Redbooks

ibm.com/redbooks

IBM Spectrum Virtualize Considerations for PCI-DSS Compliance

Clarence Pouthier

Storage

IBM

Redpaper

Introduction

The Payment Card Industry Data Security Standard (PCI-DSS) is the global information security standard for organizations that process, store, or transmit data with any of the major credit card brands. More and more organizations are looking for compliance with this standard.

This IBM® Redpaper™ publication describes how the features and functions of IBM Spectrum™ Virtualize help organizations towards compliance of their IT infrastructure on relevant areas of the PCI-DSS standard.

IBM Spectrum Virtualize™ is the software common to all IBM Storwize® products, such as IBM SAN Volume Controller (SVC), IBM Storwize V5000 family, IBM Storwize V7000, IBM FlashSystem® V9000, and IBM Spectrum Virtualize as Software. Therefore, all recommendations in this paper equally apply to these storage products.

This paper includes the following sections:

- What is the PCI-DSS certification?
- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy
- Conclusion

What is the PCI-DSS certification?

Since 2004, the PCI-DSS standard applies to any financial services company, bank, or merchant that stores, processes, or even transmits payment card data over a network. This paper only considers requirements from *Requirements and Security Procedures, Version 3.2* published on April 2016 by the PCI-DSS Council.

To obtain this certification, an audit is performed by a qualified security assessor who has been issued a certificate from the PCI-DSS Council.

This audit examines all security measures that have been put in place in a company to provide a minimum security level for sensitive data.

Then, on an annual basis, a self-assessment is performed to maintain PCI-DSS compliance.

Note: It is important to notice that *no certification is issued by the PCI-DSS Council regarding any hardware or software solution.* Their audit is much wider than reviewing the technical solutions in place because it also deals with, for example, physical access to rooms where these technical solutions are installed and the company's own security guidelines.

The PCI-DSS audit focuses on several high-level areas that will be further developed in each relevant section (see Table 1).

Table 1 PCI-DSS standard and high-level overview

PCI-DSS Standard	Overview
Build and maintain a secure network	► Install and maintain a firewall configuration to protect cardholder data ► Do not use vendor-supplied defaults for system passwords and other security paramters
Protect cardholder data	► Protect stored cardholder data ► Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	► Protect all systems against malware and regularly update anti-virus software or programs ► Develop and maintain secure systems and applications
Implement strong access control measures	► Restrict access to cardholder data by business need to know ► Identify and authenticate access to system components ► Restrict physical access to cardholder data
Regularly monitor and test networks	► Track and monitor all access to network resources and cardholder data ► Regularly test security systems and processes
Maintain an Information Security Policy	► Maintain a policy that addresses information security for all personnel

More information about PCI-DSS can be found at the PCI Security website.

Build and maintain a secure network

This section describes the aspects that need to be taken into account with regards to firewall configuration over the network and authentication aspects on the system.

Install and maintain a firewall configuration to protect cardholder data

This section describes how the firewall must be configured to ensure the protection of data.

Control plane and data plane

Because IBM Spectrum Virtualize is a block storage solution, the control plane is independent from the data plane. Only a host that is connected to this solution has access to the data on the virtual volume it is mapped to. As a consequence, IBM Spectrum Virtualize administrators are unable to directly access stored data that gives IBM Spectrum Virtualize a clear isolation, or separation, between the control plane and the data plane.

However, because mapping a volume to another host can be achieved easily from the command-line interface (CLI) or graphical user interface (GUI), so another host could access the data. Therefore, set up role-based access credentials to reduce any hacking risk. This process is covered in “Identify and authenticate access to system components” on page 13.

Using an Ethernet firewall

In a case where you want to set up a firewall on the Ethernet network to improve security, you can restrict access to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports to restrict access to the IBM Spectrum Virtualize environment.

Table 2 lists all of the ports used by IBM Spectrum Virtualize. *Optional* means that, depending on the environment settings, these ports might or might not be blocked.

Table 2 IBM Spectrum Virtualize TCP/UDP used ports

Service	Traffic direction	Protocol	Port	Service type
Email (SMTP) notification and inventory reports	Outbound	TCP	25	Optional
SNMP event notification	Outbound	UDP	162	Optional
Syslog event notification	Outbound	UDP	514	Optional
IPv4 DHCP (Node service address)	Outbound	UDP	68	Optional
IPv6 DHCP (Node service address)	Outbound	UDP	547	Optional
Network time server (NTP)	Outbound	UDP	123	Optional
SSH for CLI access	Inbound	TCP	22	Mandatory
HTTP to HTTPS redirect for GUI access	Inbound	TCP	80	Optional
HTTPS redirect for GUI access	Inbound	TCP	443	Mandatory
HTTP to HTTPS redirect for GUI access	Inbound	TCP	8080	Optional

