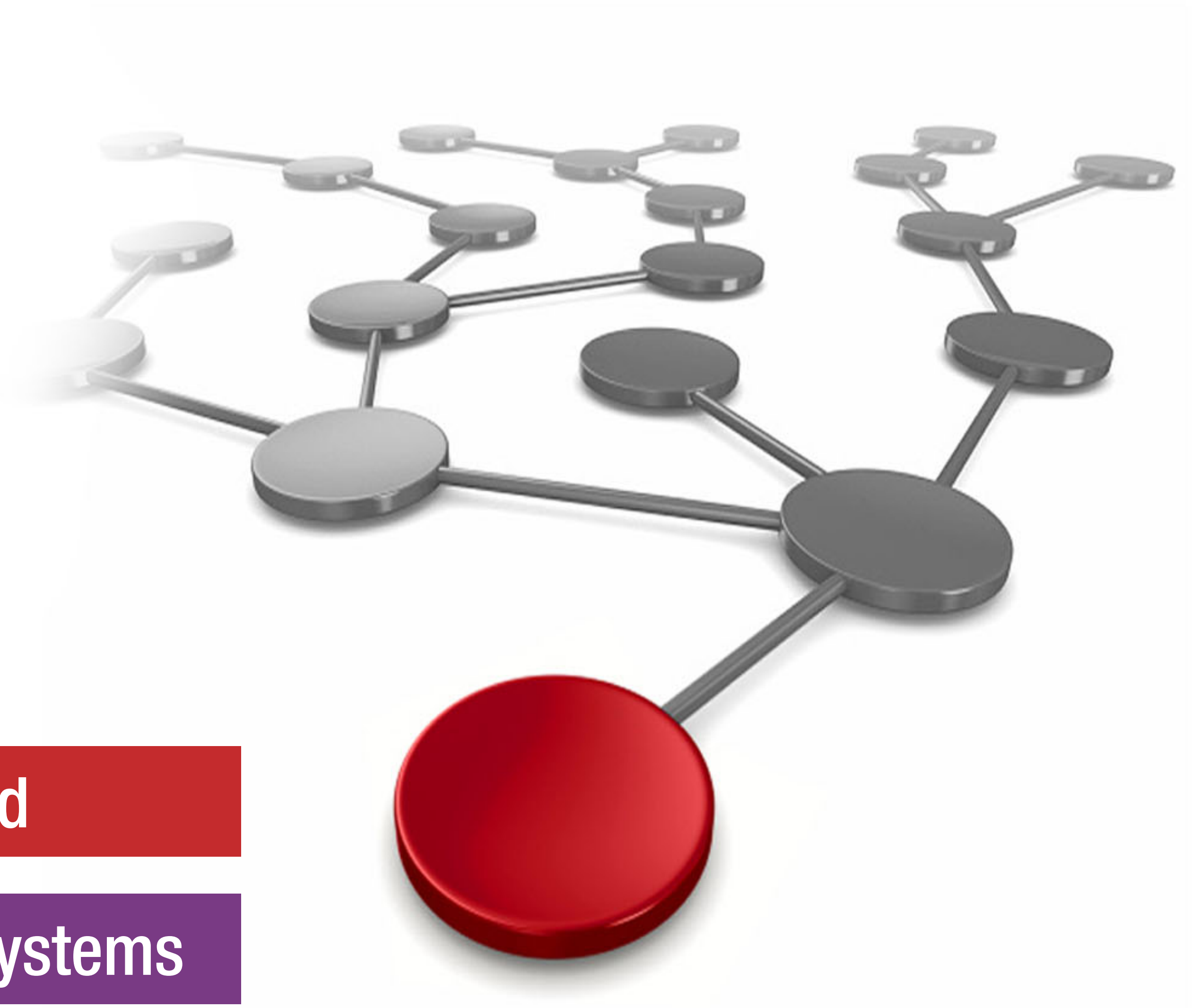
Redbooks
ibm.com/redbooks

IBM AIX and Enterprise Cloud Solutions

Ahmed Mashhour

Vivek Shukla

Shiv Kumar Tiwari



Cloud

Power Systems

IBM

Redpaper

IBM Redbooks

IBM AIX and Enterprise Cloud Solutions

June 2022

REDP-5660-00

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

First Edition (June 2022)

This edition applies to IBM AIX Standard and Enterprise Editions 7.3 (5765-G98).

This document was created or updated on June 28, 2022.

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.

AIX®
Aspera®
DB2®
IBM®
IBM Cloud®
IBM Cloud Satellite™
IBM FlashSystem®
IBM Spectrum®
Jazz®
OMEGAMON®
PIN®
Power10™
POWER8®
POWER9™
PowerHA®
PowerVM®
Redbooks®
Redbooks (logo) ®
Satellite™
SystemMirror®
Tivoli®
z/OS®

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.

Microsoft, 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 is a guide to IBM AIX and Enterprise Cloud Solutions.

AIX has a history of more than 35 years. It enables enterprise clients to run their business applications on IBM Power servers. With the passage of time, it is always upgraded with new features and technology (such as virtualization, high availability, security, and private and public clouds) to meet industry expectations.

AIX 7.3 and Power10 features further enable customers to get the best of both worlds; that is, reliable servers and operating systems with the latest technology.

The goal of this publication is to provide an overview of AIX and details about the latest Enterprise Cloud editions. It also describes AIX Automation, availability, and security, which is important information for any enterprise.

The Cloud Solutions chapter of this Redpaper publication includes information about how AIX fits into all types of cloud needs, whether private, public, or hybrid.

This publication is intended for professionals who want to update themselves with the latest features of AIX 7.3 and its Enterprise Cloud edition. It also is intended for users who want to gain a better understanding of how it fits into private, public, and hybrid cloud requirements. The target audience includes the following roles:

- Customers
- Sales and marketing professionals
- Technical support professionals
- IBM Business Partners

This book expands the set of IBM Power documentation by providing a desktop reference that offers a technical description overview of IBM AIX and Enterprise Cloud Solutions.

Authors

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

Ahmed Mashhour is a Power Systems Lab Services Consultant at IBM Egypt and IBM L2 certified Expert. He is IBM AIX, Linux, and IBM Tivoli certified with 17 years of professional experience in IBM AIX and Linux systems. He is an IBM AIX back-end SME who supports several customers in the US, Europe, and the Middle East. His core experience is in IBM AIX, Linux systems, clustering management, AIX security, virtualization tools, and various Tivoli and database products. He has authored several publications inside and outside of IBM, including co-authoring other IBM Redbooks publications. He also has hosted IBM AIX, Security, PowerVM, PowerHA, and IBM Spectrum Scale classes more than 80 times worldwide.

Vivek Shukla is a Presales Consultant for cloud, AI, and cognitive offerings in India and IBM Certified L2 (Expert) Technical Specialist. He has over 20 years of IT experience in Infrastructure Consulting, AIX, and IBM Power Servers and Storage implementations. He also has hands-on experience with IBM Power Servers, AIX and system software installations, RFP understandings, SOW preparations, sizing, performance tuning, RCA analysis, disaster recovery, and mitigation planning. He has written several Power FAQs and is Worldwide Focal for Techline FAQs Flash. He holds a Master's degree in Information Technology from IASE University and Bachelor's degree (BTech) in Electronics & Telecommunication Engineering from IETE, New Delhi. His area of expertise includes Red Hat OpenShift, Cloud Paks, and Hybrid Cloud.

Shiv Kumar Tiwari is a consultant at IBM Systems Lab Services India. He has over 17 years of expertise in IBM Power, AIX, and enterprise systems capabilities. He has worked to provide infrastructure solutions, design, and implementations for enterprise customers worldwide. Currently, his focus area is hybrid cloud and AI solutions. He holds a Master's degree in Information Management from the University of Mumbai.

The project that produced this publication was managed by Scott Vetter, PMP.

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

Ali El-Attar
Carl Burnett
Sanket Rathi
Ian Robinson
Jayen Shah
Brian Veale
IBM

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

1

Introduction to Advanced Interactive eXecutive

This chapter presents an introduction to Advanced Interactive eXecutive (AIX) and includes the following topics:

- "Advanced Interactive eXecutive overview" on page 2
- "AIX core and recent features" on page 5
- "IBM AIX 7.3 Standard Edition" on page 12

1.1 Advanced Interactive eXecutive overview

The Advanced Interactive eXecutive (AIX®) operating system is a secure, scalable, and robust open standards-based UNIX operating system. For over three decades, AIX has been the cornerstone of mission-critical computing for enterprise organizations in highly complex industries while evolving to introduce a wealth of new hybrid cloud and open source capabilities.

AIX 7.3 is the most current AIX release in the market and builds atop a strong history by providing new functions and capabilities that further improve performance, scale, availability, and security, all while maintaining application-binary compatibility to protect IT investments in AIX.

Coupled with the IBM POWER9™ and Power10™ processor-based Power Systems, AIX 7.3 delivers an optimized and even more resilient computing platform that adapts to changing business demands, including new cloud use cases and improved economics.

AIX is available in an Enterprise Edition or Enterprise Cloud Edition Bundles with PowerVC, VM Recovery Manager, and more to provide a ready to deploy private-cloud.

AIX version 7.3 is binary compatible with previous versions of the AIX operating system, including AIX 6, AIX 5L, and earlier versions of AIX. Applications that ran on earlier versions of AIX continue to run on AIX 7.3, which ensures that customers' investments are protected.

As we enter a new era of cloud-based computing, AIX continues to support the emerging technologies on which our customers' future work depends. With new technology comes new growth for the platform.

AIX 7.3 continues a 35-year tradition of innovation with enhanced capabilities that deliver resiliency, security, and scale that is needed to get your IT environment hybrid cloud ready.

AIX 7.2 and later versions include the following important features:

- Live Update

  AIX offers some unique features, such as AIX Live Kernel Update, which was introduced with AIX 7.2 to allow for general application and activation of any interim fix without a required restart. Subsequent AIX 7.2 technology level (TL) updates added support to also live update the AIX kernel with service packs and new TLs, again without the requirement to restart to activate the changes.

  Enhancements continue with AIX live update to support new use cases so that customers can broadly apply and use them. These enhancements includes recent enhancements to support live update in PowerVC managed landscapes and to automate the use of Power Enterprise Pools for CPU and memory resource management. Recently, we enabled customers to use Live Partition Mobility (LPM) to live update across frames or bring down the overall resources that are needed if LPM is not an option.

- AIX Toolbox for Open Source

  The AIX Toolbox for Open Source software is an IBM provided download site that contains a collection of Open Source software packages that are built for AIX. This software provides commonly used utilities and functions that can used for managing and operating AIX landscapes.

  It helps make AIX more compatible with other non-AIX environments that customers might be operating. The toolbox also provides open compilers, scripting languages, and libraries that can be used by ISVs or clients to develop solutions. Toolbox content is informally supported through an IBM Community-based forum.

IBM makes all reasonable efforts to provide toolbox package updates to address critical security vulnerabilities that are based on availability of resolutions from the open community.

The AIX Toolbox for Linux Applications demonstrates the strong affinity between Linux and AIX operating system. It provides important prerequisite technologies, such as Python and YUM, for solutions, such as Red Hat Ansible Automation. Packages can now be downloaded directly from AIX by using the **`dnf`** command.

- Scalability and continuous computing

  AIX offers enhanced performance for dynamic compute or memory management. It is designed for increased levels of compute and larger data storage capacities.

  JFS2 now supports up to 128 TB file system sizes and file sizes and scales up to 4 PB.

  For more information about current JFS2 size limits, see this IBM Documentation web page.

- FC-NVMe

  AIX introduced support for internal direct-attached nonvolatile memory express (NVMe) devices in version AIX 7.2 TL3, which provides access to the latest storage technology to significantly accelerate access to critical data. The trend around evolving NVMe storage continued as support was extended to more U.2 and PCIe add-in card storage options on the POWER9 platform, including up to 14 6.4 TB PCIe Gen4 internal NVMe devices on the most recent S924 platform.

  AIX is now also considering more options with support for Fibre Channel NVMe (FC-NVMe) in version AIX 7.2 TL5 and AIX 7.3. A traditional storage area network (SAN) infrastructure can now be used to connect AIX systems to some of the latest SAN-based storage systems that are running new FC-NVMe protocols.

- Artificial intelligence

  AIX workloads are a natural source for AI because these systems host a tremendous amount of high-quality data about customer behavior and transactional information that can be further use for AI.

  When customers combine historical data with emerging technologies, such as machine and deep learning all on the same platform and by using all types of sources and trained systems, they gain new insights. This AI is core to our mission as an IT provider for enterprise businesses and true investment protection.

- Hybrid cloud integration

  AIX is helping thousands of customers transform their IT infrastructure into a private, on-premises cloud with PowerVC. In 2022, we announced new hybrid cloud functions, including the ability to easily import and export AIX VMs between clouds, and new software-defined infrastructure capabilities with which you can spin up SAN-less clouds for DevOps environments.

  AIX is available on POWER9 and Power10 in IBM Cloud® through IBM Power Systems Virtual Server. AIX customers always counted on to support mission-critical databases, and they can now use greater workload scalability, better cloud automation with Ansible, enhanced security, and flexible licensing models. They can also run AIX workloads in hybrid or public cloud without having to refactor or rewrite them.

IBM embarked on hybrid on-premises to IBM Cloud integration in terms of production, nonproduction, and Disaster Recovery (DR) use cases. Sign-up for a Lite account to start building your applications and exploring services with select free Lite plans in the IBM Cloud console with the IBM Cloud free tier.

- Security enhancements

  The IBM Power Systems security portfolio improved as well with significant enhancements to PowerSC with the primary focus being AIX providing new malware intrusion detection and alerting capabilities, integration with IBM Cloud PowerVC Manager, reporting capabilities to support security audits, and more. IBM also released PowerSC Multi-Factor Authentication (PowerSC MFA) that provides the highest level of capability around the emerging requirement for two or more authentication factors for system administrators to meet mandatory regulations.

- Disaster and recovery protections

  Data center and service availability are some of the most important topics for IT infrastructure. Natural disasters not only affect normal operations, but human errors and terrorist acts can affect business continuity. Even with a fully redundant infrastructure, services are vulnerable to such disasters. Data Replication between sites is a good way to minimize business disruption because backup restores can take too long to meet business requirements, or equipment might be damaged depending on the extent of the disaster and therefore not available for restoring data.

  High availability (HA) software is intended to minimize downtime of services by automating recovery actions when failures are detected on the various elements of the infrastructure.

  PowerHA® for AIX is the premier HA/DR solution with years of continuous enhancements. It is the solution of choice for mission-critical operations in which all outage types (planned and unplanned) are covered.

  PowerHA minimizes planned and unplanned outage events, simplifies HA administration, provides multi-site solutions, and minimizes operating expenses. Lastly, Power HA and VM Recovery Manager provide solutions to address customer concerns regarding HA and DR on AIX.

1.2 AIX core and recent features

This section discusses the AIX features that were recently introduced. Enterprises need infrastructure that is secure, highly available, and adaptable to meet changing business demands. The AIX on Power Systems delivers these capabilities and more, with the performance, reliability, and security your mission-critical data requires.

For more information, see the following resources:

- IBM AIX Standard Edition
- *Data AIX: IBM AIX Modernizing businesses with AIX on IBM Power in the hybrid cloud era*

1.2.1 Logical Volume Manager and AIX Enhanced Journaled File System

This section discusses the Logical Volume Manager (LVM) and Enhanced Journaled File System.

Logical Volume Manager

The Logical Volume Manager is the base of the device framework where the data is being written. In many cases and as best practices, many customers choose to include IBM FlashSystem® storage as the preferred read LVM mirror on AIX, which provides enhanced I/O read performance and resiliency.

Setting the preferred read to a specific copy of a mirrored logical volume is done by running **mklv -R**, which sets the read preference to the copy of the logical volume. If the **-R** option is specified and the preferred copy is available, the read operation occurs from the preferred copy.

The **PreferredRead** variable can be set to a value 0 - 3. The default value is 0. To change the read preferences, run **chlv -R**, which changes the preferred read copy of the logical volume.

In AIX 7.2 and later, the LVM supports space reclamation for physical volumes (PVs) that can reclaim space. The following process is used:

1. LVM informs the disk driver, which informs the storage subsystem that the partition space is no longer in use and that the storage subsystem can reclaim the allocated space.
2. The disk driver helps LVM detect the space reclamation capability of the PV.
3. LVM and file system configuration commands, such as the **rmlv** command, **rmlvcopy** command, and the **chfs** (**shrink fs**) command start the space reclamation for the partitions after they are freed.
4. LVM detects the PV’s space reclamation capability when it opens the volume during the execution of the **varyonvg** or **extendvg** command.
5. LVM also attempts to detect it while the VG is online.
6. If the state change detection requires a PV to be reopened, the administrator must run the **varyoffvg** command and then, run the **varyonvg** command for the volume group.

Enhanced Journaled File System

The AIX Journaled File System is a hierarchical structure of files and directories. This type of structure resembles an inverted tree with the roots at the top and branches at the bottom. This file tree uses directories to organize data and programs into groups, which allows the management of several directories and files at once.

