HITACHI
Inspire the Next

Hitachi Adaptable Modular Storage Data Retention Utility User's Guide

FastFind Links

Document organization

Product version

Getting help

Contents

Hitachi Data Systems

MK-97DF8019-02

Hitachi, Ltd. and Hitachi Data Systems reserve the right to make changes to this document at any time without notice and assume no responsibility for its use. Hitachi, Ltd. and Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements.

All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

Notice: Hitachi Data Systems products and services can be ordered only under the terms and conditions of Hitachi Data Systems’ applicable agreement(s). The use of Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Preface

This document provides facilities requirements for preparing and installing Hitachi Adaptable Modular Storage (AMS) 2100, 2300, and 2500 storage systems. In this document, these storage systems are referred to collectively as the Hitachi AMS 2000 Family storage systems. If information pertains to certain members of this family, those systems are identified.

Using this document, you will be able to prepare your site for the arrival and installation of your units. To determine the total components your shipment will include, please consult your Hitachi Data Systems representative.

This preface includes the following information:

- Document revision level
- Changes in this revision
- Intended audience
- Document organization
- Document conventions
- Related documents
- Regulatory information
- Getting help
- Comments

Document revision level

This section provides a history of the revision changes to this document.

Revision	Date	Description
MK-97DF8019-00	November 2009	Initial release
MK-97DF8019-01	April 2010	Revision 01, supersedes and replaces MK-97DF8019-00
MK-97DF8019-02	August 2010	Revision 02, supersedes and replaces MK-97DF8019-01

Changes in this revision

- New conditions for when to configure Java runtime parameters in Setting an attribute on page 4-2.

Intended audience

This document is intended for personnel who will schedule, manage, and perform the tasks required to prepare your site for installing a Hitachi AMS 2000 Family storage systems.

Product version

This document applies to Hitachi AMS 2000 Family firmware version 0893 or later.

Document organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the first column to go to that chapter. The first page of every chapter or appendix contains a brief list of the contents of that section of the manual, with links to the pages where the information is located.

Chapter/Appendix Title	Description
Overview	This chapter describes the Data Retention Utility features.
Preparation	This chapter describes the environments, requirements, and specifications that you need when using the Data Retention Utility.
Installing the DRU	This chapter describes the operational procedures when using your Data Retention Utility.
Operations	This chapter describes the operational procedures when using your Data Retention Utility.
Appendix A, Operations using the CLI	This appendix describes logical unit expansion features.
Appendix B, Operations using CCI	This appendix describes operations using CCI.

Convention for storage capacity values

Physical storage capacity values (e.g., disk drive capacity) are calculated based on the following values:

Physical capaciy unit	Value
1 KB	1,000 bytes
1 MB	1,000 KB or 1,000^{2} bytes
1 GB	1,000 MB or 1,000^{3} bytes
1 TB	1,000 GB or 1,000^{4} bytes
1 PB	1,000 TB or 1,000^{5} bytes
1 EB	1,000 PB or 1,000^{6} bytes

Logical storage capacity values (e.g., logical device capacity) are calculated based on the following values:

Logical capaciy unit	Value
1 block	512 bytes
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or 1024^{2} bytes
1 GB	1,024 MB or 1024^{3} bytes
1 TB	1,024 GB or 1024^{4} bytes
1 PB	1,024 TB or 1024^{5} bytes
1 EB	1,024 PB or 1024^{6} bytes

Document conventions

This document uses the following symbols to draw attention to important safety and operational information.

Symbol	Meaning	Description
💡	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
⚠	Note	Notes emphasize or supplement important points of the main text.
⚠	Caution	Cautions indicate that failure to take a specified action could result in damage to the software or hardware.

The following typographic conventions are used in this document.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy *source-file target-file* Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.
underline	Indicates the default value. Example: [a | b]

Accessing product documentation

The AMS 2000 Family user documentation is available on the Hitachi Data Systems Portal: https://portal.hds.com. Please check this site for the most current documentation, including important updates that may have been made after the release of the product.

This documentation set consists of the following documents.

Release notes

- Adaptable Modular Storage System Release Notes
- Storage Navigator Modular 2 Release Notes

⚠ Please read the release notes before installing and/or using this product. They may contain requirements and/or restrictions not fully described in this document, along with updates and/or corrections to this document.

Installation and getting started

The following documents provide instructions for installing an AMS 2000 Family storage system. They include rack information, safety information, site-preparation instructions, getting-started guides for experienced users, and host connectivity information. The symbol ☞ identifies documents that contain initial configuration information about Hitachi AMS 2000 Family storage systems.

☞ **AMS2100/2300 Getting Started Guide**, MK-98DF8152

Provides quick-start instructions for getting an AMS 2100 or AMS 2300 storage system up and running as quickly as possible.

☞ **AMS2500 Getting Started Guide**, MK-97DF8032

Provides quick-start instructions for getting an AMS 2500 storage system up and running as quickly as possible.

AMS 2000 Family Site Preparation Guide, MK-98DF8149

Contains initial site planning and pre-installation information for AMS 2000 Family storage systems, expansion units, and high-density expansion units. This document also covers safety precautions, rack information, and product specifications.

AMS 2000 Family Fibre Channel Host Installation Guide, MK-08DF8189

Describes how to prepare Hitachi AMS 2000 Family Fibre Channel storage systems for use with host servers running supported operating systems.

AMS 2000 Family iSCSI Host Installation Guide, MK-08DF8188

Describes how to prepare Hitachi AMS 2000 Family iSCSI storage systems for use with host servers running supported operating systems.

Storage and replication features

The following documents describe how to use Storage Navigator Modular 2 (Navigator 2) to perform storage and replication activities.

Storage Navigator 2 Advanced Settings User's Guide, MK-97DF8039

Contains advanced information about launching and using Navigator 2 in various operating systems, IP addresses and port numbers, server certificates and private keys, boot and restore options, outputting configuration information to a file, and collecting diagnostic information.

Storage Navigator Modular 2 User's Guide, MK-99DF8208

Describes how to use Navigator 2 to configure and manage storage on an AMS 2000 Family storage system.

AMS 2000 Family Dynamic Provisioning Configuration Guide, MK-09DF8201

Describes how to use virtual storage capabilities to simplify storage additions and administration.

Storage Navigator 2 Storage Features Reference Guide for AMS, MK-97DF8148

Contains concepts, preparation, and specifications for Account Authentication, Audit Logging, Cache Partition Manager, Cache Residency Manager, Data Retention Utility, LUN Manager, Performance Monitor, SNMP Agent, and Modular Volume Migration.

AMS 2000 Family Copy-on-write SnapShot User Guide, MK-97DF8124

Describes how to create point-in-time copies of data volumes in AMS 2100, AMS 2300, and AMS 2500 storage systems, without impacting host service and performance levels. Snapshot copies are fully read/write compatible with other hosts and can be used for rapid data restores, application testing and development, data mining and warehousing, and nondisruptive backup and maintenance procedures.

AMS 2000 Family ShadowImage In-system Replication User Guide, MK-97DF8129

Describes how to perform high-speed nondisruptive local mirroring to create a copy of mission-critical data in AMS 2100, AMS 2300, and AMS 2500 storage systems. ShadowImage keeps data RAID-protected and fully recoverable, without affecting service or performance levels. Replicated data volumes can be split from host applications and used for system backups, application testing, and data mining applications while business continues to operate at full capacity.

AMS 2000 Family TrueCopy Remote Replication User Guide, MK-97DF8052

Describes how to create and maintain multiple duplicate copies of user data across multiple AMS 2000 Family storage systems to enhance your disaster recovery strategy.

AMS 2000 Family TrueCopy Extended Distance User Guide, MK-97DF8054

Describes how to perform bi-directional remote data protection that copies data over any distance without interrupting applications, and provides failover and recovery capabilities.

AMS 2000 Data Retention Utility User's Guide, MK-97DF8019 — this document

Describes how to lock disk volumes as read-only for a certain period of time to ensure authorized-only access and facilitate immutable, tamper-proof record retention for storage-compliant environments. After data is written, it can be retrieved and read only by authorized applications or users, and cannot be changed or deleted during the specified retention period.

Storage Navigator Modular 2 online help

Provides topic and context-sensitive help information accessed through the Navigator 2 software.

Hardware maintenance and operation

The following documents describe how to operate, maintain, and administer an AMS 2000 Family storage system. They also provide a wide range of technical information and specifications for the AMS 2000 Family storage systems. The symbol ☞ identifies documents that contain initial configuration information about Hitachi AMS 2000 Family storage systems.