Service	Traffic direction	Protocol	Port	Service type
HTTPS for GUI access	Inbound	TCP	8443	Mandatory
CIMOM (HTTPS)	Inbound	TCP	5989	Optional
CIMOM SLPD	Inbound	UDP	427	Optional
Remote user authentication service - HTTP	Outbound	TCP	16310	Optional
Remote user authentication service - HTTPS	Outbound	TCP	16311	Optional
Remote user authentication service - Lightweight Directory Access Protocol (LDAP)	Outbound	TCP	389	Optional
iSCSI	Inbound	TCP	3260	Optional
iSCSI iSNS	Outbound	TCP	3260	Optional
IP Partnership management IP communication	Inbound	TCP	3260	Optional
IP Partnership management IP communication	Outbound	TCP	3260	Optional
IP Partnership data path connections	Inbound	TCP	3265	Optional
IP Partnership data path connections	Outbound	TCP	3265	Optional

Note: The web server for the GUI runs as a non-privileged process to enhance security.

Enabling Secure Sockets Layer

The Secure Sockets Layer (SSL) protocol aims to establish an encrypted session between a web server and a browser, so that any transmitted data (user credentials, for example) cannot be intercepted and decoded easily.

SSL is used in many places within IBM Spectrum Virtualize environment for these purposes:

- Opening a secure GUI session
- Connect to the SMTP server for call home
- Secure communication for external key management server for encryption
- Secure authentication to the LDAP server

By default, IBM Spectrum Virtualize uses a self-signed certificate to secure the browser connection. However, because it is self-signed, it might generate warnings on browsers and might not comply with the company security guidelines.

In cases where security guidelines require an SSL certificate signed by a certificate authority, a request can be made through the IBM Spectrum Virtualize GUI by clicking **Settings** → **Security** → **Secure communications**.

Change vendor-supplied defaults for system passwords and other security parameters

This section describes basic operations to secure passwords and connection to the administration interface (GUI and CLI) of the system.

Changing the superuser default password

In an IBM Spectrum Virtualize system, the *superuser* account is a local account. Even if the system's authentication is based on an external directory, such as LDAP for instance, this specific account will sign in with credentials stored locally on the system.

By default, the credentials are *superuser/passw0rd* (username/password). This password must be changed to comply with the PCI-DSS requirements. This change is particularly important because this default user is member of the SecurityAdmin group, which is the most privileged group role in the system.

Note: The *superuser* account cannot be removed from the environment. There is also no specific password policy in place, so ensure that only people with a specific business need can use this credential.

Changing the superuser's password can be done by issuing the **`chuser`** CLI command or by using the graphical user interface. The password can have up to 64 ASCII characters and must not start or end with a blank.

Configuring remote authentication

Adding remote authentication to the system allows you to define security enforcement policies in regards of the PCI-DSS directives and manage user accounts in a centralized directory of the company, such as:

- Password expiration every *nn* days
- Password length
- User revocation

IBM Spectrum Virtualize supports external authentication services based on these services:

- IBM Security Directory Server
- Microsoft Active Directory
- OpenLDAP

Note: A system can be connected to several directory servers, but they should all be of the same type.

In addition, Transport Layer Security (TLS) can be selected during setup to secure authentication exchanges between the system and the directory server.

Details on how to configure remote authentication can be found in *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V7.8*, SG24-7933.

Protect cardholder data

This section describes how to restrict access to cardholder data and how to protect that data when it is transmitted over a network.

Protect stored cardholder data

There are many ways to protect data in an IBM Spectrum Virtualize environment. However, this paper focuses on the different ways to protect access to the data itself rather than describing ways to back up that data on another system or replicate it on a disaster recovery site.

iSCSI hosts

IBM Spectrum Virtualize supports the Challenge Handshake Authentication Protocol (CHAP). This protocol aims for iSCSI initiators authentication before they can log in and access IBM Spectrum Virtualize resources (LUNs).

Basically, this authentication protocol is about sharing a secret between both storage system and servers. For example, if a host does not have the same secret as the one registered on the storage system, then login is denied.

Two different types of this protocol that are supported by IBM Spectrum Virtualize:

- One-way CHAP authentication where the target (IBM Spectrum Virtualize) authenticates the initiator (the server).
- Mutual CHAP authentication where both the initiator and the target authenticate each other.

The CHAP protocol can be set up on either on an IBM Spectrum Virtualize system basis or a per host basis.

