Hitachi Data Ingestor v6.4.8-04 Release Notes

Contents

About this document

This document (RN-90HDI011-95, October 2021) provides late-breaking information about Hitachi Data Ingestor 6.4.8-04. 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 Data Ingestor.

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.

About this release

This release provides new support and resolves known problems.

Product package contents

Table 1. Product package contents

Medium	Product name	Revision
DVD-R	Hitachi Data Ingestor	6.4.8-04

New features and enhancements

Table 2. New Features and enhancements

No	Contents	Revision
1	Adobe AIR is now supported for single node GUI. When you are using single node GUI, set Internet Explorer or Firefox as Windows default browser. If you are using Internet Explorer as default browser, set options in the Internet Options as follows:	6.4.8-00

No	Contents	Revision
	• In Site of the Trusted Sites of the Security tab, add the URLs for all managed nodes and about:internet • Select the Allow active content to run in files on My Computer check box of the Advanced tab.	
2	The base version of OpenSSH that is an internal component of HDI is updated. With the update, the following functions are changed as per shown in 3 to 6 below.	6.4.8-00
3	The encryption algorithm that can be used for SSH communication and Message Authentication Code (MAC) are changed. Encryption algorithm: 6.4.7-xx and earlier: ARCFOUR128 (*1), ARCFOUR256 (*1), AES128-ctr, AES192-ctr, AES256-ctr 6.4.8-00 and later: AES128-ctr, AES192-ctr, AES256-ctr, AES128-gcm@openssh.com, AES256-gcm@openssh.com, ChaCha20-poly1305@openssh.com MACs: 6.4.7-xx and earlier: hmac-sha1, hmac-ripemd160 (*1), hmac-ripemd160@openssh.com (*1) 6.4.8-00 and later: hmac-sha1, umac-64-etm@openssh.com, hmac-sha2-256, hmac-sha2-512, umac-128@openssh.com, umac-128-etm@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com *1: ARCFOUR128, ARCFOUR256 and hmac-ripemd160 cannot be used with 6.4.8-00 and later.	6.4.8-00
4	Key Type of host key that can be used for SSH communication is changed. 6.4.7-xx and earlier: ssh-rsa, ssh-dss	6.4.8-00

No	Contents	Revision
	6.4.8-00 and later: ssh-rsa, ssh-dss (*1), ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519, rsa-sha2-256, rsa-sha2-512 *1: It is disabled as the default setting of new installation. At update installation, the previous setting value is taken over.	
5	Encryption exchange (KEX) algorithm that can be used for SSH communication is changed. 6.4.7-xx and earlier: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256 6.4.8-00 and later: diffie-hellman-group1-sha1 (*1), diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1 (*1), diffie-hellman-group-exchange-sha256, curve25519-sha256, curve25519-sha256@libssh.org, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521 *1: It is disabled as the default setting of new installation. At update installation, the previous setting value is taken over.	6.4.8-00
6	diffie-hellman-group-exchange-sha1 of key exchange algorithm can be disabled by `sshconfset` command. For the sshconfset command, see "Hitachi Data Ingestor SSH Key Exchange Algorithm Feature Supplement".	6.4.8-00
7	The base version of OpenSSL that is an internal component of HDI is updated.	6.4.8-00
8	The base version of cURL that is an internal component of HDI is updated.	6.4.8-00
9	Public keys whose key length is less than 1024bit are unavailable when RSA is used as an encryption method.	6.4.8-00