☞ **AMS 2100/2300 Storage System Hardware Guide**, MK-97DF8010

Provides detailed information about installing, configuring, and maintaining AMS 2100 and 2300 storage systems.

☞ **AMS 2500 Storage System Hardware Guide**, MK-97DF8007

Provides detailed information about installing, configuring, and maintaining an AMS 2500 storage system.

☞ **AMS 2000 Family Storage System Reference Guide**, MK-97DF8008

Contains specifications and technical information about power cables, system parameters, interfaces, logical blocks, RAID levels and configurations, and regulatory information about AMS 2100, AMS 2300, and AMS 2500 storage systems. This document also contains remote adapter specifications and regulatory information.

AMS 2000 Family Storage System Service and Upgrade Guide, MK-97DF8009

Provides information about servicing and upgrading AMS 2100, AMS 2300, and AMS 2500 storage systems.

AMS 2000 Family Power Savings User Guide, MK-97DF8045

Describes how to spin down volumes in selected RAID groups when they are not being accessed by business applications to decrease energy consumption and significantly reduce the cost of storing and delivering information.

Command and Control (CCI)

The following documents describe how to install the Hitachi AMS 2000 Family Command Control Interface (CCI) and use it to perform TrueCopy and ShadowImage operations.

AMS 2000 Family Command Control Interface (CCI) Installation Guide, MK-97DF8122

Describes how to install CCI software on open-system hosts.

AMS 2000 Family Command Control Interface (CCI) Reference Guide, MK-97DF8121

Contains reference, troubleshooting, and maintenance information related to CCI operations on AMS 2100, AMS 2300, and AMS 2500 storage systems.

AMS 2000 Family Command Control Interface (CCI) User's Guide, MK-97DF8123

Describes how to use CCI to perform TrueCopy and ShadowImage operations on AMS 2100, AMS 2300, and AMS 2500 storage systems.

Command Line Interface (CLI)

The following documents describe how to use Hitachi Storage Navigator Modular 2 to perform management and replication activities from a command line.

Storage Navigator Modular 2 Command Line Interface (CLI) Unified Reference Guide, MK-97DF8089

Describes how to interact with all Navigator 2 bundled and optional software modules by typing commands at a command line.

Storage Navigator 2 Command Line Interface Replication Reference Guide for AMS, MK-97DF8153

Describes how to interact with Navigator 2 to perform replication activities by typing commands at a command line.

Dynamic Replicator documentation

The following documents describe how to install, configure, and use Hitachi Dynamic Replicator to provide AMS Family storage systems with continuous data protection, remote replication, and application failover in a single, easy-to-deploy and manage platform.

Dynamic Replicator - Scout Release Notes, RN-99DF8211

Dynamic Replicator - Scout Host Administration Guide, MK-98DF8212

Dynamic Replicator - Scout Installation and Configuration Guide, MK-98DF8213

Dynamic Replicator - Scout Quick Start Guide, MK-98DF8214

Dynamic Replicator - Scout Host Troubleshooting Guide, MK-98DF8215

Dynamic Replicator DR-Scout ICAT Utility Guide, MK-98DF8216

Dynamic Replicator - Scout RX Server Deployment Guide, MK-98DF8217

Dynamic Replicator VX Solution for Oracle (Solaris), MK-98DF8218

Dynamic Replicator - Scout Solution for SharePoint 2007, MK-98DF8219

Dynamic Replicator - Scout Solution for MySQL (Windows), MK-98DF8220

Protecting Citrix XenServer Using Hitachi Dynamic Replicator - Scout, MK-98DF8221

Dynamic Replicator Quick Install/Upgrade Guide, MK-98DF8222

Dynamic Replicator - Scout Protecting MS SQL Server, MK-98DF8223

Dynamic Replicator - Scout - Protecting Microsoft Exchange Server, MK-98DF8224

Dynamic Replicator - Scout File Server Solution, MK-98DF8225

Dynamic Replicator - Scout ESX - Protecting ESX Server (RCLI), MK-99DF8226

Getting help

If you need to contact the Hitachi Data Systems support center, please provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any messages displayed on the host system(s).
- The exact content of any messages displayed on Storage Navigator Modualr 2.
- The Storage Navigator Modular 2 configuration information. This information is used by service personnel for troubleshooting purposes.

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, please log on to the Hitachi Data Systems Portal for contact information: https://portal.hds.com

Comments

Please send us your comments on this document:doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

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

Contents

1

Overview

The Data Retention Utility feature protects data in your disk array 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 the Data Retention Utility, you will can 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.

This chapter includes the following:

- Assigning access attribute to logical units
- Retention terms
- Protecting logical volumes from copy operations

⚠ **NOTE:** In this documentation, logical volumes are sometimes referred to as logical devices (or LDEVs). Also, logical volumes to be accessed by open-systems hosts are sometimes refereed to as logical units or LUs.

Assigning access attribute 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 the Data Retention Utility, you can use logical units as read-only volumes to protect the volumes against write operations. You can also protect logical volumes against both read and write operations. The 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 Command Control Interface (CCI) and/or Hitachi Storage Navigator Modular 2 (Navigator 2). A system administrator can set or reset one of the following access attributes for the each LU.

When the Read Only or Protect attribute is set using Navigator 2, 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 the 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.

ShadowImage, SnapShot, TrueCopy, 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 the 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.

ShadowImage, SnapShot, TrueCopy, 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.

ShadowImage, SnapShot, TrueCopy, and TCE cannot copy data to logical volumes that have Protect attribute.

Report Zero Read Cap. (Mode)

Report Zero Read Cap. mode can be set or reset by 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.

ShadowImage, SnapShot, TrueCopy, and TCE cannot copy data to an LU with an attribute that is Read Capacity 0.

Invisible (Mode)

The Invisible mode can be set or reset 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.

ShadowImage, SnapShot, TrueCopy, and TCE cannot copy data to an LU with an attribute that is in Invisible mode.

Retention terms

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 the 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 changes 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 is Read Only, Protect, Red Capacity 0, or Invisible from Inquiry Command, can be changed to Read/Write.

NOTE: The Retention Term interval is updated only when the disk array is in the Ready status. Therefore, the Retention Term may become longer than the specified term when the disk array power is turned on/off by a user. Also, the Retention Term interval may generate errors depending on the environment.

However, when the Expiration Lock is set to ON by Navigator 2, all the LU attributes, which are Read Only, Protect, Read Capacity 0, and Invisible from Inquiry Command, are unable to be changed to Read/Write.

When a host tries to write data to a Read Only logical volume, the write operation fails. The write failure is reported to the host. This occurs even when the Retention Term expires.

Also, when the Data Retention Utility is started for the first time, the Expiration Lock is set to OFF. When a host tries 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.

Protecting logical volumes from copy operations

When ShadowImage, SnapShot, TrueCopy, or TCE copies data, the data on the copy destination volume (also known as the secondary volume) is overwritten. If a volume containing important data is specified as a secondary volume by mistake, ShadowImage, SnapShot, TrueCopy, or TCE can overwrite important data on the volume and you could suffer loss of important data. The Data Retention Utility lets you avoid potential data losses.

If you assign Read Only attribute or Protect attribute to a logical volume, ShadowImage, SnapShot, TrueCopy, and TCE cannot copy data to that logical volume. Any other write operations are prohibited on that logical volume. For example, business application software will be unable to write data to such a logical volume.

To block ShadowImage, SnapShot, TrueCopy, 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 Simplex LU (S-VOL Disable)" is set for the primary volume of ShadowImage, SnapShot, TrueCopy, or TCE, the following copy procedures in the primary volume can be prevented.

- Restoration by ShadowImage or SnapShot
- Takeover by TrueCopy

NOTE: In the ShadowImage, TrueCopy, and TCE manuals, the term "S-VOL" is used in place of the term "secondary volume".

NOTE: SnapShot has two types of secondary volumes: a virtual volume (V-VOL) and an area where differential data is stored (data pool).

2

Preparation

This chapter details the environments that the Data Retention Utility (DRU) can be installed onto, and the settings required to ready the application to begin using Data Retention.