A file system is on a single logical volume. Every file and directory belongs to a file system within a logical volume. Because of its structure, some tasks are performed more efficiently on a file system than on each directory within the file system. For example, you can back up, move, or secure an entire file system. You can make a point-in-time image of a file system, which is called a *snapshot*.

JFS2 now supports up to 128 TB file system sizes and file sizes and is designed to scale up to 4 PB.

For more information about JFS capacities, see this IBM Documentation web page.

JFS2 also now includes a defragger option. If a file system is created with a fragment size smaller than 4 KB, it becomes necessary after a period to query the number of scattered unusable fragments. If many small fragments are scattered, it is difficult to find available contiguous space.

To recover these small, scattered spaces, use the **smitty dejfs2** command or the **defragfs** command. Some free space must be available for the defragmentation procedure to be used. The file system must be mounted for read/write.

The reclaim option in the Enhanced Journaled File System returns space to the disk to enact thin provisioning. Under a thin-provisioning scheme, space is not allocated until a write is issued by the host to the disk.

However, as a file system grows, more space is allocated, and even if files are deleted later, this space is not returned. In AIX 7.2 TL 03 and later, a new **chfs** command option is introduced to reclaim unused space in the file system. With this **chfs** command option, you can reclaim most of this space from the underlying disk, which allows it to be reused without shrinking the size of the file system.

The file system layer provides only a user command to run this option. The work of the reclamation is done by the LVM. This option is supported only on JFS2.

A following new attribute is available for the **chfs** command to reclaim unused space in JFS2 for the **-a** option without shrinking the file system:

```
chfs -a reclaim=[normal | fast]
```

1.2.2 AIX security

AIX includes several security features to secure your farm. The security for AIX falls in the categories that are described next.

Trusted execution

Trusted execution (TE) consists of a collection of features that are used to verify the integrity of the system and implement advanced security policies, which can be used together to enhance the trust level of the complete system. By using the TE mechanism, the system can be configured to check the integrity of the trusted object, such as a:

- Command
- Binary file
- Library
- Configuration file
- Shell script in a run time

The most common way for a malicious user to harm the system is to access the system and then install Trojans or rootkits, or tamper with some security-critical files, which results in the system becoming vulnerable and exploitable. The central idea behind the set of features under TE is the prevention of such activities (or in the worst case to identify whether any such incident occurred on the system).

For more information, see the following resources: This

- This IBM Support web page
- IBM Documentation: *Trusted Execution*
- IBM Documentation: *Security*

AIX File Permission Manager

File Permission Manager enables the hardening of an AIX system by disabling the **setuid** and **setgid** bits on many commands. This disabling is important because AIX has many *setuid* and **setgid** programs.

Usually, the **fpm** command removes the **setuid** permission's from commands and daemons that are owned by privileged users. However, it also can be used to address the specific needs of computer environments.

Before the introduction of the file permission manager, role-based access control (RBAC) were used to manage the issues of **setuid** and **setgid** programs. Now, **fpm** helps reduce the number of files, whether one uses RBAC. The **fpm** command is part of the **bos.rte.security** file set.

For more information, see the following resources:

- This IBM Support web page
- This IBM Documentation web page

AIX logical volume encryption

Logical volume (LV) encryption protects data exposure because of lost or stolen hard disk drives or because of inappropriately decommissioned computers. The base operating system performs LV data encryption and decryption during I/O operations. Applications that perform the I/O operations by using the file system interfaces or logical volume device interfaces can use the protected data without any modifications. LVM encryption also keeps data in flight protected

You must have the following file sets installed to encrypt the LV data. These file sets are included in the base operating system:

- `bos.hdcrypt`
- `bos.kmip_client`
- `bos.rte.lvm`
- `security.acf`
- `openssl.base`

You can manage all the LV encryption operations by using the **hdcryptmgr** command.

For more information, see the following resources:

- IBM Documentation: *Encrypted logical volumes*
- IBM Documentation: *hdcryptmgr Command*

IPsec enhancement

Filtering can be set up to be simple by using mostly auto-generated filter rules. It also can be customized by defining specific filter functions that are based on the properties of the IP packets.

Each line in a filter table is known as a *rule*. A collection of rules determine what packets are accepted in and out of the machine and how they are directed.

Matches to filter rules on incoming packets are done by comparing the source address and SPI value to those listed in the filter table. Therefore, this pair must be unique. Filter rules can control many aspects of communications, including source and destination addresses and masks, protocol, port number, direction, fragment control, source routing, tunnel, and interface type.

It includes the following recent enhancements:

- AIX IPsec support for IKEv2 liveness: Upon enabling this feature in the `/etc/isakmpd.conf` file, the IPsec initiator monitors the health of its peer. If a peer is abruptly down, the initiator expires Phase1 and Phase2 Security Associations.
- AIX IPsec supports the use of the same certificates at a specific endpoint to configure multiple IKEv2 tunnels when RSA signatures are used in Phase1 for IKEv2 protocol.
- AIX IPsec support for IKEv2 SA Idle Timeout support: Upon enabling this feature in the `/etc/iskampd.conf` file, IKEv2 stops the Phase2 SAs that are idle (no data traffic) for an SA idle timeout period.
- AIX IPsec support for IKEv2 retransmission control: Configuring a shorter time for retransmission of the IKEv2 negotiation packets is introduced through the **`RETRANSMISSION_ATTEMPT`** option in the **`/etc/isakmpd.conf`** file.
- AIX IPsec support for on-demand tunnels: Any outgoing packet or an only incoming IKE packet triggers the on-demand capability (if configured in the XML) on AIX and changes the tunnel states from `Dormant` to `Active`. However, on-demand tunnels are not triggered for an incoming non-IKE packet, starting with AIX 7.2 TL5.

For more information, see this IBM Documentation web page.

1.2.3 AIX Live Update

In AIX installation, several enhancements were made. including the live update and multiple alternative disk clones.

The AIX operating system includes a Live Update function, which eliminates the workload downtime that is associated with an AIX system restart that is required by AIX releases before Version 7.2 when fixes to the AIX kernel are deployed.

AIX Live Update enables the following functions:

- The workloads on the system continue running in a Live Update operation, which can use the interim fixes after the Live Update operation.
- AIX 7.2 Live Update aims to achieve zero downtime while updating operating system patches, service packs, and technology levels (TLs) without disrupting business-critical workloads.
- Live Update can save organizations on substantial costs and help them avoid a data breach while applying critical security patches, which might occur because a maintenance window was not completed on time.

For more information, see the following IBM Support web page.

In AIX 72 TL5, an enhanced scope and usability for the AIX Live Update function supports the following systems:

- Systems with IBM Spectrum® Protect LAN-free backup to N_Port ID Virtualization (NPIV)-connected tape devices
- Oracle Automatic Storage Management (ASM) that is configured on raw AIX logical volumes
- Veritas InfoScale 7.4.2 (VxDMP, VxVM, and VxFS)
- SAP applications with Live Update Planning Guide that is available

1.2.4 Multiple alternative disk clones

You can clone the AIX image running on `rootvg` to an alternative disk on the same system, install a user-defined software bundle and then, run a user-defined script to customize the AIX image on the alternative disk. Cloning the `rootvg` to an alternative disk has many advantages, including the following examples:

- An online backup us available if a disk fails. Keeping an online backup requires an extra disk or disks to be available on the system.
- When applying maintenance or TL updates, a copy of the `rootvg` is made to an alternative disk and then, updates are applied to that copy. The system runs uninterrupted during this time. When it is restarted, the system starts from the newly updated `rootvg` for testing. If the updates cause problems, the `old_rootvg` can be retrieved by resetting the boot list and then restarting.

For more information, see Managing multiple instances of altinstrootvg and applying fixes them.

1.2.5 I/O features and storage capabilities

IBM continues to enhance the Power/AIX platform with the introduction of support for Fibre Channel Non-Volatile Memory Express (FC-NVMe), which is used for bootable and nonbootable SAN storage volumes through 2 x 32 Gbps EN1A or EN1B Fibre Channel adapters.

This AIX feature enables customers to easily connect to traditional FC-SCSI SAN storage targets and new FC-NVMe SAN storage targets that might include dedicated or shared protocol Fibre Channel ports. For more information about supported configurations, see IBM System Storage Interoperation Center (SSIC).

AIX adds support for the following IBM Power Systems I/O features:

- PCIe4 Flash Adapter x8 (feature codes EN7A, EN7B, EN7C, EN7D, EN7E, and EN7F)
- PCIe3 2-Port 16 Gb FC Adapter (feature codes EN2A and EN2B)
- PCIe2 2-Port USB 3.0 Adapter (feature codes EC6K and EC6J)

AIX adds NVMe drives to the list of device types that support space reclamation for LV storage. When storage is freed through LV operations, such as the **rmlv** command, **rmlvcopy** command, or the **chfs** (shrink file system) command, corresponding blocks might be de-allocated on the NVMe drive. This reclaimation lowers random write latency and improves NVMe drive lifespan.

Enhancements to AIX Fibre Channel device drivers (including multi-pathing) for 16 Gbps and faster adapters allow AIX to receive and process SAN switch fabric congestion status, which provides better and faster pathing decisions.

AIX also supports a finer granularity for read and write timeout values of virtual storage. A single virtual SCSI adapter can include different types of virtual storage, such as physical volume, shared storage pool volume, or logical volume, with each type of virtual storage disk.

As an enhancement, multipath I/O (MPIO) features provide the ability for a device to be accessed through one or more storage paths. To use MPIO, the following main components are necessary:

- An MPIO-capable device driver that controls the target device
- A path control module (PCM) that provides path management functions

As of AIX 7.2 TL 3, the parallel SCSI, iSCSI, and FC disk device drivers and their device methods support MPIO disk devices.

1.2.6 Active memory expansion

Active memory expansion (AME) is a feature that is available on Power Systems servers. This feature can expand the amount of memory that is available to an AIX logical partition (LPAR) beyond the limits that are specified in the partition profile. AME compresses memory pages to provide more memory for a partition.

AIX is the only operating system that can use this feature. In-memory data compression is managed by the operating system, and this compression is transparent to applications and users.

Compression and decompression of memory content can provide memory expansion with percentages that can exceed 100%. So, a partition can accomplish significantly more work or support more users with the same amount of physical memory. Similarly, it can allow a server to run more partitions and perform more work for the same amount of physical memory.

AME uses the CPU resources that are allocated to the partition to compress and decompress the memory contents of the partition. AME provides a tradeoff of memory capacity for CPU cycles. The degree of compression varies and depends on how much the memory content can be compressed.

AME tends to have better results with workloads that access a smaller amount of memory. AIX features the **amepat** (AME Planning and Advisory Tool) command that can be used to estimate the compression rate for an individual workload.

When AME is enabled for an LPAR, the operating system compresses a portion of the LPAR's memory and leaves the remaining portion of memory decompressed and used to running processes access to code and data. AME results in memory effectively being broken up into a compressed pool and a decompressed pool. The AIX operating system dynamically varies the amount of memory that is compressed based on the current workload and the configuration of the LPAR.

When a process needs access to a memory page that is in the compressed pool, it causes a page interrupt and the AIX kernel decompresses the page and adds to the decompressed pool. Following this action, the process can continue to access the decompressed memory page as normal.

Meanwhile, the AIX kernel is compressing memory pages that remain unused for a time. This process balances the memory use of compressed and decompressed memory pools.

Because AME relies on memory compression, some extra CPU cycles are used when AME is used. The extra CPU cycles that are needed for AME is based on the workload and the required memory AME expansion factor. This factor is set on the HMC for each individual LPAR and can be dynamically changed.

Typical AME expansion factors are 1.5 - 2.5, but it varies by workload. A recommended expansion factor is available by running the AIX **amepat** command before you purchase AME, although many customers purchase it with their server.

For more information, see this IBM Support web page.

1.2.7 System modernization

AIX 7.2 TL5 is certified for the Open Group UNIX V7 Product Standard. This standard is granted to systems that conform to version 4 of the Single UNIX Specification. It is a significantly enhanced version of the UNIX 03 Product Standard

create_ova command

AIX added the **create_ova** command with AIX 7.2 TL5. This command creates an open virtual appliance (OVA) package. An OVA package is an archive file that can be deployed as a virtual machine.

The **create_ova** command is used to create a single-volume raw disk image and to export contents of a raw disk image to a compatible OVA package format. The OVA package can be imported into any IBM Power Virtualization Center (PowerVC) environment that contains a supported storage device.

You can also import the OVA package into any cloud service that supports the Open Virtualization Format (OVF) packaging standard. The imported OVA package can be deployed as a virtual machine.

Note: The OVA package can be used with Power Virtual Servers on the IBM cloud.

Cisco Discovery Protocol

AIX adds support for Cisco Discovery Protocol (CDP). This feature allows AIX systems that have physical network connections with supported Cisco switch products to query critical physical switch port information on-demand. This information includes layer1 and layer 2 information, switch capabilities, and protocol options. Support for the Cisco Discovery Protocol is managed by using the AIX **cdpctl** command.

Globalization enhancement

AIX adds enhancements to globalization enablement to support more national characters in different languages and locales. Consider the following points:

- AIX supports Unicode 12.1. This feature allows AIX **libc** APIs to support 137,928 characters for a total of 150 scripts.

- Common Locale Data Repository (CLDR) support: AIX rebuilt all 172 CLDR locales. This feature enables users to easily get the same locale environment on other platforms.
- AIX ships the latest ICU4C (open source) library. This feature allows AIX ISV and customers to easily port their non-AIX applications to AIX platforms.

AIX Ansible module content update

AIX started its AIX collection of module content in Ansible Galaxy. The first set of modules for the AIX collection were made available in June 2020. For more information about these modules, see Ansible's official hub for IBM AIX.

For subscribers to the Red Hat Automation Platform, the same modules are also available in the Ansible Automation Hub as fully supported content. For more information about Ansible and Power Systems, see the Ansible and IBM Power Systems web page.

1.3 IBM AIX 7.3 Standard Edition

The IBM AIX operating system is an open standards-based UNIX operating system that is the foundation of mission-critical workloads and databases for tens of thousands of customers for over 35 years. AIX provides an enterprise-class IT infrastructure that delivers the reliability, availability, performance, and security that is required for businesses to be successful in a global economy.

In today's era of hybrid cloud, an increased demand exists for flexible infrastructure, continuous availability, scalable and sustainable compute, enhanced security and data protection, and increased integration with open technologies. As businesses navigate these dynamic market conditions and IT infrastructure demands, they require an operating system that they can rely on that can be optimized to adapt to these changing business needs.

With the introduction of IBM AIX 7.3 Standard Edition, IBM addresses these needs while also continuing its tradition of providing new functions that can help dramatically improve system availability, scalability, performance, and flexibility while maintaining binary compatibility to ensure a quick and seamless transition to the new release.

Combined with IBM Power10, AIX 7.3 enables customers to modernize with a frictionless hybrid cloud experience to respond faster to business demands, protect data from core to cloud, and streamline insights and automation. AIX 7.3, coupled with IBM POWER8®, and later, technology-based systems, delivers a computing platform that is designed for hybrid cloud that is optimized, secure, and adapts to evolving business demands.

The following adapters are *not* supported in AIX 7.3:

- InfiniBand adapter feature 5283 and feature 5285 (PCIe2 dual-port 4X InfiniBand QDR adapter)
- CAPI adapter feature EJ17 and feature EJ18 (PCIe3 CAPI Fibre Channel (FC) Flash Accelerator adapters)

For more information, see the following resources:

- *AIX 7.3 release notes*
- IBM Documentation: *What's New in AIX 7.3*

1.3.1 Key requirements and features

IBM AIX Standard Edition includes the following key requirements and features:

- An IBM Power8, IBM Power9, IBM Power10 or later, technology-based server
- POWER8 Nutanix (CS821 and CS822) does not support AIX 7.3
- AIX support for vPMEM requires a POWER9 or later technology-based server

1.3.2 Respond faster to business demands

IBM AIX 7.3 is enhanced with the following features to better integrate into your enterprise:

- Adds python version 3.9.6. The new command to start python is **`/usr/bin/python3`**. The python that is shipped in AIX 7.3 works with Ansible solutions.
- Extends the scalability of AIX and supports a maximum of 240 cores (1920 hardware threads) in a single Power10 logical partition (LPAR).
- JFS2 file system size and file size limits are increased beyond 32 TB and 16 TB, respectively. For more information about supported limits, see the AIX 7.3 release notes.
- Supports the use of the on-chip NX GZIP accelerator in POWER9 and Power10 servers. The **`pigz`** (parallel **`gzip`**) open source command and the AIX zlibNX library are included in the AIX 7.3 default installation. The **`pigz`** command and the zlibNX library transparently use the NX GZIP compression accelerator.
- Provides up to twice the asynchronous I/O (AIO) on peripheral component interconnect express (PCIe) nonvolatile memory express (NVMe) scaling capabilities.
- The **`create_ova`** command now uses Power HW GZIP compression acceleration to speed up Open Virtualization Format Archive (OVA) creation and transfers on POWER9/Power10.
- TCP protocol stack now supports CUBIC congestion algorithm, which provides improved network performance in high-latency environments.
- Includes a new command (**`mksysb_iso`**) that is used to enable creating a single bootable ISO image that is larger than 4 GB.
- Adds bash version 5.1.4 that is ported from open source bash and provides similar functions. This shell is another shell that is supported on AIX, along with existing shells `ksh`, `ksh93`, `csh`, and `bsh`.

