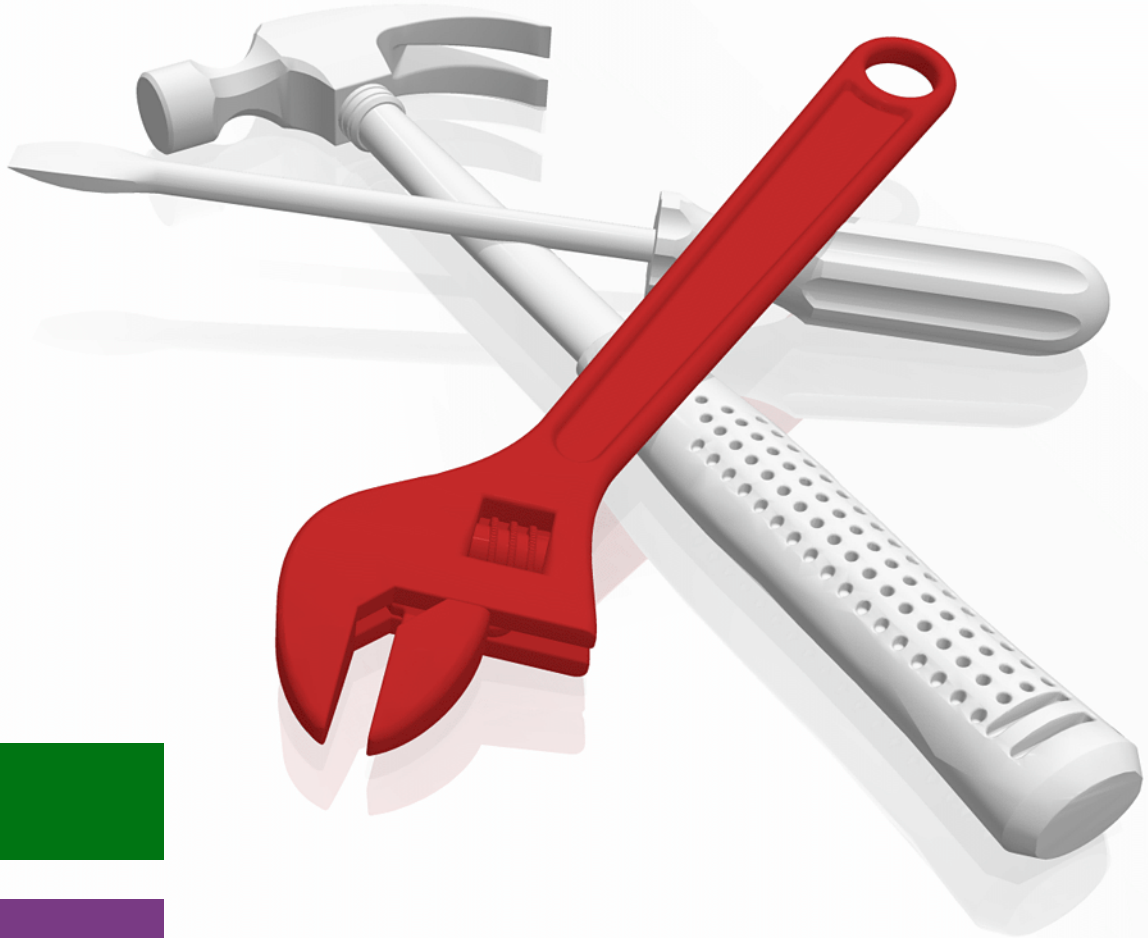
Redbooks
ibm.com/redbooks

# IBM Power Systems Security for SAP Applications

Dino Quintero

Peter Altevogt



Security

Power Systems

IBM

Redpaper

IBM Redbooks

# IBM Power Systems Security for SAP Applications

February 2020

REDP-5578-00

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

**First Edition (February 2020)**

This document was created or updated on February 19, 2020.

# Contents

# 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.

| | | |
|---|---|---|
| Redbooks (logo)  ® | Guardium® | POWER9™ |
| AIX® | IBM® | PowerVM® |
| Db2® | POWER® | Redbooks® |

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.

Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries 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 highlights the RAS and security features on the hardware, hypervisor, Linux, and SAP application levels. It highlights what is transparent, what needs enablement, and also the known prerequisites for the use of these features.

## Authors

This paper was produced in close collaboration with the IBM SAP International Competence Center (ISICC) in Walldorf, SAP Headquarters in Germany and IBM Redbooks®.


**Dino Quintero** is an IT Management Consultant and an IBM Level 3 Senior Certified IT Specialist with IBM Redbooks in Poughkeepsie, New York. He has 24 years of experience with IBM Power Systems technologies and solutions. Dino shares his technical computing passion and expertise by leading teams that develop technical content in the areas of enterprise continuous availability, enterprise systems management, high-performance computing, cloud computing, artificial intelligence, including machine and deep learning, and cognitive solutions. He also is a Certified Open Group Distinguished IT Specialist. Dino is formerly from the province of Chiriqui in Panama. Dino holds a Master of Computing Information Systems degree and a Bachelor of Science degree in Computer Science from Marist College.

**Peter Altevogt** is a performance architect at IBM Germany Research & Development GmbH in Boeblingen. He has built up and led performance teams for IBM BladeCenter systems, IBM Information Management Software products and Cloud management software. His interests include especially computer architectures, in-memory databases, and performance analysis based on discrete-event simulations and queuing modeling. Peter holds degrees in Mathematics and Physics from the University of Heidelberg and a doctorate in Theoretical Physics from the University of Karlsruhe. He joined the IBM Scientific Center in Heidelberg in 1991 to work on various High-Performance Computing projects before he moved to the IBM Germany Research & Development GmbH in 1998. In 2009, he spent several months at the IBM Zurich Research Laboratory working on processor performance modeling. He is currently working on optimizing SAP HANA for IBM Power Systems. Furthermore, Peter teaches Computer Architecture at the Karlsruhe University of Applied Sciences.

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

Wade Wallace
IBM Redbooks, Poughkeepsie Center

Katharina Probst, Walter Orb, Tanja Scheller
IBM Germany

## 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 Facebook:

  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:

  http://twitter.com/ibmredbooks
- Look for 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

1

# Reliability, Availability, and Serviceability (RAS) and security features for SAP applications

This chapter describes the RAS and security features on the hardware, hypervisor, Linux, and SAP application levels. It highlights what is transparent, what needs enablement, and also the known prerequisites for the use of these features.

This chapter covers the following topics:

- RAS introduction
- RAS features on system level
- RAS features on Linux level
- RAS features on data center level
- Conclusions for SAP applications

## 1.1 RAS introduction

The RAS properties can be defined as follows[1]:

- Reliability can be defined as the probability that a system will produce correct outputs for a stated time interval.
- Availability means the probability that a system is operational at a given time.
- Serviceability or maintainability is the simplicity and speed with which a system can be repaired or maintained.

A careful implementation of RAS features on the systems or data center level provides significant business value, for example, by supporting business continuity. This is achieved by minimizing the frequency of planned and respectively unplanned downtimes.

Some of the key methods to improve RAS properties are:

- Choosing high-quality, reliable components.
- Error checking (monitoring) and detection.
- Error correction (self-healing).
- Isolation of defect components.
- Introduction of spare (redundant) components (for example, eliminate single points of failure) and leveraging them if necessary.
- Replication of components.
- Predictive deallocation of defect components and migration of work to other components.
- Enabling concurrent maintenance, for example, the ability to replace or update defect components during system run time.
- Providing sufficient information to users in case of errors for analysis.
- Providing mechanisms to alert users in case of errors.

## 1.2 RAS features on system level

Section 1.1, “RAS introduction” outlines the methods for implementing RAS. Now in the current section, Table 1-1, “Key RAS features of POWER9 processor-based systems” provides a summary of the key RAS features for IBM POWER9™ processor-based systems. Also, see the following links for detailed descriptions of how these methods are implemented for IBM Power Systems (for example, for CPU cores, the memory subsystem, various interconnects, power supply units, and so on):