The following preparation is required for the Data Retention Utility:

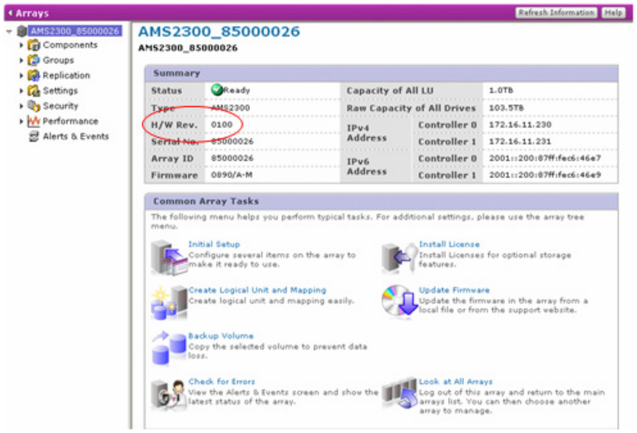
- Environments
- Requirements
- Specifications
- Notes on usage
- Operations example

Environments

Your system should be updated to the most recent firmware version and Navigator 2 software version to access all the features currently available.

- Firmware: Version 0893 or more is required for AMS2100 or AMS2300 array of the hardware revision 0100. Version 0840/A or more is required for AMS2500 array of the hardware revision 0100. Version 0893 or more is required for the AMS2100/AMS2300/AMS2500 of the hardware revision 0200.
- Navigator 2: Version 3.21 or more is required for management PC for AMS2100 or AMS2300 array of the hardware revision 0100. Version 9.30 or more is required for management PC for AMS2100/AMS2300/AMS2500 of the hardware revision 0200.
- CCI: Version 01-21-03/06 or more is required for host when CCI is used for the operation of the Data Retention Utility.
- License key for the Data Retention Utility

The hardware revision can be displayed when an individual array is selected from the Arrays list. As an example, the version 9.00 of Navigator 2 is shown in Figure 2-1.



AMS2300_85000026

AMS2300_85000026

Summary

Status	Ready	Capacity of All LU		1.0TB
Type	AMS2300	Raw Capacity of All Drives		103.5TB
H/W Rev.	0100	IPv4 Address	Controller 0	172.16.11.230
Serial No.	85000026		Controller 1	172.16.11.231
Array ID	85000026	IPv6 Address	Controller 0	2001::200:87ff:fec6:46e7
Firmware	0890/A-M		Controller 1	2001::200:87ff:fec6:46e9

Common Array Tasks

The following menu helps you perform typical tasks. For additional settings, please use the array tree menu.

Initial Setup
Configure several items on the array to make it ready to use.

Install License
Install Licenses for optional storage features.

Create Logical Unit and Mapping
Create logical unit and mapping easily.

Update Firmware
Update the firmware in the array from a local file or from the support website.

Backup Volume
Copy the selected volume to prevent data loss.

Check for Errors
View the Alerts & Events screen and show the latest status of the array.

Look at All Arrays
Log out of this array and return to the main arrays list. You can then choose another array to manage.

Figure 2-1: Identifying hardware version for DRU

Requirements

Command device (use only CCI)

Specifications

Table 2-1 shows the specifications of the Data Retention Utility.

Table 2-1: Specifications of the Data Retention Utility

Parameter	Specifications
Unit of setting	The setting is made for each unit. (However the expiration Lock is set for each disk array.)
Number of settable LUs	AMS2100: 2,048 LUs AMS2300/2500: 4,096 LUs
Kinds of access attributes	Defines the following types of attributes: • Read/Write (default setting) • S-VOL Disable • Read Only • Protect • Read Capacity 0(can be set or reset by CCI only) • Invisible from Inquiry Command Can be set or reset 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 to ON.
LUs not supported.	The following LUs are not supported: • Command device • DMLU • Sub-LU of a unified LU • Unformatted LU • LU set as a data pool of SnapShot or TCE
Relation with ShadowImage/ SnapShot/ TrueCopy/TCE	If the S-VOL Disable is set for an LU, a volume pair using the LU as an S-VOL (data pool) is suppressed. A setting of the S-VOL Disable of a volume that has already become an S-VOL (V-VOL or data pool) is not suppressed only when the pair status is Split. Besides, when the S-VOL Disable is set for a P-VOL, restoration of SnapShot, restoration of ShadowImage is suppressed but a swapping of TrueCopy 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 following a controller detachment.
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 firmware 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.

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 deletion • LU formatting • RAID group deletion
Setting by Navigator 2	Navigator 2 can set an access attribute, one LU at a time.
Unified LU	A unified LU whose access level is a value other than Read/Write can neither be composed nor dissolved.
Deleting, growing, or shrinking of LU	An LU for which an access attribute has been set cannot be deleting, growing, or shrinking. An access attribute can be set for an LU being grown or shrunken LU.
Expansion of RAID group	You can expand the RAID group to which the LUs that the access attribute is set belong.
Cache Residency Manager	An LU for which an access attribute has been set can be used for the 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 the 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.
Concurrent use of Dynamic Provisioning	Available. The DP-VOLs that creating by Dynamic Provisioning cannot be used. The Data Retention Utility can be executed to the normal LU.
Setting range of Retention Term	From the 0th to 21,900 days (60 years) or unlimited.

⚠ **NOTE:** Figure 2-2 shows the status where the migration is performed for an LU which set the Read Only attribute is shown in Figure 2.1. 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 carries 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.

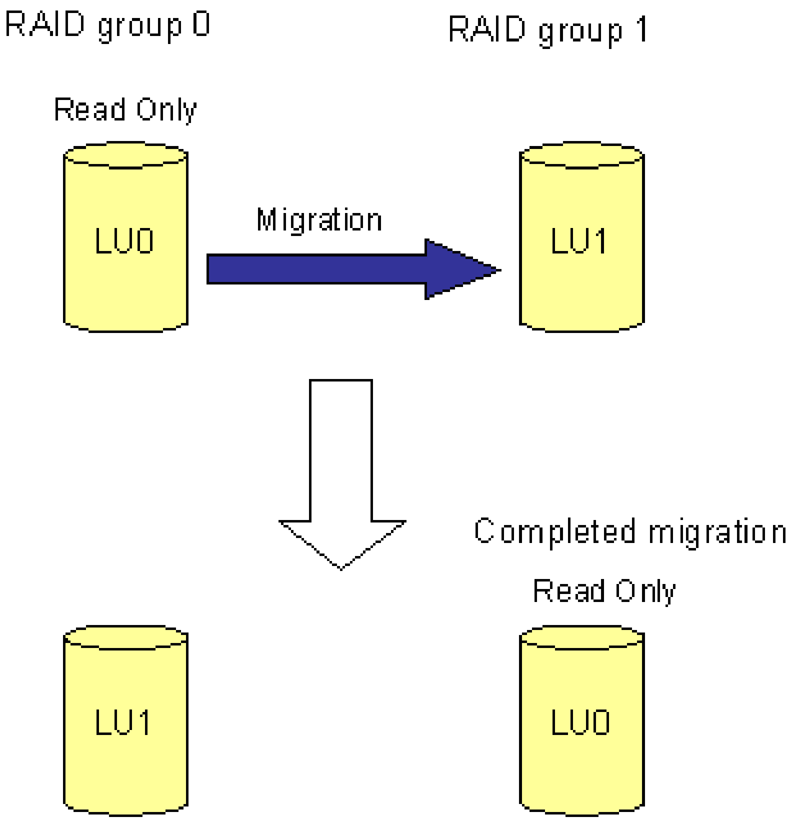


Figure 2-2: Volume Migration of Read-Only Attribute

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:

The 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 DMLU
- An uninstalled LU
- A un-formatted LU

Notes about unified LU

You cannot combine logical volumes that do not have a Read/Write attribute. A unified LU whose access attribute is not Read/Write cannot be dissolved.

Notes About SnapShot and TCE

An LU, whose access attribute is not Read/Write, cannot be assigned to a data pool. Additionally, an access attribute other than Read/Write cannot be set for an LU that has been assigned to a data pool.