1.3.3 Maximize availability and reliability

AIX 7.3 Standard Edition is enhanced with the following availability and reliability updates:

- Reduces the amount of time that is required to dynamically add processor and memory resources to a running LPAR.
- Reduces initial program load (IPL) times for multiterabyte memory LPARs.
- Live kernel update supports the changing of select boot time parameters without requiring a restart.
- Adds support for virtual persistent memory (vPMEM), where each vPMEM device is configured as an hdisk. A vPMEM hdisk features better potential performance than local NVMe disks. The contents of a vPMEM HDisk are preserved on an LPAR restart if the server is not rebooted. These AIX vPMEM hdisks can be applied for the following uses:
  - Raw disk I/O access
  - Logical Volume Manager (LVM) and Journaled File System (JFS2) support

  - Paging device
  - Flash caching device
- Provides Geographical Logical Volume Manager (GLVM) enhancements, such as the following examples:
  - Support for freeze and resume of I/Os on secondary site. This support enables you to perform storage-based backup functions, such as disk snapshots.
  - Support of multiple network sessions to better handle large network latencies between sites.
- Adds the following Server Message Block (SMB) 3.0 features:
  - Case-insensitive file and directory name support.
  - Unicode UTF-8 support.
  - System management interface tool (SMIT) support and automating `/etc/filesystems` updates.
  - SMB 3.0.2 support for Live Kernel Update (LKU).

1.3.4 Protect data from core to cloud

AIX 7.3 Standard Edition protects data from the server to the cloud by using the following enhancements:

- Adds the following IP security (IPsec) enhancements:
  - IKE fragmentation with Internet Key Exchange version 2 (IKEv2)
  - Network Address Translation-Traversal (NAT-T) with IKEv2
- Provides enhanced support for logical volume (LV) encryption to include encryption for LV support in `rootvg` and dump device.
- Sendmail includes support for Simple Authentication and Security Layer (SASL).
- Trace facility use is now limited by default to the root user.
- Uses SHA256 as the new default password algorithm with support for up to 255-character passwords.
- Uses more secure default password policy.
- In support of creating stronger security policies, several AIX networking file sets, such as `bos.net.tcp.ftp` and `bos.net.tcp.telnet` are no longer installed by default.
- Includes support for the new PCIe3 Cryptographic Coprocessor Gen3 4769.
- OpenSSL 1.1.1j is available for download on the AIX web download web page.
- Includes AIX Network Install Manager (NIM), adding the NFSv4 option (`nfs_vers`) to provide a convenient way for accessing NIM resources. This feature enables users to specify the NFS protocol version that is required for customers to access the export location of a NIM resource during operation.
- Network Time Protocol (NTP) version 4 is included as a part of base AIX installation.

1.3.5 Streamline insights and automation

AIX 7.3 uses the following tools to help you use your data:

- AIX 7.3 provides the capability to use Matrix Math Accelerator (MMA) instructions through support of Power10 processor compatibility mode.
- IBM Open XL C/C++ for AIX is a standards-based high-performance compiler that facilitates the creation and maintenance of applications that are written in C and C++ for IBM Power solutions. It generates code that can use the capabilities of the latest Power10 architecture and optimize your hardware utilization. Several new built-in functions are delivered in this release to unlock Power10 architecture MMA instructions. For more information, see Software Announcement 221-321, dated 8 September 2021.
- IBM Engineering and Scientific Subroutine Library (ESSL) 7.1 on AIX 7.3 supports MMA AI Accelerator instructions for BLAS1, BLAS2, BLAS3, and several LAPACK routines. For more information, see Software Announcement 221-221, dated 8 September 2021.
- Several open source packages, such as numpy and OpenBLAS, were tested on AIX and can be used for AI use cases, which enables inferencing at the point of data. They can be found on the AIX Toolbox for Open Source.
- Applications on AIX can call out to Red Hat Enterprise Linux (RHEL) or Red Hat OpenShift “side-cars” to use MMA-accelerated AI capability for inferencing.
- RHEL or OpenShift side-cars or Enterprise AI can also use relational databases on AIX to feed models or store predictions from inferencing.
- IBM Lab Services offerings are available that provide capabilities to use Enterprise AI use cases on AIX 7.3. (For more information, consult your IBM representative or IBM Business Partner.)

1.3.6 Other enhancements

AIX 7.3 features the following other enhancements:

- ksh93u+2012-08-01 is fully supported and can be used for production.
- Updates libpcap to version 1.9.1.
- Improved globalization enablement to support more national characters in different languages and locales:
  - Ships the latest ICU4C (open source) library. This feature enables AIX independent software vendors (ISV) and customers to easily port their non-AIX applications to AIX platforms.
  - Supports Unicode 13.0. This feature enables AIX libc APIs to support 143,859 characters for a total of 154 scripts.
  - Rebuilt all 172 Common Locale Data Repository.

1.3.7 Recent AIX Toolbox for Open Source updates

The following new packages were added recently. Packages can be downloaded from the toolbox or can be installed directly through Dandified YUM (DNF):

- etcd
- fswatch
- ipmitool
- libevent
- libgit2
- libtomcrypt
- libtommath
- libuv
- mod_auth_gssapi
- mod_auth_kerb
- mosh
- python3-Cython
- python3-pycryptodomex
- rkhunter
- sudo_noldap
- swig
- tmux

The following packages were updated:

- ansible
- autoconf
- bash
- bind
- ca
- curl
- db
- expect
- file
- freetype2
- gcc8
- gdbm
- gdk
- ghostscript
- git
- glib2
- gnupg2
- gnutls
- golang
- gtk2
- httpd
- ImageMagick
- jansson
- krb5
- lapack
- lftp
- libgcrypt
- libgpg
- libpcap
- libtiff
- libunistring
- libxml2
- libXrender
- logrotate
- lua
- lynx
- m4
- make
- mariadb
- mc
- nagios
- ncftp
- nspr
- nss
- oniguruma
- openblas
- openldap
- p11
- pcre
- perl
- php
- postgresql
- python
- python3
- readline
- salt
- samba
- sed
- snappy
- sqlite
- squid
- sshpass
- subversion
- sudo
- tar
- tcl
- tcllib
- tcpdump
- tcping
- texinfo
- tk
- unixODBC
- wget
- zeromq

The introduction of new packages, updates to packages, and notifications of security updates are announced in the AIX Open Source discussion forum. There, users can also interact with the IBM open source team and with other users to post questions about packages.

For more information, see the following IBM Power Community web pages:

- IBM delivers enhanced capabilities with IBM AIX 7.3 Standard Edition
- AIX Open Source

2

Enterprise Cloud Edition

In this chapter, we discuss the Enterprise Cloud Edition for AIX.

This chapter includes the following topics:

2.1 IBM Power Systems Enterprise Cloud Edition 1.7

The following Enterprise Cloud Editions are available:

- IBM Power Systems Enterprise Cloud Edition 1.7.0 (5765-ECB)
- IBM Power Systems Enterprise Cloud Edition with AIX 7.2 1.7.0 (5765-CBA)

IBM Power Systems Enterprise Cloud Editions offer simplified purchasing models for IBM Power Systems software offerings that primarily provide value for customers that use IBM AIX *and* Linux on Power. The offerings enable more flexible licensing models in terms of the operating system in the era of cloud.

Bundled offerings help you facilitate hybrid cloud scenarios and provide an intuitive, web-based user interface that helps you simplify and accelerate managing your highly available and secure private clouds.

The bundled software components that are offered with IBM Power Systems are discussed next.

2.1.1 IBM Enterprise Cloud Editions 1.7

IBM Enterprise Cloud Editions 1.7 (5765-ECB) now offers the following bundled software components:

- IBM PowerVC for Private Cloud 2.0
- IBM PowerSC 2.0
- IBM VM Recovery Manager DR 1.6
- IBM Aspera® Endpoint 100 Mbps 1.0
- IBM Tivoli® Monitoring 6.3

2.1.2 IBM Enterprise Cloud Edition with AIX 7

IBM Enterprise Cloud Edition with AIX 7 (5765-CBA) now offers the following bundled software components:

- IBM AIX 7.3 or IBM AIX 7.2
- IBM PowerVC for Private Cloud 2.0
- IBM PowerSC 2.0
- IBM VM Recovery Manager DR 1.6
- IBM Aspera Endpoint 100 Mbps 1.0
- IBM Tivoli Monitoring 6.3

2.2 IBM private cloud and PowerVC

This section discusses the concept of a private cloud, where the private cloud is a cloud computing environment that is dedicated to a single customer. It combines many of the benefits of cloud computing with the security and control of an on-premises IT infrastructure.

2.2.1 Private cloud

Private cloud is also known as an *internal cloud* or *corporate cloud* because it is a cloud computing environment in which all hardware and software resources are dedicated exclusively to, and accessible only by, a single customer.

Private cloud combines many of the benefits of cloud computing, including elasticity, scalability, and ease of service delivery with the access control, security, and resource customization of on-premises infrastructure.

Many companies choose private cloud over public cloud (that is, computing services that are delivered over an infrastructure that is shared by multiple customers) because private cloud is an easier way (or the only way) to meet their regulatory compliance requirements.

Others choose private cloud because their workloads deal with confidential documents, intellectual property, personally identifiable information, medical records, financial data, or other sensitive data.

By building private cloud architecture according to cloud native principles, an organization gives itself the flexibility to easily move workloads to public cloud or run them within a hybrid cloud (mixed public and private cloud) environment whenever they are ready.

How it works

Private cloud is a single-tenant environment, meaning all resources are accessible to one customer only, which is referred to *isolated access*. Private clouds are typically hosted on-premises in the customer's data center. However, private clouds can also be hosted on an independent cloud provider's infrastructure or built on rented infrastructure that is housed in an off-site data center. Management models also vary: the customer can manage everything or outsource partial or full management to a service provider.

Private cloud architecture

Single-tenant design aside, private cloud is based on the same technology as other clouds; that is, technology that enables the customer to provision and configure virtual servers and computing resources on-demand to quickly and easily (or even automatically) scale in response to spikes in usage and traffic, to implement redundancy for high availability (HA), and to optimize utilization of resources overall.

This technology includes the following examples:

- Virtualization, which enables IT resources to be abstracted from their underlying physical hardware and pooled into unbounded resource pools of computing, storage, memory, and networking capacity that can then portioned among multiple virtual machines (VMs), containers, or other virtualized IT infrastructure elements. By removing the constraints of physical hardware, virtualization enables maximum use of hardware, allows hardware to be shared efficiently across multiple users and applications, and makes possible the scalability, agility, and elasticity of the cloud.

- Management software gives administrators centralized control over the infrastructure and applications running on it. This control makes it possible to optimize security, availability, and resource utilization in the private cloud environment.
- Automation speeds tasks, such as server provisioning and integrations that are otherwise must be performed manually and repeatedly. Automation reduces the need for human intervention, which makes self-service resource delivery possible.

Benefits of private cloud

Building a private cloud makes it possible for all enterprises, even those in highly regulated industries, to avail themselves of many of the benefits of cloud computing without sacrificing security, control, and customization.

Private cloud includes the following advantages:

- Full control over hardware and software choices
- Freedom to customize hardware and software
- Greater visibility into security and access control
- Fully enforced compliance with regulatory standards

For more information, see the following IBM Cloud web pages:

- Private cloud
- What is private cloud?
- How private clous works
- Private cloud architecture
- Benefits of private cloud

2.2.2 IBM PowerVC

IBM Power Virtualization Center (IBM PowerVC) is an advanced virtualization and cloud management offering for Power Systems servers that is based on OpenStack technology. This comprehensive virtualization and cloud management offering is simple to install and use, and enables virtual machine (VM) setup and management.

IBM PowerVC simplifies the management of the virtualization for Power servers that run on IBM AIX, IBM i, and Linux operating systems.

The offering builds private cloud capabilities on Power Systems servers and improves administrator productivity. It can integrate with cloud environments through higher-level cloud orchestrators.

IBM PowerVC Version 2.0 provides functional enhancements, such as cloning volumes and VMs, snapshots, and storage-related features, such as consistency groups and IBM Global Mirror support. Also available is IBM PowerVC for Private Cloud, which includes all of the functions of IBM PowerVC and more cloud-related features that are described in the following sections:

- 2.3, “PowerSC” on page 23
- 2.4, “VM Recovery Manager” on page 25
- 2.5, “Aspera” on page 27

IBM Cloud PowerVC Manager includes all the functions of the PowerVC Standard Edition with more features, including the following examples:

- A self-service portal that allows the provisioning of new VMs without direct system administrator intervention
- Cloud management policies that simplify management of cloud deployments
- Metering data that can be used for chargeback

IBM PowerVC Version 2.0, which is designed to simplify the management of virtual resources in IBM Power Systems environments, includes the following features and enhancements to its storage integration, usability, and performance capabilities:

- Simplified virtualization and cloud management
- New GUI with improved usability based on customer feedback
- SUSE Linux Enterprise Server (SLES) support for the PowerVC management server
- Red Hat Enterprise Linux (RHEL) 8 support with Python 3 compatibility
- Volume cloning for backup purpose
- VM cloning to simplify the redundant deployment of workloads
- Support for Global Mirror for IBM Spectrum Virtualize for enabling disaster recovery (DR) in support of the IBM FlashSystem® family
- New user interface features, such as a context-sensitive log display and the eye icon to make the password visible
- Improved scalability from 6,000 VMs to 10,000 VMs, and increased storage scalability from 10,000 volumes to 20,000 volumes
- Migration of volumes with retype support for volumes
- Multifactor authentication (MFA) support
- Virtual Persistent Memory support
- Easily replicate VMs for consistency and fast deployment
- Self-service provisioning of new workloads easily into cloud
- Automated configuration of I/O resources
- Policy-based workload placement simplifies administration
- Virtual image management including VM capture

For more information, see this IBM Power Systems data sheet.

2.2.3 IBM PowerVC editions

PowerVC is available in the following stand-alone offerings:

- Standard IBM PowerVC provides comprehensive virtualization management for Power servers that are running the PowerVM® hypervisor.
- IBM PowerVC for Private Cloud provides all the virtualization management features of PowerVC plus the private cloud capabilities, including the following examples:
  - A self-service portal
  - Role-based access
  - Single-click VM deployment
  - Resource quotas
  - Policy approvals

  - Metering

The IBM PowerVC features and benefits are listed in Table 2-1.

Table 2-1 PowerVC features and benefits

PowerVC features	PowerVC benefits
Dynamic Resource Optimizer (DRO)	Policy-based automation that actively balances workloads within a host group based on CPU or memory usage and balances workloads by moving them to a less busy server or moving capacity-on-demand (CoD) compute and memory resources to the workload.
Host grouping	Provides separate policy-based control for a subset of the total managed resource.
VM remote restart	Allows VMs to be automatically restarted on a new server after a server failure.
Affinity rules	Provides a mechanism to colocate VMs within a server or to separate VMs between servers.
Automated configuration for I/O	Simplifies and automates setup for mobility and highly available I/O configurations.
Virtual image management	Accelerates repeatable deployment of VMs.
Third party-supported OpenStack drivers	Accelerates management of third-party I/O devices.
One-click system evacuation	Simplifies system evacuation for maintenance.

For more information, see the following resources:

- *IBM PowerVC Version 2.0 Introduction and Configuration*, SG24-8477
- IBM PowerVC for Private Cloud 2.0.2
- Introduction to PowerVC for Private Cloud

2.3 PowerSC

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

PowerSC provides a security and compliance solution that is optimized for virtualized environments on Power Systems servers that are running AIX, Linux, and IBM i. PowerSC includes the following suite of features:

- Security and compliance automation
- Trusted boot, firewall, and logging
- Patch management and trusted network connect
- Multi-factor authentication
- Sophisticated allow List anti-malware and Intrusion Detection Service (IDS) monitoring

The editions, features that are included in the editions, components, and processor-based hardware on which each component is available are listed in Table 2-2.

