IBM TS7700 v8.41 Phase 2

Introduction and Planning Guide

GA32-0567-25

Note

Before using this information and the product it supports, read the information in "Safety and Environmental notices" on page xi and Notices.

This edition applies to Version 4, release 1 of the *IBM TS7700 Introduction and Planning Guide* and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces GA32-0567-23.

Contents

Figures

Tables

Feedback

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have comments or suggestions for improving this publication, you can send us comments by email to starpubs@us.ibm.com or use the Readers' Comments form at the back of this publication. Be sure to include the following information in your correspondence:

- Exact publication title
- Form number (for example, GA32-0567-23), part number, or EC level (located on the back cover)
- Page numbers to which you are referring

Note: For suggestions on operating enhancements or improvements, please contact your IBM Sales team.

Safety and Environmental notices

This section contains information about safety notices that are used in this guide and environmental notices for this product.

Safety notices

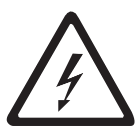
Observe the safety notices when using this product. These safety notices contain danger and caution notices. These notices are sometimes accompanied by symbols that represent the severity of the safety condition.

Most danger or caution notices contain a reference number (Dxxx or Cxxx). Use the reference number to check the translation in the *IBM Systems Safety Notices*, G229-9054 manual.

The sections that follow define each type of safety notice and give examples.

Danger notice

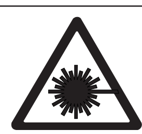
A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol always accompanies a danger notice to represent a dangerous electrical condition. A sample danger notice follows:



DANGER: An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. *(D004)*

Caution notice

A caution notice calls attention to a situation that is potentially hazardous to people because of some existing condition, or to a potentially dangerous situation that might develop because of some unsafe practice. A caution notice can be accompanied by one of several symbols:

If the symbol is...	It means...
	A generally hazardous condition not represented by other safety symbols.
 Class II	This product contains a Class II laser. Do not stare into the beam. (*C029*) Laser symbols are always accompanied by the classification of the laser as defined by the U. S. Department of Health and Human Services (for example, Class I, Class II, and so forth).
	A hazardous condition due to mechanical movement in or around the product.

If the symbol is...	It means...
 > 18 kg (40 lb)	This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (*C008*)

Sample caution notices follow:

Caution
: The battery is a lithium ion battery. To avoid possible explosion, do not burn. Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM® has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (*C007*)

Caution
: The system contains circuit cards, assemblies, or both that contain lead solder. To avoid the release of lead (Pb) into the environment, do not burn. Discard the circuit card as instructed by local regulations. (*C014*)

Caution
: When removing the Modular Refrigeration Unit (MRU), immediately remove any oil residue from the MRU support shelf, floor, and any other area to prevent injuries because of slips or falls. Do not use refrigerant lines or connectors to lift, move, or remove the MRU. Use handholds as instructed by service procedures. (*C016*)

Caution
: Do not connect an IBM control unit directly to a public optical network. The customer must use an additional connectivity device between an IBM control unit optical adapter (that is, fibre, ESCON, FICON®) and an external public network . Use a device such as a patch panel, a router, or a switch. You do not need an additional connectivity device for optical fibre connectivity that does not pass through a public network.

Environmental notices

The environmental notices that apply to this product are provided in the *Environmental Notices and User Guide*, Z125-5823-*xx* manual. A copy of this manual is located on the publications CD.

About this publication

This publication provides installation and planning information for the IBM TS7700 Series.

Organization of this book

The information in this publication is organized as follows:

- Chapter 1, "Overview," provides:
  - A discussion of the data storage values used
  - A discussion of the concepts of storage virtualization
  - An introduction to the TS7700
  - A comparison of the TS7760, TS7720, and the TS7740 system configurations
  - An overview of the components
- Chapter 2, "Planning," describes for the TS7700:
  - A discussion of the component details
  - An overview of the system requirements
  - A discussion of host compatibility
  - A discussion of infrastructure requirements
  - A discussion about planning for virtual and physical volumes
  - A discussion of the upgrade options
  - A description of the feature codes
  - Checklists for installation and post-installation
- Chapter 3, "Configuring," describes for the TS7700:
  - A discussion of possible configurations
  - A discussion of the data access and availability characteristics
  - A discussion of how to configure for disaster recovery
  - A discussion of how to configure for high availability
  - A discussion of how to configure for disaster recovery and high availability
  - Introduction of selective write protect for disaster recovery
- Chapter 4, "Security," describes TS7700:
  - Security protocols used including native LDAP and LDAP by proxy
  - Audit logging procedures
  - Remote support security procedures
- Chapter 5, "Managing," describes for the TS7700:
  - A discussion about how to connect to the management interface
  - A discussion of the many aspects of the management interface
- Chapter 6, "Recovering," describes for the TS7700:
  - A discussion about how to recover lost data
  - A discussion about how to test for grid failover
- The "Glossary" on page 345 provides definitions for terms, abbreviations, and acronyms used in this book.
- The Reference provides information about the electronic emission regulations that pertain to the TS7700 in the United States and other countries and regions.

- The Index includes keywords and terms to help retrieve information in this publication.

Who Should Read This Book

This book is intended for system planners, programmers, and administrators.

What's New in This Edition

Significant changes include:

- Support for 7/8 way grid configurations
- Support for 8 TB DDMs
- Various updates for clarity and accuracy

Related Publications

The following publications provide information related to the IBM TS7700, cache controller, cache storage, and components:

- *IBM 3592 Tape Drive and TS1120 Controller Introduction and Planning Guide (3592 Models J1A, E05, E06, EU6, E07, E08, and J70, C06, C07 Controllers)*, GA32-0555-07
- *IBM 3953 Tape System Introduction and Planning Guide*, GA32-0557-06
- *IBM TS7760/TS7760 Tape Attach Installation Roadmap*
- *IBM TS4500 Tape Library Introduction and Planning Guide*, SC27-5990-03
- *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide.* GA76-0418-08
- *IBM TS7700 Customer Information Center*

Online References

The following online references are included in this publication:

- IBM TS7700 Series Information Center
  - http://www-01.ibm.com/support/knowledgecenter/STFS69/
- Information concerning IBM product recycling offerings
  - http://www.ibm.com/ibm/environment/products/recycling.shtml
- Information concerning battery return programs
  - http://www.ibm.com/ibm/environment/products/battery.shtml
- Information concerning Web-Based Enterprise Management
  - http://www.dmtf.org/standards/wbem
- Information concerning Common Information Model, the Web-Based Enterprise Management data model
  - http://www.dmtf.org/standards/cim
- Information concerning the most recent list of supported FICON directors
  - http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FQ116133

Chapter 1. Overview

The following topics provide overview information that is related to your IBM TS7700 Series (TS7700).

Concepts of storage virtualization

Virtualization permits the full utilization of modern tape technology's underlying storage capacity and decreases the virtual volume access time of data storage and retrieval.

Virtualization reconfigures the relationship between a physical tape drive, storage media, and the application that reads and writes data. The TS7700 Cache uses disk drive modules (DDMs) as storage media and the TS7700 Server emulates the function and operation of IBM 3490 Enhanced Capacity (3490E) tape drives. These emulated tape drives are called *virtual tape drives*, and to an attached host they appear identical to physical tape drives.

Data that is written or read through a virtual tape drive resides in a *virtual volume* on the DDMs in the TS7700 Cache. To a host application, a virtual volume shows the same characteristics as a physical tape volume. The size of virtual volumes is dependent upon the size of data received from the host; virtual volumes are only as large as necessary to hold the host data. This characteristic of virtual volumes increases the efficiency of layered storage and permits physical tape volumes to maximize available storage.

When the TS7700 is attached to a tape library, the TS7700 Server manages the physical tape drives, or *physical volumes*, in the tape library and controls the movement of data between physical and virtual volumes. The TS7700 Cache temporarily holds data before writing it to tape, caches the data after a read or write operation to provide fast subsequent access, and provides source data when replicating to another cluster in a Grid. When a virtual volume is read from the TS7700 Cache DDMs and written to a physical volume, *premigration* is said to have occurred and the virtual volume becomes a *physical volume*. Conversely, when a virtual volume is moved from a physical volume to the TS7700 Cache, a *recall* is said to have occurred and the virtual volume again becomes a virtual volume. A physical volume can contain one or more virtual volumes; a physical volume that contains more than one virtual volume is referred to as a *stacked volume*.

When the TS7700 is not attached to a tape library, all data is held in virtual volumes in the TS7700 Cache. In both configurations (with or without an attached physical library), caching algorithms ensure that the cache is full of the most recently created and/or accessed data. The caching algorithms might also be influenced by cache management policies as part of the advanced policy management functions. In both configurations, the replication of a virtual volume from one site to another across the connecting infrastructure (grid network) is referred to as a *copy*.

Virtual device operation

Virtualization enables the TS7700 to appear as a collection of tape drives to an accessing host.

The virtual tape drives of a TS7700 are defined by using the same characteristics of physical tape drives. As a result, from the perspective of an accessing host the TS7700 appears as a collection of tape drives. Depending on the machine model and installed features, this collection provides up to 31 logical control units and up to 496 virtual drives. Virtual drives are organized in groups of 16 drive addresses under a single logical control unit address. Like a physical tape drive, each virtual drive has the following characteristics:

- Has a host device address
- Is included in the I/O generation for the system
- Can be varied online or offline to the host
- Supports all dynamic path creation and dynamic partitioning modes
- Signals ready when a virtual volume is loaded
- Supports all IBM 3490 tape I/O commands
- Supports host data compression controls
- Exits the ready state when a virtual volume is rewound and unloaded
- Maintains statistical counters that can be retrieved as buffered log data

A virtual tape drive differs from a physical tape drive in two important ways. First, the "media" for a virtual tape drive is a direct access storage device (DASD), which is suited for the stop-start transfer of data with low performance impact. By contrast, the media for a physical tape drive is a physical tape. When this physical tape is in motion, the host must continue to write data at a rate no slower than the rate at which data is written to the media, or the tape must stop. If the tape stops, it is repositioned, and assuming that sufficient data is buffered to write, started again. This stop-start motion is time consuming and contributes to the wear of tape media and tape drives. For 3490 and later class drives, few applications can sustain the bandwidth that is needed to 'stream' the drives to prevent frequent repositioning.

Second, the resources in a virtual drive are embodied in software and electronic storage (buffering). If the host is not sending data to a virtual drive, the drive does not consume processor cycles or storage space. Those resources remain available for use by other virtual drives. By comparison, a physical tape drive resource is dedicated to the host application that is using it for while the volume is mounted. If the host is not sending data to the drive at a high rate because of the nature of the application, the resource is underutilized.

Virtual volume tape format

A TS7700 virtualizes tape volumes and hides any physical volumes that reside behind it.

A virtual volume is stored as a standard file stored within the TS7700 tape volume cache (TVC). Any access to a volume by a host is achieved through the file or files resident in the TVC. The TS7700 manages the contents of the cache to keep it full of virtual volumes based on cache management policies.

Channel and device bytes: Data is measured in bytes, determined by its location in the storage system and can be affected by compression.

Device bytes
: Data that is received from the FICON channel, and that ultimately ends up in the TVC file or files after any enabled compression technology takes effect, is called device data. Device data is equivalent to the number of device bytes used by the emulated virtual tape media.

When standard compression is active, the device bytes tend to be lower than the channel bytes since a reduction of data takes place. Device byte values are reported to the host upon demount and stored as physical bytes.

The emulated capacity of a virtual volume can change dynamically by using the capacity defined through the Data Class storage construct on the TS7700 Management Interface. On a TS7700 system, volume capacity is measured in device bytes. You can specify 400 MiB CST (cartridge stored tape)-emulated cartridges or 800 MiB with ECCST (extended capacity cartridge storage tape)-emulated cartridges when adding volumes to the TS7700. You can use these sizes without modification or use Data Class policy management to override those sizes to provide for the following larger volume sizes:

- 1000 MiB
- 2000 MiB
- 4000 MiB
- 6000 MiB
- 25000 MiB

Note: A 25000 MiB maximum is available without restrictions when all clusters in the grid operate at microcode level 8.32.0.x or later. Otherwise, these restrictions apply:

1. The 25000 MiB maximum is not supported when at least one TS7740 in the grid operates at a microcode level earlier than 8.32.0.x.
2. In a mixed grid (where at least one cluster operates at microcode level 8.32.0.x or later and at least one cluster operates at an earlier microcode level) the following conditions apply:
   - FC 0001 must be installed on every cluster operating at a microcode level earlier than 8.32.0.x.
   - All clusters that operate at microcode levels earlier than 8.32.0.x must be TS7720 Clusters; they cannot be TS7740 clusters.
   - When the grid contains a tape-attached cluster (either a TS7740, TS7720 Tape Attach, or a TS7760 Tape Attach), FC 0001 must be installed on every cluster operating at a microcode level earlier than 8.32.0.x *before* those clusters are joined to the tape-attached cluster.
   - When the grid contains a cluster that is attached to a tape library, the 25000 MiB options are visible from the management interface in the clusters that operate at microcode level 8.32.0.x or later. The 25000 MiB options are not visible from the management interface in the clusters that operate at earlier microcode levels.
3. By default, the TS7700 Grid allows up to 128 simultaneous jobs running with 25000 MiB virtual volumes. This number of 25 MiB jobs that are allowed in the Grid is adjustable by using a host command line request.
4. Depending on the Grid network performance and the number of copy tasks for 25 GB volumes, consider increasing the volume copy timeout time from the default value of 180 minutes to 240 minutes if the copies are timing out. This can be done using the TS7700 Management Interface or using a Library Request Command.

Related information

"Virtual device operation" on page 1
Virtualization enables the TS7700 to appear as a collection of tape drives to an accessing host.

"Planning for virtual and physical volumes" on page 96
As part of your planning process, you need to determine the number of virtual and stacked physical volumes required for your workload.

Access and location of virtual volume data

Best performance is achieved by accessing virtual volumes data resident in the local cache.

Access of virtual volume data typically adheres to one of the following scenarios:

- If a recall is required to place the virtual volume in the local cache, it is done as part of the mount operation.
- If a copy of the virtual volume is not available at a local TS7700 Cluster, and a copy is available at a remote TS7700 Cluster in the grid, then the volume is accessed through the remote TS7700's cache. A virtual volume is not available on a cluster if that cluster does not have a copy or if the copy it does have is inaccessible due to an error.
- If the local copy requires a recall, and a remote copy is already resident in cache, remote access can occur if the remote access penalty is measured to be lower than the time to recall the volume locally.
- If a recall is required to place the virtual volume in the **remote** cache, it is done as part of the mount operation. If access is through a remote cache, the available data rate depends on the available bandwidth provided for the inter-cluster links and the distance between the TS7700 Clusters.

Grid network load balancing

For a TS7700 Grid link, the dynamic load balancing function calculates and stores the following information:

- Instantaneous throughput
- Number of bytes queued to transfer
- Total number of jobs queued on both links
- Whether deferred copy throttling is enabled on the remote node
- Whether a new job will be throttled (is deferred or immediate)

As a new task starts, a link selection algorithm uses the stored information to identify the link that will most quickly complete the data transfer. The dynamic load balancing function also uses the instantaneous throughput information to identify degraded link performance.

Related information

"TS7700 configurations" on page 249

Accessing virtual volumes through virtual device addresses

All virtual volumes are accessible through any of the virtual device addresses on a TS7700 in a grid configuration.

The TS7700 determines where the accessible copies of data are located and selects a TS7700 cache through which to access the data. The selected TS7700 cache is not required to be local to the TS7700 the mount request was received on, but preference is for access through the local cache to provide the best data access performance. If a remote cache is selected, the host's read and write access to the virtual volume travels over the grid WAN links. In this way, access to virtual volumes is similar to that of the prior generation when PtP routed I/O through the virtual tape controller to the VTS that contained a cached copy of the data.

Virtual volume copy availability

Whether a copy is available at another TS7700 Cluster depends on the copy consistency point that had been assigned to the virtual volume when it was written.

You choose whether a TS7700 Cluster is to have a copy of a virtual volume's data and when the copy will be performed. You can select from the following data copy policies:

- Copy data as part of the rewind unload processing (RUN) for a volume

  Important: Since immediate mode copies take place in their entirety after a volume is closed, the ability to replicate 6000 MB volumes increases the copy and Rewind-Unload (RUN) device end holding time by 50% over 4000 MB volumes. The immediate mode replication policy is not optimal for use with 6000 MB volumes.
- Defer copy after the RUN for the volume
- Defer (time-delay) copy to reduce traffic on the grid network and reduce excessive reclamation activity on target clusters
- Copy data synchronously as part of a synchronous mode copy operation
- Do not copy

The copy policies are the same as provided by the prior generation's PtP VTS. If the TS7700 Cluster used as the initial source for a virtual volume fails and another TS7700 Cluster has not completed a copy, then that virtual volume is not available during the outage and the mount request for the volume within the grid fails.

Parallel copies and pre-migrations for read mounts

This enhancement allows copies and pre-migrations within the grid to continue when a private mount occurs. Read mounts can occur in parallel to replication and pre-migration activity. If a write or update occurs, all pre-migration and replication activity for the same volume restarts sometime after the volume is closed and demounted.

TS7700 product introduction

The TS7700 is a member of the TS line of products and builds upon previous implementations of tape storage virtualization.

The TS7700 offers a modular and scalable architecture to the tape virtualization market allowing you to better customize the system to meet your particular requirements. Digital information that is generated by a smarter planet requires increasing storage and management. Online application storage and offline, permanent archive media continue to increase and require high-performance and high-capacity data storage solutions. The TS7700 is a fully integrated, tiered storage hierarchy of disk and tape. It leverages the benefits of both technologies by storing recent, frequently accessed data on disk to maximize performance in backup-and-restore operations, while moving older, less accessed data to tape, minimizing storage costs and securing long-term retention. The TS7700 can also fulfill storage requirements for applications and deployments that are designed to store data on tape, but that also require disk performance and capabilities. The

TS7700 can help reduce batch processing time, total cost of ownership, and management overhead. The TS7700 delivers significant processing power increase over previous models, resulting in:

- Greater efficiency
- Improved connectivity for grid configurations and tape and cache support
- Improved resiliency that uses 4-way and larger grid configuration support
- Improved data management in mainframe environments

Important: Microcode level 8.40.0.x can be installed only on a TS7760 Server model 3957-VEC. This microcode version is compatible with a TS7720 Server model 3957-VEB and a TS7740 Server model 3957-V07. All TS7720/TS7740 machines wishing to go to an 8.40 level should be at 8.40.1.x or higher.
The TS7700 is part of a family of IBM Enterprise tape products, and can be the answer to growing storage requirements, shrinking backup windows, and the need for access to data. Features and functionality include:

The TS7760

A virtual tape system, model 3957-VEC, that can support up to 2.5 PB of usable AES 256 encryption capable disk cache. Using 4 TB or 8 TB SAS disks in a DDP (Dynamic Disk Pooling) configuration, a base TS7760 can contain up to 618 TB in 61 TB increments. You can mix 4 TB or 8 TB drives within a frame but you cannot mix them within a drawer or enclosure. Up to two more expansion frames can be added each providing up to an additional 1607 TB of usable capacity in 61 TB increments.

The TS7760 supports the optional attachment of a TS3500 or TS4500 physical tape library. When the tape attach feature is present, the TS7760 can be referred to as a TS7760T or TS7760 Tape Attach. When tape is attached, up to 100 PB of usable storage is available per TS7760T.

The TS7700 Model 3957-VEC Server

A next generation server platform for the TS7700 Server is based on IBM Power® 8 pSeries technology. This platform offers a total of 32 GB of physical memory, and improved performance, reduced power consumption, and future scalability when compared to the first and second-generation TS7700 servers. It also includes an extra SAS controller card for redundancy, 300 GB SAS drives, and EEH and hot plug support on PCI adapters.

The TS7760 model 3957-VEC Server replaces the existing TS7720 model 3957-VEB and TS7740 model 3957-V07 IBM Power 7 pSeries technology. The minimum microcode level for the TS7760 model 3957-VEC Server is 8.40.0.x.

It supports:

- Two I/O drawers (1500-001)
- Adapter hot swap
- 16 Gb Fibre Channel interfaces for disk and back-end tape
- 4x10 Gb Ethernet Links for Grid Configurations

Note: The VEC tape-attach supports only the new 16 Gb fiber switch and not the 4 Gb nor the 8 Gb switch.

The TS7720

A virtual tape system, model 3957-VEB, that can support up to 1 PB of usable AES 256 encryption capable disk cache. Using 3 TB SAS disks in an RAID6 configuration, a base TS7720 can contain up to 240 TB in 24 TB increments. Up to two more expansion frames can be added each providing an addition 384 TB of usable capacity in 24 TB increments.

As of microcode level 8.32.0.x, the TS7720 supports the optional attachment of a TS3500 physical tape library. When the tape attach feature is present, the TS7720 can be referred to as a TS7720T or TS7720 Tape Attach. When tape is attached, up to 100 PB of usable storage is available per TS7720T as of microcode level 8.33.0.x. The TS4500 physical tape library is supported beginning with microcode level 8.40.0.x.

The TS7740
A virtual tape system, model 3957-V07, that supports up to 28 TB of usable AES 256 encryption capable disk cache and requires the attachment of a TS3500 physical tape library. Using 600 GB SAS disks in an RAID6 configuration, a TS7740 supports one, two, or three drawer configurations in 9 TB increments. With tape attached, up to 100 PB of usable storage is available per TS7740 as of microcode level 8.33.0.x.

The TS7700 Model 3957-V07/VEB Server
A second-generation platform for the TS7720 Server and TS7740 Server based on IBM Power 7 technology. This platform offers total physical memory of 16 GB, and improved performance, reduced power consumption, and future scalability when compared to first-generation TS7700 Servers.

It supports:
- Two I/O drawers
- Flexible adapter placement
- IPv6 and IPSec
- 8 Gb Fibre Channel interfaces for disk and back-end tape
- Disk encryption
- Up to 4 million virtual volumes

Enhanced user interface
An updated web interface that supports a single look and feel across storage product lines. Additional enhancements include:
- Improved summary details display
- Continuously available cluster status
- Improved health and event alert notification
- Improved visibility of copy queue information
- One-touch action items
- Support for installation of encryption and IPv6 features

Integrated Library Manager support for the TS7700
Integrates virtual volume management and some physical volume and device management into the TS7700.

16 Gb FICON host attachments
Microcode level 8.41.200.x supports 16 Gb, dual-port FICON adapters, increasing the potential bandwidth to the IBM Z® host. Each adapter has one port active by default. These adapters can be attached to FICON channels that support speeds of 4 Gbps, 8 Gbps, or 16 Gbps. Two or four 16 Gb FICON adapters can be installed in a TS7700 Server.

Note: No intermixing of 8 Gb and 16 Gb FICON adapters is allowed.

Note: Each FICON adapter supports a maximum of 512 virtual paths. When the maximum number of FICON adapters is installed, and with dual ports enabled, the total supported number of virtual paths is 4096.

The 3957-VEC server supports “FC 3402, 16 Gb FICON Short Wavelength Attachment” on page 156 and “FC 3403, 16 Gb FICON Long Wavelength Attachment” on page 157.

The 3957-V07/VEB servers do not support 16 Gb dual-port FICON adapters.

8 Gb FICON host attachments

Microcode level 8.31.0.x supports 8 Gb, dual-port FICON adapters, increasing the potential bandwidth to the IBM Z® host. Each adapter has one port active by default. These adapters can be attached to FICON channels that support speeds of 2 Gbps, 4 Gbps, or 8 Gbps. Two or four 8 Gb FICON adapters can be installed in a TS7700 Server.

Note: Each FICON adapter supports a maximum of 512 virtual paths. When the maximum number of FICON adapters is installed, and with dual ports enabled, the total supported number of virtual paths is 4096.

All 3957-V07/VEB servers with 8 Gb FICON adapters require 32 GB of memory, an increase of 16 GB of memory to the default server configuration. This includes all field upgrades from 4 Gb to 8 Gb FICON. “FC 3462, 16 GB memory upgrade” on page 159 can be installed to provide this memory upgrade.

The 3957-VEC server supports “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 157 and “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157.

16 Gb Fibre Channel HBA

The TS7760 uses new PCIe 16 Gb Fibre Channel dual ported adapters in place of the previous 8 Gb Fibre Channel adapters that were used in the 3957-V07 and 3957-VEB servers.

The 16 Gb Fibre Channel adapters are installed in the new IO drawer (1500 series). They allow the TS7700 to support the full throughput of the 3956-CSA 16 Gb disk cache controller host connection.

Support for four, 1 Gb grid Ethernet links

Support for use of the second 1 Gb Ethernet port present in both grid Ethernet adapters. This support results in availability of four total 1 Gb ports for TS7700 Grid interconnections. Each 1 Gb link requires a unique IP address. Selective device access control can be used to tune use of links between sites.

This configuration is only supported by microcode levels of 8.20.0.xx and later. It requires two dual-ported adapters and is activated via FC 1034, Enable dual port grid connection.

Support for 10 Gb grid optical Ethernet longwave connection

Support for a standard, 10-Gbps Ethernet longwave (1,310 nm) optical adapter for grid communication between TS7700 Servers.

This feature is available on a 3957-V07 or a 3957-VEB, operating at microcode level of 8.20.0.xx or later. When FC 1035, 10 Gb grid optical LW connection is installed, the 3957-V07 or 3957-VEB supports two 10 Gb Grid links. This feature is also available on a 3957-VEC. When FC 1038, 10 Gb dual port optical LW connection is installed (microcode level of 8.40.0.xx or later) or FC 1041, 10 Gb dual port optical LW connection (microcode level of 8.41.200.xx or later), the 3957-VEC supports two 10 Gb Grid links. When FC 1034, Enable dual port grid connection is installed, the 3957-VEC supports four 10 Gb Grid links.

Tape library attachment

- Attachment to an IBM TS3500 Tape Library (also referred to as the 3584 Tape Library or machine type 3584) is supported for the TS7740, TS7720 Tape Attach, and the TS7760 Tape Attach.

  For the TS7740, this configuration is enabled by installing "FC 9219, Attach to TS3500/TS4500" on page 178. The TS7740 must be at microcode level 8.5.0.xx or later.

  For the TS7720/TS7760 Tape Attach, this configuration is enabled by installing "FC 5273, TS7720/TS7760 Tape Attach enablement" on page 163 and at least one instance of "FC 5274, Enable 1 TB Pending Tape Capacity" on page 163. The TS7720 Tape Attach must be at microcode level 8.32.0.xx or later. The TS7760 Tape Attach must be at microcode level 8.40.0.xx or later. 16 Gb Fibre Channel switches are supported in the TS3500 for TS7760 Tape Attach attachment.
- The TS4500 is the next generation of the IBM TS3500 Tape Library. Attachment to an IBM TS4500 Tape Library is supported for the TS7740, TS7720 Tape Attach, and the TS7760 Tape Attach. The TS4500 supports only TS1150 and TS1140 tape drives. Customers needing a library that supports earlier generation drives must remain on the TS3500 technology. 16 Gb Fibre Channel switches are supported in the TS4500 for TS7720, TS7740 and TS7760 attachment, and in the TS3500 for TS7720, TS7740, and TS7760 attachment.

  TS7740 attachment to the TS4500 must be at 8.40.0.x or higher. In addition, "FC 5242, Dual Port 16 Gb Fibre Channel HBA" on page 162 and "FC 4880, TS7700 BE 16 Gb Fibre Channel Switch" on page 160 are required.

  For the TS7720/TS7760 Tape Attach, this configuration is enabled by installing "FC 5273, TS7720/TS7760 Tape Attach enablement" on page 163 and at least one instance of "FC 5274, Enable 1 TB Pending Tape Capacity" on page 163. The TS7720 and TS7760 Tape Attach must be at microcode level 8.40.0.xx or later. In addition, "FC 4880, TS7700 BE 16 Gb Fibre Channel Switch" on page 160 is required.

Tape drive support

Note: TS1150 Tape Drives, TS1140 Tape Drives, TS1130 Tape Drives, TS1120 Tape Drives, and 3592 J1A Tape Drives are collectively referred to as *3592 Tape Drives*.

IBM TS1150 Tape Drive

Also referred to as E08 Tape Drive or EH8 Tape Drive.

TS1150 Tape Drives support read and write operations on JC, JD, JK, and JL media types, and read-only operations on JJ media types. TS1150 Tape Drives can be intermixed with one other drive type. The E08 drives are supported in a limited heterogeneous configuration. TS1150 Tape Drives are not able to read JB and older media such as JA and JJ. In a homogeneous configuration, four or more E08 drives along with new media must be used for read/write. In a limited heterogeneous configuration, four or more E08 drives are required and two or more of the read-only older 3592-generation drives.

When the TS1150 Tape Drive is installed in a TS3500 Tape Library, it is referred to as the 3592 E08 Tape Drive. If the TS1150 Tape Drive is installed in a TS4500 Tape Library, the model is the 3592 EH8 Tape Drive. Both tape drive models are functionally equivalent.

IBM TS1140 Tape Drive

Also referred to as E07 Tape Drive or EH7 Tape Drive.

TS1140 Tape Drives support read and write operations on JB, JC, and JK media types, and read-only operations on JA and JJ media types. TS1140 Tape Drives cannot be intermixed with any other drive type.

When the TS1140 Tape Drive is installed in a TS3500 Tape Library, it is referred to as the 3592 E07 Tape Drive. If the TS1140 Tape Drive is installed in a TS4500 Tape Library, the model is the 3592 EH7 Tape Drive. Both tape drive models are functionally equivalent.

IBM TS1130 Tape Drive

Also referred to as 3592 E06 Tape Drive or 3592 EU6 Tape Drive (if converted from a 3592 E05 Tape Drive.).

Note: TS1130 Tape Drives are shipped encryption-capable. To use TS1130 Tape Drives for a TS7740, the minimum required TS7740 microcode level is 8.5.0.xx. TS1130 Tape Drives cannot be intermixed with TS1120 or 3592-J1A Tape Drives.

IBM TS1120 Tape Drive

Also referred to as 3592 E05 Tape Drive.

Note: TS1120 Tape Drives can operate in native E05 mode or in 3592 J1A emulation mode. To use TS1120 Tape Drives in E05 mode, all drives that are associated with the system must be TS1120 Tape Drives, the drives must be set to E05 native mode, and the minimum required TS7700 microcode level must be 8.0.1.xx. Encryption is supported when all drives associated with the TS7700 are encryption-capable TS1120 Tape Drives (FC 5592 or FC 9592 is ordered against each TS1120 Tape Drive) and “FC 9900, Tape Encryption configuration” on page 181 is ordered against the TS7740 Server.

IBM 3592 Tape Drive J1A

Note: When 3592 J1A drives (or 3592 E05 Tape Drives in J1A emulation) are replaced with E05 drives, E05 drives append to the filling J1A-formatted drives. As the active data on the J1A gets reclaimed or expired, the tape goes back to the scratch pool and then is reformatted to the E05 data format on its first write operation. Likewise, when 3592 J1A drives (or 3592 E05 Tape Drives in J1A emulation) are replaced with 3592 E05 Tape Drives, the TS7700 marks the J1A formatted tapes with active data FULL. By marking these tapes full, the TS7700 does not append more data since the 3592 E06 Tape Drive cannot append data to a J1A formatted tape. As the active data on the J1A gets reclaimed or expired, the tape goes back to the scratch pool and then is reformatted to the E06 data format on its first write operation.

Encryption support
Support for data encryption on tape cartridges in a library connected to a TS7700. Requires "FC 9900, Tape Encryption configuration" on page 181.

Support for encryption of disk drive modules (DDMs) within a TS7700 cache subsystem with a microcode level of 8.30.0.xx or later. Requires "FC 5272, Enable disk encryption - Local Key Management" on page 163.

External key management for the cache is also supported with a microcode level of 8.33.00.xx or later. Requires "FC 5276, Enable disk encryption - External Key Management" on page 164.

Support for a hybrid TS7700 Grid
A hybrid TS7700 Grid contains an intermix of one or more TS7700 tape-attach Clusters and one or more TS7700 disk-only Clusters, which are configured together within the same grid.

Support for 5-way or more TS7700 Grid configurations
Support for a grid that consists of 5 or more TS7700 Clusters.

Note: Support for 5- and 6-way grid configurations is available by RPQ only and supported by a microcode level of 8.7.0.xx or later. Support for 7- and 8-way grid configurations is available by RPQ only and supported by a microcode level of 8.41.x.x or later.

Support for grid merge operations
Support to merge two existing multi-cluster grids to form a single, larger grid. This support requires that all clusters in both grids operate at the microcode level of 8.21.0.xx or later. In addition, all clusters must be at the exact same code level.

TS7700 Cluster Family grouping
A user-defined grouping of clusters that share a common purpose or role; it facilitates cooperative replication and improved tape volume cache (TVC) selection. Do not confuse cluster families with disaster recovery (DR) families used as part of flash copies for DR testing.

Larger virtual volume sizes
Available virtual volume sizes include:
- 1.05 GB (1000 MiB)
- 2.1 GB (2000 MiB)
- 4.19 GB (4000 MiB)
- 6.29 GB (6000 MiB)
- 26.21 GB (25000 MiB)

Virtual volume sizes are set by data class by using the base-10 unit mebibyte (MiB). For a discussion of the relationship between decimal and base-10 units, refer to the topic *Data storage values*. Refer to the topic *Virtual volumes* to determine the number and size of virtual volumes that are required to accommodate the planned workload. Links to both topics are found in the **Related information** section.

Time delay copy policy
Enhancement to defer replication until a specified number of hours has elapsed since the volume was created or since the volume was last

accessed. When implemented, this policy can greatly reduce the copy traffic on the grid network, and reduce excessive reclamation activity on target TS7740 Clusters.

Copy export enhancements

- Copy export merge expands the range of possible restore points to include an existing TS7700 tape-attached cluster, regardless of whether that cluster is part of an existing grid, available by service offering only.
- Copy export acceleration, a new extended option, improves the speed of copy export operations by reducing the number of volumes that store a copy of the recovery database.

Parallel copies and pre-migrations during read mounts

Enhancement to allow copies and pre-migrations within the grid to continue when a private mount occurs.

On-demand capabilities

- Up to 4 million virtual volumes per TS7700.

  Note: The default maximum number of virtual volumes that is supported is 1 million. Support for additional virtual volumes can be added in 200,000 volume increments up to 4 million total by using FC 5270, Increased virtual volumes. In a grid environment, the number of virtual volumes that is supported is determined by the cluster that has the smallest number of FC 5270, Increased virtual volumes, installed.
- Up to 496 virtual tape device addresses.

  Note: The default maximum number of virtual devices, (and thus virtual addresses), that are supported is 256. Support for additional virtual devices can be added in 16 drive increments up to 496 total per cluster by using FC 5275, Additional virtual devices. In a grid environment, each cluster can contribute up to 496 virtual tape device addresses. The total maximum number is 496 times the number of grid members.

Incremental capabilities

- High performance disk cache capacity: increments of 1 TB (0.91 TiB) up to 28 TB (25.48 TiB) in the TS7740
- Host data transfer performance (increments of 100 MB/sec up to 25000 MB/sec) for the TS7700. For increments 10-24, either a 16 Gb FICON host adapter (“FC 3402, 16 Gb FICON Short Wavelength Attachment” on page 156 or “FC 3403, 16 Gb FICON Long Wavelength Attachment” on page 157) or an 8 Gb FICON host adapter must be installed (“FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 157 or “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157).

  Note: “FC 5268, 100 MB/sec increment” on page 162 enables a 100-MB/sec increment of peak data throughput. One instance of “FC 9268, Plant installation of 100 MB/s throughput” on page 178 is shipped standard and a maximum of 24 instances of “FC 5268, 100 MB/sec increment” on page 162 can be added. When the maximum number of these instances is installed, the system does not restrict peak data throughput. Unrestricted peak data throughput is not constrained by system requirements and the use of "unrestricted" does not imply unlimited peak data throughput.

- “FC 5274, Enable 1 TB Pending Tape Capacity” on page 163, limits the maximum amount of queued premigration content within a TS7720/TS7760 Tape Attach Server. The feature can be installed in increments of 1 TB, with a maximum of 10 TB.

Compression optimization
: Compression methods that are available:
  - **FICON Compression** - compression that is performed by the hardware (FICON adapters).
  - **LZ4 Compression** - software compression that uses an LZ4 algorithm. This compression method is faster and uses less CPU than the ZSTD method but it gives a lower compression ratio than ZSTD.
  - **ZSTD Compression** - software compression that uses a Zstandard algorithm. This compression method gives a higher compression ratio than LZ4 but is slower and uses more CPU than LZ4.

Logical WORM
: Emulates physical Write Once, Read Many (WORM) and leverages the host software support of physical WORM media.

Host override for cache residency
: A library request (LI REQ) command option that is used to change the way virtual volumes are managed in the tape volume cache. The option temporarily overrides the virtual volume's preference group while the volume is in cache. It also keeps a virtual volume in cache for a longer time by making it appear as the most recently accessed volume.

Control Unit Initiated Reconfiguration (CUIR)
: A library request (LI REQ) command option that automates offline/online device actions to minimize manual operator intervention during selected service or upgrade actions.

Selective write protect for disaster recovery testing
: An option configurable from the TS7700 Management Interface that permits exclusion of up to 32 categories from a cluster's write protect enablement.

  This function permits the emulation of disaster recovery events by performing test operations at a disaster recovery site within a TS7700 Grid configuration.

Flash copy for disaster recovery testing
: An operation, performed as a sequence of LI REQ commands, which mimics the consistency or inconsistency of a disaster recovery site at time zero of a simulated disaster, emulating a true disaster scenario as closely as possible.

Device allocation assistance (DAA)
: For a specific mount, returns to the host a list of prioritized clusters to determine which cluster is best configured to direct a device allocation.

Scratch allocation assistance (SAA)
: For a scratch mount, returns to the host a list of candidate clusters for the allocation request. The list of candidate clusters is a subset of all clusters in the grid that have a specific Management Class construct value. When the Scratch Mount Candidate option is selected for a Management Class, SAA returns the list of clusters specified by that Management Class. A scratch allocation request is then directed to that specific set of clusters.

Preferred migration of scratch volumes
Enhancement to migrate scratch volumes prior to non-scratch volumes.

Selective device access control
Creation of library port access groups that permit segmentation of resources and authorization by controlling access to library data ports.

Note: "FC 5271, Selective device access control" on page 163, enables this function. Each feature code key enables definition of up to eight selective device access groups, excluding the default group in the count. A feature key needs to be installed on all clusters in the grid per eight groups before the function becomes enabled. This feature is only available with microcode levels of 8.20.0.xx and later.

Remote mount IP link failover
Intelligent failover during remote mounts improves availability of remote mount connections through use of alternate links.

Advanced policy management functions
Such as:

- Physical volume pooling
- Virtual volume copies on separate physical volumes
- Extension of virtual volume size
- Multiple reclamation policies
- Grid replication policies
- Cache retention policies
- Enhanced cache removal policies for the TS7720 to permit greater control over content removal as active data approaches full capacity

Support for IPv6
Support for the IPv6 protocol standard and its associated improvements in security, auto configuration, larger packets, mobile connections, and quality of service.

Security enhancements

- System Storage® Productivity Center (SSPC) integration
- Native LDAP support with z/OS RACF
- Audit logging
- Security audit SNMP trap definition filters
- Remote support security

Enhancements for Reliability, Availability, and Serviceability (RAS)

- Machine-reported product data - vital product data (MRPD-VPD) enhancements
- Tivoli® Assist on Site (AOS) enhancements

Important: Ask your IBM service representative to receive the most current level of TS7700 code.

Related information

"About cluster families" on page 267

"Allocation assistance" on page 290

"Concepts of storage virtualization" on page 1

"Data storage values" on page 28

"Virtual volume planning" on page 97

"TS7700 system component details" on page 33
"TS7760 Storage Expansion Frame" on page 39

TS7700 system configurations

A TS7700 Server is configured in one of three ways: TS7740, or TS7720 (disk-only or Tape Attach), or TS7760 (disk-only or Tape Attach).

TS7740:

- Stores data in disk cache and on physical tape in an attached physical library.

TS7720 :

- Disk-Only: Stores all data in disk cache and does not attach to a physical library.
- Tape-Attach: Takes the TS7720 configuration and adds a Tape Attach feature.

TS7760:

- Disk-Only: Stores all data in disk cache and does not attach to a physical library.
- Tape-Attach: Takes the TS7760 configuration and adds a Tape Attach feature.

Note: The TS7740/TS7720 will not be offered once the TS7760 is released.

Table 1 displays the available system configurations of the TS7700.

Table 1. TS7700 system configurations

Disk-only TS7760	TS7760 Tape Attach	Disk-only TS7720	TS7720 Tape Attach	TS7740
TS7760 Server (3957-Vxx) TS7760 Cache Controller (3956-CSA) TS7760 Cache Drawer (3956-XSA) 3952 Tape Frame Optional cache attachment: Up to two 3952 F06 Storage Expansion Frames	TS7760 Server (3957-Vxx) TS7760 Cache Controller (3956-CSA) TS7760 Cache Drawer (3956-XSA) 3952 Tape Frame Optional cache attachment: Up to two 3952 F06 Storage Expansion Frames	TS7720 Server (3957-Vxx) TS7720 Cache Controller (3956-CS9) TS7720 Cache Drawer (3956-XS9) 3952 Tape Frame Optional cache attachment: Up to two 3952 F05 Storage Expansion Frames	TS7720 Server (3957-Vxx) TS7720 Cache Controller (3956-CS9) TS7720 Cache Drawer (3956-XS9) 3952 Tape Frame Optional cache attachment: Up to two 3952 F05 Storage Expansion Frames	TS7740 Server (3957-Vxx) TS7740 Cache Controller (3956-CC9) TS7740 Cache Drawer (3956-CX9) 3952 Tape Frame

Table 1. TS7700 system configurations (continued)

Disk-only TS7760	TS7760 Tape Attach	Disk-only TS7720	TS7720 Tape Attach	TS7740
The disk-only TS7760 does not attach to a physical library.	**Library Attachments** TS3500/TS4500 Tape Library **TS3500 Tape Library** 3592 Tape Drives • TS1150 Tape Drive (supported with 8.33.0 code or higher) • TS1140 Tape Drive • TS1130 Tape Drive • TS1120 Tape Drive (in native mode and emulating a 3592 J1A Tape Drive) • 3592 J1A Tape Drive **TS4500 Tape Library** 3592 Tape Drives • TS1150 Tape Drive • TS1140 Tape Drive **Tape Cartridges** 3592 Tape Cartridge	The disk-only TS7720 does not attach to a physical library.	**Library Attachments** TS3500/TS4500 Tape Library **TS3500 Tape Library** 3592 Tape Drives • TS1150 Tape Drive (supported with 8.33.0 code or higher) • TS1140 Tape Drive • TS1130 Tape Drive • TS1120 Tape Drive (in native mode and emulating a 3592 J1A Tape Drive) • 3592 J1A Tape Drive **TS4500 Tape Library** 3592 Tape Drives • TS1150 Tape Drive • TS1140 Tape Drive **Tape Cartridges** 3592 Tape Cartridge	**Library Attachments** TS3500/TS4500 Tape Library **TS3500 Tape Library** 3592 Tape Drives • TS1150 Tape Drive (supported with 8.33.0 code or higher) • TS1140 Tape Drive • TS1130 Tape Drive • TS1120 Tape Drive (in native mode and emulating a 3592 J1A Tape Drive) • 3592 J1A Tape Drive **TS4500 Tape Library** 3592 Tape Drives • TS1150 Tape Drive • TS1140 Tape Drive **Tape Cartridges** 3592 Tape Cartridge

Refer to the *IBM System Storage Interoperation Center (SSIC)* link in the **Related information** section for information concerning the interoperability of released IBM TS7700 microcode and components.

Related information

IBM System Storage Interoperation Center (SSIC)

"TS7700 system components"

"TS7700 system component details" on page 33

"TS7720 Storage Expansion Frame" on page 45

TS7700 system components

The TS7700 consists of several primary components that can be described in terms of their system role or according to their technical functions.

Nodes, Clusters, and Grid

The TS7700 is built on a distributed node architecture. The nodes perform either virtualization (vNode) or hierarchical data storage management (hNode). The vNode presents the virtual image of a library(ies) and the drives to a host system. When the TS7700 is attached to a physical library, the vNode also receives tape drive and library requests from the host and processes them as real devices do. It then translates the tape requests through a virtual drive and uses a file in a file system to represent the virtual tape image. Once created or altered by the host system through a vNode, a virtual volume resides in disk cache or on physical tape, where it is managed by the hNode. When the TS7700 is attached to a physical library, the hNode is the only node that is aware of physical tape resources and the relationships between the virtual and physical volumes. The hNode is also responsible for any replication of the virtual volumes and their attributes across site boundaries.

Based on the node architecture, a vNode or hNode can run on separate virtualization hardware or be combined to run on the same hardware. When a vNode and hNode are combined to run on the same virtualization hardware, they are referred to collectively as a General Node, or gNode. The TS7700 runs a gNode. See Figure 1 for an illustration of the relationship between nodes.

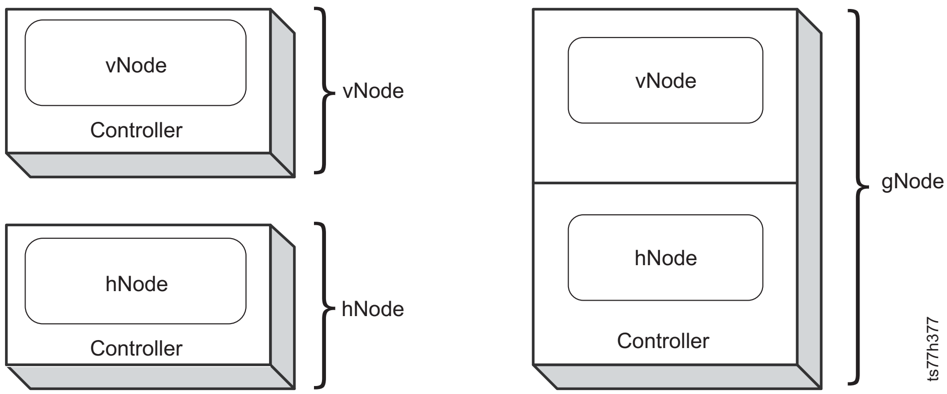


Figure 1. vNode, hNode, and gNode construction

The TS7700 *Cluster* combines the TS7700 Server with a disk subsystem, the TS7700 Cache Controller. This architecture permits additional disks or nodes to be added in future offerings to expand the capabilities of the system. Figure 2 displays a TS7700 configured as a cluster.

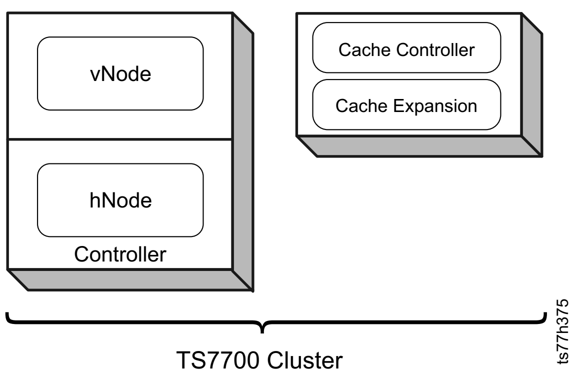


Figure 2. TS7700 Cluster configuration

The TS7700 *Grid*, or grid configuration, is a series of two or more clusters that are connected to one another to form a high availability or disaster recovery solution. Virtual volume attributes and data are replicated across the clusters in a grid to ensure the continuation of production work, should a single cluster become unavailable.

A virtual volume can be accessed from any virtual device in the system, even if the virtual volume has only a single replica. Should a failure occur at the source cluster, replicated virtual volumes are still available since any data that is replicated between the clusters is accessible through any other cluster in a grid configuration. Each copy is a valid source of the virtual volume. A grid configuration looks like a single storage subsystem to the hosts attached to the clusters; it can be described as a composite library with underlying distributed libraries similar to the prior generation's peer-to-peer (PTP) VTS. For more information about data accessibility in the event of a source cluster failure, see "The Autonomic Ownership Takeover Manager" on page 282.

A TS7700 Grid can be created by using TS7700 disk-only clusters, TS7700 tape-attached clusters, or a combination of both.

Multiple TS7700 Grids can be attached to the same host system yet operate independent of one another.

Figure 3 shows a typical six-cluster grid.

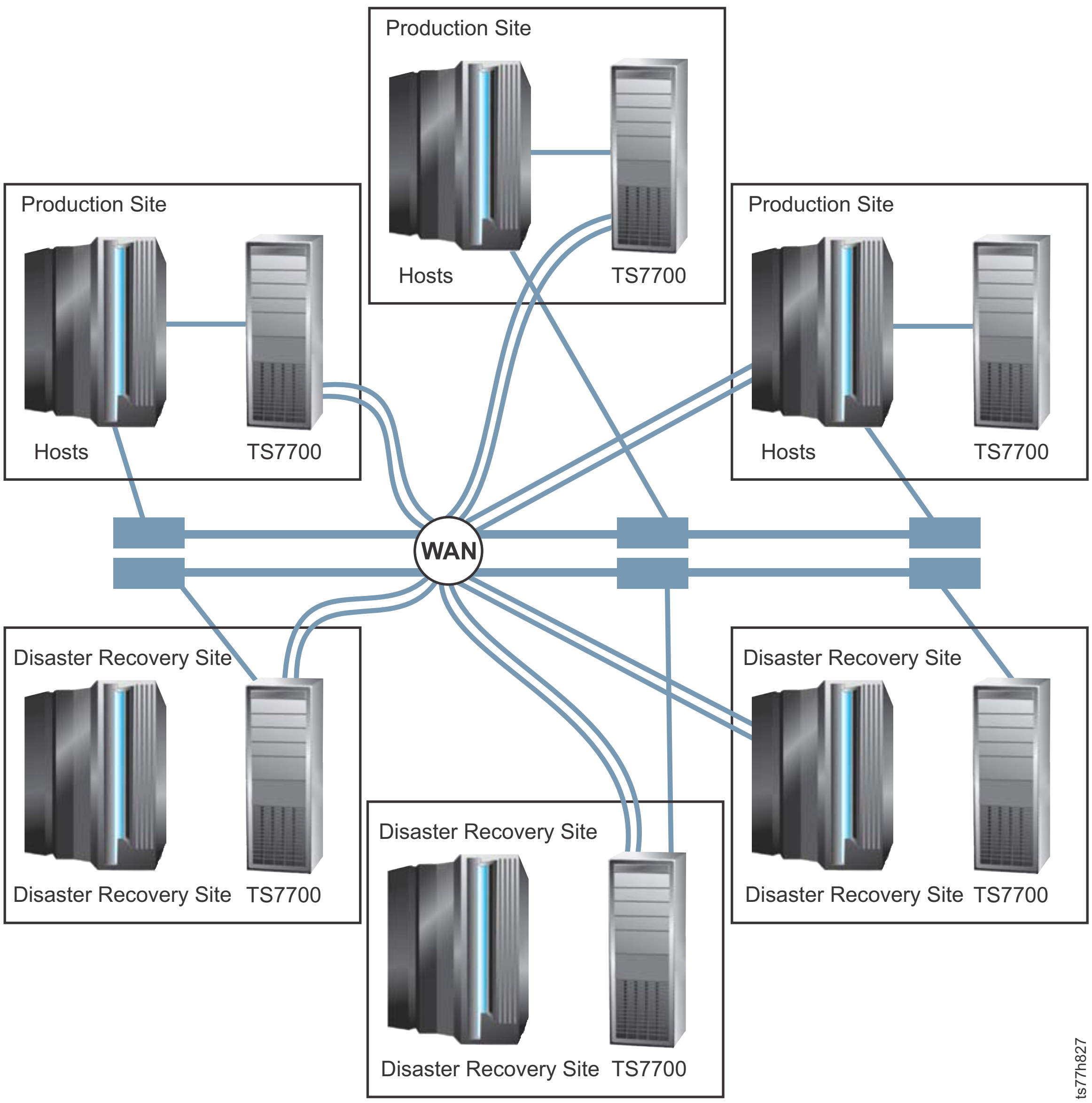


Figure 3. TS7700 six-cluster grid configuration

†FICON channel extenders are optional.

Operational components

A TS7700 configured as a gNode is consists of these major operational components:

- A TS7700 Server (includes System Unit and Expansion Unit with I/O drawers)
- A TS7700 Cache Controller
- TS7700 Cache Drawers (optional depending on configuration)
- A 3952 Tape Frame

Note: A TS7700 can also be configured to include a TS7700 Storage Expansion Frame, which houses additional TS7700 Cache Controllers and TS7700 Cache Drawers.

The configuration of these components differs depending on whether a TS7700 is configured as a TS7760, TS7720, or a TS7740.

Figure 4 compares the major operational components of the TS7700 in each of these configurations, contained by a 3952 Tape Frame.

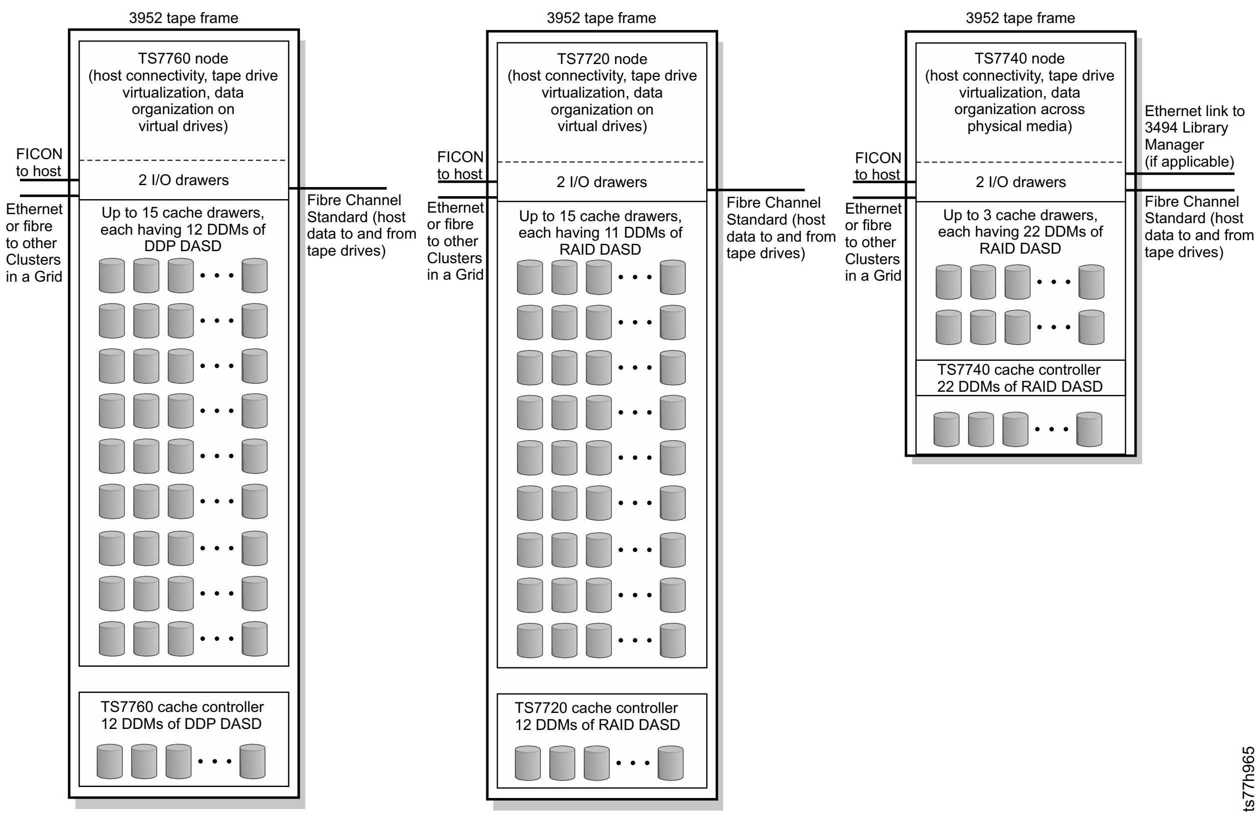


Figure 4. TS7760, TS7720, and TS7740 operational components

Related information

“Concepts of storage virtualization” on page 1
“TS7700 system configurations” on page 15
“TS7700 system component details” on page 33
“TS7700 Grid” on page 257
“TS7720 Storage Expansion Frame” on page 45

Tape frame

A TS7700 is enclosed by a 3952 Tape Frame.

A 3952 Tape Frame contains the TS7700 Server, TS7700 Cache, and the TS3000 TSSC, and additional components such as switches and power distribution units for connection to independent power sources. The 3952 Tape Frame model F05 can house either a TS7720 or a TS7740. The 3952 Tape Frame model F06 can house a TS7760.

Additionally, a 3952 Tape Frame can be designated as a TS7720 or TS7760 Storage Expansion Frame to expand the capacity of a TS7700 disk-only Cluster.

Related information

"Concepts of storage virtualization" on page 1

"TS7700 system configurations" on page 15

"TS7700 system component details" on page 33

"TS7700 Grid" on page 257

TS7700 Server

The TS7700 Server facilitates data transfer between the host and data storage, and to and from physical tape drives when the TS7700 connects to a physical tape library.

The TS7700 Server performs the following major functions:

- Host connectivity
- Virtualization of tape drives and media, when connected to a physical tape library
- Storage, replication, and organization of data, including organization across tape libraries and physical media when connected to a physical tape library

3957-VEC configuration

A TS7700 Server (3957-VEC) configuration includes:

- 2 processor sockets each 3.42 GHz with 10 processor core
- 32 GB of DDR3 CDIMM @ 1600 Mbps
- Additional SAS Solstice-crocodile controller with support for RAID 0,1,5,6 and 10
- 8 SFF 300 GB SAS 15K RPM internal drives using RAID0 (through a split back plane)
- 1 slim line DVD RAM drive
- EEH and hot plug support on PCI adapters
- Disk cache w/ 4 TB HDDs
- TS3500 and TS4500 tape library support
- 16 Gb Fibre Channel switches for back-end tape
- Grid Dual port 1 Gb (copper or optical) Ethernet or dual port 10 Gb Optical Ethernet

Table 2. TS7700 Server System Unit (3957-VEC) adapters

Slot Number	Adapter
2	Serial Adapter

Table 2. TS7700 Server System Unit (3957-VEC) adapters (continued)

Slot Number	Adapter
5	I/O Drawers Interface card
6	I/O Drawers Interface card
10	PCIe2 LP 4-port 1 Gb Ethernet Adapter
11	PCIe2 LP 4-port 1 Gb Ethernet Adapter

The TS7700 Server Expansion Unit for the 3957-VEC includes two input/output (I/O) drawers, which are identically configured and simultaneously active. The I/O drawers contain ports for connection to the host, to other internal component interfaces, and to tape drives when the TS7700 Server is connected to a tape library. Table 3 displays the slot numbers and adapters associated with ports on the expansion unit I/O drawers.

Table 3. TS7700 Server Expansion Unit I/O drawer adapters for 3957-VEC

Slot Number	Adapter
1	Grid PCIe Ethernet adapter: • Dual port 1 Gb copper ("FC 1036, 1 Gb grid dual port copper connection" on page 153), or • Dual port 1 Gb SW optical ("FC 1037, 1 Gb dual port optical SW connection" on page 153), or • Dual port 10 Gb LW optical ("FC 1038, 10 Gb dual port optical LW connection" on page 153)
2	Not used
3	16 Gb FICON attachment to host or 8 Gb FICON attachment to host‡
4	Dual port 16 Gb Fibre Channel FCoE: Cache Expansion Frames 1 and 2
5	Dual port 16 Gb Fibre Channel FCoE: Cache and Tape Attach
6	16 Gb FICON attachment to host or 8 Gb FICON attachment to host‡
‡When four FICON adapters connect to hosts **Notes:** • FICON adapters can be upgraded in number (two to four) and kind (shortwave or longwave) by using "FC 3402, 16 Gb FICON Short Wavelength Attachment" on page 156 and "FC 3403, 16 Gb FICON Long Wavelength Attachment" on page 157 or "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157 and "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157. • "FC 3401, Enable FICON dual port" on page 156 can be used to enable the second port of the FICON adapter, allowing a four-adapter cluster to upgrade to eight host connections (two per card). "FC 3402, 16 Gb FICON Short Wavelength Attachment" on page 156, "FC 3403, 16 Gb FICON Long Wavelength Attachment" on page 157, "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157 or "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157 is a prerequisite.	

The minimum required TS7760 microcode level is 8.40.0.xx for use with the 3957-VEC and TS7760 Tape Attach. Ask your IBM service representative to receive the most current level of TS7700 code.

3957-V07 and 3957-VEB configuration

Note: The TS7700 Server models 3957-V07 and 3957-VEB were withdrawn on June 2016.

A TS7700 Server (3957-V07 or 3957-VEB) configuration includes:

- 8 cores, on a 3.0 GHz processor card
- 16 GB or 32 GB of 1066 MHz ECC memory in a single processor card
- The following integrated features:
  - Service processor
  - 1 Gb or 10 Gb Ethernet
  - EnergyScale™ technology
  - 3 USB ports
  - 2 system (serial) ports
  - 2 HMC ports
  - 2 SPCN ports
- The following expansion slots:
  - 2 PCIe x8 slots (short length adapter)
  - 1 PCIe slot (full adapter length)
  - 2 PCI-X DDR slots (full adapter length)
- The following storage features:
  - An internally connected 4-drive SAS bay
  - A second 4-drive SAS bay connected by SAS adapter in the PCIe short slot
- A slim media bay for DVD-RAM

The TS7700 Server System Unit (3957-V07 or 3957-VEB) includes gigabit copper and optical fiber Ethernet adapters for grid configuration connection. Table 4 displays the slot numbers and adapters associated with ports on the system unit.

Table 4. TS7700 Server System Unit (3957-V07 or 3957-VEB) adapters

<table>
<tr><th>Slot Number</th><th>Adapter</th></tr>
<tr><td>1</td><td>PCIe dual-x4 adapter for SAS</td></tr>
<tr><td>2</td><td rowspan="2">PCIe adapter for connection to Expansion Unit I/O drawer</td></tr>
<tr><td>3</td></tr>
<tr><td>4</td><td rowspan="2">1-Gb Ethernet adapter to grid:
• Copper
– “FC 1032, 1 Gb grid dual port copper connection” on page 152
– “FC 1036, 1 Gb grid dual port copper connection” on page 153* installed on the I/O drawer
or
• Optical fiber
– “FC 1033, 1 Gb grid dual port optical SW connection” on page 152
– “FC 1035, 10 Gb grid optical LW connection” on page 153* installed on the I/O drawer
– “FC 1037, 1 Gb dual port optical SW connection” on page 153* installed on the I/O drawer</td></tr>
<tr><td>5</td></tr>
<tr><td colspan="2">*Minimum required TS7700 microcode level is 8.20.0.xx.</td></tr>
</table>

The TS7700 Server Expansion Unit for the 3957-V07 or 3957-VEB includes two input/output (I/O) drawers, which are identically configured and simultaneously active. The I/O drawers contain ports for connection to the host, to other internal component interfaces, and to tape drives when the TS7700 Server is connected to a tape library. Table 5 on page 23 displays the slot numbers and adapters associated with ports on the expansion unit I/O drawers.

Table 5. TS7700 Server Expansion Unit I/O drawer adapters for 3957-V07 or 3957-VEB

Slot Number	Adapter
1	Grid PCIe Ethernet adapter: • Dual port 1 Gb copper, or • Dual port 1 Gb optical, or • Single port 10 Gb
2	Not used
3	• PCIx 4 Gb FICON attachment to host‡, or • PCIx 8 Gb FICON attachment to host‡
4	PCIe 8 Gb dual port Fibre Channel: • Used for tape drive attachment by 3957-V07 • Present in 3957-VEB only if the optional cache expansion frame is installed
5	PCIe 8 Gb dual port Fibre Channel: • Used for primary cache controller • Used for tape drive attachment by 3957-VEB tape attach
6	• PCIx 4 Gb FICON attachment to host, or • PCIx 8 Gb FICON attachment to host
‡When four FICON adapters connect to hosts **Notes:** • FICON adapters can be upgraded in number (two to four) and kind (shortwave or longwave) by using "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157 and "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157. • "FC 3401, Enable FICON dual port" on page 156 can be used to enable the second port of the 8 Gb FICON adapter, allowing a four-adapter cluster to upgrade to eight host connections (two per card). "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157 or "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157 is a prerequisite.	

The minimum required TS7700 microcode level is 8.20.0.xx for use with the 3957-V07 and 3957-VEB. Ask your IBM service representative to receive the most current level of TS7700 code.

Related information

"Concepts of storage virtualization" on page 1

"TS7700 system configurations" on page 15

"TS7700 system component details" on page 33

"TS7700 Grid" on page 257

TS7700 Cache Controller

The TS7700 Cache Controller consists of a redundant array of independent disks (RAID) controller and associated Security Encryption Drive (SED), encryption-capable disk storage media, which act as cache storage for data.

The TS7700 Cache Controller contains up to 24 disk drive modules (DDMs), depending on your configuration.

Note: Total cache capacity that is shown reflects raw capacity and does not directly correlate to usable capacity.

TS7760 Cache Controller
The TS7760 Cache Controller (3956-CSA) contains 12 DDMs, which each have a capacity of 4 TB (3.63 TiB) or 8 TB (7.27 TiB). You can mix 4 TB or 8 TB drives within a frame but you cannot mix them within a drawer or enclosure. The 3956-CSA and corresponding 3956-XSA drawers support all encryption abilities as the 3956-CS9 controllers, including cryptographical erase, internal key management, external key management, and retro-active enablement. The 3956-CSA cache controller and supported 3956-XSA expansion drawers support the ability of Dynamic Disk Pools (DDP). This virtual RAID6 technology can provide an RAID6 level of reliability while drastically cutting down the drive rebuild times after a drive failure.

For extended cache capacity, you can order "FC 7334, TS7700 Encryption-capable expansion frame" on page 175 to obtain a new TS7700 Expansion Frame. You can order "FC 9323 Expansion frame attachment" on page 179 against an existing TS7760 Base Frame, so that the TS7760 Base Frame and the TS7700 Expansion Frame can be attached together. The TS7700 Expansion Frame contains one additional 3956-CSA cache controller with the capacity to support up to fifteen 3956-XSA Drawers with a 4 TB configuration. An 8 TB configuration can support up to fourteen 3956-XSA Cache Drawers.

TS7720 Cache Controller
The TS7720 Cache Controller (3956-CS9) contains 12 DDMs, which each have a capacity of 3 TB (2.73 TiB). Total usable capacity per controller is 24 TB (21.83 TiB) when used with RAID-6 formatting.

For extended cache capacity, you can order "FC 7323, TS7720 Storage expansion frame" on page 174 against a new 3952 Tape Frame and "FC 9323 Expansion frame attachment" on page 179 against the TS7720 Base Frame to attach a fully configured TS7720 to the TS7720 Storage Expansion Frame. This cache expansion frame contains one additional TS7720 with the capacity to support up to 15 TS7720 Cache Drawers.

TS7740 Cache Controller
The TS7740 Cache Controller (3956-CC9) contains 22 DDMs, which each have a potential capacity up to 600 GB (558.78 GiB). Total usable capacity per controller is 9.33 TB (8.49 TiB) when used with RAID-6 formatting.

Related information

"Concepts of storage virtualization" on page 1

"Data storage values" on page 28

"TS7700 feature codes" on page 143

"TS7700 system configurations" on page 15

"TS7700 system component details" on page 33

"TS7700 upgrade options" on page 106

"TS7700 Grid" on page 257

"TS7760 Cache Drawer" on page 43

"TS7760 Storage Expansion Frame" on page 39

TS7700 Cache Drawer

The TS7700 Cache Drawer acts as an expansion unit for the TS7700 Cache Controller, and collectively both are referred to as the *TS7700 Cache*.

The amount of cache available per TS7700 Cache Drawer depends on your configuration.

TS7760 Cache Drawer

Each TS7760 Cache Drawer contains 12 DDMs, which in turn each have a raw capacity of 8 TB or 4 TB.

4 TB Disk Drive Capacity Configurations

Total usable capacity per drawer is approximately 31 TB (28.29 TiB) when used with dynamic disk pool formatting.

The base TS7760 Cache (contained by the TS7760 Base Frame) can be configured to contain up to nine TS7760 Cache Drawers attached to one TS7760 Cache Controller. Fully configured, the base TS7760 Cache has a total usable capacity of 313.96 TB (285.55 TiB). Table 6 displays the storage capacities of a base TS7760 Cache Controller with a range of TS7760 Cache Drawer configurations with 4 TB DDMs.

Table 6. Base TS7760 Cache configurations and capacities with 4 TB drives. Table describes the configurations and capacities of the base TS7760 Cache.

Number of TS7760 Cache Controllers (3956-CSA)	Number of TS7760 Cache Drawers (3956-XSA) using 4 TB drives	Raw capacity	Usable (available) capacity
1	0	48 TB (43.65 TiB)	31.11 TB (28.29 TiB)
	1	96 TB (87.33 TiB)	62.53 TB (56.87 TiB)
	2	144 TB (130.99 TiB)	93.96 TB (85.46 TiB)
	3	192 TB (174.66 TiB)	125.39 TB (114.04 TiB)
	4	240 TB (218.32 TiB)	156.82 TB (142.63 TiB)
	5	288 TB (261.99 TiB)	188.25 TB (171.21 TiB)
	6	336 TB (305.65 TiB)	219.68 TB (199.79 TiB)
	7	384 TB (349.31 TiB)	251.10 TB (228.38 TiB)
	8	432 TB (392.98 TiB)	282.53 TB (256.96 TiB)
	9	480 TB (436.64 TiB)	313.96 TB (285.55 TiB)

Note: The raw capacity that is shown is the storage capacity before any formatting takes place. The formatted capacity is the storage capacity after the 3956-CSA/XSA initializes the drive(s). The usable capacity is the storage capacity available for customer use inside a GPFS file system after the formatted disks are divided into logical unit numbers (LUNs) inside a dynamic disk pool.

8 TB Disk Drive Capacity Configurations

Total usable capacity per drawer is approximately 61.55 TB (55.98 TiB) when used with dynamic disk pool formatting.

The base TS7760 Cache (contained by the TS7760 Base Frame) can be configured to contain up to nine TS7760 Cache Drawers attached to one TS7760 Cache Controller. Fully configured, the base TS7760 Cache has a total usable capacity of 618.12 TB (562.16 TiB). Table 7 displays the storage capacities of a base TS7760 Cache Controller with a range of TS7760 Cache Drawer configurations with 8 TB DDMs.

Table 7. Base TS7760 Cache configurations and capacities with 8 TB drives. Table describes the configurations and capacities of the base TS7760 Cache.

Number of TS7760 Cache Controllers (3956-CSA)	Number of TS7760 Cache Drawers (3956-XSA) using 8 TB drives	Raw capacity	Usable (available) capacity
1 **Note:** The raw capacity that is shown is the storage capacity before any formatting takes place. The formatted capacity is the storage capacity after the 3956-CSA/XSA initializes the drive(s). The usable capacity is the storage capacity available for customer use inside a GPFS file system after the formatted disks are divided into logical unit numbers (LUNs) inside a dynamic disk pool.	0	96 TB (87.33 TiB)	61.55 TB (55.98 TiB)
	1	192 TB (174.66 TiB)	123.39 TB (112.22 TiB)
	2	288 TB (261.99 TiB)	185.23 TB (168.47 TiB)
	3	384 TB (349.31 TiB)	247.07 TB (224.71 TiB)
	4	480 TB (436.64 TiB)	308.91 TB (280.96 TiB)
	5	576 TB (523.87 TiB)	370.76 TB (337.20 TiB)
	6	672 TB (611.18 TiB)	432.60 TB (393.44 TiB)
	7	768 TB (698.49 TiB)	494.44 TB (449.69 TiB)
	8	864TB (785.803 TiB)	556.28 TB (505.93 TiB)
	9	960 TB (873.115 TiB)	618.12 TB (562.16 TiB)

Note: The raw capacity that is shown is the storage capacity before any dynamic disk pool RAID or file system formatting takes place. The usable capacity is the storage capacity available for customer use after the raw capacity has dynamic disk pool RAID6 formatting applied. Roughly 20% of the capacity is reserved for disk failure rebuild, a minimal amount of capacity set aside for TS7700 use and any file system formatting overhead.

TS7760 Storage Expansion Frame

A fully configured base TS7760 Cache can be expanded by attaching to a TS7760 Storage Expansion Frame by using "FC 7334, TS7700 Encryption-capable expansion frame" on page 175. The TS7760 Storage Expansion Frame adds one TS7760 Cache Controller (3956-CSA), which can attach to a maximum of 15 TS7760 Cache Drawers (3956-XSA).

Note: This is specifically for a string that is 100% populated by drawers with 4 TB drives. A string that is 100% populated by drawers with 8 TB drives can attach up to a maximum of 14 cache drawers.

For configurations and capacities of a TS7760 Cache including a TS7760 Storage Expansion Frame, refer to "TS7760 Storage Expansion Frame Configurations with 4 TB DDMs" on page 39 and "TS7760 Storage Expansion Frame Configurations with 8 TB DDMs" on page 41in the *TS7760 Storage Expansion Frame* topic link, available in the **Related information** section.

For more information concerning field installation, see "FC 5659, Field installation of 3956-XSA" on page 170 and "FC 9355, Field merge" on page 180.

TS7720 Cache Drawer

Each TS7720 Cache Drawer contains 11 DDMs, which in turn each have a raw capacity of 3 TB (2.73 TiB). Total usable capacity per drawer is approximately 24 TB (21.83 TiB) when used with RAID-6 formatting.

The base TS7720 Cache (contained by the TS7720 Base Frame) can be configured to contain up to nine TS7720 Cache Drawers attached to one TS7720 Cache Controller. Fully configured, the base TS7720 Cache has a total usable capacity of 238.79 TB (217.18 TiB). Table 8 displays the storage capacities of a base TS7720 Cache with a range of TS7720 Cache Drawer configurations.

Table 8. Base TS7720 Cache configurations and capacities. Table describes the configurations and capacities of the base TS7720 Cache.

Number of TS7720 Cache Controllers (3956-CS9)	Number of TS7720 Cache Drawers (3956-XS9)	Raw RAID-6 capacity	GPFS-formatted capacity	Usable capacity
1	0	24 TB (21.83 TiB)	23.86 TB (21.7 TiB)	22.78 TB (20.72 TiB)
	1	48 TB (43.66 TiB)	47.86 TB (43.53 TiB)	46.78 TB (42.55 TiB)
	2	72 TB (65.48 TiB)	71.86 TB (65.36 TiB)	70.79 TB (64.38 TiB)
	3	96 TB (87.31 TiB)	95.86 TB (87.18 TiB)	94.79 TB (86.21 TiB)
	4	120 TB (109.14 TiB)	119.86 TB (109.01 TiB)	118.79 TB (108.04 TiB)
	5	144 TB (130.97 TiB)	143.86 TB (130.84 TiB)	142.79 TB (129.87 TiB)
	6	168 TB (152.8 TiB)	167.86 TB (152.67 TiB)	166.79 TB (151.69 TiB)
	7	192 TB (174.62 TiB)	191.86 TB (174.5 TiB)	190.79 TB (173.52 TiB)
	8	216 TB (196.45 TiB)	215.86 TB (196.32 TiB)	214.79 TB (195.35 TiB)
	9	240 TB (218.28 TiB)	239.86 TB (267.26 TiB)	238.79 TB (217.18 TiB)

Note: The raw capacity that is shown is that of the RAID subsystem. The General Parallel File System (GPFS) formatted capacity is the capacity that remains after the RAID is divided into logical unit numbers (LUNs), which are assigned to usable file systems. Usable capacity is that which exists after microcode introduces a read-only usage ceiling.

A fully configured base TS7720 Cache can be expanded by attaching to a TS7720 Storage Expansion Frame by using “FC 7332, TS7720 Encryption-capable expansion frame” on page 174. The TS7720 Storage Expansion Frame adds one TS7720 Cache Controller (3956-CS9), which can attach to a maximum of 15 TS7720 Cache Drawers (3 TB 3956-XS9).

In the TS7720 Storage Expansion Frame each TS7720 Cache Controller and its attached TS7720 Cache Drawers are referred to as "strings", with each TS7720 Cache Controller acting as the "head of [the] string". For configurations and capacities of a TS7720 Cache including a TS7720 Storage Expansion Frame, refer to Table 15 on page 47 in the *TS7720 Storage Expansion Frame* topic link, available in the **Related information** section.

For more information concerning field installation, see “FC 5656, Field installation of 3956-XS9” on page 169 and “FC 9355, Field merge” on page 180.

TS7740 Cache Drawer

Each TS7740 Cache Drawer contains 22 DDMs, which each has a potential capacity up to 600 GB (558.78 GiB). Total raw capacity per drawer is 9.6 TB (8.73 TiB) when used with RAID-6 formatting. Table 9 displays the storage capacities of a base TS7740 Cache with a range of TS7740 Cache Drawer configurations.

Table 9. TS7740 Cache configurations and capacities. Table describes the configurations and capacities of the TS7740 Cache .

Number of TS7740 Cache Controllers (3956-CC9)	Number of TS7740 Cache Drawers (3956-CX9)	Raw RAID-6 capacity	GPFS-formatted capacity
1	0	9.6 TB (8.73 TiB)	9.45 TB (8.59 TiB)
	1	19.2 TB (17.46 TiB)	19.03 TB (17.30 TiB)
	2	28.8 TB (26.19 TiB)	28.60 TB (26.02 TiB)

Related information

“Concepts of storage virtualization” on page 1

“Data storage values”

“TS7700 system configurations” on page 15

“TS7700 system component details” on page 33

“TS7700 upgrade options” on page 106

“TS7700 Grid” on page 257

“TS7760 Storage Expansion Frame” on page 39

Data storage values

TS7700 documentation displays data storage values by using both decimal (base-10) prefixes and binary (base-2) units of measurement.

Decimal units such as K, MB, GB, and TB have commonly been used to express data storage values, though these values are more accurately expressed by using binary units such as KiB, MiB, GiB, and TiB. At the kilobyte level, the difference between decimal and binary units of measurement is relatively small (2.4%). This difference grows as data storage values increase, and when values reach terabyte levels the difference between decimal and binary units approaches 10%.

To reduce the possibility of confusion, the IBM TS7700 Information Center represents data storage by using both decimal and binary units. Data storage values are displayed by using the following format:

```
#### decimal unit (binary unit)
```

By this example, the value 512 terabytes is displayed as:

```
512 TB (465.6 TiB)
```

Table 10 compares the names, symbols, and values of the binary and decimal units. Table 11 shows the increasing percentage of difference between binary and decimal units.

Table 10. Comparison of binary and decimal units and values

Decimal			Binary		
Name	**Symbol**	**Value (base-10)**	**Name**	**Symbol**	**Value (base-2)**
kilo	K	10^3	kibi	Ki	2^{10}
mega	M	10^6	mebi	Mi	2^{20}
giga	G	10^9	gibi	Gi	2^{30}
tera	T	10^{12}	tebi	Ti	2^{40}
peta	P	10^{15}	pebi	Pi	2^{50}
exa	E	10^{18}	exbi	Ei	2^{60}

Table 11. Percentage difference between binary and decimal units

Decimal Value	Binary Value	Percentage Difference
100 kilobytes (KB)	97.65 kibibytes (KiB)	2.35%
100 megabytes (MB)	95.36 mebibytes (MiB)	4.64%
100 gigabytes (GB)	93.13 gibibytes (GiB)	6.87%
100 terabytes (TB)	90.94 tebibytes (TiB)	9.06%
100 petabytes (PB)	88.81 pebibytes (PiB)	11.19%
100 exabytes (EB)	86.73 exbibytes (EiB)	13.27%

Dynamic Disk Pooling (DDP)

Dynamic Disk Pooling (DDP) dynamically distributes data, spare capacity, and protection information across a pool of disk drives. DDP improves the time and performance of traditional RAID arrays. DDP will only be supported on 3956-CSA/XSA subsystems.

The TS7700 3956-CSA/XSA subsystem has a dynamic disk pools (DDP) configuration by default, supported by a microcode of 8.40.0.xx or higher. Previous TS7700 releases, such as CC9/CS9 and prior, used an RAID6 configuration. DDP is also known as Distribute RAID, or D-RAID.

Because RAID cannot keep up with increasing disk capacities, DDP was created to be more versatile by providing better rebuild times. In an RAID array when a drive fails, the remaining drives are read, parity recomputed, and the result is written to the spare drive. This is done from the initial logical block of the array to the last block in the array. This operation is time consuming because all data needs to be recomputed from the beginning of the array to the end of the array, and degrades performance, because although there are parallel reads, there is one single write to the spare drive. Thus, this single write becomes a bottleneck in the system.

In DDP, a disk pool is a set of drives that are logically grouped together in the storage subsystem, where data is distributed across all drives in the pool. The drives in each disk pool must be of the same drive type and drive media type, and they must be similar in size. Unlike RAID, there is no specific spare drive, rather, all drives have spare space that is reserved. When a drive fails, the remaining drives are read, the missing data is recomputed, and the result is written to multiple drives in their spare space. This operation is done on the pieces of data that are missing. The result is parallel reads and parallel writes, which significantly speeds up the rebuild time after a single drive failure.

Both RAID and DDP are techniques for striping data and parity information across a set of disks to provide fault tolerance, but how they operate to attain this goal is different.

The DDP design offers the following features:

Dual Drawer Configuration
: **24 DDM** type (dual drawer): A pool that consists of two enclosure pairs that contain a total of 24 DDMs. The pair of enclosures consists of either a CSA and XSA or two XSAs.

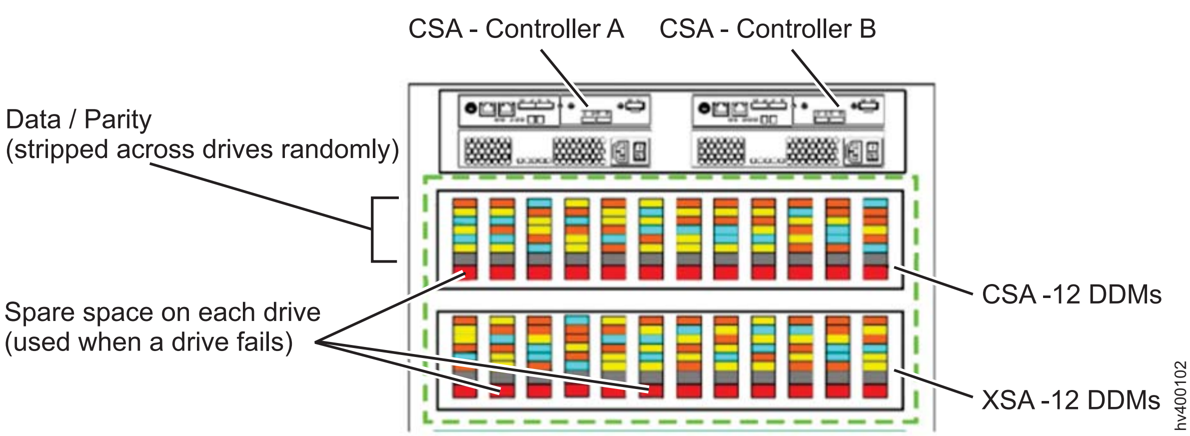


Figure 5. Dynamic Disk Pool example for a two (dual) drawer configuration (CSA and XSA)

Single Drawer Configuration
: **12 DDM** type (single drawer): A pool that consists of one enclosure that contains 12 DDMs. This type can be within a cache string that contains a single CSA with no XSA attached OR an XSA at the end of a cache string that has an odd number of enclosures (CSA + XSAs).

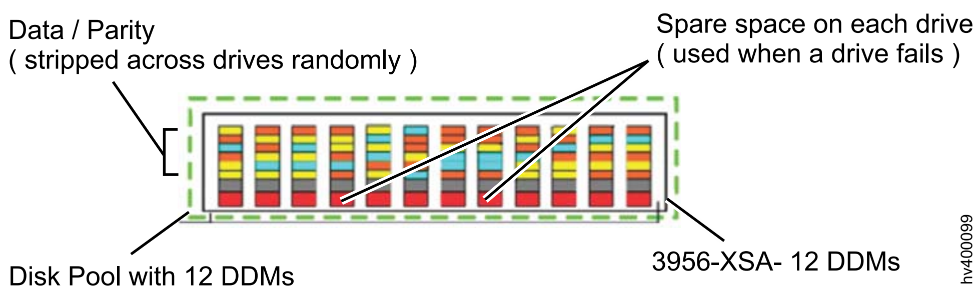


Figure 6. Dynamic Disk Pool example for a one (single) drawer configuration (XSA)

Traditional RAID Drive Rebuilds Eliminated

Data is automatically rebalanced across the drive pool.

Faster rebuild times after a drive failure.

Improved Performance

Automated load balancing.

Maintains performance under drive failure. Up to two DDMs can fail simultaneously at any time in the pool. For a pool that contains 12 drives, up to 2 DDMs can fail without shutting down the system. For a pool that contains 24 drives, up to 4 DDMs can fail.

Reserved (spare) space is allocated across all the drives within a dynamic disk pool. The amount of reserved (spare) space in a pool is equal to about two disks worth of space per drawer.

Low Maintenance

No dedicated physical spare drives.

No RAID groups.

No dedicated parity drives.

Related information

"TS7700 Cache Controller" on page 23

Chapter 2. Planning

The topics in this section provide planning information related to your TS7700.

TS7700 system component details

Major components of the TS7700 include the 3952 Tape Frame, TS7700 Server, TS7700 Cache Controller, and TS7700 Cache Drawer.

3952 Tape Frame details

This topic describes the key characteristics of the 3952 Tape Frame.

Note: Any lock on the 3952 Tape Frame prevents access to the TS7700 Emergency Power Off (EPO) switch. If a lock (FRU 12R9307) is installed on the 3952 Tape Frame, an external EPO switch or circuit breaker must be installed near the TS7700 to allow an emergency shutdown. Additionally, the emergency contact label that is included with the *Installation Instruction RPQ 8B3585 (Front/Rear and Side Panel Locking Procedure)*, PN 46X6208, must be completed and affixed to the 3952 Tape Frame door in an immediately visible location. This label must clearly indicate the location of the external EPO switch or circuit breaker.

If a lock is installed on the 3952 Tape Frame and the original key is not available, any 3952 Tape Frame key can be used to open the lock. If no frame key is available and immediate access is required to get inside the frame, you must contact a locksmith to open the lock. If the key is still unavailable after the lock is opened, you can contact your IBM service representative to order a new lock and key set (FRU 12R9307).

The 3952 Tape Frame houses TS7700 controllers and their components. The 3952 Tape Frame that is used with the TS7700 contains the following components:

- Ethernet switches
- Optional components
  - TSSC Server
  - Keyboard and monitor
  - Ethernet switch
- TS7700 Server
  - TS7760 Server (3957-VEC)
  - TS7720 Server (3957-VEB)
  - TS7740 Server (3957-V07)
- I/O drawers
- Cache controller
  - TS7760 Cache Controller (3956-CSA)
  - TS7720 Cache Controller (3956-CS9)
  - TS7740 Cache Controller (3956-CC9)
- Optional cache expansion drawers
  - TS7760 Cache Drawer (3956-XSA)
  - TS7720 Cache Drawer (3956-XS9)
  - TS7740 Cache Drawer (3956-CX9)

Table 12 lists the physical characteristics of a maximally configured 3952 Tape Frame. For physical specifications of a 3952 Tape Frame and its individual components, refer to the topic *3952 Tape Frame specifications* in the **Related information** section.

Table 12. Physical characteristics of a maximally configured 3952 Tape Frame F06

Characteristic	**Value**
Height	1930.4 mm (76 in.)
Width	616 mm (24.3 in.)
Depth	1397 mm (55 in.)
Weight	746 kg (1645 lbs.) maximally configured †
Power	240 Vac, 20 amp (single phase)
Unit height	40 U
†Refer to the topics "TS7720 specifications and requirements" on page 69, "TS7740 specifications and requirements" on page 73, and "TS7760 specifications and requirements" on page 65 for maximum configurations for the TS7720 , TS7740, and the TS7760.	

The 3952 Tape Frame can be designated as a TS7700 Storage Expansion Frame when ordered with FC 7334, TS7700 Encryption-capable expansion frame. Refer to the topic *TS7760 Storage Expansion Frame* in the **Related information** section for TS7760 Storage Expansion Frame features and storage capacities.

Related information

"3952 Tape Frame specifications" on page 63

"System requirements" on page 63

"TS7720 Storage Expansion Frame" on page 45

"TS7720 specifications and requirements" on page 69

"TS7740 specifications and requirements" on page 73

TS7700 Server details

The TS7700 Server comprises a server and two drawers for I/O adapters.

The TS7700 Server controls virtualization processes such as host connectivity and device virtualization, and hierarchical storage management (HSM) functions such as storage, replication, and organization of data across physical media and libraries.

The TS7700 Server (3957-VEC) offers the following features:

- Two 10-core 3.42 GHz POWER8 processor cards
- Processor card and memory configuration (using only 2x 16 GB DDR3 DIMMs):
  - 32 GB total memory with 1 processor card and 20 cores
- An additional SAS controller with support for RAID 0,1,5,6 and 10
- 8 SFF 300 GB SAS internal drives using RAID 0
- 1-Gb or 10-Gb Ethernet
- Four USB ports:
  - Two USB 3.0 ports for general use
  - Two USB 2.0 ports for the FSP service processor
- One system (serial) port with RJ45 connector
- Two Hardware Management Console (HMC) ports

- Extended Error Handling (EEH) and hot plug support on PCI expansion slots
- Two six-drive SAS bays
- One slim line DVD RAM drive

Each Expansion Unit I/O adapter drawer offers the following features:

- Six additional hot-pluggable PCIe cartridge styler slots (used to house FICON adapters for host attachment, Fibre Channel adapters for cache drawer attachment, Fibre Channel adapters for tape communication, and Ethernet adapters for grid communication).
  - PCIe standard achievable using Kleber riser adapters
  - PCI-X standard achievable using Oroville riser adapters
- Always redundant AC power
- Always redundant cooling
- Concurrent maintenance of:
  - PCIe or PCI-X adapters
  - Two power supplies
  - Two fans

Figure 7 and Figure 8 depict the TS7700 Server System Unit.
Figure 9 on page 36 depicts the TS7700 Server Expansion Unit I/O drawer.

Figure 7. TS7700 Server (3957-VEC) System Unit (front view)

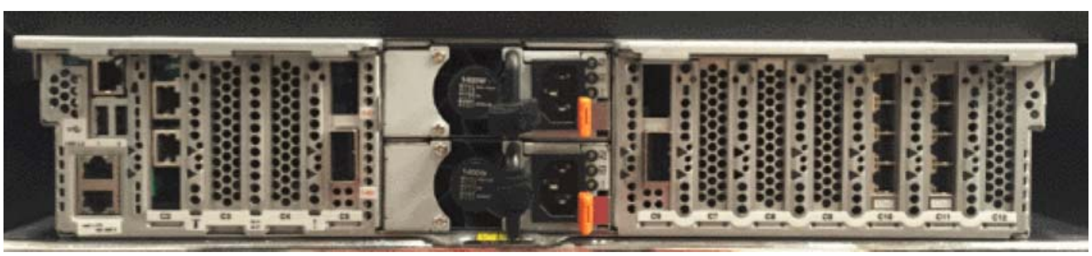


Figure 8. TS7700 Server (3957-VEC) System Unit (rear view)

Figure 9. TS7700 Server Expansion Unit I/O drawer (rear view)

Related information

"System requirements" on page 63

IBM TS7760 details

This section provides topics for the TS7760 components.

Figure 10 on page 37 displays the frame layout for a manufacturing installed TS7760.

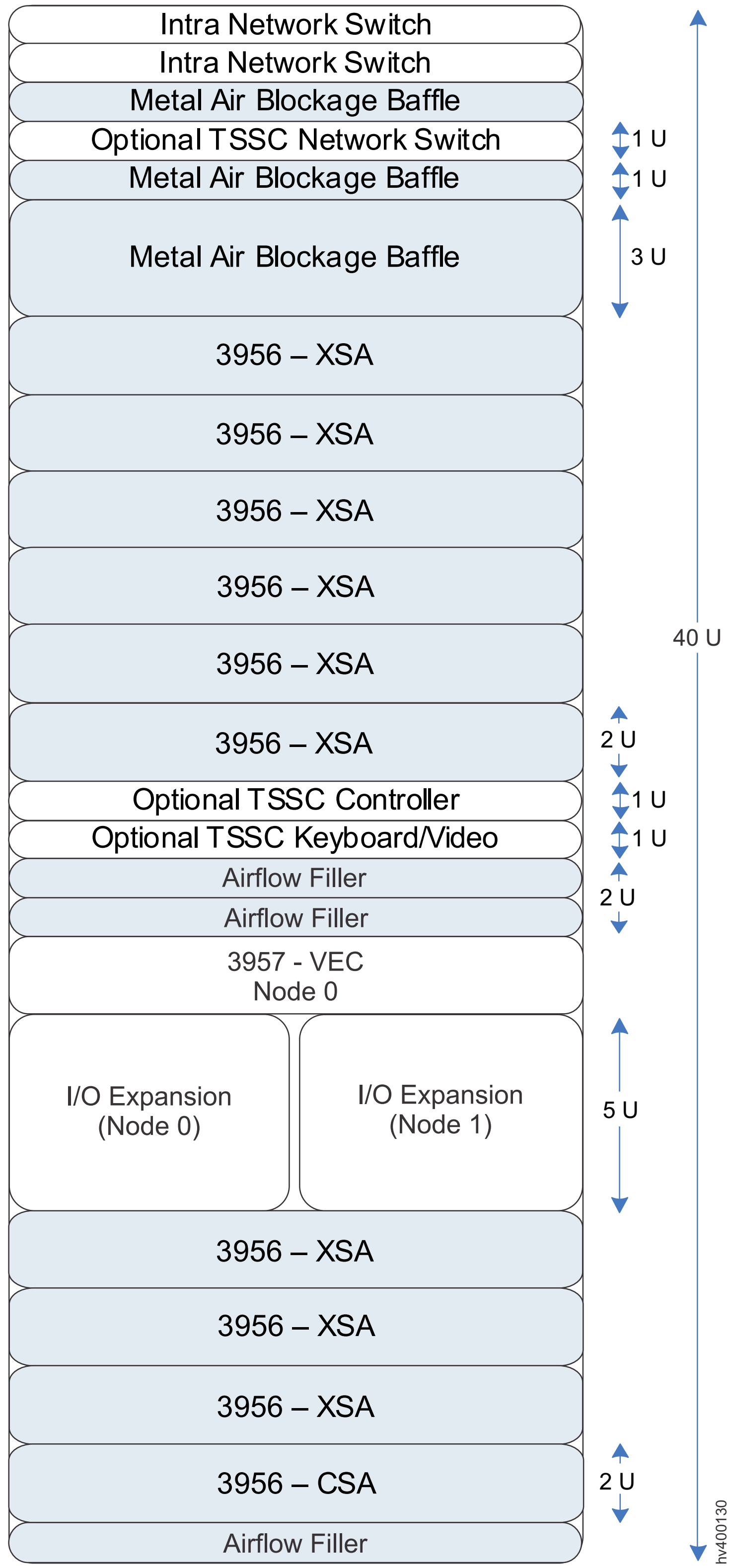


Figure 10. Single frame layout of a TS7760 with a manufacturing installed 3957-VEC, 3956-CSA, and 3956-XSA

Figure 11 on page 38 displays the frame layout for a TS7760 Storage Expansion Frame.

