Advanced
Technology
Group

IBM Storage Virtualize 8.5.3/8.5.4 Technical Update
IBM Storage Sentinel Update

Byron Grossnickle
ATG Senior Brand Technical Specialist – Storage Virtualize SME
byrongro@us.ibm.com

Est. 2003

SVC20

20 years of
Storage Virtualization

Meet the Speakers

Byron Grossnickle is an IBM Storage Technical Specialist concentrating on Storage Virtualize software. This include FlashSystem, SVC, and Storage Virtualize for Public Cloud. Byron has been with IBM 18 years exclusively in storage. Prior to working for IBM, Byron spent 6 years engineering storage in the Telcom Industry. Prior to that he worked 8 years in healthcare IT. Byron lives in the Kansas City area and is available to travel to customer engagements.

Agenda

- Long Term Support Release/Continuous Development Release
- Brief 8.5.3 Update
- 8.5.4 Update
- VMware Plugin Update
- IBM Storage Sentinel Update

Continuous Dev Release (CDR)
Long Term Release (LTR)

- There are 4 slated updates each year
- One LTR
  - New features
  - Has a formal announcement
  - Has all the enhancements of the previous CR's
  - Major numbering scheme (8.4,8.5,8.6….)
  - Will get all PTF's of problems found with existing features going forward
- Three CDR's
  - New features
  - No formal announcement
  - Can present NDA to client after Tech Update
  - All features public knowledge after eGA
  - PTF's will generally be added to the next CR unless critical

Advanced
Technology
Group

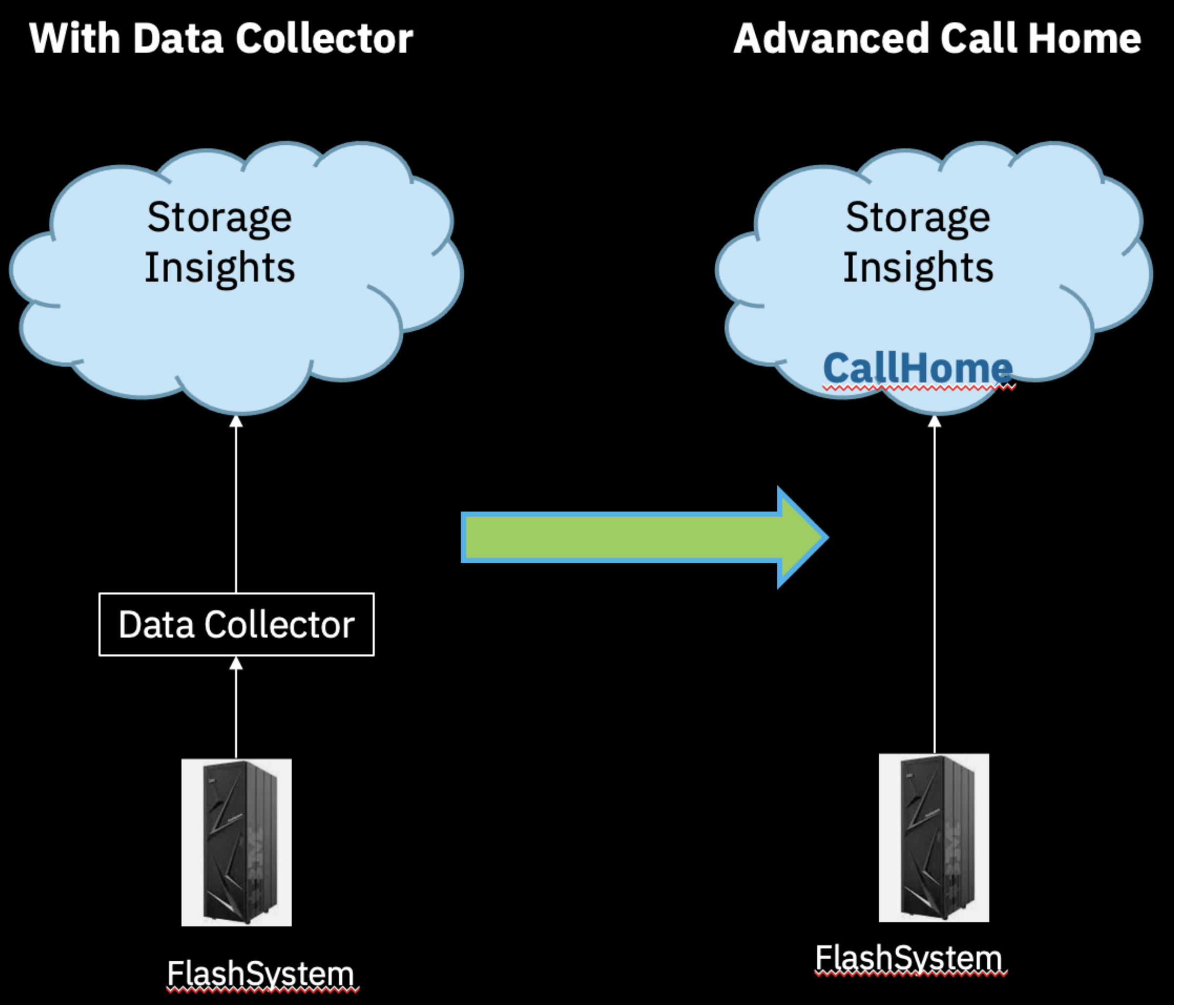
Storage Virtualize 8.5.3 Brief Updates
December 16, 2022

Advanced Call Home – No more data collector requirement

Allow Spectrum Virtualize customers to monitor their storage environment without having to download and deploy a Storage Insights data collector.

This will reduce the time to value by:

- Not having to obtain a virtual machine.
- Not having to download and deploy software.
- Not having to configure additional firewall rules.
- Not having to undergo the security process necessary to deploy and run third-party software connected to the cloud.
- No data collector to maintain and upgrade.
- More SI adoption and more SpecV sales, competitive advantages e.g. Pure systems



Advanced Call Home Caveats

- Currently, there is no way to convert an existing system from the data collector to Advanced Call Home without deleting it and re-adding it to Storage Insights
  - This would lose all the saved data
  - A migration method that would retain existing system data is planned
- Cannot be used in conjunction with data collector on the Storage Virtualize system
- Can only send data to one instance of Storage Insights

- Advanced call home is for Storage Virtualize systems only
- Other products still require the data collector
  - DS8000
  - COS
  - Scale/ESS
  - SAN Switches
  - Third Party Arrays
  - Etc.

New in Storage Virtualize 8.5.3

- The Storage Virtualize system has an internal root certificate authority which can be used to sign the system certificate
- An alternative to third-party CAs (public CAs or corporate CAs).
- The internal CA provides the same resiliency as using a third-party CA with regard to security warnings and continuity of service
- Automatic renewal of certificates
- A system that upgrades to 8.5.3 will continue to use the self-signed certificate until it expires or is renewed
- A new system on 8.5.3 will generate a system certificate that is signed by the certificate authority.
- The options to generate a new self-signed certificate on 8.5.3 have been hidden from the user.

Pre-8.5.3 options	8.5.3+ options
Self-signed certificate	Internal CA-signed certificate
External CA-signed certificate	External CA-signed certificate

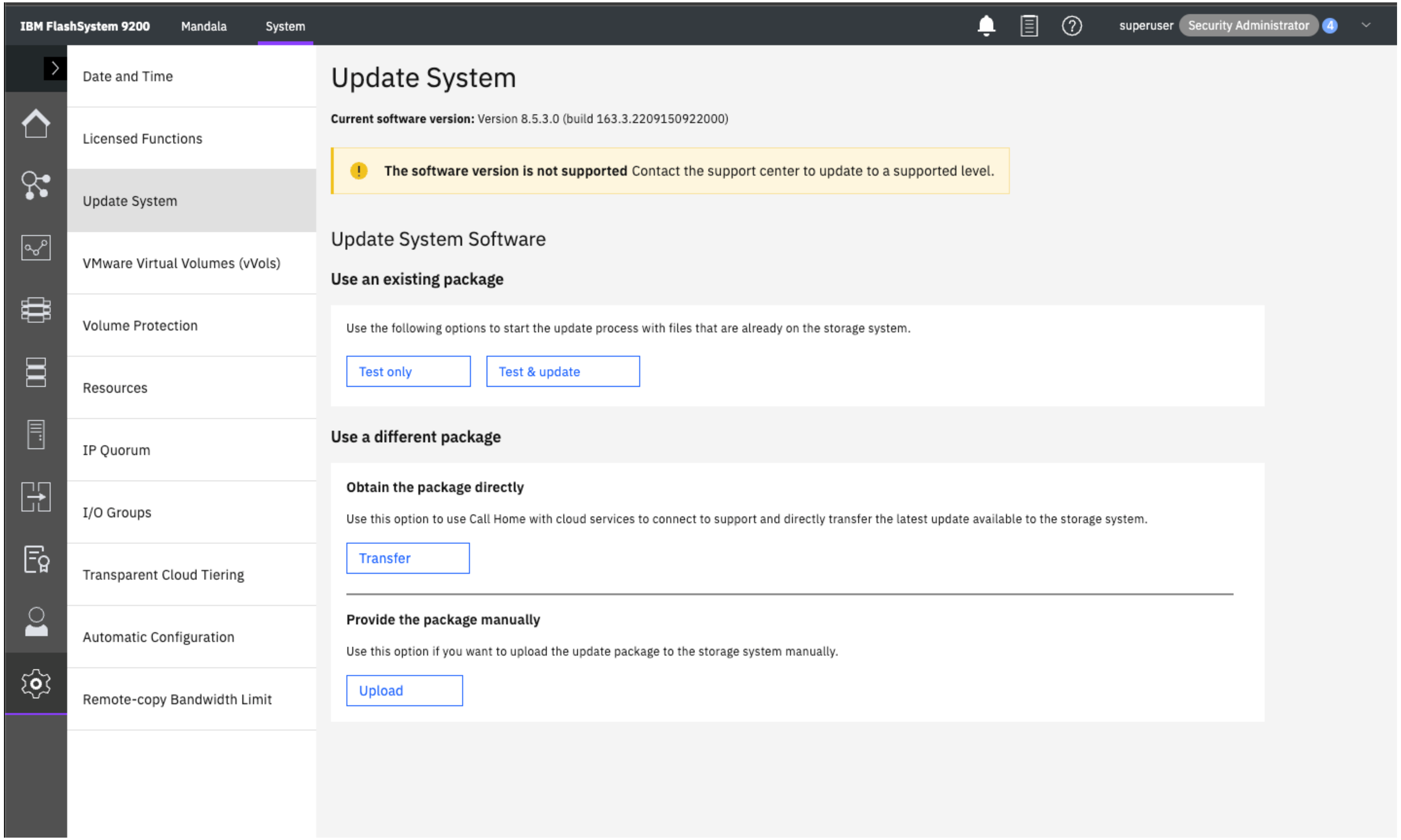
Exceptions

- With 8.5.3 root certificates will be traded, except in the following cases

  Multifactor Authentication with IBM® Security Verify uses the system certificate to sign JSON web tokens (JWTs). The system certificate must be exported and added as a signer certificate in the IBM Security Verify interface. If the system certificate expires or is renewed, access to the management GUI will be unavailable until the new system certificate is installed in IBM Security Verify. A user must use the CLI to log in to the system to export the new system certificate and install it in IBM Security Verify.

  IBM Security Guardium® Key Lifecycle Manager key servers do not currently support chain of trust checking with Storage Virtualize. The system certificate must be installed on the IBM Security Guardium Key Lifecycle Manager key servers in order to establish a connection. If the system certificate is expired or renewed, then the new system certificate must be installed on the key servers in order for IBM Storage Virtualize to establish a connection with the key servers. Access to encrypted storage is not disrupted while the connection to the key servers is unavailable, unless all nodes in the clustered system are powered off and on at the same time. Chain of trust will be supported in future versions.

Code Download Directly From IBM



Update System

Current software version: Version 8.5.3.0 (build 163.3.2209150922000)

The software version is not supported Contact the support center to update to a supported level.

Update System Software

Use an existing package

Use the following options to start the update process with files that are already on the storage system.

Use a different package

Obtain the package directly

Use this option to use Call Home with cloud services to connect to support and directly transfer the latest update available to the storage system.

Provide the package manually

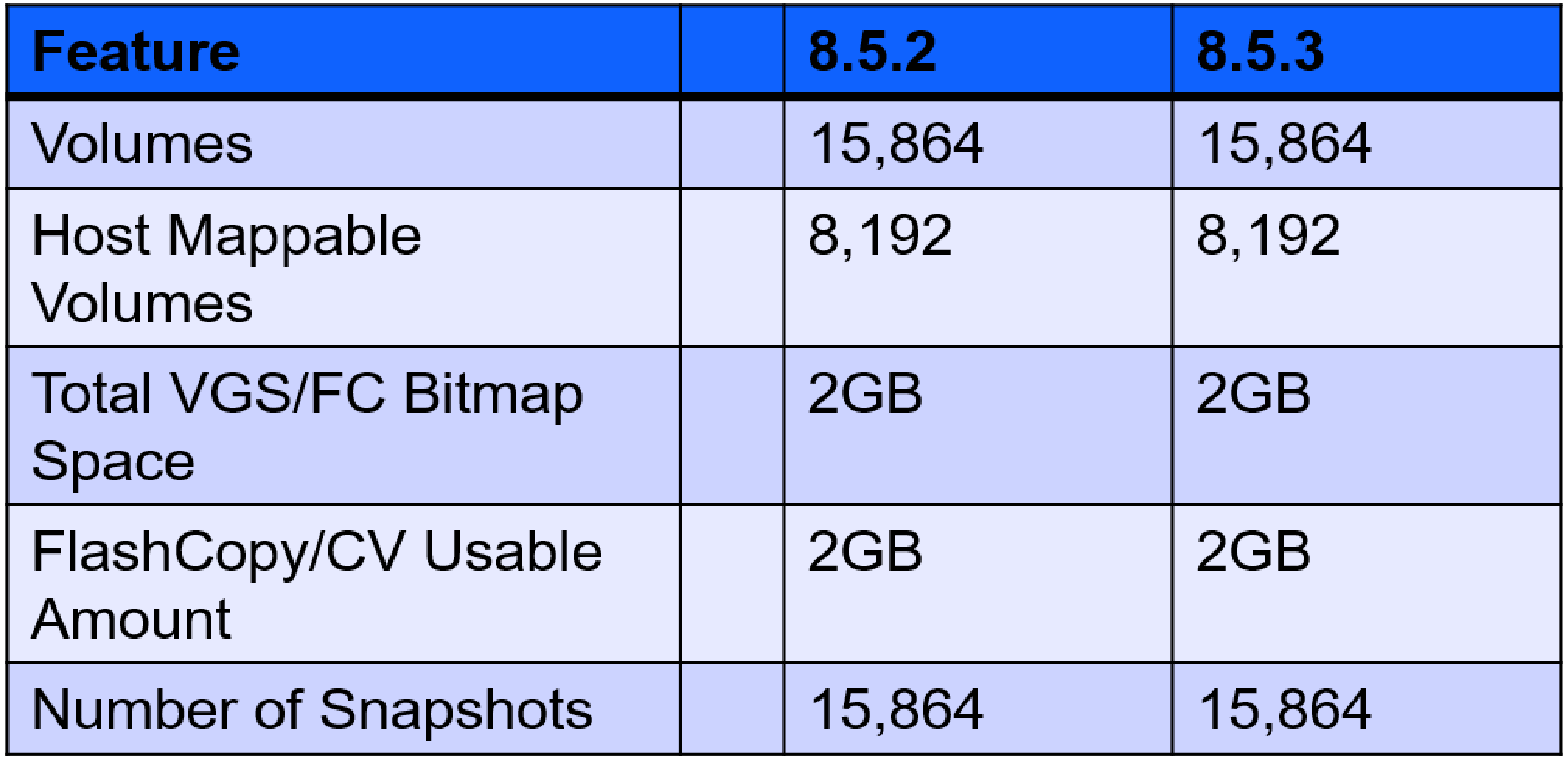
Use this option if you want to upload the update package to the storage system manually.

