

Hitachi Data Ingestor

6.1.1

Single Node Getting Started Guide

This guide provides instructions for setting up Hitachi Data Ingestor (HDI) in a single-node configuration. This guide describes the network configuration, setting up Hitachi Content Platform (HCP), and configuring an HDI environment. Additionally, this guide provides a layout of ports as well as a setup worksheet. The setup procedures described in this guide do not include linking with Hitachi Content Platform (HCP) Anywhere.

© 2017 Hitachi Ltd., All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively, "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" meantext, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.HitachiVantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

- 1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
- 2) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or web site are properties of their respective owners.



Contents

Preface.....	v
Intended audience.....	vi
Product version.....	vi
Release notes.....	vi
Organization of HDI manuals.....	vi
Abbreviation conventions.....	vii
Document conventions.....	viii
Convention for storage capacity values.....	viii
Accessing product documentation.....	viii
Getting help.....	ix
Comments.....	ix
1 Before you begin.....	1-1
Network configuration.....	1-2
2 Getting started.....	2-1
Setting up an HCP system.....	2-2
Configuring an environment.....	2-2
A Layout of the Ports on the Node.....	A-1
Layout of ports.....	A-2
B Setup Worksheet.....	B-1
Worksheet.....	B-2
C Connecting cable and the power switch location of the HDI RS LM system	
.....	C-1
Cable connection.....	C-2
Power switch location.....	C-2



Preface

This manual explains how to set up Hitachi Data Ingestor (HDI) in a single-node configuration when HCP Anywhere is not linked.

- ☐ [Intended audience](#)
- ☐ [Product version](#)
- ☐ [Release notes](#)
- ☐ [Organization of HDI manuals](#)
- ☐ [Abbreviation conventions](#)
- ☐ [Document conventions](#)
- ☐ [Convention for storage capacity values](#)
- ☐ [Accessing product documentation](#)
- ☐ [Getting help](#)
- ☐ [Comments](#)

Intended audience

This manual is intended for system administrators who operate and manage HDI systems in a single-node configuration.

Also, the user must have:

- A basic knowledge of Hitachi Content Platform (HCP) systems
- A basic knowledge of networks
- A basic knowledge of file sharing services
- A basic knowledge of CIFS
- A basic knowledge of NFS
- A basic knowledge of Windows
- A basic knowledge of Web browsers

Product version

This document revision applies to Hitachi Data Ingestor version 4.2.1 or later.

Release notes

Release notes can be found on the documentation CD. Release notes contain requirements and more recent product information that may not be fully described in this manual. Be sure to review the release notes before installation.

Organization of HDI manuals

HDI manuals are organized as shown below.

Note that whether HDI nodes can be set up in a redundant configuration depends on the HDI model. A configuration where nodes are made redundant is called a cluster configuration, and a configuration where a node is not made redundant with another node is called a single-node configuration. Which manuals you need to read depends on which configuration you are going to use.

Manual name	Description
<i>Hitachi Data Ingestor Installation and Configuration Guide, MK-90HDI002</i>	You must read this manual first to use an HDI system. This manual contains the information that you must be aware of before starting HDI system operation, as well as the environment settings for an external server.
<i>Hitachi Data Ingestor Cluster Getting Started Guide, MK-90HDI001</i>	This manual explains how to set up an HDI system in a cluster configuration.

Manual name	Description
<i>Hitachi Data Ingestor Cluster Administrator's Guide</i> , MK-90HDI038	This manual provides procedures for using HDI systems in a cluster configuration, as well as provides GUI references.
<i>Hitachi Data Ingestor Cluster Troubleshooting Guide</i> , MK-90HDI029	This manual provides troubleshooting information for HDI systems in a cluster configuration.
<i>Hitachi Data Ingestor Single Node Getting Started Guide</i> (This manual)	This manual explains how to set up an HDI system in a single-node configuration.
<i>Hitachi Data Ingestor Single Node Administrator's Guide</i> , MK-90HDI039	This manual explains the procedures for using HDI systems in a single-node configuration, as well as provides GUI references.
<i>Hitachi Data Ingestor Single Node Troubleshooting Guide</i> , MK-90HDI030	This manual provides troubleshooting information for HDI systems in a single-node configuration.
<i>Hitachi Data Ingestor CLI Administrator's Guide</i> , MK-90HDI034	This manual describes the syntax of the commands that can be used for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor API References</i> , MK-90HDI026	This manual explains how to use the API for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor Error Codes</i> , MK-90HDI005	This manual contains messages for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor File System Protocols (CIFS/NFS) Administrator's Guide</i> , MK-90HDI035	This manual contains the things to keep in mind before using the CIFS or NFS service of an HDI system in a cluster configuration or a single-node configuration from a CIFS or NFS client.

Note:

Before using the Hitachi Data Ingestor Remote Server (HDI RS LM) system, read the *HDI Remote Server Administrator Guide* (Locally Managed HDI RS).

Abbreviation conventions

This manual uses the following abbreviations for product names:


Abbreviation	Full name or meaning
Active Directory	Active Directory(R)
HCP	Hitachi Content Platform
HDI	Hitachi Data Ingestor
HDI RS LM	Locally Managed Hitachi Data Ingestor Remote Server
Windows	Microsoft(R) Windows(R) Operating System

Document conventions

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 .
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <i>copy source-file target-file</i> Note: Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: # <code>pairedisplay -g oradb</code>

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

Icon	Label	Description
	Note	Calls attention to important and/or additional information.