No	Contents	Revision
	If a public key of less than 1024bit key length is used, access with SSH is disabled. In this case, create a public key of 1024bit or larger, and then add the key again. As reference information, the following describes how to confirm the length of public keys in Linux OS or Windows 10 environment. • How to confirm the key length in Linux OS or Windows 10 environment Store the public key file to be confirmed in an arbitrary location in the Linux OS or Windows 10 environment and run the command line below. In Windows 10 environment, use the command prompt. `ssh-keygen -l -f <public key file path>` When the above command line is run, the key length is displayed in the beginning of the line. If the displayed value is less than 1024, the public key cannot be used. In addition, when an RSA public key whose key length is less than 1024bit is specified, the following sentence is displayed, and the key length cannot be confirmed. In this case, the public key cannot be used with HDI 6.4.8-00 and later too. `<public key file path>` is not a public key file.	
10	When a directory name is renamed from a non-migration target name to a migration target name, KAQM37799-E is reported to prompt users to run arccorrection.	6.4.8-01
11	Installing GUI that manages single node with an installation media is enabled. To install GUI, use the installer in "SingleNodeGUI" folder in the media.	6.4.8-01
12	A new function is added. By the function, when the authentication method of the CIFS service is Active Directory and the user mapping function is used, the user mapping information whose mapping fails is sorted into “resolved negative cache” or “unresolved negative cache” to be cached depending on the cause for the mapping failure. resolved_negative_cache is the user mapping information to be cached when mapping fails at an inquiry to a domain controller or LDAP server for user mapping. The information is cached in the following cases. - The account is deleted from the domain. - When user mapping of the RID or LDAP method is used (at automatic allocation of user ID and group ID), a user ID or group ID to be allocated is outside the specified range. - When user mapping of Active Directory schema method is used, no user ID or no group ID is set to the Active Directory.	6.4.8-03

No	Contents	Revision
	unresolved_negative_cache is the user mapping information to be cached when an inquiry to a domain controller or LDAP server for user mapping fails. The information is cached in the following case. - The communication with the domain controller or LDAP server for user mapping is disabled due to disconnection of the communication path or a failure on an external server. In addition, discarding the above cache by running a `cifscachectl` command is supported. For details of the `cifscachectl` command, see Table 8 No.13.	
13	Setting a validity period of CIFS service cache by a `cifsoptset` command is enabled. For details of the `cifsoptset` command, see Table 8 No.8 to No.12.	6.4.8-03
14	A function to transfer the login result to a syslog server is added for the GUI that manages single node. To use the function, settings by a user with root permission is required. Contact customer support. The procedure for enabling the function is as follows. 1) Set the login log output setting file below for the node. /enas/conf/hsgui/hsgui.output.auth_log Owner/Group：root/root Permission: 644 File size: 0byte 2) Log in to GUI, click “Network & System Configuration” in the Settings area in the host-name window to display the System Setup Menu page. 3) From the drop-down list in the System Setup Menu page, select “system”, click “Display”, and then click “Syslog Setup” to display the Syslog Setup page. 4) Click “Add” in the Syslog Setup page to display the Add Syslog Setup page. 5) In the Add Syslog Setup page, specify a facility “auth” for “Item name”, and its priority. Setting example) auth.* * auth.info;auth.!warn: A log is transferred only when a login is successfully done. auth.warn: A log is transferred when a login fails. auth.info: A log is transferred when a login is successfully done or fails. A facility other than “auth”: A GUI login log cannot be transferred.	6.4.8-03

No	Contents	Revision
	6) Next, specify a host name for Output destination in the form of "@<hostname>", and then click "Add" to add the transfer setting. 7) Restart the node. <Output sample > Apr 22 00:07:07 DVMSERVER hsgui[15859]: Login Failed admin:10.213.93.111 Apr 22 00:07:12 DVMSERVER hsgui[15859]: Login Successful admin:10.213.93.111 Output items are date, host name of the node, hsgui[PID of hsgui]: Login failed (when login fails) or Login Successful (when login is successfully done), login user name, and IP address of access user. At new installation, and update installation from FOS whose version is earlier than 6.4.8-03, the login log output setting file does not exist so that make sure to set the login log output file. If the login log output setting file has been set with 6.4.8-03 or later, the file is taken over at version upgrade. When the system setting backup is stored while the login log output setting file is not set, if a system LU is restored by syslurestore, the login log output setting file is not taken over. Therefore, set the login log output setting file, and then store the system setting information file by system backup.	
15	For the single node GUI, the work space size and the file system size that are set by automatic calculation are displayed in a message on the confirmation dialog of the Edit File Systems window for file systems that use the Active File Migration function.	6.4.8-04
16	The version of Java to be used is changed to 1.8.0u291.	6.4.8-04