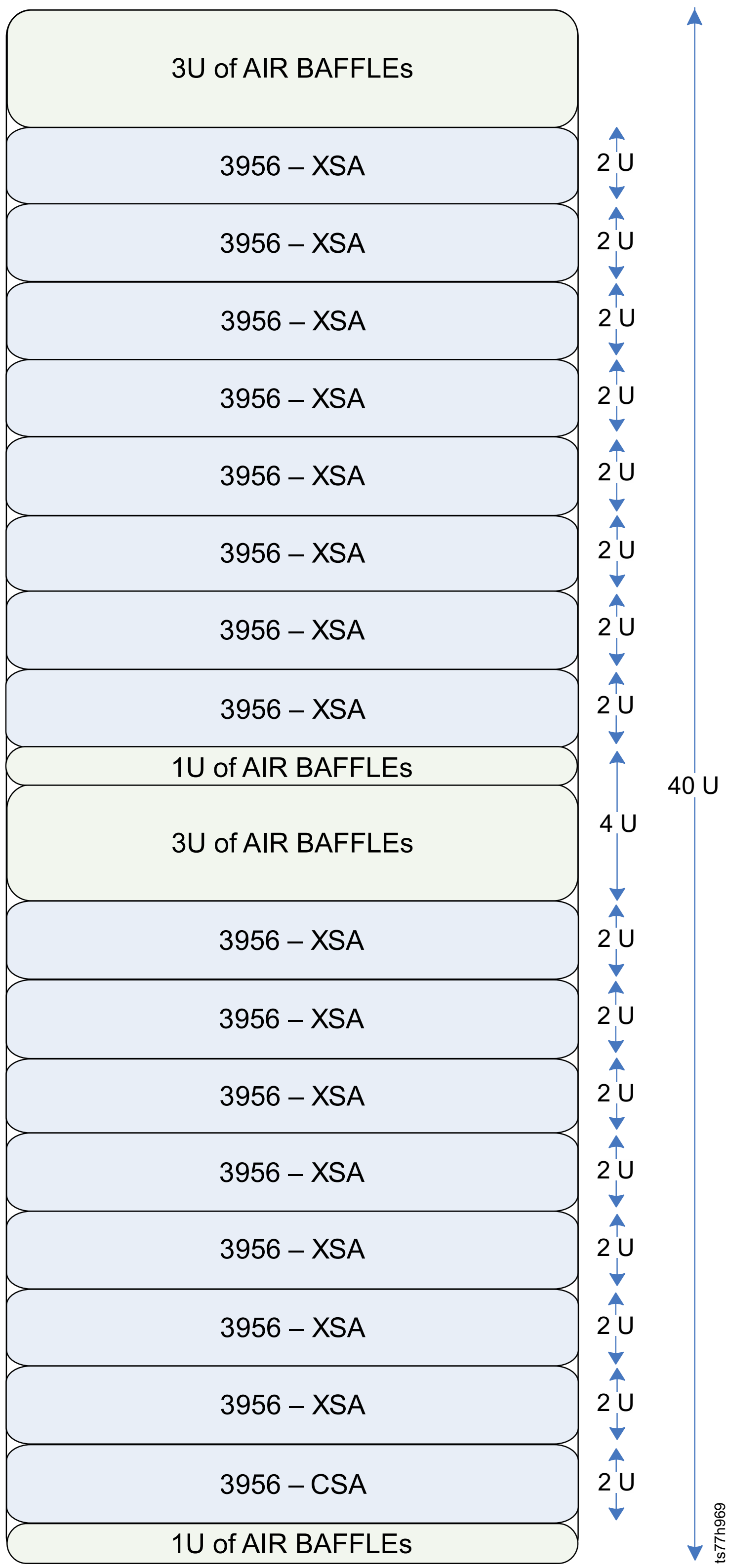


Figure 11. Layout of a TS7760 Storage Expansion Frame with 3956-CSA and 3956-XSA

Related information

"System requirements" on page 63

TS7760 Storage Expansion Frame

The TS7760 Storage Expansion Frame is a 3952 Tape Frame designated as a cache expansion frame for use with a fully configured TS7700 Base Frame.

The TS7760 Storage Expansion Frame enables expansion of the TS7760 Cache by attaching up to two more storage frames. Each frame contains one additional TS7760 Cache Controller, which can attach to a maximum of 15 additional TS7760 Cache Drawers, resulting in a maximum addition of 16 TS7760 Cache units within each TS7760 Storage Expansion Frame. A maximally configured TS7700 Base Frame with two attached and maximally configured TS7760 Storage Expansion Frames contains 42 total cache units.

A TS7760 Cache Controller and up to fifteen attached TS7760 Cache Drawers are referred to as a "string", with each TS7760 Cache Controller acting as the "head of [the] string". A single TS7700 can have up to three "strings" attached, the first in the base frame (base string) and the next two in the expansion frames (string 1 and string 2).

The distance between a TS7760 Storage Expansion Frame and the TS7700 Base Frame cannot exceed 10 meters. This distance permits connection of the frames by using a 30-meter cable.

Note: A TS7760 configured to use the TS7760 Storage Expansion Frame must operate at microcode level 8.40.0.xx or later.

The TS7760 Storage Expansion Frame consists of the following components::

- One 3952 Tape Frame
- One TS7760 Cache Controller (3956-CSA), containing 12 DDMs, each of which have a storage capacity of 4 TB or 8 TB
- Optional attachment to up to 15 TS7760 Cache Drawers (3956-XSA), each containing 12 DDMs with a storage capacity of 4 TB or optional attachment to up to 14 TS7760 Cache Drawers (3956-XSA), each containing 12 DDMs with a storage capacity of 8 TB

  Note: Mixing 4 TB and 8 TB DDMs together in a single TS7760 Cache Drawer (3956-XSA) is not supported.

Related information

"Feature details" on page 149
"System requirements" on page 63
"Upgrades for the TS7760" on page 113

TS7760 Storage Expansion Frame Configurations with 4 TB DDMs:

The TS7760 Storage Expansion Frame can be composed of 4 TB disk drive modules.

TS7760 Storage Expansion Frame Configurations with 4 TB DDMs

The following table displays the total achievable capacity for a certain number of 3956-XSA drawers with 4 TB DDMs attached to a 3956-CSA Controller(s).

Table 13. TS7760 Storage Expansion Frame configurations for 4 TB capacity drives

TS7760 Cache configuration for base frame	Cache units‡ in eachTS7760 Storage Expansion Frame cache controller (3956-CSA) plus optional cache drawers (3956-XSA)	First TS7760 Storage Expansion Frame		Second TS7760 Storage Expansion Frame	
		Total cache units (including TS7760 Base Frame)	Available capacity	Total cache units (including TS7760 Base Frame)	Available capacity
1 TS7760 Cache Controller (3956-CSA) 9 TS7760 Cache Drawers (3956-XSA)	1 (controller only)	11	345.07 TB (313.84 TiB)	27	847.60 TB (770.88 TiB)
	2	12	376.49 TB (342.42 TiB)	28	879.03 TB (799.47 TiB)
	3	13	407.92 TB (371 TiB)	29	910.45 TB (828.05 TiB)
	4	14	439.35 TB (399.59 TiB)	30	941.88 TB (856.64 TiB)
	5	15	470.78 TB (428.17 TiB)	31	973.31 TB (885.22 TiB)
	6	16	502.21 TB (456.76 TiB)	32	1004.74 TB (913.80 TiB)
	7	17	533.64 TB (485.34 TiB)	33	1036.17 TB (942.39 TiB)
	8	18	565.06 TB (513.92 TiB)	34	1067.60 TB (970.97 TiB)
	9	19	596.49 TB (542.51 TiB)	35	1099.02 TB (999.56 TiB)
	10	20	627.92 TB (571.09 TiB)	36	1130.45 TB (1028.14 TiB)
	11	21	659.35 TB (599.67 TiB)	37	1161.88 TB (1056.72 TiB)
	12	22	690.78 TB (628.26 TiB)	38	1193.31 TB (1085.31 TiB)
	13	23	722.21 TB (656.84 TiB)	39	1224.74 TB (1113.89 TiB)
	14	24	753.63 TB (685.43 TiB)	40	1256.17 TB (1142.48 TiB)
	15	25	785.06 TB (714.01 TiB)	41	1287.59 TB (1171.06 TiB)
	16	26	816.49 TB (742.59 TiB)	42	1319.02 TB (1199.64 TiB)
‡The term "Total cache units" refers to the combination of cache controllers and cache drawers.					

A new TS7760 Storage Expansion Frame can be added to a TS7760 Base Frame fully configured with a 3956-CSA cache controller and nine 3956-XSA cache drawers by using “FC 7334, TS7700 Encryption-capable expansion frame” on page 175 as a miscellaneous equipment specification (MES).

Note: A TS7700 Base Frame that contains 3956-CS8 or 3956-CS9 cache controllers but is not fully configured can add a TS7760 Storage Expansion Frame containing a 3956-CSA cache controller and up to 15 3956-XSA cache drawers.
Refer to the topic *Upgrades specific to the TS7760* in the **Related information** section for MES details and requirements.

Related information

“Feature details” on page 149

“System requirements” on page 63

"Upgrades for the TS7760" on page 113

TS7760 Storage Expansion Frame Configurations with 8 TB DDMs:

The TS7760 Storage Expansion Frame can be composed of 8 TB disk drive modules.

TS7760 Storage Expansion Frame Configurations with 8 TB DDMs

The following table displays the total achievable capacity for a certain number of 3956-XSA drawers with 8 TB DDMs attached to a 3956-CSA Controller(s).

Table 14. TS7760 Storage Expansion Frame configurations for 8 TB capacity drives

TS7760 Cache configuration for base frame	Cache units‡ in eachTS7760 Storage Expansion Frame cache controller (3956-CSA) plus optional cache drawers (3956-XSA)	First TS7760 Storage Expansion Frame		Second TS7760 Storage Expansion Frame	
		Total cache units (including TS7760 Base Frame)	Available capacity	Total cache units (including TS7760 Base Frame)	Available capacity
1 TS7760 Cache Controller (3956-CSA) 9 TS7760 Cache Drawers (3956-XSA)	1 (controller only)	11	679.67 TB (618.16 TiB)	26	1606.99 TB (1461.55 TiB)
	2	12	741.51 TB (674.40 TiB)	27	1668.83 TB (1517.80 TiB)
	3	13	803.35 TB (730.64 TiB)	28	1730.68 TB (1574.04 TiB)
	4	14	865.19 TB (786.89 TiB)	29	1792.52 TB (1630.28 TiB)
	5	15	927.03 TB (843.13 TiB)	30	1854.36 TB (1686.53 TiB)
	6	16	988.87 TB (899.38 TiB)	31	1916.20 TB (1742.77 TiB)
	7	17	1050.72 TB (955.62 TiB)	32	1978.04 TB (1799.02 TiB)
	8	18	1112.56 TB (1011.86 TiB)	33	2039.88 TB (1855.26 TiB)
	9	19	1174.40 TB (1068.11 TiB)	34	2101.72 TB (1911.50 TiB)
	10	20	1236.24 TB (1124.35 TiB)	35	2163.56 TB (1967.75 TiB)
	11	21	1298.08 TB (1180.60 TiB)	36	2225.40 TB (2023.99 TiB)
	12	22	1359.92 TB (1236.84 TiB)	37	2287.24 TB (2080.24 TiB)
	13	23	1421.76 TB (1293.08 TiB)	38	2349.08 TB (2136.48 TiB)
	14	24	1483.60 TB (1349.33 TiB)	39	2410.93 TB (2192.72 TiB)
	15	25	1545.44 TB (1405.57 TiB)	40	2472.77 TB (2248.97 TiB)
‡The term "Total cache units" refers to the combination of cache controllers and cache drawers.					

A new TS7760 Storage Expansion Frame can be added to a TS7760 Base Frame fully configured with a 3956-CSA cache controller and nine 3956-XSA cache drawers by using "FC 7334, TS7700 Encryption-capable expansion frame" on page 175 as a miscellaneous equipment specification (MES).

Note: A TS7700 Base Frame that contains 3956-CS7 or 3956-CS8 or cache controllers but is not fully configured can add a TS7760 Storage Expansion Frame containing a 3956-CSA cache controller and up to 14 3956-XSA cache drawers. Any CS9 base frames should be fully populated first prior to adding a CSA expansion frame.
Refer to the topic *Upgrades specific to the TS7760* in the **Related information** section for MES details and requirements.

Related information

"Feature details" on page 149

"System requirements" on page 63

"Upgrades for the TS7760" on page 113

TS7760 Cache Controller

The TS7760 Cache Controller is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

The TS7760 Cache Controller provides dynamic disk pools-protected virtual volume disk storage for fast retrieval of data from cache. The TS7760 Cache Controller offers the following features:

- Two Fibre Channel processor cards
- CPU microprocessor
- Two battery backup units (one for each processor card)
- Two AC power supplies with imbedded enclosure cooling units
- 12 DDMs, each with a storage capacity of 4 TB (3.63 TiB) or 8 TB (7.27 TiB)
- Supports Advanced Encryption Standard (AES) 256-bit encryption
- Optional attachment to a maximum of nine TS7760 Cache Drawers in a TS7760 Base Frame
- Optional expansion of cache capabilities (up to 16 additional Cache Drawers with 4TB DDMs, or up to 15 additional Cache Drawers if using 8TB DDMs) when a fully populated TS7760 Base Frame attaches to a fully populated TS7760 Storage Expansion Frame
- 12 Gb SAS port
- Dual active 16 Gb Fibre Channel connectivity to host (TS7700)

Figure 12. TS7760 Cache Controller 3956-CSA (front view)

Figure 13. TS7760 Cache Controller 3956-CSA (rear view)

†Refer to the topic *Trademarks* in the **Related information** section for complete attribution.

Related information

"System requirements" on page 63

"TS7760 Storage Expansion Frame" on page 39

TS7760 Cache Drawer

The TS7760 Cache Drawer is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

The TS7760 Cache Drawer expands the capacity of the TS7760 Cache Controller by providing additional dynamic disk pools-protected disk storage. Each TS7760 Cache Drawer offers the following features:

- Two ESM cards
- Two AC power supplies with imbedded enclosure cooling units
- 12 DDMs, each with a storage capacity of 4 TB (3.63 TiB) or 8 TB (7.27 TiB)
- Supports Advanced Encryption Standard (AES) 256-bit encryption
- Attachment to the TS7760 Cache Controller

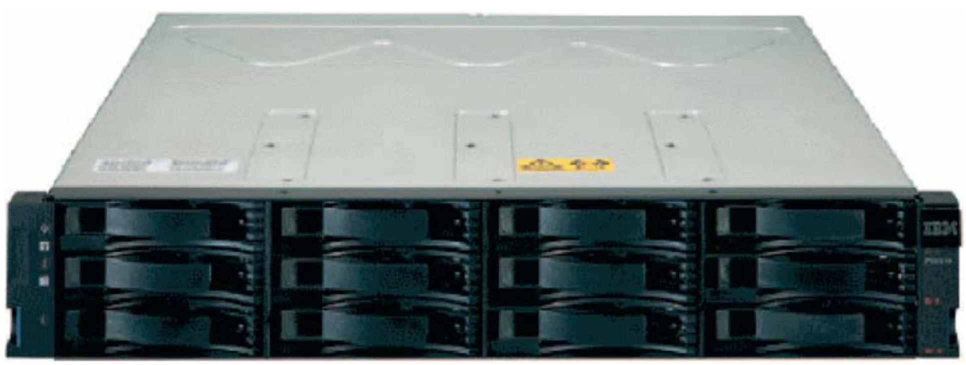


Figure 14. TS7760 Cache Drawer 3956-XSA (front view)

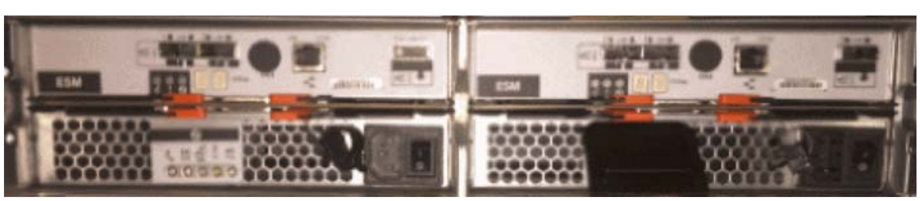


Figure 15. TS7760 Cache Drawer 3956-XSA (rear view)

Related information

"System requirements" on page 63

IBM TS7720 details

This section provides topics for the IBM TS7720 components.

Figure 16 displays the frame layout for a manufacturing installed TS7720 .

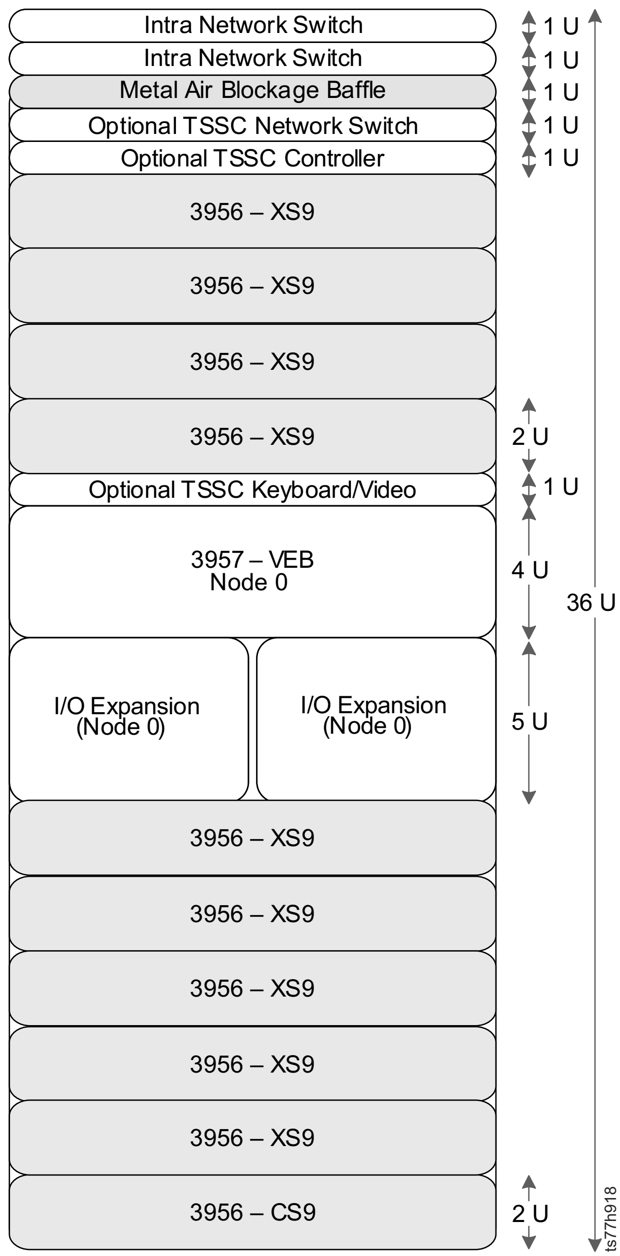


Figure 16. Single frame layout of a TS7720 with manufacturing installed 3957-VEB, 3956-CS9, and 3956-XS9

Figure 17 on page 45 displays the frame layout for a TS7720 Storage Expansion Frame.

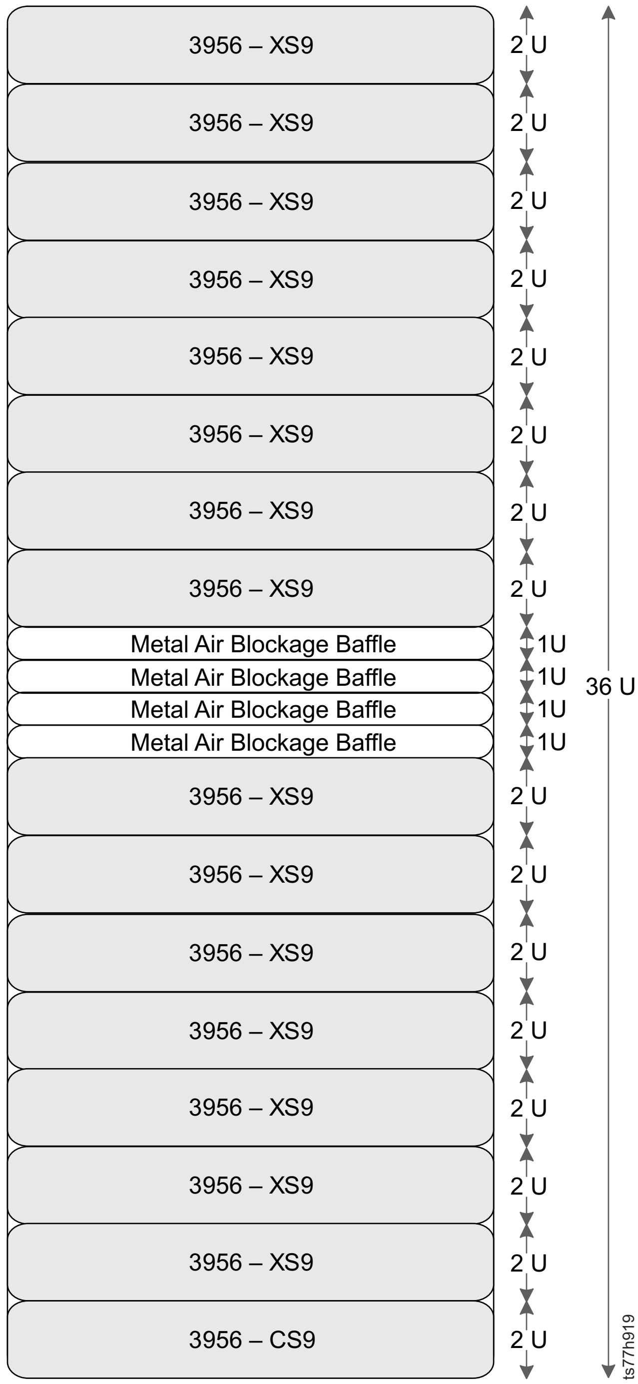


Figure 17. Layout of a TS7720 Storage Expansion Frame with 3956-CS9, and 3956-XS9.

Related information

"System requirements" on page 63

TS7720 Storage Expansion Frame

The TS7720 Storage Expansion Frame is a 3952 Tape Frame designated as a cache expansion frame for use with a fully configured TS7720 Base Frame.

The TS7720 Storage Expansion Frame enables expansion of the TS7720 Cache by attaching up to two more storage frames. Each frame contains one additional TS7720 Cache Controller, which can attach to a maximum of 15 additional TS7720

Cache Drawers, resulting in a maximum addition of 16 TS7720 Cache units within each TS7720 Storage Expansion Frame. A maximally configured TS7720 Base Frame with two attached and maximally configured TS7720 Storage Expansion Frames contains 42 total cache units.

A TS7720 Cache Controller and its attached TS7720 Cache Drawers are referred to as a "string", with each TS7720 Cache Controller acting as the "head of [the] string".

The distance between a TS7720 Storage Expansion Frame and the TS7720 Base Frame cannot exceed 10 meters, as per the prerequisites for “FC 7323, TS7720 Storage expansion frame” on page 174. This distance permits connection of the frames by using a 30-meter cable.

Note: A TS7720 configured to use the TS7720 Storage Expansion Frame must operate at microcode level 8.7.0.xx or later.

The TS7720 Storage Expansion Frame consists of the following components::
- One 3952 Tape Frame
- One TS7720 Cache Controller (3956-CS9), containing 12 DDMs, each of which have a storage capacity of 3 TB
- Optional attachment to up to 15 TS7720 Cache Drawers (3956-XS9), each containing 12 DDMs with a storage capacity of 3 TB

Table 15. TS7720 Storage Expansion Frame configurations

TS7720 Cache configuration for base frame	Cache units‡ in eachTS7720 Storage Expansion Frame cache controller (3956-CS9) plus optional cache drawers (3956-XS9)	First TS7720 Storage Expansion Frame		Second TS7720 Storage Expansion Frame	
		Total cache units (including TS7720 Base Frame)	Available capacity	Total cache units (including TS7720 Base Frame)	Available capacity
1 TS7720 Cache Controller (3956-CS9) 9 TS7720 Cache Drawers (3956-XS9)	1 (controller only)	11	263.86 TB (239.98 TiB)	27	647.86 TB (589.23 TiB)
	2	12	287.86 TB (261.81 TiB)	28	671.86 TB (611.06 TiB)
	3	13	311.86 TB (283.64 TiB)	29	695.86 TB (632.88 TiB)
	4	14	335.86 TB (305.46 TiB)	30	719.86 TB (654.71 TiB)
	5	15	359.86 TB (327.29 TiB)	31	743.86 TB (676.54 TiB)
	6	16	383.86 TB (349.12 TiB)	32	767.86 TB (698.37 TiB)
	7	17	407.86 TB (370.95 TiB)	33	791.86 TB (720.20 TiB)
	8	18	431.86 TB (392.78 TiB)	34	815.86 TB (742.02 TiB)
	9	19	455.86 TB (414.60 TiB)	35	839.86 TB (763.85 TiB)
	10	20	479.86 TB (436.43 TiB)	36	863.86 TB (785.68 TiB)
	11	21	503.86 TB (458.26 TiB)	37	887.86 TB (807.51 TiB)
	12	22	527.86 TB (480.09 TiB)	38	911.86 TB (829.34 TiB)
	13	23	551.86 TB (501.92 TiB)	39	935.86 TB (851.16 TiB)
	14	24	575.86 TB (523.74 TiB)	40	959.86 TB (872.99 TiB)
	15	25	599.86 TB (545.57 TiB)	41	983.86 TB (894.82 TiB)
	16	26	623.86 TB (567.40 TiB)	42	1007.86 TB (916.65 TiB)
‡The term "Total cache units" refers to the combination of cache controllers and cache drawers.					

A new TS7720 Storage Expansion Frame can be added to a TS7720 Base Frame fully configured with a 3956-CS9 cache controller and nine 3956-XS9 cache drawers by using “FC 7332, TS7720 Encryption-capable expansion frame” on page 174 as a miscellaneous equipment specification (MES).

Note: A TS7720 Base Frame that contains 3956-CS7 or 3956-CS8 cache controllers but is not fully configured can add a TS7720 Storage Expansion Frame containing a 3956-CS9 cache controller and up to 15 3956-XS9 cache drawers.
Refer to the topic *Upgrades specific to the TS7720* in the **Related information** section for MES details and requirements.

Related information

"Feature details" on page 149

"System requirements" on page 63

"Upgrades for the TS7720 " on page 116

TS7720 Cache Controller

The TS7720 Cache Controller is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

The TS7720 Cache Controller provides RAID-protected virtual volume disk storage for fast retrieval of data from cache. The TS7720 Cache Controller offers the following features:

- Two Fibre Channel processor cards
- Intel† xScale 667 MHz or custom ASIC microprocessor
- Two battery backup units (one for each processor card)
- Two AC power supplies with imbedded enclosure cooling units
- 12 DDMs, each with a storage capacity of 3 TB (2.73 TiB)
- Supports Advanced Encryption Standard (AES) 256-bit encryption
- Optional attachment to a maximum of nine TS7720 Cache Drawers in a TS7720 Base Frame
- Optional expansion of cache capabilities (up to 15 additional TS7720 Cache Drawers) when a fully populated TS7720 Base Frame attaches to a fully populated TS7720 Storage Expansion Frame

Figure 18. TS7720 Cache Controller 3956-CS9 (front view)

Figure 19. TS7720 Cache Controller 3956-CS9 (rear view)

†Refer to the topic *Trademarks* in the **Related information** section for complete attribution.

Related information

"System requirements" on page 63

"TS7720 Storage Expansion Frame" on page 45

TS7720 Cache Drawer

The TS7720 Cache Drawer is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

The TS7720 Cache Drawer expands the capacity of the TS7720 Cache Controller by providing additional RAID-protected disk storage. Each TS7720 Cache Drawer offers the following features:

- Two Fibre Channel processor cards
- Two AC power supplies with imbedded enclosure cooling units
- 11 DDMs, each with a storage capacity of 3 TB (2.73 TiB)
- Supports Advanced Encryption Standard (AES) 256-bit encryption
- Attachment to the TS7720 Cache Controller

Figure 20. TS7720 Cache Drawer 3956-XS9 (front view)

Figure 21. TS7720 Cache Drawer 3956-XS9 (rear view)

Related information

"System requirements" on page 63

IBM TS7740 details

This section provides topics for the IBM TS7740 components.

Figure 22 on page 50 displays the frame layout for a manufacturing installed TS7740.

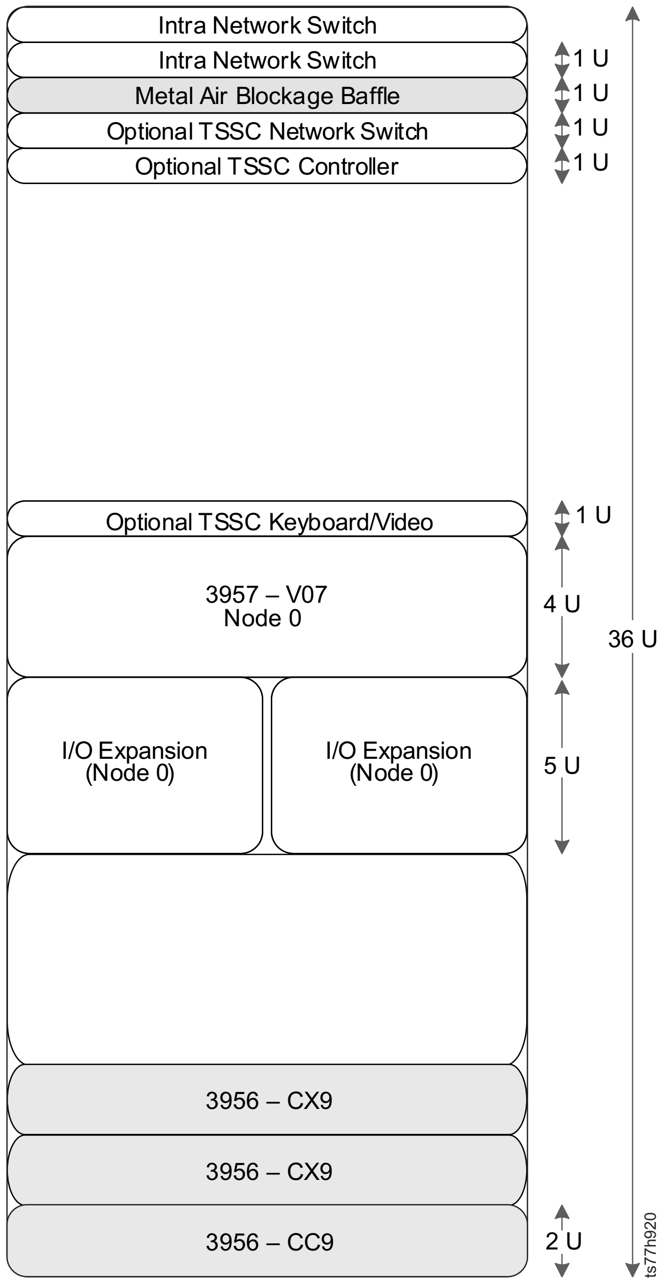


Figure 22. Single frame layout of a TS7740 with a manufacturing installed 3957-V07, 3956-CC9, and 3956-CX9

Related information

"System requirements" on page 63

TS7740 Cache Controller

The TS7740 Cache Controller is a self-contained 2U enclosure that mounts in a 3952 Tape Frame.

The TS7740 Cache Controller provides RAID-protected virtual volume disk storage to temporarily hold data from the host before writing to physical tape, then caches the data to allow fast retrieval from the disk. The TS7740 Cache Controller offers the following features:

- Two Fibre Channel processor cards

- PowerPC® 750GX 1 GHz processor
- Two battery backup units (one for each processor card)
- Two AC power supplies with imbedded enclosure cooling units
- 22 DDMs, each with a storage capacity of 600 GB (558.79 GiB)
- Optional attachment to a maximum of two TS7740 Cache Drawers.


ts77h929

Figure 23. TS7740 Cache Controller 3956-CC9 (front view)


ts77h928

Figure 24. TS7740 Cache Controller 3956-CC9 (rear view)

Related information

"System requirements" on page 63

TS7740 Cache Drawer

The TS7740 Cache Drawer is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

The TS7740 Cache Drawer expands the capacity of the TS7740 Cache Controller by providing additional RAID-protected disk storage. Each TS7740 Cache Drawer offers the following features:

- Two Fibre Channel processor cards
- Two AC power supplies with imbedded enclosure cooling units
- 22 DDMs, each with a storage capacity of 600 GB (558.79 GiB)
- Attachment to the TS7740 Cache Controller

ts77h929

Figure 25. TS7740 Cache Drawer 3956-CX9 (front view)

ts77h928

Figure 26. TS7740 Cache Drawer 3956-CX9 (rear view)

Related information

"System requirements" on page 63

Tape library attachments, drives, and media

A TS7700 system can be used with a tape library attached to a host system.

The TS7740, TS7720 Tape Attach, and the TS7760 Tape Attach store data on physical tape in the TS3500 Tape Library or the TS4500 Tape Library.

Related information

"TS7700 Grid" on page 257

"TS3500/TS4500 Tape Library attachment"

TS3500/TS4500 Tape Library attachment

A TS7740, TS7720 Tape Attach, or a TS7760 Tape Attach attached to a TS3500 or TS4500 Tape Library interfaces directly with tape drives in the library.

When attached to a TS3500 or TS4500 Tape Library, the TS7700 can attach only to 3592 Tape Drives. Up to 16 3592 Tape Drives can be attached.

Communication, control, and data signals travel along Fibre Channel connections between the TS7700 and tape drives contained in the TS3500 or TS4500 Tape Library. A pair of Fibre Channel switches routes the data to and from the correct tape drive.

Notes:

1. FC 0203, 50-micron LC/LC 31-meter provides a 50 micron, 31 m fiber cable for connection between the fiber switch and the host.

The distance between a TS3500 or TS4500 Tape Library that is attached to a TS7700 should not exceed 30 m (98.43 ft.). Although the length of Fibre Channel cables that are provided by "FC 0203, 50-micron LC/LC 31-meter" on page 150 is 31 m (101.71 ft.), the remaining 1 m (3.28 ft.) length is required to complete attachments within the frames.

To ensure correct operation of 3592 Tape Drives in a TS3500 or TS4500 Tape Library that is attached to the TS7700, you must:

- Designate four 3592 Tape Drives as control paths by using the tape library management GUI.
- If using a **8 Gb Fibre Channel switch**, verify that the ports for the 3592 Tape Drives are set up as Auto (L), not Auto (N).
- If using a **16 Gb Fibre Channel switch**, verify that the ports for the 3592 Tape Drives are set up as Auto (N), not Auto (L).

Related information

FC 0203, 50-micron LC/LC 31-meter

FC 9217, Attach to 3953 LM

Tape drives

The TS7700 supports 3592 Tape Drives.

Related information

"3592 Tape Drives"

"Secure Data Erasure" on page 57

"Tape encryption" on page 120

FC 9900, Encryption configuration

3592 Tape Drives:

This section describes the 3592 Tape Drives associated with the TS7740, TS7720 Tape Attach, and TS7760 Tape Attach.

The 3592 Tape Drives supported for use with the TS7740, TS7720 Tape Attach, and TS7760 Tape Attach include:

- TS1150 Tape Drive
- TS1140 Tape Drive
- TS1130 Tape Drives
- TS1120 Tape Drives (in native mode and emulating 3592 J1A Tape Drives)
- 3592 J1A Tape Drives

Features include:

- Dual-ported 4 Gbps Fibre Channel switch attachments for TS1130, TS1120, and 3592 J1A Tape Drives
- Dual-ported 8 Gbps Fibre Channel switch attachments for TS1140 Tape Drives
- Dual-ported 16 Gbps Fibre Channel switch attachments for TS1150 Tape Drives
- High reliability and availability
- Small form factor
- Redundant power supplies
- Dynamic digital speed matching
- Individual read/write data channel calibration
- Increased search speed
- Streaming Lossless Data Compression (SLDC) algorithm

Figure 27 illustrates the 3592 Tape Drive.

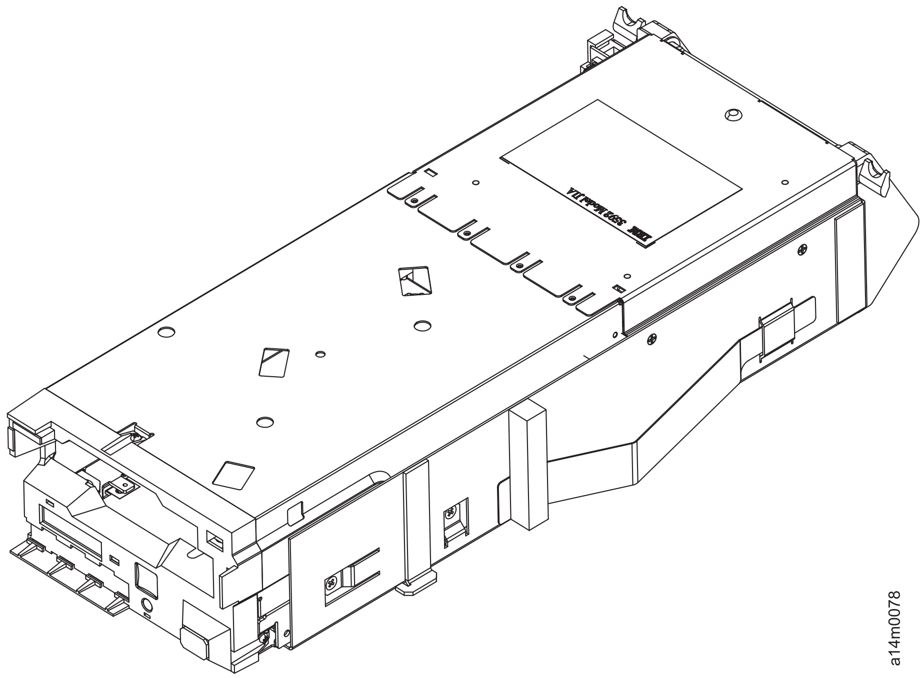


Figure 27. 3592 Tape Drive

Table 16 displays characteristics of the supported drive models. For comparison of standard features of the 3592 Tape Drives, see *IBM 3592 Tape Drive and TS1120 Controller Introduction and Planning Guide (3592 Models J1A, E05, E06, EU6, E07, E08, and J70, C06, C07 Controllers)*, GA32-0555-07, available at the *IBM Support & Downloads* link in the **Related information** section.

Table 16. Comparison of 3592 Tape Drives supported by the TS7740, TS7720 Tape Attach, or TS7760 Tape Attach

3592 Tape Drive type	Supported media types	Encryption support	Capacity	Data rate
TS1150 Tape Drive (3592 E08 or EH8 Tape Drive)	JC JD JK JL	Yes (TKLM or ISKLM only)	7.0 TB 10.0 TB 900 GB 2 TB	360 MB/s
TS1140 Tape Drive (3592 E07 or EH7 Tape Drive)	JB JC JK Media read only: JA JJ	Yes (TKLM or ISKLM only)	1.6 TB (JB native) 4.0 TB (JC native) 500 GB (JK native) 4.0 TB (maximum all)	250 MB/s
TS1130 Tape Drive (3592 EU6 or 3592 E06 Tape Drive)	JA JB JJ	Yes	640 GB (JA native) 1.0 TB (JB native) 128 GB (JJ native) 1.0 TB (maximum all)	160 MB/s
TS1120 Tape Drive (3592 E05 Tape Drive)	JA JB JJ	Yes	500 GB (JA native) 700 GB (JB native) 100 GB (JJ native) 700 GB (maximum all)	100 MB/s

Table 16. Comparison of 3592 Tape Drives supported by the TS7740, TS7720 Tape Attach, or TS7760 Tape Attach (continued)

3592 Tape Drive type	Supported media types	Encryption support	Capacity	Data rate
3592 J1A	JA JJ	No	300 GB (JA native) 60 GB (JJ native) 300 GB (maximum all)	40 MB/s

Notes:

1. To use encryption, all drives that are associated with the TS7740, TS7720 Tape Attach, or TS7760 Tape Attach must be encryption-capable and -enabled.
2. Encryption is not supported on 3592 J1A tape drives.

Restrictions for use with TS1140 Tape Drives

Note: Throughout this section, the term TS7700 refers to either the TS7740, the TS7720 Tape Attach, or the TS7760 Tape Attach.

TS1140 Tape Drives are supported in new TS7700 orders from manufacturing, and with existing TS7700s attached to a library. The following additional media restrictions apply when a library attached to a TS7740, TS7720 Tape Attach, or TS7760 Tape Attach contains TS1140 Tape Drives:

- JA and JJ media are supported for read-only operations. If JA or JJ media exist or are installed in a library that contains TS1140 Tape Drives, then:
  - Online processing succeeds but all JA and JJ media is marked read-only for reclamation

    Note: One main purpose of reclamation is to increase the number of available physical scratch volumes in the pool. When TS1140 Tape Drives are installed, JJ and JA media reclamation reduces, instead of increases, the number of available scratch volumes. Reclamation of a JA or JJ cartridge does not occur if the TS7700 is in a low scratch state (fewer than 15 available scratch volumes) for the pool. For example, if borrowing is enabled and there are JA physical volumes to be reclaimed in pool 1, the sum of available scratch tapes in pool 1 and the common scratch pool 0 must be greater than 15 for reclamation of the JA physical volumes to occur. If the system contains TS1140 or TS1150 tape drives, the system requires at least 15 scratch physical volumes to run reclamation for sunset media.
  - JA and JJ media can be ejected by using the TS7700 Management Interface once their active data is reclaimed onto newer media

  Note: JA and JJ media should not be inserted if the volumes do not exist in the TS7700 database.
- If JB media contains data that is written in E05 format, it is marked full and is supported as READ-ONLY data. Once the data is reclaimed or written in E06 or E07 format, it is supported for READ-WRITE operations. The IBM Encryption Key Manager is not supported for use with TS1140 Tape Drives. If encryption is used, either the Tivoli Key Lifecycle Manager (TKLM) or the IBM Security Key Lifecycle Manager (ISKLM) must be used.
- 3592 EU6 Tape Drives cannot be converted to TS1140 Tape Drives.

Restrictions for use with TS1150 Tape Drives (Homogeneous Configuration)

Note: Throughout this section, the term TS7700 refers to either the TS7740, the TS7720 Tape Attach, or the TS7760 Tape Attach.

TS1150 Tape Drives are supported in new TS7700 orders from manufacturing, and with existing TS7700s attached to a library. The following additional media restrictions apply when a library attached to a TS7740, TS7720 Tape Attach, or TS7760 Tape Attach contains TS1150 Tape Drives:

- JA, JJ, and JB media are not supported for read-only operations.
- The IBM Encryption Key Manager is not supported for use with 3592 E08 Tape Drive. If encryption is used, either the Tivoli Key Lifecycle Manager (TKLM) or the IBM Security Key Lifecycle Manager (ISKLM) must be used.
- TS1140 Tape Drives cannot be converted to TS1150 Tape Drives.

Restrictions for use with TS1150 Tape Drives (Heterogeneous Configuration)

Note: Throughout this section, the term TS7700 refers to either the TS7740, the TS7720 Tape Attach, or the TS7760 Tape Attach.

TS1150 Tape Drives are supported in new TS7700 orders from manufacturing, and with existing TS7700s attached to a library. The following additional media restrictions apply when a library attached to a TS7740, TS7720 Tape Attach, or TS7760 Tape Attach contains TS1150 Tape Drives:

- TS1150 Tape Drives can be intermixed with one other TS11xx drive type in a library attached to a TS7740, TS7720 Tape Attach, or TS7760 Tape Attach.
- JA, JJ, and JB media are supported for read-only operations. If JA, JJ, or JB media exist or are installed in a library that contains TS1150 Tape Drives, then:
  - Online processing succeeds but all JA, JJ, JB media is marked read-only for reclamation

    Note: One main purpose of reclamation is to increase the number of available physical scratch volumes in the pool. When TS1150 Tape Drives are installed, JJ, JA, and JB media reclamation reduces, instead of increases, the number of available scratch volumes. Reclamation of a JA, JJ, or JB cartridge does not occur if the TS7700 is in a low scratch state (fewer than 15 available scratch volumes) for the pool. For example, if borrowing is enabled and there are JA physical volumes to be reclaimed in pool 1, the sum of available scratch tapes in pool 1 and the common scratch pool 0 must be greater than 15 for reclamation of the JA physical volumes to occur. If the system contains TS1140 or TS1150 tape drives, the system requires at least 15 scratch physical volumes to run reclamation for sunset media.
  - JA, JJ, and JB media can be ejected by using the TS7700 Management Interface once their active data is reclaimed onto newer media

  Note: JA, JJ, and JB media should not be inserted if the volumes do not exist in the TS7700 database.
- The IBM Encryption Key Manager is not supported for use with TS1150 Tape Drive. If encryption is used, either the Tivoli Key Lifecycle Manager (TKLM) or the IBM Security Key Lifecycle Manager (ISKLM) must be used.
- TS1140 Tape Drives cannot be converted to TS1150 Tape Drives.

Native capacity of tape drives

The TS7700 uses the native capacity of 3592 Tape Drives with the following restrictions:

- Only a TS1120 Tape Drive can emulate a 3592 J1A Tape Drive. When the TS1120 Tape Drive is in 3592 J1A emulation mode, data is written in the 3592 J1A recording format. The TS7700 supports a mix of TS1120 Tape Drives in 3592 J1A emulation mode and 3592 J1A Tape Drives.
- The combination of encryption-capable and non-encryption-capable drives is not supported. Model 3592 J1A Tape Drives and TS1120 Tape Drives without hardware encryption modules are not encryption capable. All TS1120 Tape Drives with the hardware encryption modules, TS1130, TS1140, and TS1150 Tape Drives are encryption capable.
- When the TS7700 is online and tape drives are running in native E05 mode, 3592 J1A Tape Drives cannot be added to the configuration.
- When physical volumes are written in native E05 mode, the TS7700 can no longer operate in 3592 J1A emulation mode.

  Note: If the TS7700 is returned to 3592 J1A emulation mode after physical volumes are written in native E05 mode, the TS7700 cannot be returned to an online status.

TS1120 Tape Drives operate in native E05 mode or in 3592 J1A emulation mode. However, all 3592 Tape Drives associated with the TS7700 must be TS1120 Tape Drives in order for the TS1120 Tape Drives to operate in native E05 mode. To use TS1120 Tape Drives in native E05 mode, the drives must be set to E05 native mode. If you intend to use TS1120 Tape Drives in native E05 mode, the minimum microcode levels are 8.0.1.xx for the TS7700 and 534.2x for the Library Manager. Ask your IBM service representative to receive the most current levels of microcode.

Related information

"3592 Tape Cartridges" on page 58

http://www.ibm.com/support/us/en/

Secure Data Erasure:

The Secure Data Erasure function enables a secure data erasure reclamation policy for data stored on a 3592 Tape Drive.

The Secure Data Erasure function monitors the age of expired data on a physical volume. When the age exceeds the customer-set limit, Secure Data Erasure forces a reclaim and physical overwrite of the data on the volume.

Note: If the TS7700 system must be taken offline while data is being erased from a 3592 Tape Drive, the Secure Data Erasure function is automatically canceled during the offline process and resumes when the system is brought online.

Encryption and Secure Data Erasure

If a physical volume is encrypted, the TS7700 does not perform a physical overwrite of the data. Instead, the Encryption Key (EK) is shredded, or essential information is removed from the encrypted tape, rendering the encrypted data unrecoverable.

When compared to the normal, or long, erasure operation, EK shredding is a much faster procedure. Furthermore, normal erasure is always used for non-encrypted tapes, while EK shredding is the default used for encrypted tapes. However, the first time an encrypted tape is erased, a normal erasure is performed, followed by an EK shredding. The TS7700 can be configured to perform a normal erasure with every data operation, but this function must be configured by an IBM Service Representative.

Related information

"3592 Tape Cartridges"

"Tape encryption" on page 120

Tape media

This section describes the tape media associated with the TS7700.

3592 Tape Cartridges:

This section describes the tape cartridges that are used by 3592 Tape Drives in the TS3500 or TS4500 Tape Library.

Figure 28 shows the IBM TotalStorage 3592 Enterprise Tape Cartridge.

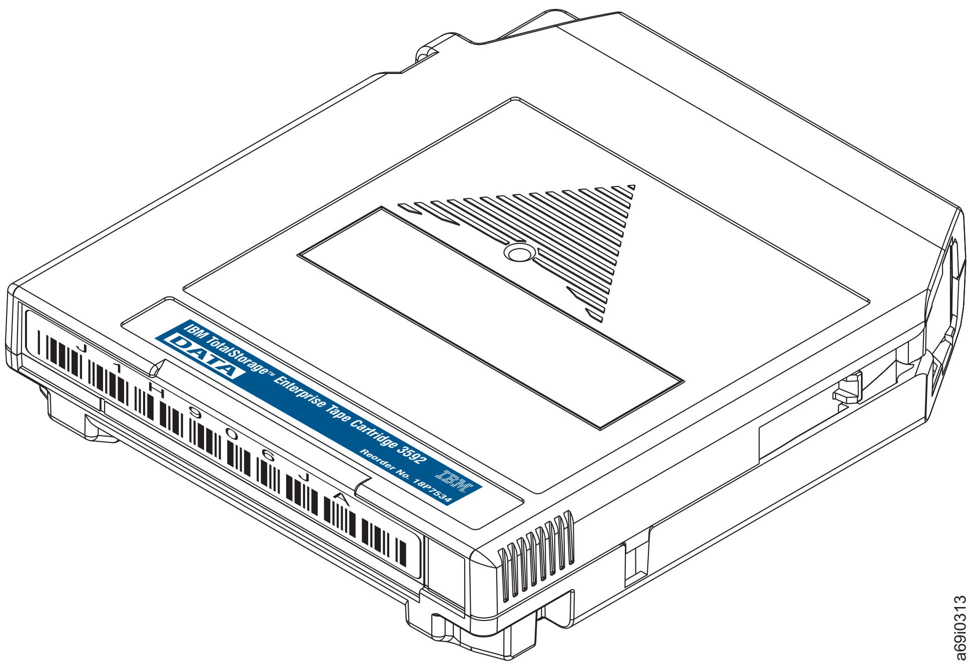


Figure 28. IBM 3592 Tape Cartridge

Tape cartridges can be distinguished by the text on the product label and by the color of the label. Table 17 on page 59 lists the characteristics of the 3592 Tape Cartridges.

Table 17. Supported IBM 3592 Tape Cartridges

Text on product label and type of media[1]	TS1150 Native Capacity	TS1140 Native Capacity	TS1130 Native Capacity	TS1120 Native Capacity	3592 J1A Native Capacity	Case color	Label, door, and write-protect switch color
Data, JA	Not supported	Read only support	640 GB (596.04 GiB) E06 format 500 GB (465.66 GiB) E05 format 300 GB (279.39 GiB) J1A format	500 GB (465.66 GiB) E05 format 300 GB (279.39 GiB) J1A format	300 GB (J1A format)	Black	Dark blue
Extended data, JB	Not supported	1600 GB (1490.12 GiB) E07 format 1000 GB (931.32 GiB) E06 format	1000 GB (931.32 GiB)	700 GB (651.93 GiB)	Not supported	Black	Dark green
Advanced data, JC	7000 GB (6519.2 GiB)	4000 GB (3725.2 GiB)	Not supported	Not supported	Not supported	Black	Dark purple
Advanced data, JD	10000 GB (9313.2 GiB)	Not supported	Not supported	Not supported	Not supported	Black	Terra-cotta
Economy, JJ	Not supported	Read only support	128 GB (119.21 GiB) E06 format 100 GB (93.13 GiB) E05 format 60 GB (58.88 GiB) J1A format	100 GB (93.13 GiB) E05 format 60 GB (58.88 GiB) J1A format	60 GB (58.88 GiB) J1A format	Black	Light blue
Advanced economy, JK	900 GB (838.19 GiB)	500 GB (465.66 GiB)	Not supported	Not supported	Not supported	Black	Light purple
Economy, JL	2000 GB (1862.64 GiB)	Not supported	Not supported	Not supported	Not supported	Black	Terra-cotta
Cleaning, CLNxxxJA[2]	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Black	Gray

Notes:

1. This designation appears as the last two characters on standard bar code labels. In addition, for cleaning cartridges, the first three characters of the volume serial (VOLSER) number are CLN.
2. Where xxx equals three numerals.

Media Types

The media type is the format of the data cartridge. The media type of a cartridge is shown by the last two characters on standard bar code labels. Supported media types include:

JA An Enterprise Tape Cartridge (ETC)

A JA cartridge can be used in native mode in a 3592 J1A drive or a 3592 E05 Tape Drive operating in either native mode or J1A emulation mode.

The native capacity of a JA tape cartridge that is used in a 3592 J1A drive or a 3592 E05 Tape Drive in J1A emulation mode is 300 GB (279.39 GiB). The native capacity of a JA tape cartridge that is used in a 3592 E05 Tape Drive drive in native mode is 500 GB (465.6 GiB).

This media type is only supported for read-only use with TS1140 Tape Drives.

JB An Enterprise Extended-Length Tape Cartridge (ETCL)

Use of JB tape cartridges is supported only with TS1140 Tape Drives, TS1130 Tape Drives and TS1120 Tape Drives operating in native capacity mode.

When used with TS1140 Tape Drives, JB media that contains data that is written in native E05 mode is only supported for READ-ONLY operations. Once this data is reclaimed or written in E06 or E07 format, it is supported for READ-WRITE operations.

TS1120 Tape Drives operate in native E05 mode or in 3592 J1A emulation mode. However, all 3592 Tape Drives associated with the TS7700 must be TS1120 Tape Drives in order for 3592 E05 Tape Drives to operate in native E05 mode. To use 3592 E05 Tape Drives in native E05 mode, the drives must be set to E05 native mode. If you intend to use TS1120 Tape Drives in native E05 Mode, the minimum microcode levels are 8.0.1.xx for the TS7700 and 534.2x for the Library Manager. Ask your IBM service representative to receive the most current levels of TS7700 and Library Manager code.

JC An Enterprise Advanced Data Cartridge (EADC)

This media type is only supported for use with TS1140 Tape Drives and TS1150 Tape Drives.

JD An Enterprise Advanced Data Cartridge (EADC)

This media type is only supported for use with TS1150 Tape Drives.

JJ An Enterprise Economy Tape Cartridge (EETC)

A JJ cartridge can be used in native mode in a 3592 J1A drive or a 3592 E05 Tape Drive operating in either native mode or J1A emulation mode.

The native capacity of a JJ tape cartridge that are used in a 3592 J1A drive or 3592 E05 Tape Drive in J1A emulation mode is 60 GB (58.88 GiB). The native capacity of a JJ tape cartridge that are used in a 3592 E05 Tape Drive in native mode is 100 GB (93.13 GiB).

This media type is only supported for read-only use with TS1140 Tape Drives.

JK An Enterprise Advanced Economy Tape Cartridge (EAETC)

This media type is only supported for use with TS1140 Tape Drives and TS1150 Tape Drives.

JL An Enterprise Advanced Economy Tape Cartridge (EAETC)

This media type is only supported for use with TS1150 Tape Drives.

Diagnostic and cleaning cartridges

CE
Customer Engineer (CE) diagnostic cartridge for use only by IBM service representatives. The VOLSER for this cartridge is `CE xxxJA`, where a space occurs immediately after `CE` and `xxx` equals three numerals.

CLN
Cleaning cartridge. The VOLSER for this cartridge is `CLN xxxJA`, where a space occurs immediately after `CLN` and `xxx` equals three numerals.

Note: When 3592 J1A drives (or 3592 E05 Tape Drives in J1A emulation) are replaced with 3592 E06 Tape Drives, the TS7700 marks the J1A-formatted tapes with active data FULL. By marking these tapes full, the TS7700 does not append more data since the 3592 E06 Tape Drive cannot append data to a J1A-formatted tape. As the active data on the J1A gets reclaimed or expired, the tape goes back to the scratch pool and then eventually gets reformatted to the E06 data format.

Workload considerations

This topic highlights some of the considerations to bear in mind when you decide what workload to place in the TS7700.

Like previous generations of VTS products, the TS7700 presents 3490 Tape Drive images. Any data that can reside on a 3480/3490/3590/3592, prior generations of VTS systems, or cartridges from other vendors can reside on the TS7700. However, processing characteristics of workloads differ, so some data are more suited for the TS7700 than other data.

Throughput

Because the TS7700 has a finite bandwidth capability, as has any other device that is attached to a host system, plan for workloads that fit its capabilities.However, since the TS7700 possesses 8 Gb FICON channels and either Tape Volume Cache or TS7700 Cache, few workloads would not be suitable based on throughput.

Drive concurrency

The TS7700 cluster appears to the host operating system as up to 496 3490E drives. If you have periods of time during the day when your tape processing jobs are limited by drive availability, the TS7700 can help your processing considerably. The design of the TS7700 cluster allows transparent access to multiple virtual volumes on the same stacked physical volume because access to the virtual volumes is solely through the TS7700 Cache. If you need access to more than one virtual volume on a physical volume, it is provided without requiring any user involvement, unlike some alternatives such as stacking by using job control language (JCL).

Cartridge capacity utilization

One of the key benefits of the TS7700 is its ability to fully use the capacity of the 3592 Tape Cartridges independent of the data set sizes that are written. Another is the ability to manage that capacity effectively without host or user involvement. A virtual volume can contain up to 6.29 GB of data (18.87 GB assuming data compressibility of 3:1) using the extended virtual volume sizes.

The actual size of a virtual volume is only the amount of data that is written by the host. If an application writes 20 MBs to a 4 GB volume, only the 20 MB is kept in the TS7700 Cache or on a physical volume in a TS7740, TS7720 Tape Attach , or TS7760 Tape Attach. Large data sets can gain little from the ability of the TS7700 to stack data, so you can decide to leave them on native 3590 or 3592 Tape Cartridges.

Volume caching

Often, one step of a job writes a tape volume and a subsequent step (or job) reads it. The TS7700 improves the efficiency of this process: As data is cached in the TS7700 Cache the rewind time, the robotics time, and load or thread times for the mount are effectively removed. When a job attempts to read a volume that is not in the TS7700 Cache, the virtual volume is recalled from a stacked physical volume back into the cache. When a recall is necessary, the time to access the data is greater than if the data were already in the cache. The size of the cache and the use of cache management policies can reduce the number of recalls. Too much recall activity can negatively affect overall throughput of the TS7700.

Scratch mount times

When a program issues a scratch mount to write data, the TS7700 completes the mount request without having to recall the virtual volume into the cache. For workloads that create many tapes, this significantly reduces volume processing overhead times and improves batch window efficiencies.

Scratch mount times are further reduced when the optimal scratch allocation assistance function is enabled. This function designates one or more clusters as preferred candidates for scratch mounts by using a Management Class construct defined from the TS7700 Management Interface. For more information, see the *Optimal scratch allocation assistance* topic in the **Related information** section.

Disaster recovery

The grid configuration of the TS7700 is a perfect integrated solution for your disaster recovery data. Multiple TS7700 Clusters can be separated over long distances and interconnected by using an IP infrastructure to provide for automatic data replication. Data that is written to a local TS7700 is accessible at the remote TS7700 as if it was created there. Flexible replication policies make it easy to tailor the replication of data to your business needs.

Another disaster recovery solution is the Copy Export function. Copy Export allows a copy of selected virtual volumes that are written to the TS7700 to be removed and taken offsite.

For more information about disaster recovery configuration, see “Configuring for disaster recovery” on page 294. For more information about the Copy Export function, see “Copy export overview” on page 130.

Multifile volumes

If you currently stack multiple files onto volumes by using JCL constructs or some other method, the reason you are stacking is most likely to better use cartridge capacity. Automatic utilization of physical cartridge capacity is one of the primary attributes of the TS7700. Therefore, in many cases manual stacking of data sets onto volumes is no longer required. If you are planning a new application that would have used JCL to stack data sets onto a volume, the TS7700 makes this JCL step unnecessary. Multifile volumes moved to the TS7700 works without modification to the stacking. However, the TS7700 recalls the complete virtual volume to the TS7700 Cache if the volume is not in cache, rather than moving each file as you access it. Therefore, in some cases, it can be advantageous to allow the TS7700 do the stacking automatically for you. It can save you manual management overhead and in some cases, host CPU cycles, channel bandwidth, DASD space, or a combination of all.

Interchange/offsite storage

As currently delivered, the TS7700 does not support a capability to remove a stacked volume to be used for interchange. Native 3490, 3590, or 3592 tapes are better suited for interchange. For disaster recovery offsite data storage, the TS7740, TS7720 Tape Attach , and the TS7760 Tape Attach models provide the Copy Export function.

Grid network load balancing

For a TS7700 Grid link, the dynamic load balancing function calculates and stores the following information:

- Instantaneous throughput
- Number of bytes queued to transfer
- Total number of jobs queued on both links
- Whether deferred copy throttling is enabled on the remote node
- Whether a new job will be throttled (is deferred or immediate)

As a new task starts, a link selection algorithm uses the stored information to identify the link that will most quickly complete the data transfer. The dynamic load balancing function also uses the instantaneous throughput information to identify degraded link performance.

The TS7700 provides a wide range of capabilities. Unless your data sets are large or require interchange or offsite storage, it is likely that the TS7700 is a suitable place to store your data.

Related information

"Copy export overview" on page 130

"Configuring for disaster recovery" on page 294

"Allocation assistance" on page 290

System requirements

You must ensure that your facility meets the system requirements for the TS7700 when planning for installation.

Complete system installation requirements for the TS7700 are determined by your configuration. They include specifications for the common use of the 3952 Tape Frame and the specifications specific to either the TS7760, TS7720, or the TS7740.

3952 Tape Frame specifications

The following specifications are for the 3952 Tape Frame, including its standard components.

Table 18 displays the physical specifications of a 3952 Tape Frame configured as a 3952 Base Frame and its individual standard components that include the following:

- 3952 Tape Frame
- Ethernet switches

Coexistence of routers and switches in the same frame is not supported. Ethernet routers are present in existing, on-site systems that shipped before December 2011. Ethernet switches are shipped from manufacturing as part of new build systems after December 2011.

Refer to the topic "TS7760 specifications and requirements" on page 65 for a description of the difference between a 3952 Tape Frame used as a TS7760 Base Frame and as a TS7760 Storage Expansion Frame.

Refer to the topic "TS7720 specifications and requirements" on page 69 for a description of the difference between a 3952 Tape Frame used as a TS7720 Base Frame and as a TS7720 Storage Expansion Frame.

Table 18. Specifications of the 3952 Tape Frame and its standard components. Table describes physical specifications of the 3952 Tape Frame and its components.

	3952 Tape Frame F05	**3952 Tape Frame F06**	**Ethernet switch (each of 2)**
Width	644 mm (25.35 in.)	635 mm (25 in.)	44 cm (17.3 in.)
Depth	1098 mm (43.23 in.)	1409.7 mm (55.5 in.)	23 cm (9.0 in.)
Height	1804 mm (71.02 in.)	1930.4 mm (76 in.)	3.3 cm (1.7 in.)
Weight	270 kg (595.25 lb.) empty	746 kg (1645 lb.) maximally configured base frame	2.87 kg (6.32 lbs.)
Power	240 V AC 15 amp (single phase)	240 V AC 20 amp (single phase)	100-240 V AC 50/60 Hz (+/- 3 Hz)
Power consumption	200 watts (maximum)	200 watts (maximum)	38 watts
Thermal output	2.046 KBtu/hour (maximum)	2.6 KBtu/hour (maximum)	Included in 3952 Tape Frame maximum
Power-source loading	0.2 kVA 3,048 (10,000 ft.) maximum altitude	0.2 kVA 3,048 (10,000 ft.) maximum altitude	Included in 3952 Tape Frame maximum
Unit height	36 U	40 U	1 U

Related information

"TS7760 specifications and requirements" on page 65
"TS7720 specifications and requirements" on page 69
"TS7740 specifications and requirements" on page 73

Ethernet switches

This topic describes the key characteristics of Ethernet switches contained by the 3952 Tape Frame.

A 3952 Tape Frame configured as a 3952 Base Frame contains two, 1 Gb intranet Ethernet switches used for private communication between components within a TS7700 Cluster. A customer network connects directly to the TS7700 Server and utilizes virtual IP address technology to virtualize one or more customer-provided IP address across two AIX® configured Ethernet connections.

Note: Intranet Ethernet switches are available only when installed from manufacturing with 3957-V07, 3957-VEB, or 3957-VEC servers. TS7700 Servers upgraded in the field to 3957-V07 or 3957-VEB servers continue to use Ethernet routers as switches.

Related information

"3952 Tape Frame specifications" on page 63

"Network switches and TCP/IP ports requirements" on page 95

"System requirements" on page 63

"TS7760 specifications and requirements"

TS7760 specifications and requirements

The following specifications and requirements are specific to the TS7760 and its components.

The 3952 Tape Frame (3952 F06) houses the components of the TS7760.

When designated as a TS7760 Base Frame ("FC 7333, TS7700 Encryption-capable base frame" on page 175), the 3952 F06 contains the following components:

- TS7760 Server (3957-VEC) (includes control unit and 2 I/O drawers)
- TS7760 Cache Controller (3956-CSA)
- TS7760 Cache Drawer(s) (3956-XSA)
- Internal power distribution units

  Note: The standard 3952 Tape Frame ships with one internal power distribution unit. However, "FC 1903, Power Distribution Unit" on page 154 is required to provide two power distribution units to support the availability characteristics of the TS7760.

If FC 7333, TS7700 Encryption-capable base frame is installed, the TS7760 Base Frame has these physical specifications when fully configured:

Table 19. Encryption-capable TS7760 Base Frame specifications

Specification	Measurement
Width	616 mm (24.3 in.)
Depth	1397 mm (55 in.)
Height	1930.4 mm (76 in.)
Weight	746 kg (1645 lb.)

When designated as a TS7760 Storage Expansion Frame ("FC 7334, TS7700 Encryption-capable expansion frame" on page 175), the 3952 F06 contains the following components:

- TS7760 Cache Controllers (3956-CSA)
- TS7760 Cache Drawer(s) (3956-XSA)

Note: "FC 9323 Expansion frame attachment" on page 179 is also required to attach the base and expansion frames.
If FC 7334, TS7700 Encryption-capable expansion frame is installed the TS7760 Storage Expansion Frame has these physical specifications when fully configured:

Table 20. Encryption-capable TS7760 Storage Expansion Frame specifications

Specification	Measurement
Width	616 mm (24.3 in.)
Depth	1397 mm (55 in.)
Height	1930.4 mm (76 in.)
Weight	794 kg (1750 lb.)

The distance between a TS7760 Storage Expansion Frame and the TS7700 Base Frame cannot exceed 10 meters. This distance permits connection of the frames by using a 30-meter cable.

Table 21 displays the maximum configuration of a TS7760. Table 22 displays the physical specifications for each TS7760 component. Use these tables and the tape frame specifications, located from the links in the **Related information** section, to determine the correct physical requirements for your configuration.

Table 21. TS7760 maximum configuration

Component	Quantity of each component in 3952 Tape Frame as TS7760 Base Frame	Quantity of each component in 3952 Tape Frame as optional TS7760 Storage Expansion Frame
TS7760 Server (3957-VEC)	1	0
TS7760 Cache Controller (3956-CSA)	1	1
TS7760 Cache Drawers (3956-XSA)	9	15

Table 22. TS7760 component specifications

Specification	TS7760 Server		TS7760 Cache Subsystem	
Type and Model	**3957-VEC**	**I/O expansion drawer (each of 2)**	**3956-CSA cache controller**	**3956-XSA cache expansion drawer**
Width	427.5 mm (16.8 in.)	440 mm (17.32 in.) Total width of two joined drawers	449 mm (17.7 in.)	449 mm (17.7 in.)
Depth	747.5 mm (29.4 in.)	800 mm (31.5 in.)	540 mm (21.3 in.)	540 mm (21.3 in.)
Height	86.5 mm (3.4 in.)	220 mm (8.66 in.)	86 mm (3.4 in.)	86 mm (3.4 in.)
Weight	29.5 kg (65 lbs.)	42.2 kg (92.8 lb.) weight of two combined Reflects weight of each, without cassettes	27 kg (59.6 lb. lb.) fully configured	26.3 kg (57.9 lb.) fully configured
Power	200-240 V AC 50/60 Hz (+/- 3 Hz)	200-240 V AC 50/60 Hz	198-264 RMS† V AC 50/60 Hz	198-264 RMS† V AC 50/60 Hz
Unit height	2 U	5 U	2 U	2 U
Temperature (non-operating)	5-45 degrees C (41-113 degrees F)	Included in 3952 Tape Frame maximum	−10-65 degrees C (14-149 F)	5-45 degrees C (41-113 F)

Table 22. TS7760 component specifications (continued)

Specification	TS7760 Server		TS7760 Cache Subsystem	
Temperature (operating)	5-40 degrees C (41-104 degrees F) Temperature depends on altitude, see Table 23. Suggested: 18-27 degrees C (64-80 degrees F)	Included in 3952 Tape Frame maximum	10-32 degrees C (50-89.6 F)	10-32 degrees C (50-89.6 F)
Relative humidity	Non-operating: 8-85% Operating: 20-60%	Included in 3952 Tape Frame maximum	Non-operating: 8-80% Operating: 20%-80%	Non-operating: 8-80% Operating: 20%-80%
Maximum wet bulb (power off)	Non-operating: 28 degrees C (82 degrees F)	Included in 3952 Tape Frame maximum	23 degrees C (73.4 F)	23 degrees C (73.4 F)
Power consumption	1400 watts (2X) max.	Included in 3952 Tape Frame maximum	406 watts	213 watts
Thermal output	6655 Btu/hour (max.)	Included in 3952 Tape Frame maximum	1329 Btu/hr	730 Btu/hr
Power-source loading	1.6 kVA (max. config.) 3,048 m (10,000 ft.) max. altitude	Included in 3952 Tape Frame maximum	0.409 kVa	0.240 kVa
† Root Mean Square. In a multi-drawer configuration, total power is predicted to be a root mean square of the individual drawer maximums.				

Table 23. 3957-VEC, Temperature Depending on Altitude

Temperature (operating)	Altitude
5-40 degrees C (41-104 degrees F) **Note:** The minimum operating temperature cannot go below 5 C (41 degrees F).	Up to 3050 meter @ 5-28 C (41-82 degrees F)
	Up to 2875 meter @ 29 C (84 degrees F)
	Up to 2700 meter @ 30 C (86 degrees F)
	Up to 2525 meter @ 31 C (88 degrees F)
	Up to 2350 meter @ 32 C (89 degrees F)
	Up to 2175 meter @ 33 C (91 degrees F)
	Up to 2000 meter @ 34 C (93 degrees F)
	Up to 1825 meter @ 35 C (95 degrees F)
	Up to 1650 meter @ 36 C (96 degrees F)
	Up to 1475 meter @ 37 C (98 degrees F)
	Up to 1300 meter @ 38 C (100 degrees F)
	Up to 1125 meter @ 39 C (102 degrees F)
	Up to 950 meter @ 40 C (104 degrees F)

TS7760 Base Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the TS7760 Base Frame. Table 24 on page 68 displays the maximum input power for a fully configured TS7760.

Table 24. TS7760 Base Frame maximum input power requirements

Power requirement	**Value**
Voltage	200-240 V AC (single phase)
Frequency	50-60 Hz (+/- 3 Hz)
Current	24 amp
Inrush current	250 amp
Power (watt)	3280 watts
Input power required	4.8 kVa (single phase)
Thermal units	11.5 kBtu/hr, 2.9 kcal/hr

TS7760 Storage Expansion Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the TS7760 Storage Expansion Frame. Table 25 displays the maximum input power for a fully configured TS7760.

Table 25. TS7760 Storage Expansion Frame maximum input power requirements

Power requirement	**Value**
Voltage	200-240 V AC (single phase)
Frequency	50-60 Hz (+/- 3 Hz)
Current	24 amp
Leakage current	13.5 ma
Inrush current	250 amp
Power (watt)	3200 watts
Input power required	4.8 kVa (single phase)
Thermal units	11.2 kBtu/hr, 2.9 kcal/hr
Exhaust capacity	750 m^3/hr
Noise level	59 db

Related information

"TS7760 Storage Expansion Frame" on page 39

FC 9954, NEMA L6-30 power cord

FC 9955, RS 9750 DP power cord

FC 9956, IEC 309 power cord

FC 9957, PDL 4.3 power cord

FC 9958, Korean 4.3-m power cord

FC 9959, Unterminated power cord

FC 9966, Unterminated power cord (China)

TS7760 minimum configuration requirements

The following components are the minimum configuration requirements for a TS7760 with microcode level 8.41.x.x.

TS7760 minimum configuration requirements with microcode level 8.41.x.x

One 3952 F06 Tape Frame with the following features:

- FC 7333, TS7700 Encryption-capable base frame
- FC 5630, Install 3957-VEC
- FC 5660, Plant installation of 3956-CSA with 8 TB DDMs
- FC 5758, Integrated control path
- FC 1903, Power Distribution Unit
- FC AGKE, Ship with R4.1 Machine Code
- A power cord appropriate for the country of installation selected from:
  - FC 9954, NEMA L6-30 power cord,
  - FC 9959, Unterminated power cord, or
  - FC 9966, Unterminated power cord (China)

One TS7760 Server (3957-VEC) with the following features:

- FC 9268, Plant installation of 100 MB/s throughput
- FC 9000, Mainframe attachment
- FC AGKE, Ship with R4.1 Machine Code
- FC 9350, Plant Install
- Two grid adapters:
  - FC 1036, 1 Gb grid dual port copper connection,
  - FC 1037, 1 Gb dual port optical SW connection, or
  - FC 1038, 10 Gb dual port optical LW connection
- Either two of host to TS7700 FICON cables (FC 0201, 9-micron LC/LC 31-meter or FC 0203, 50-micron LC/LC 31-meter) or one FC 9700, No factory cables
- Two FICON adapters:
  - Two of “FC 3402, 16 Gb FICON Short Wavelength Attachment” on page 156
  - Two of “FC 3403, 16 Gb FICON Long Wavelength Attachment” on page 157

  OR
  - Two of FC 3438, 8 Gb FICON Short Wavelength Attachment
  - Two of FC 3439, 8 Gb FICON Long Wavelength Attachment
- FC 2715, Console attachment
- FC 9277, External Disk Encryption Certificate - Plant

One TS7760 Cache Controller (3956-CSA) with the following features:

- FC 7118, 96 TB SAS Storage
- FC 9352, Plant Install

Related information

“Feature details” on page 149
“TS7700 Server details” on page 34
“TS7760 Cache Controller” on page 42

TS7720 specifications and requirements

The following specifications and requirements are specific to the TS7720 and its components.

The 3952 Tape Frame (3952 F05) houses the components of the TS7720 .

When designated as a TS7720 Base Frame (“FC 7322, TS7720 Base frame” on page 174), the 3952 F05 contains the following components:

- TS7720 Server (includes control unit and 2 I/O drawers)
- TS7720 Cache Controller
- TS7720 Cache Drawer(s)
- Internal power distribution units

  Note: The standard 3952 Tape Frame ships with one internal power distribution unit. However, “FC 1903, Power Distribution Unit” on page 154 is required to provide two power distribution units to support the availability characteristics of the TS7720 .

If FC 7331, TS7720 Encryption-capable base frame is installed, the TS7720 Base Frame has these physical specifications when fully configured:

Table 26. Encryption-capable TS7720 Base Frame specifications

Specification	Measurement
Width	644 mm (25 in.)
Depth	1102 mm (43 in.)
Height	1804 mm (71 in.)
Weight	669.1 kg (1475 lb.)

When designated as a TS7720 Storage Expansion Frame (“FC 7323, TS7720 Storage expansion frame” on page 174), the 3952 F05 contains the following components:

- TS7720 Cache Controllers
- TS7720 Cache Drawer(s)

Note: “FC 9323 Expansion frame attachment” on page 179 is also required to attach the base and expansion frames.
If FC 7332, TS7720 Encryption-capable expansion frame is installed the TS7720 Storage Expansion Frame has these physical specifications when fully configured:

Table 27. Encryption-capable TS7720 Storage Expansion Frame specifications

Specification	Measurement
Width	644 mm (25 in.)
Depth	1102 mm (43 in.)
Height	1804 mm (71 in.)
Weight	666.8 kg (1470 lb.)

The distance between a TS7720 Storage Expansion Frame and the TS7720 Base Frame cannot exceed 10 meters, as per the prerequisites for “FC 7323, TS7720 Storage expansion frame” on page 174. This distance permits connection of the frames by using a 30-meter cable.

Table 28 on page 71 displays the maximum configuration of a TS7720 . Table 29 on page 71 displays the physical specifications for each TS7720 component. Use these tables and the tape frame specifications, located from the links in the **Related information** section, to determine the correct physical requirements for your configuration.

Table 28. TS7720 maximum configuration

Component	Quantity of each component in 3952 Tape Frame as TS7720 Base Frame	Quantity of each component in 3952 Tape Frame as optional TS7720 Storage Expansion Frame
TS7720 Server	1	0
TS7720 Cache Controller	1	1
TS7720 Cache Drawers	9	15

Table 29. TS7720 component specifications

Specification	TS7720 Server		TS7720 Cache Subsystem	
Type and Model	**3957-VEB**	**I/O expansion drawer (each of 2)**	**3956-CS9 cache controller**	**3956-XS9 cache expansion drawer**
Width	443 mm (17.3 in.)	440 mm (17.32 in.) Total width of two joined drawers	449 mm (17.7 in.)	449 mm (17.7 in.)
Depth	730 mm (28.7 in.)	800 mm (31.5 in.)	540 mm (21.3 in.)	540 mm (21.3 in.)
Height	173 mm (6.81 in.)	220 mm (8.66 in.)	86 mm (3.4 in.)	86 mm (3.4 in.)
Weight	48.7 kg (107 lbs.)	42.2 kg (92.8 lb.) weight of two combined Reflects weight of each, without cassettes	27.0 kg (59.6 lb.) fully configured	26.3 kg (57.9 lb.) fully configured
Power	200-240 V AC 50/60 Hz (+/- 3 Hz)	200-240 V AC 50/60 Hz	90-136 RMS† V AC Low Range 198-264 RMS† V AC High Range 50/60 Hz	90-136 RMS† V AC Low Range 198-264 RMS† V AC High Range 50/60 Hz
Unit height	4 U	5 U	2 U	2 U
Temperature (non-operating)	5-45 degrees C (41-113 F)	Included in 3952 Tape Frame maximum	−10-65 degrees C (14-149 F)	5-45 degrees C (41-113 F)
Temperature (operating)	10-32 degrees C (50-89.6 degrees F) Suggested: 18-27 degrees C (64-80 degrees F)	Included in 3952 Tape Frame maximum	10-32 degrees C (50-89.6 F)	10-32 degrees C (50-89.6 F)
Relative humidity	Non-operating: 8-80% Operating: 20-60%	Included in 3952 Tape Frame maximum	Non-operating: 8-80% Operating: 20%-80%	Non-operating: 8-80% Operating: 20%-80%
Maximum wet bulb (power off)	Non-operating: 28 degrees C (82 degrees F) Operating: 29 degrees C (84 degrees F)	Included in 3952 Tape Frame maximum	23 degrees C (73.4 F)	23 degrees C (73.4 F)
Power consumption	1950 watts (max.)	Included in 3952 Tape Frame maximum	226 watts	213 watts
Thermal output	6655 Btu/hour (max.)	Included in 3952 Tape Frame maximum	910 Btu/hr	730 Btu/hr

Table 29. TS7720 component specifications (continued)

Specification	TS7720 Server		TS7720 Cache Subsystem	
Power-source loading	2.0 kVA (max. config.) 3,048 m (10,000 ft.) max. altitude	Included in 3952 Tape Frame maximum	0.290 kVa	0.240 kVa
† Root Mean Square. In a multi-drawer configuration, total power is predicted to be a root mean square of the individual drawer maximums.				

TS7720 Base Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the TS7720 Base Frame. Table 30 displays the maximum input power for a fully configured TS7720 .

Table 30. TS7720 Base Frame maximum input power requirements

Power requirement	Value
Voltage	200-240 V AC (single phase)
Frequency	50-60 Hz (+/- 3 Hz)
Current	20 amp
Inrush current	250 amp
Power (watt)	3140 watts
Input power required	4.0 kVa (single phase)
Thermal units	11.0 kBtu/hr, 2.76 kcal/hr

TS7720 Storage Expansion Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the TS7720 Storage Expansion Frame. Table 31 displays the maximum input power for a fully configured TS7720 .

Table 31. TS7720 Storage Expansion Frame maximum input power requirements

Power requirement	Value
Voltage	200-240 V AC (single phase)
Frequency	50-60 Hz (+/- 3 Hz)
Current	20 amp
Leakage current	13.5 mA
Inrush current	250 amp
Power (watt)	3460 watts
Input power required	4.0 kVa (single phase)
Thermal units	11.8 kBtu/hr, 2.96 kcal/hr
Exhaust capacity	750 m^3/hr
Noise level	59 db

Related information

"3952 Tape Frame specifications" on page 63
"TS7720 Storage Expansion Frame" on page 45

FC 9954, NEMA L6-30 power cord

FC 9955, RS 9750 DP power cord

FC 9956, IEC 309 power cord

FC 9957, PDL 4.3 power cord

FC 9958, Korean 4.3-m power cord

FC 9959, Unterminated power cord

FC 9966, Unterminated power cord (China)

TS7740 specifications and requirements

The following specifications and requirements are specific to the TS7740 and its components.

Table 32 displays the maximum configurations of a TS7740 in a 3952 Tape Frame. Table 33 displays the physical specifications for each TS7740 component. Use these tables and the tape frame specifications, located from the links in the **Related information** section, to determine the correct physical requirements for your configuration.

Table 32. TS7740 maximum configurations

Quantity	Component
1	TS7740 Server
1 3956-CC9	TS7740 Cache Controller
2 3956-CX9	TS7740 Cache Drawers

Table 33. TS7740 component specifications

	TS7740 Server		TS7740 Cache Subsystem	
Type and Model	**3957-V07**	**I/O expansion drawer (each of 2)**	**3956-CC9 cache controller**	**3956-CX9 cache expansion drawer**
Width	443 mm (17.3 in.)	440 mm (17.32 in.) Total width of two joined drawers	449 mm (17.7 in.)	449 mm (17.7 in.)
Depth	730 mm (28.7 in.)	800 mm (31.5 in.)	487 mm (19.2 in.)	487 mm (19.2 in.)
Height	173 mm (6.81 in.)	220 mm (8.66 in.)	88 mm (3.5 in.)	88 mm (3.5 in.)
Weight	48.7 kg (107 lbs.)	42.2 kg (92.8 lb.) weight of two combined	25.9 kg (57.1 lb.) fully configured	26.3 kg (57.9 lb.) fully configured
Power	200-240 V AC 50/60 Hz (+/- 3 Hz)	200-240 V AC 50/60 Hz	90-136 RMS† V AC 198-264 RMS† V AC	90-136 RMS† V AC 198-264 RMS† V AC
Unit height	4 U	5 U	2 U	2 U
Temperature (non-operating)	5-45 degrees C (41-113 F)	Included in 3952 Tape Frame maximum	−10-65 degrees C (14-149 F)	5-45 degrees C (41-113 F)
Temperature (operating)	10-32 degrees C (50-89.6 degrees F) Recommend: 18-27 degrees C (64-80 degrees F)	Included in 3952 Tape Frame maximum	10-32 degrees C (50-89.6 F)	10-32 degrees C (50-89.6 F)
Relative humidity	Non- operating: 8-80% Operating: 20-80%	Included in 3952 Tape Frame maximum	Non- operating: 8-80% Operating: 20-80%	Non- operating: 8-80% Operating: 20-80%

Table 33. TS7740 component specifications (continued)

	TS7740 Server		TS7740 Cache Subsystem	
Maximum wet bulb (power off)	Non- operating: 28 degrees C (82 degrees F) Operating: 29 degrees C (84 degrees F)	Included in 3952 Tape Frame maximum	23 degrees C (73.4 F)	23 degrees C (73.4 F)
Power consumption	1950 watts (maximum)	Included in 3952 Tape Frame maximum	304 watts	263watt
Thermal output	6655 Btu/hour (maximum)	Included in 3952 Tape Frame maximum	1,040 Btu/hr	900 Btu/hr
Power-source loading	2.0 kVA (max config) 3,048 m (10,000 ft.) maximum altitude	Included in 3952 Tape Frame maximum	0.334 kVa	0.298 kVa
† Root Mean Square. In a multi-drawer configuration, total power is predicted to be a root mean square of the individual drawer maximums.				

If FC 7330, TS7740 Encryption-capable base frame is installed, the 3952 Tape Frame has these physical specifications when fully configured:

Table 34. Physical specifications of an encryption-capable 3952 Tape Frame

Width	644 mm (25 in.)
Depth	1102 mm (43 in.)
Height	1804 mm (71 in.)
Weight	474.2 kg (1045 lb.)

TS7740 3952 Base Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the IBM TS7740. Table 35 displays the maximum input power for a fully configured TS7740.

Table 35. TS7740 3952 Base Frame maximum input power requirements

Power requirement	**Value**
Voltage	200-240 V AC (single phase)
Frequency	50-60 Hz (+/- 3 Hz)
Current	20 amp
Leakage current	10 mA
Inrush current	250 amp
Power (watts)	1786 watts (estimated)
Input power required	4.0 kVa (single phase)
Thermal units	6.05 kBtu/hr, 1.52 kcal/hr
Exhaust capacity	385 m^3/hr
Noise level	56 db

The 3952 Tape Frame houses the components of the TS7740. The standard 3952 Tape Frame ships with one internal power distribution unit. However, “FC 1903, Power Distribution Unit" on page 154 is required to provide two power distribution units to support the availability characteristics of the TS7740.

Related information

"3952 Tape Frame specifications" on page 63

FC 9954, NEMA L6-30 power cord

FC 9955, RS 9750 DP power cord

FC 9956, IEC 309 power cord

FC 9957, PDL 4.3 power cord

FC 9958, Korean 4.3-m power cord

FC 9959, Unterminated power cord

FC 9966, Unterminated power cord (China)

Cooling requirements

Your facility must meet the temperature requirements for the TS7700.

The 3952 Tape Frame, which contains the components of the TS7700, requires ambient room temperatures that are consistent with environmental specifications. For more information, see "Environmental requirements" on page 78. The heat load for the 3952 Tape Frame system can be found under "3952 Tape Frame specifications" on page 63. The total system heat load is the sum of the heat loads for all installed frames.

Related information

"3952 Tape Frame specifications" on page 63

Floor requirements

Your facility must meet specified floor leveling, loading, and weight distribution requirements before you can install the TS7700.

Floor – general

A 3952 Tape Frame can be installed on a raised or solid floor meeting the minimum leveling and floor-loading capacity requirements. The floor under the library must have a smooth surface with no ventilation grates under the frame's leveling pads. If the floor is carpeted, the carpeting must be approved for use in a computer environment (that is, it must display low electrostatic discharge characteristics).

Floor – leveling

The leveling pads on the 3952 Tape Frame can be adjusted to compensate for an uneven floor where the frame is to be installed. The maximum out-of-level condition is 25.4 mm (1 in.) over the frame's length and width.

Note: IBM strongly recommends that stringers be installed between all corner posts. In addition, a post should be placed under the areas where the frame's leveling pads sit. As an alternative to placing posts under the leveling pads, a post may be placed at the midpoint of the stringers in the areas where the frame sits.

Floor – weight distribution and loading

If the 3952 Tape Frame is installed on a raised floor, the raised floor should be stabilized to prevent a horizontal shift of the raised floor structure. The minimum overall floor load rating should be 256 kg/m^2 (52.6 $lb./ft.^2$). However, IBM recommends a floor load rating of at least 341 kg/m^2 (70.0 $lb./ft.^2$). These ratings do not include additional loading by personnel and equipment traffic.

In addition, the floor must support point loads exerted by the leveling pads of up to 4.8 kg/cm^2 (68.4 $lb./in.^2$).

Dimension requirements

This topic lists the dimensions of the TS7700.

Table 36 lists the dimensions of the frame enclosing the TS7700.

Table 36. Physical characteristics of a maximally configured 3952 Tape Frame F06

Characteristic	Value
Height	1930.4 mm (76 in.)
Width	616 mm (24.3 in.)
Depth	1397 mm (55 in.)
Weight	746 kg (1645 lbs.) maximally configured †
Power	240 Vac, 20 amp (single phase)
Unit height	40 U
†Refer to the topics "TS7720 specifications and requirements" on page 69, "TS7740 specifications and requirements" on page 73, and "TS7760 specifications and requirements" on page 65 for maximum configurations for the TS7720 , TS7740, and the TS7760.	

Clearance requirements

You must meet the specified clearance requirements when moving and positioning the 3952 Tape Frame.

Clearance – moving the frame

Two persons should be available to move system components between locations. Table 37 and Table 38 show the minimum aisle and door dimensions for moving components from one location to another for the 3952 Tape Frame.

Table 37. Required clearances when moving the 3952 F06 frame

Clearance item	Required clearance
Distance to ceiling†	1955.8 mm (77 in.)
Aisle and door width	736 mm (29 in.)
Corner radius	2844.8 mm (112 in.)
Ramp inclination	15°
†The 3952 F06 Tape Frame is moved on casters and has four leveling pads. The frame's nominal height is 1.94 m (76.5 in.) from the bottom of the leveling pads to the top of the frame. The leveling pads can vary the height of the frame by up to 30 mm (1.2 in.). The pads are completely raised when the frame is shipped to allow it to roll on its casters. The shipping height of the frame on its casters is 1.93 m (75.9 in.).	

Table 38. Required clearances when moving the 3952 F05 frame

Clearance item	Required clearance
Distance to ceiling†	1830 mm (72 in.)

Table 38. Required clearances when moving the 3952 F05 frame (continued)

Clearance item	Required clearance
Aisle and door width	736 mm (29 in.)
Corner radius	2237 mm (88 in.)
Ramp inclination	15°
†The 3952 F05 Tape Frame is moved on casters and has four leveling pads. The frame's nominal height is 1.815 m (71.5 in.) from the bottom of the leveling pads to the top of the frame. The leveling pads can vary the height of the frame by up to 30 mm (1.2 in.). The pads are completely raised when the frame is shipped to allow it to roll on its casters. The shipping height of the frame on its casters is 1.8 m (70.9 in.).	

Clearance – frame in position

Clearances are required around system components for the operator to perform certain tasks and for the service representative to perform certain items. Table 39 and Table 40 on page 78 list specific clearance requirements for the 3952 Tape Frame.

Figure 29 gives the opening radius of the front and rear doors when the F06 frame is in position. It also shows the side panel access distance. From these dimensions, Table 39 was constructed to allow the service personal space to move while accessing these areas. Access is needed for removing and replacing equipment in the frame.

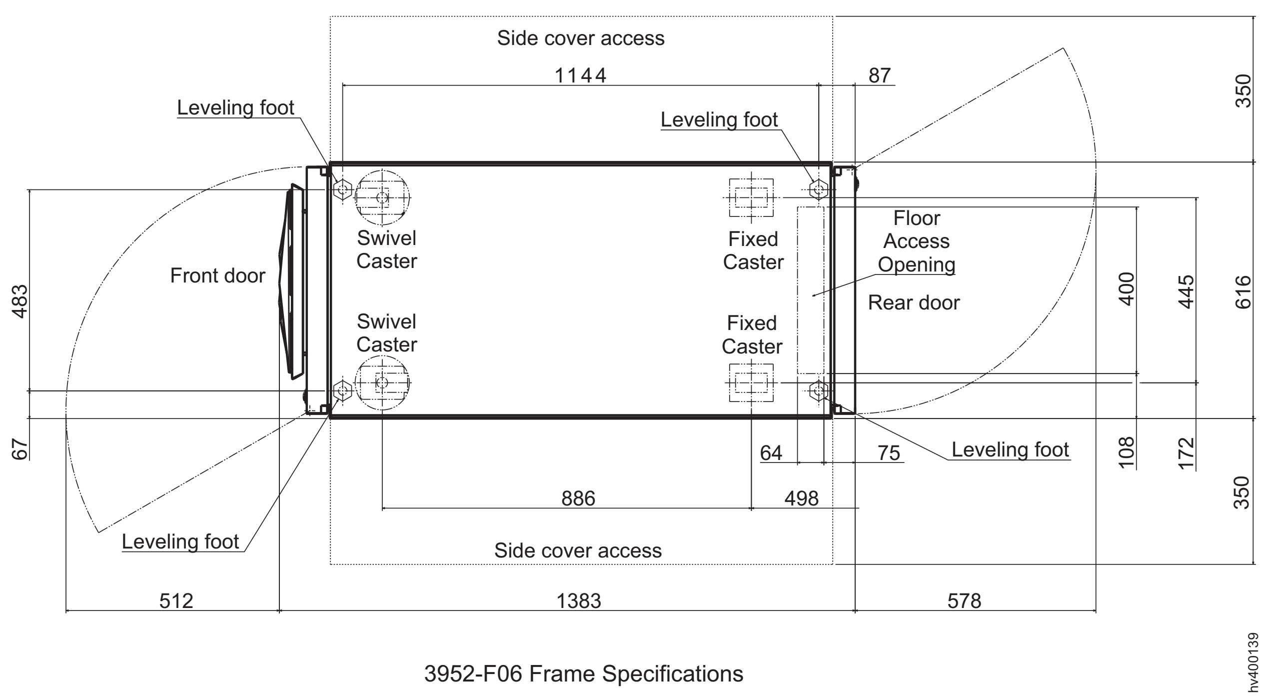


Figure 29. F06 frame dimensions when in position

Table 39. Required clearances when the F06 frame is in position

Door or panel	Required clearance
Front	690 mm (27.2 in.)

Table 39. Required clearances when the F06 frame is in position (continued)

Door or panel	Required clearance
Back	660 mm (26.0 in.)
Side	0 mm (0 in.) required, but 480 mm (18.9 in.) recommended for side panel removal.

Table 40. Required clearances when the F05 frame is in position

Door or panel	Required clearance
Front	690 mm (27.2 in.)
Back	660 mm (26.0 in.)
Side	0 mm (0 in.) required, but 480 mm (18.9 in.) recommended for side panel removal.

Related information

FC 5759, Integrated control path

Environmental requirements

Your facility should meet specified temperature, humidity, and air quality requirements before installing the TS7700.

Table 41 shows recommended environmental conditions for the TS7700.

Table 41. Temperature, altitude, and humidity specifications

Condition	Air temperature	Altitude	Relative humidity[1]	Wet bulb temperature
Operating (low altitude)	10°C to 32°C (50°F to 89.6°F)	up to 5000 ft amsl	20% to 80%	23°C (73°F)
Operating (high altitude)	10°C to 28°C (50°F to 82.4°F)	5001 ft amsl to 7000 ft amsl	20% to 60%	23°C (73°F)
Recommended Operating Range[2]	20°C to 25°C (68°F to 77°F)	up to 7000 ft amsl	40% to 55%	—
Power Off	10°C to 43°C (50°F to 109°F)	—	8% to 80%	27°C (80°F)
Storage	1°C to 60°C (33.8°F to 140°F)	—	5% to 80%	29°C (84°F)
Shipping	-40°C to 60°C (-40°F to 140°F)	—	5% to 100%	29°C (84°F)

Notelist:

1. Non-condensing
2. Although the TS7700 operates outside this range, it is advised that the user adhere to the Recommended Operating Range provided.

Table 42. Air quality specifications

Specification	Restrictions
Gaseous contamination	Severity level G1 according to ANSI/ISA 71.04-1985[1], which states that the reactivity rate of copper coupons is fewer than 300 Angstroms per month (Å/month, ≈ 0.0039 µg/cm2-hour weight gain)[2]. In addition, the reactivity rate of silver coupons is less than 300Å/month (≈ 0.0035 µg/cm^2-hour weight gain)[3]. The reactive monitoring of gaseous corrosivity should be conducted approximately 5 cm (2 in.) in front of the rack on the air inlet side at one-quarter and three-quarter frame height off the floor or where the air velocity is much higher
Particulate contamination	Data centers must meet the cleanliness level of ISO 14644-1 class 8. For data centers without airside economizer, the ISO 14644-1 class 8 cleanliness might be met by the choice of the following filtration: The room air might be continuously filtered with MERV 8 filters. Air entering a data center might be filtered with MERV 11 or preferably MERV 13 filters. For data centers with airside economizers, the choice of filters to achieve ISO class 8 cleanliness depends on the specific conditions present at that data center. The deliquescent relative humidity of the particulate contamination should be more than 60% RH[4]. Data centers must be free of zinc whiskers[5].

Notelist:

1. ANSI/ISA-S71.04. 1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*, Instrument Society of America, Research Triangle Park, NC, 1985.
2. The derivation of the equivalence between the rate of copper corrosion product thickness growth in Å/month and the rate of weight gain assumes that Cu_2S and Cu_2O grow in equal proportions.
3. The derivation of the equivalence between the rate of silver corrosion product thickness growth in Å/month and the rate of weight gain assumes that Ag_2S is the only corrosion product.
4. The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.
5. Surface debris is randomly collected from 10 areas of the data center on a 1.5-cm diameter disk of sticky electrically conductive tape on a metal stub. If examination of the sticky tape in a scanning electron microscope reveals no zinc whiskers, the data center is considered free of zinc whiskers.

Table 43. Machine-specific exhaust limits

Maximally configured machine	Maximum capacity of exhaust
TS7740	385 m^3/h
TS7720	700 m^3/h
TS7720 Storage Expansion Frame	750 m^3/h

Acoustic requirements

This topic gives the acoustic requirements for the TS7700.

Notes:

- Declared level L_{WAd} is the upper-limit A-weighted sound power level; Declared level L_{pAm} is the mean A-weighted sound pressure level measured at the 1-meter bystander positions.
- All measurements made in conformance with ISO 7779 and declared in conformance with ISO 9296.

- B, dB, abbreviations for bels and decibels, respectively. 1 B = 10 dB.

Table 44 shows the acoustic specifications for the TS7760.

Table 44. TS7760 acoustic requirements. Table describes operating and idling decibels for the TS7760.

