

Advanced
Technology
Group



Accelerate with IBM Storage: TS7700 Encryption and Data Protection

Bob Sommer
Certified Tape Specialist

-
- Please join the Advanced Technology Tape Team discuss the encryption features of the TS7700. This includes: Internal Disk Encryption, External Disk Encryption, Physical Tape Encryption, Encryption over the wire, DS8K to TS7700, and TS7700 to Cloud. Other data security discussions include Selective Data Access Control (SDAC) and Logical WORM.

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:

July 25 - [A Ceph Primer - The Difference Between IBM Storage Ceph and Ceph Fusion Data Services](#)

August 1 – [Data Resiliency with IBM Storage Scale](#)

August 22 – [Introduction to IBM's newest Tape Storage, the IBM Diamondback Tape Library](#)

August 29 – [IBM Storage Virtualize 8.6 and Storage Sentinel Technical Update](#)

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 – August 29-30, 2023, Virtual**
- IBM Storage Point of View on Cyber Resiliency
- IBM FlashSystem and Storage Virtualize
- IBM Storage for Data and AI
- **IBM FlashSystem 9500 Deep Dive & Advanced Functions – August 2-3, 2023, in Raleigh, NC**
- IBM Storage Fusion

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](https://www.menti.com) with code 2243 3599 or

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

Or

QR Code



Advanced
Technology
Group



Accelerate with IBM Storage: TS7700 Encryption and Data Protection

Bob Sommer
Certified Tape Specialist

Panelists:

Ben Smith, Toni Alexander, Carl Reasoner, Sandy Browning, Beth Stugis, Bill Banas, Nicole Payne



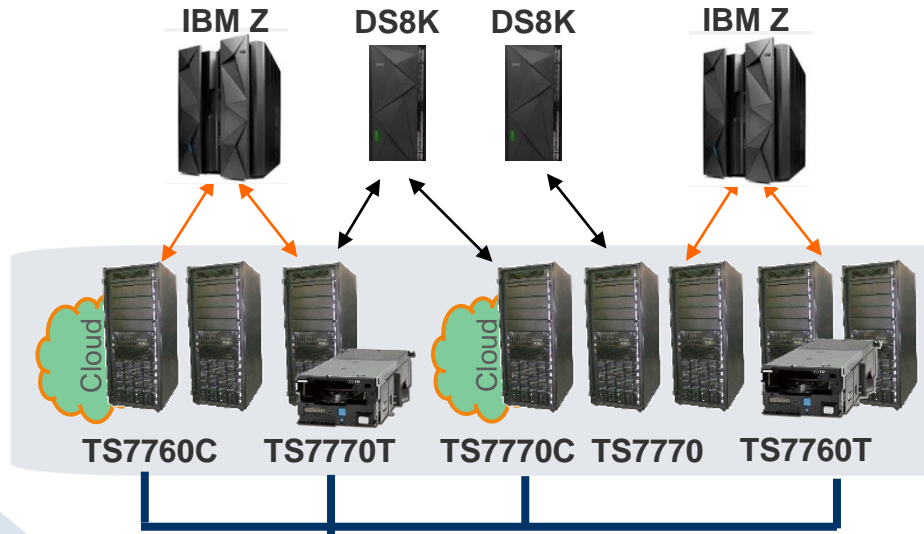
Meet the Speaker



Bob Sommer is a graduate of the Michigan State University in Math Education (Bachelor) and Montclair State College in Computer Science (Masters). After 7 years of teaching high school math, he joined IBM as a Systems Engineer. With 39 years at IBM, he has always been on the front lines with customers. He supported both Tape and Storage starting in 1990's and has been dedicated to selling and supporting Virtual Tape and Physical Tape since 1999. He is currently with the Advanced Technology Group specializing in Tape Sales and technical support.

IBM TS7700 IBM Z Virtual Tape Leveraging Grid as Cloud Tape Storage for IBM Z

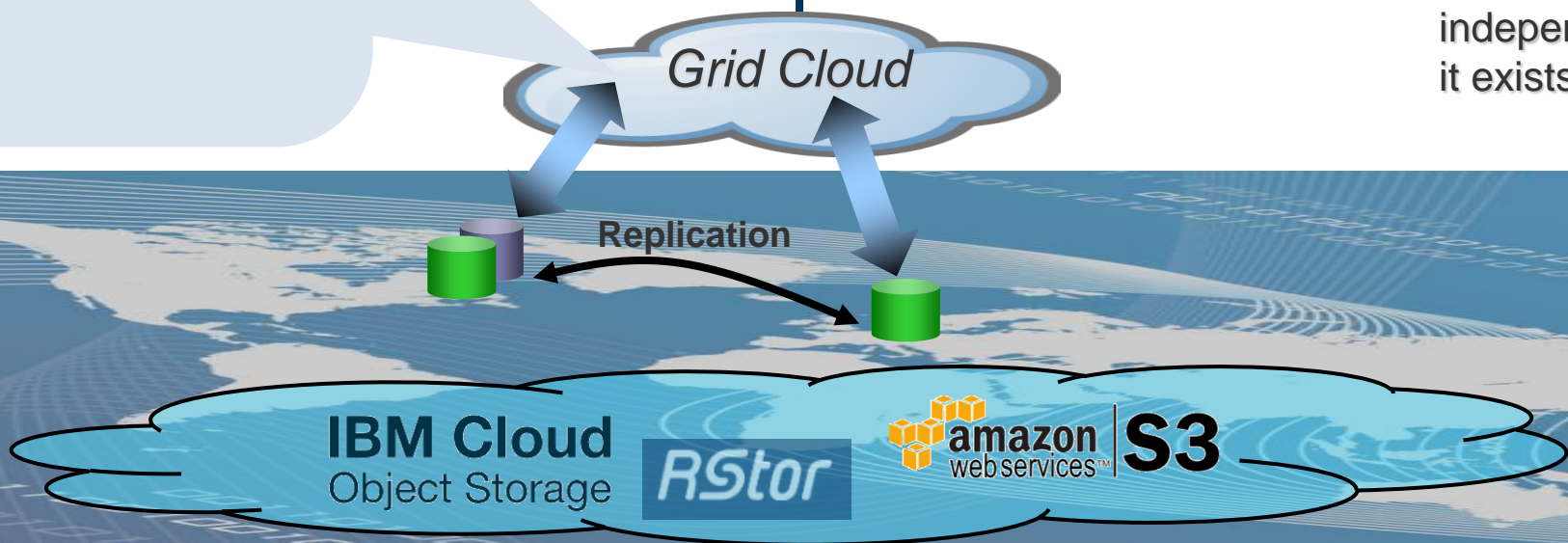
- Grid Cloud**
- 8-way consisting of any generation of TS7700 – throughput 100MBS to 4000 MBS
 - Synchronous and asynchronous replication
 - AES256 Encryption at rest and in flight
 - Tight integration with IBM Z and DFSMS policy managed
 - Optional Cloud Storage Tier to object storage
 - Optional DS8000 Offload target for DS8000 TCT
 - Optional integration with physical tape



Cumulative 16Gb FICON throughput up to 4.8GB/s * 8

IBM Z hosts view up to 496 * 8 equivalent devices

Grid access to all data independent of where it exists





CyberSecurity

Auditing & Compliancy
 Flash Copy DR Testing
 Events & Task logging (MI/SNMP)
 Rsyslog tamperproof logging
 Upload SSL Certificates or use default
 SP800-131a Compliancy Settings

Management Interface Security
 Granular Roles & Permissions
 Local or LDAP Login
 Dual Control Sensitive Settings



Cloud Tier
 Cloud Storage Tier
 Cloud Export
 Cloud Export Recovery
 Cloud Export Recovery Testing
 Logical Volume Version Retention
 Single Logical Volume Version Recovery
 PIT snapshots for airgap
 Multi-cloud support (public, private, multi-tenancy)
 Cloud device encryption

HTTPS

Secure Data Transfer (AES256)