Requirements

Requirement for use Management Console for Single Node Configuration

- Operating system requirement for management console

Table 3. Supported platforms for management console

Operating Systems
Windows® 8.1 • Windows 8.1 • Windows 8.1 Enterprise • Windows 8.1 Pro
Windows 8.1 x64 Editions • Windows 8.1 • Windows 8.1 Enterprise • Windows 8.1 Pro
Windows Server 2012 • Windows Server 2012, Standard Edition • Windows Server 2012, Datacenter Edition
Windows Server 2012 R2 • Windows Server 2012 R2, Standard Edition • Windows Server 2012 R2, Datacenter Edition
Windows 10 • Windows 10 Home • Windows 10 Enterprise • Windows 10 Pro • Windows 10 Education
Windows 10 x64 Edition • Windows 10 Home • Windows 10 Enterprise • Windows 10 Pro • Windows 10 Education
Red Hat Enterprise Linux 6.4 #1
#1: OS that does not support TLS1.1 and TLS1.2.

- Required Web browser for management console

Table 4. Supported Web browsers for management console

Web browser	Remark
Internet Explorer 11.0 #3	32-bit version
Mozilla Firefox ESR 38.0.x #1, #2	x86 version
Mozilla Firefox ESR 45.x #1, #4	x86 version
Mozilla Firefox ESR 52.x #1, #4	x86 version
#1: x means that it does not depend on the version x. #2: Supported platforms for management console is only Red Hat Enterprise Linux. #3: If an operation to open a different window or tab is performed, an unnecessary. Window may be opened concurrently. For the case, see the usage precaution. #4: Supported platforms for management console is only Windows.	

- Required programs for management console

Table 5. Required programs for management console

Required Programs
Adobe® Flash® Player 10.1 or later

- When "Manage Migration Task" is executed during HDI maintenance, the KAQM23810-E message might be displayed. The error might be caused by the resource group had been stopped at that time. Please retry the operation after confirming resource group status is Online. If problem persists, acquire all log data and contact maintenance personnel.

Prerequisite program needed to use a particular function

- To use the virus scan function, Symantec Protection Engine 7.8, Trend Micro ServerProtect 5.8 or McAfee VirusScan Enterprise 8.8 is required.
- To scan virus using Trend Micro ServerProtect, HSPA (Hitachi Server Protect Agent) need to be installed on a scan server. HSPA supports the OS below.
    - Windows Server 2012 R2
    - Windows Server 2012

License keys

Hitachi Data Ingestor is a licensed product. Hitachi Data Ingestor includes a License Key.

Restrictions

- While a file path that is a data import target contains special characters, if a file or directory being imported is migrated from HDI to HCP, a message KAQM37094-E may be output. If "Invalid XML in custom metadata" is reported as detailed information of the above message, the migration can succeed by disabling the setting of "Check on ingestion that XML in custom meta data file is well-formed" in HCP name space. Ask the HCP administrator to disable the above setting until the data import is complete.
- If the file path accessed by a CIFS client contains special characters, real-time scanning may not be complete normally. For such files that the real-time scanning is not complete normally, change the file path so as not to contain any special characters and then retry the scanning where necessary.
- Some part of the graph might not be displayed, if the file system was unmounted during the time period where the request result or the cache hit ratio is displayed in the Monitor tab on the file-system-name window in a single node GUI.
- For CIFS share with SMB3.0 encryption enabled, the client cache is disabled regardless of settings of CIFS service and CIFS share.
- If you go back to edit screen without finishing Service Configuration Wizard because an error occurs, you might not be able to change password even if [Change password] of tenant administrator is checked on HCP settings. If you want to change password, uncheck the checkbox of [Change password] and then check it again.
- When you are using Roaming Home Directory feature enabled file system, and CIFS retry feature enabled, please stop the file access from CIFS clients before restarting CIFS services. When you restart CIFS service in a state that CIFS users still access to the CIFS share, below message will be displayed in HDI GUI and CLI, and there may be a case that HDI out puts the core file. In such an occasion, please make sure there is no CIFS user access, restart the CIFS service once again, obtain the core file, and contact the maintenance personnel.

