systems include the correct security configuration in an enterprise environment.

AIX Security Expert can be run from SMIT, or you can use the **aixpert** command.

The AIX Security Expert view of security levels is derived in part from the National Institute of Standards and Technology document [Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers](#).

However, high-, medium-, and low-level security mean different things to different users. It is important to understand the environment in which your system operates. If you chose a security level that is too high, you can lock yourself out of your computer. If you chose a security level that is too low, your computer might be vulnerable to a cyberattack.

AIX Security Expert settings

The following coarse-grain security settings are available (see Table 2-1):

- ▶ High-level security
- ▶ Medium-level security
- ▶ Low-level security
- ▶ Advanced security

- ▶ Custom user-specified security
- ▶ AIX standard settings
- ▶ Undo security
- ▶ Check security

Table 2-1 AIX Security Expert level security scenario

Level	Scenarios
High	Collocating system with an Internet service provider. The system might be connected directly to the internet, runs as an HTTP server, contains sensitive user data, and must be administered remotely by the customer.
Medium	System might be connected to the corporate network, which is behind the corporate firewall. The network is secure and well-administered. The system might be used by many users who might need access to the system telnet and FTP.
Low	The customer is administering a system for some time. The system might be on an isolated secure local network. The system might be used for various people and services.

Examples

To write all of the high-level security options to an output file, use the command as shown in Example 2-4.

Example 2-4 Writing security options to output file

```
$ aixpert -l high -n -o /etc/security/aixpert/plugin/redbookYS.xml
```

After completing this command, the output file can be edited, and specific security roles can be commented out by enclosing them in the standard XML comment string (<-- begins the comment and -\> closes the comment).

To apply the security settings from a configuration file, use the command as shown in Example 2-5.

Example 2-5 Applying security settings

```
$ aixpert -f /etc/security/aixpert/plugin/redbookYS.xml
```

To check the security settings that were applied to the system and to log the rules that failed into the audit subsystem, use the command as shown in Example 2-6.

Example 2-6 Checking security settings

```
$ aixpert -c -p
```

2.2.5 Role-based access control

System administration is an important aspect of daily operations, and security is an inherent part of most system administration functions. In addition to securing the operating environment, it is necessary to closely monitor daily system activities.

Applications that require administrative privileges for specific operations include new integration options with the enhanced AIX role-based access control (RBAC) infrastructure.

These integration options center on the use of granular privileges and authorizations and the ability to configure any command on the system as a privileged command. Features of the enhanced RBAC mode are installed and enabled by default on all installations of AIX 7.2.

The enhanced RBAC mode provides a configurable set of authorizations, roles, privileged commands, devices, and files through the following RBAC databases. With enhanced RBAC, the databases can be in the local file system or can be managed remotely through LDAP:

- ▶ Authorization database
- ▶ Role database
- ▶ Privileged command database
- ▶ Privileged device database
- ▶ Privileged file database

Configuring the RBAC mode

The RBAC mode is controlled by a system-wide configuration variable in the kernel. This variable specifies whether Enhanced RBAC mode is enabled or disabled.

Enhanced RBAC mode is enabled by default. Run the command on the system to retrieve the current RBAC mode as shown in Example 2-7.

Example 2-7 Retrieving current RBAC

```
$ lsattr -E -l sys0 -a enhanced_RBAC
```

2.2.6 Encrypted file system

The encrypted file system enables individual users on the system to encrypt their data on J2 file systems through their individual keystores.

A key is associated to each user. These keys are stored in a cryptographically protected keystore. Upon successful login, the user's keys are loaded into the kernel and associated with the processes credentials.

Later on when the process must open an EFS-protected file, these credentials are tested. If a key that matches the file protection is found, the process can decrypt the file key and then, the file content.

For more information, see 3.3, “Data in transit and at rest protection with IBM Security Guardium” on page 76.

2.2.7 OpenSSH and Kerberos 5 support

Kerberos is an authentication mechanism that provides a secure means of authentication for network users. It prevents the transmission of clear text passwords over the network by encrypting authentication messages between clients and servers. In addition, Kerberos provides a system for authorization in the form of administering tokens or credentials.

OpenSSH version 3.8 and later supports Kerberos 5 authentication and authorization through NAS Version 1.4.

For more information, see [AIX 7.2 Security Guide](#).

2.2.8 Private boot with Network Installation Manager

Network Installation Manager (NIM) helps perform the following tasks, among other examples:

- ▶ Configure the NIM master server
- ▶ Manage NIM objects
- ▶ Perform various operations on NIM clients (such as software or base operating system installation)
- ▶ Update SP or TL by using NIM resources
- ▶ Rebooting

For more information about setting up NIM and secure boot operations on AIX LPARs, see [this web page](#).

2.2.9 Login control

Potential hackers can use the initial login window to obtain valuable information from the environment. System administrators can control and set up login control in the /etc/security/login.cfg file.

For more information, see this [IBM Documentation web page](#).

2.2.10 Stack execution disable protection

An increasing likelihood of computer systems falling prey to sophisticated attacks exists, which disrupts the daily operations of businesses and government agencies. Although no security measure can provide foolproof protection against attacks, you must deploy multiple security mechanisms to thwart security attacks.

This section discusses a security mechanism that is used with AIX to thwart attacks because of buffer overflow based execution.

Security breaches occur in many forms, but one of the most common methods is to monitor the system-provided administrative tools and then, look for and use buffer overflows. Buffer overflow attacks occur when an internal program buffer is overwritten because data was not suitably validated (such as command line, environmental variable, disk, or terminal I/O). Attack code is inserted into a running process through the buffer overflow, which changes the execution path of the running process.

Stack execution disable (SED) mode is implemented by using the `sedmgr` command. This command permits control of the system SED mode of operation, and sets the executable file based SED flags.

By default, `sedmgr` is set to monitor a select set of processes, as shown in Example 2-8.

Example 2-8 Using sedmgr

```
$ sedmgr
Stack Execution Disable (SED) mode: select
SED configured in kernel: select
```

Example 2-9 shows how to turn on SED by using the **sedmgr** command.

Example 2-9 Turning on SED by using sedmgr command

```
$ sedmgr -m all  
System wide SED has been set successfully. It is effective at 64 bit kernel boot time.
```

For more information, see this [IBM Documentation web page](#).

2.2.11 Managing X11 and CDE concerns

Potential security vulnerabilities exist with the X11 X server and the Common Desktop Environment (CDE).

For more information about removing and disabling CDE, see this [IBM Support web page](#).

2.2.12 List of setuid and setgid programs

Various setuid and setgid programs are available on an AIX system. You can remove these privileges on commands that do not need to be available to regular users.

Basic permissions in AIX are used to limit access to files and directories. Three basic operations are on files that are limited by permissions: read(r), write(w), and execute(x).

A sample **ls -l** output of a file that is called libsearch shows the permissions at the beginning of the line (see Example 2-10).

Example 2-10 ls -l output

```
-rwxr-xrw- 3 larry staff 102 Nov 3 2021 libsearch
```

More basic permission characters can appear in the **ls -l** output, as shown in Example 2-11.

Example 2-11 Output of the ls -l command

```
-r-sr-sr-x 3 root security 1077 Nov 21 11:17 /usr/bin/runme
```

Notice the s characters where the x characters normally appear. These s characters are called the SETUID (or SUID) and SETGID (or SGID) bits. The SETUID s character that appears in the user section of the permissions means that when this file is run, is run as though the user owner had run it.

For example, user larry ran this /usr/bin/runme file, it is run as though the owner of the file ran it (in this case, it is run as root). This process is referred to as running the file with root privileges or root authority.

Caution must be taken when setting a script as SETUID root because root authority can do almost anything on the system. A poorly written or malicious script can detrimentally affect a system when it is run with root authority.

SETUID set on a directory has no function in AIX.

For more information about file and directory permissions, see this [IBM Support web page](#).

2.2.13 AIX trusted installation and update

Starting with IBM AIX 7.2 with Technology Level 4, the software packages that are delivered in the `installp` format are digitally signed. The digital signatures of the associated software package are stored in a database that is called the Digital Signature Catalog (DSC). These digital signatures are distributed by using the ODM entries of the new `dsc_inventory` class.

For more information, see this [IBM Documentation web page](#).

The following types of AIX operating system images can be used for AIX LPAR provisioning:

- ▶ Image types that are provided by IBM Cloud and made available in IBM Catalog

The AIX LPAR is configured with an SSH key and the root password is not set. You must connect to the AIX VM by using SSH key and set the root password for the system as required. If you have network access to the AIX VM, you can use telnet from an on-premises system and set the root password.

For more information about creating SSH keys and connecting to AIX LPAR, see this [IBM Cloud Docs web page](#).

- ▶ Image types that are brought in as part of a workload migration to IBM Cloud

For the AIX images that are imported to IBM Cloud as part of migration, AIX includes security that is set up that was used for on-premises environments. It is possible to set up a Network Install Manager (NIM) in IBM Cloud to import these AIX images from on-premises.

For more information, see this [IBM Cloud Docs web page](#).

Aside from setting up a NIM server in IBM Cloud for importing AIX images from on-premises, it is also possible to import images to IBM Cloud Object Storage (ICOS). The AIX LPAR can be provisioned by those imported images.

For more information, see this [IBM Cloud Docs web page](#).

2.2.14 Network security

As best practice, install and configure IP Security, identify necessary and unnecessary network services, and audit and monitor network security.

For more information about the following services, see [AIX 7.2 Security Guide](#):

- ▶ TCP/IP security
- ▶ Network services
- ▶ Internet protocol security
- ▶ Network File System security
- ▶ Enterprise identity mapping
- ▶ Kerberos
- ▶ Remote authentication dial-in user service server
- ▶ AIX intrusion prevention

2.2.15 Network security for IBM Power Systems Virtual Server

Infrastructure provides virtual LAN (VLAN) isolation between different tenants, which are enforced at the Virtual I/O Server (VIOS) and at the physical switches and routers.

The Power Systems Virtual Server network security architecture relies on a set of fixed firewall ports open on the Juniper vSRX firewalls:

- ▶ 22 (SSH)
- ▶ 443 (HTTPS)
- ▶ 992 (IBM i5250 emulation)
- ▶ ICMP traffic

If you need extra ports to be opened, you can consider the customer-specific firewall option that is available by using an IBM Cloud firewall, such as Vyatta, Juniper vSRX, or FortiGate, and by connecting to Power Systems Virtual Server by using Direct Link Connect.

For more information about the Power Systems Virtual Server connection methods, see this [IBM Cloud Docs web page](#).

2.2.16 Backing up and restoring encryption

For more information about encrypting a file system on AIX see 3.3, “Data in transit and at rest protection with IBM Security Guardium” on page 76.

AIX JFS2 encrypted file system backup

Use AIX JFS2 Encrypted File System (EFS) to back up files in clear text or raw format. With clear text format, the file is decrypted by EFS as it is read. With raw format, the data is not decrypted. The default is raw format; however, when you set the efsdecrypt option to Yes, you receive clear text backups.

Whenever you run a backup that includes any files that are encrypted on an EFS, you must ensure that you use the correct specification of the efsdecrypt option. If the efsdecrypt option value changes between two incremental backups, all encrypted files on EFS file systems are backed up again, even if they were not changed since the last backup.

For example, if you are running an incremental backup of encrypted files that were backed up as raw, ensure that efsdecrypt is specified as No. If you change efsdecrypt to Yes, all of the files are backed up again in clear text, even if they are unchanged. Therefore, ensure that you use this option carefully.

Restoring AIX encrypted files

When files are backed up in raw format from an AIX JFS2 EFS, you can restore them only to the same or another JFS2 EFS. They cannot be restored to any different file system, or on a different platform.

When EFS files are backed up in clear text, you can restore them anywhere. If you restore them to a JFS2 EFS, they are automatically re-encrypted only if the directory to which they are restored has the AIX EFS inheritance option set.

After restoring a file that was backed up in raw format, you might find that the file cannot be decrypted. The encryption key that was originally used for the file might no longer be available in the keystore of the user. In this case, you must restore the keystore that was used at the time of backup.

Data encryption backup or archive operations with IBM Spectrum Protect 8.1

The way to ensure data security is by encrypting data. Use data encryption to protect data during a backup or archive operation. Advanced Encryption Standard (AES) 128-bit encryption is the default encryption option. For the highest level of data encryption, use 256-bit Advanced Encryption Standard (AES) data encryption by specifying the `encryptiontype` option.

The data that you include is stored in encrypted form, and encryption does not affect the amount of data that is sent or received.

The `include.encrypt` option is the only way to enable encryption on the backup-archive client. Encryption cannot occur if no `include.encrypt` statements are used.

Use the `include` and `exclude` options in `dsm.sys` to define which files to include or exclude from incremental or selective backup processing. A file is eligible for backup unless it is excluded by an `exclude` option. It is not necessary to use an `include` option to include specific files for backup unless those files are in a directory that contains other files that you want to exclude.

To encrypt file data, you must select an encryption key password, which the client uses to generate the encryption key for encrypting and decrypting the file data. Store the encryption key password for later use. You can specify whether to save the encryption key password in a file that is named `TSM.sth` by using the `encryptkey` option.

IBM Spectrum® Protect client encryption allows you to enter a value of up to 63 characters. This encryption password must be confirmed when encrypting the file for backup. It also must be entered when performing restores of encrypted files.

While restoring the encrypted file, the client prompts you for the key password to decrypt the file in the following cases:

- ▶ The `encryptkey` option is set to `Prompt`.
- ▶ The key that is supplied by the user in the previous case does not match.
- ▶ The `encryptkey` option is set to `Save` and the locally saved key password does not match the encrypted file.

2.3 IBM i security

The rising frequency of high-profile data breaches and the concomitant growth in new and extended regulatory compliance requirements, is putting great pressure on IT teams to reassure their corporate executives that mission-critical systems and data are secure.

Cyberthreats grow more sophisticated every year, raising the importance of proper security controls. A deeper understanding of the risks and the security controls built into the operating system is driving a wave of interest in prioritizing cybersecurity issues on IBM i.

IBM is an industry leader in IT infrastructure security. In the current IT threat landscape, all enterprises need to take steps to protect their vital systems from attacks, insider threats, and malware. IBM Zero Trust framework is a business-first approach that encourages clients to modernize their security procedures and adapt to new risks from changing business environments.

For more information, see this [IBM Power Community web page](#).

2.3.1 Introduction to IBM i Security

Improving confidence in companies' IT security posture requires a deep understanding of all potential vulnerabilities and the most effective best practices and technologies to minimize the possibility of a breach.

Best practices and technology can be grouped in many categories, including the following examples:

- ▶ Physical devices
- ▶ Networks
- ▶ IBM i OS setup
- ▶ System access
- ▶ Data protection at the file and field level
- ▶ System monitoring and auditing
- ▶ Application code source
- ▶ Databases

Because one category can overlap with others to provide numerous lines of defense, it is especially beneficial to think of these security categories as layers.

Figure 2-2 shows IBM i Security layers.

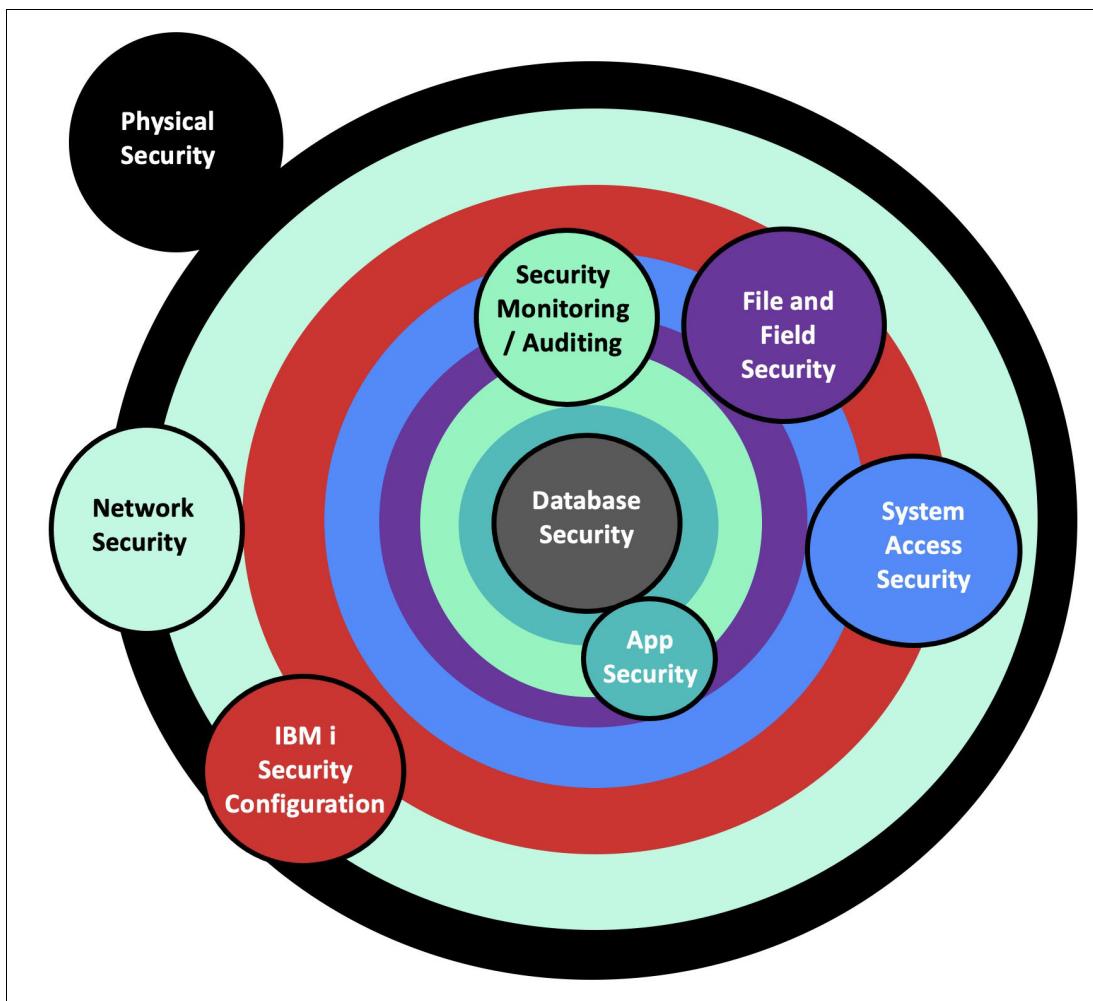


Figure 2-2 IBM i Security Layers

Physical protection

A comprehensive physical security plan requires (among other things) that computing equipment be safeguarded against theft, misuse, and purposeful or accidental tampering, in addition to managing access to computer rooms and data centers.

Network security

The networks to which an IBM i is connected must be rigorously protected. If any of these networks are connected to the internet, more vigilance is required because internet-connected networks often see thousands of bots, sniffers, and hackers that are attempting access daily.

IBM i security configuration

The correct configuration of the IBM i OS and related resources and maintaining operating system versions and PTFs up to date are essential as IBM i security best practices. This process includes the following components:

- ▶ System values settings (QSecurity System Value, QALWOBJRST, QFRCCVNRST, and so on)
- ▶ IBM i server-configuration settings (FTP, Telnet, and so on)
- ▶ Controlling access to System Service Tools
- ▶ User authority settings
- ▶ Staying current on operating system releases and PTFs

Security of system access

This layer of protection's tactics and technologies keep unauthorized users out of IBM i environments while retaining tight control over what authorized users can do after they are signed in. Controlling IBM i system access requires the use of the following tactics and technologies:

- ▶ Password management
- ▶ Multi-factor authentication
- ▶ Network-access control
- ▶ Command control

Security of files and fields

Numerous regulations mandate that firms in various industries safeguard personally identifiable information (PII), personal health information (PHI), personal credit card information, and other sensitive data if a data breach occurs.

Protecting files and data on the IBM i requires the use of the following tactics and technologies:

- ▶ Object-level authority management
- ▶ Encryption
- ▶ Tokenization of field data
- ▶ Anonymization

Security monitoring and auditing

Although the preceding security layers focus on prevention, this layer focuses on creating functions for log security-related events for tracking, documentation, and automatically informing administrators and security officials whenever suspicious activity is identified.

Application security scanning

Application security testing is the practice of finding security flaws and vulnerabilities in source code to make applications more resistant to security attacks.

You can use information that is gathered by third-party or IBM tools to run code and inspect it in real time, looking for faults that can be security flaws. These faults can include issues with:

- ▶ Query strings
- ▶ Requests and answers
- ▶ Scripts
- ▶ Memory leakage
- ▶ Cookie and session handling
- ▶ Authentication
- ▶ Execution of third-party components
- ▶ Data injection

Database monitoring and compliance

You can use tools to monitor and report on any database access on IBM i. This access includes any programs (such as RPG) that use native database I/O operations or SQL access.

You can use information that is gathered by tools (such as IBM Guardium) to create activity reports, help you meet auditing requirements, and generate alerts of unauthorized activity. Detailed auditing information includes the following examples:

- ▶ Session start and end times
- ▶ TCP/IP address and port
- ▶ Object names (for example, tables or views)
- ▶ Users
- ▶ SQLSTATEs
- ▶ Job and Job numbers
- ▶ SQL statements and variables
- ▶ Client special register values
- ▶ Interface information, such as ODBC, Toolbox, JDBC, Native JDBC, and .NET

IBM i Security Lab Services experts can help your team strengthen your IBM i security levels in various ways, including the following examples:

- ▶ Conduct in-depth risk assessments on your IBM i environments regularly.
- ▶ Provide managed-security services, which provides a dedicated IBM i security experts who, depending on the level of service that is selected, checks security configurations regularly, delivers status reports, monitors systems for security events 24 hours a day, adjusts security configurations, and more.
- ▶ Generate reports that are requested by auditors to assist the system team during compliance or security audits.

2.3.2 IBM i security assessments

To develop a suitable baseline, the IBM i Security Assessment (which is provided by IBM i Security Lab Services) scans IBM i LPARs for range of security settings and risks.

The review of the core operating system, settings, user profiles, and permissions include¹ the following tasks:

- ▶ Investigate privileged user profiles, command-line access, and other significant aspects of the user profiles on the system.
- ▶ Investigate password practices.
- ▶ Investigate the use of Group Profiles and Authorization Lists.
- ▶ Analyze the use of adopted authority and profile swapping.
- ▶ Examine:
 - Communications and TCP/IP exposures (Open Ports and Exit Points)
 - System value settings
 - System Service Tools (SST) security settings
 - Subsystem descriptions, job descriptions, output queues, and job queues
 - Security PTF levels and determine whether the customer is within those levels

¹ <https://www.ibm.com/support/pages/ibm-i-security#assessments>

- IBM i auditing and logging practices that are used by CUSTOMER and provide recommendations for improvement if determined to be insufficient
- ▶ Analyze access control for:
 - Library system objects
 - IFS directories
- ▶ Analyze file shares for ransomware exposure.
- ▶ Document the findings and recommendations for securing the system that are based on findings.
- ▶ Review user, programmer, and administrator access to data from applications.
- ▶ Recommend application security design or changes to meet security requirements.
- ▶ Provide recommendations on suitable development security best practices.

Note: Because security is a constantly changing area, IBM recommends that you conduct an annual IBM i Security Assessment to best understand the risks in your setup and configuration.

For more information, see this [IBM i Security web page](#).

2.4 Linux security

Although safeguarding Linux servers can appear to be a headache, a definite silver lining exists: it provides another level of management. Furthermore, server security is not always difficult to attain.

This section discusses a few fundamental Linux hardening and Linux server security recommended practices that can make all the difference.

2.4.1 Security best practices for Linux

Many of the security concerns you might have with Linux servers exist because such servers are not hardened ready for use. Instead, it is the user's responsibility to set up mechanisms that alert them to suspect activity. Linux servers can be startlingly susceptible if you do not make an extra effort to hardened them.

Use strong and unique passwords

Any safe server is built on the foundation of strong passwords. If possible, these passwords must be at least 10 characters, with criteria for special characters and upper and lowercase letters. *Never* use the same password for many users or software platforms. Remember to set an expiration date because no password can ensure suitable protection eternally.

Several password managers are available for the Linux platform. Many of these managers offer crucial features, such as the following examples:

- ▶ Two-factor authentication (see 4.6, “PowerSC MFA example configuration” on page 137)
- ▶ Password generators
- ▶ Cloud password storage

Generate an SSH key pair

Although strong passwords can help, other methods are available to log in to private servers that are considerably more secure. Secure Shell (SSH) key pairs are especially recommended for deployment because they make brute force hacking significantly more difficult.

To set up an SSH key, enter the command in the CLI, that is shown in Example 2-12.

Example 2-12 Setting up SSH Key

```
$ ssh-keygen -t rsa
```

You can choose where you want to save the key (as shown in Example 2-13) or press **Enter** to save it in the default location.

Example 2-13 Choosing save key location

```
$ Enter file in which to save the key (/home/youruser/.ssh/id_rsa):
```

Update your software regularly

Implementing regular software patches to address emerging vulnerabilities is an important part of properly managing your Linux server security. Software can become exploitable if it is not updated regularly, which makes it easy for hackers to gain access.

Example 2-14 shows how to update your software by way of the command line.

Example 2-14 Updating software by using yum

```
$ yum update
```

Avoid unnecessary software

Although it is enticing to adopt new software, not all online services are genuinely necessary. Each extra program increases the chances of your server becoming vulnerable to future problems.

Use a Red Hat Package Manager (RPM) to review recently downloaded packages if your server hosts much software. Next, you can remove any unwanted applications. Use the command as shown in Example 2-15 to install the package.

Example 2-15 Using rpm to remove unnecessary packages

```
$ rpm -ivh {rpm-file}
```

Close hidden open ports

While widening attack surfaces, open ports can provide network architecture information. As a result, ports that are not necessary must be closed as soon as possible. The **netstat** command can be used to determine which ports are listening and the specific information about any active connections.

Example 2-16 shows the command lines that can be used to find specific ports.

Example 2-16 Using netstat command to list listening ports

```
All TCP ports - $ netstat -at  
All UDP ports - $ netstat -au  
All listening ports - $ netstat -l  
Information for all ports - $ netstat -s
```

Scan log files

Brute force attacks on Linux systems are alarmingly widespread. However, they often succeed not because the malicious parties are exceptionally skilled or cunning, but because no preventive measures are in place beyond marginally better password security.

Consider the use of the intrusion prevention program Fail2ban as a next-level solution for combating brute force attacks. This system modifies firewall rules to prevent any address from attempting to log in more than a specific number of times. It can be used to identify and address trends of authentication failure.

Use the command in Example 2-17 to install Fail2ban.

Example 2-17 Installing Fail2ban by using yum

```
$ yum install fail2ban
```

Perform security audits

Although the tips that are discussed here can help you feel more secure while you work to strengthen the security of your Linux server, new threats are always lurking around the corner.

If not updated regularly, even the most secure server becomes vulnerable to new threats. Although software upgrades are essential, security audits can reveal other improvements that are worthwhile.

For more information about performing security and compliance audits, see the following sections:

- ▶ 2.5, “NIST Security Content Automation Protocol SCAP” on page 60
- ▶ 2.6, “Linux Integrity Measurement Architecture” on page 65
- ▶ 4.4, “PowerSC for Linux” on page 125

2.4.2 OpenSSL enhancements

OpenSSL is a library that provides cryptographic protocols to applications. The `openssl` command-line utility enables the use of the cryptographic functions from the shell. It also includes an interactive mode.

The `openssh` packages were upgraded to upstream version 8 with the following new enhancements:

- ▶ Increased default RSA key size to 3072 bits for the `ssh-keygen` tool.
- ▶ Removed support for the `ShowPatchLevel` configuration option.
- ▶ Applied numerous GSSAPI key exchange code fixes, such as the fix of Kerberos cleanup procedures.
- ▶ Removed fall back to the `sshd_net_t` SELinux context.
- ▶ Added support for Match final blocks.
- ▶ Fixed minor issues in the `ssh-copy-id` command.
- ▶ Fixed Common Vulnerabilities and Exposures (CVE) that are related to the `scp` utility (CVE-2019-6111, CVE-2018-20685, and CVE-2019-6109).

For more information, see this [Red Hat Documentation web page](#).

2.4.3 Blocking and allowing applications by using fapolicyd

Setting and enforcing a policy that allows or denies application execution based on a rule set efficiently prevents the execution of unknown and potentially malicious software.

The `fapolicyd` software framework controls the execution of applications based on a user-defined policy. This method is one of the most efficient ways to prevent running untrusted and possibly malicious applications on the system.

The `fapolicyd` framework provides the following components:

- ▶ Service
- ▶ Command-line utilities
- ▶ RPM plug-in
- ▶ Rule language

The administrator can define the allow and deny execution rules for any application with the possibility of auditing that is based on a path, hash, MIME type, or trust.

The `fapolicyd` service configuration is in the `/etc/fapolicyd/` directory with the following structure:

- ▶ The `fapolicyd.rules` file features allow and deny execution rules.
- ▶ The `fapolicyd.conf` file features the daemon's configuration options. This file is useful primarily for performance-tuning purposes.

Deploying fapolicyd

Complete the following steps to deploy the fapolicyd framework in Red Hat Enterprise Linux:

1. Install the fapolicyd package, as shown in Example 2-18.

Example 2-18 Installing fapolicyd using yum

```
$ yum install fapolicyd
```

2. Enable and start the fapolicyd service, as shown in Example 2-19.

Example 2-19 Enabling fapolicyd

```
$ systemctl enable --now fapolicyd
```

3. Verify that the fapolicyd service is running correctly, as shown in Example 2-20.

Example 2-20 Verifying status

```
$ systemctl status fapolicyd
fapolicyd.service - File Access Policy Daemon
   Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor
preset: disabled)
     Active: active (running) since Fri 2021-11-05 06:26:27 +08; 25s ago
       Process: 266903 ExecStart=/usr/sbin/fapolicyd (code=exited, status=0/SUCCESS)
     Main PID: 266904 (fapolicyd)
        Tasks: 4 (limit: 21962)
      Memory: 87.8M
         CGroup: /system.slice/fapolicyd.service
                  └─·266904 /usr/sbin/fapolicyd

Nov 05 06:26:27 psc-rh fapolicyd[266904]: Loading rpmbdb backend
Nov 05 06:26:28 psc-rh fapolicyd[266904]: No SHA256 for /etc/init.d/psad
Nov 05 06:26:28 psc-rh fapolicyd[266904]: No SHA256 for /etc/psad/auto_d1
Nov 05 06:26:28 psc-rh fapolicyd[266904]: No SHA256 for /etc/psad/icmp6_types
Nov 05 06:26:28 psc-rh fapolicyd[266904]: No SHA256 for /etc/psad/icmp_types
Nov 05 06:26:28 psc-rh fapolicyd[266904]: No SHA256 for /etc/psad/ip_options
Nov 05 06:26:29 psc-rh fapolicyd[266904]: Creating database
Nov 05 06:26:29 psc-rh fapolicyd[266904]: Loading data from rpmbdb backend
Nov 05 06:26:29 psc-rh fapolicyd[266904]: Loading data from file backend
Nov 05 06:26:29 psc-rh fapolicyd[266904]: Starting to listen for events
```

4. Log in as a user without root privileges, and check that fapolicyd is working, as shown in Example 2-21.

Example 2-21 Verifying that fapolicyd is working

```
$ cp /bin/ls /tmp
$ /tmp/ls
bash: /tmp/ls: Operation not permitted
```

2.4.4 Operating system boot security improvements

Systems can be easily configured to boot a compromised operating system kernel if no measures are taken to ensure the kernels' integrity. The following firmware features are used to improve the security of booting nonvirtualized operating systems on OpenPOWER hardware:

- ▶ Secure boot (or verified boot) checks that operating system kernels are valid before allowing them to boot. Operating system providers supply operating system kernels that they sign cryptographically.

When system administrators install operating system kernels, they also install corresponding kernel verification keys into protected system flash storage.

Before the bootloader boots a selected kernel, it uses the one of the verification keys to check the kernel against the original kernel signature. The bootloader boots the kernel only if the check succeeds, which prevents unvetted kernels or modified kernel images from booting.

- ▶ Trusted boot securely stores a cryptographic hash of a kernel image before it boots, which provides an indelible record of precisely which kernel booted for future assessment. The bootloader takes a cryptographic hash of the kernel image, records it in an event log, and uses it to update the state of a register in the Trusted Platform Module (TPM) that is called a Platform Configuration Register.

A prominent use case for trusted boot is called *remote attestation*. After a system boots, a second system can check which kernel booted on the first system by requesting its event log and TPM-signed Platform Configuration Register set. The second system can then use this data to appraise the first system's state before it continues interacting.

2.4.5 Cybersecurity profiles available with PowerSC GUI

IBM PowerSC is a suite of cybersecurity tools for IBM Power Systems. Several tools are available in this suite.

The PowerSC graphical user interface (GUI) tool uses a web browser-based interface that provides centralized security configuration, management, monitoring, and reporting information. It provides the ability to deploy a security profile, which consists of a set of operating system security settings, to multiple systems from the web browser-based centralized management server.

For Linux on Power endpoints (excluding those endpoints that are running in big-endian mode on Red Hat Enterprise Linux 8), PowerSC can provide security hardening for SUSE Linux Enterprise Server 12 SP3 and Red Hat Enterprise Linux Server 8. PowerSC provides Linux security hardening profile support for your PCI-DSS and GDPR compliance obligations. The goal of these two profiles is to help clients address the subset of their compliance requirements that relate to operating system security hardening. It is also possible to create customized profiles that include any portion or combination of these two profiles.

2.4.6 SUSE Linux Enterprise Server Security Hardening Guide for the SAP HANA Platform

If you run the SAP HANA platform for Linux on Power, you must be aware of the system hardening advice from SUSE. SUSE provides the Operating System Security Hardening Guide for SAP HANA, which offers recommendations for operating system security hardening measures for SUSE Linux Enterprise Server 11 when running SAP HANA on an SUSE Linux Enterprise Server host.

It also provides the Operating System Security Hardening Guide for SAP HANA for SUSE Linux Enterprise Server 12, which is updated for SUSE Linux Enterprise Server 12 hosts.

These guides provide many recommendations for improving the security of your operating system environments when specifically running SAP HANA on SUSE Linux Enterprise Server. Also, SUSE recently released a hardening guide version for SUSE Linux Enterprise Server 15.

For more information, see [*Operating System Security Hardening Guide for SAP HANA for SUSE® Linux Enterprise Server 15.*](#)

2.4.7 Red Hat Enterprise Linux Security Hardening Guide

The [**Red Hat Enterprise Linux 8 Security Hardening guide**](#) describes how you can approach security for any Red Hat Enterprise Linux system.

Use this guide to learn how to approach cryptography, evaluate vulnerabilities, and assess threats to various services. You also can learn how to scan for compliance standards, check file integrity, perform auditing, and encrypt storage devices.

An assessment can begin with the use of some sort of data collection tool. When evaluating the entire network, start by mapping the layout to locate the active hosts. Examine each host separately after you find them. Focusing on these hosts necessitates the use of different technologies. Knowing which tools to use can be the most important step in detecting flaws.

The following tools are available for Red Hat on IBM Power Systems:

- ▶ Nmap

This tool is a well-known utility for locating host systems and opening ports on such systems.

Enter the `yum install nmap` command as root to install Nmap, as shown in Example 2-22.

Example 2-22 Nmap installation using yum

```
$ yum install nmap
Updating Subscription Management repositories.
RedHatEnterpriseLinux8forPower_little endian-BaseOS (RPMs)
22 kB/s | 4.1 kB    00:00
RedHatEnterpriseLinux8forPower_little endian-BaseOS (RPMs)
27 MB/s | 32 MB    00:01
RedHatEnterpriseLinux8forPower_little endian-AppStream (RPMs)
30 kB/s | 4.5 kB    00:00
RedHatEnterpriseLinux8forPower_little endian-AppStream (RPMs)
40 MB/s | 27 MB    00:00
Last metadata expiration check: 0:00:07 ago on Thu 04 Nov 2021 09:22:01 PM +08.
Dependencies resolved.
=====
```

Package	Architecture
Version	Repository
Size	
<hr/>	
Installing:	
nmap ppc64le	2:7.70-5.el8
rhel-8-for-ppc64le-appstream-rpms	
5.9 M	
Transaction Summary	
<hr/>	
Install 1 Package	
<hr/>	
Total download size: 5.9 M	
Installed size: 24 M	

For this example, assume that your local network is 192.168.0.0/24, and you want to run a scan on this network. Running a scan without any argument except the network address yields the output that is shown in Example 2-23.

Example 2-23 Nmap scan

```
$ nmap 192.168.0.0/24
```

► OpenSCAP

The **oscap** command-line application and the scap-workbench graphical utility from the OpenSCAP package allow an automated compliance audit. For more information, see 2.5, “NIST Security Content Automation Protocol SCAP” on page 60.

► AIDE (Advanced Intrusion Detection Environment) is a program that creates a database of all the files on an LPAR and then, uses it to maintain file integrity and identify system intrusions.

To install AIDE, run the command as shown in Example 2-24.

Example 2-24 AIDE installation using yum

```
$ yum install aide
```

To generate an initial database, run the command as shown in Example 2-25.

Example 2-25 AIDE initial database

```
$ aide --init
```

```
Start timestamp: 2021-11-04 21:40:54 +0800 (AIDE 0.16)
AIDE initialized database at /var/lib/aide/aide.db.new.gz
```

```
Number of entries: 145114
```

```
The attributes of the (uncompressed) database(s):
```

```
/var/lib/aide/aide.db.new.gz
MD5      : ALWfHdfj8BLNGeU/CLJ8gg==
SHA1     : L/10ESrEcBMbPZI1aFMG/tP1v4A=
RMD160   : 9tfJPP012JmIjrQDky7WNsUASkE=
TIGER    : i8FWiCTTQRc0ccdYu5RxUJ1FfjiSauGf
SHA256   : Gn/W5X/HGY+sC5SjXaGWvUjsiYSxg0t9
                           2VA+Xi5DN9s=
```

```
SHA512    : m+2xbUZevXpkxYKBK4JDXu45/GWiMoA3
             UUpkSUuP42uxwEzTzBUTtk0fIUQQdiOT
             hcUj0jiaUUy4ngEDyAT/0g==
End timestamp: 2021-11-04 21:47:20 +0800 (run time: 6m 26s)
```

To start using the database, remove the .new substring from the initial database file name, as shown in Example 2-26.

Example 2-26 Start using the database

```
$ mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Start a manual check, as shown in Example 2-27.

Example 2-27 Manual check

```
$ aide --check
```

```
Start timestamp: 2021-11-04 21:50:16 +0800 (AIDE 0.16)
AIDE found NO differences between database and filesystem. Looks okay!!
Number of entries:      145114
```

The attributes of the (uncompressed) database(s):

```
/var/lib/aide/aide.db.gz
MD5      : ALWfHdfj8BLNGeU/CLJ8gg==
SHA1     : L/10ESrEcBMbPZI1aFMG/tP1v4A=
RMD160   : 9tfJPP012JmIjrQDky7WNsUASkE=
TIGER    : i8FWiCTTQRc0ccdYu5RxUJ1FfjiSauGf
SHA256   : Gn/W5X/HGY+sC5SjXaGWvUjsiYSxg0t9
             2VA+Xi5DN9s=
SHA512   : m+2xbUZevXpkxYKBK4JDXu45/GWiMoA3
             UUpkSUuP42uxwEzTzBUTtk0fIUQQdiOT
             hcUj0jiaUUy4ngEDyAT/0g==
```

```
End timestamp: 2021-11-04 21:56:25 +0800 (run time: 6m 9s)
```

► Red Hat Satellite™

This tool a systems management solution that makes deploying, scaling, and managing Red Hat infrastructure across physical, virtual, and cloud environments straightforward. Satellite allows customers to manage Red Hat systems over their entire lifecycle, which ensures that they are running efficiently, securely, and in compliance with various standards.

Satellite helps enterprises boost productivity, reduce operational expenses, and enable IT to better respond to strategic business needs by automating most processes that are connected to system maintenance.

Red Hat Satellite uses the Security Content Automation Protocol (SCAP) to define security configuration policies. For example, a security policy might specify that for hosts that are running Red Hat Enterprise Linux, logging in by way of SSH is not permitted for the root account.

For more information, see [Red Hat Satellite 6.9 Administering Red Hat Satellite: A guide to administering Red Hat Satellite](#).

2.5 NIST Security Content Automation Protocol SCAP

The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated to machines and humans.

SCAP is a set of specifications that can be used to automate configuration, vulnerability and patch checking, technical control compliance tasks, and security measurement. SCAP's development goals include standardizing system security management, increasing security product interoperability, and encouraging the adoption of standard security content expressions.

For more information, see *The Technical Specification for the Security Content Automation Protocol SCAP Version 1.3*, [NIST.SP.800-126r3](#).

[OpenSCAP](#) is a system that provides many tools to assist administrators and auditors with assessing, measuring, and enforcing security baselines.

The OpenSCAP project provides a wide range of hardening guides and configuration baselines that are established by the Open Source community. The project helps to select the security strategy that best meets your organization's needs, regardless of its size.

OpenSCAP mostly works with the XCCDF format, which is a standard manner of expressing and defining security checklist content. It also interacts with more requirements, such as CPE, CCE, and OVAL to build a SCAP-expressed checklist that SCAP-validated products can process.

Using OpenSCAP on Red Hat Enterprise Linux on IBM Power Systems

To install OpenSCAP on Red Hat Enterprise Linux 8 on Power Systems, use the command as shown in Example 2-28.

Example 2-28 Installing OpenSCAP packages on Red Hat Enterprise Linux

```
# yum install openscap-scanner  
# yum install scap-security-guide
```

The main purpose of OpenSCAP is to perform local system configuration and vulnerability scans, as shown in Example 2-29. SCAP source data streams, XCCDF benchmarks, and OVAL specifications can be evaluated by OpenSCAP and the relevant results can be generated.

Example 2-29 Scanning for vulnerabilities using #oscap command

```
# oscap xccdf eval --profile PROFILE_ID --results-arf ARF_FILE --report  
REPORT_FILE SOURCE_DATA_STREAM_FILE
```

SCAP content can be delivered as a single XML file (as a SCAP source data stream) or as numerous XML files, where:

- ▶ PROFILE_ID is the ID of an XCCDF profile.
- ▶ ARF_FILE is the file path where the results in SCAP results data stream format (ARF) are generated.
- ▶ REPORT_FILE is the file path where a report in HTML format is generated.
- ▶ SOURCE_DATA_STREAM_FILE is the file path of the evaluated SCAP source data stream.

For example, to evaluate the xccdf_org.ssgproject.content_profile_ospp profile from the /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml SCAP source data stream, run the command as shown in Example 2-30.

Example 2-30 Evaluating a profile

```
#oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_ospp  
--results-arf results.xml --report report.html  
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

For example, to evaluate the Payment Card Industry Data Security Standard (PCI-DSS) on Red Hat Enterprise Linux, use the command as shown in Example 2-31.

Example 2-31 Evaluate PCI-DSS using #oscap command

```
oscap xccdf eval \  
--results results-rhel8-ibmpower.xml \  
--profile xccdf_org.ssgproject.content_profile_pci-dss \  
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml  
$ oscap xccdf generate report --output report.html results-rhel8-ibmpower.xml  
$ firefox report.html
```

Figure 2-3 shows the OpenSCAP report after scanning.