Convention for storage capacity values

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

Capacity Unit	Physical Value	Logical Value
1 KB	1,000 bytes	1,024 (2^{10}) bytes
1 MB	1,000 KB or $1,000^2$ bytes	1,024 KB or $1,024^2$ bytes
1 GB	1,000 MB or $1,000^3$ bytes	1,024 MB or $1,024^3$ bytes
1 TB	1,000 GB or $1,000^4$ bytes	1,024 GB or $1,024^4$ bytes
1 PB	1,000 TB or $1,000^5$ bytes	1,024 TB or $1,024^5$ bytes
1 EB	1,000 PB or $1,000^6$ bytes	1,024 PB or $1,024^6$ bytes
1 block	-	512 bytes

Accessing product documentation

Product documentation is available on Hitachi Data Systems Support Connect: https://support.hds.com/en_us/documents.html. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

[Hitachi Data Systems Support Connect](https://support.hds.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Data Systems. To contact technical support, log on to Hitachi Data Systems Support Connect for contact information: https://support.hds.com/en_us/contact-us.html.

[Hitachi Data Systems Community](https://community.hds.com) is a global online community for HDS customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hds.com, register, and complete your profile.

Comments

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

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

Before you begin

Hitachi Data Ingestor (HDI) is a system that provides file system services to clients on a network. Hitachi Content Platform (HCP) can also be linked to an HDI system to provide a file system service and efficiently manage the huge amount of data that accumulates daily. This manual explains HDI systems in single-node configurations. This chapter describes what the system administrator needs to understand before setting up an HDI system in a single-node configuration.

For information about the network configuration of the HDI RS LM system, see the *HDI Remote Server Administrator Guide* (Locally Managed HDI RS).

□ [Network configuration](#)

Network configuration

Single-node HDI systems have a basic system configuration consisting of two ports: one used for system management and data access (`mng0`), and one used by maintenance personnel for maintenance operations (`pm0`). It is also possible to trunk multiple ports used for system management and data access.

The following explains the network configuration for an HDI system.

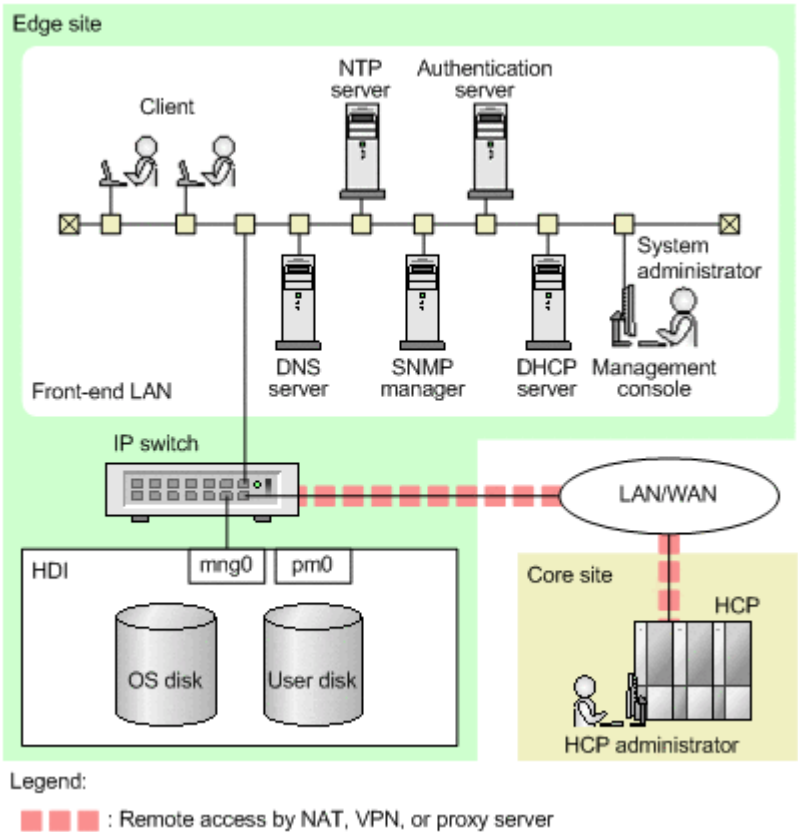


Figure 1-1 HDI system network configuration example

In addition to HDI, external servers are also needed to provide services to clients. For details about the environment settings for each external server, see the corresponding sections in the *Installation and Configuration Guide*.

When file systems are created on an HDI system in a single-node configuration, the internal hard disk in the node and the disk space in the storage system are logically partitioned and assigned. The following table describes the meaning of the terms used when creating a file system on an HDI system in a single-node configuration.

Table 1-1 Terms used when creating a file system

Terms	Meaning
LU	An abbreviation of <i>logical unit</i> . This refers to a logical disk partition.

Terms	Meaning
	<p>For an HDI system, LUs must be used that were created on the internal hard disk of the node or in a storage system.</p> <p>To use a storage system, ask the storage system administrator to create LUs for you.</p> <p>When the internal hard disk in the node is used, LUs are automatically allocated from the internal hard disk when the OS on the node starts. The system administrator does not need to create LUs.</p>
Volume group	<p>A unit that is used to manage LUs on the internal hard disk and in storage systems in order to store user data, such as file systems.</p> <p>You can allocate multiple LUs to a volume group. If you create LUs, the LUs will be automatically allocated to volume groups when you log in to the GUI. When LUs are automatically allocated to volume groups, volume groups are created for like LUs, which are divided up based on the drive type (or pool for virtual LUs) of the LUs and the chassis (internal hard drive or storage system) the LUs are stored in.</p> <p>A certain amount of capacity in a volume group is allocated to a file system. A volume group can be used by multiple file systems.</p>

Getting started

This chapter explains how to use the **System Configuration Wizard** and **Service Configuration Wizard** to perform setup.

Prepare the required information before starting setup. You can use [Appendix B, Setup Worksheet on page B-1](#) as a worksheet for collecting information.

Note:

In this chapter, "HDI system" is used to refer to both the HDI system and the HDI RS LM system.

- ☐ [Setting up an HCP system](#)
- ☐ [Configuring an environment](#)

Setting up an HCP system

Before you can start setup, the HCP administrator needs to configure an HCP environment and prepare a tenant to be assigned to the HDI system.