Transparent Cloud Tiering – What is Changing

- Cloud snapshot and Volume Group Snapshots can be enabled together on volume(s)/group(s)
- This allows to create interleaved Cloud Snapshots (TCT backups) and Volume Group Snapshots of production volume

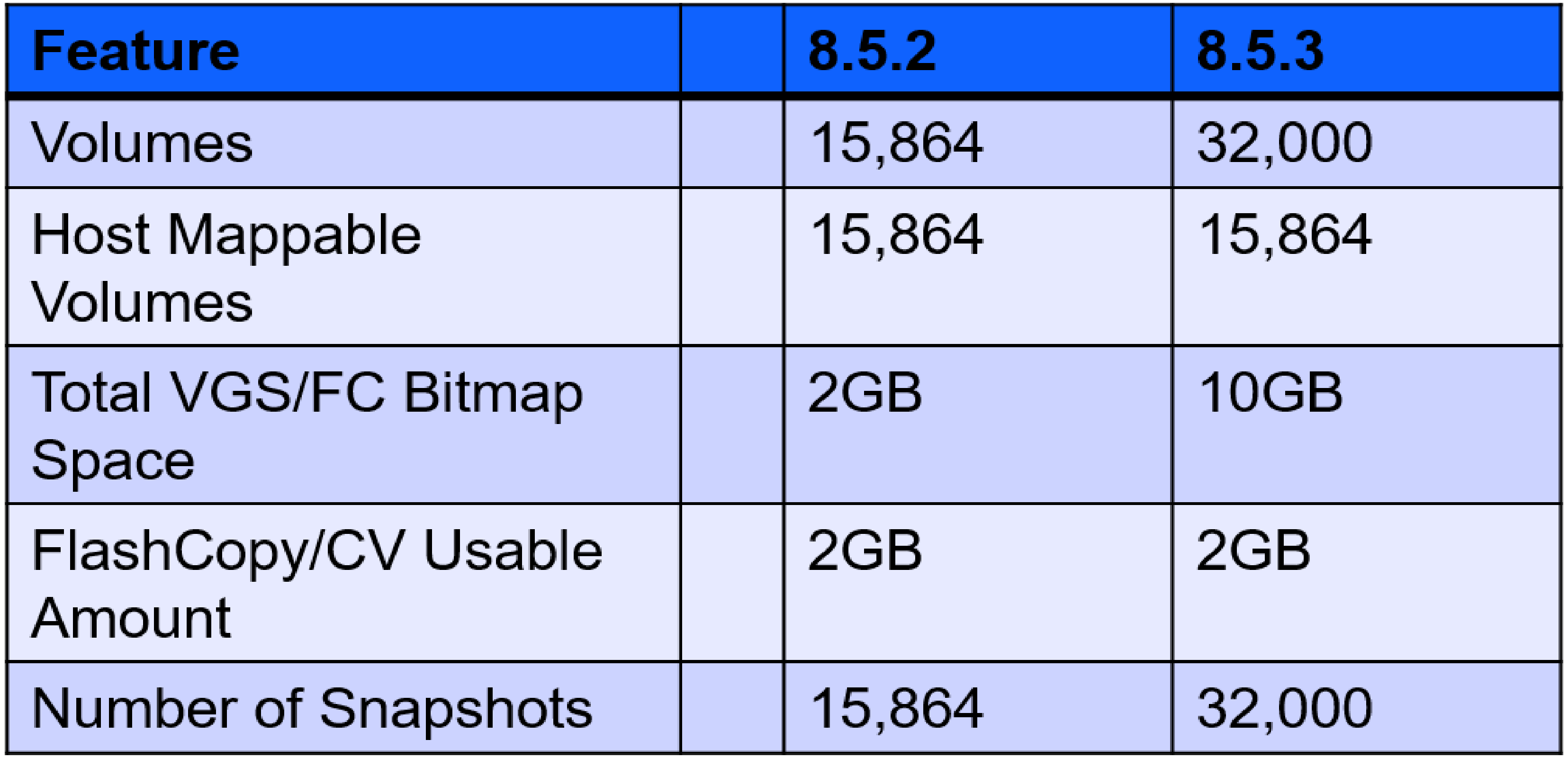
- Use Cases
- Volume Group Snapshots - short term retention of the volume copies on-prem.
- Cloud snapshots - long term retention of volume copies on low-cost object store.

FS5200 Volume Count/Bitmap



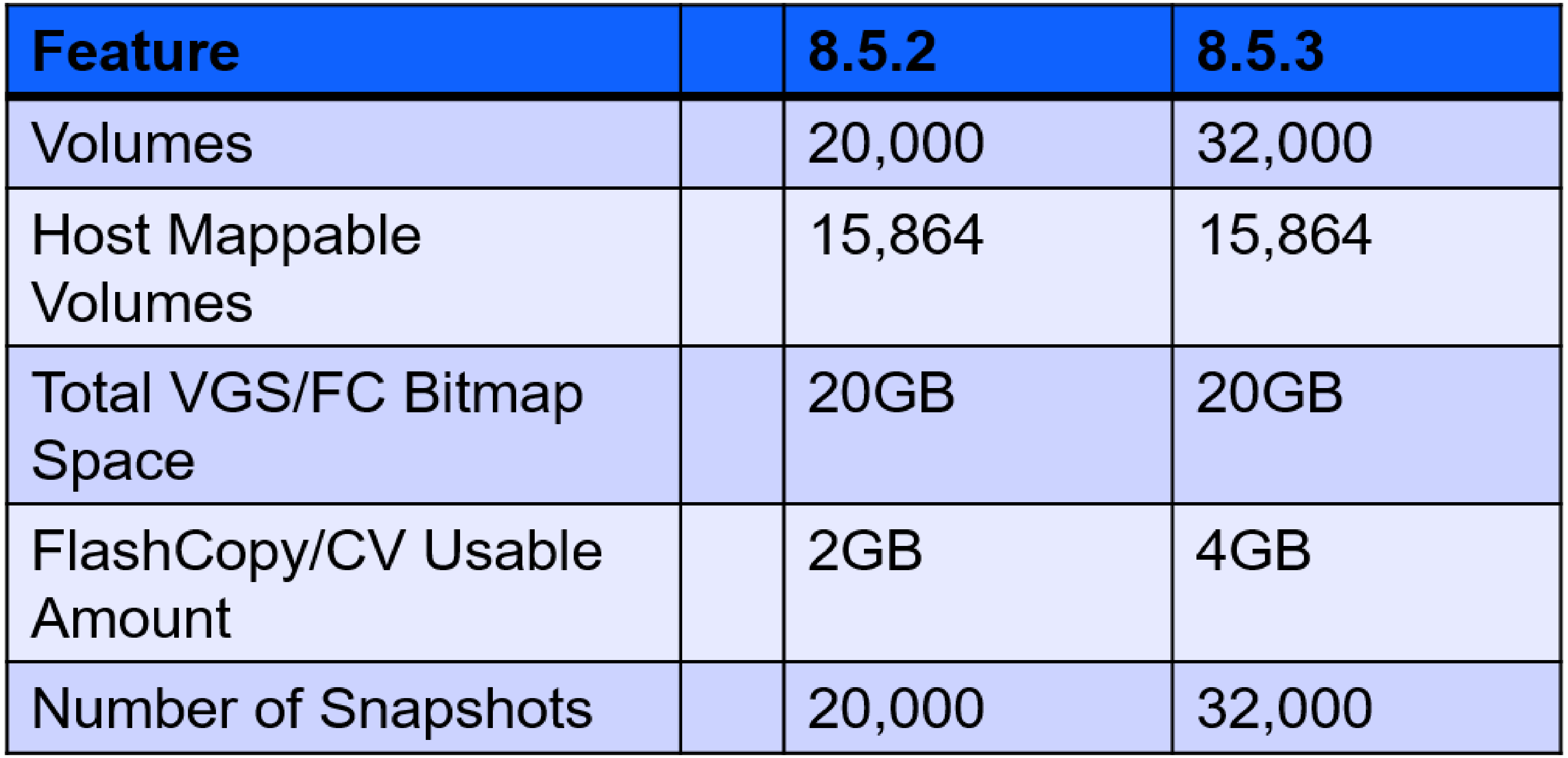
Feature		8.5.2	8.5.3
Volumes		15,864	15,864
Host Mappable Volumes		8,192	8,192
Total VGS/FC Bitmap Space		2GB	2GB
FlashCopy/CV Usable Amount		2GB	2GB
Number of Snapshots		15,864	15,864

FS7300 Volume Count/Bitmap



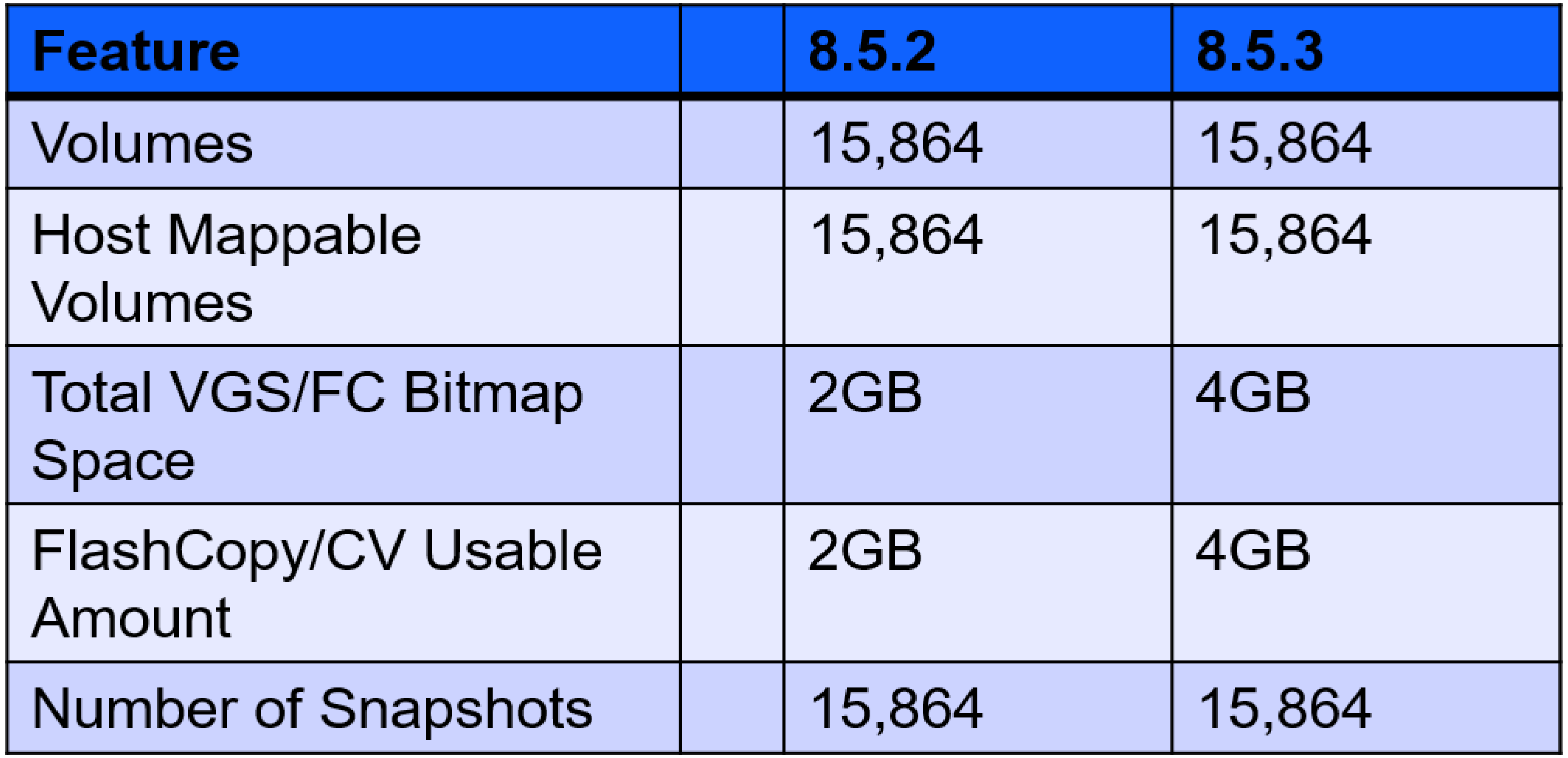
Feature		8.5.2	8.5.3
Volumes		15,864	32,000
Host Mappable Volumes		15,864	15,864
Total VGS/FC Bitmap Space		2GB	10GB
FlashCopy/CV Usable Amount		2GB	2GB
Number of Snapshots		15,864	32,000

FS9500 Volume Count/Bitmap



Feature		8.5.2	8.5.3
Volumes		20,000	32,000
Host Mappable Volumes		15,864	15,864
Total VGS/FC Bitmap Space		20GB	20GB
FlashCopy/CV Usable Amount		2GB	4GB
Number of Snapshots		20,000	32,000

SV3 Volume Count/Bitmap



Feature		8.5.2	8.5.3
Volumes		15,864	15,864
Host Mappable Volumes		15,864	15,864
Total VGS/FC Bitmap Space		2GB	4GB
FlashCopy/CV Usable Amount		2GB	4GB
Number of Snapshots		15,864	15,864

Direct Storage Controller Attachment

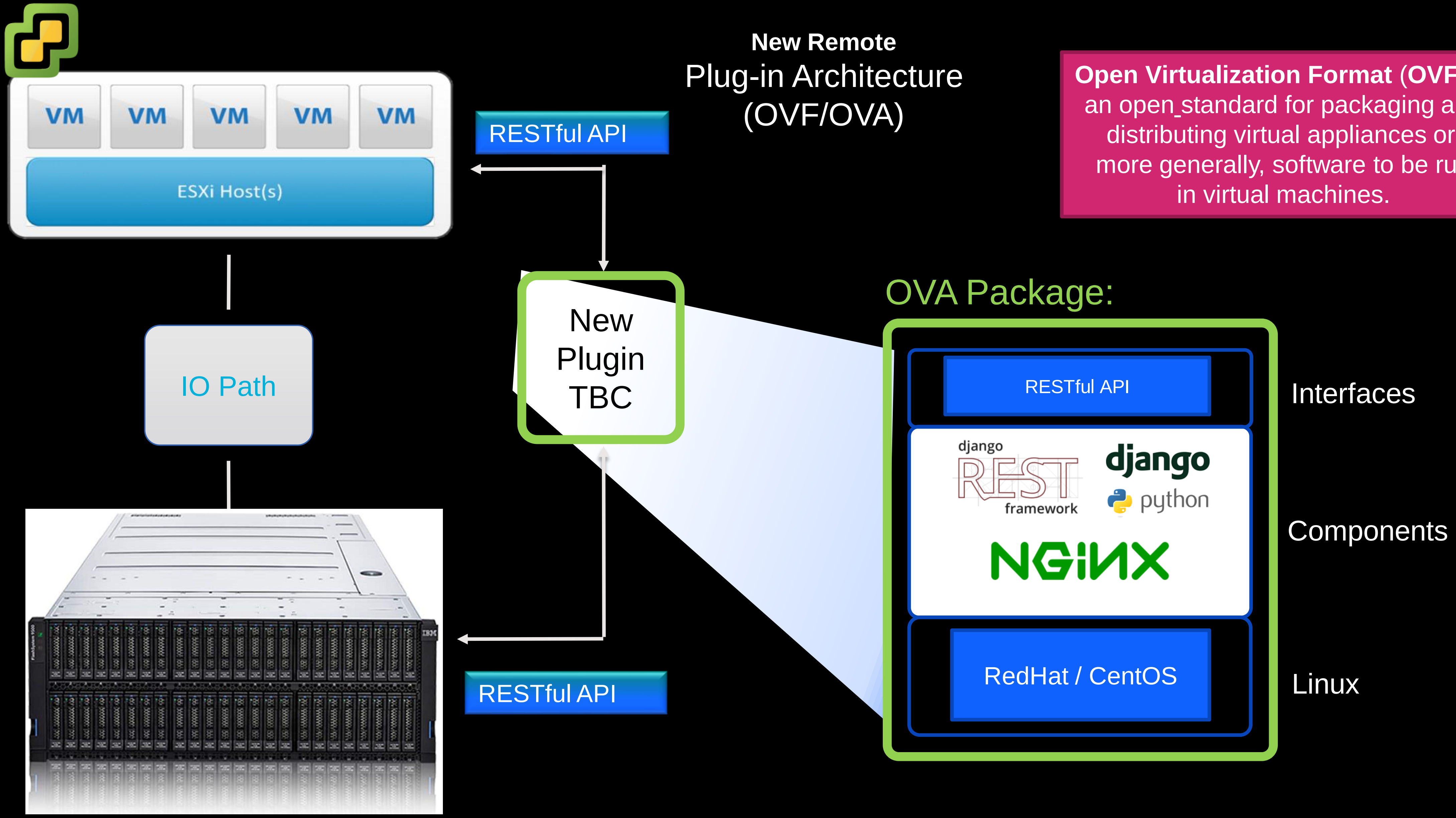
- Virtualized storage controllers were designed to be attached to a Storage Virtualize system via a SAN switch and controllers that show more than 1 WWNN currently log 1627 errors when they are directly attached to a Storage Virtualize system
- With 8.5.3 there will be a controller command to tell each controller you are direct attaching storage controllers.
- The default will be no unless the user changes this parameter
- This change is non-disruptive

- chcontroller -directattachenhanced yes // enable direct attach mode
- chcontroller -directattachenhanced no // disable direct attach mode

Overview of New vSphere Client Plug-In

New Remote
Plug-in Architecture
(OVF/OVA)

Open Virtualization Format (**OVF**) is an open standard for packaging and distributing virtual appliances or, more generally, software to be run in virtual machines.



