HITACHI
DATA SYSTEMS

Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage

Data Retention Utility Software User's Guide

MK-95DF717-05

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Please contact the Hitachi Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-95DF717-P	May 2005	Preliminary Release
MK-95DF717-00	June 2005	Initial Release, supersedes and replaces MK-95DF717-P
MK-95DF717-01	August 2005	Revision 1, supersedes and replaces MK-95DF717-00
MK-95DF717-02	February 2006	Revision 2, supersedes and replaces MK-95DF717-01
MK-95DF717-03	April 2006	Revision 3, supersedes and replaces MK-95DF717-02
MK-95DF717-04	July 2006	Revision 4, supersedes and replaces MK-95DF717-03
MK-95DF717-05	August 2006	Revision 5, supersedes and replaces MK-95DF717-04

Changes in this Revision

- Added TrueCopy Extended Distance information

Preface

This document describes how to use Data Retention Utility software on Hitachi TagmaStore™ Adaptable Modular Storage (AMS) and Workgroup Modular Storage (WMS) subsystems. For operating and setup information for your AMS or WMS subsystem, refer to the appropriate document:

- *Hitachi TagmaStore™ Adaptable Modular Storage 200™ User and Reference Guide,* MK-95DF713
- *Hitachi TagmaStore™ Adaptable Modular Storage 500™ User and Reference Guide,* MK-95DF714
- *Hitachi TagmaStore™ Workgroup Modular Storage 100 User and Reference Guide,* MK-95DF738
- *Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide*, MK-95DF711
- *Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage, Storage Navigator Modular Command Line Interface (CLI) User's Guide*, MK-95DF712

This user's guide assumes that the user:

- Has a background in data processing and understands RAID storage subsystems and their basic functions, and
- Is familiar with Windows® 98, Windows NT®, and/or Windows® 2000 operating systems.

Note: For further information, please contact your Hitachi Data Systems account team, or visit the Hitachi Data Systems worldwide Web site at http://www.hds.com.

Notice: The use of Data Retention Utility software and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Software Version

This document revision applies to TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage versions 6.0 and higher.

Convention for Storage Capacity Values

Storage capacity values for logical units (LUs) are calculated based on the following values:

1 KB (kilobyte) = 1,024 bytes
1 MB (megabyte) = $1,024^2$ bytes
1 GB (gigabyte) = $1,024^3$ bytes
1 TB (terabyte) = $1,024^4$ bytes

Referenced Documents

- *Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide*, MK-95DF711
- *Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage, Storage Navigator Modular Command Line Interface (CLI) User's Guide*, MK-95DF712
- *Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage, Command Control Interface (CCI) User and Reference Guide*, MK-95DF701

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Contents

Chapter 1 Overview of Data Retention Utility

1.1 Assigning Access Attributes to Logical Units 2
1.2 Protecting Logical Volumes from Copy Operations 4
1.3 Data Retention Utility Requirements 5
1.4 Notes on the Use of Data Retention Utility 8
1.4.1 Notes on Usage 8
1.4.2 Notes and Limitations for Each Operating System 9

Chapter 2 Preparing for Data Retention Utility Operations

2.1 Installing 12
2.2 Uninstalling 16
2.3 Enabling or Disabling 17
2.4 Setting the Command Device 19
2.5 Defining the Configuration Definition File 23
2.6 Setting the Environment Variable 25

Chapter 3 Performing Data Retention Utility Operations (CCI)

3.1 Setting an Attribute 28
3.2 Changing the Retention Term 29

Chapter 4 Performing Data Retention Utility Operations (GUI)

4.1 Setting an Attribute 32
4.2 Setting a S-VOL 34
4.3 Changing the Retention Term 35
4.4 Setting the Expiration Lock 36

Appendix A Operations Using CLI

A.1 Installing Data Retention Utility 38
A.2 Uninstalling Data Retention Utility 40
A.3 Enabling or Disabling Data Retention Utility 41
A.4 Setting the Command Device 42
A.5 Setting an Attribute 44
A.6 Setting an S-VOL 45
A.7 Changing the Retention Term 46
A.8 Setting the Expiration Lock 47

Acronyms and Abbreviations 49

Glossary 53

List of Figures

Figure 1.1 Volume Migration of Read Only Attribute 7
Figure 2.1 Showing Enable/Disable Status 18

Figure 3.1 Raidvchkset Command Example 28
Figure 3.2 Raidvchkdsp Command Example 28
Figure 3.3 Raidvchkset Command Example 29
Figure 3.4 Raidvchkset Command Example 29
Figure 3.5 Raidvchkdsp Command Example 29

List of Tables

Table 1.1 Data Retention Utility Requirements..... 5

Chapter 1 Overview of Data Retention Utility

This chapter outlines and describes the following:

- 1.1 Assigning Access Attributes to Logical Units
- 1.2 Protecting Logical Volumes from Copy Operations
- 1.3 Data Retention Utility Requirements
- 1.4 Notes on the Use of Data Retention Utility

The Data Retention Utility feature protects data in your disk subsystem from I/O operations performed at open-systems hosts. Data Retention Utility enables you to assign an access attribute to each logical volume. If you use Data Retention Utility, you will be able to use a logical volume as a read-only volume. You will also be able to protect a logical volume against both read and write operations.

Note: Logical volumes are sometimes referred to as *logical devices* or *LDEVs*. Also, logical volumes to be accessed by open-systems hosts are sometimes referred to as *logical units* or *LUs*.

1.1 Assigning Access Attributes to Logical Units

By default, all the open-systems volumes are subject to read and write operations by open-systems hosts. For this reason, data on open-systems volumes might be damaged or lost if an open-systems host performs erroneous write operations. Also, confidential data on open-systems volumes might be stolen if an operator without approved access performs read operations on open-systems hosts.

By using Data Retention Utility, you can use logical as read-only volumes to protect the volumes against write operations. You can also protect logical volumes against both read and write operations. Data Retention Utility enables you to restrict read operations and write operations on logical volumes and prevents data from being damaged, lost and stolen.

To restrict read and write operations, you must assign an access attribute to each logical volume. Set the access attribute by using Hitachi Data Systems Command Control Interface (CCI) and Storage Navigator Modular. A system administrator can set one of the following access attributes for the each LU.

When the Read Only or Protect attribute is set using Storage Navigator Modular, the S-VOL Disable attribute for prohibiting a copy operation is set automatically. However, the S-VOL Disable attribute is not set automatically when CCI is used. When setting the Read Only, Protect, Report Zero Read Cap. mode, or Invisible mode using CCI, specify the S-VOL Disable attribute for prohibiting a copy operation at the same time.

- **Read/Write**

  If a logical volume has the Read/Write attribute, open-systems hosts can perform both read and write operations on the logical volume.

  TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, and TCE can copy data to logical volumes that have Read/Write attribute. However, if necessary, you can prevent copying data to logical volumes that have Read/Write attribute.

  The Read/Write attribute is set by default for every LU.

- **Read Only**

  If a logical volume has the Read Only attribute, open-systems hosts can perform read operations but cannot perform write operations on the logical volume.

  TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, and TCE cannot copy data to logical volumes that have Read Only attribute.

- **Protect**

  If a logical volume has the Protect attribute, open-systems hosts cannot access the logical volume. Open-systems hosts cannot perform either read nor write operations on the logical volume.

  TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, and TCE cannot copy data to and from logical volumes that have Protect attribute.

- **Report Zero Read Cap. (Mode)**

  Report Zero Read Cap. mode can be set by RAID Manager (CCI) only. When the Report Zero Read Cap. mode is set for the LU, the Read Capacity of the LU becomes zero. The host becomes unable to access the LU; it can neither read nor write data from/to it.

  TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, and TCE cannot copy data to an LU with an attribute that is Read Capacity 0. Additionally, they cannot copy data from an LU with an attribute of Read Capacity 0 to the other LUs.

- **Invisible (Mode)**

  The Invisible mode can be set by CCI only. When the Invisible mode is set for the LU, the Read Capacity of the LU becomes zero and the LU is invisible from the Inquiry command. The host becomes unable to access the LU; it can neither read nor write data from/to it. The Read Capacity of the LU becomes zero and the LU is hidden from the Inquiry command.

  TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, and TCE cannot copy data to an LU with an attribute that is in Invisible mode. Additionally, they cannot copy data from an LU with an Invisible mode attribute to the other LUs.

When the access attribute is changed to Read Only, Protect, Read Capacity 0, or Invisible from Inquiry Command, another change to Read/Write is prohibited for a certain period. In Data Retention Utility, the prohibited change period is called Retention Term. When the Retention Term of an LU is "2,190 days," the access attribute of the LU cannot be changed for 2,190 days ahead.

The Retention Term is specified when the access attribute is changed to Read Only, Protect, Read Capacity 0, or Invisible from Inquiry Command from Read/Write. The Retention Term that has been specified once can be extended, but cannot be shortened.

When the Retention Term expires, the Retention Term of the LU, with an attribute of Read Only, Protect, Red Capacity 0, or Invisible from Inquiry Command, can be changed to Read/Write. However, when the Expiration Lock is set to ON by Storage Navigator Modular, all the LU attributes, which are Read Only, Protect, Read Capacity 0, and Invisible from the Inquiry Command, are unable to be changed to Read/Write. This occurs even when the Retention Term expires. When Data Retention Utility is started for the first time, the Expiration Lock is set to OFF.

Notes:

- The lapse of time concerning the Retention Term is updated only when the subsystem is in the Ready status. Therefore, the Retention Term may become longer than the specified term when the subsystem power is turned on/off by a user.
- When a host computer attempts to write data to a Read Only logical volume, the write operation fails. The write failure is reported to the host.
- When a host computer attempts to read data from or write data to a logical volume that has the Protect attribute, the attempted access fails. The access failure is reported to the host.

1.2 Protecting Logical Volumes from Copy Operations

When TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, or TCE copies data, the data on the copy destination volume (also known as *secondary volume*) will be overwritten. If a volume containing important data is specified as a secondary volume by mistake, TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, or TCE can overwrite important data on the volume and you could suffer loss of important data. Data Retention Utility enables you to avoid such loss of data.

If you assign Read Only attribute or Protect attribute to a logical volume, TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, or TCE will be unable to copy data to that logical volume. Also, any other write operations will be prohibited on that logical volume. For example, business application software will be unable to write data to such a logical volume.

To inhibit only TrueCopy Synchronous, ShadowImage, Copy-on-Write Snapshot, and TCE from assigning the LU as a secondary volume and permit the LU to be used by other data writing, set the access attribute of the LU as Read/Write. Additionally, when "Inhibition of S-VOL Making with SMPL LU (S-VOL Disable)" is set for the primary volume of TrueCopy Synchronous, ShadowImage, ShadowImage, Copy-on-Write Snapshot, or TCE, the following copy procedures in the primary volume can be prevented:

- Takeover by TrueCopy Synchronous
- Reverse resynchronization by ShadowImage
- Restoration by Copy-on-Write Snapshot

Notes:

- The terms “S-VOL” and “secondary volume” have the same meaning in this document.
- Copy-on-Write Snapshot has two types of secondary volumes: a virtual volume (V-VOL) and an area where differential data is stored (POOL).

1.3 Data Retention Utility Requirements

Table 1.1 lists and describes the operational requirements for Data Retention Utility.

Table 1.1 Data Retention Utility Requirements

Parameter	Requirement
User interface	Hitachi Command Control Interface (CCI) and Storage Navigator Modular are necessary.
Unit of setting	The setting is made for each unit. (However the expiration Lock is set for each subsystem.)
Number of settable LUs	WMS100: 512 LUs AMS200: 512 LUs AMS500: 2,048 LUs AMS1000: 4,096 LUs
Kinds of access attributes	There are the following access attributes: ▪ Read/Write (default setting) ▪ S-VOL Disable ▪ Read Only ▪ Protect ▪ Read Capacity 0 (Can be set by CCI only) ▪ Invisible from Inquiry Command (Can be set by CCI only)
Guard against a change of an access attribute	A change from Read Only, Protect, Read Capacity 0, or invisible from Inquiry Command to Read/Write is rejected when the Retention Term does not expire or the Expiration Lock is set as ON.
LUs not supported	The following LUs are not supported: ▪ Command Device ▪ DM-LU ▪ Invalidated LU ▪ Unformatted LU ▪ LU set as a POOL of Copy-on-Write Snapshot or TCE.
Relation with TrueCopy Synchronous, ShadowImage, and Copy-on-Write Snapshot/TCE	When the S-VOL Disable is set for an LU, a pair formation using the LU as an S-VOL (POOL) is suppressed. ▪ A setting of the S-VOL Disable for a volume that has already become an S-VOL (V-VOL or POOL) is not suppressed only when the pair status is PSUS. Besides, when the S-VOL Disable is set for a P-VOL, restoration of Copy-on-Write Snapshot and reverse resynchronization of ShadowImage is suppressed but a swapping of TrueCopy Synchronous is not suppressed.
Powering off/on	An access attribute that has been set is retained even when the power is turned off/on.
Controller detachment	An access attribute that has been set is retained even when a controller detachment occurs.
Relation with drive restoration	A correction copy, dynamic sparing, and copy back are performed like a usual LU.
LU detachment	An access attribute that has been set for an LU is retained even when the LU is detached.
Restriction of microprogram replacement	When an LU whose access attribute is other than Read/Write and S-VOL Disable exists, an initial setting up and initialization of settings (Configuration Clear) are suppressed.