Copies between TS7700s

Exports to cloud storage devices

DS8K to TS7700 TCT Objects

Object Store

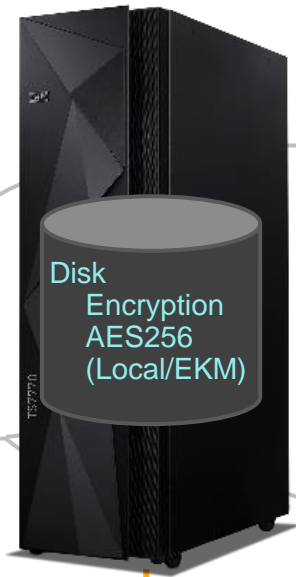
Ethernet



IBM z/OS

DS8900

GRID
 TS7700 Grid technology to store multiple copies of data anywhere in the world (up to 8 clusters)
 Fast migrate/recall at disk speeds
 Active/Active...
 Each cluster is an access point



Physical Tape Tier
 Tape Encryption AES256 (EKM)
 Copy Export Secondary Copy
 Copy Export Offsite Airgap
 Copy Export Recovery
 Copy Export Recovery Testing

TS4500



FICON



Virtual Tape

Fibre Channel

Physical Tape



Extended Retention and Access

Selective Device Access Control (SDAC)
 Category Retention w/Expire Hold

LWORM
 LWORM Retention

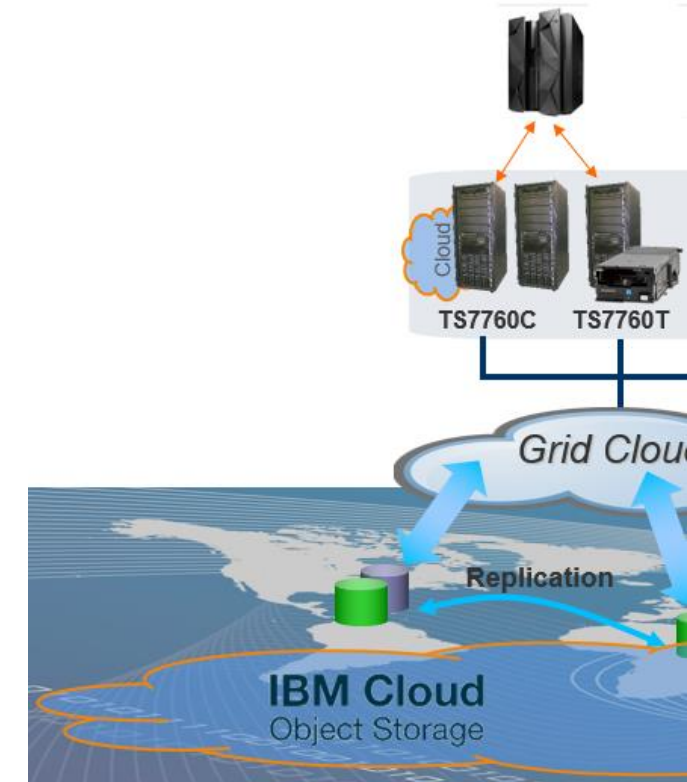
TS7770 Overview

- Built on the **Power9** platform (TS7770 VED)
 - Two 10 core, 3.8GHz processors
 - 64GB and **128GB** DDR4 Memory
 - **16Gb FICON** (up to 4 adapters, 2 ports per adapter, 512 paths per port)
 - 1Gb Copper and 10Gb LW Grid Network (up to 4 ports total)
 - 16Gb FC attachment to disk cache and tape drives (up to 16 ports)
 - **3.8TB SSD or SAS for pSeries storage**
 - **Common DS8000 pSeries hardware, I/O bays and adapters**
 - Single phase power (30AMP), Three Phase 400V support via iRPQ
 - Primary ethernet and FC adapters integrated into pSeries slots



IBM TS7700

- **z/OS Synergy**
 - No additional z/OS software required to support TS7700
 - Full access to all IBM propriety tape library command sets
 - Host sees entire TS7700 Grid versus a series of independent MTLs
 - DFSMS OAM Management of TS7700 clusters
 - TMS Integration, including house keeping
 - Device/Scratch Allocation Assist
 - 3,968 shared devices per composite library
 - Numerous exclusive functions
 - Full DFSMS volume granular policy management
 - CUIR automated device online/offline processing
 - Replication, LWORM, Cloud, Physical Tape Usage and many other features.
 - IBM Z intelligent, allowing efficiencies such as impressive zero RPO synchronous copy speeds.
 - User commands (i.e. LI REQ) and tools support.
 - Can partition with zVM, zVSE, zTPF
 - End to end FICON CRC protection



TS7770 Disk Cache

- Performance from 100 M/sec to 4000 MB/sec
- Large Capacity (Option 1)
 - 10TB 7.2K SAS Drives, RAID6 Distributed RAID Pools
 - 157 TB usable capacity per pair of drawers
 - 789 TB usable capacity base Frame
 - 2.37 PB 1x Expansion Frame,
 - 3.90 PB 2x Expansion Frames
 - Concurrent disk cache drawer expansion
- High IOPS Enabled SSD Capacity (Option 2) – NEW with 5.2
 - Performance equal to and exceeding 10 drawer SAS configurations
 - 3.84 TB SAS SSD Drives, RAID6 Distributed RAID Pools
 - 60 TB usable capacity for single drawer
 - Maximum of 4 drawers for a total of 260 TB usable capacity
 - Concurrent disk cache drawer expansion

IBM Synergy: Leveraging Flash Systems 5030



Capacity On Demand

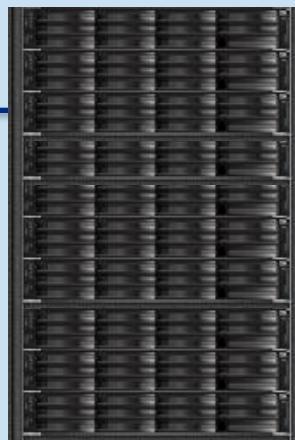
Enabled in 20TB and/or 100TB increments

Full AES256 Encryption

Both Local and External Key Management supported

Encryption must be enabled at time of purchase

TS7770
HDD cache



Select the right TS7770 solution for your use case

New

TS7770
Flash cache



New

**FC5999

TS7770
Flash cache controller



System	IBM TS7770 Capacity Model	IBM TS7770 Performance Model	IBM TS7770 High-Performance Tape/Cloud Controller
Cache Drives	10 TB NL-SAS HDD	3.84 TB SSD	3.84 TB SSD
Minimum Configuration usable capacity	157 TB	60 TB	60 TB
Usable capacity per drawer pair on base frame	157 TB	120 TB	60 TB
Cache Drawers on base frame (min / max)	2,4,6,8,10	1, 2	1
Usable capacity per system frame	789 TB	120 TB	60 TB
Usable capacity per system	3.94 PB	260 TB	60 TB
Optional Expansion frames	2	-	-
Cache Compression 5:1	19 PB	600 TB	300 TB
Added Tape attach support with 5:1 compression*	500 PB	500 PB	500 PB
Added Cloud Storage Tier with 5:1 compression*	500 PB	500 PB	500 PB
Standalone Throughput+ (32Kb, 8x16Gb FICON)	4.1 GB/sec	4.3 GB/sec	4.3 GB/sec
Bi-Directional Copy Throughput+	2.8 GB/sec	4.4 GB/sec	4.4 GB/sec
Minimum Rack Space	18 U	16 U	16 U

R5.3: Expert Care – 3948-VED

	Advanced	Premium
Hardware service / parts replacement	24x7 Contact target response time objective Severities 1 & 2 - 2 hours Severities 3 & 4 - 4 hours Onsite target objective (after PD) Severity 1 - 4 hours Severity 2 - next day Severities 3 & 4 - mutual agreement	24x7 Contact target response time objective Severities 1 & 2 - 2 hours Severities 3 & 4 - 4 hours Onsite target objective (after PD) Severity 1 - 4 hours Severity 2 - next day Severities 3 & 4 - mutual agreement
Software Support Services – how-to, installation, usage and configuration questions	Yes	Yes
Automated ticket management and alerting	Yes	Yes
Predictive Support - issue alerting	*Yes	**Yes
Dedicated Technical Account Manager (TAM)		Yes
30 min response severities 1 & 2		Yes
Remote code updates (2x per year)	Optional add-on via Feature Code (with fee)	Yes
On-site code update	Optional add-on via Feature Code (with fee)	Optional add-on via Feature Code (with fee)
Media Retention	Optional add-on via Service Pac / TSS Service	Optional add-on via Service Pac / TSS Service
IBM Installation	Optional add-on via Service Pac / TSS Service	Optional add-on via Service Pac / TSS Service

Simple to bundle

Configure system and support in one tool

Up-front and predictable pricing

Fixed percentage of system cost

Simple to choose

Which tier?

