HITACHI
Inspire the Next

Hitachi Universal Storage Platform V
Hitachi Universal Storage Platform VM
Hitachi Volume Security User's Guide

FastFind Links

Hitachi Data Systems

MK-96RD628-04

Contents

Preface

This document describes and provides instructions for configuring and performing Hitachi Volume Security operations on the Hitachi Universal Storage Platform V (USP V) and Hitachi Universal Storage Platform VM (USP VM) storage system.

Please read this document carefully to understand how to use this product, and maintain a copy for reference purposes.

This preface includes the following information:

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

Intended Audience

This document is intended for system administrators, Hitachi Data Systems representatives, and Authorized Service Providers who are involved in installing, configuring, and operating the Hitachi Universal Storage Platform V and Hitachi Universal Storage Platform VM storage system.

This document assumes the following:

- The user has a background in data processing and understands RAID storage systems and their basic functions.
- The user is familiar with the Hitachi Universal Storage Platform V and Hitachi Universal Storage Platform VM storage systems and has read the *Universal Storage Platform V and Universal Storage Platform VM User and Reference Guide*.
- The user is familiar with the Storage Navigator software for the Universal Storage Platform V and Universal Storage Platform VM and has read the *Storage Navigator User's Guide*.

Product Version

This document revision applies to Universal Storage Platform V/VM microcode 60-04-0*x* and higher.

Document Revision Level

Revision	Date	Description
MK-96RD628-P	February 2007	Preliminary Release
MK-96RD628-00	April 2007	Initial Release, supersedes and replaces MK-96RD628-P
MK-96RD628-01	May 2007	Revision 1, supersedes and replaces MK-96RD628-00
MK-96RD628-02	July 2007	Revision 2, supersedes and replaces MK-96RD628-01
MK-96RD628-03	May 2008	Revision 3, supersedes and replaces MK-96RD628-02
MK-96RD628-04	November 2008	Revision 4, supersedes and replaces MK-96RD628-03

Source Documents for this Revision

- MK-96RD628-04d.doc

Changes in this Revision

- Converted GUI text to tables (see Chapter 3).
- Updated the Volume Security Window (see Figure 3-1).
- Added information about the Select Port Dialog box (see Select Port Dialog box).
- Added information about using the Host Group to Port dialog box (see Host Group to Port dialog box).

Document Organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Overview of Volume Security	Gives an overview of Hitachi Volume Security.
About Volume Security Operations	Provides an overview of Volume Security operations.
Using the Volume Security GUI	Describes the Volume Security window.
Performing Volume Security Operations	Provides instructions for performing Volume Security operations.
Troubleshooting	Provides troubleshooting information and instructions for calling technical support.
Acronyms and Abbreviations	Defines the acronyms and abbreviations used in this document.
Index	Lists the topics in this document in alphabetical order.

Referenced Documents

Hitachi Universal Storage Platform V/VM:

- *User and Reference Guide*, MK-96RD635
- *Storage Navigator User's Guide*, MK-96RD621
- *ShadowImage™ for IBM® z/OS® User's Guide*, MK-96RD619
- *TrueCopy® for IBM® z/OS® User's Guide*, MK-96RD623

Document Conventions

The terms "Universal Storage Platform V" and "USP V" refer to all models of the Hitachi Universal Storage Platform V, unless otherwise noted.

The terms "Universal Storage Platform VM" and "USP VM" refer to all models of the Hitachi Universal Storage Platform VM, unless otherwise noted.

This document uses the following typographic conventions:

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

This document uses the following icons to draw attention to information:

Icon	Meaning	Description
	Note	Calls attention to important and/or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (e.g., disruptive operations).
	WARNING	Warns the user of severe conditions and/or consequences (e.g., destructive operations).

Convention for Storage Capacity Values

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

1 KB (kilobyte) = 1,000 bytes
1 MB (megabyte) = $1,000^2$ bytes
1 GB (gigabyte) = $1,000^3$ bytes
1 TB (terabyte) = $1,000^4$ bytes
1 PB (petabyte) = $1,000^5$ bytes

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

1 KB (kilobyte) = 1,024 ($2^{10)}$ bytes
1 MB (megabyte) = 1,024 KB or $1,024^2$ bytes
1 GB (gigabyte) = 1,024 MB or $1,024^3$ bytes
1 TB (terabyte) = 1,024 GB or $1,024^4$ bytes
1 PB (petabyte) = 1,024 TB or $1,024^5$ bytes

Getting Help

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The content of any error message(s) displayed on the host system(s).
- The content of any error message(s) displayed on Storage Navigator.
- The Storage Navigator configuration information (use the FD Dump Tool).
- The service information messages (SIMs), including reference codes and severity levels, displayed by Storage Navigator.

The Hitachi Data Systems customer support staff is available 24 hours/day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Comments

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

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

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

1

Overview of Hitachi Volume Security

This chapter gives an overview of Hitachi Volume Security.

Overview of Volume Security

Hitachi Volume Security protects data in your Hitachi Universal Storage Platform V and Hitachi Universal Storage Platform VM (hereinafter referred to as USP V/VM) from I/O operations performed at mainframe hosts. Security can be applied to logical volumes so that specified mainframe hosts are unable to read from and write to the specified logical volumes. Hitachi Volume Security also enables you to prevent data on logical volumes from being accidentally overwritten by erroneous local or remote copy operations.

Hitachi Volume Security can be used in conjunction with the Volume Security Port Option. This optional program is used to specify USP V/VM ports through which hosts can access logical volumes.

Using Hitachi Volume Security you can manipulate up to 64 hosts and 65,280 logical volumes for one USP V/VM. Volume Security also enables you to create up to 64 security groups, 64 host groups, and 64 volume groups for one USP V/VM.

Volume Security operations are performed using the licensed Storage Navigator software. The Storage Navigator software communicates directly with the USP V/VM via a local-area network (LAN). Storage Navigator displays detailed Volume Security information and allows you to configure and perform Volume Security operations for the mainframe systems data stored on the USP V/VM. For further details, refer to the *Storage Navigator User's Guide*.

Terminology

Review the following terminology note to enhance your use of this manual:

- In the USP V/VM documentation, logical volumes are sometimes referred to as logical devices (or LDEVs). Also, the USP V/VM documentation sometimes uses the term LDEV security to refer to a security policy that volume security enables you to apply to logical volumes.
- In the *TrueCopy for IBM z/OS User's Guide*, primary volumes are often referred to as M-VOLs, or main volumes. Also, secondary volumes are often referred to as R-VOLs or remote volumes.
- In the *ShadowImage for IBM z/OS User's Guide*, primary volumes are often referred to as S-VOLs, or source volumes. Secondary volumes are often referred to as T-VOLs, or target volumes.

2

About Volume Security Operations

This chapter provides an overview of Volume Security operations.

System Requirements

To be able to use Volume Security, you need:

- The USP V/VM disk subsystem
- A computer that runs Storage Navigator (Storage Navigator computer)
- A license key for the Volume Security program product

To perform Volume Security operations, you must use the Storage Navigator software, which is a Java application, on the Storage Navigator computer. To be able to use Storage Navigator, you must attach your Storage Navigator computer to the disk subsystem via a LAN, and then make appropriate browser settings. If you are able to use Storage Navigator, you must install the Volume Security program product using the license key on the Storage Navigator computer. For details, refer to the *Storage Navigator User's Guide*.

To apply port-level security, you must install the *Volume Security Port Option*. Before installing this program, ensure that Volume Security is already installed. For details on the installation procedure, refer to the *Storage Navigator User's Guide*.

Overview of Volume Security Functions

The Volume Security feature protects data in your disk subsystem from I/O operations performed at mainframe hosts. Volume Security enables you to apply security to volumes so that the specified mainframe hosts will be unable to read from and write to the specified volumes. Volume Security also enables you to prevent data on volumes from being overwritten by erroneous copy operations.

Volume Security can be used in conjunction with an optional program Volume Security Port Option. This optional program can be used to specify disk subsystem ports via which hosts can access volumes.

In the USP V/VM documentation, volumes are sometimes referred to as logical devices (or LDEVs). Also, the USP V/VM documentation sometimes uses the term LDEV security to refer to security policy that Volume Security enables you to apply to volumes.

Protecting Volumes from I/O Operations at Mainframe Hosts

Volume Security enables you to protect volumes from unauthorized accesses by mainframe hosts. To protect volumes from unauthorized accesses, you must create security groups and then register mainframe hosts and/or volumes in security groups. Security groups are classified into access groups or pool groups. If you want to allow some (but not all) mainframe hosts to access volumes, you must classify the security group as an access group. If you want to prohibit all mainframe hosts from access volumes, you must classify the security group as a pool group.

Enabling Only the Specified Hosts to Access Volumes

If you want to allow only some mainframe hosts in your network to access volumes, you must register the mainframe hosts and the volumes in an access group. For example, if you register two hosts (host_A and host_B) and two volumes (vol_C and vol_D) in an access group, only the two hosts will be able to access vol_C and vol_D. No other hosts will able to access vol_C and vol_D.

If mainframe hosts are registered in an access group, the hosts will be able to access volumes in the same access group, but will be unable to access other volumes. For example, if you register two hosts (host_A and host_B) and two volumes (vol_C and vol_D) in an access group, the two hosts can access vol_C and vol_D and cannot access other volumes.

To register hosts in an access group, you must create a host group, register the hosts in the host group, and then register the host group in the desired access group. To register volumes in an access group, you must create an LDEV group, register the volumes in the LDEV group, and then register the LDEV group in the desired access group. Any access group can only contain one host group and one LDEV group.

In Figure 2-1, six mainframe hosts are attached to a disk subsystem and two access groups are created. At this point, the following security settings are applied:

- The volumes ldev1 and ldev2 are accessible only from host1, host2, and host3 because the two volumes and the three hosts are registered in the same access group.
- The volume ldev4 is accessible only from host4 because ldev4 and host4 are registered in the same access group.
- The volume ldev5 does not belong to any access groups. For this reason, hosts in access groups cannot access ldev5. ldev5 is only accessible from host5 and host6, which are not registered in access groups.

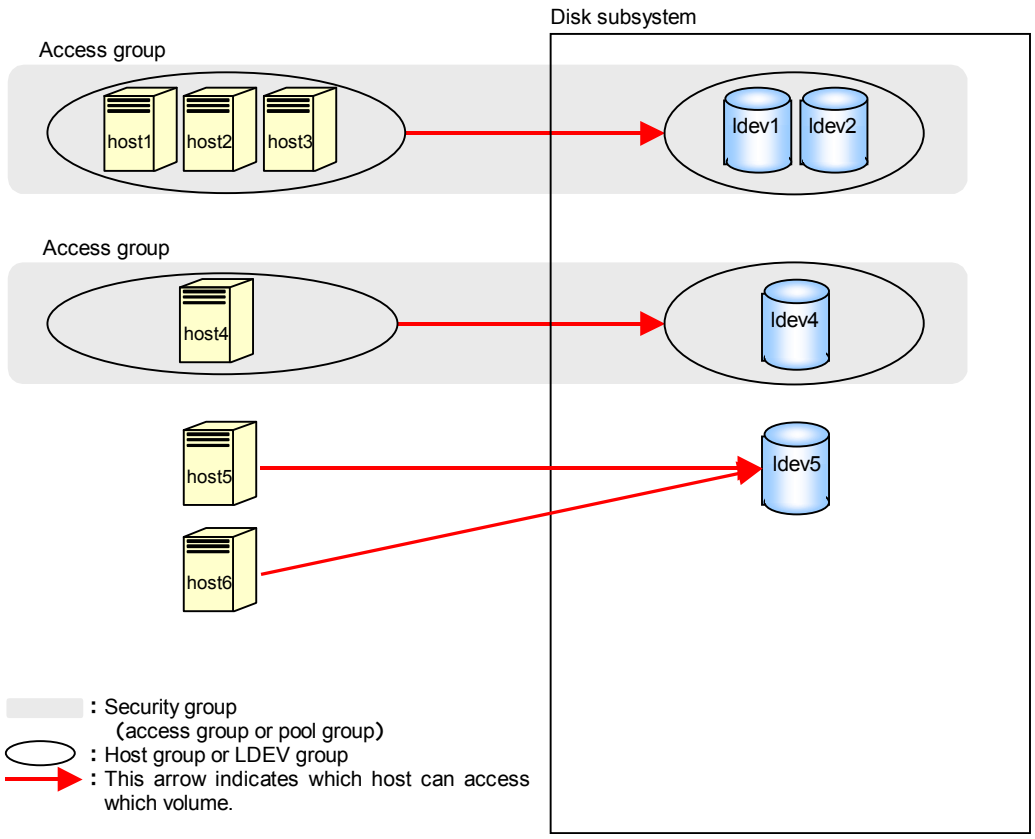


Figure 2-1 Security Example 1

Port-Level Security

Usually, hosts are connected to two or more ports via cables and have access to volumes via these ports. In the security example in Figure 2-1, hosts in access groups can access volumes via every port to which the hosts are connected.

Note, however, that Volume Security Port Option enables you to prohibit hosts from accessing volumes via specified ports. For example, if a host named **host1** is connected to two ports **port1** and **port2**, you can permit the host to access volumes via **port1** and prohibit the host from accessing volumes via **port2**.

Port-Level Security Implementation

To implement such port-level security, first you must determine ports via which hosts can access volumes, and then you must register the ports in host groups. For example, if you register **host1** and **port1** in the same host group named **hg1** and then register **hg1** in an access group, **host1** can access volume via **port1** but cannot access volumes via **port2**.

In Figure 2-2, the following security settings are applied:

- The hosts host1, host2, and host3 can access the volumes ldev1 and ldev2 via port1, port2, and port3. However, the hosts cannot access the volumes via other ports.
- The host host4 can access the volume ldev4 via port4. However, the host cannot access the volume via other ports.

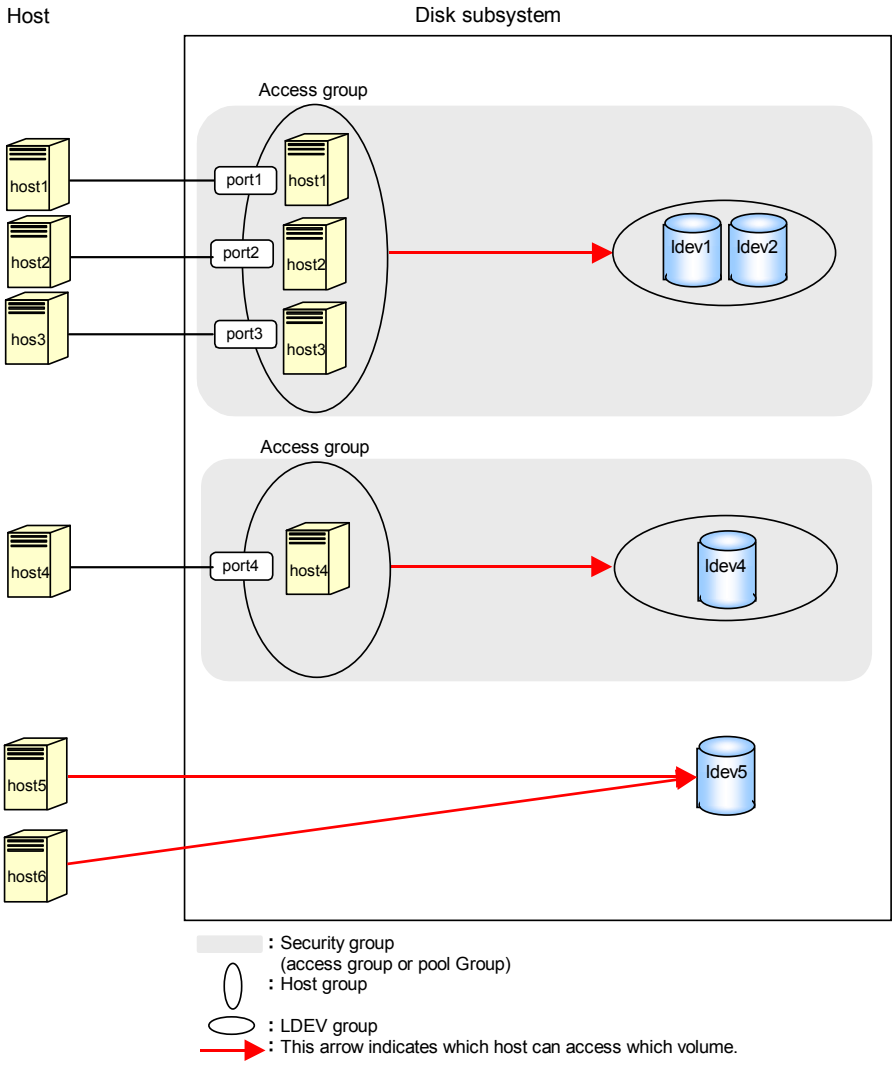


Figure 2-2 Security Example 2

If no ports are registered in a host group, hosts in the host group can access volumes via ports to which the hosts are connected.