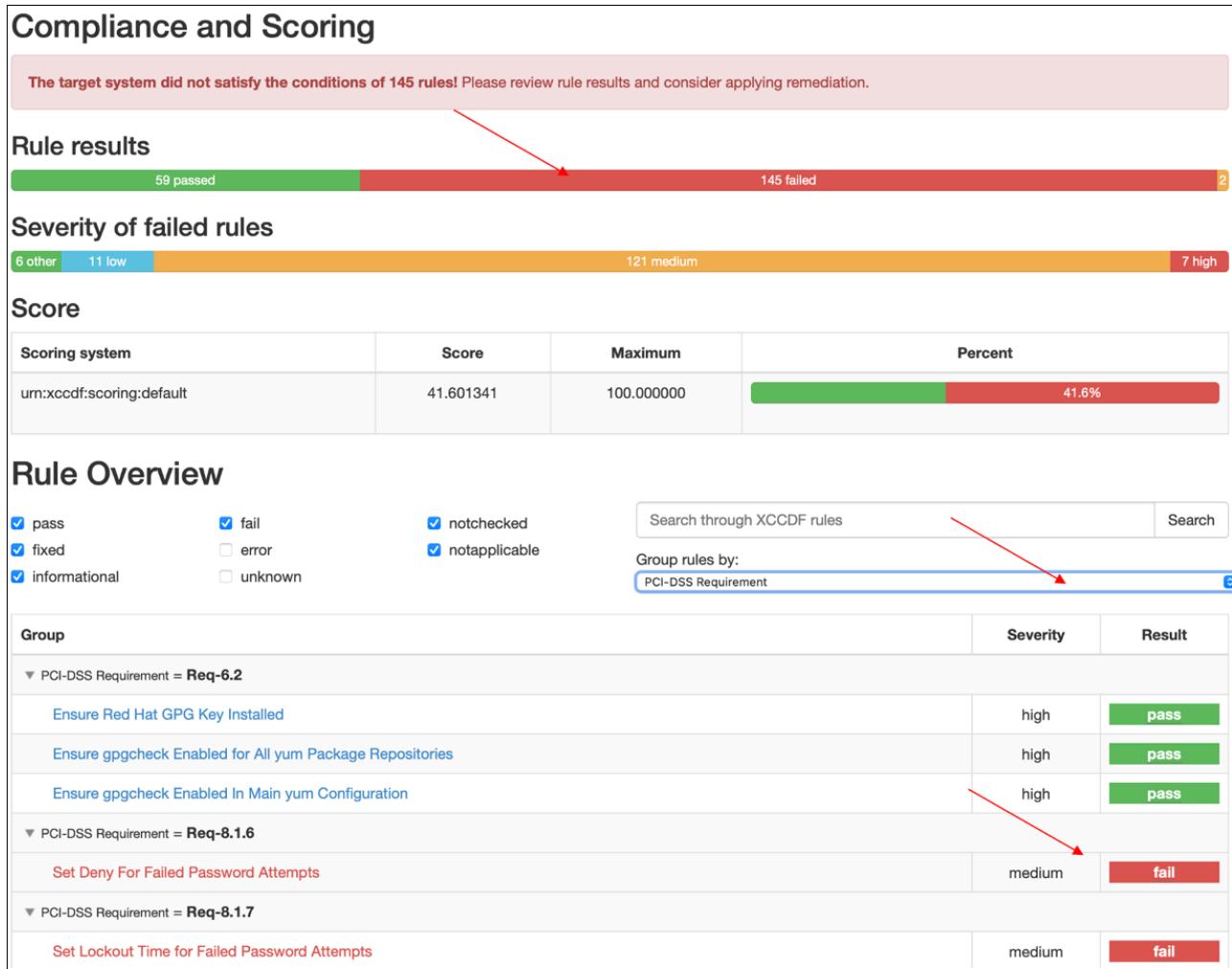


Figure 2-3 OpenSCAP report after scanning

OpenSCAP enables systems to be automatically remedied if they are discovered to be noncompliant. A remediation script must be connected to the rules in SCAP content for system remediation. To remediate Payment Card Industry Data Security Standard (PCI-DSS) findings, use the command as shown in Example 2-32.

Example 2-32 Remediate the PCI-DSS

```
$ oscap xccdf eval --remediate --profile xccdf_org.ssgproject.content_profile_ospp
--results-arf results.xml /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
$ oscap xccdf generate report --output report.html results-rhel8-ibmpower.xml
$ firefox report.html
```

Figure 2-4 shows the OpenSCAP report after remediation compliance and scoring.

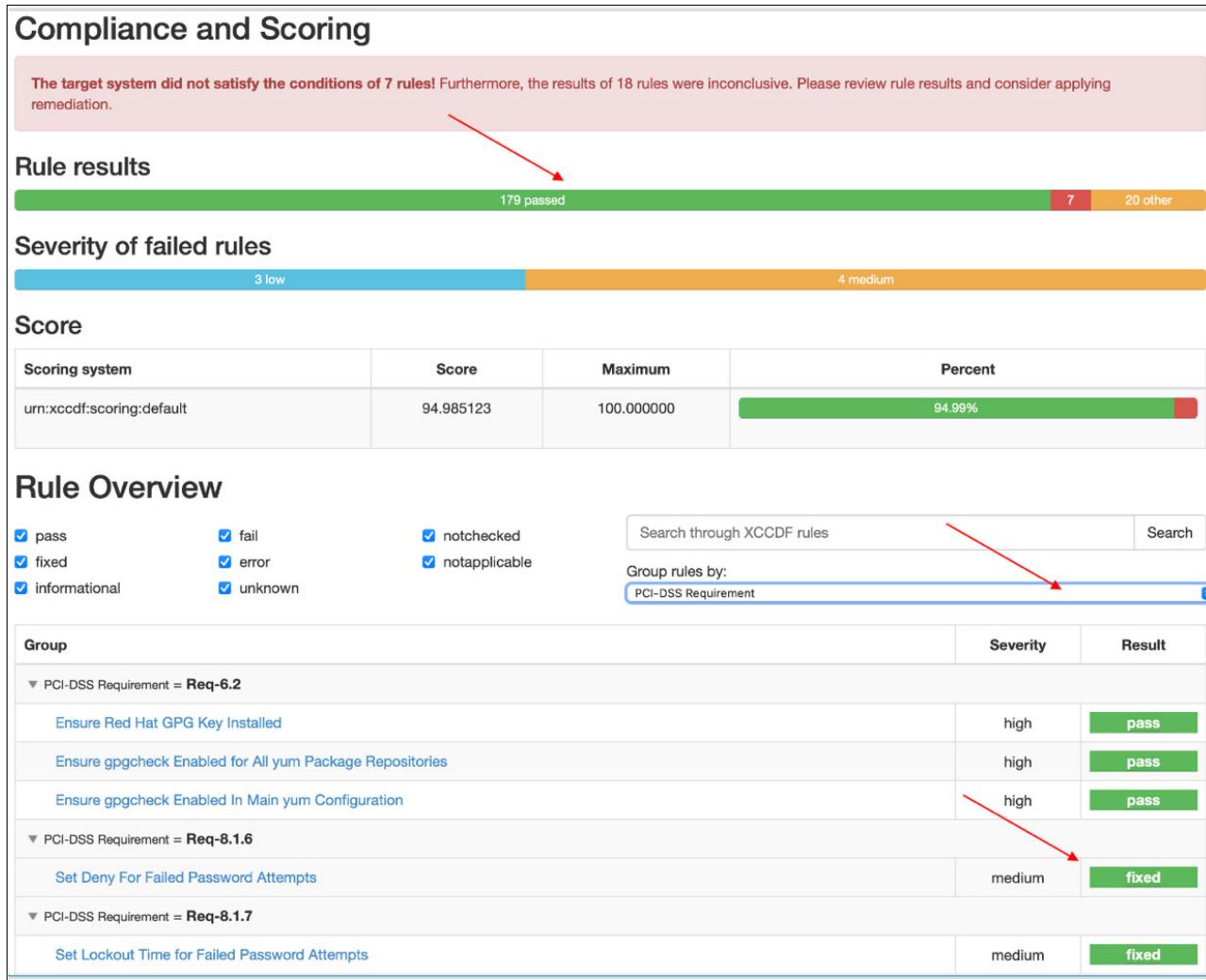


Figure 2-4 OpenSCAP report after remediation

Using OpenSCAP Workbench with Red Hat on IBM Power Systems

SCAP Workbench is a graphical program that makes performing typical OpenSCAP activities simple. Users can use this application to conduct configuration and vulnerability scans on a single local or remote system, and system remediation by using the XCCDF or SDS file provided.

Workbench can create reports in various formats that contain the findings of a system scan and allows you to easily edit an XCCDF profile without having to change the XCCDF file. The utility has a graphical interface for enabling and disabling XCCDF elements.

To install SCAP Workbench on Red Hat Enterprise Linux 8 or later, use the command as shown in Example 2-33.

Example 2-33 Installing SCAP Workbench packages on Red Hat Enterprise Linux

```
yum install scap-workbench  
# yum install scap-security-guide
```

Use the SCAP Workbench to start scanning, dry running, and remediating systems, as shown in Figure 2-5.

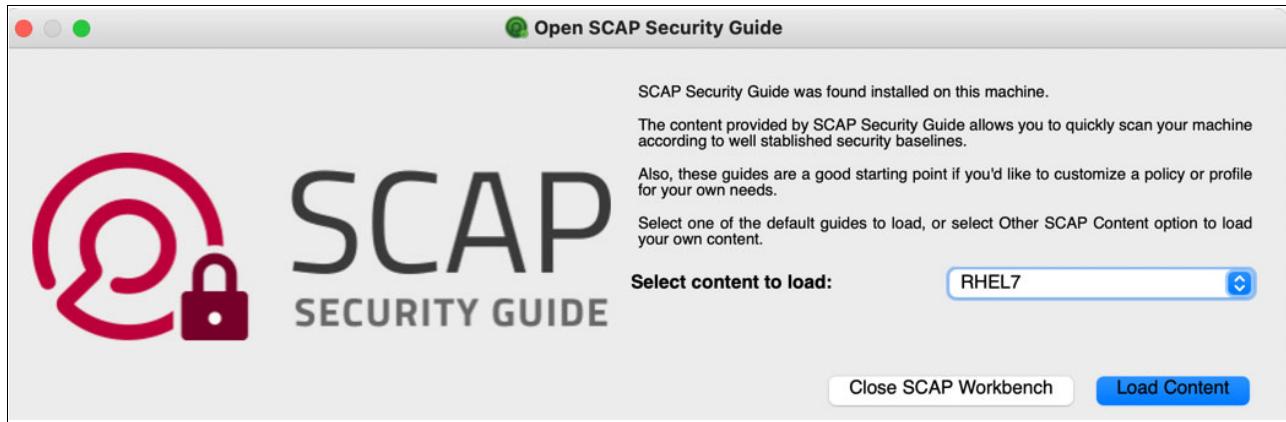


Figure 2-5 SCAP Workbench

The oscap-podman tool can be used to scan Linux containers and container images. Example 2-34 shows the installation of the tool.

Note: The oscap-podman tool is available on Red Hat Enterprise Linux 8 or later.

Example 2-34 Installing OpenSCAP podman packages on Red Hat

```
# yum install openscap-utils
```

Get the ID of a container or a container image, as shown in Example 2-35.

Example 2-35 Get ID or image of a container

```
# podman image
REPOSITORY          TAG      IMAGE ID      CREATED       SIZE
registry.redhat.io/rhel8/mariadb-103 latest  4d61c370f4a9  10 months ago  645 MB
```

Evaluate the SCAP content, as shown in Example 2-36.

Example 2-36 SCAP output content

```
# oscap-podman 4d61c370f4a9 xccdf eval --report report.html --profile ospp
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

2.6 Linux Integrity Measurement Architecture

Integrity Measurement Architecture (IMA) measurement is an Open Source, trusted computing component. If anchored in a hardware Trusted Platform Module (TPM), IMA keeps a runtime measurement list and an aggregate integrity value for this list. The advantage of anchoring the aggregate integrity value in the TPM is that any software attack cannot compromise the measurement list without being detected.

Note: IBM Power Virtual Server customer LPARs do not have access to IBM Power Server physical Trusted Platform Module.

For more information, see this [SourceForge web page](#).

IMA measurement can be used to attest to the system's runtime integrity on a trusted boot system.

The kernel integrity subsystem's objectives are to:

- ▶ Detect if files were maliciously or inadvertently remotely or locally modified.
- ▶ Appraise a file's measurement against a "good" value that is kept as an extended attribute.
- ▶ Ensure that local file integrity is maintained.

The kernel integrity subsystem is made up of two main components:

- ▶ The IMA collects file hashes, stores them in kernel memory (away from users and apps), and allows local and remote parties to validate the measured values.
- ▶ The Extended Verification Module (EVM), which detects offline alterations of the security extended features.

IMA preserves a runtime measurement list and an aggregate integrity value for this list if it is anchored in a hardware Trusted Platform Module (TPM). The benefit of anchoring the aggregate integrity value in the TPM is that it prevents a software attack from compromising the measurement list without being detected. As a result, in a trustworthy boot system, IMA measurement can be used to attest to the system's runtime integrity.

Enabling IMA on Red Hat on IBM Power Systems

The kernel integrity subsystem's components, the IMA, and the EVM improve system security in various ways. You can sign files and improve system security by configuring IMA and EVM.

The following prerequisites must be met:

- ▶ The `ima-evm-utils`, `attr`, and `keyutils` packages are installed on your system.
- ▶ The `securityfs` file system is mounted on the `/sys/kernel/security/` directory.
- ▶ The `/sys/kernel/security/ima/` directory exists.

Complete the following steps to enable IMA on Red Hat on IBM Power Systems:

1. Add the following kernel command-line parameters:

```
$ grubby --update-kernel=/boot/vmlinuz-$(uname -r) --args="ima_appraise=fix  
ima_appraise_tcb evm=fix"
```

2. Reboot for the changes to take effect and create a keyring for EVM:

```
$ evm_kr_id=$(keyctl newring _evm @u)
```

3. Create a directory for keys and generate a 1024-bit RSA private key:

```
$ mkdir -p /etc/keys/  
$ openssl genrsa -out /etc/keys/privkey.pem 1024
```

4. Use the previously created /etc/keys/privkey.pem private key to derive a corresponding RSA public key into the /etc/keys/pubkey.pem file:

```
$ openssl rsa -pubout -in /etc/keys/privkey.pem -out /etc/keys/pubkey.pem
```

5. Import the public key into the dedicated EVM keyring and create a kernel master key to protect the EVM key:

```
$ evmctl import --rsa /etc/keys/pubkey.pem $evm_kr_id  
$ dd if=/dev/urandom bs=1 count=32 2>/dev/null | keyctl padd user kmk-user @u
```

6. Create and activate an encrypted EVM key based on the kmk key:

```
$ keyctl add encrypted evm-key "new user:kmk 64" @u  
$ echo 1 > /sys/kernel/security/evm
```

7. Collect file hashes with integrity measurement architecture. Then, create a test file:

```
$ echo "Hello from Redbooks Team" > hello_file
```

8. Sign the file with the private key:

```
$ evmctl sign --imahash --key /etc/keys/privkey.pem hello_file
```

By creating a hash of the hello_file file, IMA verifies that the file is uncorrupted. EVM ensures that the IMA hash is genuine by signing the hash content that is stored in the extended attribute of hello_file.

9. Check the extended attributes of the signed file:

```
$ getfattr -m . -d hello_file
```

The output shows extended attributes that are related to the IMA and EVM hash values. EVM actively adds a security.evm extended attribute and detects any offline tampering to xattrs of other files, such as security.ima that are directly related to file content integrity.

2.7 Compressed and encrypted Live Partition Mobility data

Partition mobility, which is part of the PowerVM Enterprise Edition hardware capability, allows you to move logical partitions across systems that are running AIX, IBM i, and Linux. The system environment, which comprises the processor state, memory, associated virtual devices, and connected users, is transferred throughout the mobility process.

Data in-flight is faster and better protected during migration events following the IBM POWER9 introduction of encrypted and compressed Live Partition Mobility (LPM) features.

Active partitions can be moved from one Power server to another with minimal downtime by using LPM, as shown in Figure 2-6. Even if a planned outage occurs, such as for hardware maintenance or firmware updates, LPM ensures that operations are available 24 hours a day, seven days a week, and that the partition data that is transported between the servers is automatically encrypted for improved security and compressed for better performance.

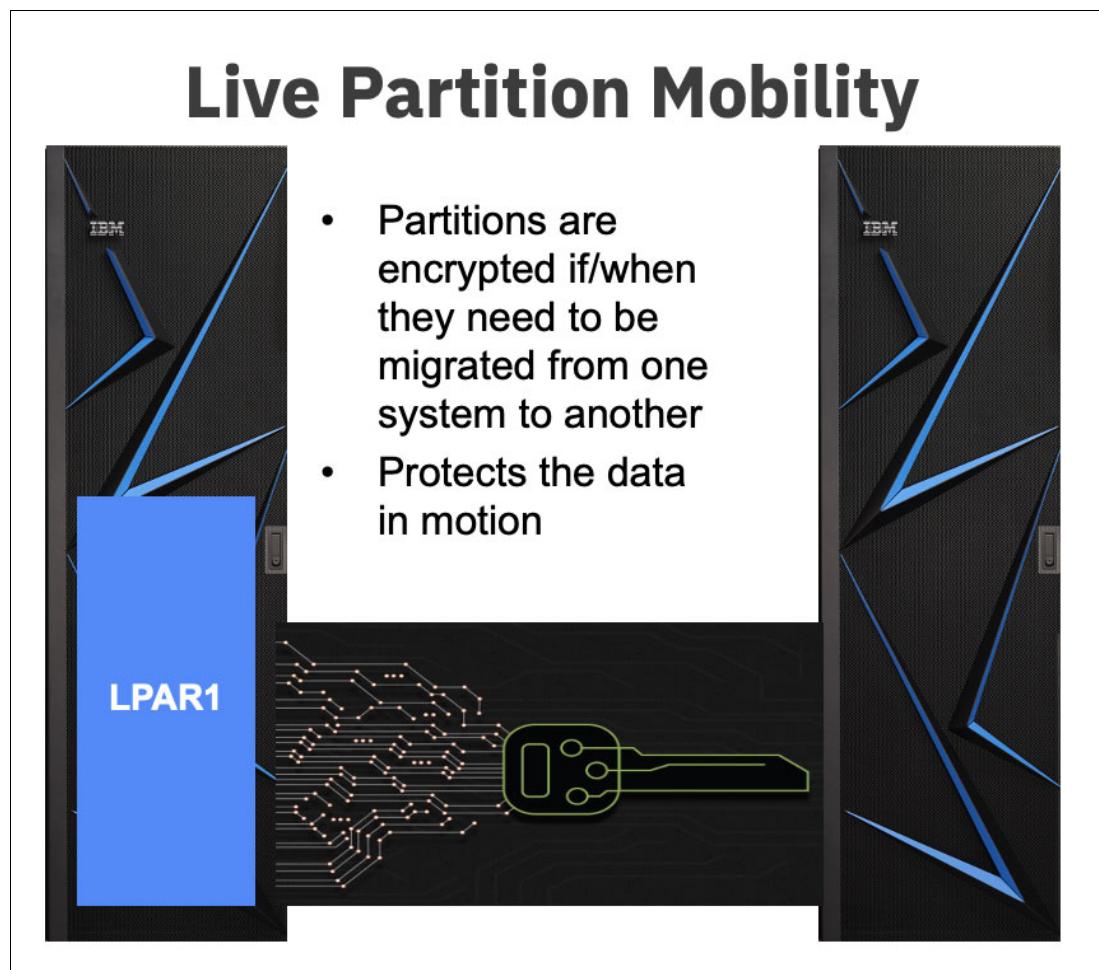


Figure 2-6 Partition data encryption when migrating an LPAR from source to target server

The hypervisor first compresses and then encrypts the partition data. Compression provides a performance benefit by reducing the amount of data that must be sent from the source to the target server.

Because the time it takes to encrypt a block of data is directly proportional to the amount of data that is encrypted, compressing the data also provides better encryption performance. When doing compression, the hypervisor presents to the NX unit the buffer of data that must be compressed. The NX unit uses the 842-compression algorithm, which provides good compression in a short period.

Note: IBM Power Virtual Server customers cannot start LPAR migration. Migration in the cloud is started only by Cloud administrators; for example, because of server maintenance, patching, reboot, and is done “under the covers”.

The use of LPM encryption capability in IBM Power Virtual Server ensures that customer applications and data are encrypted, even during maintenance actions that might require partition migration.

For the data encryption, initial set up steps are completed by the HMC and hypervisor at the start of the migration operation to ensure secure authentication and encryption. Each POWER9/POWER10 server includes a Trusted Platform Module (TPM) that is provisioned by IBM during the manufacturing process to contain a platform certificate. This certificate is used to verify the identity of the source and target servers and to create an AES-256 symmetric encryption key.

Each LPM request generates its own unique encryption key that is known only to the PowerVM hypervisor. After a buffer is compressed, the hypervisor again presents the buffer to the NX unit and encrypts the data by using the AES-256 GCM encryption function in the NX unit.



IBM Power Systems and IBM Power Systems Virtual Server advanced security capabilities

Organizations can no longer focus exclusively on external cybersecurity defenses. They need a proven strategy that considers the following facts:

- ▶ Accept the realities of data breaches.
- ▶ Malicious insiders.
- ▶ Embedded back doors in technologies from the supply chain.
- ▶ Compromised vendor, customer, contractor, partner networks, and systems.
- ▶ Security realities when cloud providers and third-party services are used.

Also, organizations methodologies must:

- ▶ Adapt to a “security over time” strategy rather than just a real-time window.
- ▶ Include recurring audits of systems, applications, devices, and logs.
- ▶ Use a long-term data logging strategy that facilitates audits.

This chapter describes advanced security capabilities for IBM Power Systems and IBM Power Systems Virtual Server that use built-in technologies and offerings from IBM Cloud and Security portfolio.

This chapter includes the following topics:

- ▶ 3.1, “IBM PowerSC and IBM PowerSC MFA” on page 70
- ▶ 3.2, “Security and compliance for Red Hat OpenShift on IBM Power Systems and IBM Power Systems Virtual Server” on page 71
- ▶ 3.3, “Data in transit and at rest protection with IBM Security Guardium” on page 76
- ▶ 3.4, “Detecting advanced threats, proving compliance, and securing cloud with IBM QRadar” on page 90
- ▶ 3.5, “Modernizing security with IBM Cloud Pak for Security” on page 108

3.1 IBM PowerSC and IBM PowerSC MFA

Some of the important components that are required to defend virtualized data centers and cloud infrastructure against growing new threats are security control and compliance.

Maintaining system security and ensuring that IT systems are consistent with common industry security standards can be a difficult, labor-intensive, and expensive task, especially in cloud and virtualized IT environments. On Power Systems servers running PowerVM, IBM PowerSC provides a security and compliance solution that is tailored for virtualized and cloud settings.

3.1.1 IBM PowerSC

IBM PowerSC provides a security and compliance solution that is optimized for virtualized environments on Power Systems servers, running IBM AIX, IBM i, and Linux. PowerSC sits on top of our Power Systems Stack. It uses and integrates the security features that are built at different layers. It also allows you to centrally manage security and compliance on Power for all AIX and Linux on Power endpoints, and receive better support for compliance audits, including GDPR.

PowerSC 2.0 provides a web-based UI to manage security and compliance:

- ▶ Security: File Integrity Monitoring (FIM), allow listing, endpoint detection, and response.
- ▶ Compliance: HIPAA, PCI, CIS, and more.
- ▶ Patch management: Trusted Network Connect (TNC), detect and alert policy issues, policy enforcement.

For more information, see Chapter 4, “IBM Power Systems advanced security implementation scenarios” on page 109.

3.1.2 IBM PowerSC Multi-Factor Authentication

IBM PowerSC Multi-Factor Authentication (MFA), provides alternative authentication mechanisms for systems that are used with RSA SecurID-based authentication systems. It also provides mechanisms for certificate authentication options, such as Common Access Card (CAC) and Personal Identification Verification (PIV) cards.

IBM PowerSC MFA allows the use of alternative authentication mechanisms instead of the standard password (see Figure 3-1).

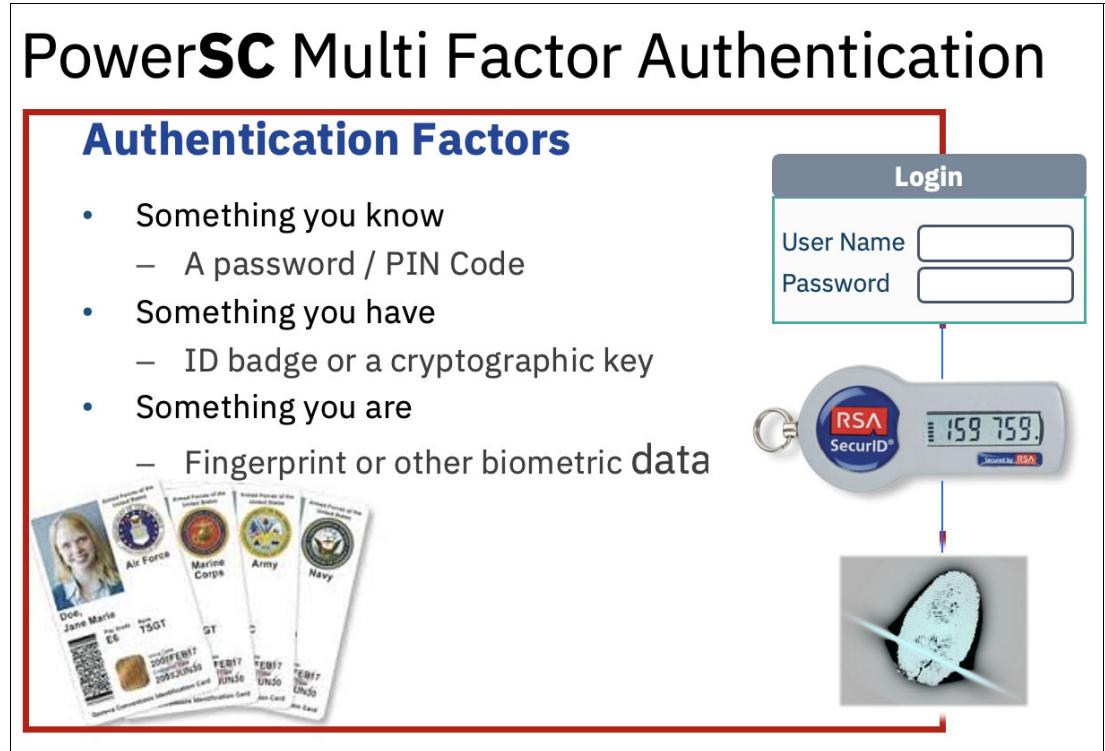


Figure 3-1 IBM PowerSC Multi Factor Authentication

For more information, see 4.6, “PowerSC MFA example configuration” on page 137.

3.2 Security and compliance for Red Hat OpenShift on IBM Power Systems and IBM Power Systems Virtual Server

Organizations are challenged with delivering extraordinary customer experiences by developing new applications and at the same time modernizing existing applications to accelerate their cloud-native journey.

Developers and IT operations teams require flexibility and agility to develop and deploy applications across multiple infrastructures, from on-premises to the public cloud.

Red Hat OpenShift on IBM Power Systems empowers organizations to accelerate digital transformation with scalability and added security across the hybrid cloud through a secure and resilient foundation for cloud-native development on IBM Power Systems.

3.2.1 Overview

Red Hat OpenShift is a trusted Kubernetes enterprise platform that supports modern, hybrid-cloud application development. It also provides a consistent foundation for applications anywhere; that is, across physical, virtual, private, and public clouds.

Red Hat OpenShift and IBM Cloud Paks on IBM Power Systems bring the consistency that developers need to build and deploy cloud-native applications across the hybrid cloud and accelerate the path to application modernization (see Figure 3-2).

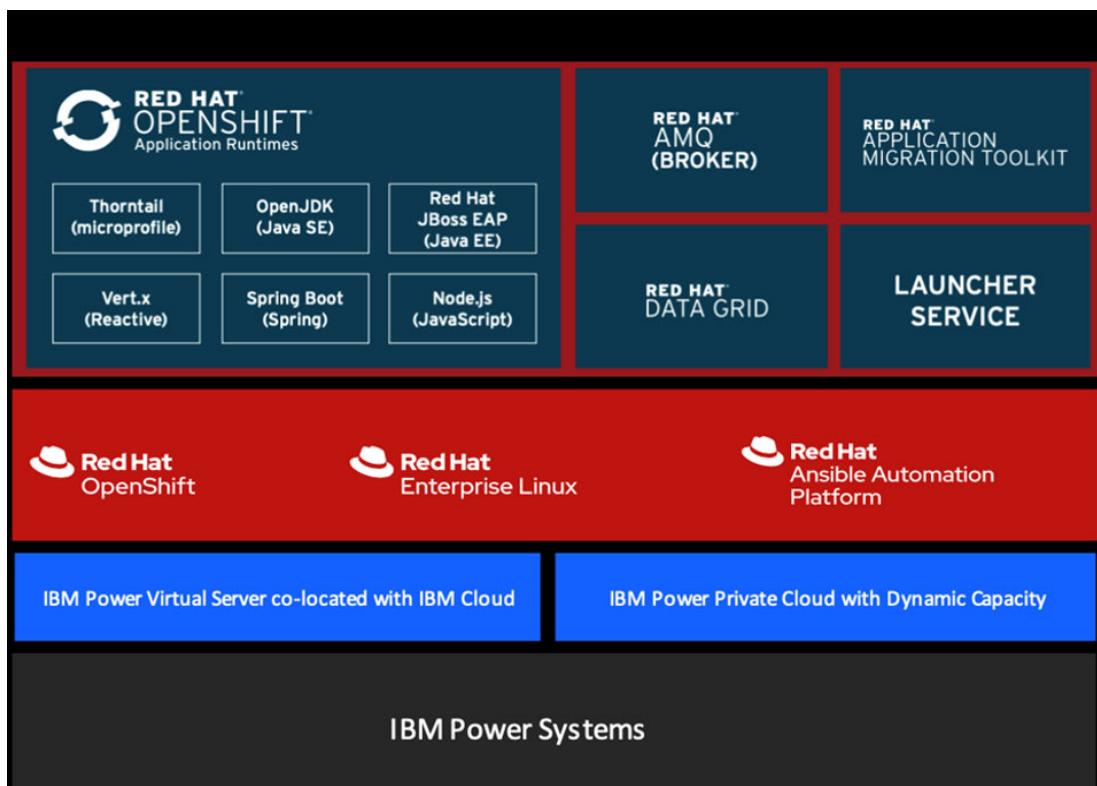


Figure 3-2 Red Hat on IBM Power Systems and IBM Power Systems Virtual Server

3.2.2 Efficient cloud infrastructure scaling

As organizations modernize applications to cloud-native architectures, scalability remains a crucial factor for delivering innovation and better customer experiences.

Red Hat OpenShift enables applications to scale to thousands of instances across hundreds of nodes in seconds, which provides the power to respond to unpredictable demands. Also, IBM Power Systems provides a pay-per-use consumption model in on-premises and off-premises environments and can scale applications up and down based on demand.

It also enables low-latency connection between applications and data by collocating cloud-native applications with virtual machine (VM)-based applications that are running on AIX, IBM i, or Linux environments.

Also, with built-in virtualization, users can dynamically add or remove memory and CPUs that are allocated to worker node VMs. This offering allows organizations to take advantage of the scalability of Red Hat OpenShift and IBM Power Systems to deliver excellent customer experiences, regardless of demand.

3.2.3 Proven security and reliability

Red Hat OpenShift on IBM Power Systems empowers organizations to modernize applications with a strong foundation that is built for security and reliability. IBM Power Systems supports live partition mobility for uninterrupted access to critical data and applications, which gives teams the confidence they need to develop and deploy applications more securely.

The compute infrastructure reduces unplanned downtime with less than two minutes per year, which improves productivity for IT teams while reducing impact for users and critical business processes. With Red Hat OpenShift on IBM Power Systems, teams can develop and deploy applications across the hybrid cloud with the security they need for critical workloads.

3.2.4 Red Hat OpenShift on IBM Power Systems Virtual Server

Red Hat OpenShift can be a critical part in helping organizations build an agile hybrid cloud. It is available on IBM Power Systems Virtual Server that use Red Hat OpenShift's platform-neutral installer.

IBM Power Systems Virtual Server is an enterprise Infrastructure-as-a-Service offering that is built around IBM POWER9 servers that are collocated in IBM Cloud and offer access to over 200 IBM Cloud services. In addition, IBM Power Systems Virtual Server clients can now run leading business applications, such as SAP HANA in an IBM POWER9-based cloud.

3.2.5 Containers security

Securing a containerized application relies on multiple levels of security:

- ▶ Container security begins with a trusted base container image and continues through the container build process as it moves through your CI/CD pipeline.
- ▶ When a container is deployed, its security depends on it running on secure operating systems and networks and establishing firm boundaries between the container and the users and hosts that interact with it.
- ▶ Continued security relies on scanning container images for vulnerabilities and having an efficient way to correct and replace vulnerable images.

Auditing

Red Hat OpenShift Container Platform auditing provides a security-relevant chronological set of records that document the sequence of activities that affected the system by individual users, administrators, or other components of the system. Administrators can configure the audit log policy and view audit logs.

Complete the following steps to configure the audit log policy to use when logging requests that come to the API servers:

1. Edit the APIServer resource, as shown in Example 3-1.

Example 3-1 Edit APIServer

```
$ oc edit apiserver cluster
```

2. Update the spec.audit.profile field, as shown in Example 3-2.

Example 3-2 Update spec.audit.profile

```
$apiVersion: config.openshift.io/v1
  kind: APIServer
  metadata:
    ...
  spec:
    audit:
      profile: WriteRequestBodies
```

Set the file to Default, WriteRequestBodies, or AllRequestBodies. (The default profile is Default). Save the file to apply the changes.

3. Verify that a new revision of the Kubernetes API server pods rolled out, as shown in Example 3-3. This process takes several minutes to complete.

Example 3-3 Verify new revision

```
$ oc get kubeapiserver -o=jsonpath='{range
.items[0].status.conditions[?(@.type=="NodeInstallerProgressing")]}{.reason}{"\n"
{.message}}{"\n"}'
```

4. Review the NodeInstallerProgressing status condition for the Kubernetes API server to verify that all nodes are at the latest revision.

Viewing the audit logs

You can view the logs for the Red Hat OpenShift API server, Kubernetes API server, and Red Hat OpenShift OAuth API server for each control plane node (also known as the *master node*).

The Red Hat OpenShift API server logs that are available for each control plane node can be listed, as shown in Example 3-4.

Example 3-4 Listing Red Hat OpenShift API server logs

```
$ oc adm node-logs --role=master --path=openshift-apiserver
ci-1n-m0vpfjd-f79a1-vb5x-master-0 audit-2021-03-11T00-12-11.374.log
ci-1n-m0vpfjd-f79a1-vnb5x-master-0 audit.log
ci-1n-m0vpfjd-f79a1-vnb5x-master-1 audit-2021-03-11T00-12-29.941.log
ci-1n-m0vpfjd-f79a1-vnb5x-master-1 audit.log
ci-1n-m0vpfjd-f79a1-vnb5x-master-2 audit-2021-03-011T00-14-03.137.log
ci-1n-m0vpfjd-f79a1-vnb5x-master-2 audit.log
```

A specific Red Hat OpenShift API server log can be viewed by providing the node name and the log name, as shown in Example 3-5.

Example 3-5 Verify Red Hat OpenShift API logs

```
$ oc adm node-logs <node_name> --path=openshift-apiserver/<log_name>
```

Certificates

Certificates are used by various components to validate access to the cluster. Administrators can replace the default ingress certificate, add API server certificates, or add a service certificate.

You can also review more information about the following types of certificates that are used by the cluster:

- ▶ User-provided for the API server.
- ▶ Proxy
- ▶ Service CA
- ▶ Node
- ▶ Bootstrap
- ▶ etcd
- ▶ OLM
- ▶ User-provided for default ingress
- ▶ Ingress
- ▶ Monitoring and cluster logging Operator component
- ▶ Control plane

Encrypting data

You can enable etcd encryption for your cluster to provide another layer of data security. For example, it can help protect the loss of sensitive data if an etcd backup is exposed to the incorrect parties.

When you enable etcd encryption, the following Red Hat OpenShift API server and Kubernetes API server resources are encrypted:

- ▶ Secrets
- ▶ Configuration maps
- ▶ Routes
- ▶ OAuth access tokens
- ▶ OAuth authorize tokens

Vulnerability scanning

Administrators can use the Container Security Operator (CSO) to run vulnerability scans and review information about detected vulnerabilities. For more information, see this [Red Hat Documentation web page](#).

They can also use tools, such as OpenSCAP, as described in 2.5, “NIST Security Content Automation Protocol SCAP” on page 60.

Compliance overview

For many Red Hat OpenShift Container Platform customers, regulatory readiness or compliance is required on some level before any systems can be put into production. That regulatory readiness can be imposed by national standards, industry standards, or the organization’s corporate governance framework.

Compliance checking

Administrators can use the Compliance Operator to run compliance scans and recommend remediations for any found issues. The `oc-compliance` plug-in is a Red Hat OpenShift CLI (`oc`) plug-in that provides a set of utilities to easily interact with the Compliance Operator.

To fetch the results of all the scans from a `scansettingbinding`, run the command that is shown in Example 3-6.

Example 3-6 Fetch results of all scans

```
$ oc compliance fetch-raw scansettingbinding nist-moderate -o resultsdir/
```

Example 3-7 shows creating a report of the compliance standards and controls that a benchmark fulfills. It also shows the rules that address each control.

Example 3-7 Creating compliance report

```
$ oc compliance controls profile rhcos4-moderate
```

File integrity checking

Administrators can use the file integrity operator to continually run file integrity checks on cluster nodes and provide a log of files that were modified.

3.3 Data in transit and at rest protection with IBM Security Guardium

The demand for data security on-premises and in the cloud is increasing at an exponential rate. Encryption was implemented at many stages (in hardware, on data, and in applications) as a response.

As a result of this reaction, encryption silos can emerge, with disparate methods to key management. Because no explicit key management process is in place in some circumstances, organizations are at risk of losing control of their data if key management is fragmented or non-existent. They require a system that can work with other key managers and self-encrypting devices by way of common protocols, and centralize encryption key management.

3.3.1 IBM Security Guardium

Organizations that deploy IBM System feature protection that is built to include security in the processor, operating system, storage, and applications. However, even these environments need protection against growing threats and their new levels of sophistication.

They must also comply with an expanding number of business and government requirements, and address public concerns about data security. As a result, businesses are implementing new safeguards to help safeguard critical information from unwanted access.

Simultaneously, these controls must be backed up by extensive audit trails that confirm compliance. Creating audit trails by relying on database administrators and manual, homegrown processes is wasteful and violates segregation-of-duties standards.

Unauthorized database access is impossible to prevent. Furthermore, database auditing includes a large overhead cost, which prompts some firms to stop auditing completely. For IBM Power Systems, IBM Security Guardium provides an optimized, integrated, and comprehensive way of securing sensitive data across the company.

IBM Security Guardium enables security teams to defend against threats and data loss by allowing them to:

- ▶ Detect and classify sensitive data automatically and analyze data access patterns and alerting if unusual behavior occurs.
- ▶ Detect threats.
- ▶ Prevent unauthorized database access.
- ▶ Use real-time blocking, quarantining, and encryption to protect sensitive data.

The Guardium portfolio is shown in Figure 3-3.

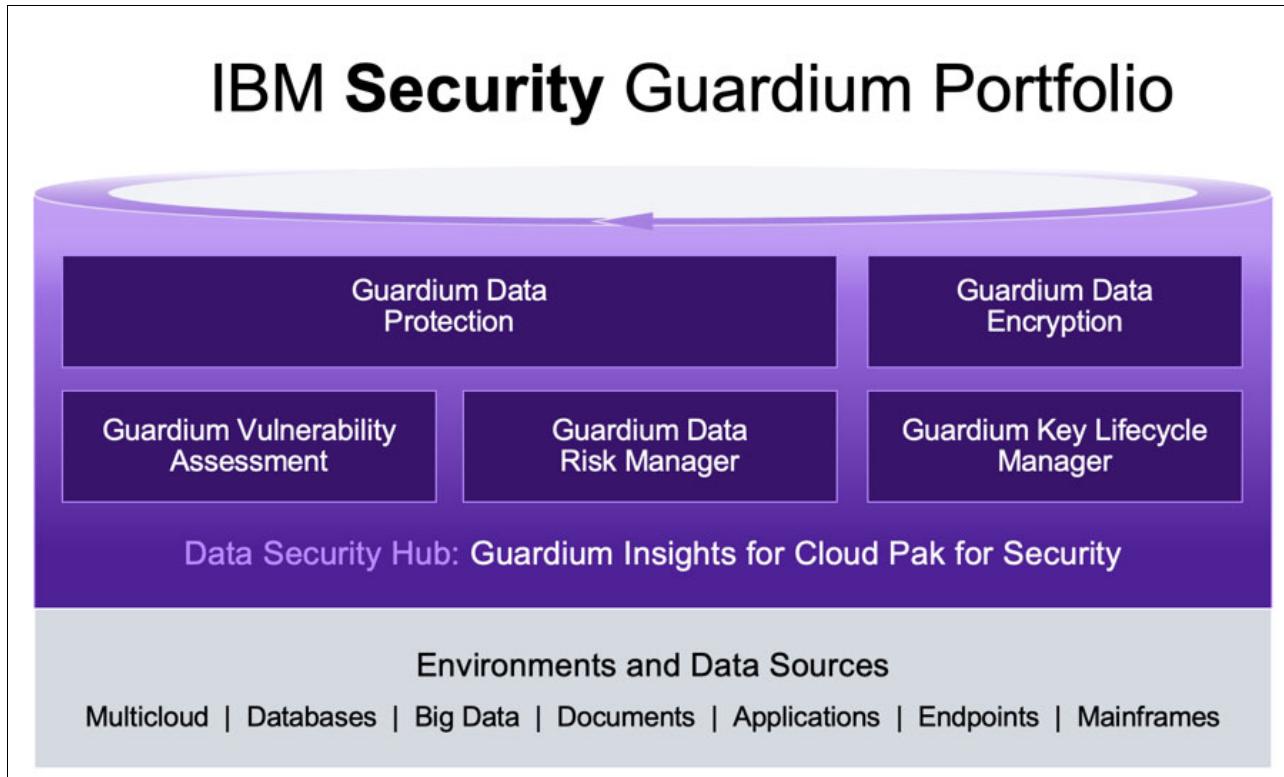


Figure 3-3 IBM Security Guardium Portfolio

To fulfill security standards, such as the Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI-DSS), and data privacy laws, Guardium features automated compliance workflows and prepackaged templates.

These templates can also be customized, and organizations can generate their own bespoke reports. You can help ensure that the correct reports get to the correct individuals in time for sign-off by using the solution's automated compliance workflows.

Guardium also helps minimize total cost of ownership and increase manageability by combining automation and intelligence.

The solution can be used for the environment only. It also can be combined with other Guardium data security and monitoring components to provide a powerful, centralized data security solution across the enterprise's dispersed systems.

3.3.2 IBM Security Guardium Data Encryption

Encryption can help to make data unusable if it is hacked or stolen. Think of it as the first and last line of defense that can help protect any data from full exposure.

The correct encryption strategy helps protect sensitive data and strengthens an organization's compliance posture by making data unreadable in all states: at-rest or in-transit.

IBM Guardium Data Encryption provides encryption offerings that make data unreadable at the file, database, or application level, regardless of where it is stored.

By using methods, such as tokenization, it can convert a meaningful piece of data (for example, an account number) into a random string of characters (a token) that has no meaningful value if breached.

Other capabilities include data masking that is useful when only parts of a data field must be obfuscated. This encryption solution can also assist administrators who must establish and maintain access control policies that can be mapped to compliance requirements for audit reporting.

IBM Guardium Data Encryption provides the following benefits:

- ▶ Granular data encryption at the file, database, or application level for data that is stored on-premises or in the cloud.
- ▶ Obscure data at rest with tokenization or specific parts of data fields with data masking.
- ▶ Consistent policy enforcement for encryption key management and user access controls.

IBM Guardium Data Encryption uses software agents that are installed in operating systems to apply policies that determine whether the data must be encrypted or decrypted. It can be deployed across environments, including Red Hat and SUSE on Power Systems, AIX, in addition to SAP HANA and Teradata file systems and cloud storage environments.

IBM Guardium Data Encryption consists of a Data Security Manager (DSM) and one or more IBM Guardium Data Encryption agents that are on your protected hosts. Protected hosts contain your sensitive data. If connected to an NAS or SAN, the protected host accesses your sensitive data. Protected hosts can be on-site, in the cloud, or a hybrid of both.

The DSM is the central component of the IBM Guardium Data Encryption and is tasked with storing and managing data encryption keys, data access policies, administrative domains, and administrator profiles. Thales provides the DSM as a security-hardened physical appliance or a virtual appliance. The agents communicate with the DSM and implement the security policies on their protected host systems.

How it works

IBM Guardium Data Encryption provides the following benefits:

- ▶ Encrypt files and raw data
- ▶ Control that users can decrypt and access that data and processes and executables can use to decrypt and encrypt that data
- ▶ Generation of fine-grained audit trails on those processes, executables, and users

With complete transparency to users and applications, and with no changes to your infrastructure, IBM Guardium Data Encryption supports separation of duties and data access between data owners, system administrators, and security administrators.

Data is protected by creating policies that specify file encryption, data access, and auditing on specific directories on your protected hosts. These directories are called *GuardPoints*. Policies specify whether the resting files are encrypted, who can access decrypted files and when, what level of file access auditing is wanted, and so on.

Policies are created by using the DSM GUI that is called the *Management Console*. After the policies are created and pushed to protected hosts, the IBM Guardium Data Encryption agents implement those policies.

Installing AIX Agent

To install AIX Agent, complete the following steps:

1. Install the agent on the protected AIX LPAR:
 - a. Obtain the agent installation image from Thales. The format for VTE Agent file names is: vee-<agent_type-build-system>.bin; for example, vee-fs-5.2.7.9-aix71.bin.
 - b. Log in to the host system as root and copy or mount the installation file onto the host system.
 - c. Start the installation, as shown in Example 3-8.

Example 3-8 Accepting the license

```
$ ./vee-fs-5.2.7.9-aix71.bin  
Do you accept this license agreement? (Y/N) [N]: Y
```

The VTE agent is installed on the host, but not yet registered. The prompt that is shown in Example 3-9 appears.

Example 3-9 Registering the VTE Agent