Notes and restrictions for each operating system

- Use an LU whose access attributes have been set from the OS:
  - If access attributes are set from the OS, they must be set before mounting the LU. If the access attributes are set to the LU after it is mounted, the system may not operate properly.
  - If a command (create partition, format, etc.) is issued to an LU with access attributes, from the operating system, it appears as if the command ended normally. The information is written to the host cache memory, the new information is not reflected in the LU.
  - An OS may not recognize an LU when the LUN is larger than the one on which the Invisible mode was set.
- Microsoft Windows® 2000:
  - An LU with a Read Only access attribute cannot be mounted.
- Microsoft Windows Server 2003/Windows Server 2008
  - When mounting an LU with a Read Only attribute, do not use the diskpart command to mount and un-mount a volume. Use the -x mount and -x umount commands of CCI.
- Using Windows® 2000/Windows Server 2003/Windows Server 2008:
  - When setting a volume used by Windows® 2000/Windows Server 2003/Windows Server 2008 as the Data Retention Utility LU, the Data Retention Utility can be applied to a basic disk only. When the Data Retention Utility is applied to a dynamic disk, an LU is not correctly recognized.
- Unix® OS
  - When mounting an LU with a is Read Only attribute, mount it as Read Only (using the mount -r command).
- HP-UX®

    - If there is an LU with a Read Only attribute, host shutdown might not be possible. When shutting down the host, change the attribute of LU from Read Only to Protect in advance.
    - An LU with a Protect attribute, host startup time may be lengthy. When starting the host, either change the attribute of LU from Protect to Read Only, or use mapping functions to make the LU unrecognizable from the host.
    - If a write is completed on the LU with a Read Only attribute, it can results in no response; therefore, do not perform write commands (e.g. dd command).
    - If a Read/Write operation is performed on an LU with a Protect attribute, this may result in no response; therefore, do not perform read or write commands (for example, dd command).
- Using LVM
    - If you change the LVM configuration, including Data Retention LU, the specified LU must be temporarily blocked 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 times when an LU to which the Data Retention Utility is applied might not 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 to check propriety of the resource.

Operations example

The operations procedure to use of the Data Retention Utility are shown in the following sections.

Initial settings

Table 2-2 indicates what chapters contain topics on initial settings.

Table 2-2: Where to Find Initial Settings Topics

Parameter	See
Confirm environments and requirements of the Data Retention Utility	Chapter 1, Overview
Installing	Chapter 3, Installing the DRU
Setting the command device when used CCI.	Setting the command devices on page B-2
Setting the configuration definition file when used CCI.	Setting the environment variable on page B-5
Setting the environment variable when used CCI.	Setting the environment variable on page B-5

Optional Operations

Table 2-3 indicates what chapters contain topics on optional operations.

Table 2-3: Where to Find Optional Operations Topics

Parameter	Specifications
Setting an Attribute	Setting an attribute on page 4-2
Changing the Retention Term	Changing the retention term on page 4-5
Setting an S-VOl Disable	Setting an S-VOL on page 4-4
Setting the Expiration Lock	Setting the expiration lock on page 4-6

3

Installing the DRU

When installing, uninstalling, or enabling the Data Retention Utility, the utility is usually locked and cannot be selected. To make it available, 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. The Data Retention Utility is installed and uninstalled using Navigator 2.

Installing, uninstalling, enabling, and disabling the Data Retention Utility feature are set for each disk array. Before installing and uninstalling, verify that the storage system is in normal operating condition. If a controller blockade has occurred, you cannot perform installation and un-installation operations.

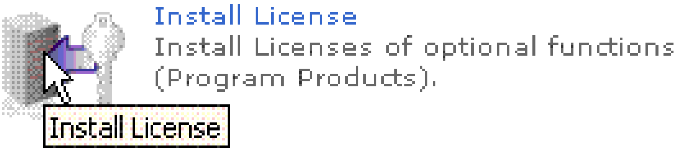
This chapter outlines and describes the following topics:

- ❒ Installing
- ❒ Uninstalling the Data Retention Utility
- ❒ Enabling or disabling the Data Retention Utility

Installing

Follow the instructions below the list to install the Data Retention Utility feature.

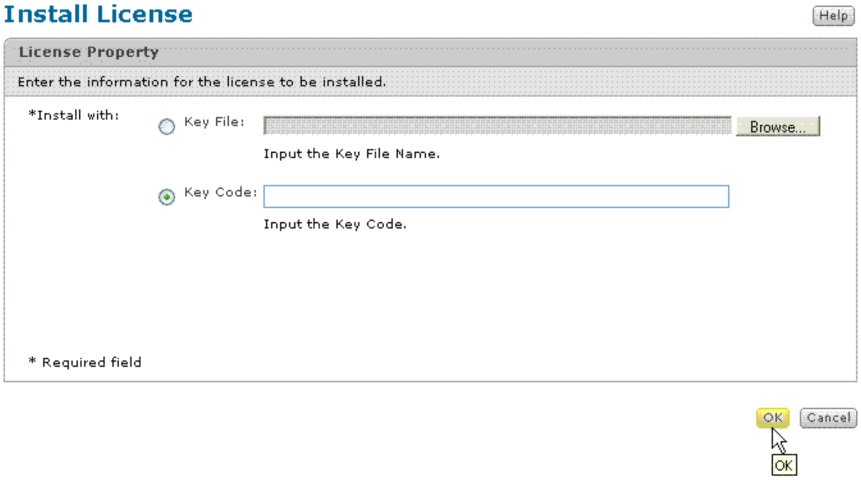
1. Start Navigator 2.
2. Log in as a registered user to Navigator 2.
3. Select the array in which you will install the Data Retention Utility.
4. Click **Show & Configure Array**.
5. Select the **Install License** icon.



Install License

Install Licenses of optional functions (Program Products).

The Install License screen appears.



Install License

License Property

Enter the information for the license to be installed.

*Install with: ○ Key File: Browse...

Input the Key File Name.

● Key Code:

Input the Key Code.

* Required field

6. When you install the option using the key code, click **Key Code**, and then set up the key code. When you install the option using the key file, click **Key File**, and then set up the path for the key file. Click ⚐☺.

⚠ **NOTE:** Browse is used to set the path to a key file correctly.

A screen requests your confirmation to install the Data Retention Utility option.

7. Click **Confirm**.
8. Click **Close**.

Uninstalling the Data Retention Utility

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

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

To uninstall the Data Retention Utility:

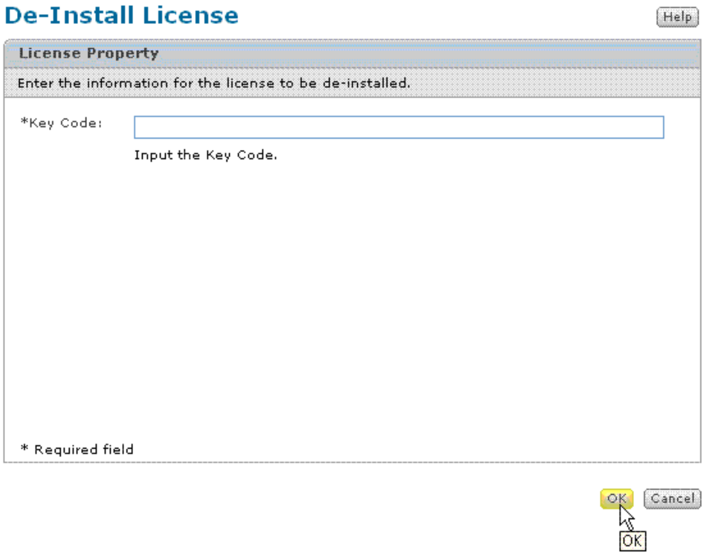
1. Start Navigator 2.
2. Log in as a registered user to Navigator 2.
3. Select the storage system where you will uninstall the Data Retention Utility.
4. Click **Show & Configure Array**.
5. Select the Licenses icon in the Settings tree view.

   Navigator 2:

   - Version 5.00 or higher
   - Version 4.00 or higher
   - Version 3.21

   The Licenses list appears.
6. Click **De-install License**.

   The De-Install License screen appears.



De-Install License

License Property

Enter the information for the license to be de-installed.

*Key Code:

Input the Key Code.

* Required field

7. Enter a key code in the text box. Click **OK**.

   A screen appears, requesting a confirmation to uninstall the Data Retention Utility option.
8. Click **Close**.

Enabling or disabling the Data Retention Utility

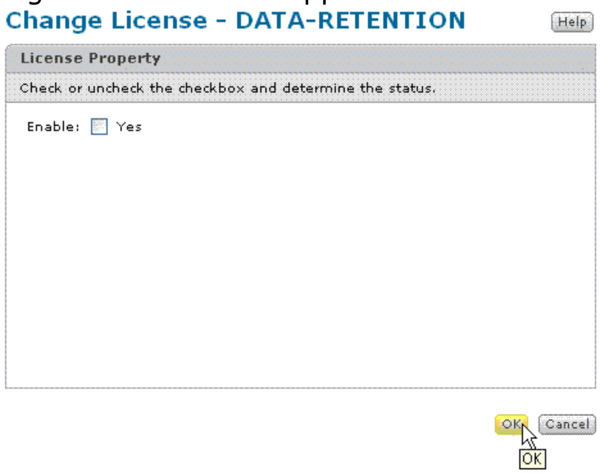
After installation, you can enable or disable the Data Retention Utility.

