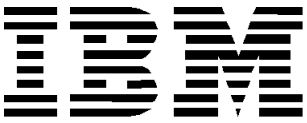
IBM® Storage

IBM Spectrum Virtualize, IBM FlashSystem, and IBM SAN Volume Controller Security Feature Checklist



Contents

Executive summary

IBM Spectrum® Virtualize based storage systems are secure storage platforms that implement various security-related features, in terms of system-level access controls and data-level security features.

This document outlines the available security features and options of IBM Spectrum Virtualize based storage systems. It is not intended as a “how to” or best practice document. Instead, it is a checklist of features that can be reviewed by a user security team to aid in the definition of a policy to be followed when implementing IBM FlashSystem®, IBM SAN Volume Controller, and IBM Spectrum Virtualize for Public Cloud.

IBM Spectrum Virtualize features the following levels of security to protect against threats and to keep the attack surface as small as possible:

- The first line of defense is to offer strict verification features that stop unauthorized users from using login interfaces and gaining access to the system and its configuration.
- The second line of defense is to offer least privilege features that restrict the environment and limit any effect if a malicious actor does access the system configuration.
- The third line of defense is to run in a minimal, locked down, mode to prevent damage spreading to the kernel and rest of the operating system.
- The fourth line of defense is to protect the data at rest that is stored on the system from theft, loss, or corruption (malicious or accidental).

The topics that are discussed in this paper can be broadly split into two categories:

- System security

  This type of security encompasses the first three lines of defense that prevent unauthorized access to the system, protect the logical configuration of the storage system, and restrict what actions users can perform. It also ensures visibility and reporting of system level events that can be used by a Security Information and Event Management (SIEM) solution, such as IBM QRadar®.

  These security features include, but are not limited to:

  - Multifactor authentication (MFA)
  - Role-based access control (RBAC)
  - Object-based access control (OBAC)
  - Disabling access to the command-line interface (CLI), graphical user interface (GUI), and Representational State Transfer (REST) interface
- Data security

  This type of security encompasses the fourth line of defense. It protects the data that is stored on the system against theft, loss, or attack. These data security features include, but are not limited to, encryption of data at rest (EDAR) or IBM Safeguarded Copy (SGC).

This document is correct as of IBM Spectrum Virtualize version 8.5.0.

System security capabilities

For the purposes of this document, the term *system* is used to mean any platform that runs the IBM Spectrum Virtualize software, including all IBM FlashSystem 5000, 7000, 9000 and IBM SAN Volume Controller products, and IBM Spectrum Virtualize for Public Cloud. Where applicable, code levels are supported, which also relates to the IBM Storwize® family of products.

Physical security measures must be implemented in accordance with organizational mandates in addition to the logical, network, and hardware features that are discussed in this publication.

The system is designed to limit the number and means of user access to a restricted set of known, policed, and secured access points.

User authentication

An authenticated user is required to administer, configure, and monitor the system. The system supports the following types of users:

- Local

  These users are defined on the system and managed internally by the system. The system supports up to 200 or 400 local users, depending on your platform.

- Remote

  These users are defined on an external authentication server. Remote users can be defined in an external Lightweight Directory Access Protocol (LDAP) repository, such as Microsoft Active Directory. The details of the LDAP server and groups must be configured on the system.

Remote authentication

Remote authentication allows users to authenticate to the system by using credentials that are stored on an external authentication service. When you configure remote authentication, users do not need to be configured on the system or assigned more passwords. Instead, passwords and user groups that are defined on the external authentication service are used. This mechanism can be used to separate user management from storage management.

A remote user is authenticated on a remote server that implements LDAPv3. A remote user does not need to be added to the list of users on the system, although they can be added to configure optional SSH keys. Remote users have their groups defined by the remote authentication service. User groups must be created locally on the system to reflect the group names, and their roles, that are defined by the remote authentication service.

LDAP authentication is only a replacement for “first factor” authentication for local users. It is possible to have native LDAP authentication enabled for first factor authentication. Then, native MFA can be configured to provide second factor authentication.

In contrast, with single sign-on (SSO), the system delegates all authentication (first and second factor) to the remote Identity Provider/SSO service. However, unlike LDAP (which can authenticate logins by way of all interfaces), SSO can be used only to authenticate logins by using the GUI.

For more information, see this IBM Documentation web page.

Role Based Access Control

A local user can be assigned to a single user group on the system. The system supports up to 256 user groups. Each user group is assigned a role that is associated with a set of privileges and commands that can be run.