The HCP management API (MAPI) must be enabled for an HCP system connected to an HDI system. The following settings must be configured for tenants that are assigned to the HDI system:

- Grant the Monitor, Administrator, Compliance, and Security roles to the user account.
- Set a hard quota for the tenant capacity.
- Allow retention mode to be selectable.
- Enable the versioning functionality.
- If the version of the linked HCP system is 4.1 or later, specify a value of at least *number-of-file-system-namespaces* + 1 for the namespace quota.
- Enable the HCP management API (MAPI).

To use the replication functionality on the HCP system after a migration to the HCP system has been started, the replication functionality must be enabled for all the namespaces, including the namespace that contains the system settings file (*system-backup-data*).

Configuring an environment

The following describes how to use the GUI to configure an HDI environment. For details about the displayed GUI items, see the *Single Node Administrator's Guide*. For details about management-console machine requirements and Web browser settings (such as pop-up blocks and security settings), see the *Installation and Configuration Guide*.

1. To use UPnP (Universal Plug and Play), configure the following settings on the management console.
 - Enable **Network discovery**
 - Configure the firewall to allow UDP port communication (port number: 1900)
 - On the screen for managing Windows services, start **SSDP Discovery**



Note: When the HDI system is first installed, UPnP can be used. If there is no need to use UPnP, disable UPnP by using the `upnpctl` command after finishing setting up.

2. Access HDI on the management console.

When using UPnP, in **Other Devices** in the management console network list, click the icon representing HDI.

If UPnP is not used, launch the Web browser, and enter a URL in the following format in the address bar:

```
https://HDI-IP-address-or-host-name/admin/
```


3. In the Login window, enter the following user ID and password, and click the **Login**.
 - **User ID:** admin
 - **Password:** chang3me!
4. If you are accessing the GUI for the first time, in the **Change System Admin Password** dialog box, change the password, and then click the **OK**.
Provisioning Wizard is started if you make the setting for the first time. If linking to HCP Anywhere is needed, follow the instructions from the HCP Anywhere administrator.
 If linking to HCP Anywhere is unneeded, click the **Manual Settings** on the **1. Introduction** page. A confirmation dialog box is displayed, and then **System Configuration Wizard** is started. Move on to the next step.
5. On the **1. Introduction** page of **System Configuration Wizard**, click **Next**.
6. On the **2. License Settings** page, set the license and then click **Next**. To set the license, you can specify a license key file or directly enter a license key string into the dialog box.
 If the license for the following software is specified, encryption-related functions^{#1} cannot be used to save, send, or receive user data:
 - Base software without DIFE
7. On the **3. Basic Settings** page, enter the following information, and then click **Next**.
 Registering node network information:
 - Host name
 - Whether to configure network information (information used for system management such as IP addresses or netmasks) on a node by using DHCP
 - System management IP address (when DHCP is not used)
 - Netmask or prefix length (when DHCP is not used)
 - IP address of the default gateway (optional) (when DHCP is not used)
 Registering the DNS server:
 - IP address of the primary server (optional when DHCP is used)
 - IP address of the secondary server (optional)
 - Default domain name (optional)
 Setting the time on the node:
 - Time zone
 - Specify the NTP server name, or specify the time manually.
 Encryption settings (If an encryption license is set):
 - Whether to encrypt local data (internal hard disks containing user data)

- Whether to encrypt data to be stored in an HCP system
8. On the **4. Confirmation** page, check the displayed information, select the check box, and then click **Apply**.
The **5. Execution** page appears, and setup of the system starts.
When setup finishes, the **6. Completion** page appears.
 9. On the **6. Completion** page, check the processing results, and then click the displayed URL.
 10. In the Login window, enter the user ID and password, and then click **Login**.
If a dialog box prompts you about whether you want to automatically allocate LUs to the volume group, click **Yes**. Check the processing results, and then click **Close**.
The Service Configuration Wizard starts when you configure the environment the first time. To manually start the Service Configuration Wizard, from the **Action** menu in the upper-left corner of the GUI, choose **Configuration Wizards**, and then **Service Configuration Wizard**.
When the wizard has started, go to step 19.
However, if you are creating a file system in the internal hard disk of the node and want to change the RAID level of the disk, go to the next step without logging on to the system.
 11. Use the `internalraidlevelset` command to change the RAID level setting.
 12. Use the `internalraidlevelget` command to make sure that the RAID level setting has been changed.
 13. Use the `vgrdelete` command to delete the volume group.
 14. Use the `internalludelete` command to delete the registration of the user disk.
 15. After executing the `lumaplist` command, execute the `hwstatus` command and check the status of the internal hard disk.
Make sure that the RAID level has been changed to the value you specified in step 11.
 16. From the Web browser, log on again to the system.
A dialog box that asks you whether you want to automatically allocate LUs to the volume group appears.
 17. Click **Yes**.
 18. Check the processing results, and then click **Close**.
The **Service Configuration Wizard** starts.
 19. On the **1. Introduction** page, click **Next**.
 20. To link with an HCP system, select the check box in the **2. HCP Settings** page, and then specify the HCP information described below. To use a proxy server for communication between a node and the HCP system, you also need to specify the proxy server information.
If you do not want to link with the HCP system, go to step 22.
Registering HCP information:

- System name (host name in FQDN format)
- Tenant name
- Host name or IP address that has been made external and is used to connect to the HCP system (if any relay device such as a load balancer is used when connecting the linked HCP system to the network)
- User name and password of the tenant administrator
To change a password issued by an HCP administrator, enter the new password.
- Replica HCP system name (when the replication function is used on the HCP system)
- Host name or IP address that has been made external and is used to connect to the replica HCP system (if any relay device such as a load balancer is used when connecting the replica HCP system to the network)

Registering proxy server information:

- Host name
- Port number
- User name and password

21. Click **Test Connection**.

Check the connection for communicating with the HCP system.