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

To enable or disable the Data Retention Utility:

1. Start Navigator 2.
2. Log in as the registered user to Navigator 2.
3. Select the storage system where you will set the Data Retention Utility.
4. Click **Show & Configure Array**.
5. Select the Licenses icon in the tree view.
6. Select the **DATA-RETENTION** in the Licenses list.
7. Click the **Change Status**.

   The Change License screen appears.



Change License - DATA-RETENTION

License Property

Check or uncheck the checkbox and determine the status.

Enable: □ Yes

8. To disable, uncheck the checkbox and click **OK**. To enable, check the checkbox and click **OK**.

   A message appears, confirming that this feature is set.
9. Click **Close**.

4

Operations

Configuring and modifying key settings in the DRU software can help customize the data retention process so it fits your needs. Attributes that set access privileges and the secondary volume (S-VOL) object, which acts as a active standby storage system, both enable you to tune your storage system to perform in a desired manner.

Also both the retention term and expiration lock objects enable you to define how long the storage system holds specific data, enabling you to create the appropriate amount of space on the system and to optimize its performance.

This chapter outlines and describes the following topics:

Displaying the Navigator 2 applet screen

To display the applet screen of Navigator 2 in Internet Explorer set the Java runtime parameters by a computer that starts Navigator 2.

When you use the JRE less than 1.6.0_10, setting the Java runtime parameters are necessary in a client to start Navigator 2. When you use the JRE 1.6.0_10 or greater, you do not need to set the Java runtime parameters in a client to start Navigator 2. However, you need to set Java runtime parameters if after starting **Open Advanced Settings**, the system displays the following message:

> DMEG0002F0: Since memories required for the Advanced Settings are insufficient, a screen cannot be displayed. Change a setup of Java Plug-in installed in the client and increase the usable memories.

The procedure is shown below.

1. In the Windows **Start** menu, click **Settings** > Control Panel.
2. From the Control Panel, click**Java**.
3. Click the top View button.
4. Type **-Xmx216m** to the **Java Runtime Parameters** field.
5. Click **OK**.
6. Click **OK** in the **Java** tab.
7. Close the Control Panel.

Setting an attribute

To set an attribute:

1. Start Navigator 2.
2. Log in as a registered user to Navigator 2.
3. Select the storage system in which you will set up an attribute.
4. Click **Show & Configure Array**.
5. Select the **Advanced Settings** icon in the tree view.
6. Click **Open Advanced Settings**.

   After a few minutes, an Array Unit (Applet) screen appears.

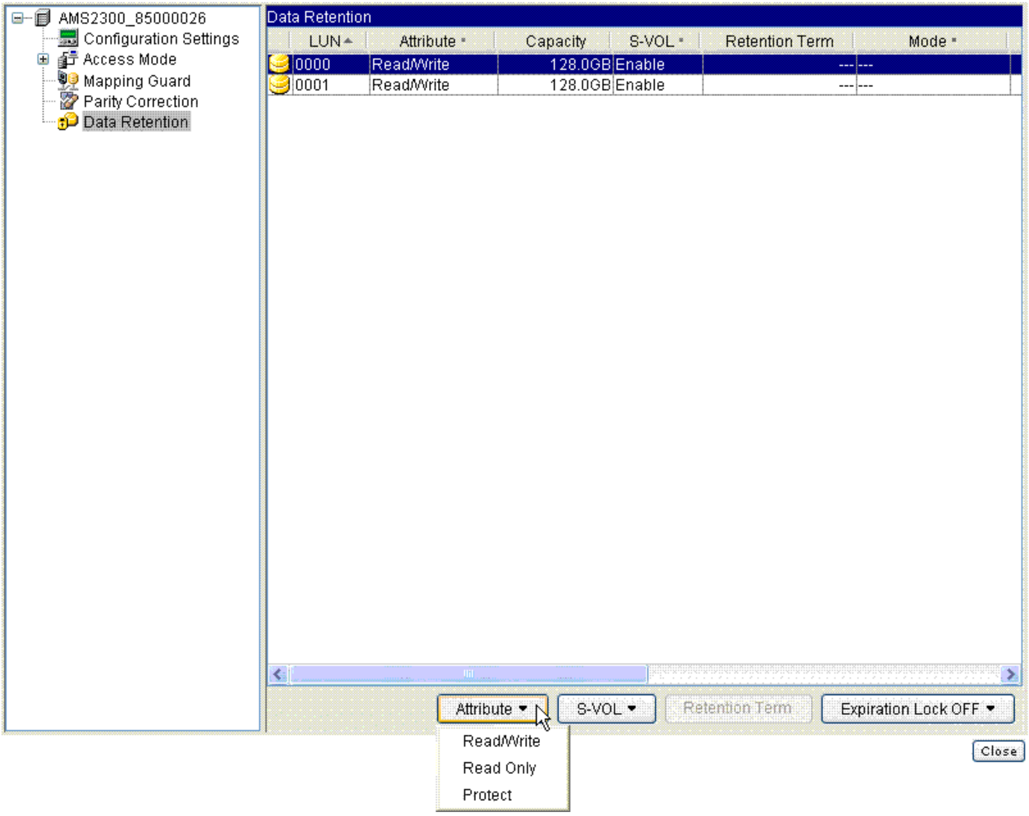
   The Applet screen is displayed connected to the SNM2 Server. If 20 minutes elapses while displaying the Applet screen, you will not be able to operate it due to the automatic logoff function. If the operation is completed, close the screen.

   If the Applet screen cannot be displayed, the login to the SNM2 Server may have failed. In this case, the Applet screen cannot be displayed again. The code: 0x000000000000b045 or "DMEG800003: The error occurred in connecting RMI server." is displayed on the Applet screen. Take the following actions.

   - Close the Web browser, stop the SNM2 Server once, restart it, and display the screen of the Array you want to operate.

- Close the Web browser; confirm the SNM2 Server is started. If it has stopped, start it and display the screen of the Array that you want to operate.
- Return to the Array screen after 20 minutes elapsed and display the screen of the Array you want to operate.

7. Select the Data Retention icon in the applet tree view.



Data Retention

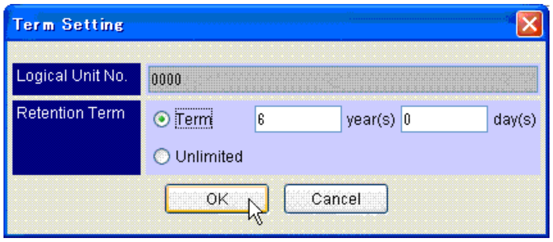
LUN ▴	Attribute ▪	Capacity	S-VOL ▪	Retention Term	Mode ▪
0000	Read/Write	128.0GB	Enable	---	---
0001	Read/Write	128.0GB	Enable	---	---

- **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.
- **Retention Term**:The length of time for retention (Unlimited or ---) is displayed.
- **Mode**: Mode (Read Capacity 0 (Zero), hiding from Inquiry Command Mode (Zer/Inv), or un-specifying (---)) is displayed.