Table 2-2 PowerSC components, description, and operating system and hardware support

Components	Description	Operating system supported
Security and Compliance Automation	Automates the setting, monitoring, and auditing of security and compliance configuration for the following standards: ▸ Payment Card Industry Data Security Standard (PCI DSS) ▸ Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT) ▸ U.S. Department of Defense (DoD) STIG ▸ Health Insurance Portability and Accountability Act (HIPAA) ▸ SAP compliance for AIX ▸ Center for Internet Security benchmarks compliance for AIX ▸ IBM i best practices	▸ AIX 5.3 ▸ AIX 6.1 ▸ AIX 7.1 ▸ AIX 7.2
Trusted Boot	Measures the boot image, operating system, and applications, and attests their trust by using the virtual trusted platform module (TPM) technology.	▸ AIX 6 with 6100-07, or later ▸ AIX 7 with 7100-01, or later
Trusted Firewall	Saves time and resources by enabling direct routing across specified virtual LANs (VLANs) that are controlled by the same Virtual I/O Server.	▸ AIX 6.1 ▸ AIX 7.1 ▸ AIX 7.2 ▸ VIOS Version 2.2.1.4, or later

Components	Description	Operating system supported
Trusted Logging	The logs of AIX are centrally located on the Virtual I/O Server (VIOS) in real time. This feature provides tamper proof logging and convenient log backup and management.	► AIX 5.3 ► AIX 6.1 ► AIX 7.1 ► AIX 7.2
Trusted Network Connect and Patch Management	Verifies that all AIX systems in the virtual environment are at the specified software and patch level and provides management tools to ensure that all AIX systems are at the specified software level. Provides alerts if a down-level virtual system is added to the network or if a security patch is issued that affects the systems.	► AIX 5.3 ► AIX 6.1 ► AIX 7.1 ► AIX 7.2
Trusted Network Connect Client	The Trusted Network Connect customer requires one of the components that are listed with the operating system.	► AIX 6.1 with 6100-06, or later ► AIX version 7.1 Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management ► AIX version 7.2.1 Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management
Allow List	You can configure File Access Policy Daemon (fapolicyd) for a specific Red Hat Enterprise Linux Server endpoint. fapolicyd is a user space daemon that determines access rights to files based on a trust database and file or process attributes.	Red Hat Enterprise Linux Server 8.3 or later
Intrusion Detection Service (IDS)	You can configure Port Scan Attack Detector (psad) for a specific Red Hat Enterprise Linux Server endpoint. psad makes use of iptables log messages to detect, alert, and (optionally) block port scans and other suspect traffic.	

Components	Description	Operating system supported
IBM PowerSC Multi-Factor Authentication	IBM PowerSC Multi-Factor Authentication is installed separately and provides alternative authentication mechanisms for systems. You can optionally use IBM PowerSC Multi-Factor Authentication to authenticate to the PowerSC GUI server.	► AIX 5.3 ► AIX 6.1 ► AIX 7.1 ► AIX 7.2

2.4 VM Recovery Manager

IBM VM Recovery Manager (VMR) for Power Systems is an economical HA/DR solution for AIX, IBM i, and Linux environments.

VMR is an active/inactive configuration in which the production VMs can be moved to a cold standby configuration by using LPM or a VM restart procedure. The active/inactive configuration means that software licenses are not required on the target system because the production applications and operating system are restarted onto the target system.

For more information, see *VM Recovery Manager for IBM Power Systems*.

2.4.1 AIX license transfers

You can use the Entitled Systems Support website to download Power software products when your software order is processed. The download site is enhanced to allow all Power software product licenses that are transferable to be transferred from a donor server to a target server.

Complete the following steps to transfer software:

1. Go to the Enterprise Storage Server website.
2. Log in by using your IBM ID.
3. Select your customer number and verify your authorizations that apply to the customer number. To verify that you have View ePoE authorization for your customer number, use View my authorizations on the left side of the menu.
4. If you have Transfer ePoE authorizations for your customer number, your license information is shown under Entitlements after you select the machine type serial number of your server.

To begin transferring your licenses, you first need to view them. Complete the following steps:

1. Select the donor and target machines.

   Both your donor and your target machine's inventory is available on one page. All permanent entitlements are visible even though they might not be transferable.

   A tool tip is available on each product that provides more information, such as SWMA status.

2. Select the entitlements for transfer.

   After you select the donor and the target machine, all entitlements are available for transfer can be checked. Entitlements that are nontransferable are unavailable.

   Select the entitlements that you want to transfer and click **Continue**. The ePoEs then appear in the target inventory, which includes a “NEW!” label.

3. Click **Confirm** at the bottom of the page to process the transfer.

   The entitlements are now available under the target machine.

If you do not have the necessary authorizations, you must register for your customer number. Complete the following steps:

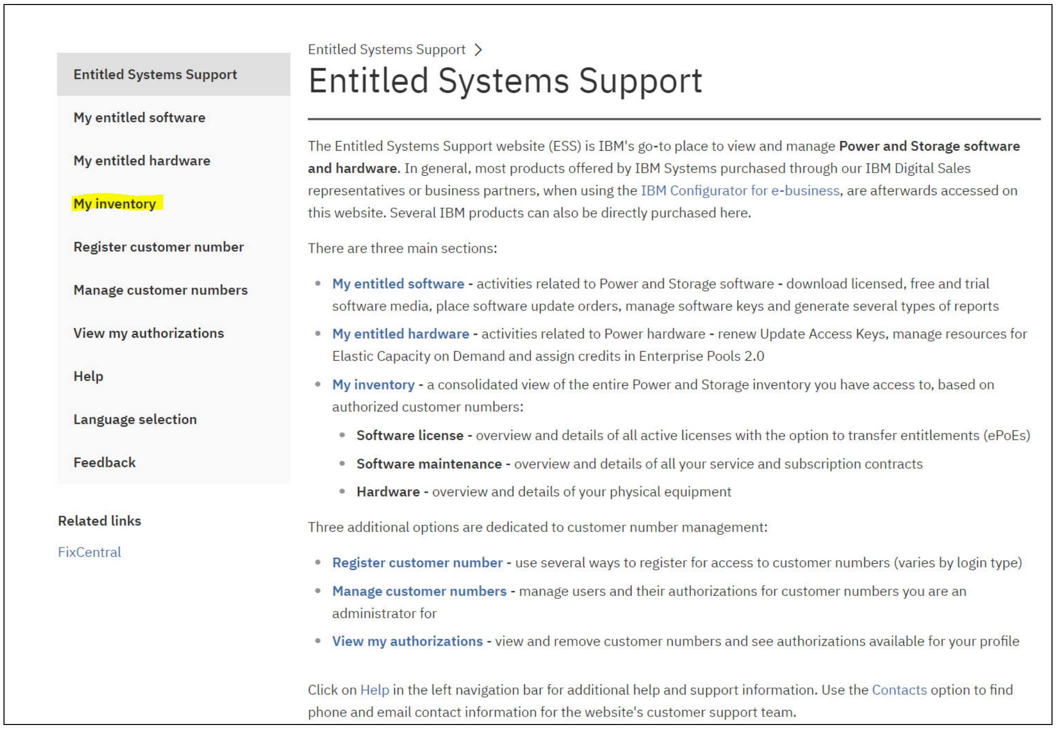
1. Go to Register IBM customer number, which is under the My Profile tab.
2. After entering your customer number, to get View and Transfer authorization for it, you must authenticate by using the order number, SWMA contract number, or system number. The use of the hardware serial number option grants access only to the software download.

   After you complete your registration, your license information is accessible under the Entitlements section.

To access an in-depth User’s Guide, complete the following steps:

1. Go to the Enterprise Storage Server website.
2. Click **Help** on the left side.
3. Download and open the *Enterprise Storage Server Registration IBM Customers Guidelines* PDF file.

Figure 2-1 shows the Entitled Systems Support window.



Entitled Systems Support

The Entitled Systems Support website (ESS) is IBM's go-to place to view and manage **Power and Storage software and hardware.** In general, most products offered by IBM Systems purchased through our IBM Digital Sales representatives or business partners, when using the IBM Configurator for e-business, are afterwards accessed on this website. Several IBM products can also be directly purchased here.

There are three main sections:

- **My entitled software** - activities related to Power and Storage software - download licensed, free and trial software media, place software update orders, manage software keys and generate several types of reports
- **My entitled hardware** - activities related to Power hardware - renew Update Access Keys, manage resources for Elastic Capacity on Demand and assign credits in Enterprise Pools 2.0
- **My inventory** - a consolidated view of the entire Power and Storage inventory you have access to, based on authorized customer numbers:
  - **Software license** - overview and details of all active licenses with the option to transfer entitlements (ePoEs)
  - **Software maintenance** - overview and details of all your service and subscription contracts
  - **Hardware** - overview and details of your physical equipment

Three additional options are dedicated to customer number management:

- **Register customer number** - use several ways to register for access to customer numbers (varies by login type)
- **Manage customer numbers** - manage users and their authorizations for customer numbers you are an administrator for
- **View my authorizations** - view and remove customer numbers and see authorizations available for your profile

Click on Help in the left navigation bar for additional help and support information. Use the Contacts option to find phone and email contact information for the website's customer support team.

Figure 2-1 Entitled Systems Support window

Note: Consider the following points:

- IBM charges for the transfer of software from the lower tier server to the higher tier server (such as small tier to medium tier) and transfers between similar tiers (such as small tier to small tier) are no charge. If your transfer is to a higher server tier, contact your IBM representative to process the upgrade order.
- On completion of your license transfer, be sure to contact your local TSS/CHIS representative to manually modify the existing service agreement.
- PowerVM software *cannot* be transferred between servers.

For more information, see this IBM Entitled Systems Support web page (login required).

2.5 Aspera

Power Systems Enterprise Cloud Edition with AIX includes Aspera High-Speed Transfer Endpoint 100 Mbps (1 Endpoint per server).

With shrinking timelines for digital production and the growing size of high-definition digital assets, organizations are looking for an integrated high-speed, secure, scalable, cost-effective data transfer and storage solution. This solution must ingest, distribute, and store any size and any number of files and data sets to enable collaboration over any distance in real time.

Aspera is a data transport and streaming technology company that provides high-speed data transfer services. Aspera belongs to the hybrid cloud business unit of IBM.

IBM Aspera helps businesses move critical data hundreds of times faster by using their IT infrastructure.

IBM Aspera takes a different approach to tackling the challenges of big data movement over global WANs. Rather than optimize or accelerate data transfer, Aspera eliminates underlying bottlenecks by using a breakthrough transport technology. It fully uses available network bandwidth to maximize speed and quickly scale up with no theoretical limit.

IBM Aspera Advanced Edition offers a simplified ordering option that enables customers to integrate all of the capabilities of the Aspera software stack by using a single part number. The offering is priced based on the number of virtual processor cores (VPCs) your server uses, which is the unit of measure by which the program can be licensed. This offering includes the following fast file transfer and streaming solutions that use Aspera’s patented high-speed transfer technology:

- Big data transport and synchronization

  Aspera helps to transfer, distribute, and synchronize huge files and data sets globally. IBM Aspera High-Speed Transfer Server enables high-speed transfers of files, directories, and large data sets by using desktop, mobile, and web applications.

  IBM Aspera Sync enables maximum speed replication and synchronization over WANs to handle today’s largest data.

- Large-file sharing

  Aspera accelerates collaboration with teams around the world on big data and large files.

- Transfer management

  Aspera helps to automate, monitor, and control data transfers and workflows. IBM Aspera High-Speed Transfer Endpoint starts and automates high-speed transfers with Aspera transfer servers from the desktop.

- Any bit-rate streaming

  Aspera helps to deliver data of any size and almost unlimited bit-rate video with near-zero latency. IBM Aspera Streaming provides highly efficient transfer of video streams or data feeds over commodity internet WANs as they are being created or captured.

- Hybrid cloud workflows

  Aspera helps to build highly scalable workflows that are running on-premises, in the cloud, or both. IBM Aspera Orchestrator enables customers to automate virtually any file-based workflow to seamlessly move data between any location, whether on premises or in public or private cloud platforms.

- Secure asset exchange

  Aspers uses blockchain technology to add security to digital asset movement. IBM Aspera Proxy Server protects customer organization networks while enabling secure, high-speed transfers for users within highly restrictive network environments.

2.6 IBM Tivoli Monitoring

IBM Tivoli Monitoring monitors and manages system and network applications on various operating systems, tracks the availability and performance of your enterprise system, and provides reports to track trends and troubleshoot problems.

IBM Tivoli Monitoring products monitor the performance and availability of distributed operating systems and applications. These products are based on a set of common service components, referred to collectively as *Tivoli Management Services*.

Tivoli Management Services components provide security, data transfer and storage, notification mechanisms, user interface presentation, and communication services in an agent-server-customer architecture. These services are shared by several other products, including:

- IBM Tivoli XE mainframe monitoring products
- IBM Tivoli Composite Application Manager products
- Other IBM Tivoli Monitoring products, including:
  - Applications
  - Cluster Managers
  - Databases
  - Energy Management
  - Messaging and Collaboration
  - Messaging and Collaboration
  - Virtual Environments

IBM Tivoli Monitoring monitors and manages system and network applications on various operating systems, tracks the availability and performance of your enterprise system, and provides reports to track trends and troubleshoot problems.

The following enhancements to the Tivoli Management Services components affect the system administrator for Version 6.3:

- Jazz® for Service Management

  Jazz for Service Management brings together the Open Services for Lifecycle Collaboration (OSLC) community's open specifications for linking data, shared administrative services, dashboard, and reporting services. Through these facets, Jazz for Service Management accelerates deployment, integration, and workflow automation across IBM, partner, and third-party tools.

  Jazz for Service Management is included with IBM Tivoli Monitoring. Jazz for Service Management includes several integration services, such as Administration, Registry, IBM Tivoli Common Reporting, Security, and IBM Dashboard Application Services Hub. These integration services provide key features including the following examples:

  - Shared data repository for products that are integrating through Jazz for Service Management
  - Consistent UI experience through Dashboard Application Services Hubin Jazz for Service Management
  - Simplified administration of products and solutions that are integrating through Jazz for Service Management
  - Ad hoc, self-service reporting through Tivoli Common Reporting in Jazz for Service Management

  For more information about Jazz for Service Management, see the Jazz for Service Management Information Center.

- IBM Tivoli Monitoring dashboard data provider for retrieving monitoring data for display in IBM Dashboard Application Services Hub dashboards

  The IBM Tivoli Monitoring dashboard data provider retrieves monitoring agent data for display in the IBM Dashboard Application Services Hub component of Jazz for Service Management. The dashboard data provider is optionally installed during the Tivoli Enterprise Portal Server configuration.

  With the dashboard data provider enabled, Dashboard Application Services Hub users can retrieve read-only data from the hub monitoring server and monitoring agent for display in dashboards that are provided by the agents or in custom dashboards.

  IBM Tivoli Monitoring V6.3 includes the Infrastructure Management Dashboards for Servers that display data for the operating system agents. These server dashboards use the dashboard data provider to retrieve data. A connection to the dashboard data provider must be configured in Dashboard Application Services Hub.

- IBM Infrastructure Management Dashboards for Servers running on the Dashboard Application Services Hub V3.1 or later

  With the IBM Tivoli Monitoring dashboard data provider enabled, Dashboard Application Services Hub users can retrieve managed system groups and events for all monitoring agents and Linux operating system agent, UNIX operating system agent, and Windows operating system agent health metrics by using the Infrastructure Management Dashboards for Servers application. This application is installed and configured into Dashboard Application Services Hub V3.1 or later by using IBM Installation Manager.

- Open Services Lifecycle Collaboration Performance Monitoring service provider

  The Tivoli Enterprise Monitoring Automation Server component contains the Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) service provider and is installed on the same systems as your hub Tivoli Enterprise Monitoring Server. The service provider registers monitoring resources with the Jazz for Service Management Registry Services component and supports integration with other products by using OSLC linked data interfaces.

- Role-based authorization policies

  The Tivoli Authorization Policy Server feature provides you with greater access control capabilities than possible with the Tivoli Enterprise Portal Server authorization model. You can protect your resources from unauthorized access by users of monitoring dashboards in the IBM Dashboard Application Services Hub.

  IBM Tivoli Monitoring V6.3 with the Authorization Policy Server feature enabled provides the following capabilities:

  - The ability to restrict access for dashboard users to specific managed system groups and to individual managed systems.
  - The ability to assign role-based policies to users and user groups in a federated LDAP user registry to simplify policy management.
  - A new command-line interface that is highly automatable.
  - Central management of authorization policies for multiple IBM Tivoli Monitoring environments, also called *domains*.

  To implement the feature, you must install IBM Installation Manager packages for the Tivoli Authorization Policy Server and the `tivcmd` CLI for Authorization Policy. The Authorization Policy Server is installed with your Dashboard Application Services Hub and the `tivcmd` CLI is installed on the computers that are used by the administrators who are creating authorization policies. After successful installation of these two packages, you can run various CLI commands as required to create roles, grant permissions, exclude permissions, and so on.

- OS Agents Report Prerequisites Scanner report

  The OS Agents Report Prerequisites Scanner report is delivered and installed through the operating system agent report package. It can be used to check that your system's IBM Tivoli Monitoring prerequisites are configured correctly to use Tivoli Common Reporting without errors.

- Creating and maintaining the dimension tables that are required for Tivoli Common Reporting using the Summarization and Pruning agent

  You no longer must periodically run the Tivoli Common Reporting and operating system agent scripts to maintain the IBM_TRAM schema and populate the MANAGEDSYSTEM table. You can configure the Summarization and Pruning agent to create, populate, and maintain the dimension tables.

