

Hitachi Dynamic Link Manager (for VMware®) 8.8.3-04 Release Notes

Contents

About this document.....	1
Intended audience.....	1
Getting help.....	2
Accessing product downloads.....	2
About this release.....	2
Product package contents.....	2
New features and important enhancements.....	3
System requirements.....	3
Resolved problems.....	5
Known problems.....	6
Installation precautions.....	12
Usage precautions.....	14
Documentation.....	17
Appendix A.....	18
Copyrights and licenses.....	38

About this document

This document (RN-91HC190-46, August 2022) provides late-breaking information about Hitachi Dynamic Link Manager (for VMware) 8.8.3-04. It includes information that was not available at the time the technical documentation for this product was published, as well as a list of known problems and solutions.

Intended audience

This document is intended for customers and Hitachi Vantara partners who license and use Hitachi Dynamic Link Manager (for VMware).

Getting help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information:

https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for 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.hitachivantara.com, register, and complete your profile.

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: <https://support.hitachivantara.com/>.

Log in and select Product Downloads to access the most current downloads, including important updates that may have been made after the release of the product.

About this release

This is a minor release that adds new features and resolves multiple known problems.

Product package contents

Medium	CD-ROM	Revision	Release Type	Prerequisite version of Service Pack
Software	Hitachi Dynamic Link Manager (for VMware)	8.8.3-04	Full Package	-

New features and important enhancements

8.8.3-03 Additional Functions and Modifications

- A function that suppresses path failure messages is now supported.
For details, see Appendix A.

8.8.3-02 Additional Functions and Modifications

- VMware vSphere ESXi 7.0 Update 3 is now supported.
However, ESXi 7.0U3, ESXi 7.0U3a, and ESXi 7.0U3b are not supported.

8.8.3-00 Additional Functions and Modifications

- VMware vSphere ESXi 7.0 Update 2 is now supported.
- The version of JDK that bundled with HDLM has been changed to 11.0.
- The log utility bundled with HDLM has changed from Log4j1 1.2.3 to Log4j2 2.17.1.

System requirements

For system requirements, see Chapter 3. Creating an HDLM Environment in the Hitachi Dynamic Link Manager (for VMware®) User Guide.

Host

For details on supported hosts, see Chapter 3. Creating an HDLM Environment in the Hitachi Dynamic Link Manager (for VMware®) User Guide.

Creating an HDLM Environment - HDLM System Requirements - Hosts and OSs Supported by HDLM

Host Bus Adapter (HBA)

Applicable HBAs and HBA drivers:

- Inbox driver for ESXi 6.5/6.7/7.0 or HBA drivers that support ESXi 6.5/6.7/7.0 as listed in VMware Compatibility Guide.
- HBAs and HBA drivers for BladeSymphony that support ESXi 6.5/6.7/7.0 as listed in VMware Compatibility Guide.

Storage

For supported storage systems, see Chapter 3. Creating an HDLM environment in the Hitachi Dynamic Link Manager (for VMware®) User Guide.

Creating an HDLM Environment - HDLM System Requirements - Storage Systems Supported by HDLM

Operating Systems Requirements

The following operating systems are supported.

- VMware vSphere ESXi 6.5 Update 3 Standard Edition/ Enterprise Edition/ Enterprise Plus Edition
Only ESXi 6.5 P06 or later versions are supported.
- VMware vSphere ESXi 6.7 Update 3 Standard Edition/ Enterprise Edition/ Enterprise Plus Edition
Only ESXi 6.7 P03 or later versions are supported.
- VMware vSphere ESXi 7.0 Standard Edition/ Enterprise Edition/ Enterprise Plus Edition
- VMware vSphere ESXi 7.0 Update 1 Standard Edition/ Enterprise Edition/ Enterprise Plus Edition
- VMware vSphere ESXi 7.0 Update 2 Standard Edition/ Enterprise Edition/ Enterprise Plus Edition
- VMware vSphere ESXi 7.0 Update 3 Standard Edition/ Enterprise Edition/ Enterprise Plus Edition
However, ESXi 7.0U3, ESXi 7.0U3a, and ESXi 7.0U3b are not supported.
For details on the versions of ESXi, see VMware's Knowledge Base such as KB2143832.

Prerequisite Programs

Host

None

Remote management host

- NET Framework 4.7 or a later version
When using VMware vSphere CLI
- VMware vSphere CLI 6.5/6.7

When using VMware PowerCLI

- VMware PowerCLI 11.3/11.4/11.5/12.0/13.0

Resolved problems

8.8.3-04 Modifications

The following problems have been corrected:

- If you set only the execution policy for LocalMachine scope to RemoteSigned in Windows 10, an attempt to connect to the ESXi host by using the HDLM command fails, and the KAPL01148-E message is output.
- The following vulnerabilities related to the Java that comes with HDLM. CVE-2022-21434, CVE-2022-21443, CVE-2022-21476, CVE-2022-21496

8.8.3-02 Modifications

- The following vulnerabilities related to the Java that comes with HDLM. CVE-2022-21248, CVE-2022-21271, CVE-2022-21277, CVE-2022-21282, CVE-2022-21283, CVE-2022-21291, CVE-2022-21293, CVE-2022-21294, CVE-2022-21296, CVE-2022-21305, CVE-2022-21340, CVE-2022-21341, CVE-2022-21360, CVE-2022-21365, CVE-2022-21366

8.8.3-00 Modifications

The following problem have been corrected:

- During an unattended installation of HDLM, if no value is specified for installfile_location in the installation-information settings file, or the installfile_location itself is omitted, the following message is incorrectly output: "KAPL09195-W The setup.exe file does not exist."
- The following vulnerabilities related to the JRE that comes with HDLM. CVE-2021-2341, CVE-2021-2369, CVE-2021-2388, CVE-2021-35567, CVE-2021-35550, CVE-2021-35586, CVE-2021-35564, CVE-2021-35556, CVE-2021-35559, CVE-2021-35561, CVE-2021-35565, CVE-2021-35578, CVE-2021-35603, CVE-2021-35588

Known problems

- When you remove HDLM by using removehdlm (utility for Removing HDLM) in "HDLM-installation-folder\bin", perform the following operations.
 - "HDLM-installation-folder\bin" is not deleted. Delete "HDLM-installation-folder".
 - The dialog box "removehdlm is in use" is displayed during a remove. Select "Continue" to continue the remove.

The above phenomena can be avoided by performing either of the following procedures.