```
Welcome to the Vormetric Encryption Expert File System Agent  
Registration Program.  
Agent Type: Vormetric Encryption Expert File System Agent  
Agent Version: X.X.X.XX  
In order to register the Vormetric Encryption Expert File System Agent  
with a Vormetric Data Security Server:  
1) you must know the host name of the machine running the  
Security Server (the host name is displayed on the  
Dashboard window of the Management Console), and  
2) unless you intend to use the 'shared secret' registration method,  
the agent's host machine must be pre-configured on the  
Security Server as a host with the 'Reg. Allowed'  
checkbox enabled for this agent type on the Hosts window of the  
Management Console.
```

Do you want to continue with agent registration? (Y/N) [Y]:

2. Register the protected host with the DSM so they can communicate with each other (in this section we use Shared Secret Registration method):
 - a. Verify that the DSM Administrator created a shared secret for the domain or host group in which the new protected host is stored.
 - b. Enter Y when you see the prompt that is shown in Example 3-10.

Example 3-10 Continuing with registration

```
Do you want to continue with agent registration? (Y/N) [Y]: Y  
Please enter the primary Security Server host name:
```

- c. Enter the DSM FQDN and then Y, as shown in Example 3-11. Request that the DSM Administrator gets this information from the dashboard of the DSM Management Console.

Example 3-11 Confirming FQDN

```
ys1.redbooks-power-security.com  
You entered the host name gde.redbooks-power-security.com  
Is this host name correct? (Y/N) [Y]: Y
```

- d. You are prompted for the AIX hostname, as shown in Example 3-12.

Example 3-12 Confirming hostname

Please enter the host name of this machine or select from the following list. If using the "fingerprint" registration method, the name you provide must precisely match the name used on the "Add Host" page of the Management Console.

[1] ysl.redbooks.com
[4] 192.168.0.100

Enter a number, or type a different host name or IP address in manually:

What is the name of this machine? [1]: 1

- e. Enter the AIX hostname. This hostname must match the name that is used on the Add Host page of the Management Console (adding the hostname is not needed for the shared secret method). You are prompted for the registration method. Select (S), as shown in Example 3-13.

Example 3-13 Confirming shared secret registration

You selected " ysl.redbooks.com ".

Would you like to register to the Security Server using a registration shared secret (S) or using fingerprints (F)? (S/F) [S]: S

- f. If the Shared Secret information is correct, enter Y. You are prompted if you want to enable hardware association, as shown in Example 3-14.

Example 3-14 Confirming correct

It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the DSM or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again.

Do you want to enable this functionality? (Y/N) [Y]:

- g. Enter Y or N, as shown in Example 3-14. If everything is working, the installation program generates certificate signing requests and the signed certificates are generated, as shown in Example 3-15.

Example 3-15 Example of successful generation of certificate

Generating certificate signing request for the kernel component...done.

Signing certificate...done.

Generating EC certificate signing request for the vmd...done.

Signing certificate...done.

Generating EC certificate signing request for the vmd...done.

Signing certificate...done.

Successfully registered the Vormetric Encryption Expert File System Agent with the primary Vormetric Data Security Server on gde.redbooks-power-security.com.

Installation success.

- h. Verify the installation by checking the agent processes on the protected host, as shown in Example 3-16.

Example 3-16 Verifying the agent process

```
$ vmd -v  
$ secfsd -status pslist  
$ tail -f /var/log/vormetric/install.fs.log.<date>  
$ tail -f /var/log/vormetric/vorvmrd_root.log
```

3.3.3 IBM Security Guardium Key Lifecycle Manager

IBM Security Guardium Key Lifecycle Manager centralizes, simplifies, and automates the encryption key management process to help protect encrypted data and simplify encryption key management. It offers secure, robust key storage, key serving and key lifecycle management for self-encrypting applications and solutions by using interoperability protocols, including KMIP, IPP, and REST.

Guardium Key Lifecycle Manager helps customers meet regulations, such as PCI DSS, Sarbanes-Oxley, and HIPAA by providing access control, key rotation, and other automated key lifecycle management processes.

Security Key Lifecycle Manager is an enterprise-level encryption key manager that uses the IBM Proprietary Protocol (IPP) and the Key Management Information Protocol (KMIP) that were adopted by OASIS and SNIA-SSIF certification as a standard for encryption key distribution (see Figure 3-4).

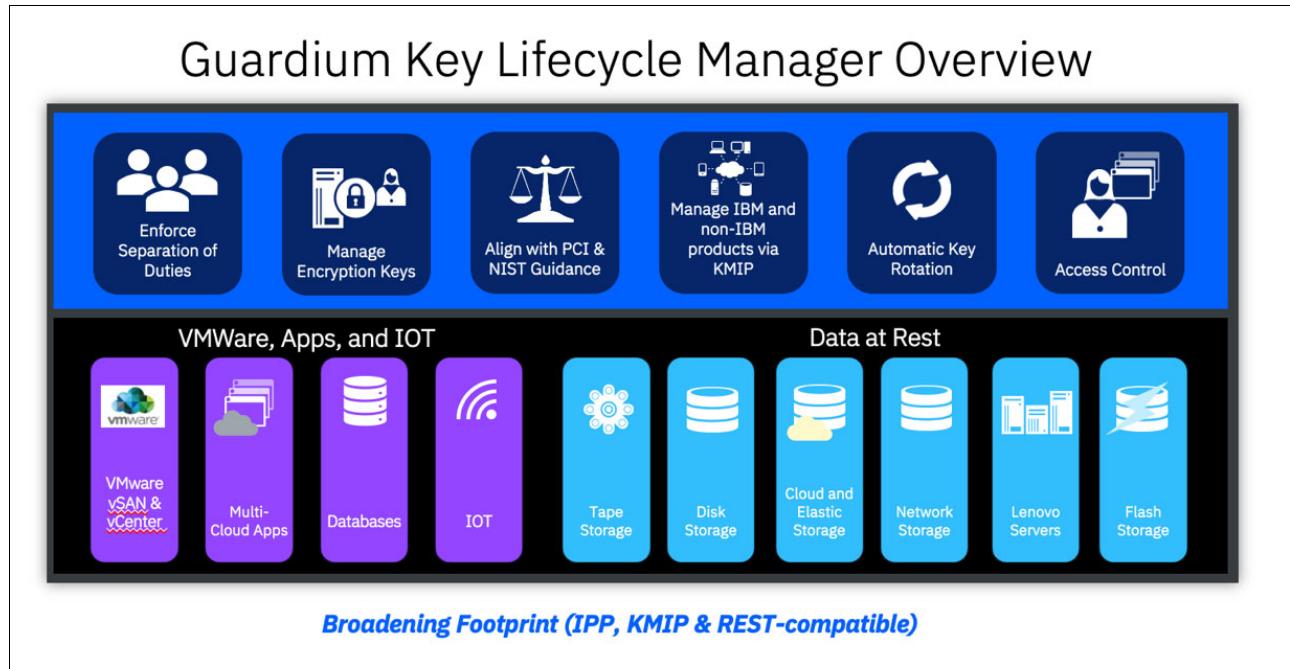


Figure 3-4 IBM Security Guardium Key Lifecycle Manager

Using IBM Security Guardium KLM and AIX 7.2 TL5 LV data encryption

Starting with IBM AIX 7.2 with Technology Level 5, the Logical Volume Manager (LVM) supports the data encryption at the logical volume (LV) level. By using this feature, you can encrypt the at-rest data to protect data exposure because of lost or stolen hard disk drives or because of inappropriately decommissioned computers. The term *data at rest* refers to an inactive data that is stored physically in any digital form.

Each LV is encrypted with a unique key. The logical volume data is encrypted before the data is written to the physical volume. This data is decrypted when it is read from the physical volume.

By default, data encryption is not enabled in logical volumes. You must enable the data encryption option at the volume group level before you enable the data encryption option at the logical volume level.

The following Logical Volume Encryption key protection methods are supported:

- ▶ Paraphrase
- ▶ Keyfile
- ▶ Platform Key Store (PKS); available in the IBM PowerVM firmware of the IBM Power System FW950
- ▶ Key Server- Key Management Interoperability Protocol (KMIP) compliant key management servers

In this section, we demonstrate the use of two key protection methods: Paraphrase and IBM Security Guardium key Lifecycle Manager as the key server.

Before encrypting an AIX LV, and for demonstration purposes, we deploy a Docker image for IBM Security Guardium Key Lifecycle Manager on Red Hat Enterprise Linux 8.4 on IBM Power Systems.

Installing IBM Security Guardium KLM on Red Hat 8.4 on IBM POWER

Deploy IBM Security Guardium Key Lifecycle Manager with PostgreSQL by using podman on Red Hat Enterprise Linux 8 on IBM Power Systems.

Note: Podman is a small, secure, daemon-less container engine for developing, managing, and running Open Container Initiative (OCI)-compliant containers on your Linux system.

The following Host IP addresses are used in this scenario:

- ▶ Host to be protected: IBM AIX 7.2 TL5 LPAR IP address: 192.168.0.201
- ▶ IBM Security Guardium Key Lifecycle Manager Server: Red Hat Enterprise Linux 8.4 on Power Systems IP address: 192.168.0.200

Complete the following steps to start the installation:

1. Install podman on Red Hat Enterprise Linux 8.4 on Power Systems, as shown in Example 3-17.

Example 3-17 Installing podman

```
$ yum install podman
```

- Set up the PostgreSQL Container, as shown in Example 3-18.

Example 3-18 Configuring PostgreSQL

```
$ podman run -d -v sklmpostgresdbvolume:/var/lib/postgresql/data -e  
POSTGRES_PASSWORD=sklmpostgres -e POSTGRES_USER=sklmb41 -e  
POSTGRES_DB=sklmb41 -p 5432:5432 docker.io/library/postgres:latest
```

- Get the IP address of the PostgreSQL database, as shown in Example 3-19.

Example 3-19 Displaying address of the database

```
$ podman ps  
CONTAINER ID  IMAGE                                COMMAND      CREATED  
STATUS        PORTS                               NAMES  
6644541d1d9e  docker.io/library/postgres:latest  postgres    21 seconds ago Up  
21 seconds ago  0.0.0.0:5432->5432/tcp  xenodochial_mendeleev  
  
$podman inspect 6644541d1d9e  
$ podman inspect 6644541d1d9e | grep IP address  
"IP address": "10.88.0.2",
```

- Set up IBM Security Guardium Key Lifecycle Manager Container, as shown in Example 3-20.

Example 3-20 Configuring KLM container

```
$ podman run --name sklm -h sklm.com -p 9443:9443 -p 3801:3801 -p 5696:5696  
-p 1441:1441 -e LICENSE=accept -e SKLMADMIN_USERNAME=skladminuser -e  
LIBERTY_KEY_STORE_PASSWORD=yS1ToNyfKo0hIdIn0_2023@12 -e  
SKLMADMIN_PASSWORD=sklmpswd -e DB_HOST=10.88.0.2 -e DB_PORT=5432 -e  
SKLM_SEED=68d95f0081f1dbfc0b06de9b0916df1c -e DB_PASSWORD=sklmpostgres -e  
DB_TYPE=postgres -e DB_USER=sklmb41 -e DB_NAME=sklmb41 -v  
sklmAppVolume:/opt/ibm/wlp/usr/products docker.io/ibmcom/sklm:latest
```

- Start the IBM Security Guardium Key Lifecycle Manager GUI, as shown in Example 3-21.

Example 3-21 Starting the KLM GUI

<https://192.168.0.200/ibm/SKLM/login.jsp>

- On the Configuration page that appears:
 - Click **License Agreements** to review the license terms.
 - Select the **I accept the terms in the License Agreements** checkbox.
 - Click **Activate License**.
- Obtain the license activation file for IBM Security Guardium Key Lifecycle Manager from IBM Passport Advantage®, and then, rename the file as `sklm.license.zip`.

Note: To obtain license, search for the following product name and part number: IBM Security Guardium Key Lifecycle Manager V4.1.1 Docker License Multiplatform Multilingual.

The IBM Security Guardium Key Lifecycle Manager Login window is shown in Figure 3-5.



Figure 3-5 IBM Security Guardium Key Lifecycle Manager admin console

For demonstration purposes, we use a self-signed certificate, as shown in Figure 3-6.

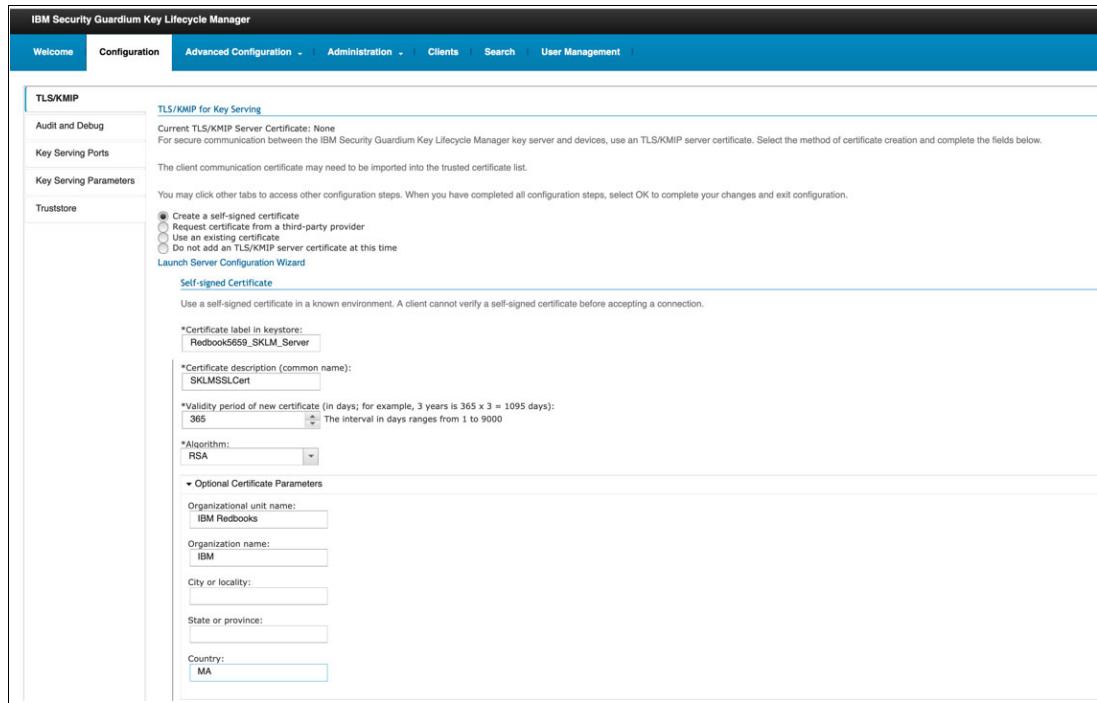


Figure 3-6 IBM Security Guardium Key Lifecycle Manager configuration tab

8. Restart IBM Security Guardium Key Lifecycle Manager Server, as shown in Figure 3-7.

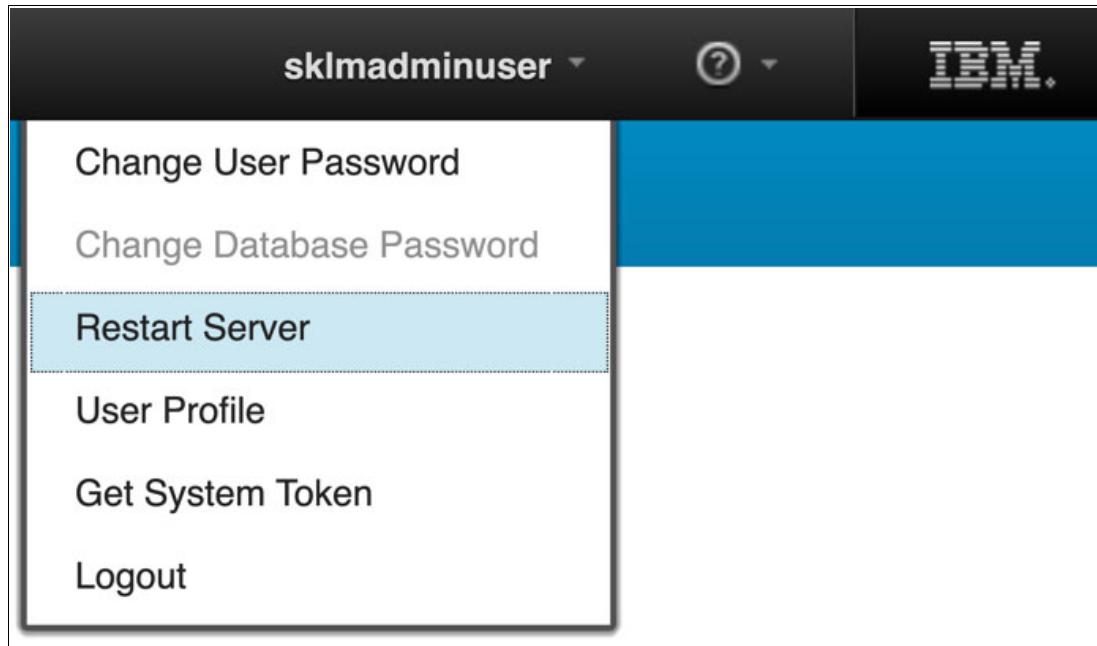


Figure 3-7 Restart server

- Check the status of the server certificate, as shown in Figure 3-8.

Certificates	Communication Type	In Use	Expiration Date	Status	Algorithm	Download
redbook5659_skm_server	TLS/KMIP	✓	Oct 26 2022, 04:45:49 PM GMT+01:00 (GMT+01:00)	OK	RSA	Download

Total: 1 Selected: 0 10 25 50

Figure 3-8 IBM Security Guardium Key Lifecycle Manager advanced configuration tab

- Export the certificate to redbooks5659_skm_serveras, shown in Figure 3-9.

Figure 3-9 Export certificate

- Copy the server certificate redbooks5659_skm_server.crt from the IBM Security Guardium Key Lifecycle Manager Server LPAR to the AIX 7.2 LPAR.

- Log in to the AIX 7.2 LPAR as root and create client certificate, as shown in Example 3-22.

Example 3-22 Create client certificate

```
$ openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout
sysaixPrivateKey.key -out sysaixcert.cer
Generating a RSA private key
```

```
.....+++++
.....+++++
writing new private key to 'sysaixPrivateKey.key'
```

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:MA
State or Province Name (full name) []:Casablanca
Locality Name (eg, city) [Default City]:Casablanca
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:yslaix72
Email Address []:

-
13. Copy the client certificate sysaixcert.crt to the AIX 7.2 LPAR and to the IBM Security Guardium Key Lifecycle Manager Server LPAR.
 14. Import certificate sysaixcert.crt on IBM Security Guardium Key Lifecycle Manager Server LPAR, as shown in Figure 3-10.

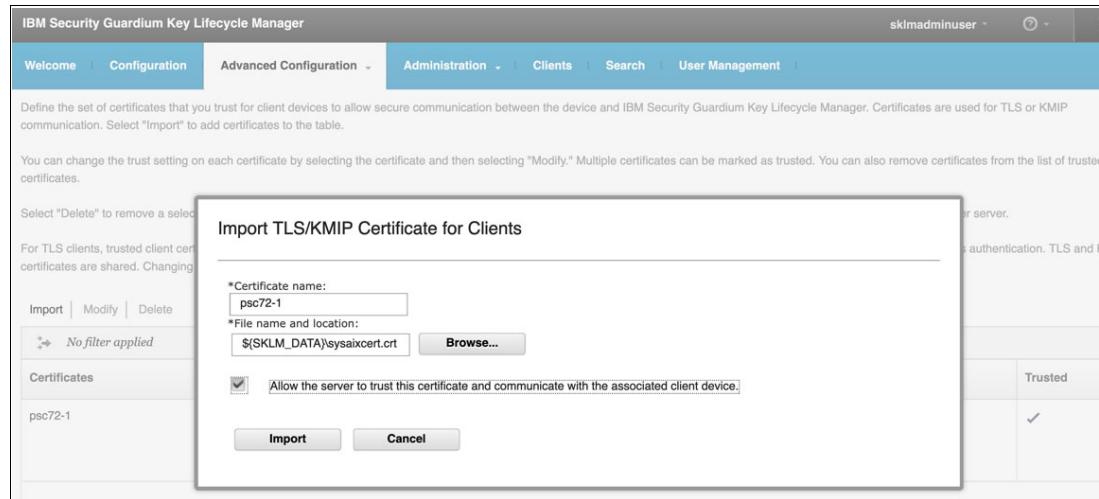


Figure 3-10 Import TLS/KMIP certificate for clients

Encrypting AIX LV by using IBM Security Guardium KLM

To enable logical volume encryption, complete the following steps:

1. Create a volume group with the data encryption option enabled, run the command as shown in Example 3-23 (where securevg is the name of the new volume group, and hdisk1 is the physical volume that is used for the volume group).

Example 3-23 Creating encryption enabled VG

```
$ mkvg -f -k y -y securevg hdisk1
```

2. To create a logical volume with the data encryption option enabled, run the command as shown in Example 3-24 (where securelv is the name of the new logical volume and testvg is the volume group in which the logical volume must be created).

Example 3-24 Creating encryption enabled LV

```
$ mklv -k y -y securelv securevg 10
```

3. To initialize the primary encryption key of the logical volume, run the command as shown in Example 3-25.

Example 3-25 Initializing the primary key for the LV

```
$ hdcryptmgr authinit securelv
```

4. Check the encryption state of varied on volume groups, as shown in Example 3-26.

Example 3-26 Checking encryption state of the volume groups

```
$ hdcryptmgr showvg
VG NAME / ID          ENCRYPTION ENABLED
securevg               yes
ys1vg                  no
rootvg                no
```

5. Verify that the logical volume is encrypted, as shown in Example 3-27.

Example 3-27 Verify the LV encryption

```
1slv securelv
LOGICAL VOLUME:      securelv
VOLUME GROUP:        securevg
LV IDENTIFIER:       00fb284400004c0000000206437c6663.1 PERMISSION:
read/write
VG STATE:            active/complete           LV STATE:
closed/syncd
TYPE:                jfs
WRITE VERIFY:        off
MAX LPs:              512
SIZE:                8 megabyte(s)           PP
COPIES:              1
SCHED POLICY:        parallel
LPs:                 10
PPs:                 10
STALE PPs:           0
BB POLICY:           relocatable
INTER-POLICY:        minimum RELOCATABLE: yes
INTRA-POLICY:         middle UPPER BOUND: 32
MOUNT POINT:          N/A LABEL:           None
MIRROR WRITE CONSISTENCY: on/ACTIVE
EACH LP COPY ON A SEPARATE PV ?: yes
Serialize IO ?:       NO
INFINITE RETRY:      no PREFERRED READ: 0
ENCRYPTION:           yes
```

6. Initialize the primary key for an encrypted logical volume, as shown in Example 3-28. The logical volume is not accessible until the first passphrase method is initialized.

Example 3-28 Initialize the primary key for the encrypted LV

```
$ hdcryptmgr authinit securelv
Enter Passphrase:
Confirm Passphrase:
Passphrase authentication method with name "initpwd" added successfully.
```

7. Check the authentication status and authentication methods, as shown in Example 3-29.

Example 3-29 Check the authentication status and methods

```
$ hdryptmgr showlv securely -v
LV NAME CRYPTO ENABLED AUTHENTICATED ENCRYPTION (%) CONVERSION
securelv yes yes 100 done
-- Authentication methods -----
INDEX TYPE NAME
#0 Passphrase initpwd
```

8. Run the **varyoff** and **varyon** commands on the volume group and check the authentication status, as shown in Example 3-30.

Example 3-30 Deactivate and active the VG

```
$ varyoffvg securevg
$ varyonvg securevg
```

9. Run the commands that are shown in Example 3-31.

Example 3-31 Unlock the LV

```
$ hdryptmgr authunlock securely
Enter Passphrase:
Passphrase authentication succeeded.
$ hdryptmgr showlv securely
LV NAME CRYPTO ENABLED AUTHENTICATED ENCRYPTION (%) CONVERSION
securelv yes yes 100 done
```

10. Add IBM Security Key Lifecycle Manager as an encryption key server. Use the **keysvrmgr** command to add encryption key server to the client LPAR, as shown in Example 3-32.

Example 3-32 Add Security Key Lifecycle Manager as encryption server

```
$ keysvrmgr add -i 192.168.0.200 -s /tmp/ redbooks5659_skm_server.crt -c
/tmp/sysaixcert.cer redbookskeyserver
Key server keyserver1 successfully added
$ keysvrmgr show
List of key servers:
ID PWD IP:PORT
redbookskeyserver N 192.168.0.200:5696
```

Encryption key server information is saved in the ODM KeySvr object class, as shown in Example 3-33.

Example 3-33 Display information in ODM

```
# odmget KeySvr
KeySvr:
    keysvr_id = "redbookskeyserver"
    ip_addr = "192.168.0.200"
    port = 5696
    svr_cert_path = "/tmp/ redbooks5659_skm_server.cer"
    cli_cert_path = /tmp/sysaixcert.cer"
    flags = 0
```

11. Add keyserv authentication method to the logical volume, as shown in Example 3-34.

Example 3-34 Add keyserver as the authentication method for the LV

```
$ hdcryptmgr authadd -t keyserv -n key_sk1m -m redbookskeyserver securelv
Keyserver authentication method with name "key_sk1m" added successfully.
$ hdcryptmgr showlv securelv -v
LV NAME CRYPTO ENABLED AUTHENTICATED ENCRYPTION (%) CONVERSION
securelv yes yes 100 done
-- Authentication methods -----
INDEX TYPE NAME
#0 Passphrase initpwd
#1 Keyserver key_sk1m
```

3.4 Detecting advanced threats, proving compliance, and securing cloud with IBM QRadar

Protecting today's networks from more hostile and clever attackers is a never-ending task. Organizations that want to secure their customers' identities, defend their intellectual property, and avoid business disruption must monitor their environment proactively so that they can discover threats quickly and respond effectively before attackers can cause serious damage.

IBM QRadar Security Information and Event Management (SIEM) is a consolidated security information and event management (SIEM) solution that gives security teams centralized visibility into enterprise-wide security data and actionable insights into the most critical threats.

3.4.1 Enhancing compliance and security in the cloud with IBM QRadar

IBM QRadar SIEM assists security teams in detecting and prioritizing threats across the organization. It also provides intelligent insights that enable teams to respond rapidly to incidents to minimize their impact.

IBM QRadar connects all this disparate information and aggregates similar events into single alerts to accelerate incident investigation and remediation by aggregating log events and network flow data from thousands of devices, endpoints, and applications spread throughout your network.

IBM QRadar support the four key pillars of capability, which empowers its users to address their most important security challenges, as shown in Figure 3-11.

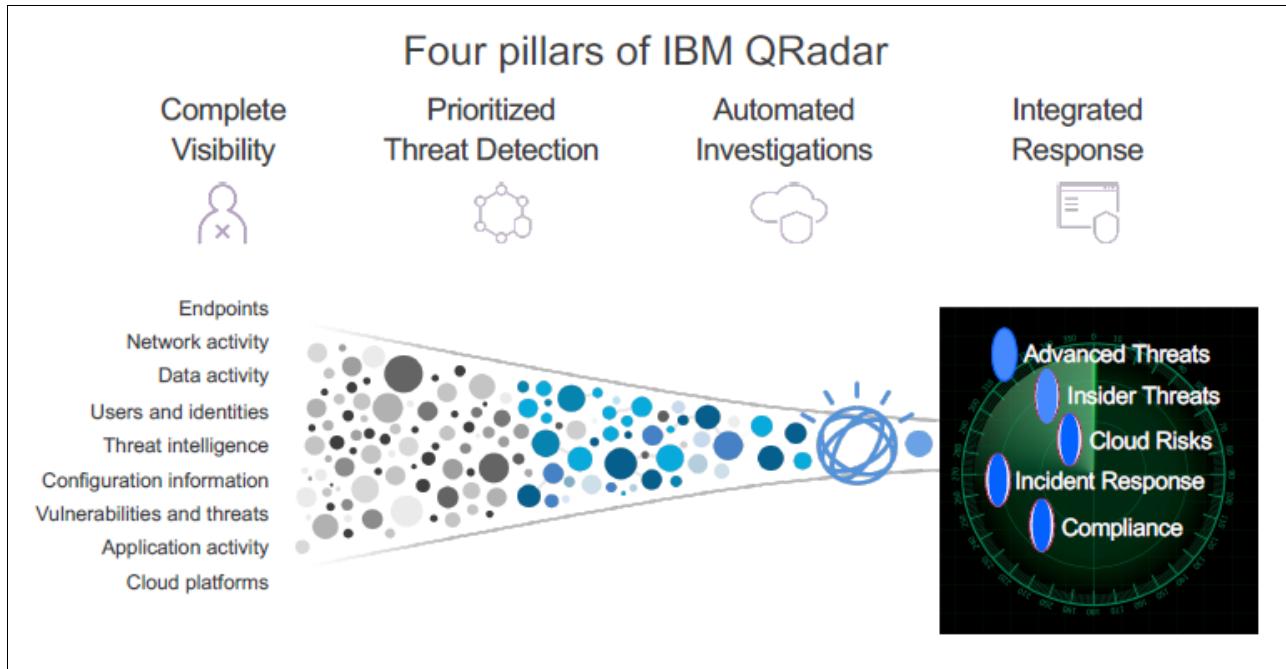


Figure 3-11 Four pillars of IBM QRadar

IBM QRadar provides complete visibility, prioritized threat detection, automated investigations, and integrated response to incidents. Consider the following points:

- ▶ IBM QRadar gives IBM clients complete visibility into their environments by collecting data from networks, servers, endpoints, cloud environments, applications, and even other security tools and data lakes.
 - ▶ IBM QRadar applies advanced analytics to prioritize the most critical threats by using methods, such as the MITRE ATT&CK framework, advanced modeling including behavioral analysis, and correlation with global threat intelligence sources, such as IBM X-Force.
 - ▶ IBM QRadar automates investigations through machine learning and artificial intelligence (AI), which reduces the time between threat detection and analysis. This ability allows security teams to investigate and triage threats more quickly by using fewer resources.
- IBM QRadar also discovers anomalies, patterns, and correlations within large data sets to predict outcomes. It supports federated searching, which does not require security data to be moved because it can be included in a search.
- ▶ One of the biggest concerns IBM hears from customers is the difficulties that they encounter while attempting to find skilled security analysts because of budgetary issues or the inability to find and hire qualified individuals. This issue severely hampers their ability to triage, investigate, and remediate identified threats.

IBM QRadar on Cloud

IBM QRadar on Cloud provides the security monitoring that you need and the ability to adapt your monitoring operations as your requirements change in an environment where security requirements are dynamic.

You can protect your network and meet compliance monitoring and reporting requirements while lowering your total cost of ownership with IBM QRadar on Cloud. You do not need to install any extra hardware on-premises besides a data gateway appliance to connect to IBM QRadar.

You benefit from all of the IBM QRadar features without having to invest in the hardware and software that are required for an on-premises IBM QRadar deployment, as shown in Figure 3-12.

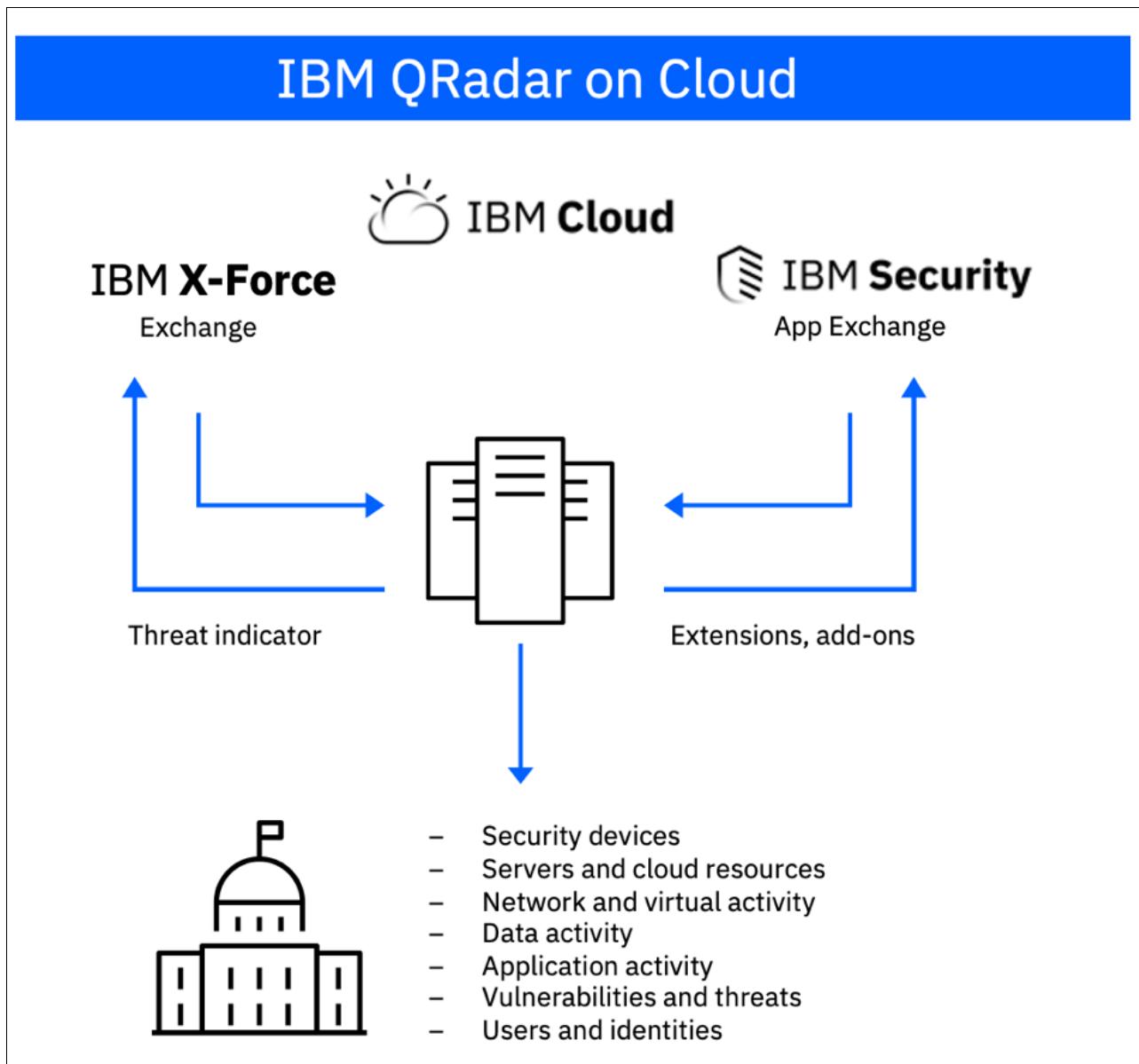


Figure 3-12 IBM QRadar on Cloud

IBM QRadar on Cloud provides some of the capabilities as those provided by IBM QRadar on premises (see Table 3-1).

Table 3-1 IBM QRadar On premises versus on Cloud

Service component	On-premises	IBM QRadar on Cloud
Capital expense (CAPEX) budget item	✓	
OPEX budget item	✓	✓
IBM installation, deployment, and upgrade		✓
IBM professionally managed infrastructure		✓
System health monitoring		✓
Configure data collection (DSMs) ^a	✓	✓
Compliance reporting	✓	✓
Advanced attack detection	✓	✓
Incident detection and management ^a	✓	✓
Asset modeling and vulnerability correlation	✓	✓
QVM ^b , QFlows	✓	✓
QNI ^c	✓	✓
IBM QRadar ^b Advisor with Watson	✓	✓
App Exchange ^c	✓	✓
Admin Access	root	SaaS Admin

a. DSM = Device support module

b. QVM = QRadar Vulnerability Manager

c. QNI = QRadar Network Insights

Using IBM QRadar with Device Support Module or Parser for IBM AIX, IBM i, and Linux

In this section, we use the IBM QRadar Community Edition 7.3.3 to demonstrate how to install Device Support Module (DSM) for operating systems that are supported by IBM Power Systems (the same steps apply when IBM QRadar on Cloud is used). For production environments, use the full version of IBM QRadar or IBM QRadar on Cloud.

Community Edition is a fully featured, no-cost version of QRadar that is low memory, low EPS, and includes a perpetual license. This version is limited to 50 events per second and 5,000 network flows a minute, supports applications, but is based on a smaller footprint for nonenterprise use.

IBM QRadar Community Edition is packaged as an OVA, which makes it easier to get started with IBM QRadar on your virtualization platform of choice. The OVA file is easily downloaded and requires minimal configuration to get IBM QRadar up and running.

IBM QRadar Community Edition 7.3.3 includes the following system requirements:

- ▶ Memory minimum: 8 GB RAM or 10 GB with applications
- ▶ Disk space minimum: 250 GB
- ▶ CPU: 2 cores (minimum) or 6 cores (recommended)
- ▶ One network adapter with access to the internet
- ▶ A static public and private IP addresses for IBM QRadar Community Edition
- ▶ The assigned hostname must be a fully qualified domain name

To install IBM QRadar Community Edition in a VM, complete the following steps:

1. Download the QRadar Community Edition OVA file from this [IBM Developer web page](#).
2. Create a VM with the OVA file that meets the requirements.
3. Log in as the root user and enter a password.
4. Start the set-up process by running the command that is shown in Example 3-35.

Example 3-35 Starting the setup process

```
$ /root/setup
```

5. Press **Enter** to accept the CentOS user license agreement (EULA).
6. Enter a password for the admin account.
7. Restart the appliance by running the command that is shown in Example 3-36.

Example 3-36 Restarting the appliance

```
reboot
```

8. Log in to the IBM QRadar Community Edition user interface as the admin user and accept the EULA.

9. Access IBM QRadar Community Edition in a web browser at https://<ip_address>/console (see Figure 3-13).



Figure 3-13 QRadar community edition console

10. Install the most recent version of the following RPMs on your IBM QRadar Console (see Example 3-37):

- ▶ DSM Common RPM
- ▶ IBM AIX Server DSM RPM
- ▶ IBM AIX Audit DSM
- ▶ IBM i DSM RPM

Example 3-37 installing DSM RPMs

```
sudo mount /opt/ibm/cloud/iso/QRadarCE2019_14_0_20191031163225.GA.iso  
/media/cdrom  
$ cd /media/cdrom/post/dsmrpms  
$ yum -y install DSM-DSMCommon-7.3-20170407183723.noarch.rpm  
$ yum -y install DSM-IBMAIXAudit-7.3-20160908133313.noarch.rpm  
$ yum -y install DSM-IBMAIXServer-7.3-20161201184135.noarch.rpm  
$ yum -y install DSM-IBMiSeries-7.3-20160908133313.noarch.rpm
```

11.On the Admin tab, click **Deploy Changes**, as shown in Figure 3-14.

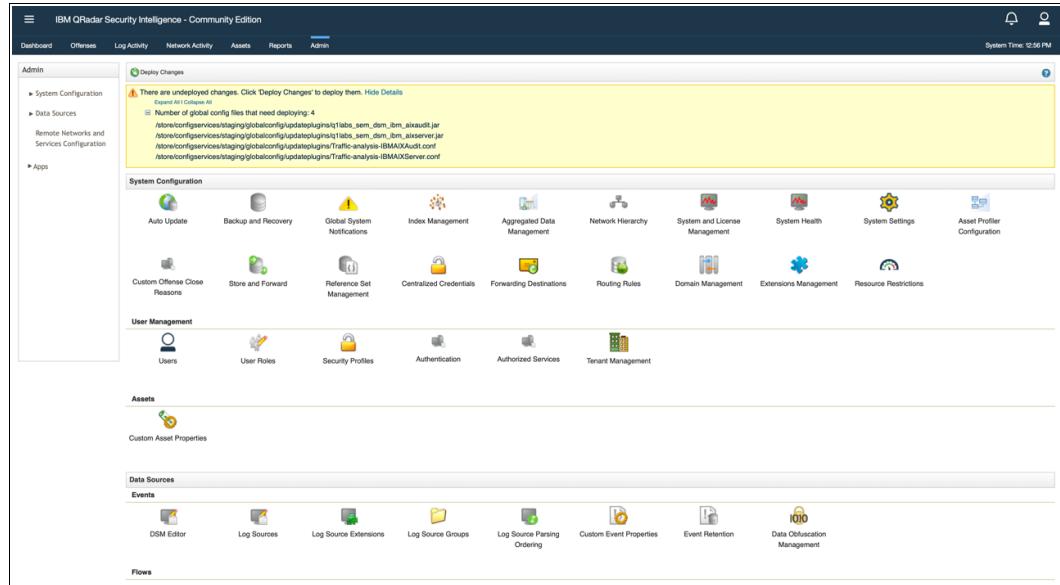


Figure 3-14 Deploying changes to apply DSM RPMs

12.On the Admin tab, select **Advanced** → **Restart Web Server**.

13.Update the license file, as shown in Example 3-38.

Example 3-38 Updating license file

```
if [ -f /opt/qradar/ecs/license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/qradar/ecs/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt ; fi ; if [ -f /usr/eventgnosis/ecs/license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /usr/eventgnosis/ecs/license.txt ; fi ; if [ -f /opt/qradar/conf/templates/ecs_license.txt ] ; then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDF0gB1WaXwok0Dc:12/31/20" > /opt/qradar/conf/templates/ecs_license.txt ; fi
```

14.Log in to the QRadar Console.

15.Click the **Log Activity** tab.

IBM AIX Audit DSM events with IBM QRadar

IBM QRadar provides the IBM AIX Audit and IBM AIX Server DSMs to collect and parse audit or operating system events from IBM AIX devices.

The IBM AIX Server DSM collects operating system and authentication events by using syslog for users that interact or log in to your IBM AIX appliance.

Configuring IBM AIX Server DSM

To integrate IBM AIX Server events with QRadar, complete the following steps:

1. Download and install the most recent version of the following RPMs to your IBM QRadar Console:
 - DSM Common RPM
 - IBM AIX Server DSM RPM
2. Configure your IBM AIX Server device to send syslog events to IBM QRadar.
3. Configure a syslog-based log source for your IBM AIX Server device. Use the following protocol-specific parameters:
 - Log Source Type: IBM AIX Server
 - Protocol Configuration Syslog

Note: The procedure is described in “Using IBM QRadar with Device Support Module or Parser for IBM AIX, IBM i, and Linux” on page 93.

2. Configure your IBM AIX Server device to send syslog events to IBM QRadar.
3. Configure a syslog-based log source for your IBM AIX Server device. Use the following protocol-specific parameters:
 - Log Source Type: IBM AIX Server
 - Protocol Configuration Syslog

To configure your IBM AIX Server device to send syslog events to IBM QRadar, log in to your IBM AIX LPAR as a root user and configure the syslogd, as shown in Example 3-39.

Example 3-39 Configuring syslogd

```
$ vi /etc/syslog.conf file  
Add the following line to the file: auth.info @QRadar_IP_address  
$ refresh -s syslogd
```

Configuring IBM AIX Audit DSM

The IBM AIX Audit DSM collects detailed audit information about events that occur on your IBM AIX LPAR.

To integrate IBM AIX Audit events with QRadar, complete the following steps:

1. Download the latest version of the IBM AIX Audit DSM from this [IBM Support web page](#).
2. For syslog events, complete the following steps:
 - a. Configure your IBM AIX Audit device to send syslog events to IBM QRadar.
 - b. Add an IBM AIX Audit log source. Use the following IBM AIX Audit-specific values in the log source configuration:
 - Log Source Type: IBM AIX Audit
 - Protocol Configuration: syslog

Note: The procedure is described in “Using IBM QRadar with Device Support Module or Parser for IBM AIX, IBM i, and Linux” on page 93.

3. For log file protocol events, complete the following steps:
 - a. Configure your IBM AIX Audit device to convert audit logs to the log file protocol format.
 - b. Configure a log file protocol-based log source for your IBM AIX Audit device. Table 3-2 lists protocol-specific values in the log source configuration.

Table 3-2 Log source parameters for IBM AIX Audit device

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Log file
Service Type	The protocol to retrieve log files from a remote server.
Remote Port	If the host for your event files uses a nonstandard port number for FTP, SFTP, or SCP, adjust the port value.
SSH Key File	If you select SCP or SFTP as the Service Type, use this parameter to define an SSH private key file. When you provide an SSH Key File, the Remote Password parameter is ignored.
Remote Directory	The directory location on the remote host where the files are retrieved. Specify the location relative to the user account you use to log in.
FTP File Pattern	The FTP file pattern must match the name that you assigned to your AIX audit files with the -n parameter in the audit script.
FTP Transfer Mode	ASCII is required for text event logs that are retrieved by the log file protocol by using FTP.
Processor	None
Event Generator	LineByLine

To collect syslog audit events from your IBM AIX Audit device, redirect your audit log output from your IBM AIX device to the IBM QRadar Console or Event Collector. Complete the following steps:

1. Log in to your IBM AIX appliance. Configure the auditing streams mode, as shown in Example 3-40.

Example 3-40 Auditing streams mode

```
$ vi /etc/security/audit/config file
Add the following line to the file:
binmode = off
streammode = on
```

2. Edit the classes section to specify which classes to audit, as shown in Example 3-41.

Example 3-41 Edit streamcmds file