On an IBM Spectrum Virtualize system basis, a CHAP secret is set up on the system side. That CHAP secret is then shared among all hosts that are connected through iSCSI. So, technically, if the storage administrator wants to remove access to a specific server, then they will also have to remove the CHAP secret on this server so that it cannot log in anymore.

On a per-host basis, this configuration means that each server that is connected to the storage system has its own CHAP secret that will be also registered into the host definition on the IBM Spectrum Virtualize system. In this case, if the storage administrator wants to remove a host access to the system, they must simply remove the host definition from the IBM Spectrum Virtualize system.

Thus, for the highest security level, enable mutual CHAP authentication on a per-host basis because it makes access management more efficient.

Note: CHAP authentication can also be used when configuring an IP partnership on a remote IBM Spectrum Virtualize system for replication purposes. It can also be used for storage virtualization through iSCSI since IBM Spectrum Virtualize 7.1.

Fibre Channel hosts

As a general statement, Fibre Channel (FC) hosts are not connected to Ethernet networks to access IBM Spectrum Virtualize resources. Rather, they are connected to SAN switches (except for iSCSI traffic, see “iSCSI hosts” on page 6).

There are only a few solutions to enhance FC traffic security from the host to the storage system:

- Data encryption done at the application layer or at the multipathing driver level might affect performance because extra memory and processor resources are needed to encrypt data.
- Data encryption done through a specific host bus adapter on servers that have specific hardware where the encryption algorithm runs.

Because of data-at-rest encryption, these two methods are being deployed less (see “Encryption” on page 7).

As a consequence, strictly applying SAN switches vendors best practices, such as one target and one initiator per zone, as well as correct zoning provides the environment security and best performance for traffic from the host to the storage system.

Encryption

Encryption is probably the most important security measure to implement to protect cardholder data.

IBM Spectrum Virtualize provides a licensed data-at-rest encryption capability. That capability means that data is encrypted in-flight as it is written on the disks by the IBM Spectrum Virtualize controllers, and not by the disks themselves.

Note: Encryption is not available for IBM Storwize V5010 models.

Data encryption uses the Advanced Encryption Standard (AES) algorithm that uses a 256-bit symmetric encryption key in XTS mode, as defined in the Institute of Electrical and Electronics Engineers (IEEE) 1619-2007 standard as XTS-AES-256.

The data encryption key is itself protected by a 256-bit AES key wrap when stored in non-volatile form.

Note: Only data at rest is encrypted. Replication and host-to-storage communication is not encrypted. For more information, see “Fibre Channel switch encryption” on page 9.

Key management is done either by supplying USB keys or a key management server, such as IBM Secure Key Lifecycle Manager, which supports the Key Management Interoperability Protocol (KMIP).

Encryption is implemented in two different ways depending on the configured environment and the IBM Spectrum Virtualize installation. It can be done either by the hardware itself (for internal disks), or by the software (for virtualized storage arrays). See Figure 1. In either case, the algorithms are the same. The encryption method cannot be selected manually.