- Obtain the HDLM installation DVD, and then remove HDLM by using removehdlm utility stored in "drive-containing-installation-DVD-ROM:\HDLM_VMware\DLMTTools".
 - Copy removehdlm utility in "HDLM-installation-folder\bin" to any location, and then remove HDLM by using the copied removehdlm utility.
- When you change the setting of user account or Credential Store file by dlrmcenv (utility for Configuring HDLM Remote Management Client Environments), restart the following two services by using the Windows service console to enable the change.
 - DLManagerVM
 - HBsA Service
 - A dialog box is displayed to prompt a system reboot even when a new installation or upgrade installation is aborted. Select "No" since the reboot associated with the installation abort is not required.
 - When you create a cluster configuration in a virtual machine environment by using cluster software (such as MSCS or HA Monitors) that uses SCSI reservations, you cannot apply the following HDLM load balancing algorithms:
 - Extended Round Robin: HTI_PSP_HDLM_EXRR
 - Extended Least I/Os: HTI_PSP_HDLM_EXLIO
 - Extended Least Blocks: HTI_PSP_HDLM_EXLBK
 - When you create a cluster configuration in a virtual machine environment by using cluster software that uses SCSI reservations, specify one of the following load balancing algorithms for the LUs assigned to the virtual machine:
 - Most Recently Used (VMware): VMW_PSP_MRU
 - Round Robin (VMware): VMW_PSP_RR

Note that you can specify settings for each LU by using VMware (by means such as the `esxcli` commands or vSphere Web Client) or by using Global Link Manager.

- When you use VMware PowerCLI, use the command prompt of Windows PowerShell to execute the utility for collecting HDLM error information (DLMgetras).
- When VMware PowerCLI is used on Windows Server 2012 R2 in an environment where Windows PowerShell 4.0 is installed, if an HDLM command is terminated by performing one of the following operations, subsequent HDLM commands might fail, and the KAPL01148-E message might be output. In addition, if the HDLM command is run in another Windows PowerShell command prompt window, the command will not end.
 - Pressing Ctrl+C
 - Selecting End task in Task Manager
 - Closing the Windows PowerShell command prompt window

Example of an error message that is output:

```
# dlnkmgr -s host-name -u user-name -p password view -sys  
KAPL01148-E An attempt to connect to the specified server has  
failed. Operation name = view
```

If this problem occurs, close all Windows PowerShell command prompt windows. Then, open a new Windows PowerShell command prompt window and run the HDLM command.

As a solution to this problem, consider upgrading Windows PowerShell from 4.0 to 5.1.

- When you install VMware PowerCLI, note the following restrictions:
 - Do not install the product into the following folder:
\$PSHome\Modules
(%Windir%\System32\WindowsPowerShell\v1.0\Modules)

This folder is reserved for modules provided by Windows.
 - When linking with Global Link Manager, install the product into the following folder, which is accessible to all users:
\$Env:ProgramFiles\WindowsPowerShell\Modules
(%ProgramFiles%\WindowsPowerShell\Modules)

If you use the `Install-Module` command of Windows PowerShell to install the product, specify All Users for the `-Scope` parameter.

Notes:

When linking with Global Link Manager, VMware PowerCLI is used not only by current users but also by the SYSTEM built-in account.

Verify that the Windows system environment variable PSModulePath contains the folder where VMware PowerCLI is installed.

If the variable does not contain it, add the folder path.

- When not linking with Global Link Manager, install the product into the following folder, which is only accessible to current users:

```
$Home\Documents\WindowsPowerShell\Modules  
(%UserProfile%\Documents\WindowsPowerShell\Modules)
```

If you use the Install-Module command of Windows PowerShell to install the product, specify Current User for the -Scope parameter.

In addition, you can install the product into the following folder, which is accessible to all users:

```
$Env:ProgramFiles\WindowsPowerShell\Modules  
(%ProgramFiles%\WindowsPowerShell\Modules)
```

- When you install VMware vSphere CLI and VMware PowerCLI on the same remote management client, do not perform an operation with the Credential Store file for vSphere CLI by using PowerCLI cmdlets, or do not perform an operation with the Credential Store file for PowerCLI by using credstore_admin.pl of vSphere CLI.

The password encryption and decryption algorithms are not same between vSphere CLI and PowerCLI, so if you perform these operations, the Credential Store file might become unusable.

If you want to perform such operations, you will need to delete the Credential Store file and then create it again.

In addition, in an environment where the Credential Store file created by using credstore_admin.pl of vSphere CLI, if you use the dlnkmg command by switching CLI to PowerCLI, the following error message might be output when you do not specify a user name or password.

```
KAPL01183-E The HDLM command cannot be executed because the VMware  
PowerCLI settings are not configured properly.
```

If the above message is output, specify a user name or password.

- When you remove HDLM plugins from the ESXi host and install an older version of the HDLM plugins, delete the module option information of the HDLM first, and then install the older version of HDLM.

If you do not delete the information, HDLM SATP might not be loaded. If HDLM SATP is not loaded, an error message is output to vmkwarning.log. In addition, the `dlnmgr view -sys` command terminates with an error.

<vmkwarning.log>

```
WARNING: NMP: nmpSatpCheckLoadedModule:794: SATP instance,
name=HTI_SATP_HDLM:
Load Failed! [Bad parameter]
```

<Command error message>

```
# dlnmgr connection-options view -sys
KAPL01181-E The HDLM driver is not installed correctly.
```

To delete the module option information, execute the following command on the ESXi host:

```
# esxcfg-module --set-options "" hti_satp_hdlm
```

Delete the module option information after one of the following two operations:

1) Removing the HDLM plugins:

Delete the module option information after performing step 4 "Remove HDLM" in the section "When using VMware vSphere CLI" or "When using VMware Power CLI" in "Chapter 3. Creating an HDLM Environment - Removing HDLM" of the Hitachi Dynamic Link Manager User Guide for VMware®.

2) Removing HDLM plugins and then re-installing an older version of the HDLM plugins:

Delete the module option information, and then restart the ESXi host.

When you delete the module option information, the option settings of HDLM are also deleted. Therefore, check the option settings of HDLM before the deletion, and then reconfigure them by using the `dlnmgr set` command.

- When you install HDLM by using vSphere Lifecycle Manager, for ESXi 7.0 Update 1 or later, use the Depot file instead of the addon file.
- When you incorrectly specify host name, user name, or password of the host connection options in the command prompt of Windows PowerShell in an environment where VMWare PowerCLI is installed to execute `DLMGetras`, the KAPL10957-W message is output instead of the KAPL10956-W message.

```
# DLMgetras -s XXX.XXX.XXX.XXX -u XXXX -p XXXXXXXXX
'"esxcli.exe"' is not recognized as an internal or external command,
operable program or batch file.
KAPL10957-W The utility for collecting HDLM error information cannot
be executed because the VMware vSphere CLI or VMware PowerCLI is not
installed.
```

This is a problem due to an error of the output message, and there is no problem in this environment.