```
$ vi /etc/security/audit/streamcmds file
Add the following line to the file:
/usr/sbin/auditstream | /usr/sbin/auditselect -m -e "command != logger &&
command != auditstream && command != auditpr && command != auditselect" | auditpr
-t0 -h eclrRdi -v | awk -u 'NR%2{printf "%s ",$0;next}{print;}' |
/usr/bin/logger -p local0.debug -r &
```

3. Edit the syslog configuration file to specify a debug entry and the IP address of the IBM QRadar Console or Event Collector, as shown in Example 3-42.

Example 3-42 Configure syslog

```
* .debug @ip_address  
$ refresh -s syslogd  
$ audit start
```

To configure IBM AIX Audit DSM to send log file protocol events to IBM QRadar, complete the following steps:

1. Log in to your IBM AIX LPAR.
2. Configure the audit configuration file, as shown in Example 3-43.

Example 3-43 Start auditing

```
$ vi etc/security/audit/config  
Edit the Start section to enable the binmode element.  
binmode = on  
In the Classes section, edit the configuration to determine which classes are  
audited.  
$ audit start
```

3. Download the audit script from the [IBM Support web page](#).
4. Copy the audit script to a folder on your IBM AIX LPAR. Run the audit script, as shown in Example 3-44.

Example 3-44 Run audit script

```
$ ./audit.pl  
$ audit start
```

Linux operating system DSM for IBM Security QRadar

The Linux operating system DSM for IBM QRadar records Linux operating system events and forwards the events by using syslog or syslog-ng.

The Linux OS DSM supports the following event types:

- ▶ Cron
- ▶ HTTPS
- ▶ FTP
- ▶ NTP
- ▶ Simple Authentication Security Layer (SASL)
- ▶ SMTP
- ▶ SNMP
- ▶ SSH
- ▶ Switch User (SU)
- ▶ Pluggable Authentication Module (PAM) events

To configure Linux OS to forward events by using the syslog protocol, complete the following steps:

1. Log in to your Linux OS server as a root user. Then, configure syslogd, as shown in Example 3-45.

Example 3-45 Configure syslogd

```
$ vi /etc/rsyslog.conf
Add the following facility information:
authpriv.*@<ip_address>
where:
<ip_address> is the IP address of IBM QRadar.
$ service syslog restart
```

2. Log in to the IBM QRadar console and add a Linux OS log source on the IBM QRadar console.

To configure Red Hat Enterprise Linux 8 to send audit logs to IBM QRadar, complete the following steps:

1. Log in to your Linux OS device as a root user and run the commands as shown in Example 3-46.

Example 3-46 Run the commands on your device

```
$ yum install audit audispd-plugins
$ service auditd start
$ chkconfig auditd on
```

2. Open the /etc/audit/plugins.d/syslog.conf file and verify that the parameters match the values, as shown in Example 3-47.

Example 3-47 Confirm audit syslog configuration

```
active = yes
direction = out
path = builtin_syslog
type = builtin
args = LOG_LOCAL6
format = string
```

3. Open the /etc/rsyslog.conf file and add the line as shown in Example 3-48 at the end of the file.

Example 3-48 Change syslogd configuration

```
local6.* @@<QRadar_Collector_IP_address>
```

- Run the commands, as shown in Example 3-49.

Example 3-49 restart auditd and syslogd

```
$ service auditd restart
$ service syslog restart
```

- Log in to the IBM QRadar Console. At the Admin Tab, select **Log Sources**, as shown in Figure 3-15.

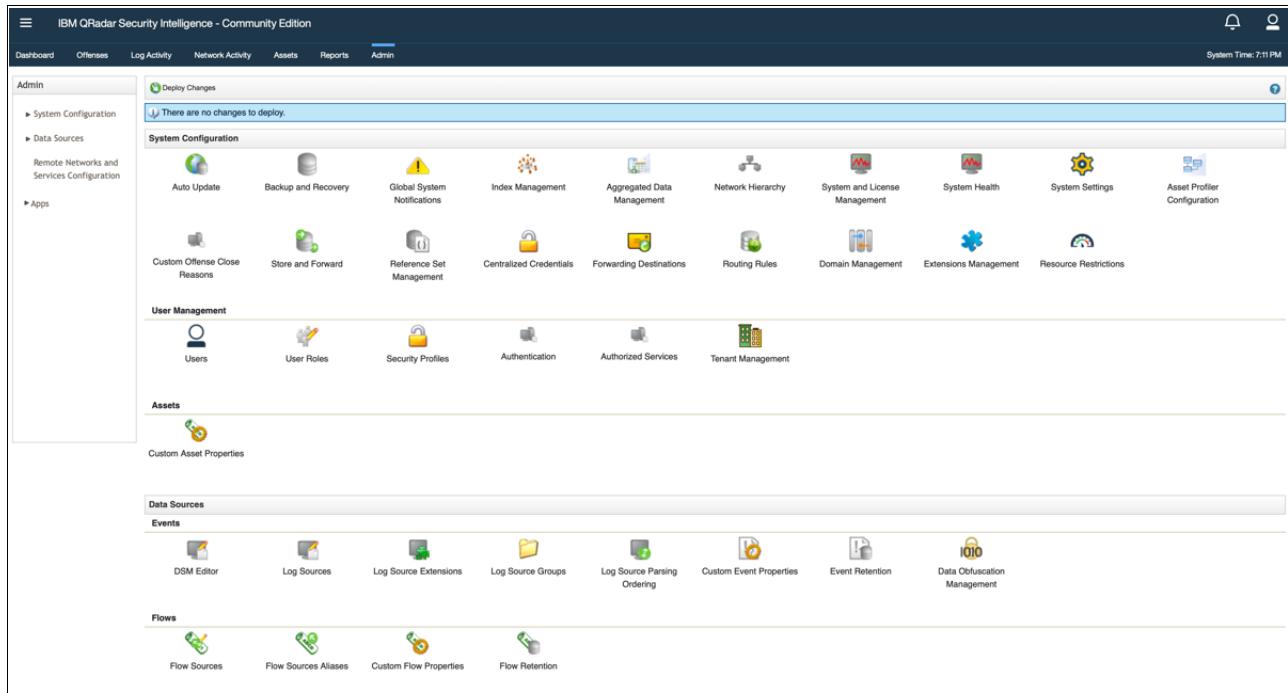


Figure 3-15 Admin Tab and Log Sources selection

6. Add a Linux OS log source on the IBM QRadar Console by clicking **Add**, as shown in Figure 3-16.

Add a log source

Log Source Name	Redbook-PowerSecure
Log Source Description	<input type="text"/>
Log Source Type	Linux OS
Protocol Configuration	Syslog
Log Source Identifier	192.168.0.121
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: ysl
Coalescing Events	<input checked="" type="checkbox"/>
Incoming Payload Encoding	UTF-8
Store Event Payload	<input checked="" type="checkbox"/>
Please select any groups you would like this log source to be a member of:	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 3-16 Add log source: Log source Identifier is the IP address source of Red Hat Power Systems LPAR

7. Display logs by Source IP under **Log Sources** → **Quick Filter** → **IP Source**, as shown in Figure 3-17.

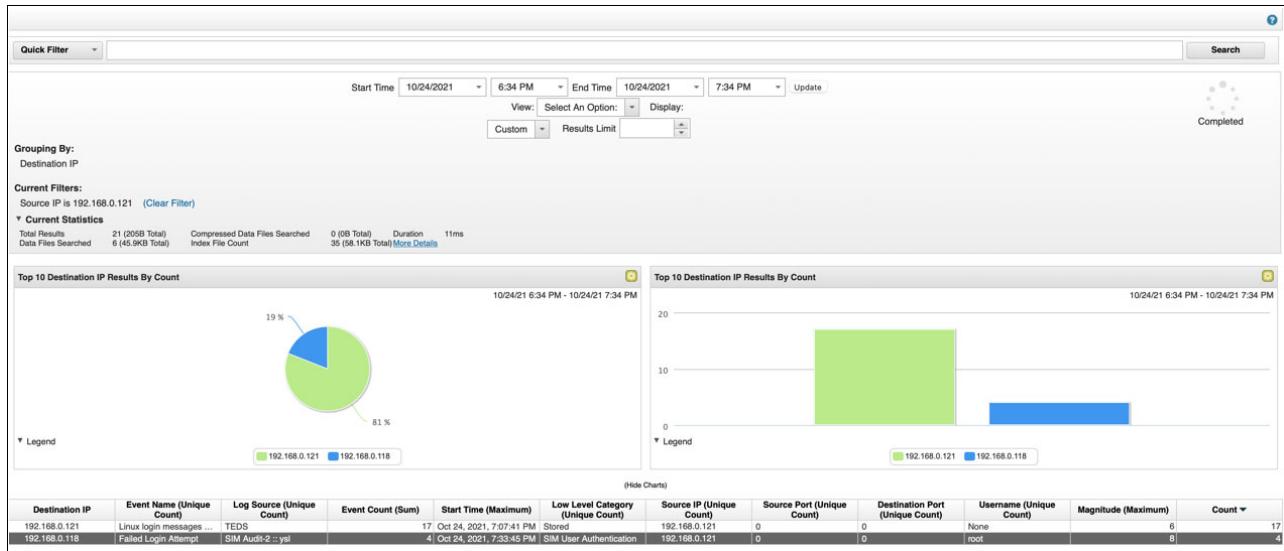


Figure 3-17 Filter by Source IP

Figure 3-18 shows multiple failed login attempt events that were gathered from the Red Hat Enterprise Linux on Power Systems LPAR.

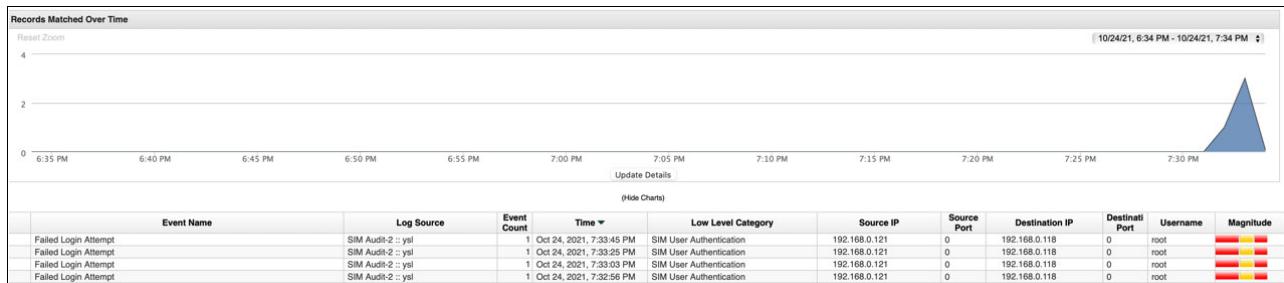


Figure 3-18 Details of Failed Login Attempt Event on IBM QRadar Console

IBM QRadar DSM for IBM System i

The IBM QRadar DSM for IBM i collects audit records and event information from IBM i LPARs.

When you send your log file data to IBM Security QRadar, it is first parsed inside a Device Support Module (DSM) so that QRadar can fully use the normalized data for event and offense processing. Sometimes, you encounter data that cannot be correctly parsed, or you are dealing with multiple log sources that are running on one physical system.

Table 3-3 lists the specifications for the IBM i DSM.

Table 3-3 IBM i DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM i
Supported versions	V7R1 and later
RPM file name	DSM-IBMi-QRadar_version-build_number.noarch.rpm
Protocol	<ul style="list-style-type: none"> ▶ Log File Protocol ▶ Syslog
Event Format	Common Event Format (CEF); CEF:0 is supported.
Recorded event types	Audit records and events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No

To collect events from IBM i systems, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM i DSM RPM from the [IBM Support web page](#) onto your IBM QRadar Console.
2. Configure your IBM i system to communicate with IBM QRadar.
3. Add an IBM i log source on the IBM QRadar Console by using Table 3-4 to configure the parameters that are required to collect IBM i events.

Table 3-4 IBM i log source parameters

Parameter	Value
Log source type	IBM i
Protocol configuration	<p>Log File</p> <p>If you use the PowerTech Interact or LogAgent for System i software to collect CEF formatted syslog messages, you must select the Syslog option.</p>
Service type	Secure File Transfer Protocol (SFTP)

Note: For more information about QRadar for IBM i, see the following IBM Documentation and IBM Support web pages:

- ▶ [Configuring IBM i to integrate with IBM QRadar](#)
- ▶ [Manually extracting journal entries for IBM i](#)
- ▶ [Pulling Data when you use the Log File Protocol](#)
- ▶ [Configuring Townsend Security Alliance LogAgent to integrate with QRadar](#)
- ▶ [IBM i sample event message](#)
- ▶ [How to create a passwordless SSH log in for log file protocol](#)
- ▶ [Commonly Asked IBM i \(AS/400 iSeries\) DSM Integration Questions for QRadar](#)

IBM QRadar Content Pack Compliance

The Compliance content pack provides rules and reports content to implement general compliance and policy controls, as shown in Figure 3-19.



Figure 3-19 IBM Security Content Pack

The content pack contains daily, weekly, and monthly reporting about the following topics:

- ▶ Authentication Activity
- ▶ Attacker and Target Summary
- ▶ Top Malware Activity
- ▶ DoS Activity
- ▶ Exploit Activity
- ▶ Policy Violation Summary
- ▶ Account Activity
- ▶ Remote Access Activity
- ▶ Web Access Summary
- ▶ Traffic Summary

For example, the PCI content pack provides rules and reports content to implement Payment Card Industry controls. The content pack contains daily reporting about the following topics:

- ▶ Policy Violation Summary
- ▶ Network Traffic Monitoring
- ▶ Audit of Data
- ▶ User management
- ▶ Vulnerability monitoring
- ▶ Incident Response
- ▶ Malware Monitoring
- ▶ Remote attacks
- ▶ Access to sensitive system

The Extensions Management window in IBM QRadar is used to add applications or content extensions to your deployment to improve the function of IBM QRadar. Extensions can contain content, such as rules, reports, searches, reference sets, and dashboards.

Extensions can also install applications that deliver specific new functions to IBM QRadar. The About tab outlines the contents of the extension that are being added to IBM QRadar. Content extensions that are installed do not disrupt IBM QRadar user activity or restart services.

To use PCI content Pack, complete the following steps:

1. Log in to the IBM QRadar Console as an administrator.
2. Download the file to your Notebook or workstation from the [X-Force App Exchange](#). Then, select the PCI content to download, as shown in Figure 3-20.

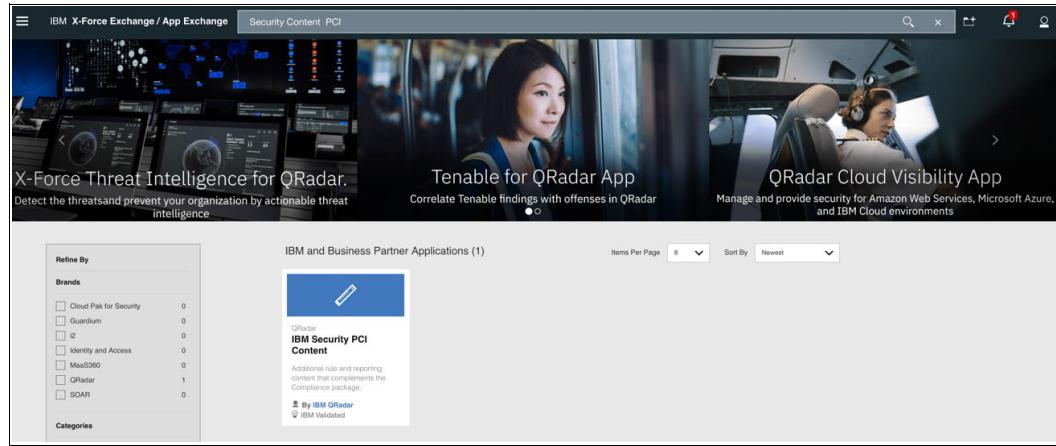


Figure 3-20 IBM Security PCI Content download

3. Click the **Admin** tab and then, click **Extensions Management** in the System Configuration section.
4. To upload an extension, click **Add** and select the extension to upload.
5. To install the extension immediately, select the **Install immediately** checkbox and then, click **Add**, as shown in Figure 3-21.

The screenshot shows a modal dialog box titled 'Add a New Extension'. Inside the dialog, there is a text input field labeled 'From local storage:' containing the file path 'ContentPackage-Internal-PCI_Port-1.zip'. To the right of the input field is a 'Browse' button. Below the input field is a checkbox labeled 'Install immediately' which is checked. At the bottom of the dialog are two buttons: a large blue 'Add' button on the left and a white 'Cancel' button on the right.

Figure 3-21 Upload Content Package PCI

6. A preview of the content is displayed before the extension is installed. The content items are compared to content items that are in the deployment.

If the content items exist, you can choose to overwrite them or to keep the existing data. If you choose to keep the existing data, no updated content extension items are installed.

7. Select **Overwrite** when prompted to add the new data to your IBM QRadar appliance.

The installation is complete, and the status is displayed in IBM QRadar.

8. In the Report tab, use Report Wizard to generate PCI DSS Compliance Reports for IBM Power Systems, as shown in Figure 3-22.

The screenshot shows the IBM QRadar Security Intelligence interface. The top navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports (which is the active tab), Admin, and User Analytics. Below the navigation is a search bar with the text 'Group: PCI'. To the right of the search bar are buttons for 'Manage Groups', 'Actions', 'Hide Inactive Reports', and a search icon. Further right is a link to 'View the IBM App Exchange for'. The main content area is titled 'Reports' and contains a table. The table has columns for 'Report Name', 'Group', and 'Schedule'. The 'Report Name' column lists numerous PCI-DSS related reports such as 'Network Traffic Volume', 'Top Users by Remote Access Activity', 'PCI 8.1 - User Account Additions and Changes (Weekly)', etc. The 'Group' column shows categories like 'Compliance, Executive, Network Ma...', 'FISMA, GLBA, GSX-Memo22, HIPAA...', 'PCI', etc. The 'Schedule' column indicates the frequency of each report, mostly set to 'Daily' or 'Weekly'.

	Report Name	Group	Schedule
	Network Traffic Volume	Compliance, Executive, Network Ma...	Daily
	Top Users by Remote Access Activity	FISMA, GLBA, GSX-Memo22, HIPAA...	Weekly
	Network Traffic Volume	Compliance, Executive, Network Ma...	Weekly
	PCI 8.1 - User Account Additions and Changes (Weekly)	PCI	Weekly
	PCI 8.1 - User Account Additions and Changes (Monthly)	PCI	Monthly
	PCI 7.1 - Access to Cardholder and Trusted Systems (Weekly)	PCI	Weekly
	PCI 7.1 - Access to Cardholder and Trusted Systems (Monthly)	PCI	Monthly
	PCI 6.6 - Attacks against Public Facing Applications or Services (Weekly)	PCI	Weekly
	PCI 6.6 - Attacks against Public Facing Applications or Services (Monthly)	PCI	Monthly
	PCI 5.2 - Malware (Weekly)	PCI	Weekly
	PCI 5.2 - Malware (Monthly)	PCI	Monthly
	PCI 4.1 - Traffic to Trusted Segments from Untrusted Segments (Weekly)	PCI	Weekly
	PCI 4.1 - Traffic to Trusted Segments from Untrusted Segments (Monthly)	PCI	Monthly
	PCI 2.3 - Traffic to Trusted Segments (Weekly)	PCI	Weekly
	PCI 2.3 - Traffic to Trusted Segments (Monthly)	PCI	Monthly
	PCI 2.1 - Vendor Defaults (Monthly)	PCI	Monthly
	PCI 12.9 Incident Response (Offense Summary) - Weekly	PCI	Weekly
	PCI 10.2 - User Accounts Additions by Admin (Weekly)	PCI	Weekly
	PCI 10.2 - User Accounts Additions by Admin (Monthly)	PCI	Monthly
	PCI 10 - Audit of Data (Weekly)	PCI	Weekly
	PCI 10 - Audit of Data (Monthly)	PCI	Monthly
	PCI 1.3 - Traffic Summaries (Weekly)	PCI	Weekly
	PCI 1.3 - Traffic Summaries (Monthly)	PCI	Monthly
	PCI 1.2.1b - Inbound and Outbound Traffic (Weekly)	PCI	Weekly
	PCI 1.2.1b - Inbound and Outbound Traffic (Monthly)	PCI	Monthly
	PCI 1.2.1a - Internal Network (not DMZ) to Internet (Weekly)	PCI	Weekly
	PCI 1.2.1a - Internal Network (not DMZ) to Internet (Monthly)	PCI	Monthly
	PCI 6.1 - Vulnerabilities	PCI	Weekly
	PCI 11.3/11.2 Vulnerability Report	PCI	Weekly
	PCI 7.1 - Access to Cardholder and Trusted Systems	PCI	Daily
	PCI 10 - Audit of Data	PCI	Daily
	PCI 10.2 - User Accounts Additions by Admin	PCI	Daily
	PCI 8.1 - User Account Additions and Changes	PCI	Daily
	PCI 6.6 - Attacks against Public Facing Applications or Services	PCI	Daily
	PCI 5.2 - Malware or Virus Clean Failed	PCI, Security	Daily
	PCI 5.2 - Top Malware Activity	PCI, Security	Daily
	PCI 5.2 - Malware	PCI	Daily
	PCI 4.1 - Traffic to Trusted Segments from Untrusted Segments	PCI	Daily
	PCI 2.3 - Traffic to Trusted Segments	PCI	Daily
	PCI 2.2 - Server Function	PCI	Daily

Figure 3-22 PCI-DSS reports

3.5 Modernizing security with IBM Cloud Pak for Security

IBM Cloud Pak for Security is an open security platform that connects to your data sources to generate deeper insights and enables you to act faster with automation. Whether your data is on IBM or third-party tools, on-premises, or multiple cloud environments, the platform helps you to find and respond to threats and risks, all while leaving your data where it is.

Therefore, you can uncover hidden threats, make more informed risk-based decisions, and respond to incidents faster.

IBM Cloud Pak for Security features the following benefits:

- ▶ Modular capabilities can be used and licensed individually or together and combined with platform services to unify data and workflows across different security teams. As your program grows, you can easily add capabilities as you need them.
- ▶ With platform services that work across the security capabilities, you can reduce complexity and gain efficiency by connecting to tools, use the data across Cloud Pak for Security capabilities, and bring tools and teams together with various features, such as case management, orchestration, and automation. Furthermore, Cloud Pak for Security includes development tools to enable customers and Business Partners to connect to custom data sources and build out more capabilities to run on the platform.
- ▶ Built on open source software that was contributed to the Open Cybersecurity Alliance (OCA) and extended through an open system of data connectors, Cloud Pak for Security helps promote open and interoperable security. It also supports the tools that you use or can use in the future (see Figure 3-23).

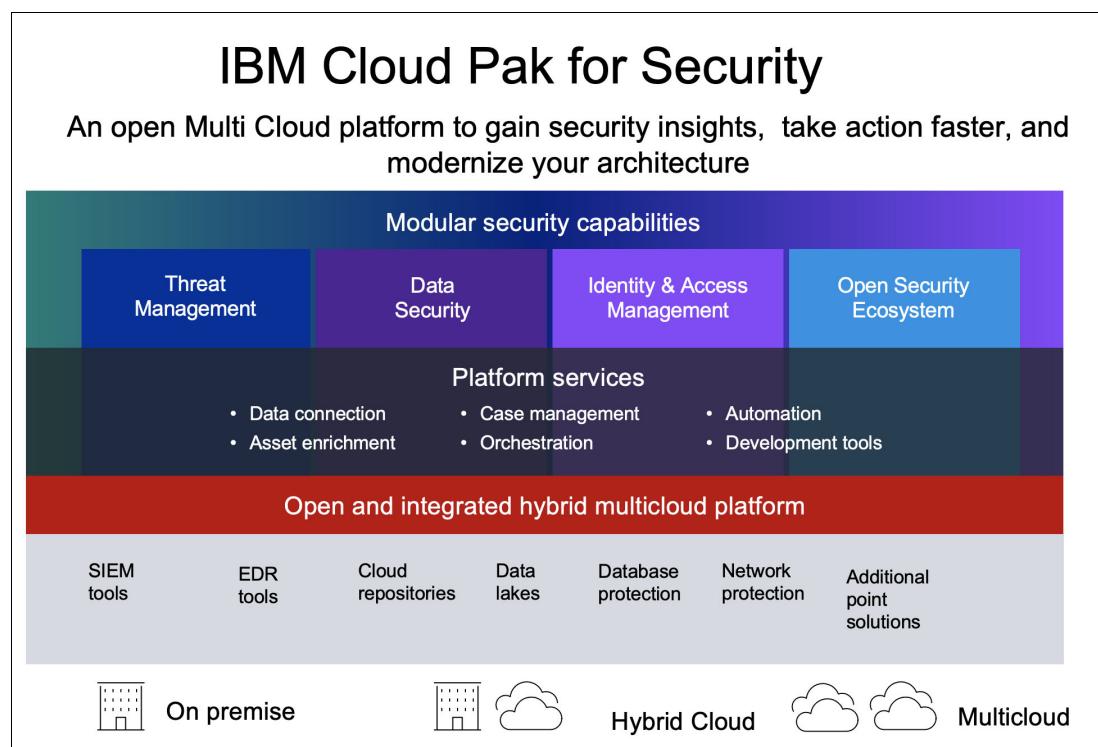


Figure 3-23 IBM Cloud Pak for Security

For more information, see [IBM Cloud Pak for Security Documentation](#).



IBM Power Systems advanced security implementation scenarios

This chapter describes implementation scenarios for advanced IBM Power Systems security built-in capabilities that are based on IBM PowerSC.

This chapter also discusses IBM PowerSC Multi-Factor Authentication (MFA), which helps to raise the assurance level of Power Systems and Power Systems Virtual Server by requiring users to log in with multiple authentication factors.

This chapter includes the following topics:

- ▶ 4.1, “PowerSC for AIX” on page 110
- ▶ 4.2, “Security and compliance tools for IBM i” on page 114
- ▶ 4.3, “PowerSC for IBM i” on page 123
- ▶ 4.4, “PowerSC for Linux” on page 125
- ▶ 4.5, “Allowing and denying list management” on page 127
- ▶ 4.6, “PowerSC MFA example configuration” on page 137
- ▶ 4.7, “PowerSC MFA 2.0 high availability” on page 155
- ▶ 4.8, “PowerSC MFA out-of-band authentication” on page 162
- ▶ 4.9, “PowerVC security services” on page 162

4.1 PowerSC for AIX

This section covers the following topics:

- ▶ Installing the PowerSC Server on AIX Server
- ▶ Installing the PowerSC Agent on a AIX Server
- ▶ Compliance checking

4.1.1 Prerequisites

Before you install the PowerSC GUI server or PowerSC GUI agent on AIX, ensure that the following prerequisites are met:

- ▶ The following products are installed:
 - PowerSC GUI server and agent AIX: Java 8, 64-bit
 - PowerSC GUI server: AIX 7.1 or later
 - PowerSC GUI agent: AIX 7.1.2.15 or later
- ▶ The sendmail daemon is running for the PowerSC GUI server
- ▶ The `bos.loc.utf.<LANG>` fileset is installed so that the PowerSC GUI correctly displays profile rule descriptions in languages other than English

The PowerSC GUI server listens on TCP port 443 for all communication from the PowerSC GUI agent, or from any web browser.

The PowerSC GUI agent that is running on each endpoint listens on TCP port 11125 for all communication from the PowerSC GUI server.

Note: At the time of this writing, PowerSC 2.0 Standard Edition was tested with Java 1.8.0_251. Other Java 8 versions can work, but were not yet tested.

4.1.2 Installing PowerSC on AIX systems

The following filesets are available to install each PowerSC component:

- ▶ `powerscStd.ice`: Installed on AIX systems that require the Security and Compliance Automation feature of PowerSC. Compliance program requires at least 5 MB of available disk space in the "/" file system.
- ▶ `powerscStd.vtpm`: Installed on AIX systems that require the Trusted Boot feature of PowerSC. You can obtain the `powerscStd.vtpm` fileset from the AIX base media or from this [IBM MRS Tool web page](#).
- ▶ `powerscStd.vlog`: Installed on AIX systems that require the Trusted Logging feature of PowerSC.
- ▶ `powerscStd.tnc_pm`: Installed on AIX 7.2 TL3 or later. `Curl 7.65.1-1`, `ca-certificates-2016.10.7-2`, and `libgcc-8.1.0-2` is installed on the TNC Patch Management server for secure transmission of interim fixes from the IBM Security Site.
- ▶ `powerscStd.svm`: Installed on AIX systems that might benefit from the routing feature of PowerSC.
- ▶ `powerscStd rtc`: Installed on AIX systems that require the Real-Time Compliance feature of PowerSC.

- ▶ `powerscStd.uiAgent.rte`: Installed on AIX systems are to be managed by using the PowerSC GUI. The fileset `powerscStd.ice` is required to install `powerscStd.uiAgent.rte`.
- ▶ `powerscStd.uiServer.rte`: Installed on the AIX system that is configured specifically for running the PowerSC GUI server.
- ▶ `powerscStd.uiRelay`: Installed on AIX systems that might benefit from the network security zones feature of PowerSC.

You can install each of the filesets by using one of the following interfaces:

- ▶ The `installp` command from the CLI
- ▶ SMIT

4.1.3 Installing PowerSC GUI AIX agent and server

This section shows how to install the PowerSC GUI AIX agent and server.

PowerSC GUI server

The PowerSC GUI server can run on any AIX or Linux system. It is recommended that you create a dedicated AIX LPAR or Linux LPAR on which you can install and run the PowerSC GUI server.

IBM recommends a minimum of 4 GB of RAM on the system on which you plan to run the PowerSC GUI server.

You use the `installp` command to install `powerscStd.uiServer.rte` fileset for the PowerSC GUI server. Figure 4-1 shows the `installp` command that is run on each endpoint to install the compliance, license, and agent components of the product.

```
$ installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license
powerscStd.uiServer.rte
```

Figure 4-1 Installing PowerSC GUI AIX server

PowerSC GUI agent

The PowerSC GUI agent must be installed on every AIX, Linux, or IBM i endpoint that is to be monitored. The PowerSC GUI agent tracks activity on the endpoint and provides that information to the PowerSC GUI server.

The PowerSC GUI agent also runs the commands that are triggered from the PowerSC GUI. All communication between PowerSC GUI agents and the PowerSC GUI server is encrypted.

You use the `installp` command to install `powerscStd.uiAgent.rte` fileset for the PowerSC GUI agent on AIX endpoints. Figure 4-2 shows the `installp` command that is run on each endpoint to install the compliance, license, and agent components of the product.

```
$ installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license
powerscStd.uiAgent.rte
```

Figure 4-2 Installing PowerSC GUI AIX agent

Viewing PowerSC License

You can view the PowerSC software license for an AIX system by using the **installp** command.

The software license can be viewed in the CLI by using the command as shown in Figure 4-3.

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

Figure 4-3 Viewing PowerSC license

4.1.4 Distributing the truststore security certificate to endpoints

System administrators must deploy the truststore security certificate on all endpoints.

During installation, a truststore file (`endpointTruststore.jks`) is created and it can be used by all endpoints. The file is placed in the `/etc/security/powersc/uiServer/` directory.

After installation, you must place the `endpointtruststore.jks` file on each endpoint for the PowerSC GUI agent on that endpoint to make contact with the PowerSC GUI server and to start the process that results in the creation of the keystore on the endpoint.

You can distribute the truststore file by using one of the following methods:

- ▶ Manually copy the `endpointTruststore.jks` file to each endpoint.
- ▶ If PowerVC (or another virtualization manager) is used in your environment, the `endpointTruststore.jks` file can be put onto the PowerVC image. When the PowerVC image is deployed to an endpoint, the PowerSC GUI agent *and* the truststore file are included.

Before the PowerSC GUI communicates with an endpoint, the truststore security certificate must be deployed on it. During the installation of PowerSC, a truststore file (`endpointTruststore.jks`) is created and can be used by all the endpoints. The file is in `/etc/security/powersc/uiServer` on the server and in `/etc/security/powersc/uiAgent` on the endpoint.

When the PowerSC GUI agent starts on an endpoint, it uses the local truststore file to make a secure contact with the PowerSC GUI server and starts creating the keystore on the endpoint.

After the `endpointTruststore.jks` file is deployed to the endpoints, and when an endpoint starts running, the PowerSC GUI agent uses the truststore file to determine the location where the PowerSC GUI server is running. The PowerSC GUI agent then sends a message to the PowerSC GUI server with a request to join the list of available and monitored endpoints.

The truststore file can be distributed by using one of the following methods:

- ▶ Manually copying `endpointTruststore.jks` file to each endpoint.
- ▶ If a virtualization manager is used (for example PowerVC), the truststore can be included in the image.

If you copied the truststore file to the endpoint, you must stop and restart the agent, as shown in Figure 4-4.

```
$ stopsrc -s pscuiagent  
$ startsrc -s pscuiagent
```

Figure 4-4 Starting and stopping the PowerSC AIX GUI agent

4.1.5 Compliance checking

The **pscxpert** command sets various system configuration settings to enable the specified security level.

Implement or check the compliance profile by using the **pscxpert** command on AIX, and the **viosecure** command on the Virtual I/O Server (VIOS).

The list of PowerSC compliance profiles for an AIX system is available on this [IBM Documentation web page](#).

To write all of the high-level security options to an output file, enter the command that is shown in Figure 4-5.

```
$ pscxpert -l high -n /etc/security/pscxpert/plugin/RedbooksSecurity.xml
```

Figure 4-5 Writing high-level security option to output file using pscxpert

After you run the command that is shown in Figure 4-5, the output file can be edited and specific security roles can be commented out by enclosing them in the standard XML comment string (<-- begins the comment and -\> closes the comment).

To apply the security settings from the Payment card industry-Data security standard configuration file, enter the commands as shown in Figure 4-6.

```
$ pscxpert -f /etc/security/aixpert/custom/PCIv3.xml  
$ viosecure -file /etc/security/aixpert/custom/PCIv3.xml
```

Figure 4-6 Applying PCI-DSS on AIX and VIOS level using pscxpert and viosecure commands

To check the security settings of the system, and to log the rules that failed into the audit subsystem, enter the command as shown in Figure 4-7.

```
$ pscxpert -c -p
```

Figure 4-7 Checking security settings

To check the custom level of the security settings for the Payment card industry-Data security standard profile on the system, and to log the rules that failed into the audit subsystem, enter the command as shown in Figure 4-8.

```
$ pscxpert -c -p -l PCI
```

Figure 4-8 Checking PCI-DSS compliance

To generate reports and to write them to the /etc/security/aixpert/check_report.txt file, enter the command as shown in Figure 4-9.