VM VM VM VM VM

ESXi Host(s)

RESTful API

IO Path

New Plugin TBC

RESTful API

OVA Package:

RESTful API

Interfaces

Components

RedHat / CentOS

Linux

IBM Storage vSphere Plugin Info

- The plugin will support existing installations of Storage Virtualize platforms running 8.4.2+
- Development will happen quickly with updates coming quarterly
- Not tied to Storage Virtualize development unless support for new features is needed
- If the customer’s vCenters are in linked mode, one instance of the plugin will service all linked vCenters.
- If the customer’s vCenters are standalone, then you need an instance of the plugin per vCenter

Advanced
Technology
Group

IBM

Storage Virtualize 8.5.4 Updates
March 24, 2023

IBM

List of Features

Two Person Integrity

Non-Disruptive Security/Software Patches

TCT Support for Azure Blob Storage

AWS 8.5.4 Update

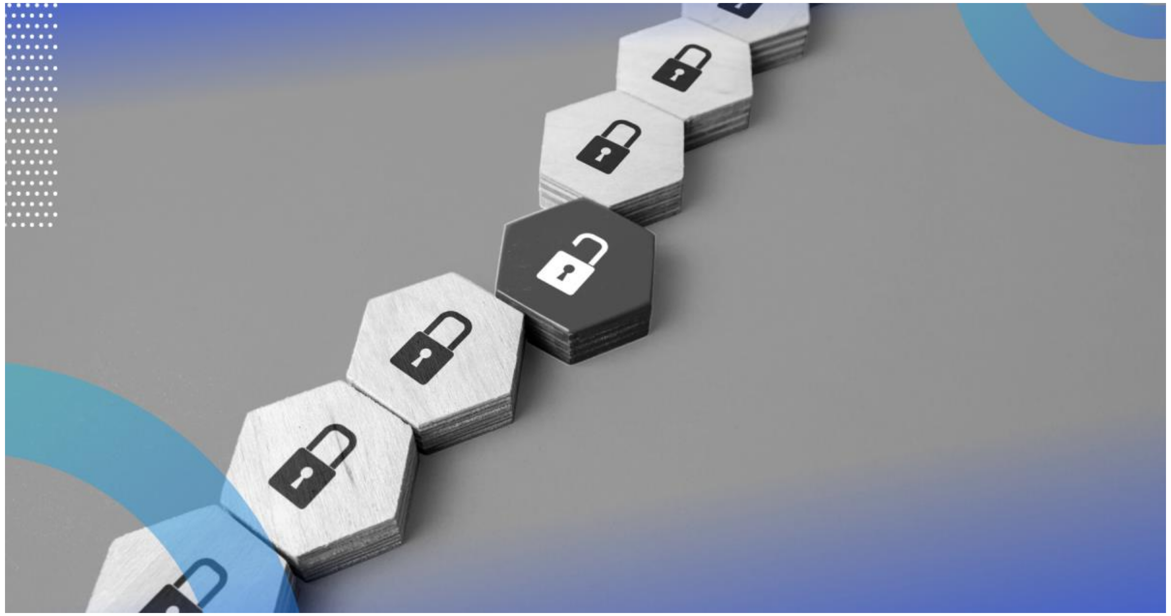
Misc Updates

- TLS Tunnel for SRA
- AIX Volume Mobility Enablement
- Volume Limit Increase FS9500/FS7300
- lsportstats via the RESTapi

vSphere Plugin Update

Storage Sentinel Update

Two Person Integrity



What is Two Person Integrity

- Prevents a rogue user from purposely deleting Safeguarded snapshots and deleting/changing other critical storage security configurations
  - Restricts Security Admin role usage when TPI enabled
    - When Security Admin role is needed, it can be unlocked with the approval of another Security Admin
  - Additional protection for Safeguarded Copy
  - Uses existing superuser locking capability

Existing User Role Descriptions

Superuser

- Security Administrator with extra privileges
- Highest authority
- Completely unrestricted
- Maintenance commands:
    - Initial setup activity
    - Rebooting nodes in a failure state
    - Installing software in service state

Security Administrator

- User management: create and delete user and user groups
- Change system date time settings
- Change Safeguarded snapshot configuration
- Change security settings
    - LDAP server settings
    - Change certificates
    - Password rules
    - MFA settings
    - Delete Safeguarded snapshots
- Change system time

Administrator

- Day to day storage configuration tasks
- Create/Remove regular volumes and pools
- Create/Remove host mappings
- Grow/Shrink volumes and pools
- Cannot remove Safeguarded snapshots

Other roles

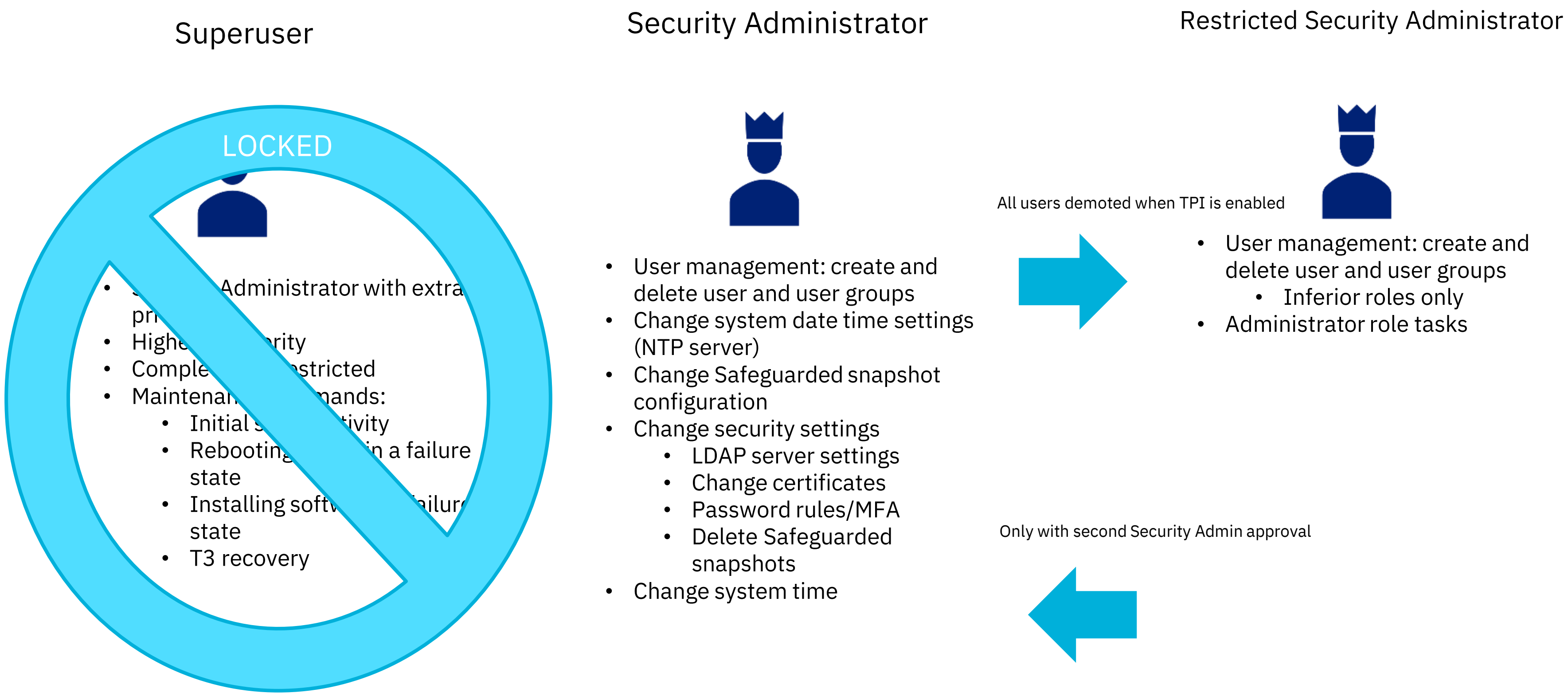
Copy Operator

Service

Monitor

Two Person Integrity (TPI): Time Based User Promotion

Existing User role with TPI enabled



Superuser

LOCKED

- Administrator with extra pr
- Highe rity
- Comple stricted
- Maintenan mands:
  - Initial s tivity
  - Rebooting in a failure state
  - Installing softw ailure state
  - T3 recovery

Security Administrator

- User management: create and delete user and user groups
- Change system date time settings (NTP server)
- Change Safeguarded snapshot configuration
- Change security settings
  - LDAP server settings
  - Change certificates
  - Password rules/MFA
  - Delete Safeguarded snapshots
- Change system time

All users demoted when TPI is enabled

Only with second Security Admin approval

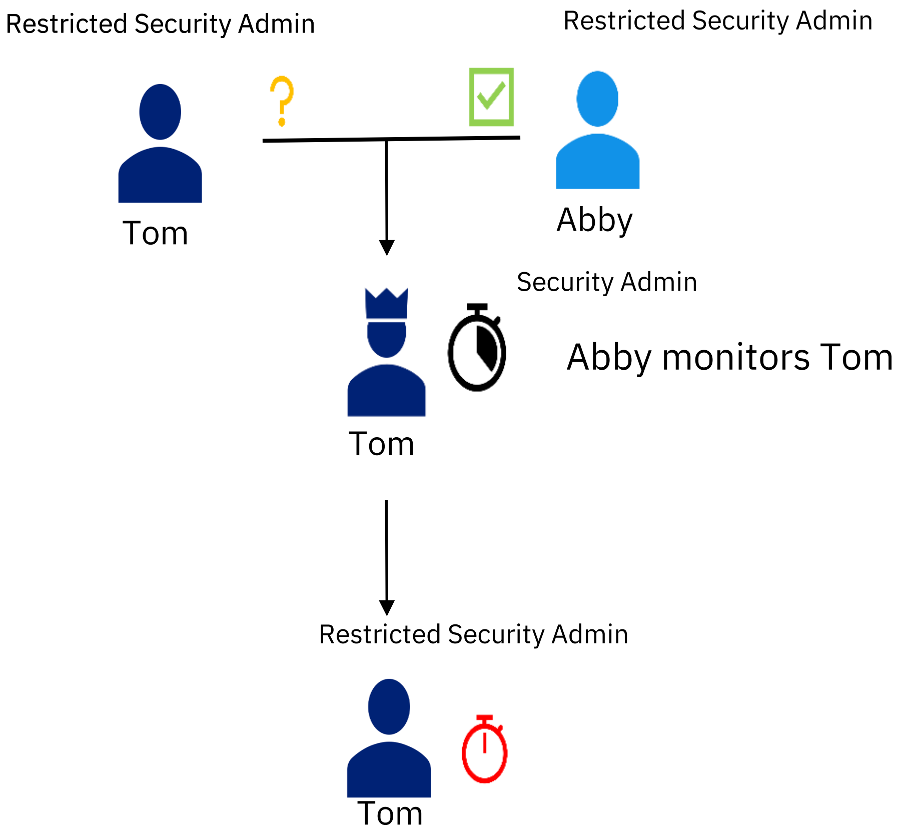
Restricted Security Administrator

- User management: create and delete user and user groups
  - Inferior roles only
- Administrator role tasks

Two Person Integrity (TPI): Time Based User Promotion

Allows a user to request elevated privileges for a specified amount of time

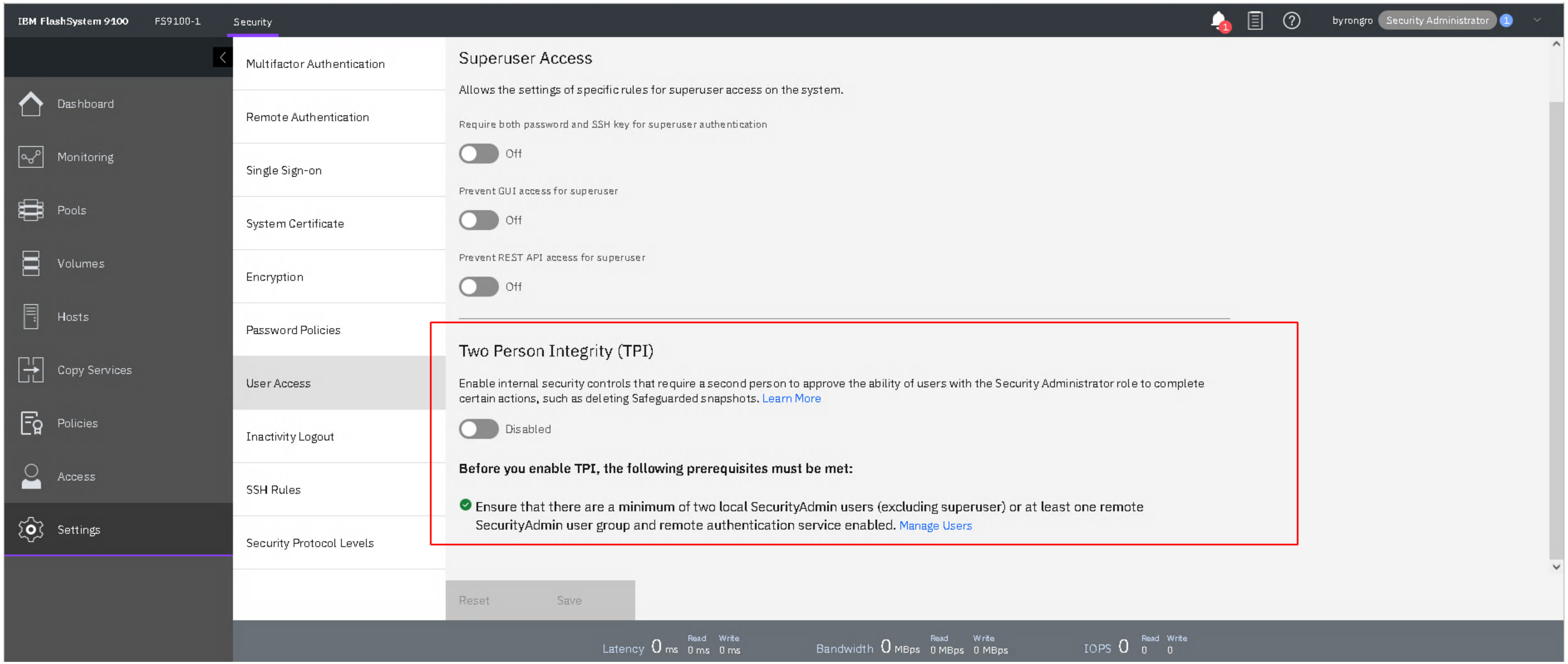
- System wide setting (on/off)
- Locks the superuser account
- Changes Security Admin users to Restricted Security Admin role which has privileges similar to Administrator
- Only Restricted Security Admin users can be elevated to Security Admin role and it is time limited
- Approvers can only have Restricted Security Admin or Security Admin role
- Approver can specify the time limit for the elevated privileges
- System enforces a maximum time allowed for elevated privileges of 24 hours
- Works with remote or local users
- Maximum of 4 elevated users at a time


Restricted Security Admin
Tom
?
✓
Restricted Security Admin
Abby
Security Admin
Tom
Abby monitors Tom
Restricted Security Admin
Tom

Requirements to Enable

- Two local Security Admin users excluding superuser or a remote user group with Security Admin role
- Can be enabled by superuser or another Security Administrator
- Platform must support a technician port
  - Prevent user from locking themselves out of system

Enable TPI



Superuser Access

Allows the settings of specific rules for superuser access on the system.