Parameter	Requirement
Restriction of access attribute setting	The following operations for an LU whose access attribute is other than Read/Write and for a RAID group that includes the LU are suppressed: ▪ LU elimination ▪ LU formatting ▪ RAID group elimination
Setting by Storage Navigator Modular	When Storage Navigator Modular sets an access attribute, it can only be set for one LU at a time.
LUN Expansion	A unified LU whose access level is other than Read/Write can neither be composed nor dissolved.
Cache Residency Manager	An LU for which an access attribute has been set can be used for Cache Residency Manager. On the other hand, an access attribute can be set for an LU being used for the Cache Residency Manager.
Concurrent use of LUN Manager	Available
Concurrent use of Volume Migration	Available The LU which executed the migration carries over the access attribute and the retention term set by Data Retention Utility to the LU of the migration destination of the data and releases the access attribute and the retention term of migration resource (see ***Note*** below). When the access attribute is other than Read/Write, the LU cannot be specified as an S-VOL of Volume Migration.
Concurrent use of Password Protection	Available
Concurrent use of SNMP Agent	Available
Concurrent use of Cache Partition Manager	Available
Setting range of Retention Term	From the 0th to 21,900 days (60 years) or unlimited.

Note: The status where the migration is executed for an LU which set the Read Only attribute is shown in Figure 1.1. When the migration of the LU0 which set the attribute of Read Only to the LU1 in the RAID group 1 is executed, the Read Only attribute is carried over to the LU of the migration destination of the data. Therefore, the LU0 is in the status that the Read Only attribute is set irrespective of the execution of the migration. The Read Only attributes not copied to the LU1. When the migration pair is released and the LU1 is deleted from the reserved LU, a host can Read/Write to the LU1.

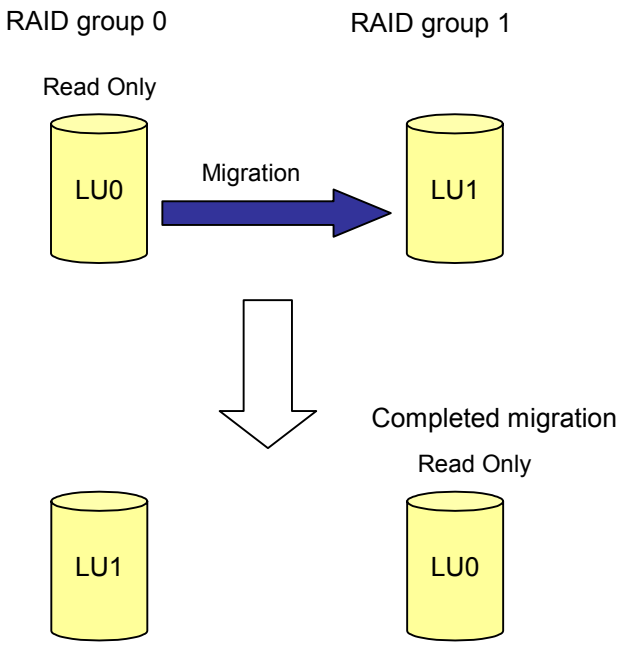


Figure 1.1 Volume Migration of Read Only Attribute

1.4 Notes on the Use of Data Retention Utility

1.4.1 Notes on Usage

- The access attribute for an LU should not be modified while an operation is performed on the data residing on the LU. The operation may terminate abnormally.
- Logical volume for which the access attribute cannot be changed.

  Data Retention Utility does not enable you to change the access attributes of the following logical volumes:

  - An LU assigned to Command Device.
  - An LU assigned to DM-LU.
  - An uninstalled LU.
  - A hidden LU.
- Note on LUN Expansion:

  You cannot combine logical volumes that do not have a Read/Write attribute. Unification of a unified LU, whose access attribute is not Read/Write, cannot be dissolved.
- Note on Copy-on-Write Snapshot/TCE:

  An LU whose access attribute is not Read/Write cannot be assigned to a POOL. Additionally, an access attribute other than Read/Write cannot be set for an LU that has been assigned to a POOL.
- Notes on SYNCHRONIZE CACHE Command:
  - When a SYNCHRONIZE CACHE command is received from a host, it usually writes the entire write pending data stored in the cache memory to drives. However, in case that Data Retention Utility is installed, the write pending data is not written to drives on the SYNCHRONIZE CACHE command.
  - When you need to write the entire write pending data stored in the cache memory to drives on the SYNCHRONIZE CACHE command in case that Data Retention Utility is installed, it is required to turn on the Synchronize Cache Execution Mode through Storage Navigator Modular.

Note: When Data Retention Utility is used cooperating with the application of the host, it is required to be sure to turn off the Synchronize Cache Execution Mode. If Synchronize Cache Execution Mode is turned on, the application of the host may fail.

- Host side application example:
  - There is IXOS-eCONserver.

1.4.2 Notes and Limitations for Each Operating System

- Using an LU whose access attributes have been set from the OS:
  - When access attributes are set from the OS, they must be set before mounting the LU. If access attributes are set to the LU after it is mounted, the system may not operate properly.
  - When a command (create partition, format, etc.) is issued to an LU with access attributes, from the operating system, it will appear as if the command ended normally. However, although the information is written to the host cache memory, the new information is not reflected onto the LU.
  - An OS may not recognize an LU when the LUN is larger than the one on which the Invisible mode was set.
- Using Windows NT®/ Windows® 2000:
  - An LU with a Read Only access attribute cannot be mounted.
- Using Windows® Server ™ 2003:
  - When mounting an LU with a Read Only attribute, do not use the diskpart command to mount and unmount a volume. Use the -x mount and -x unmount commands of CCI.
- Using Windows NT®/ Windows® 2000/Windows Server™ 2003:
  - When setting a volume used by Windows NT® Windows® /2000/Windows Server™ 2003 as Data Retention Utility LU, Data Retention Utility can be applied to a basic disk only. When Data Retention Utility is applied to a dynamic disk, an LU is not correctly recognized.
- Using an UNIX® OS:
  - When mounting an LU with a Read Only attribute, mount it as Read Only (using the mount –r command).
- Using HP-UX:
  - If there is an LU with a Read Only attribute, host shutdown may not be possible. When shutting down the host, change the attribute of LU from Read Only to Protect in advance.
  - If there is an LU with Protect attribute, host startup time may be lengthy. When starting the host, either change the attribute of LU from Protect to Read Only, or make the LU unrecognizable from the host by using mapping functions.
  - If a write is completed on the LU with a Read Only attribute, this may result in no response; therefore, do not perform write commands (e.g. dd command).
  - If Read/Write is done on an LU with a Protect attribute, this may result in no response; therefore, do not perform read or write commands (e.g. dd command).

- Using LVM:
  - When changing the configuration of the LVM, including Data Retention LU, the specified LU must be temporarily inhibited by the **raidvchkset -vg** command. Place the LU again in the status in which it is checked when the LVM configuration change is completed.
- Using HA Cluster Software:
  - There may be a case where an LU to which Data Retention is applied cannot be used as a resource of the HA cluster software (such as the MSCS). This is because the HA cluster software (such as the MSCS) writes management information in the management area periodically in order to check propriety of the resource.

Chapter 2 Preparing for Data Retention Utility Operations

This chapter outlines and describes the following:

- 2.1 Installing
- 2.2 Uninstalling
- 2.3 Enabling or Disabling
- 2.4 Setting the Command Device
- 2.5 Defining the Configuration Definition File
- 2.6 Setting the Environment Variable

When installing, uninstalling, or enabling Data Retention Utility:

- The Data Retention Utility feature is usually not selectable (locked); to make it available, you must install the Data Retention Utility feature and make its functions selectable (unlocked). **To install this function, the key code or key file provided with the optional feature is required.** Use the following instructions to install the Data Retention Utility feature. Data Retention Utility is installed and uninstalled using the Storage Navigator Modular program.
- Installing, uninstalling, enabling, and disabling of the Data Retention Utility feature are set for each disk array subsystem.
- Before installing and uninstalling, verify that the array unit is in normal operating condition. If a failure such as a controller blockade has occurred, installation and uninstallation operations cannot be performed.

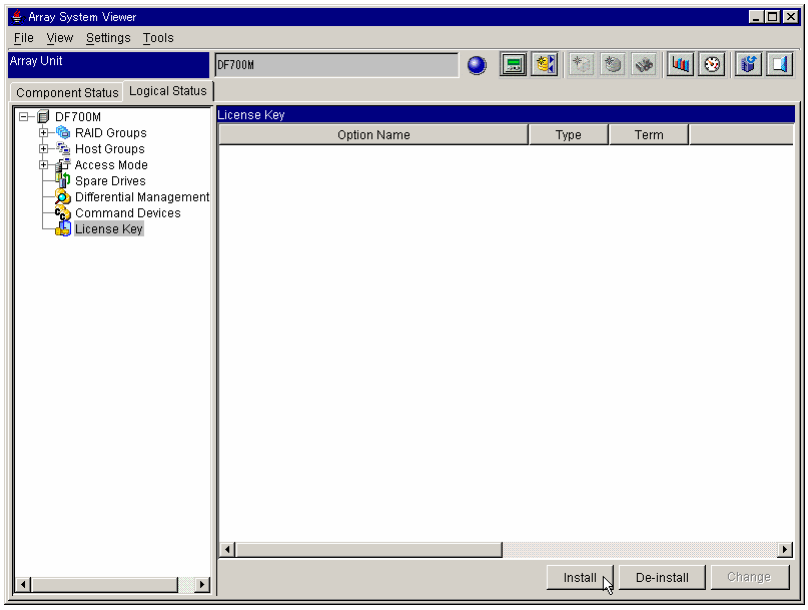
2.1 Installing

To install the Data Retention Utility feature using the GUI version of the Storage Navigator Modular program:

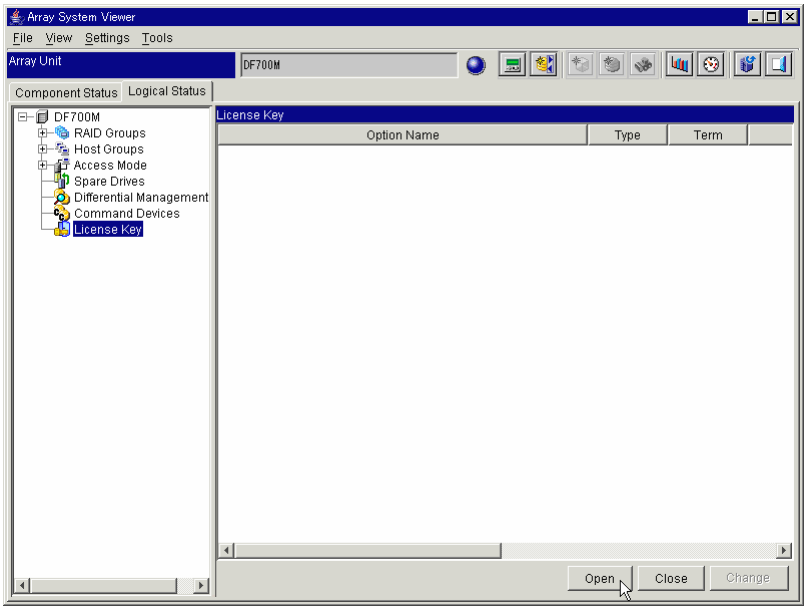
Note: For additional installation information, refer to the *Hitachi TagmaStore™ Adaptable Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide*, MK-95DF711.

1. Start the Storage Navigator Modular program and change the operation mode to **Management Mode** (administrator mode).
2. Register the subsystem (array unit) in which you will install the Data Retention Utility feature. **Connect to the subsystem**.

   The Array System Viewer panel displays with the connected subsystem.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon.



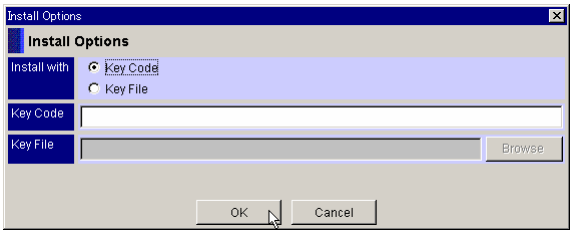
Storage Navigator version 5.0 or later



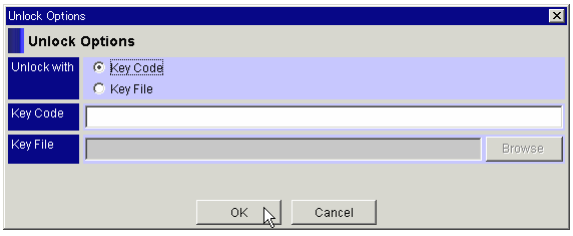
Storage Navigator versions earlier than 5.0

5. Click **Install**. The **Install Options** dialog box is displays: (Storage Navigator version 5.0 or later)

   Click **Open**. The **Unlock Options** dialog box displays: (Storage Navigator versions earlier than 5.0)

