

IBM TS7700/TS7770 Tape Attach
8.522

Introduction and Planning Guide



Note

Before using this information and the product it supports, read the information in [“Safety and Environmental notices ”](#) on page xix and [“Notices”](#) on page xvii.

This edition applies to Version 5, release 22 of the *IBM TS7700 Introduction and Planning Guide* and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces GA32-0567-32.

© **Copyright International Business Machines Corporation 2021.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures.....	vii
Tables.....	xi
Feedback.....	xv
How to send your comments.....	xv
Notices.....	xvii
Safety and Environmental notices	xix
Safety notices.....	xix
Environmental notices.....	xx
About this publication	xxi
Organization of this book.....	xxi
Who Should Read This Book.....	xxii
What's New in This Edition.....	xxii
Related Publications.....	xxii
Online References.....	xxiii
Overview.....	1
Concepts of storage virtualization.....	1
Virtual device operation.....	1
Virtual volume tape format.....	2
Access and location of virtual volume data.....	3
Accessing virtual volumes through virtual device addresses.....	3
Virtual volume copy availability.....	4
TS7700 product introduction.....	4
TS7700 system configurations.....	12
TS7700 system components.....	13
Tape frame.....	16
TS7700 Server.....	16
TS7770 with 3956-CFC Cache Controller.....	21
TS7770 with 3956-XFC Cache Expansion Enclosure.....	21
TS7770 with 3956-CSB Cache Controller.....	22
TS7770 with 3956-XSB Cache Expansion Enclosure.....	23
Data storage values.....	26
Planning.....	27
Storage Acclimation.....	27
TS7700 system component details.....	27
3952 Tape Frame details.....	27
IBM TS7770 details R5.2.....	28
IBM TS7770 details.....	31
IBM TS7760 details.....	35
Tape library attachments, drives, and media.....	43
Workload considerations.....	52
System requirements.....	54
TS7770 specifications and requirements R5.2.....	54

3952 Tape Frame specifications.....	59
TS7770 specifications and requirements.....	60
TS7760 specifications and requirements.....	67
Cooling requirements.....	72
Floor requirements.....	72
Clearance requirements.....	73
Environmental requirements.....	75
Acoustic requirements.....	77
Host compatibility.....	78
Supported hosts.....	78
Host configurations.....	82
Infrastructure requirements.....	83
TS7700 Grid interconnect LAN/WAN requirements.....	83
Network adapter assignments.....	85
Network switches and TCP/IP ports requirements.....	87
Planning for virtual and physical volumes.....	88
Volume serial numbering.....	89
Virtual volume planning.....	89
Physical.....	91
Migrating data to a new media type.....	93
Merging clusters or grids.....	94
Merging clusters.....	94
Merging grids.....	95
TS7700 upgrade options.....	96
Concurrent TS7700 upgrade options.....	96
Non-concurrent TS7700 upgrade options.....	97
Adding TS7700 Clusters to a grid.....	99
Upgrades for the TS7770.....	101
Upgrades for the TS7760.....	102
Upgrades for the TS7700 Tape Attach.....	103
TS7700 feature codes.....	115
Feature details.....	115
Capacity on Demand.....	160
Checklists.....	161
Planning for new system arrival (customer tasks).....	161
Post-installation tasks.....	195
Configuring.....	201
TS7700 configurations.....	201
TS7700 Cluster.....	201
TS7700 Grid.....	202
TS7700C (Cloud).....	209
Cloud export recovery.....	214
Removing a cluster from a grid and cluster cleanup.....	215
Data access and availability.....	215
Direct host attachment to TS7700.....	216
Virtual volume data.....	216
Physical volume data.....	233
Allocation assistance.....	233
Selective device access control.....	235
Circumstances of a job failure.....	236
Configuring for disaster recovery.....	237
Cloud export for disaster recovery.....	237
Flash Copy for disaster recovery.....	238
Selective write protect for disaster recovery.....	239
Configuring for high availability.....	240
Configuring for both disaster recovery and high availability.....	240

CUIR automation.....	241
Security.....	243
LDAP and role-based access control.....	243
Configuring for service personnel access when LDAP is enabled.....	243
Native LDAP using MSAD.....	245
Native LDAP with z/OS RACF.....	245
System Storage Productivity Center and Spectrum Control	247
Audit logging.....	248
SNMP MIB definitions.....	250
Remote support security.....	261
Overview.....	261
Managing remote support.....	264
Managing.....	281
Connecting to the management interface.....	281
Downloading comma-separated value files.....	282
Preserving leading zeros in downloaded data.....	282
Shutting down the TS7700.....	283
Regenerating keys support (rekeying).....	283
Recovering.....	285
Recovering lost data.....	285
Recovering data from a physical volume.....	286
Recovering data from a virtual volume.....	287
Testing grid failover.....	287
Reference.....	289
Management interface messages.....	289
Perform Library Function codes.....	289
Error Recovery Action codes.....	289
Completion codes.....	314
Immediate copy failure reason codes.....	319
Operator information messages.....	322
Other host messages.....	364
Service information messages.....	366
Read Diagnostic Parameter (RDP).....	373
INTERFACE ID value from DISPLAY M=DEV command.....	381
Notices.....	383
Trademarks.....	384
Homologation.....	385
Safety and environmental notices.....	385
Glossary.....	393
A.....	393
B.....	395
C.....	396
D.....	398
E.....	400
F.....	402
G.....	403
H.....	404
I.....	406
J.....	407
K.....	408
L.....	408
M.....	410

N.....	412
O.....	413
P.....	413
R.....	415
S.....	417
T.....	421
U.....	422
V.....	422
W.....	423
Reference.....	425
Index.....	427

Figures

1. vNode, hNode, and gNode construction.....	14
2. TS7700 Cluster configuration.....	14
3. TS7700 six-cluster grid configuration.....	15
4. TS7770 Server (3957-VED) System Unit (rear view).....	17
5. New adapter cards in TS7770 v5.0.....	17
6. TS7770 Server (3957-VED) System Unit (front view).....	18
7. TS7770 Server (3957-VED) Expansion Unit I/O drawer (rear view).....	18
8. TS7770 Server (3957-VED) Expansion Unit I/O Drawer (FICON Connections).....	18
9. TS7760 Server (3957-VEC) System Unit (front view).....	19
10. TS7760 Server (3957-VEC) System Unit (rear view).....	19
11. TS7760 Server Expansion Unit I/O drawer (rear view).....	20
12. 3956-CFC.....	21
13. 3956-XFC.....	22
14. Base frame of TS7700 with 3956-CFC/XFC.....	29
15. TS7770 Cache Controller 3956-CFC (front view).....	30
16. TS7770 Cache Controller 3956-CFC (rear view).....	30
17. TS7770 Cache Drawer 3956-XFC (front view).....	30
18. TS7770 Cache Drawer 3956-XFC (rear view).....	30
19. Front and rear view frame layout of the TS7770 base frame.....	31
20. TS7770 Cache Controller 3956-CSB (front view).....	32
21. TS7770 Cache Controller 3956-CSB (rear view).....	32
22. TS7770 Cache Controller 3956-XSB (rear view).....	32
23. TS7770 First Expansion Frame cache layout. (String 2).....	34

24. TS7770 Cache Drawer 3956-XSB (front view).....	34
25. TS7770 Cache Drawer 3956-XSB (rear view).....	35
26. TS7770 Cache Controller 3956-CSB (rear view).....	35
27. Single frame layout of a TS7760 with a manufacturing installed 3957-VEC, 3956-CSA, and 3956-XSA.....	36
28. Layout of a TS7760 Storage Expansion Frame with 3956-CSA and 3956-XSA.....	37
29. TS7760 Cache Controller 3956-CSA (front view)	42
30. TS7760 Cache Controller 3956-CSA (rear view).....	42
31. TS7760 Cache Drawer 3956-XSA (front view)	43
32. TS7760 Cache Drawer 3956-XSA (rear view).....	43
33. 3592 Tape Drive.....	45
34. IBM 3592 Tape Cartridge.....	49
35. Bottom view of F06 frame dimensions when in position.....	74
36. 3952-F07 frame dimensions when in position.....	75
37. IBM Z® host attachment to TS7700 (at speed of 8 Gb/second).....	80
38. TS7700 I/O drawer FICON Cable Connections.....	81
39. Currently active feature licenses.....	104
40. Three possible locations for encryption policy engine and key management.	106
41. An encryption key server uses both symmetric and asymmetric encryption keys.....	108
42. Example of a TS7760 and TS7770 8-way hybrid Grid configuration.....	204
43. Example of a TS7760 hybrid configuration.....	205
44. TS7700 3957-VEC stand-alone with 2 or 4 Ethernet connections.....	213
45. Order of copy queue prioritization.....	221
46. Autonomic Ownership Takeover Manager configuration for four clusters.....	227
47. Autonomic Ownership Takeover Manager configuration for four clusters in a hybrid grid.....	227
48. Autonomic Ownership Takeover Manager configuration in a three-cluster Grid.....	228

49. TSSC Connection Diagram	263
50. Menu to enable and disable host notification	322
51. Host notification state by cluster dialog box.....	323
52. Description of Service Information Message Format.....	371
53. FIRST.....	374
54. LAST.....	374
55. REFRESH.....	375
56. COMPARE.....	376
57. Before error.....	377
58. Error occurrence.....	377
59. After error.....	377
60. Comparison of stats from 12/16 to 12/26 to search for invalid CRC and FEC uncorrected value changes.....	377
61. FEC uncorrected value.....	379
62. dBm errors.....	380
63. I/O enclosure cables, rear (FICON).....	382

Tables

1. TS7770 system configurations.....	12
2. TS7760 system configurations.....	13
3. System Unit (3957-VED) adapters.....	17
4. FICON connection order for both 2 and 4 card configurations(3957-VED) adapters.....	18
5. TS7760 Server System Unit (3957-VEC) adapters.....	19
6. TS7700 Server Expansion Unit I/O drawer adapters for 3957-VEC.....	20
7. Base Cache configurations and capacities with 4 TB drives. Table describes the configurations and capacities of the base Cache.....	24
8. Base Cache configurations and capacities with 8 TB drives. Table describes the configurations and capacities of the base Cache.....	25
9. Comparison of binary and decimal units and values.....	26
10. Percentage difference between binary and decimal units.....	26
11. TS7760 Storage Expansion Frame configurations for 4 TB capacity drives.....	39
12. TS7760 Storage Expansion Frame configurations for 8 TB capacity drives.....	41
13. Comparison of 3592 Tape Drives supported by the TS7770 Tape Attach or TS7760 Tape Attach.....	45
14. Supported IBM 3592 Tape Cartridges.....	49
15. Encryption-capable TS7770 physical frame F07 characteristics (FC 7339)	54
16. TS7770 maximum configuration	55
17. TS7770 component specifications.....	56
18. 3957-VED Temperature Depending on Altitude.....	57
19. TS7770 Base Frame maximum input power requirements.....	57
20. TS7770 maximum configuration frame with all components.....	58
21. Encryption- capable TS7770 physical frame F06 characteristics (FC 7335 and FC 7336).....	60
22. Encryption- capable TS7770 physical frame F07 characteristics (FC 7337 and FC 7338 and FC 7339).....	61

23. TS7770 maximum configuration	63
24. TS7770 component specifications.....	63
25. 3957-VED Temperature Depending on Altitude.....	64
26. TS7770 Base Frame maximum input power requirements.....	65
27. TS7770 maximum configuration frame with all components.....	65
28. TS7770 Storage Expansion Frame maximum input power requirements.....	65
29. Encryption-capable TS7760 Base Frame specifications.....	67
30. Encryption-capable TS7760 Storage Expansion Frame specifications.....	68
31. TS7760 maximum configuration	68
32. TS7760 component specifications.....	68
33. 3957-VEC, Temperature Depending on Altitude.....	70
34. TS7760 Base Frame maximum input power requirements.....	70
35. TS7760 Storage Expansion Frame maximum input power requirements.....	70
36. Required clearances when moving the 3952 F06 or F07 frame.....	73
37. Required clearances when the F06 frame is in position.....	74
38. Temperature, altitude, and humidity specifications.....	75
39. Air quality specifications.....	76
40. TS7700 FICON Cable Connections.....	81
41. Subsystem identification definitions.....	82
42. Grid WAN TCP/IP port assignments.....	87
43. Join rules.....	99
44. Supported join and merge scenarios.....	99
45. TS7700 features.....	133
46. Cluster Description Table and Notes.....	163
47. TS3500 or TS4500 Tape Library Configuration Information Table and Notes.....	166

48. TS3500 or TS4500 Tape Library Drive Information Table and Notes.....	170
49. TS3500 Limited Drive Support Table.....	173
50. Media Volume Serial (VOLSER) Range Table and Notes.....	174
51. Encryption Key Information Table.....	174
52. TS4500 Limited Drive Support Table.....	174
53. Code Activation/VPD Information Table and Notes.....	175
54. TS7700 Customer Network Configuration Information Table and Notes.....	179
55. TSSC Configuration Information Table and Notes.....	182
56. TSSC AOS version 3.3 and earlier.....	183
57. TSSC AOS version 4.0.....	183
58. URL table for Legacy ECC.....	184
59. URL table for Edge ECC.....	184
60. URL table for Fix Download.....	184
61. Grid Local Address Table and Notes.....	186
62. Summary Table.....	189
63. TSSC Grid Configuration Information Table and Notes.....	194
64. Hybrid grid configurations.....	206
65. IP information for the TS7700 cluster and the cloud.....	209
66. TS7700 4.2 GA support for joins and merges.....	211
67. WWID and write-mount count scenarios.....	217
68. Effects of Retain Copy Mode in mount scenarios.....	219
69. Active cache capacity state thresholds.....	223
70. Conditions under which AOTM takes over a failed cluster.....	228
71. Conditions under which AOTM does not takeover a failed cluster.....	229
72. Expected results when one or both "S" locations are unavailable at mount time.....	232

73. SNMP MIB definitions.....	250
74. TSSC External Port Information.....	262
75. TSSC Components.....	263
76. Supported browsers.....	264
77. Remote support center server information.....	278
78. Selections available from the Network Information page.....	278
79. Supported browsers.....	281
80. ERA codes.....	290
81. Completion codes.....	314
82. Immediate copy failure reason codes, unexpected reasons.....	320
83. Immediate copy failure reason codes, expected reasons.....	320
84. Message severity.....	324
85. Intervention message texts.....	325
86. Other host messages.....	365
87. Service information message (SIM) Sense Bytes	366
88. Description of fibre connection (FICON) media information message format.....	371
89. Description of Media Information Message Format.....	373
90. INTERFACE ID value.....	381
91. I/O enclosure cables, rear (FICON).....	382

Feedback

How to send your comments

To submit any comments about this publication or any other IBM product documentation, send your comments by email to ibmkc@us.ibm.com. Be sure to include the following information:

- Exact publication title and version
- Publication form number (for example, GA32-1234-00)
- Page, table, or illustration numbers that you are commenting on
- A detailed description of any information that should be changed

Notices

The information provided by this media supports the products and services described with consideration for the conditions described herein.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries to:

*IBM Corporation
Almaden Research
Bldg 80, D3-304, Department 277
650 Harry Road
San Jose, CA 95120-6099
U.S.A.*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

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.
	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.
	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
 - 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 393](#) provides definitions for terms, abbreviations, and acronyms used in this book.
- The [“Reference” on page 289](#) 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

Feature	Related Topic
Introduction of the TS7770	“TS7700 product introduction” on page 4
Introduction of the TS7770 3957-VED Server	“TS7700 product introduction” on page 4
Introduction of the TS7770 Cache Controller 3956-CSB and Cache Enclosure 3956-XSB	• The TS7770 Cache Controller (3956-CSB) contains twelve 10 TB NL-SAS 7.2k RPM drives. • The CSB and corresponding XSB enclosure supports encryption, including cryptographic erase, internal key management, external key management, and retro-active enablement. • The CSB cache controller and supported XSB expansion enclosure support the ability of Distributed RAID (DRAID). The enclosure will consist of 12 drives in a MDisk with 2 two rebuild areas (equivalent to the capacity of two DDMS) • The TS7770 Cache (3956-CSB/XSB) expansion frame can be attached to add more cache to the TS7770 base frame. • Encryption: – Disk Enabled Encryption (Installed in Manufacturing only) – Disk Encrypt-External Key Manager (Only IBM Security Key Lifecycle Manager (SKLM)) Note: Encryption cannot be retroactively enabled, the Cache enclosure will need to be shipped from MFG with Disk Enabled Encryption.
Introduction of the TS7770 V5000 Management GUI	The TS7770 V5000 Management GUI provides service with a guided procedure in repairing the TS7770 cache enclosures.
Introduction of the TS7770	The TS7770 will have a dedicated TSSC.
DS8000 Object Store (FC 5282)	This feature allows the TS7700 to store Objects from DS8000. Refer to “FC 5282, DS8000 Object Store” on page 122 for more details.
Secure Data Transfer (FC 5281)	This feature enables Grid Encryption. Refer to “FC 5281, Secure Data Transfer” on page 122 for more details.

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
 - <https://www.ibm.com/docs/en/ts7700-virtual-tape>
- 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>

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

Notes:

- 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.

- 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 88](#)

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 201](#)

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.

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 or 25000 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

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 8.52.100.x can be installed only on a TS7770 Server model 3957-VED and TS7760 Server model 3957-VEC.

Note: It is recommended to regularly update a system to recommended and/or latest code. See recommendation: <https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010472>

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:

TS7770 with 3956-CFC/XFC

A TS7770 virtual tape system, model 3957-VED with 3956-CFC and 3956-XFC enclosures can support up to 133 TB of usable encryption capable disk cache. Each type of enclosure uses 24 - 3.84 TB SSD drives in a Distributed RAID (DRAID) configuration. A minimum configuration base TS7770 with a 3956-CFC can contain up to 63 TB of usable encryption capable disk cache.

The TS7770

A virtual tape system, model 3957-VED, that can support up to 2.3 PB of usable encryption capable disk cache. The 3956-CSB/XSB uses twelve 10 TB SAS disks in a DRAID (Distributed RAID) configuration; a base TS7770 can contain up to .76 PB of usable encryption capable disk cache. Up to two more 3956-CSB/XSB expansion frames can be added to a base TS7770 which providing up to a total 2.3 PB of usable encryption capable disk cache.

A second expansion frame delivers up to 3.94 PB of capacity with two fully populated expansion frames.

The TS7770 supports the optional attachment of a TS3500 or TS4500 physical tape library. When the tape attach feature is present, the TS7770 can be referred to as a TS7770T or TS7770 Tape Attach. When tape is attached, up to 100 PB of usable storage is available per TS7770T.

Note: The VED tape-attach supports only the new 16 Gb fiber switch.

TS7770 Tier to Cloud supports both the largest and smallest TS7700 users to deploy TS7700 in new use cases, such as; archival of massive data stores, and supporting DR without a grid presence (TS7770 stand-alone) or TS7770 in a GRID. TS7770 Tier to Cloud supports Amazon S3 and IBM COS S3.

Note: The VED tape-attach is not supported with a Tier to Cloud enabled cluster.

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.

TS7760 Tier to Cloud supports both the largest and smallest TS7700 users to deploy TS7700 in new use cases, such as; archival of massive data stores, and supporting DR without a grid presence (TS7760 stand-alone) or TS7760 in a GRID. TS7760 Tier to Cloud supports Amazon S3 and IBM COS S3.

Note: The VEC tape-attach is not supported with a Tier to Cloud enabled cluster.

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 SW FICON Adapter” on page 118](#) and [“FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118](#).

8 Gb FICON host attachments (not supported on TS7770)

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.

The 3957-VEC server supports [“FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 118](#) and [“FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 118](#).

16 Gb Fibre Channel HBA

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.

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.

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 8.52.100.xx or later), the TS7700 supports two 10 Gb Grid links. When FC 1034, Enable dual port grid connection is installed, the TS7700 supports four 10 Gb Grid links.

Tape library attachment

- For TS7700 Tape Attach, use Installation Instructions FC 5273/5274 (Enable TS7700 Tape Attach) to enable the feature codes and configure the TS7700.
- Attachment to an IBM TS3500 Tape Library (also referred to as the 3584 Tape Library or machine type 3584) is supported for the TS7700 Tape Attach.

For the TS7700 Tape Attach, this configuration is enabled by installing [“FC 5273, TS7770 Tape Attach” on page 121](#) and at least one instance of [“FC 5274, Enable 1 TB Pending Tape Capacity” on page 121](#). 16 Gb Fibre Channel switches are supported in the TS3500 for TS7760/TS7770 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 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 TS7760/TS7770 attachment, and in the TS3500 for TS7760/TS7770 attachment.

For the TS7760/TS7770 Tape Attach, this configuration is enabled by installing [“FC 5273, TS7770 Tape Attach”](#) on page 121 and at least one instance of [“FC 5274, Enable 1 TB Pending Tape Capacity”](#) on page 121. In addition, [“FC 4880, TS7700 BE 16 Gb Fibre Channel Switch”](#) on page 120 is required.

Tier to cloud

For the TS7700 Tier to Cloud, this configuration is enabled by installing FC 5278, Enable Cloud Storage Tier, and at least one instance of FC 5274, 1 TB Active Pre-Migration Queue. The customer network needs to allow connectivity between the TS7700 GRID network and the IBM COS endpoints or AMAZON region endpoints.

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. TS1130 Tape Drives cannot be intermixed with TS1120 or 3592-J1A Tape Drives.

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 Tape”](#) on page 130.

Support for encryption of disk drive modules (DDMs) within a TS7700 cache subsystem. Requires [“FC 5272, Disk Enabled Encryption”](#) on page 121.

External key management for the cache is also supported. Requires [“FC 5276, Disk encrypt - External key manager”](#) on page 122.

Encryption Support for 3956 CFC or 3956-CSB

Unlike the previous 3956-CSA controller, encryption (FC 5272/5276) CANNOT be retroactively enabled after the TS7770 has been installed. Therefore, CSB/XSB drawers MUST be encryption enabled when shipped from manufacturing.

- Cache controller models CSB and their cache module models XSB are encryption-capable devices.
- All disk units in the entire TS7770 cluster must be encryption capable for encryption to be enabled.
- Disk cache encryption may be selected and enabled to deliver protection for data as it resides in the TS7770 disk repository.
- The 3956 CFC or 3956-CSB Cache Controller maintains the encryption keys when feature 5272 Disk Enabled Encryption is selected.
- Options enable the user to choose encryption using externally managed keys, or using local or internally managed keys.
 - Feature #5272 Disk Enabled Encryption is not available for field Install on the TS7770 and needs to be shipped from manufacturing for any Encryption.
 - Feature #7405 must be ordered on every 3956 CFC or 3956-CSB in the TS7770 configuration. Feature #7405 will provide four USBs sticks per 3956 CFC or 3956-CSB used to store the local encryption keys.

If external key management is later enabled, these USB sticks are no longer needed.

- Feature #5276 and #5272 must be initially plant-installed on the TS7700 server to enable TS7770 disk-based encryption using externally managed keys

Note:

1. All TS7700 configurations with any encryption type enabled will ALWAYS ship with local key management enabled first.
 2. Once a TS7770 with feature #5272 is configured in a customer environment and able to communicate with an external key server, then feature #5276 can be activated to transition to external key management.
- For feature 5276 Disk Encrypt-External Key Manager, encryption keys are maintained outside of the TS7700 and passed to the TS7700 from an encryption key manager. Only IBM Security Key Lifecycle Manager (SKLM) will be supported.
 - For the TS7770 to successfully communicate with the SKLM servers, an X.509 encryption certificate is required. Every TS7770 system shipped with R5.0 will contain a Public Key Cryptography Standards (PKCS) file using format #12, even if encryption is not enabled on the TS7770. Feature #9277, PKCS #12 File - Plant, will be included on each of these systems to indicate the certificate file is installed.
 - Disk encryption using externally managed keys with SKLM requires software entitlements . For more information about SKLM, see the [IBM Security Key Lifecycle Manager website](#).

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 7-way or more TS7700 Grid configurations

Support for a grid that consists of 7 or more TS7700 Clusters.

Note: 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 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 TS7700 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

- Capacity on Demand allows customers to enable disk capacity in 20 TB and 100 TB increments concurrently.

- A maximum of 4x #5262 20TB Cache Enablement Features may be selected for any one single order, either Initial order or MES
- More than 4x #5262 20TB Cache Enablement Features may exist on the machine .
- If 5x 5262 20TB Cache Enablement Features are desired in one single order, 1x 5263 - 100TB Cache Enablement Feature will be enabled (enforced via e-Config).
- At least 1 TB of licensed capacity must be enabled on the next set of drawer pairs (through features #5262 and #5263) before the next drawer pair may be installed. Adding physical drawer pairs without at least 1 TB of licensed capacity enabled is not supported.
- Features #5262 and #5263 should be ordered on 3957-VED model.
- At least one feature #5262 20 TB or #5263 100 TB cache enablement increment minimum must be plant installed.

For more details, please see: <https://www.ibm.com/docs/en/ts7700-virtual-tape/5.0?topic=codes-capacity-demand>.

The TS7770 Cache Controller Model CSB and TS7770 Cache Module Model XSB

- up to 780 TB* usable capacity in a base frame only configuration (1 CSB + 9 XSBs).
- up to 2.36 PB usable capacity in a base frame with one expansion frame fully populated with 20 drawers (2 CSBs + 18 XSBs)
- up to 3.94 PB usable capacity in a base frame with two expansion frames fully populated with 20 drawers (2 CSBs + 18 XSBs)

Release 5 delivers 10 TB 7.2K SAS disk drives with 157 TB usable capacity per drawer pair. Using the ENERGY STAR-compliant IBM Storwize V5030E model, the TS7770 cache enclosures must be installed in pairs, two drawers at a time. Additional pairs of XSB drawers now support concurrent expansion, which is unique to the TS7770 model.

- Host data transfer performance (increments of 100 MB/sec up to 4000 MB/sec) for the TS7700 “FC 5268, 100 MB/sec Increment” on page 121 enables a 100-MB/sec increment of peak data throughput. One instance of “FC 9268, Plant installation of 100 MB/s throughput” on page 128 is shipped standard and a maximum of 39 instances of “FC 5268, 100 MB/sec Increment” on page 121 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.
- 1 TB Active Premigration Queue (FC 5274) designates that up to 1 TB of data across all tape-managed and cloud-managed partitions may be waiting to be written to a physical tape cartridge or cloud storage. One instance of FC 5274 is required on a TS7700C or TS7700T. Up to 10 instances of FC 5274 may be installed. 5 TB Active Premigration Queue (#5279) designates that up to 5 TB of additional data across all tape-managed and cloud-managed partitions may be waiting to be written to a physical tape cartridge or to cloud storage. All 10 instances of FC 5274 are required before the first instance of FC 5279 may be installed. Up to 10 instances of FC 5279 may be installed. Once all 10 instances of FC 5274 and 10 instances of FC 5279 are installed, the size of the premigration queues is unconstrained by these feature codes and is limited only by the size of the disk repository.

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 121](#), 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.

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

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
- Assist on Site (AOS) enhancements

Important: Ask your IBM service representative to receive the most current level of TS7700 microcode. With Remote Code Load (RCL) service, the microcode will not come from an IBM service representative. It needs to be installed by the RCL team.

TS7700 system configurations

A TS7700 system is configured in one of following configurations:

TS7770 series: (see [Table 1 on page 12](#) that displays the available system configurations of the TS7770.)

- TS7770
- TS7770 Tape Attach
- TS7770 Cloud Attach

TS7760 series: (see [Table 2 on page 13](#) that displays the available system configurations of the TS7760.)

- TS7760
- TS7760 Tape-Attach
- TS7760 Cloud Attach

Table 1. TS7770 system configurations	
TS7770	
TS7770 TS7770 Server (3957-VED) TS7770 Cache Controller (3956-CFC) TS7770 Cache enclosure (3956-XFC) TS7770 Cache Controller (3956-CSB) TS7770 Cache enclosure (3956-XSB) Optional cache attachment: Up to two 3952 F0x Storage Expansion Frames each with one or two 3956-CSB cache controllers.	TS7770 Tape Attach TS7770 Server (3957-VED) TS7770 Cache Controller (3956-CFC) TS7770 Cache enclosure (3956-XFC) TS7770 Cache Controller (3956-CSB) TS7770 Cache enclosure (3956-XSB) TS7770 Tape Attach (Feature Code 5273) 3952 tape frame optional cache attachment: Up to two 3952 F0 Storage Expansion Frames with two 3956-CSB cache controllers. TS3500 tape library or TS4500 tape library Tape Drives • TS1150 tape drive • TS1140 tape drive Tape cartridges 3592 tape cartridge

Table 1. TS7770 system configurations (continued)	
TS7770	
TS7770 Cloud Attach TS7770 Server (3957-VED) TS7770 Cache Controller (3956-CFC) TS7770 Cache enclosure (3956-XFC) TS7770 Cache Controller (3956-CSB) TS7770 Cache enclosure (3956-XSB) TS7770 Cloud Attach (Feature Code 5278) Optional cache attachment: Up to two 3952 F0x Storage Expansion Frames each with one or two 3956-CSB cache controllers.	Cloud supports Amazon S3 and IBM COS S3

Table 2. TS7760 system configurations	
TS7760	
TS7760 TS7760 Server (3957-VEC) TS7760 Cache Controller (3956-CSA) TS7760 Cache Drawer (3956-XSA) Optional cache attachment: Up to two 3952 F0x Storage Expansion Frames each with one 3956-CSA cache controller	TS7760 Tape Attach TS7760 Server (3957-VEC) TS7760 Cache Controller (3956-CSA) TS7760 Cache Drawer (3956-XSA) TS7760 Tape Attach (Feature Code 5273) 3952 tape frame Optional cache attachment: Up to two 3952 F0x Storage Expansion Frames each with one 3956-CSA cache controller TS3500 tape library or TS4500 tape library Tape Drives • TS1150 tape drive • TS1140 tape drive Tape cartridges 3592 tape cartridge
TS7760 Cloud Attach TS7760 Server (3957-VEC) TS7760 Cache Controller (3956-CSA) TS7760 Cache Drawer (3956-XSA) TS7760 Cloud Attach (Feature Code 5278) Optional cache attachment: Up to two 3952 F0x Storage Expansion Frames each with one 3956-CSA cache controller	Cloud supports Amazon S3 and IBM COS S3

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 on page 14](#) for an illustration of the relationship between nodes.

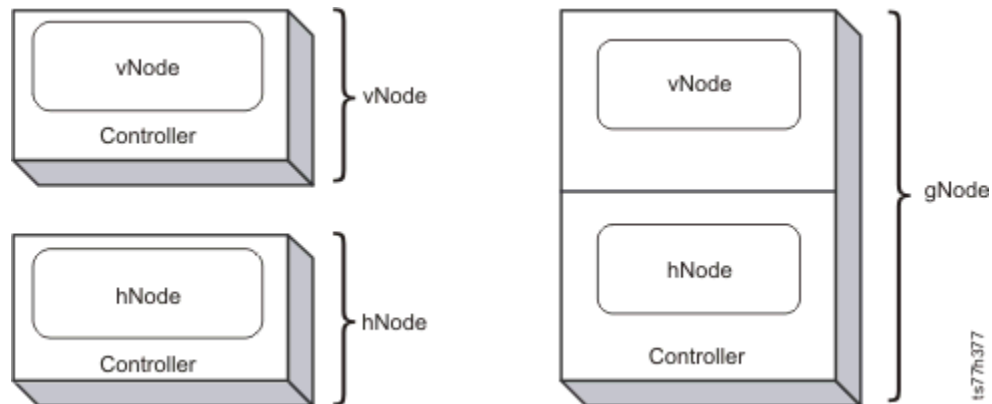


Figure 1. vNode, hNode, and gNode construction

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 on page 14](#) displays a TS7700 configured as a cluster.

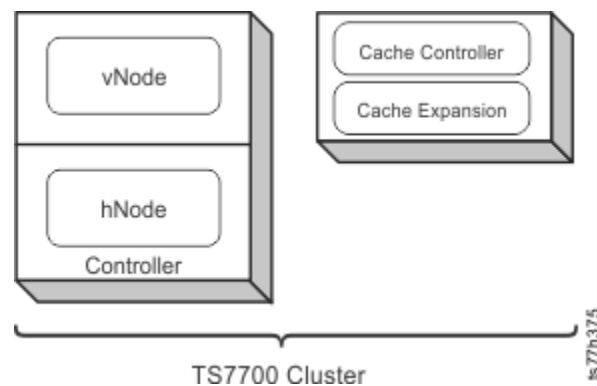


Figure 2. TS7700 Cluster configuration

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. For more information about data accessibility in the event of a source cluster failure, see [“The Autonomic Ownership Takeover Manager” on page 226](#).

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 on page 15 shows a typical six-cluster grid.

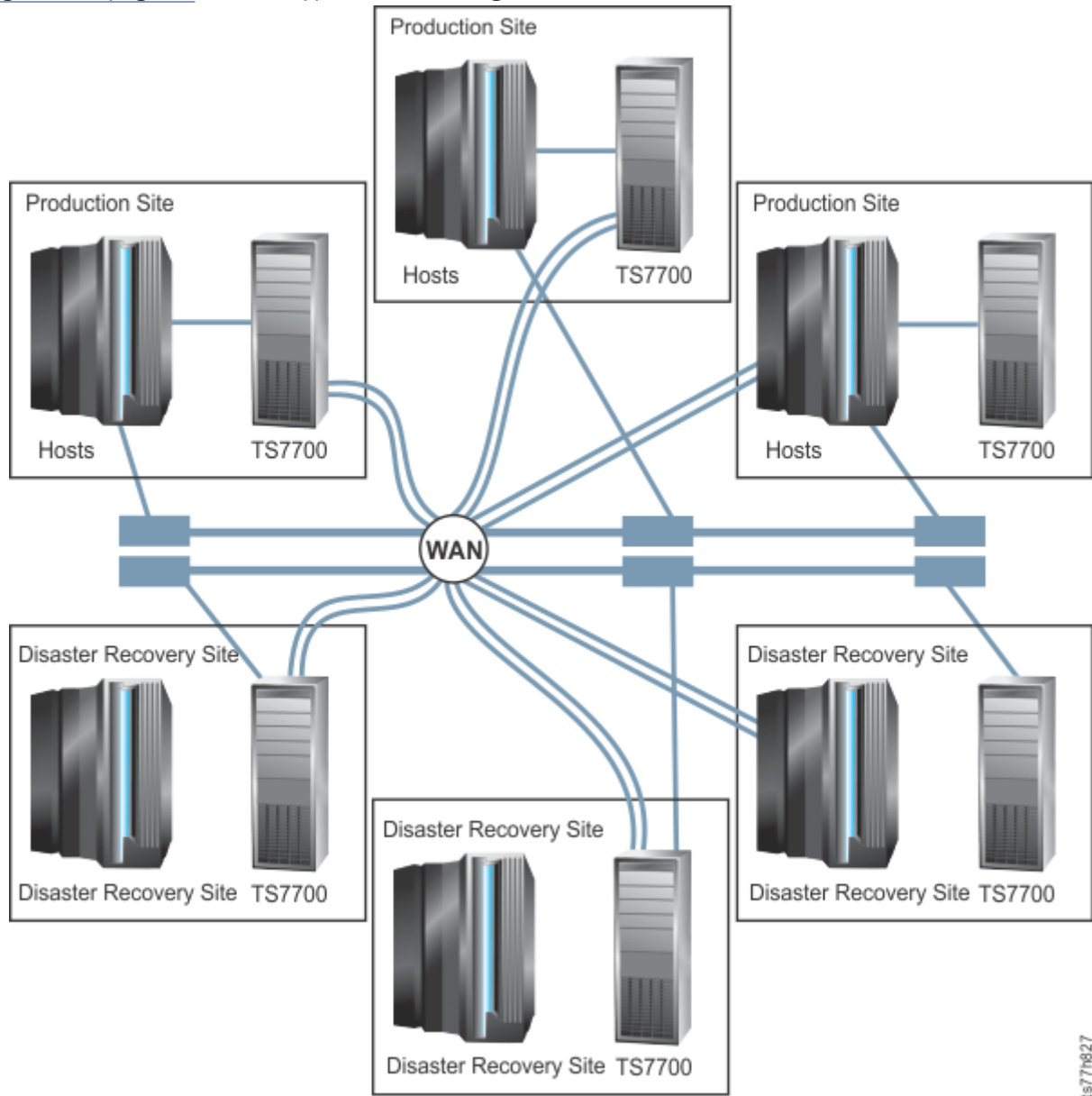


Figure 3. TS7700 six-cluster grid configuration

†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 TS7770 or a TS7760.

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 F06 or F07 can house either a TS7760 or a TS7770.

Additionally, a 3952 Tape Frame can be designated as a TS7760 or TS7770 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 12](#)

[“TS7700 system component details” on page 27](#)

[“TS7700 Grid” on page 202](#)

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-VED configuration

A TS7700 Server (3957-VED) configuration includes:

- Two 10-core 3.8 GHz POWER9 processor cards
- Six 600GB HDDs or 775GB SSD
- 64 GB total memory
- SAS controller with support for RAID 0,1,5,6 and 10
- 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.
- Four USB ports:
 - Two USB 3.0 ports for general use
 - Two USB 2.0 ports for the FSP service processor
- No DVD RAM drive
- Two or four Quad-port 1 Gbps copper ethernet adapter
- Two quad-port 16Gbps FCS adapter

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

- Eight additional hot-plugged PCIe cartridge styler slots (used to house FICON adapters for host attachment, Fibre Channel adapters for the cache enclosure attachment and Fibre Channel adapters).
 - 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
 - Four fans

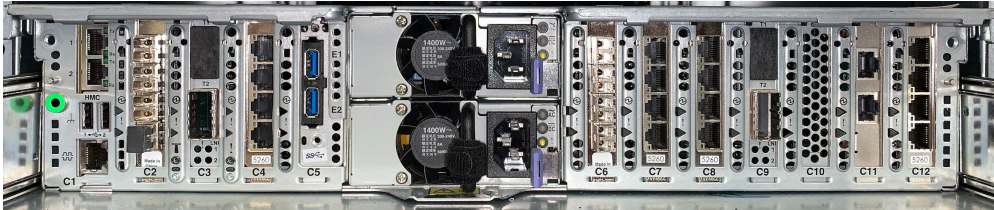


Figure 4. TS7770 Server (3957-VED) System Unit (rear view)

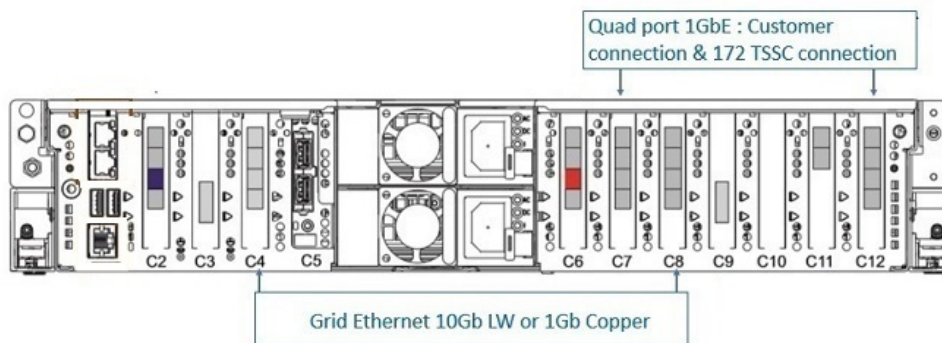


Figure 5. New adapter cards in TS7770 v5.0

Slot Number	Adapter
C2	16 Gb Quad port FC HBA
C3	I/O Drawer Interface card
C4	1Gb Quad port or 10Gb dual port Optical
C6	16 Gb Quad port FC HBA
C7	16Gb Quad port Ethernet adapter
C8	1Gb Quad port or 10Gb dual port Optical
C9	I/O Drawer Interface card
C11	Serial adapter
C12	16Gb Quad port Ethernet adapter



Figure 6. TS7770 Server (3957-VED) System Unit (front view)



Figure 7. TS7770 Server (3957-VED) Expansion Unit I/O drawer (rear view)

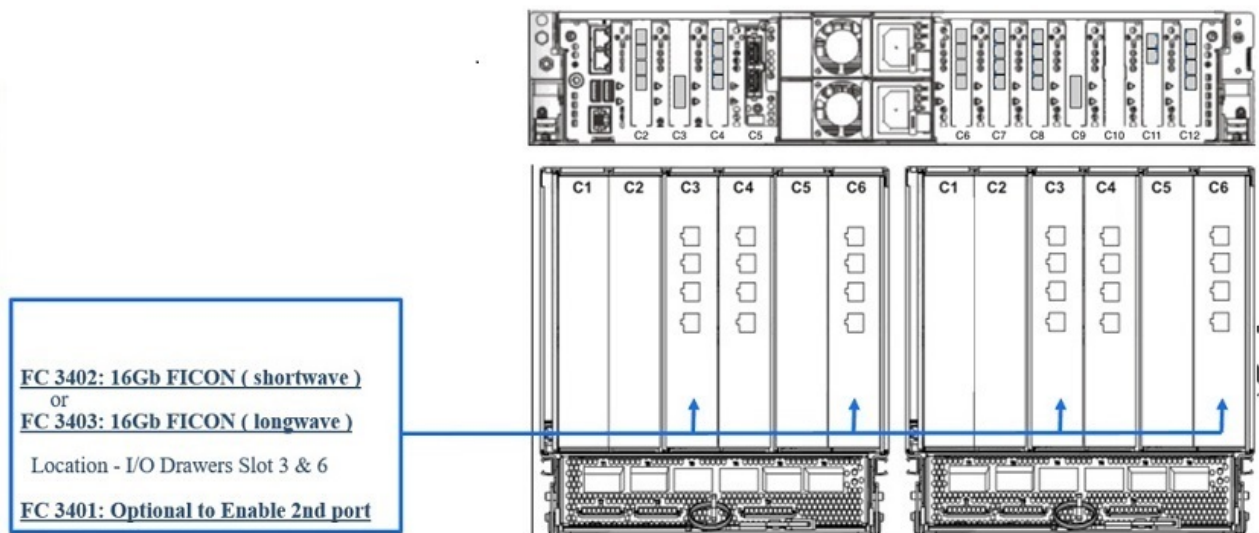


Figure 8. TS7770 Server (3957-VED) Expansion Unit I/O Drawer (FICON Connections)

Table 4. FICON connection order for both 2 and 4 card configurations(3957-VED) adapters	
Slot Number	Adapter
C3	I/O Drawer Interface card
C6	16 Gb Quad port FC HBA

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

Figure 9 on page 19 and Figure 10 on page 19 depict the TS7760 System Unit.



Figure 9. TS7760 Server (3957-VEC) System Unit (front view)

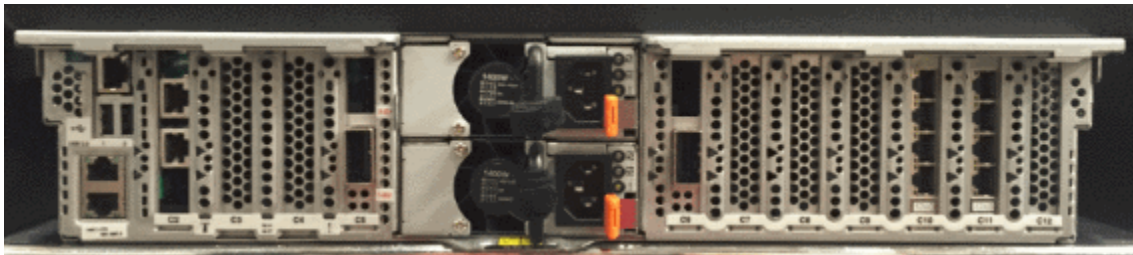


Figure 10. TS7760 Server (3957-VEC) System Unit (rear view)

Figure 11 on page 20 depicts the TS7760 Server Expansion Unit I/O drawer.

Table 5. TS7760 Server System Unit (3957-VEC) adapters	
Slot Number	Adapter
2	Serial 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 TS7760 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 6 on page 20 displays the slot numbers and adapters associated with ports on the expansion unit I/O drawers.



Figure 11. TS7760 Server Expansion Unit I/O drawer (rear view)

Table 6. 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 116), or • Dual port 10 Gb LW optical (“FC 1038, 10 Gb Quad Port Grid Optical LW Connection” on page 116)
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 SW FICON Adapter” on page 118 and “FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118 or “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 118 and “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 118.	

Related information

[“Concepts of storage virtualization”](#) on page 1

[“TS7700 system configurations”](#) on page 12

[“TS7700 system component details”](#) on page 27

[“TS7700 Grid”](#) on page 202

TS7770 with 3956-CFC Cache Controller

TS7700 supports the 3956-CFC/XFC enclosures with 3.84 TB capacity and 12 GB speed SSD drives. Each enclosure contains 24 SSD drives.

The 3956-CFC and the corresponding 3956-XFC enclosures support encryption abilities like earlier, including internal and external key management.

The following are the highlights of 3956-CFC:

- 2U bays supporting 24 drives
- SAS drive technology using SAS backbone between enclosures that support both SAS and NL-SAS disks, including SAS SSD
- Minimum configuration of one 3956-CFC
- Maximum configuration of one 3956-CFC and one 3956-XFC
- Dual active 16 Gb FC connectivity to host
- Negligible performance impact for encryption
 - Internal key management
 - External ISKLM/TKLM support



Figure 12. 3956-CFC

TS7770 with 3956-XFC Cache Expansion Enclosure

The 3956-XFC enclosure is configured with 24 SSD drives with 3.84 TB capacity and 12 GB speed.

The 3956-CFC controllers support only one 3956-XFC expansion enclosure, which contains the same size drives that are in 3956-CFC. The 3956-CFC and the corresponding 3956-XFC enclosure support encryption abilities, as earlier, including internal and external key management.



Figure 13. 3956-XFC

For a list of the available disk cache capacity options, refer to [“Capacity on Demand” on page 160](#).

TS7770 with 3956-CSB Cache Controller

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

The TS7700 Cache Controller contains 12 disk drive modules (DDMs).

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

TS7770 Cache Controller

The CSB may be utilized for all models of TS7700 and is offered with **10TB** NL-SAS 7.2k RPM drives.

The CSB and corresponding XSB drawers supports encryption abilities, as before, including internal key management and external key management.

Highlights of the CSB are:

- 2U bays supporting 12 3.5” disks
- SAS drive technology utilizing SAS backbone between drawers o Supporting both SAS and NL-SAS disks, including SAS SSD
- Dual active 16 Gb FC connectivity to host
- Negligible performance impact for encryption.
 - Internal key management
 - External ISKLM/TKLM/GKLM support

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, TS7760 Encryption Capable Expansion Frame (VEC section below)” on page 126 to obtain a new TS7700 Expansion Frame. You can order FC 9336 or FC 9337 against an existing TS7760 / TS7770 Base Frame, so that the TS7760/TS7770 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.

Related information

[“Concepts of storage virtualization” on page 1](#)

[“Data storage values” on page 26](#)

[“TS7700 feature codes” on page 115](#)

[“TS7700 system configurations” on page 12](#)

[“TS7700 system component details” on page 27](#)

[“TS7700 upgrade options” on page 96](#)

[“TS7700 Grid” on page 202](#)

[“TS7760 Cache Drawer” on page 43](#)

[“TS7760 Storage Expansion Frame” on page 37](#)

TS7770 with 3956-XSB Cache Expansion Enclosure

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.

TS7770 Cache Drawer

The drives used for CSB and its attached XSB will be 10TB NL-SAS 7.2k RPM normal drives.

CSB controllers will only support XSB expansion drawers which contain the same size drives as are in the CSB.

The CSB and corresponding XSB drawers will support encryption abilities, as before, including internal key management and external key management.

See “Capacity on Demand” on page 160, for a list of the available disk cache capacity options.

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 7 on page 24](#) displays the storage capacities of a base TS7760 Cache Controller with a range of TS7760 Cache Drawer configurations with 4 TB DDMs.

Table 7. Base Cache configurations and capacities with 4 TB drives. Table describes the configurations and capacities of the base 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 8 on page 25](#) displays the storage capacities of a base TS7760 Cache Controller with a range of TS7760 Cache Drawer configurations with 8 TB DDMs.

Table 8. Base Cache configurations and capacities with 8 TB drives. Table describes the configurations and capacities of the base 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	864 TB (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, TS7760 Encryption Capable Expansion Frame \(VEC section below\)” on page 126](#). 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).

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 38](#) and [“TS7760 Storage Expansion Frame Configurations with 8 TB DDMs” on page 40](#) in 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 123](#) and [“FC 9355, Field merge XFC” on page 129](#).

Related information

[“TS7700 system configurations” on page 12](#)

[“TS7760 Storage Expansion Frame” on page 37](#)

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 9 on page 26 compares the names, symbols, and values of the binary and decimal units. [Table 10 on page 26](#) shows the increasing percentage of difference between binary and decimal units.

Table 9. 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 10. 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%

Planning

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

Storage Acclimation

Server and storage equipment (racks and frames) must be gradually acclimated to the surrounding environment to prevent condensation.

ACCLIMATION STATEMENT:

<https://www.ibm.com/docs/en/power-sys-solutions/0000-PUR?topic=planning-acclimation>

Server and storage equipment (racks and frames) must be gradually acclimated to the surrounding environment to prevent condensation.

When server and storage equipment (racks and frames) is shipped in a climate where the outside temperature is below the dew point of the destination (indoor location), there is a possibility that water condensation can form on the cooler inside and outside surfaces of the equipment when the equipment is brought indoors.

Sufficient time must be allowed for the shipped equipment to gradually reach thermal equilibrium with the indoor environment before you remove the shipping bag and energize the equipment. Follow these guidelines to properly acclimate your equipment:

- Leave the system in the shipping bag. If the installation or staging environment allows it, leave the product in the full package to minimize condensation on or within the equipment.
- Allow the packaged product to acclimate for 24 hours. If there are visible signs of condensation (either external or internal to the product) after 24 hours, acclimate the system without the shipping bag for an additional 12 - 24 hours or until no visible condensation remains.
- Acclimate the product away from perforated tiles or other direct sources of forced air convection to minimize excessive condensation on or within the equipment.

Note: Condensation is a normal occurrence, especially when you ship equipment in cold-weather climates. All IBM® products are tested and verified to withstand condensation that is produced under these circumstances. When sufficient time is provided to allow the hardware to gradually acclimate to the indoor environment, there should be no issues with long-term reliability of the product.

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, FOx requires RPQ 8b3669 (Front/Rear and Side Panel Locking Procedure), PN 00VJ478, 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
 - TS7770 Server (3957-VED)
 - TS7760 Server (3957-VEC)
- I/O drawers
- Cache controller
 - TS7770 Cache Controller (3956-CSB)
 - TS7760 Cache Controller (3956-CSA)
- Optional cache expansion drawers
 - TS7770 Cache Drawer (3956-XSB)
 - TS7760 Cache Drawer (3956-XSA)

IBM TS7770 details R5.2

This section provides topics for the TS7770 components.

The following figure displays the base frame of 3956-CFC/XFC TS7700:



Figure 14. Base frame of TS7700 with 3956-CFC/XFC

TS7770 Cache Controller Enclosure (3956-CFC)

The TS7770 Cache controller is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

The TS7770 Cache controller provides dynamic disk pools-protected virtual volume disk storage for fast retrieval of data from cache. The TS7770 Cache controller offers the following features:

- Two node canisters, each with a six-core processor
- Two battery backup units (one for each node canister)
- Two AC power supplies with embedded enclosure cooling units
- 24 x 3.84 TB SSD in 2.5" SFF carrier
- 12 Gb SAS backbone between drawers
- Dual active 16 Gb FC connectivity to 3957-VED processor
- Negligible performance impact for encryption.
 - Internal key management
 - External ISKLM/TKLM support
- Optional attachment to a maximum of one TS7770 Cache Enclosure
- 64 GB cache (32 GB per canister)

For the 3956-CFC front view, see the following figure:



Figure 15. TS7770 Cache Controller 3956-CFC (front view)

For the 3956-CFC back view, see the following figure:



Figure 16. TS7770 Cache Controller 3956-CFC (rear view)

TS7770 Cache Expansion Enclosure (3956-XFC)

The TS7770 Cache Enclosure is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

SSD drives are used for both the 3956-CFC and 3956-XFC enclosures.

The 3956-XFC Expansion Enclosure offers the following features:

- Two AC power supplies with embedded enclosure cooling units
- 24 x 3.84 TB SSD in 2.5" SFF carrier
- The 3956-XFC is attached to the 3956-CFC Cache controller

For the 3956-XFC front view, see the following figure:



Figure 17. TS7770 Cache Drawer 3956-XFC (front view)

For the 3956-XFC back view, see the following figure:



Figure 18. TS7770 Cache Drawer 3956-XFC (rear view)

TS7770 Storage Capacity

Refer to Capacity on Demand.

The TS7770 Storage Capacity is delivered using a Capacity on Demand license model. Refer to table in [“Capacity on Demand” on page 160](#) for a list of the available licensed capacities

IBM TS7770 details

This section provides topics for the TS7770 components.

Figure 1 displays the frame layout for a manufacturing installed TS7770 base and expansion frame.

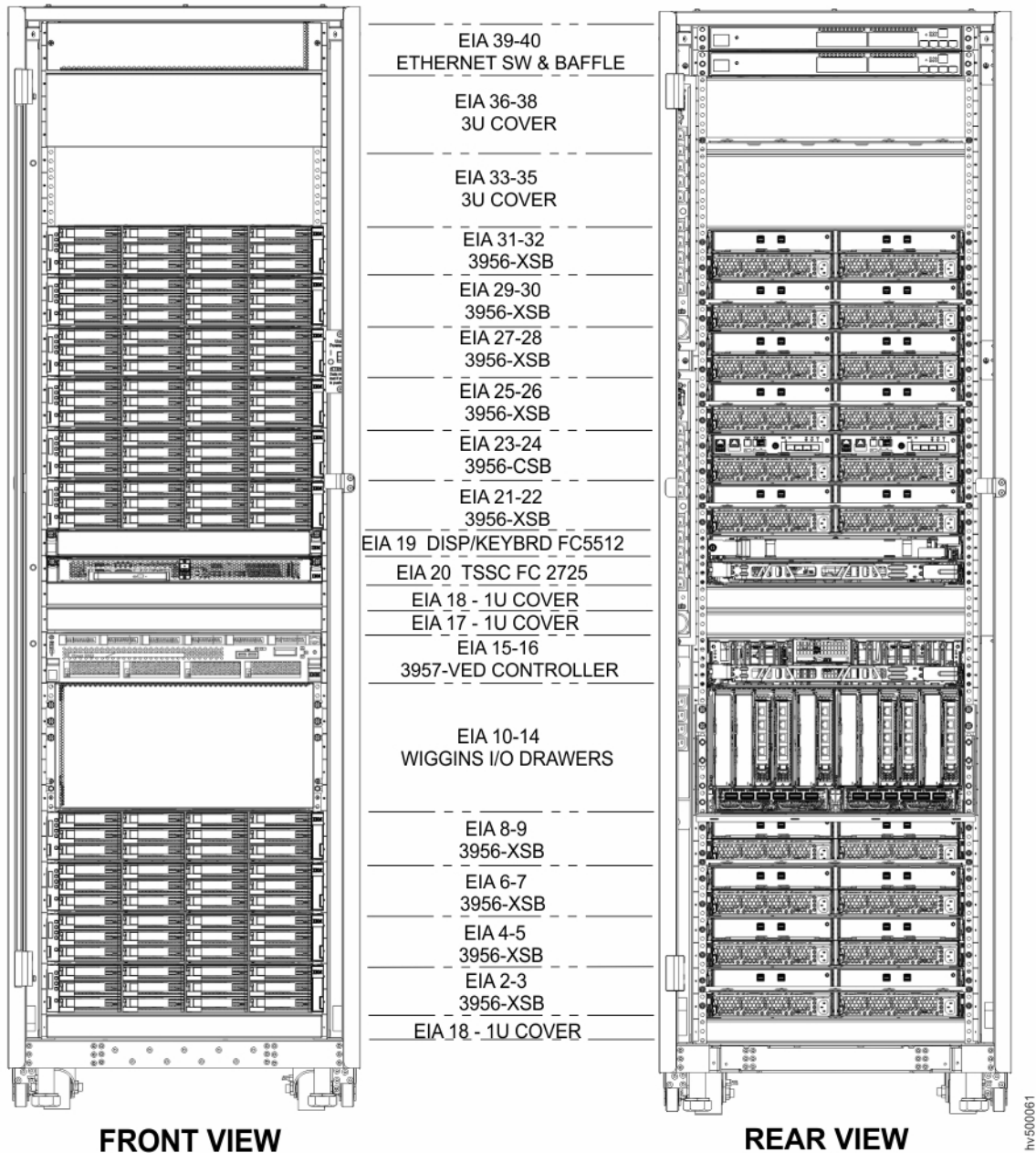


Figure 19. Front and rear view frame layout of the TS7770 base frame

TS7770 Cache Controller

The TS7770 Cache Controller is a self-contained 2U enclosure that mounts in the 3952 Tape Frame.

The TS7770 Cache Controller provides dynamic disk pools-protected virtual volume disk storage for fast retrieval of data from cache. The TS7770 Cache Controller offers the following features:

- Two node canisters, each with a six-core processor
- Two battery backup units (one for each node canister)
- Two AC power supplies with imbedded enclosure cooling units
- 12 NL-SAS 7.2k 3.5" SAS DDMs, each with a storage capacity of 10 TB (9.09 TiB)

- 12 Gb SAS backbone between drawers
- Dual active 16 Gb FC connectivity to 3957-VED processor
- Negligible performance impact for encryption.
 - Internal key management
 - External ISKLM/TKLM support
- Optional attachment to a maximum of nine TS7770 Cache Drawers in a TS7770 Base Frame
- Optional expansion of cache capabilities:
 - Once a TS7770 Base Frame is fully populated, a TS7770 Storage Expansion Frame can be added with a minimum of one TS7770 Cache Controller and one TS7770 Cache Drawer.
 - Once a total nine TS7770 cache drawers are added to the first controller in the expansion frame, a second TS7770 Cache Controller along with a minimum of one TS7770 Cache drawer can be added to the frame. The second controller can support a maximum of nine TS7770 Cache Drawers (same as the first controller in the frame) Figure 15. TS7770 Cache Controller 3956-CSB (front view) Figure 16.



Figure 20. TS7770 Cache Controller 3956-CSB (front view)



Figure 21. TS7770 Cache Controller 3956-CSB (rear view)



Figure 22. TS7770 Cache Controller 3956-XSB (rear view)

TS7770 Storage Capacity

Refer to Capacity on Demand.

The TS7770 Storage Capacity is delivered using a Capacity on Demand license model. Refer to table in [“Capacity on Demand” on page 160](#) for a list of the available licensed capacities

TS7770 Storage Expansion Frame

The TS7770 Storage Expansion Frame is a 3952 Tape Frame designated as a cache expansion frame for use with a fully configured TS7770 Base Frame.

The TS7770 Storage Expansion Frame enables expansion of the TS7770 Cache by attaching up to two more storage frames. Each frame contains one or two additional TS7770 Cache Controllers. Each controller can attach to a maximum of 9 additional TS7770 Cache Drawers, resulting in a maximum addition of 20 TS7770 Cache units within each TS7770 Storage Expansion Frame. A maximally configured TS7770 Base Frame with two attached and maximally configured TS7770 Storage Expansion Frames contains 50 total cache units.

A TS7770 Cache Controller and up to nine attached TS7770 Cache Drawers are referred to as a "string", with each TS7770 Cache Controller acting as the "head of [the] string". A single TS7770 can have up to five "strings" attached, the first in the base frame (base string) and the next four in the expansion frames (strings 1 and 2 in frame 1 and strings 3 and 4 in frame 2).

The distance between the first or second TS7770 Storage Expansion Frame and the TS7770 Base Frame cannot exceed 10 meters. This distance permits connection of the frames by using a 30-meter cable.

The TS7770 Storage Expansion Frame consists of the following components:

- One 3952 Tape Frame
- One TS7770 Cache Controller (3956-CSB)
- Optional attachment of up to 9 TS7770 Cache Drawers (3956-XSB)
- Optional attachment of a second TS7770 Cache Controller (3956-CSB)
- Optional attachment of up to 9 TS7770 Cache Drawers (3956-XSB) to the second TS7770 Cache Controller
- Each TS7770 Cache Controller (3956-CSB) or Cache Drawer (3956-XSB) contains 12 DDMs with a raw storage capacity of 10 TB per DDM

TS7770 First Expansion Frame cache layout. (String 2)

- minimum configuration - two cache enclosures (one 3956-CSB and one 3956-XSB)
- maximum configuration - ten cache enclosures (one 3956-CSB and nine 3956-XSB)

Note:

1. All cache enclosures are shipped from manufacturing in pairs.
2. If string 2 hardware is being added to an existing frame then it will be installed in pairs.
3. Any additional cache enclosures will be installed in pairs.

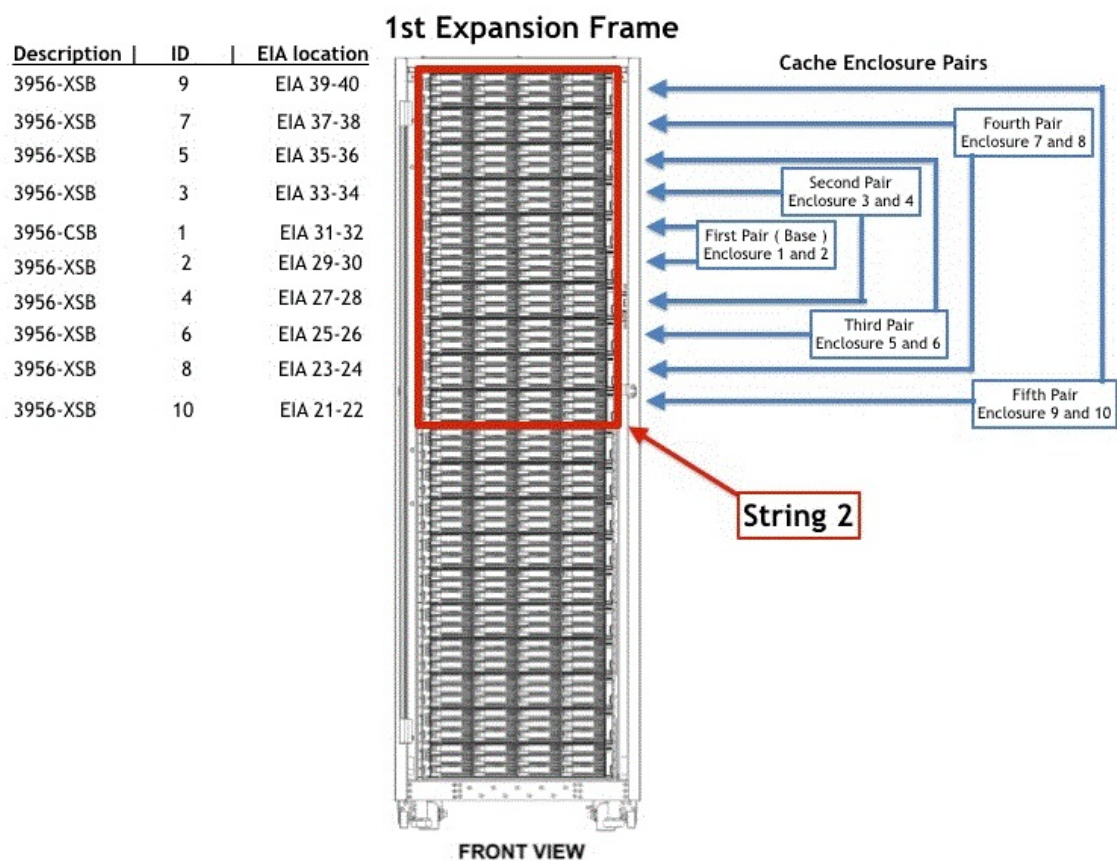


Figure 23. TS7770 First Expansion Frame cache layout. (String 2)

TS7770 Cache Drawer

The TS7770 Cache Drawer is a self-contained 2U enclosure that mounts in the 3952 Tape Frame. The drives used for CSB and its attached XSB will be 10TB NL-SAS 7.2k RPM normal drives.

- Two AC power supplies with imbedded enclosure cooling units
- 12 NL-SAS 7.2k 3.5" SAS DDMs, each with a storage capacity of 10 TB (9.09 TiB)
- Attachment to the TS7770 Cache Controller Figure



Figure 24. TS7770 Cache Drawer 3956-XSB (front view)



Figure 25. TS7770 Cache Drawer 3956-XSB (rear view)



Figure 26. TS7770 Cache Controller 3956-CSB (rear view)

IBM TS7760 details

This section provides topics for the TS7760 components.

[Figure 27 on page 36](#) displays the frame layout for a manufacturing installed TS7760.