Check the host connection options, and then re-execute the command.

- In an environment where VMWare vSphere CLI or VMWare PowerCLI is already installed, when you execute DLMGetras in the command prompt of Windows PowerShell, an error of thumbprint might be output.

```
# dlmgetras -s XXX.XXX.XXX.XXX -u XXXX -p XXXXXXXXX
Certificate error. Server SHA-1 thumbprint:
AA:BB:CC:DD:EE:FF:GG:HH:II:JJ:KK:LL:MM:NN:OO:PP:QQ:RR:SS:TT (not
trusted)
C:\hdlmtemp\hdlmgetras_XX
KAPL10043-I Error information is being collected. (XX%)
```

This message is output if one of the following conditions such as 1 and 2 is met:

1) Removing the HDLM plugins:

- The dlmmcenv utility has not been executed in the vSphere CLI prompt.
- When DLMGetras is executed, the host connection options are incorrect, or the specified host is not responded.

2) If you have set vSphere CLI as communication interface of HDLM:

- The dlmmcenv utility has been executed in the vSphere CLI prompt.
- PowerCLI is specified as CLI to acquire host information.
- The specified host information when DLMGetras is executed is not stored in the Credential Store file.

This problem is due to an output of the error message, and DLMGetras is executed without any problem if the KAPL10043-I message is output.

If the KAPL10043-I is not output, check the host connection options, and then re-execute the command.

- When you use ESXi 7.0 Update 2 or later, HDLM cannot be linked with Global Link Manager. In addition, when you use VMware PowerCLI, use VMware PowerCLI version 12.3.0.
- When HDLM is linked with Global Link Manager, VMware PowerCLI 12.1.0 or later is not supported. Use PowerCLI 12.0.0.
- Storage systems which have following functions are no longer supported.
 - Dynamic load balance control function
 - High Availability Manager function
 - Virtual ID function for storage migration

But the parameters for these functions are displayed in the format of set or view operation of the HDLM command when help operation is executed. And the following item is displayed when view -sys operation is executed:

Dynamic I/O Path Control

- When you use any of the following special characters in your password for the ESXi host, HDLM cannot connect to the ESXi host. When setting your password for the ESXi host, do not use the following characters:

```
# " ' ` $ | > < &
@ , ( ) { } ] ; _ spaces
```

- If the property "QuickEdit Mode" is enabled in the command prompt or in the Windows PowerShell prompt, the command processing stops when you select text in a window where the DLMgetras command is running. While text is selected, the window displays "Select", and the command processing will not restart until you press the Enter key.
- When you execute the dlmpinfo utility or the DLMgetras utility from the PowerShell command prompt while you do not have system administrator permissions, the User Account Control (UAC) dialog box does not appear.

The following warning messages are output, and the utility cannot be executed:

- For the dlmpinfo utility: "KAPL13038-W A parameter is invalid."
- For the DLMgetras utility: "KAPL10005-W The number of parameters is insufficient."

Closing known problems

8.8.3-04 Modifications

- When you set the execution policy of Windows PowerShell in Windows 10, set the execution policy for the MachinePolicy, UserPolicy, or Current User scope to RemoteSigned. If you set only the execution policy for LocalMachine scope to RemoteSigned, an attempt to connect to the ESXi host by using the HDLM command fails, and the KAPL01148-E message is output.

```
KAPL01148-E An attempt to connect to the specified server has failed. Operation name = view
```

8.8.3-00 Modifications

- If you do not specify installfile_location in the installation information settings file to perform an unattended installation, the following message is output: “KAPL09195-W The setup.exe file does not exist.”

Installation precautions

For details on HDLM installation, see the Hitachi Dynamic Link Manager (for VMware®) User Guide.

Chapter 3. Creating an HDLM Environment - Installing HDLM

Additional Precautions

- ESXi and VIB package that is a module package of VMware respectively have four acceptance levels: VMwareCertified, VMwareAccepted, PartnerSupported and CommunitySupported, from higher levels. If the acceptance level of an ESXi is higher than that of a VIB package, the VIB package cannot be installed on the ESXi. In this case, an operation of lowering the acceptance level of the ESXi to an appropriate level is required. For the operation procedures, see the Hitachi Dynamic Link Manager (for VMware®) User Guide.

Chapter 3. Creating an HDLM Environment - Installing HDLM

- Names of offline bundle files and plugin modules provided in this version are listed below.

- Install file name and information of plugins

Install file name	Displaying the HDLM version of the host	Plugin name	Version *1	Acceptance level
hdlm-0883000301-0600.zip *2	8.8.3-03	satp-hdlm	08.8.3-03.0600	VMware Accepted
		psp-hdlm-exlio	08.8.0-00.0600	VMware Accepted
		psp-hdlm-exlbc	08.8.0-00.0600	VMware Accepted
		psp-hdlm-exrr	08.8.0-00.0600	VMware Accepted
		hex-hdlm-dlnkmgr	08.8.3-03.0600	PartnerSupported
hdlm-0883000301-0700-depot.zip*3	8.8.3-03	satp-hdlm	08.8.3-03.0700	VMware Accepted
		psp-hdlm-exlio	08.8.0-00.0700	VMware Accepted
		psp-hdlm-exlbc	08.8.0-00.0700	VMware Accepted
		psp-hdlm-exrr	08.8.0-00.0700	VMware Accepted
		hex-hdlm-dlnkmgr	08.8.3-03.0700	PartnerSupported

*1: You can check the version information of each plugin on an ESXi host by executing the following command.

```
# esxcli software vib list | grep hdlm
```

*2: This is the offline bundle file for ESXi6.x

*3: This is the depot file for ESXi7.x

- Before installing HDLM, make sure that VMware vSphere CLI (vCLI) is installed and the ESXi server can be accessed by vCLI.
- If HDLM is managed with HGLM, confirm the following before the operation of "Hitachi Dynamic Link Manager User Guide for VMware® - Settings When Managing HDLM by Using Global Link Manager".