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

8. Select the LUN, from the drop-down list of the **Attribute** button, select **Read Only** or **Protect**.

9. The Term Setting dialog box appears. Select **Term** or **Unlimited** from **Retention Term**.



Term Setting

Logical Unit No.: 0000

Retention Term: ● Term 6 year(s) 0 day(s)
○ Unlimited

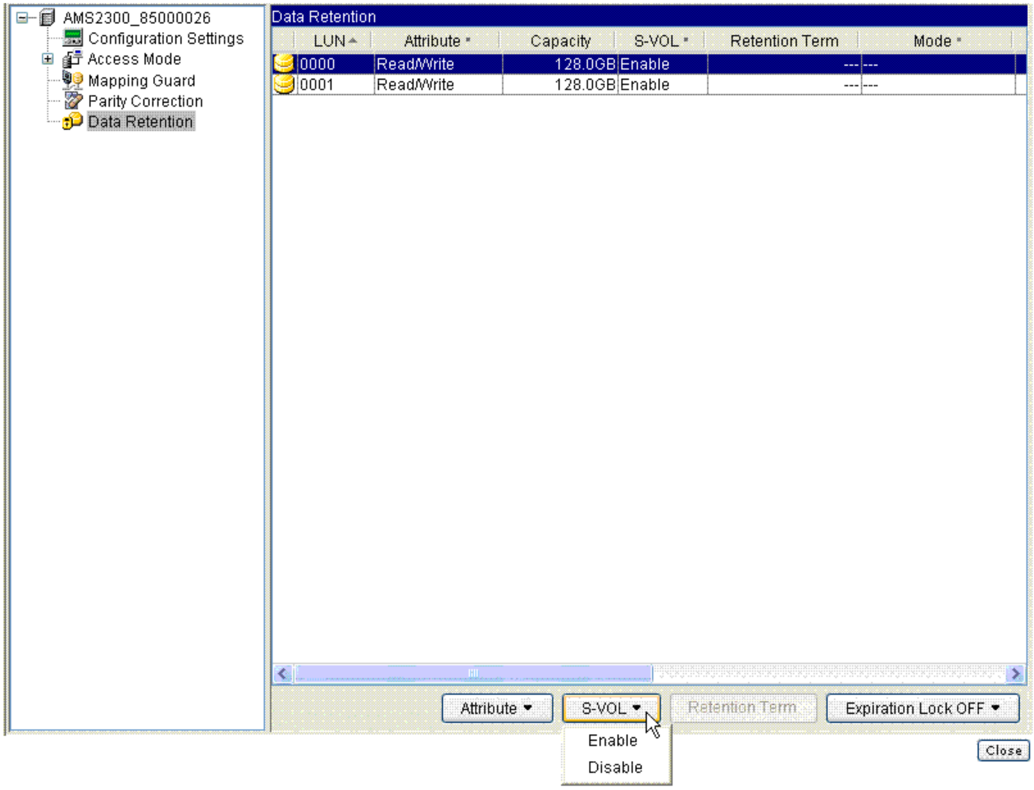
10. On the **Term Setting** dialog box, Click **OK**.
11. The confirmation message appears. Click **OK** three times.

Setting an S-VOL

An S-VOL A replica of the primary volume (P-VOL) at the time of a backup and is kept on a standby storage system. Recurring differential data updates are performed to keep the data in the S-VOL consistent with data in the P-VOL.

To set an S-VOL:

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



Data Retention

LUN	Attribute	Capacity	S-VOL	Retention Term	Mode
0000	Read/Write	128.0GB	Enable	---	---
0001	Read/Write	128.0GB	Enable	---	---

Figure 4-1: S-VOL Drop-Down List

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

Changing the retention term

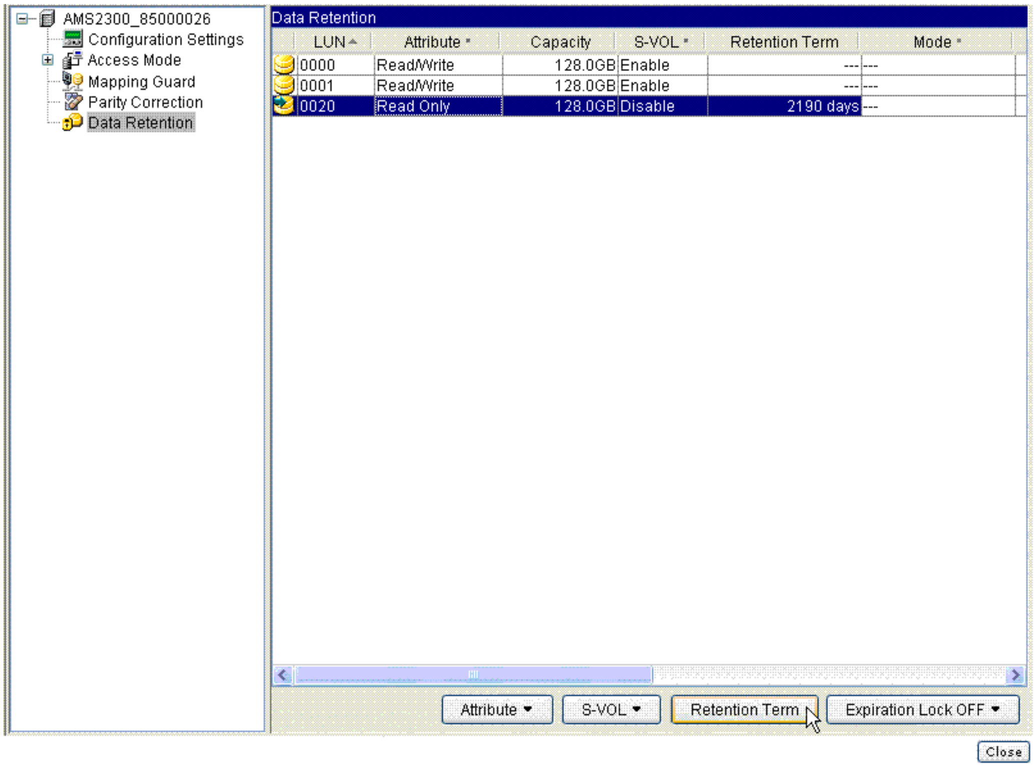
NOTE: The Data Retention Utility cannot shorten the Retention Term.

The retention term is the length of time that the storage system keeps the desired content. It can be either Unlimited or an integer value. If no retention time is specified, the notation for three dotted lines (---) displays as output.

To change the retention term:

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

   The Term Setting dialog box appears.

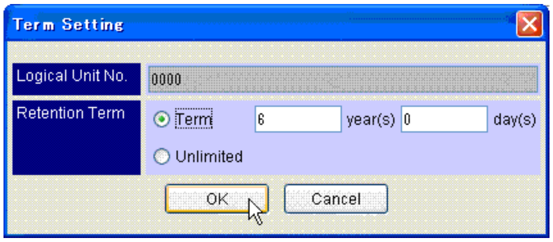


Data Retention

LUN	Attribute	Capacity	S-VOL	Retention Term	Mode
0000	Read/Write	128.0GB	Enable	---	---
0001	Read/Write	128.0GB	Enable	---	---
0020	Read Only	128.0GB	Disable	2190 days	---

Figure 4-2: Data Retention dialog box

2. Select **Term** or **Unlimited** from **Retention Term**.



Logical Unit No.	0000
Retention Term	● Term 6 year(s) 0 day(s) ○ Unlimited

Figure 4-3: Retention Term region of Term Setting dialog box

3. 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.

4. Click **OK**.

   The confirmation message appears.

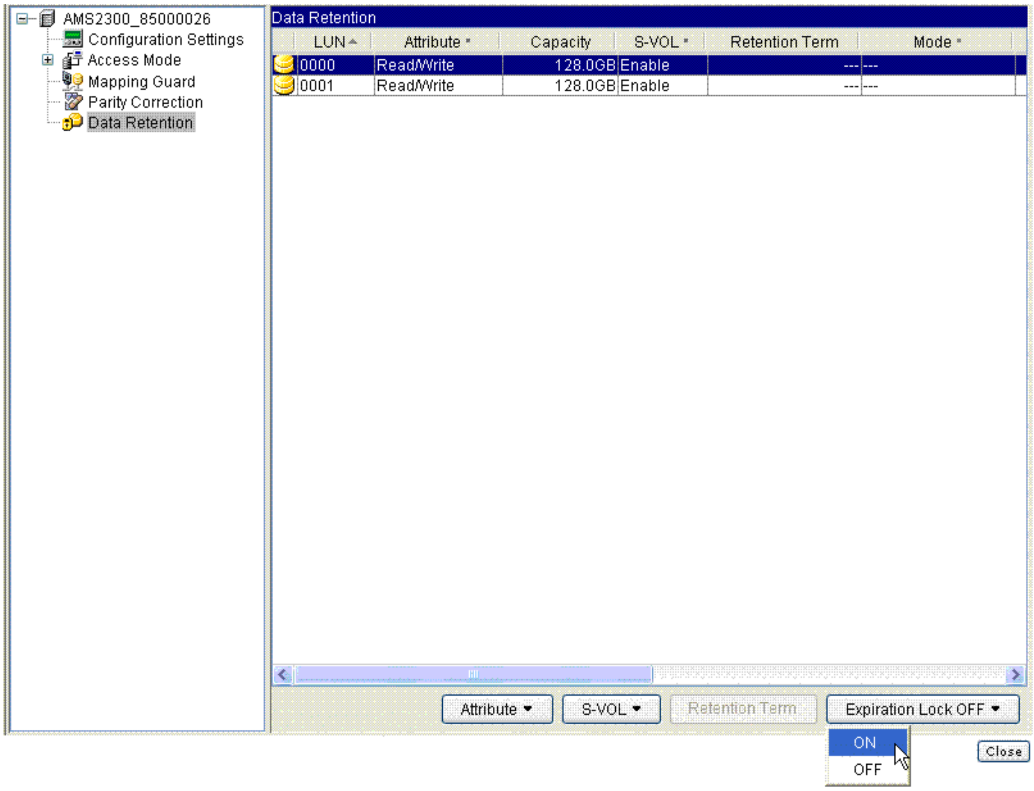
5. Click **OK** two times.