- Tivoli Data Warehouse range partitioning

  Range partitioning is a database data organization feature that can significantly improve pruning and query performance in large Tivoli Data Warehouse databases. You can migrate your tables to a partitioned table to take advantage of the performance improvements that are provided with partitioned tables. Range partitioning allows the database to limit the scope of queries when the column that is part of the partitioning key is used in the WHERE clause.

- Take Action identity auditing

  You can now audit any commands that are run on a system at the agent level. The originator’s user ID and network information are securely transferred to the agent and then recorded in the agent’s audit log. The audit log can be historically collected. You can create situations and monitor centrally from the Tivoli Enterprise Portal.

- AAGP authorization controls

  The Access Authorization Group Profile (AAGP) authorization framework is now integrated with the Take Action identity auditing. The AAGP policies now selectively allow specific users to run take actions from Tivoli Enterprise Portal or by using **tacmd** run action to run commands by using the **tacmd** run command, or to create and modify situations and workflow policies that specify a take action command.

  The AAGP policy no longer requires the Central Configuration server to deliver the AAGP policy. The policy can be configured from the Agent Service Interface and stored locally on the agent.

- SOAP security enhancements

  You can now enable security for CT_EMail and CT_Export requests by using the SOAP_IS_SECURE environment variable on the monitoring server.

- Duper process optimization

  The duper process now supports situations that contain reflex actions or display items.

- Changes to default self-describing agent behavior and new **tacmd** commands

  You can now specify what products and versions are installed on your monitoring server and portal server by the automatic self-describing agent process.

- Updates for private situations

  IBM Tivoli Monitoring frequently requires text scan and pattern matching upon event and sample data, such as name, address, message, and log record. You can add the Regular Expression predicate filter to private situations to enhance agent monitoring event detection.

  You can now use the DELETE= attribute in a private situation to dynamically remove a private situation without recycling the agent or deleting the local private situation XML file.

- Ability to clear the Deployment Status table transactions

  Each time that you issue an IBM Tivoli Monitoring **tacmd** command or use the Tivoli Enterprise Portal navigator to remotely manage a Tivoli Enterprise Monitoring Agent, information about the transaction is preserved in the Tivoli Enterprise Monitoring Server Deployment Status table. To make it easier to manage the contents of this table (especially in large environments), you can schedule the periodic removal of completed transactions from the table.

- Use of login daemon scripts that are available on IBM Service Management Connect

  In IBM Tivoli Monitoring V6.3 or later, monitoring servers can now use the IBM Tivoli Monitoring login daemon solution that is available on IBM Service Management Connect to change the monitoring server to which an agent connects.

- Setting the locale for the browser customer

  Administrators can no longer set the locale for the Tivoli Enterprise Portal browser client Enterprise-wide. The language can be changed through the Java control window at the client computer if the underlying operating system platform was installed by using a different locale than the one you want to use with the Tivoli Enterprise Portal.

- Tivoli Integrated Portal name change

  The V3.1 release of Tivoli Integrated Portal is now referred to as the *Dashboard Application Services Hub*.

- i5/OS agent name change

  The i5/OS monitoring agent is now referred to as the *IBM i monitoring agent*.

2.6.1 Tivoli Management Services components

The following Tivoli Management Services components provide the infrastructure for your Tivoli Enterprise Monitoring Agents.

- Client

  The IBM Tivoli Monitoring client, Tivoli Enterprise Portal is a Java-based user interface for viewing and monitoring your enterprise network. Depending on how it was installed, you can start Tivoli Enterprise Portal as a desktop application or through your browser as a web application.

- Presentation server

  The Tivoli Enterprise Portal client connects to the Tivoli Enterprise Portal Server. The Tivoli Enterprise Portal Server is a collection of software services for the client that enables retrieval, manipulation, and analysis of data from the monitoring agents on your enterprise.

  The Tivoli Enterprise Portal Server also includes the optional dashboard data provider, which is used to retrieve read-only monitoring data for display in monitoring dashboards.

- Management server

  The Tivoli Enterprise Portal Server connects to the main (or hub) Tivoli Enterprise Monitoring Server. The monitoring server acts as a collection and control point for alerts that are received from the enterprise monitoring agents, and collects performance and availability data from them. The hub monitoring server correlates the monitoring data that is collected by monitoring agents and any remote monitoring servers. Then, it passes it to the portal server for presentation in the portal console.

  The automation server, Tivoli Enterprise Monitoring Automation Server, is an optional component that can be installed on the same system as the hub monitoring server. It extends the functions of the hub monitoring server. The automation server includes the Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) service provider.

- Dashboard server

  IBM Dashboard Application Services Hub is a Jazz for Service Management component that provides dashboard visualization and reporting services. Operators of the dashboard access it through a web browser interface. IBM Dashboard Application Services Hub uses the dashboard data provider component of the portal server to retrieve monitoring data.

  You can install the IBM Infrastructure Management Dashboards for Servers application into Dashboard Application Services Hub to display situation event information, managed system groups, and key health metrics for Windows operating system agents, Linux operating system agents, and UNIX operating system agents. You can also create custom dashboard pages that display monitoring data.

  You can also install the Authorization Policy Server and `tivcmd` CLI for Authorization Policy (`tivcmd CLI`) to use role-based authorization policies to control what monitored resources are displayed in dashboards.

- Help server

  The IBM User Interface Help System that is built on Eclipse is installed with the portal server. It provides presentation and search features for the integrated help system.

- `tacmd` Command-Line Interface (tacmd CLI)

  The `tacmd` CLI is used to manage your monitoring environment. IT also can be used to automate many of the administrative functions that are performed by using the Tivoli Enterprise Portal. The CLI commands send requests to the hub monitoring server or the portal server.

- Agents

  Tivoli Enterprise Monitoring Agents are installed on the systems or subsystems whose applications and resources you want to monitor. An agent collects monitoring data from the managed system and passes it to the monitoring server to which it is connected.

  The portal client and dashboard server gather the current values of the attributes and produces reports that are formatted into tables, charts, and relational table-based topology views.

  The agents and monitoring servers can also test the values of the current attributes against a threshold. When a threshold is exceeded or a value is matched, an alert icon can be displayed in the portal client or monitoring dashboard. Then, the hub monitoring server can forward an event to an event server, such as IBM Tivoli Netcool/OMNIbus. The attribute value conditions to test are called *situations*.

  Operating system agents can be installed outside the enterprise as Tivoli System Monitor Agents. They do not connect to nor have any reliance on the Tivoli Enterprise Monitoring Server. They can run private situations, which are independent of the monitoring server, save data samples for attribute groups as private history, and send SNMP alerts or EIF events to IBM Tivoli Netcool/OMNIbus.

- Data warehouse

  The Tivoli Data Warehouse is an optional component for storing historical data that is collected from agents in your environment. The data warehouse is on a supported database (such as DB2®, Oracle, or Microsoft SQL).

- Shared user registry

  A shared user registry is an LDAP server, such as Tivoli Directory Server or Microsoft Active Directory, that can be used to authenticate portal server users, IBM Dashboard Application Services Hub users, and other application users, such as Netcool/OMNIbus Web GUI users.

  When a shared user registry is used, users are authenticated by the first server that they access and authentication tokens are passed to the other servers so that the user is not required to reenter their credentials.

- Event synchronization

  The event synchronization component is optional. It is configured to send situation event updates that were forwarded to a IBM Tivoli Enterprise Console Event Server or a Netcool/OMNIbus ObjectServer back to the monitoring server.

2.6.2 IBM Tivoli Monitoring family of products

IBM Tivoli Monitoring products help you manage the performance and availability of distributed operating systems and applications. These products are based on a set of common service components, which are referred to collectively as *Tivoli Management Services*.

Tivoli Management Services provides security, data transfer and storage, notification mechanisms, user interface presentation, and communication services in an agent-server-client architecture. These services are common to many product suites, such as IBM Tivoli OMEGAMON® XE mainframe monitoring and IBM Tivoli Composite Application Manager.

3

AIX automation, availability, and security

In this chapter, AIX automation, AIX availability, and AIX security are discussed.

This chapter includes the following topics:

3.1 AIX automation

This section describes AIX automation by using various tools.

Infrastructure is an IT practice that manages an application's underlying IT infrastructure through programming. This approach to resource allocation allows developers to logically manage, monitor, and provision resources

AIX always can be integrated with automation tools, such as Terraform, Ansible, Chef, and Puppet for ease of patching, deployment, and performing tasks.

3.1.1 Terraform automation

Terraform allows users to define their entire infrastructure simply by using configuration files and version control. When a command is given to deploy and run a server, database, or load balancer, Terraform parses the code and translates it into an application programming interface (API) call to the resource provider. Because Terraform is open source, developers always can extend the tool's usefulness by writing plug-ins or compiling different versions of existing plug-ins.

Terraform feature the following important components:

- Terraform core

  Oversees the reading and interpolation of resource plan executions, resource graphs, state management features, and configuration files. Core is composed of compiled binaries that are written in the Go programming language. Each compiled binary acts as a command-line interface (CLI) for communicating with plug-ins through remote procedure calls (RPC).

- Terraform plug-in

  Responsible for defining resources for specific services, including authenticating infrastructure providers and initializing the libraries that are used to make API calls. Terraform plug-ins are written in Go as executable binaries that can be used as a specific service or a provisioner.

To deploy AIX by using the Terraform engine directly, you must obtain and install the Terraform CLI on a system with connectivity to your IBM PowerVC environment.

For more information about Terraform, see this website.

3.1.2 Ansible automation

Ansible is an open source, third-party tool that you can use for configuration management and automating repetitive tasks. Ansible is agent-less and performs actions on a set of servers from an Ansible control node. The Ansible engine must be installed on only the system that operates as the control node.

Ansible securely communicates with your AIX-based system by using the OpenSSH protocol. It can use password-based authentication or SSH key-based authentication.

With Ansible, you define the state of a system and allow Ansible to make changes to match the needed state; for example, ensuring that a specific file set is installed or an attribute of a specific AIX device is set to the needed value.

Ansible engine can be installed on AIX. It is available as part of the AIX Toolbox for Open Source.

IBM now supports the use of `dnf` to install open source packages from the AIX Toolbox for Open Source.

For more information, see this Ansible web page.

3.1.3 Chef automation

Chef is a configuration management tool that operates on a server/client model. Chef client agents are available for AIX 7.1 and AIX 7.2. By using Chef, you can turn your infrastructure into code and deploy environments in a testable and repeatable manner.

Chef can also be used for ongoing maintenance of your environment by running cookbooks periodically against your AIX systems to apply required changes on your environment, including tasks, such as patch management and security configuration.

The Chef client communicates with the Chef server securely by using the HTTPS protocol. The use of a pull model requires clients to authenticate with key-based authentication with the Chef server. Push jobs can also be started on Chef clients from the Chef server if required.

Along with many built-in resources that support AIX, Chef also has many community-contributed modules in the Chef supermarket. Regarding AIX, the open source community contributed many custom resources that can be used during Chef cookbook development to simplify your code and manage your AIX environment. These custom resources are available from the Chef Supermarket and can be used as part of your development efforts. Custom resources exist for most aspects of management for AIX.

For more information, see the following web pages:

- Chef Infra Overview
- Chef Supermarket: AIX Cookbook

3.1.4 Puppet automation

Puppet Enterprise is a configuration management tool and IT automation software that defines and enforces the state of your infrastructure throughout your software development cycle.

Puppet Enterprise is written in a declarative language in which you specify the needed state, and Puppet Enterprise performs the steps that are required to meet that state.

Puppet Enterprise operates on a client/server model, but you can also operate a client in stand-alone mode. Puppet Enterprise supports running the Puppet Enterprise agent on AIX 6L and AIX 7L.

For more information, see this website.

3.2 AIX availability

This section discusses the AIX availability option in terms of high availability (HA) within same site or in a Disaster Recovery (DR) site, with the options to migrate it online or offline.

3.2.1 Live Partition Mobility and Simplified Remote Restart

Live Partition Mobility (LPM) and Simplified Remote Restart (SRR) are essential capabilities for managing your server environment. In the normal course of maintaining your systems, you might need to move partitions because of hardware repairs, firmware updates, or VIOS updates.

LPM allows you to keep partitions running during such moves. It can also help with load balancing and energy conservation. If one of your servers unexpectedly goes down, SRR can help you move partitions within minutes of a crash, which helps you reduce downtime.

Live Partition Mobility

Partition mobility, a component of the PowerVM Enterprise Edition hardware feature, provides the ability to migrate AIX, IBM i, and Linux logical partitions from one system to another. The mobility process transfers the system environment that includes the processor state, memory, attached virtual devices, and connected users.

By using active partition migration, or LPM, you can migrate AIX, IBM i, and Linux logical partitions that are running (including the operating system and applications) from one system to another. The logical partition and the applications that are running on that migrated logical partition do not need to be shut down.

By using Inactive partition migration, or cold partition mobility, you can migrate a powered off AIX, IBM i, or Linux logical partition from one system to another. You can use the Hardware Management Console (HMC) to migrate an active or inactive logical partition from one server to another.

Because the HMC always migrates the last activated profile, an inactive logical partition that was activated cannot be migrated. For inactive partition mobility, you can select the partition state that is defined in the hypervisor, or select the configuration data that is defined in the last activated profile on the source server.

For more information, see the following web pages:

- IBM Documentation: Partition mobility
- IBM Support: Live Partition Mobility

Simplified Remote Restart

When a server encounters an unexpected hardware outage, the partitions on that server also crash and you must wait to take an action and repair the server.

SRR uses many of the basic underlying principles of LPM so that it can rebuild the LPAR on another system.

This ability allows you to move and restart an LPAR within minutes after a Power System server crashes. Because the server crashed, a live mobility cannot be done to move the LPAR. This feature was part of POWER8 servers and later models, including support for IBM AIX and IBM i.

Enabling SRR and running a real SRR to another Power Server from HMC CLI is shown in Example 3-1.

Example 3-1 Enable SRR and run SRR to another Power Server

```
$ for i in ` lssyscfg -r lpar -m S1-MANAGED_SYSTEM -F name | grep -iv vios`
do
chsyscfg -r lpar -m S1-MANAGED_SYSTEM -i
"name=$i,simplified_remote_restart_capable=1"
done

$ rrstartlpar -o validate -m 1-MANAGED_SYSTEM_1 -t S1-MANAGED_SYSTEM_2 -p LPAR1
$ rrstartlpar -o restart -m 1-MANAGED_SYSTEM_1 -t S1-MANAGED_SYSTEM_2 -p LPAR1
```

For more information, see the following web pages:

- IBM Documentation: Remote restart states
- IBM Documentation: Validating the simplified remote restart logical partition
- IBM Documentation: Enabling or disabling the simplified remote restart capability
- IBM Support: Simplified Remote Restart via HMC or PowerVC

3.2.2 AIX high availability solutions

This section presents HA and DR solutions in IBM Power Systems environments. These typical solutions are used to provide HA and DR capabilities for LPARs that are running AIX.

PowerHA

IBM PowerHA SystemMirror® for AIX (previously known as *HACMP* and now referred to as *PowerHA*) is the Power Systems data HA solution for applications that are running on AIX LPARs.

It monitors, detects, and reacts to an extensive list of events that might affect application availability. PowerHA relies on services that are provided by Reliable Scalable Cluster Technology (RSCT) and Cluster Aware AIX (CAA).

RSCT is a set of low-level operating system components that allow the implementation of clustering technologies. CAA is an AIX feature that was introduced in AIX 6.1 TL6 and AIX 7.1.

PowerHA editions

PowerHA SystemMirror for AIX can be distributed in Standard Edition or Enterprise Edition.

Standard Edition provides local clustering capabilities. Typically, all cluster nodes share a common storage infrastructure and can see the same storage.

Enterprise Edition provides local and remote replication functions. In this case, cluster nodes are in different data centers that are separated by significant distances and integrate with storage level replication services such as Copy Services or IP Replication.

For more information, see this IBM PowerHA web page.

Recent PowerHA features

PowerHA SystemMirror V7.2 supports the latest AIX and PowerVM enhancements, such as the following examples:

- CAA
- AIX Live Update
- PEP
- LPM
- Logical Volume Manager (LVM) rootvg failure monitoring

For more information about PowerHA SystemMirror 7.2, see *IBM PowerHA SystemMirror V7.2.3 for IBM AIX and V7.22 for Linux*, SG24-8434.

IBM VM Recovery Manager for Power Systems

IBM VM Recovery Manager for Power Systems is an enterprise-grade availability solution that provides automated recovery for virtual machines (VMs) that are running on Power Systems servers. VMs on Power Systems are referred to as LPARs.

IBM VM Recovery Manager is a VM-level technology. On Power Systems servers, VMs are treated as containers that can host various systems. Therefore, IBM VM Recovery Manager is an operating system-neutral solution.

