Advanced Technology Group

IBM Storage Virtualize 8.6.0 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

Accelerate with ATG Technical Webinar Series

Advanced Technology Group experts cover a variety of technical topics.

Audience: Clients who have or are considering acquiring IBM Storage solutions. Business Partners and IBMers are also welcome.

To automatically receive announcements of upcoming Accelerate with IBM Storage webinars, Clients, Business Partners and IBMers are welcome to send an email request to accelerate-join@hursley.ibm.com.

2023 Upcoming Webinars – click on the link to register for the live event:

September 21 – IBM DS8900F Copy Services Manager: How to create a 3-site multi-target solution in CSM

September 26 – New SAN Products: IBM b-type Gen 7 (64G) Storage Extension, High-Density Director Blade, Enhanced Security and New SANnav Release

Important Links to bookmark:

ATG Accelerate Support Site: https://www.ibm.com/support/pages/node/1125513

ATG MediaCenter Channel: https://ibm.biz/BdfEgQ

ATG-Storage Offerings

CLIENT WORKSHOPS

- IBM DS8900F Advanced Functions
- IBM Storage Point of View on Cyber Resiliency – **Coming Soon**
- IBM FlashSystem and Storage Virtualize
- IBM Storage for Data and AI
- IBM FlashSystem 9500 Deep Dive & Advanced Functions
- **IBM Storage Fusion – October 24-25 (Herndon, VA)**

Please reach out to your IBM Rep or Business Partner for future dates and to be nominated.

TEST DRIVE / DEMO'S

- North America ATG Storage - IBM Storage Scale and Storage Scale System GUI
- North America ATG Storage - IBM Storage Virtualize Test Drive
- North America ATG Storage - IBM DS8900F Storage Management Test Drive
- North America ATG Storage - Managing Copy Services on the DS8000 Using IBM Copy Services Manager Test Drive
- North America ATG Storage - IBM DS8900F Safeguarded Copy (SGC) Test Drive
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (Appliance based)
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (VMware based)
- North America ATG Storage - IBM Storage Protect Live Test Drive
- North America ATG Storage - IBM Storage Protect Plus Live Test Drive
- North America ATG Storage - IBM Storage Ceph Test Drive - (VMware based)

Please reach out to your IBM Rep or Business Partner for more information.

Accelerate with ATG Technical Webinar Series - Survey

Please take a moment to share your feedback with our team!

You can access this 6-question survey via Menti.com with code 2243 3599 or

Direct link https://www.menti.com/albneqj15g57

Or

QR Code

Advanced Technology Group

IBM Storage Virtualize 8.6.0 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

- Release Schedule
- NVMe-TCP
- ISCSI Improvements
  - Increased host count
  - Relax Adapter Policing in FS9500
  - ISCSI rewrite
- Converged LTS SV4PC Release – Amazon/Azure
- Support for TLS 1.3
- SMTP Authentication for e-mail notifications
- 65K objects on 9500
- Limit superuser commands
- Integrated ransomware detection
- SGC with mirrored snapshots (SVC ESC)
- Continue GM while transitioning to PBR
- vSphere Plugin Update
- Storage Sentinel Update

Release Schedule

- RFA Announce – 8.6.0 – May 23, 2023
- eGA – 8.6.0 – June 9, 2023
- eGA – SV4PC – 8.6.0 AWS/Azure – June 23, 2023

8.6.0 is a Long-Term Support Release (LTS). The means that it will get patches and updates until going EOS. It includes all updates in 8.5.1, 8.5.2, 8.5.3, 8.5.4.

Spectrum Virtualize is now known as Storage Virtualize

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

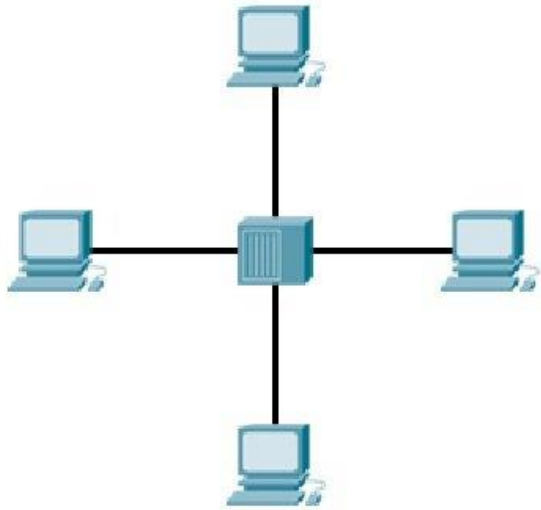
- There are 4 slated updates each year
- One LTR
  - New features
  - Has a formal announcement
  - Has all the enhancements of the previous CR's
  - Major numbering scheme (8.4,8.5,8.6....)
  - Will get all PTF's of problems found with existing features going forward
- Three CDR's
  - New features
  - 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

Prior Tech Updates

- Storage Virtualize 8.5.3/8.5.4 Technical Updates
- Storage Virtualize 8.5.2 Technical Updates

Advanced Technology Group

NVMe-TCP



Current NVMe support in FlashSystem

- NVMe/FC
  - Supported since 8.2.1 [4Q18]
  - Supported with 16/32 Gb FC adapters
  - Supports SLES/RH/ESX/Windows as initiators
  - Will support 64Gb FC adapters

- NVMe/RoCE
  - Supported since 8.5.0 [1Q22]
  - Supports RoCE (Mellanox CX-4/CX-6) adapters with 25Gb/100Gb speeds on storage (target) side
  - Supports SLES/RH/ESX as host initiators OS, with RoCE 25/40/100Gb (Mellanox CX-4/CX-5/CX-6), and Broadcom adapters
  - Requires RoCE supported Ethernet infrastructure.

Why NVMe/TCP?

- NVMe/NVMeOF protocol is designed to fully exploit the performance of all-flash storage
- Ethernet storage connection technology is gaining ground in data centers
- NVMe/RoCE requires special infrastructure
- NVMe/TCP is a ubiquitous transport and does not require special infrastructure
- First release (8.6.0) is controller based, but will take advantage of hardware offload in the future, making the increased speeds comparable with NVMe/RoCE without the need for special networking hardware

NVMe/TCP – HW, and Protocol Co-existence

- In the first release, NVMe/TCP will be supported on FlashSystem platforms that are installed with RoCE 25Gb/100Gb (Mellanox CX-4 or CX-6) adapters
- iSCSI, iWarp, iSER, NVMe/RDMA and NVMe/TCP can coexist on the same storage port with different host mapping types. This includes the ports used for replication
- The product will not support a single host working with multiple protocols, but different hosts can have different protocols working with the same i/o group/cluster
- Each NVMe/TCP port on FlashSystem supports multiple IPs and multiple VLANs

Interoperability / OS supported

- ❑ The following OS will be supported in the first release:
  - ✓ SUSE SLES 15 SP3 or later
  - ✓ RHEL 9.0 (9.2 will be qualified at a later time)
  - ✓ vSphere 7u3 or later
- ❑ The following host adapters will be supported in the first release :
  - ✓ Mellanox CX-4/5/6
  - ✓ Broadcom
  - ✓ Intel ethernet adapters
- ❑ As per host OS vendor recommendation only NVMe Native Multipath is supported for NVMe/TCP
- ❑ The NVMe/TCP implementation should work on any Ethernet switch
  - ✓ The list of switches we tested will be published

NVMe/TCP platforms supported and max number of hosts

Platform	Hosts Limit per I/O group	Hosts Limit per system
FlashSystem 9500	256	1024
FlashSystem 9200	256	1024
FlashSystem 9100	256	1024
FlashSystem 7300	256	1024
FlashSystem 7200	256	1024
FlashSystem 5200	256	512
SVC – SV2	256	1024
SVC – SV3	256	1024

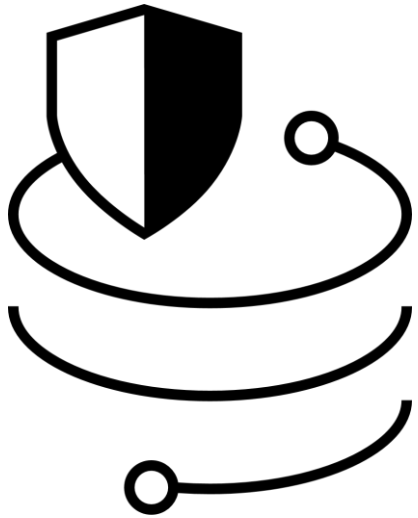
* Support for more hosts is in progress

Following initial release – more to come

- HW acceleration support
- Support additional Ethernet adapters (both target and initiator)
- Continued qualification of updated host OS releases