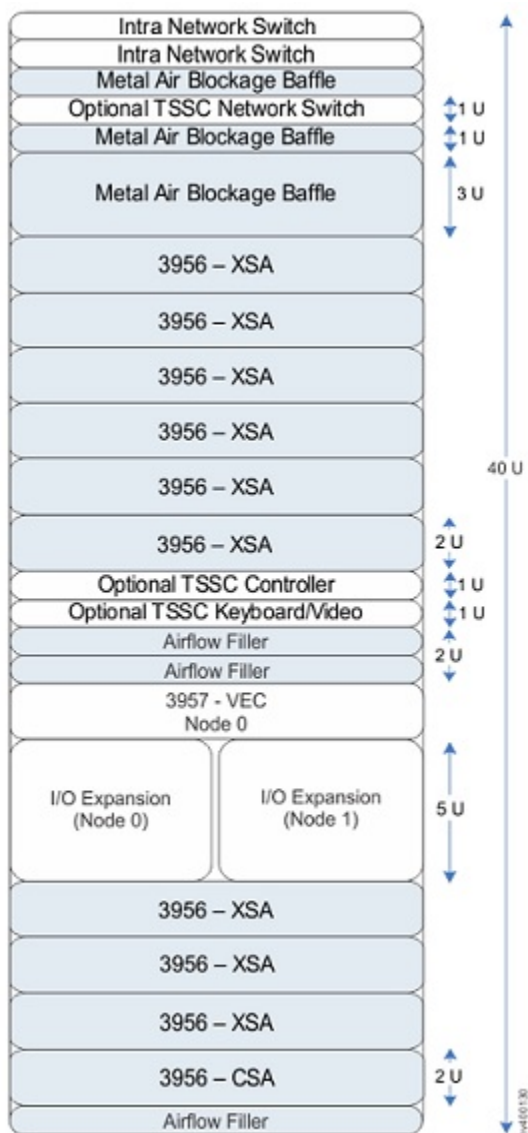


Figure 27. Single frame layout of a TS7760 with a manufacturing installed 3957-VEC, 3956-CSA, and 3956-XSA

Figure 28 on page 37 displays the frame layout for a TS7760 Storage Expansion Frame.

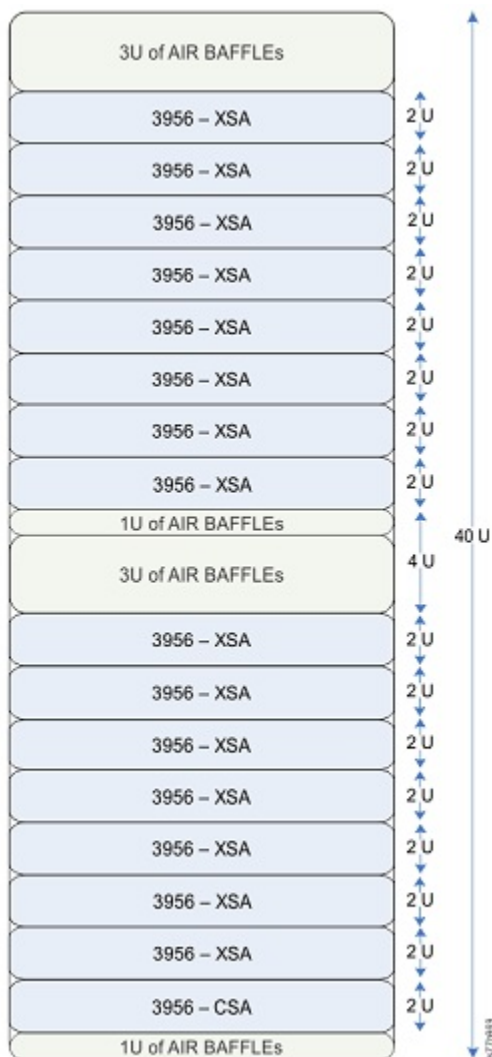


Figure 28. Layout of a TS7760 Storage Expansion Frame with 3956-CSA and 3956-XSA

Related information

["System requirements" on page 54](#)

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.

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 115](#)

[“System requirements” on page 54](#)

[“Upgrades for the TS7760” on page 102](#)

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 11. TS7760 Storage Expansion Frame configurations for 4 TB capacity drives

TS7760 Cache configuration for base frame	Cache units‡ in each TS7760 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, TS7760 Encryption Capable Expansion Frame (VEC section below)” on page 126 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 115](#)

[“System requirements” on page 54](#)

[“Upgrades for the TS7760” on page 102](#)

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 12. TS7760 Storage Expansion Frame configurations for 8 TB capacity drives

TS7760 Cache configuration for base frame	Cache units‡ in each TS7760 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, TS7760 Encryption](#)

Capable Expansion Frame (VEC section below)” on page 126 as a miscellaneous equipment specification (MES).

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 115](#)

[“System requirements” on page 54](#)

[“Upgrades for the TS7760” on page 102](#)

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 29. TS7760 Cache Controller 3956-CSA (front view)



Figure 30. 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 54](#)

[“TS7760 Storage Expansion Frame” on page 37](#)

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 31. TS7760 Cache Drawer 3956-XSA (front view)



Figure 32. TS7760 Cache Drawer 3956-XSA (rear view)

Related information

[“System requirements” on page 54](#)

Tape library attachments, drives, and media

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

The TS7770 Tape Attach and TS7760 Tape Attach store data on physical tape in the TS3500 Tape Library or the TS4500 Tape Library.

Related information

[“TS7700 Grid” on page 202](#)

[“TS3500/TS4500 Tape Library attachment” on page 44](#)

TS3500/TS4500 Tape Library attachment

A TS7770 Tape Attach or 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. The tape drives must reside in either Model L22, L23, D22, or D23 frames in the tape library. Each frame can contain up to 12 3592 Tape Drives.

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: 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](#) 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” on page 44](#)

[“Secure Data Erasure” on page 48](#)

[“Tape encryption” on page 103](#)

[FC 9900, Encryption configuration](#)

3592 Tape Drives

This section describes the 3592 Tape Drives associated with the TS7770 Tape Attach and TS7760 Tape Attach.

The 3592 Tape Drives supported for use with the TS7770 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 33 on page 45 illustrates the 3592 Tape Drive.

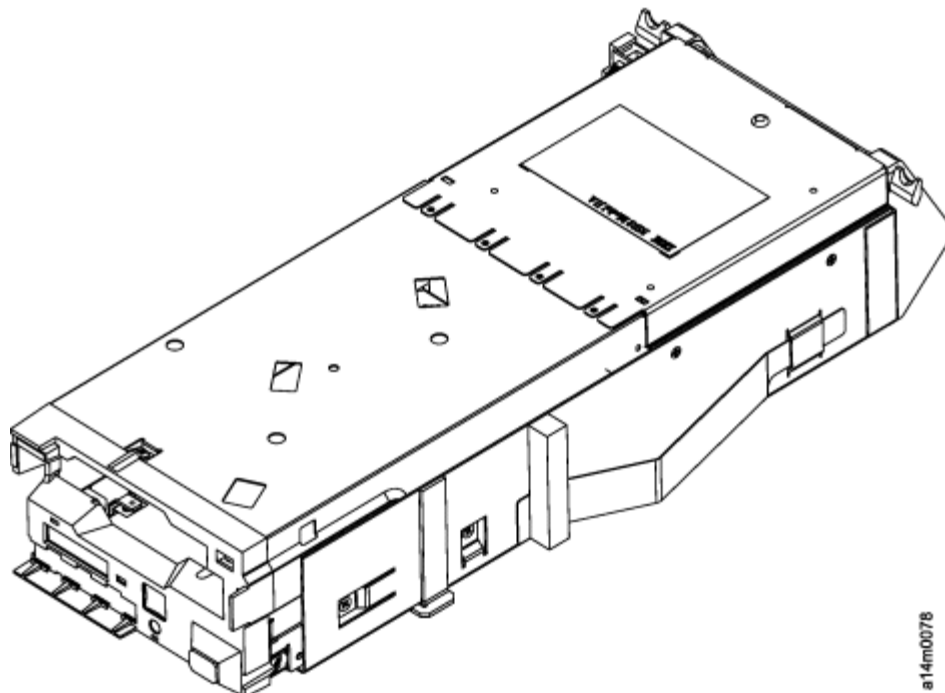


Figure 33. 3592 Tape Drive

Table 13 on page 45 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 13. Comparison of 3592 Tape Drives supported by the TS7770 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, ISKLM, or GKLM 4.1 only)	7.0 TB 10.0 TB 900 GB 2 TB	360 MB/s

Table 13. Comparison of 3592 Tape Drives supported by the TS7770 Tape Attach or TS7760 Tape Attach (continued)

3592 Tape Drive type	Supported media types	Encryption support	Capacity	Data rate
TS1140 Tape Drive (3592 E07 or EH7 Tape Drive)	JB JC JK Media read only: JA JJ	Yes (TKLM, ISKLM, or GKLM 4.1 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
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 TS7770 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 TS7770 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 TS7770 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), the IBM Security Key Lifecycle Manager (ISKLM), or the IBM Guardium Key Lifecycle Manager (GKLM) 4.1 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 TS7770 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 TS7770 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), the IBM Security Key Lifecycle Manager (ISKLM), or the IBM Guardium Key Lifecycle Manager (GKLM) 4.1 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 TS7770 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 TS7770 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 TS7770 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), the IBM Security Key Lifecycle Manager (ISKLM), or the IBM Guardium Key Lifecycle Manager (GKLM) 4.1 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.

Related information

[“3592 Tape Cartridges” on page 49](#)

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” on page 49](#)

[“Tape encryption” on page 103](#)

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 34 on page 49 shows the IBM TotalStorage™ 3592 Enterprise Tape Cartridge.

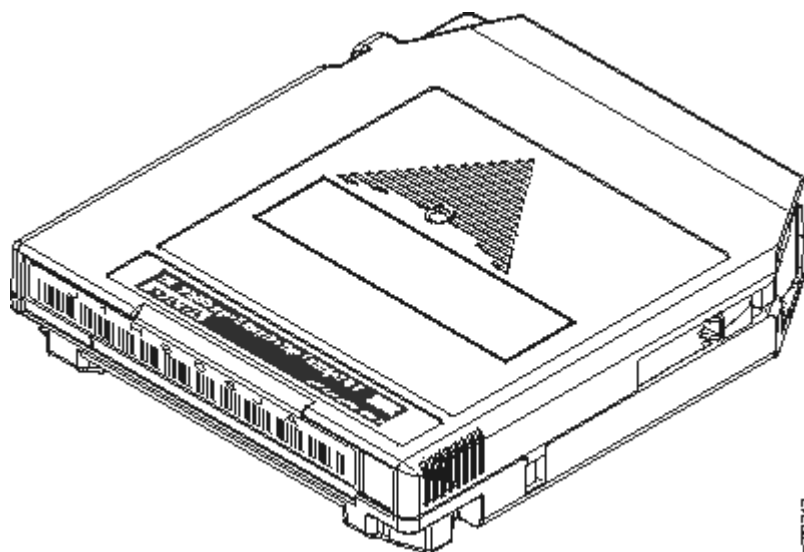


Figure 34. IBM 3592 Tape Cartridge

Tape cartridges can be distinguished by the text on the product label and by the color of the label. Table 14 on page 49 lists the characteristics of the 3592 Tape Cartridges.

Table 14. 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

Table 14. Supported IBM 3592 Tape Cartridges (continued)

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
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.

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.

The TS7700 presents 3490 Tape Drive images. Any data that can reside on a 3480/3490/3590/3592 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 TS7770 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 237](#). For more information about the Copy Export function, see [“Copy export overview” on page 112](#).

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 TS7770 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 112](#)

[“Configuring for disaster recovery” on page 237](#)

[“Allocation assistance” on page 233](#)

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 TS7770 or the TS7760.

TS7770 specifications and requirements R5.2

The following specifications and requirements are specific to the TS7770 R5.2 and its components.

The 3952 Tape Frame (3952-F07) houses the components of the TS7770 R5.2

When designated as a TS7770 R5.2 Base Frame ([FC 7339 TS7700 Encryption-capable base frame](#)), the 3952-F07 contains the following components:

- TS7770 Server (3957-VED) (includes two I/O drawers)
- TS7770 Cache Controller (3956-CFC)
- TS7770 Cache Expansion (3956-XFC)

Note: The standard 3952 Tape Frame ships with one internal power distribution unit. However, [FC 1912, Power Distribution Unit](#) is required to provide two power distribution units to support the availability characteristics of the TS7770.

If [FC 7339 TS7700 Encryption-capable base frame](#) is installed, the TS7770 R5.2 Base Frame has these physical specifications when fully configured.

If [FC 7338, TS7700 Encryption-capable expansion frame](#) is installed the TS7770 Storage Expansion Frame has these physical specifications when fully configured: The distance between a TS7770 Storage Expansion Frame and the TS7770 Base Frame cannot exceed 10 meters. This distance permits connection of the frames by using a 30-meter cable.

Table 15. Encryption-capable TS7770 physical frame F07 characteristics (FC 7339)			
	Base Frame	Expansion Frame, each (up to 2)	Client Rack Mount (min config/ max config)
Width	616 mm (24.25 in.)	616 mm (24.25 in.)	483 mm (19.0 in.) of each component
Depth	1274 mm (50.16 in.)	1274 mm (50.16 in.)	Depth of the deepest component 3757-VED (p9 pSeries) from front to back of the cable management arm & cables in the arm 38.9 inches (98.8 cm)

<i>Table 15. Encryption-capable TS7770 physical frame F07 characteristics (FC 7339) (continued)</i>			
	Base Frame	Expansion Frame, each (up to 2)	Client Rack Mount (min config/ max config)
Height	1930 mm (76 in.)	1930 mm (76 in.)	2 disk module config 18U in height = Min config 4 disk module config 22U in height 6 disk module config 26U in height 8 disk module config 30U in height 10 disk module config 34U in height = Max config
Weight	max 706.7 Kg (1558 lbs)	max 900.8 Kg (1986 lbs)	Min weight of components for configuration with 2 disk cache drawers is 243 kg (536.4 lbs) Max weight of components for configuration with 10 disk cache drawers is 456 kg (1,006 lbs)
Power consumption	max 3480 watts	max 4400 watts	max 3480 watts
Power phase options	single phase (240 V AC) or three phase (400 V AC)		single phase only (240 V AC)
Power frequency	50 Hz - 60 Hz (+/- 3 Hz)		
Dry bulb temperature (recommended operating range)	20°C to 25°C (68°F to 77°F)		
Relative humidity (recommended operating range)	40 % to 55%		

Table 16 on page 55 displays the maximum configuration of a TS7770. Table 17 on page 56 displays the physical specifications for each TS7770 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.

<i>Table 16. TS7770 maximum configuration</i>	
Component	Quantity of each component in 3952 Tape Frame as TS7770 Base frame
TS7770 Server (3957-VED)	1
TS7770 Cache Controller (3956-CFC)	1
TS7770 Cache Drawers (3956-XFC)	1

Table 17. TS7770 component specifications

Specification	TS7770 Server		TS7770 Cache Subsystem	
Type and Model	3957-VED	I/O expansion drawer (each of 2)	TS7770 cache controller 3956-CFC	TS7770 cache expansion drawer 3956-XFC
Width	482 mm (18.97 in)	440 mm (17.32 in.) Total width of two joined drawers	483 mm (19.0 in)	483 mm (19.0 in)
Depth	766.5 mm (30.2 in)	800 mm (31.5 in.)	556 mm (21.9 in)	556 mm (21.9 in)
Height	86.7 mm (3.4 in)	220 mm (8.66 in.)	87 mm (3.4 in)	87 mm (3.4 in)
Weight	30.4 kg (67 lbs)	42.2 kg (92.8 lb.) weight of two combined Reflects weight of each, without cassettes	27.7 kg (61.0 lb) fully configured	26.7 kg (58.7 lb) fully configured
Power	180-240 V AC 50/60 Hz (+/- 3 Hz)	180-240 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)
Temperature (operating)	5-40 degrees C (41-104 degrees F) Temperature depends on altitude, see Table 18 on page 57 . 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	810 watts	540 watts
Thermal output	6416 Btu/hour (max.)	Included in 3952 Tape Frame maximum	2730 Btu/hr	1820 Btu/hr
Power-source loading	1.6 kVA (max. config.) 3,048 m (10,000 ft.) max. altitude	Included in 3952 Tape Frame maximum	0.9 kVA	0.6 kVA

Table 17. TS7770 component specifications (continued)		
Specification	TS7770 Server	TS7770 Cache Subsystem
† Root Mean Square. In a multi-drawer configuration, total power is predicted to be a root mean square of the individual drawer maximums.		

Table 18. 3957-VED 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)

TS7770 Base Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the TS7770 Base Frame. The following table displays the maximum input power for a fully configured TS7770.

Table 19. TS7770 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)	3480 watts
Input power required	4.8 kVA (single phase)
Thermal units	12.2kBTU/hr, 3.06 kcal/hr

TS7770 Base Frame operating environment

The following table displays the total frame including VED, CSB, nine XSB, TSSC, and Integrated control path.

Table 20. TS7770 maximum configuration frame with all components

Operating environment	Value
Temperature	10° to 32.0° C (50° to 89.6° F) up to 5,000 feet 10 to 28.0° C (50° to 82.4° F) 5,001 to 7,000 feet
Relative humidity	20% to 80% up to 5000 feet and 20% to 60% from 5001 to 7000 feet
Heat output (caloric value)	12.2 kBTU/hr, 3.06 kcal/hr
Wet bulb (caloric value)	23° C
Electrical power	3480 watts
Capacity of exhaust	775 m3/h
Noise level	58 db at ambient 25° C and 65 db at high temperature 32° C
Leakage	10 mA

TS7770 minimum configuration requirements

The following components are the minimum configuration requirements for a TS7770 with microcode level 8.50.x.x.

TS7770 minimum configuration requirements with microcode level 8.50.x.x:

One 3952 F0x Tape Frame with the following features:

- FC 1512, Single phase PDU
- [FC 1904](#), Redundant power
- FC 2725, Rackmount TS3000 System Console
- FC 5512, KVM
- [FC 5631](#), Install 3957-VED
- [FC 5663](#), Plant installation of 3956-CSB
- [FC 5664](#), Plant installation of 3956-XSB
- [FC 5756](#), Integrated control path
- [FC 7335](#) or [FC 7337](#) or [FC 7339](#), TS7770 Encryption-capable base frame
- [FC 9906](#), New order install
- [FC AGKT](#), Ship with R5.0 Machine Code
- A power cord appropriate for the country of installation selected from:
 - [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, or
 - [FC 9966](#), Unterminated power cord (China)

One TS7770 Server (3957-VED) with the following features:

- [FC 9268](#), Plant installation of 100 MB/s throughput
- [FC 9000](#), Mainframe attachment

- [FC AGKT](#), Ship with R5.0 Machine Code
- [FC 9350](#), Plant Install
- Two grid adapters:
 - [FC 1039](#), 1 Gb grid quad port copper connection
 - [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 SW FICON Adapter” on page 110
 - Two of “[FC 3403](#), 16 Gb FICON Long Wavelength Attachment” on page 110

[FC 2715](#), Console attachment

[FC 9277](#), External Disk Encryption Certificate - Plant

One TS7770 Cache Controller (3956-CSB) with the following features:

- [FC 7119](#), 120 TB (78.75 TB Usable) SAS
- [FC 9352](#), Plant Install

One TS7770 Cache Module (3956-XSB) with the following features:

- [FC 7119](#), 120 TB (SAS) Storage
- [FC 9354](#), Plant Install XSB

3952 Tape Frame specifications

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

The individual standard components include the following:

- 3952 Tape Frame
- Ethernet switches

Refer to the topic “[TS7770 specifications and requirements](#)” on page 60 for a description of the difference between a 3952 Tape Frame used as a TS7770 Base Frame and as a TS7770 Storage Expansion Frame.

Refer to the topic “[TS7760 specifications and requirements](#)” on page 67 for a description of the difference between a 3952 Tape Frame used as a TS7760 Base Frame and as a TS7760 Storage Expansion Frame.

Related information

[“TS7770 specifications and requirements” on page 60](#)

[“TS7760 specifications and requirements” on page 67](#)

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.

Related information

[“3952 Tape Frame specifications” on page 59](#)

[“Network switches and TCP/IP ports requirements” on page 87](#)

[“System requirements” on page 54](#)

TS7770 specifications and requirements

The following specifications and requirements are specific to the TS7770 and its components.

The 3952 Tape Frame (3952 F06 or F07) houses the components of the TS7770.

When designated as a **TS7770 Base Frame** ([FC 7335](#) or [FC 7337](#), [TS7700 Encryption-capable base frame](#)), the 3952 F06 or F07 contains the following components:

- TS7770 Server (3957-VED) (includes control unit and 2 I/O drawers)
- TS7770 Cache Controller (3956-CSB)
- TS7770 Cache Drawer(s) (3956-XSB) Internal power distribution units

Note: The standard 3952 Tape Frame ships with one internal power distribution unit. However, [FC 1904](#), [Power Distribution Unit](#) is required to provide two power distribution units to support the availability characteristics of the TS7770.

If [FC 7335](#) or [FC 7337](#), [TS7700 Encryption-capable base frame](#) is installed, the TS7770 Base Frame has these physical specifications when fully configured.

When designated as a **TS7770 Storage Expansion Frame** ([FC 7336](#) or [FC 7338](#), [TS7700 Encryption Capable Expansion Frame](#) the 3952 F06 or F07) contains the following components:

- TS7770 Cache Controllers (3956-CSB)
- TS7770 Cache Drawer(s) (3956-XSB)

Note: [FC 9336](#) or [FC 9337](#) is also required to attach the base and expansion frames.

If [FC 7336](#), [TS7700 Encryption-capable expansion frame](#) is installed the TS7770 Storage Expansion Frame has these physical specifications when fully configured: The distance between a TS7770 Storage Expansion Frame and the TS7770 Base Frame cannot exceed 10 meters. This distance permits connection of the frames by using a 30-meter cable.

Table 21. Encryption- capable TS7770 physical frame F06 characteristics (FC 7335 and FC 7336)			
	Base Frame	Expansion Frame, each (up to 2)	Client Rack Mount (min config/ max config)
Width	616 mm (24.25 in.)	616 mm (24.25 in.)	483 mm (19.0 in.) of each component
Depth	1425 mm (56.1 in.)	1425 mm (56.1 in.)	Depth of the deepest component 3757-VED (p9 pSeries) from front to back of the cable management arm & cables in the arm 38.9 inches (98.8 cm)

Table 21. Encryption- capable TS7770 physical frame F06 characteristics (FC 7335 and FC 7336)
(continued)

	Base Frame	Expansion Frame, each (up to 2)	Client Rack Mount (min config/ max config)
Height	1930.4 mm (76 in.)	1930.4 mm (76 in.)	2 disk module config 18U in height = Min config 4 disk module config 22U in height 6 disk module config 26U in height 8 disk module config 30U in height 10 disk module config 34U in height = Max config
Weight	max 735.3 Kg (1,621 lib)	max 929.3 Kg (2,049 lbs)	Min weight of components for configuration with 2 disk cache drawers is 243 kg (536.4 lbs) Max weight of components for configuration with 10 disk cache drawers is 456 kg (1,006 lbs)
Power consumption	max 3480 watts	max 4400 watts	max 3480 watts
Power phase options	single phase (240 V AC) or three phase (400 V AC)		single phase only (240 V AC)
Power frequency	50 Hz - 60 Hz (+/- 3 Hz)		
Dry bulb temperature (recommended operating range)	20°C to 25°C (68°F to 77°F)		
Relative humidity (recommended operating range)	40 % to 55%		

If FC 7338, TS7700 Encryption-capable expansion frame is installed the TS7770 Storage Expansion Frame has these physical specifications when fully configured: The distance between a TS7770 Storage Expansion Frame and the TS7770 Base Frame cannot exceed 10 meters. This distance permits connection of the frames by using a 30-meter cable.

Table 22. Encryption- capable TS7770 physical frame F07 characteristics (FC 7337 and FC 7338 and FC 7339)

	Base Frame	Expansion Frame, each (up to 2)	Client Rack Mount (min config/ max config)
Width	616 mm (24.25 in.)	616 mm (24.25 in.)	483 mm (19.0 in.) of each component

Table 22. Encryption- capable TS7770 physical frame F07 characteristics (FC 7337 and FC 7338 and FC 7339) (continued)

	Base Frame	Expansion Frame, each (up to 2)	Client Rack Mount (min config/ max config)
Depth	1274 mm (50.16 in.)	1274 mm (50.16 in.)	Depth of the deepest component 3757-VED (p9 pSeries) from front to back of the cable management arm & cables in the arm 38.9 inches (98.8 cm)
Height	1930 mm (76 in.)	1930 mm (76 in.)	2 disk module config 18U in height = Min config 4 disk module config 22U in height 6 disk module config 26U in height 8 disk module config 30U in height 10 disk module config 34U in height = Max config
Weight	max 706.7 Kg (1558 lbs)	max 900.8 Kg (1986 lbs)	Min weight of components for configuration with 2 disk cache drawers is 243 kg (536.4 lbs) Max weight of components for configuration with 10 disk cache drawers is 456 kg (1,006 lbs)
Power consumption	max 3480 watts	max 4400 watts	max 3480 watts
Power phase options	single phase (240 V AC) or three phase (400 V AC)		single phase only (240 V AC)
Power frequency	50 Hz - 60 Hz (+/- 3 Hz)		
Dry bulb temperature (recommended operating range)	20°C to 25°C (68°F to 77°F)		
Relative humidity (recommended operating range)	40 % to 55%		

Table 23 on page 63 displays the maximum configuration of a TS7770. Table 24 on page 63 displays the physical specifications for each TS7770 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 23. TS7770 maximum configuration

Component	Quantity of each component in 3952 Tape Frame as TS7770 Base frame	Quantity of each component in 3952 Tape Frame as optional TS7770 Storage Expansion Frame with FC 9336 1st Expansion Frame	Quantity of each component in 3952 Tape Frame as optional TS7770 Storage Expansion Frame with FC 9337 2nd Expansion Frame
TS7770 Server (3957-VED)	1	0	0
TS7770 Cache Controller (3956-CSB)	1	2	2
TS7770 Cache Drawers (3956-XSB)	9	18	18

Table 24. TS7770 component specifications

Specification	TS7770 Server		TS7770 Cache Subsystem	
Type and Model	3957-VED	I/O expansion drawer (each of 2)	TS7770 cache controller 3956-CSB	TS7770 cache expansion drawer 3956-XSB
Width	482 mm (18.97 in)	440 mm (17.32 in.) Total width of two joined drawers	483 mm (19.0 in)	483 mm (19.0 in)
Depth	766.5 mm (30.2 in)	800 mm (31.5 in.)	556 mm (21.9 in)	556 mm (21.9 in)
Height	86.7 mm (3.4 in)	220 mm (8.66 in.)	87 mm (3.4 in)	87 mm (3.4 in)
Weight	30.4 kg (67 lbs)	42.2 kg (92.8 lb.) weight of two combined Reflects weight of each, without cassettes	27.7 kg (61.0 lb) fully configured	26.7 kg (58.7 lb) fully configured
Power	180-240 V AC 50/60 Hz (+/- 3 Hz)	180-240 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)
Temperature (operating)	5-40 degrees C (41-104 degrees F) Temperature depends on altitude, see Table 25 on page 64 . 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)

Table 24. TS7770 component specifications (continued)				
Specification	TS7770 Server		TS7770 Cache Subsystem	
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	810 watts	540 watts
Thermal output	6416 Btu/hour (max.)	Included in 3952 Tape Frame maximum	2730 Btu/hr	1820 Btu/hr
Power-source loading	1.6 kVA (max. config.) 3,048 m (10,000 ft.) max. altitude	Included in 3952 Tape Frame maximum	0.9 kVA	0.6 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 25. 3957-VED 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)

TS7770 Base Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the TS7770 Base Frame. [Table 26 on page 65](#) displays the maximum input power for a fully configured TS7770.

Table 26. TS7770 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)	3480 watts
Input power required	4.8 kVA (single phase)
Thermal units	12.2kBTU/hr, 3.06 kcal/hr

TS7770 Base Frame operating environment

Table 27 on page 65 displays the total frame including VED, CSB, nine XSB, TSSC, and Integrated control path.

Table 27. TS7770 maximum configuration frame with all components

Operating environment	Value
Temperature	10° to 32.0° C (50° to 89.6° F) up to 5,000 feet 10 to 28.0° C (50° to 82.4° F) 5,001 to 7,000 feet
Relative humidity	20% to 80% up to 5000 feet and 20% to 60% from 5001 to 7000 feet
Heat output (caloric value)	12.2 kBTU/hr, 3.06 kcal/hr
Wet bulb (caloric value)	23° C
Electrical power	3480 watts
Capacity of exhaust	775 m3/h
Noise level	58 db at ambient 25° C and 65 db at high temperature 32° C
Leakage	10 mA

TS7770 Storage Expansion Frame power requirements

Your facility must ensure an available power supply to meet the input voltage requirements for the TS7770 Storage Expansion Frame. Table 28 on page 65 displays the maximum input power for a fully configured TS7770.

Table 28. TS7770 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

Table 28. TS7770 Storage Expansion Frame maximum input power requirements (continued)

Power requirement	Value
Power (watt)	4400 watts
Input power required	4.8 kVA (single phase)
Thermal units	15.4 kBtu/hr, 4.0 kcal/hr
Exhaust capacity	1030 m ³ /hr
Noise level	59 db

TS7770 minimum configuration requirements

The following components are the minimum configuration requirements for a TS7770 with microcode level 8.50.x.x.

TS7770 minimum configuration requirements with microcode level 8.50.x.x:

One 3952 F0x Tape Frame with the following features:

- FC 1512, Single phase PDU
- FC 1904, Redundant power
- FC 2725, Rackmount TS3000 System Console
- FC 5512, KVM
- FC 5631, Install 3957-VED
- FC 5663, Plant installation of 3956-CSB
- FC 5664, Plant installation of 3956-XSB
- FC 5756, Integrated control path
- FC 7335 or FC 7337 or FC 7339, TS7770 Encryption-capable base frame
- FC 9906, New order install
- FC AGKT, Ship with R5.0 Machine Code
- A power cord appropriate for the country of installation selected from:
 - 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, or
 - FC 9966, Unterminated power cord (China)

One TS7770 Server (3957-VED) with the following features:

- FC 9268, Plant installation of 100 MB/s throughput
- FC 9000, Mainframe attachment
- FC AGKT, Ship with R5.0 Machine Code
- FC 9350, Plant Install
- Two grid adapters:
 - FC 1039, 1 Gb grid quad port copper connection
 - 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 SW FICON Adapter](#)” on page 110
 - Two of “[FC 3403, 16 Gb FICON Long Wavelength Attachment](#)” on page 110

[FC 2715](#), Console attachment

[FC 9277](#), External Disk Encryption Certificate - Plant

One TS7770 Cache Controller (3956-CSB) with the following features:

- [FC 7119](#), 120 TB (78.75 TB Usable) SAS
- [FC 9352](#), Plant Install

One TS7770 Cache Module (3956-XSB) with the following features:

- [FC 7119](#), 120 TB (SAS) Storage
- [FC 9354](#), Plant Install XSB

TS7760 specifications and requirements

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

The 3952 Tape Frame (3952 F06 or 3952 F07) houses the components of the TS7760.

When designated as a TS7760 Base Frame (“[FC 7333, TS7700 Encryption-capable base frame](#)” on page 126), the 3952 F06 or 3952 F07 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 116 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:

<i>Table 29. Encryption-capable TS7760 Base Frame specifications</i>	
Specification	Measurement
Width	616 mm (24.25 in.)
Depth	1425 mm (56.1 in.)
Height	1930.4 mm (76 in.)
Weight	1644 lbs (745.7 kg)

When designated as a TS7760 Storage Expansion Frame (“[FC 7334, TS7760 Encryption Capable Expansion Frame \(VEC section below\)](#)” on page 126), the 3952 F06 or 3952 F07 contains the following components:

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

Note: [FC 9336](#) or [FC 9337](#) 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 30. Encryption-capable TS7760 Storage Expansion Frame specifications

Specification	Measurement
Width	616 mm (24.25 in.)
Depth	1425 mm (56.1 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 31 on page 68 displays the maximum configuration of a TS7760. Table 32 on page 68 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 31. 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 32. 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

Table 32. TS7760 component specifications (continued)

Specification	TS7760 Server		TS7760 Cache Subsystem	
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)
Temperature (operating)	5-40 degrees C (41-104 degrees F) Temperature depends on altitude, see Table 33 on page 70. 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 33. 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 34 on page 70](#) displays the maximum input power for a fully configured TS7760.

Table 34. 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 35 on page 70](#) displays the maximum input power for a fully configured TS7760.

Table 35. 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

Table 35. TS7760 Storage Expansion Frame maximum input power requirements (continued)

Power requirement	Value
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

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 or 3952 F07 Tape Frame with the following features:

- [FC 7333, TS7700 Encryption-capable base frame](#)
- [FC 5630, Install 3957-VECFC 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” on page 128](#)
- [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 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 SW FICON Adapter” on page 118](#)
 - Two of [“FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118](#)

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 115](#)

[“TS7760 Cache Controller” on page 42](#)

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 75](#). The heat load for the 3952 Tape Frame system can be found under [“3952 Tape Frame specifications” on page 59](#). The total system heat load is the sum of the heat loads for all installed frames.

Related information

[“3952 Tape Frame specifications” on page 59](#)

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 for the base frame

If the 3952 Tape Expansion 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 398 kg/m² (81.5 lb./ft.²) when frames are stacked side by side. However, IBM recommends an extra 12 inch clearance on both sides of the frame in addition to the door opening clearance on the front of the frame and on the rear of the frame. This will give a floor load rating needed of at least 291 kg/m² (59.6 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 5.41 kg/cm² (77 lb./in.²).

Floor – weight distribution and loading for the expansion frame

If the 3952 Tape Expansion 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 478 kg/m² (97.86 lb./ft.²) when frames are stacked side by side. However, IBM recommends an extra 12 inch clearance on both sides of the frame in addition to the door opening clearance on the front of the frame and on the rear of the frame. This will give a floor load rating needed of at least 340 kg/m² (69.7 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 6.82 kg/cm² (97 lb./in.²).

Clearance requirements

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

Clearance – moving the frame

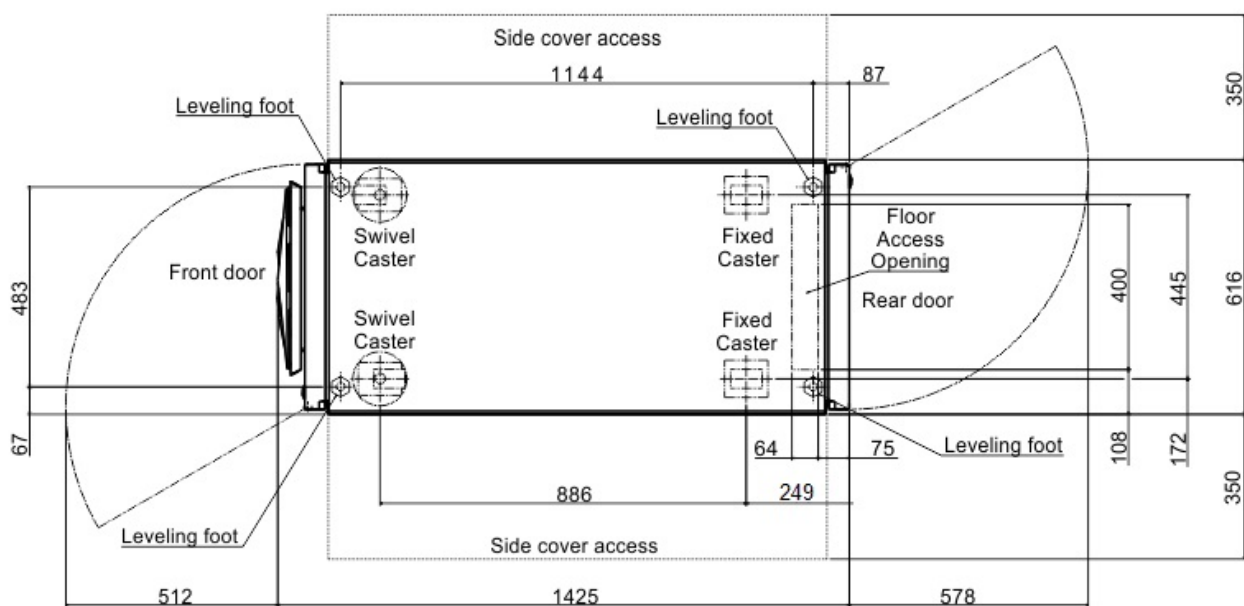
Two persons should be available to move system components between locations. [Table 36 on page 73](#) shows the minimum aisle and door dimensions for moving components from one location to another for the 3952 Tape Frame.

Table 36. Required clearances when moving the 3952 F06 or F07 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 or F07 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.).	

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 37 on page 74](#) lists the specific clearance requirements for the 3952 Tape Frame.

[Figure 35 on page 74](#) gives the opening radius of the front and rear doors when the F06 or F07 frame is in position. It also shows the side panel access distance. From these dimensions, [Table 37 on page 74](#) 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.



FRAME HEIGHT = 1930.4 mm
 FRAME WEIGHT = 746 kg (1645 lb)

3952-F06 FRAME SPECIFICATIONS

hy400139

Figure 35. Bottom view of F06 frame dimensions when in position

Table 37. Required clearances when the F06 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.

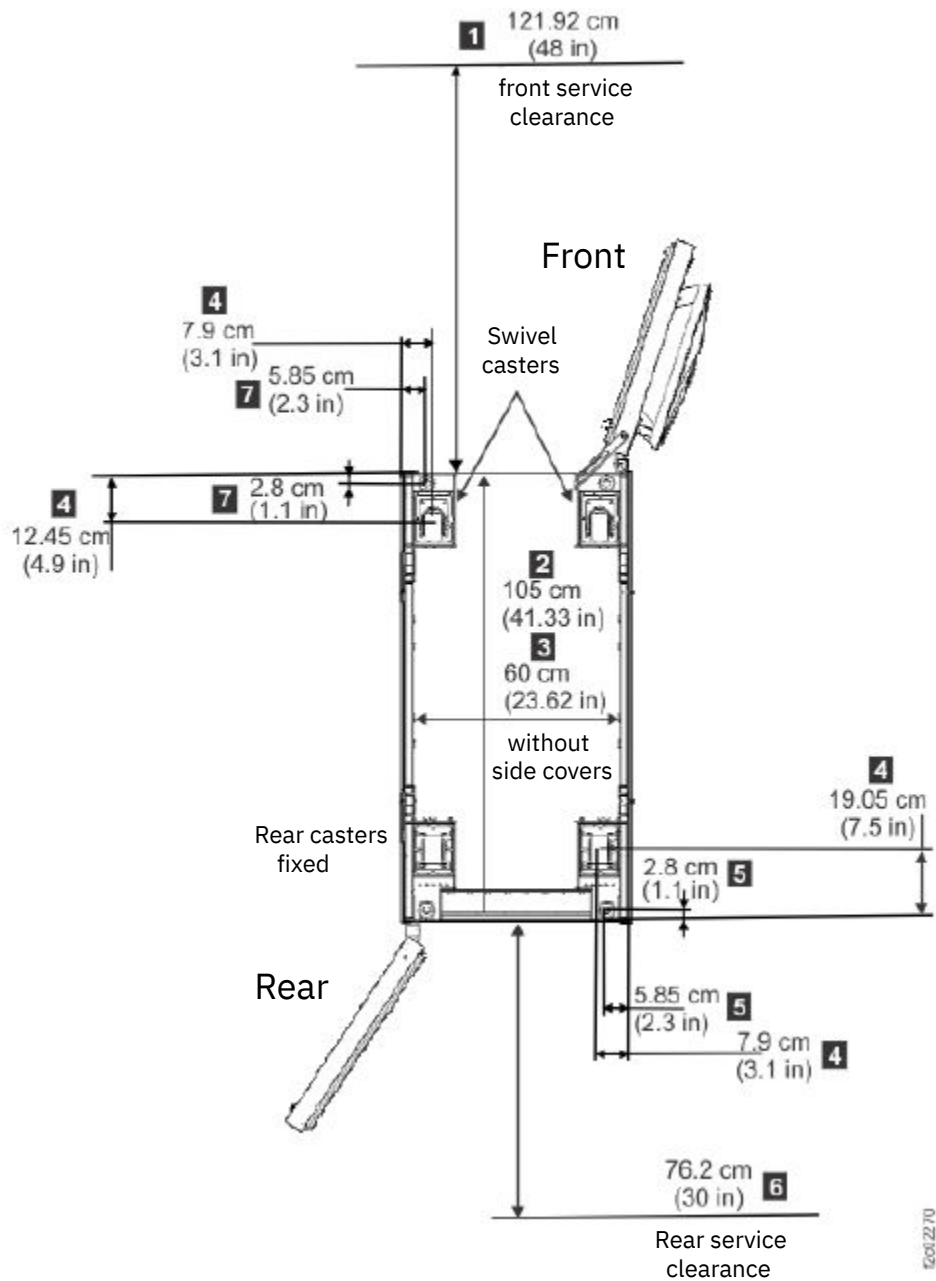


Figure 36. 3952-F07 frame dimensions when in position

Environmental requirements

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

Table 38 on page 75 shows recommended environmental conditions for the TS7700.

Table 38. 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)

Table 38. Temperature, altitude, and humidity specifications (continued)

Condition	Air temperature	Altitude	Relative humidity ¹	Wet bulb temperature
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 39. 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 ($\text{\AA}/\text{month}$, $\approx 0.0039 \mu\text{g}/\text{cm}^2\text{-hour weight gain}$) ² . In addition, the reactivity rate of silver coupons is less than $300\text{\AA}/\text{month}$ ($\approx 0.0035 \mu\text{g}/\text{cm}^2\text{-hour weight gain}$) 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 .

Table 39. Air quality specifications (continued)

Specification	Restrictions
Notelist: 1. ANSI/ISA-S71.04. 1985. <i>Environmental conditions for process measurement and control systems: Airborne contaminants</i>, 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 Cu₂S and Cu₂O 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 Ag₂S 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.	

Acoustic requirements

This topic gives the acoustic requirements for the TS7700.

Notes:

1. Declared level LWA,m is the upper-limit A-weighted sound power level; Declared level LpA,m is the mean A-weighted sound pressure level measured at the 1-meter bystander positions.
2. The statistical adder for verification, Kv, is a quantity to be added to the declared mean A-weighted sound power level, LWA,m such that there will be a 95% probability of acceptance, when using the verification procedures of ISO 9296, if no more than 6.5% of the batch of new equipment has A-weighted sound power levels greater than (LWA,m + Kv).
3. The quantity LWA,c (formerly called LWAd), can be computed from the sum of LWA,m and Kv.
4. All measurements made in conformance with ISO 7779 and declared in conformance with ISO 9296.
5. B, dB, abbreviations for bels and decibels, respectively. 1 B = 10 dB.
6. Under certain environments, configurations, system settings and/or workloads, fan speeds increase resulting in high noise levels
7. Notice: 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. 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.
8. Measurement given is worst of front- and back-side service position measurements.

Declared noise emission values in accordance with ISO 9296 ⁽¹⁻⁶⁾						
Product description TS7770 3957-VED	Declared A-weighted sound power level, $L_{W,A,m}$ (B)		Declared A-weighted emission sound pressure level, $L_{p,A}$ (dB)		Statistical adder for verification, K_v (B)	
	Operating	Idling	Operating	Idling	Operating	Idling
Nominal Configuration: 23±2°C	7.1	7.1	56	56	0.3	0.3
Nominal Configuration: 27°C, 500m	7.2	7.2	57	57	0.3	0.3
Maximum Configuration: 37°C	8.6 ^[7]	8.6 ^[7]	72	72	0.3	0.3
Maximum Configuration: 37°C, Pull 1 of dual-frame power legs	8.6 ^[7]	8.6 ^[7]	72	72	0.3	0.3
Worst Case Service Position: 37°C, Pull 1 of dual-frame power legs 0.5 m from noise source, 1.0 m from ground	-	-	84 ^[8]	-	-	-

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.
- z/TPF, 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

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 37 on page 80 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.

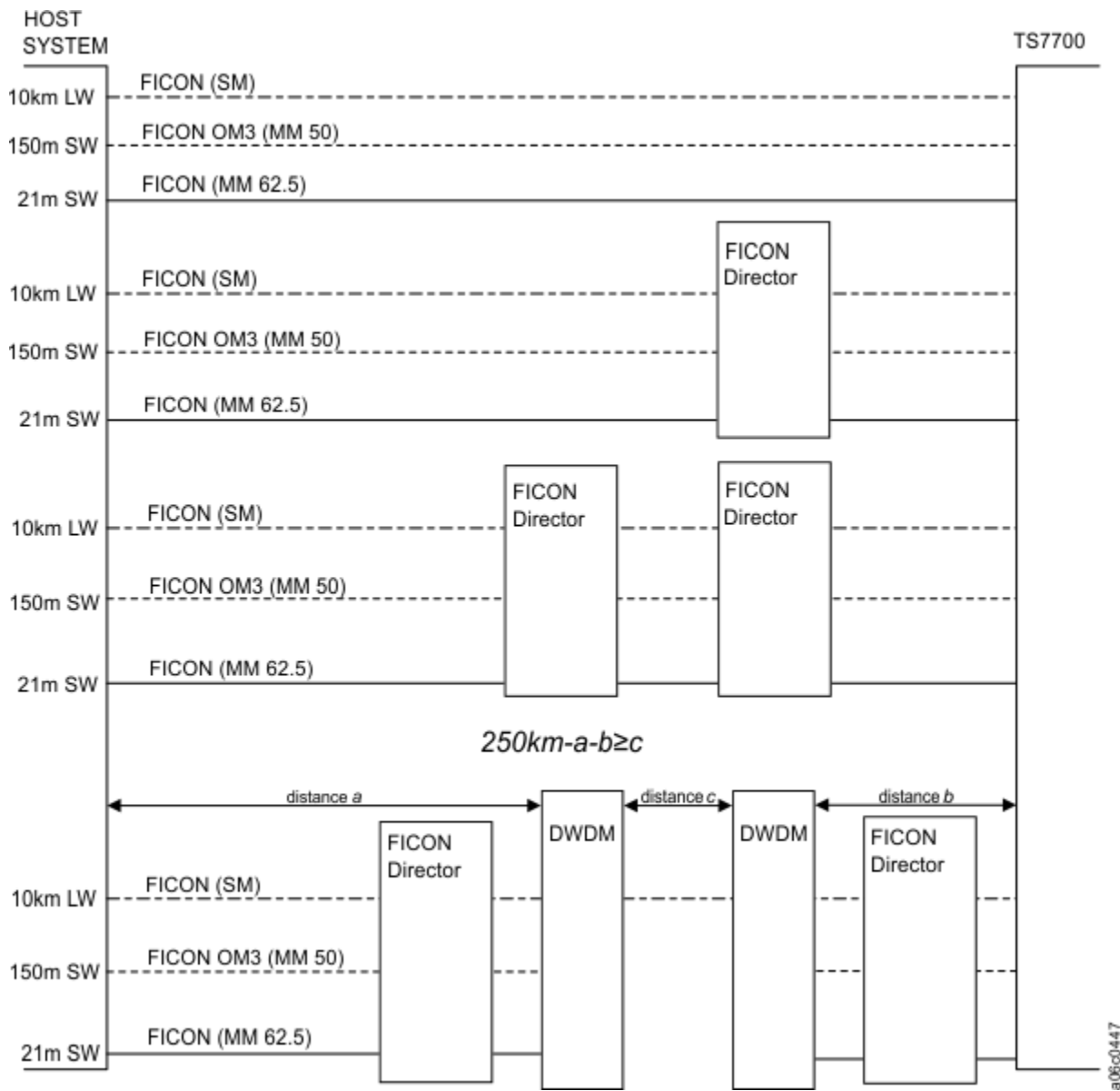


Figure 37. IBM Z® host attachment to TS7700 (at speed of 8 Gb/second)

Restrictions:

1. The FICON long-wavelength attachment that is shown in Figure 37 on page 80 is “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 118, 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 SW FICON Adapter” on page 118 and “FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118 or “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 118 and “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 118.

“FC 3402, 16 Gb SW FICON Adapter” on page 118, “FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118, “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 118 or “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 118 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 38 on page 81](#).

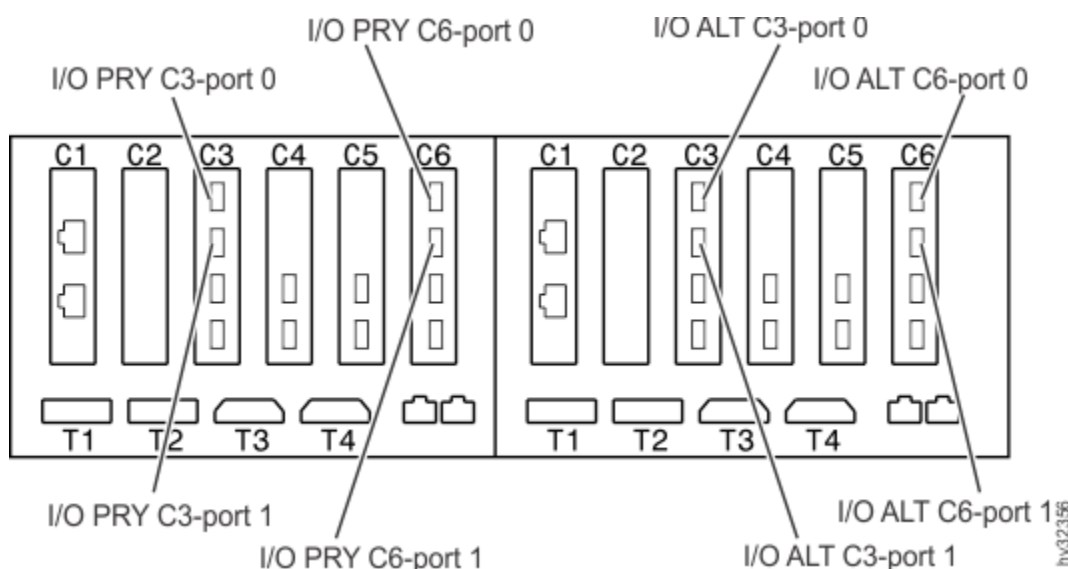


Figure 38. TS7700 I/O drawer FICON Cable Connections

When an additional FICON attachment (“FC 3402, 16 Gb SW FICON Adapter” on page 118, “FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118, “FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 118 or “FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 118) is installed on a TS7700, 2 more FICON cards are installed in primary and alternate drawers in slot C3, as shown in [Figure 38 on page 81](#) and listed on [Table 40 on page 81](#).

Table 40. 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.

Related information

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 41 on page 82 shows required definitions of subsystem IDs.

Table 41. Subsystem identification definitions				
Cluster	Vnode	Logical CU (Hex)	Cluster Logical Devices (Hex)	Subsystem ID/ LIBPORT-ID (Hex)†
0	0	0x00-0x1E	0x0000-0x01EF	0x01-0x1F
1	0	0x00-0x1E	0x0000-0x01EF	0x41-0x5F‡
2	0	0x00-0x1E	0x0000-0x01EF	0x81-0x9F‡
3	0	0x00-0x1E	0x0000-0x01EF	0xC1-0xDF‡
4	0	0x00-0x1E	0x0000-0x01EF	0x21-0x3F‡
5	0	0x00-0x1E	0x0000-0x01EF	0x61-0x7F‡
6	0	0x00-0x1E	0x0000-0x01EF	0xA1-0xBF‡
7	0	0x00-0x1E	0x0000-0x01EF	0xE1-0xFF‡
†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. Command set, responses to inquiries, and accepted parameters match the defined functional specifications of a 3490 drive.

Related information

[“Copy export overview” on page 112](#)

[“Allocation assistance” on page 233](#)

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.

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.

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.

The default configuration for a TS7700 Server from manufacturing 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. The default configuration for a TS7700 Server from manufacturing is two dual-ported PCIe 1 Gb Ethernet adapters. 10 Gb Ethernet adapters are available as well and are recommended for clusters using the cloud-attach or DS8K Object Store functions. 10 Gb connections improve data copy replication and cloud data transfer rates.

For a 3957-VEC, you can use either FC 1036, 1 Gb Grid dual port copper connection to add support for two 1 Gb copper (RJ-45) Ethernet adapters or FC 1038, 10 Gb dual port optical LW connection to add support for two 10 Gb optical longwave Ethernet adapters.

For a 3957-VED, you can use either FC 1039, 1 Gb Grid quad port copper connection to add support for two 1 Gb copper (RJ-45) Ethernet adapters or FC 1038, 10 Gb dual port optical LW connection to add support for two 10 Gb optical longwave Ethernet adapters.

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. 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
- PCF(Priority Control Flow) is not supported.
- 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.
- PCF(Priority Control Flow) is not supported.

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 copper (RJ-45) or 10 Gb Ethernet with longwave optical. For copper networks, Cat 5E or 6 Ethernet cabling can be used for the copper connections, but Cat 6 cabling is recommended to achieve the highest throughput.

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 10 Gb longwave 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 115](#)

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

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

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

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 condition:

- They are online.

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

Related information

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 42 on page 87 displays TCP/IP port assignments for the grid WAN.

Table 42. 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 42. 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 85](#)

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” on page 91](#)

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 or 25000 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 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 233](#)

[“Physical” on page 91](#)

[“Define virtual volume expiration time” on page 198](#)

Physical

Use this section to determine the number of physical volumes that are required to accommodate the workload you are planning for the TS7770 Tape Attach and 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” on page 91](#)
- [“Average compression ratio achieved per workload” on page 91](#)
- [“Average utilization rate of filling physical volumes” on page 91](#)
- [“Scratch physical volumes” on page 91](#)

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:

$$Px = (Da/Cr) / (Pc \times Ut/100)$$

Next, add in physical scratch counts and the Px results from all known workloads:

$$Pv = Ps + P1 + P2 + P3 + \dots$$

For example, by using the following assumptions:

Workload 1

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

$$P1 = (100/2) / (10 \times 67.5/100) = 8 \text{ physical volumes}$$

Workload 2

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

$$P2 = (150/2) / (7 \times 67.5/100) = 16 \text{ physical volumes}$$

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 TS7770 Tape Attach or the TS7760 Tape Attach:

$$Pv = Ps + P1 + P2 = 15 + 8 + 16 = 39 \text{ physical volumes}$$

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.

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” on page 94 through “9” on page 94 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

[“Feature details” on page 115](#)

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 99](#)

[“Feature details” on page 115](#)

[“TS7700 Cache thresholds and removal policies” on page 221](#)

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 99](#) 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.

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). 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 99](#)

[“Feature details” on page 115](#)

[“TS7700 Cache thresholds and removal policies” on page 221](#)

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:

- The final resulting grid configuration cannot have more than three different microcode levels. The microcode level is shown on the login screen.
- 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 99](#)

[“Feature details” on page 115](#)

[“TS7700 Cache thresholds and removal policies” on page 221](#)

TS7700 upgrade options

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

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

Capacity on Demand allows customers to enable disk capacity in 20 TB (FC 5262) and 100 TB (FC 5263) increments concurrently. See [“Capacity on Demand” on page 160](#).

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 121](#) 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, (to complement [“FC 9268, Plant installation of 100 MB/s throughput” on page 128](#) 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 121](#).

Note: All host data transfers through the TS7700 Cluster are considered for the data transfer limit regardless of which TS7700 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 121 to add this upgrade. For more information, see *Selective device access control* in the **Related information** section.

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 Logical Volumes”](#) on page 121 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-VEC when [“FC 1038, 10 Gb Quad Port Grid Optical LW Connection”](#) on page 116 is present.
- On a 3957-VED when [“FC 1039, 1Gb Grid Quad Port Copper Connection”](#) on page 116 or [“FC 1038, 10 Gb Quad Port Grid Optical LW Connection”](#) on page 116.

Use [“FC 1034, Enable Second Port Grid Connection”](#) on page 115 to achieve these upgrades.

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

TS7700 Expansion Frame

For F06, you can add a cache expansion frame to a fully configured TS7770 using [FC 7336, Encryption Capable Expansion Frame](#) with [FC 9336, 1st Exp Frame Attachment](#) and [FC 9337, 2nd Exp Frame Attachment](#).

For F07, you can add a cache expansion frame to a fully configured TS7770 using [FC 7338, Encryption Capable Expansion Frame](#) with [FC 9336, 1st Exp Frame Attachment](#) and [FC 9337, 2nd Exp Frame Attachment](#).

TS7700 Expansion Frame String (3956-CSB)

You can add an additional cache string to the first expansion frame that contains only one 3956-CSB string using [“FC 5666, Field Install 3956 CSB”](#) on page 124 and [“FC 5665, Field Install 3956 XSB”](#) on page 124. For upgrade requirements, configurations, and feature details, refer to the topics [“Upgrades for the TS7770”](#) on page 101 and [“Feature details”](#) on page 115 in the Related information section.

TS7700 Expansion Enclosures (3956-XSB)

You can add an additional cache enclosures to the Base Frame or first expansion frame using [“FC 5665, Field Install 3956 XSB”](#) on page 124. For upgrade requirements, configurations, and feature details, refer to the topics [Upgrades specific to the TS7770](#) 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 121, 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 [“TS7770 Disk encryption”](#) on page 109 for details and prerequisites.

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.

TS7770/TS7760 enable tape attach

For TS7770/TS7760 servers (VED/VEC hardware), use the following features to upgrade and enable the server to attach to a tape library:

- [“FC 5273, TS7770 Tape Attach” on page 121](#)
- [“FC 5274, Enable 1 TB Pending Tape Capacity” on page 121](#)

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

Ethernet adapters for grid communication

Longwave fibre Ethernet

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

For a 3957-VEC/VED use [“FC 1038, 10 Gb Quad Port Grid Optical LW Connection” on page 116](#) to achieve this upgrade.

Copper Ethernet

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

For a TS7700 Server (3957-VEC/VED) use [“FC 1039, 1Gb Grid Quad Port Copper Connection” on page 116](#) 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 Second Port Grid Connection” on page 115](#) to achieve this upgrade.

For a TS7760 Server (3957-VEC) [“FC 1036, 1 Gb grid dual port copper connection” on page 116](#) or [“FC 1038, 10 Gb Quad Port Grid Optical LW Connection” on page 116](#) is also required.

For a TS7770 Server (3957-VED) [“FC 1039, 1Gb Grid Quad Port Copper Connection” on page 116](#) or [“FC 1038, 10 Gb Quad Port Grid Optical LW Connection” on page 116](#) 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 116](#) to achieve this upgrade.

FC 5275 Additional virtual devices

Each instance of FC 5275, Additional virtual devices enables up to 16 additional virtual devices (virtual tape drives).

TS7700 Server FICON adapter installation

You can install a FICON adapter to connect a TS7700 Server (3957-VEC or 3957-VED) to a host system. FICON adapter conversion is non-concurrent when used with a 3957-VEC or 3957-VED. For 3957-VED use [“FC 3402, 16 Gb SW FICON Adapter” on page 118](#), or [“FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118](#), Enable FICON dual port.

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 TS7760 Server (3957-VEC) to a host system. FICON adapter conversion is non-concurrent. Use [“FC 3438, 8 Gb FICON Short Wavelength Attachment” on page 118](#), or [“FC 3439, 8 Gb FICON Long Wavelength Attachment” on page 118](#) to achieve this installation.

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 SW FICON Adapter” on page 118](#), or [“FC 3403, 16 Gb Long Wavelength FICON Adapter” on page 118](#) to achieve this installation.

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 120](#) to achieve this installation.

You can install two Fibre Channel interface cards in the TS7770 Server (3957-VED) to connect the TS7770 Server to the disk arrays in the TS7770 Storage Expansion Frame. Use [“FC 5243, Quad Port 16 Gb FC HBA” on page 120](#) to achieve this installation.

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 microcode level for the joining cluster must be equal to or later than the microcode level for any existing cluster.
- The final resulting grid configuration cannot have more than three different microcode levels.
- If FC 1035 is installed on the joining cluster, the existing infrastructure must support 10 Gbps grid communications for optimal performance.

Table 43 on page 99 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 43. Join rules						
	Joining	8.33.x.x	8.40.x.x	8.41.x.x	8.42.x.x	8.50.x.x
Existing cluster(s)	8.33.x.x	Y	Y	Y	Y	Y
	8.40.x.x	N	Y	Y	Y	Y
	8.41.x.x	N	N	Y	Y	Y
	8.42.x.x	N	N	N	Y	Y
	8.50.x.x	N	N	N	N	Y

GRID - Join and Merge Support

Table 44. Supported join and merge scenarios			
Type	Joining/merging cluster(s)	Existing clusters	Supported
Join	No cloud enabled	No cloud enabled	Yes
Join	Cloud enabled	No cloud enabled	Yes*
Join	No cloud enabled	Cloud enabled	Yes
Join	Cloud enabled	Cloud enabled	Yes*

Table 44. Supported join and merge scenarios (continued)

Type	Joining/merging cluster(s)	Existing clusters	Supported
Merge	No cloud enabled	No cloud enabled	Yes
Merge	Cloud enabled	No cloud enabled	Yes
Merge	No cloud enabled	Cloud enabled	Yes
Merge	Cloud enabled	Cloud enabled	Yes**

* Only supported if the joining cluster does not have any configured cloud pools, cloud accounts, containers, or URLs.

** Only supported if the resulting grid contains no more than one cloud pool and no more than 256 items for each of the following: cloud accounts, containers, cloud URLs, and cluster associations.

Whether performing a join or a merge, it is important to note that the actual data does not get copied from one cluster to another. This process creates place holders for all of the logical volumes in the final grid. When joining to an existing grid or merging with an existing grid, the process is initiated to a single cluster in the grid and the information is populated to all members of the grid.



Attention:

- If a join or merge does not complete successfully, it is not sufficient to just clear the online block and return the system to the customer. It is not sufficient to just verify that the VPD has been updated. Contact support for directions on how to continue.
- If a join or merge results in a grid that is greater than six clusters, run VTD_EXE.271 for microcode levels earlier than 8.41.x.x so that the entire grid is viable.

To achieve any of the following upgrades, you must order [“FC 4015, Grid Enablement” on page 119](#) against the TS7700 Server.

Note: An RPQ is required for any intended 7- 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 202](#)

[“FC 4015, Grid Enablement” on page 119](#)

Upgrades for the TS7770

This section describes the use of miscellaneous equipment specifications (MES) to upgrade the TS7770.

TS7770 Cloud attach

The TS7770 attached to cloud supports both the largest and smallest TS7700 users to deploy TS7700 in new use cases, such as; archival of massive data stores, and supporting DR without a grid presence (TS7770 stand-alone) or TS7760 in a GRID. TS7760 Tier to Cloud supports Amazon S3 and IBM COS S3.

The functionality is enabled by FC 5278, Enable Cloud Storage Tier. Each instance of FC 5279, 5 TB Active Premigration Queue enables an additional 5TB of data in the active premigration queues for tape and cloud data.

TS7770 Tape Attach

The TS7770 can be attached to the TS3500 Tape Library or TS4500 Tape Library.

This functionality is enabled by [“FC 5273, TS7770 Tape Attach” on page 121](#).

Addition of cache drawers

Additional enclosures can be added using FC 5665 (Field Install 3956-XSB Cache Enclosures) for a maximum of nine 3956-XSB drawers to a TS7770 Base frame. At least one instance of FC 5274, 1 TB Active Premigration Queue, must be ordered, up to a maximum of 10, to increase the amount of data that is pending migration. Once ten FC 5274 have been ordered, up to an additional ten FC 5279, 5 TB Active Premigration Queue, can be ordered.

You can use FC 7336, TS7770 Encryption-capable expansion frame as an MES to add up to two expansion frames to a fully configured TS7770 cache subsystem operating with a 3956-CSB controller. Each FC 7336, TS7770 Encryption-capable expansion frame contains one or two cache controllers. Up to nine additional cache drawers can be added to each controller.

Related information

[“System requirements” on page 54](#)

[“TS7700 feature codes” on page 115](#)

Upgrades for the TS7760

This section describes the use of miscellaneous equipment specifications (MES) to upgrade the TS7760.

TS7760 Cloud attach

The TS7760 attached to cloud supports both the largest and smallest TS7700 users to deploy TS7700 in new use cases, such as; archival of massive data stores, and supporting DR without a grid presence (TS7760 stand-alone) or TS7760 in a GRID. TS7760 Tier to Cloud supports Amazon S3 and IBM COS S3.

The functionality is enabled by FC 5278, Enable Cloud Storage Tier. Each instance of FC 5279, 5 TB Active Premigration Queue enables an additional 5TB of data in the active premigration queues for tape and cloud data.

TS7760 Tape Attach

The TS7760 can be attached to the TS3500 Tape Library or TS4500 Tape Library.

This functionality is enabled by “FC 5273, TS7770 Tape Attach” on page 121. 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, 1 TB Active Premigration Queue 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.

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.

Related information

[“System requirements” on page 54](#)

[“TS7700 feature codes” on page 115](#)

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 TS7770 Tape Attach and the TS7760 Tape Attach models.