Basic, Advanced or Premium

And for how long?

1-5 years

*Advanced - Storage Insights enablement
 **Premium - Storage Insights Pro enablement
 Warranty - 1 yr 24x7 Same Day IBM On-site Repair

TS7770 Encryption and Data Security

- **Internal Disk Encryption**
- **External Disk Encryption**
- **Physical Tape Encryption**
- **Secure Data Transfer**
- **DS8K to TS7770 Encryption**
- **TS7770 to Cloud Encryption**
- **Other Topics for Data Security**
 - **SDAC**
 - **Dual Authentication**
 - **Logical Worm**

TS7770 Internal Disk Encryption

- **Prerequisites**

- Disk encryption is available on a new order from manufacturing that ordered either [FC 5272, Disk Enabled Encryption](#) or [FC 5276, Enable disk encryption - External Key Management](#). An order of [FC 5272](#) or [FC 5276](#) come with [FC 7405, Encryption CSB \(USB Flash Drives \(Four Pack\)\)](#) which provides four USB sticks. An entire file system must be encrypted; All arrays in all strings must be encrypted. All strings in the cluster must be encrypted.
- All TS7770 configurations with 3948 or 3956-CSB/XSB cache that have any encryption type that is enabled is ALWAYS shipped with local key management enabled ([FC 5272](#)). This encrypts the data in the CSB processor and places that encrypted data onto regular disk drives.
- The local encryption (FC 5272 Disk Enabled Encryption) is configured during the TS7770 initial installation by the service person. FC 5272 Disk Enabled Encryption is not available for field Install on the TS7770 and needs to be shipped from manufacturing for any Encryption.
- FC 7405 must be ordered on every 3956-CSB in the TS7770 configuration.
- [FC 7405 provides four USBs sticks per 3956-CSB used to store the local encryption keys.](#)

TS7770 External Disk Encryption

- The External Key Encryption ([FC 5276](#)) must have [FC 5272](#) installed on the TS7770 server before initial installation. All TS7700 configurations with any encryption type enabled is ALWAYS shipped with local key management enabled first
- Once a TS7770 with FC 5272 is configured in a customer environment and able to communicate with an external key server, then FC 5276 can be activated to transition to external key management..
- You can manage the encryption key for the disk drive modules (DDMs) externally.
- You can manage the encryption key for the cache disk drive modules (DDMs) externally.
- For external key management of encryption, the encryption must be enabled onsite by an IBM service representative.
- The encryption key server is installed and configured on the network.
 - Supported on TS7770 with 8.50.0.xx microcode:
 - IBM Security Key Lifecycle Manager (SKLM) - Now GKLM
- Supported on TS7760 ([goes end of service on 12/31/24](#)) with 8.4x.x.xx microcode and higher levels:
 - IBM Security Key Lifecycle Manager (SKLM) – Now GKLM

TS7770 Tape Attached Encryption

- FC9900 is put on TS7770
- TS1150, TS1160 in a TS3500 (goes end of service 12/31/23)/TS4500 are supported
- The encryption key server is installed and configured on the network.

Supported on TS7770 with 8.50.0.xx microcode:

- IBM Security Key Lifecycle Manager (SKLM) - Now GKLM
- Supported on TS7760 with 8.4x.x.xx microcode and higher levels:
 - IBM Security Key Lifecycle Manager (SKLM) – Now GKLM

For Sizing for GKLM physical tape only, multiply number of physical drives by largest native(raw)TB cartridge size. Example: 16 TS1160's holding 20TB – JE media -320TB

Though, at this number, going to 1 PB is actually cheaper. Check econfig.

GKLM also can be used for External TS7700 disk encryption as well as DS8K

GKLM


- 1) IBM Security® Guardium® Key Lifecycle Manager provides a simple solution to the complex problem of encryption key management. Encryption keys have their own lifecycles that are separate from the data that they protect.
- 2) IBM Security Guardium Key Lifecycle Manager helps you control key lifecycle processes from initialization and activation through rotation and deletion.
- 3) The solution helps you simplify and automate manual tasks which can reduce operational costs
- 4) At least **two** GKLM servers would be required.

IBM's centralized key management solution for all encryption solutions

Guardium Key Lifecycle Manager




Manage Encryption Keys



Align with PCI & NIST Guidance



Manage IBM and non-IBM products via KMIP/REST



Automatic Key Rotation



Transparent Encryption and Key Management


Storage Devices



Tape:
IBM LTO/
TSxxxx,
Virtualization
Engine,
Quantum,
Spectra Logic



IBM Disk:
DS8xxx
family,
DS5xxx
family




Flash Storage




Cloud Storage, Elastic Storage, Big Data, Data Warehouse (Spectrum family, Netezza)



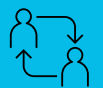
Network Storage (NetApp)



Servers (Lenovo System x)



TDE Database (Oracle)



3rd Parties: EMC, Bloombase, Hitachi, Fujitsu ...

Non-Storage

Sensus Smart Meters

VMware vSAN & vCenter

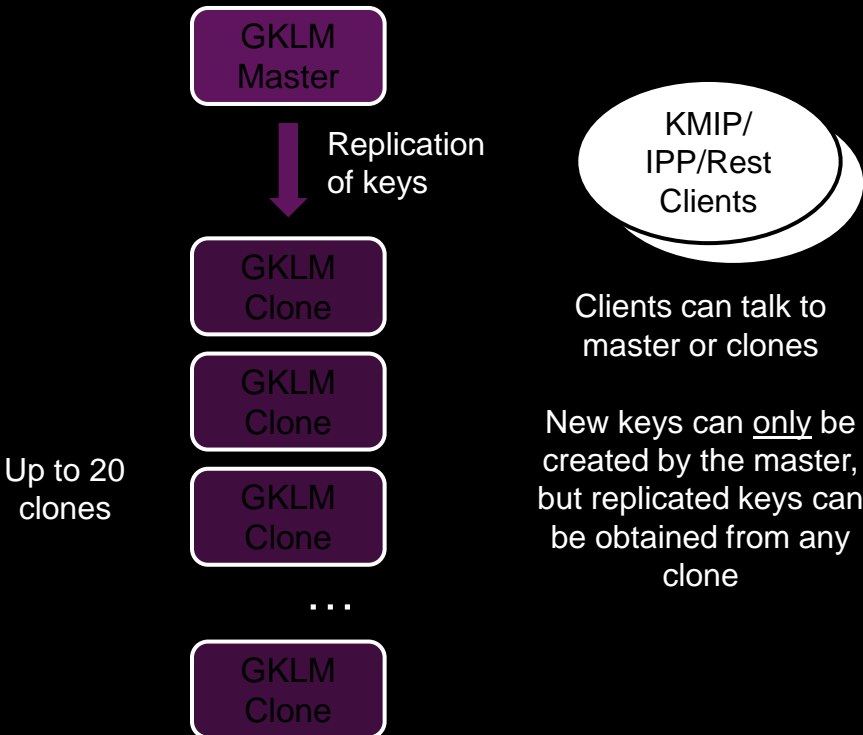


DB2 ...

