Understanding Cloud Security Guidelines for IBM Power Systems

IBM Redbooks Solution Guide

IBM® Power Systems™ are uniquely suited for cloud environments, with their industry leading virtualization, enterprise-class security, elastic scalability, and reliability, availability, and serviceability (RAS). As with most new technology paradigms, security concerns surrounding cloud computing have become the most widely talked-about inhibitor of widespread usage, whether for public, private, or hybrid cloud installations.

In this IBM Redbooks® Solution Guide, we describe some of the processes and tools that should be implemented by system architects or administrators to ensure that your Power System-based private cloud environment is secure. Figure 1 shows an example Power Systems cloud structure.

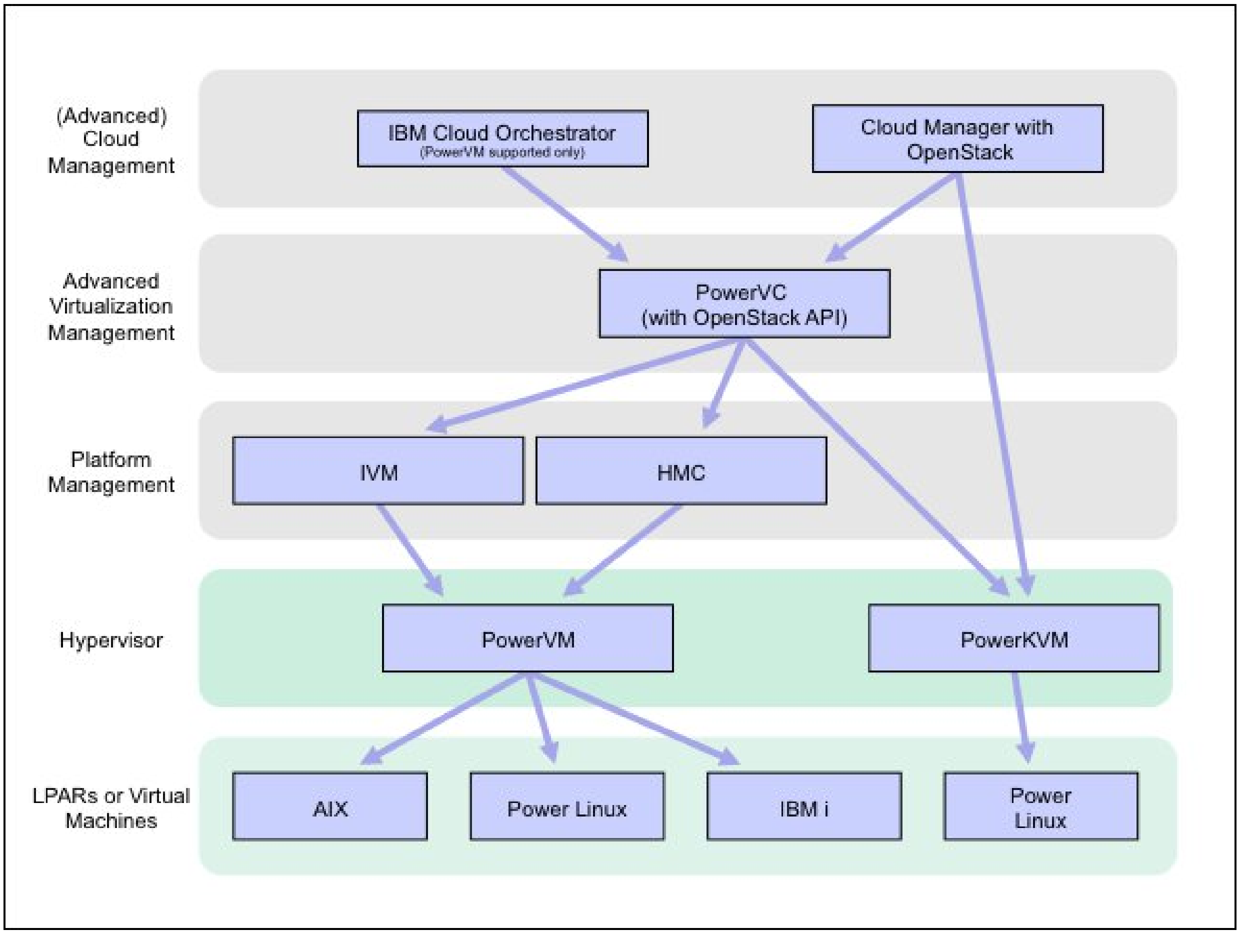

Figure 1. Power Systems cloud management hierarchy

Did you know?

IBM Power Systems provide a choice of hypervisor, using either IBM PowerVM® or the open source IBM PowerKVM.

PowerVM efficiently uses system resources and imposes a negligible impact on performance, because PowerVM is designed for and built directly into the firmware of all Power Systems. Being part of the firmware also means that PowerVM is secure by design.

IBM PowerKVM presents a choice for organizations looking for a low cost, open source virtualization solution for Linux on Power Systems built on the IBM POWER8™ architecture. IBM PowerKVM provides support for Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Ubuntu guests.