```
pscxpert -c -r
```

Figure 4-9 Generate report

4.2 Security and compliance tools for IBM i

Security and compliance tools for IBM i helps clients ensure a higher level of security and compliance on their systems, networks, and data.

The tools are provided as a service offering; they are *not* a licensed program product. For more information, see [IBM i Security web page](#).

Attention: Security and compliance tools for IBM i are a set of service offerings that are available from IBM Systems Lab Services.

The following IBM Lab Services offerings for IBM i security are available:

- ▶ IBM i Security assessment
- ▶ IBM i Single Sign on Implementation
- ▶ IBM i Security Remediation
- ▶ IBM i Encryption assistance
- ▶ PowerSC Standard Edition for IBM i implementation

For more information about the tools on security for IBM i, contact the following people:

- ▶ Terry Ford: taford@us.ibm.com
Project Manager - Security Services Delivery
- ▶ Robert D. Andrews: robert.andrews@us.ibm.com
Executive Security Consultant - Team Lead

Client benefits

The following client benefits are available:

- ▶ Simplifies management and measurement of security and compliance.
- ▶ Reduces cost of security and compliance.
- ▶ Improves detection and reporting of security exposures.
- ▶ Improves auditing and monitoring to meet reporting requirements.
- ▶ Guides your business toward a more secure operational demonstrate.

Table 4-1 lists the offerings for security and compliance tools for IBM i.

Table 4-1 Security and compliance tools for IBM i offerings

Security and compliance tools for IBM i	Benefits
Compliance Automation Reporting Tool (CART) that includes event monitoring	Demonstrate adherence to predefined and customer-defined security policies and system component inventory. Centralize and automate security management and reporting by way of DB2 Web Query.
Security Diagnostics	Decreases operator time included in remediating exposures.
Privileged Elevation Tool	Ensures compliance with guidelines on privileged users.

Security and compliance tools for IBM i	Benefits
Access Control Monitor	Prevents user application failures because of inconsistent controls.
SYSLOG Reporting Manager	Simplifies QAUDJRN/IFS file change events to syslog (CEF).
Network Interface Firewall	Reduces threat of unauthorized security breach and data loss.
Certificate Expiration Manager	Prevents system outages because of expired certificates.
Password Synchronization	Ensure that service accounts adhere to password policy and are synchronized across all LPARs this includes SVRAUTE. Also, Password Validation.
Advanced Authentication	Enhance applications with time-based one-time password (TOTP) service program.
Single Sign on (SSO) Suite	Reduces password resets and simplifies user experience.

Important: When discussing IBM i tools versus IBM security vendor competitors, it is important to distinguish IBM i tools as niche; that is, targeted at meeting specific requirements. They do the job. Consider the following analogy: Microsoft Office provides numerous functions; 80% of its function is not needed by most people that just want a document editor. IBM i tools are similar in that they provide specific functions and meet specific requirements.

Some customers want to address a specific issue and do not want to invest in a full robust product. The niche solution approach of IBM i gives them an option to do just that at a generally affordable price.

The security and compliance tools for IBM i are a service offering with each tool that is targeted to a specific security function. The tools provide various security and compliance capabilities that can enhance the integrated security features of the IBM i operating system.

Each tool can be used autonomously and are not integrated as a single program product (see Table 4-2).

Table 4-2 Security and compliance tools for IBM i features, functions, and benefits

Tools and feature	Function	Benefit
Compliance Automation and Reporting Tool (CART) with event monitoring	Daily compliance dashboard reports at LPAR, system, or enterprise level by using event monitoring.	Enables compliance officer to demonstrate adherence to predefined security policies.
Security Diagnostics	Reports detailing security configuration settings and identifying deficiencies.	Reduces operator time that is involved in remediating security exposures.
Privileged Elevation Tool (FIRECALL)	Controls the number of privileged users.	Ensures compliance with industry guidelines on privileged users.
Access Control Monitor	Monitors security deviations from application design.	Prevents user application failures because of inconsistent access controls.
Network Interface Firewall for IBM i Exit Points.	Control access to Exit Point interfaces, such as ODBC, FTP, and RMTCMD.	Reduces threat of unauthorized security breach and data loss.
SYSLOG Reporting Manager	Simplifies QAUDJRN/IFS file change events to syslog (CEF).	Utility to allow the IBM i to participate with SIEM solutions.

Tools and feature	Function	Benefit
Certificate Expiration Manager	Simplifies management of digital certificates expiration.	Helps operators prevent system outages because of expired certificates.
Password Synchronization	Aids users with enhanced PWD management.	Maintains consistent PWDs and SVRAUTE.
Single Sign on (SSO) Suite	Simplifies implementation of SSO and password synchronization.	Reduces password resets and simplifies user experience.
Advanced Authentication (MFA)	Service Program to enable MFA in applications.	Includes PWD Reset and Sign-on utilities.

Next, we provide more information about the tools and features of the security and compliance tools for IBM i.

Compliance Automation and Event Monitoring tool

The Compliance Automation and Event Monitoring tool provides centralized reporting of IBM i security with easy to use dashboards for a rapid daily review of security.

Although this tool is extensible, its primary purpose is driving security compliance with client-defined policies and standards. Best practice comparisons are standard. Client-defined policies and exceptions can be implemented with interfaces that are included in the tool. including the following example:

- ▶ An automated collection, analysis, and reporting tool on over 1200 security-related risks, information, statistics, and demographics.
- ▶ The tool includes the following interfaces:
 - Audit Journal and QHST Event Monitoring/Alerts
 - Password management
 - Profile administration
 - Special authorities
 - Group inheritance
 - Network configuration
 - NetServer attributes
 - Operational security
 - Security risks
- ▶ Daily compliance dashboards reports at the LPAR, system, or enterprise level.
- ▶ Enables compliance officer to demonstrate adherence to predefined or customer-defined security policies.

Security diagnostics

The compliance assessment and reporting tool provide daily monitoring compliance and identifying exceptions in the enterprise.

When security exceptions are identified, the Security Diagnostics tool drills down and pinpoints the root cause of the issue.

Although this tool is used by IBM Consultants as part of a detailed security assessment or remediation service, it also can be purchased for client remediation for their own environment.

In-depth security collection and reporting includes the following features:

- ▶ Reduces the security administrator time that is involved in remediating exposures.
- ▶ Reports on:
 - User profiles
 - Adopted authority programs
 - Trigger programs
 - Work management
 - Auditing configuration
 - Network attributes
 - Integrated File System

Privileged Elevation Tool (FIRECALL)

Regardless of the operating system or platform, privileged access is one of the biggest security concerns in IT. Generally, too many people have too much access.

One reason this privileged access is so prevalent is that it often is used for infrequent or ad hoc administrative tasks. By using the Privileged Access Control tool, privileged access can be elevated or provided only when needed, which reduces the exposure of too many users with permanent privileged access.

Moreover, it ensures compliance with industry guidelines about privileged users. Without careful control, privileged users can pose a risk to your system security. This tool enables the security administrator to reduce privileged accounts, with a mechanism to temporarily elevate privileges to users when needed (see Figure 4-10).

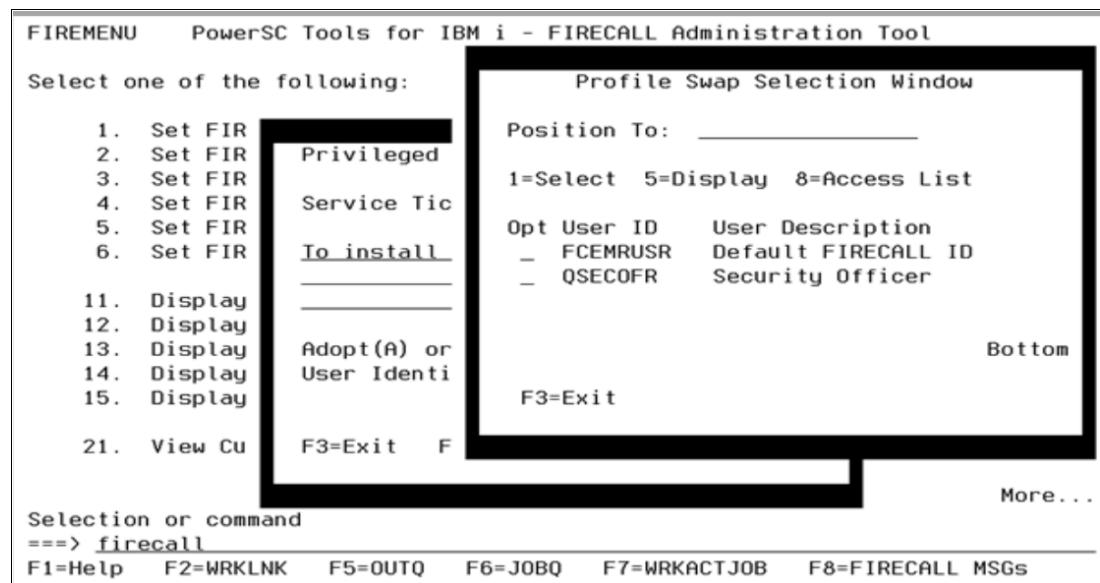


Figure 4-10 FIRECALL Administration tool

The tool includes the following features:

- ▶ Option is available to change identity for troubleshooting, IFS access, and object ownership requirements
- ▶ Automated email notifications are sent to a distribution list when the tool is started that includes a log of activities that were performed
- ▶ Fully audited

- ▶ Customizable
- ▶ Service Ticket Manager

Access Control Monitor

Many security assessments reveal inconsistent ownership, with overuse of *PUBLIC authorities and excessive permissions that are granted to applications and files.

The Access Control Monitor tool allows the clients to define a policy or standard by which an application is secured and then, report on exceptions when application components fall out of compliance with those policies and standards.

The tool monitors security deviations from the application design by using the following features:

- ▶ Ad hoc or scheduled reporting to check and report on application objects that are out of corporate security policy standards, data classifications, or other security-related configurations.
- ▶ Prevents user application failures that occur because of inconsistent access controls.
- ▶ Monitors compliance of libraries, objects, and authorization lists.
- ▶ It is customer-extensible to permit automation of object back into compliance.

Network interface firewall for IBM i exit points

Exit programs exist for many IBM i functions and applications. The purpose of these exit points is different for each exit program and their associated application.

However, many of these programs, such as Telnet and FTP exit programs, can be used to perform more checking during authentication or can be used to control what an authenticated user can do. All exit programs must be registered and the Network Interface Firewall for IBM i Exit Point tool makes this process easier by using a simple user interface (see Figure 4-11).

Work with Exit Point Definitions				11:42:36		
Position to: _____		Filter Definitions: _____	ALLOBJ: *NOTUSED			
Type options, press Enter.						
5=Display 8=Add Exit 9=Remove Exit N=*ON F=*OFF L=*LOGONLY W=WRKREGINF						
Opt	Definition	Exit Point Name	Exit Point Description	Status		
_	DRDADDM	CHGNETA	DRDA/DDM Logon	*ADDED2NAT		
_	DSTPGMC	QIBM_QZRC_RMT	Distributed Program Call			
_	DTAQSRVR	QIBM_QZHQ_DATA_QUEUE	Host Servers DATAQ Server			
_	FILESRVR	QIBM_QPWFS_FILE_SERV	Host Servers File Server			
_	FTPCLNRQ	QIBM_QTMF_CLIENT_REQ	FTP Client Request Validation			
_	FTPLOGON	QIBM_QTMF_SVR_LOGON	FTP Server Logon	*ADDED2XPT		
_	FTPSVRRQ	QIBM_QTMF_SERVER_REQ	FTP Request Validation			
_	HSTPRT	QIBM_QNPS_ENTRY	Host Server Net Print Server			
_	OJDBC	QIBM_QZDA_INIT	DB Logon - ODBC/JDBC/File XFR	*ADDED2XPT		
_	OSQL1	QIBM_QZDA_SQL1	DB Server SQL Access			
_	OSQL2	QIBM_QZDA_SQL2	DB Server SQL Access			
_	REXECREQ	QIBM_QTMX_SERVER_REQ	RExec Request Validation			
_	RMTCMD	QIBM_QZRC_RMT	RMTCMD Logon			
More...						
F3=Exit F5=Refresh F6=Create Definition F9=Command Line						

Figure 4-11 Working with Exit Points definitions

Logging and auditing is an important aspect when monitoring security. IBM i exit programs enhance customer logging mechanisms for their various system applications. For example, the FTP server does not provide a standard interface to enable logging of FTP subcommands that are performed by a signed on user. However, this information is now logged with the help of this tool.

The tool also addresses the challenge of remote command (RMTCMD) not honoring limited capabilities settings in a users profile. This tool enforces this setting when a user connects outside of the 5250 command line.

In summary, the tool reduces threat of unauthorized network access by using the following features:

- ▶ Exit programs permit IBM i system administrators to control which activities a user account is allowed for each of the specific servers. This easy-to-use interface addresses the most commonly used network interfaces.
- ▶ Users are denied by default for greater security.
- ▶ Allowed users are added by using a menu.
- ▶ Access is permitted by way of Group Profiles:
 - Restrict by IP address range
 - Log only mode
 - Current exit point coverage:
 - DRDA and DDM
 - IFS
 - FTP
 - ODBC/JDBC/File transfer
 - REXEC
 - RMTCMD
 - SQL CLI
 - TELNET
 - Host Server
 - IBM i common restrictions
- ▶ Customization is available for other network interfaces.

SYSLOG Reporting Manager

The Syslog Reporting Manager (SRM) makes it easy to integrate your IBM i Audit Journal, History Logs, Application Messages, and IFS log file, and more. Overall, it streamlines the administration and detailing of IBM i SIEM events by using the following features:

- ▶ Monitors QAUDJRN, QHST messages, MSGQs, IFS stream file changes, and others.
- ▶ Formats events to Common Event Format (CEF and LEEF) for Security Information and Event Management consumption.
- ▶ Reports events by using SYSLOG messages in close genuine time.
- ▶ Features a simple configuration.

Certificate Expiration Manager tool

Certificates are issued and signed by certificate authorities (CAs) and are valid for a specific time range only (typically one year). Most server services do not accept any new connection requests for expired certificates.

With the number of services that require a certificate increasing, certificate expiration becomes more complex and important to prevent outages. The Certificate Expiration Manager (CEM) tool simplifies the management of digital certificates and helps prevent outages that are caused by expired certificates.

It is important to distinguish between well-known (public) CAs and private (intranet) CAs. Well-known CAs charge money for issuing certificates. Privately operated CAs are typically no-charge.

Generally, it is these privately operated CAs that are of most concern. Well-known CAs often (but not always) inform certificate requesters about upcoming certificate expiration. Privately operated CAs must manage certificate expiration and renewal.

Overall, the CEM tool rearranges the administration of digital certificates by using the following features:

- ▶ Keeps up a log of all expiration activities.
- ▶ Sends a notice by way of email and a SYSLOG message.
- ▶ The simple to use setup GUI is included for overseeing the XML settings.
- ▶ It can be run on any platform that supports Java.
- ▶ Avoid blackouts that occur because of expired certificates.

Password validation

Despite warnings, one in five users choose a noncompliant password to protect their identity. Although the IBM i operating system enables password rules, the Password Validation tool provides tighter protection with stricter, client-defined password criteria.

The Password Validation tool validates and ensures that passwords meet company-defined and industry-recommended rules and guidelines.

The tool also allows the security administrator to establish a dictionary of excluded terms to further tighten password security.

IBM i password synchronization

The password synchronization tool enhances protection with extra password checking. The tool also provides the following features:

- ▶ Checks the password to see whether it contains the following potential issues:
 - Any words from a maintainable dictionary of disallowed words. It is seeded with the top 10,000 passwords that are found in globally reported breaches.
 - Previous passwords from all IBM i LPARs.

It was originally written for customers who were unable to move from V5R4. It is useful for all customers who want to prevent users from entering trivial passwords. This check is first line of defense in administrative security.

- ▶ Federated database of profiles across all IBM i LPARs.
- ▶ Filters are included for subsets of users or systems.
- ▶ Server authentication entries are updated.
- ▶ Ensures the security administrator that entered passwords are not trifling.
- ▶ Checks against the password rules of each system.
- ▶ Fully audited.

Advanced authentication

The advanced authentication tool limits access to applications and systems, correctly authenticates users, and includes the following features:

- ▶ Generates highly secure, RFC6238-based, one-time passwords (time-based one-time passwords [TOTPs]), which ensures that only correctly authenticated users are authorized access to critical applications and data.
- ▶ Use IBM i based QR code generator.
- ▶ No internet connection is required.
- ▶ Registration and use are audited.
- ▶ It can be used as a sign-on application or as a service program in your own application.

Single Sign on Suite

The following Single Sign on (SSO) Suite tools simplify SSO implementation and help to reduce Help Desk costs that are associated with forgotten or expired passwords:

- ▶ Enterprise Identity Mapping (EIM) CL Commands

This tool adds and removes an identifier and an association, which is useful for customers who want to add their own EIM-related maintenance into their user provisioning CL code.
- ▶ EIM Populator

Users can take a spreadsheet of known user IDs or names and create identifiers and mappings for each user.
- ▶ EIM Management Utility

The tool provides all information in one window rather than a series of windows; therefore, fewer clicks are needed to get to all of the information. It also is used to back up your EIM (XML).
- ▶ EIM Based CRTUSRPRF

This tool features exit programs that automatically create the EIM identifier and associations when CRTUSRPRF is run. Therefore, it assumes that the user's Windows ID is same as IBM i user profile, but can be customized (for example, to list the windows ID in the user profile description).
It also includes a DLTUSRPRF exit program that deletes the EIM identifier when DLTUSRPRF is run.

► Windows Active Directory (AD) Profile Synchronization

This Java program (which can run wherever a JRE is present) runs on a scheduled basis and polls Active Directory (AD) for users that are added to or removed from groups that are defined in configuration XML. The program uses the IBM i Java Toolbox to automatically create or delete profiles that are based on information from the AD poll. It also enables or disables profiles that are based on the AD account being enabled or disabled (see Figure 4-12).

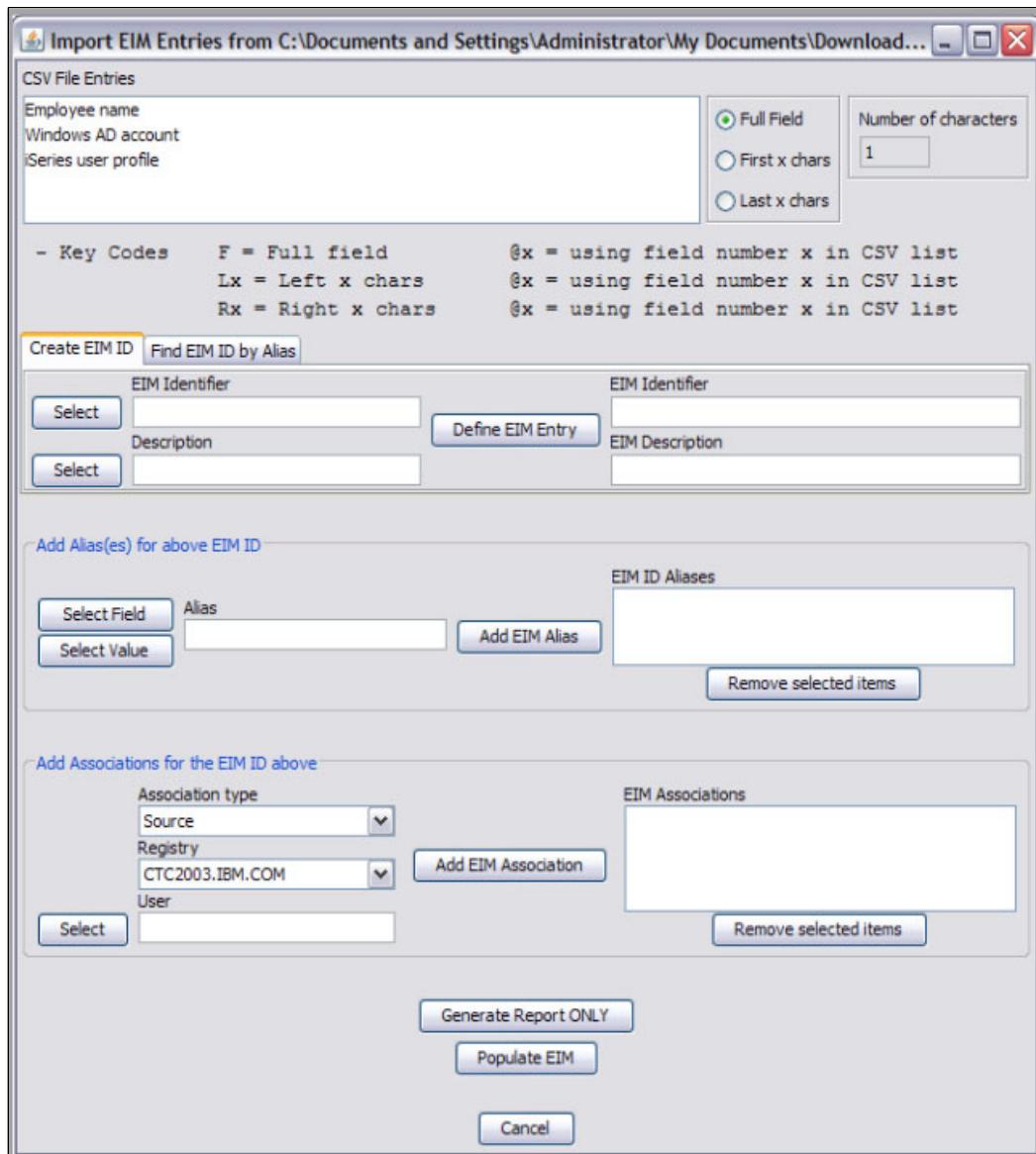


Figure 4-12 Windows Active Directory Profile Synchronization

4.3 PowerSC for IBM i

This section discusses PowerSC 2.0 supported features for IBM i and agent prerequisites. Also described are the steps for installing the PowerSC for IBM i agent and how to use the PowerSC GUI.

Finally, administering compliance levels and profiles is described.

4.3.1 PowerSC 2.0 supported features for IBM i

The following PowerSC 2.0 features are supported for IBM i:

- ▶ Automated compliance: The IBM i best practices automate the recommended system configuration for securing your IBM i system.
For more information, see the “Best practices for securing an IBM i system” section of [IBM PowerSC: PowerSC 2.0](#).
- ▶ Compliance reporting capabilities (includes timelines).
- ▶ File integrity monitoring.
- ▶ Multifactor authentication.

4.3.2 PowerSC for IBM i Agent prerequisites

The following system and software requirements must be met:

- ▶ Java JRE: In PowerSC 2.0, the JRE is no longer included in the product distribution. Before you install the PowerSC GUI agent on IBM i, the Java JRE (Java 8, 64-bit or Java 8, 32-bit) must be installed.
- ▶ Operating system: IBM i V7R2M0 or later.

The PowerSC GUI agent that is running on each endpoint listens on TCP port 11125 for all communication from the PowerSC GUI server.

4.3.3 PowerSC for installing IBM i Agent

The PowerSC for IBM i package includes the security and compliance automation and the PowerSC GUI agent features of PowerSC.

The PowerSC QIBMPSC.SAVF save file must be installed on IBM i systems that require the security and compliance automation and the PowerSC GUI agent features. For more information, see this [IBM Documentation web page](#).

To install PowerSC on IBM i systems, complete the following steps:

1. Ensure that your account includes sufficient privileges to perform the installation.
2. Create the /QSYS.LIB/QGPL.LIB/QIBMPSC.SAVF save file on the IBM i system, as shown in Example 4-1.

Example 4-1 Create /QSYS.LIB/QGPL.LIB/QIBMPSC.SAVF

```
CRTSAVF FILE(QGPL/QIBMPSC)
```

3. Use a method of your choice to copy the QIBMPSC.SAVF save file from the distribution into the /QSYS.LIB/QGPL.LIB/QIBMPSC.SAVF save file that you created, as shown in Example 4-2.

Example 4-2 Copy the QIBMPSC.SAVF

```
CPYOBJ('distribution-location/QIBMPSC.SAVF')
TOOBJ('QSYS.lib/QGPL.lib/QIBMPSC.file') TOCODEPAGE(*CALC) REPLACE(*YES)
```

4. Accept the license agreement, as shown in Example 4-3.

Example 4-3 Accept license agreement

```
RSTLICPGM LICPGM(0G060PS) DEV(*SAVF) SAVF(QGPL/QIBMPSC)
```

5. Copy the endpoint truststore /etc/security/powersc/uiServer/endpointTruststore.jks file to the /etc/security/powersc/uiAgent/endpointTruststore.jks file on each IBM i endpoint.
6. Start the PowerSC GUI agent and then, enter the command as shown in Example 4-4.

Example 4-4 Start PowerSC GUI agent

```
STRTCPVR SERVER(*UIAGENT)
```

4.3.4 Using the PowerSC GUI

You can use the PowerSC GUI to perform the following tasks:

- ▶ View the endpoints that are discovered on your system
- ▶ Create customized groups and profiles
- ▶ Copy custom profiles to endpoints
- ▶ Apply profiles

Use the Main, Compliance, and Security pages to get more information about the following topics:

- ▶ Total IBM i Audit Events
- ▶ The operating system on the endpoint (IBM i)
- ▶ The number of endpoints with IBM i audit events

4.3.5 Administering compliance levels and profiles

System administrators can apply, check, or undo built-in and custom compliance levels and profiles on several endpoints.

Systems administrators can use redefined profiles and compliance levels for IBM i supported by PowerSC: IBMi_best_practices.

From the Compliance page in the PowerSC GUI, you can perform the following tasks:

- ▶ Select and apply a defined profile or level to one or many endpoints.
- ▶ Trigger an undo operation on one or multiple endpoints.
- ▶ Check a defined profile or level against the state for one or multiple endpoints. The check operation does not result in any changes to the endpoint, but sets the Checked Timestamp value to indicate when the last check was performed.

4.4 PowerSC for Linux

This section describes how to install the PowerSC Agent on a Linux Server.

4.4.1 Prerequisites

PowerSC 2.0 Agent is supported on Linux on Power servers that are running:

- ▶ SUSE Linux Enterprise Server 15
- ▶ Red Hat Enterprise Linux Server 8.3, or later

If Red Hat Enterprise Linux Server is used, you can configure Port Scan Attack Detector (psad).

Consider the following points:

- ▶ The PowerSC GUI agent that is running on each endpoint listens on TCP port 11125 for all communication from the PowerSC GUI server.
- ▶ The PowerSC GUI agent uses minimum resources (during normal activity, it uses less than 25 MB RAM and almost zero CPU). However, configuring real-time scanning on the endpoint is likely to increase the CPU usage, with the amount depending on the number of files and breadth of the scan.

Note: At the time of this writing, PowerSC Standard Edition was tested with Java 1.8.0_251. Other Java 8 versions can work, but were not yet tested.

The following commands provide the installation steps for the PowerSC agent (where VER = rhe18 | sles 15):

```
bash powersc-pscxpert-2.0.0.VER.ppc64le.sh  
bash powersc-uiAgent-2.0.0.VER.ppc64le.sh  
dnf install psad-3.0-1.ppc64le.rpm
```

If fapolicyd is not running, the PowerSC agent installation on Linux systems displays the error that is shown in Example 4-5. This error is an informational message only.

Example 4-5 Message if fapolicyd is not running

```
Open: /run/fapolicyd/fapolicyd fifo -> No such file or directory
```

4.4.2 Configuring Intrusion Detection Service on Red Hat Enterprise Linux

The Port Scan Attack Detector (psad) must be installed to configure the intrusion detection services. The package (psad-3.0-1.ppc64le.rpm) is in the RPMS/ppc directory in the installation package.

The PowerSC psad package is in the RPMS/ppc directory.

4.4.3 Distributing the truststore

Before the PowerSC GUI communicates with an endpoint, the truststore security certificate must be deployed on it. During the installation process of PowerSC, a truststore file (`endpointTruststore.jks`) is created and can be used by all the endpoints. The file is in `/etc/security/powersc/uiServer` on the server and in `/etc/security/powersc/uiAgent` on the endpoint.

When the PowerSC GUI Agent starts on an endpoint, it uses the local truststore file to make a secure contact with the PowerSC GUI Server. It also starts the process of creating the keystore on the endpoint.

The truststore file is distributed in the following ways:

- ▶ Manually copy the `endpointTruststore.jks` file to each endpoint.
- ▶ If a virtualization manager is used (for example PowerVC), the truststore can be included in the image.

If you copied the truststore file to the endpoint, the agent must be stopped and restarted, as shown in Figure 4-13.

```
systemctl stop powersc-uiAgent.service  
systemctl start powersc-uiAgent.service
```

Figure 4-13 starting and stopping the PowerSC GUI Agent

4.4.4 Troubleshooting

If problems are encountered when the agent is started, the most likely problem is that the `jrePath` was not set. Figure 4-14 shows how to set the path.

```
# pscuiagentctl set jrePath "/usr/java8_64/jre"  
jrePath=/usr/java8_64/jre
```

Figure 4-14 Set the `jrePath`

The command `pscuiagentctl get jrePath` can be used to check whether the path is set.

If IBM Support is contacted about an issue with the PowerSC Agent, use the `/opt/powersc/uiAgent/bin/pscuiSnap` command to collect the necessary system data to provide to support in addition to a detailed description of the problem.

Packages can be removed by using the `dnf remove [package_name]` command.

4.5 Allowing and denying list management

This section provides examples of how to allow and deny list management on AIX and trusted execution logging on AIX. Also described is how to allow and deny list management on Linux.

4.5.1 On AIX (Trusted Execution)

Trusted Execution (TE) is an AIX in-built security feature for maintaining the integrity of files and executables on the system. By default, AIX includes a database of system files with their trusted signatures, the Trusted Signature Database (TSD). TE checks any deviation from these signatures and reports it as an integrity breach.

The AIX TE feature can be used for integrity check of critical files by running a full audit, or as they are accessed. TE can be used in offline mode, online mode, or both. Often it is recommended to initially use TE in offline mode and then, after monitoring, turn it online.

TE can be managed from the command line (`trustchk`) or through the PowerSC GUI. The design of TE is shown in Figure 4-15.

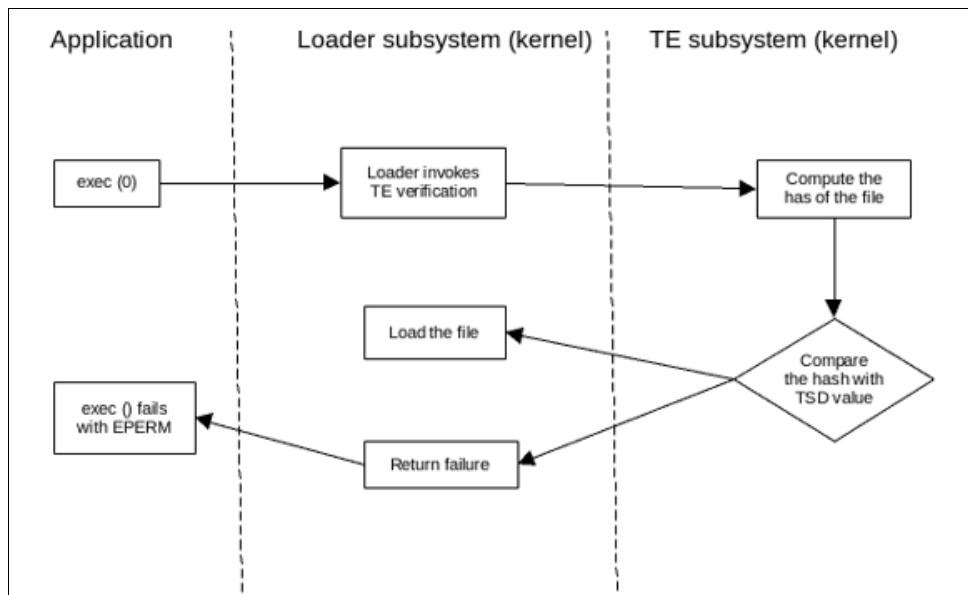


Figure 4-15 TE design

The Trusted Signature Database

Similar to the Trusted Computing Base (TCB), a database is available that is used to store critical security parameters of trusted files present on the system. This database, called *Trusted Signature Database* (TSD), is in `/etc/security/tsd/tsd.dat` or can be stored centrally in LDAP.

A *trusted file* is a file that is critical from the security perspective of the system. If this file is compromised, the security of the entire system can be jeopardized. These types of files include the following examples:

- ▶ Kernel (operating system)
- ▶ All setuid root programs
- ▶ All setgid root programs

- ▶ Any program that is exclusively run by the root user or by a member of the system group
- ▶ Any program that must be run by the administrator while on the trusted communication path (for example, the `1s` command)
- ▶ The configuration files that control system operation
- ▶ Any program that is run with the privilege or access rights to alter the kernel or the system configuration files

Every trusted file ideally includes an associated stanza or a file definition that is stored in the TSD. A file can be marked as trusted by adding its definition in the TSD by using the `trustchk` command. The `trustchk` command can be used to add, delete, or list entries from the TSD.

Auditing AIX by using trustchk

The following options are available to check the integrity of critical files:

- ▶ Check the integrity of records in the TSD
- ▶ Check for Trojan horse files

Auditing records in TSD

The TSD consists of detailed information about trusted files. The TSD contains the following details:

- ▶ owner: The owner of the file. This value is computed by the `trustchk` command when the file is being added to TSD.
- ▶ group: The group to which the file belongs. This value is computed by the `trustchk` command.
- ▶ mode: A comma-separated list of values. The following values are available:
 - SUID (SUID set bit)
 - SGID (SGID set bit)
 - SVTX (SVTX set bit)
 - TCB (Trusted Computing Base)

The file permissions must be the last value and can be specified as an octal value. For example, for a file that is set with uid and includes permission bits as `rwxr-xr-x`, the value for mode is SUID, 755. The value is computed by the `trustchk` command.

- ▶ type: The type of the file. This value is computed by the `trustchk` command. The following values are available:
 - FILE
 - DIRECTORY
 - MPX_DEV
 - CHAR_DEV
 - BLK_DEV
 - FIFO
- ▶ hardlinks: A list of hardlinks to the file. This value cannot be computed by the `trustchk` command. Instead, it must be supplied by the user when a file is added to the database.
- ▶ symlinks: List of symbolic links to the file. This value cannot be computed by the `trustchk` command. Instead, it must be supplied by the user when a file is added to the database.
- ▶ size: This value defines size of the file. The VOLATILE value means that the file is changed frequently.

- ▶ cert_tag: This field maps the digital signature of the file with the associated certificate that can be used to verify the signature of the file. This field stores the certificate ID and is computed by the **trustchk** command the file is added to the TSD. The certificates are stored in /etc/security/certificates directory.
- ▶ signature: The digital signature of the file. The VOLATILE value means that the file is changed frequently. This field is computed by the **trustchk** command.
- ▶ hash_value: The cryptographic hash of the file. The VOLATILE value means that the file is changed frequently. This field is computed by the **trustchk** command.
- ▶ minlabel: Defines the minimum sensitivity label for the object.
- ▶ maxlabel: Defines the maximum sensitivity label for the object (valid on Trusted AIX system). This attribute is not applicable to regular files and fifo.
- ▶ intlabel: Defines the integrity label for the object (valid on Trusted AIX system).
- ▶ accessauths: Defines the access authorization on the object (valid on Trusted AIX system).
- ▶ innateprivs: Defines the innate privileges for the file.
- ▶ proxyprivs: Defines the proxy privileges for the file.
- ▶ authprivs: Defines the privileges that are assigned to the user after specific authorizations are assigned.
- ▶ secflags: Defines the file security flags that are associated with the object.
- ▶ t_accessauth: Defines the extra Trusted AIX with Multi-Level Security (MLS)-specific access authorizations (valid on Trusted AIX system).
- ▶ t_innateprivs: Defines the extra Trusted AIX with MLS-specific innate privileges for the file (valid on Trusted AIX system).
- ▶ t_proxyprivs: Defines the additional Trusted AIX with MLS-specific proxy privileges for the file (valid on Trusted AIX system).
- ▶ t_authprivs: Defines the extra Trusted AIX with MLS-specific privileges that are assigned to the user after specific authorizations are assigned (valid on Trusted AIX system).
- ▶ t_secflags: Defines the extra Trusted AIX with MLS-specific file security flags that are associated with the object (valid on Trusted AIX system).

TSD features the entries in the binary **/usr/bin/mv** as shown in Example 4-6.

Example 4-6 TSD entries for mv

```
trustchk -q /usr/bin/mv
/usr/bin/mv:
    owner = bin
    group = bin
    mode = 555
    type = FILE
    hardlinks =
    symlinks =
    size = 22332
    cert_tag = 49424d4149583a31324331342d33314332303a324b3a41
    signature =
7fbb9f9275d599d281cc54fbe2b46001621bf3c279f69cc353b631ee00c13f202aaafc4e9619bfde25
f5e416e9121ace222400c607ad61c5372b75dccfd91ae601c65a0c205fb57cdfb8e466f4ba9c79ad05
6fd7d6c813882cdb85759e91b8b9b37560bd22efcd2dcde0c27d2e0061386906c44d622fdf851e73b6
eaf8857de302ef22ddee32ea78f185d9d6d47a97819e5c5890fed90e86576356d8d5531f70d11d58b0
5bf32b3edad4ef3b5c65089ceaa0e0264f17993205e57d07561c24c578b7b354c5b235750fbe371d1f
```

```
b2b01ded811dc1c967d56b43d1de7c3f0985a21d7c63f51207ee92754ab70d4f37534367c49bdffcb2  
b22f28d27b97b0fb4187  
hash_value =  
fee1e43033ffd5d3e242f2059be8146c5ffdbe751335ffed1b71b815a1a15dd1  
minslabel =  
maxslabel =  
intlabel =  
accessauths =  
innateprivs =  
inheritprivs =  
authprivs =  
secflags =
```

When an audit is run, the information in the TSD is compared with the properties of the file. Any errors can be reported and corrected, as shown in Example 4-7.

Example 4-7 Audit of all files set to just notify

```
# trustchk -n ALL  
trustchk: /etc/security/rtc/rtcd.conf: Verification of attributes failed: mode  
trustchk: /var/adm/cron/cron.deny: Verification of attributes failed: owner group  
trustchk: /usr/bin/rexec: Verification of attributes failed: mode  
trustchk: /usr/bin/rdist: Verification of attributes failed: mode
```

Checking for Trojan horses

The **trustchk** command also can be used to scan the system for any executable files that are not part of the TSD (also known as *Trojan horse files*), but are suspect from a privilege escalation perspective. Files are reported as suspect if they meet any the following criteria:

- ▶ Have setuid or setgid set, owner root or group security, but not in the TSD
- ▶ Are owned by root and not in the TSD
- ▶ Are a privileged command (RBAC) and not in the TSD
- ▶ Are a symbolic link to a privileged command (RBAC) and not in the TSD

To audit for Trojan horse files, run the **trustchk -n tree** command.

Adding records to the TSD

You can add your own binaries to the TSD to extend the auditing and control of TE. All that is required is to set up a private key and a certificate, which can be used to generate the checksums for the TSD.

Because an OpenSSL creates its keys and certificates in a privacy-enhanced mail (PEM) security certificate format, they must be converted into ASN.1/PKCS8/DER (distinguished encoding rules) format to become usable for TE. This process can be done quickly by completing the following steps:

1. Generate a 2048-bit private key in PEM format by using the following command:

```
# openssl genrsa -out TEprivkey.pem 2048
```

2. Create the public key and certificate that lasts approximately 10 years by using the following command:

```
# openssl req -new -x509 -key TEprivkey.pem -outform DER -out TEcert.der -days 3650
```

- Convert the private key from PEM into DER format by using the following command:

```
# openssl pkcs8 -inform PEM -in TEprivkey.pem -topk8 -nocrypt -outform DER -out TEprivkey.der
```

After the conversion, the private key in PEM format is no longer needed. Only the TEprivkey.der and TECert.der files are needed to add to the TSD, as shown in Example 4-8.

Example 4-8 Add TEprivkey.der and TECert.der

```
# trustchk -s TEprivkey.der -v TECert.der -a /path/to/binary
```

Note: An entry in the TSD cannot be modified if the binary is changed. The record must be deleted and then, re-created.

Example 4-9 shows how to modify a binary in the TSD.

Example 4-9 Modifying binary to the TSD

```
# trustchk -d /path/to/binary  
# trustchk -s privkey.der -v cert.der -a /path/to/binary
```

If the size of the file changes, it is important to specify that it is volatile, as shown in Example 4-10.

Example 4-10 Rule to mark a file volatile

```
# trustchk -s privkey.der -v cert.der -a /path/to/binary size=VOLATILE
```

Note: Consider the following points:

- If the record exists in the TSD and the hash value is calculated, the keys can be excluded from the command.
- If the TSD_FILES_LOCK policy is set, volatile files cannot be modified.

4.5.2 Trusted Execution policies

The following TE policies can be set (yes or no):

- TE: Enables or disables TE. All other policies can be activated only if TE is set to ON.
- CHKEXEC: Checks the integrity of executable files that belong to the TSD before starting them.
- CHKSCRIPT: Checks the integrity of shell scripts that belong to the TSD before starting them.
- CHKKERNELNEXT: Checks the integrity of the kernel extensions that belong to the TSD before loading them.
- CHKSHLIB: Checks the integrity of shared libraries that belong to the TSD before loading them.
- LOCK_KERN_POLICIES: If this policy is enabled, all other policies are locked. Restart is required to change this policy.
- STOP_ON_CHKFAIL: Stops loading files whose integrity check fails.

- ▶ STOP_UNTRUSTD: Stops loading files that are not in the TSD.
- ▶ TROJAN: Stops loading files that are not in the TSD and files that match the properties of a Trojan horse file.
- ▶ TEP: Sets the value of TE path, and enables or disables it. When this policy is enabled, the files that belong to only these directory paths are allowed to be started.
- ▶ TLP: Sets the value of Trusted Library path, and enables or disables it. When this policy is enabled, the libraries that belong to only these directory paths can be loaded.
- ▶ TSD_LOCK: Disallows opening a TSD file (/etc/security/tsd/tsd.dat) in write mode to disable editing the TSD.
- ▶ TSD_FILES_LOCK: Disables opening files that belong to the TSD in write mode.
- ▶ WARNING: Files that are defined as VOLATILE cannot be modified.
- ▶ EXVOL: Disables opening only the nonvolatile files that belong to the TSD in write mode. The volatile files can be changed.

Turning on TE, checking scripts and executables (but not stopping), and locking the TSD is shown in Example 4-11.

Example 4-11 Check scripts and executables

```
# trustchk -p te=on chkexec=on chkscript=on tsd_lock=on
# trustchk -p
TE=ON
CHKEXEC=ON
CHKSHLIB=OFF
CHKSCRIPT=ON
CHKKERNEXT=OFF
STOP_UNTRUSTD=OFF
STOP_ON_CHKFAIL=OFF
LOCK_KERN_POLICIES=OFF
TSD_FILES_LOCK=OFF
TSD_LOCK=ON
TEP=OFF
TLP=OFF
```

4.5.3 Trusted execution logging on AIX (syslog and AIX auditing)

This section describes how to enable trusted execution logging on AIX.

Adding Trusted Execution messages to syslog

Add the entry to syslogd.conf, as shown in Figure 4-16. Then, create the file and refresh syslogd.

kern.debug <te_out_file>

Figure 4-16 Entry in syslogd.conf

Example 4-12 shows the entries in the log file.

Example 4-12 TE entries in syslog

```
Mar 5 03:55:01 aix-72 kern:info unix: Trusted Execution: pid=11600228, euid=0, ruid=0: File not in TSD: /usr/bin/lsred
Mar 5 03:55:01 aix-72 kern:err|error unix: Trusted Execution: pid=11600228, euid=0, ruid=0: Crypto hash verification failed: /usr/bin/lsred
Mar 5 03:55:20 aix-72 kern:info unix: Trusted Execution: pid=11600234, euid=0, ruid=0: File not in TSD: /usr/bin/lsred
```

Using the AIX audit system

Auditing can be configured in by using bin or streams modes. For the purposes of this example, we use streams mode.

The following events are defined in /etc/security/audit/events:

- ▶ TSDTPolicy
- ▶ TE_Untrusted
- ▶ TE_FileWrite

Include the following modifications in /etc/security/config:

- ▶ Create a class, as shown in Figure 4-17.

```
my_te = TSDTPolicy,TE_Untrusted,TE_FileWrite
```

Figure 4-17 Create a class

- ▶ Assign the class to the user, as shown in Figure 4-18.

```
root = my_te
```

Figure 4-18 Assign a class

Examples of streams report

This section shows streams report examples.

For a base report, use `/usr/sbin/auditstream | auditpr`. The report is shown in Example 4-13.

Example 4-13 Basic audit report for TE activity

event	login	status	time	command	wpar	name
S_PASSWD_READ	root	OK	Tue Jun 15 23:48:24 2021	sshd	Global	
TSDTPolicy	root	OK	Tue Jun 15 23:48:32 2021	trustchk	Global	
TSDTPolicy	root	OK	Tue Jun 15 23:48:32 2021	trustchk	Global	
TSDTPolicy	root	OK	Tue Jun 15 23:48:34 2021	trustchk	Global	

For a base report with details, use `/usr/sbin/auditstream | auditpr -v`. The report is shown in Example 4-14.

Example 4-14 Detailed audit report for TE activity

event	login	status	time	command	wpar name
<hr/>					
TSDTPolicy	root	OK	Tue Jun 15 23:53:01 2021	trustchk	Global
	TE set				
TSDTPolicy	root	OK	Tue Jun 15 23:53:01 2021	trustchk	Global
	TE set				
TSDTPolicy	root	OK	Tue Jun 15 23:53:03 2021	trustchk	Global
	TE policy reset				

Format the report by using `/usr/sbin/auditstream | auditpr -h elrRtc -w`, as shown in Example 4-15.

Example 4-15 Format through auditpr

event	login	real	status	time	command
<hr/>					
TSDTPolicy	root	root	OK	Tue Jun 15 23:14:41 2021	trustchk TE set
TSDTPolicy	root	root	OK	Tue Jun 15 23:14:41 2021	trustchk TE set
TSDTPolicy	root	root	OK	Tue Jun 15 23:14:43 2021	trustchk TE policy reset
TSDTPolicy	red	root	OK	Tue Jun 15 23:15:25 2021	trustchk TE set
TSDTPolicy	red	root	OK	Tue Jun 15 23:15:25 2021	trustchk TE set
TSDTPolicy	red	root	OK	Tue Jun 15 23:15:27 2021	trustchk TE policy reset

Forwarding auditing to syslog daemon

A simple process can be used to redirect AIX Audit stream to syslog. This process is done by writing to a local file, forwarding it to a central syslog server, or both.

Complete the following steps to forward auditing to the syslog daemon:

1. Configure the `/etc/syslog.conf` file.

Each line in the file specifies the facility, priority, and destination. For this scenario, we use the `local6` facility with priority of notice and send to a local file, as shown in Figure 4-19.

```
local6.notice /data/red/syslog_te.out rotate size 2m files 4 time 1w
```

Figure 4-19 Configure the local file

This command sends the information to the `/data/red/syslog_te.out` file, rotating the file when it reaches 3 months (m) or 1 week (w) old (which ever comes first) across four files.

Figure 4-20 shows sending the information to a central syslog server.

```
local6.notice @my_syslog_server
```

Figure 4-20 Send the information a central syslog server

Then, the file must be created and the `syslogd` daemon refreshed.

2. Configure /etc/security/audit/config.

Confirm that streams mode is turned on and check the location of your streamcmds file (by default, it is in /etc/security/audit/streamcmds).

3. Modify the streamcmds file as shown in Figure 4-21.

```
/usr/sbin/auditstream | /usr/sbin/auditselect -m -e "command != logger &&
command != auditstream && command != auditpr && command !=
auditselect" | auditpr -t0 -h eclrRdt -w | /usr/bin/logger -p local6.notice -r
&
```

Figure 4-21 Modify the streamcmds file

The use of this command results in the following modifications:

- Reads events from the audit subsystem and passes them to the **auditselect** command.
- The **auditselect** command filters out commands that are generated by the streams pipeline.
- Runs the **auditpr** command to format the output.
- Sends the events to the syslogd subsystem on the local6 facility with a severity of notice.
- Uses the **-r** flag to retry any messages that are dropped by the syslog daemon until these messages are accepted.
- Keeps running in the background by issuing the **&!** command.

4.5.4 Allowing and denying list management on Linux (fapolicyd)

The fapolicyd software framework controls the execution of applications based on a user-defined policy. This method is one of the most efficient ways to prevent running untrusted and possibly malicious applications on your system.

The fapolicyd framework provides the following components:

- ▶ Service
- ▶ Command-line utilities
- ▶ RPM plug-in
- ▶ Rule language

The administrator can define the allow and deny execution rules for any application with the possibility of auditing that is based on a path, hash, MIME type, or trust.

The fapolicyd framework introduces the concept of trust. An application is trusted when it is correctly installed by the system package manager; therefore, it is registered in the system RPM database.

The fapolicyd daemon (user space) uses the RPM database as a list of trusted binaries and scripts. The fapolicyd RPM plug-in registers any system update that is handled by the YUM package manager or the RPM Package Manager. The plug-in notifies the fapolicyd daemon about changes in this database.

Other methods that can be used to add applications require creating custom rules and restarting the fapolicyd service.

The fapolicyd service configuration is in the /etc/fapolicyd/ directory with the following structure (in /etc/fapolicyd):

- ▶ The fapolicyd.rules file contains allow and deny execution rules.
- ▶ The fapolicyd.conf file contains the daemon's configuration options. This file is useful primarily for performance-tuning purposes.
- ▶ Since Red Hat Enterprise Linux 8.3, the fapolicyd framework also supports the of the fapolicyd.trust plain-text file as a source of trust. This file can be modified by using a text editor or the **fapolicyd** CLI commands.

You can use one of the methods to check the integrity of fapolicyd:

- ▶ File-size checking
- ▶ Comparing SHA-256 hashes
- ▶ Integrity Measurement Architecture (IMA) subsystem

By default, fapolicyd does not perform integrity checking. Integrity checking that is based on the file size is fast, but an attacker can replace the content of the file and preserve its byte size.

Computing and checking SHA-256 checksums is more secure, but it affects the performance of the system. The integrity = ima option in fapolicyd.conf file requires support for files' extended attributes (also known as xattr) on all file systems that contain executable files.

The fapolicyd is not included with PowerSC Standard Edition. You must first install it before you can use it with PowerSC GUI.

Common missing configuration scenarios include the following examples:

- ▶ fapolicyd is not installed on the PowerSC GUI agent.
 Use yum or dnf to install fapolicyd.
- ▶ fapolicyd is running on the PowerSC GUI agent.

You must configure fapolicyd to allow the PowerSC GUI agent to run:

- a. Run the **fapolicyd** commands as root on the agent:

```
/usr/sbin/fapolicyd-cli -f add /opt/powersc/uiAgent/bin/uiAgent  
/usr/sbin/fapolicyd-cli -u
```

- b. Restart the agent:

```
systemctl restart powersc-uiAgent
```

4.6 PowerSC MFA example configuration

This section describes how to configure PowerSC MFA GUI on an AIX Server. Also discussed is how to set up authentication for an AIX and a Red Hat Enterprise Linux client.

4.6.1 Configuring the MFA Server

For this example, we installed the MFA Server on AIX 7.2, but you also can install it on Red Hat Enterprise Linux or SUSE Linux Enterprise Server.

Requirements

AIX includes the following requirements:

- ▶ AIX 7.1.5.2 and later or 7.2.3.0 and later
- ▶ The security.pkcs11 and security.pkcs11.tools are installed

The following ports are opened:

- ▶ Server Authentication Port 6793
- ▶ Mutual Authentication Port 6794

The following filesets must be installed on each MFA Server:

- ▶ powerscMFA.license
- ▶ powerscMFA.server
- ▶ powerscMFA.pam.fallback

Creating a PKCS#11 token

The first task is to create a PKCS#11 token. If the server is to be configured for HA, both share a replicated copy of the database. Also, the token must be created and then imported into the second node.

Complete the following steps to create the token:

1. Start the p11admin tool, as shown in Example 4-16.

Example 4-16 Starting the administration tool

```
PKCS#11 Administration Tool
· Main Menu ..... Information .....
·
· Select Source PKCS#11 Slot/Token ..... Select a PKCS#11 slot and token to manage. .....
· Manage PKCS#11 Slots ..... .
· Manage PKCS#11 Tokens ..... .
· Manage Y4 Adapters ..... .
· Manage IBM 4767 Adapters ..... .
· Exit Menu ..... .
·
·
·
·
·
· Status ..... .
· Source Provider: none ..... .
·
· Token: n/a ..... .
.....
F1:[Help] F3:[Back] r:[adjust right] l:[adjust left]
```

- From the main menu, select **Source PKCS#11 Slot/Token** and then, press **Enter**.

Select the slot and token that you want to use. If the token is not in use for another purpose, you can accept the default of Token: Default GLOBAL token 1 (Slot 0). Then, exit the menu (see Example 4-17).

Example 4-17 Selecting the token

```
PKCS#11 Administration Tool
· Select PKCS#11 Token ..... Information .....
·
· Token: Default GLOBAL token 1
· Load PKCS#11 Path:
· Exit Menu
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
·
· Status ..... [More...34]
· Source Provider: none
· Token: n/a
···
F1:[Help] F3:[Back] r:[adjust right] l:[adjust left]
```

- Select **Manage PKCS#11 Tokens** from the front menu (see Example 4-16 on page 137).
- Select **Initialize Source Token**, as shown in Example 4-18.

Example 4-18 Initializing the source token

```
PKCS#11 Administration Tool
· PKCS#11 Token Management ..... Information .....
·
· Initialize Source Token
· Security Officer Login
· Change Security Officer Password
· Reset User Password
· View Clock
· Set Clock
· Manage Object Trust
· Exit Menu
·
·
·
·
·
·
·
·
·
·
·
· Status ..... .
· Source Provider: Build Jul 27 2020 - 18:09:26
· Token: Default GLOBAL token 1 (Slot 0)
···
F1:[Help] F3:[Back] r:[adjust right] l:[adjust left]
```

5. Enter a new token label and a PIN, as shown in Example 4-19. These values are used to configure the MFA GUI.

Example 4-19 Entering a token label and PIN

```
PKCS#11 Administration Tool
· Initialize Token ..... Information .....
·
· New Token Label: ..... Enter a new label for the PKCS#11
· S.O. PIN : ..... token being initialized.
· Verify S.O. PIN : ..... .
· Exit Menu ..... .
·
·
·
·
·
·
·
·
· Status ..... .
· Source Provider: Build Jul 27 2020 - 18:09:26
·
· Token: Default GLOBAL token 1 (Slot 0)
..... F1:[Help] F3:[Back] r:[adjust right] l:[adjust left]
```

6. Exit the menu. Then, exit the tool.
7. Configure PAM for the GUI by adding the lines to /etc/pam.conf, as shown in Example 4-20.

Example 4-20 Configuring PAM