Product	**Declared Sound Power Level, L_{WAd}**		**Mean A-weighted sound pressure level at 1-m (bystander) positions, L_{pAm}**	
	Operating (B)	Idling (B)	Operating (dB)	Idling (dB)
TS7760 (3952-F06)	7.7	7.85	59	62
TS7760 (3952-F06) at high ambient	8.6‡	8.6‡	70	70
‡Government regulations (such as those prescribed by OSHA or European Community Directives) may govern noise level exposure in the workplace and may apply to you and your server installation. This IBM system is available with an optional acoustical door feature that can help reduce the noise emitted from this system. The actual sound pressure levels in your installation depend upon a variety of factors, including the number of racks in the installation; the size, materials, and configuration of the room where you designate the racks to be installed; the noise levels from other equipment; the room ambient temperature, and employees' location in relation to the equipment. Further, compliance with such government regulations also depends upon a variety of additional factors, including the duration of employees' exposure and whether employees wear hearing protection. IBM recommends that you consult with qualified experts in this field to determine whether you are in compliance with the applicable regulations.				

Table 45 shows the acoustic specifications for the TS7720 .

Table 45. TS7720 acoustic requirements. Table describes operating and idling decibels for the TS7720 .

Declared Sound Power Level, L_{WAd}		**Mean A-weighted sound pressure level at 1-m (bystander) positions, L_{pAm}**	
Operating (B)	Idling (B)	Operating (dB)	Idling (dB)
7.7	7.7	58	58

Table 46 shows the acoustic specifications for the TS7740.

Table 46. TS7740 acoustic requirements. Table describes operating and idling decibels for the TS7740.

Declared Sound Power Level, L_{WAd}		**Mean A-weighted sound pressure level at 1-m (bystander) positions, L_{pAm}**	
Operating (B)	Idling (B)	Operating (dB)	Idling (dB)
7.0	7.0	53	53

Host compatibility

This section describes host compatibility requirements for installation of the TS7700.

You must ensure that your hosts are compatible with the IBM TS7700 when planning for installation.

Supported hosts

This section describes hosts supported by the IBM TS7700.

The TS7700 supports the following host attachments:

- IBM Z® mainframe
- IBM s390 server

The TS7700 supports the following operating systems:

- z/OS®, V1R13 and later (earlier release levels were initially supported, however those release levels are no longer in service. Refer to Preventive Service Planning bucket D/T3957 from the *IBM Support and Downloads* link in the **Related information** section for the list of applicable maintenance)
- z/VM®, V5.4.0 and later. V5.4.0 or later with the PTFs for APAR VM64979 is required for both guest and native VM support providing base CP functions.
- z/VSE®, 4.3 and later. With z/VSE, the TS7700 is transparent to host software. z/VSE supports the TS7700 as a stand-alone system in transparency mode. z/VSE 5.1 or later supports copy export and a multi-cluster grid.
- zTPF, V1.1 and later. With z/TPF the TS7700 is supported in both a single node and a grid environment with the appropriate software maintenance. The category reserve and release functions are not supported by the TS7700.

Later versions of host software might be required to fully use TS7700 enhancements.

Notelist:

- Native VM Tape library support for these drives is provided by DFSMS/VM FL221 with PTFs for RMS APAR VM64773 and VM65005 and their prerequisite service.
- EREP V3.5 plus PTFs is required.

Supported hosts connect to the TS7700, which connects to a TS3500 or TS4500 Tape Library.

A host connects to the TS7700 via the 8 Gb or 16 Gb FICON adapters. Each installed adapter supports 512 virtual paths.

Related information

http://www.ibm.com/support/us/en/

IBM Z host attachment to the TS7700

FICON attachments between an IBM Z® host and a TS7700 can be single-mode long wave laser or multi-mode short wave laser.

These attachments are abbreviated as:

- SM = Single Mode Fiber
- LW = Long Wave Laser
- MM = Multi-Mode Fiber
- SW = Short Wave Laser

Note: Long wave cables attach only to long wave adapters and short wave cables attach only to short wave adapters.

Figure 30 shows typical FICON attachments between a host and a TS7700. The TS7700 supports IBM Z® servers by using 8 Gbps or 16 Gbps FICON at distances of up to 250 km (155 miles) by using dense wavelength division multiplexing (DWDM) in combination with switches, or more extended distances by using supported channel extension products.

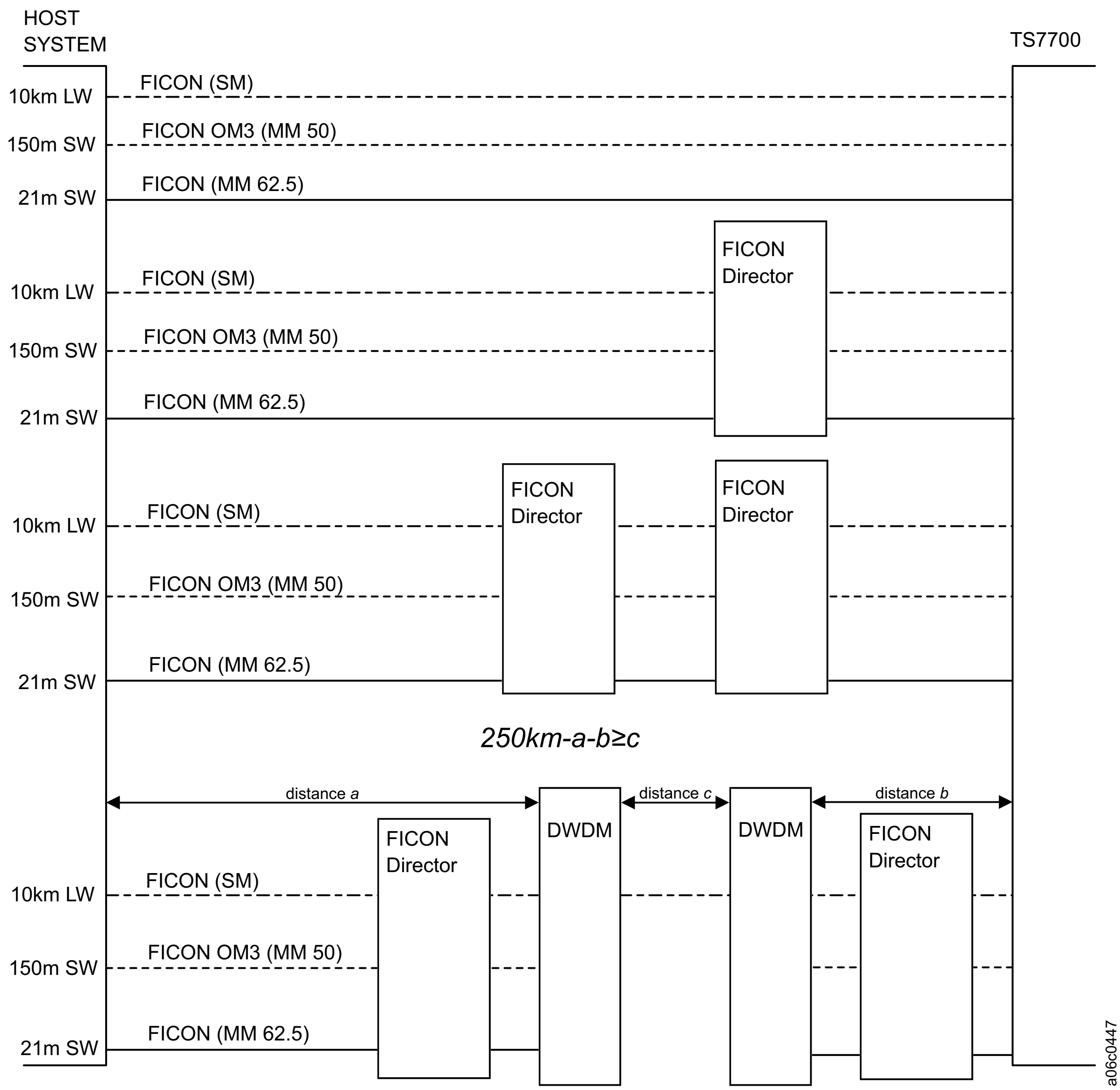


Figure 30. IBM Z® host attachment to TS7700 (at speed of 8 Gb/second)

Restrictions:

1. The FICON long-wavelength attachment that is shown in Figure 30 is “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157, which has a maximum cable length of 10 km.
2. The distance between a TS7700 and the first powered or active switch, director, or host cannot exceed 10 km. Distances greater than 10 km require addition of switches or directors.

3. Distances greater than 30 km require DWDM in combination with qualified switches or directors with adequate RAM buffer on line cards. Adequate RAM buffer is defined as being capable of reaching distances of 100-250 km.

FICON adapters can be upgraded in number (two to four) and kind (shortwave or longwave) by using "FC 3402, 16 Gb FICON Short Wavelength Attachment" on page 156 and "FC 3403, 16 Gb FICON Long Wavelength Attachment" on page 157 or "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157 and "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157.

"FC 3401, Enable FICON dual port" on page 156 can be used to enable the second port of the FICON adapter, allowing a four-adapter cluster to upgrade to eight host connections (two per card). "FC 3402, 16 Gb FICON Short Wavelength Attachment" on page 156, "FC 3403, 16 Gb FICON Long Wavelength Attachment" on page 157, "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157 or "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157 is a prerequisite.

Important 8 Gb installation information: Due to **higher sensitivity** (increased FICON speed 4G -> 8G) before using a wrap plug or plugging a new or existing cable into any LC Duplex connector, ensure the cable ends and the adapter duplex connector laser transmit/receive ports in the SFP are also cleaned with **Fiber Cleaning Tool P/N 54Y4392** before making a connection. Fibre cables to the affected FICON ports must be undamaged and clean. Use **Fiber Cleaning Tool P/N 54Y4392** to clean FICON host cables and host adapter LC duplex connector. If errors that occur during installation of the 8 Gb FICON adapters and cables are not corrected during cable and SFP cleaning and card replacement then you must contact your cabling contractor.

For the most recent list of supported FICON directors, refer to the *IBM Techdocs Library* web page linked in the **Related information** section.

In a base TS7700, 2 FICON cards are installed: one in the primary and one in the alternate I/O drawer. Each card is installed in slot C6 in the rear of the I/O drawer, as shown in Figure 31.

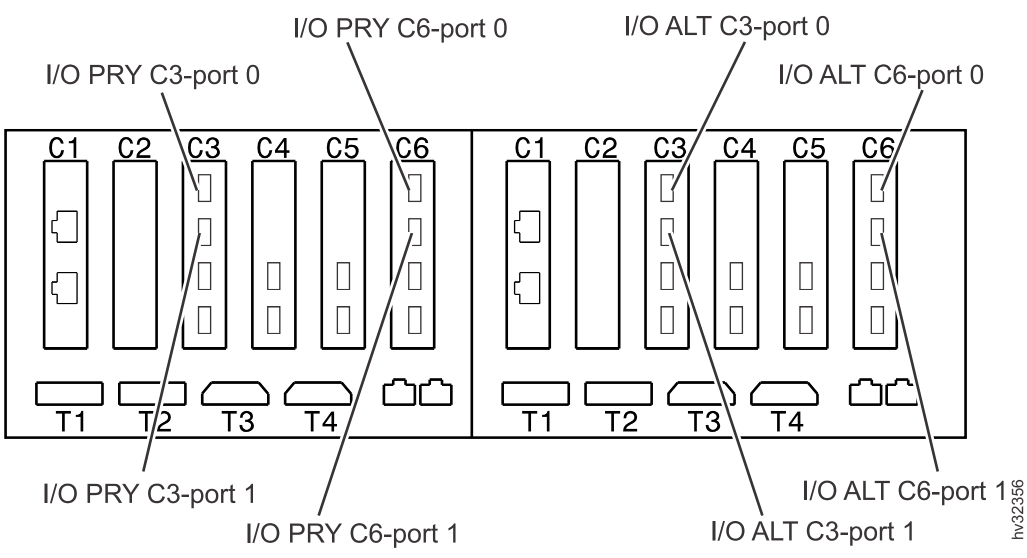


Figure 31. TS7700 I/O drawer FICON Cable Connections

When an additional FICON attachment (“FC 3402, 16 Gb FICON Short Wavelength Attachment” on page 156, “FC 3403, 16 Gb FICON Long Wavelength Attachment” on page 157, “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 157 or “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157) is installed on a TS7700 2 more FICON cards (either “FC 3441, FICON short-wavelength attachment” on page 158, “FC 3442, FICON long-wavelength attachment” on page 158, or “FC 3443, FICON 10-km long-wavelength attachment” on page 158) are installed in primary and alternate drawers in slot C3, as shown in Figure 31 on page 83 and listed on Table 47.

Table 47. TS7700 FICON Cable Connections

FICON Configuration	First I/O Drawer (Primary)		Second I/O Drawer (Alternate)	
	Slot 3 (C3)	**Slot 6 (C6)**	**Slot 3 (C3)**	**Slot 6 (C6)**
2 cards	Not installed	FICON	Not installed	FICON
4 cards	FICON	FICON	FICON	FICON

Each FICON card contains four ports, but only two ports can be enabled per card. Port 0 is enabled by default and port 1 is enabled when “FC 3401, Enable FICON dual port” on page 156 is installed.

Related information

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FQ116133

Host configurations

This section lists and describes host configurations for use with the TS7700.

z/OS I/O definitions

This section defines the I/O of the z/OS operating system used by the IBM Z® host attached to the TS7700.

Subsystem identification

Each logical controller, or 16-device group, must present a unique subsystem identification to the IBM Z® host. This ID is a 1-byte field that uniquely identifies each device associated with the logical controller within the larger storage controller. The value of this ID cannot be 0. The subsystem ID must match the LIBPORT-ID defined in the host Hardware Configuration Definition (HCD).

Table 48 shows required definitions of subsystem IDs.

Table 48. Subsystem identification definitions

Cluster	Vnode	Logical CU (Hex)	Cluster Logical Devices (Hex)	Subsystem ID/LIBPORT-ID (Hex)†
0	0	0x00-0x1E	0x0000-0x01EF	0×01-0×1F
1	0	0x00-0x1E	0x0000-0x01EF	0×41-0×5F‡
2	0	0x00-0x1E	0x0000-0x01EF	0×81-0×9F‡
3	0	0x00-0x1E	0x0000-0x01EF	0×C1-0×DF‡
4	0	0x00-0x1E	0x0000-0x01EF	0×21-0×3F‡
5	0	0x00-0x1E	0x0000-0x01EF	0×61-0×7F‡
6	0	0x00-0x1E	0x0000-0x01EF	0×A1-0×BF‡

Table 48. Subsystem identification definitions (continued)

Cluster	Vnode	Logical CU (Hex)	Cluster Logical Devices (Hex)	Subsystem ID/LIBPORT-ID (Hex)†
7	0	0x00-0x1E	0x0000-0x01EF	0×E1-0×FF‡
†Identical to configured LIBPORT-ID ‡Every logical controller image represents 16 tape device images and must have a unique LIBPORT-ID. The system has reserved ranges of LIBPORT-IDs to account for future node expansions at each distributed library.				

Cluster and grid reporting

Every virtual device that is attached to a IBM Z® host and the TS7700 must report the same library sequence number that is known as the *composite library ID*. This is true whether the grid configuration is distributed across multiple sites, or consists of a single site. The composite library ID allows the host to consider the grid configuration as a single library.

Each cluster in a grid configuration possesses a unique library sequence number that is known as the *distributed library ID*, that identifies it among the clusters in its grid. A distributed library ID is given to a cluster during the teach of the integrated Library Manager for the TS7700 partition. This ID is reported to the IBM Z® host upon request and is used to distinguish one cluster from another in a grid.

Host console request facility

The TS7700 permits you to make problem determinations from the IBM Z® host console by using the host console request (HCR) facility, or MVS™ Library Request (LI REQ) command. This facility performs similarly to existing library query commands; it permits an operator to request TS7700 operational information or take a limited set of actions.

For example, you can use this command to request information about the following:

- The current state of grid links and copy activity between clusters
- The current state of the cache and the data managed within it associated with the specified distributed library
- The status and attributes of virtual volumes
- Usage of physical volumes and their relationships with distributed libraries
- Media types and counts for volume pools
- The content of the recall queue starting with a specified virtual volume

You can also use this command to take actions such as the following:

- Define settings for thresholds and priorities for various resources
- Define settings that control how the TS7700 manages data movement
- Promote a volume in the recall queue
- Enable or disable copies to and from a specified distributed library by using the host copy enable function
- Control deferred copy throttling

You can use HCR to temporarily override a virtual volume's assigned disk cache preference group while the volume resides in disk cache. This function can also be used to update the last recently used position of the volume as if the volume had just been mounted. If you intend to access the volume again soon, you can use this function to retain the volume in cache for a longer period. Or, you can use this function to request that the volume be migrated from cache sooner.

For a full description of how the HCR facility can be used, and for additional information regarding the MVS Library Request command syntax, refer to the white paper: *IBM TS7700 Series z/OS Host Command Line Request User's Guide* at the Techdocs Library link in the *Related information* section.

Presented drive image

The IBM TS7700 presents a tape drive image of a 3490 C2A, identical to that of current VTS and peer-to-peer (PtP) subsystems. Command set, responses to inquiries, and accepted parameters match the defined functional specifications of a 3490 drive.

Related information

"Copy export overview" on page 130

"Allocation assistance" on page 290

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/Web/WhitePapers

Infrastructure requirements

You must ensure that your infrastructure meets TS7700 requirements when planning for installation.

Call Home infrastructure requirements

The TS3000 System Console (TSSC) enables remote enhanced service connection of a TS7700 Server for Call Home. You must ensure that an analog telephone line or a broadband connection is available to enable Call Home functionality.

TS7700 Grid interconnect LAN/WAN requirements

This topic gives LAN/WAN requirements for the TS7700 cross-site grid TCP/IP network infrastructure.

The TS7700 Grid TCP/IP network infrastructure must be in place before the grid is activated so that the clusters can communicate with one another as soon as they are online. Two or four 1 Gb Ethernet or two Grid Optical LW connections must be in place before grid installation and activation, including the following equipment:

Intranet Ethernet switches
Intranet Ethernet switches are used primarily for private communication between components within a cluster. Ethernet switches are available from manufacturing with 3957-VEC, 3957-VEB, or 3957-V07 servers.

ATM switches

Ethernet extenders
An Ethernet extender or other extending equipment is used to complete extended distance Ethernet connections. Extended grid Ethernet connections can be any of the following:

1 Gb copper 10/100/1000 Base-TX
This adapter conforms to the IEEE 802.3ab 1000Base-T standard,

which defines gigabit Ethernet operation over distances up to 100 meters using four pairs of CAT-6 copper cabling.

1 Gb optical shortwave
This SX adapter has an LC Duplex connector that attaches to 50 micron or 62.5 micron multimode fibre cable. It is a standard SW (850 nm) adapter that conforms to the IEEE 802.3z standards. This adapter supports distances of 2 to 260 meters for 62.5 micron and 2 to 550 meters for 50 micron Multimode Fiber (MMF).

10 Gb optical longwave
This adapter supports a maximum of 10 kilometers of 1310 nm, 9µm, single-mode fiber optic cable. It conforms to the IEEE 802.3ae standard. This adapter requires 9µm single-mode fiber optic cables and uses an LC connector to connect to network infrastructure components. This adapter must be used with a 3957-VEC, 3957-VEB, or 3957-V07.

The default configuration for a TS7700 Server from manufacturing (3957-VEC, 3957-VEB, or 3957-V07) is two dual-ported PCIe 1 Gb Ethernet adapters. For a 3957-VEC you can use FC 1038, 10 Gb dual port optical LW connection to add support for two 10 Gb optical longwave Ethernet adapters. For a 3957-VEB or 3957-V07 you can use FC 1035, 10 Gb grid optical LW connection to add support for two 10 Gb optical longwave Ethernet adapters. This feature improves data copy replication while providing minimum bandwidth redundancy. Configured clusters that use two 10 Gb, four 1 Gb, or two 1 Gb clusters, can be interconnected within the same TS7700 Grid. Adapter types can be mixed within a grid, but not within a single cluster.

Note: A network infrastructure and switches capable of supporting 10 Gb adapters must be in place before installing the 10 Gb optical longwave Ethernet adapters. If the TS7700 Server is a 3957-VEC, two instances of FC 1036, 1 Gb grid dual port copper connection or FC 1037, 1 Gb dual port optical SW connection must be installed. If the TS7700 Server is a 3957-V07 or 3957-VEB, two instances of either FC 1036, 1 Gb grid dual port copper connection or FC 1037, 1 Gb dual port optical SW connection must be installed. If the TS7700 Server is a 3957-V06 or 3957-VEA, it must operate with a microcode level of 8.20.x.x or later and two instances of either FC 1032 1Gb grid dual port copper connection, or FC 1033, 1 Gb grid dual port optical SW connection, must be installed. Refer to the *Feature details* topic in the section **Related information** for feature requirements and prerequisites.

Important: Identify, order, and install any new equipment to fulfill grid installation and activation requirements. Prior to grid activation, you must test connectivity and performance of the Ethernet connections. You must ensure installation and testing of this network infrastructure is complete before grid activation.

Bandwidth considerations

The customer network between the TS7700s should have sufficient bandwidth to account for the total replication traffic. For customers that share network switches among multiple TS7700 paths or with other network traffic, the total of bandwidth on that network should be sufficient to account for all of the network traffic.

The TS7700 uses the TCP/IP protocol for moving data between each cluster. Bandwidth is a key factor that affects throughput for the TS7700. Other key factors that can affect throughput include:

- Latency between the TS7700s
- Network efficiency (packet loss, packet sequencing, and bit error rates)
- Network switch capabilities
- Flow control to pace the data from the TS7700s
- Inter-switch link capabilities: flow control, buffering, and performance

The TS7700 attempts to drive the network links at the full 1 Gb or 10 Gb rate, which might exceed the network infrastructure capabilities. The TS7700 supports the IP flow control frames so that the network paces the level at which the TS7700 attempts to drive the network. The best performance is achieved when the TS7700 is able to match the capabilities of the underlying network, resulting in fewer dropped packets.

Note: When the system exceeds the network capabilities, packets are lost. This causes TCP to stop, resync, and resend data, resulting in a much less efficient use of the network.

To maximize network throughput, ensure that the underlying network:

- Has sufficient bandwidth to account for all network traffic that is expected to be driven through the system to eliminate network contention.
- Can support flow control between the TS7700s and the switches. This allows the switch to pace the TS7700s to the WAN capability. Flow control between the switches is also a potential factor to ensure that the switches can pace their rates to one another. The performance of the switch handles data rates expected from all of the network traffic.

In short, latency between the sites is the primary factor. However, packet loss due to bit error rates or insufficient network capabilities can cause TCP to resend data, thus multiplying the effect of the latency. The TS7700 uses your LAN/WAN to replicate virtual volumes, access virtual volumes remotely, and perform cross-site messaging. The LAN/WAN should have adequate bandwidth to deliver the throughput necessary for your data storage requirements. The cross-site grid network is 1 Gb Ethernet with either shortwave fiber or copper (RJ-45). For copper networks, Cat 5E or 6 Ethernet cabling can be used, but Cat 6 cabling is recommended to achieve the highest throughput. Refer to the *Feature details* topic in the section **Related information** for requirements and prerequisites for the following grid network connections:

3957-VEC connections

- FC 1036, 1 Gb grid dual port copper connection
- FC 1037, 1 Gb dual port optical SW connection
- FC 1038, 10 Gb dual port optical LW connection

3957-V07 or 3957-VEB connections

- FC 1035, 10 Gb grid optical LW connection
- FC 1036, 1 Gb grid dual port copper connection
- FC 1037, 1 Gb dual port optical SW connection

3957-V06 or 3957-VEA connections

- FC 1032, 1 Gb grid dual port copper connection
- FC 1033, 1 Gb grid dual port optical SW connection

The TS7700 does not encrypt the data that it sends over the LAN/WAN.

Note: To avoid any network conflicts, the following subnets must **not** be used for LAN/WAN IP addresses (Gridlink) or management interface primary, secondary, or virtual IP addresses:

- 192.168.251.xxx
- 192.168.250.xxx
- 172.31.1.xxx
- 10.10.10.1
- 10.10.10.2

Network redundancy

The TS7700 provides up to four independent 1 Gb copper (RJ-45) or shortwave fiber Ethernet links for grid network connectivity. It is recommended that you connect each through an independent WAN interconnection to be protected from a single point of failure that would disrupt service to both WAN paths from a node.

Related information

"Feature details" on page 149

Network adapter assignments

This topic gives required assignments for TS7700 network adapters.

Adapter assignments that are required for the TS7700 include:

- TCP/IP address
- Gateway IP address
- Subnet mask

TCP/IP addresses

Local IP addresses for management interface access

You must provide three TCP/IP addresses on the same subnet. Two of these addresses are assigned to physical links, while the third is a virtual IP address used to connect to the TS7700 Management Interface.

The third IP address should be used to access a TS7700; it automatically routes between the two addresses assigned to physical links. The virtual IP address enables access the TS7700 Management Interface by using redundant paths, without the need to manually specify different IP addresses for the different paths. If one path is unavailable, the virtual IP address will automatically connect through the remaining path.

Note: If FC 9900, Tape Encryption configuration, is installed, this same connection is used for communications between the TS7700 and the Encryption Key Server or Tivoli Key Lifecycle Manager (TKLM). Because encryption occurs on attached physical tape drives, encryption support does not exist for non-tape attached instances of the TS7700, and the virtual connection is used exclusively to create redundant paths.

You must provide one gateway IP address.

You must provide one subnet mask address.

Grid WAN IP addresses

For TS7700s configured in a Grid, the following additional assignments need to be made for the Grid WAN adapters. For each adapter, you must supply:

- A TCP/IP address
- A gateway IP address
- A subnet mask

TSSC Network IP addresses

For each cluster in your configuration, you must ensure the availability of five IP addresses on the TSSC network (see Table 49). For an expansion frame, you will need two more IP addresses for each frame per "string" attached to the system (see Table 50). If using Cisco switches for a tape attach system, add two more IP addresses on the TSSC network for each switch (see Table 51).

Note: A TS7700 Cache Controller and its attached TS7700 Cache Drawers are referred to as a "string."

Table 49. Number of TSSC network IP addresses required per cluster

Number of clusters	Total number of IP addresses required on TSSC network
1	5
2	10
3	15
4	20
5	25
6	30

Table 50. Number of extra TSSC network IP addresses required per expansion frame

Number of clusters	Total number of IP addresses required on TSSC network
1	2
2	4
3	6

Table 51. Number of extra TSSC network IP addresses required per tape attach with Cisco switch

Number of clusters	Total number of IP addresses required on TSSC network
1	2
2	4
3	6
4	8
5	10
6	12

Note: The IP address that is used for the master console network must be entered as an increment of 10 between 10 and 240. The TS7700 configuration uses this address and the next nine sequential addresses for master console configuration. To prevent network problems, do **NOT** configure these addresses on this master console for another system.

TSSC IP Address Table and Notes

Note: The terms *Master Console* (MC), *System Console* (SC), and *TotalStorage Master Console* (TSMC) might be encountered on the screens used on various products. All of these terms are used to refer to the *TS3000 system console* (TSSC). The term *Service Console* can refer to the TS3000 system console (TSSC) or the TS4500 integrated management console (IMC).

Table 52. TSSC IP Address Table and Notes

Field	Value	Notes
Service Console IP address	172.31.1.1	IP address of the Service Console.
Service Console Hostname	xxxxxx	tssnet1 is the default setting for the Service Console.
3957-Vxx IP address on the Service Console Network	172.31.1.xx	This is the recommended IP address for the first TS7700 attached to a master console. The last octet of this IP address must be in an increment of 10 between 10 and 240 (that is. 10, 20 ... 230, 240). The TS7700 switch configuration will use this and the following 9 IP addresses (example: .150 - .159) so no other device should be set to an IP address in this range.
Subnet Mask on the Service Console Network	255.255.255.0	

To allow connection to a TSSC network, the IP addresses used by the TS7700 must not conflict with any other TS7700 connected to a common TSSC. Any IP addresses used are TSSC-assigned. Each TS7700 is assigned a range of ten IP addresses, where X is the lowest value in the IP address range and all components within a TS7700 are then assigned IP addresses as a value of X.

Table 53 on page 92 displays the TCP/IP configuration for a TS7740 attached to a TS3500 or TS4500 Tape Library.

Table 53. TS7740 TCP/IP address assignments

Component	Location	Role	TCP/IP address
TS7740 Server	Slot 4, Port 0	TS7740 Inbound Cache Controller/TSSC	172.31.1.(X+7)
	Slot 5, Port 0	TS7740 Inbound Cache Controller/TSSC	172.31.1.(X+8)
	Slot 4, Port 1	Inbound management interface/customer key server/LDAP/SNMP	Customer assigned
	Slot 5, Port 1	Inbound management interface/customer key server/LDAP/SNMP	Customer assigned
	Slots 4 and 5, Ports 0	TS7740 Inbound Cache Controller/TSSC	172.31.1.X (Virtual IP address [VIPA])
	Slots 4 and 5, Ports 1	Inbound management interface	Customer assigned (VIPA)
I/O drawers	Drawer 0, Slot 1, Port 0	Cross-cluster WAN	Customer Assigned
	Drawer 0, Slot 1, Port 1 (dual port)		
	Drawer 1, Slot 1, Port 0		
	Drawer 1, Slot 1, Port 1 (dual port)		
TS7740 Cache Controller	CEC 0	TS7740 Cache Controller	172.31.1.(X+1)
	CEC 1		172.31.1.(X+2)

Table 53 displays the TCP/IP configuration for a TS7720.

Table 54. TS7720 TCP/IP address assignments

Component	Location	Role	TCP/IP address
TS7720 Server	Slot 4, Port 0	TS7720 Inbound Cache Controller/TSSC	172.31.1.(X+7)
	Slot 5, Port 0	TS7720 Inbound Cache Controller/TSSC	172.31.1.(X+8)
	Slot 4, Port 1	Inbound management interface/customer key server/LDAP/SNMP	Customer assigned
	Slot 5, Port 1	Inbound management interface/customer key server/LDAP/SNMP	Customer assigned
	Slots 4 and 5, Ports 0	TS7720 Inbound Cache Controller/TSSC	172.31.1.X (VIPA)
	Slots 4 and 5, Ports 1	Inbound management interface	Customer assigned (VIPA)
I/O drawers	Drawer 0, Slot 1, Port 0	Cross-cluster WAN	Customer Assigned
	Drawer 0, Slot 1, Port 1 (dual port)		
	Drawer 1, Slot 1, Port 0		
	Drawer 1, Slot 1, Port 1 (dual port)		

Table 54. TS7720 TCP/IP address assignments (continued)

Component	Location	Role	TCP/IP address
TS7720 Cache Controller	CEC 0, 3952 Base Frame	TS7720 Cache Controller	172.31.1.(X+1)
	CEC 1, 3952 Base Frame		172.31.1.(X+2)
	Controller 0 (bottom) CEC 0, 3952 Storage Expansion Frame		172.31.1.(X+3)
	Controller 0 (bottom) CEC 1, 3952 Storage Expansion Frame		172.31.1.(X+4)
	Controller 1 (top) CEC 0, 3952 Storage Expansion Frame		172.31.1.(X+5)
	Controller 1 (top) CEC 1, 3952 Storage Expansion Frame		172.31.1.(X+6)

Table 53 on page 92 displays the TCP/IP configuration for a TS7760.

Table 55. TS7760 TCP/IP address assignments

Component	Location	Role	TCP/IP address
TS7760 Server	Slot 10, Port 1	TS7760 Inbound Cache Controller/TSSC	172.31.1.(X1+7)
	Slot 11, Port 1	TS7760 Inbound Cache Controller/TSSC	172.31.1.(X1+8)
	Slot 10, Port 3	Inbound management interface/customer key server/LDAP/SNMP	Customer assigned
	Slot 11, Port 3	Inbound management interface/customer key server/LDAP/SNMP	Customer assigned
	Slots 10 and 11, Ports 1	TS7760 Inbound Cache Controller/TSSC	172.31.1.X1 (VIPA)
	Slots 10 and 11, Ports 3	Inbound management interface	Customer assigned (VIPA)†
I/O drawers	Drawer 0, Slot 1, Port 0	Cross-cluster WAN	Customer Assigned
	Drawer 0, Slot 1, Port 1 (dual port)		
	Drawer 1, Slot 1, Port 0		
	Drawer 1, Slot 1, Port 1 (dual port)		
	Drawer 0, Slot 5, Port 1	16 Gb Fibre Channel switch (Tape attach only)	172.31.1.(X1+9)
	Drawer 1, Slot 5, Port 1	16 Gb Fibre Channel switch (Tape attach only)	172.31.1.(X1+10)

Table 55. TS7760 TCP/IP address assignments (continued)

Component	Location	Role	TCP/IP address
TS7760 Cache Controller	CEC 0, 3952 Base Frame	TS7760 Cache Controller	172.31.1.(X+1)
	CEC 1, 3952 Base Frame		172.31.1.(X+2)
	Controller 0 CEC 0, 3952 Storage Expansion Frame 2		172.31.1.(X+3)
	Controller 0 CEC 1, 3952 Storage Expansion Frame 2		172.31.1.(X+4)
	Controller 0 CEC 0, 3952 Storage Expansion Frame 3		172.31.1.(X+5)
	Controller 0 CEC 1, 3952 Storage Expansion Frame 3		172.31.1.(X+6)

†You should have 3 IPs for the Virtual IP Addresses (VIPA). 2 IP addresses will be assigned to the physical ports and 1 IP address will point to the 2 IP addresses assigned to the physical ports.

Using IPv6 and IPSec

Internet Protocol Version 6 (IPv6) is the next evolution in Internet Protocol beyond the IPv4 standard currently in use in most networks today. The key IPv6 enhancement is the expansion of the IP address space from 32 bits to 128 bits, enabling virtually unlimited IP addresses. This addressing capability, along with new functions enabling end-to-end security, improved mobility support, simplified address configuration and management, make IPv6 a critical component in the evolution of e-business and the next generation Internet. IPSec is a security enhancement tool used in securing Internet Protocol communications by authenticating and encrypting every setup communication session in a TS7700.

Prerequisites

Your network must support IPv6 addresses.

IPv6 addresses must exist for your network and the TSSC.

Each TSSC attached to a cluster must be configured for IPv6 addresses if AOTM is to be used with IPv6.

Limitations

Supported TS7700 Servers include only 3957-V07, 3957-VEB, and 3957-VEC.

Grid cluster link functionality is not supported for use with IPv6.

Grid cluster link with code level 8.30.x.x and higher on ALL clusters in the Grid supports IPSec.

IPSec is not enabled by default.

Note: Enabling IPSec negatively affects system performance.

Dynamic host configuration protocol (DHCP), which allows a server to assign network IP addresses, is not supported for use with IPv6.

You cannot simultaneously enable IPv4 and IPv6.

You can use the TS7700 Management Interface to enable IPv6.

1. Log in to the management interface for the cluster on which you want to enable IPv6.

2. Open **Settings>Cluster Network Settings**. Select **Customer IP Addresses**.
3. Select the **IPv6** radio button.
4. Enter values for these required fields:
   - Primary Address
   - Secondary Address
   - Prefix Length
5. Click **Submit**.

You can use the TS7700 Management Interface to enable IPSec.

1. From any cluster, log in to the management interface.
2. Open **Settings>Cluster Network Settings**. Select **Encrypt Grid Communication**.
3. Enter in a password that will be used as an encryption key.
4. Check the box next to each cluster communication path to enable IPSec.
5. Click **Submit**.

Note: You can select a communication path between two clusters only if both clusters meet all the following conditions:

- They are online.
- They operate at microcode level 8.30.0.x or later.
- They operate by using IPv6-capable servers (3957-V07/VEB/VEC).

Note: If you enable Encrypt Grid Communication (IPsec), the performance of the grid network might be decreased by 70% or more.

Related information

"Planning for new system arrival (customer tasks)" on page 211

Network switches and TCP/IP ports requirements

This topic gives network switch and TCP/IP ports requirements for the WAN of a TS7700 in grid configuration.

Note: These requirements apply only to the grid LAN/WAN; the TS7700 network is managed and controlled by internal code.

Table 56 displays TCP/IP port assignments for the grid WAN.

Table 56. Grid WAN TCP/IP port assignments

Link	TCP/IP port	Role
TS7700 Management Interface	ICMP	For dead gateway detection
	123	Network time protocol (UDP) time server
	443	Access the TS7700 Management Interface (HTTPS)
	80	Access the remote management interface when clusters are operating at different microcode levels (HTTP)
	1443	Encryption key server (secure socket layer [SSL])
	3801	Encryption key server (TCP/IP)

Table 56. Grid WAN TCP/IP port assignments (continued)

Link	TCP/IP port	Role
TS7700 Grid	ICMP	Check cluster health
	9	Discard port for speed measurement between grid clusters
	80	Access the remote management interface when clusters are operating at different microcode levels (HTTP)
	123	Network time protocol (NTP) time server
	1415	WebSphere message queues (grid-to-grid)
	1416	WebSphere message queues (HDM-to-HDM)
	443	Access the TS7700 Management Interface
	5988	CIM Server
	350	TS7700 file replication (distributed library file transfer)
	20	Recommended to remain open for FTP data
	21	Recommended to remain open for FTP control
	500	IPsec Key Exchange (TCP and UDP): must remain open when grid encryption is enabled
	8500	IPsec Key Exchange (TCP and UDP): must remain open when grid encryption is enabled
TSSC External	80	Call home
	443	
	53	Recommended to remain open for domain name server (DNS)
	ICMP	
TSSC Grid	80	Autonomic Ownership Takeover Mode (AOTM)
	22	Recommended to remain open
	443	
	9666	
	ICMP	

Related information

"Network adapter assignments" on page 89

Planning for virtual and physical volumes

As part of your planning process, you need to determine the number of virtual and stacked physical volumes required for your workload.

The topics in this section provide information to help you determine the total number of virtual volumes that are required, suggestions about the volume serial number (VOLSER) ranges to define and the number of physical volumes required. The VOLSER of the virtual and physical volumes must be unique throughout a system-managed storage complex (SMSplex) and throughout all storage hierarchies such as DASD, tape, and optical storage media. To minimize the risk of misidentifying a volume, the VOLSER should be unique throughout the grid and across different clusters in different TS3500 or TS4500 libraries.

Volume serial numbering

This topic describes the volume serial numbers (VOLSERs) used to identify virtual and physical volumes.

The TS7700 determines how to establish increments of VOLSER values based on whether the character in a particular position is a number or a letter. For example, inserts starting with ABC000 and ending with ABC999 add virtual volumes with VOLSERs of ABC000, ABC001, ABC002...ABC999 into the inventory of the TS7700.

Note: A valid volume serial number (VOLSER) is a 6-digit sequence number composed only of uppercase alphabetic characters [A-Z] and numerals in the range [0-9]. Embedded blank spaces cannot be used.

Plan for growth by reserving multiple ranges for each installed TS7700.

Note: Multiple TS7700s in a grid configuration share the same ranges; reservation of multiple ranges applies only to TS7700s that are part of different composite libraries.

Related information

"Physical volume planning" on page 99

Virtual volume planning

Use this section to determine the number of virtual volumes required to accommodate the workload you are planning for the TS7700.

A TS7700 supports a maximum of four million virtual volumes. To determine the number of virtual volumes that are required to accommodate your workload consider:

- The size of your virtual volumes
- The number of scratch volumes needed per day
- The time required for return-to-scratch processing
- How often scratch processing is performed

Size of virtual volumes

The TS7700 supports virtual volumes with maximum sizes of 400, 800, 1000, 2000, 4000, and 6000, and 25000 MiB. Effective sizes can be even larger if data is compressed. For instance, if your data compresses with a 3:1 ratio, the effective maximum virtual volume size for a 4000 MiB virtual volume is 12000 MiB.

Important: Since immediate mode copies take place in their entirety after a volume is closed, the ability to replicate 6000 MB volumes increases the copy and Rewind-Unload (RUN) device end holding time by 50% over 4000 MB volumes. The immediate mode replication policy is not optimal for use with 6000 MB volumes.

Depending on the virtual volume sizes that you choose, the number of volumes that are required to store your data can change depending on the media size from which you are converting. If you currently store your data on native 3490 cartridges, the number of virtual volumes that are needed likely remains the same, except multi-volume data sets. If you migrate a multi-volume data set that uses native 3490 Enhanced Capacity cartridges (800 MiB) and your target virtual volume size is 4000 MiB, then approximately five of the original volumes of a multi-volume data set can fit on one virtual volume. In this scenario, the number of virtual volumes that are needed is reduced. If your data sets currently fill native 3590 volumes you would need many more virtual volumes to store your data (as multi-volume sets), even using 4000 MiB virtual volumes.

A virtual volume's size can be set by VOLSER and can change dynamically using the DFSMS (data facility system managed storage) Data Class storage construct. You can specify 400 MiB CST (cartridge stored tape)-emulated cartridges or 800 MiB with ECCST (extended capacity cartridge storage tape)-emulated cartridges when adding volumes to the TS7700. You can use these sizes without modification or use policy management to override those sizes to provide for the 400, 800, 1000, 2000, 4000, and 6000, and 25000 MiB sizes.

The amount of data that is copied to the stacked cartridge is only the amount of data that has been written to a virtual volume. The choice between all available virtual volume sizes does not affect the real space used in either the TS7700 Cache or the stacked volume. In general, unless you have a special need for CST emulation (400 MiB), specify the ECCST media type when inserting volumes in the TS7700.

Number of scratch volumes needed per day

As you run your daily production workload, plan for enough virtual volumes in scratch status to support the data that is written to the TS7700. This could be hundreds or thousands of volumes, depending on your workload. More than a single day's worth of scratch volumes should be available at any point in time.

Time required for return-to-scratch processing

Return-to-scratch processing involves running a set of tape management tools that identifies the virtual volumes that no longer contain active data and then communicating with the TS7700 to change the status of those volumes from private to scratch. The amount of time the process takes depends on the type of tape management system being employed and how busy the TS7700 is when it is processing the volume status change requests and whether a grid configuration is being used. You should expect that when a TS7700 is not handling a daily workload peak that up to 5000 virtual volumes per hour can be returned to scratch for a single cluster and up to 2500 virtual volumes per hour can be returned to scratch in a two-cluster grid configuration.

To modify according to preferred configuration, refer to *Define virtual volume expiration time* and to the description of Set Expire Hold in *Categories*.

How often return-to-scratch processing is performed

If the number of virtual volumes that are used daily is small (less than a few thousand), you can choose to perform return-to-scratch processing only every few days. A good rule of thumb is to plan for no more than a four-hour time period to run return to scratch. By ensuring a nominal run time of four hours, enough time exists during first shift to run the process twice should problems be encountered during the first attempt. For example, assume that you use 2000 scratch volumes per night on a two-cluster grid configuration. A four-hour return-to-scratch period returns up to 10000 virtual volumes to scratch status. Running return-to-scratch processing every five days would keep up with the rate at which the scratch virtual volumes are being used. Therefore, running return-to-scratch every three or four days would provide some buffer in the number of available scratch virtual volumes.

In planning for the number of virtual volumes that are needed, first determine the number of private volumes that make up the current workload being migrated. One way to do this is by looking at the amount of data on your current volumes and then matching that to the supported virtual volume sizes. You would match the volume sizes taking into account the compressibility of your data. If you do not know what the average ratio is, a conservative value of 2:1 may be used.

If you define more volumes than you need, at a later time you can delete the additional volumes; unused virtual volumes do not consume space. Refer to the topic *Physical volumes* linked from the **Related information** section for implications of a large number of previously used, but now scratch, virtual volumes.

Preferred migration of scratch volumes

TS7700 Tape Attach Clusters operating at microcode level 8.21.0.xx or later use the preferred migration of scratch volumes enhancement, which migrates scratch volumes before migrating non-scratch volumes. This enhancement modifies the least recently used (LRU) algorithm to ensure that more critical data remains in cache for a longer period of time.

Under this preferred migration, hierarchical storage management (HSM) first migrates all volumes in a scratch category according to size (largest first). Only when all volumes (PG0 or PG1) in a scratch category have been migrated and the PG1 threshold is still unrelieved does HSM begin to operate on private PG1 volumes in LRU order.

Note: You must define all scratch categories prior to using the preferred migration enhancement.

Related information

"Allocation assistance" on page 290

"Physical volume planning"

"Define virtual volume expiration time" on page 246

Physical volume planning

Use this section to determine the number of physical volumes that are required to accommodate the workload you are planning for the TS7740, the TS7720 tape attach, or the TS7760 tape attach.

To determine the number of physical volumes that are required to accommodate your workload, consider:

- "Amount of data stored for a given host workload"
- "Average compression ratio achieved per workload" on page 100
- "Average utilization rate of filling physical volumes" on page 100
- "Scratch physical volumes" on page 100

Amount of data stored for a given host workload

The amount of data that is stored per workload can be extracted from your Tape Management System, such as RMM, or from TS7700 by using VEHSTATS.

Average compression ratio achieved per workload

The data that a host writes to a virtual volume might be compressible. The space that is required on a physical volume is calculated after the effect of compression. If you do not know the average number for your data, assume a conservative 2:1 ratio.

Average utilization rate of filling physical volumes

The average utilization rate of filling physical volumes can be calculated from the Reclaim Threshold Percentage. The percentage that is used to determine when to perform reclamation of free storage on a stacked volume. When the amount of active data on a physical stacked volume drops below this percentage, a reclaim operation is performed on the stacked volume. The valid range of possible values is 0 - 95%; 35% is the default value. Therefore, the utilization rate of filling physical volumes should range from 35% to 100%. The average utilization rate of filling physical volumes can be calculated as (35+100)/2 = 67.5%.

Scratch physical volumes

You should refer the following diagram to determine the number of scratch physical volumes you need for each pool.

1. **Is the E08 or E07 drive installed?**
   - Yes
     a. **Is borrow/return sharing enabled?**
        - Yes: 15 volumes in the common scratch pool
        - No: 15 volumes in each dedicated pool
   - No
     a. **Is borrow/return sharing enabled?**
        - Yes: 50 volumes in the common scratch pool
        - No: 50 volumes in each dedicated pool

If the number of scratch physical volumes in your system is fewer than these thresholds:

- Reclamation of sunset media does not occur
- Reclamation runs more frequently

You can have less than 15 or 50 volumes in your pool if these conditions are acceptable. Keep in mind that you need at least 2 scratch physical volumes to avoid an out of scratch state.

The following is a suggested formula to calculate the number of physical volumes needed:

Where:

Pv =	Total number of physical volumes needed
Da =	Total amount of data that is returned from your Tape Management System or VEHSTATS per workload
Cr =	Compression Ratio per workload (Use Cr=1 when Da represents previously compressed data)
Ut =	Average utilization rate of filling physical volumes
Pc =	Capacity of a physical volume in TB
Px =	Resulting number of physical volumes needed for a particular workload "x"

Ps = Number of physical volumes in common scratch pool

For each workload, calculate the number of physical volumes needed:
`Px = (Da/Cr)/(Pc × Ut/100)`

Next, add in physical scratch counts and the Px results from all known workloads:
`Pv = Ps + P1 + P2 + P3 + ...`

For example, by using the following assumptions:

Workload 1

Da	=	100 TB
Cr	=	2
Ut	=	67.5%
Pc	=	10 TB (capacity of a JD volume)

`P1 = (100/2)/(10 × 67.5/100) = 8` physical volumes

Workload 2

Da	=	150 TB
Cr	=	2
Ut	=	67.5%
Pc	=	7 TB (capacity of a JC volume in 3592-E08 format)

`P2 = (150/2)/(7 × 67.5/100) = 16` physical volumes

If the number of physical volumes in the common scratch pool is Ps = 15, you would need to plan on the following number of physical volumes in the TS7740, the TS7720 tape attach, or the TS7760 tape attach:

`Pv = Ps + P1 + P2 = 15 + 8 + 16 = 39` physical volumes

If you need dual copied virtual volumes, you need to double the number of physical volumes for that workload. If a workload uses dedicated pools with the borrow/return sharing disabled, then each workload must have its own dedicated additional scratch count versus the shared Ps count.

Migrating data to a new media type

You can migrate data from an existing media type to a new media type for use with a TS7700.

Note: Migration from a VTS B10/B20 is a service now provided by Global Technical Services. For additional information concerning VTS features please refer to *IBM TotalStorage Virtual Tape Server: Planning, Implementing, and Monitoring Redbook, SG24-2229*, available from the *IBM Support & Downloads* web page link in the **Related information** section.

Three paths exist to migrate data to a new media type:

Natural reclamation

Natural reclamation is the most efficient method to migrate data to a new media type. Follow these steps to migrate data using natural reclamation:

1. Insert the new media type into the library.
2. Open the *Modify pool properties* panel of the management interface for the TS7700 attached to the library.

3. In the **First Media (Primary)** field, select the NEW media type that you want to migrate data to. All new physical mounts for volume stacking use this media type.
4. In the **Second Media (Secondary)** field, select **none**. Any data on the existing, OLD media becomes read only.
5. When natural reclamation occurs, data is migrated from the old media to the new media designated by the **First Media (Primary)** field. All empty, old media is returned to a scratch state.
6. Open the *Eject physical volumes* panel of the management interface.
7. Use the **Eject Range of Scratch Only Volumes** field to eject old media that is empty or has been returned to scratch. You can narrow the range of volumes ejected using the **Media Type** option.

Forced eject

You can use a forced eject to migrate data to a new media type. Follow these steps to migrate data using forced eject:

1. Insert the new media type into the library.
2. Open the *Modify pool properties* panel of the management interface for the TS7700 attached to the library.
3. In the **First Media (Primary)** field, select the NEW media type that you want to migrate data to. All new physical mounts for volume stacking use this media type.
4. In the **Second Media (Secondary)** field, select **none**. Any data on the existing, OLD media becomes read only.
5. Open the *Eject physical volumes* panel of the management interface.
6. Use the **Eject Range of Physical Volumes** field and the **Media Type** option to eject the old media. All empty media of the old media type are ejected. Any volumes on the old media type that have virtual volume stacked content are first reclaimed, then ejected. The reclamation process moves content from the old media to the new media.

Note: You can use the force eject method in combination with the natural reclamation method to migrate data from outlier media that escape natural reclamation due to minimal data expiration.

Virtual volume move

You can use a virtual volume move operation to migrate data to a new media type, but this is the least optimal alternative. Follow these steps to migrate data using a virtual volume move:

1. Insert the new media type into the library.
2. Open the *Modify pool properties* panel of the management interface for the TS7700 attached to the library.
3. For each pool currently in use (old pool), configure a new version (new pool) with the following media type settings:
   - In the **First Media (Primary)** field, select the NEW media type that you want to migrate data to. All new physical mounts for volume stacking use this media type.
   - In the **Second Media (Secondary)** field, select **none**. Any data on the existing, OLD media becomes read only.
4. Modify constructs through the management interface so that all new allocations use the newly created pools.
5. Open the *Move virtual volumes* panel on the management interface.

6. In the **Existing Ranges** field, select a range that is associated with the old media type.
7. In the **Target Pool** field, select the new pool.
8. In the **Media Type** field, select the new media type.
9. Select **Move** to begin the move operation. Data on the old media is reclaimed and moved to the new pool on the new media.
10. Complete steps 6 through 9 for each pool on the old media. Each pool must be moved individually.
11. Open the *Eject physical volumes* panel of the management interface.
12. Use the **Eject Range of Physical Volumes** field and the **Media Type** option to eject the old media.
13. Open the *Modify pool properties* panel of the management interface for the TS7700 attached to the library.
14. Deconfigure each old pool no longer in use.

Related information

"Quick reference by component" on page 143

"Feature details" on page 149

http://www.ibm.com/support/us/en/

Merging clusters or grids

You can add an existing TS7700 Cluster to another cluster or TS7700 Grid. You can also merge two existing TS7700 Grids.

Related information

"Adding TS7700 Clusters to a grid" on page 111

"Feature details" on page 149

"TS7700 Cache thresholds and removal policies" on page 276

Merging clusters

You can add an existing TS7700 Cluster to an existing TS7700 Grid or to another existing TS7700 Cluster to form a grid for the first time.

An installed and operational TS7700 Cluster that contains data can be merged with a previously installed and operational TS7700 Cluster or TS7700 Grid. Refer to the topic "Adding TS7700 Clusters to a grid" on page 111 in the **Related information** section for available cluster merge scenarios.

Important: You cannot insert or eject any virtual or physical volumes during a grid join. Do not begin the merge operation until all insert and eject operations are complete on all clusters in both grids.

FC 4015, Grid enablement must be installed on all TS7700 Clusters that operate in a grid configuration. All clusters must operate at the same microcode level, and the microcode level must be 8.21.0.xx or later.

You might need to access the merging cluster before it becomes part of a grid (for example, to remove duplicate volumes that would prevent a successful grid join). Plan to complete any access to the soon-to-be merged (stand-alone) cluster before initiating any host configuration changes. Plan for the following host configuration changes, which must be completed before using the newly-joined cluster:

- All HCDs (hardware configuration definition: the MVS [multiple virtual storage] component that builds the I/O definitions), subsystem IDs, and Port IDs must be updated.
- The RMM (Removal Media Manager) and volcat (volume category) ranges must be updated within their respective storage groups. These ranges must be unique to ensure that the merge proceeds as expected. Updating the ranges is necessary to maintain continued access to the original volumes that were created when the system(s) were configured as stand-alone cluster(s).

Plan to define the following management and data policies after the TS7700 Cluster merge is complete:
- Define stacked volume ranges
- Define scratch categories
- Define the expired virtual volume data policy
- Define inhibit reclaim schedule

  Note: Prior to microcode level 8.5.0.xx, inhibit reclaim schedules were designated by using local time instead of Coordinated Universal Time (UTC). If you have upgraded from a microcode level of 8.4.0.xx, verify that your inhibit reclaim schedule displays the correct day and time before you start an inhibit reclaim operation using the new code version.
- Define reclaim threshold percentage

If categories and constructs are already defined on the merging cluster, verify that the total number of each category and construct that will exist in the grid following the merge does not exceed 256. If necessary, delete existing categories or constructs from the merging clusters before the grid join occurs.

Each TS7700 Grid supports a maximum of 256 of each of the following categories and constructs:
- Scratch categories
- Management Classes
- Data Classes
- Storage Classes
- Storage Groups

Important: Each TS7700 Grid supports a maximum of four million virtual volumes (available with FC 5270 when operating at microcode level 8.30.0.xx or later, or by RPQ otherwise). Verify that the total number of virtual volumes to exist in the grid following the merge does not exceed four million. If necessary, remove existing virtual volumes from the merging clusters before the grid join occurs. Verify that no duplicate VOLSERs exist between the merging clusters. Each cluster within the TS7700 Grid must have at least 16 GB of physical memory installed before four million virtual volumes are supported. Verify that each cluster possesses enough physical memory before merging clusters.

Related information

"Adding TS7700 Clusters to a grid" on page 111

"Feature details" on page 149

"TS7700 Cache thresholds and removal policies" on page 276

Merging grids

You can merge two existing TS7700 Grids to create a larger grid. This solution permits you to keep redundant copies of data within both grids during the entire merge process versus needing to remove one or more clusters first and exposing them to a single copy loss condition.

This solution permits merging of two grids while retaining redundant copies of data within both grids during the merge process. By this method, it is not necessary to first remove one or more clusters from a grid, avoiding exposure to a single copy loss condition.

The following restrictions apply:

- Cluster joins at different TS7700 microcode levels are supported when the existing cluster x is at 8.21.x.x or later.
- The final resulting grid configuration cannot have more than three different microcode levels. The microcode level is shown on the login screen. For example, cluster 0 at 8.30.1.15, cluster 1 at 8.30.1.15, cluster 2 at 8.21.0.163, and cluster 3 at 8.32.0.x is valid; cluster 0 at 8.30.0.87, cluster 1 at 8.30.1.15, cluster 2 at 8.21.0.163, and cluster 3 at 8.32.0.x is not valid.
- Feature codes on both grids must be compatible
- All cluster IDs must be unique
- All virtual volumes must be unique
- The new (merging) grid should have fewer virtual volumes than the existing (receiving) grid
- The total number of virtual volumes in the grid cannot exceed four million
- The final, merged grid cannot contain more than eight clusters.

Feature Codes

All clusters in a grid must have FC 4015 (Grid Enablement) installed before the beginning of the merge. This feature is typically installed in manufacturing. However, it is possible that a TS7700 ordered originally as a stand-alone cluster does not have FC 4015 installed. In this instance, FC 4015 must be purchased and installed before the beginning of the merge. Use the installation instructions and license key that are delivered with FC 4015 to complete the grid configuration before beginning the merge operation.

To maximize the full number of virtual volumes that are supported on the grid, the quantity of installed instances of FC 5270 and FC 5271 must be the same for all clusters in the final, merged grid. If this requirement is not met, then the number of volumes that the grid supports is determined by the cluster with the lowest number of FC 5270 and FC 5271 instances installed.

To create a grid with more than two clusters, first create a two-cluster grid by using one of the following conditions:

- If one cluster is empty and another cluster contains data (an existing cluster), join the empty cluster to the existing cluster
- If both clusters are empty or both clusters have data, it is suggested to join the higher-numbered cluster to the lower-numbered cluster (i.e. cluster 1 to cluster 0) to form a grid

Complete the worksheet **TS7700 Grid local addresses** in the topic *Planning for new system arrival (customer tasks)* in preparation for any upcoming merge operation. A link to this topic is in the **Related information** section.

Related information

"Adding TS7700 Clusters to a grid" on page 111

"Feature details" on page 149

"Planning for new system arrival (customer tasks)" on page 211

"TS7700 Cache thresholds and removal policies" on page 276

TS7700 upgrade options

This section contains information about field-installable upgrades that enable onsite configuration of the TS7700.

Related information

"TS7700 Grid" on page 257

FC 1031, 1-Gb optical SW connection

FC 1032, 1-Gb Grid copper connection

FC 1033, 1-Gb Optical SW connection

FC 1034, Enable Dual Port Grid Connection

FC 1036, 1-Gb Grid Dual Port Copper Connection

FC 1037, 1-Gb Grid Dual Port Optical SW Connection

FC 1038, 10-Gb Dual Port Grid Optical LW Connection

FC 3401, Enable 8-Gb FICON dual port

FC 3438, 8-Gb FICON Short Wavelength Attachment

FC 3439, 8-Gb FICON Long Wavelength Attachment

FC 3441, FICON short-wavelength attachment

FC 3442, FICON long-wavelength attachment

FC 3443, FICON 10–km long-wavelength attachment

FC 4015, Grid enablement

FC 4880, 16 Gb Fibre Channel Switch

FC 5242, Dual Port 16-Gb Fibre Channel HBA

FC 5268, 100-MB/sec increment

FC 5659, Field install 3956-XSA

FC 5656, Field install 3956-XS9

FC 9218, Attach to 3494 LM

FC 9323 Expansion frame attachment

Attach to TS3500

http://www.ibm.com/support/us/en/

Concurrent TS7700 upgrade options

Concurrent system upgrades can be installed while the TS7700 is online and operating.

The following component upgrades can be made concurrently to an existing, onsite TS7700:

Incremental disk cache capacity
You can add a 1 TB (0.91 TiB) increment of disk cache to store virtual

volumes, up to 28 TB (25.46 TiB). Use "FC 5267, 1 TB cache enablement" on page 162 to achieve this upgrade. This feature is only available with a TS7740.

Incremental data throughput

You can add a 100-MB/sec increment of peak data throughput, up to your system's hardware capacity. When the maximum number of performance increments are installed, the system no longer restricts performance. Use "FC 5268, 100 MB/sec increment" on page 162 to achieve this upgrade.

Peak data throughput increments of 100 MB/sec are available as transferred from a host to a vNode before compression. If additional peak data throughput capacity is needed, up to 10 more increments can be ordered for the 3957-V07/VEB when FC 3441/3442/3443 (4 Gb FICON) is installed, or up to 24 can be ordered for the 3957-V07/VEB/VEC when FC 3438/3439 (8 Gb FICON) is installed (to complement "FC 9268, Plant installation of 100 MB/s throughput" on page 178 installed at the plant). If the maximum number of increments is installed, the TS7700 places no limits on data transfers through the cluster. This installation is performed by you through the TS7700 Management Interface by entering the license key obtained with the purchase of "FC 5268, 100 MB/sec increment" on page 162.

Note: All host data transfers through the TS7740 Cluster are considered for the data transfer limit regardless of which TS7740 Cluster initiated or received the data transfer.

Selective device access control

You can grant exclusive access to one or more VOLSER ranges by only certain logical control units or subsystem IDs within a composite library for host-initiated mounts, ejects, and changes to attributes or categories. Use "FC 5271, Selective device access control" on page 163 to add this upgrade. For more nformation, see *Selective device access control* in the **Related information** section. This feature is available only with a microcode level of 8.20.0.xx or later.

Increased virtual volumes

You can add support for additional virtual volumes in 200,000 volume increments, up to a total of four million virtual volumes. Use "FC 5270, Increased virtual volumes" on page 162 to achieve this upgrade.

Note: In a grid configuration, the maximum number of supported virtual volumes is determined by the cluster having the fewest installed instances of FC 5270, Increased virtual volumes. In order to increase the number of supported virtual volumes across a grid, the required number of FC 5270, Increased virtual volumes, must be installed on each cluster in the grid.

Dual port grid connection

You can concurrently enable the second port of each dual port, 1 Gb grid connection adapter in the following TS7700 Server configurations:

- On a 3957-V07, 3957-VEB, or 3957-VEC when "FC 1036, 1 Gb grid dual port copper connection" on page 153 or "FC 1037, 1 Gb dual port optical SW connection" on page 153 are present.
- On a 3957-VEC when "FC 1038, 10 Gb dual port optical LW connection" on page 153 is present.

Use "FC 1034, Enable dual port grid connection" on page 152 to achieve these upgrades.

Note: A non-concurrent install is required to change grid adapters to a different configuration.

TS7700 Expansion Frame

You can add up to two cache expansion frames to a fully configured TS7760 using "FC 9323 Expansion frame attachment" on page 179 and applying "FC 7334, TS7700 Encryption-capable expansion frame" on page 175 to a 3952 F06 Tape Frame. For upgrade requirements, configurations, and feature details, refer to the topics *Upgrades specific to the TS7760* and *Feature details* in the **Related information** section.

You can add up to two cache expansion frames to a fully configured TS7720 using "FC 9323 Expansion frame attachment" on page 179 and applying "FC 7323, TS7720 Storage expansion frame" on page 174 to a 3952 F05 Tape Frame. For upgrade requirements, configurations, and feature details, refer to the topics *Upgrades specific to the TS7720* and *Feature details* in the **Related information** section.

Enable 1 TB pending tape capacity (feature code 5274)

Each instance of "FC 5274, Enable 1 TB Pending Tape Capacity" on page 163, enables up to 1 TB of data to be pending migration to physical tape. Up to 10 instances can be installed.

Disk encryption

You can encrypt the disk drive modules (DDMs) within a TS7700 disk storage system. Refer to "Disk encryption" on page 128 for details and prerequisites.

Related information

"Feature details" on page 149

"Selective device access control" on page 292

"TS7700 Grid" on page 257

"TS7700 feature codes" on page 143

"Upgrades for the TS7760" on page 113

"Upgrades for the TS7720 " on page 116

http://www.ibm.com/support/us/en/

Non-concurrent TS7700 upgrade options

Non-concurrent upgrades require the TS7700 to be brought offline prior to installation.

The following component upgrades must be made non-concurrently to an existing, onsite TS7700. In some instances, the targeted component must be reconfigured before the upgrade takes effect.

TS7720 /TS7760 enable tape attach

For TS7720 /TS7760 servers (VEB/VEC hardware), use the following features to upgrade and enable the server to attach to a tape library:

- "FC 5273, TS7720/TS7760 Tape Attach enablement" on page 163
- "FC 5274, Enable 1 TB Pending Tape Capacity" on page 163

Before installing the features, ensure that all prerequisites are met.

Ethernet adapters for grid communication

Shortwave fibre Ethernet

You can add a 1-Gb shortwave fibre Ethernet adapter for grid communication between TS7700s.

For a TS7760 Server (3957-VEC) use “FC 1037, 1 Gb dual port optical SW connection” on page 153 to achieve this upgrade.

For a 3957-V07 or 3957-VEB use “FC 1037, 1 Gb dual port optical SW connection” on page 153 to achieve this upgrade.

Longwave fibre Ethernet
You can add a longwave fibre Ethernet adapter for grid communication between TS7700s.

For a 3957-VEC use “FC 1038, 10 Gb dual port optical LW connection” on page 153 to achieve this upgrade.

For a 3957-V07 or 3957-VEB use “FC 1035, 10 Gb grid optical LW connection” on page 153 to achieve this upgrade.

Copper Ethernet
You can add a 1-Gb copper Ethernet adapter for grid communication between TS7700s.

For a TS7760 Server (3957-VEC) use “FC 1036, 1 Gb grid dual port copper connection” on page 153 to achieve this upgrade.

For a 3957-V07 or 3957-VEB use “FC 1036, 1 Gb grid dual port copper connection” on page 153 to achieve this upgrade.

Enable four grid Ethernet ports
You can enable two additional ports for grid communication between TS7700s, for a total of four grid Ethernet connections. Use “FC 1034, Enable dual port grid connection” on page 152 to achieve this upgrade.

For a TS7760 Server (3957-VEC) “FC 1036, 1 Gb grid dual port copper connection” on page 153, “FC 1037, 1 Gb dual port optical SW connection” on page 153, or “FC 1038, 10 Gb dual port optical LW connection” on page 153 is also required.

For a 3957-V07 or 3957-VEB “FC 1036, 1 Gb grid dual port copper connection” on page 153 or “FC 1037, 1 Gb dual port optical SW connection” on page 153 is also required.

TS7700 Server dual copper/optical Ethernet swap
You can swap a dual port grid Ethernet adapter in a TS7700 Server for a dual port adapter of the opposite type. You can swap a dual port copper for a dual port optical Ethernet adapter, or swap a dual port optical for a dual port copper Ethernet adapter.

For a TS7760 Server (3957-VEC), use “FC 1036, 1 Gb grid dual port copper connection” on page 153 or “FC 1037, 1 Gb dual port optical SW connection” on page 153 to achieve this upgrade.

For a 3957-V07 or 3957-VEB use “FC 1036, 1 Gb grid dual port copper connection” on page 153 or “FC 1037, 1 Gb dual port optical SW connection” on page 153 to achieve this upgrade.

Additional virtual devices
Each instance of “FC 5275, Additional virtual devices” on page 164 enables up to 16 additional virtual devices (virtual tape drives).

TS7700 Server physical memory upgrade
You can add 16 GB of physical memory to a 3957-V07 or 3957-VEB that contains 16 GB, for a resulting total of 32 GB of physical memory. Use “FC 3462, 16 GB memory upgrade” on page 159 to achieve this upgrade.

TS7700 Server FICON adapter installation

You can install a FICON adapter to connect a TS7700 Server (3957-V07 or 3957-VEB) to a host system. FICON adapter conversion is non-concurrent when used with a 3957-V07 or 3957-VEB. Use “FC 3441, FICON short-wavelength attachment” on page 158, “FC 3442, FICON long-wavelength attachment” on page 158, or “FC 3443, FICON 10-km long-wavelength attachment” on page 158 to achieve this installation.

TS7700 Server 8 Gb FICON adapter installation

You can install up to two 8 Gb FICON adapters or exchange adapters for another type (SW-to-LW or LW-to-SW) to connect a TS7700 Server (3957-V07, 3957-VEB, or 3957-VEC) to a host system. FICON adapter conversion is non-concurrent when used with a 3957-V07, 3957-VEB, or 3957-VEC. Use “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 157, or “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157 to achieve this installation. You can also use “FC 3401, Enable FICON dual port” on page 156 to enable a second 8 Gb FICON adapter port for double the number of host connections.

Important 8 Gb installation information: Due to **higher sensitivity** (increased FICON speed 4G -> 8G) before using a wrap plug or plugging a new or existing cable into any LC Duplex connector, ensure the cable ends and the adapter duplex connector laser transmit/receive ports in the SFP are also cleaned with **Fiber Cleaning Tool P/N 54Y4392** before making a connection. Fibre cables to the affected FICON ports must be undamaged and clean. Use **Fiber Cleaning Tool P/N 54Y4392** to clean FICON host cables and host adapter LC duplex connector. If errors that occur during installation of the 8 Gb FICON adapters and cables are not corrected during cable and SFP cleaning and card replacement then you must contact your cabling contractor.

TS7700 Server 16 Gb FICON adapter installation

You can install up to two 16 Gb FICON adapters or exchange adapters for another type (SW-to-LW or LW-to-SW) to connect a TS7700 Server (3957-VEC) to a host system. FICON adapter conversion is non-concurrent when used with a 3957-VEC. Use “FC 3402, 16 Gb FICON Short Wavelength Attachment” on page 156, or “FC 3403, 16 Gb FICON Long Wavelength Attachment” on page 157 to achieve this installation. You can also use “FC 3401, Enable FICON dual port” on page 156 to enable a second 16 Gb FICON adapter port for double the number of host connections.

TS7700 Server Fibre Channel host bus adapter installation

You can install two Fibre Channel interface cards in the TS7760 Server (3957-VEC) to connect the TS7760 Server to the disk arrays in the TS7760 Storage Expansion Frame. Use “FC 5242, Dual Port 16 Gb Fibre Channel HBA” on page 162 to achieve this installation.

You can install two Fibre Channel interface cards in the TS7720 Server (3957-VEB) to connect the TS7720 Server to the disk arrays in the TS7720 Storage Expansion Frame. Use “FC 5241, Dual port FC HBA” on page 161 to achieve this installation.

Related information

“TS7700 Grid” on page 257

FC 1032, 1 Gb grid dual port copper connection

FC 1033, 1 Gb grid dual port optical SW connection

FC 1035, Grid optical LW connection

FC 1036, 1 Gb grid dual port copper connection

FC 1037, 1 Gb dual port optical SW connection

FC 1038, 10 Gb dual port optical LW connection

FC 5267, 1 TB cache enablement

FC 5268, 100 MB/sec increment

http://www.ibm.com/support/us/en/

Adding TS7700 Clusters to a grid

You can upgrade an existing, on-site TS7700 Grid by adding a TS7700 Cluster. This is referred to as a join. A join is whenever an empty cluster joins an existing cluster or grid with existing data. An empty cluster is one which has not had logical volumes or physical volumes inserted. When you join one cluster to a cluster in an existing grid, all clusters in the existing grid are automatically joined.

The following restrictions apply:

- The joining cluster must not contain any data.
- The joining cluster must operate at microcode level 8.20.0.xx or later.
- The microcode level for the joining cluster must be equal to or later than the microcode level for any existing cluster.
- The existing cluster(s) must operate at microcode level 8.7.0.xx or later.
- The final resulting grid configuration cannot have more than three different microcode levels. The microcode level is shown on the login screen. For example, cluster 0 at 8.30.1.15, cluster 1 at 8.30.1.15, cluster 2 at 8.21.0.163, and cluster 3 at 8.32.0.x is valid; cluster 0 at 8.30.0.87, cluster 1 at 8.30.1.15, cluster 2 at 8.21.0.163, and cluster 3 at 8.32.0.x is not valid.
- If FC 1035 is installed on the joining cluster, the existing infrastructure must support 10 Gbps grid communications for optimal performance.
- When the grid contains virtual volumes with a maximum size of 25000 MiB, and when either one of the following is true, FC 0001 must be installed on every cluster operating at a microcode level earlier than 8.32.0.x:
  - The grid consists only of TS7700 Clusters that are not attached to a physical library (that is, disk-only TS7700 Clusters), or
  - Tape-attached Clusters are added to a grid that previously contained only disk-only Clusters

Table 57 shows joining rules for different microcode levels. For example, it shows what the minimum microcode level is for existing clusters to be joined to a new member with later microcode.

Table 57. Join rules

	Joining	**8.21.x.x**	**8.30.x.x**	**8.31.x.x**	**8.32.x.x**	**8.33.x.x**	**8.40.x.x**	**8.41.x.x**
Existing cluster(s)								
	8.21.x.x	Y	Y	Y	Y	Y	Y	Y
	8.30.x.x	N	Y	Y	Y	Y	Y	Y
	8.31.x.x	N	N	Y	Y	Y	Y	Y
	8.32.x.x	N	N	N	Y	Y	Y	Y
	8.33.x.x	N	N	N	N	Y	Y	Y
	8.40.x.x	N	N	N	N	N	Y	Y
	8.41.x.x	N	N	N	N	N	N	Y

Table 57. Join rules (continued)

Joining	8.21.x.x	8.30.x.x	8.31.x.x	8.32.x.x	8.33.x.x	8.40.x.x	8.41.x.x
1) No more than two microcode levels can be active across all clusters of a grid at any time. Beginning with 8.32.x.x, up to three microcode levels are allowed in a grid (with a minimum of 8.21.x.x). 2) RPQ/SCORE is required. Runtime should be minimized (for example, a few weeks only). The intent is to drain the 8.7.x.x cluster(s) and remove them from the grid.							

To achieve any of the following upgrades, you must order "FC 4015, Grid enablement" on page 159 against the TS7700 Server.

Note: An RPQ is required for any intended 5- way or more Grid configuration.

Two-cluster TS7700 Grid
: You can add a new, empty TS7700 Cluster to an existing TS7700 Cluster to create a two-cluster TS7700 Grid.

  You can combine two existing TS7700 Clusters to create a two-cluster TS7700 Grid.

Three-cluster TS7700 Grid
: You can add a new, empty TS7700 Cluster to an existing two-cluster TS7700 Grid to create a three-cluster TS7700 Grid.

  You can add an existing TS7700 Cluster to an existing two-cluster TS7700 Grid to create a three-cluster TS7700 Grid.

Four-cluster TS7700 Grid
: You can add a new, empty TS7700 Cluster to an existing three-cluster TS7700 Grid to create a four-cluster TS7700 Grid.

  You can add an existing TS7700 Cluster to an existing three-cluster TS7700 Grid to create a four-cluster TS7700 Grid.

Five-cluster TS7700 Grid
: You can add a new, empty TS7700 Cluster to an existing four-cluster TS7700 Grid to create a five-cluster TS7700 Grid.

  You can add an existing TS7700 Cluster to an existing four-cluster TS7700 Grid to create a five-cluster TS7700 Grid.

Six-cluster TS7700 Grid
: You can add two new, empty TS7700 Clusters to an existing four-cluster TS7700 Grid to create a six-cluster TS7700 Grid.

  You can add two existing TS7700 Clusters to an existing four-cluster TS7700 Grid to create a six-cluster TS7700 Grid.

Seven-cluster TS7700 Grid
: You can add two new, empty TS7700 Clusters to an existing five-cluster TS7700 Grid to create a seven-cluster TS7700 Grid.

  You can add two existing TS7700 Clusters to an existing five-cluster TS7700 Grid to create a seven-cluster TS7700 Grid.

Eight-cluster TS7700 Grid
: You can add two new, empty TS7700 Clusters to an existing six-cluster TS7700 Grid to create a eight-cluster TS7700 Grid.

  You can add two existing TS7700 Clusters to an existing six-cluster TS7700 Grid to create a eight-cluster TS7700 Grid.

Related information

"TS7700 Grid" on page 257

"FC 4015, Grid enablement" on page 159

http://www.ibm.com/support/us/en/

http://w3-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD106064

Upgrades for the TS7760

This section describes the use of miscellaneous equipment specifications (MES) to upgrade the TS7760.

TS7760 Tape Attach

The TS7760 can be attached to the TS3500 Tape Library or TS4500 Tape Library.

This functionality is enabled by FC 5273, TS7720/TS7760 Tape Attach enablement. Included with FC 5273 is one instance of FC 5659, Field installation of 3956-XSA, which enables up to 1 TB of data to be pending migration to tape. Additional instances of FC 5274, Enable 1 TB Pending Tape Capacity can be ordered, up to a maximum of 10, to increase the amount of data that is pending migration.

Addition of cache drawers

You can use FC 5659, Field installation of 3956-XSA or FC 5662, Field installation of 3956-XSA with 8 TB DDMs as an MES to add up to a maximum of nine TS7760 Cache Drawers to an existing TS7760 Cache subsystem operating with a 3956-CSA controller.

Note: FC 5659, Field installation of 3956-XSA is the same as FC 5662, Field installation of 3956-XSA with 8 TB DDMs in all aspects, except for the drives that are installed in the drawer.

- If the TS7760/TS7760T has any 8 TB drives already installed in a string, then only 3957-XSA expansion drawers with 8 TB drives can be added. For instance, if the 3957-CSA cache controller and the first 3957-XSA expansion drawer in the string contain 4 TB drives, but the second 3957-XSA expansion drawer contains 8 TB drives, then every other additional 3957-XSA expansion drawer must contain 8 TB drives as well.
- If the cache string has an odd number of drawers (Controller + Expansion drawers) that already contain 4 TB drives, then FC 5659, Field installation of 3956-XSA should be installed first. This will complete the dynamic disk pool (DDP), and ensure that all drawers in the pool contain the same size drives. If FC 5662, Field installation of 3956-XSA with 8 TB DDMs is installed in this scenario, then the 8 TB drives will be configured to use only 4 TB of space to complete the DDP.
- For example: If a TS7760/TS7760T has a 3956-CSA with two 3956-XSA expansion drawers (3 total drawers) that contain 4 TB drives, then the next drawer installed should be FC 5659, Field installation of 3956-XSA which contains 4 TB drives.

Table 58 on page 114 shows the resulting usable capacity associated with each upgrade configuration available to an existing TS7760 Cache.

Table 58. Upgrade configurations for an existing TS7760 Cache

Existing minimum TS7760 Cache configuration	Additional TS7760 Cache Drawer(s) (instances of FC 5659, Field installation of 3956-XSA)	Total count of TS7760 Cache units	Usable capacity
1 TS7760 Cache Controller (3956-CSA)	1	2	62.53 TB (56.87 TiB)
	2	3	93.96 TB (85.46 TiB)
	3	4	125.39 TB (114.04 TiB)
	4	5	156.82 TB (142.63 TiB)
	5	6	188.25 TB (171.21 TiB)
	6	7	219.68 TB (199.79 TiB)
	7	8	251.86 TB (229 TiB)
	8	9	282.53 TB (256.96 TiB)
	9	10	313.96 TB (285.55 TiB)

You can use FC 7334, TS7700 Encryption-capable expansion frame, as an MES to add up to two expansion frames to a fully configured TS7760 Cache subsystem operating with a 3956-CSA controller. Each FC 7334, TS7700 Encryption-capable expansion frame contains one more cache controller, controlling up to fifteen additional expansion drawers. Table 59 on page 115 and Table 60 on page 116 show the resulting usable capacity associated with each upgrade configuration.

Table 59. TS7760 Storage Expansion Frame configurations for 4 TB capacity drives

TS7760 Cache configuration for base frame	**Cache units‡ in eachTS7760 Storage Expansion Frame cache controller (3956-CSA) plus optional cache drawers (3956-XSA)**	**First TS7760 Storage Expansion Frame**		**Second TS7760 Storage Expansion Frame**	
		Total cache units (including TS7760 Base Frame)	**Available capacity**	**Total cache units (including TS7760 Base Frame)**	**Available capacity**
1 TS7760 Cache Controller (3956-CSA) 9 TS7760 Cache Drawers (3956-XSA)	1 (controller only)	11	345.07 TB (313.84 TiB)	27	847.60 TB (770.88 TiB)
	2	12	376.49 TB (342.42 TiB)	28	879.03 TB (799.47 TiB)
	3	13	407.92 TB (371 TiB)	29	910.45 TB (828.05 TiB)
	4	14	439.35 TB (399.59 TiB)	30	941.88 TB (856.64 TiB)
	5	15	470.78 TB (428.17 TiB)	31	973.31 TB (885.22 TiB)
	6	16	502.21 TB (456.76 TiB)	32	1004.74 TB (913.80 TiB)
	7	17	533.64 TB (485.34 TiB)	33	1036.17 TB (942.39 TiB)
	8	18	565.06 TB (513.92 TiB)	34	1067.60 TB (970.97 TiB)
	9	19	596.49 TB (542.51 TiB)	35	1099.02 TB (999.56 TiB)
	10	20	627.92 TB (571.09 TiB)	36	1130.45 TB (1028.14 TiB)
	11	21	659.35 TB (599.67 TiB)	37	1161.88 TB (1056.72 TiB)
	12	22	690.78 TB (628.26 TiB)	38	1193.31 TB (1085.31 TiB)
	13	23	722.21 TB (656.84 TiB)	39	1224.74 TB (1113.89 TiB)
	14	24	753.63 TB (685.43 TiB)	40	1256.17 TB (1142.48 TiB)
	15	25	785.06 TB (714.01 TiB)	41	1287.59 TB (1171.06 TiB)
	16	26	816.49 TB (742.59 TiB)	42	1319.02 TB (1199.64 TiB)
‡The term "Total cache units" refers to the combination of cache controllers and cache drawers.					

Table 60. TS7760 Storage Expansion Frame configurations for 8 TB capacity drives

TS7760 Cache configuration for base frame	Cache units‡ in eachTS7760 Storage Expansion Frame cache controller (3956-CSA) plus optional cache drawers (3956-XSA)	First TS7760 Storage Expansion Frame		Second TS7760 Storage Expansion Frame	
		Total cache units (including TS7760 Base Frame)	**Available capacity**	**Total cache units (including TS7760 Base Frame)**	**Available capacity**
1 TS7760 Cache Controller (3956-CSA) 9 TS7760 Cache Drawers (3956-XSA)	1 (controller only)	11	679.67 TB (618.16 TiB)	26	1606.99 TB (1461.55 TiB)
	2	12	741.51 TB (674.40 TiB)	27	1668.83 TB (1517.80 TiB)
	3	13	803.35 TB (730.64 TiB)	28	1730.68 TB (1574.04 TiB)
	4	14	865.19 TB (786.89 TiB)	29	1792.52 TB (1630.28 TiB)
	5	15	927.03 TB (843.13 TiB)	30	1854.36 TB (1686.53 TiB)
	6	16	988.87 TB (899.38 TiB)	31	1916.20 TB (1742.77 TiB)
	7	17	1050.72 TB (955.62 TiB)	32	1978.04 TB (1799.02 TiB)
	8	18	1112.56 TB (1011.86 TiB)	33	2039.88 TB (1855.26 TiB)
	9	19	1174.40 TB (1068.11 TiB)	34	2101.72 TB (1911.50 TiB)
	10	20	1236.24 TB (1124.35 TiB)	35	2163.56 TB (1967.75 TiB)
	11	21	1298.08 TB (1180.60 TiB)	36	2225.40 TB (2023.99 TiB)
	12	22	1359.92 TB (1236.84 TiB)	37	2287.24 TB (2080.24 TiB)
	13	23	1421.76 TB (1293.08 TiB)	38	2349.08 TB (2136.48 TiB)
	14	24	1483.60 TB (1349.33 TiB)	39	2410.93 TB (2192.72 TiB)
	15	25	1545.44 TB (1405.57 TiB)	40	2472.77 TB (2248.97 TiB)
‡The term "Total cache units" refers to the combination of cache controllers and cache drawers.					

Related information

"System requirements" on page 63

"TS7700 feature codes" on page 143

Upgrades for the TS7720

This section describes the use of miscellaneous equipment specifications (MES) to upgrade the TS7720 .

TS7720 Tape Attach

The TS7720 can be attached to the TS3500 or TS4500 Tape Library.

This functionality is enabled by FC 5273, TS7720/TS7760 Tape Attach enablement. Included with FC 5273 is one instance of FC 5274, Enable 1 TB Pending Tape Capacity, which enables up to 1 TB of data to be pending migration to tape. Additional instances of FC 5274 can be ordered, up to a maximum of 10, to increase the amount of data that is pending migration.

Addition of cache drawers

You can use FC 5656, Field installation of 3956-XS9, as an MES to add up to a maximum of nine TS7720 Cache Drawers to an existing TS7720 Cache subsystem operating with a 3956-CS9 controller. Table 61 shows the resulting usable capacity associated with each upgrade configuration available to an existing TS7720 Cache.

Table 61. Upgrade configurations for an existing TS7720 Cache

Existing minimum TS7720 Cache configuration	Additional TS7720 Cache Drawer(s) (instances of FC 5656, Field installation of 3956-XS9)	Total count of TS7720 Cache units	Usable capacity
1 TS7720 Cache Controller (3956-CS9)	1	2	47.86 TB (43.53 TiB)
	2	3	71.86 TB (65.36 TiB)
	3	4	95.86 TB (87.18 TiB)
	4	5	119.86 TB (109.01 TiB)
	5	6	143.86 TB (130.84 TiB)
	6	7	167.86 TB (152.67 TiB)
	7	8	191.86 TB (174.50 TiB)
	8	9	215.86 TB (196.32 TiB)
	9	10	239.86 TB (218.15 TiB)

You can use FC 7323, TS7720 Storage expansion frame, as an MES to add up to two expansion frames to a fully configured TS7720 Cache subsystem operating with a 3856-CS9 controller. Each TS7720 Storage Expansion Frame contains one more cache controller, controlling up to fifteen additional expansion drawers. Table 62 on page 118 shows the resulting usable capacity associated with each upgrade configuration.

Table 62. TS7720 Storage Expansion Frame configurations

TS7720 Cache configuration for base frame	Cache units‡ in eachTS7720 Storage Expansion Frame cache controller (3956-CS9) plus optional cache drawers (3956-XS9)	First TS7720 Storage Expansion Frame		Second TS7720 Storage Expansion Frame	
		Total cache units (including TS7720 Base Frame)	**Available capacity**	**Total cache units (including TS7720 Base Frame)**	**Available capacity**
1 TS7720 Cache Controller (3956-CS9) 9 TS7720 Cache Drawers (3956-XS9)	1 (controller only)	11	263.86 TB (239.98 TiB)	27	647.86 TB (589.23 TiB)
	2	12	287.86 TB (261.81 TiB)	28	671.86 TB (611.06 TiB)
	3	13	311.86 TB (283.64 TiB)	29	695.86 TB (632.88 TiB)
	4	14	335.86 TB (305.46 TiB)	30	719.86 TB (654.71 TiB)
	5	15	359.86 TB (327.29 TiB)	31	743.86 TB (676.54 TiB)
	6	16	383.86 TB (349.12 TiB)	32	767.86 TB (698.37 TiB)
	7	17	407.86 TB (370.95 TiB)	33	791.86 TB (720.20 TiB)
	8	18	431.86 TB (392.78 TiB)	34	815.86 TB (742.02 TiB)
	9	19	455.86 TB (414.60 TiB)	35	839.86 TB (763.85 TiB)
	10	20	479.86 TB (436.43 TiB)	36	863.86 TB (785.68 TiB)
	11	21	503.86 TB (458.26 TiB)	37	887.86 TB (807.51 TiB)
	12	22	527.86 TB (480.09 TiB)	38	911.86 TB (829.34 TiB)
	13	23	551.86 TB (501.92 TiB)	39	935.86 TB (851.16 TiB)
	14	24	575.86 TB (523.74 TiB)	40	959.86 TB (872.99 TiB)
	15	25	599.86 TB (545.57 TiB)	41	983.86 TB (894.82 TiB)
	16	26	623.86 TB (567.40 TiB)	42	1007.86 TB (916.65 TiB)
‡The term "Total cache units" refers to the combination of cache controllers and cache drawers.					

Related information

"System requirements" on page 63
"TS7700 feature codes" on page 143

Upgrades for the TS7740

This section describes the use of miscellaneous equipment specifications (MES) to upgrade the TS7740.

Cache drawer upgrades

One to Two TS7740 Cache Drawers
: You can add one TS7740 Cache Drawer to an existing one-drawer TS7740 Cache subsystem. Use "FC 5642, Field installation of 3956-CX7" on page 167 to achieve this upgrade.

Two to Four TS7740 Cache Drawers
: You can add two TS7740 Cache Drawers to an existing two-drawer TS7740 Cache subsystem. Use "FC 5642, Field installation of 3956-CX7" on page 167 to achieve this upgrade.

  Note: No MES is available to upgrade an existing one-drawer TS7740 cache subsystem directly to a four-drawer TS7740 cache subsystem. A one-drawer cache subsystem must be upgraded to a two-drawer cache subsystem before an upgrade to a four-drawer cache subsystem can occur.

TS7740 Server 1 Gb grid dual port copper connection
: You can add a 1 Gb copper Ethernet adapter for grid communication between TS7740s with a single port enabled. Use "FC 1036, 1 Gb grid dual port copper connection" on page 153 to achieve this upgrade on the 3957-V07.

TS7740 Server 1 Gb grid dual port optical connection
: You can add a 1 Gb dual port optical shortwave Ethernet adapter for grid communication between TS7740s with a single port enabled. Use "FC 1037, 1 Gb dual port optical SW connection" on page 153 to achieve this upgrade on the 3957-V07.

TS7740 Server 10 Gb grid dual port optical connection
: You can add a 10 Gb dual port optical longwave Ethernet adapter for grid communication between TS7740s with a single port enabled. Use "FC 1035, 10 Gb grid optical LW connection" on page 153 to achieve this upgrade on the 3957-V07.

Related information

"System requirements" on page 63

"TS7700 feature codes" on page 143

5642, Field install 3956-CX7

FC 5649, Field install 3956-CX6

Incremental cache

Incremental features help tailor storage costs and solutions to your specific data requirements.

Subsets of total cache and peak data throughput capacity are available through incremental features "FC 5267, 1 TB cache enablement" on page 162 and "FC 5268, 100 MB/sec increment" on page 162. These features enable a wide range of factory-installed configurations and permit you to enhance and update an existing system. They can help you meet specific data storage requirements by increasing cache and peak data throughput capability to the limits of your installed hardware. Increments of cache and peak data throughput can be ordered and installed concurrently on an existing system through the TS7740 Management Interface.

Note: It is recommended that you **do not** remove any installed peak data throughput features as removal can affect host jobs.

Incremental disk cache capacity

Incremental disk cache capacity is available in 1 TB (0.91 TiB) increments in a TS7740 Cluster. Disk cache is used for data:

- Originated by a host through the vNode(s) of a local or remote cluster
- Recalled from a physical tape drive associated with the cluster
- Copied from another cluster

Any excess installed capacity remains unused. Additional cache can be installed up to the maximum capacity of the installed hardware. Table 63 displays the maximum physical capacity of the TS7740 Cache configurations and the instances of "FC 5267, 1 TB cache enablement" on page 162 required to achieve each maximum capacity. Complete the installation of cache increments through the TS7740 Management Interface.

Note: Total cache capacity that is shown reflects raw capacity and does not directly correlate to usable capacity.

Table 63. Supported TS7740 Cache configurations using the 3956-CC9 cache controller

Configuration	Physical capacity	Quantity of FC 5267‡
1 TS7740 Cache Controller (3956-CC9)	9.33 TB (8.49 TiB)	10
1 TS7740 Cache Controller (3956-CC9) 1 TS7740 Cache Drawer (3956-CX9)	18.66 TB (16.97 TiB)	19
1 TS7740 Cache Controller (3956-CC9) 2TS7740 Cache Drawer (3956-CX9)	27.99 TB (25.46 TiB)	28
‡Number of instances that are required to use maximum physical capacity.		

Incremental data throughput

Incremental data throughput is available in 100-MB/sec increments, up to the limits of the installed hardware. Use "FC 5268, 100 MB/sec increment" on page 162 to add data throughput increments. For more information, see *Concurrent TS7700 upgrade options* in the **Related information** section.

Related information

"Concurrent TS7700 upgrade options" on page 106

FC 5267, 1-TB cache enablement

FC 5268, 100-MB/sec increment

"Planning for virtual and physical volumes" on page 96

"Workload considerations" on page 61

Upgrades for the TS7700 Tape Attach

This section describes the use of miscellaneous equipment specifications (MES) to upgrade TS7700s that attach to tape libraries. This includes the TS7740, TS7720 Tape Attach , and the TS7760 Tape Attach models.

Related information

"System requirements" on page 63

"TS7700 feature codes" on page 143

Tape encryption

You can encrypt tape drives used with the TS7700 Tape Attach.

The IBM TS1150 Tape Drive (3592 E08/EH8), IBM TS1140 Tape Drive (3592 E07/EH7), IBM TS1130 Tape Drive (3592 E06/EU6), and IBM TS1120 Tape Drive (3592 E05) encrypt data as it is written to any size IBM 3592 Enterprise Tape Cartridge (3592 Tape Cartridge), including WORM cartridges. Encryption is performed at full line speed in the tape drive after compression (compression is more efficiently done before encryption). This new capability adds a strong measure of security to stored data without the processing overhead and performance degradation associated with encryption performed on the server or the expense of a dedicated appliance.

Note: The IBM Encryption Key Manager is not supported for use with TS1140 Tape Drives. If encryption is used, either the Tivoli Key Lifecycle Manager (TKLM) or the IBM Security Key Lifecycle Manager (ISKLM) must be used.

Three major elements comprise the tape drive encryption solution:

Encryption-enabled tape drive

All TS1150 Tape Drives, TS1140 Tape Drives, and TS1130 Tape Drives are *encryption-capable*. All TS1120 Tape Drives installed with FC 5592 or 9592 are *encryption-capable*. This means that they are functionally capable of performing hardware encryption, but this capability is not yet activated. To perform hardware encryption, TS1150 Tape Drives, TS1140 Tape Drives, TS1130 Tape Drives and TS1120 Tape Drives must be *encryption-enabled*. In a TS3500 or TS4500 Tape Library, these tape drives can be encryption-enabled through the tape library management GUI. When TS1150 Tape Drives, TS1140 Tape Drives, TS1130 Tape Drives or TS1120 Tape Drives are attached to a controller, an IBM representative is required to set up the drive as encryption-enabled. Only encryption-enabled TS1150 Tape Drives, TS1140 Tape Drives, TS1130 Tape Drives or TS1120 Tape Drives can be used to read and write encrypted 3592 Tape Cartridges.

Encryption key management

Encryption involves the use of several kinds of keys in successive layers. How these keys are generated, maintained, controlled, and transmitted depends upon the operating environment in which the encrypting tape drive is installed. Some applications perform key management. For environments without such applications, IBM provides a key server such as the IBM Encryption Key Server component for the Java™† platform or the Tivoli Key Lifecycle Manager to perform all necessary key management tasks. "Managing tape encryption" on page 124 describes these tasks in more detail.

Encryption policy configuration

Encryption policy configuration is the set of rules, or policies, that specify which volumes are to be encrypted. How and where these rules are established depends on the existing operating environment. For more information, see "Managing tape encryption" on page 124.

The tape drive encryption solution supports:

- Out-of-band key exchanges (network connection to encryption key servers)
- Key specification by one or two Key Encryption Key (KEK) labels or the use of default key labels
- Label and hash key methods
- Up to two encryption key servers

†Refer to the topic *Trademarks* in the **Related information** section for complete attribution.

Related information

Enabling tape encryption:

This topic provides an overview of how to enable encryption on the TS7700. You can enable encryption on back-end drives so that virtual drive operations on your TS7700 do not change. You can also manage encryption key server or Tivoli Key Lifecycle Manager communications through the network to avoid interference with host operations. You can also control encryption by pools.

Before you begin

Before you enable encryption on the TS7700, you must ensure that the correct minimum required levels of microcode are installed. You must also ensure that:

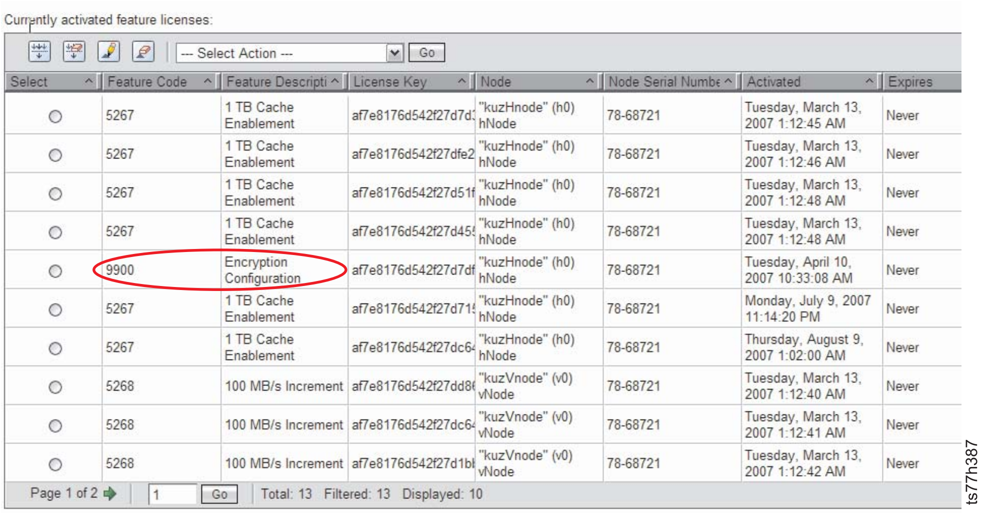
- The tape drives (TS1150 Tape Drives, TS1140 Tape Drives, TS1130 Tape Drives or TS1120 Tape Drives) are encryption-capable and enabled.
- The encryption key server, TKLM (Tivoli Key Lifecycle Manager), or ISKLM (IBM Security Key Lifecycle Manager for z/OS) is installed and configured on the network.
- Key-encrypting keys (KEKs) are defined.
- The license key for "FC 9900, Tape Encryption configuration" on page 181 is installed and activated.

No new host software is required.

Verify correct minimum microcode levels are installed

Ask your IBM service representative to receive the most current level of TS7700 code.