Setting the expiration lock

The expiration lock sets the time limit on when the data in your storage system is no longer needed.

To set the expiration lock:

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



LUN	Attribute	Capacity	S-VOL	Retention Term	Mode
0000	Read/Write	128.0GB	Enable	---	---
0001	Read/Write	128.0GB	Enable	---	---

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

Operations using the CLI

You can perform the same tasks that you did in Navigator 2 by using the command line interface (CLI) provided with your AMS 2000 Family storage system. This appendix covers the following topics, configurable from the CLI:

❒ Installing the Data Retention Utility

❒ Uninstalling the Data Retention Utility

❒ Enabling or disabling the Data Retention Utility

❒ Setting an attribute

❒ Setting an S-VOL

❒ Changing the retention term

❒ Setting the expiration lock

Installing the Data Retention Utility

The Data Retention Utility option is usually not selectable (locked). To make this option available, you must install the 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.

The Data Retention Utility is installed and uninstalled through Navigator 2 (CLI).

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

⚠ **NOTE:** Before installing/uninstalling the 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/un-installation cannot be performed.

To install the Data Retention Utility using the CLI version of Navigator 2:

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

   Example:

   ```
   Cache Partition Manager is enabled

   % auopt -unit array-name -lock off -keycode key code

   Are you sure you want to unlock the option?

    (y/n [n]): y
   ```

   When Cache Partition Manager is enabled, if the option using the data pool will be enabled the default cache partition information will be restored.

   ```
   Do you want to continue processing? (y/n [n]): y

   The option is unlocked.

   %
   ```

   Example:

   ```
   % auopt -unit array-name -refer

   Option NameType      Term     Status

   DATA-RETENTIONPermanent ---      Enable

   %
   ```

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

The Data Retention Utility is installed and uninstalled through Navigator 2.

To uninstall the Data Retention Utility using the CLI version of Navigator 2:

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

   Example:

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

   Example:

   ```
   % auopt -unit array-name -refer
   DMEC002015:No information displayed.
   %
   ```

Enabling or disabling the Data Retention Utility

The Data Retention Utility can be set to enable or disable after installation. This allows the 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 the Data Retention Utility using the CLI version of Navigator 2:

1. From the command prompt, register the array (array unit) in which the status of the Data Retention Utility is to be changed, then connect to the array.
2. Issue 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 array-name -option DATA-RETENTION -st disable
Are you sure you want to disable the option?
 (y/n [n]): y
The option has been set successfully.
%
```

Example:

```
% auopt -unit array-name -refer
Option NameType      Term     Status
DATA-RETENTIONPermanent ---      Disable
%
```

Setting an attribute

To set an attribute:

1. From the command prompt, register the array to which you want to set the attribute of the Data Retention Utility feature, then connect to the array.
2. Issue 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 array-name -set -lu 1 -attr Protect  -term 0 0
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.

3. 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.
%
```

4. When setting the attribute as Read Only, specify -attr Read-Only; when setting the attribute as Read/Write, specify -attr Read Write.
5. Issue the **auluguard** command to confirm whether an attribute has been set.

Example:

```
% auluguard -unit array-name -refer
Expiration Lock = OFF
```

```
 LUN  Attribute    Capacity    S-VOL    Retention Term  Mode
   0  Can't Guard      1.0 GB  ---      ---             ---
   1  Protect        2.0 MB  Disable    0 days        ---
   2  Read/Write       2.0 MB  Enable  ---            ---
%
```

Table A-1: Attribute Settings

Column	Description
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.
Retention Term	The length of time for retention (Unlimited or ---) is displayed.
Mode	Mode (Read Capacity 0 (Zero), hiding from Inquiry Command Mode (Zer/Inv), or un-specifying (---)) is displayed. (For reference only.)

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

Setting an S-VOL

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

1. From the command prompt, register the array to which you want to set the attribute of the Data Retention Utility feature, then connect to the array.
2. Issue 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 array-name -set -lu 2 -svol disable
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.

3. 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 an S-VOL, it is specified -**svol enable**.

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

Example:

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

Changing the retention term

NOTE: The Data Retention Utility cannot shorten the Retention Term.

To change the retention term:

1. From the command prompt, register the array in which you will set the Data Retention Utility attribute. Connect to the array.

2.Issue 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).

Example:

```
% auluguard -unit array-name -set -lu 1 -term 0 1
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.
%
```

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

Example:

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

Setting the expiration lock

To set the expiration lock:

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

   Example:

   ```
       % auluguard -unit array-name -set -exlock on

       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.

Example:

```
% auluguard -unit array-name -refer

Expiration Lock = ON

 LUN  Attribute    Capacity    S-VOL    Retention Term  Mode

   0  Can't Guard      1.0 GB  ---      ---             ---

   1  Protect         2.0 MB  Disable      1 days       ---

   2  Read/Write      2.0 MB  Disable  ---              ---

%
```

B

Operations using CCI

You can perform the same tasks that you did in Navigator 2 by using the CCI provided with your AMS 2000 Family storage system.

This appendix covers the following topics:

- Preparing for using CCI
- Setting the command devices
- Defining the configuration definition file
- Setting the environment variable
- Setting an attribute
- Changing the retention term

Preparing for using CCI

To use the Data Retention Utility for CCI, the following contents are necessary:

- Setting the command devices for CCI
- Defining the configuration definition file for CCI
- Setting the environment variable for CCI

Setting the command devices

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

In order to accept read and write commands that are executed by the disk array 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. Up to 128 command devices can be designated for the disk array. You can designate command devices using Navigator 2.

NOTE: Us set for command devices must be recognized by the host. The command device LU size must be greater than or equal to 33 MB.

To designate command device(s):

1. From the command prompt, register the array to which you want to create the command device. Connect to the array.
2. Issue the **aucmddev** command to create a command device.

   First, displays LUs to be assignable command device, and later create a command device. The following is an example of specifying LU 200 for command device 1.
3. To use the protection function of CCI, enter enable following the -dev option.

   Example:

```
% aucmddev -unit array-name -availablelist
Available Logical Units
  LUN  Capacity RAID Group  DP Pool RAID Level  Type Status
  200   35.0 MB         0     N/A   5( 4D+1P) SAS  Normal
  300   35.0 MB         0     N/A   5( 4D+1P) SAS  Normal
%
% aucmddev -unit array-name -set -dev 1 200
Are you sure you want to set the command devices?
 (y/n [n]): y
The command devices have been set successfully.
```

```
%
```

4. Issue the **aucmddev** command to verify that the command device has been created. The following shows an example.

   Example:

```
% aucmddev -unit array-name -refer
  Command Device    LUN  RAID Manager Protect
                1    200  Disable
%
```

5. To release a command device that has already been set, specify as follows:

   The following is an example of releasing command device 1.

   Example:

```
% aucmddev -unit array-name -rm -dev 1
Are you sure you want to release the command devices?
 (y/n [n]): y
This operation may cause the CCI, which is accessing to this command device, to
freeze.
Please make sure to stop the CCI, which is accessing to this command device, bef
ore performing this operation.
Are you sure you want to release the command devices? (y/n [n]): y
The specified command device will be released.
Are you sure you want to execute? (y/n [n]): y
The command devices have been released successfully.
%
```

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

Defining the configuration definition file

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.

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).

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.
2. In the command prompt, make a copy of the sample file (**horcm.conf**).

   Example:

   ```
   c:\HORCM\etc> copy \HORCM\etc\horcm.conf \WINDOWS\horcm0.conf
   ```
3. Open **horcm0.conf** using a 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).

5. In the **HORCM_CMD** section, specify the physical drive (command device) on the array:
6. In the **HORCM_LDEV** section, set the necessary parameters. Also, the item MU# must be added after the LU#, and the value must be set as 0 (zero).
7. Save (overwrite) the file.
8. Repeat steps 4 to 7 for the **horcm1.conf** file.
9. Enter the following in the command prompt to verify the connection between CCI and the array.

   Example:

   ```
   C:\>cd horcm\etc
   C:\HORCM\etc>echo hd1-3 | .\inqraid
   Harddisk 1 -> [ST] CL1-A Ser =85000174 LDEV =   0 [HITACHI  ] [DF600F-CM       ]
   Harddisk 2 -> [ST] CL1-A Ser =85000174 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 =85000174 LDEV =   2 [HITACHI  ] [DF600F          ]
             HORC = SMPL  HOMRCF[MU#0 = SMPL  MU#1 = NONE  MU#2 = NONE]
             RAID5[Group 2-0] SSID = 0x0000
   C:\HORCM\etc>
   ```

Setting the environment variable

To perform the 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. Issue 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      85000174     1  E E E E E   E E E E E      0
   ```

   Preparing for Data Retention Utility operation is now complete.