Because IBM VM Recovery Manager does not have any operating system or middleware dependencies, it can be used to deploy uniform HA/DR solutions in heterogeneous environments that might include AIX, IBM i, and all Linux distributions that are supported by Power Systems servers.

See more information, see the following web pages:

- IBM VM Recovery Manager for IBM Power Systems
- System Software Solution Brief: *VM Recovery Manager for IBM Power Systems*

IBM VM Recovery Manager versions

IBM VM Recovery Manager is available in the following versions:

- VM Recovery Manager HA (VMR HA)
- VM Recovery Manager DR (VMR DR), formerly known as *Geographically Dispersed Resiliency (GDR)*

VM Recovery Manager HA

With VMR HA, you can move VMs between different Power Systems servers by using LPM for planned outages or VM restart for unexpected outages. VMR HA solutions can be deployed in environments where Power Systems servers are in the same site and can access the same network and storage devices.

During a failover, VMs on a Power Systems server are moved by LPM or restarted on a different Power Systems server. VMR HA is an availability solution that can be used in Power Systems environments where PowerHA is not used.

For more information, see the IBM Documentation web page.

VM Recovery Manager DR

Unlike VMR HA, VM Recovery DR (VMR DR) is a DR solution that provides automated recovery for VMs running on Power Systems servers that are at different sites and can access different storage devices. The distance between primary and DR sites can be several to thousands of kilometers. VMR DR relies on an out-of-band monitoring and management component and consistently uses storage replication technologies.

During the failover from the primary site to the secondary site, VMR DR orchestrates the shutdown of the VMs on the primary site, manages storage-level replication between the two sites to preserve data consistency, and starts VMs at the secondary site.

For more information, see this IBM Documentation web page.

3.3 AIX security features

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.

3.3.1 Securing the base operating system

Securing the base operating system provides information about how to protect the system, regardless of network connectivity. The following base operating system components enhance security:

- Secure system installation and configuration
- Users, groups, and passwords
- Role-based access control
- Access Control Lists
- Auditing
- Lightweight Directory Access Protocol
- Encrypted File System (EFS)
- Public Key Cryptography Standards #11
- Pluggable Authentication Modules
- OpenSSH and Kerberos Version 5 support
- Encrypted logical volumes

3.3.2 Securing the network

This section describes how to install and configure IP security and identify necessary and unnecessary network services, and auditing and monitoring network security. The following components assist you in securing the network:

- 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

3.3.3 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` fileset. AIX Security Expert provides simple menu settings for high-, medium-, and low-level security.

AIX standard security settings 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 a large number of papers about security hardening and then, individually implementing each security element.

AIX Security Expert settings

The following coarse-grain security settings are available:

- High-level
- Medium-level
- Low-level
- Advanced
- AIX standard
- Undo
- Check

3.3.4 Security checklist

The following checklist of security actions can be used to track what is performed on a newly installed or existing system. Although this list is not a complete security checklist, it can be used as a foundation to build a security checklist for your environment:

- When installing a new system, install AIX from secure base media. Perform the following procedures at installation time:

  > **Note:** Do not install desktop software, such as CDE, GNOME, or KDE on servers.

  - Install the required security fixes and any recommended maintenance and technology level fixes. For more information about for the newest service bulletins, security advisories, and fixes, see the IBM Support Fix Central web page.
  - Back up the system after the initial installation and store the system backup in a secure location.
- Establish access control lists for restricted files and directories.
- Disable unnecessary user accounts and system accounts, such as daemon, bin, sys, adm, lp, and uucp. Deleting accounts is *not* recommended because it deletes account information, such as user IDs and usernames, which might still be associated with data on system backups. If a user is created with a previously deleted user ID and the system backup is restored on the system, the new user might have unexpected access to the restored system.
- Regularly review the `/etc/inetd.conf`, `/etc/inittab`, `/etc/rc.nfs`, and `/etc/rc.tcpip` files and remove all unnecessary daemons and services.

- Verify that the permissions for the following files are set correctly:
  - `-rw-rw-r-- root system /etc/filesystems`
  - `-rw-rw-r-- root system /etc/hosts`
  - `-rw------- root system /etc/inittab`
  - `-rw-r--r-- root system /etc/vfs`
  - `-rw-r--r-- root system /etc/security/failedlogin`
  - `-rw-rw---- root audit /etc/security/audit/hosts`
- Disable the root account from being able to remotely log in. The root account logs in from the system console only.
- Enable system auditing.
- Enable a login control policy.
- Disable user permissions to run the **`xhost`** command.
- Prevent unauthorized changes to the PATH environment variable.
- Disable telnet, rlogin, and rsh.
- Establish user account controls.
- Enforce a strict password policy.
- Establish disk quotas for user accounts.
- Allow only administrative accounts to use the **`su`** command. Monitor the **`su`** command's logs in the `/var/adm/sulog` file.
- Enable screen locking when X-Windows is used.
- Restrict access to the **`cron`** and **`at`** commands to only the accounts that need access to them.
- Use an alias for the **`ls`** command to show hidden files and characters in a file name.
- Use an alias for the **`rm`** command to avoid accidentally deleting files from the system.
- Disable unnecessary network services.
- Perform frequent system backups and verify the integrity of backups.
- Subscribe to security-related email distribution lists.

3.3.5 Summary of common AIX system services

Common system services are available within AIX. For more information, see this IBM Documentation web page.

3.3.6 Summary of network service options

To achieve a higher level of system security, several network options can be changed by using `0` to disable and `1` to enable. For more information, see this IBM Documentation web page.

3.3.7 Security model changes in AIX 7.3

Starting with AIX 7.3, the following security models are not available (they were removed from the operating system installation menus and the `bosinst.data` templates):

- Trusted AIX
- Trusted AIX LAS/EAL4+ Configuration Install
- BAS and EAL4+ Configuration Install

For more information, see this IBM Documentation web page.

3.3.8 4765 PCIe Cryptographic Coprocessor AIX CCA Support Program Installation 4.4 and 4767 Program Installation 5.3

The IBM® Common Cryptographic Architecture (CCA) Support Program consists of several components, including:

- Device drivers and an operating system for the PCIe cryptographic coprocessor hardware
- Support for the IBM CCA application program interface (API)
- A function-control vector (FCV)
- Utility applications where the coprocessor must be installed that runs on the host machine

For more information about 4765 PCIe Cryptographic Coprocessor AIX CCA Support Program Installation 4.4, see this BM Documentation web page.

For more information about 4767 4765 PCIe Cryptographic Coprocessor AIX CCA Support Program Installation 5.3, see this IBM Documentation web page.

3.4 PowerSC Multi-Factor Authentication

This section describes the PowerSC Multi-Factor Authentication concept and requirements.

IBM PowerSC Multi-Factor Authentication (PowerSC MFA) provides alternative authentication mechanisms for systems. You can use IBM PowerSC MFA with various applications that use pluggable authentication modules (PAM) for authentication.

Note: Since PowerSC 2.0, the PowerSC MFA product was included in the PowerSC offering as a single product. For more information, see this web page.

The most common method for authenticating users to AIX applications is by using passwords. Unfortunately, passwords can present a relatively simple point of attack for exploitation.

For systems that rely on passwords to be secure, the system administrator must enforce password controls and provide user education. Users tend to pick common passwords, write down passwords, and unintentionally install malware that can log passwords. Additionally, building a powerful, dedicated password-cracking computer system is trivial and low cost.

IBM PowerSC MFA provides a method that is used to raise the assurance level of systems by requiring extra authentication factors for users. IBM PowerSC MFA relies on multiple authentication factors.

3.4.1 Authentication factors

Multi-factor authentication is a method of computer access control in which a user is granted access only after successfully providing several authentication factors to an authentication mechanism. The authentication factors are typically from at least two of the following categories:

- Knowledge (something they know)

  For example, a password, passphrase, confirmation number, or personal identification number.

- Possession (something they have)

  For example, a badge, picture, QR code, access card, identity card, key, or a cryptographic token.

- Inheritance (something they are)

  For example, a fingerprint, retina scan, or other biometric data, such as data that is stored on chips that are on a biometric passport.

3.4.2 Authentication methods

Multiple authentication factors improve the security of user accounts. Users provide the credentials directly in the application (in-band) or out-of band:

- For in-band authentication, users can generate a token to satisfy a policy and use that token to directly log in.
- Out-of-band authentication allows users to authenticate on a user-specific web page with one or more authentication methods to retrieve a cache token credential (CTC) that they then use to log in.

For more information, see the following IBM Documentation web pages:

- IBM PowerSC MFA concepts
- IBM PowerSC MFA Server requirements
- RSA Authentication Manager concepts

4

Cloud solutions

In this chapter, we discuss cloud solutions that use AIX. This chapter includes the following topics:

- “IBM public cloud and PowerVS” on page 48
- “Cloud architect diagram for cloud environments” on page 52
- “AIX migration to cloud” on page 54
- “Power Enterprise Pools” on page 56
- “IBM Cloud Management Console” on page 58

4.1 IBM public cloud and PowerVS

This section discusses various cloud solutions that use PowerVS.

4.1.1 Public cloud

The rise and adoption of public cloud services is one of the most important shifts in the history of enterprise computing. A public cloud is a type of cloud computing in which a third-party service provider makes computing resources (which can include anything from ready-to-use software applications, to individual virtual machines [VMs] to complete enterprise-grade infrastructures and development platforms) available to users over the internet. These resources might be accessible for free, or access might be sold according to subscription-based or pay-per-usage pricing models.

The public cloud provider owns and administers the data centers where customers' workloads run. Service providers assume responsibility for all hardware and infrastructure maintenance. They also provide high-bandwidth network connectivity to ensure rapid access to applications and data.

The cloud provider also manages the underlying virtualization software. In its simplest form, the public cloud model is the computing version of the "utility" model that is used when electricity or water is used in homes.

Public cloud architectures are multi-tenant environments; that is, users share a pool of virtual resources that are automatically provisioned for and allocated to individual tenants through a self-service interface. Therefore, multiple tenants' workloads might be running CPU instances that are running on shared physical server at the same time. Each cloud tenant's data is logically isolated from that of other tenants.

Many enterprises are moving portions of their computing infrastructure to the public cloud because public cloud services are elastic and readily scalable, flexibly adjusting to meet changing workload demands. Others are attracted by the promise of greater efficiency and fewer wasted resources because customers pay only for what they use. Still others seek to reduce spending on hardware and on-premises infrastructures.

4.1.2 IBM public cloud

IBM Cloud supports over 1,000 enterprise clients, providing them with access to the industry's leading security infrastructure, which includes built-in workload isolation and network segmentation along with continuous container security and end-to-end data encryption.

The IBM public cloud was built on an open source software foundation. IBM Cloud employees are major longtime contributors to key cloud native and open source projects, including Kubernetes, Istio, and Knative. The strength of IBM's commitment to the open source system provides its cloud customers with flexible developer tools and access to resources without vendor lock-in.

Working with Red Hat, IBM Cloud introduced a managed Red Hat OpenShift environment on the IBM public cloud that quickly became the number-one open source solution for customers who want to simplify the management of their container-based architectures and speed development pipelines.

IBM also provides continuous edge-to-cloud support for hybrid workloads, whether they are VMware-based, built to run on bare metal servers, or cloud native. IBM Cloud incorporates robust data protection and visibility features to protect information throughout the whole of its lifecycle, no matter where it is stored.

Built with Red Hat OpenShift, IBM Cloud Satellite™ addresses how building, deploying, and managing applications across multiple cloud environments can degrade application performance. Satellite offers a fully managed set of core application services that run across cloud environments, including IBM Cloud, on-premises, and edge. You operate development processes, methods, and tools in a single and consistent way across all types of cloud environments, including the environments of other public cloud vendors.

4.1.3 PowerVS

IBM Power Systems Virtual Server is a Power Systems offering. Power Systems Virtual Servers are in the IBM data centers, 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 a logical partition (LPAR), in a matter of minutes.

IBM Power Systems customers who typically relied upon on-premises-only infrastructure can now quickly and economically extend their Power IT resources off-premises. Such customers avoid the large capital expense or added risk when migrating their essential workloads by using Power Systems Virtual Servers.

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 as the Power Systems Virtual Server architecture is identical to certified on-premises infrastructure.

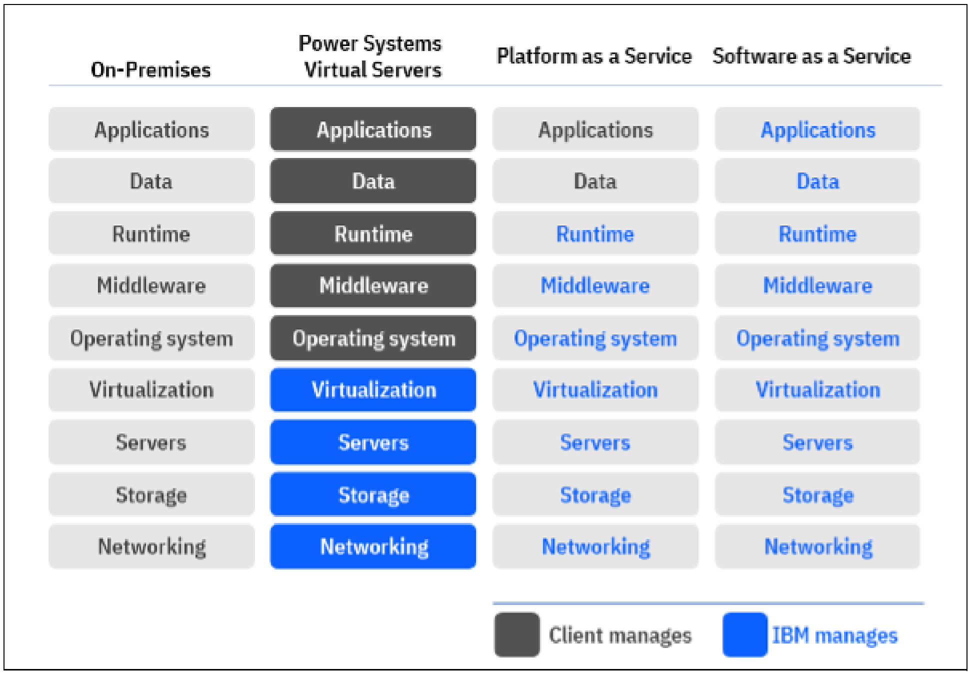
Power Systems Virtual Servers integrate your AIX, IBM i, or Linux capabilities in an off-premises environment that is distinct from the IBM Cloud. You get fast, self-service provisioning, and flexible management on-premises and off-prmises. Similar to on-premises, it can be connected to access a stack of enterprise services from IBM, all with pay-as-you-use billing with which you can easily scale up and out.

You also can quickly deploy a Power Systems Virtual Server to meet your specific business needs and easily control workload demands. The virtual servers run on IBM Power Systems hardware with the PowerVM hypervisor.

With the Power Systems Virtual Server service, you can quickly create and deploy one or more virtual servers that are running the AIX, IBM i, or Linux operating systems. After you provision the Power Systems Virtual Server, you get access to infrastructure and physical computing resources without the need to manage or operate them.

However, you must manage the operating system and the software applications and data.

Figure 4-1 shows a responsibility assignment (RACI) matrix for Power Systems Virtual Servers.



On-Premises	Power Systems Virtual Servers	Platform as a Service	Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating system	Operating system	Operating system	Operating system
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

⬛ Client manages 🟦 IBM manages

Figure 4-1 Power Systems Virtual Server responsibility assignment matrix

Key features

Some of the key features of the Power Systems Virtual Server service are described next.

Straightforward billing

The Power Systems Virtual Server service uses a monthly billing rate that includes the licenses for the AIX and IBM i operating systems. This rate is pro-rated by the hour based on the resources that are deployed to the Power Systems Virtual Server instance for the month.

When you create the Power Systems Virtual Server instance, you can see the total cost for your configuration based on the options that you specify. You can quickly identify what configuration options provide you with the best value for your business needs.

Infrastructure customization

You can configure and customize the following options when you create a Power Systems Virtual Server:

- Number of virtual server instances
- Number of cores
- Amount of memory
- Data volume size and type
- Network interfaces

Bring your own image

IBM provides you with stock AIX and IBM i images when you create a Power Systems Virtual Server. However, you can always bring your own custom AIX, IBM i, or Linux image that you tested and deployed.

Support for SAP NetWeaver or SAP HANA applications

When you provision a Power Systems Virtual Server instance to support SAP NetWeaver applications, select a version of the IBM-provided AIX or Linux stock operating system image.

When you provision a Power Systems Virtual Server instance to support the SAP HANA applications, select a version of the IBM provided Linux stock image. IBM i operating system and custom AIX and Linux images are not supported for SAP workloads.

Support for deploying a Red Hat OpenShift Cluster

When you provision a Red Hat OpenShift Cluster on Power Systems Virtual Server, it is easier to use the IBM provided automation to create the entire cluster of servers and install Red Hat OpenShift rather than individually provisioning Power Systems Virtual Server instances.