This manual uses the term **port-level security**, which is a security policy for enabling hosts to access volumes only via ports registered in host groups and thus prohibiting hosts to access the volumes via other ports.

Caution: Before applying security, you must confirm which hosts are performing I/O operations on which volumes in the access groups. If any hosts are performing I/O operations on volumes in access groups to which the hosts do not belong, you must stop the I/O operations before applying security. For example, if you attempt to apply security settings illustrated in Figure 2-2, an error occurs and the attempt fails if host4 and host5 are performing I/O operations on ldev1. To be able to apply the security settings, ensure that host4 and host5 are not performing I/O operations on ldev1.

Prohibiting All Hosts from Accessing Volumes

If you want to prevent all the mainframe hosts from accessing volumes, you must register the volumes in a pool group (Note that you do not need to register hosts in pool groups). For example, if you register two volumes (vol_A and vol_B) in a pool group, all the mainframe hosts connected to your disk subsystem will be unable to access vol_A and vol_B. To register volumes in a pool group, you must create an LDEV group, register the volumes in the LDEV group, and then register the LDEV group in the desired pool group. Any pool group can only contain one LDEV group.

In Figure 2-3, a pool group is created. Volumes in this pool group (i.e., ldev7, ldev8, and ldev9) are inaccessible from all the hosts:

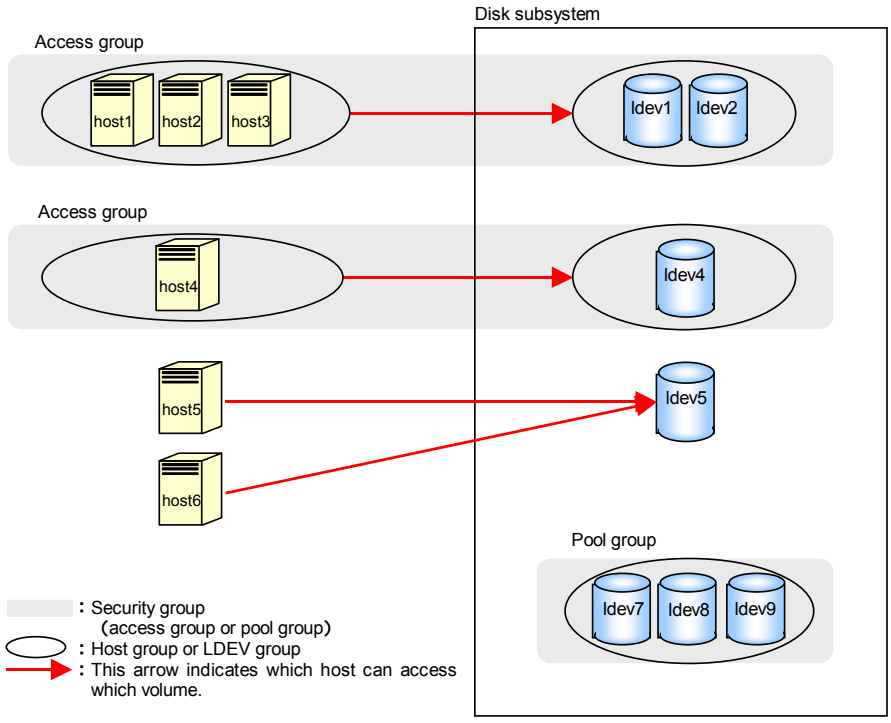


Figure 2-3 Security Example 3

Protecting Volumes from Erroneous Copy Operations

When USP V/VM copy software (TrueCopy for z/OS® (TCz), Universal Replicator for z/OS®, ShadowImage for z/OS® (SIz), and Compatible FlashCopy® or Compatible FlashCopy® V2) is used to perform copy operations, data is overwritten onto the secondary volumes (i.e., the copy destination volumes). If a volume containing important data is specified as a secondary volume (i.e., the copy destination volume) by mistake, USP V/VM copy software operations can overwrite important data on the volume and you could suffer loss of important data.

Volume Security enables you to avoid such loss of data. If a volume contains data that must not be overwritten, you can prevent the volume from being used as a secondary volume (i.e., the copy destination volume).

Secondary volumes (i.e., copy destination volumes) are often referred to as remote volumes or R-VOLs in the *TrueCopy for IBM z/OS User's Guide*. Also, secondary volumes are referred to as target volumes or T-VOLs in the *ShadowImage for IBM z/OS User's Guide*.

Warnings Regarding Volume Security

WARNINGS:

There are three primary warnings for applying Volume Security:

1: Do not apply security to volumes on which any job is running. If you apply security to such a volume, the job may end abnormally.

2: When applying security, make sure that your security settings are correct. If incorrect security settings are made, the system will be difficult or impossible to control.

3: If the CPU of a mainframe host is upgraded after you apply security settings, you must execute the system command "D M=CPU" at the mainframe host to obtain the latest information about the host. Next, you must use the latest information to update host information in the Add/Change Host dialog box. If you do not update host information, the system will be impossible to control.

- **If you are using USP V/VM copy software (TrueCopy for z/OS (TCz), Universal Replicator for z/OS, ShadowImage for z/OS (SIz), and Compatible FlashCopy or Compatible FlashCopy V2):** When you use Volume Security to make security settings, you must register the primary volume and the secondary volume (i.e., the copy source volume and the copy destination volume) in the same LDEV group. For details on how to register volumes in LDEV groups, see Registering Volumes in an LDEV Group.

  If you apply security to a primary volume (i.e., copy source volume) of a pair of USP V/VM copy software, some or all mainframe hosts might become unable to read from and write to the primary volume. However, the copy operation will be performed normally; data will be copied from the primary volume to the secondary volume.

  If you register a primary volume or secondary volume in a security group and then make a setting for preventing the volume from being used as a secondary volume, this setting will take effect after the pair is split.

  Mainframe hosts cannot access volumes in pool groups. If a volume in a pool group is specified as a primary volume, the pair creation command might fail.

  In the *TrueCopy for IBM z/OS User's Guide*, primary volumes (i.e., copy source volumes) are often referred to as M-VOLs or main volumes. Also, secondary volumes (i.e., copy destination volumes) are often referred to as R-VOLs or remote volumes.

  In the *ShadowImage for IBM z/OS User's Guide*, primary volumes (i.e., copy source volumes) are often referred to as S-VOLs or source volumes. Also, secondary volumes (i.e., copy destination volumes) are often referred to as T-VOLs or target volumes.

- **If you are using Virtual LVI/LUN (VLL) volumes:** If you apply security to a VLL volume, you will be unable to change the VLL settings on the volume. If you want to change the VLL settings, you must use Volume Security to disable security on the VLL volume.
- **If you are using Compatible PAV:** If you apply security to a Compatible PAV base volume, the security settings will also apply to the corresponding alias volume.
- **Removing secured volumes:** If you apply security to a volume, you will be unable to remove the volume. If you want to remove the volume, you must disable security on the volume.
- **Removing PCBs with secured ports:** If port-level security is applied to your disk subsystem, you cannot remove the PCBs (printed circuit boards) that include secured ports. If you want to remove PCBs that include secured ports, you must use Volume Security Port Option to disable security on the ports.

Supported Volume Emulation Types

Table 2-1 lists the emulation types that Volume Security supports.

Table 2-1 Supported Volume Emulation Types

Supported Volume Emulation Types	Description
3390-3, -3R, -9, -L, -M 3380-3 *	These logical volumes can be used only by mainframe hosts.
3390-3A, 3390-3B, 3390-3C 3390-9A, 3390-9B, 3390-9C 3390-LA, 3390-LB, 3390-LC 3390-MA, 3390-MB, 3390-MC 3380-3A, 3380-3B, 3380-3C *	These logical volumes can be used by mainframe hosts and open-systems hosts. ***Notes:*** ▪ You must ensure that the access attribute of these logical volumes is *Read/Write*. ▪ Access attributes only take effect when mainframe hosts access logical volumes. Access attributes does not take effect when open-system hosts access logical volumes.

* Use of 3380 LVIs is restricted to Fujitsu OS environments.

Maximum Number of Groups

Volume Security enables you to create up to 128 security groups per disk subsystem, and up to 64 security groups per Logical DKC (LDKC). Security groups are classified into access groups and pool groups:

- One access group can contain only one host group and one LDEV group. One host group can contain up to 32 hosts. One LDEV group can contain up to 65,280 volumes.
- One pool group can contain only one LDEV group. One LDEV group can contain up to 65,280 volumes.

The maximum number of host groups is 128 per disk subsystem, and 64 per LDKC.

The maximum number of LDEV groups is 128 per disk subsystem, and 64 per LDKC.

Maximum Number of Hosts and Volumes

Volume Security allows you to manipulate up to 128 hosts for disk subsystem, and up to 64 hosts per LDKC. Volume Security enables you to manipulate up to 130,560 volumes per disk subsystem, and up to 65,280 volumes per LDKC.

3

Using the Volume Security GUI

This chapter describes the various *elements* of the Volume Security window graphical user interface (GUI) and its associated dialog boxes.

This chapter describes only the Volume Security GUI and dialog boxes. For general information on the Storage Navigator features, see the *Storage Navigator User's Guide*.

Volume Security Window

The Volume Security window opens when you start Volume Security and is the starting point for all the Volume Security operations. The Volume Security window displays all the security information for the connected USP V/VM storage system and provides access to all volume security operations. To use Volume Security, the Volume Security Port Option must already be installed.

To start the Volume Security software:

1. Log on to the SVP to open the Storage Navigator main window. For details, refer to *Storage Navigator User's Guide*.
2. Click **Go**, **Mainframe Connection**, and then **Volume Security** on the menu bar of the Storage Navigator main window.

Two operational guidelines:

- To make security settings and apply the settings, you must use a user account that has the write permission (For example, the Administrator account). If you use a user account that does not have the write permission, you will be able to view security settings but will neither be able to make security settings nor apply security settings.
- To set security using Volume Security, you must make sure that Storage Navigator is in Modify mode. For detailed information on how to do this, please refer to *Storage Navigator User's Guide*.

Figure 3-1 shows the Volume Security window when a Security Group belonging to an LDKC is selected.

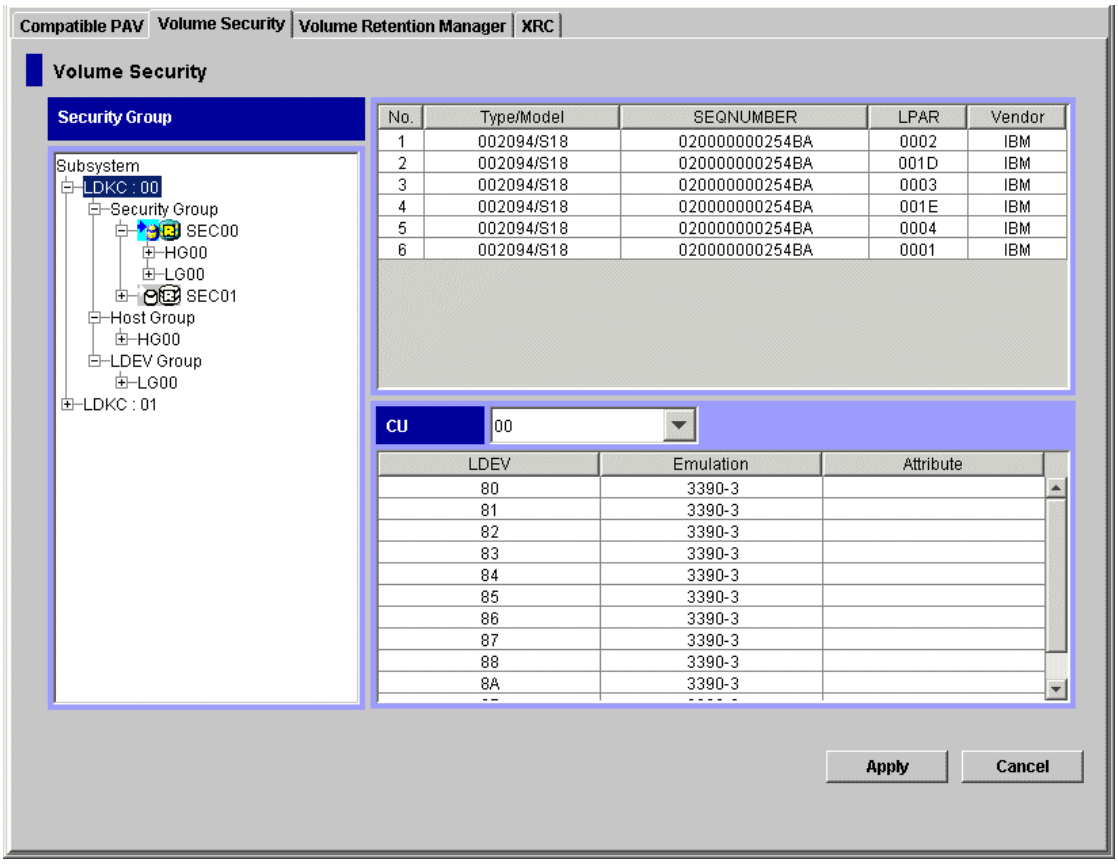


Figure 3-1 Volume Security Window

Item	Description
Security Group tree	Displays the security, host, and LDEV groups assigned to each LDKC defined on the storage subsystem. For details see Security Group Tree.
Hosts table	Displays the type, model, SEQNUMBER, Logical Partition (LPAR) and vendor of each host. For details, see Hosts Table.
CU list	Allows you to select the desired command unit(s) available in each group. When you select a CU image, the table below shows a list of volumes in the selected CU image
LDEVs table	Shows the LDEV, emulation, and attribute information assigned to each logical device on the storage subsystem. For details, see LDEVs Table.
Apply	Applies the requested XRC setting changes to the storage system. Any change made to a volume appears in blue italics until you click **Apply**.
Cancel	Discards the requested changes without applying them to the storage system. A confirmation message appears to allow you to cancel the requested operation(s). Click **OK** on the confirmation message to cancel the requested operation(s), or click **Cancel** to keep (but not start) the requested operation(s).

Security Group Tree

Figure 3-2 shows the Security Group tree where you can select the LDKC (logical disk controller), and then choose a security group, host group, or LDEV group residing on that LDKC.

When you double-click **LDKC:00** or **LDKC:01**, you can display a list of security groups, host groups, and LDEV groups in that LDKC. Once you have selected the LDCK you can choose from these options:

- Double-click **Security Group** and a list of security groups appears. Then select a host group or LDEV group in that security group.
- Double-click **Host Group** and a list of host groups appears. Then select a specific host group.
- Double-click **LDEV Group** The tree view shows the host group and/or LDEV group registered in the security group.