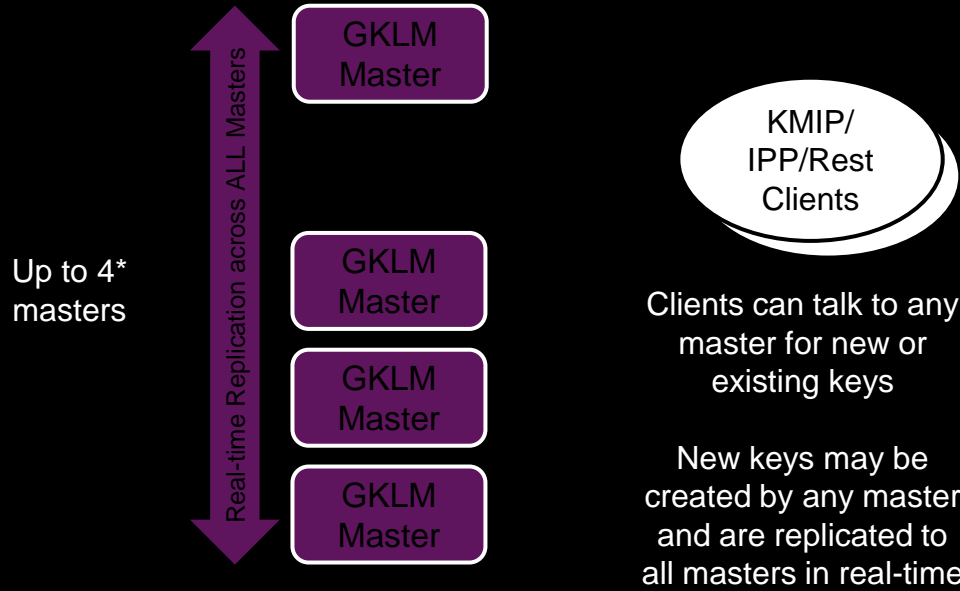
Broadening Footprint



Redundancy and high availability options via clones and multi-master set up



GKLM v2.7 (prior release to v3.0)

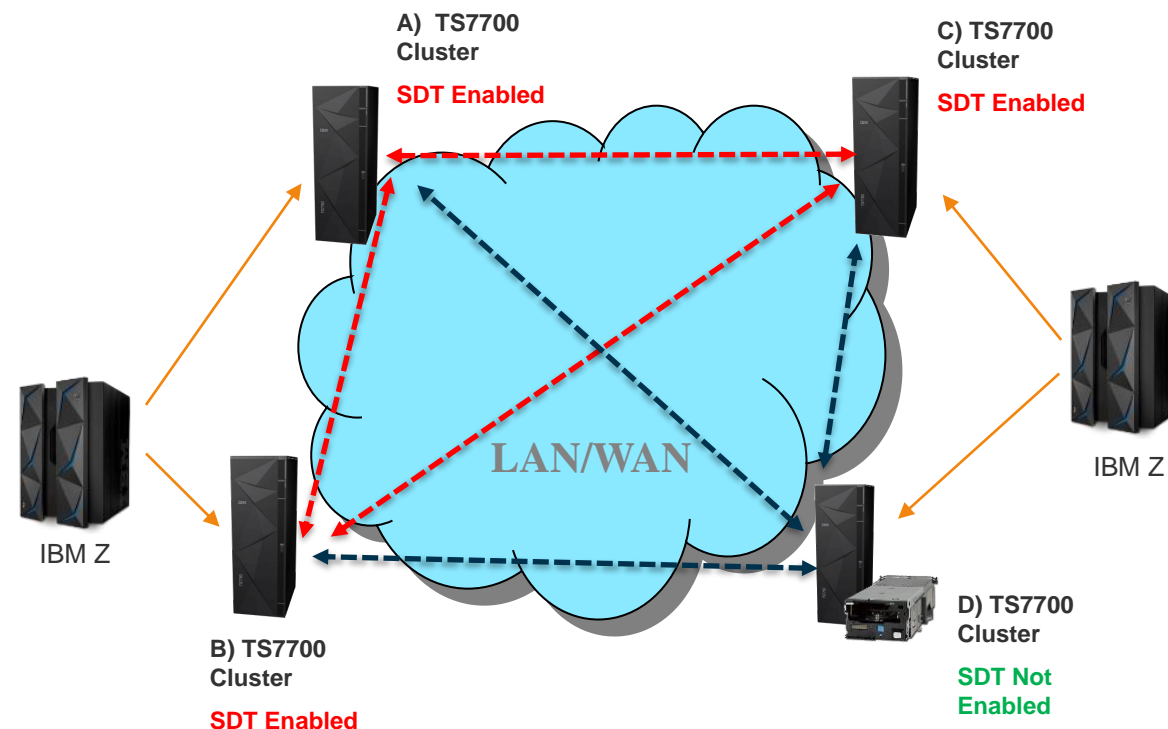


GKLM v3.0 (latest release is GKLM v4.2)

*Versions v3.0 to v4.1 allow for up to 20 masters

R 5.0 Secure Data Transfer

- **Secure Data Transfer Between Clusters in a Grid**
 - **All logical volume access including copies and remote reads and writes are encrypted in flight**
 - FC based function can be enabled concurrently at each location on TS7760 or TS7770
 - Any two locations with enablement will begin communicating using encryption
 - Clusters without enablement or down level can co-exist (non encrypted)
- **TLS 1.2 Support**
 - **TLS 1.2 used to create a secure connection per logical volume**
 - **Default or customer provided certificate supported**
 - **AES128 or AES256 is utilized once the connection is created**
- **High Performance**
 - Exploits the Power9 and Power8 encryption instruction set
 - Minimal performance and CPU overhead



Transport Layer Security

- All protected data must be encrypted when transmitted between applications residing on separate operating systems or virtual containers.
- All public web sites and services must provide service through secure connections. Encrypted connections protect against data being modified by an attacker, eavesdropping, and tracking.
- TLS Requirements
 - **Only TLS 1.2 or TLS 1.3 may be used. (TLS 1.3 preferred.)**
 - Prior versions have security vulnerabilities/use weak crypto, have been considered outdated, and not supported by many.
 - **For any public site/service, certificates must be issued by an IBM approved Certificate Authority and not self-signed. SDT required that IBM Certificate Authority**

DS8K -TCT Secure Data Transfer & Compression to TS7700

(DS8K GA Oct 2020 & TS7700 R5.0 & higher)

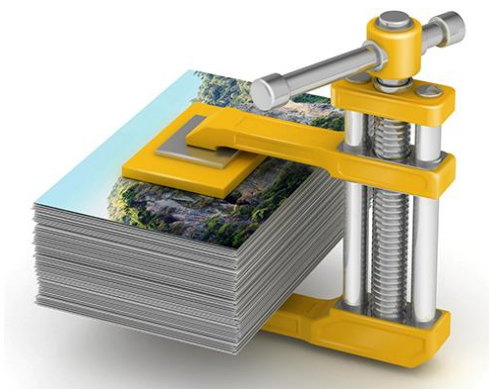
Encryption

- Requires DS8900F R9.1 microcode
- TS7700 R5.0 and higher with **FC 5281** installed
- Hardware accelerated via POWER9 crypto engine
- **AES 256-bit TLS 1.2 Encryption over Ethernet TCP/IP**
- **Encryption of data in flight**