Related information

[“System requirements” on page 54](#)

[“TS7700 feature codes” on page 115](#)

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), the IBM Security Key Lifecycle Manager (ISKLM), or the IBM Guardium Key Lifecycle Manager (GKLM) 4.1 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 105](#) 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 105](#).

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 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), ISKLM (IBM Security Key Lifecycle Manager for z/OS), or Guardium Key Lifecycle Manager (GKLM) 4.1 is installed and configured on the network.
- Key-encrypting keys (KEKs) are defined.
- The license key for “FC 9900, Tape Encryption Tape” on page 130 is installed and activated.

No new host software is required.

Verify correct license keys 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 39 on page 104. Verify that FC 9900, Tape Encryption configuration, displays on this table.

Currently activated feature licenses:

Select	Feature Code	Feature Description	License Key	Node	Node Serial Number	Activated	Expires
☐	5267	1 TB Cache Enablement	a7e6176d54267d7a	"yourNode" (x0) Node	7B-68721	Tuesday, March 13, 2007 1:12:45 AM	Never
☐	5267	1 TB Cache Enablement	a7e6176d54267d7b	"yourNode" (x0) Node	7B-68721	Tuesday, March 13, 2007 1:12:46 AM	Never
☐	5267	1 TB Cache Enablement	a7e6176d54267d7c	"yourNode" (x0) Node	7B-68721	Tuesday, March 13, 2007 1:12:46 AM	Never
☐	5267	1 TB Cache Enablement	a7e6176d54267d7d	"yourNode" (x0) Node	7B-68721	Tuesday, March 13, 2007 1:12:46 AM	Never
☐	9900	Encryption Configuration	a7e6176d54267d7e	"yourNode" (x0) Node	7B-68721	Tuesday, April 10, 2007 10:33:08 AM	Never
☐	5267	1 TB Cache Enablement	a7e6176d54267d7f	"yourNode" (x0) Node	7B-68721	Monday, July 9, 2007 11:14:20 PM	Never
☐	5267	1 TB Cache Enablement	a7e6176d54267d80	"yourNode" (x0) Node	7B-68721	Thursday, August 9, 2007 1:02:00 AM	Never
☐	5268	100 MB/s Increment	a7e6176d54267d81	"yourNode" (x0) Node	7B-68721	Tuesday, March 13, 2007 1:12:40 AM	Never
☐	5268	100 MB/s Increment	a7e6176d54267d82	"yourNode" (x0) Node	7B-68721	Tuesday, March 13, 2007 1:12:41 AM	Never
☐	5268	100 MB/s Increment	a7e6176d54267d83	"yourNode" (x0) Node	7B-68721	Tuesday, March 13, 2007 1:12:42 AM	Never

Page 1 of 2 1 Go Total: 13 Filtered: 13 Displayed: 10

Figure 39. 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*

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.

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 Tape”](#) on page 130.

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

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”](#) on page 105.
 - **No**, order [“FC 9900, Tape Encryption Tape”](#) on page 130 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 107

[FC 9900, Encryption configuration](#)

[“Managing tape encryption”](#) on page 105

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 107.) 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 40](#) on page 106.

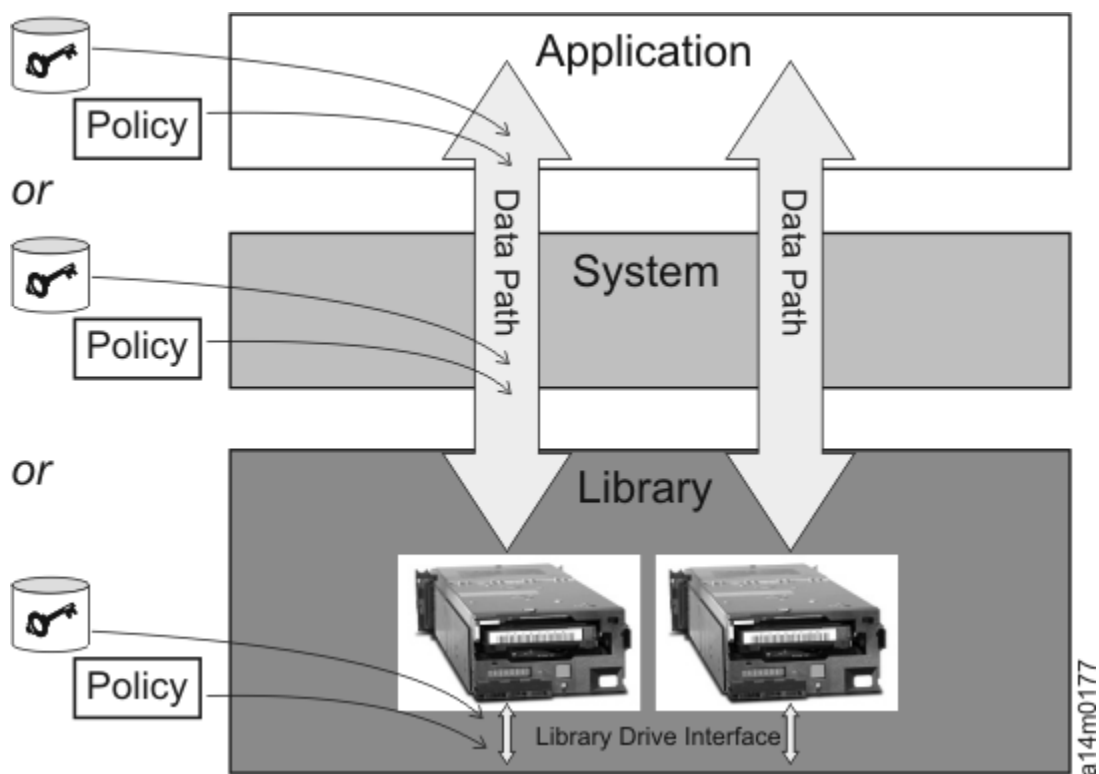


Figure 40. Three possible locations for encryption policy engine and key management.

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 104](#)

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 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 41 on page 108](#) illustrates the symmetric and asymmetric processes.

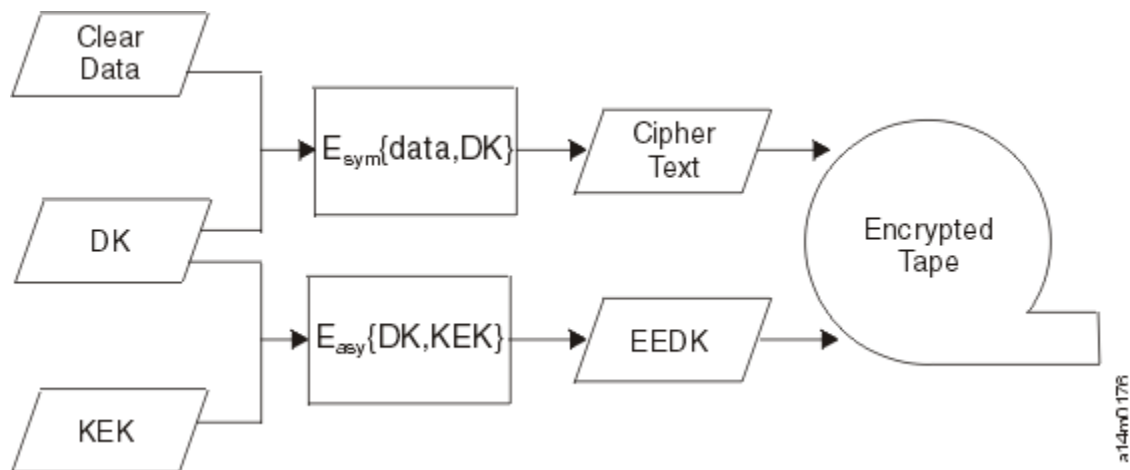


Figure 41. An encryption key server uses both symmetric and asymmetric encryption keys

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 Secure Key Lifecycle Manager (SKLM) server.

External encryption key management removes the responsibility of managing the key from the disk subsystem controllers. The key is stored in volatile memory inside the controllers. This means that if the 3956-CSA or 3956-CSB controller is powered off and powered back on, the controller must obtain the security key from the SKLM server again. The 3956-CSA or 3956-CSB controller does not connect directly to the SKLM server. The 3956-CSA or 3956-CSB controller connects to the SKLM server through a proxy server. The proxy server is provided by the 3057-VEC or 3957-VED. The proxy server requests keys to

the SKLM servers on behalf of the 3956-CSA or 3956-CSB controllers. The keys are then given to the 3956-CSA or 3956-CSB 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-CSA or 3956-CSB and the SKLM server using the proxy server.

Related information

[“Physical” on page 91](#)

[“Enabling tape encryption” on page 104](#)

[“Managing tape encryption” on page 105](#)

TS7770 Disk encryption

You can encrypt the disk drive modules (DDMs) within a TS7700 disk storage system.

Prerequisites

Disk encryption is available on a new order from manufacturing that ordered either “FC 5272, Disk Enabled Encryption” on page 121 or “FC 5276, Disk encrypt - External key manager” on page 122. An order of FC 5272 or FC 5276 come with “FC 7405, Encryption CFC/CSB (USB Flash Drives (Four Pack))” on page 126 which provides four USB sticks. The following condition must also be met:

- 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 encrypted. All strings in the cluster must be encrypted.

All TS7770 configurations with 3956-CSB/XSB cache that have any encryption type that is enabled is ALWAYS shipped with local key management enabled (FC 5272). This encrypts the data in the CSB processor and places that encrypted data onto regular disk drives.

The local encryption (FC 5272 Disk Enabled Encryption) is configured during the TS7770 initial installation by the service person.

- FC 5272 Disk Enabled Encryption is not available for field Install on the TS7770 and needs to be shipped from manufacturing for any Encryption.
- FC 7405 must be ordered on every 3956-CSB in the TS7770 configuration.
- FC 7405 provides four USBs sticks per 3956-CSB used to store the local encryption keys.

Note: If external key management is later enabled, these USB sticks are no longer needed.

The External Key Encryption ([FC 5276](#)) must have [FC 5272](#) installed on the TS7770 server before initial installation.

- All TS7700 configurations with any encryption type enabled is ALWAYS shipped with local key management enabled first
- Once a TS7770 with FC 5272 is configured in a customer environment and able to communicate with an external key server, then FC 5276 can be activated to transition to external key management..

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.

You can manage the encryption key for the cache disk drive modules (DDMs) externally.

For external key management of encryption, the encryption must be enabled onsite by an IBM service representative.

The encryption key server is installed and configured on the network.

- Supported on TS7700 with 8.51.1.xx microcode:
 - IBM Guardium Key Lifecycle Manager (GKLM) 4.1
- Supported on TS7770 with 8.50.0.xx microcode:
 - IBM Security Key Lifecycle Manager (SKLM)
- Supported on TS7760 with 8.4x.x.xx microcode and higher levels:
 - IBM Security Key Lifecycle Manager (SKLM)

The following functions are addressed:

- Enable the Feature Keys for Local Encryption (not for TS7770)
- Enable the Feature Keys for External Key management.
- Configure external key encryption (from SMIT only)
- Switch from internal key management to external key management (from SMIT only)
- Rekey (from SMIT and Management Interface)

TS7770

All TS7770 configurations with 3956-CSB/XSB cache that have any encryption type enabled is ALWAYS shipped with local key management enabled (FC 5272).

The local encryption (#5272 Disk Enabled Encryption) is configured during the TS7770 initial installation by the service person.

- Feature #5272 Disk Enabled Encryption is not available for field Install on the TS7770 and needs to be shipped from manufacturing for any Encryption.
- Feature #7405 must be ordered on every 3956-CSB in the TS7770 configuration.
- Feature #7405 provides four USBs sticks per 3956-CSB used to store the local encryption keys.

Note: If external key management is later enabled, these USB sticks are no longer needed.

The External Key Encryption (#5276) must have Feature codes #5272 installed on the TS7770 server before initial installation.

- All TS7700 configurations with any encryption type enabled is ALWAYS shipped with local key management enabled first.
- Once a TS7770 with feature #5272 is configured in a customer environment and able to communicate with an external key server, then feature #5276 can be activated to transition to external key management.

TS7760 with 8.4x.x.xx microcode and higher levels

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 126](#), Encryption or as an MES that uses [“FC 5272, Disk Enabled Encryption” on page 121](#). The following conditions must also be met:

- 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

Configuring IBM Security Key Lifecycle Manager key servers

Steps to configuring IBM Security Key Lifecycle Manager key servers.

IBM Security Key Lifecycle Manager key servers support Key Management Interoperability Protocol (KMIP), which is a standard for encryption of stored data and management of cryptographic keys.

The system supports different types of key server configurations on IBM Security Key Lifecycle Manager. The following configurations are supported:

- One primary (master) key server and several secondary key servers: IBM Security Key Lifecycle Manager key servers designate one master or primary key server, which can have up to three secondary key servers (also known as clones) defined. These additional key servers support more paths when it delivers keys to the system; however, during rekeying only the path to the primary key server is used. When the system is rekeyed, secondary key servers are unavailable until the primary key server replicates the new keys to these secondary key servers. The amount of time it takes to replicate the key to a secondary key server depends on the amount of key and certificate information that is being replicated. Each replication to a secondary key server can take some time. Replication must complete before keys can be used on the system. You can either schedule automatic replication or complete it manually with IBM Security Key Lifecycle Manager. During replication, key servers are not available to distribute keys or accept new keys. The total time that it takes for a replication to complete on the IBM Security Key Lifecycle Manager depends on the number of key servers that are configured as clones. If replication is triggered manually, the IBM Security Key Lifecycle Manager issues a completion message when the replication completes. Verify that all key servers contain replicated key and certificate information before keys are used on the system.
- Multiple master key servers: Key servers can be configured in a multi-master configuration where each key server has the ability to create new encryption keys. In this instance, any server can be set as the primary key server. The primary key server is the key server that the system uses when you create any new key server encryption keys. If multi-master mode is enabled on the IBM Security Key Lifecycle Manager, the key is immediately replicated to the other key servers in the configuration.

Ensure that you complete the following tasks on the IBM Security Key Lifecycle Manager before you enable encryption:

1. Define the IBM Security Key Lifecycle Manager to use Transport Layer Security version 1.2 (TLSv1.2). The default setting on IBM Security Key Lifecycle Manager is TLSv1, but the system supports only version 1.2. On the IBM Security Key Lifecycle Manager, set the value to SSL_TLSv2, which is a set of protocols that includes TLSv1.2.
2. Ensure that the database service is started automatically on startup.
3. Ensure that a valid SSL certificate from IBM Security Key Lifecycle Manager is installed on the system and in use. If automatic replication is configured on IBM Security Key Lifecycle Manager, then this certificate needs to be uploaded to the system once. However, if automatic replication is not configured on the IBM Security Key Lifecycle Manager, a certificate for each stand-alone key server must be uploaded to the system.
4. Specify the SPECTRUM_VIRT device group for the system definition. If you are configuring multiple key servers, the SPECTRUM_VIRT device group must be defined on the primary and all secondary key servers.
5. If you currently have encryption enabled with USB flash drives, at least one of the USB flash drives must be inserted into the system before key servers can be configured for managing keys.

For more information about completing these tasks, see the IBM Documentation for IBM Security Key Lifecycle Manager. When you create key server objects on the system for IBM Security Key Lifecycle Manager key servers, you must create a device group, in addition to name, IP address, port and certificate information. The device group is a collection of security credentials (including keys and groups of keys) that allows for restricted management of subsets of devices within a larger pool. The system must be defined on the key server to the SPECTRUM_VIRT device group if you are using the default settings. If the SPECTRUM_VIRT device group does not exist on the key server, it must be created based on the GPFS

device family. If you are configuring multiple key servers, the SPECTRUM_VIRT device group must be defined on the primary and all additional key servers.

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 216](#)

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 216](#)

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.

Related information

[“Logical WORM” on page 216](#)

TS4500 support

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 44](#)

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 TS7760 3957-VEC or TS7770 3957-VED tape attach
- from a TS7740 3957-V07 to a TS7760 3957-VEC or TS7770 3957-VED tape attach
- from a TS7720 3957-VEB tape attach to a TS7760 3957-VEC or TS7770 3957-VED tape attach
- from a TS7760 3957-VEC tape attach to a TS7770 3957-VED tape attach

Note: Frame replacement migration is only done on a TS7760, 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 4](#)

TS7700 feature codes

This topic links to descriptions of TS7700 features according to component, feature code, and feature conversion (if applicable).

Feature details

This topic describes feature codes for the TS7700.

FC 0201, 9 Micron LC/LC 31 Meter

This feature provides one 31 meter (101 ft.) 9 micron single mode fibre cable with LC Duplex connectors on both ends, for connection between the Long Wavelength FICON Channel feature and a host system or fibre component long wavelength channel with a 9 micron fibre cable LC Duplex adapter.

Refer to [FC 0201](#) in [Table 45 on page 133](#) for requirements and other information.

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

This feature provides one 31 meter (101 ft.) 50 micron multimode fibre cable with LC Duplex connectors on both ends, for connection between the Short Wavelength FICON Channel feature and a host system or fibre component short wavelength channel with a 50 micron fibre cable LC Duplex adapter.

Refer to [FC 0203](#) in [Table 45 on page 133](#) for requirements and other information.

FC 0983, TAA Compliance

FC 0983, TAA Compliance, indicates that the product is TAA compliant. This feature specifies the machine shipment is to comply with the U.S. Trade Agreements Act for USA orders only.

Refer to [FC 0983](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1034, Enable Second Port Grid Connection

This feature enables the second port of the quad port 1Gb, or dual port 10 Gb Grid Connection adapters provided by #1036, #1037, #1038 or #1039. **(#1041 will go out with Phase II RFA)**

Refer to [FC 1034](#) in [Table 45 on page 133](#) 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, 1Gb grid dual port copper connection in [Table 45 on page 133](#) for requirements and other information.

FC 1038, 10 Gb Quad Port Grid Optical LW Connection

This feature 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.

Refer to [FC 1038](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1039, 1Gb Grid Quad Port Copper Connection

This feature provides a quad port 1-Gbps 10/100/1000Base-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. This adapter conforms to the IEEE 802.3ab 1000Base-T standard. It supports distances of up to 100 meters using four pairs of Cat6 balanced copper cabling.

Customer supplied Cat6 cables must be used with the adapter when Grid Enablement (#4015) is installed.

Refer to [FC 1039](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1041, 10 Gb Dual Port Grid Optical LW Connection

This feature provides a dual port 10 Gbps Ethernet longwave adapter for Grid Communication between TS7700s and replaces #1038. The 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. The adapter supports up to 10 km distance.

Note:

- This adapter cannot negotiate down to run at 1 Gb.
- This adapter is only for TS7770 installations and is not supported in TS7760.

Refer to [1041](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1776, US RoHS Indicator

The state of Wisconsin requires RoHS compliant equipment. This feature will be selected as needed in the configurator for equipment that will be shipped to or used in Wisconsin.

Refer to [FC 1776](#) in [Table 45 on page 133](#) 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](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1904, Switching PDU (For 3952-F07)

This feature provides power switching to allow true power redundancy.

Refer to [FC 1904](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1904, Switching PDU (For 3957-VED)

This feature provides power switching to allow true power redundancy.

Refer to [FC 1904](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1912, Single Phase Power Distribution Unit (For 3952-F07)

This feature provides two single phase 10 outlet PDUs to allow connection to independent branch power circuits.

Refer to [FC 1912](#) in [Table 45 on page 133](#) for requirements and other information.

FC 1912, Single Phase Power Distribution Unit

This feature provides two single phase 10 outlet PDUs to allow connection to independent branch power circuits.

Refer to [FC 1912](#) in [Table 45 on page 133](#) 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](#) in [Table 45 on page 133](#) for requirements and other information.

FC 2715, Console attachment

FC 2715, Console attachment, provides a cable to attach to a TS3000 System Console.

Refer to [FC 2715, Console attachment](#) in [Table 45 on page 133](#) for requirements and other information.

FC 2725 Rack Mount TS3000 System Console

This feature 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 (features #2722, #2724, #2730, or #2732).

Refer to [FC 2725](#) in [Table 45 on page 133](#) for requirements and other information.

FC 2725 Rack Mount TS3000 System Console (For 3952-F07)

This feature provides the enhanced rack-mountable TSSC 1U server and an ethernet cable for connection to the rack mount switch

Refer to [FC 2725](#) in [Table 45 on page 133](#) 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](#) in [Table 45 on page 133](#) for requirements and other information.

FC 2748, Optical drive (For 3952-F07)

This feature provides the optical drive.

Refer to [FC 2748](#) in [Table 45 on page 133](#) for requirements and other information.

FC 3401, Enable FICON second port

FC 3401, Enable FICON second port, enables the second port on each installed FICON adapter.

Refer to [FC 3401](#), Enable FICON dual port 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 SW FICON Adapter

This feature 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.

Refer to [FC 3402](#) in [Table 45 on page 133](#) for requirements and other information.

FC 3403, 16 Gb Long Wavelength FICON Adapter

This feature 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 1](#) 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

Refer to [FC 3438, 8 Gb FICON Short Wavelength Attachment](#) in [Table 45 on page 133](#) 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.

Note: This feature is not supported in TS7770.

Refer to [FC 3439, 8 Gb FICON Long Wavelength Attachment](#) in [Table 45 on page 133](#) for requirements and other information.

FC 3466, 32 GB memory upgrade

FC 3466, 32 GB memory upgrade, provides an additional 32 GB RAM to the TS7700 Server.

Refer to [FC 3466, 32 GB memory upgrade](#) for requirements and other information.

FC 4015, Grid Enablement

This feature delivers a key to enable the communication function that would allow communication with other TS7700s in a Grid configuration. A path to each TS7700 must be enabled on one of the G Nodes. Each TS7700 in a Grid must enable communication with other TS7700s in the configuration.

Refer to [FC 4015](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4016, Remove Cluster from Grid

This feature delivers instructions for a one time process to remove a cluster from a Grid. This is required before a Cluster Cleanup can be performed on any cluster which is configured to participate in a Grid. If this cluster is returned to service after the cleanup is performed, and it joins a Grid, another instance of #4016 is required if the cluster will be removed from the new Grid.

Refer to [FC 4016](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4017, Cluster Cleanup

This feature facilitates a one-time Cluster Cleanup, to clean the database, delete logical volumes from the Tape Volume Cache, and removing configuration data for host connections from a TS7700 cluster. Before the cleanup can occur, a cluster with #4015, Grid Enable, must be removed from the Grid using #4016. If another cleanup is required on this cluster, another instance of #4017 is required.

Refer to [FC 4017](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4643, Rack Mount Kit VED with CSB

The Rack Mount kit delivers the mounting hardware, required to install the TS7700 Server in a customer provided 19" rack.

Refer to [FC 4643](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4647, Rack Mount Kit CSB

The Rack Mount kit delivers the mounting hardware and cables required to install the TS7700 Cache Controller in a customer provided 19" rack along with a rack mounted TS7700 Server.

Refer to [FC 4647](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4648, Rack Mount Kit XSB

The Rack Mount kit delivers the mounting hardware and cables required to install the TS7700 Cache Controller in a customer provided 19" rack along with a rack mounted TS7700 Server.

Refer to [FC 4648](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4649, Rack Mount Kit VED with CFC

The Rack Mount kit delivers the mounting hardware required to install the TS7700 Server in a customer provided 19" rack.

Refer to [FC 4649](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4698, Initial Order XFC Customer Rack

This feature allows the initial order of a TS7700 Cache Module into a customer installed Rack. This feature must be ordered on the 3957 VED and the Rack Install feature #4651 must appear on the 3956 model XFC TS7700 Cache Module order.

Refer to [FC 4698](#) in [Table 45 on page 133](#) for requirements and other information.

FC 4699, Field Order XFC for Customer Rack

This feature allows the Field installation of a TS7700 Cache Module into a customer installed Rack. This feature must be ordered on the 3957 VED and the Field Merge feature #9355 must appear on the 3956 model XFC TS7700 Cache Module order.

Refer to [FC 4699](#) in [Table 45 on page 133](#) 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 45 on page 133](#) 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 45 on page 133](#) 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 1](#) for requirements and other information.

FC 5243, Quad Port 16 Gb FC HBA

This feature delivers two quad-ported 16 Gb Fibre Channel HBAs and associated cables. These HBAs connect to the TS7700 #7338 Expansion frame.

Refer to [FC 5243](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5262, 20 TB cache enablement

This feature enables a 20 TB increment of disk cache to store user data. Feature Type: Chargeable.

Refer to [“Capacity on Demand” on page 160](#) for table showing 20TB and then 100 TB increments.

Refer to [FC 5262](#) in [Table 45 on page 133](#) for requirements and other information.

Note: The capacity on demand is related to physical cache size. It is not related to compression.

FC 5263, 100TB cache enablement

This feature enables a 100TB increment of disk cache to store user data.

Refer to [“Capacity on Demand” on page 160](#) for table showing 20TB and then 100 TB increments.

Refer to [FC 5263](#) in [Table 45 on page 133](#) for requirements and other information.

Note: The capacity on demand is related to physical cache size. It is not related to compression.

FC 5268, 100 MB/sec Increment

This feature 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 Virtualization Engine will perform at that data throughput level.

Refer to [FC 5268](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC 5270, Increased Logical Volumes

Each instance of this feature increases the number of logical volumes supported by 200,000. Up to one million Logical Volumes are supported by default. Up to four million Logical Volumes are supported with the maximum quantity of fifteen feature #5270 installed.

Note: In a Grid configuration, feature #5270 must be installed on every cluster in the Grid to increase the number of supported logical volumes in that Grid. The number of logical volumes supported in a Grid is set by the cluster with the smallest number of feature #5270 increments installed.

Refer to [FC 5270](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC 5271, Selective Device Access Control

This feature 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.

Note: In a Grid configuration, feature #5271 must be installed on every cluster in the Grid before any Selective Device Access Control policies can be defined in that Grid.

Refer to [FC 5271](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC 5272, Disk Enabled Encryption

This feature delivers the product license key required to enable disk-based encryption.

Note: For TS7770, Feature #5272 Disk Enabled Encryption is not available for field Install on the TS7770 and needs to be shipped from manufacturing with the Feature code already installed.

Refer to [FC 5272](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC 5273, TS7770 Tape Attach

Enable this TS7760 or TS7770 to be connected to a TS3500 or TS4500 Tape Library with Machine Type 3952 tape drives dedicated to the TS7700.

Refer to [FC 5273](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC 5274, Enable 1 TB Pending Tape Capacity

Each instance of feature 5274 enables 1 TB of data in the active pre-migration queue for back-end tape or cloud data.

Refer to [FC 5274](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC 5275, Additional virtual devices

Each instance of feature 5275 enables up to 16 additional virtual devices (virtual tape drives).

Note: Installation of those feature requires SMIT (the system management interface tool). For more information contact your IBM Service Representative.

Refer to [FC 5275](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC 5276, Disk encrypt - External key manager

This feature delivers the product license key required to enable disk-based encryption using keys managed by an external key manager.

Note:

1. All TS7770 configurations with any encryption type enabled will ALWAYS ship with local key management enabled first.
2. Once a TS7770 with feature #5272 is configured in a customer environment and able to communicate with an external key server, then feature #5276 can be activated to transition to external key management.

Refer to [FC 5276](#) in [Table 45 on page 133](#) 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 45 on page 133](#) for requirements and other information.

FC 5278, Enable Cloud Storage Tier

Enables transparent cloud tiering for cloud storage behind TS7700.

Refer to [FC 5278](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5279, 5 TB Active Pre-Migration Queue

Each instance of feature 5279 enables 5 TB of data in the active pre-migration queues for back-end tape or cloud data.

Refer to [FC 5279](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5281, Secure Data Transfer

FC 5281 (SDT) is required on any cluster sending or receiving encrypted data across a grid link.

Refer to [FC 5281](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5282, DS8000 Object Store

This feature allows the TS7700 to store Objects from DS8000.

Refer to [FC_5282](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5512, TS3000 Ssystem Console KVM display, Keyboard, mouse

FC 5283, DS8000 Object Store Grid Policy Management

This feature provides grid-wide object management including grid awareness of objects and grid replication.

Refer to [FC 5283](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5512, KVM

This feature provides the KVM Display, Keyboard, Mouse and mounting hardware to be plant installed in the frame or delivered for installation in a rack.

Refer to [FC 5512](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5512, KVM (For 3952-F07)

This feature provides the KVM Display, Keyboard, Mouse and mounting hardware to be plant installed in the frame or delivered for installation in a rack.

Refer to [FC 5512 in Table 45 on page 133](#) 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 45 on page 133](#) for requirements and other information.

FC 5631, Install 3957 VED

This feature indicates a TS7700 Server will be installed into this 3952 Tape Frame. This feature must appear on the 3952 Tape Frame order, and the Plant Install feature #9350 must appear on the TS7700 Server order.

Refer to [FC 5631 in Table 45 on page 133](#) 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 45 on page 133](#) 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 45 on page 133](#) 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 45 on page 133](#) 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 45 on page 133](#) 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 45 on page 133](#) 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 45 on page 133](#) for requirements and other information.

FC 5663, Plant Install 3956 CSB

This feature allows the factory installation of a TS7700 Cache Controller Model CSB into a new 3952 Tape Frame coming from the plant. This feature must appear on the 3952 Tape Frame order, and the Plant Install a 3956 Cache Controller feature #9352 must appear on the TS7700 Cache Controller Model CSB order.

Refer to [FC 5663](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5664, Plant Install 3956 XSB

This feature allows the factory installation of a TS7700 Cache Module model XSB into a new 3952 Tape Frame coming from the plant. This feature must appear on the 3952 Tape Frame order, and the Plant Install a 3956 Cache Module feature #9354 must appear on the TS7700 Cache Module order.

Refer to [FC 5664](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5665, Field Install 3956 XSB

This feature allows the field installation of a TS7700 Cache Module into a customer installed 3952 Tape Frame. This feature must be ordered on the 3952 Tape Frame and the Field Merge a 3956 Cache Module feature #9355 must appear on the TS7700 Cache Module order.

Refer to [FC 5665](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5666, Field Install 3956 CSB

This feature allows the field installation of a TS7700 Cache Controller Model CSB into a customer installed 3952 Tape Frame. This feature must be ordered on the 3952 Tape Frame and the Field Merge a 3956 Cache Controller feature #9353 must appear on the TS7700 Cache Module order.

Refer to [FC 5666](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5667, Plant Install 3956 CFC

This feature allows the factory installation of a TS7700 SSD Cache Controller Model CFC into a new 3952 Tape Frame F07 coming from the plant. This feature must appear on the 3952 Tape Frame order, and the Plant Install a 3956 Cache Controller feature #9352 must appear on the TS7700 Cache Controller Model CFC order. Feature type: Chargeable.

Refer to [5667](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5668, Plant Install 3956 XFC

This feature allows the factory installation of a TS7700 3956-XFC SSD Cache Module into a new 3952-F07 Tape Frame coming from the plant. This feature must appear on the 3952-F07 Tape Frame order, and the Plant Install a 3956-XFC SSD Cache Module feature #9354 must appear on the TS7700 Cache Module order. Feature type: Chargeable.

Refer to [5668](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5669, Field Install 3956 XFC

This feature allows the field installation of a TS7700 3956-XFC SSD Cache Module into a customer installed 3952 Tape Frame. This feature must be ordered on the 3952-F07 Tape Frame and the Field Merge a 3956-XFC SSD Cache Module feature #9355 must appear on the TS7700 Cache Module order. Feature type: Chargeable.

Refer to [5669](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5756, Integrated Control Path (3956-XSB)

This feature 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 5756](#) in [Table 45 on page 133](#) for requirements and other information.

FC 5756, Integrated Control Path (3956-XFC)

This feature provides two Ethernet switches and cables to manage the network to the internal TS7700 drawer components.

Refer to [FC 5756](#) in [Table 45 on page 133](#) 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 45 on page 133](#) for requirements and other information.

FC 5904, Remote Code Load Exception

This feature indicates that the customer requires someone to physically go to the datacenter to do a code load upgrade. This feature has a price and IBM reserves the right to modify the machine records associated with features 5904 and 9904, based on the actual method used to update the code on the customer's unit. Each system requires one of features 5904 or 9904 to be included.

Refer to [FC 5904](#) in [Table 45 on page 133](#) 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 45 on page 133](#) 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 TS7760.

Refer to [FC 7333, TS7700 Encryption-capable base frame](#) in for requirements and other information.

FC 7334, TS7760 Encryption Capable Expansion Frame (VEC section below)

This feature identifies this 3952 Tape Frame as the expansion frame for a TS7760 encryption-capable configuration.

- Up to two #7334 expansion frames may be attached to the #7333 TS7700 Encryption Capable Base Frame.

Refer to [FC 7334](#) in [Table 45 on page 133](#) for requirements and other information.

FC 7335 TS7770 Encryption Capable Base Frame

This feature designates the 3952 F06 Tape Frame for use as a TS7770 Encryption-Capable Base Frame.

Refer to [FC 7335](#) in [Table 45 on page 133](#) for requirements and other information.

FC 7336, TS7700 Encryption Capable Expansion Frame

This feature identifies this 3952 Tape Frame as the expansion frame for a TS7770 encryption-capable configuration. Up to two #7336 expansion frames may be attached to the #7335 or #7337 TS7770 Encryption Capable Base Frame.

Refer to [FC 7336](#) in [Table 45 on page 133](#) for requirements and other information.

FC 7337 TS7770 Encryption Capable Base Frame

This feature designates the 3952 F07 Tape Frame for use as a TS7770 Encryption-Capable Base Frame.

Refer to [FC 7337](#) in [Table 45 on page 133](#) for requirements and other information.

FC 7338, Encryption Capable Expansion Frame

This feature identifies this 3952 Tape Frame as the expansion frame for a TS7770 encryption-capable configuration. Up to two #7338 expansion frames may be attached to the #7335 or #7337 TS7770 Encryption Capable Base Frame.

Refer to [FC 7338](#) in [Table 45 on page 133](#) for requirements and other information.

FC 7339, TS7700 Encryption Capable Base Frame (F07)

This feature designates the Tape Frame for use as an SSD TS7700 encryption-capable frame. It should be used when one 3956-CFC and up to one 3956-XFC are used.

Refer to [FC 7339](#) in [Table 45 on page 133](#) 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](#) in [Table 45 on page 133](#) for requirements and other information.

FC 7405, Encryption CFC/CSB (USB Flash Drives (Four Pack))

. This feature must be ordered on every 3956-CFC (for CFC) or 3956-CSB (for CSB) in the TS7770 configuration. It provides four USBs sticks per 3956-CFC (for CFC) or 3956-CSB (for CSB) to store the

local encryption keys. If external key management is enabled later on, then these USB sticks are no longer needed.

Refer to [FC 7405](#) in [Table 45 on page 133](#) for requirements and other information.

FC 8080, 600GB HDDs in VED

This feature specifies this device will be fully loaded with six 600GB HDDs.

Refer to [FC 8080](#) in [Table 45 on page 133](#) for requirements and other information.

FC 8081, 775GB SSDs in VED

This feature specifies this device will be fully loaded with six 775GB SSDs.

Refer to [FC 8081](#) in [Table 45 on page 133](#) for requirements and other information.

FC 8083, 3.84TB SSDs in VED

This feature allows the field or plant installation of 2 x 3.84TB SSDs into empty slots of new or existing VED. It is not available for VEC. This feature must be ordered when ordering FC 5283. This feature specifies the option to add 2 x 3.84TB BSDs. Feature type: Chargeable.

Refer to [8083](#) in [Table 45 on page 133](#) 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

Refer to FC 9000, Mainframe attachment in [Table 45 on page 133](#) for requirements and other information.

FC 9217 Attach to TS7700

FC 9217 Attach to TS7700, indicates that a TS3500 or TS4500 tape library attaches to a TS7700 system.

This feature is available on the TS3500 and TS4500 tape libraries.

Refer to [FC 9217, Attach to TS7700](#) in for requirements and other information.

FC 9219, Tape Library Attach

This feature enables the TS7700 Server to attach directly to the TS3500 or TS4500 Tape Library. It's also possible to mount them in a nearby frame or a top hat.

Note:

- Mounting in the customer rack or top hat requires additional FCs.
- 16-Gb Fibre Channel switch features are required in the 3584 Tape Library frames containing the backend drives.

Refer to [FC 9219](#) for requirements and other information.

FC 9268, Plant installation of 100 MB/s throughput

This feature delivers a key to enable the first 100-MB/sec increment of potential peak data throughput on TS7770 or the TS7760 Server (3957-VEC). Enabling a data throughput increment does not guarantee that the overall Virtualization Engine performs at that data throughput level. However, installation of the maximum allowed number of features results in unrestricted peak data throughput capabilities. Installing the maximum number of feature #9268 plus #5268 removes any throughput limits. This feature is restricted to new factory installation and represents the first 100-MB/s increment.

Refer to [FC 9269](#), 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 45 on page 133](#) for requirements and other information.

FC 9336, R5 Expansion Frame Attachment

This feature identifies this TS7700 base frame 3952 Model F07 with #7337 has a first 3952 Model F07 with #7338 storage expansion frame attached to it.

Refer to [FC 9336](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9337, R5 2nd Expansion Frame Attachment

This feature identifies this TS7700 base frame 3952 Model F07 with #7337 has a 2nd R5 3952 Model F07 with #7338 storage expansion frame attached to it.

Refer to [FC 9337](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9339, Replacing TS7740 System

This feature instructs Manufacturing to ship the installation instructions to re-place an existing TS7700 system with this new TS7770 system.

Refer to [FC 9339](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9350, Plant Install

FC 9350, Plant Install, specifies the factory installation of a TS7700 Server model VED into a new 3952 Tape Frame coming from the plant..

You must also order FC 5630, Install 3957-VEC, against the 3952 Tape Frame when ordering this feature for the 3957-VEC.

Refer to [FC 9350, Plant Install](#) for requirements and other information.

FC 9352, Plant Install CFC

This code specifies plant install of a cache controller 3956-CFC into a new 3952 Tape Frame.

Note: This feature must appear on the TS7700 Model CFC order, and the Plant Install feature (#5667) must appear on the 3952 Tape Frame model F07 order.

Refer to [FC 9352](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9352, Plant Install CSB

This code specifies plant install of a cache controller 3956-CSB into a new 3952 Tape Frame.

Note: This feature must appear on the TS7700 Model CSB order, and the Plant Install feature (#5663) must appear on the 3952 Tape Frame order.

Refer to [FC 9352](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9353, Field merge CSB

This specify code allows the field merge of a TS7700 Cache Controller Model CSB into a previously installed 3952 Tape Frame.

Note: This feature must appear on the TS7760 Model CSB order, and the Plant Install feature #5666 must appear on the 3952 Tape Frame model F06 or F07 order.

Refer to [FC 9353](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9354, Plant Install XFC

This code specifies the factory installation of a cache expansion drawer into a new 3952 Tape Frame coming from the plant.

Note: This feature must appear on the TS7770 Model XFC order, and the Plant Install feature #5667 must appear on the 3952 Tape Frame model F07 order.

Refer to [FC 9354](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9354, Plant Install XSB

This code specifies the factory installation of a cache drawer into a new 3952 Tape Frame coming from the plant.

Note: This feature must appear on the TS7760 Model XSB order, and the Plant Install feature #5664 must appear on the 3952 Tape Frame order.

Refer to [FC 9354](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9355, Field merge XFC

This code specifies the field merge of a cache expansion drawer into a previously installed 3952 Tape Frame.

Note: This feature must appear on the TS7770 Model XFC order, and the Field Merge feature #5669 must appear on the 3952 Tape Frame model F07 order.

Refer to [FC 9355](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9355, Field merge

This code specifies the field merge of a cache drawer into a previously installed 3952 Tape Frame.

Note: This feature must appear on the TS7760 Model XSB order, and the Plant Install feature #5665 must appear on the 3952 Tape Frame model F07 order.

Refer to [FC 9355](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9700, No factory cables

FC 9700, No factory cables should be specified if you do not want the factory to ship any cable features with the new machine.

Refer to FC 9700, No factory cables in [Table 45 on page 133](#) for requirements and other information.

FC 9900, Tape Encryption Tape

This feature should be ordered when encryption will be used in a 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. Customer initiated procedures need to be completed for enabling and configuring the TS3500/TS4500 Tape Library or TS7700 cluster to support encryption with the TS11xx encryption capable tape drive.

FC 9900, Tape Encryption Tape is supported only with encryption-capable TS1150/TS1140/TS1130/TS1120 Tape Drives. It is not supported by 3592 J1A or 3590 Tape Drives.

Refer to [FC 9900](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9904, Remote Code Load Service

This feature is an indicator that the code load upgrades in the unit will be done remotely. This feature is the default option between features 5904 and 9904 and IBM reserves the right to modify the machine records associated with feature 5904 and 9904, based on the actual method used to update code on the customer's unit. Each system requires one of features 5904 or 9904 to be included.

Refer to [FC 9904](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9906, New order install

This feature identifies an Expansion frame attachment as part of an initial order. The presence of this feature eliminates shipment of redundant publications.

Refer to [FC 9906](#) in [Table 45 on page 133](#) for requirements and other information.

FC 990x, To order Hard Copy Pubs to help cost savings

FC 9954, NEMA L6-30 Power Cord

This feature provides a NEMA L6-30 non-watertight 4.3 meter (14 foot) power cord, 200-208, 240 Vac, 24 Amps, used in U.S., Canada, Latin America, and Japan.

Refer to [FC 9954](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9955, RS 3750 DP Power Cord

This feature provides a Russellstoll 3750DP Watertight 4.3 meter (14 foot) power cord, 200-208, 240 Vac, 24 Amps, used in U.S, Chicago, Canada, LA, and Japan.

Refer to [FC 9955](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9956, IEC 309 Power Cord

This feature provides a IEC 309, p+n+g, 32A, 4.3 meter (14 foot) power cord, 230 Vac, 24 Amps, used in EMEA.

Refer to [FC 9956](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9957, PDL 4.3 Power Cord

This feature provides a PDL 4.3 meter (14 foot) power cord, 230-240 Vac, 23 Amps, used in Australia and New Zealand.

Refer to [FC 9957](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9958, Korean 4.3m Power Cord

This feature provides a NEMA L6-30 non-watertight 4.3 meter (14 foot) power cord, 200-208, 240 Vac, 24 Amps, with a Korean plug, used in North and South Korea.

Refer to [FC 9958](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9959, Unterminated Power Cord

This feature provides an unterminated, non-watertight 4.3 meter (14 foot) power cord, 200-208, 240 Vac, 24 Amps power cord with IRAM and BSMI agency certifications. This is the recommended cord for Argentina and Taiwan.

Refer to [FC 9959](#) in [Table 45 on page 133](#) for requirements and other information.

FC 9966, China Unterminated Power Cord

This feature provides an unterminated, non-watertight 4.3 meter (14 foot), 200-208, 240 Vac, 24 Amps power cord with CCC agency certification. This is the recommended power cord for China.

Refer to [FC 9966](#) in [Table 45 on page 133](#) for requirements and other information.

FC AG00, Shipping and Handling - No charge (For 3952-F07)

This feature indicates there are no shipping and handling charge added to the order.

Refer to [FC AG00](#) in [Table 45 on page 133](#) for requirements and other information.

FC AG00, Shipping and Handling - No charge (For 3956-XFC)

This feature indicates that there are no shipping and handling charge added to the order

Refer to in [FC AG00](#) [Table 45 on page 133](#) for requirements and other information.

FC AGGA, Shipping and Handling

This feature indicates each 3952 Tape Frame on the order will have a shipping and handling charge added to the order.

Refer to [FC AGGA](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGGU, Shipping and Handling - No charge (For 3956-CSB)

This feature indicates there will be shipping and handling charge.

Refer to [FC AGGU](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGGU, Shipping and Handling - No charge (For 3956-CFC)

This feature indicates that the order will have a shipping and handling charge added to the order.

Refer to [FC AGGU](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGGV, Shipping and Handling - No Charge

This feature indicates that there is no shipping and handling charge added to the order.

Refer to [FC AGGV](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGGV, Shipping and Handling - XFC

This feature indicates that there is no shipping and handling charge added to the order.

Refer to [FC AGGV](#) in [Table 45 on page 133](#) 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 or F07 frames must be the same.

Refer to [FC AGK0](#) in [Table 45 on page 133](#) 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 or F07 frames must be the same.

Refer to [FC AGKE](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGKR, Ship with R4.1.2 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 or F07 frames must be the same.

Refer to [FC AGKE](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGKT, Ship with R5.0 Machine Code

Instructs Manufacturing to load the latest manufacturing level of Release 5.0 machine code on TS7700. For Field orders of R5.0 machine code #AGKT, micro-code must be ordered via Super Shipper. The Field order of #AGKT allows for R5.0 machine code level prerequisite requirements on certain hardware features. This feature in itself does not provide microcode items. A one page flyer with instructions on how to order machine code via Super Shipper is provided.

Refer to [FC AGKT](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGKU, Ship with R5.1 Machine Code

Instructs Manufacturing to load the latest manufacturing level of Release 5.1 machine code on TS7700. For Field orders of R5.1 machine code #AGKU, microcode must be ordered via Super Shipper. The Field order of #AGKU allows for R5.1 machine code level prerequisite requirements on certain hardware features. This feature in itself does not provide microcode items. A one-page flyer with instruction on how to order machine code via Super Shipper is provided

Refer to [FC AGKV](#) in [Table 45 on page 133](#) for requirements and other information.

FC AGKV, Ship with R5.2 Machine Code

Instructs Manufacturing to load the latest manufacturing level of Release 5.2 machine code on TS7700. For Field orders of R5.2 machine code #AGKV, microcode must be ordered via Super Shipper. The Field order of #AGKV allows for R5.2 machine code level prerequisite requirements on certain hardware features. This feature in itself does not provide microcode items. A one-page flyer with instruction on how to order machine code via Super Shipper is provided.

Refer to [FC AGKV](#) in [Table 45 on page 133](#) for requirements and other information.

FC RPQ 8B3723, TS7770 - 3 PHASE POWER (cord)

RPQ 8B3723 provides a pair of 415 volt three-phase WYE power cables for TS7770 3952-F07. The cable is 4.3 meters (14.1-feet) long and ships with the connectors: Hubbell Part Number: C532P6W. Male, Plug, 32A 220/380-240/415V, 4-Pole 5-Wire Grounding, Screw Terminals, Red, C-Series, Water-tight. This RPQ requires lab approval before ordering. When three-phase is selected, the frame UPO switch will no longer control any power for the frame. Instead, power should be removed for each three-phase PDU.

Refer to [FC RPQ 8B3723](#) in [Table 45](#) on [page 133](#) for requirements and other information.

FC RPQ 8B3722, TS7770 - 3 PHASE POWER (PDU)

RPQ 8B3722 provides a three-phase power distribution unit (PDU) for TS7770 (MTM 3952 Model F07) for users who need 400-volt support. It provides an appropriate 3 phase WYE power cord (415 volt) and can be used when the user needs a top exit cabling. This RPQ requires lab approval before ordering.

Refer to [FC RPQ 8B3722](#) in [Table 45](#) on [page 133](#) for requirements and other information.

Table 45. TS7700 features					
Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 0201, 9 Micron LC/LC 31 Meter	0	8 (Initial order maximum: 8)	Limitations: - Feature #9700 is required, or - When #3401 is installed, 2 x #0201 for each #3439/#3403 is required, or - When #3401 is not installed, 1 x #0201 for each #3439/#3403 is required or	Plant / Field installable: Both	Yes
FC 0203, 50 Micron LC/LC 31 Meter	0	8 (Initial order maximum: 8)	Prerequisite: None Limitation: - Feature #9700 is required - When #3401 is installed, 2 x #0203 for each #3438/#3402 is required, or - When #3401 is not installed, 1 x #0203 for each #3438/#3402 is required	Plant / Field installable: Both	Yes
FC 0983, TAA Compliance	0	1 (Initial order maximum: 1)	Limitations: Feature #0983 is not available in India for use.	Plant / Field installable: Initial	No
FC 1034, Enable Second Port Grid Connection	0	1 (Initial order maximum: 1)	Prerequisites: #1038, #1039, or #1041 is required.	Plant / Field installable: Both	Yes

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
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
FC 1038, 10 Gb Quad Port Grid Optical LW Connection	0	2 (Initial order maximum: 2)	Limitation: Mutually exclusive with #1039 and #1041 Comments: • These adapters cannot negotiate down to run at 1 Gb. They must be connected to a 10Gb network device • Two of #1038, #1039, and #1041 are required	Plant / Field installable: Both	Yes
FC 1039, 1Gb Grid Quad Port Copper Connection	0	2 (Initial order maximum: 2))	Prerequisite: None Limitation: Mutually exclusive with #1038 and #1041 Comments: Two of #1038, #1039, or #1041 are required	Plant / Field installable: Both	Yes
FC 1041, 10 Gb Dual Port Grid Optical LW Connection	None	2	Prerequisite: • Mutually exclusive with #1038 and #1039. • Two of #1038, #1039, or #1041 are required.	Plant or Field	Yes
FC 1776, US RoHS Indicator	0	1 (Initial order maximum: 1)	None	Plant / Field installable: Initial	Non-applicable
FC 1903, Power Distribution Unit	One of #1903 or #1912 or iRPQ 8B3722	1	Limitations: • Mutually exclusive with #1912 or iRPQ 8B3722 • VEC can only have FC 1903 • (R4.0 F06 or F07 only) – Not on R5 This feature provides one additional PDU to allow connection to independent branch power circuits. When this feature is ordered, two power cords will be provided.	Plant only	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 1904, Switching PDU (For 3952-F07)	0	1 (Initial order maximum: 1)	Prerequisite: Required when #2725 is installed Customer setup: No Limitation: Mutually exclusive with #7338	Plant / Field installable: Initial	No
FC 1904, Redundant AC Power (For 3957-VED)	0	1 (Initial order maximum: 1)	Corequisites: #4643 or #4649 Rack Mount Kit VED	Plant / Field installable: Initial	No
FC 1912, Single Phase PDU (For 3952-F07)	0	1 (Initial order maximum: 1)	Prerequisites: #7337, #7338 is required or #7339 Customer setup: No Limitations: • One of #1912 or 8B3722 is required • Mutually exclusive with iRPQ 8B3722 Comments: Minimum is one of #1912 or iRPQ8B3722	Plant / Field installable: Initial	No
FC 1912, Single Phase PDU	0	1 (Initial order maximum: 1)	Prerequisite: One of #9954, #9955, #9956, #9957, #9958, #9959, or #9966 is required Corequisites: #4643 or #4649 Rack Mount Kit VED	Plant / Field installable: Initial	No
FC 2704, TS3000 System Console expansion 26-port Ethernet switch/rackmount	0	1	Limitations: • Refer to the Limitations section to see a list of countries in which the switch has been qualified for use. • Mutually exclusive with #7335 or #7337 or #7339	Plant or field	Yes
FC 2715, Console attachment	0	1	Mutually exclusive with FC 2714. You must order one instance of either FC 2714 or FC 2715.	Plant or field	Yes
FC 2725 Rack Mount TS3000 System Console	0	1 (Initial order maximum: 1)	Corequisite: #2748, #5512, #4643, or #4649 Rack Mount Kit VED	Plant / Field installable: Initial	Yes
FC 2725 Rack Mount TS3000 System Console (For 3952-F07)	0	1 (Initial order maximum: 1)	Prerequisites: #7337 or #7339 Corequisites: #1904, #2748, and #5512 Customer setup: No	Plant / Field installable: Initial	Yes

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 2748, Optical drive	0	1 (Initial order maximum: 1)	Corequisite: • Feature #2725 • Feature #4643 or 4649 Rack Mount Kit VED	Plant / Field installable: Initial	Yes
FC 2748, Optical drive (For 3952-F07)	0	1 (Initial order maximum: 1)	Corequisites: #2725 Customer setup: No	Plant / Field installable: Initial	Yes
FC 3401, Enable FICON second port	0	1 (Initial order maximum: 1)	Prerequisites: FC 3402, FC 3403, FC 3438, or FC 3439 is required. Corequisites: • FC 9700 is required or • 2 x FC 0201 for each FC 3403 or FC 3439 installed, or • 2 x FC 0203 for each FC 3402 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 3403 or FC 3439 FICON card configured, and two FC 0203 for each FC 3402 or FC 3438 FICON card configured.	Plant / Field installable: Both	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 3402, 16 Gb SW FICON Adapter	0	4 (Initial order maximum: 4)	Limitations - Valid quantities of #3402 are 0, 2, or 4 - Two of #3402, #3403, #3438 or #3439 are required - The maximum quantity of #3402, #3403, #3438 plus #3439 is 4. Compatibility conflicts: OM1 is not recommended for 16 Gb FICON connections Comments: - At 16 Gb/sec speed, the total cable length cannot exceed: 130 meters using 50 micron OM4 (4700MHz*km) Aqua blue colored fibre 100 meters using 50 micron OM3 (2000MHz*km) Aqua blue colored fibre 35 meters using 50 micron OM2 (500MHz*km) Orange colored fibre	Plant / Field installable: Both	Yes
FC 3403, 16 Gb LW FICON Adapter	0	4 (Initial order maximum: 4)	Limitations: - Valid quantities of #3403 are 0, 2 or 4 - Two of #3402, #3403, #3438 or #3439 are required. - The maximum quantity of #3402, #3403, #3438 plus #3439 is 4 Customer setup: No	Plant / Field installable: Both	Yes
FC 3438, 8 Gb FICON Short Wavelength Attachment	0	4	Corequisite: - 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 3438 - FC 3439	Plant or field	Yes

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 3439, 8 Gb FICON Long Wavelength Attachment	0	4	Corequisite: - 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 3438 - FC 3439	Plant or field	Yes
FC 3466, 32 GB memory upgrade	0	1	Prerequisite: FC 5278	Plant or field	No
FC 4015, Grid Enablement	0	1 (Initial order maximum: 1)	None	Plant / Field installable: Both	No
FC 4016, Remove Cluster from Grid	0	99 (Initial order maximum: 99)	Prerequisite: FC 4015	Plant / Field installable: MES	No
FC 4017, Cluster Cleanup	0	99 (Initial order maximum: 99)	Prerequisite: None	Plant / Field installable: MES	No
FC 4643, Rack Mount Kit VED with CSB	0	1 (Initial order maximum: 1)	Prerequisite: #1904, 1912, #2725, #5756 are required - A minimum of 1 #4694 is required Limitation: Mutually exclusive with #4649 or #9350	Plant / Field installable: Initial	No
FC 4647, Rack Mount Kit CSB	0	1 (Initial order maximum: 1)	Prerequisites: #iRPQ 8B3721 is required - One of #4647 or #9352 or #9353 is required - One rack mount 3957 model VED with #4643 must be ordered and installed with this CSB - One of AG00 or AGGU is required Limitations: Mutually exclusive with #9352 or #9353	Plant / Field installable: Initial	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 4648, Rack Mount Kit XSB	0	1 (Initial order maximum: 1)	Prerequisites: • #iRPQ 8B3721 is required • One of #4648 or #9354 or #9355 is required • One rack mount 3957 model VED with #4643 must be ordered and installed with this CSB • One of AG00 or AGGU is required Limitations: Mutually exclusive with #9354 or #9355	Plant / Field installable: Initial	No
FC 4649, Rack Mount Kit VED with CFC	0	1 (Initial order maximum: 1)	Prerequisites: #1904, #1912, #2725, and #5756 are required Limitations: • Mutually exclusive with #4643 or #9350 • A 3956 model CFC with #4650 must be ordered and installed with this VED	Plant / Field installable: Initial	No
FC 4698, Initial Order XFC Customer Rack	0	1	Corequisite: #4649 Rack Mount Kit VED Limitation: Valid quantities of #4698 are 0, 1	Plant / Field installable: Initial	No
FC 4699, Field Order XFC for Customer Rack	0	1	Corequisite: #4649 Rack Mount Kit VED Limitation: Valid quantities of #4698 and #4699 are 1, 2	Plant / Field installable: MES	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
FC 5242, Dual Port 16 Gb Fibre Channel HBA	0	1	Prerequisite: <u>FC 9336, 1st Exp Frame</u> or <u>FC 9337, 2nd Exp Frame</u> is required on the 3952 F06 or 3952 F07 where the 3957-VEC is installed.	Plant or field	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5243, Quad Port 16 Gb FC HBA	0	2 (Initial order maximum: 2)	Prerequisite: • #9336 (1st Expansion Frame Attach) is required on the 3952-F06 or F07 where this 3957-VED is installed when #5243 equals one • #9336 (1st Expansion Frame Attach) and #9337 (2nd Expansion Frame Attach) are required on the 3952-F07 where this 3957-VED is installed, when #5243 equals two Compatibility conflict: Not available with 3956-CFC Comments: Can only be used with CSB/XSB configurations	Plant / Field installable: Both	No
FC 5262, 20 TB cache enablement	0	99 (Initial order maximum: 4)	Customer set up : Yes Limitations: • 1 x #5262 or 1 x #5263 minimum must be plant installed • At least 1 TB must be enabled before next 3956 Cache drawer pair may be installed (enforced via e-config) Comments: • A Maximum of 4x #5262 20TB Cache Enablement Features may be selected for any one single order, either Initial order or MES • More than 4x #5262 20TB Cache Enablement Features may exist on the machine • If 5x 5262 20TB Cache Enablement Features are desired in one single order, 1x 5263 - 100TB Cache Enablement Feature will be enabled (enforced via e-Config)	Plant / Field installable: Both	No
FC 5263, 100TB cache enablement	0	39 (Initial order maximum: 39)	Customer setup: Yes Limitations: • A minimum of 1 x #5262 or 1x 5263 must be plant installed • At least 1 TB must be enabled before the next 3956 Cache drawer pair may be installed (enforced via e-config)	Plant / Field installable: Both	No

Table 45. TS7700 features (continued)					
Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5268, 100 MB/sec Increment	0	39 (Initial order maximum: 39)	Customer setup: Yes	Plant / Field installable: Both	No
FC 5270, Increased Logical Volumes	0	15 (Initial order maximum: 15)	Customer setup: Yes	Plant / Field installable: Both	No
FC 5271, Selective Device Access Control	0	2 (Initial order maximum: 2)	None	Plant / Field installable: Both	No
FC 5272, Disk Enabled Encryption	0	1 (Initial order maximum: 1)	Prerequisite: • #9277 is required • When feature #5272 is installed, feature #7405 is required on each 3956-CSB and/or 3956-CFC model in the TS7700 cluster • TS11xx encryption capable tape drives are required, if tape attached Limitations: #5272 is not available in the People's Republic of China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia Note: For TS7770, Feature #5272 Disk Enabled Encryption is not available for field Install on TS7770 and needs to be shipped from manufacturing with the Feature code already installed. Customer Setup: No	Plant / Field installable: Initial	No
FC 5273, TS7770 Tape Attach	0	1 (Initial order maximum: 1)	Prerequisite: At least 1 x #5274 is required. Limitation: Mutually exclusive with #5278	Plant / Field installable: Both	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5274, Enable 1 TB Pending Tape Capacity	0	10 (Initial order maximum: 10)	Corequisite: Feature #5273 or #5278 is required Compatibility conflicts: None Customer setup: Yes Limitations: None Cable order: N/A Comments: 3 x #5274 is the recommended minimum pre-migration queue size	Plant / Field installable: Both	No
FC 5275, Additional virtual devices	0	15 (Initial order maximum: 15)	Prerequisite: None Customer setup: Yes	Plant / Field installable: Both	No
FC 5276, Disk Encrypt-External Key Manager	0	1	Prerequisites: • #9277 is required • #5272 is required • When feature #5276 is installed, feature #7405 is required on each 3956-CSB and/or 3956-CFC model in the TS7700 cluster • TS11xx encryption capable tape drives are required (Remove #7404) • When feature #5276 is installed, feature 5272 is required Limitations: • #5276 is not available not available in the People's Republic of China Customer setup (CSU): NO	Plant or field	No
FC 5277, External Disk Encryption Certificate - Field	0	1	Mutually exclusive with: • FC 9277 Prerequisites: • FC 5276	Field Only	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5278, Cloud Enablement	0	1 (Initial order maximum: 1)	Corequisite: - At least 1 x #5274 is required Prerequisite: #3466 for VEC only, not required for the VED Limitations: - Requires a minimum 64 GB RAM to support Cloud Enablement Feature #5278. Memory upgrade available #3466 on the VEC only. - Mutually exclusive with #5273 Important: 3 x #5274 is the recommended minimum premigration queue size Customer setup: NO	Plant or field	No
FC 5279, 5 TB Active Premigration Queue	0	10 (Initial order maximum: 10)	Prerequisite: - Feature #AGKS or #AGKT is required 10 x #5274 are required before the first instance of #5279 may be installed Corequisites: Feature #5273 or #5278 is required Compatibility conflicts: None Customer setup: Yes Limitations: None Comments: Once 10 x #5279 are installed, the amount of data pending active pre-migration for tape or cloud is no longer constrained by features #5274 and #5279.	Plant or field	No
FC 5281 - Secure Data Transfer	0	1	Prerequisite: #5281 (SDT) is required on any cluster sending or receiving encrypted data across a grid link. #AGKT Customer setup required: Yes	Plant or field	Yes

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5282 – DS8000 Object Store	0	1	Prerequisite: #AGKT Restrictions: 1. DS8000 objects cannot be migrated to physical tape or cloud (Storage Class, Storage Group). It is used for virtual volumes. 2. DS8000 objects cannot be replicated to other clusters in the grid using Grid replication (Management Class). 3. Only one object cache partition is allowed (Cache Partition). 4. Compression is not available for DS8000 objects (Data Class). Define, modify, copy, or delete an IBM® TS7700 data class for volume sizes and LWORM policy assignment. Data class policies do not apply to DS8000 Object data.	Plant or field	Yes
FC 5283, DS8000 Object Store Grid Policy Management	0	1	Prerequisites: • FC 8083 (Installed during MES) • SSDs installed in P9 server • VED	Field	No
FC 5512, KVM	0	1 (Initial order maximum: 1)	Corequisites: #4643 or #4649 Rack Mount Kit VED	Plant / Field installable: Initial	Yes
FC 5512, KVM (For 3952-F07)	0	1 (Initial order maximum: 1)	Corequisites: #2725	Plant / Field installable: Initial	Yes
FC 5630, Install 3957-VEC	0	1	Prerequisites: • FC 7333 Corequisites: FC 9350 on 3957-VEC	Plant only	No
FC 5631, Install 3957 VED	0	1 (Initial order maximum: 1)	Prerequisites: • #7337 or #7339 is required • #9350 on 3957 VED is required. Customer setup: No Comments: • #7337 is required for CSB/XSC • #7339 is required for CFC/XFC • #9350 on 3957 VED is required	Plant / Field installable: Initial	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
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
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

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
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 5663, Plant Install 3956 CSB	0	2 (Initial order maximum: 2)	Prerequisites: #9352 on 3956 CSB is required. #7337 or #7338 is required 1 x #5262 or #5263 minimum must be ordered on the 3957-VED Customer setup: No Comments: - When #7337 is present, maximum of 3956-CSB allowed is one - When #7338 is present, maximum of 3956-CSB allowed is two	Plant / Field installable: Initial	No
FC 5664, Plant Install 3956 XSB	0	18 (Initial order maximum: 18)	Prerequisites: #5663 #9354 on 3956 XSB is required Limitations: - Valid quantities of #5663 plus #5664 plus #5665 with #7335 or #7337 are 2, 4, 6, 8 and 10. - Valid quantities when #5663 equal one, #5663 plus #5664 plus #5665 with #7338 are even numbers from 2, 4, 6, 8, and 10 - Valid quantities when #5663 plus #5666 equal two, #5663 plus #5664 plus #5665 plus #5666 with #7338 are even numbers from 12, 14, 16, 18, and 20 - Each 3956-CSB can have valid quantities of 1, 3, 5, 7, or 9 3956-XSBs 1 x #5262 or #5263 minimum must be ordered on the 3957-VED	Plant / Field installable: Initial	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5665, Field Install 3956 XSB	0	17 (Initial order maximum: 17)	Prerequisites: • #5663 • #9355 on 3956 XSB is required Limitations: • Valid quantities of #5663 plus #5664 plus #5665 with #7335 or #7337 are 2, 4, 6, 8 and 10 • Valid quantities when #5663 equal one, #5663 plus #5664 plus #5665 with #7338 are even numbers from 2, 4, 6, 8, and 10 • Valid quantities when #5663 plus #5666 equal two, #5663 plus #5664 plus #5665 plus #5666 with #7338 are even numbers from 12, 14, 16, 18, and 20 • Each 3956-CSB can have valid quantities of 1, 3, 5, 7, or 9 3956-XSBs	Plant / Field installable: MES	No
FC 5666, Field Install 3956 CSB	0	1 (Initial order maximum: 1)	Prerequisites: • #5663 • #9353 on 3956 CSB is required Comment: When #7338 is present, valid combined quantities of Plant Install 3956-CSB #5663 and Field install 3956-CSB #5666 is one or two	Plant / Field installable: MES	No
FC 5667, Plant Install 3956 CFC	0	1 (Initial order maximum: 1)	Prerequisites: • #9352 on 3956 CFC is required • #7339 is required • 1 x #5262 or #5263 as a minimum must be ordered on the 3957-VED • #8081 on 3957 VED is required Limitation: When #7339 is present, maximum of 3956-CFC allowed is one.	Plant / Field installable: Initial	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 5668, Plant Install 3956 XFC	0	1 (Initial order maximum: 1)	Prerequisites: • #5667 • #9354 on 3956 XFC is required Limitations: • Valid quantities of #5667, #5668, #5669 with #7339 are 1 or 2 • 1 x #5262 or #5263 minimum must be ordered on 3957-VED	Plant / Field installable: Initial	No
FC 5669, Field Install 3956 XFC	0	1 (Initial order maximum: 1)	Prerequisites: • #5667 • #9355 on 3956 XFC is required Customer setup: No Limitations: Valid quantities of #5667, #5668, #5669 with #7339 are 1 or 2	Plant / Field installable: MES	No
FC 5756, Integrated Control Path (3956-XSB)	0	1 (Initial order maximum: 1)	Corequisites: #4643 or #4649 Rack Mount Kit VED	Plant / Field installable: Initial	No
FC 5756, Integrated Control Path (3956-XFC)	0	1 (Initial order maximum: 1)	Prerequisites: #7337 and or #7339 Customer setup: No	Plant / Field installable: Initial	No
FC 5758, Integrated control path	0	1	Prerequisites: One total instance of: • FC 7333	Plant only	No
FC 5904, Remote Code Load Exception	0	1 (Initial order maximum: 1)	Limitation: • Must have one #5904 or #9904 Customer set up: No Comment: Maximum number is one of #5904 or #9904	Plant / Field installable: Both	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