Business value

Interest in cloud computing is strong among today's Chief Information Officers (CIOs) and business leaders. In one recent IBM study (**Source**: *Under Cloud Cover*, IBM Center for Applied Insights, 2013), it was found that the cloud's strategic importance to decision-makers, such as Chief Executive Officers (CEOs), Chief Marketing Officers (CMOs), finance, Human Resources (HR), and procurement executives, is poised to double from 34% - 72%. The survey found that one out of five organizations is ahead of the curve on cloud adoption and achieving competitive advantage, not just cutting costs and driving efficiency, through cloud computing.

Pacesetters in cloud adoption have reported impressive competitive advantages from cloud computing, but the journey has not been easy. Forty-four percent of respondents believe that cloud introduces greater complexity into their organization. To manage this growing complexity, early adopters are more likely to share the following characteristics:

- Have an enterprise-wide cloud strategy
- Favor open source cloud platforms
- Use a hybrid cloud
- Have executive support for cloud experimentation

The following list describes some key business drivers for business adoption of cloud computing:

- Use cloud infrastructure with confidence that they are secure, compliant, and meet regulatory requirements.
- Leverage existing investment, and extend current infrastructure to implement security for virtual infrastructure.
- Decrease delivery and provisioning time for secure new services through standardization and automation.
- Maintain service-level compliance, accuracy, repeatability, and traceability for the cloud environment.
- Align Information Technology (IT) resource allocation with business goals.

A cloud computing environment built with IBM Power Systems can help organizations transform their data centers to become cloud ready.

Power Systems are uniquely suited for cloud environments, with their industry leading virtualization, enterprise-class security, elastic scalability, and reliability, availability, and serviceability (RAS). Power Systems provide the necessary memory bandwidth and compute power to deliver performance that big data, analytics, and other compute-intensive cloud services require.

Solution overview

The IBM Cloud Computing Reference Architecture (CCRA) provides prescriptive guidance on how to best build cloud computing implementations.

The CCRA V3.0 identifies four cloud adoption patterns:

- Cloud-enabled data center, also called Infrastructure as a Service (IaaS)
- Platform Services, also called Platform as a Service (PaaS)
- Software Services, also called Software as a Service (SaaS)
- Cloud service provider (CSP)

Some of the attributes of each adoption pattern are shown in Figure 2. Different security controls are appropriate for different cloud needs. The challenge becomes one of integration, coexistence, and recognizing what solution is best for a given workload.

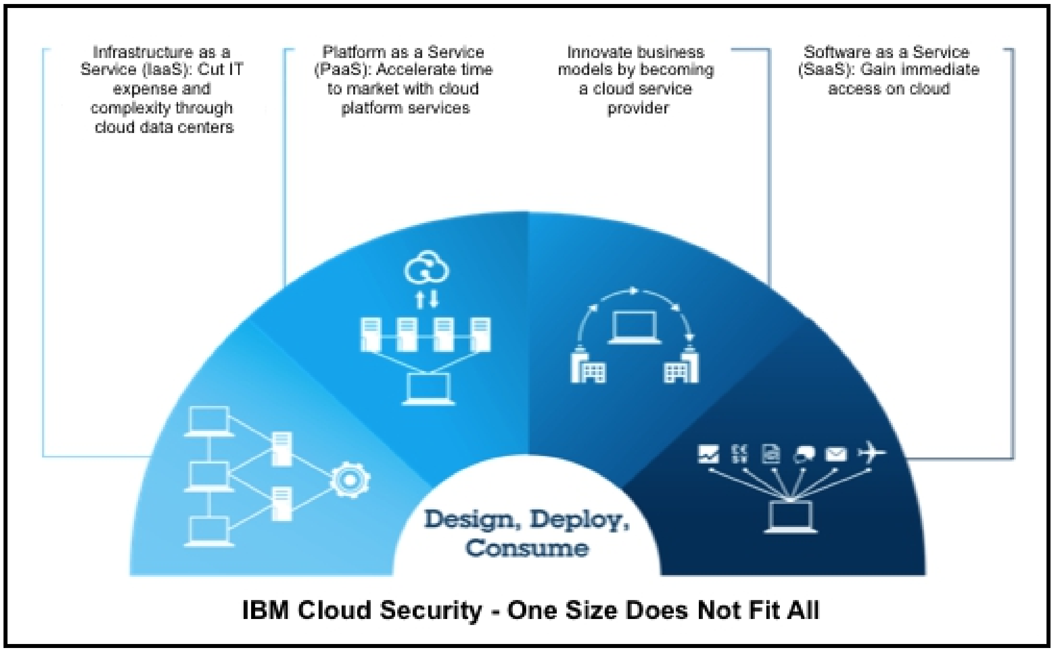
Infrastructure as a Service (IaaS): Cut IT expense and complexity through cloud data centers
Platform as a Service (PaaS): Accelerate time to market with cloud platform services
Innovate business models by becoming a cloud service provider
Software as a Service (SaaS): Gain immediate access on cloud
Design, Deploy, Consume
IBM Cloud Security - One Size Does Not Fit All

Figure 2. IBM cloud security: One size does not fit all

Based on the IBM Security Framework, the CCRA articulates eight Foundational Controls to address security in cloud environments:

- Cloud governance
- Security governance, risk management, and compliance
- Problem and information security incident management
- Identity and access management
- Discover, categorize, and protect data and information assets
- Information systems acquisition, development, and maintenance
- Secure infrastructure against threats and vulnerabilities
- Physical and personnel security

An overview of the IBM security framework and cloud foundational controls can be seen in Figure 3.