  KAQG62001-W: smbd ended abnormally, and the core file was generated.

- When VSP Fx00 series is connected with HDI, the HDI recognizes the model name of the storage system as VSP Gx00, so that there are the following restrictions.
  - When the storage information is referred using HFSM or `fpstatus`, `fslist`, `lumaplist`, `lulist`, `vgrlist`, `clstatus`, or `horcdevlist` command, the model name is displayed as [VSP Gx00]. Therefore, identify the connected storage system using the serial number.

    - When specifying a model of storage system using `fpoffline`, `fponline`, `lumapadd`, `lumapdelete`, or `lumaplist` command, use [VSP_Gx00] but do not use [VSP Fx00].

- On the page of Task Management dialog, some keyboard operations may not be available. For example, choosing items from pull-down menu cannot be done from keyboard.
- In case user set the migration interval for 4 weeks with either of `arcmigset` or `arcmigedit` command, the operation you have done through [Edit Task] in migration task window will not be reflected to the settings.
- User cannot specify a character which consists of 4 bytes code in UTF-8 to following field.

    1) [Task Comment] field in [Add Task] and [Edit Task]
    2) [File name] field and [Directory path] field in policy information
    3) Arguments of `arcmigset` and `arcmigedit` commands

- The Service Configuration Wizard appears needlessly when the provisioning process complete successfully. Please close the Service Configuration Wizard.
- When combining with HCP, set a user name or password of HCP tenant administrator using 64 or less one-byte alphanumeric characters.
- When restoring system LU using the system setting information that is stored while a read-write-content-sharing file system exists, if Background is specified for the method of data restoring interactively for `syslurestore` command, KAQM37483-E message is displayed as a system message and is notified via an SNMP, but no action is required to take for the message. The data of the file system is recovered without any problem.
- Under the following conditions, even if then KAQM37751-E message is displayed and is notified via an SNMP during stopping OS, the OS is stopped successfully. The action for this message is not needed.

    - Single node configuration.
    - There are file systems which the Active File Migration function is used.

- When a user who belongs to an external server (Active Directory, NIS, LDAP) is used as an FTP user, the user cannot access data with permission of non-primary group defined in external authentication server.
- When data is migrated to HCP using Active File Migration functionality, if the capacity of work space is insufficient, the recommended size of work space displayed in message KAQM37753-W is smaller than the actually required capacity. If the message appears, verify the status of work space, refer Installation and Configuration Guide, and calculate the recommended size corresponding to the work space status. After that, expand the capacity of work space to be larger than the recommended size.
- While a file system that uses Active File Migration functionality exists, if a system LU is restored using stored system setting information and the used size of work space

exceeds 80% after that, KAQS19001-W message is displayed as a system message and it is reported using SNMP.
No actions are required for the message.

- When data is shared between HDIs by using the read-write-content-sharing function or the home-directory-roaming function, if a file is deleted or renamed at a site, KAQM37780-E message may be output at a different site. If the message is output in an environment where the read-write-content-sharing or home-directory-roaming function is used, take the actions below.

1. Download all log data.

2. Check the target file from the file path output in hsmarc_stub.err included in /enas/log/ufmras.tar.gz of all log data.

3. Verify whether the target file has been deleted or renamed at a different site. If it cannot be confirmed, verify whether removing the file is OK or not. If the file has been deleted or renamed at a different site, or the file is the one that can be deleted, take step 4. If whether the file is deleted or renamed is unknown, or the file is the one that should not be deleted, take step 5.

4. Open the folder/directory of the target file. If message KAQM37780-E is still output continuously after opening the folder or directory, contact the maintenance personnel in accordance with the action in the message.