Hardware specifications

The following IBM Power Systems can host a Power Systems Virtual Server:

- IBM Power System E880 (9119-MHE); Dallas 13 only
- IBM Power System S922 (9009-22A)
- IBM Power System E980 (9080-M9S)

Storage tiers

For each Power Systems Virtual Server instance, you must select a storage tier (Tier 1 or Tier 3). The storage tiers in Power Systems Virtual Server are based on I/O operations per second (IOPS). It means that the performance of your storage volumes is limited to the maximum number of IOPS based on volume size and storage tier.

Although the exact numbers might change over time, the Tier 3 storage currently is set to 3 IOPS/GB; the Tier 1 storage is set to 10 IOPS/GB.

For example, a 100 GB Tier 3 storage volume can receive up to 300 IOPs, and a 100 GB Tier 1 storage volume can receive up to 1000 IOPS. After the IOPS limit is reached for the storage volume, the I/O latency increases.

Public and private networks

When you create a Power Systems Virtual Server, you can select a private or public network interface.

Public network

Consider the following points about public networks:

- Easy and quick method to connect to a Power Systems Virtual Server instance.
- IBM configures the network environment to enable a secure public network connection from the internet to the Power Systems Virtual Server instance.
- Connectivity is implemented by using an IBM Cloud Virtual Router Appliance (VRA) and a Direct Link Connect connection.
- Protected by a firewall and supports the following secure network protocols:
  - SSH
  - HTTPS
  - Ping
  - IBM i 5250 terminal emulation with SSL (port 992)

Private network

Consider the following points about private networks:

- Allows your Power Systems Virtual Server instance to access IBM Cloud resources, such as IBM Cloud Bare Metal Servers, Kubernetes containers, and Cloud Object Storage.
- Uses a Direct Link Connect connection to connect to your IBM Cloud account network and resources.
- Required for communication between different Power Systems Virtual Server instances.

For more information, see this IBM Documentation web page.

4.2 Cloud architect diagram for cloud environments

This section describes different cloud environments and their integration.

4.2.1 Cloud environment

The cloud environment can always be different from one customer to another; however, the cloud environment offers several important benefits:

- Rapid deployment, scalability, ease of use, and elasticity to adapt to demand
- Predictable cost, optimized for workload demand
- DevOps support, which increases developers productivity

Private cloud

A private cloud is an environment in which all hardware and software resources are dedicated exclusively to, and accessible only by, a single customer. Private cloud combines many of the benefits of cloud computing, including elasticity, scalability, and ease of service delivery with the access control, security, and resource customization of on-premises infrastructure.

For more information, see this IBM Cloud Learn Hub web page.

Private cloud adds the following assurances:

- Knowledge of where data is stored
- Apply own enterprise security and governance policies
- Simplify integration to on-premises business functions

For more information, see this web page.

Public cloud

The rise and adoption of public cloud services is one of the most important shifts in the history of enterprise computing. A public cloud is a type of cloud computing in which a third-party service provider makes computing resources, which can include anything from ready to use software applications, to individual virtual machines (VMs) to complete enterprise grade infrastructures and development platforms, which are available to users over the public internet. These resources might be accessible for free, or access might be sold according to subscription-based or pay-per-usage pricing models.

For more information, see this web page.

Hybrid cloud

Hybrid cloud integrates public cloud services, private cloud services, and on-premises infrastructure and provides orchestration, management, and application portability across all three.

The result is a single, unified, and flexible distributed computing environment where an organization can run and scale its traditional or cloud-native workloads on the most appropriate computing model.

For more information, see the following IBM Cloud web pages:

- What is Hybrid cloud?
- Hybrid cloud solutions

4.2.2 Cloud diagrams

IBM has several designs for cloud types, including an integration for the components and infrastructures that are managed.

You can integrate different cloud environments and platforms. Figure 4-2 shows the architecture for IBM cloud components.

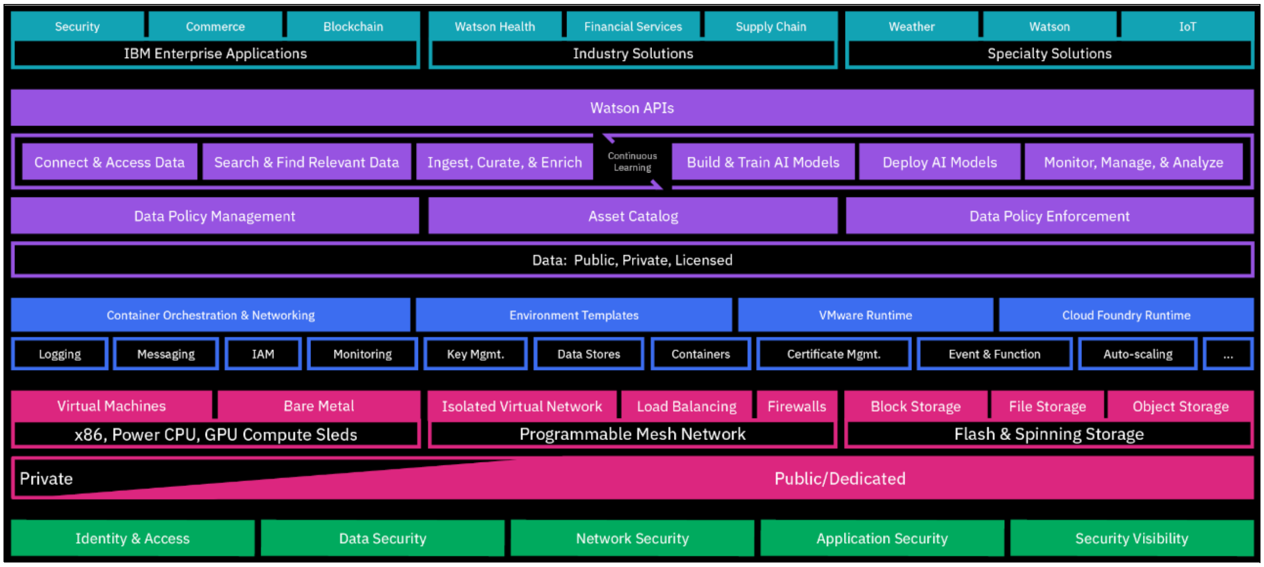


Figure 4-2 IBM cloud architecture

At a high level, hybrid integration is a broad integration framework. It seamlessly bridges all owned environments, whether direct data sources, applications, or APIs, and can connect to them wherever they might be: on-premises, IaaS, PaaS, or SaaS.

Figure 4-3 shows a hybrid cloud integration.

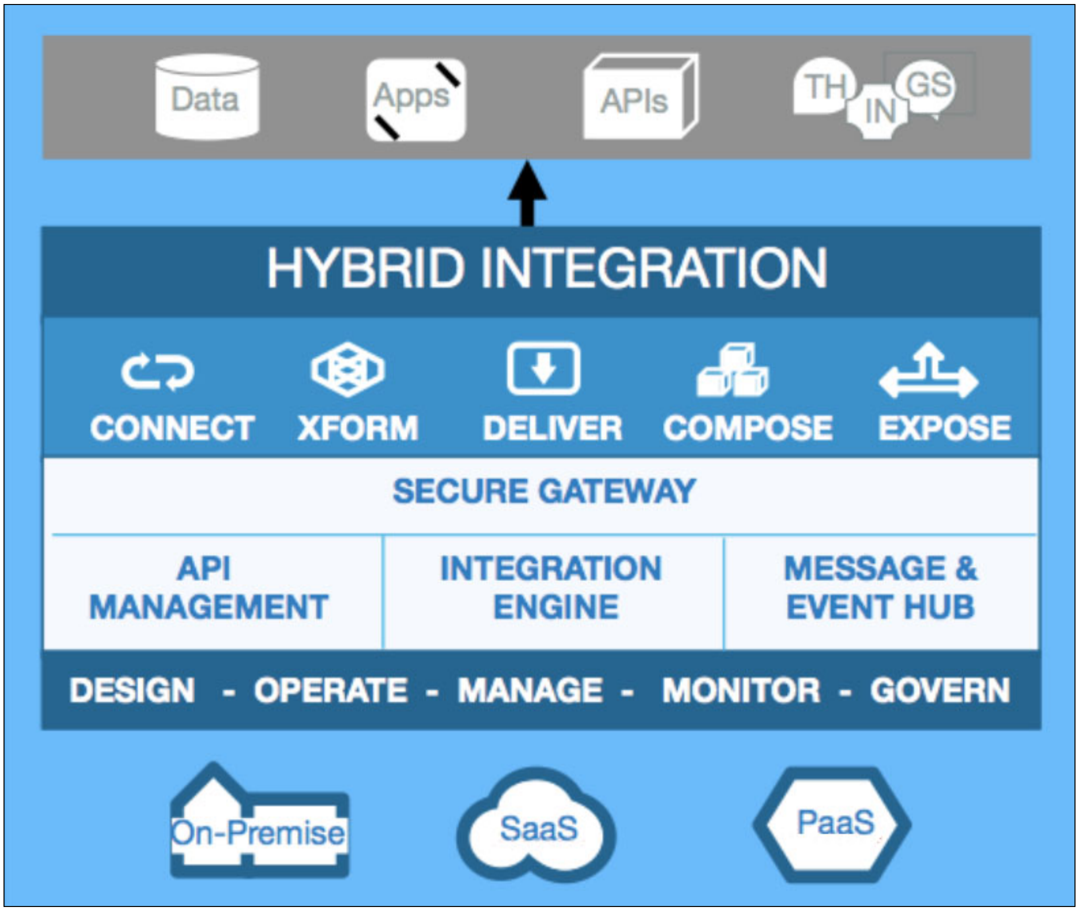


Figure 4-3 Hybrid cloud integration

Hybrid integration must contain broad connectivity capabilities for modern cloud-based applications. It is important to define hybrid integration as a whole, and we must consider how integration needs are changing and recognize the two different audiences that are involved.

4.3 AIX migration to cloud

This section discusses AIX possible migration to cloud.

The adoption of cloud of has become so prevalent today, it is an assumed part of enterprise IT strategy. What is not usually clear is how enterprises apply cloud computing and infrastructure models to applications that are responsible for core business functions.

Most Fortune 500 companies, along with many other enterprises, are running business-critical applications on AIX and IBM Power Systems. For these businesses, incorporating AIX workloads into an enterprise cloud strategy can present significant challenges, most notably the lack of support for these workloads from typical cloud infrastructure providers.

For more information, see this IBM Cloud computing news web page.

4.3.1 Migration goals

Migration to cloud can benefit enterprises and make a significant impact in terms of performance, ease of management, and cost reduction.

Data center consolidation results in a cost reduction. It is possible to migrate AIX applications without refactoring or rewriting them, which accelerates the migration journey and decreases migration costs and resources. The migration provides IT teams with increased visibility and control over resource utilization and costs, including role-based access and granular quota management.

The first step in the migration process is to evaluate your AIX workloads and identify their requirements. The organization must perform its own assessment that is inclusive of any business-specific considerations; however, the following issues provide a good basis for beginning the evaluation:

- Capacity on-demand: Where payment options are provided for teams who need to smooth out the costs that are associated with erratic or unpredictable workloads
- Cloud deployment and workload requirements: Where you can choose between the following:
  - Public or private global data center regions
  - Scale up for CPUs and memory or scale out by adding VMs or LPARs to the same environment
  - Networking and VPN
  - Operating system and support

4.3.2 Migration consideration

If you use a private cloud, such as IBM PowerVC, it is easy to get your LPARs or VMs managed by IBM PowerVC if it is a fully virtual environment that relies on IBM PowerVM.

For more information about IBM PowerVC, see the following resources:

- *IBM PowerVC Version 2.0 Introduction and Configuration*, SG24-8477
- Introduction to PowerVC
- Migration requirements

If you are considering migrating to a public cloud, such as IBM PowerVS, extra steps must be taken, including performing backups and the use of migration and replication methods.

For more information about migrating AIX, see *AIX Migration to Cloud with IBM Power Virtual Server: An IBM Systems Lab Services Tutorial*.

4.4 Power Enterprise Pools

This section introduces the concepts, features, and benefits of Power Enterprise Pools (PEP), a technology that shares processor cores and memory among a pool of Power Systems servers. PEP is the natural response to an increased demand for flexibility and responsiveness.

PEPs are available in two versions:

- Version 1.0 that uses the mobile capacity on demand
- Version 2 that uses the utility capacity

4.4.1 Power Enterprise Pools version 1.0

With PEP version 1.0, you can benefit from resources that are on different Power Systems servers. It is centered on the concept of resource activation.

Power Systems servers feature hardware resources, such as processor cores and memory, and processor books, and memory cards. Depending on the machine type and model, a Power Systems server can have a specific number and type of cores and memory modules physically installed.

As a result of the purchasing process, some or all of these resources can be activated before the system is shipped. For example, a Power Systems server might have 32 cores and 8 TB of memory that is installed, but only 16 cores and 6 TB of memory can be activated. All installed resources that are inactive at the time of shipment can be activated anytime by using an activation code.

At this PEP version, activations can be divided into the following categories:

- Static

  Resources that are associated to this type of activation are activated and bound to the Power Systems server where they are activated. They cannot be moved from one system to another.

- Mobile

  Resources that can be activated on any Power Systems server that is part of the pool and has inactive resources. Mobile resources can float from one Power Systems server to another and can be active on only one Power Systems server concurrently; therefore, the amount of usable resources on any individual system is the sum of static and mobile resources that are activated on the system.

- Dark

  Resources that are physically installed in Power Systems servers, but are not activated. They are activated when mobile, static, or CoD activation codes are used.

4.4.2 IBM Power Systems Private Cloud with Shared Utility Capacity

PEP version 2.0 is officially named IBM® Power Systems Private Cloud with Shared Utility Capacity. It is a model for sharing compute resources. This model is available for only IBM Power E1080, Power System E980, and the scale-out servers. Mobile resources do not need to be moved from one system to another nor do static resources need to be converted into mobile resources.

In contrast to PEP version 1.0, which is a resource-centric model, this version is time-based and uses a “pay-as-you-go” model.

Each system in the pool has a permanent base activation. This base is a subset of the resources that are physically installed on the Power E980 systems when they are purchased.

Depending on the operating systems that are installed in the LPARs, there might be one or more of the following types of processor-related capacity charges:

- Any operating system core

  This type is generic and the cores can run any of the operating systems that is supported by Power E980 systems.

- Linux or VIOS core

  These cores can run any supported Linux distribution or VIOS software. Although software charges are not incurred for Linux or VIOS partitions, a valid Linux license entitlement must be acquired separately to ensure that all cores or sockets that are used for Linux LPARs are licensed correctly.

- AIX software

  These cores can run only AIX software.

- IBM i software

  These cores can run only IBM i software.

The metering solution uses the IBM Cloud as a single point of control (SPOC) and management and requires a connection to IBM Cloud Management Console (IBM CMC). Because this solution is based on metering, each master Hardware Management Control (HMC) must have network time protocol (NTP) enabled. Also, performance and capacity monitoring must be enabled for each Power E980 server that is in the pool.

Customers must purchase capacity credits in advance that are used when the pool usage exceeds the base capacity of the pool. Capacity credits can be purchased from IBM, IBM Business Partners, or the IBM Entitled Systems Support website. Capacity credits are charged in real time.

IBM CMC provides a wide range of features that allow for pool, usage, and budget management, such as the following examples:

- Pool management
- Defining thresholds for systems and partitions, budget, and credit balance
- Defining alerts at the pool level based on budget and resource consumption
- Detailed analysis of usage of resources, such as metered minutes, credits, system or pool level cores, and memory
- Monitoring and management of capacity credit budget

For more information, see the following resources:

- Power Enterprise Pools 2.0 with Utility Capacity
- IBM CMC for Power Systems: FAQ
- IBM Power Enterprise Pools 2.0 delivers enhanced Utility Capacity for processors and memory across a collection of IBM Power E980 servers: Technical Information

4.5 IBM Cloud Management Console

IBM Cloud Management Console (CMC) for IBM Power Systems Servers provides a consolidated view of the IBM Power servers in your enterprise. It runs as a service that is hosted in the IBM Cloud, and you can access it securely anytime and anywhere to monitor and gain insights about your IBM Power servers.

IBM CMC can be deployed based on customer input to different IBM Cloud regions. Supported regions are US South (Dallas), Germany (Frankfurt), UK (London), and Australia (Sydney).

IBM CMC provides the following features:

- Inventory
- Capacity Monitoring
- Logging
- Patch Planning
- Support to manage application links for the following on-premises software:
  - IBM PowerVS
  - IBM PowerVC
  - PowerHA
  - IBM PowerSC
  - IBM PowerSC MFA
  - VM Recovery Manager for High Availability (HA)
- IBM Power Systems Private Cloud with Shared Utility Capacity
  (in CMC, IBM Power Systems Private Cloud with Shared Utility Capacity is referred to as Power Enterprise Pools 2.0 or Enterprise Pools 2.0.)