22. Click **Next**.

23. On the **3. Resource Settings** page, select whether to allocate the file system capacity automatically or manually.

If the file system is linked to the HCP system at the share level, you must manually allocate the file system capacity.

24. In the **Create File Systems** area, click **Add**.

25. Of the following information, specify the necessary information required for each file system, and then click **Next**:

- File system name
- Client access protocol (CIFS, NFS, or both)
- Storage destination of the file system (when multiple volume groups exist): Chassis (internal hard disk or storage system), volume groups
- Capacity (for manual allocation)
- Whether the WORM functionality is enabled
- Whether to enable the CIFS bypass traverse checking
- Name of the shared directory
- CIFS share options: name of the CIFS share, whether to automatically create the home directory in the CIFS share, and whether to encrypt the communication with CIFS clients if you use SMB 3.0
- Client host or network whose access to a file share is restricted
- Access permission settings when creating a new CIFS file or directory

- ACL settings for the shared directory

To link with the HCP system, you need to specify the following information:

- How the HCP system is linked to (at the file system or share level)
- How the data is shared with other HDI systems via the linked HCP system (Content sharing setting: Off, On (Read-Only), On (Read/Write), or Home directory)
- If you do not synchronize data with other HDI systems via the linked HCP system (the content sharing setting is Off), the following information is also required:
 - Namespace quota for the data migration destination^{#2}
 - Data migration schedule: Initial start date, execution interval, start time, maximum execution time
 - Whether to create an account for accessing a namespace^{#2}
 - Whether to show clients the past version files (past version directories) that were migrated to the HCP system
- If you want to reference data from other HDI systems as read-only (the content sharing setting is On (Read-Only)), the following information is also required:
 - Name of the namespace in which data of other HDI systems is referenced as read-only^{#2}
 - Host name or IP address that has been made external and is used to connect to the HCP system (if any relay device such as a load balancer is used when connecting the linked HCP system to the network)^{#2}
 - User name and password of the namespace-access account^{#2}
 - Replica system name of the HCP system to be referenced^{#2}
 - Host name or IP address that has been made external and is used to connect to the replica HCP system (if any relay device such as a load balancer is used when connecting the replica HCP system to the network)^{#2}
- If you want to use the read-write-content-sharing functionality for sharing data among HDI systems (the content sharing setting is On (Read/Write)), the following information is also required:
 - Whether to create a namespace for the data-migration destination when the file system is created or to use a previously-created namespace
 - Quota allocated to the namespace (when a namespace is created)
 - Name of the namespace (when using a previously-created namespace)
 - Whether to show clients the past version files (past version directories) that were migrated to the HCP system
- If you want to enable roaming among HDI systems for home directory data created for each end user (the content sharing settings is Home directory), the following information is also required:

- Whether to create a namespace for the data-migration destination when the file system is created or to use a previously-created namespace
- Quota allocated to the namespace (when a namespace is created)
- Name of the namespace (when using a previously-created namespace)
- Whether to show clients the past version files (past version directories) that were migrated to the HCP system

#2:

This item can be specified if the file system is linked to the HCP system at the file system level.

If the file system is linked to the HCP system at the share level, do the following after the file system is created: Use the **Add Share** dialog box to add the file share directly under the mount point, and then allocate the namespace to the file share. For details about the **Add Share** dialog box, see the *Single Node Administrator's Guide*.

26. On the **4. CIFS User Authentication Settings** page, select the CIFS user authentication method.
An authentication method that is neither Active Directory authentication nor local authentication by the node OS can be selected if a domain controller within the domain authenticates users when IPv4 is used. In this case, after the wizard is finished, set the appropriate information in the **Access Protocol Configuration** dialog box.
27. If you select Active Directory authentication or local authentication by the node OS, specify the following information and then click **Next**. If you select any other authentication method, click **Next** without specifying anything.
When Active Directory authentication is selected
 - o DNS name
 - o User name and password for the domain controller
 When local authentication is selected
 - o Workgroup name
 - o User name and user ID (optional)
 - o Name and ID of the group to which the user belongs (optional)
 - o User password (optional)
28. Check the information displayed on the **5. Confirmation** page, select the check box, and then click **Apply**.
The **6. Execution** page appears, and setup of the service starts.
When setup finishes, the **7. Completion** page appears.
29. On the **7. Completion** page, check the processing results, and then click **Finish**.
30. Choose **Resources** tab in the top-left corner of the GUI.
31. From the tree on the left side of the GUI, click *host-name*.
The *host-name* window opens.

32. In the *host-name* window, click **Backup Configuration** in the **Settings** area.
The **Backup Configuration** dialog box opens.
33. On the **Save System Settings Menu** page, click **Save All System Settings**.
34. On the **Save All System Settings** page, click **Download**, and download the system settings file to storage media outside the system.
The system settings information is downloaded.



Note: If an error occurs in the HDI system, you can use the system settings file and backed up data to restore file systems. The system administrator must download the system settings file to storage media outside the system whenever the HDI system configuration is changed. If the HDI system is linked to the HCP system, then after you start using the HDI system, the system settings file is periodically saved to the HCP system.

35. If encrypting data to be stored in an HCP system, save the common key used for encryption outside the system.
The following describes how to save the common key used for encryption outside the system.
- Set up an SSH environment to use commands.
For the settings for using commands, see the *Single Node Administrator's Guide*.
 - Use the `hcpdisplaykey` command to display the key to be saved on external storage media, and then save the key.
 - Use the `hcpverifykey` command to verify the common key saved on an OS disk and the key saved on external storage media.



Note: If you are using the local data encryption functionality, and then you periodically save the system configuration information on the HCP system, when an encryption key saved on the HCP system cannot be obtained, user data will no longer be available. To prepare for failures, after enabling the encryption functionality, we recommend that you use the `encdisplaykey` command to display the key to save on storage media outside the system, and then save the key. After saving the key on storage media outside the system, use the `encverifykey` command to cross-check the key that is saved on the HCP system and the key saved on storage media outside the system.