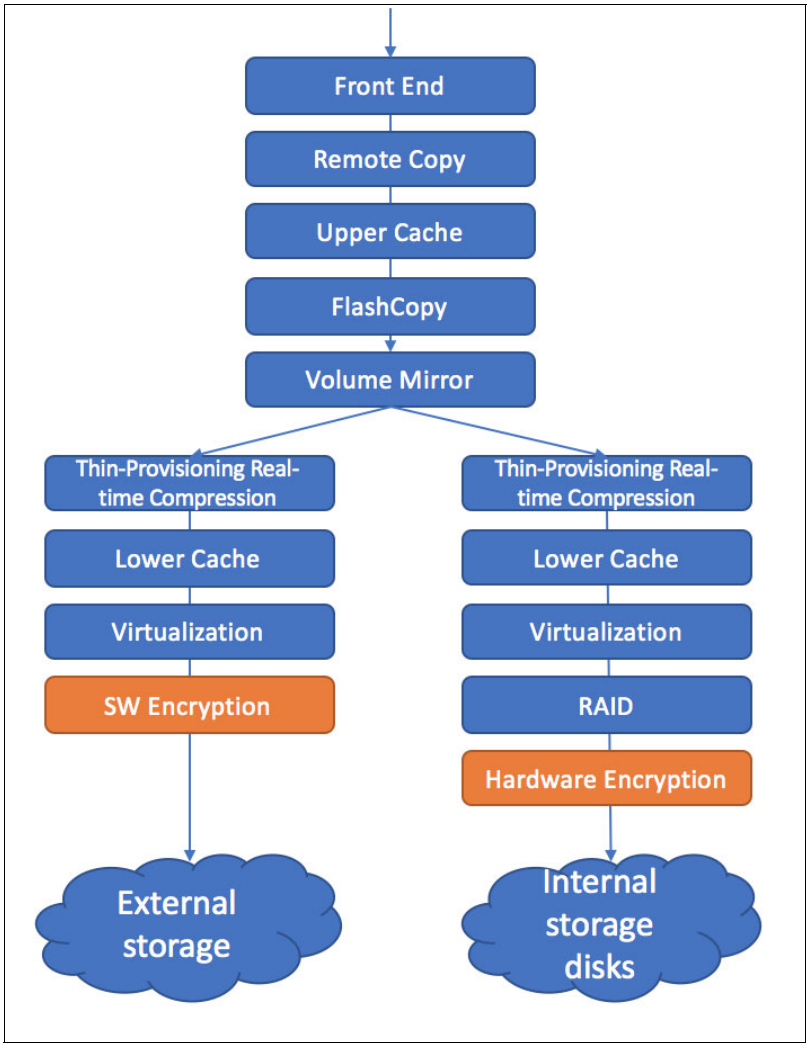

Figure 1 Encryption in the IBM Spectrum Virtualize software stack

For further in-depth information, see *Implementing the IBM Storwize V7000 and IBM Spectrum Virtualize V7.8*, SG24-7938, which provides a step-by-step guide to enable encryption on those systems.

Since V7.8, IBM Spectrum Virtualize also provides the ability through Transparent Cloud Tiering (TCT) to copy volume data to a public or private cloud storage provider. TCT is a licensed function and therefore will need encryption licenses to maintain PCI-DSS compliance.

Note: Encryption on cloud accounts is optional. You can choose to have an unencrypted cloud account with unencrypted cloud data if you want. Cloud accounts are unencrypted by default unless encryption is enabled, in which case they are encrypted by default. Encryption also requires a license.

The encryption mechanisms and algorithms are the same as the ones used for standard encryption, hence the need for encryption licenses.

Encrypt transmission of cardholder data across open, public networks

This section describes ways to encrypt data transmission over an FC network.

Fibre Channel switch encryption

PCI-DSS actively seeks to ensure that data is secure as it flows across the IT infrastructure, and this includes secure data transmission across the SAN.

As seen in “Fibre Channel hosts” on page 6, SAN encryption from hosts to storage systems is not easy to enable due to the constraints that it imposes on the physical environment. Therefore, this section focuses on switch-to-switch communication within fabrics, such as that for replication.

To enable Fibre Channel switch encryption, this feature needs to be available on the hardware along with proper licensing if required.

In large environments where the SAN architecture is based on a core/edge architecture, the first step to ensure security is to set up inter-switch link (ISL) FC encryption between the core switches and the edge switches as shown in Figure 2.

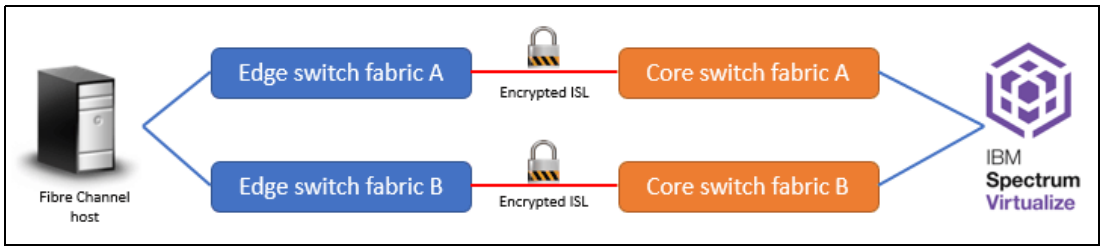

Figure 2 Fibre Channel ISL encryption in a core/edge SAN architecture

Moreover, security is even more important when using replication or an IBM Spectrum Virtualize stretched cluster implementation because these practices might require the use of third-party public networks.

In both architectures, the data traffic can flow using two different technologies:

- Fibre Channel over IP (FCIP): FC frames are encapsulated on TCP/IP frames.
- Dark fiber and dedicated fiber: FC frames generally travel through wavelength-division multiplexing equipment at each end and benefit from an optical network between each site.

Note: Because FCIP uses both Fibre Channel and TCP/IP protocols, LAN/WAN security measures must also be deployed on IP links that flow data between each site. This topic is beyond the intended scope of this paper because it varies depending on the equipment vendor and telecom facilities.

Figure 3 shows a typical implementation of encryption between two sites that are connected through an IP WAN.