The following roles are available:

- Monitor

  Users with this role can view all objects, but cannot manage the system or its resources. Support personnel can be assigned this role to monitor the system and to determine the cause of problems. This role is suitable for use by automation tools, such as the Storage Insights data collector for collecting status about the system.

- Copy Operator

  Users with this role have monitor role privileges and can create, change, and manage all Copy Services functions (Remote Copy and IBM FlashCopy), but cannot create consistency groups or modify host mappings.

- FlashCopy Administrator

  Users can create, change, and delete all the FlashCopy mappings and consistency groups, and create and delete host mappings.

- Administrator

  Users with this role can access all functions on the system, except those functions that involve managing users, user groups, and authentication. This standard role is assigned to users who administer the system and perform tasks, such as provisioning storage.

- Security Administrator

  Users with this role can access all functions on the system, including managing users, user groups, all aspects of security, and user authentication.

- Service

  These users can delete dump files, add and delete nodes, apply service, and shut down the system. These users also can perform the same tasks as users in the Monitor role.

- Restricted Administrator

  Users with this role can perform the same tasks as the Security Administrator role, but are restricted from deleting specific objects. Support personnel can be assigned this role to solve problems.

- 3-Site Administrator

  Users with this role can configure, manage, and monitor 3-site replication configurations by using specific command operations that are available only on the 3-Site Orchestrator. This role is the only role that is intended to be used with the 3-site orchestrator.

- VASA Provider

  Users with this role can manage virtual volumes (VVOLs) that are used by VMware vSphere and managed by using IBM Spectrum Connect software.

For more information, see this IBM Documentation web page.

Default users

Upon creation, the system defines a single local Security Administrator user that is called *superuser*. For newly created systems, the default superuser password must be changed on first login. Although this user cannot be deleted or configured for remote authentication, it can be disabled.

During initial setup, the suitable users for the system are defined. After this process is complete, the default superuser can be disabled. This user can be reenabled with physical access to the system only by using the technician port, by another user with the Security Administrator role, or by a support engineer that uses remote support assistance (RSA).

If a SIEM solution is used, consider forwarding the system audit log so that the SIEM system can be triggered when this action occurs.

Some CLI commands and service procedures are available that can be performed only by the superuser. If the superuser account is disabled, it might be necessary to temporarily re-enable the account occasionally.

If you choose not to disable the superuser account, ensure that the highest level of protection is afforded to the superuser account. For example, use a strong password, limit the knowledge of the password, and configure multi-factor authentication.

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

- The chuser command
- The chsecurity command
- Password policy

Object-Based Access Control

In addition to role-based access control, other restrictions can be implemented on a per-user group basis to limit the set of objects that users can view, manage, and configure. For example, you might configure two different groups of administrators: the first group is limited to provisioning storage to test or development systems; the second group can provision storage to production systems.

OBAC can be used to separate parts of the system between users; for example, different storage administrators can administer different pools of storage. OBAC also can be used by managed service providers to implement a form of multi-tenancy between multiple clients that are hosted on the same system.

Role-based and object-based access control can be configured simultaneously and provide two different ways of enforcing least privilege by restricting what users can do on the system.

Ownership groups are used to maintain groupings of users and objects. Only users with the Security Administrator role can define ownership groups.

Access to the following objects can be controlled by using an ownership group:

- Child pools
- Volumes
- Volume groups
- Hosts
- Host clusters
- FlashCopy® mappings
- FlashCopy consistency groups

- User groups
- Port sets

The system supports up to 64 ownership groups.

For more information, see this IBM Documentation web page.

Login interfaces

The system provides a CLI, GUI, and a REST application programming interface (API), all of which authenticate users and allow them to administer the system. All interfaces implement data in-flight encryption to secure the login and all subsequent interactions with the system.

Command-line interface

Users log in to the CLI by using an SSH client terminal window. Logging in to the system by using a terminal places the user in a highly restricted shell. For example, the user cannot run a change directory command and can run only the commands that are designated by IBM as required to administer the system.

Consider the following points:

- This login interface can be disabled on a per-user group basis.
- This login interface cannot be disabled for superuser.

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

- UNIX commands available in interactive SSH sessions
- Command-line interface
- Changing user groups

Graphical user interface

Users log in to the GUI is by way of a Hypertext Transfer Protocol Secure (HTTPS) connection from Transport Layer Security by using a supported web browser.