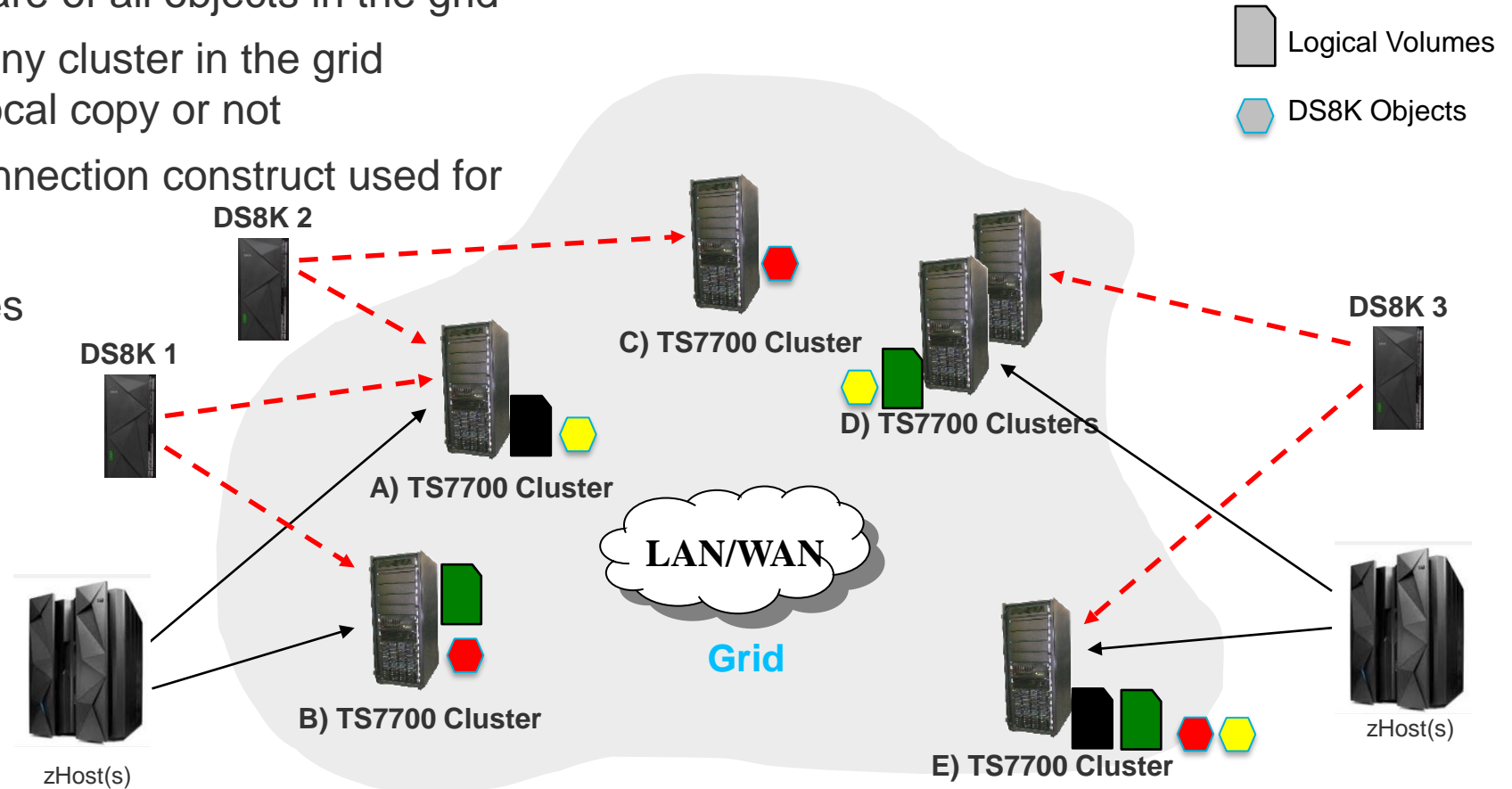
Compression

- Support requires DS8900F R9.1 microcode and z/OS APARS
- TS7700 R5.0 and higher, no additional feature codes
- Only supported when TS7700 is configured as the object store
- Only customer data is compressed
 - Metadata objects are not compressed
 - Data lands in TS7700 compressed and is only uncompressed when recalled back in DS8900F
- Hardware accelerated in POWER9
- DFSMS controls the use of compression
 - Will avoid compression if the dataset is host compressed/encrypted
 - z/OS APAR: OA59465



DS8K TCT TS7700 Release 5.22 Enhancements - Object Grid Awareness

- Support Grid Architecture for DS8K Objects
 - All TS7700 clusters are aware of all objects in the grid
 - Access to all objects from any cluster in the grid whether the cluster has a local copy or not
 - DFSMS Cloud Network Connection construct used for policy management
 - Automatic healing of changes during cluster outages
 - **Secure Data Transfer of Objects between TS7700 clusters (FC 5281 required)**

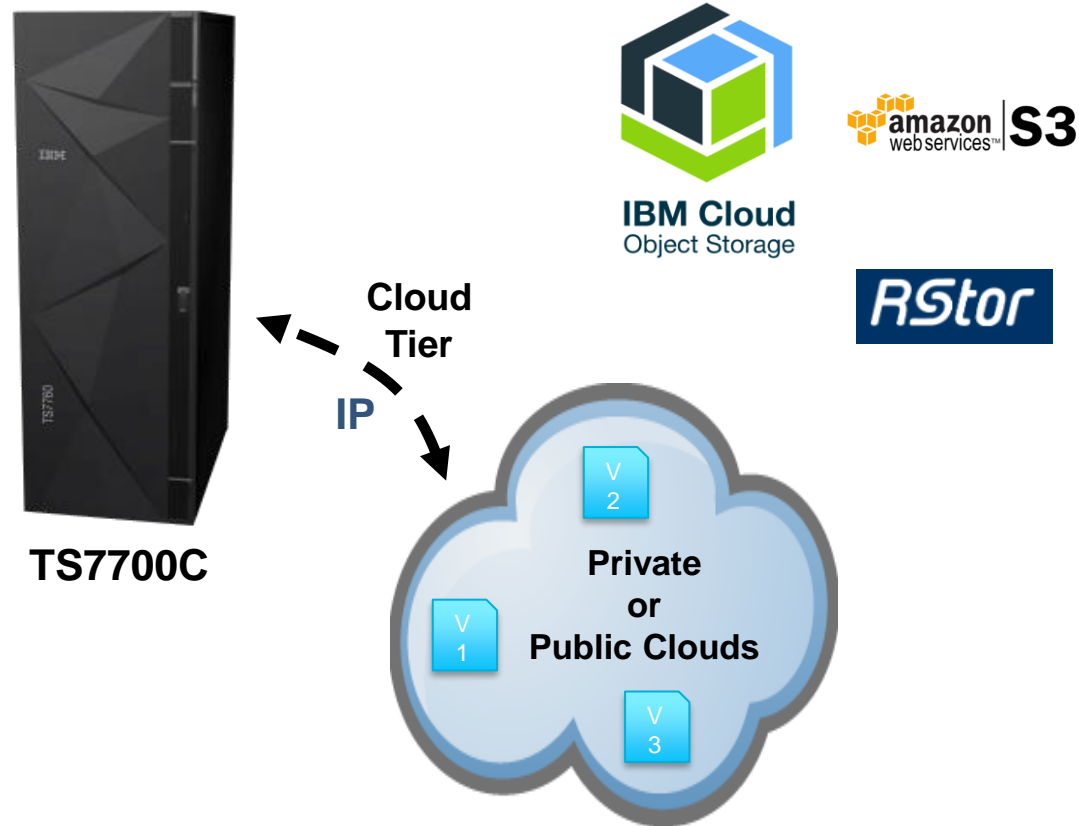


DS8K TCT TS7700 Configuration Rules

- **DS8K Advanced Object Store feature only supported on TS7770 (VED)**
- **128 GB memory recommended (128 GB required beginning R5.3). 10Gb Ethernet recommended**
- **Supported on TS7770D, TS7770T, or TS7700C with a mixture allowed in the same Grid.**
- **Note: Objects cannot migrate to tape or cloud.**
- **Older TS7700 models can exist in the grid but cannot be DS8K TCT targets with this new feature.**
- **Any cluster that will support this new feature must be at 8.52.200.111 code or higher. Next Code level is 5.3**
- **More than one DS8000 can target a TS7700 cluster**
- **Maximum 256 Object Store Connections allowed to a TS7700 Grid**
- **MES procedure for FC 8083 (P9 server SSD installation) must be performed**
- **MES procedure for FC 5283 (Advanced Object Management) must be performed**
- **Any TS7700 VED that previously had FC5282 must upgrade to the new **FC 5283** before other FC 5283 systems can be introduced (note: migration path available in R5.3 PGA1) or FC5282 is removed from the grid before installing FC5283 (VTD_EXEC.385 required).**
- **A copy refresh Lab Service offering is available for objects as of R5.3**
- **Grid unjoins of a cluster containing objects not yet supported.**