Advanced Technology Group

iSCSI Improvements



Increase iSCSI/iSER Hosts per I/O Group

- **Previous Limits**

- 512 Hosts per I/O Group
- 2048 Hosts per Cluster

- **New Limits**

- 1024 Hosts per I/O group
- 2048 Hosts per Cluster

- Hardware

- FS9500, FS7300, SV3

- Hardware Supported with SCORE*
  - FS9200, FS9150, FS9110, FS7200

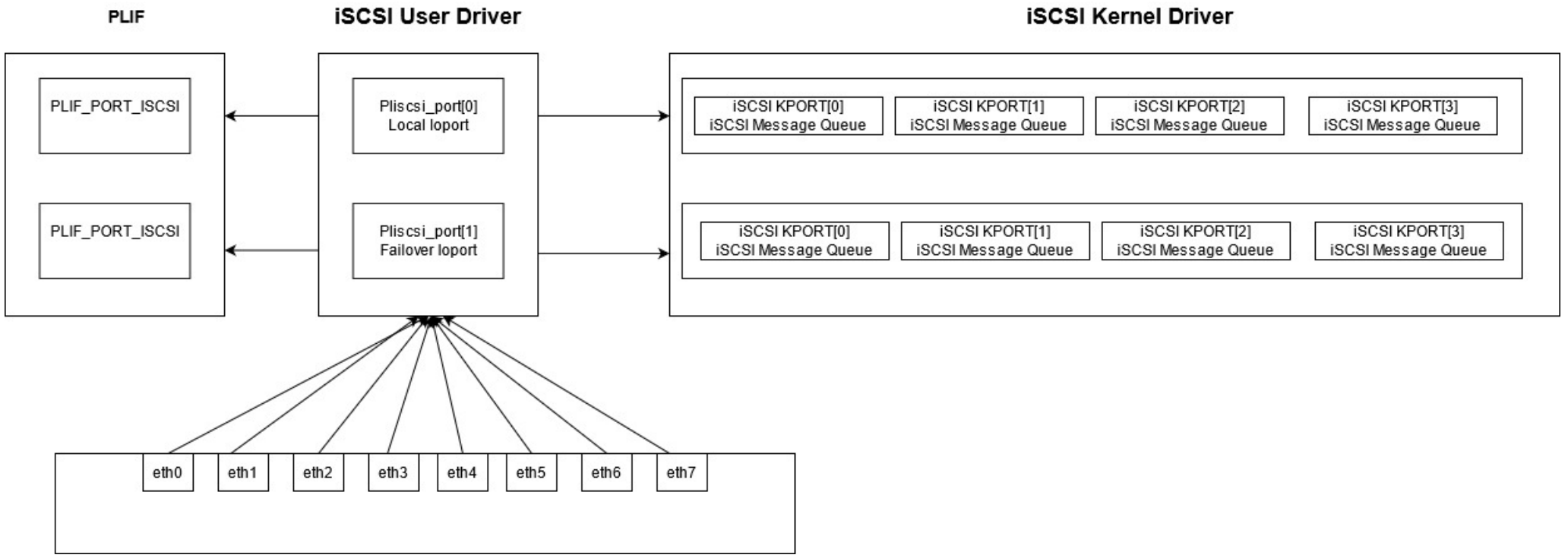
* The setlimit command needs to be run on hardware requiring a SCORE

Easing Ethernet Port Restrictions on FS9500/SV3 and FS5200

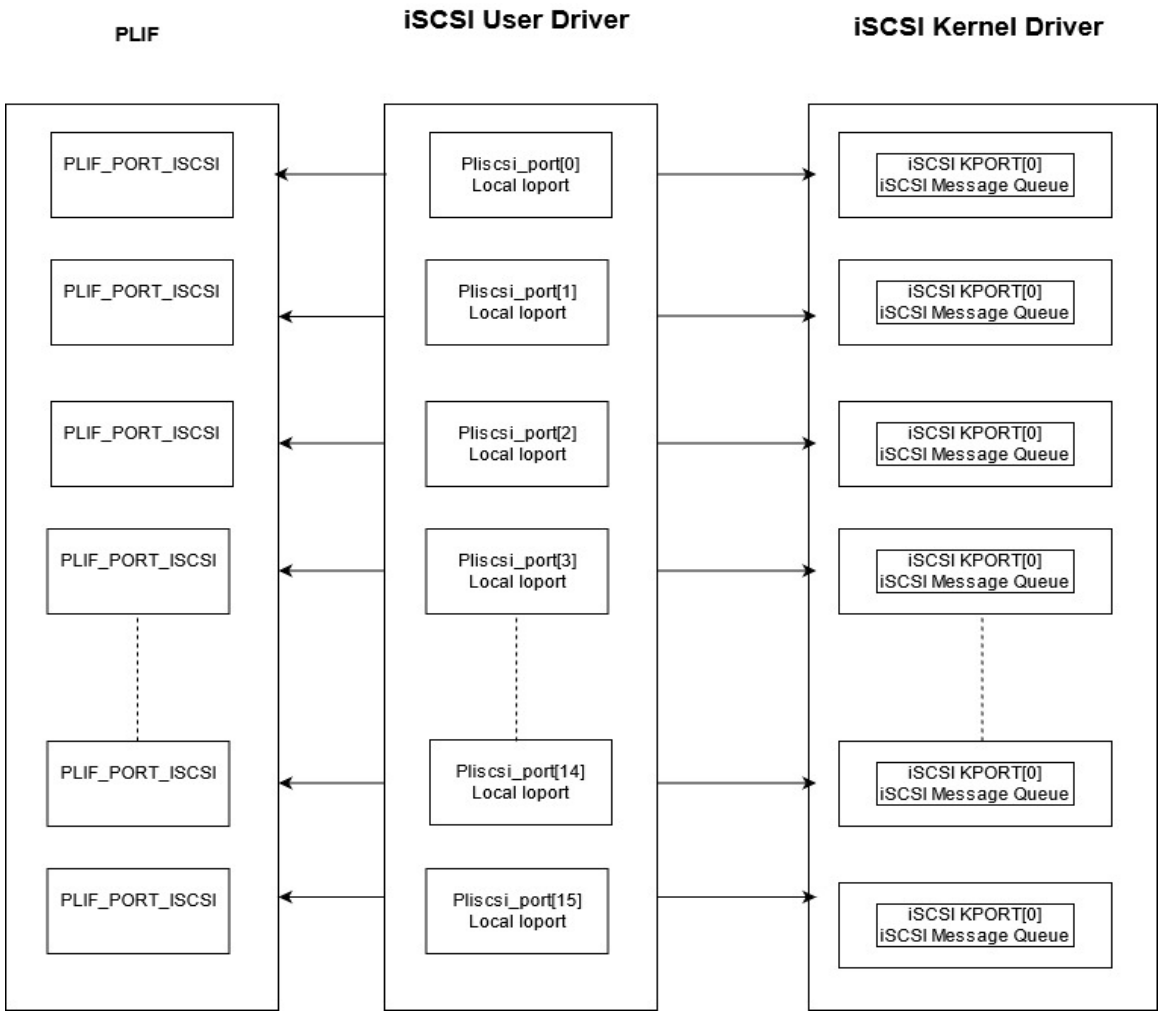
- Ethernet restrictions have been removed on the FS9500/SV3
- All cages can be fully populated with two port 25Gb/100Gb Ethernet cards
  - 12 Ethernet ports per controller/node
  - 24 per I/O Group
- For **100Gb adapters** fully populating a cage means the **bandwidth will be oversubscribed**. Each adapter will get 128Gb of it's theoretical 200Gb capability (as in the FS7300)
  - Some clients need maximum bandwidth from a card, others need more ports

- Ethernet restrictions have been removed on the FS5200 as well
- 2 – 4 port 10Gb adapters are allowed per controller
- Maximum 8 – 10Gb ports per controller
  - 16 per I/O group

Old iSCSI Model



New iSCSI Model



- Lower end platform have 8 Local-8 Failover iSCSI ioports
- Higher end platform can have up to 40Local -40 Failover iSCSI ioports.
- Each ioport is mapped to every physical port

Hardware Mappings

Number of iSCSI IOports on different platforms

Product Name	Model Number	iSCSI IOport count (Local, Failover)
9500	AH8	(40,40) Total 80
SVC	SV3	(40,40) Total 80
7300	900	(16,16) Total 32
9200	AG8	(24,24) Total 48
9150	AF8	(24,24) Total 48
9110	AF7	(12,12) Total 24
7200	AG7/800	(12,12) Total 24
SVC	SV2	(24,24) Total 48
SVC	SA2	(12,12) Total 24
5200	5H2/6H2	(8,8) Total 16
5015/5035	TWL(5015)/TWM(5035)	(8,8) Total 16
SVPC	SW1/SW2	(8,8) Total 16

Key Features

1. Optimized CPU utilization for iSCSI processing
2. Optimized CPU utilization for Soft IRQ processing
3. Higher improvement on higher-end platform
4. More bandwidth saturation for 25G/100G adapters
5. Load balancing
6. Enabled 100G adapter for iSCSI host attachment
7. No CLI changes

Upgrade Considerations

1. Smooth upgrade from previous releases
2. While upgrade no performance impact
3. Performance boost will be seen soon after the upgrade
4. Upgrade Restriction:
    1. IPs configured on a single node of an iogrp, is not allowed
    2. Hardware adapter invalid, is not allowed

Performance Improvements

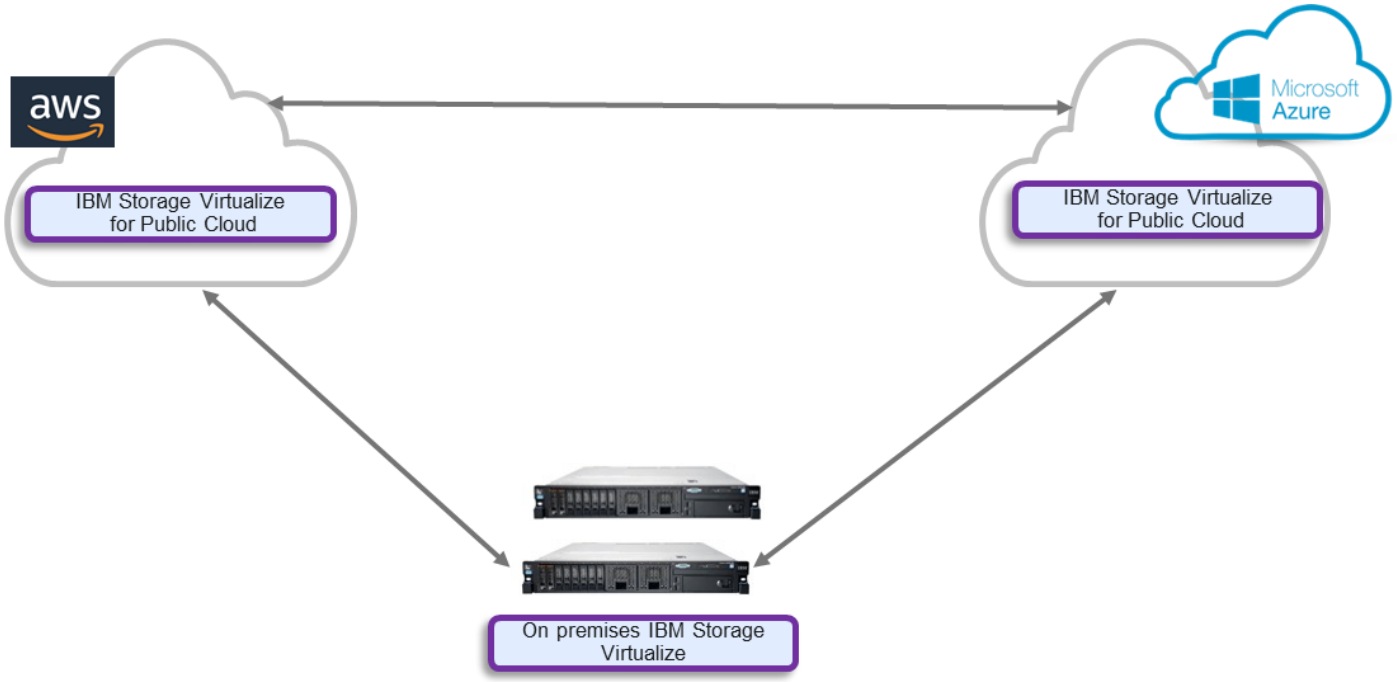
- iSCSI performance has been improved up to 2.5X in v8.6.0 compared to v8.5.3. (ex. On FS9500)
  - The greater the storage CPU core count the greater the improvement
- The performance with the new NVMEoTCP protocol is equivalent/slightly better to iSCSI on it’s initial release
  - Future enhancements will make it significantly faster than iSCSI