You can install certificates that are signed by a certificate authority (CA) with the suitable certificate chain. The system supports the following system certificate key types:

- RSA 2048-bit
- ECDSA 384-bit
- ECDSA 521-bit

The system presents the installed system certificate and chain to web browsers when they connect to the system.

This login interface can be disabled on a per user group basis.

By default, the superuser is exempt from disabling this interface. To disable this interface for the superuser, run the **chsecurity -disablesuperusergui yes** command.

The system currently supports a single certificate that is shared by the GUI, Encryption Key servers, IP Quorum, CIMOM, and Rest API interfaces.

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

- Managing certificates for secure communications
- Changing user groups

Representational State Transfer API

The system provides a REST model API. This interface is accessed by using an HTTPS connection. The REST API implements a full function list that is equivalent to the CLI interface.

Connections to the REST API can be made only by using a suitable authenticated user, for which a session token is generated. The session timeout, the elapsed time before the user or application must reauthenticate can be defined in the security policy. The RBAC and OBAC user restrictions are enforced.

This login interface can be disabled on a per-user group basis.

By default, the superuser is exempt from disabling this interface. To disable this interface for the superuser, use the **`chsecurity -disablesuperuserrest yes`** command.

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

- Spectrum Virtualize RESTful API
- Changing user groups

Password Policy

The Security Administrator can define a set of policies regarding all users on the system. This set of attributes can be tailored to match your organizational mandates about password rules.

The following attributes can be defined:

- Minimum password length (6 - 64 characters)
- Minimum number of uppercase characters (1 - 3)
- Minimum number of lower-case characters (1 - 3)
- Minimum number of special characters (1 - 3)
- Minimum number of digits (1 - 3)
- History check (0 - 10) before password reuse
- Password expiry (0 - 365 days)
- Password expiry warning (0 - 30 days): Displayed on CLI at login only
- Password age (1 - 365 days): Minimum age before password can change
- Force change on next login: One time option by Security Administrator

The force password change on next login can be used to keep a newly created user account deactivated until the user logs in for the first time.

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

- Password policy
- The chsecurity password

Account locking

The Security Administrator can manually lock or unlock a user account at any time. In addition, the following system-wide policies can be set:

- Automatic lock after (0-10) consecutive failed login attempts

  A value of 0 means that the account does not lock because of failed login attempts.
- Set length of time auto-lock applies for (0-10080) minutes (7 days maximum)

  A value of 0 means that the account remains locked out indefinitely.
- Superuser account can be locked from general login

By default, the superuser is exempt from the system-wide policy for manual or automatic account locking. To apply this policy to the superuser, use the **`chsecurity -superuserlocking enable`** command.

The superuser is the only user account that can run service assistant commands. Special care must be taken to not lose access. Before adding security controls to the superuser, it is recommended to review the documentation and form a plan for recovering access and reenabling the superuser.

For more information, see this IBM Documentation web page.

Session timeouts

The CLI and GUI can include defined independent session timeouts. These timeouts can be 5 - 240 minutes.

The REST interface also can include a defined token session timeout of 10 - 120 minutes.

The grace time for SSH sessions can be configured to specify the duration of time a user must authenticate per SSH connection before the connection is terminated (15 - 18000 seconds).

The maximum number of login retries that can be attempted per single SSH session also is configurable (1 - 10 attempts).

For more information, see this IBM Documentation web page.

Login banner

A customizable login banner can be modified to match your organizational requirements and display on the CLI or GUI login window before logging in.

For more information, see this IBM Documentation web page.

Multifactor authentication

The system supports the configuration of multifactor authentication. Two different methods are available to configure multifactor authentication: by using the native multifactor authentication feature, or by configuring single sign-on and then, using a multifactor authentication solution that integrates with your single sign-on identity provider.

As of this writing, native multifactor authentication requires IBM Security™ Verify cloud-based software as the authentication service, which can be configured to enforce a wide range of other authentication options. The system connects to the multifactor authentication service by using the industry-standard OpenID Connect protocol.

After multifactor authentication is enabled system-wide, it can be enabled on a per-user group basis.

Note: By default, the superuser is exempt from the default user group's multifactor authentication setting. To enable multifactor authentication for the superuser, use the **`chsecurity -superusermultifactor yes`** command.

The superuser is the only user account that can run service assistant commands. Special care must be taken not to lose access. Before adding security controls to the superuser, it is recommended to review the documentation and form a plan for recovering access and reenabling superuser.