Require both password and SSH key for superuser authentication: Off

Prevent GUI access for superuser: Off

Prevent REST API access for superuser: Off

Two Person Integrity (TPI)

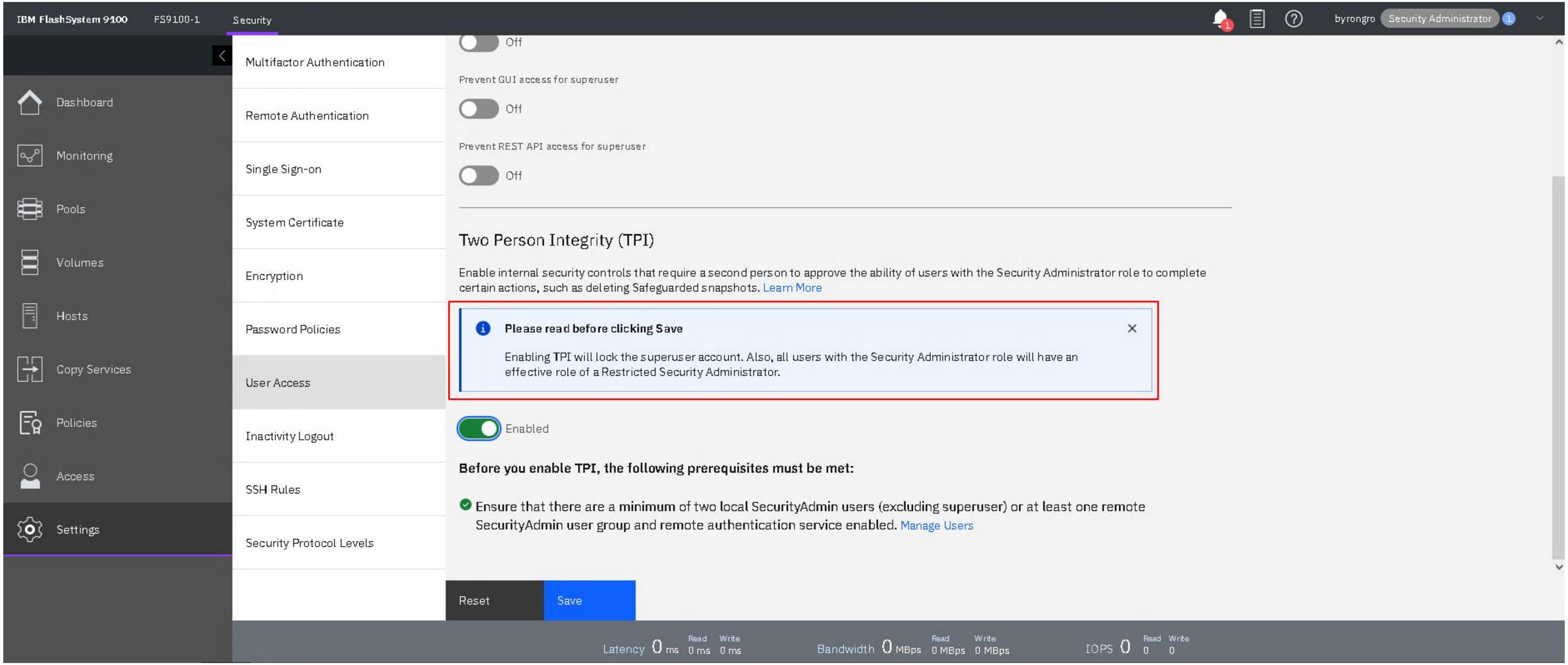
Enable internal security controls that require a second person to approve the ability of users with the Security Administrator role to complete certain actions, such as deleting Safeguarded snapshots. Learn More

Disabled

Before you enable TPI, the following prerequisites must be met:

✓ Ensure that there are a minimum of two local SecurityAdmin users (excluding superuser) or at least one remote SecurityAdmin user group and remote authentication service enabled. Manage Users

Enable TPI - 2



Off

Prevent GUI access for superuser

Off

Prevent REST API access for superuser

Off

Two Person Integrity (TPI)

Enable internal security controls that require a second person to approve the ability of users with the Security Administrator role to complete certain actions, such as deleting Safeguarded snapshots. Learn More

Please read before clicking Save

Enabling TPI will lock the superuser account. Also, all users with the Security Administrator role will have an effective role of a Restricted Security Administrator.

Enabled

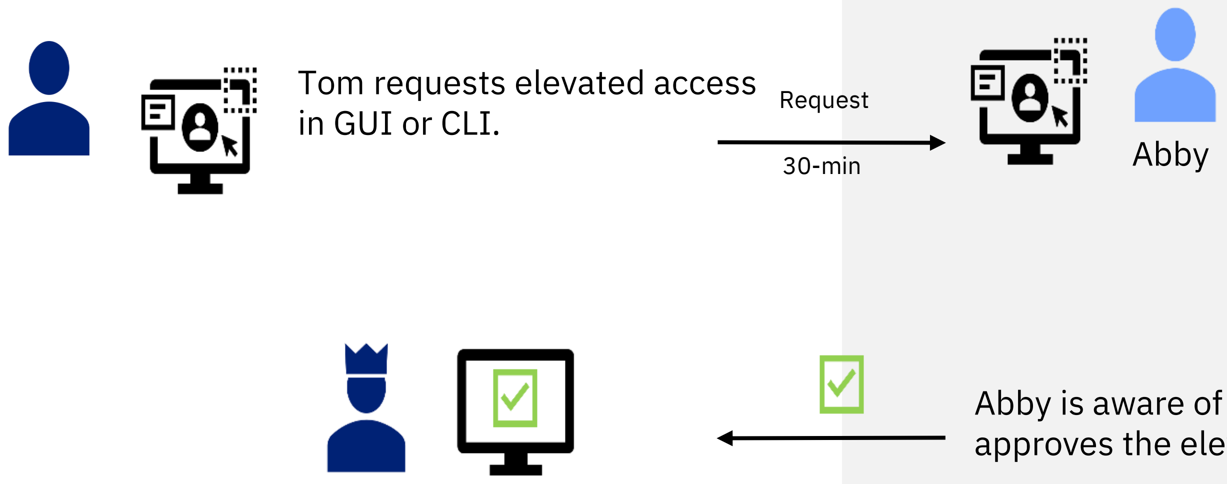
Before you enable TPI, the following prerequisites must be met:

✓ Ensure that there are a minimum of two local SecurityAdmin users (excluding superuser) or at least one remote SecurityAdmin user group and remote authentication service enabled. Manage Users

Two-Person Integrity: Time Based User Promotion Example

Due to application changes, Tom needs to reconfigure his Safeguarded Copy policy

Tom needs to request that another Security Admin approves his request



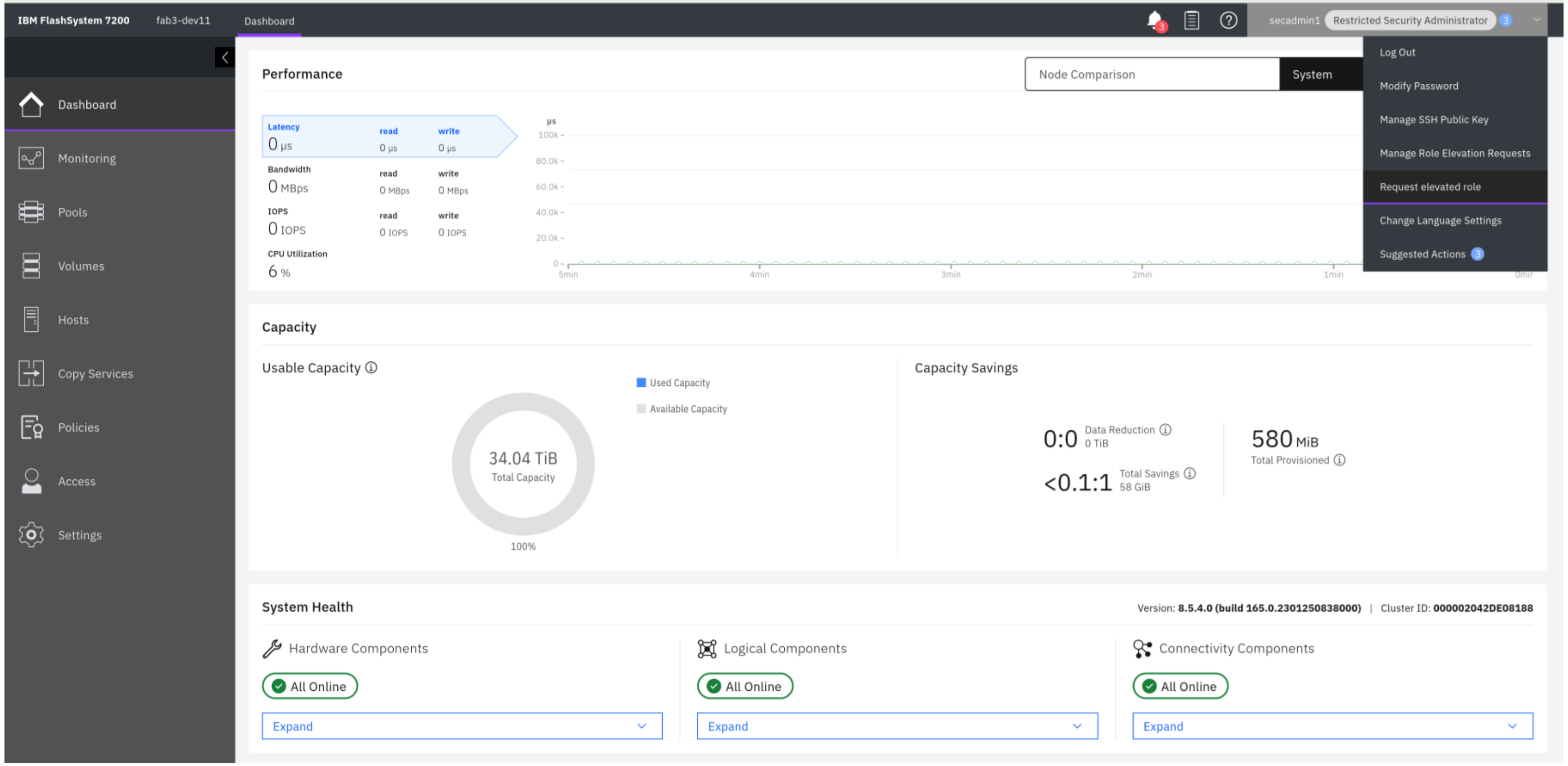
Tom requests elevated access in GUI or CLI.

Abby is aware of the application changes and approves the elevated access

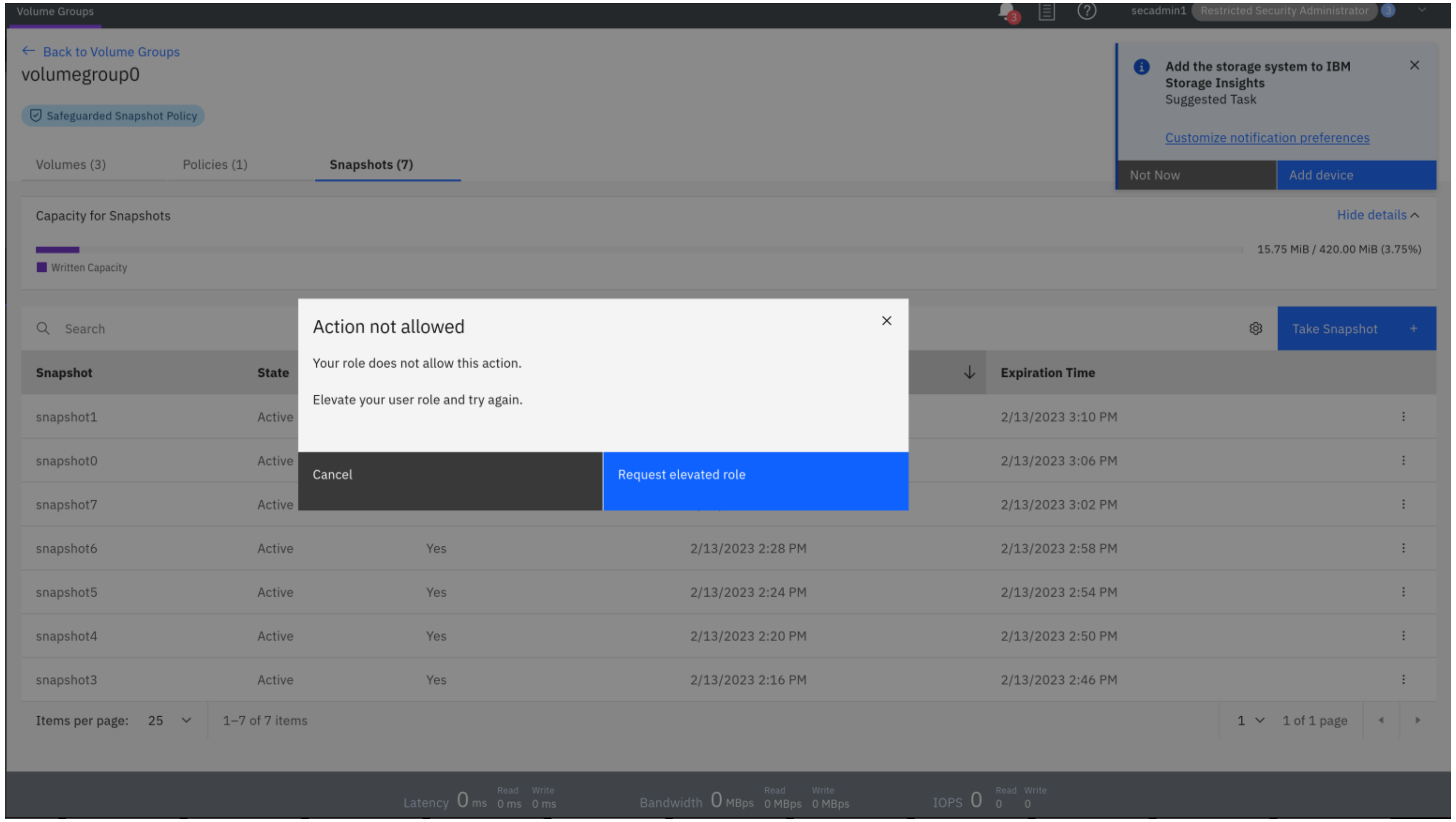
Tom has 30-min of elevated access to perform the changes on Safeguarded Policy before the system terminates his access.

Abby monitors the audit log to ensure Tom is performing the desired actions. If necessary, Abby can cancel his elevated access with a click of a button.

Creating A Request



Creating A Request



volumegroup0

Add the storage system to IBM Storage Insights
Suggested Task

Capacity for Snapshots

Action not allowed

Your role does not allow this action.

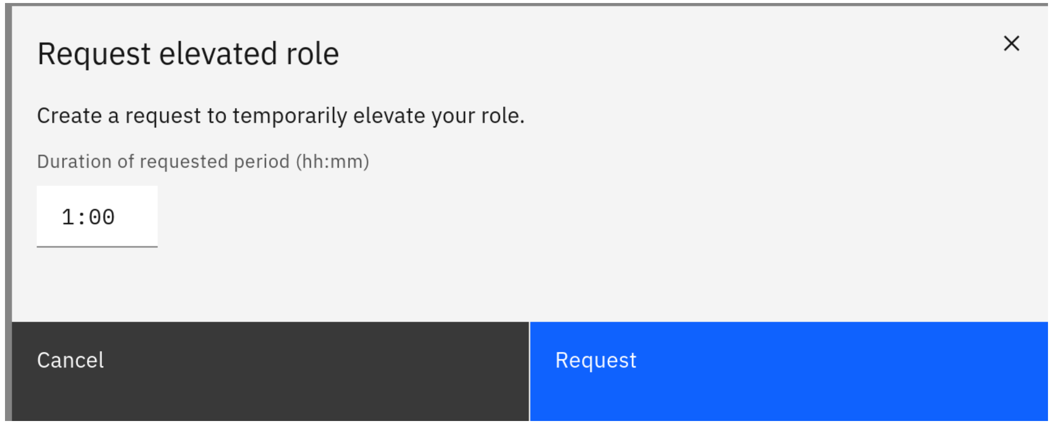
Elevate your user role and try again.