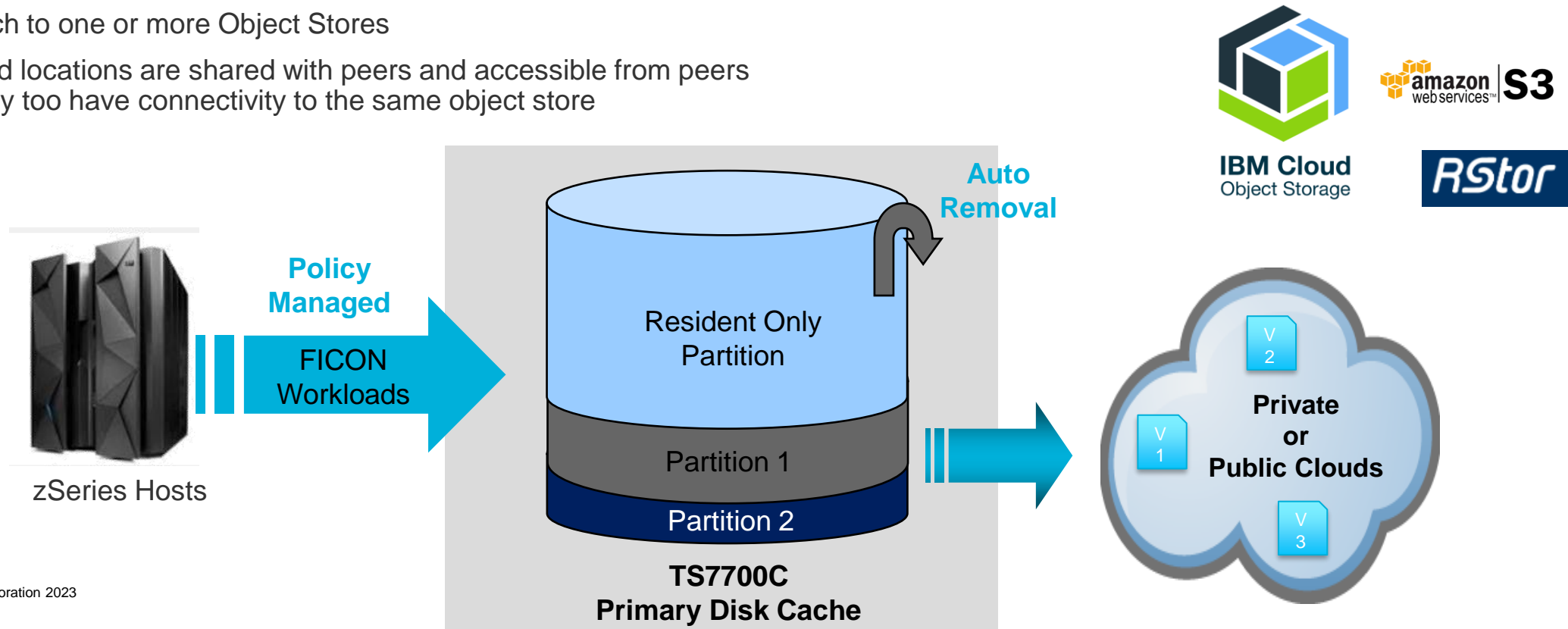
TS7700 Cloud Storage Tier (TS7700C)



- Leverage Cloud Storage Tier for off load to public or private cloud
- Using policy management, put a copy of logical volumes into an object store
- **Once one cluster puts a logical volume in the cloud, all clusters have access to the copy in the cloud (R5.1 improvement)**
- Support on-prem and off-prem S3 clouds
 - IBM ICOS Private Cloud
 - IBM ICOS Public (iRPQ)
 - Amazon AWS S3 Public
 - Rstor private and public (iRPQ)
- Cross-Regional replication and Vault Mirroring supported
- Object Locking/Object Retention at vault level not supported
- Shares Grid Network for cloud connectivity
- **Supports TLS1.2 for cloud connectivity**
- A TS7700 can be either a TS7700C or TS7700T

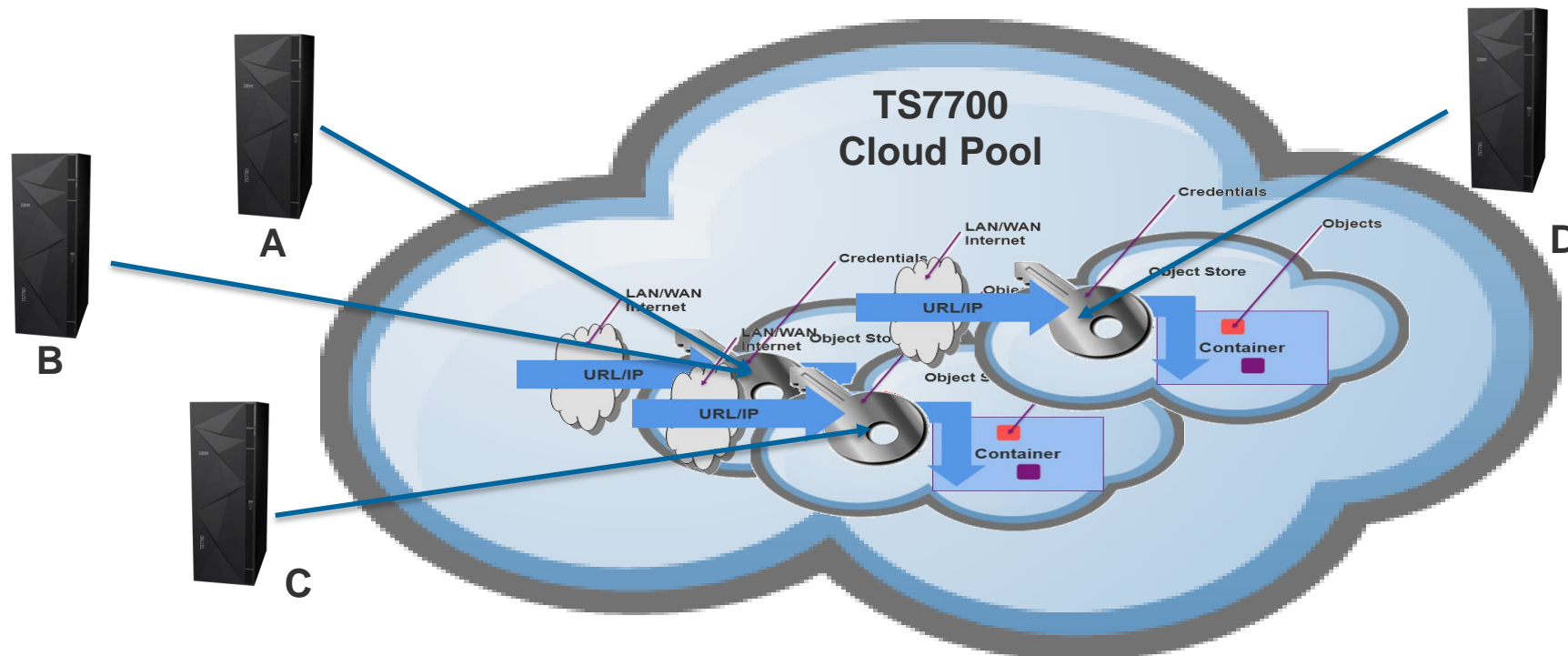
TS7700C Partitions

- Define partitions
 - Same partition concepts of traditional TS7700T tape attach
 - Content can go to Cloud via Cloud Storage Tier just like it can go to physical tape
 - Policy managed as to which partition and which cloud
 - Same pre-migration queue size features as used for tape attach and cloud storage tier
- Cloud Attach Options
 - Attach to one or more Object Stores
 - Cloud locations are shared with peers and accessible from peers if they too have connectivity to the same object store