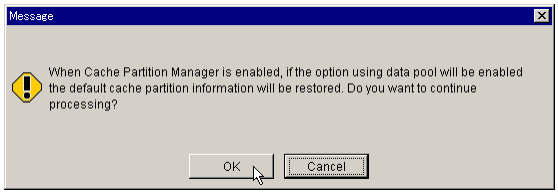


Storage Navigator version 5.0 or later

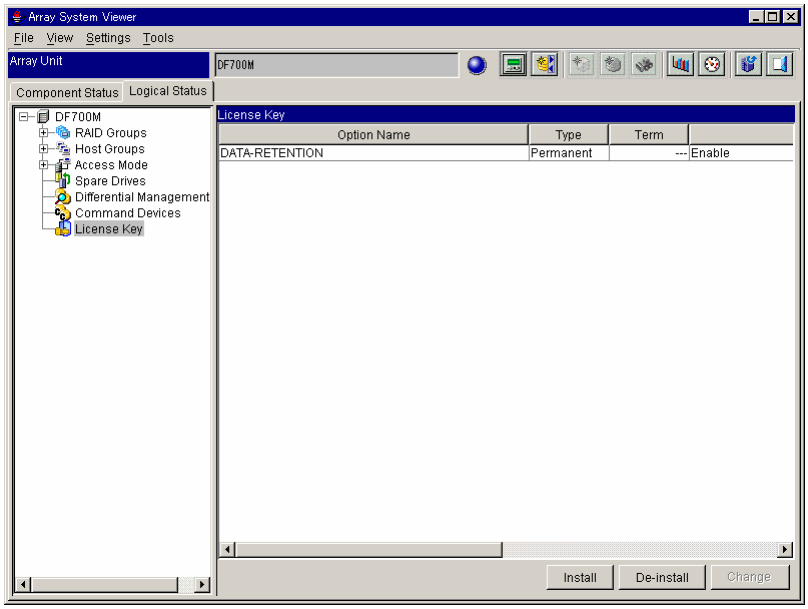


Storage Navigator versions earlier than 5.0

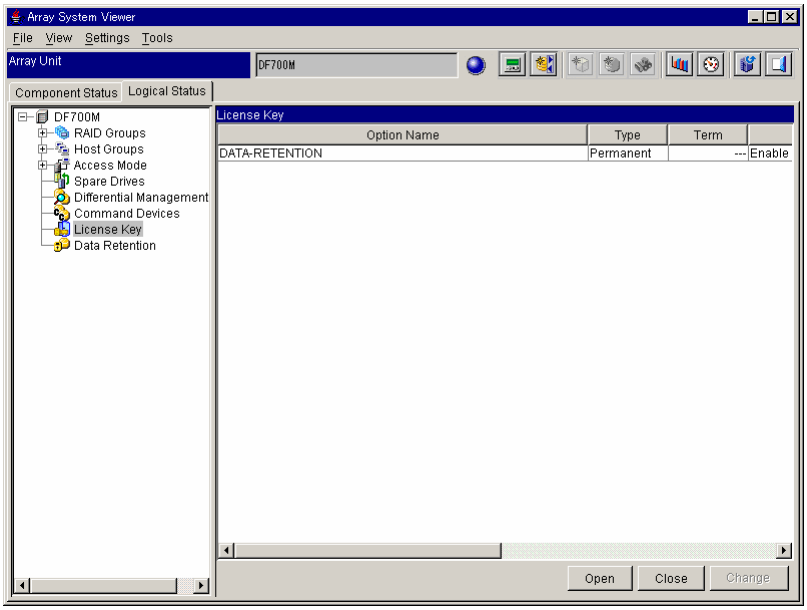
6. Choose an install option:
   - Key Code: Select the Key Code option. In the Key Code field, enter the key code and click **OK**.
   - Key File: Select the Key File option. In the Key File field, enter the path to the key file (or click **Browse** to find the file) and click **OK**. In the **Install/Unlock Options** box that appears, select Data Retention Utility and click **OK**.
7. In any confirmation screens that displays, click **OK** or **Close** to continue.
8. When Navigator version is 3.00 or later and Cache Partition Manager is enabled, the following message is displayed. Since Data Retention Utility does not use the data pool, click the **OK** button at this point without doing anything else.



9. A message box displays requesting confirmation to install Data Retention Utility. Click **OK**.
10. The Array System View panel displays with **DATA-RETENTION** as the Option name and status as **Enable**.



Storage Navigator version 5.0 or later



Storage Navigator versions earlier than 5.0

The Data Retention Utility feature is now installed.

2.2 Uninstalling

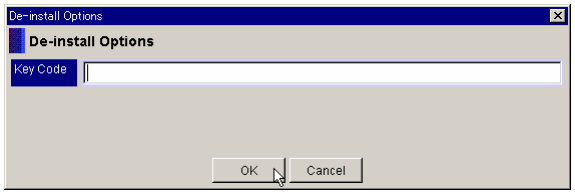
Follow the instructions below to uninstall the Data Retention Utility feature. When it is uninstalled, the Data Retention Utility feature is not available (locked) until it is installed by the key code.

Note: When disabling or uninstalling Data Retention Utility, return the LU attributes that have been set to the initial setting (Read/Write).

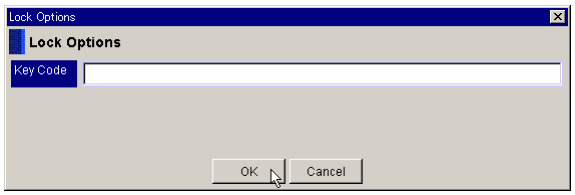
Follow the instructions below to uninstall Data Retention Utility:

1. Start Storage Navigator Modular and change the operation mode to **Management Mode** (administrator mode).
2. Register the subsystem (array unit) in which you will uninstall the Data Retention Utility feature. **Connect to the subsystem**.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon.
5. Click **De-install**. The **De-install Options** dialog box displays: (Storage Navigator version 5.0 or later)

   Click **Close**. The **Lock Options** dialog box displays: (Storage Navigator versions earlier than 5.0)



Storage Navigator version 5.0 or later



Storage Navigator versions earlier than 5.0

6. Enter a key code in the text box, and then click **OK**.
7. A message box displays requesting confirmation to uninstall Data Retention Utility. Click **OK**.

The Data Retention Utility feature is now uninstalled.

2.3 Enabling or Disabling

The Data Retention Utility feature can be set to enable or disable when it is installed.

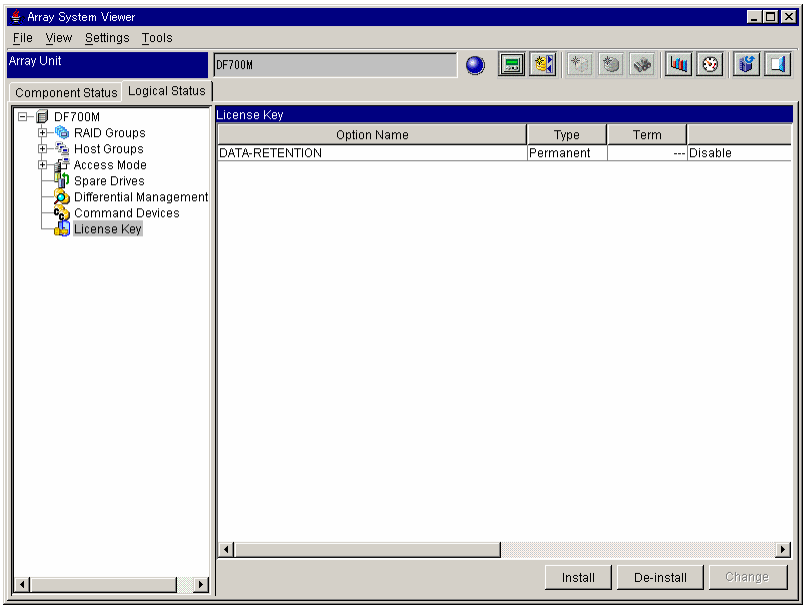
Note: When disabling or uninstalling Data Retention Utility feature, return the LU attributes that have been set to the initial setting (Read/Write).

Follow the instructions below to enable/disable Data Retention Utility:

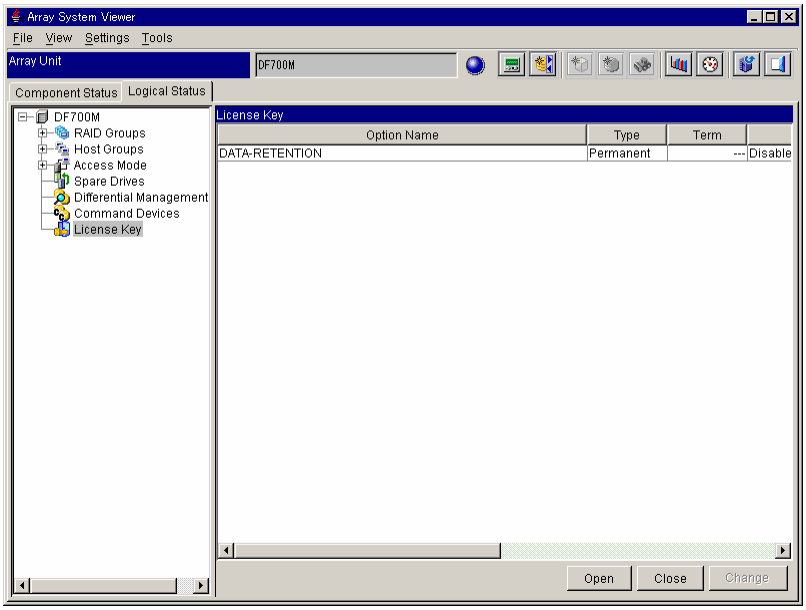
1. Start Storage Navigator Modular and change the operation mode to **Management Mode** (administrator mode).
2. Register the subsystem (array unit) in which you will change the status of the Data Retention Utility feature. **Connect to the subsystem**.

   The Array System Viewer panel displays with the connected subsystem.
3. On the Parameter panel, select the **Options** tab.
4. Click the **Logical Status** tab.
5. Click the **License Key** icon.
6. From the **Option Name**, select **DATA-RETENTION** and then click **Change**.
7. A message box displays confirming that you want to change the status (enable or disable). Click **OK**.

Figure 2.1 shows the Array System View panel with the status of the Data Retention Utility changed (enabled/disabled).



Storage Navigator version 5.0 or later



Storage Navigator versions earlier than 5.0

Figure 2.1 Showing Enable/Disable Status

2.4 Setting the Command Device

Note: When operation is not performed through CCI, no setting of the command device is required.

The Command Device is a user-selected, dedicated logical volume on the subsystem which functions as the interface to the CCI software. The Data Retention Utility commands are issued by the CCI (HORCM) to the subsystem through the Command Device.

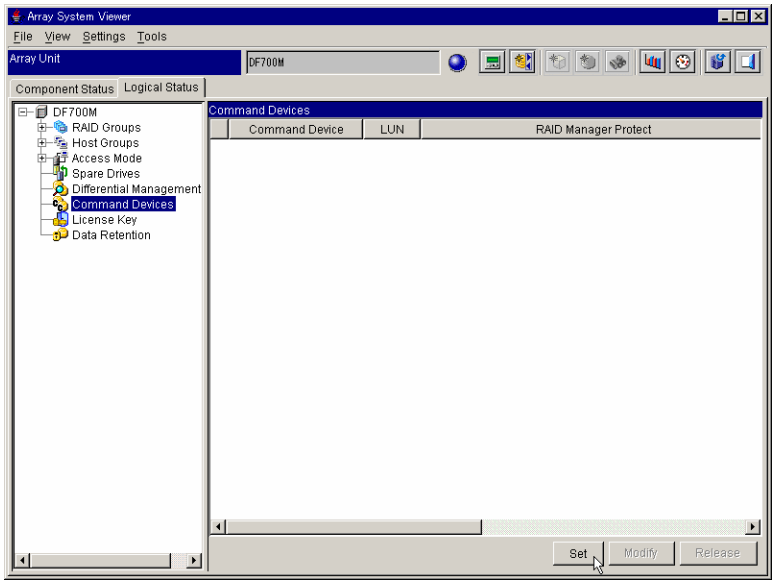
To accept read and write commands that are executed by the subsystem and return read requests to the UNIX®/PC host, the Command Device must be set. The Command Device must be defined in the HORCM_CMD section of the configuration definition file for the CCI instance on the attached host. Two Command Devices can be set for the subsystem. You can set Command Devices using the Storage Navigator Modular.

Notes:

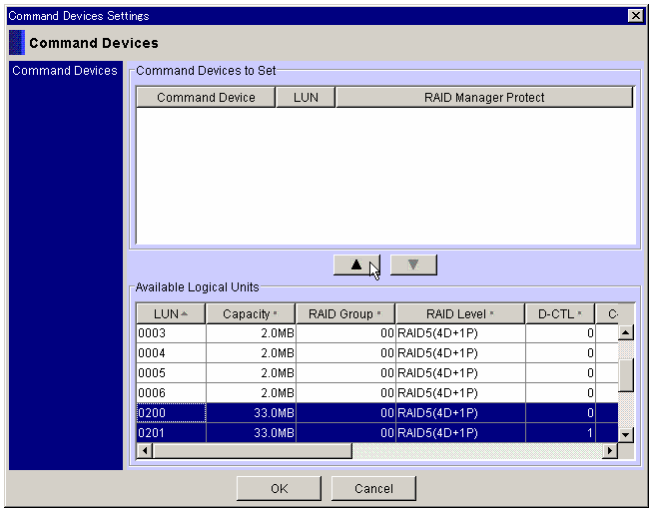
- LUs set for Command Devices must be recognized by the host. The command device LU size must be greater than or equal to 33 MB.
- The following restrictions apply when either pair of ShadowImage, SnapShot or TrueCopy exists or the path of True Copy is defined:
  - When two command devices are set, only one command device can be released.
  - When only one command device is set, the command device cannot be released.