- IBM POWER® Processor-Based Systems RAS

  https://www.ibm.com/downloads/cas/2RJYYJML
- IBM Power System L922 Technical Overview and Introduction, REDP-5496-00

  http://www.redbooks.ibm.com/redpapers/pdfs/redp5496.pdf
- IBM Power System AC922 Technical Overview and Introduction, REDP-5494-00

  http://www.redbooks.ibm.com/abstracts/redp5494.html?Open

[1] Reliability, availability and serviceability: https://en.wikipedia.org/wiki/Reliability,_availability_and_serviceability

- IBM Power System E950 Technical Overview and Introduction, REDP-5509-00
  http://www.redbooks.ibm.com/abstracts/redp5509.html?Open
- IBM Power System E980 Technical Overview and Introduction, REDP-5510-00
  http://www.redbooks.ibm.com/abstracts/redp5510.html?Open

For convenience, a summary of the key RAS features for IBM POWER9 processor-based systems are shown in Table 1-1. For further details, see the white paper POWER Processor-Based Systems RAS[2].

*Table 1-1 Key RAS features of POWER9 processor-based systems*

| System components | RAS feature | POWER9 based systems | | |
|---|---|---|---|---|
| | | **1 and 2 socket systems[a]** | **IBM Power Systems E950** | **IBM Power Systems E980** |
| **Processor** | First failure data capture[b] | Yes[c] | Yes | Yes |
| | Processor instruction retry | Yes[c] | Yes | Yes |
| | Power and cooling monitor function integrated into processors on chip controllers | Yes[c] | Yes | Yes |
| | CRC checked processor fabric bus retry with spare data lane | Yes[c] | Yes | Yes |
| | Extended L2/L3 cache line delete | No | Yes | Yes |
| | Core contained checkstops | No | Yes | Yes |
| | Redundant global processor clocks with concurrent failover | No | No | Yes |
| **SMP fabric** | Multi-node RAS | N/A | N/A | Yes |
| **PCIe** | Hot-plug with processor-integrated PCIe controller | Yes | Yes | Yes |
| **Memory** | DIMM ECC supporting x4 Chipkill[a] | Yes | Yes | Yes |
| | Uses IBM memory buffer and has spare DRAM module capability with x4 DIMMS[c] | No | Yes | Yes |
| | x8 DIMM support with Chipkill correction for marked a DRAM[c] | N/A | N/A | Yes |
| | Custom DIMM support with additional spare DRAM capability[c] | No | No | Yes |
| | Active memory mirroring for the hypervisor | No | Yes (feature) | Yes (base) |
| **Service Processor** | Redundant service processor and related book facilities | No | No | Yes |
| **Trusted Platform Module (TPM)** | Redundant TPM | No | No | Yes |

[2] POWER Processor-Based Systems RAS: https://www.ibm.com/downloads/cas/2RJYYJML

| System components | RAS feature | POWER9 based systems | | |
|---|---|---|---|---|
| **Multi-node** | Multi-node support | No | No | Yes |
| **Power supply** | Redundant or spare voltage phases on voltage converters for levels that feed processor and custom memory DIMMs or memory risers | No | Redundant only | Redundant and space |

a. IBM Power System S914, IBM Power System S922, IBM Power System S924, IBM Power System H922, IBM Power System S924, IBM Power System H924.

b. “First failure data capture” (FFDC) refers to automated solutions that are typically “on” and ready to work the first time that an error or failure occurs. FFDC also refers to reducing the burdens of problem reproduction and repetitive data capture.

c. In scale-out systems, Chipkill capability is per rank of a single Industry Standard DIMM (ISDIMM). In IBM Power System E950, Chipkill and spare capability is per rank spanning across an ISDIMM pair. And in the IBM Power System E980, it is per rank spanning across two ports on a Custom DIMM.The E950 system also supports DRAM row repair.

## 1.3 RAS features on Linux level

A general description of RAS support by the Linux kernel can be found in:

- The Linux kernel user’s and administrator’s guide

  https://www.kernel.org/doc/html/v4.20/admin-guide/ras.html

This section focuses on one distinguishing serviceability feature of POWER-based Linux systems, namely the firmware-assisted kernel dump (fadump).

The fadump solves some drawbacks of the standard Linux kernel dump (kdump) facility: after Linux crashes, the system is in an inconsistent state, especially the PCIe and I/O devices. In some rare cases, a rogue DMA or ill-behaving device drivers can cause the kdump capture to fail. The fadump addresses this problem by the firmware taking over control, rebooting the entire system (preserving only the memory), and resetting all other devices by going through the BIOS.