Snapshot	State			Expiration Time
snapshot1	Active			2/13/2023 3:10 PM
snapshot0	Active			2/13/2023 3:06 PM
snapshot7	Active			2/13/2023 3:02 PM
snapshot6	Active	Yes	2/13/2023 2:28 PM	2/13/2023 2:58 PM
snapshot5	Active	Yes	2/13/2023 2:24 PM	2/13/2023 2:54 PM
snapshot4	Active	Yes	2/13/2023 2:20 PM	2/13/2023 2:50 PM
snapshot3	Active	Yes	2/13/2023 2:16 PM	2/13/2023 2:46 PM

Items per page: 25
1–7 of 7 items
1
1 of 1 page
Latency 0 ms Read 0 ms Write 0 ms
Bandwidth 0 MBps Read 0 MBps Write 0 MBps
IOPS 0 Read 0 Write 0

Creating Request

- 10 minutes to 24 hours
- Unapproved requests expire after 24 hours
- Elevated privileges start when request is approved
- Notify user outside of the system
- Request ID or user name to track request



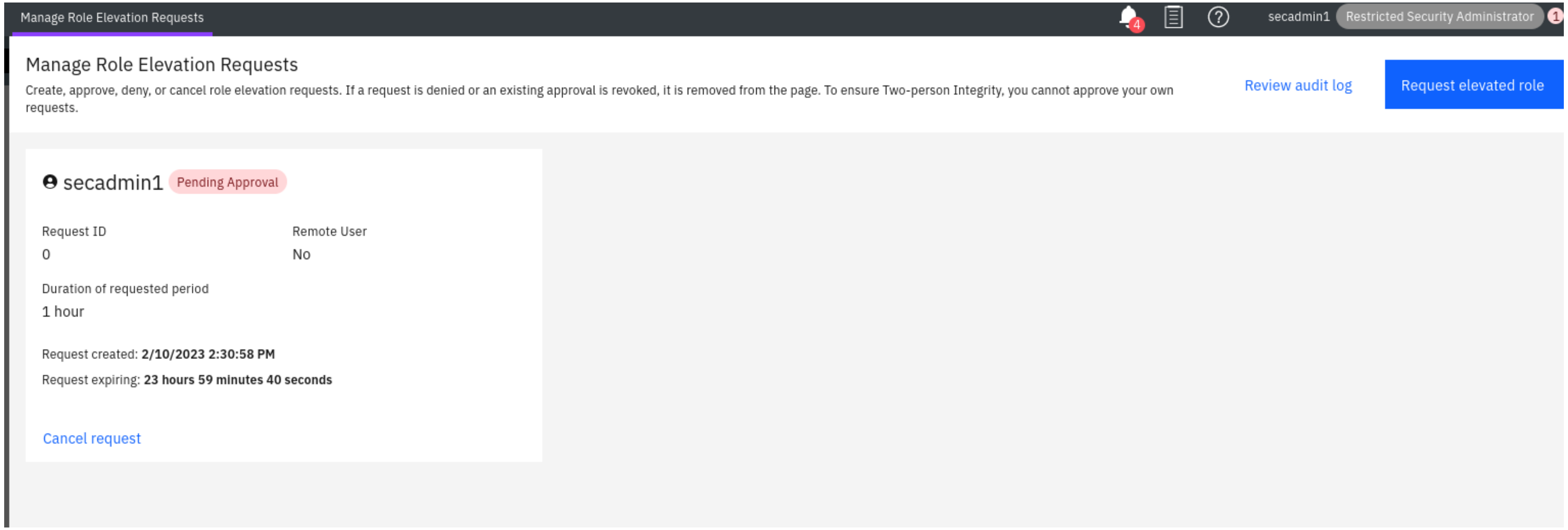
Request elevated role

Create a request to temporarily elevate your role.

Duration of requested period (hh:mm)

1:00

Request Waiting For Approval



Manage Role Elevation Requests
4
secadmin1
Restricted Security Administrator
1

Manage Role Elevation Requests

Create, approve, deny, or cancel role elevation requests. If a request is denied or an existing approval is revoked, it is removed from the page. To ensure Two-person Integrity, you cannot approve your own requests.

Review audit log
Request elevated role

secadmin1 Pending Approval

Request ID: 0

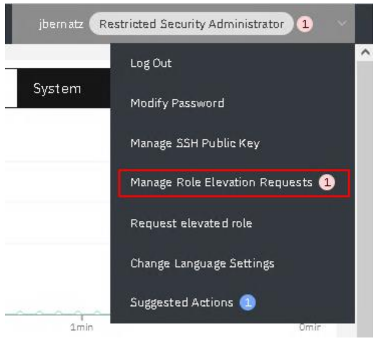
Remote User: No

Duration of requested period: 1 hour

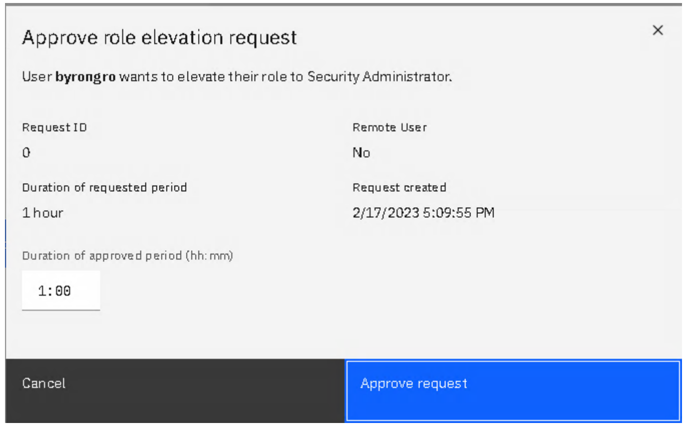
Request created: **2/10/2023 2:30:58 PM**

Request expiring: **23 hours 59 minutes 40 seconds**

Approving Requests



1



Approve role elevation request

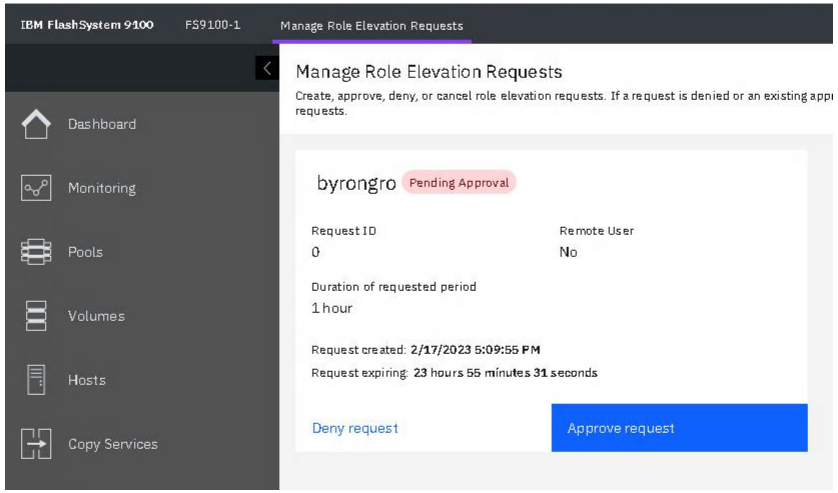
User **byrongro** wants to elevate their role to Security Administrator.

Request ID 0	Remote User No
Duration of requested period 1 hour	Request created 2/17/2023 5:09:55 PM

Duration of approved period (hh: mm)

1:00

3



Manage Role Elevation Requests

Create, approve, deny, or cancel role elevation requests. If a request is denied or an existing appı requests.

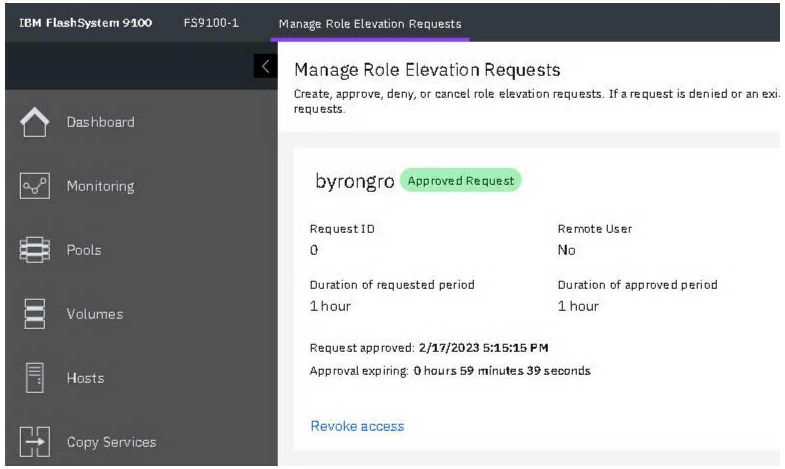
byrongro Pending Approval

Request ID 0	Remote User No
Duration of requested period 1 hour	

Request created: **2/17/2023 5:09:55 PM**

Request expiring: **23 hours 55 minutes 31 seconds**

2



Manage Role Elevation Requests

Create, approve, deny, or cancel role elevation requests. If a request is denied or an exi requests.

byrongro Approved Request

Request ID 0	Remote User No
Duration of requested period 1 hour	Duration of approved period 1 hour

Request approved: **2/17/2023 5:15:15 PM**

Approval expiring: **0 hours 59 minutes 39 seconds**

4

Unlock Superuser

- Superuser is needed to accomplish a service action (satask command)
- Elevated user can unlock superuser
  - Remote support can unlock superuser (same as today)
- Warning of TPI inconsistency if superuser is unlocked

TPI Logged Events

- These events will be listed in the event log

- Informational events to indicate:
  - TPI enabled
  - TPI disabled
- Warning events triggered when:
  - TPI request is pending approval
  - TPI elevated user is active
  - Superuser unlocked while TPI is enabled

Normal Security Administrator Commands

- chusergrp
- mkkeyserver
- mkldapserver
- mkownershipgroup
- mktruststore
- mktwopersonintegrityrequest
- mkuser
- mkusergrp
- rmkeyserver
- rmldapserver
- rmownershipgroup
- rmtruststore
- rmuser
- rmusergrp
- setpwdreset
- setsystemtime
- chauthmultifactorduo
- chauthmultifactorverify
- chauthservice
- chauthsinglesignon
- chencryption
- chkeyserver
- chkeyserverciphertrustmanager
- chkeyserverisklm
- chldap
- chldapserver
- chownershipgroup
- chsecurity
- chsystemcert
- chtruststore
- chtwopersonintegrityrequest
- chuser

Restricted Security Administrator Commands

- Cannot create, delete, or change a user or user group that refers to Security Administrator role.

- Issue any command Administrator can in addition to:
- chtwopersonintegrityrequest
- mktwopersonintegrityrequest
- chuser
- chusergrp
- mkuser
- mkusergrp
- rmuser
- rmusergrp

New CLI Commands

- **chtwopersonintegrityrequest** - Approve/cancel a two person integrity request.
- **lstwopersonintegrityrequest** - Displays two person integrity requests.
- **mktwopersonintegrityrequest -** Creates a two person integrity request for the current user.

Non-Disruptive Security/Software Patching

The Nature of the Problem

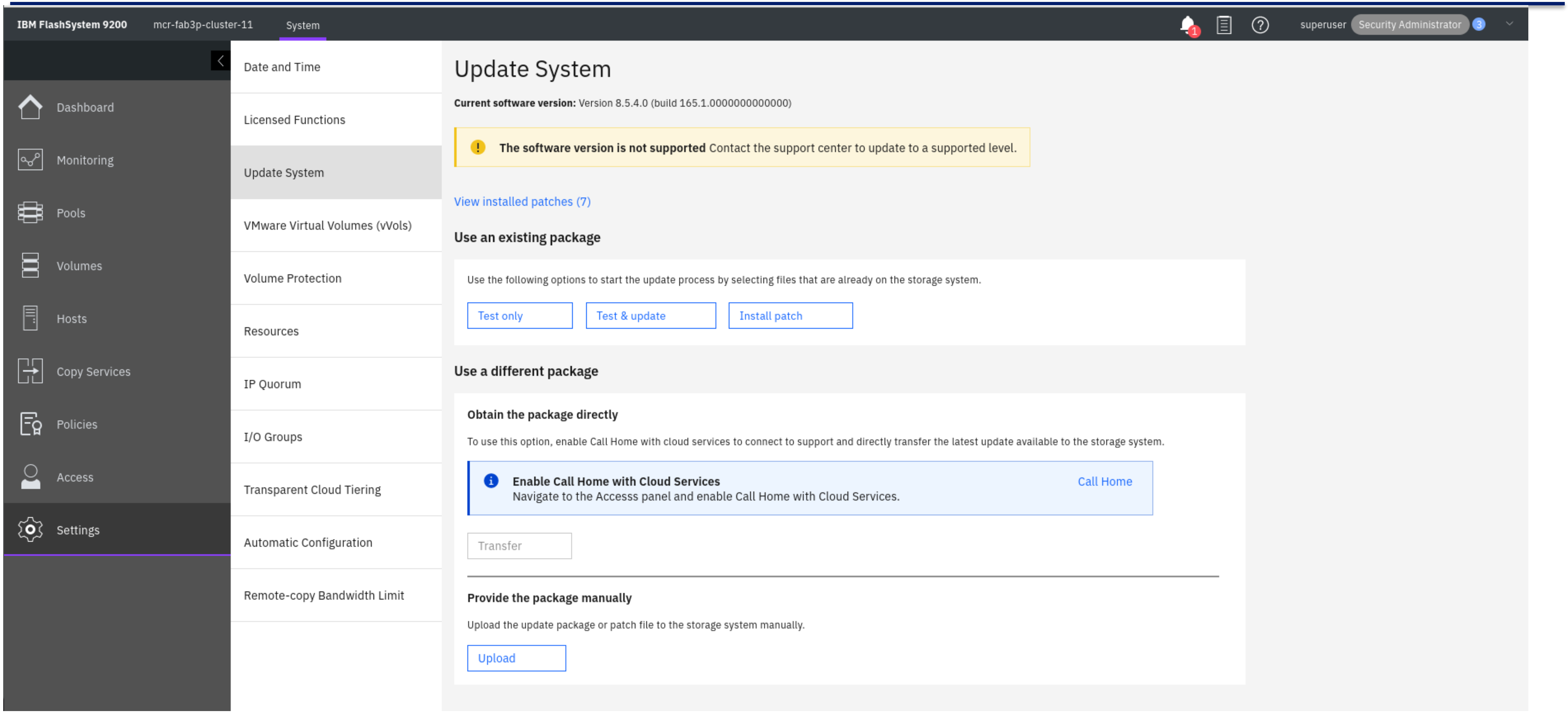
- In the past Storage Virtualize code has been a single stack regardless of whether the software was in the I/O path, device firmware, management functions (GUI/CLI/RESTapi).
- In order to patch any of these components a full software upgrade needed to be done
  - This required nodes restarting, I/O path failovers, etc

The Solution

- Code not directly used by the IO stack may be patched (the I/O process remains running), to fix published security issues. Examples of which are:
  - Linux Utilities
  - Other open-source software (Open SSL, Apache, Tomcat)
  - Device firmware

- Allow Storage Virtualize products to have non-I/O path code non-disruptively and quickly patched (without having to stop the I/O process on each node).

Security Patching



Update System

Current software version: Version 8.5.4.0 (build 165.1.0000000000000)

The software version is not supported Contact the support center to update to a supported level.

View installed patches (7)

Use an existing package

Use the following options to start the update process by selecting files that are already on the storage system.