Multifactor authentication is not supported on the REST API. Use user groups, roles, and user group access controls to disable REST API access for higher privileged users, while having less privileged users with REST enabled for monitoring and automation.

For more information, see this IBM Documentation web page.

Single sign-on

The system supports the configuration of single sign-on. The system connects to the Identity Provider by using the industry standard OpenID Connect protocol and supports the following services:

- Microsoft Active Directory Federation Services (AD FS): On-premises
- Microsoft Azure AD: Cloud-based
- IBM Security Verify: Cloud-based

After single sign-on is configured, it can be enabled on a per-user group basis. Single sign-on is *not* supported for local user accounts (including superuser) because it requires the delegation of all authentication to an external Identity Provider (IdP).

Single sign-on applies only to logins to the GUI and does *not* apply to the CLI or REST interfaces. If you have any local users on the system, it is recommended to disable CLI and REST access for those user groups or enable the "password and key required" feature, which enforces CLI users to provide a password (something you know) and public key (something you have) during authentication.

For user accounts that are used for monitoring and automation, it is recommended not to enable passwords. Instead, put these users in a separate user group so they can be assigned different access controls. Also, assign these users the least privileged role that is required for the functions that they are performing.

For more information, see this IBM Documentation web page.

Auditing and reporting

The system includes an internal tamper-proof audit log that can be viewed and exported if required. The internal audit log traces all successful configuration command execution on the system, along with details of the user, where they connected from (IP address), and date/time stamps.

The system also can send audit information to an external server by using syslog or SNMP.

When the audit log is exported, more information is provided. In addition to logging successful configuration commands, unsuccessful configuration commands are logged. The exported audit log also can include entries for successful and attempted logins by using the GUI, CLI, or REST interfaces.

For more information, see this IBM Documentation web page.

Secure and trusted boot

Secure boot encrypts the file systems and relies on a hardware root of trust that extends all the way through to the operating system and initrd to unlock the file system.

The system checksums and validates the file systems at boot time to protect against system files and executables being corrupted (maliciously or by hardware or software faults).

For more information, see this IBM Documentation web page.

Secure sockets and Secure Shell settings

Secure sockets (SSL/TLS) and Secure Shell (SSH) are used to establish authenticated and encrypted connections to the system for management interfaces, such as the GUI, CLI, REST, and when the system connects to remote servers, such as email, LDAP, or external key managers. Secure sockets and Secure Shell define a set of protocols, cipher suites, and key exchange algorithms that can be used.

When a connection is established, the local and remote system negotiates which protocol, cipher, and key exchange algorithm is used. Some users might want to restrict the permitted choices to increase security by disabling algorithms that provide weaker security.

The system defines levels of security for secure sockets and SSH. The lower levels implement a wider choice of algorithms to maximize compatibility. The higher levels restrict the choice of algorithms to provide higher levels of security, but might be incompatible with older software.

Note: Systems that created on older software versions and upgraded over time might still use weaker protocol levels. Each level must be considered carefully and set according to your current security requirements, and adjusted over time as your requirements change or newer levels are added.

Consider the following points:

- SSL security levels are 1 - 4; the default for new systems is level 3.
- SSH security levels are 1 - 2; the default for new systems is level 2.

For more information, see these IBM Documentation web pages:

- Changing SSL/TLS/SSH levels for the system using the CLI
- Security levels and supported security ciphers

SSL/TLS certificates

SSL certificates are used for various of secure communications, including the following examples:

- GUI
- Encryption key servers
- IP quorum
- Common Interface Model - Object Manager (CIMOM)
- REST API

When a system is initially configured, a default self-signed certificate is generated. Users replace the self-signed certificate with one that contains more information or generate a certificate request, get the certificate signed by a certificate authority (CA) and then, install the certificate. The system certificate must be configured before features and interfaces are used.

The system raises a warning event 30 days before the system certificate expires. Another alert event is raised after it expires.

For more information, see this IBM Documentation web page.

Disabling USB ports

For companies with security policy that restricts the use of USB ports, these ports can be disabled on a per-node basis on systems with a supported BIOS. After the ports are disabled, they are electronically disabled at the BIOS level and are rendered non-operational.

This feature can be combined with encryption key management on local USB flash drives to keep the ports disabled during day-to-day use and only reenabled when a key must be provided.

For more information, see this IBM Documentation web page.

Network Time Protocol

To mitigate against attacks that are based on the system time/date being out of sync with other services, the system supports a configurable Network Time Protocol (NTP) server to control the system time. An NTP server can be configured only by a user with the Security Administrator role.