- On Remote Management Client, a host name of an ESXi host can be resolved into an IP address.
- A Credential Store file is created by using the resolved IP address.
- The command prompt which is displayed during an installation, upgrade, or uninstallation of remote management client is automatically closed after the operation is completed. Make sure not to close it during the operation. If Command Prompt is closed during the operation, the operation of an installation, upgrade, or uninstallation ends before completion. In this case, perform an upgrade installation.
- The maximum number of LUs including all SCSI devices such as built-in disks and CD-ROM drives is 512 for ESXi 6.5 and 1024 for ESXi 6.7 or later. Therefore, the maximum number of LUs for a storage system manageable by HDLM will be smaller than the maximum for ESXi, depending on the status of other connected devices. Before applying HDLM to an ESXi host, confirm that the ESXi host correctly recognizes the LUs to be managed by HDLM.
- When HDLM is installed on an ESXi7.0 Update 1 or later host, a “Jumpstart dependency error” for HDLM plugins is output to the ESXi log or console, but there is no problem with the system.

Remove Precautions

For details on removing HDLM uninstallation, see the Hitachi Dynamic Link Manager (for VMware®) User Guide.

Chapter 3. Creating an HDLM Environment - Removing HDLM

Usage precautions

Notes on General procedures

- HDLM provides NMP sub-plugins(SATP/PSP) to enable multipath management for Hitachi storages. For the information of NMP/SATP/PSP, refer to the following documentation(*).

<https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-storage-guide.pdf>

<https://docs.vmware.com/en/VMware-vSphere/7.0/vsphere-esxi-vcenter-server-70-storage-guide.pdf>

(*): It is the information as of June 2020.

- Any restrictions and precautions for NMP which VMware announces are applied to your environment using HDLM. Check the restrictions and precautions before you build an environment.
- Any restrictions and precautions for PSP VMW_PSP_RR (Round Robin) that is provided by VMware are applied to the following HDLM load balances.
 - HTI_PSP_HDLM_EXLIO
 - HTI_PSP_HDLM_EXLBK
 - HTI_PSP_HDLM_EXRR
- In HDLM 8.6.0 and later, the specifications were changed to match those of VMW_PSP_RR (a PSP of VMware NMP) so that "Active(I/O)" is displayed as the status for all active paths in vSphere Client and in vSphere Web Client. If you want to revert to the previous specification, in which "Active(I/O)" is displayed only for the last-used path, execute the following commands, and then restart the host:
 - `esxcli host-connection-option system module parameters set -m=hti_psp_hdlm_exlio -p reportWorkingPaths=1`
 - `esxcli host-connection-option system module parameters set -m=hti_psp_hdlm_exlbc -p reportWorkingPaths=1`
 - `esxcli host connection option system module parameters set -m=hti_psp_hdlm_exrr -p reportWorkingPaths=1`

This setting is enabled as long as a new installation of ESXi is not performed.

Note that if you specify 2 for `reportWorkingPaths` in the preceding commands, "Active(I/O)" is displayed as the path status for all active paths. You can check the setting values for `reportWorkingPaths` by using the following commands:

- `esxcli host-connection-option system module parameters list -m=hti_psp_hdlm_exlio`
- `esxcli host-connection-option system module parameters list -m=hti_psp_hdlm_exlbc`
- `esxcli host-connection-option system module parameters list -m=hti_psp_hdlm_exrr`
- Values that can be specified for `reportWorkingPaths`:
 - Null character or 2: Display "Active(I/O)" for all active paths.
 - 1: Display "Active(I/O)" for the last-used path.

(Note that if you change this setting, the new setting value becomes valid after the host is restarted.)

- When you remove a remote client, a dialog box displaying "Location is not available." might be output. However, the processing to remove it performs properly. Select the OK button to close the dialog box.
- When path failures occur frequently due to hardware failures, such as HBA, or the SCSI reserve for a shared disk, many HDLM path failure messages are output to the system log, which might impact system log performance. To avoid performance degradation of the system log, we recommend that you enable the path failure message suppression function.

1) How to enable the path failure message suppression function

a) When setting up on a host:

```
# esxcli hdlm dlnkmgr system set --option=pfs:ON
```

b) When setting up on a remote management client:

<Procedure for setting up by using VMware vSphere CLI>

```
# esxcli host connection option hdlm dlnkmgr system set --option=pfs:ON
```

<Procedure for setting up by using VMware PowerCLI>

```
# EsxCli-Object (*1).hdlm.dlnkmgr.system.set.invoke(@{option="pfs:ON"}) | ConvertTo-Json
```

(*1): This is one EsxCli object that was acquired for each host by using the Get-EsxCli cmdlet.

2) How to disable the path failure message suppression function

a) When setting up on a host:

```
# esxcli hdlm dlnkmgr system set --option=pfs:OFF
```

b) When setting up on a remote management client:

<Procedure for setting up by using VMware vSphere CLI>

```
# esxcli host connection option hdlm dlnkmgr system set --option=pfs:OFF
```

<Procedure for setting up by using VMware PowerCLI>

```
# EsxCli-Object (*1).hdlm.dlnkmgr.system.set.invoke(@{option="pfs:OFF"}) | ConvertTo-Json
```

(*1): One EsxCli object per host obtained with the Get-EsxCli cmdlet.

For the message suppression interval, the message suppression count, and error causes for message suppression, default values are configured as

recommended settings based on HDLM examples. However, you can change these settings.

For details about the path failure message suppression function, see Appendix A Path failure message suppression function.

For details about the command for setting the path failure message suppression function, see Appendix A 1.6 Configuring the path failure message suppression information.

The recommended settings are in (3).

Documentation

Available documents

Document name	Document number	Issue date
Hitachi Dynamic Link Manager (for VMware®) User Guide	MK-92DLM130-30	February 2022

Appendix A

1. Path failure message suppression function

1.1 Overview of the path failure message suppression function

When path failures occur frequently due to hardware failures, such as HBA, or the SCSI reserve for a shared disk, many HDLM path failure messages are output to the system log. This situation might impact system performance. The impact on the system log can be avoided by suppressing path failure messages caused by the same reason to a certain interval or a certain count. This function is called path failure message suppression function.

1.2 Configuring the path failure message suppression function

Specify conditions to suppress path failure messages by using the `hdlm dlnkmgr system` set operation of the extended `esxcli` command provided by HDLM. The path failure messages will be suppressed while the specified values in the conditions are satisfied.