#1:

The following functions cannot be used:

- Communication with HCP using HTTPS
- SFTP service
- Encryption of communication with CIFS clients (SMB encryption)
- Use of the `krb5p` security flavor in NFS services
- Encryption of local data
- Encryption of data to be stored in HCP

If you attempt to use the CLI or API to enable these functions, the KAQM14180-E message is output and the attempt fails. In addition, you cannot enable these functions by using the GUI.

Layout of the Ports on the Node

This appendix describes the layout of **ports**.

- [Layout of ports](#)

Layout of ports

This section describes the layout of ports on the various types of nodes. The following figures show the layout of the ports on nodes. You can check the model name of the node by using the `hwstatus` command.

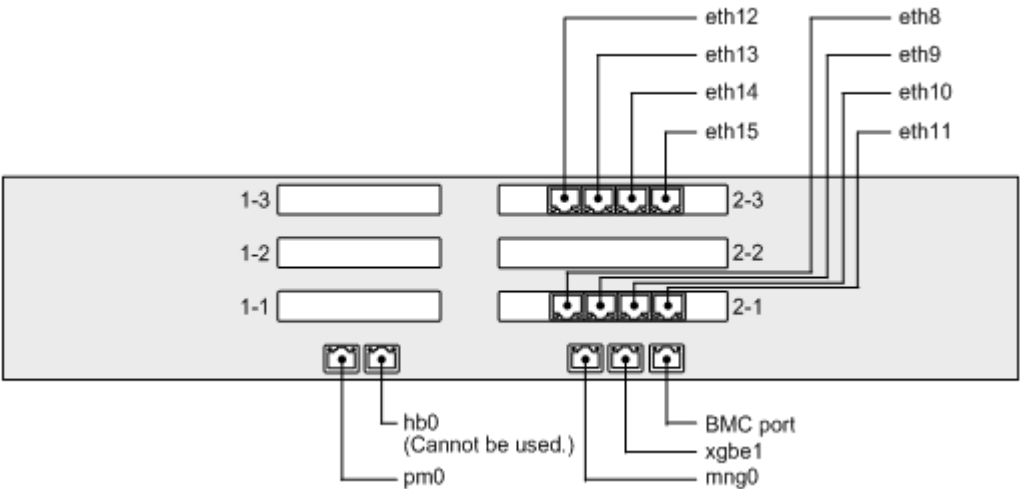


Figure A-1 Port layout example (when the node model is D51B-2U, and a GbE card is in an expansion slot)

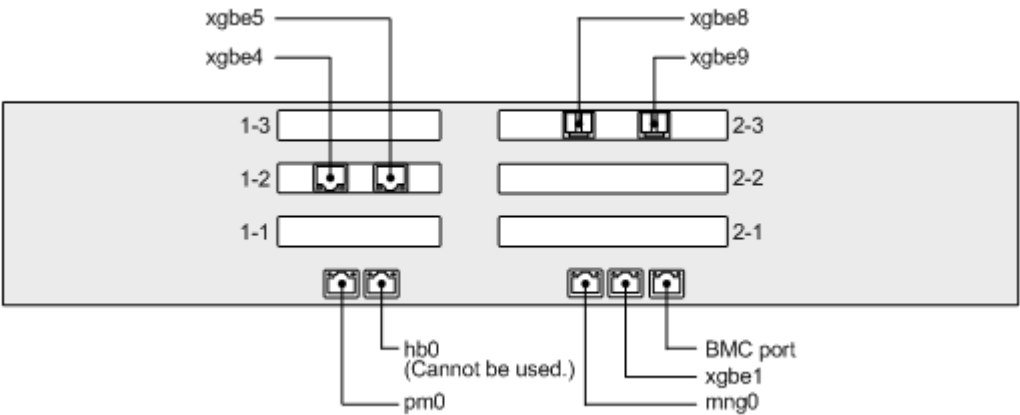


Figure A-2 Port layout example (when the node model is D51B-2U, and a 10GbE card is in an expansion slot)

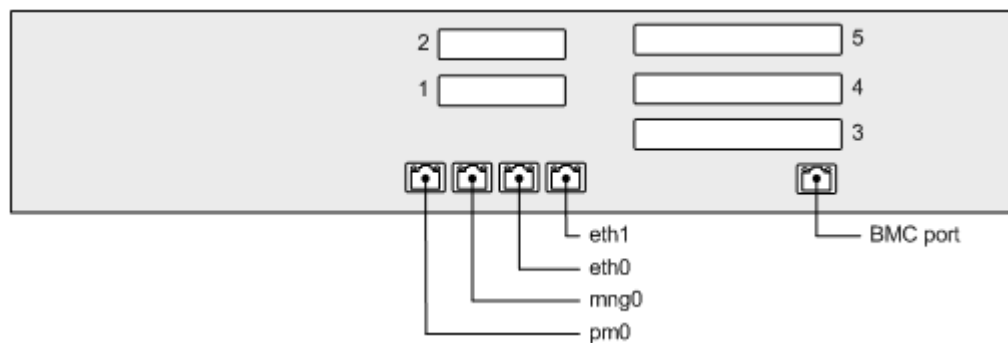


Figure A-3 Port layout example (when the node model is Compute Rack 220S)