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).

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

1. Execute the **raidvchkset** command to set the attribute.

   Example:

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

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

   Example:

   ```
   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         85000174    3  E E D D D   E E E D D    365
   VG01   oradb2   Unknown         85000174    4  E E E E E   E E E E E     -
   The attribute type is changed.
   ```

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**.

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: The 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.

   Example:

   ```
   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         85000174     1  E E D D D   E E E D D     365
   ```

2. Issue 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.

   Example:

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

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

   Example:

   ```
   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          85000174     1  E E D D D   E E E D D     730
```

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

Glossary

This glossary provides definitions of general storage networking terms as well as specific terms related to the technology that supports Hitachi Data Systems products. Click the letter of the glossary section to display that page.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1000BASE-T

A specification for Gigabit Ethernet over copper wire. The standard defines 1 Gbps data transfer over distances of up to 100 meters using four pairs of Category 5 balanced copper cabling and a 5-level coding scheme.

Array

A set of hard disks grouped logically together to function as one contiguous storage space.

ATA

Advanced Technology Attachment, a disk drive implementation that integrates the controller on the disk drive.

BIOS

Basic Input Output System, built-in software code that determines the functions that a computing device can perform without accessing programs from a disk.

Bps

Bits per second, the standard measure of data transmission speeds.

BSD syslog protocol

This protocol has been used for the transmission of event notification messages across networks for many years. While this protocol was originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, its value to operations and management has led it to be ported to many other operating systems as well as being embedded into many other networked devices.

Cache

A temporary, high-speed storage mechanism. It is 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.

Capacity

The amount of information (usually expressed in megabytes) that can be stored on a disk drive. It 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.

Challenge Handshake Authentication Protocol

A security protocol that requires users to enter a secret for access.

CHAP

See Challenge Handshake Authentication Protocol.

command control interface (CCI)

Hitachi's Command Control Interface software provides command line control of Hitachi array and software operations through the use of commands issued from a system host. Hitachi’s CCI also provides a scripting function for defining multiple operations.

command line interface (CLI)

A method of interacting with an operating system or software using a command line interpreter. With Hitachi’s Storage Navigator Modular Command Line Interface, CLI is used to interact with and manage Hitachi storage and replication systems.

DHCP

Dynamic Host Configuration Protocol, allows a computer to join an IP-based network without having a pre-configured IP address. DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network.

Differential Management Logical Unit (DMLU)

The volumes used to manage differential data in a storage system. In a TrueCopy Extended Distance system, there may be up to two DM logical units configured per storage system. For Copy-on-Write and ShadowImage, the DMLU is an exclusive volume used for storing data when the array system is powered down.

Duplex

The transmission of data in either one or two directions. Duplex modes are full-duplex and half-duplex. Full-duplex is the simultaneous transmission of data in two direction. For example, a telephone is a full-duplex device, because both parties can talk at once. In contrast, a walkie-talkie is a half-duplex device because only one party can transmit at a time.

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.

FC

Fibre channel.

Firmware

Software embedded into a storage device. It may also be referred to as Microcode.

Full-duplex

The concurrent transmission and the reception of data on a single link.

Gbps

Gigabit per second.

GUI

Graphical user interface.

HBA

Host bus adapter, a circuit board and/or integrated circuit adapter installed in a workstation or server that provides input/output processing and physical connectivity between a server and a storage device. An iSCSI HBA implements the iSCSI and TCP/IP protocols in a combination of a software storage driver and hardware.

HDD

Hard disk drive.

Initiator

A system component that originates an I/O command over an I/O bus or network, such as an I/O adapters or network interface cards.

I/O

Input/output.

# A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

IP

Internet Protocol, specifies the format of packets and addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255 (for example, 192.168.0.200).

IP-SAN

Block-level Storage Area Networks over TCP/IP using the iSCSI protocol.

iSCSI

Internet SCSI, an IP-based standard for connecting data storage devices over a network and transferring data using SCSI commands over IP networks. iSCSI enables a Storage Area Network to be deployed in a Local Area Network.

iSNS

Internet Storage Name Service, a protocol that allows automated discovery, management and configuration of iSCSI devices on a TCP/IP network.

L

LAN

Local Area Network, a computer network that spans a relatively small area, such as a single building or group of buildings.

LU

Logical unit.

LUN

Logical unit number.

Middleware

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.

MIB

Message Information Block.

NIC

Network Interface Card, an expansion board in a computer that allows the computer to connect to a network.

NTP

Network Time Protocol, a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP port 123 as its transport layer. It is designed particularly to resist the effects of variable latency (jitter).

Pool volume

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

primary volume (P-VOL)

The storage volume in a volume pair. It is 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).

RAID

Redundant Array of Independent Disks, a disk array in which part of the physical storage capacity is used to store redundant information about user data stored on the remainder of the storage capacity. The redundant information enables regeneration of user data in the event that one of the array's member disks or the access path to it fails. SNIA.

RAID 6

An extension of the RAID 5 array, that allows for two simultaneous drive failures without downtime or data loss.recovery point objective (RPO).

After a recovery operation, the recovery point objective (RPO) is the maximum desired time period, prior to a disaster, in which changes to data may be lost. This measure determines up to what point in time data should be recovered. Data changes preceding the disaster are preserved by recovery.

SAN

Storage Area Network, a network of shared storage devices that contain disks for storing data.

SAS

Serial Attached SCSI, an evolution of parallel SCSI into a point-to-point serial peripheral interface in which controllers are linked directly to disk drives. SAS delivers improved performance over traditional SCSI because SAS enables up to 128 devices of different sizes and types to be connected simultaneously.

SATA

Serial ATA is a computer bus technology primarily designed for the transfer of data to and from hard disks and optical drives. SATA is the evolution of the legacy Advanced Technology Attachment (ATA) interface from a parallel bus to serial connection architecture.

SCSI

Small Computer System Interface, a parallel interface standard that provides faster data transmission rates than standard serial and parallel ports.

Session

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 is the exchange of data between groups of primary and secondary volumes.

secondary volume (S-VOL)

A replica of the primary volume (P-VOL) at the time of a backup and is kept on a standby storage system. Recurring differential data updates are performed to keep the data in the S-VOL consistent with data in the P-VOL.

SMTP

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

Software initiator

A software application initiator communicates with a target device. A software initiator does not require specialized hardware because all processing is done in software, using standard network adapters.

Storage Navigator Modular 2

A multi-featured scalable storage management application that is used to configure and manage the storage functions of Hitachi arrays. Also referred to as Navigator 2.

Subnet

In computer networks, a subnet or subnetwork is a range of logical addresses within the address space that is assigned to an organization. Subnetting is a hierarchical partitioning of the network address space of an organization (and of the network nodes of an autonomous system) into several subnets. Routers constitute borders between subnets. Communication to and from a subnet is mediated by one specific port of one specific router, at least momentarily. SNIA.

Switch

A network infrastructure component to which multiple nodes attach. Unlike hubs, switches typically have internal bandwidth that is a multiple of link bandwidth, and the ability to rapidly switch node connections from one to another. A typical switch can accommodate several simultaneous full link bandwidth transmissions between different pairs of nodes. SNIA.

Target

Devices that receive iSCSI requests that originate from an iSCSI initiator.

TOE

A dedicated chip or adapter that handles much of the TCP/IP processing directly in hardware. TCP/IP transmission is inherently a CPU-intensive operation. Therefore, using dedicated hardware that can operate in parallel with the main processor allows for superior system performance. Although all iSCSI HBAs have a TOE, a generic TOE only implements TCP/IP, while an iSCSI HBA implements the iSCSI protocol in addition to TCP/IP.

User Datagram Protocol (UDP)

UDP is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagrams (using Datagram Sockets) to one another.

UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order, appear duplicated, or go missing without notice. Avoiding the overhead of checking whether every packet actually arrived makes UDP faster and more efficient, at least for applications that do not need guaranteed delivery. Time-sensitive applications often use UDP because dropped packets are preferable to delayed packets. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients. Unlike TCP, UDP is compatible with packet broadcast (sending to all on local network) and multicasting (send to all subscribers).

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 logical unit or a group of logical units.

Index

Hitachi Data Systems

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com

Hitachi Data Systems

MK-97DF8019-02