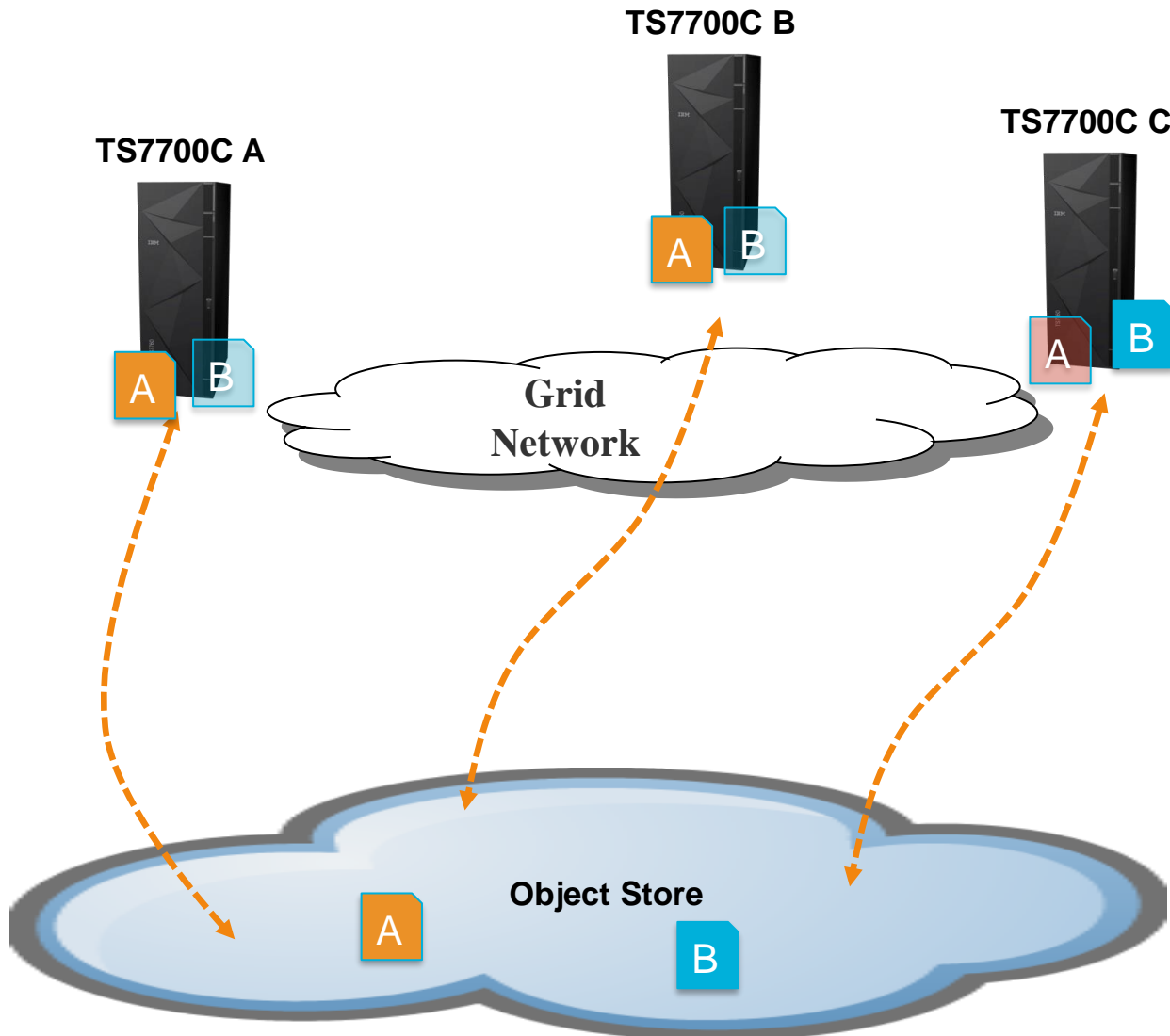


TS7700 Cloud Storage Tier – Access Hierarchy

- A TS7700 “Cloud Pool” is a virtual bucket in the sky - Grid scope – can have multiple cloud pools.
- A Cloud pool is associated with a cloud container and requires account credentials for access. Can have encryption enabled (TLS 1.2 - data in flight)
- Multiple, unique access points (URLs) can be configured for each cluster in the grid
- A given Cloud Pool must have access to all the same or mirrored data within the object store from each cluster that will be a target for that data (e.g IBM COS Erasure, Vault Mirror, AWS Cross Regional Replication)
- Whether the underlying object store is one global store or sub-stores that replicate containers, it’s all still accessible using an URL, Container and set of Credentials from a given cluster.



R5.1: TS7700C grid awareness



Contents in the cloud is synchronized with all peers

- Once any cluster puts a volume in the cloud, all clusters (existing and future) in the same grid will have immediate access to the volume in the cloud
 - Replication can be skipped when a copy is already in the cloud

In addition to Grid Replication

- A cluster can get access to the data in the cloud if it has connectivity to the cloud pool where the data is stored
- Optionally, rely on cloud redundancy instead of grid replication for less critical workloads

Ghost copy

- Grid copies that are time delayed or setup as Preference Group 0 at the copy target will skip the copy after verifying the content is already accessible in the cloud

Cluster join

- Once a cluster joins the grid, it automatically has access to all content in the cloud

R5.1: TS7700C cloud export and recovery

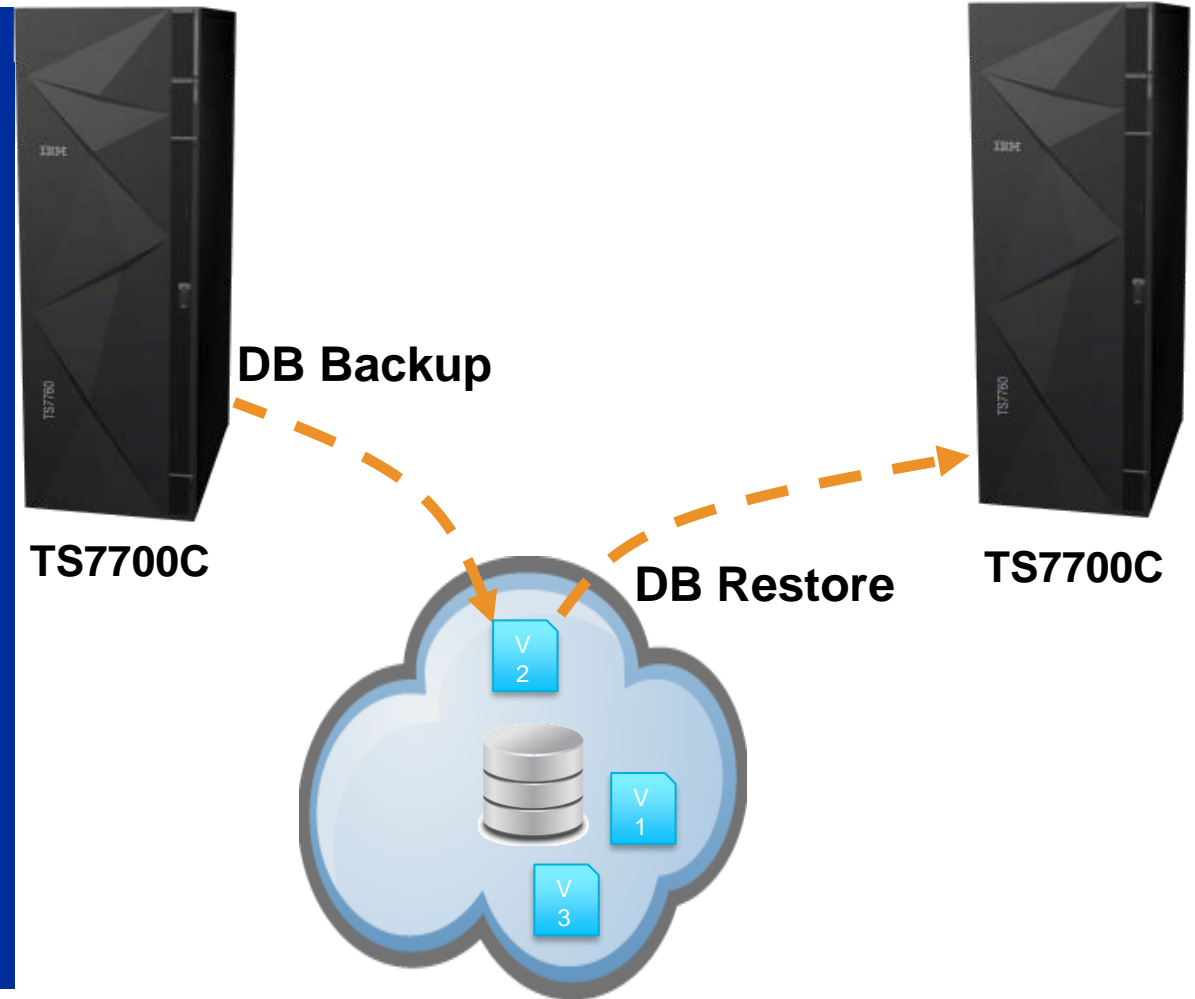
<https://www.ibm.com/support/pages/ts7700-cloud-storage-tier-export-recovery-and-testing-guide>

