Overland Storage

SnapSAN™ Compliance (WORM)

User Guide

S5000

January 2013

10400415-002

The names of companies and individuals used in examples are fictitious and intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is coincidental.

PROPRIETARY NOTICE

All information contained in or disclosed by this document is considered proprietary by Overland Storage. By accepting this material the recipient agrees that this material and the information contained therein are held in confidence and in trust and will not be used, reproduced in whole or in part, nor its contents revealed to others, except to meet the purpose for which it was delivered. It is understood that no right is conveyed to reproduce or have reproduced any item herein disclosed without express permission from Overland Storage.

Overland Storage provides this manual as is, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Overland Storage may make improvements or changes in the product(s) or programs described in this manual at any time. These changes will be incorporated in new editions of this publication.

Overland Storage assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of this manual, nor for any problem that might arise from the use of the information in this manual.

Preface

This user guide explains WORM which is a function for disabling write operations on volumes for a specified time period; a function for controlling access permissions and WORM periods in a disk array. This guide assumes that you are familiar with computer hardware, data storage, and network administration terminology and tasks. It also assumes you have basic knowledge of Internet SCSI (iSCSI), Serial-attached SCSI (SAS), Serial ATA (SATA), Storage Area Network (SAN), and Redundant Array of Independent Disks (RAID) technology.

This guide assumes that you are familiar with computer hardware, data storage, and network administration terminology and tasks. It also assumes you have basic knowledge of Internet SCSI (iSCSI), Serial-attached SCSI (SAS), Serial ATA (SATA), Storage Area Network (SAN), and Redundant Array of Independent Disks (RAID) technology.

Product Documentation and Firmware Updates

Overland Storage SnapSAN product documentation and additional literature are available online, along with the latest release of the SnapSAN 3000/5000 software.

Point your browser to:

http://docs.overlandstorage.com/snapsan

Follow the appropriate link to download the **latest** software file or document. For additional assistance, search at http://support.overlandstorage.com.

Overland Technical Support

For help configuring and using your SnapSAN 3000/5000, search for help at:

http://support.overlandstorage.com/kb

You can email our technical support staff at techsupport@overlandstorage.com or get additional technical support information on the Contact Us web page:

http://www.overlandstorage.com/company/contact-us/

For a complete list of support times depending on the type of coverage, visit our web site at:

http://support.overlandstorage.com/support/overland_care.html

Conventions

This user guide exercises several typographical conventions:

Convention	Description & Usage
Boldface	Words in a boldface font (**Example**) indicate items to select such as menu items or command buttons.
Ctrl-Alt-r	This type of format details the keys you press simultaneously. In this example, hold down the **Ctrl** and **Alt** keys and press the **r** key.
NOTE	A Note indicates neutral or positive information that emphasizes or supplements important points of the main text. A note supplies information that may apply only in special cases—for example, memory limitations or details that apply to specific program versions.
IMPORTANT ➡	An Important note is a type of note that provides information essential to the completion of a task or that can impact the product and its function.
CAUTION ⚠	A Caution contains information that the user needs to know to avoid damaging or permanently deleting data or causing physical damage to the hardware or system.
WARNING ⚠	A Warning contains information concerning personal safety. Failure to follow directions in the warning could result in bodily harm or death.
Menu Flow Indicator (>)	Words in bold font with a greater than sign between them indicate the flow of actions to accomplish a task. For example, **Setup > Passwords > User** indicates that you should press the Setup button, then the Passwords button, and finally the User button to accomplish a task.

Information contained in this guide has been reviewed for accuracy, but not for product warranty because of the various environments, operating systems, or settings involved. Information and specifications may change without notice.

Contents

Preface

Chapter 1 - WORM

Chapter 2 - Volume List

Chapter 3 - WORM Operations

Chapter 4 - Installation (Windows)

Chapter 5 - Maintenance (Windows)

Chapter 6 - Notes (Windows)

Chapter 7 - Installation (Linux)

Chapter 8 - Maintenance (Linux)

Chapter 9 - Notes (Linux)

Index

Chapter 1

WORM

Overview

WORM - Write Once, Read Many sets access permissions and WORM periods on a volume-by-volume basis to prevent unauthorized data modification or accidental data corruption, offering long-term storage of data in non-falsifiable format. A volume here means any of logical disks bound in a disk array.

Data protection is becoming increasingly important because of the regulations and the like that require business documents and emails to be stored in non-falsifiable format over a specified period of time; WORM function provides base functions for supporting operation management according to data types, including appropriate data storage and access control.

This chapter describes the basics, such as an overview, hardware configuration, and software configuration of WORM function.

WORM is a function for disabling write operations on volumes for a specified time period; a function for controlling access permissions and WORM periods is included in a disk array. When WORM function is implemented at a storage level, it is also possible to prevent data modification with unauthorized access bypassing the OS.

In an empty volume in the archive storage, store business data that needs long-term storage. Then, perform WORM operations to disable write operations from servers for a specified time period. This prevents unauthorized data falsification and accidental data corruption.

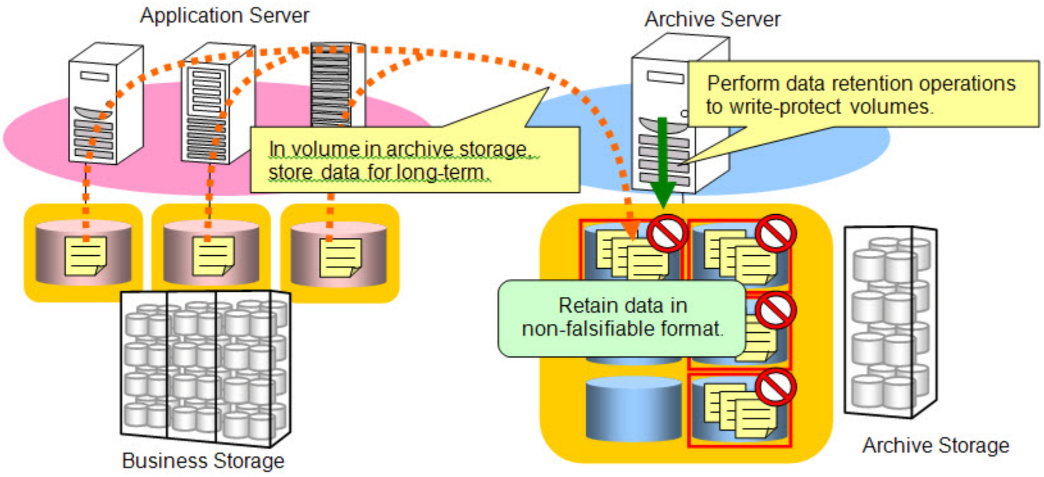

Application Server
Archive Server
Perform data retention operations to write-protect volumes.
In volume in archive storage, store data for long-term.
Retain data in non-falsifiable format.
Business Storage
Archive Storage

Figure 1-1: Overview of WORM Function

System Configuration

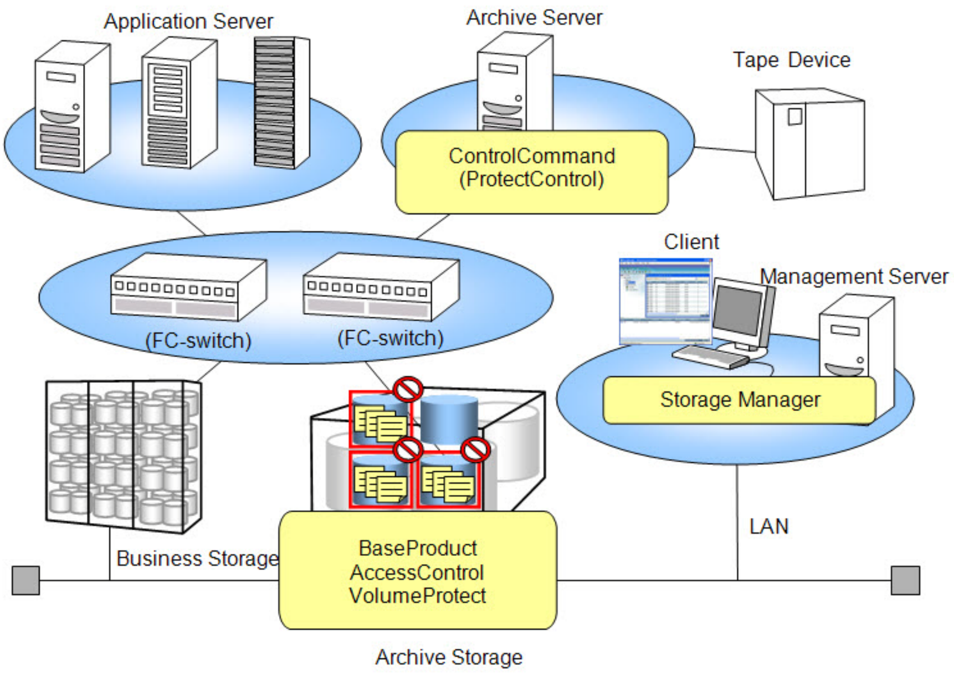


Figure 1-2: System Configuration of WORM Function

Hardware configuration

To install WORM function for use, the following hardware devices are needed.

Archive Storage

A disk array on which WORM function (VolumeProtect) is installed is needed.

Management server/client

A management server, where SnapSAN Manager is installed, monitors disk arrays. This device allows you to manage disk arrays and obtain the state of a protected volume.

Archive Server

Performs tasks including WORM operations and backups of protected volumes. The supported OS is Windows or Linux.

Software configuration

Software that executes WORM function consists of the following components.

VolumeProtect

Provides the function to set access permissions and WORM periods on a volume-by-volume basis to prevent unauthorized data modification or accidental data corruption, offering long-term storage of data in non-falsifiable format.

ControlCommand

Includes ProtectControl.

Provides the function to give operational instructions from the archive server to WORM function (VolumeProtect) using the command line interface.

BaseProduct

BaseProduct includes storage control software that administers basic control of the disk array and SnapSAN Manager software that enables you to monitor states of the disk array basically.

Storage Manager

Provides the functions to display the configuration and state of the disk array.

Also provides the function to display the state of a volume protected by WORM function.

AccessControl

Provides the function to set logical disks that can be accessed for each server.

WORM Operations on Volumes

WORM function allows you to control access permissions to volumes and protect the volumes by setting three attributes below on a volume-by-volume basis.

Protection States

Attribute set by a WORM operation on a volume-by-volume basis; this attribute is a permission indicating whether to enable I/O from a server.

Retention Period

Attribute set by a WORM operation on a volume-by-volume basis; this attribute is a period during which release of protection from the target volume is disabled.

Retention Mode

Attribute set by a WORM operation on a volume-by-volume basis; this attribute is a definition of constraints governing resetting the protection state and retention period of the target volume.

When you release protection from a protected volume to make the volume accessible again, you can use the volume reinitialization function to clear the stored data from the volume.

Protection States

A protection state is an attribute set by a WORM operation on a volume-by-volume basis; this attribute is a permission indicating whether to enable I/O from a server.

Setting Protection States

When setting protection for a volume, you can set the protection state of the volume to ReadOnly or NotAccessible. When the protection state is set to ReadOnly, the volume is read-only from a server. When the protection state is set to NotAccessible, the volume is read/write-protected from the server, indicating the volume is not accessible. Setting a protection state during volume protection setting disables write operations from the server to prevent unauthorized data modification or accidental data corruption.

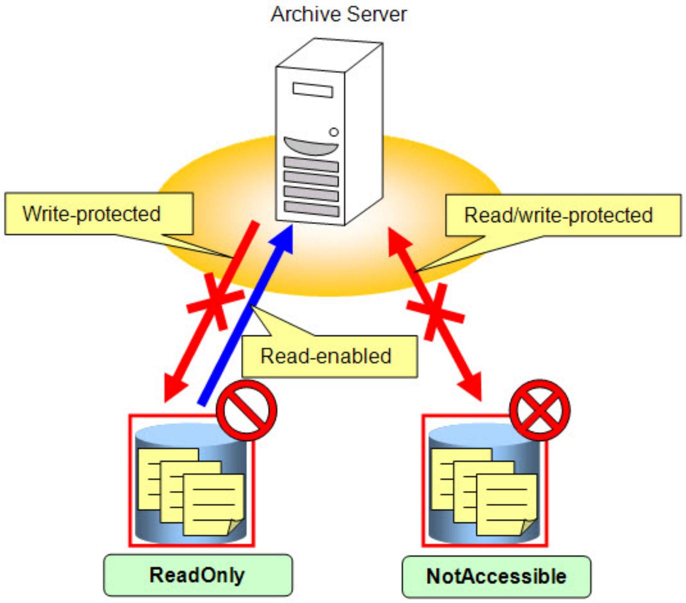


Figure 1-3: Protection States

Protection State	Volume State	I/O-Enabled/Disabled
ReadOnly (RO)	Protected	Read-enabled and write-protected from server
NotAccessible (NA)	Protected	Read/write-protected from server

To allow reference to protected data after volume protection setting, a protection state must be set to ReadOnly. To disallow reference to protected data to maintain the confidentiality of the data after volume protection setting, set a protection state to NotAccessible.

When you set protection for a volume and set the protection state of the volume to ReadOnly, note the following during operation:

<On the Linux system>

A file system must be mounted as read-only.

Changing Protection States

When you change protection settings of a volume, you can switch the protection state of the volume from ReadOnly to NotAccessible, or from NotAccessible to ReadOnly. If the retention mode is set to strict, however, the protection state cannot be changed.

Releasing Protection States

When you release protection from a volume, the protection state is released from the volume. The volume from which the protection state has been released is made read/write-enabled from the server again.

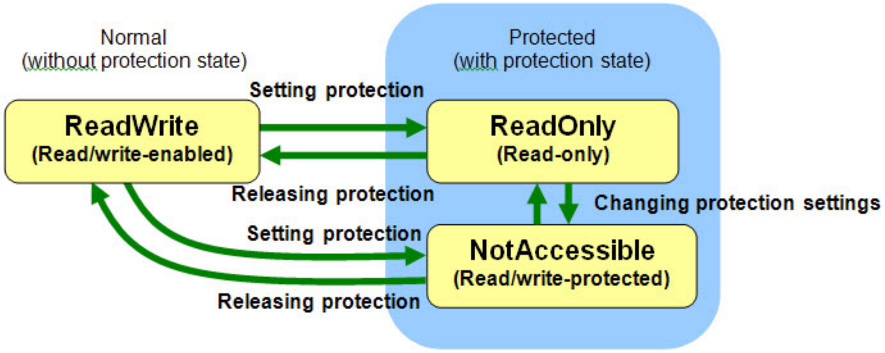


Figure 1-4: Protection State Transition

Retention Periods

A retention period is an attribute set by a WORM operation on a volume-by-volume basis; this attribute is a period during which release of protection from the target volume is disabled.

Setting Retention Periods

When setting protection for a volume, you can set the retention period of the volume. During the retention period, protection cannot be released from the volume. If the retention mode is set to normal, however, volume protection can be released even during the retention period. There are three options for volume retention periods: duration-designated, date-designated, and permanent.

- For the duration-designated option, the retention period of the volume is set as the specified duration starting at the current date.
- For the date-designated option, the retention period of the volume is set as the time until the specified date.
- For the permanent option, the retention period of the volume is set as permanent.

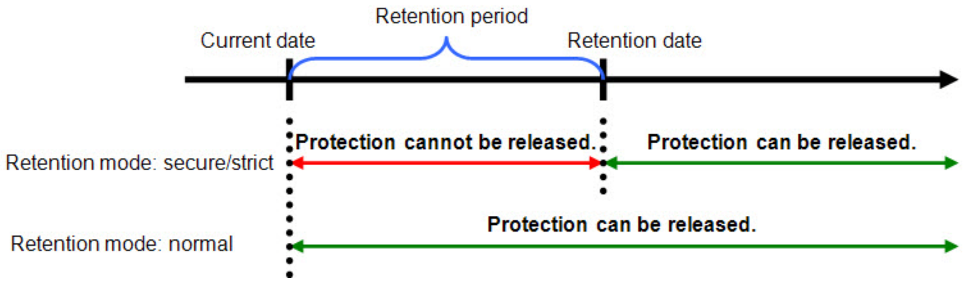

Retention period
Current date
Retention date
Protection cannot be released.
Protection can be released.
Retention mode: secure/strict
Protection can be released.
Retention mode: normal

Figure 1-5: Retention Periods Specifiable for Volumes

Changing Retention Periods

When you change protection settings, whether or how the retention period can be changed depends on the retention mode already set for the target volume. When the retention mode is normal, the retention period of the volume can be changed. When the retention mode is secure, the retention period of the volume can only be extended. When the retention mode is strict, the retention period of the volume cannot be changed.

Releasing Retention Periods

When you release protection from a volume, the retention period is released from the volume.

Retention Modes

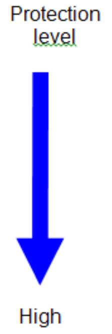
A retention mode is an attribute set by a WORM operation on a volume-by-volume basis; this attribute is a definition of constraints governing resetting the protection state and retention period of the target volume.

Setting Retention Modes

When setting protection for a volume, you can set the retention mode of the volume to normal, secure, or strict. When the retention mode is set to normal, you can release protection from the volume and change the protection settings at any time. When the retention mode is set to secure, you cannot release protection from the volume until the retention period has elapsed, but you can change the protection state or extend the retention period on the condition that data is protected. When the retention mode is set to strict, you cannot release protection from the volume or change the protection settings until the retention period has elapsed.

When the retention mode is normal, you can freely set protection to suit your operation type without constraints on releasing or changing protection settings, even if you set the retention period of a volume. When the retention mode is secure or strict, the protection function conformable to the WORM regulations is provided. Release of protection is disabled until the retention period has elapsed, and the data integrity is ensured at a storage level over the retention period.

Retention Mode	Operation Overview	Description
normal	During the retention period, protection can be released. Settings can also be changed.	Flexible volume-protected operation can be performed which allows you to release protection or change protection settings freely, to suit your operation type.
secure	During the retention period, protection cannot be released. There are constraints on changing settings.	Volume-protected operation can be performed which ensures the data integrity over the retention period and conforms to the WORM regulations.
strict	During the retention period, protection cannot be released. Settings cannot be changed, either.	Strict volume-protected operation can be performed which ensures the data integrity over the retention period and conforms to the WORM regulations.



Retention Mode	Protection	Protection State	Retention Period	Retention Mode
normal	Can be released at any time	Can be changed between RO Û NA	Can be changed	Can be changed to secure or strict
secure	Can be released after the elapse of the retention period	Can be changed between RO Û NA	Can only be extended	Can be changed to strict
strict	Can be released after the elapse of the retention period	Cannot be changed	Cannot be changed	Cannot be changed

Changing Retention Modes

When you change protection settings, whether or how the retention mode already set for the target volume can be changed depends on that retention mode. When the retention mode of the volume is normal, it can be changed to secure or strict. When the retention mode of the volume is secure, it can be changed only to strict. When the retention mode of the volume is strict, it cannot be changed.

Releasing Retention Modes

When you release protection from a volume, the retention mode is released from the volume.

Volume Reinitialization

Volume reinitialization is a function for reinitializing a volume and clearing the stored data when protection is released from the volume. If the target volume is not being used by the data replication function, when performing a protection release operation, you can specify whether to use volume reinitialization. The confidentiality of protected data can be maintained by clearing the data.

When you use volume reinitialization, initialization continues for a volume even after protection has been completely released from the volume.

You can check information about the progress of volume initialization by performing command operations from the server that has ProtectControl installed or using the GUI of SnapSAN Manager.

During initialization, the volume is read/write-protected and cannot be accessed from a server.

Volume reinitialization clears all data, including the management information (such as partition information) about the OS of the target volume.

WORM Operations

WORM operations below are provided for volumes.

Setting Volume Protection

This function is used to set the protection state, retention period, and retention mode for a volume, and disable write operations from a server for a specified time period.

Changing Volume Protection Settings

This function is used to change the protection state, retention period, and retention mode set for a volume. However, there may be constraints on changing settings, depending on the set retention mode.

Releasing Volume Protection

This function is used to release volume protection. When protection is released, the protection state set for a volume is released, and the volume is made read/write-enabled from a server again. Upon protection release, the stored data can also be cleared from the volume.

Displaying Volume Protection Information

This function is used to display information about protection (protection state, retention period, begin date, and retention mode) set for a volume.

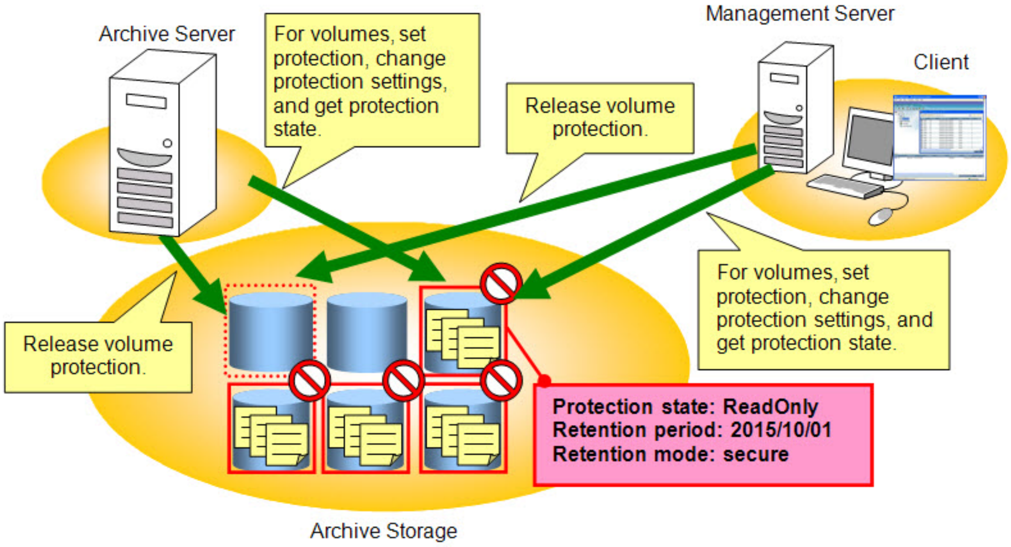

Archive Server
For volumes, set protection, change protection settings, and get protection state.
Management Server
Client
Release volume protection.
For volumes, set protection, change protection settings, and get protection state.
Release volume protection.
Protection state: ReadOnly
Retention period: 2015/10/01
Retention mode: secure
Archive Storage

Figure 1-6: WORM Operations

Volume Protection Settings

This function is used to set the protection state, retention period, and retention mode for a volume, and disable write operations from a server for a specified time period.

The protection state specifies whether to enable I/O on the volume from the server. The retention period specifies the duration for which to disable release of volume protection. The retention mode defines constraints governing resetting the protection state and retention period of the volume.

You can set volume protection by command operations from the archive server that has ProtectControl installed or GUI operations with SnapSAN Manager.

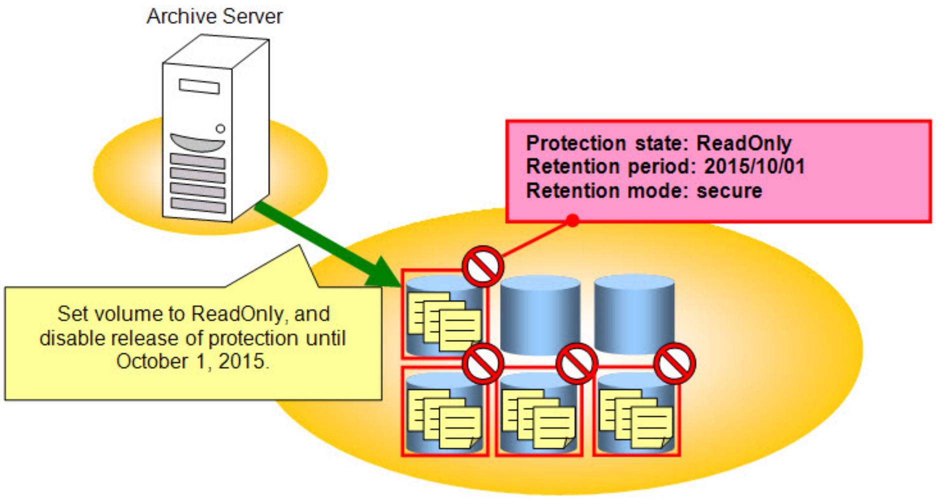

Archive Server
Protection state: ReadOnly
Retention period: 2015/10/01
Retention mode: secure
Set volume to ReadOnly, and disable release of protection until October 1, 2015.

Figure 1-7: Setting Volume Protection

To set volume protection, the following conditions must be satisfied.

- The target volume is not being used by the snapshot function.
- The target volume is unmounted.
- If the target volume is paired as MV or RV for replication, replication must be in the Separated state.
- The target volume is registered in the volume list (only for command operations).
- Alternatively, if the target volume is paired as RV for replication, the MV to be paired with the RV must be registered in the volume list (only for command operations).
- The volume list is not being created or refreshed (only for command operations).

Changing Volume Protection Settings

This function is used to change the protection state, retention period, and retention mode set for a volume. However, there may be constraints on changing settings, depending on the set retention mode.

Which protection setting changes are allowed can be specified by the retention mode set for the target volume.

You can change the volume protection settings by command operations from the archive server that has ProtectControl installed or GUI operations with SnapSAN Manager.

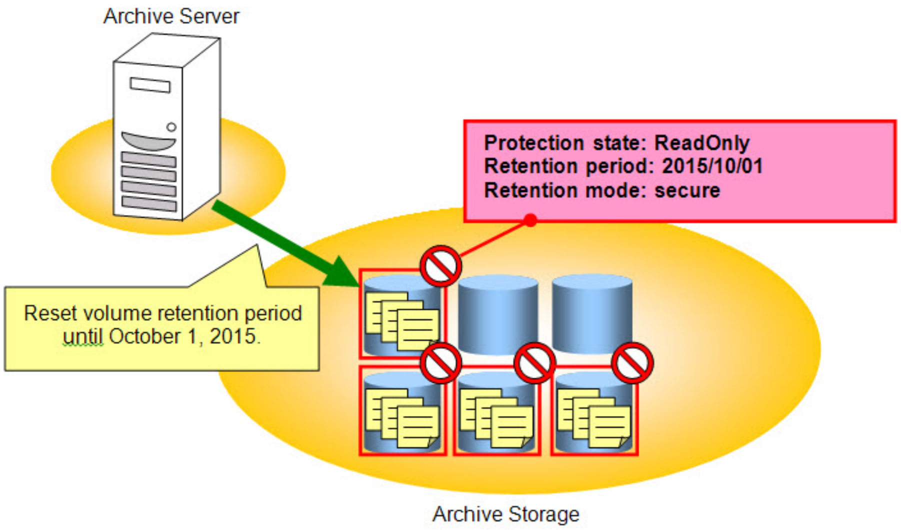

Archive Server
Protection state: ReadOnly
Retention period: 2015/10/01
Retention mode: secure
Reset volume retention period until October 1, 2015.
Archive Storage

Figure 1-8: Changing Volume Protection Settings

To change volume protection settings, the following conditions must be satisfied.

The target volume is not being used by the snapshot function.

The target volume is unmounted.

If the target volume is paired as MV or RV for replication, replication must be in the Separated state.

The target volume is registered in the volume list (only for command operations).

Alternatively, if the target volume is paired as RV for replication, the MV to be paired with the RV must be registered in the volume list (only for command operations).

The volume list is not being created or refreshed (only for command operations).

Releasing Volume Protection

This function is used to release volume protection. When protection is released, the protection state set for a volume is released, and the volume is made read/write enabled from a server again.

When releasing protection from a volume, you can use the data clear function to maintain the confidentiality of the data stored in the volume.

You can release volume protection by command operations from the archive server that has ProtectControl installed or GUI operations with SnapSAN Manager.

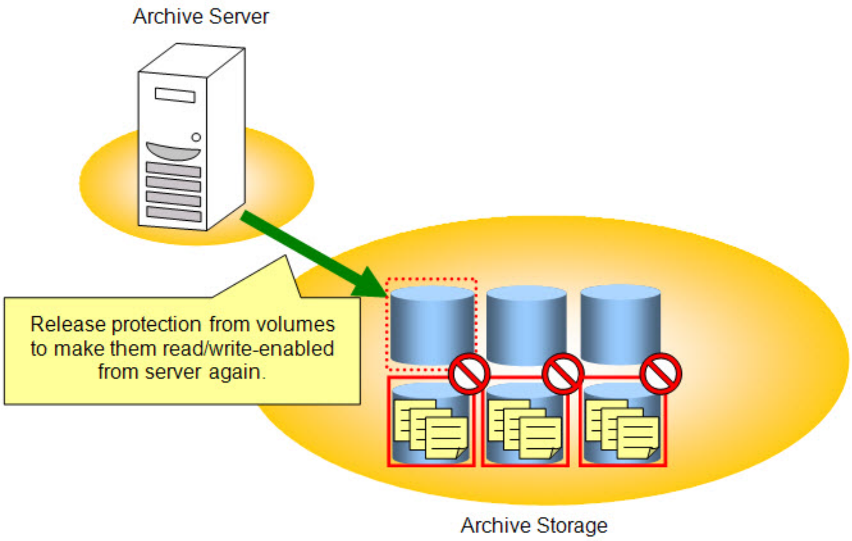

Archive Server
Release protection from volumes to make them read/write-enabled from server again.
Archive Storage

Figure 1-9: Releasing Volume Protection

To release volume protection, the following conditions must be satisfied.

- The target volume is protected.
- The target volume is not being used by the snapshot function.
- The target volume is unmounted.
- If the target volume is paired as MV or RV for replication, replication must be in the Separated state.
- The volume being used by the data replication function cannot be reinitialized.
- The target volume is registered in the volume list (only for command operations).
- Alternatively, if the target volume is paired as RV for replication, the MV to be paired with the RV must be registered in the volume list (only for command operations).
- The volume list is not being created or updated (only for command operations).

Displaying Volume Protection Information

This function is used to display information about protection (protection state, retention period, begin date, and retention mode) set for a volume, as well as information about the progress of the data clear function.

To display volume protection information, you can perform command operations from the archive server that has ProtectControl installed or perform GUI operations from SnapSAN Manager.

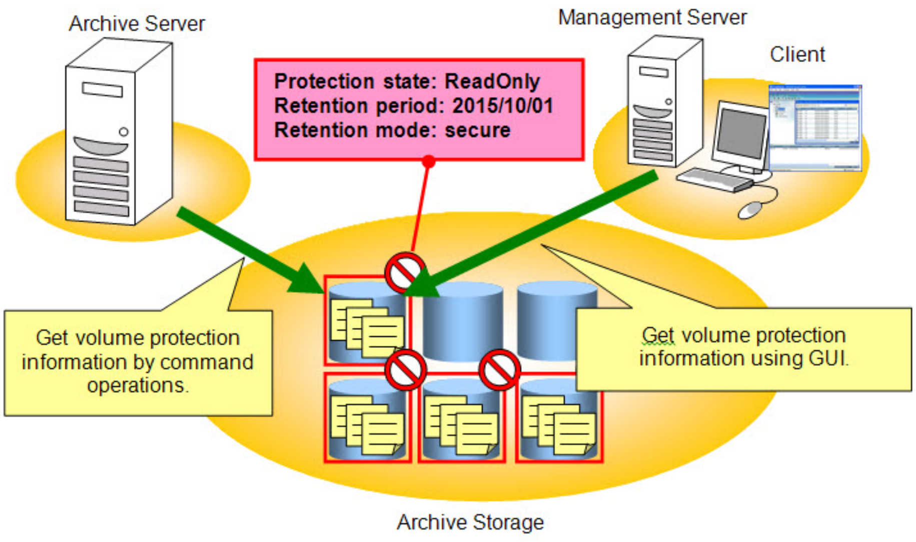

Archive Server
Management Server
Client
Protection state: ReadOnly
Retention period: 2015/10/01
Retention mode: secure
Get volume protection information by command operations.
Get volume protection information using GUI.
Archive Storage

Figure 1-10: Displaying Volume Protection Information

To display volume protection information, the following conditions need to be satisfied.

The target volume or the volume to be paired with the target volume is registered in the volume list (only for command operations).

The volume list is not being created or updated (only for command operations).

Concurrent Use With Replication Function

This section describes the effects and methods when the data replication function and the WORM function are concurrently used.

The data replication is a function to create a Replication Volume (RV) of Master Volume (MV). Since the replication volume is physically independent from the master volume, it is suitable for the secondary use of volume, backup operation, and other operations requiring high performance and high reliability.

The WORM function enables to disable write operations to the volumes for a specified time period, control the access permissions and WORM period, and prevent unauthorized data modification or accidental data corruption to achieve long-term storage of data in non-falsifiable format.

Back up the data to be stored for a long term by the data replication function and then protect the replication volume for a specified time period by the WORM operations. By this means, you can prevent data corruption by physical failure of volumes and logical data corruption by illegal data falsification or mis-operation.

Concurrent Operation with Replication Function

<Creating replication>

Synchronously back up the data updated every day to RV by the data replication function.

Perform the separation operation regularly (for example, once per month) to create a replication to RV. This enables to respond to the physical faults of the master volume.

Predetermine the validity period of replication and protect the replication RV for a specified period by the WORM function. This enables to respond to the logical data corruption including unauthorized data modification and mis-operation to the replication.

After the validity period expired, the replication RV can be reused by the data replication function.

<Merits of concurrent use method>

Regularly creating a replication RV by the data replication enables to recover a physical fault quickly (restore from the RV).

Predetermine the validity period of replication and protect the created replication RV for a specified period by the WORM function. This enables to prevent logical data correction including unauthorized data modification or mis-operation to the RV during the validity period.

After the validity period expired, the replication RV can be reused by the data replication function.

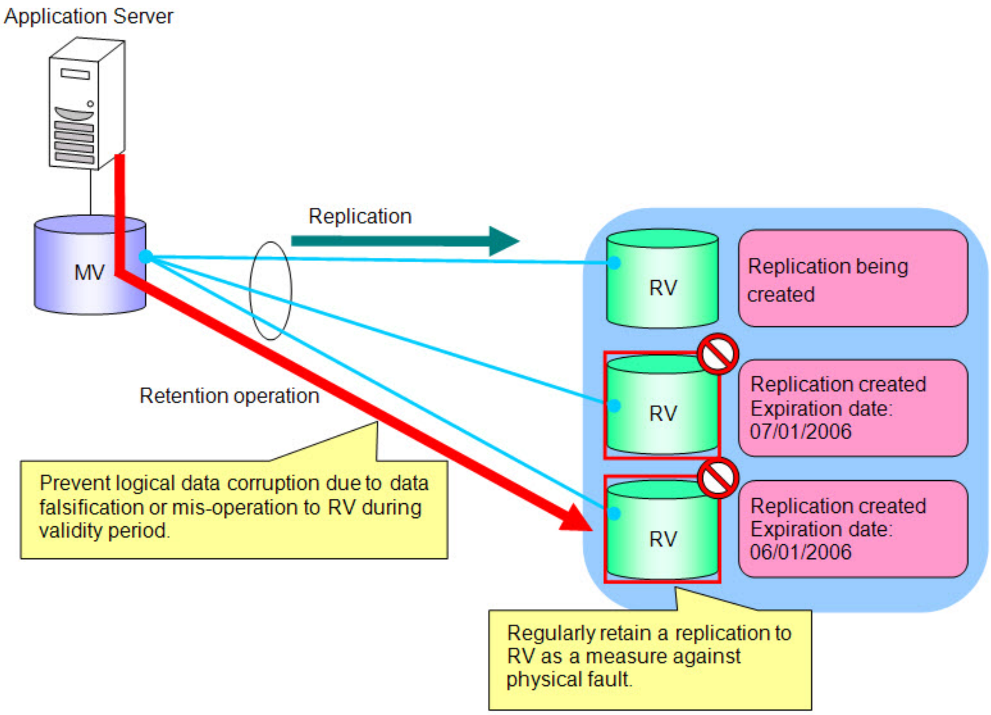

Application Server
Replication
MV
Retention operation
RV
RV
RV
Replication being created
Replication created Expiration date: 07/01/2006
Replication created Expiration date: 06/01/2006
Prevent logical data corruption due to data falsification or mis-operation to RV during validity period.
Regularly retain a replication to RV as a measure against physical fault.

Figure 1-11: Concurrent Use

Concurrent Use with Replication

This subsection describes the execution conditions of each operation when the WORM function and the replication function are concurrently used.

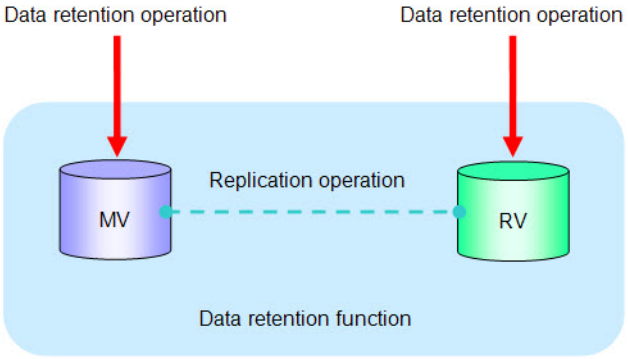


Figure 1-12: Concurrent Use Replication Operation

WORM operations and replication status

For the WORM operations to MV or RV, the execution conditions are defined depending on the replication status of pair of MV and RV.

Status	MV			
Operation	Replication	Separation		Restoration
	rpl/preparing rpl/exec, rpl/sync	sep/preparing sep/exec	separated	rst/preparing rst/exec, rst/sync
Setting protection	-	-	P	-
Changing protection setting	-	-	P	-
Releasing protection (not reinitializing)	-	-	P	-
Releasing protection (reinitializing)	-	-	-	-
Referencing protection information	P	P	P	P

P: Can be executed   -: Cannot be executed

*In Separate (immediate) (separation that makes RV available immediately), it is possible to use RV even during separate execution (sep/exec), as reflecting the difference between MV and RV into RV. Since the data has not been established, however, when performing a protection operation, the state needs to be in the separated state. In the case of forced separate (cancel) or separate due to fault, the RV data becomes invalid and the protection operation cannot be performed to RV.

Replication Operations and Worm Status

For the replication operations to the pair, of which MV or RV is protected by the WORM function, the execution conditions are defined depending on the protection status of MV or RV.

Status	Protection Status of Volume			
Operation	MV : Not protected	MV : Not protected	MV : Protected (RO)	Other than those on the left
	RV : Not protected	RV : Protected (RO)	RV : Not protected	
Replication	✓	-	✓	-
Separation	✓	-	✓	-
Restoration	✓	✓	-	-

✓: Can be executed   - : Cannot be executed

Other notes

WORM operation cannot be performed to a logical disk belonging to an Atomic Group.

A volume being used by the data replication function cannot be reinitialized by the WORM function.

Chapter 2

Volume List

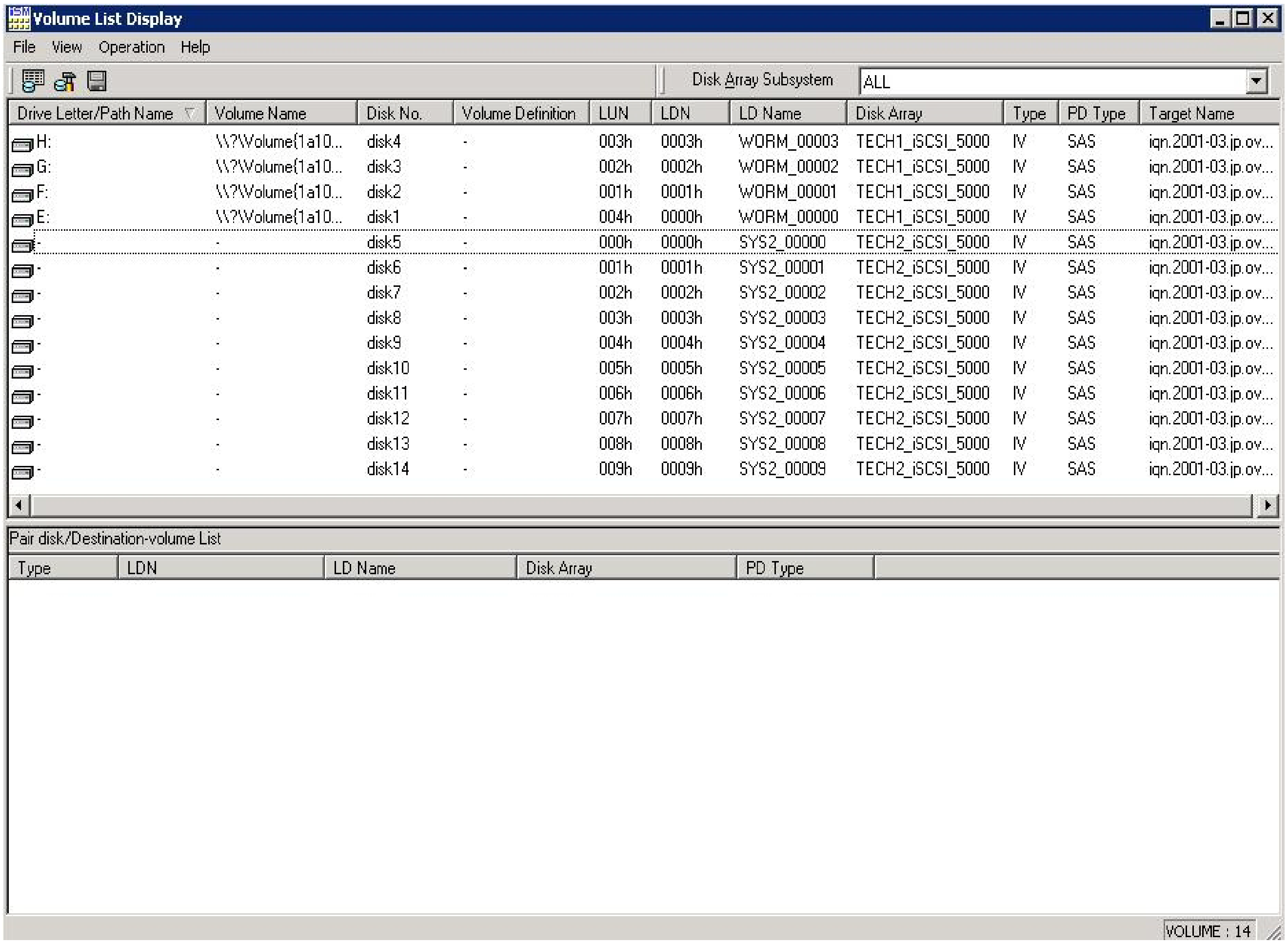
Start/Terminate Volume List

On the Windows system, the volume list creation and display function can be used via the GUI. The GUI functions include volume list display, selective display of disk arrays, and creation and update of the volume list.

The function to define control volumes used for the application server to operate the WORM function is also provided.

Screen Configuration

To create or display the volume list with GUI, use the Volume List Display screen. The following is the layout of the Volume List Display screen.



Drive Letter/Path Name	Volume Name	Disk No.	Volume Definition	LUN	LDN	LD Name	Disk Array	Type	PD Type	Target Name
H:	\\?\Volume{1a10...	disk4	-	003h	0003h	WORM_00003	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
G:	\\?\Volume{1a10...	disk3	-	002h	0002h	WORM_00002	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
F:	\\?\Volume{1a10...	disk2	-	001h	0001h	WORM_00001	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
E:	\\?\Volume{1a10...	disk1	-	004h	0000h	WORM_00000	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk5	-	000h	0000h	SYS2_00000	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk6	-	001h	0001h	SYS2_00001	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk7	-	002h	0002h	SYS2_00002	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk8	-	003h	0003h	SYS2_00003	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk9	-	004h	0004h	SYS2_00004	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk10	-	005h	0005h	SYS2_00005	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk11	-	006h	0006h	SYS2_00006	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk12	-	007h	0007h	SYS2_00007	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk13	-	008h	0008h	SYS2_00008	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk14	-	009h	0009h	SYS2_00009	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...

Pair disk/Destination-volume List

Type	LDN	LD Name	Disk Array	PD Type

VOLUME : 14

Figure 2-1: Layout of Volume List Display

Title bar

Displays the title of the Volume List Display function.

Menu bar

Toolbar buttons

Toolbar Button	Description
Create/Update Volume List	Clicking this button has the same effect as selecting Create/Update Volume List from the menu.
Define Control Volume	Clicking this button has the same effect as selecting Define Control Volume from the menu.
CSV Output of Information List	Clicking this button has the same effect as selecting CSV Output of Information List from the menu.

Pair disk/Destination-volume List

Displays the volume information of pair disks set by the data replication function, or the volume information of destination-volumes linked by the snapshot function, for the volume selected on the screen of Volume List Display. The information is acquired from the disk array.

Status bar

The following information appears on the status bar.

VOLUME: Displays the number of volume information items to be displayed on the Volume List Display screen. If volume information of all disk arrays is displayed, the number of volume information items in the volume list is displayed. For display by narrowing down disk arrays, the number of volume information items of the disk array is displayed.

Disk Array Selection Combo box

Clicking the pull-down button displays the list of disk arrays currently registered in the volume list file.

Drive Letter/Path Name

Displays path information in the volume list file.

Icon	Description
	Indicates logical disks that can be used from the server.
CTL	Indicates logical disks defined as control volumes.

Icon	Description
CTL	Indicates that logical disks which were defined as control volumes are in an inappropriate state. The following is the corresponding operations. • Setting the control volume in a pair as an RV • Specifying the control volume as a base-volume (BV) by adding a snapshot generation to it • Making the control volume usable from the server by building a link-volume (LV) with the same logical disk number as for the control volume • Making the control volume unusable from the server by canceling Access Control or unbinding the volume • Making unrecognizable the disk array to which the defined control volume belongs ”.

Volume Name

Displays volume names in the volume list file.

Disk No.

Displays physical disk numbers in the volume list file.

Volume Definition

Displays the identification information of control volume definition.

LUN

Displays logical unit numbers in the volume list file.

LDN

Displays logical disk numbers in the volume list file.

LD Name

Displays logical disk names in the volume list file.

Disk Array

Displays disk array names in the volume list file.

Type

Displays the type (volume attribute) of volumes regarding data replication and snapshot by obtaining from a disk array.

Display	Description
FC	Indicates that the physical disk type is FC.
SAS	Indicates that the physical disk type is SAS.
SSD	Indicates that the physical disk type is SSD.
SAS(SED)	Indicates that the physical disk type is encrypted SAS.
NLSAS	Indicates that the physical disk type is nearline SAS.