1. In the address bar of a web browser, enter the URL of the TS7700. For example, type: `http://virtual IP/Console`
2. At the TS7700 welcome screen, enter the userid and the password to log on to the TS7700, and select **Login**.
3. From the navigation select **Settings>Feature Licenses**.
4. The Feature Licenses page is displayed, including the table shown in Figure 32 on page 123. Verify that FC 9900, Tape Encryption configuration, displays on this table.



Currently activated feature licenses:

--- Select Action --- Go

Select	Feature Code	Feature Descripti	License Key	Node	Node Serial Numbe	Activated	Expires
	5267	1 TB Cache Enablement	af7e8176d542f27d7d	"kuzHnode" (h0) hNode	78-68721	Tuesday, March 13, 2007 1:12:45 AM	Never
	5267	1 TB Cache Enablement	af7e8176d542f27dfe2	"kuzHnode" (h0) hNode	78-68721	Tuesday, March 13, 2007 1:12:46 AM	Never
	5267	1 TB Cache Enablement	af7e8176d542f27d51f	"kuzHnode" (h0) hNode	78-68721	Tuesday, March 13, 2007 1:12:48 AM	Never
	5267	1 TB Cache Enablement	af7e8176d542f27d45	"kuzHnode" (h0) hNode	78-68721	Tuesday, March 13, 2007 1:12:48 AM	Never
	9900	Encryption Configuration	af7e8176d542f27d7df	"kuzHnode" (h0) hNode	78-68721	Tuesday, April 10, 2007 10:33:08 AM	Never
	5267	1 TB Cache Enablement	af7e8176d542f27d71	"kuzHnode" (h0) hNode	78-68721	Monday, July 9, 2007 11:14:20 PM	Never
	5267	1 TB Cache Enablement	af7e8176d542f27dc6	"kuzHnode" (h0) hNode	78-68721	Thursday, August 9, 2007 1:02:00 AM	Never
	5268	100 MB/s Increment	af7e8176d542f27dd8	"kuzVnode" (v0) vNode	78-68721	Tuesday, March 13, 2007 1:12:40 AM	Never
	5268	100 MB/s Increment	af7e8176d542f27dc6	"kuzVnode" (v0) vNode	78-68721	Tuesday, March 13, 2007 1:12:41 AM	Never
	5268	100 MB/s Increment	af7e8176d542f27d1b	"kuzVnode" (v0) vNode	78-68721	Tuesday, March 13, 2007 1:12:42 AM	Never

Page 1 of 2 | 1 Go | Total: 13 Filtered: 13 Displayed: 10

Figure 32. Currently active feature licenses

If using TS1120 Tape Drives, verify they are encryption-capable

1. From the navigation, select **Physical>Physical Tape Drives**.
2. Select the radio button next to the drive you want to verify and select **Select Action>Details**. Then click **Go**.
3. If **Yes** displays in the second column, adjacent to **Encryption Capable**, encryption capability and enablement are set. If **No** displays in the column adjacent to **Encryption Capable**, encryption capability and enablement are **NOT** set.

   Attention: If encryption capability and enablement are not set, contact your IBM Service Representative to enable encryption following the procedures in the *IBM System Storage TS1120, TS1130, and TS1140 Tape Drives (16th Edition - June 2011) Maintenance Information IBM 3592 Models J1A, E05, E06, EU6, and E07*.

Verify encryption key server or TKLM is installed and configured on the network

1. From the navigation select **Settings>Cluster Settings> Encryption Key Server Addresses**.
2. Verify that at a minimum, the **Primary key server address** and **Port** fields are complete.

   Attention: If encryption key server or TKLM is not installed and configured, contact your IBM Service Representative to enable encryption following the procedures in the *IBM Encryption Key Server component for the Java† platform Introduction, Planning, and User's Guide*, the *IBM Tivoli Key Lifecycle Manager Information Center*, or the *IBM Tivoli Key Lifecycle Manager Quick Start Guide*.

†Refer to the topic *Trademarks* in the **Related information** section for complete attribution.

About this task

To enable encryption on the TS7700, you must enable the tape drives for encryption, then install and activate the license key for "FC 9900, Tape Encryption configuration" on page 181.

Enable the TS1150 Tape Drives, TS1140 Tape Drives, TS1130 Tape Drives or TS1120 Tape Drives for encryption.

Note: If you intend to use tape drives in encryption mode, you must enable encryption on all tape drives that you attach to the TS7700.

Ask your IBM service representative to receive the most current levels of TS7700 code.

Install and activate the encryption license key

Procedure

1. Enable the tape drives for encryption.
   a. Set the drives to native mode through the TS3500 or TS4500 Tape Library interface; do not use the TS7700 Management Interface.

      Note: You must take the TS7700 offline to perform this task.
   b. Enable encryption on all drives.

      Note: You can perform this task when the TS7700 is either online or offline.
2. Determine whether or not you have the license key. Do you have the license key?
   - **Yes**, go to step 3.
   - **No**, order "FC 9900, Tape Encryption configuration" on page 181 to get the license key.
3. Install and activate the license key through the TS7700 Management Interface.

   Related information

   "About tape encryption keys" on page 126

   FC 9900, Encryption configuration

   "Managing tape encryption"

Managing tape encryption:

This topic defines the encryption key server component that is used to manage encryption on the IBM TS7700.

The encryption key server component is a software program such as the IBM® Encryption Key Server component for the Java† platform or the Tivoli Key Lifecycle Manager that assists IBM encryption-enabled tape drives in generating, protecting, storing, and maintaining encryption keys that are used to encrypt information that is being written to, and decrypt information that is being read from, tape media (tape and cartridge formats). An encryption key server operates on z/OS, i5/OS, AIX, Linux†, HP-UX, Sun Solaris, and Windows†, and is a shared resource deployed in several locations within an Enterprise. It can serve numerous IBM encrypting tape drives, regardless of where those drives reside (for example, in tape library subsystems, connected to mainframe systems through various types of channel connections, or installed in other computing systems).

An encryption key server is a process that protects data by using key generation and retrieval. Requests for key generation or retrieval are sent to the encryption key server through a TCP/IP connection from a tape library, subsystem, or drive. When a tape drive writes encrypted data, it first requests an encryption key from the encryption key server. Upon receipt of the request, the encryption key server generates an Advanced Encryption Standard (AES) key and serves it to the tape drives in two protected forms:

- Encrypted, or *wrapped*, using Rivest-Shamir-Adleman (RSA) key pairs. When using this form of protection, the tape drive writes this copy of the key to the cartridge memory and three more places on the tape for redundancy.
- Separately wrapped for secure transfer to the tape drive, where it is unwrapped upon arrival and used to encrypt the data that is being written to tape.

When an encrypted tape cartridge is read by a tape drive (TS1150 Tape Drive, TS1140 Tape Drive, TS1130 Tape Drive or TS1120 Tape Drive), the protected AES key on the tape is sent to the encryption key server where it is decrypted. The AES key is then wrapped for secure transfer back to the tape drive, where it is unwrapped and used to decrypt the data stored on the tape. The encryption key server also allows AES keys to be rewrapped, *or rekeyed*, by using RSA keys different from the original ones that were used. (For more information, see "About tape encryption keys" on page 126.) Rekeying is useful when shipping tapes for use on external systems.

Three methods of encryption management exist; which you choose depends on your operating environment and where you locate your encryption key server application. The encryption key server and the encryption policy engine can be in the application, system, or library layer, as illustrated by Figure 33.

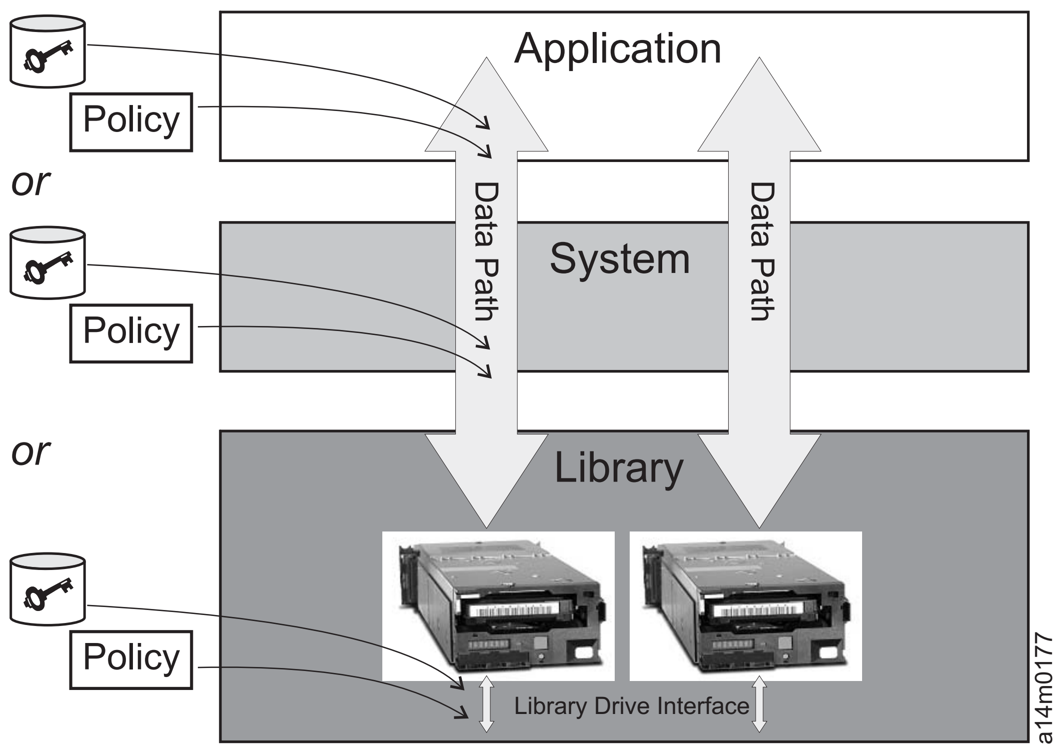


Figure 33. Three possible locations for encryption policy engine and key management.

Application Layer
: The application layer initiates data transfer for tape storage, for example Tivoli Storage Manager (TSM).

System Layer
: The system layer contains everything between the application and the tape drives, for example the operating system, z/OS DFSMS, device drivers, and FICON controllers.

Library Layer
: The library layer contains the enclosure for tape storage, such as the TS3500 or TS4500 Tape Library. A modern tape library contains an internal interface to each tape drive.

†Refer to the topic *Trademarks* in the **Related information** section for complete attribution.

Related information

"Enabling tape encryption" on page 122

About tape encryption keys:

This topic describes the encryption keys that can be used by The IBM Encryption Key Server component for the Java† platform or the Tivoli Key Lifecycle Manager.

An AES encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created by using algorithms that are designed to ensure that each key is unique and unpredictable. The longer the key string, the harder it is to break the encryption code. Both the IBM and T10 methods of encryption use 256-bit AES algorithm keys to encrypt data. 256-bit AES is the encryption standard that is recognized and recommended by the U.S. government.

Encryption method

Two types of encryption algorithms are used by the encryption key server: symmetric algorithms and asymmetric algorithms. Symmetric, or secret key encryption, uses a single key for both encryption and decryption. Symmetric key encryption is used for encrypting large amounts of data efficiently. Asymmetric encryption, or public/private key encryption, uses a pair of keys. Data encrypted using one key can be decrypted only by using the other key in the asymmetric key pair.

When an asymmetric key pair is generated, the public key is typically used to encrypt, and the private key is typically used to decrypt. The encryption key server uses both types: symmetric encryption for high-speed encryption of user or host data, and asymmetric encryption (which is necessarily slower) for protecting the symmetric key that is used to encrypt the data (key wrapping).

Encryption keys can be generated by the encryption key server, by applications such as Tivoli Storage Manager, or by a utility such as keytool. The responsibility for generating AES keys and the manner in which they are transferred to the tape drive depends on the tape drive type and the method of encryption management. However, it is be helpful to understand the difference between how the encryption key server uses encryption keys and how other applications use them.

How the encryption key server processes encryption keys

In system-managed and library-managed tape encryption, unencrypted data (clear text) is sent to the tape drive (TS1150 Tape Drive, TS1140 Tape Drive, TS1130 Tape Drive or TS1120 Tape Drive), and converted to ciphertext by using a symmetric

256-bit AES Data Key (DK) generated by the encryption key server. The ciphertext is then written to tape. The encryption key server uses a single, unique Data Key for each Enterprise Tape Cartridge. This Data Key is also encrypted, or wrapped, by the encryption key server by using the public key from an asymmetric Key Encrypting Key (KEK) pair. This process creates an Externally Encrypted Data Key (EEDK). The EEDK is written to the cartridge memory and to three more places on the tape media in the cartridge. The tape cartridge now holds both the encrypted data and the means to decrypt it for anyone that holds the private part of the KEK pair.

The DK can also be wrapped a second time by using the public key of another party to create another EEDK. Both EEDKs can be stored on the tape cartridge. In this way, the tape cartridge can be shipped to a business partner who holds the corresponding private key. That private key would allow the DK to be unwrapped and the tape decrypted by the business partner. Figure 34 illustrates the symmetric and asymmetric processes.

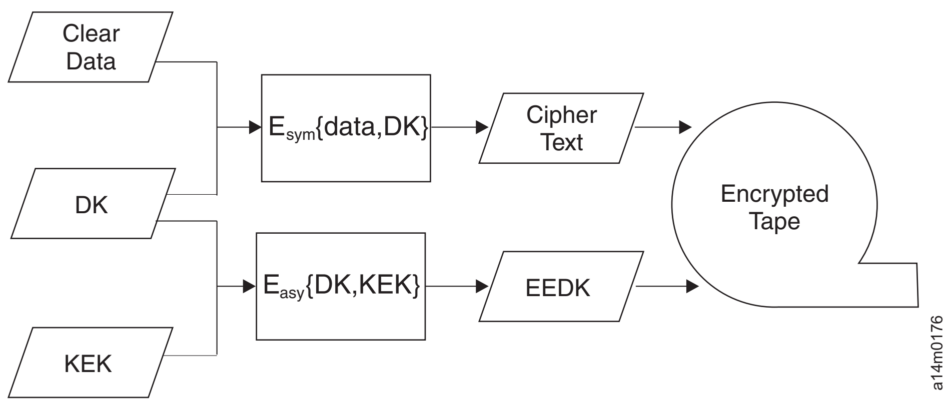


Figure 34. An encryption key server uses both symmetric and asymmetric encryption keys

Encryption key server default keys

This function introduces the ability to allow the TS7700 to use default keys defined within the external key server. If multiple libraries exist, this function is required so that key management and assignment can be done in an external centralized location instead of updating each library every time a key is changed or regenerated.

Note: Your encryption key server software must support default keys to use this option.

The physical volume pool property settings continue to provide an option for two keys. In addition to providing a manually entered key, the management interface provides a mutually exclusive check box per key that states a default key should be used for that particular key. Each of the two keys for each pool can be set up differently, allowing one key to be the default while another is manually entered. For example, key 1 may be set up to use a default key while key 2 is manually provided. Or, both keys can use the default or both keys can be provided manually. When a physical volume is written from beginning of tape and one or both key settings are configured to use default keys, the TS7700 informs the drive that one or both keys are set up for default. The drive negotiates through the TS7700 to the key server and requests that the key server use default keys currently configured within the key server. Since the key is provided by the key server, the TS7700 is not aware of what key is used for the physical volume when default keys are used.

The user should be able to determine whether either or both keys that are used for a particular encrypted physical volume are default keys or manually provided keys. To help with enhancements that require ranges of physical volumes based on when they were encrypted, a new time of encryption timestamp is introduced into the physical volume table. Each time a physical volume is written from beginning of tape with encryption enabled by using any key type, this timestamp is updated to the current time. This new timestamp can be used to determine when the volume keyed and is included in the physical volume BVIR output.

†Refer to the topic *Trademarks* in the **Related information** section for complete attribution.

External key management for disk encryption

In addition to local key management for disk encryption, some TS7700 machines support external key management disk encryption, which stores the secure key in an IBM Tivoli Key Lifecycle Manager (TKLM) server or an IBM Secure Key Lifecycle Manager (SKLM) server. The machines that support external key management are the TS7760 Cache Controller 3956-CSA, the TS7720 Cache Controller 3956-CS9, and the TS7740 Cache Controller 3956-CC9. A microcode level of at least 8.33.0.0 is required (8.40.0.0 for machines with 3956-CSA cache models).

External encryption key management removes the responsibility of managing the key from the 3957-VEC, 3957-VEB, and 3957-V07 servers and from the disk subsystem controllers. The key is stored in volatile memory inside the 3956-CSA, 3956-CC9, or 3956-CS9 controllers. This means that if the 3956-Cxx controller is powered off and powered back on, the controller must obtain the security key from the TKLM or SKLM server again. The 3956-Cxx controller does not connect directly to the TKLM or SKLM server. The 3956-Cxx controller connects to the TKLM or SKLM server through a proxy server. The proxy server is provided by the 3957-VEC or 3957-V07/VEB. The proxy server requests keys to the TKLM or SKLM servers on behalf of the 3956-Cxx controllers. The keys are then given to the 3956-Cxx controllers by the proxy server.

Proper configuration is necessary for the disk subsystem controllers to communicate with the proxy server. The following figure shows the interconnection of the 3956-Cxx and the TKLM server using the proxy server.

External key management proxy server

Related information

"Physical volume planning" on page 99
"Enabling tape encryption" on page 122
"Managing tape encryption" on page 124

Disk encryption

You can encrypt the disk drive modules (DDMs) within a TS7700 disk storage system.

Full Disk Encryption (FDE) can be enabled in one or more DDMs in a cache subsystem. Encrypted data becomes readable using an encryption key that is stored locally within the cache controller. When encryption is enabled in a disk subsystem, it cannot be easily disabled. After a cache subsystem is encrypted, a complete erase (secure erase) of the physical disks (FDE-capable DDMs) is required to use those drives without encryption.

Prerequisites

Disk encryption is available on a new order from manufacturing that uses "FC 7404, Encryption" on page 175 or as an MES that uses "FC 5272, Enable disk encryption - Local Key Management" on page 163. The following conditions must also be met:

- The TS7740 must contain a 3957-V07. The TS7720 must contain a 3957-VEB. The TS7760 must contain a 3957-VEC.
- FDE drives must be a 600 GB Fibre Channel drive (TS7740), a 3 TB near-line SAS drive (TS7720), or a 4 TB near-line SAS drive (TS7760).
- Encryption is enabled on site following code activation by an IBM Service Representative.
- An entire file system must be encrypted; a mixture of encrypted and non-encrypted arrays is not supported. All arrays in all strings must be encryption-capable.

Related information

Internal key management:

You can manage the encryption key for the disk drive modules (DDMs) internally.

Related information

External key management:

You can manage the encryption key for the 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, Tivoli Key Lifecycle Manager (TKLM), or IBM Security Key Lifecycle Manager (ISKLM) is installed and configured on the network.

The following tasks can be done:

- Re-key (from SMIT and Management Interface)
- Activate (from SMIT only)
- Switch from internal key management to external key management (from SMIT only)

Prerequisites

The prerequisites are the same as for internal key management for encryption.

Disk encryption is available on a new order from manufacturing that uses "FC 7404, Encryption" on page 175 or as an MES that uses "FC 5272, Enable disk encryption - Local Key Management" on page 163. The following conditions must also be met:

- The TS7740 must contain a 3957-V07. The TS7720 must contain a 3957-VEB. The TS7760 must contain a 3957-VEC.

- FDE drives must be a 600 GB Fibre Channel drive (TS7740), a 3 TB near-line SAS drive (TS7720), or a 4 TB near-line SAS drive (TS7760).
- Encryption is enabled onsite following code activation by an IBM Service Representative.
- An entire file system must be encrypted; a mixture of encrypted and non-encrypted arrays is not supported. All arrays in all strings must be encryption-capable.

Related information

Copy export overview

The copy export function allows a copy of selected virtual volumes that are written to the TS7700 to be removed and taken offsite for disaster recovery purposes.

The copy export function builds on the existing capability to create a copy of virtual volumes on a secondary physical volume pool. When a copy export is completed, physical volumes from the secondary physical volume pool are removed from the library that is associated with the TS7700 and sent to an offsite location for disaster recovery. The benefits of volume stacking, which places many virtual volumes on a physical volume, are retained. Additionally, since the exported data is a copy of the virtual volumes, it remains accessible to the production host system.

Note: The copy export function does not apply to disk-only TS7700 configurations.

Similar to the traditional use of tape for disaster recovery, it is expected that the copy export operation is completed regularly and that additional physical volumes are sent offsite daily. Should the production site become unusable and it becomes necessary to use the offsite volumes for disaster recovery, access to the exported data is reestablished through a disaster recovery procedure instead of a data import procedure:

1. All exported physical volumes are placed into a library attached to an empty TS7700.
2. A disaster recovery procedure is invoked through the TS7700 Management Interface.

   Note: You must also restore the host environment (tape catalog, tape management system, and so on.).
3. The disaster recovery procedure reestablishes access to the virtual volumes contained on the exported physical volume.

Although the exported physical volumes are removed from the TS7700 and located outside of the physical library, they continue to be managed by the source TS7700 regarding space management. As virtual volumes resident on the exported physical volumes are expired, rewritten, or otherwise invalidated, the amount of valid data on an exported physical volume decreases until the physical volume becomes eligible for reclamation based on your criteria. When an exported physical volume is reclaimed, it is not brought back to the source TS7700 for processing; instead, a new secondary copy of the remaining valid virtual volumes is made by using the primary virtual volume copy as a source. The next time the copy export operation is performed, the physical volume with the new copies is also exported. The exported physical volumes that were reclaimed and are offsite no longer have valid data and can be returned to the source TS7700 to be used as new scratch volumes.

Note: If two or more TS7700s are configured in a Grid, only one TS7700 can perform a copy export operation at any time.

The Export List Volume is a virtual volume that provides completion status and export operation information for the copy export function. The host that initiates copy export creates an Export List Volume on the TS7700 that performs the operation. The TS7700 performing the operation uses the Export List Volume for project status, export information, and execution instructions. The TS7700 then creates response records in the Export List Volume that list the virtual volumes exported and the physical volume that they reside on. You can use this information as a record for data that is offsite. Finally, the TS7700 writes records in the Export List Volume for any offsite physical volumes that have been reclaimed and no longer contain any active data. The Bulk Volume Information Retrieval (BVIR) function can provide a list of the offsite physical volumes that are empty in the Export List Volume and can be used to obtain a current list of exported physical volumes for a secondary pool. Information is provided for the amount of active data contained by each exported physical volume.

Host Console Request and Host Copy Enable. The Host Console Request (HCR) and Host Copy Enable functions expand the range of copy operations.

The copy export function is also supported by the HCR function. Through HCR, you can request that a physical volume exported with copy export be queued for reclamation, regardless of whether it has met any of the reclaim criteria you have established for the TS7700. You can use the HCR function from the zOS host console to remove a physical volume that is exported with copy export that no longer has any valid data on it. For detailed information about the copy export function, please refer to the IBM White Paper, *IBM Virtualization Engine TS7700 Series Copy Export User's Guide*, WP101092, available at the *IBM Support & Downloads* web page linked in the **Related information** section.

Host Copy Enable permits the host to enable or disable copies to and from the specified distributed library. A request to disable copies permits any copies in progress to continue, but prevents initiation of additional copy operations to the specified distributed library. Copy operations continue to queue and operations between other distributed libraries in the TS7700 Grid remain unaffected. A request to enable copies allows the specified distributed library to again become a source for copies and initiate copy operations where it is the target.

Host Override for Cache Residency. You can also use the HCR function to modify how virtual volumes are managed in the tape volume cache. The Host Override for Cache Residency function allows the preference group for a virtual volume to be temporarily overridden while the volume is in cache. This function also permits you to keep a virtual volume in cache longer by making it appear as the most recently accessed volume.

Copy Export Recovery Code Level Limitations. A copy export recovery can occur only within a TS7700 that is operating a code level equal to or later than the microcode level of the TS7700 that exported the physical volumes.

Related information

"Logical WORM" on page 270

http://www.ibm.com/support/us/en/

Copy export merge:

The copy export merge function allows a copy of selected virtual volumes that are stacked to tape to be merged into an existing TS7700 that already contains data and that may be part of a grid.

Copy export merge enhances the copy export function by expanding the range of possible restore points to include an existing TS7700 Cluster, regardless of whether that cluster is empty or part of an existing grid. Scenarios that would use this function include disaster recovery to an existing TS7700 Cluster, as well as moving content from one datacenter to another.

Note: A partial workload move (leaving some workload data behind) may not be recommended due to the complexities of host environment changes and source cleanup required.

The following restrictions apply:

- You must coordinate with your IBM Service Representative to initiate a copy export merge operation. Recovery into a stand-alone, empty TS7700 Cluster is still supported without additional IBM coordination.
- Only virtual volumes targeting the copy export recovery pools are restored, unless you use the option to restore an entire TS7700 Cluster.

  Note: An option is available to restore the entire contents of a TS7700 Cluster independent of whether all source data existed in a copy export pool at the time of export. At least one copy export tape is required to provide the database that defines all tapes previously contained within the source TS7700 Cluster. All pools being restored, independent of whether they were copy export pools, can be redirected to unused pools during the restore process.
- Recovered virtual volumes cannot conflict with virtual volumes in the existing TS7700 Cluster.
  - If any virtual volumes conflict, the restore operation is canceled before the restore point is changed.
  - If the primary or secondary pool for any virtual volume conflicts with an existing primary or secondary pool, the restore operation is canceled before the restore point is changed.
- The existing TS7700 Cluster can be a member of a grid, however:
  - Only the TS7700 Cluster that is used as the restore point contains restored volume data. This data does not automatically replicate to any peer location. You must coordinate with your IBM Service Representative to use tools such as VESYNC to replicate restored content to any peer locations.
  - The restore TS7700 Cluster must be put into service then offline during the restore.
  - All other clusters in the grid must remain online during the restore operation.
- The Copy Export Disaster recovery test mode cannot be used during a copy export restore merge scenario. Disaster recovery test mode is only available as an option if the restore operation targets an empty TS7700 Cluster.
- The total number of virtual volumes that follow the restore merge operation cannot exceed the total number available as designated by FC 5270. If the total number of virtual volumes does exceed the number available by FC 5270, the restore operation is canceled before the restore location is changed.

Following a copy export merge operation, data is restored into a distributed and composite library that is different from the source. You must update host catalogues to reflect the new data location.

Related information

"Logical WORM" on page 270

http://www.ibm.com/support/us/en/

Copy export acceleration:

Copy export acceleration improves the speed of large copy export operations by reducing the number of physical volumes that store a copy of the database used for recovery.

By reducing the number of tapes that contain a copy of the database that is used for recovery, most of the physical volumes that are exported then need to be only ejected, instead of modified and ejected. This difference greatly reduces the time of the export operation. Copy export acceleration uses a copy export request attribute to append the recovery database snapshot to only the first two and last two copy export tapes in a given set. Copy export acceleration can greatly reduce the amount of time spent on a large copy export operation. With the acceleration feature, the resulting list file can be used to determine which volumes contain the database, and therefore should be used during any future restore operation. Since the first and last two volumes that contain the database are not necessarily the first and last two tapes that are physically removed from the library, the list file should be used to determine which four physical volumes contain the database.

Note: Copy export acceleration is supported for use only with TS7700 Clusters attached to physical tape drives, operating at a microcode level of 8.21.0.xx or later.

Related information

"Logical WORM" on page 270

http://www.ibm.com/support/us/en/

TS4500 support

When you upgrade to a microcode level of 8.40.xx, support for the TS7700 tape attach to a TS4500 tape library is available.

The TS4500 Tape Library is the next generation of the TS3500 tape library, and is expected to be equivalent or better than the TS3500 in capabilities. New features and functions in the TS4500, such as native LDAP support, can be independently leveraged when used behind a TS7700.

Notes:

1. When the TS7700 is attached to a TS4500 Tape Library, the following drive configurations are supported:
   a. Up to 16 TS1150 tape drives *or*
   b. Up to 16 tape drives consisting of TS1150 and TS1140 tape drives
2. The media types that are supported for reading and writing include JC, JK, JD, and JL.
3. All physical tape encryption support will remain unchanged.
4. The TS4500 Tape Library supports only 16 Gb Fibre Channel switches. Older 8 Gb and 4 Gb switches will be supported in TS3500 configurations.

Related information

"TS3500/TS4500 Tape Library attachment" on page 52

Frame replacement migration

You can replace older TS7700 hardware with a newer model.

Frame replacement migration is the frame replacement of an existing cluster with the latest hardware to stay current with the TS7700 technology and to be on supported hardware.

Frame replacement migration is available for the following configurations:

- from a TS7740 3957-V06 to a TS7740 3957-V07
- from a TS7740 3957-V06 to a TS7720 3957-VEB tape attach
- from a TS7740 3957-V06 to a TS7760 3957-VEC tape attach
- from a TS7740 3957-V07 to a TS7720 3957-VEB tape attach
- from a TS7740 3957-V07 to a TS7760 3957-VEC tape attach
- from a TS7720 3957-VEB tape attach to a TS7760 3957-VEC tape attach

Note: Frame replacement migration is only done on a TS7740 or TS7720 tape attach to upgrade to newer hardware.

Contact your sales representative to initiate a frame replacement migration procedure.

Related information

"TS7700 product introduction" on page 5

Withdrawn hardware and features

This section lists TS7700 hardware and features scheduled for withdrawal, along with any replacements.

Table 64. Withdrawn TS7700 hardware

Hardware	Replaced by	Scheduled for withdrawal
TS7720 Server 3957-VEA	TS7720 Server 3957-VEB	August 2011
TS7720 Server 3957-VEB	TS7760 Server 3957-VEC	June 2016
TS7740 Server 3957-V06	TS7740 Server 3957-V07	August 2011
TS7740 Server 3957-V07	TS7760 Server 3957-VEC	June 2016
TS7720 Cache Controller 3956-CS7	TS7720 Cache Controller 3956-CS8†	June 2010
TS7720 Cache Controller 3956-CS8	TS7720 Cache Controller 3956-CS9	December 2013
TS7720 Cache Drawer 3956-XS7	TS7720 Cache Drawer 3956-XS9	December 2013
TS7740 Cache Controller 3956-CC6	TS7740 Cache Controller 3956-CC7†	February 2009
TS7740 Cache Controller 3956-CC7	TS7740 Cache Controller 3956-CC8†	June 2010
TS7740 Cache Controller 3956-CC8	TS7740 Cache Controller 3956-CC9†	January 2013
TS7740 Cache Controller 3956-CC9	TS7760 Cache Controller 3956-CSA	June 2016
TS7740 Cache Drawer 3956-CX6	TS7740 Cache Drawer 3956-CX9	February 2012
TS7740 Cache Drawer 3956-CX7	TS7740 Cache Drawer 3956-CX9	December 2013
3952 F05 Tape Frame	3952 F06 Tape Frame	June 2016
†This hardware component has since been withdrawn.		

Table 65. Replacement TS7700 features

Withdrawn feature	Associated Machine type-model	Replacement feature	Associated Machine type-model
FC 5627, Install 3957-VEB	3952 F05	FC 5630, Install 3957-VEC	3952 F06
FC 5629, Install 3957-V07	3952 F05	FC 5630, Install 3957-VEC	3952 F06
FC 5652, Plant installation of 3956-CC9	3952 F05	FC 5657, Plant installation of 3956-CSA	3952 F06
FC 7330, TS7740 Encryption-capable base frame	3952 F05	FC 7333, TS7700 Encryption-capable base frame	3952 F06
FC 7331, TS7720 Encryption-capable base frame	3952 F05	FC 7334, TS7700 Encryption-capable expansion frame	3952 F06
FC 9116, Ship with R3.3 Machine Code	3952 F05	FC AGK0, Ship with R4.0 Machine Code	3952 F06
FC 7124, 13.2 TB SAS storage	3956-CC9	FC 7117, 48 TB SAS Storage	3956-CSA
FC 7403, Enable first expansion drawer	3956-CC7	No replacement	
FC 9352, Plant Install	3956-CC8, 3956-CS8, 3956-CC9	FC 9352, Plant Install	3956-CSA
FC 9354, Plant Install	3956-CX7, 3956-XS7	FC 9354, Plant Install	3956-XSA
FC 9355, Field merge	3956-CX6	FC 9355, Field merge	3956-XSA
FC 0983, TAA Compliance	3957-V07, 3957-VEB	FC 0983, TAA Compliance	3957-VEC
FC 0201, 9-micron LC/LC 31-meter	3957-V06, 3957-VEA	FC 0201, 9-micron LC/LC 31-meter	3957-VEC
FC 0203, 50-micron LC/LC 31-meter	3957-V06, 3957-VEA	FC 0203, 50-micron LC/LC 31-meter	3957-VEC
FC 0521, Functional enhancement field	3957-V06, 3957-VEA	No replacement	
FC 1032, 1 Gb grid dual port copper connection	3957-V06, 3957-VEA	FC 1032, 1 Gb grid dual port copper connection	3957-VEC
FC 1033, 1 Gb grid dual port optical SW connection	3957-V06, 3957-VEA	FC 1033, 1 Gb grid dual port optical SW connection	3957-VEC
FC 1034, Enable dual port grid connection	3957-V06, 3957-VEA	FC 1034, Enable dual port grid connection	3957-VEC
FC 2715, Console attachment	3957-V06, 3957-V07, 3957-VEB	FC 2715, Console attachment	3957-VEC
FC 3461, 8 GB Memory upgrade, field	3957-V06, 3957-VEA	No replacement	
FC 4015, Grid enablement	3957-V06, 3957-VEA	FC 4015, Grid enablement	3957-VEC

Table 65. Replacement TS7700 features (continued)

Withdrawn feature	Associated Machine type-model	Replacement feature	Associated Machine type-model
FC 4016, Remove Cluster from Grid	3957-V06, 3957-VEA	FC 4016, Remove Cluster from Grid	3957-VEC
FC 4017, Cluster cleanup	3957-V06, 3957-VEA	FC 4017, Cluster cleanup	3957-VEC
FC 5240, Dual port fibre channel host bus adapter	3957-VEA	FC 5242, Dual Port 16 Gb Fibre Channel HBA	3957-VEC
FC 5241, Dual port FC HBA	3957-V07	FC 5242, Dual Port 16 Gb Fibre Channel HBA	3957-VEC
FC 5267, 1 TB cache enablement	3957-V06	FC 5267, 1 TB cache enablement	3957-VEC
FC 5268, 100 MB/sec increment	3957-V06, 3957-VEA	FC 5268, 100 MB/sec increment	3957-VEC
FC 5270, Increased virtual volumes	3957-V06, 3957-VEA	FC 5270, Increased virtual volumes	3957-VEC
FC 5271, Selective device access control	3957-V06, 3957-VEA	FC 5271, Selective device access control	3957-VEC
FC 9000, Mainframe attachment	3957-V07, 3957-VEB	FC 9000, Mainframe attachment	3957-VEC
FC 9116, Ship with R3.3 Machine Code	3957-V07, 3957-VEB	FC AGK0, Ship with R4.0 Machine Code	3957-VEC
FC 9219, Attach to TS3500/TS4500	3957-V07	FC 9219, Attach to TS3500/TS4500	3957-VEC
FC 9350, Plant Install	3957-V07, 3957-VEB	FC 9350, Plant Install	3957-VEC
FC 9351, Field merge TS7700 Server in 3952 F05	3957-V07, 3957-VEB	FC 9351, Field merge TS7700 Server in 3952 F05	3957-VEC
FC 9700, No factory cables	3957-V07, 3957-VEB	FC 9700, No factory cables	3957-VEC
FC 9900, Tape Encryption configuration	3957-V06	FC 9900, Tape Encryption configuration	3957-VEC

Table 66. Withdrawn TS7700 features

Associated machine type and model	Feature code withdrawn	Scheduled for withdrawal
3952 F05 Tape Frame	FC 2719, Console upgrade	September 2010
	FC 2730, TS3000 System Console	January 2010
	FC 2732, TS3000 System Console	January 2013
	FC 2733, Internal modem	January 2013
	FC 5626, Plant installation of 3957-VEA	August 2011
	FC 5627, Install 3957-VEB	June 2016
	FC 5628, Plant installation of 3957-V06	August 2011
	FC 5629, Install 3957-V07	June 2016
	FC 5635, Plant installation of 3956-CS8	January 2013
	FC 5636, Plant installation of 3956-CS7	July 2010
	FC 5638, Plant installation of 3956-CC6	February 2009
	FC 5639, Plant installation of 3956-CC7	June 2010
	FC 5640, Plant installation of 3956-CC8	January 2013
	FC 5641, Plant installation of 3956-CX7	January 2013

Table 66. Withdrawn TS7700 features (continued)

Associated machine type and model	Feature code withdrawn	Scheduled for withdrawal
3952 F05 Tape Frame (continued)	FC 5642, Field installation of 3956-CX7	January 2013
	FC 5646, Plant installation of 3956-XS7	January 2013
	FC 5647, Field installation of 3956-XS7	January 2013
	FC 5648, Plant installation of 3956-CX6	February 2009
	FC 5649, Field installation of 3956-CX6	February 2012
	FC 5652, Plant installation of 3956-CC9	June 2016
	FC 5759, Integrated control path	August 2011
	FC 7312, TS7740 Base frame	January 2013
	FC 7322, TS7720 Base frame	January 2013
	FC 7323, TS7720 Storage expansion frame	January 2013
	FC 7330, TS7740 Encryption-capable base frame	June 2016
	FC 7331, TS7720 Encryption-capable base frame	June 2016
	FC 9110, Ship with R1.7 machine code	February 2012
	FC 9111, Ship with R2.0 machine code	January 2013
	FC 9112, Ship with R2.1 machine code	December 2013
	FC 9113, Ship with R3.0 machine code	April 2014
	FC 9114, Ship with R3.1 machine code	January 2015
	FC 9115, Ship with R3.2 Machine Code	June 2016
	FC 9116, Ship with R3.3 Machine Code	June 2016

Table 66. Withdrawn TS7700 features (continued)

Associated machine type and model	Feature code withdrawn	Scheduled for withdrawal
TS7740 Server 3957-V06	FC 0201, 9-micron LC/LC 31-meter	June 2016
	FC 0202, 9-micron LC/SC 31-meter	December 2009
	FC 0203, 50-micron LC/LC 31-meter	June 2016
	FC 0204, 50-micron LC/SC 31-meter	August 2011
	FC 0205, 62.5-micron LC/LC 31-meter	December 2009
	FC 0206, 62.5-micron LC/SC 31-meter	December 2009
	FC 0521, Functional enhancement field	June 2016
	FC 1030, 1Gb grid copper connection	February 2009
	FC 1031, 1Gb optical SW connection	February 2009
	FC 1032, 1 Gb grid dual port copper connection	June 2016
	FC 1033, 1 Gb grid dual port optical SW connection	June 2016
	FC 1034, Enable dual port grid connection	June 2016
	FC 2714, Console expansion	August 2011
	FC 2715, Console attachment	June 2016
	FC 2719, Console upgrade	December 2008
	FC 2720, TS3000 System Console	December 2008
	FC 3461, 8 GB Memory upgrade, field	June 2016
	FC 4015, Grid enablement	June 2016
	FC 4016, Remove Cluster from Grid	June 2016
	FC 4017, Cluster cleanup	June 2016
	FC 5240, Dual port fibre channel host bus adapter	August 2011
	FC 5267, 1 TB cache enablement	June 2016
	FC 5268, 100 MB/sec increment	June 2016
	FC 5270, Increased virtual volumes	June 2016
	FC 5271, Selective device access control	June 2016
	FC 9000, Mainframe attachment	August 2011
	FC 9217, Attach to 3953 LM	February 2009
	FC 9218, Attach to 3494 LM	August 2011
	FC 9219, Attach to TS3500/TS4500	August 2011
	FC 9350, Plant Install	August 2011
	FC 9461, 8 GB Memory upgrade, plant	August 2011
	FC 9700, No factory cables	August 2011

Table 66. Withdrawn TS7700 features (continued)

Associated machine type and model	Feature code withdrawn	Scheduled for withdrawal
TS7740 Server 3957-V07	FC 0983, TAA Compliance	June 2016
	FC 2714, Console expansion	January 2013
	FC 2715, Console attachment	June 2016
	FC 5241, Dual port FC HBA	June 2016
	FC 9000, Mainframe attachment	June 2016
	FC 9111, Ship with R2.0 machine code	January 2013
	FC 9112, Ship with R2.1 machine code	December 2013
	FC 9113, Ship with R3.0 machine code	April 2014
	FC 9114, Ship with R3.1 machine code	January 2016
	FC 9116, Ship with R3.3 Machine Code	June 2016
	FC 9219, Attach to TS3500/TS4500	June 2016
	FC 9350, Plant Install	June 2016
	FC 9351, Field merge TS7700 Server in 3952 F05	June 2016
	FC 9700, No factory cables	June 2016

Table 66. Withdrawn TS7700 features (continued)

Associated machine type and model	Feature code withdrawn	Scheduled for withdrawal
TS7720 Server 3957-VEA	FC 0201, 9-micron LC/LC 31-meter	June 2016
	FC 0202, 9-micron LC/SC 31-meter	December 2009
	FC 0203, 50-micron LC/LC 31-meter	June 2016
	FC 0204, 50-micron LC/SC 31-meter	August 2011
	FC 0205, 62.5-micron LC/LC 31-meter	December 2009
	FC 0206, 62.5-micron LC/SC 31-meter	December 2009
	FC 0521, Functional enhancement field	June 2016
	FC 1032, 1 Gb grid dual port copper connection	June 2016
	FC 1033, 1 Gb grid dual port optical SW connection	June 2016
	FC 1034, Enable dual port grid connection	June 2016
	FC 2714, Console expansion	August 2011
	FC 2715, Console attachment	June 2016
	FC 3461, 8 GB Memory upgrade, field	June 2016
	FC 4015, Grid enablement	June 2016
	FC 4016, Remove Cluster from Grid	June 2016
	FC 4017, Cluster cleanup	June 2016
	FC 5242, Dual Port 16 Gb Fibre Channel HBA	June 2016
	FC 5268, 100 MB/sec increment	June 2016
	FC 5270, Increased virtual volumes	June 2016
	FC 5271, Selective device access control	June 2016
	FC 9000, Mainframe attachment	August 2011
	FC 9268, Plant installation of 100 MB/s throughput	August 2011
	FC 9350, Plant Install	August 2011
	FC 9461, 8 GB Memory upgrade, plant	August 2011
	FC 9700, No factory cables	August 2011

Table 66. Withdrawn TS7700 features (continued)

Associated machine type and model	Feature code withdrawn	Scheduled for withdrawal
TS7720 Server 3957-VEB	FC 0983, TAA Compliance	June 2016
	FC 2714, Console expansion	January 2013
	FC 2715, Console attachment	June 2016
	FC 9111, Ship with R2.0 machine code	June 2016
	FC 9111, Ship with R2.0 machine code	January 2013
	FC 9116, Ship with R3.3 Machine Code	June 2016
	FC 9350, Plant Install	June 2016
	FC 9351, Field merge TS7700 Server in 3952 F05	June 2016
	FC 9700, No factory cables	June 2016
TS7740 Cache Controller 3956-CC6	FC 6003, Intraframe fibre cable to 3957-V06	February 2009
	FC 7120, 1.7 TB fibre storage	February 2009
	FC 9230, Attach to 3957-V06	February 2009
	FC 9352, Plant Install	February 2009
TS7740 Cache Controller 3956-CC7	FC 7121, 3.43 TB fibre storage	June 2010
	FC 7403, Enable first expansion drawer	January 2013
	FC 9352, Plant Install	June 2010
TS7740 Cache Controller 3956-CC8	FC 7123, 9.6 TB Fibre storage	January 2013
	FC 7403, Enable first expansion drawer	January 2013
	FC 9352, Plant Install	January 2013
TS7740 Cache Controller 3956-CC9	FC 7124, 13.2 TB SAS storage	June 2016
	FC 9352, Plant Install	June 2016
TS7720 Cache Controller 3956-CS7	FC 7113, 16 TB SATA storage	June 2010
	FC 9352, Plant Install	June 2010
TS7720 Cache Controller 3956-CS8	FC 7114, 32 TB SATA storage	January 2013
	FC 9352, Plant Install	January 2013
TS7740 Cache Drawer 3956-CX6	FC 6000, Intraframe fibre cable to 3956-CC6	February 2012
	FC 7120, 1.7 TB fibre storage	February 2012
	FC 9354, Plant Install	February 2009
	FC 9355, Field merge	January 2013
TS7740 Cache Drawer 3956-CX7	FC 7121, 3.43 TB fibre storage	June 2010
	FC 7123, 9.6 TB Fibre storage	January 2013
	FC 9354, Plant Install	January 2013
	FC 9355, Field merge	January 2013

Table 66. Withdrawn TS7700 features (continued)

Associated machine type and model	Feature code withdrawn	Scheduled for withdrawal
TS7720 Cache Drawer 3956-XS7	FC 7113, 16 TB SATA storage	June 2010
	FC 7114, 32 TB SATA storage	January 2013
	FC 9354, Plant Install	January 2013
	FC 9355, Field merge	January 2013
†This feature has since been withdrawn.		

Related information

"Feature details" on page 149

"Quick reference by component"

TS7700 feature codes

This topic links to descriptions of TS7700 features according to component, feature code, and feature conversion (if applicable).

Quick reference by component

This topic lists feature codes for the TS7700 according to component machine type and model.

3952 Tape Frame features

Note: All TS7700 features are shown on this page. Withdrawn features and components are included for reference purposes, but are marked by a footnote.

3952 F06 Tape Frame features

- “FC 9954, NEMA L6-30 power cord” on page 181
- “FC 9955, RS 9750 DP power cord” on page 182
- “FC 9956, IEC 309 power cord” on page 182
- “FC 9957, PDL 4.3 power cord” on page 182
- “FC 9958, Korean 4.3-m power cord” on page 182
- “FC 9959, Unterminated power cord” on page 182
- “FC 9966, Unterminated power cord (China)” on page 182
- “FC AG00, Shipping and Handling - No charge” on page 183
- “FC AGGA, Shipping and Handling - F06” on page 183
- “FC AGKE, Ship with R4.1 Machine Code” on page 183

3952 F05 Tape Frame features

- “FC 1903, Power Distribution Unit” on page 154
- “FC 1904, Switching PDU” on page 154
- “FC 2704, TS3000 System Console expansion 26-port Ethernet switch/rackmount” on page 154
- “FC 2719, Console upgrade” on page 155†
- “FC 2725, Rackmount TS3000 System Console” on page 155
- “FC 2730, TS3000 System Console” on page 156†
- “FC 2732, TS3000 System Console” on page 156†
- “FC 2733, Internal modem” on page 156†
- “FC 2748, Optical drive” on page 156
- “FC 4743, Remove 3957-V06/VEA” on page 160
- “FC 5512, TS3000 System Console KVM display, keyboard, mouse” on page 164
- “FC 5626, Plant installation of 3957-VEA” on page 164†
- “FC 5627, Install 3957-VEB” on page 165
- “FC 5628, Plant installation of 3957-V06” on page 165†
- “FC 5629, Install 3957-V07” on page 165
- “FC 5635, Plant installation of 3956-CS8” on page 166†
- “FC 5636, Plant installation of 3956-CS7” on page 166†
- “FC 5638, Plant installation of 3956-CC6” on page 166†
- “FC 5639, Plant installation of 3956-CC7” on page 166†
- “FC 5640, Plant installation of 3956-CC8” on page 167†
- “FC 5641, Plant installation of 3956-CX7” on page 167†
- “FC 5642, Field installation of 3956-CX7” on page 167†
- “FC 5646, Plant installation of 3956-XS7” on page 167†
- “FC 5647, Field installation of 3956-XS7” on page 167†
- “FC 5648, Plant installation of 3956-CX6” on page 168†
- “FC 5649, Field installation of 3956-CX6” on page 168†
- “FC 5651, Plant installation of 3956-CS9” on page 168
- “FC 5652, Plant installation of 3956-CC9” on page 168
- “FC 5653, Plant installation of 3956-CX9” on page 169
- “FC 5654, Field installation of 3956-CX9” on page 169
- “FC 5655, Plant installation of 3956-XS9” on page 169
- “FC 5656, Field installation of 3956-XS9” on page 169

- “FC 5758, Integrated control path” on page 171
- “FC 5759, Integrated control path” on page 171†
- “FC 7312, TS7740 Base frame” on page 174†
- “FC 7322, TS7720 Base frame” on page 174†
- “FC 7323, TS7720 Storage expansion frame” on page 174†
- “FC 7330, TS7740 Encryption-capable base frame” on page 174
- “FC 7331, TS7720 Encryption-capable base frame” on page 174
- “FC 7332, TS7720 Encryption-capable expansion frame” on page 174
- “FC 9110, Ship with R1.7 machine code” on page 176†
- “FC 9111, Ship with R2.0 machine code” on page 176†
- “FC 9112, Ship with R2.1 machine code” on page 176†
- “FC 9113, Ship with R3.0 machine code” on page 176†
- “FC 9114, Ship with R3.1 machine code” on page 177†
- “FC 9323 Expansion frame attachment” on page 179
- “FC 9339, Replacing TS7740 System” on page 179
- “FC 9954, NEMA L6-30 power cord” on page 181
- “FC 9955, RS 9750 DP power cord” on page 182
- “FC 9956, IEC 309 power cord” on page 182
- “FC 9957, PDL 4.3 power cord” on page 182
- “FC 9958, Korean 4.3-m power cord” on page 182
- “FC 9959, Unterminated power cord” on page 182
- “FC 9966, Unterminated power cord (China)” on page 182

3953 F05 Tape Frame features

- “FC 2721, Rack mountable TS3000 System Console” on page 155
- “FC 4888, Switch mount kit” on page 160
- “FC 4897, Reinstall 4 Gb FC Switch” on page 161
- “FC 9013, Attach to TS7700” on page 176

†Withdrawn or to be withdrawn soon.

3957-Vxx Server features

3957-V07 Server features

- “FC 0201, 9-micron LC/LC 31-meter” on page 149
- “FC 0203, 50-micron LC/LC 31-meter” on page 150
- “FC 1034, Enable dual port grid connection” on page 152
- “FC 1035, 10 Gb grid optical LW connection” on page 153
- “FC 1036, 1 Gb grid dual port copper connection” on page 153
- “FC 1037, 1 Gb dual port optical SW connection” on page 153
- “FC 2714, Console expansion” on page 154†
- “FC 2715, Console attachment” on page 154
- “FC 3401, Enable FICON dual port” on page 156
- “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 157
- “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157
- “FC 3441, FICON short-wavelength attachment” on page 158
- “FC 3442, FICON long-wavelength attachment” on page 158

- “FC 3443, FICON 10-km long-wavelength attachment” on page 158
- “FC 4015, Grid enablement” on page 159
- “FC 4016, Remove Cluster from Grid” on page 159
- “FC 4017, Cluster cleanup” on page 160
- “FC 5241, Dual port FC HBA” on page 161
- “FC 5267, 1 TB cache enablement” on page 162
- “FC 5268, 100 MB/sec increment” on page 162
- “FC 5270, Increased virtual volumes” on page 162
- “FC 5271, Selective device access control” on page 163
- “FC 5272, Enable disk encryption - Local Key Management” on page 163
- “FC 5273, TS7720/TS7760 Tape Attach enablement” on page 163
- “FC 5274, Enable 1 TB Pending Tape Capacity” on page 163
- “FC 5275, Additional virtual devices” on page 164
- “FC 9000, Mainframe attachment” on page 175
- “FC 9111, Ship with R2.0 machine code” on page 176†
- “FC 9112, Ship with R2.1 machine code” on page 176†
- “FC 9113, Ship with R3.0 machine code” on page 176
- “FC 9114, Ship with R3.1 machine code” on page 177
- “FC 9219, Attach to TS3500/TS4500” on page 178†
- “FC 9350, Plant Install” on page 179†
- “FC 9351, Field merge TS7700 Server in 3952 F05” on page 179
- “FC 9700, No factory cables” on page 181
- “FC 9900, Tape Encryption configuration” on page 181

3957-VEB Server features

- “FC 0201, 9-micron LC/LC 31-meter” on page 149
- “FC 0203, 50-micron LC/LC 31-meter” on page 150
- “FC 1034, Enable dual port grid connection” on page 152
- “FC 1035, 10 Gb grid optical LW connection” on page 153
- “FC 1036, 1 Gb grid dual port copper connection” on page 153
- “FC 1037, 1 Gb dual port optical SW connection” on page 153
- “FC 2714, Console expansion” on page 154†
- “FC 2715, Console attachment” on page 154
- “FC 3401, Enable FICON dual port” on page 156
- “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 157
- “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157
- “FC 3441, FICON short-wavelength attachment” on page 158
- “FC 3442, FICON long-wavelength attachment” on page 158
- “FC 3443, FICON 10-km long-wavelength attachment” on page 158
- “FC 4015, Grid enablement” on page 159
- “FC 4016, Remove Cluster from Grid” on page 159
- “FC 4017, Cluster cleanup” on page 160
- “FC 5241, Dual port FC HBA” on page 161
- “FC 5268, 100 MB/sec increment” on page 162
- “FC 5270, Increased virtual volumes” on page 162
- “FC 5271, Selective device access control” on page 163

- “FC 5272, Enable disk encryption - Local Key Management” on page 163
- “FC 5273, TS7720/TS7760 Tape Attach enablement” on page 163
- “FC 5274, Enable 1 TB Pending Tape Capacity” on page 163
- “FC 5275, Additional virtual devices” on page 164
- “FC 9000, Mainframe attachment” on page 175
- “FC 9111, Ship with R2.0 machine code” on page 176†
- “FC 9112, Ship with R2.1 machine code” on page 176†
- “FC 9113, Ship with R3.0 machine code” on page 176
- “FC 9114, Ship with R3.1 machine code” on page 177
- “FC 9268, Plant installation of 100 MB/s throughput” on page 178
- “FC 9350, Plant Install” on page 179
- “FC 9351, Field merge TS7700 Server in 3952 F05” on page 179
- “FC 9700, No factory cables” on page 181

3957-VEC Server features

- “FC 0201, 9-micron LC/LC 31-meter” on page 149
- “FC 0203, 50-micron LC/LC 31-meter” on page 150
- “FC 0983, TAA Compliance” on page 151
- “FC 1034, Enable dual port grid connection” on page 152
- “FC 1036, 1 Gb grid dual port copper connection” on page 153
- “FC 1037, 1 Gb dual port optical SW connection” on page 153
- “FC 1038, 10 Gb dual port optical LW connection” on page 153
- “FC 2715, Console attachment” on page 154
- “FC 3401, Enable FICON dual port” on page 156
- “FC 3402, 16 Gb FICON Short Wavelength Attachment” on page 156
- “FC 3403, 16 Gb FICON Long Wavelength Attachment” on page 157
- “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 157
- “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 157
- “FC 4015, Grid enablement” on page 159
- “FC 4016, Remove Cluster from Grid” on page 159
- “FC 4017, Cluster cleanup” on page 160
- “FC 5242, Dual Port 16 Gb Fibre Channel HBA” on page 162
- “FC 5268, 100 MB/sec increment” on page 162
- “FC 5270, Increased virtual volumes” on page 162
- “FC 5271, Selective device access control” on page 163
- “FC 5272, Enable disk encryption - Local Key Management” on page 163
- “FC 5273, TS7720/TS7760 Tape Attach enablement” on page 163
- “FC 5274, Enable 1 TB Pending Tape Capacity” on page 163
- “FC 5275, Additional virtual devices” on page 164
- “FC 9000, Mainframe attachment” on page 175
- “FC 9219, Attach to TS3500/TS4500” on page 178
- “FC 9268, Plant installation of 100 MB/s throughput” on page 178
- “FC 9350, Plant Install” on page 179
- “FC 9700, No factory cables” on page 181
- “FC 9900, Tape Encryption configuration” on page 181
- “FC AGKE, Ship with R4.1 Machine Code” on page 183

| • "FC AGKR, Ship with R4.1.2 Machine Code" on page 183

†Withdrawn or to be withdrawn soon.

3956-CC7, 3956-CC8, 3956-CC9, 3956-CS8, 3956-CS9, and 3956-CSA Cache Controller features

3956-CC7† Cache Controller features

- "FC 7121, 3.43 TB fibre storage" on page 173†
- "FC 7403, Enable first expansion drawer" on page 175†
- "FC 9352, Plant Install" on page 179†
- "FC 9353, Field merge in 3952 F05" on page 180

3956-CC8† Cache Controller features

- "FC 7123, 9.6 TB Fibre storage" on page 173†
- "FC 7403, Enable first expansion drawer" on page 175†
- "FC 9352, Plant Install" on page 179

3956-CC9† Cache Controller features

- "FC 7124, 13.2 TB SAS storage" on page 173
- "FC 7404, Encryption" on page 175
- "FC 9352, Plant Install" on page 179

3956-CS7† Cache Controller features

- "FC 7113, 16 TB SATA storage" on page 172†
- "FC 9352, Plant Install" on page 179†

3956-CS8† Cache Controller features

- "FC 7114, 32 TB SATA storage" on page 172
- "FC 9352, Plant Install" on page 179

3956-CS9† Cache Controller features

- "FC 7115, 36 TB SAS storage" on page 172
- "FC 7404, Encryption" on page 175
- "FC 9352, Plant Install" on page 179

3956-CSA Cache Controller features

- "FC 0983, TAA Compliance" on page 151
- "FC 7117, 48 TB SAS Storage" on page 172
- "FC 7118, 96 TB SAS Storage" on page 173
- "FC 7404, Encryption" on page 175
- "FC 9352, Plant Install" on page 179

†Withdrawn or to be withdrawn soon.

3956-CX7, 3956-CX9, 3956-XS7, 3956-XS9, and 3956-XSA Cache Drawer features

3956-CX7† Cache Drawer features

- "FC 7123, 9.6 TB Fibre storage" on page 173†
- "FC 9354, Plant Install" on page 180
- "FC 9355, Field merge" on page 180

3956-CX9 Cache Drawer features

- “FC 7124, 13.2 TB SAS storage” on page 173
- “FC 7404, Encryption” on page 175
- “FC 9354, Plant Install” on page 180
- “FC 9355, Field merge” on page 180

3956-XS7† Cache Drawer features

- “FC 7113, 16 TB SATA storage” on page 172†
- “FC 7114, 32 TB SATA storage” on page 172†
- “FC 9354, Plant Install” on page 180
- “FC 9353, Field merge in 3952 F05” on page 180

3956-XS9 Cache Drawer features

- “FC 7404, Encryption” on page 175
- “FC 7116, 33 TB SAS storage” on page 172
- “FC 9354, Plant Install” on page 180
- “FC 9355, Field merge” on page 180

3956-XSA Cache Drawer features

- “FC 0983, TAA Compliance” on page 151
- “FC 7117, 48 TB SAS Storage” on page 172
- “FC 7118, 96 TB SAS Storage” on page 173
- “FC 7404, Encryption” on page 175
- “FC 9354, Plant Install” on page 180
- “FC 9355, Field merge” on page 180

†Withdrawn or to be withdrawn soon.

Related information

“Feature details”

Feature details

This topic describes feature codes for the TS7700.

FC 0201, 9-micron LC/LC 31-meter

FC 0201, 9-micron LC/LC 31-meter, provides a 31-meter (101 ft.), 9-micron, single mode FICON cable with LC Duplex connectors on both ends for connection between the long wavelength FICON channel feature and a host system or a fibre component long wavelength channel with a 9–micron fibre cable LC Duplex adapter.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 0201, 9-micron LC/LC 31-meter in Table 67 on page 184 for requirements and other information.

FC 0202, 9-micron LC/SC 31-meter

FC 0202, 9-micron LC/SC 31-meter, provides a 31-meter, (101 ft.), 9-micron, single mode FICON cable with and LC Duplex connector on one end for connection to the long wavelength FICON channel feature, and an SC Duplex connector on the other end for connection to a host system or fibre component long wavelength channel with a 9–miron fibre cable SC Duplex adapter.

Note: This feature has been withdrawn.

Refer to FC 0202, 9-micron LC/SC 31-meter in Table 67 on page 184 for requirements and other information.

FC 0203, 50-micron LC/LC 31-meter

FC 0203, 50-micron LC/LC 31-meter, provides a 31-meter (101 ft.), 50-micron, single mode FICON cable with LC Duplex connectors on both ends for connection between the long wavelength FICON channel feature and a host system or a fibre component short wavelength channel with a 50–micron fibre cable LC Duplex adapter.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 0203, 50-micron LC/LC 31-meter in Table 67 on page 184 for requirements and other information.

FC 0204, 50-micron LC/SC 31-meter

FC 0204, 50-micron LC/SC 31-meter, provides a 31-meter, (101 ft.), 50-micron, single mode FICON cable with and LC Duplex connector on one end for connection to the short wavelength FICON channel feature, and an SC Duplex connector on the other end for connection to a host system or fibre component long wavelength channel with a 50–micron fibre cable SC Duplex adapter.

Note: This feature is withdrawn from use with a 3957-V06/VEA. It is still available for use with a 3957-V07/VEB.

Refer to FC 0204, 50-micron LC/SC 31-meter in Table 67 on page 184 for requirements and other information.

FC 0205, 62.5-micron LC/LC 31-meter

FC 0205, 62.5-micron LC/LC 31-meter, provides a 31-meter (101 ft.), 62.5-micron, single mode FICON cable with LC Duplex connectors on both ends for connection between the long wavelength FICON channel feature and a host system or a fibre component long wavelength channel with a 62.5–micron fibre cable LC Duplex adapter.

Note: This feature has been withdrawn.

Refer to FC 0205, 62.5-micron LC/LC 31-meter in Table 67 on page 184 for requirements and other information.

FC 0206, 62.5-micron LC/SC 31-meter

FC 0206, 62.5-micron LC/SC 31-meter, provides a 31-meter, (101 ft.), 62.5-micron, single mode FICON cable with and LC Duplex connector on one end for connection to the long wavelength FICON channel feature, and an SC Duplex connector on the other end for connection to a host system or fibre component long wavelength channel with a 62.5–micron fibre cable SC Duplex adapter.

Note: This feature has been withdrawn.

Refer to FC 0206, 62.5-micron LC/SC 31-meter in Table 67 on page 184 for requirements and other information.

FC 0521, Functional enhancement field

FC 0521, Functional enhancement field, provides a one-time update to the microcode of an installed TS7700 to provide enhanced functions contained in the latest level of functional microcode firmware support. Newer microcode levels may be required when adding new functions.

Note: This feature was withdrawn on June 2016.

Refer to FC 0521, Functional enhancement field in Table 67 on page 184 for requirements and other information.

FC 0983, TAA Compliance

FC 0983, TAA Compliance, indicates that the product is TAA compliant.

Note: This feature is not available in India for use.

Refer to FC 0983, TAA Compliance in Table 67 on page 184 for requirements and other information.

FC 1030, 1Gb grid copper connection

FC 1030, 1Gb grid copper connection, provides an Ethernet 1000BaseT adapter for grid communication between TS7740s. You must supply your own Ethernet cables when FC 4015, Grid enablement, is installed. Cat-5 Ethernet cables are not allowed. This adapter has an RJ-45 connector and conforms to the IEEE 802.3ab 1000Base-T standard. The Ethernet cables used with the adapter must be Cat-5e or Cat-6, though Cat-6 is preferred. It supports distances of up to 100 meters using four pairs of Cat-5e or Cat-6 balanced copper cabling.

Note: This feature has been withdrawn.

Refer to FC 1030, 1Gb grid copper connection in Table 67 on page 184 for requirements and other information.

FC 1031, 1Gb optical SW connection

FC 1031, 1Gb optical SW connection, provides a 1-Gb shortwave adapter for grid communication between TS7740s. It replaces RPQ #Q8B3409. This adapter has an LC Duplex connector for attaching a 50.0- or 62.5-micron, multi-mode fibre cable. This is a standard shortwave (850 nm) adapter that conforms to the IEEE 802.3z standards. It supports distances of 2 to 260 meters for 62.5-micron cable and 2 to 550 meters for 50.0-micron cable. Multi-mode fibre cables must be used with the adapter when FC 4015, Grid enablement, is installed.

Note: This feature has been withdrawn.

Refer to FC 1031, 1Gb optical SW connection in Table 67 on page 184 for requirements and other information.

FC 1032, 1 Gb grid dual port copper connection

FC 1032, 1 Gb grid dual port copper connection, provides a dual port, 1-Gbps 10/100/1000Base-TX adapter for grid communication between TS7700s with a single port enabled. This adapter has an RJ-45 connector for attaching Cat-5e or Cat-6 cables. This adapter conforms to the IEEE 802.3ab 1000Base-T standard. It supports distances up to 100 meters using four pairs of Cat-5e or Cat-6 balanced copper cabling. You must supply Cat-5e or Cat-6 cables for use with the adapter when FC 4015, Grid enablement is installed. This feature is supported only on a 3957-V06 or 3957-VEA operating a microcode level of 8.5.0.xx or later.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 1032, 1 Gb grid dual port copper connection in Table 67 on page 184 for requirements and other information.

FC 1033, 1 Gb grid dual port optical SW connection

FC 1033, 1 Gb grid dual port optical SW connection, provides a dual port, 1-Gbps Ethernet shortwave adapter for grid communication between TS7700s with a single port enabled. This adapter has an LC Duplex connector for attaching 50-micron or 62.5-micron, multimode fibre cable. This is a standard shortwave (850 nm) adapter that conforms to the IEEE 802.3z standards. It supports distances of 260 meters for 62.5-micron and 550 meters for 50.0-micron cable. Multi-mode fibre cables must be used with the adapter when FC 4015, Grid enablement is installed. This feature is supported only on a 3957-V06 or 3957-VEA operating a microcode level of 8.5.0.xx or later.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 1033, 1 Gb grid dual port optical SW connection in Table 67 on page 184 for requirements and other information.

FC 1034, Enable dual port grid connection

FC 1034, Enable dual port grid connection, enables the second port of each dual port 1-Gb grid connection adapter provided by FC 1032, FC 1033, FC 1036, FC 1037, or FC 1038. This feature is supported only with a microcode level of 8.20.0.xx or later.

All clusters on the grid must comply with the grid compatibility rules before this feature is enabled. If the TS7700 Server is currently configured as a stand-alone cluster but will be joined to one or more clusters in a grid you must replace the adapters of all other systems in the grid before joining the clusters. If the TS7700 Server is already part of a grid and IP addresses are being added or changed, you must activate the additional ports on the adapters of all other systems in the grid. Before you configure the TS7700 Grid communications for new IPs, verify that adapters are fully installed on all clusters, all grid adapter ports are activated and all clusters are properly cabled.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 1034, Enable dual port grid connection in Table 67 on page 184 for requirements and other information.

FC 1035, 10 Gb grid optical LW connection

FC 1035, 10 Gb grid optical LW connection, provides a single port, 10-Gbps Ethernet longwave adapter for grid communication between TS7700s. This adapter has an LC Duplex connector for attaching 9-micron, single-mode fibre cable. This is a standard longwave (1,310 nm) adapter that conforms to the IEEE 802.3ae standards. It supports distances up to 10 km. This feature is supported only on a 3957-V07 or 3957-VEB operating a microcode level of 8.20.0.xx or later.

Note: These adapters cannot negotiate down to run at 1 Gb. They must be connected to a 10-Gb network device or light point.

Refer to FC 1035, 10 Gb grid optical LW connection in Table 67 on page 184 for requirements and other information.

FC 1036, 1 Gb grid dual port copper connection

FC 1036, 1 Gb grid dual port copper connection provides a dual port 1-Gbps 10/100/1000 Base-TX PCIe Ethernet adapter for grid communication between TS7700s with a single port enabled. This adapter has an RJ-45 connector for attaching Cat6 cables. It conforms to the IEEE 802.3ab 1000 Base-T standard. It supports distances of up to 100 meters using four pairs of Cat6 balanced copper cabling. This feature is supported only on a 3957-V07, 3957-VEB, or 3957-VEC operating a microcode level of 8.20.0.xx or later.

When FC 4015, Grid enablement, is installed customer-supplied Cat6 cables must be used with this adapter.

Refer to FC 1036, 1 Gb grid dual port copper connection in Table 67 on page 184 for requirements and other information.

FC 1037, 1 Gb dual port optical SW connection

FC 1037, 1 Gb dual port optical SW connection provides a dual port 1-Gbps shortwave PCIe Ethernet adapter for grid communication between TS7700s with a single port enabled. This adapter has an LC Duplex connector for attaching 50 micron or 62.5 micron multimode fibre cable. It is a standard shortwave (850 nm) adapter conforming to the IEEE 802.3z standards. It supports distances of up to 260 meters when used with a 62.5 micron cable and up to 550 meters when used with a 50.0 micron cable. This feature is supported only on a 3957-V07, 3957-VEB, or 3957-VEC operating a microcode level of 8.20.0.xx or later.

When FC 4015, Grid enablement, is installed multi-mode fiber cables must be used with this adapter.

Refer to FC 1037, 1 Gb dual port optical SW connection in Table 67 on page 184 for requirements and other information.

FC 1038, 10 Gb dual port optical LW connection

FC 1038, 10 Gb dual port optical LW connection provides a dual port 10-Gbps Ethernet longwave adapter for Grid Communication between TS7700s. This adapter has an LC Duplex connector for attaching 9 micron single mode fibre cable. It is a standard longwave (1,310 nm) adapter conforming to the IEEE 802.3ae standards. It supports distances up to 10 km.

Note: These adapters can not negotiate down to run at 1 Gb. They must be connected to a 10 Gb network device.

Refer to FC 1038, 10 Gb dual port optical LW connection in Table 67 on page 184 for requirements and other information.

FC 1903, Power Distribution Unit

FC 1903, Power Distribution Unit, provides one additional PDU to allow connection to independent branch power circuits. This feature supplies two power cords when ordered.

Refer to FC 1903, Power Distribution Unit in Table 67 on page 184 for requirements and other information.

FC 1904, Switching PDU

FC 1904, Switching PDU, provides power switching to allow a TS7700 full power redundancy.

Refer to FC 1904, Switching PDU in Table 67 on page 184 for requirements and other information.

FC 2704, TS3000 System Console expansion 26-port Ethernet switch/rackmount

FC 2704, TS3000 System Console expansion 26-port Ethernet switch/rackmount, provides a 26-port Ethernet switch and attachment cable for connection to a IBM TS3000 System Console (TSSC). Up to 24 additional connections are provided by this feature for connection of TSSC FC 2714, 2715, or another FC 2704.

Refer to FC 2704, TS3000 System Console expansion 26-port Ethernet switch/rackmount in Table 67 on page 184 for requirements and other information.

FC 2714, Console expansion

FC 2714, Console expansion, provides an attachment cable, rack-mounted Ethernet switch, and associated mounting hardware to attach the TS7700 Server to an existing external TS3000 System Console (FC 2720, FC 2721, FC 2722, FC 2730, or FC 2732) or IBM Master Console for Service (FC 2718, obsolete).

Note: This feature is withdrawn from use with a 3957-V06/VEA. It is still available for use with a 3957-V07/VEB.

Refer to FC 2714, Console expansion in Table 67 on page 184 for requirements and other information.

FC 2715, Console attachment

FC 2715, Console attachment, provides a cable to attach to the Ethernet hub provided by an existing TS3000 System Console (FC 2720, 2721, 2722, 2730 or 2732) or IBM TotalStorage Master Console for Service (FC 2718), or Console Expansion (FC 2714). A maximum of 40 of FC 2715 may be included in a single console facility.

Note: This feature is withdrawn from use with a 3957-V06/V07/VEB.

Refer to FC 2715, Console attachment in Table 67 on page 184 for requirements and other information.

FC 2719, Console upgrade

FC 2719, Console upgrade, provides a second Ethernet network interface card to allow redundant attachment to the service network. This feature provides a memory upgrade to 2 GB total RAM and a second Ethernet card to allow redundant connections into the service network. This feature only applies to consoles shipped with FC 2718, FC 2720, TS3000 System Console, or by FC 2721, Rack mountable TS3000 System Console. It is required for use with any TS7700 using features FC 2714, Console expansion, FC 2715, Console attachment, or FC 2720, TS3000 System Console.

Note: This feature has been withdrawn.

Refer to FC 2719, Console upgrade in Table 67 on page 184 for requirements and other information.

FC 2720, TS3000 System Console

FC 2720, TS3000 System Console, provides the IBM TotalStorage Master Console, an Ethernet hub, and a cable and connectors to enable remote enhanced service connection of a TS7740 to an IBM-supplied modem. The Ethernet hub provides 14 additional connections for cables supplied with FC 2714, Console expansion, or FC 2715, Console attachment. You should specify FC 2720, TS3000 System Console on the first unit in an installation connected to a master console facility. Support for this feature on the 3957-V06 was withdrawn on December 5, 2008. To use this feature, order it against the 3953 F05 Tape Frame.

Note: Most customers prefer to use the rack mount TSSC on the 3953 F05 Tape Frame, (FC 2721, Rack mountable TS3000 System Console) instead of the desktop TSSC.

Refer to FC 2720, TS3000 System Console in Table 67 on page 184 for requirements and other information.

FC 2721, Rack mountable TS3000 System Console

FC 2721, Rack mountable TS3000 System Console, provides the rack mountable TS3000 System Console, an Ethernet switch for the Master Console and a cable and connector for connection of one subsystem.

Refer to FC 2721, Rack mountable TS3000 System Console in Table 67 on page 184 for requirements and other information.

FC 2725, Rackmount TS3000 System Console

FC 2725, Rackmount TS3000 System Console provides the enhanced rack-mountable TSSC 1U server and an Ethernet cable for connection to the rack mount switch. This feature is an enhanced replacement of the IBM TS3000 System Console for Service (feature #2722, #2724, #2730, or #2732).

Refer to FC 2725, Rackmount TS3000 System Console in Table 67 on page 184 for requirements and other information.

FC 2730, TS3000 System Console

FC 2730, TS3000 System Console provides a rack mount version of the TS3000 System Console for installation in a TS7720 or TS7740 3952 F05 frame or a customer provided rack. FC 2730, TS3000 System Console provides a 1U server, keyboard, display, mouse, and Ethernet switch.

Note: This feature has been withdrawn.

Refer to FC 2730, TS3000 System Console in Table 67 on page 184 for requirements and other information.

FC 2732, TS3000 System Console

FC 2733, Internal modem

FC 2734, TS3000 System Console USB modem

FC 2734, TS3000 System Console USB modem provides a USB modem for use with FC 2724.

Note: This feature has been withdrawn.

Refer to FC 2734, TS3000 System Console USB modem in Table 67 on page 184 for requirements and other information.

FC 2748, Optical drive

FC 2748, Optical drive provides an optical drive for use with the TS3000 System Console.

Refer to FC 2748, Optical drive in Table 67 on page 184 for requirements and other information.

FC 3401, Enable FICON dual port

FC 3401, Enable FICON dual port, enables the second port on each installed FICON adapter.

Refer to FC 3401, Enable FICON dual port in Table 67 on page 184 for requirements and other information.

Note: Unless No Factory Cables (FC 9700) has been selected, two cables are required for each active FICON port. When installing FC 3401, include two FC 0201 cables for each FC 3403 or FC 3439 FICON card configured, and two FC 0203 for each FC 3402 or FC 3438 FICON card configured.

FC 3402, 16 Gb FICON Short Wavelength Attachment

FC 3402, 16 Gb FICON Short Wavelength Attachment, provides one short-wavelength FICON adapter with an LC Duplex connector. One port is active by default. The adapter attaches to a FICON host system short wave channel utilizing a 50 micron or 62.5 micron multimode fibre cable. Each FICON attachment can support up to 512 logical channels. At 16 Gb/sec speed, the total cable length cannot exceed:

- 130 meters using 50 micron OM4 (4700 MHz*km) Aqua blue colored fibre

- 100 meters using 50 micron OM3 (2000 MHz*km) Aqua blue colored fibre
- 35 meters using 50 micron OM2 (500 MHz*km) Orange colored fibre
- OM1 is not recommended for 16 Gb FICON connections

Refer to FC 3402, 16 Gb FICON Short Wavelength Attachment in Table 67 on page 184 for requirements and other information.

FC 3403, 16 Gb FICON Long Wavelength Attachment

FC 3403, 16 Gb FICON Long Wavelength Attachment, provides one long-wavelength FICON adapter, with an LC Duplex connector. One port is active by default. The adapter attaches to a FICON host system long wave channel utilizing a 9-micron single-mode fibre cable. The total cable length cannot exceed 10 km. Each FICON attachment can support up to 512 logical channels.

Refer to FC 3403, 16 Gb FICON Long Wavelength Attachment in Table 67 on page 184 for requirements and other information.

FC 3438, 8 Gb FICON Short Wavelength Attachment

FC 3438, 8 Gb FICON Short Wavelength Attachment provides one short-wavelength FICON adapter with an LC Duplex connector, for attachment to a FICON host system short wave channel utilizing a 50 micron or 62.5 micron multimode fibre cable. Each FICON attachment can support up to 512 logical channels. At 8 Gb/sec speed, the total cable length cannot exceed:

- 150 meters using 50 micron OM3 (2000MHz*km) Aqua blue colored fibre
- 50 meters using 50 micron OM2 (500MHz*km) Orange colored fibre
- 21 meters using 62.5 micron OM1 (200MHz*km) Orange colored fibre

Important 8 Gb installation information: Due to **higher sensitivity** (increased FICON speed 4G -> 8G) before using a wrap plug or plugging a new or existing cable into any LC Duplex connector, ensure the cable ends and the adapter duplex connector laser transmit/receive ports in the SFP are also cleaned with **Fiber Cleaning Tool P/N 54Y4392** before making a connection. Fibre cables to the affected FICON ports must be undamaged and clean. Use **Fiber Cleaning Tool P/N 54Y4392** to clean FICON host cables and host adapter LC duplex connector. If errors that occur during installation of the 8 Gb FICON adapters and cables are not corrected during cable and SFP cleaning and card replacement then you must contact your cabling contractor.

Refer to FC 3438, 8 Gb FICON Short Wavelength Attachment in Table 67 on page 184 for requirements and other information.

FC 3439, 8 Gb FICON Long Wavelength Attachment

FC 3439, 8 Gb FICON Long Wavelength Attachment provides one long-wavelength FICON adapter, with an LC Duplex connector, for the attachment to a FICON host system long wave channel utilizing a 9-micron single-mode fibre cable. The total cable length cannot exceed 10 km. Each FICON attachment can support up to 512 logical channels.

Important 8 Gb installation information: Due to **higher sensitivity** (increased FICON speed 4G -> 8G) before using a wrap plug or plugging a new or existing cable into any LC Duplex connector, ensure the cable ends and the adapter duplex connector laser transmit/receive ports in the SFP are also cleaned with **Fiber**

Cleaning Tool P/N 54Y4392 before making a connection. Fibre cables to the affected FICON ports must be undamaged and clean. Use **Fiber Cleaning Tool P/N 54Y4392** to clean FICON host cables and host adapter LC duplex connector. If errors that occur during installation of the 8 Gb FICON adapters and cables are not corrected during cable and SFP cleaning and card replacement then you must contact your cabling contractor.

Refer to FC 3439, 8 Gb FICON Long Wavelength Attachment in Table 67 on page 184 for requirements and other information.

FC 3441, FICON short-wavelength attachment

FC 3441, FICON short-wavelength attachment provides one short-wavelength 4-Gbps FICON adapter with an LC duplex connector for attachment to a FICON host system short-wavelength channel using a 50- or 62.5-micron multi-mode fibre cable. At 4 Gb/sec, the maximum fibre cable length allowed by 50-micron cable is 150 m (492 ft.), 55 m (180 ft.) if using 62.5-micron cable. Each 4-Gbps FICON attachment can support up to 256 virtual channels.

Refer to FC 3441, FICON short-wavelength attachment in Table 67 on page 184 for requirements and other information.

FC 3442, FICON long-wavelength attachment

FC 3442, FICON long-wavelength attachment provides one long-wavelength 4-Gbps FICON adapter with an LC duplex connector for attachment of a TS7700 to a FICON host system long-wavelength channel using a 9-micron single-mode fibre cable. The maximum fibre cable length is 4 km (2.48 mi.). Each 4-Gbps FICON attachment can support up to 256 virtual channels.

Refer to FC 3442, FICON long-wavelength attachment in Table 67 on page 184 for requirements and other information.

FC 3443, FICON 10-km long-wavelength attachment

FC 3443, FICON 10-km long-wavelength attachment provides one long-wavelength 4-Gbps FICON adapter with an LC duplex connector for attachment to a FICON host system long-wavelength channel using a 9-micron single-mode fibre cable. The maximum fibre cable length is 10 km (6.21 mi.). Each 4-Gbps FICON attachment can support up to 256 virtual channels.

Refer to FC 3443, FICON 10-km long-wavelength attachment in Table 67 on page 184 for requirements and other information.

FC 3461, 8 GB Memory upgrade, field

FC 3461, 8 GB Memory upgrade, field, delivers a field-installable TS7700 Server memory upgrade to 16 GB RAM. This feature is supported only on the 3957-V06 or 3957-VEA and is required to install a microcode level of 8.20.0.xx or later.

Note: This feature was withdrawn on June 2016.

Refer to FC 3461, 8 GB Memory upgrade, field in Table 67 on page 184 for requirements and other information.

FC 3462, 16 GB memory upgrade

FC 3462, 16 GB memory upgrade, provides an additional 16 GB RAM to the TS7700 Server.

Refer to FC 3462, 16 GB memory upgrade in Table 67 on page 184 for requirements and other information.

FC 3488, 4 Gb Fibre Channel Switch

FC 3488, 4 Gb Fibre Channel Switch, provides a 4 Gb fibre channel switch to attach to 3592 Tape Drives in the 3584 Tape Library. The 4 Gb fibre channel switch has dual power connection for optional attachment to separate power supplies. The fibre channel switch types must be the same (2 Gb or 4 Gb) and cannot be intermixed within FC 4888, Switch mount kit.

Note: This feature has been withdrawn.

Refer to FC 3488, 4 Gb Fibre Channel Switch in Table 67 on page 184 for requirements and other information.

FC 4015, Grid enablement

FC 4015, Grid enablement, provides a key to enable the communication function that allows a TS7700 to communicate with other TS7700s in a grid. Each TS7700 must have this feature to be able to participate in a grid configuration.

Note: If all clusters in a grid configuration already have FC 4015, Grid enablement installed, contact your IBM Service Representative to properly set up, connect, and configure the grid environment.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 4015, Grid enablement in Table 67 on page 184 for requirements and other information.

FC 4016, Remove Cluster from Grid

FC 4016, Remove Cluster from Grid, delivers instructions for a one-time process to remove a TS7700 Cluster from a TS7700 Grid. You must order this feature before you can perform a cluster cleanup (FC 4017, Cluster cleanup) on any TS7700 Cluster configured to participate in a TS7700 Grid. If a TS7700 Cluster is removed from a TS7700 Grid, cleaned up using FC 4017, Cluster cleanup, and then joined to a new TS7700 Grid, another instance of FC 4016, Remove Cluster from Grid, is required to remove the cluster from the new Grid.

Note: If the cluster removal process is initiated from a cluster operating a microcode level earlier than 8.7.0.134 , all clusters in the grid must be at the same level of code before this feature can be used. If the cluster removal process is initiated from a cluster operating a microcode level of 8.7.0.134 code or later, then an intermix of code levels is permitted for use with this feature.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 4016, Remove Cluster from Grid in Table 67 on page 184 for requirements and other information.

FC 4017, Cluster cleanup

FC 4017, Cluster cleanup, facilitates a one-time cluster cleanup to clean the database, delete virtual volumes from the Tape Volume Cache, and remove configuration data for host connections from a TS7700 Cluster. If the cluster is a member of a TS7700 Grid, the cluster must first be removed from the Grid using FC 4016, Remove Cluster from Grid. If another cleanup is required on this TS7700 Cluster, another instance of FC 4017, Cluster cleanup, is required.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 4017, Cluster cleanup in Table 67 on page 184 for requirements and other information.

FC 4743, Remove 3957-V06/VEA

FC 4743, Remove 3957-V06/VEA, directs the removal of the 3957-V06 or 3957-VEA from the 3952 F05 Tape Frame. A new 3957-V07 (FC 5629, Install 3957-V07) must be ordered to replace a removed 3957-V06. A new 3957-VEB (FC 5627, Install 3957-VEB) must be ordered to replace a removed 3957-VEA. The instructions for the field installation of a new model 3957-V07 or 3957-VEB are delivered with this feature.

Refer to FC 4743, Remove 3957-V06/VEA in Table 67 on page 184 for requirements and other information.

FC 4879, TS7700 BE Switch Mounting Hardware

FC 4879, TS7700 BE Switch Mounting Hardware, provides mounting hardware for two Fibre Channel switches including rack brackets and power cords.

Refer to FC 4879, TS7700 BE Switch Mounting Hardware in Table 67 on page 184 for requirements and other information.

FC 4880, TS7700 BE 16 Gb Fibre Channel Switch

FC 4880, TS7700 BE 16 Gb Fibre Channel Switch, provides one 16 Gb Fibre channel switch.

Refer to FC 4880, TS7700 BE 16 Gb Fibre Channel Switch in Table 67 on page 184 for requirements and other information.

FC 4888, Switch mount kit

FC 4888, Switch mount kit, provides the mounting hardware for up to two fibre channel switches on the 3953 F05 Tape Frame that contains a 3592 J70 Controller or is attached to a VTS. It includes the required mounting hardware, bifurcated power cables, and instructions for installing up to two fibre channel switches in the 3953 F05 Tape Frame. The fibre channel switch types must be the same (2-Gb or 4-Gb) and cannot be intermixed within FC 4888, Switch mount kit.

Refer to FC 4888, Switch mount kit in Table 67 on page 184 for requirements and other information.

FC 4897, Reinstall 4 Gb FC Switch

FC 4897, Reinstall 4 Gb FC Switch, provides a customer-owned 4 Gb fibre channel switch to attach to 3592 Tape Drives in the 3584 Tape Library. The 4 Gb fibre channel switch has dual power connection for optional attachment to separate power supplies. The fibre channel switch types must be the same (2 Gb or 4 Gb) and cannot be intermixed within FC 4888, Switch mount kit.

Refer to FC 4897, Reinstall 4 Gb FC Switch in Table 67 on page 184 for requirements and other information.

FC 5240, Dual port fibre channel host bus adapter

FC 5240, Dual port fibre channel host bus adapter, installs two fibre channel interface cards in the TS7700 Server (3957-V06 or 3957-VEA) and provides two 31 Meter, 50 µ fibre channel cables to connect the TS7700 Server to the fibre channel switch.

When ordered against the TS7720 Server (3957-VEA), this feature connects the disk arrays in the 3952 Storage Expansion Frame with the 3957-VEA.

For situations where customer-supplied fibre channel cables connect the TS7700 to the Fibre Channel switches, and a 4 Gb/second rate is expected, the following maximum length restrictions apply:

- 50 µ, 500 MHz multimode fibre channel cables cannot exceed 150 meters.
- 62.5 µ, 200 MHz fibre channel cables cannot exceed 70 meters.

Note: This feature was withdrawn on June 2016.

Refer to FC 5240, Dual port fibre channel host bus adapter in Table 67 on page 184 for requirements and other information.

FC 5241, Dual port FC HBA

FC 5241, Dual port FC HBA, installs two fibre channel interface cards in the TS7700 Server (3957-V07 or 3957-VEB) and provides two 31 Meter, 50 µ fibre channel cables to connect the TS7700 Server to the fibre channel switch.

When ordered against the TS7740 Server (3957-V07), this feature connects a fibre switch and back-end tape drives to the 3957-V07. When ordered against the TS7720 Server (3957-VEB), this feature connects the disk arrays in the 3952 Storage Expansion Frame with the 3957-VEB.

For situations where customer-supplied fibre channel cables connect the TS7700 to the Fibre Channel switches, and a 8 Gb/second rate is expected, the following maximum length restrictions apply:

- 50 µ, 2000 MHz multimode fibre channel aqua blue cables cannot exceed 150 meters.
- 50 µ, 500 MHz multimode fibre channel orange cables cannot exceed 50 meters.
- 62.5 µ, 200 MHz fibre channel cables cannot exceed 21 meters.

Note: This feature was withdrawn on June 2016.

Refer to FC 5241, Dual port FC HBA in Table 67 on page 184 for requirements and other information.

FC 5242, Dual Port 16 Gb Fibre Channel HBA

FC 5242, Dual Port 16 Gb Fibre Channel HBA, delivers two dual-ported 16 Gb Fibre Channel HBAs and associated cables. These HBAs connect to the TS7700 Expansion frame.

FC 5242, Dual Port 16 Gb Fibre Channel HBA is used only for the TS7700 Expansion frames. For situations where customer-supplied Fibre Channel cables connect the TS7700 to the TS7700 Expansion frames, and a 16 Gb/second rate dictates, the following maximum length restrictions apply:

- 50 µ, 2000 MHz multimode Fibre Channel aqua blue cables cannot exceed 100 meters.
- 50 µ, 500 MHz multimode Fibre Channel orange cables cannot exceed 35 meters.

Refer to FC 5242, Dual Port 16 Gb Fibre Channel HBA in Table 67 on page 184 for requirements and other information.

FC 5267, 1 TB cache enablement

FC 5267, 1 TB cache enablement, delivers a key to enable a 1 TB increment of disk cache to store virtual volumes. Enabling a cache increment does not guarantee that amount of additional cache capacity. The amount of additional cache capacity provided is limited by the capacity of the underlying physical cache installed.

This feature is available only with the TS7740.

Note: This feature is withdrawn from use with a 3957-V06.

Refer to FC 5267, 1 TB cache enablement in Table 67 on page 184 for requirements and other information.

FC 5268, 100 MB/sec increment

FC 5268, 100 MB/sec increment, delivers a key to enable an additional 100 MB/sec increment of potential Peak Data Throughput. Enabling a data throughput increment does not guarantee that the overall TS7700 performs at that data throughput level. However, installation of the maximum allowed feature codes results in unrestricted peak data throughput capabilities.

A maximum of 6 instances of 100 MB/sec is allowed on a 3957-V06 or 3957-VEA, where FC 9268 represents the first instance for a 3957-VEA. If FC 3441, FC 3442, or FC 3443 is installed, a maximum of 10 instances of 100 MB/sec is allowed on the 3957-V07 or 3957-VEB, where FC 9268 represents the first instance for a 3957-VEB. If FC 3438 or FC 3439 is installed, a maximum of 25 instances of 100 MB/sec is allowed on the 3957-V07, 3957-VEB, or 3957-VEC where FC 9268 represents the first instance for a 3957-VEB or 3957-VEC.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

FC 5270, Increased virtual volumes

FC 5270, Increased virtual volumes, increases by 200,000 the number of virtual volumes supported on a cluster. You can use multiple increments of this feature to increase the maximum number of supported virtual volumes from one million (default) to four million. Fifteen instances of FC 5270, Increased virtual volumes are required to support a new maximum of four million virtual volumes.

In a grid configuration, the maximum number of supported virtual volumes is determined by the cluster having the fewest installed instances of FC 5270, Increased virtual volumes. In order to increase the number of supported virtual volumes across a grid, the required number of FC 5270, Increased virtual volumes, must be installed on each cluster in the grid.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 5270, Increased virtual volumes in Table 67 on page 184 for requirements and other information.

FC 5271, Selective device access control

FC 5271, Selective device access control, authorizes the use of a set of Management Class policies that allow only certain logical control units or subsystem IDs within a composite library to have exclusive access to one or more volumes. Each instance of this feature enables definition of eight selective device access groups. The default group provides a single access group, resulting in nine total possible access groups. In a grid configuration, FC 5271, Selective device access control, must be installed on each cluster in the grid before any selective device access control policies can be defined in that grid.

In a grid configuration, FC 5271, Selective device access control, must be installed on each cluster in the grid before any selective device access control policies can be defined in that grid.

Note: This feature is withdrawn from use with a 3957-V06/VEA.

Refer to FC 5271, Selective device access control in Table 67 on page 184 for requirements and other information.

FC 5272, Enable disk encryption - Local Key Management

FC 5272, Enable disk encryption - Local Key Management, delivers a product license key to enable disk-based encryption using keys managed by the disk controller.

Refer to FC 5272, Enable disk encryption - Local Key Management in Table 67 on page 184 for requirements and other information.

FC 5273, TS7720/TS7760 Tape Attach enablement

FC 5273, TS7720/TS7760 Tape Attach enablement, enables the TS7720 or TS7760 to be connected to a TS3500 or TS4500 Tape Library with Machine Type 3952 tape drives dedicated to the TS7700.

Refer to FC 5273, TS7720/TS7760 Tape Attach enablement in Table 67 on page 184 for requirements and other information.

FC 5274, Enable 1 TB Pending Tape Capacity

Each instance of FC 5274, Enable 1 TB Pending Tape Capacity enables up to 1 TB of data to be pending migration to physical tape.

Refer to FC 5274, Enable 1 TB Pending Tape Capacity in Table 67 on page 184 for requirements and other information.

FC 5275, Additional virtual devices

Each instance of FC 5275, Additional virtual devices, enables up to 16 additional virtual devices (virtual tape drives).

Refer to FC 5275, Additional virtual devices in Table 67 on page 184 for requirements and other information.

FC 5276, Enable disk encryption - External Key Management

FC 5276, Enable disk encryption - External Key Management, delivers a product license key to enable disk-based encryption using keys managed by an external key manager.

Refer to FC 5276, Enable disk encryption - External Key Management in Table 67 on page 184 for requirements and other information.

FC 5277, External Disk Encryption Certificate - Field

FC 5277, External Disk Encryption Certificate - Field, delivers a DVD containing a PKCS #12 file containing the X.509 certificate required for communication with the external key manager.

Refer to FC 5277, External Disk Encryption Certificate - Field in Table 67 on page 184 for requirements and other information.

FC 5278, Enable Cloud Storage Tier

FC 5278, Enable Cloud Storage Tier, enables the TS7760 to store and retrieve objects from cloud-based storage.

Refer to FC 5278, Enable Cloud Storage Tier in Table 67 on page 184 for requirements and other information.

FC 5512, TS3000 System Console KVM display, keyboard, mouse

FC 5512, TS3000 System Console KVM display, keyboard, mouse, provides the KVM display, keyboard, mouse and mounting hardware.

Refer to FC 5512, TS3000 System Console KVM display, keyboard, mouse in Table 67 on page 184 for requirements and other information.

FC 5626, Plant installation of 3957-VEA

FC 5626, Plant installation of 3957-VEA, allows the factory installation of a TS7720 Server (3957-VEA) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9350, Plant Install against the 3957-VEA when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 5626, Plant installation of 3957-VEA in Table 67 on page 184 for requirements and other information.

FC 5627, Install 3957-VEB

FC 5627, Install 3957-VEB allows installation of a TS7720 Server in a 3952 F05 Tape Frame. This feature occurs on the 3952 F05 Tape Frame order.

You must also order FC 4743, Remove 3957-V06/VEA to remove the existing 3957-VEA as well as FC 9350, Plant Install or FC 9351, Field merge TS7700 Server in 3952 F05 against the TS7720 Server when ordering this feature.

Note: This feature was withdrawn on June 2016.

Refer to FC 5627, Install 3957-VEB in Table 67 on page 184 for requirements and other information.

FC 5628, Plant installation of 3957-V06

FC 5628, Plant installation of 3957-V06, allows plant installation of a TS7740 3957-V06 into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9350, Plant Install, against the TS7740 3957-V06 when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 5628, Plant installation of 3957-V06 in Table 67 on page 184 for requirements and other information.

FC 5629, Install 3957-V07

FC 5629, Install 3957-V07 allows installation of a TS7740 Server in a 3952 F05 Tape Frame. This feature occurs on the 3952 F05 Tape Frame order.

You must also order FC 4743, Remove 3957-V06/VEA to remove the existing 3957-V06, as well as FC 9350, Plant Install or FC 9351, Field merge TS7700 Server in 3952 F05 against the TS7740 Server when ordering this feature.

Note: This feature was withdrawn on June 2016.

Refer to FC 5629, Install 3957-V07 in Table 67 on page 184 for requirements and other information.

FC 5630, Install 3957-VEC

FC 5630, Install 3957-VEC, allows installation of a TS7700 Server in a 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9350, Plant Install against the TS7700 Server when ordering this feature.

Refer to FC 5630, Install 3957-VEC in Table 67 on page 184 for requirements and other information.

FC 5635, Plant installation of 3956-CS8

FC 5635, Plant installation of 3956-CS8, allows the factory installation of a TS7720 Cache Controller (3956-CS8) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install against the 3956-CS8 when ordering this feature.

Refer to FC 5635, Plant installation of 3956-CS8 in Table 67 on page 184 for requirements and other information.

FC 5636, Plant installation of 3956-CS7

FC 5636, Plant installation of 3956-CS7, allows the factory installation of a TS7720 Cache Controller (3956-CS7) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install against the 3956-CS7 when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 5636, Plant installation of 3956-CS7 in Table 67 on page 184 for requirements and other information.

FC 5638, Plant installation of 3956-CC6

FC 5638, Plant installation of 3956-CC6, allows factory installation of a TS7740 Cache Controller (3956-CC6) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install, against the 3956-CC6 when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 5638, Plant installation of 3956-CC6 in Table 67 on page 184 for requirements and other information.