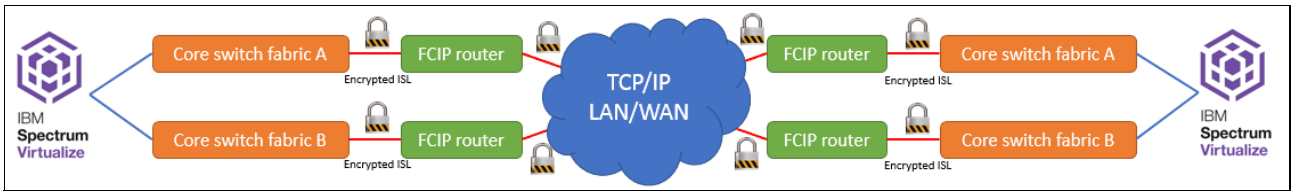

Figure 3 Typical FCIP encryption architecture

FCIP architectures are generally qualified as low-cost ones because an IP link between two sites is a lot cheaper than dark fiber. Moreover this technology provides an efficient way to keep costs lower by using compression on FCIP routers. Hopefully, enabling encryption will not have any effect on compression because vendors generally run a compression algorithm on FC frames and then use classical IP encryption techniques such as IPSec.

So, even if this kind of architecture requires a lot of configuration and knowledge, if we consider new network technologies such as 10 Gbps Ethernet and beyond, this kind of architecture will be more and more popular.

Using dark fiber is undoubtedly the best way to secure data transmission over a network because it will not mix heterogeneous technologies, such as those used for FCIP. Actually, the less complex is your architecture, the fewer security breaches it will generally have.

In such cases, no TCP/IP knowledge is involved. Wavelength-division multiplexing equipment, known as xWDM, are only responsible for multiplexing different wavelength on the same dark fiber by using colored optical transceiver modules (SFP). Therefore, independent virtual circuits extend the local SAN over a long distance.

Figure 4 shows a typical xWDM architecture using dark fiber to link both sites. Note that for illustration clarity, we have only represented one dark fiber. However, this architecture should be doubled for resiliency purposes.

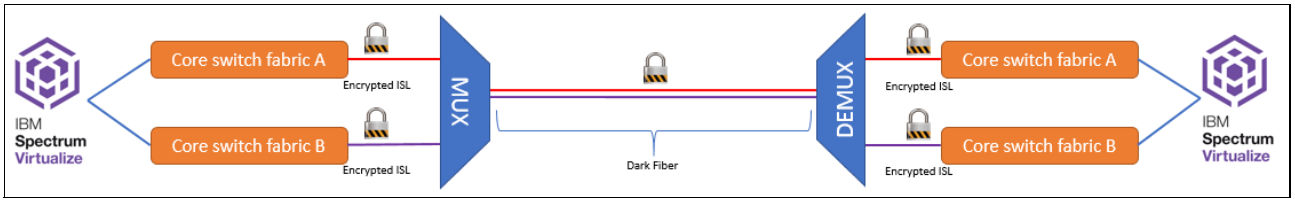

Figure 4 Typical xWDM architecture

Maintain a vulnerability management program

Meeting the vulnerability management program requirement can be achieved using best practices such as keeping the IBM Spectrum Virtualize up to date, but also through other security techniques and demonstrating that a secure methodology is applied during product development.

Protecting all systems against malware and regularly updating anti-virus software or programs

Use the techniques in this section to protect your systems.

Secure boot and read-only file system

To prevent IBM Spectrum Virtualize from booting on a potentially hacked code version, most of the file systems are checksummed. The checksums are checked at boot time. If they do not match, the system will not boot to prevent running potentially insecure code.

Moreover, to prevent any attacker from injecting malicious code lines within the system through any security breach, IBM Spectrum Virtualize code runs from a read only file system.

The combination of these two techniques prevents IBM Spectrum Virtualize from being infected by malware or viruses.

Update the system for latest fixes on security issues

Recent, well-documented attacks that have had huge repercussions for IT environments all over the world show us how security breaches can suspend production and business.

Updating IBM Spectrum Virtualize regularly is a common sense approach to ensuring security because new code releases not only bring new functionality, but also fix issues. Among these issues, there are likely to be security updates and fixes that will make the system even more reliable and secure.

New code releases and the release notes that detail the issues that are fixed are available from the IBM Support website (Fix Central).

Subscribe to IBM My notifications

IBM My Notifications is a powerful alerting center that you can subscribe to. It sends pro-active notifications of new and important technical support content about the products you have purchased, and relevant products that you add a subscription for.

Security issues, critical fix packs, operational warnings, good practices, and troubleshooting tips are some of the document types you can enable for these notifications.

Subscribing to IBM My notifications requires getting an IBM ID and then accessing the IBM Support site.

After you have logged in, click the profile icon in the top right of the page and select **My notifications** as shown in Figure 5.