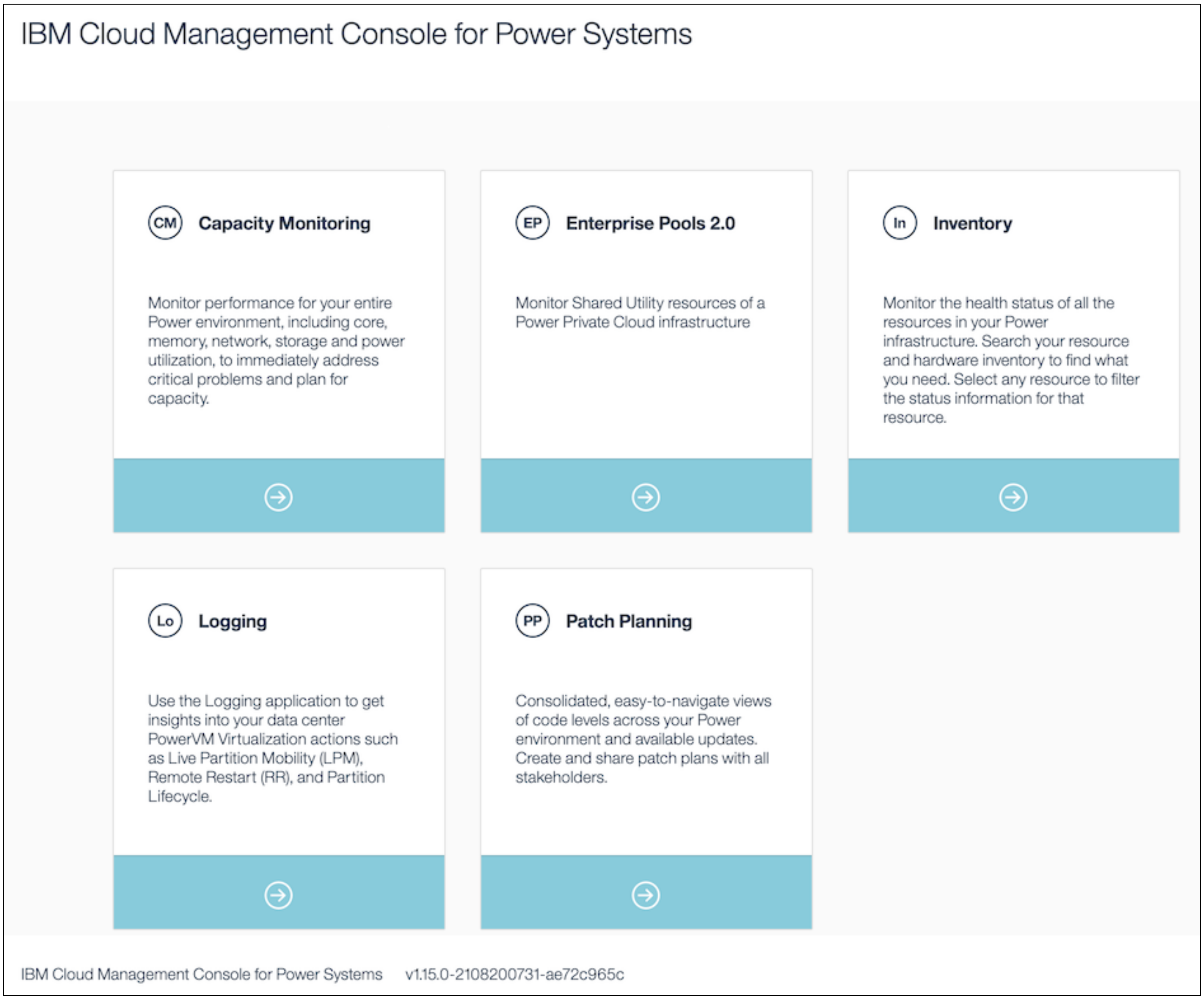
You can start any of these applications from the IBM CMC dashboard or from the navigation menu.

To enable IBM CMC to monitor the servers in your enterprise, it needs data that is uploaded by the HMC in your data center. Secure Cloud Connector is the HMC component that uploads data to the IBM CMC cloud. Secure Cloud Connector verifies the identity of your IBM CMC instance and provides end-to-end encryption between the instance and the HMC in your data center.

IBM CMC is supported for any IBM POWER8 or later processor-based servers.

The solution is built for mobile devices, tablets, and desktop browsers to provide convenient access to the application.

Figure 4-1 shows the IBM CMC dashboard.



IBM Cloud Management Console for Power Systems

Capacity Monitoring

Monitor performance for your entire Power environment, including core, memory, network, storage and power utilization, to immediately address critical problems and plan for capacity.

Enterprise Pools 2.0

Monitor Shared Utility resources of a Power Private Cloud infrastructure

Inventory

Monitor the health status of all the resources in your Power infrastructure. Search your resource and hardware inventory to find what you need. Select any resource to filter the status information for that resource.

Logging

Use the Logging application to get insights into your data center PowerVM Virtualization actions such as Live Partition Mobility (LPM), Remote Restart (RR), and Partition Lifecycle.

Patch Planning

Consolidated, easy-to-navigate views of code levels across your Power environment and available updates. Create and share patch plans with all stakeholders.

IBM Cloud Management Console for Power Systems v1.15.0-2108200731-ae72c965c

Figure 4-4 IBM Cloud Management Console

4.5.1 IBM Cloud Management Console features

With IBM CMC, you can securely view information and gain insights about the IBM Power servers in your enterprise. This section gives an overview of the IBM CMC functions.

The features of the IBM Cloud Management Console are listed in Table 4-1.

Table 4-1 Summary of IBM Cloud Management Console features

Feature	Benefits
Offered as a service in the IBM Cloud	► Customers do not have to install and maintain the software. ► Customers can use the solution function faster, and IBM can deliver new functions faster.
Inventory	► Enterprise-wide views of IBM Power servers, HMCs, LPARs, and resources that are associated with these components. ► View the state of the resources of your IBM Power servers. ► Provides the hardware inventory. ► Simplified views with grouping of resources by using client-supplied tags.
Capacity Monitoring	► Aggregated performance views that provide resource consumption and performance data for IBM Power servers, LPARs, and I/O components. ► Energy monitoring.
Logging	► System log aggregation across the IBM Power servers in your enterprise. ► Gain insights into virtualization operations, which include Live Partition Mobility, remote restart, and other partition activities.
Patch Planning	View patch planning needs across all the IBM Power server resources in your environment. The resources include firmware, VIOS partitions, operating systems, adapters, and HMCs. ► View the code levels and available updates. ► Create and share patch plans with all stakeholders.
PEP 2.0	Manage and monitor IBM Power Systems Private Cloud with Shared Utility Capacity.
Software launch capability	Start IBM Power software, such as PowerVC, IBM PowerSC, and PowerHA.

Inventory

The Inventory application displays an aggregated view of all the data centers and the resources in your environment.

If you click **Inventory** and then, click the **Dashboard** tab, you can view the state summary of managed systems, LPARs, and VIOSs in the data center. Each resource type is identified as being in a good state (such as operating or initializing for a managed system) or bad state (such as no connection or failed authentication for a managed system).

Capacity Monitoring

This feature provides aggregated performance views for your entire IBM Power environment. It displays core, memory, network, storage, and power utilization data. You can view real-time and historical performance data, which can help you to identify bottlenecks, analyze critical problems, and plan for capacity.

To view the performance data of a resource, go to the navigation menu, click **Capacity Monitoring**, and then, select the resource that you want to view in the content area. The following resources are available:

- Systems
- Partitions
- Shared Processor Pools
- Shared Storage Pool Clusters

Logging application

The Logging application displays the different Live Partition Mobility (LPM) and Remote Restart (RR) operations that are performed on the LPARs in your inventory.

The Partition Lifecycle tab provides a view of the following operations on LPARs in your inventory:

- Create
- Activate or Apply Configuration
- Shut down
- Delete

Patch Planning

The Patch Planning application provides a comprehensive view of the current and latest patch levels for the resources in your inventory. You can use this feature to perform the following actions:

- View the current patch level and latest patch update or latest patch upgrade that are available for a resource. The resources can have the following views:
  - List of all resources patch information
  - List of resources that need a patch update
  - List of resources that are up to date on their patch levels

  The resources include operating systems, firmware, VIOSs, adapters, and HMCs.
- Create and share patch plans with all stakeholders.

Enterprise Pools 2.0

The Enterprise Pools 2.0 application in IBM CMC monitors and manages PEP 2.0.

To access IBM Power Systems Private Cloud with Shared Utility Capacity, complete the following steps:

1. Click the navigation menu and then, click **Enterprise Pools 2.0**.
2. In the contents area, click any of the available pools to manage or monitor it. The following choices are available for a pool:
   - Inventory
   - Core Usage
   - Memory Usage
   - Budget
   - Usage Statement
   - Events

Software launch capability

IBM CMC provides a software launch capability for IBM Power software, such as PowerVC, IBM PowerSC, IBM PowerSC MFA, PowerHA, and VM Recovery Manager for HA. Users can add links for this software.

Multiple links can be added for each application. A unique name must be given for each link. You can access the links from the IBM CMC dashboard or from the navigation menu.

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 topics in this document. Some publications that are referenced in this list might be available in softcopy only:

- *IBM AIX Enhancements and Modernization*, SG24-8453
- *PowerVC 2.0 Introduction and Configuration,* SG24-8477
- *IBM AIX Version 7.1 Differences Guide*, SG24-7910
- *IBM PowerHA SystemMirror V7.2.3 for IBM AIX and V7.22 for Linux*, SG24-8434
- *IBM PowerVC Version 1.3.2 Introduction and Configuration*, SG24-8199
- *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940
- *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590
- *Implementing IBM VM Recovery Manager for IBM Power Systems*, SG24-8426
- *iSCSI Implementation and Best Practices on IBM Storwize Storage Systems*, SG24-8327
- *NIM from A to Z in AIX 5L*, SG24-7296

You can search for, view, download, or order these documents and other Redbooks, Redpapers, web docs, drafts, and additional materials, at the following website:

ibm.com/redbooks

Online resources

The following websites are also relevant as further information sources:

- AIX documentation for current JFS2 size limits:

  https://www.ibm.com/docs/en/aix/7.3?topic=limitations-jfs2-size-limits

- General AIX information:

  https://www.ibm.com/products/aix

- IBM AIX data sheet download:

  https://www.ibm.com/docs/en/aix/7.3?topic=limitations-jfs2-size-limits

- Trusted Execution:

  – https://www.ibm.com/support/pages/trusted-execution-enablement
  – https://www.ibm.com/docs/en/aix/7.2?topic=configuration-trusted-execution
  – https://www.ibm.com/docs/en/aix/7.2?topic=security

- AIX File Permission Manager:

  – https://www.ibm.com/support/pages/aix-fpm-file-permission-manager-setup
  – https://www.ibm.com/docs/en/aix/7.2?topic=f-fpm-command

- Logical volume encryption:
  - https://www.ibm.com/docs/fr/aix/7.2?topic=system-encrypted-logical-volumes
  - https://www.ibm.com/docs/fr/aix/7.2?topic=h-hdcryptmgr-command
- IP encryption configuration:

  https://www.ibm.com/docs/en/aix/7.2?topic=security-ip-filter-configuration
- AIX Live Update:

  https://www.ibm.com/support/pages/ibm-aix-72-live-kernel-update-reboot-free-world
- Alternative disk cloning:
  - https://www.ibm.com/support/pages/multiple-alternate-rootvg-criteria
  - https://www.ibm.com/support/pages/managing-multiple-instances-altinstrootvg-and-applying-fixes-them
- AIX and Ansible:
  - https://galaxy.ansible.com/ibm/power_aix
  - https://www.ansible.com/integrations/infrastructure/ibm-power-systems
  - https://www.ansible.com/blog/aix-patch-management-with-ansible
- AIX 7.3 release notes:

  https://www.ibm.com/docs/en/ssw_aix_73/pdf/rnbase730_pdf.pdf
- AIX 7.3 What’s New documentation:

  https://www.ibm.com/docs/en/aix/7.3?topic=whats-new
- AIX Toolbox for Open Source:
  - https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/8/897/ENUS221-328/index.html&request_locale=en
  - https://community.ibm.com/community/user/power/communities/community-home?CommunityKey=10c1d831-47ee-4d92-a138-b03f7896f7c9
- AIX and the cloud:
  - https://www.ibm.com/cloud/learn/introduction-to-private-cloud#toc-what-is-pr-G90T95hf
  - https://www.ibm.com/cloud/learn/introduction-to-private-cloud#toc-how-privat-uhGAG2N1
  - https://www.ibm.com/cloud/learn/introduction-to-private-cloud#toc-private-cl-w3kR8ZY8
  - https://www.ibm.com/cloud/learn/introduction-to-private-cloud#toc-benefits-o-6HNN95IF
  - https://www.ibm.com/cloud/learn/introduction-to-private-cloud
- PowerVC:

  https://www.ibm.com/downloads/cas/KZXBYY0G
- PowerSC:
  - http://www.redbooks.ibm.com/abstracts/sg248477.html?Open
  - https://www.ibm.com/docs/en/powervc-cloud/2.0.2
  - https://www.ibm.com/docs/en/powervc-cloud/2.0.2?topic=introduction
- VM Recovery Manager:

  https://www.ibm.com/downloads/cas/79KXQORP

- AIX Licensing:

  https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss
- AIX and Tivoli:

  http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html
- AIX and Terraform:

  https://www.terraform.io/
- Chef automation:

  https://docs.chef.io/chef_overview/

  https://supermarket.chef.io/cookbooks/aix
- Puppet automation:

  https://puppet.com/
- Partition mobility:a
  - https://www.ibm.com/docs/en/power9?topic=environment-live-prtition-mobility
  - https://www.ibm.com/support/pages/live-partition-mobility
  - https://www.ibm.com/support/pages/how-perform-remote-partition-mobility-remote-lpm
  - https://www.ibm.com/docs/en/power9?topic=partitions-remote-restart-states
  - https://www.ibm.com/docs/en/power9?topic=rrs-validating-simplified-remote-restart-logical-partition-by-using-hmc
  - https://www.ibm.com/docs/en/power9?topic=rrs-enabling-disabling-simplified-remote-restart-capability-logical-partition-by-using-hmc
  - https://www.ibm.com/support/pages/simplified-remote-restart-hmc-or-powervc
- PowerHA:

  https://www.ibm.com/products/powerha
- VM Recovery Manager:
  - https://www.ibm.com/products/vm-recovery-manager
  - https://www.ibm.com/downloads/cas/79KXQORP
  - https://www.ibm.com/docs/en/vmrmha/1.5?topic=overview
  - https://www.ibm.com/docs/en/vmrmdr/1.5?topic=overview
- AIX system service summary:

  https://www.ibm.com/docs/en/aix/7.2?topic=security-summary-common-aix-system-services
- AIX network service summary:

  https://www.ibm.com/docs/en/aix/7.2?topic=security-summary-network-service-options
- PCI encryption:
  - https://www.ibm.com/docs/en/aix/7.2?topic=security-4765-pcie-cryptographic-coprocessor-aix-cca-support-program-installation-44
  - https://www.ibm.com/docs/en/aix/7.2?topic=security-4767-pcie-cryptographic-coprocessor-aix-cca-support-program-installation-53

- PowerSC multifactor support:
  - https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_sm/3/877/ENUS5765-CD3/index.html
  - https://www.ibm.com/docs/en/powersc-mfa/2.0?topic=powersc-mfa-concepts
  - https://www.ibm.com/docs/en/powersc-mfa/2.0?topic=aix-powersc-mfa-server-requirements
  - https://www.ibm.com/docs/en/powersc-mfa/2.0?topic=concepts-rsa-authentication-manager
- Securing the cloud:

  https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-getting-started
- Private cloud:
  - https://www.ibm.com/cloud/learn/introduction-to-private-cloud
  - https://ibm-cloud-architecture.github.io/refarch-integration/journey
- Public cloud:

  https://www.ibm.com/cloud/learn/public-cloud
- Hybrid cloud:
  - https://www.ibm.com/cloud/learn/hybrid-cloud
  - https://www.ibm.com/cloud/hybrid
- Migration to the cloud:
  - https://www.ibm.com/blogs/cloud-computing/2015/02/13/aix-public-private-cloud-ibm-managed-services/
  - http://www.redbooks.ibm.com/abstracts/sg248477.html?Open
  - https://www.ibm.com/docs/en/powervc/2.0.2?topic=introduction-powervc
  - https://www.ibm.com/docs/en/powervc/2.0.2?topic=machine-migration-requirements
  - https://cloud.ibm.com/media/docs/downloads/power-iaas-tutorials/PowerVS_AIX_Migration_Tutorial_v1.pdf
- Power Enterprise Pools:
  - https://ibmcmc.zendesk.com/hc/en-us/articles/360021928094-Enterprise-Pools-2-0
  - https://ibmcmc.zendesk.com/hc/en-us/sections/207305647-FAQ
  - https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/3/872/ENUSAG19-0003/index.html&lang=en&request_locale=en#hardx

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

REDP-5660-00

ISBN 073846063x

Printed in U.S.A.