To set command device(s):

1. Start Storage Navigator Modular, and change the operation mode to **Management Mode** (administrator mode).
2. **Connect to the subsystem**. The Array System Viewer panel opens displaying the connected subsystem.
3. Click the **Logical Status** tab.
4. Click the **Command Devices** icon:

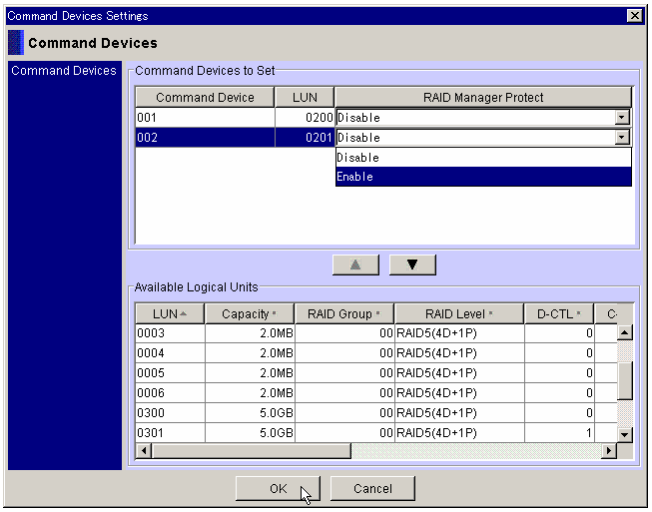


5. Click **Set**. The **Command Devices Settings** dialog box displays:



6. In **Available Logical Units** list, select the **LUN** for setting the command devices, and then click the ▲ button.

   The selected **LUN** moves to the **Command Devices to Set** list:

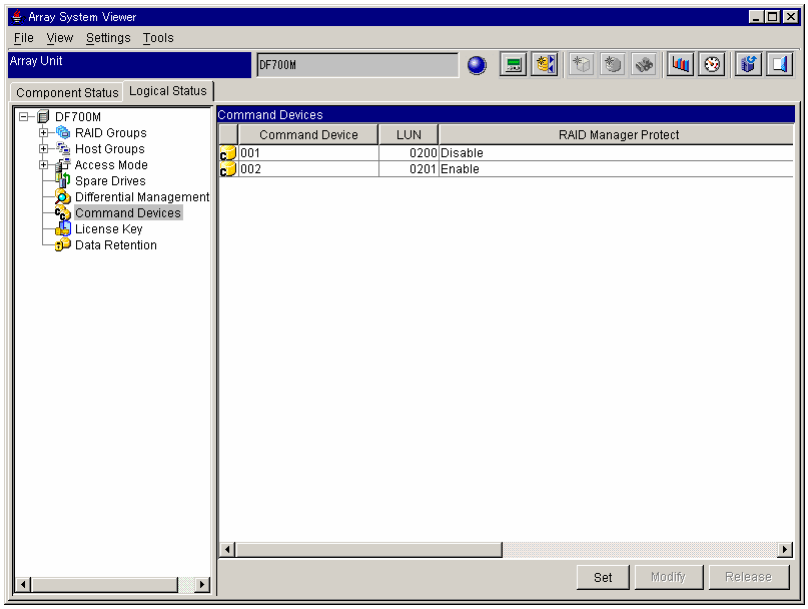


7. When you want to use the RAID Manager Protect function, select **Disable** or **Enable** from the **RAID Manager Protect** drop-down list.

   When you want to change the already set command devices, select the **LUN** on the **Command Devices to Set** list, and then click the ▼ button.

   The selected **LUN** moved to the **Available Logical Units** list.

8. Click **OK**. The setting information displays:



Note: To use the alternate Command Device function, designate two Command Devices. For details on the alternate Command Device function, refer to the *Hitachi TagmaStore™ Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide* MK-95DF701.

9. **To release an already set command device**, select the LUN of the command device you want to release, and then click **Release**.
10. Click **OK**.
11. A confirmation message box displays. Click **OK** to continue.

    The setting information displays.

Setting the command device is now complete.

2.5 Defining the Configuration Definition File

Note: When operation is not performed through CCI, no setting of configuration definition file is required.

The configuration definition file describes the system configuration necessary to make CCI operational. The configuration definition file is a text file created and/or edited using any standard text editor, and can be defined from the PC where the CCI software is installed. This sample configuration definition file (HORCM_CONF) is included with the CCI software, and this file should be used as the basis for creating your configuration definition file(s). The system administrator should copy the sample file, set the necessary parameters in the copied file, and place the copied file in the proper directory. For details on the configuration definition file, refer to the *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.

The configuration definition file can be automatically created using the **mkconf** command tool. However, the parameters such as poll (10ms) must be set manually (see step 4 below). For details on the mkconf command tool, refer to the *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.

The following steps describe an example for manually defining the configuration definition file:

1. On the host where CCI is installed, verify that the CCI is not running. If the CCI software is still running, shut down the CCI software using the **horcmshutdown** command. For details on horcmshutdown, refer to the *Hitachi TagmaStore Adaptable Modular Storage: Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.
2. In the command prompt, make a copy of the sample file (horcm.conf).

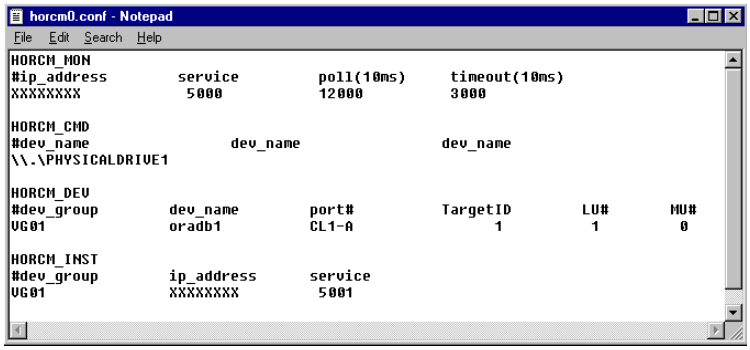
   Example:

   ```
   c:\HORCM\etc> copy \HORCM\etc\horcm.conf \WINNT\horcm0.conf
   ```

3. Open `horcm0.conf` using the text editor.
4. In the **HORCM_MON** section, set the necessary parameters.

   Note: A value more than or equal to 6000 must be set for poll (10ms). For details on calculating the poll(10ms) value, please refer to *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701, Specifying the value incorrectly may cause a conflict in the internal process, which suspends the process temporary and stops the internal process of the subsystem. For more details on configuration parameters, refer to *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.

5. In the **HORCM_CMD** section, specify the physical drive (Command Device) on the subsystem:



6. Save the configuration definition file and use the **horcmstart** command to start the CCI software. For details on horcmstart, refer to the *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.
7. Execute the **raidscan** command, and make sure you write down the target ID displayed in the execution result. For details on the raidscan command, refer to the *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.
8. Shut down the CCI software and then open the configuration definition file again.
9. In the **HORCM_DEV** section, set the necessary parameters. For the target ID, set the ID of the raidscan result you wrote down. Also, the item MU# must be added after the LU#, and the value must be set as 0 (zero).
10. In the **HORCM_DEV** section, set the necessary parameters, and then save (overwrite) the file.
11. Repeat steps 4 to 10 for the `horcm1.conf` file.
12. Enter the following in the command prompt to verify the connection between CCI and the subsystem.

    Example:

```
C:\>cd horcm\etc

C:\horm\etc>echo hd1-3 | .\inqraid
Harddisk 1 -> [ST] CL1-A Ser =75000174 LDEV =   0 [HITACHI  ] [DF600F-CM       ]
Harddisk 2 -> [ST] CL1-A Ser =75000174 LDEV =   1 [HITACHI  ] [DF600F          ]
              HORC = SMPL  HOMRCF[MU#0 = SMPL  MU#1 = NONE  MU#2 = NONE]
              RAID5[Group 1-0] SSID = 0x0000
Harddisk 3 -> [ST] CL1-A Ser =75000174 LDEV =   2 [HITACHI  ] [DF600F          ]
              HORC = SMPL  HOMRCF[MU#0 = SMPL  MU#1 = NONE  MU#2 = NONE]
              RAID5[Group 2-0] SSID = 0x0000

C:\horm\etc>
```

For details on the configuration definition file, refer to the *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.

2.6 Setting the Environment Variable

To perform Data Retention Utility operations, you must set the environment variable for the execution environment.

1. Set the environment variable for each instance. Enter the following from the command prompt.

   Example:

```
C:\HORCM\etc>set HORCMINST=0
```

2. Set the environment variable shown below.

   Example:

```
C:\HORCM\etc>set HORCC_MRCF=1
```

3. Execute the horcmstart script, and then execute the **raidvchkdsp** command to verify the configuration.

   Example:

```
C:\HORCM\etc>horcmstart 0
starting HORCM inst 0
HORCM inst 0 starts successfully.

C:\HORCM\etc>raidvchkdsp -g vg01 -fd -v gflag
Group  PairVol  Device_File      Seq# LDEV# GI-C-R-W-S  PI-C-R-W-S  R-Time
vg01   oradb1   Harddisk2       75000174     1  E E E E E   E E E E E       0
```

Preparing for Data Retention Utility operation is now complete.

Chapter 3 Performing Data Retention Utility Operations (CCI)

This chapter outlines and describes the following:

- 3.1 Setting an Attribute
- 3.2 Changing the Retention Term

This chapter also illustrates using the command-line interface on Windows® 2000 systems.

3.1 Setting an Attribute

The attributes that can be set are the Read Only, Protect, Report Zero Read Cap., Invisible, and Inhibition of S-VOL Making with SMPL LU.

The following is an example of an attribute that is changed from one that enables a Read/Write (default attributes) to one that prohibits Read/Write Inhibition (Protect). The Retention Term is set as one year (365 days).

1. ***For example***, if the group name in the configuration definition file is VG01, follow these steps:

```
C:\HORCM\etc\raidvchkset -g VG01 -d oradb1 -vg rwd svd 365
```

Figure 3.1 Raidvchkset Command Example

2. Execute the raidvchkdsp command to verify the setting attribute.

```
C:\HORCM\etc\raidvchkdsp -g VG01 -fd -v gflag
Group  PairVol  Device_File      Seq# LDEV# GI-C-R-W-S  PI-C-R-W-S  R-Time
VG01   oradb1   Unknown         75000067     3  E E D D D   E E E D D     365
VG01   oradb2   Unknown         75000067     4  E E E E E   E E E E E       -
```

Figure 3.2 Raidvchkdsp Command Example

The attribute type is changed. For details on the **raidvchkset** and **raidvchkdsp** commands and their options, refer to the *Hitachi TagmaStore Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide,* MK-95DF701.

To return the attribute to its initial state (Read/Write), execute the raidvchkset command without specifying anything for the -vg option of the raidvchkset command. However, this operation is in error when the Retention Term does not expire or the Expiration Lock has been turned on.

Example:

```
C:\HORCM\etc\raidvchkset -g VG01 -d oradb1 -vg
```

Other attributes and mode options include the following:

- inv: The object volume is hidden from the Inquiry command.
- sz0: The object volume returns the size zero in reply to the Read Capacity command.
- rwd: Read/Write inhibition.
- wtd: Write inhibition (Read only).
- svd: The object volume is inhibited to assign the SMPL status to an S-VOL (S-VOL Disable).

Note: When the access attribute of the LU is set as inv, sz0, rwd, or wtd, it must be set together with svd.

3.2 Changing the Retention Term

The following example is of a Retention Term that is extended from one year (365 days) to two years (730 days).

Note: Data Retention Utility cannot shorten the Retention Term.

1. Name the group and volume in the configuration definition file VG01 and oradb1 respectively for the LU to which the Retention Term is to be extended. View its current attribute and Retention Term by executing the raidvchkdsp command.

```
C:\HORCM\etc\raidvchkdsp -g VG01 -d oradb1 -fd -v gflag
Group  PairVol  Device_File      Seq# LDEV# GI-C-R-W-S  PI-C-R-W-S  R-Time
VG01   oradb1   Unknown         75000067     1  E E D D D   E E E D D     365
```

Figure 3.3 Raidvchkset Command Example

2. Execute the raidvchkdsp command by specifying the same attribute as the current one and the Retention Term to be changed. If a Retention Term shorter than the current one is specified, that specification is erroneous.

```
C:\HORCM\etc\raidvchkset -g VG01 -d oradb1 -vg rwd svd 730
```

Figure 3.4 Raidvchkset Command Example

3. Verify the attribute and Retention Term that have been set by executing the **raidvcchkdsp** command.

```
C:\HORCM\etc\raidvchkdsp -g VG01 -d oradb1 -fd -v gflag
Group  PairVol  Device_File      Seq# LDEV#  GI-C-R-W-S  PI-C-R-W-S  R-Time
VG01   oradb1   Unknown         75000067     1  E E D D D   E E E D D     730
```

Figure 3.5 Raidvchkdsp Command Example

Note: Expiration Lock status is shown as the retention time plus 1000000. "R-Time + 1000000" shows the retention time with Expiration Lock status.

Chapter 4 Performing Data Retention Utility Operations (GUI)

This chapter outlines and describes the following:

- 4.1 Setting an Attribute
- 4.2 Setting a S-VOL
- 4.3 Changing the Retention Term
- 4.4 Setting the Expiration Lock

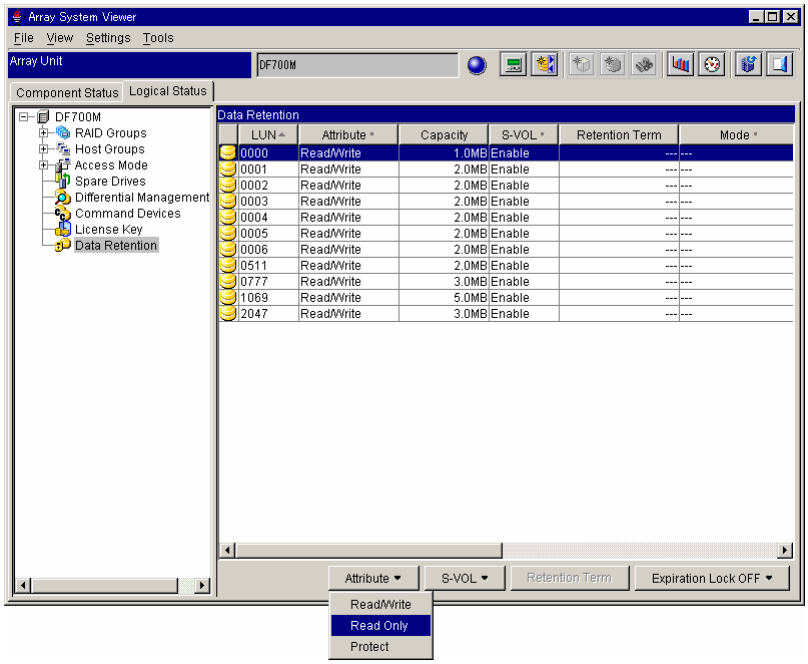
Also described in this chapter are operations using the graphical user interface (GUI).