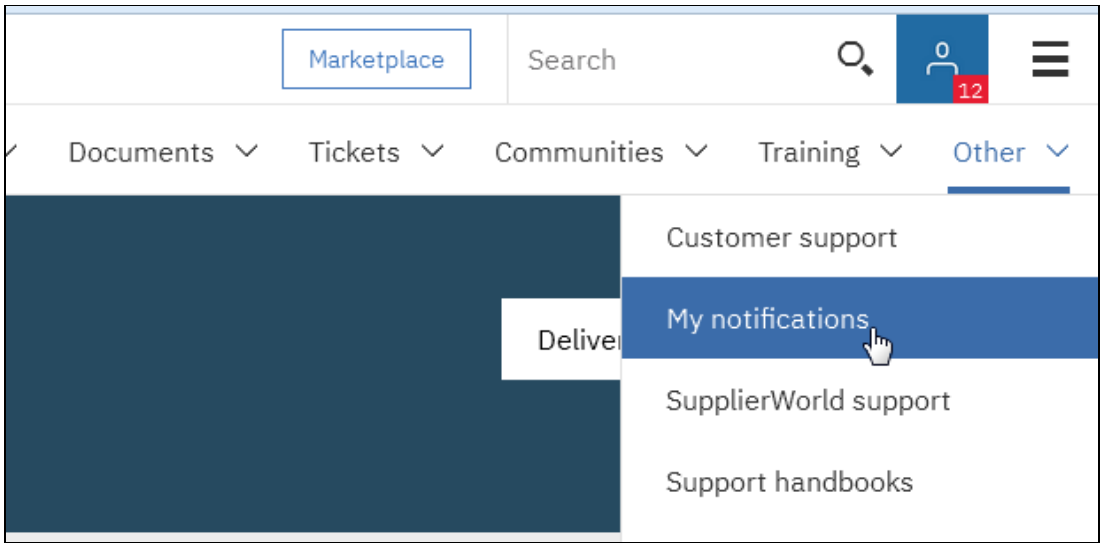

Figure 5 Access My notifications from the profile icon

In the **Product lookup** field, search for the product that you want to add to My notifications (Figure 6 is an example for IBM Spectrum Virtualize software) and then click **Subscribe**.

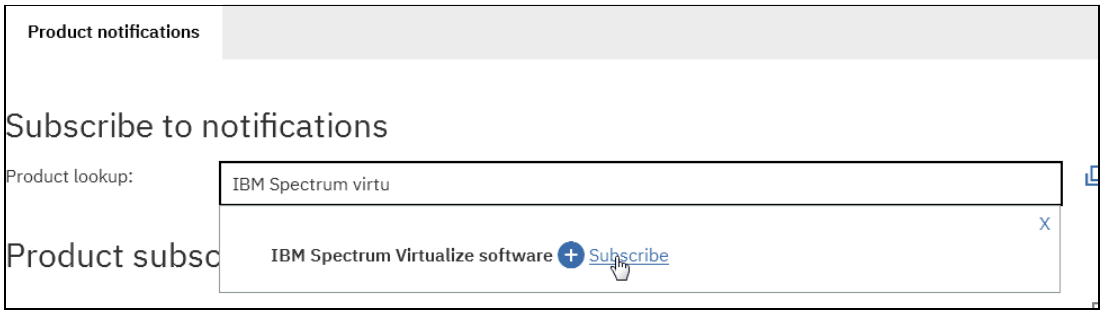

Figure 6 Subscribe to My notifications for IBM Spectrum Virtualize Software

After you are subscribed, the product is displayed in the list of IBM My notifications, and the ID used to configure IBM My notifications will receive all relevant alert emails.

Develop and maintain secure systems and applications

This section describes how to develop and maintain secure systems and applications.

IBM Secure engineering practices

The IBM Secure Engineering Framework reflects the best practices from across the company and directs our development teams to direct proper attention to security during the development lifecycle. These practices are intended to help enhance product security, protect IBM intellectual property, and support the terms of warranty of IBM products.

Secure Engineering is an important element of the overall IBM security strategy. It is reflected in our internal initiatives that work to address the dynamic nature of security in our development process. It is also reflected in our drive to meet the demand for high quality, high assurance business solutions, services, and Information Technologies for our customers and for our own operation.

The IBM Secure Engineering Framework is detailed in *Security in Development: The IBM Secure Engineering Framework*, REDP-4641.

Implement strong access control measures

This PCI-DSS requirement dictates how people within the company access cardholder data.

Restrict access to cardholder data based on business need to know

The company security policy should include a process to enable categorization of any individuals in terms of the privileges that they should be granted according to their job role, and then ensuring that only the privileges that are applicable are granted to them.