Export one or more cloud pools with a point in time DB backup in the cloud

Restore any cloud export backup into an empty TS7700C cluster

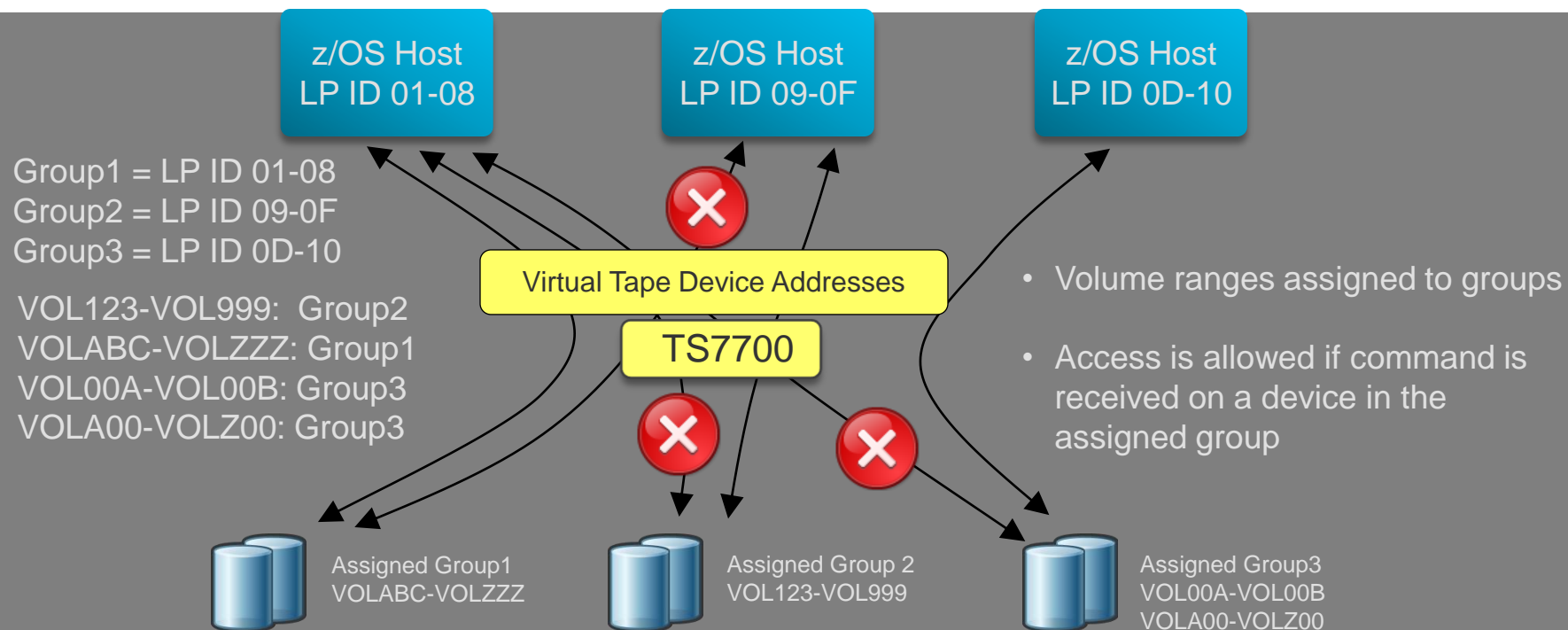
Support DR testing with read-only restore

Leverages TS7700C Volume Version Retention for backup retention



Selective Device Access Control (SDAC)

- **Enables hard partitioning of a TS7700 between several hosts or plexes**
 - Blocks access and control of volumes between system plexes
 - Separated by tape management systems, independent volume ranges and scratch pools
 - Access is allowed through “Hard Partitioning” or specific Library Port IDs (virtual device addresses)
 - Limit of 16 Groups (2x 8 FCs)

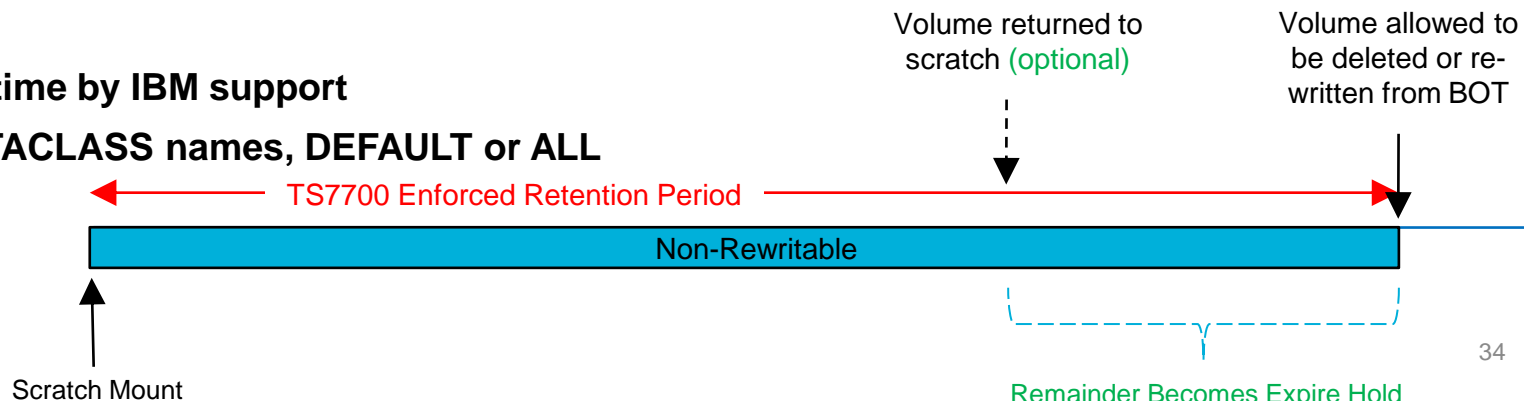


TS7700 R5.1 - MI Dual Control

- **TS7700 Management Interface now provides an optional way to require two individuals to complete sensitive changes to certain MI settings**
 - Once enabled, “Checker” policy can be added to team members
 - Modify & Delete Category and TS7700C Cloud Pool policies protected
 - Any user with privileges to modify category or cloud pool settings will continue to be allowed to attempt a change, but the change is queued instead of being completed
 - A member with “checker” privileges must then reject or approve the queued request
 - Requester can also be a checker, but can’t approve his or her own requests
 - The ability to change dual control settings and related role security settings also requires dual control approval
 - Requires all clusters in a grid be running 5.1 before this feature can be enabled
 - Future releases to dual protect other MI settings

TS7700 LWORM Retention

- Extension of LWORM for Cyber Security
 - **Three choices for retention duration at volume creation**
 - Fixed duration with option to extend at mod time
 - HDR1 Tape Management System provided expiration date
 - Fixed/Added Duration at return to scratch time (**dynamic expire-hold**)
 - **Numerous settings allow customized behaviors**
 - Fixed durations on create and MOD, including an option of “forever”
 - How to handle TMS dates that imply “Application Managed”
 - How to handle cases where no HDR1 date is provided
 - Whether to allow return to scratch before retention period expires
 - If allowed, the volume will go into an expire-hold state until the retention period passes supporting move back to private if needed
 - Option to extend or introduce a retention period when returned to scratch providing a data class granular expire-hold capability
 - **Initial support available through iRPQ**
 - Settings are chosen at enablement time by IBM support
 - Can be applied to specific DATACLASS names, DEFAULT or ALL



Transport Layer Security details

- 3. Use strong crypto - use at least AES-128. Disable weak cipher suites. Do not use weak crypto - do not use 3DES, MD5, or RC4. HMAC_SHA1 is acceptable but HMAC_SHA256 is preferred. Use RSA or ECDSA keys, not DSS.
- 4. For TLS 1.2 - provide at least one cipher suite that offers an AEAD cipher (such as AES_GCM) AND perfect forward secrecy (DHE or ECDHE).
- Recommendations for TLS 1.2
 - 1. Prefer cipher suites that provide perfect forward secrecy (PFS) - prioritize cipher suites that provide PFS higher.
 - 2. Prefer AEAD ciphers over non-AEAD ciphers - for example, prefer AES_GCM over AES_CBC. (In TLS 1.3, all ciphers are AEAD ciphers.)
 - 3. Prefer HMAC_SHA256 over HMAC_SHA1.
 - 4. If possible, only enable cipher suites that provide perfect forward secrecy and AEAD ciphers.
 - 5. Plan to upgrade to TLS 1.3.

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](https://www.menti.com) with code 2243 3599 or

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

Or

QR Code