5. Contact maintenance personnel in accordance with the action in the message KAQM37780-E.

- If there are 30,000 or more pinned files, Download List of Pinned Files on single node GUI may turn to error. In this case, use `arcresidentlist` command.
- When accessing a single node GUI while connection to HCP is disabled, "The set up account does not have the permissions required to access the namespace. Ask the HCP administrator to set the proper permissions for the account." or "A data access account for managing namespaces does not exist. Executing the Service Settings wizard will create an account." might be displayed in the dashboard. In this case, check the network status, remove the cause for disabled connection to HCP, and then perform refresh.
- "app:/swf/MainConsole.swf" is displayed on the title of the following dialogs.
    - Upload License key file dialog box in the License Settings.
    - Upload Mapping file dialog box in the Import Files dialog box.
    - Download Scan Failure List dialog box in the Import Files dialog box.
    - Download Read Failure List dialog box in the Import Files dialog box.
    - Download Import Failure List dialog box in the Import Files dialog box.
    - Download Chargeback Report dialog box.
    - Download All Log Data dialog box.
    - Download List of Pinned Files dialog box in the Cache Resident Policy.

Cautions

Caution for update installation

- It was revised to display a confirmation message at the time of command practice for the following commands which involves a stop of the service.
  Therefore when you perform an update installation from a version former than 02-02-01-00-00, confirm whether you are using a command listed below in a script, and if there is a point being used, specify a `-y` option, and suppress the output of the execution confirmation message.
  - `clstop`
  - `ndstop`
  - `rgstop`
  - `rgmove`
- With the introduction of the SMB3.0 feature in 6.0.0-00, HDI consumes more memory than it used to do. We recommend to install additional memory for the HDI models on CR servers as such with CR upgrade kit, and for HDI VM model, we recommend to add virtual memory to 8GB and more as instructed in (Link: https://knowledge.hitachivantara.com/Documents/Storage/Data_Ingestor/6.4.8/Install_and_configure_HDI/Data_Ingestor_Virtual_Appliance_Installation_Guide).
- "VNDB_LVM", "VNDB_Filesystem" and "VNDB_NFS" are unavailable as HDI cluster name and node name.
  To update from a version earlier than 5.0.0-01, verify if "VNDB_LVM", "VNDB_Filesystem", and "VNDB_NFS" are not used as a cluster name and node name before the update installation.
  If any of the above names are used, change the cluster name and node name before the update installation.
- Do not perform HDI node software update installation concurrently with an operation to delete LUN assigned to HDI or to change configuration, such as size change, running on a storage sub-system connected to HDI. If the operations are performed at the same time, the node software update installation may fail.
- In cluster configuration where the version of a node (node1) is 6.0.2-00 or later and that of the other node (node2) is earlier than 6.0.2-00, when failover or failback is performed from node1 to node2, the option value of service performance statistics collection function of CIFS service is taken over from node1 to node2. If the value taken over needs to be turned back to the previous, run `perfmonctl` (managing the service performance statistics) command for the resource group on the node2 side.
- When SHA-1 signed public key certificate issued by Certificate Authority is used, obtain a SHA-2 signed certificate from Certificate Authority and then set it after update installation. If a public key certificate issued by Certificate Authority is not used before the update installation, set SHA-2 self-signed public key certificate in the same way as new installation.

- When a character string consisting of 65 or more characters is specified for `--key-passwd` as a password of private key for public key certificate prepared by administrator, access from a browser is disabled at update installation. For this, run the `certctl` command with `--reset` option specified to initialize the set certificate before the update installation to a version 6.1.1-00 or later.
  During the course of update installation, below anomalies occur on HDI Single node and Cluster model in case the certificate is NOT initialized. For Single node model, log in screen for the management UI is not available after the update installation. For Cluster model, after the completion of node0 update installation, node restart fails then HFSM access to the nodes becomes unavailable with issuing KAQM20046-E message on HFSM screen.
  Please perform below procedure for Single Node and Cluster Models respectively, for the recovery.