Target Name

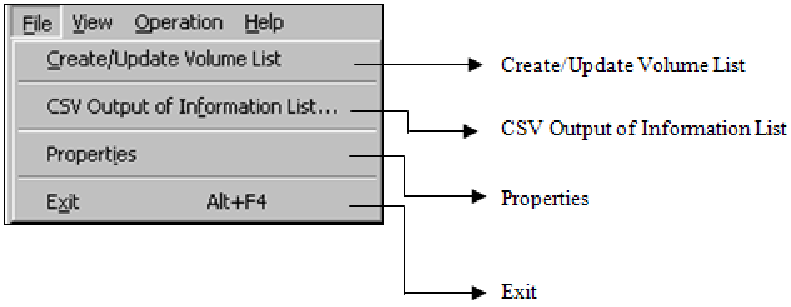
Displays Target information of the logical disk.

The information items are displayed by obtaining from a disk array.

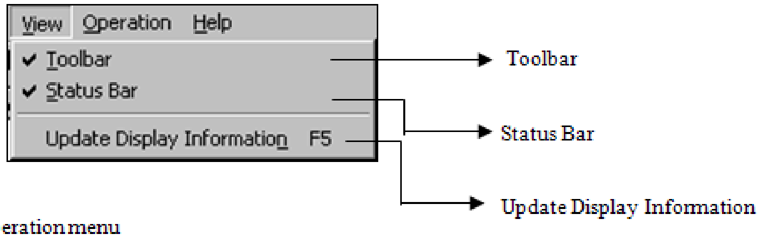
Menu Item List

This section describes the items on the menu bar of the Volume List Display screen.

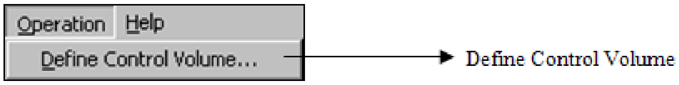
- File menu


File
View
Operation
Help
Create/Update Volume List
CSV Output of Information List...
Properties
Exit
Alt+F4
Create/Update Volume List
CSV Output of Information List
Properties
Exit

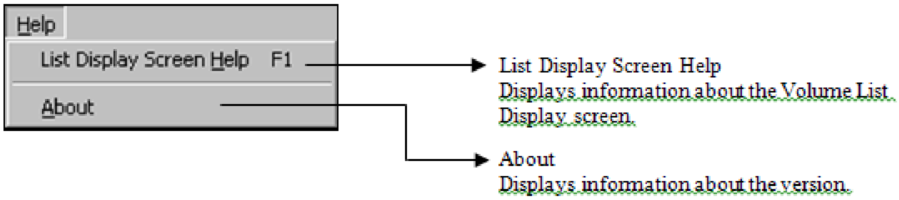
- View menu



- Operation menu



- Help menu

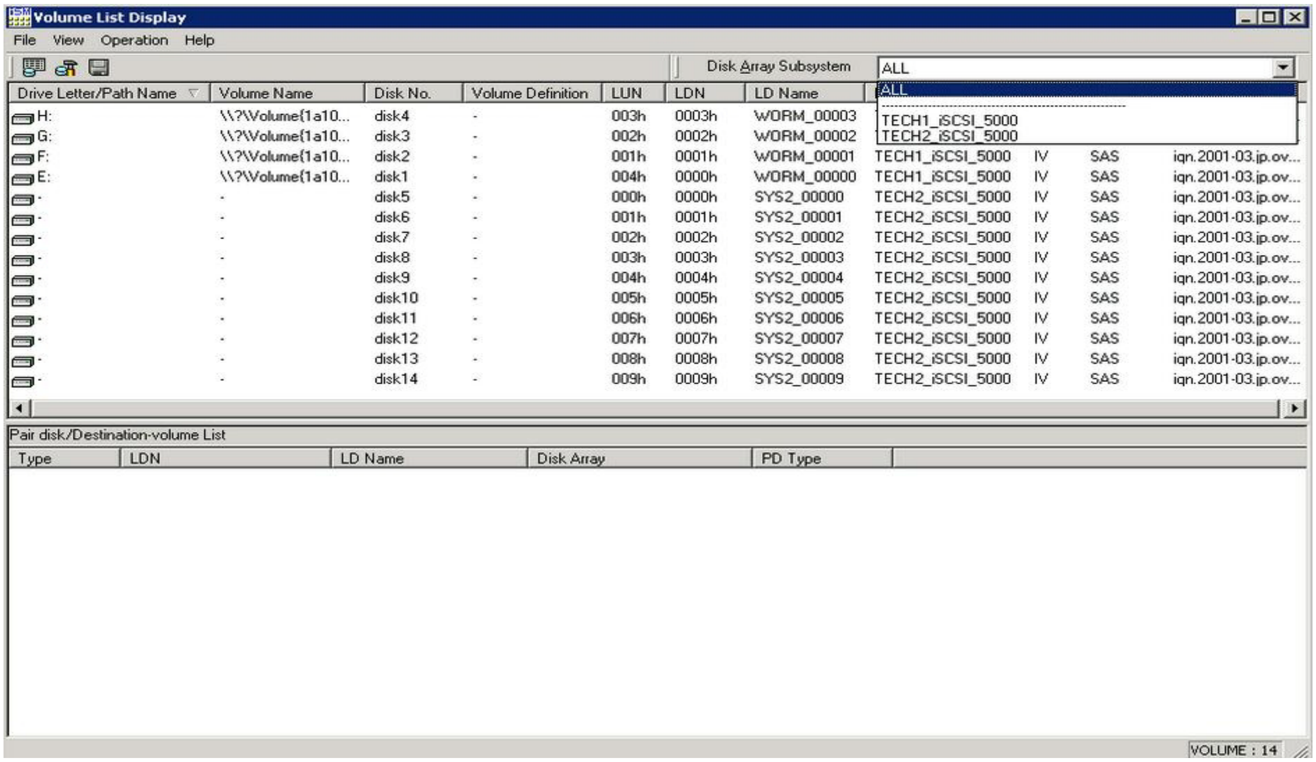


Displays information about the Volume List Display screen.

Displays information about the version.

This section describes the procedures for starting and terminating the Volume List Display function.

1. Select Start of Windows►All Programs - ControlCommand - Storage Manager Agent Utility - Volume List Display.
2. The Volume List Display screen appears



Disk Array Subsystem: ALL

Drive Letter/Path Name	Volume Name	Disk No.	Volume Definition	LUN	LDN	LD Name				
H:	\\?\Volume{1a10...	disk4	-	003h	0003h	WORM_00003				
G:	\\?\Volume{1a10...	disk3	-	002h	0002h	WORM_00002				
F:	\\?\Volume{1a10...	disk2	-	001h	0001h	WORM_00001	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
E:	\\?\Volume{1a10...	disk1	-	004h	0000h	WORM_00000	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk5	-	000h	0000h	SYS2_00000	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk6	-	001h	0001h	SYS2_00001	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk7	-	002h	0002h	SYS2_00002	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk8	-	003h	0003h	SYS2_00003	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk9	-	004h	0004h	SYS2_00004	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk10	-	005h	0005h	SYS2_00005	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk11	-	006h	0006h	SYS2_00006	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk12	-	007h	0007h	SYS2_00007	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk13	-	008h	0008h	SYS2_00008	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk14	-	009h	0009h	SYS2_00009	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...

Pair disk/Destination-volume List

Type	LDN	LD Name	Disk Array	PD Type

VOLUME : 14

Figure 2-2: Volume List Display

Terminating the Volume List Display screen

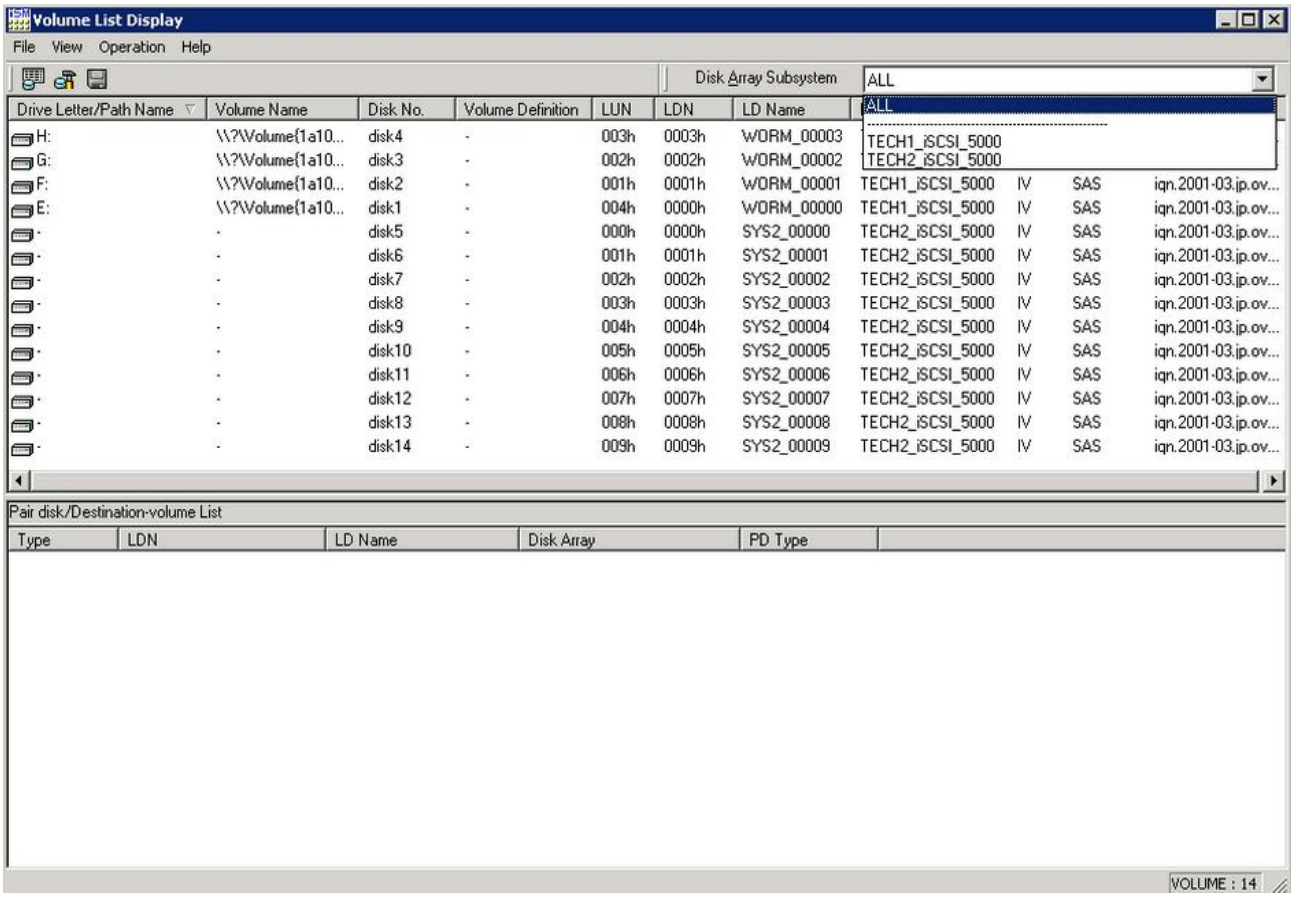
Do one of the following:

1. Select Exit in File on the menu bar of the Volume List Display screen.
2. Click the close button of the system menu.

When the Volume List Display screen is terminated, the window size, column width of the list view, and screen position on the Volume List Display screen being displayed are stored automatically. The stored screen information takes effect when the Volume List Display screen is started next.

Select Disk Array Name

1. Click the pull-down button of disk array Selection Combo box on the Volume List Display screen, and select the target disk array. The information of only the selected disk array is displayed.
2. Select the target disk array from the disk array Selection Combo box on the Volume List Display screen.
3. The volume information on the selected disk array is listed.



Disk Array Subsystem: ALL

- ALL
- TECH1_iSCSI_5000
- TECH2_iSCSI_5000

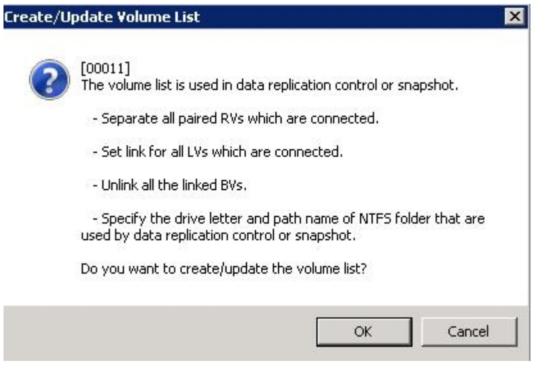
Drive Letter/Path Name	Volume Name	Disk No.	Volume Definition	LUN	LDN	LD Name				
H:	\\?\Volume{1a10...	disk4	-	003h	0003h	WORM_00003				
G:	\\?\Volume{1a10...	disk3	-	002h	0002h	WORM_00002				
F:	\\?\Volume{1a10...	disk2	-	001h	0001h	WORM_00001	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
E:	\\?\Volume{1a10...	disk1	-	004h	0000h	WORM_00000	TECH1_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk5	-	000h	0000h	SYS2_00000	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk6	-	001h	0001h	SYS2_00001	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk7	-	002h	0002h	SYS2_00002	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk8	-	003h	0003h	SYS2_00003	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk9	-	004h	0004h	SYS2_00004	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk10	-	005h	0005h	SYS2_00005	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk11	-	006h	0006h	SYS2_00006	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk12	-	007h	0007h	SYS2_00007	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk13	-	008h	0008h	SYS2_00008	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...
-	-	disk14	-	009h	0009h	SYS2_00009	TECH2_iSCSI_5000	IV	SAS	iqn.2001-03.jp.ov...

Type	LDN	LD Name	Disk Array	PD Type

Figure 2-3: Disk Array List

Create/Update Volume List

1. To create and update the volume list, select File and then select Create/Update Volume List on the Volume List Display screen.
2. Select File and then select Create/Update Volume List on the Volume List Display screen. The following inquiry message is displayed:



Create/Update Volume List

[00011]
The volume list is used in data replication control or snapshot.

- Separate all paired RVs which are connected.

- Set link for all LVs which are connected.

- Unlink all the linked BVs.

- Specify the drive letter and path name of NTFS folder that are used by data replication control or snapshot.

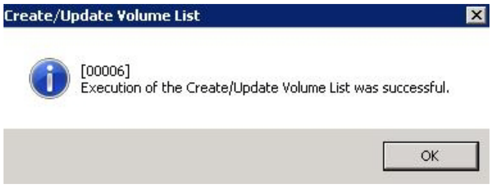
Do you want to create/update the volume list?

Figure 2-4: Execution Confirmation Screen for Create/Update Volume List

Clicking the OK button executes Create/Update Volume List.

Clicking the Cancel button cancels Create/Update Volume List and returns to the Volume List Display screen.

The following message appears when the volume list has been created/updated successfully.



Create/Update Volume List

[00006]
Execution of the Create/Update Volume List was successful.

Figure 2-5: Create Update Volume List Confirmation

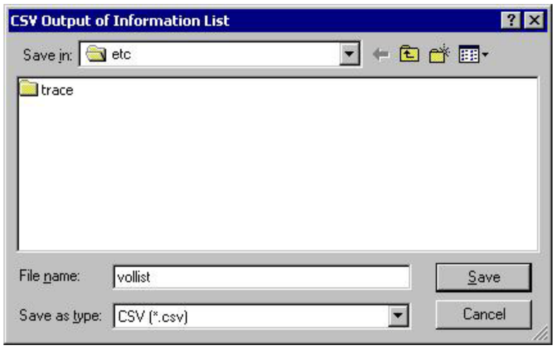
3. Clicking the OK button returns to the Volume List Display screen.

The Volume List Display screen is automatically updated after the volume list file has been created/updated.

CSV Output

The information displayed on the Volume List Display screen is output as a CSV file and then saved.

1. Select File and then select CSV Output of Information List on the Volume List Display screen. The CSV Output of Information List screen appears.



Save in: etc

trace

File name: vollist

Save as type: CSV (*.csv)

Figure 2-6: CSV Output

Specify the save destination.

The default save destination is the etc folder in the installation directory.

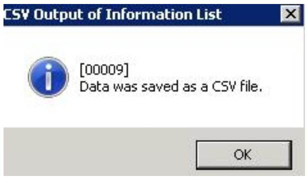
2. Specify the file name.

The default file name is vollist.csv.

3. Click the Save button to save the input information.

When the Cancel button is clicked, the screen is returned to the Volume List Display screen without saving the file.

4. When the file has been saved successfully, the following message appears:



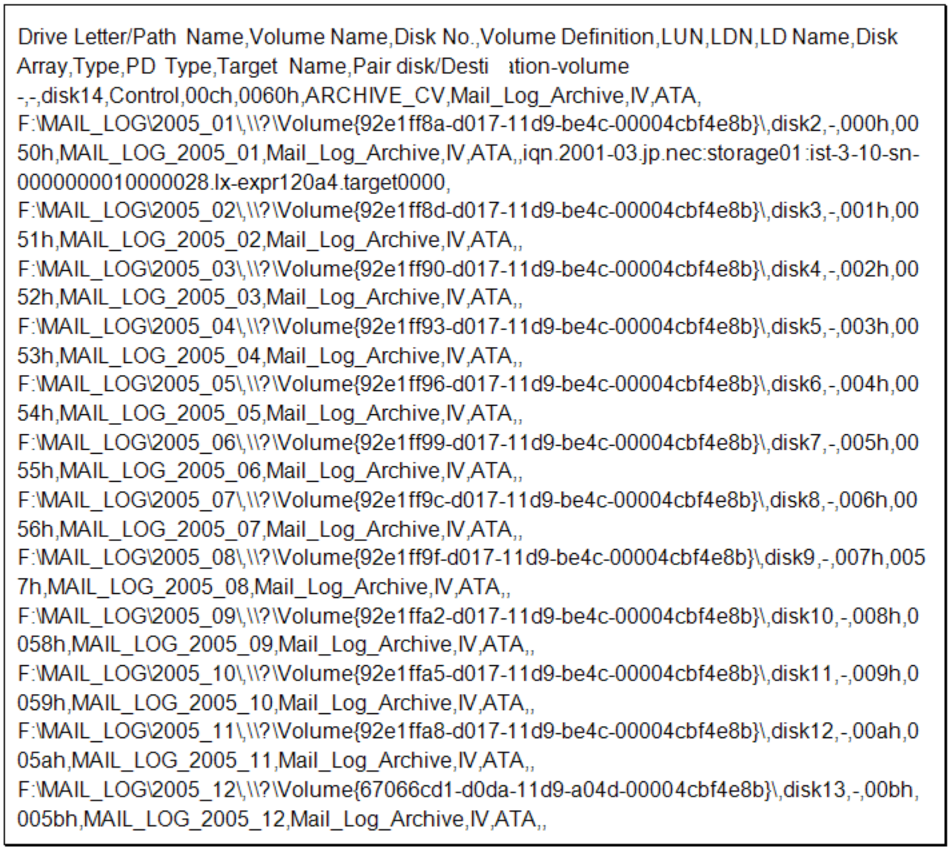
[00009]
Data was saved as a CSV file.

Figure 2-7: CSV Output of Information List

5. Click OK button to return to the Volume List Display screen.

File Example

The following example shows the CSV file that is output as the result of the CSV output of the information display list.



```
Drive Letter/Path Name,Volume Name,Disk No.,Volume Definition,LUN,LDN,LD Name,Disk
Array,Type,PD Type,Target Name,Pair disk/Desti ation-volume
-,-,disk14,Control,00ch,0060h,ARCHIVE_CV,Mail_Log_Archive,IV,ATA,
F:\MAIL_LOG\2005_01\,\\?\Volume{92e1ff8a-d017-11d9-be4c-00004cbf4e8b}\,disk2,-,000h,00
50h,MAIL_LOG_2005_01,Mail_Log_Archive,IV,ATA,,iqn.2001-03.jp.nec:storage01:ist-3-10-sn-
0000000010000028.lx-expr120a4.target0000,
F:\MAIL_LOG\2005_02\,\\?\Volume{92e1ff8d-d017-11d9-be4c-00004cbf4e8b}\,disk3,-,001h,00
51h,MAIL_LOG_2005_02,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_03\,\\?\Volume{92e1ff90-d017-11d9-be4c-00004cbf4e8b}\,disk4,-,002h,00
52h,MAIL_LOG_2005_03,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_04\,\\?\Volume{92e1ff93-d017-11d9-be4c-00004cbf4e8b}\,disk5,-,003h,00
53h,MAIL_LOG_2005_04,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_05\,\\?\Volume{92e1ff96-d017-11d9-be4c-00004cbf4e8b}\,disk6,-,004h,00
54h,MAIL_LOG_2005_05,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_06\,\\?\Volume{92e1ff99-d017-11d9-be4c-00004cbf4e8b}\,disk7,-,005h,00
55h,MAIL_LOG_2005_06,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_07\,\\?\Volume{92e1ff9c-d017-11d9-be4c-00004cbf4e8b}\,disk8,-,006h,00
56h,MAIL_LOG_2005_07,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_08\,\\?\Volume{92e1ff9f-d017-11d9-be4c-00004cbf4e8b}\,disk9,-,007h,005
7h,MAIL_LOG_2005_08,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_09\,\\?\Volume{92e1ffa2-d017-11d9-be4c-00004cbf4e8b}\,disk10,-,008h,0
058h,MAIL_LOG_2005_09,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_10\,\\?\Volume{92e1ffa5-d017-11d9-be4c-00004cbf4e8b}\,disk11,-,009h,0
059h,MAIL_LOG_2005_10,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_11\,\\?\Volume{92e1ffa8-d017-11d9-be4c-00004cbf4e8b}\,disk12,-,00ah,0
05ah,MAIL_LOG_2005_11,Mail_Log_Archive,IV,ATA,,
F:\MAIL_LOG\2005_12\,\\?\Volume{67066cd1-d0da-11d9-a04d-00004cbf4e8b}\,disk13,-,00bh,
005bh,MAIL_LOG_2005_12,Mail_Log_Archive,IV,ATA,,
```

This file outputs information displayed on the Volume List Display screen by separating each piece of information by commas.

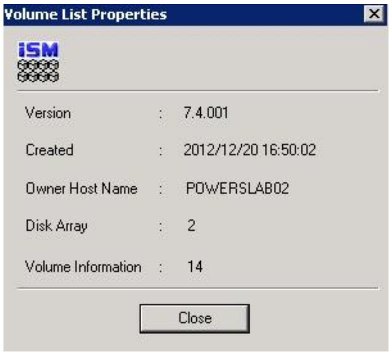
The information for a volume is output as information for a line.

Displaying Property Information of Volume List

To check property information of the volume list, select File Properties on the Volume List Display screen.

To display property information, select File Properties on the Volume List Display screen.

To return to the Volume List Display screen, click the Close button.



Version : 7.4.001

Created : 2012/12/20 16:50:02

Owner Host Name : POWERSLAB02

Disk Array : 2

Volume Information : 14

Figure 2-8: Volume List Properties

Version: Displays the version information of the Storage Manager Volume List used to create the volume list.

Created: Displays the date when the volume list was created.

Owner Host Name:

Displays the host name of the server owning the volume list.

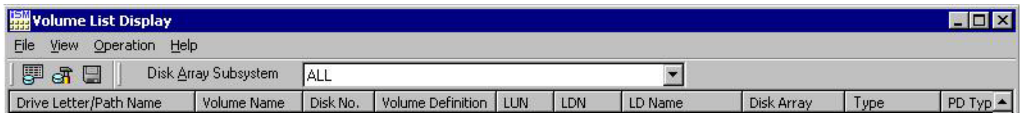
Disk Array: Displays the total number of disk arrays in the volume list.

Volume Information:

Displays the total number of volume information items in the volume list.

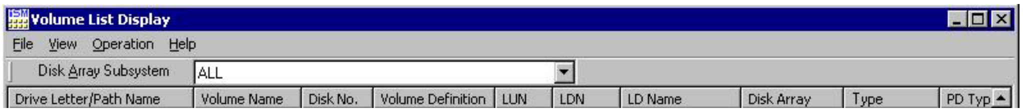
Viewing/Hiding Toolbar

To select whether to view or hide the toolbar, specify View Toolbar.



Disk Array Subsystem ALL

Figure 2-9: Viewing Toolbar



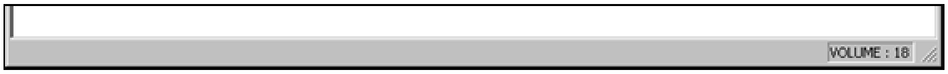
Disk Array Subsystem ALL

Figure 2-10: Hiding Toolbar

View/Hide Status Bar

To select whether to view or hide the status bar, specify View Status Bar.

Figure 2-11:



Viewing Status Bar

Figure 2-12: View/Hide Status Bar

Update Display Information

To update the information of the volume list file, select View and then select Update Display Information on the Volume List Display screen.

The volume list file contents are updated and the Volume List Display screen is automatically refreshed.

Defining Control Volume

To start the screen for defining a control volume, select Operation   Define Control Volume from the Volume List Display screen.

A control volume is a volume used for issuing a control I/O to a disk array from a server. When defining a control volume, select a standard volume that is not used by data replication, snapshot, or WORM. Allocate the control volume as a dedicated volume and do not store business data in it.

The purpose (attribute) of logical disks built as control volumes can be identified with the following SnapSAN S3000/S5000.

When the logical disk information is displayed by the SnapSAN Manager client (and so on) for disk arrays on which the purpose (attribute) of a control volume can be identified, the identification information indicating the control volume as a logical disk purpose (attribute) is displayed.

The control volume setting procedure differs depending on the disk array functions as shown below.

Disk Arrays Identifying the Control Volume Attribute

It is unnecessary to define the control volume using this function.

First build the control volume using the SnapSAN Manager server's configuration function; once the control volume is recognized by the server, create or update the volume list.

When the volume list is created or updated, the disk array identifies the control volume attribute from the logical disks connected to the server and registers it on the volume list.

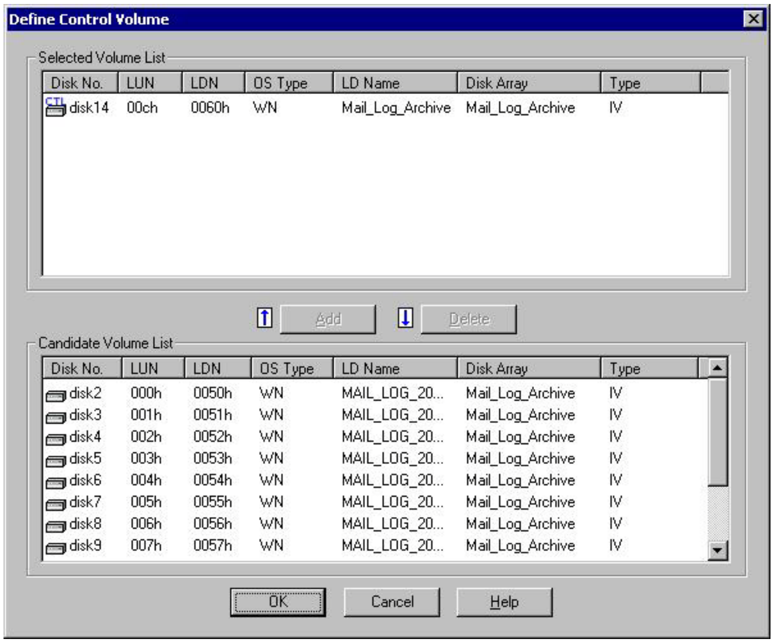
Other Disk Arrays

It is necessary to define the control volume using this function.

In disk arrays with which the control volume attribute can be identified, the logical disk that is built as a control volume is not displayed on the control volume definition screen; it cannot be added, changed, or deleted.

Define Control Volume

To display the Define Control Volume screen, select Operation Define Control Volume from the Volume List Display screen.



Selected Volume List

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk14	00ch	0060h	WN	Mail_Log_Archive	Mail_Log_Archive	IV

Candidate Volume List

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk2	000h	0050h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk3	001h	0051h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk4	002h	0052h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk5	003h	0053h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk6	004h	0054h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk7	005h	0055h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk8	006h	0056h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk9	007h	0057h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV

Figure 2-13: Define Control Volume

Display items on the Define Control Volume screen are described below.

Selected Volume List

Lists already-registered control volumes.

CTL: Displays a logical disk selected as a control volume.

Candidate Volume List

Lists candidates of logical disks that can be registered as a control volume. Type of listed logical disks is IV or MV.

: Displays logical disks that can be registered as a control volume.

When the Define Control Volume screen is started, if an error is detected in the saved definition information, one of the following icons indicating an error appears.

Icon	Explanation and Action	
CTL	Explanation	Indicates that logical disks which were defined as control volumes are in an inappropriate state. The following is the corresponding operations. • Setting the control volume in a pair as an RV • Specifying the control volume as a base-volume (BV) by adding a snapshot generation to it • Making the control volume usable from the server by building a link-volume (LV) with the same logical disk number as for the control volume • Making the control volume unusable from the server by canceling Access Control or unbinding the volume • Making unrecognizable the disk array to which the defined control volume belongs
	Action	Redefine as a control volume a volume that is not used with data replication or snapshot (IV). Alternatively, take any of the following actions depending on the control volume state. • If the control volume has been set in a pair, make it unpaired. • If a snapshot generation has been added or an LV has been built, unbind the snapshot. • If the control volume has been unrecognizable, check the connection state of the control volume and make it recognizable again. • If the disk array has been unrecognizable, check the connection state of the disk array and make it recognizable again. • If any inconsistency is found in the control volume definition, delete the control volume definition.
	Explanation	Indicates that defined control volumes are invalid. The following is the corresponding operations. • Building the control volume using the SnapSAN Manager configuration setting function and making it available from the server in a disk array with which the control volume attribute can be identified.
	Action	Delete the existing control volume definition since the control volume definition becomes unnecessary for the disk array.

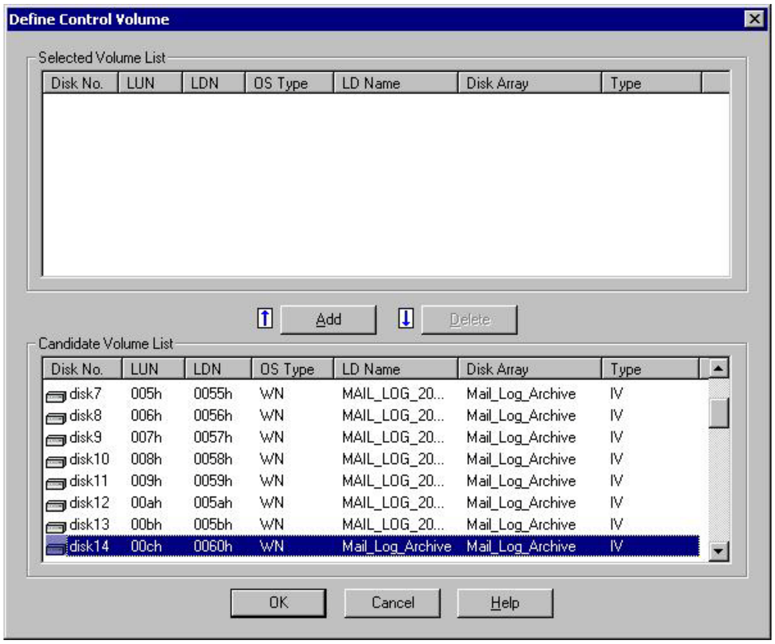
Register, change, or delete a control volume

A control volume is used to issue a control I/O to a disk array from a server. A logical disk can be selected for each disk array.

As a control volume, select a standard volume that is not used by data replication, snapshot, or WORM function. Allocate the control volume as a dedicated volume and do not store business data in it.

Register or change a control volume

To register or change a control volume, select the logical disk to be used as a control volume from Candidate Volume List and click the Add or Update button.



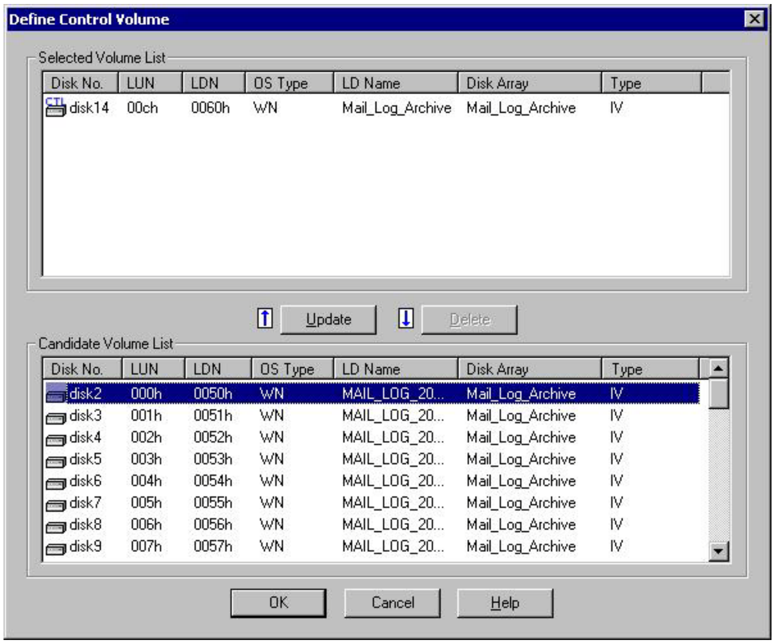
Selected Volume List

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type

Candidate Volume List

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk7	005h	0055h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk8	006h	0056h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk9	007h	0057h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk10	008h	0058h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk11	009h	0059h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk12	00ah	005ah	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk13	00bh	005bh	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk14	00ch	0060h	WN	Mail_Log_Archive	Mail_Log_Archive	IV

Figure 2-14: Candidate Volume List



Selected Volume List

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk14	00ch	0060h	WN	Mail_Log_Archive	Mail_Log_Archive	IV

Candidate Volume List

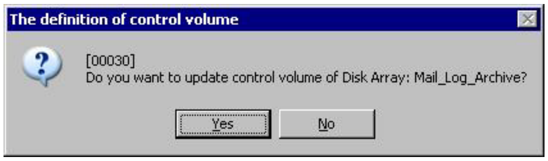
Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk2	000h	0050h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk3	001h	0051h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk4	002h	0052h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk5	003h	0053h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk6	004h	0054h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk7	005h	0055h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk8	006h	0056h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk9	007h	0057h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV

Figure 2-15: Change Control Volume

When you try to change a control volume that has already been registered in Candidate Volume List, the following confirmation screen appears.

To change the control volume to the logical disk selected from Selected Volume List, click the Yes button.

To return to the Define Control Volume screen without update, click the No button.



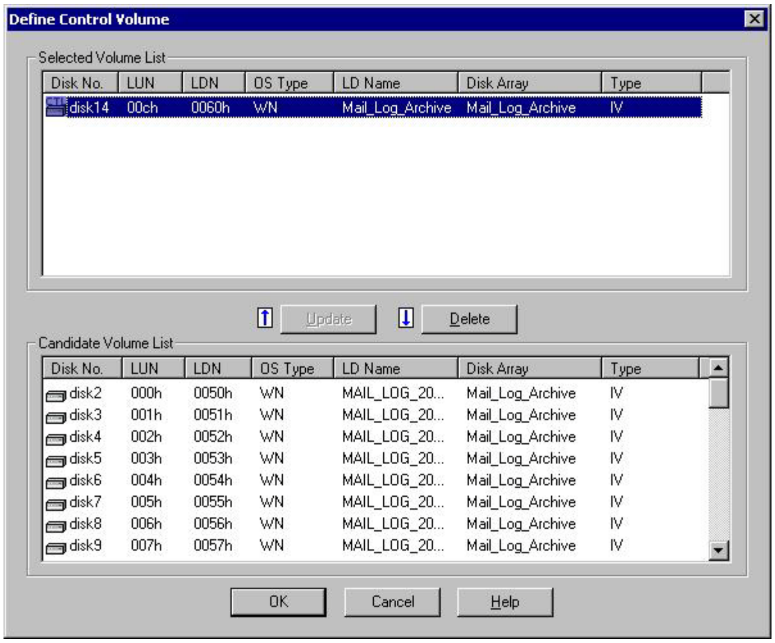
The definition of control volume

[00030]
Do you want to update control volume of Disk Array: Mail_Log_Archive?

Figure 2-16: Define Control Volume

Delete a control volume

To delete the control volume that has already been registered in Selected Volume List, select the logical disk to be deleted from Selected Volume List and click the Delete button.



Define Control Volume

Selected Volume List

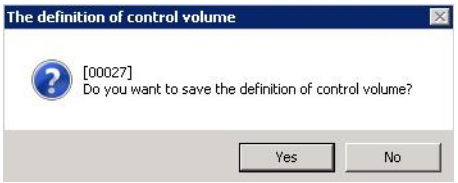
Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk14	00ch	0060h	WN	Mail_Log_Archive	Mail_Log_Archive	IV

Candidate Volume List

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk2	000h	0050h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk3	001h	0051h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk4	002h	0052h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk5	003h	0053h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk6	004h	0054h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk7	005h	0055h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk8	006h	0056h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk9	007h	0057h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV

Figure 2-17: Delete Control Volume

When you click the OK button on the Define Control Volume screen, the message for confirming whether to save the definition information appears.



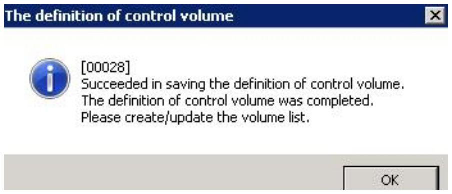
The definition of control volume

[00027]
Do you want to save the definition of control volume?

Figure 2-18: Save Confirmation

When you click the Yes button for the confirmation, the definition information is saved and the completion message appears.

To return to the Define Control Volume screen, click the No button.



The definition of control volume

[00028]
Succeeded in saving the definition of control volume.
The definition of control volume was completed.
Please create/update the volume list.

Figure 2-19: Completion

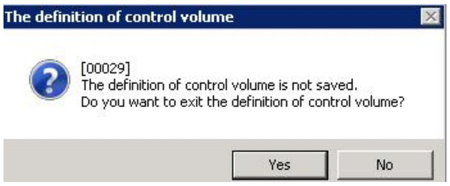
To close the Define Control Volume screen and return to the Volume List Display screen, click the OK button.

To enable the saved definition information, create or update the volume list to reflect the definition information of the control volume to the volume list.

When you click the Cancel button on the Define Control Volume screen, the message for confirming whether to cancel the definition appears.

When you click the Yes button for the confirmation, the definition information is not saved. The Define Control Volume screen is closed and returned to the Volume List Display screen.

To return to the Define Control Volume screen, click the No button.



The definition of control volume

[00029]
The definition of control volume is not saved.
Do you want to exit the definition of control volume?

Figure 2-20: Cancel Confirmation Screen of Define Control Volume

Update the volume list to reflect the updated definition information to the volume list.

Select File Create/Update Volume List from the Volume List Display screen to create and update the volume list, and reflect the saved definition information of the control volume to the volume list for registration.

When the volume list is created or updated, the display of the Volume List Display screen is updated automatically. Confirm that the definition information is updated correctly by checking the displayed information of Volume Definition.

Logical Disk Information Display Command

To perform logical disk information display, the SnapSAN Manager rc_ldlist command is used.

The SnapSAN Manager rc_ldlist command obtains and displays logical disks and associated information of disk arrays recognized by the system.

[Main Options]

For the iSMrc_sense command, you can specify the following options.

(i)Specification of the volume (-vol volume -volflg mv_flg)

Specify the volume and volume type.

For the volume types, refer to 3.3 "Volume Types".

Display of the attribute information (-attr)

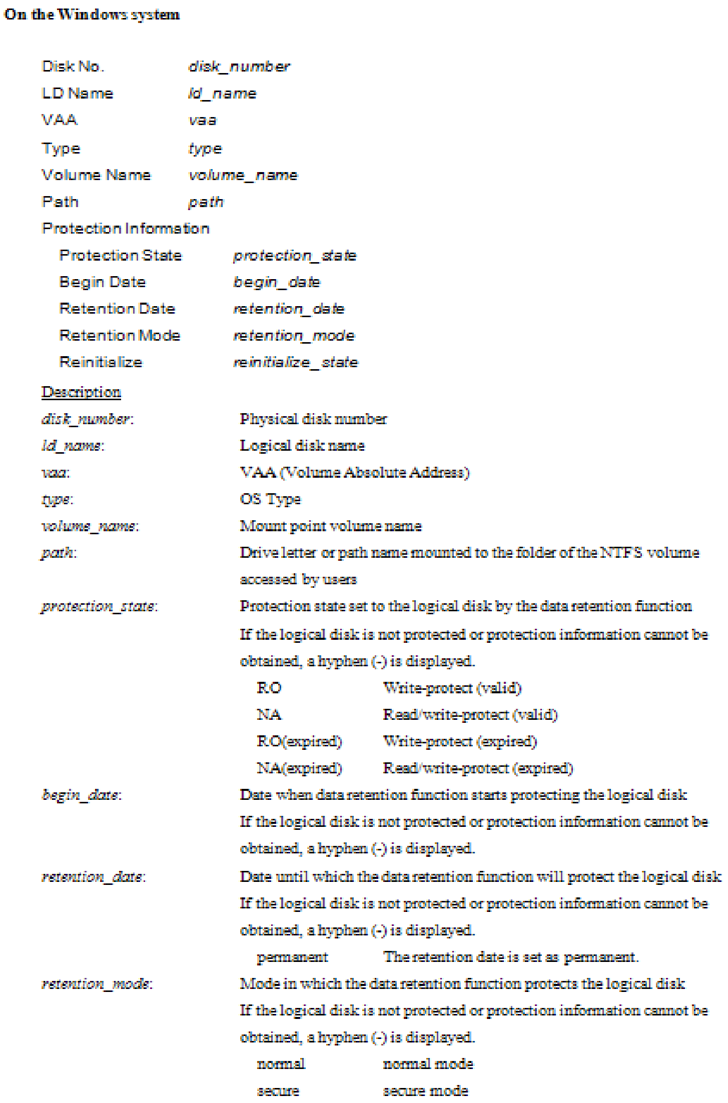
Displays the logical disk attributes and link status of the link-volume (LV). For the attribute information to display, refer to "ControlCommand Command Reference".

Display of the volume protection information (-protect)

Displays the logical disk attributes in the data retention function.

[Displayed Information]

iSMrc_sense -protect displays the following information.



On the Windows system

```
Disk No.            disk_number
LD Name             ld_name
VAA                 vaa
Type                type
Volume Name         volume_name
Path                path
Protection Information
  Protection State      protection_state
  Begin Date            begin_date
  Retention Date        retention_date
  Retention Mode        retention_mode
  Reinitialize          reinitialize_state
```

Description

disk_number: Physical disk number

ld_name: Logical disk name

vaa: VAA (Volume Absolute Address)

type: OS Type

volume_name: Mount point volume name

path: Drive letter or path name mounted to the folder of the NTFS volume accessed by users

protection_state: Protection state set to the logical disk by the data retention function

If the logical disk is not protected or protection information cannot be obtained, a hyphen (-) is displayed.

RO	Write-protect (valid)
NA	Read/write-protect (valid)
RO(expired)	Write-protect (expired)
NA(expired)	Read/write-protect (expired)

begin_date: Date when data retention function starts protecting the logical disk

If the logical disk is not protected or protection information cannot be obtained, a hyphen (-) is displayed.

retention_date: Date until which the data retention function will protect the logical disk

If the logical disk is not protected or protection information cannot be obtained, a hyphen (-) is displayed.

permanent	The retention date is set as permanent.

retention_mode: Mode in which the data retention function protects the logical disk

If the logical disk is not protected or protection information cannot be obtained, a hyphen (-) is displayed.

normal	normal mode
secure	secure mode

	strict	strict mode
reinitialize_state:	Logical disk reinitialization state If reinitialization has not been performed, a hyphen (-) is displayed.	
	formatting(*nn*%)	Reinitialization in progress A value indicating the progress of initialization is displayed in *nn*.
	format-fail	Reinitialization failed

```
ldn      type       ld_name                    attribute      capacity     pd_type
```

Description

Receiving…: Message indicating that data is being received.
During a joint operation with iSM, this message remains until data reception is completed. The number of dots "." increases as data reception progresses.

disk_array_name: Disk array name

management: Identifies whether the system recognizes the disk array.

direct	Disk array directly recognized by the system.
indirect	Disk array which is not recognized by the system

type: OS type

ldn: Logical disk number

ld_name: Logical disk name

attribute: Logical disk attribute

capacity: Logical disk capacity

pd_type: PD Type (attribute of the physical disk configuring the logical disk)

FC	Logical disk configured of physical disks with the FC attribute
ATA	Logical disk configured of physical disks with the ATA attribute
SAS	Logical disk configured of physical disks with the SAS attribute
SSD	Logical disk configured of physical disks with the SSD attribute

(2) When the -d option is specified:
Logical disk information as shown below is displayed.

```
Receiving…
------------------------------------------------------------------------------------
Disk Array Name                         Management
------------------------------------------------------------------------------------
disk_array_name                         management
```

Description

Receiving…: Message indicating that data is being received.
During a joint operation with iSM, this message remains until data reception is completed. The number of dots "." increases as data reception progresses.

disk_array_name Disk array name

management Identifies whether the system recognizes the disk array.
direct Disk array directly recognized by the system
indirect Disk array which is not recognized by the system

(3) When the -protect only option or the -protect all option is specified:
Logical disk information as shown below is displayed.

```
Receiving...
--------------------------------------------------------------------------------
[Disk Array Name](Management)
LDN    OS Type  LD Name         Attribute     Capacity  PD Type  Data Protection
--------------------------------------------------------------------------------
[disk_array_name](management)
ldn    type     ld_name         attribute     capacity  pd_type  protection_state
```

Description

The items not described below are the same as those in (1). Refer to (1) for the description of these items.

protection_state: Whether the logical disk is protected by the data retention function
protection Protected logical disk
- Unprotected logical disk

(4) When the -node option is specified:
Logical disk information as shown below is displayed.

```
Receiving...
----------------------------------------------------------------------------------
[Disk Array Name](Management)
LDN    OS Type  LD Name         Attribute     Capacity  PD Type  Node Number
----------------------------------------------------------------------------------
[disk_array_name](management)
ldn    type     ld_name         attribute     capacity  pd_type  node_number
```

Description

The items not described below are the same as those in (1). Refer to (1) for the description of these items.

node_number: Node number to which the logical disk belongs
When it is not a logical disk of the disk array with node or that the node number cannot be acquired, "-" (hyphen) is displayed.

[Execution Conditions]

To display the volume protection information, the following conditions must be satisfied.