Table 45. 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	Compatibility conflicts: • Mutually exclusive with all other #73xx features • Mutually exclusive with all TSSC features Prerequisites: • Must attach to a TS7700 base frame installed within 10 meters of this frame • Power Distribution Unit, #1903, is required • One of Plant Install 3956 CSA, #5657, or Plant Instl CSA w 8TB DDM, #5660, is required Limitations: • When #5657 is present, valid quantities of model XSA, #5658 plus #5659 plus #5662 are 0 to 15 • When #5660 is present, valid quantities of model XSA, #5661 plus #5662 are 0 to 14 • This expansion frame may not be attached to a #7335 or #7337 base frame.	Plant only	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7335, TS7700 Encryption Capable Base Frame	0	1	Compatibility conflicts: • Mutually exclusive with all other #73xx features. • Mutually exclusive with #2704 Prerequisites: • PDU, #1912 or RPQ 8B3722 is required • Plant Install VED, #5631 is required • Integrated Control Path, #5756, is required • Ship with R5.0 Machine Code, #AGKT, is required • Plant Install CSB, #5663, is required Limitations: • When #5663 is present, Valid quantities of model XSB #5664 plus #5665 are 2, 4, 6, 8 and 10. • Valid quantities of model XSB #5664, #5665 are 1, 3, 5, 7, & 9 • If Korea, valid quantities of XSB #5664, #5665 are 1	Plant only	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7336, TS7700 Encryption Capable Base Frame	0	1 (Initial order maximum: 1)	Prerequisites: • Must attach to a TS7700 base frame installed within 10 meters of this frame • Power Distribution Unit, #1912 or RPQ 8B3722, is required • Plant Install 3956 CSB, #5663 is required Compatibility conflicts: • Mutually exclusive with all other #73xx features • Mutually exclusive with #2725 Limitations: • Feature #7336 is not available in South Korea for use • When quantity #5663 is one, valid quantities of #5663 plus #5664 plus #5665 are 2, 4, 6, 8, and 10 • When quantity #5663, #5666 is two, valid quantities of #5663 plus #5664 plus #5665 plus #5666 are 12, 14, 16, 18, and 20 Comments: F06 expansion frame (#7336) may be attached to a F06 base frame (#7335) or F07 base frame (#7337)	Plant only	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7337, TS7700 Encryption Capable Base Frame	0	1 (Initial order maximum: 1)	Compatibility conflicts: • Mutually exclusive with all other #73xx features. • Mutually exclusive with #2704 Prerequisites: • PDU, #1912 or RPQ 8B3722 is required • Plant Install VED, #5631 is required • Integrated Control Path, #5756, is required • Ship with R5.2 Machine Code, #AGKT, or R5.1 Machine Code #AGKU is required • Plant Install CSB, #5663, is required • Rack Mount TS3000 System Console #2725 is required Limitations: • When #5663 is present, valid quantities of #5663 plus #5664 plus #5665 are 2, 4, 6, 8 and 10 • Valid quantities of model XSB #5664, #5665 are 1, 3, 5, 7, and 9 • If Korea, valid quantities of XSB #5664, #5665 are 1 and 3	Plant / Field installable: Initial	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7338, TS7700 Encryption Capable Expansion Frame	0	1 (Initial order maximum: 1)	Compatibility conflicts: • Mutually exclusive with all other #73xx features • Mutually exclusive with #2725 Prerequisites: • Must attach to a TS7700 base frame installed within 10 meters of this frame • Power Distribution Unit, #1912 or RPQ 8B3722, is required • Plant Install 3956 CSB #5663, is required Limitations: • #7336 is not available in South Korea for use • #7338 is not available in South Korea for use • #7338 with #9336 represents the 1st Exp Frame Attachment and the Base Frame with #7337 must also have #9336 • #7338 with #9337 represents the 2nd Exp Frame Attachment and the Base Frame with #7337 must also have #9337 • When quantity #5663 is one, valid quantities of #5663, #5664, and #5665 are 2, 4, 6, 8, 10 • When quantity #5663, #5666 is two, valid quantities of #5663, #5666, #5664, and #5665 are 12, 14, 16, 18, and 20 Comments: F07 expansion frame (#7338) may be attached to a F06 base frame (#7335) or F07 base frame (#7337)	Plant / Field installable: Initial	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 7339, TS7700 Encryption Capable Base Frame (F07)	0	1 (Initial order maximum: 1)	Prerequisites: • PDU, #1912 or RPQ 8B3722 is required • Plant Install VED, #5631 is required • Integrated Control Path, #5756, is required • Ship with R5.2 Machine Code, #AGKV • Plant Install CFC, #5667, is required • Rack Mount TS3000 System Console #2725 is required Compatibility conflicts: Mutually exclusive with all other #73xx features Customer setup: No Limitations: When #5667 is present, valid quantities of #5667 and #5668, or #5669 are 1 or 2	Plant / Field installable: Initial	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 7405, Encryption CFC (USB Flash Drives (Four Pack))	0	1	Prerequisite: Required when #5272 or #5276 is installed on the 3957-VED TS7770 server. Limitations: • Feature #7405 is not available in the People's Republic of China. • Feature #7405 is not available in the following countries: Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia. • Each 3956-CFC must have #7405	Plant only	No
FC 8080, 600GB HDDs in VED	0	1 ((Initial order maximum: 1)	Limitation: • Must have one #8080 or #8081 Comments: Maximum number is one of #8080 or #8081	Plant / Field installable: Initial	No
FC 8081, 775GB SSDs in VED	0	1 (Initial order maximum: 1)	Limitation: • Must have one #8080 or #8081	Plant / Field installable: Initial	No

Table 45. TS7700 features (continued)					
Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 8083, 3.84TB SSDs in VED	0	1	None	Both	No
FC 9000, Mainframe Attachment†	1	1 (Initial order maximum: 1)	None	Plant / Field installable: Initial	No
FC 9217, Attach to TS7700	0	0	FC 9219 must be ordered on the TS7700	Plant or field	Yes
FC 9219, Tape Library Attach †	0	1 (Initial order maximum: 1)	Corequisite: FC 5273 is required	Plant / Field installable: Both	Yes
FC 9268, Plant installation of 100 MB/s Throughput †	1	1 (Initial order maximum: 1)	Prerequisite: None.	Plant / Field installable: Initial	No
FC 9277, External Encryption Certificate - Plant	1	1 (Initial order maximum: 1)	Prerequisite: None	Plant / Field installable: Initial	No
FC 9336, R5 1st Expansion Frame Attachment	0	1 (Initial order maximum: 1)	Compatibility conflict: Mutually exclusive with #7333 Prerequisites: • #7337 or #7338 is required • Feature #5243 is required on the model VED installed in this frame • When #5663 is present, 9 x #5664 plus #5665 are required on this base frame • #9336 is also required on the Base Frame 3952-F07 which has #7337	Plant / Field installable: Both	No
FC 9337, R5 2nd Expansion Frame Attachment	0	1 (Initial order maximum: 1)	Prerequisites: • 7337 or 7338 is required • Feature quality two of #5243 is required on the model VED installed in this frame • #9336 is also required on the Base Frame 3952-F07 which has #7337 • #9337 is also required on the Base Frame 3952-F07 which has #7337 Customer setup: No	Plant / Field installable: Both	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9339, Replacing TS7740 System	0	1 1 (Initial order maximum: 1)	Prerequisite: Feature #5273 is required on the 3957-VEC or 3957-VED installed in this model F07. Customer setup: No	Plant / Field installable: Initial	No
FC 9350, Plant Install†	1	1 (Initial order maximum: 1)	Prerequisite: Feature #5631 on 3952 Model F06 or F07 is required. Limitations: Mutually exclusive with #4643 or #4649 Technical note: This feature must appear on the TS7700 Server model VED order, and the Install 3957 VED feature (#5631) must appear on the 3952 Tape Frame order.	Plant / Field installable: Initial	No
FC 9352, Plant Install CFC†	0	1	Prerequisite: One of #9352 or #4650 is required Limitations: Mutually exclusive with #4650 (Rack Mount)	Plant only	No
FC 9352, Plant Install CSB	0	1	Prerequisite: One of #9352 or #9353 or #4647 is required Limitation: Mutually exclusive with #4647 (Rack Mount) or #9353 (Field install CSB)	Plant only	No
FC 9353, Field merge CSB (3952 F05)	0	1	Prerequisite: FC 9352 or FC 9353 or FC9355 is required. Limitation: FC 9352 (Plant Install CSB)	Plant only	No
FC 9354, Plant Install XFC†	0	1	Prerequisite: One of #4651 or #9354 or #9355 is required Limitation: Mutually exclusive with #4651 (Rack Mount) or #9355 (Field install XFC)	Plant only	No
FC 9354, Plant Install XSB	0	1	Prerequisites: One of #4648 or #9354 or #9355 is required Limitations: Mutually exclusive with #4648 (Rack Mount) or #9355	Plant only	No
FC 9355, Field merge XFC	0	1	Prerequisite: One of #4651 or #9354 or #9355 is required. Limitation: Mutually exclusive with #4651 (Rack Mount) or #9354 (Plant Install XFC)	Plant only	No

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9355, Field merge	0	1	Prerequisite: One of #4648 or #9354 or #9355 is required. Limitations: • Mutually exclusive with #0983 and #ADZ1 • Mutually exclusive with #4648 (Rack Mount) or #9354	Plant only	No
FC 9700, No Factory Cables†	0	1 (Initial order maximum: 1)	Prerequisites: None.	Plant / Field installable: Initial	No
FC 9900, Tape Encryption Tape	0	1 (Initial order maximum: 1)	Prerequisite: #5273 Customer Setup (CSU): Yes. Limitation: Feature #9900 is not available in the People's Republic of China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia	Plant / Field installable: Both	No
FC 9904, Remote Code Load Service	0	1 (Initial order maximum: 1)	Limitation: Must have one #9904 or #5904 Comments: Maximum is one of #9904 or #5904	Plant / Field installable: Both	No
FC 9906, New order install	0	1 (Initial order maximum: 1)	Prerequisites: 3952-F07 must have feature #7338, and must have a 3952-F07 with feature #7337 on the same order Limitations: Mutually exclusive with #7337 Customer setup: No Comments: #9906 is required on any 3952-F07 with #7338 when ordered with new 3952-F07 with #7337	Plant / Field installable: Initial	Not applicable
FC 9954, NEMA L6-30 Power Cord	0	1(Initial order maximum: 1)	Limitations: One of 9954, 9955, 9956, 9957, 9958, 9959, or 9966 is required.	Plant / Field installable: Both	Yes
FC 9955, RS 3750 DP Power Cord	0	1 (Initial order maximum: 1)	Limitations: One of 9954, 9955, 9956, 9957, 9958, 9959, or 9966 is required Customer setup: No	Plant / Field installable: Both	Yes

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC 9956, IEC 309 Power Cord	0	1 (Initial order maximum: 1)	Limitations: One of 9954, 9955, 9956, 9957, 9958, 9959 or 9966 is required. Customer setup: No	Plant / Field installable: Both	Yes
FC 9957, PDL 4.3 power cord	0	1 (Initial order maximum: 1)	Limitations: One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966 is required Customer setup: No	Plant / Field installable: Both	Not applicable
FC 9958, Korean 4.3-m power cord	0	1 (Initial order maximum: 1)	Limitations: One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966 is required Customer setup: No	Plant / Field installable: Both	Not applicable
FC 9959, Unterminated power cord	0	1 (Initial order maximum: 1)	One of FC 9954, 9955, 9956, 9957, 9958, 9959, or 9966 is required	Plant / Field installable: Both	Not applicable
FC 9966, China Unterminated Power Cord	0	1 (Initial order maximum: 1)	Limitations: One of 9954, 9955, 9956, 9957, 9958, 9959, or 9966 is required Customer setup: No	Plant / Field installable: Both	Not applicable
FC AG00, Shipping and Handling - No Charge (For 3952-F07)	0	1 (Initial order maximum: 1)	Limitations: One of FC AG00 or AGGA is required. Customer setup: No	Plant / Field installable: Initial	No
FC AG00, Shipping and Handling - No Charge (For 3956-XFC)	0	1 (Initial order maximum: 1)	Prerequisites: #9355 or 4651 Limitations: One of AG00 or AGGV is required	Plant / Field installable: Initial	No
FC AGGA, Shipping and Handling	0	1 (Initial order maximum: 1)	One of FC AG00 or AGGA is required. Customer setup: No	Plant / Field installable: Initial	No
FC AGGU, Shipping and Handling - No Charge (For 3956-CSB)	0	1 (Initial order maximum: 1)	Prerequisites: Feature #9353 or #4647 Limitations: - One of AG00 or AGGU is required - Mutually exclusive with feature #9352	Plant / Field installable: Initial	Not applicable

Table 45. TS7700 features (continued)

Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC AGGU, Shipping and Handling - CFC (For 3956-CFC)	0	1 (Initial order maximum: 1)	Prerequisites: #4650 Limitations: - One of AG00 or AGGU is required - Mutually exclusive with #9352	Plant / Field installable: Initial	Not applicable
FC AGGV, Shipping and Handling - No Charge	0	1 (Initial order maximum: 1)	Prerequisites: Feature #9355 or #4648 Limitations: - One of AG00 or AGGV is required - Mutually exclusive with feature #9354	Plant / Field installable: Initial	Not applicable
FC AGGV, Shipping and Handling - XFC	0	1 (Initial order maximum: 1)	Prerequisites: #9354 Limitations: - One of AG00 or AGGV is required - Mutually exclusive with #9352	Plant / Field installable: Initial	Not applicable
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
FC AGKT, Ship with R5.0 Machine Code	0	1 (Initial order maximum: 1)	Limitations: - One of #AGKE or #AGK0 or #AGKR or #AGKS or AGKT is required - Mutually exclusive with #AGK0, #AGKR, #AGKE, #AGKS	Plant or Field	Yes
FC AGKU, Ship with R5.1 Machine Code	0	1 (Initial order maximum: 1)	Prerequisites: #7337 is required Mutually exclusive with AGKT, AGKV Customer setup: No	Plant/Field installable: Both	

Table 45. TS7700 features (continued)					
Feature	Minimum	Maximum	Requirements	Installation	Removable?
FC AGKV, Ship with R5.2 Machine Code	0	1 (Initial order maximum: 1)	Prerequisites: #7339 and #7337 are required Limitations: Mutually exclusive with AGKT, AGKU Customer setup: No	Plant/Field installable: Both	No
FC RPQ 8B3723, TS7770 - 3 PHASE POWER (cord)	0	1	Prerequisites: RPQ 8B3722 is required Limitations: Mutually exclusive with #9954, #9955, #9956, #9957, #9958, #9959, and #9966	Plant only	Yes
FC RPQ 8B3722, TS7770 - 3 PHASE POWER (PDU)	0	1	Prerequisites: • #7337, #7338, and/or #7339 is required • RPQ 8B3723 is required Limitations: Mutually exclusive with #1912		
† Withdrawn for at least one component. Refer to the <i>Quick reference by component</i> topic in the Related information section to verify availability.					

Related information

[“System requirements” on page 54](#)

Capacity on Demand

Capacity on Demand allows customers to enable disk capacity in 20 TB and 100 TB increments concurrently.

- A maximum of 4x #5262 20 TB Cache Enablement Features can be selected for any one single order, either Initial order or MES.
- More than 4x #5262 20 TB Cache Enablement Features may exist on the machine.
- If 5x 5262 20 TB Cache Enablement Features are wanted in one single order, 1x 5263 - 100 TB Cache Enablement Feature would be enabled (enforced via e-Config).
- At least 1 TB of licensed capacity must be enabled on the next set of drawer pairs (through features #5262 and #5263) before the next drawer pair may be installed. Adding physical drawer pairs without at least 1 TB of licensed capacity enabled is not supported.
- Features #5262 and #5263 must be ordered on 3957-VED model.
- At least one feature #5262 20 TB or #5263 100 TB cache enablement increment minimum must be plant installed.

TS7770 with 3956-CSB and 3956-XSB enclosures

- Up to 780 TB* usable capacity in a base frame only configuration (1 CSB + 9 XSBs).
- Up 2.36 PB usable capacity in a base frame with one expansion frame fully populated with 20 drawers (2 CSBs + 18 XSBs)
- Up to 3.94 PB usable capacity in a base frame with two fully populated expansion frames, each frame with 20 drawers (2 CSBs + 18 XSBs)

- Up to 133 TB* usable capacity in a base frame only configuration (1 CFC + 1 XFC)

Note:

- Release 5 delivers 10 TB 7.2 K SAS disk drives with 157 TB usable capacity per drawer pair. Using the ENERGY STAR-compliant IBM Storwize V5030E model, the TS7770 cache enclosures must be installed in pairs, two drawers at a time. Additional pairs of XSB drawers now support concurrent expansion, which is unique to the TS7770 model.
- The capacity on demand is related to physical cache size. It is not related to compression.

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 46 on page 163](#) through [Table 63 on page 194](#).

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 46 on page 163](#))
- TS3500 or TS4500 Tape Library Configuration Information Table and Notes ([Table 47 on page 166](#))
- TS3500 or TS4500 Tape Library Drive Information Table and Notes ([Table 48 on page 170](#))
- TS3500 Limited Drive Support Table ([Table 49 on page 173](#))
- Media Volume Serial (VOLSER) Range Table and Notes ([Table 50 on page 174](#))
- Encryption Key Information Table ([Table 51 on page 174](#))
- TS4500 Limited Drive Support Table ([Table 52 on page 174](#))
- Review media types in “3592 Tape Cartridges” on page 49
- TS7700 Code Activation/VPD Information Table and Notes ([Table 53 on page 175](#))
- TS7700 Customer Network Configuration Table and Notes ([Table 54 on page 179](#))
- TSSC Configuration Information Table and Notes ([Table 55 on page 182](#))
- Grid Local Address Table and Notes ([Table 61 on page 186](#))
- Summary Table ([Table 62 on page 189](#))
- TSSC Grid Configuration Information Table and Notes ([Table 63 on page 194](#))

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 TS7760s, or TS7760TAs participating in a GRID (peer to peer) configuration, but you can have a mix (hybrid) configuration of TS7770, TS7760, TS7770T 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 46 on page 163](#) 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 46. Cluster Description Table and Notes

Cluster	Component Serial Numbers	Description of Location
Cluster 0	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 1	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 2	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	

Table 46. Cluster Description Table and Notes (continued)

Cluster	Component Serial Numbers	Description of Location
Cluster 3	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 4	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 5	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	

Table 46. Cluster Description Table and Notes (continued)

Cluster	Component Serial Numbers	Description of Location
Cluster 6	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3584 Lxx: (if installing a TS7700 with tape attached)	
Cluster 7	3957-Vxx:	
	3952 F05:	
	3952 F0x: Optional attachment to a TS7700 Storage Expansion Frame:	
	3952 F0x: 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 47 on page 166](#) and [Table 48 on page 170](#). 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 47. 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 47. 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 47. 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 47. 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 48. 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__	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__
	CLUSTER 2: F=Frame, C=Column, R=Row WWNN=World Wide Node Name	CLUSTER 3: F=Frame, C=Column, R=Row WWNN=World Wide Node Name

Table 48. TS3500 or TS4500 Tape Library Drive Information Table and Notes (continued)

Field	Values
	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__ 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__
	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__ 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__

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 50 on page 174 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 49 on page 173](#) 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 53 on page 175](#).

(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 TS7760, the microcode level must be at 8.33.x.x or later and has a limited heterogeneous drive support shown in [Table 49 on page 173](#):

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.

	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 TS7700 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 50. 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 51. 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 52 on page 174](#).

Table 52. TS4500 Limited Drive Support Table				
	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	Supported	2 – 12	4 – 14	16

TS7700 configuration

Provide values for each of the defined TS7700 configuration fields defined in [Table 53 on page 175](#) and [Table 54 on page 179](#). 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 53. 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 53. 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.

Table 53. Code Activation/VPD Information Table and Notes (continued)

Field	Value	Notes®
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.
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.

Table 53. Code Activation/VPD Information Table and Notes (continued)

Field	Value	Notes®
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.

Table 53. Code Activation/VPD Information Table and Notes (continued)

Field	Value	Notes®
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 Switch.

Table 54. 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: _____._____._____._____._____._____._____._____._____._____	

Table 54. TS7700 Customer Network Configuration Information Table and Notes (continued)

Field	Value	Notes
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: _____._____._____._____	
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: _____._____._____._____	

Table 54. TS7700 Customer Network Configuration Information Table and Notes (continued)

Field	Value	Notes
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 55. 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 56 on page 183 for a list that provides the IP addresses that AOS 3.3 needs to get through the firewall. Refer to Table 57 on page 183 for a list that provides the IP addresses that AOS 4.0 needs to get through the firewall. Refer to Table 58 on page 184 for a list that provides the IP addresses that Legacy ECC Broadband Call Home needs to get through the firewall. Refer to Table 59 on page 184 for a list that provides the IP addresses that Edge ECC Broadband Call Home needs to get through the firewall. Refer to Table 60 on page 184 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 55. 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).

TSSC Remote Support Information

Table 56. 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
aosrelay1.us.ihost.com	72.15.223.60	80, 443, 8200 ¹⁾	Americas Relay
¹⁾ Port 8200 optional only			

Table 57. 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 58. 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 59. 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 60. 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

Table 60. URL table for Fix Download (continued)			
Hostname	IP address	Port	Description
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 264 for important configuration information.

TS7700 Grid local addresses

The following notes apply to [Table 61 on page 186](#).

1. If the TS7700 being installed is a stand-alone machine (not part of a grid configuration), then you should not complete [Table 61 on page 186](#).
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 61. 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 61. 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 61. 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 61. 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 62 on page 189](#) 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 62](#) on page 189 are optional.

Table 62. 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					

Table 62. Summary Table (continued)					
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					

<i>Table 62. Summary Table (continued)</i>					
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 62. 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)					

Table 62. Summary Table (continued)					
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)					

TSSC Grid Configuration Information Table and Notes

The following notes apply to [Table 63 on page 194](#).

- If the TS7700 you are installing is a stand-alone machine (not part of a grid configuration) then leave [Table 63 on page 194](#) 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 63 on page 194](#) blank.
- If the Autonomic Ownership Takeover Manager (AOTM) will not be used, then leave [Table 63 on page 194](#) blank.

- Refer to “Ownership takeover” on page 226 and “The Autonomic Ownership Takeover Manager” on page 226 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 63. 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: _____._____._____._____	
TSSC Grid Interface Gateway	CLUSTER 0: _____._____._____._____	
	CLUSTER 1: _____._____._____._____	
	CLUSTER 2: _____._____._____._____	
	CLUSTER 3: _____._____._____._____	
	CLUSTER 4: _____._____._____._____	
	CLUSTER 5: _____._____._____._____	
	CLUSTER 6: _____._____._____._____	
	CLUSTER 7: _____._____._____._____	

Table 63. TSSC Grid Configuration Information Table and Notes (continued)		
Field	Value	Notes
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 195](#)

If you are a customer, use the checklist in this section to prepare your TS7700 for use after installation.

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 Documentation.

__ 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 publication, available from the web link in the **Related information** section:

- *z/OS DFSMSdfp Storage Administrator Reference*,

Related information

[“Native LDAP using MSAD” on page 245](#)

[“z/OS I/O definitions” on page 82](#)

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 195](#)

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.

- When specifying years the max value is 2000
- When specifying days the max value is 3650
- When specifying hours the max value is 87600

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 2000 years can be specified. Specifying a value of "No expiration" 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 Documentation.
- For TS3500, refer to *Changing the maximum allowable quantity of cartridges in a logical library* in the IBM TS3500 Customer documentation in IBM Documentation.

- __ 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 Documentation.
 - For TS3500, refer to *Changing the quantity of virtual I/O slots in a logical library* in the IBM TS3500 Customer documentation in IBM Documentation.
- __ 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 Documentation.
 - For TS3500, refer to *Adding a drive to a logical library* in the IBM TS3500 Customer documentation in IBM Documentation.
- __ 4. Assign control paths to the logical library.
 - For TS4500, refer to *Using control path drives* in the IBM TS4500 Customer documentation in IBM Documentation.
 - For TS3500, refer to *Enabling or disabling a control path in a logical library* in the IBM TS3500 Customer documentation in IBM Documentation.
- __ 5. Set the Cartridge Assignment Policy.
 - For TS4500, refer to *Assigning or unassigning cartridges* in the IBM TS4500 Customer documentation in IBM Documentation.
 - For TS3500, refer to *Working with a cartridge assignment policy* in the IBM TS3500 Customer documentation in IBM Documentation.
- __ 6. Set Encryption method if necessary.
 - For TS4500, refer to *Choosing or modifying an encryption method* in the IBM TS4500 Customer documentation in IBM Documentation.
 - For TS3500, refer to *Setting up and using encryption* in the IBM TS3500 Customer documentation in IBM Documentation.
- __ 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 Documentation.
 - 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 Documentation.

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 TS7760T and TS7770T configurations, the cluster includes the disk cache and that part of the tape library assigned to the TS7700.

FICON® connections to the host

The following configurations are supported:

- (#0201) 9 Micron LC/LC 31 Meter - This feature provides one 31 meter (101 ft.) 9 micron single mode fibre cable with LC Duplex connectors on both ends, for connection between the Long Wavelength FICON Channel feature and a host system or fibre component long wavelength channel with a 9 micron fibre cable LC Duplex adapter.
- (#0203) 50 Micron LC/LC 31 Meter - This feature provides one 31 meter (101 ft.) 50 micron multimode fibre cable with LC Duplex connectors on both ends, for connection between the Short Wavelength FICON Channel feature and a host system or fibre component short wavelength channel with a 50 micron fibre cable LC Duplex adapter.

TS7700 Tape Attach -- Supported Tape Libraries

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 54](#)

[“TS7760 Storage Expansion Frame” on page 37](#)

[“Upgrades for the TS7760” on page 102](#)

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 15](#) 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.

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.

Note: Each 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. 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 215](#)

[“Feature details” on page 115](#)

[“Selective device access control” on page 235](#)

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.

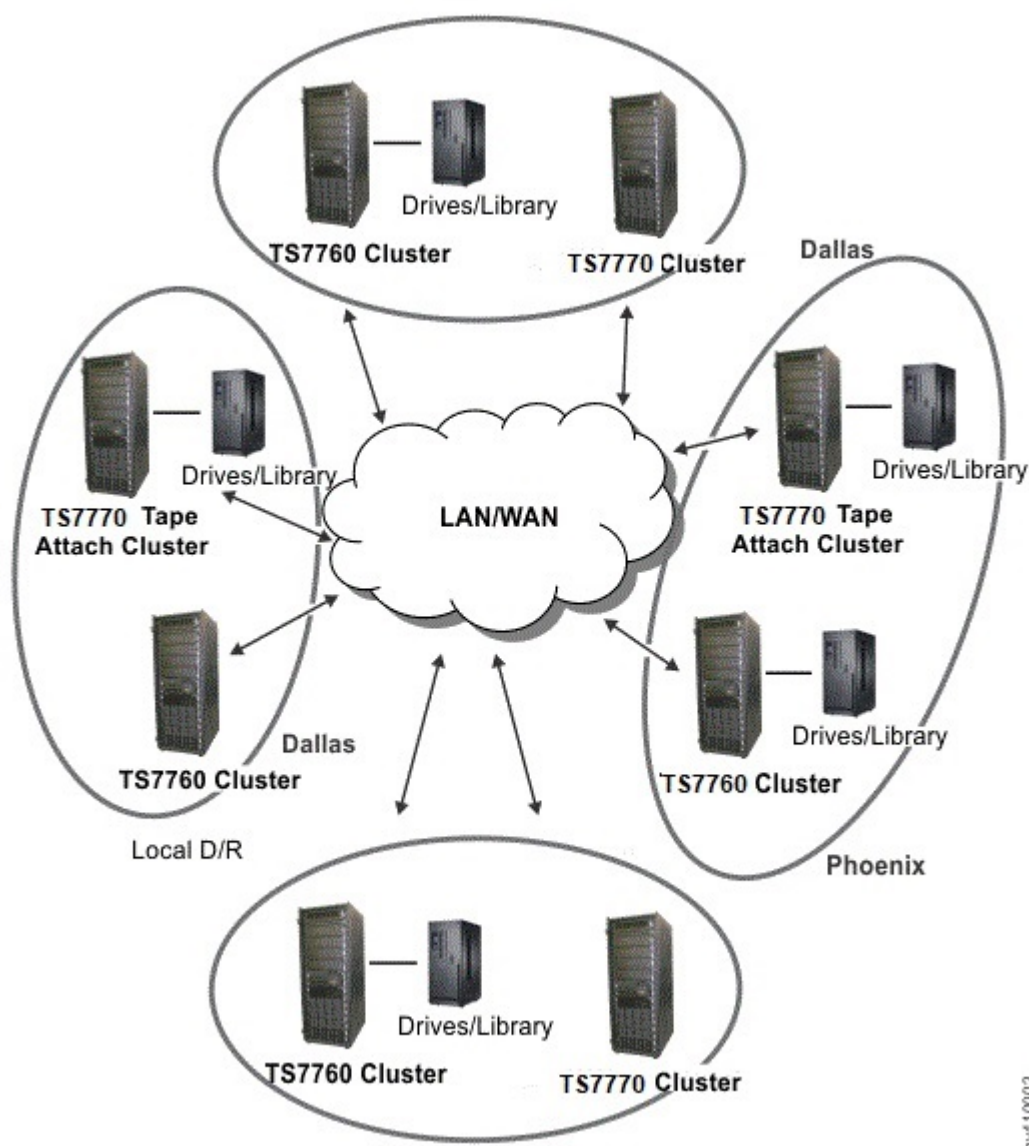


Figure 42. Example of a TS7760 and TS7770 8-way hybrid Grid configuration

Five- or six- cluster hybrid

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.

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.

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.

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.

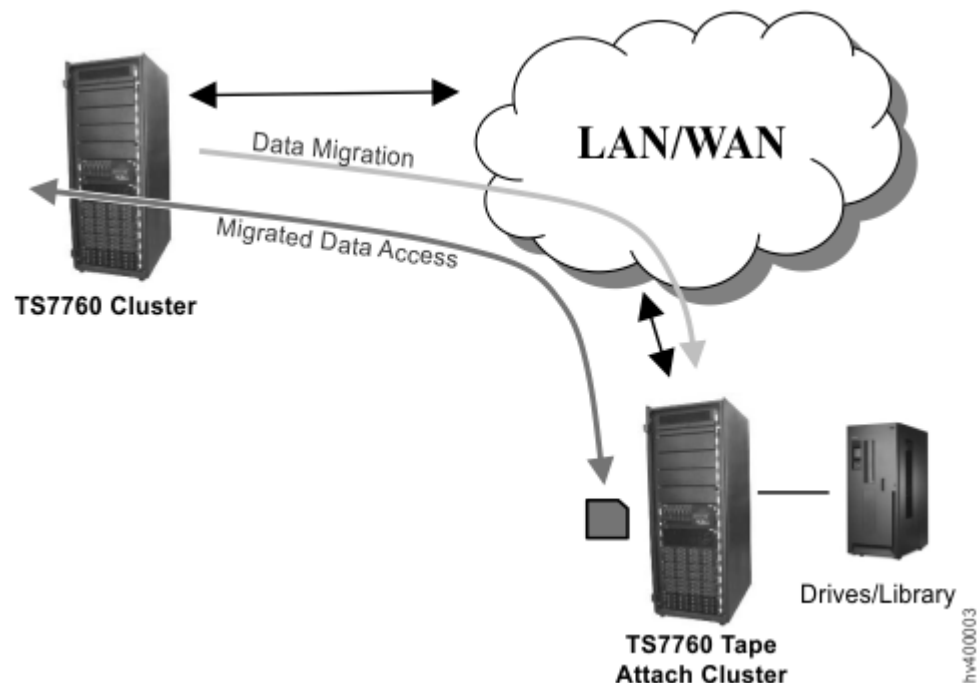


Figure 43. Example of a TS7760 hybrid configuration

Table 64 on page 206 summarizes the possible configurations of a hybrid TS7700 Grid.

Table 64. 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.
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.

Total clusters	Site A	Site B	Site C	Expectations
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” on page 208](#)

[“Copy export overview” on page 112](#)

[“TS7700 Cache thresholds and removal policies” on page 221](#)

[“Retain Copy Mode” on page 219](#)

About cluster families

Cluster families group clusters that operate with a common purpose or under a common set of guidelines.

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.

TS7700C (Cloud)

A TS7700 cluster with Tier Cloud enabled.

TS7700C (Cloud) Requirements, Restrictions, and prerequisites

TS7700 cluster with Tier Cloud, requirements, restrictions and prerequisites.

Requirements:

The following TS7700 Cloud Storage Tier targets are supported:

- IBM Cloud Object Storage (IBM COS, ICOS) on-premise
- Amazon S3 public
- ICOS public with NGINX reverse proxy (via RPQ)
- RStor with NGINX reverse proxy (via RPQ)

For more details, refer to [IBM TS7700 R5.1 Cloud Storage Tier Guide](#).

Restrictions:

- The time on the TS7700 and the cloud endpoint must be synchronized before you perform the tier to Cloud MES.

Note: If the time difference between the TS7700 and cloud endpoint is greater than 10 minutes, then the MES fails.

- If HTTPS will be used, the TLS version must be the same at both the TS7700 and the cloud server to avoid problems with the SSL Certificate Retrieve.

Prerequisites:

- The TS7760 must be at a microcode level of 8.42.x.x or later for cloud support. If the TS7760 is in a grid, then all clusters need to be at 8.42.x.x or later. To check the microcode level either
 - from the TS7700 Management Interface screen, select **Access > Infocenter Setting**. Look for the **Released Code Level** for the current active code or
 - from the TS7700 Management Interface screen, click on the "?" icon and choose "About".
- The TS7760 memory must be upgraded to 64 GB before starting this installation. This is done by using the FC 3466: 32 GB Memory Upgrade.
- The cloud infrastructure (IBM COS or Amazon AWS) needs to be installed and configured before starting this FC 5278 installation.

A cloud container is accessible via a Uniform Resource Locator (URL) which includes either a host's name or Internet Protocol (IP) address. An Amazon web Services (AWS) URL includes an automatically generated host name. A host name is resolved to an IP address by a Domain Name System (DNS). A TS7700's DNS IP address must be specified whether a cloud URL includes a host name.

- The customer network must allow connectivity between the TS7700 GRID network and the IBM COS endpoints or AMAZON region endpoints.
- The cloud account information in [Table 65 on page 209](#) needs to be provided before starting the FC 5278 installation.

Table 65. IP information for the TS7700 cluster and the cloud		
MI fields	Value	Notes
Cloud Pools		
- Nickname	Nickname of a cloud pool	Alphanumeric string up to 8 characters

Table 65. IP information for the TS7700 cluster and the cloud (continued)		
MI fields	Value	Notes
- Cloud Data Format	Standard format	In 8.42.x.x, standard format is supported.
Cloud Accounts		
- Nickname	Nickname of a cloud account	Alphanumeric string up to 8 characters
- Type	Amazon S3 or IBM COS S3	
- Health check	Event , Periodic , or Disable	Health check interval is requested if user selects Periodic . Default value is Event .
- Access Key ID	Access Key ID of Amazon S3 or IBM COS	Access Key ID and Secret Access Key can be created using the Amazon S3 or IBM COS management console. See https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html for Amazon S3 Access Keys. For IBM COS Access Keys, open the Security tab, select an account, click Change Keys , and click Generate New Access Key .
- Secret Access Key	Secret Access Key ID of Amazon S3 or IBM COS	
- Notes		
Containers		
- Container name	Name of Amazon S3 bucket or IBM COS vault	This name must exactly match the name of the COS vault or AWS bucket that has already been established by the customer. Note: Container names must not contain uppercase characters or underscores. Amazon S3 bucket or IBM COS vault needs to be created before creating a container on TS7700. For Amazon S3 bucket, select one of the regions in the link: https://www.ibm.com/docs/en/spectrum-scale/5.0.1?topic=services-managing-cloud-storage-account If Amazon S3 bucket is created in a region not listed in the link, cloud tier configuration will fail.
- Cloud Pool		
- Cloud Account		

Table 65. IP information for the TS7700 cluster and the cloud (continued)		
MI fields	Value	Notes
- Cloud URL	URL of IBM COS accessor nodes	This information is not needed for Amazon S3. The Cloud URLs for COS systems are the addresses for the Accesser devices.
- Cloud URL	URL of IBM COS accessor nodes	
..	URL of IBM COS accessor nodes	
..	URL of IBM COS accessor nodes	
..	URL of IBM COS accessor nodes	
- Cloud URL	URL of IBM COS accessor nodes	
- Cloud URL	URL of IBM COS accessor nodes	
Certificate Alias	SSL certificate alias to be used for https access.	SSL certificate needs to be imported from the cloud storage before setting certificate alias. To import a SSL certificate on TS7700, go to Access > SSL Certificates and click New Certificate . Then, select Retrieve certificate from server , press Next , enter IP address or a hostname of the cloud storage endpoint, press Next , enter Alias , and press Finish .
- Cluster Association for Cloud URL		
- Cluster Association for Cloud URL		

- For merge and join:

In table 2, "cloud enabled" means the FC MES 5278 has been completed. Some possible merge situations are

- two Cloud enabled clusters or
- a Cloud enabled cluster with a grid containing at least one Cloud enabled cluster or
- two grids each with at least one Cloud enabled cluster

where one party (either cluster or grid) MUST NEVER HAVE had a Cloud Pool created.



Warning: If you intend on joining a cloud enabled cluster to an existing grid, that cluster must not have any configured cloud settings.

Table 66. TS7700 4.2 GA support for joins and merges			
Type	Joining/Merging Cluster(s)	Existing Cluster(s)	4.2 GA Supported?
Join	No Cloud Enabled	No Cloud Enabled	Yes
Join	Cloud Enabled	No Cloud Enabled	Yes*
Join	No Cloud Enabled	Cloud Enabled	Yes
Join	Cloud Enabled	Cloud Enabled	Yes*
Merge	No Cloud Enabled	No Cloud Enabled	Yes

Table 66. TS7700 4.2 GA support for joins and merges (continued)			
Type	Joining/Merging Cluster(s)	Existing Cluster(s)	4.2 GA Supported?
Merge	Cloud Enabled	No Cloud Enabled	Yes
Merge	No Cloud Enabled	Cloud Enabled	Yes
Merge	Cloud Enabled	Cloud Enabled	Yes**

* = Only supported if the joining cluster does not have any configured cloud pools, cloud accounts, containers, or URLs.

** = Only supported if the resulting grid contains no more than one cloud pool and no more than 256 items for each of the following: cloud accounts, containers, cloud URLs, and cluster associations.

- The following Feature Keys is needed PRIOR to starting the MES script. These keys must be provided and the installation instruction documents explain how to install them using the **TS7700 Management Interface**

Feature Keys for this II:

- FC 5278 - Cloud Enablement
- FC 5274 - Enable 1 TB Active Premigration Queue (minimum 1 FC required, maximum 10)

Note: You must install 10 FC 5274s before installing FC 5279.

- Optional

FC 5279 - 5 TB Active Premigration Queue (maximum 10)

Note: FC 5279 is an optional start for the MES.

Postinstallation:

This post instruction is for GRID only.

Network traffic to and from the cloud can interfere with the native TS7700 load balancing algorithm for normal Grid copies. If your network sees an unusual number of warnings about DegradedGrid links after the activation of FC 5278, then contact Service to establish a more reasonable threshold for these warnings.

Possible solutions: Reduce the NTC default 60% value to a lower value to minimize the false warnings or disable the check altogether by setting the threshold to 0%.

TS7700C (Cloud) Configuration

TS7700 Cloud configuration

TS7700C configuration consists of the Cloud Storage Service provider, a TS7700 with FC 5278 and GRID network connection.

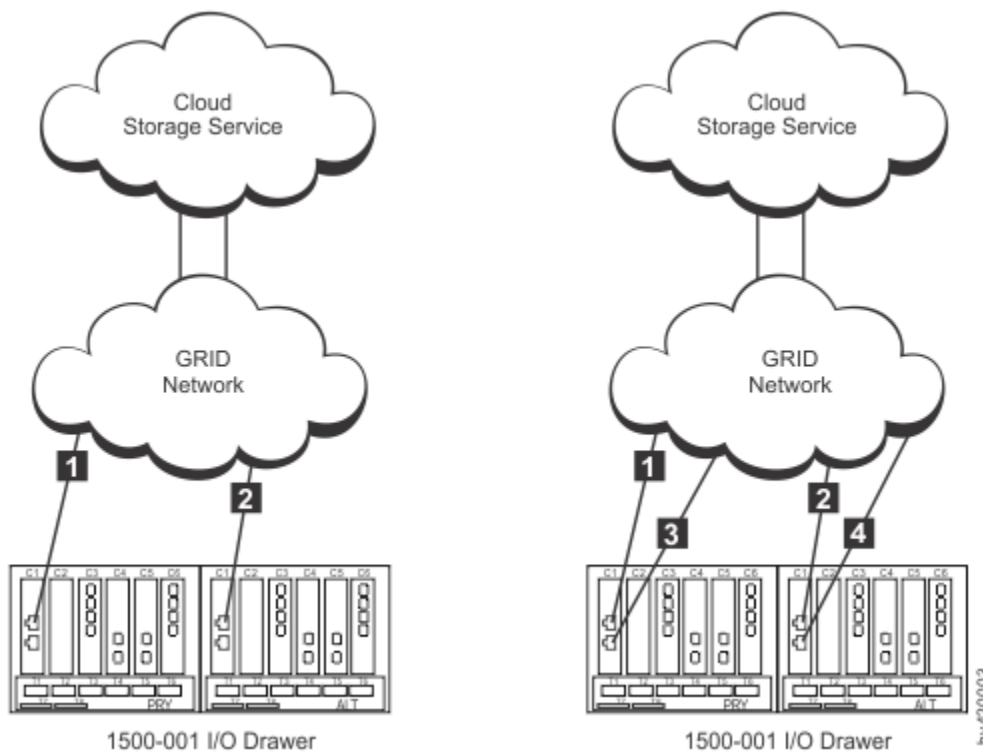


Figure 44. TS7700 3957-VEC stand-alone with 2 or 4 Ethernet connections

The TS7700C is created by installing and configuring the FC 5278 cloud enablement on a running TS7700.

Customer responsibility before an FC 5278 installation:

1. The Cloud Storage Service provider must be installed, configured, and, accessible. (IBM COS or Amazon ASW)
 - The information used to configure for the Cloud Storage Service is also used to enable FC 5278.
 - The information is added to [Table 65 on page 209](#) of the FC 5278 instructions.
2. Cables
 - (Stand-alone cluster) Ethernet cables or Fiber cables (Fiber over Ethernet) will need to be installed and configured to the network.
 - (GRID) - No additional cables needed.
 - Verify that all clusters in the GRID are at 8.42.x.x or higher.

FC 5278 installation process:

1. Customer installs the feature codes by using the TS7700 MI.
 - FC 5278 - Cloud enablement.
 - FC 5274 - 1 TB Active Premigration Queue (at least one is required).
 - FC 5279 - 5 TB Active Premigration Queue (Optional after 10 FC 5274 have been installed).
2. Customer stops I/O activity before the FC 5278 installation.
3. Service conducts the following:
 - a. Installs additional 32 GB of memory
 - b. (Stand-alone only) Connect ethernet/fiber cables to TS7700.
 - Configure the GRID IPs for cloud.

- c. (cluster in a GRID) - check for fenced clusters. - Service prep
 - d. Offline cluster
 - e. Conduct the Cloud MES.
 - f. Online the cluster
4. Customer can start I/O.
 5. Customer sets up cloud accounts and configure pools, containers, and storage groups.
NOTE: There will need to be connectivity between the TS7700 GRID network and Cloud network.
Conduct a ping test for connectivity.
 6. Service tests the TS7700.
 7. The Cloud MES is complete.

Cloud export recovery

Use this page to recover stored virtual volumes for restoration of data.

Before initiating a cloud export recovery process, ensure the following:

1. All VEC/VED's are at R5.1 or higher code level.
2. A copy of the database is required for recovery purposes.
3. All devices are offline to the host throughout the process.
4. Gather information about the last backup needed for recovery.

To recover a copy of a virtual volume for disaster recovery purposes, perform the following steps:

1. Select **Service > Cloud Export Recovery**.
2. Enter the following: **Container ID** of the volume to be restored.

Container ID

The id of the volume to be restored.

Serial number of the original TS7700

The serial number of the corrupted TS7700.

Cloud backup ID

The ID of the backup volume version.

Test Mode

Toggle to enable or disable disaster recovery testing.

3. Click **Recover Cluster**.

The TS7700 locates a backup list for the cluster serial number and then backup ID from the list to retrieve the object name. Once the correct backup is located, the database backup from the cloud is imported and the recovery process begins.

4. If data is detected data in the system (meaning, logical volumes exist), the system must be cleaned up before the recovery can continue.

Option	Description
Yes	To continue with the recovery process.
No	To cancel the recovery process.

Note:

- Cloud credentials related to the container ID are preserved.
- If the new cloud pool or account names match names in the restored database, the new credentials will overwrite the old.

During the restore process:

- The TS7700 is taken offline and brought back online when restore completed.
 - The Cloud Export Recovery page displays a status of the operation.
5. To cancel the recovery process, click **Cancel**.

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 119](#), and [“FC 4017, Cluster Cleanup” on page 119](#). Following removal and cleanup, the TS7700 Cluster can be relocated and reused.

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 119](#) 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 119](#).

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 119](#) 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 54](#)

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.

Related information

[“Planning for virtual and physical volumes” on page 88](#)

[“Workload considerations” on page 52](#)

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.

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 by 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. Before 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). Before 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 is 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:

<i>Table 67. WWID and write-mount count scenarios.</i> 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.

Table 67. WWID and write-mount count scenarios. Table describes conditions of host write-mount count scenarios. (continued)

If	Then	Result
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. Retention concepts that prevent early expiration by using fixed durations or DFSMS HDR1 expiration dates was introduced in 8.51.1.X release. For details, refer to [white paper](#).

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 EOVS 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 112](#)

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 68. 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

Table 68. Effects of Retain Copy Mode in mount scenarios. Table describes scenarios and results for Retain Copy Mode settings. (continued)

Scenario	Retain Copy Mode setting enabled?	Result
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 112](#)

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 45 on page 221](#) depicts the order in which copy types are acquired to satisfy incoming copy queue requests.

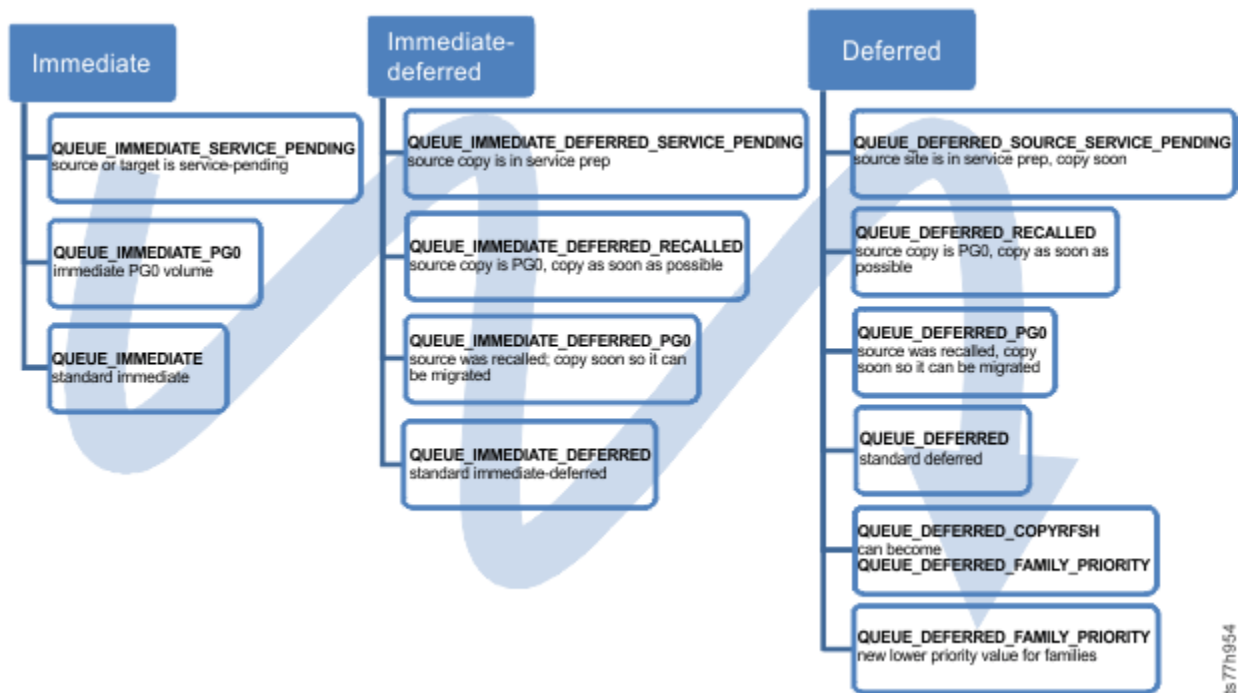


Figure 45. Order of copy queue prioritization

Related information

[“Access and location of virtual volume data” on page 3](#)

[“Virtual volume copy availability” on page 4](#)

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,SETTING,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,SETTING,CACHE,REMOVTHR,{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:

- LMTDTHR was introduced in [White Paper - TS7700 Library Request Command](#).
- 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 69 on page 223](#) displays the start and stop thresholds for each of the active cache capacity states defined.

Table 69. 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 TB) ²	>(X + 1.5 TB) ²	Console message
Notelist: 1. When enabled 2. Where X is the value given by the <i>TS7700 Temporary Removal Threshold</i> for the given cluster.			

Volume removal policies in a grid configuration

Removal policies 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.

Note: 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

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,REMOVTHR,{VALUE}
```

Temporary Removal Thresholds

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 203](#)

[“Virtual volume data” on page 216](#)

The following features describe data stored on virtual volumes.

[“Merging clusters or grids” on page 94](#)

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 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 Tape Attach environment can be designated for time-delayed premigration.

Related information

[“Virtual volume data” on page 216](#)

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.

Note: 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.

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.

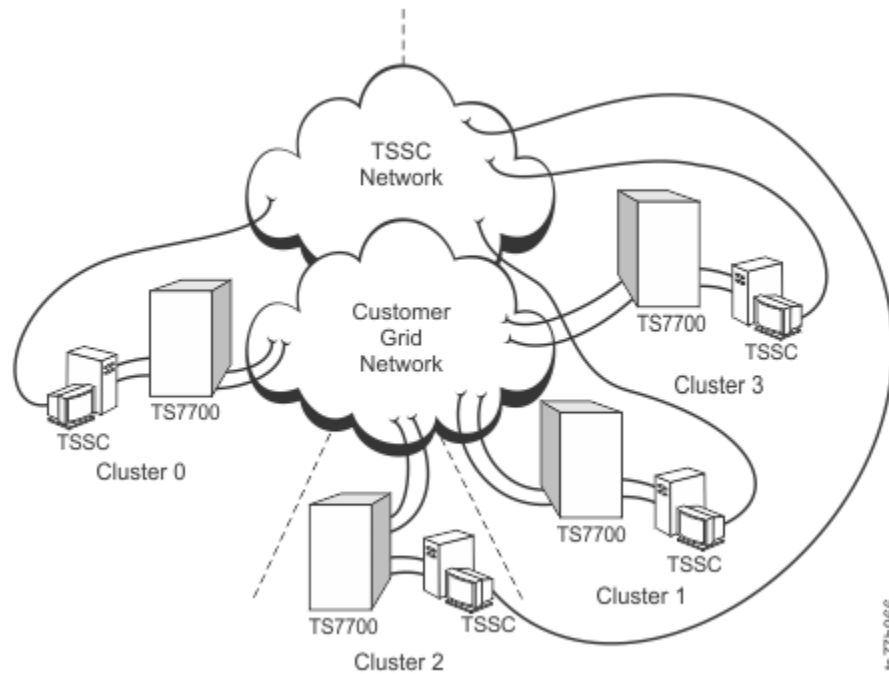


Figure 46. Autonomic Ownership Takeover Manager configuration for four clusters

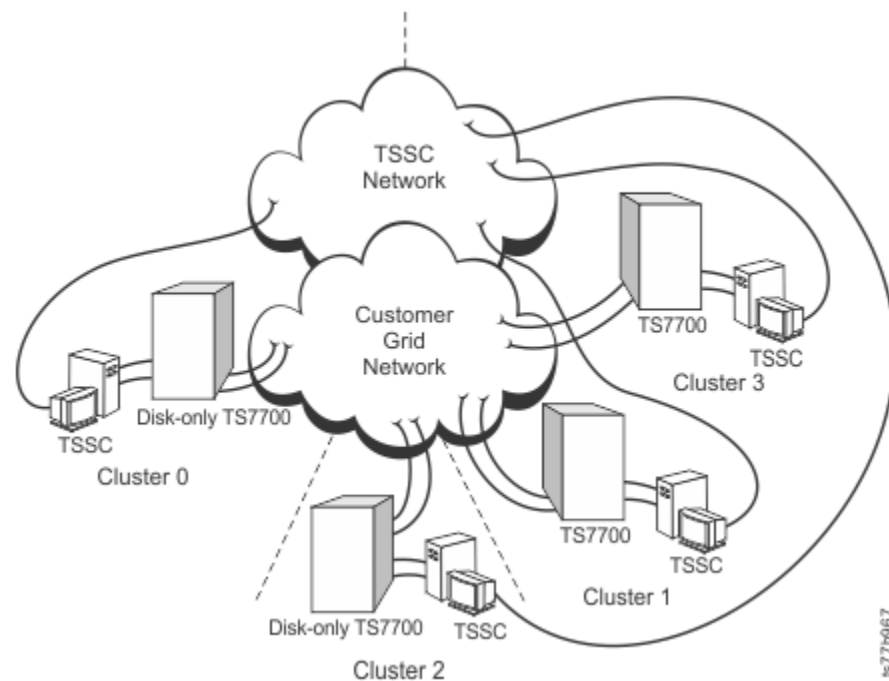


Figure 47. Autonomic Ownership Takeover Manager configuration for four clusters in a hybrid grid

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 48 on page 228 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.

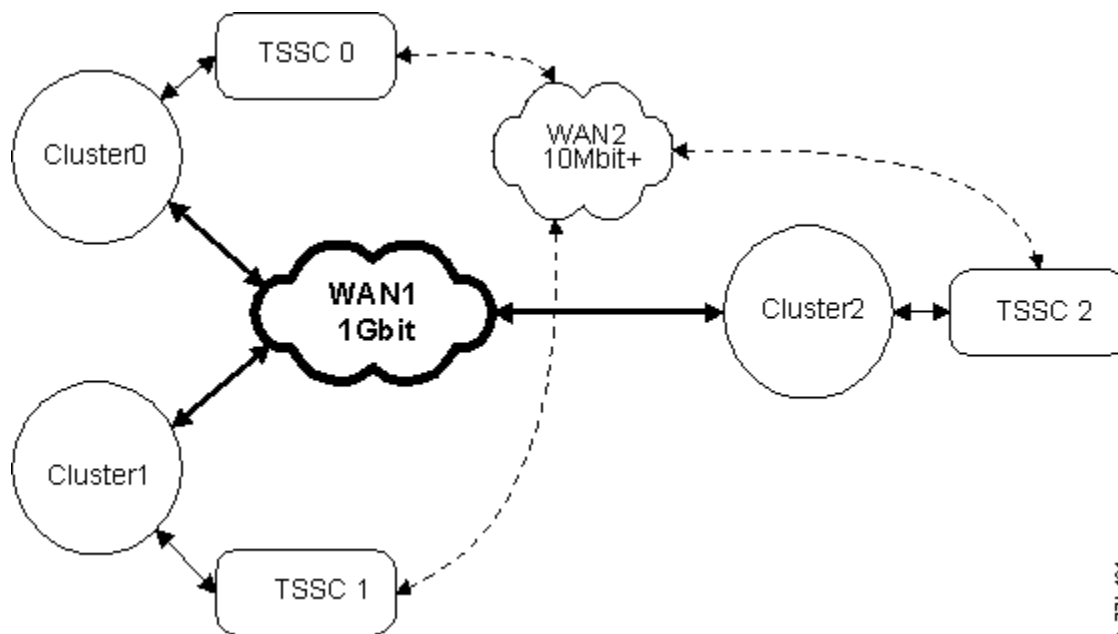


Figure 48. Autonomic Ownership Takeover Manager configuration in a three-cluster Grid

Table 70 on page 228 displays the conditions under which AOTM takes over a failed cluster.

Table 70. 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	
Down	Down	Yes	Not applicable	Connected	Down	Connected	

<i>Table 70. Conditions under which AOTM takes over a failed cluster (continued)</i>							
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	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 71 on page 229 displays the conditions under which AOTM does **NOT** takeover a failed cluster.

<i>Table 71. Conditions under which AOTM does not takeover a failed cluster</i>							
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, DFSMSdftp 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 DFSMSdftp 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

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 72 on page 232 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 72. 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 on page 232	Results when one or both "S" locations are unavailable at mount time ² on page 232			
			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 on page 232	No	No	Yes
3	Private	Disabled	N/A	Set	N/A	Both	Yes	Success ³ on page 232	No	Yes	No
4	Private	Enabled	N/A	Set	N/A	Both	Yes	Success ³ on page 232	No	No	Yes
5	Private	Disabled	N/A	N/A	Set	Both ⁴ on page 232	Yes ⁵ on page 232	Success ³ on page 232	No	Yes ⁵ on page 232 ⁷ on page 232	No ⁶ on page 232
6	Private	Enabled	N/A	N/A	Set	Both ⁴ on page 232	Yes ⁵ on page 232	Success ³ on page 232	No	No	Yes
7	Private	Disabled	Set	N/A	N/A	Single	No	Success ³ on page 232	No	No	Yes
8	Private	Enabled	Set	N/A	N/A	Single	No	Success ³ on page 232	No	No	Yes

Notelist:

- Any delay due to a paused state is applicable only if a recall is required.
- Assumes at least one healthy (and consistent for private mount) cluster when both 'S' locations are unavailable.
- The best TVC choice (preferring locations in this order: "S", "R", "D", and "T") is used to satisfy the mount before it continues.
- With *Open both copies on z/OS implied update* specified: Both when requested by the host; Single when not requested by the host.
- With *Open both copies on z/OS implied update* specified: Yes when requested by the host; No when not requested by the host.
- With *Open both copies on z/OS implied update* specified: No when requested by the host; Yes when not requested by the host.
- 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 (ROR) 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 ROR for recovery. HSM requires that a certain number of drives be available for a period of time before ROR 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 ROR recovery of that physical volume to the next hourly cycle.

In a TS7700 Grid configuration, if a virtual volume cannot be recovered from the ROR 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 enabled by default. 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.

Before SAA is visible or operational, all of the following must be true:

1. 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.

2. 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 219](#)

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 115](#)

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 restriction applies:

- 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 230](#)

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 202](#) 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.

Cloud export for disaster recovery

The cloud export function allows copies of virtual volumes to be stored for disaster recovery purposes.

Using the Cloud export you can take a snapshot of the TS7700 database, which contains all the information needed to recover a TS7700, and store it in a cloud storage device. The benefit of the cloud export function is that you are not required to move data offsite. Instead, the cloud device itself is considered the offsite facility.

Note: Cloud export is only supported on VEC/VEDs in a grid that are at R5.1 code level.

By creating cloud pools to segregate data, logical volumes can be assigned and ranked through policy management.

Prior to R5.1, the TS7700 did not keep versions of logical volumes directly. There are some situations where two versions of data can be stored for a short period of time but this is not done for the specific reason to keep versions.

When the TS7700 implemented Cloud Storage Tier in R4.2, a logical volume is written or appended, placed in the premigration queue, and then copied to the Cloud associated with that pool. If that logical volume is modified or deleted, and has reached its expiration, HSM marks the cloud data as ready to be deleted but does not immediately delete it. Instead, it creates a new version of the data in the cloud and the old version is left to be cleaned up by a different process.

HSM has a process that runs once an hour to delete those volumes marked for deletion. Therefore, more than one version of a volume can exist in the cloud storage device for a short time.

In R5.1, a user can select how many days to preserve a version of a volume by setting the number of retention days when a cloud pool is created.

Note: All VEC/VED's in a grid must be at R5.1 or higher code level before this versioning feature can be used.

There are three main scenarios where cloud volume versioning periods might be used:

- When volumes are delete-expired, ejected or deleted
- When volumes are appended
- When determining whether to retain Cloud Export Backups

Running the cloud export function will depend on your specific requirements and can be set at scheduled intervals or following the completion of a batch job.

For information about storing and recovering data from a virtual volume, refer to [“Cloud export” on page 238](#) and [“Cloud export recovery” on page 214](#).

Cloud export

Use LIBRARY EXPORT command to capture a database snapshot that can be used as a recovery restore point.

Consideration must be given for how long it will take to complete a Cloud Export process if scheduling frequently. It could take minutes or hours depending on the size of the premigration queue.

Tip: Keeping frequent backups will ensure a tighter restore point.

To run a cloud export process, issue a **LIBRARY EXPORT <volser>** command from the host.

Note: The **LIBRARY EXPORT** command requires a VOLSER be specified when invoked. This VOLSER is a logical volume that contains the following three files:

Export List

Contains instruction on the logical volumes that should be exported from the VTS. For Cloud Export, the logical volumes are derived by listing the Cloud Pools they are associated with. A maximum of 80 characters per line is supported in this file.

Reserved

The reserved file does not contain any information and only contains a header that identifies it as the reserve file. The reserve file is required to exist.

Export Status

The status file is an empty file that the TS7700 will use to return information about the database backup that was taken as well as a list of logical volumes exported. A maximum of 900 characters per line is supported in this file for Cloud Export results.

Notice: If any of these three files are missing from the volume, the LIBRARY EXPORT will fail.

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 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 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.
- 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 203

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 203](#)

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 202](#) 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.

CUIR automation

The control unit initiated reconfiguration (CUIR) function is a LI REQ enabled operation that enables service and unhealthy device information to be automatically communicated with attached z/OS hosts. It automates offline or online device actions to minimize manual operator intervention during selected service actions as well as unhealthy cluster outages during fence operations.

Service preparation

When service-prep is initiated on the cluster, a Distributed Library Notification is surfaced from the cluster. It requests the attached host to vary off the devices automatically when the following conditions are met:

- All clusters in the grid are at microcode level 8.41.200.xx or later.
- One or more attached z/OS host logical partitions support CUIR service vary function (APAR OA52376).
- The CUIR function is enabled by using the following LI REQ command:

```
LIBRARY REQUEST,library-name,CUIR,SETTING,SERVICE,ENABLE
```

When service is canceled and the local cluster comes online, a Distributed Library Notification is surfaced from the cluster. It requests the attached host to vary on the devices automatically when the following conditions are met:

- All clusters in the grid are at microcode level 8.41.200.xx or later.
- One or more attached host logical partitions supports CUIR service vary function (APAR OA52376).
- The CUIR service vary offline attention was previously surfaced as mentioned above.
- The AONLINE service notification is enabled from the command line, by using the following LI REQ command:

```
LIBRARY REQUEST,library-name,CUIR,AONLINE,SERVICE,ENABLE
```

If the AONLINE SERVICE notification is disabled by the LI REQ command **LIBRARY REQUEST,library-name,CUIR,AONLINE,SERVICE,DISABLE**, then a blue informational icon is shown on the lower left corner of the cluster image. It alerts the user that the cluster's devices need to be varied online manually.

1. Select **Vary Devices Online** from the **Actions** menu in the cluster summary panel.
2. Select the cluster you want to vary devices online for and then click **OK**. Click **Cancel** to exit without varying devices online.

Unhealthy/fence vary

When a fence operation is initiated on the cluster due to an unhealthy condition or manual fence operation, a Distributed Library Notification is surfaced from one or more clusters. It requests the attached hosts to vary off the devices automatically to the unhealthy cluster when the following conditions are met:

- All clusters in the grid are at microcode level 8.52.1xx.xx or later.
- The attached host logical partition supports the CUIR unhealthy vary function (APAR OA60929).
- The CUIR fence function is enabled using the following LI REQ command:

```
LIBRARY REQUEST,library-name,CUIR,SETTING,FENCE,ENABLE
```

When the cluster is unfenced and the unhealthy cluster returns to an online state, a Distributed Library Notification is surfaced from the previous unhealthy cluster. It requests the attached hosts to vary on the devices automatically when the following conditions are met:

- All clusters in the grid are at microcode level 8.52.1xx.xx or later.
- The attached host logical partition supports CUIR unhealthy vary function (APAR OA60929).
- The CUIR unhealthy vary offline attention was previously surfaced as described above.
- The AONLINE fence notification is enabled by using the following LI REQ command:

```
LIBRARY REQUEST,library-name,CUIR,AONLINE,FENCE,ENABLE
```

If the AONLINE FENCE notification is disabled by the LI REQ command **LIBRARY REQUEST,library-name,CUIR,AONLINE,FENCE,DISABLE**, then a blue informational icon is shown on the lower left corner of the cluster image. It alerts the user that the cluster's devices need to be varied online manually.

1. Select **Vary Devices Online** from the **Actions** menu in the cluster summary panel.
2. Select the cluster you want to vary devices online for and then click **OK**. Click **Cancel** to exit without varying devices online.

Note: Only after a cluster has exited the fenced state, the CUIR fence vary online attention is attempted. You may need to manually unfence the cluster before devices can be varied online. .

For detailed information on CUIR, refer to [TS7700 Series CUIR Users Guide](#).

Security

The topics in this section provide information about security protocols for the TS7700.

Policies can be assigned on a per cluster basis. One cluster can employ local authentication, while a different cluster within the same grid domain can employ an external policy. Also, each cluster in a grid can operate its own external policy. However, only one policy can be enabled on a cluster at a time.

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).

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.

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.

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.

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) Define the following required Direct LDAP values:
 - Policy Name
 - Primary Server URL
 - Base Distinguish Name
 - User name Attribute
 - f) 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 243.
 - 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.

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

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) Spectrum Control to manage RBAC, refer to the topic [“System Storage Productivity Center and Spectrum Control ” on page 247](#).

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 243](#) 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 SDBM 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.

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.

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 [https://www-01.ibm.com/servers/resourceink/svc00100.nsf/pages/zOSV2R3sc236788/\\$file/glpa200_v2r3.pdf](https://www-01.ibm.com/servers/resourceink/svc00100.nsf/pages/zOSV2R3sc236788/$file/glpa200_v2r3.pdf).
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” on page 246.](#)

Related information

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.

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.

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**.

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.

System Storage Productivity Center and Spectrum Control

You can use the System Storage Productivity Center (SSPC), a server operating with the Spectrum Control 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 Spectrum Control 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 Spectrum Control. The SAS client is integrated into the TS7700 microcode, while the SAS server and the WebSphere Federated Repositories are integrated into Spectrum Control. Spectrum Control 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 Spectrum Control, 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 Spectrum Control 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 Spectrum Control, which forwards the authentication status through the SAS to the requesting device. The MSAD server that is attached to the SSPC or Spectrum Control 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 Spectrum Control, 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 Spectrum Control security features, including the external topic *Using Microsoft Active Directory for authentication*.

Related information

[“Connecting to the management interface” on page 281](#)

[“Establish a connection to the Storage Authentication Server” on page 248](#)

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.

Note: If Https is used, the TLS version must be the same at both the TS7700 and the Cloud Server in order to avoid problem with the SSL Certificate Retrieve.

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 281](#)

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 249.
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 73 on page 250](#) to identify a specific trap type present on the MIB log.

<i>Table 73. SNMP MIB definitions</i>	
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).
hydAddAccessGroupVolumeRange s	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.
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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
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.
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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
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.
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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
hydForce3957Offline	This trap is sent when a SMIT command is executed. It logs when a 3957 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.
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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
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.
hydPrepareNonConcurrentLoad	This trap is sent when a SMIT command is executed. It the log preparation of a non-concurrent disk cache 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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
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.
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 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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
hydRunFibreSwitchUtility	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.
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 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 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.

Table 73. SNMP MIB definitions (continued)

Trap type	Description
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 73. 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

Table 73. SNMP MIB definitions (continued)

Trap type	Description
hydType (continued)	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 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 is varied offline on the TS7700.
hydVary3957Online	This trap is sent when a SMIT command is executed. It logs when the 3957 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.

Table 73. SNMP MIB definitions (continued)	
Trap type	Description
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 281](#)

Remote support security

The topics in this section describe remote support security for the TS7700.

Related information

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 Cognitive Support Platform (CSP). Call Home uses a broadband internet connection to perform this “Dial-Out” function.

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 CSP
- Graphical user interface for configuring, backing up, and restoring system console settings

Note: For customer functions, go to [“System console management GUI”](#) on page 265.

The TSSC provides Ethernet outbound connectivity through the customer's network to CSP. The TSSC uses the following protocols to port numbers, as shown in [Table 74](#) on page 262:

- 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.

<i>Table 74. TSSC External Port Information</i>			
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 CSP. 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. CSP 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 CSP 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, CSP 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 49 on page 263 is a representation of a potential connection scheme for the TSSC.

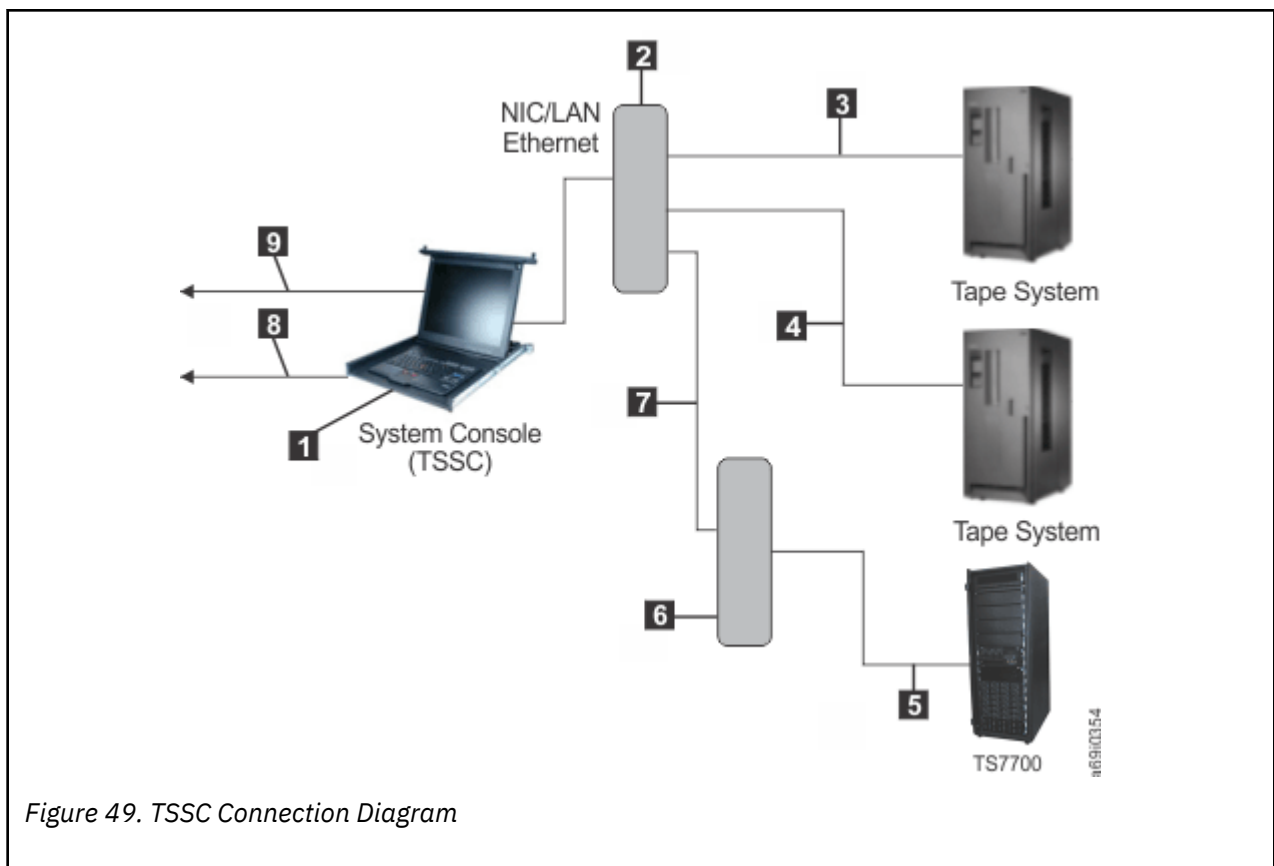


Table 75. TSSC Components

1 Serial connector	6 Ethernet expansion FC2714
2 Ethernet switch FC 2704/FC2732	7 Cable supplied with FC2714
3 Cable supplied with FC 2704/FC2732	8 Second modem (not on all RMSS products)
4 Cable supplied with FC 2715	9 Customer supplied Ethernet connection
5 Cable supplied with FC2714	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.

Logging in to the system console

This topic provides instructions for logging into the system console.

To login to the system console locally, see [“Logging in locally” on page 264](#). To login to the system console remotely, see [“Logging in remotely” on page 264](#).

Logging in locally

This topic provides instructions for logging into the system console locally.

To log in to the system console locally, perform the following steps:

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.

You can access the system console remotely through a web browser.

Refer to the following table for a list of supported browsers.

Table 76. 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

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.

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.

Note: If Https is used, the TLS version must be the same at both the TS7700 and the Cloud Server in order to avoid problems with the SSL Certificate Retrieve.

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:
 - i) Enter the certificate name in the **Alias** field.
 - ii) Enter the server URL in the **Server URL** field.
 - iii) Enter the server port in the **Port** field.
 - iv) Click **Retrieve Certificate**.
 - b) To upload a certificate, under the Proxy Certificates heading:
 - i) Click **Browse** to locate the file.
 - ii) 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.

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.

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.

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.
1. From the System console management GUI, click **Access > Security SettingsConsole Settings > Security Settings**.
A screen appears with options to add users, delete users, or change user passwords.
 2. From the Authentication PoliciesAdminister Users area, choose the appropriate option that you want to use.

Adding a user

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 minimum, and at least one uppercase letter, one lowercase letter, one number, and one special character (for example, !?%&).

3. Click **Add**.

Deleting a user

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

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 minimum, and at least one uppercase letter, one lowercase letter, one number, and one special character (for example, !?%&).

3. Click **Change**.

Changing a user role

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

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.

To enable or disable SNMP trap forwarding, follow these instructions:

Enabling SNMP trap forwarding

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

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.

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 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.

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.

Use the **Attached Systems** page to add or delete an attached system, or to monitor an attached system.

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.

Use the **RSYSLOG Settings** page to configure the RSYSLOG settings.

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.

Use the **Log Settings** page to view or download log files.

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.

Use the **Custom Firewall Settings** page to customize firewall settings.

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.

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.

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.

Use the **Test ECC Connectivity** page to test the Call Home (CSP) connection.

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.

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.

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.

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.

Supported Certificate File Types:

TSSC/IMC accepts the following types of certificates that are based on the X.509 standard.

- Base64-encoded X.509 Certificate (.cer, .pem or .crt)
- DER-encoded binary X.509 Certificate (.cer, .der or .crt)

Supported One-way Hash Functions (for public keys contained in a certificate.)

- MD5, SHA, SHA1, SHA224, SHA256, SHA384 and SHA512
Supported Signature Algorithms (for public keys contained in a certificate.)
- RSA, DSA, ECDSA

The following file types are not supported:

- Cryptographic Message Syntax Standard (PKCS#7) Certificate (.p7b, .p7r or .spc)
(It is generally used by the CA to provide certificate chain to clients.)
- Certification Revocation List (.crl extension)
(It identifies whether a certificate has been revoked or not.)

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

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 base distinguished name (Base DN) that uniquely identifies a set of entries in a realm of both users and groups. This field is required but blank by default. The value in this field is composed of one to 254 Unicode characters.

Example: DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com

Bind Distinguished Name (Optional)

The LDAP bind distinguished name (Bind DN) is an object that you bind to inside LDAP to give you permission to access. Most of LDAP instances doesn't allow anonymous binds. Therefore, a bind DN must

be specified in case of a simple authentication with the password. The value in this field is composed of one to 254 Unicode characters.

Example: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com

Bind Password (Optional)

The bind password must be specified for the Bind DN in case of simple authentication.

Username Attribute

The attribute name that is 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.

Example: In case of the following example(Microsoft Active Directory), "cn" or "sAMAccountName" can be specified as the username attribute.

```
$ ldapsearch -x -H ldaps://beat.gdl.mex.ibm.com:636 -w "*****" -D
"CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" -b
"DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" "(&(objectClass=person)(cn=FVT3))"
....
dn: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
objectClass: person
....
objectClass: user
cn: FVT3
....
distinguishedName: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
sAMAccountName: FVT3
.....
```

Group Member Attribute

The attribute name that is used to identify group members. The group members in this attribute must be provided as the user distinguished name (CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com for example.). This field is optional and contains the value member by default. This field can contain up to 61 Unicode characters.

Example: In case of the following example(Microsoft Active Directory), "member" can be specified as the group member attribute.

```
$ ldapsearch -x -H ldaps://beat.gdl.mex.ibm.com:636 -w "*****" -D
"CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" -b
"DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" "(&(objectClass=group)(cn=TS4500_NEW))"
....
dn: CN=TS4500_NEW,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
objectClass: group
cn: TS4500_NEW
member: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
member: CN=RVT2,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
```

Group Name Attribute

The attribute name that is 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.

Example: In case of the following example(Microsoft Active Directory), "cn" or "sAMAccountName" can be specified as the group name attribute.

```
$ ldapsearch -x -H ldaps://beat.gdl.mex.ibm.com:636 -w "*****" -D
"CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" -b
"DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" "(&(objectClass=group)(cn=TS4500_NEW))"
....
dn: CN=TS4500_NEW,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
objectClass: group
cn: TS4500_NEW
member: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
member: CN=RVT2,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
distinguishedName: CN=TS4500_NEW,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
```

```
....
SAMAccountName: TS4500_NEW
....
```

Username filter

Used to filter and verify validity of an entered username. This field is optional and contains the value (cn=*) by default. This field can contain up to 254 Unicode characters.

Example: Refer the attribute values for each user instances.
"(cn=*)", "(cn={0})", "(objectClass=user)" or "(objectClass=person)" can be specified as the filter.

```
$ ldapsearch -x -H ldaps://beat.gdl.mex.ibm.com:636 -w "*****" -D
"CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" -b
"DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" "(&(objectClass=person)(cn=FVT3))"
....
dn: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
objectClass: person
....
objectClass: user
cn: FVT3
....
distinguishedName: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
SAMAccountName: FVT3
.....
```

Group Name filter

Used to filter and verify validity of an entered group name. This field is optional and contains the value (cn=*) by default. This field can contain up to 254 Unicode characters.

Example: Refer the attribute values for each group instances.
"(cn=*)" or "(objectClass=group)" can be specified as the filter.

```
$ ldapsearch -x -H ldaps://beat.gdl.mex.ibm.com:636 -w "Passw0rd123456" -D
"CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" -b
"DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com" "(&(objectClass=group)(cn=TS4500_NEW))"
....
dn: CN=TS4500_NEW,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
objectClass: group
cn: TS4500_NEW
member: CN=FVT3,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
member: CN=FVT2,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
member: CN=FVT,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
distinguishedName: CN=TS4500_NEW,CN=Users,DC=beat,DC=gdl,DC=mex,DC=ibm,DC=com
....
SAMAccountName: TS4500_NEW
.....
```

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 Spectrum Control

You can use the System Storage Productivity Center (SSPC), a server operating with the Spectrum Control 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.

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.

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.

Use the remote support center settings page to customize remote support center settings.

1. From the System console management GUI, select **Console Settings > Remote Support Center 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 77 on page 278](#).
- 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 77. 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.

Use the **Network Information** page to view information about the systems network connections.

1. From the System console management GUI, select **Network Information**.
2. Refer to [Table 78 on page 278](#) for information available from the **Network Information** page.

Table 78. 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, bond0, 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: a. Select the Adapter type. b. Enter the Port and Duration. c. Click the check box for Call home collected data if wanted. d. Then, click Run TCP Dump .

<i>Table 78. Selections available from the Network Information page (continued)</i>	
Item	Description
Nslookup	Enter the Host name and select Nslookup Host .

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.

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 79. Supported browsers	
Browser recommended	Version tested
Microsoft Edge	44
Microsoft Internet Explorer†	10, 11
Mozilla Firefox	60 ESR
Google Chrome	77

†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 10.
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.

IBM® supports higher versions of the browsers as long as the vendors do not remove or disable functionality that the product relies upon. For browser levels higher than the versions that are certified with the product, customer support accepts usage-related and defect-related service requests. As with operating system and virtualization environments, if the support center cannot re-create the issue in our lab, we might ask the client to re-create the problem on a certified browser version to determine whether a product defect exists. Defects are not accepted for cosmetic differences between browsers or browser versions that do not affect the functional behavior of the product. If a problem is identified in the product, defects are accepted. If a problem is identified with the browser, IBM might investigate potential solutions or workaround that the client can implement until a permanent solution becomes available.

The following steps help you connect to the TS7700 Management Interface through an installed web browser.

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.

This procedure is for Windows XP† SP2 users that are not presented with a download dialog box after selecting to download a .csv file.

In Microsoft Internet Explorer:

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.

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 282](#)

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.

Regenerating keys support (rekeying)

This topic describes regeneration of keys support (rekeying).

Rekeying is the process of creating a new key for the disk storage system. Rekeying can be done locally or externally.

Regenerating keys support locally

Any TS7700 configured with Local Key Management encryption can be rekeyed with new encryption keys on-demand with no downtime and no performance loss during or after the rekey operation. The rekey operations require physical access to the disk storage system. Therefore, the rekey operations can be initiated only from the TS7700 Smit menus. Following is the Smit menus for the 3956-CSB rekey operations:

Smit > IBM TS7700 Maintenance > Utility Menus > Disk Cache Utility Menus > Re-generate Encryption Key.

During the rekeying process, a new key is generated and copied to the USB flash drives. By default, rekeying creates four copies out of which two are expected to be connected and two are for backup drives. The new key is then used in place of the current key.

Note:

- Before you create a new key, ensure that at least one USB port has a USB flash drive that contains the current valid key. The rekey operation fails unless at least one USB flash drive contains the current key.
- To rekey the disk storage system, at least four USB flash drives are needed to store the copied key material.

Regenerating keys support externally

If external encryption enablement is configured to manage encryption keys, 3956-CSB can generate new keys with the encryption key servers. During the rekey process, the key server generates a new key and the existing key becomes obsolete. In configurations with a single primary key server and multiple secondary key servers, only the primary key server is updated during the rekey operation.

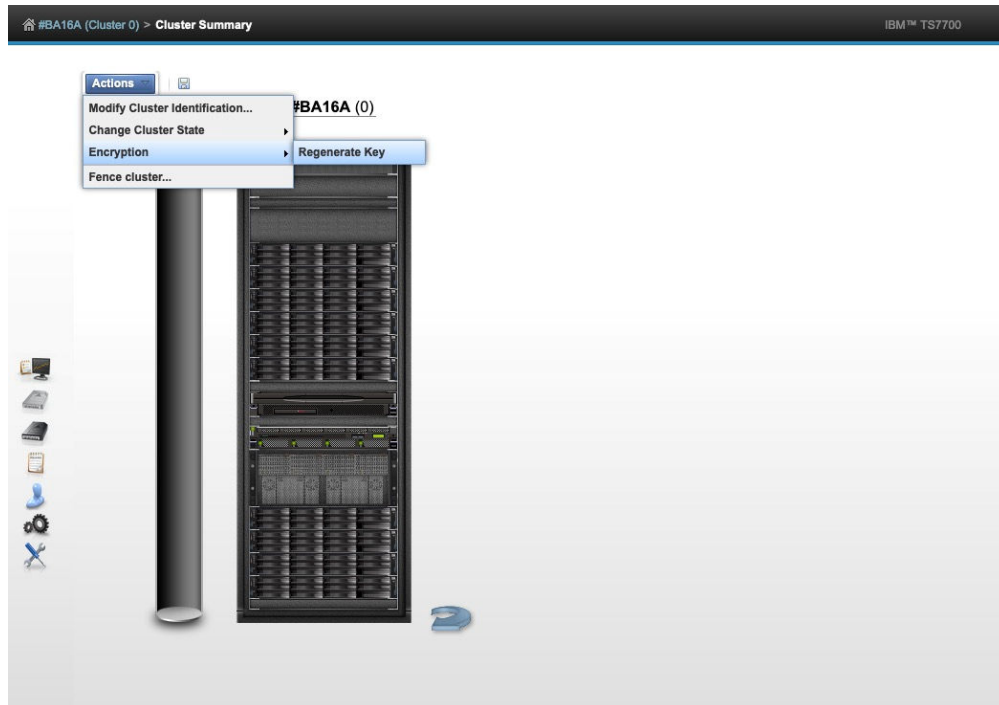
Note: To create a new key, enable encryption on the disk storage system.

Any TS7700 configured with External Key Management Encryption depends on the ISKLM server to manage the encryption keys. TS7700 does not support backing up the encryption keys to external media, such as DVD discs, USB flash drives. ISKLM must instead be used to perform key backups. However, from

the TS7700 service menu, a request can be sent to ISKLM to issue a new key to the disk subsystem for the rekey. TS7700 does not store any encryption key permanently. All copies of the encryption keys remain only in ISKLM indefinitely. TS7700 supports up to two synchronized ISKLM servers for redundancy.

External rekey can be performed in the following ways:

- From the TS7700 Smit menus **Smit > IBM TS7700 Maintenance > Utility Menus > Disk Cache Utility Menus > Re-generate Encryption Key**
- From the TS7700 Management Interface **Cluster Summary > Actions > Encryption > Regenerate Key**



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.

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 copy of the internal TS7700 database. This copy 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.

Disaster recovery environments can assume many configurations:

Multi-cluster TS7700 Grid

The grid contains two or more TS7700 systems. Virtual volumes contain the replicated recovery data.

Empty TS7770T or TS7760T

Physical volumes that contain the replicated recovery data and that have been copy exported are restored to the empty cluster.

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 Cognitive Support Platform (CSP) case 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 233](#)

Automated read-only (ROR) 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.

Recovering data from a virtual volume

Cloud export recovery allows you to recover stored virtual volumes for restoration of data.

Cloud storage provides a cost efficient solution to storing data long-term or as a means to store another copy of data in the case of a disaster. In the event of a disaster, a recovery process is needed to access that data. Cloud Export Recovery provides the ability to quickly restore a TS7700 production environment in the case of a total loss of a TS7700 Grid.

Note: Cloud export recovery is only supported on VEC/VEDs in a grid that are at R5.1 code level.

For information about recovering data from a virtual volume, refer to [“Cloud export recovery” on page 214](#).

Testing grid failover

This topic describes how to test for grid failover.

You must be familiar with how to use the virtual tape systems that are attached to zOS environments.

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

Reference

This section lists codes and descriptions for TS7700 Management Interface error messages and events, ERA codes, operator information messages, and service information messages. In this section you can also find glossary definitions and a list of trademarks.

Management interface messages

Use this section to locate additional information about TS7700 Management Interface error messages. Error codes associated with these messages begin with the identifier HYDME.

Expand the [“Management interface messages”](#) on [page 289](#) parent topic in the left navigation pane to view the complete list of HYDME error codes.

Perform Library Function codes

This topic describes the Perform Library Function (PLF) codes that can be returned when an IBM TS7700 Grid operates attached to a physical library.

The PLF command is used to pass command and control information to a library manager through the controller that services the attached drive string. This command transfers an order-dependent number of data bytes, which contain an order code, common information, and order unique parameters. The order code specifies what operation is to be completed by the library manager.

Operations are either run immediately or queued by the library manager as an asynchronous operation. Immediate operations are completed before the ending status is presented. Asynchronous operations are completed after the ending status is presented and can result in the generation of a delayed response attention message.

Error conditions that are related to PLF commands can be detected either during execution of the PLF command or during execution of a resulting asynchronous operation. Errors that are detected during command execution are reported with ending status as a unit check and associated sense data, described by **Error Recovery Action (ERA) codes**. Errors that are detected during the execution of an asynchronous operation are reported through **completion codes**. They are presented in a delayed response message or through the presentation of unsolicited unit checks and/or unsolicited attention messages.

Related information

[“Completion codes”](#) on [page 314](#)

[“Error Recovery Action codes”](#) on [page 289](#)

[“Operator information messages”](#) on [page 322](#)

Error Recovery Action codes

Error Recovery Action (ERA) codes can be returned to a user performing operations in the IBM TS7700 Grid. These codes are returned when a command fails before the operation begins. The format for the ERA codes is **ERA code XX Mod YY**, where **XX** is the ERA code and **YY** is its modifier.

Refer to the *IBM TS7700 Customer Information Center* link in the **Related information** section for current ERA code reasons and descriptions.

The following table defines the ERA codes that you can encounter:

Table 80. ERA codes	
ERA code	Reason - Modifier - Description
00	Unsolicited Sense The sense command was issued without an existing contingent allegiance. Any existing unit check conditions and associated sense data remain pending in the controller.
23	Read Data Check An unrecoverable error was detected while attempting to read a data block or tape mark. The controller attempts, if possible, to send whatever data is read, correct or incorrect, to the host before presenting unit check status. Failure to perform DDR recovery can result in the controller preventing further access to the volume.
26	Read Opposite A Read Backward command was issued to the subsystem.
27	Command Reject The command cannot be accepted for any of the following conditions: • An undefined command was issued. • The parameter data for a command is invalid. • A command sequence error was detected Check the Modifier to determine the reason for the reject. When this unit check is presented to a Perform Subsystem Function command that specifies one of the following orders: • Set Volume Token (SVT) • Prepare for Read Volume Token (PRVT) • Delete Volume Token (DVT) • Control File Access (CFA) • Restricted Command Control (RCC) • Present Message Notification Attention (PMNA) • Create Token List File (CTLF) • PTP Mode Control (PMC) • PTP Query Data (PQD)

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
	Format 20 sense byte 8 reports the Reason code (RC) and byte 9 reports the Reason Qualifier Code (RQC) associated with the error detected. The following RC-RQC values are defined: X'20'-X'13' Process Sequence: The command is incompatible with the state of the subsystem or a resource in the subsystem established by a prior command. X'20'-X'17' Process Sequence: The resource requested by the command is in use by another process in the subsystem. X'20'-X'30' Parameter Error: An invalid parameter has been specified. X'20'-X'32' Parameter In Conflict: A valid parameter has been specified that is incompatible with the state of the subsystem. X'20'-X'33' Reserved Field Error: A reserved field has been set to a non-zero value.
	Modifier - Description
	01 - A reserved field in a Library Mount or Library Universal Mount order is invalid.
	02 - A reserved field in a Library Demount order is invalid.
	03 - A reserved field in a Library Set Volume Category order is invalid.
	04 - A reserved field in a Library Set Volume Attribute order is invalid.
	07 - A reserved field in a Library Cancel order is invalid.
	08 - A reserved field in a Prepare for Read Subsystem Data order is invalid.
	09 - A reserved field in a Library Export order is invalid.
	0A - A reserved field in a Library Audit order is invalid.
	0B - A reserved field in a Library Import order is invalid.
	0C - A reserved field in a Library Set Device Category order is invalid.
	0D - A reserved field in a Library Release Category order is invalid.
	0E - A reserved field in a Library Reserve Category order is invalid.
	0F - A reserved field in a Library Add Volume Information order is invalid and no other reserved field error code applies.
	11 - The VOLSER is all blanks and the source category is NULL, VOLSER-specific category or is in the range reserved for hardware other than Insert category, or the alternate source category is in the range reserved for hardware other than Insert Category, or the second alternate source category is in the range reserved for hardware other than Insert Category.
	12 - An invalid target-category is specified in a Library Demount order.
	13 - The target-category is not Eject and the Message Required Bit is set in a Library Set Volume Category order.
	14 - A target VOLSER of all blanks is specified in a Library Set Volume Attribute order.
	17 - An invalid attribute is specified in a Library Cancel order.
	18 - An invalid information type is specified in a PLF- Prepare For Read Subsystem Data order.

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
	19 - A VOLSER of all blanks is specified in a Library Export order.
	1A - An invalid audit type is specified in a Library Audit order.
	1B - A VOLSER of all blanks is specified in a Library Import order.
	1C - The Demount Category Assignment specified in a Library Set Device Category order is the Volser-Specific category or in the range reserved for hardware.
	1D - An undefined release attribute is specified in a Library Release Category order.
	1E - The number of categories field in a Library Reserve Category order specified X'00'.
	1F - A reserved field in a Library Set Category attribute order is invalid.
	21 - The target category specified is in the range reserved for hardware. (X 'FF00-FFFE').
	22 - The VOLSER specified in a Library Demount order contains embedded blanks or illegal characters.
	23 - The VOLSER specified in a Library Set Volume Category order is not all blanks and the target category is in the range reserved for hardware but is not the eject, bulk-eject, or purge-volume category.
	24 - The target or clone VOLSER specified in a Library Set Volume Attribute order contains leading or embedded blanks or illegal characters.
	27 - The cancel attribute specifies - Message ID Cancel in a Library Cancel order and the Message ID parameter is all X'0'.
	28 - An invalid source-category is specified in a PLF- Prepare for Read Subsystem Data order.
	29 - The VOLSER specified in a Library Export order contains embedded blanks or illegal characters.
	2A - A VOLSER of all blanks is specified in a Library Audit order.
	2B - The VOLSER specified in a Library Import order contains embedded blanks or illegal characters.
	2C - An invalid device-category is specified in a Library Set Device Category order.
	2D - The Identification Token specified in a Library Release Category order is either all Nulls, Blanks, or contains one or more invalid characters or has no reserved categories.
	2E - The Identification Token specified in a Library Reserve Category order is either all Nulls or blanks or contains one or more invalid characters.
	2F - The Null category is specified in the Category field of a Library Set Category Attribute order.
	31 - The VOLSER has leading or embedded blanks.
	32 - The VOLSER specified in a Library Demount order is non-blank and it does not match the VOLSER that was mounted on the device.
	33 - The VOLSER specified in a Library Set Volume Category order is all blanks.
	34 - One or more of the storage management construct names specified in a Library Set Volume Attribute or Library Universal Mount order contains leading or embedded blanks or illegal characters.
	38 - The information type specified in a PLF- Prepare For Read Subsystem Data order requires a VOLSER to be specified, but the VOLSER specified is all blanks.

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
	3A - The VOLSER specified in a Library Audit order contains embedded blanks or illegal characters.
	3D - The Release Category specified in a Library Release Category order is outside of the range reserved for General-Programming-Use categories.
	3E - The Requested Category specified in a Library Reserve Category order is in the range reserved for hardware.
	3F - The category specified in the Category field of a Library Set Category Attribute order is not reserved.
	41 - In a Library Mount or Library Universal Mount order, a VOLSER was not specified, the alternate source- category parameter does not specify the null category and a previous library set device category order for the device specified the source-category and the category order parameter as active.
	42 - The VOLSER specified in a Library Demount order is not all blanks, and a mount operation for a different VOLSER is queued for the device.
	43 - The target-category specified in a Library Set Volume Category order is purge-volume and the VOLSER specified is not misplaced, not assigned to the exported category or not assigned to the manually ejected category.
	44 - The target category of a Library Set Volume Attribute order specified one of the eject categories.
	45 - Reserved (internal library manager error return)
	48 - The VOLSER specified in a PLF- Prepare For Read Subsystem Data order contains embedded blanks or illegal characters.
	4D - The Release Category specified in a Library Release Category order is not reserved for the specified System Token.
	4F - In a Library Set Category Attribute order, the attribute specified is X'01' but there are illegal characters in the Category Name field.
	53 - The VOLSER specified in a Library Set Volume Category order contains embedded blanks or illegal characters.
	54 - The target VOLSER specified in a Library Set Volume Attribute order is not all blanks and the category specified in the target-category parameter is in the range reserved for hardware and is not the insert category or the purge-volume category.
	58 - The priority field specified in a Perform Library Function command is not X'0'.
	5D - The Release attribute of a Library Release Category order specifies X'00' and there are volumes currently assigned to the Release Category specified.
	5F - In a Library Set Category Attribute order, the attribute specified is X'01' but the combination of the Identification Token and the Category Name is not unique.
	61 - Reserved
	63 - The source category field specified in a Library Set Volume Category or Library Set Volume Attribute order was not the null category and did not match the current assignment of the specified volume.
	64 - A Library Mount or Library Universal Mount order is issued to a device for which a previous Library Set Device Category order had specified the Enable Auto Mount parameter as active.

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
	65 - The mount issued was received on an invalid port number for the partition this TS7700 is attached.
	66 - The source storage group name parameter specified in a Library Universal Mount order contains leading or embedded blanks or illegal characters.
	68 - The System Token specified in a PLF- Prepare for Read Subsystem data order is either all nulls or blanks or contains one or more invalid characters.
	6E - The volume attribute parameters in a Library Add Volume Information order specified an undefined combination.
	70 - The VOLSER specified in a Library Add Volume Information order is all blanks or has embedded blanks or contains illegal characters.
	71 - The target category specified in a Library Add Volume Information order is incorrect. Refer to the order description for the specific conditions.
	74 - The target-category specified in a Library Set Volume Attribute order is purge-volume and the target VOLSERr specified is not misplaced, not assigned to the exported category or not assigned to the manually ejected category.
	88 - In a PLF- Prepare for Read Subsystem Data order that requests Expanded Volume Data, the Last Use Date Format or Field Separator for Last Use Date fields specified a value that is not defined.
	FD - An internal microcode error was detected while attempting to execute a Perform Library Function order.
	FE - The format level specified in a Perform Library Function command is not supported.
	FF - The Perform Library Function order specified is not supported.
29	Function Incompatible A command issued requested an operation that is understood by the subsystem, but cannot be performed due to the state of the subsystem, its configuration, or the set of installed features. This ERA code is indicated for the following conditions:
	- For commands other than Clear Virtual Device, the path or path group a command was issued on is disabled for that command. For the Clear Virtual Device command, the path group ID specified in the command is disabled for restricted commands. Sense bytes 8:9 will also indicate X'2015'. - A Perform Subsystem Function command was issued which specified the Set Volume Token or Delete Volume Token order and the token specified in the current token field did not match the token currently associated with the specified volume in the Volume/token database. Sense bytes 8:9 will also indicate X'3150'. - A Perform Subsystem Function command was issued which specified the Set Volume Token order and the volume specified does not have an entry in the volume/token database and the database is at its maximum capacity. Sense bytes 8:9 will also indicate X'3151'.
	- A Perform Library Function command was issued, the microcode to support this command is installed, but the function requested by the command is not supported as described below. - A Perform Library Function command was issued, the microcode to support this command is installed, but the function cannot be performed due to the current state of the library as described below.

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
	Note: If the installed microcode does not support the Library Attachment Facility, ERA 27, Command Reject is indicated. When this unit check is presented to a Perform Library Function command in format 23 sense data, byte 8, check the Modifier to determine the reason for the reject.
	Modifier - Description
	00 - The function requested in the Perform Library Function order is not supported by the subsystem the order was issued to.
	01 - Library Attachment Facility Not Installed and Allowed
	02 - Reserved
	03 - Library Set Volume Category order issued specifying a target category of bulk-eject and the bulk input and output facility is not configured in the library.
	04 - Reserved
	05 - Attempting to cause a wrong type cartridge to be mounted on a device (for example a 3590 cartridge on a 3490 device).
	06 - The PLF Library Set Volume Category order specified an eject category for a virtual volume. k Virtual volumes cannot be ejected from the library unless they are in the insert category and have k a mount count of zero or assigned to a category that has the scratch (fast-ready) attribute set or the Ignore j Current Category for Virtual Volume Eject flag is active.
	07 - A PLF Library Cancel order was issued to cancel a pending export or import operation and one of the following conditions apply: • The Export/Import List VOLSER field specifies all binary zeros and there was not a corresponding operation pending in the library. • The Export/Import List VOLSER field specifies a VOLSER that does not match the VOLSER that was specified when the corresponding operation was initiated.
	08 - A PLF Library Import or Export order was issued to a Virtual Tape Server subsystem that has less than four available physical drives.
	10 - A library mount or library universal mount PLF order specified a source or alternate-source category that is a scratch category or the scratch (fast-ready) bit in the flag byte was active and it is issued to a device in a cluster in a TS7700 Grid configuration that is in write protect or read-only takeover mode.
	11 - A Perform Library Function command was issued, which specified the Prepare for Read Subsystem data order, to obtain information about configurable facilities in the library and the requested facilities are not supported. This error is reported for the following conditions: • The information type specified is X'1D', All Device Data and the device set being requested is not configured in the library. • The information type specified is X'29', Volume Pool Statistical data and the pool set being requested is not configured in the library.
	12 - The Bypass Data Security Hold Checking flag (bit 7) in the flag byte is not active, a volume was specified in the command that has a non-zero expire time associated with it and the category to which it is assigned also has the hold check box active. A volume in this state cannot be mounted, moved, or have its attributes modified until the expire time has elapsed.

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
	18 - One or more of the specified construct names doesn't exist and the Construct Creation Actions parameter in an LSVA PLF order specified the operation is to fail if a specified construct doesn't exist.
	19 - In a LSVA PLF order, one or more of the specified construct names doesn't exist, the Construct Creation Actions parameter specified that the construct is to be created but the maximum number of unique names for a construct has already been reached (255 maximum).
	20 - One or more of the following conditions apply: • A library mount or library universal mount PLF order is issued to a device in a cluster in a TS7700 Grid configuration and the cluster the command was received on is in service or service preparation mode.
	30 - A PLF command is issued to a device in a cluster in a TS7700 Grid configuration to update or query information associated with a virtual volume and the cluster the command was received on does not have an available path to the cluster that currently owns the volume and ownership takeover is not enabled.
	32 - A PLF export command is issued to a device in a cluster in a TS7700 Grid configuration, a distributed library is not specified and there are more than one valid copy of the export list file volume specified.
	33 - A PLF Export order is issued to a TS7700 and it is performing a global operation. Global operations are volume inserts, volume deletions through the management interface, damaged volume recovery and disaster recovery.
2B	Environmental Data Present ERA 2B, Environmental Data Present, occurs in log data presented to a Read Buffered Log command. In this case, unit check is not presented and, consequently, there is no software recovery action invoked.
2C	Permanent Equipment Check The controller presents unit check status with associated sense data indicating ERA 2C, Permanent Equipment Check, when the controller detects an unrecoverable error due to subsystem hardware or microprogram failure.
2D	Data Security Erase Failure The controller presents unit check status with associated sense data indicating ERA 2D, Data Security Erase Failure, in ending status to a Data Security Erase command if the controller cannot complete the command.
2E	Not Capable The controller presents unit check status with associated sense data indicating ERA 2E, Not Capable, when the controller is unable to process the information on tape. This unit check is presented for any of the following reasons: • The information in the block ID field of a virtual block requested by a Read Forward or Read Backward command is invalid or requires facilities which are not available on this subsystem. • A read command is issued to a virtual device in a Virtual Tape Server subsystem and the current data record is in a compressed format and the subsystem does not support compressed data.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
2F	Limited Shared Access Violation If a set of protected device-path pairs for a device have been established, any tape motion command other than Rewind/Unload, Write, Write Tape Mark, or Synchronize issued to that device on a path not in the protected set is presented unit check status with associated sense data indicating ERA 2F, Limited Shared Access Violation. Notes: 1. The device assignment may have been reset or was never established. If the device is shared between multiple hosts which are not coupled, the device may be assigned to another host and not be accessible by the host executing the job. 2. Sense byte 10:11 will indicate X'B300'. Sense byte 12 contains channel link ID of the accessing host.
30	Write Protected The controller presents unit check status with associated sense data indicating ERA 30, Write Protected, when a write-type command is issued to a volume: • Which is physically or virtually write protected. • In a VTC that is in read only or write protect mode. Sense bytes 8:9 will also contain X'2222'. • A specific volume mount was received while the TS7700 was in the out of cache resources state and a g subsequent write type command was issued to the volume.
35	Drive Equipment Check The controller presents unit check status with associated sense data indicating ERA 35, Drive Equipment Check, when any one of the following conditions occurs: • The virtual tape device has encountered an unrecoverable error. • To satisfy a virtual tape mount a recall is necessary and the recall could not be successfully completed. Note: In the case of a recall failure, the controller first indicates that the device is ready, then presents this error to the first I/O command.
36	End of Data Controller presents unit check status with associated sense data indicating ERA 36, End of Data, to a forward motion command if the controller detects it is at the end of the data previously written to the volume.
38	Physical End of Volume The controller presents unit check status with associated sense data indicating ERA 38, Physical End of Volume, when the virtual drive has reached the maximum amount of data allowed for the media type mounted while executing a forward-motion-type command.
39	Backward at Beginning of Tape The controller presents unit check status with associated sense data indicating ERA 38, Physical End of Volume, when the virtual drive has reached the maximum amount of data allowed for the media type mounted while executing a forward-motion-type command.
3C	Reserved

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
3D	Block Not Found Before Timeout The controller presents unit check status with associated sense data indicating ERA 3D, Block Not Found Before Timeout, when the timeout value specified in a search command has been reached prior to finding a block that satisfies the search expression. Sense bytes 8:9 will also indicate X'3114'.
3E	Reserved
3F	Reserved
41	Record Sequence Error The controller presents unit check status with associated sense data indicating ERA 41, Record Sequence Error, if the controller detected a Block ID number in a record indicating that it was not in proper sequence on the tape. The controller may prevent further accesses to the volume (see ERA 47, Volume Fenced).
42	Degraded Mode The controller presents unit check status with associated sense data indicating ERA 42, Degraded Mode, when it detects a condition which indicates that certain subsystem resources are either unavailable or performing in a degraded mode. The subsystem remains operational, but degraded performance may be observed. If tape positioning has been lost, the controller will prevent further accesses to the volume (see ERA 47, Volume Fenced).
43	Drive Not Ready The controller presents unit check initial status with associated sense data indicating ERA 43, Drive Not Ready, when a command is issued and the device state in the controller is not ready and command requires the device to be ready.
44	Locate Block Unsuccessful The controller presents unit check status with associated sense data indicating ERA 44, Locate Block Unsuccessful, if the tape could not be positioned at the end of the block preceding the block specified by a Locate command.
45	Drive Assigned Elsewhere The controller presents unit check status with associated sense data indicating ERA 45, Drive Assigned Elsewhere, if the device is disabled via dynamic partitioning on the channel path issuing the command. Note: The device has been explicitly enabled on some other channel path(s), but is not explicitly enabled on the path used to issue the command. The device assignment may have been reset or was never established. If the device is shared between multiple hosts which are not coupled, the device may be assigned to another host and not be accessible by the host executing the job.
47	Volume Faced The controller presents unit check status with associated sense data indicating ERA 47, Volume Fenced, if a condition has occurred which has resulted in the loss of volume integrity due to lost positioning or assignment. The controller prevents further access to the tape volume by generating deferred unit checks with associated sense data indicating ERA 47, Volume Fenced, for all eligible commands until the condition is reset or until the cartridge is unloaded. The original condition which subsequently caused ERA 47, Volume Fenced, to be presented has already been indicated by a previous unit check and associated sense data.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
48	Unsolicited Informational Data The controller presents unit check status with associated sense data indicating ERA 48, Unsolicited Informational Data, when there is unsolicited data to be logged as an OBR record in the ERDS file. It is also presented when the transfer of parameter or tape record data is interrupted from the channel due to a halt condition. Presentation of this ERA code in sense format 20 causes the host to reissue the command that was interrupted. The controller may prevent further accesses to the volume (see ERA 47, Volume Fenced). Note: Sense records which are generated as a result of forced error logging (Format 19 sense data) contain ERA 48, Unsolicited Informational Data.
4D	Resetting Event The controller presents unit check status with associated sense data indicating ERA 4D, Resetting Event, when resetting event notification is pending for a device-path pair and a command is issued which is eligible to receive this indication.
4E	Maximum Block Size Exceeded The controller presents unit check status with associated sense data indicating ERA 4E, Maximum Block Size Exceeded, when the host issues a write command that would write a data block larger than the maximum size that the controller can write. The data block is not written to tape.
4F	Reserved
50	Read Buffered Log (Overflow) The controller presents unit check status with associated sense data indicating ERA 50, Read Buffered Log (Overflow), when there is an overflow condition in the device's buffered log data and the controller is requesting the control program to issue a Read Buffered Log command and record the data as an MDR record in the ERDS file. Note: This unit check is generated when a counter in buffered log data has reached its overflow threshold and the controller is operating in extended buffered log mode. The sense data presented with ERA 50, Read Buffered Log (Overflow), is always in sense format X'20'. The log data presented to the Read Buffered Log command issued as a result of ERA 50, Read Buffered Log (Overflow), is always in log format X'30' and contains ERA 2B, Environmental Data Present.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
51	Read Buffered Log (EOV) The controller presents unit check status with associated sense data indicating ERA 51, Read Buffered Log (EOV), to indicate the controller is requesting the control program to issue a Read Buffered Log command. Buffered log data may or may not be present when this ERA is presented and an MDR record may or may not be required to be written in the ERDS file. Notes: 1. ERA 51, Read Buffered Log (EOV), provides an indication that an MDR type 90 record should be generated, provided the control program does not automatically issue a Read Buffered Log command prior to issuing a Rewind Unload command. Programs which automatically issue a Read Buffered Log command prior to issuing a Rewind Unload should perform the indicated recovery action and should also check the data received prior to logging to determine if there is any data present. 2. This unit check is generated as part of end of volume processing if the controller is operating in extended buffered log mode. The sense data presented with ERA 51, Read Buffered Log (EOV), is always in sense format X'20'. The log data presented to the Read Buffered Log command issued as a result of ERA 51, Read Buffered Log (EOV), is always in log format X'30' and contains ERA 2B, Environmental Data Present.
52	End of Volume Complete The controller presents unit check status with associated sense data indicating ERA 52, End of Volume Complete, to indicate the successful completion of a Rewind Unload command. Notes: 1. The presentation of unit check to a Rewind Unload is required by VM to detect the end of volume processing. The sense data presented basically indicates that the unit check was not required because the command was successful. 2. ERA 52, End of Volume Complete is only presented on controllers which are operating in extended buffered log mode. The sense data presented with ERA 52, End of Volume Complete, is always in sense format X'22'. There is no log data present in this format.
53	Global Command Intercept The controller presents unit check status with associated sense data indicating ERA 53, Global Command Intercept, when a global command is issued on a channel path which is associated with a path group when the global command intercept condition is active.
54	Channel Interface Recovery - Temporary The controller presents unit check status with associated sense data indicating ERA 54, Channel Interface Recovery - Temporary, when: • The channel has requested channel initiated retry or unit check, the generation of unit check is appropriate for the request, and the command in progress can be reissued. • An abnormal condition is detected on the interface which results in a device level error, the generation of command retry is not appropriate, and the command in progress can be reissued.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
55	Channel Interface Recovery - Permanent The controller presents unit check status with associated sense data indicating ERA 55, Channel Interface Recovery - Permanent, when: • The channel has requested channel initiated retry or unit check, the generation of unit check is appropriate for the request, and the command in progress cannot be reissued. • An abnormal condition is detected on the interface which results in a device level error, the generation of command retry is not appropriate, and the command in progress cannot be reissued.
56	Channel Protocol Error The controller presents unit check status with associated sense data indicating ERA 56, Channel Protocol Error, under the following conditions: • When the channel stacks a command response indication on a parallel channel interface. In this case, unit check is presented in ending status. • When a device level error is detected on a serial channel interface and there is an I/O operation in progress for the device with owed ending status. In this case, unit check is presented in ending status. • When a device level error is detected on a serial channel interface and there is no I/O operation in progress for the device with owed ending status. In this case, a deferred unit check is generated for the device.
57	Global Status Intercept When attention-intercept status (X'82') or not ready to ready-intercept status (X'87') is presented, the associated sense data indicates ERA 57, Global Status Intercept. Notes: 1. Attention-intercept status and not ready to ready-intercept status are unsolicited status conditions. As such, either one may be received as an unsolicited status condition in the absence of I/O activity or it may be presented in initial status to the first command of a command chain. 2. This ERA code should not be surfaced to a program which has not issued a Perform Subsystem Function command which specifies the Set Special Intercept Condition order.
58	Reserved
59	Reserved
5F	No PGID Established The controller presents unit check status with associated sense data indicating ERA 5F, No PGID Established, to a command issued on channel path for which a path group ID has not been established and the command processing requires that a path group ID is established. Sense bytes 8:9 will also indicate X'3155'.
60	Library Attachment Facility Equipment Check The controller presents unit check status, to a Perform Library Function command, with associated sense data indicating ERA 60, Library Attachment Facility Equipment Check, if the controller detects an unrecoverable error on the library attachment interface either during initialization or during subsequent command processing and there are no other operational paths between the controller and the library manager.
61	Reserved

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
62	Library Manager Offline to Subsystem The controller presents unit check status with associated sense data indicating ERA 62, Library Manager Offline to Subsystem, if any of the following conditions apply: • A PLF command is issued and the library manager is offline to the subsystem. Note: In a TS7700 Grid configuration, ERA 62, Library Manager Offline to Subsystem, is j not presented in the Out of Stacked Volumes state case. Mount operations continue to be accepted.
	Modifier - Description
	00 - Microcode Levels Incompatible
	01 - Subsystem Sequence Number Mismatch
	02 - Message Incompatible
64	Library VOLSER in Use The controller presents unit check status with associated sense data indicating ERA 64, Library VOLSER in Use, if the VOLSER specified, in certain orders of the Perform Library Function command, is in use. Sense byte 8, Library Error Modifier, indicates which of the following reasons is being reported:
	Modifier - Description
	01 - Mounted on another device.
	02 - Queued for Mounting on another device.
	03 - In the process of being ejected.
	04 - Queued for Eject.
	05 - Export is pending.
	06 - Import is pending.
65	Library Volume Reserved The controller presents unit check status with associated sense data indicating ERA 65, Library Volume Reserved, if the VOLSER specified, in certain orders of the Perform Library Function command, is reserved. Sense byte 8, Library Error Modifier, indicates which of the following reasons is being reported:
	Modifier - Description
	00 - Reserved
	01 - VOLSER specified is assigned to the Cleaner-Volume category.
	02 - VOLSER specified is assigned to the Stacked-Volume category.
	03 - VOLSER specified is assigned to the Export-Hold category.
	04:FF - Reserved

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
66	Library VOLSER Not in Library The controller presents unit check status with associated sense data indicating ERA 66, Library VOLSER Not in Library, if the VOLSER specified, in certain orders of the Perform Library Function command, is not in the library partition the command was issued to. This unit check is also presented to a PLF - LUM or PLF - LSVA order if the clone VOLSER field specifies a VOLSER that is not in the library or the type of media is incompatible. Sense byte 8, Library Error Modifier, indicates which of the following reasons is being reported:
	Modifier - Description
	00 - A VOLSER is specified and it is not in the library inventory of the library partition the command was issued to, but is in another partition in the library.
	01 - The VOLSER specified in a Library Mount PLF order is not present in the library inventory of any library partition.
	03 - The VOLSER specified in a Library Set Volume Category PLF order is not present in the library inventory of any library partition.
	04 - The VOLSER specified in a Library Set Volume Attribute PLF order is not present in the library inventory of any library partition.
	08 - The VOLSER specified in a Library Import PLF order is not present in the library inventory of any library partition.
	09 - The VOLSER specified in a Library Export PLF order is not present in the library inventory of any library partition.
	0A - The VOLSER specified in a Library Audit PLF order is not present in the library inventory of any library partition.
	12 - The VOLSER specified in a Library Universal Mount PLF order is not present in the library inventory of any library partition.
	18 - The information type specified is either Volume Data, Expanded Volume Data, Volume Attribute Data or Device Allocation Assistance Data and the specified VOLSER is not present in the library inventory of any library partition.
	20 - A clone VOLSER is specified in a Library Universal Mount or Library Set Volume Attribute PLF order and it is not in the library inventory of the library partition the command was issued to.
	21 - A clone VOLSER is specified in a Library Universal Mount or Library Set Volume Attribute PLF order and its not the same type of media (virtual/physical).

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
67	Library Category Empty The controller presents unit check status with associated sense data indicating ERA 67, Library Category Empty, if: For a Perform Library Function Library Mount order There is no VOLSER specified and the category specified by the source-category parameter does not contain any assigned volumes, and, if not X'0000', the alternate-source-category does not contain any assigned volumes. Sense byte 8, Library Error Modifier, is set to X'01'. The mount is issued to a TS7700 Grid configuration and there is no VOLSER specified and the category specified by the source-category parameter does not contain any compatible volumes owned by the cluster performing the mount, and, if not X'0000', the alternate-source-category does not contain any compatible volumes owned by the cluster performing the mount. Sense byte 8 will also indicate X'01'. There is no VOLSER specified and the source-category specified had been assigned to the device by a previous library set device category order which also specified the category order parameter as active and all of the volumes assigned to the category have already been mounted. Sense byte 8, Library Error Modifier, is set to X'02'. There is no VOLSER specified and the source-category specified had been assigned to the device by a previous library set device category order which also specified the category order parameter as active and the next volume in the specified category, whose media type is compatible with the device the order was issued to, is in-use, inaccessible, misplaced or has been manually ejected or in a TS7700 Grid configuration, is owned by another cluster and ownership cannot be obtained. Sense byte 8, Library Error Modifier, is set to X'03'.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
	For a Perform Library Function Library Universal Mount order The source-category or alternate-source category specified has not been assigned to the device by a previous library set device category order which also specified the category order parameter as active, the enable blank storage group selection parameter is inactive and the categories specified by the source category and alternate-source-category do not contain any available volumes that meet the specified selection criteria. In a TS7700 Grid configuration, part of the selection criteria is whether the cluster processing the mount has ownership of the volume. Sense byte 8, Library Error Modifier, is set to X'01'. The source-category or alternate-source category specified has not been assigned to the device by a previous library set device category order which also specified the category order parameter as active, the enable blank storage group selection parameter is active and the categories specified by the source category and the alternate-source-category parameters have no available volumes that meet the specified selection criteria including a blank storage group assignment. In a TS7700 Grid configuration, part of the selection criteria is whether the cluster processing the mount has ownership of the volume. Sense byte 8, Library Error Modifier, is set to X'01'. The source-category specified had been assigned to the device by a previous library set device category order which also specified the category order parameter as active and all of the volumes meeting the specified selection criteria in the category have already been mounted. Sense byte 8, Library Error Modifier, is set to X'02'. The source-category specified had been assigned to the device by a previous library set device category order which also specified the category order parameter as active and the next volume in the specified category that meets the specified selection criteria is in-use, inaccessible, misplaced or has been manually ejected or in a TS7700 Grid configuration, is owned by another cluster and ownership cannot be obtained. Sense byte 8, Library Error Modifier, is set to X'03'. For a Perform Library Function Library Import order There are no volumes assigned to the import category. The import operation cannot start until the stacked volumes to import have been added to the library. Sense byte 8, Library Error Modifier, is set to X'04'. There are no scratch stacked volumes. Sense byte 8, Library Error Modifier, is set to X'05'. For a Perform Library Function Library Export order There are no scratch stacked volumes. Sense byte 8, Library Error Modifier, is set to X'05'. All other values of sense byte 8 are reserved.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
68	Library Order Sequence Check The controller presents unit check status with associated sense data indicating ERA 68, Library Order Sequence Check, if any one of the following conditions apply: • The drive to which a Perform Library Function Library Mount or Library Universal Mount order was issued already has a Library Mount request queued or a mount operation in progress or is already loaded and a demount operation is not pending. • The drive to which a Perform Library Function Library Demount order was issued already has a Library Demount request queued or does not have a volume mounted. • A Perform Library Function - Library Export order was issued to a virtual library that already has an export or import operation queued or in progress. • A Perform Library Function - Library Import order was issued to a physical library that already has an import operation queued or in progress or an export operation is queued or in progress for the virtual library. • A Perform Library Function - Library Import order was issued to a virtual library that had one or more volumes assigned to the insert category with an active Import Volume flag. • A Perform Library Function - Library Export order was issued to a virtual library that had one or more volumes assigned to the exported category. Sense byte 8, Library Error Modifier, is set to one of the following values based on the condition being reported:
	Modifier - Description
	01 - Mount is in progress or volume mounted.
	02 - Mount is already pending.
	03 - Demount was already pending.
	04 - No volume is mounted.
	05 - Export or Import operation queued or already in progress.
	06 - Host processing for a previous import or export operation did not complete. Volumes are assigned to the insert category with an active Import Volume flag or there are volumes assigned to the exported category.
6A	Reserved
6B	Library Volume Misplaced The controller presents this ERA in sense data for the following conditions: • A Perform Library Function command is issued whose order specifies a VOLSER that is in the library inventory, but is flagged as a misplaced volume and the Volume Was Used During Manual Mode state is not active. The command is presented unit check status with associated sense data indicating ERA 6B, Library Volume Misplaced. • During processing in the library, a VOLSER was detected as being misplaced and cannot be located. The VOLSER is flagged in the inventory as misplaced and a Volume Exception attention message and unsolicited unit check status with associated sense data indicating ERA 6B, Library Volume Misplaced, is generated to report that the volume has been misplaced.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
6C	Library Misplaced Volume Found The controller presents a Volume Exception attention message and unsolicited unit check with associated sense data indicating ERA 6C, Library Misplaced Volume Found, if during processing in the library, a volume is found that is flagged as misplaced in the inventory.
6D	Library Drive Not Unloaded The controller presents unit check status with associated sense data indicating ERA 6D, Library Drive Not Unloaded, if A Perform Library Function, Library Demount order does not have the Force Unload on Demount flag as active and it is issued for a device which has a mount operation in progress or is already loaded and a Rewind Unload command has not been executed.
6E	Library Inaccessible Volume Restored The controller presents a Volume Exception attention message and unsolicited unit check with associated sense data indicating ERA 6E, Library Inaccessible Volume Restored, if during processing in the library, a volume that is flagged as inaccessible in the inventory is no longer inaccessible.
6F	Library Vision Failure The controller presents this ERA in sense data for the following conditions: • A Perform Library Function command is issued that requires the vision system to be operational and the vision system is not operational. The command is presented unit check status with associated sense data indicating ERA 6F, Library Vision Failure. • During processing in the library, the vision system has become non-operational. An unsolicited attention message, Operational State Change, with an unsolicited unit check, with associated sense data indicating ERA 6F, Library Vision Failure, is generated to report the failure of the vision system.
70	Library Manager Equipment Check During processing in the library, the library manager has become non-operational. An unsolicited attention message, Operational State Change, with an unsolicited unit check, with associated sense data indicating ERA 70, Library Manager Equipment Check, is generated to report the failure.
71	Library Equipment Check The controller presents an unsolicited unit check with associated sense data indicating ERA 71, Library Equipment Check, when the library has detected an unrecoverable error which causes the library to automatically enter the Pause state. Notes: 1. Any Perform Library Function orders that were in execution when the failure occurred will be re-queued for execution by the library manager. 2. The library will switch to 'Pause' status. Subsequent Perform Library Function orders will be accepted but orders requiring robotics motion will be queued but not executed. 3. The library console will indicate additional information to aid the service representative in determining the cause of the equipment check.

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
72	Library Not Capable - Manual Mode The controller presents unit check status with associated sense data indicating ERA 72, Library Not Capable - Manual Mode, when a Perform Library Function command specifies an order that cannot be performed because the library is operating in manual mode.
73	Library Intervention Required The controller presents an unsolicited attention message, Operational State Change, with an unsolicited unit check, with associated sense data indicating ERA 73, Library Intervention Required, when intervention is required to retrieve a cartridge that has become inaccessible to the library.
74	Library Informational Data The controller presents an unsolicited unit check with associated sense data indicating ERA 74, Library Informational Data, when an event in the library needs to be logged. Depending on what condition is being reported, the unit check may be associated with an Operational State Change attention message. Sense byte 8, Library Error Modifier, is used with ERA 74, Library Informational Data, to provide further information on the reason for the unsolicited unit check as follows:
	Modifier - Description
	00 - Reserved
	01 - A library component has become unavailable.
	02 - A library component previously unavailable has become available.
	03:0F - Reserved
	10 - A device clean operation has been performed based on a time of day value.
	11 - A device clean operation has been performed based on a count of the number of mounts.
	12 - A device clean operation has been performed based on a SARS request.
	13 - Reserved
	14:20 - Reserved
	21 - A device has been made unavailable through the library manager console.
	22 - A previously unavailable device has been made available through the library manager console.
	23:7F - Reserved
	80 - Preventive Maintenance Message
	81 - Error Threshold Exceeded
	82:FF - Reserved

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
75	Library Volume Inaccessible The controller presents this ERA in sense data for the following conditions: • A Perform Library Function command is issued whose order specifies a VOLSER that is in the library inventory, but is flagged as an inaccessible volume. The command is presented unit check status with associated sense data indicating ERA 75, Library Volume Inaccessible. Sense byte 8 will also indicate X'00'. • A PLF Audit order is issued to a device in a TS7700 and the data associated with the specified volume had been deleted with the delete expired volume data function. Sense byte 8 will also indicate x'01'. • A PLF Audit order is issued to a device in a TS7700 in a Grid configuration and a consistent version of the specified volume does not exist. Sense byte 8 will also indicate x'01'. • During processing in the library, a volume has become inaccessible. The volume is flagged in the inventory as inaccessible and a Volume Exception attention message and unsolicited unit check status with associated sense data indicating ERA 75, Library Volume Inaccessible, is generated to report that the volume has become inaccessible.
76	Library All Cells Full The controller presents this ERA in sense data for the following conditions • The Library Add Volume Information order of the Perform Library Function command is issued and the number of virtual volumes defined to the library inventory is at the maximum limit for the library. The command is presented unit check status with associated sense data indicating ERA 76, Library All Cells Full. • The Library Import order of the Perform Library Function command is issued and the number of virtual volumes defined to the library inventory is at the maximum limit for the library. The command is presented unit check status with associated sense data indicating ERA 76, Library All Cells Full. • During the execution of an insert or import operation in the library, all available physical storage cells in the library have been filled or the number of virtual volumes defined in the library has reached its limit. An unsolicited attention message, Operational State Change, with an unsolicited unit check, with associated sense data indicating ERA 76, Library All Cells Full, is generated to report this condition. :
77	Library Duplicate VOLSER Ejected The controller presents an unsolicited attention message, Volume Exception, with an unsolicited unit check, with associated sense data indicating ERA 77, Library Duplicate VOLSER Ejected, during the execution of an operation, when a duplicate VOLSER was found in the library. The VOLSER that is ejected is the one that is not at the location indicated by the inventory.
78	Library Duplicate VOLSER Left In Input Station The controller presents an unsolicited attention message, Volume Exception, with an unsolicited unit check, with associated sense data indicating ERA 78, Library Duplicate VOLSER Left In Input Station, during the execution of an insert operation, when a duplicate VOLSER was found in the input station.

Table 80. ERA codes (continued)

ERA code	Reason - Modifier - Description
79	Library Unreadable or Invalid VOLSER Left In Input Station The controller presents an unsolicited attention message, Volume Exception, with an unsolicited unit check, with associated sense data indicating ERA 79, Library Unreadable or Invalid VOLSER Left In Input Station, during the execution of an insert operation, for any of the following conditions: • A volume is found with an unreadable VOLSER label. • A volume is found without a label. • A volume is found whose VOLSER contains one or more invalid characters.
7A	Read Library Statistics The controller presents an unsolicited unit check with associated sense data indicating ERA 7A, Read Library Statistics, about once an hour when the subsystem is installed in a library and the library manager is online to the subsystem.
7B	Library Volume Manually Ejected The controller presents unit check status with associated sense data indicating ERA 7B, Library Volume Manually Ejected, if the volume specified in certain orders of the Perform Library Function command has been assigned to the manually-ejected category.
7C	Library Out Of Cleaner Volumes The controller presents an unsolicited attention message, Operational State Change, with an unsolicited unit check, with associated sense data indicating ERA 7C, Library Out Of Cleaner Volumes, when a drive cleaning operation is attempted but there are no cleaner volumes in the library.
7D	Library Volume Exported The controller presents unit check status with associated sense data indicating ERA 7D, Library Volume Exported, if the virtual volume specified in certain orders of the Perform Library Function command has been assigned to the exported category Note: This error is reported only on IBM libraries that have a Virtual Tape Server installed that also supports the export/import functions.
7E	Reserved

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
7F	Library Category in Use The controller presents unit check status with associated sense data indicating ERA 7F, Library Category In Use, if one of the following conditions exist for a Perform Library Function command: • A Library Set Device Category order was accepted previously for a different device and the same category and it had specified category order. Sense byte 8, Library Error Modifier, is set to X'01'. • The current Library Set Device Category order specifies category order and a category that is already assigned to another device. Sense byte 8, Library Error Modifier, is set to X'02'. • A Library Mount or Library Universal Mount order specifies a category in the source-category parameter that is assigned to another drive address and the library set device category order that made that assignment also specified the category order parameter as active. Sense byte 8, Library Error Modifier, is set to X'03'. • A Library Mount or Library Universal Mount order specifies a category in the alternate-source-category parameter that is assigned to another drive address and the library set device category order that made that assignment also specified the category order parameter as active. Sense byte 8, Library Error Modifier, is set to X'04'. All other values of sense byte 8 are reserved.
80	Library Unexpected Volume Ejected The controller presents an unsolicited attention message, Volume Exception, with an unsolicited unit check, with associated sense data indicating ERA 80, Library Unexpected Volume Ejected, during the execution of an operation, when a volume was found in the library that was not in the inventory. The volume is ejected from the library.
81	Library I/O Station Door Open The controller presents an unsolicited attention message, Library I/O Station State Change, with an unsolicited unit check, with associated sense data indicating ERA 81, Library I/O Station Door Open, when one of the I/O station doors is detected to be open. Sense byte 8, Library Error Modifier, is used with ERA 81, Library I/O Station Door Open, to provide further information on the reason for the unsolicited unit check as follows:
	Modifier - Description
	00 - Reserved
	01 - An input station door is open.
	01 - An output station door is open.
	03:FF - Reserved
82	Library Manager Program Exception The controller presents an unsolicited unit check with associated sense data indicating ERA 82, Library Manager Program Exception, when a program exception has been detected by the library manager.

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
83	Library Drive Exception The controller presents an unsolicited unit check, for a specific device address, with associated sense data indicating ERA 83, Library Drive Exception, when the enhanced device error recovery on a 3490 device installed in a managed tape library was successful. Note: Although this ERA code is generated by the library, it is reported in sense format 20 to provide information about the specific device error.
85	Library Environmental Alert The controller presents an unsolicited attention message, Operational State Change, with an unsolicited unit check, with associated sense data indicating ERA 85, Library Environmental Alert, when an environmental alert condition has been detected in the library enclosure. Sense byte 8 indicates the reason for the environmental alert as follows:
	Modifier - Description
	00 - Reserved
	01 - Smoke was detected by the internal smoke detector.
	02 - Smoke was detected by a third party supplied system.
	03:FF - Reserved
86	Library All Categories Reserved The controller presents unit check status with associated sense data indicating ERA 86, Library All Categories Reserved, to a Library reserve Category order of the Perform Library Function command when there are not enough available categories to satisfy the request or if the Requested Category field is not X'0000' and the specified category is reserved for another identification token.
87	Library Duplicate Volume Add Requested The controller presents unit check status with associated sense data indicating ERA 87, Library Duplicate Volume Add Requested, during the execution of a Library Add Volume Information PLF order when a VOLSER is specified which is already in the library inventory. Sense byte 8, Library Error Modifier, is set to one of the following values based on the condition being reported.
	Modifier - Description
	00 - The VOLSER specified is already in the library inventory of the library partition the command was issued to.
	01 - The VOLSER specified is already in the library inventory of another library partition of the library.
88	Damaged Cartridge Ejected The controller presents an unsolicited attention message, Volume Exception, with an unsolicited unit check, with associated sense data indicating ERA 88, Damaged Cartridge Ejected, when the library determines that a problem exists with the cartridge or media and has ejected the cartridge to an output station. Sense byte 8 indicates the reason why the cartridge was ejected:
	Modifier - Description

Table 80. ERA codes (continued)	
ERA code	Reason - Modifier - Description
	00 - Reserved
	01 - Either the cartridge is missing a leader block or the tape media has become detached from the leader block.
	02:FF - Reserved
89:8F	Reserved
90	File Contention Notification When the subsystem needs to notify a host, that has established access to a file in a Virtual Tape Server subsystem, that the file is needed for a higher priority access, the next Read Forward or Write command issued for the file is presented unit check status with associated sense data indicating ERA 90, File Contention Notification. Sense bytes 8:9 will indicate X'8030'.
91	Valid Volume Inaccessible The controller presents unit check status with associated sense data indicating ERA 91, Valid Volume Inaccessible, to a Library Mount or Library Universal Mount order of the Perform Library Function command, if: • The VOLSER specified in the order is in the library inventory but a valid copy of the volume is not currently accessible. • The cluster receiving the mount request does not have a consistent volume or a path to an available j cluster with a consistent volume. Sense byte 8 is set as follows:
	Modifier - Description
	01 - The vol_damaged flag is set in the volume's tokens.
92	Command Time Limit Exceeded The controller presents unit check status with associated sense data indicating ERA 92, Command Time Limit Exceeded, to the Perform Subsystem Function - Remote Command Execution order if during synchronous execution, the execution time of the script specified in the parameter data exceeds the time limit also specified in the parameter data.
93	Script Command Error The controller presents unit check status with associated sense data indicating ERA 93, Script Command Error, to the Perform Subsystem Function - Remote Command Execution order if during synchronous execution, the script specified in the parameter data detects an error.
94	File Access Denied - OOS The controller presents unit check status with associated sense data indicating ERA 94, File Access Denied - OOS, to the Perform Subsystem Function - Control File Access order if the order specifies that a file is to be opened and the volume pool the resulting file would be premigrated to does not have any scratch physical volumes. Sense bytes 8:9 will indicate X'2018'.
95:FF	Reserved

Related information

[“Operator information messages” on page 322](#)

Completion codes

This topic lists and explains the completion codes that can be returned by a delayed response message to a user performing operations in the IBM TS7700 Grid. These codes are generally returned after a command is accepted and the operation begins.

The results of an asynchronous operation are reported back to the host or hosts through a delayed response message. Whether the message is a directed delayed response message (sent to a single host) or a broadcast delayed response message (sent to all hosts attached to the I/O subsystem), all delayed response messages generated for the Perform Library Function (PLF) command share a common set of completion codes as shown in [Table 81 on page 314](#).

<i>Table 81. Completion codes</i>	
Completion code	Description
X'00'	Complete - No Errors or Exceptions The requested function was completed and there were no unusual conditions detected.
X'01'	Complete - Vision Not Operational The requested function was completed without VOLSER validation. The requested function normally uses the vision system to validate the VOLSER on the volume label as part of the execution of the function. However, the vision system was not operational at the time the function was performed.
X'02'	Complete - VOLSER Not Readable The requested function was completed without VOLSER validation. The requested function normally uses the vision system to validate the VOLSER on the volume label as part of the execution of the function. However, the VOLSER was not recognized by the vision system because the label was not readable or not present at the time the function was performed.
X'04'	Complete - Demount Signaled Complete before Execution The requested function was a library demount and in order to optimize a subsequent command execution, the demount is signaled as complete before its actual execution has begun.
X'05'	Complete - With Exceptions The requested function has completed but during the execution of the function, exceptions were encountered. • If the request was for an Export or Import operation, the status file on the volume specified in the completion message should be examined to determine what exceptions were encountered. • If the request was for an export operation, virtual volumes specified in the export list volume that are not in the library performing the export are not considered exceptions that would result in this completion code. • If the request was for an import operation, physical volumes specified in the import list volume that are not in the import category of the library performing the import are not considered exceptions that would result in this completion code.

Table 81. Completion codes (continued)	
Completion code	Description
X'06'	Complete - No Volumes Found to Export or Import The request was for an Export operation, but none of the virtual volumes in the export volume list were found in the Virtual Tape Server subsystem the request was issued to. The request was for an Import operation, but there were no stacked volumes in the import category, in the library the request was issued to, that matched any of the stacked volumes specified in the import volume list.
X'07'	Complete - Construct Assignments not Changed The requested function was completed, but construct assignment included in the function could not be completed due to an internal processing error.
X'08'	Complete - Construct Limit Exceeded The requested function was completed, but construct creation included in the function could not be performed because the maximum number of unique names for one of the constructs has already been reached.
X'20'	Canceled - Program Request The requested function was canceled due to the program issuing a Perform Library Function command which specified the Library Cancel order.
X'22'	Canceled - Manual Mode The requested function was canceled because the automated tape library entered manual mode after the operation was queued and the requested function is not allowed in manual mode.
X'23'	Canceled - Library Operator The requested function was canceled by an operator through the library manager console.
X'40'	Failed - Hardware The requested function failed because of some hardware failure condition at the time the function was attempted.
X'41'	Failed - Vision Not Operational The requested function failed because the vision system was not operational at the time the function was attempted. The requested operation requires validation of the VOLSER in order to complete normally.
X'42'	Failed - VOLSER Not Readable The requested function failed because the vision system could not validate the VOLSER of the volume because the label was unreadable or not present at the time the function was attempted. The requested operation requires validation of the VOLSER in order to complete normally.
X'43'	Failed - Volume Inaccessible The requested function failed because the volume specified was in a position which was inaccessible to the library at the time the function was attempted. This completion code is also returned for a Library Mount order that specifies a source category and the device had previously accepted a Library Set Device Category order which specified the Category Order option for the same category and the next volume in the category compatible with the type of device the Perform Library Function order was issued to is inaccessible.

Table 81. Completion codes (continued)

Completion code	Description
X'44'	Failed - Volume Misplaced The requested function failed because the volume specified is misplaced at the time the function was attempted. This completion code is also returned for a Library Mount order that specifies a source category and the device had previously accepted a Library Set Device Category order which specified the Category Order option for the same category and the next volume in the category compatible with the type of device the Perform Library Function order was issued to is misplaced.
X'45'	Failed - Category Empty The requested function failed because it requested a volume using the category parameter from a category which contained no available volumes compatible with the type of device the Perform Library Function order was issued to at the time the function was attempted. The function requires a volume in order to complete normally.
X'47'	Failed - Volume Manually Ejected The requested function failed because the volume had been manually ejected from the library between the time the function was requested and attempted.
X'48'	Failed - Volume No Longer In Inventory The requested function failed because the volume was deleted from the inventory between the time the function was requested and attempted.
X'49'	Failed - Device No Longer Available The requested function failed because the device requested is no longer available to the library.
X'4A'	Failed - Unrecoverable Load Failure The requested function failed because the device requested had an unrecoverable load failure during the attempt to perform the function.
X'4B'	Failed - Damaged Cartridge Ejected For physical volumes The requested function failed because the library determined that the cartridge was damaged in such a way that it could not be loaded on a drive and it has been ejected.
X'4C'	Failed - Device not Rewound and Unloaded A request to demount a volume was received from a direct attached Library Manager control path and the specified device still has a volume mounted. Note: This completion code is not applicable to hosts that send PLF commands through the hosts data path to a device.
X'4D'	Failed - Export or Import List Volume Could Not Be Processed During the execution of an Export or Import Operation, the virtual volume containing the list of volumes to export or import could not be processed. The operation completion message will contain a text message indicating the reason that the volume could not be processed.

Table 81. Completion codes (continued)

Completion code	Description		
X'4E'	Failed - Virtual Volume Mount	Reason Code	Description
	The delayed response message for the mount request indicates the reason for the failure: CBR4171I Mount failed LVOL virtual-volser LIB library-name PVOL physical-volser RSN reason-code	X'10'	Internal error detected
		X'11'	Resend special case
		X'20'	Specific volume is in use on another cluster
		X'21'	Scratch volume selected is in use on another cluster
		X'22'	Valid volume is inaccessible
		X'23'	Local cluster path to volume's data is no longer available
		X'24'	Remote cluster path to volume's data is no longer available
		X'25'	Copy required, but cluster copying is inhibited
		X'26'	Internal Message Timeout During Open Request
		X'27'	Unable to Meet The Configured Synchronous Copy Requirements
		X'30'	Local cluster recall failed; the stacked volume is misplaced
		X'31'	Local cluster recall failed; the stacked volume is inaccessible
		X'32'	Local cluster recall failed; the stacked volume is unavailable
		X'33'	Local cluster recall failed; the stacked volume is no longer in library
		X'34'	Local cluster recall failed; the stacked volume load failure
		X'35'	Local cluster recall failed; the stacked volume access error
		X'38'	Remote cluster recall failed; stacked volume is misplaced
		X'39'	Remote cluster recall failed; stacked volume is inaccessible

Table 81. Completion codes (continued)			
Completion code	Description		
		X'3A	Remote cluster recall failed; stacked volume is unavailable
		X'3B'	Remote cluster recall failed; stacked volume is no longer in library
		X'3C'	Remote cluster recall failed; stacked volume load failure
		X'3D'	Remote cluster recall failed; stacked volume access error
		X'40'	Insufficient cache space
		X'41'	World-wide ID mismatch
		X'42'	Excessive concurrent large volume mounts detected
		X'43'	BVIR volume is too small to store the result
		X'44'	Encryption Exchange Failed Due To An Expired Certificate
		X'45'	BVIR Failure Due to a MC With More Than One Copy Consistency Point Defined
X'80'	Reserved This completion code is reserved for host control program usage only.		

Note: For the IBM tape libraries, the verification that a volume is in the correct location is performed when the door to the library is closed, not at the execution of the operation unless that operation is the result of a library audit order.

When the library attempts to execute an eject operation as a result of a Library Set Volume Category PLF order and the operation fails for one of the following completion codes, the volume is re-assigned to the category it was in before the Library Set Volume Category PLF order was accepted:

- **X'40'** Failed - Hardware
- **X'43'** Failed - Volume Inaccessible
- **X'44'** Failed - Volume Misplaced

Note: A device can become unavailable to the library either through action at the library manager console or due to a failure of the device detected by the library manager. In general, a device is made not available to the library so that service can be performed on the device.

Related information

[“Error Recovery Action codes” on page 289](#)

[“Operator information messages” on page 322](#)

[“Reference” on page 289](#)

Immediate copy failure reason codes

This topic lists and explains the failure codes that can be returned with a Rewind-Unload command where one or more of the immediate copies associated with the volume did not complete.

If an immediate copy fails before the Rewind-Unload command completes, a host must be able to isolate the reason for the failure. Enhanced sense data is captured to provide the extra information that software or the operator can use to determine subsequent recovery actions. Failure reason codes are returned that contain the enhanced sense data. Upon receipt of these codes, the software or operator can choose to continue with the copies completed, resubmit the job, or fail the job. Possible reasons for an immediate copy failure include:

- Copies are disabled because the cluster is out of physical scratch volumes
- Copies are disabled because the cluster is out of cache space
- Copies have been disabled using a Host Console Request
- A cluster has enter the Service state

The failure reason codes identify any of the applicable reasons for the failure, and indicate whether the failure is expected (due to service or copy disabled) or unexpected (due to link failures or copy timeout). Additionally, sense data also includes counts for required immediate copies and actual number completed.

Sense data: immediate copy count

The firmware storage manager (FSM) Error field displays an error code in the following format: X'1C'. It provides information about the number of copies that were required and the number of copies that were able to be completed due to the reason code specified in byte 19:

Reason codes X'00'-X'7F'

The condition affecting the number of copies was unexpected.

Reason codes X'80'-X'FF'

The condition affecting the number of copies was expected.

The following sense data, specified in byte 18, is also provided:

Bits 0-3

Copies expected

Number of immediate mode copies required based on management class definition

Copy count override, including the source copy

Bits 4-7

Copies completed

Number of immediate mode copies completed, including the source copy

Note: When operating in an IBM Z® (z/OS) environment, this sense information is also provided and formatted in the IOS0001 message.

[Table 82 on page 320](#) and [Table 83 on page 320](#) displays a list of possible reason codes and their conditions. The conditions are valid when:

- Not all copies or the required RUN copies defined in Copy Override Settings have succeeded.
- The number of required copies is not satisfied due to one or more conditions described by the **Description** column.

<i>Table 82. Immediate copy failure reason codes, unexpected reasons</i>		
Completion code	Reason code tag	Description
0x01	GCM_RUN_FAIL_NO_SOURCE	All the consistent copy sources are unavailable. The reason is undetermined and can include: host copy is disabled, cluster is offline, an unexpected outage occurred, or the cluster is in forced service mode.
0x02	GCM_RUN_FAIL_CL_OUTAGE	At least one copy source is available. One or more target or source clusters have experienced an unexpected outage (offline, dual link failures, or other).
0x03	GCM_RUN_FAIL_JOB_TIMEOUT	At least one copy source is available. The target cluster is running, but the monitor cluster detects the job is timed out by taking too long (40 minutes or longer) None of the failed sites have an unexpected outage.
0x04	GCM_RUN_FAIL_JOB_DOWNGRADE	At least one copy source is available. One or more targets downgraded a copy job from immediate to immediate-deferred after 3 unsuccessful copy attempts, or because all the sources are already migrated. None of the failed sites have an unexpected outage. None of the failed sites have a job timeout.
0x05	GCM_RUN_FAIL_UNEXPECT_RSN	At least one copy source is available. One or more targets have an unexpected outage that is not categorized by any other reason codes.

<i>Table 83. Immediate copy failure reason codes, expected reasons</i>		
Completion code	Reason code tag	Description
0x80	GCM_RUN_FAIL_NO_SCRATCH	At least one copy source is available. One or more targets are copy-disabled due to an out-of-physical-scratch state. None of the failed sites have unexpected error reason

<i>Table 83. Immediate copy failure reason codes, expected reasons (continued)</i>		
Completion code	Reason code tag	Description
0x81	GCM_RUN_FAIL_LOW_CACHE_RESOURCE	At least one copy source is available. One or more targets are copy-disabled due to low cache resources. None of the failed sites have an unexpected error reason. None of the failed sites are copy-disabled due to an out-of-physical-scratch state.
0x82	GCM_RUN_FAIL_CL_IN_SERVICE	At least one copy source is available. One or more targets or sources are in service. None of the failed sites have an unexpected error reason. None of the failed sites are copy-disabled due to an out-of-physical-scratch state. None of the failed sites are in a low-cache-resources state.
0x83	GCM_RUN_FAIL_HOST_COPY_DISABLE	At least one copy source is available. One or more targets or sources are host copy-disabled. None of the failed sites have an unexpected error reason. None of the failed sites are copy-disabled due to an out-of-physical-scratch state. None of the failed sites are in a low-cache-resources state.
0x84	GCM_RUN_FAIL_HOT_LVOL	At least one copy source is available. The copy is deferred due to a hot token at the target cluster Reconciliation is required first. None of the sources or targets are host copy-disabled. None of the failed sites have an unexpected error reason. None of the failed sites are copy-disabled due to an out-of-physical-scratch state. None of the failed sites are in a low-cache-resources state.

If multiple reason codes can be applicable, the lowest number of reason code is surfaced. This is because reason code numbers are inversely proportional to the critical level of the situation: lower code numbers indicate a higher critical level of solution in the domain. For example, in a three-way domain where all

three clusters have RUN copy mode enabled and no copy override settings are defined. When one target is in service and another target is offline the following two reason codes below are applicable:

- 0x02: GCM_RUN_FAIL_CL_OUTAGE
- 0x82: GCM_RUN_FAIL_CL_IN_SERVICE

However, only the reason code with the smaller number (0x02) is returned.

Related information

[“Copy export overview” on page 112](#)

[“Error Recovery Action codes” on page 289](#)

[“Virtual volume planning” on page 89](#)

[“Operator information messages” on page 322](#)

[“Physical” on page 91](#)

[“z/OS I/O definitions” on page 82](#)

Operator information messages

This topic defines the intervention and informational messages for Library, Media, Tape Drive, Library Manager, TS7700, and Controller that are used by an operator or storage administrator.

During normal and exception processing, intervention or action by an operator or storage administrator may be required. The intervention or action requires immediate attention to continue library processing or something that can be handled later. A TS7700 product can also generate informational messages. Informational messages provide information about an operation that is taking place within the machine that might require operator action. Informational messages are always sent to the available notification channels by default.

When these conditions or events are encountered, a text message is logged to the available notification channels: host console, MI event page, SNMP, and RSyslog. You can view and monitor these messages (Event, Host Message, or Call Home MDE) through the host console and the events by using the **Events** panel on the TS7700 MI. You can also view and modify these messages by using the **Notification Settings** panel on the TS7700 MI. The **Notifications Settings** panel also works as a catalog to search for descriptions of Event, Host Message, or Call Home MDE. From this panel, you can set up to send the text messages to all the hosts attached to the subsystem by enabling the **Host Notification** option. These text messages can be monitored through the host console, TS7700 web interface, SNMP and/or RSyslog which are called notification channels.

To set up to send all messages to the hosts attached to a TS7700, go to the **Notification Settings** panel and select **Actions > Modify Host Notification State by Cluster**. See [Figure 50 on page 322](#) for an example of the **Notification Settings** panel that is displayed on the TS7700 MI.

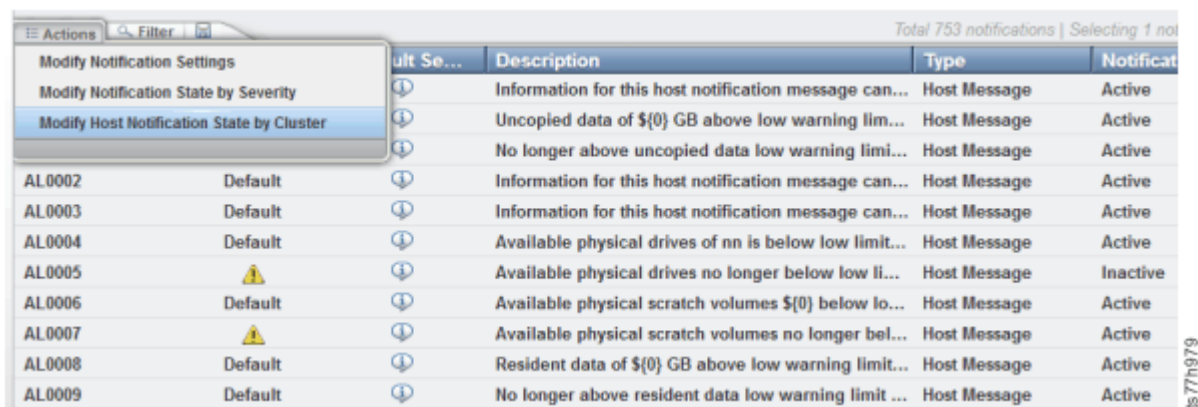


Figure 50. Menu to enable and disable host notification

From the **Modify Host Notification State by Cluster** dialog box, select **Cluster Name**, **Active**, and then click **OK**. See [Figure 51 on page 323](#).



Figure 51. Host notification state by cluster dialog box

Notification messages

There are three types of notifications that are generated by the system:

- Events (OPxxxx messages in a CBR3750I message in the host)
- Host Message (Gxxxx, ALxxxx, EXXXX, Rxxxx in a CBR3750I message in the host)
- Call Home MDE in SIM (in a IEA480E message in the host)

In addition to notifications described above, the z/OS platform also supports displaying the following host console message:

```
CBR3750I Message from library library-name: message-text:Severity Impact: severity-impact-text*. Customer impact: customer-impact-text*
```

Where:

- *library-name* identifies the source of the message. Messages can come from a native library partition or the composite or distributed libraries in a TS7700. This is an eight-character library name that was previously defined on library definitions panels through z/OS.
- *message-text* contains the information being provided. It includes a five-character message ID field that can be examined by message automation software to filter or route specific messages. Message-text can be up to 240 characters in length.
- *severity-impact-text* describes the severity of the message. See [Table 84 on page 324](#).
- *customer-impact-text* contains an optional information customer can set up through TS7700 MI Notification Settings interface. If the user (customer) provides a custom severity as part of the Notification Settings table on the TS7700 MI, the custom severity is included in this field.

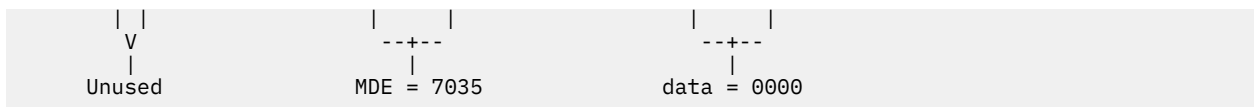
For a Call Home MDE, the system generates an IEA480E message. IEA480E is a Service Information Message (SIM) console message and has the following format:

```
IEA480E Message yyyy, {TLIB | TCU | TVIR | TAPE}, mt, {ACUTE | SERIOUS | MODERATE | SERVICE} ALERT,
```

```
SER=mmpp-sssss, MC=mc, ES=es, ID=id, REF= ref1-ref2-ref3, UM=um1-um2-um3, {CLEAN | CLEAN/SERVICE | CLEANED} , REPEATED
```

The Call Home MDE is part of SIM REFCODE= nnnn-nnnn-nnnn. The following diagram is an example of how to locate the MDE code:

REFCODE 1	REFCODE 2	REFCODE 3
E 0 0 0	7 0 3 5	0 0 0 0



Note: The host message contains only the MDE code. To view the description of MDE, use the **Notification Settings** panel on the TS7700 MI.

For more information about SIMS, refer to [“Service information messages”](#) on page 366.

Message severity

For each message, a severity code is assigned based on the action required and potential to impact operations. The following table describes message severity and the action that needs to be taken:

Table 84. Message severity

Impact	Description	Action
Critical	Operations in the reporting TS7700/Library are stopped, all jobs allocated may fail.	Immediate action by operator, system administrator or service representative is needed.
Serious/Error	One or more jobs may fail, some virtual volumes may be inaccessible, mounts are suspended, performance may be degraded.	Important to examine message, take action as needed.
Impact	No immediate impact to operations, but ejects cannot proceed, input station processing problem, early warning for serious type interventions including performance degradation, copies may not be performed or are degraded.	Examine message as time allows.
Warning	No immediate impact to operations, redundant resource lost, installation/configuration problem or change, drive cleaning may be impacted.	Examine message as time allows.
Information	Informational message about operations in TS7700/Library	Log for historical review.

Message product area

The product area associated with the message is also listed and it could be used to decide who to evaluate the message. The product areas are:

- Library - regarding a physical library
- Media - regarding a physical tape cartridge
- Tape Drive - regarding a physical tape device
- Library Manager - regarding a library manager code and hardware
- TS7700 - regarding the TS7700 code and hardware
- Controller - regarding the controller code or hardware

Intervention message text

The following table describes the intervention message texts:

The Trigger Type (TT) column provides guidelines on which interventions or events would be monitored by host automation. The column indicates whether the event is a setting of a condition (“C” or “S”) or

a clearing of a condition (“c” or “r”). The column also indicates whether the intervention or event is a customer (“C” and “c”) responsibility or an IBM (“S” and “r”) responsibility.

- C – Customer responsibility – Condition is set
- c – Customer responsibility – Condition is cleared
- S – IBM responsibility – Condition is set – Notify IBM
- r – IBM Responsibility – Condition is reset – Notify IBM
- Blank – requires no trigger

Table 85. Intervention message texts				
Message ID	Impact	TT	Product Area	Intervention Message Text
None	Informational		TS7700	Temporary Conflict for Volser xxxxxx - LM paused or long drive op
AL0000	Informational	C	TS7700	Uncopied data of xxxx GB above low warning limit of yyyy GB.
AL0001	Informational	c	TS7700	No longer above uncopied data low warning limit of yyyy GB.
AL0004	Informational	S	TS7700	Available physical drives of nn is below low limit of xx
AL0005	Informational	r	TS7700	Available physical drives no longer below low limit of xx
AL0006	Informational	C	TS7700	Available physical scratch volumes nnn below low limit of xxx for pool yy
AL0007	Informational	c	TS7700	Available physical scratch no longer below low limit of xxx for pool yy
AL0008	Informational	C	TS7700	Resident data of nnnn GB above low warning limit of xxxx GB
AL0009	Informational	c	TS7700	No longer above resident data low warning limit of xxxx GB
AL0010	Informational	C	TS7700	Distributed Library xx has a total pending inbound copy backlog of yyyy GB, which is above the low warning limit of zzzz GB
AL0011	Information	c	TS7700	Distributed Library xx has successfully fallen below the inbound copy backlog low warning limit of zzzz GB
AL0012	Information	C	TS7700 TA, CA	Sum of resident data in virtual tape volume tiered partitions of 'xx' GB above low warning limit of 'yy' GB
AL0013	Information	c	TS7700 TA, CA	Sum of resident data in virtual tape volume tiered partitions no longer above low warning limit of 'xx' GB
AL0014	Information	C, S	TS7700	Distributed Library 'xx' has an inbound all copy type backlog that exceeds the high warning limit of 'yy' hours. Volser 'zzzzz' is the oldest copy job in this group at 'nn' hours.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
AL0015	Information	C, S	TS7700	Distributed Library 'xx' has falling below the inbound all copy type backlog high limit of 'yy' hours.
AL0016	Information	C, S	TS7700	Distributed Library 'xx' has an inbound all copy type backlog that exceeds the low warning limit of 'yy' hours. Volser 'zzzzzz' is the oldest copy job in this group at 'nn' hours.
AL0017	Information	C, S	TS7700	Distributed Library 'xx' has falling below the inbound all copy type backlog low limit of 'yy' hours.
AL0018	Information	C, S	TS7700	Distributed Library 'xx' has an inbound non time-delayed copy type backlog that exceeds the high warning limit of 'yy' hours. Volser 'zzzzzz' is the oldest copy job at 'nn' hours.
AL0019	Information	C, S	TS7700	Distributed Library 'xx' has falling below the inbound non time-delayed copy type backlog high limit of 'yy' hours.
AL0020	Information	C, S	TS7700	Distributed Library 'xx' has an inbound non time-delayed copy type backlog that exceeds the low warning limit of 'yy' hours. Volser 'zzzzzz' is the oldest copy job at 'nn' hours.
AL0021	Information	C, S	TS7700	Distributed Library 'xx' has falling below the inbound non time-delayed copy type backlog low limit of 'yy' hours.
AL2000	Informational		TS7700	Database Backup written to Encrypted Physical Tape vvvvvv
AL2001	Informational	C	TS7700	TS7700 is unable to communicate with at least one Encryption Key Manager.
AL3000	Impact	c	TS7700	The TS7700 Virtualization Engine has restored communication with the primary Encryption Key Manager .
AL3001	Impact	c	TS7700	The TS7700 Virtualization Engine has restored communication with the alternate Encryption Key Manager.
AL5000	Informational	C	TS7700	Uncopied data of nnnn GB above high warning limit of xxxx GB
AL5001	Informational	c	TS7700	No longer above uncopied data high warning limit of xxxx GB
AL5004	Informational	S	TS7700	Available physical drives of nnn is below critical limit of xxx
AL5005	Informational	r	TS7700	Available physical drives no longer below critical limit of xxx
AL5006	Informational	C	TS7700	Available physical scratch volumes nnn below critical limit of xxx for pool yy
AL5007	Informational	c	TS7700	Available physical scratch no longer below critical limit of xxx for pool yy

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
AL5008	Informational	C	TS7700	Resident data of xxxx GB above high warning limit of yyyy GB
AL5009	Informational	c	TS7700	No longer above resident data high warning limit of yyyy GB
AL5010	Informational	C	TS7700	Distributed Library xx has a total pending inbound copy backlog of yyyy GB, which is above the critical warning limit of zzzz GB
AL5011	Informational	c	TS7700	Distributed Library xx has successfully fallen below the inbound copy backlog critical warning limit of zzzz GB
AL5012	Informational		TS7700	Auto removal of volumes has completed on this disk-only cluster
AL5013	Informational		TS7700	Physical volume xxxxxx from <cluster name or library id> has been erased
AL5014	Informational		TS7700	BVIR volume map exceeds <maximum number of records> records
AL5015	Information	C	TS7700, TA, CA	Sum of resident data in virtual tape volume tiered partitions of 'xx' GB above high warning limit of 'yy' GB
AL5016	Information	c	TS7700, TA, CA	Sum of resident data in virtual tape volume tiered partitions no longer above resident data high warning limit of 'xx' GB
AL5021	Information	C	TS7700	Sum of resident data in objects partitions of 'xx' GB above high warning limit of 'yy' GB
AL5022	Information	c	TS7700	Sum of resident data in objects partitions no longer above resident data high warning limit of 'xx' GB
AL5023	Information	C	TS7700	Sum of resident data in objects partitions of 'xx' GB above low warning limit of 'yy' GB
AL5024	Information	c	TS7700	Sum of resident data in objects partitions no longer above low warning limit of 'xx' GB
E0000	Information		TS7700	Export operation started for export list volume 'xx'
E0002	Information	S, C	TS7700	Opening export list volume 'xx' failed
E0005	Information		TS7700	All export processing completed for export list volume 'xx'
E0006	Information		TS7700	Stacked volume 'xx' from 'yy' in 'zz'
E0013	Information		TS7700	Export processing suspended, waiting for scratch volume
E0014	Information		TS7700	Export processing resumed, scratch G0077 made available
E0015	Information	C	TS7700	Export processing terminated, waiting for scratch volume

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
E0016	Information		TS7700	Copying logical export volumes from cache to stacked volumes
E0017	Information		TS7700	Completed copy of logical export volumes to stacked volumes
E0018	Information	C	TS7700	Export terminated, excessive time for copy to stacked volumes
E0019	Information		TS7700	Export processing started for pool 'xx'
E0020	Information		TS7700	Export processing completed for pool 'xx'
E0021	Information		TS7700	DB backup written to stacked volumes 'xx'
E0022	Information		TS7700	Export recovery started
E0023	Information		TS7700	Export recovery completed
E0024	Information		TS7700	'xx' logical volume with invalid copy on 'yy'
E0025	Information		TS7700	Physical volume 'xx' not exported, primary copy for 'yy' unavailable
E0026	Information		TS7700	DB backup written to all of stacked volumes
E0030	Information		TS7700	Stacked volume 'ZZZ' returned to the library 'LLLL'
G0001	Informational		TS7700	Service preparation has started for distributed library xx.
G0002	Informational		TS7700	Service preparation has completed for distributed library xx.
G0003	Warning		TS7700	Service preparation has failed for distributed library xx.
G0004	Information		TS7700	Service preparation has exited for distributed library 'xx'.
G0005	Warning		TS7700	Distributed library xx has entered the immediate deferred state.
G0006	Informational		TS7700	Distributed library xx has exited the immediate deferred state.
G0007	Warning		TS7700	A user at library xx has enabled Read/Write takeover against library yy.
G0008	Warning		TS7700	A user at library xx has enabled Read-Only takeover against library yy.
G0009	Serious/Error	S	TS7700	Autonomic ownership takeover manager within library xx has determined that library yy is unavailable. The Read/Write ownership takeover mode has been enabled.
G0010	Serious/Error	S	TS7700	Autonomic ownership takeover manager within library xx has determined that library yy is unavailable. The Read-Only ownership takeover mode has been enabled.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
G0011	Informational	r	TS7700	Ownership takeover mode within library xx has been automatically disabled now that library yy has become available.
G0012	Warning		TS7700	A user at library xx has disabled the ownership takeover mode within the grid against library yy.
G0013	Serious/Error	S	TS7700	Library xx has experienced an unexpected outage with its peer library yy. Library yy may be unavailable or a communication issue may be present.
G0014	Informational	r	TS7700	Library xx is now available to the peer library yy.
G0015	Informational	r	TS7700	Library xx has restored communication and is now available to the peer library yy.
G0020	Informational		TS7700	Library xx has taken over ownership of volume yyyyyy from library zz using a read/write takeover mode. mmmmmm total volumes have been taken over from peer clusters.
G0021	Informational		TS7700	Library xx has taken over ownership of volume yyyyyy from library zz using a read-only takeover mode. mmmmmm total volumes have been taken over from peer clusters.
G0022	Informational		TS7700	Library xx has reconciled volume yyyyyy against library zz with respect to ownership takeover. mmmmmm total volumes remain in the takeover state against one or more peer libraries.
G0023	Serious/Error	S	TS7700	Library xx has moved volume yyyyyy into the damaged state due to ownership takeover conflict. mmmmmm total volumes now exist in the damaged state.
G0024	Serious/Error	S	TS7700	Library xx has moved volume yyyyyy into the damaged state due to token corruption. mmmmmm total volumes now exist in the damaged state.
G0025	Serious/Error	S	TS7700	Library xx has moved volume yyyyyy into the damaged state due to disaster recovery. mmmmmm total volumes now exist in the damaged state.
G0026	Serious/Error	S	TS7700	Library xx has moved volume yyyyyy into the damaged state. mmmmmm total volumes now exist in the damaged state.
G0027	Informational	r	TS7700	Library xx has moved volume yyyyyy out of the damaged state and into the insert category. mmmmmm total volumes remain in the damaged state.
G0030	Warning	S	TS7700	Library 'xx' Pri,Alt,Pri2,Alt2 Grid Link are degraded.
G0031	Informational	r	TS7700	All grid links for this cluster have left the degraded state.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
G0032	Informational	C	TS7700	XX copies have been queued for over 24 hours. Check Incoming Copy Queue on the management interface for details.
G0033	Informational	c	TS7700	Distributed Library xx has entered the synchronous deferred state due to VOLSER yyyyyy.
G0034	Informational		TS7700	Distributed Library xx has exited the synchronous deferred state.
G0035	Serious/Error	C	TS7700	Distributed Library xx mount failed due to excessive large volume mounts.
G0036	Informational		TS7700	Distributed Library xx completed GGM copy of volume yyyyyy from the composite library zz with CC cc.
G0037	Informational		TS7700	Distributed Library xx failed GGM copy of volume yyyyyy from the composite library zz with CC cc.
G0038	Informational		TS7700	Distributed Library xx failed GGM copy of volume yyyyyy from the composite library zz due to communication failure.
G0039	Impact	S	TS7700	Hot token merge with peer library xx has failed. Retries will be attempted.
G0040	Informational		TS7700	Hot token merge with peer library xx has recovered.
G0041	Warning	S	TS7700	Grid has detected the temporary cache access failure.
G0042	Informational		TS7700	Temporary cache access failure has been recovered.
G0043	Critical	S	TS7700	Cluster will reboot in xx seconds because the cache access has been totally lost.
G0044	Informational	C	TS7700	Distributed Library zz is an island and can not communicate with yy. (*) This message is surfaced only when PFE/Development sets the backdoor manually.
G0045	Informational	c	TS7700	Distributed Library zz is no longer an island. (*) This message is surfaced only when PFE/Development sets the backdoor manually.
G0046	Information		TS7700	Library 'xx' has crossed remote cluster fence threshold. 'yy' has been reported. Library 'zz' has applied 'nn' remote fence action
G0047	Information		TS7700	Library 'xx' has successfully applied remote fence action 'yy' to peer library 'zz'.
G0048	Information		TS7700	Library 'xx' has failed to apply remote fence action 'yy' to peer library 'zz'.
G0049	Information		TS7700	Library 'xx' has successfully applied secondary fence action to peer library 'yy'.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
G0050	Information		TS7700	Library 'xx' has failed to apply secondary fence action to peer library 'yy'.
G0051	Information		TS7700	Library 'xx' has been unfenced successfully.
G0052	Information		TS7700	Unfence library 'xx' has failed
G0053	Information		TS7700	Library 'xx' has applied 'yy' local fence action. Reason: 'zz'
G0054	Information		TS7700	Library 'xx' has detected the remote library 'yy' has applied 'zz' local fence action. Reason: 'nn'
G0055	Information		TS7700	Library 'xx' has crossed the remote cluster fence threshold. 'yy' has been reported. But library 'zz' thinks that library 'nn' looks healthy. Remote cluster fence is not applied
G0056	Information		TS7700	Library 'xx' has crossed remote cluster fence threshold. 'yy' has been reported. Library 'zz' will apply 'nn' remote fence action in 'mm' minutes.
G0057	Information		TS7700	Library 'xx' has successfully surfaced required CUIR vary online attentions.
G0058	Information		TS7700	Library 'xx' has failed to surface required CUIR vary online attentions.
G0059	Information		TS7700	Library 'xx' has successfully surfaced required CUIR vary offline attentions.
G0060	Information		TS7700	Library 'xx' has failed to surface required CUIR vary offline attentions.
G0061	Information		TS7700	Library 'xx' has given up surfacing CUIR vary online attentions to zLPARs 'yy'.
G0062	Information		TS7700	DRSETUP 'xx' HAS SUCCESSFULLY COMPLETED
G0063	Information		TS7700	DRSETUP FAILED. DR FAMILY 'xx' IS EMPTY, CAN NOT PROCEED
G0064	Information		TS7700	DRSETUP FAILED. CANNOT PERFORM THE REQUEST. A CLUSTER IN THE DR FAMILY IS NOT ONLINE
G0065	Information		TS7700	DRSETUP FAILED. WRITE PROTECT IS ALREADY ENABLED FROM THE MANAGEMENT INTERFACE
G0066	Information		TS7700	DRSETUP FAILED. WRITE PROTECT IS ALREADY ENABLED
G0067	Information		TS7700	DRSETUP FAILED. WRITE PROTECT IS NOT ENABLED
G0068	Information		TS7700	DRSETUP FAILED. WRITE PROTECT EXCLUDED CATEGORIES NOT IN SYNC WITHIN THE DR FAMILY
G0069	Information		TS7700	DRSETUP FAILED. CANNOT DISABLE WRITE PROTECT MODE. FLASH COPY EXISTS

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
G0070	Information		TS7700	DRSETUP FAILED. AN ERROR OCCURED PROCESSING THE HOST REQUEST. RETURN CODE = 'xx'
G0071	Information		TS7700	DRSETUP FAILED. VPD UPDATE FAILED
G0072	Information		TS7700	DRSETUP FAILED. VPD SYNCHRONIZATION FAILED
G0073	Information		TS7700	
G0074	Information		TS7700	DRSETUP FAILED. CANNOT DISABLE FLASH COPY FLASH COPY VOLUME IS STILL MOUNTED
G0075	Information		TS7700	DRSETUP FAILED. FLASH COPY OPERATION FAILED
G0076	Information		TS7700	DRSETUP RESETTNG ASYNCHRONOUS OPERATION FLAG HAS FAILED
G0077	Information		TS7700	DRSETUP FAILED. CANNOT ENABLE DOALL/FLASH. FLASH COPY ALREADY EXISTS
G0078	Information		TS7700	Storage Group 'xx' needs a cloud pool assignment on logical volume 'yyyyyy'
G0079	Information		TS7700	Accessible cloud pool needs to be created and assigned to the storage group 'xx' on logical volume 'yyyyyy'
HA001	Critical	S	TS7700	This cluster has entered an error state and will be rebooted
MDE1C03	Warning	S	TS7700	Listener thread exited prematurely
MDE55B9	Warning	S	TS7700	Timeout waiting for LP-Bin execution.
MDE8083	Information	S	TS7700	INFO SIM - Drive Dump Retrieved by Atape
MDE8109	Warning	S	Cache	A cache controller has failed
MDE812B	Warning	S	Cache	Unsupported number of drive enclosures
MDE812C	Warning	S	Cache	Wrong data rate of the cache channel, not set as expected
MDE8185	Critical	S	TSSC	TSSC both Ethernet Paths are down
MDE8186	Warning	S	TS7700 CA	The Transparent Cloud Tiering daemon has died
MDE8195	Warning	S	Cache	Found mismatched drive(s) in Disk Pool
MDE8196	Critical	S	Cache	The status of Array is Failed
MDE8197	Warning	S	Cache	Disk Pool is not encrypted
MDE81A2	Critical	S	Cache	Logical Drive has not optimal status
MDE81A3	Critical	S	Cache	Volume in cache is in a state other than optimal
MDE81A4	Critical	S	Cache	Mdisk in cache is in a state other than optimal
MDE81A5	Critical	S	Cache	Pool in cache is in a state other than optimal
MDE81A6	Warning	S	Cache	Volumes in cache are not on preferred paths

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
MDE81A7	Critical	S	Cache	Node Canister in cache is in a state other than optimal
MDE81A8	Warning	S	Cache	Battery in cache is in a state other than optimal
MDE81A9	Critical	S	Cache	Enclosure in cache is in a state other than optimal
MDE81AA	Warning	S	Cache	Errors for monitoring USBs when cache local encryption is enabled
MDE81AC	Warning	S	Cache	An expansion canister in the cache has failed or been removed
MDEB080	Warning	S	TS7700 CA	The Transparent Cloud Tiering configuration during online processing has failed. A call home will be initiated if this setting is enabled
MDEB081	Critical	S	TS7700 CA	The Transparent Cloud Tiering configuration continues to fail persistently. A call home will be initiated if this setting is enabled
MDEBA00	Critical	S	TS7700 CA	Time skew with a cloud provider
MDEBA01	Critical	S	TS7700 CA	Transparent Cloud Tiering node network down
MDEBA02	Critical	S	TS7700 CA	Bad request for a cloud provider
MDEBA03	Critical	S	TS7700 CA	Precondition failed for a cloud provider
MDEBA04	Critical	S	TS7700 CA	Container creation failed
MDEBA05	Critical	C, S	TS7700 CA	Container already exists
MDEBA06	Critical	S	TS7700 CA	Cloud provider server error
MDEBA07	Critical	S	TS7700 CA	Data Base corrupted for Transparent Cloud Tiering
MDEBA08	Critical	S	TS7700 CA	Internal directory not found for Transparent Cloud Tiering
MDEBA09	Critical	S	TS7700 CA	Resource address file not found for Transparent Cloud Tiering
MDEBA0A	Critical	S	TS7700 CA	LKM down for Transparent Cloud Tiering
MDEBA0B	Critical	S	TS7700 CA	Filesystem corrupted for Transparent Cloud Tiering
MDEBA0C	Critical	S	TS7700 CA	Directory error for Transparent Cloud Tiering
MDEBA0D	Critical	S	TS7700 CA	Key manager error for Transparent Cloud Tiering
MDEBA0E	Critical	S	TS7700	Container pair root directory not found for Transparent Cloud Tiering
MDEBA0F	Critical	S	TS7700 CA	SSL handshake exception for a cloud provider
MDEBA10	Critical	S	TS7700 CA	SSL handshake bad certificate exception for a cloud provider
MDEBA11	Critical	S	TS7700 CA	SSL handshake invalid path certificate exception for a cloud provider

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
MDEBA12	Critical	S	TS7700 CA	SSL handshake unknown exception for a cloud provider
MDEBA13	Critical	S	TS7700 CA	SSL peer unverified exception for a cloud provider
MDEBA14	Critical	S	TS7700 CA	SSL protocol exception for a cloud provider
MDEBA15	Critical	S	TS7700 CA	SSL exception for a cloud provider
MDEBA16	Critical	S	TS7700 CA	SSL no cert exception for a cloud provider
MDEBA17	Critical	S	TS7700 CA	SSL not trusted cert exception for a cloud provider
MDEBA18	Critical	S	TS7700 CA	SSL invalid algorithm exception for a cloud provider
MDEBA19	Critical	S	TS7700 CA	SSL invalid padding exception for a cloud provider
MDEBA1A	Critical	S	TS7700 CA	SSL unrecognized message for a cloud provider
MDEBA1B	Critical	S	TS7700	Unexpected Error for Transparent Cloud Tiering
OP0001	Serious/Error	C	Library	The convenience I/O station should be empty but is not. Visually check the station.
OP0002	Serious/Error	S	Library	A cartridge has been dropped.
OP0003	Information	C	Library	* The I/O station is full.
OP0004	Information	C	Library	* The virtual library is full.
OP0005	Serious/Error	C	Media	A duplicate VOLSER (xxxxxx) was ejected to the convenience I/O station.
OP0006	Impact	C	Media	A duplicate VOLSER (xxxxxx) was left in the convenience I/O station.
OP0007	Impact	C	Media	A VOLSER (xxxxxx) with an unknown media type has been ejected to the convenience I/O station.
OP0009	Impact	C	Media	An invalid VOLSER (xxxxxx) has been ejected to the convenience I/O station.
OP0010	Impact	C	Library	*During an inventory update operation, a VOLSER (xxxxxx) was ejected to the convenience I/O station because there were no free cells.
OP0011	Impact	S	Media	An error occurred for cartridge xxxxxx during insert from convenience I/O slot number yy to cell: Rack number: nn Rack column: mm Rack row: zz
OP0012	Impact	C	Media	An unreadable VOLSER was left in high-capacity input rack cell yyyy.
OP0013	Impact	C	Media	The cartridge label located at cell (rack number: nn, rack column: mm, rack row: zz) has an unknown media type.
OP0014	Impact	C	Media	An invalid VOLSER (xxxxxx) was left in the convenience I/O station.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0015	Impact	C	Media	The cartridge label located at cell (rack number: nn, rack column: mm, rack row: zz) is unreadable.
OP0016	Impact	C	Media	The cartridge label located at cell (rack number: nn, rack column: mm, rack row: zz) is invalid.
OP0017	Warning	S	Tape Drive	A load or unload failure has occurred on device: 'xxxx'
OP0018	Impact	C	Media	Target Storage Pool nn is out of physical volumes.
OP0019	Impact	S	Media	VOLSER xxxxxx is damaged.
OP0020	Impact	C	Library	* The convenience I/O station door is open.
OP0021	Impact	C	Library	* The convenience I/O station door is open.
OP0022	Serious/Error	S	Media	Unknown intervention for condition xxxxxx.
OP0023	Serious/Error	C	Media	VOLSER (xxxxxx) could not be put away. It was ejected to high-capacity output rack cell: yyyy.
OP0024	Impact	C	Library	A duplicate VOLSER has been found at cell nnn.
OP0025	Serious/Error	S	Library	A duplicate VOLSER has been found at cell nnn. A cartridge could not be released from gripper x, accessor y.
OP0026	Serious/Error	S	Library	A cartridge has been dropped.
OP0027	Serious/Error		Library	Pool nn is defined with a different media class and was reset to match.
OP0028	Critical, Serious/Error Note 1	S	Library	An emergency stop has occurred.
OP0029	Serious/Error	C	Media	Damaged VOLSER (xxxxxx) ejected to the convenience I/O station.
OP0030	Serious/Error	C	Media	Cartridge (xxxxxx) has been left in uninstalled device.
OP0031	Impact	S	Tape Drive	Device xxx is not ready.
OP0032	Impact	S	Tape Drive	Device xxx is reporting an element address of zero. Call service.
OP0033	Impact	C	Library	High capacity input station should be empty but is not.
OP0034	Impact	C	Media	A mislabeled cleaner cartridge has been left in device xxx feed slot. Remove the cartridge.
OP0035	Warning	S	Tape Drive	A recoverable error occurred on device xxx. A service call may be needed if the error persists.
OP0036	Warning	C	Media	A cartridge containing invalid media has been left in device xxx feed slot. Remove the cartridge.
OP0037	Warning	C	Media	An invalid media VOLSER <xxxxxx> has been ejected to the convenience I/O station.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0038	Serious/Error	C	Media	A cartridge or cartridge label located at cell x y zz is upside-down.
OP0039	Serious/Error	C	Media	A duplicate VOLSER has been found at cell yyyy.
OP0040	Serious/Error	C	Media	The cartridge label located at cell yyyy is unreadable.
OP0041	Serious/Error	C	Media	The cartridge label located at cell yyyy is invalid.
OP0042	Critical, Serious/Error Note 1	S	Library	The system has failed. A service call is required.
OP0043	Critical	S	Library	* The accessor or gripper configuration has changed.
OP0044	Impact	C	Library	* The top two I/O station cells are inaccessible. Move cartridges to cell 3.
OP0045	Information	C	Media	VOLSER xxxxxx cannot be removed from its home location.
OP0046	Impact	C	Library	VOLSER (xxxxxx) cannot be removed from the high-capacity station cell: yyyy.
OP0047	Impact	S	Tape Drive	The device xxxxxx has failed and a service call is required to correct the problem.
OP0048	Warning	C	Media	A VOLSER 'xxxxxx' has an incorrect media type on the external label.
OP0049	Serious/Error	S	Media	A physical device's install status or online status has changed for a device attached to the TS7700.
OP0050	Serious/Error	S	Media	Control of this physical device has been switched to the node on this cluster (the cluster where the operator intervention is listed).
OP0051	Warning		Media	* The library is out of HPCT cleaner cartridges.
OP0052	Serious/Error	C	Media	A VOLSER (xxxxxx) with an unknown media type has been ejected to the convenience I/O station.
OP0053	Serious/Error	C	Media	A VOLSER (xxxxxx) with an unknown media type has been ejected to high-capacity output facility cell: yyyy.
OP0054	Impact	C	Media	VOLSER (xxxxxx) cannot be removed from convenience I/O station.
OP0056	Impact	C	Media	A VOLSER (xxxxxx) with an unknown media type has been left in the convenience input station.
OP0057	Impact	C	Media	A VOLSER (xxxxxx) with an unknown media type has been left in the high-capacity input station.
OP0058	Serious/Error	C	Media	An invalid VOLSER (xxxxxx) has been ejected to the convenience I/O station.
OP0059	Serious/Error	C	Media	The cartridge label located at cell yyyy has an unknown media type.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0060	Serious/Error	C	Media	During an Inventory Update operation, VOLSER xxxxxx was ejected to the convenience I/O station because there were no free cells.
OP0061	Serious/Error	C	Media	During an Inventory Update operation, VOLSER xxxxxx was ejected to the high capacity station because there were no free cells.
OP0062	Critical, Impact Note 1	S	Library	Power failure on accessor x. A service call is required.
OP0063	Warning	C	TS7700	Limited cache free space.
OP0064	Warning	S	Library Manager	Dual Write has failed. A service call is required.
OP0065	Impact	C	TS7700	Out of cache resources.
OP0066	Information		Media	*One or more volumes have been inserted into the library and marked unassigned.
OP0067	Impact		Media	Eject failed for VOLSER xxxxxx. This operation was initiated by the Library Manager.
OP0068	Informational		Library Manager	A Library Manager switch has completed. This switch was initiated by the operator.
OP0069	Warning		Library Manager	A Library Manager switch has completed. This switch was due to an error.
OP0070	Warning		Library Manager	A hard drive has failed. Call service.
OP0071	Warning		Library Manager	Mirroring disabled. Call service. Library is operational but degraded. Or LM-x mirroring disabled. Call service. Library is operational but degraded.
OP0072	Critical	S	Library	Barrier door A is not fully retracted. Call service.
OP0073	Critical	S	Library	Barrier door B is not fully retracted. Call service.
OP0074	Serious/Error		Library Manager	Controller on port xx requires a higher level of Library Manager.
OP0075	Impact		Library Manager	Database discrepancies have been found. Call service. Library is still operational.
OP0076	Serious/Error	S	Media	VOLSER xxxxxx cannot be found. Check home cell: yyyy and accessor A, gripper 1.
OP0077	Serious/Error	S	Media	VOLSER xxxxxx cannot be found. Check home cell: yyyy and accessor A, gripper 2.
OP0078	Serious/Error	S	Media	VOLSER xxxxxx cannot be found. Check home cell: yyyy and accessor B, gripper 1.
OP0079	Serious/Error	S	Media	VOLSER xxxxxx cannot be found. Check home cell: yyyy and accessor B, gripper 2.
OP0080	Warning		Library	Error writing to dual write log (on Library Manager A or B).
OP0081	Critical	S	Library	An emergency stop has occurred, or accessor A or B has failed. A service call is required.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0082	Impact	S	Media	VOLSER xxxxxx left in convenience I/O slot nn due to vision system failure.
OP0083	Impact	S	Media	VOLSER xxxxxx left in high capacity rack cell xx y zz due to vision system failure.
OP0084	Warning		Library Manager	Scratch mount performance is degraded. A service call is required.
OP0085	Warning		Library Manager	Database performance is degraded.
OP0086	Warning		Library Manager	Problem detected with Token Ring connection. Call service.
OP0087	Warning	S	Library Manager	Logging is now disabled on LM-x. Call service.
OP0089	Warning		TS7700	The number of xxxxxxxx constructs has reached the maximum number allowed (yyy).
OP0090	Warning		Library Manager	The number of xxxxxxxx constructs has exceeded yyy. The maximum number allowed is zzz.
OP0091	Serious/Error	S	Library Manager	The yyyyy internal LAN switch (HUB) has failed or is not configured correctly. Call service.
OP0092	Serious/Error	S	Library Manager	A database error has occurred. View help panel for SQL error code xxxx. Call service.
OP0093	Warning	S	Library Manager	NVRAM read failure on LM-A. Call service.
OP0094	Warning	S	Library Manager	NVRAM write failure on LM-A. Call service.
OP0095	Warning	S	Library Manager	NVRAM read failure on LM-B. Call service.
OP0096	Warning	S	Library Manager	NVRAM write failure on LM-B. Call service.
OP0098	Serious/Error	S	Library Manager	The yyyyy internal LAN switch (HUB) is not configured correctly. Call service.
OP0099	Informational	C	TS7700	VOLSER xxxxxx was ejected during recovery processing.
OP0100	Information	C	Media	A read-only status physical volume 'xxxxxx' has been ejected.
OP0101	Critical	C	Media	* The cluster is out of empty physical volumes.
OP0102	Critical	C	Media	A physical volume has a label error. Internal: 'xxxxxx', External: 'yyyyyy'.
OP0103	Critical	S	TS7700	A permanent, non-recoverable tape volume cache error has occurred.
OP0104	Serious/Error	S	TS7700	An orphaned virtual volume (xxxxxx) has been found. Call service.
OP0106	Information	C	TS7700	Virtual volume 'xxxxxx' was only partially read.
OP0107	Warning	S	TS7700	Virtual volume 'xxxxxx' was not fully recovered from damaged physical volume 'yyyyyy'.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0112	Warning	S	Tape Drive	Device serial number 'xxxx' has been made offline and/or unavailable by the TS7700 engine with a reason code of 'yy'.
OP0115	Information	S	Media	The cluster attempted unsuccessfully to eject a damaged physical volume 'xxxxxx'.
OP0119		S		Database restore from volume <xxxxxx> failed. Attempting to restore from next most recent event.
OP0120	Information	C	Media	Mount of virtual volume 'xxxxxx' failed because physical volume 'yyyyyy' is misplaced. (reason code='zz')
OP0121	Warning	S	Media	Mount of virtual volume 'xxxxxx' failed because physical volume 'yyyyyy' is inaccessible.
OP0122	Warning	C	Media	Mount of virtual volume 'xxxxxx' located on physical volume 'yyyyyy' failed. (reason code='zz')
OP0123	Information	C	Media	Physical volume 'xxxxxx' is in read-only status due to successive media errors.
OP0124	Warning	C	Media	Physical volume 'xxxxxx' is unavailable.
OP0127	Critical	S	Tape	An invalid mixture of physical drive types was detected.
OP0128	Critical	S	Tape Drive	The TS7700 engine does not have enough physical drives to continue operation.
OP0130	Information	C	Media	Physical volume 'xxxxxx' failed scratch mount. Its label cannot be read and the tape must be re-initialized.
OP0132	Warning	C	TS7700	Stacked volume xxxxxx could not be ejected because the convenience I/O station is full, or the door is open.
OP0134	Information	C	Media	Physical volume 'xxxxxx' is write-protected.
OP0135	Information		Media	TS7700 unsuccessfully attempted to eject write-protected physical volume 'xxxxxx'.
OP0136	Information	S	Media	Physical volume 'xxxxxx' moved to category FF08 due to unrecovered active data.
OP0138	Critical	C	Media	The common scratch pool (Pool 00) is out of 'xxxx' media physical volumes.
OP0139	Critical	C	Media	Storage pool 'xx' is out of scratch physical volumes.
OP0140	Information		Media	VOLSER 'xxxxxx' could not be moved from Storage Pool 'yy' to Storage Pool 'zz'. Error code = 'nn'.
OP0144	Warning	S	Media	Eject failed on physical volume 'xxxxxx' that contains active data. Error code = 'yy'.
OP0145	Warning	S	TS7700	Unable to make stacked volume xxxxxx read-only.
OP0146	Warning	S	TS7700	Unable to make stacked volume xxxxxx read-write.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0147	Warning	S	TS7700	Stacked volume xxxxxx is in an invalid state.
OP0149	Critical	C	Media	Storage pool 'xx' is out of write compatible physical scratch volumes.
OP0150	Information	C	Media	The physical volume 'xxxxxx' is near or has reached the End of Life Threshold.
OP0151	Warning	S	TS7700	The time on the TS7700 could not be adjusted. Contact your IBM service representative.
OP0152	Information	C	Media	Active data on ejected physical volume 'xxxxxx' need to be recovered.
OP0153	Information	C	Media	Physical volume 'xxxxxx' is misplaced.
OP0155	Impact	S	f	TS7700 Device nnnn is configured incorrectly. 3592-E05 must be set to emulate a 3592-J1A.
OP0164	Information		TS7700	The TS7700 Engine has initiated auto removal of volumes on this disk-only cluster.
OP0165	Information	C	Media	One or more non-writable physical volumes were found.
OP0166	Information	C	Media	Copy export did not export physical volume 'xxxxxx' because of an incorrect format.
OP0167	Information	C	Media	Unsupported media (for example: JA, JJ) is set for First Media,Second Media, or both for Physical Volume Pools(s): 'xx'.
OP0168	Information	C	Media	One or more unsupported empty media has been found and cannot be used by the installed tape drives.
OP0169	Critical	C	TS7700	The 'xx' is out of cache space. The total used, 'yy' TiB, is less than 1 TiB from the total cache space or less than 5% below the total cache space, 'zz' TiB.
OP0170	Warning	C	TS7700	The 'xx' has limited cache free space. The total used, 'yy' TiB, is less than 3 TiB from the total cache space or less than 15% of the total cache space, 'zz' TiB.
OP0171	Information	C	Media	Unsupported scratch media of type 'xxxx' were inserted into the library.
OP0172	Information		TS7700	Automatic removal of logical volumes on this cluster has been disabled due to a small cache resident only partition size.
OP0173	Information		TS7700	Automatic removal of logical volumes on this cluster has been enabled because the cache resident-only partition size is now sufficient.
OP0200	Warning	C, S	TS7700	The local cluster is operating in immediate copy mode and at least one copy did not finish prior to the completion of the Rewind/Unload command.
OP0201	Information	c, r	TS7700	All immediate deferred copy operations are complete.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0202	Warning	C, S	TS7700	One or more volumes opened as part of a synchronous mode copy operation did not synchronize completely across both clusters.
OP0203	Information	c, r	TS7700	Synchronization across both clusters has completed for all volumes that were in the synchronous deferred state.
OP0204	Warning	C, S	TS7700	Copy operations for the local cluster are disabled by the system.
OP0205	Information	c, r	TS7700	The system has enabled copy operations at the local cluster.
OP0206	Information	C	TS7700	Copy operations for the local cluster are disabled by the host.
OP0207	Information	c	TS7700	Copy operations for the local cluster are enabled by the host.
OP0208	Warning	C, S	TS7700	The cluster 'xx' has applied 'yy' local cluster fence action. Reason: 'zz' .
OP0209	Warning	C, S	TS7700	The cluster 'xx' has detected the remote cluster 'yy', has applied 'zz' local fence action. Reason: 'nn'
OP0210	Warning	C, S	TS7700	The cluster 'xx' has successfully completed the remote fence action 'yy' to the peer cluster 'zz'. Reason: 'nn'
OP0211	Impact	c, r	TS7700	The cluster 'xx' has been unfenced successfully.
OP0212	Critical	C, S	TS7700	The cluster 'xx' has failed to apply the remote fence action 'yy' to the peer cluster 'zz' .
OP0213	Critical	C, S	TS7700	Unfence cluster 'xx' has failed.
OP0214	Impact	C, S	TS7700	The cluster 'xx' has crossed remote cluster fence threshold. 'yy' has been reported. The cluster 'zz' has applied 'nn' remote fence action.
OP0215	Warning	C, S	TS7700	The cluster 'xx' has crossed remote cluster fence threshold. 'yy' has been reported. But, the cluster 'zz' assumes the cluster 'nn' looks healthy. Remote cluster fence action is not applied.
OP0216	Impact	C	TS7700	Inbound Copy operations for the COPYRFSH copy jobs on the local cluster 'xx' are disabled by the host.
OP0217	Impact	c	TS7700	Inbound Copy operations for COPYRFSH copy jobs on the local cluster 'xx' are enabled by the host.
OP0218	Impact	C	TS7700	Inbound Copy operations for the deferred copy jobs on the local cluster 'xx' are disabled by the host.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0219	Impact	c	TS7700	Inbound Copy operations for deferred copy jobs on the local cluster 'xx' are enabled by the host.
OP0300	Impact	S	TS7700	One or more virtual volumes have corrupted tokens. Call service.
OP0308	Critical		TS7700	A TS7700 has been taught/configured incorrectly as a cluster.
OP0309	Critical		TS7700	Cluster has been taught/configured incorrectly as a TS7700.
OP0310	Information		TS7700	The data class 'xxxx' was automatically created with the default actions for volume 'yyyyyy'.
OP0311	Information		TS7700	The Storage Class 'xxxx' was automatically created with the default actions for volume 'yyyyyy'.
OP0312	Information		TS7700	The Management Class 'xxxx' was automatically created with the default actions for volume 'yyyyyy'.
OP0313	Information		TS7700	The Storage Group 'xxxx' was automatically created with the default actions for volume 'yyyyyy'.
OP0314	Information		TS7700	The inhibit create command was ignored and one or more constructs were automatically created with the default actions for volume 'xxxxxx' as a result of an imbalance of defined SMS constructs across the domain
OP0315	Information		TS7700	The maximum number of defined constructs has been reached. An imbalance of defined SMS constructs across the domain has occurred. Default constructs were assigned for volume 'xxxxxx'.
OP0316	Critical	S	TS7700	The TS7700 Engine has detected corrupted tokens for one or more virtual volumes.
OP0400	Warning	C	Media	* The library is out of ETC cleaner cartridges.
OP0401	Informational	C	Media	* xxxxx cleaner cartridge (yyyyyy) was ejected due to maximum use.
OP0402	Warning	S	Library	xx percent of mounts performed by accessor y over the past hour required excessive mount recovery. Call service.
OP0403	Warning	S	Library	xx percent of mounts performed by accessor y over the past 24 hours required excessive mount recovery. Call service.
OP0404	Warning	S	Library	Device zzz required excessive mount recovery (xx percent of mounts) over the past hour (accessor y). Call service.
OP0405	Warning	S	Library	Device zzz required excessive mount recovery (xx percent of mounts) over the past 24 hours (accessor y). Call service.
OP0406	Warning		Library Manager	Logging is degraded on LM-x. Call service.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0407	Warning		Library Manager	Communication with the MasterConsole has failed (LM rc = xx, MasterConsole rc = yy). Call service.
OP0408	Warning		Library Manager	LM-x: MasterConsole configuration has failed (rc = yy). Call service.
OP0409	Information		TS7700	The volume hold function was disabled for scratch category 'xxxx'.
OP0410	Information		TS7700	The hold/expire time has been changed to 'xx' hours for scratch category 'yyyy'.
OP0411	Information		TS7700	A fast-ready attribute was deleted for category 'xxxx'.
OP0412	Warning		Media	VOLSER (xxxxxx) has been returned to the station. A service cartridge cannot be inserted via CIO or HCIO.
OP0413	Warning		Library Manager	Possible hard drive failure detected. View help panel for error code = yy.
OP0414	Impact	S	Library	Error threshold exceeded for accessor x. View help panel for error code = yy.
OP0416	Warning		Library	Preferred EASH in frame xx is not responding. Call service.
OP0417	Warning		Library	Non-preferred EASH in frame xx is not responding. Call service.
OP0418	Warning		Library	Port xx on the preferred EASH in frame yy has failed. Call service.
OP0419	Warning		Library	Port xx on the non-preferred EASH in frame yy has failed. Call service.
OP0422	Warning		Library	Device xxx with World Wide Node Name yy.yy is cabled incorrectly. It is in the wrong virtual or physical library.
OP0423	Warning	C	Media	A VOLSER (xxxxxx) with an unsupported media type has been left in the convenience input station.
OP0424	Impact	S	Media	An unreadable VOLSER was left in the convenience I/O station, element address xxxx.
OP0425	Warning	S	Tape Drive	Two devices (xxx, yyy) have the same serial number (zzzzzz). Both have been uninstalled. Call service.
OP0426	Warning	S	Tape Drive	Two devices (xxx, yyy) have the same element addr (zzzz). Both have been uninstalled. Call service.
OP0427	Warning	S	Library	The 3584 library reported that calibration is required.
OP0428	Warning	S	Library	The 3584 library reported a hardware error ('xx') . Contact your IBM service representative.
OP0430	Critical	S	Library	The TS7700 has issues communicating with the tape library or the tape library is not responsive to requests. Contact your IBM service representative.
OP0431	Information			Reserved
OP0432	Information			Reserved

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0433	Information		TS7700	The Send Interventions to Host Console settings on the Events panel has been turned on.
OP0434	Information		TS7700	The Send Interventions to Host Console settings on the Events panel has been turned off.
OP0435	Serious/Error	S	Tape Drive	Two devices (xxx;yyy) have the same serial number (zzzzzz). Second has been uninstalled. Call service.
OP0436	Warning	S	Tape Drive	Two devices (xxx;yyy) have the same element address (zzzz). Second has been uninstalled. Call service.
OP0437	Serious/Error	S	Tape Drive	Cartridge xxxxxx has been left in uninstalled device yyy. Call service.
OP0438	Warning	S	Tape Drive	Device yyy is reporting an element address of zero. Call service.
OP0439	Warning	C	TS7700	TS7700 has lost communication with the primary Encryption Key Server.
OP0440	Warning	C	TS7700	TS7700 has lost communication with the alternate Encryption Key Server.
OP0441	Information	S	Library	Possible degradation due to 3584 TapeAlert error (nnnn). Service call Home has been generated.
OP0442	Information	C	Library	Physical volume 'xxxxxx' is inaccessible.
OP0443	Information	S	Library	The virtual tape library has detected an inconsistency with the physical tape library.
OP0444	Warning		Library	LM PC has not been rebooted in 6 months.
OP0445	Warning	C	TS7700	The primary Encryption Key Server was set to UNAVAILABLE.
OP0446	Warning	C	TS7700	The alternate Encryption Key Server was set to UNAVAILABLE.
OP0448	Information	C	Media	More than 'xx' errors were encountered for physical volume 'yyyyyy'.
OP0449	Information	C	Media	Pool 'xx' has physical volumes of the wrong media class.
OP0450	Information	C	Media	The media type of VOLSER 'xxxxxx' does not match its VOLSER range. The VOLSER was not assigned to a cluster.
OP0451	Critical	C	TS7700	Encryption is enabled. No Encryption Key Servers are configured.
OP0452	Warning	C	TS7700	Encryption Key Server error 'xx' prevented device 'yyyyyy' from encrypting data in storage pool 'zz'.
OP0453	Warning	C	TS7700	Device 'xxxxxx' could not append encrypted data to cartridge 'yyyyyy' (Encryption Key Server error 'zz').
OP0454	Warning	C	TS7700	Device 'xxxxxx' could not decrypt data from cartridge 'yyyyyy' (Encryption Key Server error 'zz').

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0455	Warning	S	Tape Drive	Device 'xxxx' is not in 3592 E05 Native mode. The device was made unavailable.
OP0456	Warning	C	TS7700	Encryption is enabled on the virtual tape library. Device 'xxxx' is not enabled for System Managed Encryption.
OP0457	Warning	S	Tape Drive	Device nnnnn is not in 3592 J1A emulation mode. The device was made unavailable.
OP0458	Serious/Error	S	TS7700	An internal hardware/software error has occurred.
OP0459	Serious/Error	S	TS7700	A disk cache error has occurred.
OP0460	Warning	S	TS7700	A Grid link error xxxxxx has occurred.
OP0461	Impact	S	Tape Drive	A tape drive error: xxxxxx has occurred.
OP0462	Impact	S	TS7700	A fibre switch error xxxxxx has occurred.
OP0463	Warning	S	TS7700	A TSSC error has occurred. The TSSC is unable to call home.
OP0464	Impact	S	Library	A library error has occurred.
OP0465	Impact	S	TS7700	An Autonomic Ownership Takeover Mode communications error occurred. The device is unable to communicate with the remote cluster.
OP0466	Impact	C	TS7700	An encryption key server error xxxxxx error has occurred.
OP0467	Impact	S	Media	Tape cartridge xxxxxx is stuck in a storage cell.
OP0468	Warning		Library	The 3494 Library Manager has an event.
OP0469	Warning		Library	The 3494 Library Manager is in a degraded state.
OP0470	Information		TS7700	Delete Expire capability has been disabled.
OP0471	Critical	C	Media	The Field Microcode Replacement tape 'xxxxxx' cannot be used as a data cartridge.
OP0472	Information		Media	The database backup to physical volume 'xxxxxx' failed during the Copy Export operation as a result of a media error.
OP0473	Information		Media	A media error occurred during the Copy Export operation and the physical volume 'xxxxxx' has been ejected. The medium may be degraded and should not be reused in an export pool.
OP0474	Information		Media	The Copy Export operation did not export physical volume 'xxxxxx' because the primary copy for virtual volume 'yyyyy' is currently unavailable.
OP0475	Information		Media	Copy Export did not export virtual volume 'xxxxxx' because it was not able to premigrate the volume to the export pool.
OP0476	Information		TS7700	The event was cleared automatically.
OP0477	Information		TS7700	The event was cleared by 'xxxx' .

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0480	Information	S	TS7700	Service Call Home will be initiated.
OP0481	Information	S	TS7700	Service Call Home was initiated.
OP0482	Information	S	TS7700	Service Call Home was initiated with CSP case number TSxxxxxxx. Note: - Case number DUP00000000 indicates that no new case was opened as a duplicate case already exists. - Case number CLS00000000 indicates that the case was automatically closed.
OP0483	Critical	S	Cache	A permanent cache problem was encountered.
OP0484	Critical	S	Cache	A permanent cache problem was encountered.
OP0485	Critical	S	Cache	A 3956-CC6 permanent check was encountered.
OP0486	Critical	S	TS7700	A CHECK1 condition was encountered.
OP0487	Critical	S	TS7700	An adapter microcode CHECK1 condition occurred.
OP0488	Critical	C	TS7700	A channel event occurred.
OP0489	Critical	S	TS7700	An undetermined error occurred.
OP0490	Critical	C	TS7700	An operator notification occurred.
OP0491	Critical	S	TS7700	A microcode exception occurred in the ATL daemon.
OP0492	Critical	S	TS7700	An undetermined error occurred.
OP0493	Critical		Control Unit	An informational message was presented by CU.
OP0494	Critical	C	TS7700	An environmental problem has occurred.
OP0495	Critical	S	TS7700	A microcode exception occurred in the tape daemon.
OP0496	Critical	S	TS7700	The tape daemon detected a CRC error.
OP0497	Critical	S	TS7700	A microcode exception occurred in the tape daemon.
OP0498	Critical	S	TS7700	A microcode exception occurred in the BATE daemon.
OP0499	Information	S	TS7700	An error was detected and a Service Call Home has been generated. The call home includes the following SIM(s): SIMID-RESOURCE-REF_CODES 'xx'.
OP0500	Information		TS7700	The times displayed by the local and remote clusters 'xx' differ by more than 5 seconds.
OP0510	Information		TS7700	'xxxx' logged into the Web interface.
OP0511	Information		TS7700	'xxxx' logged out of the Web interface.
OP0512	Information		TS7700	User 'xx' the setting to send future events to host.
OP0514	Information		TS7700	Custom Role 'xxxx' has been changed.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0515	Information		TS7700	SNMP settings have changed. \n Values are: \n SNMP Version: 'xx' \n Enable SNMP Traps: 'yy' \n Trap Community Name: 'zz'
OP0516	Informational		TS7700	Stand-alone mount was initiated for volume xxxxxx on device zzz.
OP0517	Informational		TS7700	Stand-alone demount was initiated on device zzz.
OP0518	Informational		TS7700	Node nnnn has been shut down.
OP0519	Informational		TS7700	Custom Role mmmm has been created.
OP0520	Informational		TS7700	Custom Role mmmm has been deleted.
OP0521	Informational		TS7700	The security settings for local authentication have changed. Local Account Expiration: mmmm. The account will expire if the password is not changed in n days.
OP0522	Informational		TS7700	The security settings for local authentication have changed. Local Account Expiration: mmmm.
OP0523	Informational		TS7700	The security settings for local authentication have changed. Local Account Lock: mmmm. The account will be locked after n unsuccessful attempts to enter the password.
OP0524	Informational		TS7700	The security settings for local authentication have changed. Local Account Lock: mmmm.
OP0525	Critical	S	TS7700	A TAPE DRIVE FAILURE has occurred
OP0526	Critical	S	TS7700	A FibrePath, FibreSwitch, or FibreInterface error has occurred.
OP0527	Informational		TS7700	Stand-alone mount for volume xxxxxx on device zzz completed successfully.
OP0528	Informational		TS7700	Stand-alone demount for volume xxxxxx on device zzz completed successfully.
OP0529	Warning		TS7700	Stand-alone mount for volume xxxxxx on device zzz failed with error code nnnn.
OP0530	Warning		TS7700	Stand-alone demount for volume xxxxxx on device zzz failed with error code nnnn.
OP0531	Warning	C, S	TS7700	The network connection on grid port xx with IP address: n.m.y.z experienced a possible loss of connectivity.
OP0532	Critical	C, S	TS7700	The network connection on grid port xx with IP address: n.m.y.z is not responding.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0533	Informational	C, S	TS7700	The connection between the local cluster and the remote cluster is interrupted or may be experiencing a small level of unbalanced usage. Remote cluster: 'xx' Remote port: 'yy' Remote IP address: 'z.z.z.z' Local cluster: 'nn'
OP0534	Warning	C, S	TS7700	The connection between the local cluster and the remote cluster is losing packets, the connection is unavailable, or the connection is experiencing a level of unbalance usage. Remote cluster: 'xx' Remote port: 'yy' Remote IP address: 'z.z.z.z' Local cluster: 'n'
OP0535	Critical	C, S	TS7700	The connection of local cluster to remote cluster was not available. Remote cluster: 'xx' Remote port: 'yy' Remote IP address: 'z.z.z.z' Local cluster: 'nn'
OP0536	Critical	S	TS7700	The link from local cluster to remote cluster is in the offline state. Remote cluster: 'xx' Remote IP address: 'z.z.z.z' Local cluster: 'nn'
OP0537	Information	C, S	TS7700	The connection of local cluster to remote cluster was unavailable for a brief time or the local cluster was unable to retrieve the status of the remote adapter. Remote cluster: 'xx' Remote port: 'yy' Remote IP address: 'z.z.z.z' Local cluster: 'nn'
OP0538	Warning	C, S	TS7700	The connection of local cluster to remote cluster is not available because the local cluster reports the status of the remote adapter as not available. Remote cluster: 'xx' Remote port: 'yy' Remote IP address: 'z.z.z.z' Local cluster: 'nn'
OP0539	Critical	S	TS7700	The connection between the local cluster and the remote cluster is not available, because the state of the remote adapter is Failed. Remote cluster: 'xx' Remote port: 'yy' Remote IP address: 'z.z.z.z' Local cluster: 'nn'
OP0540	Critical	C, S	TS7700	The link to remote cluster: 'xx' With IP address: 'yyyy' is in the offline state. Network Traffic Controller (NTC) reports link state: 'zz'
OP0541	Warning	C, S	TS7700	Degraded state to gateway IP: gateway IP address.
OP0542	Critical	C, S	TS7700	Failed state to gateway IP: gateway IP address.
OP0543	Warning	C, S	TS7700	The primary and alternate grid adapters have different speeds: Primary nnnn link speed is: xxx Alternate mmmm link speed is: yyy
OP0544	Critical	S	TS7700	The primary grid Ethernet port 'xx' is down.
OP0545	Critical	S	TS7700	The alternate grid Ethernet port 'xx' is down.
OP0546	Informational	S	TS7700	Could not retrieve the date on cluster nnnn.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0547	Critical	C, S	TS7700	A time synchronization failure was detected between cluster nnnn and Cluster mmmm.
OP0548	Warning	S	TS7700	There is no communication with one or more clusters in the Grid.
OP0549	Warning		TS7700	One or more clusters in the Grid are in Service status.
OP0550	Impact	C	TS7700	Service Call Home, TSSC was unable to generate a CSP case number
OP0551	Critical	S	TS7700	A permanent cache problem was encountered.
OP0552	Critical	S	TS7700	A temporary cache problem was encountered.
OP0553	Critical	S	TS7700	The cache has an unreadable sector.
OP0554	Critical	S	TS7700	A cache power supply has failed.
OP0555	Critical	S	TS7700	A cache power or fan assembly has failed.
OP0556	Critical	S	TS7700	The cache has lost redundancy.
OP0557	Critical	S	TS7700	A problem exists with the cabling or drive path inside the cache enclosure.
OP0558	Critical	S	TS7700	A cache component has failed or been removed.
OP0559	Critical	S	TS7700	A cache controller has failed or been removed.
OP0560	Critical	S	TS7700	An environmental service module (ESM) canister in the cache has failed or been removed.
OP0561	Critical	S	TS7700	A cache drive is missing.
OP0562	Critical	S	TS7700	A cache drive is in a degraded state.
OP0563	Critical	S	TS7700	A cache disk has reported errors.
OP0564	Critical	S	TS7700	A cache RAID array has failed drives.
OP0565	Critical	S	TS7700	An unsupported number of drive enclosures exists on a cache loop.
OP0566	Critical	S	TS7700	The reported data rate of a cache drive channel is outside the expected range.
OP0567	Critical	S	TS7700	The data rate could not be obtained on a drive channel for the cache.
OP0568	Critical	S	TS7700	An incorrect number of enclosures exists on a cache loop.
OP0569	Critical	S	TS7700	The number of enclosures on a cache loop cannot be determined.
OP0570	Critical	S	TS7700	Mismatched drives exist in a cache array.
OP0571	Critical	S	TS7700	Disk operation in the cache is degraded.
OP0572	Impact	S	TS7700	Network errors were detected while connecting to the cache.
OP0573	Critical	S	TS7700	An unreadable sector exists in the cache.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0574	Critical	S	TS7700	A parity error occurred in the cache.
OP0575	Critical	S	TS7700	A cache media error occurred.
OP0576	Impact	S	TS7700	A temporary cache problem was encountered.
OP0577	Critical	S	TS7700	The cache has an unreadable sector.
OP0578	Critical	S	TS7700	A cache power supply has failed.
OP0579	Critical	S	TS7700	A cache power or fan assembly has failed.
OP0580	Critical	S	TS7700	The cache has lost redundancy.
OP0581	Critical	S	TS7700	A problem exists with the cabling or drive path inside the cache enclosure.
OP0582	Critical	S	TS7700	A cache component has failed or been removed.
OP0583	Critical	S	TS7700	A cache controller has failed or been removed.
OP0584	Critical	S	TS7700	An environmental service module (ESM) canister in the cache has failed or been removed.
OP0585	Critical	S	TS7700	A cache drive is missing.
OP0586	Critical	S	TS7700	A cache drive is in a degraded state.
OP0587	Critical	S	TS7700	A cache disk has reported errors.
OP0588	Critical	S	TS7700	A cache RAID array has failed drives.
OP0589	Critical	S	TS7700	An unsupported number of drive enclosures exists on a cache loop.
OP0590	Critical	S	TS7700	The reported data rate of a cache drive channel is outside the expected range.
OP0591	Critical	S	TS7700	The data rate could not be obtained on a drive channel for the cache.
OP0592	Critical	S	TS7700	An incorrect number of enclosures exists on a cache loop.
OP0593	Critical	S	TS7700	The number of enclosures on a cache loop cannot be determined.
OP0594	Critical	S	TS7700	Mismatched drives exist in a cache array.
OP0595	Critical	S	TS7700	Disk operation in the cache is degraded.
OP0596	Critical	S	TS7700	Network errors were detected while connecting to the cache.
OP0597	Critical	S	TS7700	An unreadable sector exists in the cache.
OP0598	Critical	S	TS7700	A parity error occurred in the cache.
OP0599	Critical	S	TS7700	A cache media error occurred.
OP0600	Warning,Serious/Error See note 2	S	Control Unit	A temporary cache problem was encountered.
OP0601	Critical	S	TS7700	The cache has an unreadable sector.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0602	Critical	S	TS7700	A cache power supply has failed.
OP0603	Critical	S	TS7700	A cache power or fan assembly has failed.
OP0604	Critical	S	TS7700	The cache has lost redundancy.
OP0605	Critical	S	TS7700	A problem exists with the cabling or drive path inside the cache enclosure.
OP0606	Critical	S	TS7700	A cache component has failed or been removed.
OP0607	Critical	S	TS7700	A cache controller has failed or been removed.
OP0608	Critical	S	TS7700	An environmental service module (ESM) canister in the cache has failed or been removed.
OP0609	Critical	S	TS7700	A cache drive is missing.
OP0610	Critical	S	TS7700	A cache drive is in a degraded state.
OP0611	Critical	S	TS7700	A cache disk has reported errors.
OP0612	Critical	S	TS7700	A cache RAID array has failed drives.
OP0613	Critical	S	TS7700	An unsupported number of drive enclosures exists on a cache loop.
OP0614	Critical	S	TS7700	The reported data rate of a cache drive channel is outside the expected range.
OP0615	Critical	S	TS7700	The data rate could not be obtained on a drive channel for the cache.
OP0616	Critical	S	TS7700	An incorrect number of enclosures exists on a cache loop.
OP0617	Critical	S	TS7700	The number of enclosures on a cache loop cannot be determined.
OP0618	Critical	S	TS7700	Mismatched drives exist in a cache array.
OP0619	Critical	S	TS7700	Disk operation in the cache is degraded.
OP0620	Critical	S	TS7700	Network errors were detected while connecting to the cache.
OP0621	Critical	S	TS7700	An unreadable sector exists in the cache.
OP0622	Critical	S	TS7700	A parity error occurred in the cache.
OP0623	Critical	S	TS7700	A cache media error occurred.
OP0624	Critical	S	TS7700	An error was detected in the disk cache.
OP0625	Critical	S	TS7700	A system reboot interrupted a call home.
OP0626	Impact	S	TS7700	One or more issues on the system have persisted for longer than 24 hours.
OP0627	Critical	S	TS7700	There is a problem with network communication required for autonomic ownership takeover.
OP0628	Critical	S	TS7700	The cache controller is not configured.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0629	Critical	S	TS7700	The cache file system is inefficiently allocating its available space.
OP0630	Critical	S	TS7700	There is a problem with the network fail over code.
OP0631	Critical	S	TS7700	The error detection feature has restarted five times in 24 hours.
OP0632	Critical	S	TS7700	The available memory is not configured correctly.
OP0633	Critical	S	TS7700	A CPU has failed.
OP0634	Critical	S	TS7700	Port 0 on the customer network has failed.
OP0635	Critical	S	TS7700	Port 1 on the customer network has failed.
OP0636	Critical	S	TS7700	Both Ethernet routers have failed.
OP0637	Critical	S	TS7700	The primary Ethernet router has failed.
OP0638	Critical	S	TS7700	The alternate Ethernet router has failed.
OP0639	Critical	S	TS7700	The Network Time Protocol (NTP) server is not responding.
OP0640	Critical	S	TS7700	A port in an Ethernet router has failed.
OP0641	Critical	S	TS7700	A port in an Ethernet router shows increasing errors.
OP0642	Critical	S	TS7700	Communication between the disk cache and the primary switch has failed.
OP0643	Critical	S	TS7700	Communication between the disk cache and the alternate switch has failed.
OP0644	Critical		TS7700	One or more arrays are not encrypted.
OP0645	Impact		TS7700	This is a cache Call Home test.
OP0646	Warning	C	TS7700	Encryption is enabled on the virtual tape library. Device xxxxxxxx is not encryption-capable. The device was made unavailable.
OP0647	Critical	C, S	TS7700	Host Adapter adapter is not available and offline.
OP0648	Information	C, S	TS7700	The host adapter 'xx' has link 'yy' unavailable.
OP0649	Critical	S	TS7700	No IBM media changer devices were found on the system.
OP0650	Warning	S	TS7700	The system identified 'xxxx' IBM media changer devices. This is an incorrect number of devices.
OP0651	Impact	S	TS7700	The IBM media changer 'xxxx' is in an unknown state.
OP0652	Impact	S	TS7700	The fibre channel adapter for tape interface 'xx' cannot be identified.
OP0653	Impact	S	TS7700	The drive name 'xx' does not match port 'yy' .
OP0654	Critical	S	TS7700	Drives could not be configured on a 3590 or 3592 tape drive.
OP0655	Warning	S	TS7700	The physical tape SCSI device 'xxxx' is in the state: 'yyyy' .

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0656	Critical	S	TS7700	Primary and alternate paths for tape SCSI device 'xxxx' are unavailable.
OP0657	Warning	S	TS7700	The tape drive device 'xxxx' is shown as 'yyyy' in the cluster.
OP0658	Impact	S	TS7700	The tape drive device 'xxxx' is in the state 'yyyy' .
OP0659	Warning	S	TS7700	The path 'xx' for tape drive 'yyyy' is unavailable.
OP0660	Critical	S	TS7700	Both primary and alternate paths for tape drive device 'xxxx' are unavailable.
OP0661	Impact	S	TS7700	Tape device 'xxxx' is in an unknown state.
OP0662	Impact	S	TS7700	The path 'xx' to tape device 'yyyy' is disabled.
OP0663	Critical	S	TS7700	No tape drives were found in the system.
OP0664	Warning	S	TS7700	All paths on the 'xx' lower channel protocol interface failed.
OP0665	Critical		TS7700	All paths on the primary and alternate lower fibre channel protocol interface failed.
OP0666	Critical	S	TS7700	The primary and alternate paths for 'xxxx' on the lower fibre channel protocol interface failed.
OP0667	Warning	S	TS7700	The tape SCSI device path 'xxxx' on lower fibre channel protocol interface failed.
OP0668	Warning	S	TS7700	For library 'xx', the state of drive 'yyyy' could not be obtained.
OP0669	Impact	C, S	TS7700	The tape drive 'xxxx' is not available to the physical library 'yy' .
OP0670	Impact	S	TS7700	This system contains both E05 drives in native mode and J1A drives.
OP0671	Impact	S	TS7700	All drives are reported as in the busy state.
OP0672	Impact	S	TS7700	The world wide node name (WWNN) could not be obtained for drive 'xxxx' .
OP0673	Impact	C, S	TS7700	The physical volume status could not be obtained.
OP0674	Impact	C, S	TS7700	No physical volumes are found on the system.
OP0675	Impact	C, S	TS7700	The physical volume pool status could not be obtained.
OP0676	Warning	C	TS7700	Physical volume pool 'xx' is out of scratch volumes.
OP0677	Impact	C, S	TS7700	Volume 'xxxxxx' reports a state 'yyyyyy' with access in 'zz' status.
OP0678	Impact	C, S	TS7700	LDAP server connection ('xxxx') experienced a loss of connectivity.
OP0679	Critical	C, S	TS7700	LDAP server connection ('xxxx') is not responding.
OP0680	Critical	C	TS7700	LDAP server service is down. IP: 'xxxx' Port: 'yy'

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0681	Warning	C, S	TS7700	LDAP server connection is not correctly configured. IP: 'xxxx' Port: 'yy'
OP0682	Impact	C, S	TS7700	Authentication server 'xxxx' connection ('yyyy') experienced a loss of connectivity.
OP0683	Critical	C, S	TS7700	Authentication server 'xxxx' service is down. IP: 'yyyy' Port: 'zz'
OP0684	Warning	C, S	TS7700	The connection to authentication server 'xxxx' is not correctly configured. IP: 'yyyy' Port: 'zz'
OP0687	Critical	S	TS7700	An unknown cache problem was encountered. Disk model: 'xxxx' .
OP0688	Critical	S	TS7700	The cache has an unreadable sector error. Disk model: 'xxxx' .
OP0689	Critical	S	TS7700	A cache power supply has failed. Disk model: 'xxxx' .
OP0690	Critical	S	TS7700	A loss of redundancy has occurred in cache. Disk model: 'xxxx' .
OP0691	Critical	S	TS7700	A problem exists with the cabling or drive path inside the cache enclosure. Disk model: 'xxxx' .
OP0692	Critical	S	TS7700	A DDM is missing. Disk model: 'xxxx' .
OP0693	Critical	S	TS7700	A cache controller has failed or been removed. Disk model: 'xxxx' .
OP0694	Critical	S	TS7700	An environmental service module (ESM) canister in the cache has failed or been removed. Disk model: 'xxxx' .
OP0695	Critical	S	TS7700	A cache component has failed or been removed. Disk model: 'xxxx' .
OP0696	Critical	S	TS7700	Failed drives exist in a cache RAID array. Disk model: 'xxxx' .
OP0697	Critical	S	TS7700	Mismatched drives exist in a cache array. Disk model: 'xxxx' .
OP0698	Critical	S	TS7700	Disk operation in the cache is degraded. Disk model: 'xxxx' .
OP0699	Critical	S	TS7700	Network errors were detected while connecting to the cache. Disk model: 'xxxx' .
OP0700	Critical	S	TS7700	An unsupported number of drive enclosures exists on a cache loop. Disk model: 'xxxx' .
OP0701	Critical	S	TS7700	The reported data rate of a cache drive channel is outside the expected range. Disk model: 'xxxx' .
OP0702	Critical	S	TS7700	The data rate could not be obtained on a drive channel for the cache. Disk model: 'xxxx' .
OP0703	Critical	S	TS7700	An incorrect number of enclosures exists on a cache loop. Disk model: 'xxxx' .

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0704	Critical	S	TS7700	The number of enclosures on a cache loop cannot be determined. Disk model: 'xxxx' .
OP0705	Critical	S	TS7700	An unreadable sector exists in the cache. Disk model: 'xxxx' .
OP0706	Critical	S	TS7700	A disk cache parity mismatch error occurred in the cache. Disk model: 'xxxx' .
OP0707	Critical	S	TS7700	A cache media error occurred. Disk model: 'xxxx' .
OP0708	Critical	S	TS7700	A cache power or fan assembly has failed. Disk model: 'xxxx' .
OP0709	Critical	S	TS7700	A cache drive is in a degraded state. Disk model: 'xxxx' .
OP0710	Critical	S	TS7700	A cache disk has reported errors. Disk model: 'xxxx' .
OP0711	Critical	S	TS7700	The cache battery in a degraded state. Disk model: 'xxxx' .
OP0712	Critical	S	TS7700	The cache controller in a degraded state. Disk model: 'xxxx' .
OP0713	Critical	S	TS7700	Information for this event cannot be displayed on this cluster.
OP0714	Warning	S	TS7700	A cache DDM has failed. String: 'xx' , enclosure: 'yy' , slot: 'zz' . The disk model is: 'nnnn'.
OP0715	Impact		TS7700	Connection to TSSC is broken.
OP0716	Impact		TS7700	High packet loss occurred on the connection from TS7700 to TSSC.
OP0717	Impact		TS7700	TSSC call home is in locked state.
OP0718	Impact		TS7700	TSSC not communicating with external network.
OP0719	Warning		TS7700	TSSC 'xx' port is down or in unknown state.
OP0720	Critical		TS7700	Both TSSC ports are down or in unknown state.
OP0721	Warning		TS7700	TSSC virtual interface 'xx' is not configured properly.
OP0722	Warning		TS7700	TSSC IP address: 'xxxx' is responding intermittently.
OP0723	Critical		TS7700	TSSC IP address: 'xxxx' is not responding.
OP0724	Critical	C, S	TS7700	The connection to 'xx' adapter link is not UP. Has not been UP for up to 'yy' minutes.
OP0725	Warning	C, S	TS7700	Adapter 'xx' link is experiencing a high level of CRC errors.
OP0726	Warning	C, S	TS7700	Adapter 'xx' link is experiencing a high level of collisions.
OP0727	Critical	C, S	TS7700	Ping test to address 'xx' failed. Has been in this condition for up to 'yy' minutes.
OP0728	Warning	C, S	TS7700	Ping test to address 'xx' has an excessive packet loss. Has been in this condition for up to 'yy' minutes.

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0729	Warning	C, S	TS7700	The connection to 'xx' adapter link is not UP. Has not been UP for up to 'yy' minutes.
OP0730	Warning	S	TS7700	Call Home is currently disabled.
OP0731	Warning	S	TS7700	The number of CRC errors is close to the threshold.
OP0732	Critical	S	TS7700	The number of CRC errors has exceeded the threshold.
OP0733	Warning	S	TS7700	EKM Server 'xx' : 'yy' is not connected.
OP0734	Warning	S	TS7700	Stand-alone system has GRID IP address configured.
OP0735	Warning	S	TS7700	Virtual interface for MI is not correctly configured.
OP0736	Warning	S	TS7700	Traffic on the external virtual interface is being redirected through an alternate path.
OP0737	Critical	S	TS7700	Internal configuration for ordering name resolution has the incorrect look-up order for hosts.
OP0738	Warning	C, S	TS7700	NTP Server has been unavailable for more than 30 minutes.
OP0739	Critical	C, S	TS7700	NTP Server has been unavailable for more than 'xx' minutes.
OP0740	Critical	S	TS7700	Invalid configuration found in Domain Name Protocol file.
OP0741	Critical	S	TS7700	Invalid configuration found in routing table.
OP0742	Warning	S	TS7700	'xx' path in the customer network is down.
OP0743	Critical	S	TS7700	Both ethernet paths to the external network are down.
OP0744	Warning	S	TS7700	Performance settings for storage related devices are not set correctly.
OP0745	Critical	S	TS7700	Problems found with mirrored disks ('xx' and 'yy')
OP0746	Critical	S	TS7700	Disk: 'xx' was found on state: 'yy' .
OP0747	Warning	S	TS7700	Configured memory size is: 'xx' MB, and the expected memory size is: 'yy' MB.
OP0748	Information	S	TS7700	A problem was detected with the media in the system.
OP0749	Critical	S	TS7700	Both switches must be configured with the same type (internal or external).
OP0750	Critical	C, S	TS7700	Fibre Channel communication error.
OP0751	Critical	C, S	TS7700	Fibre Channel hardware error.
OP0752	Warning	S	TS7700	Fan or Power Supply failure detected in the server.
OP0753	Warning	S	TS7700	PCI slot failure detected in the server.
OP0754	Warning	S	TS7700	SPCN failure detected in the system.

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0755	Warning	S	TS7700	A sysplanar failure was detected. The reported system reference code (SRC) is: 'xx' .
OP0756	Critical	S	TS7700	Adapter: 'xx' is in status: 'yy' .
OP0757	Critical	S	TS7700	Unable to communicate with the 'xx' I/O adapter card.
OP0758	Critical	S	TS7700	Unable to communicate with the 'xx' I/O drawer.
OP0759	Warning	S	TS7700	A problem was found on the volume group or file system: 'xx' , problem reported is: 'yy' .
OP0760	Warning	S	TS7700	File system: 'xx' , is using 'yy' % if its available space.
OP0761	Critical	S	TS7700	File system: 'xx' , is using 'yy' % of its available space.
OP0762	Information	S	TS7700	Media is having problems; the reported operation is: 'xx' .
OP0763	Impact	S	TS7700	System health checks were placed in skip mode. Call Home has been temporally disabled.
OP0764	Warning	S	TS7700	The tape drive device 'xxxx' with serial number: 'yyyy' is shown as 'zzzz' in the cluster.
OP0765	Critical	S	Cache	For disk model 'xxxx', the power supply/fan assembly 'yy' in the enclosure 'zz' has failed or has been removed.
OP0766	Critical	S	Cache	For disk model 'xxxx', the environmental service module (ESM) canister 'yy' in the expansion 'zz' has failed or has been removed, FRU: 'nnnn'.
OP0767	Warning	C, S	TS7700	The host adapter 'xx' has link 'yy' unavailable.
OP0768	Impact	C	Media	Physical volume 'xxxxxx' already exists. Duplicate physical volumes cannot be inserted.
OP0769	Warning	S	TS7700	Unable to retrieve primary and secondary cache IP values from VPD for cache string: 'xx' .
OP0770	Warning	S	TS7700	Cache controller for string: 'xx' , in slot: 'yy' is in the 'zz' state.
OP0771	Warning	S	TS7700	The status of the cache controller: 'xx' for string: 'yy' is unknown.
OP0772	Warning	S	TS7700	The status of the battery for controller: 'xx' , in string: 'yy' , is degraded.
OP0773	Warning	S	TS7700	Adapter 'xx' path to cache, for string: 'yy' is inactive.
OP0774	Warning	S	TS7700	Unable to detect a controller connected to adapter 'xx' , for string: 'yy' .
OP0775	Warning	S	TS7700	Unable to find the link to the cache controller for string: 'xx' .
OP0776	Warning	S	TS7700	Only one link to cache controller found for string: 'xx' .

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0777	Warning	S	TS7700	All of the spare disks in the string are missing.
OP0778	Warning	S	TS7700	Unable to retrieve information about spare disks.
OP0779	Warning	S	TS7700	Number of spare disks found is 'xx' when the expected number is 'yy' .
OP0780	Critical	S	TS7700	One or more processes for the Hnode are not running.
OP0781	Warning	S	TS7700	An error occurred when retrieving Grid information from VPD.
OP0782	Warning	C, S	Library	Physical Library reported: 'xx' status.
OP0783	Critical	C, S	Library	Unable to retrieve physical library state.
OP0784	Warning	S	Media	A tape drive mismatch has been detected. The tape drives on the Virtual Library are not the same as in Physical Library.
OP0785	Warning	S	TS7700	Expected 'xx' grid links for this configuration, but found only 'yy' links.
OP0786	Critical	S	Tape Drive	The TS7700 does not have enough sunset physical drives to read active data from sunset media.
OP0787	Warning	C	TS7700	AOTM is unable to communicate with the local TSSC.
OP0788	Warning	C	TS7700	AOTM is unable to communicate with the remote TSSC of node 'xx' .
OP0789	Warning	C	TS7700	AOTM is unable to communicate with the remote node 'xx' .
OP0790	Critical	S	TS7700	A memory leak has been detected.
OP0791	Warning	S	TS7700	Disk array 'xx' for string: 'yy' does not support encryption.
OP0792	Warning	S	TS7700	Disk array 'xx' for string: 'yy' is not encrypted.
OP0793	Warning	S	TS7700	Disk at enclosure 'xx' , slot 'yy' does not support encryption.
OP0794	Warning	S	TS7700	Imbalance in SMFS detected.
OP0795	Warning	C, S	TS7700	The grid link adapter is running at 'xx' Mbps, but the expected speed is 'yy' Mbps.
OP0796	Warning	S	TS7700	Unable to query the Grid network adapters.
OP0797	Warning	C, S	TS7700	HDM inter-cluster heartbeats are taking longer than expected.
OP0798	Warning	S	TS7700	The system is running on 'xx' CPUs, when the expected number of CPUs are 'yy' .
OP0799			TS7700	The system is running on 'xx' CPU cores, when the expected number of CPU cores are 'yy' .
OP0800	Warning	S	TS7700	The router firmware level is 'xx' , but the expected level is 'yy' .

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0801	Warning	S	TS7700	The router ROM level is 'xx' , but the expected level is 'yy' .
OP0802	Warning	C, S	TS7700	Both the Active and Standby Library Managers are offline.
OP0803	Warning	C, S	TS7700	The Active Library Manager is offline.
OP0804	Warning	S	TS7700	Invalid configuration found in ordering name resolution file.
OP0805	Warning	S	TS7700	Could not find 'xx' in the list of 'yy' Disks on this system.
OP0806	Critical	S	TS7700	At least one vital process for Vnode is not running.
OP0807	Warning	S	TS7700	Unable to retrieve the information about Logical Devices.
OP0808	Warning	S	TS7700	The number of logical devices is 'xx' , number of tape daemons is 'yy' .
OP0809	Warning	C	TS7700	AOTM is enabled, but the cluster detected errors.
OP0810	Impact	C	TS7700	A scratch sunset physical volume 'xxxxxx' was inserted into the library that the TS7700 cannot use.
OP0811	Warning	S	TS7700	The communication to the External Key Server for Cache is down.
OP0812	Critical	S	TS7700	At least one vital process for Vnode is not running.
OP0813	Warning	S	TS7700	The state for proxy ip 'xx' is in state ('yy') The state: 0 is Offline 1 is Unknown
OP0814	Warning	S	TS7700	Fibre Channel switch 'xx' FW level is downlevel: 'yy' .
OP0815	Warning	S	TS7700	All paths in the PRI switch are down.
OP0816	Warning	S	TS7700	All paths in the ALT switch are down.
OP0817	Critical	S	TS7700	Problems found with mirrored disk 'xx' .
OP0818	Critical	S	TS7700	Problems found with disks in rootvg volume group.
OP0819	Warning	S	TS7700	Disk pool 'xx' for string: 'yy' does not support encryption.
OP0820	Warning	S	TS7700	Disk pool 'xx' for string: 'yy' is not encrypted.
OP0821	Warning	S	TS7700	Mismatched drives exist in a cache disk pool. Disk model: 'xxxx'
OP0822	Critical	S	TS7700	Failed Disk pool 'xx' in string: 'yy' .
OP0823	Warning	S	Cache	String: 'xx' , disk array ID 'yy' with preservation capacity of 'zz' rebuild areas is now using 'nn'.
OP0824	Critical	S	TS7700	String: 'xx' , Failed drives exist in a cache disk pool. Disk model: 'yyyy'
OP0825	Critical	S	Library	Fibre Channel communication error to both switches.
OP0826	Critical	S	TS7700	I/O Drawer 'xx' is reporting error(s): 'yy' .

Table 85. Intervention message texts (continued)

Message ID	Impact	TT	Product Area	Intervention Message Text
OP0827	Critical	C, S	TS7700	Fiber switch hardware issues found in 'xx' path(S).
OP0828	Critical	C, S	TS7700	Communication error in the 'xx' path in between the TS7700 and the fiber switch.
OP0830	Warning	S	TS7700 CA	The Transparent Cloud Tiering daemon has died.
OP0831	Critical	C	TS7700 CA	The Transparent Cloud Tiering service is unreachable: 'xx'. cloud account ('yy'), container ('zz'), url ('nn')
OP0832	Critical	C	TS7700 CA	The URL associated with container is invalid: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0833	Critical	C	TS7700 CA	The URL associated with container is malformed: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0834	Critical	C	TS7700 CA	Route to Cloud Storage Provider is unreachable: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0835	Critical	C	TS7700 CA	Connect exception to Cloud Service Provider: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0836	Critical	C	TS7700 CA	Socket timeout for a cloud connection: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0837	Critical	C	TS7700 CA	Invalid cloud configuration: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0838	Critical	C	TS7700 CA	Invalid credentials for cloud provider: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0839	Critical	C	TS7700 CA	Transparent Cloud Tiering node network is down.
OP0840	Critical	C	TS7700 CA	SSL handshake exception for a cloud provider: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0841	Critical	C	TS7700 CA	SSL handshake bad certificate exception for a cloud provider: 'xx' . cloud account ('yy'), container ('zz'), url ('nn')
OP0842	Critical	C	TS7700 CA	SSL handshake socket closed exception for a cloud provider.
OP0843	Warning	C	TS7700 CA	The TS7700 cannot communicate with the Cloud provider
OP0844	Impact	C	TS7700 CA	Virtual volumes with Storage Class 'xx' is set to offload to cloud storage, but the storage group 'yy' does not have the cloud premigration rank set properly.
OP0845	Impact	C	TS7700 CA	Unable to write to Cloud Container 'xx'
OP0846	Critical	C	TS7700 CA	Mount of virtual volume 'xxxxxx' from the cloud pool 'yy' failed
OP0847	Warning	C	TS7700 CA	Cloud pre-migration for virtual volume 'xxxxxx' to cloud pool 'yy' timed out with 'zz' seconds, where CPMTOUT is 'nn' and size of the virtual volume is 'mm' GiB

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0848	Warning	C	TS7700 CA	Cloud recall for virtual volume 'xxxxxx' from cloud pool 'yy' timed out with 'zz' seconds, where CRCTOUT is 'nn' and size of the virtual volume is 'mm' GiB
OP0849	Warning	C	TS7700 CA	Deleting object 'xxxxxx' from container 'yy' of cloud pool 'zz' timed out with CDELTOU ('nn' seconds)
OP0850	Critical	C	TS7700 CA	SSL handshake invalid path certificate exception for a cloud provider
OP0851	Critical	C	TS7700 CA	SSL handshake failure exception for a cloud provider
OP0852	Critical	C	TS7700 CA	SSL handshake unknown exception for a cloud provider
OP0853	Critical	C	TS7700 CA	SSL peer unverified exception for a cloud provider
OP0854	Critical	C	TS7700 CA	SSL protocol exception for a cloud provider
OP0855	Critical	C	TS7700 CA	SSL exception for a cloud provider
OP0856	Critical	C	TS7700 CA	SSL no cert exception for a cloud provider
OP0857	Critical	C	TS7700 CA	SSL not trusted cert exception for a cloud provider
OP0858	Critical	C	TS7700 CA	SSL invalid algorithm exception for a cloud provider
OP0859	Critical	C	TS7700 CA	SSL invalid padding exception for a cloud provider
OP0860	Critical	C	TS7700 CA	SSL unrecognized message for a cloud provider
OP0861	Critical	C	TS7700 CA	Bad request for a cloud provider
OP0862	Critical	C	TS7700 CA	Precondition failed for a cloud provider.
OP0863	Critical	C	TS7700 CA	Container creation failed: container ('xx')
OP0864	Critical	C	TS7700 CA	Cloud Bucket limit exceeded: container ('xx')
OP0865	Critical	C	TS7700 CA	Container does not exist: container ('xx')
OP0866	Critical	C	TS7700 CA	Time skew with a cloud provider
OP0867	Critical	C	TS7700 TA	Cloud provider server error
OP0868	Critical	S	TS7700 TA	Internal directory not found for Transparent Cloud Tiering
OP0869	Critical	S	TS7700 TA	Resource address file not found for Transparent Cloud Tiering
OP0870	Critical	S	TS7700 TA	Database corrupted for Transparent Cloud Tiering
OP0871	Critical	C	TS7700 TA	LKM down for Transparent Cloud Tiering
OP0872	Critical	C	TS7700 TA	Access forbidden for a cloud account: cloud account ('xx')
OP0873	Critical	C	TS7700 TA	Access denied for a cloud account: ('xx')
OP0874	Critical	C	TS7700 TA	Filesystem corrupted for Transparent Cloud Tiering
OP0875	Critical	C	TS7700 TA	Directory error for Transparent Cloud Tiering

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0876	Critical	C	TS7700 TA	Key manager error for Transparent Cloud Tiering
OP0877	Critical	C	TS7700 TA	Container pair root directory not found for Transparent Cloud Tiering
OP0878	Critical	C	TS7700 TA	Container already exists: 'xx'. cloud account ('yy'), container ('zz'), url ('nn')
OP0879	Critical	C	TS7700 TA	RKM down for Transparent Cloud Tiering: 'xx'. cloud account ('yy'), container ('zz'), url ('nn')
OP0880	Critical	C	TS7700 TA	SSL handshake certificate exception for a cloud provider: 'xx'. cloud account ('yy'), container ('zz'), url ('nn')
OP0881	Critical	C	TS7700 TA	SSL key exception for a cloud provider: 'xx'. cloud account ('yy'), container ('zz'), url ('nn')
OP0882	Critical	C	TS7700 TA	Transparent Cloud Tiering container 'xx' inaccessible by url 'yy' for unexpected reason: 'zz', failure detail: 'nn'
OP0883	Warning	S	Cache	Logical drive(s) with no optimal status: 'xx'
OP0884	Warning	S	Cache	Cache volume with nonoptimal status. Volume ID: 'xxxxxx' was found in string 'yy' for cache type: 'zz'
OP0885	Warning	S	Cache	Cache Mdisk with nonoptimal status. Mdisk ID: 'xx' was found in string 'yy' for cache type: 'zz'
OP0886	Warning	S	Cache	Cache pool with nonoptimal status. Pool ID: 'xx' was found in string 'yy' for cache type: 'zz'
OP0887	Warning	S	Cache	Cache node canister with nonoptimal status. Node Canister ID: 'xx' was found in string 'yy' for cache type: 'zz'
OP0888	Warning	S	Cache	Cache battery with nonoptimal status. Battery ID: 'xx' was found in string 'yy' for cache type: 'zz'
OP0889	Warning	S	Cache	Cache enclosure with nonoptimal status. Enclosure ID: 'xx' was found in string 'yy' for cache type: 'zz'
OP0890	Warning	C, S	Cache	USB with nonoptimal status was found at cache controller node: 'xx' in string 'yy' for cache type: 'zz'
OP0891	Impact	c	TS7700	The lwiks certificate for Cluster 'xx' will expire within 'yy' days
OP0892	Critical	c	TS7700	The lwiks certificate for Cluster 'xx' has expired
OP0893	Critical	C	TS7700	Secure Data Transfer failed. The lwiks certificate for Cluster 'xx' has expired. Fingerprint: 'yy'
OP0894	Critical	C	TS7700	Secure Data Transfer failed. An internal error has occurred (Server Cluster Id: 'xx')
OP0895	Critical	C	TS7700	Secure external encryption failed. The encryption key server offered a certificate that cannot be verified. Subject: 'xx'

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0896	Critical	C, S	TS7700	Secure external encryption failed. An internal error has occurred. Key Server IP: 'xxxx' . Port: 'yy'
OP0897	Critical	S	Cache	For disk model: 'xxxx', the power supply/fan assembly 'yy' in enclosure 'zz' and string 'nn' has failed or has been removed
OP0898	Warning	c	TS7700	The lwiks certificate for Cluster 'xx' will expire within 'yy' days please replace the certificate
OP0899	Critical	S	Cache	Another disk failure can cause data loss. String: 'xx' , disk array ID 'yy' with preservation capacity of 'zz' rebuild areas, is now using 'nn' rebuild areas and has a total of 'mm' failed disks
OP0900	Warning	C, S	Library	Physical library is in degraded state
OP0901	Warning	C, S	Cache	The TS7700 cache string 'xx' type 'yy' lost communication with the primary Encryption Key Server
OP0902	Warning	C, S	Cache	The TS7700 cache string 'xx' type 'yy' lost communication with the alternate Encryption Key Server
OP0903	Impact	C	Library	Stacked volume 'xx' ejected from the library 'yy'
OP0904	Warning	S	Cache	Cache expansion canister with nonoptimal status: 'xx' was found in enclosure 'yy' at string 'zz' for cache type: 'nn'
OP0905	Warning	C	Cache	Partition ('xx') entered overcommit state because the partition usage exceeded allocated partition size
OP0906	Information		Cache	Partition ('xx') exited overcommit state because the partition usage became under the allocated partition size
OP0907	Information		Cache	Cache file list initialization process completed.
OP0908	Warning	C, S	Cache	Problems detected retrieving External Encryption Key Servers health information from string 'x', please verify network connection from server to switches and the string.
OP0909	Warning	C	CA	The amount of data stored in the cloud pool 'xx' crossed the high warning level ('y') TB.
OP0910	Warning	C	CA	The amount of data stored in the cloud pool 'xx' crossed the low warning level ('yy' TB).
OP0911	Information		CA	The amount of data stored in the cloud pool 'xx' is below high warning level ('yy' TB).
OP0912	Information		CA	The amount of data stored in the cloud pool 'xx' is below low warning level ('yy' TB).
OP0914	Warning	C, S	TS7700	The TS7700 lost communication with the Encryption Key Server (IP 'x.x.x.x', Port 'yy').

Table 85. Intervention message texts (continued)				
Message ID	Impact	TT	Product Area	Intervention Message Text
OP0915	Warning	S	TS7700	File system 'xx' is using 'yy' % of its available inode capacity, its mounting point is at 'zz'.
OP0916	Critical	S	TS7700	File system 'xx' is using 'yy'% of its available inode capacity, its mounting point is at 'zz'.
OP0917	Information	C	TS7700	Dual control request has been discarded from the system. Request description: 'xx'
OP0918	Warning	C	CA	Cloud pool ('xx') needs a cloud account, URL, and cluster association to pre-migrate the volume ('yyyy') to the cloud.
OP0919	Information	C	CA	Cloud export completed OK. However, the cloud export status report had been truncated using logical volume 'xxxx' due to the volume size being too small.
PP0010	Informational		TS7700	Due to an imbalance of defined SMS constructs across the Domain, the constructs were automatically created with the default actions on the following distributed Cluster(s): xx.
PP0011	Informational		TS7700	Due to an imbalance of defined SMS constructs across the Domain, the default constructs were assigned on the following distributed Cluster(s): xx.
R0000	Information	c	TS7700	Reclaim successful for exported stacked volume 'xx' - You can return it to the specified library 'yy'
VT0103	Informational		TS7700	Warning: Primary Cluster volume xxxxxx copied from Secondary.

Notes:

1. Two impact levels are listed. The first has to do with the physical library the condition occurred in. The second impact is if there is a TS7700 that the host is connected to.
2. Two impact levels are listed. The first one is if communication is lost to just one of the two encryption key servers. The second is if communication is lost to both encryption key servers.

Related information

[“Error Recovery Action codes” on page 289](#)

[“Reference” on page 289](#)

Other host messages

In addition to CBR37501 and IEA480E, there are other host messages that can be used when monitoring the TS7700 storage system.

The following table lists other host messages:

TT – Trigger Type – This column provides guidelines on which interventions or events would be monitored by using host automation. The column indicates whether the event is a setting of a condition (“C” or “S”) or a clearing of a condition (“c” or “r”). The column also indicates whether the intervention or event is a customer (“C” and “c”) responsibility or an IBM (“S” and “r”) responsibility.

- C – Customer responsibility – Condition is set
- c – Customer responsibility – Condition is cleared
- S – IBM responsibility – Condition is set – Notify IBM

- r – IBM Responsibility – Condition is reset – Notify IBM
- * – S if initiated based on error, no action when initiated manually
- Blank – requires no trigger

Table 86. Other host messages		
Message ID	TT	Message text
CBR3002E	S	Library not operational
CBR3730E		Synchronous mode copies deferred state (CBR3731I when state is left)
CBR3736E		Cloud object store degraded (CBR3737I when state is left)
CBR3750I		A general message that documents errors that are reported from library to host (refer to TS7700 white paper)
CBR3751I	S	Device unavailable
CBR3752I	r	Device now available (can be varied online)
CBR3758E	S	Degraded message
CBR3760E	S	Vision system not operational (TS7740)
CBR3761E	S	Library manager offline
CBR3762E	S	Intervention required
CBR3763E	S	Library check 1
CBR3764E	C	All storage cells full (TS7740)
CBR3765E	C	No cleaner volumes (TS7740)
CBR3766E	S	Dual write disabled (TS7740)
CBR3770I	C	Volume misplaced
CBR3776I	C	Volume inaccessible
CBR3781I	C	No MEDIAx scratch volumes available
CBR3783E	*	Library manager switchover in progress
CBR3784I	r	Library manager switchover is complete (you might need to restart jobs or CBR4196D retries)
CBR3785E		Copy operations that are disabled
CBR3786E		VTs operations degraded (CBR3768I when state is left)
CBR3787E		Immediate mode copies deferred (CBR3791I when state is left)
CBR3788E		Service preparation that is occurring
CBR3789E		Out of VTS stacked volumes (TS7740)
CBR3790E		VTS library has insufficient resources to continue mount processing (TS7740)
CBR3792E		Limited cache free space warning state (TS7720) (CBR3793I when state is left)
CBR3794E		Out of cache resource critical state (TS7720) (CBR3795I when state is left)
CBR3796E	C	Grid links degraded (CBR3797I when state is left)
CBR3798E	S	A forced pause in the library
CBR3799E		Copy operations that are disabled by LIBRARY REQUEST command

<i>Table 86. Other host messages (continued)</i>		
Message ID	TT	Message text
CBR3660A	C	Scratch threshold message - below threshold notification
CBR3615E		Problem with the cartridge entry exit CBRUXENT (entry processing disabled)
CBR3655E		Problem with the cartridge eject exit CBRUXEJC (eject processing disabled)
CBR4225E		Problem with change use attribute exit CBRUXCUA (private -> scratch processing disabled)
CBR4196D		Mount retry message (many different error codes are associated with this message)
CBR4197D		Automated mount retry (see CBROAMxx SETTLIB keywords)
CBR3006I		Library unknown in I/O configuration (the message is valid irrespective of the state of the library)
CBR3710I		Failure communicating with the library (LIBSERV failure)
CBR3715I		No paths available for I/O
IOS000I		Messages are always helpful as well as any other IOSxxxx messages
IEA439I		A four-minute timeout message is created by device services when the library doesn't respond

Service information messages

Service information messages (SIM) and FICON media information messages (MIM) provide information about abnormal conditions in the subsystem or media.

The SIMs and MIMs are a primary function in the TS7700 Server plan for improved product availability:

- A SIM alerts the customer of an abnormal condition in the subsystem. Information in the SIM identifies the affected drive, the controller (or control unit [CU]), the failing component, the severity of the fault condition, and the expected impact of the pending service action.

A SIM contains the machine type, machine serial number, and field replaceable unit (FRU) Identifier (FID) information required for service personnel to repair the machine fault.

SIM sense bytes

The following table defines SIM Sense Bytes.

<i>Table 87. Service information message (SIM) Sense Bytes</i>		
0-7 Common Sense Bytes		
Byte	Meaning	
0	Flags 0	
1	Flags 1	

Table 87. Service information message (SIM) Sense Bytes (continued)		
2	Bit Description 0-1 Basic Recovery Action (BRAC) 1 Continue 2 Re-issue 2-4 Logging Code (LC) 3 A3 5 VLF Active 6 Synchronous Transfer Mode 7 Medium Positioning	
3	Error Recovery Action (ERA) 48 Unsolicited Informational Data	
4-5	Reason Code (RC) - Reason Qualifier Code (RQC) 11-01 I/O-Subsystem SIM 11-02 Device SIM	
6	Message Code (MC) F1 I/O-Subsystem SIM F2 Device SIM	
7	Sense Format 71 SIM Sense	
8-22 Format-dependent Sense Bytes		
Byte	I/O-Subsystem SIM Sense (Message Code=F1) Meaning	Device SIM Sense (Message Code=F2) Meaning

Table 87. Service information message (SIM) Sense Bytes (continued)

8-9	Message Modifier	Message Modifier
	Bit Description 0-3 Exception Message Code 0 Reserved 1 Effect of failure is unknown 2 CU Exception - No Performance Impact 3-F Reserved 4-7 Service Message Code 0 Reserved 1 Repair Impact is unknown 2 Repair will not impact CU performance 3-F Reserved 8-9 Report Severity 0 Service 1 Moderate 2 Serious 3 Acute 10 Repeated Report Presentation: set to '1'b if this SIM was previously reported. 11 Message To Operator (MTO): set to '1'b if this SIM should be reported to the operator console. 12-14 Reserved 15 Message Data Flag	Bit Description 0-3 Exception Message Code 0 Reserved 1 Effect of failure is unknown 2 DV Exception - No performance Impact 3 DV Exception on Interface xx 4 DV Exception on ACF 5 DV Exception on Operator Panel 6 DV Exception on Tape path 7 DV Exception in Drive 8 DV Preventive Maintenance Required 9-F Reserved Where italicized fields are determined as follows: xx Format 71, byte 10 4-7 Service Message Code 0 Reserved 1 Repair Impact is unknown 2-6 Reserved 7 Repair will disable access to DV 8 Repair will disable message display <i>ids</i> on DV 9 DV Cleaning Required A DV Cleaning Complete B-F Reserved 8-9 Report Severity 0

Table 87. Service information message (SIM) Sense Bytes (continued)

10-12	Message Data Reserved, set to X'000000'	Byte Meaning 10 Exception Data xx 11 SIM Message Code Value (ASCII) Description '00' No Message '41' Device Degraded - Call for Service '42' Device Hardware Failure - Call for Service '43' Service Circuits Failed, Operations Not Affected - Call for Service '55' Drive Needs Cleaning: Load Cleaning Cartridge '57' Drive Cleaning Complete: Cleaning Cartridge Ejected 12 Reserved - set to X'00'
13	SIM Identifier This field contains the same value when a SIM is presented more than once and can be used in interactions with the product during maintenance activities.	SIM Identifier This field contains the same value when a SIM is presented more than once and can be used in interactions with the product during maintenance activities.
14-15	Unit Modifier Microcode EC level	Unit Modifier Expert Systems Data from Log Page 31, bytes 16-19 (ASCII->HEX)

Table 87. Service information message (SIM) Sense Bytes (continued)		
16-17	REF Code 1 Bit Description 0-2 SIM Type B'000' Hardware, non-encoded SRN (HDWE) B'001' Hardware, encoded POST error (EPOST) (future) B'111' Microcode Detected Error (MDE) 3-15 Reserved (used for encoded POST errors in future)	REF Code 1 Bit Description 0-2 SIM Type B'011' Device SIM 3-7 Reserved 8-15 FRU Identifier (FID)
18-19	REF Code 2 HDWE SIM Type Bits 0-7 are set to X'00' Bits 8-15 are set to the first 2 digits of the SRN MDE SIM Type Bits 0-15 are set to the CU MDE code	REF Code 2 For Device SIMs, this value will be set to the 1st FSC code reported from the device.
20-21	REF Code 3 HDWE SIM Type Bits 0-15 are set to the last 4 digits of the SRN MDE SIM Type Bits 0-15 contain CU MDE supporting data	REF Code 3 For Device SIMs, this value will be set to the last FSC code reported from the device.
22	Reserved	Reserved
23-31 Common Sense Bytes		
Byte	Meaning	
23	Flags 3	
24	Flags 4	
25-26	Product Identifier (MM-PP)	
27-29	Product Serial (SSSSS)	
30	CU/Library Type-Model	
31	Device Type-Model	

FICON MIM formats

The following figure displays FICON MIM format.

1

2

TAPE SERVICE INFORMATION MESSAGES

REPORT DATE 263 96

3

PERIOD FROM 363 98

4

5

3

7

8

DEVICE-0860 S/N 01113-07780 DATE-007/99 TIME-12:23:58:70 ID=1F

9 10 11 12 13 14

*ACUTE ALERT D/T UNKNOWN REF-60B0 REF-305D REF3-305D

UM-2268

* SERVICE ALERT D/T-3494-B11 REF1-60FF REF2-C559 REF3-C559 UM-1229

15

* DV EXCEPTION IN DRIVE

16

* REPAIR WILL DISABLE ACCESS TO DV

DEVICE-0815 S/N 0113-23456 DATE-007/99 TIME-01:44:53:87 ID=97

* ACUTE ALERT D/T-3590-A00 REF1-E000 REF2-30B7 REF3-0000 UM-0913

* EFFECT OF FAILURE IS UNKNOWN

* REPAIR IMPACT IS UNKNOWN

DEVICE-08A2 S/N 0113-00011 DATE-006/99 TIME-11:25:38:00 ID=6C

* SERVICE ALERT D/T-3590-A00 REF1-E000 REF2-8083 REF3-0000 UM-0000

* Controller (Control unit [CU]) EXCEPTION - NO PERFORMANCE IMPACT

* REPAIR WILL NOT IMPACT CU PERFORMANCE

DEVICE-08A3 S/N 0113-0001A DATE-007/99 TIME-11:29:56:01 ID=1B

* SERVICE ALERT D/T-3590-B11 REF1-60FF REF2-C559 REF3-C559 UM-160F

* DV PREVENTIVE MAINTENANCE COMPLETED

* DV CLEANING COMPLETE

DEVICE-086F S/N 0113-23A56 DATE-007/99 TIME-03:44:53:87 ID=23

* SERIOUS ALERT D/T-3590-A00 REF1-0000 REF2-0089 REF3-0109 UM-0913

* EFFECT OF FAILURE IS UNKNOWN

*REPAIR IMPACT IS UNKNOWN

DEVICE-087F S/N 0113-23C56 DATE-007/99 TIME-04:44:53:87 ID=21

* ACUTE ALERT D/T-3590-B11 REF1-60E5 REF2-9999 REF3-DECC UM-160F

* DV EXCEPTION IN DRIVE

* REPAIR WILL DISABLE ACCESS TO DV

Figure 52. Description of Service Information Message Format

The following table describes the FICON MIM format.

Table 88. Description of fibre connection (FICON) media information message format	
Reverse Keys	Field Explanation
1	Type of EREP report - service information messages (SIMs)
2	Julian date the report ran
3	Julian date of the earliest record
4	The 4 hex digits of the controller address
5	Plant of manufacture and the machine sequence number
6	Date of failure

Table 88. Description of fibre connection (FICON) media information message format (continued)

Reverse Keys	Field Explanation
7	Time of failure
8	SIM identifier. Contains the same value when presented more than once
9	Severity: Moderate, Serious, Acute or Service
10	Machine type and model number
11	Reference code from bytes 16 and 17 in format 71 sense
12	Reference code from bytes 18 and 19 in format 71 sense
13	Reference code three from bytes 20 and 21 in format 71 sense
14	Unit modifier for Expert System Data
15	Informational message
16	Informational message

Other MIM formats

The following figure is a sample MIM EREP report.