Converged SV4PC LTS 8.6.0 Release for AWS/Azure

IBM

Converged 8.6.0 Azure/AWS Release

- Additional support of AWS more durable io2 EBS
- AWS and Azure Host VM based on RHEL 8.7
- Multi cloud use case - Replication support between AWS and Azure
- Rebranding from IBM Spectrum to IBM Storage
- New key features support



Hybrid Multi Cloud Solution

Multi-Cloud Use Case Amazon/Azure

- Select cloud provider as per requirement like below while avoiding vendor lock-in
  - Cost reduction
  - Infrastructure optimization
  - Quality and performance
  - Cloud services and features

- Easily perform below tasks using IBM Storage Virtualize for Public Cloud across different clouds
  - Distribute workload
  - Migrate data
  - Backup data
  - Plan for disaster recovery

Policy-based replication between AWS and Azure

Maximum Round trip time (RTT) between two replicating clusters should not exceed 80 ms for Policy-based replication to work properly. While selecting AWS and Azure regions for replication keep RTT into consideration

New Key Feature Support in 8.6.0

Supported Features	Appliance release target	SVPC specific comments
iSCSI IOPs and bandwidth performance improvement	23Q2 (8.6.0)	More number of cores utilization for iSCSI processing.
TLS 1.3 support	23Q2 (8.6.0)	No support for chsecurity -sslprotocol 6 and 7.
Rebranding from IBM Spectrum to IBM Storage	23Q2 (8.6.0)	New product name - IBM Storage Virtualize for Public Cloud
SMTP authentication	23Q2 (8.6.0)	Same behavior as Appliance
Non disruptive security/software patching	23Q1 (8.5.4)	
IBM Storage Insights integration by using Call Home with cloud services	22Q4(8.5.3)	Only supported on Azure D64 VM type. (Note: Feature still under consideration, changes can happen)

– Note: The list can change. Refer to IBM Documentation version 8.6.0 for a final list of supported features

Supported ECS Configurations AWS

- Support of both public and private deployment
- Support of 2 node and 4 node cluster deployment from AWS marketplace

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

Supported EBS Configurations AWS

Supported Managed Disk	Disk Type	Use Cases	Max Disk Size (TiB)	Max throughput	Max Iops
io1/io2	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

Supported Configurations Azure

- Azure shared managed disk support for high availability
- Enhanced security with private IP deployment with Azure Network Security Group rules
- Azure load balancer support for fast cluster IP failover

Supported Managed Disk	Disk Type	Scenario	Max Disk Size (GiB)	Max throughput	Max Iops
Standard SSD	SSD	Web servers, lightly used enterprise applications and dev/test	32,767 GiB	750 MB/s	6,000
Premium SSD	SSD	Production and performance sensitive workloads	32,767 GiB	900 MB/s	20,000

Supported VM Size	vCPU	Memory GiB	Temp Storage (SSD) GiB	Max Data Disk	Max uncached disk throughput: IOPs/MBps	Max NICs/Network bandwidth (Mbps)
Standard_D16s_v3	16	64	128	32	25600/384	8/8000
Standard_D32s_v3	32	128	256	32	51200/768	8/16000
Standard_D64s_v3	64	256	512	32	80000/1200	8/30000
Standard_B1ms (Quorum Only)	1	2	4	2	640/10	2/-

Upgrade Paths to 8.6.0

- AWS
- 8.5.4 to 8.6.0 upgrade is supported

- Azure
- 8.4.3.x or 8.5.2.x to 8.6.0 is supported

TLS 1.3 Support

Motivation for Support

- NIST document**, NIST SP 800-52 Rev.2**, that provides guidance for when **TLS1.3 support will become mandatory** for US Federal users
- This Special Publication also provides guidance on certificates and TLS extensions that impact security
- It requires that TLS 1.2 be configured with FIPS-based cipher suites be supported by all government TLS servers and clients and **requires support for TLS 1.3 by January 1, 2024**

- **Implications**

- IBM should be looking to implement TLS1.3 into the next Long Term Support (LTS) for Storage Virtualize for 1H23 at the latest, as we will expect RFPs from Federal clients to start including this requirement in their 2023

What is New in TLS 1.3

- This version of the protocol uses just 5 cipher suites, all with perfect forward secrecy (PFS),
- Authenticated encryption and additional data (AEAD),
- All non-AEAD ciphers have been removed due to possible weaknesses or vulnerabilities
- Ciphers must use an ephemeral key exchange algorithm so that new key pairs are generated for every exchange
- The handshake state machine has been significantly restructured to be more consistent and to remove superfluous messages,
- All handshake messages after the ServerHello are now encrypted
- The TLS 1.2 version negotiation mechanism has been deprecated in favour of a version list in an extension

Protocol Levels on Storage Virtualize

- 2 - TLS 1.2, allow TLS 1.0, 1.1, and 1.2 ciphers
- 3 - TLS 1.2, allow TLS 1.2 ciphers
- 4 - TLS 1.2, allow TLS 1.2 ciphers but disallow RSA and static key exchange ciphers
- 5 - TLS 1.2 and TLS 1.3, disallow static key exchange ciphers **New**
- 6 - TLS 1.3, allow only TLS 1.3 ciphers **New**
- 7 - TLS 1.3, allow only ciphers that support FIPS **New**

- On a new system, the default SSL protocol level is 5 (compatibility level), whereas the default SSH protocol is 3.
- Legacy SSL protocol level 1 has been deprecated due to security reasons.

Storage Virtualize Protocol Ciphers

Table 1. Extension to the SpecV Protocol Security Levels

New SV Protocol Security Level	TLS version and Cipher suites
5	• Intended to be a compatibility mode which supports both TLS 1.2 and 1.3. • It aims to try and negotiate TLS 1.3 first, and fall back to TLS 1.2 if necessary: as per Appendix D.1 of the TLS 1.3 Spec.
	Ciphers supported for TLS 1.3: • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_GCM_SHA256 • TLS_AES_128_CCM_8_SHA256 • TLS_AES_128_CCM_SHA256
	Ciphers supported for TLS 1.2: • Subset from level 3 with the static ciphers RSA or ECDH for key exchange removed • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, • TLS_DHE_DSS_WITH_AES_256_GCM_SHA384, • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, • TLS_DHE_DSS_WITH_AES_128_GCM_SHA256.
6	• Only uses TLS 1.3 • Offers the five ciphers mentioned above.
7	• Only uses TLS 1.3 • Only offers cipher TLS_AES_256_GCM_SHA384 (FIPS mode complaint).

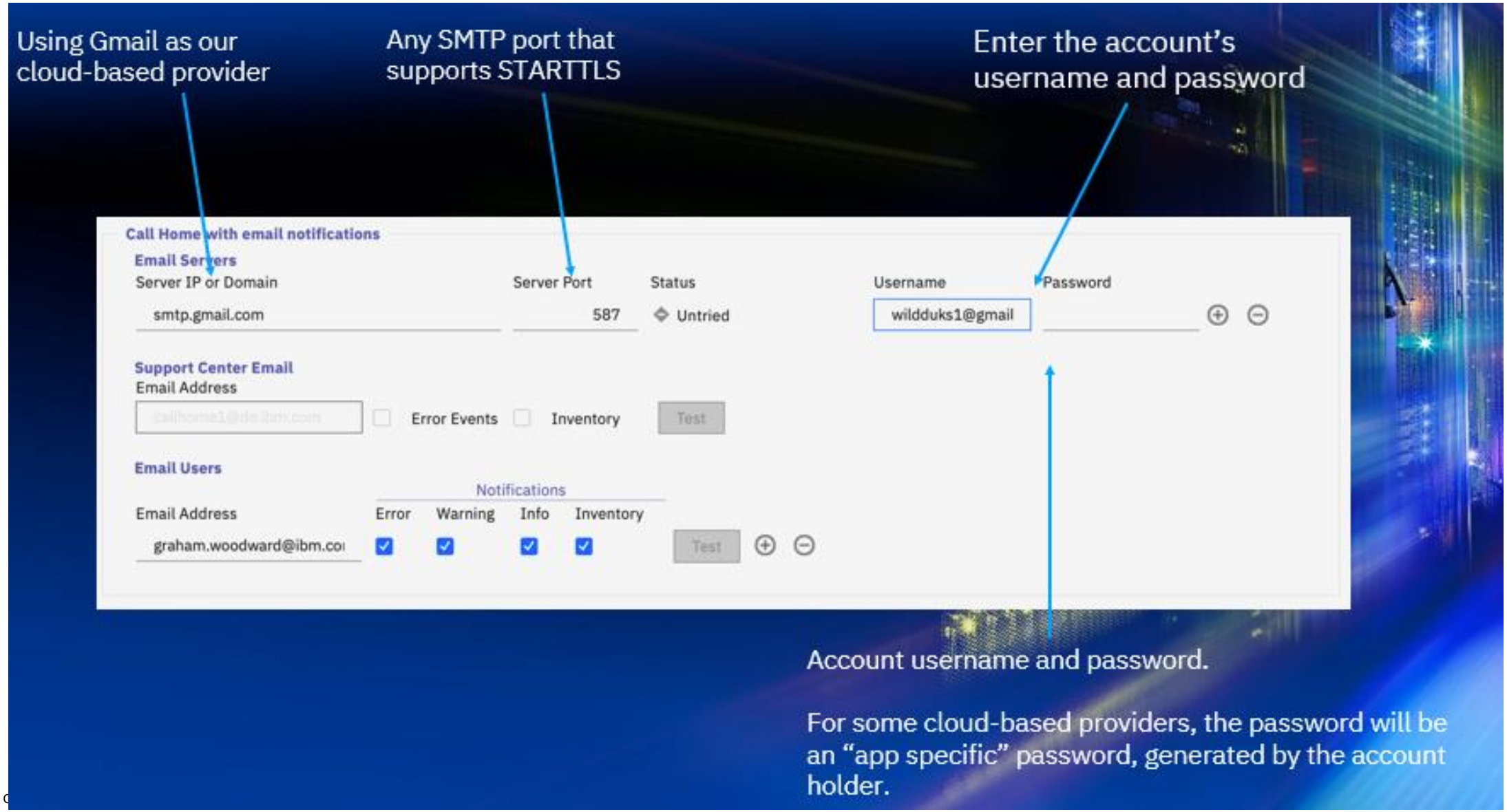
New “Suggested Protocol Level”