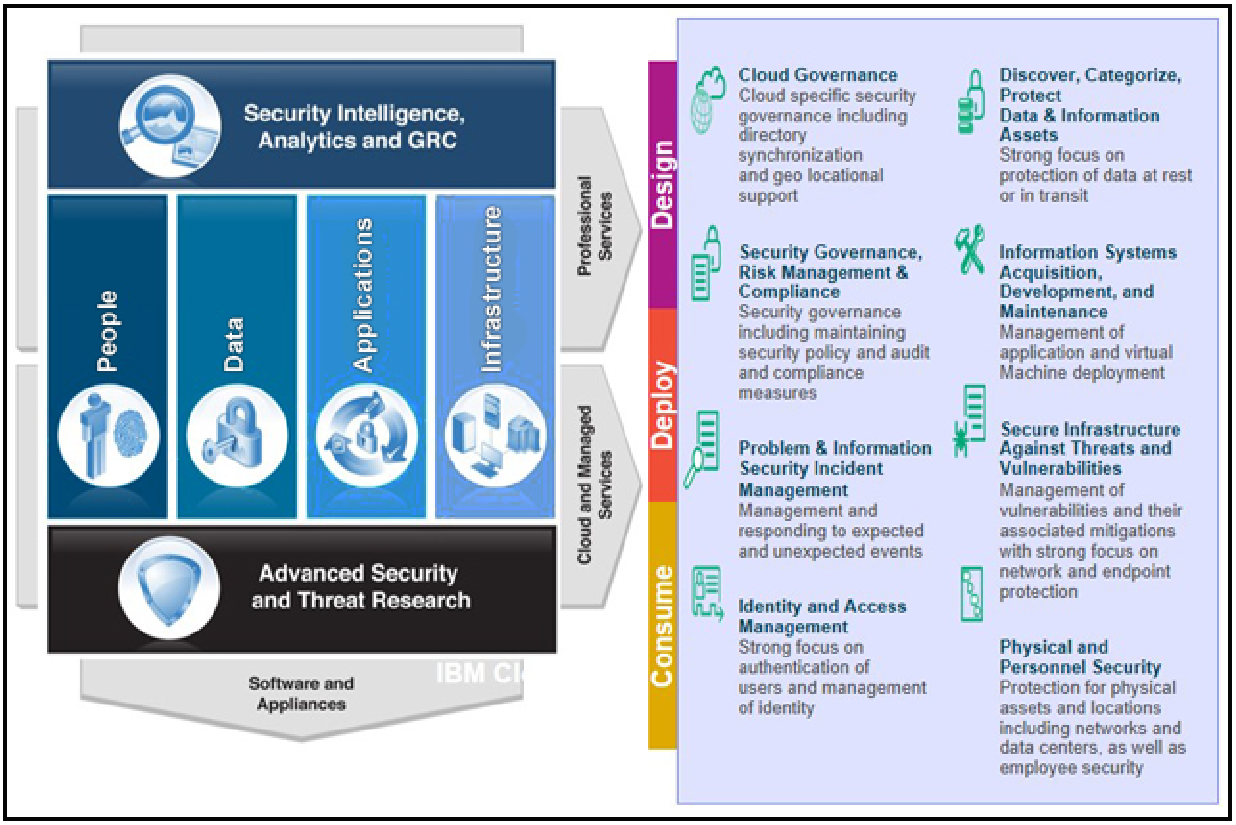
Security Intelligence, Analytics and GRC
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Software and Appliances
IBM Cl
Professional Services
Cloud and Managed Services
Design
Deploy
Consume
Cloud Governance
Cloud specific security governance including directory synchronization and geo locational support
Discover, Categorize, Protect Data & Information Assets
Strong focus on protection of data at rest or in transit
Security Governance, Risk Management & Compliance
Security governance including maintaining security policy and audit and compliance measures
Information Systems Acquisition, Development, and Maintenance
Management of application and virtual Machine deployment
Problem & Information Security Incident Management
Management and responding to expected and unexpected events
Secure Infrastructure Against Threats and Vulnerabilities
Management of vulnerabilities and their associated mitigations with strong focus on network and endpoint protection
Identity and Access Management
Strong focus on authentication of users and management of identity
Physical and Personnel Security
Protection for physical assets and locations including networks and data centers, as well as employee security

Figure 3. IBM Security Framework and cloud Foundational Controls

Cloud-enabled data centers

IaaS is the typical starting point for most organizations when moving to a cloud computing environment. IaaS can be used for the delivery of resources, such as compute, storage, and network services, through a self-service portal. This solution guide takes a close look at secure implementations of Power Systems in a private cloud-enabled data center or IaaS cloud. Because hybrid cloud solutions become increasingly important, we also discuss security considerations when planning to extend your private cloud with hybrid functionality.

Note: When implementing a private cloud, you have several choices. You can build it yourself on premises, or you can contract a CSP to provide it for you. If you are evaluating CSPs, the Cloud Security Alliance (CSA) has several documents that enable you to assess the potential security risks associated with CSPs. See https://cloudsecurityalliance.org for more details.