For further details, see the following references and the appropriate documentation for the SLES and RHEL Linux distributions:

- Configuring fadump on SLES12 SP3 and SLES 15

  https://www.suse.com/support/kb/doc/?id=7023277

- Kernel Administration Guide. Chapter 7. Kernel crash dump guide

  https://red.ht/2XQiJlh

## 1.4 RAS features on data center level

The methods outlined in section 1.1, “RAS introduction” on page 2 can also be implemented on the data center level. For example, you can introduce redundant networks, backup power generators, backup virtual machines, and so on. This approach is described in detail in the following resources:

- IBM VM Recovery Manager HA for Power Systems, V1.3 provides availability management for virtual machines

  https://ibm.co/35Gyvls

- Implementing High Availability and Disaster Recovery Solutions with SAP HANA on IBM Power Systems, REDP-5443-00

  http://www.redbooks.ibm.com/redpapers/pdfs/redp5443.pdf

- SAP HANA on IBM Power Systems: High Availability and Disaster Recovery Implementation Updates, SG24-8432-00

  http://www.redbooks.ibm.com/abstracts/sg248432.html?Open

- SAP HANA – High Availability V5.0, SAP March 2017

  https://bit.ly/2TUvc7i

## 1.5 Conclusions for SAP applications

Business processes supported by SAP applications frequently need to be available 24 x 7, because they are used by customers worldwide. Therefore, a key requirement against SAP applications (and especially against the systems infrastructure that supports these applications) is to provide long time intervals between system failures and scheduled maintenance windows. The high availability designs described in section 1.4, “RAS features on data center level” on page 5 are useful here but expensive and elaborate to implement in a reliable manner. Therefore, the excellent RAS features provided by IBM Power Systems addressing enterprise-level requirements on the system level frequently make such a data center level solution superfluous.

## 1.6 References

This section provides additional referential materials that compliment the information in this chapter and in this publication.


1. Reliability, availability, and serviceability

   https://en.wikipedia.org/wiki/Reliability,_availability_and_serviceability

2. POWER Processor-Based Systems RAS

   https://www.ibm.com/downloads/cas/2RJYYJML

3. IBM Power System L922 Technical Overview and Introduction, REDP-5496-00

   http://www.redbooks.ibm.com/redpapers/pdfs/redp5496.pdf

4. IBM Power System AC922 Technical Overview and Introduction, REDP-5472-00

   http://www.redbooks.ibm.com/abstracts/redp5472.html?Open

5. IBM Power System E950 Technical Overview and Introduction, REDP-5509-00

   http://www.redbooks.ibm.com/abstracts/redp5509.html?Open

6. IBM Power System E980 Technical Overview and Introduction, REDP-5510-00

   http://www.redbooks.ibm.com/abstracts/redp5510.html?Open

7. The Linux kernel user's and administrator's guide

   https://www.kernel.org/doc/html/v4.20/admin-guide/ras.html

8. Configuring fadump on SLES12 SP3 and SLES 15

   https://www.suse.com/support/kb/doc/?id=7023277

9. Kernel Administration Guide. Chapter 7. Kernel crash dump guide

   https://red.ht/2NW2UWm

10. IBM VM Recovery Manager HA for Power Systems, V1.3 provides availability management for virtual machines

    https://ibm.co/38FNBJw

11. Implementing High Availability and Disaster Recovery Solutions with SAP HANA on IBM Power Systems, REDP-5443-00

    http://www.redbooks.ibm.com/redpapers/pdfs/redp5443.pdf

12. SAP HANA on IBM Power Systems: High Availability and Disaster Recovery Implementation Updates, SG24-8432-00

    http://www.redbooks.ibm.com/abstracts/sg248432.html?Open

13. SAP HANA - High Availability V5.0, SAP March 2017

    https://bit.ly/3OO8TSr

2

# Security considerations for SAP applications

This chapter describes system level and operating system security considerations.