FC 5639, Plant installation of 3956-CC7

FC 5639, Plant installation of 3956-CC7 allows factory installation of a TS7740 Cache Controller (3956-CC7) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install against the 3956-CC7 when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 5639, Plant installation of 3956-CC7 in Table 67 on page 184 for requirements and other information.

FC 5640, Plant installation of 3956-CC8

FC 5640, Plant installation of 3956-CC8, allows the factory installation of a TS7740 Cache Controller (3956-CC8) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install against the 3956-CC8 when ordering this feature.

Refer to FC 5640, Plant installation of 3956-CC8 in Table 67 on page 184 for requirements and other information.

FC 5641, Plant installation of 3956-CX7

FC 5641, Plant installation of 3956-CX7, allows the factory installation of a TS7740 Cache Drawer (3956-CX7) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9354, Plant Install against the 3956-CX7 when ordering this feature.

Refer to FC 5641, Plant installation of 3956-CX7 in Table 67 on page 184 for requirements and other information.

FC 5642, Field installation of 3956-CX7

FC 5642, Field installation of 3956-CX7, allows the field installation of a TS7740 Cache Drawer (3956-CX7) into an existing customer 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 7312, TS7740 Base frame against the 3952 Tape Frame and FC 9355, Field merge against the 3956-CX7 when ordering this feature.

Refer to FC 5642, Field installation of 3956-CX7 in Table 67 on page 184 for requirements and other information.

FC 5646, Plant installation of 3956-XS7

FC 5646, Plant installation of 3956-XS7, allows the factory installation of a TS7720 Cache Drawer (3956-XS7) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 7322, TS7720 Base frame or FC 7323, TS7720 Storage expansion frame against the 3952 Tape Frame and FC 9354, Plant Install against the 3956-XS7 when ordering this feature.

Refer to FC 5646, Plant installation of 3956-XS7 in Table 67 on page 184 for requirements and other information.

FC 5647, Field installation of 3956-XS7

FC 5647, Field installation of 3956-XS7, allows the field installation of a TS7720 Cache Drawer (3956-XS7) into an existing 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 7322, TS7720 Base frame or FC 7323, TS7720 Storage expansion frame against the 3952 Tape Frame and FC 9355, Field merge against the 3956-XS7 when ordering this feature.

Refer to FC 5647, Field installation of 3956-XS7 in Table 67 on page 184 for requirements and other information.

FC 5648, Plant installation of 3956-CX6

FC 5648, Plant installation of 3956-CX6, allows plant installation of a TS7740 Cache Drawer (3956-CX6) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9354, Plant Install, against the 3956-CX6 when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 5648, Plant installation of 3956-CX6 in Table 67 on page 184 for requirements and other information.

FC 5649, Field installation of 3956-CX6

FC 5649, Field installation of 3956-CX6, allows the field installation of a TS7740 Cache Drawer (3956-CX6) into an existing customer 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9355, Field merge against the 3956-CX6 when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 5649, Field installation of 3956-CX6 in Table 67 on page 184 for requirements and other information.

FC 5651, Plant installation of 3956-CS9

FC 5651, Plant installation of 3956-CS9, allows plant installation of a TS7720 Cache Controller (3956-CS9) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install, against the 3956-CS9 when ordering this feature.

Refer to FC 5651, Plant installation of 3956-CS9 in Table 67 on page 184 for requirements and other information.

FC 5652, Plant installation of 3956-CC9

FC 5652, Plant installation of 3956-CC9, allows plant installation of a TS7740 Cache Controller (3956-CC9) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install, against the 3956-CC9 when ordering this feature.

Note: This feature was withdrawn on June 2016.

Refer to FC 5652, Plant installation of 3956-CC9 in Table 67 on page 184 for requirements and other information.

FC 5653, Plant installation of 3956-CX9

FC 5653, Plant installation of 3956-CX9, allows plant installation of a TS7740 Cache Drawer (3956-CX9) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9354, Plant Install, against the 3956-CX9 when ordering this feature.

Refer to FC 5652, Plant installation of 3956-CC9 in Table 67 on page 184 for requirements and other information.

FC 5654, Field installation of 3956-CX9

FC 5654, Field installation of 3956-CX9, allows the field installation of a TS7740 Cache Drawer (3956-CX9) into an existing customer 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9355, Field merge against the3956-CX9 when ordering this feature.

Refer to FC 5654, Field installation of 3956-CX9 in Table 67 on page 184 for requirements and other information.

FC 5655, Plant installation of 3956-XS9

FC 5655, Plant installation of 3956-XS9, allows plant installation of a TS7720 Cache Drawer (3956-XS9) into a new 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9354, Plant Install against the 3956-XS9 when ordering this feature.

Refer to FC 5655, Plant installation of 3956-XS9 in Table 67 on page 184 for requirements and other information.

FC 5656, Field installation of 3956-XS9

FC 5656, Field installation of 3956-XS9, allows the field installation of a TS7720 Cache Drawer (3956-XS9) into an existing customer 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9355, Field merge against the 3956-XS9 when ordering this feature.

Refer to FC 5656, Field installation of 3956-XS9 in Table 67 on page 184 for requirements and other information.

FC 5657, Plant installation of 3956-CSA

FC 5657, Plant installation of 3956-CSA, allows the factory installation of a TS7700 Cache Controller (3956-CSA) into a new 3952 Tape Frame coming from the plant. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install, against the 3956-CSA when ordering this feature.

Refer to FC 5657, Plant installation of 3956-CSA in Table 67 on page 184 for requirements and other information.

FC 5658, Plant installation of 3956-XSA

FC 5658, Plant installation of 3956-XSA, allows the factory installation of a TS7700 Cache Drawer (3956-XSA) into a new 3952 Tape Frame coming from the plant. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9354, Plant Install against the 3956-XSA when ordering this feature.

Refer to FC 5658, Plant installation of 3956-XSA in Table 67 on page 184 for requirements and other information.

FC 5659, Field installation of 3956-XSA

FC 5659, Field installation of 3956-XSA, allows the field installation of a TS7700 Cache Drawer (3956-XSA) into an existing customer 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9355, Field merge against the 3956-XSA when ordering this feature.

Refer to FC 5659, Field installation of 3956-XSA in Table 67 on page 184 for requirements and other information.

FC 5660, Plant installation of 3956-CSA with 8 TB DDMs

FC 5660, Plant installation of 3956-CSA with 8 TB DDMs, allows the factory installation of a TS7700 Cache Controller (3956-CSA) containing 8 TB DDMs into a new 3952 Tape Frame coming from the plant. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9352, Plant Install and FC 7118, 96 TB SAS Storage against the 3956-CSA when ordering this feature.

Refer to FC 5660, Plant installation of 3956-CSA with 8 TB DDMs in Table 67 on page 184 for requirements and other information.

FC 5661, Plant installation of 3956-XSA with 8 TB DDMs

FC 5661, Plant installation of 3956-XSA with 8 TB DDMs, allows the factory installation of a TS7700 Cache Drawer (3956-XSA) containing 8 TB DDMs into a new 3952 Tape Frame coming from the plant. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9354, Plant Install and FC 7118, 96 TB SAS Storage against the 3956-XSA when ordering this feature.

Refer to FC 5661, Plant installation of 3956-XSA with 8 TB DDMs in Table 67 on page 184 for requirements and other information.

FC 5662, Field installation of 3956-XSA with 8 TB DDMs

FC 5662, Field installation of 3956-XSA with 8 TB DDMs, allows the field installation of a TS7700 Cache Drawer (3956-XSA) into an existing customer 3952 Tape Frame. This feature occurs on the 3952 Tape Frame order.

You must also order FC 9355, Field merge and FC 7118, 96 TB SAS Storage against the 3956-XSA when ordering this feature.

Refer to FC 5662, Field installation of 3956-XSA with 8 TB DDMs in Table 67 on page 184 for requirements and other information.

FC 5758, Integrated control path

FC 5758, Integrated control path, provides the Ethernet switches and cables to manage the network address translation between the Management Interface on the customer's network, and the internal TS7700 network.

Refer to FC 5758, Integrated control path in Table 67 on page 184 for requirements and other information.

FC 5759, Integrated control path

FC 5759, Integrated control path, provides the router cables necessary to create the control path between the TS7740 and the Library Manager.

Note: This feature is withdrawn from use with a 3957-V06/VEA. It is still available for use with a 3957-V07/VEB.

Refer to FC 5759, Integrated control path in Table 67 on page 184 for requirements and other information.

FC 6000, Intraframe fibre cable to 3956-CC6

FC 6000, Intraframe fibre cable to 3956-CC6, provides one 1m fibre cable and is also used to connect TS7740 Cache Drawers.

Note: This feature has been withdrawn.

Refer to FC 6000, Intraframe fibre cable to 3956-CC6 in Table 67 on page 184 for requirements and other information.

FC 6003, Intraframe fibre cable to 3957-V06

FC 6003, Intraframe fibre cable to 3957-V06, provides one 2m fibre cable.

Note: This feature has been withdrawn.

Refer to FC 6003, Intraframe fibre cable to 3957-V06 in Table 67 on page 184 for requirements and other information.

FC 7113, 16 TB SATA storage

FC 7113, 16 TB SATA storage, installs a complete set of 16 1000 GB, 7,200rpm, SATA disk drive modules in a TS7720 Cache Controller (3956-CS7) or TS7720 Cache Drawer (3956-XS7), providing 16 TB of unformatted disk storage capacity. Usable capacity is 10 TB with RAID 6 formatting.

Note: This feature has been withdrawn.

Refer to FC 7113, 16 TB SATA storage in Table 67 on page 184 for requirements and other information.

FC 7114, 32 TB SATA storage

FC 7114, 32 TB SATA storage, installs a complete set of 16 2000 GB, 7200 rpm, SATA disk drive modules in the TS7720 Cache Controller (3956-CS8), providing 32 TB of unformatted disk storage capacity.

Note: Usable capacity is approximately 22 TB when used with RAID 6 formatting.

Refer to FC 7114, 32 TB SATA storage in Table 67 on page 184 for requirements and other information.

FC 7115, 36 TB SAS storage

FC 7115, 36 TB SAS storage, installs a complete set of 12 encryption-capable, 3 TB, 7200 rpm, SAS disk drive modules in the TS7720 Cache Controller (3956-CS9), providing 36 TB of unformatted disk storage capacity.

Note: Usable capacity is approximately 24 TB when used with RAID 6 formatting.

Refer to FC 7115, 36 TB SAS storage in Table 67 on page 184 for requirements and other information.

FC 7116, 33 TB SAS storage

FC 7116, 33 TB SAS storage, installs a complete set of 11 encryption-capable, 3 TB, 7200 rpm, SATA disk drive modules in the TS7720 Cache Drawer (3956-XS9), providing 33 TB of unformatted disk storage capacity.

Note: Usable capacity is approximately 24 TB when used with RAID 6 formatting.

Refer to FC 7116, 33 TB SAS storage in Table 67 on page 184 for requirements and other information.

FC 7117, 48 TB SAS Storage

FC 7117, 48 TB SAS Storage, installs a complete set of 12 encryption-capable, 4 TB, 7200 rpm, SAS disk drive modules, providing 48 TB of unformatted disk storage capacity.

Note: Approximately 31.43 TB useable capacity with dynamic disk pooling.

Refer to FC 7117, 48 TB SAS Storage in Table 67 on page 184 for requirements and other information.

FC 7118, 96 TB SAS Storage

FC 7118, 96 TB SAS Storage, installs a complete set of 12 FIPS 140-2 capable, self encrypting, 8 TB, 7,200 rpm, SAS HDDs providing 96 TB unformatted disk storage capacity.

Note: Approximately 62.21 TB useable capacity with dynamic disk pooling.

Refer to FC 7118, 96 TB SAS Storage in Table 67 on page 184 for requirements and other information.

FC 7120, 1.7 TB fibre storage

FC 7120, 1.7 TB fibre storage, installs a complete set of 16 fibre channel-capable disk drive modules in the TS7740 Cache Controller (3956-CC6) or, TS7740 Cache Drawer (3956-CX6) providing 1.7 TB of usable storage capacity.

Note: This feature has been withdrawn.

Refer to FC 7120, 1.7 TB fibre storage in Table 67 on page 184 for requirements and other information.

FC 7121, 3.43 TB fibre storage

FC 7121, 3.43 TB fibre storage, installs a complete set of 16 300 GB, 15k rpm, fibre channel-capable disk drive modules in the TS7740 Cache Controller (3956-CC7) or TS7740 Cache Drawer (3956-CX7), providing 3.43 TB of usable storage capacity.

Note: This feature has been withdrawn.

Refer to FC 7121, 3.43 TB fibre storage in Table 67 on page 184 for requirements and other information.

FC 7123, 9.6 TB Fibre storage

FC 7123, 9.6 TB Fibre storage, installs a complete set of 16 600 GB, 15k rpm, fibre channel-capable disk drive modules in the TS7740 Cache Controller (3956-CC8), providing 9 TB of unformatted storage capacity.

Note: Usable capacity is 6.86 TB when used with RAID 5 formatting.

Refer to FC 7123, 9.6 TB Fibre storage in Table 67 on page 184 for requirements and other information.

FC 7124, 13.2 TB SAS storage

FC 7124, 13.2 TB SAS storage, installs a complete set of 22 600 GB, 10k rpm, SAS disk drive modules in the TS7740 Cache Controller (3956-CC9), providing 13.2 TB of unformatted storage capacity. Usable capacity is 9.3 TB when used with RAID 6 formatting.

Note: This feature was withdrawn on June 2016.

Refer to FC 7124, 13.2 TB SAS storage in Table 67 on page 184 for requirements and other information.

FC 7312, TS7740 Base frame

FC 7312, TS7740 Base frame, identifies this 3952 Tape Frame as the base unit for the TS7740.

Refer to FC 7312, TS7740 Base frame in Table 67 on page 184 for requirements and other information.

FC 7322, TS7720 Base frame

FC 7322, TS7720 Base frame identifies a 3952 Tape Frame as the base unit for a TS7720.

Refer to FC 7322, TS7720 Base frame in Table 67 on page 184 for requirements and other information.

FC 7323, TS7720 Storage expansion frame

FC 7323, TS7720 Storage expansion frame, identifies a 3952 Tape Frame as the disk storage expansion unit for a TS7720.

Refer to FC 7323, TS7720 Storage expansion frame in Table 67 on page 184 for requirements and other information.

FC 7330, TS7740 Encryption-capable base frame

FC 7330, TS7740 Encryption-capable base frame, identifies a 3952 Tape Frame as an encryption-capable base unit for a TS7740.

Note: This feature was withdrawn on June 2016.

Refer to FC 7330, TS7740 Encryption-capable base frame in Table 67 on page 184 for requirements and other information.

FC 7331, TS7720 Encryption-capable base frame

FC 7331, TS7720 Encryption-capable base frame, identifies a 3952 Tape Frame as an encryption-capable base unit for a TS7720.

Note: This feature was withdrawn on June 2016.

Refer to FC 7331, TS7720 Encryption-capable base frame in Table 67 on page 184 for requirements and other information.

FC 7332, TS7720 Encryption-capable expansion frame

FC 7332, TS7720 Encryption-capable expansion frame, identifies a 3952 Tape Frame as an encryption-capable disk storage expansion unit for a TS7720. You can attach one expansion frame (FC 7332) to a base frame using FC 7331. You can attach one expansion frame (FC 7332) to a base frame using FC 7322, provided no other expansion frames (FC 7323) are attached.

Refer to FC 7332, TS7720 Encryption-capable expansion frame in Table 67 on page 184 for requirements and other information.

FC 7333, TS7700 Encryption-capable base frame

FC 7333, TS7700 Encryption-capable base frame, identifies a 3952 Tape Frame as an encryption-capable base unit for a TS7700.

Refer to FC 7333, TS7700 Encryption-capable base frame in Table 67 on page 184 for requirements and other information.

FC 7334, TS7700 Encryption-capable expansion frame

FC 7334, TS7700 Encryption-capable expansion frame, identifies a 3952 Tape Frame as an encryption-capable disk storage expansion unit for a TS7700. You can attach up to two expansion frames (FC 7334) to a base frame (FC 7331) when no TS7720 Encryption Capable Expansion Frames (FC 7332) are attached. You can attach one expansion frame (FC 7334) to a TS7720 Encryption Capable Base Frame (FC 7331) when one TS7720 Encryption Capable Expansion Frame (FC 7332) is already attached. You can attach up to two expansion frames (FC 7334) to the TS7700 Encryption Capable Base Frame (FC 7333).

Refer to FC 7334, TS7700 Encryption-capable expansion frame in Table 67 on page 184 for requirements and other information.

FC 7403, Enable first expansion drawer

FC 7403, Enable first expansion drawer, is required on a TS7740 Cache Controller (3956-CC7) to allow attachment of the first TS7740 Cache Drawer (3956-CX7) in its storage string. If no cache drawers are attached to the cache controller, this feature is not required.

Note: This feature was withdrawn on June 2016.

Refer to FC 7403, Enable first expansion drawer in Table 67 on page 184 for requirements and other information.

FC 7404, Encryption

FC 7404, Encryption, enables the use of disk-based encryption on this device.

Refer to FC 7404, Encryption in Table 67 on page 184 for requirements and other information.

FC 9000, Mainframe attachment

FC 9000, Mainframe attachment, is a specify feature that indicates attachment to one of the following host platforms:

- z/OS
- z/VM
- z/VSE
- zTPF
- TPF

Restriction: Refer to “Supported hosts” on page 81 for supported operating system versions.

Note: This feature is withdrawn from use with a 3957-V06/VEA, and effective June 2016 is withdrawn from use with a 3957-V07/VEB. It is still available for use with a 3957-VEC.

Refer to FC 9000, Mainframe attachment in Table 67 on page 184 for requirements and other information.

FC 9013, Attach to TS7700

FC 9013, Attach to TS7700, is a specify feature that indicates attachment to a TS7700. This feature cannot be used with TS7740 servers operating at microcode level 8.5.0.x or later.

Refer to FC 9013, Attach to TS7700 in Table 67 on page 184 for requirements and other information.

Note: This feature has been withdrawn.

FC 9110, Ship with R1.7 machine code

FC 9110, Ship with R1.7 machine code, instructs factory installation of the latest manufacturing level of R1.7 machine code on the TS7700. This feature is supported only on the 3957-V06 or 3957-VEA.

Note: This feature has been withdrawn.

Refer to FC 9110, Ship with R1.7 machine code in Table 67 on page 184 for requirements and other information.

FC 9111, Ship with R2.0 machine code

FC 9111, Ship with R2.0 machine code, instructs factory installation of the latest manufacturing level of R2.0 machine code on the TS7700.

Note: This feature has been withdrawn.

Refer to FC 9111, Ship with R2.0 machine code in Table 67 on page 184 for requirements and other information.

FC 9112, Ship with R2.1 machine code

FC 9112, Ship with R2.1 machine code, instructs factory installation of the latest manufacturing level of R2.1 machine code on the TS7700.

Note: This feature has been withdrawn.

Refer to FC 9112, Ship with R2.1 machine code in Table 67 on page 184 for requirements and other information.

FC 9113, Ship with R3.0 machine code

FC 9113, Ship with R3.0 machine code, instructs factory installation of the latest manufacturing level of R3.0 machine code on the TS7700.

Note: This feature has been withdrawn.

Refer to FC 9113, Ship with R3.0 machine code in Table 67 on page 184 for requirements and other information.

FC 9114, Ship with R3.1 machine code

FC 9114, Ship with R3.1 machine code, instructs factory installation of the latest manufacturing level of R3.1 machine code on the TS7700.

Note: This feature has been withdrawn.

Refer to FC 9114, Ship with R3.1 machine code in Table 67 on page 184 for requirements and other information.

FC 9115, Ship with R3.2 Machine Code

FC 9115, Ship with R3.2 Machine Code, instructs factory installation of the latest manufacturing level of R3.2 machine code on the TS7700.

Note: This feature has been withdrawn.

Refer to FC 9115, Ship with R3.2 Machine Code in Table 67 on page 184 for requirements and other information.

FC 9116, Ship with R3.3 Machine Code

FC 9116, Ship with R3.3 Machine Code, instructs factory installation of the latest manufacturing level of R3.3 machine code on the TS7700.

Note: This feature was withdrawn on June 2016.

Refer to FC 9116, Ship with R3.3 Machine Code in Table 67 on page 184 for requirements and other information.

FC 9217, Attach to 3953 LM

FC 9217, Attach to 3953 LM, is a specify feature that indicates that the TS7740 Server (3957-V06) attaches to a 3953 L05 Library Manager. This feature cannot be used with TS7740 servers operating at microcode code level 8.5.0.x or later.

Refer to FC 9217, Attach to 3953 LM in Table 67 on page 184 for requirements and other information.

Note: This feature has been withdrawn.

FC 9218, Attach to 3494 LM

FC 9218, Attach to 3494 LM, is a specify feature that indicates that the TS7740 Server (3957-V06) attaches to a Library Manager in a 3494 Tape Library. Attachment to a 3494 Tape Library is not supported by microcode levels of 8.20.0.xx or later. This feature must be removed before installing a microcode level or 8.20.0.xx or later.

Note: This feature is withdrawn from use with a 3957-V06/VEA. It is still available for use with a 3957-V07/VEB.

Refer to FC 9218, Attach to 3494 LM in Table 67 on page 184 for requirements and other information.

FC 9219, Attach to TS3500/TS4500

FC 9219, Attach to TS3500/TS4500 enables the TS7700 Server to attach directly to the TS3500 or TS4500 Tape Library.

Note: 16-Gb Fibre Channel features are required in the 3584 Tape Library frames containing the backend drives.

Note: This feature is withdrawn from use with a 3957-V06/VEA, and effective June 2016 is withdrawn from use with a 3957-V07.

Refer to FC 9219, Attach to TS3500/TS4500 in Table 67 on page 184 for requirements and other information.

FC 9230, Attach to 3957-V06

FC 9230, Attach to 3957-V06, is a specify feature that indicates a TS7740 Cache Controller (3956-CC6) is attached to a TS7740 Server (3957-V06). This feature occurs on the 3956-CC6 order.

You must also order FC 9352, Plant Install, against the IBM TS7700 and FC 5638, Plant installation of 3956-CC6, against the 3952 Tape Frame when ordering this feature.

Note: This feature has been withdrawn.

Refer to FC 9230, Attach to 3957-V06 in Table 67 on page 184 for requirements and other information.

FC 9268, Plant installation of 100 MB/s throughput

FC 9268, Plant installation of 100 MB/s throughput, delivers a key to enable the first 100-MB/sec increment of potential peak data throughput on the TS7720 Server (3957-VEA or 3957-VEB) or the TS7760 Server (3957-VEC). Enabling a data throughput increment does not guarantee that the overall TS7700 performs at that data throughput level. However, installation of the maximum allowed number of features results in unrestricted peak data throughput capabilities. This feature is restricted to new factory installation and represents the first 100-MB/s increment.

Note: This feature is withdrawn from use with a 3957-V06/VEA. It is still available for use with a 3957-V07/VEB.

Refer to FC 9268, Plant installation of 100 MB/s throughput in Table 67 on page 184 for requirements and other information.

FC 9277, External Disk Encryption Certificate - Plant

FC 9277, External Disk Encryption Certificate - Plant, instructs Manufacturing to install a PKCS #12 file containing the X.509 certificate required for communication with the external key manager.

Refer to FC 9277, External Disk Encryption Certificate - Plant in Table 67 on page 184 for requirements and other information.

FC 9323 Expansion frame attachment

FC 9323 Expansion frame attachment indicates that a 3952 Tape Frame (base frame) used with a TS7720 or TS7760 is attached to a 3952 Storage Expansion Frame.

Refer to FC 9323 Expansion frame attachment in Table 67 on page 184 for requirements and other information.

FC 9339, Replacing TS7740 System

FC 9339, Replacing TS7740 System, instructs Manufacturing to ship the installation instructions to replace an existing TS7740 system with this new TS7700 system.

Refer to FC 9339, Replacing TS7740 System in Table 67 on page 184 for requirements and other information.

FC 9350, Plant Install

FC 9350, Plant Install, allows the plant installation of a TS7700 Server (3957-VEC) into a new 3952 Tape Frame. This feature occurs on the TS7700 Server order.

You must also order FC 5630, Install 3957-VEC, against the 3952 Tape Frame when ordering this feature for the 3957-VEC.

Note: This feature is withdrawn from use with a 3957-V06/VEA, and effective June 2016 is withdrawn from use with a 3957-V07/VEB. It is still available for use with a 3957-VEC.

Refer to FC 9350, Plant Install in Table 67 on page 184 for requirements and other information.

FC 9351, Field merge TS7700 Server in 3952 F05

FC 9351, Field merge TS7700 Server in 3952 F05, allows the field merge of a TS7700 Server into an existing installed 3952 Tape Frame.

You must also order FC 4743, Remove 3957-V06/VEA, against the 3952 Tape Frame. when ordering this feature.

Note: This feature is withdrawn from use with a 3957-V07/VEB effective June 2016. It is still available for use with a 3957-VEC.

Refer to FC 9351, Field merge TS7700 Server in 3952 F05 in Table 67 on page 184 for requirements and other information.

FC 9352, Plant Install

FC 9352, Plant Install, allows the factory installation of a TS7700 Cache Controller into a new 3952 Tape Frame coming from the plant.

If installing a 3956-CS9, you must also order FC 5651, Plant installation of 3956-CS9 against the 3952 Tape Frame.

If installing a 3956-CSA, you must also order FC 5657, Plant installation of 3956-CSA or FC 5660, Plant installation of 3956-CSA with 8 TB DDMs against the 3952 Tape Frame.

Note: This feature has been withdrawn for the 3956-CC6, 3956-CC7, 3956-CC8, 3956-CC8, and 3956-CS8.

Refer to FC 9352, Plant Install in Table 67 on page 184 for requirements and other information.

FC 9353, Field merge in 3952 F05

FC 9353, Field merge in 3952 F05, allows the field merge of a TS7720 Cache Controller into a customer installed 3952 Tape Frame.

This feature must be installed on the TS7720 Cache Controller and FC 5637 must be ordered against the 3952 Tape Frame.

Refer to FC 9353, Field merge in 3952 F05 in Table 67 on page 184 for requirements and other information.

FC 9354, Plant Install

FC 9354, Plant Install, allows the factory installation of a TS7700 Cache Drawer into a new 3952 Tape Frame coming from the plant.

If installing a 3956-CX9, you must also order FC 5653, Plant installation of 3956-CX9 against the 3952 Tape Frame.

If installing a 3956-XS9, you must also order FC 5655, Plant installation of 3956-XS9 against the 3952 Tape Frame.

If installing a 3956-XSA, you must also order FC 5658, Plant installation of 3956-XSA or FC 5661, Plant installation of 3956-XSA with 8 TB DDMs against the 3952 Tape Frame.

Note: This feature has been withdrawn for the 3956-CX6, 3956-CX7, and 3956-XS7.

Refer to FC 9354, Plant Install in Table 67 on page 184 for requirements and other information.

FC 9355, Field merge

FC 9355, Field merge, is a specify code that allows the field merge of a TS7700 Cache Drawer into a previously installed 3952 Tape Frame.

If installing a 3956-CX7, you must also order FC 5642, Field installation of 3956-CX7 against the 3952 Tape Frame.

If installing a 3956-XS7, you must also order FC 5647, Field installation of 3956-XS7 against the 3952 Tape Frame.

If installing a 3956-XSA, you must also order FC 5659, Field installation of 3956-XSA or FC 5662, Field installation of 3956-XSA with 8 TB DDMs against the 3952 Tape Frame model F06.

Refer to FC 9355, Field merge in Table 67 on page 184 for requirements and other information.

FC 9461, 8 GB Memory upgrade, plant

FC 9461, 8 GB Memory upgrade, plant, allows the factory installation of 16 GB RAM in the TS7700 Server. This feature is supported only on the 3957-V06 or 3957-VEA.

Note: This feature is withdrawn from use with a 3957-V06/VEA. It is still available for use with a 3957-V07/VEB.

Refer to FC 9461, 8 GB Memory upgrade, plant in Table 67 on page 184 for requirements and other information.

FC 9700, No factory cables

FC 9700, No factory cables, instructs the plant not to ship any FICON cables with the TS7700 Server .

Note: This feature is withdrawn from use with a 3957-V06/VEA, and effective June 2016 is withdrawn from use with a 3957-V07/VEB. It is still available for use with a 3957-VEC.

Refer to 9700FC 9700, No factory cables in Table 67 on page 184 for requirements and other information.

FC 9900, Tape Encryption configuration

Order FC 9900, Tape Encryption configuration when encryption will be used in a 3494 Tape Library, TS3500/TS4500 Tape Library or TS7700 Cluster. It includes publication updates with information on enabling and configuring the library (virtual or real) to support encryption. This feature also provides an encryption key server publication. Customer initiated procedures need to be completed for enabling and configuring the 3494 Tape Library, TS3500/TS4500 Tape Library or TS7700 Cluster to support encryption with the TS11xx encryption capable tape drive.

FC 9900, Tape Encryption configuration is supported only with encryption-capable TS1150/TS1140/TS1130/TS1120 Tape Drives. FC 9900, Tape Encryption configuration, is not supported by 3592 J1A or 3590 Tape Drives.

Note: This feature is withdrawn from use with a 3957-V06.

Refer to FC 9900, Tape Encryption configuration in Table 67 on page 184 for requirements and other information.

FC 9954, NEMA L6-30 power cord

FC 9954, NEMA L6-30 power cord, provides a National Electrical Manufacturers Association (NEMA) L6-30 non-watertight, 4.3-m (14-ft.) power cord, rated for 200 V ac to 208 V ac or 240 V ac and 24 A. This power cord is suggested for use in the USA, Canada, Latin America, and Japan. This feature occurs on the 3952 Tape Frame order.

Refer to FC 9954, NEMA L6-30 power cord in Table 67 on page 184 for requirements and other information.

FC 9955, RS 9750 DP power cord

FC 9955, RS 9750 DP power cord, provides a Russellstoll 3750 DP, watertight, 4.3-m (14-ft.) power cord, rated for 200 V ac to 208 V ac or 240 V ac and 24 A. This power cord is suggested for use in the USA (highly recommended in Chicago, Illinois, to conform with local requirements), Canada, Latin America, and Japan. This feature occurs on the 3592 Tape Frame order.

Refer to FC 9955, RS 9750 DP power cord in Table 67 on page 184 for requirements and other information.

FC 9956, IEC 309 power cord

FC 9956, IEC 309 power cord, provides an International Electrotechnical Commission (IEC) 309 p+n+g, 32 A plug, 4.3-m (14-ft.) power cord, rated for 230 V ac and can safely carry 24 A in all countries. This power cord is suggested for use in Europe, the Middle East, and Africa. This feature occurs on the 3952 Tape Frame order.

Refer to FC 9956, IEC 309 power cord in Table 67 on page 184 for requirements and other information.

FC 9957, PDL 4.3 power cord

FC 9957, PDL 4.3 power cord, provides a PDL 4.3-m (14-ft.) power cord, rated for 230 V ac to 240 V ac and 24 A. This power cord is suggested for use in Australia and New Zealand. This feature occurs on the 3952 Tape Frame order.

Refer to FC 9957, PDL 4.3 power cord in Table 67 on page 184 for requirements and other information.

FC 9958, Korean 4.3-m power cord

FC 9958, Korean 4.3-m power cord, provides a NEMA L6-30 non-watertight, 4.3-m (14-ft.) power cord, rated for 200 V ac to 208 V ac or 240 V ac and 24 A, with a Korean plug. This power cord is suggested for use in North and South Korea. This feature occurs on the 3952 Tape Frame order.

Refer to FC 9958, Korean 4.3-m power cord in Table 67 on page 184 for requirements and other information.

FC 9959, Unterminated power cord

FC 9959, Unterminated power cord, provides an unterminated, non-watertight, 4.3-m (14-ft.) power cord, rated for 200 V ac to 208 V ac, or 240 V ac and 24 Amp, with IRAM and BSMI agency certifications. This is the recommended cord for Argentina and Taiwan. This feature occurs on the 3952 Tape Frame order.

Refer to FC 9959, Unterminated power cord in Table 67 on page 184 for requirements and other information.

FC 9966, Unterminated power cord (China)

FC 9966, Unterminated power cord (China), provides an unterminated, non-watertight, 4.3-m (14-ft.) power cord, rated for 200 V ac to 208 V ac, or 240 Vac and 24 Amp, with CCC agency certifications. This is the recommended cord for China. This feature occurs on the 3952 Tape Frame order.

Refer to FC 9966, Unterminated power cord (China) in Table 67 on page 184 for requirements and other information.

FC AG00, Shipping and Handling - No charge

FC AG00, Shipping and Handling - No charge, indicates Model F05 will have no shipping and handling charge added to the order.

Refer to FC AG00, Shipping and Handling - No charge in Table 67 on page 184 for requirements and other information.

FC AGGA, Shipping and Handling - F06

FC AGGA, Shipping and Handling - F06, indicates each 3952 Tape Frame on the order will have a shipping and handling charge added to the order.

Refer to FC AGGA, Shipping and Handling - F06 in Table 67 on page 184 for requirements and other information.

FC AGK0, Ship with R4.0 Machine Code

FC AGK0, Ship with R4.0 Machine Code, instructs factory installation of the latest manufacturing level of R4.0 machine code on the TS7700.

Note: The machine code levels on the 3957-VEC server and the 3952 F06 frames must be the same.

Refer to FC AGK0, Ship with R4.0 Machine Code in Table 67 on page 184 for requirements and other information.

FC AGKE, Ship with R4.1 Machine Code

FC AGKE, Ship with R4.1 Machine Code, instructs factory installation of the latest manufacturing level of R4.1.1 machine code on the TS7700.

Note: The machine code levels on the 3957-VEC server and the 3952 F06 frames must be the same.

Refer to FC AGKE, Ship with R4.1 Machine Code in Table 67 on page 184 for requirements and other information.

FC AGKR, Ship with R4.1.2 Machine Code

FC AGKR, Ship with R4.1.2 Machine Code, instructs factory installation of the latest manufacturing level of R4.1 Phase 2 machine code on the TS7700.

Refer to FC AGKR, Ship with R4.1.2 Machine Code in Table 67 on page 184 for requirements and other information.

Table 67. TS7700 features

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 0201, 9-micron LC/LC 31-meter	2	8	Prerequisite: You must order **EITHER**: • One instance of FC 9700 **OR** • When FC 3401 is installed, two instances of FC 0201 or FC 0203 for each: – FC 3402 – FC 3403 – FC 3438 – FC 3439 **OR** • When FC 3401 is installed, one instance of FC 0201 or FC 0203 for each: – FC 3402 – FC 3403 – FC 3438 – FC 3439 – FC 3441 – FC 3442 – FC 3443	Plant or field	Yes
FC 0202, 9-micron LC/SC 31-meter†	2	4	You must order **EITHER** two instances of one of the following: • FC 0201 • FC 0202 • FC 0203 • FC 0204 • FC 0205 • FC 0206 **OR**, one instance of FC 9700	Plant or field	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 0203, 50-micron LC/LC 31-meter	2	8	Prerequisite: You must order **EITHER**: • One instance of FC 9700 **OR** • When FC 3401 is installed, two instances of FC 0201 or FC 0203 for each: – FC 3402 – FC 3403 – FC 3438 – FC 3439 **OR** • When FC 3401 is installed, one instance of FC 0201 or FC 0203 for each: – FC 3402 – FC 3403 – FC 3438 – FC 3439 – FC 3441 – FC 3442 – FC 3443	Plant or field	Yes
FC 0204, 50-micron LC/SC 31-meter†	2	4	You must order **EITHER** two instances of one of the following: • FC 0201 • FC 0202 • FC 0203 • FC 0204 • FC 0205 • FC 0206 **OR**, one instance of FC 9700	Plant or field	Yes
FC 0205, 62.5-micron LC/LC 31-meter†	2	4	You must order **EITHER** two instances of one of the following: • FC 0201 • FC 0202 • FC 0203 • FC 0204 • FC 0205 • FC 0206 **OR**, one instance of FC 9700	Plant or field	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 0206, 62.5-micron LC/SC 31-meter†	2	4	You must order **EITHER** two instances of one of the following: • FC 0201 • FC 0202 • FC 0203 • FC 0204 • FC 0205 • FC 0206 **OR**, one instance of FC 9700	Plant or field	Yes
FC 0521, Functional enhancement field	0	No Maximum	This feature is a one-time code update. It includes the minimum level of library manager microcode required to support the current level of TS7700 microcode.	Field only	No
FC 0983, TAA Compliance	0	1	None	Plant only	No
FC 1030, 1Gb grid copper connection†	0	2	This feature is available as a concurrent MES. This feature is mutually exclusive with FC 1031. You must order two of **EITHER** FC 1030 **OR** FC 1031.	Plant or field	Yes
FC 1031, 1Gb optical SW connection†	0	2	This feature is available as a concurrent MES. This feature is mutually exclusive with FC 1030. You must order two of **EITHER** FC 1031 **OR** FC 1030.	Plant or field	Yes
FC 1032, 1 Gb grid dual port copper connection	0	2	This feature is mutually exclusive with: • FC 1030 • FC 1031 • FC 1033 You must order two instances of one of the following: • FC 1030 • FC 1031 • FC 1032 • FC 1033	Plant or field	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 1033, 1 Gb grid dual port optical SW connection	0	2	This feature is mutually exclusive with: • FC 1030 • FC 1031 • FC 1032 You must order two instances of one of the following: • FC 1030 • FC 1031 • FC 1032 • FC 1033	Plant or field	Yes
FC 1034, Enable dual port grid connection	0	1	Prerequisites: Two instances of one of the following on the 3957-V06/VEA: • FC 1032 • FC 1033 on the 3957-V07/VEB: • FC 1036 • FC 1037 or on the 3957-VEC: • FC 1036 • FC 1037 • FC 1038	Plant or field	No
FC 1035, 10 Gb grid optical LW connection	0	2	Mutually exclusive with: • FC 1036 • FC 1037 You must order two instances of one of the following: • FC 1035 • FC 1036 • FC 1037	Plant or field	Yes
FC 1036, 1 Gb grid dual port copper connection	0	2	Mutually exclusive with: • FC 1037 • FC 1038 You must order two instances of one of the following: • FC 1036 • FC 1037 • FC 1038	Plant or field	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 1037, 1 Gb dual port optical SW connection	0	2	Mutually exclusive with: • FC 1036 • FC 1038 You must order two instances of one of the following: • FC 1036 • FC 1037 • FC 1038	Plant or field	Yes
FC 1038, 10 Gb dual port optical LW connection	0	2	Mutually exclusive with: • FC 1036 • FC 1037 You must order two instances of one of the following: • FC 1036 • FC 1037 • FC 1038	Plant or field	Yes
FC 1903, Power Distribution Unit	1	1	This feature is required if you are ordering FC 7312, FC 7322, FC 7330, FC 7331, FC 7333, or FC 7334.	Plant only	No
FC 1904, Switching PDU	0	1	Prerequisite: FC 1903 Required when FC 2725 is installed.	Plant or field	No
FC 2704, TS3000 System Console expansion 26-port Ethernet switch/ rackmount	0	1	Prerequisites: • FC 4641 • One instance of FC 2704, FC 2714, FC 2715, FC 2724, FC 2725, or FC 2732 Corequisite: FC 7330 when ordered against the 3952 F05.	Plant or field	Yes
FC 2714, Console expansion†	0	1	Mutually exclusive with FC 2715. You must order one instance of either FC 2714 or FC 2715. Prerequisites: This feature must attach to one of the following: • FC 2720 • FC 2721 • FC 2722 • FC 2730 • FC 2732 • FC 2718 (obsolete) Attachment to FC 2713 is not allowed.	Plant or field	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 2715, Console attachment	0	1	Mutually exclusive with FC 2714. You must order one instance of either FC 2714 or FC 2715. Prerequisites: This feature must attach to one of the following: • FC 2714 • FC 2720 • FC 2721 • FC 2722 • FC 2730 • FC 2732 • FC 2718 (obsolete) Attachment to FC 2713 is not allowed.	Plant or field	Yes
FC 2719, Console upgrade†	0	1	When FC 2714/FC 2715 are installed on a 3957-V06, this feature and FC 2718, FC 2720, or FC 2721 must be installed on the same machine type model.Support for this feature on the 3957-V06 was withdrawn on December 5, 2008. To use this feature, order it against the 3953 F05 Tape Frame.	Field	No
FC 2720, TS3000 System Console	0	1	You must order one of FC 2714, FC 2715, or FC 2720. Support for this feature on the 3957-V06 was withdrawn on December 5, 2008. To use this feature, order it against the 3953 F05 Tape Frame.	Plant only	No
FC 2721, Rack mountable TS3000 System Console	0	1	You can install the TS3000 System Console FC 2721 on the 3953 F05 Tape Frame connecting to the TS7740 using FC 2714 or FC 2715.	Plant or field	Yes
FC 2725, Rackmount TS3000 System Console	0	1	Prerequisites: • FC 7333 Corequisites: • FC 1904 • FC 2704 • FC 2748 • FC 5512	Plant or field	Yes
FC 2730, TS3000 System Console†	0	1	Prerequisites: • FC 1904 • FC 2719 You must order one instance of one of the following: • FC 7312 • FC 7313 • FC 7322	Plant or field	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 2734, TS3000 System Console USB modem	0	1	Prerequisite: FC 2724 Corequisite: FC 7330 when ordered against the 3952 F05. **Note:** This feature has been withdrawn.	Plant or field	Yes
FC 2748, Optical drive	0	1	Corequisite: FC 2725	Plant or field	Yes
FC 3401, Enable FICON dual port	0	1	Prerequisites: • FC 3403, FC 3404, FC 3438 or FC 3439 • One instance of FC 9700 OR **EITHER** two instances of FC 0201 for each instance of FC 3404 or FC 3439 installed **OR** two instances of FC 0203 for each instance of FC 3403 or FC 3438 installed **Note:** Unless No Factory Cables (FC 9700) has been selected, two cables are required for each active FICON port. When installing FC 3401, include two FC 0201 cables for each FC 3404 or FC 3439 FICON card configured, and two FC 0203 for each FC 3403 or FC 3438 FICON card configured.	Plant only	No
FC 3402, 16 Gb FICON Short Wavelength Attachment	2	4	Corequisites: • Total quantities of FC 3402 are 0, 2, or 4 • Two of FC 3402, FC 3403, FC 3438 or FC 3439 are required • The maximum quantity of FC 3402, FC 3403, FC 3438 plus FC 3439 is 4	Plant or field	Yes
FC 3403, 16 Gb FICON Long Wavelength Attachment	2	4	Corequisites: • Total quantities of FC 3403 are 0, 2 or 4 • Two of FC 3402, FC 3403, FC 3438 or FC 3439 are required • The maximum quantity of FC 3402, FC 3403, FC 3438 plus FC 3439 is 4	Plant or field	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 3438, 8 Gb FICON Short Wavelength Attachment	0	4	Corequisite: • FC 3462 • Total quantities of 0, 2, or 4 of FC 3438 and FC 3439 You must order at least two instances of any of the following features: • FC 3441 • FC 3442 • FC 3443 • FC 3438 • FC 3439 Mutually exclusive with FC 3441, FC 3442, and FC 3443	Plant or field	Yes
FC 3439, 8 Gb FICON Long Wavelength Attachment	0	4	Corequisite: • FC 3462 • Total quantities of 0, 2, or 4 of FC 3438 and FC 3439 You must order at least two instances of any of the following features: • FC 3441 • FC 3442 • FC 3443 • FC 3438 • FC 3439 Mutually exclusive with FC 3441, FC 3442, and FC 3443	Plant or field	Yes
FC 3441, FICON short-wavelength attachment	0	4	This feature is available as a concurrent MES. You must order this feature in quantities of zero, two, or four. The total quantity of all the following features must be 2 or 4: • FC 3441 • FC 3442 • FC 3443	Plant or field	Yes
FC 3442, FICON long-wavelength attachment	0	4	This feature is available as a concurrent MES. You must order this feature in quantities of zero, two, or four. The total quantity of all the following features must be 2 or 4: • FC 3441 • FC 3442 • FC 3443	Plant or field	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 3443, FICON 10-km long-wavelength attachment	0	4	This feature is available as a concurrent MES. You must order this feature in quantities of zero, two, or four. The total quantity of all the following features must be 2 or 4: • FC 3441 • FC 3442 • FC 3443	Plant or field	Yes
FC 3461, 8 GB Memory upgrade, field	0	1	Mutually exclusive with FC 9461	Field only	No
FC 3462, 16 GB memory upgrade	0	1	Prerequisite: Microcode level 8.31.0.x or later.	Plant or field	No
FC 3488, 4 Gb Fibre Channel Switch†	0	6	You must order two instances of this feature for each of the following features ordered: • FC 9013 • FC 9020 Prerequisite: One instance of FC 4888 for each pair of FC 3488 ordered.	Plant and Field	Yes
FC 4015, Grid enablement	0	1	Prerequisites: When this feature is installed on a 3957-V06 or 3957-VEA you must order two instances of one of the following: • FC 1035 • FC 1036 • FC 1037 When this feature is installed on a 3957-V07 or 3957-VEB you must order two instances of **EITHER** FC 1032 **OR** FC 1033	Plant or field	No
FC 4016, Remove Cluster from Grid	0	99	Prerequisite: FC 4015	Field only	No
FC 4017, Cluster cleanup	0	99	Prerequisite: FC 4016 if cluster is part of a grid configuration	Field only	No
FC 4743, Remove 3957-V06/VEA	0	1	Mutually exclusive with FC 5638. Corequisites: FC 5627 or FC 5629	Field only	No
FC 4879, TS7700 BE Switch Mounting Hardware	0	1	On the 3584 Models L25 & D25: Mutually exclusive with FC 1951 and FC 2704.	Plant or field	No
FC 4880, TS7700 BE 16 Gb Fibre Channel Switch	0	2	Prerequisite: FC 4879	Plant or field	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 4888, Switch mount kit	0	3	Fibre channel switch types must be the same (2 GB or 4 GB) and cannot be intermixed within FC 4888.	Plant or field	No
FC 4897, Reinstall 4 Gb FC Switch	0	6	Prerequisites: One FC 4888 for each ordered pair of the following: • FC 3487 • FC 3488 • FC 4889 • FC 4890 • FC 4897	Plant and field	Yes
FC 5240, Dual port fibre channel host bus adapter†	1	1	You must order one instance of this feature. Corequisite: FC 9323 is required on 3952 F05 when FC 5626 is installed.	Plant	No
FC 5241, Dual port FC HBA	0	1	Corequisite: FC 9323 is required on the 3952 F05 when this feature is installed. Prerequisite: FC 5627	Plant or field	No
FC 5242, Dual Port 16 Gb Fibre Channel HBA	0	1	Prerequisite: FC 9323 is required on the 3952 F06 where the 3957-VEC is installed.	Plant or field	No
FC 5267, 1 TB cache enablement	1	28	This feature is available as a concurrent MES for the TS7740 only. It is not available for the TS7720 . Total hardware capacity may not be enabled unless appropriate quantities of FC 5267 are ordered. Total usable capacity is 13.42 TB.	Plant or field	No
FC 5268, 100 MB/sec increment	1	24 (when installed with a 3957-VEB or 3957-VEC) 25 (when installed with a 3957-V07)	This feature is available as a concurrent MES. • If FC 3441, FC 3442, or FC 3443 is installed, a maximum of 10 instances of 100 MB/sec is allowed on the 3957-V07 or 3957-VEB, where FC 9268, Plant installation of 100 MB/s throughput represents the first instance for a 3957-VEB. • If FC 3438 or FC 3439 is installed, a maximum of 25 instances of 100 MB/sec is allowed on the 3957-V07, 3957-VEB, or 3957-VEC where FC 9268, Plant installation of 100 MB/s throughput represents the first instance for a 3957-VEB or 3957-VEC. • A maximum of 6 instances of 100 MB/sec is allowed on a 3957-V06 or 3957-VEA, where FC 9268 represents the first instance for a 3957-VEA.	Plant or field	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5270, Increased virtual volumes	0	15	This feature is available as a concurrent, customer installed MES. It requires a microcode level of 8.20.0.xx or later. In a grid configuration, FC 5270, Increased virtual volumes, must be installed on every cluster in the grid to increase the number of supported virtual volumes in that grid.Prerequisites (for use with 3957-V06 or 3957-VEA): • FC 3461 • FC 9461	Plant or field	No
FC 5271, Selective device access control	0	1	This feature is available as a concurrent, customer installed MES. In a grid configuration, FC 5271, Selective device access control, must be installed on every cluster in the grid to increase the number of supported virtual volumes in that grid.	Plant or field	No
FC 5272, Enable disk encryption - Local Key Management	0	1	Prerequisite: • FC 9113 Corequisite: • FC 7330 is required on the 3952 machine type, where this TS7700 server is installed. • FC 7404 is required on each 3956 model in the configuration.	Plant only	Yes

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5273, TS7720/TS7760 Tape Attach enablement	0	1	Corequisite: When installed on a TS7720 with a 3957-VEB: • FC 5242 • At least one FC 5274 must be installed with this feature. When installed on a TS7700 with a 3957-VEC: • At least one FC 5274 must be installed with this feature. Mutually exclusive with: When installed on a TS7720 with a 3957-VEB: • RPQ 8B3604, 2nd Expansion Frame for TS7720 • TS7720 systems with one TS7720 Expansion Frame (3952-F05 with FC 7323) plus one TS7720 Encryption Capable Expansion Frame (3952-F05 with FC 7332)	Plant or field	No
FC 5274, Enable 1 TB Pending Tape Capacity	0	10	Corequisite: • FC 5273 must be installed with this feature.	Plant or field	No
FC 5275, Additional virtual devices	0	15	Prerequisite: • FC 3438 or FC 3439 **Note:** Installation of this feature requires SMIT (the system management interface tool). For more information, contact your IBM Service Representative.	Plant or field	No
FC 5276, Enable disk encryption - External Key Management	0	1	Mutually exclusive with: • FC 5272 Prerequisites: • FC 9113 Corequisite: • FC 7330 is required on the 3952 machine type, where this TS7700 server is installed. • FC 7404 is required on each 3956 model in the configuration.	Plant or field	No
FC 5277, External Disk Encryption Certificate - Field	0	1	Mutually exclusive with: • FC 9277 Prerequisites: • FC 5276	Field Only	No
FC 5278, Enable Cloud Storage Tier	0	1	None	Plant or field	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5512, TS3000 System Console KVM display, keyboard, mouse	0	1	Corequisite: FC 2725	Plant or field	Yes
FC 5626, Plant installation of 3957-VEA†	0	1	Prerequisites: • FC 7322 • At least one instance of FC 5636 • No more than six total instances of FC 5646 and FC 5647 Corequisite: FC 9350 on 3957-VEA	Plant only	Yes
FC 5627, Install 3957-VEB	0	1	Mutually exclusive with: • FC 5626 (if on 3957-VEA) • FC 5628 (if on 3957-V06) • FC 5629 (if on 3957-V07) Prerequisites: • FC 7322 • FC 4743 if this is a field-installed feature Corequisites: FC 9350 or FC 9351 on 3957-VEB	Plant or field	No
FC 5628, Plant installation of 3957-V06†	0† 1‡ † for the TS7720 ‡ for the TS7740	5† 6‡	Corequisite: FC 9350 against the IBM TS7700. If you have FC 7312 installed, the minimum requirement is 1. No minimum of this feature is required for the TS7720 since the first instance is shipped from the plant with FC 9268.	Plant only	Yes
FC 5629, Install 3957-V07	0	1	Mutually exclusive with: • FC 5626 (if on 3957-VEA) • FC 5627 (if on 3957-VEB) • FC 5628 (if on 3957-V06) Prerequisites: • FC 7312 • FC 4743 if this is a field-installed feature Corequisites: FC 9350 or FC 9351 on 3957-V07	Plant or field	No
FC 5630, Install 3957-VEC	0	1	Prerequisites: • FC 7333 Corequisites: FC 9350 on 3957-VEC	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5635, Plant installation of 3956-CS8	0	2	Prerequisites: • One instance of **EITHER** FC 7322 **OR** FC 7323 • For each instance of FC 5635 ordered, exactly five instances of FC 5646 are required Corequisite: FC 9352 is required against the 3956-CS8	Plant only	No
FC 5636, Plant installation of 3956-CS7†	0	1	Prerequisites: • FC 5626 • FC 7322 Corequisite: FC 9352 on 3956-CS7	Plant only	No
FC 5638, Plant installation of 3956-CC6†	0	1	Corequisite: FC 9352 against the TS7700 cache controller. If you have FC 7312 installed, the minimum requirement is 1.	Plant only	No
FC 5639, Plant installation of 3956-CC7†	0	2	Prerequisites: One instance of one of the following: • FC 7312 • FC 7313 • FC 7324 Corequisite: FC 9352 is required on 3956-CC7	Plant only	No
FC 5640, Plant installation of 3956-CC8	0	1	Prerequisite: FC 7312 Corequisite: FC 9352 is required on 3956-CC8	Plant only	No
FC 5641, Plant installation of 3956-CX7	0	6	Prerequisites: One instance of one of the following: • FC 7312 • FC 7313 • FC 7324 FC 5639 is required. Valid total quantities of FC 5641 and FC 5642 are 0, 1, and 3. Corequisite: FC 9354 is required on 3956-CX6.	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5642, Field installation of 3956-CX7	0	6	Prerequisites: One instance of one of the following: • FC 7312 • FC 7313 • FC 7324 FC 5639 is required. Valid total quantities of FC 5641 and FC 5642 are 0, 1, and 3. Corequisite: FC 9355 is required on 3956-CX7.	Field only	No
FC 5646, Plant installation of 3956-XS7	0	10	Prerequisites: • One of FC 7322 or FC 7323 • FC 5626 • FC 5636 Corequisite: FC 9354 on 3956-XS7 Valid total quantities of FC 5646 and FC 5647 are: • 1 to 6 when used with FC 7322 • 0 to 10 when used with FC 7323	Plant only	No
FC 5647, Field installation of 3956-XS7	0	5	Prerequisites: • One of FC 7322 or FC 7323 • FC 5626 • FC 5636 Corequisite: FC 9355 on 3956-XS7 Valid total quantities of FC 5646 and FC 5647 are: • 1 to 6 when used with FC 7322 • 0 to 10 when used with FC 7323	Field only	No
FC 5648, Plant installation of 3956-CX6†	1	3	Corequisite: FC 9354 against the TS7700 cache drawer. If you have FC 7312 installed, you must order a total of 0, 1, or 3 instances of FC 5648 and FC 5649.	Plant only	No
FC 5649, Field installation of 3956-CX6†	0	5	Prerequisites: • FC 7312 • FC 5638 Mutually exclusive with FC 5639. The total quantity ordered of FC 5649 and FC 5639 must be 0, 1, 3, or 5. When 5 are installed, the first 3 instances are achieved using FC 5648 and the last 2 instances using FC 5649.	Field only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5651, Plant installation of 3956-CS9	0	1	Prerequisites: • FC 5627 • FC 9352 on the 3956-CS9 • FC 7331 or FC 7332 on the 3952 F05	Plant only	No
FC 5652, Plant installation of 3956-CC9	0	1	Prerequisites: • FC 7330 • FC 9352 on the 3956-CC9	Plant only	No
FC 5653, Plant installation of 3956-CX9	0	2	Prerequisites: • FC 7330 • FC 9354 on the 3956-CX9	Plant only	No
FC 5654, Field installation of 3956-CX9	0	2	Prerequisites: • FC 7330 • FC 9355 on the 3956-CX9 • No more than two total instances of FC 5652, FC 5653, or FC 5654	Field only	No
FC 5655, Plant installation of 3956-XS9	0	15	Prerequisites: • FC 5627 and FC 5651 • FC 9354 on the 3956-XS9 • One instance of FC 7331 or FC 7332 on the 3952 F05 Valid total quantities of FC 5655 and FC 5656 are: • 0 to 15 with FC 7332	Plant only	No
FC 5656, Field installation of 3956-XS9	0	15	Prerequisites: • FC 5626 • FC 5636 • FC 9355 on the 3956-XS9 • One instance of FC 7331 or FC 7332 on the 3952 F05 Valid total quantities of FC 5655 and FC 5656 are: • 0 to 9 with FC 7331 • 0 to 15 with FC 7332	Field only	No
FC 5657, Plant installation of 3956-CSA	0	1	Prerequisites: • FC 7333 or FC 7334 • FC 9352 on the 3956-CSA	Plant only	No
FC 5658, Plant installation of 3956-XSA	0	15	Prerequisites: • FC 5657 • FC 9355 on the 3956-XSA Valid total quantities of FC 5658 plus FC 5659 plus FC 5661 and FC 5662 are: • 0 to 9 with FC 7333 • 0 to 15 with FC 7334 Mutually exclusive with FC 5660.	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5659, Field installation of 3956-XSA	0	15	Prerequisites: • FC 5657 • FC 9354 on the 3956-XSA Valid total quantities of FC 5659 plus FC 5658 plus FC 5661 and FC 5662 are: • 0 to 9 with FC 7333 • 0 to 15 with FC 7334 Mutually exclusive with FC 5660.	Field only	No
FC 5660, Plant installation of 3956-CSA with 8 TB DDMs	0	1	Prerequisites: • FC 9352 on the 3956-CSA • FC 7333 or FC 7334	Plant only	No
FC 5661, Plant installation of 3956-XSA with 8 TB DDMs	0	15	Prerequisites: • FC 5660 • FC 9354 on the 3956-XSA Valid total quantities of FC 5661 plus FC 5662 are: • 0 to 9 with FC 7333 • 0 to 14 with FC 7334	Plant only	No
FC 5662, Field installation of 3956-XSA with 8 TB DDMs	0	15	Prerequisites: • FC 5657 or FC 5660 • FC 9355 on the 3956-XSA Valid total quantities of FC 5658 plus FC 5659 plus FC 5661 plus FC 5662 are: • 0 to 9 with FC 7333 • 0 to 14 with FC 7334	Field only	No
FC 5758, Integrated control path	0	1	Prerequisites: • FC 4743 One total instance of: • FC 7312 • FC 7322 • FC 7330 • FC 7331 • FC 7333	Plant only	No
FC 5759, Integrated control path†	0	1	Prerequisite: FC 7312	Plant only	No
FC 6000, Intraframe fibre cable to 3956-CC6†	4	4	1-m Cable. One cable will be shipped per feature code.	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 6003, Intraframe fibre cable to 3957-V06†	4	4	2-m cable	Plant only	No
FC 7113, 16 TB SATA storage†	1	1	None.	Plant only	No
FC 7114, 32 TB SATA storage	1	1	None	Plant only	No
FC 7115, 36 TB SAS storage	1	1	None	Plant only	No
FC 7116, 33 TB SAS storage	1	1	None	Plant only	No
FC 7117, 48 TB SAS Storage	1	1	One of FC 7117 or FC 7118 is required.	Plant only	No
FC 7118, 96 TB SAS Storage	1	1	One of FC 7117 or FC 7118 is required. Mutually exclusive with FC 7117.	Plant only	No
FC 7120, 1.7 TB fibre storage, for the TS7740 cache controller†	1	1	1.7 TB is usable capacity.	Plant only	No
FC 7121, 3.43 TB fibre storage, for the TS7740 cache controller†	1	1	None. **Note:** This feature has been withdrawn.	Plant only	No
FC 7123, 9.6 TB Fibre storage	1	1	None	Plant only	No
FC 7124, 13.2 TB SAS storage	1	1	None	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7312, TS7740 Base frame	0	1	Mutually exclusive with the following: • FC 7310 • FC 7311 • FC 7315 • FC 7316 • 7317 • 7318 • 7319 • 7320 Prerequisites: • FC 1903 • FC 5629 • FC 5758 • One instance of FC 5638, FC 5639, **OR** FC 5640 – If ordering FC 5638, you must also order FC 5648 **OR** FC 5649 in quantities of: 0, 1, or 3 – If ordering FC 5639 or FC 5640, you must also order FC 5641 **OR** 5642 in quantities of: 0, 1, 3	Plant only	No
FC 7322, TS7720 Base frame	0	1	Mutually exclusive with: • All other 73xx features Prerequisites: • FC 1903 • FC 5758 • FC 5627 • FC 5635 **OR** FC 5636 • Between one and six instances of FC 5647	Plant only	No
FC 7323, TS7720 Storage expansion frame	0	1	Mutually exclusive with: • All other 73xx features Prerequisites: • One additional 3952 F05 with FC 7322 must be located within 10 meters of this frame. • FC 1903 • Two instances of FC 5635 • Up to 10 total instances of FC 5646 and FC 5647	Plant only	

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7330, TS7740 Encryption-capable base frame	0	1	Mutually exclusive with: • All other 73xx features Prerequisites: • FC 1903 • One instance of FC 2724 can be used with FC 2704, FC 2734, or FC 5512. • FC 5629 • FC 5758 • FC 9113 • FC 5652 • Valid total quantities of FC 5653 and FC 5654 are 0 to 1.	Plant only	No
FC 7331, TS7720 Encryption-capable base frame	0	1	Mutually exclusive with: • All other 73xx features Prerequisites: • FC 1903 • One instance of FC 2724 can be used with FC 2704, FC 2734, or FC 5512. • FC 5267 • FC 5651 • FC 5758 • FC 9113 • Valid total quantities of FC 5655 and FC 5656 are 0 to 9.	Plant only	No
FC 7332, TS7720 Encryption-capable expansion frame	0	1	Mutually exclusive with: • All TSSC features • All other 73xx features Prerequisites: • FC 1903 • FC 5630 • FC 5758 • Ship with R4.0 Machine Code, FC AGK0 • FC 5657 • Valid total quantities of FC 5658 and FC 5659 are 0 to 9.	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7333, TS7700 Encryption-capable base frame	0	1	Mutually exclusive with: • All other 73xx features Prerequisites: • FC 1903 • FC 5630 • FC 5758 • FC AGK0 • FC 5657 or FC 5660 • When FC 5657 is installed, valid quantities of FC 5658, FC 5659, and FC 5662 are 0 to 9 • When FC 5660 is installed, valid quantities of FC 5661 and FC 5662 are 0 to 9	Plant only	No
FC 7334, TS7700 Encryption-capable expansion frame	0	1	Mutually exclusive with: • All TSSC features • All other 73xx features Prerequisites: • This frame must be installed within 10 meters to an attached TS7700 Base Frame. • FC 1903 • FC 5657 or FC 5660 Limitations: • When FC 5657 is installed, valid quantities of FC 5658, FC 5659, plus FC 5662 are 0 to 15 • When FC 5660 is installed, valid quantities of FC 5661 plus FC 5662 are 0 to 14	Plant only	No
FC 7403, Enable first expansion drawer, for the TS7740 cache controller	0	1	If at least one cache expansion drawer is attached to the TS7740 Cache Controller, then this feature is required.	Plant or field	No
FC 7404, Encryption	0	1	Prerequisite: This feature is required when FC 5272 is installed on the TS7700 Server	Plant or field	No
FC 9000, Mainframe attachment†	1	1	Prerequisite: up to four total instances of any of the following • FC 3441 • FC 3442 • FC 3443	Plant only	No
FC 9013, Attach to TS7700†	0	1	Prerequisites: FC 3488 and FC 1901 Mutually exclusive with FC 9010 and FC 9015	Plant and Field	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9110, Ship with R1.7 machine code	0	1	Prerequisites: One of the following feature sets: • FC 7312 • FC 5628 • FC 5640 **OR** • FC 7322 • FC 5626 • FC 5635	Plant only	No
FC 9111, Ship with R2.0 machine code	0	1	One instance of any of the following features is required against the 3952 F05 and either the3957-V07 or 3957-VEB: • FC 9111 • FC 9112 • FC 9113 • FC 9114 Prerequisites: One of the following feature sets: • FC 7312 • FC 5629 • FC 5640 **OR** • FC 7322 • FC 5627 • FC 5635	Plant only	No
FC 9112, Ship with R2.1 machine code	0	1	One instance of any of the following features is required against the 3952 F05 and either the3957-V07 or 3957-VEB: • FC 9111 • FC 9112 • FC 9113 • FC 9114 Prerequisites: One of the following feature sets: • FC 7312 • FC 5629 • FC 5640 **OR** • FC 7322 • FC 5627 • FC 5635	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9113, Ship with R3.0 machine code	0	1	One instance of any of the following features is required against the 3952 F05 and either the3957-V07 or 3957-VEB: • FC 9111 • FC 9112 • FC 9113 • FC 9114 Prerequisites: One of the following feature sets: • FC 7312 • FC 5629 • FC 5640 **OR** • FC 7322 • FC 5627 • FC 5635	Plant only	No
FC 9114, Ship with R3.1 machine code	0	1	One instance of any of the following features is required against the 3957-V07 or 3957-VEB: • FC 9111 • FC 9112 • FC 9113 • FC 9114 FC 9114 is required against a new 3952 F05 ordered from manufacturing.	Plant only	No
FC 9115, Ship with R3.2 Machine Code	0	1	One instance of any of the following features is required against the 3957-V07 or 3957-VEB: • FC 9111 • FC 9112 • FC 9113 • FC 9114 • FC 9115 FC 9115 is required against a new 3952 F05 ordered from manufacturing.	Plant only	No
FC 9116, Ship with R3.3 Machine Code	0	1	One instance of any of the following features is required against the 3957-V07 or 3957-VEB: • FC 9111 • FC 9112 • FC 9113 • FC 9114 • FC 9115 • FC 9116 FC 9116 is required against a new 3952 F05 ordered from manufacturing.	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9217, Attach to 3953 LM†	0	1	This feature is mutually exclusive with FC 9218.	Plant only	Yes
FC 9218, Attach to 3494 LM†	0	1	This feature is mutually exclusive with FC 9217. This feature is not supported by microcode levels of 8.20.0.xx or later. It must be removed before upgrading to 8.20.0.xx or later.	Plant or field	Yes
FC 9219, Attach to TS3500/TS4500†	0	1	Corequisite: FC 5273.	Plant or field	No (initially)
FC 9230, Attach to 3957-V06†	1	1	Prerequisite: Four instances of FC 6003.	Plant only	No
FC 9268, Plant installation of 100 MB/s throughput†	1	1	In addition to this feature, you can order multiple instances of FC 5268, 100 MB/sec increment against the TS7700: • 24 instances of FC 5268 when feature code 3438 or 3439 is installed • 9 instances of FC 5268 when feature code 3441, 3442, or 3443 is installed	Plant only	No
FC 9277, External Disk Encryption Certificate - Plant	0	1	Mutually exclusive with: • FC 5277	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9323 Expansion frame attachment	0	2	When installed on an encryption-capable TS7720 Base Frame (3952-F05 containing FC 7331) and attaching an encryption-capable TS7720 Expansion Frame (3952-F05 containing FC 7332) with a 3957-VEB: • Maximum quantity of two requires R3.1 machine code or later. • FC 5241 is required on the 3957-VEB • Nine total instances of FC 5655 and FC 5656 are required. • If two (FC 7334) encryption-capable expansion frames are also attached to this base frame, the first expansion frame must contain a total of 15 instances of FC 5655 and FC 5656. When installed on an encryption-capable TS7720 Base Frame (3952-F05 containing FC 7331) and attaching an encryption-capable TS7700 Expansion Frame (3952-F06 containing FC 7334) with a 3957-VEB: • Maximum quantity of two requires R4.0 machine code or later. • Nine total instances of FC 5655 and FC 5656 are required. • If two (FC 7332) encryption-capable expansion frames are also attached to this base frame, the first expansion frame must contain a total of 15 instances of FC 5655 and FC 5656. **Note:** When operating a microcode level of 8.32.0.x or later, VTD_EXEC.155 is not required.	Plant or field	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9323 Expansion frame attachment (continued)	0	2	When installed on an encryption-capable TS7760 Base Frame (3952-F06 containing FC 7333) with a 3957-VEC: • Maximum quantity of two requires R4.0 machine code or later. • FC 5242 is required on the 3957-VEC • When FC 5657 is installed, nine total instances of FC 5658, plus FC 5659, and FC 5662 are required. • When FC 5660 is installed, nine total instances of FC 5661 plus FC 5662 are required. • If two (FC 7334) encryption-capable expansion frames are also attached to this base frame, the first (FC 7334) expansion frame must contain a total of 15 instances of FC 5658, FC 5659 and FC 5662 or 15 instances of FC 5661 and FC 5662.	Plant or field	No
FC 9339, Replacing TS7740 System	0	1	Prerequisite: FC 5273 is required on the 3957-VEC installed on 3952 F06	Plant only	No
FC 9350, Plant Install†	0	1	Mutually exclusive with: • FC 9351 • FC 4743 on the 3952 F05 Tape Frame. Corequisite: • FC 5628 against 3952 F05 • FC 5630 against 3952 F06	Plant only	No
FC 9351, Field merge TS7700 Server in 3952 F05	0	1	Mutually exclusive with FC 9350 Corequisite: FC 4743 against the 3952 F05	Plant only	
FC 9352, Plant Install†	1	1	You must order one instance of FC 9352 **OR** FC 9353. Corequisites: • FC 5651 against the 3952 F05 if installing a 3956-CS9 • FC 5652 against the 3952 F05 if installing a 3956-CC9 • FC 5657 or FC 5660 against the 3952 F06 if installing a 3956-CSA	Plant only	No
FC 9353, Field merge in 3952 F05	0	1	You must order one of **EITHER** FC 9352 **OR** FC 9353. Corequisite: FC 5637 against the 3952 F05	Plant only	No

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9354, Plant Install†	0	1	You must order one total instance of FC 9354 **OR** FC 9355.Corequisite: • FC 5658 or FC 5661 against the 3952 F06 if installing an 3956-XSA	Plant only	No
FC 9355, Field merge	0	1	You must order one total instance of FC 9354 **OR** FC 9355Corequisite: • FC 5654 against the 3952 F05 if installing a 3956-CX9 • FC 5656 against the 3952 F05 if installing an 3956-XS9 • FC 5659 or FC 5662 against the 3952 F06 if installing an 3956-XSA	Plant only	No
FC 9461, 8 GB Memory upgrade, plant†	0	1	Mutually exclusive with FC 3461 This feature is required on all new 3957-V06/VEA TS7700 servers released with microcode level 8.7.0.xx or later.	Plant only	No
FC 9700, No factory cables†	0	1	You must order **EITHER** one instance of FC 9700 **OR** two instances of one of the following: • FC 0201 • FC 0202 • FC 0203 • FC 0204 • FC 0205 • FC 0206	Plant only	Yes
FC 9900, Tape Encryption configuration	0	1	This feature is available as a concurrent MES if the TS11xx encryption capable tape drives were running in native mode prior to the TS7700's current online process.	Plant or Field	No
FC 9954, NEMA L6-30 power cord	0	1	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966.	Plant or field	Not applicable
FC 9955, RS 9750 DP power cord	0	1	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966.	Plant or field	Not applicable
FC 9956, IEC 309 power cord	0	1	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966.	Plant or field	Not applicable
FC 9957, PDL 4.3 power cord	0	1	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966.	Plant or field	Not applicable
FC 9958, Korean 4.3-m power cord	0	1	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966.	Plant or field	Not applicable
FC 9959, Unterminated power cord	0	1	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966.	Plant or field	Not applicable

Table 67. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9966, Unterminated power cord (China)	0	1	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966.	Plant or field	Not applicable
FC AG00, Shipping and Handling - No charge	0	1	One of FC AG00 or AGGA is required.	Plant only	No
FC AGGA, Shipping and Handling - F06	0	1	One of FC AG00 or AGGA is required.	Plant only	No
FC AGK0, Ship with R4.0 Machine Code	0	1	Prerequisite: • FC 7333 One of FC AGK0 or FC AGKE is required. Mutually exclusive with FC AGKE.	Plant only	No
FC AGKE, Ship with R4.1 Machine Code	0	1	Prerequisite: • FC 7333 One of FC AGK0 or FC AGKE is required. Mutually exclusive with FC AGK0.	Plant only	No
FC AGKR, Ship with R4.1.2 Machine Code	0	1	One of FC AGK0, FC AGKE, or FC AGKR is required. Mutually exclusive with FC AGK0 and FC AGKE.	Plant only	No
† Withdrawn for at least one component. Refer to the *Quick reference by component* topic in the **Related information** section to verify availability.					

Related information

"System requirements" on page 63

"Quick reference by component" on page 143

Checklists

This section links to checklists that help you plan for the arrival of your new TS7700 and ensure completion of post-installation tasks.

Planning for new system arrival (customer tasks)

Use this section to locate and collect information required to install a TS7700.

As you plan for the installation of your new system, consult the following tables and consider the values that you would provide to match the information listed in the **Field** column. This information will be used to install your TS7700 and as reference during any future service actions. If you are working from an electronic copy of this information center, consider printing this topic to use it as a working document.

Before the service support representative (SSR) arrives, you should complete the **Systems Assurance Worksheets**. You can get the **Systems Assurance Worksheets** from your marketing representative or from your Field Technical Support Specialist.

The **Systems Assurance Worksheets** are similar to Table 68 on page 214 through Table 86 on page 241.

Important: The information that is requested in the tables should be completed before the arrival of the SSR. This information is used by the SSR to perform installation tasks. The pre-installation information should be recorded in tables in the following sections:

- Cluster Description Table and Notes (Table 68 on page 214)
- TS3500 or TS4500 Tape Library Configuration Information Table and Notes (Table 69 on page 216)
- TS3500 or TS4500 Tape Library Drive Information Table and Notes (Table 70 on page 220)
- TS3500 Limited Drive Support Table (Table 71 on page 224)
- Media Volume Serial (VOLSER) Range Table and Notes (Table 72 on page 224)
- Encryption Key Information Table (Table 73 on page 224)
- TS4500 Limited Drive Support Table (Table 74 on page 225)
- Review media types in “3592 Tape Cartridges” on page 58
- TS7700 Code Activation/VPD Information Table and Notes (Table 75 on page 225)
- TS7700 Customer Network Configuration Table and Notes (Table 76 on page 228)
- TSSC Configuration Information Table and Notes (Table 77 on page 230)
- TSSC IP Address Table and Notes (Table 78 on page 231)
- Grid Local Address Table and Notes (Table 84 on page 234)
- Summary Table (Table 85 on page 237)
- TSSC Grid Configuration Information Table and Notes (Table 86 on page 241)

After you complete the **Systems Assurance Worksheets**, ensure that you store the Worksheets with the TS7700 so the worksheets are available for future service calls.

Cluster Descriptions

Complete the **Description of Location** column with geographical information that is unique to each cluster. Complete as much information as possible. Some suggestions for descriptions are the x, y coordinates within a data center, room number, floor number, building number, city, and so on.

- If you are installing a stand-alone (non-GRID) TS7700, then choose a cluster number designation 0 - 7 and complete the **cluster j** information, but leave the other cluster fields blank.
- If you are joining to an existing stand-alone cluster to create a two cluster GRID TS7700, then complete the **cluster j** (new joining cluster) and **cluster x** (existing cluster) information, but leave the remaining cluster fields blank.
- If you are installing a three-cluster GRID TS7700, then complete the Cluster 0, Cluster 1, and Cluster 2 information but leave the Cluster 3, Cluster 4, Cluster 5, Cluster 6, and Cluster 7 fields blank.

- If you are installing a four-cluster GRID TS7700, then complete the Cluster 0, Cluster 1, Cluster 2, and Cluster 3 information but leave the Cluster 4, Cluster 5, Cluster 6, and Cluster 7 fields blank.
- If you are installing a five-cluster GRID TS7700, then complete the Cluster 0, Cluster 1, Cluster 2, Cluster 3, and Cluster 4 information but leave the Cluster 5, Cluster 6, and Cluster 7 fields blank. An RPQ is required for a grid of five or more clusters.
- If you are installing a six-cluster GRID TS7700, then complete the Cluster 0, Cluster 1, Cluster 2, Cluster 3, Cluster 4, and Cluster 5 information. Leave the Cluster 6 and Cluster 7 fields blank. An RPQ is required for a grid of five or more clusters.
- If you are installing a seven-cluster GRID TS7700, complete the Cluster 0, Cluster 1, Cluster 2, Cluster 3, Cluster 4, Cluster 5, and Cluster 6 information. Leave the Cluster 7 field blank. An RPQ is required for a grid of five or more clusters.
- If you are installing an eight-cluster GRID TS7700, complete the Cluster 0, Cluster 1, Cluster 2, Cluster 3, Cluster 4, Cluster 5, Cluster 6, and Cluster 7 information. An RPQ is required for a grid of five or more clusters.

Note: The terms CLUSTER 0, CLUSTER 1, CLUSTER 2, CLUSTER 3, CLUSTER 4, CLUSTER 5, CLUSTER 6, and CLUSTER 7 refer to eight separate TS7740s, TS7720s, TS7720TAs, TS7760s, or TS7760TAs participating in a GRID (peer to peer) configuration, but you can have a mix (hybrid) configuration of TS7740, TS7720, TS7720 Tape Attach, TS7760, and TS7760 Tape Attach. The cluster number identifiers in a grid must be unique but they do not need to be in a specific order. For example, you might have a 3-way grid that is composed of CLUSTER 2, CLUSTER 3, and CLUSTER 6. In choosing a cluster number identifier, it is important for the customer to plan for future configurations. For example, the customer might set up two 2-way grids and assign cluster identifiers of CLUSTER 0 and CLUSTER 1 for grid-A and CLUSTER 2 and CLUSTER 3 for grid-B. Eventually, the customer might plan on merging the two grids to create a four-way grid that is composed of CLUSTER 0-3. Advanced planning removes extra steps in a grid merge process.

For 3-way or higher configurations, the customer can make use of cluster families. The customer will have the ability to group two or more clusters together into a family. Clusters within a family will then cooperate with each other in order to most efficiently bring copies into their cluster family. At any one time, only one cluster within a family will copy a volume into a family group from an external family. If a copy already exists on at least one cluster within the family, replication among clusters in the family is deferred for that volume. Once all volumes external to the family exist within at least one of the clusters in the family, the clusters will then replicate among each other in order to be brought up to consistency. (The copies between family members will actually start if there are available copy tasks that are not tied up with remote copies, that is, there are less than 20 remote copies remaining). This provides improved copy performance based on using additional copy task within the family to pull copies into the family. This might be configured by the customer from the management interface after some performance runs.

Provide the serial number and location of the machines that make up each cluster. The information in Table 68 on page 214 helps the installer know which TS7700 is designated as Cluster 0, which is Cluster 1, which is Cluster 2, which is Cluster 3, which is Cluster 4, which is Cluster 5, which is Cluster 6, and which is Cluster 7.

Table 68. Cluster Description Table and Notes

Cluster	Component Serial Numbers	Description of Location
Cluster 0	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 1	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 2	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 3	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	

Table 68. Cluster Description Table and Notes (continued)

Cluster	Component Serial Numbers	Description of Location
Cluster 4	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 5	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 6	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 7	3957-Vxx:	
	3952 F05:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F06: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	

Tape Library Attachment Configuration.

Provide values for each of the TS3500 or TS4500 configuration fields defined in Table 69 and Table 70 on page 220. Required information includes:

- Network Ethernet configuration method
- Network Ethernet IP address for TS3500 or TS4500 management GUI access
- TS3500 or TS4500 Ethernet hostname
- Network Ethernet gateway
- Network Ethernet subnet mask
- Maximum number of physical cartridges
- Logical library name for the TS3500 or TS4500
- Physical position and World Wide Node Name (WWNN) of each drive in the TS3500 or TS4500, according to cluster

Table 69. TS3500 or TS4500 Tape Library Configuration Information Table and Notes

Field	Value	Notes
TS3500 or TS4500 Tape Library Serial Number	CLUSTER 0 - 7	The serial number of the TS3500 or TS4500 Tape Library model Lxx (frame 1) is a 7 character serial number consisting of the 2-digit Plant of Mfg code and the 5 character sequence number. It can be found on the back door of the TS3500 or TS4500 Tape Library Lxx frame, or by viewing library Vital Product Data (VPD) on the library operator panel or web user interface.
TS3500 or TS4500 Tape Library Ethernet Network Configuration Method (customer network) Library Type:	CLUSTER 0: DHCP [ ] Fixed IP [ ]	The network configuration method is specified by the customer's LAN administrator. It is either Fixed IP or Dynamic Host Configuration Protocol (DHCP). **Note:** Fixed IP is recommended.
	CLUSTER 1: DHCP [ ] Fixed IP [ ]	
	CLUSTER 2: DHCP [ ] Fixed IP [ ]	
	CLUSTER 3: DHCP [ ] Fixed IP [ ]	
	CLUSTER 4: DHCP [ ] Fixed IP [ ]	
	CLUSTER 5: DHCP [ ] Fixed IP [ ]	
	CLUSTER 6: DHCP [ ] Fixed IP [ ]	
	CLUSTER 7: DHCP [ ] Fixed IP [ ]	

Table 69. TS3500 or TS4500 Tape Library Configuration Information Table and Notes (continued)

Field	Value	Notes
TS3500 or TS4500 Tape Library Ethernet IP address (customer network) (Used for Web interface access)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	If Network Configuration Method is DHCP, then this field is not used. **Note:** The Ethernet ports are 10/100 Mb only.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
TS3500 or TS4500 Tape Library Ethernet Hostname	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	The entry in this field is used to identify the machine in remote support logs. **Note:** Even if hostnames are not typically used by the customer, this hostname is still required. A typical hostname is ATL1.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 69. TS3500 or TS4500 Tape Library Configuration Information Table and Notes (continued)

Field	Value	Notes
TS3500 or TS4500 Tape Library Ethernet Subnet Mask (customer network)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	If Network Configuration Method is DHCP, then this field is not used.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
TS3500 or TS4500 Tape Library Ethernet Gateway (customer network)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	If Network Configuration Method is DHCP, then this field is not used.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 69. TS3500 or TS4500 Tape Library Configuration Information Table and Notes (continued)

Field	Value	Notes
TS3500 or TS4500 Tape Library Logical Library Name (for TS7700 attachment)		Each TS7700 must be connected to a single TS3500 or TS4500 tape library logical library. This logical library must have a name, which should have been assigned when the logical library was created. Record the logical library name (assign it if necessary). The logical library name is needed to perform the following tasks: • Configuring the logical library. • Obtaining the Starting Element Address for the logical library • Obtaining the physical position of tape drives within the logical library • Obtaining the WWNNs of those tape drives • Setting the Cartridge Assignment Policy • Configuring Control paths • Setting Exports to Show (default) • Setting Encryption method if necessary • Configuring ALMS
Max Cartridges		This value defaults to the number of physical cartridge slots that are currently installed in the TS3500 or TS4500 tape library. Valid values range 1 - 6260. You might want to set a different value in the following cases: • The customer wants to restrict the number of cartridges in the logical library to manage the cost of application licensing. • The TS3500 or TS4500 tape library will be expanded later and you want to avoid reconfiguring the host then.

Notes:

- A TS7700 cluster must have a minimum of 4 and maximum of 16 tape drives that can be connected.
- It is recommended that the drives for a single TS7700 are listed in order by using the frame and row. As an example, if a TS7700 has eight drives that are in F4,R01 - F4,R08, then drive 1 should be F4,R01, drive 2 should be F4,R02, and so on. If a second TS7700 has four drives in F2,R11, F2,R12, F3R1, and F3R2, then drive 1 should be F2,R11, drive 2 should be F2,R12, drive 3 should be F3,R01, and drive 4 should be F3,R02. This is not a requirement, but it might help avoid confusion when identifying drives during future troubleshooting.
- Distributing the tape drives across 2 TS3500 or TS4500 frames is recommended to improve availability. Placing up to eight drives (two control path drives) in one frame and up to eight drives (two control path drives) in a second frame is recommended.

TS3500 or TS4500 Tape Library Drive Information Table and Notes

Table 70. TS3500 or TS4500 Tape Library Drive Information Table and Notes

Field	**Values**	
Tape Drive Physical Positions (Fn,Rnn) in the TS3500 or TS4500 tape library for the drives that are assigned to each 3957-Vxx. Record the physical position and the last two digits of the World Wide Node Name (WWNN) for each tape drive. Circle the drives that will be control paths. Read the notes below this table for guidance in completing the values.	**CLUSTER 0:** F=Frame, C=Column, R=Row WWNN=World Wide Node Name **Note:** For the TS3500 tape library, complete F (Frame) and R (Row) only. • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___	**CLUSTER 1:** F=Frame, C=Column, R=Row WWNN=World Wide Node Name **Note:** For the TS3500 tape library, complete F (Frame) and R (Row) only. • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___
	CLUSTER 2: F=Frame, C=Column, R=Row WWNN=World Wide Node Name **Note:** For the TS3500 tape library, complete F (Frame) and R (Row) only. • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___	**CLUSTER 3:** F=Frame, C=Column, R=Row WWNN=World Wide Node Name **Note:** For the TS3500 tape library, complete F (Frame) and R (Row) only. • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___

Table 70. TS3500 or TS4500 Tape Library Drive Information Table and Notes (continued)

Field	Values	
	CLUSTER 5: F=Frame, C=Column, R=Row WWNN=World Wide Node Name **Note:** For the TS3500 tape library, complete F (Frame) and R (Row) only. • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___	**CLUSTER 6:** F=Frame, C=Column, R=Row WWNN=World Wide Node Name **Note:** For the TS3500 tape library, complete F (Frame) and R (Row) only. • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___ • F___C___R___WWNN___

Notes:

- A TS7700 cluster must have a minimum of 4 and maximum of 16 tape drives that can be connected.
- It is recommended that the drives for a single TS7700 attached to a TS3500 are listed in order by using the frame and row. As an example, if a TS7700 has eight drives that are in F4,R01 - F4,R08, then drive 1 should be F4,R01, drive 2 should be F4,R02, and so on. If a second TS7700 has four drives in F2,R11, F2,R12, F3R1, and F3R2, then drive 1 should be F2,R11, drive 2 should be F2,R12, drive 3 should be F3,R01, and drive 4 should be F3,R02. This is not a requirement, but it might help avoid confusion when identifying drives during future troubleshooting.
- Distributing the tape drives across two TS3500 or TS4500 frames is recommended to improve availability. Placing up to eight drives (two control path drives) in one frame and up to eight drives (two control path drives) in a second frame is recommended.

To obtain the WWNN, press **Menu** > **Vital Product Data** > **World Wide Node Names**.

Media Volume Serial (VOLSER) Range Table and Notes

Complete Table 72 on page 224 with the requested information. There might be one or many **Media Volume Serial Ranges** so complete as many rows as apply to your system.

From, To

This is a range containing the bar code label VOLSERs of all the cartridges assigned to a single TS7700. As an example, if cartridges assigned to a TS7700 have bar code labels in the range from A00000JA - A00500JA, then record the following:

- From: __A00000_
- To:__A00500

Media Type

The type is indicated by the last two characters of the 8character bar code label VOLSER on the cartridges. As an example, if the cartridges are labeled 123456JA then the media type is JA. Label rules are defined in the following notes.

Notes:

- JA and JJ tape cartridges are supported and can be mixed in a TS7700. JA and JJ media is supported in "read-only" mode when E07 tape drives are connected to the TS7700. JA and JJ tape cartridges are not supported by E08 tape drives.
- JB tape cartridges are also supported (and can be mixed with JA and JJ tape cartridges, except when E07 tape drives are installed) if all of the tape drives associated with the TS7700 are 3592 model E05, E06/EU6, or E07 tape drives and none of them are in J1A emulation mode. JB tape cartridges are not supported by E08 tape drives.
- JC and JK tape cartridges are supported by E07 and E08 tape drives.
- JD and JL tape cartridges are only supported by E08 tape drives.
- No other tape types are currently supported for use with the TS7700.
- If there is at least one 3592 model J1A tape drive associated with the TS7700, then ALL 3592 model E05 tape drives associated with the TS7700 must be in J1A emulation mode.
- If at least one tape cartridge associated with a TS7700 has been written by a 3592 model E05 tape drive that is NOT in J1A emulation mode, then the TS7700 no longer supports any 3592 model J1A tape drives or any 3592 model E05 tape drive that is in J1A emulation mode. Once you go to 'E05 Native' mode, you cannot go back to J1A mode. This is because the J1A tape drive cannot read or write a tape cartridge that is written in E05 mode and the TS7700 does not currently support mixed J1A and E05 tape drives (unless all E05 tape drives are in J1A emulation mode).
- The capacity of a JJ tape cartridge is 60 GB if written by a J1A tape drive (or an E05 tape drive that is in J1A emulation mode), or 100 GB if written by an E05 tape drive that is NOT in J1A emulation mode, or 128 GB if written by an E06 tape drive.
- The capacity of a JA tape cartridge is 300 GB if written by a J1A tape drive (or an E05 tape drive that is in J1A emulation mode) or 500 GB if written by an E05 tape drive that is NOT in J1A emulation mode, or 640 GB if written by an E06/EU6 tape drive.
- The capacity of a JB cartridge is 700 GB if written by an E05 tape drive that is not in J1A emulation mode, or 1 TB if written by an E06/EU6 tape drive, or 1.6 TB if written by an E07 tape drive.

- The capacity of a JC cartridge is 4 TB if written by an E07 tape drive or 7 TB if written by an E08 tape drive.
- The capacity of a JK cartridge is 500 GB if written by an E07 tape drive or 900 GB if written by an E08 tape drive.
- The capacity of a JD cartridge is 10 TB if written by an E08 tape drive.
- The capacity of a JL cartridge is 2 TB if written by an E08 tape drive.
- 3592 model E06/EU6 tape drives CANNOT be intermixed with 3592 model J1A, 3592 model E05, or 3592 model E07 tape drives.
- 3592 model E08/EH8 tape drives can be intermixed with 3592 model J1A, E05, E06, and E07 tape drives. See Table 71 on page 224 for valid combinations.
- TS7700 Feature Code 9900 (Encryption) requires that all E05 tape drives are in E05 'Native' mode. The Encryption feature is NOT compatible with J1A emulation mode. The E06 drives support encryption and do not require to be set into any mode.

If you are installing 3592 E05 tape drives, use the rules that are defined in the previous step to determine whether you want the 3592 E05 tape drives attached to the TS7700 to be in J1A emulation mode or in E05 native mode. Record this value in the **E05 in J1A Emulation** entry in Table 75 on page 225.

(Distributed) Library Sequence Number

The Library Sequence Number is assigned by your administrator. This is a 5 hex character name that is used as an identifier for a specific cluster and the associated Library in a grid configuration. This identifier is specified in the TS7700 configuration.

It is required even if the TS7700 is not in a Grid configuration.

Note: Each VTS partition must have a single, unique value for the Distributed Library Sequence Number. For the TS7700, a typical value is the last five digits of the 3952 Tape Frame serial number.

Home Pool

Also called Scratch Pool. A pool is a group of physical tape cartridges. A scratch pool is a group of cartridges that are considered to be scratch, meaning that they are ready for use by any write job.

You may have assigned a Home Pool value. If one has not been set, the default value is 00.

If you are installing a 3592 model E08 (TS1150) drive in a TS7740/TS7760, the microcode level must be at 8.33.x.x or later and has a limited heterogeneous drive support shown in Table 71 on page 224:

Note: When using E08 tape drives, go to the MI Pool Properties page to ensure that media settings are set to either **Any 3592** or an E08 compatible media type.

Table 71. TS3500 Limited Drive Support Table

	Pre-E08 Drive Type 2	Min and Max Number of E08 (Heterogeneous) Drives Allowed	Min and Max Number of E08 (Homogeneous) Drives Allowed	Combined Maximum Number of Tape Drives Allowed
3592 J1A	3592 E05 in J1A emulation mode	2 – 12 (any combo up to 12)	4 – 14	16
3592 E05 in Native Mode	Not supported	2 – 12	4 – 14	16
3592 E06	Not supported	2 – 12	4 – 14	16
3592 E07	Not supported	2 – 12	4 – 14	16

- If you are installing a 3592 model E08 (TS1150) drive into a TS3500 Tape Library and it is connected to a TS7700 with tape drives attached, the microcode level must be at 8.33.x.x or later and supports the following homogeneous tape drive configurations:
  - Up to 16 drives in a single logical library for a new TS7760 installation
  - Up to 16 drives in a single logical library for a TS7720 MES conversion to a TS7760
  - Up to 16 drives in a single logical library for existing TS7700 with active data on JK and/or JC cartridges only

  Note: The following cartridges can be used as scratch media: JK, JC, JL, and JD.

Table 72. Media Volume Serial (VOLSER) Range Table and Notes

Cluster (0 to 7)	From	To	Media Type	(Distributed) Library Sequence Number	Home Pool	Scratch Category

Table 73. Encryption Key Information Table

Key Server Address	Address	Port
Primary		
Secondary		

- If you are installing a 3592 model EH8 (TS1150) tape drive into a TS4500 Tape Library and it is connected to a TS7700 with tape drives attached, the microcode level must be at 8.40.x.x or later and supports the following tape drive configurations shown in Table 74.

Table 74. TS4500 Limited Drive Support Table

	Pre-EH8 Drive Type 2	Min and Max Number of EH8 (Heterogeneous) Drives Allowed	Min and Max Number of EH8 (Homogeneous) Drives Allowed	Combined Maximum Number of Tape Drives Allowed
3592 EH7	Not supported	2 – 12	4 – 14	16

TS7700 configuration

Provide values for each of the defined TS7700 configuration fields defined in Table 75 and Table 76 on page 228. Required information includes:

- Library sequence numbers (composite and distributed)
- Disk cache type
- IP addresses (logical, primary, alternate, NTP)
- Subnet mask
- Gateway
- Tape drive format
- Network speed settings

Table 75. Code Activation/VPD Information Table and Notes

Field	Value	Notes®
Machine model		
Cluster Index	CLUSTER 0:	
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER 4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	
TS7700 3952-F0x Base Frame serial number	CLUSTER 0:	Refer to the frame serial number, on a label in the bottom of the 3952 Tape Frame inside the rear door. Use the last 5 characters of the serial number that is shown on the label.
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER 4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	

Table 75. Code Activation/VPD Information Table and Notes (continued)

Field	Value	Notes®
TS7700 3952-F0x Storage Expansion Frame serial number	CLUSTER 0:	
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER 4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	
TS7700 3952-F0x Storage Expansion Frame serial number (Optional)	CLUSTER 0:	
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER \4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	
Composite Library Sequence Number		This 5-character hexadecimal name must be the same on all clusters (peers) within the same grid. This identifier is specified in the TS7700 configuration. It is required even if the machine is not in a grid configuration. **Note:** This is the Composite Library Sequence Number. It must be different than the Distributed Library Sequence number specified below.
Distributed Library Sequence Number		This 5-character hexadecimal number is assigned by the customer's administrator and is used as an identifier for a specific cluster. Each TS7700 must have a single, unique value for the Distributed Library Sequence Number. A typical value is the last five digits of the 3952 Tape Frame serial number. **Note:** This number must be different than the Composite Library Sequence number.
TS3500 or TS4500 attached	Y or N	Reply yes or no if there will be a TS3500 or TS4500 tape library attached at the time of the TS7700 installation.
E05 in J1A Emulation	Y or N or NA	
TS7700 cache type		The TS7700 Cache distributed from manufacturing with microcode 8.40.0.xx uses a DS3000(r) cache type. For a new TS7700, the cache type is 3956-CSA.

Table 75. Code Activation/VPD Information Table and Notes (continued)

Field	Value	Notes®
TS7700 cache controller serial number (Base Frame)	CLUSTER 0:	Refer to the serial number label on the front of the bottom cache drawer. The serial number is on a label on the detachable cover on the right side of the cache drawer. **Note:** This serial number is only used for reporting installation or repair of the cache. The TS7700 microcode activation process allows you to change the serial number, but you should always use the serial number that was set during the manufacturing process.
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER 4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	
Additional controllers		Enter the number of additional cache controllers that are installed. **Note:** There is only 1 controller per frame.
TS7700 cache controller serial number (Cache Frame 1)	CLUSTER 0:	Refer to the serial number label on the front of the bottom cache drawer. The serial number is on a label on the detachable cover on the right side of the cache drawer. **Note:** This serial number is only used for reporting installation or repair of the cache. The TS7700 microcode activation process allows you to change the serial number, but you should always use the serial number that was set during the manufacturing process.
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER 4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	
TS7700 cache controller serial number (Cache Frame 2)	CLUSTER 0:	Refer to the serial number label on the front of the bottom cache drawer. The serial number is on a label on the detachable cover on the right side of the cache drawer. **Note:** This serial number is only used for reporting installation or repair of the cache. The TS7700 microcode activation process allows you to change the serial number, but you should always use the serial number that was set during the manufacturing process.
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER 4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	
Cluster Index	CLUSTER 0 - 7	This value is the same as the cluster number used throughout these tables.
Cluster IP address for the TSSC	CLUSTER 0:	
	CLUSTER 1:	
	CLUSTER 2:	
	CLUSTER 3:	
	CLUSTER 4:	
	CLUSTER 5:	
	CLUSTER 6:	
	CLUSTER 7:	
Internal network type		For a new TS7700, the Internal network type is SMC.