The IBM CCRA security architecture describes five key security requirements for cloud-enabled data centers:

- Manage identities and access:
  - Manage data center identities and securely connect users to the cloud (authentication and authorization)
  - Provide role-based access to cloud resources, image library, and storage
  - Provision user IDs on the virtual machine (VM) for access to the VM or LPAR
  - Manage confidentiality and integrity of the storage, images, and metadata associated with the master image
  - Privileged administrator management

- Protect virtual infrastructure:
  - Secure and protect the virtual infrastructure (VM instances, LPARs, and hypervisors) according to IT Security Policy
  - Storage encryption
  - Network protection through firewalls and intrusion prevention systems (IPS)
  - Host security and vulnerability scanning
- Patch default images:
  - Image library and software catalog
- Provide visibility into virtual infrastructure:
  - Maintaining audit logs for virtual infrastructure compliance and audit readiness
  - Monitoring cloud infrastructure
  - Monitor and manage workloads
- Network isolation:
  - Implement virtual local area networks (VLANs), physical network separation, firewall devices, and intrusion detection systems as appropriate

In the following sections, we provide suggestions about how to improve the security of your Power Systems cloud infrastructure. It is the responsibility of the reader to ensure that their environment is compliant with whatever regulations, standards, or security frameworks are applicable to them.

Cloud computing and regulatory compliance

Regulatory compliance refers to externally imposed conditions on transactions in business systems and their companies. Regulations can be imposed by industry bodies, regulatory agencies, and government agencies.

Non-conformance with regulations can result in legal ramifications. A civil or criminal liability or regulatory penalty from a security incident, or attack, negatively affects your business.

Applicable regulations and steps to ensure compliance must be factored into cloud projects.

The following partial list is intended as a starting point for researching what standards and regulations are applicable to your cloud environment:

- National Institute of Standards and Technology (NIST) and the Special Publication 800 series: http://csrc.nist.gov/
- Federal Information Security Management Act (FISMA): http://csrc.nist.gov/sec-cert/
- Federal Risk and Authorization Management Program (FedRAMP): http://cloud.cio.gov/fedramp
- Federal Information Processing Standards (FIPS): http://csrc.nist.gov/publications/PubsFIPS.html
- Common Criteria: http://www.commoncriteriaportal.org/
- Payment Card Industry Data Security Standard (PCI-DSS): https://www.pcisecuritystandards.org/
- Health Insurance Portability and Accountability Act of 1996 (HIPAA): http://www.hhs.gov/ocr/privacy/
- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/cobit/
- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC 27001:2005): http://www.27000.org/
- Statement on Standards for Attestation Engagements (SSAE16): http://ssae16.com/
- Homeland Security Presidential Directive 12: https://hspd12.usda.gov
- Financial Services Roundtable / BITS: http://www.bits.org/
- Sarbanes-Oxley (SOX): http://www.soxlaw.com/
- Generally Accepted Privacy Principles (GAPP): http://www.aicpa.org/

Note: It is not possible to provide a complete list of all security standards and frameworks to cover every country or industry.

Solution architecture

The IBM Power Systems cloud offerings can be broken down into five distinct layers (also see the first figure, Figure 1):

- Hypervisors
- Platform management
- Advanced virtualization management
- Cloud management and advanced cloud management
- Guest operating systems (LPARs or VMs)

Next, examine these layers in a bit more detail.

Hypervisors

PowerVM makes efficient use of system resources and imposes a negligible impact on performance, because PowerVM is designed for and built directly into the firmware of all Power Systems. Being part of the firmware also means that PowerVM is secure by design, with zero reported Common Vulnerabilities and Exposures (CVE) for the PowerVM hypervisor in the US Government National Institute of Standards and Technology (NIST, source: http://nvd.nist.gov) National Vulnerabilities Database (NVD). PowerVM supports IBM AIX®, Power Linux, and IBM i as guest operating systems.

IBM PowerKVM presents a choice for organizations looking for a low-cost, open source virtualization solution for Linux on Power Systems built on the POWER8 architecture. IBM PowerKVM provides support for RHEL, SLES, and Ubuntu guests, and is optimized for Power Systems, with support for processor and memory sharing over-commit for higher utilizations, dynamic addition and removal of virtual devices, and live VM migration.

Platform management

Platform management is usually implemented using a web interface, and enables basic interaction with the hypervisor, including such things as create and delete LPARs or VMs, start and stop instances, and so on.

The IBM Hardware Management Console (HMC) is an appliance for planning, deploying, and managing Power Systems. With the HMC, a system administrator can perform LPAR functions, service functions, and various system management functions by using either the web browser-based user interface (UI), or the command-line interface (CLI).

The functionality of the HMC extends beyond the basic administration of LPARs, and is described in the IBM Redbooks publication *IBM Power Systems HMC Implementation and Usage Guide*, SG24-7491. The enhancements to V8 of the HMC, including updates to NIST SP800 131A support, are described in the IBM Redbooks publication *IBM Power Systems Hardware Management Console Version 8 Release 8.1.0 Enhancements*, SG24-8232.