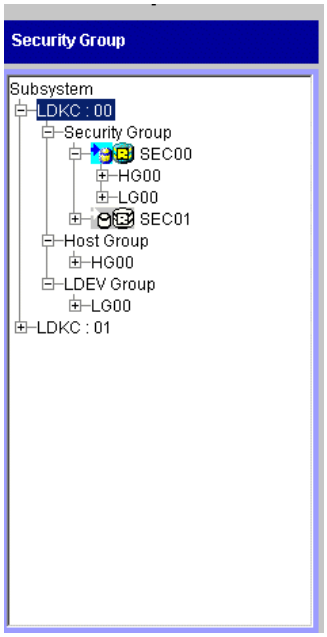


Figure 3-2 Security Group tree

Icon	Description
	Indicates an access group whose volumes can be used as secondary volumes (i.e., copy destination volumes) for copy operations.
	Indicates an access group whose volumes cannot be used as secondary volumes (i.e., copy destination volumes) for copy operations.
	Indicates a pool group whose volumes can be used as secondary volumes (i.e., copy destination volumes) for copy operations.
	Indicates a pool group whose volumes cannot be used as secondary volumes (i.e., copy destination volumes) for copy operations.

	Indicates that the security settings in this security group are currently disabled. If you enable the security settings, this security group is classified as an access group. Also, volumes in this security group can be used as secondary volumes (i.e., copy destination volumes) for copy operations.
	Indicates that the security settings in this security group are currently disabled. If you enable the security settings, this security group will be classified as an access group. Also, volumes in this security group are unavailable for use as secondary volumes (i.e., copy destination volumes) for copy operations.
	Indicates that the security settings in this security group are currently disabled. If you enable the security settings, this security group will be classified as a pool group. Also, volumes in this security group will be available for use as secondary volumes (i.e., copy destination volumes) for copy operations.
	Indicates that the security settings in this security group are currently disabled. If you enable the security settings, this security group will be classified as a pool group. Also, volumes in this security group will be unavailable for use as secondary volumes (i.e., copy destination volumes) for copy operations.

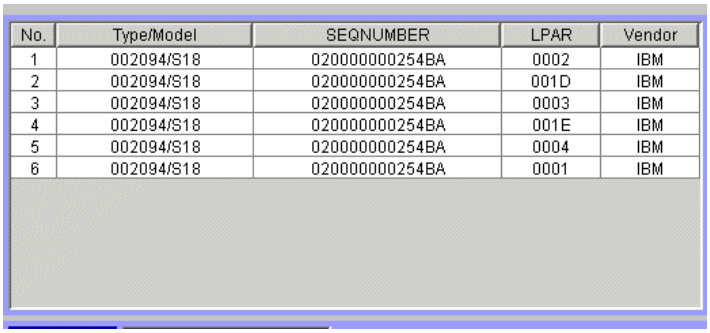
To make changes to a group, right-click a group or the group entry in the tree, then select **Add/Change** from the pop-up menu. Changes you make in the resulting dialog box appear in blue italics until you click **Apply** or **Cancel**.

Note: If you make Volume Security settings on one LDKC and then move on to another LDKC, click **Apply** or **Cancel** before moving on to the LDKC.

Hosts Table

This table provides information about hosts. The table contents depend on the selection in the **Security Group** tree, as explained below:

- If you select **Subsystem**, **LDKC:00**, **LDKC:01, Security Group**, **Host Group**, or **LDEV Group**, the table shows information about all the hosts.
- If you select a security group, the table shows information about all the hosts that belong to the selected security group.
- If you select a host group, the table shows information about all the hosts that belong to the selected host group.
- If you select an LDEV group, the table displays nothing.



No.	Type/Model	SEQNUMBER	LPAR	Vendor
1	002094/S18	020000000254BA	0002	IBM
2	002094/S18	020000000254BA	001D	IBM
3	002094/S18	020000000254BA	0003	IBM
4	002094/S18	020000000254BA	001E	IBM
5	002094/S18	020000000254BA	0004	IBM
6	002094/S18	020000000254BA	0001	IBM

Figure 3-3 Hosts Table

Column	Description
No.	A sequential number associated with a host (or channel extender).
Type/Model	Type and model number of a host (or a channel extender).
SEQNUMBER	Node ID of a host (or a channel extender).
LPAR	The logical partition number of a host.
Vendor	The host vendor. Vendors include **FJT** (Fujitsu), **IBM**, **HTC** (Hitachi), and **CNT(Ex)**. If **CNT(Ex)** appears, the table row indicates the type, model number, and node ID of a channel extender.

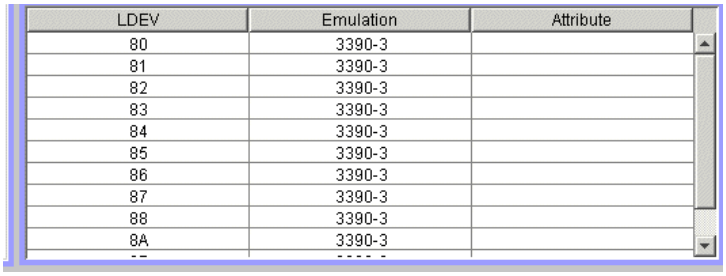
If you make any change to a host, the host appears in blue italics. When you click **Apply** or **Cancel**, the host is restored to its original typeface and color.

The Basic Information Display dialog boxes in Storage Navigator also show information about hosts. For details, refer to the *Storage Navigator User's Guide*.

LDEVs Table

The LDEVs table (Figure 3-4) provides information about volumes. The information available depends on the selection in the Security Group tree:

- If you select **Subsystem**, **Security Group**, **Host Group**, or **LDEV Group**, the table provides information about all the volumes that are accessible from the mainframe hosts.
- If you select a security group, the table provides information about all the volumes that belong to the selected security group.
- If you select an LDEV group, the table provides information about all the volumes that belong to the selected LDEV group.
- If you select a host group, the table displays nothing.



LDEV	Emulation	Attribute
80	3390-3	
81	3390-3	
82	3390-3	
83	3390-3	
84	3390-3	
85	3390-3	
86	3390-3	
87	3390-3	
88	3390-3	
8A	3390-3	

Figure 3-4 LDEVs Table

Column	Description
LDEV	The volume ID (in hexadecimal from 00 to FF) ***Note:*** A volume ID ending in # (for example, 00#) indicates , the volume is an external volume.
Emulation	The emulation type of the volume
Attribute	The volume status: ▪ An asterisk (*) denotes a secondary volume (copy destination) for USP V/VM copy software. ▪ A plus symbol (+) denotes that one or more LU paths are assigned to the volume.

Add/Change Security Group Dialog Box

The Add/Change Security Group dialog box (see Figure 3-5) opens when you right-click a security group or the **Security Group** entry in the tree view of the Volume Security window, and then select **Add/Change** from the pop-up menu. Use this dialog box to:

- Create a security group and classify the security group as an access group or a pool group
- Prevent data in volumes from being overwritten by copy operations
- Disable security settings
- Rename security groups
- Delete security groups

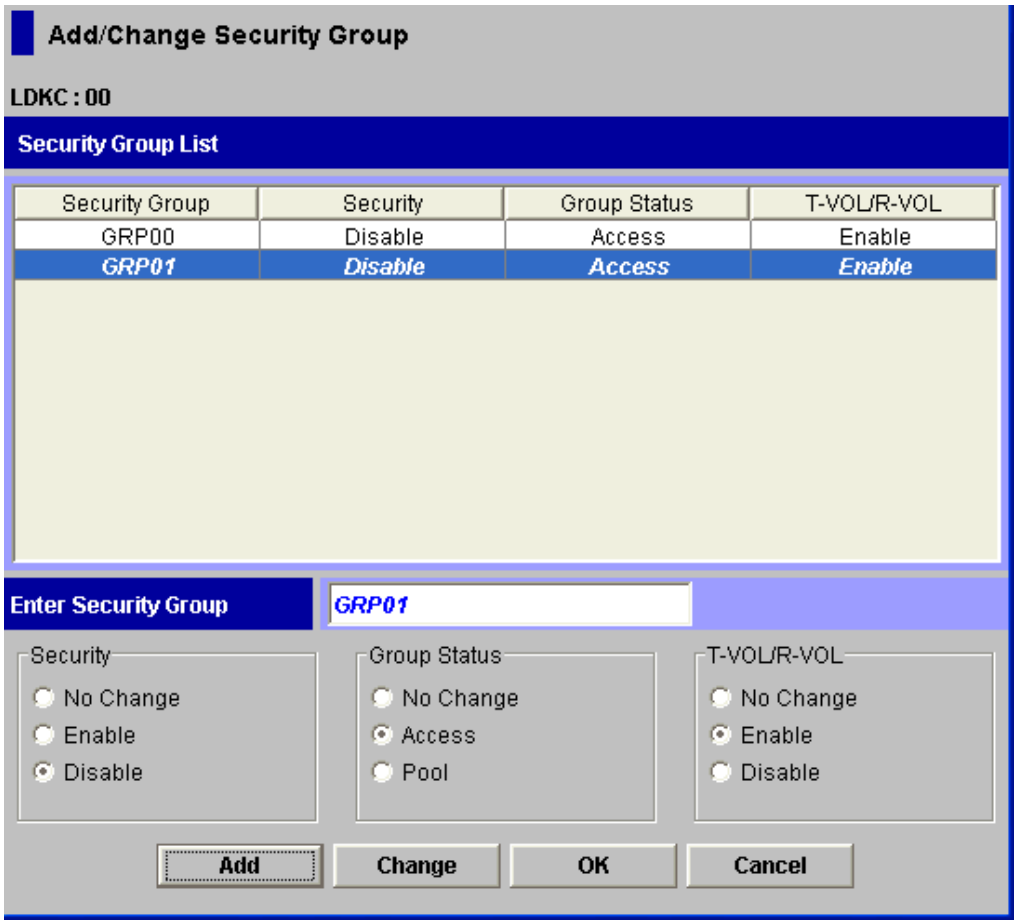


Figure 3-5 Add/Change Security Group Dialog Box

Item	Description
LDKC	Indicates the selected LDKC number.
Security Group List table	Descriptive information about the security groups in the LDKC. ▪ **Security** indicates whether the security settings in the security group are Enabled or Disabled. ***Caution:*** It is possible that security settings are disabled even if **Enabled** is displayed. If the **Status** is **Access** and the security group contains neither a host nor an LDEV group, security settings in the security group are disabled unconditionally. ▪ **Group Status** indicates whether the security group is an Access or a Pool group. If **Access** appears, the security group is an access group; volumes in the group can be accessed only by hosts registered in the same group. If **Pool** appears, the security group is a pool group; volumes in the group cannot be accessed by any hosts. ▪ **T-VOL/R-VOL** indicates whether volumes in the security group can be used as secondary volumes (i.e., copy destination volume). **Enable** indicates the volumes can be used as secondary volumes. **Disable** indicates the volumes cannot be used as secondary volumes. ***Note***: Secondary volumes (i.e., copy destination volumes) are often referred to as remote volumes or R-VOLs in the *TrueCopy for IBM z/OS User's Guide*. Also, secondary volumes are referred to as target volumes or T-VOLs in the *ShadowImage for IBM z/OS User's Guide*.
Enter Security Group	When creating a new security group, enter the name of the security group. When renaming an existing security group, select the security group in the **Security Group List** table and then enter a new name. The following conventions apply to security group names: ▪ Up to eight characters can be used ▪ Characters are case-sensitive ▪ The following characters cannot be used: \ , / : ; * ? " < > | ▪ The first character and the last character must not be a space.
Security	Select to make no changes, enable, or disable security settings. The default is **Enable**. ▪ **No Change** does not change the security status of the security groups selected in the **Security Group List** table. For example, if you select a security-enabled group and a security-disabled group in the table, **Disable** disables security settings in both groups, but **No Change** does not change the current security status for both groups (the former remains security-enabled and the latter remains security-disabled). ▪ **Enable** enables the security settings that are made in the security groups selected in the **Security Group List** table. ***Caution:*** It is possible that security settings are disabled even if **Enable** is selected. If **Access** is selected in the **Group Status** box (see below) and the security group contains a host group nor an LDEV group, security settings in the security group are disabled unconditionally. ▪ **Disable** disables the security settings that are made in the security groups selected in the **Security Group List** table.

Item	Description
Group Status	Sets a selected security group as access groups or pool groups. The default is **Access**. ▪ **No Change** prevents a change in the group status of the security groups selected in the **Security Group List** table. For example, if you select one access group and one pool group, **Access** changes the two groups into access groups, but **No Change** does not change the two groups (The former remains an access group and the latter remains a pool group). ▪ **Access** specifies the selected security groups as access groups. Volumes in an access group can only be accessed by hosts registered in the same access group but cannot be accessed by other hosts. ▪ **Pool** specifies the selected security groups as pool groups. Volumes in a pool group cannot be accessed by any hosts.
T-VOL/R-VOL	Specifies whether volumes in the security group can be used a secondary volumes (i.e., copy destination volumes). The default is **Enable**. ▪ **No Change** does not change the secondary volume settings of the security groups selected in the **Security Group List** table. For example, if volumes in one of the selected security groups are usable as copy destinations, but volumes in the other security group are unusable, **Enable** makes volumes in both groups usable as destinations. However, **No Change** does not change volumes in both groups (The former remains usable, and the latter remains unusable). ▪ **Enable** makes volumes in the selected security groups usable as secondary volumes (copy destinations). ▪ **Disable** makes volumes in the selected security groups unusable as secondary volumes (copy destinations). ***Note:*** Secondary volumes (i.e., copy destination volumes) are often referred to as *remote volumes* or *R-VOLs* in the *TrueCopy for z/OS User's Guide*. Also, secondary volumes are referred to as *target volumes* or *T-VOLs* in the *ShadowImage for IBM z/OS User's Guide*.
Add	Enter the name of a new security group and click **Add**. Then the new security group is added to the **Security Group List** table.
Change	When settings of the selected security groups are changed, click **Change** to make the changes appear in the **Security Group List** table.
OK	Applies settings in the Add/Change Security Group dialog box to the Volume Security window, and then closes the dialog box. ***Caution:*** **Clicking OK** applies the settings to the Volume Security window, but does *not* apply the settings to the storage subsystem. To apply the security settings to the subsystem, you must continue to click **Apply** in the Volume Security window until they appear in the dialog box.
Cancel	Discards settings in the Add/Change Security Group dialog box and closes the dialog box

Add/Change Host Group Dialog Box

The Add/Change Host Group dialog box opens when you right-click a host group or the **Host Group** entry in the tree view of the Volume Security window and then select **Add/Change** from the pop-up menu. Use this dialog box to:

- Create host groups
- Rename host groups
- Delete host groups

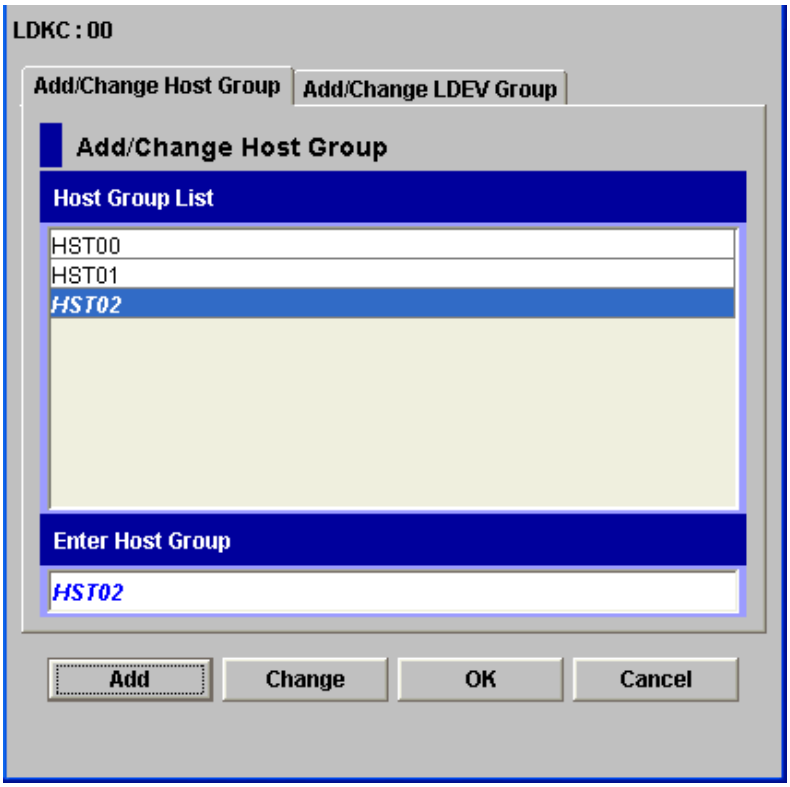


Figure 3-6 Add/Change Host Group Dialog Box

Item	Description
LDKC	Indicates the selected LDKC number.
Host Group List	A list of host groups in the LDKC.
Enter Host Group	When creating a new host group, enter the name of the host group in this text box. When renaming an existing host group, select the host group in the **Host Group List** table and then enter a new name. The following conventions apply to security group names: ▪ Up to eight characters can be used ▪ Characters are case-sensitive ▪ The following characters cannot be used: \ , / : ; * ? " < > | ▪ The first character and the last character must not be a space.
Add	Enter the name of a new host group, click **Add**, and the new security group is added to the **Host Group List** table.
Change	When settings of the selected host groups are changed, click **Change** to make the changes appear in the **Host Group List** table.
OK	Applies settings in the Add/Change Host Group dialog box to the Volume Security window, and then closes the dialog box. ***Caution:*** Clicking **OK** applies the settings to the Volume Security window, but does *not* apply the settings to the storage subsystem. To apply the security settings to the subsystem, you must continue to click **Apply** in the Volume Security window until they appear in the dialog box.
Cancel	Discards settings in the Add/Change Host Group dialog box and closes the dialog box

Add/Change LDEV Group Dialog Box

The Add/Change LDEV Group dialog box opens when you right-click an LDEV group or the **LDEV Group** entry in the tree view of the Volume Security window and then select **Add/Change** from the pop-up menu. Use this dialog box to:

- Create LDEV groups
- Rename LDEV groups
- Delete LDEV groups

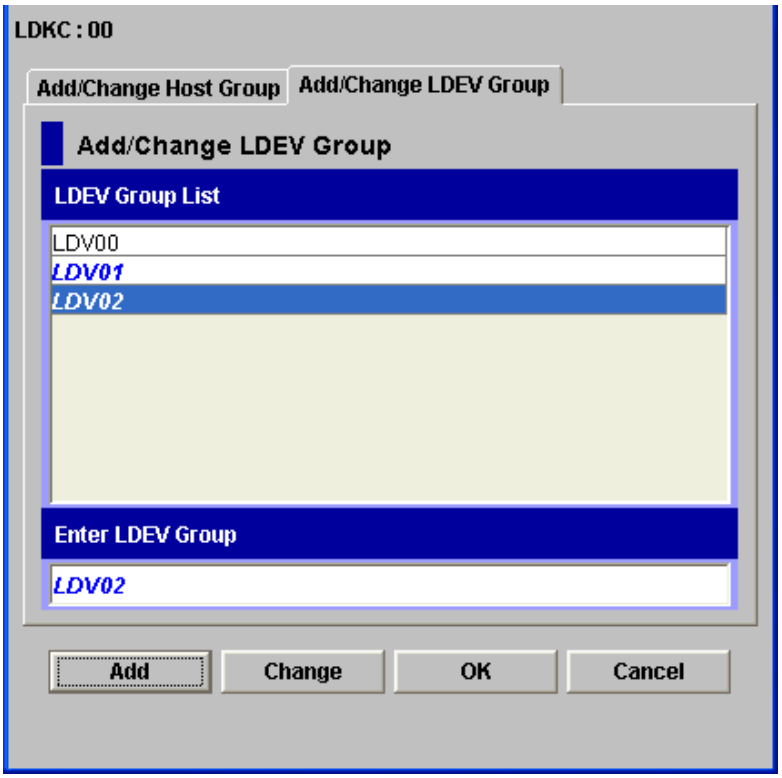


Figure 3-7 Add/Change LDEV Group Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
LDEV Group List	A list of LDEV groups in the LDKC.
Enter LDEV Group	When creating a new LDEV group, enter the name of the LDEV group in this text box. When renaming an existing LDEV group, select the LDEV group in the **LDEV Group List** table and then enter a new name. The following conventions apply to security group names: ▪ Up to eight characters can be used ▪ Characters are case-sensitive ▪ The following characters cannot be used: \ , / : ; * ? " < > | ▪ The first character and the last character must not be a space.
Add	Enter the name of a new LDEV group and click **Add**. Then the new LDEV group is added to the **LDEV Groups List** table.
Change	When settings of the selected LDEV groups are changed, click **Change** to make the changes appear in the **LDEV Groups List** table.
OK	Applies settings in the Add/Change LDEV group dialog box to the Volume Security window, and then closes the dialog box. ***Caution:*** Clicking **OK** applies the settings to the Volume Security window, but does *not* apply the settings to the storage subsystem. To apply the security settings to the subsystem, you must continue to click **Apply** in the Volume Security window until they appear in the dialog box.
Cancel	Discards settings in the Add/Change LDEV Group dialog box and closes the dialog box

Add/Change Host Dialog Box

The Add/Change Host dialog box opens when you right-click a host group in the tree view of the Volume Security window and select **Specify** and then **Host** from the pop-up menu. Use this dialog box to:

- Register hosts attached to the disk subsystem in host groups
- Register hosts unattached to the disk subsystem in host groups
- Delete hosts from host groups

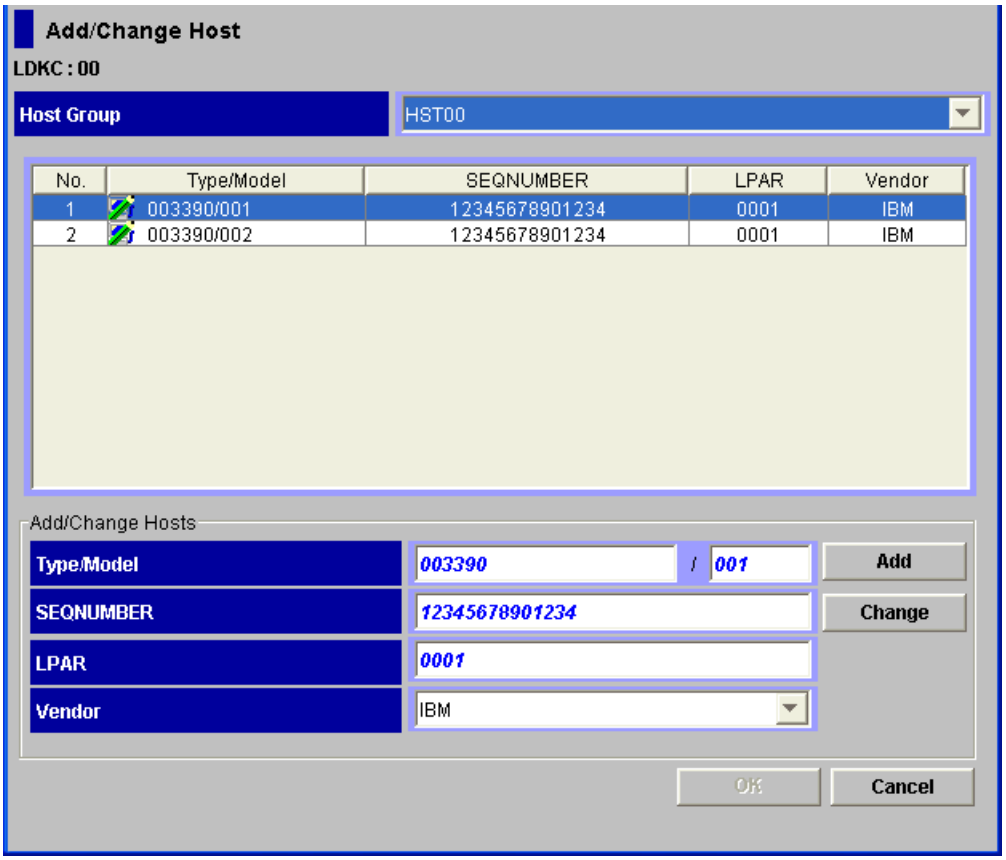


Figure 3-8 Add/Change Host Dialog Box

Item	Description
LDKC	Indicates number of the selected LDKC.
Host Group List	Specify the name of the host group in which hosts will be registered.
Host table	Host information. ▪ **No.** A sequential number associated with a host. ***Note:*** Each table row usually shows information about a host. However, if a host is attached to the disk subsystem via a channel extender, the table row shows information about the channel extender. ▪ **Type/Model** indicates the type and the model number of a host (or a channel extender). The **Type** appears on the left of the slash (/) and the **Model** on the right. An icon indicates the registration status of the host:  The host is registered in the current host group (which is displayed above the table), and is attached to the disk subsystem via a cable.  The host is registered in the current host group, and is *not* attached to the disk subsystem.  The host is registered in another host group (though the host can be registered in the current host group). The host is attached to the disk subsystem via a cable.  The host is registered in another host group (though the host can be registered in the current host group). The host is *not* attached to the disk subsystem. *No icon* The host is *not* registered in any host group. The host is attached to the disk subsystem via a cable. ▪ **SEQNUMBER** indicates the node ID of a host (or a channel extender). ▪ **LPAR** indicates the logical partition number of a host. Logical partitions are virtual systems created by sectioning a computer's memory into separate units. ▪ **Vendor** indicates the vendor of a host. Vendors include **FJT** (Fujitsu), **IBM**, **HTC** (Hitachi), and **CNT(Ex)** for channel extender; if this is the case the **Type/Model** and the **SEQNUMBER** indicates the node ID of the channel extender.
Add/Change Hosts table	Host group information. ▪ **Type/Mode** indicates the type and the model number of a host (or a channel extender). ▪ **SEQNUMBER** indicates the node ID of a host (or a channel extender). ▪ **LPAR** indicates the logical partition number of a host. ▪ **Vendor** indicates the vendor of a host. Vendors include **FJT** (Fujitsu), **IBM**, **HTC** (Hitachi) and **CNT(Ex)** for channel extender.
OK	Applies settings in the Add/Change Host dialog box to the Volume Security window, and then closes the dialog box. ***Caution:*** Clicking **OK** applies the settings to the Volume Security window, but does *not* apply the settings to the storage subsystem. To apply the security settings to the subsystem, you must continue to click **Apply** in the Volume Security window until they appear in the dialog box.
Cancel	Discards settings in the Add/Change Host dialog box and closes the dialog box.

Select LDEV Dialog Box

The Select LDEV dialog box opens when you right-click an LDEV group in the tree view of the Volume Security window, and select **Specify**, and then **LDEV** from the pop-up menu. Use this dialog box to:

- Register volumes (LDEVs) in an LDEV group
- Delete volumes from an LDEV group

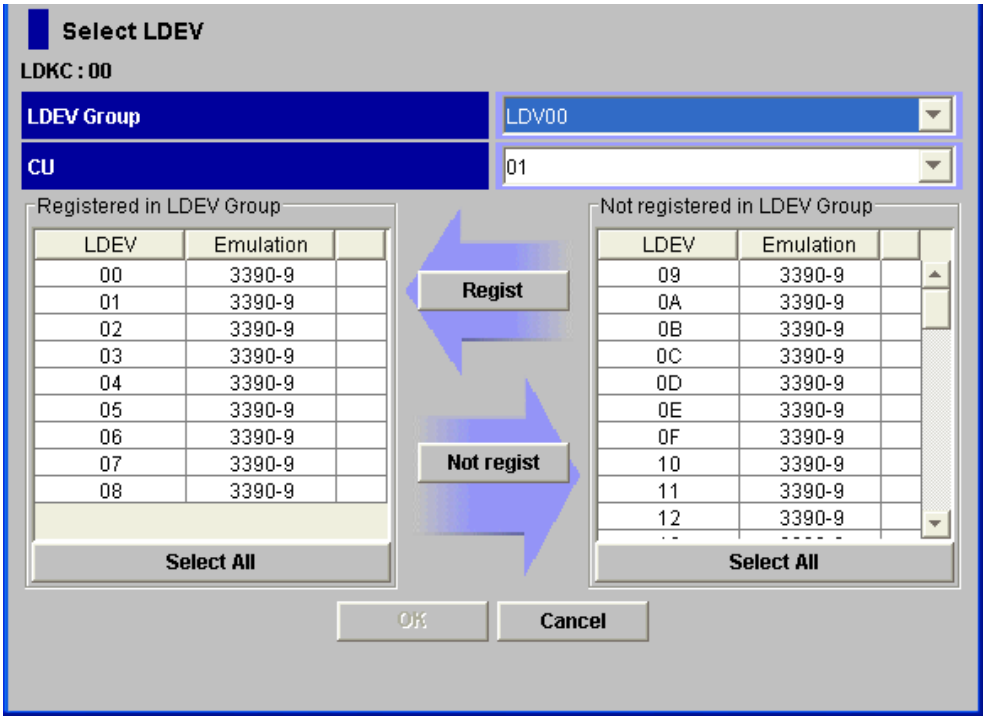


Figure 3-9 Select LDEV Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
LDEV Group	Specifies the name of the LDEV in which the volumes are registered.
CU	Selects the number of the logical CU image. The two tables below this list provide information about the volumes in the selected CU image.
Registered in LDEV Group table	Lists volumes registered in the LDEV groups. One table row indicates one volume. ▪ **LDEV** displays the LDEV numbers. ***Note:*** A volume ID ending in # (for example, 00#) indicates the volume is an external volume. ▪ The **Emulation** column indicates emulation types of volumes. If an asterisk (*) appears in the cell on the right, the volume is a secondary volume (i.e., copy destination volume for copy operations) or a SIz reserved volume. If a plus symbol appears in the cell on the right, one or more LU paths are assigned to the volume. ▪ **Select All** selects all volumes in the table.
Not Registered in LDEV Group table	Lists volumes that not registered in the LDEV groups. One table row indicates one volume. ▪ **LDEV** displays the LDEV numbers. ▪ The **Emulation** column indicates emulation types of volumes. ▪ **Select All** selects all volumes in the table.
Regist	Registers volumes in the LDEV group. Select volumes in **Not Registered in LDEV group** and then click this button to move the selected volumes to **Registered in LDEV group.**
Not Regist	Deletes volumes from the LDEV group. Select volumes in **Registered in LDEV group** and then click this button to move the selected volumes to **Not registered in LDEV group.**
OK	Applies settings in the Select LDEV dialog box to the Volume Security window and closes dialog box. ***Caution:*** Clicking **OK** applies the settings to the Volume Security window, but does *not* apply the settings to the storage subsystem. To apply the security settings to the subsystem, you must continue to click **Apply** in the Volume Security window until they appear in the dialog box.
Cancel	Discards settings in the Select LDEV dialog box and closes the box.

Select Port Dialog Box

To use the Select Port dialog box, the Volume Security Port Option must already be installed.

The Select Port dialog box opens when you right-click a host group in the tree view of the Volume Security window and then select **Specify -> Port** from the pop-up menu. Use this dialog box to register ports in the specified host group.