Table 76. TS7700 Customer Network Configuration Information Table and Notes

Field	Value	Notes
Dead Gateway Detection	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	Select either **Enable** or **Disable**.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Customer IP 1 (Virtual)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	**Used For**: TS7700 web Management Interface **Note:** This number is a virtual IP that is not associated with a physical cable. It communicates through the Primary IP, and automatically fails over to the Alternate IP when required. 1 Gbps can use CAT 5e or CAT 6. 10 Gbps need CAT 6.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Customer IP 2 (Primary)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	This is the IP address that is used to connect to the TS7700 through the internal primary network. This IP address should not be used by the customer unless the Virtual IP is inaccessible. **Note:** On a V07/VEB Customer IPs are capable of 1000 MB/s. 1 Gbps can use CAT 5e or CAT 6. 10 Gbps need CAT 6.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Customer IP 3 (Alternate)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	This is the IP address that is used to connect to the TS7700 through the internal alternate network. This IP address should not be used by the customer unless the Virtual IP is inaccessible. **Note:** On a V07/VEB Customer IPs are capable of 1000 MB/s. 1 Gbps can use CAT 5e or CAT 6. 10 Gbps need CAT 6.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Customer Gateway	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	This is used with the virtual, primary, and alternate customer IP addresses.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 76. TS7700 Customer Network Configuration Information Table and Notes (continued)

Field	Value	Notes
Customer Subnet Mask	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	This is used with the virtual, primary, and alternate customer IP addresses.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Customer Network Speed/Duplex Setting		This is the network setting the customer wants to use for their customer interface. The default value is Auto-Negotiate. The customer can specify one of the following values: • Auto-Negotiate • 100 Full Duplex • 100 Half Duplex • 10 Full Duplex • 10 Half Duplex
Customer Library IP	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
3957-Vxx IP address on the TSSC Network	172.31.1.xx	This is the recommended IP address for the first TS7700 attached to a TSSC. The last octet of this IP address must be in an increment of 10 between 10 and 240 (that is, 10, 20 ... 230, 240). The TS7700 switch configuration uses this and the following 9 IP addresses (example: .150 - .159) so no other device should be set to an IP address in this range.
NTP server IP address (if used). **Using an NTP server is strongly recommended to ensure that all components have consistent time settings.**	_ _ _._ _ _._ _ _._ _ _	**Notes:** • The TCP/IP address you obtain from the customer is either the NTP server at their site (if they maintain one locally), or an internet server. Use of an internet server assumes that the customer allows access to the internet on the NTP services port (TCP/IP port 123). • Only 1 NTP server can be used for the entire Grid and ALL clusters in the Grid need to be able to access that specific NTP server.

TSSC Configuration Information Table and Notes

Table 77. TSSC Configuration Information Table and Notes

Field	Value	Notes
IP address for the External connection that is used for ECC, AOS, and SNMP	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	**Note:** Ethernet Call Home is **required** for FC 2725 (M93p Tiny PC TSSC), but **optional** for older models of TSSC. This is an optional (but strongly recommended) IP address on the customer network that allows the TSSC to Call Home by using a high-speed connection through the customer network to the internet. Ports 443 (https) and 80 (http) on this IP address must be free for outbound traffic through the customer network to the internet. Call Home through an Ethernet connection greatly improves the speed of the data transfer, making the data available to support personnel more quickly. IBM recommends enabling Call Home to improve data collection when a problem occurs. Call Home through an Ethernet connection provides better throughput and lower cost than Call Home through a modem connection. Refer to Table 79 on page 231 for a list that provides the IP addresses that AOS 3.3 needs to get through the firewall. Refer to Table 80 on page 232 for a list that provides the IP addresses that AOS 4.0 needs to get through the firewall. Refer to Table 81 on page 232 for a list that provides the IP addresses that Legacy ECC Broadband Call Home needs to get through the firewall. Refer to Table 82 on page 232 for a list that provides the IP addresses that Edge ECC Broadband Call Home needs to get through the firewall. Refer to Table 83 on page 233 for a list that provides the IP addresses that the Fix Download needs to get through the firewall.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Subnet Mask (for Ethernet Call Home)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	This is the subnet mask that is associated with the IP address (for Ethernet Call Home).
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 77. TSSC Configuration Information Table and Notes (continued)

Field	Value	Notes
Gateway (for Ethernet Call Home)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	This is the gateway that is associated with the IP address (for Ethernet Call Home).
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
DNS (Domain Name Server) IPs	_ _ _._ _ _._ _ _._ _ _ _ _ _._ _ _._ _ _._ _ _ _ _ _._ _ _._ _ _._ _ _ _ _ _._ _ _._ _ _._ _ _ _ _ _._ _ _._ _ _._ _ _	Nearly all networks use Domain Name Servers to convert names (such as www.ibm.com) to numeric IP addresses. Domain Name Servers significantly improve the reliability of AOS connections to the TSSC. Provide numeric IP addresses for Domain Name Servers (at least one is required for DNS functionality, two or more are recommended).
DNS Domain Names	1. ______________________________ 2. ______________________________ 3. ______________________________	Enter the Domain Names. An example is **myServer.CompanyXYZ.com**.

TSSC IP Address Table and Notes

The terms *Master Console* (MC), *System Console* (SC), and *TotalStorage Master Console* (TSMC) might be encountered on the screens used on various products. All of these terms have been used to refer to the *TS3000 system console* (TSSC).

Table 78. TSSC IP Address Table and Notes

Field	Value	Notes
Service Console IP address	172.31.1.1	IP address of the Service Console.
Service Console Hostname	xxxxxx	tssnet1 is the default setting for the Service Console.
3957-Vxx IP address on the Service Console Network	172.31.1.xx	This is the recommended IP address for the first TS7700 attached to a master console. The last octet of this IP address must be in an increment of 10 between 10 and 240 (that is. 10, 20 ... 230, 240). The TS7700 switch configuration will use this and the following 9 IP addresses (example: .150 - .159) so no other device should be set to an IP address in this range.
Subnet Mask on the Service Console Network	255.255.255.0	

TSSC Remote Support Information

Table 79. TSSC AOS version 3.3 and earlier

Hostname	IP address	Port	Description
aos.us.ihost.com	72.15.208.234	80, 8200[1)]	Main AOS Server

Table 79. TSSC AOS version 3.3 and earlier (continued)

Hostname	IP address	Port	Description
aosrelay1.us.ihost.com	72.15.223.60	80, 443, 8200[1)]	Americas Relay
[1)] Port 8200 optional only			

Table 80. TSSC AOS version 4.0

Hostname	IP address	Port	Description
aos.uk.ihost.com	195.171.173.165	443	UK AOS Broker
aoshats.us.ihost.com[1)]	72.15.223.62	443	UK AOS Broker
[1)] Requires a minimum of TSSC code v7.5.3 + "TSSC 7.5.x AOS 4.0 proxy patch"			

Table 81. URL table for Legacy ECC

Hostname	IP address	Port	Description
eccgw01.boulder.ibm.com	207.25.252.197	443	ECC transaction gateway
eccgw02.rochester.ibm.com	129.42.160.51	443	ECC transaction gateway
www.ecurep.ibm.com	192.109.81.20	443	File upload for status reporting and problem reporting.
www6.software.ibm.com	170.225.15.41	443	File upload for status reporting and problem reporting. Proxy to testcase.boulder.ibm.com
www-945.ibm.com	129.42.26.224	443	Problem reporting server v4
www-945.ibm.com	129.42.42.224	443	Problem reporting server v4
www-945.ibm.com	129.42.50.224	443	Problem reporting server v4
www.ibm.com	129.42.56.216	443	Service provider file (CCF) download
www.ibm.com	129.42.58.216	443	Service provider file (CCF) download
www.ibm.com	129.42.60.216	443	Service provider file (CCF) download
www-03.ibm.com	204.146.30.17	443	Service provider file (CCF) download

Table 82. URL table for Edge ECC

Hostname	IP address	Port	Description
esupport.ibm.com	129.42.54.189	443	ECC transaction gateway
esupport.ibm.com	129.42.56.189	443	ECC transaction gateway
esupport.ibm.com	129.42.60.189	443	ECC transaction gateway
www6.software.ibm.com	170.225.15.41	443	File upload of files larger than 250 MB.
Notes: • It is recommended customers open 129.42.0.0/18 for convenience. • The IPs are not pingable. Use the following link to verify a connection: https://esupport.ibm.com/eccedge/gateway/services/projects/ecc/iepd/services/ProblemReport.			

Table 83. URL table for Fix Download

Hostname	IP address	Port	Description
download3.boulder.ibm.com	170.225.15.76	80	Fix Download
download3.mul.ie.ibm.com	129.35.224.114	80	Fix Download
download4.boulder.ibm.com	170.225.15.107	80	Fix Download
download4.mul.ie.ibm.com	129.35.224.107	80	Fix Download
delivery04-bld.dhe.ibm.com	170.225.15.104 129.35.224.104	80	Fix Download
delivery04-mul.dhe.ibm.com	129.35.224.115 170.225.15.115	80	Fix Download
delivery04.dhe.ibm.com	129.35.224.105 170.225.15.105	80	Fix Download

Go to "Managing remote support" on page 320 for important configuration information.

TS7700 Grid local addresses

The following notes apply to Table 84 on page 234.

1. If the TS7700 being installed is a stand-alone machine (not part of a grid configuration), then you should not complete Table 84 on page 234.
2. The Grid interfaces are the network connections between clusters allowing them to automatically remain in sync.
3. IBM strongly recommends that the primary and alternate Grid interfaces be on redundant networks.
4. The TS7700 Management Interface requires connections that use the following TCP/IP ports and settings:
   - Internet Control Message Protocol (ICMP) to gateway for dead gateway detection

     Note: If ICMP has been blocked, then Dead Gateway Detection incorrectly disables all connectivity on the MI network outside the local subnet. To prevent this, disable Dead Gateway Detection from the SMIT menu, IBM TS7700 Maintenance, by selecting **Subsystem Configuration Menus > Customer Network Configuration Menus > Set Customer Network Configuration**.
   - 123: Network Time Protocol (NTP) Time Server (TCP- Transmission Control Protocol / UDP - User Datagram Protocol)
   - 443: Hypertext Transfer Protocol (HTTPS)
   - 80: Hypertext Transfer Protocol (HTTP)
   - 1443: Encryption Key Management (EKM)
   - 3801: Encryption Key Management (EKM)
5. The Grid interfaces require connections using the following TCP/IP ports in both directions for all clusters:
   - 7 Internet Control Message Protocol (ICMP)
   - 9 (Discard service, for bandwidth measuring tools)
   - 123 (Network Time Protocol)
   - 350 (Distributed Library to Distributed Library file transfer)
   - 1415 (WebSphere® message queues Grid to Grid)
   - 1416 (WebSphere message queue HDM to HDM)

- 80: Remote Management Interface (Remote MI)
- 433: Management Interface (MI)

6. The following TCP/IP ports are useful in service scenarios if allowed:
   - 22: SSH
   - 20 and 21: File transfer Protocol (FTP)
7. The TS3000 system console (TSSC) or referred to as Master Console or System Console "external" link is as follows:
   - 80 (Call home)
   - 443 (Call home)
     – Recommended
     – 53: Domain Name Server (DNS)
     – Internet Control Message Protocol (ICMP)
8. The TSSC Grid link is as follows:
   - 80: Automatic Ownership Takeover Manager (AOTM)
     – Recommended
     – 9666 - Internal TSSC network communication protocol
     – 443 - Secure HTTP (outbound broadband call home)
     – Internet Control Message Protocol (ICMP)
     – 22: Secure Shell (ssh)

Table 84. Grid Local Address Table and Notes

Field	**Value**	**Notes**
IP address Primary Grid Interface Port A	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	The Primary Grid Port A Interface is the Ethernet adapter in slot C1 (port 0, top port) of the 3957-Vxx. The Primary Grid Port A Interface at each cluster connect to the Primary Grid Port A Interface at each of the other clusters in the same Grid. **Note:** IBM strongly recommends that the primary and alternate Grid interfaces exist on separate subnets. If the Grid interfaces are directly connected (without using Ethernet switches), then using separate subnets is required.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
IP address Primary Grid Interface Port B (if applicable)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	The Primary Grid Port B Interface is the Ethernet adapter in slot C1 (port 1, bottom port) of the 3957-Vxx. The Primary Grid Port B Interface at each cluster connect to the Primary Grid Port B Interface at each of the other clusters in the same grid.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 84. Grid Local Address Table and Notes (continued)

Field	Value	Notes
Primary Grid Port A Network Mask	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Primary Grid Port B Network Mask (if applicable)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Primary Grid Port A Gateway	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	If a Gateway is not used, leave this field blank. If using a direct connection (without Ethernet switches), you must not specify a Gateway. Primary Grid Interface Port A: _ _ _._ _ _._ _ _._ _ _
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Primary Grid Port B Gateway (if applicable)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	If a Gateway is not used, leave this field blank. If using a direct connection (without Ethernet switches), you must not specify a Gateway. Primary Grid Interface Port B: _ _ _._ _ _._ _ _._ _ _
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 84. Grid Local Address Table and Notes (continued)

Field	Value	Notes
IP address Alternate Grid Interface Port A	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	The Alternate Grid Port A Interface is the Ethernet adapter in slot C1 (port 0, top port) of the 3957-Vxx. The Alternate Grid Port A Interface at each cluster connect to the Alternate Grid port A Interface at each of the other clusters in the same grid. **Note:** IBM strongly recommends that the primary and alternate Grid interfaces exist on separate subnets. If the Grid interfaces are directly connected (without using Ethernet switches), then using separate subnets is required.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
IP address Alternate Grid Interface Port B (if applicable)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	The Alternate Grid Interface Port B is the Ethernet adapter in slot C1 (port 1, bottom port) of the 3957-Vxx. The Alternate Grid Port B Interface at each cluster connect to the Alternate Grid Port B Interface at each of the other clusters in the same grid.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Alternate Grid Port A Network Mask	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Alternate Grid Port B Network Mask (if applicable)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 84. Grid Local Address Table and Notes (continued)

Field	Value	Notes
Alternate Grid Port A Gateway	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	If a Gateway is not used, leave this field blank. If using a direct connection (without Ethernet switches) you must not specify a Gateway. Alternate Grid Interface Port A: _ _ _._ _ _._ _ _._ _ _
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Alternate Grid Port B Gateway (if applicable)	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	If a Gateway is not used, leave this field blank. If using a direct connection (without Ethernet switches) you must not specify a Gateway. Alternate Grid Interface Port B: _ _ _._ _ _._ _ _._ _ _
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Customers can use Table 85 or one similar to it to summarize Grid Local Address information.

Note: Virtual Local Area Network (VLAN) and Classless Inter-Domain Routing (CIDR) listed in Table 85 are optional.

Table 85. Summary Table

Name: __________ **CL__**					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					
Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					
Primary Grid Port A Interface					
Alternate Grid Port A Interface					
Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					

Table 85. Summary Table (continued)

Name: __________ CL__					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					
Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					
Primary Grid Port A Interface					
Alternate Grid Port A Interface					
Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					
Name: __________ CL__					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					
Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					
Primary Grid Port A Interface					
Alternate Grid Port A Interface					
Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					
Name: __________ CL__					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					

Table 85. Summary Table (continued)

Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					
Primary Grid Port A Interface					
Alternate Grid Port A Interface					
Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					
Name: __________ CL__					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					
Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					
Primary Grid Port A Interface					
Alternate Grid Port A Interface					
Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					
Name: __________ CL__					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					
Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					

Table 85. Summary Table (continued)

Primary Grid Port A Interface					
Alternate Grid Port A Interface					
Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					
Name: __________ CL__					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					
Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					
Primary Grid Port A Interface					
Alternate Grid Port A Interface					
Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					
Name: __________ CL__					
Description	**IP Address**	**Gateway**	**Subnet Mask**	**VLAN**	**CIDR**
Customer IP 1 (Virtual)					
Customer IP 2 (Primary)					
Customer IP 3 (Alternate)					
Ethernet Call Home					
Primary Grid Port A Interface					
Alternate Grid Port A Interface					

Table 85. Summary Table (continued)

Primary Grid Port B Interface (if applicable)					
Alternate Grid Port B Interface (if applicable)					

TSSC Grid Configuration Information Table and Notes

The following notes apply to Table 86.

- If the TS7700 you are installing is a stand-alone machine (not part of a grid configuration) then leave Table 86 blank.
- If no host attachment is available on a cluster, Autonomic Ownership Takeover Manager (AOTM) does not need to be set up. However, it is recommended that AOTM remains set up so that it is available if host attachment is ever made. Leave Table 86 blank.
- If the Autonomic Ownership Takeover Manager (AOTM) will not be used, then leave Table 86 blank.
- Refer to "Ownership takeover" on page 281 and "The Autonomic Ownership Takeover Manager" on page 282 for more information on AOTM before you continue. Do **NOT** attempt to configure AOTM. Use these sections to make an informed decision whether to use AOTM.
- The TSSC grid interface is only used for AOTM.
- Each cluster can be configured to use AOTM to provide ownership takeover for one cluster.
- The AOTM requires the following TCP/IP ports: 7 (Ping), 80 (HTTP) open.

Table 86. TSSC Grid Configuration Information Table and Notes

Field	Value	Notes
TSSC Grid Interface IP Address	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	The TSSC Grid Interface is used to allow the TSSC at one cluster to communicate with the TSSC(s) at other cluster(s) in the same Grid network.
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
TSSC Grid Interface Subnet Mask	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	

Table 86. TSSC Grid Configuration Information Table and Notes (continued)

Field	Value	Notes
TSSC Grid Interface Gateway	CLUSTER 0: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 1: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 2: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 3: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 4: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 5: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 6: _ _ _._ _ _._ _ _._ _ _	
	CLUSTER 7: _ _ _._ _ _._ _ _._ _ _	
Takeover Mode - Select One	DISABLED:	The Takeover Modes are DISABLED, Read Ownership Takeover (ROT), or Write Ownership Takeover (WOT). When DISABLED, no auto takeover is allowed. ROT allows only the local cluster to read but not write to volumes to the remote cluster. WOT allows the local cluster to read OR write to any volumes it takes over from the remote cluster. ROT is recommended because it automatically gives you read access to any consistent copies of data without any requirement for manual intervention during reconciliation after the failed cluster is repaired. WOT is appropriate if your application must be able to update existing logical volumes, but it can cause different copies of a logical volume to be inconsistent, requiring manual intervention during reconciliation after the failed cluster is repaired.
	ROT:	
	WOT:	
Grace Period (Minutes)		When a cluster detects that another cluster in the same grid has failed, it waits for the number of minutes specified as the Grace Period before it attempts to take over the volumes of the failed cluster. A typical Grace Period is 25 minutes. In most cases, this is the same for both clusters.
Retry Period (Minutes)		The retry period is the number of minutes between attempts to take over ownership of the volumes that are associated with a failed cluster. A typical Retry Period is 5 minutes. In most cases, this is the same for both clusters.

Related information

"Post-installation tasks" on page 243

Post-installation tasks

If you are a customer, use the checklist in this section to prepare your TS7700 for use after installation.

__ 1. Define data ranges, categories, and policies.

If your IBM System Service Representative (SSR) has installed your TS7700, perform the following definitions at the TS7700 Management Interface:

Note: Links to all related topics are collected in the **Related information** section.

__ a. Define stacked volume ranges.

Refer to the topic Define VOLSER ranges for physical volumes, and the management interface help topic Physical volume ranges, for more information.

__ b. Define scratch categories.

Refer to the topic Categories, and the associated management interface help topic Categories, for more information.

Note: The scratch category number you define is the same value as defined for MEDIA1 or MEDIA2, as specified in the DEVSUPxx PARMLIB number.

__ c. Define the expired virtual volume data policy.

Refer to the topic Define virtual volume expiration time and the management interface help topic Categories, for more information.

__ d. Define the following TS7700 management policies:

- Inhibit reclaim schedule

  Note: Prior to microcode level 8.5.0.xx, inhibit reclaim schedules were designated by using local time instead of Coordinated Universal Time (UTC). If you have upgraded from a microcode level of 8.4.0.xx, verify that your inhibit reclaim schedule displays the correct day and time before you start an inhibit reclaim operation using the new code version.
- Reclaim threshold percentage

Refer to the topic Physical volumes and the management interface help topics Inhibit reclaim schedules and Active data distribution, for more information.

__ 2. Enable the Advanced Library Management System (ALMS). Refer to *Enabling the Advanced Library Management System* in the IBM TS3500 Customer documentation or IBM TS4500 Customer documentation in IBM Knowledge Center.

__ 3. Configure the TS3500 or TS4500 Tape Library logical library for TS7700 attachment. Refer to the topic Configuring the TS3500 or TS4500 Tape Library logical library, for more information.

__ 4. If stacked volume media are available, insert the physical volumes by using one of the following methods:

- Open the library doors and directly insert the volumes into tape library storage cells
- Use the TS3500 or TS4500 Tape Library I/O station

Note: Inserted media must be uninitialized, labeled with an IBM Standard Label, or contain a tapemark at the beginning of tape.

__ 5. Create TCDB. Refer to *z/OS DFSMS Object Access Method Planning, Installation, and Storage Administration Guide* for instructions to create TCDB as part of the tape library support installation. This publication can be accessed from the web link in the **Related information** section.

__ 6. Insert virtual volumes

__ 7. If using Native LDAP, create a Direct LDAP policy for use by IBM service representatives. Refer to the topic Native LDAP in the **Related information** section for additional instructions.

__ 8. The TS7700 is now ready for use.

Tip: For help in navigating the ISMF screens, and for detailed information pertaining to the defining of the DFSMS constructs, refer to the following publications, available from the web link in the **Related information** section:

- *IBM TotalStorage 3494 Tape Library: A Practical Guide to Tape Drives and Tape Automation*, SG24-46322
- *z/OS DFSMSdfp Storage Administrator Reference*,

Related information

"Native LDAP using MSAD" on page 301

"z/OS I/O definitions" on page 84

http://www.ibm.com/support/us/en/

Define VOLSER ranges for physical volumes

This topic provides instructions to define VOLSER ranges for physical volumes.

When a cartridge is assigned to a partition, the TS7700 uses the VOLSER ranges defined in its VOLSER Range table to direct the cartridge to the proper partition and assigns to it the proper category. Best practices recommend defining the proper policies in the VOLSER Range table before inserting the cartridges into the tape library.

Important:

- When using a TS3500 or TS4500 Tape Library, you must assign VOLSER ranges (called Cartridge Assignment Policies (CAP) on the TS3500) at the library hardware level before using the library with IBM Z® hosts.
- When using a TS3500 or TS4500 Tape Library, the native physical volume ranges must fall within the ranges assigned to IBM Z® host logical libraries.
- The policies for the IBM Z® host cartridge ranges must match any host tape management policies.

Use the following panels of the TS7700 management interface to manage physical volume ranges or unassigned physical volumes in a library attached to a TS7700.

- *Physical volume ranges*

  Use this panel to view a range or ranges of physical volumes recently added to an attached physical library. The **Physical Volume Ranges** table displays the list of defined VOLSER ranges for a given cluster
- *Add physical volume range*

  Use this panel to add a range of unassigned physical volumes to a library attached to a TS7700.

Note: The VOLSER ranges you define on the TS3500 or TS4500 Tape Library apply to physical cartridges only. You should not define VOLSER ranges for virtual volumes for a TS7700. You must define virtual volumes through the TS7700 management interface.

- *Modify physical volume range*

  Use this panel to modify a range of unassigned physical volumes in a library attached to a TS7700.
- *Confirm delete physical volume range*

  Use this page to delete a range of unassigned physical volumes in a library attached to a TS7700.
- *Eject unassigned physical volume*

  Use this page to eject unassigned physical volumes from a library attached to a TS7700.

For the TS7700, no additional definitions are required at the hardware level other than setting up the proper VOLSER ranges at the TS3500 or TS4500 Tape Library.

Notelist:
- If a physical volume's VOLSER occurs within a defined range, that volume, upon being inserted, can be inventoried according to its VOLSER definition. If the physical volume's VOLSER occurs outside a defined range, user intervention is required to assign the inserted physical volume to TS7700 resources.
- Although you could now enter cartridges into the TS3500 or TS4500 Tape Library, best practices recommend that you complete the required definitions at the host, as defined in the topic *Post-installation tasks* before you insert any physical cartridges.

Related information

"Post-installation tasks" on page 243

Define Fast Ready scratch categories

This topic provides instructions to define Fast Ready scratch categories.

The Fast Ready scratch attribute allows you to take advantage of the scratch mount performance of the TS7700 when defined on categories used by the host for scratch volumes. When defined, it also prevents recalls for scratch mounts. The MOUNT FROM CATEGORY command, as used for scratch mounts, is not exclusively used for scratch mounts; therefore, the TS7700 cannot assume that any MOUNT FROM CATEGORY is for a scratch volume. The Fast Ready scratch attribute provides a definition of a category to supply scratch mounts. The Fast Ready definition is achieved by using the Categories panel on the TS7700 Management Interface.

The actual category hexadecimal number depends on the software environment (for z/OS) and on the definitions in the SYS1.PARMLIB member DEVSUPxx for library partitioning. Also, the DEVSUPxx member must be referenced in IEASYSxx to be activated.

Note: Any category up to and including the X'FEFF' may be overridden in DEVSUPxx, but be aware that categories may only be overridden if the TS7700 will not be accessed by the owning operating systems
When defining a Fast Ready scratch category, you can also set up an expire time and further define the expire time as an expire hold time.

Note: Best practices recommend that you add a comment to DEVSUPnn to ensure that the Fast Ready scratch categories are updated whenever the category values in DEVSUPnn are changed. They need to be in sync at all times.

Define virtual volume expiration time

This topic provides instructions to define virtual volume expiration time.

Use the Categories panel on the TS7700 Management Interface to define the virtual volume expiration time. If the Delete Expired Volume Data setting is not used, virtual volumes occupy space on the physical volumes even after they have been returned to scratch. In that case, only when a virtual volume is rewritten is the old data that is released to reduce the amount of active data on the physical volume. With the Delete Expired Volume Data setting, the data that is associated with volumes that have been returned to scratch are deleted after a time period and their old data released.

For example, assume that you have 20 000 virtual volumes in scratch status at any point in time, that the average amount of data on a virtual volume is 400 MB, and that the data compresses at a 2:1 ratio. The space that is occupied by the data on those scratch volumes is 4 000 000 MB or the equivalent of 14 (fourteen) 3592 JA cartridges. By using the Delete Expired Volume Data setting, you could reduce the number of cartridges required in this example by 14.

The parameter Expire Time specifies the amount of time in hours, days, or years. The data continues to be managed by the TS7700 after a virtual volume is returned to scratch before the data that is associated with the virtual volume is deleted. A minimum of 1 hour and a maximum of 2,147,483,647 hours (approximately 244,983 years) can be specified. Specifying a value of zero means that the data that is associated with the volume is to be managed as it was before the addition of this option. This means that it is never deleted. In essence, specifying a value (other than zero) provides a "grace period" from when the virtual volume is returned to scratch until its associated data is eligible for deletion. A separate Expire Time can be set for each category defined as scratch.

Configuring the TS3500 or TS4500 Tape Library logical library

This topic provides instructions to configure a TS3500 or TS4500 Tape Library logical library for TS7700 attachment.

Complete the following items to configure a logical library.

__ 1. Set the maximum number of cartridges for the logical library.
   - For TS4500, refer to *Modifying the maximum cartridges for a logical library* in the IBM TS4500 Customer documentation in IBM Knowledge Center.
   - For TS3500, refer to *Changing the maximum allowable quantity of cartridges in a logical library* in the IBM TS3500 Customer documentation in IBM Knowledge Center.

__ 2. Set the maximum number of virtual I/O slots.
   - For TS4500, refer to *Performing other logical library tasks from the CLI* and *setMaximumVIOCartridges* in the IBM TS4500 Customer documentation in IBM Knowledge Center.
   - For TS3500, refer to *Changing the quantity of virtual I/O slots in a logical library* in the IBM TS3500 Customer documentation in IBM Knowledge Center.

__ 3. Assign drives to the logical library.

- For TS4500, refer to *Assigning and unassigning tape drives to a logical library* in the IBM TS4500 Customer documentation in IBM Knowledge Center.
- For TS3500, refer to *Adding a drive to a logical library* in the IBM TS3500 Customer documentation in IBM Knowledge Center.

__ 4. Assign control paths to the logical library.
- For TS4500, refer to *Using control path drives* in the IBM TS4500 Customer documentation in IBM Knowledge Center.
- For TS3500, refer to *Enabling or disabling a control path in a logical library* in the IBM TS3500 Customer documentation in IBM Knowledge Center.

__ 5. Set the Cartridge Assignment Policy.
- For TS4500, refer to *Assigning or unassigning cartridges* in the IBM TS4500 Customer documentation in IBM Knowledge Center.
- For TS3500, refer to *Working with a cartridge assignment policy* in the IBM TS3500 Customer documentation in IBM Knowledge Center.

__ 6. Set Encryption method if necessary.
- For TS4500, refer to *Choosing or modifying an encryption method* in the IBM TS4500 Customer documentation in IBM Knowledge Center.
- For TS3500, refer to *Setting up and using encryption* in the IBM TS3500 Customer documentation in IBM Knowledge Center.

__ 7. Verify that Exports is set to Show (default setting).
- For TS4500, refer to *Logical library commands* and *showQueuedExports* in the IBM TS4500 Customer documentation in IBM Knowledge Center.
- For TS3500, refer to *Hiding a host application's view of cartridges that have been queued for export* and *Removing data cartridges when virtual I/O slots are enabled* in the IBM TS3500 Customer documentation in IBM Knowledge Center.

Chapter 3. Configuring

This section provides topics about configuring the TS7700.

TS7700 configurations

The TS7700 is configured as a cluster and clusters can be combined in a TS7700 Grid.

TS7700 Cluster

The TS7700 cluster combines the TS7700 with a disk subsystem cache.

The architecture allows more disks or nodes to be added in the future to expand the capabilities of the system. A cluster provides FICON host attachment and up to 496 virtual tape device addresses. In the IBM TS7740 configuration, the cluster includes the disk cache and that part of the tape library assigned to the TS7700.

Related information

"TS7700 Grid" on page 257

"TS7700 system component details" on page 33

"Tape library attachments, drives, and media" on page 52

"Tape drives" on page 53

"Tape media" on page 58

Disk-only TS7760 Cluster

The disk-only TS7760 Cluster provides a disk-only TS7760 virtual tape subsystem.

A disk-only TS7760 Cluster typically consists of:

FICON connections to the host

The following configurations are supported:

- 2 FICON adapters
- 4 FICON adapters

Note: FICON adapters can be upgraded in number (two to four) and kind (shortwave to longwave) by using:

- "FC 3402, 16 Gb FICON Short Wavelength Attachment" on page 156
- "FC 3403, 16 Gb FICON Long Wavelength Attachment" on page 157

OR

- "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157
- "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157

Up to 8 FICON channels can be configured. No intermixing of 8 Gb and 16 Gb FICON adapters is allowed.

The TS7760

Consisting of:

A 3952 Tape Frame

The 3952 Tape Frame is the frame that encloses the TS7760.

A TS7760 can also be attached to up to two more 3952 Tape Frames that are identified as TS7700 Storage Expansion Frames by using "FC 7334, TS7700 Encryption-capable expansion frame" on page 175. Refer to the topic *TS7760 Storage Expansion Frame* in the **Related information** section for TS7760 Storage Expansion Frame configuration options.

A 3957-VEC

A TS7760 Cache subsystem

A TS7760 Cache subsystem consists of:

- A TS7760 Cache Controller (3956-CSA)
- Up to nine TS7760 Cache Drawers (3956-XSA)

A base TS7760 Cache can be expanded by adding a TS7700 Storage Expansion Frame by using "FC 7334, TS7700 Encryption-capable expansion frame" on page 175 and "FC 9323 Expansion frame attachment" on page 179. Refer to the topic *TS7760 Storage Expansion Frame* in the **Related information** section for TS7760 Storage Expansion Frame configuration options.

Note: An existing TS7760 Cache operating a microcode level of 8.7.0.xx or later can be upgraded by MES to include a TS7760 Storage Expansion Frame. Refer to the topic *Upgrades specific to the TS7760* in the **Related information** section for requirements.

Related information

"System requirements" on page 63

"TS7760 Storage Expansion Frame" on page 39

"Upgrades for the TS7760" on page 113

"TS7760 Tape Attach Cluster"

TS7760 Tape Attach Cluster

The TS7760 Tape Attach Cluster combines the TS7700 with a tape library to form a virtual tape subsystem.

A TS7760 Tape Attach Cluster typically consists of:

FICON connections to the host

The following configurations are supported:

- 2 FICON adapters
- 4 FICON adapters

Note: FICON adapters can be upgraded in number (two to four) and kind (shortwave to longwave) by using:

- "FC 3402, 16 Gb FICON Short Wavelength Attachment" on page 156
- "FC 3403, 16 Gb FICON Long Wavelength Attachment" on page 157

OR

- "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157
- "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157

Up to 8 FICON channels can be configured. No intermixing of 8 Gb and 16 Gb FICON adapters is allowed.

The TS7760

Consisting of:

A 3952 Tape Frame
The 3952 Tape Frame is the frame that encloses the TS7760.

A TS7760 can also be attached to up to two more 3952 Tape Frames, which are identified as TS7700 Storage Expansion Frames by using "FC 7334, TS7700 Encryption-capable expansion frame" on page 175. Refer to the topic *TS7760 Storage Expansion Frame* in the **Related information** section for TS7760 Storage Expansion Frame configuration options.

A 3957-VEC

A TS7760 Cache subsystem
A TS7760 Cache subsystem consists of:

- A TS7760 Cache Controller (3956-CSA)
- Up to nine TS7760 Cache Drawers (3956-XSA)

A base TS7760 Cache can be expanded by adding a TS7700 Storage Expansion Frame by using "FC 7334, TS7700 Encryption-capable expansion frame" on page 175 and "FC 9323 Expansion frame attachment" on page 179. Refer to the topic *TS7760 Storage Expansion Frame* in the **Related information** section for TS7760 Storage Expansion Frame configuration options.

Note: An existing TS7760 Cache operating a microcode level of 8.7.0.xx or later can be upgraded by MES to include a TS7760 Storage Expansion Frame. Refer to the topic *Upgrades specific to the TS7760* in the **Related information** section for requirements.

A TS3500 or TS4500 Tape Library
The TS3500 Tape Library contains:

Tape drives
The TS7700 tape attach supports a minimum of four and a maximum of 16 tape drives. When connected to a TS3500 Tape Library, 16 tape drives (TS1150, TS1140, TS1130, TS1120, or 3592 J1A) can be used, though at least two TS3500 Tape Library frames are required. The TS1150 tape drives can be mixed with one other 3592 tape drive type but the total count cannot exceed 16.

Tape cartridges
The tape cartridges can contain data for multiple virtual volumes and are sometimes referred to as physical stacked volumes.

The TS4500 Tape Library contains:

Tape drives
The TS7700 supports a minimum of four and a maximum of 16 tape drives. When connected to a TS4500 Tape Library, 16 tape drives (TS1150, TS1140) can be used, though at least two TS4500 Tape Library frames are required.

Tape cartridges
The tape cartridges can contain data for multiple virtual volumes and are sometimes referred to as physical stacked volumes.

Important:

A TS7700 tape-attach cluster that is attached to a TS3500 or TS4500 Tape Library can be used in a grid configuration. Each TS7700 tape-attach cluster in a grid can be attached to a separate physical library, or the clusters can share the same physical library.

However, sharing a physical library is not recommended and does not conform to best practices. A single library in a grid configuration limits overall performance since systems in the same grid are busy during the same batch windows. Furthermore, mount requests occur during these same peak demand times, limiting performance. A single library in a grid configuration also negates the advantage of independent and redundant subsystems for high availability. The redundancy available on the TS3500 or TS4500 Tape Library (dual accessors, dual grippers, dual power, and the like) can help to mitigate this increased risk, but is still not considered the best practice.

Related information

"System requirements" on page 63

"TS7760 Storage Expansion Frame" on page 39

"Upgrades for the TS7760" on page 113

Disk-only TS7720 Cluster

The disk-only TS7720 Cluster provides a disk-only TS7700 virtual tape subsystem.

A disk-only TS7720 Cluster typically consists of:

FICON connections to the host

The following configurations are supported:
- 2 FICON adapters
- 4 FICON adapters

Note: FICON adapters can be upgraded in number (two to four) and kind (shortwave to longwave) by using:
- "FC 3441, FICON short-wavelength attachment" on page 158
- "FC 3442, FICON long-wavelength attachment" on page 158
- "FC 3443, FICON 10-km long-wavelength attachment" on page 158
- "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157
- "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157

Up to 8 FICON channels can be configured.

The TS7720

Consisting of:

A 3952 Tape Frame

The 3952 Tape Frame is the frame that encloses the TS7720 .

A TS7720 can also be attached to up to two more 3952 Tape Frames that are identified as TS7720 Storage Expansion Frames by using "FC 7323, TS7720 Storage expansion frame" on page 174. Refer to the topic *TS7720 Storage Expansion Frame* in the **Related information** section for TS7720 Storage Expansion Frame configuration options.

A 3957-VEB

A TS7720 Cache subsystem

A TS7720 Cache subsystem consists of:
- A TS7720 Cache Controller (3956-CS9)

- Up to nine TS7720 Cache Drawers (3956-XS9)

A base TS7720 Cache can be expanded by adding a TS7720 Storage Expansion Frame by using "FC 7323, TS7720 Storage expansion frame" on page 174 and "FC 9323 Expansion frame attachment" on page 179. Refer to the topic *TS7720 Storage Expansion Frame* in the **Related information** section for TS7720 Storage Expansion Frame configuration options.

Note: An existing TS7720 Cache operating a microcode level of 8.7.0.xx or later can be upgraded by MES to include a TS7720 Storage Expansion Frame. Refer to the topic *Upgrades specific to the TS7720* in the **Related information** section for requirements.

Related information

"System requirements" on page 63

"TS7720 Storage Expansion Frame" on page 45

"Upgrades for the TS7720 " on page 116

"Disk-only TS7720 Cluster" on page 252

TS7720 Tape Attach Cluster

The TS7720 Tape Attach Cluster combines the TS7700 with a tape library to form a virtual tape subsystem.

A TS7720 Tape Attach Cluster typically consists of:

FICON connections to the host

The following configurations are supported:

- 2 FICON adapters
- 4 FICON adapters

Note: FICON adapters can be upgraded in number (two to four) and kind (shortwave to longwave) by using:

- "FC 3441, FICON short-wavelength attachment" on page 158
- "FC 3442, FICON long-wavelength attachment" on page 158
- "FC 3443, FICON 10-km long-wavelength attachment" on page 158
- "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157
- "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157

Up to 8 FICON channels can be configured.

The TS7720

Consisting of:

A 3952 Tape Frame

The 3952 Tape Frame is the frame that encloses the TS7720 .

A TS7720 can also be attached to up to two more 3952 Tape Frames, that are identified as TS7720 Storage Expansion Frames by using "FC 7323, TS7720 Storage expansion frame" on page 174. Refer to the topic *TS7720 Storage Expansion Frame* in the **Related information** section for TS7720 Storage Expansion Frame configuration options.

A 3957-VEB

A TS7720 Cache subsystem

A TS7720 Cache subsystem consists of:

- A TS7720 Cache Controller (3956-CS9)
- Up to nine TS7720 Cache Drawers (3956-XS9)

A base TS7720 Cache can be expanded by adding a TS7720 Storage Expansion Frame by using "FC 7323, TS7720 Storage expansion frame" on page 174 and "FC 9323 Expansion frame attachment" on page 179. Refer to the topic *TS7720 Storage Expansion Frame* in the **Related information** section for TS7720 Storage Expansion Frame configuration options.

Note: An existing TS7720 Cache operating a microcode level of 8.7.0.xx or later can be upgraded by MES to include a TS7720 Storage Expansion Frame. Refer to the topic *Upgrades specific to the TS7720* in the **Related information** section for requirements.

A TS3500 or TS4500 Tape Library

The TS3500 Tape Library contains:

Tape drives

The TS7720 tape attach supports a minimum of four and a maximum of 16 tape drives. When connected to a TS3500 Tape Library, 16 tape drives (TS1150, TS1140, TS1130, TS1120, or 3592 J1A) can be used, though at least two TS3500 Tape Library frames are required. The TS1150 tape drives can be mixed with one other 3592 tape drive type but the total count cannot exceed 16.

Tape cartridges

The tape cartridges can contain data for multiple virtual volumes and are sometimes referred to as physical stacked volumes.

The TS4500 Tape Library contains:

Tape drives

The TS7700 supports a minimum of four and a maximum of 16 tape drives. If connected to a TS4500 Tape Library, 16 tape drives (TS1150, TS1140) can be used, though at least two TS4500 Tape Library frames are required.

Tape cartridges

The tape cartridges can contain data for multiple virtual volumes and are sometimes referred to as physical stacked volumes.

Important:

A TS7700 tape-attach cluster that is attached to a TS3500 or TS4500 Tape Library can be used in a grid configuration. Each TS7700 tape-attach cluster in a grid can be attached to a separate physical library, or the clusters can share the same physical library.

However, sharing a physical library is not recommended and does not conform to best practices. A single library in a grid configuration limits overall performance since systems in the same grid are busy during the same batch windows. Furthermore, mount requests occur during these same peak demand times, limiting performance. A single library in a grid configuration also negates the advantage of independent and redundant subsystems for high availability. The redundancy available on the TS3500 or TS4500 Tape Library (dual accessors, dual grippers, dual power, and the like) can help to mitigate this increased risk, but is still not considered the best practice.

Related information

"System requirements" on page 63

"TS7720 Storage Expansion Frame" on page 45

"Upgrades for the TS7720 " on page 116

TS7740 Cluster

The TS7740 Cluster combines the TS7700 with a tape library to form a virtual tape subsystem.

A TS7740 Cluster typically consists of:

FICON connections to the host

The following configurations are supported:

- 2 FICON adapters
- 4 FICON adapters

Note: FICON adapters can be upgraded in number (two to four) and kind (shortwave to longwave) by using:

- "FC 3441, FICON short-wavelength attachment" on page 158
- "FC 3442, FICON long-wavelength attachment" on page 158
- "FC 3443, FICON 10-km long-wavelength attachment" on page 158
- "FC 3438, 8 Gb FICON Short Wavelength Attachment" on page 157
- "FC 3439, 8 Gb FICON Long Wavelength Attachment" on page 157

Up to 8 FICON channels can be configured.

The TS7740

Consisting of:

A 3952 Tape Frame

A or 3957-V07

A TS7740 Cache subsystem

A TS7740 Cache subsystem consists of:

- One TS7740 Cache Controller with no attached TS7740 Cache Drawer (single-drawer cache configuration).
- One TS7740 Cache Controller attached to one TS7740 Cache Drawer (two-drawer cache configuration).
- One TS7740 Cache Controller attached to two TS7740 Cache Drawers (three-drawer cache configuration).

Important: A field-installable upgrade (MES) is available for TS7740 cache configurations. An existing one-drawer TS7740 cache configuration can be upgraded to a two-drawer TS7740 cache configuration. An existing two-drawer TS7740 cache configuration can be upgraded to a three-drawer TS7740 cache configuration. No MES is available to upgrade an existing one-drawer TS7740 cache configuration directly to a three-drawer TS7740 cache configuration. A one-drawer cache configuration must be upgraded to a two-drawer cache configuration before an upgrade to a three-drawer cache configuration can occur. For more information, see "FC 5642, Field installation of 3956-CX7" on page 167 and "FC 9355, Field merge" on page 180.

A TS3500 or TS4500 Tape Library

The TS3500 Tape Library contains:

Tape drives

The TS7700 supports a minimum of four and a maximum of 16 tape drives. If connected to a TS3500 Tape Library, 16 tape drives (TS1150, TS1140, TS1130, TS1120, or 3592 J1A) can be used, though at least two TS3500 Tape Library frames are required. The TS1150 tape drives can be mixed with one other 3592 tape drive type but the total count cannot exceed 16.

If the TS7700 is connected to a 3494 Tape Library, 12 is the maximum number of tape drives that can be used. The 3494 Tape Library supports only a single-frame option. Each 3494 Tape Library tape frame can contain only 12 drives. It is not required that the tape drives be housed in only two frames. If desired, tape drives can be spread across many frames in the library.

Tape cartridges

The tape cartridges can contain data for multiple virtual volumes and are sometimes referred to as physical stacked volumes.

The TS4500 Tape Library contains:

Tape drives

The TS7700 supports a minimum of four and a maximum of 16 tape drives. If connected to a TS4500 Tape Library, 16 tape drives (TS1150, TS1140) can be used, though at least two TS4500 Tape Library frames are required.

Tape cartridges

The tape cartridges can contain data for multiple virtual volumes and are sometimes referred to as physical stacked volumes.

Important: A TS7700 attached to a TS3500 or TS4500 Tape Library can be used in a grid configuration. Each TS7700 in a grid can be attached to a separate physical library, or to the same physical library. Each TS7740 that connects to the same physical library must operate a microcode level of 8.4.0.xx or earlier and each must attach to its own 3953 Library Manager. However, sharing a physical library is not recommended and does not conform to best practices. A single library in a grid configuration limits overall performance since systems in the same grid are busy during the same batch windows. Furthermore, mount requests occur during these same peak demand times, limiting performance. A single library in a grid configuration also negates the advantage of independent and redundant subsystems for high availability. The redundancy available on the 3584 Tape Library (dual accessors, dual grippers, dual power, and the like) can help to mitigate this increased risk, but is still not considered the best practice.

Related information

"TS7700 Grid" on page 257

"TS7700 system component details" on page 33

"Tape library attachments, drives, and media" on page 52

"Tape drives" on page 53

"Tape media" on page 58

TS7700 Grid

A TS7700 Grid refers to two or more physically separate TS7700 Clusters connected to one another by using a customer-supplied Internet Protocol network. A TS7700 Grid can contain disk-only clusters that do not attach to a physical tape library, clusters that do attach to a physical tape library, or a combination of both.

The TCP/IP infrastructure that connects a TS7700 Grid is known as the *Grid Network*. The grid configuration is used to form a disaster recovery solution and provide remote virtual volume replication. The term *grid* refers to the code and functionality that provides replication and management of virtual volumes and their attributes in cluster configurations. A Grid can be used to form disaster recovery and high availability solutions. A disaster recovery solution is achieved when multiple clusters are geographically distant from one another. A high availability solution is achieved when multiple clusters are in close proximity to one another.

The clusters in a TS7700 Grid can, but do not need to be, geographically dispersed. In a multiple-cluster grid configuration, two clusters are often located within 100 km of one another, while the remaining clusters can be located more than 1,000 km away. This provides both a highly available and redundant regional solution while also providing a remote disaster recovery solution outside of the region. Any TS7700 Cluster can also be in relatively distant proximity to one another; discuss this type of configuration with your IBM representative for any planning considerations. Any TS7700 Clusters in relatively close proximity would typically use an immediate mode copy policy. TS7700 Clusters in relatively distant proximity would typically use a deferred mode copy policy.

Refer to Figure 3 on page 18 for an illustration of a typical multi-cluster grid configuration.

Each TS7700 Cluster provides FICON host attachments and between 256 and 496 virtual tape device addresses, depending on the installed features. The clusters in a Grid configuration are connected together through dual 1 Gb Ethernet links. The links use standard 1000 Base-T adapters for CAT-5E or CAT6 (CAT6 is highly recommended) balanced copper cabling or standard shortwave adapters for multimode fiber cable. Each grid Ethernet adapter contains two 1 Gb ports. You can use both ports on each adapter, for four total 1 Gb Ethernet grid links. The same Ethernet links are used for the replication of data between clusters. They pass control information and access between a local cluster's virtual tape device and a virtual volume's data in a remote cluster's TS7700 Cache. For a multiple-site grid Ethernet connection, you have a choice of the following adapters:

1 Gb dual port copper Ethernet
: This adapter is a full duplex, dual ported, Gb Ethernet adapter that can be configured to run each port at 10, 100, or 1000 Mbps data rates. The adapter conforms to the IEEE 802.3ab 1000 Base-T standard.

  Note: Only the primary port can be used for the grid network unless FC 1034, Enable dual port grid connection is installed. Refer to the topic *Feature details* in the **Related information** section for feature code prerequisites and other requirements.

1 Gb Grid dual port optical Ethernet
: This is a dual port adapter that provides 1 Gbps throughput on a standard

shortwave (850 nm) 50/62.5 micron multimode optical cable. It conforms to the IEEE 802.3z standard and supports distances of 260 m for 62.5µ multimode fiber (MMF) and 550 m for 50.0µu MMF.

Note: Only the primary port can be used for the grid network unless FC 1034, Enable dual port grid connection is installed. Refer to the topic *Feature details* in the **Related information** section for feature code prerequisites and other requirements.

1 Gb fiber
This adapter provides 1000 Mbps throughput on a standard shortwave (850 nm) 50/62.5 micron multimode optical cable and conforms to the IEEE 802.3z standard and supports distances of 260 m for 62.5µ multimode fiber (MMF) and 550 m for 50.0µu MMF.

1 Gb optical shortwave
This Ethernet SX adapter has an LC Duplex connector that attaches to 50-micron or 62.5-micron multimode fiber cable. This is a standard SW (850 nm) adapter that conforms to the IEEE 802.3z standards. It supports distances of 2 - 260 meters for 62.5-micron and 2 - 550 meters for 50-micron MMF.

10 Gb Optical longwave
This adapter supports a maximum of 10 kilometers of 1310 nm, 9µm, single-mode fiber optic cable. It conforms to the IEEE 802.3ae standard. This adapter requires 9µm single-mode fiber optic cables and uses an LC connector to connect to network infrastructure components. This adapter must be used with a 3957-VEC, 3957-VEB, or 3957-V07.

Note: Each 1 Gb link requires a unique, customer assigned IP address.
Ethernet activity is specific to each adapter and port pairing. As a result, clusters in a grid do not necessarily all require the same number of ports. Clusters with 10 Gb, four 1 Gb, and two 1 Gb Ethernet connections can be part of the same grid configuration. Use of the second 1 Gb Ethernet port present in both grid Ethernet adapters is supported. This results in availability of four total 1 Gb ports for TS7700 Grid interconnections. This configuration is supported only for microcode levels of 8.20.0.xx and later. It requires two dual-ported adapters and is activated by using FC 1034, Enable dual port grid connection.

You can use Selective Device Access Control to tune the use of grid links. For more information, see *Selective device access control* in the **Related information** section.

Related information

"Data access and availability" on page 269

"Feature details" on page 149

"Selective device access control" on page 292

Hybrid TS7700 Grid configurations

A hybrid TS7700 Grid is one that contains an intermix of one or more TS7700 tape-attach Clusters and one or more TS7700 disk-only Clusters that are configured together within the same grid.

The hybrid grid configuration is used for archival and data retention purposes where data consistency shifts from disk-only clusters (clusters that do not connect to a physical library) to clusters that do connect to a physical library. Data that is contained within any TS7700 Cluster can be accessed by any peer cluster, regardless of either cluster's connection to a physical library.

A hybrid TS7700 Grid can be configured by using between two and six TS7700 Clusters.

Seven- or eight- cluster hybrid
Seven- and eight-cluster hybrid grid configurations are supported by RPQ only. Possible configurations of seven and eight cluster grids include:

Three production sites each with two clusters, plus a one- or two-cluster disaster recovery site
Each production site contains one disk-only cluster combined with one cluster attached to a physical library. When part of a seven-cluster grid, the disaster recovery site contains one cluster attached to a physical library. When part of a eight-cluster grid, the disaster recovery site also contains a disk-only cluster.

Each production site writes and reads only to its local clusters and all data that is written within either production site is replicated to the adjacent cluster and all disaster recovery clusters.

One production site with four clusters, plus one disaster recovery site with four clusters

Each site contains two disk-only clusters and one cluster attached to a physical library. This configuration is available only with a eight-cluster grid.

Data that is written to a production cluster is replicated to one adjacent cluster and to at least two disaster recovery clusters.

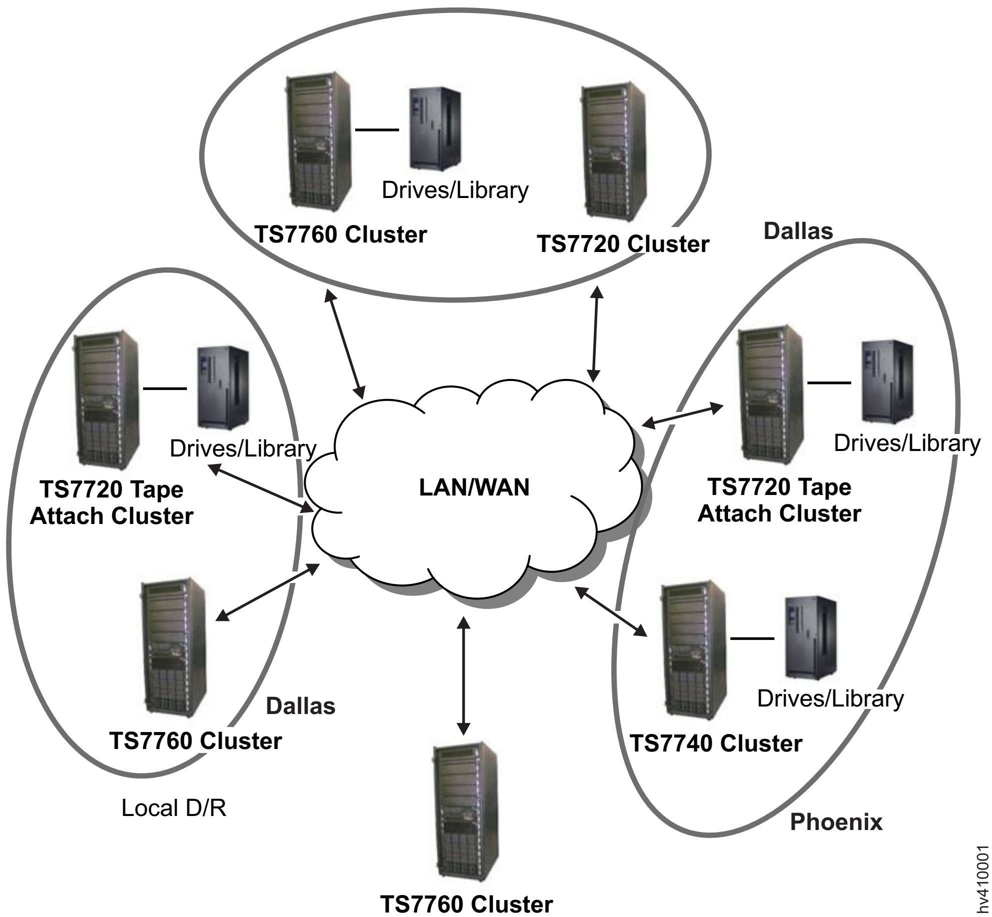


Figure 35. Example of a TS7720, TS7740, and TS7760 7-way hybrid Grid configuration

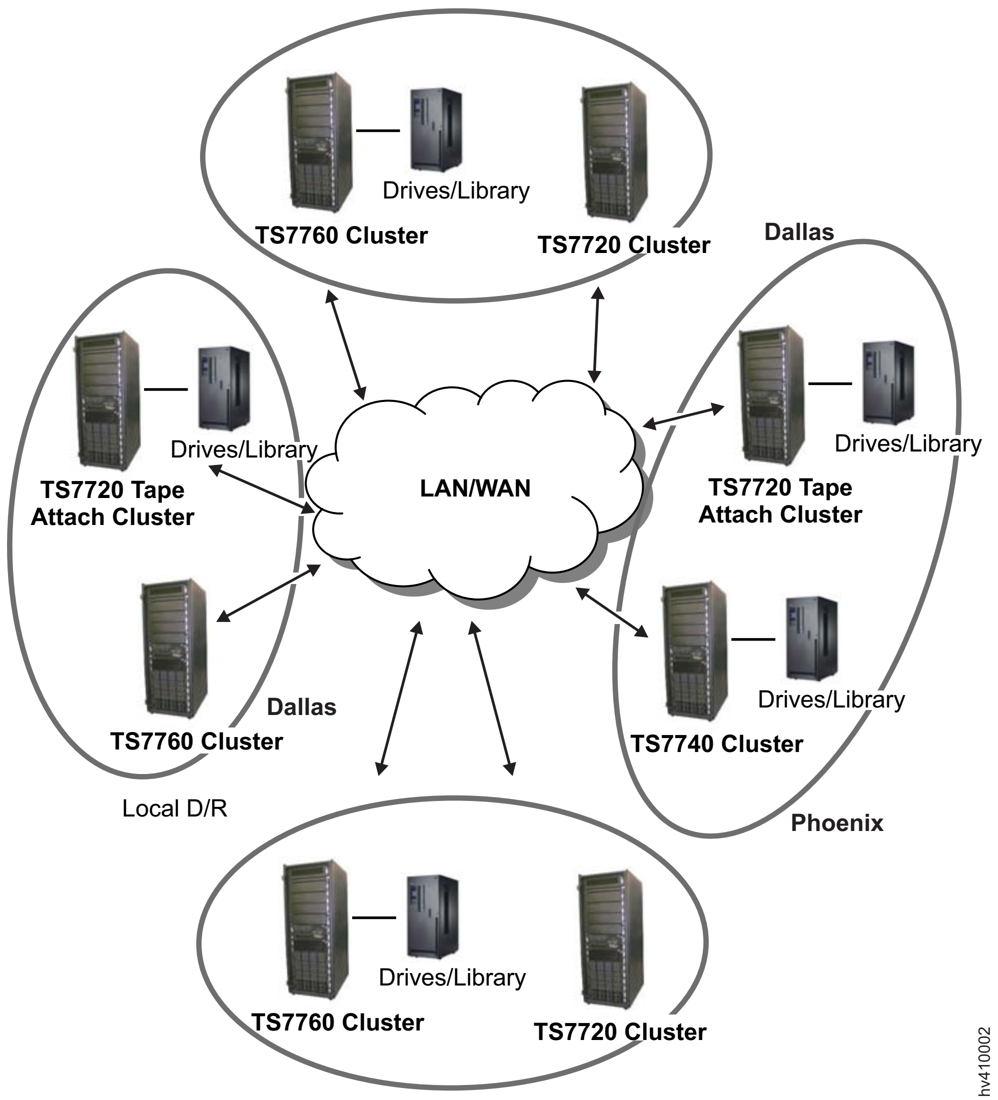


Figure 36. Example of a TS7720, TS7740, and TS7760 8-way hybrid Grid configuration

Five- or six- cluster hybrid

Five- and six-cluster hybrid grid configurations are supported by RPQ only. Possible configurations of five and six cluster grids include:

Two production sites each with two clusters, plus a one- or two-cluster disaster recovery site

Each production site contains one disk-only cluster combined with one cluster attached to a physical library. When part of a five-cluster grid, the disaster recovery site contains one cluster attached to a physical library. When part of a six-cluster grid, the disaster recovery site also contains a disk-only cluster.

Each production site writes and reads only to its local clusters and all data that is written within either production site is replicated to the adjacent cluster and all disaster recovery clusters.

One production site with three clusters, plus one disaster recovery site with three clusters

Each site contains two disk-only clusters and one cluster attached to a physical library. This configuration is available only with a six-cluster grid.

Data that is written to a production cluster is replicated to one adjacent cluster and to at least two disaster recovery clusters.

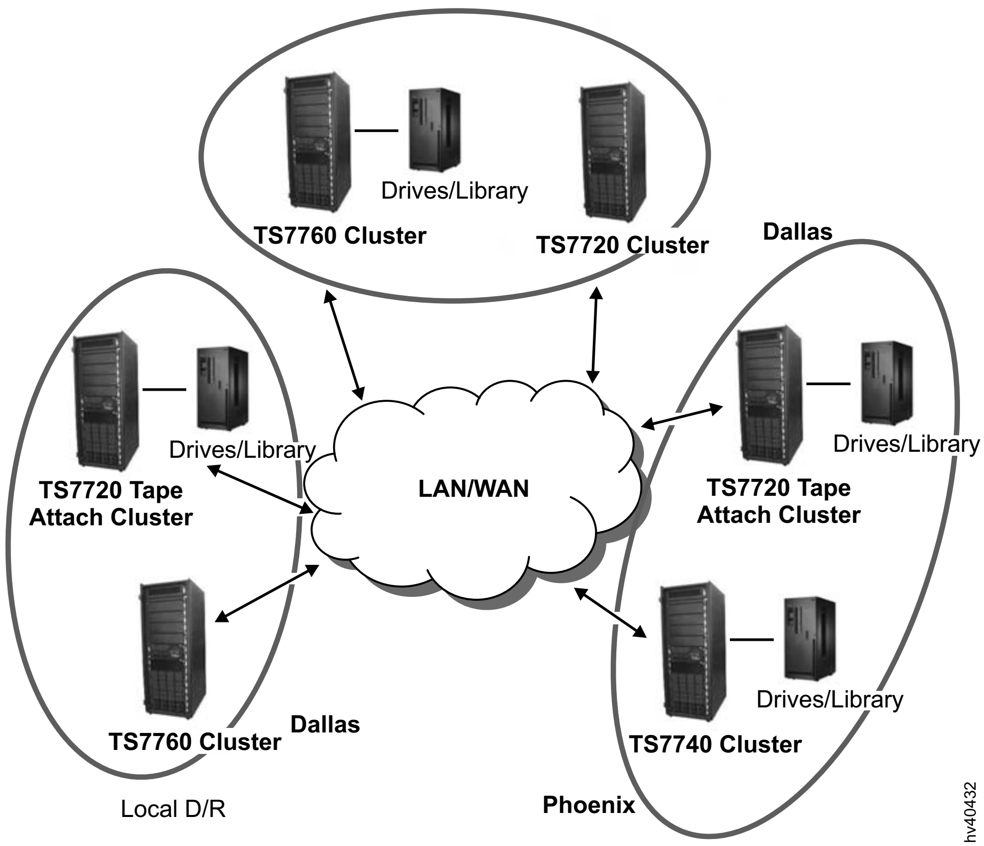


Figure 37. Example of a TS7720, TS7740, and TS7760 6-way hybrid Grid configuration

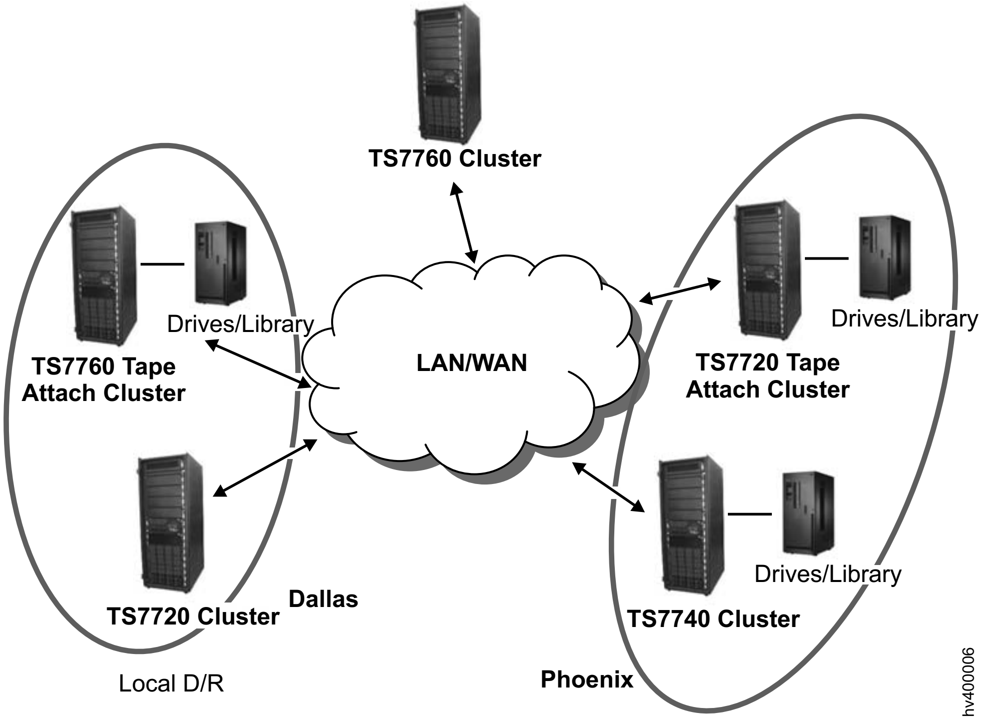


Figure 38. Example of a TS7720, TS7740, and TS7760 5-way hybrid Grid configuration

Four-cluster hybrid

There are two common configurations of a four-cluster grid:

Two disk-only production clusters, plus two remote clusters attached to physical libraries

Disk-only clusters are used for production data, while clusters attached to physical libraries are used for archival or disaster recovery purposes. Optimally, the clusters that are attached to physical libraries are at metro distances to separate long-term data from a single point of loss.

All clusters are configured for high availability. However, the production clusters are also configured for high cache hit rates. Long-term retention data migrates to the clusters attached to physical libraries. The copy export function can be used on these clusters to produce a second or third offsite copy of long-term retention data.

Identical production and remote configurations

One configuration is duplicated at multiple sites: one disk-only cluster combined with one cluster attached to a physical library. This provides a high-availability solution for both production and archival data centers, while distancing the clusters attached to physical libraries for disaster recovery purposes. All clusters are configured for high cache hit rates.

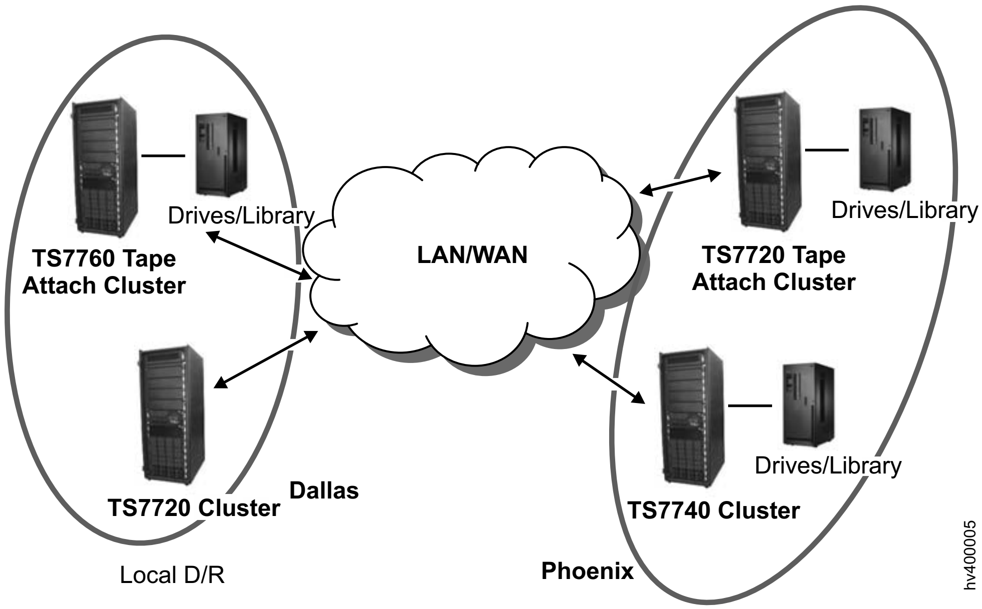


Figure 39. Example of a TS7720, TS7740, and TS7760 4-way hybrid Grid configuration

Three-cluster hybrid
One disk-only cluster is used for production, as is one of the clusters attached to a physical library. The other cluster that is attached to a physical library is used for archival or disaster recovery purposes. This solution is a high availability production configuration that also provides the benefits of high cache hit rates for recent data.

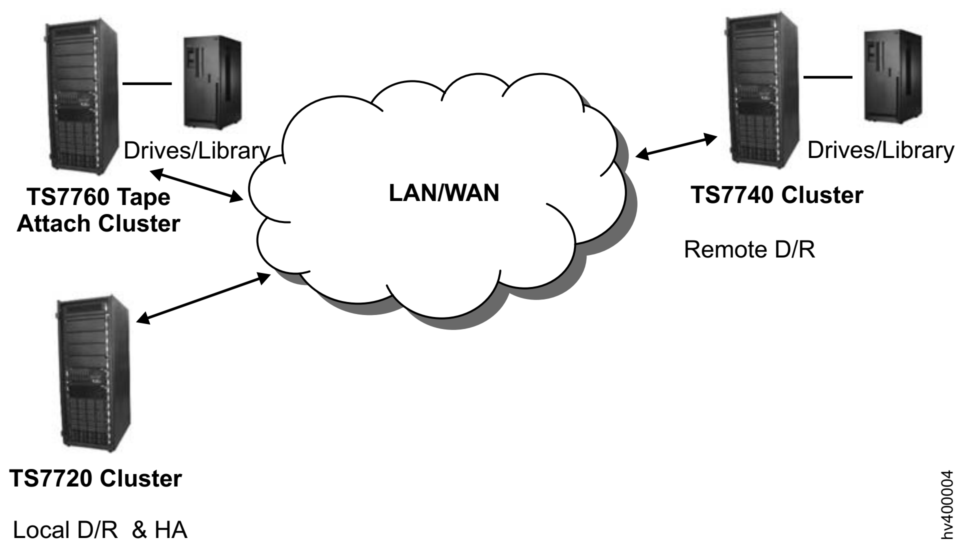


Figure 40. Example of a TS7720, TS7740, and TS7760 3-way hybrid Grid configuration

Two-cluster hybrid
One disk-only cluster is used for production, while one cluster attached to a physical library is used for archival or disaster recovery purposes. Copy export can be used to produce a second offsite copy of the long-term data that resides only in the cluster attached to a physical library.

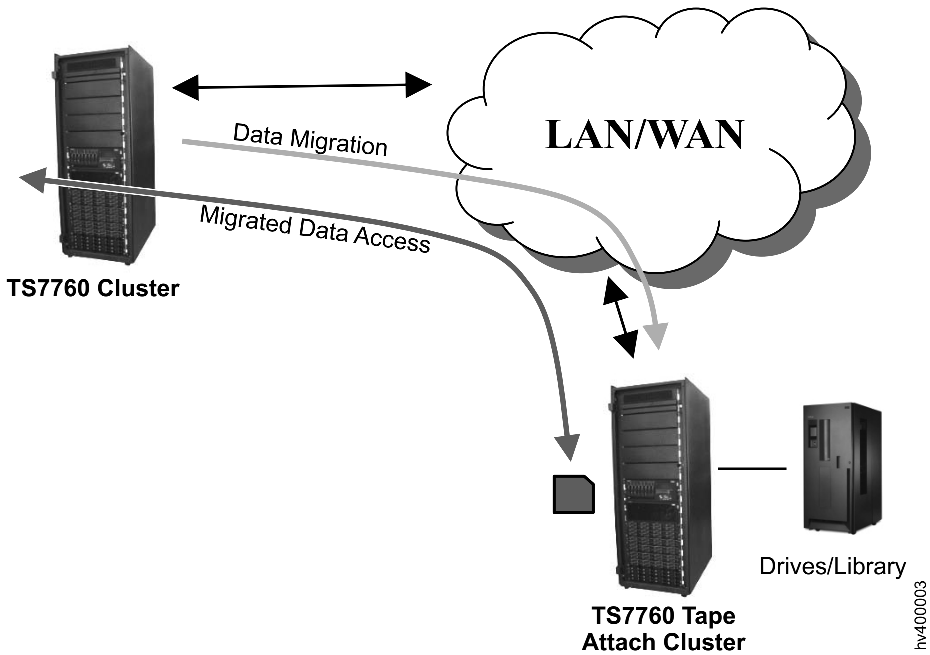


Figure 41. Example of a TS7760 hybrid configuration

Table 87 summarizes the possible configurations of a hybrid TS7700 Grid.

Table 87. Hybrid grid configurations

Total clusters	Site A	Site B	Site C	Expectations
8	Production 1 disk-only cluster 1 library-attached cluster	Production 1 disk-only cluster 1 library-attached cluster	Backup 1 disk-only cluster 1 library-attached cluster	• High availability at two sites. • Remote access for volumes no longer in disk-only cache. • Optimal cache hits of newer content at production sites. • Copy export is optionally used to create offsite copies of long-term content.
8	Production and backup 2 disk-only clusters 1 library-attached cluster	Production and backup 2 disk-only clusters 1 library-attached cluster	No third site	• High availability at both sites. • Local access for volumes no longer in disk-only cache. • Copy export is optionally used to create offsite copies of long-term content.
7	Production 1 disk-only cluster 1 library-attached cluster	Production 1 disk-only cluster 1 library-attached cluster	Backup 1 1 library-attached cluster	• High availability at both sites. • Local access for volumes no longer in disk-only cache. • Optimal cache hits of newer content at production sites. • Copy export is optionally used to create offsite copies of long-term content.

Table 87. Hybrid grid configurations (continued)

Total clusters	Site A	Site B	Site C	Expectations
6	Production 1 disk-only cluster 1 library-attached cluster	Production 1 disk-only cluster 1 library-attached cluster	Backup 1 disk-only cluster 1 library-attached cluster	• High availability at two sites. • Remote access for volumes no longer in disk-only cache. • Optimal cache hits of newer content at production sites. • Copy export is optionally used to create offsite copies of long-term content.
6	Production and backup 2 disk-only clusters 1 library-attached cluster	Production and backup 2 disk-only clusters 1 library-attached cluster	No third site	• High availability at both sites. • Local access for volumes no longer in disk-only cache. • Copy export is optionally used to create offsite copies of long-term content.
5	Production 1 disk-only cluster 1 library-attached cluster	Production 1 disk-only cluster 1 library-attached cluster	Backup 1 library-attached cluster	• High availability at both sites. • Local access for volumes no longer in disk-only cache. • Optimal cache hits of newer content at production sites. • Copy export is optionally used to create offsite copies of long-term content.
4	Production 2 disk-only clusters	Backup 2 library-attached clusters	No third site	• High availability at both sites. • Remote access for volumes no longer in disk-only cache. • Optimal cache hits of newer content at the production site. • Copy export is optionally used to create offsite copies of long-term content.
4	Production 1 disk-only cluster 1 library-attached cluster	Production or backup 1 disk-only cluster 1 library-attached cluster		• High availability at both sites. • Local access to volumes on tape. • Second production site as backup. • Optimal cache hits at both production and backup sites.
3	Production 1 disk-only cluster 1 library-attached cluster	Backup 1 library-attached cluster		• High availability at the production site. • Can require remote mount if local library-attached cluster is down and volume is not in cache. • Optimal cache hits at the production site.
2	Production 1 disk-only cluster 1 library-attached cluster	No remote clusters		• High availability for recently used volumes. • Copy export is optionally used to create offsite copies of long-term content. • Loss of cluster attached to physical library can prevent access to older volumes. • For scheduled outages, a pre-removal of volumes from the disk-only cluster would be required to assure enough cache space is available.

Important: Copy policies must be set up correctly across the hybrid grid. Optimally, all volumes that are created on a disk-only cluster have a copy policy that creates a copy on one or more clusters attached to a physical library. Otherwise, the automatic removal cannot remove volumes from the disk-only cache, leading to the disk-only cache reaching its maximum capacity. If this happens, a manual intervention is required to reduce the volume use of the disk-only cluster.

TS7700 Clusters that attach to a physical library have a much higher total storage capacity than disk-only TS7700 Clusters. In a hybrid grid, a copy export from a cluster that is attached to a physical library can export all the contents of the library including any hybrid-migrated data that resides only on the TS7700 Clusters attached to a physical library. Therefore, when a complete failure occurs to a copy export parent site, it is possible that the copy exported volumes are the only source for the hybrid-migrated data. A recovery in this scenario can occur by initiating a disaster recovery process into a new TS7700 Cluster attached to a physical library by using the copy exported volumes. This allows the data to be merged back into the composite library and any preexisting TS7700 Clusters remain present with valid content. This disaster recovery approach, as opposed to a copy export recovery approach, does not require the recovery point to be a stand-alone TS7700 Cluster attached to a physical library.

Related information

"About cluster families"

"Copy export overview" on page 130

"TS7700 Cache thresholds and removal policies" on page 276

"Retain Copy Mode" on page 273

About cluster families

Cluster families group clusters that operate with a common purpose or under a common set of guidelines.

Note: The cluster family configuration is supported only when all clusters in the grid operate at microcode level 8.6.0.x or later.

Clusters can be grouped in families to accomplish a particular task more efficiently or to imply a specific purpose within a grid. For example, one cluster family in a grid can be viewed as a production family. Another cluster family in the same grid can be viewed as an archive or as a family in the disaster recovery (DR) location. In either case, clusters within a common family perform certain grid-related tasks more effectively than clusters that do not share a family.

All members of a family employ Cooperative Replication and tape volume cache (TVC) Selection for Mounts enhancements. During a mount scenario, these enhancements improve control and performance by favoring cluster family members when remote mounts are required. The favoring of cluster family members is especially beneficial in distinguishing a set of production clusters from clusters intended for disaster recovery or archival purposes. Consistency across the family is the primary goal for cluster family members, and they collaborate to achieve this goal. Upon reaching family-wide consistency, the cluster family members then share data to bring each individual member up to the family consistency level.

The maximum number of possible families is equal to the maximum number of clusters in the grid. However, for cluster family benefits to be observed a cluster family must possess at least two cluster members. A cluster can belong only to one family at any time, but can change from one family to another. A cluster is not required to be a part of any family.

You can create, modify, or delete cluster families by using the TS7700 Management Interface.

Cooperative Replication

Cooperative Replication improves the efficiency and versatility of the TS7700's Copy Management function. Its enhancements to TVC selection enable the preferential selection of clusters within a cluster family when compared with clusters outside that family. As a result, clusters within the same cluster family can share the "Deferred" copy workload, optimizing throughput, and improving the overall time-to-family consistency.

When a family becomes consistent regarding volumes outside of the family, the members of the family replicate among each other. This allows a family to become consistent at up to $1/n$ the time of volumes outside the family, where n is the number of clusters in the family. Since the clusters in a family are assumed to be at metro distances, the replication between them that later occurs is also accelerated.

Related information

Grid operational states

This topic describes how to locate and identify grid operational states that can indicate a cluster or network problem.

You can identify and trace grid warning states and network problems by using the **Grid summary** panel on the TS7700 Management Interface. The **Grid summary** panel shows a visual summary of the TS7700 Grid, its clusters and families, and health status. This panel also displays warning states, such as a virtual library out of scratch or copies disabled across the grid. If any operational state bits are not normal, the management interface degrades the health of the cluster that is shown on the grid summary panel and displays a warning message for the affected cluster.

Removing a cluster from a grid and cluster cleanup

One or more TS7700 Clusters can be removed from an existing TS7700 Grid erased of virtual volumes and configuration information for reuse.

In some circumstances, it might be desirable to remove a TS7700 Cluster from a TS7700 Grid or restore it to a state similar to new. For instance, cluster removal can be used with cluster cleanup in a datacenter consolidation scenario. In this scenario, a TS7700 Cluster that used Grid replication to copy data to a primary datacenter could be detached and then cleaned up using “FC 4016, Remove Cluster from Grid” on page 159, and “FC 4017, Cluster cleanup” on page 160. Following removal and cleanup, the TS7700 Cluster can be relocated and reused.

Note: If the cluster removal process is initiated from a cluster that operates a microcode level earlier than 8.7.0.134, all clusters in the grid must be at the same level of code before “FC 4016, Remove Cluster from Grid” on page 159 can be used. If the cluster removal process is initiated from a cluster that operates a microcode level of 8.7.0.134 code or later, then an intermix of code levels is permitted for use with “FC 4016, Remove Cluster from Grid” on page 159.

TS7700 Cluster removal

You can remove a TS7700 Cluster from a TS7700 Grid concurrently with operations on the remaining TS7700 Clusters if you do not inhibit inserts, ejects, or exports. Use "FC 4016, Remove Cluster from Grid" on page 159 to remove a TS7700 Cluster from a TS7700 Grid. You must determine ahead of the removal process how to address volumes that have only a copy consistency point at the TS7700 Cluster being removed. Before the cluster's removal, these volumes must be ejected, moved to the scratch category, or copied to another cluster through Management Class mount and demount operations.

Note: After the TS7700 Cluster is removed, data still on that cluster (in cache or on tape) is unavailable. Development support must manually recover any data from a TS7700 Cluster removed by using "FC 4016, Remove Cluster from Grid" on page 159.

TS7700 Cluster cleanup

You can clean up a stand-alone TS7700 Cluster or one that is removed from a TS7700 Grid to achieve a state similar to new. Use "FC 4017, Cluster cleanup" on page 160 to return the TS7700 Cluster to a state similar to one received from manufacturing with the original feature codes still in place.

Note: To ensure that all volumes are present following removal of a TS7700 Cluster, you can decide to delay subsequent cleanup for a short period while the TS7700 Grid continues operation. Recovery of any missed data requires development support.

Related information

FC 4016, Remove Cluster from Grid

FC 4017, Cluster cleanup

Removing a TS7700 Cluster

A TS7700 Cluster can be removed from a TS7700 Grid.

FC 4016, Remove Cluster from Grid, delivers instructions for a one-time process to remove a TS7700 Cluster from a TS7700 Grid. You must order this feature before you can complete a cluster cleanup (FC 4017, Cluster cleanup) on any TS7700 Cluster configured to participate in a TS7700 Grid. If a TS7700 Cluster is removed from a TS7700 Grid, cleaned up, and then joined to a new TS7700 Grid, another instance of FC 4016, Remove Cluster from Grid is required to remove the cluster from the new Grid.

Related information

"System requirements" on page 63

Data access and availability

A TS7700 Grid configuration provides the following data access and availability characteristics:

Direct host attachment to TS7700

Hosts are directly attached to a TS7700, which affects how a mount request is issued.

A host mount request must be issued on a virtual device address defined for that cluster. The virtual device addresses for each cluster are independent. This is different than the prior generation's PtP VTS where the mount request was issued on a virtual device address defined for a virtual tape controller and the virtual tape controller then decided which VTS to use for data access.

Related information

“Planning for virtual and physical volumes” on page 96

“Workload considerations” on page 61

Virtual volume data

The following features describe data stored on virtual volumes.

Logical WORM

Logical WORM (LWORM) is a software-emulated, virtual equivalent of the Write-Once, Read-Many (WORM) capability available on physical tape media.

The LWORM attribute emulates physical WORM to leverage host software support of WORM physical media. With LWORM, an attached host recognizes the TS7700 as an LWORM-compliant library, able to contain WORM-compliant virtual drives.

Note: The LWORM attribute is supported only when all clusters in the grid operate at microcode level 8.6.0.x or higher.

The LWORM attribute provides the following functions:

- Assigns a data class construct property to volumes assigned as LWORM-compliant, either upon the first mount or during reuse from scratch
- Generates a temporary World Wide Identifier (WWID) during WORM type assignment that is sent to the host, then bound (persistently saved) to the volume
- Generates and maintains a persistent write-mount count for each LWORM volume synchronized to the host software
- Permits appends to LWORM volumes using only physical WORM append guidelines
- Permits host software to access LWORM attributes for a given, mounted volume

Logical WORM attributes cannot be appended to previously written volumes. In order for the volume to be LWORM-compliant, it must be assigned so before data is written to it, either upon the first mount or during reuse from scratch. When all clusters within a TS7700 are LWORM-compliant, the host Read Device Characteristics commands begin to set a new flag stating the device or composite-library is LWORM-compliant.

Data Class LWORM assignment (binding)

Virtual volumes are configured as LWORM volumes in the Data Class record, modifiable on the Data Class panel of the TS7700 Management Interface. Binding refers to the process of persistently saving a type or attribute property of a volume. Prior to the binding of the property, any derived or assigned properties can be utilized but they are not permanent until the binding event occurs. Once the binding succeeds, the type and or attributes are said to be “bound” to the volume.

LWORM can be set for a new or existing Data Class, however the WWID for the volume can only be bound or cleared upon one of the following:

- The first use of the volume after insert

- The first reuse of the volume after scratch

The first use or reuse of an LWORM volume is only valid when the first write also occurs at the load point beginning of tape (BOT). Prior to the first write at BOT, the volume is only a candidate for use or reuse and any previously bound or NULL information remains unchanged.

Mount with expected WORM binding or clearing

During a mount, the TS7700 creates a new WWID for the volume if both of the following are true:

1. The pending Data Class assignment states the volume should be treated as an LWORM
2. The volume has never accepted a write operation (is newly inserted) or the mount sequence is scratch

If the pending Data Class assignment states the volume should not be treated as a logical worm and the other variables are true, then a temporary NULL WWID value is assumed.

Once a WWID is bound to a volume, all future non-scratch mounts treat the volume as an LWORM volume independent of any currently configured Data Class settings. Once a WWID is already bound, changes to the Data Class name or attributes for the volume do not affect the binding of the LWORM volume type. A bound LWORM volume is composite in scope, which means that when it is bound with a WWID, all clusters within a grid honor all LWORM rules associated with that volume. Binding (to a new WWID or clearing of an existing WWID) can only occur at first use or reuse of a volume.

Important: A non-LWORM volume with existing data cannot be bound to a WWID by configuring a Data Class then performing a mount or demount sequence unless the mount is a scratch mount and a write operation occurs at BOT. Any previously bound WWID can be cleared (NULL WWID) through the binding process only if a scratch mount operation has a pending non-LWORM Data Class setting and a first write occurs at BOT. This is the means of which an LWORM volume can legally be reused as a standard read and write volume.

WWID and write-mount count z/OS DFSMS synchronization

The write-mount count is a host software synchronized value that mimics tape media WORM behavior. Each time a volume is assigned a new WWID, a write-mount count (initially set to zero) must be associated with and bound to the volume during the first write from BOT. Each time a volume is mounted thereafter and at least one write operation of any kind is issued during that mount, the write-mount count for the volume is increased by one. The write-mount count can be used to count the total number of times a volume was mounted with modifications. When the write-mount count is bound for the first time it has a value of 1, which represents the initial value of 0 increased by one due to the first write from BOT.

To keep the host and the TS7700 data facility system managed storage (DFSMS) synchronized, WWID and write-mount count are handled as follows:

Table 88. WWID and write-mount count scenarios. Table describes conditions of host write-mount count scenarios.

If	Then	Result
The host has previously expired and reused a volume and the user designates the volume can be reused.	The Removal Media Manager (RMM) resets the explicit WORM identifier, the WWID, and write-mount count within the host catalogue.	The host is informed that the current reset assignment represents a standard read and write volume without any WORM obligations. Host software can mark the volume for scratch and it can be returned to scratch during the next scratch processing phase.
During host software mount processing, a mount with expected WORM binding or clearing occurs.	A WWID is temporarily generated and eventually bound or cleared at first write from BOT.	If a first write from BOT does not occur, this temporary WWID is discarded leaving any previously bound WWID value intact.
A new WWID is temporarily assigned.	The TS7700 resets the write-mount count for the volume to 0 (within memory).	During the first write from BOT, this write-mount count is increased to a value of 1 and bound when the temporary WWID is bound. If a first write from BOT does not occur, this write-mount count is discarded, leaving any previously bound write-mount count value intact. If a NULL-WWID is to be bound (for example, standard read and write volume), the write-mount count is not increased with each first write operation.

Logical WORM volume usage restrictions

Logical WORM volumes must have Non-Rewriteable concepts implied by the LWORM type of the volume. Once a WWID is bound to a volume, only WORM-supported appends are allowed. No retention concepts such as prevention of eject, delete, delete-expire, nor assignment to scratch categories are restricted by the TS7700.

However, any attempt to overwrite previously written data on an LWORM bound volume (independent of write-mount count) fails if it does not meet the Append Only Rules, as follows:

1. Appending restrictions are the same as those for physical WORM.
2. If a volume has previously accepted a completed EOV construct sequence followed by one or two tape marks, the volume can no longer be written to.
3. Writing is not allowed at any location prior to the start of a construct sequence, where both of the following are true:

- The sequences are those explicitly enumerated below
- At least one non-construct record has been written to the tape (rule 6 is an exception)

4. Writing is not allowed over or before any construct sequence that is followed by another construct sequence or data virtual block that have been explicitly or implicitly synchronized. The synchronization event should, at a minimum, progress the legal append point to the block following the last completed construct sequence. Explicit synchronization results from the acceptance of one of the following commands:
   - SYNC
   - WTM
   - RUN

   Implicit synchronization includes:
   a. Synchronize Buffer
   b. Forward Space Block, Forward Space File, Backward Space Block, Backward Space File, Rewind, Rewind Unload, Write Tape Mark, Erase Gap, Data Security Erase or Locate Block
   c. Read Forward, Read Previous or Read Backward and there is buffered write data
   d. A Write command is issued in a command chain following either a Mode Set command that specifies tape write immediate mode or a Set Tape Write Immediate command
   e. The virtual end of volume point is reached or exceeded
5. Overwriting of any data virtual block that has been explicitly or implicitly synchronized is not allowed. The synchronization event, at a minimum, advances the legal append point to the block following the last completed non-construct data virtual block.
6. Full overwrite of the entire tape and any constructs is permitted so long as no data virtual blocks (non-constructs) have been written.
7. All or partial overwrite of the last construct sequence is permitted when the construct sequence is either incomplete, or is not followed by additional data or tape marks.
8. Writing is not allowed at points other than following the last complete volume record of any type when a volume is loaded and its ending disposition cannot be definitively determined. This can occur after an outage or after a volume corruption where the last known persistent append point is either unknown or no longer valid.

   Related information

   "Copy export overview" on page 130

Retain Copy Mode

Retain Copy Mode prevents the copy modes of a virtual volume from being refreshed by an accessing host device if the accessing cluster is not the same cluster that created the volume.

Use the Management Classes panel on the TS7700 Management Interface to enable or disable the Retain Copy Mode. To verify that the Retain Copy Mode is enabled and working, check that the Copy Mode displayed on the Virtual Volume Details page of the management interface remains unchanged following any access of the non-scratch virtual volumes associated with the Management Class in question.

In some grid configurations, virtual volume copies are either not required or intentionally avoided on all clusters. This may be to reduce the replication counts of a volume, or to partition the overall capacity of a grid configuration through selective replication. When these volumes are read or modified through a device on a cluster that did not create the content, the copy modes for the virtual volume can be refreshed, or updated with values from the accessing cluster. The resulting copy modes can be a combination of old and new copy modes, leading to the creation of additional copies not originally requested. When Retain Copy Mode is enabled through the management interface, previously assigned copy modes are retained and subsequent read or modify access does not refresh, update, or merge copy modes. This allows the original number of copies to remain in place.

Note: The Retain Copy Mode option is available only on non-scratch virtual volume mounts.

When enabled for a particular Management Class, Retain Copy Mode ensures that the existing copy mode setting is not changed when any non-scratch virtual volumes that are associated with that Management Class are accessed. Retain Copy Mode does not eliminate existing extra copies, but when enabled prevents extra copies from being made. If copy modes are updated for a given Management Class where Retain Copy Mode is enabled, the new copy modes are only applied to scratch mounts; non-scratch mounts retain the earlier copy mode settings.

Table 89. Effects of Retain Copy Mode in mount scenarios. Table describes scenarios and results for Retain Copy Mode settings.

Scenario	**Retain Copy Mode setting enabled?**	**Result**
Scratch mount is issued	Yes	Retain Copy Mode setting ignored
Non-scratch mount is issued	Yes	Grid uses volume's existing copy modes
Non-scratch mount is issued	No	Grid uses copy modes defined by cluster emulating the device used for the mount
New volume or copy mode not established	Yes	Grid uses copy modes associated with assigned Management Class
Retain Copy Mode setting is modified on associated Management Classes	Yes	Management Classes are updated; subsequent copy actions updated only on scratch mounts associated with each Management Class

Related information

"Copy export overview" on page 130

Copy queue prioritization

The incoming copy queue for a cluster lists those volumes waiting to be copied to a cluster.

Each cluster maintains its own list of copies to acquire, then satisfies that list by requesting copies from other clusters in the grid according to queue priority. Prioritization of volumes that are acquired to satisfy the copy queue occurs according to virtual volume copy type in the following order:

1. Immediate
2. Synchronous-deferred
3. Immediate-deferred
4. Deferred

Virtual volume copy types can be more precisely under each of the parent categories listed above. Acquisition of volumes to satisfy copy queue requests will exhaust all volume copy types in one parent category before making a request from another parent copy type. Figure 42 depicts the order in which copy types are acquired to satisfy incoming copy queue requests.

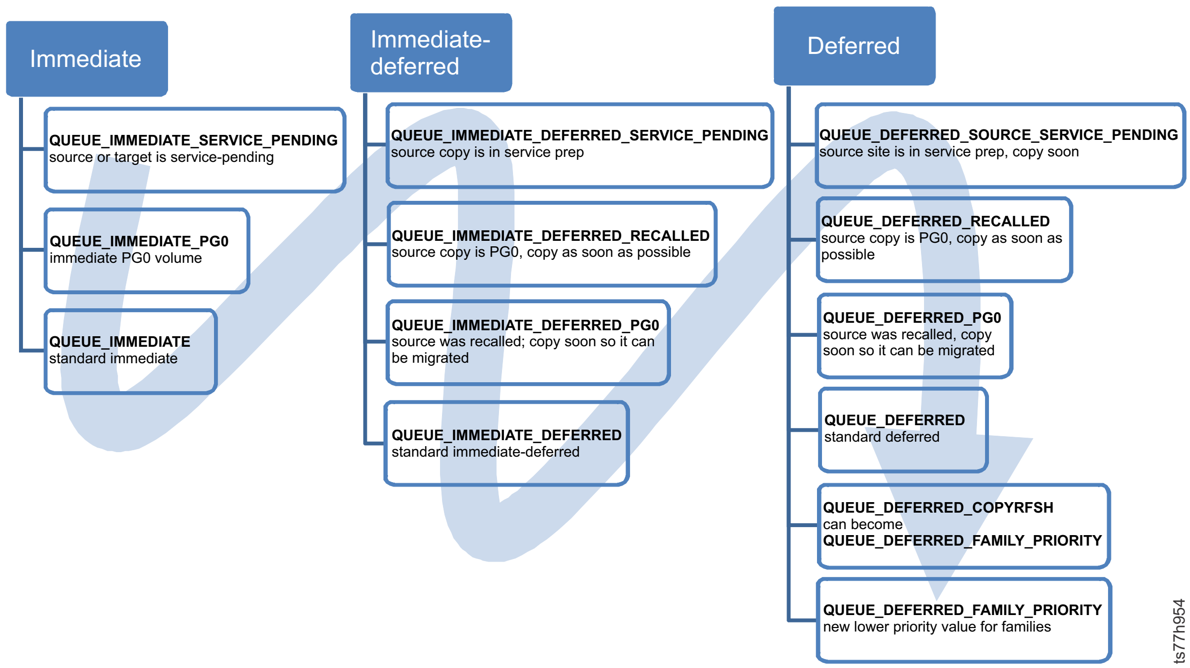


Figure 42. Order of copy queue prioritization

Related information

"Access and location of virtual volume data" on page 4
"Virtual volume copy availability" on page 5

Ownership-dependent access to a virtual volume

To access a virtual volume through a TS7700, that TS7700 must have ownership of the volume.

At any point in time, a virtual volume is 'owned' by a TS7700 Cluster. The owning cluster has control over access to the volume and changes to the attributes associated with the volume (such as category or storage constructs). Cluster ownership of a virtual volume can change dynamically based on which cluster in the grid configuration is requesting a mount of the volume. If a local TS7700 Cluster receives a mount request for a volume it does not own, it must first obtain ownership from the owning cluster. If the TS7700 Clusters are in a grid configuration and at least one of the 1-Gb Ethernet links between them are operational, any required change of ownership is automatic. This change of ownership adds a small amount of time to the mount operation.

TS7700 Cache thresholds and removal policies

This topic describes the boundaries (thresholds) of free cache space in a TS7700 and the policies that can be used to manage available (active) cache capacity in a grid configuration.

Cache thresholds for a disk-only TS7700 Cluster

There are three thresholds that define the capacity of cache partition 0 (CP0) in a TS7700 Tape Attach and the active cache capacity in a disk-only TS7700. (Because a disk-only TS7700 does not attach to a physical backend library, all of its virtual volumes are stored in the cache.)

These thresholds determine the state of the cache as it relates to remaining free space. In ascending order of occurrence, they are:

Automatic removal

By default this state occurs when the cache is 3 TB below the out-of-cache-resources threshold. In the automatic removal state, the TS7700 automatically removes volumes from the disk-only cache to prevent the cache from reaching its maximum capacity. This state is identical to the limited-free-cache-space-warning state unless the Temporary Removal Threshold is enabled.

Note:

- To perform removal operations in a TS7700 Tape Attach Cluster, the size of cache partition 0 (CP0) must be at least 10 TB. You can disable automatic removal within any given disk-only TS7700 Cluster by using the following library request command:

  `LIBRARY REQUEST` *`library-name`*`,CACHE,REMOVE,{ENABLE|DISABLE}`
- The default automatic removal threshold can be changed from the command line, by using the following library request command:

  `LIBRARY REQUEST` *`library-name`*`,CACHE,REMVTHR,{VALUE}`

Limited free cache space warning

This state occurs when there is less than 3 TB of free space left in the cache. When the cache passes this threshold and enters the limited-free-cache-space-warning state, write operations can use only an additional 2 TB before the out-of-cache-resources state is encountered. When a disk-only TS7700 Cluster enters the limited-free-cache-space-warning state, it remains in this state until the amount of free space in the cache exceeds 3.5 TB. Messages that can be displayed on the management interface during the limited-free-cache-space-warning state include:

- HYDME0996W
- HYDME1200W

For more information about each of these messages, see the **Related information** section.