The Integrated Virtualization Manager (IVM) is a simplified hardware management solution that inherits most of the HMC features. IVM provides a web-based management interface for a single system, and targets small and medium systems, where use of a dedicated HMC appliance might not be cost-effective. IVM is an enhancement of the Virtual input/output (I/O) Server (VIOS), the product that enables I/O virtualization in Power Systems. The IVM is described in more detail in the IBM Redpaper™ publication *Integrated Virtualization Manager for IBM Power Systems Servers*, REDP-4061.

Kimchi is the IBM PowerKVM open source management layer built on open standards including libvirt, virsh, and OpenStack. Kimchi provides a web interface for managing IBM PowerKVM, and virtual machines, built on a Representational State Transfer (REST)-ful application programming interface (API).

Advanced virtualization management

Advanced virtualization management tools build on the basic capabilities of platform management tools, and enhance the management of resources, images, and deployments.

Advanced virtualization management is provided by IBM Power Virtualization Center (IBM PowerVC). Built on OpenStack, it allows Power System cloud infrastructure to plug into a broad array of management solutions.

IBM PowerVC allows the system administrator to perform the following activities:

- Create VMs and resize their processor and memory.
- Attach disk volumes to them.
- Import existing VMs and volumes so that they can be managed by IBM PowerVC.
- Monitor the use of the resources that are in your environment.
- Migrate VMs while they are running (live migration between physical servers).
- Deploy images quickly to create new VMs that meet the demands of dynamic business needs. At the time of writing this publication, IBM PowerVC can deploy VMs using AIX or Linux operating systems.

IBM PowerVC is deployed between the HMC and IBM cloud management offerings. It provides a systems management product that large organizations require to effectively manage the advanced features offered by Power Systems hardware. It enhances resource use, and manages workloads for performance and availability.

Cloud management and advanced cloud management

Cloud management layers are differentiated from advanced virtualization management layers by the ability to manage hypervisors on different platforms, or even from different vendors.

IBM Cloud Manager with OpenStack (formerly IBM SmartCloud® Entry) is a modular, highly flexible, and easy to use solution designed to deliver cloud services for private or public clouds, across a heterogeneous infrastructure including Power Systems and x86.

Cloud administration is simplified through an intuitive interface for managing projects, users, and applications, in addition to monitoring heterogeneous workloads and cloud resources.

IBM Cloud Manager with OpenStack also provides an entry point to more advanced IBM cloud offerings, such as IBM Cloud Orchestrator.

IBM offers solutions to deliver advanced cloud capabilities, such as rapid and scalable provisioning optimized for service providers, robust workflow orchestration, virtualization lifecycle management, and sophisticated billing and chargeback with IBM Cloud Orchestrator.

These solutions, built on open source solutions including OpenStack and Chef, are designed to reduce the risk associated with software integration, and accelerate delivery of advanced cloud computing capabilities.

Guest operating systems

The PowerVM hypervisor supports LPARs running either AIX, IBM i, or PowerLinux.

The IBM PowerKVM hypervisor supports VMs running PowerLinux. The supported distributions are RHEL, SLES, and Ubuntu.

Security recommendations

To expand on the five key security requirements identified by the IBM CCRA for a cloud-enabled data center, the accompanying IBM Redbooks publication provides more detailed information and suggestions for securing PowerVM, IBM PowerKVM, IBM PowerVC, and Cloud Manager with OpenStack.

Manage identities and access

Consider the following information when planning to manage identities and access:

- IBM Cloud Manager with OpenStack and IBM PowerVC support Lightweight Directory Access Protocol (LDAP) as a user authentication directory. IBM Cloud Manager with OpenStack supports OpenLDAP and IBM Directory Server. IBM PowerVC supports OpenLDAP and Microsoft Active Directory. Connections from the management layer server to the directory server should be encrypted with Transport Layer Security (TLS).
- IBM PowerKVM and PowerVM (VIOS) both support LDAP at the operating system level. However, using LDAP authentication for the hypervisor is not critical, because users access hypervisor resources through other management layers (for example, IBM PowerVC or IBM Cloud Manager with OpenStack).
- Role-based access should be configured for IBM PowerVC and IBM Cloud Manager with OpenStack. *Admin*, *deployer*, and *viewer* are the three default LDAP roles or user groups used in IBM PowerVC. *Keystone* is the OpenStack component that handles users' identities. IBM Cloud Manager with OpenStack also supports user roles and group membership through the OpenStack user and tenant model provided by the Keystone component.
- Management layers that have a web interface (for example, HMC, IVM, Kimchi, IBM PowerVC, and IBM Cloud Manager with OpenStack) should have Hypertext Transfer Protocol Secure (HTTPS) enabled for user access. Where it is possible to choose which cipher suite is used in Secure Sockets Layer (SSL) handshake negotiation, the strongest suite supported by the user's browsers should be selected. For example, TLS 1.2 might be mandated by some security standards, but might not be supported by all browsers. The authentication process in particular must be encrypted from end-to-end (from user browser to LDAP server).
- Federated identity management is not essential with an on-premises private cloud, but the growing popularity of hybrid clouds requires consideration to be given to federated identity technologies, such as OpenID, OAuth, and Security Assertion Markup Language (SAML).
- Manage privileged administrative user access through processes or tools. Access to privileged user accounts, such as root or padmin, should be managed securely to prevent accountability and compliance issues, and to decrease the risk of sabotage and data loss.