This chapter covers the following topics:

- Introduction
- System level security
- Operating system and application level security
- Conclusions for SAP applications
- References

## 2.1 Introduction

Essentially, computer security deals with computer-related assets that are subject to a variety of threats and for which various measures are taken to protect those assets[1]. In other words, computer security engineering needs to address the following three fundamental questions:

1. What assets require protection?
2. How are those assets threatened?
3. What can we do to counter those threats?

The assets of an SAP solution consist of server and storage hardware, the software stack and networks. All these assets require protection to ensure, for example, data confidentiality and integrity, privacy, system integrity, availability, and accountability. A security breach can have a severe impact on the organizational operations and the types of security threats and attacks are manifold. A comprehensive approach to security requires a security strategy that leverages basic security design principles[2].

This section focuses on some important security features provided by IBM POWER9 Systems hardware and the PowerVM® Hypervisor, Linux on IBM POWER9 Systems and their meaning for SAP applications.

## 2.2 System level security

This section describes the system security level features.

### 2.2.1 Secure boot

The key PowerVM features available in IBM POWER9 include,[3, 4]

- A secure initial program load (IPL) process (respectively the Secure Boot feature) allows only appropriately signed firmware components to run on the system processors. Each component of the firmware stack, including hostboot, the POWER Hypervisor (PHYP), and partition firmware (PFW), is signed by the platform manufacturer and verified as part of the IPL process.
- A framework to support remote attestation of the system firmware stack through a hardware trusted platform module (TPM).
- Trusted Boot seeks to create cryptographically strong and well-protected platform measurements to prove that particular firmware components have executed on the system. Subsequently, interested parties can assess the measurements by way of trusted protocols to make inferences about the system's state and use that information to make security decisions.

The Secure Boot feature prevents unauthorized access to customer data through these means: unauthorized firmware that runs on a system processor, by access through security vulnerabilities in authorized service processor firmware, or through hardware service interfaces accessed through flexible service processor (FSP).

---

[1] An Introduction to Computer Security: The NIST Handbook. National Institute of Standards and Technology, Special Publication 800-12, October 1995.
[2] Computer Security: Principles and Practice, Fourth Edition. Pearson Education, Inc., 2017.
[3] Secure Boot in PowerVM: https://www.ibm.com/support/knowledgecenter/en/POWER9/p9ia9/p9ia9_kickoff.htm
[4] POWER9 Introduces Secure Boot to PowerVM: https://ibm.co/2ruvpCa

The presented mechanisms do not provide protection against:

- Operating system software-based attacks to gain unauthorized access to customer data
- Rogue system administrators
- Hardware physical attacks (for example, chip substitutions and bus-traffic recording)

### 2.2.2 Security between different LPARS

PowerVM takes advantage of the POWER hardware to provide high levels of security. The hardware is designed with three different protection domains:

- Hypervisor
- Kernel
- Application

The hardware limits the instructions that can be executed based on the current protection domain, and the hardware provides specific entry points to transition between domains. If a lower-priority domain attempts to issue an instruction reserved for a higher priority domain, the instruction will generate an instruction interrupt within the current domain. The most privileged level is the hypervisor domain, which is where the PowerVM security engineering takes place. For example, instructions that change the mapping of partition addresses to physical real addresses and instructions that modify specific hardware registers are restricted such that they are only allowed in hypervisor mode.

When the processor initially starts executing at server power-on, the processor is running in hypervisor mode. The service processor has ensured that the firmware that is executing has been digitally signed. As a result, you are assured this firmware was created by IBM for this server (2.2.1, “Secure boot” on page 8). The PowerVM hypervisor will initialize all of the data structures that are needed to provide a secure environment for running multiple virtual machines (LPARs) on the server. When a partition is started, the hypervisor dispatches the partition to run on a physical hardware thread. This process of dispatching partitions also changes the security domain from hypervisor to kernel or application domains. If the partition needs to make a request of the hypervisor, the partition issues a system call instruction. This instruction switches the processor to hypervisor mode and changes the next instruction to a fixed interrupt address in physical real memory. In addition to the system call instruction, there are a couple of other interrupts that are directed to the hypervisor instead of being handled by a partition.

To sum up, the system has been designed such that it enters hypervisor mode only at power-on and at fixed interrupt locations. This architecture is the basis of the separation of hypervisor functions from OS and applications functions.