- The logical disk attribute indicating the reserve attribute is not displayed.
- The logical disk attribute indicating the snapshot data volume (SDV) of the snapshot function is not displayed.
- At least one logical disk of the target disk array is registered in the volume list.
- The volume list is not being created or updated.
- The iSM-only special file must not be being created (Linux version only).

WORM with SnapSAN Manager

This chapter describes how to operate WORM with SnapSAN Manager.

SnapSAN Manager consists of server and client functions, the former controls the storage and the latter executes monitoring and operations, which allows the storage to be managed remotely.

In addition, the client function provides the following two GUIs:

- GUI based on Windows
- GUI based on the Web

In this manual, SnapSAN Manager client or client is used for describing the client function without separating the above two.

Also, to describe the former GUI only, SnapSAN Manager client (Win GUI) or client (Win GUI) is used, and to describe the latter GUI only, SnapSAN Manager client (Web GUI) or client (Web GUI) is used.

SnapSAN Manager provides the function for operating WORM and displaying information. You can perform the volume protection setting operation by the WORM function and view the protection status using the SnapSAN Manager client's GUI.

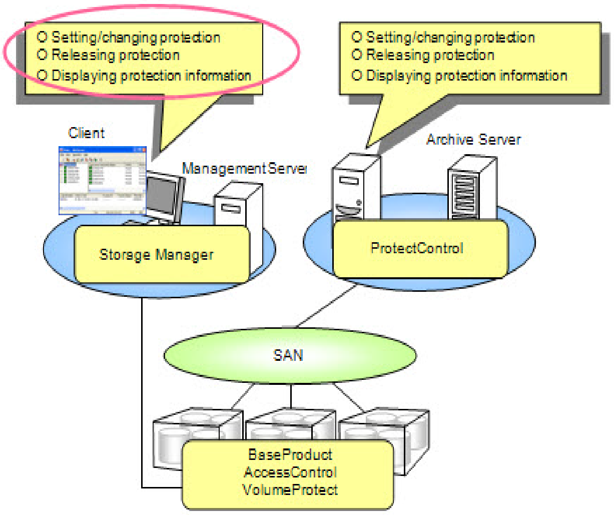


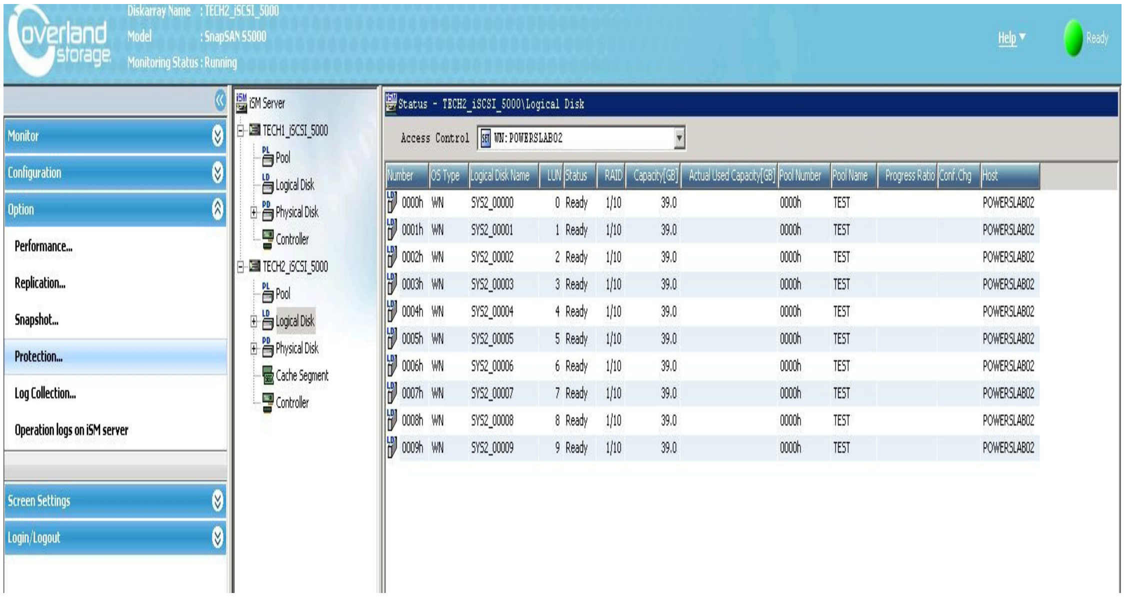
Figure 2-21: Opening WORM

SnapSAN Manager Main Window

The SnapSAN Manager main window is the first window that appears when you connect the SnapSAN Manager client to the SnapSAN Manager server. It displays the information about the configuration of the disk arrays monitored by SnapSAN Manager and the states of the resources. You can start the WORM management screen from the menu on the SnapSAN Manager main window.

The SnapSAN Manager main window displays the following information related to WORM.

Volume Protection Status



Diskarray Name : TECH2_iSCSI_5000
Model : SnapSAN S5000
Monitoring Status : Running

Status - TECH2_iSCSI_5000\Logical Disk

Access Control WN:POWERSLAB02

Number	OS Type	Logical Disk Name	LUN	Status	RAID	Capacity[GB]	Actual Used Capacity[GB]	Pool Number	Pool Name	Progress Ratio	Conf.Chg	Host
0000h	WN	SYS2_00000	0	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0001h	WN	SYS2_00001	1	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0002h	WN	SYS2_00002	2	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0003h	WN	SYS2_00003	3	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0004h	WN	SYS2_00004	4	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0005h	WN	SYS2_00005	5	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0006h	WN	SYS2_00006	6	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0007h	WN	SYS2_00007	7	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0008h	WN	SYS2_00008	8	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0009h	WN	SYS2_00009	9	Ready	1/10	39.0		0000h	TEST			POWERSLAB02

Figure 2-22: Main

To implement long-term storage of data in non-falsifiable format, the SnapSAN Manager WORM management screen provides management screens for making various settings such as protection status and retention period on a volume-by-volume basis.The SnapSAN Manager WORM management screen provides the function for operating the WORM and displaying the information by using the SnapSAN Manager client.

The SnapSAN Manager WORM management screen provides the following operations related to WORM and the function for displaying the information. Executing the WORM operations requires that the user role of the client be operator or administrator.

- Setting volume protection
- Changing volume protection settings
- Releasing volume protection
- Initializing volume contents
- Initializing volume OS Type/Logical Disk Name

The WORM management screen consists of the configuration display area displaying the disk array configuration and states on the left side of the screen and the information list display area on the right side of the screen that displays the information about the item selected in the configuration display area.

Configuration Display Area

The configuration display area displays the configuration information of WORM function in the format of a tree view.

The configuration display area displays a list of disk arrays that are being monitored by SnapSAN Manager and for which the WORM function can be used.

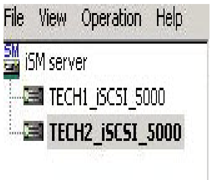


Figure 2-23: Configuration Display

In the configuration display area, the state of each managed item is indicated by the shape of the icon and the shading of the color.

The icon of a disk array not being monitored is shaded in gray.

Information List Display Area

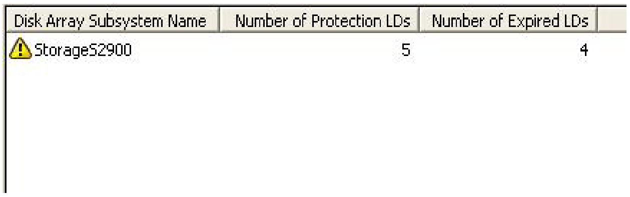
This area displays lists of detailed information about the components one level below the layer selected in the configuration display area.

Clicking an item name sorts the list. The icon of a disk array not being monitored is shaded in gray.

Item Selected in the Configuration Display Area	Item Displayed in the Information List Display Area
SnapSAN Manager server	Disk array list
Disk array	Volume list

The items displayed in the list are described below.

Disk Array List



Disk Array Subsystem Name	Number of Protection LDs	Number of Expired LDs
⚠ StorageS2900	5	4

Figure 2-24: Disk Array List

The disk array list displays the information about the items described below. Double-clicking an item switches the display to the volume list of the disk array.

Disk Array Subsystem Name

The names of disk arrays that are being monitored by SnapSAN Manager and that can use the WORM function are displayed. Disk arrays which do not support the WORM function or for which WORM has not been purchased are not displayed.

Icon	Description
▬ etc.	Indicates that the disk array is operating normally.
⚠	Indicates that a volume in the expired status exists in the disk array.

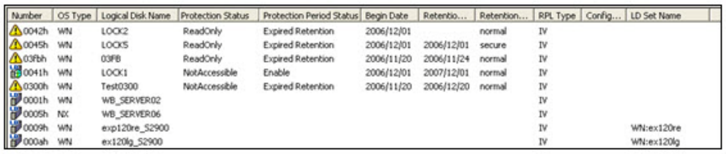
Number of Protection LDs

Displays the number of volumes for which volume protection setting has already been made.

Number of Expired LDs

Displays the number of volumes in the expired status.

Volume list



Number	OS Type	Logical Disk Name	Protection Status	Protection Period Status	Begin Date	Retentio...	Retention...	RPL Type	Config...	LD Set Name
⚠ 0042h	WN	LOCK2	ReadOnly	Expired Retention	2006/12/01		normal	IV		
⚠ 0045h	WN	LOCK5	ReadOnly	Expired Retention	2006/12/01	2006/12/01	secure	IV		
⚠ 03fbh	WN	03FB	ReadOnly	Expired Retention	2006/11/20	2006/11/24	normal	IV		
LD 0041h	WN	LOCK1	NotAccessible	Enable	2006/12/01	2007/12/01	normal	IV		
⚠ 0300h	WN	Test0300	NotAccessible	Expired Retention	2006/11/20	2006/12/20	normal	IV		
LD 0001h	WN	WB_SERVER02						IV		
LD 0005h	NX	WB_SERVER06						IV		
LD 0009h	WN	exp120re_S2900						IV		WN:ex120re
LD 000ah	WN	ex120lg_S2900						IV		WN:ex120lg

Figure 2-25: Volume List

The volume list displays the information about the items described below.

Number

- Displays the logical disk number of a volume in hexadecimal.
- Displays the state of a volume with the icon next to number.

Icon	Description
LD	Indicates that the volume is in the data protection state .
ⓘ	Indicates that the volume is in the data protection state and the state of retention date approached.
⚠	Indicates that the volume is in the data protection state and the expired retention state.
LD	Indicates that the volume is not in the data protection state .
LD 🔒	Indicates that the volume is locked.

OS Type

Displays the OS type of volume.

Display	Description
A2	Indicates the logical disk is operating on the ACOS-2 system.
AX	Indicates the logical disk is operating on the AIX system.
CX	Indicates the logical disk is operating on the Solaris system.
LX	Indicates the logical disk is operating on the Linux system.
NX	Indicates the logical disk is operating on the HP-UX system.
SX	Indicates the logical disk is operating on the SUPER-UX system.
WN	Indicates the logical disk is operating on the Windows system (excluding GPT disk).
WG	Indicates the logical disk is operating on the GPT disk of the Windows system.

Logical Disk Name

Displays the logical disk name of the volume.

Protection Status

Displays the protection status of the volume.

Display	Description
ReadOnly	Read-enabled and write-protected
NotAccessible	Read/write-protected
(Blank)	Protection has not been set.

Protection Period Status

Displays the protection period status of the volume.

Display	Description
Enable	Within the retention period
Enable (Retention date approached)	Within the retention period and the status of retention date approached
Expired Retention	Retention period expired.
(Blank)	Protection has not been set.

Begin Date

Displays the date on which protection is set in the yyyy/mm/dd format. If protection has not been set, it is displayed in blank.

Retention Date

Displays the retention date in the yyyy/mm/dd format. If protection has not been set or that the retention date was not set at protection setting, it is displayed in blank. If the retention expiration was set to permanent, Permanent is displayed.

Retention Mode

Displays the retention mode of the volume.

Display	Description
normal	You can release protection and reset the retention period at any time.
secure	You cannot release protection until the retention period has elapsed. However, you can extend the retention period or change the protection status.
strict	You cannot release protection until the retention period has elapsed. Neither can you reset the retention period and protection status.
(Blank)	Protection has not been set.

RPL Type

Displays the replication type of the volume.

This column does not appear when none of Overland Volume Cloning and Replication and Mirroring is purchased.

Display	Description
IV	Not used as a replication volume
MV	Used as a replication source volume
RV	Used as a replication destination volume
RV/MV	Used as both RV and MV

Configuration Change

Displays the setting status of configuration setting operation guard of the volume.

Display	Description
Lock	Guard has been set.
(Blank)	Guard has not been set.

LD Set Name

Displays up to four LD Set Names to which the volume belongs (numbers exceeding four are indicated by … at the end of line).

LD to be displayed must satisfy the following conditions.

- RPL type is IV, MV, RV, or RV/MV.
- Does not belong to a reserve group.
- Not a Snapshot-related volume.
- Not a System Volume.
- Not a work disk for optimization.

- Not a L2 Cache volume.

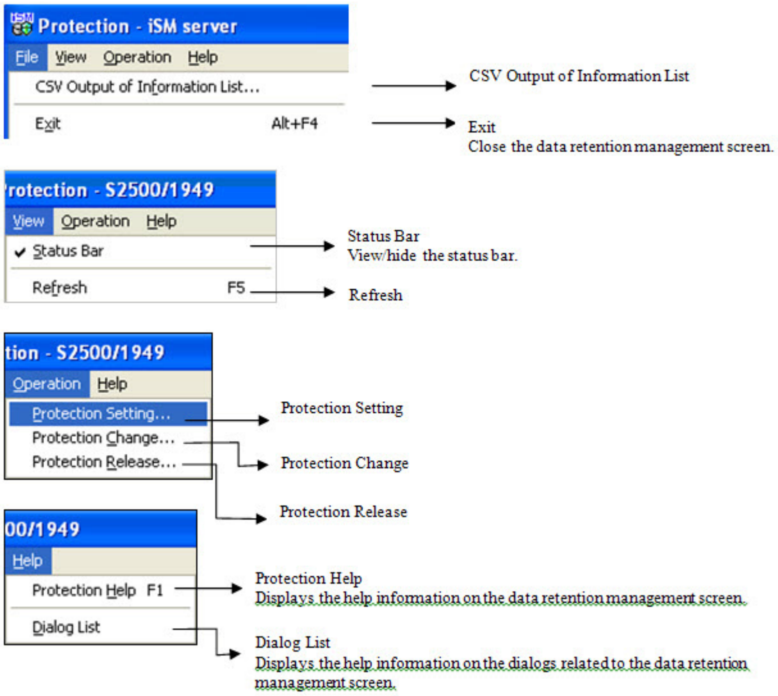
Partition Name

The name of partition to which the volume belongs is displayed.

This column is not displayed for disk arrays for which Virtual Storage Partitioning has not been unlocked.

Menu Item List

The items on the menu bar of the WORM management screen are described below.



CSV Output of Information List

Exit
Close the data retention management screen.

Status Bar
View/hide the status bar.

Refresh

Protection Setting

Protection Change

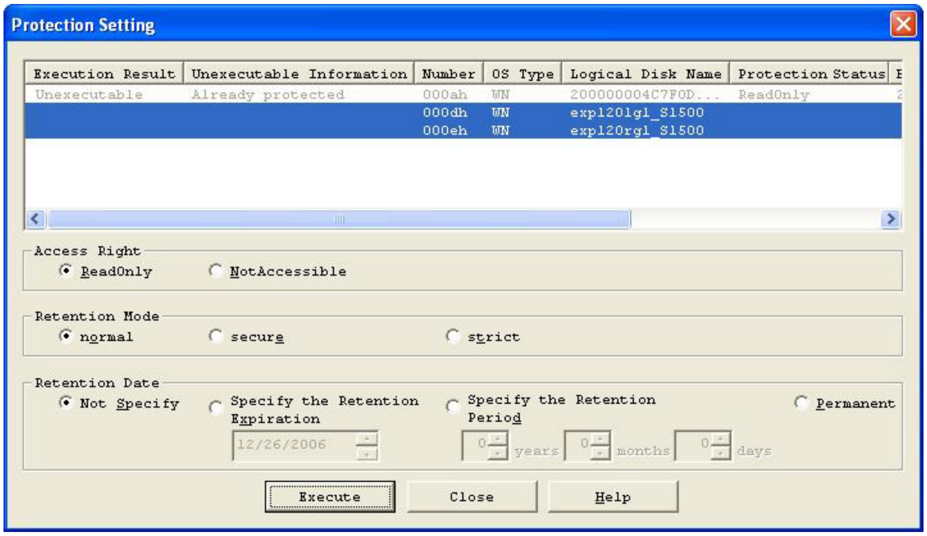
Protection Release

Protection Help
Displays the help information on the data retention management screen.

Dialog List
Displays the help information on the dialogs related to the data retention management screen.

Protection Setting/Change Dialog

The execution dialogs displayed for individual protection operations are described below.



Protection Setting

Execution Result	Unexecutable Information	Number	OS Type	Logical Disk Name	Protection Status	E
Unexecutable	Already protected	000ah	WN	200000004C7F0D...	ReadOnly	2
		000dh	WN	expl20lgl_S1500		
		000eh	WN	expl20rgl_S1500		

Access Right
● ReadOnly ○ NotAccessible

Retention Mode
● normal ○ secure ○ strict

Retention Date
● Not Specify ○ Specify the Retention Expiration 12/26/2006 ○ Specify the Retention Period 0 years 0 months 0 days ○ Permanent

Figure 2-26: Protection Setting

The information screen of the execution dialog displays the information about the items described below. The information of each individual item is updated only when the Execute button is clicked.

Execution Result

Displays the result of execution. The operation cannot be executed for a volume for which Unexecutable is displayed.

Unexecutable Information

Displays the reason why operation cannot be executed.

Number

Displays the logical disk number in hexadecimal.

OS Type

Displays the volume OS type.

Logical Disk Name

Displays the logical disk name.

Protection Status

Displays the protection status of the volume.

Begin Date

Displays the date on which protection is set.

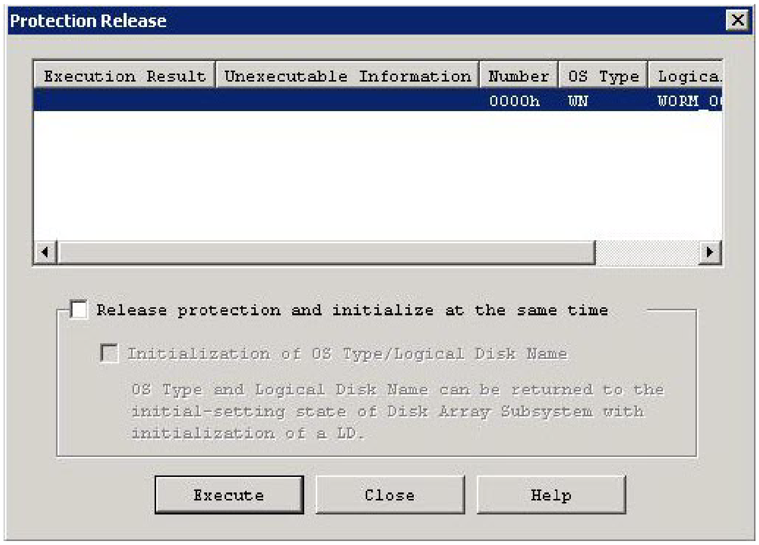
Retention Date

Displays the retention date.

Retention Mode

Displays the retention mode of the volume.

Protection Release Dialog



Protection Release

Execution Result	Unexecutable Information	Number	OS Type	Logica
		0000h	WN	WORM_0

□ Release protection and initialize at the same time

□ Initialization of OS Type/Logical Disk Name

OS Type and Logical Disk Name can be returned to the initial-setting state of Disk Array Subsystem with initialization of a LD.

Figure 2-27: Protection Release Dialog

The information screen of the Protection Release dialog displays the information about the items described below. The information of each individual item is updated only when the Execute button is clicked.

Execution Result

Displays the result of execution. The operation cannot be executed for a volume for which Unexecutable is displayed.

Unexecutable Information

Displays the reason why operation cannot be executed.

Number

Displays the logical disk number in hexadecimal.

OS Type

Displays the volume OS type.

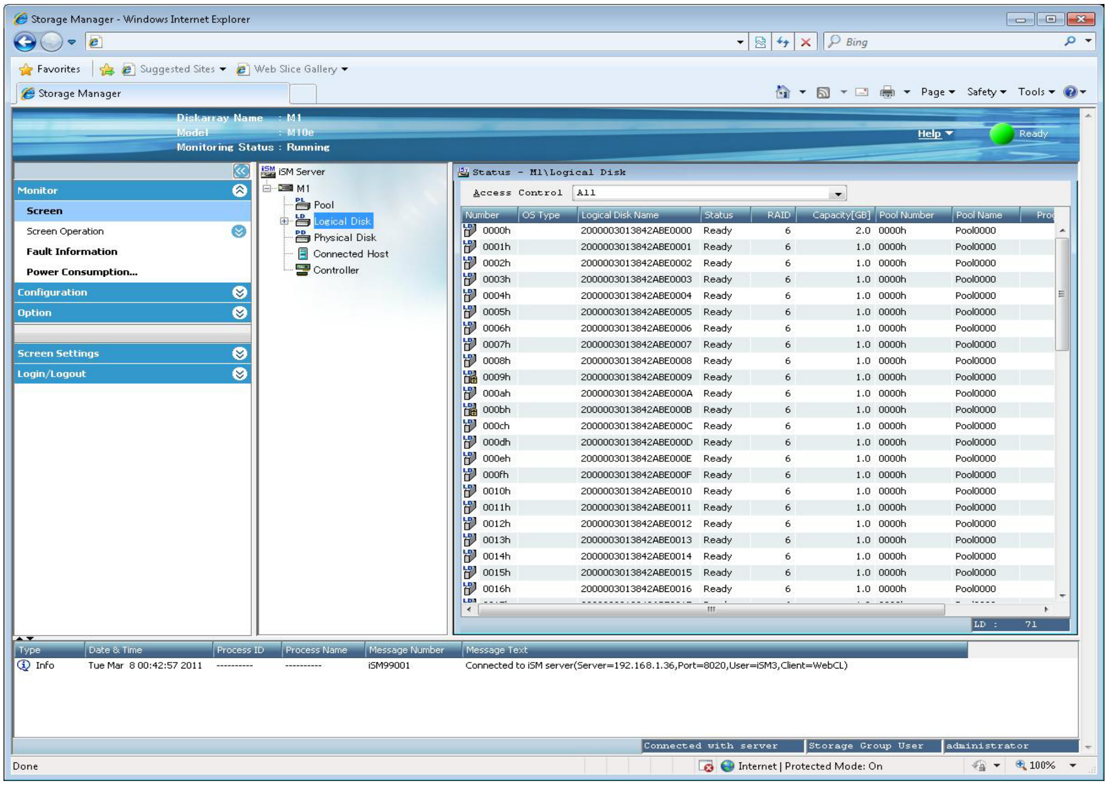
Logical Disk Name

Displays the logical disk name.

SnapSAN Manager Main Window

The SnapSAN Manager main window is the first window that appears when you connect the SnapSAN Manager client to the SnapSAN Manager server. It displays the information about the configuration of the disk arrays monitored by SnapSAN Manager and the states of the resources.

You can view the volume protection conditions of the WORM function in the logical disk list screen and logical disk details information screen within the SnapSAN Manager main window.



Diskarray Name : M1
Model : M10e
Monitoring Status : Running

Status - M1\Logical Disk

Access Control All

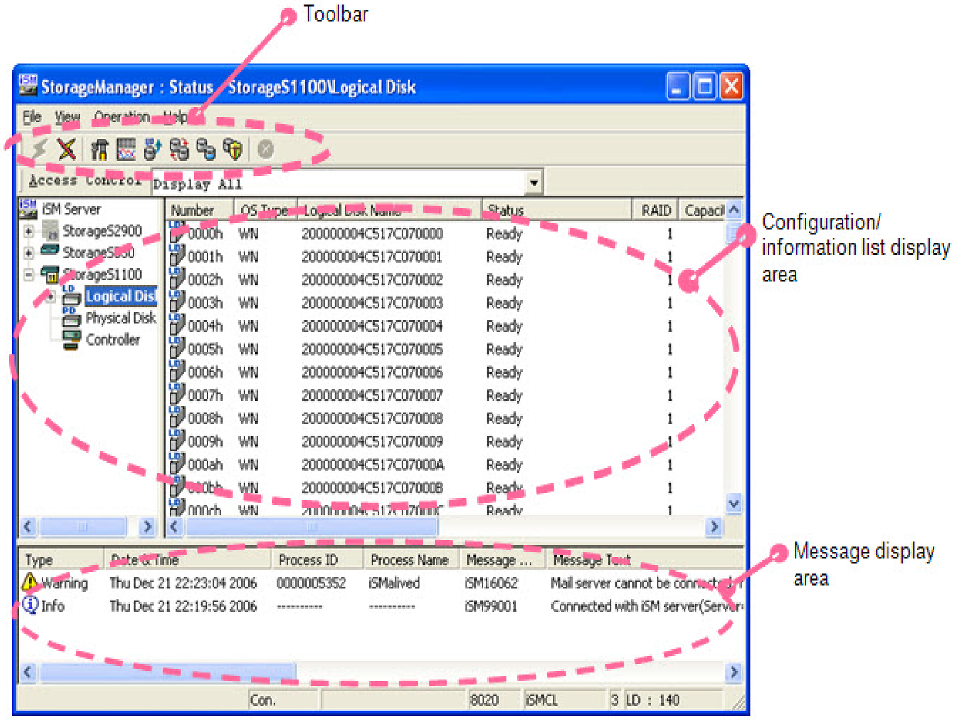
Number	OS Type	Logical Disk Name	Status	RAID	Capacity[GB]	Pool Number	Pool Name	Pro
0000h		2000003013842ABE0000	Ready	6	2.0	0000h	Pool0000	
0001h		2000003013842ABE0001	Ready	6	1.0	0000h	Pool0000	
0002h		2000003013842ABE0002	Ready	6	1.0	0000h	Pool0000	
0003h		2000003013842ABE0003	Ready	6	1.0	0000h	Pool0000	
0004h		2000003013842ABE0004	Ready	6	1.0	0000h	Pool0000	
0005h		2000003013842ABE0005	Ready	6	1.0	0000h	Pool0000	
0006h		2000003013842ABE0006	Ready	6	1.0	0000h	Pool0000	
0007h		2000003013842ABE0007	Ready	6	1.0	0000h	Pool0000	
0008h		2000003013842ABE0008	Ready	6	1.0	0000h	Pool0000	
0009h		2000003013842ABE0009	Ready	6	1.0	0000h	Pool0000	
000ah		2000003013842ABE000A	Ready	6	1.0	0000h	Pool0000	
000bh		2000003013842ABE000B	Ready	6	1.0	0000h	Pool0000	
000ch		2000003013842ABE000C	Ready	6	1.0	0000h	Pool0000	
000dh		2000003013842ABE000D	Ready	6	1.0	0000h	Pool0000	
000eh		2000003013842ABE000E	Ready	6	1.0	0000h	Pool0000	
000fh		2000003013842ABE000F	Ready	6	1.0	0000h	Pool0000	
0010h		2000003013842ABE0010	Ready	6	1.0	0000h	Pool0000	
0011h		2000003013842ABE0011	Ready	6	1.0	0000h	Pool0000	
0012h		2000003013842ABE0012	Ready	6	1.0	0000h	Pool0000	
0013h		2000003013842ABE0013	Ready	6	1.0	0000h	Pool0000	
0014h		2000003013842ABE0014	Ready	6	1.0	0000h	Pool0000	
0015h		2000003013842ABE0015	Ready	6	1.0	0000h	Pool0000	
0016h		2000003013842ABE0016	Ready	6	1.0	0000h	Pool0000	

LD : 71

Type	Date & Time	Process ID	Process Name	Message Number	Message Text
Info	Tue Mar 8 00:42:57 2011	----------	----------	iSM99001	Connected to iSM server(Server=192.168.1.36,Port=8020,User=iSM3,Client=WebCL)

Connected with server | Storage Group User | administrator

Figure 2-28: Main



Toolbar

Configuration/ information list display area

Message display area

StorageManager : Status StorageS1100\Logical Disk

Number	OS Type	Logical Disk Name	Status	RAID	Capaci
0000h	WN	200000004C517C070000	Ready	1	
0001h	WN	200000004C517C070001	Ready	1	
0002h	WN	200000004C517C070002	Ready	1	
0003h	WN	200000004C517C070003	Ready	1	
0004h	WN	200000004C517C070004	Ready	1	
0005h	WN	200000004C517C070005	Ready	1	
0006h	WN	200000004C517C070006	Ready	1	
0007h	WN	200000004C517C070007	Ready	1	
0008h	WN	200000004C517C070008	Ready	1	
0009h	WN	200000004C517C070009	Ready	1	
000ah	WN	200000004C517C07000A	Ready	1	
000bh	WN	200000004C517C07000B	Ready	1	
000ch	WN	200000004C517C07000C	Ready	1	

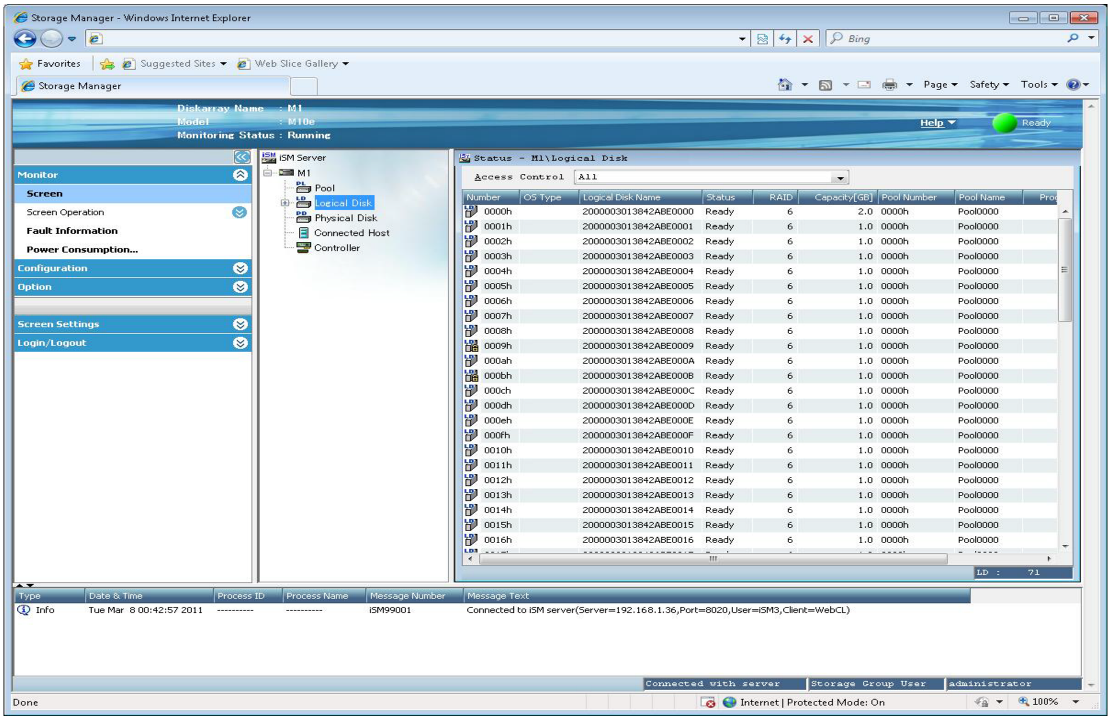
Type	Date & Time	Process ID	Process Name	Message ...	Message Text
Warning	Thu Dec 21 22:23:04 2006	0000005352	iSMalived	iSM16062	Mail server cannot be connected. (
Info	Thu Dec 21 22:19:56 2006	----------	----------	iSM99001	Connected with iSM server(Server:

Con. 8020 iSMCL 3 LD : 140

Figure 2-29: Main

Logical Disk List Screen

You can display the logical disk list screen by selecting (clicking the left button on) Logical Disk in configuration display area. This screen displays various attribute information such as logical disk name, operating status, and capacity. When WORM has been purchased, the volume protection conditions of the WORM function are also displayed.



Storage Manager - Windows Internet Explorer

Diskarray Name : M1
Model : M10e
Monitoring Status : Running

Status - M1\Logical Disk

Access Control: All

Number	OS Type	Logical Disk Name	Status	RAID	Capacity[GB]	Pool Number	Pool Name	Proc
0000h		2000003013842ABE0000	Ready	6	2.0	0000h	Pool0000	
0001h		2000003013842ABE0001	Ready	6	1.0	0000h	Pool0000	
0002h		2000003013842ABE0002	Ready	6	1.0	0000h	Pool0000	
0003h		2000003013842ABE0003	Ready	6	1.0	0000h	Pool0000	
0004h		2000003013842ABE0004	Ready	6	1.0	0000h	Pool0000	
0005h		2000003013842ABE0005	Ready	6	1.0	0000h	Pool0000	
0006h		2000003013842ABE0006	Ready	6	1.0	0000h	Pool0000	
0007h		2000003013842ABE0007	Ready	6	1.0	0000h	Pool0000	
0008h		2000003013842ABE0008	Ready	6	1.0	0000h	Pool0000	
0009h		2000003013842ABE0009	Ready	6	1.0	0000h	Pool0000	
000ah		2000003013842ABE000A	Ready	6	1.0	0000h	Pool0000	
000bh		2000003013842ABE000B	Ready	6	1.0	0000h	Pool0000	
000ch		2000003013842ABE000C	Ready	6	1.0	0000h	Pool0000	
000dh		2000003013842ABE000D	Ready	6	1.0	0000h	Pool0000	
000eh		2000003013842ABE000E	Ready	6	1.0	0000h	Pool0000	
000fh		2000003013842ABE000F	Ready	6	1.0	0000h	Pool0000	
0010h		2000003013842ABE0010	Ready	6	1.0	0000h	Pool0000	
0011h		2000003013842ABE0011	Ready	6	1.0	0000h	Pool0000	
0012h		2000003013842ABE0012	Ready	6	1.0	0000h	Pool0000	
0013h		2000003013842ABE0013	Ready	6	1.0	0000h	Pool0000	
0014h		2000003013842ABE0014	Ready	6	1.0	0000h	Pool0000	
0015h		2000003013842ABE0015	Ready	6	1.0	0000h	Pool0000	
0016h		2000003013842ABE0016	Ready	6	1.0	0000h	Pool0000	

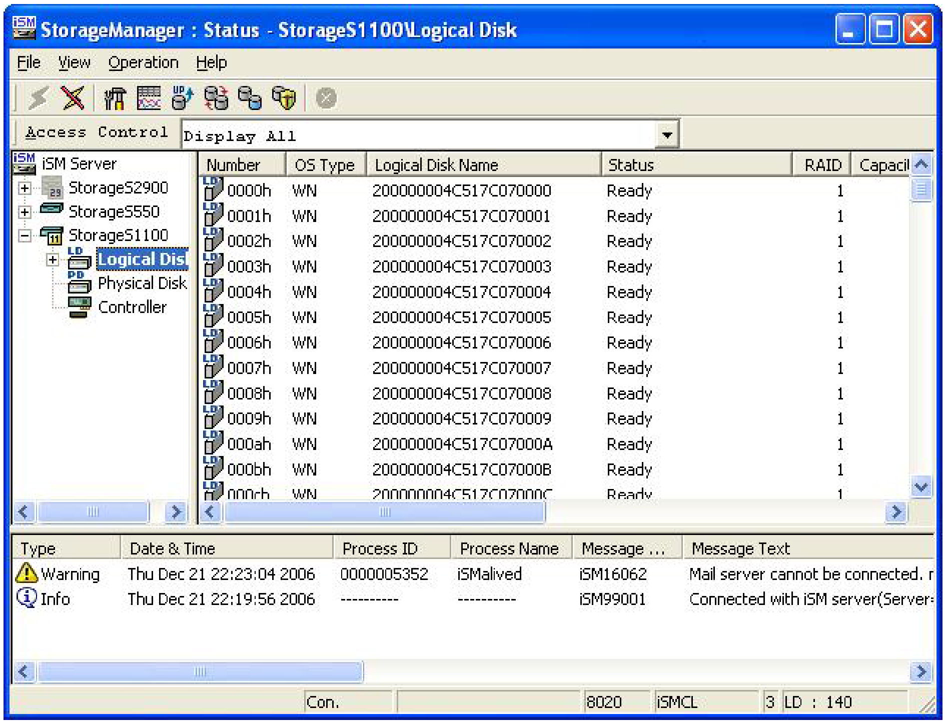
LD : 71

Type	Date & Time	Process ID	Process Name	Message Number	Message Text
Info	Tue Mar 8 00:42:57 2011	----------	----------	iSM99001	Connected to iSM server(Server=192.168.1.36,Port=8020,User=iSM3,Client=WebCL)

Connected with server | Storage Group User | administrator

Done | Internet \| Protected Mode: On | 100%

Figure 2-30: Logical Disk



StorageManager : Status - StorageS1100\Logical Disk

Access Control: Display All

Number	OS Type	Logical Disk Name	Status	RAID	Capacit
0000h	WN	200000004C517C070000	Ready	1	
0001h	WN	200000004C517C070001	Ready	1	
0002h	WN	200000004C517C070002	Ready	1	
0003h	WN	200000004C517C070003	Ready	1	
0004h	WN	200000004C517C070004	Ready	1	
0005h	WN	200000004C517C070005	Ready	1	
0006h	WN	200000004C517C070006	Ready	1	
0007h	WN	200000004C517C070007	Ready	1	
0008h	WN	200000004C517C070008	Ready	1	
0009h	WN	200000004C517C070009	Ready	1	
000ah	WN	200000004C517C07000A	Ready	1	
000bh	WN	200000004C517C07000B	Ready	1	
000ch	WN	200000004C517C07000C	Ready	1	

Type	Date & Time	Process ID	Process Name	Message ...	Message Text
Warning	Thu Dec 21 22:23:04 2006	0000005352	iSMalived	iSM16062	Mail server cannot be connected. r
Info	Thu Dec 21 22:19:56 2006	----------	----------	iSM99001	Connected with iSM server(Server:

Con. | 8020 | iSMCL | 3 | LD : 140

Figure 2-31: Logical Disk Status

The items below show the volume protection conditions.

Purpose

Displays the purpose of a logical disk in any of the following at Purpose column.

RPL: Logical disk to which only a pair for replication is set

Snapshot: Logical disk to which only snapshot is set

Link-volume: Logical disk that is a link-volume (LV)

RPL/snapshot: Logical disk to which a pair for replication and snapshot setting have already been set

Optimization: Work disk for performance optimization

Data Protection: Logical disk to which the data protection setting has already been set

RPL/Data Protection: Logical disk to which a pair for replication and data protection setting have already been set

System Volume: Volume to store storage system information

Replication Reserved Volume:

Volume to store the data replication management information

Data Migration Reserved Volume:

Volume to store the data migration management information

Control Volume: Logical disks for control volumes

L2 Cache: Logical disks for L2 Cache

(Blank): General logical disk to which no specific purpose is set

Data Protection

Displays whether a logical disk is protected in any of the following at the Data Protection column. When WORM has not been purchased, this item does not appear.

protection: Protected

(Blank): Unprotected

When you have set the WORM function to enable volume reinitialization upon protection release, you can view the following items to check the state or progress ratio of reinitialization.

Status

Displays the reinitialization status of logical disk in any of the following at Status column.

Ready: Logical disk is in normal operation. (Reinitialization completed)

Attn.(formatting): During logic formatting (Being initialized)

* The logical disk is not available until logic formatting is completed.

Attn.(format-fail): Fails in logic formatting (Reinitialization failed)

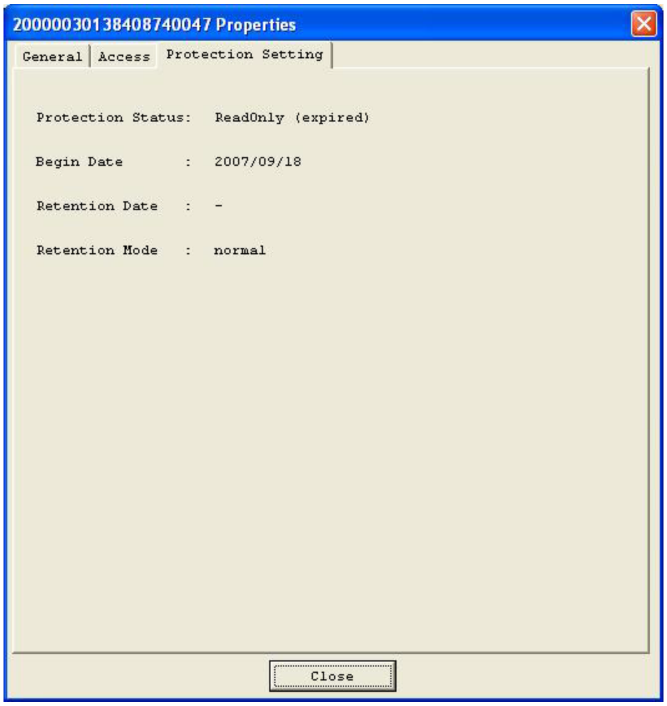
Attn.(stop): Logical disk is in rotation stop status

Progress Ratio

Displays the progress ratio in logical disk where a formatting event occurs.

Logical Disk Details Information Screen

You can display the logical disk details information screen by selecting (clicking the left button on) an optional logical disk, right clicking the logical disk, and selecting Properties (or selecting View   Properties from the menu (for SnapSAN Manager clients (Win GUI))) in configuration display area or information list display area.



Protection Status: ReadOnly (expired)

Begin Date : 2007/09/18

Retention Date : -

Retention Mode : normal

Figure 2-32: Protection Setting Properties

Protection Status

Displays the protection status in any of the following.

ReadOnly: Read-only

NotAccessible: Read/write-protect

ReadOnly (expired): Read-only (expired)

NotAccessible (expired): Read/write-protect (expired)

Begin Date

Displays the date on which protection is set.

Retention Date

Displays the WORM date.

When the retention date has not been set, a hyphen (-) is displayed. If the retention date was set to permanent, Permanent is displayed.

Retention Mode

Displays the retention mode in any of the following.

normal: You can release protection and reset the retention period at any time.

secure: You cannot release protection until the retention period has elapsed. However, you can extend the retention period or change the protection status.

strict: You cannot release protection until the retention period has elapsed. Neither can you reset the retention period and protection status.

WORM Operations

Protection is set on a volume-by-volume basis. Since the write operation to the protected volumes is prevented, the data consistency is guaranteed.

You perform each operation by first selecting the target volume from the volume list displayed in the WORM management screen and then using the relevant menu that is chosen from the menu bar or displayed when you right-click on it.

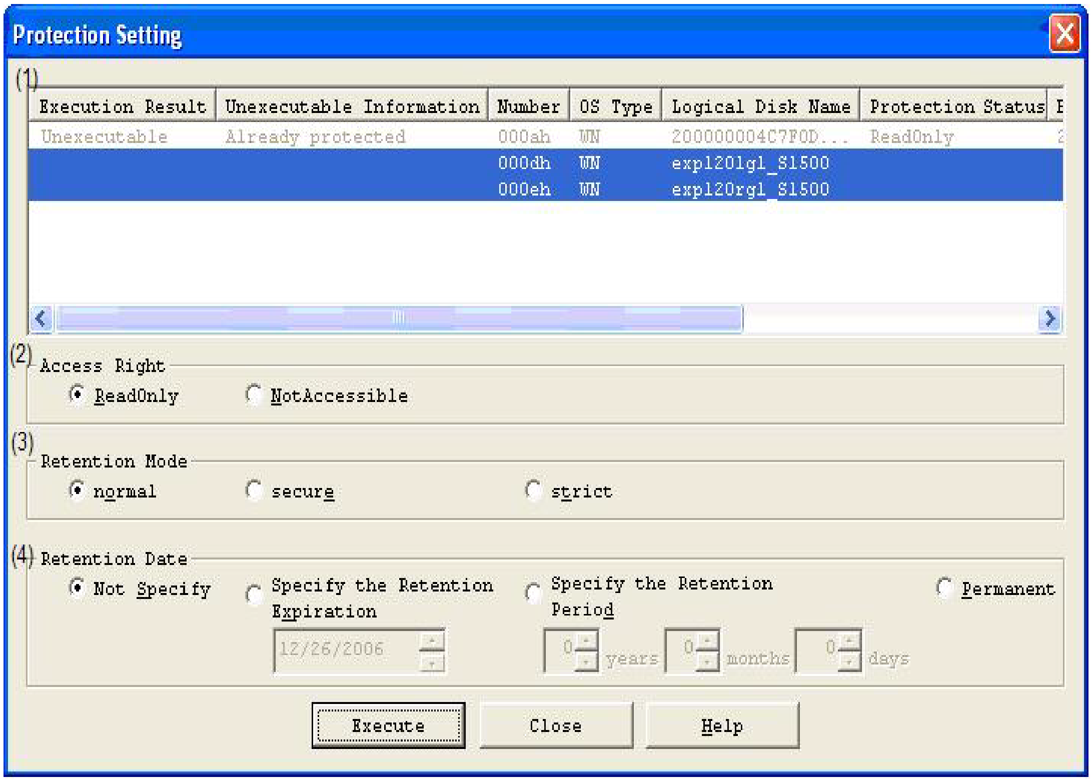
Volume Protection Setting

Protection is set on a volume-by-volume basis. Since the write operation to the protected volumes is prevented, the data consistency is guaranteed.

Operating Procedure

Display the Protection Setting screen using one of the following procedures.

- Select a desired volume from the information list display area. Then, from the menu bar of the WORM management screen, select Operation   Protection Setting.
- Select a desired volume from the information list display area. Then, right-click on it and select Protection Setting.



Protection Setting

(1)

Execution Result	Unexecutable Information	Number	OS Type	Logical Disk Name	Protection Status	E
Unexecutable	Already protected	000ah	WN	200000004C7F0D...	ReadOnly	2
		000dh	WN	expl201gl_S1500		
		000eh	WN	expl20rgl_S1500		

(2) Access Right

● ReadOnly ○ NotAccessible

(3) Retention Mode

● normal ○ secure ○ strict

(4) Retention Date

● Not Specify ○ Specify the Retention Expiration 12/26/2006 ○ Specify the Retention Period 0 years 0 months 0 days ○ Permanent

Figure 2-33: Protection Setting

Select the volume for which you want to set protection from the list, specify the access right, retention mode, and retention date, and then click the Execute button.

You can specify two or more volumes at a time and execute the operation for all of them simultaneously.

Unexecutable volumes are shaded in gray and cannot be selected.