Note: Host writes to the TS7700 Cluster and inbound copies continue during this state.

Out of cache resources

This state occurs when there is less than 1 TB of free space left in the cache. When the cache passes this threshold and enters the out-of-cache-resources state, it remains in this state until the amount of free space in the cache exceeds 3.5 TB. When a disk-only TS7700 Cluster is in the out-of-cache-resources state, volumes on that cluster become read-only and one or more out-of-cache-resources messages are displayed on the management interface. These messages can include:

- HYDME0997W
- HYDME1133W
- HYDME1201W

For more information about each of these messages, see the **Related information**.

Note: New host allocations do not choose a disk-only TS7700 Cluster in this state as a valid tape volume cache candidate. New host allocations that are issued to a disk-only TS7700 Cluster in this state choose a remote tape volume cache instead. If all valid clusters are in this state or unable to accept mounts, the host allocations fail. Read mounts can choose the disk-only TS7700 Cluster in this state, but modify and write operations fail. Copies inbound to this cluster are queued as deferred until the cluster exits this state.

Table 90 displays the start and stop thresholds for each of the active cache capacity states defined.

Table 90. Active cache capacity state thresholds. Table describes thresholds for active cache capacity states.

State	Enter state (free space available)	Exit state (free space available)	Host message displayed
Automatic removal	<4 TB	>4.5 TB	CBR3750I when automatic removal begins
Limited free cache space warning (CP0 for a TS7700 Tape Attach)	≤3 TB or ≤15% of the size of cache partition 0, whichever is less	>3.5 TB or >17.5% of the size of cache partition 0, whichever is less	CBR3792E upon entering state CBR3793I upon exiting state
Out of cache resources (CP0 for a TS7700 Tape Attach)	<1 TB or ≤5% of the size of cache partition 0, whichever is less	>3.5 TB or >17.5% of the size of cache partition 0, whichever is less	CBR3794A upon entering state CBR3795I upon exiting state
Temporary removal[1]	$<(X + 1\text{ TB})^2$	$>(X + 1.5\text{ TB})^2$	Console message
Notelist: 1. When enabled 2. Where *X* is the value given by the *TS7700 Temporary Removal Threshold* for the given cluster.			

Volume removal policies in a grid configuration

Removal polices determine when virtual volumes are removed from the cache of a TS7700 Cluster in a grid configuration. These policies provide more control over the removal of content from a TS7700 Cache as the active data reaches full capacity. To perform removal operations in a TS7700 Tape Attach Cluster, the size of cache partition 0 (CP0) must be at least 10 TB.

A TS7700 Tape Attach Cluster can have up to 7 tape-attached partitions. When a new partition is created, the resulting partition 0 (CP0) must have 2 TB free space.

The temporary removal function, working with the volume removal policies you have defined, can be used to release the required space in CP0 (at least 2 TB plus the size of the new partition).

To guarantee that data will always reside in a TS7700 or will reside for at least a minimal amount of time, a pinning time must be associated with each removal policy. This pin time in hours will allow volumes to remain in a TS7700 tape volume cache for at least *x* hours before it becomes a candidate for removal, where *x* is between 0 and 65,536. A pinning time of zero assumes no minimal pinning requirement. In addition to pin time, three policies are available for each volume within a disk-only TS7700 and for cache partition 0 (CP0) within a TS7700 Tape Attach. These policies are as follows:

Pinned
: The copy of the volume is never removed from this TS7700 Cluster. The pinning duration is not applicable and is implied as infinite. When a pinned volume is moved to scratch, it becomes a priority candidate for removal similarly to the next two policies. This policy must be used cautiously to prevent TS7700 Cache overruns.

Prefer Remove - When Space is Needed Group 0 (LRU)
: The copy of a private volume is removed if an appropriate number of copies exists on peer clusters, the pinning duration (in *x* hours) has elapsed since last access, and the available free space on the cluster has fallen below the removal threshold. The order of which volumes are removed under this policy is based on their least recently used (LRU) access times. Volumes in Group 0 are removed before the removal of volumes in Group 1 except for any volumes in scratch categories, which are always removed first. Archive and backup data would be a good candidate for this removal group since it will not likely be accessed once written.

Prefer Keep - When Space is Needed Group 1 (LRU)
: The copy of a private volume is removed if an appropriate number of copies exists on peer clusters, the pinning duration (in *x* hours) has elapsed since last access, the available free space on the cluster has fallen below a threshold, and LRU group 0 has been exhausted. The order of which volumes are removed under this policy is based on their least recently used (LRU) access times. Volumes in Group 0 are removed before the removal of volumes in Group 1 except for any volumes in scratch categories, which are always removed first.

Prefer Remove and **Prefer Keep** are similar to cache preference groups PG0 and PG1 with the exception that removal treats both groups as LRU versus using the volume size.

In addition to these policies, volumes that are assigned to a scratch category that have not been previously delete-expired are also removed from cache when the free space on a cluster has fallen below a threshold. Scratch category volumes, regardless of what their removal policies are, are always removed before any other removal candidates in volume size descending order. Pin time is also ignored for scratch volumes. Only when the removal of scratch volumes does not satisfy the removal requirements will Group 0 and Group 1 candidates be analyzed for removal. The requirement for a scratch removal is that an appropriate number of volume copies exist elsewhere. If one or more peer copies cannot be validated, the scratch volume is not removed.

These new policies are visible within the management interface only when all TS7700s within a grid are operating at microcode level 8.7.0.xx or later. All records creations before this time should maintain the default Removal Group 1 policy and be assigned a zero pin time duration.

Note: As of microcode level 8.7.0.xx, there is no automatic method to re-introduce a consistent instance of a previously removed volume into a TS7700 Cache simply by accessing the volume. Only when the copy override **Force Local Copy** or the volume is modified will a consistent version of a previously removed volume be re-introduced into a TS7700 Cache as a result of a mount operation.

Removal policy settings can be configured by using the **TS7700 Temporary Removal Threshold** option on the **Actions** menu available on the Grid Summary page of the TS7700 Management Interface. These settings include:

(Permanent) Removal Thresholds

Note: The Removal Threshold is not supported on the TS7740.
The default, or permanent, Removal Threshold is used to prevent a cache overrun condition in a TS7700 Cluster that is configured as part of a grid. By default it is a 4 TB value (3 TB fixed plus 1 TB) that, when taken with the amount of used cache, defines the upper size limit for a TS7700 Cache or for a TS7700 Tape Attach CP0. Above this threshold, virtual volumes begin to be removed from a TS7700 Cache. Virtual volumes are removed from a TS7700 Cache in this order:

1. Volumes in scratch categories
2. Private volumes least recently used, using the enhanced removal policy definitions

Once removal begins, the TS7700 continues to remove virtual volumes until the Stop Threshold is met. The Stop Threshold is a value that is the Removal Threshold minus 500 GB.

A particular virtual volume cannot be removed from a TS7700 Cache until the TS7700 verifies that a consistent copy exists on a peer cluster. If a peer cluster is not available, or a volume copy has not yet completed, the virtual volume is not a candidate for removal until the appropriate number of copies can be verified later.

Note: The default removal threshold can be changed from the command line, by using the following library request command:

`LIBRARY REQUEST` *`library-name`*`,SETTING,CACHE,REMVTHR,{VALUE}`

Temporary Removal Thresholds

Note: The Temporary Removal Threshold is not supported on the TS7740.
The Temporary Removal Threshold lowers the default Removal Threshold to a value lower than the Stop Threshold in anticipation of a Service mode event.

The Temporary Removal Threshold value must be equal to or greater than the expected amount of compressed host workload written, copied, or both to the TS7700 during the service outage. The Temporary Removal Threshold is 4 TB providing 5 TB (4 TB plus 1 TB) of free space exists, but you can lower the threshold to any value between 2 TB and full capacity minus 2 TB.

All TS7700 Clusters in the grid that remain available automatically lower their Removal Thresholds to the Temporary Removal Threshold value defined for each. Each TS7700 Cluster may use a different Temporary Removal Threshold. The default Temporary Removal Threshold value is 4 TB or an additional 1 TB more data than the default removal threshold of 3 TB. Each TS7700 Cluster will use its defined value until any cluster in the grid enters Service mode or the temporary removal process is canceled. The cluster that initiates the temporary removal process will not lower its own removal threshold during this process.

Related information

"Hybrid TS7700 Grid configurations" on page 258

"Virtual volume data" on page 270
The following features describe data stored on virtual volumes.

"Merging clusters or grids" on page 103
You can add an existing TS7700 Cluster to another cluster or TS7700 Grid. You can also merge two existing TS7700 Grids.

TS7700 Cache migration threshold

This topic describes the preference groups that manage virtual volume migration from cache in a TS7700, and the threshold that determines when migration begins.

Virtual volumes in a TS7740, a TS7720 Tape Attach , or a TS7760 Tape Attach are managed by preference group (PG). These groups determine how soon volumes are migrated from cache following their copy to backend physical tape and are classified either as PG0 or PG1. The migration threshold applies only to PG1, which is the last group of volumes migrated from disk cache.

Preference Group 0 (PG0)

When space is needed, volumes are migrated from cache according to size. Largest volumes are migrated first.

This group is assigned to volumes that are unlikely to be accessed after being created. There is no need to keep them in cache any longer than is necessary to copy them to physical tape. When a volume is assigned as PG0, the TS7700 gives it preference to be copied to physical tape. When space is needed in the tape volume cache (TVC), the TS7700 first selects a PG0 volume that has been copied to a physical volume and then deletes it from cache, leaving a copy only on physical tape. PG0 volumes are selected by largest size first, independent of how long they have been resident in cache. If no PG0 volumes remain that are resident in cache and have also been copied to physical tape, the TS7700 begins to select preference group 1 (PG1) volumes for migration.

The TS7700 also migrates PG0 volumes from cache if the subsystem is relatively idle. There is a small amount of internal processing impact to migrating a volume from cache, so there is some benefit in migrating them when extra processing capacity is available. In the case where the TS7700 migrates PG0 volumes during idle times, it selects them by smallest size first.

Preference Group 1 (PG1)

When space is needed, volumes are migrated from cache according to last recently used (LRU) access time.

This group is assigned to volumes that are likely to be accessed after being created. One example of volumes in this category are those that contain master files created as part of the nightly batch run. Because the master files are likely to be used as input for the next night's batch run, it is beneficial for these volumes to stay in the TVC for as long as possible. When a volume is assigned as PG1, the TS7700 adds it to the queue of volumes to be copied to physical tape soon after the volume is demounted. It is copied to tape with a lower priority than PG0 volumes that have not yet been copied to tape. When space is needed in cache, the TS7700 first determines whether any PG0 volumes can be migrated. If not, the TS7700 selects PG1 volumes to be migrated based on an LRU algorithm. The LRU algorithm causes volumes that have already been copied to physical tape and that have been resident in cache the longest without access to be migrated first. The selected volumes are deleted from disk cache, leaving a copy of the volume only on physical tape.

The migration threshold for PG1 is 95% of full capacity or full capacity minus 300 GB, whichever value permits more active content to remain in cache.

When a preference group is assigned to a volume, that assignment is persistent until the volume is reused for scratch or remounted and a new preference group is assigned. Thus, a volume that is assigned as PG0 maintains that preference group when it is subsequently recalled into cache. You can use the *Storage Class* panel of the management interface to set a volume preference group as PG0 or PG1.

Note: When a second physical tape copy is requested within a volume's management class, copies to both physical tape pools must complete before the volume is a candidate for migration.

Virtual volumes in a TS7720 Tape Attach environment can be designated for time-delayed premigration. For more information, see *Virtual volume details*.

Related information

"Virtual volume data" on page 270

Ownership takeover

If a TS7700 Cluster fails, ownership transfer of the volumes that it owned is not automatic. In order for another cluster to access and manage those volumes, the failed TS7700 Cluster is placed in an ownership takeover mode.

The ownership takeover modes are set through the TS7700's System Management Interface Tool panel. Three modes are provided:

Read Ownership Takeover
When Read Ownership Takeover (ROT) is enabled for a failed cluster, volume ownership is allowed to be taken from a failed TS7700 Cluster by any other available TS7700 Cluster. Only read access to the volume is allowed through the remaining TS7700 Clusters if the volume is taken over. When ownership for a volume has been taken in this mode, any operation attempting to modify data on that volume or change its attributes fails.

Write Ownership Takeover
When Write Ownership Takeover (WOT) is enabled for a failed TS7700 Cluster, volume ownership is allowed to be taken from a failed TS7700 Cluster. Full access is allowed through the remaining available TS7700 Clusters in the Grid.

Service Preparation/Service Mode
When a TS7700 Cluster is placed into service preparation and successfully enters the service mode, ownership of its volumes is allowed to be taken by the remaining available TS7700 Clusters in the Grid. Full access is allowed.

The Autonomic Ownership Takeover Manager:

The Autonomic Ownership Takeover Manager (AOTM) is a method by which either Read-Only Takeover (ROT) or Write-Only Takeover (WOT) can be automatically enabled against a failed TS7700 Cluster through internal negotiation methods. AOTM is optionally configurable.

When communication between two or more TS7700 clusters is disrupted, the clusters (local and remote) are no longer able to negotiate ownership of virtual volumes. In this scenario, ownership takeover, or human intervention, is sometimes utilized to establish temporary access to data resources. Ownership takeover occurs when an operator, working with the knowledge that one cluster is in a failed state, physically intervenes to obtain permission to access that cluster's data. When network problems cause a communication failure, ownership takeover is not the correct solution to reestablish access.

One solution is an automated process (AOTM) that permits a local cluster to access data from a remote cluster if normal communication is interrupted. Communication between clusters can be interrupted by a failure of the Grid Network, or by failure of a cluster. Since data can be lost or compromised if a local cluster is allowed to access data from a working remote cluster, AOTM only automatically grants a local cluster permission access to a remote cluster when normal communication between the clusters is disrupted and the local cluster can verify that the remote cluster is offline or otherwise not operating.

Notelist:

1. Ownership takeover, including ROT, WOT, and AOTM, should only be enabled when the TS7700 Cluster in question has actually failed. If communication is only interrupted via a network failure, a takeover mode should not be enabled. AOTM attempts to distinguish between a cluster failure and a network failure.
2. The minimum required TS7700 microcode level to enable AOTM is 8.0.1.xx.

   Ask your IBM service representative to receive the most current level of TS7700 code.

Before AOTM intervenes to allow a working cluster access to data from a remote cluster, it must determine whether the remote cluster is inaccessible due to failure of the cluster itself or failure of the Grid network. AOTM does this by sending a status message across a network connecting the Master Consoles associated with the clusters. This network is referred to as the Master Console Grid Network and illustrated by the following figures.

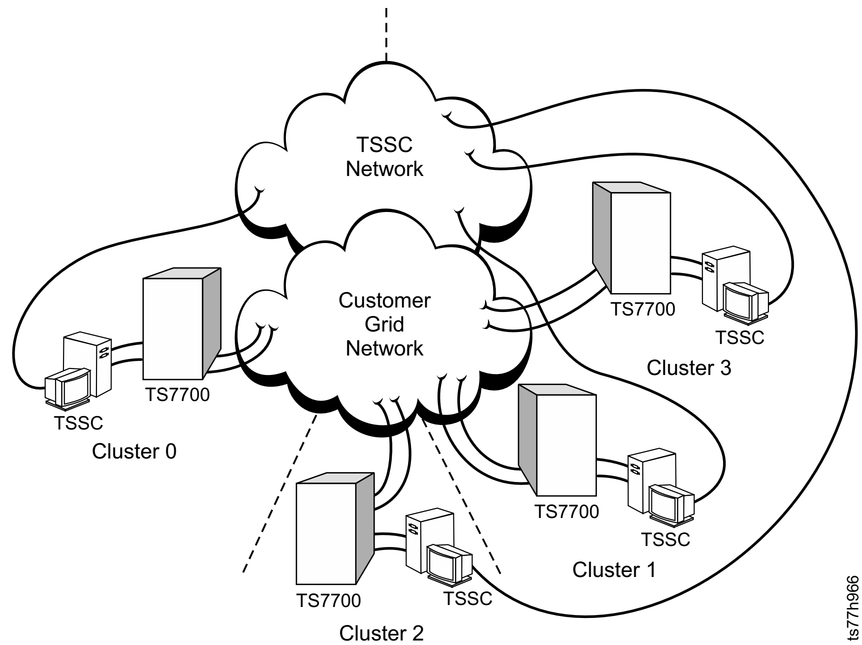


Figure 43. Autonomic Ownership Takeover Manager configuration for four clusters

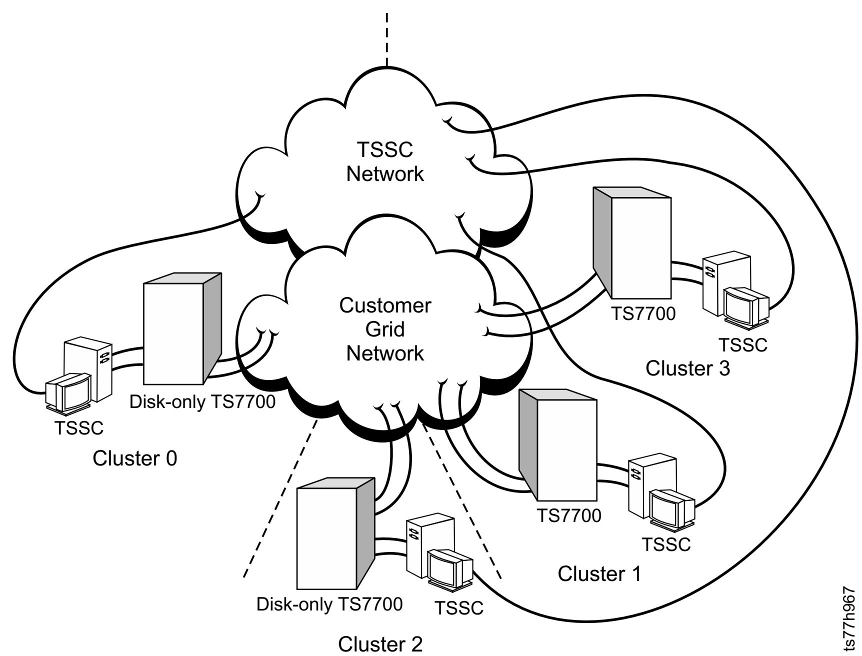


Figure 44. Autonomic Ownership Takeover Manager configuration for four clusters in a hybrid grid

If a working cluster in a TS7700 Grid is unable to process transactions with a remote cluster because communication with the remote cluster has been lost, the local cluster starts an AOTM grace period timer. When the grace period configured by you expires, the AOTM cluster outage detection process is initiated. The local cluster communicates with the local Master Console, which then forwards a request to a remote Master Console. The remote Master Console then attempts to communicate with the remote cluster. Only when the remote Master Console request returns and agrees that the remote cluster has failed is the configured takeover mode enabled. When enabled, access to data that is owned by the failed cluster is allowed by using the enabled takeover mode.

Conditions required for takeover

When AOTM is enabled on multiple systems in a TS7700 Grid environment, takeover occurs when one TS7700 Cluster fails if all TSSC system consoles attached to the TS7700 Clusters remain in communication with one another.

Note: To complete the communication path between TS7700 Clusters, each TSSC system console must have a designated IP address.

Figure 45 illustrates AOTM as configured on a three-cluster Grid. In an optimal situation, WAN1 and WAN2 would reside on different physical networks. Any outage within WAN1 might appear as a TS7700 Cluster outage. This failure can be validated through WAN2 with the help of the TSSCs. If the secondary TSSC path shows the TS7700 Cluster to be available, then the failure can be isolated to the network. If both TSSCs show the TS7700 Cluster as unavailable, then it is safe to assume that the TS7700 Cluster is in a failed state.

Note: Each TS7700 Cluster requires a **regionally local** TSSC. However, clusters in a TS7700 Grid can share a TSSC and AOTM is supported with a single, shared TSSC when the clusters are in close proximity.

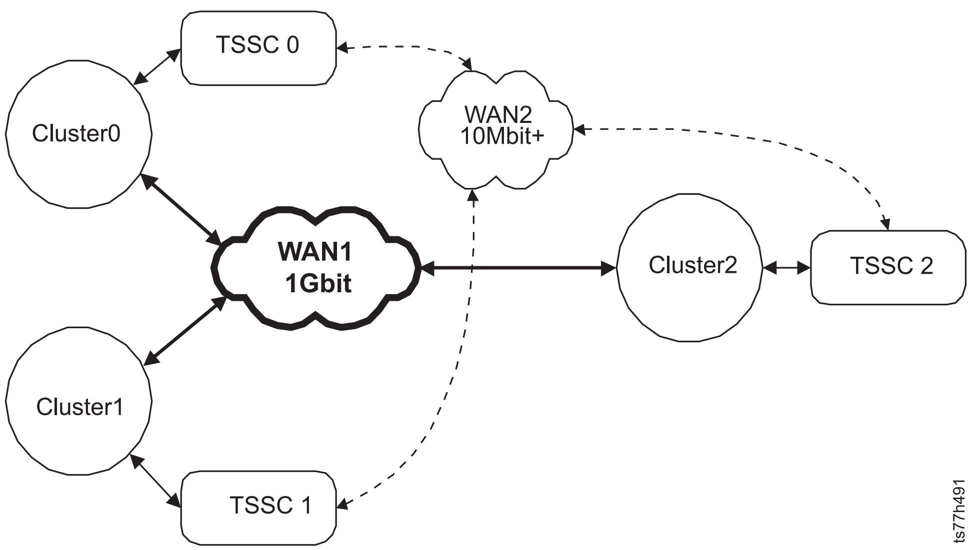


Figure 45. Autonomic Ownership Takeover Manager configuration in a three-cluster Grid

Table 91 displays the conditions under which AOTM takes over a failed cluster.

Table 91. Conditions under which AOTM takes over a failed cluster

Remote cluster appearance	Remote cluster actual state	Does present third peer recognize cluster as down?	Status of Grid links	Status of links between local TSSC and local cluster	Status of links between remote TSSC and remote cluster	Status of links between TSSCs	Notes
Down	Down	Yes	Not applicable	Connected	Connected	Connected	

Table 91. Conditions under which AOTM takes over a failed cluster (continued)

Remote cluster appearance	Remote cluster actual state	Does present third peer recognize cluster as down?	Status of Grid links	Status of links between local TSSC and local cluster	Status of links between remote TSSC and remote cluster	Status of links between TSSCs	Notes
Down	Down	Yes	Not applicable	Connected	Down	Connected	
Down	Online	Not present	Down	Connected	Down	Connected	Cluster is assumed down since last network path is down.
Down	Offline	Yes	Not applicable	Connected	Not applicable	Connected	

Table 92 displays the conditions under which AOTM does **NOT** takeover a failed cluster.

Table 92. Conditions under which AOTM does not takeover a failed cluster

Remote cluster appearance	Remote cluster actual state	Does present third peer recognize cluster as down?	Status of Grid links	Status of links between local TSSC and local cluster	Status of links between remote TSSC and remote cluster	Status of links between TSSCs	Notes
Down	Down	Yes/not present	Not applicable	Connected	Not applicable	Down	
Down	Down	Yes/not present	Not applicable	Down	Not applicable	Not applicable	
Down	Online	No	Down	Not applicable	Not applicable	Not applicable	Third cluster prevents takeover
Down	Online	Not present	Down	Connected	Connected	Connected	
Down	Offline	Yes	Not applicable	Down	Not applicable	Down	Takeover not enabled if TSSC is not present or accessible
Down	Offline	Yes	Not applicable	Connected	Not applicable	Down	Takeover not enabled if TSSC is not present or accessible

Differences between forms of takeover

AOTM is not the only form of ownership takeover that can be employed in the event of a system failure. The following descriptions of *Service Ownership Takeover*

(SOT), *Read Only Takeover/Write Only Takeover* (ROT / WOT), and AOTM are provided to avoid confusion when discussing options for ownership takeover.

SOT
SOT is activated during normal operating conditions prior to bringing a system offline for upgrade, maintenance, or relocation purposes. A TS7700 Cluster in the SOT state surrenders ownership of all its data and other TS7700 Clusters in the Grid may access and mount its virtual volumes.

ROT / WOT
ROT / WOT is employed when a TS7700 Cluster is in the failed state and cannot be placed in SOT, or Service mode. In this state, the virtual volumes that belong to the failed TS7700 Cluster cannot be accessed or modified. You must use the TS7700 Management Interface from an active TS7700 Cluster in the Grid to establish ROT / WOT for the failed TS7700 Cluster.

AOTM represents an automation of ROT / WOT. AOTM makes it unnecessary for a user to physically intervene through the TS7700 Management Interface to access data on a failed TS7700 Cluster. AOTM limits the amount of time that virtual volumes from a failed TS7700 Cluster are inaccessible and reduces opportunities for human error while establishing ROT / WOT.

Synchronous mode copy:

Use synchronous mode copy to enable tape synchronization across two clusters within a grid configuration.

Refer to the glossary for definitions of terms used in the following paragraphs.

Synchronous mode copy is a form of replication similar to host-initiated duplexing that provides a zero recovery point objective (RPO) for sets of records (data sets) or byte-stream data (objects) written to virtual tape. IBM Z® applications like DFSMShsm, DFSMSdfp OAM Object Support, and other workloads can achieve a zero RPO when using this method of replication. When zero RPO is achieved, any exposure to delayed replication is eliminated and host-initiated duplexing is not required.

Synchronous mode copy duplexes all compressed host writes simultaneously to two library locations. Before any host-initiated explicit or implicit synchronize tape operation can succeed, all content written on virtual tape up to that point is written to persistent disk cache at both library locations. If a cluster fails, the host application or job can access the secondary copy with consistent access up to the last completed synchronization point. No disk cache read is necessary to replicate the written content since all writes are duplexed. This reduces the overhead on the disk cache repository. Additional options enable a user to enforce strict synchronization for a given workload, or permit a write workload to enter a synchronous-deferred state when full synchronization is not possible.

Applications such as DFSMShsm and DFSMSdfp OAM Object Support often store data sets or objects on virtual tape. Then, the host application issues an explicit synchronize operation that forces all previously written records to tape volume cache (TVC). Finally, the host application then classifies the data set or object as written to tape and discards the primary host source copy before the volume is closed.

Note: Applications that use data set-style stacking and migration are the expected use case for synchronous mode copy. However, any host application that requires near-zero RPOs can benefit from the synchronous mode copy feature. There is no host software dependency other than the ability to issue an implicit or explicit synchronize command after critical data has been written. The synchronous mode copy or duplexing occurs external to the IBM Z® server, within the TS7700, and relies entirely on the TS7700 Grid network. No FICON channel activity occurs to the secondary duplexed location.

Supported configurations

All clusters in a grid must operate at microcode level 8.21.0.xx or later to use synchronous mode copy. To enable synchronous mode copy, create a management class that specifies exactly two grid clusters with the synchronized ("S") copy mode. Synchronous mode copy is configured using the following construct options on the *Management Class* panel of the TS7700 Management Interface:

Synchronous Mode Copy Settings

These settings specify how the library or virtual tape drive operates when the two "S" locations are not synchronized, and whether the library opens the volume on both TVC clusters when a private mount occurs. These options are available only when synchronous mode copy is enabled.

Default Settings

By default, the synchronous-mode-copy clusters fail mount and tape operations if two copies of a volume cannot be maintained during an update (synchronous failure). When the synchronous failure setting is used, a zero RPO is provided for the target workload, independent of failures. Consider the following circumstances when using the default strict synchronization behavior include:

- If the failure to synchronize is detected after the mount has already occurred, then tape operations fail to the targeted volume until a RUN occurs and a demount command is issued.
- If content was written prior to the synchronization failure, then previous content on the emulated volume *up to the last successful tape synchronization operation point* is considered persistently synchronized and can be accessed later from either "S" consistency point.
- If either "S" consistency point is unavailable, then scratch mount operations fail.

Synchronous Deferred On Write Failure

Enable this option to permit update operations to continue to any valid consistency point in the grid. If there is a write failure the failed "S" locations are set to a state of "synchronous-deferred". After the volume is closed, any synchronous-deferred locations are updated to an equivalent consistency point through asynchronous replication. If the **Synchronous Deferred On Write Failure** option is not checked and a write failure occurs at either of the "S" locations, then host operations fail.

Note: An "R", "D," or "T" site is chosen as the primary consistency point only when both "S" locations are unavailable.

On Private Mount: Always open single copy

By default, synchronous mode copy opens only one TVC during a private mount. The best TVC choice is used to satisfy the mount. The best TVC choice selection is made with location preferences in this order: synchronized ["S"], RUN ["R"], deferred ["D"], and time-delayed ["T"]. If a write operation occurs, the job enters the synchronous-deferred state regardless of whether the *Synchronous Deferred On Write Failure* option is enabled.

On Private Mount: Always open both copies
Enable this option to open both previously written "S" locations when a private mount occurs. If one or both "S" locations are on back end tape, the tape copies are first recalled into disk cache within those locations. The **Always open both copies** option is useful for applications that require synchronous updates during appends. Private mounts can be affected by cache misses when this option is used. Other circumstances to consider include:

- If a private mount on both locations is successfully opened, then all read operations use the primary location. If any read fails, then the host read also fails and no failover to the secondary source occurs unless a z/OS DDR swap is initiated.
- If a write operation occurs, both locations receive write data and must synchronize it to TVC disk during each implicit or explicit synchronization command.
- If either location fails to synchronize, the host job either fails or enters the synchronous-deferred state, depending on whether the *Synchronous Deferred On Write Failure* option is enabled.

On Private Mount: Open both copies on z/OS implied update
Open both previously written "S" locations only when requested by the host to do so. This takes place when the mount request from the host has either *write from BOT* or *update intent* specified.

Table 93 displays valid combinations of the options and mount types and what happens when one or both "S" locations do not exist at mount time.

Table 93. Expected results when one or both "S" locations are unavailable at mount time

Scenario	Mount type	Synch Deferred On Write Failure	On Private Mount			Dual opened?	Mount delay if either or both "S" are paused or out of physical scratch[1]	Results when one or both "S" locations are unavailable at mount time[2]			
			Always open single copy	Always open both copies	Open both copies on z/OS implied update			Mount result	Enter synch defer on mount finish	Fail when write received	Enter synch defer when write received
1	Scratch	Disabled	N/A	N/A	N/A	Both	Yes	Failure	No	N/A	N/A
2	Scratch	Enabled	N/A	N/A	N/A	Both	Yes	Success[3]	No	No	Yes
3	Private	Disabled	N/A	Set	N/A	Both	Yes	Success[3]	No	Yes	No
4	Private	Enabled	N/A	Set	N/A	Both	Yes	Success[3]	No	No	Yes
5	Private	Disabled	N/A	N/A	Set	Both[4]	Yes[5]	Success[3]	No	Yes[5 7]	No[6]
6	Private	Enabled	N/A	N/A	Set	Both[4]	Yes[5]	Success[3]	No	No	Yes
7	Private	Disabled	Set	N/A	N/A	Single	No	Success[3]	No	No	Yes
8	Private	Enabled	Set	N/A	N/A	Single	No	Success[3]	No	No	Yes

Table 93. Expected results when one or both "S" locations are unavailable at mount time (continued)

Notelist:
1. Any delay due to a paused state is applicable only if a recall is required.
2. Assumes at least one healthy (and consistent for private mount) cluster when both 'S' locations are unavailable.
3. The best TVC choice (preferring locations in this order: "S", "R", "D", and "T") is used to satisfy the mount before it continues.
4. With *Open both copies on z/OS implied update* specified: Both when requested by the host; Single when not requested by the host.
5. With *Open both copies on z/OS implied update* specified: Yes when requested by the host; No when not requested by the host.
6. With *Open both copies on z/OS implied update* specified: No when requested by the host; Yes when not requested by the host.
7. The library always enters the synchronous-deferred state independent of whether the *Synchronous Deferred On Write Failure* option is specified.

Primary "S" selection

One location is identified as the primary when both "S" locations are available. The primary location receives all inline host operations and can only buffer read and write operations when remote. All implicit or explicit synchronization operations are sent to the primary location first, then to the secondary location when available. The local cluster always takes precedence over remote clusters for primary identification. If both "S" locations are remote, the "S" location within the same cluster family takes precedence. If both "S" locations are within the same family or are external to the mount-point family, then the existing performance-based and latency-based selection criteria is used. If only one "S" location is available, it takes precedence over all "R", "D", and "T" locations. If neither "S" location is available, the "R", then "D", then "T" locations take precedence. All read operations are always sent to the primary location. If a read fails at any time when two instances of a volume are open, the read does not failover to the secondary location and the host command fails.

Synchronous-deferred state

If one or both "S" locations are not in an active, synchronized state and a write operation is permitted to continue, the distributed library enters the synchronous-deferred state. The distributed library remains in this state until all "S" copies managed by the distributed library are replicated using an alternative method. The "S" copies managed by the distributed library are those that were initiated through mounts targeting the distributed library. If one or more distributed libraries enter the synchronous-deferred state, the composite library also enters this state. The composite library exits this state when no distributed libraries are in the synchronous-deferred state. The priority of the synchronous-deferred copy is one level above immediate-deferred.

Use with other functions

Scratch mount candidates
There is no direct association between the scratch mount candidates and clusters that are enabled with synchronous mode copy. If neither of the "S" locations are identified as scratch mount candidates, then they are not included in the candidate list that is returned to the host.

Copy policy override
The synchronous copy mode takes precedence over any copy override settings. If the **force local copy** policy override is selected on a cluster with the **No Copy** copy mode selected, the copy policy override is ignored and up to two clusters are selected as TVC.

Related information

Physical volume data

The following features describe data stored on physical volumes.

Automated read-only recovery

Automated read-only (RO) recovery is the process by which hierarchical storage management (HSM) recalls all active data from a particular physical volume that has exceeded its error thresholds, encountered a permanent error, or is damaged.

Some HSM functions such as reclaim or secure data erase will designate a physical volume as RO for recovery. HSM requires that a certain number of drives be available for a period of time before RO is allowed to proceed. At least one drive must be free for five minutes, or two drives must be free for any period of time. If either of these criteria is not met, HSM will defer the RO recovery of that physical volume to the next hourly cycle.

In a TS7700 Grid configuration, if a virtual volume cannot be recovered from the RO volume and a valid copy exists on another TS7700 Cluster, the remote virtual volume will be copied to the cluster performing the recovery and afterwards migrated to another physical volume. In this way, the previously unrecoverable copy is recovered. If the virtual volume cannot be recovered, an intervention is reported.

Allocation assistance

Tape library performance can be increased by using allocation assistance to identify the subset of available clusters best suited for a given allocation (mount) request.

Device allocation assistance

Device allocation assistance (DAA) is a function that allows the host to query the TS7700 to determine which clusters should be preferred for a private (specific) mount request. When enabled, DAA returns to the host a ranked list of clusters (the preferred cluster is listed first) that determines for a specific VOLSER which cluster is best to use for device allocation.

DAA is available, and is enabled by default, when all clusters in the grid have a microcode level of 8.5.0.xx or later. When all clusters in the grid have a microcode level of 8.20.0.xx or later, DAA can be disabled by using the following LIBRARY REQUEST command:

```
LIBRARY REQUEST,library-name,SETTING,DEVALLOC,PRIVATE,[ENABLE|DISABLE]
where library-name = composite-library-name
```

The selection algorithm orders the clusters first by those having the volume already in cache, then by those having a valid copy on tape, and then by those without a valid copy. If the mount is directed to a cluster without a valid copy, then a remote mount is the result. Thus, in special cases, even if DAA is enabled remote mounts and recalls can still occur.

Scratch allocation assistance

Scratch allocation assistance (SAA) is an extension of the DAA function for scratch mount requests. SAA filters the list of clusters in a grid to return to the host a smaller list of candidate clusters specifically designated as scratch mount candidates. By identifying a subset of clusters in the grid as sole candidates for scratch mounts, SAA optimizes scratch mounts to a TS7700 Grid.

A cluster is designated as a candidate for scratch mounts using the Scratch Mount Candidate option on the management class construct, accessible from the TS7700 Management Interface (refer to the *Management Classes* topic in the **Related information** section for additional information about the management class construct). Only those clusters specified through the assigned management class are considered for the scratch mount request. When queried by the host preparing to issue a scratch mount, the TS7700 considers the candidate list associated with the management class, along with cluster availability. The TS7700 then returns to the host a filtered, but unordered, list of candidate clusters suitable for the scratch mount operation. The z/OS allocation process then randomly chooses a device from among those candidate clusters to receive the scratch mount. If all candidate clusters are unavailable or in service, all clusters within the grid become candidates. In addition, if the filtered list returns clusters that have no devices that are configured within z/OS, all clusters in the grid become candidates.

In a hybrid configuration, the SAA function can be used to direct certain scratch allocations (workloads), to one or more TS7720s or TS7760s for fast access, while other workloads can be directed to TS7740s for archival purposes.

Before SAA is visible or operational, all of the following must be true:

1. All clusters in the grid have a microcode level of 8.20.x.x or later and the necessary z/OS host software support is installed. Refer to Authorized Program Analysis Report (APAR) OA32957, at the Techdocs Library link in the **Related information** section for additional information.
2. The z/OS environment uses Job Entry Subsystem (JES) 2.

   Note: JES3 does not support DAA or SAA for JES3 systems running on release levels earlier than z/OS V2R1. With z/OS V2R1, JES3 supports DAA and SAA. Refer to the OAM Planning, Installation, and Storage Administration Guide for Tape Libraries for details on the JES3 support.
3. SAA is enabled with the host Library Request command by using the following LIBRARY REQUEST command:

   ```
   LIBRARY REQUEST,library-name,SETTING,DEVALLOC,SCRATCH,[ENABLE|DISABLE]
   where library-name = composite-library-name
   ```

   Disabled is the default setting.
4. An adequate number of devices connected to the scratch mount candidate clusters are online at the host.

   Note: If the clusters are online, but too few or no devices are online at the host, jobs that use SAA can go into allocation recovery. In allocation recovery, the existing MVS allocation options for device allocation recovery (`WTOR|WAITHOLD|WAITNOH|CANCEL`) are used. If all or many devices associated with the candidate clusters need to be taken offline, as when servicing a cluster, then SAA should first be disabled by using the host Library Request command. Thus, other clusters in the grid can be used for SAA during the outage. Alternatively, you can extend the list of candidate clusters to include clusters that have devices remaining online at the host during the outage. Use the management class construct to extend the list of candidate clusters.

Related information

"Retain Copy Mode" on page 273

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/Web/Techdocs

Selective device access control

This topic provides information about use of selective device access control in a TS7700 Grid configuration.

Selective device access control (SDAC) allows exclusive access to one or more VOLSER ranges by only certain logical control units or subsystem IDs within a composite library for host-initiated mounts, ejects, and changes to attributes or categories.

You can use SDAC to configure hard partitions at the LIBPORT-ID level for independent host logical partitions or system complexes. Hard partitioning prevents a host logical partition or system complex with an independent tape management configuration from inadvertently modifying or removing data owned by another host. It also prevents applications and users on one system from accessing active data on volumes owned by another system.

SDAC is enabled by using FC 5271, Selective device access control. For more information about this feature, see the topic *Feature details* in the **Related information** section. Each instance of this feature enables definition of eight SDAC groups, excluding the default group. This feature license key must be installed on all clusters in the grid before SDAC is enabled.

Important: If a cluster is to be joined to a grid that has SDAC enabled, the feature key must be installed on the joining cluster before the join is attempted. Otherwise, SDAC can be disabled on the grid when the join occurs.

You can specify one or more LIBPORT-IDs per SDAC group. Each access group is given a name and assigned mutually exclusive VOLSER ranges. Use the *Library port access groups* panel on the TS7700 Management Interface to create and configure library port access groups for use with SDAC. Access control is imposed as soon as a VOLSER range is defined. As a result, selective device protection applies retroactively to pre-existing data.

When using library port access groups on a system where both FC 5271 (SDAC) and FC 5275 (add virtual devices) are in use, you must define separate SDA groups for each and modify their defaults accordingly.

Host controls

An integral part of the function is the control of the input-output definition file (IODF) configuration on the host that controls which devices can be used by the various host partitions. The host IODF configuration activity needs to be access controlled (i.e. remote access control file [RACF]) to assure devices adhere to the hard partitioning definition. Restricted access to the MI (Management Interface) panels that control the definition of the access groups and configuring them to the volser ranges is also required to assure security.

For a host services and storage service provider, it is assumed that the provider owns the hosts and the storage so that the configuration can be controlled by the above protection.

Depending on the model and installed features there is a minimum of 16 and a maximum of 31 logical control units in each cluster giving a maximum of 496 devices per cluster. Library port IDs from each cluster in a Grid should be included in an access group for high availability access and for disaster recover testing. You are allowed to define 50 volser ranges. Each volser range needs to be a unique set of volumes, which means there can be no overlap between ranges. New volumes that are inserted which are not covered by an existing volser range will be covered by the default access group until a valid volser range is defined for it. The volser ranges and access group panel can be provided only if the feature is installed on all clusters within the Grid.

The access control is imposed as soon as an access group is assigned to a volser range. This allows all pre-existing data to be retroactive with respect to selective device access control protection.

Expected configuration and use scenarios

The main goal of the configuration phase is to setup independent sysplexes that are hard partitioned for devices, volumes and scratch categories. Sharing any three of these items across sysplexes is not supported.

- The customers that use this function have 2 to 8 sysplexes installed, all running independent instances of tape management software. This means that they do not share common TCDB databases.
- Each sysplex defines its own set of ranges of virtual volumes and associate each range to the corresponding sysplex group name. Therefore, any one volume should only be defined within one of the up to 8 sysplexes.
- Each sysplex defines its own scratch category that must be unique to its sysplex.
- Each sysplex has exclusive access to one or more LIBPORT-IDs within the TS7700. Each sysplex should only configure the LIBPORT-IDs that it anticipates using and therefore, only the devices associated with these LIBPORT-IDs are varied on.
- An access group for each sysplex should be defined. Each access group definition then has only the LIBPORT-IDs defined within it that correspond to the LIBPORT-IDs configured for that sysplex. Overlap between sysplexes and therefore storage group name LIBPORT-ID definitions is not expected, except when sysplex volume sharing is necessary.
- Access group names should be created with LIBPORT-IDs along with the SDAC volser ranges at the TS7700.
- As volumes are inserted into the TS7700, only the sysplex that has a corresponding volume range definition processes the volumes and moves them into its independent scratch category.

Once configured, the following items are examples of usage requirements.

- Any attempt of one sysplex to access private volumes of another sysplex or attempt to manipulate their properties should fail.
- Any attempt of one sysplex to issue a scratch mount to a category that does not contain volumes that can be accessed by the device should fail. Thus, independent scratch categories are required.
- Any accidental or malicious manual volume configuration in one sysplex that overlaps another sysplex should not cause any harm. It is not possible to:
  - Manipulate the other sysplexes private volumes or scratch volumes
  - Return to scratch the other sysplex's private volumes
  - Eject another sysplex's volumes

- Move another sysplex's volumes into any scratch category and then proceed to Eject the volumes
- If a sysplex wants to surrender a volume range to another sysplex, perform the following:
  - Undefine them at sysplex A
  - Define them at sysplex B
  - Change the access group on the SDAC volser range to allow sysplex B devices to access the volumes
  - Or, define a common or shared group name

Related information

"Feature details" on page 149

Circumstances of a job failure

A job failure can result from failure of the TS7700 or of a link between TS7700 Clusters.

Failure of a TS7700

A failure of a TS7700 causes any job using that virtual device addresses to fail. The job also fails if the failed cluster is the one sourcing the data "remote TVC". To re-run the jobs, host connectivity to the virtual device addresses in another TS7700 must be enabled and an appropriate ownership takeover mode selected. If the other TS7700 has a valid copy of a virtual volume, the jobs can be retried.

Remote mount IP link failover

If a grid link fails during a remote mount the Remote Mount IP Link Failover function attempts to reestablish the connection through an alternate link. During a failover, up to three more links are attempted. If all four link connections fail, the remote mount fails, resulting in a host job failure or a synchronous mode copy break. When Synchronous Mode Copy is in use and one or both "S" sites incur a TCP/IP link failure, this intelligent failover function recovers by using an alternate link. The following restrictions apply:

- Every cluster in the grid must operate using a microcode level of 8.21.0.xx or later.
- At least two grid connections must exist between clusters in the grid (either two or four 1 Gbps grid links or two 10 Gbps grid links).

Related information

"Synchronous mode copy" on page 286

Configuring for disaster recovery

This topic provides planning information for a TS7700 Grid configuration to be used specifically for disaster recovery (DR) purposes.

In a grid configuration that supports DR, TS7700 Clusters reside in different locations, should a natural or human-caused event render the production TS7700 Cluster unavailable. Production and DR clusters are separated by a distance that is dictated by DR requirements established by your company.

Note: Refer to "TS7700 Grid" on page 257 for guidelines that pertain to geographic location of TS7700 Clusters in a TS7700 Grid configuration.
Only the TS7700 Grid interconnection and the TSSC network connect the local site

to the DR site. No host connectivity exists between local hosts and the FICON channels on the TS7700 at the DR site. As part of planning a TS7700 Grid configuration to address this solution, you must consider the following:

- Plan for the necessary WAN infrastructure and bandwidth to meet the copy requirements that you need. You generally require more bandwidth if you are primarily using a copy consistency point of RUN since any delays in copy time caused by bandwidth limitations result in an elongation of job run times. If you have limited bandwidth available between sites, use the deferred copy consistency point or copy only the data that is critical to the recovery of your key operations.
- Plan for backup host connectivity at your DR site with sufficient resources to perform your critical workloads.
- Design and code the Data Facility System Managed Storage (DFSMS) Automatic Class Selection routines to control what data gets copied and by which copy consistency point.
- Prepare procedures that your operators would execute if the local site became unusable. The procedures would include such tasks as bringing up the DR host, varying the virtual drives online, and enabling one of the ownership takeover modes against the failed primary TS7700 Cluster.

You can test DR preparedness by emulating DR events and performing test operations at a TS7700 Grid DR site.

Flash Copy for disaster recovery

The Flash Copy function is an LI REQ operation performed at the host that groups one or more clusters into a disaster recovery (DR) "family”. The DR family contains all the clusters in a DR site or sites and can be used to test DR preparedness.

Note: DR families should not be confused with *Cluster Families*.

To use Flash Copy for DR, configure “DR Families” via LI REQ at the host, then enable write protect or flash from the LI REQ command against all clusters in a DR family. Write protection is enabled across all clusters in a DR family, which permits them to move to the write protected state at the same time.

When the volume repository for all TS7720 and TS7760 Clusters in a DR family are flash copied a snapshot (flashed instance) is created for all content in that repository. Changes that occur to volumes after the snapshot is created are updated in the live file system, while the original files remain unchanged and in the read-only state. This function is carried out among all TS7720 and TS7760 Clusters in a DR family at the same time, which is referred to as "time zero". The snapshot process does not duplicate data, manages only two instances of each file. When a snapshot is created, changes to files are saved as a delta. Each subsequent host access references either the live version or the snapshot version, based on the selective write protect state. Host mounts to write-protected volumes access the snapshot, while volumes excluded from write protect access live data.

Restrictions:

- Clusters in a DR family are assumed to remain operational in the event of a production outage.
- Though a TS7700 Tape Attach Cluster can exist in a DR family, volumes in migrated state that belong to a TS7700 Tape Attach Cluster are not flash copied.

- For a TS7720 or TS7760 Tape Attach Cluster the flash copy will be performed only for the cache partitions. Volumes cannot be flash copied to physical tapes.
- If no cluster has a valid copy at time zero within the DR family, the DR host mount fails.
- Tape Volume Cache selection of snapshot data is limited only to those clusters in the DR family.
- Snapshot data within a DR family is not replicated to peer DR family clusters. However, a mount to a write protected volume at the DR cluster creates a DR instance of ownership that is exchanged among peer clusters in a DR family. This allows DR host mounts and live production mounts to occur in parallel.
- If a TS7700 Tape Attach Cluster exists in the DR family, its live content can be accessed only if no TS7700 Cluster in the DR family has a snapshot instance and the TS7700 Tape Attach Cluster is shown to have had a copy before time zero. You must invoke an LI REQ command to enable the use of the live copy before starting the mount operation. This step permits the microcode to access live content on the TS7700 Tape Attach Cluster in the DR family.
- Volume removal is supported within flashed TS7700 Clusters, but the HSM component of the TS7700 must initiate the removal of the Flash Copy instances of that file. Delete-expired volumes are deleted in the flash snapshot only if that option is set to TRUE using the LI REQ command. Deleting data within the flash snapshot too early can cause the DR test to fail given the volumes are still viewed as private and accessible within the DR host-plex. Removal of a file from a snapshot is not supported; after the DR test completes, the volume flash is dissolved through a single LI REQ command.

Related information

"Hybrid TS7700 Grid configurations" on page 258
A hybrid TS7700 Grid is one that contains an intermix of one or more TS7700 tape-attach Clusters and one or more TS7700 disk-only Clusters that are configured together within the same grid.

Selective write protect for disaster recovery

The selective write protect function that is configured through the *Write Protect Mode* panel on the TS7700 Management Interface creates categories that are excluded from write protection on a cluster. You can use this function to test disaster recovery (DR) preparedness.

You can use selective write protect during a DR test when a recovery host that is connected to a non-production cluster must access and validate production data without any risk of modifying it.

When Write Protect Mode is enabled on a cluster, host commands fail if they are issued to virtual devices in that cluster and attempt to modify a volume's data or attributes. Meanwhile, host commands that are issued to virtual devices in peer clusters are allowed to continue with full read and write access to all volumes in the library. A cluster can be placed into Write Protect Mode only if the cluster is online. When set, the mode is retained through intentional and unintentional outages and can be disabled only through the same management interface panel that is used to enable the function. When a cluster within a grid configuration has Write Protect Mode enabled, standard grid functions such as virtual volume replication and virtual volume ownership transfer are unaffected.

Related information

"Hybrid TS7700 Grid configurations" on page 258
A hybrid TS7700 Grid is one that contains an intermix of one or more TS7700

tape-attach Clusters and one or more TS7700 disk-only Clusters that are configured together within the same grid.

Configuring for high availability

This topic provides information that is needed to plan for a TS7700 Grid configuration to be used specifically for high availability.

The assumption is that continued access to data is critical and no single point of failure, repair, or upgrade can be allowed to impact the availability of data. In a high availability configuration, two or more TS7700 Clusters are in close proximity to one another at the same site. The TS7700 Clusters are connected through a LAN. If one of the TS7700 Clusters becomes unavailable because it has failed, is undergoing service, or is being updated, data can be accessed through another TS7700 Cluster until the original TS7700 Cluster is again available. As part of planning a TS7700 Grid configuration to address this solution, you must consider the following:

- Plan for the virtual device addresses in the clusters to be configured to the local hosts. In this way, a total of 1024 virtual tape devices (256 from each TS7700 Cluster) are available for use.
- Set up a copy consistency point of RUN for all data to be made highly available. With this copy consistency point, as each virtual volume is closed it is copied to another TS7700 Cluster.
- Design and code the data facility system managed storage (DFSMS) Automatic Class Selection routines to set the necessary copy consistency point.
- Design and code the DFSMS Automatic Class Selection routines to control what data gets copied and by which copy consistency point.
- Prepare procedures that your operators would execute if one of the TS7700 Clusters becomes unavailable. The primary task is to enable an ownership takeover mode against a failed TS7700 Cluster to maintain continued access to data owned by the failed TS7700 Cluster.

Configuring for both disaster recovery and high availability

This topic provides information that is needed to plan for a TS7700 Grid configuration to be used for disaster recovery and high availability.

It is possible to configure a TS7700 Grid to provide for both disaster recovery and high availability solutions. The assumption is that two or more TS7700 Clusters reside in different locations, separated by a distance dictated by your company's requirements for disaster recovery. In a three-cluster or four-cluster grid configuration, disaster recovery and high availability can also be achieved simultaneously by ensuring:

- Two local, high availability clusters possess RUN volume copies and have shared access to the host
- The third and fourth remote clusters possess deferred volume copies for disaster recovery

Note: Refer to "TS7700 Grid" on page 257 for guidelines that pertain to geographic location of TS7700 Clusters in a TS7700 Grid configuration.

In addition to the considerations for configuring for disaster recovery, you must plan for:

- Access from your local site's hosts to the FICON channels on the TS7700 Cluster at the disaster recovery site(s). This may involve connections that use dense wavelength-division multiplexing (DWDM) or channel extension equipment, depending on the distance that separates the sites. If the local TS7700 Cluster becomes unavailable, you would use this remote access to continue your operations by using a remote TS7700 Cluster.

- Differences in read or write performance as compared to the virtual devices on the local TS7700 Cluster. These can occur because the virtual devices on a remote TS7700 Cluster are connected to the host through channel extensions. If performance differences are a concern, when the local TS7700 is unavailable consider using only the virtual device addresses in a remote TS7700 Cluster. If performance differences are an important consideration, provide procedures both for ownership takeover and for an operator to vary the virtual devices in a remote TS7700 from online to offline.
- Creation of separate copy consistency policies for disaster recovery data and data that requires high availability.

Chapter 4. Security

The topics in this section provide information about security protocols for the TS7700.

LDAP and role-based access control

Role-based access control (RBAC) is a general security model that simplifies administration by assigning roles to users and then assigning permissions to those roles. Lightweight Directory Access Protocol (LDAP) is a protocol to implement an RBAC methodology.

The TS7700 supports RBAC through the System Storage Productivity Center or by native LDAP by using Microsoft Active Directory (MSAD) or IBM's Resource Access Control Facility (RACF).

Note: You can create a direct LDAP policy only when every cluster in the grid operates at a microcode level of 8.30.x.x or later.

Configuring for service personnel access when LDAP is enabled

If LDAP is enabled, it is important to create at least one external authentication policy to permit access by an IBM service representative.

About this task

Before a service event, create at least one external authentication policy for IBM service personnel access. Use these instructions to create a policy for service personnel access. IBM service representatives can operate locally or remotely. You can create different LDAP policies and assigned custom roles for local and remote IBM service representatives, which are based on how those personnel access the machine and what permissions they require.

Important: By default, when LDAP is enabled, the TS7700 can be accessed only through the LDAP server with a valid user ID and password combination. All local and remote access to the TS7700 is controlled through secured (encrypted) or plain text authentication. If the LDAP server is not accessible, the TS7700 is not accessible. Therefore, it is recommended that you allow IBM service personnel to connect without LDAP credentials, as described in the following steps.

Procedure

1. Create a Direct LDAP policy for IBM service personnel.
   a. On the management interface, go to **Access** > **Security Settings**.
   b. Select **Add Direct LDAP Policy** from the **Select Action** drop-down list.
   c. Click **Go**.
   d. Check the options you want to enable for IBM Service Representative access. These settings become active only when the associated policy is assigned to a cluster. You can check both options. These options are not visible if the grid contains a cluster operating at microcode level of 8.30.0.xx or earlier.

Important: These options permit IBM Service Representatives to access a cluster as if no external (SAS or LDAP) policy was in force. When enabled, they create a mechanism by which an IBM Service Representative can reset an authentication policy to resolve a lockout scenario. If no option is checked, IBM Service personnel must log in to the cluster using LDAP credentials obtained from the system administrator. If no option is checked and the LDAP server is inaccessible, IBM Service Representatives cannot access the cluster.

Allow IBM support to connect if they have physical access (Recommended)
: Check this box to allow an IBM Service Representative to log in physically without LDAP credentials to connect to the cluster. At least one IBM Service Representative must have direct, physical access to the cluster. An onsite IBM Representative can grant temporary remote access to an offsite IBM Representative. This is the recommended option.

Allow IBM support to connect remotely
: Check this box to allow an IBM Service Representative to log in remotely without LDAP credentials to connect to the cluster.

e. Required: Define the following required Direct LDAP values:
   - Policy Name
   - Primary Server URL
   - Base Distinguish Name
   - User name Attribute
f. Optional: Define any of the following optional Direct LDAP values:
   - Alternative Server URL
   - Group Member Attribute
   - Group Name Attribute
   - User name filter
   - Group Name filter
   - Direct LDAP User Distinguished Name
   - Direct LDAP Password
g. Click **OK**.

2. Define a Custom Role for use by IBM service personnel.
   a. On the management interface, go to **Access** > **Roles & Permissions**.
   b. Select the check box next to the Custom Role you want to define.
   c. Select **Properties** from the **Select Action** drop-down list.
   d. Click **Go**.
   e. Name the Custom Role with a name that is easily identified as for use by IBM service representatives.
   f. Select a role template that is based on the tasks you want to assign to this service role. Refer to the management interface Roles and permissions help page for role descriptions.
   g. In the **Roles and Assigned Permissions** table, check the box next to any additional tasks that are permitted for this service role. Be sure to check the box next to the **Service Login** task at the bottom of this table. If this task is not checked, IBM service personnel might not have access to adequate troubleshooting information.
   h. Click **Submit Changes**.

3. Modify the new Direct LDAP policy to assign it the Custom Role you created.
   a. On the management interface, go to **Access** > **Security Settings**.
   b. Select the radio button next to the Direct LDAP Policy Name you created in Step 1 on page 299.
   c. Select **Modify** from the **Select Action** drop-down list.
   d. Click **Go**.
   e. Navigate to the **External Policy Users/Groups** table.
   f. Select **Add User** from the **Select Action** drop-down list.
   g. Click **Go**.
   h. Enter a user name that can be easily identified as for use by IBM service representatives.
   i. Select the name of the Custom Role you created from the **Role** drop-down list.
   j. Select all clusters in the grid from the **Clusters Access** table.
   k. Click **OK**.
4. Record the Direct LDAP Policy name, user name, and password that is created for IBM service representatives. Store this login information where it can be easily accessed during a service event.

Results

When LDAP authentication is enabled, management interface access is controlled by the LDAP server. Service access requires the user to authenticate through the normal service login and then authenticate again by using the IBM service representative Direct LDAP Policy.

Related information

http://www-01.ibm.com/support/knowledgecenter/SSEQTP_7.0.0/com.ibm.websphere.base.doc/info/aes/ae/cwim_fedrepos.html

Native LDAP using MSAD

You can use a Microsoft Active Directory (MSAD) Lightweight Directory Access Protocol (LDAP) server directly to centrally manage role-based access controls (RBAC) on the TS7700.

The TS7700 supports LDAP authentication and authorization directly through an LDAP server. The TS7700 can communicate with any LDAP server that operates with MSAD.

If you plan to use the System Storage™ Productivity Center (SSPC) Tivoli Storage Productivity Center (TPC) to manage RBAC, refer to the topic “System Storage Productivity Center and Tivoli Storage Productivity Center” on page 304.

Important: When LDAP is enabled, the TS7700 can be accessed only through the LDAP server by using a valid user ID and password combination. All local and remote access to the TS7700 is controlled through secured (encrypted) or plain text authentication. If the LDAP server is not accessible, the TS7700 is not accessible. It is important to create at least one external authentication policy for IBM service personnel access before a service event. Refer to the topic “LDAP and role-based access control” on page 299 for instructions to create an external authentication policy for IBM service personnel.

Related information

Native LDAP with z/OS RACF

You can use IBM's Resource Access Control Facility (RACF) to manage access profiles and services for Lightweight Directory Access Protocol (LDAP) in an IBM Z® environment, including a host attached to a TS7700.

The RACF security server functions as a layer in the operating system to verify user authentication and authorization to system resources. RACF provides:

- Identification, classification, and protection of assets.
- Control of access to protected assets.
- User authentication through identification and verification of user IDs and passwords.
- User authorization through maintenance of access rights to protected resources.
- Access audits by logging instances of access to protected assets.

RACF sets security policies for files and file types to enable consistent security policy application for existing files and future files.

While RACF can address all secure access needs for IBM Z® servers and operating systems, it does not provide a direct interface for external storage devices that can be used to tie those together. When RACF is connected to an LDAP server through a Secured Database Manager (SDBM), the LDAP server can provide access to the user and group information stored in RACF. The SDMB acts as an LDAP front end for the RACF database. You can use SDBM with RACF and an LDAP server to:

- Add users and groups to RACF.
- Add users to groups.
- Modify RACF user and group information.
- Retrieve RACF user and group information.
- Delete users and groups from RACF.
- Remove users from groups.
- Retrieve an RACF user password.

Configuring an IBM Z environment for RACF

Configuration of the IBM Z® environment to use the Resource Access Control Facility (RACF) should be performed by a customer system administrator.

About this task

Configuration steps should include set up of RACF, Secured Database Manager (SDBM), and the Lightweight Directory Access Protocol (LDAP) server. Specific details of these steps differ between customer environments. Refer to the IBM Redbook *ABCs of z/OS System Programming* at http://www.redbooks.ibm.com/redbooks/pdfs/sg246986.pdf for detailed setup instructions. The following procedure is a summary outline.

Procedure

1. Set up the environment for your LDAP server so that the LDAP service is running in the same partition as the RACF.
2. Edit and update user settings and files that are required to provide LDAP support. Refer to the topic Steps for configuring an LDAP server in *IBM Tivoli Directory Server Administration and Use for z/OS* at http://www.ibm.com/support/knowledgecenter/SSLTBW_1.13.0/com.ibm.zos.r13.glpa200/tivstp.htm.
3. After the setup steps are complete, give LDAP access to one or more user IDs.

4. Refresh RACF.
5. Proceed to the topic "Configuring the TS7700 for RACF."

   Related information

   http://www.ibm.com/support/knowledgecenter/SSEQTP_7.0.0/com.ibm.websphere.base.doc/info/aes/ae/cwim_fedrepos.html

Configuring the TS7700 for RACF

Configuration of the TS7700 to use the Resource Access Control Facility (RACF) should be performed through the management interface by a customer system administrator.

About this task

Perform steps to configure the TS7700 after the host is properly configured. Refer to the management interface help topic *Add External policy* (and its subtopics) for definitions and restrictions associated with LDAP configuration.

Procedure

1. Log in to the management interface for the TS7700 Cluster attached to the IBM Z® host where RACF for LDAP has already been configured.
2. Go to `Access > Security Settings > Add External policy`
3. On the Authentication Policies table, select **Add Direct LDAP policy** from the **Select Action** menu.
4. In the Server Settings section, create a policy name that can be identified as using RACF.
5. Select **Allow an IBM service representative to connect through physical access if available**.
6. The **Primary Server URL** must be the same as the LDAP server.
7. The **Base Distinguished Name** must match the `SDBM_SUFFIX` value.
8. In the LDAP Attributes section, enter values for all LDAP attributes and filters.
9. In the Server Authentication section, specify a **User Distinguished Name** using all parameters specific to RACF and defined in the LDAP Attributes section. For example, if **Username Attribute**=racfid, **Group Member Attribute**=user, and **Group Name Attribute**=RACF, then this field would have a value like: `racfid=RACFUSER,profiletype=user,cn=RACF`.
10. Enter a password.
11. Click **OK**.

Results

After the preceding steps are complete, you can use the Modify External Policy page of the management interface to add users to the RACF external profile. Then, use the Assign authentication policy page to assign the new RACF External policy to one or more clusters.

Related information

System Storage Productivity Center and Tivoli Storage Productivity Center

You can use the System Storage Productivity Center (SSPC), a server operating with the Tivoli Storage Productivity Center (TPC) software, as an LDAP proxy to enforce Role-Based Access Controls (RBAC) on the TS7700.

Remote authentication is supported on a TS7700 by using the Tivoli Secure Authentication Service (SAS) client and server, and the WebSphere Federated Repositories. The TS7700 must connect to an SSPC appliance or a server by using TPC. The SAS client is integrated into the TS7700 microcode, while the SAS server and the WebSphere Federated Repositories are integrated into TPC 4.1 and later. TPC is available as a software-only package or as an integrated solution on the SSPC appliance.

When SAS is enabled, the TS7700 passes user authentication requests to the SAS server on the SSPC or TPC, where they are forwarded to the customer's Lightweight Directory Access Protocol (LDAP) such as provided by a Microsoft Active Directory (MSAD) server. The MSAD server then authenticates the user's ID and password; if they are valid then one or more user groups are assigned. The TS7700 then assigns the user a role based on the LDAP or MSAD group.

This central repository allows you to accomplish the following security tasks from a single interface, without logging in to multiple machines:

- Add or remove a user
- Reset or change a password
- Assign, change, or delete the role of a user

A central repository can also simplify the process of responding to new security requirements. For instance, rules for passwords can be changed in one location without reconfiguring multiple, affected machines. By comparison, when local authentication is employed, each individual machine maintains an internal database of user IDs, with corresponding passwords and roles.

LDAP dependency

The WebSphere Federated Repositories component of the SSPC or TPC receives authentication requests from attached devices such as the TS7700 through the SAS. The SAS passes user ID and password information to the MSAD server. The MSAD server returns authentication status to the SSPC or TPC, which forwards the authentication status through the SAS to the requesting device. The MSAD server that is attached to the SSPC or TPC manages the following information:

User ID
A string to identify a specific user

User password
A password for each user ID

Groups
Strings to identify one or more groups of users. The TS7700 can assign groups of users a particular role.

Each user is defined as a member of one or more groups, meaning the user assumes the roles defined by those groups.

Mapping groups to roles

When a user is successfully authenticated by using the SAS client, the resulting user information includes a list of groups the user belongs to. You can use the TS7700 Management Interface to define how groups are mapped to roles.

For more information about TPC, visit the web at http://www-03.ibm.com/systems/storage/software/center/index.html. Refer to the Information Center link in the **Related information** section for additional information about TPC security features, including the external topic *Using Microsoft Active Directory for authentication*.

Related information

"Connecting to the management interface" on page 337

"Establish a connection to the Storage Authentication Server"

http://www-01.ibm.com/support/knowledgecenter/SSEQTP_7.0.0/com.ibm.websphere.base.doc/info/aes/ae/cwim_fedrepos.html

Establish a connection to the Storage Authentication Server

This topic provides instructions for establishing a connection to the Storage Authentication Server for the System Storage Productivity Center.

To establish a connection to the Storage Authentication Server, you must use an integrated portal and the TS7700 Management Interface.

1. Set up a System Storage Productivity Center by configuring the TotalStorage Productivity Center to communicate with an external Lightweight Directory Access Protocol (LDAP) repository.

   Note: Refer to the topic *Changing the user authentication method*, available from the PUBLIB link in the **Related information** section for configuring instructions.
2. Use the *Add Storage Authentication Service policy* panel of the TS7700 Management Interface to create a new storage authentication service policy. On this panel:
   a. Enter a unique policy name
   b. Enter an address for the TotalStorage Productivity Center
   c. Retrieve the certificate
   d. Enter an administrative user name and password for the TotalStorage Productivity Center
   e. Click **OK**
3. Use the *Modify Storage Authentication Service policy* panel of the TS7700 Management Interface to modify the new storage authentication service policy.

   Add users and groups from the LDAP server that you want to give permission to access the management interface.
4. Use the *Assign authentication policy* panel of the TS7700 Management Interface to assign the new authentication policy to one or more clusters.

   Enter the user name and password for the user(s) assigned to the administrator role by the new policy.

Related information

"Connecting to the management interface" on page 337

http://www-01.ibm.com/support/knowledgecenter/SSNE44_4.1.0/com.ibm.tpc_V41.doc/fqz0_c_change_user_auth_method.html

Audit logging

Audit logging tracks user actions that have the potential to negatively affect TS7700 operations if performed incorrectly or maliciously.

User actions that have the potential to negatively affect operations include such things as:
- Log on and log out events
- Configuration changes
- Varying the machine on or off
- User-initiated media export
- Code updates

Audit logging events are captured by Simple Network Management Protocol (SNMP) traps that capture the following information that is associated with the event:
- Identification of the machine affected, by IP address
- User ID
- Description of the event
- Any applicable parameter data

These SNMP traps occur in real time (log events are sent as they occur). The logs are maintained on a remote server in a secure area.

Configuring SNMP on a TS7700

You can use the TS7700 Management Interface to configure and test SNMP traps on a TS7700 Cluster.
1. Log in to the cluster on which you want to enable SNMP.
2. Navigate to **Settings>SNMP**.
3. Check the **Enable SNMP Traps** box.
4. Enter a **Trap Community Name**.
5. Click **Submit Changes**.
6. On the **Destination Settings** table, select **Add** from the **Select Actions** drop-down menu.
7. Enter a value for **IP address**. The machine with this IP address becomes the dedicated trap destination.

   Note: An SNMP monitoring application like The Tivoli Security Information Event Manager must be installed on this machine to receive log events.
8. Leave the value for **Port** unchanged.
9. Click **OK**.
10. Download an SNMP Management Information Block (MIB) file as described in "Download an SNMP MIB file" on page 307.
11. Import the SNMP MIB file into your SNMP monitoring application on your trap destination machine.
12. Test your SNMP trap configuration by clicking **Send Test Trap** on the SNMP page. If your configuration is correct, your SNMP monitoring application displays a successful capture of the test trap.

Download an SNMP MIB file

You can use any SNMP monitoring application to receive log events. The same application can also be used to filter the logged events, allowing for a single monitoring and filtering application for all clusters in the grid. The use of an SNMP MIB file permits you to replace a full text log description with a message identifier, preserving valuable storage space. The Tivoli Security Information Event Manager is an SNMP monitoring application that can be used to achieve these benefits.

Follow these instructions to locate and download a SNMP MIB file:

1. Open the following link in your web browser: http://www-933.ibm.com/support/fixcentral/.
2. Select **System Storage** from the **Product selector** menu.
3. Select **Tape Systems**.
4. Select **Tape Virtualization**.
5. Select **TS7700**.
6. Click **Continue**.
7. On the Select Fixes page, check the box next to the SNMP MIB file you want.
8. Click **Continue**.
9. On the Download Options page, select **Download using Download Director**.
10. Select the check box next to **Include prerequisites and co-requisite fixes**.
11. Click **Continue**.
12. On the Download files using Download Director page, ensure that the check box next to the SNMP MIB file version you want is checked and click **Download now**. The Download Director applet opens. The downloaded file is saved at `C:\DownloadDirector\`.

Related information

SNMP MIB definitions

This topic defines the trap type values that can be present on an SNMP Management Information Block (MIB) log file.

Refer to Table 94 to identify a specific trap type present on the MIB log.

Table 94. SNMP MIB definitions

Trap type	Description
hydAccountManagement	This trap is sent when a new task is created in the task_tracking database. It logs account management on the TS7700.
hydActivateCodeImage	This trap is sent when a SMIT command is executed. It logs activation of TS7700 code images on the TS7700.
hydActivateTapeMicrocode	This trap is sent when a SMIT command is executed. It logs activation of tape drive microcode on the TS7700.
hydActivateTapeMicrocode2	This trap is sent when a SMIT command is executed. It logs activation of tape drive microcode on the TS7700 (Duplicate SMIT type entry).
hydAddAccessGroupVolumeRanges	This trap is sent when a new task is created in the task_tracking database. It logs when access group volume ranges are added to the TS7700.
hydAddLibraryPortAccessGroup	This trap is sent when a new task is created in the task_tracking database. It logs when a library port access group is added or modified on the TS7700.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydAddModifyOrDeleteUser	This trap is sent when a new task is created in the task_tracking database. It logs when a user account is added, modified or deleted on the TS7700.
hydAddOrModifyCategory	This trap is sent when a new task is created in the task_tracking database. It logs when a category is added or modified on the TS7700.
hydAddOrModifyConstruct	This trap is sent when a new task is created in the task_tracking database. It logs when a construct is added or modified on the TS7700.
hydAutomaticOwnership	This trap is sent when a SMIT command is executed. It logs configuring automatic ownership takeover manager to a remote cluster on the TS7700.
hydBringNodeOffline	This trap is sent when a new task is created in the task_tracking database. It logs that a node was brought offline on the TS7700.
hydBringOnline	This trap is sent when a new task is created in the task_tracking database. It logs that the TS7700 was brought online.
hydCacheFailure	This trap is sent when a physical drive failure is detected on the TS7700.
hydCacheRebuild	This trap is sent when a physical drive is being rebuilt on the TS7700.
hydCacheReplaceSuccess	This trap is sent when a physical drive has been successfully replaced on the TS7700.
hydCallHomeFilters	This trap is sent when a SMIT command is executed. It logs the changing or displaying of call home filters on the TS7700.
hydCallHomeRemoteServices	This trap is sent when a SMIT command is executed. It logs the changing or displaying of call home or remote services on the TS7700.
hydCancelCopyExport	This trap is sent when a new task is created in the task_tracking database. It logs when a copy export is cancelled on the TS7700.
hydCancelMove	This trap is sent when a new task is created in the task_tracking database. It logs when a move or eject of physical volumes is canceled on the TS7700.
hydCancelOperation	This trap is sent when a new task is created in the task_tracking database. It logs when an operation is cancelled on the TS7700.
hydCancelService	This trap is sent when a SMIT command is executed. It logs when service/service prep is cancelled on the TS7700.
hydCancelServicePrep	This trap is sent when a new task is created in the task_tracking database. It logs when a service prep is cancelled from the interface on the TS7700.
hydChangeStackedVolumeToRO	This trap is sent when a SMIT command is executed. It logs when the stacked volume is changed to read only on the TS7700.
hydChangeTapeDriveSettings	This trap is sent when a SMIT command is executed. It logs when the tape drive settings are changed on the TS7700.
hydChangeVPD	This trap is sent when a SMIT command is executed. It logs changes to Vital Product Data (VPD) on the TS7700.
hydClusterFamilies	This trap is sent when a new task is created in the task_tracking database. It logs when cluster families change on the TS7700.
hydClusterHealthScan	This trap is sent when a new task is created in the task_tracking database. It logs a cluster health scan on the TS7700.
hydClusterNetworkSettings	This trap is sent when a new task is created in the task_tracking database. It logs cluster network settings on the TS7700.
hydCommandText	The message with a more detailed description of the task, this can be empty if it is not sent in the trap. Access the TS7700 Management Interface to view the command text.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydCommandTextId	The message ID mapped to a string with a more detailed description of the task. The full string is shown in the TS7700 Management Interface. The text may be sent in the hydCommandText value.
hydCommandTextInserts	The specific inserts for the message with details info about the task. Used to insert context-sensitive values into the static message mapped to hydCommandTextId.
hydCompleteNonConcurrentLoad	This trap is sent when a SMIT command is executed. It logs completing a non-concurrent 3956 microcode load on the TS7700.
hydConfigTSSCIP	This trap is sent when a SMIT command is executed. It logs the IBM TSSC TCP/IP configuration on the TS7700.
hydConfigureFICON	This trap is sent when a SMIT command is executed. It logs configuration of FICON 1Gbit/2Gbit/4Gbit settings on the TS7700.
hydConfigureGridDegradation	This trap is sent when a SMIT command is executed. It logs configuration of grid degradation detection settings on the TS7700.
hydConfigureLocalCluster	This trap is sent when a SMIT command is executed. It logs configuration of the local cluster with remote cluster network IPs on the TS7700.
hydConfigureLocalGrid	This trap is sent when a SMIT command is executed. It logs configuration of the local GRID network IPs on the TS7700.
hydConfigureNetworkPort	This trap is sent when a SMIT command is executed. It logs configuration of network ports for remote connection on the TS7700.
hydCopyExport	This trap is sent when a new task is created in the task_tracking database. It logs a copy export on the TS7700.
hydCopyExportSettings	This trap is sent when a new task is created in the task_tracking database. It logs a copy of export settings on the TS7700.
hydCopyPolicy	This trap is sent when a new task is created in the task_tracking database. It logs the copy policy on the TS7700.
hydCurrentStep	The current step that is being executed for the task. Used in conjunction with hydTotalSteps to determine how far the task has progressed. Since the notification is sent when the task is first created, the user will not see a progression of the task. The management interface for the TS7700 provides updated status on the progression of a task.
hydCustomerConfig	This trap is sent when a SMIT command is executed. It logs customer configuration settings on the TS7700.
hydDeleteAccessGroupVolumeRanges	This trap is sent when a new task is created in the task_tracking database. It logs when access group volume ranges are deleted from the interface on the TS7700.
hydDataManagement	This trap is sent when a SMIT command is executed. It logs data management settings on the TS7700.
hydDeleteCategory	This trap is sent when a new task is created in the task_tracking database. It logs deletion of a category on the TS7700.
hydDeleteConstruct	This trap is sent when a new task is created in the task_tracking database. It logs deletion of a construct on the TS7700.
hydDeleteLibraryPortAccessGroup	This trap is sent when a new task is created in the task_tracking database. It logs deletion of a library port access group on the TS7700.
hydDeleteRange	This trap is sent when a new task is created in the task_tracking database. It logs deletion of a range on the TS7700.
hydDisableTapeDrivePath	This trap is sent when a SMIT command is executed. It logs when a tape drive path is disabled on the TS7700.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydDisasterRecovery	This trap is sent when a new task is created in the task_tracking database. It logs recovery from disaster on the TS7700.
hydEjectPhysicalVolumes	This trap is sent when a new task is created in the task_tracking database. It logs when unassigned physical volumes are ejected on the TS7700.
hydEnableTapeDrivePath	This trap is sent when a SMIT command is executed. It logs when a tape drive path is enabled on the TS7700.
hydExport	This trap is sent when a new task is created in the task_tracking database. It logs an export on the TS7700.
hydForce3957Offline	This trap is sent when a SMIT command is executed. It logs when a 3957-V06/VEA is forced offline on the TS7700.
hydGeneric	This trap is sent when a new task is created in the task_tracking database. It logs a generic task on the TS7700.
hydGridProperties	This trap is sent when a new task is created in the task_tracking database. It logs changes to grid properties on the TS7700.
hydImport	This trap is sent when a new task is created in the task_tracking database. It logs an import on the TS7700.
hydInfoCenterSettings	This trap is sent when a new task is created in the task_tracking database. It logs changes to InfoCenter settings on the TS7700.
hydInitiateForcedServicePrep	This trap is sent when a SMIT command is executed. It logs initiation of a forced service prep on the TS7700.
hydInitiateMicrocodeActivation	This trap is sent when a SMIT command is executed. It logs TS7700 microcode activation on the TS7700.
hydInitiateServicePrep	This trap is sent when a SMIT command is executed. It logs initiation of service prep on the TS7700.
hydIntCancelService	This trap is sent when a new task is created in the task_tracking database. It logs a cancellation of service from the interface on the TS7700.
hydJoinLocalSystem	This trap is sent when a SMIT command is executed. It logs joining a local system with a remote cluster on the TS7700.
hydLogicalVolumeDelete	This trap is sent when a new task is created in the task_tracking database. It logs deletion of virtual volumes on the TS7700.
hydLogicalVolumeInsert	This trap is sent when a new task is created in the task_tracking database. It logs insertion of virtual volumes on the TS7700.
hydLoginLogout	This trap is sent when a new task is created in the task_tracking database. It logs user log in and log out events on the TS7700.
hydLowerRemovalThreshold	This trap is sent when a new task is created in the task_tracking database. It logs temporary lower removal threshold on the TS7700.
hydMicrocodeUpdate	This trap is sent when a new task is created in the task_tracking database. It logs an update of the microcode on the TS7700.
hydMigrateAllIvols	This trap is sent when a SMIT command is executed. It logs when all the virtual volumes in cache are migrated to tape and clears the cache (-m) on the TS7700.
hydModifyClusterPairProperties	This trap is sent when a new task is created in the task_tracking database. It logs a change to cluster pair properties on the TS7700.
hydModifyClusterProperties	This trap is sent when a new task is created in the task_tracking database. It logs a change to cluster properties on the TS7700.
hydModifyDateAndTimeSettings	This trap is sent when a new task is created in the task_tracking database. It logs a change to the date and time on the TS77000.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydModifyFeatureLicensing	This trap is sent when a new task is created in the task_tracking database. It logs a change to feature licensing on the TS7700.
hydModifyKeyManager	This trap is sent when a new task is created in the task_tracking database. It logs a change to the key manager on the TS7700.
hydModifyLogicalVolumes	This trap is sent when a new task is created in the task_tracking database. It logs a change to virtual volumes on the TS7700.
hydModifyNodeNickname	This trap is sent when a new task is created in the task_tracking database. It logs a change to a node nickname on the TS7700.
hydModifyPool	This trap is sent when a new task is created in the task_tracking database. It logs a change to a pool on the TS7700.
hydModifyPoolEncryption	This trap is sent when a new task is created in the task_tracking database. It logs a change to pool encryption on the TS7700.
hydModifyRange	This trap is sent when a new task is created in the task_tracking database. It logs when a range is modified on the TS7700.
hydModifyRemovalThreshold	This trap is sent when a new task is created in the task_tracking database. It logs a change to the cache of temporary removal threshold on the TS7700.
hydModifyRolePermissions	This trap is sent when a new task is created in the task_tracking database. It logs a change to role permissions on the TS7700.
hydMoveListLogicalVolumes	This trap is sent when a new task is created in the task_tracking database. It logs moving a list of virtual volumes on the TS7700.
hydMoveLogicalVolumePools	This trap is sent when a new task is created in the task_tracking database. It logs moving of virtual volume pools on the TS7700.
hydMovePoolsLogicalVolumes	This trap is sent when a new task is created in the task_tracking database. It logs the moving of pools for a list of virtual volumes on the TS7700.
hydMoveQuantity	This trap is sent when a new task is created in the task_tracking database. It logs when a move or eject of a quantity of physical volumes occurs on the TS7700.
hydMoveRange	This trap is sent when a new task is created in the task_tracking database. It logs when a move or eject of a range of physical volumes occurs on the TS7700.
hydNodeHealth	This trap is sent when a new task is created in the task_tracking database. It logs the node health on the TS7700.
hydOperationalMode	This trap is sent when a new task is created in the task_tracking database. It logs that the TS7700 is in operational mode.
hydOperatorInterventionsChange	This trap is sent when a new task is created in the task_tracking database. It logs when operator interventions are changed on the TS7700.
hydOperatorInterventionsClear	This trap is sent when a new task is created in the task_tracking database. It logs when operator interventions are cleared on the TS7700.
hydOwnershipTakeover	This trap is sent when a new task is created in the task_tracking database. It logs an ownership takeover on the TS7700.
hydOwnershipTakeoverMode	This trap is sent when a new task is created in the task_tracking database. It logs the ownership takeover mode on the TS7700.
hydPerformDB2Reorg	This trap is sent when a SMIT command is executed. It logs performing a database (DB2®) reorganization on the TS7700.
hydPerformSwitchover	This trap is sent when a SMIT command is executed. It logs the event of switching to a new microcode image on the TS7700.
hydPremigrateIvols	This trap is sent when a SMIT command is executed. It logs when all resident virtual volumes are premigrated to tape (-p) on the TS7700.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydPrepareNonConcurrentLoad	This trap is sent when a SMIT command is executed. It the log preparation of a non-concurrent 3956-CC6 microcode load on the TS7700.
hydProgressText	The message with a progress information for the task, this can be empty if it is not sent in the trap. Access the TS7700 Management Interface to view the progress text.
hydProgressTextId	The message ID that maps to a string with a more detailed description of the current progress of a task. The full string is shown in the TS7700 Management Interface. The text may be sent in the hydProgressText value.
hydProgressTextInserts	The specific inserts for the message with details on the progress of the task. Used to insert context-sensitive values into the static message mapped to hydProgressTextId.
hydPromoteRecallQueue	This trap is sent when a new task is created in the task_tracking database. It logs a promotion of the recall queue on the TS7700.
hydReclaimSchedule	This trap is sent when a new task is created in the task_tracking database. It logs when an inhibit reclaim schedule is added or modified on the TS7700.
hydReconfigureAllTape	This trap is sent when a SMIT command is executed. It logs the usage of vtd_hardconf_config, which reconfigures all tape devices on the TS7700.
hydRemoteLogin	This trap is sent when a new task is created in the task_tracking database. It logs a remote login on the TS7700.
hydRemoveClusterFromGrid	This trap is sent when a SMIT command is executed. It logs the removal of a cluster from the grid on the TS7700.
hydRemoveClusterHardwareChange	This trap is sent when a new task is created in the task_tracking database. It logs the removal of a cluster due to hardware change on the TS7700.
hydRemoveDefectiveControllerCard	This trap is sent when a SMIT command is executed. It logs the removal of a defective cache controller adapter card on the TS7700.
hydRemoveDefectiveDisk	This trap is sent when a SMIT command is executed. It logs the removal or replacement of a defective system hard disk (not 3956-Cxx disk cache) on the TS7700.
hydRemoveDefectiveEthernetCard	This trap is sent when a SMIT command is executed. It logs the removal of a defective Ethernet adapter card on the TS7700.
hydRemoveDefectiveFibre	This trap is sent when a SMIT command is executed. It logs the removal or replacement of a defective fibre switch on the TS7700.
hydRemoveDefectiveHostCard	This trap is sent when a SMIT command is executed. It logs the removal of a defective host adapter card on the TS7700.
hydRemoveDefectiveRouter	This trap is sent when a SMIT command is executed. It logs the removal or replacement a defective router on the TS7700.
hydRemoveDefectiveTapeCard	This trap is sent when a SMIT command is executed. It logs the removal of a defective tape adapter card on the TS7700.
hydRemoverClusterDisasterRecovery	This trap is sent when a new task is created in the task_tracking database. It logs the removal of a cluster due to disaster recovery on the TS7700.
hydRepairFibrePaths	This trap is sent when a SMIT command is executed. It logs repairing fibre paths to disk cache controllers on the TS7700.
hydRepairLogicalVolumes	This trap is sent when a new task is created in the task_tracking database. It logs the repair of damaged virtual volumes on the TS7700.
hydResetCallHomeDaemon	This trap is sent when a SMIT command is executed. It logs a reset of the call home daemon on the TS7700.
hydResetFCPPath	This trap is sent when a SMIT command is executed. It logs the reset of a fibre channel path (FCP) on the TS7700.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydResetFCPPath2	This trap is sent when a SMIT command is executed. It logs the reset of an FCP on the TS7700 (Duplicate SMIT type entry).
hydResetHostAdapterCode	This trap is sent when a SMIT command is executed. It logs the reset of host adapter code on the TS7700.
hydResetNetworkInterface	This trap is sent when a SMIT command is executed. It logs the reset of a network adapter interface on the TS7700.
hydResetNetworkInterface2	This trap is sent when a SMIT command is executed. It logs the reset of a network adapter interface on the TS7700 (Duplicate SMIT type entry).
hydResetRouter	This trap is sent when a SMIT command is executed. It logs the reset of the router on the TS7700.
hydResetRouter2	This trap is sent when a SMIT command is executed. It logs the reset of the router on the TS7700 (Duplicate SMIT type entry)
hydRestart3957	This trap is sent when a SMIT command is executed. It logs a shut down and restart of the 3957-V06/VEA on the TS7700.
hydResumeFailedHotSwap	This trap is sent when a SMIT command is executed. It logs resumption of operations following a failed adapter card hotswap on the TS7700.
hydResyncDatabase	This trap is sent when a SMIT command is executed. It logs a resynchronization of the database with the physical library inventory on the TS7700.
hydResyncTapeDrive	This trap is sent when a SMIT command is executed. It logs a resynchronization of a tape drive following activation of tape drive code on the TS7700.
hydRLogin	This trap is sent when a SMIT command is executed. It logs a remote log in on the TS7700.
hydRLogout	This trap is sent when a SMIT command is executed. It logs a remote log out on the TS7700.
hydRunFibreSwitchSetup	This trap is sent when a SMIT command is executed. It logs when the fibre switch setup is run on the TS7700.
hydRunFibreSwitchUtilitiy	This trap is sent when a SMIT command is executed. It logs when the fibre switch utility is run on the TS7700.
hydRunPFE	This trap is sent when a SMIT command is executed. It logs when PFE/Support Center provided functions are run from a CD-ROM on the TS7700.
hydSecuritySettings	This trap is sent when a new task is created in the task_tracking database. It logs changes to the security settings on the TS7700.
hydService	This trap is sent when a new task is created in the task_tracking database. It logs service on the TS7700.
hydServicePrep	This trap is sent when a new task is created in the task_tracking database. It logs a service prep initiated from the interface on the TS7700.
hydSetCustomerRouterConfig	This trap is sent when a SMIT command is executed. It logs when customer router configuration is set on the TS7700.
hydSetDateAIX	This trap is sent when a SMIT command is executed. It logs when the date/time using the AIX Tool (ONLY for first time installs) is set on the TS7700.
hydSetDateStandard	This trap is sent when a SMIT command is executed. It logs when the date/time using standard format is set on the TS7700.
hydSetFullRouterConfig	This trap is sent when a SMIT command is executed. It logs when the full router configuration is set on the TS7700.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydSetLocalGridTSSCIP	This trap is sent when a SMIT command is executed. It logs when the local grid TSSC IP is set on the TS7700.
hydSetNTPAddress	This trap is sent when a SMIT command is executed. It logs when the NTP server address for date/time synchronization is set on the TS7700.
hydSetTSSCRouterConfig	This trap is sent when a SMIT command is executed. It logs when the TSSC router configuration is set on the TS7700.
hydShutdown3957	This trap is sent when a SMIT command is executed. It logs when the 3957-V06/VEA is shut down on the TS7700.
hydShutdownCache	This trap is sent when a SMIT command is executed. It logs when the cache (3956-Cxx) and 3957-V06/VEA are shut down on the TS7700.
hydShutdownNode	This trap is sent when a new task is created in the task_tracking database. It logs that a node was shut down on the TS7700.
hydSmitInvokedCommand	This trap is sent when a new task is created in the task_tracking database. It logs when a command is invoked in SMIT on the TS7700.
hydSNMPSettings	This trap is sent when a new task is created in the task_tracking database. It logs changes to the SNMP settings on the TS7700.
hydSpeedDuplexSettings	This trap is sent when a SMIT command is executed. It logs showing or changing the customer network speed and duplex settings on the TS7700.
hydStandAloneDemount	This trap is sent when a new task is created in the task_tracking database. It logs that a stand-alone volume was demounted on the TS7700.
hydStandaloneMount	This trap is sent when a new task is created in the task_tracking database. It logs that a stand-alone volume was mounted on the TS7700.
hydStatus	The current status of the task. The possible values are: in progress (1), finished with success (2), cancelled (3), failed (4), finished successfully with some extra information provided (5), finished successfully with some warnings (6), in the process of cancelling (7)
hydSynchronizeTime	This trap is sent when a SMIT command is executed. It logs the synchronization of time between clusters on the TS7700.
hydTapeDriveUtilities	This trap is sent when a SMIT command is executed. It logs the usage of tape drive utilities (tapeutil) on the TS7700.
hydTaskId	A unique ID assigned to each task in the TS7700 database.
hydTaskName	The string representation of the task type. This value should be the same value that is mapped to hydType.
hydTimeCreated	The timestamp when the task record is created. The time is in GMT. The timestamp is given in the following format: YYYY-MM-DD-HH.MM.SS.SSSSSS
hydTotalSteps	The total number of steps involved in completing this particular task. Used in conjunction with the hydCurrentStep to determine progress of a task. Since the notification is sent when the task is first created, the user will not see a progression of the task. The management interface for the TS7700 provides updated status on the progression of a task.

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydType	The integer specifies the type of task that was initiated by the user. Current values are: 1. Insert virtual volumes 2. Delete virtual volumes 3. Stand-alone mount 4. Import 5. Export 6. Operational mode 7. Microcode update 8. Bring node offline 9. Shutdown node 10. Ownership Takeover mode 11. Bring online 12. Modify feature licensing 13. Add, modify, or delete user 14. Modify role permissions 15. Modify date and time settings 16. Modify node nickname 17. Modify cluster properties 18. Modify grid properties 19. Generic 20. Service 21. Stand-alone demount 22. Account Management 23. Cluster Network Settings 24. Write-Protect Mode 25. Node Health 26. Cluster Health Scan 27. Copy Policy 28. Disaster Recovery 29. Modify Pool Encryption 30. Modify Key Manager 31. Cancel operation 32. Repair damaged virtual volumes 33. Ownership Takeover 34. Promote recall queue 35. Remove cluster - hardware change 36. Remove cluster - disaster recovery 37. Add or Modify Category 38. Delete Category 39. Add or Modify Construct 40. Delete Construct 41. Modify Pool 42. Modify Range 43. Delete Range 44. Add/Modify Inhibit Reclaim Schedule 45. Eject unassigned physical volume(s) 46. Move/Eject Quantity of Physical Volumes 47. Move/Eject Range of Physical Volumes 48. Cancel Move/Eject of Volumes 49. Modify Cluster Pair Properties 50. Operator Interventions change

Table 94. SNMP MIB definitions (continued)

Trap type	Description
hydType (continued)	51. Operator Interventions clear 52. Move List of Virtual Volumes 53. Move Pools for List of Virtual Volumes 54. Modify Virtual Volumes 55. Move Virtual Volume Pools 56. Copy Export 57. Cancel Copy Export 58. Add or Modify Library Port Access Group 59. Delete Library Port Access Group 60. Cluster Families 61. Security Settings 62. SNMP Settings 63. InfoCenter Settings 64. Temporary Lower Removal Threshold 65. Modify Cache Temporary Removal Threshold 66. Login/Logout 67. Copy Export Settings
hydUpdateAIXLevel	This trap is sent when a SMIT command is executed. It logs an update to the AIX maintenance level on the TS7700.
hydUpdateVPD	This trap is sent when a SMIT command is executed. It logs an update to VPD from current physical router settings on the TS7700.
hydUserControlledEvent	This trap is sent when a SMIT command is executed. It logs the addition or removal of a user-controlled event for online capability on the TS7700.
hydUserName	The username that was used to log in to the TS7700 and initiate the particular task.
hydVary3957Offline	This trap is sent when a SMIT command is executed. It logs when the 3957-V06/VEA is varied offline on the TS7700.
hydVary3957Online	This trap is sent when a SMIT command is executed. It logs when the 3957-V06/VEA is varied online on the TS7700.
hydVaryHostAdapterOffline	This trap is sent when a SMIT command is executed. It is sent when offline host adapters are varied on the TS7700.
hydVaryHostAdapterOnline	This trap is sent when a SMIT command is executed. It is sent when online host adapters are varied on the TS7700.
hydVaryTapeOffline	This trap is sent when a SMIT command is executed. It logs when a tape drive is varied offline on the TS7700.
hydVaryTapeOnline	This trap is sent when a SMIT command is executed. It logs when a tape drive is varied online on the TS7700.
hydWriteProtectMode	This trap is sent when a new task is created in the task_tracking database. It logs write-protect mode on the TS7700.
ibmTaskTrackingNotificationsGroup	This group defines those notifications that MUST be implemented by a compliant implementation.
ibmTaskTrackingObjectsGroup	This group defines those MIB objects that MUST be implemented by a compliant implementation.

Related information

"Connecting to the management interface" on page 337

Remote support security

The topics in this section describe remote support security for the TS7700.

Related information

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102531
IBM Data Protection & Retention (DP&R) System Connectivity and Security

Overview

The TS3000 system console (TSSC) provides Ethernet connectivity through a private internal network for the TS7700.

The TS7700 uses the TSSC to communicate back to IBM to accommodate different client environments. The TS7700 is configured by the SSR to define how the outbound connectivity back to IBM will occur. The TS7700 uses the TSSC to connect to IBM for various situations including reporting problems, downloading system fixes, reporting inventory, and transmitting error data.

The Call Home feature sends service related information from the TS7700 to the IBM Remote Technical Assistance Information Network (RETAIN®). Call Home uses a broadband internet connection or an analog modem via a secure network to perform this “Dial-Out” function. Broadband based Call Home is the preferred method.

Remote support capabilities of the TSSC, in conjunction with tape systems, include:

- Call Home problem reporting capability with staged, error-specific Data Gathering for support
- Call-in capability with authenticated access including file transfer and multiple connections with attached systems
- Simultaneous call home and call-in capability using broadband
- Automatic wellness checking for attached systems
- Automatic download and storage of tape tools and codes images

Additionally, the TSSC provides a convenient focal point for local service activities within the data center. The system console is attached via 1 Gbps Ethernet to each tape system. Many tape system service functions can be performed at the console. The TSSC provides the following local service tool applications for the IBM support representative:

- Ability to connect to multiple tape systems and simultaneously perform multiple service tasks from the system console
- Graphical user interface for tape system and tape drive service diagnostic utilities
- Ability to broadcast control unit and tape drive code images to tape systems for subsequent activation from the system console
- Diagnostic tools for verifying communications with IBM RETAIN®
- Graphical user interface for configuring, backing up, and restoring system console settings

Note: For customer functions, go to “System console management GUI” on page 322.

The TSSC provides Ethernet outbound connectivity through the customer's network to the IBM service support system, RETAIN®. The TSSC uses the following protocols to port numbers, as shown in Table 95 on page 318:

- Call Home:
  - HTTPS: Port 443

- HTTP: Port 80
- DNS: Port 53
- Web Access:
  - HTTPS: Port 443
  - HTTP: Port 80
  - LDAP: Port 389
  - LDAP with SSL: Port 636
  - LDAP using SAS: Port 16311

  Note: The standard HTTP/S port, 80/443, allows inbound communication to the TSSC.
- SNMP Trap Notification:
  - SMNP: Port 161/162

    Note: Ports 161 and 162 are the standard ports for sending SNMP traps. (SNMP traps can be sent from the TSSC. The TSSC can be configured to send traps to SNMP target machines. In this case, the firewall needs to allow outbound connections from the library from its port 161 to port 162 on the listening SNMP target machine.