4.1 Setting an Attribute

To set an attribute:

1. Start the Storage Navigator Modular program and change the operation mode to **Management Mode** (administrator mode).
2. Register the subsystem (array unit) in which you will set the attribute of the Data Retention Utility feature. **Connect to the subsystem**.

   The Array System Viewer panel appears; it displays the connected subsystem.
3. Select the **Logical Status** tab.
4. Select the **LDEV Guard** icon:

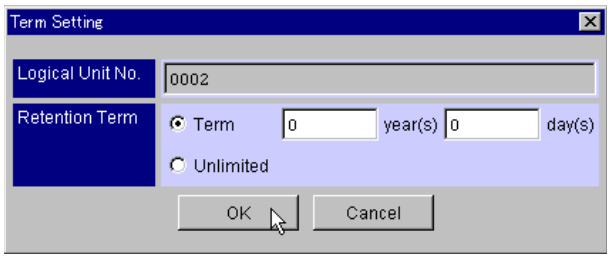


- **LUN:** LU number is displayed.
- **Attribute:** Attribute (Read/Write, Read Only, Protect, or Can't Guard) is displayed.
- **Capacity:** Capacity of the LU is displayed.
- **S-VOL:** Whether the LU can be set to S-VOL (Enable) or is inhibited from being set to S-VOL (Disable) is displayed.
- **Mode:** Mode (Read Capacity 0 (Zero), hiding from Inquiry Command Mode (Zer/Inv), or un-specifying (---)) is displayed. (For reference only.)
- **Retention:** The length of time for retention (Unlimited or ---) is displayed.

Note: When Read only or Protect is set as the attribute, S-VOL will be disabled.

5. Select the **LUN** from the **Attribute** drop-down list, or select **Read Only** or **Protect**. Alternately, select the **LUN** from a drop-down menu by right-clicking the selected LUN's icon. From the drop-down menu, select **Attribute → Read Only** or **Protect**.
6. The Term Setting dialog box displays. Select **Term** or **Unlimited** from **Retention Term**.

   If you select **Term**, set a Retention Term in years (0 to 60) and days (0 to 21,900). A term of six years has been entered in default.
7. On the Term Setting dialog box, Click **OK**.

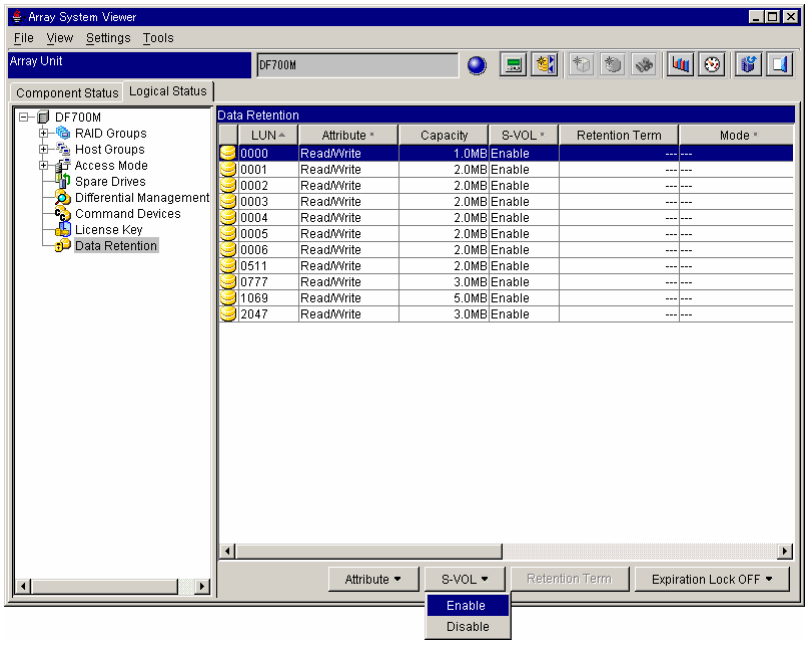


8. The confirmation message displays. Click **OK** three times.

4.2 Setting a S-VOL

To set a S-VOL:

1. Select the **LUN**.
2. From the drop-down list of the **S-VOL** button, select **Disable**:



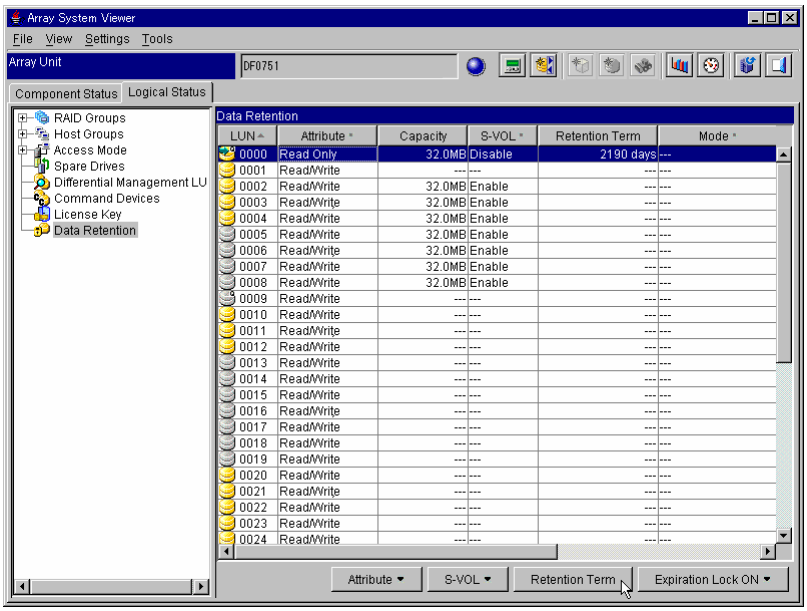
3. Click **OK** to continue through the confirmation messages that display.

4.3 Changing the Retention Term

Note: Data Retention Utility cannot shorten the Retention Term.

To change the retention term:

1. Select the **LUN**, and then click **Retention Term**:



2. The Term Setting dialog box displays. Select **Term** or **Unlimited** from **Retention Term**.

   If you select Term, set a Retention Term in years (0 to 60) and days (0 to 21,900). A term of six years has been entered in default.

3. Click **OK**.

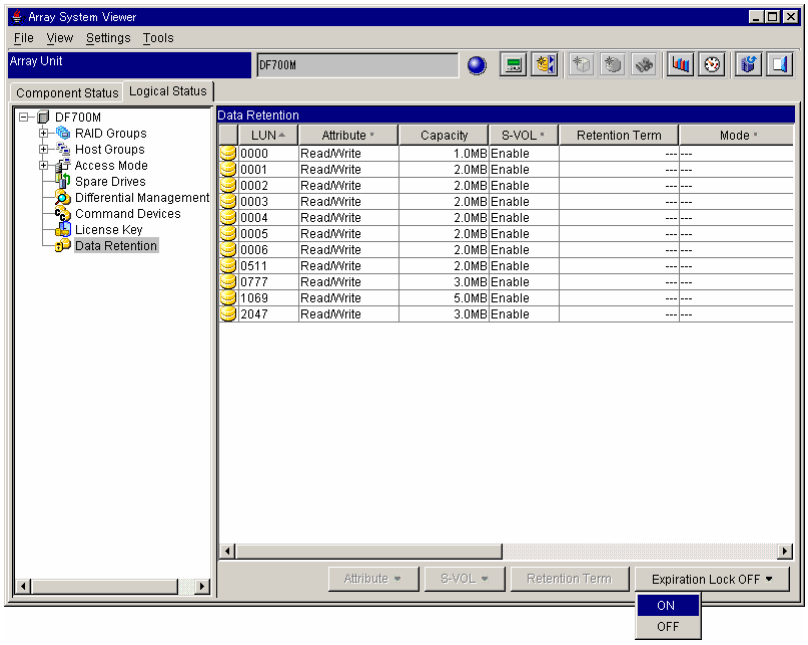
4. The confirmation message displays. Click **OK** two times.

   The term setting is updated and the window displays.

4.4 Setting the Expiration Lock

To set the expiration lock:

1. Select the **Data Retention** icon.
2. From the drop-down list of the **Expiration Lock ON** button, select **ON**:



3. One or more confirmation messages display. Click **OK** as needed to confirm.

Appendix A Operations Using CLI

This Appendix includes the following:

- A.1 Installing Data Retention Utility
- A.2 Uninstalling Data Retention Utility
- A.3 Enabling or Disabling Data Retention Utility
- A.4 Setting the Command Device
- A.5 Setting an Attribute
- A.6 Setting an S-VOL
- A.7 Changing the Retention Term
- A.8 Setting the Expiration Lock

For details on Storage Navigator Modular, refer to the *Hitachi TagmaStore™ Adaptable Modular Storage, Storage Navigator Modular Command Line Interface (CLI) User's Guide*, MK-95DF712.

A.1 Installing Data Retention Utility

The Data Retention Utility option is usually not selectable (locked). To make this option available, you must install Data Retention Utility and make its functions selectable (unlocked). To install this function, use the key code or key file provided with the optional feature.

Data Retention Utility is installed and uninstalled through the Storage Navigator Modular program (CLI).

To install this function, the key code or key file provided with this optional feature is required.

Note: Before installing/uninstalling Data Retention Utility, verify that the array unit to be operated is functioning normally. If a failure such as a controller blockage has occurred, installation/uninstallation cannot be performed.

To install Data Retention Utility using the CLI version of Storage Navigator Modular:

1. From the command prompt, register the subsystem (array unit) in which the Data Retention Utility feature is to be installed. Connect to the subsystem.
2. Install the optional features by executing the **auopt** command as follows:

   Example:

   Navigator version is 5.00 or later and Cache Partition Manager is enabled

```
% auopt -unit subsystem-name -lock off -keycode Key code
Password: manager-password
Are you sure you want to install the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is installed successfully.
%
```

   Navigator version earlier than 5.00 and Cache Partition Manager is enabled

```
% auopt -unit subsystem-name -lock off -keycode Key code
Password: manager-password
Are you sure you want to unlock the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is unlocked.
%
```

   Navigator version earlier than 3.00 and Cache Partition Manager is enabled

```
% auopt -unit subsystem-name -lock off -keycode Key code
Password: manager-password
Are you sure you want to unlock the option? (y/n [n]): y
The option is unlocked.
%
```

Example:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name      Type      Term    Status
DATA-RETENTION   Permanent  ---    Enable
%
```

A.2 Uninstalling Data Retention Utility

When the Data Retention Utility feature is uninstalled, the Data Retention Utility feature is not available (locked) until it is installed by the key code or key file.

Note: When disabling or uninstalling this Data Retention Utility feature, LU attributes that have been set must be returned to the initial attribute (Read/Write).

To uninstall Data Retention Utility, use the key code provided with the optional feature.

Data Retention Utility is installed and uninstalled through the Storage Navigator Modular program.

To uninstall Data Retention Utility using the CLI version of the Storage Navigator Modular program:

1. From the command prompt, register the subsystem (array unit) in which Data Retention Utility is to be uninstalled, then connect to the subsystem.
2. Uninstall the optional features by executing the **auopt** command as follows:

   Example:

   Storage Navigator version 5.0 or later

```
% auopt -unit subsystem-name -lock on -keycode Key code
Password: manager-password
Are you sure you want to de-install the option? (y/n [n]): y
The option is de-installed successfully.
%
```

   Storage Navigator versions earlier than 5.0

```
% auopt -unit subsystem-name -lock on -keycode Key code
Password: manager-password
Are you sure you want to lock the option? (y/n [n]): y
The option is locked.
%
```

   Example:

```
% auopt -unit subsystem-name -refer
Password: manager-password
DMEC002015:No information displayed.
%
```

A.3 Enabling or Disabling Data Retention Utility

Data Retention Utility can be set to enable or disable after installation. This allows Data Retention Utility to be activated or deactivated without the necessity of using the key code or key file.

Note: When disabling or uninstalling this Data Retention Utility feature, LU attributes that have been set must be returned to the initial attribute (Read/Write).

To enable/disable Data Retention Utility using the CLI version of the Storage Navigator Modular program**:**

1. From the command prompt, register the subsystem (array unit) in which the status of the Data Retention Utility is to be changed, then connect to the subsystem.
2. Execute the auopt command to change the status (enable or disable) of the Data Retention Utility feature.

The following is an example of how to change the status from enable to disable. To change the status from disable to enable, enter **enable** after the **-st** option.

Example:

```
% auopt -unit subsystem-name -option DATA-RETENTION -st disable
Password: manager-password
Are you sure you want to disable the option? (y/n [n]): y
The option has been set successfully.
%
```

Example:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name  Type      Term    Status
DATA-RETENTION       Permanent  ---    Enable
%
```

A.4 Setting the Command Device

Note: When operation is not performed through CCI, no setting of the command device is required.

The Command Device is a user-selected, dedicated logical volume on the disk subsystem that functions as the interface to the CCI software. The Data Retention Utility commands are issued by the CCI (HORCM) to the disk subsystem Command Device.

In order to accept read and write commands that are executed by the disk subsystem and return read requests to the UNIX/PC host, the Command Device must be designated. The Command Device must be defined in the HORCM_CMD section of the configuration definition file for the CCI instance on the attached host. Two Command Devices can be designated for the disk subsystem. You can designate Command Devices using the Storage Navigator Modular.

Notes:

- LUs set for Command Devices must be recognized by the host. The command device LU size must be greater than or equal to 33 MB.
- The following restrictions apply when either pair of ShadowImage, SnapShot or TrueCopy, or TCE exists or the path of True Copy , or TCE is defined:
  - When two command devices are set, only one command device can be released.
  - When only one command device is set, the command device cannot be released.