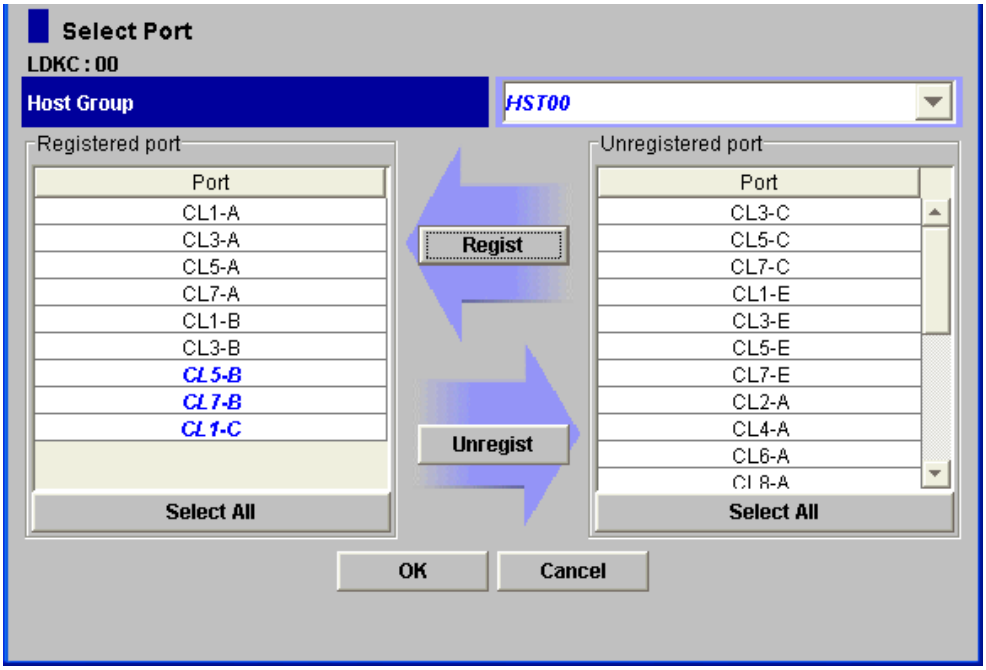


Figure 3-10 Select Port Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
Host Group	Specifies a host group in which ports will be registered.
Registered Port table	Shows the registered ports in the host group: ▪ **LDEV** displays the LDEV numbers. ***Note:*** When the dialog box opens for the first time, the **Port** list does not display ports. This means that hosts in the host group can access volumes via every port displayed in the **Port** list in the **Unregistered port** box. ▪ **Select All** selects all ports in the **Port** list.
Unregistered Port table	Lists ports that not registered. ▪ The **Port** list lists ports that are not registered in the host group. When the dialog box is displayed for the first time, the **Port** list shows all ports on the disk subsystem. ▪ **Select All** selects all ports in the **Port** list.
Regist	Registers ports in the host group. If you select ports in the **Unregistered port** table and then click this button, the selected ports are moved to the Port list under **Registered port.**
Not Regist	Deletes registered ports from the host group. If you select a port in the **Registered port** table and then click this button, the selected port(s) are moved to **Unregistered port** table.
OK	Applies settings in the Select Port dialog box to the Volume Security window, and then closes the Select Port dialog box. ***Caution:*** Clicking **OK** applies the settings to the Volume Security window, but does *not* apply the settings to the storage subsystem. To apply the security settings to the subsystem, you must continue to click **Apply** in the Volume Security window until they appear in the dialog box.
Cancel	Discards settings in the Select Port dialog box, and then closes the dialog box.

Specify Security Group Dialog Box

The Specify Security Group dialog box opens when you right-click an LDKC or a security group in the tree view of the Volume Security window, select **Specify** and then **Security Group** from the pop-up menu. Use this dialog box to register a host group and an LDEV group in a security group.

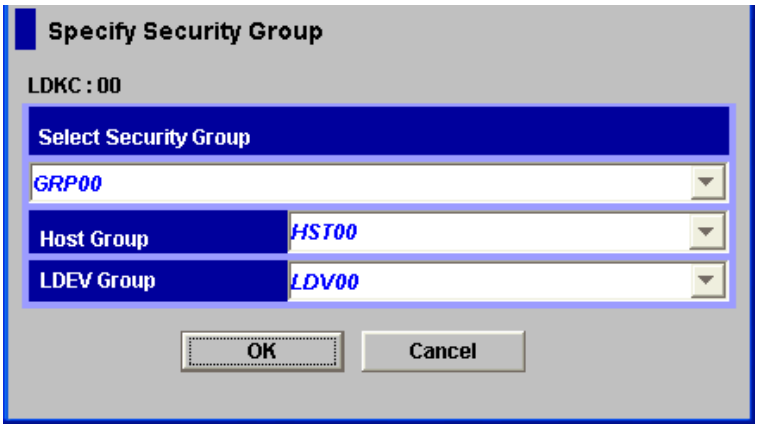


Figure 3-11 Specify Security Group Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
Select Security Group	Specifies the security group in which you want to register a host group and an LDEV group.
Host Group	Specifies a host group that you want to register in the security group.
LDEV Group	Specifies an LDEV group that you want to register in the security group.
OK	Applies settings in the Specify Security Group dialog box to the Volume Security window and closes the dialog box. ***Caution:*** Clicking **OK** applies the settings to the Volume Security window, but does *not* apply the settings to the storage subsystem. To apply the security settings to the subsystem, you must continue to click **Apply** in the Volume Security window until they appear in the dialog box.
Cancel	Discards settings in the Specify Security Group dialog box and closes the dialog box.

Host to Security Group Dialog Box

The Host to Security Group dialog box opens when you do either of the following in the Volume Security window:

- Right-click a host from the upper-right table and then select **Host to Security Group** from the pop-up menu.
- Right-click an item in the tree view and then select **List -> Host to Security Group** from the pop-up menu. The **List -> Host to Security Group** command is unavailable if you double-click a security group and then right-click a host group or LDEV group from immediately below the security group.

Use this dialog box to specify a host and then view security groups in which the host is registered (see Locating Security Groups that Contain a Specified Host).

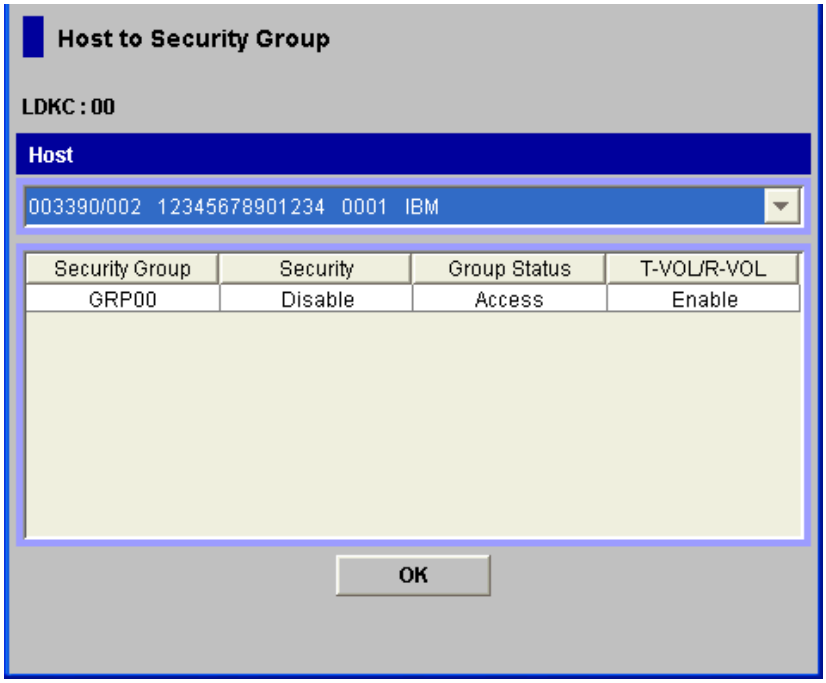


Figure 3-12 Host to Security Group Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
Host	Provides information about a host, where the number groups, from left to right, indicate: ▪ **First:** The Type/Model the type and model number of a host (or a channel extender). ▪ **Second:** The Node ID of a host (or a channel extender). ▪ **Third:** The Logical Partition Number of the host. ▪ **Fourth:** The vendor of the host. Vendors include: **FJT** (Fujitsu), **IBM**, **HTC** (Hitachi), and **CNT(Ex)**. If **CNT(Ex)** appears, the table row indicates the type, model number, and node ID of a channel extender.
Host Group	Specifies a host group that you want to register in the security group.
Security Group table	Lists security groups in which the specified host is registered. ▪ **Security Group** indicates the name of a security group. ▪ **Security** indicates whether the security settings in the security group are enabled or disabled. ▪ **Group Status** indicates whether the security group is an access group or a pool group. ▪ **T-VOL/R-VOL** indicates whether volumes in the security group can be used as secondary volumes (i.e., copy destination volume). **Enable** indicates the volumes can be used as secondary volumes. **Disable** indicates the volumes cannot be used as secondary volumes.
OK	Closes the dialog box.

Host to LDEV Dialog Box

Use the Host to LDEV dialog box to specify a host and then view volumes in the security group in which the host is registered (see Locating Volumes in a Security Group that Contains a Specified Host). It opens when you do either of the following in the Volume Security window:

- Right-click a host from the upper-right table and then select **Host to LDEV** from the pop-up menu.
- Right-click an item in the tree view and then select **List -> Host to LDEV** from the pop-up menu. The **List -> Host to LDEV** command is unavailable if you double-click a security group and then right-click a host group or LDEV group from immediately below the security group.

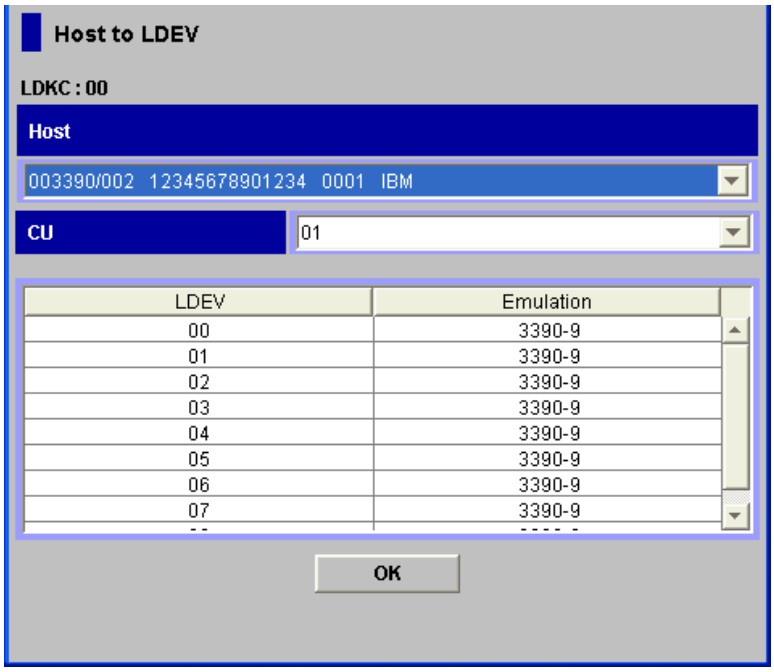


Figure 3-13 Host to LDEV Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC
Host	Provides information about a host, where the number groups, from left to right, indicate: ▪ **First:** The Type/Model the type and model number of a host (or a channel extender). ▪ **Second:** The Node ID of a host (or a channel extender). ▪ **Third:** The Logical Partition Number of the host. ▪ **Fourth:** The vendor of the host. Vendors include **FJT** (Fujitsu), **IBM**, **HTC** (Hitachi), and **CNT(Ex)**. If **CNT(Ex)** appears, the table row indicates the type, model number, and node ID of a channel extender.
CU	Specifies a CU image number.
LDEV table	Lists host groups in which the specified CU is registered. ▪ **LDEV** indicates the name of an LDEV. A volume ID ending in # (for example, 00#) indicates the volume is an external volume. ▪ **Emulation** indicates the emulation types of volumes.
OK	Closes the dialog box.

Host Group to Security Group Dialog Box

The Host Group to Security Group opens when you right-click an item in the tree view of the Volume Security window and then select **List -> Host Group to Security Group** from the pop-up menu. The **List -> Host Group to Security Group** command is unavailable if you double-click a security group and then right-click a host group or LDEV group from immediately below the security group.

Use this dialog box to specify a host group and then view security groups in which the specified host group is registered (see Locating Security Groups that Contain a Specified Host Group).

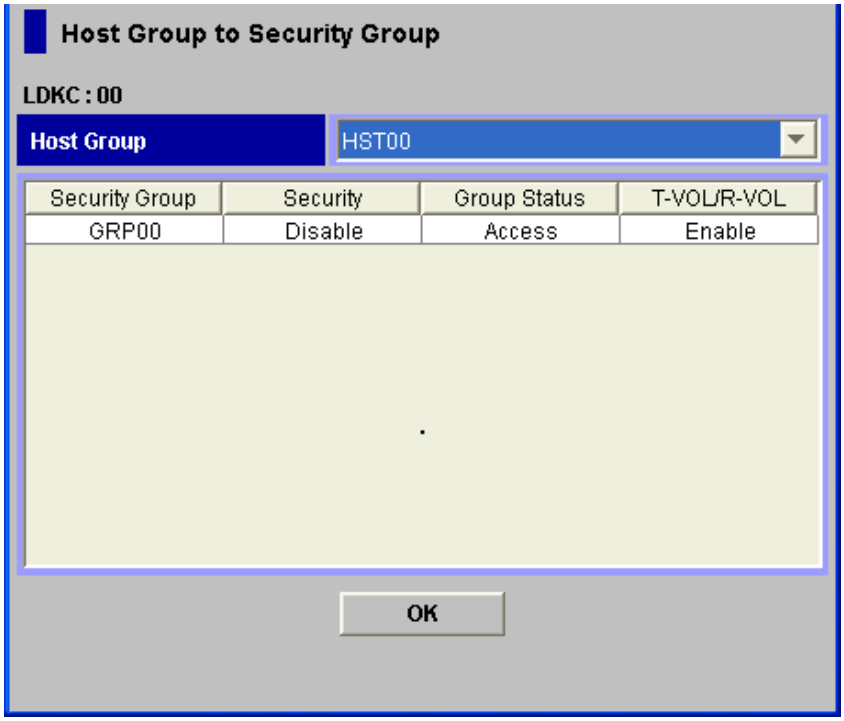


Figure 3-14 Host Group to Security Group Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC
Host Group	Specifies a host group.
Security Group table	Lists information about the security groups in which the specified host group is registered. ▪ **Security Group** indicates the name of a security group. ▪ **Security** indicates whether the security settings in the security group are enabled or disabled. ▪ **Group Status** indicates whether the security group is an access group or a pool group. ▪ **T-VOL/R-VOL** indicates whether volumes in the security group can be used as secondary volumes (i.e., copy destination volume). **Enable** indicates the volumes can be used as secondary volumes. **Disable** indicates the volumes cannot be used as secondary volumes.
OK	Closes the dialog box.

Host Group to Port Dialog Box

To use the Host Group to Port dialog box, you must have already installed the Volume Security Port Option.

The Host Group to Port dialog box opens when you right-click an item in the tree view of the Volume Security window and then select **List -> Host Group to Port** from the pop-up menu. Use this dialog box to find ports on which hosts can access volumes (see Locating Ports through Which Hosts Can Access Volumes).

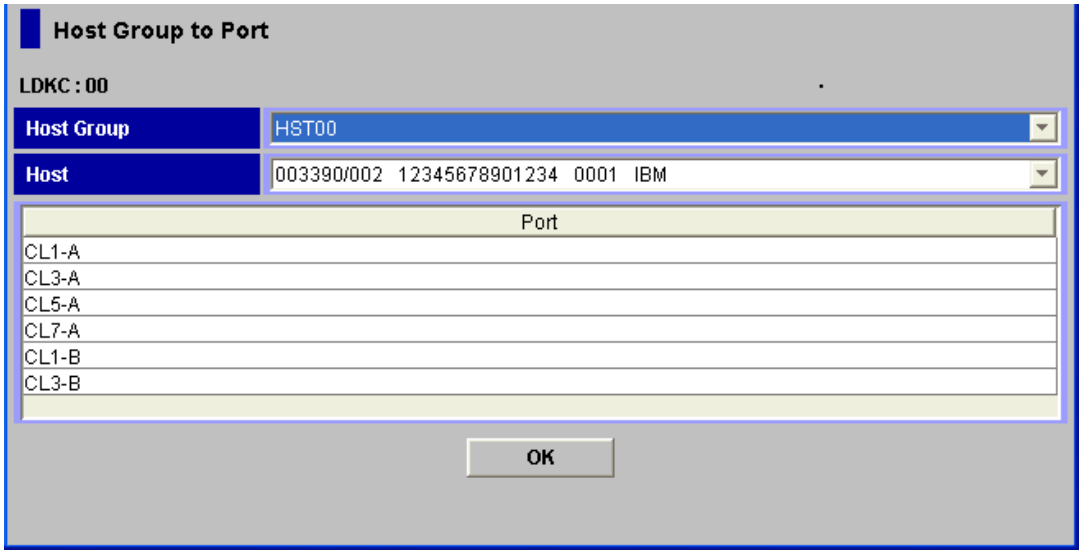


Figure 3-15 Host Group to Port Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
Host Group	Provides information about a host group, where the number groups, from left to right, indicate: ▪ **First:** The Type/Model the type and model number of a host (or a channel extender). ▪ **Second:** The Node ID of a host (or a channel extender). ▪ **Third:** The Logical Partition **Number** of the host. ▪ **Fourth:** The vendor of the host. Vendors include **FJT** (Fujitsu), **IBM**, **HTC** (Hitachi), and **CNT(Ex)**. If **CNT(Ex)** appears, the table row indicates the type, model number, and node ID of a channel extender.
Port table	Lists ports that are available and registered.
OK	Closes the dialog box.