Use a different package

Obtain the package directly

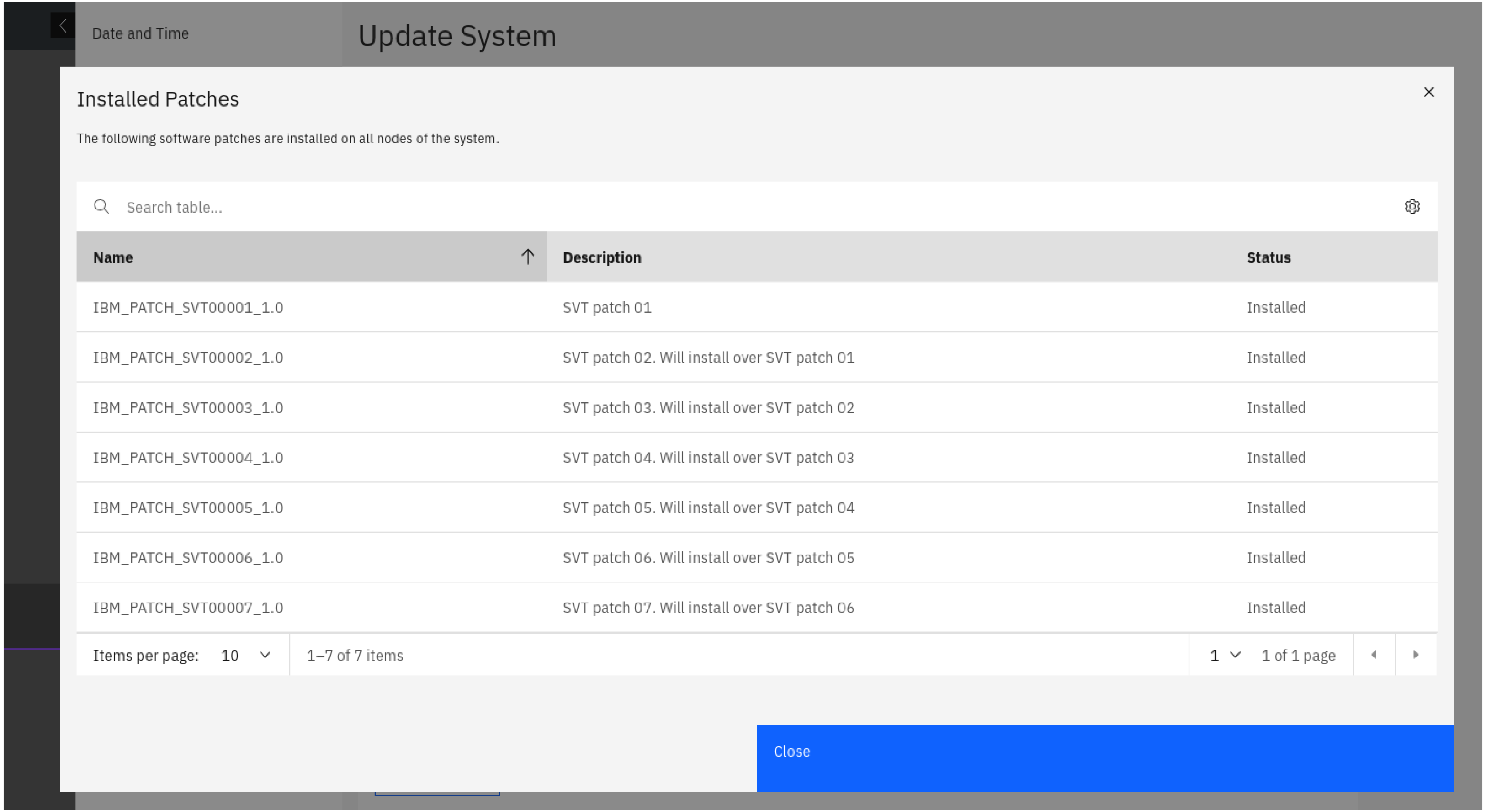
To use this option, enable Call Home with cloud services to connect to support and directly transfer the latest update available to the storage system.

Enable Call Home with Cloud Services
Navigate to the Accesss panel and enable Call Home with Cloud Services.

Provide the package manually

Upload the update package or patch file to the storage system manually.

Security Patching



Installed Patches

The following software patches are installed on all nodes of the system.

Name	Description	Status
IBM_PATCH_SVT00001_1.0	SVT patch 01	Installed
IBM_PATCH_SVT00002_1.0	SVT patch 02. Will install over SVT patch 01	Installed
IBM_PATCH_SVT00003_1.0	SVT patch 03. Will install over SVT patch 02	Installed
IBM_PATCH_SVT00004_1.0	SVT patch 04. Will install over SVT patch 03	Installed
IBM_PATCH_SVT00005_1.0	SVT patch 05. Will install over SVT patch 04	Installed
IBM_PATCH_SVT00006_1.0	SVT patch 06. Will install over SVT patch 05	Installed
IBM_PATCH_SVT00007_1.0	SVT patch 07. Will install over SVT patch 06	Installed

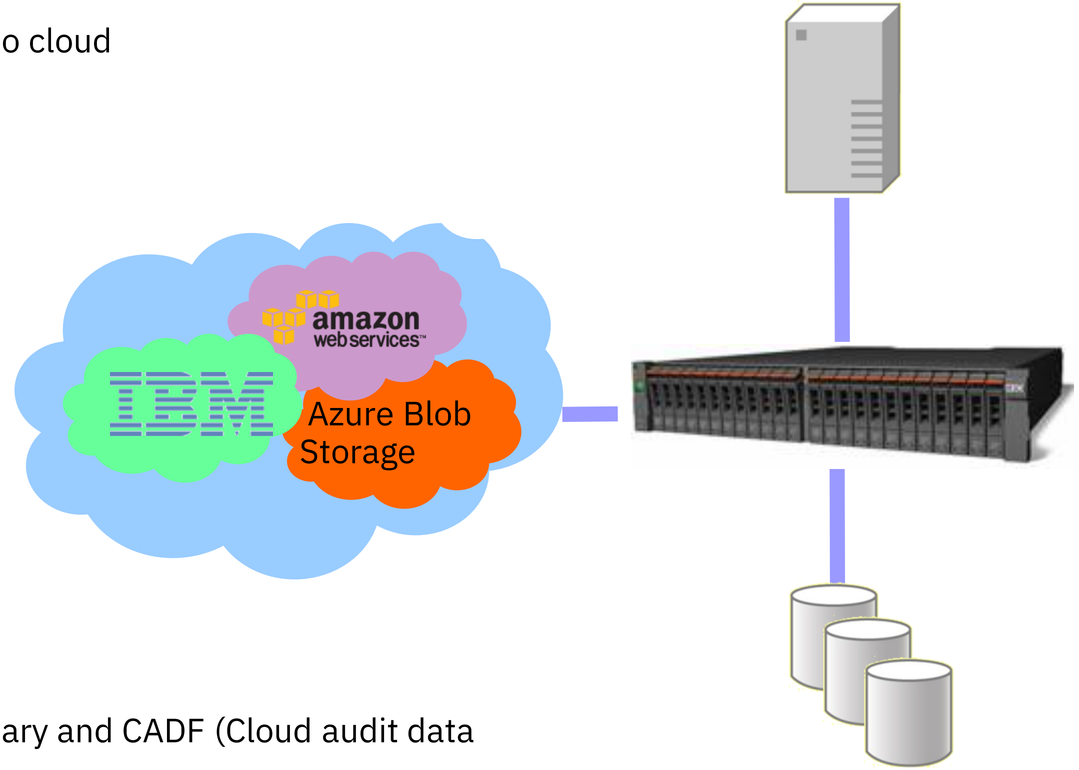
Items per page: 10 1–7 of 7 items 1 1 of 1 page

Transparent Cloud Tiering to Azure Blob Storage

Azure Blob Storage

Transparent Cloud Tiering (TCT) Recap

- Connects Storage Virtualize and FlashSystem to cloud object storage.
- Full and incremental snapshots of Storage Virtualize volumes to cloud object storage.
- Volume data is compressed and encrypted before being sent to cloud
- Zeros are not sent
- Support volume groups for mutual consistency
- Full and incremental restore from cloud snapshots
- Import of volumes on different cluster(import mode)



- Support for Cloud Provides: Amazon S3, Azure Blob storage, Openstack Swift,.
- Connects to the cloud with secure (TLS) sockets
- Authentication with certificates and cloud account credentials
- Integrity is checked using CRC, hashes and checksum
- Audit log records all backup and restore operations in proprietary and CADF (Cloud audit data format) as well
- Health Check of cloud object storage at regular interval or at user’s demand

Use Cases

- Backup/Restore

- Provide create, delete, restore, and monitor option for turning snapshot placed onto cloud as a backup copy
- Provide crash-consistent backup facility
  - Need external management software(client’s software) to have application consistent backup

- Archive

- If a volume has a full backup in the cloud, the local volume can be deleted
- Restore it later if necessary
- Longer Term SGC Storage

- Migrate/Clone

- A FlashSystem can access backup data from a different system and clone a backed-up volume
- A FlashSystem can access backup data from a different system and take over a volume's backup history
- Requires encryption key exchange

Azure as Cloud Service Provider for Object Storage

- The Azure account is **a global unique entity that gets you access to Azure services and your Azure subscriptions**
- In your subscription(s) you can manage resources in resources groups. (Hierarchy is in next slide) You can create multiple subscriptions in your Azure account

- We are supporting **standard general-purpose v2 blob storage account** on Azure with blobs as storage
- We will use containers from Storage account to achieve cloud backup into Azure blob storage

Azure Account Hierarchy

Prerequisites - Azure resource group and storage account before we could consume Azure CSP in Storage Virtualize .

Ways to create –

A) Through Azure portal
B) Azure PowerShell
C) Azure CLI
D) Azure Resource Manager Template.

Check Azure blob storage documentation for same.

*https://mynamespace.blob.core.windows.net /mycontainer/myobject

✓ Subscriptions - To use Azure's cloud-based services, you must first purchase a subscription. It acts as a single billing unit for Azure resources, with subscriptions billed for services used in Azure.

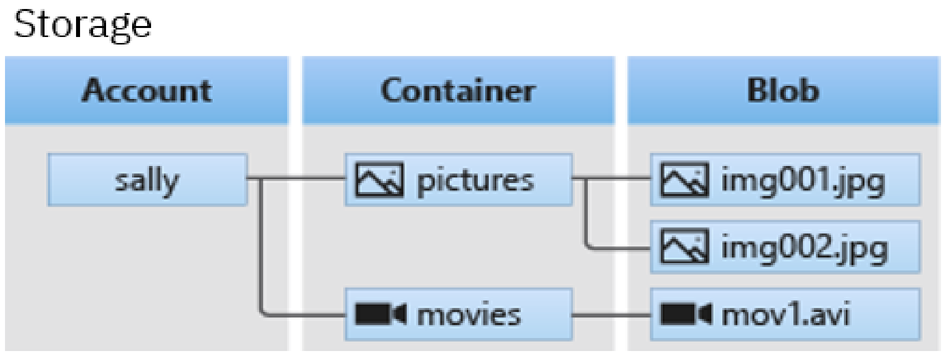
Resource group - Logical container for grouping of your Azure services. Every resource, including an Azure storage account, must belong to an Azure resource group. Location is one important attribute.

Storage account - Storage account provides a unique namespace for your Azure storage data that's accessible from anywhere in the world. It contains all storage data objects i.e., blobs, files, queues, and tables. IBM Flash System only deals with Blob data objects. The name of storage account forms first part(public) of your credential.

Storage account keys - Azure generates two 512-bit storage account access keys for that account. They are the private part of credential tuple.

Containers

Blobs



Limitations/Supported Systems

- Supported platforms

- SA2, SV2, SV3
- FS9500, FS9200, FS9100, FS7200, FS5200, FS7300
- SVPC

- Single cloud account
- 1024 Volumes with cloud snapshot enabled
- 256 snapshot generations per volume
- Cloud traffic uses config node management port
- Licensing - Flash Copy function is used by cloud snapshots. Flash Copy operations used on internal storage are part of the base license (requires license for external storage only)
- Encryption is recommended
- Volume cannot be
  - Part of a remote copy relationship
  - vVol
  - Volume mirrored with copies in different storage pools
  - Being migrated
  - Associated with a legacy FlashCopy mapping

Storage Virtualize for Public Cloud AWS 8.5.4 Update

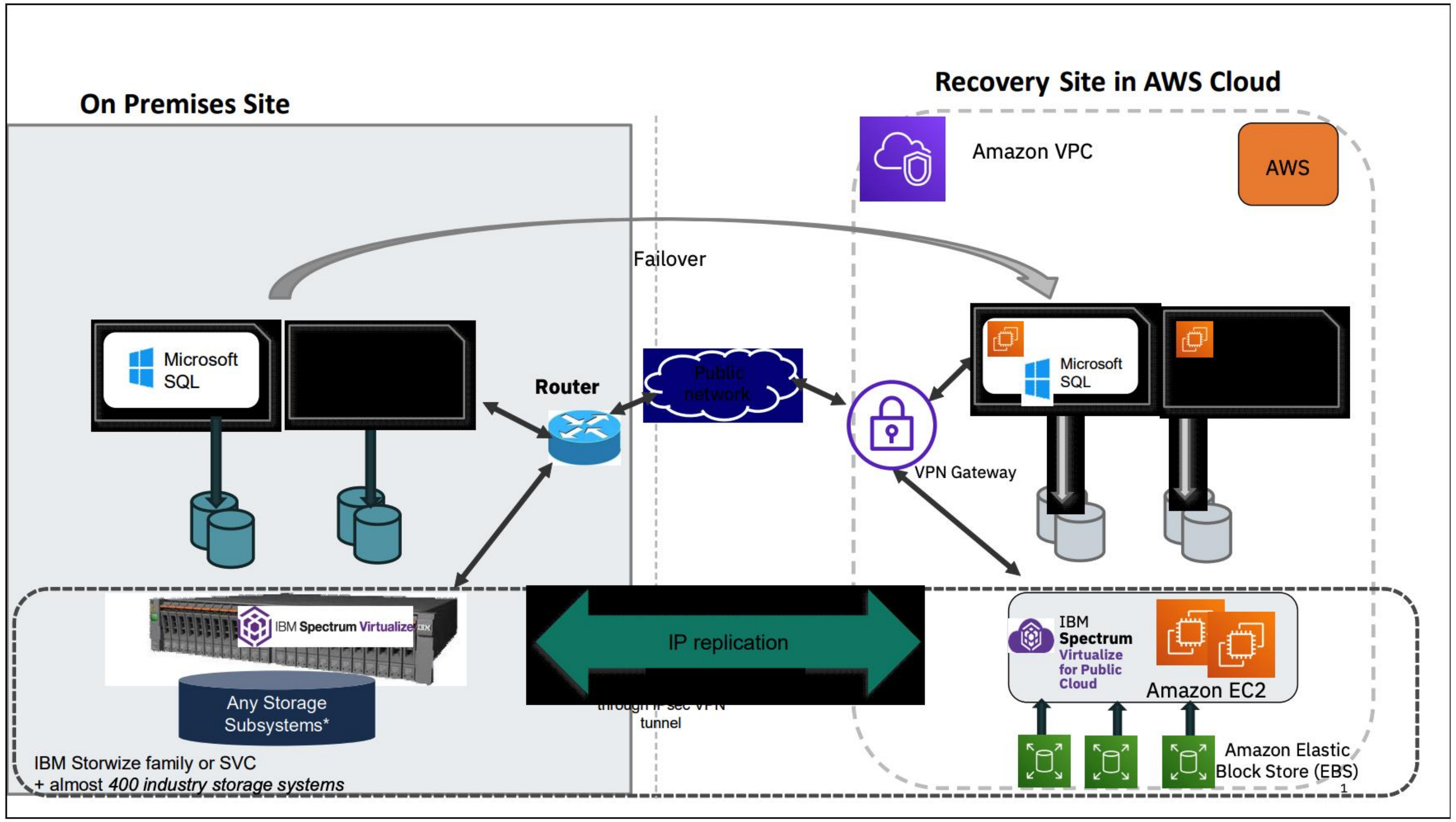
Recap of SV4PC on AWS 8.3.1 release

- 8.3.1 was the previous release of SVPC on AWS
- Key Storage Virtualize features support like IP replication, deduplicated and compressed volumes , easy tier, thin provisioning, FlashCopy etc
- Support of 2 node and 4 node cluster deployment from AWS marketplace
- AWS Host VM based on Centos 7

Supported VM Size	vCPU	Memory GiB	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
C5.4xlarge	16	32	Up to 10	4750
C5.9xlarge	36	72	10	9500
C5.18xlarge	72	144	25	19000
C5.large (Quorum Only)	2	4	Up to 10	Up to 4750

SVPC on AWS 8.5.4 Release

1. Same VM type support as in 8.3.1. Additional support of gp3 EBS
2. AWS Host VM based on RHEL 8.6 kernel version 4.18.0-372.9.1
3. No upgrade support from SVPC 8.3.1 to 8.5.4 version
4. Support of both public and private deployment
5. New Key features support