To designate Command Device(s):

1. From the command prompt, register the subsystem (array unit) to which you want to create the Command Device. **Connect to the subsystem**.
2. Execute the **aucmddev** command to create a Command Device.
   The following is an example of specifying LU 200 for Command Device 1.

   To use the protection function of CCI, enter **enable** following the **-dev** option.

   Example:

```
% aucmddev –unit subsystem-name –set –dev 1 200
Password: manager-password
Are you sure you want to set the command devices? (y/n [n]): y
The command devices have been set successfully.
%
```

3. Execute the **aucmddev** command to verify that the Command Device has been created. The following shows an example.

   Note: To set the alternate Command Device function or to avoid data loss and subsystem downtime, designate two Command Devices. For details on alternate Command Device function, refer to the *Hitachi TagmaStore™ Adaptable Modular Storage, Command Control Interface (CCI) User and Reference Guide*, MK-95DF701.

   Example:

```
% aucmddev -unit subsystem-name -refer
Password: manager-password
Command Device  LUN  RAID Manager Protect
1               200  Disable
%
```

4. **To release an already set Command Device**, specify as follows:

   The following is an example of releasing Command Device 1.

   Example:

```
% aucmddev -unit subsystem-name -rm -dev 1
Password: manager-password
Are you sure you want to set the command devices? (y/n [n]): y
The command devices have been set successfully.
%
```

5. **To change an already set Command Device**, release the already set Command Device first, then change the LU number. The following is an example of specifying LU 201 for Command Device 1.

   Example:

```
% aucmddev -unit subsystem-name -set -dev 1 201
Password: manager-password
Are you sure you want to set the command devices? (y/n [n]): y
The command devices have been set successfully.
%
```

A.5 Setting an Attribute

To set an attribute:

1. From the command prompt, register the subsystem (array unit) to which you want to set the attribute of the Data Retention Utility feature, then **connect to the subsystem**.
2. Execute the **auluguard** command to set the attribute of the Data Retention Utility feature.

   An example, in which an attribute type of the LU 1 is changed from Read/Write (default attribute) to Read/Write Inhibition (Protected), is shown here. Specify it as the -term option on years (0 to 60) and days (0 to 21,900).

   Example:

```
% auluguard -unit subsystem-name -set -lu 1 -attr Protect  -term 0 0
Password: manager-password
Are you sure you want to change the access level of logical unit? (y/n[n]): y
When setting starts, the subsystem stops accepting access to the logical unit from
the host.
Before setting, stop access to the logical unit from the host.
Do you want to continue processing? (y/n[n]): y
The access level of logical unit has been successfully changed.
%
```

   When setting the attribute as Read Only, specify -attr Read-Only; when setting the attribute as Read/Write, specify -attr Read Write.

3. Execute.

   Example:

```
% auluguard -unit subsystem-name -refer
Expiration Lock = OFF
  LUN  Attribute    Capacity      S-VOL     Retention Term   Mode
    0  Can't Guard     1.0 Gbyte  ---       ---              ---
    1  Protect         2.0 Mbyte  Disable   0 days           ---
    2  Read/Write      2.0 Mbyte  Enable    ---              ---
%
```

   - **LUN:** LU number is displayed.
   - **Attribute:** Attribute (Read/Write, Read Only, Protect, or Can't Guard) is displayed.
   - **Capacity:** Capacity of the LU is displayed.
   - **S-VOL:** Whether the LU can be set to S-VOL (Enable) or is inhibited from being set to S-VOL (Disable) is displayed.
   - **Mode:** Mode (Read Capacity 0 (Zero), hiding from Inquiry Command Mode (Zer/Inv), or un-specifying (---)) is displayed. (For reference only.)
   - **Retention:** The length of time for retention (Unlimited or ---) is displayed.

Note: When Read only or Protect is set as the attribute, S-VOL will be disabled.

A.6 Setting an S-VOL

The following steps describe the procedure to se an S-VOL:

1. From the command prompt, register the subsystem (array unit) to which you want to set the attribute of the Data Retention Utility feature. **Connect to the subsystem**.
2. Execute the **auluguard** command to set the attribute of the Data Retention Utility feature.

   An example in which the LU 2 is made unable to be assigned to an S-VOL is shown here.

   Example:

```
% auluguard -unit subsystem-name -set -lu 2 -svol disable
Password: manager-password
Are you sure you want to change the access level of logical unit? (y/n[n]): y
When setting starts, the subsystem stops accepting access to the logical unit from
the host.
Before setting, stop access to the logical unit from the host.
Do you want to continue processing? (y/n[n]): y
The access level of logical unit has been successfully changed.
%
```

   When setting up so that it can be specified as a S-VOL, it is specified **-svol enable**.

3. Execute the **auluguard** command to confirm whether an attribute has been set. An example is shown below.

   Example:

```
% auluguard -unit subsystem-name –refer
Expiration Lock = OFF
  LUN  Attribute    Capacity      S-VOL     Retention Term   Mode
    0  Can't Guard     1.0 Gbyte  ---       ---              ---
    1  Read/Write      2.0 Mbyte  Disable   0 days           ---
    2  Read/Write      2.0 Mbyte  Disable   ---              ---
%
```

A.7 Changing the Retention Term

Note: Data Retention Utility cannot shorten the Retention Term.

To change the retention term:

1. From the command prompt, register the subsystem (array unit) in which you will set the Data Retention Utility attribute. **Connect to the subsystem**.
2. Execute the **auluguard** command to set the Data Retention Utility attribute.

   The following is an example of changing the LU 1 retention term. Specify it as the -term option on years (0 to 60) and days (0 to 21,900).

```
% auluguard -unit subsystem-name -set -lu 1 -term 0 1
Password: manager-password
Are you sure you want to change the retention term of logical unit? (y/n[n]): y
The retention term of logical unit has been successfully changed.
%
```

3. Execute the **auluguard** command to confirm that an attribute has been set. An example is shown below.

```
% auluguard -unit subsystem-name -refer
Expiration Lock = OFF
  LUN  Attribute    Capacity      S-VOL    Retention Term   Mode
    0  Can't Guard     1.0 Gbyte  ---      ---              ---
    1  Protect         2.0 Mbyte  Disable      1 days       ---
    2  Read/Write      2.0 Mbyte  Disable  ---              ---
%
```

A.8 Setting the Expiration Lock

To set the expiration lock:

1. From the command prompt, register the subsystem (array unit) in which you will set the Data Retention Utility attribute. **Connect to the subsystem**.
2. Execute the **auluguard** command to set the Data Retention Utility attribute.

```
% auluguard -unit subsystem-name -set -exlock on
Password: manager-password
Are you sure you want to set the expiration lock to ON? (y/n[n]): y
If the expiration lock is set to ON, you cannot change access level of the logical
unit to Read/Write after the retention term expires. Are you sure? (y/n[n]): y
The expiration lock has been set successfully.
%
```

3. Execute the **auluguard** command to confirm that an attribute has been set. An example is shown below.

```
% auluguard -unit subsystem-name -refer
Expiration Lock = ON
  LUN  Attribute    Capacity      S-VOL    Retention Term   Mode
    0  Can't Guard     1.0 Gbyte  ---      ---              ---
    1  Protect         2.0 Mbyte  Disable  1 day           ---
    2  Read/Write      2.0 Mbyte  Disable  ---              ---
%
```

Acronyms and Abbreviations

A	Ampere
AL-PA	arbitrated loop-physical address
AMS	Adaptable Modular Storage
API	application programming interface
ASTM	American Society for Testing Materials
ATA	Advanced Technology Attachment standard
ATM	asynchronous transfer mode
BC	business continuity
BS	Basic (power) supply
BSA	bus adapter
BTU	British thermal unit
CCI	command control interface
CEC	Canadian Electroacoustic Community
CFW	cache fast write
CHAP	challenge handshake authentication protocol
CIFS	common internet file system
CKD	count-key data
CLI	command line interface
CSA	Canadian Standards Association
CSV	comma separated value
CTG	consistency group
CTL	controller
CU	controller unit
CUDG	control unit diagnosis
dB(A)	decibel (A-weighted)
D-CNT	default (owner) controller
DAMP	Disk Array Management Program
DDL	data definition language
DHCP	dynamic host configuration protocol
DKC	disk controller unit
DLM	data lifecycle management
DM-LU	differential management logical unit
DRAM	dynamic random access memory
DWDM	dense wavelength division multiplexer
EMI	electromagnetic interference
EPO	emergency power-off
FC	fibre channel
FC-AL	fibre channel-arbitrated loop
FCC	Federal Communications Commission
FCP	fibre-channel protocol
Gbps	gigabit per second

HA	high availability
HACMP	high availability cluster multi-processing
HBA	host bus adapter
HDLM	Hitachi Dynamic Link Manager
HORCM	Hitachi Open Remote Copy Manager
H-LUN	host logical unit
H-RAIN	heterogeneous redundant array of independent nodes
HSN	hierarchical star network
HWM	high water mark
IDE	integrated drive electronics; see also ATA.
IIS	Internet Information Service
IOPS	input output operations per second
IOS	internet work operating system
iSCSI	internet small computer system interface
JRE	Java 2 runtime environment
LCP	local control port
LD	logical device
LDEV	logical device
LDM	logical device manager
LIP	loop initialization primitive
LRU	least recently used
LUN	logical unit number
LUSE	LU size expansion
LVI	logical volume image
LVM	logical volume manager
MCU	main control unit
NDMP	Network Data Management Protocol
MDB	master directory block
MIB	message information block
μP	microprocessor
MR	magneto-resistive
MU	mirror unit
MVS	multiple virtual storage
MVS/ESA	multiple virtual storage /enterprise systems architecture
MVS/XA	multiple virtual storage /extended architecture
NAS	network attached storage
NBU	NetBackup (a Symantec product)
NEC	National Electrical Code
NFS	network file system
NIC	network interface card
NIS	network information service
NNC	network node controller
NSC	network storage controller
NTP	network time protocol

NVS	nonvolatile storage
OCI	Oracle Call Interface
ODM	object data manager
OFC	open fibre control
ORM	online read margin
OSI	open systems interconnection
PCI	power control interface
PDL	product documentation library
PFUS	pool full status
POSIX	portable operating system interface
PPRC	peer-to-peer remote copy
PSUE	pair suspended-error status
PSUS	pair suspended-split
PSUS(N)	pair suspended – not restored status
PV	physical volume
P-VOL	primary volume
RAID	redundant array of independent disks
RC	reference code
RCU	remote control unit
RPO	recovery point objective
RTC	real-time clock
RTO	recovery time objective
SAN	storage-area network
SATA	serial ATA
SCSI	small computer system interface
SIM	service information message
SM	shared memory module
SMB	server message block
SMTP	simple mail transfer protocol
SNIA	Storage Networking Industry Association
SNMP	simple network management protocol
SONET	synchronous optical network
SSL	secure socket layer
SSWS	suspend for swapping S-VOL
S-VOL	secondary volume
TID	target identifier
TPOF	tolerable points of failure
UDP	user diagram protocol
UL	Underwriters' Laboratories
USP	Universal Storage Platform
VCS	Veritas Cluster Server™
VDE	Verband Deutscher Elektrotechniker
VIB	volume information block
VOLID	volume identifier

V-VOL	virtual volume (Snapshot Image)
VxVM	Veritas Volume Manager
WDM	wavelength division multiplexing

Glossary

A

Asynchronous

The term asynchronous is used to describe data communications between computers and devices which occurs intermittently rather than in a steady stream. Communication within a computer, however, is usually synchronous and is governed by the microprocessor clock.

Attribute

As used in this document, an attribute is one or more qualities possessed by an object.

Attribute

An attribute is one or more qualities possessed by an object.

B

background copy

A physical copy of all tracks from the source volume to the target volume

Bind

To bind is to assign a value to a symbolic placeholder. For example, when a program is bound, or linked, the binder replaces the symbolic addresses in the code with real machine addresses.

C

Cache

Cache is a temporary, high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are found in computers: memory caching and disk caching. Memory caches are built into the architecture of microprocessors and often computers have external cache memory. Disk caching works like memory caching; however, it uses slower, conventional main memory that on some devices is called a memory buffer.

Cache fast write (CFW)

CFW is an attribute of record caching in which the cache fast write access function (either Simplex Write or Duplex Write) enables the specified record ID to be placed in the volatile control unit cache when a file-type macro is issued and the cache is available. If the cache is not available, the record is written directly to the DASD surface. A single write is issued to the prime module only or a duplexed write is issued to both the prime and the duplicate modules.

Cache Partition Manager

Cache Partition Manager (CPM) is an optional feature of the Hitachi AMS/WMS disk array subsystem. It enables the user data area of cache to be more finely tuned to the application and enables cache to be divided into sections called partitions to which logical units may be assigned.

Capacity

Capacity is the amount of information (in bytes) that can be stored on a disk drive. The capacity of a hard disk drive is usually expressed in megabytes. Capacity is the measure of the potential contents of a device; the volume it can contain or hold. In communications, capacity refers to the maximum possible data transfer rate of a communications channel under ideal conditions.

cascade configuration

A cascade configuration is a connection configuration of volume pairs in which a P-VOL or an S-VOL from a pair belonging to one copy function is used as a P-VOL or S-VOL of the other copy function. TCE supports cascading with ShadowImage and SnapShot.

Channel

A channel is the path data communication follows between two nodes of a network. It is the link between the central processor and the peripherals. A channel can be the physical cabling that connects the nodes on a network, an electronic signal traveling over a pathway, or a sub-channel in a carrier frequency.

channel adapter (CHA)

Provides the channel interface control functions and intercache data transfer functions. It is used to convert the data format between CKD and FBA. The CHA contains an internal processor and 128 bytes of edit buffer memory.

channel extender

A channel extender is a device used to increase the communication distances between channel-connected mainframe computers or between a computer and peripheral devices such as workstations, printers, and storage devices. Optical fiber channel connections are part of the system.