Secure virtual machines

Consider the following information when planning VM security:

- Encryption of data at rest can be a requirement of some security standards (for example, PCI-DSS or HIPAA). The hypervisor may support encrypted data at the storage area network (SAN) level by use of a disk array with hardware encryption (for example, IBM DS8000®), or an encrypting SAN switch (for example, SAN32B-E4). An alternative solution is to use an encrypted file system on the guest operating system. Encrypted File System (EFS) and IBM General Parallel File System (IBM GPFS™) on AIX, and dm-crypt, Linux Unified Key Setup (LUKS), or Enterprise Cryptographic File System (eCryptFS) on Linux, are examples.
- Encryption of data backups is also a factor to be considered. Tape drives with encryption hardware do not impose any performance degradation. Key management also becomes a priority when managing encryption keys across several separate platforms.

- Packet filtering at the VM host level should also be implemented. On AIX, Transmission Control Protocol/Internet Protocol (TCP/IP) filters are included in the IP Security (IPSec) packages (`bos.net.ipsec.keymgt` and `bos.net.ipsec.rte`). The default packet filter for recent Linux distributions is iptables. Some time must be invested to survey what TCP/IP ports must be allowed through the packet filter, based on administration, management, and application requirements. Access should be restricted to the appropriate IP addresses or subnets wherever possible.
- Hosts should also be subject to some degree of "hardening" by removing unnecessary software packages (for example, consider whether an HTTP server package is required on a compute node). This is best done at the image library level, but there are both benefits and pitfalls with multi-purpose images. A better approach is to start with a hardened base image, and require the user to choose packages or functionality from a software catalog at deployment time.
- Standard system administrator best practices should be followed. A non-exhaustive list includes the following actions:
    - Enforcing password policy (complexity, aging, and re-use)
    - Changing default system and application passwords
    - Backing up critical data
    - Using Network Time Protocol (NTP) to synchronize time across all systems
- Routine vulnerability scanning is also suggested. Scanning can be done on the local host with health check tools, or done remotely over the network, or preferably a combination of both.

Patch default images

Consider the following information when planning security patch maintenance:

- Cloud administrators must be diligent in ensuring that their image library is kept current with regards to security patches. More sophisticated cloud managers have more advanced tools for maintaining image libraries.
- Compliance tools, such as endpoint managers or management frameworks, can be beneficial in keeping VMs, hypervisors, and management servers up to date with security patches.

Manage logs and audit data

Consider the following information when planning to manage logs and audit data:

- All layers of the Power Systems stack support syslog for logging system events. All management nodes and virtual machines should be configured to forward syslog messages to an event management system at the least. The use of a security information and event management (SIEM) solution is highly suggested, particularly one with advanced threat protection (ATP).
- In addition to syslog, SIEM systems might have event or audit agents that are required to be installed on the end-points (management servers or VMs).
- Time must be invested to produce a baseline of events processed by the event manager with minimal false positives. Procedures must be in place for first responders to act on escalated events in a timely manner.

Network isolation

Consider the following information when planning network isolation:

- Management interfaces, such as HMC, IVM, and hypervisors, need to be kept isolated from networks used for VMs, and from other networks.
- In addition, networks used for functions, such as live migration and backups, should not be accessible by the user.

- Use the appropriate combination of VLANs, physical network separation, and firewalls as deemed appropriate. Again, the use of next-generation firewalls with integrated IPS and advanced threat protection (ATP) is highly suggested.
- With increasing uptake of hybrid clouds, virtual private networks (VPNs) also become a requirement. Two-factor authentication is usually a requirement for VPN access.

Usage scenario

The following section describes a generic use case in a cloud-enabled data center or IaaS cloud. In Figure 4, the security enforcement points are indicated with numbers.