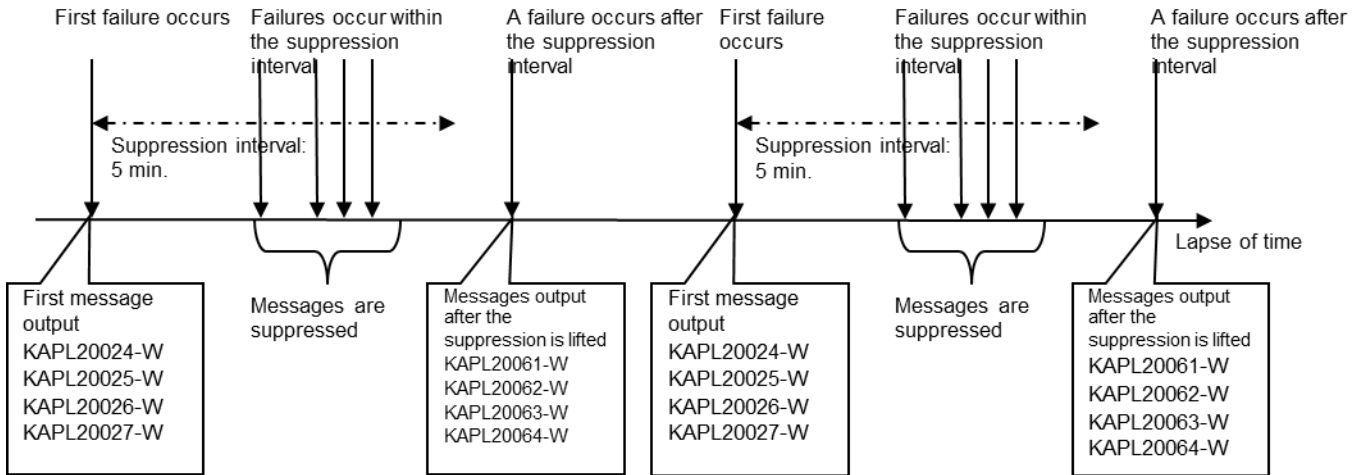
As conditions for suppressing path failure messages, you can specify the suppression interval, suppression count, and codes that determine the cause of failure. For failure causes, specific causes can be specified for each of host status, plugin status, device status, and SCSI sense key.

The following table lists the messages to be suppressed:

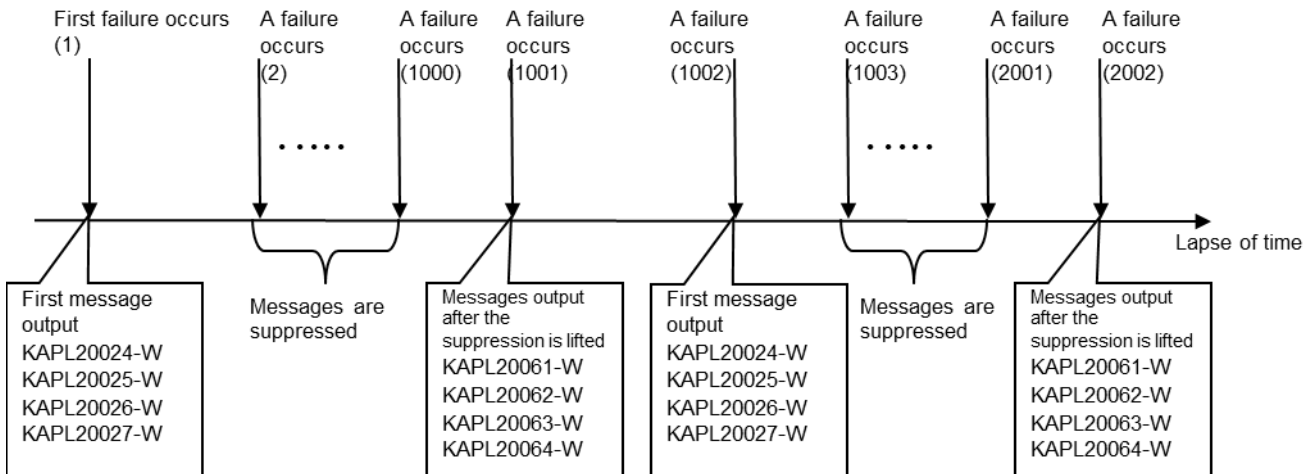
Messages to be suppressed and messages to be output after the suppression is lifted

No.	Messages to be suppressed	Messages to be output after the suppression is lifted
1	KAPL20024-W	KAPL20061-W
2	KAPL20025-W	KAPL20062-W
3	KAPL20026-W	KAPL20063-W
4	KAPL20027-W	KAPL20064-W

The following diagram shows an example when 5 minutes is specified for the suppression interval:



The following diagram shows an example when 1000 is specified for the message suppression count:



If you specify both the suppression interval and suppression count, the path failure messages will be suppressed while both conditions are satisfied.

For details of the hdlm dlncmgr system set operation of the extended escli command, see 1.6 Configuring the path failure message suppression information.

1.3 Checking the path failure message suppression function

You can check whether the path failure message suppression function is configured by the execution result of the hdlm dlncmgr system get operation of the extended escli command.

For details of the hdlm dlncmgr system get operation, see 1.7 Confirming the information about the path failure message suppression.

1.4 Triggers for starting and lifting suppression of path failure messages for each path

The trigger for starting suppression of path failure messages for each path is as follows:

Trigger for starting the suppression	Messages output when the suppression starts
When a path failure occurs in an environment where the path failure message suppression function is enabled. (Paths added while the path failure message suppression function is enabled are also included.)	Depending on the cause of failure, one of the following messages is output: KAPL20024-W KAPL20025-W KAPL20026-W KAPL20027-W

The triggers for lifting the suppression of path failure messages for each path are as follows:

Triggers for lifting the suppression	Messages output when the suppression is lifted
When a path failure occurs after the suppression interval from the start of suppression passed. If no path failure occurs after the suppression interval, the suppression is lifted by the VMware path polling (5 minutes by default).	Depending on the cause of failure, one of the following messages is output: KAPL20061-W KAPL20062-W KAPL20063-W KAPL20064-W
When a path failure occurs exceeding the suppression count from the start of the suppression.	
When you disable the path failure message suppression function with the extended esxcli command.	
When the path failure is blocked.	
When the path is turned offline with the offline command.	
When the path or device is deleted.	
When more than 20 different failure causes occur for each of the host status, plugin status, device status, and sense key. The suppression for the oldest failure cause will be lifted.	