LDEV to Security Group Dialog Box

The LDEV to Security Group dialog box opens when you do either of the following in the Volume Security window:

- Right-click a volume from the lower right table and then select **LDEV to Security Group** from the pop-up menu.
- Right-click an item in the tree view and then select **List -> LDEV to Security Group** from the pop-up menu. The **List -> LDEV to Security Group** command is unavailable if you double-click a security group and then right-click a host group or LDEV group from immediately below the security group.

Use this dialog box to specify a volume and then view security groups in which the volume is registered (see Locating Security Groups that Contain a Specified Volume).

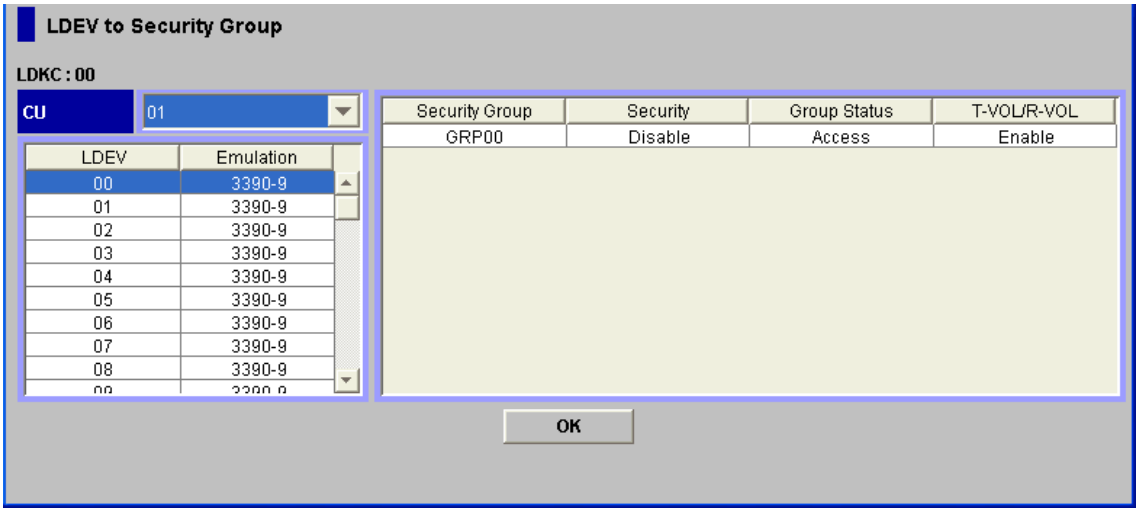


Figure 3-16 LDEV to Security Group Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
CU	Specifies a CU image number.
LDEV table	Describes the available LDEVs: ▪ **LDEV** indicates a number assigned to the LDEV. ▪ **Emulation** indicates the emulation types of the volume. ***Note:*** A volume ID ending in # (for example, 00#) indicates the volume is an external volume.
Security Group table	Lists security groups in which the specified volume is registered: ▪ **Security Group** indicates the name of a security group. ▪ **Security** indicates whether the security settings in the security group are enabled or disabled. ▪ **Group Status** indicates whether the security group is an access group or a pool group. ▪ **T-VOL/R-VOL** indicates whether volumes in the security group can be used as secondary volumes (i.e., copy destination volume). **Enable** indicates the volumes can be used as secondary volumes. **Disable** indicates the volumes cannot be used as secondary volumes.
OK	Closes the dialog box.

LDEV to Host Dialog Box

The LDEV to Host dialog box opens when you do either of the following in the Volume Security window:

- Right-click a volume from the lower right table and then select **LDEV to Host** from the pop-up menu.
- Right-click an item in the tree view and then select **List -> LDEV to Host** from the pop-up menu. The **List -> LDEV to Host** pop-up command is unavailable if you double-click a security group and then right-click a host group or LDEV group from immediately below the security group.

Use this dialog box to specify a volume and then view hosts in the security group in which the specified volume is registered (see Locating Hosts in a Security Group that Contains a Specified Volume).

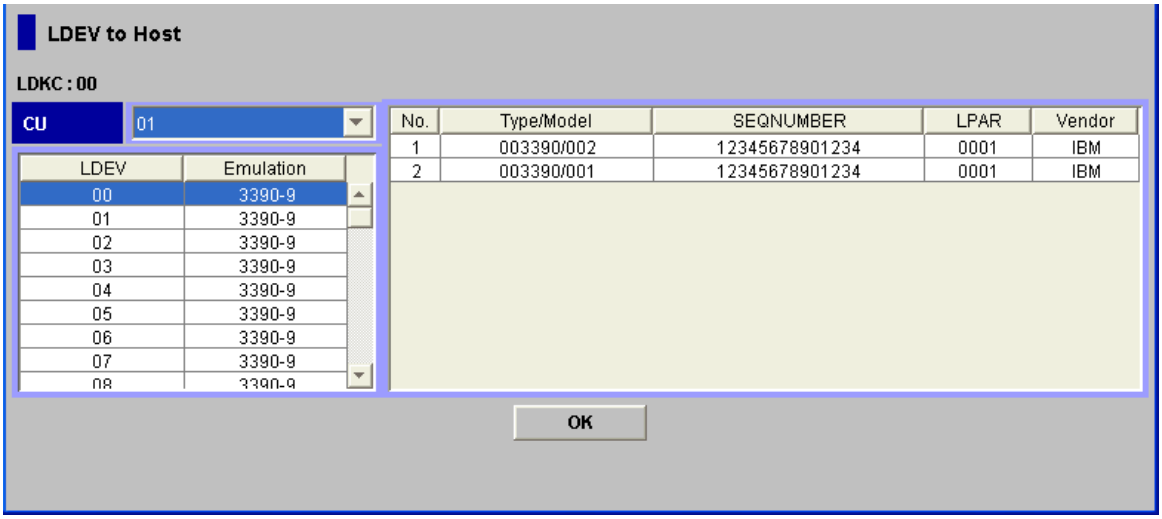


Figure 3-17 LDEV to Host Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
CU	Specifies a CU image number.
LDEV table	Describes the available LDEVs: ▪ **LDEV** indicates a number assigned to the LDEV. ▪ **Emulation** indicates the emulation types of the volume. ***Note:*** A volume ID ending in # (for example, 00#) indicates the volume is an external volume.
Host table	Lists hosts in the security group in which the specified volume is registered. ▪ **No.** A sequential number associated with a host. ***Note:*** Each table row usually shows information about a host. However, if a host is attached to the disk subsystem via a channel extender, the table row shows information about the channel extender. ▪ **Type/Model** indicates the type and the model number of a host (or a channel extender). The **Type** appears on the left of the slash (/). The **Model** number appears on the **right** of the slash. Before the Type/Model, an icon indicates the registration status of the host in these ways: ▪ **SEQNUMBER** indicates the node ID of a host (or a channel extender). ▪ **LPAR** indicates the logical partition number of a host. Logical partitions are virtual systems created as a result of sectioning a computer's memory into separate units. ▪ **Vendor** indicates the vendor of a host. Vendors include **FJT** (Fujitsu), **IBM**, **HTC** (Hitachi), and **CNT(Ex)**. If **CNT(Ex)** appears, the **Type/Model** column indicates the type and the model number of a channel extender, and the **SEQNUMBER** column indicates the node ID of the channel extender.
OK	Closes the dialog box.

LDEV Group to Security Group Dialog Box

The LDEV Group to Security Group dialog box opens when you right-click an item in the tree view of the Volume Security window and then select **List -> LDEV Group to Security Group** from the pop-up menu. The **List -> LDEV Group to Security Group** command is unavailable if you double-click a security group and then right-click a host group or LDEV group from immediately below the security group.

Use this dialog box to specify an LDEV group and then view security groups in which the specified LDEV group is registered (see Locating Security Groups that Contain a Specified LDEV Group).

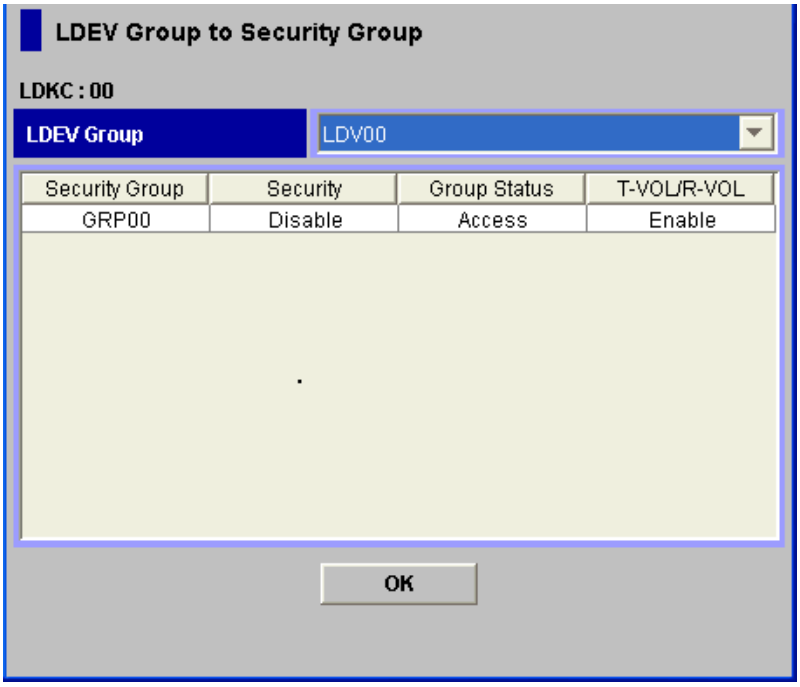


Figure 3-18 LDEV Group to Security Group Dialog Box

Item	Description
LDKC	Indicates the number of the selected LDKC.
LDEV Group	Specifies an LDEV group.
Security Group table	Lists information about the security groups in which the specified LDEV group is registered. ▪ **Security Group** indicates the name of a security group. ▪ **Security** indicates whether the security settings in the security group are enabled or disabled. ▪ **Group Status** indicates whether the security group is an **Access** or a **Pool** group. ▪ **T-VOL/R-VOL** indicates whether volumes in the security group can be used as secondary volumes (i.e., copy destination volume). **Enable** indicates the volumes can be used as secondary volumes. **Disable** indicates the volumes cannot be used as secondary volumes.
OK	Closes the dialog box.

Error Detail Dialog Box

When you attempt to apply security in the Volume Security window, an error might occur if hosts are performing I/O operations (for details, see the ***Caution*** in Port-Level Security Implementation). Use the Error Detail dialog box to find hosts that are performing I/O operations.

For instructions on how to remove errors, see Troubleshooting.

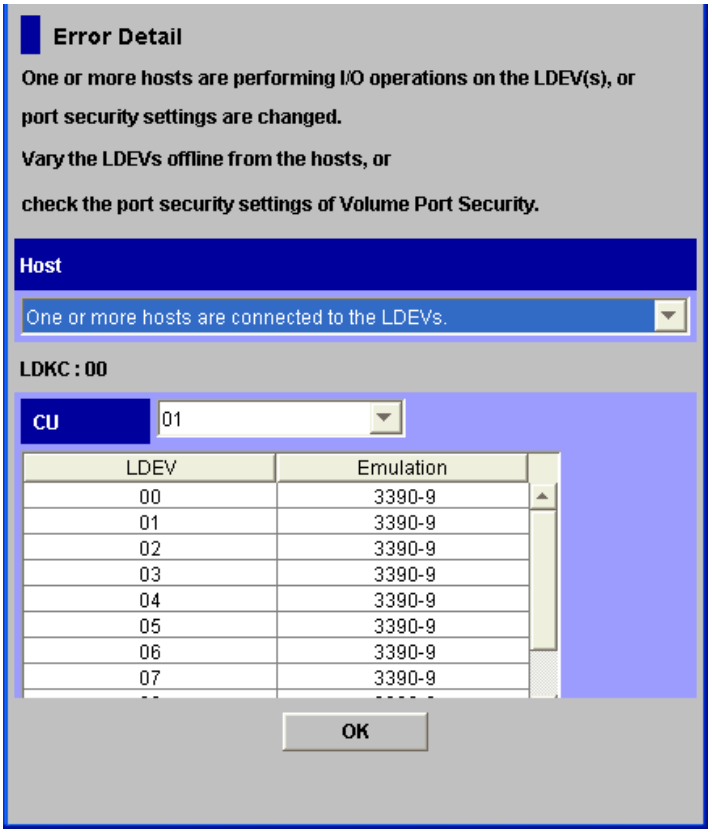


Figure 3-19 Error Detail Dialog Box

Item	Description
Host	Lists the number of the host available on the selected LDKC which are performing I/O operations.
LDKC	Indicates the number of the selected LDKC.
CU	Specifies a Command Unit image and forces the display of any volumes on which the host is performing I/O operations and which belong to the specified CU image.
LDEV table	Provides information about the selected CU. ▪ **LDEV:** The available LDEV numbers. ▪ **Emulation:** The emulation types of volumes.
OK	Closes the dialog box.

4

Performing Volume Security Operations

This chapter provides instructions for performing Volume Security operations.

Launching Volume Security

This section describes how to start the Volume Security software.

If Volume Security Port Option is installed, the functions of the Volume Security Port Option program become usable when you start Volume Security.

To start the Volume Security software:

1. Log on to the SVP to open the Storage Navigator main window. For details, refer to *Storage Navigator User's Guide*.

   To make security settings and apply the settings, you must use a user account that has the write permission (For example, the Administrator account). If you use a user account that does not have the write permission, you will be able to view security settings but will neither be able to make security settings nor apply security settings.

2. Click **Go**, **Mainframe Connection**, and then **Volume Security** on the menu bar of the Storage Navigator main window. The Volume Security window opens.

   To set security using Volume Security, you must make sure that Storage Navigator is in Modify mode. For detailed information on how to do this, please refer to *Storage Navigator User's Guide*.

Viewing Security Settings

This section describes how to view security settings.

Locating Volumes in a Specified Security Group

To search a security group for volumes, please select the security group in the tree view of the Volume Security window and then see the list of volumes in the lower-right table.

Locating Security Groups that Contain a Specified Host

Use one of the two following procedures to specify a host and find the security groups in which the host is registered.

- Use the first procedure if the desired host is displayed in the upper-right table of the Volume Security window.
- Use the second procedure if the desired host is not displayed in the upper-right table.

If the desired host appears in the upper-right table:

1. Right-click the host in the table.
2. From the pop-up menu, select **List -> Host to Security Group**. The Host to Security Group dialog box opens showing the security groups that you want.

If the desired host does not appear in the upper-right table:

1. In the tree view of the Volume Security window, right-click an item except for a host group or LDEV group that appears immediately below a security group.
2. From the pop-up menu, select **List -> Host to Security Group**. The Host to Security Group dialog box opens.
3. From the **Host** list, select the desired host. The table lists the security groups that you want.