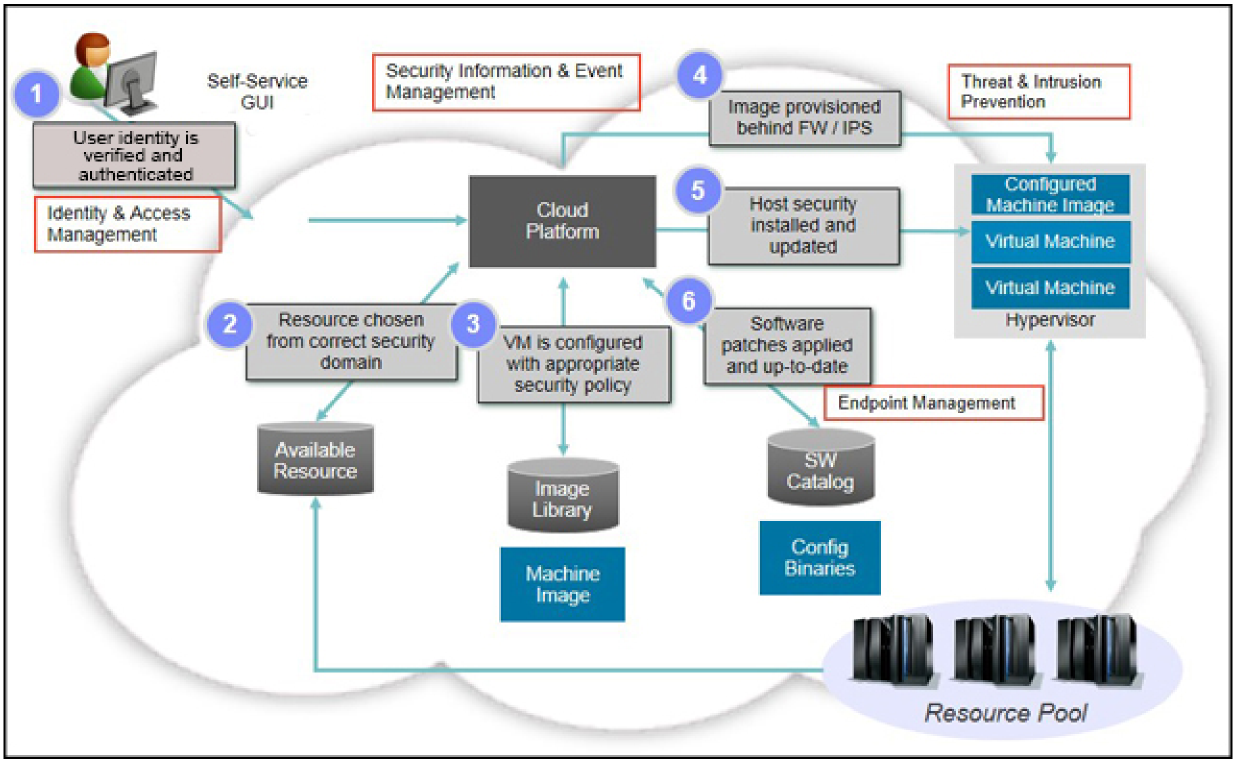
1
User identity is verified and authenticated
Identity & Access Management
Self-Service GUI
Security Information & Event Management
4
Image provisioned behind FW / IPS
Threat & Intrusion Prevention
Cloud Platform
5
Host security installed and updated
Configured Machine Image
Virtual Machine
Virtual Machine
Hypervisor
2
Resource chosen from correct security domain
3
VM is configured with appropriate security policy
6
Software patches applied and up-to-date
Endpoint Management
Available Resource
Image Library
Machine Image
SW Catalog
Config Binaries
Resource Pool

Figure 4. Generic use case for a cloud-enabled data center

The following list numbers provide details about the corresponding security enforcement points shown in Figure 4:

1. The user logs in to a self-service graphical user interface (GUI) using a web browser. Security considerations include the following factors:
   - The HTTPS connection should be encrypted with appropriate key lengths and ciphers.
   - An LDAP user directory should be used.
   - LDAP authentication should be encrypted end-to-end.
   - The identity lifecycle should be managed in an enterprise-wide manner.
2. When authenticated, the user should be granted access to appropriate resources based on the user's functional role. Additional fine-grained access controls can be implemented with enterprise-wide access management tools.
3. Required VM images are selected from a pre-configured image library. Stored images in the image library should have all appropriate management tools installed, and required security policies (end-point management agents, password policy, and so on) should be applied.

4. Images should then be provisioned onto a dedicated VM network. Segregation of different functional networks (management networks, workgroup or team networks, staging and production networks, and so on) should be enforced with the appropriate combinations of VLANs, physical network separation, firewalls, and access control lists (ACLs). The use of next-generation firewalls with IPS and ATP is highly suggested.
5. Host security of the VM should be installed or updated when deployed. This might include updating end-point manager policies, configuring logging destinations for event management, or installing specific user keys for access to the VM.
6. There might be too many combinations of application software versions to allow pre-configured images of every combination to be stored in the image library. Software would then be installed and updated from a software catalog post deployment.

Integration

The security processes and suggestions described in this Redbooks Solution Guide and accompanying IBM Redbooks publication integrate with the following IBM products shown in Table 1.

Table 1. Integration between IBM Power Systems cloud offerings and other IBM products

Component	Functionality	Example product
Security Information and Event Management (SIEM)	Provides extensive visibility and actionable insight to help protect networks and IT assets from a wide range of advanced threats. An SIEM solution helps detect and remediate breaches faster, helps address compliance, and can improve the efficiency of security operations.	● IBM Security QRadar® SIEM ● IBM Security QRadar Log Manager ● IBM SmartCloud Monitoring
Identity and Access Management (IAM)	● Manages identity lifecycle and provides self-service for the consumer and provider. ● Enforces fine-grained access policies on cloud, social, and mobile applications. ● Provides single sign-on (SSO) capability for non-web-based applications. ● Manages user credential storage in registry with LDAP access. ● Synchronizes user credentials between separate registries. ● Extends on-premises IAM infrastructure to cloud applications.	● IBM Security Identity Manager ● IBM Security Access Manager ● IBM Security Access Manager for Enterprise Single Sign-On ● IBM Security Directory Server ● IBM Security Directory Integrator ● IBM Security Federated Identity Manager
Endpoint Management	Provides patch management, security configuration management, and standards-based key management on multiple encryption targets.	● IBM Endpoint Manager for SmartCloud ● IBM Systems Director ● IBM Security Key Lifecycle Manager
Threat and Intrusion Prevention	Protects the network infrastructure from a wide range of attacks.	● IBM Security Network Protection (XGS and GX) ● IBM Security Network Intrusion Protection ● IBM Security SiteProtector™ System

Supported platforms

Table 2 describes the hardware and software requirements for the products discussed in this Redbooks Solution Guide.