  <Single Node Model>
  1. Log in to node via ssh
  2. Confirm the HDI version is updated by `versionlist` command.
  3. Confirm resource group is up and running by `rgstatus` command.
  4. Initialize certificate by `certctl` command with reset option (`--reset`).
  5. Confirm log in screen is available on Browser.

  <Cluster Model>
  1. Log in to node1 via ssh and execute following steps.
  1) Confirm the cluster node and resource group status as below by `clstatus` command.
  a) Node status: node 0 is "INACTIVE", node1 is "UP"
  b) Resource Group status: Resource groups of both nodes are running on node1 and show status "Online"
  2) Confirm the HDI version is NOT updated, by `versionlist` command.
  3) Initialize certificate by `certctl` command with reset option (`--reset`).

  2. Log in to node0 via ssh and execute following steps.
  1) Confirm the HDI version is updated, by `versionlist` command.
  2) Initialize certificate by `certctl` command with reset option (`--reset`).
  3) Start node0 by `ndstart` command.
  4) Confirm node0 status is "UP" by `clstatus` command.

  3. Log in to HFSM to perform following steps.
  1) Execute "Refresh Processing Node" to check connection error doesn't occur.
  2) Failover both resource groups to node0 from "Cluster Management" screen.
  3) Execute "Refresh Processing Node" to refresh the HFSM information.
  4) Execute "Update Software" from "System Software" pane to update node1.
  5) After the completion of update install, confirm HDI version of both nodes are up to date.

6) Both resource groups are running on node0. Failback one of the resource group whose default host node is node1.

Caution for update installation from version earlier than 6.1.0-00

At update installation from a version earlier than 6.1.0-00, the migration task setting changes as follows. Record the task setting before update installation, and then apply the setting again after update installation.

Function	Interval	Duration	Policy (Filter Condition)	Task Status
Content Sharing OFF (If Criteria condition is [File Is All])	1 hour	None	None	Enabled
Content Sharing OFF (If Criteria condition is not [File Is All])	1 hour	None	None	Disabled
Content Sharing ON (Home directory)	1 hour	None	None	Enabled
Content Sharing ON (Read/Write)	10 minutes	None	None	Enabled

With versions earlier than 6.1.0-00, there is a restriction that only 4 migration tasks can work concurrently, which is lifted from 6.1.0-00 so that multiple migration tasks can run concurrently, but it may cause CPU and memory to be depleted. Therefore, if there are 8 or more file systems, verify the schedule and pay attention so that 8 or more migration tasks are not performed simultaneously.

Caution for system creation

Upper limit for resource

Upper limit (recommended value) for each resource of HDI is as follows.

No	Resource		Upper limit (Recommended value)	Note
1	Number of migration	Content Sharing OFF	8	If file systems exceeding the recommended value are created, memory usage and CPU utilization
2				

No	Resource		Upper limit (Recommended value)	Note
	target file systems	Content Sharing ON (Read-Only)		increase, giving impact on the system performance. To create file systems exceeding the value, it is recommended to use separate systems.
3		Content Sharing ON (Home directory , Read/Write)	1	
4				
5	Number of threads (for migration, for others)		90 for each	- If the number of CPU cores or memory size is small, do not increase the number of threads. - If client I/O performance degrades during migration, reduce the number of threads, which can mitigate the impact on client I/Os.
6	File system size	Active File Migration function is enabled	Less than 32TB	If the size exceeds the value, to disable the AFM function or to divide file systems is recommended.
		HDI Remote Server	Less than 17TB	If the size exceeds the value, to divide file systems is recommended.
7	Number of files or directories per file system		Less than 1 hundred million	Increase in the number of files or directories causes the file system performance to degrade or a recovery operation at a failure to take a long time. If the number of files or directories exceeds the value, to divide file systems is recommended.
8	File size		Up to 2TB	The upper limit of file size on HCP is 2TB.
9	Number of ACEs		700 for each file/directory	Setting over 700 ACEs causes an error.
10		Per system	4000	Tune Custom schedule so that the total sum of the number of past version directories per share does