1.5 Details of new messages output when using the path failure suppression function

Message ID	Message Text	Explanation
KAPL20061-W	KAPL20024 I/O (aa...aa) to path (bb...bb) failed. Sense key= cc...cc ASC/ASCQ= dd...dd Count= ee...ee	<p>Details</p> <p>An I/O error was detected, and the message was suppressed.</p> <p>aa...aa: SCSI command bb...bb: Name of Path that had I/O error cc...cc: Sense key dd...dd: ASC/ASCQ ee...ee: Suppression count of message outputs</p> <p>Action</p> <p>Check the status of the path for which the error was detected based on the sense code and the explanation of the additional sense code.</p>
KAPL20062-W	KAPL20025 I/O (aa...aa) to path (bb...bb) failed. Plugin status= cc...cc Count= dd...dd	<p>Details</p> <p>An I/O error was detected, and the message was suppressed.</p> <p>aa...aa: SCSI command bb...bb: Name of Path that had I/O error cc...cc: Plugin status dd...dd: Suppression count of message outputs</p> <p>Action</p> <p>Execute the DLMgetras utility for collecting HDLM error information, and then contact your HDLM vendor or the maintenance company if you have a maintenance contract for HDLM.</p>

		For details on the DLMgetras utility, see The DLMgetras utility for collecting HDLM error information on page 7-2. of the HDLM User Guide.
KAPL20063-W	KAPL20026 I/O (aa...aa) to path (bb...bb) failed. Host status= cc...cc Count= dd...dd	<p>Details</p> <p>An I/O error was detected, and the message was suppressed.</p> <p>aa...aa: SCSI command</p> <p>bb...bb: Name of Path that had I/O error</p> <p>cc...cc: Host status</p> <p>dd...dd: Suppression count of message outputs</p> <p>Action</p> <p>Execute the DLMgetras utility for collecting HDLM error information, and then contact your HDLM vendor or the maintenance company if you have a maintenance contract for HDLM.</p> <p>For details on the DLMgetras utility, see The DLMgetras utility for collecting HDLM error information on page 7-2. of the HDLM User Guide.</p>
KAPL20064-W	KAPL20027 I/O (aa...aa) to path (bb...bb) failed. Device status= cc...cc Count= dd...dd	<p>Details</p> <p>An I/O error was detected, and the message was suppressed.</p> <p>aa...aa: SCSI command</p> <p>bb...bb: Name of Path that had I/O error</p> <p>cc...cc: Device status</p> <p>dd...dd: Suppression count of message outputs</p> <p>Action</p> <p>Execute the DLMgetras utility for collecting HDLM error information, and then contact your HDLM vendor or the</p>

		<p>maintenance company if you have a maintenance contract for HDLM.</p> <p>For details on the DLMgetras utility, see The DLMgetras utility for collecting HDLM error information on page 7-2. of the HDLM User Guide.</p>
KAPL20065-E	Warning messages cannot be suppressed for the path (aa..aa) because of insufficient memory.	<p>Details</p> <p>Warning messages cannot be suppressed for the path (aa..aa) because of insufficient memory.</p> <p>aa...aa: Path name</p> <p>Action</p> <p>Re-execute the command. If the same error occurs repeatedly, check that the system memory is sufficient.</p>
KAPL30001-W	The hdlm command error.,reason code=(a)	<p>Details</p> <p>The specified parameter is incorrect.</p> <p>A: Reason code (decimal)</p> <ol style="list-style-type: none"> 1. Syntax error 2. The specified value is outside the value range <p>Action</p> <p>Check the command format and execute the command again.</p>

1.6 Configuring the path failure message suppression information

(1) Format

When executing on a host:

```
# esxcli hdlm dlnkmgr system set
--option=pfs:{ON|OFF}.
[Path failure message suppression interval].
[Path failure message suppression count].
[Host status setting code].
[Plugin status setting code].
[Device status setting code].
[SCSI sense key setting code]
```

When executing from a remote management client:

< For VMware vSphere CLI>

```
# esxcli host connection option hdlm dlnkmgr system set
--option=pfs:{ON|OFF}.
[Path failure message suppression interval].
[Path failure message suppression count].
[Host status setting code].
[Plugin status setting code].
[Device status setting code].
[SCSI sense key setting code]
```

< For VMware PowerCLI >

```
# EsxCli-Object (*1).hdlm.dlnkmgr.system.set.invoke
(@{option="pfs:{ON|OFF}.
[Path failure message suppression interval].
[Path failure message suppression count].
[Host status setting code].
[Plugin status setting code].
[Device status setting code].
[SCSI sense key setting code]"} | ConvertTo-Json

(*1): One EsxCli object per host obtained with the Get-EsxCli cmdlet.
```

(2) Parameters

pfs:{ON|OFF}

This parameter enables or disables the path failure message suppression function. The default value is OFF: Disable.

ON: Enabled.

OFF: Disabled.

Path failure message suppression interval

Specify the interval in seconds to suppress path failure messages whose cause is specified by the failure cause setting code. Specify a value from 0 to 3600. The default value is 10 seconds. If you specify 0, messages will not be suppressed by an interval.

If a path failure whose cause is specified by the monitored failure cause setting code occurs several times within the path failure message suppression interval specified here, the second and subsequent messages will be suppressed. When a failure occurs after the suppression interval and after the suppressed message is output with the message suppression count, the suppression will be lifted.

Path failure message suppression count

Specify the path failure message suppression count whose cause is specified by the failure cause setting code. Specify 0 or a value from 10 to 3600000. The default value is 3000. If you specify 0, messages will not be suppressed by suppression count.

If a path failure whose cause is specified by the monitored failure cause setting code occurs several times within the path failure message suppression count specified here, the second and subsequent messages will be suppressed. When a failure occurs exceeding the suppression count and after the suppressed message is output with the message suppression count, the suppression will be lifted.

Host status setting code

Specify a failure cause setting code (decimal) that corresponds to the SCSI host status. Specify a value from 0 to 32767. The default value is 2113. 2113 is the value that suppresses NO_CONNECT, ERROR, and RETRY. If you want to specify more than one causes, specify the sum of the setting codes. If you specify 0, suppression by host status is not performed. If you specify the maximum value, all the failure causes will be suppressed.

The following table describes the setting codes that correspond to each SCSI host status:

Setting codes that correspond to each SCSI host status.

SCSI host status	Host status code	Setting code
NO_CONNECT	0x01	1
BUS_BUSY	0x02	2
TIMEOUT	0x03	4
BAD_TARGET	0x04	8
ABORT	0x05	16
PARITY	0x06	32
ERROR	0x07	64
RESET	0x08	128
BAD_INTR	0x09	256
PASSTHROUGH	0x0a	512
SOFT_ERROR	0x0b	1024
RETRY	0x0c	2048
REQUEUE	0c0d	4096
PI_REF_ERROR	0x0e	8192
PI_GENERIC_ERROR	0x0f	16384

For details on the host status, see the information provided from VMware (e.g., VMware Knowledge Base KB289902).