- Intended to be a compatibility mode which supports both TLS 1.2 and 1.3 (Level 5)
- It aims to try and negotiate TLS 1.3 first, and fall back to TLS 1.2 if necessary
- Can be selected from the GUI as **Automatic** for the protocol level.
- Future system code upgrades will automatically update the protocol level to the new suggested level

SMTP Authentication

SMTP Authentication

- In this 8.6.0.0 release, Storage Virtualize now supports Cloud-based email providers
- Including providers such as Google mail (both Gmail and G-Suite for Business), Microsoft Outlook, Yahoo and more…
- An appropriate account username and password is required when sending emails via these providers
- Storage Virtualize can now also authenticate the email server (cloud and on-prem) via the server’s public certificate
- Storage Virtualize also provides customers with the ability to specify a different “from: ” email address separate to their call home reply email address


Using Gmail as our cloud-based provider
Any SMTP port that supports STARTTLS
Enter the account's username and password
Call Home with email notifications
Email Servers
Server IP or Domain
Server Port
Status
Username
Password
smtp.gmail.com
587
Untried
wildduks1@gmail
Support Center Email
Email Address
Error Events
Inventory
Test
Email Users
Notifications
Email Address
Error
Warning
Info
Inventory
graham.woodward@ibm.co
Test
Account username and password.
For some cloud-based providers, the password will be an "app specific" password, generated by the account holder.

The optional secure argument

- CLI only
- Tells the SMTP client how to connect to the remote email server
- 3 options available - New email servers will default to ***-secure yes***

mkemailserver ... -secure yes (the default if not specified)

- SMTP client queries the email server
- If the server supports STARTTLS, then a secure connection is created
- If the server does not support STARTTLS, then the connection is terminated, and the email not sent

mkemailserver ... -secure try

- SMTP client queries the email server
- If the server supports STARTTLS, then a secure connection is created
- If the server does not support STARTTLS, then the connection continues insecurely

mkemailserver ... -secure no

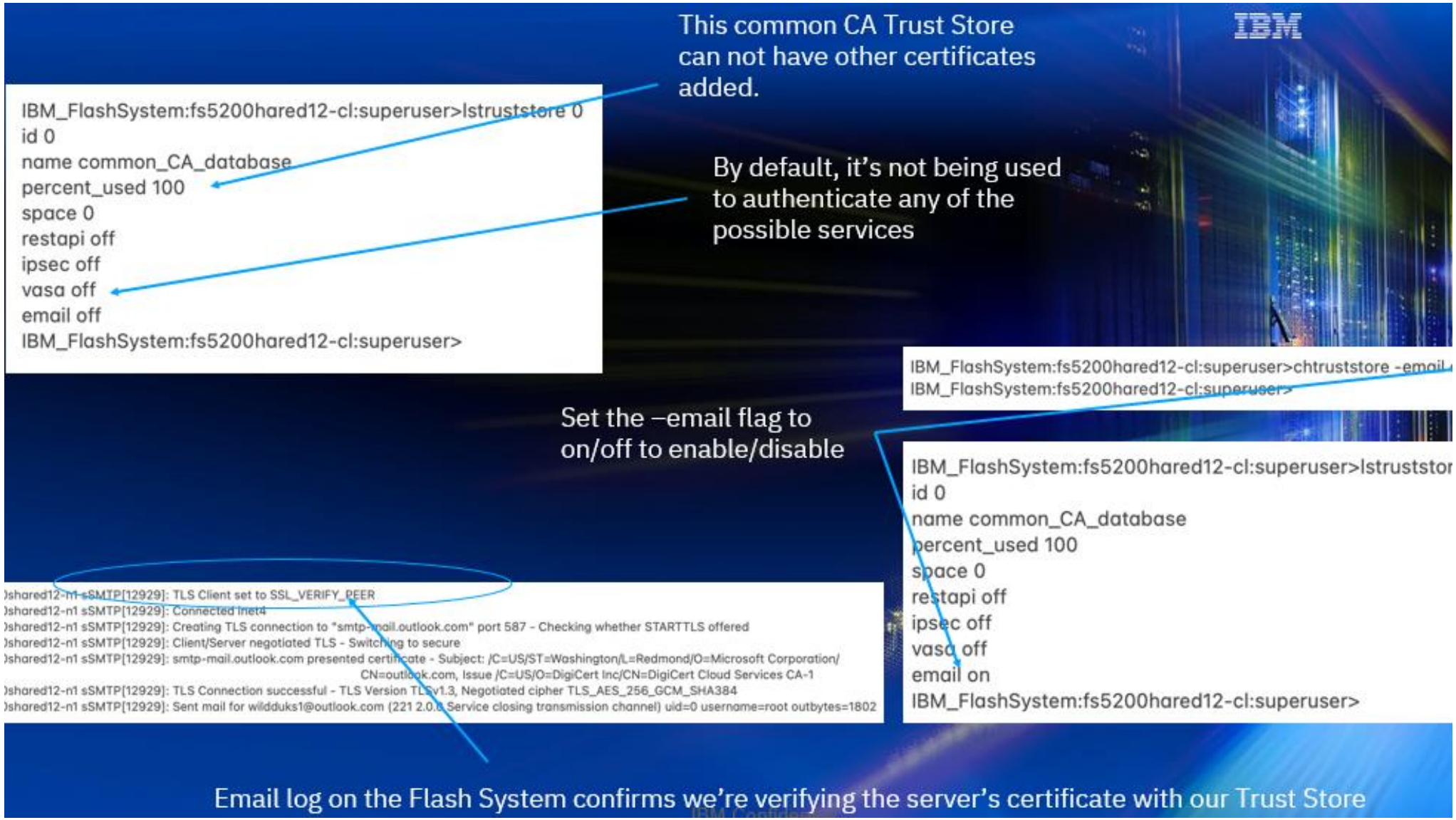
- SMTP connects insecurely and sends emails insecurely
- Used to support old legacy email servers that do not support TLS

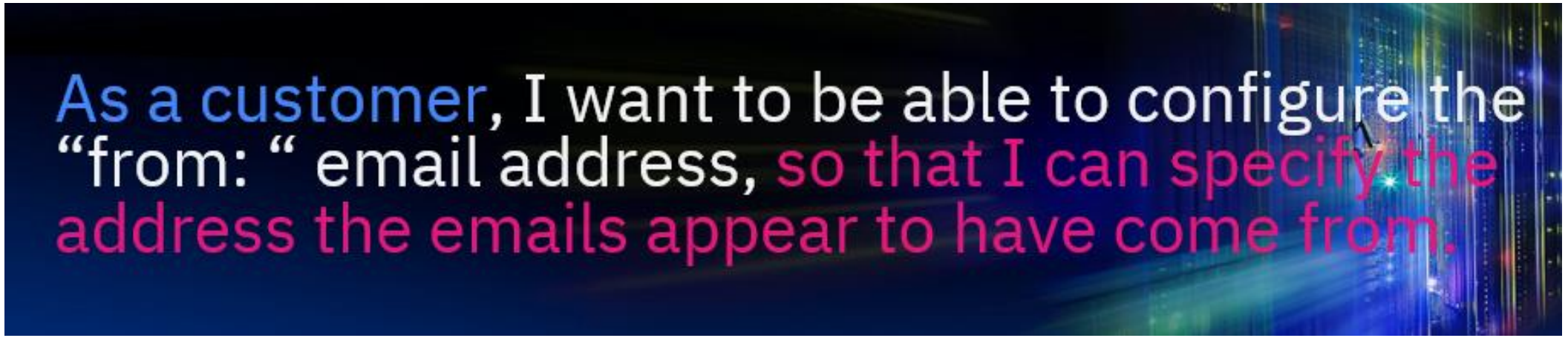
Caution...