Selected Volume List

Information list of the volume selected in the information list display area appears.

If Unexecutable is shown in the Execution Result field, the volume does not meet the execution conditions and therefore cannot be selected.

For the unexecutable volume, refer to Unexecutable Information and take one of the following actions.

Unexecutable Information	Action
Error LD	Retry after checking the LD status.
Already protected	Protection cannot be set again to the volume that has been already protected.
Have been registered to Atgroup	Retry after deleting the volume from the ATgroup.
The volume cannot be operated for its state.	Retry after checking the LD status.
Monitoring stop	Retry after setting the disk array to be monitored.
The pair state of LD cannot be operated.	Retry after checking the pair status.
Data being migrated	Retry after checking the volume status.

Access Right

Specify the protection status of the volume. The following access rights can be specified.

Radio Button	Description
ReadOnly	The target volume is write-protected from the server.
NotAccessible	The target volume is read/write-protected from the server.

* Note that setting ReadOnly to a volume of which OS type is WN/WG may disable to mount it to the host.

Retention Mode

Specify the retention mode of the volume. The following retention modes can be specified.

Radio Button	Description
normal	Protection can be released or protection settings can be changed, regardless of the retention period.
secure	Protection cannot be released during the retention period. There are constraints on changing protection settings.

Radio Button	Description
strict	Protection cannot be released during the retention period. Protection settings cannot be changed, either.

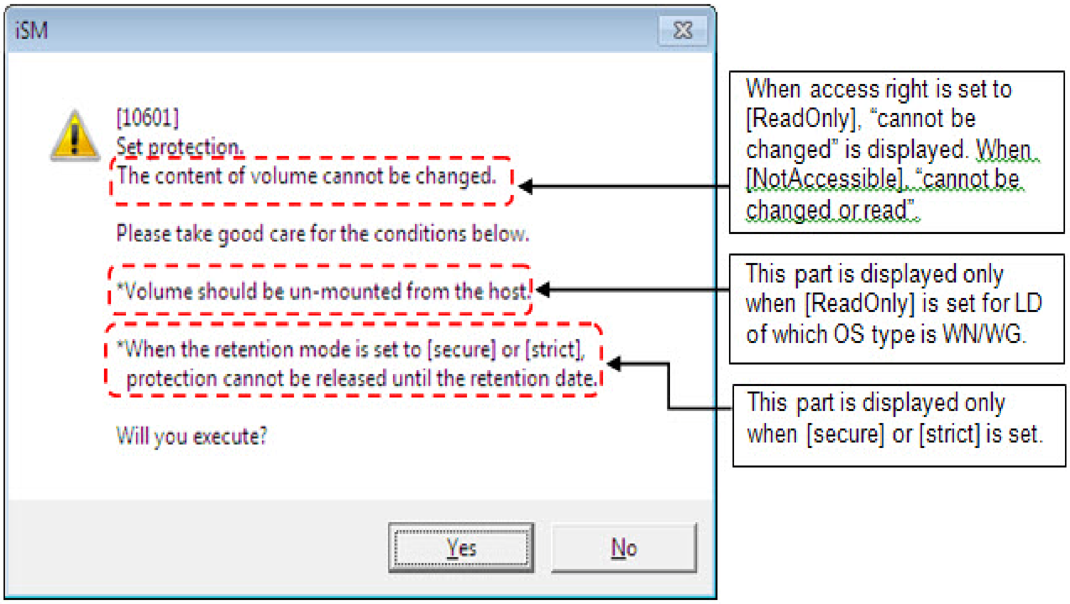
Retention Date

Specify the retention period of the volume. The retention period can be specified in the following formats.

Radio Button	Description
Not Specify	The retention period is set to 0, indicating the condition in which the volume retention period has already elapsed.
Specify the Retention Expiration	The retention period is set as the time from the current date to the specified date (year, month, and day). The volume is protected from the current date to the specified date.
Specify the Retention Period	Specify the number of years, months, or days for the retention period. The volume is protected for the specified duration starting at the current date.
Permanent	The retention period is permanent. The volume is permanently protected from the current date.

* When Not Specify is selected, note that the volume immediately becomes the status in which protection can be released.

When the Execute button is clicked, the following confirmation message appears.



[10601]
Set protection.
The content of volume cannot be changed.

Please take good care for the conditions below.

*Volume should be un-mounted from the host.

*When the retention mode is set to [secure] or [strict],
protection cannot be released until the retention date.

Will you execute?

When access right is set to [ReadOnly], "cannot be changed" is displayed. When [NotAccessible], "cannot be changed or read".

This part is displayed only when [ReadOnly] is set for LD of which OS type is WN/WG.

This part is displayed only when [secure] or [strict] is set.

Figure 2-34: Confirmation

In this case, selecting No stops the processing.

Execution Conditions

To perform protection setting, the following conditions must be satisfied.

- The target volume is not protected.
- The target volume has not been assigned to a reserve group.
- The target volume is not a System Volume.
- The target volume is not a snapshot-related volume (SDV, BV, SV, SV*, LV).
- The target volume is not being initialized.
- The target volume has not been registered to ATgroup.
- When the target volume is a replication volume, the pair has been separated.
- The target volume is not being used by the performance optimization function (not being scheduled, either).
- The target volume is not in rotation stop state.
- The target volume is not a control volume.
- Data of the target volume is not being migrated by the DataMigration function.
- The target volume is not a L2 Cache volume.
- The target volume must have been unmounted from the host.

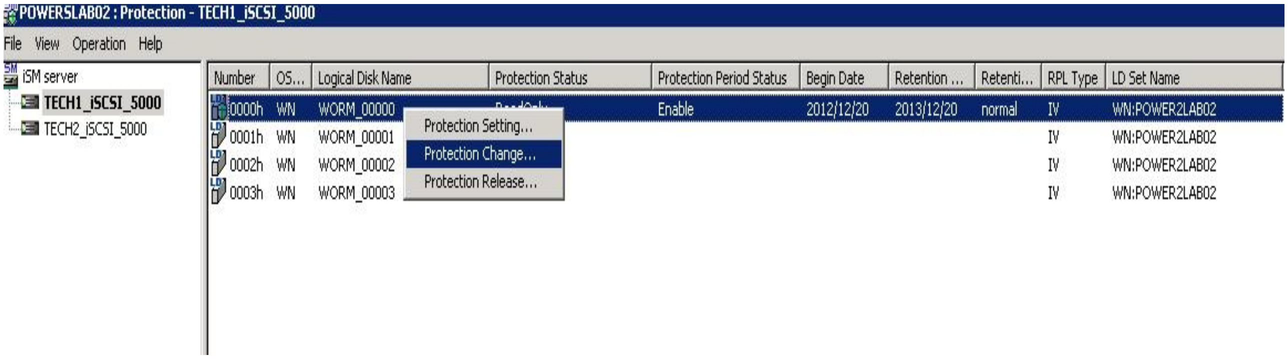
Volume Protection Change

Protection setting can be changed on a volume-by-volume basis. You can extend the retention period or change the protection status.

Operating Procedure

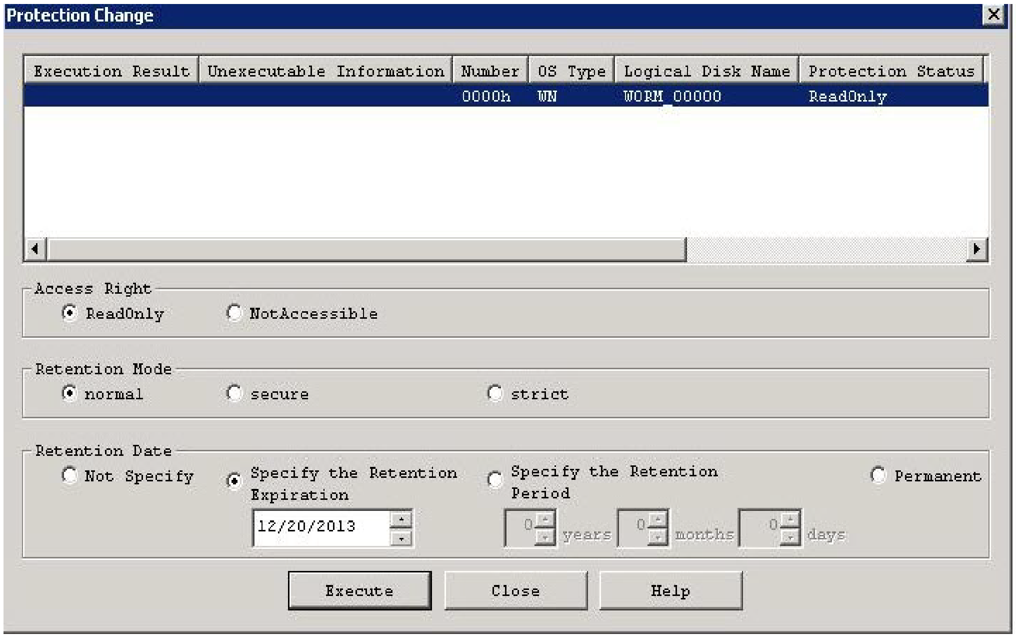
Display the Protection Change screen using one of the following procedures.

- Select a desired volume from the information list display area. Then, from the menu bar of the WORM management screen, select Operation   Protection Change.
- Select a desired volume from the information list display area. Then, right-click on it and select Protection Change.



Number	OS...	Logical Disk Name	Protection Status	Protection Period Status	Begin Date	Retention ...	Retenti...	RPL Type	LD Set Name
0000h	WN	WORM_00000	ReadOnly	Enable	2012/12/20	2013/12/20	normal	IV	WN:POWER2LAB02
0001h	WN	WORM_00001						IV	WN:POWER2LAB02
0002h	WN	WORM_00002						IV	WN:POWER2LAB02
0003h	WN	WORM_00003						IV	WN:POWER2LAB02

Figure 2-35: Protection Change



Execution Result	Unexecutable Information	Number	OS Type	Logical Disk Name	Protection Status
		0000h	WN	WORM_00000	ReadOnly

Access Right: ● ReadOnly ○ NotAccessible

Retention Mode: ● normal ○ secure ○ strict

Retention Date: ○ Not Specify ● Specify the Retention Expiration 12/20/2013 ○ Specify the Retention Period 0 years 0 months 0 days ○ Permanent

Figure 2-36: Protection Change Execution Dialog

Select the volume for which you want to change the setting, specify the access right, retention mode, and retention date, and then click the Execute button.

You can specify two or more volumes at a time and execute the operation for all of them simultaneously.

Unexecutable volumes are shaded in gray and cannot be selected.

Selected Volume List

Information list of the volume selected in the information list display area appears.

The information of each individual item is updated only when the Execute button is clicked.

If Unexecutable is shown in the Execution Result field, the volume does not meet the execution conditions and therefore cannot be selected.

For the unexecutable volume, refer to Unexecutable Information and take one of the following actions.

Unexecutable Information	Action
Error LD	Retry after checking the LD status.
Not Protected	It cannot be executed when protection has not been set.
Retention mode is strict	Setting cannot be changed when the retention mode is strict.
Have been registered to Atgroup	Retry after deleting the volume from the ATgroup.
The volume cannot be operated for its state.	Retry after checking the volume state.
Monitoring stop	Retry after setting the disk array to be monitored.

Unexecutable Information	Action
The pair state of LD cannot be operated.	Retry after checking the pair state.
Retention mode cannot be changed to normal mode in secure mode	When the retention mode is secure, it cannot be changed to the normal mode.
Wrong retention date	Retry after checking the retention date.
Retention period cannot be changed shorter than before in secure mode	When the retention mode is secure, the retention period cannot be shortened.

Access Right

Specify the protection status of the volume. The following access rights can be specified.

Radio Button	Description
ReadOnly	The target volume is write-protected from the server.
NotAccessible	The target volume is read/write-protected from the server.

* Note that setting ReadOnly to a volume of which OS type is WN/WG may disable to mount it to the host.

Retention Mode

Specify the retention mode of the volume. The following retention modes can be specified.

Radio Button	Description
normal	Protection can be released or protection settings can be changed, regardless of the retention period.
secure	Protection cannot be released during the retention period. There are constraints on changing protection settings.
strict	Protection cannot be released during the retention period. Protection settings cannot be changed, either.

Retention Date

Specify the retention period of the volume. The retention period can be specified in the following formats.

Radio Button	Description
Not Specify	The retention period is set to 0, indicating the condition in which the volume retention period has already elapsed.
Specify the Retention Expiration	The retention period is set as the time from the current date to the specified date (year, month, and day). The volume is protected from the current date to the specified date.

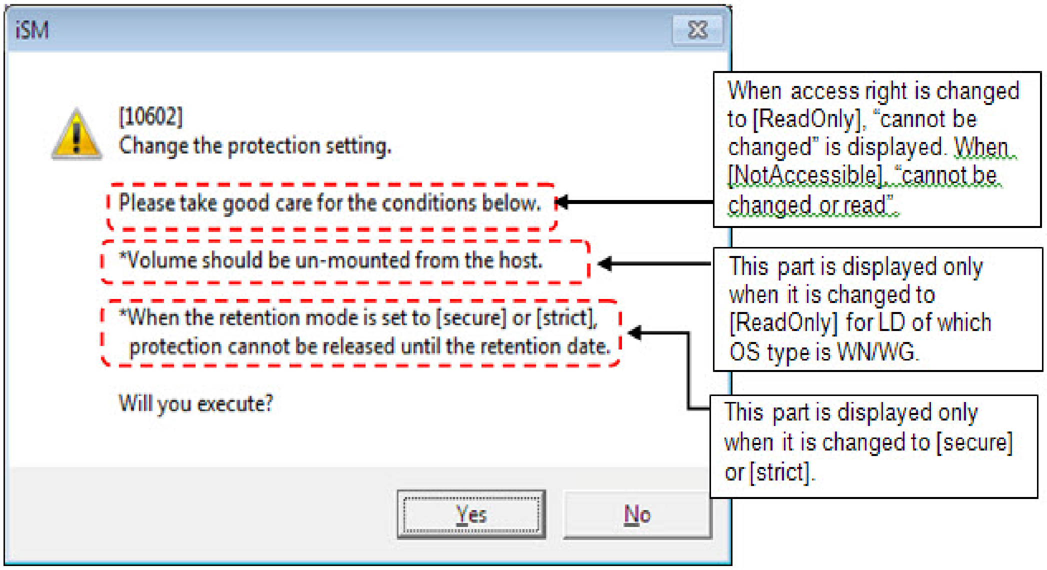
Radio Button	Description
Specify the Retention Period	Specify the number of years, months, or days for the retention period. The volume is protected for the specified duration starting at the current date.
Permanent	The retention period is permanent. The volume is permanently protected from the current date.

* When Not Specify is selected, note that the volume immediately becomes the status in which protection can be released.

When multiple volumes are selected, for the items of which settings for individual volumes are the same, the setting values are selected.

For the items of which settings for individual volumes are not the same, nothing is selected. If it is executed while nothing is selected, the item keeps the original setting of each volume.

When the Execute button is clicked, the following confirmation message appears.


iSM

[10602]
Change the protection setting.

Please take good care for the conditions below.

*Volume should be un-mounted from the host.

*When the retention mode is set to [secure] or [strict], protection cannot be released until the retention date.

Will you execute?

When access right is changed to [ReadOnly], "cannot be changed" is displayed. When [NotAccessible], "cannot be changed or read".

This part is displayed only when it is changed to [ReadOnly] for LD of which OS type is WN/WG.

This part is displayed only when it is changed to [secure] or [strict].

Figure 2-37: Confirmation

In this case, selecting No stops the processing.

Execution Conditions

To perform protection change, the following conditions must be satisfied.

- The target volume has been protected.
- The target volume has not been registered to ATgroup.
- The retention mode of the target volume is not strict.
- When the target volume is a replication volume, the pair has been separated.
- The target volume is not in rotation stop state.

The target volume must have been unmounted from the host.

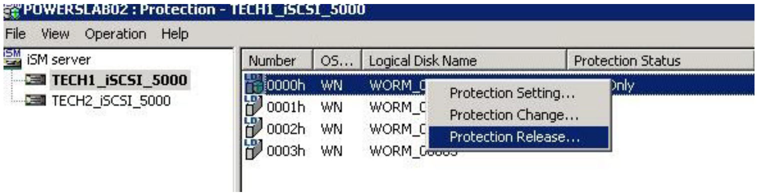
Volume Protection Release

Protection setting of a protected volume is released. When you release protection from a protected volume, you can also reinitialize the volume to clear the stored data.

Operating Procedure

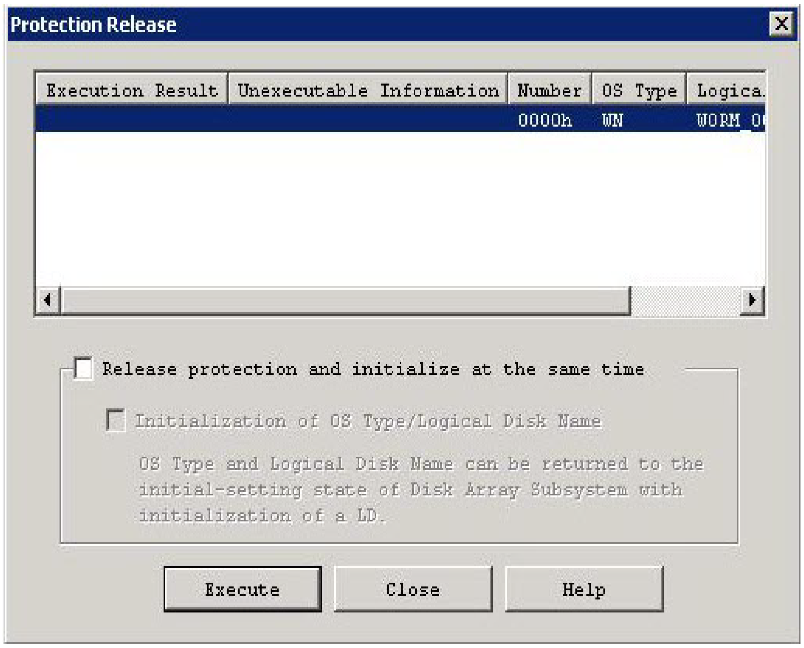
Display the information screen of the dialog for releasing a protected volume using one of the following procedures.

- Select a desired volume from the information list display area. Then, from the menu bar of the WORM management screen, select Operation   Protection Release.
- Select a desired volume from the information list display area. Then, right-click on it and select Protection Release.



Number	OS...	Logical Disk Name	Protection Status
0000h	WN	WORM_	Only
0001h	WN	WORM_C	
0002h	WN	WORM_C	
0003h	WN	WORM_0003	

Figure 2-38: Protection Release



Execution Result	Unexecutable Information	Number	OS Type	Logica
		0000h	WN	WORM_0

□ Release protection and initialize at the same time

□ Initialization of OS Type/Logical Disk Name

OS Type and Logical Disk Name can be returned to the initial-setting state of Disk Array Subsystem with initialization of a LD.

Figure 2-39: Information Screen Example of Release Dialog

Select the volume which you want to release from the list and then click the Execute button.

You can specify two or more volumes at a time and execute the operation for all of them simultaneously.

Unexecutable volumes are shaded in gray and cannot be selected.

Selected Volume List

Information list of the volume selected in the information list display area appears.

The information of each individual item is updated only when the Execute button is clicked.

If Unexecutable is shown in the Execution Result field, the volume does not meet the execution conditions and therefore cannot be selected.

For the unexecutable volume, refer to Unexecutable Information and take one of the following actions.

Unexecutable Information	Action
Error LD	Retry after checking the LD status.
Not Protected	It cannot be executed when protection has not been set.
Retention mode is secure	Protection cannot be released within the retention period because the retention mode is secure.
Retention mode is strict	Protection cannot be released within the retention period because the retention mode is strict.
The pair state of LD cannot be operated.	Retry after checking the pair status.
Monitoring stop	Retry after restarting monitoring.
The volume cannot be operated for its state.	Retry after checking the volume status.

For the volume of Cannot execute initialization, refer to Unexecutable Information and take one of the following actions.

Unexecutable Information	Action
Formatting	Retry after formatting is completed.
Cannot execute initialization on MV/RV	Initialization cannot be executed because the volume is MV or RV.

For the volume of Cannot execute initialization of OS Type/Logical Disk Name, refer to Unexecutable Information and take one of the following actions.

Unexecutable Information	Action
Cannot execute initialization of OS Type/Logical Disk Name on lock LD	Retry after unlocking the locked volume.

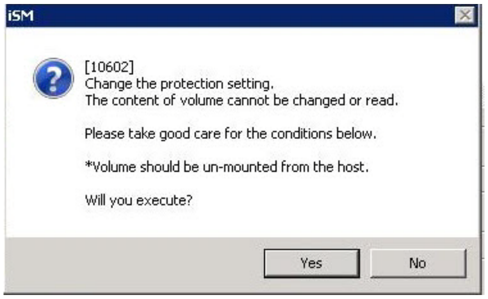
Release protection and initialize at the same time

When the checkbox is marked, the initialization of volume contents is executed at the same time of protection release.

Initialization of OS Type/Logical Disk Name

When the checkbox is marked, the OS Type/Logical Disk Name is returned to the initial setting of the disk array at the same time of the initialization.

When Release protection and initialize at the same time is not selected, clicking the Execute button displays the following confirmation message.



[10602]
Change the protection setting.
The content of volume cannot be changed or read.

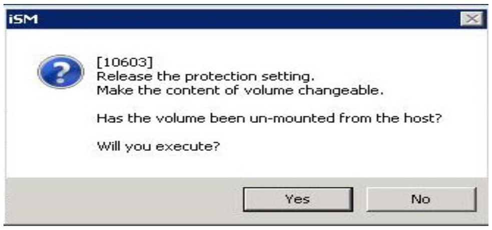
Please take good care for the conditions below.

*Volume should be un-mounted from the host.

Will you execute?

Figure 2-40: Execute Release Protection Confirmation

When Release protection and initialize at the same time is selected, clicking the Execute button displays the following confirmation message.



[10603]
Release the protection setting.
Make the content of volume changeable.

Has the volume been un-mounted from the host?

Will you execute?

Figure 2-41: Release Protection Setting Confirmation

Execution Conditions

To perform protection release, all of the following conditions must be satisfied.

When the retention mode is normal:

The target volume has been protected.

When the target volume is a replication volume, the pair has been separated.

The target volume is not in rotation stop state.

When the retention mode is secure or strict:

The target volume has been protected.

The protection period has been expired.

When the target volume is a replication volume, the pair has been separated.

The target volume is not in rotation stop state.

To initialize the volume contents, both of the following conditions must be satisfied.

The target volume is not a replication volume.

The target volume is not being formatted.

To initialize the OS Type/Logical Disk Name, the following conditions must be satisfied.

The target volume has not been locked.

The target volume is not a volume bound using the quick format.

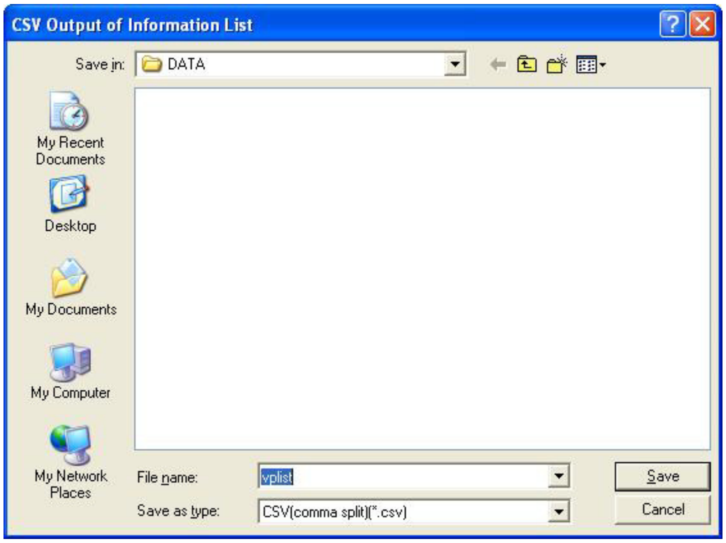
- When initialization is executed, only the start is displayed for the initialization operation. For the progress ratio and result of initialization, check the main screen (state monitoring screen). Even when initialization of OS Type/Logical Disk Name is executed, the OS Type/Logical Disk Name in the dialog is not changed. For the result of initialization of OS Type/Logical Disk Name, check the volume list on the WORM management screen.
- The target volume must have been unmounted from the host.

CSV Output of Information List

The information currently displayed in the information list display area is output as a CSV file and then saved.

Operating Procedure

To display the CSV Output of Information List Display screen, Select File CSV Output of Information List from the menu bar of the WORM management screen.



Save in: DATA

File name: vplist

Save as type: CSV(comma split)(*.csv)

Figure 2-42: CSV File

- Specify the save destination.
- Specify the file name.

The default file name is vplist.csv.

- Click the Save button to save the input information.

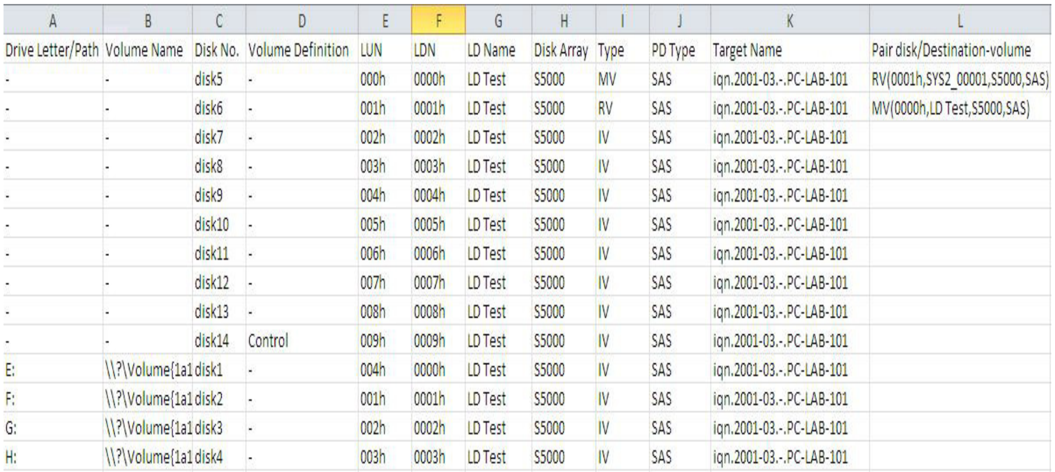
When the Cancel button is clicked, the screen is returned to the WORM management screen without saving the file.

CSV File of Information List

A CSV file example to be output when CSV Output of Information List is executed is shown below.

This file outputs information displayed on the screen by separating each piece of information by commas.

File Example



A	B	C	D	E	F	G	H	I	J	K	L
Drive Letter/Path	Volume Name	Disk No.	Volume Definition	LUN	LDN	LD Name	Disk Array	Type	PD Type	Target Name	Pair disk/Destination-volume
-	-	disk5	-	000h	0000h	LD Test	S5000	MV	SAS	iqn.2001-03.-.PC-LAB-101	RV(0001h,SYS2_00001,S5000,SAS)
-	-	disk6	-	001h	0001h	LD Test	S5000	RV	SAS	iqn.2001-03.-.PC-LAB-101	MV(0000h,LD Test,S5000,SAS)
-	-	disk7	-	002h	0002h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
-	-	disk8	-	003h	0003h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
-	-	disk9	-	004h	0004h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
-	-	disk10	-	005h	0005h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
-	-	disk11	-	006h	0006h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
-	-	disk12	-	007h	0007h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
-	-	disk13	-	008h	0008h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
-	-	disk14	Control	009h	0009h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
E:	\\?\Volume{1a1	disk1	-	004h	0000h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
F:	\\?\Volume{1a1	disk2	-	001h	0001h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
G:	\\?\Volume{1a1	disk3	-	002h	0002h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	
H:	\\?\Volume{1a1	disk4	-	003h	0003h	LD Test	S5000	IV	SAS	iqn.2001-03.-.PC-LAB-101	

Updating to the Latest Information

Executing the refresh function with the SnapSAN Manager server selected in the configuration display area updates the information about the disk array connected to the server. Also, the information displayed on the screen is cleared.

Executing the refresh function with a disk array selected in the configuration display area updates all the information about the selected disk array and leads to the state with the disk array selected.

In either case, if you cancel the refresh operation before it is completed, execute Refresh.

Perform one of the following procedures.

- From the menu bar, select View   Refresh.
- Press the F5 key.

Notification of Expired Retention

SnapSAN Manager provides the WORM notification function. Expired retention and a retention date approached set by the WORM function can be notified.

SnapSAN Manager regularly checks the protection status of a volume and notifies of the expired retention. When the protection state of the volume becomes expired retention, SnapSAN Manager records the message to syslog and the event log and displays the message to SnapSAN Manager client's GUI.

The message telling expired retention is output at one of the following timings during a specified period. For setting the check time of the protection status, refer to the installation guide attached to SnapSAN Manager.

- When starting the SnapSAN Manager server:
- When restarting monitoring of the disk array:
- At the check time of the protection status once a day:

The notification of expired retention is performed within the period specified in the environment definition file (default value is 1 day). For specifying the output period of the message of expired retention, refer to the installation guide attached to SnapSAN Manager.

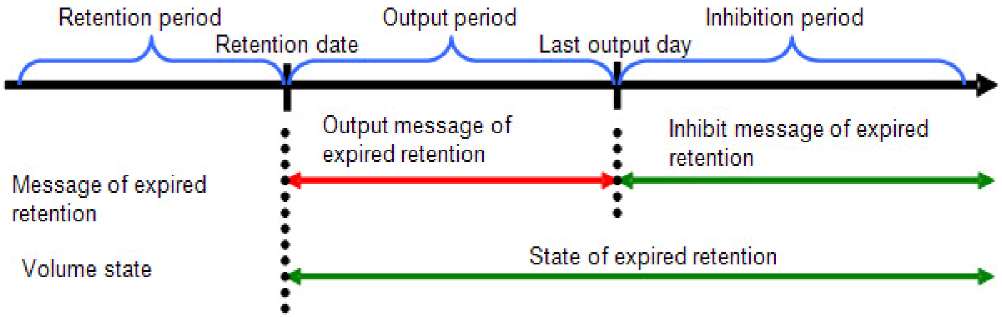

Retention period
Retention date
Output period
Last output day
Inhibition period
Output message of expired retention
Inhibit message of expired retention
Message of expired retention
Volume state
State of expired retention

Figure 2-43: Output Period of Message of Expired Retention

Example: When the retention date (the last day for protection) of a volume is December 1, 2009:

If the output period of the message of expired retention is set to two days, the output period of the message of expired retention is from December 2, 2009 to December 3, 2009. (Two days from the date on which retention expired, December 2, 2009.)

Retention Date Approached

SnapSAN Manager sends a notification of retention date approached to the administrator before the protection status of a volume becomes expired retention. On the specified day of previous notification, it records the message of retention date approached to syslog and the event log and displays the message to SnapSAN Manager client's GUI.

The message of retention date approached is output at one of the following timings on the specified day of previous notification. For setting the check time of the protection status, refer to the installation guide attached to SnapSAN Manager.

- When starting the SnapSAN Manager server:
- When restarting monitoring of the disk array:
- At the check time of protection status once a day:

Note that the notification of retention date approached is performed within the period specified in the environment definition file (default value is 0 day (that is, no previous notification)). For specifying the day of previous notification of retention date approached, refer to the installation guide attached to SnapSAN Manager.

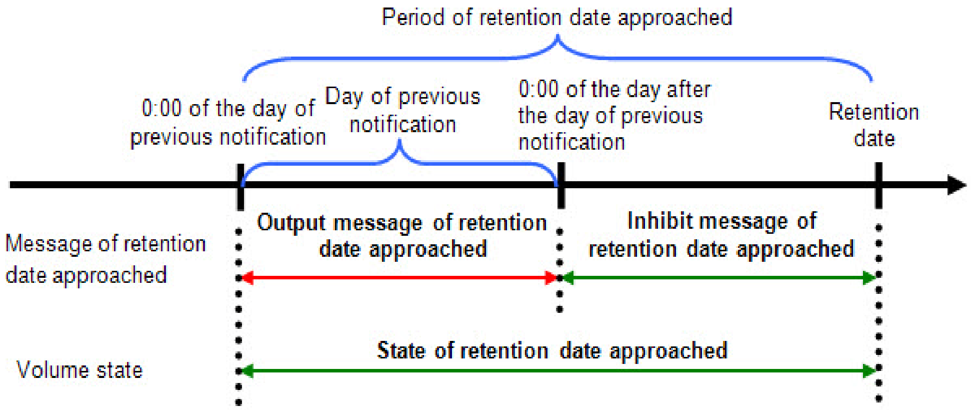

Period of retention date approached
0:00 of the day of previous notification
Day of previous notification
0:00 of the day after the day of previous notification
Retention date
Message of retention date approached
Output message of retention date approached
Inhibit message of retention date approached
Volume state
State of retention date approached

Figure 2-44: Output Period of Message of Retention Date Approached

Example: When the retention date (the last day for protection) of a volume is December 1, 2009:

If the period of retention date approached is set to two days before the retention date, the output period of the message of retention date approached is November 30, 2009. (Two days before the date on which retention expires, December 2, 2009.)

Chapter 3

WORM Operations

Operating WORM with SnapSAN Manager

This chapter describes how to operate WORM with Storage Manager (SnapSAN Manager).

SnapSAN Manager consists of server and client functions, the former controls the storage and the latter executes monitoring and operations, which allows the storage to be managed remotely.

In addition, the client function provides the following two GUIs:

- GUI based on Windows
- GUI based on the Web

In this manual, SnapSAN Manager client or client is used for describing the client function without separating the above two.

Also, to describe the former GUI only, SnapSAN Manager client (Win GUI) or client (Win GUI) is used, and to describe the latter GUI only, SnapSAN Manager client (Web GUI) or client (Web GUI) is used.

SnapSAN Manager provides the function for operating WORM and displaying information. You can perform the volume protection setting operation by the WORM function and view the protection status using the SnapSAN Manager client's GUI.

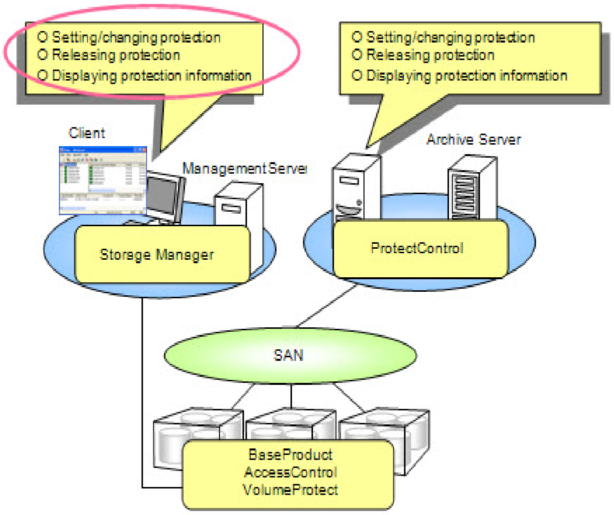


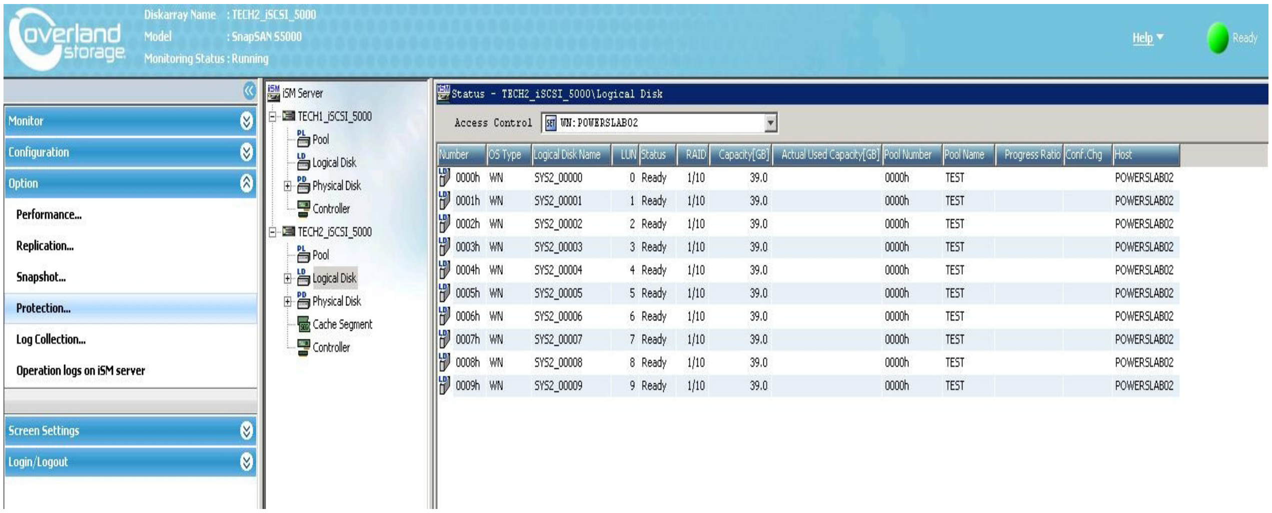
Figure 3-1: Opening WORM

SnapSAN Manager Main Window

The SnapSAN Manager main window is the first window that appears when you connect the SnapSAN Manager client to the SnapSAN Manager server. It displays the information about the configuration of the disk arrays monitored by SnapSAN Manager and the states of the resources. You can start the WORM management screen from the menu on the SnapSAN Manager main window.

The SnapSAN Manager main window displays the following information related to WORM.

Volume Protection Status



Diskarray Name : TECH2_iSCSI_5000
Model : SnapSAN S5000
Monitoring Status : Running

Status - TECH2_iSCSI_5000\Logical Disk

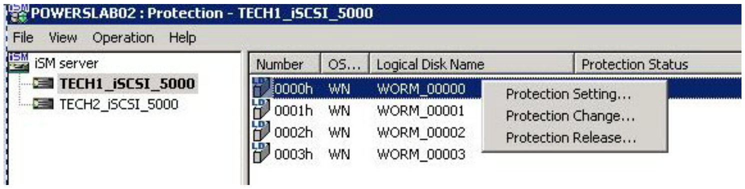
Access Control WN:POWERSLAB02

Number	OS Type	Logical Disk Name	LUN	Status	RAID	Capacity[GB]	Actual Used Capacity[GB]	Pool Number	Pool Name	Progress Ratio	Conf.Chg	Host
0000h	WN	SYS2_00000	0	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0001h	WN	SYS2_00001	1	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0002h	WN	SYS2_00002	2	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0003h	WN	SYS2_00003	3	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0004h	WN	SYS2_00004	4	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0005h	WN	SYS2_00005	5	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0006h	WN	SYS2_00006	6	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0007h	WN	SYS2_00007	7	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0008h	WN	SYS2_00008	8	Ready	1/10	39.0		0000h	TEST			POWERSLAB02
0009h	WN	SYS2_00009	9	Ready	1/10	39.0		0000h	TEST			POWERSLAB02

Figure 3-2: Main

SnapSAN Manager WORM Management

To implement long-term storage of data in non-falsifiable format, the SnapSAN Manager WORM management screen provides management screens for making various settings such as protection status and retention period on a volume-by-volume basis.



POWERSLAB02 : Protection - TECH1_iSCSI_5000

Number	OS...	Logical Disk Name	Protection Status
0000h	WN	WORM_00000	
0001h	WN	WORM_00001	
0002h	WN	WORM_00002	
0003h	WN	WORM_00003	

Figure 3-3: WORM Main

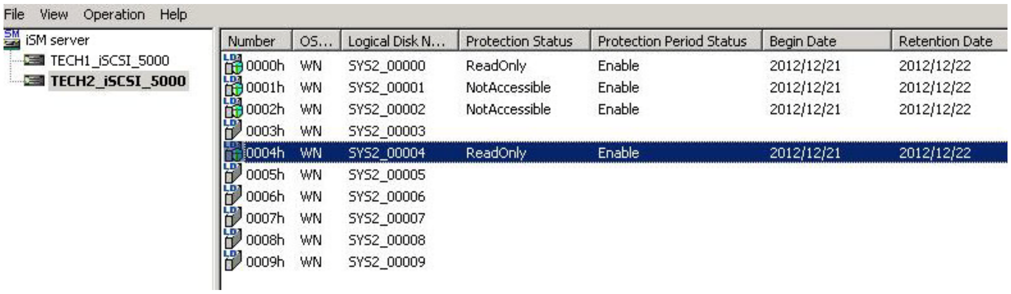
The SnapSAN Manager WORM management screen provides the function for operating the WORM and displaying the information by using the SnapSAN Manager client.

The SnapSAN Manager WORM management screen provides the following operations related to WORM and the function for displaying the information. Note that executing the WORM operations requires that the user role of the client be operator or administrator.

- Setting volume protection
- Changing volume protection settings

- Releasing volume protection
- Initializing volume contents
- Initializing volume OS Type/Logical Disk Name

The WORM management screen consists of the configuration display area] displaying the disk array configuration and states on the left side of the screen and the information list display area] on the right side of the screen that displays the information about the item selected in the configuration display area.



iSM server
TECH1_iSCSI_5000
TECH2_iSCSI_5000

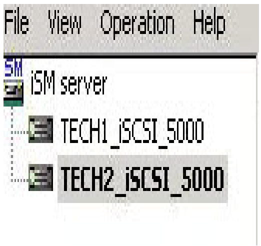
Number	OS...	Logical Disk N...	Protection Status	Protection Period Status	Begin Date	Retention Date
0000h	WN	SYS2_00000	ReadOnly	Enable	2012/12/21	2012/12/22
0001h	WN	SYS2_00001	NotAccessible	Enable	2012/12/21	2012/12/22
0002h	WN	SYS2_00002	NotAccessible	Enable	2012/12/21	2012/12/22
0003h	WN	SYS2_00003				
0004h	WN	SYS2_00004	ReadOnly	Enable	2012/12/21	2012/12/22
0005h	WN	SYS2_00005				
0006h	WN	SYS2_00006				
0007h	WN	SYS2_00007				
0008h	WN	SYS2_00008				
0009h	WN	SYS2_00009				

Figure 3-4: WORM Management

Configuration Display Area

The configuration display area displays the configuration information of WORM function in the format of a tree view.

The configuration display area displays a list of disk arrays that are being monitored by SnapSAN Manager and for which the WORM function can be used.



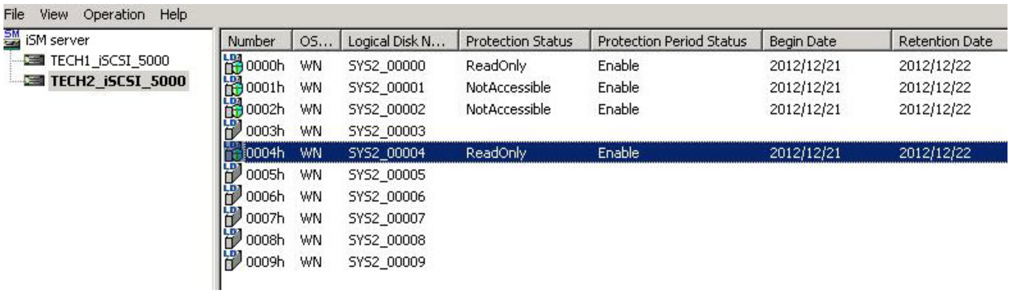
iSM server
TECH1_iSCSI_5000
TECH2_iSCSI_5000

Figure 3-5: Configuration Display

In the configuration display area, the state of each managed item is indicated by the shape of the icon and the shading of the color.

The icon of a disk array not being monitored is shaded in gray.

Information List Display Area



Number	OS...	Logical Disk N...	Protection Status	Protection Period Status	Begin Date	Retention Date
0000h	WN	SYS2_00000	ReadOnly	Enable	2012/12/21	2012/12/22
0001h	WN	SYS2_00001	NotAccessible	Enable	2012/12/21	2012/12/22
0002h	WN	SYS2_00002	NotAccessible	Enable	2012/12/21	2012/12/22
0003h	WN	SYS2_00003				
0004h	WN	SYS2_00004	ReadOnly	Enable	2012/12/21	2012/12/22
0005h	WN	SYS2_00005				
0006h	WN	SYS2_00006				
0007h	WN	SYS2_00007				
0008h	WN	SYS2_00008				
0009h	WN	SYS2_00009				

Figure 3-6: Information List Display Area

The disk array list displays the information about the items described below. Double-clicking an item switches the display to the volume list of the disk array.

Disk Array Subsystem Name

The names of disk arrays that are being monitored by SnapSAN Manager and that can use the WORM function are displayed. Disk arrays which do not support the WORM function or for which WORM has not been purchased are not displayed.

Icon	Description
▬ etc.	Indicates that the disk array is operating normally.
⚠	Indicates that a volume in the expired status exists in the disk array.

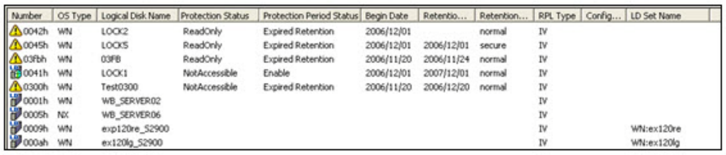
Number of Protection LDs

Displays the number of volumes for which volume protection setting has already been made.

Number of Expired LDs

Displays the number of volumes in the expired status.

Volume list



Number	OS Type	Logical Disk Name	Protection Status	Protection Period Status	Begin Date	Retentio...	Retention...	RPL Type	Config...	LD Set Name
0042h	WN	LOCK2	ReadOnly	Expired Retention	2006/12/01		normal	IV		
0045h	WN	LOCK5	ReadOnly	Expired Retention	2006/12/01	2006/12/01	secure	IV		
03fbh	WN	03FB	ReadOnly	Expired Retention	2006/11/20	2006/11/24	normal	IV		
0041h	WN	LOCK1	NotAccessible	Enable	2006/12/01	2007/12/01	normal	IV		
0300h	WN	Test0300	NotAccessible	Expired Retention	2006/11/20	2006/12/20	normal	IV		
0001h	WN	WB_SERVER02						IV		
0005h	NX	WB_SERVER06						IV		
0009h	WN	exp120re_S2900						IV		WN:ex120re
000ah	WN	ex120lg_S2900						IV		WN:ex120lg

Figure 3-7: Volume List

The volume list displays the information about the items described below.

Number

Displays the logical disk number of a volume in hexadecimal.

Displays the state of a volume with the icon next to number.

Icon	Description
LD	Indicates that the volume is in the data protection state.
ⓘ	Indicates that the volume is in the data protection state and the state of retention date approached.
⚠	Indicates that the volume is in the data protection state and the expired retention state.
LD	Indicates that the volume is not in the data protection state.
LD	Indicates that the volume is locked.