Plugin status setting code

Specify a failure cause setting code (decimal) that corresponds to the plugin status. Specify a value from 0 to 255. The default value is 0. If you specify 0, the plugin status will not be suppressed. If you want to specify more than one causes, specify the sum of the setting codes. If you specify the maximum value, all the failure causes will be suppressed.

The following table describes the setting codes that correspond to each plugin status:

Setting codes that correspond to each plugin status.

Plugin status	Plugin status code	Setting code
TRANSIENT	0x01	1
SNAPSHOT	0x02	2
RESERVATION_LOST	0x03	4
REQUEUE	0x04	8
ATS_MISCOMPARE	0x05	16
THINPROV_BUSY_GROWING	0x06	32
THINPROV_ATQUOTA	0x07	64
THINPROV_NOSPACE	0x08	128

For details on the plugin status, see the information provided from VMware (e.g., VMware Knowledge Base KB2004086).

Device status setting code

Specify a failure cause setting code (decimal) that corresponds to the SCSI device status. Specify a value from 0 to 1023. The default value is 32. 32 is the value that suppresses RESERVATION_CONFLICT. If you want to specify more than one causes, specify the sum of the setting codes. If you specify 0, the device status will not be suppressed. If you specify the maximum value, all the failure causes will be suppressed.

The following table describes the setting codes that correspond to each SCSI device status:

Setting codes that correspond to each SCSI device status

SCSI device status	Device status code	Setting code
CHECK_CONDITION	0x02	1
CONDITION_MET	0x04	2
BUSY	0x08	4
INTERMEDIATE	0x10	8
INTERMEDIATE_CONDITION_MET	0x14	16
RESERVATION_CONFLICT	0x18	32
COMMAND_TERMINATED	0x22	64
QUEUE_FULL	0x28	128
ACA_ACTIVE	0x30	256

For details on the device status, see the information provided from VMware (e.g., VMware Knowledge Base KB289902).

SCSI sense key setting code

Specify a failure cause setting code (decimal) that corresponds to the SCSI sense key. Specify a value from 0 to 32767. The default value is 0. If you specify 0, the SCSI sense key will not be suppressed. If you want to specify more than one causes, specify the sum of the setting codes. If you specify the maximum value, all the failure causes will be suppressed.

The following table describes the setting codes that correspond to each SCSI sense key:

Setting codes that correspond to each SCSI sense key

SCSI sense key	Sense key	Setting code
RECOVERED_ERROR	0x01	1
NOT_READY	0x02	2
MEDIUM_ERROR	0x03	4
HARDWARE_ERROR	0x04	8
ILLEGAL_REQUEST	0x05	16
UNIT_ATTENTION	0x06	32
DATA_PROTECT	0x07	64
BLANK_CHECK	0x08	128
VENDOR_SPECIFIC	0x09	256
COPY_ABORTED	0x0a	512
ABORTED_COMMAND	0x0b	1024
EQUAL	0x0c	2048
VOLUME_OVERFLOW	0c0d	4096
MISCOMPARE	0x0e	8192
COMPLETED	0x0f	16384

For details on the sense key, check with the hardware (storage) provider because this is hardware-specific information.

(3) Recommended parameter settings

The following table describes recommended parameter settings:

Parameters		When only failure causes (*1) that occur frequently are suppressed	When all failure causes are suppressed
Parameter settings	Path failure message suppression interval	10 (Default value)	10 (Default value)
	Path failure message suppression count	3000 (Default value)	3000 (Default value)
	Setting code of the host status	2113 (Default value)	32767 (Maximum value)
	Setting code of the plugin status	0 (Default value)	255 (Maximum value)
	Setting code of the device status	32 (Default value)	1023 (Maximum value)
	Setting code of the SCSI sense key	0 (Default value)	32767 (Maximum value)
Description format for the above parameters		<p><When setting a parameter for the first time></p> <p>pfs:ON</p> <p><When a parameter has been set in the past></p> <p>pfs:ON.10.3000.2113.0.32.0</p>	<p>pfs:ON.10.3000.32767.255.1023.32767</p>

(*1): Failure causes that were frequently asked in the past.

(4) Usage example

The following is an example of setting the path failure message suppression function so that it is enabled and setting the path failure message suppression interval to 5 minutes, the path failure message suppression count to 1000, and targeting all failure causes as the suppression conditions.

```
# esxcli hdlm dlnkmgr system set --
option=pfs:ON.300.1000.32767.255.1023.32767

Version: 8.8.3-03

SPVersion:

HostName: esxi7x

MaxDevices: 1024

MaxPaths: 4096

SysInfo: SATP.Flags:67108864, SATP.MaxDevs:1024, SATP.MaxPaths:4096,
SATP.MaxStorages:256, SATP.IemIntvl:30, SATP.IemNum:3, SATP.Loglevel:0,
SATP.Timeout:10000, SATP.PslogSize:1024, SATP.PslogSizeInit:1024,
SATP.PslogSizeNext:1024, SATP.DPC.TARGET:240, SATP.DPC.SYSTEM:0,
SATP.DPC.INTVL:10, SATP.HaBlockType:0, SATP.PfmIntvl:1, SATP.PfmNum:10,
SATP.PfmShs:64, SATP.PfsIntvl:300, SATP.PfsNum:1000, SATP.PfsShs:32767,
SATP.PfsPlg:255, SATP.PfsSds:1023, SATP.PfsSky:32767,
PSP(0)@HTI_PSP_HDLM_EXRR.Exlimit:100,
PSP(0)@HTI_PSP_HDLM_EXRR.ExRndlimit:1,
PSP(0)@HTI_PSP_HDLM_EXRR.Loglevel:0,
PSP(0)@HTI_PSP_HDLM_EXRR.SpuLimit:100,
PSP(0)@HTI_PSP_HDLM_EXRR.SpuDuration:60,
PSP(0)@HTI_PSP_HDLM_EXRR.SpuDuration:60,
PSP(1)@HTI_PSP_HDLM_EXLIO.Exlimit:100,
PSP(1)@HTI_PSP_HDLM_EXLIO.ExRndlimit:1,
PSP(1)@HTI_PSP_HDLM_EXLIO.Loglevel:0,
PSP(1)@HTI_PSP_HDLM_EXLIO.SpuLimit:100,
PSP(1)@HTI_PSP_HDLM_EXLIO.SpuDuration:60,
PSP(1)@HTI_PSP_HDLM_EXLIO.SpuDuration:60,
PSP(2)@HTI_PSP_HDLM_EXLBK.Exlimit:100,
PSP(2)@HTI_PSP_HDLM_EXLBK.ExRndlimit:1,
PSP(2)@HTI_PSP_HDLM_EXLBK.Loglevel:0,
PSP(2)@HTI_PSP_HDLM_EXLBK.SpuLimit:100,
PSP(2)@HTI_PSP_HDLM_EXLBK.SpuDuration:60,
PSP(2)@HTI_PSP_HDLM_EXLBK.SpuDuration:60

SatpName: HTI_SATP_HDLM

ClaimRules:
```

DefaultPSP:

SATP.Flags (Enable or disable path failure message suppression function): 67108864

If the least significant bit is 0th bit and the 26th bit is 0, it is disabled. If the 26th bit is 1, it is enabled.