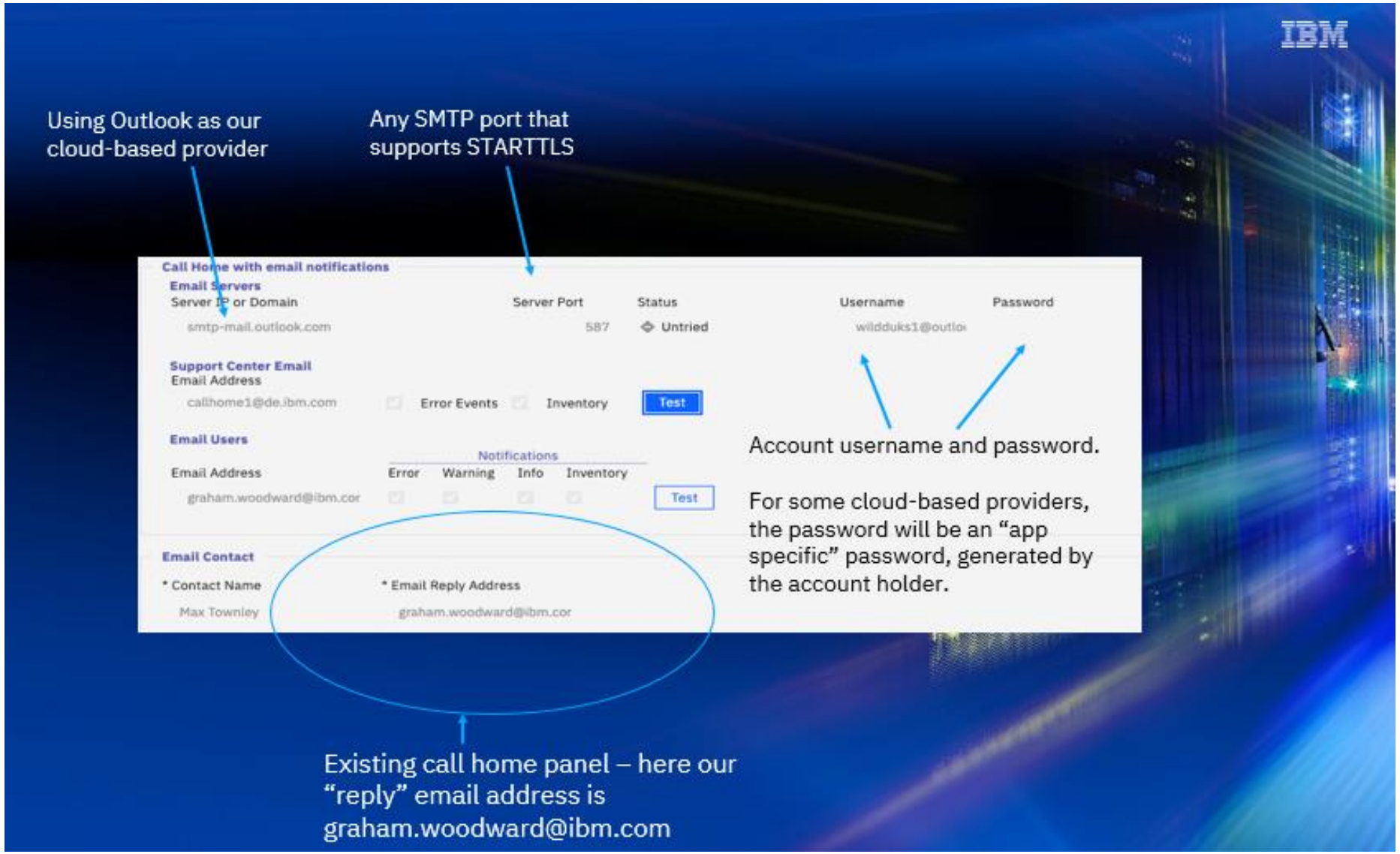
Using ***-secure no*** on cloud-based providers will fail...the email server won't want you sending the auth details insecurely...See the next slide

Trust Stores

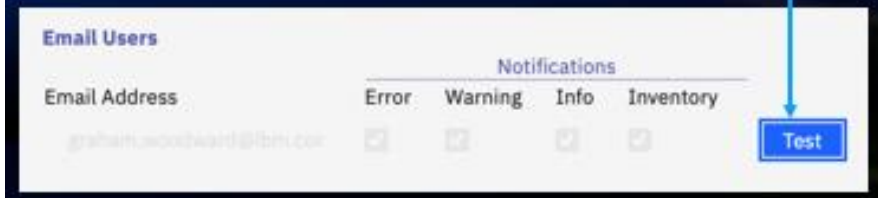
- Storage Virtualize 8.5.1.0 introduced a concept of Trust Stores
  - The ability to upload public X509 certificates in to a trust store
  - These trust stores can be used to authenticate the configured remote services/systems
- Storage Virtualize 8.6.0.0 is bundled with a common Certificate Authority bundle
  - Contains the public intermediate certificates used to sign common cloud-based email providers

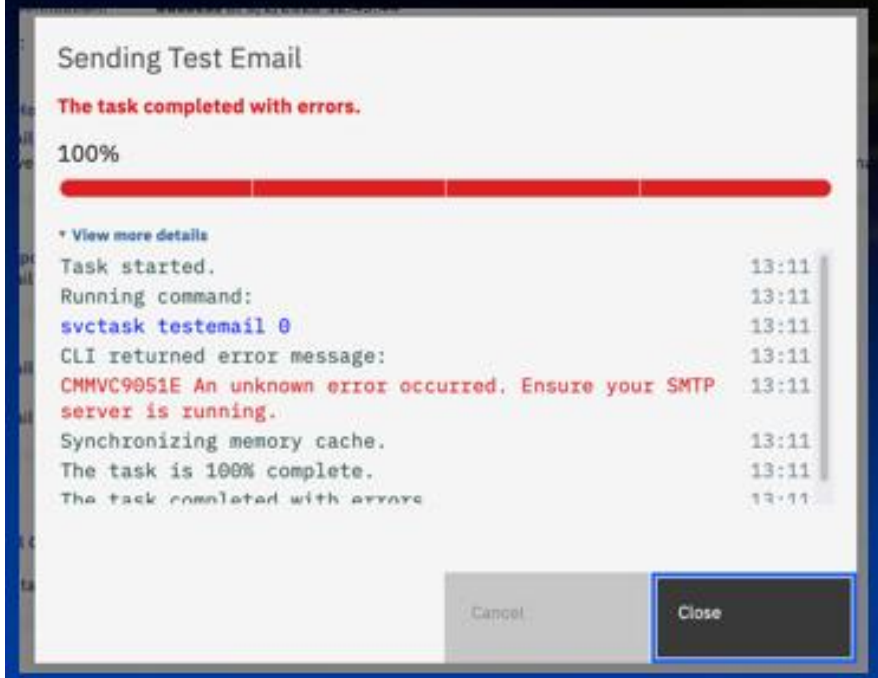






Let's try a test email






```
IBM_FlashSystem:fs5200hared12-cl:superuser>lsemailserver 0
id 0
name emailserver0
IP_address smtp-mail.outlook.com
port 587
status failed_temporary
error_description mail from denied / mailbox unavailable
username wildduks1@outlook.com
password_set yes
secure yes
IBM_FlashSystem:fs5200hared12-cl:superuser>
```

The ***error_description*** field is giving us a clue as to why the email was not successfully sent.

Here we see ***mail from denied / mailbox unavailable***

65K Objects on FS9500

Limit Commands Requiring Superuser

65K Volume Objects on the FS9500

- 8.5.4:

- FS9500 supports 32,100 objects
- FS7300 supports 32,100 objects

- 8.6.0:

- FS9500 supports 65,000 objects
- FS7300 supports 32,100 objects

Performance Recommendations

- We do not recommend over 50K objects for systems not using DRP pools
- We recommend volume group sizes of no more than 128 volumes when using over 32,100 objects

Limit Commands Requiring superuser

- With the advent of Two Person Integrity (TPI) and an increased focus on security, more and more clients are wanting to lock the superuser account
- Current commands requiring the superuser account makes this difficult
- IBM is decreasing the number of commands that require superuser privileges

New ‘svctask’ Commands

Service Assistant Command	Cluster Command
satask chserviceip	svctask chnodeserviceip
satask restartservice	svctask restartservice
satask startservice	svctask stopsystem –enterservicestate
satask stopservice	svctask startsystem -exitservicestate

– All of these commands, except for `svctask chnodeserviceip`, can be run by users with the SecurityAdmin and Administrator roles. The `svctask chnodeserviceip` command can only be run by users with the SecurityAdmin role.

New ‘sainfo’ Commands

Service Assistant Command	Cluster Command
sainfo lsservicestatus	svcinfo lsnodestatus
sainfo traceroute	svcinfo traceroute

Integrated Ransomware Detection

New IDCD within Storage Virtualize

Inline data corruption detection with AI and ML

Today, IBM FlashSystem, a key component of our IBM Storage for Data Resiliency portfolio, handles some of the most challenging application and data workloads our clients have and is engineered to deliver fast response and recovery operations from data breaches and cyber-attacks—ransomware or state-sponsored. IBM FlashSystem is designed to offer verified and validated recovery times from data corruption events within hours.

We are excited to continue innovating in this space by introducing a new feature: inline corruption detection that uses AI and ML services to detect data changes that can be indicative of threats or direct attacks on your data sets in near real-time. In the second half of the year, we will extend these capabilities down to our patented computational storage flash drives—FlashCore Modules—to bring detection as close to the data as possible, further reducing time to detection. This will help your staff to act quickly and decisively, and continue to deliver business outcomes while your team mitigates and recovers from a threat efficiently.