OS Type

Displays the OS type of volume.

Display	Description
A2	Indicates the logical disk is operating on the ACOS-2 system.
AX	Indicates the logical disk is operating on the AIX system.
CX	Indicates the logical disk is operating on the Solaris system.
LX	Indicates the logical disk is operating on the Linux system.
NX	Indicates the logical disk is operating on the HP-UX system.
SX	Indicates the logical disk is operating on the SUPER-UX system.
WN	Indicates the logical disk is operating on the Windows system (excluding GPT disk).
WG	Indicates the logical disk is operating on the GPT disk of the Windows system.

Logical Disk Name

Displays the logical disk name of the volume.

Protection Status

Displays the protection status of the volume.

Display	Description
ReadOnly	Read-enabled and write-protected
NotAccessible	Read/write-protected
(Blank)	Protection has not been set.

Protection Period Status

Displays the protection period status of the volume.

Display	Description
Enable	Within the retention period
Enable (Retention date approached)	Within the retention period and the status of retention date approached
Expired Retention	Retention period expired.
(Blank)	Protection has not been set.

Begin Date

Displays the date on which protection is set in the yyyy/mm/dd format. If protection has not been set, it is displayed in blank.

Retention Date

Displays the retention date in the yyyy/mm/dd format. If protection has not been set or that the retention date was not set at protection setting, it is displayed in blank. If the retention expiration was set to permanent, Permanent is displayed.

Retention Mode

Displays the retention mode of the volume.

Display	Description
normal	You can release protection and reset the retention period at any time.
secure	You cannot release protection until the retention period has elapsed. However, you can extend the retention period or change the protection status.
strict	You cannot release protection until the retention period has elapsed. Neither can you reset the retention period and protection status.
(Blank)	Protection has not been set.

RPL Type

Displays the replication type of the volume.

This column does not appear when none of Overland Volume Cloning and Replication and Mirroring is purchased.

Display	Description
IV	Not used as a replication volume
MV	Used as a replication source volume
RV	Used as a replication destination volume
RV/MV	Used as both RV and MV

Configuration Change

Displays the setting status of configuration setting operation guard of the volume.

Display	Description
Lock	Guard has been set.
(Blank)	Guard has not been set.

LD Set Name

Displays up to four LD Set Names to which the volume belongs (numbers exceeding four are indicated by … at the end of line).

LD to be displayed must satisfy the following conditions.

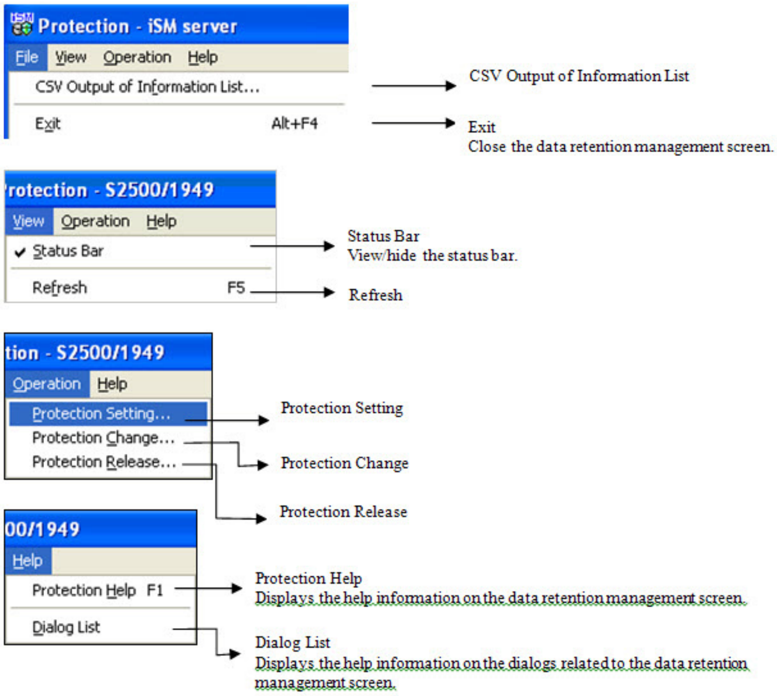
- RPL type is IV, MV, RV, or RV/MV.
- Does not belong to a reserve group.
- Not a Snapshot-related volume.
- Not a System Volume.
- Not a work disk for optimization.
- Not a L2 Cache volume.

Partition Name

The name of partition to which the volume belongs is displayed.

This column is not displayed for disk arrays for which Virtual Storage Partitioning has not been unlocked.

Menu Item List



CSV Output of Information List

Exit
Close the data retention management screen.

Status Bar
View/hide the status bar.

Refresh

Protection Setting

Protection Change

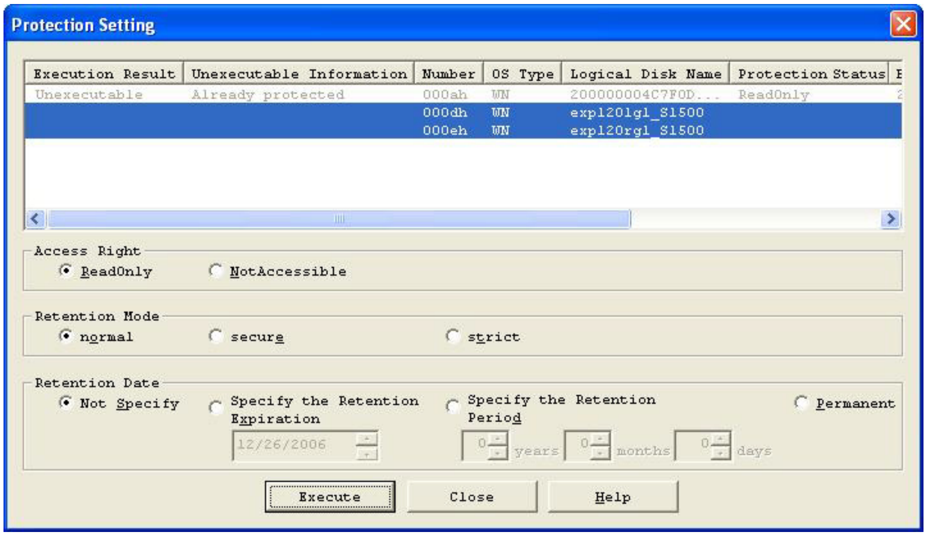
Protection Release

Protection Help
Displays the help information on the data retention management screen.

Dialog List
Displays the help information on the dialogs related to the data retention management screen.

Protection Setting/Change Dialog

The execution dialogs displayed for individual protection operations are described below.



Protection Setting

Execution Result	Unexecutable Information	Number	OS Type	Logical Disk Name	Protection Status	B
Unexecutable	Already protected	000ah	WN	200000004C7F0D...	ReadOnly	2
		000dh	WN	expl20lgl_S1500		
		000eh	WN	expl20rgl_S1500		

Access Right
● ReadOnly ○ NotAccessible

Retention Mode
● normal ○ secure ○ strict

Retention Date
● Not Specify ○ Specify the Retention Expiration 12/26/2006 ○ Specify the Retention Period 0 years 0 months 0 days ○ Permanent

Figure 3-8: Protection Setting

The information screen of the execution dialog displays the information about the items described below. The information of each individual item is updated only when the Execute] button is clicked.

Execution Result

Displays the result of execution. The operation cannot be executed for a volume for which Unexecutable is displayed.

Unexecutable Information

Displays the reason why operation cannot be executed.

Number

Displays the logical disk number in hexadecimal.

OS Type

Displays the volume OS type.

Logical Disk Name

Displays the logical disk name.

Protection Status

Displays the protection status of the volume.

Begin Date

Displays the date on which protection is set.

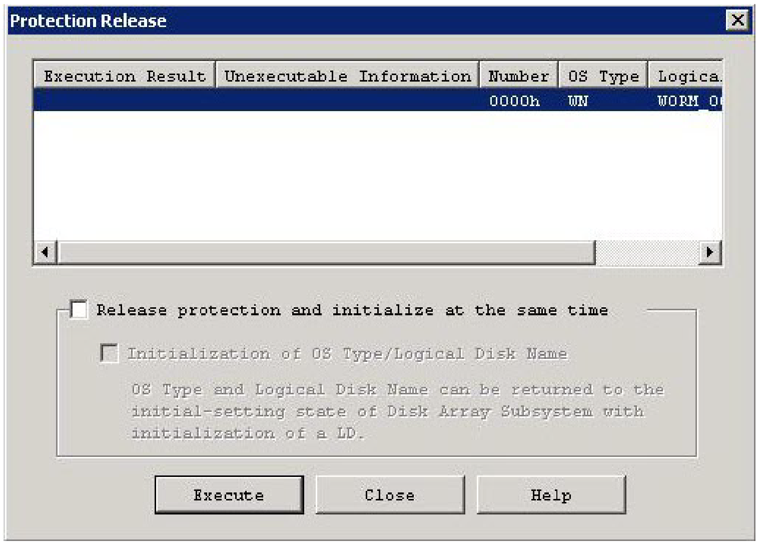
Retention Date

Displays the retention date.

Retention Mode

Displays the retention mode of the volume.

Protection Release Dialog



Execution Result	Unexecutable Information	Number	OS Type	Logica
		0000h	WN	WORM 0

□ Release protection and initialize at the same time

□ Initialization of OS Type/Logical Disk Name

OS Type and Logical Disk Name can be returned to the initial-setting state of Disk Array Subsystem with initialization of a LD.

Figure 3-9: Protection Release Dialog

The information screen of the Protection Release dialog displays the information about the items described below. The information of each individual item is updated only when the Execute] button is clicked.

Execution Result

Displays the result of execution. The operation cannot be executed for a volume for which Unexecutable is displayed.

Unexecutable Information

Displays the reason why operation cannot be executed.

Number

Displays the logical disk number in hexadecimal.

OS Type

Displays the volume OS type.

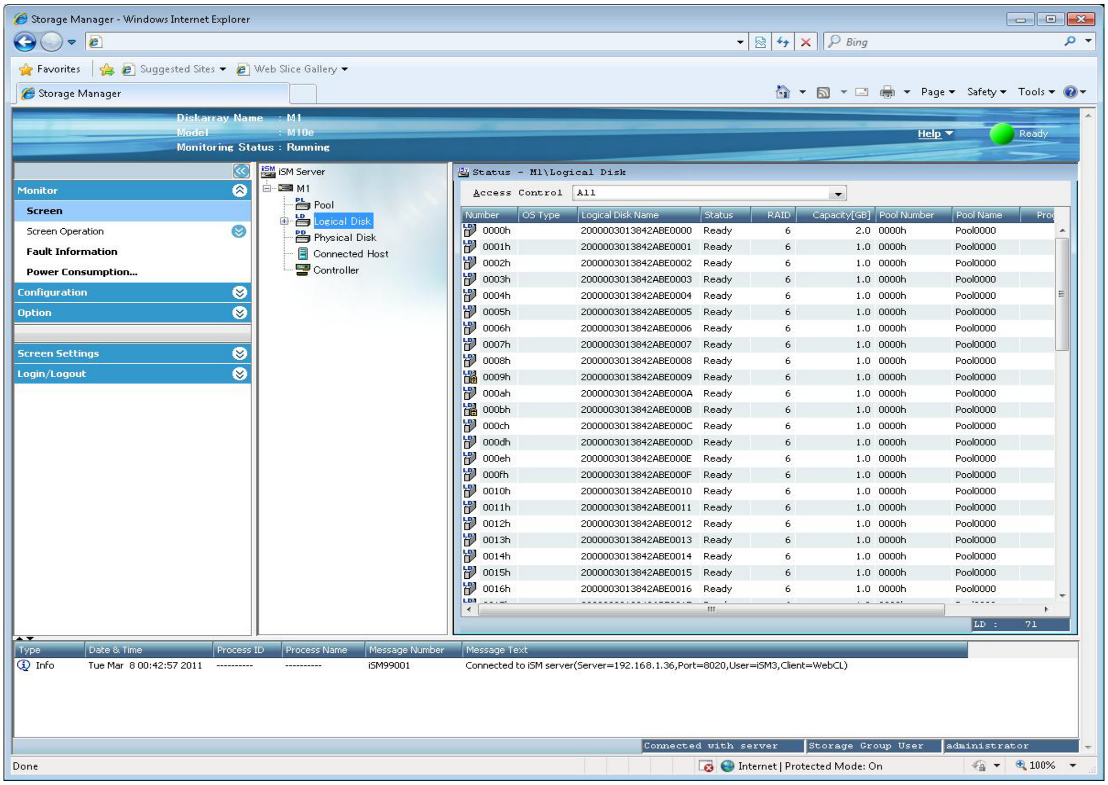
Logical Disk Name

Displays the logical disk name.

SnapSAN Manager Main Window

The SnapSAN Manager main window is the first window that appears when you connect the SnapSAN Manager client to the SnapSAN Manager server. It displays the information about the configuration of the disk arrays monitored by SnapSAN Manager and the states of the resources.

You can view the volume protection conditions of the WORM function in the logical disk list screen and logical disk details information screen within the SnapSAN Manager main window.



Diskarray Name : M1
Model : M10e
Monitoring Status : Running

Status - M1\Logical Disk

Access Control: All

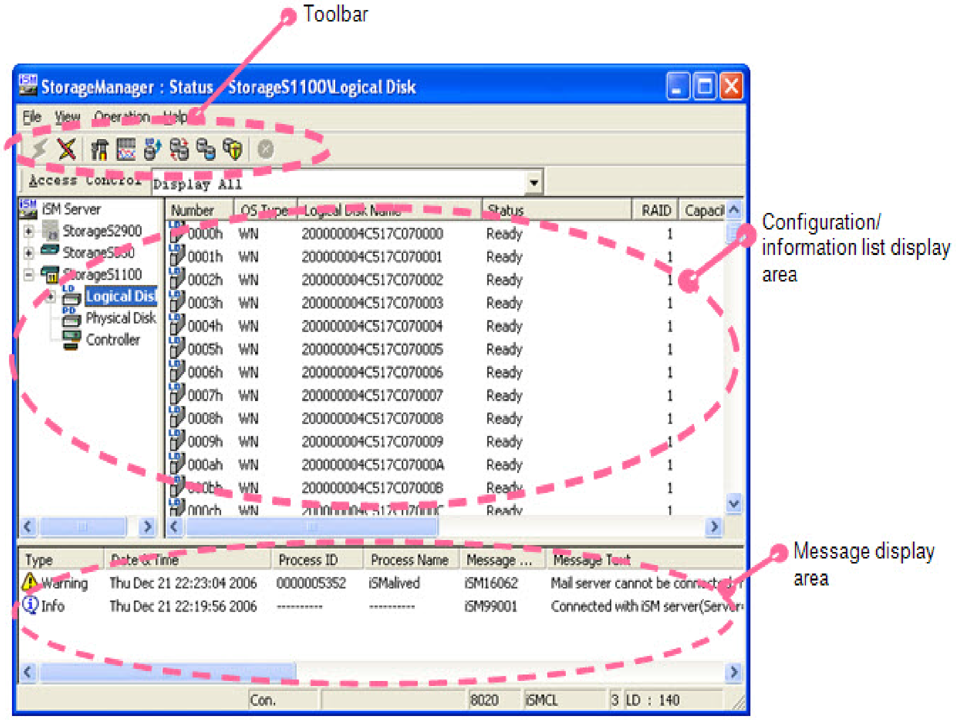
Number	OS Type	Logical Disk Name	Status	RAID	Capacity[GB]	Pool Number	Pool Name	Pro
0000h		2000003013842ABE0000	Ready	6	2.0	0000h	Pool0000	
0001h		2000003013842ABE0001	Ready	6	1.0	0000h	Pool0000	
0002h		2000003013842ABE0002	Ready	6	1.0	0000h	Pool0000	
0003h		2000003013842ABE0003	Ready	6	1.0	0000h	Pool0000	
0004h		2000003013842ABE0004	Ready	6	1.0	0000h	Pool0000	
0005h		2000003013842ABE0005	Ready	6	1.0	0000h	Pool0000	
0006h		2000003013842ABE0006	Ready	6	1.0	0000h	Pool0000	
0007h		2000003013842ABE0007	Ready	6	1.0	0000h	Pool0000	
0008h		2000003013842ABE0008	Ready	6	1.0	0000h	Pool0000	
0009h		2000003013842ABE0009	Ready	6	1.0	0000h	Pool0000	
000ah		2000003013842ABE000A	Ready	6	1.0	0000h	Pool0000	
000bh		2000003013842ABE000B	Ready	6	1.0	0000h	Pool0000	
000ch		2000003013842ABE000C	Ready	6	1.0	0000h	Pool0000	
000dh		2000003013842ABE000D	Ready	6	1.0	0000h	Pool0000	
000eh		2000003013842ABE000E	Ready	6	1.0	0000h	Pool0000	
000fh		2000003013842ABE000F	Ready	6	1.0	0000h	Pool0000	
0010h		2000003013842ABE0010	Ready	6	1.0	0000h	Pool0000	
0011h		2000003013842ABE0011	Ready	6	1.0	0000h	Pool0000	
0012h		2000003013842ABE0012	Ready	6	1.0	0000h	Pool0000	
0013h		2000003013842ABE0013	Ready	6	1.0	0000h	Pool0000	
0014h		2000003013842ABE0014	Ready	6	1.0	0000h	Pool0000	
0015h		2000003013842ABE0015	Ready	6	1.0	0000h	Pool0000	
0016h		2000003013842ABE0016	Ready	6	1.0	0000h	Pool0000	

LD : 71

Type	Date & Time	Process ID	Process Name	Message Number	Message Text
Info	Tue Mar 8 00:42:57 2011	----------	----------	iSM99001	Connected to iSM server(Server=192.168.1.36,Port=8020,User=iSM3,Client=WebCL)

Connected with server | Storage Group User | administrator

Figure 3-10: Main



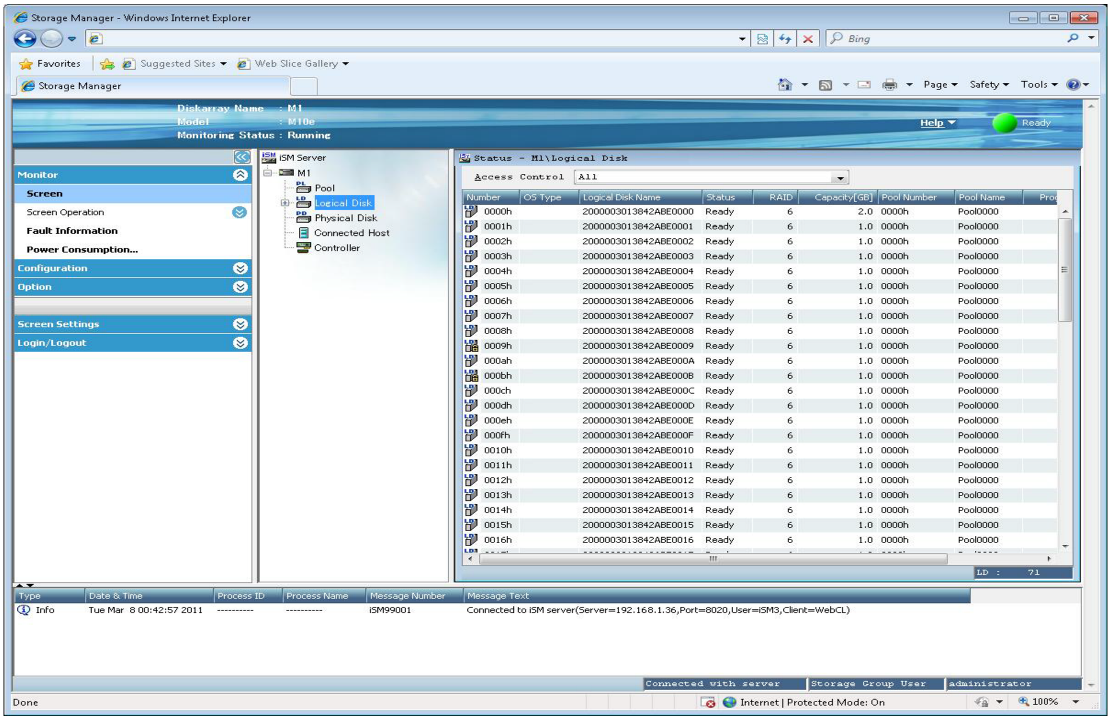
Number	OS Type	Logical Disk Name	Status	RAID	Capaci
0000h	WN	200000004C517C070000	Ready	1	
0001h	WN	200000004C517C070001	Ready	1	
0002h	WN	200000004C517C070002	Ready	1	
0003h	WN	200000004C517C070003	Ready	1	
0004h	WN	200000004C517C070004	Ready	1	
0005h	WN	200000004C517C070005	Ready	1	
0006h	WN	200000004C517C070006	Ready	1	
0007h	WN	200000004C517C070007	Ready	1	
0008h	WN	200000004C517C070008	Ready	1	
0009h	WN	200000004C517C070009	Ready	1	
000ah	WN	200000004C517C07000A	Ready	1	
000bh	WN	200000004C517C07000B	Ready	1	
000ch	WN	200000004C517C07000C	Ready	1	

Type	Date & Time	Process ID	Process Name	Message ...	Message Text
Warning	Thu Dec 21 22:23:04 2006	0000005352	iSMalived	iSM16062	Mail server cannot be connected. (
Info	Thu Dec 21 22:19:56 2006	----------	----------	iSM99001	Connected with iSM server(Server:

Figure 3-11: Main

Logical Disk List Screen

You can display the logical disk list screen by selecting (clicking the left button on) Logical Disk] in configuration display area. This screen displays various attribute information such as logical disk name, operating status, and capacity. When WORM has been purchased, the volume protection conditions of the WORM function are also displayed.



Diskarray Name : M1
Model : M10e
Monitoring Status : Running

Status - M1\Logical Disk

Access Control: All

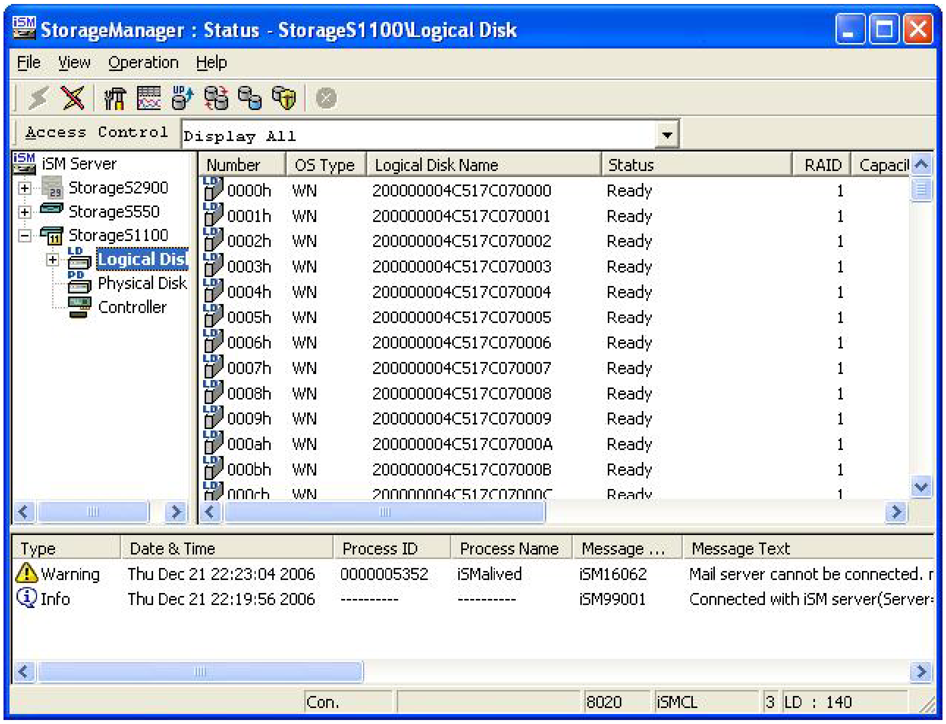
Number	OS Type	Logical Disk Name	Status	RAID	Capacity[GB]	Pool Number	Pool Name	Pro
0000h		2000003013842ABE0000	Ready	6	2.0	0000h	Pool0000	
0001h		2000003013842ABE0001	Ready	6	1.0	0000h	Pool0000	
0002h		2000003013842ABE0002	Ready	6	1.0	0000h	Pool0000	
0003h		2000003013842ABE0003	Ready	6	1.0	0000h	Pool0000	
0004h		2000003013842ABE0004	Ready	6	1.0	0000h	Pool0000	
0005h		2000003013842ABE0005	Ready	6	1.0	0000h	Pool0000	
0006h		2000003013842ABE0006	Ready	6	1.0	0000h	Pool0000	
0007h		2000003013842ABE0007	Ready	6	1.0	0000h	Pool0000	
0008h		2000003013842ABE0008	Ready	6	1.0	0000h	Pool0000	
0009h		2000003013842ABE0009	Ready	6	1.0	0000h	Pool0000	
000ah		2000003013842ABE000A	Ready	6	1.0	0000h	Pool0000	
000bh		2000003013842ABE000B	Ready	6	1.0	0000h	Pool0000	
000ch		2000003013842ABE000C	Ready	6	1.0	0000h	Pool0000	
000dh		2000003013842ABE000D	Ready	6	1.0	0000h	Pool0000	
000eh		2000003013842ABE000E	Ready	6	1.0	0000h	Pool0000	
000fh		2000003013842ABE000F	Ready	6	1.0	0000h	Pool0000	
0010h		2000003013842ABE0010	Ready	6	1.0	0000h	Pool0000	
0011h		2000003013842ABE0011	Ready	6	1.0	0000h	Pool0000	
0012h		2000003013842ABE0012	Ready	6	1.0	0000h	Pool0000	
0013h		2000003013842ABE0013	Ready	6	1.0	0000h	Pool0000	
0014h		2000003013842ABE0014	Ready	6	1.0	0000h	Pool0000	
0015h		2000003013842ABE0015	Ready	6	1.0	0000h	Pool0000	
0016h		2000003013842ABE0016	Ready	6	1.0	0000h	Pool0000	

LD : 71

Type	Date & Time	Process ID	Process Name	Message Number	Message Text
Info	Tue Mar 8 00:42:57 2011	----------	----------	iSM99001	Connected to iSM server(Server=192.168.1.36,Port=8020,User=iSM3,Client=WebCL)

Connected with server | Storage Group User | administrator

Figure 3-12: Logical Disk



Access Control: Display All

Number	OS Type	Logical Disk Name	Status	RAID	Capacil
0000h	WN	200000004C517C070000	Ready	1	
0001h	WN	200000004C517C070001	Ready	1	
0002h	WN	200000004C517C070002	Ready	1	
0003h	WN	200000004C517C070003	Ready	1	
0004h	WN	200000004C517C070004	Ready	1	
0005h	WN	200000004C517C070005	Ready	1	
0006h	WN	200000004C517C070006	Ready	1	
0007h	WN	200000004C517C070007	Ready	1	
0008h	WN	200000004C517C070008	Ready	1	
0009h	WN	200000004C517C070009	Ready	1	
000ah	WN	200000004C517C07000A	Ready	1	
000bh	WN	200000004C517C07000B	Ready	1	
000ch	WN	200000004C517C07000C	Ready	1	

Type	Date & Time	Process ID	Process Name	Message ...	Message Text
Warning	Thu Dec 21 22:23:04 2006	0000005352	iSMalived	iSM16062	Mail server cannot be connected. r
Info	Thu Dec 21 22:19:56 2006	----------	----------	iSM99001	Connected with iSM server(Server=

Con. | 8020 | iSMCL | 3 | LD : 140

Figure 3-13: Logical Disk Status

The items below show the volume protection conditions.

Purpose

Displays the purpose of a logical disk in any of the following at Purpose column.

RPL: Logical disk to which only a pair for replication is set

Snapshot: Logical disk to which only snapshot is set

Link-volume: Logical disk that is a link-volume (LV)

RPL/snapshot: Logical disk to which a pair for replication and snapshot setting have already been set

Optimization: Work disk for performance optimization

Data Protection: Logical disk to which the data protection setting has already been set

RPL/Data Protection: Logical disk to which a pair for replication and data protection setting have already been set

System Volume: Volume to store storage system information

Replication Reserved Volume:

Volume to store the data replication management information

Data Migration Reserved Volume:

Volume to store the data migration management information

Control Volume: Logical disks for control volumes

L2 Cache: Logical disks for L2 Cache

(Blank): General logical disk to which no specific purpose is set

Data Protection

Displays whether a logical disk is protected in any of the following at the Data Protection column. When WORM has not been purchased, this item does not appear.

protection: Protected

(Blank): Unprotected

When you have set the WORM function to enable volume reinitialization upon protection release, you can view the following items to check the state or progress ratio of reinitialization.

Status

Displays the reinitialization status of logical disk in any of the following at Status column.

Ready: Logical disk is in normal operation. (Reinitialization completed)

Attn.(formatting): During logic formatting (Being initialized)

* The logical disk is not available until logic formatting is completed.

Attn.(format-fail): Fails in logic formatting (Reinitialization failed)

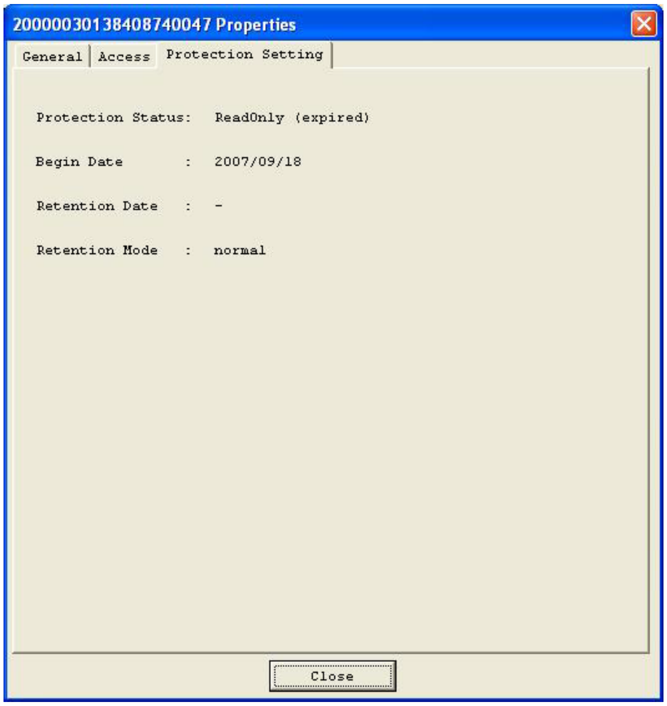
Attn.(stop): Logical disk is in rotation stop status

Progress Ratio

Displays the progress ratio in logical disk where a formatting event occurs.

Logical Disk Details Information Screen

You can display the logical disk details information screen by selecting (clicking the left button on) an optional logical disk, right clicking the logical disk, and selecting Properties] (or selecting View]   Properties] from the menu (for SnapSAN Manager clients (Win GUI))) in configuration display area or information list display area.



Protection Status: ReadOnly (expired)

Begin Date : 2007/09/18

Retention Date : -

Retention Mode : normal

Figure 3-14: Protection Setting Properties

Protection Status

Displays the protection status in any of the following.

ReadOnly: Read-only

NotAccessible: Read/write-protect

ReadOnly (expired): Read-only (expired)

NotAccessible (expired): Read/write-protect (expired)

Begin Date

Displays the date on which protection is set.

Retention Date

Displays the WORM date.

When the retention date has not been set, a hyphen (-) is displayed. If the retention date was set to permanent, Permanent is displayed.

Retention Mode

Displays the retention mode in any of the following.

normal: You can release protection and reset the retention period at any time.

secure: You cannot release protection until the retention period has elapsed. However, you can extend the retention period or change the protection status.

strict: You cannot release protection until the retention period has elapsed. Neither can you reset the retention period and protection status.

WORM Operations

Protection is set on a volume-by-volume basis. Since the write operation to the protected volumes is prevented, the data consistency is guaranteed.

You perform each operation by first selecting the target volume from the volume list displayed in the WORM management screen and then using the relevant menu that is chosen from the menu bar or displayed when you right-click on it.

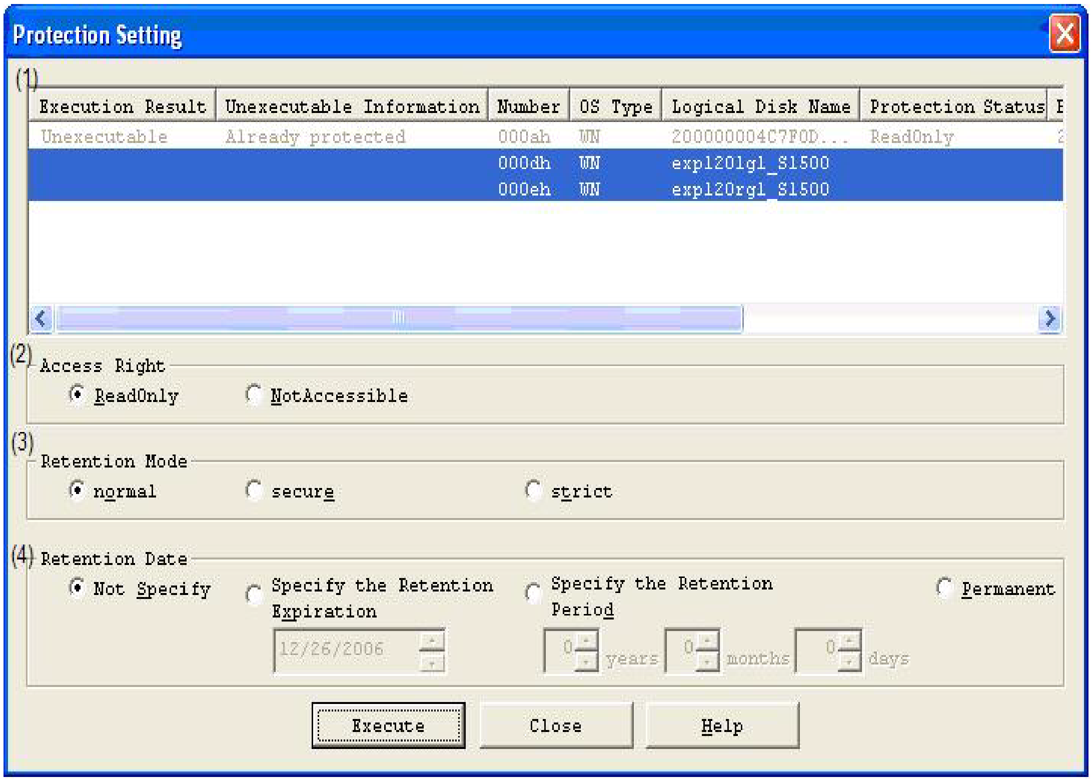
Volume Protection Setting

Protection is set on a volume-by-volume basis. Since the write operation to the protected volumes is prevented, the data consistency is guaranteed.

Operating Procedure

Display the Protection Setting screen using one of the following procedures.

- Select a desired volume from the information list display area. Then, from the menu bar of the WORM management screen, select Operation]   Protection Setting].
- Select a desired volume from the information list display area. Then, right-click on it and select Protection Setting].



Protection Setting

(1)

Execution Result	Unexecutable Information	Number	OS Type	Logical Disk Name	Protection Status	F
Unexecutable	Already protected	000ah	WN	200000004C7F0D...	ReadOnly	2
		000dh	WN	expl20lgl_S1500		
		000eh	WN	expl20rgl_S1500		

(2) Access Right

● ReadOnly ○ NotAccessible

(3) Retention Mode

● normal ○ secure ○ strict

(4) Retention Date

● Not Specify ○ Specify the Retention Expiration 12/26/2006 ○ Specify the Retention Period 0 years 0 months 0 days ○ Permanent

Figure 3-15: Protection Setting

Select the volume for which you want to set protection from the list, specify the access right, retention mode, and retention date, and then click the Execute] button.

You can specify two or more volumes at a time and execute the operation for all of them simultaneously.

Unexecutable volumes are shaded in gray and cannot be selected.

Selected Volume List

Information list of the volume selected in the information list display area appears.

If Unexecutable is shown in the Execution Result] field, the volume does not meet the execution conditions and therefore cannot be selected.

For the unexecutable volume, refer to Unexecutable Information] and take one of the following actions.

Unexecutable Information	Action
Error LD	Retry after checking the LD status.
Already protected	Protection cannot be set again to the volume that has been already protected.
Have been registered to Atgroup	Retry after deleting the volume from the ATgroup.
The volume cannot be operated for its state.	Retry after checking the LD status.
Monitoring stop	Retry after setting the disk array to be monitored.
The pair state of LD cannot be operated.	Retry after checking the pair status.
Data being migrated	Retry after checking the volume status.

Access Right

Specify the protection status of the volume. The following access rights can be specified.

Radio Button	Description
ReadOnly	The target volume is write-protected from the server.
NotAccessible	The target volume is read/write-protected from the server.

* Note that setting [ReadOnly] to a volume of which OS type is WN/WG may disable to mount it to the host.

Retention Mode

Specify the retention mode of the volume. The following retention modes can be specified.

Radio Button	Description
normal	Protection can be released or protection settings can be changed, regardless of the retention period.
secure	Protection cannot be released during the retention period. There are constraints on changing protection settings.

Radio Button	Description
strict	Protection cannot be released during the retention period. Protection settings cannot be changed, either.

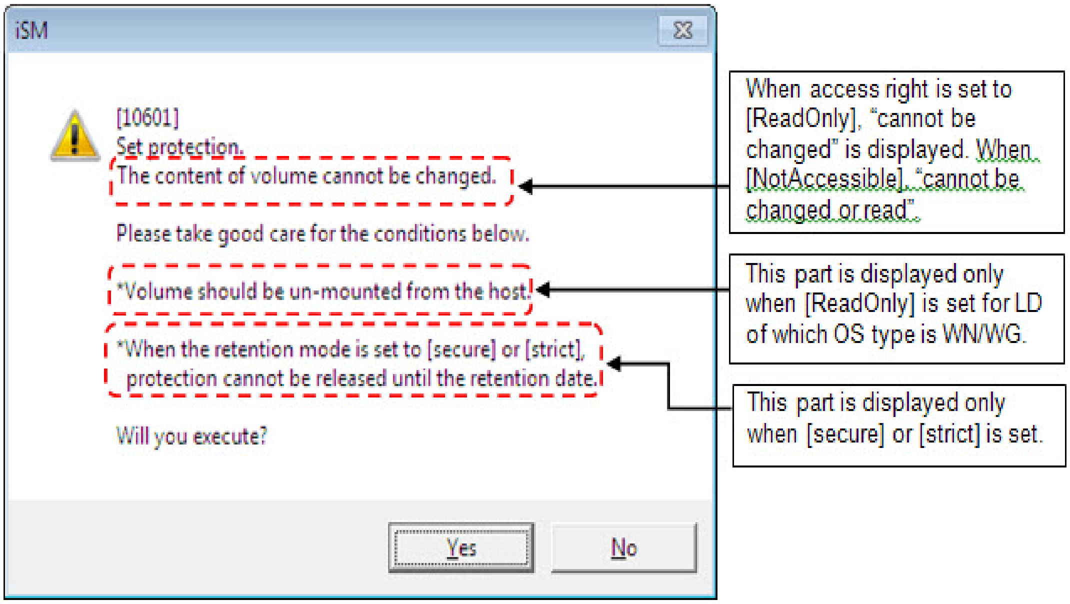
Retention Date

Specify the retention period of the volume. The retention period can be specified in the following formats.

Radio Button	Description
Not Specify	The retention period is set to 0, indicating the condition in which the volume retention period has already elapsed.
Specify the Retention Expiration	The retention period is set as the time from the current date to the specified date (year, month, and day). The volume is protected from the current date to the specified date.
Specify the Retention Period	Specify the number of years, months, or days for the retention period. The volume is protected for the specified duration starting at the current date.
Permanent	The retention period is permanent. The volume is permanently protected from the current date.

* When Not Specify] is selected, note that the volume immediately becomes the status in which protection can be released.

When the Execute] button is clicked, the following confirmation message appears.



[10601]
Set protection.
The content of volume cannot be changed.

Please take good care for the conditions below.

*Volume should be un-mounted from the host.

*When the retention mode is set to [secure] or [strict], protection cannot be released until the retention date.

Will you execute?

When access right is set to [ReadOnly], "cannot be changed" is displayed. When [NotAccessible], "cannot be changed or read".

This part is displayed only when [ReadOnly] is set for LD of which OS type is WN/WG.

This part is displayed only when [secure] or [strict] is set.

Figure 3-16: Confirmation

In this case, selecting No] stops the processing.

Execution Conditions

To perform protection setting, the following conditions must be satisfied.

- The target volume is not protected.
- The target volume has not been assigned to a reserve group.
- The target volume is not a System Volume.
- The target volume is not a snapshot-related volume (SDV, BV, SV, SV*, LV).
- The target volume is not being initialized.
- The target volume has not been registered to ATgroup.
- When the target volume is a replication volume, the pair has been separated.
- The target volume is not being used by the performance optimization function (not being scheduled, either).
- The target volume is not in rotation stop state.
- The target volume is not a control volume.
- Data of the target volume is not being migrated by the DataMigration function.
- The target volume is not a L2 Cache volume.
- The target volume must have been unmounted from the host.

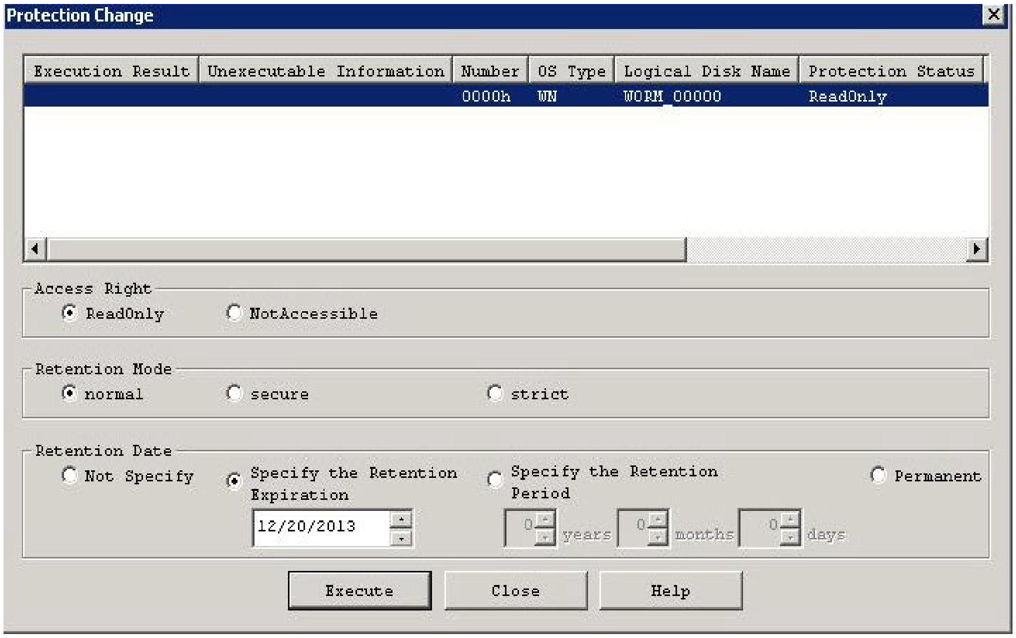
Volume Protection Change

Protection setting can be changed on a volume-by-volume basis. You can extend the retention period or change the protection status.

Operating Procedure

Display the Protection Change screen using one of the following procedures.

- Select a desired volume from the information list display area. Then, from the menu bar of the WORM management screen, select Operation] Protection Change].
- Select a desired volume from the information list display area. Then, right-click on it and select Protection Change].



Protection Change

Execution Result	Unexecutable Information	Number	OS Type	Logical Disk Name	Protection Status
		0000h	WN	WORM_00000	ReadOnly

Access Right

● ReadOnly ○ NotAccessible

Retention Mode

● normal ○ secure ○ strict

Retention Date

○ Not Specify ● Specify the Retention Expiration 12/20/2013 ○ Specify the Retention Period 0 years 0 months 0 days ○ Permanent

Figure 3-17: Information Screen Example of Protection Change Execution Dialog

Select the volume for which you want to change the setting, specify the access right, retention mode, and retention date, and then click the Execute] button.

You can specify two or more volumes at a time and execute the operation for all of them simultaneously.

Unexecutable volumes are shaded in gray and cannot be selected.

Selected Volume List

Information list of the volume selected in the information list display area appears.

The information of each individual item is updated only when the Execute] button is clicked.

If Unexecutable is shown in the Execution Result] field, the volume does not meet the execution conditions and therefore cannot be selected.

For the unexecutable volume, refer to Unexecutable Information] and take one of the following actions.

Unexecutable Information	Action
Error LD	Retry after checking the LD status.
Not Protected	It cannot be executed when protection has not been set.
Retention mode is strict	Setting cannot be changed when the retention mode is strict.
Have been registered to Atgroup	Retry after deleting the volume from the ATgroup.
The volume cannot be operated for its state.	Retry after checking the volume state.
Monitoring stop	Retry after setting the disk array to be monitored.

Unexecutable Information	Action
The pair state of LD cannot be operated.	Retry after checking the pair state.
Retention mode cannot be changed to normal mode in secure mode	When the retention mode is secure, it cannot be changed to the normal mode.
Wrong retention date	Retry after checking the retention date.
Retention period cannot be changed shorter than before in secure mode	When the retention mode is secure, the retention period cannot be shortened.

Access Right

Specify the protection status of the volume. The following access rights can be specified.

Radio Button	Description
ReadOnly	The target volume is write-protected from the server.
NotAccessible	The target volume is read/write-protected from the server.

* Note that setting ReadOnly] to a volume of which OS type is WN/WG may disable to mount it to the host.

Retention Mode

Specify the retention mode of the volume. The following retention modes can be specified.

Radio Button	Description
normal	Protection can be released or protection settings can be changed, regardless of the retention period.
secure	Protection cannot be released during the retention period. There are constraints on changing protection settings.
strict	Protection cannot be released during the retention period. Protection settings cannot be changed, either.

Retention Date

Specify the retention period of the volume. The retention period can be specified in the following formats.

Radio Button	Description
Not Specify	The retention period is set to 0, indicating the condition in which the volume retention period has already elapsed.
Specify the Retention Expiration	The retention period is set as the time from the current date to the specified date (year, month, and day). The volume is protected from the current date to the specified date.