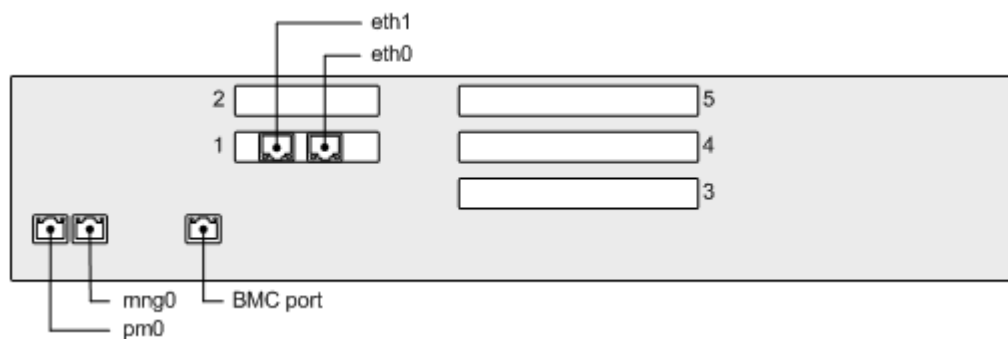


Figure A-4 Port layout example (when the node model is Compute Rack 220)

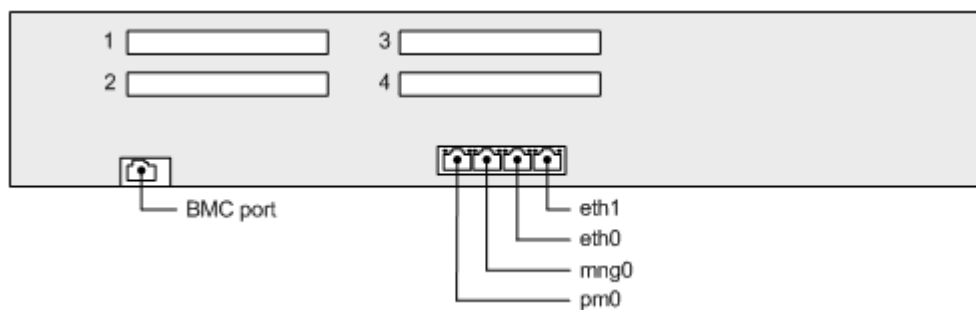


Figure A-5 Port layout example (when the node model is PowerEdge)



Setup Worksheet

This appendix provides a worksheet used for collecting necessary information for setup.

☐ [Worksheet](#)

Worksheet

We recommend that you prepare the following information before starting setup. For details about the HCP information, contact your HCP administrator.

Table B-1 Setup worksheet

Type of information	Item		Input value
License	License key file or license key		
Node network information (when DHCP is used)	Host name ^{#1}		
	Use DHCP to set the node network information		Yes
Node network information (when DHCP is not used)	Host name ^{#1}		
	Use DHCP to set the node network information		No
	IPv4 settings	IP address used for system management	
		Netmask	
		IP address of the default gateway ^{#2}	
	IPv6 settings	IP address used for system management	
		Prefix length	
		IP address of the default gateway ^{#2}	
DNS server	IP address of the primary server		
	IP address of the secondary server		
	Default domain name		
NTP server	NTP server name		
Encryption setting ^{#3}	Whether to encrypt local data (internal hard disks containing user data)		Yes / No
	Whether to encrypt data to be stored in an HCP system		Yes / No
HCP	System name (host name in FQDN format)		
	Tenant name		
	Host name or IP address that has been made external and is used to connect to the HCP system		

Type of information	Item		Input value
	User name and password of the tenant administrator user account		User name: Password issued by the HCP administrator: New password (when changing the password issued by an HCP administrator):
	Replica system name (host name in FQDN format)		
	Host name or IP address that has been made external and is used to connect to the replica HCP system		
Proxy server used for communication with HCP	Host name		
	Port number		
	User name and password when user authentication is used in the proxy server		
Allocation method for file system capacity	Automatic or manual ^{#4}		
File system	File system name ^{#5}		
	Client access protocol		CIFS / NFS / both
	How the HCP system is linked to ^{#4}		At the file system level / At the share level / Namespaces are not used
	Content sharing setting ^{#6}		Off / On (Read-Only) / On (Read/Write) / Home directory
	When the content sharing setting is "Off"	Quota for the data migration-destination namespace	
		Data migration schedule	First start date: Execution interval (15 minutes to a week): Start time: Maximum execution time (0 to 23 hours) ^{#7} :
		Create a namespace-access account	Yes / No Password:
		Show clients the past version files (past version)	Yes / No Custom schedule:

Type of information	Item		Input value
		directories) that were migrated to the HCP system	Number of days to wait until past versions of files are deleted (1 to 36,500 days):
	When the content sharing setting is "On (Read-Only)"	Name of the namespace (FQDN) in which data of other HDI systems is referenced as read-only	
		Host name or IP address that has been made external and is used to connect to the HCP system	
		Namespace-access account	User name: Password:
		Replica system name of the HCP system being referenced (host name in FQDN format)	
		Host name or IP address that has been made external and is used to connect to the replica HCP system	
	When the content sharing setting is "On (Read/Write)"	Create a data-migration-destination namespace when the file system is created	Yes / No
		Quota for the data migration-destination namespace (when a namespace is created)	
		Name of the migration-destination namespace (when using a previously created namespace)	
		Show clients the past version files (past version	Yes / No Custom schedule:

Type of information	Item		Input value
		directories) that were migrated to the HCP system	Number of days to wait until past versions of files are deleted (1 to 36,500 days):
	When the content sharing setting is "Home directory"	Create a data-migration-destination namespace when the file system is created	Yes / No
		Quota for the data migration-destination namespace (when a namespace is created)	
		Name of the migration-destination namespace (when using a previously created namespace)	
		Show clients the past version files (past version directories) that were migrated to the HCP system	Yes / No Custom schedule: Number of days to wait until past versions of files are deleted (1 to 36,500 days):
	Storage destination of the data in the file system (when multiple volume groups exist)		Internal hard disk / storage system storage system name:
	Volume group name used by the file system (when multiple volume groups exist)		
	Capacity (when allocated manually)		
	Enable WORM functionality ^{#8#9}		Yes / No
	Enable CIFS bypass traverse checking ^{#8}		Yes / No
	Shared directory name ^{#10}		
	CIFS share options		CIFS share name ^{#11} : Whether to automatically create the home directory in the CIFS share: Yes / No Encrypting communication with CIFS clients when you use SMB 3.0: Follow the configuration definition of the CIFS service / Encrypt the communication only