```
# Added by redpaper team - 26/10/21, MFA install project
pmfaserver auth required pam_ckfile
pmfaserver auth required pam_permission file=/etc/security/access.conf found=allow
pmfaserver auth required pam_aix
# End of hack
```

Note: IBM PowerSC Multi-Factor Authentication Version 2.0.0 Installation and Configuration GUI recommends adding the pam_permission.

For more information, see the “Editing the IBM PowerSC MFA PAM modules” section of [IBM PowerSC Multi-Factor Authentication Version 1.2.0: Installation and Configuration](#).

Obtaining the PKCS#12 file and certificate password

Obtain the PKCS#12 file and the server certificate password for your IBM PowerSC MFA server system from your security administrator and copy it to the following directory:

/etc/security/pmfa/certificates

For more information about creating a test certificate, see this [IBM Documentation web page](#).

Configuring the GUI

The first step in the process to configure the GUI is to edit the GUI configuration file (/etc/security/pmfa/pmfaserver_setup.conf), as shown in Example 4-21.

Example 4-21 Editing the GUI configuration file

```
# initial trace level for MFA server
INITIAL TRACE LEVEL=3

# location of the P12 identity certificate for the MFA server
P12 LOCATION=/etc/security/pmfa/certificates/server_p12.pfx

# PKCS11 token used while encrypting P12 password
PKCS11 TOKEN NAME=MFA_TOKEN

# directory or PEM file containing CAs that will be trusted by the MFA server
CAS LOCATION=/etc/security/pmfa/certificates/cas

# location that the OOB files were unpacked to
WEB DOCUMENT ROOT=/opt/IBM/powersc/MFA/mfa

# port to use for server-authentication
SERVER AUTH PORT=6793

# port to use for mutual authentication
MUTUAL AUTH PORT=6794
```

Next, the following command must be run to configure the web server:

```
/opt/IBM/powersc/MFA/bin//pmfa_webserver_config
/etc/security/pmfa/pmfaserver_setup.conf
```

Note: If you run the command after you configured options in the MFA GUI, you must reconfigure and restart the GUI.

After the GUI is configured, the GUI can be started.

Starting and stopping the GUI

Example 4-22 shows the status of the MFA GUI on AIX.

Example 4-22 Showing the GUI status

```
# lssrc -s pscuiserver
Subsystem          Group          PID      Status
pscuiserver        pscuiserver   15466980  active
```

Example 4-23 shows starting the MFA GUI on AIX.

Example 4-23 Starting the MFA GUI

```
# startsrc -s pscuiserver
0513-059 The pscuiserver Subsystem has been started. Subsystem PID is 15466982.
```

Example 4-24 shows stopping the MFA GUI on AIX.

Example 4-24 Stop the MFA GUI

```
# stopsrc -s pscuiserver  
0513-044 The pscuiserver Subsystem was requested to stop.
```

Configuring MFA GUI users and managing the administration IDs

Unlike the PowerSC GUI, MFA GUI users do not have to be members of the security group. Also, all control is done by using the pmfa_administrator_util utility.

This section shows some common examples of the use of this utility:

- ▶ Add users

Use the following command (see Example 4-25):

```
/opt/IBM/powersc/MFA/bin/pmfa_administrator_util <username> <Role>
```

Where the Role can be NONE, READ, ADD, UPDATE, DELETE, CONTOL, or SUPERADMIN.

Example 4-25 Creating a super admin user

```
/opt/IBM/powersc/MFA/bin/pmfa_administrator_util add pscadm SUPERADMIN  
Successfully added/updated administrator user pscadm with permission SUPERADMIN
```

- ▶ List users (see Example 4-26)

Use the following command:

```
/opt/IBM/powersc/MFA/bin/pmfa_administrator_util list
```

Example 4-26 List users

```
/opt/IBM/powersc/MFA/bin/pmfa_administrator_util list  
adminuser: SUPERADMIN  
user1: DELETE,UPDATE,READ
```

- ▶ Delete users

Use the command:

```
/opt/IBM/powersc/MFA/bin/pmfa_administrator_util delete <username>
```

4.6.2 Configuring the timed-based one-time password authentication

A user that is configured to use TOTP authentication can log in by using quick response (QR) codes on an Android or Apple iOS device.

A QR code application, such as IBM Verify, Google Authenticator, or Duo Mobile must be installed. Then, the users logs in by using their user name and the TOTP that is generated by their device. The TOTP that is entered must match the TOTP that is generated by the MFA server.

PowerSC MFA supports the following authentication methods:

- ▶ In-band
- Users generate the suitable token and use it directly to log in.
- ▶ Out-of-band

Users authenticate with a specific web page in the MFA GUI by using the required authentication methods. A cached token credential (CTC) is created with which they can use to authenticate with the required applications.

The following process is used to configure an authentication method for a user:

1. An authentication method is created and activated.
2. A policy is created.
3. The users are provisioned and a policy is assigned.

These steps are described next.

Creating the authentication method

Complete the following steps to configure the TOTP authentication method:

1. Log in to the MFA GUI as an administrator, as shown in Figure 4-22.

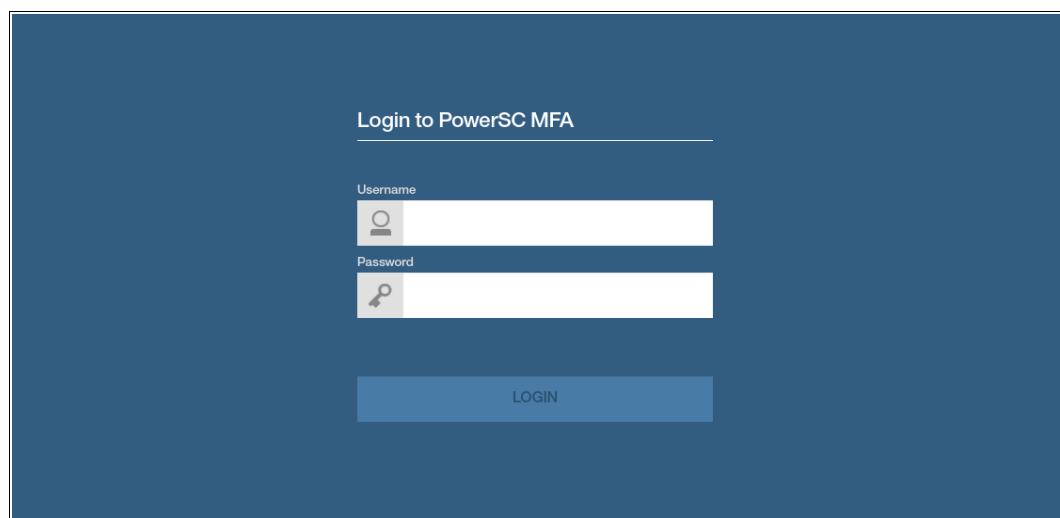


Figure 4-22 Logging in to PowerSC MFA GUI

2. Select the **Authentication Methods** tab and then, select the **TOTP authentication method** on the left side, as shown in Figure 4-23.

Figure 4-23 Selecting TOTP authentication method

3. Enter the following configuration:

- Consecutive failures before TOTP suspension: Limits the number of consecutive times a user fails to provide a valid TOTP before disabling the user. The value of 0 disables the user.
- Trace level: Values are 0 - 3.
- Enable single key encryption: If enabled, a single factor-level encryption key is used when user registration information is encrypted. It is recommended that it is enabled because it reduces the proliferation of encryption keys.
- Realm name: The realm name for your web services server is used to generate the label for the users TOTP account. This label uses the following in the form:
`<user ID>@<Realm Name>`
- Digest algorithm: TOTP uses the digest algorithm, shared secret key, and current time to generate the TOTP value. Choices are SHA1, SHA256, SHA384, and SHA512.
- Token digits: The number of digits that is generated by the token. Choices are 6, 7, or 8.
- Authentication window: The skew interval to allow for a delay in synchronization between the MFA Server and the client. Each interval is 30 seconds and allows for that number of intervals in the past and the future. Therefore, a value of 1 allows for the passwords that were generated 30 seconds ago, the current 30 seconds, and the next 30 seconds.
- Token period seconds: The number of seconds before the next value of the token is generated. Choices are 15, 30, and 60 seconds.

4. Select **Save**.

5. Select **Configuration → Server Options** and then, enable **TOTP Services**.

6. Restart the MFA Server from the command line (as shown in Example 4-27) or from under the Settings tab in the GUI.

Example 4-27 Restarting MFA Server

```
$ stopsrc -s pmfad
$ startsrc -s pmfad
$ lssrc -s pmfad
$ Subsystem          Group          PID          Status
pmfad                           1             active
```

Creating a policy definition

Complete the following steps to create a policy definition:

1. After logging in to the MFA GUI as an administrator, select the **Policy Definitions** tab, as shown in Figure 4-24.

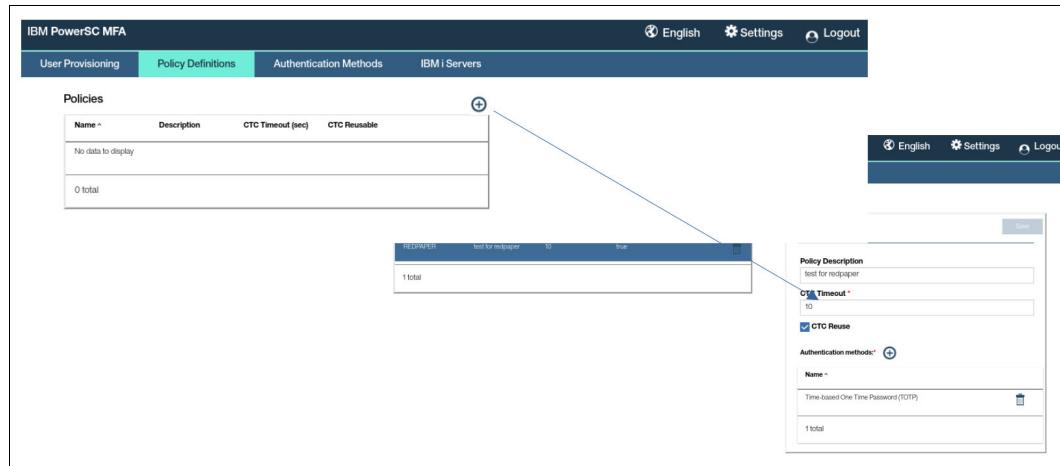


Figure 4-24 IBM PowerSC MFA GUI: Policy Definitions

2. Click + to create a Policy Definition and enter the following information:
 - Policy name: A name for the policy (start with a character; no spaces are allowed).
 - Policy description: A description for the policy.
 - CTC timeout: The number of seconds that the cached credential is valid for before it times out.
 - CTC reuse: Select whether you want the cached token credential to be reusable during the timeout period.
3. Click + to add an authentication method. The available methods are displayed.
4. Select the authentication methods and save.

For this example, a policy called redpaper was created.

Note: The policy name is displayed as REDPAPER, but the user can use the name in lower case for in-band and out-of-band authentication.

Provisioning users and assigning a policy

Users can be provisioned by using the GUI or the command line.

Bulk provisioning of users

Installing the MFA Server also installs the following programs to provision users and define their policies. IBM PowerSC MFA provides programs and shell scripts that you can use to provision users with policies:

- ▶ **pmfauser ingest**: An AIX-only command that reads a user-created text file to provision those users (without assigning a policy or authentication method). The text file can be created by running the `lsuser -C -a gecos {ALL|user_list}` command.
- ▶ **pmfabulk**: A general program that reads a user-created text file to provision users. The text file includes one record per line with the following fields (separated by a space):
 - User ID
 - Policy Name
 - Authentication Method
 - ADD (and optionally supply USERNAME= to add GECOS details)

Two scripts are generated, which can be checked before running the provision of the users.

For more information, see [IBM PowerSC Multi-Factor Authentication Version 1.1.0: Installation and Configuration](#).

Provisioning the user by using the GUI

Complete the following steps to provision the user by using the GUI:

1. Log in to the MFA GUI and select the **User Provisioning** tab.
2. Click **+** that is next to the user icon, as shown in Figure 4-25.

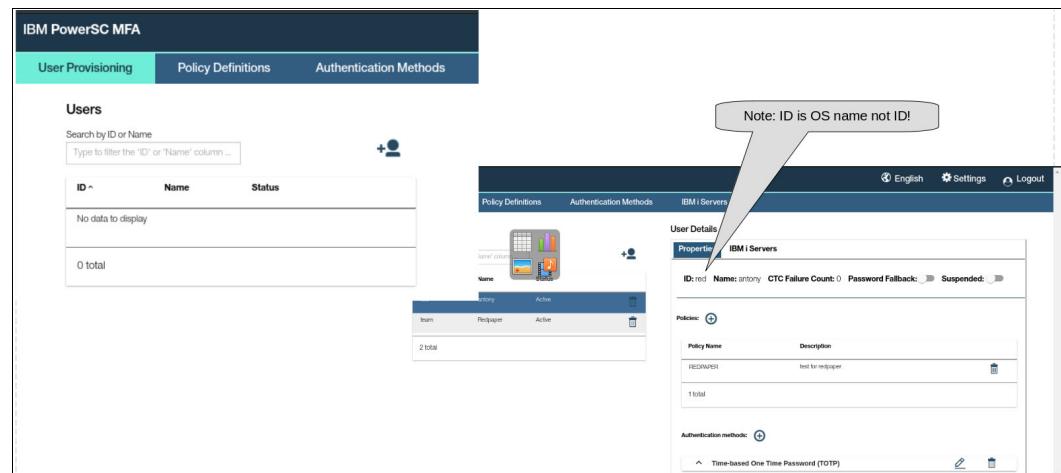


Figure 4-25 IBM PowerSC MFA: User Provisioning

3. Enter the following information for the user:
 - MFA ID: This ID is the AIX or Linux user name. It is *not* the UID.
 - Name: The MFA name for the user.
 - Password fallback: If the authentication fails, the user can log in by using their AIX or Linux password.
4. Click **Save** to store the details.

- Click **+** to add a policy for the user. All available policies are displayed. Select one or more policies for the user.

Note: If no policy is selected for the user, MFA assumes that password fallback was configured for the user, regardless of the user setting.

- The authentication method for the selected policy is added. Select the edit icon to configure the registration details, as shown in Figure 4-26.

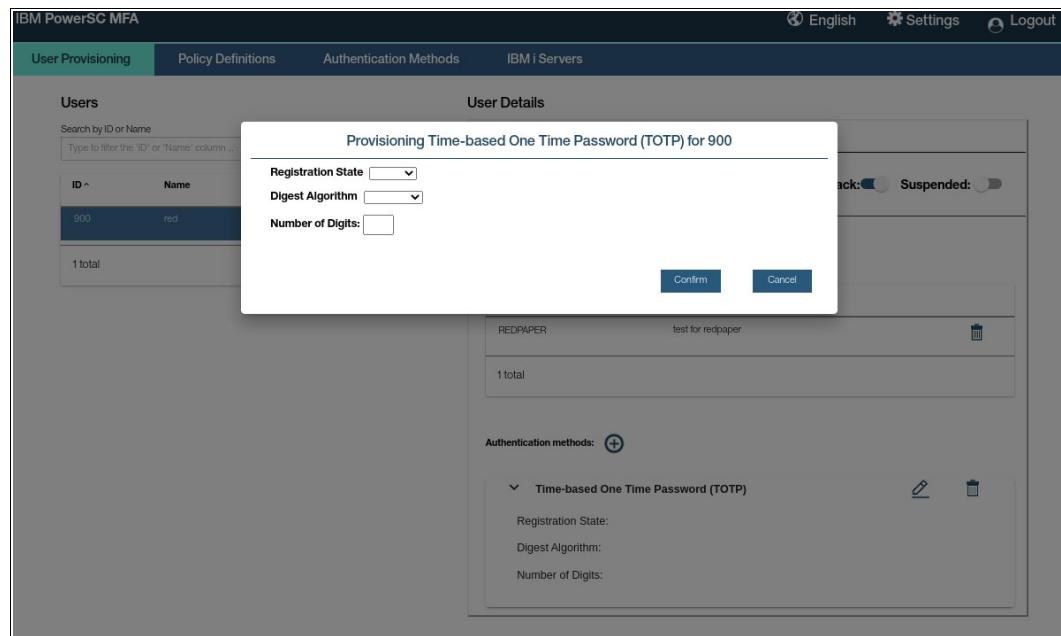


Figure 4-26 IBM PowerSC MFA: User Details

- Configure the following information:
 - Registration state: Select **OPEN** so that a user can register their TOTP device.
 - Digest algorithm: Select the suitable digest algorithm.
 - Number of digits: Select the number of digits for the token.
- Click **Confirm**.

This example created a user to use the redpaper policy and the TOTP authentication method.

After the user is created, the administrator can modify the users password fallback status or suspend or reactivate the user. This setting is required if the user exceeds their CTC failure count and is suspended.

Preparing the user to use TOTP authentication

After the user installs the application, their device must be enrolled with the MFA Server.

The user must perform the following steps:

- Install the QR code application.
- Go to the TOTP enrollment page:

https://<mfa_server>:6793/AZFTOTP1/genericStart

- Enter their AIX or Linux username and password, as shown in Figure 4-27. Then, they scan the image by using the authentication application.

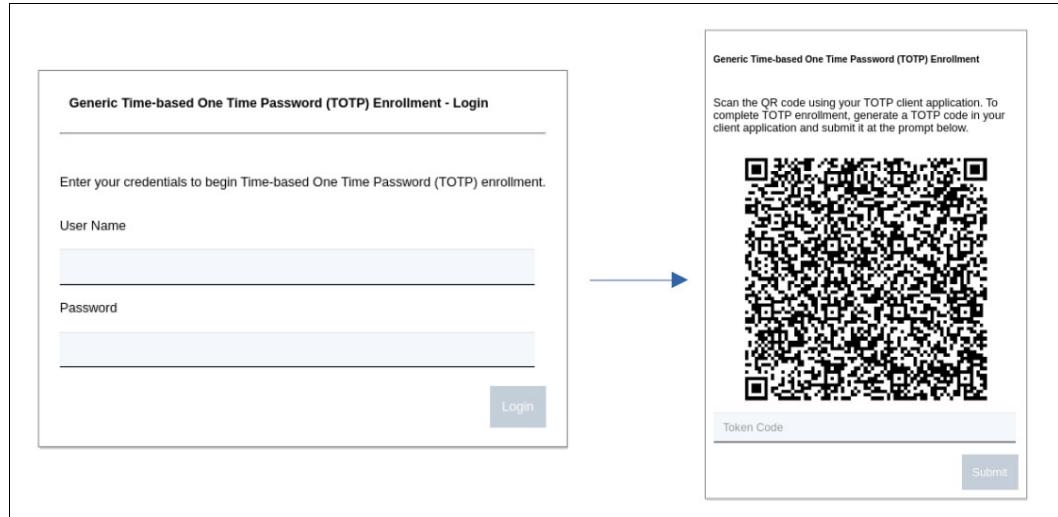


Figure 4-27 Enrollment window for TOTP

Note: At the time of this writing, an issue occurred with the Google Authenticator Application while testing by using AIX 7.3 and PowerSC MFA 2.0.0.2. However, the IBM Security Verify application worked.

- After successfully authenticated, a QR code is displayed. This code is scanned by the user's application. This scanning creates a token generator with the name <user>@<realm name>.
- The user enters the token value and clicks **Submit** to confirm validity of the token, as shown in Figure 4-28.

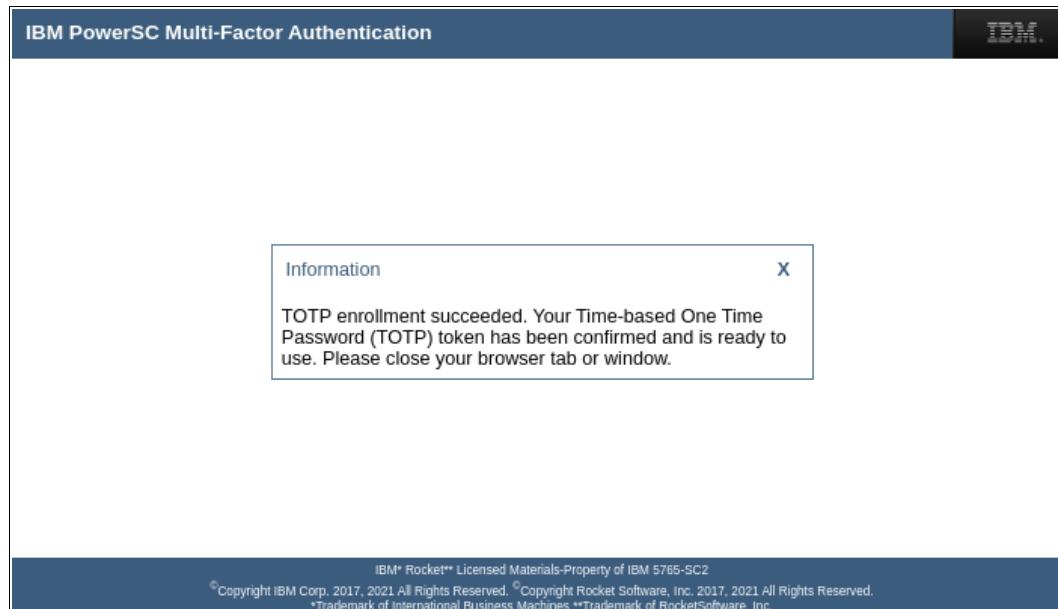


Figure 4-28 TOTP device enrolled successfully

4.6.3 Troubleshooting

The following information is useful when troubleshooting the PowerSC MFA Server:

- ▶ To start the MFA Server database

```
su - postgres
pg_ctl -D /opt/IBM/powersc/MFA/mfadb start
```
- ▶ To stop the MFA Server database

```
su - postgres
pg_ctl -D /opt/IBM/powersc/MFA/mfadb stop
```
- ▶ MFA Server Logs: The MFA Server logs are in /var/log/powersc/MFA.
- ▶ PowerSC MFA Server URLs:
 - The Server URL:
`https://<Server_Address>:6793/mfaadmin/index.html`
 - The MFA Policy out-of-band URL:
`https://<Server_Address>:6793/mfa/<POLICY_NAME>`
For example, for TOTP:
`https://mfa_server:6793/mfa/<AZFTOTP1>`

4.6.4 Configuring AIX SSH client for MFA

Complete the following steps to configure an AIX client to use MFA:

1. Install the following filesets:
 - powerscMFA.license
 - powerscMFA.pam.base

This module processes IBM PowerSC MFA credentials for provisioned users and fails incorrect IBM PowerSC MFA credentials.

 - powerscMFA.pam.fallback

When you use password fallback, this module must be installed.
2. Configure a truststore on each client so that the client trusts the MFA Server. Consider the following points:
 - If you are not configuring the MFA GUI Server HA, copy `gui_server.pem` to `/etc/security/pmfa/certificates` on each client.
 - If you are configuring the MFA GUI Server for availability:

```
cat server1.pem > mfa_keys.pem
cat server2.pem >> mfa_keys.pem
```

copy `mfa_keys.pem` to `/etc/security/pmfa/certificates` on each client.
3. Modify the `/etc/security/pmfa/pam_pmfa.conf` file with the following information (see Example 4-28 on page 149):
 - TRUSTEDCAS: Use the truststore from Step 1.
 - MFA-URL: The URL for the MFA server.
 - MFA-URL2,3: The Availability options.
 - CTC-PROMPT-ONLY: If set to Y, only out-of-band authentication by using a cached token is allowed; setting to N allows for both.

Example 4-28 Modified pam_pmfa.conf file

```
# IBM PowerSC Multi-Factor Authentication - pam_pmfa configuration file

# The TRUSTEDCAS directive is required. It specifies the fully qualified
# path to file containing a concatenation of PEM-format X.509 certificates.
TRUSTEDCAS = /etc/security/pmfa/certificates/mfa_keys.pem
or
TRUSTEDCAS = /etc/security/pmfa/certificates/mfa_server.pem

# The MFA-URL directive is required. It specifies the URL of the
# PowerSC MFA server. Optionally, MFA-URL2 and MFA-URL3 can be used to
# specify fallback servers.
MFA-URL = https://mfa_server:6793/policyAuth/
#MFA-URL2 = https://pmfa2.example.com:6793/policyAuth/
#MFA-URL3 = https://pmfa3.example.com:6793/policyAuth/

# When enabled, CTC-PROMPT-ONLY instructs the PAM module to only support CTC
# credentials, and disables support for policy based in-band authentication.
CTC-PROMPT-ONLY = N
```

4. Add the entries to the /etc/pam.conf file, as shown in Example 4-29.

Example 4-29 Additions to pam.conf

sshd	auth	required	/usr/lib/security/pam_ckfile
sshd	auth	required	/usr/lib/security/pam_permission file=/etc/security/access.conf found=allow
sshd	auth	required	/usr/lib/security/pam_aix
sshd	auth	required	/usr/lib/security/pam_pmfa /etc/security/pmfa/pam_pmfa.conf
sshd	auth	required	/usr/lib/security/pam_pmfa_fallback /etc/security/pmfa/pam_pmfa.conf
sshd	account	required	/usr/lib/security/pam_aix
sshd	password	required	/usr/lib/security/pam_aix
sshd	session	required	/usr/lib/security/pam_aix
sshd	session	optional	/usr/lib/security/pam_mkuserhome

The following options and modules are available:

- pam_ckfile: Denies all non-root user logins if /etc/nologin or an optionally specified file is present.
- pam_aix: The AIX PAM module.
- pam_pmfa: The PowerSC MFA PAM module.
- pam_pmfa_fallback: The PowerSC MFA PAM module to allow password fallback.
- pam_permission: An authentication and account-service PAM module that uses an access-control list to determine whether to permit or deny authentication requests. The module scans the file by using the authenticating user name and groups. The first match is then used to determine the result.

An entry in the access-control file uses the following general syntax:

[+|-] [@]<name>

The use of found={allow | prohibit} determines the action if the matched entry is not preceded by a "+" or "-". The default is prohibit.

- pam_mkuserhome: This module creates a home directory on login if it does not exist.

- Authentication: Authenticates a user through their AIX password.
- Account management: Verifies that an authenticated user is permitted onto the system and checks for expired passwords. Checks are performed by using the `passwdexpired()` and `loginrestrictions()` subroutines.
- Session management: Opens a new session and logs the session information.
- Password management: Allows a user to set or modify their AIX password if it is possible. Then, `pam_aix` updates the user's password entry in the suitable password table. When `pam_aix` is used for password management, it is used as required or requisite.

The following rules dictate the stacking behavior of the modules:

- Required: All required modules in a stack must pass for a successful result. If one or more of the required modules fail, all of the required modules in the stack are attempted, but the error from the first failed required module is returned.
- Requisite: Similar to Required rule, except that if a requisite module fails, no other modules in the stack are processed and it immediately returns the first failure code from a Required or Requisite module.
- Sufficient: If a module flagged as Sufficient succeeds and no previous Required modules failed, all remaining modules in the stack are ignored and success is returned.
- Optional: If none of the modules in the stack are required and no sufficient modules succeeded, at least one optional module for the service must succeed. If another module in the stack is successful, a failure in an optional module is ignored.

5. Change the `/etc/ssh/sshd_config` file as shown in Example 4-30.

Example 4-30 Changes to sshc_config file

```
UsePAM yes
ChallengeResponseAuthentication yes
```

6. Change `auth_type` to `PAM_AUTH` in `/etc/security/login.cfg`, as shown in Example 4-31.

Example 4-31 Changes to login.cfg

```
usw:
    shells =
/bin/sh,/bin/bsh,/bin/csh,/bin/ksh,/bin/tsh,/bin/ksh93,/usr/bin/sh,/usr/bin/bsh
,/usr/bin/csh,/usr/bin/ksh,/usr/bin/tsh,/usr/bin/ksh93,/usr/bin/rksh,/usr/bin/r
ksh93,/usr/sbin/uucp/uucico,/usr/sbin/sliplogin,/usr/sbin/snappd
    maxlogins = 32767
    logintimeout = 30
    maxroles = 8
    auth_type = PAM_AUTH
    pwd_algorithm = ssh256
```

7. Restart the `sshd` daemon, as shown in Example 4-32.

Example 4-32 Restart sshd

```
stopsrc -s sshd
startsrc -s sshd
```

8. Users can now log in either using in-band or out-of-band authentication.

- a. Using in-band authentication as shown in Example 4-33.

Example 4-33 Example of in-band authentication

```
# ssh red@psc72-2
red's Password:
Type MFA Policy Name or press Enter for CTC: redpaper
Enter your TOTP credential:
Last unsuccessful login: Mon Oct 25 01:09:25 CDT 2021 on ssh from 192.168.140.109
Last login: Mon Oct 25 01:31:53 CDT 2021 on ssh from 192.168.140.109
*****
*
*
*   Welcome to AIX Version 7.2!
*
*
*   Please see the README file in /usr/lpp/bos for information pertinent to
*   this release of the AIX Operating System.
*
*
*****
psc72-2:/home/red$
```

By using out-of-band authentication, the user gets their cached token from the address: https://mfa_server:6793/mfa.

- b. Enter the policy name (in this example, redpaper) and click **Continue**, as shown in Figure 4-29.

The screenshot shows a web-based interface titled "IBM PowerSC Multi-Factor Authentication". At the top right is the IBM logo. The main content area has a title "PowerSC MFA Out of Band Interface". Below it is a "Policy Name" label followed by an input field. At the bottom right of the input field is a "Continue" button. The footer contains legal text: "IBM® Rocket® Licensed Materials-Property of IBM 5765-SC2", "©Copyright IBM Corp. 2017, 2021. All Rights Reserved.", "©Copyright Rocket Software, Inc. 2017, 2021 All Rights Reserved.", and "Trademark of International Business Machines ®Trademark of RocketSoftware, Inc."

Figure 4-29 Enter the policy name

- c. In the next window, you are prompted for your User ID and the TOTP credential from your device, as shown in Figure 4-30.

The screenshot shows a web-based authentication interface. At the top, a dark blue header bar displays the text "IBM PowerSC Multi-Factor Authentication" on the left and the "IBM" logo on the right. Below the header, the main content area has a light gray background. On the left side of the content area, there is a vertical white sidebar containing the text "REDPAPER". The main content area contains two input fields: one labeled "User ID" with the value "red" entered, and another labeled "Time-based One Time Password (TOTP)" with a placeholder "Enter your TOTP credential" and a masked input field showing "*****". A "Submit" button is located at the bottom right of the main content area. At the very bottom of the page, a dark blue footer bar contains the text "IBM® Rocket® Licensed Materials-Property of IBM 5765-SC2", "©Copyright IBM Corp. 2017, 2021 All Rights Reserved.", "©Copyright Rocket Software, Inc. 2017, 2021 All Rights Reserved.", and "★Trademark of International Business Machines ★Trademark of RocketSoftware, Inc."

Figure 4-30 Entering the User ID and TOTP password

- d. Get the TOTP Credential from your device, as shown in Figure 4-31.

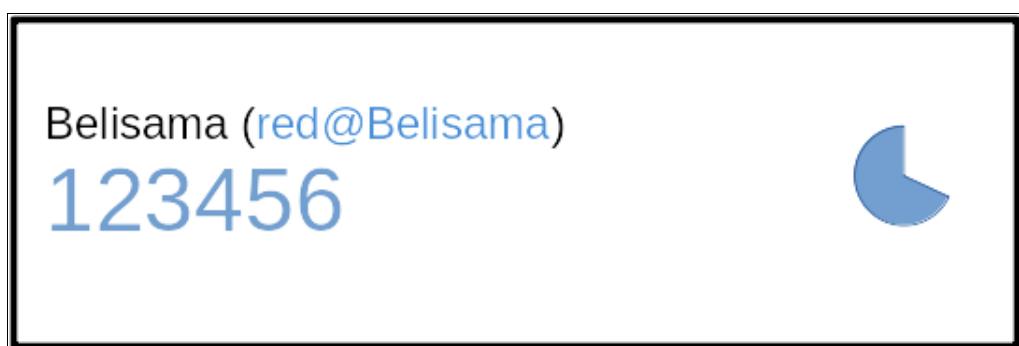


Figure 4-31 TOTP Credential displayed on device

- e. Copy the CTC from the next window, as shown in Figure 4-32.



Figure 4-32 Copy CTC credential

- f. Log in to the SSH client by using the following information (see Example 4-34):

- User ID: UNIX user name.
- Password: UNIX password.
- No Policy name: Press **Enter** to use CTC.
- Enter CTC: The CTC that was copied from the previous step (see Figure 4-32).

Example 4-34 SSH to the client

```
ssh red@psc72-2
red's Password:
Type MFA Policy Name or press Enter for CTC:
Enter CTC:
Last unsuccessful login: Mon Oct 25 01:09:25 CDT 2021 on ssh from
192.168.140.109
Last login: Mon Oct 25 01:43:21 CDT 2021 on ssh from 192.168.140.109
*****
*                                                 *
*                                                 *
*   Welcome to AIX Version 7.2!                 *
*                                                 *
*                                                 *
*   Please see the README file in /usr/lpp/bos for information pertinent to      *
```

```
* this release of the AIX Operating System.  
*  
*  
*****  
psc72-2:/home/red$
```

4.6.5 Configuring Linux SSH Client for MFA

Complete the following steps to configure a Linux client to use MFA:

1. Run the following scripts:

- pmfa-pambase-2.0.0.0-2108121024.rhel8.ppc64le.sh
 - pmfa-pamfallback-2.0.0.0-2108121025.rhel8.ppc64le.sh
- If password fallback is used, this script must be run.

Note: If you rerun the installation for any reason, the PAM configuration file (`/etc/security/pmfa/pam_pmfa.conf`) is overwritten and the previous version is saved as `pam_pmfa.conf.rpmnew`.

2. Configure a truststore on each client for the client to trust the MFA Server.

- If you are not configuring the MFA GUI Server for high availability (HA), copy `gui_server.pem` to `/etc/security/pmfa/certificates` on each client.
- If you are configuring the MFA GUI Server for availability, run the following commands:

```
# cat server1.pem > mfa_keys.pem  
# cat server2.pem >> mfa_keys.pem
```

Copy `mfa_keys.pem` to `/etc/security/pmfa/certificates` on each client.

3. Modify the `/etc/security/pmfa/pam_pmfa.conf` file with the following settings (see Example 4-35):

- TRUSTEDCAS: Use the truststore from Step 2.
- MFA-URL: The URL for the MFA Server.
- MFA-URL2,3: Availability options.
- CTC-PROMPT-ONLY: If set to Y, it allows only out-of-band authentication by using a cached token. If set to N, it allows for both.

Example 4-35 Modified pam_pmfa.conf file

```
# IBM PowerSC Multi-Factor Authentication - pam_pmfa configuration file  
  
# The TRUSTEDCAS directive is required. It specifies the fully-qualified  
# path to file containing a concatenation of PEM-format X.509 certificates.  
TRUSTEDCAS = /etc/security/pmfa/certificates/mfa_keys.pem  
or  
TRUSTEDCAS = /etc/security/pmfa/certificates/mfa_server.pem  
  
# The MFA-URL directive is required. It specifies the URL of the  
# PowerSC MFA server. Optionally, MFA-URL2 and MFA-URL3 can be used to  
# specify fallback servers.  
MFA-URL = https://mfa_server:6793/policyAuth/  
#MFA-URL2 = https://pmfa2.example.com:6793/policyAuth/  
#MFA-URL3 = https://pmfa3.example.com:6793/policyAuth/
```

```
# When enabled, CTC-PROMPT-ONLY instructs the PAM module to only support CTC  
# credentials, and disables support for policy based in-band authentication.  
CTC-PROMPT-ONLY = N
```

4. Add the entries to /etc/pam.conf, as shown in Example 4-36.

Example 4-36 Additions to pam.conf

```
 #%PAM-1.0  
auth required pam_sepermit.so  
auth sufficient pam_pmfa.so /etc/security/pmfa/pam_pmfa.conf  
auth required pam_pmfa_fallback.so /etc/security/pmfa/pam_pmfa.conf  
auth substack password-auth  
auth include postlogin
```

4.7 PowerSC MFA 2.0 high availability

Before PowerSC MFA 2.0, HA was configured by using shared storage. However, this configuration was not always suitable for many customers, particularly those customers who did not have storage that is shared across sites (and did not want to add Geographic Logical Volume Manager to the mix).

To get around this limitation, some customers configured database replication by using [Postgres Write Ahead Logs](#) (WAL). This solution was a simple and reliable and is now officially supported by IBM PowerSC MFA 2.0.

Note: This configuration is purely for HA and not load balancing because only one of the PowerSC MFA Servers is available at any one time.

The active Postgres database is replicated to a remote secondary copy (standby database), which is in read-only mode. If the primary PowerSC MFA server becomes unavailable, the database on the secondary server can be promoted from standby. Only one copy of the database can be primary at any time.

Note: Only the database is replicated. Any files that are in /opt/IBM/powersc/MFA/mfadb must be backed up before PowerSC MFA is reinstalled.

For the scenario that is presented here, we tested by using PowerSC MFA 2.0.0.2 and AIX 7.3. When another operating system (IBM i or Linux) is used, extra steps can be required (for more information, see this [IBM Documentation web page](#)).

4.7.1 Configuring the servers

For the lab environment, we used two AIX LPARs (see Table 4-3) that were installed with AIX 7.3.

Table 4-3 Laboratory environment

Server	Private network
server_prod	192.168.1.1
server_dr	192.168.1.2

Complete the following steps to configure two PowerSC MFA Servers in a highly available configuration:

1. On the primary server:

- a. Install and configure IBM PowerSC MFA by using the steps that are described in 4.6.1, “Configuring the MFA Server” on page 137.
- b. Export the PKCS#11 token (as shown in Example 4-37), which is used for the primary server and copy it to the secondary server, bu using the following command:

```
pmfa_masterkey_transport -e|-i <Data File name> <Token Name>
```

Where:

- -i: Import the key stored that is in data file into the local PKCS11 token.
- -e: Export the local master key into the specified data file.

Example 4-37 Exporting the PKCS#11 token

```
# /opt/IBM/powersc/MFA/bin/pmfa_masterkey_transport -e mfa_tok mfatest
Created PBKDF2 password hashing context: (pwhashCtx:0x2000a5b8)
Enter transport password:
Confirm Enter transport password password:
Exporting master key to file mfa_tok
Successfully exported master key from token mfatest to file mfa_tok
```

- c. Copy the data file (mfa_tok, as shown in Example 4-37) to the secondary server.

2. On the secondary server:

- a. Create the PKCS#11 token (see “Creating a PKCS#11 token” on page 137).
- b. Import the created data file, as shown in Example 4-38.

Example 4-38 Importing the data file on secondary server

```
# /opt/IBM/powersc/MFA/bin/pmfa_masterkey_transport -i mfa_tok mfatest
Created PBKDF2 password hashing context: (pwhashCtx:0x2000a5b8)
Enter transport password:
Confirm Enter transport password password:
Importing key from mfa_tok into Token name mfatest.
Successfully imported key data from file 536904744 and inserted into token
mfatest with label PMFASTC.AESKEY
```

- c. Ensure that the secondary server truststore file has the same location and name as it does on the primary server.

Note: If the SecurID authentication method or IBM i are used, extra steps are required, as described next.

- a. Install the IBM PowerSC MFA software, as described in 4.6.1, “Configuring the MFA Server” on page 137. Check that the same prerequisites are met.
- b. Edit the PAM configuration as primary and add the lines that are shown in Example 4-39.

Example 4-39 Lines to add to /etc/pam.conf

```
pmfaserver auth required pam_ckfile
pmfaserver auth required pam_permission
file=/etc/security/access.conf found=allow
pmfaserver auth required pam_aix
```

3. On the primary server:

- a. As the postgres user, create a postgres replication user, as shown in Example 4-40.

Example 4-40 Creating the postgres replication user

```
# su - postgres
$ createuser -P -c5 --replication mfarePLIC
Enter password for new role:
Enter it again:
```

- b. Create an archive directory; for example, /opt/IBM/powersc/MFA/mfadb/archive.
 - c. Add the replication details to pg_hba.conf, as shown in Example 4-41.

Example 4-41 Lines to add to /opt/IBM/powersc/MFA/mfadb/pg_hba.conf

```
#MFA HA Hack
host    replication    mfarePLIC      192.168.1.2/32      md5
#End of MFA HA Hack
```

- d. Add the secondary server details to postgresql.conf, as shown in Example 4-42.

Example 4-42 Lines to add to /opt/IBM/powersc/MFA/mfadb/postgresql.conf

```
#MFA HA Hack
listen_addresses = '*'
wal_level = replica
archive_mode = on
archive_command = 'test ! -f /opt/IBM/powersc/MFA/mfadb/archive/%f && cp %p
/opt/IBM/powersc/MFA/mfadb/archive/%f'
#End MFA HA Hack
```

- e. Stop and start the database, as shown in Example 4-43.

Example 4-43 Stopping and starting the database

```
$ pg_ctl -D /opt/IBM/powersc/MFA/mfadb restart
waiting for server to shut down.... done
server stopped
waiting for server to start...2021-12-14 17:23:03.442 CST [6947094] LOG:
listening on IPv4 address "0.0.0.0", port 5432
```

```
2021-12-14 17:23:03.442 CST [6947094] LOG: listening on IPv6 address "::",
port 5432
.2021-12-14 17:23:03.444 CST [6947094] LOG: listening on Unix socket
"/tmp/.s.PGSQL.5432"
2021-12-14 17:23:03.499 CST [9765178] LOG: database system was shut down at
2021-12-14 17:23:03 CST
2021-12-14 17:23:03.524 CST [6947094] LOG: database system is ready to
accept connections
done
server started
```

- f. Exit as the postgres user.
4. On the secondary server:
 - a. As the postgres user, stop the database, as shown in Example 4-44.

Example 4-44 Stopping the postgres database

```
# su - postgres
$ pg_ctl -D /opt/IBM/powersc/MFA/mfadb stop
waiting for server to shut down.... done
server stopped
```

- b. As the root user, remove the database, as shown in Example 4-45.

Example 4-45 Removing the postgres database on the secondary server

```
$ exit
psc73-2:/etc# cd /opt/IBM/powersc/MFA/mfadb
# rm -fr *
```

- c. Confirm that /opt/IBM/powersc/MFA/mfadb permissions are set as 700.
- d. As the postgres user, copy the database from the primary server, as shown in Example 4-46. The command can take a couple of minutes before completing.

Example 4-46 Copying the primary database to the secondary server

```
# su - postgres
psc73-2:/var/lib/postgresql$ pg_basebackup -h 192.168.1.2 -U mfarePLIC
--checkpoint=fast -D /opt/IBM/powersc/MFA/mfadb -R
Password:
```

- e. List the contents of the database directory to check the success of the initial copy.
- f. Start the database running on the secondary server to receive the updates from the primary server, as shown in Example 4-47.

Example 4-47 Starting the secondary database in standby mode

```
$ pg_ctl -D /opt/IBM/powersc/MFA/mfadb start
waiting for server to start....2021-12-14 17:37:36.238 CST [9765174] LOG:
listening on IPv4 address "0.0.0.0", port 5432
2021-12-14 17:37:36.239 CST [9765174] LOG: listening on IPv6 address "::",
port 5432
2021-12-14 17:37:36.241 CST [9765174] LOG: listening on Unix socket
"/tmp/.s.PGSQL.5432"
2021-12-14 17:37:36.296 CST [9306428] LOG: database system was interrupted;
last known up at 2021-12-14 17:30:42 CST
```

```
2021-12-14 17:37:36.352 CST [9306428] LOG: entering standby mode
2021-12-14 17:37:36.358 CST [9306428] LOG: redo starts at 0/2000028
2021-12-14 17:37:36.361 CST [9306428] LOG: consistent recovery state
reached at 0/2000130
2021-12-14 17:37:36.363 CST [9765174] LOG: database system is ready to
accept read only connections
2021-12-14 17:37:36.382 CST [10092862] LOG: started streaming WAL from
primary at 0/3000000 on timeline 1
done
server started
```

This scenario has created a running IBM PowerSC MFA instance on the primary server with the database being replicated to the secondary server.

4.7.2 Changing the PowerSC MFA clients

Previously, the MFA PAM configuration used the certificate for a single server. However, because two servers are used now, a certificate must be built that can use both servers. The URL for both servers also must be defined.

If you do not follow these steps, you must change the pam_pmfa.conf file on every client whenever the active MFA server changes.

Complete the following steps to create a concatenation of certificates:

1. Run the following commands:

```
# cat <Prim_Server>.pem > mfa_keys.pem
# cat <Sec_Server>.pem >> mfa_keys.pem
```

2. Modify the pam_pmfa.conf file, as shown in Example 4-48.

Example 4-48 Changing /etc/security/pmfa/pam_pmfa.conf

```
# IBM PowerSC Multi-Factor Authentication - pam_pmfa configuration file

# The TRUSTEDCAS directive is required. It specifies the fully qualified
# path to file containing a concatenation of PEM-format X.509 certificates.
TRUSTEDCAS = /etc/security/pmfa/certificates/mfa_keys.pem

# The MFA-URL directive is required. It specifies the URL of the
# PowerSC MFA server. Optionally, MFA-URL2 and MFA-URL3 can be used to
# specify fallback servers.
MFA-URL = https://192.168.1.1:6793/policyAuth/
MFA-URL2 = https://192.168.1.2:6793/policyAuth/
#MFA-URL3 = https://pmfa3.example.com:6793/policyAuth/

# When enabled, CTC-PROMPT-ONLY instructs the PAM module to only support CTC
# credentials, and disables support for policy based in-band authentication.
CTC-PROMPT-ONLY = N
```

4.7.3 Switching the active IBM PowerSC MFA server

For this scenario, assume that the primary server is unavailable and that you must revert or use the secondary server.

For testing, complete the following steps to stop the MFA instance on the primary server, as shown in Example 4-49:

Example 4-49 Stopping the MFA instance on the primary server

```
# stopsr -s pmfad  
0513-044 The pmfad Subsystem was requested to stop.
```

1. On the nonactive server (which in this case is the secondary server):

- a. Promote the database replica to primary, as shown in Example 4-50.

Example 4-50 Promoting the standby database on the secondary

```
# su - postgres  
$ pg_ctl -D /opt/IBM/powersc/MFA/mfadb promote  
waiting for server to promote....2021-12-14 17:40:15.295 CST [9306428] LOG:  
received promote request  
2021-12-14 17:40:15.295 CST [10092862] FATAL: terminating walreceiver  
process due to administrator command  
2021-12-14 17:40:15.298 CST [9306428] LOG: invalid record length at  
0/30013E0: wanted 24, got 0  
2021-12-14 17:40:15.298 CST [9306428] LOG: redo done at 0/30013A8  
2021-12-14 17:40:15.299 CST [9306428] LOG: last completed transaction was  
at log time 2021-12-14 17:39:10.170267-06  
2021-12-14 17:40:15.300 CST [9306428] LOG: selected new timeline ID: 2  
2021-12-14 17:40:15.827 CST [9306428] LOG: archive recovery complete  
done  
server promoted  
2021-12-14 17:40:15.908 CST [9765174] LOG: database system is ready to  
accept connections
```

- b. Start the PowerSC MFA server as root, as shown in Example 4-51.

Example 4-51 Start PowerSC MFA server

```
# startsr -s pmfad  
0513-059 The pmfad Subsystem has been started. Subsystem PID is 9568640.  
  