On Premises Site
Recovery Site in AWS Cloud
Amazon VPC
AWS
Failover
Microsoft SQL
Router
Public network
VPN Gateway
Microsoft SQL
IBM Spectrum Virtualize
Any Storage Subsystems*
IBM Storwize family or SVC
+ almost 400 industry storage systems
IP replication
through IP sec VPN tunnel
IBM Spectrum Virtualize for Public Cloud
Amazon EC2
Amazon Elastic Block Store (EBS)

SVPC DR solution

Supported Disk Types

Supported Managed Disk	Disk Type	Use Cases	Max Disk Size (TiB)	Max throughput	Max **Iops**
io1	SSD	• Workloads that require sustained IOPS performance or more than 16,000 IOPS • I/O-intensive database workloads	16 TiB	1000 MB/s	64,000
gp2/gp3	SSD	• Transactional workloads • Virtual desktops • Medium-sized, single-instance databases • Low-latency interactive applications • Boot volumes • Development and test environments	16 TiB	1000 MB/s for gp3 250 MB/s for gp2	16,000
st1	HDD	• Big data • Data warehouses • Log processing	16 TiB	500 MB/s	500
sc1	HDD	• Throughput-oriented storage for data that is infrequently accessed • Scenarios where the lowest storage cost is important	16 TiB	250 MB/s	250

Benefit of gp3 Over gp2

- gp2 volumes performance is tied to storage capacity
- To get higher IOPS and throughput customer needs to provision larger storage volume size on gp2
- gp3 volumes deliver a baseline performance of 3,000 IOPS and 125MB/s at any volume size
- Scale up to 16,000 IOPS and 1,000 MB/s for an additional fee on gp3

Benefit of replacing default data disk and OS disk during deployment from gp2 to gp3 in 8.5.4

Disk Disk functionality	Disk size GiB	Old disk type and price	Old disk baseline IOPs and throughput MiB/s	New disk type	New disk baseline IOPs and throughput MiB/s
SV Node OS disk	250	gp2 $0.10/GB-month	750, N/A	gp3 $0.08/GB-month	3000, 125
SV Node default data disk provisioned during deployment	512	gp2 $0.10/GB-month	1536, N/A	gp3 $0.08/GB-month	3000, 125
Quorum Node OS disk	10	gp2 $0.10/GB-month	100, N/A	gp3 $0.08/GB-month	3000, 125

From the table it can be seen for the same capacity compared to gp2, gp3 disk are 20% less in price and give more baseline performance

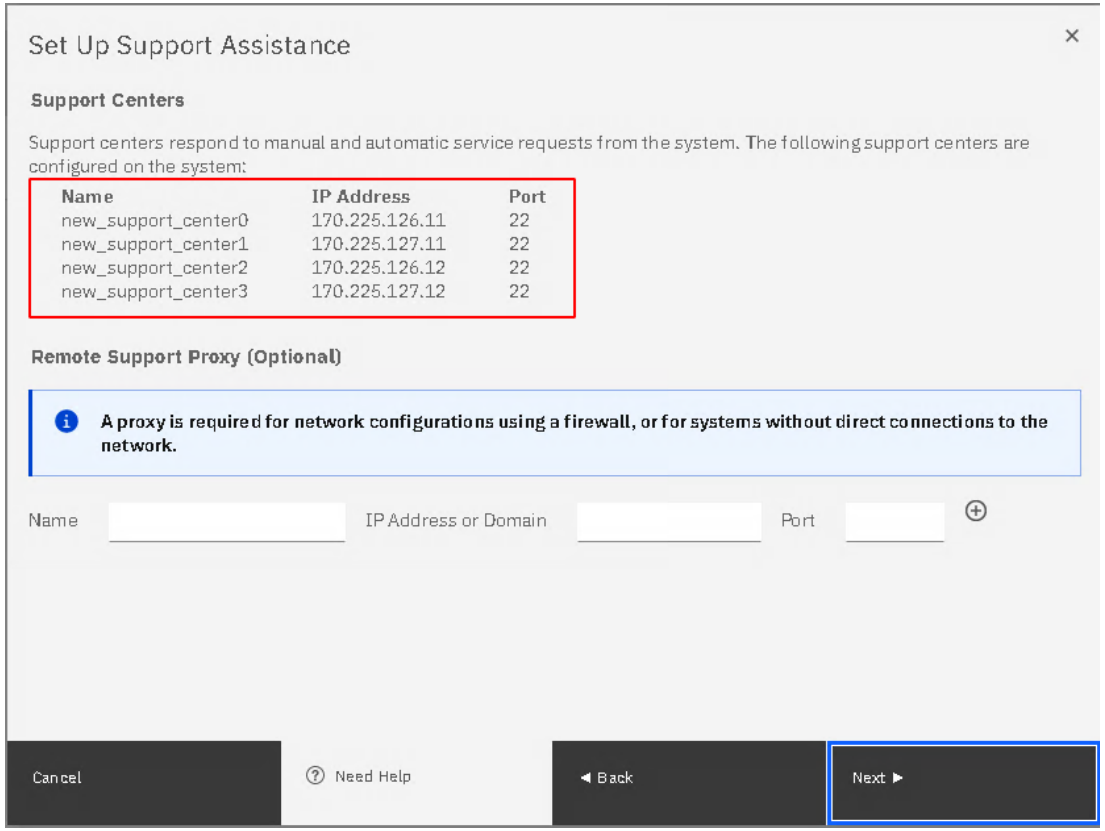
New Features to Deploy

- Volume Group Snapshots
- Safeguarded Copy for Volume Group Snapshots
- Multi-Factor Authentication
- Policy Based Replication
- IPSec over IP based replication
- Transparent Cloud Tiering

Misc. Updates

TLS Tunnel for Remote Support

- In the past remote support has used SSH port 22 to establish a connection to a clients Storage Virtualize system
- Starting with 8.5.4 remote support will try TLS on port 443 first and then if that fails it will fall back to SSH on port 22
- The system can be forced to use TLS only by switching out the servers for SRA to port 443 only



Set Up Support Assistance

Support Centers

Support centers respond to manual and automatic service requests from the system. The following support centers are configured on the system:

Name	IP Address	Port
new_support_center0	170.225.126.11	22
new_support_center1	170.225.127.11	22
new_support_center2	170.225.126.12	22
new_support_center3	170.225.127.12	22

Remote Support Proxy (Optional)

A proxy is required for network configurations using a firewall, or for systems without direct connections to the network.

Name

IP Address or Domain

Port

AIX Works with Volume Mobility

- Storage Virtualize 8.5.0 added support for non-disruptive volume mobility between systems
- System multipath drivers need to support standby paths for this function to work
- AIX 7.3 TL1 now supports Volume Mobility

Volume Count Increase

- FS7300/FS9500

- New volume count is 32,100
  - This allows for 32,099 snapshots
  - Host mappable volume count of 15,864 has not changed

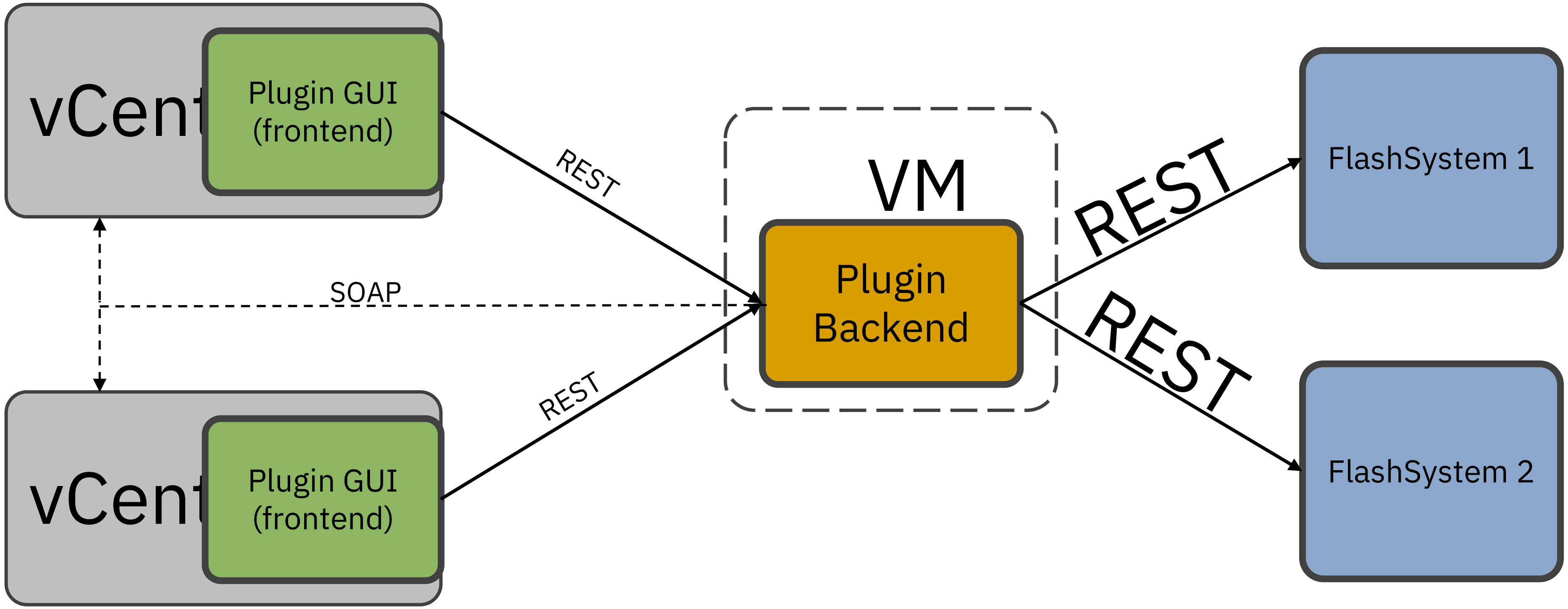
RESTful API Change

- The command lsportstats can now be generated from the RESTful API

VMWare Plugin Update

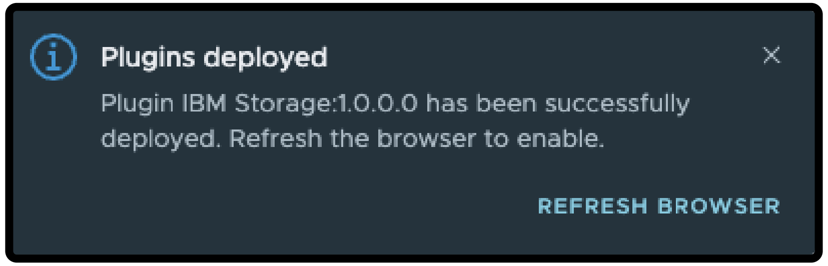
Plugin Overview

- All the plugin functionality is accessible directly from the vSphere web UI.



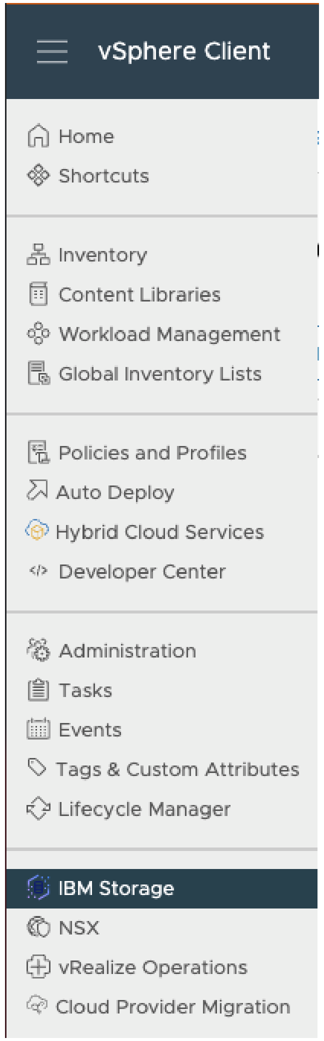
Deployment and Setup

- Download the OVA (Open Virtualization Appliance).
- Deploy OVA into a VM (follow network configuration wizard).
- SSH login to the VM, then register plugin with vCenter.
- Plugin is deployed - the rest of the functionality can now be accessed directly from vSphere UI.



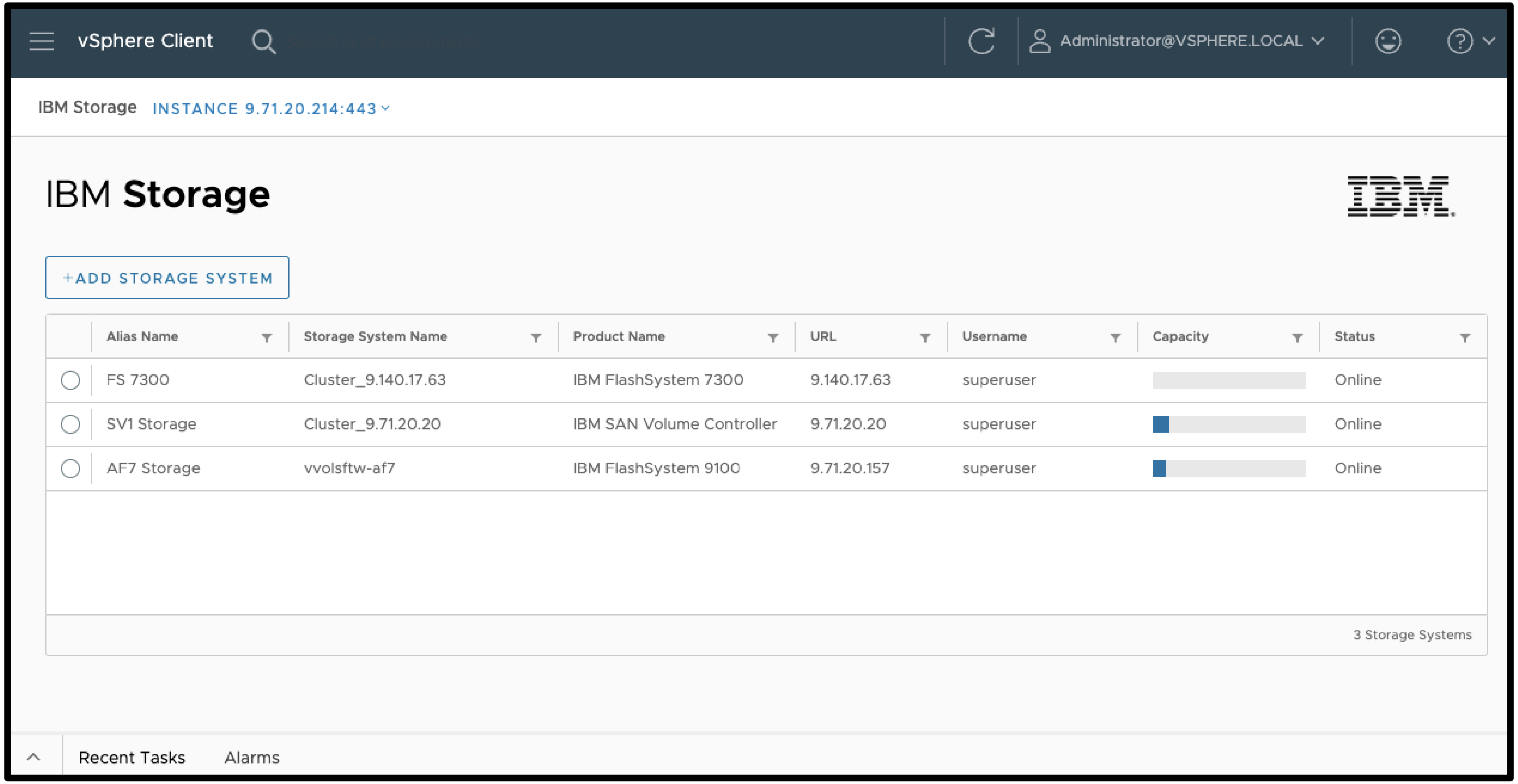
Plugins deployed

Plugin IBM Storage:1.0.0.0 has been successfully deployed. Refresh the browser to enable.



Plugin Dashboard

- The dashboard presents all the registered IBM storage systems and specific information for each of them.