Locating Volumes in a Security Group that Contains a Specified Host

If a security group is classified as an access group, the security group contains both host and volumes. Use one of the following procedures to specify a host and to find volumes in the security group in which the specified host is registered.

- Use the first procedure if the desired host is displayed in the upper-right table of the Volume Security window.
- Use the second procedure if the desired host is not displayed in the upper-right table.

If the desired host appears in the upper-right table:

1. Right-click the host in the table.
2. From the pop-up menu, select **List -> Host to LDEV**.
   The Host to LDEV dialog box opens showing a list of volumes.
3. Right-click an arrow at the right end of the **CU** list, and then see how many CU image numbers appear.
   - If only one CU image number appears, the table in the dialog box displays all the volumes that you want.
   - If two or more CU image numbers appear, the table in the dialog box currently displays some of the volumes that you want. Select each CU image number to find volumes in the specified CU image.

If the desired host does not appear in the upper-right table:

1. In the tree view of the Volume Security window, right-click an item except for a host group or LDEV group that appears immediately below a security group.
2. From the pop-up menu, select **List -> Host to LDEV**. The Host to LDEV dialog box opens.
3. From the **Host** list, select the desired host.
4. Right-click an arrow at the right end of the **CU** list, and then see how many CU image numbers appear.
   - If only one CU image number appears, the table in the dialog box displays all the volumes that you want.
   - If two or more CU image numbers appear, the table in the dialog box currently displays some of the volumes that you want. Select each CU image number to find volumes in the specified CU image.

Locating Ports through Which Hosts Can Access Volumes

To find ports through which a host can access volumes, you must ensure that Volume Security Port Option is already installed by using the following procedure.

To find ports via which a host can access volumes:

1. In the Volume Security window, right-click an item in the tree view and then select **List -> Host Group to Port** from the pop-up menu. The Host Group to Port dialog box opens.
2. Select a host group from the **Host Group** list.
3. Select a host from the **Host** list. The **Port** list shows ports on which the specified host can access volumes.
4. Click **OK** to close the Host Group to Port dialog box and return to the Volume Security window.

Locating Security Groups that Contain a Specified Volume

If you want to specify a volume and find the security groups in which the volume is registered, you can follow either of the two procedures below.

- Use the first procedure if the desired volume is displayed in the lower-right table of the Volume Security window.
- Use the second if the desired volume is not displayed in the lower-right table.

If the desired volume appears in the lower-right table:

1. Right-click the volume in the table.
2. From the pop-up menu, select **List -> LDEV to Security Group**. The LDEV to Security Group dialog box opens showing the security groups that you want.

If the desired volume does not appear in the lower-right table:

1. In the tree view of the Volume Security window, right-click an item except for a host group or LDEV group that appears immediately below a security group.
2. From the pop-up menu, select **List -> LDEV to Security Group**. The LDEV to Security Group dialog box opens.
3. Select a CU image number from the **CU** list, and then select an LDEV number from the lower-left table. The table on the right lists the security groups that you want.

Locating Hosts in a Security Group that Contains a Specified Volume

Use one of the following procedures to specify a volume and to find hosts in the security group in which the specified volume is registered.

- Use the first procedure if the desired volume is displayed in the lower-right table of the Volume Security window.
- Use the second if the desired volume is not displayed in the lower-right table.

If the desired volume appears in the lower-right table:

1. Right-click the volume in the table.
2. From the pop-up menu, select **List -> LDEV to Host**. The LDEV to Host dialog box opens showing a list of hosts.

If the desired volume does not appear in the lower-right table:

1. In the tree view of the Volume Security window, right-click an item except for a host group or LDEV group that appears immediately below a security group.
2. From the pop-up menu, select **List -> LDEV to Host**. The LDEV to Host dialog box opens.
3. Select a CU image number from the **CU** list, and then select an LDEV number from the lower-left table. The table on the right lists the security groups that you want.

Locating Security Groups that Contain a Specified Host Group

To specify a host group and then find security groups in which the specified host group is registered, use the following procedure:

1. In the tree view of the Volume Security window, right-click an item except for a host group or LDEV group that appears immediately below a security group.
2. From the pop-up menu, select **List -> Host Group to Security Group**. The Host Group to Security Group dialog box opens.
3. From the **Host Group** list, select the desired host Group. The table lists the security groups that you want.

Locating Security Groups that Contain a Specified LDEV Group

To specify an LDEV group and then find security groups in which the specified LDEV group is registered, use the following procedure:

1. In the tree view of the Volume Security window, right-click an item except for a host group or LDEV group that appears immediately below a security group.
2. From the pop-up menu, select **List -> LDEV Group to Security Group**. The LDEV Group to Security Group dialog box opens.
3. From the **LDEV Group** list, select the desired LDEV Group. The table lists the security groups that you want.

Limiting Host Access

Use the following procedures to enable some hosts to access certain volumes and prevent other hosts from accessing these volumes:

- ☐ Creating a Host Group
- ☐ Registering Hosts in a Host Group
- ☐ Registering Ports in a Host Group
- ☐ Creating an LDEV Group
- ☐ Registering Volumes in an LDEV Group
- ☐ Creating a Security Group for Use As an Access Group
- ☐ Registering a Host Group and an LDEV Group in a Security Group

Creating a Host Group

To specify hosts that can access specific volumes, create a host group and then register the hosts in the host group.

The following is the procedure for creating a host group. For details on how to register hosts in a host group, see Registering Hosts in a Host Group.

Caution: When creating a host group, it is strongly recommended that you click **Apply** in the Volume Security window, as described in the last step of the following procedure. If you forget to click **Apply**, the host group can be lost if you encounter an error registering the host group and the LDEV group (see Registering a Host Group and an LDEV Group in a Security Group).

To create a host group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **Host Group**. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change Host Group dialog box opens.
5. In the **Enter Host Group** box, enter the name of the host group that you want to create, and then click **Add**.

   Host group names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable in host group names:
   `\ , / : ; * ? " < > |`
6. Confirm that the new host group is displayed by blue in **Host Group List**, and then click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.

7. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
8. Click **Yes**. The settings are applied to the disk subsystem.

Registering Hosts in a Host Group

Now that you have created a host group, you need to register hosts in the host group.

Caution: When registering hosts into a host group, you are strongly recommended to click **Apply** in the Volume Security window, as described in the last step of the following procedure. If you forget to click **Apply**, you might lose the host group when you encounter an error registering the host group and the LDEV group (see Registering a Host Group and an LDEV Group in a Security Group).

To register hosts in a host group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click a host group. A pop-up menu appears.
4. Select **Specify** and then **Host** from the pop-up menu. The Add/Change Host dialog box opens showing a list of hosts.
5. Select and then right click one or more hosts that you want to register.

   If a host is indicated by the icon or , the host is already registered in the specified host group. For details on the meaning of icons, see Add/Change Host Dialog Box.

   If ports are registered in the displayed host group, you can register only the hosts that do not belong to any other host group. You cannot register hosts that belong to any other host group.

   If no ports are registered in the displayed host group, you can register the following hosts:

   - hosts that do not belong to any host group
   - hosts belonging to host groups in which no ports are registered.

   However, you cannot register hosts belonging to host groups in which ports are registered.
6. Select **Registration** and then **Register Host in Host Group** from the pop-up menu. The specified hosts are displayed by blue and also indicated by the icon or the icon.
7. Click **OK** in the Add/Change Host dialog box. At this point, the settings in the window have not been applied to the disk subsystem.
8. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.

9. Click **Yes**. The settings are applied to the disk subsystem.

Registering Ports in a Host Group

After registering hosts in a host group, you can register ports in the host group to implement port-level security.

If you want to register ports in a host group, you must ensure that Volume Security Port Option is already installed.

If you do not want to implement port-level security, you do not need to register ports in host groups. If no ports are registered in a host group, hosts in the host group can access volumes via every port to which the hosts are connected.

Caution: When you register ports in a host group, it is strongly recommended that you click **Apply** in the Volume Security window at the end of the operation (see the end of the following procedure). If you do not click **Apply,** registration of ports could be cancelled when an error occurs registering a host group and an LDEV group (see Registering a Host Group and an LDEV Group in a Security Group).

To register ports in a host group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click a host group. A pop-up menu appears.
4. Select **Specify** and then **Port** from the pop-up menu. The Select Port dialog box opens and displays a list of ports.
5. From the **Port** list in the **Unregistered port** box, select one or more ports on the hosts in the host group to enable their accessing these volumes. Next, click **Regist**. The specified ports are displayed in blue in the **Port** list in the **Registered port** box.

   To select all the ports in the **Port** list in the **Unregistered port** box, click **Select All**.

   If hosts registered in the host group are also registered in another host group, you cannot register ports in the **Port** list in the **Registered port** box, and thus you cannot implement port-level security.
6. Click **OK** in the Select Port dialog box. The Select Port dialog box closes and you are returned to the Volume Security window. At this point, the settings in the window have not been applied to the disk subsystem.
7. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
8. Click **Yes**. The settings are applied to the disk subsystem.

Creating an LDEV Group

To specify volumes to be secured, you must create an LDEV group and then register the volumes in the LDEV group.

The following procedure explains how to create an LDEV group. For details on how to register volumes in an LDEV group, see Registering Volumes in an LDEV Group.

Caution: When creating an LDEV group, you are strongly recommended to click **Apply** in the Volume Security window, as described in the last step of the following procedure. If you forget to click **Apply**, you might lose the LDEV group when you encounter an error registering the host group and the LDEV group (see Registering a Host Group and an LDEV Group in a Security Group).

To create an LDEV group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **LDEV Group**. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change LDEV Group dialog box opens.
5. In the **Enter LDEV Group** box, enter the name of the LDEV group that you want to create, and then click **Add**.

   Names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable:
   `\ , / : ; * ? " < > |`
6. Confirm that the new LDEV group is displayed by blue in **LDEV Group List**, and then click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
7. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
8. Click **Yes**. The settings are applied to the disk subsystem.

Registering Volumes in an LDEV Group

Once an LDEV group has been created, the next step is to register the volumes in the LDEV group.

Caution: When registering volumes in an LDEV group, you are strongly recommended to click **Apply** in the Volume Security window, as described in the last step of the following procedure. If you forget to click **Apply**, the volumes might be unregistered when you encounter an error registering the host group and the LDEV group (see Registering a Host Group and an LDEV Group in a Security Group).

To register volumes in an LDEV group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click an LDEV group. A pop-up menu appears.
4. Select **Specify** and then **LDEV** from the pop-up menu. The Select LDEV dialog box opens.
5. Use the **CU** list to specify a CU image. The two boxes beneath the list show volumes in the specified CU image.
   - The **Registered in LDEV group** box displays volumes registered in the LDEV group.
   - The **Not registered in LDEV group** box displays volumes that are not registered in the LDEV group.
6. In the **Not registered in LDEV group** box, select volumes that you want to register. Then, click **Regist**. The selected volumes move to the **Registered in LDEV group** box.
7. If you want to register volumes in other CU images, return to step 5.
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
10. Click **Yes**. The settings are applied to the disk subsystem.

Creating a Security Group for Use As an Access Group

To make security settings, you must create security groups. Security groups can be classified as access groups or pool groups. You must classify a security group as an access group if you want to allow volumes to be accessed only by specified hosts.

To create a security group and classify the group as an access group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **Security Group**. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change Security Group dialog box opens.
5. In the **Enter Security Group** box, enter the name of the security group that you want to create.

   Names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable:
   \ , / : ; * ? " < > |
6. In the **Security** box, select **Enable**.
7. In the **Group Status** box, select **Access**.
8. In the **T-VOL/R-VOL** box, select **Enable** or **Disable**.
   - Select **Enable** if you want make volumes in the security group usable as secondary volumes (i.e., copy destination volumes) for copy operations.
   - Select **Disable** if you want make volumes in the security group unusable as secondary volumes (i.e., copy destination volumes) for copy operations.
9. Click **Add**. Information about the new security group is added to the **Security Group List** table and is displayed in blue.
10. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
11. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
12. Click **Yes**. The settings are applied to the disk subsystem.

Registering a Host Group and an LDEV Group in a Security Group

Now that you have classified your security group as an access group, your next (and the last) task is to register your host group and LDEV group into the security group. When you finish registration, the volumes in the LDEV group are secured and can only be accessed by hosts in the host group. Other hosts cannot access the volumes.

Caution: Before applying security, confirm which hosts are performing I/O operations on volumes in access groups. If any hosts are performing I/O operations on volumes in access groups to which the hosts do not belong, you must stop the I/O operations before applying security.

To register a host group and an LDEV group into a security group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click a security group. A pop-up menu appears.
4. Select **Specify** and then **Security Group** from the pop-up menu. The Specify Security Group dialog box opens.
5. Use the **Select Security Group** list to select the security group in which you want to register a host group and an LDEV group.
6. Use the **Host Group** list to select the host group that you want to register in the security group.
7. Use the **LDEV Group** list to select the LDEV group that you want to register in the security group, and then click **OK**.
8. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
9. Click **Yes**. The settings are applied to the disk subsystem.

Prohibiting Host Access

Volume Security enables you to prohibit all the hosts from accessing the specified volumes. To do this, take the following steps:

- ☐ Creating an LDEV Group
- ☐ Registering Volumes in an LDEV Group
- ☐ Creating a Security Group for Use As a Pool Group
- ☐ Registering an LDEV Group in a Security Group

Creating an LDEV Group

To specify volumes to be secured, you must create an LDEV group and then register the volumes in the LDEV group.

The following procedure explains how to create an LDEV group. For details on how to register volumes in an LDEV group, see Registering Volumes in an LDEV Group.

Caution: When creating an LDEV group, it is strongly recommended that you click **Apply** in the Volume Security window, as described in the last step of the following procedure. If you forget to click **Apply**, you might lose the LDEV group when you encounter an error registering the LDEV group (see Registering an LDEV Group in a Security Group)

To create an LDEV group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **LDEV Group**. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change LDEV Group dialog box opens.
5. In the **Enter LDEV Group** box, enter the name of the LDEV group that you want to create, and then click **Add**.

   Names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable:
   `\ , / : ; * ? " < > |`
6. Confirm that the new LDEV group is displayed by blue in **LDEV Group List**, and then click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
7. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
8. Click **Yes**. The settings are applied to the disk subsystem.

Registering Volumes in an LDEV Group

Now that you have created an LDEV group, then you need to register volumes in the LDEV group.

Caution: When registering volumes in an LDEV group, you are strongly recommended to click **Apply** in the Volume Security window, as described in the last step of the following procedure. If you forget to click **Apply**, the volumes might be unregistered when you encounter an error registering the LDEV group (see Registering an LDEV Group in a Security Group).

To register volumes in an LDEV group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click an LDEV group. A pop-up menu appears.
4. Select **Specify** and then **LDEV** from the pop-up menu. The Select LDEV dialog box opens.
5. Use the **CU** list to specify a CU image. The two boxes below the list show volumes in the specified CU image.
   - The **Registered in LDEV group** box displays volumes registered in the LDEV group.
   - The **Not registered in LDEV group** box displays volumes that are not registered in the LDEV group.
6. In the **Not registered in LDEV group** box, select volumes that you want to register. Then, click **Regist**.
   The selected volumes move to the **Registered in LDEV group** box.
7. If you want to register volumes in other CU images, return to step 5.
8. Click **OK**. At this point the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
10. Click **Yes**. The settings are applied to the disk subsystem.

Creating a Security Group for Use As a Pool Group

To make security settings, you must create security groups. Security groups can be classified as access groups or pool groups. You must classify a security group as a pool group if you want to prohibit all the hosts from accessing volumes.

To create a security group and classify the group as a pool group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.

3. Right-click **Security Group**. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change Security Group dialog box opens.
5. In the **Enter Security Group** box, enter the name of the security group that you want to create.