Identify and authenticate access to system components

IBM Spectrum Virtualize provides role-based access to the system for management purposes.

The *superuser* account is a member of the highest privileged group (*SecurityAdmin* in Table 3) and cannot be removed from the system. Therefore, change the default password immediately and restrict access to this credential to specific people as described in “Changing the superuser default password” on page 5.

By default, each role is associated to a user group. More user groups can be created and associated with one or more roles. However, any new role can be added in the system.

Table 3 Roles and default user groups

Default user group	Role	Comment on the role
SecurityAdmin	Security Administrator	Users can manage all functions of the system, including managing users, user groups, and user authentication. Security-administrator-role users can run any system commands from the CLI. However, they cannot run the **`sainfo`** and **`satask`** commands from the CLI. Only the superuser ID can run **`sainfo`** and **`satask`** commands.
Administrator	Administrator	Users can manage all functions of the system except those functions that manage users, user groups, and authentication. Administrator-role users can run the system commands that the security-administrator-role users can run from the CLI except for commands that deal with users, user groups, and authentication.

Default user group	Role	Comment on the role
RestrictedAdmin	Restricted Administrator	Users can perform the same tasks and run most of the same commands as administrator-role users. However, users with the Restricted Administrator role are not authorized to run the **rmvdisk**, **rmvdiskhostmap**, **rmhost**, or **rmmdiskgrp** commands. Support personnel can be assigned this role to help resolve errors and fix problems.
CopyOperator	Copy Operator	Users can start and stop all existing IBM FlashCopy®, Metro Mirror, and Global Mirror relationships. Copy-operator-role users can run the system commands that administrator-role users can run that deal with FlashCopy, Metro Mirror, and Global Mirror relationships.
Monitor	Monitor	Users have access to all system viewing actions. Monitor-role users cannot change the state of the system nor change the resources that the system manages. Monitor-role users can access all information-related GUI functions and commands, back up configuration data, and change their own passwords.
Service	Service	Users can set the time and date on the system, delete dump files, add and delete nodes, apply service, and shut down the system. Users can also complete the same tasks as users in the monitor role.
-	VASA Provider	Users with this role can manage VMware vSphere Virtual Volumes.

Restrict physical access to cardholder data

This PCI-DSS requirement is linked directly to the company's global security policies in terms of access to areas where cardholder data is stored.

Thus, physical access to data stored on the IBM Spectrum Virtualize environment cannot be restricted by IBM Spectrum Virtualize itself.

It is beyond the intended scope of this paper to describe all the techniques to restrict physical access. However, techniques such as access restriction to the physical rooms where the solution is installed, and installing the solution in a locked rack is a good place to start.

Hardware disposal, replacement, and secure erase

There are several places where data can be stored for I/O processing such as ROM, EPROM, RAM, DRAM, and NVRAM.

IBM has put in place specific processes and techniques to ensure that any user data kept or stored anywhere in the system is deleted to ensure that it cannot be accessed or otherwise compromised.

Your IBM representative should be contacted so that a “Statement of Volatility (SOV) and clearing procedures” document can be issued for the appropriate levels of hardware and software in the environment. This document provides all the necessary steps to securely erase all data from a system, and avoid any data being able to leave the secure data center by accident or design.

For replacement purposes, for example for a single disk (which is typically the most frequent case), data on this disk would not be readable if encryption has been enabled on the system. Encrypted data is written to the disk and the encryption key is not stored on the disk itself, so any disk replacement in a secured environment where encryption has been turned on is secure. Therefore, enable encryption to protect your data (see “Encryption” on page 7).

Regularly monitor and test networks

This section details how to monitor the IBM Spectrum Virtualize system to prevent, detect, or minimize the impact of data compromise and the techniques put in place to analyze vulnerabilities in the system.

Track and monitor all access to network resources and cardholder data

This section covers tracking and monitoring access to your resources and data.

Audit log

IBM Spectrum Virtualize logs any action commands that are run through the GUI or CLI session. It is a particularly useful tool to monitor past configuration events such as volume creation and deletion.

The audit log tracks the following information about a command:

- The user who issued the action command
- Name of the command
- Time stamp when the command was issued
- IP address from where the command was issued
- Command parameters

It is important to note that the audit log will not log a failed command, the result object ID of node type (for the **addnode** command), and views. Moreover, some specific commands will not be tracked:

- **dumpconfig**
- **cpdumps**
- **cleandumps**
- **finderr**
- **dumperrlog**
- **dumpintervallog**
- **svcservicetask dumperrlog**
- **svcservicetask finderr**

Note: The audit log is included in the **svc_snap** support data to help during problem determination. Under no circumstances will *any* cardholder data on the system be included in the snap package.

svcinfo catauditlog is a CLI command that provides the list of all the tracked action commands from the audit log. Through an external scheduled script, the audit log can be imported to a database if the company centralizes all audit logs from all equipment.