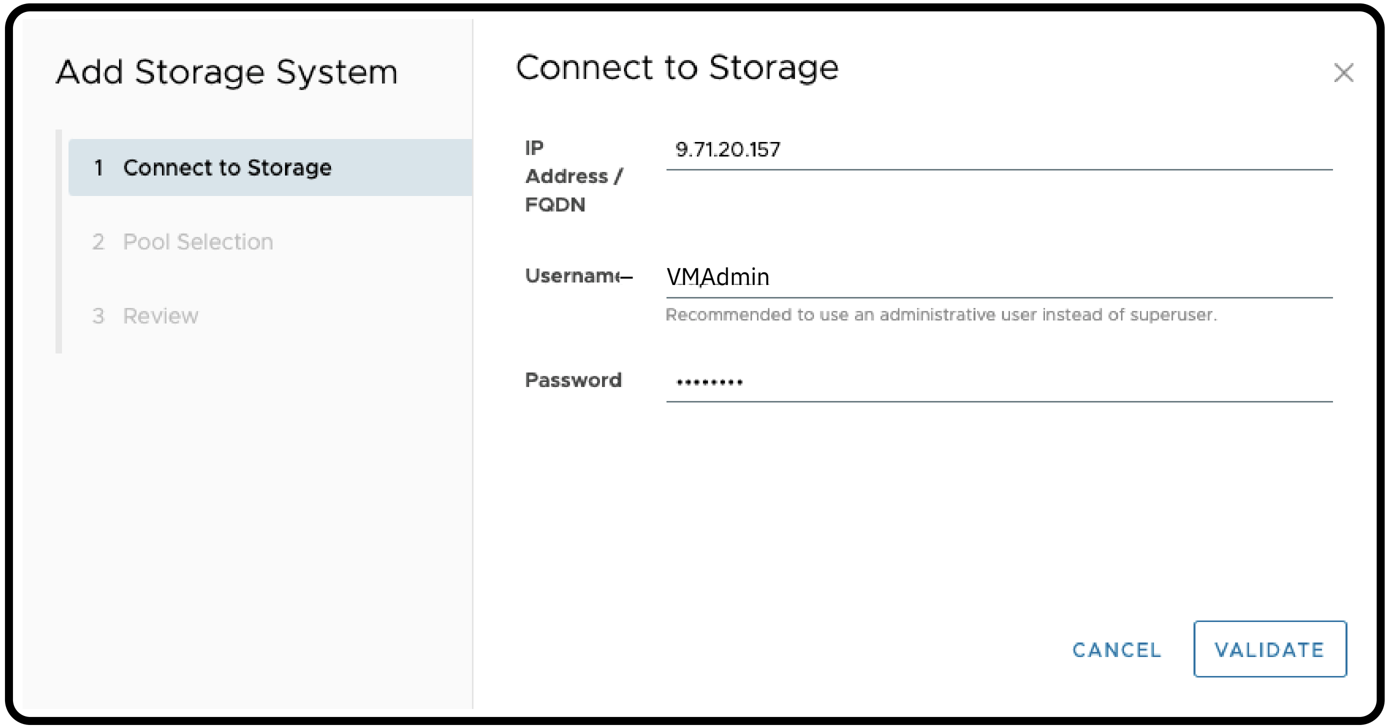


	Alias Name	Storage System Name	Product Name	URL	Username	Capacity	Status
○	FS 7300	Cluster_9.140.17.63	IBM FlashSystem 7300	9.140.17.63	superuser		Online
○	SV1 Storage	Cluster_9.71.20.20	IBM SAN Volume Controller	9.71.20.20	superuser		Online
○	AF7 Storage	vvolsftw-af7	IBM FlashSystem 9100	9.71.20.157	superuser		Online

3 Storage Systems

Supported Features

- Ability to add IBM storage systems to the plugin.
- Input admin credentials to access the storage system.
- Select a pool for the plugin to manage.



Add Storage System

1 Connect to Storage

2 Pool Selection

3 Review

Connect to Storage

IP Address / FQDN: 9.71.20.157

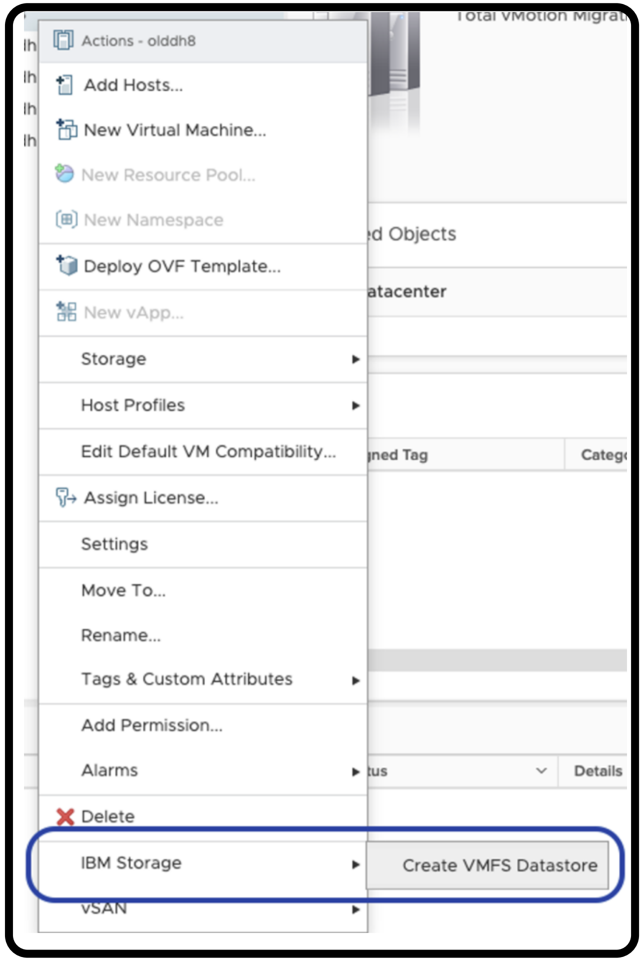
Username: VMAdmin

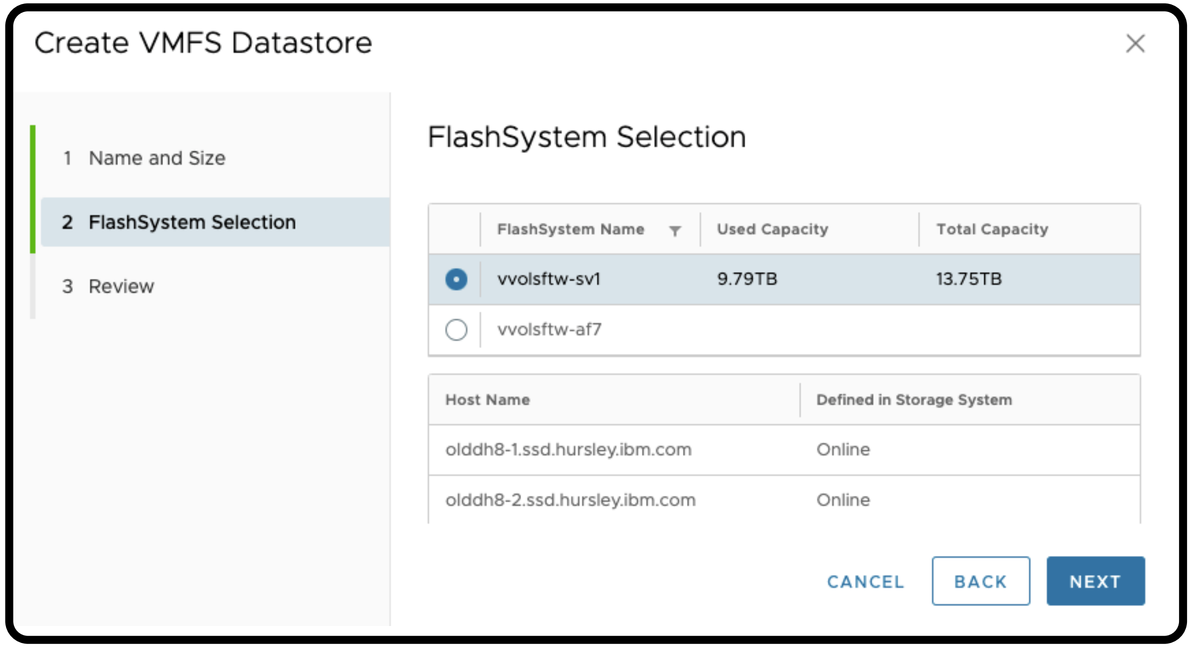
Recommended to use an administrative user instead of superuser.

Password: ••••••••

Supported Features

- VMware Admin can create datastores (manual host mapping currently required).
- Plugin creates volumes on the storage backend and maps them to the selected vSphere host cluster.





Create VMFS Datastore

1 Name and Size
2 FlashSystem Selection
3 Review

FlashSystem Selection

	FlashSystem Name	Used Capacity	Total Capacity
●	vvolsftw-sv1	9.79TB	13.75TB
○	vvolsftw-af7		

Host Name	Defined in Storage System
olddh8-1.ssd.hursley.ibm.com	Online
olddh8-2.ssd.hursley.ibm.com	Online

Other Features

- Register to multiple vCenters (in linked topology)
  - If vCenters are not linked a plugin deployment is needed for each
- Secure REST communication between frontend and backend (with authentication)
- Encrypted storage systems credentials, stored in plugin’s internal DB.
- OVA footprint is small (~760 MBs)
- Dockerised plugin implementation makes it future-proof:
  - Easier to scale, deploy and update
  - App isolation and consistency, regardless of the changes in the environment

Upcoming Features

Second qtr of 2023

- “Recent Tasks” informational messages showing in vSphere UI
- Logs capturing through CLI command (“ibm-plugin snap”)
- Improved GUI:
- info/config panels for hosts and datastores
- improved dashboard
- Automated workflow for datastore deletion
- Expand datastores
- Create multiple datastores in one go
- Ability to upgrade plugin

IBM Storage Sentinel Update

IBM Storage Sentinel 1.1.3 SW Summary

Storage Sentinel support for Epic on Power running AIX

What: Test/validation of Sentinel with Epic on Power AIX

Why:

- 2Q22 = Epic on Power running x86 with Cache / IRIS database.
- 2Q23 = Extend support to Epic on Power running AIX
  = Penetrate further into the Epic target healthcare market

Limitations:

- SCDM is validated with EPIC on Power AIX on bare metal only, not virtual.
  - No support for virtualized EPIC on Power AIX
- No support for EPIC running in the cloud
  - SCDM not qualified for cloud

IBM Storage Sentinel
Integrated Ransomware Protection solution with FlashSystem storage

Looks for *evidence* of a ransomware attack in snapshots

Delivered in 2Q22:

- SCDM integration with SGC
- Support for Epic Cache/IRIS (x86/Linux)

Delivered 3Q22:

- Support for SAP HANA *(x86, Power Linux)*

Delivered in 4Q22:

- Sentinel for SAP HANA with RH8.4
- Sentinel HA support – HyperSwap with SGC

Coming in 1Q23:

- Support for Epic Cache/Iris on Power AIX

Off-the-shelf solution with IBM CyberVault blueprint

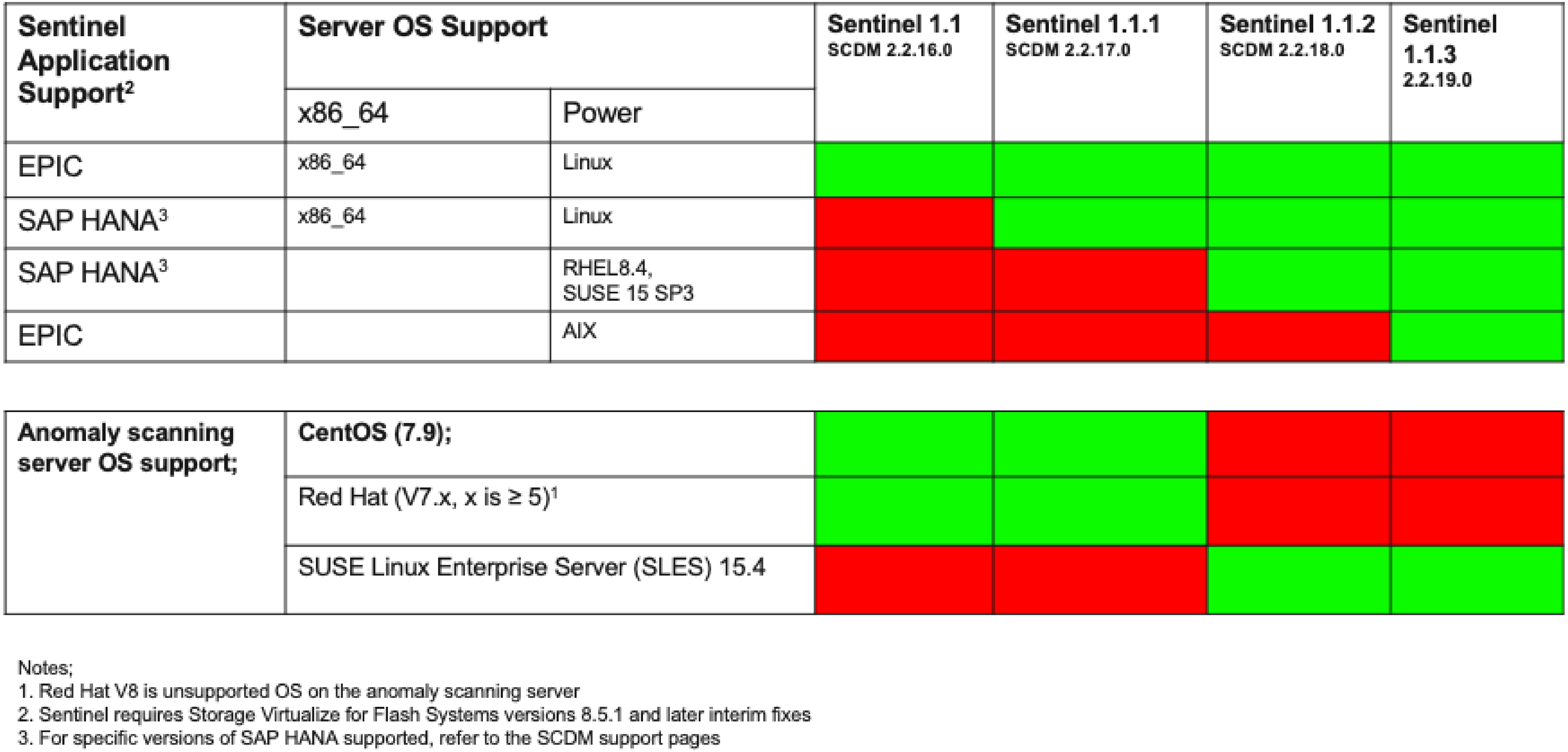
SCDM – Management of application-consistent, immutable snapshot/backup orchestration

OEM Anomoly scanning engine for detection and analysis of potential corruption

Multiple application, database support e.g.

Epic Cache/IRIS, MS SQL, Oracle, SAP HANA, VMWare, …

Summary: SCDM orchestrates the creation, management of application-aware Safeguarded copies/backups for Ransomware scan and facilitates faster recovery of data from clean copies in primary storage



Sentinel Application Support[2]	Server OS Support		Sentinel 1.1 SCDM 2.2.16.0	Sentinel 1.1.1 SCDM 2.2.17.0	Sentinel 1.1.2 SCDM 2.2.18.0	Sentinel 1.1.3 2.2.19.0
	x86_64	Power				
EPIC	x86_64	Linux	🟩	🟩	🟩	🟩
SAP HANA[3]	x86_64	Linux	🟥	🟩	🟩	🟩
SAP HANA[3]		RHEL8.4, SUSE 15 SP3	🟥	🟥	🟩	🟩
EPIC		AIX	🟥	🟥	🟥	🟩

Anomaly scanning server OS support;	**CentOS (7.9);**	🟩	🟩	🟥	🟥
	Red Hat (V7.x, x is ≥ 5)[1]	🟩	🟩	🟥	🟥
	SUSE Linux Enterprise Server (SLES) 15.4	🟥	🟥	🟩	🟩

Notes;
1. Red Hat V8 is unsupported OS on the anomaly scanning server
2. Sentinel requires Storage Virtualize for Flash Systems versions 8.5.1 and later interim fixes
3. For specific versions of SAP HANA supported, refer to the SCDM support pages

Thank you!