For more information, see this IBM Documentation web page.

IP address and network port allocation: Network firewall considerations

The system uses several IP addresses for management, iSCSI, and other secure interfaces.

If specific interfaces or features are not used, access might need to be disabled by using firewall rules that are provided by the network team. Similarly, if specific interfaces are to be used, ensure that the firewall rules are set correctly.

Alternatively, a proxy server can be configured on the system to manage connections between your internal network and any entity outside of your network.

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

- IP address allocation and usage
- Defining an HTTP proxy server

Internal software execution protection mechanisms

The IBM Spectrum Virtualize software runs on a hand-picked Linux installation with a bare minimum of carefully selected packages. The kernel configuration is locked down and tightly controlled. Only software that is required for the interaction between the hardware and the IBM Spectrum Virtualize software is installed.

By limiting the packages that are installed and preventing the installation of extra packages, many operating system vulnerabilities are prevented from affecting the system.

Preventing access as root

On traditional Linux installations, a user with `root` privileges can perform any system action and bypass any security control.

The `root` access is not permitted on the system. Logging in as `root` is not permitted by way of the network, console, or any other back-door methods.

The management software in the system runs as an internal Linux user, without `root` privileges. Although external users cannot access this software, an attacker might leverage a weakness to compromise the system. Even in this circumstance, they do not have root privileges.

File system protection

Secure boot encrypts the file systems and relies on a hardware root of trust. The boot drives are tied to the Trusted Platform Module chip.

Checksums and validation of the file systems at boot time provide security against files and executables being corrupted maliciously or by hardware or software faults.

Most file systems are mounted as read-only; the others are mounted with `'noexec'`, `'nosuid'`, and `'nodev'` attributes to minimize security risks.

New software can be installed only by using the built-in software update technology. All software packages are validated and must be signed by a private key that is held within IBM servers. This configuration ensures that the tight control on software is maintained for all systems that are deployed at customers.

These techniques are used to prevent an attacker from running arbitrary code, which is a prerequisite for most security vulnerabilities. They also minimize the attack surface as possible.

Disabling service assistant password reset

The superuser is the only user account that is permitted to run service assistant commands on the system. When the superuser password is lost, the following methods can be used to reset the password:

- Gaining physical access to the system and inserting a suitably prepared USB flash drive to run the **`resetpassword`** command.
- The use of another SecurityAdmin user on the system to change the superuser password
- Connecting physically by way of the technician port and selecting **Reset Superuser Credentials** in the service assistant GUI.
- The use of the remote support assistant feature to allow the engineer with RestrictedAdmin role to log in to the system by way of a challenge/response and then, reset the password.

For organizations with a security policy that requires this ability to be disabled, the password reset feature can be disabled on a per-system basis. After this ability is disabled, it is no longer possible to reset the superuser password.

To view the status of the password reset feature, use the **`setpwdreset -show`** command. To disable the password reset feature, use the **`setpwdreset -disable`** command. To enable the password reset feature, use the **`setpwdreset -enable`** command.

Note: Care must be taken when disabling the superuser password reset feature. If the superuser password is lost and is unrecoverable, and if the superuser password reset feature was disabled, the superuser cannot be accessed and IBM Support *must* be engaged.

The recovery procedure is disruptive and involves system downtime.

For more information, see this IBM Documentation web page.

Data security capabilities

The system provides external access to data by way of the SCSI, iSCSI, SAS, or NVMe-based protocols over your chosen SAN network connectivity. It is assumed that this physical connectivity is secured by using normal data center means.

In this section, the extra data security features that are provided by the system are discussed.

Encrypting data at rest

All NVMe drives that are supported by the system, including IBM FlashCore® Modules (FCMs) and a range of other third-party drives, are self-encrypting drives (SEDs) that encrypt data within the electrical circuit of each individual drive.

NVMe SEDs automatically lock on power loss and require unlocking by using an access key. On systems with encryption enabled, the individual SED access keys are protected by the overall system master key. Despite NVMe drives being automatically self-encrypting, a well-known access key is used to protect the SEDs if encryption is disabled system-wide. That is, the data that is stored at rest is not protected from physical theft.

As of this writing, the IBM FlashCore Modules are FIPS 140-2 Level 2 validated and undergoing FIPS 140-3 validation.

When drives are connected by way of the Serial Attached SCSI (SAS) network, the SAS protocol chip provides data encryption capabilities. The system uses a PMC Sierra PM8073 SPCve+ 12G chip, which uses algorithms that are compliant to FIPS 140-2 Level 1.