Check only the 26th bit to confirm whether the path failure message suppression function is enabled or disabled.

Ignore cases if 1 is set for another bit.

Decimal 67108864

Binary 0100 0000 0000 0000 0000 0000 0000

↑

↑

When enabled, the 26th bit is 1.

0 bit

SATP.PfsIntvl (Path failure message suppression interval):300

SATP.PfsNum (Consecutive number of path failures):1000

SATP.PfsShs (Setting code of the host status): 32767

SATP.PfsPlg (Setting code of the plugin status): 255

SATP.PfsSds (Setting code of the device status):1023

SATP.PfsSky (Setting code of the sense key):32767

(5) Notes

- Use a period as a delimiter between parameters.
- A period-delimited string is assumed as specified value.
- If a parameter is omitted, the default value is set for that parameter. Parameters that have already been set will inherit the values from the previous settings.
- If an extra parameter is specified, that extra parameter is ignored.
- While the path failure message suppression function is enabled (pfs:ON), the following settings will result in a syntax error.
When both the suppression interval and the suppression count are set to 0.
When all the failure cause setting codes are set to 0.
- If failures are detected by different SCSI commands even for the same failure causes, they are treated as different failure causes.
- The maximum number of path failure causes for the message suppression is 20 per host status, plugin status, device status, and sense key.

- Parameter values that have been set will be inherited even after HDLM is updated or reinstalled.

1.7 Confirming the information about the path failure message suppression

(1) Format

When executing on a host:

```
# esxcli hdlm dlnkmgr system get
```

When executing from a remote management client:

< For VMware vSphere CLI >

```
# esxcli host connection option hdlm dlnkmgr system get
```

< For VMware PowerCLI >

```
# EsxCli-Object (*1).hdlm.dlnkmgr.system.get.invoke() | ConvertTo-Json
```

(*1): One EsxCli object per host obtained with the Get-EsxCli cmdlet.

(2) Parameters

None.

(3) Usage example

An example of usage is shown below:

```
# esxcli hdlm dlnkmgr system get
```

```
Version: 8.8.3-03
```

```
SPVersion:
```

```
HostName: esxi7x
```

```
MaxDevices: 1024
```

```
MaxPaths: 4096
```

```
SysInfo: SATP.Flags:67108864, SATP.MaxDevs:1024, SATP.MaxPaths:4096,  
SATP.MaxStorages:256, SATP.IemIntvl:30, SATP.IemNum:3, SATP.Loglevel:0,  
SATP.Timeout:10000, SATP.PslogSize:1024, SATP.PslogSizeInit:1024,  
SATP.PslogSizeNext:1024, SATP.DPC.TARGET:240, SATP.DPC.SYSTEM:0,  
SATP.DPC.INTVL:10, SATP.HaBlockType:0, SATP.PfmIntvl:1, SATP.PfmNum:10,  
SATP.PfmShs:64, SATP.PfsIntvl:300, SATP.PfsNum:1000, SATP.PfsShs:32767,  
SATP.PfsPlg:255, SATP.PfsSds:1023, SATP.PfsSky:32767,  
PSP(0)@HTI_PSP_HDLM_EXRR.Exlimit:100,  
PSP(0)@HTI_PSP_HDLM_EXRR.ExRndlimit:1,  
PSP(0)@HTI_PSP_HDLM_EXRR.Loglevel:0,  
PSP(0)@HTI_PSP_HDLM_EXRR.SpuLimit:100,  
PSP(0)@HTI_PSP_HDLM_EXRR.SpuDuration:60,  
PSP(0)@HTI_PSP_HDLM_EXRR.SpuDuration:60,  
PSP(1)@HTI_PSP_HDLM_EXLIO.Exlimit:100,  
PSP(1)@HTI_PSP_HDLM_EXLIO.ExRndlimit:1,  
PSP(1)@HTI_PSP_HDLM_EXLIO.Loglevel:0,  
PSP(1)@HTI_PSP_HDLM_EXLIO.SpuLimit:100,  
PSP(1)@HTI_PSP_HDLM_EXLIO.SpuDuration:60,  
PSP(1)@HTI_PSP_HDLM_EXLIO.SpuDuration:60,  
PSP(2)@HTI_PSP_HDLM_EXLBK.Exlimit:100,  
PSP(2)@HTI_PSP_HDLM_EXLBK.ExRndlimit:1,  
PSP(2)@HTI_PSP_HDLM_EXLBK.Loglevel:0,  
PSP(2)@HTI_PSP_HDLM_EXLBK.SpuLimit:100,  
PSP(2)@HTI_PSP_HDLM_EXLBK.SpuDuration:60,  
PSP(2)@HTI_PSP_HDLM_EXLBK.SpuDuration:60
```

```
SatpName: HTI_SATP_HDLM
```

```
ClaimRules:
```

DefaultPSP:

SATP.Flags (Enable or disable path failure message suppression function): 67108864

If the least significant bit is 0th bit and the 26th bit is 0, it is disabled. If the 26th bit is 1, it is enabled.

Check only the 26th bit to confirm whether the path failure message suppression function is enabled or disabled.

Ignore cases if 1 is set for another bit.

Decimal 67108864

Binary 0100 0000 0000 0000 0000 0000 0000

↑

↑

When enabled, the 26th bit is 1.

0 bit

SATP.PfsIntvl (Path failure message suppression interval):300

SATP.PfsNum (Consecutive number of path failures):1000

SATP.PfsShs (Setting code of the host status): 32767

SATP.PfsPlg (Setting code of the plugin status): 255

SATP.PfsSds (Setting code of the device status):1023

SATP.PfsSky (Setting code of the sense key):32767

Copyrights and licenses

© 2022 Hitachi Vantara LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (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" mean text, 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 LLC 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 LLC.

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; and
- 2) Verifying that your 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.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Edge, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft corporate logo, the Microsoft Edge 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 website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html> or <https://knowledge.hitachivantara.com/Documents/Open Source Software>.