No	Resource		Upper limit (Recommended value)	Note
	Number of past version directories			not exceed the value. If the number of past version directories exceeds the value, stopping resource groups takes a long time and Failover may fail.
		Per file system	60	Tune Custom schedule so that the number of past version directories in last one week does not exceed the value. If the number of past version directories exceeds the value, CIFS clients cannot refer the past version data on the [Previous Versions] tab from the property of folder or file.
11	Network with HCP		Bandwidth: 10Mbps or higher Delay: 100msec or shorter	If network bandwidth is not sufficient, migration operation takes a longer time and it may turn to time-out. Tune the time-out value.
12	Maximum number of CIFS to be connected		6000 or less	The upper limit varies depending on the memory size and auto-reload setting.

Caution when editing link trunking

- When link trunking information is edited, virtual IP addresses are reset. The time required to reset the virtual IP address is about 10 to 20 seconds per virtual IP address.
  For this, if all the following conditions are met, editing link trunking may turn to time-out and fail. (Time-out time is 30 minutes.)

  1) Multiple VLAN interfaces are set to the link trunking port.
  2) 90 or more virtual IP addresses in total are set to the set VLAN interfaces.

When the link trunking is edited under the above conditions, delete the interfaces set to the target link trunking port, reduce the number of virtual IP addresses to be less than that of (2), and then edit the link trunking. After editing link trunking is complete, set the interfaces again.

Caution when using RID method user mapping

- Make sure to set mapping for a domain registered to node.
  If the above mapping is not set, access to share directory from a trusted domain user is disabled.

Caution for subtree Quota monitoring function

- When the subtree Quota monitoring is set with versions earlier than 3.2.0-00, "the measure for the problem of CPU usage increase at subtree Quota monitoring" with versions 5.2.0-00 and later does not become effective.
- To enable the measure, set the subtree Quota monitoring again to one of directories with the subtree Quota monitoring set in each file system.

Caution for Read Write Content Sharing

- If a file with a long name is migrated to a .conflict directory concurrently with an update in a different location, the file cannot be opened and copied to an arbitrary location other than .conflict directory. Therefore, set a file name to be 235 bytes or less in the case of NFS client.
- If power supply of node stops during migration, all end users who use Read Write Content Sharing cannot operate directories.
  At the time, the message below is output in hsmarc.log of each node.

  KAQM37038-E Migration failed because a file of the same name exists on the HCP system. (file path = /system/*namespace-name*/mig_results/sync_list.*number*)

  Also, the size of the following object referred from HCP namespace browser is 0.

  `https://rwcs-system.`*tenant-name*`.`*host-name*`/rest/system/`*namespace-name*`/mig_results/sync_list.`*maximum-number*

  To restore the status, contact HCP administrator and ask to download and upload the latest version of "sync_list.*maximum-number*" displayed on [Show versions] of HCP namespace browser.
- When an RWCS file system that has not been mounted for a long period of time (default: 7 or more days) is mounted again, KAQM37021-E error may be reported. In this case, inconsistency of file system occurs so that run `arcrestore` command to ensure the consistency of file system.

Caution when linking with HCP Anywhere

- When you stop a power supply of HCP Anywhere or HCP in environment linking with HCP Anywhere, please stop a power supply of the HDI earlier.

If you stop a power supply of HCP Anywhere or HCP without stopping a power supply of the HDI, reporting from HDI to HCP Anywhere might fail in KAQM71018-E (authentication error) and service of the HDI might stop.
If KAQM71018-E (authentication error) occurs, please start HCP Anywhere and HCP, ask a manager of HCP Anywhere to reissue the password for the authentication, and perform [Update HCP Anywhere Credentials] in GUI of the HDI.

Caution for SMB3.0 encryption function

- A CIFS client supporting SMB3.0 can access CIFS share with SMB3.0 encryption enabled.
  For the setting on HDI when the encryption is used, see the table below.