Type of information	Item	Input value
		when the client supports encryption / Always encrypt the communication / Do not encrypt the communication
	Host or network whose access to a CIFS share is restricted ^{#12}	
	Access permission settings when creating a new CIFS file or directory	Owner: RW / RO / None Owner group: RW / RO / None Others: RW / RO / None
	Client host or network specified as a public destination in NFS ^{#12}	Host name or network address: Users to be mapped as anonymous users: Anonymous user mapping is not performed / Only the root user / All users
	ACL settings for the shared directory	When the client access protocol is CIFS, or both CIFS and NFS: User name / group name: Access permission: Apply the settings to subfolders and files: Yes / No When the client access protocol is NFS: Owner of the shared directory: Owner group of the shared directory: Access permission for the shared directory: Set a sticky bit in the shared directory: Yes / No
CIFS user authentication (When Active Directory is used) ^{#13}	Domain DNS name ^{#14}	
	User name and password for the domain controller	User name: Password:
CIFS user authentication (when local authentication is used)	Workgroup name ^{#15}	
	Newly created user ^{#16}	User name: User ID (200 to 2147483147): Name of group to which user belongs: ID of group to which user belongs (200 to 2147483147): User password:

#1: The host name can have a maximum of 15 characters. You can use alphanumeric characters including hyphens (-). The host name must begin with an alphabetic letter, and must not end with a hyphen (-). You cannot also specify system-reserved words in upper case or lower case. For details about reserved words, see the *Single Node Administrator's Guide*. Note that in the initial settings, a unique name is assigned to each node.

#2: Required when connected through a router to an external network segment.

#3: You can specify this when an encryption license is set. For details on encrypting local data and the data to be stored in an HCP system, see the *Installation and Configuration Guide*.

#4: If the file system linked to the HCP system at the share level, you must manually allocate the file system capacity. If the file system linked to the HCP system at the file system level, you can select whether to allocate the file system capacity automatically or manually. When the file system capacity is automatically allocated, the capacity of the volume group that can be used by each file system depends on the quota allocated to the HCP namespace for the file system. For example, if you create three file systems for a volume group with a total capacity of 1 TB, and the namespace quota for each file system is 400 GB, 600 GB, and 1 TB, allocated capacities are as follows:

- File system 1 (with a namespace quota of 400 GB): 200GB
- File system 2 (with a namespace quota of 600 GB): 300GB
- File system 3 (with a namespace quota of 1 TB): 500GB

All the capacity in the volume group used by the file systems is allocated to the file systems. You can check automatically allocated capacities of file systems from a window. After checking the capacities, if necessary, change the setting so that the capacities can be manually allocated.

#5: Specify this item using 16 or fewer alphanumeric characters or underscores (_).

#6: For content sharing, specify how to share data with other HDI systems via the linked HCP.

- Off: Do not synchronize the data with other HDI systems.
- On (Read-Only): Reference the data of other HDI systems as read-only.
- On (Read/Write): Use the read-write-content-sharing functionality to share the data among HDI systems. Make sure that the file system is linked to the HCP system at the file system level.
- Home directory: The home-directory-roaming functionality is used. Roaming among HDI systems is enabled for home directory data created for each end user. The CIFS protocol must be set for the client access protocol. Make sure that the file system is linked to the HCP system at the file system level.

#7: Specify the maximum time a migration can take. To not set a limit, specify 0.

#8: This function cannot be enabled if the home-directory-roaming functionality is used.

#9: Once a file system is created, whether the WORM functionality is enabled cannot be changed for the file system.

If the WORM functionality is enabled, the following default settings are used for the WORM settings:

- Minimum retention period: 0 days, 0 hours, and 0 minutes
- Maximum retention period: Infinite

#10: If the NFS protocol is used, make sure that the total length of the file system name and directory path is no more than 58 characters. The characters that can be used to specify this item are alphanumeric characters and the following symbols:

- . / _

If only the CIFS protocol is used, make sure that the total length of the file system name and directory path is no more than 251 characters. The characters that can be used are alphanumeric characters, spaces, and the following symbols. You can also specify multibyte characters.

! # \$ % & ' () + , - . / ; = @ [] ^ _ ` { } ~

#11: This item must be specified with no more than 80 characters. The characters that can be used are alphanumeric characters, spaces, and the following symbols:

! # \$ % & ' () + , - . ; = @ [] ^ _ ` { } ~

You can also specify multibyte characters. However, you cannot specify only a dollar sign or periods (e.g., \$, ., or ..) in the string, and you cannot specify a period at the end (e.g., Abc.). If the string ends with a dollar sign, you cannot specify a period just before the dollar sign (e.g., Abc.\$). Spaces specified at the end are deleted.

In addition, the CIFS share name cannot be `global`, `homes`, `printers`, `admin`, `$`, `c$`, `global$`, `homes$`, `ipc$`, or `printers$`.

In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.

The maximum of 1,024 NFS shares can be created. The maximum number of CIFS shares varies depending on whether the configuration definition of the CIFS service is set so that the settings on CIFS shares are automatically reloaded and applied to the CIFS client environment. For details about the maximum number of CIFS shares, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

#12: For details about the specification format, see the explanation of the **Edit CIFS Share Host or Network** dialog box or **Edit NFS Share Host or Network** dialog box in the *Single Node Administrator's Guide*.

#13: If Active Directory is used for user authentication, only users authenticated by Active Directory can access CIFS shares. Users locally authenticated by the HDI system cannot access CIFS shares.