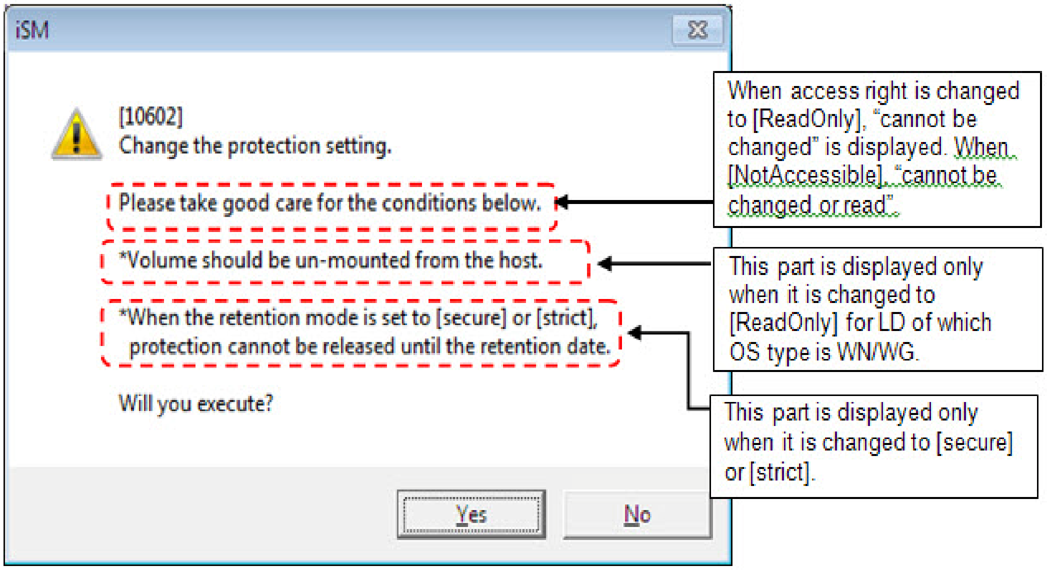
Radio Button	Description
Specify the Retention Period	Specify the number of years, months, or days for the retention period. The volume is protected for the specified duration starting at the current date.
Permanent	The retention period is permanent. The volume is permanently protected from the current date.

* When Not Specify] is selected, note that the volume immediately becomes the status in which protection can be released.

When multiple volumes are selected, for the items of which settings for individual volumes are the same, the setting values are selected.

For the items of which settings for individual volumes are not the same, nothing is selected. If it is executed while nothing is selected, the item keeps the original setting of each volume.

When the Execute] button is clicked, the following confirmation message appears.



[10602]
Change the protection setting.

Please take good care for the conditions below.

*Volume should be un-mounted from the host.

*When the retention mode is set to [secure] or [strict], protection cannot be released until the retention date.

Will you execute?

When access right is changed to [ReadOnly], "cannot be changed" is displayed. When [NotAccessible], "cannot be changed or read".

This part is displayed only when it is changed to [ReadOnly] for LD of which OS type is WN/WG.

This part is displayed only when it is changed to [secure] or [strict].

Figure 3-18: Confirmation

In this case, selecting No] stops the processing.

Execution Conditions

To perform protection change, the following conditions must be satisfied.

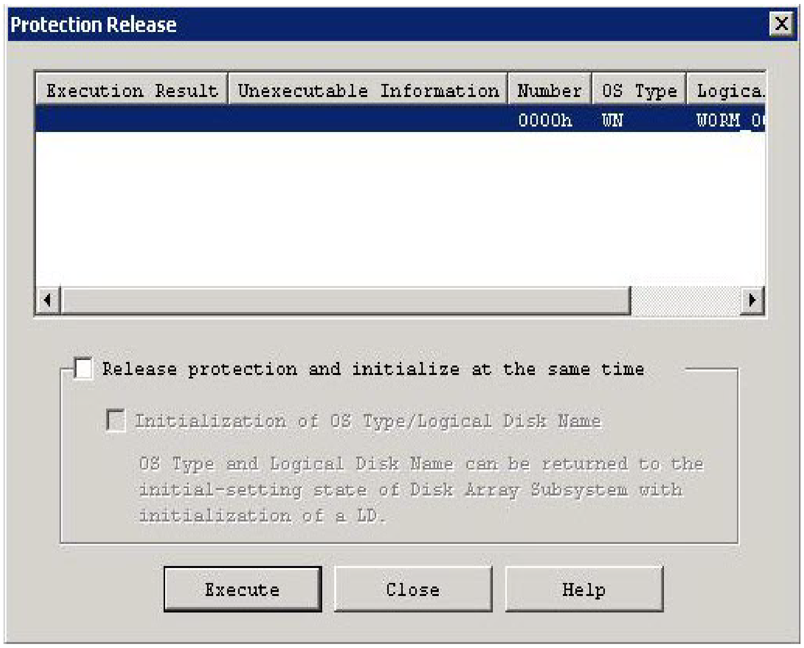
- The target volume has been protected.
- The target volume has not been registered to ATgroup.
- The retention mode of the target volume is not strict.
- When the target volume is a replication volume, the pair has been separated.
- The target volume is not in rotation stop state.
- The target volume must have been unmounted from the host.

Volume Protection Release

Protection setting of a protected volume is released. When you release protection from a protected volume, you can also reinitialize the volume to clear the stored data.

Display the information screen of the dialog for releasing a protected volume using one of the following procedures.

- Select a desired volume from the information list display area. Then, from the menu bar of the WORM management screen, select Operation] Protection Release].
- Select a desired volume from the information list display area. Then, right-click on it and select Protection Release].


Protection Release

Execution Result	Unexecutable Information	Number	OS Type	Logica
		0000h	WN	WORM_0

□ Release protection and initialize at the same time

□ Initialization of OS Type/Logical Disk Name

OS Type and Logical Disk Name can be returned to the initial-setting state of Disk Array Subsystem with initialization of a LD.

Figure 3-19: Information Screen Example of Release Dialog

Select the volume which you want to release from the list and then click the Execute] button.

You can specify two or more volumes at a time and execute the operation for all of them simultaneously.

Unexecutable volumes are shaded in gray and cannot be selected.

Selected Volume List

Information list of the volume selected in the information list display area appears.

The information of each individual item is updated only when the Execute] button is clicked.

If Unexecutable is shown in the Execution Result] field, the volume does not meet the execution conditions and therefore cannot be selected.

For the unexecutable volume, refer to Unexecutable Information] and take one of the following actions.

Unexecutable Information	Action
Error LD	Retry after checking the LD status.
Not Protected	It cannot be executed when protection has not been set.
Retention mode is secure	Protection cannot be released within the retention period because the retention mode is secure.
Retention mode is strict	Protection cannot be released within the retention period because the retention mode is strict.
The pair state of LD cannot be operated.	Retry after checking the pair status.
Monitoring stop	Retry after restarting monitoring.
The volume cannot be operated for its state.	Retry after checking the volume status.

For the volume of Cannot execute initialization, refer to Unexecutable Information] and take one of the following actions.

Unexecutable Information	Action
Formatting	Retry after formatting is completed.
Cannot execute initialization on MV/RV	Initialization cannot be executed because the volume is MV or RV.

For the volume of Cannot execute initialization of OS Type/Logical Disk Name, refer to Unexecutable Information] and take one of the following actions.

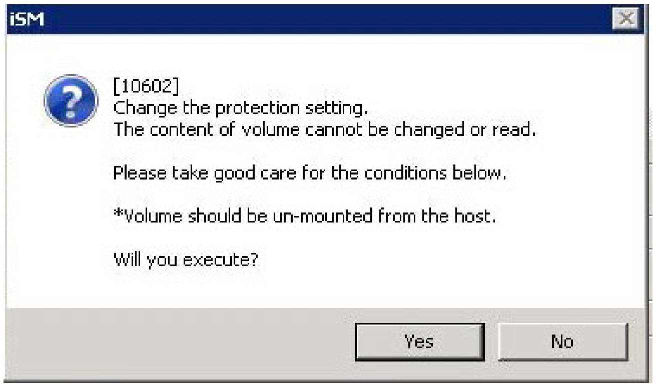
Unexecutable Information	Action
Cannot execute initialization of OS Type/Logical Disk Name on lock LD	Retry after unlocking the locked volume.

Release protection and initialize at the same time

- When the checkbox is marked, the initialization of volume contents is executed at the same time of protection release.

Initialization of OS Type/Logical Disk Name

- When the checkbox is marked, the OS Type/Logical Disk Name is returned to the initial setting of the disk array at the same time of the initialization.
- When Release protection and initialize at the same time] is not selected, clicking the Execute] button displays the following confirmation message.



iSM

[10602]
Change the protection setting.
The content of volume cannot be changed or read.

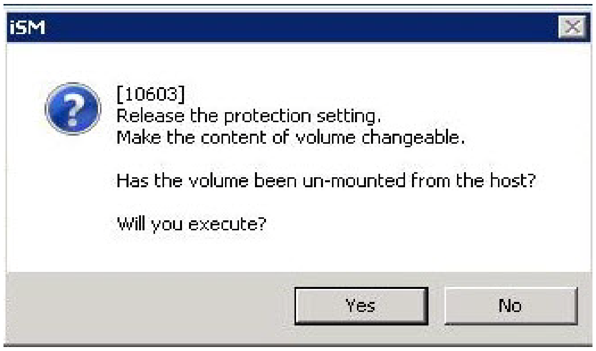
Please take good care for the conditions below.

*Volume should be un-mounted from the host.

Will you execute?

Figure 3-20: Execute Confirmation

When Release protection and initialize at the same time] is selected, clicking the Execute] button displays the following confirmation message.



iSM

[10603]
Release the protection setting.
Make the content of volume changeable.

Has the volume been un-mounted from the host?

Will you execute?

Figure 3-21: Confirmation Screen (Initialization of OS Type/Logical Disk Name])

Execution Conditions

To perform protection release, all of the following conditions must be satisfied.

- When the retention mode is normal:
- The target volume has been protected.
- When the target volume is a replication volume, the pair has been separated.
- The target volume is not in rotation stop state.
- When the retention mode is secure or strict:
- The target volume has been protected.
- The protection period has been expired.
- When the target volume is a replication volume, the pair has been separated.
- The target volume is not in rotation stop state.
- To initialize the volume contents, both of the following conditions must be satisfied.
- The target volume is not a replication volume.
- The target volume is not being formatted.
- To initialize the OS Type/Logical Disk Name, the following conditions must be satisfied.
- The target volume has not been locked.

- The target volume is not a volume bound using the quick format.

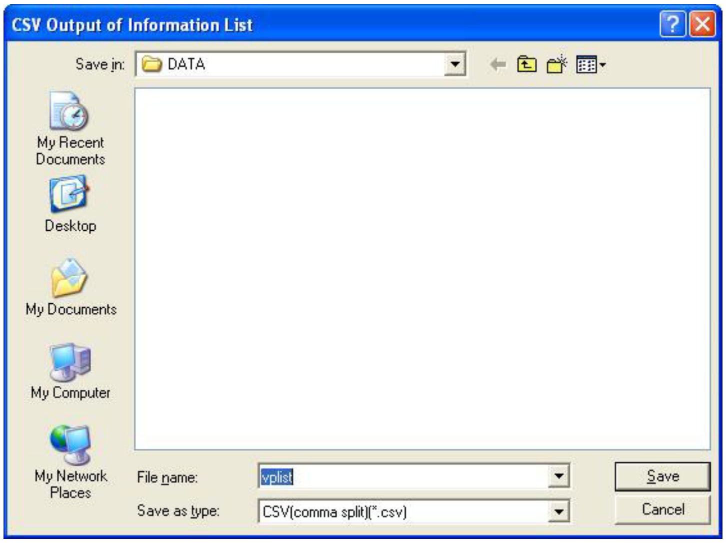
1. When initialization is executed, only the start is displayed for the initialization operation. For the progress ratio and result of initialization, check the main screen (state monitoring screen). Even when initialization of OS Type/Logical Disk Name is executed, the OS Type/Logical Disk Name in the dialog is not changed. For the result of initialization of OS Type/Logical Disk Name, check the volume list on the WORM management screen.
2. The target volume must have been unmounted from the host.

CSV Output of Information List

The information currently displayed in the information list display area is output as a CSV file and then saved.

Operating Procedure

To display the CSV Output of Information List Display screen, Select File]   CSV Output of Information List] from the menu bar of the WORM management screen.



File name: vplist

Save as type: CSV(comma split)(*.csv)

Figure 3-22: CSV Output of Information List

Specify the save destination.

Specify the file name.

The default file name is vplist.csv.

Click the Save] button to save the input information.

When the Cancel] button is clicked, the screen is returned to the WORM management screen without saving the file.

CSV File of Information List

A CSV file example to be output when CSV Output of Information List] is executed is shown below.

This file outputs information displayed on the screen by separating each piece of information by commas.

File Example

```
Disk Array

Disk Array Subsystem Name,Number of Protection LDs,Number of Expired LDs

S2500/0021,0,0

S2500/1008,6,6

Volume

Number,OS Type,Logical Disk Name,Protection Status,Protection Period Status,Begin
Date,Retention Date,Retention Mode,RPL Type,Configuration Change,LD Set Name

0200h,WN,BV1,NotAccessible,Enable,2005/10/12,2006/10/13,normal,

IV,Lock,CX:refamsun

02e1h,LX,GP_1,ReadOnly,Enable,2005/10/12,2006/12/12,secure,

IV,,LX:exp1246
```

Recording Screen Information

The information displayed on the WORM management screen is automatically recorded when closing the screen.

The recorded information is added next time the WORM management screen is activated.

Information to Be Recorded

Item width

Item position

Screen size

Screen position

Status bar view status

Update Disk Array Information

Executing the refresh function with the SnapSAN Manager server selected in the configuration display area updates the information about the disk array connected to the server. Also, the information displayed on the screen is cleared.

Executing the refresh function with a disk array selected in the configuration display area updates all the information about the selected disk array and leads to the state with the disk array selected.

In either case, if you cancel the refresh operation before it is completed, execute Refresh].

Perform one of the following procedures.

1. From the menu bar, select View]   Refresh].
2. Press the F5 key.

Notification of Expired Retention

SnapSAN Manager provides the WORM notification function. Expired retention and a retention date approached set by the WORM function can be notified.

SnapSAN Manager regularly checks the protection status of a volume and notifies of the expired retention. When the protection state of the volume becomes expired retention, SnapSAN Manager records the message to syslog and the event log and displays the message to SnapSAN Manager client's GUI.

The message telling expired retention is output at one of the following timings during a specified period. For setting the check time of the protection status, refer to the installation guide attached to SnapSAN Manager.

- When starting the SnapSAN Manager server:
- When restarting monitoring of the disk array:
- At the check time of the protection status once a day:

NOTE: The notification of expired retention is performed within the period specified in the environment definition file (default value is 1 day). For specifying the output period of the message of expired retention, refer to the installation guide attached to SnapSAN Manager.

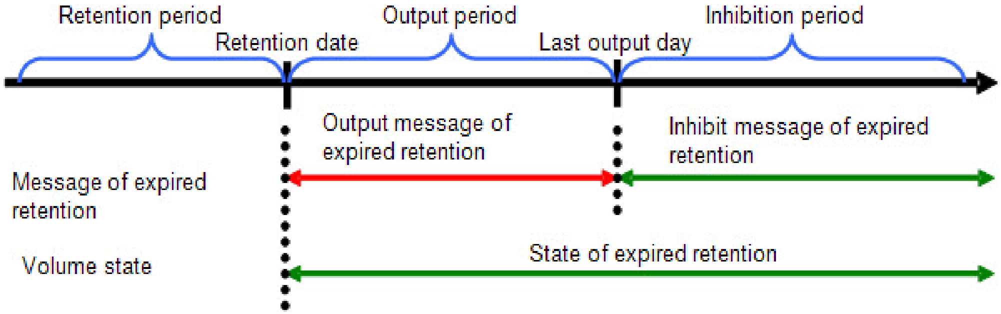

Retention period
Retention date
Output period
Last output day
Inhibition period
Output message of expired retention
Inhibit message of expired retention
Message of expired retention
Volume state
State of expired retention

Figure 3-23: Output Period of Message of Expired Retention

Example: When the retention date (the last day for protection) of a volume is December 1, 2009:

If the output period of the message of expired retention is set to two days, the output period of the message of expired retention is from December 2, 2009 to December 3, 2009. (Two days from the date on which retention expired, December 2, 2009.)

Retention Date Approached

SnapSAN Manager sends a notification of retention date approached to the administrator before the protection status of a volume becomes expired retention. On the specified day of previous notification, it records the message of retention date approached to syslog and the event log and displays the message to SnapSAN Manager client's GUI.

The message of retention date approached is output at one of the following timings on the specified day of previous notification. For setting the check time of the protection status, refer to the installation guide attached to SnapSAN Manager.

- When starting the SnapSAN Manager server:
- When restarting monitoring of the disk array:
- At the check time of protection status once a day:

Note that the notification of retention date approached is performed within the period specified in the environment definition file (default value is 0 day (that is, no previous notification)). For specifying the day of previous notification of retention date approached, refer to the installation guide attached to SnapSAN Manager.

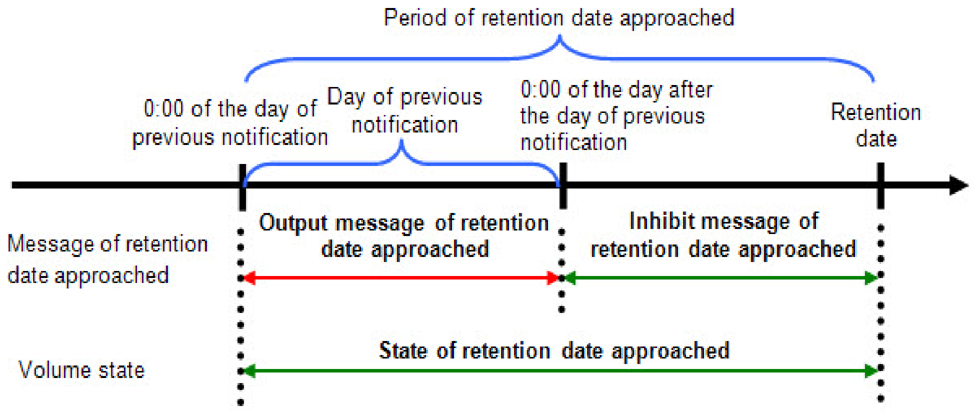

Period of retention date approached
0:00 of the day of previous notification
Day of previous notification
0:00 of the day after the day of previous notification
Retention date
Message of retention date approached
Output message of retention date approached
Inhibit message of retention date approached
Volume state
State of retention date approached

Figure 3-24: Output Period of Message of Retention Date Approached

Example: When the retention date (the last day for protection) of a volume is December 1, 2009:

If the period of retention date approached is set to two days before the retention date, the output period of the message of retention date approached is November 30, 2009. (Two days before the date on which retention expires, December 2, 2009.)

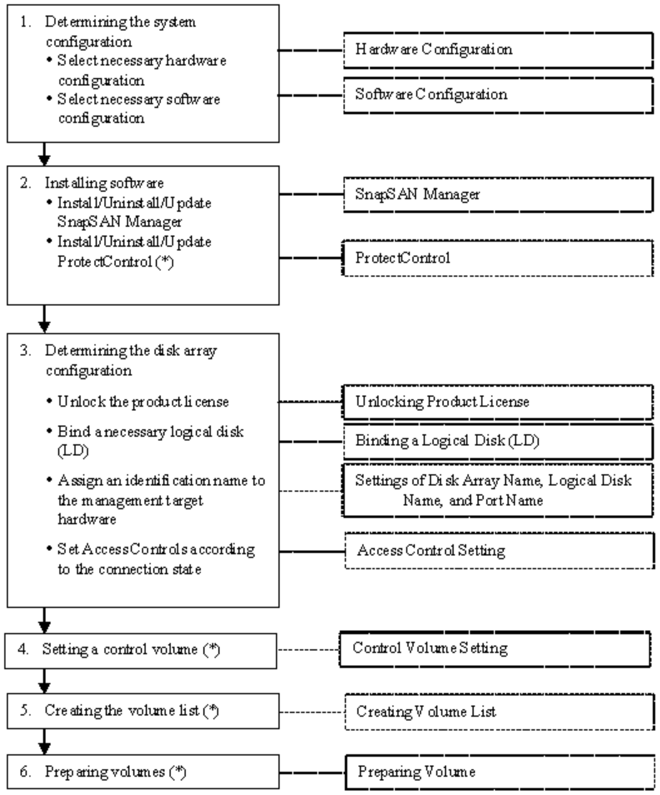
Chapter 4

Installation (Windows)

Installation Procedure

This chapter describes the system installation procedures showing an example to establish a WORM system using disk arrays in an existing operation system.

Installation works are outlined below. Works followed by (*) mark are necessary for servers where ProtectControl will be installed.


1. Determining the system configuration
• Select necessary hardware configuration
• Select necessary software configuration
Hardware Configuration
Software Configuration
2. Installing software
• Install/Uninstall/Update SnapSAN Manager
• Install/Uninstall/Update ProtectControl (*)
SnapSAN Manager
ProtectControl
3. Determining the disk array configuration
• Unlock the product license
• Bind a necessary logical disk (LD)
• Assign an identification name to the management target hardware
• Set Access Controls according to the connection state
Unlocking Product License
Binding a Logical Disk (LD)
Settings of Disk Array Name, Logical Disk Name, and Port Name
Access Control Setting
4. Setting a control volume (*)
Control Volume Setting
5. Creating the volume list (*)
Creating Volume List
6. Preparing volumes (*)
Preparing Volume

System Configuration

Hardware Configuration

Select hardware components according to the business conditions, requirements, disk capacity, and so forth.

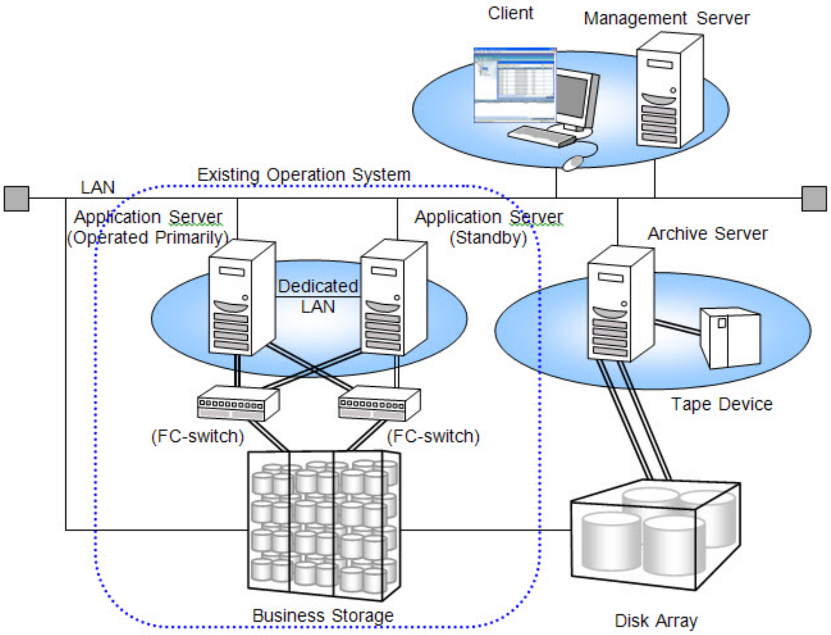


Figure 4-1: Hardware Configuration

Though a business or archive server may also be used as a management server, using a specific management server is recommended. Use of LAN connection is strongly recommended for connection with disk array.

Connect the path of individual servers, to be connected to the disk array, to the port of different directors, limiting the servers to be accessed by Access Control.

In the above configuration example, the application servers are installed in a cluster and mutually connected through the dedicated LAN.

Software Configuration

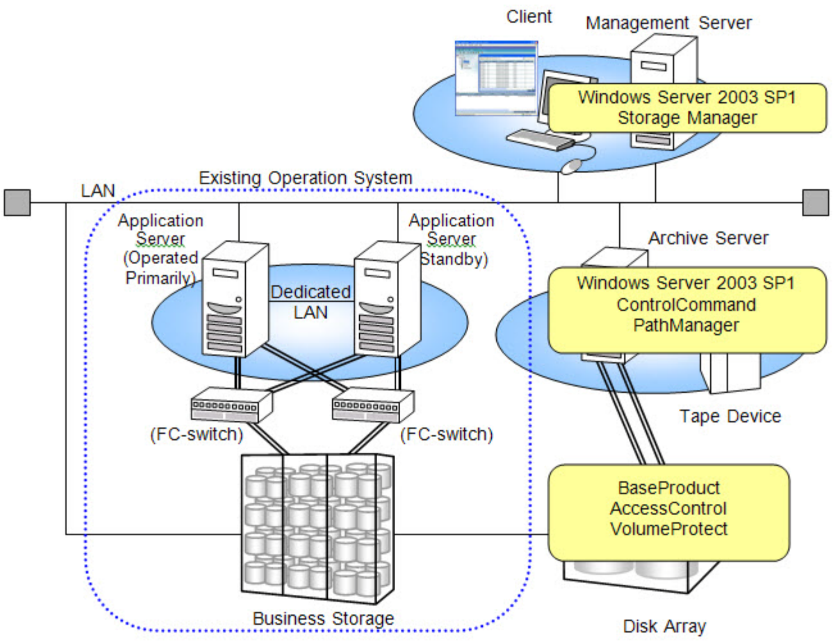


Figure 4-2: Software Configuration

Install the backup software in the archive server.

Install the management software in the management server. Install the SnapSAN Manager in the management server.

Install the ProtectControl in the archive server. ProtectControl is included in ControlCommand.

WORM and AccessControl are installed in the disk array. They become available by unlocking the license.

Windows Server 2003 SP1 or later must be installed in the archive server.

Software Installation

Storage Manager

Operating Environment

SnapSAN Manager Server

SnapSAN Manager Client (GUI)

Installation

SnapSAN Manager Server Installation

SnapSAN Manager Server Setting

Create the environment according to the installation guide attached to SnapSAN Manager.

SnapSAN Manager Client Installation

Install the SnapSAN Manager client according to the installation guide attached to SnapSAN Manager.

Uninstall

SnapSAN Manager Server Uninstallation

Uninstall the SnapSAN Manager server according to the installation guide attached to the SnapSAN Manager.

SnapSAN Manager Client

Uninstall the SnapSAN Manager client according to the installation guide attached to the SnapSAN Manager.

Update

SnapSAN Manager Server Update

To update the SnapSAN Manager software, uninstall the existing software, and then install the new software.

ProtectControl

Operating Environment

Operating system and linkage software

Required Disk Free Space

Required memory

Installation

Install ProtectControl that is included in ControlCommand.

Setting Operating Environment

When you use ProtectControl, you can use the option setting file (iSMrpl.ini) to set various operations at command execution.

Uninstallat

Uninstall ProtectControl.

Update

To update the ProtectControl software, uninstall the existing software, and then install the new software.

Disk Array Configuration

For the disk array to be connected, determine the configuration for using the WORM function.

Unlocking Product License

To use the VolumeProtect, you must unlock the product license set in the disk array. To unlock the license, you must purchase the corresponding products equal to or greater than the total capacity of the data disk.

At execution, ProtectControl checks the license status of the products and check whether they are available.

If the total capacity of the data disk exceeds the product's specified capacity because physical disks are added to the disk array system, it is necessary to unlock the product licenses equal to or greater than lack of licenses.

Binding a Logical Disk (LD)

Bind volumes for use with the WORM function.

For the data that must conform to the regulations and the like that require data storage in non-falsifiable format, you should consider the frequency of occurrence of the data, the size of the data, the specified retention period, and the maximum LUN that can be recognized by the OS. Then, determine the capacity and number of volumes for use with the WORM function, and bind logical disks in disk arrays.

Settings of Disk Array Name, Logical Disk Name, and Port Name

You can assign identification names to hardware components managed by the SnapSAN Manager. Identification names can be given to the following items:

- Disk array subsystem name
- Logical disk name (plus OS type)
- Port name

It is better to set a disk array subsystem name, port name, and logical disk name according to the operating conditions and server connection conditions.

When you use the WORM function, you do not need to note disk array names and port names. For the OS type of a logical disk, you need to note the following.

- A logical disk name must be set so as to identify data to be stored.
- The OS type of a logical disk must be appropriate for the supporting platform.

These settings are performed from an SnapSAN Manager client.This is an example of setting a disk array name for saving the e-mail log data for a long period.

Disk Array Subsystem: S1800AT

Disk Array Subsystem Name: Mail_Log_Archive

This is a setting example conforming to the connection configuration of servers.

Director Number	Port Number	Port Name	Connected Server
00h	00h	ARCHIVE_PRIMARY	Archive server
01h	00h	ARCHIVE_SECONDARY	

Setting Logical Disk Names and OS Types

LD No.	OS Type	Logical Disk Name	Remarks
0050h	WN	MAIL_LOG_2005_01	Volume for e-mail log of January 2005
0051h		MAIL_LOG_2005_02	Volume for e-mail log of February 2005
0052h		MAIL_LOG_2005_03	Volume for e-mail log of March 2005
0053h		MAIL_LOG_2005_04	Volume for e-mail log of April 2005
0054h		MAIL_LOG_2005_05	Volume for e-mail log of May 2005
0055h		MAIL_LOG_2005_06	Volume for e-mail log of June 2005
0056h		MAIL_LOG_2005_07	Volume for e-mail log of July 2005
0057h		MAIL_LOG_2005_08	Volume for e-mail log of August 2005
0058h		MAIL_LOG_2005_09	Volume for e-mail log of September 2005
0059h		MAIL_LOG_2005_10	Volume for e-mail log of October 2005
005ah		MAIL_LOG_2005_11	Volume for e-mail log of November 2005
005bh		MAIL_LOG_2005_12	Volume for e-mail log of December 2005
0060h		ARCHIVE_CV	Control volume

Set the OS type to WN, the default value for the Windows operating systems.

This example shows logical disk names when archiving the e-mail log once a month.

Access Control is necessary for a system in which WORM function is installed.

Before performing the following operations, enable Access Control setting. In addition, Access Control setting needs to be performed for volumes that have already been used for other operations.

Access Control Setting

To prevent a wrong update to a volume or a wrong modification of the disk configuration, usually you need to set the system with WORM function so that volumes to be used by WORM function cannot be referenced by a server other than an archive server.

Therefore, to use WORM function, you need to limit logical disks that can be accessed from a server by using Access Control.

To use WORM function, also take note the following points and set Access Control.

Setting Access Control

Assign volumes to be used by WORM function to an archive server.

Before introducing servers, you must determine the server connection modes and design Access Control settings. Access Control can be set for individual ports or WWNs. Setting for Access Controls requires purchasing the AccessControl.

Control Volume Setting

A control volume is used when a server issues control I/O to the relevant disk array. Select one of logical disks connected to an archive server as the volume for issuing I/O to that disk array and register the volume in the volume list.

The purpose (attribute) of logical disks built as control volumes can be identified with the following SnapSAN S3000/S5000.

When the logical disk information is displayed by the SnapSAN Manager client (and so on) for disk arrays on which the purpose (attribute) of a control volume can be identified, the identification information indicating the control volume as a logical disk purpose (attribute) is displayed.

The control volume setting procedure differs depending on the disk array functions as shown below.

Disk Arrays identifying the Control Volume Attribute

First build the control volume using the SnapSAN Manager server's configuration function; once the control volume is recognized by the server, create the volume list.

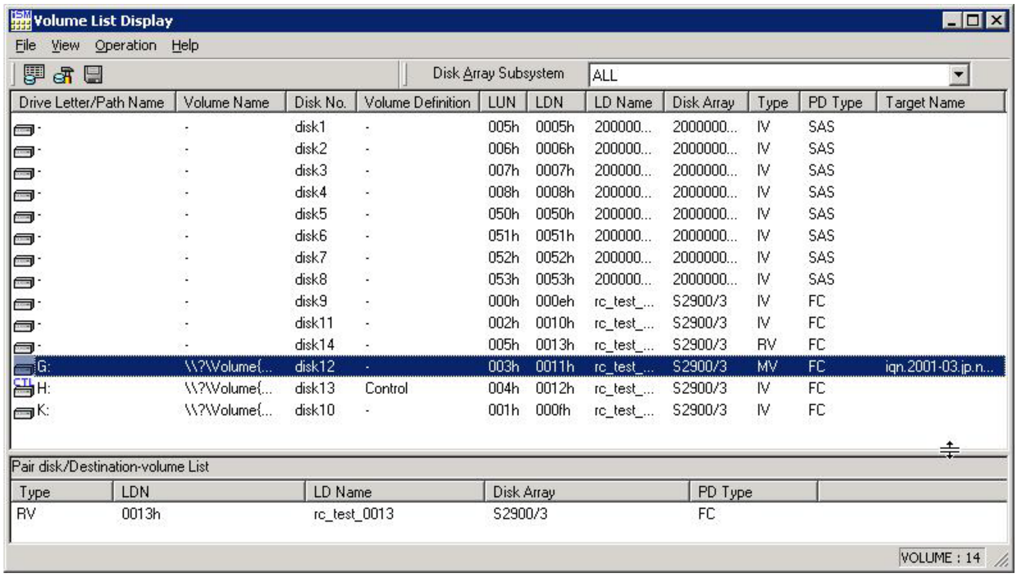
There is no need to register the control volume on the definition screen of the volume list display function. When the volume list is created or updated, the disk array identifies the control volume attribute from the logical disks connected to the server and registers it on the volume list.

Other Disk Arrays

It is necessary to register the control volume on the definition screen of the volume list display function.

Starting Volume List Display Function

To start the Volume List Display function, select [Start] of Windows [All Programs] [ControlCommand] [Storage Manager Agent Utility] [Volume List Display].



Drive Letter/Path Name	Volume Name	Disk No.	Volume Definition	LUN	LDN	LD Name	Disk Array	Type	PD Type	Target Name
-	-	disk1	-	005h	0005h	200000...	2000000...	IV	SAS	
-	-	disk2	-	006h	0006h	200000...	2000000...	IV	SAS	
-	-	disk3	-	007h	0007h	200000...	2000000...	IV	SAS	
-	-	disk4	-	008h	0008h	200000...	2000000...	IV	SAS	
-	-	disk5	-	050h	0050h	200000...	2000000...	IV	SAS	
-	-	disk6	-	051h	0051h	200000...	2000000...	IV	SAS	
-	-	disk7	-	052h	0052h	200000...	2000000...	IV	SAS	
-	-	disk8	-	053h	0053h	200000...	2000000...	IV	SAS	
-	-	disk9	-	000h	000eh	rc_test_...	S2900/3	IV	FC	
-	-	disk11	-	002h	0010h	rc_test_...	S2900/3	IV	FC	
-	-	disk14	-	005h	0013h	rc_test_...	S2900/3	RV	FC	
G:	\\?\Volume{...	disk12	-	003h	0011h	rc_test_...	S2900/3	MV	FC	iqn.2001-03.jp.n...
H:	\\?\Volume{...	disk13	Control	004h	0012h	rc_test_...	S2900/3	IV	FC	
K:	\\?\Volume{...	disk10	-	001h	000fh	rc_test_...	S2900/3	IV	FC	

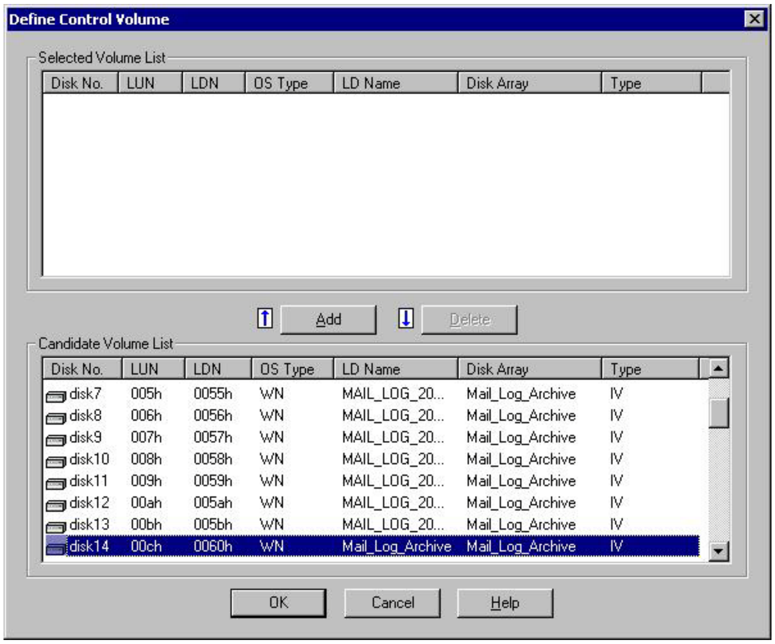
Pair disk/Destination-volume List

Type	LDN	LD Name	Disk Array	PD Type
RV	0013h	rc_test_0013	S2900/3	FC

VOLUME : 14

Figure 4-3: Volume List

Then, select [Define Control Volume] in [Operation] in the Volume List Display screen to open the Define Control Volume screen



Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk7	005h	0055h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk8	006h	0056h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk9	007h	0057h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk10	008h	0058h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk11	009h	0059h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk12	00ah	005ah	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk13	00bh	005bh	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk14	00ch	0060h	WN	Mail_Log_Archive	Mail_Log_Archive	IV

Figure 4-4: Define Control Volume

Selected Volume List

Lists already registered control volumes.

Candidate Volume List

Lists candidate logical disks that can be registered as a control volume. Type of listed logical disks is IV or MV.

In disk arrays with which the control volume attribute can be identified, the logical disk that is built as a control volume is not displayed on the control volume definition screen; it cannot be added, changed, or deleted.

Registering Control Volume

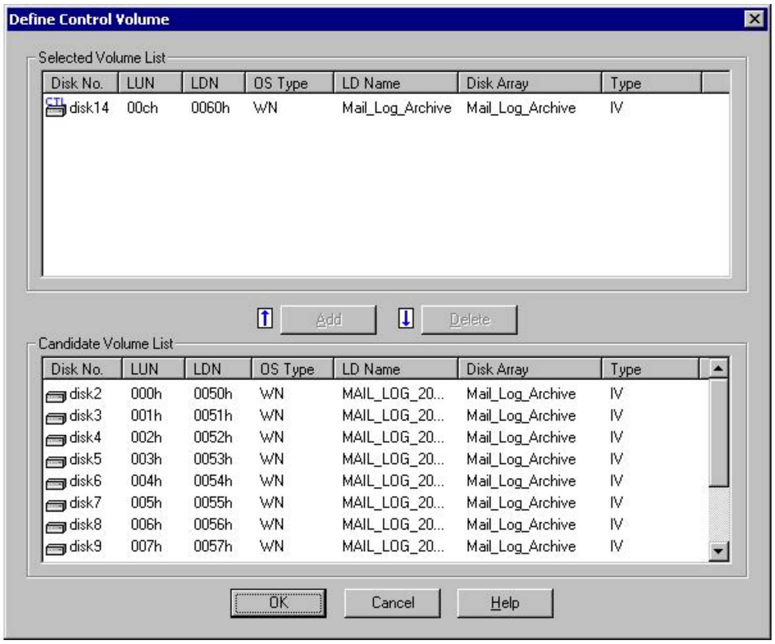
A control volume is used when a server issues control I/O to the relevant disk array. You can select one logical disk for each disk array as a control volume. Prepare a volume with which the server can properly issue I/O to the disk array.

Select a normal volume that is not used for data replication, snapshot, and WORM functions for a control volume. Prepare a control volume as a dedicated volume and do not assign business data.

Select a logical disk you want to use as a control volume from Candidate Volume List.

Click the [Add] button.

The selected logical disk is added to Selected Volume List.



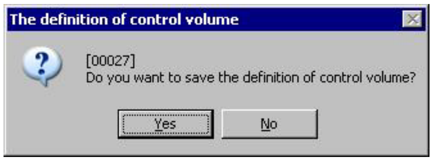
Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
CTL disk14	00ch	0060h	WN	Mail_Log_Archive	Mail_Log_Archive	IV

Disk No.	LUN	LDN	OS Type	LD Name	Disk Array	Type
disk2	000h	0050h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk3	001h	0051h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk4	002h	0052h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk5	003h	0053h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk6	004h	0054h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk7	005h	0055h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk8	006h	0056h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV
disk9	007h	0057h	WN	MAIL_LOG_20...	Mail_Log_Archive	IV

Figure 4-5: Define Control Volume

Saving Registered Data

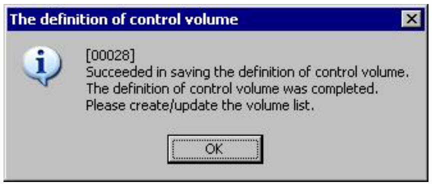
Click the [OK] button on the Define Control Volume screen. A confirmation message appears asking if you want to save definition information



[00027]
Do you want to save the definition of control volume?

Figure 4-6: Save Definition

Clicking the [Yes] button for the message saves definition information and displays a termination message. Clicking the [No] button displays the Define Control Volume screen again.

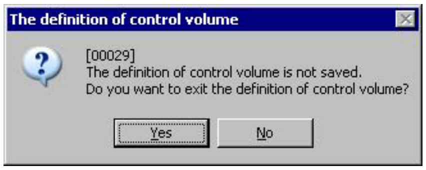


[00028]
Succeeded in saving the definition of control volume.
The definition of control volume was completed.
Please create/update the volume list.

Figure 4-7: Confirm Termination

Clicking the [OK] button closes the Define Control Volume screen and displays the Volume List Display screen again.

Clicking the [Cancel] button in the Define Control Volume screen displays a confirmation message asking if you want to cancel the definition.



The definition of control volume

[00029]
The definition of control volume is not saved.
Do you want to exit the definition of control volume?

Figure 4-8: Cancel Confirmation

Clicking the [Yes] button for the message cancels saving of the definition information. The Define Control Volume screen is closed and the Volume List Display screen appears again.

Clicking the [No] button displays the Define Control Volume screen again.

Reflecting Data to Volume List

Select [Create/Update Volume List] from [File] in the Volume List Display screen to create or update the volume list, reflect the saved registration data of the control volume to the volume list, and register it.

When the volume list file has been created or updated, the Volume List Display screen is automatically refreshed. Confirm that Control is set for Volume Definition for the logical disk selected as a control volume.

Creating Volume List

Creation of a volume list is required before using ProtectControl command. To create a volume list, execute the iSMvollist command with the -cr option specified or execute the [Create/Update Volume List] operation in the Volume List Display screen (screen operation). The user must belong to the Administrators group to create a volume list.

The following command line shows an example to create a volume list with the iSMvollist command.

```
iSMvollist -cr
```

Upon successful creation of volume list, the following message appears:

iSM11701: Volume list is created successfully.

If creation of a volume list fails, execution of ProtectControl command is disabled. Troubleshoot in accordance with an error message or with operation error tracing, create a volume list again.

Create a volume list in the following states.

- The path between the disk array and the server is normally connected.
- The logical disk in the disk array is recognized as a server (OS) disk device.
- The volume (partitions) in the disk is recognized by the server (OS).

Execute the following operation before creating a volume list if you use a control volume in the disk array with which the control volume attribute cannot be identified.

Register the logical disk to be used as a control volume in advance by executing the [Define Control Volume] operation in the Volume List Display screen.

To successfully register volume information in the volume list, create a volume list in the following states.

- Pairs are separated when the RV in the data replication function is connected to the server.
- The link-volume (LV) and snapshot-volume (SV) are linked when the LV in the snapshot function is connected to the server. The base-volume (BV) and LV are also not linked when the BV is connected to the server.
- Protected data is readable when the logical disk for which the WORM function is applied is connected to the server.
- The volume is in the In use state and accessible when the logical disk for which the power saving function is applied is connected to the server.
- All the volumes are mounted and every mount point to be used (drive letter or NTFS folder name) is set.
- The link path between disk arrays is normal when the Replication and Mirroring is configured for the disk array.

After successfully creating a volume list, display the information registered in the volume list to check that the items to be used such as logical disks, partitions (mount point volume names), and mount points (drive letters or NTFS folder names) are all registered.

Once the volume list is successfully created, that information is maintained for operation. It is not necessary to update the volume list during operation. However, if the disk array, server (OS) volume, or other configuration is changed, it is required to recreate the volume list to reflect the new information. Note that an error or inconsistency may occur at execution of ProtectControl command unless the volume list is updated.

Preparing Volume

When using a volume for the first time for WORM operation, execute the steps given below for the target volume. The following is an example of the procedure for creating partitions and a file system on a volume to be used by WORM function.

Suppressing automatic volume mounting (archive server)

Suppress automatic volume mounting.

Enter MOUNTVOL /N on command prompt.

```
MOUNTVOL /N
```

Creating partitions (archive server)

Using [Disk Management] (Windows), create partitions on a volume to be used by WORM function.

In a recommended partition configuration, one logical disk contains one partition.

Creating file system (archive server)

Create a file system on a disk where a partition has been created and assign an NTFS folder to the file system. An NTFS folder name must be set so as to identify data to be stored.

Creating volume list (archive server)

Since a partition has been created on the volume and a new NTFS folder has been assigned, recreate a volume list using the iSMvollist command.

Enter the following command to create a volume list.

```
iSMvollist -cr
```

Upon successful creation of volume list, the following message appears:

```
iSMvollist: Info:   iSM11701: Volume list is created successfully.
```

Output the volume list data into the vollist_data.txt.

```
iSMvollist -a > vollist_data.txt
```

*To use a control volume, before creating a volume list, select and register the control volume using the Define Control Volume function from the Volume List Display screen.

Researching mount point volume name (archive server)

A mount point volume name used for operation must be researched.

Enter MOUNTVOL /L on command prompt.

```
MOUNTVOL /L
```

Then, the list of volumes available on system is displayed as follows:

```
\\?\Volume{e2464851-8089-11d2-8803-806d6172696f}\
   F:\MAIL_LOG\2005_01
\\?\Volume{e2464852-8089-11d2-8803-806d6172696f}\
   F:\MAIL_LOG\2005_02
\\?\Volume{e2464850-8089-11d2-8803-806d6172696f}\
   F:\MAIL_LOG\2005_03
```

A mount point volume name is required for WORM operation. Take a memo of the mount point volume names, which are displayed in the mount point volume name list, to use in the operation.

Now, the volume is ready.

Chapter 5

Maintenance (Windows)

Operations

This chapter describes an example of operation using the WORM function, the operation procedure for WORM function, and the trouble-shooting for faults that may occur during operations.

Operation Design

To use the WORM function to enable operation that supports long-term storage of business data in non-falsifiable format, you must consider the following items:

Capacity and Number of Volumes

For the data that must conform to the regulations and the like that require data storage in non-falsifiable format, you should consider the frequency of occurrence of the data, the size of the data, the specified retention period, and the maximum LUN that can be recognized by the OS. Then, determine the capacity and number of volumes for use with the WORM function.