   Names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable:
   `\ , / : ; * ? " < > |`
6. In the **Security** box, select **Enable**.
7. In the **Group Status** box, select **Pool**.
8. In the **T-VOL/R-VOL** box, select **Enable** or **Disable**.
   - Select **Enable** if you want make volumes in the security group usable as secondary volumes (i.e., copy destination volumes) for copy operations.
   - Select **Disable** if you want make volumes in the security group unusable as secondary volumes (i.e., copy destination volumes) for copy operations.
9. Click **Add**. Information about the new security group is added to the **Security Group List** table and is displayed in blue.
10. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
11. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
12. Click **Yes**. The settings are applied to the disk subsystem.

Registering an LDEV Group in a Security Group

Now that you have classified your security group as a pool group, your next (and the last) task is to register your LDEV group into the security group. When you finish registration, the volumes in the LDEV group are secured and inaccessible from any hosts.

Caution: Before applying security, confirm which hosts are performing I/O operations on volumes in access groups. If any hosts are performing I/O operations on volumes in access groups to which the hosts do not belong, you must stop the I/O operations before applying security.

To register an LDEV group into a security group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click a security group and a pop-up menu appears.

4. Select **Specify** and then **Security Group** from the pop-up menu. The Specify Security Group dialog box opens.
5. Use the **Select Security Group** list to select a security group in which you want to register an LDEV group.
6. Use the **LDEV Group** list to select an LDEV group that you want to register in the security group, and then click **OK**.
7. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
8. Click **Yes**. The settings are applied to the disk subsystem.

Protecting Volumes from Copy Operations

The following procedure makes volumes in a security group unusable as secondary volumes (i.e., copy destination volumes) for copy operations, so you will be able to protect data the volumes from being overwritten by copy operations.

To make volumes in a security group unusable as secondary volumes:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **Security Group** or the desired security group. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change Security Group dialog box opens.
5. Ensure that the desired security group is selected in the **Security Group List** table.
6. Select **Disable** in the **T-VOL/R-VOL** box.
7. Click **Change**. The change is reflected in the dialog box.
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
10. Click **Yes**. The settings are applied to the disk subsystem.

Tip: To make volumes in your security group usable as secondary volumes (i.e., copy destination volumes) for copy operations, select the security group in the Add/Change Security Group dialog box and then select **Enable** in the **T-VOL/R-VOL** box. Next, click **Change** and then **OK**. Finally, click **Apply** in the Volume Security window

Disabling Volume Security

If you use the following procedure to manipulate a security group, you can disable security on volumes in the security group. If security is disabled, volumes in the security group are accessible from all hosts and are usable as secondary volumes (i.e., copy destination volumes) for copy operations, regardless of whether the security group is an access group or a pool group. If you want to restore security, you can restore it in an easy and simple operation.

If you are sure that you will not need to restore security, you can delete your security group to disable security. For details on how to delete security groups, see Deleting Security Groups.

To disable security on volumes:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click the security group in which the desired volumes are registered. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change Security Group dialog box opens.
5. Ensure that the desired security group is selected in the **Security Group List** table.
6. Select **Disable** in the **Security** box.
7. Click **Change**. The change is reflected in the dialog box.
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
10. Click **Yes**. The settings are applied to the disk subsystem.

Tip: To restore security, select the security group in the Add/Change Security Group dialog box and then select **Enable** in the **Security** box. Next, click **Change** and then **OK**. Finally, click **Apply** in the Volume Security window.

Editing Security Groups

This section describes the operations used to edit your security groups:

- ☐ Unregistering a Host Group
- ☐ Unregistering an LDEV Group
- ☐ Renaming a Security Group
- ☐ Deleting a Security Group

Unregistering a Host Group

To unregister a host group from a security group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Locate and double-click a security group. The tree view displays the host group in the specified security group.
4. Right-click the host group and the select **Delete** from the pop-up menu. A message appears asking whether to unregister the specified host group.
5. Click **Yes** to close the message. At this point, the settings in the window have not been applied to the disk subsystem.
6. Click **Apply** in the Volume Security window. A message appears asking whether to apply the changes to the disk subsystem.
7. Click **Yes**. The changes are applied to the disk subsystem.

Unregistering an LDEV Group

To unregister an LDEV group from a security group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Locate and double-click a security group. The tree view displays the LDEV group in the specified security group.
4. Right-click the LDEV group and the select **Delete** from the pop-up menu. A message appears asking whether you want to unregister the specified LDEV group.
5. Click **Yes** to close the message. At this point, the settings in the window have not been applied to the disk subsystem.
6. Click **Apply** in the Volume Security window. A message appears asking whether to apply the changes to the disk subsystem.
7. Click **Yes**. The changes are applied to the disk subsystem.

Renaming a Security Group

To rename a security group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **Security Group** or a security group. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change Security Group dialog box opens.
5. Ensure that the desired security group is selected in the **Security Group List** table.
6. In the **Enter Security Group** box, enter the new name for the security group.

   Names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable: `\ , / : ; * ? " < > |`
7. Click **Change**. The change is reflected in the dialog box.
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the change to the disk subsystem.
10. Click **Yes**. The change is applied to the disk subsystem.

Deleting a Security Group

To delete a security group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Do either of the following:
   - Right-click a security group in the tree view.
   - Right-click **Security Group** in the tree view and then select **Add/Change** from the pop-up menu. Next, in the Add/Change Security Group dialog box, select one or more security groups in the **Security Group List** table and right-click the selection.
4. Select **Delete** from the pop-up menu. A message appears asking whether you want to delete the specified security group(s).
5. Click **Yes** to close the message. If the Add/Change Security Group dialog box still remains displayed, click **OK** to close the dialog box. At this point, the settings in the window have not been applied to the disk subsystem.
6. Click **Apply** in the Volume Security window. A message appears asking whether to apply the change to the disk subsystem.
7. Click **Yes**. The change is applied to the disk subsystem.

Editing Host Groups

This section explains the following operations, which allow you to edit your host groups:

- ☐ Registering Hosts to be Attached to the Disk Subsystem
- ☐ Deleting Hosts from Host Groups
- ☐ Deleting Ports from Host Groups
- ☐ Renaming Host Groups
- ☐ Deleting Host Groups

Registering Hosts to be Attached to the Disk Subsystem

If your organization is planning to attach new mainframe hosts to the disk subsystem, you will possibly need to revise security settings on volumes. For example, if you do not want to allow the new hosts to access some volumes, you might need to register the new hosts in the host group in an existing access group. Volume Security enables you to register new hosts in host groups before the new hosts are attached via cables to the disk subsystem.

To register a mainframe host to be attached into a host group:

1. Execute the following system command at the mainframe host:

   ```
   D  M=CPU
   ```

   This command displays the type, the model number, the node ID, and the logical partition number of the host. Record this information.

   For details of the system command, refer to the documentation for system commands.
2. Ensure that you are in Modify mode.
3. In the Volume Security window, double-click an LDKC number.
4. Right-click **Host Group** to display a list of host groups.
5. Right-click the host group in which you want to register the host. Next, select **Specify** and then **Host** from the pop-up menu. The Add/Change Host dialog box opens.
6. Use the text boxes and the drop-down list to specify information about the host you want to register; you have already obtained the information earlier in this procedure (refer to step 1).
7. Click **Add**. The specified host is added to the table and is indicated by the icon  .
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
10. Click **Yes**. The settings are applied to the disk subsystem.

Tips:

- If you registered a host in an incorrect host group, first follow the above procedure to register the host in the correct host group. Then, follow the procedure in Deleting Hosts from Host Groups to remove the host from the incorrect host group.
- You can modify information about hosts indicated by  in the Add/Change Host dialog box. To modify information, first select the desired host in the table and then use text boxes and/or drop-down lists to change information. Next, click **Change** and then **OK**. Finally, click **Apply** in the Volume Security window.
- To delete a host indicated by  from the Add/Change Host dialog box, first select and right-click the host, select **Delete** from the pop-up menu, and then select **OK**. Finally, click **Apply** in the Volume Security window.

Deleting Hosts from Host Groups

To delete hosts from a host group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click a host group. A pop-up menu appears.
4. Select **Specify** and then **Host** from the pop-up menu. The Add/Change Host dialog box opens and displays a list of hosts. The icons  and  indicate hosts registered in the specified host group.
5. Select and then right click one or more hosts (indicated by  or ) that you want to delete.
6. Select **Registration** and then **Unregister Host from Host Group** from the pop-up menu. The specified hosts are displayed by blue. Also, icons disappear or change to  or  , indicating that the host is registered in another host group.
7. Click **OK** in the Add/Change Host dialog box. At this point, the settings in the window have not been applied to the disk subsystem.
8. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
9. Click **Yes**. The settings are applied to the disk subsystem.

Deleting Ports from Host Groups

If you want to delete ports from host groups, you must ensure that Volume Security Port Option is already installed.

To delete ports from a host group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click a host group. A pop-up menu appears.
4. Select **Specify** and then **Port** from the pop-up menu. The Select Port dialog box opens.
5. In the **Port** list in the **Registered port** box, select one or more ports that you want to delete. Next, click **Unregist**.

   The specified ports are displayed in blue in the **Port** list in the **Unregistered port** box.

   If you want to select all ports in the **Port** list in the **Registered port** box, click **Select All**.
6. Click **OK** in the Select Port dialog box. The Select Port dialog box closes and you are returned to the Volume Security window. At this point, the settings in the window have not been applied to the disk subsystem.
7. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
8. Click **Yes**. The settings are applied to the disk subsystem.

Renaming Host Groups

To rename a host group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **Host Group** or a host group. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change Host Group dialog box opens.
5. Ensure that the desired host group is selected in the **Host Group List** table.
6. In the **Enter Host Group** box, enter the new name for the host group.

   Names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable: \ , / : ; * ? " < > |
7. Click **Change**. The change is reflected in the dialog box.
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the change to the disk subsystem.
10. Click **Yes**. The change is applied to the disk subsystem.

Deleting Host Groups

To delete a host group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Do either of the following:
   - Right-click a host group in the tree view.
   - Right-click **Host Group** in the tree view and then select **Add/Change** from the pop-up menu. Next, in the Add/Change Host Group dialog box, select one or more host groups in the **Host Group List** table and right-click the selection.
4. Select **Delete** from the pop-up menu. A message appears asking whether you want to delete the specified host group(s).
5. Click **Yes** to close the message. If the Add/Change Host Group dialog box still remains displayed, click **OK** to close the dialog box. At this point, the settings in the window have not been applied to the disk subsystem.
6. Click **Apply** in the Volume Security window. A message appears asking whether to apply the change to the disk subsystem.
7. Click **Yes**. The change is applied to the disk subsystem.

Editing LDEV Groups

This section explains the following operations, which allow you to edit your host groups:

- ☐ Deleting Volumes from an LDEV Group
- ☐ Renaming an LDEV Group
- ☐ Deleting an LDEV Group

Deleting Volumes from an LDEV Group

To delete volumes from an LDEV group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click an LDEV group. A pop-up menu appears.
4. Select **Specify** and then **LDEV** from the pop-up menu. The Select LDEV dialog box opens.
5. Use the **CU** list to specify a CU image. The two boxes below the list show volumes in the specified CU image.
   - The **Registered in LDEV group** box shows volumes registered in the LDEV group.
   - The **Not registered in LDEV group** box shows volumes that are not registered in the LDEV group.
6. In the **Registered in LDEV group** box, select volumes that you want to delete. Then, click **Not Regist**. The selected volumes move to the **Not registered in LDEV group** box.
7. If you want to delete volumes in other CU images, return to step 5.
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the settings to the disk subsystem.
10. Click **Yes**. The settings are applied to the disk subsystem.

Renaming an LDEV Group

To rename an LDEV group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Right-click **LDEV Group** or an LDEV group. A pop-up menu appears.
4. Select **Add/Change** from the pop-up menu. The Add/Change LDEV Group dialog box opens.

5. Ensure that the desired LDEV group is selected in the **LDEV Group List** table.
6. In the **Enter LDEV Group** box, enter the new name for the LDEV group.

   Names can be up to eight characters and are case-sensitive. The first character and the last character must not be a space. Also, the following characters are unusable:

   \ , / : ; * ? " < > |
7. Click **Change**. The change is reflected in the dialog box.
8. Click **OK**. At this point, the settings in the window have not been applied to the disk subsystem.
9. Click **Apply** in the Volume Security window. A message appears asking whether to apply the change to the disk subsystem.
10. Click **Yes**. The change is applied to the disk subsystem.

Deleting an LDEV Group

To delete an LDEV group:

1. Ensure that you are in Modify mode.
2. In the Volume Security window, double-click an LDKC number.
3. Do either of the following:
   - Right-click an LDEV group in the tree view.
   - Right-click **LDEV Group** in the tree view and then select **Add/Change** from the pop-up menu. Next, in the Add/Change LDEV Group dialog box, select one or more LDEV groups in the **LDEV Group List** table and right-click the selection.
4. Select **Delete** from the pop-up menu. A message appears asking whether you want to delete the specified LDEV group(s).
5. Click **Yes** to close the message. If the Add/Change LDEV Group dialog box still remains displayed, click **OK** to close the dialog box. At this point, the settings in the window have not been applied to the disk subsystem.
6. Click **Apply** in the Volume Security window. A message appears asking whether to apply the change to the disk subsystem.
7. Click **Yes**. The change is applied to the disk subsystem.

5

Troubleshooting

This chapter provides troubleshooting information for Volume Security and instructions for calling technical support.

Troubleshooting

The Error Detail dialog box may appear when you attempt to apply security settings. The probable causes of the error are:

- Some hosts in one security group are accessing volumes in another security group.
- Some hosts do not belong to any security group, but the hosts are accessing volumes in a security group.

To remove this error, you must find the hosts and the volumes that caused the error. Use the following procedure to find the hosts and the volumes that caused the error:

1. In the Error Detail dialog box, click the arrow button at the right end of the **Host** list.
   - If the list shows only one entry, only one host is causing the error.
   - If the list shows two or more entries, two or more hosts are causing the error.
2. Select a host from the **Host** list.
3. Right-click the arrow button at the right end of the **CU** list, and then check how many CU images are displayed in the list.
   - If the list shows only one entry, the table displays all the volumes that are causing the error.
   - If the list shows two or more entries, some of the error-causing volumes are displayed in the table. To view other error-causing volumes, use the **CU** list to specify another CU image.
4. If two or more hosts are causing the error, please repeat steps 2 and 3.

If error-causing hosts and volumes are detected, do either of the following to remove the error:

- Vary the error-causing volume offline from the error-causing host. For detailed information about varying the volume offline, refer to the documentation for host commands.
- Find the security group that contains the error-causing hosts and the error-causing volumes. Next, disable the security settings of the security group (see Disabling Volume Security).

Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The content of any error message(s) displayed on the host system(s).
- The content of any error message(s) displayed on Storage Navigator.
- The Storage Navigator configuration information (use the FD Dump Tool).
- The service information messages (SIMs), including reference codes and severity levels, displayed by Storage Navigator.

The Hitachi Data Systems customer support staff is available 24 hours/day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Acronyms and Abbreviations

GB	gigabytes (see Convention for Storage Capacity Values)
KB	kilobytes (see Convention for Storage Capacity Values)
LDEV	logical device
LDKC	logical disk controller
MB	megabytes (see Convention for Storage Capacity Values)
M-VOL	main volume
MVS	Multiple Virtual Storage
PB	petabytes (see Convention for Storage Capacity Values)
PC	personal computer
PCB	printed circuit board
R-SIM	remote service information message
R-VOL	remote volume
SI	ShadowImage
SIM	service information message
SIz	ShadowImage for IBM z/OS
SVP	service processor
TB	terabyte (see Convention for Storage Capacity Values)
TC	TrueCopy
TCz	TrueCopy for IBM z/OS
TCzA	TrueCopy Asynchronous for IBM z/OS
T-VOL	target volume

Index

T

V

W

Hitachi Data Systems

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

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

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

Hitachi Data Systems

MK-96RD628-04