Remember: Using these ports are optional, depending on if the user decides to enable Call Home, web access, or SNMP.

Table 95. TSSC External Port Information

Port	Type of data	Direction	Protocol
	PING	Outbound	ICMP
53	DNS	Outbound	UDP
80	HTTP	Bidirectional	TCP
161/162	SNMP	Bidirectional	UDP
389	LDAP	Outbound	TCP
443	HTTPS	Bidirectional	TCP
636	LDAP with SSL	Outbound	TCP
16311	LDAP using SAS	Outbound	TCP

Note: Bidirectional in case of customer web access, otherwise Outbound only.

Dial-out security features of the TSSC

Dial-out is used by the Call Home feature to send service-related information from the attached systems to the IBM service support system, RETAIN®. Dial-out is available through the system console and the modem. Dial out security properties for the attached systems are as follows:

1. Dial-out is from the customer location to the IBM connection point. The IBM service support system (RETAIN®) does not initiate connections to the attached systems.
2. Dial-out through the system console can either be over a modem connection or over an outbound Ethernet connection to the customer network. All outbound traffic is limited to HTTP, HTTPS, and DNS information. All service-related data is communicated by using HTTPS and is therefore encrypted.

3. The data that is exchanged between the attached systems and RETAIN® is service-related data. The protocol that is used is specific to this application and not publicly available.
4. On the first data exchange of each transmission, RETAIN® validates that the calling system is entitled to service. If the calling system is not validated, it is disconnected.
5. The default setting for the Call Home feature is enabled. The Call Home feature can be disabled by an IBM service representative.

Dial in security features of the TSSC
Dial-in is used by IBM service representatives to log on to the system console and provide service support. All dial-in connectivity to the system console is through either a modem or broadband connection, which restricts all incoming traffic. Separate logon IDs are required for access to each attached system.

Figure 46 is a representation of a potential connection scheme for the TSSC.

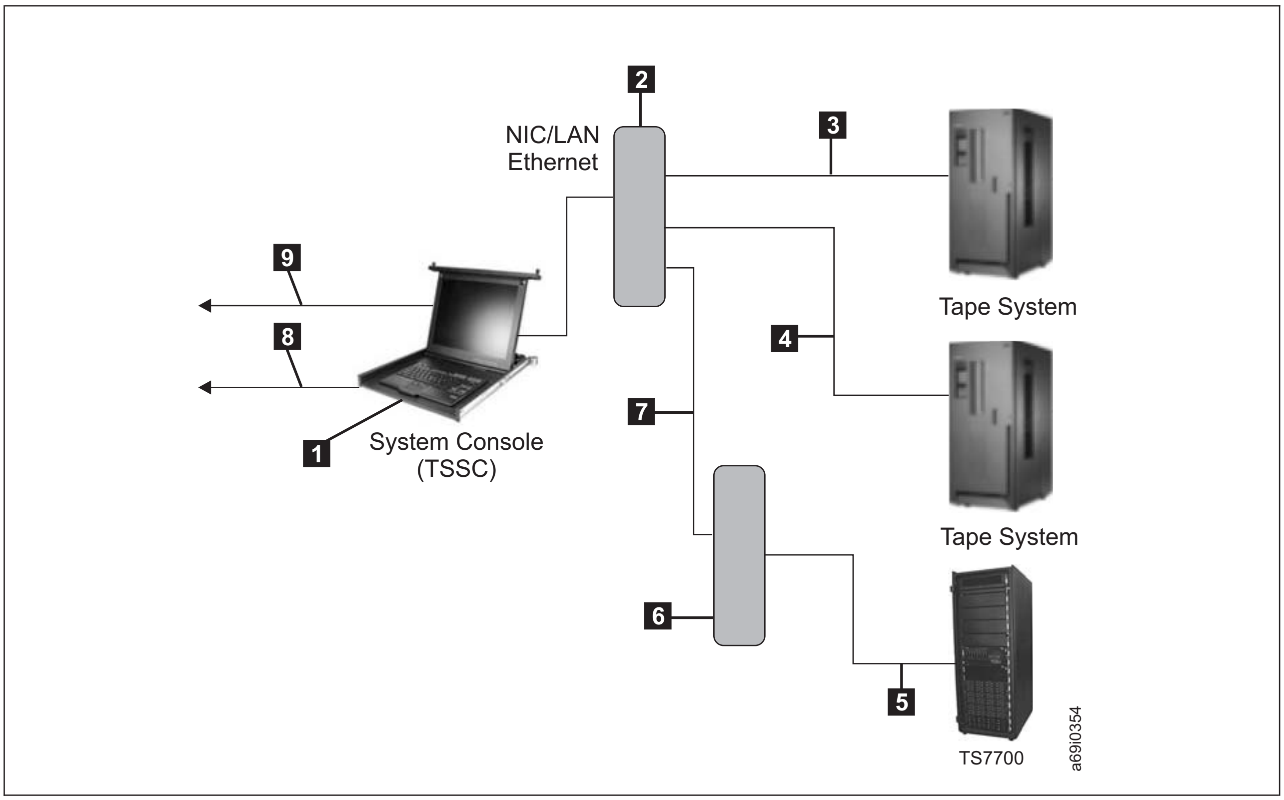


Figure 46. TSSC Connection Diagram

Table 96. TSSC Components

1 Serial connector	6 Ethernet expansion FC 2714
2 Ethernet switch FC 2704/FC 2732	7 Cable supplied with FC 2714
3 Cable supplied with FC 2704/FC 2732	8 Second modem (not on all RMSS products)
4 Cable supplied with FC 2715	9 Customer supplied Ethernet connection
5 Cable supplied with FC 2714	1 Gbps can use CAT 5e or CAT 6, 10 Gbps will need CAT 6.

Managing remote support

This section provides instructions for connecting to the system console, and the procedures you can perform by using the System console management GUI.

Note: The following sections are for System console management GUI version 8.3.x or later. For the previous version of the GUI, refer to the TS7700 Customer documentation version 4.1.0 in IBM Knowledge Center.

Logging in to the system console

This topic provides instructions for logging into the system console.

About this task

To login to the system console locally, see "Logging in locally." To login to the system console remotely, see "Logging in remotely."

Logging in locally:

This topic provides instructions for logging into the system console locally.

About this task

To log in to the system console locally, perform the following steps:

Procedure

1. At the System Console Login screen, in the **Login** field type *customer* and press Enter.
2. In the **Password** field, type *customer* and press Enter. The System console management GUI Welcome Page is displayed.

Logging in remotely:

This topic provides instructions for logging into the system console remotely.

About this task

You can access the system console remotely through a web browser.

Refer to the following table for a list of supported browsers.

Table 97. Supported browsers

Browser	Version supported
Microsoft Edge	25.x
Microsoft Internet Explorer	9, 10 or 11
Mozilla Firefox	24.0, 24.x ESR, 31.0, 31.x ESR, 38.0, 38.x ESR or higher
Google Chrome	Chrome 39.x or Chrome 42.x

Procedure

To connect to the system console through a web browser, perform the following steps:

1. In the address bar of a supported browser, enter the system console IP address or host name, followed by `/TSSC/`.
   For example, `<IP ADDRESS>/TSSC/`
2. Press the Enter key on your keyboard or the **Go** button on your web browser.
3. Enter the **Login** *customer* and **Password** *customer*, then click **Login**. The System console management GUI Welcome Page is displayed.

Adding an SSL or CA certificate

This topic provides instructions for adding a secure socket layer (SSL) certificate, or a certificate authority (CA) certificate, also known as a proxy certificate.

About this task

Importing a customer provided certificate allows the System console management GUI (on the TSSC hardware) and customer proxy to communicate.

Use the Certificates page to add or delete certificates.

Note: Only the customer user, and users with administration role, have access to modify Security Settings, Certificates, and Roles Management.

Procedure

1. From the System console management GUI, select **Console Settings** > **Certificates**.
2. To add an SSL certificate, under the SSL Certificates heading:
   a. Enter the certificate name in the **Alias** field.
   b. Enter the server URL in the **Server URL** field.
   c. Enter the server port in the **Port** field.
   d. Click **Retrieve Certificate**.
3. To add a proxy certificate, select a method to add the certificate (**Retrieve certificate from server** or **Upload a certificate file**).
   a. To retrieve a certificate, under the Proxy Certificates heading:
      1) Enter the certificate name in the **Alias** field.
      2) Enter the server URL in the **Server URL** field.
      3) Enter the server port in the **Port** field.
      4) Click **Retrieve Certificate**.
   b. To upload a certificate, under the Proxy Certificates heading:
      1) Click **Browse** to locate the file.
      2) Then, click **Upload**.
4. Once done, verify that the certificate is added to the trusted certificate table.
5. To remove a certificate, select the certificate from the list and click **Delete Selected Entry**.

Logging out of the system console

This topic provides instructions for logging out of the system console.

About this task

After you complete your current task on the system console, you should log out.

Note: Any time a user exits the System console management GUI, the user is logged out of the system console. You must close the web browser for the log off to be complete.

Procedure

To log out of the system console locally, perform the following steps:
1. Right-click from anywhere in the Desktop to view the Main Menu.
2. Click **Logout**.

System console management GUI

This topic describes the System console management GUI.

The System console management GUI is the interface that you can use to manage the following items:
- Administer Users
- SNMP Trap Forwarding
- AOS Settings
- Attached Systems
- Audit Logs
- Firewall Settings
- IP Whitelist
- Test Call Home
- Call Home Settings
- Security Settings
- Remote Support Settings
- Backup/Restore
- Roles Management
- Network Information

Note: Any time a user exits the System console management GUI by closing the web browser, the user is logged out of the system console.

Administering users

This topic provides instructions for adding users, deleting users, or changing user passwords.

About this task

Use the Security Settings page to add users, delete users, or change user passwords.

Notes:
- A customer user can add, delete, or change passwords for any users in the customer group who use the Administer Users tools.
- The "customer" user ID cannot be deleted.
- A customer user cannot modify the user IDs for service users, and service users cannot modify customer group users.

Procedure

1. From the System console management GUI, click **Console Settings** > **Security Settings**. A screen appears with options to add users, delete users, or change user passwords.
2. From the Administer Users area, choose the appropriate option that you want to use.

Adding a user:
Procedure

To add a user to the customer group, under the **Add User** heading:

1. Enter a new user ID in the **User ID** field (8-character maximum).
2. Enter a password in the **New Password** field and repeat the password in the **Confirm New Password** field.

   Note: The password requirements are: 8-character maximum, and at least one uppercase letter, one lowercase letter, one number, and one special character (for example, !?$%&).
3. Click **Add**.

Deleting a user:
Procedure

To delete a user from the customer group, under the **Delete User** heading:

1. Select a user ID from the User ID drop-down list.
2. Click **Delete**.

Changing a user password:
Procedure

To change a user's password, under the **Change User Password** heading:

1. Select a user ID from the User ID drop-down list.
2. Enter a password in the **New Password** field and repeat the password in the **Confirm New Password** field.

   Note: The password requirements are: 8-character maximum, and at least one uppercase letter, one lowercase letter, one number, and one special character (for example, !?$%&).
3. Click **Change**.

Changing a user role:
Procedure

To change a user's role, under the **Change User Role** heading:

1. Select a user ID from the User ID drop-down list.
2. Select the new role.
3. Click **Change Role**.

Exporting or importing a user:
Procedure

To export or import a user, under the **Export or Import Users** heading:

1. Select either export or import users to a file.

2. Enter the path of where to store or retrieve the file.
3. Click **Perform Action**.

Setting SNMP trap forwarding

This topic provides instructions for enabling or disabling SNMP trap forwarding.

About this task

To enable or disable SNMP trap forwarding, follow these instructions:

Enabling SNMP trap forwarding:
Procedure

To enable SNMP trap forwarding, perform the following steps:

1. From the System console management GUI, select **Call Home Settings** > **SNMP Settings**.
2. In the **IP or Hostname** field, enter the customer's network IP address or hostname.
3. Ensure that the **Send traps** check boxes are selected.
4. Click **Apply**.

Disabling SNMP trap forwarding:
Procedure

To disable SNMP trap forwarding, perform the following steps:

1. From the System console management GUI, select **Call Home Settings** > **SNMP Settings**.
2. Ensure that the **Send traps** check boxes are not selected.
3. Click **Apply**.

Managing Assist On-Site settings

This topic provides instructions for managing Assist On-Site (AOS) settings.

About this task

Assist On-Site (AOS) allows IBM Support engineers to remotely access customers' computers to identify and resolve technical issues in real time. AOS facilitates problem determination and remediation by providing a powerful suite of tools that enables IBM Support engineers to quickly complete root cause analysis and take appropriate corrective action.

AOS implements outbound connections that are protected by state-of-the-art 128-bit MARS (AOS 3.3) or TLS (AOS 4.0) encryption over a port 443 session to prevent intruder access to the information exchanged during all AOS sessions. Chat, screen viewing, screen sharing, and file transfer data are encrypted end to end, and packets are never decrypted in transit by the communication servers.

Note: AOS 4.0 client can access only servers with AOS 4.0 and later. AOS 3.3 client can access only servers with AOS 3.3 and earlier. Current system console code (7.4.x or later) uses AOS 4.0. System console code earlier than 7.4.x uses AOS 3.3.

To access AOS Settings, from the System console management GUI, select **Call Home Settings** > **AOS Settings**.

Start, Stop, or Restart AOS:

To Start, Stop, or Restart the AOS service, click the corresponding button in the **AOS Configuration** section.

If you want only Customer users to have control over AOS settings, click **Take Control of This Page From IBM Service** in the **AOS Configuration** section. Alternately, if you want IBM and Customer users to have control, select **Transfer Control of This Page to IBM Service**.

Enable or Disable Unattended Mode (AOS Lights Out):

To enable unattended mode (AOS Lights Out), select the **Enable Unattended Mode** check box and click **Apply**.

If you want attended mode (Lights On), clear the **Enable Unattended Mode** check box and click **Apply**.

To back out and not make any changes, select **Cancel**.

Configure a Proxy Server:

1. Select the **Connect Through HTTP Proxy** check box.
2. Select the **Proxy server requires authentication** check box.
3. Enter the URL of the server in the **Proxy Address** field.
4. Enter the port number in the **Proxy Port** field.
5. Enter the User ID in the **User ID** field.
6. Enter the password in the **Password** field.
7. Reenter the password in the **Confirm Password** field.
8. Select **Apply**.
9. To back out and not make any changes, select **Cancel**.

```
CHARACTER       ENABLE VIA GUI       ENABLE VIA RAS MENU
~               OK                   OK
`               not allowed          OK
!               requires \!          requires \!
@               not allowed          not allowed
#               requires \#          requires \#
$               OK                   OK
%               OK                   OK
^               OK                   OK
&               OK                   OK
*               OK                   OK
(               OK                   OK
)               OK                   OK
_               OK                   OK
-               OK                   OK
+               OK                   OK
=               OK                   OK
[               OK                   OK
]               OK                   OK
{               OK                   OK
}               OK                   OK
|               OK                   OK
\               requires \\          requires \\
:               OK, but display cuts off everything after :
;               OK                   OK
"               OK                   OK
'               OK                   OK
<               OK                   OK
>               OK                   OK
,               OK                   OK
.               OK                   OK
?               OK                   OK
/               not allowed          not allowed
```

Change the DNS Mode:

If you are not using DNS, ensure that the **Enable No-DNS mode** check box is selected. Enter the IP address of the AOS relay server. If the IP address is not known, leave the **IP Address** field blank to accept the default. Click **Apply**.

If you are using DNS, clear the **Enable No-DNS mode** check box. Then, click **Apply**.

To back out and not make any changes, select **Cancel**.

Managing attached systems

This topic provides instructions for managing attached systems.

About this task

Use the Attached Systems page to add or delete an attached system, or to monitor an attached system.

Procedure

1. From the System console management GUI, select **Attached Systems**.
2. To add an attached system, enter the IP address of the system you want to add and select **Add System**.
3. Verify that the system you added is now shown in the Device table.
4. To remove a system from the attached system list, select the check box next to the device you want to remove and click **Delete Selected**.

Configuring log settings

This topic provides instructions for configuring RSYSLOG settings.

About this task

Use the RSYSLOG Settings page to configure the RSYSLOG settings.

Procedure

1. From the System console management GUI, select **Console Settings** > **RSYSLOG Settings** .
2. If you see the message `Take Control of This Page From IBM Service`, select **Take Control of This Page From IBM Service**.

   Note: To transfer control back to IBM service personnel, select **Transfer Control of This Page to IBM Service**.
3. To sync with the customer syslog server:
   a. In the RSYSLOG Server Settings area, select the log files that you want to send or synchronize to the server.
   b. In the **Port** field, enter the port number of the server.
   c. In the **Server Hostnames** field, enter the hostname or IP address of the syslog server.
   d. Then, select **Update RSYSLOG Settings**.

Viewing or downloading logs

This topic provides instructions for viewing or downloading audit log files.

About this task

Use the Log Settings page to view or download log files.

Procedure

1. From the System console management GUI, select **Console Settings** > **Log Settings**.
2. To download any of the log files that are listed, select the file, then select **Download Log Files**.
3. To view a select number of lines from a log file, in the Tail Log File area, select a file, then enter the number of lines, and click **Tail**.

Managing firewall settings

This topic provides instructions for managing firewall settings.

About this task

Use the Custom Firewall Settings page to customize firewall settings.

Procedure

1. From the System console management GUI, select **Console Settings** > **Custom Firewall Settings**.
2. If you see the message `Take Control of This Page From IBM Service`, select **Take Control of This Page From IBM Service**.

   Note: To transfer control back to IBM service personnel, select **Transfer Control of This Page to IBM Service**.
3. Click the radio button in the **Accept** column to authorize a port or in the **Drop** column to disallow a port name.
4. You can add custom rules at the bottom, specifying the values, then click **Update Firewall Settings** after you have made all of your selections.
5. To modify a custom rule, enter the information for the custom rule, change whether to Accept or Drop, and click **Update Firewall Settings**.

Updating the IP Whitelist

This topic provides instructions for updating the IP whitelist.

About this task

The IP whitelist defines a set of IP addresses that are allowed to access the system console on any port. If the list is empty or has not yet been synced to the system IP tables, IP addresses are not filtered. If the list is populated and has been synced to the system IP tables, only the IP addresses in the list will be allowed to access the system console. Take great care in setting the IP whitelist to include all addresses prior to synchronization that need to access the system console. For example, if you are using AOS to edit the IP whitelist and do not include the IP addresses of the AOS broker, you will be locked out of using the system console until a local user edits the list to include the AOS broker's IP address.

Procedure

1. From the System console management GUI, select **Console Settings** > **IP Whitelist**.
2. If you see the message `Take Control of This Page From IBM Service`, select **Take Control of This Page From IBM Service**.

Note: To transfer control back to IBM service personnel, select **Transfer Control of This Page to IBM Service**.

3. Type in the addresses that you want to allow system console access. When the list is satisfactory, click **Sync List With IP Tables** to enforce access to the system console by only the addresses on the list.

Testing Call Home

This topic provides instructions for testing the Call Home connection.

About this task

Use the Test ECC Connectivity page to test the Call Home (RETAIN) connection.

Procedure

1. From the System console management GUI, select **Call Home Settings** > **Test ECC Connectivity**
2. Click **Test Connection** to begin the test.
3. To see the current ECC IP addresses and ports, select **Show ECC Info**.

Managing Call Home settings

This topic provides instructions for managing Call Home settings.

About this task

Use the Call Home Settings page to customize Call Home settings.

Attention: Changing Call Home settings might make Call Home not usable if settings are not correct.

Procedure

1. From the System console management GUI, select **Call Home Settings**.
2. If you see the message `Take Control of This Page From IBM Service`, select **Take Control of This Page From IBM Service**.

   Note: To transfer control back to IBM service personnel, select **Transfer Control of This Page to IBM Service**.
3. Select an interface to be used for call home:
   - Modem
     - If you select the modem call home interface, the Modem Port selection box under Call Home Communication Setup enables.
     - If you select the modem port by using the Modem Port selection box, select "/dev/ttyS0" ("/dev/ttyS0" is the serial port COM1 and "/dev/ttyS1" is serial port COM2, as labeled on the back of the system console).

     Notes:
     - Using this method disables all broadband call home.
     - If "/dev/ttyS1" is selected but unavailable, no call home activity takes place on the console and no warning or error messages are given.
     - When two modems are installed, the modem on COM1 can be configured to be the inbound modem, and the modem on COM2 can be configured to be the outbound modem. If only one modem is installed, it must be installed on COM1, and it is used for inbound and outbound communication.

– Call Homes that are present in the Call Home Queue are sent home every 5 minutes to ensure that the modem line is not always in use.

- Ethernet
  – If you select the Ethernet call home interface, the Ethernet Communication section enables, under the Call Home Communication Setup.
  – Select a method for broadband call home based on the customer's network configuration:
    - Direct Communication implies there is not an HTTP proxy between the configured TS3000 and the outside network to IBM. Selecting this method requires no further setup.
    - Connect Through HTTP Proxy implies there is a customer HTTP Proxy server that the customer requires all call home traffic to go through. When you select this option, enter the Proxy IP Address and Proxy Port. If necessary, enter any required proxy server username and password. For proxy password limitations, see Configure a Proxy Server.

    Notes:
    - Using this method disables all modem call home transmission (outbound only).
    - Ensure that the External Network Interface has been set up in Console Settings.
    - Obtain the IP Address, Subnet Mask, and Default Gateway from the customer.
    - Port 443 (HTTPS) must be free for outbound traffic.
    - If ECC is locked due to too many failed tries, you can clear the lock by clicking **Unlock Call Home**.
    - Call Homes are sent home back-to-back until the Call Home queue is empty.
- Autoselect
  – If you select Autoselect call home interface, the system console first attempts to call home over the Ethernet. If an Ethernet interface failure is encountered, call home is attempted over the modem. Both Modem Port and Ethernet Connection sections become enabled.
  – Select a modem port and Ethernet Communication settings, as described in Modem and Ethernet section.

4. To select the ECC type, choose either **Edge** or **Legacy**.
5. If you want to enable the system console heartbeat, check **Enable System Console Heartbeat**, then select the day interval (usually set to **3**). This interval is the number of days between heartbeats. Select **Apply**.
6. To disallow inbound modem connections, select the **Disallow Inbound** option in the **Modem Connections** section and click **Apply**. This allows outbound connectivity through the modem for call home while ignoring any incoming calls. To allow incoming calls, select the **Allow Inbound** option and click **Apply**.
7. To return control of Call Home settings to IBM, select **Transfer Control of This Page to IBM Service**.

Managing security settings

This topic provides instructions for managing security settings.

About this task

Use the Security Settings page to create, modify, delete, and assign authentication policies. There are two types of policies for authentication, System Storage™ Productivity Center or native LDAP using Microsoft Active Directory.

Note: Only the customer user, and users with administration role, have access to modify Security Settings, SSL Certificates, and Roles Management.

Procedure

1. From the System console management GUI, select **Console Settings** > **Security Settings**.
2. Enter values for any of the optional fields you want to define:

   Policy Name
   The name of the policy that defines the authentication settings. The policy name is a unique value that is composed of one to 50 Unicode characters. Blank spaces and special characters are not permitted.

   Primary Server URL
   The primary URL for the Storage Authentication Service. The value in this field is composed of one to 254 Unicode characters and takes one of the following formats:

   ```
   https://<server_address>:secure_port/TokenService/services/Trust
   ldaps://<server_address>:secure_port
   ldap://<server_address>:port
   ```

   Note: If this value is a Domain Name Server (DNS) address you must activate and configure a DNS server on the **Console Settings** > **IP Settings** page.

   Alternate Server URL
   The alternate URL for the Storage Authentication Service if the primary URL cannot be accessed. The value in this field is composed of one to 254 Unicode characters and takes one of the following formats:

   ```
   https://<server_address>:secure_port/TokenService/services/Trust
   ldaps://<server_address>:secure_port
   ldap://<server_address>:port
   ```

   The server address value in the Primary or Alternate Server URL can be an IP or DNS address. Valid IP formats include:

   IPv4 Is 32 bits long, consists of four decimal numbers, each ranging from 0 to 255, separated by periods, like:

   ```
   98.104.120.12
   ```

   IPv6 Is an 128-bit long hexadecimal value enclosed by brackets and separated into 16-bit fields by colons, like:

   ```
   [3afa:1910:2535:3:110:e8ef:ef41:91cf]
   ```

   Leading zeros can be omitted in each field, so that :0003: can be written as :3:. A double colon (::) can be used once per address to replace multiple fields of zeros. For example,

   ```
   [3afa:0:0:0:200:2535:e8ef:91cf]
   can be written as:
   [3afa::200:2535:e8ef:91cf]
   ```

If the Primary or Alternate Server URL uses the https protocol, a certificate for that address must be defined on the SSL Certificates page or retrieved with the Retrieve Certificates.

Policy Scope

Select the scope of the policy as follows:

- **Remote:** The authentication policy will apply only on remote access
- **Local:** The authentication policy will apply only on local access (Login directly on the machine)
- **Both:** The authentication policy will apply to both local and remote accounts

What to do next

Creating a Storage Authentication Service (SAS) policy or Direct LDAP policy:

1. Click **New Policy** in the Policy Configuration panel to enable the configuration fields.
2. Select the policy type **SAS** or **Direct LDAP**.
3. Enter values for the following required fields:

Server Authentication

Values in the following fields are required if WebSphere® Application Server security is enabled on the WebSphere Application Server hosting the Authentication Service.

User ID

The user name used with HTTP basic authentication for authenticating to the Storage Authentication Service. This field supports a maximum length of 254 Unicode characters.

Password

The password used with HTTP basic authentication for authenticating to the Storage Authentication Service. This field supports a maximum length of 254 Unicode characters.

Direct LDAP

Values in the following fields are required.

User Distinguished Name

The user distinguished name used to authenticate to the LDAP authentication service. This field supports a maximum length of 254 Unicode characters. For example:

```
CN=Administrator,CN=users,DC=mycompany,DC=com
```

If you selected Add Direct LDAP Policy in Step 2, enter values for LDAP Attributes:

Base Distinguish Name

The LDAP distinguished name (DN) that uniquely identifies a set of entries in a realm. This field is required but blank by default. The value in this field is composed of one to 254 Unicode characters.

Username Attribute

The attribute name used for the username during authentication. This field is required and contains the value uid by default. The value in this field is composed of one to 61 Unicode characters.

Group Member Attribute

The attribute name used to identify group members. This field is optional and contains the value member by default. This field can contain up to 61 Unicode characters.

Group Name Attribute

The attribute name used to identify the group during authorization. This field is optional and contains the value cn by default. This field can contain up to 61 Unicode characters.

Username filter

Used to filter and verify validity of an entered username. This field is optional and contains the value (uid={0}) by default. This field can contain up to 254 Unicode characters.

Group Name filter

Used to filter and verify validity of an entered group name. This field is optional and contains the value (cn={0}) by default. This field can contain up to 254 Unicode characters.

Note: These fields will depend on the customer's individual network configuration. Consult with the customer to collect the necessary values.

4. Click **Save Changes** to save the policy.

5. To retrieve the certificate, click **Retrieve Certificate**. To confirm that it was successful, select the **SSL Certificates** tab at the top of the page.

Note: The Retrieve Certificate option will retrieve certificates for both the primary and alternate server.

Edit Policy

1. In the Authentication Policies Panel, select the policy to be edited.
2. Click **Edit Policy**, the fields will be enabled in the Policy Configuration panel.
3. Make the changes.
4. Click **Save Changes**.

Notes:

- If the URL changed, it is necessary to Retrieve another Certificate
- If the policy name changed, a new policy will be created

- You are required to re-enter the Authentication Password to save any changes made to SAS policies

- Every time a policy is edited, it must be re-tested before it can be assigned as the active policy

Test Policy

This section is to test policies already saved. With this function you can verify that the configuration of the policy is correct.

1. Enter a valid user ID and password.
2. Click **Test**.

Notes:

- This function is only available on policies already saved.

- Before assigning a policy, the policy should be tested to guarantee a correct log in.

Assign Policy

1. In the Authentication Policies Panel select the policy.
2. Test the policy in the right panel at the bottom to make sure that it is correctly configured.
3. Click **Assign Policy** in the Authentication Policies panel.

Notes:

- If the Policy has not been tested, you will not be able to assign the policy

- Only one policy can be active at a time.

Delete Policy

1. In the Authentication Policies Panel select the policy to delete.
2. Click **Delete Policy**.

Note: When LDAP authentication is enabled, remote and local access is controlled by the LDAP server. Service access requires the user to authenticate through the normal service login and then authenticate again using the IBM service representative Direct LDAP Policy.

System Storage Productivity Center and Tivoli Storage Productivity Center

You can use the System Storage Productivity Center (SSPC), a server operating with the Tivoli® Storage Productivity Center (TPC) software, as an LDAP proxy to enforce Access Controls on the TSSC.

Native LDAP

You can use a Microsoft Active Directory (MSAD) Lightweight Directory Access Protocol (LDAP) server directly to centrally manage access controls on the TSSC.

Certificates

Use this page to display, add, and delete SSL Certificates.

If any SSL certificates have been retrieved, they are displayed in the SSL Certificates area on the Certificates page.

Add SSL Certificate

1. Enter an Alias for the Certificate.
2. Type the URL.
3. Type the port.
4. Click **Retrieve Certificate**.

Delete SSL Certificate

1. Select an SSL Certificate.
2. Click **Delete Selected Entry**.

Managing roles

This topic provides instructions for managing roles.

About this task

Use the Roles Management page to review the system defined roles (Customer, Service and Administrator) or to customize the user defined roles. Each role has its description, role name and a set of the system console permissions. The Security Roles section is used to select one of the eight roles (three system roles and five custom roles). When a selection is made, the settings for that role are displayed in the Role Settings section. The system roles have fixed settings and it is not possible to change these settings. The remaining five roles can be customized.

Procedure

1. From the System console management GUI, select **Console Settings** > **Roles Management**.

To customize a user defined role:

2. Select one of the custom roles from the Security Roles section.
3. Assign the Role Name and Description.
4. Mark the System Console Permissions for this role, optionally by selecting a role in the **Apply Template** drop box, you can copy the permissions of one of the system roles.
5. Click **Apply Changes** for the changes to take affect. A message displays if the changes were applied successfully.
6. Click **Cancel** to cancel the changes.

Managing the remote support center settings

This topic provides instructions for managing remote support center settings.

About this task

Use the remote support center settings page to customize remote support center settings.

Procedure

1. From the System console management GUI, select **Console Settings** > **Remote Support Settings**.
2. If you see the message `Take Control of This Page From IBM Service`, select **Take Control of This Page From IBM Service**.

   Note: To transfer control back to IBM service personnel, select **Transfer Control of This Page to IBM Service**.

3. To **Start** or **Stop** a connection with the remote support center click the corresponding buttons in the **Status** section.
4. Configure the following settings:
   - **Remote Support Configuration:**
     - To enable debugging features in the log, place a check mark next to **Enable debug**.

       Note: Enable debugging if requested by support center personnel.
     - If required, enter the Field Password to connect to the system, or to generate a random Field Password, click **Generate Field Password**.

       Note: The defined or generated password must be available for remote support personnel in order to be able to connect to the TSSC. The password should be defined per customer requirements, or left blank.
     - Enter the idle timeout period (in minutes) in the Connection timeout field.
   - **Server Settings:**
     - In the Support Center String field, enter the IP or hostname and port (<IP or hostname>:<port #>) for each remote support center. Refer to Table 98.
     - To use a proxy server, place a check mark next to **Enable Proxy**.
     - In the Proxy String field, enter the IP or hostname and port (<IP or hostname>:<port #>) for each proxy server.
5. Select **Apply changes** to accept any changes that were made.
6. Select **Reset Config** to reset the configuration to the installation defaults.
7. Select **View log file** to view the Remote Support Settings log file.

Table 98. Remote support center server information

Hostname	IP	Ports	Description
y03lcxapp002.ahe.boulder.ibm.com	204.146.30.139	22	remote support center server
y01lcxapp002.ahe.pok.ibm.com	129.33.206.139	22	remote support center server
sc-rsc-front2.haifa.il.ibm.com	195.110.41.141	22	remote support center server
sc-rsc-front3.haifa.il.ibm.com	195.110.41.142	22	remote support center server

Viewing network information

This topic provides instructions for viewing network information.

About this task

Use the Network Information page to view information about the systems network connections.

Procedure

1. From the System console management GUI, select **Network Information**.
2. Refer to Table 99 on page 336 for information available from the Network Information page.

Table 99. Selections available from the Network Information page

Item	Description
Ping	To test a connection, enter the Host name or TCP/IP address and click **Ping Host**.
Network Statistics	Shows the active Internet connections (w/o servers) and the active UNIX domain sockets (w/o servers).
Interfaces	Shows the systems interfaces. For example, External, Grid, bond:0, and bond0:1.
Address	Shows the IP addresses for all network interfaces, including displaying values for bond0 and bond0:1 if the External and Grid adapters are bonded.
Routes	Shows the Kernel IP routing table.
ARP	Shows the IP address and hardware type of each interface.
Sockets	Shows active Internet connections (servers)
TCP	Shows active Internet connections (w/o servers)
UDP	Shows active Internet connections (w/o servers)
NTP	Shows whether the NTP server is enabled.
Tracepath	To run a traceroute, enter the Host name or TCP/IP address and click **Run Tracepath**.
TCP Dump	To run a TCP Dump: 1. Select the Adapter type. 2. Enter the Port and Duration. 3. Click the check box for **Call home collected data** if wanted. 4. Then, click **Run TCP Dump**.
Nslookup	Enter the Host name and select **Nslookup Host**.

Chapter 5. Managing

This section provides instructions for connecting to the TS7700 Management Interface and shutting down the TS7700.

Connecting to the management interface

This topic describes how to connect to the IBM TS7700 Management Interface.

Before you begin

The TS7700 must first be installed and configured. A supported web browser must also be installed. To ensure that all the functions of the management interface are usable, you need to enable cookies and JavaScript™ in the browser and disable the browser's function of blocking pop-up windows. If you use an unsupported browser, some pages might not display correctly.

Refer to the following table for a list of supported browsers.

Table 100. Supported browsers

Browser	Versions supported	Version tested
Microsoft Edge	25.x	25.0
Microsoft Internet Explorer†	9, 10 or 11	11
Mozilla Firefox	24.0, 24.x ESR, 31.0, 31.x ESR, 38.0 or 38.x ESR	38.0 ESR
Google Chrome	39.x or 42.x	42.0

†Compatibility View is not supported by the TS7700. To toggle **OFF** Compatibility View:

1. Open the TS7700 Management Interface for a cluster by using Internet Explorer version 9.
2. In the browser menu bar, deselect **Tools > Compatibility View** or select the **Compatibility View** button on the browser address bar to change it from an active icon to an outline. Internet Explorer remembers this setting each time the management interface address is accessed.

Note: You cannot open the management interface in multiple tabs or windows by using the same browser.

About this task

The following steps help you connect to the TS7700 Management Interface through an installed web browser.

Procedure

1. In the address bar of a supported web browser, enter **http://** followed by the **virtual IP** entered during installation, followed by **/Console**. The virtual IP is one of three customer IP addresses given during installation. The complete URL takes this form: **http://virtual IP address/Console**.

HTTPS Note: If HTTPS exclusive access is enabled, you cannot access the management interface of a remote cluster. You can only access the management interface of the accessing, local cluster.

2. Press the **Enter** key on your keyboard or the **Go** button on your web browser.

   Bookmarking Note: The web browser redirects to **http://virtual IP address/cluster ID associated with virtual IP address**. If you bookmark this link and the cluster ID changes, you must update your bookmark before the bookmark resolves correctly. Alternatively, you can bookmark the more general URL, **http://virtual IP address/Console**, which does not require an update following a cluster ID change.
3. The login page for the management interface loads. The default login name is **admin** and the default password is **admin**.

Downloading comma-separated value files

Use this procedure to configure Microsoft Internet Explorer† to allowing downloading of comma-separated value (.csv) files in the IBM TS7700.

Before you begin

This procedure is for Windows XP† SP2 users that are not presented with a download dialog box after selecting to download a .csv file.

About this task

In Microsoft Internet Explorer:

Procedure

1. Select **Tools > Internet Options** from the menu bar.
2. Select the **Security** tab.
3. Click the **Local intranet** icon in the **Select a Web content zone to specify its security settings** box.
4. Click the **Sites** button.
5. Check the all check boxes in the dialog box. The default is for all to be checked.
6. Click the **Advanced** button.
7. Input the address of the cluster, for example **http://cluster.address.com:PORT**, into **Add this Web site to the zone:** entry field and click **Add** button. The specified address is added in **Web sites:** list box.
8. Uncheck **Require server verification (https:) for all sites in this zone** check box. The default is unchecked.
9. Click **OK**.
10. Close all dialog boxes by clicking **OK** in each one.

What to do next

The dialog box for .csv file downloads should now appear when downloading .csv files.

†Refer to the topic *Trademarks* in the **Related information** section for complete attribution.

Related information

Preserving leading zeros in downloaded data

This page provides a workaround solution to the problem created when leading zeros are removed from the VOLSER field for downloaded .csv-formatted data.

Excel removes leading zeros from downloaded .csv (comma-separated value) files, which can lead to errors when data is displayed in a spreadsheet format. For example, if a volser in a downloaded list has a value of **012345**, it will appear in Excel as **12345**. To preserve the leading zeros in your downloaded .csv files, take the following steps:

1. When downloading a report in .csv format, click the **Download** button and then click **Save** on the dialog box that appears.
2. When the downloading file name appears, change the file extension from .csv to .txt. For instance, if the default name of the downloading file is "copies.csv", change the name to "copies.txt". The downloaded file will retain the comma-delimited format.

To open the downloaded file in Excel and retain any leading zeros, take the following steps:

1. Open Excel.
2. Select **File>Open** and browse to the .txt file you downloaded. Highlight the .txt file and click **Open**. The *Text Import Wizard* will open.
3. In Step 1 of the *Text Import Wizard*, select "delimited" as the original data type and click **Next**.
4. In Step 2 of the *Text Import Wizard*, select "comma" as the delimiter and click **Next**.
5. In Step 3 of the *Text Import Wizard*, select "text" as the column data format and click **Finish**.

You will now be able to save the downloaded file with a .txt or .xls extension while retaining any leading zeros.

Related information

"Downloading comma-separated value files" on page 338

Shutting down the TS7700

This page provides instructions to power off a TS7700 Cluster.

To power off a TS7700 Cluster, you must be logged in to the TS7700 Management Interface.

1. Connect to the management interface of the TS7700 Cluster you want to shut down. Refer to the topic Connecting to the management interface in the **Related information** section for instructions to log in to the management interface for a given TS7700 Cluster.
2. From the **Cluster Summary** page select **Actions > Change Cluster State > Force Shutdown**. Refer to the help topic Cluster Actions menu in the **Related information** section for restrictions on changing the state of a cluster.

Chapter 6. Recovering

This section provides information related to recovering lost data and testing grid failover.

Recovering lost data

This topic describes how to recover lost data.

About this task

The capability to resume business operations if a product or site failure is provided by the grid configuration of the TS7700. In a grid configuration, two or three TS7700 clusters are interconnected and can replicate data that is created on either TS7700 cluster to the other. Data can be restored if the recovery data is contained entirely on or through a mixture of:

- Copy export physical volumes
- Virtual volumes within a TS7700
- Physical tape
- Replicated disk

When you restore a library environment, it is important to consider and plan for:

- Restoration of the tape management system database
- Restoration of system catalogues, including the tape configuration database (TCDB) (the VOLCAT)
- Restoration of the key management environment for encrypted cartridges
- Location of input/output definition file (IODF) for devices and the LIBRARY-ID and LIBPORT-ID of the recovery TS7700
- Location of the storage management subsystem (SMS) control data set (SCDS) containing library definitions of the recovery TS7700, and construct and automatic class selection (ACS) routine definitions
- Activation of IODF and SCDS and bringing the library and devices online
- Insertion of virtual volumes that are needed for new allocations
- Restoration of the system environment and required application data

Note: Virtual volumes and data set names that are needed during the recovery process must be known. If copy export was used, a physical volume from the last copy export set must be known since it contains the latest VTS database that describes the most recent and all previous copy export sets. Contact your IBM Service Representative for additional information.

You can Use DFSMSdss to dump recovery data at the production site to virtual volumes in a TS7700.

When no z/OS environment exists:

- Use DSS Stand-Alone Services to restore system-related data.
- Use Standard DFSMSdss RESTORE to restore other dumped data when the rescue system has been restored.

When a z/OS basic (starter) environment exists:

- Use RESTORE to recover dumped data.

  Note: TCBD and SCDS are required to mount initial recovery volumes in the TS7700 since production TCBD and SCDS can reside on virtual volumes in the recovery TS7700.
- Use ISMF to define recovery library definitions and any required constructs for a base SMS configuration if SCDS is NULL in the starter system.
- Activate SCDS.
- Use IDCAMS to create volume records for recovery volumes in the TCDB if the TCBD VOLCAT in the starter system is empty.
- Verify OAM is configured.

When a recovery environment exists at a DR site, both disk and tape replication are used, and recovery site system closely mirrors that at the production site:
- Use disk replication to replicate system catalogues, TCBD, SCDS, tape management system database, and other databases and data sets.
- Determine recovery point objectives and whether asynchronous or synchronous disk replication were used.
- Use TS7700 copy policies to replicate other production-related data to the DR site.

As part of a total systems design, you must develop business continuity procedures that instruct I/T personnel what actions to take when a failure occurs. The best time to test the procedures is during an initial installation of the system or at some interval.

For more information about recovering lost data, see *IBM TS7700 Series Grid Failover Scenarios* at http://www-03.ibm.com/support/techdocs/atsmastr.nsf/Web/AdvSearch.

Recovering data from a physical volume

This topic describes scenarios where data can be recovered from a damaged physical volume.

When the TS7700 detects damaged physical volumes, the automated read-only recovery process starts. The TS7700 detects that a physical volume is bad when the physical volume is being mounted for a back-end tape operation. If the physical volume is damaged, you can contact an IBM service representative and have the service representative manually place the volume in automated read-only recovery.

Many error events might be posted to the TS7700 Events Page during the recovery. If you are concerned about the progress of the recovery, contact a service representative to evaluate the progress.

For more information about automated read-only recovery, see the topic *Automated read-only recovery* in the **Related information** section.

Note: A service representative can also force a manual read-only recovering by marking a physical volume as "read_only". This operation should be performed only by an IBM service representative.

Physical volume recovery scenarios

There are four possible scenarios in which data recovery can be attempted from a physical volume. They include:

Read operations failures on a physical volume exceed the error threshold
: In this scenario, the physical volume can be mounted. The TS7700 recognizes that the volume requires read-only recovery and makes it eligible for automated read-only recovery.

A permanent error occurs for the physical volume
: In this scenario, a permanent error such as failure to mount causes the physical volume to become eligible for automated read-only recovery.

Physical damage occurs to the cartridge
: In this scenario, the cartridge that contains the physical volume is damaged to an extent that reinsertion into the library can cause the volume to become stuck in a drive. To resolve this condition and recover the virtual volumes on the cartridge, contact the IBM Support Center and request a problem management hardware (PMH) ticket number.

Physical damage occurs to the physical volume
: In this scenario, only the physical volume is damaged (for example, the tape is broken) and the cartridge can be reinserted in the library without becoming stuck. Subsequent mount attempts fail and automatic read-only recovery is started for that physical volume.

Related information

"Automated read-only recovery" on page 290
Automated read-only (RO) recovery is the process by which hierarchical storage management (HSM) recalls all active data from a particular physical volume that has exceeded its error thresholds, encountered a permanent error, or is damaged.

Testing grid failover

This topic describes how to test for grid failover.

Before you begin

You must be familiar with how to use the virtual tape systems that are attached to zOS environments.

About this task

For documentation about how to test grid failover, refer to:

- *IBM TS7700 Series Grid Failover Scenarios*

This document is available from the IBM Techdocs search portal link in the **Related information** section. Enter the document title in the **Enter optional search string:** field, then click **Search**. The most recent version of the *IBM TS7700 Series Grid Failover Scenarios* document is then returned.

This document contains information to assist with the creation of a test plan. In addition, you can also find a series of grid failover test scenarios for zOS, which were performed in an IBM laboratory environment. Single failures of all major components and communication links and some multiple failures are simulated.

Not all possible grid failover situations are covered in *IBM TS7700 Series Grid Failover Scenarios*. However, you can find documentation that focuses on the scenarios that demonstrate the critical hardware and microcode failover capabilities of the TS7700 Grid configuration.

Related information

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/Web/AdvSearch

Glossary

If you do not find the term you are looking for, see the *IBM Terminology Database* located at the following website: IBM Terminology website.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

"A" "B" on page 347 "C" on page 348 "D" on page 350 "E" on page 353 "F" on page 354 "G" on page 356 "H" on page 357 "I" on page 359 "J" on page 360 "K" on page 361 "L" on page 361 "M" on page 363 "N" on page 365 "O" on page 366 "P" on page 367 "R" on page 369 "S" on page 370 "T" on page 375 "U" on page 376 "V" on page 376 "W" on page 377

A

above mean sea level (amsl)
: The elevation or altitude of an object that is used in broadcasting and other telecommunications by engineers to determine the coverage area a station will be able to reach.

ac See alternating current.

AC See alternating current.

ACF See automatic cartridge facility.

Advanced Encryption Standard (AES)
: A data encryption technique that improved upon and officially replaced the Data Encryption Standard (DES).

advanced library management system (ALMS)
: A library management system that virtualizes the locations of cartridges in the TS3500 tape library.

Advanced Peer-to-Peer Networking (APPN)
: An extension to SNA that features distributed network control, dynamic definition of network resources, automated resource registration, and automated directory lookup. This network architecture supports the routing of data in a network between two or more Advanced Peer-to-Peer Communication (APPC) systems that do not need to be directly connected.

Advanced System Management Interface (ASMI)
: A graphical interface that is part of the service processor firmware. The ASMI manages and communicates with the service processor. The ASMI is required to set up the service processor and to perform service tasks, such as reading service processor error logs, reading vital product data, and controlling the system power.

AES See Advanced Encryption Standard.

AIX A UNIX operating system developed by IBM that is designed and optimized to run on POWER microprocessor-based hardware such as servers, workstations, and blades.

ALMS See advanced library management system.

alternating current (AC)
An electric current that reverses its direction at regularly recurring intervals.

American Standard Code for Information Interchange (ASCII)
A standard code used for information exchange among data processing systems, data communication systems, and associated equipment. ASCII uses a coded character set consisting of 7-bit coded characters. See also Extended Binary Coded Decimal Interchange Code.

amsl See above mean sea level.

AOTM
See Autonomic Ownership Takeover Manager.

APAR See authorized program analysis report.

application-specific integrated circuit (ASIC)
In computer chip design, a integrated circuit created by first mounting an array of unconnected logic gates on a substrate and later connecting these gates in a particular configuration for a specific application. This design approach allows chips for a variety of applications to be made from the same generic gate array, thereby reducing production costs.

APPN See Advanced Peer-to-Peer Networking.

array A structure that contains an ordered collection of elements of the same data type in which each element can be referenced by its index value or ordinal position in the collection.

ASCII See American Standard Code for Information Interchange.

ASIC See application-specific integrated circuit.

ASMI See Advanced System Management Interface.

assignment
The naming of a specific device to perform a function.

asynchronous
Pertaining to events that are not synchronized in time or do not occur in regular or predictable time intervals.

attention
An informational, warning or error event that is surfaced to the operator in the form of a message as a means to inform the user of the event.

audit logging
The process of keeping a log of all activities of interest to security personnel. These activities are those that can negatively affect operations if completed incorrectly or maliciously. They include such events as: login attempts, configuration changes, status changes, and code updates.

authentication
In computer security, verification of the identity of a user or process and the construction of a data structure that contains the privileges that were granted to the user or process.

authorization (AuthZ)
In computer security, the right granted to a user to communicate with or make use of a computer system.

authorized program analysis report (APAR)
A request for correction of a defect in a supported release of a program supplied by IBM.

AuthZ See authorization.

automatic cartridge facility (ACF)
A small automatic tape cartridge loading device that can manage a small number of tapes for a single 3590 Magstar tape drive.

Autonomic Ownership Takeover Manager (AOTM)
A method by which either Read-Only Takeover (ROT) or Write-Only Takeover (WOT) can be automatically enabled against a failed TS7700 Cluster through internal negotiation methods.

B

b See byte.

B See byte.

back up
To save information or objects on a system, usually to tape or diskette, for safekeeping.

backup object
The first or second backup copy of a primary object in an object backup storage group. Backup copies reside on optical or tape storage.

base operating system (BOS)
The collection of programs that controls the resources and the operations of the computer system.

basic input/output system (BIOS)
The code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BER See bit error rate.

bezel A removable cover for a computer tower or drive.

binding
The process of persistently saving a type or attribute property of a volume.

BIOS See basic input/output system.

BIST See built-in self-test.

bit error rate (BER)
The probability that a transmitted bit will be erroneously received. The BER is measured by counting the number of bits in error at the output of a receiver and dividing by the total number of bits in the transmission. BER is typically expressed as a negative power of 10.

BOS See base operating system.

buffer An area of storage that compensates for the different speeds of data flow or timings of events by temporarily holding a block of data that is waiting to be processed or written to an I/O device.

built-in self-test (BIST)
An internal testing routine that validates the basic operations of a hardware component.

bulk volume information retrieval (BVIR)
A facility that allows a host job to request and obtain information about all of the logical volumes managed by a virtual tape server (VTS), including a Peer-to-Peer VTS.

bus A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment.

BVIR See bulk volume information retrieval.

byte (B)
A string that represents a character and usually consists of eight binary digits that are treated as a unit. A byte is the smallest unit of storage that can be addressed directly.

C

call home
A communication link established between a product and a service provider. The product can use this link to place a call to IBM or to another service provider when it requires service. With access to the machine, service personnel can perform service tasks, such as viewing error and problem logs or initiating trace and dump retrievals.

capacity
The amount of data that can be contained on a storage medium, expressed in bytes of data.

cartridge storage tape (CST)
The base format of a IBM Z® written 3490 compatible tape cartridge, for example MEDIA1 400MB CST.

CCIN See custom card identification number.

CD-ROM
See compact-disc read-only memory.

CDT See common development test.

CEC See central electronics complex.

central electronics complex (CEC)
See central processor complex.

central processor complex (CPC)
A physical collection of hardware that consists of main storage, one or more central processors, timers, and channels.

CIM See Common Information Model.

CKD See count key data.

CLI See command-line interface.

cluster
The combination of a TS7700 Virtualization Engine, 3953 L05 Library Manager, and aTS3500 Tape Library to form a virtual tape subsystem.

cluster family
A group of clusters all configured with the same family value in vital product data (VPD).

command-line interface (CLI)
A computer interface in which the input and output are text based.

common development test (CDT)
A development and test environment for GNA/GWA applications, designed and built in accordance with customer requirements and GWA and GNA standards.

Common Information Model (CIM)
An implementation-neutral, object-oriented schema for describing network management or systems management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

communication scanner processor (CSP)
A processor in the 3725 Communication Controller that contains a microprocessor with a control code. The code controls transmission of data over links attached to the CSP.

compact-disc read-only memory (CD-ROM)
High-capacity read-only memory in the form of an optically read compact disc.

Composite Library ID
The library sequence number reported to a host by each attached virtual device.

concurrent
Pertaining to diagnostic, maintenance, or replacement procedures that can be performed on a system without interrupting customer applications.

construct
A collective term used to refer to the policies that automate storage management through classification of data sets. These include: storage groups, management classes, storage classes, data classes.

controller
A device that coordinates and controls the operation of one or more input/output devices (such as workstations) and synchronizes the operation of such devices with the operation of the system as a whole.

controller drawer
A physical enclosure which contains controller cards. See also expansion drawer.

control unit (CU)
A device that coordinates and controls the operation of one or more input/output devices. For example, a TS7700 has up to 31 control units, each one emulating 16 3490E logical tape drives.

Coordinated Universal Time (UTC)
The international standard of time that is kept by atomic clocks around the world.

copy The replication of a virtual volume from one site to another across the connecting infrastructure.

count key data (CKD)
A data recording format that uses self-defining record formats in which

each record on a volume is represented by up to three fields: a count field identifying the record and specifying its format, an optional key field that can be used to identify the data area contents, and an optional data field that typically contains the user data.

CPC See central processor complex.

CRC See cyclic redundancy check.

CRU See customer-replaceable unit.

CSP See communication scanner processor.

CST See cartridge storage tape.

CSV file
A text file that contains comma-separated values. A CSV file is commonly used to exchange files between database systems and applications that use different formats.

CU See control unit.

custom card identification number (CCIN)
A unique alphanumeric number that is assigned many individual hardware parts or assemblies.

customer-replaceable unit (CRU)
An assembly or part that can be replaced in its entirety by a user when any one of its components fails.

cyclic redundancy check (CRC)
A system of error checking performed at both the sending and receiving station after a block-check character has been accumulated.

D

DAA See device allocation assistance.

DASD
See direct access storage device.

data A representation of facts or instructions in a form suitable for communication, interpretation, or processing by human or automatic means. Data includes constants, variables, arrays, and character strings.

Data Facility Storage Management Subsystem (DFSMS)
An operating environment that helps automate and centralize the management of storage. To manage storage, the storage management subsystem (SMS) provides the storage administrator with control over data class, storage class, management class, storage group, and automatic class selection (ACS) routine definitions.

data key (DK)
In cryptography, a key that is used to encrypt or decrypt data only, but not to encrypt or decrypt other keys.

DC See direct current.

DDM See disk drive module.

DDR1 See double data rate first generation.

dedicated service tool (DST)
The part of the service function used to service the system when the operating system is not running.

dense wavelength division multiplexing (DWDM)
A technology that places many optical signals onto one single-mode fiber using slightly different optical frequencies. DWDM enables many data streams to be transferred in parallel.

detent A catch or lever that holds another part in place.

device allocation assistance (DAA)
A function that allows the host to query the TS7740 Virtualization Engine to determine which clusters should be preferred for a private (specific) mount request.

DFS See Distributed File Service.

DFSMS
See Data Facility Storage Management Subsystem.

DFSMSdfp
A DFSMS functional component and a base element of z/OS that provides functions for storage management, data management, device management, and distributed data access.

DFSMShsm
A DFSMS functional component or base element of z/OS that provides functions for backing up and recovering data, and managing space on volumes in the storage hierarchy.

DFSMSrmm
A DFSMS functional component or base element of z/OS, that manages removable media (tape volumes, tape data sets, and tape libraries).

DHCP See Dynamic Host Configuration Protocol.

digital versatile disc (DVD)
An optical disc that has the same overall dimensions of a CD-ROM, but has significantly higher capacities than a CD-ROM. DVDs are also double sided, whereas CD-ROMs are single sided.

DIMM
See dual inline memory module.

direct access storage device (DASD)
A device that allows storage to be directly accessed, such as a disk drive. See also random access memory.

direct current (DC)
Electric current that flows in a single direction and at a constant voltage.

direct memory access (DMA)
The transfer of data between memory and an input/output device without processor intervention.

disk drive module (DDM)
A field-replaceable unit (FRU) that consists of a single disk drive and its associated packaging.

disk-only
Pertaining to a cluster that does not attach to a physical tape library; it stores all data in cache.

disk storage subsystem
See disk subsystem.

disk subsystem
: The part of a computer system that provides the storage. It includes the controller and disk drives.The IBM TS7700 and No-tape Virtual Tape, 3956-CC7/CS7/CC8/CS8 are collectively referred to as a disk subsystem.

Distributed File Service (DFS)
: A component of a Distributed Computing Environment (DCE) that enables a single, integrated file system to be shared among all DCE users and host computers in a DCE cell. DFS prevents DCE users from simultaneously modifying the same information.

Distributed Library ID
: The unique library sequence number possessed by each cluster in a grid configuration.

DK See data key.

DLO See document library object.

DLPAR
: See dynamic LPAR.

DMA See direct memory access.

document library object (DLO)
: Any system object that resides in the document library, such as RFT and FFT documents, folders, and PC files.

double data rate first generation (DDR1)
: The first generation of memory DIMMs which have double the speed of single data rate (SDR) memory.

DRAM
: See dynamic random access memory.

drawer
: A unit that contains multiple disk drive modules (DDMs) and provides power, cooling, and related interconnection logic to make the DDMs accessible to attached host systems.

DST See dedicated service tool.

dual inline memory module (DIMM)
: A small circuit board with memory-integrated circuits containing signal and power pins on both sides of the board.

DVD See digital versatile disc.

DWDM
: See dense wavelength division multiplexing.

Dynamic Host Configuration Protocol (DHCP)
: A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

dynamic LPAR (DLPAR)
: The ability to move processors, memory, and interactive performance between logical partitions without restarting a logical partition or the server. See also logical partition.

dynamic random access memory (DRAM)
: Storage in which the cells require repetitive application of control signals to retain stored data.

E

EBCDIC
See Extended Binary Coded Decimal Interchange Code.

EC See engineering change.

ECC See error correction code.

EEDK See externally encrypted data key.

EEH See extended error handling.

EIA See Electronics Industries Association.

EIA unit
A unit of measure, established by the Electronic Industries Association, equal to 44.45 millimeters (1.75 inches).

EiB See exbibyte.

EKM See External Key Manager.

electromagnetic compatibility (EMC)
The design and test of products to meet legal and corporate specifications dealing with the emissions and susceptibility to frequencies in the radio spectrum. Electromagnetic compatibility is the ability of various electronic equipment to operate properly in the intended electromagnetic environment.

Electronics Industries Association (EIA)
An organization of electronics manufacturers that advances the technological growth of the industry, represents the view of its members, and develops industry standards.

electrostatic discharge (ESD)
The flow of current that results when objects having a static charge come into close enough proximity to discharge.

EMC See electromagnetic compatibility.

emergency power off (EPO)
A means of turning off power during an emergency, referring usually to a switch.

enclosure services manager (ESM)
A redundant and hot-swappable SAS communication FRU that provides SAS expander and SES functions.

engineering change (EC)
An update to a machine, part, or program. Each EC for a given unit is assigned a unique number referred to as an EC level or EC number.

environmental recording, editing, and printing (EREP)
The program that formats and prepares reports from the data contained in the error recording data set.

EPO See emergency power off.

EPROM
See erasable programmable read-only memory.

equipment check
An asynchronous indication of a malfunction.

erasable programmable read-only memory (EPROM)
A type of memory chip that can retain its contents without electricity. Unlike the programmable read-only memory (PROM), which can be programmed only once, the EPROM can be erased by ultraviolet light and then reprogrammed.

ERDS See error-recording data set.

EREP See environmental recording, editing, and printing.

error correction code (ECC)
A code appended to a data block that has the capability to detect and correct multiple bit errors within the block.

error log
A data set or file that is used to record error information about a product or system.

error-recording data set (ERDS)
On S/390 and zSeries hosts, a data set that records data-storage and data-retrieval errors. A service information message (SIM) provides the error information for the ERDS.

ESD See electrostatic discharge.

ESM See enclosure services manager.

exbibyte (EiB)
IEC Standard is 1024 pebibytes.

expansion drawer
A drawer that expands the disk capacity of the disk subsystem. These drawers do not contain any controller cards. See also controller drawer.

Extended Binary Coded Decimal Interchange Code (EBCDIC)
A coded character set of 256 8-bit characters developed for the representation of textual data. See also American Standard Code for Information Interchange.

extended error handling (EEH)
An error-recovery mechanism for errors that occur during load and store operations on the PCI bus.

External Key Manager (EKM)
The external server used to manage the EEDK keys in a solution which supports encryption (for example: ISKLM).

externally encrypted data key (EEDK)
A method of cryptographically encrypting a Data Key (DK) using an externally managed encryption key, allowing the data key to be stored within the media device in encrypted form.

F

failing function code (FFC)
A numeric code that identifies which function failed within the system.

fault symptom code (FSC)

1. A hexadecimal code generated by the drive or the control unit microcode in response to a detected subsystem error.
2. A numeric code that identifies which process or component that appears to be at fault for a system or hardware failure.

FC See feature code.

FC-AL See Fibre Channel Arbitrated Loop.

FCP See Fibre Channel Protocol.

FDDI See Fiber Distributed Data Interface.

feature code (FC)
A code used by IBM to process hardware and software orders.

FEC “Forward error correction (FEC)” on page 356

FFC See failing function code.

Fiber Distributed Data Interface (FDDI)
An American National Standards Institute (ANSI) standard for a 100 Mbps LAN using fiber optic cables.

Fibre Channel Arbitrated Loop (FC-AL)
An implementation of the Fibre Channel standards that uses a ring topology for the communication fabric; refer to American National Standards Institute (ANSI) INCITS 272-1996, (R2001). In this topology, two or more Fibre Channel end points are interconnected through a looped interface.

Fibre Channel Protocol (FCP)
The serial SCSI command protocol used on Fibre Channel networks.

Fibre connection channel (FICON)
A communication protocol, over Fibre Channel, designed for IBM mainframe computers and attached storage peripherals.

FICON
See Fibre connection channel.

FID See FRU Identifier.

field-replaceable unit (FRU)
An assembly or part that is replaced in its entirety by service personnel when any one of its components fails.

FIFO See first-in first-out.

file A named set of records stored or processed as a unit.

file system (FS)

1. The collection of files and file management structures on a physical or logical mass storage device, such as a diskette or minidisk.
2. In the hierarchical file system, the underlying system support that manages I/O operations to files and controls the format of information on the storage media. A file system allows applications to create and manage files on storage devices and to perform I/O operations to those files.
3. A collection of files and certain attributes associated with those files.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

first-in first-out (FIFO)
A queuing technique in which the next item to be retrieved is the item that has been in the queue for the longest time.

flexible service processor (FSP)
Firmware that provides diagnostics, initialization, configuration, runtime error detection, and correction. The flexible service processor connects the managed system to the Hardware Management Console.

format
The arrangement or layout of data in a data medium.

Forward error correction (FEC)
Forward error correction (FEC) or channel coding is a technique used for controlling errors in data transmission over unreliable or noisy communication channels.

FRU See field-replaceable unit.

FRU Identifier (FID)
A short code that can be used by service technicians to isolate problems with the 3592 tape drive.

FS See file system.

FSC See fault symptom code.

FSP See flexible service processor.

FTP See File Transfer Protocol.

functional microcode
Microcode that is resident in the machine during normal customer operation.

G

Gb See gigabit.

GB See gigabyte.

Gbps See gigabits per second.

General Parallel File System (GPFS)
A high-performance shared-disk file system that can provide data access from nodes in a clustered system environment.

GHz See gigahertz.

GiB See gibibyte.

gibibyte (GiB)
In digital information storage, a base-2 unit of measurement equal to 1,073,741,824 bytes (2 to the 30th power). See also gigabyte.

Gigabaud Link Module (GLM)
An encoding/decoding device that is a Class-1 laser component assembly with transmitting and receiving receptacles that connect to fiber-optic cables. The GLM provides the link-control facility for an N_port. It converts electrical signals from parallel to serial to optical when transmitting, and the opposite when receiving. GLMs are not hot-swappable.

gigabit (Gb)
In data communications, 10 to the power of 9 or 1,000,000,000 bits. See also gigabyte.

gigabits per second (Gbps)
A measure of high speed bandwidth on a digital data transmission medium such as optical fiber.

gigabyte (GB)
For processor storage, real and virtual storage, and channel volume, two to the power of 30 or 1,073,741,824 bytes. For disk storage capacity and communications volume, 1,000,000,000 bytes. See also gibibyte, gigabit.

gigahertz (GHz)
A unit of frequency equal to 1,000,000,000 hertz.

GLM See Gigabaud Link Module.

GMT See Greenwich mean time.

gNode
The combination of the distributed nodes hNode and vNode in the TS7700 Virtualization Engine

GPFS See General Parallel File System.

graphical user interface (GUI)
A computer interface that presents a visual metaphor of a real-world scene, often of a desktop, by combining high-resolution graphics, pointing devices, menu bars and other menus, overlapping windows, icons and the object-action relationship.

Greenwich mean time (GMT)
The mean solar time at the meridian of Greenwich, England.

grid A series of clusters connected to one another by means of TCP/IP to form a disaster recovery solution where virtual volume attributes and data are replicated across the clusters to ensure the continuation of production work.

grid network
The TCP/IP infrastructure connecting a grid.

GUI See graphical user interface.

H

HA See high availability.

hardware configuration definition (HCD)
An interactive interface in z/OS that is used to define hardware configurations to the operating system and the channel subsystem.

Hardware Management Console (HMC)
A system that controls managed systems, including the management of logical partitions and use of Capacity Upgrade on Demand. Using service applications, the HMC communicates with managed systems to detect and consolidate information, which is then sent to IBM for analysis.

hardware service manager (HSM)
A tool for displaying and working with system hardware from both a logical and a packaging viewpoint, for debugging input/output processors (IOPs) and devices, and for fixing failing and missing hardware.

HBA See host bus adapter.

HCA See host channel adapter.

HCD See hardware configuration definition.

head of string
The first controller enclosure in a string. See also string.

hertz (Hz)
A unit of frequency equal to one cycle per second.

hex See hexadecimal.

hex, HEX
See hexadecimal.

hexadecimal (hex, hex, HEX)
Pertaining to a numbering system that has a base of 16.

hierarchical storage management (HSM)
A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

High-Performance Parallel Interface (HIPPI)
An ANSI-standard, high-speed, connection-oriented, communication channel. It is used primarily to connect supercomputers and as a high-speed LAN.

high-speed link (HSL)
A hardware connectivity architecture that links system processors to system I/O buses and other systems.

HIPPI See High-Performance Parallel Interface.

HiPPI See High-Performance Parallel Interface.

HMC See Hardware Management Console.

hNode
A distributed node in the TS7700 Virtualization Engine that performs all management of a virtual volume residing in disk cache or physical tape after it has been created or altered by the host system through a vNode.

host A z system partition that is connected over FICON to the TS7700 and runs one or more applications that require the use of 3490 virtual tape drives.

host adapter
See host port.

host bus adapter (HBA)
An interface card that connects a host bus, such as a peripheral component interconnect (PCI) bus, to the storage area network.

host channel
The communication path between the disk subsystem and the AIX controller. The disk subsystem has fibre connections to the AIX controller and to its physical drives. From the viewpoint of the disk subsystem, the AIX controller is the host.

host channel adapter (HCA)
Based on InfiniBand technology, a port connection on a system allowing a network fabric interconnect.

host group
A group of hosts that together share certain logical volumes in a disk subsystem.

host port
A physical connection to a host using fibre cards.

host port identifier
The unique numerical identifier to a host port using the adapter's world-wide node name (WWNN) which is set by factory for each adapter and is unique to that adapter.

HSL See high-speed link.

HSM
1. See hardware service manager.
2. See hierarchical storage management.

HTML
See Hypertext Markup Language.

Hypertext Markup Language (HTML)
A markup language that conforms to the Standard Generalized Markup Language (SGML) standard and was designed primarily to support the online display of textual and graphical information, including hypertext links.

Hz See hertz.

I

IB See InfiniBand.

ICSF See integrated cryptographic service facility.

ID See identifier.

IDE See integrated development environment.

identifier (ID)
1. A sequence of bits or characters that identifies a user, program, device, or system to another user, program, device, or system.
2. In programming languages, a lexical unit that names a language object, such as the name of an array, record, label, or procedure. An identifier usually begins with a letter optionally followed by letters, digits, or other characters.
3. One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element.

IEC See International Electrochemical Commission.

IML See initial microprogram load.

IMPL See initial microprogram load.

InfiniBand (IB)
An industry-standard specification that defines an I/O architecture used to connect servers, communications infrastructure equipment, storage, and embedded systems.

initial microprogram load (IML, IMPL)
The action of loading microprograms into computer storage.

initial program load (IPL)
The process that loads the system programs from the system auxiliary storage, checks the system hardware, and prepares the system for user operations.

initiator
The component that executes a command. The initiator can be the host system or the tape control unit.

input/output (I/O)
Pertaining to a device, process, channel, or communication path involved in data input, data output, or both.

integrated cryptographic service facility (ICSF)
A software element of z/OS that works with hardware cryptographic features and RACF to provide secure, high-speed cryptographic services.

integrated development environment (IDE)
A set of software development tools, such as source editors, compilers, and debuggers, that are accessible from a single user interface.

Interactive Storage Management Facility (ISMF)
An Interactive System Productivity Facility (ISPF) application that provides an interactive set of space management functions for users and storage administrators.

interface
A shared boundary between independent systems. An interface can be a hardware component used to link two devices, a convention that supports communication between software systems, or a method for a user to communicate with the operating system, such as a keyboard.

International Electrochemical Commission (IEC)
The international standards-setting organization responsible for electrical and electrotechnical issues. IEC often cooperates with ISO via technical committees on the definition of standards.

inter-switch link (ISL)
The physical connection that carries a protocol for interconnecting multiple routers and switches in a storage area network (SAN).

I/O See input/output.

IPL See initial program load.

ISL See inter-switch link.

ISMF See Interactive Storage Management Facility.

J

JBOD See just a bunch of disks.

JCL See job control language.

JFS See journaled file system.

job control language (JCL)
A command language that identifies a job to an operating system and describes the job requirements.

journaled file system (JFS)
The local file system in the AIX operating system.

just a bunch of disks (JBOD)
Hard disks that haven't been configured according to the RAID system to increase fault tolerance and improve data access performance.

K

KB See kilobyte.

KEK See key-encrypting key.

key-encrypting key (KEK)
A key that is used exclusively for encrypting and decrypting keys.

KiB See kibibyte.

kibibyte (KiB)
A base-2 unit of measurement that is equal to 1,024 bytes (2 to the 10th power). See also kilobyte.

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 2 to the power of 10 or 1,024 bytes. For disk storage capacity and communications volume, 1,000 bytes. See also kibibyte.

kilovolt amperes (kVA)
A unit of power.

kVA See kilovolt amperes.

L

LAN See local area network.

LAU See local authentication.

LBA See logical block address.

LDAP See Lightweight Directory Access Protocol.

LED See light-emitting diode.

library manager (LM)
The software application that controls all operations in an Automated Tape Library Dataserver (ATLDS) or in a file.

LIC See Licensed Internal Code.

Licensed Internal Code (LIC)
The layered architecture below the machine interface (MI). The Licensed Internal Code is a proprietary system design that carries out many functions. These functions include but are not limited to storage management, pointers and addressing, program management functions, exception and event management, data functions, I/O managers, and security.

LID See local identifier.

light-emitting diode (LED)
A semiconductor chip that gives off visible or infrared light when activated.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

Lightweight Third Party Authentication (LTPA)
An authentication framework that allows single sign-on across a set of web servers that fall within an Internet domain.

LIP See loop initialization primitive.

LM See library manager.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network. See also wide area network.

local authentication (LAU)
The process of validating a user identity to the system according to the local operating system account to which the user logged in. If the user is authenticated, the user is mapped to a principal.

local identifier (LID)
In a distributed relational database, an identifier or short label that is mapped by the environmental descriptors to a named resource.

logical block address (LBA)
The block number on a disk.

logical partition (LP, LPAR)
One or more virtualized images of a hardware computing system that can include shared and dedicated resources assigned from the pool of resources available on a physical server. Each image appears to the operating system running within it to be a unique instance of a physical server. See also dynamic LPAR.

logical subsystem (LSS)
The logical functions of a storage controller with which one or more host I/O interfaces can access a set of devices. The controller groups the devices according to the addressing mechanisms of the associated I/O interfaces. One or more LSSs exist on a storage controller. In general, the controller associates a given set of devices with only one LSS.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier used to differentiate devices, each of which is a logical unit (LU).

logical volume (LV)
A collection of physical partitions organized into logical partitions, all contained in a single volume group. Logical volumes are expandable and can span several physical volumes in a volume group.

Logical Volume Manager (LVM)
A set of system commands, library routines, and other tools that allow the user to establish and control logical volume (LVOL) storage. The LVM maps data between the logical view of storage space and the physical disk drive module (DDM).

long wave laser (LW)
Single Mode Fibre (SMF), which utilizes a transmitter which emits light in longer wavelength forms. Such Fibre Channel connections tend to support longer single fibre distances when compared to its counterpart Multi Mode Fibre (MMF) or shortwave connections.

loop initialization primitive (LIP)
A Fibre Channel primitive used to indicate a loop failure, reset a specific node, or initiate a procedure that results in unique addressing for all nodes.

LP See logical partition.

LPAR See logical partition.

LSS See logical subsystem.

LTPA See Lightweight Third Party Authentication.

LUN See logical unit number.

LV See logical volume.

LVM See Logical Volume Manager.

LW See long wave laser.

M

MAC See Media Access Control.

magnetic tape
A tape with a magnetic surface layer on which data can be stored.

main storage dump (MSD)
A process of collecting data from the system's main storage. It can be done automatically by the service processor as a result of a system failure, or it can be performed manually by the operator when there appears to be a system failure.

maintenance analysis procedure (MAP)
In hardware maintenance, a step-by-step procedure that assists an IBM service representative to trace a symptom to the cause of the failure.

MAP See maintenance analysis procedure.

mask

1. To use a pattern of characters to control retention or elimination of portions of another pattern of characters.
2. A pattern of bits or characters that controls the keeping, deleting, or testing of portions of another pattern of bits or characters.

MB See megabyte.

Mbps See megabits per second.

MCM See multiple chip module.

MDE See microcode detected error.

mebibyte (MiB)
A base-2 unit of measurement that is equal to 1,048,576 bytes (2 to the 20th power). See also megabyte.

Media Access Control (MAC)
In networking, the lower of two sublayers of the Open Systems Interconnection model data link layer. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.

media information message (MIM)
A message that identifies problems with the media (tape) and the volume number of the bad cartridge. This identification allows the customer to do maintenance within the tape library and to prevent unnecessary service calls when the fault is media.

megabits per second (Mbps)
A measure of bandwidth on a data transmission medium, where 1 Mbps = 1,000,000 bits per second.

megabyte (MB)
For processor storage, real and virtual storage, and channel volume, 2 to the 20th power or 1,048,576 bytes. For disk storage capacity and communications volume, 1,000,000 bytes. See also mebibyte.

megahertz (MHz)
A unit of measure of frequency. One megahertz equals 1 000 000 hertz.

MES See miscellaneous equipment specification.

MHz See megahertz.

MiB See mebibyte.

microcode

1. To design, write, and test one or more microinstructions.
2. Stored microinstructions, not available to users, that perform certain functions.
3. A code, representing the instructions of an instruction set, that is implemented in a part of storage that is not program-addressable. See also microprogram.

microcode detected error (MDE)
A numeric 16-bit value that is assigned to a particular error or event which was detected by the solution microcode.

microinstruction
A basic or elementary machine instruction.

microprogram
A group of microinstructions that when executed performs a preplanned function. Micorinstructions can include a dynamic arrangement or selection of one or more groups of microinstructions for execution to perform a particular function. See also microcode.

MIM See media information message.

miscellaneous equipment specification (MES)
A hardware change that is made after the time of the initial order.

MMF See multimode fiber.

modifier
A word or quantifier that is used to change an instruction, thereby causing the execution of a different instruction. Consequently, the original instruction, successively changed by a modifier, can be used repetitively to carry out a different operation each time it is used.

mount A host command to load a tape cartridge into a tape drive.

MPIO See multipath I/O.

MSD See main storage dump.

multimode fiber (MMF)
An optical fiber that is designed to carry multiple light rays or modes concurrently, each at a slightly different reflection angle within the optical fiber core.

MMF fiber is currently 50 microns in diameter (older version was 62.5 micron) and carries Short Wave length optical signals. The length allowed decreases as the gig hertz of the optical signal increases. The MM fiber casing (used to be orange in color) and the improved MM fiber casing is aqua in color.

multipath
A storage configuration that supports multiple paths from servers to disks.

multipath I/O (MPIO)
A framework that enables multiple storage connections and provides automatic failover between connections to ensure that storage is accessible in case of a hardware failure.

multiple chip module (MCM)
The fundamental processor building block of some IBM Power Systems servers.

Multiple Virtual Storage (MVS)
An IBM operating system that accesses multiple address spaces in virtual storage.

MVS See Multiple Virtual Storage.

N

NAT See network address translation.

NENR See Non-Erasable Non-Rewritable.

NetTerm
A configurable terminal emulator designed for Internet and intranet connections.

network address translation (NAT)
1. The conversion of a network address that is assigned to a logical unit in one network into an address in an adjacent network.
2. In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network file server (NFS)
A protocol that allows a computer to access files over a network as if they were on its local disks.

Network Installation Management (NIM)
An environment that provides installation and configuration of software within a network interface.

network interface controller (NIC)
Hardware that provides the interface control between system main storage and external high-speed link (HSL) ports.

Network Time Protocol (NTP)
A protocol that synchronizes the clocks of computers in a network.

NFS See network file server.

NIC See network interface controller.

NIM See Network Installation Management.

node A single replaceable unit within a IBM® Virtualization Engine TS7700. Nodes are the elements that run the functional code and perform all the system logic. Each node consists of one or more processors, memory, and I/O ability.

nonce A random, unique text string that is encrypted along with data and then is used to detect attacks against the system that sends the encrypted data. A nonce is used especially for authentication and ensures that encrypted data is different each time that it is encrypted.

Non-Erasable Non-Rewritable (NENR)
A compliance term that refers to a solution that not only prevents rewrite (Write Once, Read Many, or, WORM), but also prevents deletion (erasing) through retention. LWORM (logical WORM), used with host software retention characteristics, provide a NENR-compliant solution.

nonvolatile random access memory (NVRAM)
Random access memory (storage) that retains its contents after the electrical power to the machine is shut off.

NTP See Network Time Protocol.

NVRAM
See nonvolatile random access memory.

O

Object Data Manager (ODM)
A data manager intended for the storage of system data. The ODM is used for many system management functions. Information used in many commands and System Management Interface Tool (SMIT) functions is stored and maintained in the ODM as objects with associated characteristics.

object information repository (OIR)
In System Manager, the information about each object that identifies which product it is associated with, such as the release level, option, and the load identifier.

ODM See Object Data Manager.

offline
Pertaining to the operation of a device that is not under the control of a system. See also online.

OIR See object information repository.

online Pertaining to the operation of a functional unit or device that is under the control of the system or of a host. See also offline.

overrun
The loss of data because a receiving device is unable to accept data at the rate it is transmitted.

P

PAL See product activity log.

parameter
A variable that is given a constant value for a specified application and that may denote the application.

PCC See power control compartment.

PCI See Peripheral Component Interconnect.

PCI host bridge (PHB)
A device that merges data from PCI bridges for delivery to the system processor.

PDF See Portable Document Format.

PDU See power distribution unit.

pebibyte (PiB)
A base-2 unit of measurement that is equal to 1 125 899 906 842 624 bytes bytes (2 to the 50th power).

peer-to-peer (PtP)
Pertaining to a form of distributed processing, in which the front-end and back-end of a conversation switch control between themselves. It is communication between equals.

perform library function (PLF)
A family of commands which IBM Z® utilizes to communicate with IBM branded automated tape libraries, such as the TS7700 or 3992 Tape Controller Model C07.

Peripheral Component Interconnect (PCI)
A local bus that provides a high-speed data path between the processor and attached devices.

PFA See Predictive Failure Analysis.

PHB See PCI host bridge.

physical mount
A virtual action in which a virtual volume is assigned to a virtual tape drive. See also virtual.

physical volume
A volume that has a one-to-one association with physical tape media and is used directly by z/OS applications. Physical volumes may reside in an Automated Tape Library Dataserver (ATLDS) or be kept on shelf storage either at vault sites or within the data center where they can be mounted on stand-alone tape drives.

PiB See pebibyte.

PLF See perform library function.

pool A group of physical tape cartridges.

POR See power-on reset.

port An end point for communication between applications, generally referring to a logical connection. A port provides queues for sending and receiving data. Each port has a port number for identification.

Portable Document Format (PDF)
A standard specified by Adobe Systems, Incorporated, for the electronic distribution of documents. PDF files are compact; can be distributed globally via email, the web, intranets, or CD-ROM; and can be viewed with the Acrobat Reader.

POST See power-on self-test.

power control compartment (PCC)
The rack component that logically controls the application of alternating current power to the units in the rack.

power cord
The electrical connection between the AC power source and the computer.

power distribution unit (PDU)
A device that is used to distribute electrical power to datacenter equipment.

power-on reset (POR)
A key sequence that restarts the operating system (or other program) without turning off the electrical power of the system.

power-on self-test (POST)
A series of internal diagnostic tests activated each time the system power is turned on.

PPS See primary power supply.

Predictive Failure Analysis (PFA)
A scheduled evaluation of system data that detects and signals parametric degradation which might lead to functional failures.

premigration
The process of copying data that is eligible for migration to a lower tier of storage, such as physical tape, but leaving the original instance intact.

primary object
An object that in the OAM storage hierarchy (disk, optical, or tape) that can be retrieved through the OAM Retrieve API.

primary power supply (PPS)
A power supply that attaches to the customer's ac input power; generates and distributes 390 V dc; and controls and monitors associated power functions.

processor
In a computer, the part that interprets and executes instructions. Two typical components of a processor are a control unit and an arithmetic logic unit.

product activity log (PAL)
A log of system data, Licensed Internal Code data, software components, subsystem information, and I/O device data.

program temporary fix (PTF)
A fix that is made available to all customers. A program temporary fix is tested by IBM. It contains a PTF record.

PTF See program temporary fix.

PtP See peer-to-peer.

R

RACF See Resource Access Control Facility.

RAID See Redundant Array of Independent Disks.

RAM See random access memory.

random access memory (RAM)
Computer memory in which any storage location can be accessed directly. See also direct access storage device.

RAS See reliability, availability, and serviceability.

RBAC See role-based access control.

read-only
Pertaining to data that can be read but cannot be modified.

read-only memory (ROM)
Memory in which stored data cannot be changed by the user except under special conditions.

read ownership takeover (ROT)
A mode enabled for a failed cluster that allows volume ownership to be taken from a failed TS7700 Cluster by any other available TS7700 Cluster. Only read access to the volume is allowed through the remaining TS7700 Clusters in the event the volume is taken over. Once ownership for a volume has been taken in this mode, any operation attempting to modify data on that volume or change its attributes fails.

reason code
A value used to indicate the specific reason for an event or condition.

recall To move a virtual volume from a physical volume to the cache.

recoverable error
An error condition that can be automatically corrected (for example, by retry operation) and, when corrected, allows continued processing of a job, a program, or a hardware function.

reduced instruction set computing (RISC)
A computer that uses a small, simplified set of frequently used instructions for rapid processing.

Redundant Array of Independent Disks (RAID)
A collection of two or more physical disk drives that present to the host an image of one or more logical disk drives. In the event of a physical device failure, the data can be read or regenerated from the other disk drives in the array due to data redundancy. See also Serial Storage Architecture.

reference code
A group of characters that identifies the machine status or a specific error condition.

reliability, availability, and serviceability (RAS)
A combination of design methodologies, system policies, and intrinsic capabilities that, taken together, balance improved hardware availability with the costs required to achieve it. Reliability is the degree to which the hardware remains free of faults. Availability is the ability of the system to

continue operating despite predicted or experienced faults. Serviceability is how efficiently and nondisruptively broken hardware can be fixed.

Remote Supervisor Adapter (RSA)
An IBM service processor that is built into some System x servers and available as an optional adapter for use with others. When used as a gateway service processor, the RSA can communicate with all service processors on the Advanced System Management (ASM) interconnect.

Resource Access Control Facility (RACF)
An IBM licensed program that provides access control by identifying users to the system; verifying users of the system; authorizing access to protected resources; logging unauthorized attempts to enter the system; and logging accesses to protected resources.

resource ID
The programmable list entry ID that IMS specifies for a resource to ensure name uniqueness. The first byte is the name type, and the remaining 11 bytes are the resource name, padded with blanks.

resource manager (RM)
A subsystem or component that manages resources that can be involved in transactions. Resource managers can be categorized as work managers, data resource managers, and communication resource managers.

Returned Part Miscellaneous Equipment Specification (RPMES)
A special miscellaneous equipment specification that requires the return of selected parts to IBM on completion of the MES.

RISC See reduced instruction set computing.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

RM See resource manager.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

ROM See read-only memory.

ROT See read ownership takeover.

RPMES
See Returned Part Miscellaneous Equipment Specification.

RSA

1. See Remote Supervisor Adapter.
2. See Rivest-Shamir-Adleman algorithm.

S

SAA See scratch allocation assistance.

SAN See storage area network.

SAS See serial-attached SCSI.

SATA See Serial Advanced Technology Attachment.

SC See Standard Connector.

SCC See Serial Communication Controller.

scratch allocation assistance (SAA)
An extension of the device allocation assistance (DAA) function for scratch mount requests. It filters the list of clusters in a grid to return to the host a smaller list of candidate clusters specifically designated as scratch mount candidates.

scratch pool
The collection of tape cartridges from which requests for scratch tapes can be satisfied.

SCSI See Small Computer System Interface.

SCSI Enclosure Services (SES)
A subset of the small computer system interface (SCSI) protocol used to monitor temperature, power, and fan status for enclosure devices.

SDAC See selective device access control.

SDLC See Synchronous Data Link Control.

SDRAM
See synchronous dynamic random access memory.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective device access control (SDAC)
A function that allows only certain logical control units or subsystem IDs within a composite library to have exclusive access to one or more VOLSER ranges of volumes for host-initiated mounts, ejects, and attributes or categories changes.

Serial Advanced Technology Attachment (SATA, Serial ATA)
A standard for connecting storage devices such as hard drives and CD ROM drives to computer systems that is based on serial signaling technology.

Serial ATA
See Serial Advanced Technology Attachment.

serial-attached SCSI (SAS)
A data-transfer technology that moves data to and from computer storage devices. Serial-attached SCSI uses a point-to-point serial protocol, which replaces the traditional, parallel SCSI bus technology.

Serial Communication Controller (SCC)
A MULTIBUS board providing four high-speed RS-232-C serial interface ports to support the High-Level Data Link Control (HDLC) data-link protocol for use in X.25 networks.

Serial Storage Architecture (SSA)
An American National Standards Institute (ANSI) standard, implemented by IBM, for a high-speed serial interface that provides point-to-point connection for peripherals, such as storage arrays. See also Redundant Array of Independent Disks.

service information message (SIM)
A message, generated by a storage subsystem, that is the result of error event location and analysis. A SIM indicates that some service action is required.

service request number (SRN)
A code that is used by service technicians or the customer to determine the failing area of the system.

SES See SCSI Enclosure Services.

SFP See Small Form-factor Pluggable.

short wave laser (SW)
Single Mode Fibre (SMF), which utilizes a transmitter that emits light in shorter wavelength forms. Such Fibre Channel connections tend to support shorter single fibre distances when compared to its counterpart Multi Mode Fibre (MMF) or longwave connections.

SIM See service information message.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP trap.

Simple Network Management Protocol Management Information Block (SNMP MIB)
A file used by an SNMP monitoring application to relate a message identifier to a corresponding text string.

single-mode optical fiber (SM)
Single mode fiber is fiber that is 9 microns in diameter and carries Long Wave length optical signals. The SM fiber casing is yellow in color.

SLDC See streaming lossless data compression.

SM See single-mode optical fiber.

Small Computer System Interface (SCSI)
An ANSI-standard electronic interface that allows personal computers to communicate with peripheral hardware, such as disk drives, tape drives, CD-ROM drives, printers, and scanners faster and more flexibly than previous interfaces.

Small Form-factor Pluggable (SFP)
An optical transceiver used to convert signals between optical fiber cables and switches.

SMI-S See Storage Management Initiative Specification.

SMIT See System Management Interface Tool.

SMS See system management services.

SMSplex
See system-managed storage complex.

SNA distribution services
See Systems Network Architecture distribution services.

SNADS
See Systems Network Architecture distribution services.

SNIA See Storage Networking Industry Association.

SNMP
See Simple Network Management Protocol.

SNMP MIB
See Simple Network Management Protocol Management Information Block.

SNMP Monitoring Application
An application running on a network-attached server. It receives SNMP traps from network-attached devices, expands those traps using a MIB file, and can take a variety of actions based on the SNMP traps, including filtering , keeping a history log, and sending emails or text messages to users.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOM See System Object Model.

spare An extra storage component, such as a drive or tape, that is predesignated for use as a replacement for a failed component.

SPCN See system power control network.

SRAM
See static random access memory.

SRC See system reference code.

SRN See service request number.

SSA See Serial Storage Architecture.

SSID See subsystem identifier.

SSL See Secure Sockets Layer.

SST See system service tools.

stacked volume
A volume that has a one-to-one association with physical tape media and is used in a virtual tape server (VTS) to store logical volumes (LVOLs). Stacked volumes are not used by MVS applications but by the VTS and its associated utilities. They may be removed from a VTS to allow transportation of LVOLs to a vault or to another VTS.

Standard Connector (SC)
The larger of two most popular push-pull type fibre cable connector types.

static random access memory (SRAM)
Random access memory that holds its data in static form (without refreshing), for as long as power is supplied to the circuit.

storage area network (SAN)
A dedicated storage network tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

Storage Authentication Service policy authentication
A Role-Based Access Control method of authentication that uses LDAP to create a central repository for storage and management of user IDs, passwords, and roles.

Storage Management Initiative Specification (SMI-S)
A design specification developed by the Storage Networking Industry Association (SNIA) that specifies a secure and reliable interface with which storage management systems (SMSs) can identify, classify, monitor, and control physical and logical resources in a storage area network (SAN). The interface integrates the various devices to be managed in a SAN and the tools used to manage them.

Storage Networking Industry Association (SNIA)
An alliance of computer vendors and universities that focus on developing and promoting industry standards for storage networks.

streaming lossless data compression (SLDC)
A form of lossless compression that compresses the data stream realtime as it is written/sent or decompresses it realtime as it's read/received.

string
The individual combination of a controller drawer and one or more expansion drawers connected to that controller drawer. See also head of string.

subsystem
A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system.

subsystem identifier (SSID)
A user-assigned number that identifies a direct access storage device (DASD) subsystem. This number is set by the service representative at the time of installation and is included in the vital product data (VPD).

SUID
See system unique identifier.

SW
See short wave laser.

symmetric multiprocessing
A system in which all processors are identical, and any processor can execute both user code and kernel code.

Synchronous Data Link Control (SDLC)
A protocol for managing synchronous information transfer over a data link connection.

synchronous dynamic random access memory (SDRAM)
A type of dynamic random access memory (DRAM) with features that make it faster than standard DRAM.

system-managed storage complex (SMSplex)
A group of one or more systems that share a common storage management subsystem (SMS) configuration. All systems in an SMSplex share a common set of SMS control data sets: the active control data set (ACDS) and the communications data set (COMMDS).

System Management Interface Tool (SMIT)
An interface tool of the AIX operating system for installing, maintaining, configuring, and diagnosing tasks.

system management services (SMS)
An interface that provides information about a system or logical partition and that performs tasks such as changing the boot list and setting the network parameters. This interface is used for AIX or Linux logical partitions.

System Object Model (SOM)
Object-oriented programming technology for building, packaging, and manipulating binary class libraries.

system power control network (SPCN)
An asynchronous serial communications network. SPCN connects the power system in participating components to the operating system and can report critical changes and power failures in those components to the operating system. SPCN gives the operating system control of electrical power.

system reference code (SRC)
1. An alphanumeric string of characters (code) that contains information, such as a failing field-replaceable unit, for a service representative, customer engineer, or customer to use for servicing a system.
2. The characters that identify the name of the unit that detected the condition and the reference code that describes the condition.

system service tools (SST)
The part of the service function used to service the system while the operating system is running.

Systems Network Architecture distribution services (SNA distribution services, SNADS)
An IBM asynchronous distribution service that defines a set of rules to receive, route, and send electronic mail in a network of systems.

system unique identifier (SUID)
A 12-character ID that is assigned by the manufacturer.

T

tape controller
A logic card located in some tape units that controls input/output tape devices and synchronizes their operation with the operation of the system as a whole.

TB See terabyte.

TCP/IP
See Transmission Control Protocol/Internet Protocol.

tebibyte (TiB)
A base-2 unit of measurement that is equal to 1,099,511,627,776 bytes (2 to the 40th power).

terabyte (TB)
For processor storage, real and virtual storage, and channel volume, 2 to the 40th power or 1 099 511 627 776 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 bytes.

terminal type (tty)
A generic device driver for a text display. A tty typically performs input and output on a character-by-character basis.

TiB See tebibyte.

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

tty See terminal type.

U

UART See Universal Asynchronous Receiver/Transmitter.

unit reference code (URC)
A group of numbers displayed on the console or control panel that identifies failing parts, system or device states, or system or device status conditions.

Universal Asynchronous Receiver/Transmitter (UART)
An electronic circuit that transmits and receives data through a serial port.

Universally Unique Identifier (UUID)
The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier.

Universal Serial Bus (USB)
A serial-interface standard for telephony and multimedia connections to personal computers.

URC See unit reference code.

USB See Universal Serial Bus.

UTC See Coordinated Universal Time.

utility program
A computer program in general support of computer processes; for example, a diagnostic program, a trace program, a sort program.

UUID See Universally Unique Identifier.

V

V ac See volts alternating current.

V dc See volts direct current.

VDP See vital product data.

VIO See virtual input/output.

virtual
Pertaining to not physically existing as such but made by software to appear to do so. See also physical mount.

virtual input/output (VIO)
A set of storage, server, and network virtualization features that improve performance by binding input/output to a single connection.

virtual partition
A subset of a single server that contains resources (processors, memory, and input/output devices). A logical partition operates as an independent system. If hardware requirements are met, multiple logical partitions can exist within a system.

virtual service processor (VSP)
The firmware that controls the powering on and powering off of a logical partition, including loading the firmware that controls the I/O slots and initializing the memory space of the logical partition.

virtual tape drive
A tape drive for which the TS7740 Server emulates the function and operation of 3490 Enhanced Capacity (3490E) tape drives.

Virtual Tape Server (VTS)
An enterprise virtual tape system that combines high-speed disk access with low-cost tape storage by virtualizing data in a disk cache buffer. Storage management routines efficiently utilize tape cartridge capacity which reduces the number of required tape cartridges.

virtual terminal
A system object, created and controlled by an application program, that provides a functional representation or simulation of a physical display station.

virtual volume (VVOL)
A tape volume that resides in a tape volume cache of a virtual tape server (VTS). Whether the volume resides in the tape volume cache as a virtual volume or on a stacked volume as a logical volume (LVOL) is transparent to the host.

vital product data (VDP, VPD)
Information that uniquely defines system, hardware, software, and microcode elements of a processing system.

vNode
A distributed node in the TS7700 Virtualization Engine that presents the image of virtual drives to the host system.

VOLSER
See volume serial number.

volts ac
See volts alternating current.

volts alternating current (V ac, volts ac)
Unit of potential difference for alternating current.

volts dc
See volts direct current.

volts direct current (V dc, volts dc)
Unit of potential difference for direct current.

volume serial number (VOLSER)
An identification number in a volume label that is assigned when a volume is prepared for use on the system.

VPD See vital product data.

VSP See virtual service processor.

VTS See Virtual Tape Server.

VVOL See virtual volume.

W

WAN See wide area network.

WBEM
See Web Based Enterprise Management.

Web Based Enterprise Management (WBEM)
A set of Distributed Management Task Force (DMTF) standards that defines the protocols used to communicate with a particular Common Information Model (CIM) implementation that uses CIM servers.

wide area network (WAN)
A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN). See also local area network.

worldwide ID (WWID)
A name identifier that is unique worldwide and that is represented by a 64-bit value that includes the IEEE-assigned organizationally unique identifier (OUI).

worldwide node name (WWNN)
A unique 64-bit identifier for a host containing a Fibre Channel port. See also worldwide port name.

worldwide port name (WWPN)
A unique 64-bit identifier associated with a Fibre Channel adapter port. The WWPN is assigned in an implementation-independent and protocol-independent manner. See also worldwide node name.

WORM
See Write Once Read Many.

WOT See write-ownership takeover.

write-mount count
A 16-bit sister value of WWID (World Wide Identifier) that represents the total number of times an LWORM volume is mounted and modified due to a write operation. This value is seeded to zero for a newly bound LWORM volume prior to the first write from BOT (beginning of tape).

Write Once Read Many (WORM)
Pertaining to a form of optical storage that permits data to be recorded once, read an unlimited number of times, but not erased.

write-ownership takeover (WOT)
A permission that when enabled allows volume ownership to be taken from a failed TS7700 Cluster. Full access is allowed through the remaining available TS7700 Clusters in the grid.

WWID
See worldwide ID.

WWNN
See worldwide node name.

WWPN
See worldwide port name.

Index

D

E

F

G

P

R

S

T

U

V

W

Z

Printed in USA

GA32-0567-25