If **Custom settings** is selected, the domain name (NetBIOS), the server name or the IP address of the domain controller, and user mapping form can also be specified. If **Custom settings** is not selected, a domain name (NetBIOS) and up to five DC servers based on the specified domain name (DNS) are automatically searched for and set. When only the CIFS protocol is used, RID user mapping is selected and an ID range from 70000 through 4069999 (4,000,000 IDs) is set for the domain name (NetBIOS) that was automatically searched for. When both the CIFS and the NFS protocol are used, Active Directory schema-form user mapping is selected, and the RFC2307 schema is set to be used for acquiring user IDs and group IDs from the domain controller.

#14: All entered lowercase characters are recognized as uppercase characters. For use as both an Active Directory domain controller and KDC server, the name specified here is used as the name of the domain to which the KDC server belongs.

#15: Specify a name other than the host name.

#16: User names already registered in the HDI system, the NIS server, or LDAP server used for user authentication cannot be specified for the user name and group name. Specify a name no longer than 16 characters. The first character must be an alphanumeric character. The second and subsequent characters can be alphanumeric characters, hyphens (-), or underscores (_). Entered uppercase characters and lowercase characters are treated the same by Windows. Specify a name that is unique regardless of case. Names in the list of reserved terms in the *Single Node Administrator's Guide* are reserved by the OS and cannot be specified.

Also, the names used for existing groups set to use ACL functionality cannot be specified as user names.

IDs already registered in the HDI system, the NIS server, or LDAP server for user authentication, and also the ID 65534 cannot be specified. When user mapping is used, IDs in the range set for user mapping cannot be specified.

Passwords must be specified between 6 and 20 characters. You can specify the alphanumeric characters and the following symbols:

! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

Connecting cable and the power switch location of the HDI RS LM system

This chapter provides information about cable connection and the power switch location of the HDI RS LM system.

- ☐ [Cable connection](#)
- ☐ [Power switch location](#)

Cable connection

The following figure shows the cable connection of the HDI RS LM system.

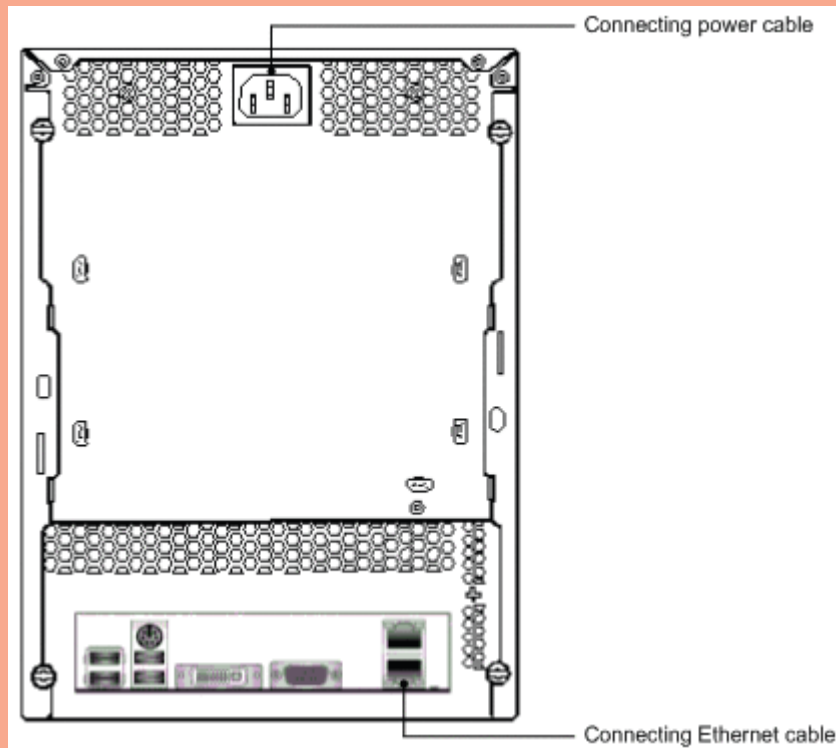


Figure C-1 Cable connection

Power switch location

The following figure shows the power switch location of the HDI RS LM system.

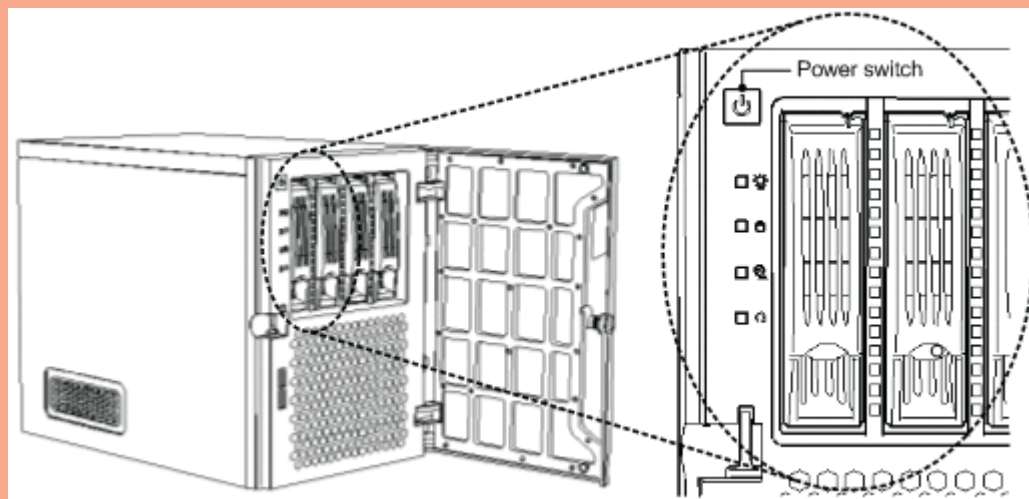


Figure C-2 Power switch location

Hitachi Vantara



Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.com
community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com