Whether to Allow Data Reference

Determine the protection state you should specify when you set volume protection, depending on whether to allow stored data to be referenced from an archive server.

WORM Period

Determine the retention period you should specify when you set volume protection, based on the regulations and the like that require data storage in non-falsifiable format.

Archive Operation

This section describes an archive operation by using the WORM function.

Although the text describes the commands in input order, it is recommended to automate the command execution by job scheduling software on the system built actually.

Protect business data that needs long-term storage and save the data in non-falsifiable format (data protection). When necessary, reference the protected data in long-term storage (protected data reference) or change volume protection settings (protection settings change).

After the elapse of the period specified by any of the regulations and the like that require data storage in non-falsifiable format, you should delete the protected data (protected data deletion).

Data Protection

Select an empty volume in the archive storage as an archive volume. Transfer to the archive server business data that needs long-term storage in non-falsifiable format, and store the data in the archive volume. Accumulate business data until no more space is available on the archive volume, and then unmount the volume. Use the volume protection setting command to disable write operations on the volume. For the purposes of guarding the archive volume against physical faults and storing the data permanently, you should use backup software to save the volume data to tape after setting volume protection.

For the specific operations, refer to Operation flow (data protection) and Operation procedure (data protection).

Protected Data Reference

To reference the data stored in the protected volume, mount the volume and access the protected data you want to reference.

For the specific operations, refer to Operation flow (protected data reference) and Operation procedure (protected data reference).

Protection Settings Change

After the data stored in the protected volume is saved to tape, you should use the volume protection setting change command when you want to perform operations for changing the protection settings for the volume, such as changing the protection state and extending the WORM period.

For the specific operations, refer to Operation flow (protection settings change) and Operation procedure (protection settings change).

Protected Data Deletion

After the elapse of the retention period set for the volume, use the volume protection release command to release protection from the volume, thereby enabling the volume to be reused.

For the specific operations, refer to Operation flow (protected data deletion) and Operation procedure (protected data deletion).

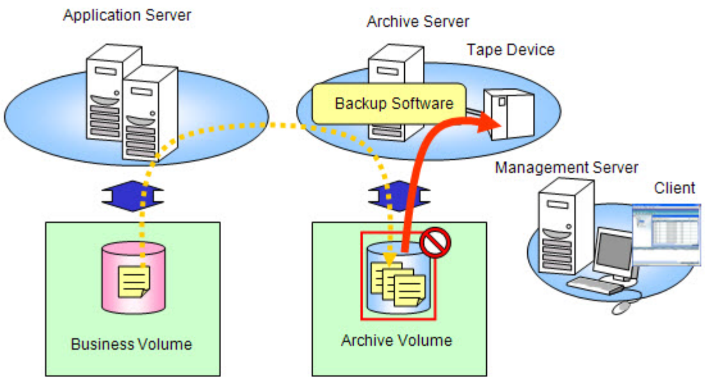


Figure 5-1: Archive Operation

Prerequisites

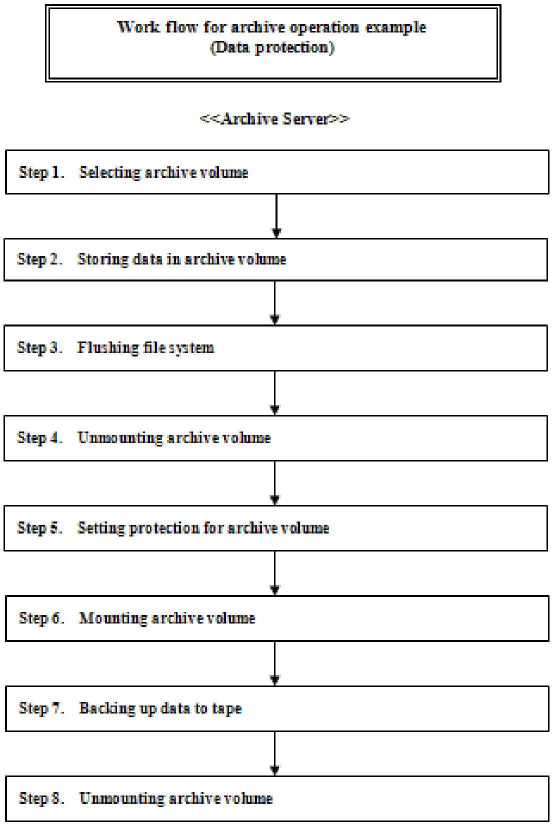
The archive server OS should be Windows Server 2003 SP1 or later, which allows creation of partitions and file systems on archive volumes.

It is assumed that partitions and a file system have been created and an NTFS folder has been allocated for the archive volume. The logical disk name and assigned NTFS folder name for the archive volume are assumed to be as follows:

Archive volumeLogical disk name (MAIL_LOG_2005_01)

NTFS folder name (F:\MAIL_LOG\2005_01)

Operation flow (data protection)


Work flow for archive operation example
(Data protection)
<<Archive Server>>
Step 1. Selecting archive volume
Step 2. Storing data in archive volume
Step 3. Flushing file system
Step 4. Unmounting archive volume
Step 5. Setting protection for archive volume
Step 6. Mounting archive volume
Step 7. Backing up data to tape
Step 8. Unmounting archive volume

Operation Procedure (Data Protection)

Select an empty volume in the archive storage as an archive volume.

Storing data in archive volume (archive server)

Use a function such as ftp to transfer to the archive server business data that needs long-term storage in non-falsifiable format. Then, store data until no more space is available on the selected archive volume.

Flushing file system (archive server)

Exit or abort an application accessing the archive volume.

Flush the file system on the archive volume, and write to a disk the data in the file system buffer that has not been written.

```
iSMrc_flush -mdir F:\MAIL_LOG\2005_01
```

Unmount the Archive Volume in Preparation for Protection

When the archive volume is unmounted, the drive letter or NTFS folder name set for the volume is automatically deleted.

```
iSMrc_umount -mdir F:\MAIL_LOG\2005_01 -offline
```

Setting Protection for Archive Volume (Archive Server)

Set protection for the archive volume.

In this example, which involves tape backup in a later step, the protection state is set to ReadOnly, the retention date to March 31, 2015, and the retention mode to secure.

```
iSMpc_protect -vol MAIL_LOG_2005_01 -volflg ld -set ro -expire 20150331
-mode secure
```

Mounting Archive Volume (Archive Server)

Mount the archive volume in preparation for tape backup.

When the drive letter or NTFS folder name is also included in the mount command, the drive letter or NTFS folder is automatically reset after the archive volume is mounted.

```
iSMrc_mount -mvol \\?\Volume{37d84cca-2507-11d5-a0f7-00004c714491}\ -
mdir F:\MAIL_LOG\2005_01
```

Backing Up Data to Tape (Archive Server)

Use backup software to back up the archive volume data to a medium such as tape.

The contents of the backed-up data and the protection settings (protection state, retention date, and retention mode) should be recorded on a label or the like to allow you to check them.

Unmount Archive Volume (Archive Server)

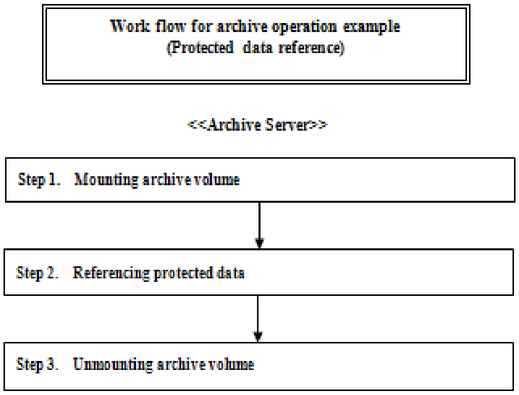
Unmount the archive volume after tape backup.

When the archive volume is unmounted, the drive letter or NTFS folder name set for the volume is automatically deleted.

```
iSMrc_umount -mdir F:\MAIL_LOG\2005_01 -offline
```

Before you perform an operation for setting volume protection, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection setting command, the volume is unmounted within the command.

Operation Flow (Protected Data Reference)


Work flow for archive operation example
(Protected data reference)
<<Archive Server>>
Step 1. Mounting archive volume
Step 2. Referencing protected data
Step 3. Unmounting archive volume

Operation Procedure (Protected Data Reference)

Mounting Archive Volume (Archive Server)

Mount the archive volume to reference its data file.

When the drive letter or NTFS folder name is also included in the mount command, the drive letter or NTFS folder is automatically reset after the archive volume is mounted.

```
iSMrc_mount -mvol \\?\Volume{37d84cca-2507-11d5-a0f7-00004c714491}\ -
mdir F:\MAIL_LOG\2005_01
```

Referencing Protected Data (Archive Server)

Reference a data file in the archive volume.

You cannot perform a write operation on data files because the archive volume is protected by the WORM function.

Unmount archive volume (archive server)

Unmount the archive volume after referencing its data file.

When the archive volume is unmounted, the drive letter or NTFS folder name set for the volume is automatically deleted.

```
iSMrc_umount -mdir F:\MAIL_LOG\2005_01 -offline
```

Operation Flow (Protection Settings Change)

Changing protection settings for archive volume (archive server)

Change the protection settings for the archive volume.

In this example, the protection state of the archive volume is changed to NotAccessible, the retention date to March 31, 2025, and the retention mode to strict.

```
iSMpc_protect -vol MAIL_LOG_2005_01 -volflg ld -set na -expire 20250331
-mode strict
```

Before you perform an operation for changing volume protection settings, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection change command, the volume is unmounted within the command.

Operation Flow (Protected Data Deletion)

Releasing protection from archive volume (archive server)

Release protection from the archive volume.

In this example, data is cleared upon release of protection from the archive volume.

```
iSMpc_release -vol MAIL_LOG_2005_01 -volflg ld -reinit
```

Before you perform an operation for releasing volume protection, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection release command, the volume is unmounted within the command.

Example of Restoring Archive Volume Data

This section describes procedures of restoring archive volume data.

If a physical fault occurs, preventing you from accessing an archive volume protected by the WORM function or data files in that volume, you can restore the archive volume from a backup in a medium such as tape.

Assuming that a physical fault has occurred on a data file in the protected archive volume, this section describes the procedure for restoring the volume from a backup medium. It is also assumed that the backup of the archive volume to be restored has been made in the backup medium.

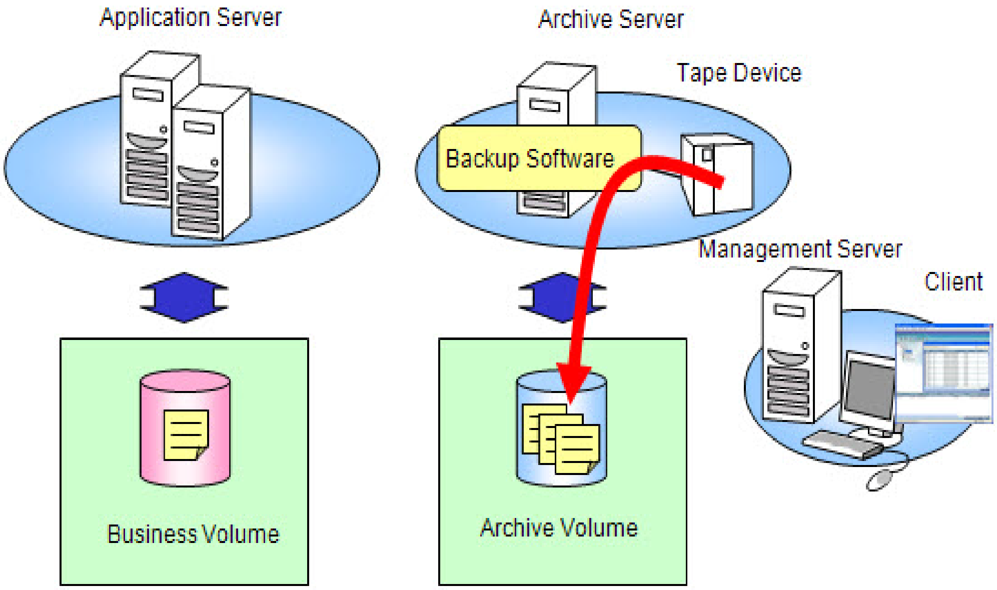


Figure 5-2: Physical Fault

Prerequisites

The archive server OS should be Windows Server 2003 SP1 or later, which allows creation of partitions and file systems on archive volumes. It is assumed that before occurrence of a physical fault, partitions and a file system have been created and an NTFS folder has been assigned for the archive volume. The logical disk name and assigned NTFS folder name for the archive volume are assumed to be as follows:

- Archive volumeLogical disk name (MAIL_LOG_2005_01)
- NTFS folder name (F:\MAIL_LOG\2005_01)

Operation Flow (Data Recovery)

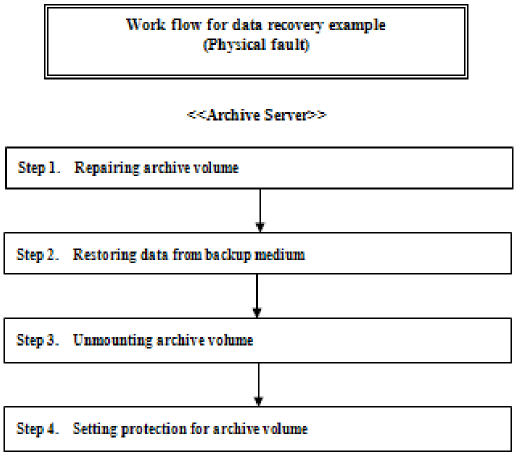

Work flow for data recovery example
(Physical fault)
<<Archive Server>>
Step 1. Repairing archive volume
Step 2. Restoring data from backup medium
Step 3. Unmounting archive volume
Step 4. Setting protection for archive volume

Figure 5-3: Physical Fault - Data Recovery

Operation Procedure (Data Recovery)

Repairing Archive Volume (Archive Server)

You may bind a new logical volume when, for example, a hardware fault has occurred and you repair the archive volume by rebuilding it. In such a case, use [Disk Management] (Windows) to create a disk signature.

Then set partitions, perform formatting to create a file system, and reset the drive letter or NTFS folder. For the partitions, file system, and drive letter or NTFS folder, make the same settings as you did before occurrence of the fault.

You must also re-create and update a volume list.

```
iSMvollist -cr
```

Restoring Data From Backup Medium (Archive Server)

Use backup software to restore the data saved in the backup medium to the archive volume.

Unmounting Archive Volume (Archive Server)

Unmount the archive volume in preparation for protection.

When the archive volume is unmounted, the drive letter or NTFS folder name set for the volume is automatically deleted.

```
iSMrc_umount -mdir F:\MAIL_LOG\2005_01 -offline
```

Setting Protection For Archive Volume (Archive Server)

Set protection for the archive volume.

Check the protection settings (protection state, retention date, and retention mode) recorded when you created the backup, and make the same settings as you did before occurrence of the fault. In this example, the protection state is set to ReadOnly, the retention date to March 31, 2015, and the retention mode to secure.

```
iSMpc_protect -vol MAIL_LOG_2005_01 -volflg ld -set ro -expire 20150331
-mode  secure
```

Concurrent Operation with Replication Function

This section describes an example of operation by concurrently using the WORM function and data replication function. Although the text describes the commands in input order, it is recommended to automate the command execution by job scheduling software on the system built actually.

Data Backup and Protection

Back up the data to be stored for a long term by the data replication function and then protect the replication volume for a specified time period by the WORM operations (data backup and protection). When necessary, reference the protected data in long-term storage (protected data reference). When data in a master volume is corrupted by physical failure or mis-operation, the master volume is restored from the backed-up replication volume (data recovery of master volume). After the elapse of the period specified at data protection, protected data is deleted (protected data deletion).

Select a target replication volume to be used from a replication volume group that has been bound and pair it with a master volume. Back up data in the master volume into the replication volume by using the data replication function. After backup, protect the backed-up replication volume entirely by executing protection operation of the WORM function. Unpair the protected replication volume from the master volume and store it for a long period.

For the specific operations, refer to Operation flow (data backup and protection) and Operation procedure (data backup and protection).

Protected Data Reference

To reference the data stored in the protected volume, mount the volume and access the protected data you want to reference.

Data Recovery of Master Volume

When data in a master volume is corrupted by physical failure or mis-operation, the master volume is restored from the backed-up replication volume.

Protected Data Deletion

After the elapse of the retention period set for the volume, use the volume protection release command to release protection from the volume, thereby enabling the volume to be reused.

It is assumed that the environment of the protection operation concurrently using the data replication function.

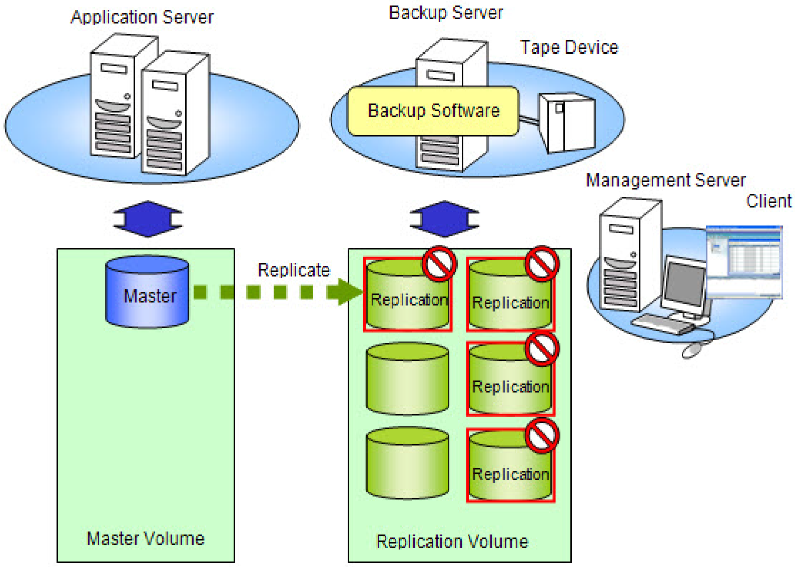


Figure 5-4: Data Replication and Retention

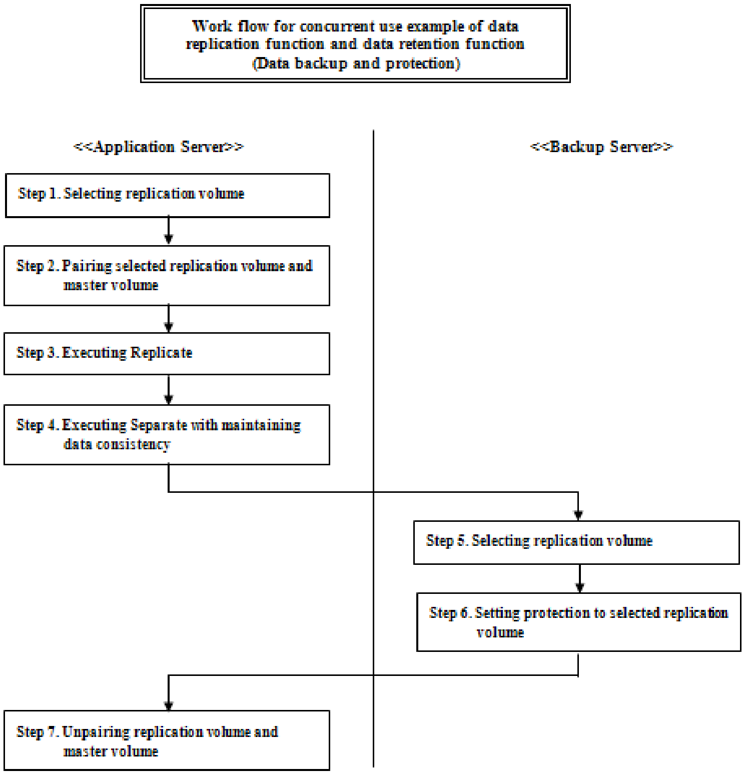
Prerequisites

The backup server OS should be Windows Server 2003 SP1 or later. Refer also to an explanation of Windows system.

It is necessary to create a replication volume, in advance, of the same capacity and OS Type as a master volume. It is assumed that a replication volume is an empty volume and has not been mounted to the backup server. The logical disk names of a master volume and replication volume, which are used in the following description, are assumed to be a follows:

- Master volumeLogical disk name (DB_MASTER)
- Replication volume to be usedLogical disk name (DB_BK_2006_06)

Operation Flow (Data Backup and Protection)


Work flow for concurrent use example of data replication function and data retention function (Data backup and protection)
<<Application Server>>
<<Backup Server>>
Step 1. Selecting replication volume
Step 2. Pairing selected replication volume and master volume
Step 3. Executing Replicate
Step 4. Executing Separate with maintaining data consistency
Step 5. Selecting replication volume
Step 6. Setting protection to selected replication volume
Step 7. Unpairing replication volume and master volume

Operation Procedure (Data Backup And Protection)

Selecting replication volume (application server)

Select a replication volume to be used from replication volumes that have been created.

Pairing selected replication volume and master volume (application server)

Set a pair of a selected replication volume and a master volume.

```
iSMrc_pair -pair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Executing Replicate (application server)

Execute Replicate and copy data from a master volume to a replication volume to synchronize the data.

```
iSMrc_replicate -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld -
wait
```

Executing Separate with maintaining data consistency (application server)

After maintaining data consistency of a master volume, execute Separate and establish the data of a replication volume.

Selecting replication volume (backup server)

Select a replication volume for which backup is established.

Setting Protection To Selected Replication Volume (Backup Server)

Execute the volume protection operation for a replication volume.

In this example, the protection state, retention period, and retention mode are set to ReadOnly, one year, and secure, respectively, to reference the data in the subsequent step.

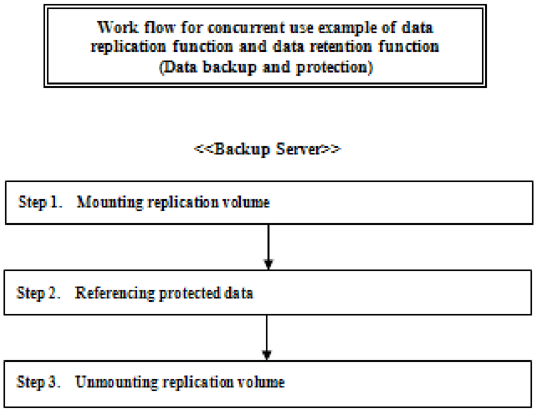
```
iSMpc_protect -vol DB_BK_2006_06 -volflg ld -set ro -expire +1y -mode
secure
```

Unpair Replication Volume And Master Volume (Application Server)

Unpair a replication volume and a master volume.

```
iSMrc_pair -unpair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Operation Flow (Data Backup and Protection)


Work flow for concurrent use example of data replication function and data retention function (Data backup and protection)
<<Backup Server>>
Step 1. Mounting replication volume
Step 2. Referencing protected data
Step 3. Unmounting replication volume

Operation Procedure (Protected Data Reference)

Mounting Replication Volume (Backup Server)

Mount a replication volume to reference its file.

When the drive letter or NTFS folder name is also included in the mount command, the drive letter or NTFS folder is automatically reset after the replication volume is mounted.

```
iSMrc_mount -mvol \\?\Volume{37d84cca-2507-11d5-a0f7-00004c714491}\ -
drv F:
```

Referencing Protected Data (Backup Server)

Reference a data file of the replication volume.

Since protection is set to the replication volume by the WORM function, you cannot write to the data file.

Unmounting replication volume (backup server)

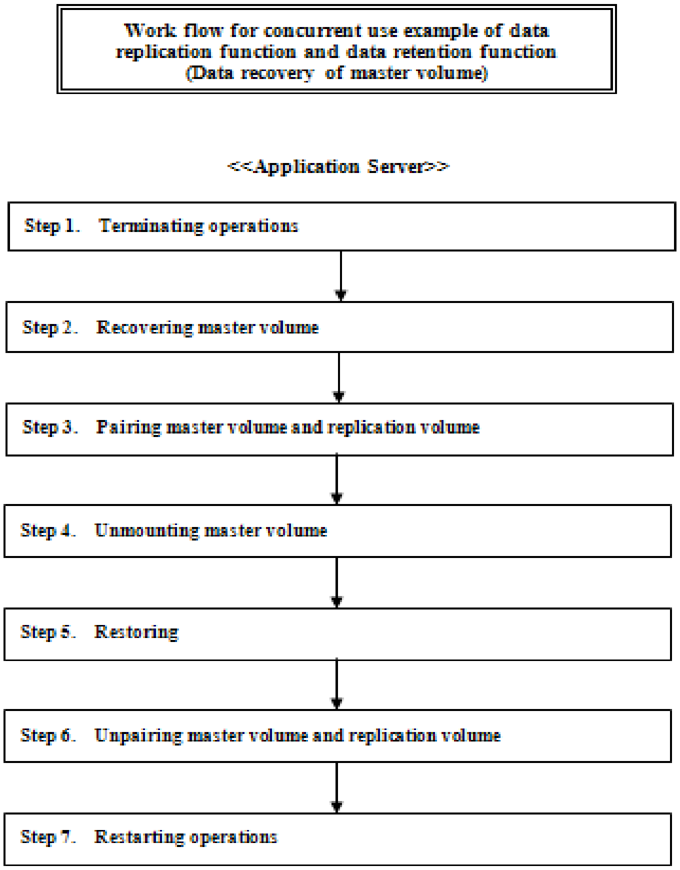
Unmount the replication volume after referencing it.

When the replication volume is unmounted, the drive letter or NTFS folder name set for the volume is automatically deleted.

```
iSMrc_umount -drv F: -offline
```

Operation flow (data recovery of master volume)

(7) Operation flow (data recovery of master volume)


Work flow for concurrent use example of data replication function and data retention function (Data recovery of master volume)
<<Application Server>>
Step 1. Terminating operations
Step 2. Recovering master volume
Step 3. Pairing master volume and replication volume
Step 4. Unmounting master volume
Step 5. Restoring
Step 6. Unpairing master volume and replication volume
Step 7. Restarting operations

Operation procedure (Data Recovery of Master Volume)

Terminating operations (application server)

Terminate or halt the operations that are accessing the volume where a fault has occurred.

Repairing master volume (application server)

You may bind a new logical volume when, for example, a hardware fault has occurred and you repair the master volume by rebuilding it. In such a case, use [Disk Management] (Windows) to create a disk signature.

Then set partitions, perform formatting to create a file system, and reset the drive letter or NTFS folder. For the partitions, file system, and drive letter or NTFS folder, make the same settings as you did before the occurrence of fault.

You must also re-create and update a volume list.

```
iSMvollist -cr
```

Pairing master volume and replication volume (application server)

Pair the master volume and backed up replication volume.

```
iSMrc_pair -pair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Unmount Replication Volume (Application Server)

Unmount the master volume in preparation for restoration.

```
iSMrc_umount -drv D: -offline
```

Restoring (Application Server)

Specify Restore(protect) and restore the backup data from the replication volume to the master volume.

```
iSMrc_restore -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld -mode
protect -wait
```

Unpair Master Volume And Replication Volume (Application Server)

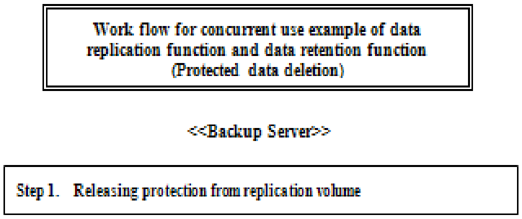
Unpair the master volume and replication volume.

```
iSMrc_pair -unpair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Restarting Operations (Application Server)

Restart the operations that have been terminated.

Operation Flow (Protected Data Deletion)


Work flow for concurrent use example of data replication function and data retention function (Protected data deletion)
<<Backup Server>>
Step 1. Releasing protection from replication volume

Operation procedure (Protected Data Deletion)

Releasing protection from replication volume (backup server)

Release protection from the replication volume.

In this example, protection setting for the replication volume is released.

```
iSMpc_release -vol DB_BK_2006_06 -volflg ld
```

Before you perform an operation for releasing volume protection, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection release command, the volume is unmounted within the command.

Measures for Errors

This section describes how to take measures against faults that occur during WORM operation. Measures against following faults are described in this section.

Volume reinitialization fault

SnapSAN Manager Server or client fault

ProtectControl abnormal end

Invalid product

How to collect information necessary to analyze unidentified faults is also described.

Volume Reinitialization Fault

If volume initialization by the volume reinitialization function has aborted due to a problem such as a hardware fault, the volume is still read/write-protected and cannot be accessed from a server.

When you have determined that volume initialization by a command operation or the SnapSAN Manager GUI has failed, consult your maintenance engineer.

SnapSAN Manager Server or Client Fault

For faults when the SnapSAN Manager server and the SnapSAN Manager client are used, refer to the following manuals supporting platforms on which the SnapSAN Manager server is running.

User's Manual

Abnormal End of ProtectControl

ProtectControl outputs error contents and messages to the standard output, standard error output, event log, command trace, or operation trace when an error has occurred.

The internal information necessary for analyzing faults is recorded in operation trace.

The following describes a ProtectControl error that requires a special action.

Failure to clear the read-only attribute from the volume

When you set or release volume protection using the WORM function, Windows Server 2003 SP1 or later uses the relevant function of Virtual Disk Service (VDS) to work with the read-only attribute of the volume.

When you release protection from a volume, the message below may be output, indicating a failure to clear the read-only attribute from the volume.

```
iSM21901: Failed to clear Read-Only volume attribute to target volume.
VOL:<aaa...a>
```

Write operation on the volume cannot be performed from a server. If this happens, clear the read-only attribute from the volume using the attributes volume command of the DISKPART utility, which is installed as standard with Windows.

An example of executing the attributes volume command is shown below. In this example, the number of the target volume is 3.

DISKPART> select volume 3

DISKPART> attributes volume clear readonly

Invalid Product

If the product for WORM function has not been purchased, the protection setting for a volume through the WORM abnormally terminates.

For purchased products, check disk array Properties in the State Monitoring screen of the SnapSAN Manager.

Information Gathering in the Event of a Fault

When an error whose reason is unknown has occurred and you want to request the provider to investigate the error, you must collect information required for error analysis.

For ProtectControl error

Follow the steps below to execute the command and collect the operation trace and other fault information at a time.

A disk for storing fault information must have at least about 4 MB of unused space. The total size of fault information files differs depending on the system status, and it may exceed 4 MB. It is advisable to allocate an unused space of enough size.

Log on as a member in the Administrators group.

Select [Start] of Windows   [All Programs]   [ControlCommand]   [Storage Manager Volume List]   [Difficulty Information Gather].

Confirm that the iSMvolgather directory is created under the installation directory when the storage destination directory is not changed or under the specified directory when it is changed, and obtain the files under that directory.

Operations when the Configuration is Changed

It is necessary to recreate the volume list to reflect the new configuration information to the volume list when you change the disk array or server (OS) configuration.

Conditions Requiring Volume List Update

Be sure to recreate and update the volume list after changing the following configurations:

- Change of disk array configuration
- Change of disk array name
- Change of logical disk name
- Change of logical disk OS type
- Adding of logical disk, and change and deleting of configuration
- Change of Access Control setting
- Adding and deleting of disk array connected by Replication and Mirroring

If the disk array configures Replication and Mirroring and the above configurations are changed in the remote-side disk array, be sure to update the volume list as well.

Change of server configuration

- Adding, change and deleting of partition
- Adding, change and deleting of mount point set to the volume (drive letter or NTFS folder name)
- Adding, deleting and change of control volume definition (only when the control volume is used)
- Change of connection configuration (path) between the disk array and server

Updating Volume List

To update a volume list, execute the iSMvollist command with the -cr option specified or execute the [Create/Update Volume List] operation in the Volume List Display screen (screen operation). The user must belong to the Administrators group to update a volume list.

When updating a volume list, note the following points so that the information to be registered in the volume list including the logical disk and volume information already registered is complete.

Update a volume list in the following states.

- The path between the disk array and the server is normally connected.
- The logical disk in the disk array is recognized as a server (OS) disk device.
- The volume (partitions) in the disk is recognized by the server (OS).

When you add, delete, or change the control volume definition in the disk array with which the control volume attribute cannot be identified, execute the following operation before updating a volume list.

- Register the logical disk to be used as a control volume in advance by executing the [Define Control Volume] operation in the Volume List Display screen.
- Define the logical disk to be used as the control volume in advance in the control volume definition file.

To successfully register volume information in the volume list, update a volume list in the following states.

- Pairs are separated when the RV is connected to the server.
- The link-volume (LV) and snapshot-volume (SV) are linked when the LV in the snapshot function is connected to the server. The base-volume (BV) and LV are not linked when the BV is connected to the server.
- Protected data is readable when the logical disk for which the WORM function is applied is connected to the server.
- The volume is in the In use state and accessible when the logical disk for which the power saving function is applied is connected to the server.
- All the volumes are mounted and every mount point to be used (drive letter or NTFS folder name) is set.
- The link path between disk arrays is normal when the Replication and Mirroring is configured for the disk array.

After updating the volume list, display the information registered in the volume list to check that the items to be used such as logical disks, partitions (mount point volume names), and mount points (drive letters or NTFS folder names) are all registered.

If the batch file or the like used for operation describes the logical disks, partitions (mount point volume names), mount points (drive letters or NTFS folder names), and other information to be operated, reflect the updated information in the volume list to that file.

Note that the ReplicationControl command execution may abnormally end in the future operation if the information in the volume list contains an error or if the volume list information is inconsistent with the batch or other file used for operation.

Chapter 6

Notes (Windows)

Windows Systems

This chapter describes some notes regarding management and operations of WORM function.

The OS for a server on which to perform WORM must be at least Windows Server 2003 with Service Pack 1.

Window 2000 Server and Windows Server 2003 without Service Pack are not supported because they may cause unintended write operations on the file system created on a volume.

Windows System Volumes and Partitions

Disk Type	Volume Type	Availability
Basic disk	Primary partition (MBR format)	✓
	Primary partition (GPT format)	✓*
	Logical volume on expanded partition	✓
Dynamic disk	Simple volume	-
	Span volume	-
	Stripe volume	-
	Mirror volume	-
	RAID-5 volume	-

✓:Available

-:Operation inhibited

*:With notes

The following conditions must be met when using partition disks in GPT (GUID partition table) format.

- The OS type of the logical disk is WG.
- The option setting file is set so as to enable to use partition disks in GPT (GUID partition table) format.

For details on the option setting file, refer to the ControlCommand Command Reference.

Use the MOUNTVOL command provided by the system at system startup to disable automatic volume mounting before operation.

To disable automatic volume mounting, specify the N option and execute the MOUNTVOL command as follows:

```
MOUNTVOL   /N
```

Disk Containing Multiple Partitions or Logical Volumes

Even when a certain mount point volume name is specified to execute WORM operation for a logical disk containing multiple partitions or logical volumes, all partitions or logical volumes on the logical disk become the target for WORM operation. This is because WORM operation is executed for an individual logical disk.

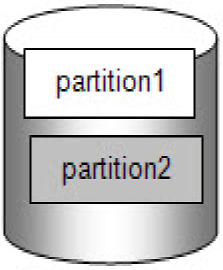


Figure 6-1: Snapshot for a Disk Containing Multiple Partitions

WORM operation using a logical disk containing multiple partitions or logical volumes is not recommended.

When the volume to be operated is recognized from the server (operating system) and can be accessed, ProtectControl obtains disk configuration information of that volume. When the volume contains multiple partitions or logical volumes, ProtectControl does not allow operation (by default).

You can perform operation for a logical disk containing multiple partitions or logical volumes by changing settings in the option setting file. In this case, however, be extremely careful about operation.

Management and Operations of WORM Function

- The number of volumes to allocate to servers, including those volumes for date retention, must be no larger than the maximum LUN that can be recognized by the OS.
- A volume for WORM cannot be allocated to LUN0. Allocate to LUN0 a normal volume that is not used by WORM function.
- The OS for a server on which to perform WORM must be Windows Server 2003 SP1 or later. WORM is performed on a volume in which RAW devices and a basic disk's primary partitions and extended partitions are set.
- Care must be taken in setting and operating partitions because WORM operations are performed on a disk-by-disk basis, not on a partition-by-partition basis.

- In a remote desktop environment where Windows Server 2003 or later is running, volumes can be used and ControlCommand can be executed from multiple remote desktop environments. However, to handle a volume by using ControlCommand, the volume must be exclusively used. Therefore, note the following to prevent an unmount command (iSMrc_umount) from terminating abnormally or automount from causing unexpected data corruption after unmounting the volume.
  - When executing a ControlCommand command, do not use a volume being used by another remote desktop.
  - When a volume is being used by a ControlCommand command executed by another terminal service, do not reference the volume by using Windows Explorer or an application.
- On Windows Server 2003, use the MOUNTVOL command provided by the system at system startup to disable automatic volume mounting (MOUNTVOL /N) before operation.
- VERITAS VxVM is not supported.
- To unmount a target volume of WORM, use the iSMrc_umount with the -offline option. In this case, note the following.
  - Only one mount point (drive letter or NTFS folder name) needs to be set to the volume to be unmounted. If no mount point or multiple mount points are set, unmounting cannot be executed. Therefore, the volume cannot be unmounted if all mount points are deleted using the MOUNTVOL command with D option specified. When multiple mount points are set for a volume, use the D option of the MOUNTVOL command to set only one mount point for the volume, and then unmount the volume.
- In a system configuration with MSCS, a target volume for WORM cannot be used as a shared disk for a cluster.
- When performing WORM, ensure that an update to a target volume has been accepted and cache data in the OS file system has been reflected to the disk. If the data has not completely reflected to the disk and volume protection is performed, there is a risk of protecting a volume storing inconsistent data.
- If an incorrect protection setting for an unintended volume prevents you from releasing protection from the volume, consult your maintenance engineer.
- When you perform [Rescan Disks] and [Refresh] in Windows [Disk Management] after setting the target volume to NotAccessible by the WORM operation on a Windows Server 2008, the following error message may be recorded in the event log. However, the operation is not affected.

  <Message example>

  SourceVirtual Disk Service

  Event ID1

  Description: Unexpected failure. Error code: 13@02000018

  * A different value may be displayed for the error code.
- When you protect MV or RV of the data replication function, the volume must have been separated. When you perform Separate (immediate) of the replication function, the RV becomes available (available for read or write) but cannot be protected because the data has not been established. Wait until Separate is completed.

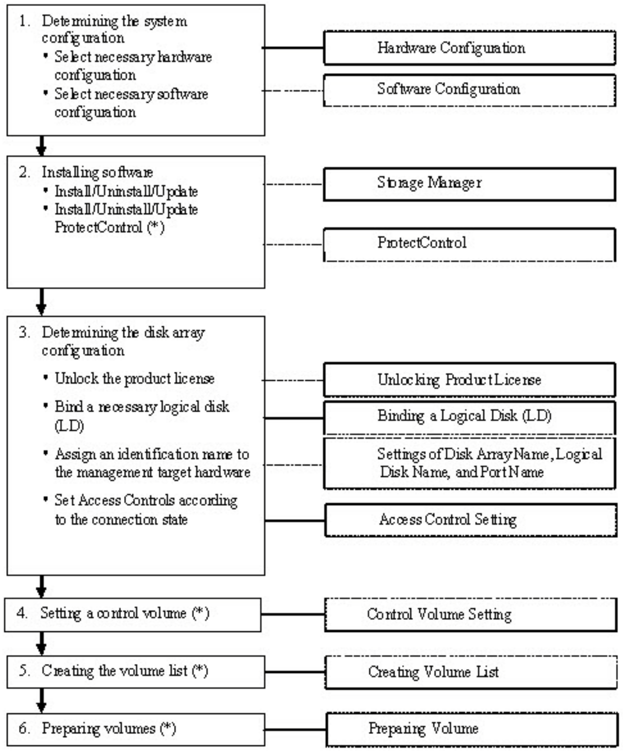
Chapter 7

Installation (Linux)

System Configuration

This chapter describes the system installation procedures showing an example to establish a WORM system using disk arrays in an existing operation system.

Installation works are outlined below. For details of the procedures, refer to the associated sections. Works followed by (*) mark are necessary for servers where ProtectControl will be installed.



1. Determining the system configuration
• Select necessary hardware configuration
• Select necessary software configuration
Hardware Configuration
Software Configuration
2. Installing software
• Install/Uninstall/Update
• Install/Uninstall/Update ProtectControl (*)
Storage Manager
ProtectControl
3. Determining the disk array configuration
• Unlock the product license
• Bind a necessary logical disk (LD)
• Assign an identification name to the management target hardware
• Set Access Controls according to the connection state
Unlocking Product License
Binding a Logical Disk (LD)
Settings of Disk Array Name, Logical Disk Name, and Port Name
Access Control Setting
4. Setting a control volume (*)
Control Volume Setting
5. Creating the volume list (*)
Creating Volume List
6. Preparing volumes (*)
Preparing Volume

Figure 7-1: Install Flow - Linux

Hardware Configuration

Select hardware components according to the business conditions, requirements, disk capacity, and so forth.

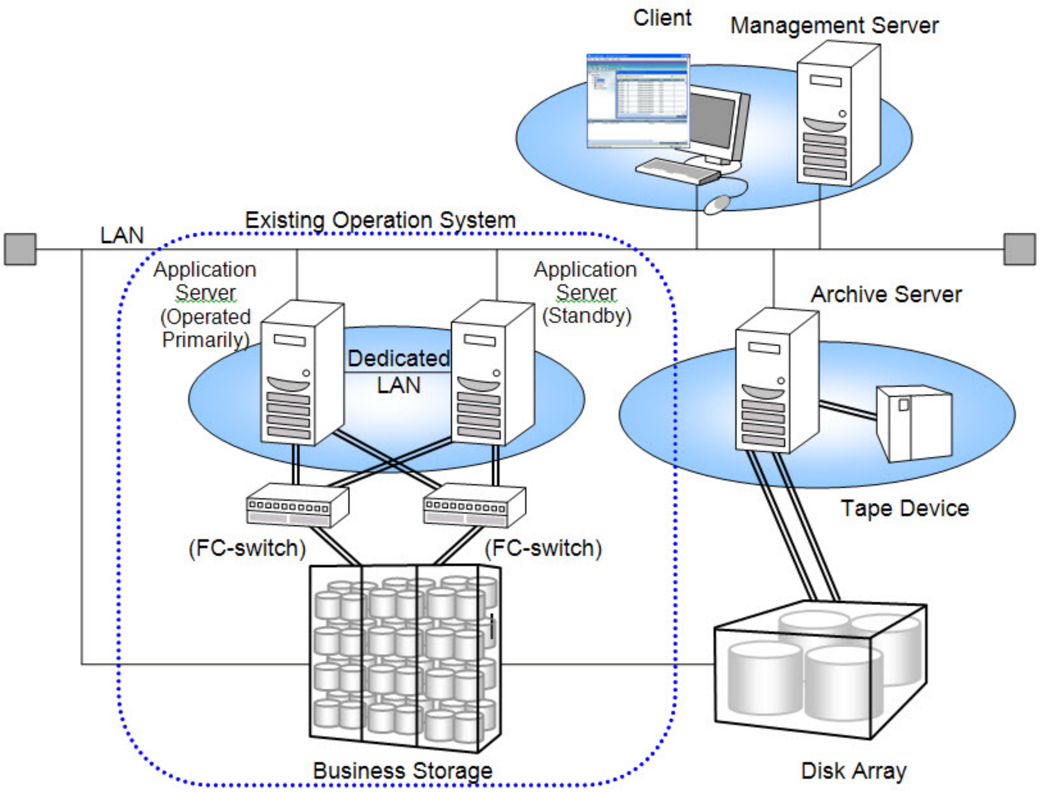


Figure 7-2: Hardware Configuration

- Though a business or archive server may also be used as a management server, using a specific management server is recommended. Use of LAN connection is strongly recommended for connection with disk array.
- Connect the path of individual servers, to be connected to the disk array, to the port of different directors, limiting the servers to be accessed by Access Control.
- In the above configuration example, the application servers are installed in a cluster and mutually connected through the dedicated LAN.

Software Configuration

Select software to be used according to the hardware components, operating conditions, etc.

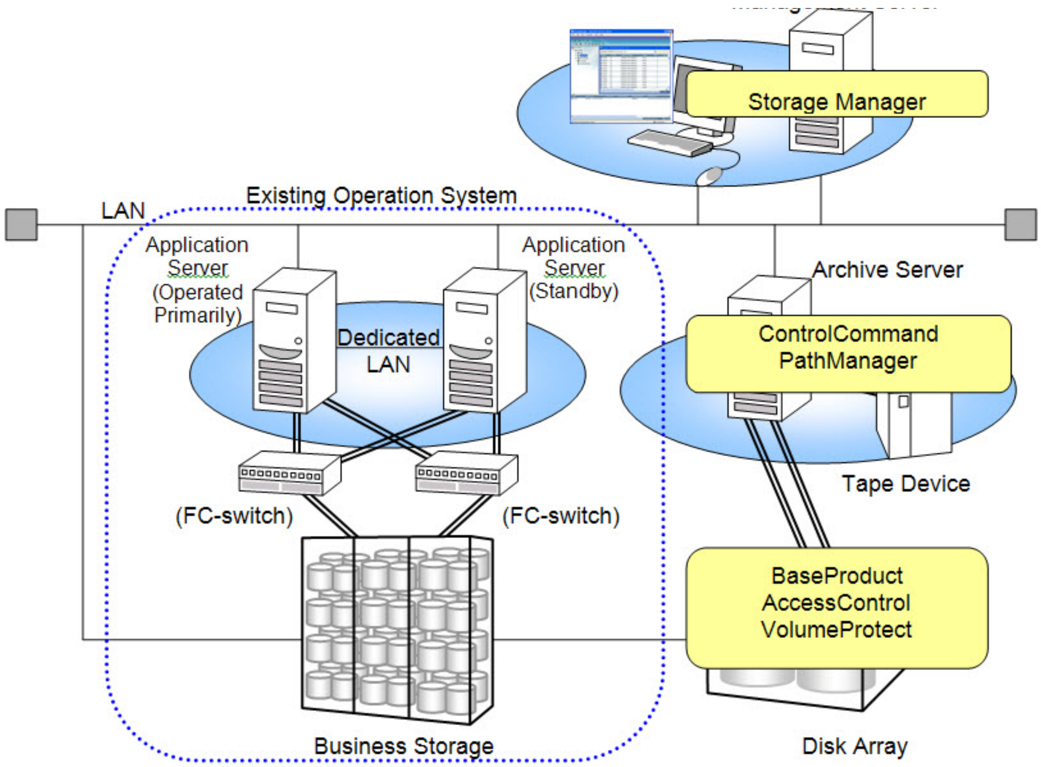


Figure 7-3: Software Configuration

- Install the backup software in the archive server.
- Install the management software in the management server. Install the SnapSAN Manager in the management server.
- Install the ProtectControl in the archive server. ProtectControl is included in ControlCommand.
- VolumeProtect and AccessControl are installed in the disk array. They become available by unlocking the license.