This data encryption capability allows all data at rest (on the drive) to be stored as encrypted, and in all cases is applied after data reduction technologies.

All data encryption keys (DEKs) and key encryption keys (KEKs) on the system are AES-256bit keys. Data encryption keys are used to perform AES-XTS, and all keys are protected by using an AES wrap key.

The IBM Spectrum Virtualize software also can apply encryption to devices that do no support in-built encryption. This ability mainly applies to the IBM SAN Volume Controller product in which you can use IBM SAN Volume Controller to virtualize (and hence encrypt) underlying storage that does not support encryption (for example, external storage that is connected by using other protocols, such as Fibre Channel or iSCSI). The system uses FIPS-compliant data encryption algorithms to perform software-based encryption.

To enable encryption of data at rest, some form of key management must be configured. Key management can be handled by the system (with the use of local USB flash drives) to manage master keys, or by an external key management server (with the use of IBM GKLM, SafeNet KeySecure or Thales CipherTrust Manager). Conversion between these two mechanisms is possible.

Alternatively, both key management methods can be enabled simultaneously, which keeps local USB flash drives as a backup method for urgent scenarios in which the key server might be disabled.

For more information, see this IBM Documentation web page.

Secure Erasure

Drives that are still functional and are being retired or returned can be erased by using a secure erase function. This erase can be cryptographic, block erase, or data over-write, and is determined by the drive type that is used.

NVMe drives use the industry-standard NVMe Sanitize and NVMe Format commands. Support can vary between different drive models.

For more information, see this IBM Documentation web page.

Volume delete protection

The system can be enabled with volume delete protection. This feature can be configured at the system-wide or pool/child pool level.

Volume delete protection prevents any user from deleting a volume if the system received read or write I/O requests for the volume within the defined period. The Security Administrator can set the period 5 minutes - 24 hours.

For more information, see this IBM Documentation web page.

Safeguarded copy: Immutable snapshots

The system provides a mechanism to set a policy on a group of volumes to enable automated immutable snapshot volumes to be taken at regular intervals. These volume snapshots cannot be read from or written to by any host system. A restore or recovery of a safeguarded copy must be performed before access is granted.

Users cannot delete or modify immutable snapshots.

An external REST API is available to trigger instant immutable copies by using an external scheduler tool; for example, if your SEIM tool detects an immanent security threat.

Safeguarded copy can be combined with the IBM CyberVault architecture to build a fast recovery environment in the case of ransomware attacks.

For more information, see this IBM Documentation web page.

Logical port isolation

In addition to traditional SAN Fabric zoning mechanism, the system provides means to define logical port sets. These port sets can be used to further restrict the login traffic from a host, or set of hosts, to isolate traffic to specific SAN paths.

IP-based Ethernet and Fibre Channel-based port sets can be defined.

For more information, see this IBM Documentation web page.

Authors

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

Bill Scales is a distinguished engineer for IBM Systems and is based in the IBM Hursley Lab, UK. He has over 25 years of experience with IBM storage and is one of the architects for the IBM Spectrum Virtualize products.

Barry Whyte is an IBM Master Inventor working in the IBM Systems Group. Based in Auckland, New Zealand, Barry is an IBM Advanced Technical Specialist team member, covering storage across the Asia Pacific region. Barry primarily works with the IBM Spectrum Virtualize (IBM SAN Volume Controller, IBM Storwize, and IBM FlashSystem) family of virtual disk systems. Barry graduated from The University of Glasgow in 1996 with a B.Sc (Hons) in Computing Science. In his 23 years at IBM, he has also worked on the successful Serial Storage Architecture (SSA) and the IBM DS8000® products. Barry joined the IBM SAN Volume Controller development team soon after its inception and has held many positions before he took on the role as performance architect.

James Whitaker is a software engineer for IBM Systems based in the IBM Manchester Lab, UK. He has 10 years of experience designing, developing, and testing IBM Spectrum Virtualize. He also has worked on various software features and hardware platforms across the portfolio. In his current role, he is the technical lead of the team that is responsible for delivering new security and encryption features.

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 FlashCore®
IBM FlashSystem®
IBM Security™
IBM Spectrum®
QRadar®
Redbooks®
Redbooks (logo)  ®
Storwize®

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

VMware, VMware vSphere, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

March 2022

Please recycle

ISBN 0738460435

REDP-5678-00