– https://www.ibm.com/blog/announcement/ibm-storage-more-value-in-store/

But How Do You Detect Ransomware

Detection By

Network Signals	Network-Level Monitoring for Anomalies
Threat Signature	Sample Hash Comparison

But How Do You Detect Ransomware

Detection By

Network Signals	Network-Level Monitoring for Anomalies
	Network level
Threat Signature	Sample Hash Comparison
	File System Level
Data Behavior Signals	Monitoring for Anomalies

But How Do You Detect Ransomware

Detection By

Network Signals — Network-Level Monitoring for Anomalies

Network level

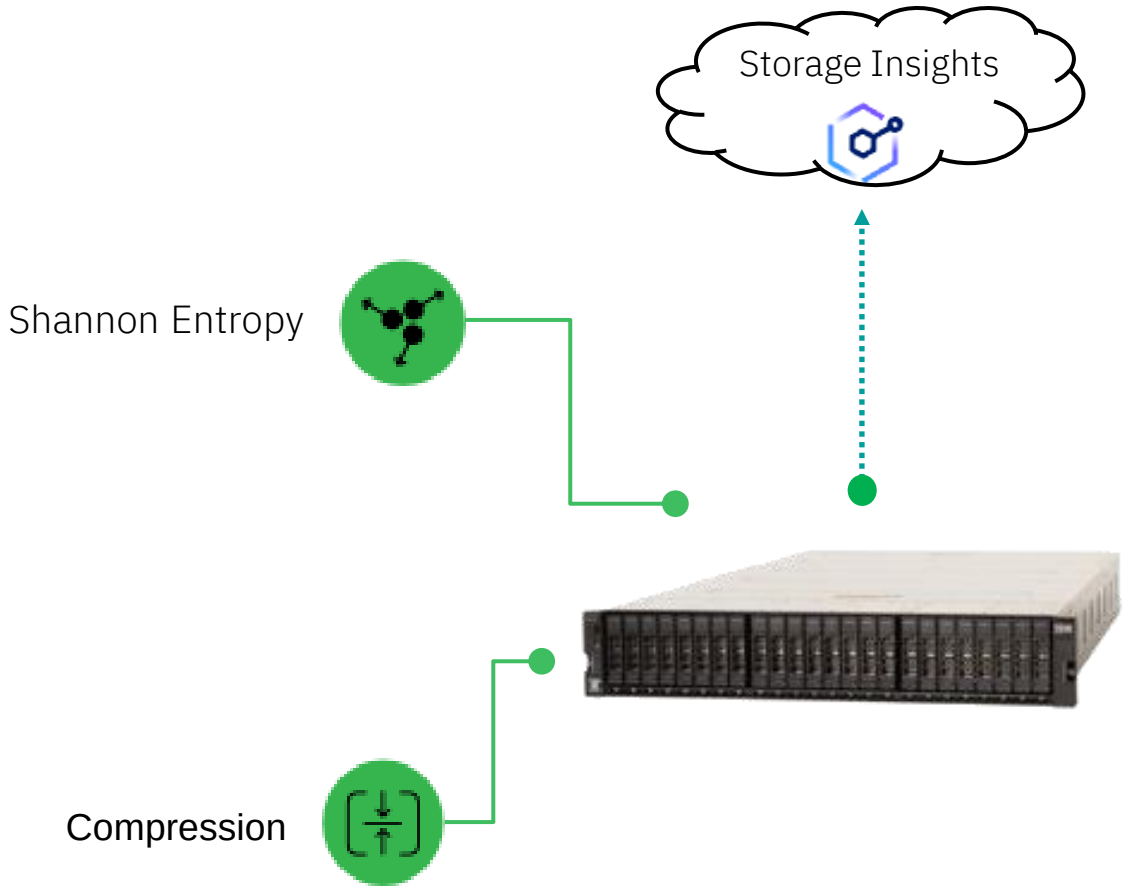
Threat Signature — Sample Hash Comparison

File System Level

Data Behavior Signals

Block Level Monitoring for Anomalies

Workload anomaly alerts in **8.6.0**



- Using FlashSystem controller CPU, calculate Shannon Entropy on **incoming write I/Os**

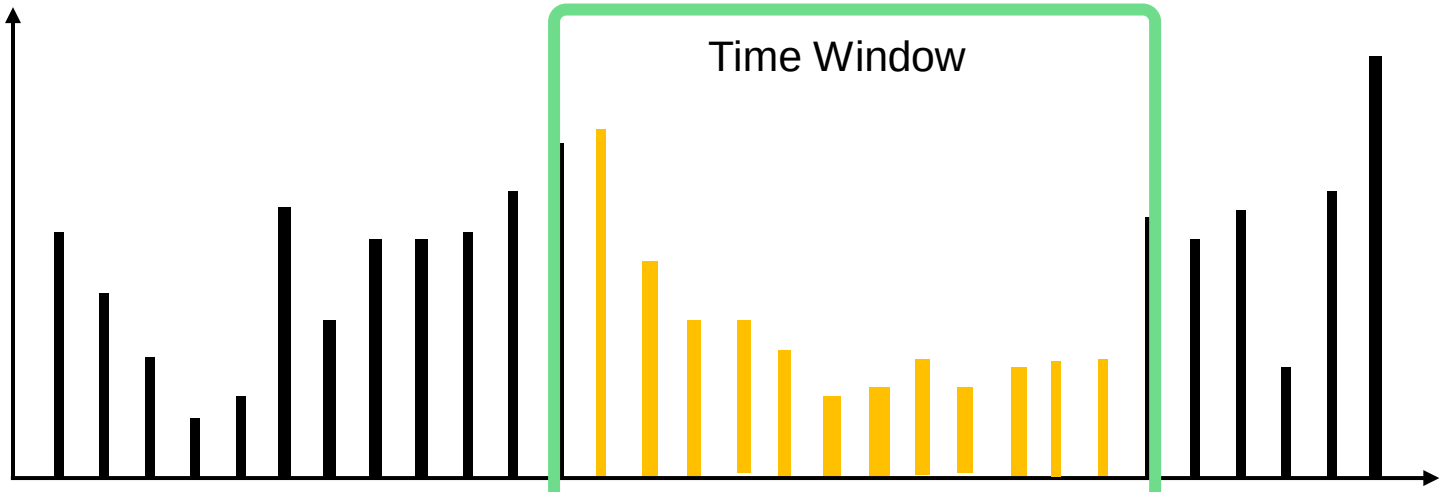
- Shannon entropy is used to detect highly random data, such as encrypted data written in by ransomware

Shannon Entropy is calculated (byte by byte) in the write cache destage, but it is computationally intensive.

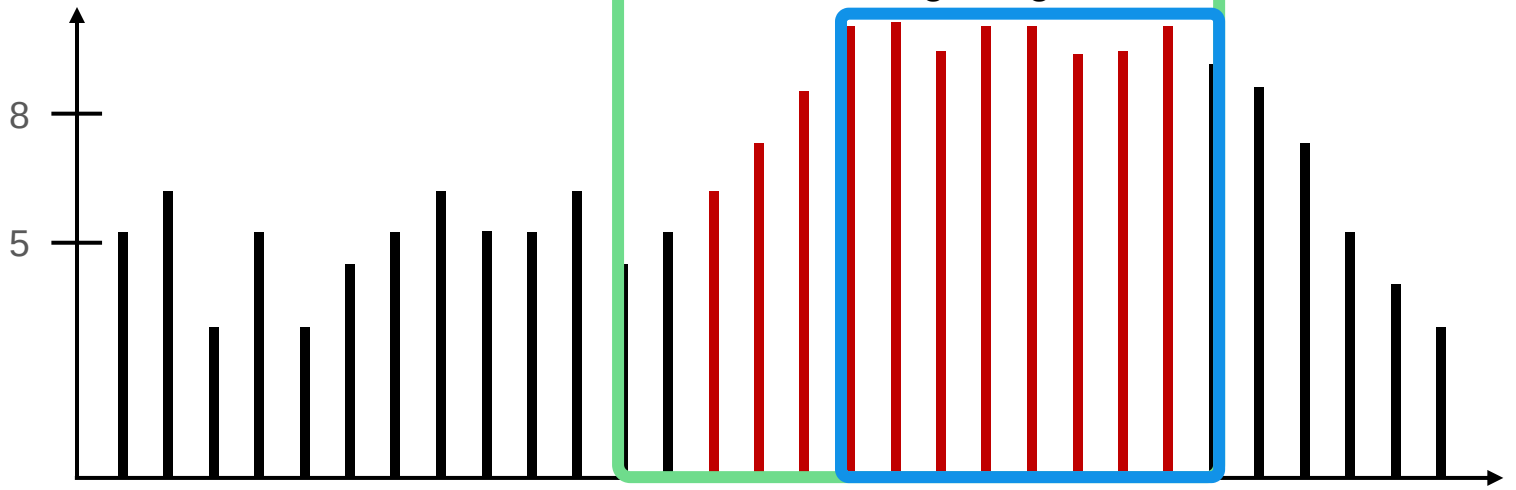
To reduce performance impacts, it is sampled in 1 in ever 100 IOs