```

1          2
TAPE MEDIA INFORMATION MESSAGES          REPORT DATE 008 99
                                           3
                                           PERIOD FROM 363 98
                                           TO    008 99

*****
4          5          6          7
VOLUME-0883          DEVICE-0333          DATE-006/99
TIME-07:45:44:04
8
9
    * D/T-3590-B1A          S/N 1804-MXGKM
    10          11          12          13
    * MODERATE ALERT          REFCODE-6157          MEDIA IDENTIFIER-0130          IDENTIFIER-23
    14
    * DATA DEGRADED
    14
    * REFERENCE MEDIA MAINTENANCE PROCEDURE 57

VOLUME-JANZ01 DEVICE-0338 DATE-006/99 TIME-07:40:45:04
    * D/T-3590-B1A          S/N 160G-*****
    * MODERATE ALERT REFCODE-6103 MEDIA IDENTIFIER-0002 IDENTIFIER-01
    * MEDIUM EXCEPTION
    * REFERENCE MEDIA MAINTENANCE PROCEDURE 03

VOLUME-JAAZ01 DEVICE-1741 DATE-007/99 TIME-07:40:45:04 **REPEATED**
    * D/T-3590-B1A          S/N 16G4-*****
    * MODERATE ALERT REFCODE-6157 MEDIA IDENTIFIER-0130 IDENTIFIER-23
    * DATA DEGRADED
    * REFERENCE MEDIA MAINTENANCE PROCEDURE 57

VOLUME-JANZ04 DEVICE-0336 DATE-008/99 TIME-07:45:44:04
    * D/T-3590-B1A          S/N 160G-*****
    * MODERATE ALERT REFCODE-6155 MEDIA IDENTIFIER-0130 IDENTIFIER-23
    * BLOCK 0 ERROR
    * REFERENCE MEDIA MAINTENANCE PROCEDURE 55

VOLUME-JANZ04 DEVICE-0337 DATE-007/99 TIME-07:39:44:0
    * D/T-3590-B1A          S/N 16G4-*****
    * MODERATE ALERT REFCODE-6157 MEDIA IDENTIFIER-0130 IDENTIFIER-23
    * DATA DEGRADED
    * REFERENCE MEDIA MAINTENANCE PROCEDURE 57

*****

```

The following table describes the MIM format.

Table 89. Description of Media Information Message Format	
Reverse Keys	Field explanation
1	Type of report - Media Information Messages (MIM)
2	Julian date the report ran
3	Julian date of the earliest record and latest record
4	The VOLID from bytes 16 - 21 in format 70 sense
5	The drive the tape was on when the failure occurred
6	Julian date of the MIM sent to the host
7	Time the failure occurred
8	Device type
9	Machine sequence number
10	Severity: high number of temporary R/W errors , serious permanent R/W errors , acute block 0 , cartridge type , or volume label errors were detected (R/W errors)
11	Reference code taken from bytes 10 and 11 of format 70 sense
12	Media identifier taken from bytes 12 and 13 of format 70 sense
13	Format identifier taken from byte 22 of format 70 sense
14	Informational message for problem correction

Related information

[“Error Recovery Action codes” on page 289](#)

[“Operator information messages” on page 322](#)

[“Reference” on page 289](#)

Read Diagnostic Parameter (RDP)

TS7700 with 16Gb FICONs supports Read Diagnostic Parameters (RDP). RDP is useful in diagnosing performance problems and/or interface issues.

The command is issued in MVS, option s;log. The MVS command syntax is:

D M=DEV(devno, (chp)), LINKINFO={FIRST | LAST | REFRESH | COMPARE}

The LINKINFO parameter may only be specified when a path is specified on the D M=DEV command.

The example shows a switched configuration with 16Gb end to end ports. The Buffer Credit and Forward Error Correction (FEC) uncorrected error counters are not available at this time.

- FIRST - displays the link diagnostic information that was obtained during IPL or when the physical path was brought online for the first time after IPL.

The command is issued in MVS, option s;log.

```
IEE584I 13.37.13 DISPLAY M          FRAME LAST  F    E    SYS=SSA
DEVICE 0D800 STATUS=ONLINE
Link Information: First
Description      Channel      Entry Port  Exit Port  Cntl Unit
Identifier       01F0        2E         29        0032
Date Retrieved   04/06/2016   04/06/2016 04/06/2016 04/06/2016
Time Retrieved   08:52:29     08:52:29   08:52:29   08:52:29
Tx Power (dBm)   0.66         -0.73       0.39        0.29
Rx Power (dBm)   -0.35        -0.32       0.09       -9.05
Tx Bias (mA)     39.1         51.1        40.2        40.8
Temperature (C)  33.3         54          55          41.6
Voltage (V)      3.26         3.36        3.31        3.32
Capable Speed    16G          16G         16G         16G
Operating Speed  16G          16G         16G         16G
Buffer Credits   90           Not Avail   Not Avail   90
Link Failures    8            24          39          0
Loss of Sync     11           0           0           16
Loss of Signal   11           28          16          14
Primitive Seq Err 0            0           0           0
Invalid Trans Word 876         1005        10021285    172
Invalid CRC      9           464         0           409
FEC Uncorrected  242         Not Avail   Not Avail   363
```

Figure 53. FIRST

- LAST - Displays the link diagnostic information that was last retrieved by the system. The system retrieves new information for a physical path every 24 hours or when LINKINFO=REFRESH is specified.

```
IEE584I 14.02.01 DISPLAY M          FRAME LAST  F    E    SYS=SSA
DEVICE 0D800 STATUS=ONLINE
Link Information: Last
Description      Channel      Entry Port  Exit Port  Cntl Unit
Identifier       01F0        2E         29        0032
Date Retrieved   04/08/2016   04/08/2016 04/08/2016 04/08/2016
Time Retrieved   14:02:01     14:02:01   14:02:01   14:02:01
Tx Power (dBm)   0.66         -0.78       0.37        0.32
Rx Power (dBm)   -0.57        -0.24       0.06       -9.19
Tx Bias (mA)     39.6         51.1        40.2        40.8
Temperature (C)  34.7         55          55          42
Voltage (V)      3.26         3.36        3.31        3.32
Capable Speed    16G          16G         16G         16G
Operating Speed  16G          16G         16G         16G
Buffer Credits   90           Not Avail   Not Avail   90
Link Failures    8            24          39          0
Loss of Sync     11           0           0           16
Loss of Signal   11           28          16          14
Primitive Seq Err 0            0           0           0
Invalid Trans Word 876         1005        10021285    172
Invalid CRC      9           464         0           409
FEC Uncorrected  242         Not Avail   Not Avail   0
```

Figure 54. LAST

- REFRESH - Requests that the system obtain new link diagnostic information for the physical path and then displays that information. This causes the prior information to be replaced and a subsequent LINKINFO=LAST request will also show this new information.

Note:

1. A REFRESH request does not cause the entry switch port, exit switch port and control unit port to retrieve new optical transceiver information. It simply causes the last retrieved values to be returned to the channel subsystem. The frequency that a port retrieves its own optical transceiver information is manufacturer and model specific.
2. A REFRESH request will be rejected if the channel specified in the command is already processing the maximum number of concurrent requests. These requests could be from this system or other systems on the same processor. The maximum number of concurrent requests allowed for a channel is model dependent.

```

IEE584I 14.05.45 DISPLAY M          FRAME LAST  F      E      SYS=SSA
DEVICE 0D800 STATUS=ONLINE
Link Information: Last (Refresh)
Description      Channel      Entry Port      Exit Port      Cntl Unit
Identifier       01F0          2E              29             0032
Date Retrieved   04/08/2016     04/08/2016     04/08/2016     04/08/2016
Time Retrieved   14:05:45       14:05:45       14:05:45       14:05:45
Tx Power (dBm)   0.67           -0.79          0.35           0.27
Rx Power (dBm)   -0.57          -0.23          -0.08          -9.16
Tx Bias (mA)     39.5           51.1           40.2           40.8
Temperature (C)  34.2           55             56             42.8
Voltage (V)      3.26           3.36           3.31           3.32
Capable Speed    16G            16G            16G            16G
Operating Speed  16G            16G            16G            16G
Buffer Credits   90             Not Avail      Not Avail      90
Link Failures    8              24             39             0
Loss of Sync     11            0              0              16
Loss of Signal   11            28             16             14
Primitive Seq Err 0              0              0              0
Invalid Trans Word 876           1005           10021285       172
Invalid CRC      9             464            0              409
FEC Uncorrected  242           Not Avail      Not Avail       0

```

Figure 55. REFRESH

- COMPARE - Displays a comparison of the first and last set of link diagnostic information that was retrieved by the system.

```

IEE586I 14.11.55 DISPLAY M          FRAME 1      F      E      SYS=SSA
DEVICE 0D800 STATUS=ONLINE
Channel Information: CHPID=94, PCHID=01F0, WWPN=C05076FEFE801F01
Description          First      Last
Date Retrieved       04/06/2016 04/08/2016
Time Retrieved       08:52:29 14:05:45
Tx Power (dBm)       0.66    0.67
Rx Power (dBm)       -0.35   -0.57
Tx Bias (mA)         39.1    39.5
Temperature (C)      33.3    34.2
Voltage (V)          3.26    3.26
Capable Speed        16G     16G
Operating Speed      16G     16G
Buffer Credits       90      90
Link Failures        8       8
Loss of Sync         11      11
Loss of Signal        11      11
Primitive Seq Err     0       0
Invalid Trans Word    876    876
Invalid CRC           9       9
FEC Uncorrected      242    242

Switch Entry Port Information: Link=2E, WWPN=202E000533B3D100
Description          First      Last
Date Retrieved       04/06/2016 04/08/2016
Time Retrieved       08:52:29 14:05:45
Tx Power (dBm)       -0.73   -0.79
Rx Power (dBm)       -0.32   -0.23
Tx Bias (mA)         51.1    51.1
Temperature (C)      54      55
Voltage (V)          3.36    3.36
Capable Speed        16G     16G
Operating Speed      16G     16G
Buffer Credits       Not Avail Not Avail
Link Failures        24      24
Loss of Sync         0       0
Loss of Signal        28      28
Primitive Seq Err     0       0
Invalid Trans Word   1005    1005
Invalid CRC          464     464
FEC Uncorrected      Not Avail Not Avail

Switch Exit Port Information: Link=29, WWPN=2029000533B3D100
Description          First      Last
Date Retrieved       04/06/2016 04/08/2016
Time Retrieved       08:52:29 14:05:45
Tx Power (dBm)       0.39    0.35
Rx Power (dBm)       0.09    -0.08
Tx Bias (mA)         40.2    40.2
Temperature (C)      55      56
Voltage (V)          3.31    3.31
Capable Speed        16G     16G
Operating Speed      16G     16G
Buffer Credits       Not Avail Not Avail
Link Failures        39      39
Loss of Sync         0       0
Loss of Signal        16      16
Primitive Seq Err     0       0
Invalid Trans Word   10021285 10021285
Invalid CRC           0       0
FEC Uncorrected      Not Avail Not Avail

Control Unit Information: Intid=0032, WWPN=50050763070391C4
Description          First      Last
Date Retrieved       04/06/2016 04/08/2016
Time Retrieved       08:52:29 14:05:45
Tx Power (dBm)       0.29    0.27
Rx Power (dBm)      -9.05   -9.16
Tx Bias (mA)         40.8    40.8
Temperature (C)      41.6    42.8
Voltage (V)          3.32    3.32
Capable Speed        16G     16G
Operating Speed      16G     16G
Buffer Credits       90      90
Link Failures        0       0
Loss of Sync         16      16
Loss of Signal        14      14
Primitive Seq Err     0       0
Invalid Trans Word    172    172
Invalid CRC          409     409
FEC Uncorrected      363     0

```

Figure 56. COMPARE

Error counters are cumulative. The error counters are cumulative, so seeing a very large error counter may not indicate a problem. Observing how error counters change over time is what matters. During the attenuator test to degrade the optical signal between the channel and entry switch ports, interface control checks occurred because of the weak optical signal, which resulted in many IOS050I CHANNEL DETECTED ERROR messages. Notice how the error counters (Link Failures, Loss of Signal, Invalid Trans Word and Invalid CRC) changed as a result of the test.

Before


```

D M=DEV(D800,(99)),LINKINFO=REFRESH
IEE584I 10.50.41 DISPLAY M 524
DEVICE 0D800 STATUS=ONLINE
Link Information: Last (Refresh)

```

Description	Channel	Entry Port	Exit Port	Cntl Unit
Identifier	01CD	162E	16A0	0230
Date Retrieved	05/12/2016	05/12/2016	05/12/2016	05/12/2016
Time Retrieved	10:50:41	10:50:41	10:50:41	10:50:41
Tx Power (dBm)	0.89	0.15	0.33	0.67
Rx Power (dBm)	-1.36	-0.49	-0.87	-0.01
Tx Bias (mA)	33.9	49.2	41.6	39.5
Temperature (C)	32.2	51	41	43.3
Voltage (V)	3.26	3.32	3.32	3.31
Capable Speed	16G	16G	16G	16G
Operating Speed	16G	16G	16G	16G
Buffer Credits	90	Not Avail	Not Avail	90
Link Failures	5	38	0	5
Loss of Sync	0	0	0	4
Loss of Signal	0	52	0	4
Primitive Seq Err	0	0	0	0
Invalid Trans Word	88	2515	10157	27400
Invalid CRC	0	351	1	0
FEC Uncorrected	Not Avail	Not Avail	Not Avail	0

Figure 57. Before error

IOS050I CHANNEL DETECTED ERRORs occurring

```

IOS050I CHANNEL DETECTED ERROR ON D804,99,E7,**02,PCHID=01CD
IOS050I CHANNEL DETECTED ERROR ON D901,99,85,**02,PCHID=01CD
IOS1050I CHANNEL DETECTED ERROR ON 3D840,99,E7,**02,PCHID=01CD
IOS050I CHANNEL DETECTED ERROR ON D803,99,E7,**02,PCHID=01CD
IOS1050I CHANNEL DETECTED ERROR ON 3DB46,99,E7,**02,PCHID=01CD
IOS1050I CHANNEL DETECTED ERROR ON 3DB44,99,E7,**02,PCHID=01CD
IOS1050I CHANNEL DETECTED ERROR ON 3DA44,99,E7,**02,PCHID=01CD
IOS1050I CHANNEL DETECTED ERROR ON 3D846,99,E7,**02,PCHID=01CD
IOS1050I CHANNEL DETECTED ERROR ON 3D941,99,E7,**02,PCHID=01CD
IOS050I CHANNEL DETECTED ERROR ON C503,99,E3,**02,PCHID=01CD
IOS050I CHANNEL DETECTED ERROR ON C504,99,E3,**02,PCHID=01CD
IOS050I CHANNEL DETECTED ERROR ON C505,99,E3,**02,PCHID=01CD
IOS050I CHANNEL DETECTED ERROR ON C506,99,E3,**02,PCHID=01CD

```

Figure 58. Error occurrence

After

```

DEVICE 0D800 STATUS=ONLINE
Link Information: Last (Refresh)

```

Description	Channel	Entry Port	Exit Port	Cntl Unit
Identifier	01CD	162E	16A0	0230
Date Retrieved	05/12/2016	05/12/2016	05/12/2016	05/12/2016
Time Retrieved	13:17:35	13:17:35	13:17:35	13:17:35
Tx Power (dBm)	0.85	0.17	0.34	0.71
Rx Power (dBm)	-2.01	-0.56	-0.7	0.01
Tx Bias (mA)	33.5	49.2	41.6	39.4
Temperature (C)	31.7	51	41	42.5
Voltage (V)	3.26	3.32	3.32	3.31
Capable Speed	16G	16G	16G	16G
Operating Speed	16G	16G	16G	16G
Buffer Credits	90	Not Avail	Not Avail	90
Link Failures	8	40	0	5
Loss of Sync	0	0	0	4
Loss of Signal	0	54	0	4
Primitive Seq Err	0	0	0	0
Invalid Trans Word	168	10172	10157	27400
Invalid CRC	0	529	1	0
FEC Uncorrected	Not Avail	Not Avail	Not Avail	0

Figure 59. After error

TS7700 examples

Example #1: TS7700 host jobs failing due to link errors:

Figure 60. Comparison of stats from 12/16 to 12/26 to search for invalid CRC and FEC uncorrected value changes

```

D M=DEV(5000,(4D)),LINKINFO=REFRESH
IEE584I 09.50.51 DISPLAY M 266
DEVICE 05000 STATUS=ONLINE
Identifier      0228(4D)  8101
Date Retrieved  12/26/2017 12/26/2017
Time Retrieved  09:50:51  09:50:51
Tx Power (dBm)  0.84      0.78
Rx Power (dBm)  -0.63     -0.66
Tx Bias (mA)    39.2      43
Temperature (C) 23.6      43.1
Voltage (V)     3.31      3.31
Capable Speed   16G       16G
Operating Speed 16G       16G
Buffer Credits  90        90
Link Failures   13        0
Loss of Sync    0         0
Loss of Signal  0         0
Primitive Seq Err 0        0
Invalid Trans Word 0       0
Invalid CRC     0         20
FEC Uncorrected 0         91915

```

```

/D M=DEV(5000,(4D)),LINKINFO=REFRESH

```

```

IEE584I 10.24.30 DISPLAY M 881
DEVICE 05000 STATUS=ONLINE
Link Information: Last (Refresh)
Description      Channel  Cntl Unit
Identifier       0228(4D)  8101
Date Retrieved   12/16/2017 12/16/2017
Time Retrieved   10:24:30  10:24:30
Tx Power (dBm)   0.73      0.79
Rx Power (dBm)   -0.55     -0.69
Tx Bias (mA)     38.3      43.3
Temperature (C)  23.3      43.6
Voltage (V)      3.31      3.32
Capable Speed    16G       16G
Operating Speed  16G       16G
Buffer Credits   90        90
Link Failures    1         0
Loss of Sync     0         0
Loss of Signal   0         0
Invalid CRC      0         0
FEC Uncorrected  0         18942

```

Example #2: TS7700 host jobs failing due to link errors

For CHPID AB, It looks like there is a big power drop at the receiver of the CHPID. The CU Tx power says it's good, so maybe a problem with the SFP on the channel side (or the one link in that direction at the patch panel somewhere).

IEE584I 17.14.37 DISPLAY M 822			D M=DEV(4A00,(AB)),LINKINFO=REFRESH		
DEVICE 04A00 STATUS=ONLINE			IEE584I 07.18.56 DISPLAY M 835		
Link Information: Last (Refresh)			DEVICE 04A00 STATUS=ONLINE		
Description	Channel	Cntl Unit	Description	Channel	Cntl Unit
Identifier	02E0(AB)	8011	Identifier	02E0(AB)	8011
Date Retrieved	12/18/2017	12/18/2017	Date Retrieved	12/19/2017	12/19/2017
Time Retrieved	17:14:38	17:14:38	Time Retrieved	07:18:56	07:18:56
Tx Power (dBm)	0.67	0.82	Tx Power (dBm)	0.69	0.81
Rx Power (dBm)	-6.27	-0.62	Rx Power (dBm)	-6.26	-0.6
Tx Bias (mA)	41.8	43.6	Tx Bias (mA)	41.8	43.6
Temperature (C)	35.7	41.3	Temperature (C)	34.9	41.3
Voltage (V)	3.27	3.3	Voltage (V)	3.27	3.3
Capable Speed	16G	16G	Capable Speed	16G	16G
Operating Speed	16G	16G	Operating Speed	16G	16G
Buffer Credits	90	90	Buffer Credits	90	90
Link Failures	2	0	Link Failures	2	0
Loss of Sync	10	1	Loss of Sync	10	1
Loss of Signal	10	1	Invalid Trans Word	0	0
Invalid CRC	341724	0	Invalid CRC	341724	0
FEC Uncorrected	87407814	0	FEC Uncorrected	87410651	0

Figure 61. FEC uncorrected value

Example #3: dBm errors:

The "Rx Power (dBm)" value of ficon2 port1 was very bad than the other port. It was -15.9 dBm , although the others are approximately -1.5 through -2.5 dBm.

Adapter		Local Node ID				Remote Node ID				
Name	Intf	Type	Model	Serial Number	Tag	Type	Model	Serial Number	Tag	
ficon2:0	003490	C2A	IBM	78-00000BD34V	0200	002499	816	IBM	CA-00010189KV	0096
FEC is inactive.										
ficon2:1	003490	C2A	IBM	78-00000BD34V	0201	002499	816	IBM	CA-00010189KV	00BE
FEC is inactive.										

WWNN : 50050764058004CE Link-Max Actual
 WWPN[0]: 50050764050004CE Negotiate 16Gbit
 WWPN[1]: 50050764050084CE Negotiate 16Gbit

ficon2:1

/D M=DEV(D000,(E5)),LINKINFO=COMPARE

D M=DEV(D000,(E5)),LINKINFO=COMPARE

IEE586I 07.32.06 DISPLAY M 854

DEVICE OD000 STATUS=ONLINE

Link Information: Compare

Channel Information: **CHPID=E5**, PCHID=02A0, WWPN=C05076D638082A01

Description	First	Last
Date Retrieved	12/14/2017	12/21/2017
Time Retrieved	20:34:09	07:25:58
Tx Power (dBm)	0.32	0.32
Rx Power (dBm)	-0.29	-0.23
Tx Bias (mA)	20.6	20.4
Temperature (C)	21.9	20.6
Voltage (V)	3.29	3.29
Capable Speed	16G	16G
Operating Speed	16G	16G
Buffer Credits	90	90
Link Failures	0	1
Loss of Sync	0	0
Invalid Trans Word	0	0
Invalid CRC	0	0
FEC Uncorrected	0	0

Switch Entry Port Information: Link=BC, WWPN=20BC000533FDEA54

Description	First	Last
Date Retrieved	12/15/2017	12/21/2017
Time Retrieved	09:54:27	07:25:58
Tx Power (dBm)	0.19	0.21
Rx Power (dBm)	2.62	2.51
Tx Bias (mA)	42.9	42.8
Temperature (C)	49	48
Voltage (V)	3.31	3.31
Capable Speed	16G	16G
Operating Speed	16G	16G

Description	First	Last
Buffer Credits	Not Avail	Not Avail
Link Failures	4	5
Loss of Sync	0	0
Invalid Trans Word	0	0
Invalid CRC	0	0
FEC Uncorrected	0	0

Switch Exit Port Information: Link=**BE**, WWPN=20BE000533FDEA54

Description	First	Last
Date Retrieved	12/15/2017	12/21/2017
Time Retrieved	16:44:05	07:25:58
Tx Power (dBm)	0.28	0.32
Rx Power (dBm)	0.56	0.62
Tx Bias (mA)	41.8	41.8
Temperature (C)	52	52
Voltage (V)	3.3	3.3
Capable Speed	16G	16G
Operating Speed	16G	16G
Buffer Credits	Not Avail	Not Avail
Link Failures	136	153
Loss of Sync	0	0
Invalid Trans Word	0	0
Invalid CRC	0	0
FEC Uncorrected	0	0

Control Unit Information: Intid=8001, WWPN=50050764050084CE

Description	First	Last
Date Retrieved	12/15/2017	12/21/2017
Time Retrieved	16:44:05	07:25:58
Tx Power (dBm)	0.95	0.86
Rx Power (dBm)	-15.9	-15.8
Tx Bias (mA)	45.6	45.1
Temperature (C)	46.4	47.1
Voltage (V)	3.31	3.31
Capable Speed	16G	16G
Operating Speed	16G	16G
Buffer Credits	90	90
Link Failures	0	0
Loss of Sync	0	0
Invalid Trans Word	0	0
Invalid CRC	0	0
FEC Uncorrected	0	0

Figure 62. dBm errors

INTERFACE ID value from DISPLAY M=DEV command

This topic describes how the DISPLAY M=DEV command would be issued to display information that is related to a certain control unit of TS7700.

The DISPLAY M=DEV command is used to display information that is related to a certain control unit. The output of the command is as follows.

```
D M=DEV(B80)
IEE174I 14.31.22 DISPLAY M 871
DEVICE 00B80 STATUS=ONLINE
CHP C4 C5 C6 C7 C0 C1 C2 C3
ENTRY LINK ADDRESS 62 62 63 63 30 30 01 01
DEST LINK ADDRESS 65 65 36 36 04 04 64 64
PATH ONLINE Y Y Y Y Y Y Y Y
CHP PHYSICALLY ONLINE Y Y Y Y Y Y Y Y
PATH OPERATIONAL Y Y Y Y Y Y Y Y
MANAGED N N N N N N N N
CU NUMBER 0B80 0B80 0B80 0B80 0B80 0B80 0B80 0B80
INTERFACE ID 8100 8101 8110 8111 8000 8001 8010 8011
MAXIMUM MANAGED CHPID(S) ALLOWED: 0
DESTINATION CU LOGICAL ADDRESS = 08
SCP CU ND = 003490.C2A.IBM.78.0000000H1234.0000
SCP TOKEN NED = 003490.C2A.IBM.78.0000000H1234.0008
SCP DEVICE NED = 003490.C2A.IBM.78.00000001234.0080
```

For general guidance and details on the DISPLAY M command, refer to the [z/OS MVS system commands reference](#).

The INTERFACE ID value is specific to the hardware product. The following table shows the INTERFACE ID value of TS7700:

Table 90. INTERFACE ID value	
8DCP	
First nibble	Always 8
Second nibble (D)	I/O Drawer (0 = primary drawer, 1 = alternate drawer)
Third nibble (C)	Card (0 or 1) Note: TS7760/TS7770 supports two FICON cards per I/O drawer.
Fourth nibble (P)	Port (0 or 1) Note: TS7760/TS7770 supports only two of the four physical ports.

The following figure represents two I/O drawers (primary and alternate) with various adapter cards inside the drawers.

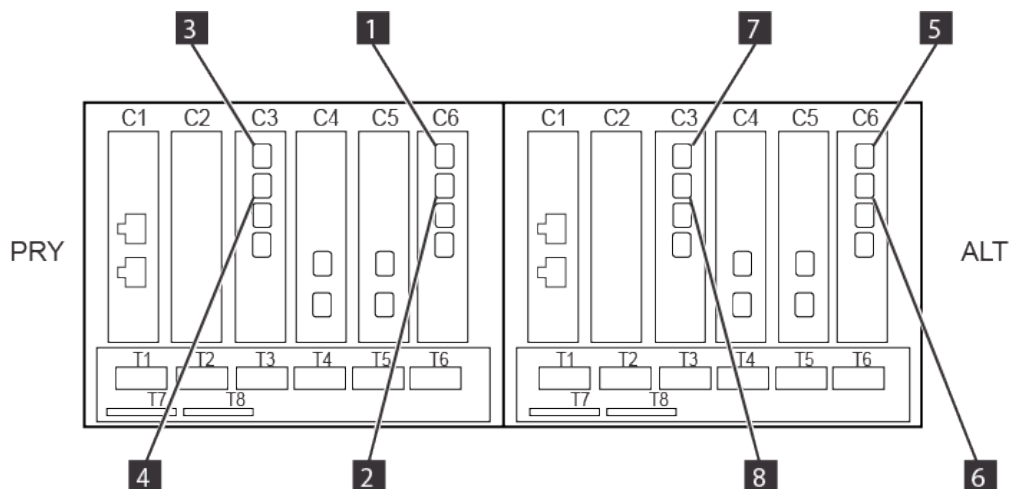


Figure 63. I/O enclosure cables, rear (FICON)

FICON cards are found in slots C3 and C6 in either I/O drawer.

PRY= I/O Drawer 0, ALT=I/O Drawer 1, C6=Card 0, C3=Card 1, Top Port=Port 0, and Second Port=Port 1

Also, only eight variations are possible which are described as follows:

8000 - I/O Drawer 0, Card 0, Port 0

8001 - I/O Drawer 0, Card 0, Port 1

8010 - I/O Drawer 0, Card 1, Port 0

8011 - I/O Drawer 0, Card 1, Port 1

8100 - I/O Drawer 1, Card 0, Port 0

8101 - I/O Drawer 1, Card 0, Port 1

8110 - I/O Drawer 1, Card 1, Port 0

8111 - I/O Drawer 1, Card 1, Port 1

The following table references the used ports (1 to 8) with two each per FICON card.

Table 91. I/O enclosure cables, rear (FICON)		
Index	Part name	Part number
1, 2, 3, 4, 5, 6, 7	Customer FICON Connection	Customer-supplied, no IBM PN
FICON cable cleaning tool	Fiber Cleaning Tool Note: Clean the FICON cable and SFP (Small Form factor Pluggable) before you use a wrap plug or plug a new or existing cable into any LC Duplex connector. Use the Fibre Cleaning Tool P/N 54Y4392 on the FICON cable and SFP before any connection.	54Y4392

Table 91. I/O enclosure cables, rear (FICON) (continued)

Index	Part name	Part number
Fiber loopback plugs	Fiber loopback plugs - you need to order two packs. Note: To complete the FICON wrap test, you need two fiber loopback plugs.	11P3847

Notices

The information provided by this media supports the products and services described with consideration for the conditions described herein.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries to:

IBM Corporation
 Almaden Research
 Bldg 80, D3-304, Department 277
 650 Harry Road
 San Jose, CA 95120-6099
 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and

cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

- AIX
- Enterprise Storage Server
- ESCON
- FICON
- i5/OS
- iSeries
- IBM
- pSeries
- S/390
- System Storage
- TotalStorage
- z/OS
- zSeries
- IBM Z

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ((R) or (TM)), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

Homologation

This section contains the homologation statement specific to Ethernet interfaces.

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Please contact IBM for information.

Safety and environmental notices

Review the safety notices, environmental notices, and electronic emission notices for the TS7700 before you install and use the product.

Safety notices

This publication contains the safety notices for the IBM Systems products in English and other languages. The safety notices include danger and caution notices. Anyone who plans, installs, operates, or services the system must be familiar with and understand the safety notices. Read the related safety information before beginning work.

Refer to *IBM Systems Safety Notices*, distributed on the CD *IBM Warranty, License, Environmental and Safety Notices Publication*.

Safety labels

This publication contains the safety information labels for the IBM Systems products in English and other languages. The safety information labels include danger and caution labels. Anyone who plans, installs, operates, or services the system must be familiar with and understand the safety labels. Read the related safety information before beginning work.

To view a PDF file, you need a PDF reader like Adobe Acrobat Reader.

Power cords

For your safety, IBM provides a power cord with a grounded attachment plug to use with this IBM product. To avoid electrical shock, always use the power cord and plug with a correctly grounded outlet.

IBM power cords used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).

For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.

For units intended to be operated at 230 volts (US use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.

For units intended to be operated at 230 volts (outside the US): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.

IBM power cords for a specific country or region are usually available only in that country or region.

Environmental notices

This publication contains all the required environmental notices for IBM Systems products in English and other languages. The environmental notices include statements on limitations, product recycling and disposal, product information, the battery return program, flat panel display, monitors and workstations, refrigeration, and water cooling systems.

Refer to *IBM Systems Environmental Notices and User Guide*, z125-5823, distributed on the CD *IBM Warranty, License, Environmental and Safety Notices Publication*,.

To view a PDF file, you need a PDF reader like Adobe Acrobat Reader.

Taiwan Hazardous Substance Table

限用物質含有情況標示

The Presence Condition of the Restricted Substances Marking

設備名稱：伺服器，儲存設備 Equipment Name: Server，Storage		類型指定：所有銷售至台灣之型號 Type Designation: All				
單位 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent Chromium (Cr+6)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
電池/電池組 Battery/Battery pack	-	O	O	O	O	O
CD/DVD 驅動器 CD/DVD Drive	-	O	O	O	O	O
風扇 Fans	-	O	O	O	O	O
硬碟 Hard Disk Drive	-	O	O	O	O	O
擴充抽取盒 I/O Drawer	-	O	O	O	O	O
機械組件 Mechanical Assemblies	-	O	O	O	O	O
塑膠材料 Plastics	O	O	O	O	O	O
PCI 介面卡 PCI Card	-	O	O	O	O	O
電源線 Power Cord	-	O	O	O	O	O
電源供應器 Power Supply	-	O	O	O	O	O
印刷電路板 Printed Circuit Board	-	O	O	O	O	O
處理器模組 Processor Module	-	O	O	O	O	O
固態硬碟 Solid State Drive	-	O	O	O	O	O
儲存裝置 Storage Device	-	O	O	O	O	O
磁帶匣 Tape Cartridge	-	O	O	O	O	O
磁帶機 Tape Drive	-	O	O	O	O	O
不斷電系統 (UPS) Uninterruptible Power Supply	-	O	O	O	O	O
備考 1: “超出 0.1 wt %” 及 “超出 0.01 wt %” 係指限用物質之百分比含量超出百分比含量基準值。 Note 1: “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of the presence condition. 備考 2: “O” 係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2: “O” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence. 備考 3: “-” 係指該項限用物質為排除項目。 Note 3: “-” indicates that the restricted substance corresponds to the exemption. 法律免責聲明 CNS 15663 免責聲明：此表格提供的資訊僅符合台灣適用法律。並不代表 IBM 向客戶履行任何保證或責任。該表格的假設正常條件是產品的使用情況與 IBM 操作手冊運作一致。 CNS 15663 Disclaimer: The information provided in this table is solely to comply with applicable laws of Taiwan. It does not create any warranties or liabilities on behalf of IBM to customers. The table assumes that the product will be used under normal conditions in accordance with the IBM operating manual.						

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other regions.

United States Federal Communications Commission (FCC) Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Responsible Party:

International Business Machines Corporation

New Orchard Road

Armonk, NY 10504

Contact for FCC compliance information only: fccinfo@us.ibm.com

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Union Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

European community contact:

IBM Deutschland GmbH

Technical Regulations, Department M372

IBM-Allee 1, 71139 Ehningen, Germany

Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233

Email: halloibm@de.ibm.com

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Germany Electromagnetic Compatibility Directive

Deutschsprachiger EU Hinweis:

Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein. Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 / EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV-Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 800 225 5426
e-mail: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

Deutschsprachiger EU Hinweis:

Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein. Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV-Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 800 225 5426
e-mail: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022/ EN 55032 Klasse B.

People's Republic of China Class A Electronic Emission statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Taiwan contact information

This topic contains the product service contact information for Taiwan.

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

12c00790

Japan Voluntary Control Council for Interference (VCCI) Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策
を講ずるよう要求されることがあります。

VCCI-A

Japan Electronics and Information Technology Industries Association Statement

This statement explains the Japan JIS C 61000-3-2 product wattage compliance.

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値： Knowledge Centerの各製品の
仕様ページ参照

This statement explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement explains the JEITA statement for products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類：6（単相、P F C回路付）
- 換算係数：0

This statement explains the JEITA statement for products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類：5（3相、P F C回路付）
- 換算係数：0

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

0123456789

Korean Electromagnetic Interference (EMI) Statement

This explains the Korean Electromagnetic Interference (EMI) statement.

**이기는업무용환경에서사용할목적으로적합성평가를받은기기로서
가정용환경에서사용하는경우 전파간섭의우려가있습니다.**

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” on page 393](#) [“B” on page 395](#) [“C” on page 396](#) [“D” on page 398](#) [“E” on page 400](#) [“F” on page 402](#) [“G” on page 403](#) [“H” on page 404](#) [“I” on page 406](#) [“J” on page 407](#) [“K” on page 408](#) [“L” on page 408](#) [“M” on page 410](#) [“N” on page 412](#) [“O” on page 413](#) [“P” on page 413](#) [“R” on page 415](#) [“S” on page 417](#) [“T” on page 421](#) [“U” on page 422](#) [“V” on page 422](#) [“W” on page 423](#)

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.

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.

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.

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 a TS3500 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.

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 TS7700 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.

DFSMSshsm

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 3956-CSA and 3956-CSB cache controllers along with the 3956-XSA and 3956-XSB cache drawers 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 403](#)

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. Microinstructions 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](#).

overflow

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 (2 to the 50th power).

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 3592 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](#).

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](#).

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 TS7700 Server emulates the function and operation of 3490 Enhanced Capacity (3490E) tape drives.

virtual terminal

A system object, created and controlled by an application program, that provides a functional representation or simulation of a physical display station.

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](#).

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](#).

Reference

This section lists codes and descriptions for TS7700 Management Interface error messages and events, ERA codes, operator information messages, and service information messages. In this section you can also find glossary definitions and a list of trademarks.

Index

Numerics

3490 Enhanced Capacity (3490E) Tape Drive
 and virtual volume size [89](#)
 appearance of in TS7700
 presented drive image [83](#)
3584 Tape Library [161](#)
3584 Tape Library Specialist Information [161](#)
3590 Tape Cartridges
 and cartridge capacity utilization [52](#)
3592 E05 Tape Drives
 native capacity
 and 3592 J1A emulation mode [44](#)
 and 3592 J1A Tape Drives [44](#)
3592 J1A Tape Drive [4, 7](#)
3592 Tape Cartridges
 cartridge capacity utilization [52](#)
 illustration [49](#)
3592 Tape Drives
 attached to TS3500/TS4500 Tape Library
 designated as control path [44](#)
 in Model D22 frame [44](#)
 in Model D23 frame [44](#)
 in Model L22 frame [44](#)
 in Model L23 frame [44](#)
 compared to 3590 Tape Drive [44](#)
 features [44](#)
 illustration [44](#)
3952 F05 (see [3952 Tape Frame](#)) [13](#)
3952 Tape Base Frame
 floor requirements
 weight distribution and loading [72](#)
3952 Tape Expansion Frame
 floor requirements
 weight distribution and loading [73](#)
3952 Tape Frame
 acoustic requirements [77](#)
 and TS7760 Cache Controller [42](#)
 clearance requirements
 frame in position table [73](#)
 moving the frame table [73](#)
 cooling requirements [72](#)
 environmental requirements
 air temperature [75](#)
 altitude [75](#)
 relative humidity [75](#)
 shipping [75](#)
 storage [75](#)
 wet bulb temperature [75](#)
 floor requirements
 general [72](#)
 leveling [72](#)
 function [13](#)
 physical characteristics [27, 59, 73](#)
 power requirements
 internal power distribution unit [67](#)
 specifications table [59](#)

3957 V06 (see [TS7700 Node](#)) [13](#)
6 TB high-performance cache [4](#)

A

abbreviations [393](#)
accessibility [385](#)
acoustic requirements [77](#)
acronyms [393](#)
adapter assignments table [13](#)
adapters
 adapters
 assignments [13](#)
 assignments
 table of [13](#)
 Ethernet [13](#)
 Fibre (or fiber) channel [13](#)
 FICON [13](#)
 Input/Output (I/O)
 adapter assignments table [13](#)
 network [85](#)
 to TSSC [13](#)
add
 users to customer group [266](#)
administer users [266](#)
advanced policy management functions
 and cache management policies
 and volume caching [52](#)
 and TS7700
 dual copy [4, 11](#)
 multiple reclamation policies [4, 11](#)
 virtual volume size [4, 11](#)
 volume pooling [4, 11](#)

AES [106](#)
AIX [105](#)
Alternate Local Interface IP [161](#)
Alternate Router IP [161](#)
and TS7760 Cache Controller [42](#)
and TS7760 Cache Drawer [43](#)
AOTM [226, 227](#)
Assist On-Site (AOS) [267](#)
attached systems [268](#)
audit logs
 downloading [269](#)
 viewing [269](#)
automated read-only recovery [233](#)
Autonomic Ownership Takeover Manager [226, 227](#)

B

bandwidth
 throughput [52](#)
Base Numbering [26](#)
Beg DevID [161](#)
binary [26](#)
Bulk Volume Information Retrieval [112](#)
BVIR [112](#)

C

- cache [4](#)
- Call Home [83](#)
- call home settings [270](#)
- Call-in Modem Number [161](#)
- capacity on demand [4](#)
- Cartridge Assignment Policy [161](#)
- cartridge capacity utilization
 - and 3590 Tape Cartridges [52](#)
 - and 3592 Tape Cartridges [52](#)
 - and physical volume [52](#)
 - and TS7700 Cache [52](#)
 - and virtual volume [52](#)
- caution [385](#)
- certificate
 - proxy [264](#)
- change
 - password [266](#)
- checklists
 - customer tasks [161](#)
- clearance requirements
 - frame in position table [73](#)
 - moving the frame table [73](#)
- cluster families [208](#)
- cluster family [208](#)
- Cluster Index [161](#)
- Cluster Number for the Remote System [161](#)
- components, system console [263](#)
- components, TSSC [263](#)
- composite library
 - and grid configuration [13](#)
 - composite library ID in z/OS I/O [82](#)
- Composite Library Sequence Number [161](#)
- configuring
 - Assist On-Site settings [267](#)
- connected to I/O drawer [13](#)
- console
 - logout [265](#)
 - management GUI [265](#)
- cooling requirements [72](#)
- copy export
 - acceleration [114](#)
 - and disaster recovery [112](#)
 - and physical volumes [112](#)
 - and virtual volumes [112](#)
 - disaster recovery [112](#)
 - merge [113](#)
- Copy queue [220](#)
- customer
 - group, add users to or delete users from [266](#)
- Customer Contact Phone Number [161](#)
- Customer Gateway [161](#)
- Customer ID [161](#)
- Customer IP Address [161](#)
- Customer Name [161](#)
- Customer Subnet Mask [161](#)

D

- danger [385](#)
- DASD [88](#)

- data protection [103](#)
- data storage [26](#)
- definitions [393](#)
- delete users from the customer group [266](#)
- DFSMS [240](#)
- DHCP [161](#)
- disable SNMP trap forwarding [267](#)
- disaster recovery
 - and grid configuration [13](#), [202](#), [237–240](#)
 - and TS7700 Cluster [240](#)
 - and workload considerations [53](#)
 - plans
 - DFSMS [237](#)
 - host connectivity [237](#)
 - procedures [237](#)
 - WAN infrastructure and bandwidth [237](#)
- disaster recovery and high availability
 - planning
 - access to host FICON [240](#)
 - copy consistency policies [241](#)
 - DWDM [240](#)
- disk drive modules (DDM)
 - and TS7700 Cache Controller [13](#)
 - and TS7700 Cache Drawer [13](#)
 - and TS7760 Cache Controller [42](#)
 - and TS7760 Cache Drawer [43](#)
- distributed library
 - and grid configuration [13](#)
 - distributed library ID in z/OS I/O [82](#)
 - subsystem identification definitions [82](#)
- Distributed Library Sequence Number [161](#)
- drive concurrency
 - access to multiple virtual volumes on stacked volume [52](#)
 - and job control language (JCL) [52](#)
 - and TS7700 Cache [52](#)
- Drive range locations [161](#)
- Dual LM [161](#)
- Dual LM Library Indicator [161](#)
- Dynamic Host Configuration Protocol [161](#)

E

- ECCST media [90](#)
- Elem Addr Range [161](#)
- enable
 - SNMP trap forwarding [267](#)
- encryption
 - across LAN/WAN [85](#)
 - algorithms [107](#)
 - and TS3500/TS4500 Tape Library [103](#)
 - asymmetric encryption [107](#)
 - data key [107](#)
 - disk [109](#)
 - encryption
 - encryption key management [103](#)
 - key management [103](#)
 - policy configuration [103](#)
 - encryption-capable tape drive
 - TS1120 Tape Drive [103](#)
 - encryption-enabled tape drive
 - TS1120 Tape Drive [103](#)
 - external [109](#)
 - externally encrypted data key [107](#)
 - internal [109](#)

- encryption (*continued*)
 - key encrypting key [107](#)
 - key management [109](#)
 - key wrapping [107](#)
 - keys [105](#), [107](#)
 - overview [103](#)
 - policy configuration [103](#)
 - private key [107](#)
 - public key [107](#)
 - symmetric encryption [107](#)
- Encryption
 - management locations
 - in application [106](#)
 - in library [106](#)
 - in system [106](#)
- encryption key management
 - AIX [105](#)
 - and Advanced Encryption Standard [106](#)
 - and encryption-enabled drives [105](#)
 - and key generation [106](#)
 - and key retrieval [106](#)
 - and RSA key pairs [106](#)
 - description [105](#)
 - HP-UX [105](#)
 - i5/OS [105](#)
 - Java [105](#)
 - Linux [105](#)
 - Sun Solaris [105](#)
 - through TCP/IP [106](#)
 - Windows [105](#)
 - z/OS [105](#)
- environmental notices [386](#)
- environmental requirements
 - air temperature [75](#)
 - altitude [75](#)
 - relative humidity [75](#)
 - shipping [75](#)
 - storage [75](#)
 - wet bulb temperature [75](#)
- Ethernet
 - adapters table [13](#)
 - failure between clusters [236](#)
 - LAN/WAN
 - network redundancy [85](#)
- Ethernet Gateway [161](#)
- Ethernet Hostname [161](#)
- Ethernet IP Address [161](#)
- Ethernet Network Configuration Method [161](#)
- Ethernet Subnet Mask [161](#)
- Export List Volume [112](#)

F

- FC 0500 [161](#)
- features
 - FC 1903, Dual AC Power [67](#)
- fiber [221](#)
- Fibre (or fiber) channel
 - adapter table [13](#)
 - and TS3500 Tape Library [44](#)
 - and TS7760 Cache Controller [42](#)
 - and TS7760 Cache Drawer [43](#)
 - attachment to IBM Z host
 - multi-mode [79](#)

- Fibre (or fiber) channel (*continued*)
 - attachment to IBM Z host (*continued*)
 - single mode [79](#)
 - virtual devices [13](#)
- Fibre Channel [44](#)
- FICON
 - adapters table [13](#)
 - and throughput [52](#)
- firewall settings [269](#)
- Fixed IP [161](#)
- flash copy [238](#)
- floor requirements
 - general [72](#)
 - leveling [72](#)
 - weight distribution and loading [72](#), [73](#)
- forwarding, enabling SNMP trap [267](#)
- From, To [161](#)

G

- G [26](#)
- Gateway Address for the Alternate Local Interface [161](#)
- Gateway Address for the Primary Local Interface [161](#)
- General Node
 - also gNode [13](#)
- Gi [26](#)
- glossary [393](#)
- gNode
 - also General Node [13](#)
 - and hNode [13](#)
 - and vNode [13](#)
 - as TS7700
 - illustration [13](#)
 - function [13](#)
 - illustration [13](#)
 - role [13](#)
- grid
 - network
 - load balancing [3](#), [53](#)
- Grid [161](#)
- Grid Adapter Card [161](#)
- grid link statistics [3](#), [53](#)
- Grid Network
 - role of TCP/IP [202](#)
- grid network load balancing [3](#), [53](#)

H

- HCD [161](#)
- hierarchical storage management [233](#)
- hierarchical storage management (HSM)
 - and hNode [13](#)
- high availability
 - and LAN [240](#)
 - and TS7700 Cluster [240](#)
 - in grid configuration [240](#)
 - planning
 - DFSMS [240](#)
 - ownership takeover [240](#)
 - procedures [240](#)
 - RUN [240](#)
 - virtual device configuration [240](#)
- high reliability [44](#)

- hNode
 - and physical volumes [13](#)
 - and virtual volumes [13](#)
 - combined with vNode to form gNode [13](#)
 - function [13](#)
 - hierarchical storage management [13](#)
 - illustration [13](#)
 - role [13](#)
- Home Pool [161](#)
- host
 - compatibility [78](#)
 - configurations
 - hardware configuration definition (HCD) [82](#)
 - z/OS I/O definitions [82](#)
 - mount request [216](#)
 - supported hosts
 - IBM Z [78](#)
 - s390 [78](#)
 - supported operating systems
 - z/OS 1.4 [78](#)
- Host console request
 - cache [82](#)
 - command [82](#)
 - LI REQ [82](#)
 - logical volume [82](#)
 - media [82](#)
 - physical drive [82](#)
 - physical volume [82](#)
 - TS7700 Grid [82](#)
- host console request function
 - and copy export [112](#)
- HP-UX [105](#)
- HSM [233](#)
- human intervention [226](#)

I

- i5/OS [105](#)
- IBM System Storage TS3000 System Console [261](#)
- IBM Z
 - attachment to TS7700
 - illustration [79](#)
 - long wave laser [79](#)
 - multi mode fiber [79](#)
 - short wave laser [79](#)
 - single mode fiber [79](#)
 - supported on TS7700 [78](#)
 - z/OS I/O definitions
 - Cluster and Grid reporting [82](#)
 - presented drive image [83](#)
 - subsystem identification [82](#)
- incremental capabilities [4](#)
- infrastructure requirements
 - network adapter assignments [85](#)
 - network switches and TCP/IP Ports [87](#)
- Input/Output (I/O)
 - adapter assignments table [13](#)
 - z/OS I/O definitions
 - Cluster and Grid reporting [82](#)
 - composite library identification [82](#)
 - presented drive image [83](#)
 - subsystem identification [82](#)
- interchange/offsite
 - storage

- interchange/offsite storage (*continued*)
 - suitability [53](#)
- intervention, human [226](#)
- IP Address for the Remote System [161](#)
- IP whitelist [269](#)

K

- K [26](#)
- keyboards
 - accessibility features [385](#)
- Ki [26](#)

L

- LAN [161](#)
- LAN/WAN
 - encryption [85](#)
 - network conflicts [85](#)
 - network redundancy [85](#)
- laser
 - long wave [79](#)
 - short wave [79](#)
- LDAP
 - service access [243](#)
- Library Sequence Number [161](#)
- Library Type Indicator [161](#)
- Library VTS Partition [161](#)
- Linux [105](#)
- load balance
 - dynamic load balancing [3](#), [53](#)
- load balancing [3](#), [53](#)
- local cache [3](#)
- log settings [269](#)
- logging in [264](#)
- Logical Library Name [161](#)
- Logical WORM [216](#)
- login
 - system console [264](#)
- login options
 - local [264](#)
 - remote [264](#)
- logout [265](#)

M

- M [26](#)
- management GUI
 - attached systems [268](#)
 - call home settings [270](#)
 - firewall settings [269](#)
 - log settings [269](#)
 - RSYSLOG settings [269](#)
 - system console [265](#)
 - test call home [270](#)
- Management Interface
 - and disaster recovery [112](#)
- managing
 - login options
 - local [264](#)
 - remote [264](#)
- Max Cartridges [161](#)
- Media Type [161](#)

Media Volume Serial Range [161](#)
metric [26](#)
Mi [26](#)
migration [220](#)
modem [83](#)
multifile volumes
 replacing need for JCL constructs [53](#)

N

network
 adapter assignments
 gateway IP [85, 86](#)
 subnet mask [85, 86](#)
 TCP/IP [85, 86](#)
 Grid WAN
 TCP/IP port assignments table [87](#)
 switches, infrastructure requirements [87](#)
network information [278](#)
Network Mask for the Alternate Local Interface [161](#)
Node Index [161](#)
Node Number for the Remote System [161](#)
notices
 environmental [386](#)
NTP server TCP/IP [161](#)

O

Off Shift Customer Contact Phone Number [161](#)
on-demand
 virtual devices [4, 9](#)
 virtual volumes [4, 9](#)
operating systems [78](#)
ownership takeover
 and TS7700 failure [236](#)
 as a result of a failed cluster [226](#)
 Read Ownership Takeover (ROT) [226](#)
 Write Ownership Takeover (WOT) [226](#)

P

password
 change [266](#)
peer-to-peer [161](#)
peer-to-peer (PtP) compared to grid configuration [13](#)
performance [4, 10](#)
physical volume
 and cartridge capacity utilization [52](#)
 and virtual volume [13](#)
 planning
 amount of data stored [91](#)
 average compression ratio [91](#)
 average utilization rate [91](#)
 formula to calculate number needed [92](#)
 scratch physical volumes [91](#)
 recovery
 automated read-only recovery [233](#)
physical volumes
 recovering data from [286](#)
planning
 checklists [161](#)
 feature codes [115](#)
 grid configuration [203](#)

planning (*continued*)
 host
 compatibility [78](#)
 infrastructure requirements [83](#)
 physical volumes [88](#)
 stacked volume [88](#)
 system requirements [54](#)
 virtual volumes [88](#)
 workload considerations [52](#)
power
 3952 Tape Frame
 internal power distribution unit [67](#)
 FC 1903, Dual AC Power [67](#)
 requirements [67](#)
Primary Customer IP [161](#)
Primary Fibre channel switch type [161](#)
Primary Local Interface IP [161](#)
Primary Local Network Mask Address [161](#)
Primary Router IP [161](#)
proxy certificate [264](#)

R

RACF
 IBM Z [246](#)
 TS7700 [246](#)
Read Ownership Takeover (ROT) [226](#)
recovering
 data
 from physical volumes [286](#)
redundant array of independent disks (RAID)
 and TS7700 Cache Controller [13](#)
 and TS7760 Cache Controller [42](#)
 and TS7760 Cache Drawer [43](#)
remote cache [3](#)
remote security through the IMC [261](#)
remote support
 security [261](#)
remote support security [261](#)
Retain Copy Mode [219](#)
return-to-scratch processing
 frequency of [90](#)
rewind unload processing (RUN) [4](#)
roles management [277](#)
RSYSLOG settings [269](#)
RUN [237, 240](#)

S

s390
 supported on TS7700 [78](#)
safety [385](#)
safety notices [385](#)
Scratch Pool [161](#)
scratch volumes
 mount times
 virtual volume recall [52](#)
 numbers needed per day [90](#)
 return-to-scratch processing
 and grid configuration [90](#)
 time required [90](#)
Secure Data Erasure
 and 3592 Tape Cartridges [48](#)

- Secure Data Erasure (*continued*)
 - and Encryption [48](#)
 - and physical volumes [48](#)
- security [261](#)
- security settings [271](#)
- selective device access control
 - and TS7700 Cluster [235](#)
 - in grid configuration [235](#)
- serial port
 - connecting to
 - x306 [263](#)
 - x306m [263](#)
- Service Mode [226](#)
- Service Preparation/Service Mode [226](#)
- setting
 - IP whitelist [269](#)
 - roles management [277](#)
 - SNMP trap forwarding [267](#)
- settings
 - security [271](#)
- SI [26](#)
- SLDC [44](#)
- SMSplex [88](#)
- SSL or CA certificate [264](#)
- stacked volume
 - and drive concurrency [52](#)
 - and multifile volumes [53](#)
 - and volume caching [52](#)
 - planning
 - affected by virtual volume size [90](#)
- Starting Element Address [161](#)
- Streaming Lossless Data Compression (SLDC) [44](#)
- subsystem identification
 - hardware configuration definition [82](#)
 - z/OS I/O definitions [82](#)
- Sun Solaris [105](#)
- sync mode copy [230](#)
- synchronous mode copy [230](#)
- system console
 - management GUI
 - administer users [266](#)
 - attached systems [268](#)
 - firewall settings [269](#), [270](#)
 - log settings [269](#)
 - RSYSLOG settings [269](#)
 - test call home [270](#)
- system requirements
 - 3592 Tape Frame specifications [59](#)
 - acoustic requirements [77](#)
 - clearance requirements
 - frame in position table [73](#)
 - moving the frame table [73](#)
 - cooling requirements [72](#)
 - environmental requirements [75](#)
 - floor requirements
 - general [72](#)
 - leveling [72](#)
 - weight distribution and loading [72](#), [73](#)
 - power requirements [67](#)
- System Storage TS3000 System Console (see TSSC)
 - adapter assignments table [13](#)

T

- T [26](#)
- tables
 - system console components [263](#)
- tape drive
 - 3592 Tape Drive
 - 3592 J1A Tape Drive [4](#), [7](#)
 - 3592 Tape Drives [44](#), [49](#)
 - encryption-capable [103](#)
 - encryption-enabled [103](#)
 - virtual tape drive [13](#)
 - virtual tape image [13](#)
- Tape Drive Physical Positions [161](#)
- tape synchronization [230](#)
- TCP/IP
 - network adapter assignments
 - Grid WAN addresses [86](#)
- TCP\IP
 - in TS7700 Grid [202](#)
 - infrastructure requirements [87](#)
 - network adapter assignments [86](#)
 - network conflicts across LAN/WAN [85](#)
 - network port assignments table [87](#)
- telephone line [83](#)
- terms [393](#)
- test call home [270](#)
- throughput
 - and FICON [52](#)
 - bandwidth [52](#)
 - in TS7700 [52](#)
 - reduced by recall activity [52](#)
- Ti [26](#)
- Tivoli Storage Manager [106](#)
- Trademarks [384](#)
- trap forwarding, enabling SNMP [267](#)
- TS3000 system console (TSSC)
 - security when providing remote support [261](#)
- TS3500 Tape Library
 - attached to TS7700 [79](#)
 - attachment to TS7700 [4](#), [6](#), [43](#)
 - TS4500 Tape Library [107](#)
- TS3500/TS4500 Tape Library
 - 3592 Tape Drives
 - attached to [44](#)
 - designated as control path [44](#)
 - in Model D22 frame [44](#)
 - in Model D23 frame [44](#)
 - in Model L22 frame [44](#)
 - in Model L23 frame [44](#)
 - Advanced Library Management System (ALMS) [44](#)
 - and Fibre channel [44](#)
- TS4500 Tape Library
 - attachment to TS7700 [4](#), [6](#)
- TS7700
 - and ownership takeover [236](#)
 - appearing as 3490E strings [52](#)
 - architecture
 - modular and scalable [4](#)
 - as gNode
 - illustration [13](#)
 - cluster [201](#)
 - cluster configuration
 - illustration [13](#)

TS7700 (continued)

- distributed node architecture - gNode [13](#)
- distributed node architecture - hNode [13](#)
- distributed node architecture - vNode [13](#)
- failure [236](#)
- host compatibility
 - IBM Z [78](#), [79](#)
 - s390 [78](#)
- host configurations
 - z/OS I/O definitions [82](#)
- infrastructure requirements
 - adapter assignments [85](#)
 - network switches and TCP/IP Ports [87](#)
- library attachments [43](#)
- photograph of [4](#)
- supported storage media
 - cartridge capacity utilization [52](#)
- supported tape drives
 - 3592 E05 Tape Drives [44](#)
 - 3592 Tape Drives [44](#)
- supported tape libraries
 - TS3500 Tape Library [4](#), [6](#), [43](#), [44](#)
 - TS4500 Tape Library [6](#), [44](#)
- system components
 - TS7700 Cache Controller [13](#)
 - TS7700 Cache Drawer [13](#)
 - TS7700 Node [13](#)
 - TS7700 Server [13](#)
 - TS7760 Cache Controller [42](#)
 - TS7760 Cache Drawer [43](#)
- system configurations
 - cluster [201](#), [208](#)
 - cluster families [208](#)
- system requirements
 - 3592 Tape Frame specifications [59](#)
 - acoustic requirements [77](#)
 - clearance requirements [73](#)
 - cooling requirements [72](#)
 - environmental requirements [75](#)
 - floor requirements [72](#), [73](#)
- TS7760 tape attach [43](#)
- workload considerations
 - cartridge capacity utilization [52](#)
 - disaster recovery [53](#)
 - drive concurrency [52](#)
 - interchange/offsite storage [53](#)
 - multifile volumes [53](#)
 - scratch mount times [52](#)
 - throughput [52](#)
 - volume caching [52](#)

TS7700 Cache

- and volume caching [52](#)

TS7700 Cache Controller

- elements
 - disk drive modules [13](#)
 - Fibre (or fiber) channel adapter table [13](#)
 - redundant array of independent disks [13](#)
- related to TS7700 Cache Drawer [13](#)
- related to TS7700 Cache Module [13](#)

TS7700 Cache Drawer

- elements
 - disk drive modules [13](#)
- related to TS7700 Cache Controller [13](#)

TS7700 Cache Module

- elements
 - disk drive modules [13](#)
 - related to TS7700 Cache Controller [13](#)

TS7700 Cluster

- and disaster recovery [237](#)–[239](#)
- and TS3500 Tape Library
 - tape cartridges [201](#)
 - tape drive [201](#)
- and TS4500 Tape Library
 - tape cartridges [201](#)
 - tape drive [201](#)
- and virtual volume attributes [13](#)
- and virtual volume copies [4](#)
- flash copy [238](#)
- illustration [13](#), [201](#)
- in grid configuration [13](#), [221](#)
- in Grid configuration [202](#)
- reporting to a IBM Z host [82](#)
- virtual volume ownership [221](#)
- write protect [239](#)

TS7700 Grid

- and read-only recovery [233](#)
- and return-to-scratch processing [90](#)
- and TCP/IP [202](#)
- and TS7700 Cluster [13](#), [201](#)
- and virtual volume attributes [13](#), [202](#)
- appearing as a composite library
 - and distributed library [13](#)
- as a disaster recovery system [13](#), [53](#), [202](#)
- as a remote virtual volume replication system [202](#)
- configuring
 - flash copy [238](#)
 - for disaster recovery [238](#), [239](#)
 - for disaster recovery and high availability [240](#)
 - for high availability [240](#)
 - selective device access control [235](#)
 - write protect [239](#)
- data access and availability [3](#)
- description [202](#)
- hybrid [203](#)
- illustration [13](#)
- reporting to a IBM Z host [82](#)
- TS7760 Tape Attach Cluster [201](#)
- virtual volume
 - mount request [221](#)
- WAN IP addresses [86](#)

TS7700 Server

- functions [13](#)

TS7700 Virtualization Engine

- concepts [1](#)
- host compatibility [78](#)
- supported storage media
 - 3592 Tape Cartridges [49](#)
- supported storage media. [1](#)
- supported tape drives [1](#)
- supported tape libraries [1](#)
- system components [1](#)
- system configurations [1](#)

TS7700 Virtualization Engine Grid

- configuring
 - for disaster recovery [237](#)

TS776 Cache Controller

- elements

- TS776 Cache Controller (*continued*)
 - elements (*continued*)
 - Fibre (or fiber) channel [42](#)
- TS7760
 - and 3952 Tape Frame [37](#)
 - and TS7760 Storage Expansion Frame [37](#)
 - system requirements
 - power requirements [67](#)
- TS7760 Cache
 - and disk drive modules [42](#), [43](#)
- TS7760 Cache Controller
 - and 3952 F06 or F07 Tape Frame
 - specifications [73](#)
 - and 3952 Tape Frame [42](#)
 - elements
 - disk drive modules [42](#)
 - Fibre (or fiber) channel [42](#)
 - redundant array of independent disks [42](#)
 - photograph [42](#)
 - related to TS7760 Cache Drawer [42](#)
 - role [42](#)
- TS7760 Cache Drawer
 - and 3952 F06 or F07 Tape Frame
 - specifications [73](#)
 - and redundant array of independent disks [43](#)
 - elements
 - disk drive modules [43](#)
 - Fibre channel [43](#)
 - photograph [43](#)
 - role [43](#)
- TS7760 Server
 - and 3952 F06 or F07 Tape Frame
 - specifications [73](#)
- TSSC
 - adapter assignments table [13](#)

U

- units [26](#)
- user login [264](#)
- users
 - add or delete [266](#)
 - administer [266](#)

V

- V06-1 [161](#)
- V06-2 [161](#)
- Virtual Device IDs [161](#)
- virtual devices [1](#), [4](#), [9](#)
- Virtual Library Name [161](#)
- virtual path [79](#)
- virtual tape drive
 - related to virtualization [13](#)
 - vNode [13](#)
- virtual volume
 - and cartridge capacity utilization [52](#)
 - and drive concurrency [52](#)
 - and hNode [13](#)
 - and physical volume [13](#)
 - and volume caching [52](#)
 - attributes and data replicated between clusters [13](#)
 - attributes and data replication in grid configuration [3](#), [13](#)

- virtual volume (*continued*)
 - copies [4](#)
 - location selection for access [3](#)
 - LWORM [216](#)
 - multiple, transparent access to [52](#)
 - ownership by TS7700 Cluster [221](#)
 - planning
 - formula to calculate number needed [89](#)
 - recall to virtual volume
 - volume caching [53](#)
 - scratch volumes
 - mount times [52](#)
 - numbers needed per day [89](#)
 - return-to-scratch processing [89](#)
 - size
 - set by VOLSER [89](#)
 - with data compression [89](#)
 - WORM [216](#)
- virtual volume format [2](#)
- virtual volumes [4](#), [220](#)
- virtualization
 - and hNode [13](#)
 - and vNode [13](#)
 - role of TS7700 Server [13](#)
- Virtualization Engine TS7700, *See* TS7700
- vNode
 - and virtual tape drive [13](#)
 - combined with hNode to form gNode [13](#)
 - function [13](#)
 - illustration [13](#)
 - role [13](#)
- VOLSER
 - planning
 - with physical volumes [88](#)
 - with virtual volumes [88](#)
 - planning with virtual and physical volumes
 - setting virtual volume size [89](#)
- volume caching
 - advanced policy management functions
 - cache management policies [52](#)
 - and stacked volume [52](#)
 - and TS7700 Cache [52](#)
 - and virtual volume
 - recall to virtual volume and throughput [52](#)
- volume serial numbering [89](#)

W

- Windows [105](#)
- workload considerations
 - cartridge capacity utilization [52](#)
 - disaster recovery [53](#)
 - drive concurrency [52](#)
 - interchange/offsite storage [53](#)
 - multifile volumes [53](#)
 - scratch mount times [52](#)
 - throughput [52](#)
 - volume caching [52](#)
- wrapped key pairs [106](#)
- Write Ownership Takeover (WOT) [226](#)
- write protect
 - selective [239](#)

Z

z/OS

I/O definitions

Cluster and Grid reporting [82](#)

composite library identification [82](#)

Host console request [82](#)

presented drive image [83](#)

subsystem identification - hardware configuration
definition (HCD) [82](#)

subsystem identification table [82](#)

z/VM [78](#)

z/VSE [79](#)

zTPF [79](#)



Printed in USA

GA32-0567-33