Configuration

Configuration for hardware involves setting various switches and jumpers. For software it means defining the values of parameters. For hardware and software respectively, configuration is the arrangement of the components that make up the system or the set up and set values of the software.

CIFS

Common Internet File System is a protocol used to expose the contents of an archive. CIFS allows clients to access files on a remote Windows computer as if they were part of the local file system.

Cluster

A cluster is group of disk sectors. The operating system assigns a unique number to each cluster and then keeps track of files according to which clusters they use.

cluster capacity

Cluster capacity is the total amount of disk space in a cluster, excluding the space required for system overhead and operating system. Cluster capacity is the amount of space available for all archive data, including original file data, metadata, and redundant data.

command devices

Command devices are dedicated logical volumes that are used only by management software such as CCI, to interface with the storage subsystems. Command devices are not used by ordinary applications. Command devices can be shared between several hosts. Up to two command devices can be configured per TCE subsystem.

concurrency of S-VOL

A state resulting when an S-VOL is synchronized, by simultaneously updating S-VOL with P-VOL data and data cached in the primary host memory. There may be discrepancies in S-VOL data, if data is cached in the primary host memory between two write operations. This data which is not available on the P-VOL, is not reflected on to the S-VOL. To ensure concurrency of S-VOL, cached data is written onto the P-VOL before subsequent remote copy operations

concurrent copy

Concurrent copy is a combined hardware, license, and software systems management solution that creates data dumps or copies while other applications are updating that data, allowing end-user processing to continue. Concurrent copy allows you to update the data in the files being copied, but the copy or dump of the data it secures does not contain any of the intervening updates.

configuration

Configuration for hardware involves setting various switches and jumpers. For software it means defining the values of parameters. For hardware and software respectively, configuration is the arrangement of the components that make up the system or the set up and set values of the software

configuration definition file

The configuration definition file describes the system configuration for making CCI operational in a TCE environment. The configuration definition file is a text file created and/or edited using any standard text editor, and can be defined from the PC where the CCI software is installed. The configuration definition file describes configuration of new TCE pairs on the primary or remote subsystem.

consistency group

A consistency group is a group of two or more logical units in a file system or logical volume. When a file system or a logical volume which stores application data, is configured from two or more logical units, these multiple logical units are managed as a consistency group (CTG) and treated as a single entity. A set of volume pairs can also be managed and operated as a consistency group.

consistency of S-VOL

A state in which a reliable copy of S-VOL data from a previous update cycle, is available at all times on the remote subsystem. A consistent copy of S-VOL data is internally pre-determined during each update cycle and maintained in the remote data pool. When remote takeover operations are performed, this reliable copy is restored to the S-VOL, eliminating any data discrepancies. Data consistency at the remote site enables quicker restart of operations upon disaster recovery.

console (administrative)

The cluster-specific web application that allows monitoring and managing of a HCA cluster and its individual nodes.

control unit (CU)

The control unit is a CPU component that implements microprocessor instructions.

count-key data (CKD)

Format for encoding data on hard drives, typically used in the mainframe environment. It is a physical disc format (Count, Key, Data) introduced by IBM with Series/360 2311 disks in 1964. Count-key-data (CKD) disks format each track as a new file is written on that track (all files have at least one track). CKD disks like SCSI and IDE have sector (count) ID fields and data fields. CKD disks can also have a third kind of field between ID and data called a key field.

cycle time

Cycle time is a user specified time interval used to execute recurring data updates for remote copying. Cycle time cycle updates are set for each subsystem and are calculated based on the number of CTGs.

cycle update

Cycle update processing involves periodically transferring differential data updates from the P-VOL to the S-VOL. TCE remote replication processes are implemented as recurring cycle update operations executed in specific time periods (cycles).

cycle update

Cycle update processing involves periodically transferring differential data updates from the P-VOL to the S-VOL. TCE remote replication processes are implemented as recurring cycle update operations executed in specific time periods (cycles).

D

dark fiber

A dark fiber is an optical fiber cable that has been physically laid but is still unactivated.

Dark Fiber

The dark fiber is the optical fiber that does not work but it is laid. The optical fibers are generally laid by several dozen fibers to several hundred. Only fibers to be needed are activated and others are left as the dark fiber.

data pools

A data pool is a group of one or more disk volumes, designated to temporarily store untransferred differential data (in the local subsystem) or snapshots of backup data (in the remote subsystem). The saved snapshots are useful for accurate data restoration (of the P-VOL) and faster remote takeover processing (using the S-VOL).

data volume

A data volume is a volume that stores database information, whereas other files, such as index files and data dictionaries, store administrative information, known as metadata.

dataset

A dataset is a named collection of data in an IBM mainframe operating system. A dataset in an IBM mainframe is the equivalent of a file in other operating systems, such as Mac OS, Windows and UNIX, for PCs.

device emulation

See logical volume image (LVI).

differential-data

The data to be updated from the suspended status of the pair volume to the primary volume.

differential-data

Differential-data is a set of snapshot data that consists of only the data that changed since a previous snapshot was taken. A backup of differential-data is called an incremental backup.

Differential data control

To control the differential data constantly.

Differential data copy

To copy the updated data to the secondary volume. The data is updated from the differential data control status (the pair volume is under the suspended status) to the primary volume.

Differential Management Logical Unit (DM-LUs)

Differential management logical units are logical units used to manage differential data in a storage subsystem. In a TCE system, there may be up to two DM-LUs configured per subsystem.

direct access storage device (DASD) fast write (DFW)

DFW is an attribute of record caching (while DASD Fast Write Access is a function of record caching) in which a specified record ID is placed in the cache and nonvolatile storage when a file-type macro is issued. If the cache is not available or the nonvolatile storage is not available, the record is written directly to the DASD surface.

disaster recovery

Disaster recovery implies procedures executed to recover critical application data and processing after a disaster Disaster recovery processes include failover and failback procedures.

disaster recovery

To recover the data and to keep an operation going when a critical failure.

Disc array device

Disc array subsystem. The disc array subsystem is referred to as “Disc array device” or “Disc subsystem” in this manual.

disk array device

In this manual, a disk array subsystem is sometimes referred to as a disk array device.

disk controller unit (DKC)

A disk controller unit consisting of CHA, CHF, DKA, Cache and other components except DKU.

DNS manager

The Domain Name System (manager) provides host-name resolution services to clients. It also balances requests across all nodes to ensure maximum cluster throughput and availability.

dual copy

Dual copy is the process of simultaneously updating of a P-VOL and S-VOL using a single write operation.

E

emulation

Emulation is the ability of a program or device to imitate another program or device. Emulation causes a software package to accept that a device it is talking to is really another device. At the system level, emulation is a package of hardware, firmware, and software able to recreate a target machine environment on a new system.

Entire copy

To copy all data in the primary volume to the secondary volume for conforming the data of both volumes completely.

Extender

A converter that changes a signal to other signal.

When the data is transmitted to a distance, an extender is used for changing a signal for Fibre Channel to a signal for a dark fiber or an Ethernet (IP).

Extender

An extender is a converter used to change signals when data is transmitted over long distances. For instance, changing a fiber channel signal to a signal for dark fiber or an Ethernet (IP).

extent

An extent is a contiguous area of storage in a computer file system that is reserved for writing or storing a file.

F

fabric

The hardware that connects workstations and servers to storage devices in a SAN. The SAN fabric enables any-server-to-any-storage device connectivity through the use of Fibre Channel switching technology.

Failover

To take over a process or a data with an alternative host when a failure occurs in a host. By using the High Availability software, an automatically switching the hosts is possible.

Failover

A failover operation involves takeover of critical application processing by an alternate host in the event of a failure at the primary site. Automatic switching of hosts is possible using High Availability software.

fallback

Fallback refers to the process of restarting business operations at a local site using the P-VOL, after the storage subsystems have been recovered.

Fibre channel

Input/output channel using Fibre cable.

fibre channel (FC)

Input/output channel using optical fiber cables. It is the physical media that forms the lowest layer of fibre channel transport.

firmware

Microcode complementing the hardware used to implement the architecture of a system.

fixed block architecture

A model of disks in which storage space is organized as linear, dense address spaces of blocks of a fixed size. Abbreviated FBA. Fixed block architecture is the disk model on which SCSI is predicated. cf. count-key-data.

fixed-content data

Fixed-content data is an exact digital reproduction of a data file as it existed before the file was archived. Fixed-content data cannot be modified or deleted before its retention period expires.

G

gateway

A gateway is a protocol that provides users and applications access to data in a cluster.

granularity of differential data

The granularity of differential data refers to the size or amount of data transferred to the S-VOL during an update cycle. Since only the differential data in the P-VOL is transferred to the S-VOL, the size of data sent to S-VOL is often the same as that of data written to P-VOL. The amount of differential data that can be managed per write command is limited by the difference between the number of incoming host write operations (inflow) and outgoing data transfers (outflow).

H

HCA cluster

An HCA cluster is an implementation of Hitachi Content Archiver. An HCA cluster is both a repository that stores terabytes of data and a gateway that enables access to that data.

High Availability (HA) software

High Availability software is used for automatically switching to a stand-by host, in the event of primary host or disk failure. High availability software has to be installed on the primary and secondary hosts.

High Availability (HA) Software

Software that automatically switches a host to a stand-by host (fail-over) during a failure of a host and disks. High Availability software is installed in more than one host respectively.

H-RAIN

Heterogeneous Redundant Array of Independent Nodes. A collection of networked servers that can differ by vendor or model.

HTTP

Hypertext Transfer Protocol is one of the protocols used to expose the contents of an archive. Using HTTP, archived files and directories can be viewed on a web page.

HTTPS

HTTPS is HTTP with SSL security.

ICKDSF

A DSF command used to perform media maintenance.

I

initial copy

An initial copy operation involves copying all data in the primary volume to the secondary volume prior to any update processing. Initial copy is performed when a volume pair is created.

initiator ports

A port-type used for MCU port of Fibre Remote Copy function.

iSCSI

iSCSI (Internet-Small Computer Systems Interface) is used as an IP-based standard for carrying SCSI commands over IP networks which link data storage devices and allows the transfer of data.

Java applet

A Java applet is a program written in the JavaTM programming language that can be included in an HTML page. When you use a Java technology-enabled browser to view a page that contains an applet, the applet's code is transferred to your system and executed by the browser's Java Virtual Machine (JVM).

J

journal volume

A journal volume is a volume in which the hard disk maintains data integrity in the event of a system crash. The journal volume maintains a log or journal of the activities that have taken place in the volume. This journal allows any lost data to be recreated, because updates to the metadata in directories and bit maps have been written to a serial log.

L

logical

Logical is used to describe a user's view of the way data or systems are organized. The opposite of logical is physical, which refers to the real organization of a system. A logical description of a file is that it is a quantity of data collected together in one place. The file appears this way to users. Physically, the elements of the file could live in segments across a disk.

logical device (LDEV)

A logical device is a group of hardware items that the operating system treats as a single unit.

Logical Unit (LU)

See User Logical Unit (LU)

logical unit number (LUN)

LUN is a three-bit code identifier for a logical unit. LUN0-7 can be assigned.

logical volume

An area on a disk consisting of device files that are logically integrated using a volume manager.

logical volume image (LVI)

LVI (also called device emulation) is a feature used to create virtual LUs that are up to 36 times larger than the standard OPEN-x LUs.

Logical Volume

An area on a disk consisting of device files that are logically integrated using a volume manager.

LU

Logical unit in a device that is connected with Fibre.

LUN

Logical Unit Number. The number of the unit that is connected with Fibre.

M

mainframe

A mainframe is a large and expensive computer capable of simultaneously supporting thousands of users. In this document the term mainframe is used for IBM computers (zSeries® and S/390®-based systems). This term also marks a distinction between Unix or Windows server computers and the larger more, powerful mainframe. A mainframe is also commonly referred to as the *host*, even though any computer host having a unique IP address can equally be referred to as a *host*.

metadata

Metadata is information about an archived object.

microcode

Microcode is the lowest-level instructions directly controlling a microprocessor. Microcode is generally hardwired and cannot be modified.

Microsoft cluster server

Microsoft Cluster Server is a clustering technology built that supports clustering of two NT servers to provide a single fault-tolerant server.

middleware

Middleware is software that connects two otherwise separate applications. For example, a middleware product can be used to link a database system to a Web server. Using forms, users request data from the database; then, based on the user's requests and profile, the Web server returns dynamic Web pages to the user.

mount

To mount a device or a system means to make a storage device available to a host or platform.

mount point

Mount points are the location in your system where you mount your file systems or devices. For a volume that is attached to an empty folder on an NTFS file system volume, the empty folder is a mount point. In some systems a mount point is simply a directory.

multiple allegiance support

The multiple allegiance support means that the storage unit can accept concurrent I/O requests for a volume from multiple channel paths. Therefore the storage unit can process requests from separate FICON hosts in parallel, improving throughput and performance.

multiple virtual storage

MVS (including MVS/370, MVS/ESA, MVS/XA) is an operating system that runs on IBM or compatible mainframe computers. The host component works on MVS/ESA (Enterprise Systems Architecture) and MVS/XA (Extended Architecture).

N

NDMP

Network Data Management Protocol is a protocol used to backup and restore archived objects.

NFS

Network File System is a protocol used to expose the contents of an archive. NFS allows clients to access files on a remote computer as if they were part of a local file system.

node

In networks, a node is a processing location. A node can be a computer or some other device, such as a printer. Every node has a unique network address. In HCA clusters, nodes are Linux-based servers running HCA software and networked to form an HCA cluster.

open device

Collectively refers to the host computer, peripheral control units, and intelligent peripherals that are connected to fibre channel.

P

pair

See ShadowImage pair.