Regularly test security systems and processes

You should regularly test your security systems and processes. Running regular penetration tests is a requirement of the PCI-DSS certification process. However, it is also a good way to improve security within the environment as hacking techniques evolve and to guard against complacency.

There has always been some confusion between penetration tests and vulnerability tests. Typically a vulnerability test runs in a few seconds or minutes with automated tools. On the other hand, a penetration test first lists all vulnerabilities, and then identifies ways to exploit them. This difference makes a penetration test more complex and time consuming. This kind of test must be run at least yearly.

As covered in *Security in Development: The IBM Secure Engineering Framework*, REDP-4641, testing applications for security defects is an integral part of the software testing process.

Typically, IBM runs a first penetration test approximately three months before each major release's general availability (GA) and then a second follow-up before GA to ensure that any vulnerabilities found are fixed before the new version is released.

Obviously, because these tests cannot guarantee that the system will not be exposed to new hacking techniques in the future, customers can run their own penetration test on the IBM Spectrum Virtualize environment.

Note: For security reasons, the *root* password will *never* be communicated by IBM.

Maintain an information security policy

It is important that all individuals involved in handling cardholder data should be aware of the PCI-DSS requirements. Regular training should be provided and carried out to both new and existing employees.

Maintain a policy that addresses information security for all personnel

Any individual within a company should be aware of security risks. Risks are not linked only to hardware or software resources, but can be linked to people too.

Thus, for example, nobody must share their own credentials used to access a system as there might be malicious intent behind any such request. It could provide the attacker with privileged access that they would not have had with their own credentials.

Therefore, security is a matter of common sense for the overall company and information and education on this should be organized by the Chief Security Officer to raise awareness of this. It should ensure that people can stay up-to-date with potential and common security breaches, as well as defining their corporate responsibilities to security.

Conclusion

This document describes the techniques that IBM Spectrum Virtualize and Storwize have put in place during product development, and also techniques that any organization should put in place to secure their environment. Some of these techniques are not directly linked to IBM products. As a consequence, the list of recommendations in this paper is not as exhaustive as it could be concerning the entire environment. Remember that PCI-DSS applies to the environment and not a product. This document should be considered a basic security guide to satisfy specific PCI-DSS requirements as they relate to Spectrum Virtualize and Storwize.

Also, though this paper only deals with PCI-DSS standards, all the security facts and recommendations detailed might also apply to other regulatory standards.

Authors

This paper was produced by a team of specialists from around the world working at the IBM Hursley and Manchester Labs.

Clarence Pouthier is an IBM Certified Expert IT Specialist in the IBM Pan-Market technical sales team. He joined IBM in 2008 as an IBM Power Systems™ IT specialist for GTS after graduating with a Network and Security Master degree from Université Pierre et Marie Curie and Telecom Paris in France. In 2011, Clarence joined the French IBM Systems pre-sales storage team. His role became pan-European in 2015 covering a wide range of IBM storage offerings. Now, as an IBM Systems Data Architect within the Pan-Market technical sales team, he works closely with all client lines of business to assess data sources and develop the appropriate infrastructure building blocks to develop new workloads (analytics, machine learning, and artificial intelligence).

Jon Tate is a Project Manager for IBM System Storage® SAN Solutions at the International Technical Support Organization (ITSO), San Jose Center. Before joining the ITSO in 1999, he worked in the IBM Technical Support Center, providing Level 2/3 support for IBM mainframe storage products. Jon has over 30 years of experience in storage software and management, services, and support, He is an IBM Certified IT Specialist, an IBM SAN Certified Specialist, and is Project Management Professional (PMP) certified. He is also the UK Chairman of the Storage Networking Industry Association.

Jon was the project manager for this paper.

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

Paul Cashman
Connor Fawcett
Robin Findlay
Steve Randle
Bill Scales

Martyn Spink
James Whitaker
IBM Systems

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 ITSO 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

Stay connected to IBM Redbooks

- Find us on Facebook:

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

  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new IBM 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

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.

FlashCopy®
IBM®
IBM FlashSystem®
IBM Spectrum™
IBM Spectrum Virtualize™
Power Systems™
Redbooks®
Redpaper™
Redbooks (logo)  ®
Storwize®
System Storage®

The following terms are trademarks of other companies:

Microsoft, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

REDP-5453-00

ISBN 0738456365

Printed in U.S.A.