The way that the hardware has been designed, only the hypervisor is able to access memory by way of a physical real address. Code that runs in partitions accesses memory only through a layer of indirection where the partition’s addresses are actually aliases to the physical real memory. In other words, every memory request from a partition is validated by the hypervisor. And therefore, PowerVM is able to maintain isolation of the memory contents between partitions. This provides partition isolation.

For more details about security between LPARs, see *How does PowerVM provide security between different LPARs* at the following website:

https://ibm.co/2uclLWt

This strong LPAR isolation makes IBM Power Systems servers with PowerVM a good match for Managed Service Providers and Cloud Solution Providers implementing multiple-LPAR support for SAP applications.

## 2.3 Operating system and application level security

Building and deploying an SAP system on Linux must be a planned process that is designed to counter security threats and maintain security during its operational lifetime. This process must include,[5]

- Assessing risks and plan the system deployment.
- Securing the underlying operating system and then the SAP applications.
- Ensuring that any critical content is secured.
- Ensuring that appropriate network protection mechanisms are used.
- Ensuring that appropriate processes are used to maintain security.

Furthermore, the following issues must be considered:

- The purpose of the system, the type of information stored, the applications and services provided, and their security requirements.
- The categories of users of the system, the privileges they have, and the types of information they can access.
- How the users are authenticated.
- How access to the information stored on the system is managed.
- What access the system has to information that is stored on other hosts, such as file or database servers, and how this is managed.
- Who will administer the system, and how they will manage the system (by way of local or remote access).
- Any additional security measures required on the system, including the use of host firewalls, anti-virus or other malware protection mechanisms, and logging.

### 2.3.1 Linux security

A critical step in securing an SAP application on Linux is to secure the base operating system upon which all other applications and services rely. A good security foundation must have a properly installed, patched, and configured operating system.

The following basic steps must be used to secure any operating system:[6]

- Install and patch the operating system.
- Harden and configure the operating system to adequately address the identified security needs of the system by,
  - Removing unnecessary services, applications, and protocols.
  - Configuring users, groups, and permissions.
  - Configuring resource controls.
  - IBM ships PowerSC,[7] which is able to provide Industry- and Application-aware, predefined security hardening automation also for SAP applications. Furthermore, it includes all related hardening aspects such as IBM Virtual I/O Server (VIOS)[8].

[5] Scarfone, K.; Jansen, W.; and Tracy, M. Guide to General Server Security, NIST Special Publication 800-123, July 2008: https://csrc.nist.gov/publications/detail/sp/800-123/final

[6] Ibid

[7] Simplify Management of IT Security and Compliance with IBM PowerSC in Cloud and Virtualized Environments: http://www.redbooks.ibm.com/abstracts/sg248082.html?Open

[8] IBM Knowledge Center Virtual I/O Server overview: https://ibm.co/3aUt5qv

- Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection systems (IDS), if needed.
- Test the security of the basic operating system to ensure that the steps taken adequately address its security needs.

To ensure Linux security, the following items are worth considering:

- Ensure physical server security
- Encrypt data communication (in flight and in rest)
- Avoid the use of FTP, telnet, and rlogin or rsh services
- Minimize installed software to minimize vulnerability
- Use only one network service per system
- Keep Linux kernel and software up to date
- Use Linux security extensions
- Use SELinux
- Implement a good and strong password policy
- Set up password aging
- Restrict use of previous passwords
- Lock user accounts after login failures
- Verify that no accounts have empty passwords
- Make sure that no non-root accounts have UID set to 0
- Disable root login
- Disable unwanted services
- Find unwanted listening network ports
- Delete X Window Systems (X11)
- Configure iptables and tcpwrappers based firewall
- Harden */etc/sysctl.conf*
- Separate disk partitions for system and user data
- Enable disk quotas for all users
- Turn off IPv6 only if you are *not* using it
- Disable unwanted SUID and SGID binaries
- Find all world-writable files and correct permissions
- Find noowner files and assign or delete them
- Use a centralized authentication service
- Use Kerberos
- Enable and configure logging and auditing
- Monitor suspicious log messages, for example, with logwatch or logcheck
- Enable system accounting with auditd
- Secure the OpenSSH server
- Install and use intrusion detection system
- Disable USB, firewire, and thunderbolt devices
- Disable unused services
- Use fail2ban or denyhost as IDS (install an intrusion detection system)
- Secure Apache, PHP, and Nginx server
- Encrypt files, directories, and email
- Make backups