Software Installation

ProtectControl

To install ProtectControl software that is included in ControlCommand, use the rpm command.

Setting Operating Environment

You can set various types of operations when executing a command by using the environment variables.

Uninstall

To uninstall ProtectControl software, use the rpm command.

For details on the uninstallation procedure, refer to the installation guide attached to this software.

Update

To update the ProtectControl software, uninstall the existing software, and then install the new software.

Disk Array Configuration

For the disk array to be connected, determine the configuration for using the WORM function.

Unlocking Product License

To use the VolumeProtect, you must unlock the product license set in the disk array. To unlock the license, you must purchase the corresponding products equal to or greater than the total capacity of the data disk.

At execution, ProtectControl checks the license status of the products and check whether they are available.

If the total capacity of the data disk exceeds the product's specified capacity because physical disks are added to the disk array system, it is necessary to unlock the product licenses equal to or greater than lack of licenses.

Binding a Logical Disk (LD)

Bind volumes for use with the WORM function.

For the data that must conform to the regulations and the like that require data storage in non-falsifiable format, you should consider the frequency of occurrence of the data, the size of the data, the specified retention period, and the maximum LUN that can be recognized by the OS. Then, determine the capacity and number of volumes for use with the WORM function, and bind logical disks in disk arrays. For details on the operation procedure, refer to the Configuration Setting Tool User's Manual (GUI).

Settings of Disk Array Name, Logical Disk Name, and Port Name

You can assign identification names to hardware components managed by the SnapSAN Manager. Identification names can be given to the following items:

- Disk array subsystem name
- Logical disk name (plus OS type)
- Port name

It is better to set a disk array subsystem name, port name, and logical disk name according to the operating conditions and server connection conditions.

When you use the WORM function, you do not need to note disk array names and port names. For the OS type of a logical disk, you need to note the following.

- A logical disk name must be set so as to identify data to be stored.
- The OS type of a logical disk must be appropriate for the supporting platform.

These settings are performed from an SnapSAN Manager client.

Disk Array Name Setting: S1800AT Mail_Log_Archive

Port Names:

Director Number	Port Number	Port Name	Connected Server
00h	00h	ARCHIVE_PRIMARY	Archive server
01h	00h	ARCHIVE_SECONDARY	

This is a setting example conforming to the connection configuration of servers.

Setting Logical Disk Names and OS Types

LD No.	OS Type	Logical Disk Name	Remarks
0050h	LX	MAIL_LOG_2005_01	Volume for e-mail log of January 2005
0051h		MAIL_LOG_2005_02	Volume for e-mail log of February 2005
0052h		MAIL_LOG_2005_03	Volume for e-mail log of March 2005
0053h		MAIL_LOG_2005_04	Volume for e-mail log of April 2005
0054h		MAIL_LOG_2005_05	Volume for e-mail log of May 2005
0055h		MAIL_LOG_2005_06	Volume for e-mail log of June 2005
0056h		MAIL_LOG_2005_07	Volume for e-mail log of July 2005
0057h		MAIL_LOG_2005_08	Volume for e-mail log of August 2005
0058h		MAIL_LOG_2005_09	Volume for e-mail log of September 2005
0059h		MAIL_LOG_2005_10	Volume for e-mail log of October 2005
005ah		MAIL_LOG_2005_11	Volume for e-mail log of November 2005
005bh		MAIL_LOG_2005_12	Volume for e-mail log of December 2005
0060h		ARCHIVE_CV	Control volume

- Set the OS type as LX, which is the Linux operating system default value.
- This example shows logical disk names when archiving the e-mail log once a month.

Access Control is necessary for a system in which WORM function is installed.

Before performing the following operations, enable Access Control setting. In addition, Access Control setting needs to be performed for volumes that have already been used for other operations.

Access Control Setting

To prevent a wrong update to a volume or a wrong modification of the disk configuration, usually you need to set the system with WORM function so that volumes to be used by WORM function cannot be referenced by a server other than an archive server.

Therefore, to use WORM function, you need to limit logical disks that can be accessed from a server by using Access Control.

To use WORM function, also take note the following points and set Access Control.

Setting Access Control

- Assign volumes to be used by WORM function to an archive server.

Before introducing servers, you must determine the server connection modes and design Access Control settings. Access Control can be set for individual ports or WWNs. Setting for Access Controls requires purchasing the AccessControl.

Control Volume Setting

A control volume is used when a server issues control I/O to the relevant disk array. Register one logical disk for each disk array as the volume for issuing I/O to that disk array in the volume list.

RV, or a base-volume (BV) and link-volume (LV) for the snapshot function cannot be registered as a control volume because it may enter the Not Ready state during operation.

The following series disk arrays can identify the purpose (attribute) of the logical disk bound as a control volume.

When the logical disk information is displayed by the SnapSAN Manager client and so on these disk arrays that can identify the purpose (attribute) of a control volume, the identification information indicating that the purpose (attribute) of the logical disk is a control volume.

The control volume setting procedure differs depending on the disk array functions as shown below.

Disk Arrays Identifying the Control Volume Attribute

Create or update the volume list when the logical disk bound as a control volume is recognized as a disk by the server. The disk array identifies the logical disk having the control volume attribute from the logical disks connected to the server and automatically registers it in the volume list.

After creating or updating the volume list, list the control volumes using the iSMvollist command to check that the control volume has been successfully registered in the volume list.

```
iSMvollist -ctl
```

Other Disk Arrays

It is necessary to select the control volume from the logical disks connected to the server, and describe it in the control volume definition file on the server for definition. Describe the logical disk number (LDN) and disk array name of the logical disk to be used as a control volume in the control volume definition file.

You can check the information on the logical disk using the iSMrc_ldlist command. This information includes the list of disk arrays connected to the server, disk array names, list of logical disks in each disk array, and logical disk numbers.

- To display the list of disk arrays and disk array names

```
iSMrc_ldlist -d
```

- To display the list of logical disks in the disk arrays and the logical disk information

```
iSMrc_ldlist -de Disk array name
```

Select and describe one logical disk for each disk array. If you describe multiple logical disks in the same disk array, the information on the first one becomes valid and the information on the second and subsequent ones is ignored.

[File location and file name]

```
/etc/iSMrpl/ctlvol.conf
```

[Format]

Describe the sets of logical disk numbers and disk array names of all the control volumes used in the relevant server, one by one on a line each, by delimiting with line feed. The logical disk number on each line should be in hexadecimal. Delimit the logical disk number and disk array name with a space or tab character. On each line, the text after the pound symbol (#) is regarded as a comment and ignored.

A description example is shown below.

```
# ControlVolumes
# LDN    Disk Array Name
002a     Mail_Log_Archive
```

Rules

- Start description at the first column on the line.
- Use the line feed to delimit records.
- One record should be up to 1,024 (1-byte) characters.
- One record describes one control volume.
- The text from the pound symbol (#) to the end of the record is regarded as a comment.

Control Volume Registration

You should have updated the volume list to reflect the setting information described in the control volume definition file.

After creating or updating the volume list, list the control volumes using the iSMvollist command to check that the control volume has been successfully registered in the volume list.

```
iSMvollist -ctl
```

Creating Volume List

Creation of a volume list is required before using ProtectControl command. A volume list is created by the iSMvollist command with the -r option specified. Create a volume list with the appropriate user privilege.

The following command line shows an example to create a volume list with the iSMvollist command.

```
iSMvollist -r
```

Upon successful creation of volume list, the following message appears:

```
iSM11100: Command has completed successfully.
```

If creation of a volume list fails, execution of ProtectControl command is disabled. Troubleshoot in accordance with an error message or with operation error tracing, create a volume list again.

If the SnapSAN Manager server is running on the same server, it is required to exit SnapSAN Manager before creating a volume list.

Create a volume list in the following states.

- The path between the disk array and the server is normally connected.
- The logical disk in the disk array is recognized as a server (OS) disk device.
- The volume in the disk is recognized by the server (OS).

Execute the following operation before creating a volume list if you use a control volume in the disk array with which the control volume attribute cannot be identified.

- Define the logical disk to be used as a control volume in advance in the control volume definition file.

To successfully register volume information in the volume list, create a volume list in the following states.

- Pairs are separated when the RV in the data replication function is connected to the server.
- The link-volume (LV) and snapshot-volume (SV) are linked when the LV in the snapshot function is connected to the server. The base-volume (BV) and LV are also linked when the BV is connected to the server.
- Protected data is readable when the logical disk for which the WORM function is applied is connected to the server.
- The volume is in the In use state and accessible when the logical disk for which the power saving function is applied is connected to the server.
- The link path between disk arrays is normal when the Remote Replication is configured for the disk array.

After successfully creating a volume list, display the information registered in the volume list to check that the items to be used such as logical disks and special file names are all registered.

Once the volume list is successfully created, that information is maintained for operation. It is not necessary to update the volume list during operation. However, if the disk array, server (OS) volume, or other configuration is changed, it is required to recreate the volume list to reflect the new information. Note that an error or inconsistency may occur at execution of ProtectControl command unless the volume list is updated.

Preparing Volume

When using a volume for the first time for WORM operation, execute the steps given below for the target volume. The following is an example of the procedure for creating a file system on a volume to be used by WORM function.

Creating file system (archive server)

Create a file system to be used in WORM function if necessary.

Create a file system by entering the following.

The file system type supported for WORM function is ext2. Create an ext2 file system on the volume.

```
mkfs -t ext2 /dev/ddb
```

Mounting file system (archive server)

Mount a file system created on the volume.

```
mount -t ext2 /dev/ddb /MAIL_LOG/2005_01
```

Now, the volume is ready.

Volume management software such as LVM and VxVM cannot be used for volumes of WORM operation.

Chapter 8

Maintenance (Linux)

Operation Design

This chapter describes an example of operation using the WORM function, the operation procedure for WORM function, and the trouble-shooting for faults that may occur during operations.

To use the WORM function to enable operation that supports long-term storage of business data in non-falsifiable format, you must consider the following items:

Capacity and Number of Volumes

For the data that must conform to the regulations and the like that require data storage in non-falsifiable format, you should consider the frequency of occurrence of the data, the size of the data, the specified retention period, and the maximum LUN that can be recognized by the OS. Then, determine the capacity and number of volumes for use with the WORM function.

Whether to Allow Data Reference

Determine the protection state you should specify when you set volume protection, depending on whether to allow stored data to be referenced from an archive server.

WORM Period

Determine the retention period you should specify when you set volume protection, based on the regulations and the like that require data storage in non-falsifiable format.

Archive Operation

This section describes an example of archive operation by using the WORM function.

Although the text describes the commands in input order, it is recommended to automate the command execution by job scheduling software on the system built actually.

Protect business data that needs long-term storage and save the data in non-falsifiable format (data protection). When necessary, reference the protected data in long-term storage (protected data reference) or change volume protection settings (protection settings change). After the elapse of the period specified by any of the regulations and the like that require data storage in non-falsifiable format, you should delete the protected data (protected data deletion).

Data Protection

Select an empty volume in the archive storage as an archive volume. Transfer to the archive server business data that needs long-term storage in non-falsifiable format, and store the data in the archive volume. Accumulate business data until no more space is available on the archive volume, and then unmount the volume. Use the volume protection setting command to disable write operations on the volume. For the purposes of guarding the archive volume against physical faults and storing the data permanently, you should use backup software to save the volume data to tape after setting volume protection.

Protected Data Reference

To reference the data stored in the protected volume, mount the volume and access the protected data you want to reference.

Protection Settings Change

After the data stored in the protected volume is saved to tape, you should use the volume protection setting change command when you want to perform operations for changing the protection settings for the volume, such as changing the protection state and extending the WORM period.

Protected Data Deletion

After the elapse of the retention period set for the volume, use the volume protection release command to release protection from the volume, thereby enabling the volume to be reused.

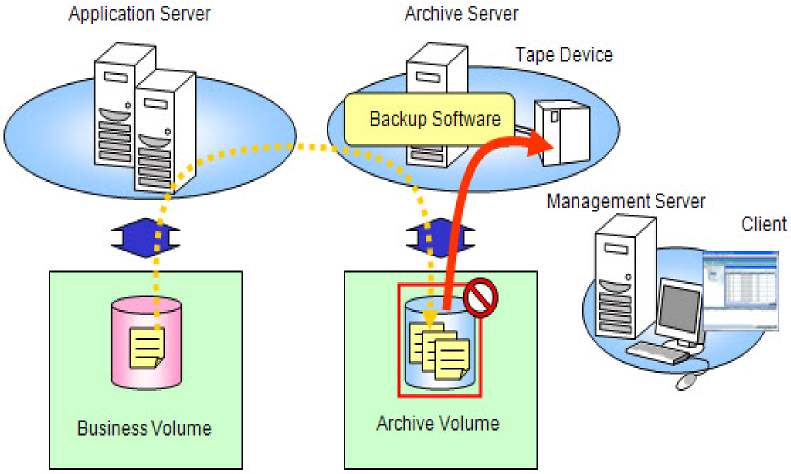


Figure 8-1: Archive Operations

Prerequisites

It is assumed that a file system has been created on the archive volume. The logical disk name and assigned mount point name for the archive volume are assumed to be as follows:

- Archive volume
  - Logical disk name (MAIL_LOG_2005_01)
  - Mount point name (/MAIL_LOG/2005_01)

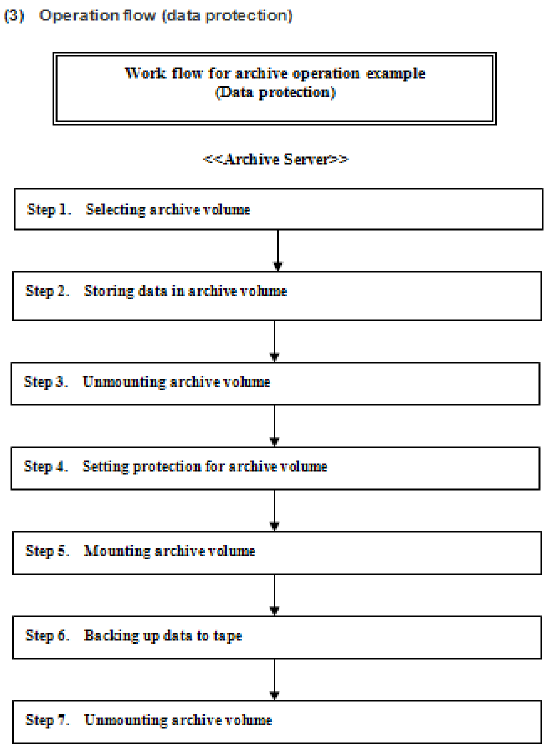

(3) Operation flow (data protection)
Work flow for archive operation example
(Data protection)
<<Archive Server>>
Step 1. Selecting archive volume
Step 2. Storing data in archive volume
Step 3. Unmounting archive volume
Step 4. Setting protection for archive volume
Step 5. Mounting archive volume
Step 6. Backing up data to tape
Step 7. Unmounting data archive volume

Figure 8-2: Operation Flow - Archive Operation

Operation Procedure (Data Protection)

Selecting archive volume (archive server)

Select an empty volume in the archive storage as an archive volume.

Storing data in archive volume (archive server)

Use a function such as FTP to transfer to the archive server business data that needs long-term storage in non-falsifiable format. Then, store data until no more space is available on the selected archive volume.

Unmount archive volume (archive server)

Unmount the archive volume in preparation for protection.

```
umount  /MAIL_LOG/2005_01
```

Setting protection for archive volume (archive server)

Set protection for the archive volume.

In this example, which involves tape backup in a later step, the protection state is set to ReadOnly, the retention date to March 31, 2015, and the retention mode to secure.

```
iSMpc_protect -vol MAIL_LOG_2005_01 -volflg ld -set ro -expire 20150331
-mode  secure
```

Mounting archive volume (archive server)

Mount the archive volume in preparation for tape backup.

```
mount -r -t ext2 /dev/ddb /MAIL_LOG/2005_01
```

Backing up data to tape (archive server)

Use backup software to back up the archive volume data to a medium such as tape.

The contents of the backed-up data and the protection settings (protection state, retention date, and retention mode) should be recorded on a label or the like to allow you to check them.

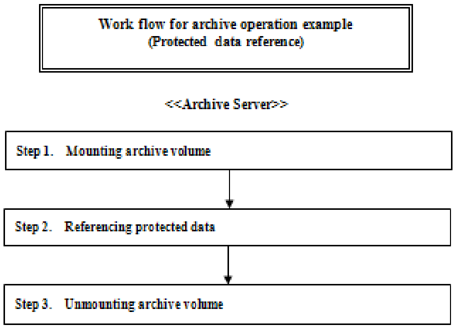
Unmounting archive volume (archive server)

Unmount the archive volume after tape backup.

```
umount /MAIL_LOG/2005_01
```

Before you perform an operation for setting volume protection, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection setting command, the command determines that the volume is mounted and stops setting protection.

(5) Operation flow (protected data reference)


Work flow for archive operation example
(Protected data reference)
<<Archive Server>>
Step 1. Mounting archive volume
Step 2. Referencing protected data
Step 3. Unmounting archive volume

Operation Procedure (Protected Data Reference)

Mounting Archive Volume (Archive Server)

Mount the archive volume to reference its data file.

```
mount -r -t ext2 /dev/ddb /MAIL_LOG/2005_01
```

Referencing Protected Data (Archive Server)

Reference a data file in the archive volume.

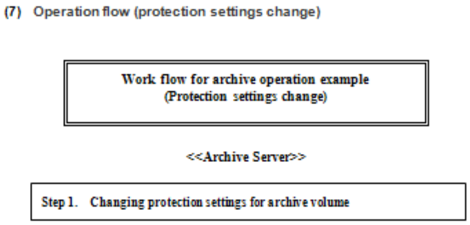
You cannot perform a write operation on data files because the archive volume is protected by the WORM function.

Unmounting archive volume (archive server)

Unmount the archive volume after referencing its data file.

```
umount /MAIL_LOG/2005_01
```

Operation Flow (Protection Settings Change)



(7) Operation flow (protection settings change)

Work flow for archive operation example
(Protection settings change)

<<Archive Server>>

Step 1. Changing protection settings for archive volume

Operation procedure (protection settings change)

Changing protection settings for archive volume (archive server)

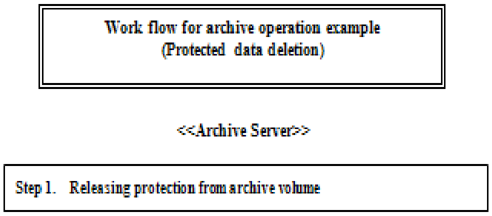
Change the protection settings for the archive volume.

In this example, the protection state of the archive volume is changed to NotAccessible, the retention date to March 31, 2025, and the retention mode to strict.

```
iSMpc_protect -vol MAIL_LOG_2005_01 -volflg ld -set na -expire 20250331
-mode strict
```

Before you perform an operation for changing volume protection settings, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection change command, the command determines that the volume is mounted and stops changing the protection settings.

Operation Flow (Protected Data Deletion)



Work flow for archive operation example
(Protected data deletion)

<<Archive Server>>

Step 1. Releasing protection from archive volume

Operation Procedure (Protected Data Deletion)

Releasing protection from archive volume (archive server)

Release protection from the archive volume.

In this example, data is cleared upon release of protection from the archive volume.

```
iSMpc_release -vol MAIL_LOG_2005_01 -volflg ld -reinit
```

Before you perform an operation for releasing volume protection, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection release command, the command determines that the volume is mounted and stops releasing protection.

Restoring Archive Volume Data

This section describes procedures of restoring archive volume data.

If a physical fault occurs, preventing you from accessing an archive volume protected by the WORM function or data files in that volume, you can restore the archive volume from a backup in a medium such as tape.

Assuming that a physical fault has occurred on a data file in the protected archive volume, this section describes the procedure for restoring the volume from a backup medium. It is also assumed that the backup of the archive volume to be restored has been made in the backup medium.

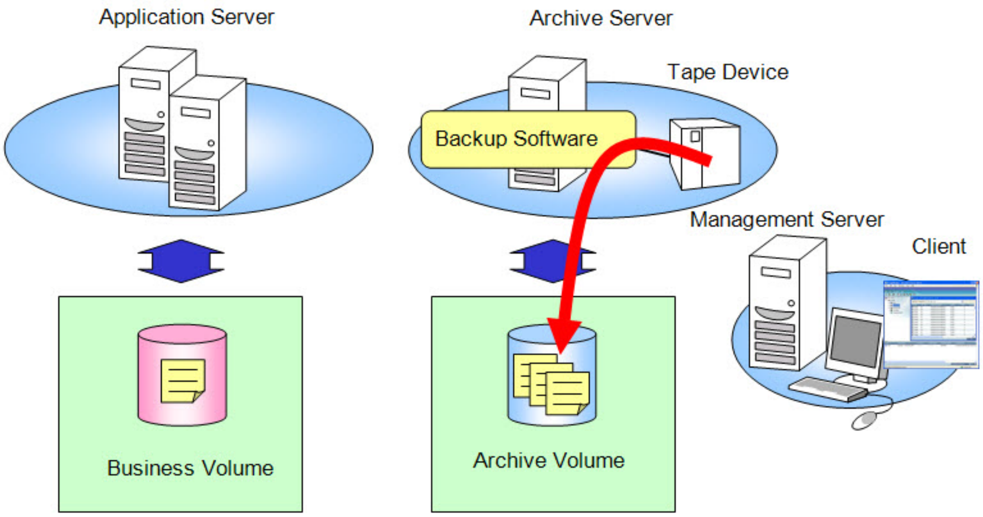


Figure 8-3: Case of Physical Fault

Prerequisites

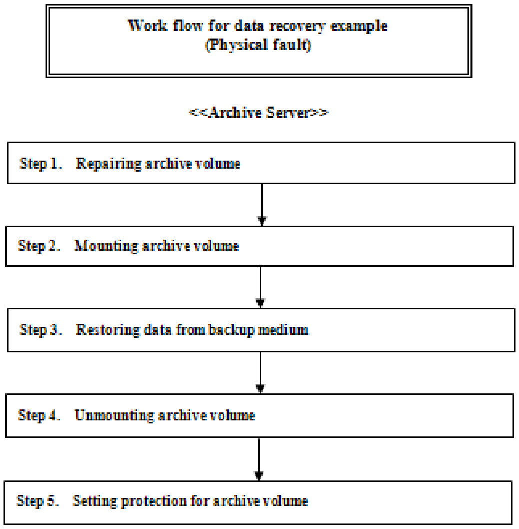
It is assumed that a file system has been created on the archive volume before occurrence of a physical fault. The logical disk name and assigned mount point name for the archive volume are assumed to be as follows:

Archive volume

- Logical disk name (MAIL_LOG_2005_01)
- Mount point name (/MAIL_LOG/2005_01)

Operation Flow (Data Recovery)

(3) Operation flow (data recovery)


Work flow for data recovery example
(Physical fault)
<<Archive Server>>
Step 1. Repairing archive volume
Step 2. Mounting archive volume
Step 3. Restoring data from backup medium
Step 4. Unmounting archive volume
Step 5. Setting protection for archive volume

Operation Procedure (Data Recovery)

Repairing Archive Volume (Archive Server)

You may bind a new logical volume when, for example, a hardware fault has occurred and you repair the archive volume by rebuilding it. In such a case, re-create a file system with the same settings as you did before occurrence of the fault.

You must also re-create and update a volume list.

```
iSMvollist -r
```

Mounting Archive Volume (Archive Server)

Mount the archive volume to establish an association between the archive volume and file system.

```
mount -t ext2 /dev/ddb /MAIL_LOG/2005_01
```

Restoring Data From Backup Medium (Archive Server)

Use backup software to restore the data saved in the backup medium to the archive volume.

Unmounting Archive Volume (Archive Server)

Unmount the archive volume in preparation for protection.

```
umount /MAIL_LOG/2005_01
```

Setting Protection for Archive Volume (Archive Server)

Set protection for the archive volume.

Check the protection settings (protection state, retention date, and retention mode) recorded when you created the backup, and make the same settings as you did before occurrence of the fault. In this example, the protection state is set to ReadOnly, the retention date to March 31, 2015, and the retention mode to secure.

```
iSMpc_protect -vol MAIL_LOG_2005_01 -volflg ld -set ro -expire 20150331
-mode  secure
```

Concurrent Operation with Replication Function

This section describes an example of operation by concurrently using the WORM function and data replication function.

Although the text describes the commands in input order, it is recommended to automate the command execution by job scheduling software on the system built actually.

Back up the data to be stored for a long term by the data replication function and then protect the replication volume for a specified time period by the WORM operations (data backup and protection). When necessary, reference the protected data in long-term storage (protected data reference). When data in a master volume is corrupted by physical failure or mis-operation, the master volume is restored from the backed-up replication volume (data recovery of master volume). After the elapse of the period specified at data protection, protected data is deleted (protected data deletion).

Data Backup and Protection

Select a target replication volume to be used from a replication volume group that has been created and pair it with a master volume. Back up data in the master volume into the replication volume by using the data replication function. After backup, protect the backed-up replication volume entirely by executing protection operation of the WORM function. Unpair the protected replication volume from the master volume and store it for a long period.

For the specific operations, refer to Operation flow (data backup and protection) and Operation procedure (data backup and protection).

Protected Data Reference

To reference the data stored in the protected volume, mount the volume and access the protected data you want to reference.

For the specific operations, refer to Operation flow (protected data reference) and Operation procedure (protected data reference).

Data Recovery of Master Volume

When data in a master volume is corrupted by physical failure or mis-operation, the master volume is restored from the backed-up replication volume.

For the specific operations, refer to Operation flow (data recovery of master volume) and Operation procedure (data recovery of master volume).

Operation Procedure (Data Recovery)

Repairing Archive Volume (Archive Server)

You may bind a new logical volume when, for example, a hardware fault has occurred and you repair the archive volume by rebuilding it. In such a case, re-create a file system with the same settings as you did before occurrence of the fault.

You must also re-create and update a volume list.

```
iSMvollist -r
```

Mounting Archive Volume (Archive Server)

Mount the archive volume to establish an association between the archive volume and file system.

```
mount -t ext2 /dev/ddb /MAIL_LOG/2005_01
```

Restoring Data From Backup Medium (Archive Server)

Use backup software to restore the data saved in the backup medium to the archive volume.

Unmounting Archive Volume (Archive Server)

Unmount the archive volume in preparation for protection.

```
umount /MAIL_LOG/2005_01
```

Setting Protection For Archive Volume (Archive Server)

Set protection for the archive volume.

Check the protection settings (protection state, retention date, and retention mode) recorded when you created the backup, and make the same settings as you did before occurrence of the fault. In this example, the protection state is set to ReadOnly, the retention date to March 31, 2015, and the retention mode to secure.

```
iSMpc_protect -vol MAIL_LOG_2005_01 -volflg ld -set ro -expire 20150331
-mode secure
```

Concurrent Operation with Replication Function

This section describes an example of operation by concurrently using the WORM function and data replication function.

Although the text describes the commands in input order, it is recommended to automate the command execution by job scheduling software on the system built actually.

Back up the data to be stored for a long term by the data replication function and then protect the replication volume for a specified time period by the WORM operations (data backup and protection). When necessary, reference the protected data in long-term storage (protected data reference). When data in a master volume is corrupted by physical failure or mis-operation, the master volume is restored from the backed-up replication volume (data recovery of master volume). After the elapse of the period specified at data protection, protected data is deleted (protected data deletion).

Data Backup and Protection

Select a target replication volume to be used from a replication volume group that has been created and pair it with a master volume. Back up data in the master volume into the replication volume by using the data replication function. After backup, protect the backed-up replication volume entirely by executing protection operation of the WORM function. Unpair the protected replication volume from the master volume and store it for a long period.

For the specific operations, refer to Operation flow (data backup and protection) and Operation procedure (data backup and protection).

Protected Data Reference

To reference the data stored in the protected volume, mount the volume and access the protected data you want to reference.

For the specific operations, refer to Operation flow (protected data reference) and Operation procedure (protected data reference).

Data Recovery of Master Volume

When data in a master volume is corrupted by physical failure or mis-operation, the master volume is restored from the backed-up replication volume.

For the specific operations, refer to Operation flow (data recovery of master volume) and Operation procedure (data recovery of master volume).

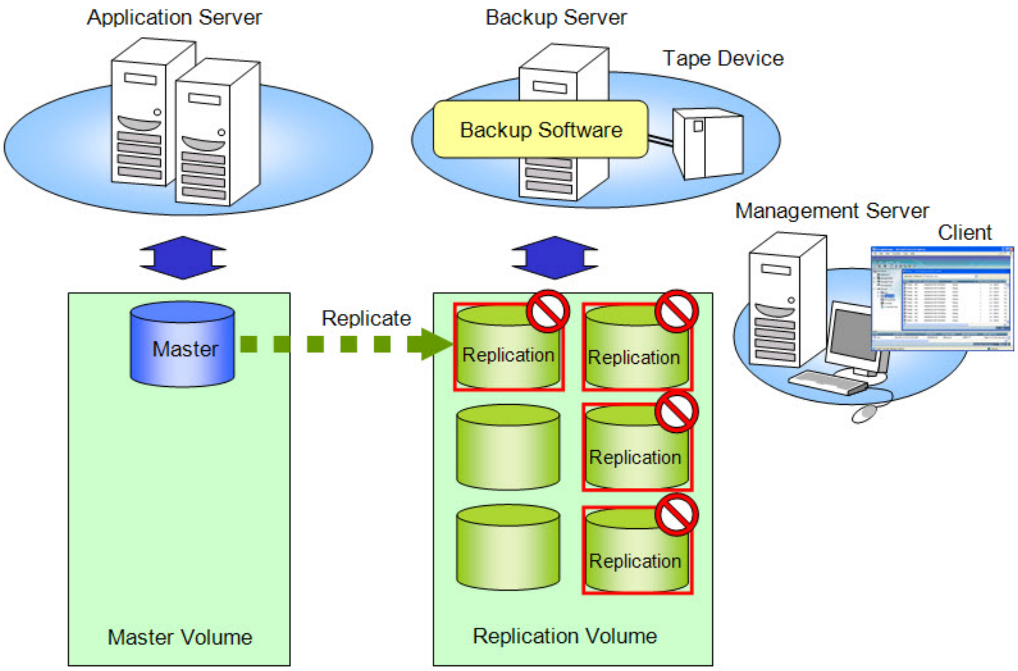


Figure 8-4: Data Replication and WORM

Prerequisites

It is necessary to create a replication volume, in advance, of the same capacity and OS Type as a master volume and make the backup server recognize it. It is assumed that a replication volume is an empty volume and has not been mounted to the backup server. The logical disk names of a master volume and replication volume, which are used in the following description, are assumed to be a follows:

- Master volumeLogical disk name (DB_MASTER)
- Replication volume to be usedLogical disk name (DB_BK_2006_06)

Operation Flow (Data Backup and Protection)

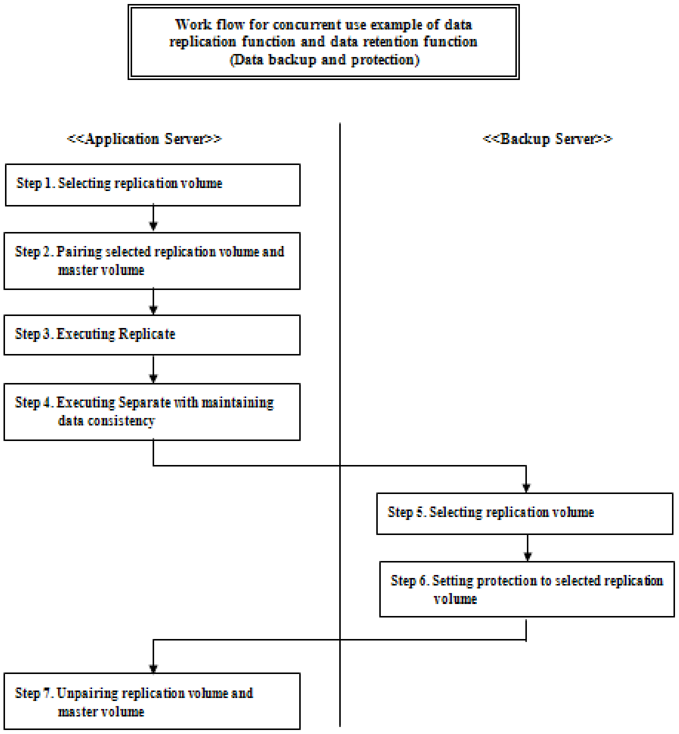

Work flow for concurrent use example of data replication function and data retention function (Data backup and protection)
<<Application Server>>
<<Backup Server>>
Step 1. Selecting replication volume
Step 2. Pairing selected replication volume and master volume
Step 3. Executing Replicate
Step 4. Executing Separate with maintaining data consistency
Step 5. Selecting replication volume
Step 6. Setting protection to selected replication volume
Step 7. Unpairing replication volume and master volume

Figure 8-5: Data Backup and Protection

Data Backup and Protection

Selecting Replication Volume (Application Server)

Select a replication volume to be used from replication volumes that have been created.

Pairing Selected Replication Volume and Master Volume (Application Server)

Set a pair of a selected replication volume and a master volume.

```
iSMrc_pair -pair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Executing Replicate (Application Server)

Execute Replicate and copy data from a master volume to a replication volume to synchronize the data.

```
iSMrc_replicate -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld -
wait
```

Executing Separate with Maintaining Data Consistency (Application Server)

After maintaining data consistency of a master volume, execute Separate and establish the data of a replication volume.

Selecting Replication Volume (Backup Server)

Select a replication volume for which backup is established.

Setting Protection to Selected Replication Volume (Backup Server)

Execute the volume protection operation for a replication volume.

In this example, the protection state, retention period, and retention mode are set to ReadOnly, one year, and secure, respectively, to reference the data in the subsequent step.

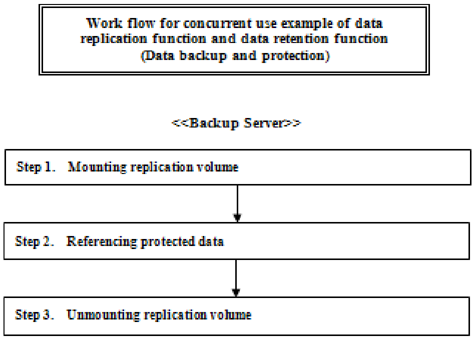
```
iSMpc_protect -vol DB_BK_2006_06 -volflg ld -set ro -expire +1y -mode
secure
```

Unpairing Replication Volume and Master Volume (Application Server)

Unpair a replication volume and a master volume.

```
iSMrc_pair -unpair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Operation Flow (Data Backup and Protection)


Work flow for concurrent use example of data
replication function and data retention function
(Data backup and protection)
<<Backup Server>>
Step 1. Mounting replication volume
Step 2. Referencing protected data
Step 3. Unmounting replication volume

Operation Procedure (Protected Data Reference)

Mounting Replication Volume (Backup Server)

Mount a replication volume in ReadOnly to reference its file.

```
mount -r -t ext2 /dev/ddb /DB_BK/2006_06
```

Referencing Protected Data (Backup Server)

Reference a data file of the replication volume.

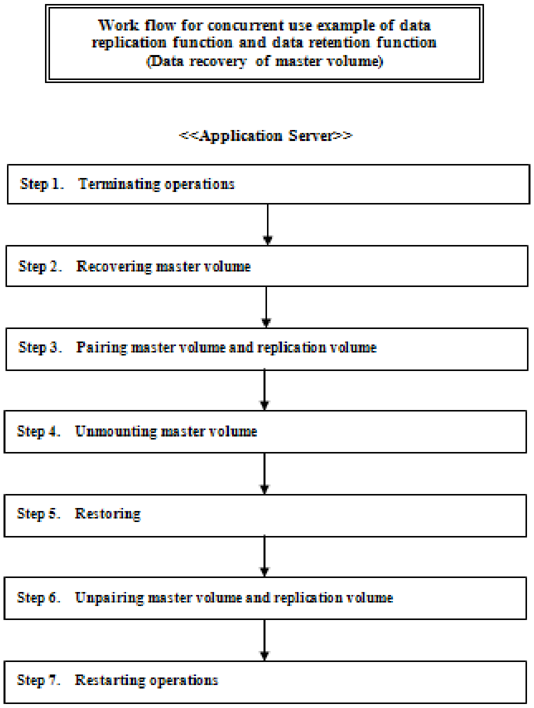
Since protection is set to the replication volume by the WORM function, you cannot write to the data file.

Unmounting Replication Volume (Backup Server)

Unmount the replication volume after referencing it.

umount /DB_BK/2006_06

Operation Flow (Data Recovery Of Master Volume)


Work flow for concurrent use example of data replication function and data retention function (Data recovery of master volume)
<<Application Server>>
Step 1. Terminating operations
Step 2. Recovering master volume
Step 3. Pairing master volume and replication volume
Step 4. Unmounting master volume
Step 5. Restoring
Step 6. Unpairing master volume and replication volume
Step 7. Restarting operations

Operation Procedure (Data Recovery of Master Volume)

Terminating Operations (Application Server)

Terminate or halt the operations that are accessing the volume where a fault has occurred.

Repairing master volume (application server)

You may bind a new logical volume when, for example, a hardware fault has occurred and you repair the master volume by rebuilding it. In such a case, re-create a file system with the same settings as you did before the occurrence of fault.

You must also re-create and update a volume list.

```
iSMvollist -r
```

Pairing Master Volume and Replication Volume (Application Server)

Pair the master volume and backed-up replication volume.

```
iSMrc_pair -pair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Unmounting Replication Volume (Application Server)

Unmount the master volume in preparation for restoration.

```
umount /DB_BK/2006_06
```

Restoring (Application Server)

Specify Restore(protect) and restore the backup data from the replication volume to the master volume.

```
iSMrc_restore -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld -mode
protect  -wait
```

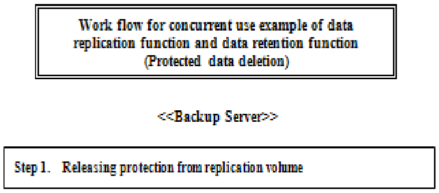
Unpairing Master Volume and Replication Volume (Application Server)

Unpair the master volume and replication volume.

```
iSMrc_pair -unpair -mv DB_MASTER -mvflg ld -rv DB_BK_2006_06 -rvflg ld
```

Restarting Operations (Application Server)

Restart the operations that have been terminated in Step 1.


Work flow for concurrent use example of data replication function and data retention function (Protected data deletion)
<<Backup Server>>
Step 1. Releasing protection from replication volume

Operation Procedure (Protected Data Deletion)

Releasing protection from replication volume (backup server)

Release protection from the replication volume.

In this example, protection setting for the replication volume is released.

```
iSMpc_release -vol DB_BK_2006_06 -volflg ld
```

Before you perform an operation for releasing volume protection, the volume must already be unmounted. If the volume has not been unmounted and you execute the volume protection release command, the command determines that the volume is mounted and stops releasing protection.

Measures for Errors

This section describes how to take measures against faults that occur during WORM operation. Measures against the following faults are described in this section.

- Volume reinitialization fault
- SnapSAN Manager Server or client fault
- ProtectControl abnormal end
- Invalid product

How to collect information necessary to analyze unidentified faults is also described.

Volume Reinitialization Fault

If volume initialization by the volume reinitialization function has aborted due to a problem such as a hardware fault, the volume is still read/write-protected and cannot be accessed from a server.

When you have determined that volume initialization by a command operation or the SnapSAN Manager GUI has failed, consult your maintenance engineer.

SnapSAN Manager Server or Client Fault

Abnormal End of ProtectControl

ProtectControl outputs error contents and messages to the standard output, standard error output, system log, command trace, or operation trace when an error has occurred.

The standard output, standard error output, system log, or command trace records the messages described in the Messages Handbook. Take necessary actions depending on the message.

The command trace is output in the etc folder (/opt/iSMrpl/etc/) under the folder where ProtectControl has been installed as a text file beginning with iSM_Log. Check the contents using a text editor.

The internal information necessary for analyzing faults is recorded in operation trace.

Invalid Product

If the product for WORM function has not been purchased, the protection setting for a volume through the WORM abnormally terminates.

For purchased products, check disk array Properties in the State Monitoring screen of the SnapSAN Manager.

Information Gathering in the Event of a Fault

When an error whose reason is unknown has occurred and you want to request the provider to investigate the error, you must collect information required for error analysis.

For ProtectControl error

Follow the steps below to execute the command and collect the operation trace and other fault information at a time.

A disk for storing fault information must have at least about 4 MB of unused space. The total size of fault information files differs depending on the system status, and it may exceed 4 MB. It is advisable to allocate an unused space of enough size.

1. Log in as root.
2. Execute the iSMvolgather command.

```
# iSMvolgather[Directory name]
```

* Be sure to specify the directory name with the absolute path name.

- The iSMvolgather directory is created under the /opt/iSMvol/ directory if you do not specify any directory name. If you specify a directory, the iSMvolgather directory is created under the specified directory. Check that the iSMvolgather.tar.Z file is created under the directory and obtain the file.

Operations when the Configuration is Changed

It is necessary to recreate the volume list to reflect the new configuration information to the volume list when you change the disk array or server (OS) configuration.

Conditions Requiring Volume List Update

Be sure to recreate and update the volume list after changing the following configurations:

Change of disk array configuration

- Change of disk array name
- Change of logical disk name
- Change of logical disk OS type
- Adding of logical disk, and change and deleting of configuration
- Change of Access Control setting
- Adding and deleting of disk array connected by Remote Replication

If the disk array configures Remote Replication and the above configurations are changed in the remote-side disk array, be sure to update the volume list as well.

Change of Server Configuration

- Adding, deleting and change of control volume definition
- Change of connection configuration (path) between the disk array and server

Updating Volume List

To update a volume list, execute the iSMvollist command with the -r option specified. Update a volume list with the appropriate user privilege.

When updating a volume list, note the following points so that the information to be registered in the volume list including the logical disk and volume information already registered is complete.

Update a volume list in the following states.

- The path between the disk array and the server is normally connected.
- The logical disk in the disk array is recognized as a server (OS) disk device.
- The volume in the disk is recognized by the server (OS).

When you add, delete, or change the control volume definition in the disk array with which the control volume attribute cannot be identified, execute the following operation before updating a volume list.

- Define the logical disk to be used as the control volume in advance in the control volume definition file.

To successfully register volume information in the volume list, update a volume list in the following states.

- Pairs are separated when the RV in the data replication function is connected to the server.
- The link-volume (LV) and snapshot-volume (SV) are linked when the LV in the snapshot function is connected to the server. The base-volume (BV) and LV are not linked when the BV is connected to the server.
- Protected data is readable when the logical disk for which the WORM function is applied is connected to the server.
- The volume is in the In use state and accessible when the logical disk for which the power saving function is applied is connected to the server.
- The link path between disk arrays is normal when the Remote Replication is configured for the disk array.

After updating the volume list, display the information registered in the volume list to check that the items to be used such as logical disks and special file names are all registered.

If the script or the like used for operation describes the logical disks, special file names, and other information to be operated, reflect the updated information in the volume list to the script or the like.

The ProtectControl command execution may abnormally end in the future operation if the information in the volume list contains an error or if the volume list information is inconsistent with the script or others used for operation.

Chapter 9

Notes (Linux)

Linux Systems

This chapter contains notes regarding management and operations of WORM function.

- The file system type below is supported for WORM function.
  - ext2
- The number of volumes to allocate to servers, including those volumes for date retention, must be no larger than the maximum LUN that can be recognized by the OS.
- A volume for WORM cannot be allocated to LUN0. Allocate to LUN0 a normal volume that is not used by WORM function.
- Volume management software such as LVM and VxVM cannot be used for volumes of WORM.
- If an incorrect protection setting for an unintended volume prevents you from releasing protection from the volume, consult your maintenance engineer.
- If a server using a volume is restarted in the state where the protection state of the volume is set to NotAccessible by WORM operation, the volume is not recognized by the OS. To make the OS recognize the volume, release volume protection, and then restart the server.
- To register in a volume list a logical disk to be used, a special file in the /dev/sd# format for the logical disk must already be created. Before creating or updating a volume list, you must use the /dev/MAKEDEV or mknod command to create all special files for logical disks you want to use.
- When you specify the value of a special file name in a command option, the value must be in the /dev/sd# format. The special file name is displayed in the /dev/sd# format.
- The LUN settings assigned to logical disks must be sequential values starting at 0. The system can recognize only a range of logical disks with sequential LUN values starting at 0; the first logical disk to have a non-sequential LUN value and subsequent logical disks are not recognized.
- To add or delete disk arrays, the system must be restarted.
- If an attempt is made to access a volume with the protection state of ReadOnly or NotAccessible, a message indicating an SCSI error (refer to <Message example> below) may be recorded in syslog. If you execute a command, such as fsck, that tries to access all volumes in a server, a message similar to the example below may be recorded for every volume in the server with the protection state of ReadOnly or NotAccessible.

<Message example>

```
Dec 10 14:48:14 sv001 kernel: sd 4:0:1:1: SCSI error : return code =
0x08000002
Dec 10 14:48:14 sv001 kernel: sde: Current sense key : Data Protect
Dec 10 14:48:14 sv001 kernel: <<vendor>> ASC=0xf4 ASCQ=0xb ASC=0xf4
ASCQ=0xb
Dec 10 14:48:14 sv001 kernel: Info fld=0x0
Dec 10 14:48:14 sv001 kernel: end_request: I/O error, dev sde, sector 0
```

In an environment that has PathManager installed, if such a message is recorded, the PathManager path to the volume may be broken, preventing the volume from being accessed.

Release protection to make the volume read/write-enabled, and then recover the broken path using the recoverpath command of PathManager. If the path to a volume with the protection state of ReadOnly is broken, recovery is automatically performed by path monitoring of PathManager after a fixed time period (monitoring interval). For details of PathManager, refer to the PathManager User's Manual (Linux).

In an environment that does not have PathManager installed, there is no operational problem even if a message similar to the above example is recorded.

- When you protect MV or RV of the data replication function, the volume must have been separated. When you perform Separate (immediate) of the replication function, the RV becomes available (available for read or write) but cannot be protected because the data has not been established. Wait until Separate is completed.
- A target volume for WORM cannot be used as a shared disk for a cluster.

Index