How statistics will be used

Drive level Compressibility



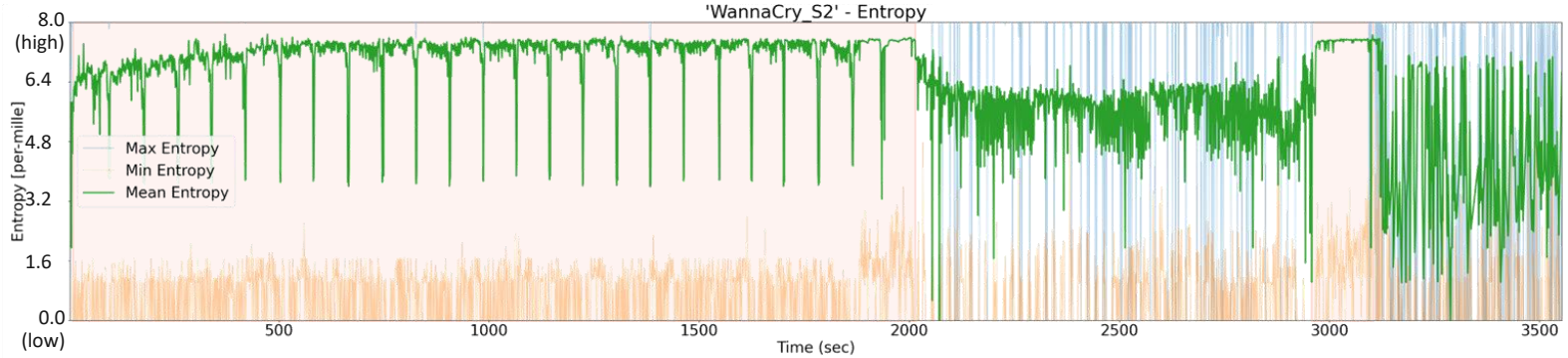
Entropy of Incoming Writes



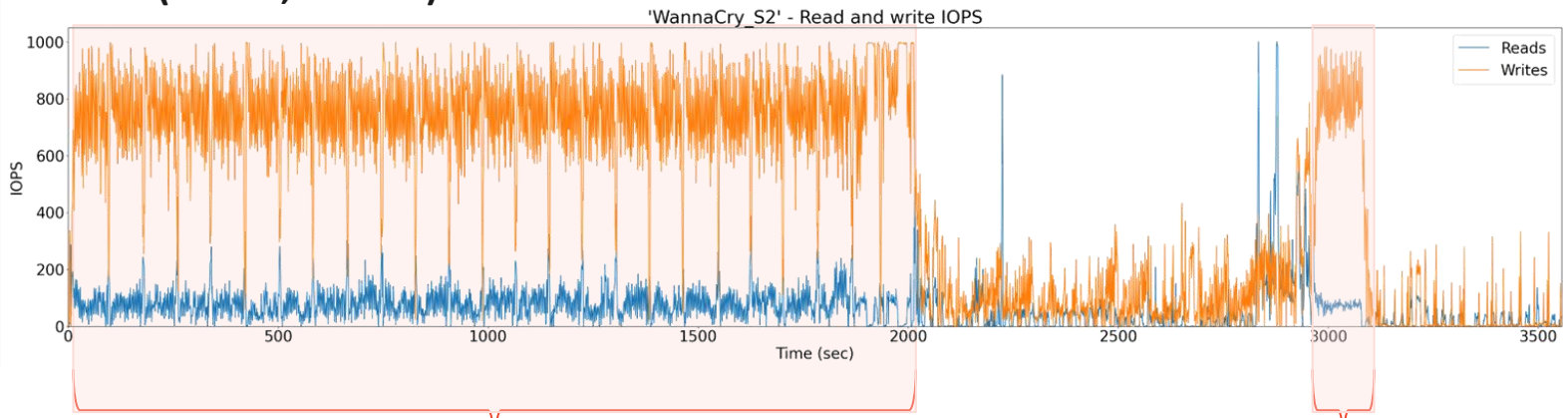
Characteristics found in IO traces from ransomware

- Malware such as ransomware attacks can be detected from storage IO patterns and data analysis
- Example “Wannacry”:

Encrypted payload (– avg, – max, – min):

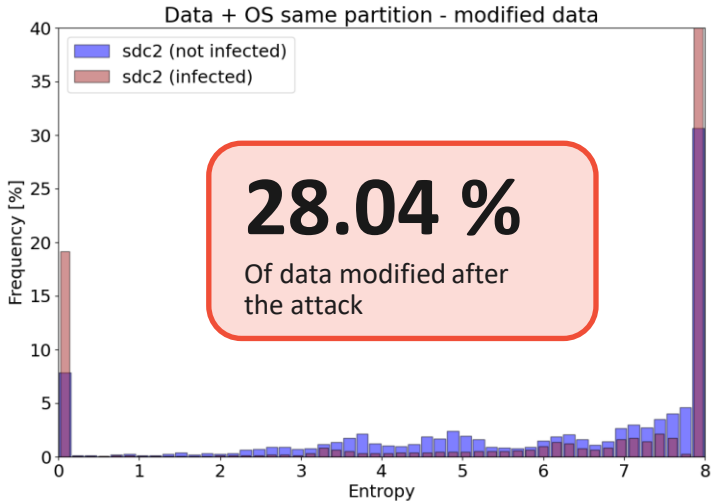


IOPS (– read, – write):



IO activity of ransomware

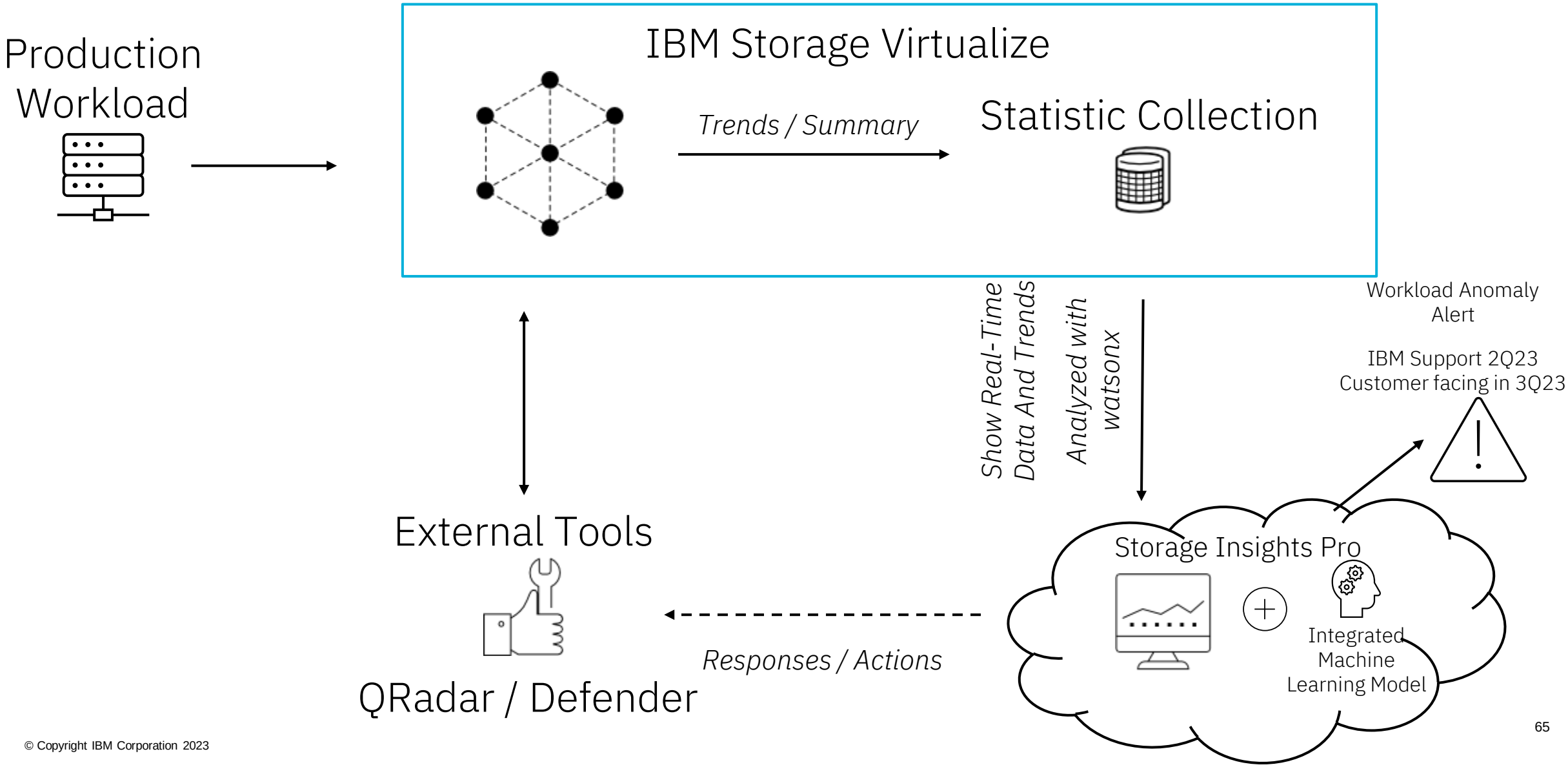
Payload encrypted – before and after attack:



28.04 %

Of data modified after the attack

Ransomware Monitoring Architectural Overview



SGC with Mirrored Snapshots

Bitmap Increases for SV3

Out of Space Option

VGS Support for Mirrored Snapshots

- Prior to 8.6.0, volume group snapshots were only allowed on non-mirrored volumes

- With 8.6.0
  - Snapshots can be added to volume groups containing mirrored volumes – snapshots will be mirrored automatically
    - **This means Volume Group Snapshots now support SVC Enhanced Stretched Cluster**
  - Mirrored copies can be added to volumes with snapshots – copies must be manually added to snapshots first
  - Mirrored snapshots work with Safeguarded Copy and internal scheduler

Adding Mirrored Copies to Volumes with Snapshots

- For existing volumes with snapshots, mirrored copies must be added to the snapshots before being added to the parent volume
- New fields have been added to lsvolumesnapshot to help users find the relevant snapshots

```
lsvolumesnapshot -showhidden -delim :

snapshot_id:snapshot_name:volume_id:volume_name:volume_group_id:volume_group_name:parent_uid:time:expiration_time:state:safeguarded:mirrored:
pool_1_id:pool_1_name:pool_2_id:pool_2_name:snapshot_vdisk_id:snapshot_vdisk_name:snapshot_mapping_id:snapshot_mapping_name

1:snapshot1:2:fred3:0:fred:0:220707160003::active:no:yes:0:mdiskgrp0:1:mdiskgrp1:15859:vdisk4:15859:fcmap4

1:snapshot1:1:fred2:0:fred:0:220707160003::active:no:no:1:mdiskgrp1:::15860:vdisk3:15860:fcmap3

1:snapshot1:0:fred1:0:fred:0:220707160003::active:no:no:0:mdiskgrp0:::15861:vdisk2:15861:fcmap2

0:snapshot0:1:fred2:0:fred:0:220707154401::active:no:no:1:mdiskgrp1:::15862:vdisk1:15862:fcmap1

0:snapshot0:0:fred1:0:fred:0:220707154401::active:no:no:0:mdiskgrp0:::15863:vdisk0:15863:fcmap0
```

Increased Bitmap Space on SV3

- FlashCopy,VGS and mirroring now share bitmap space on SV3 nodes only
- SV3 has 20 GiB of combined bitmap space per I/O group for VGS, FlashCopy and mirroring
  - VGS or mirroring could use all 20GB if available
- FlashCopy, PBR and CV still limited 4 GiB of the 20 per I/O group

SV3	8.5.4	8.6.0
FlashCopy	4 GiB	4 GiB
Volume Group Snapshots	4 GiB	20 GiB
Vdisk mirroring	512 MiB	20 GiB

New Out of Space Behavior Option

- New global option to control out of space behaviour for the system:
- chsystem -snapshotpreserveparent yes

- The default is no

snapshotpreserveparent setting	no	yes
Behaviour when latest snapshot goes offline	Parent goes offline Snapshot remains	Parent stays online Snapshots may be deleted

Continue GM While Transitioning to PBR

Converting to PBR

- Prior to 8.6.0

  - Each consistency group needed to be stopped, with the consistency group and relationships deleted (keeping a target point in time) and then a policy could be added to a volume group to implement PBR
    - When the volume group was in sync the original target could be retired

- With 8.6.0 +

  - MM or GM (not GMCV) can continue to run while syncing PBR volume groups
  - This helps with clients who feel they MUST continue GM while transitioning to PBR.