Table 2. Supported platforms for selected IBM Power Systems offerings

Product	Supported hardware	Software requirements
IBM Cloud Manager with OpenStack for Power V4.1	One of the following systems: ● IBM Power Systems server ● IBM BladeCenter server with IBM POWER® technology-based microprocessor	For operating system, database, runtime environment, user registry, browser, PowerVM, Hyper-V, KVM, IBM PowerKVM, IBM z/VM®, and VMware vSphere software requirements, see the IBM Cloud Manager with OpenStack for Power V4.1 Administrators Guide for detailed information: http://ibm.co/1sDhXWK
IBM PowerVC Express V1.2.1	Any IBM system that includes an IBM POWER7® or IBM POWER7+™ processor on a Power Server or IBM PureFlex® Foundation (build to order) that is classified as a small server and that is managed through IVM	Management server: RHEL Server version 6.4 and 6.5 for IBM Power or x86_64 For supported guest operating systems, see the following website: http://ibm.co/1uRu4tw
IBM PowerVC Standard V1.2.1	Any IBM system that includes an IBM POWER6®, POWER7, or POWER7+ processor on a Power Server or PureFlex Foundation (build to order) that is managed through HMC	Management server: RHEL Server, version 6.4 and 6.5 for IBM Power or x86_64 For supported guest operating systems, see the following website: http://ibm.co/1syVchf
IBM PowerKVM V2.1	Requires Power System scale-out servers 8247-21L or 8247-22L	Supported PowerLinux distributions are RHEL, SLES, and Ubuntu. For specific version information, see the following website: http://ibm.co/1qYWs1y
IBM PowerVM V2.2 (Express, Standard, and Enterprise)	IBM Power Systems server	IBM AIX, IBM i, and PowerLinux are supported guest operating systems. See the operating system documentation for minimum version requirements for specific hardware.

Ordering information

Ordering information is shown in Table 3.

Table 3. Ordering part numbers and feature codes

Program name	PID number	Charge unit description
IBM PowerVC Standard Edition V1.2.1	5765-VCS	Per processor core Small, Medium, or Large
IBM PowerVC Express Edition V1.2.1	5765-VCX	Per processor core Small, Medium, or Large
IBM Cloud Manager with OpenStack for Power V4.1	5765-OSP	Per processor core Small, Medium, or Large
IBM PowerVM Express v2.2	5765-PVX	N/A
IBM PowerVM Standard v2.2	5765-PVS	N/A
IBM PowerVM Enterprise v2.2	5765-PVE	N/A
IBM PowerKVM V2.1	5765-KVM	Per two sockets
Rack-mount Hardware Management Console V8.8.1.0	7042-CR8	N/A

Related information

For more information, see the following documents:

- IBM Offering Information page (to search on announcement letters, sales manuals, or both):
  http://www.ibm.com/common/ssi/index.wss?request_locale=en
  On this page, enter <*solution name*; remove angle brackets>, select the information type, and then click Search. On the next page, narrow your search results by geography and language.
- IBM Redbooks publication: IBM PowerVM Virtualization Managing and Monitoring, SG24-7590
  http://www.redbooks.ibm.com/abstracts/sg247590.html
- IBM Redbooks publication: IBM PowerKVM Configuration and Use, SG24-8231
  http://www.redbooks.ibm.com/abstracts/sg248231.html
- IBM Redbooks publication: IBM PowerVC Version 1.2.1 Introduction and Configuration, SG24-8199
  http://www.redbooks.ibm.com/abstracts/sg248199.html
- IBM Redbooks publication: IBM Power Systems HMC Implementation and Usage Guide, SG24-7491
  http://www.redbooks.ibm.com/abstracts/sg247491.html
- IBM Redbooks publication: IBM Power Systems Hardware Management Console Version 8 Release 8.1.0 Enhancements, SG24-8232
  http://www.redbooks.ibm.com/abstracts/sg248232.html
- IBM Redbooks publication: IBM SmartCloud: Building a Cloud Enabled Data Center, REDP-4893
  http://www.redbooks.ibm.com/abstracts/redp4893.html
- IBM PowerVM product page
  http://www.ibm.com/systems/power/software/virtualization/
- IBM PowerKVM product page

http://www.ibm.com/systems/power/software/linux/powerkvm/

- IBM PowerVC product page
  http://www.ibm.com/systems/power/software/virtualization-management/
- IBM Cloud Manager with OpenStack product page
  http://www.ibm.com/systems/x/solutions/cloud/cloud-manager-openstack/

Notices

This information was developed for products and services offered in the U.S.A.

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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. 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. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

This document was created or updated on December 17, 2014.

Send us your comments in one of the following ways:

- Use the online **Contact us** review form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at http://www.ibm.com/redbooks/abstracts/tips1240.html .

Trademarks