For the technical details and further references on Linux security in general, see Linux Server Hardening Security Tips at the following website:

`https://www.cyberciti.biz/tips/linux-security.html`

For comprehensive introductions to security aspects of the SUSE Linux Enterprise Server and Red Hat Enterprise Linux 8, refer to the following publications:

- Security Guide, SUSE Linux Enterprise Server 12 SP4

  `https://documentation.suse.com/sles/12-SP4/pdf/book-security_color_en.pdf`

- Security Guide, SUSE Linux Enterprise Server 15 SP1

  https://documentation.suse.com/sles/15-SP1/pdf/book-security_color_en.pdf
- Red Hat Enterprise Linux 8, Security hardening

  https://red.ht/38Bafm3

### 2.3.2 SAP application security

SAP application security is covered in great detail in various SAP security guides, for example:

- SAP HANA Security Guide

  https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.02/en-US
- SAP NetWeaver Application Server for ABAP Security Guide

  https://bit.ly/2Gqrdr7
- SAP NetWeaver Process Integration Security Guide

  https://bit.ly/2tE6U79

## 2.4 Conclusions for SAP applications

Ensuring security of an SAP solution requires a comprehensive approach that involves all hardware, software, and human resources involved. The combination of IBM POWER9 systems hardware and IBM PowerVM security features enables Secure Boot and a secure separation between different logical partitions by design. This provides a solid basis to ensure security of a complete SAP application stack. Also, along the stack looking into compliance and regulations, IBM provides additional SAP-integrated products to,

1. Harden all LPARs (IBM AIX®, Linux, and VIOS) with IBM PowerSC.
2. Run databases compliant to regulations (IBM Db2®, Oracle, Sybase, HANA) with IBM Guardium®.

## 2.5 References

This section provides additional reference materials that compliment the information in this chapter and in this publication.


1. Computer Security: Principles and Practice, Fourth Edition. Pearson Education, Inc., 2017
2. An Introduction to Computer Security: The NIST Handbook. National Institute of Standards and Technology, Special Publication 800-12, October 1995
3. Secure Boot in PowerVM

   https://www.ibm.com/support/knowledgecenter/en/POWER9/p9ia9/p9ia9_kickoff.htm
4. POWER9 Introduces Secure Boot to PowerVM

   https://ibm.co/3aIQgUj
5. How does PowerVM provide security between different LPARs

   https://ibm.co/38yOe96
6. Scarfone, K.; Jansen, W.; and Tracy, M. Guide to General Server Security, NIST Special Publication 800-123, July 2008

7. Linux Server Hardening Security Tips
   https://www.cyberciti.biz/tips/linux-security.html
8. Security Guide, SUSE Linux Enterprise Server 12 SP4
   https://documentation.suse.com/sles/12-SP4/pdf/book-security_color_en.pdf
9. Security Guide, SUSE Linux Enterprise Server 15 SP1
   https://documentation.suse.com/sles/15-SP1/pdf/book-security_color_en.pdf
10. Red Hat Enterprise Linux 8, Security hardening
    https://red.ht/2uzwDOj
11. SAP HANA Security Guide
    https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.02/en-US
12. SAP NetWeaver Application Server for ABAP Security Guide
    https://bit.ly/3aEX719
13. SAP NetWeaver Process Integration Security Guide
    https://bit.ly/2RpOBNS

# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

## IBM Redbooks

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

## Online resources

These websites are also relevant as further information sources:

- Linux kernel user's and administrator's guide

  https://www.kernel.org/doc/html/v4.20/admin-guide/ras.html
- Linux Server Hardening Security Tips

  https://www.cyberciti.biz/tips/linux-security.html

## Help from IBM

IBM Support and downloads

**ibm.com**/support

IBM Global Services

**ibm.com**/services

REDP-5578-00

ISBN 0738458511

Printed in U.S.A.