Restrictions

- The RC relationship cannot have a primary change volume configured
- The Remote Copy relationship cannot have its direction switched or be made a secondary by starting following a stop-with-access
- The common volume cannot be made a PBR recovery volume
- Remote Copy cannot be configured on a PBR volume (it's a one-way migration!)
- The relationship must be either a Metro Mirror or Global Mirror relationship
- The relationship must not be in a consistency group (this also excludes three-site relationships)
- The relationship must be consistent synchronized and clean
- The relationship must not be a migration Metro Mirror relationship.
- The volume being moved must be the primary
- A change volume must not be allowed to be moved between IO groups

VMWare Plugin Update

New vSphere Plugin

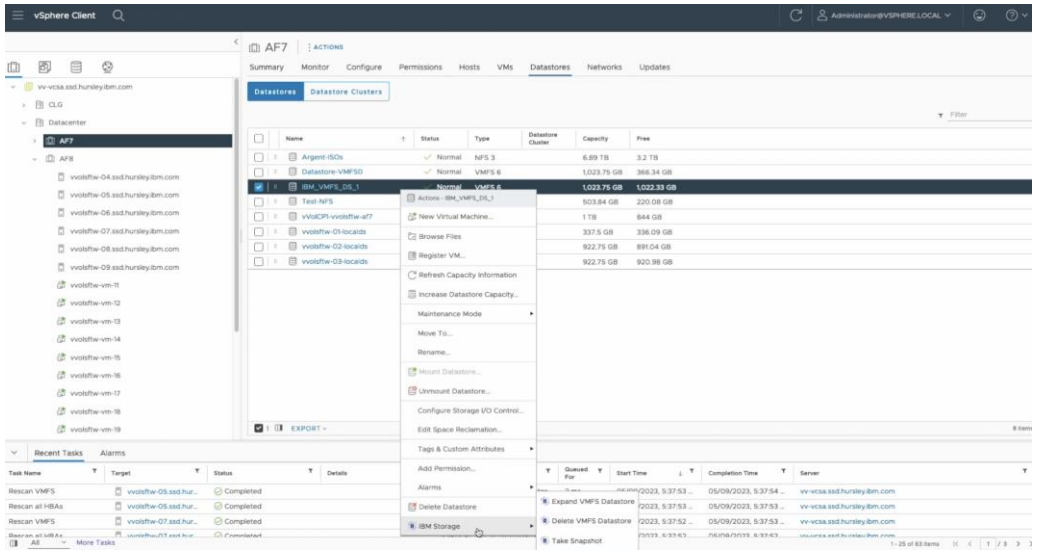
Version 1.1 available in 2Q23

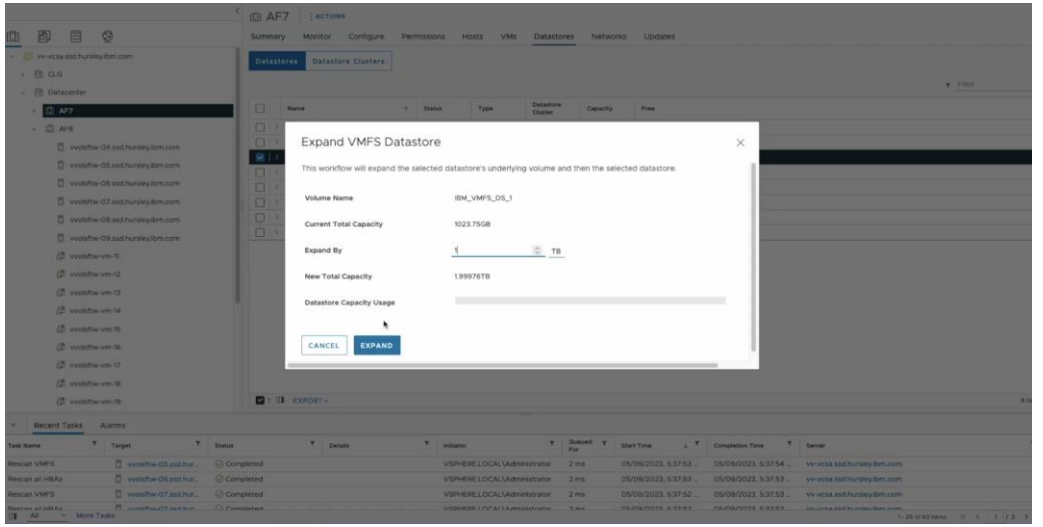
Create multiple VMFS datastores

Expand datastores

Delete datastores

Simple snapshot creation





IBM Storage Sentinel Update

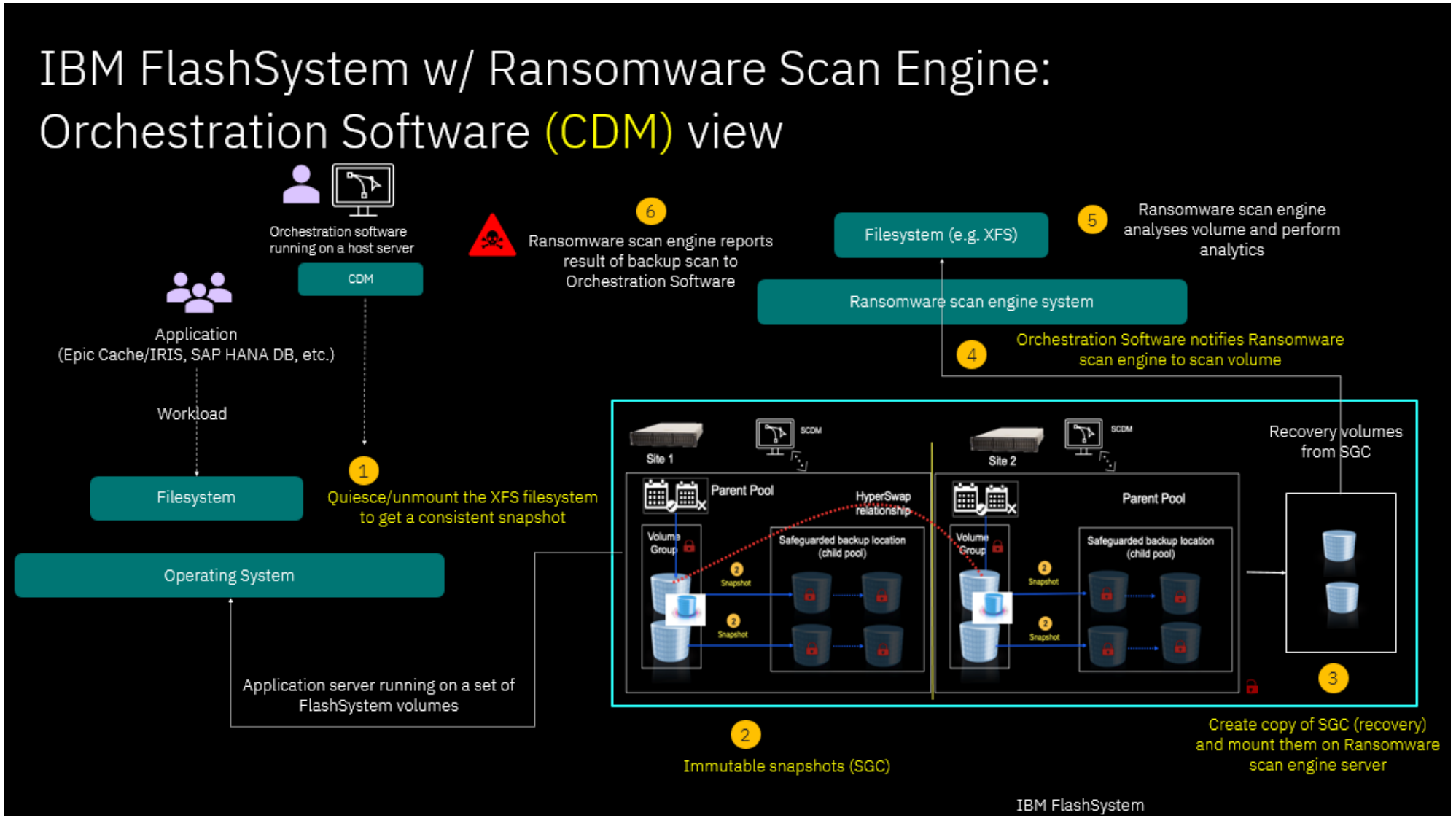
Storage Sentinel Overview

- Launched June 9, 2022
- Sentinel 1.1 – Initial launch
  - Scan Safeguarded copies that were Flashcopies in a Safeguarded Child pool
  - Scan EPIC Cache and IRIS databases running on Linux
- Sentinel 1.1.1 - 22Q3
  - Support scanning SAP HANA databases
- Sentinel 1.1.2 - 22Q4
  - Expand support for HANA databases on RHEL 8
  - Changed OS requirement for anomaly scan server to SLES 15
- Sentinel 1.1.3 – 23Q1
  - Scan EPIC databases running on AIX
  - Requires AIX proxy to mount to anomaly scan server

Sentinel 1.1.4

- Scan Oracle databases running on either Linux or AIX
- Oracle versions supported
  - 12c
  - 18c
  - 19c
  - Only supported databases running as standalone, RAC is not supported
- OS support for Oracle scanning
  - RHEL 7
  - SUSE 12
  - AIX 7.2
  - AIX 7.3 is currently being qualified

IBM FlashSystem w/ Ransomware Scan Engine: Orchestration Software (CDM) view



Thank you!

Accelerate with ATG Technical Webinar Series - Survey

Please take a moment to share your feedback with our team!

You can access this 6-question survey via Menti.com with code 2243 3599 or

Direct link https://www.menti.com/albneqj15g57

Or

QR Code