P-VOL

Primary volume, the volume on the primary side of the pair volume. The primary volume controls the pair status, and the status reflects on the secondary volume.

pair splitting

Pair splitting refers to the termination of a volume pair relationship to temporarily stop update copy processing for the specified volume pair. Pairs may also be split before system reduction tasks.

pair status

A pair status is an internal status assigned to a volume pair before or after pair operations. Pair status transitions occur when pair operations are performed or as a result of failures. Pair statuses are used to monitor copy operations and detect system failures.

Pair status

The status of the logical volume that is paired.

Paired volume

Primary and secondary volume that are paired in a disk array device.

paired volumes

Paired volumes are primary and secondary volumes comprising a volume pair.

Panel

In this document, a *panel* is equivalent to a *window*.

Parity

The quality of being either odd or even. The fact that all numbers have a parity is commonly used in data communications to ensure the validity of data. This is called parity checking. So parity provides an error detection scheme that uses an extra checking bit, called the parity bit, to allow the receiver to verify that the data is error free.

parity groups

RAID groups can contain single or multiple parity groups where the parity group acts as a partition of that container.

path blockade watch

The path blockade watch setting specifies the time for monitoring blockade in the Fibre Channel paths on the MCU side. The path blockade watch value must be from 0 to 45 seconds. This setting is available for Fibre Channel interface only.

pattern file

A pattern is a table that contains the access attributes of all logical volumes. Pattern files enable administrators to change the access attributes of all logical volumes quickly and easily.

peer-to-peer remote copy (PPRC)

The Peer-to-Peer Remote Copy (PPRC) function is a hardware-based solution for mirroring logical volumes from a primary site (the application site) onto the volumes of a secondary site (the recovery site).

permission

Using SMB/CIFS, HTTP, WebDAV, and SMTO gateways, permissions are granted from the owner to members of a group or other users to allow access to data files or directories in an archive. Read, write, and execute permissions can be granted for files, directories, or symbolic links.

point-in-time logical copy

A logical copy or snapshot of a volume at a point in time. This allows a backup or mirroring application to run concurrently with the system.

point-to-point

A configuration that allows two ports to be connected serially.

policy

A policy is a process that performs a specific function to aid maintenance of the overall health of a cluster. For example, authentication, cluster balance, garbage collection, protection, retention, and scavenging.

pool volume

A pool volume is used to store backup versions of files, archive copies of files, and files migrated from other storage.

POSIX

Portable Operating System Interface for UNIX is a set of standards that define an application programming interface (API) for software designed to run under heterogeneous operating systems.

primary or local site

A site where the production applications run.

primary volume (P-VOL)

A primary volume is the storage volume in a volume pair, used as the source of a copy operation. In copy operations a copy source volume is called the "P-VOL" while the copy destination volume is called "S-VOL" (secondary volume).

Q

quota values

Quota values are set for users with write access to volumes providing data storage limits for that user/volume. Quota values are applied to a snapshot and set for the target file system when the snapshot is taken.

R

RCU target port

A port-type used for RCU port of Fibre Remote Copy function. This port allows LOGIN of host computers and MCUs.

recovery point objective

Recovery point objective is the maximum desired time period prior to a disaster, during which changes to data may be lost as a result of recovery. This measure determines up to what point in time data should be recovered in the event of a disaster. Data changes preceding the disaster by at least this time period are preserved by recovery.

recovery time objective

Recovery time objective is the maximum desired time period required to bring one or more applications and associated data back to a correct operational state. It defines the time frame within which specific business operations or data must be restored to avoid any business disruption.

Remote or target site

A site that has the mirrored data of the production site.

remote or target site

A site that has the mirrored data of the primary site.

remote path

A remote path is a route connecting identical ports on the local subsystem and the remote subsystem. Two remote paths must be setupup for each subsystem (one path for each of the two controllers built in the subsystem).

remote volume stem

In TrueCopy operations, the remote volume (R-VOL) is a volume located in a different subsystem from the primary host subsystem.

repeater

A repeater is a network device used to regenerate or replicate a signal. A repeater relays messages between sub-networks that use different protocols or cable types. A repeater cannot do the intelligent routing performed by bridges and routers.

Resynchronization

Resynchronization is a copy operation performed to make data in the secondary volume consistent with data in the primary volume. This operation involves copying only untransferred differential data to the target secondary volume.

Resynchronization (TrueCopy)

To copy the differential data to the secondary volume for conforming the data of both the primary and secondary volumes. When the resynchronization is completed, the status changes to the pair status.

S

SATA

Serial ATA is a serial link, a single cable with a minimum of four wires creates a point-to-point connection between devices. ATA is a computer bus technology primarily designed for transfer of data to and from a hard disk. SATA is the successor to the legacy Advanced Technology Attachment standard (ATA, also known as IDE or Integrated Drive Electronics).

secondary volume (S-VOL)

A secondary volume (S-VOL) is a replica of the primary data volume (P-VOL), maintained on the standby subsystem. Recurring differential data updates are performed to keep the data in the S-VOL consistent with data in the P-VOL.

sequential data striping

Sequential data striping refers to writing to multiple disk drives in a pre-planned sequence. Because the processor writes faster than the disk can accept, it has the left-over capacity to locate the next segment of the logically sequential data and prepare to write to it.

Service

A service is the set of functions that one of the seven (7) Open Systems Interconnection (OSI) model layers delivers to the layer above it. For example, the TCP layer provides a reliable byte-stream service to the application layer above it.

server set identifier

The SSID is an alphanumeric name that is 1-32 bytes. The purpose of an SSID is to help hardware clients find and connect to an access point (AP) on the correct network.

session

A session is a series of communications or exchanges of data between two end points that occurs during the span of a single connection. The session begins when the connection is established at both ends and terminates when the connection is ended. For some applications each session is related to a particular port. In this document a session the exchange of data between groups of primary and secondary volumes

ShadowImage

ShadowImage is a software program that replicates user data on TagmaStore AMS/WMS disks, bypassing the host system.

ShadowImage

ShadowImage is a software program that replicates user data on TagmaStore® USP disks, bypassing the host system.

Shadowimage Pair

A disk is a Logical Volume Image (LVI). S-VOLs and T-VOLs are ShadowImage volumes for Source and Target. Data is physically copied from the S-VOL to the T-VOL.

shared memory module (SM)

Stores the shared information about the system and the cache control information (director names). This type of information is used for the exclusive control of the system. Like CACHE, shared memory is controlled as two areas of memory and fully non-volatile (sustained for approximately 7 days).

sidefile

A sidefile is an area of a controller's storage that occupies about 1MB of the controller storage. The sidefile is used to hold data that is changed or updated while being backed up or copied. The sidefile holds it for later integration into the copied data.

SMB

Server Message Block is a protocol used to expose the contents of an archive. SMB allows clients to access files on a remote computer as if they were part of a local file system.

SMTP

Simple Mail Transfer Protocol is a protocol used to receive and store email data directly from email servers.

Snapshot

A term used to denote a copy of the data and data-file organization on a node in a disk file system. A snapshot is a replica of the data as it existed at a particular point in time.

SNMP

Simple Network Management Protocol is a protocol used to facilitate monitoring and management of clusters through an external interface. SNMP sends notifications to IP addresses whenever certain types of events occur.

source copy

Source copy is the place from which data is taken. The place from which the data is moved is called the source. The source can also indicate the node on a network from which data is sent to its destination.

SSL

Secure Sockets Layer is a key-based Internet protocol for transmitting documents through an encrypted link.

SSL certificate

An SSL certificate is a file containing the cryptographic keys and signatures used with an SSL protocol to verify the authenticity of web sites to protect data sent to or from that site.

Status transition

To change the pair status of the pair volume

Storage Navigator

The TagmaStore Storage Navigator consists of a group of Java™ applet programs that enable users to manage the TagmaStore subsystem. Storage Navigator Java™ applet programs run on a web browser to provide a user-friendly interface for TagmaStore web client functions.

Suspended status

The status when the update operation is suspended with keeping the pair status. Under this status, the differential data control for the updated data is performed in the primary volume.

S-VOL

Secondary volume, the volume on the secondary side of the pair volume. The primary volume controls the pair status, and the status reflects on the secondary volume.

S-VOL determination

S-VOL determination is an internal process on the remote subsystem, which replicates the S-VOL independent of the update operations. This process occurs at the end of each update cycle. This process allows a pre-determined copy of S-VOL data consistent with P-VOL data (as of the previous cycle) to be maintained on the remote site at all times.

sysplex

Sysplex denotes *system complex*. This is a processor complex formed by connecting a number of processors together into a single unit through channel-to-channel adapters or ESCON/FICON fiber optic links. The processors are synchronized using a Sysplex Timer and are managed as a single system image (SSI1). The Sysplex Timer is an invaluable component when systems on multiple CPCs share access to the same data.

system reduction

System reduction refers to maintenance tasks performed to improve system performance. These tasks may include pair deletion, deletion of command devices and data pools.

takeover processing

Takeover processing involves transferring of critical application processing to the S-VOL on the remote standby subsystem. The remote S-VOL is immediately enabled to process subsequent host I/O operations.

target copy

Target copy is a file, device or any type of location to which data is moved or copied.

target port

A port-type which is different from "Initiator Port" and "RCU Target Port". This port is a normal target port which is used without configuration of Fibre Remote Copy. This "Target port" allows LOGIN of host computers. It does not allow LOGIN of MCUs

target site

See Remote or target site.

tier architecture

Tier 1 is fully supported computing expected to be production quality. Tier 2 platforms are not supported by the security officer and release engineering teams. Tier 2 systems are targeted at Tier 1 support, but are still under development. Tier 3 platforms are architectures for which hardware is not or will not be available or which are considered legacy systems unlikely to see broad future use. Tier 4 systems are not supported in any way.

Tier 1: Static content, Tier 2: Application logic, Tier 3: Database

TPOF

Tolerable points of failure consists of the number of concurrent failures beyond with a cluster is no longer viable. A failure is defined as either a node or a disk not functioning properly or responsively.

track

A track is a ring on a disk where data can be written. For hard disks, tracks aggregate into platters and a single track location that cuts through all platters is termed a cylinder. Each track can be subdivided into a number of sectors. The operating system and disk drive find stored information using its track and sector numbers.

truck size

Truck size represents a fixed sector size for each volume type.

Target site

See Remote or target site.

Trap

A program interrupt usually caused by some exceptional situation in a user program. In most cases, the OS performs some action and then returns control to the program.

TrueCopy

TrueCopy is a software program that replicates user data between two TagmaStore USP disks, bypassing the host system.

TrueCopy

The TrueCopy™ feature enables you to create and maintain duplicate copies of all user data stored on a Hitachi TagmaStore™ subsystem for data duplication, backup, and disaster recovery purposes.

TrueCopy

TrueCopy is a software program that replicates data between two TagmaStore disks, independent of the host system. TrueCopy versions are available for TagmaStore AMS/WMS and USP/NSC subsystems. TrueCopy for z/OS is a mainframe version.

U

User Logical Unit (LU)

A user logical unit is a term used to describe any device file located on an external disk subsystem connected to the TagmaStore USP or NSC by a fibre channel.

user logical unit (LU)

A user logical unit is a term used to describe any device file located on an external disk subsystem connected to the TagmaStore subsystem by a fibre channel.

V

Volume

A volume is the basic unit of storage that includes recovery logs and storage pools. A volume can be a logical volume management (LVM) logical volume, a standard file system file, a tape cartridge, or an optical cartridge. The various types of defined volumes include: external, internal, copy source, copy destination, reserve, data, journal, virtual, pool, system, LUSE, copy pair, and USP.

Volume copy

To copy all data of P-VOL into S-VOL.

virtual LVI/ LUN (VLL)

Virtual LVI/LUN is an option that enables the configuration of custom-size logical device images and logical units, which are smaller than standard size devices.

volume

A volume is the basic unit of storage that includes recovery logs and storage pools. A volume can be a logical volume management (LVM) logical volume, a standard file system file, a tape cartridge, or an optical cartridge. The various types of defined volumes include: external, internal, copy source, copy destination, reserve, data, journal, virtual, pool, system, LUSE, copy pair, and USP.

Volume copy

To copy all data of P-VOL into S-VOL.

volume pair

A volume pair is formed by pairing two logical data volumes. It typically consists of one primary volume (P-VOL) on the local storage subsystem and one secondary volume (S-VOL) on the remote storage subsystems. TCE remote copy operations are performed using logical volume pairs.

volume signature

A volume signature is an integer that is an element in the master directory block (MDB) (volume information block (VIB)). For example, for HFS volumes, this field (drSigWord) contains the number $4244.

WDM

Wavelength Division Multiplexing. Generally, WDM is to multiplex the optical signal of several channels and DWDM (Dense WDMP) is to multiplex the optical signal of several dozen channels. Generally, WDM is to multiplex the optical signal of several channels and DWDM (Dense WDM) is to multiplex the optical signal of several dozen channels.

WDM/DWDM

WDM denotes Wave Division Multiplexing technology used to multiplex optical signals from multiple channels. DWDM denotes Dense Wave Division Multiplexing and is used to multiplex optical signals of several dozen channels.

World Wide Name (WWN)

A unique identifier for an open systems host. It consists of a 64-bit physical address (the IEEE 48-bit format with a 12-bit extension and a 4-bit prefix). The WWN is essential for defining the SANtinel™ parameters because it determines whether the open systems host is to be allowed or denied access to a specified LU or a group of LUs.

WORM

Write once, read many is a data storage technique in which files are protected from being modified, overwritten, or deleted.

write order guarantee

The write order guarantee feature ensures that data is updated in S-VOL in the same order that the host was updated data in the P-VOL, particularly when there are multiple write operations in one update cycle. This feature is critical to maintain data consistency in the remote S-VOL and is implemented by inserting sequence numbers in each update record. Update records are then sorted in the cache within the remote system, to assure write sequencing.