# lssrc -s pmfad  
Subsystem           Group          PID      Status  
pmfad                           9568640    active
```

- c. Check that the GUI is working.

After the primary server is available, complete the following steps to configure the database to run in standby mode and secondary server, which is now the active MFA instance:

1. On the secondary server:

- Correct the replication details in the pg_hba.conf file because it is pointing to itself, as shown in Example 4-52.

Example 4-52 Changing pg_hba.conf to point to the primary (now standby) server

```
MFA HA hack
host    replication      mfarePLIC      192.168.1.1/32      md5
#End of MFA HA hack
```

- Stop and restart the database, as shown in Example 4-53.

Example 4-53 Stopping and restarting the database

```
$ pg_ctl -D /opt/IBM/powersc/MFA/mfadb restart
waiting for server to shut down..... done
server stopped
waiting for server to start....2021-12-14 23:30:21.073 CST [9699636] LOG:
listening on IPv4 address "0.0.0.0", port 5432
2021-12-14 23:30:21.073 CST [9699636] LOG: listening on IPv6 address "::",
port 5432
2021-12-14 23:30:21.110 CST [9699636] LOG: listening on Unix socket
"/tmp/.s.PGSQL.5432"
2021-12-14 23:30:21.223 CST [10682714] LOG: database system was shut down
at 2021-12-14 23:30:20 CST
2021-12-14 23:30:21.303 CST [9699636] LOG: database system is ready to
accept connections
done
server started
```

- When the primary server recovers, you can choose to promote it to primary, or to keep running on the secondary server.

4.7.4 Administrative tasks

In addition to the steps to change servers in a highly available configuration (see 4.7.3, “Switching the active IBM PowerSC MFA server” on page 160), it is also recommended to create a backup of the Postgres database, as shown in Example 4-54.

Example 4-54 Creating a backup of the Postgres database

```
$ /usr/bin/pg_dump -f ./mfadb.sql -d mfadb
psc73-2:/var/lib/postgresql$ ls -al mfadb.sql
-rw-r--r--    1 postgres postgres    26984 Dec 15 17:04 mfadb.sql
```

Note: The database can be re-created from this backup only. Do *not* overwrite a database with existing records. If a database exists, drop it and then, create a new database.

4.8 PowerSC MFA out-of-band authentication

IBM PowerSC MFA out-of-band authentication allows a user to authenticate PowerSC MFA by using a web browser. You can configure the out-of-band authentication for one or more users.

You can configure the authentication methods that the user must specify, and the user is then provided with a user-specific, out-of-band web page for the configured authentication methods. If the out-of-band authentication is successful, the user then uses the resulting cache token credential to log in.

A cache token credential is created whenever a user successfully logs in by using the out-of-band authentication type. If the authentication policy specifies that the cache token credential can be reused by an application, it is usable until the first cache sweep after the cache token credential expires.

4.9 PowerVC security services

IBM PowerVC provides security services that support a secure environment and in particular, the following security features:

- ▶ Management of users, groups, and projects.
- ▶ Starting with IBM PowerVC Version 2.0.0, another authentication mechanism (TOTP) was added to provide enhanced security for the users that are logging in to IBM PowerVC. For a user to be authenticated, TOTP (along with a password) must be provided by the user.
- ▶ PowerVC uses the HSTS, X-XSS-Protection, and X-Content-Type-Options type HTTP security response headers.
- ▶ Signing packages adds an extra level of trustworthiness towards a product. IBM PowerVC ships RPM packages and Debian packages with its installer.

4.9.1 Managing users, groups, and projects

Building on the operating system security, PowerVC manages access security through the control of users, groups, and projects (for multi-tenanted environments).

User management planning

When you install IBM PowerVC, it is configured to use the security features of the operating system on the management host by default. This configuration sets the root operating system user account as the only initially available account with access to the IBM PowerVC server.

Upon installation of IBM PowerVC, a new operating system group that is named `powervc-filter` is created. The root user account is added to this group by default. IBM PowerVC has visibility only to the user and group accounts that are part of the `powervc-filter` group. The other operating system users and groups are not exposed to PowerVC unless they are added to the `powervc-filter` group.

As a preferred practice, create at least one system administrator user account to replace the root user account as the IBM PowerVC management administrator. After a new administrator ID is defined, remove the IBM PowerVC administrator rights from the root user ID.

Note: IBM PowerVC also requires user IDs that are defined in /etc/passwd that must not be modified, such as nova, neutron, keystone, and cinder. All of these users use OpenStack and they must not be changed or deleted. For security purposes, you cannot connect remotely to these user IDs. These users are configured with the login shell /sbin/nologin.

User account planning is important to define standard accounts and the process and requirements for managing these accounts. An IBM PowerVC management host can use user accounts that are managed by the Linux operating system security tools. They also can be configured to use the services that are provided by LDAP.

IBM PowerVC does not create users or groups in the underlying operating system. PowerVC backups include information about the configured user and group filters. If operating system users and groups are configured differently when the backup is restored, it can lead to administration issues.

Table 4-4 lists the available attributes to use when working with user and group filters.

Table 4-4 User and group filters

Attribute name	Description
User filter	Limits which users are visible to PowerVC. The default is "(memberOf=powervc-filter)".
Group filter	Limits which groups are visible to PowerVC. The default is "(name=powervc-filter)".

A newly installed PowerVC system displays the default values, as shown in Example 4-55.

Example 4-55 Default user and group filter settings

```
#powervc-config identity repository
Type: os
User filter: (memberOf=powervc-filter)
Group filter: (name=powervc-filter)
```

Projects and role management planning

This section describes the settings that are required for each user and group to operate and perform actions and work with projects.

Managing projects

A project, sometimes referred to as a *tenant*, is a unit of ownership. Virtual machines (VMs), volumes, images, and networks belong to a specific project. Only users with a role assignment for a specific project can work with the resources belonging to that project. At the time of installation, the ibm-default project is created, but IBM PowerVC also supports the creation of more projects for resource separation.

To work with projects, an administrator can log in to the ibm-default project and click **Projects** from the Configuration page.

You can also use the **openstack** project command to manage projects as needed. As a OpenStack administrator, you can run commands to create, delete, list, set, and show projects:

- ▶ Create a project:

```
openstack project create project-name
```

- ▶ Delete a project:

```
openstack project delete project-name
```

- ▶ List projects:

```
openstack project list
```

- ▶ Set project properties (name, or description):

```
openstack project set --name <name> project-name
```

```
openstack project set --description <description> project-name
```

- ▶ Display project details:

```
openstack project show project-name
```

After you create a project, you must grant at least one user a role on that project.

Project quotas

Project quotas set limits on the various types of resources within each project.

Administrators can edit, enable, and disable the quotas. Project quotas are set from the Project quotas tab of the user interface in the Dashboard menu.

Notes: Consider the following points:

- ▶ When a quota is disabled, that resource is unlimited.
- ▶ A quota can be set to be smaller than its current value (the quota is considered exceeded in this case). PowerVC does not change the effective resource usage, but subsequent requests for resources fail.

Table 4-5 lists the quotas that can be set per project.

Table 4-5 Available quotas

Quota	Description	Default
Colocation Rules	The total number of colocation rules that is allowed.	25
External IP addresses	The maximum number of external (floating) IP addresses that can be assigned in the project.	100
Injected files	The total number of injected files that is allowed for a project. The data is injected at the time of VM provisioning.	5
Injected File Content (Bytes)	The maximum size of each injected file that is allowed in the project.	10240
Injected File Path (Bytes)	The maximum length of each injected file path.	255
Memory (GB)	The total memory that can be used across all VMs in the project.	40000 GB
Per Volume (GB)	The maximum amount of storage that can be allocated to each volume in the project in GB.	Unlimited (disabled)
Processing Units	The total number of entitled processing units of all VMs within the project.	5500
Snapshots	The total number of volume snapshots that is allowed in the project.	100000
Virtual machines	The total number of VMS that is allowed in the project.	5500
Virtual Processors	The total number of virtual processors (cores) that is allowed across all VMs in the project.	55000
Volume Backup (GB)	The total amount of storage for volume backups that is allowed per project.	15000
Volume Backups	The number of volume backups that is allowed per project.	30
Volume Groups	The number of volume groups that is allowed per project.	200
Volume Storage (GB)	The total amount of disk space that can be used across all volumes within the project.	10000000
Volumes	The total number of volumes that can be part of the project.	100000

Managing roles

Roles are assigned to a user or group. They are inherited by all users in that group. A user or group can have more than one role, which allows them to perform any action that at least one of their roles allows.

Roles are used to specify what actions users can perform. Table 4-6 lists the available roles and the tasks that each role can perform.

Table 4-6 IBM PowerVC security roles

Role	Tasks
Administrator (admin)	Users with this role can perform all tasks and can access all resources.
Administrator assistant (admin_assist)	Users with this role can create and edit tasks, but cannot perform remove or delete operations. The admin_assist user can perform all VM, image, and volume lifecycle operations, except Delete.
Deployer (deployer)	Users with this role can perform the following tasks: <ul style="list-style-type: none">▶ Deploy a VM from an image.▶ View all resources, except users and groups.
Image manager (Image_manager)	Users with this role can perform the following tasks: <ul style="list-style-type: none">▶ Create, capture, import, or delete an image.▶ Edit an image description.▶ View all resources, except users and groups.
Storage manager (storage_manager)	Users with this role can perform the following tasks: <ul style="list-style-type: none">▶ Create, delete, or resize a volume.▶ View all resources, except users and groups.
Viewer (viewer)	Users with this role can view resources and the properties of resources, but can perform no tasks. They also cannot view users and groups.
Virtual Machine Manager (vm_manager)	Users with this role can perform the following tasks: <ul style="list-style-type: none">▶ Deploy a VM from an image.▶ Delete, resize, start, stop, or restart a VM.▶ Attach or detach a volume.▶ Snapshot and restore a volume.▶ Attach or detach a network interface.▶ Edit details of a deployed VM.▶ View all resources, except users and groups.▶ Create, attach, detach, or delete floating IP addresses.
Virtual machine user (vm_user)	Users with this role can perform the following tasks: <ul style="list-style-type: none">▶ Start, stop, or restart a VM.▶ View all resources, except users and groups.

Role assignments are specific to a project. Users can log in to only one project at a time in the IBM PowerVC user interface. If a user has a role on multiple projects, they can switch to one of those other projects without logging out and back in.

When users log in to a project, they see only resources, messages, and other information that belong to that project. They cannot see or manage resources that belong to a project in which they have no role assignment. One exception to this rule exists: The admin role can operate across projects in many cases. Be mindful of this exception when admin role assignments are made.

Important: OpenStack does *not* support moving resources from one project to another project. Volumes can be moved by unmanaging them and then, remanaging them in the new project. However, it is not possible to perform the same action for VMs because the network on which that VM depends is tied to the original project.

4.9.2 Ports that are used by IBM PowerVC

For more information about the ports that are used on the management server, by IBM PowerVC on the management server, and by PowerVM NovaLink managed hosts, see this [IBM Documentation web page](#).

4.9.3 Providing a certificate

The IBM PowerVC management server uses a self-signed X.509 certificate (by default) to secure its web interface and REST APIs. Because that self-signed certificates can be created by anyone, they are not trusted by client's web browsers automatically.

To improve security, a certificate that is signed by a certificate authority is used to replace the default self-signed certificate. Expiring or revoked certificates also must be replaced.

The web interface and REST APIs use the private key and certificate at the following locations:

- ▶ /etc/pki/tls/private/powervc.key
- ▶ /etc/pki/tls/certs/powervc.crt

For more information about replacing the PowerVC access certificate, see this [IBM Support web page](#).



A

Use case for security compliance on IBM Power Systems through Red Hat Ansible

This appendix describes how to use Red Hat Ansible for security and compliance verifications and remediations for IBM i, IBM AIX, and Red Hat on IBM Power Systems.

This appendix includes the following topics:

- ▶ “IBM Power Systems and the Red Hat Ansible Automation Platform” on page 170.
- ▶ “Security and compliance with Red Hat Ansible for IBM AIX and Red Hat on Power Systems” on page 171.
- ▶ “Security and compliance with Red Hat Ansible for IBM i” on page 179.

IBM Power Systems and the Red Hat Ansible Automation Platform

IT administrators, developers, and QA engineers are continuously seeking opportunities to streamline and automate anything that is repetitive to save time, increase reliability, and minimize human error. In a hybrid multicloud landscape, streamlining starts with establishing consistent tools and processes across all environments.

It is for this reason that Red Hat Ansible Automation Platform is enabled for IBM Power Systems across AIX and IBM i, and environments running on Power Systems private and public cloud infrastructures.

Red Hat Ansible Certified Content for IBM Power Systems helps you include workloads on the POWER platform as part of your wider enterprise automation strategy through the Red Hat Ansible Automation Platform system. Enterprises that use Red Hat Ansible for other IT infrastructure (such as x86 or IBM Z® servers) can seamlessly integrate Power Systems servers as well.

The Red Hat Ansible content helps enable DevOps automation through unified workflow orchestration with configuration management, provisioning, and application deployment in one, easy-to-use platform. This step is important in delivering a comprehensive enterprise-grade solution for building and operating IT automation at scale.

A core value of Red Hat Ansible is that it can integrate with what you have or build new playbooks with certified or open source content to create something new. IBM created an extensive set of Red Hat Ansible modules for the Power Systems user community that range from operating system management to cloud management and everything in between.

Solution benefits

The solution includes the following benefits:

- ▶ **Consistency**
 - Enable consistent enterprise automation strategy across:
 - AIX and IBM i environments
 - POWER Hypervisor
 - Hybrid applications and infrastructure management
- ▶ **Transparency:**
 - Enable complete visibility of Power Systems automation across AIX and IBM i environments.
 - Use best practices to manage automation in source control to move towards infrastructure as code.
 - Contribute to breaking down silos between IT teams.
- ▶ **Skills:**
 - Use Red Hat Ansible and Python skills, which are readily available and can be applied to AIX and IBM i environments.
 - Use modules to codify key maintenance and operational tasks for AIX and IBM i software so that you can focus on business priorities.

- ▶ Red Hat Ansible use cases:
 - Operating system configuration management AIX and IBM i
 - Patch management
 - Security management
 - OS and application deployment
 - Continuous delivery
 - Centralized backup and recovery
 - Virtualization management and provisioning

Security and compliance with Red Hat Ansible for IBM AIX and Red Hat on Power Systems

Red Hat Ansible is an IT automation engine that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and various other IT tasks.

Red Hat Ansible was built from the ground up for multi-tier deployments. Instead of controlling one system at a time, it models your IT architecture by defining how all of your systems interact.

It is straightforward to deploy because it does not require any agents or other security infrastructure. Instead, it uses a simple language (YAML, in the form of Red Hat Ansible Playbooks) to define your automation jobs.

Basic Red Hat Ansible concepts

Consider the following Red Hat Ansible concepts:

- ▶ Playbooks are used, which are ordered lists of tasks and variables that are performed against an inventory of hosts.
- ▶ Tasks are a single unit of action in Ansible, which calls a module.
- ▶ Modules are code that Ansible runs.
- ▶ Roles are repeatable bundles of tasks that are contained in a specific directory structure.
- ▶ Variables within Red Hat Ansible are called by using “ ”.
- ▶ Task delegation is used to delegate tasks to another host in the inventory, other than the host that the Red hat Ansible run is targeted against.

For our demonstration, we use the setup that is shown in Figure A-1.

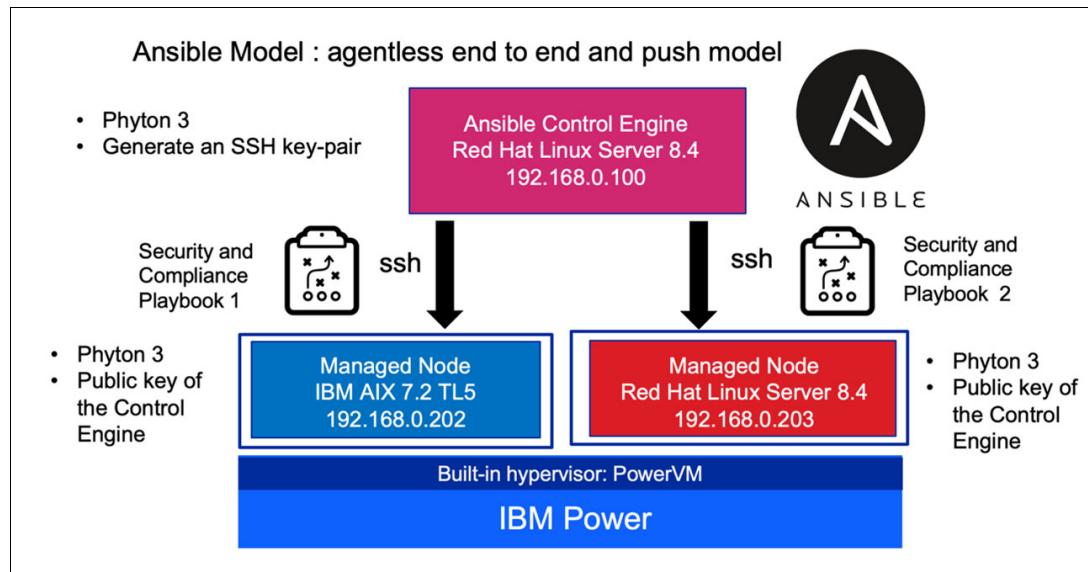


Figure A-1 Ansible setup for security and compliance playbooks

Red Hat Ansible connects to our two LPAR and sends small programs known as *Ansible modules* to them. These programs are resource models for the system's wanted state. Red Hat Ansible then runs these modules (by default over SSH) and removes them after they are done.

Installing Red Hat Ansible Engine and AIX collection

Complete the following steps to install and use AIX collection and run a playbook for Red Hat Enterprise Linux on Power Systems with Red Hat Ansible:

1. Connect as root to the Red Hat Ansible Engine and run the command that is shown in Example A-1.

Example A-1 Installing Red Hat Ansible

```
$ ssh root@192.168.0.100
$ yum install ansible
```

2. Add the repository, as shown in Example A-2.

Example A-2 Adding Red Hat Ansible repository

```
$ sudo subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-rpms
```

3. After Red Hat Ansible is installed, install the `ibm.power_aix` collection, as shown in Example A-3.

Example A-3 Installing the AIX collection

```
$ ansible-galaxy collection install ibm.power_aix
```

- When Red Hat Ansible is installed, a default inventory file (/etc/ansible/hosts) is created. Now, we include two hosts (IBM AIX LPAR and Red Hat Enterprise Linux on Power System LPAR), as shown in Example A-4.

Example A-4 Updating Red Hat Ansible hosts

```
$ vi /etc/ansible/hosts
aixlpar ansible_host=192.168.0.202 ansible_user=root
rhelpar ansible_host=192.168.0.203 ansible_user=root
```

- Run the **ssh-copy-id** command to distribute SSH public key to the AIX and Red Hat servers, as shown in Example A-5.

Example A-5 Distributing SSH public key

```
$ ssh-copy-id root@rhelpar
$ ssh-copy-id root@aixlpar
```

- Use the Red Hat Ansible ping module to check connection to the two hosts in the Red Hat Ansible inventory, as shown in Example A-6.

Example A-6 Ping Red Hat Ansible managed nodes

```
$ ansible -m ping all
PLAY [Ansible Ad-Hoc]
*****
TASK [ping] *****
ok: [aixlpar]
ok: [rhelpar]
PLAY RECAP *****
aixlpar: ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0
ignored=0
rhelpar: ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0
ignored=0
```

- Install Yum and Python on the AIX LPAR by using the commands that are shown in Example A-7.

Example A-7 Installing Yum and Python on AIX

```
$ ssh root@192.168.0.203
$ yum install python39
Download yum.sh
from https://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/ezinstall/ppc/

$ ssh root@192.168.0.202
$ ./yum.sh

Attempting download of rpm.rte & yum_bundle.tar ...
Installing rpm.rte at the latest version ...
This may take several minutes depending on the number of rpms installed...
+-----+
Pre-installation Verification...
+-----+
Verifying selections...done
Verifying requisites...done
Results...
WARNINGS
```

Problems described in this section are not likely to be the source of any immediate or serious failures, but further actions may be necessary or desired.

Already Installed

The number of selected filesets that are either already installed or effectively installed through superseding filesets is 1. See the summaries at the end of this installation for details.

NOTE: Base level filesets may be reinstalled using the "Force" option (-F flag), or they may be removed, using the deinstall or "Remove Software Products" facility (-u flag), and then reinstalled.

<< End of Warning Section >>

+-----+
BUILDDATE Verification ...
+-----+

Verifying build dates...done

FILESET STATISTICS

1 Selected to be installed, of which:

1 Already installed (directly or via superseding filesets)

0 Total to be installed

Pre-installation Failure/Warning Summary

Name	Level	Pre-installation Failure/Warning
rpm.rte	4.15.1.3	Already installed
Extracting yum_bundle.tar ...		
x ca-certificates-2016.10.7-2.aix6.1.ppc.rpm	214726 bytes, 420 media blocks.	
x curl-7.52.1-1.aix6.1.ppc.rpm	533288 bytes, 1042 media blocks.	
x db-4.8.24-3.aix6.1.ppc.rpm	2897799 bytes, 5660 media blocks.	
x gdbm-1.8.3-5.aix5.2.ppc.rpm	56991 bytes, 112 media blocks.	
x gettext-0.19.7-1.aix6.1.ppc.rpm	4036762 bytes, 7885 media blocks.	
x glib2-2.14.6-2.aix5.2.ppc.rpm	1686134 bytes, 3294 media blocks.	
x pysqlite-1.1.7-2.aix6.1.ppc.rpm	51749 bytes, 102 media blocks.	
x python-2.7.10-1.aix6.1.ppc.rpm	23333701 bytes, 45574 media blocks.	
x python-devel-2.7.10-1.aix6.1.ppc.rpm	15366474 bytes, 30013 media blocks.	
x python-iniparse-0.4-1.aix6.1.noarch.rpm	37912 bytes, 75 media blocks.	
x python-pycurl-7.19.3-1.aix6.1.ppc.rpm	162093 bytes, 317 media blocks.	
x python-tools-2.7.10-1.aix6.1.ppc.rpm	830446 bytes, 1622 media blocks.	
x python-urlgrabber-3.10.1-1.aix6.1.noarch.rpm	158584 bytes, 310 media blocks.	
x readline-6.1-2.aix6.1.ppc.rpm	489547 bytes, 957 media blocks.	
x sqlite-3.15.2-1.aix6.1.ppc.rpm	3570302 bytes, 6974 media blocks.	
x yum-3.4.3-8.aix6.1.noarch.rpm	1385622 bytes, 2707 media blocks.	
x yum-metadata-parser-1.1.4-2.aix6.1.ppc.rpm	62283 bytes, 122 media blocks.	

\$ yum search python3
\$ yum install python3.ppc

8. Install python39 on the Red Hat Enterprise Linux on Power Systems LPAR by using the commands that are shown in Example A-8.

Example A-8 Installing latest version of Python for Red Hat Enterprise Linux on Power

```
$ ssh root@192.168.0.203
$ yum install python39
```

Now, the Red Hat Ansible Engine is up and running, the AIX collection is installed, and the hosts are communicating correctly with the engine with all prerequisites met.

Running security and compliance playbook on Red Hat on IBM Power by using Red Hat Ansible and OpenSCAP

We use the command and fetch modules of Red Hat Ansible to run reports on remote hosts and pull all the reports back to a single machine.

The playbook includes, in sequence:

- ▶ Installs and updates OpenSCAP and the security guide.
- ▶ Runs a scan.
- ▶ Downloads the generated HTML report and stores it under the inventory hostname in a folder.

Complete the following steps:

1. Create a simple run-oscrap.yml file, as shown in Example A-9.

Example A-9 Creating run-oscrap.yml file

```
- hosts: all
  vars:
    oscap_profile: xccdf_org.ssgproject.content_profile_pci-dss
    oscap_policy: ssg-rhel-dss
    tasks:
      - name: install openscap scanner
        package:
          name: "{{ item }}"
          state: latest
        with_items:
          - openscap-scanner
          - scap-security-guide
            - block:
              - name: run openscap
                command: oscap xccdf eval \
                  --profile {{ oscap_profile }} \
                  --results-arf /tmp/oscrap-arf.xml \
                  --report /tmp/oscrap-report.html \
                  /usr/share/xml/scap/ssg/content/{{ oscap_policy }}.xml
            always:
              - name: download report
                fetch:
                  src: /tmp/oscrap-report.html
                  dest: ../oscrap-reports/{{ inventory_hostname }}.html
                  flat: yes
```

- Run the playbook by using the command that is shown in Example A-10 to generate the HTML report.

Example A-10 Running run-oscap.yml playbook

```
$ ansible-playbook run-oscap.yml
PLAY [all] ****
TASK [Gathering Facts] ****
ok: [rhelpar]
TASK [install openscap scanner]
*****
ok: [rhelpar] => (item=openscap-scanner)
ok: [rhelpar] => (item=scap-security-guide)
TASK [run openscap] *****
```

3. Review the report `rhelpar.html` report to confirm the compliance and scoring report, as shown in Figure A-2.

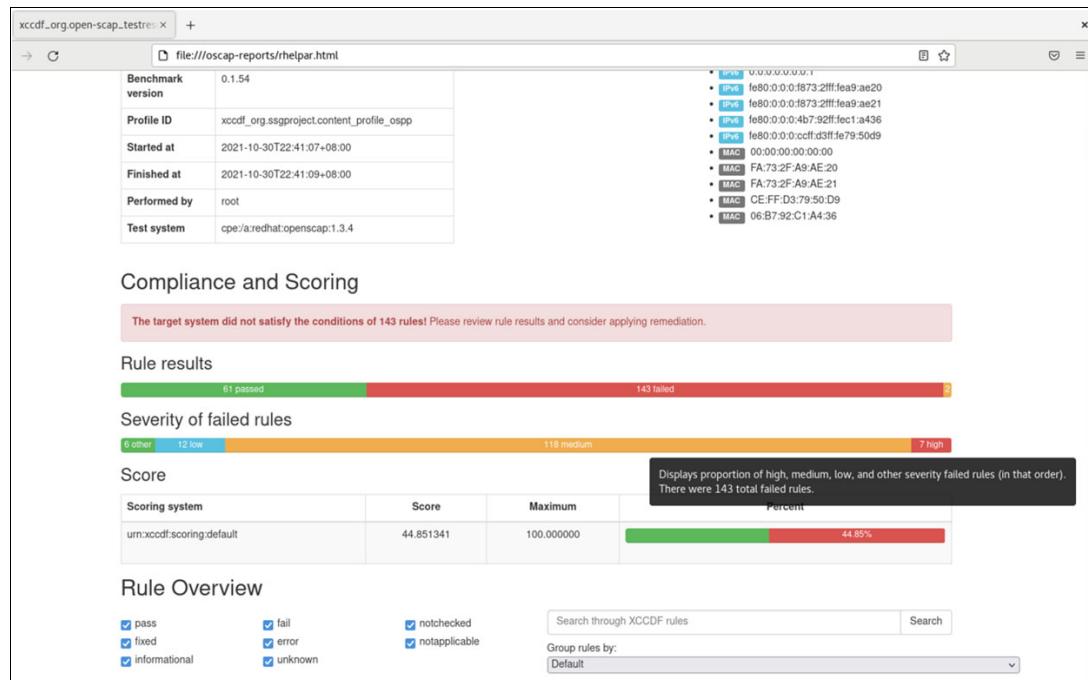


Figure A-2 Security and compliance playbook report using OpenSCAP and Ansible

Running security and compliance playbook on AIX using Red Hat Ansible and AIXpert

The command and fetch modules of Red Hat Ansible are used to run reports on the remote hosts and pull all the reports back to a single machine.

The playbook includes, in sequence:

- As a best practice, upgrades packages (excluding kernel related packages). We use `ansible-power-aix/playbooks/demo_yum.yml` (downloaded from <https://github.com/IBM/ansible-power-aix>), as shown in Figure A-3.

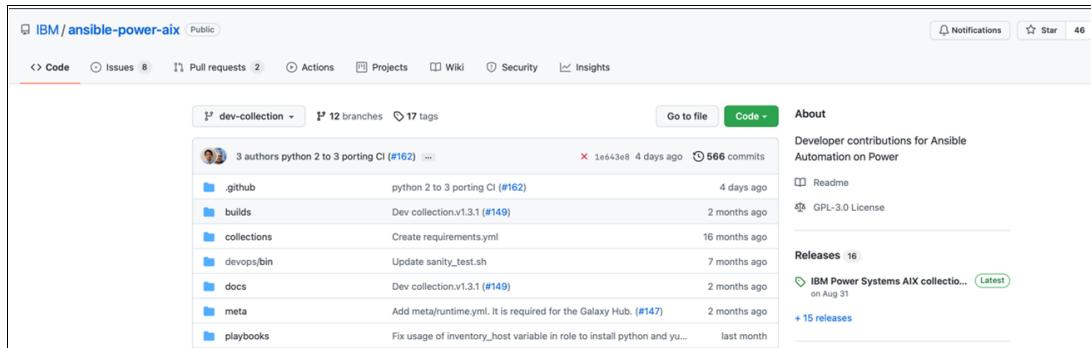


Figure A-3 AIX Playbooks from GitHub

- Applies Low level security of AIXpert.
- Checks the security settings after applying the low level security.
- Generates compliance reports (.txt and .csv).
- Downloads the generated CSV report and stores it under the inventory hostname in a folder.

Complete the following steps:

1. Create a simple `run-aixpert-low.yml` file, as shown in Example A-11.

Example A-11 Creating `run-aixpert-low.yml` file

```
- hosts: all
  vars:
    AIXpert_level: low
- name: "YuM Check-Update"
  hosts: all
  gather_facts: yes
  vars:
    name: '*'
    state: latest
    exclude: kernel*
  tasks:
    - name: Upgrade packages, excluding kernel related packages
      yum:
        name: "{{ name }}"
        state: "{{ state }}"
        exclude: "{{ exclude }}"
      register: output
    - debug: var=output - block:
```

```

- name: Apply Low level
  command: aixpert -l {{ AIXpert_level }}
- name: Check the security settings
  command: aixpert -cp
- name: Generate compliance reports
  command: aixpert -c -r
  always:
    - name: Download report
      fetch:
        src: /etc/security/aixpert/check_report.csv
        dest: ../oscap-reports/{{ inventory_hostname }}.csv
        flat: yes

```

2. Run the playbook by using the command that is shown in Example A-12 to generate the HTML report.

Example A-12 Running run-aixpert-low.yml playbook

```

$ ansible-playbook run-aixpert-low.yml
PLAY [all] ****
TASK [Gathering Facts] ****
ok: [aix1par]
TASK [Upgrade packages, excluding kernel related packages]
*****
[...]
ok: [aix1par]
TASK [Apply Low level] ****
do_action(): rule(l1s_tcbupdate): warning.
do_action(): Warning: Prereq failed for prereqtcb
do_action(): rule(l1s_ISSServerSensorFull): warning.
do_action(): Warning: Prereq failed for prereqRSSSFULL
do_action(): rule(l1s_ISSServerSensorLite): warning.
do_action(): Warning: Prereq failed for prereqRSSSLITE
Processedrules=50  Passedrules=47  PrereqFailedrules=3    Failedrules=0
Level=LLS Input file=/etc/security/aixpert/core/aixpertall.xml
ok: [aix1par]
TASK [Check the security settings]
*****
Processing l1s_maxage_DD881156 :done.
Processing l1s_maxexpired_DD881156 :done.
Processing l1s_minlen_DD881156 :done.
Processing l1s_minalpha_DD881156 :done.
Processing l1s_minother_DD881156 :done.
Processing l1s_mindiff_DD881156 :done.
Processing l1s_histexpire_DD881156 :done.
Processing l1s_histsize_DD881156 :done.
Processing l1s_pwdwarntime_DD881156 :done.
[...]
ok: [aix1par]
TASK [Generate compliance reports] ****
ok: [aix1par]
TASK [Download report] ****
[...]

```

- Review the rhelpar.csv report to confirm the compliance and scoring report, as shown in Figure A-4.

***** aixlpar.yxl.ma : Oct 30 22:57:35 *****				
***** aixlpar.yxl.ma : Oct 30 23:21:15 *****				
validate_check: Failed to execute /usr/bin/usrcck				
Processedrules=47 Passedrules=46 Failedrules=1 Level=LLS				
Input file=/etc/security/aixpert/core/appliedaixpert.xml				
Admin:root				
Report date and Time:Oct 30 23:26:22				
Report Version 1.0				
HostName	IP Address	Description	Command Arguments	Result
aixlpar.yxl.ma	192.168.0.202	"Maximum age for password: Specifies the maximum number of weeks (13 weeks) that a password is valid."	"/etc/security/aixpert/bin/chusr attr maxage=13 ALL lls_maxage"	PASS
aixlpar.yxl.ma	192.168.0.202	"Time to change password after the expiration: Specifies the maximum number of weeks to 8 weeks"	"/etc/security/aixpert/bin/chusr attr maxlen=8 ALL lls_maxlen"	PASS
aixlpar.yxl.ma	192.168.0.202	"Minimum length for password: Specifies the minimum length of a password to 8."	"/etc/security/aixpert/bin/chusr attr minlen=8 ALL lls_minlen"	PASS
aixlpar.yxl.ma	192.168.0.202	"Minimum number of alphabetic chars: Specifies the minimum number of alphabetic characters in a password to 2."	"/etc/security/aixpert/bin/chusr attr minalpha=2 ALL lls_minalpha"	PASS
aixlpar.yxl.ma	192.168.0.202	"Minimum number of non-alphabetic chars: Specifies the minimum number of non-alphabetic characters in a password to 2."	"/etc/security/aixpert/bin/chusr attr minother=2 ALL lls_minother"	PASS
aixlpar.yxl.ma	192.168.0.202	"Password reuse time: Specifies the number of previous passwords a user cannot reuse to 4."	"/etc/security/aixpert/bin/chusr attr histsize=4 ALL lls_histsize"	PASS
aixlpar.yxl.ma	192.168.0.202	"Check user definitions: Verifies the correctness of user definitions and fixes the errors."	"/etc/security/aixpert/bin/validate_check ""usrcck""	FAIL
aixlpar.yxl.ma	192.168.0.202	"Check password definitions: Verifies the correctness of password definitions and fixes the errors."	"/etc/security/aixpert/bin/validate_check ""pwdck""	PASS
aixlpar.yxl.ma	192.168.0.202	"Check group definitions: Verifies the correctness of group definitions and fixes the errors."	"/etc/security/aixpert/bin/validate_check ""grpck""	PASS
aixlpar.yxl.ma	192.168.0.202	"Delay between unsuccessful logins: Specifies the delay between unsuccessful logins to 5 seconds."	"/etc/security/aixpert/bin/chdef stanza /etc/security/login.cfg logindelay=5 default lls_logindelay"	PASS
aixlpar.yxl.ma	192.168.0.202	"Login timeout: Specifies the time interval (60 seconds) to type in a password."	"/etc/security/aixpert/bin/chdef stanza /etc/security/login.cfg logintimeout=60 usw lls_logintimeout"	PASS

Figure A-4 Security and compliance playbook report using AIXpert and Red Hat Ansible

Security and compliance with Red Hat Ansible for IBM i

This section shows how to configure security and compliance with Red Hat Ansible for IBM i.

Overview

IBM i is an operating system that includes thousands of core workloads that are running for different industries worldwide. Red Hat Ansible for IBM i can fit most of the on-premises tasks and cloud automation requirements for IBM i customers.

The following cases are examples of where IBM i customers or independent software vendors (ISVs) can use Red Hat Ansible:

- Automate traditional IBM i administration tasks, such as PTF management, system and application configuration, and application deployment and installation. These tasks are common and repeatedly run in a user environment.

Automating such tasks and processes can improve system management efficiency.

- ▶ Improve application development processes and efficiency to shorten the software delivery cycle. CI/CD delivery is mentioned more by IBM i customers, who need tools to bring Report Program Generator (RPG), written PGMs, and object-based applications into the CI/CD world.

- ▶ Manage multiple IBM i systems with interactive command-line interfaces (CLIs). A single place to manage all the Linux (or other platforms) and IBM i partitions together is important for Managed Services Providers (MSPs) and cloud users.

Many cases exist in which IT environments and solutions are built on many different systems; therefore, the central management of these systems is important.

Red Hat Ansible supports different platforms, and the workflow can be managed by playbooks that are written in YAML. By using playbooks, a complex IT environment can be managed from a single place.

- ▶ Automate IBM i tasks with reusable playbooks. Several cases exist in which playbooks can be reused for IBM i customers. For example, for the tasks dealing with open-source software in Portable Application Solution Environment (PASE), playbooks that are written for the AIX platform can be reused with few modifications in some situations.

In this appendix, the Red Hat Ansible for IBM i on Security Management use case is shown that checks suggestions from CIS IBM i Benchmark documentation. The following playbook checks the following aspects regarding the IBM i:

- ▶ System values
- ▶ Object authorities
- ▶ User profiles
- ▶ Networking settings

Running a playbook for Secure Compliance for IBM i

Important: This scenario shows two IBM i on-premises systems: one acts as an IBM i controller node, and the other IBM i VM acts as a manage node, each of them is running V7R4.

To run playbooks, the requirements on both sides must be met (for more information, see [Power IBM i collections for Ansible](#)). That playbook is the playbook that can be interpreted correctly by Python at the controller node and managed node with the YAML file. Python3 is highly recommend to be used.

The playbooks of Secure Compliance for IBM i are part of the Red Hat Ansible collections for IBM i that can be found at GitHub [Security Management use case](#).

After the installation of Red Hat Ansible open source tool at IBM i controller node, install the collection by running the `ansible-galaxy` command:

```
ansible-galaxy collection install ibm.power_ibmi
```

Complete the following steps to run the playbook:

1. On your IBM i controller node, set up the Red Hat Ansible configuration file, as shown in Example A-13.

Example A-13 Red Hat Ansible configuration file on IBM i

```
qsecofr@V529-CONTROLLER-T1:as45g01# vi ansible.cfg
[defaults]
inventory = /home/QSECOFR/as45g01/hosts_ibmi.ini
library=~/ansible/collections/ansible_collections/ibm/power_ibmi/plugins/modules
action_plugins=~/ansible/collections/ansible_collections/ibm/power_ibmi/plugins/action
interpreter_python=/QOpenSys/pkgs/bin/python3
roles_path = /home/qsecofr/as45groles
```

2. Configure the inventory file on the IBM i controller node, as shown in Example A-14.

Example A-14 Inventory file on IBM i

```
qsecofr@V529-CONTROLLER-T1:as45g01# cat hosts_ibmi.ini
[ibmi]
10.8.29.103 ansible_ssh_user=qsecofr ansible_ssh_pass=PASSWORD

[ibmi:vars]
ansible_python_interpreter="/QOpenSys/pkgs/bin/python3"
ansible_ssh_common_args=' -o StrictHostKeyChecking=no'
```

3. To run the playbook, use the **ansible-playbook** command (as shown in Example A-15) from the IBM i controller node. Then, press **Enter**.

Note: Consider the following points:

- ▶ In this playbook, prompts exist about checks for only the managed node or remediation or both. Other prompts about level of definitions also exist, such as: Level 1: Corporate/Enterprise Environment, and Level 2: High Security/Sensitive Data Environment.
- ▶ When the playbook is run, you might notice some fail messages during tasks. Consider these messages as false-positive results. The final result generates some JSON files that are reports to check the results on the IBM i managed node, which are generated in the /tmp directory.

Example A-15 Playbook's output of the Secure compliance for IBM i

```
qsecofr@V529-CONTROLLER-T1:security_management# ansible-playbook main.yml
PLAY [ibmi]
*****
TASK [Gathering Facts]
*****
ok: [10.8.29.103]

TASK [pause]
*****
[pause]
You're going to do system value compliance check on 10.8.29.103
```

```
Please input A,B or C for mode selection:  
Check only(A) / Remediate only(B) / Check and Remediate(C)  
:A  
ok: [10.8.29.103]  
  
TASK [set_fact]  
*****  
ok: [10.8.29.103]  
  
TASK [fail]  
*****  
skipping: [10.8.29.103]  
  
TASK [pause]  
*****  
[pause]  
Please read level definition and make selection:  
* Level 1: Corporate/Enterprise Environment (general use)  
  Items in this profile intend to:  
    - be practical and prudent  
    - provide a clear security benefit  
    - not negatively inhibit the utility of the technology beyond acceptable means  
* Level 2: High Security/Sensitive Data Environment (limited functionality)  
  Items in this profile may have the following characteristic(s):  
    - are intended for environments or use cases where security is paramount  
    - acts as defense in depth measure  
    - may negatively inhibit the utility or performance of the technology  
Type 1 or 2 and press Enter  
:2  
ok: [10.8.29.103]  
  
TASK [set_fact]  
*****  
ok: [10.8.29.103]  
  
TASK [fail]  
*****  
skipping: [10.8.29.103]  
  
TASK [set_fact]  
*****  
ok: [10.8.29.103]  
  
TASK [set_fact]  
*****  
ok: [10.8.29.103]  
  
TASK [set_fact]  
*****  
skipping: [10.8.29.103]  
  
TASK [set_fact]  
*****  
ok: [10.8.29.103]
```



```
ok: [10.8.29.103]
```

```
TASK [Checking system value QALWUSRDMN]
```

```
*****  
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "QTEMP", "msg": "Compliant check failed", "name": "QALWUSRDMN", "rc": -2, "type": "500A", "value": "*ALL"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}  
...ignoring
```

```
TASK [set_fact]
```

```
*****  
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QALWUSRDMN'})  
ok: [10.8.29.103] => (item={'key': 'expect', 'value': 'QTEMP'})  
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*ALL'})  
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})  
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})
```

```
TASK [set_fact]
```

```
*****  
skipping: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****  
ok: [10.8.29.103]
```

```
TASK [Checking system value QAUDCTL]
```

```
*****  
ok: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****  
skipping: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****  
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QAUDCTL'})  
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*OBJAUD *AUDLVL'})  
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*AUDLVL'})  
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal_as_list'})  
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': True})
```

```
TASK [set_fact]
```

```
*****  
ok: [10.8.29.103]
```

```
TASK [Checking system value QAUDENDACN]
```

```
*****  
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "*PWRDWNNSYS", "msg": "Compliant check failed", "name": "QAUDENDACN", "rc": -2, "type": "12A", "value": "*NOTIFY"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
```

...ignoring

TASK [set_fact]

```
*****  
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QAUDENDACN'})  
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*PWRDWNSYS'})  
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*NOTIFY'})  
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})  
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})
```

TASK [set_fact]

```
*****  
skipping: [10.8.29.103]
```

TASK [set_fact]

```
*****  
ok: [10.8.29.103]
```

TASK [Checking system value QAUDFRCLVL]

```
*****  
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "1", "msg": "Compliant check failed", "name": "QAUDFRCLVL", "rc": -2, "type": "10i0", "value": "0"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}  
...ignoring
```

TASK [set_fact]

```
*****  
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QAUDFRCLVL'})  
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '1'})  
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '0'})  
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})  
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})
```

TASK [set_fact]

```
*****  
skipping: [10.8.29.103]
```

TASK [set_fact]

```
*****  
ok: [10.8.29.103]
```

TASK [Checking system value QAUTOVRT]

```
*****  
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "0", "msg": "Compliant check failed", "name": "QAUTOVRT", "rc": -2, "type": "10i0", "value": "32767"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}  
...ignoring
```

```

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QAUTOVRT'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '0'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '32767'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QCRTAUT]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "*EXCLUDE", "msg": "Compliant check failed", "name": "QCRTAUT", "rc": -2, "type": "12A", "value": "*CHANGE"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QCRTAUT'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*EXCLUDE'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*CHANGE'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QCRTOBJAUD]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "*ALL", "msg": "Compliant check failed", "name": "QCRTOBJAUD", "rc": -2, "type": "12A", "value": "*NONE"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QCRTOBJAUD'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*ALL'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*NONE'})

```

```

ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QDSCJOBITV]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "15", "msg": "Compliant check failed", "name": "QDSCJOBITV", "rc": -2, "type": "12A", "value": "0000000240"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QDSCJOBITV'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '15'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '0000000240'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QFRCCVNRST]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "7", "msg": "Compliant check failed", "name": "QFRCCVNRST", "rc": -2, "type": "4A", "value": "1"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QFRCCVNRST'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '7'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '1'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****

```

```

skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QINACTITV]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "0000000015", "msg": "Compliant check failed", "name": "QINACTITV", "rc": -2, "type": "12A", "value": "*NONE"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QINACTITV'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '0000000015'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*NONE'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QINACTMSGQ]
*****
ok: [10.8.29.103]

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QINACTMSGQ'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*ENDJOB'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*ENDJOB'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': True})

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QLMTDEVSSN]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "1", "msg": "Compliant check failed", "name": "QLMTDEVSSN", "rc": -2}]}

```

```

-2, "type": "4A", "value": "0"}], "message": "", "msg": "non-zero return code when get system
value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines":
["non-zero return code when get system value:-2"], "sysval": []
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QLMTDEVSSN'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '1'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '0'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QMAXSGNACN]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal",
"compliant": false, "expect": "3", "msg": "Compliant check failed", "name": "QMAXSGNACN", "rc": -2,
"type": "4A", "value": "1"}], "message": "", "msg": "non-zero return code when get system
value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines":
["non-zero return code when get system value:-2"], "sysval": []
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QMAXSGNACN'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '3'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '1'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QMAXSIGN]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal",
"compliant": false, "expect": "000003", "msg": "Compliant check failed", "name": "QMAXSIGN",
"rc": -2, "type": "8A", "value": "*NOMAX"}], "message": "", "msg": "non-zero return code when
get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2",
"stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []
...ignoring

```

```

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QMAXSIGN'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '000003'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*NOMAX'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QPWDCHGBLK]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "99", "msg": "Compliant check failed", "name": "QPWDCHGBLK", "rc": -2, "type": "12A", "value": "*NONE"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QPWDCHGBLK'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '99'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*NONE'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QPWDLVL]
*****
ok: [10.8.29.103]

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QPWDLVL'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '3'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '3'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})

```

```

ok: [10.8.29.103] => (item={'key': 'compliant', 'value': True})

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QPWDRQDDIF]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "1", "msg": "Compliant check failed", "name": "QPWDRQDDIF", "rc": -2, "type": "4A", "value": "0"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QPWDRQDDIF'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '1'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '0'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QPWDRULES]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal_as_list", "compliant": false, "expect": "*ALLCRTCHG *DGTLMTAJC *DGTLMTFST *DGTLMTLST *DGTMIN1 *LMTPRFNAME *MAXLEN128 *MINLEN14 *REQANY3 *SPCCHRLMTAJC *SPCCHRLMTFST *SPCCHRLMTLST", "msg": "Compliant check failed", "name": "QPWDRULES", "rc": -2, "type": "752A", "value": "*PWDSYSVAL"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QPWDRULES'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*ALLCRTCHG *DGTLMTAJC *DGTLMTFST *DGTLMTLST *DGTMIN1 *LMTPRFNAME *MAXLEN128 *MINLEN14 *REQANY3 *SPCCHRLMTAJC *SPCCHRLMTFST *SPCCHRLMTLST'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*PWDSYSVAL'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal_as_list'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

```

```

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QPWDVLDPGM]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "*REGFAC", "msg": "Compliant check failed", "name": "QPWDVLDPGM", "rc": -2, "type": "20A", "value": "*NONE"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QPWDVLDPGM'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*REGFAC'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*NONE'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QRMTSIGN]
*****
ok: [10.8.29.103]

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QRMTSIGN'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '*FRCSIGNON'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '*FRCSIGNON'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': True})

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QRETSVRSEC]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "0", "msg": "Compliant check failed", "name": "QRETSVRSEC", "rc": -2, "type": "4A", "value": "1"}], "message": "", "msg": "non-zero return code when get system

```

```

value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QRETSVRSEC'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '0'})

ok: [10.8.29.103] => (item={'key': 'actual', 'value': '1'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Checking system value QVFYOBJRST]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "fail_list": [{"check": "equal", "compliant": false, "expect": "5", "msg": "Compliant check failed", "name": "QVFYOBJRST", "rc": -2, "type": "4A", "value": "3"}], "message": "", "msg": "non-zero return code when get system value:-2", "rc": -2, "stderr": "non-zero return code when get system value:-2", "stderr_lines": ["non-zero return code when get system value:-2"], "sysval": []}
...ignoring

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'name', 'value': 'QVFYOBJRST'})
ok: [10.8.29.103] => (item={'key': 'expect', 'value': '5'})
ok: [10.8.29.103] => (item={'key': 'actual', 'value': '3'})
ok: [10.8.29.103] => (item={'key': 'check', 'value': 'equal'})
ok: [10.8.29.103] => (item={'key': 'compliant', 'value': False})

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Generate report to file]
*****
changed: [10.8.29.103]

TASK [Check completes]
*****
ok: [10.8.29.103] => {
    "msg": "Security check report generated successfully, please review at /tmp/security_management_sysval_report-level2-10.8.29.103-20211020T171243.json"
}

```

```
}

PLAY [ibmi]
*****
TASK [Gathering Facts]
*****
ok: [10.8.29.103]

TASK [pause]
*****
[pause]
You're going to do user profile security compliance check on 10.8.29.103
Please input A,B or C for mode selection:
Check only(A) / Remediate only(B) / Check and Remediate(C)
: A
ok: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [fail]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [3.1 PUBLIC authority to all user profiles should be EXCLUDE with the following exception
QDBSHR QDBSHRDO QTMLPD]
*****
ok: [10.8.29.103]

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.1'})
ok: [10.8.29.103] => (item={'key': 'desc', 'value': '3.1 PUBLIC authority to all user profiles
should be EXCLUDE with the following exceptions QDBSHR QDBSHRDO QTMLPD'})
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

```
TASK [3.2 All Private authorities to all user profiles other than the owner's and the profile itself should be removed.]
```

```
*****
```

```
ok: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****
```

```
skipping: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****
```

```
skipping: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****
```

```
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.2'})
```

```
ok: [10.8.29.103] => (item={'key': 'desc', 'value': "3.2 All Private authorities to all user profiles other than the owner's and the profile itself should be removed."})
```

```
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

```
TASK [3.3 All IBM Supplied Profiles shall be owned by QSYS with the following exceptions QFAXMSF shall be owned by QAUTPROF QRDARS400xx shall be owned by QRDARS400 QTIVOLI, QTIVROOT and QTIVUSER shall be owned by QTIVOLI Non-IBM (user created) profiles shall be owned by QSECOFR or QSYS] ***
```

```
ok: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****
```

```
ok: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****
```

```
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.3'})
```

```
ok: [10.8.29.103] => (item={'key': 'desc', 'value': '3.3 All IBM Supplied Profiles shall be owned by QSYS with the following exceptions QFAXMSF shall be owned by QAUTPROF QRDARS400xx shall be owned by QRDARS400 QTIVOLI, QTIVROOT and QTIVUSER shall be owned by QTIVOLI Non-IBM (user created) profiles shall be owned by QSECOFR or QSYS.'})
```

```
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})
```

```
ok: [10.8.29.103] => (item={'key': 'vulnerables', 'value': 'QFAXMSF, QICC'})
```

```
ok: [10.8.29.103] => (item={'key': 'remediation', 'value': 'CHGOBJOWN OBJ(SYS_ONAME_REPLACE) OBJTYPE(*USRPRF) NEWOWN(QSECOFR) CUROWNAUT(*REVOKE) '})
```

```
TASK [set_fact]
```

```
*****
```

```
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '3.3'})
```

```
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': '3.3 All IBM Supplied Profiles shall be owned by QSYS with the following exceptions QFAXMSF shall be owned by QAUTPROF QRDARS400xx shall be owned by QRDARS400 QTIVOLI, QTIVROOT and QTIVUSER shall be owned by QTIVOLI Non-IBM (user created) profiles shall be owned by QSECOFR or QSYS.'})
```

```
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

```
TASK [3.6 Default passwords provide an opportunity for someone to enter your system, if someone knows your policy for assigning profile names and knows that a new person is joining your organization. Additionally, accounts with default passwords are often used for shared (non-unique) accounts. Tell the new user the password confidentially, such as in a "Welcome to
```

```
the System" letter that outlines your security policies. Require the user to change the password  
the first time that the user signs on by setting the user profile to PWDEXP(*YES)] ***  
ok: [10.8.29.103]
```

```
TASK [set_fact]  
*****
```

```
ok: [10.8.29.103]
```

```
TASK [set_fact]  
*****
```

```
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.6'})  
ok: [10.8.29.103] => (item={'key': 'desc', 'value': "3.6 Default passwords provide an  
opportunity for someone to enter your system, if someone knows your policy for assigning profile  
names and knows that a new person is joining your organization. Additionally, accounts with  
default passwords are often used for shared (non-unique) accounts. Tell the new user the  
password confidentially, such as in a 'Welcome to the System' letter that outlines your security  
policies. Require the user to change the password the first time that the user signs on by  
setting the user profile to PWDEXP(*YES)."})  
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})  
ok: [10.8.29.103] => (item={'key': 'vulnerables', 'value': 'AS45G01, MARCE'})  
ok: [10.8.29.103] => (item={'key': 'remediation', 'value': 'CHGUSRPRF USRPRF(USER_NAME_REPLACE)  
PWDEXP(*YES)'})
```

```
TASK [set_fact]  
*****
```

```
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '3.6'})  
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': "3.6 Default passwords provide an  
opportunity for someone to enter your system, if someone knows your policy for assigning profile  
names and knows that a new person is joining your organization. Additionally, accounts with  
default passwords are often used for shared (non-unique) accounts. Tell the new user the  
password confidentially, such as in a 'Welcome to the System' letter that outlines your security  
policies. Require the user to change the password the first time that the user signs on by  
setting the user profile to PWDEXP(*YES)."})  
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

```
TASK [3.7 Disable inactive user profiles within 90 days.]  
*****
```

```
ok: [10.8.29.103]
```

```
TASK [set_fact]  
*****
```

```
ok: [10.8.29.103]
```

```
TASK [set_fact]  
*****
```

```
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.7'})  
ok: [10.8.29.103] => (item={'key': 'desc', 'value': '3.7 Disable inactive user profiles within  
90 days.'})  
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})  
ok: [10.8.29.103] => (item={'key': 'vulnerables', 'value': 'QTFTP, QSRV, QLPISTALL, QDFTOWN,  
QDSNX, QSRVBAS, QAUTPROF, QNETSPLF, QSVCCS, QCLUSTER, QSPL, QDLFM, QTMHHTP1, QCOLSRV, QMGTC,  
CLPADMIN, QLPAUTO, QSOC, QSNADS, QANZAGENT, QTSTRQS, QYCMCIMOM, QGATE, QEJB, QDOC, QPEX,  
QFAXMSF, QEJBSVR, QNFSANON, QTMLPLD, QIBMHELP, QFNC, QIPP, QWSERVICE, QDBSHR, QNTP, QOBJC, QICC,  
QDBSHRDO, QRJE'})
```

```
ok: [10.8.29.103] => (item={'key': 'remediation', 'value': 'CHGUSRPRF USRPRF(USER_NAME_REPLACE)  
STATUS(*DISABLED)'})
```

```
TASK [set_fact]
```

```
*****  
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '3.7'})  
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': '3.7 Disable inactive user profiles  
within 90 days.'})  
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

TASK [3.8 User Profiles with non-expiring passwords are never required to change their Service accounts may be excluded from the audit and remediation. A service account is a user account that is created explicitly to provide a security context for automated system and application services running on the system. Service accounts should be configured with a non-trivial, complex password that is used in an automated service process and never used interactively. Service accounts should be documented and their Password expiration interval should be set to *NOMAX. A process should then be documented and executed to periodically change their passwords manually] ***

```
ok: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****  
ok: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****  
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.8'})  
ok: [10.8.29.103] => (item={'key': 'desc', 'value': '3.8 User Profiles with non-expiring  
passwords are never required to change their Service accounts may be excluded from the audit and  
remediation. A service account is a user account that is created explicitly to provide a  
security context for automated system and application services running on the system. Service  
accounts should be configured with a non-trivial, complex password that is used in an automated  
service process and never used interactively. Service accounts should be documented and their  
Password expiration interval should be set to *NOMAX. A process should then be documented and  
executed to periodically change their passwords manually.'})  
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})  
ok: [10.8.29.103] => (item={'key': 'vulnerables', 'value': 'QBRMS, QTMPPLD'})  
ok: [10.8.29.103] => (item={'key': 'remediation', 'value': 'CHGUSRPRF USRPRF(USER_NAME_REPLACE)  
PWDEXPITV(*SYSVAL)'})
```

```
TASK [set_fact]
```

```
*****  
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '3.8'})  
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': '3.8 User Profiles with non-expiring  
passwords are never required to change their Service accounts may be excluded from the audit and  
remediation. A service account is a user account that is created explicitly to provide a  
security context for automated system and application services running on the system. Service  
accounts should be configured with a non-trivial, complex password that is used in an automated  
service process and never used interactively. Service accounts should be documented and their  
Password expiration interval should be set to *NOMAX. A process should then be documented and  
executed to periodically change their passwords manually.'})  
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

TASK [3.9 User Profiles with command line access can run commands they are authorized to from a command line.]

```
*****
```

ok: [10.8.29.103]

TASK [set_fact]

```
*****
```

ok: [10.8.29.103]

TASK [set_fact]

```
*****
```

ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.9'})

ok: [10.8.29.103] => (item={'key': 'desc', 'value': '3.9 User Profiles with command line access can run commands they are authorized to from a command line.'})

ok: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})

ok: [10.8.29.103] => (item={'key': 'vulnerables', 'value': 'QTFTP, QSRV, QLPISTALL, QSSHD, QSRVAGT, AS45G01, QDFTOWN, QDSNX, QSVMSS, QIJS, QSRVBAS, QSYSOPR, QAUTPROF, QNETSPLF, QTCTM, QHAUSRPRF, QSVCCS, QCLUSTER, QBRMS, QSPL, QDLFM, QTMHHTP1, QCOLSRV, QSVSM, MARCE, QMGTC, CLPADMIN, QRJE, QPM400, QLPAUTO, QUSER, QSOC, QMSF, QSNADS, QANZAGENT, QTSTRQS, QWEBADMIN, QYCMCIMOM, QGATE, QSECOFR, QEJB, QDOC, QPEX, QFAXMSF, QPGMR, QEJBSVR, QCIUSER, QNFSANON, QTMLPLD, QIBMHELP, QLWISVR, QFNC, QSYS, QIPP, QWSERVICE, QTCP, QDBSHR, QNTP, QOBJC, QSPLJOB, QICC, QTMHHTTP, QDBSHRD0, QCLUMGT, QYPSJSVR'})

ok: [10.8.29.103] => (item={'key': 'remediation', 'value': 'CHGUSRPRF USRPRF(USER_NAME_REPLACE) LMTCPB(*YES)'})

TASK [set_fact]

```
*****
```

skipping: [10.8.29.103] => (item={'key': 'id', 'value': '3.9'})

skipping: [10.8.29.103] => (item={'key': 'desc', 'value': '3.9 User Profiles with command line access can run commands they are authorized to from a command line.'})

skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})

TASK [3.10A This section contains information about the IBM-Supplied user profiles that are shipped with the system and Licensed Program Products. These profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.] ***

ok: [10.8.29.103]

TASK [set_fact]

```
*****
```

ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.10A'})

ok: [10.8.29.103] => (item={'key': 'desc', 'value': '3.10A Check some parameters if they match the default values that are used for all IBM-supplied user profiles.'})

ok: [10.8.29.103] => (item={'key': 'sql', 'value': "SELECT AUTHORIZATION_NAME, NO_PASSWORD_INDICATOR, STATUS, USER_CLASS_NAME, INITIAL_PROGRAM_NAME, LIMIT_CAPABILITIES, SPECIAL_AUTHORITIES FROM QSYS2/USER_INFO WHERE AUTHORIZATION_NAME LIKE 'Q%' AND NO_PASSWORD_INDICATOR = 'NO' OR AUTHORIZATION_NAME LIKE 'Q%' AND STATUS = '*DISABLED' OR AUTHORIZATION_NAME LIKE 'Q%' AND USER_CLASS_NAME <> '*USER' OR AUTHORIZATION_NAME LIKE 'Q%' AND INITIAL_PROGRAM_NAME <> '*NONE' OR AUTHORIZATION_NAME LIKE 'Q%' AND LIMIT_CAPABILITIES <> '*NO' OR AUTHORIZATION_NAME LIKE 'Q%' AND SPECIAL_AUTHORITIES <> '*NONE'"}))

ok: [10.8.29.103] => (item={'key': 'remediation', 'value': 'Review the results. This indicates that one or more of the following parameters of the profiles in the list does not match the default values that are used for all IBM-supplied user profiles. x NO_PASSWORD_INDICATOR (PASSWORD) = YES (Default) x STATUS (STATUS) = *ENABLED (Default) x USER_CLASS_NAME (USRCLS) = *USER (Default) x INITIAL_PROGRAM_NAME (INLPGM) = *NONE (Default) x LIMIT_CAPABILITIES (LMTCPB) = *NO (Default)'})

```
= *NO (Default) x SPECIAL_AUTHORITIES (SPCAUT) = *NONE (Default) x Compare the results of the screen output to information about IBM-supplied profiles, their purpose, and values for any IBM-supplied profiles that are different from the defaults from the shipped defaults from the following link.
```

```
https://www.ibm.com/support/knowledgecenter/en/ssw\_ibm\_i\_74/rzarl/rzarlibmprfa.htm'}
```

```
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})
```

```
TASK [set_fact]
```

```
*****
```

```
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '3.10A'})
```

```
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': '3.10A Check some parameters if they match the default values that are used for all IBM-supplied user profiles.'})
```

```
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

```
TASK [3.10B To check if IBM Supplied Profiles are being used as Group Profiles.]
```

```
*****
```

```
ok: [10.8.29.103]
```

```
TASK [set_fact]
```

```
*****
```

```
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '3.10B'})
```

```
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': '3.10B To check if IBM Supplied Profiles are being used as Group Profiles.'})
```

```
skipping: [10.8.29.103] => (item={'key': 'sql', 'value': "SELECT T01.GROUPNAME, T01.USERNAME FROM QSYS2.GROUPLIST T01 INNER JOIN QSYS2.USER_INFO T02 ON T01.GROUPNAME = T02.USER_NAME WHERE T02.USER_NAME LIKE '%Q%' AND T02.USER_NAME NOT IN ('QBRMS', 'QMQMADM', 'QONDADM', 'QRDARS400', 'QRDARSADM', 'QWQADMIN')"})
```

```
skipping: [10.8.29.103] => (item={'key': 'remediation', 'value': 'Review the results of the screen output. The following are valid exclusions from the audit. x QBRMS x QMQMADM x QONDADM x QRDARS400 x QRDARSADM x QWQADMIN\nRemediation: x Change any IBM-Supplied user profile found in the audit that are different from the defaults or values different from the list in the referenced table'}}
```

```
https://www.ibm.com/support/knowledgecenter/en/ssw\_ibm\_i\_74/rzarl/rzarlibmspp1.htm CHGUSRPRF USRPRF\(<xxxxxx>\) <parameter>\(<xxxxxx>\) x Change any User Profile that is a group member of an IBM-Supplied user profile found in the audit to remove the IBM-Supplied user profile from its Group (GRPPRF) and/or Supplemental Group (SUPGRPPRF) parameters. CHGUSRPRF USRPRF(<xxxxxx>) GRPPRF(<xxxxxx>) SUPGRPPRF(<xxxxxx>) Impact: Functions using the authorities and parameters of any profile you change may fail. You may want to contact IBM or your business partner for guidance prior to making any changes.\nReferences: 1.
```

```
https://www.ibm.com/support/knowledgecenter/en/ssw\_ibm\_i\_74/rzarl/rzarlibmprfa.htm\n2.
```

```
https://www.ibm.com/support/knowledgecenter/en/ssw\_ibm\_i\_74/rzarl/rzarldftusrprf.htm\n3.
```

```
https://www.ibm.com/support/knowledgecenter/en/ssw\_ibm\_i\_74/rzarl/rzarlibmspp1.htm'
```

```
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})
```

```
TASK [set_fact]
```

```
*****
```

```
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.10B'})
```

```
ok: [10.8.29.103] => (item={'key': 'desc', 'value': '3.10B To check if IBM Supplied Profiles are being used as Group Profiles.'})
```

```
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})
```

```
TASK [3.11 Group profiles should not have a password as they are usually not associated with a unique account.]
```

```
*****
```

```
ok: [10.8.29.103]
```

```

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
skipping: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'id', 'value': '3.11'})
ok: [10.8.29.103] => (item={'key': 'desc', 'value': 'Group profiles should not have a password as they are usually not associated with a unique account.'})
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})

TASK [5.1 QSECOFR Profile Shall Be DISABLED]
*****
ok: [10.8.29.103]

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'id', 'value': '5.1'})
ok: [10.8.29.103] => (item={'key': 'desc', 'value': 'QSECOFR Profile Shall Be DISABLED.'})
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})
ok: [10.8.29.103] => (item={'key': 'vulnerables', 'value': 'QSECOFR'})
ok: [10.8.29.103] => (item={'key': 'remediation', 'value': 'CHGUSRPRF USRPRF(QSECOFR) STATUS(*DISABLED)'})

TASK [set_fact]
*****
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '5.1'})
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': 'QSECOFR Profile Shall Be DISABLED.'})
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})

TASK [5.2 QSECOFR Shall Not be Configured as a Group Profile]
*****
fatal: [10.8.29.103]: FAILED! => {"changed": false, "cmd": "DSPUSRPRF USRPRF(QSECOFR) TYPE(*GRPMBR)", "delta": "0:00:00.264472", "end": "2021-10-20 17:16:27.767073", "job_log": [], "job_name": "", "joblog": true, "msg": "non-zero return code:255", "rc": 255, "start": "2021-10-20 17:16:27.502601", "stderr": "CPF2257: User profile QSECOFR not a group profile.\n", "stderr_lines": ["CPF2257: User profile QSECOFR not a group profile."], "stdout": "", "stdout_lines": []}
...ignoring

TASK [set_fact]
*****
skipping: [10.8.29.103] => (item={'key': 'id', 'value': '5.2'})
skipping: [10.8.29.103] => (item={'key': 'desc', 'value': 'QSECOFR Shall Not be Configured as a Group Profile.'})
skipping: [10.8.29.103] => (item={'key': 'result', 'value': 'FAIL'})
skipping: [10.8.29.103] => (item={'key': 'vulnerables', 'value': 'QSECOFR'})
skipping: [10.8.29.103] => (item={'key': 'remediation', 'value': 'CHGUSRPRF USRPRF(QSECOFR) GRPPRF(*NONE)'})

```

```

TASK [set_fact]
*****
ok: [10.8.29.103] => (item={'key': 'id', 'value': '5.2'})
ok: [10.8.29.103] => (item={'key': 'desc', 'value': 'QSECOFR Shall Not be Configured as a Group Profile.'})
ok: [10.8.29.103] => (item={'key': 'result', 'value': 'PASS'})

TASK [set_fact]
*****
ok: [10.8.29.103]

TASK [Generate report to file]
*****
changed: [10.8.29.103]

TASK [Check completes]
*****
ok: [10.8.29.103] => {
    "msg": "Security check report generated successfully, please review at /tmp/security_management_userprofile_check_result-10.8.29.103-20211020T171519.json"
}

PLAY [ibmi]
*****

TASK [Display the authority of QGPL]
*****
ok: [10.8.29.103]

PLAY [ibmi]
*****

TASK [4.2.1 Check network attribute JOBACN of network attribute]
*****
ok: [10.8.29.103]

TASK [Get network attribute JOBACN of network attribute]
*****
ok: [10.8.29.103] => {
    "msg": "*FILE"
}

TASK [Specifies the action taken for input streams received through the SNA network by the system. The JOBACN value should be set to *REJECT to secure your system from job streams received through the network.] ***
fatal: [10.8.29.103]: FAILED! => {
    "assertion": "JOBACN.output['JOBACN'] == '*REJECT'",
    "changed": false,
    "evaluated_to": false,
    "msg": "Assertion failed"
}
...ignoring

```

```
TASK [4.4.1 Configuring SSH ? server protocol 2  
/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file and allow the SSH2 protocol only. This  
is the SSH server configuration file.] *****  
ok: [10.8.29.103]
```

```
TASK [/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file and allow the SSH2 protocol only.  
This is the SSH server configuration file.]  
*****  
ok: [10.8.29.103] => {  
    "changed": false,  
    "msg": "All assertions passed"  
}
```

```
TASK [4.4.2 Configuring SSH ? banner configuration The recommendation is to edit the  
/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file and configure a path to a login herald  
message] ****  
ok: [10.8.29.103]
```

```
TASK [The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file  
and configure a path to a login herald message]  
*****  
fatal: [10.8.29.103]: FAILED! => {  
    "assertion": "'/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' in  
(ssh_server_banner.files | map(attribute='path') | join(', '))",  
    "changed": false,  
    "evaluated_to": false,  
    "msg": "Assertion failed"  
}  
...ignoring
```

```
TASK [4.4.3 Configuring SSH ? disallow host based authentication The recommendation is to edit  
the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file to ensure that host-based  
authentication is disallowed.] ***  
ok: [10.8.29.103]
```

```
TASK [The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file  
to ensure that host-based authentication is disallowed.]  
*****  
fatal: [10.8.29.103]: FAILED! => {  
    "assertion": "'/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' in  
(disallow_host_based_auth.files | map(attribute='path') | join(', '))",  
    "changed": false,  
    "evaluated_to": false,  
    "msg": "Assertion failed"  
}  
...ignoring
```

```
TASK [4.4.4 Configuring SSH ? set privilege separation The recommendation is to edit the  
/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file to ensure that privilege separation is  
enabled. Note, that as of OpenSSH 7.5 this configuration directive has been deprecated.] ***  
ok: [10.8.29.103]
```

```
TASK [Setting privilege separation helps to secure remote ssh access. Once a user is  
authenticated the sshd daemon creates a child process which has the privileges of the  
authenticated user and this then handles incoming network traffic. The aim of this is to prevent
```

```

privilege escalation through the initial root process. The recommendation is to edit the
/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file to ensure that privilege separation is
enabled. Note, that as of OpenSSH 7.5 this configuration directive has been deprecated.] ***
fatal: [10.8.29.103]: FAILED! => {
    "assertion": "'/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' in
(privilege_separation.files | map(attribute='path') | join(', '))",
    "changed": false,
    "evaluated_to": false,
    "msg": "Assertion failed"
}
...ignoring

```

TASK [4.4.5 Configuring SSH ? set MaxAuthTries to 4 or Less The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.] ***
ok: [10.8.29.103]

```

TASK [The MaxAuthTries parameter specifies the maximum number of authentication attempts
permitted per connection. When the login failure count reaches half the number, error messages
will be written to the syslog file detailing the login failure.] ***
fatal: [10.8.29.103]: FAILED! => {
    "assertion": "'/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' in
(max_auth_retries.files | map(attribute='path') | join(', '))",
    "changed": false,
    "evaluated_to": false,
    "msg": "Assertion failed"
}
...ignoring

```

TASK [4.4.6 Configuring SSH ? set Idle Timeout Interval for User Login Profile Applicability The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time.] ***
ok: [10.8.29.103]

```

TASK [The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh
sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for
the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd
will send client alive messages at every ClientAliveInterval interval. When the number of
consecutive client alive messages are sent with no response from the client, the ssh session is
terminated. For example, if the ClientAliveInterval is set to 15 seconds and the
ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of
idle time. Verify ClientAliveCountMax is 0.] ***
fatal: [10.8.29.103]: FAILED! => {
    "assertion": "'/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' in (idle_timeout.files |
map(attribute='path') | join(', '))",
    "changed": false,
    "evaluated_to": false,
    "msg": "Assertion failed"
}

```

```
...ignoring
```

```
TASK [4.4.6 Configuring SSH ? set Idle Timeout Interval for User Login Profile Applicability The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time. Verify ClientAliveInterval is between 1 and 300.] ***  
ok: [10.8.29.103]
```

```
TASK [The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time.] ***
```

```
fatal: [10.8.29.103]: FAILED! => {  
    "assertion": "'/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' in (idle_timeout2.files  
| map(attribute='path') | join(', '))",  
    "changed": false,  
    "evaluated_to": false,  
    "msg": "Assertion failed"  
}  
...ignoring
```

```
TASK [4.4.7 Configuring SSH ? restrict Cipher list This variable limits the types of ciphers that SSH can use during communication.]  
*****
```

```
ok: [10.8.29.103]
```

```
TASK [This variable limits the types of ciphers that SSH can use during communication. Verify the ciphers value should be Ciphers aes256-ctr,aes192-ctr,aes128-ctr]  
*****
```

```
fatal: [10.8.29.103]: FAILED! => {  
    "assertion": "'/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' in (ciphers.files  
| map(attribute='path') | join(', '))",  
    "changed": false,  
    "evaluated_to": false,  
    "msg": "Assertion failed"  
}  
...ignoring
```

```
PLAY RECAP  
*****
```

```
10.8.29.103 : ok=167  changed=2    unreachable=0    failed=0    skipped=45  
rescued=0   ignored=29
```

4. Go to the /tmp directory at the IBM i managed node through SSH and verify that the reports are created, as shown in Example A-16.

Example A-16 Checking the JSON reports at IBM i managed node

```
qsecopr@SYS8781-VM2-T1:tmp# ls
bootstrap.sh
bootstrap.tar.Z
brms
ibm-portal-base.xsd
ibm-portal-security.xsd
ibm-portal-topology.xsd
lprcume.log
lpume.log
npm-314-3c402edc
npm-326-bbb41aa5
qareconf.log
s.slapd
s.slapd.QUSRDIR
security_management_sysval_report-level2-10.8.29.103-20211020T171243.json
security_management_userprofile_check_result-10.8.29.103-20211020T171519.json
```

5. To display the reports, use the **cat** command, as shown in Example A-17.

Example A-17 Security management system values report

```
# cat security_management_sysval_report-level2-10.8.29.103-20211020T171243.json
[
  {
    "name": "QALWOBJRST",
    "expect": "*NONE",
    "actual": "*ALL",
    "check": "equal",
    "compliant": false
  },
  {
    "name": "QALWUSRDMN",
    "expect": "QTEMP",
    "actual": "*ALL",
    "check": "equal",
    "compliant": false
  },
  {
    "name": "QAUDCTL",
    "expect": "*OBJAUD *AUDLVL",
    "actual": "*AUDLVL",
    "check": "equal_as_list",
    "compliant": true
  },
  {
    "name": "QAUDENDACN",
    "expect": "*PWRDWNSYS",
    "actual": "*NOTIFY",
    "check": "equal",
    "compliant": false
  },
  {
    "name": "QAUDENZACN",
    "expect": "*PWRDWNSYS",
    "actual": "*NOTIFY",
    "check": "equal",
    "compliant": false
  }
]
```

```

        "name": "QAUDFRCLVL",
        "expect": "1",
        "actual": "0",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QAUTOVRT",
        "expect": "0",
        "actual": "32767",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QCRTAUT",
        "expect": "*EXCLUDE",
        "actual": "*CHANGE",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QCRTOBJAUD",
        "expect": "*ALL",
        "actual": "*NONE",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QDSCJOBITV",
        "expect": "15",
        "actual": "0000000240",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QFRCCVNRST",
        "expect": "7",
        "actual": "1",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QINACTITV",
        "expect": "0000000015",
        "actual": "*NONE",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QINACTMSGQ",
        "expect": "*ENDJOB",
        "actual": "*ENDJOB",
        "check": "equal",
        "compliant": true
    },

```

```

{
    "name": "QLMTDEVSSN",
    "expect": "1",
    "actual": "0",
    "check": "equal",
    "compliant": false
},
{
    "name": "QMAXSGNACN",
    "expect": "3",
    "actual": "1",
    "check": "equal",
    "compliant": false
},
{
    "name": "QMAXSIGN",
    "expect": "000003",
    "actual": "*NOMAX",
    "check": "equal",
    "compliant": false
},
{
    "name": "QPWDCHGBLK",
    "expect": "99",
    "actual": "*NONE",
    "check": "equal",
    "compliant": false
},
{
    "name": "QPWDLVL",
    "expect": "3",
    "actual": "3",
    "check": "equal",
    "compliant": true
},
{
    "name": "QPWDRQDDIF",
    "expect": "1",
    "actual": "0",
    "check": "equal",
    "compliant": false
},
{
    "name": "QPWDRULES",
    "expect": "*ALLCRTCHG *DGTLMTAJC *DGTLMTFST *DGTLMLTSLT *DGTMIN1 *LMTPRFNAME *MAXLEN128
*MINLEN14 *REQANY3 *SPCCCHRLMTAJC *SPCCCHRLMTFST *SPCCCHRLMLTSLT",
    "actual": "*PWDSYSVAL",
    "check": "equal_as_list",
    "compliant": false
},
{
    "name": "QPWDVLDPGM",
    "expect": "*REGFAC",
    "actual": "*NONE",
    "check": "equal",
    "compliant": true
}

```

```

        "compliant": false
    },
    {
        "name": "QRMTSIGN",
        "expect": "*FRCSIGNON",
        "actual": "*FRCSIGNON",
        "check": "equal",
        "compliant": true
    },
    {
        "name": "QRETSVRSEC",
        "expect": "0",
        "actual": "1",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QSECURITY",
        "expect": "50",
        "actual": "50",
        "check": "equal",
        "compliant": true
    },
    {
        "name": "QSHRMMEMCTL",
        "expect": "0",
        "actual": "1",
        "check": "equal",
        "compliant": false
    },
    {
        "name": "QVFYOBJRST",
        "expect": "5",
        "actual": "3",
        "check": "equal",
        "compliant": false
    }
}

```

Tip: The first JSON file shows which IBM i system values are compliant and which must be adjusted.

The other report on JSON files is shown in Example A-18.

Example A-18 IBM i user profiles check results

```
# cat security_management_userprofile_check_result-10.8.29.103-20211020T171519.json
[
    {
        "id": "3.1",
        "desc": "3.1 PUBLIC authority to all user profiles should be EXCLUDE with the following exceptions QDBSHR QDBSHRDO QTMLPLD",
        "result": "PASS"
    },
    {
        "id": "3.2",

```

```

    "desc": "3.2 All Private authorities to all user profiles other than the owner's and the
profile itself should be removed.",
    "result": "PASS"
},
{
    "id": "3.3",
    "desc": "3.3 All IBM Supplied Profiles shall be owned by QSYS with the following
exceptions QFAXMSF shall be owned by QAUTPROF QRDARS400xx shall be owned by QRDARS400 QTIVOLI,
QTIVROOT and QTIVUSER shall be owned by QTIVOLI Non-IBM (user created) profiles shall be owned
by QSECOFR or QSYS.",
    "result": "FAIL",
    "vulnerables": "QFAXMSF, QICC",
    "remediation": "CHGOBJOWN OBJ(SYS_ONAME_REPLACE) OBJTYPE(*USRPRF) NEWOWN(QSECOFR)
CUROWNAUT(*REVOKE)"
},
{
    "id": "3.6",
    "desc": "3.6 Default passwords provide an opportunity for someone to enter your system,
if someone knows your policy for assigning profile names and knows that a new person is joining
your organization. Additionally, accounts with default passwords are often used for shared
(non-unique) accounts. Tell the new user the password confidentially, such as in a 'Welcome to
the System' letter that outlines your security policies. Require the user to change the password
the first time that the user signs on by setting the user profile to PWDEXP(*YES).",
    "result": "FAIL",
    "vulnerables": "AS45G01, MARCE",
    "remediation": "CHGUSRPRF USRPRF(USER_NAME_REPLACE) PWDEXP(*YES)"
},
{
    "id": "3.7",
    "desc": "3.7 Disable inactive user profiles within 90 days.",
    "result": "FAIL",
    "vulnerables": "QTFTP, QSRV, QLPISTALL, QDFTOWN, QDSNX, QSRVBAS, QAUTPROF, QNETSPLF,
QSVCCS, QCCLUSTER, QSPL, QDLFM, QTMHHTP1, QCOLSRV, QMGTC, CLPADMIN, QLPAUTO, QSOC, QSNADS,
QANZAGENT, QTSTRQS, QYCMCIMOM, QGATE, QEJB, QDOC, QPEX, QFAXMSF, QEJBSVR, QNFSANON, QTMLPD,
QIBMHELP, QFNC, QIPP, QWSERVICE, QDBSHR, QNTP, QOBJC, QICC, QDBSHRDO, QRJE",
    "remediation": "CHGUSRPRF USRPRF(USER_NAME_REPLACE) STATUS(*DISABLED)"
},
{
    "id": "3.8",
    "desc": "3.8 User Profiles with non-expiring passwords are never required to change
their Service accounts may be excluded from the audit and remediation. A service account is a
user account that is created explicitly to provide a security context for automated system and
application services running on the system. Service accounts should be configured with a
non-trivial, complex password that is used in an automated service process and never used
interactively. Service accounts should be documented and their Password expiration interval
should be set to *NOMAX. A process should then be documented and executed to periodically change
their passwords manually.",
    "result": "FAIL",
    "vulnerables": "QBRMS, QTMLPD",
    "remediation": "CHGUSRPRF USRPRF(USER_NAME_REPLACE) PWDEXPITV(*SYSVAL)"
},
{
    "id": "3.9",
    "desc": "3.9 User Profiles with command line access can run commands they are authorized
to from a command line."
}

```

```

        "result": "FAIL",
        "vulnerables": "QTFTP, QSRV, QLPINSTALL, QSSHDL, QSRVAGT, AS45G01, QDFTOWN, QDSNX,
QSVMSS, QIJS, QSRVBAS, QSYSOPR, QAUTPROF, QNETSPLF, QTCM, QHAUSRPRF, QSVCCS, QCLUSTER, QBRMS,
QSPL, QDLFM, QTMHHTP1, QCOLSRV, QSVSM, MARCE, QMGTC, CLPADMIN, QRJE, QPM400, QLPAUTO, QUSER,
QSOC, QMSF, QSNADS, QANZAGENT, QTSTRQS, QWEBADMIN, QYCMCIMOM, QGATE, QSECOFR, QEJB, QDOC, QPEX,
QFAXMSF, QPGMR, QEJBSVR, QCIUSER, QNFSANON, QTMLPD, QIBMHELP, QLWISVR, QFNC, QSYS, QIPP,
QWSERVICE, QTCP, QDBSHR, QNTP, QOBJC, QSPLJOB, QICC, QTMHHTP, QDBSHRDO, QCLUMGT, QYPSJSVR",
        "remediation": "CHGUSRPRF USRPRF(USER_NAME_REPLACE) LMTCPB(*YES)"
    },
    {
        "id": "3.10A",
        "desc": "3.10A Check some parameters if they match the default values that are used for all IBM-supplied user profiles.",
        "sql": "SELECT AUTHORIZATION_NAME, NO_PASSWORD_INDICATOR, STATUS, USER_CLASS_NAME,
INITIAL_PROGRAM_NAME, LIMIT_CAPABILITIES, SPECIAL_AUTHORITIES FROM QSYS2/USER_INFO WHERE
AUTHORIZATION_NAME LIKE 'Q%' AND NO_PASSWORD_INDICATOR = 'NO' OR AUTHORIZATION_NAME LIKE 'Q%'
AND STATUS = '*DISABLED' OR AUTHORIZATION_NAME LIKE 'Q%' AND USER_CLASS_NAME <> '*USER' OR
AUTHORIZATION_NAME LIKE 'Q%' AND INITIAL_PROGRAM_NAME <> '*NONE' OR AUTHORIZATION_NAME LIKE 'Q%'
AND LIMIT_CAPABILITIES <> '*NO' OR AUTHORIZATION_NAME LIKE 'Q%' AND SPECIAL_AUTHORITIES <>
'*NONE''",
        "remediation": "Review the results. This indicates that one or more of the following parameters of the profiles in the list does not match the default values that are used for all IBM-supplied user profiles. x NO_PASSWORD_INDICATOR (PASSWORD) = YES (Default) x STATUS (STATUS) = *ENABLED (Default) x USER_CLASS_NAME (USRCLS) = *USER (Default) x INITIAL_PROGRAM_NAME (INLPGM) = *NONE (Default) x LIMIT_CAPABILITIES (LMTCPB) = *NO (Default) x SPECIAL_AUTHORITIES (SPCAUT) = *NONE (Default) x Compare the results of the screen output to information about IBM-supplied profiles, their purpose, and values for any IBM-supplied profiles that are different from the defaults from the shipped defaults from the following link.  

https://www.ibm.com/support/knowledgecenter/en/ssw\_ibm\_i\_74/rzarl/rzarlibmprfa.htm",

        "result": "FAIL"
    },
    {
        "id": "3.10B",
        "desc": "3.10B To check if IBM Supplied Profiles are being used as Group Profiles.",
        "result": "PASS"
    },
    {
        "id": "3.11",
        "desc": "Group profiles should not have a password as they are usually not associated with a unique account.",
        "result": "PASS"
    },
    {
        "id": "5.1",
        "desc": "QSECOFR Profile Shall Be DISABLED.",
        "result": "FAIL",
        "vulnerables": "QSECOFR",
        "remediation": "CHGUSRPRF USRPRF(QSECOFR) STATUS(*DISABLED)"
    },
    {
        "id": "5.2",
        "desc": "QSECOFR Shall Not be Configured as a Group Profile.",
        "result": "PASS"
    }

```

Related publications

The publications that are listed in this section are considered particularly suitable for a more detailed discussion of the topics that are covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide more information about the topic in this document. Note that some publications that are referenced in this list might be available in softcopy only:

- ▶ *Simplify Management of IT Security and Compliance with IBM PowerSC in Cloud and Virtualized Environments*, SG24-8082
- ▶ *IBM PowerVM Adds Support for Little Endian Linux Workloads*, TIPS1317
- ▶ *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940
- ▶ *Red Hat OpenShift and IBM Cloud Paks on IBM Power Systems: Volume 1*, SG24-8459
- ▶ *SUSE and IBM Power Systems for SAP HANA*, REDP-5620
- ▶ *IBM Power Systems Security for SAP Applications*, REDP-5578
- ▶ *IBM QRadar Version 7.3 Planning and Installation Guide*, SG24-8412
- ▶ *Deployment Guide for InfoSphere Guardium*, SG24-8129
- ▶ *IBM PowerVC Version 1.3.2 Introduction and Configuration*, SG24-8199
- ▶ *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, SG24-8100
- ▶ *IBM Power E1080 Technical Overview and Introduction*, REDP-5649

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Other publications

The following publications also are relevant as further information sources:

- ▶ AIX 7.2 Security Guide:
https://www.ibm.com/docs/en/ssw_aix_72/security/security_pdf.pdf
- ▶ Red Hat Enterprise Linux 8 Security Hardening:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/red_hat_enterprise_linux-8-security_hardening-en-us.pdf
- ▶ Operating System Security Hardening Guide for SAP HANA for SUSE Linux Enterprise Server 15:
https://documentation.suse.com/sbp/all/pdf/OS_Security_Hardening_Guide_for_SAP_HANA_SLES15_color_en.pdf

- ▶ IBM X-Force Threat Intelligence Index 2021:
<https://www.ibm.com/downloads/cas/M1X3B7QG>

Online resources

The following websites also are relevant as further information sources:

- ▶ IBM PowerSC 2.0 Documentation:
<https://www.ibm.com/docs/en/powersc-standard/2.0>
- ▶ IBM Power Systems Virtual Server Documentation:
<https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-getting-started>
- ▶ IBM Cloud Architecture Center:
<https://www.ibm.com/cloud/architecture/>
- ▶ IBM PowerSC Multi Factor Authentication 2.0 Documentation:
<https://www.ibm.com/docs/en/powersc-mfa/2.0>
- ▶ National Institute of Standards and Technology Security Content Automation Protocol:
<https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Release/scap-1-3>

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



REDP-5659-00

ISBN 0738460508

Printed in U.S.A.

Get connected