No	Encryption setting	CIFS service [SMB encryption] value	CIFS share [SMB Encryption] value
1	Encryption	Mandatory	Inherit CIFS service default
2	Non-encryption	Disabled	Inherit CIFS service default
3	Encryption and non-encryption	Auto	Encryption [Mandatory] Non-encryption [Disable]

Caution ACL for the shared directory

All of the information regarding ACL for the shared directory are stored in share_info.tdb. Maximum size of share_info.tdb is 64 Mbyte. CIFS service failure may be caused due to the disk space shortage if the size is more than 64 Mbyte. Size of share_info.tdb depends on "the number of CIFS share" and "total of the number of ACE for the shared directory of each share". For this reason, set "the number of CIFS share" and "total of the number of ACE for the shared directory of each share" so that the size of share_info.tdb does not exceed 64 Mbyte. The following is the example of setting.

#	Number of CIFS share	Total of the number of ACE for the shared directory of each share	Size of share_info.tdb
1	21	1820	16 Mbyte
2	1000	1820	64 Mbyte
3	7500	210	60 Mbyte

You can see the size of share_info.tdb by collecting node log files and checking the share_info.tdb size shown below.

- Cluster Model

  (node 0)
  `/enassys/hifailsafe/CHN1/share_info.tdb`

  (node 1)
  `/enassys/hifailsafe/CHN5/share_info.tdb`

- Non-Cluster Model

  `/etc/cifs/CHN/CHN1/share_info.tdb`

Caution when deny setting of ACL is prioritized

In versions earlier than 5.0.1-00, deny setting of ACL does not take priority as intended due to the problem that has been fixed with 5.0.1-00. The priority order of deny setting incorrectly may be higher caused by this problem. As a solution, set the ACL order again by the following resetting procedures after update installation.

To reset, perform one of the following operations.

- Resetting procedure from Windows command.

  1) Run `icacls` command for the topmost directory (*1) of the resetting target file.

     Record all of ACLs under the specified directories displayed.

  2) Make the setting from the topmost directory (*1) to all of subordinate directories/files by `icacls` command based on the ACLs recorded in (1).

Example)

  - ACL displayed in (1).

file-path userA`:(OI)(CI)(W)`

  - For the command of the setting in (2), change options according to the ACLs displayed in (1).

`icacls` *file-path* `/grant` *userA*`:(OI)(CI)(W)`

- Resetting procedure from Windows Properties window.

  1) From the topmost directory (*1) of resetting target to all of subordinate directories/files, display ACLs by selecting [Properties], [Security], and then [Detailed setting] and record all ACLs.
  2) From the topmost directory (*1) to all subordinate directories/files, delete entries of deny access setting by selecting [Properties], [Security], [Detailed setting] and then [Change access permission], and then set the access permission in an arbitrary order based on the ACLs recorded in (1).

*1: The topmost directory means the following.

- In case of setting recursively the ACL to the directory tree, it means the top of the directory of the tree.
- In case of setting the ACL only to specific directory, it means the directory.
- In case of setting the ACL only to specific file, it means the directory in which the file belongs.

Caution for NFS share creation

For a host that is allowed to access the NFS share, specify a host name that starts with an alphabet and consists of alphanumeric, hyphen (-) and underscore (_).

Caution when outputting system operation information

When operation information of the system is output to a directory on a file system by running `sysinfoget` command, if the directory name contains any multi-byte characters, extracting the archive file output by `sysinfoget` command may fail depending on the OS environment where the operation information is transferred.

To output operation information to a directory on the file system, output the information to a directory whose name does not contain multi-byte characters, or convert the character code of the archive file to the one that is used in the OS environment where the information is transferred by using an application for conversion.

Caution when creating keytab file for Kerberos authentication

Do not use space, quotation mark ("), and colon (:) for a name of keytab file for Kerberos authentication.

Caution for file system setting information display

If a failure occurs on a file system, the setting information of the file system may not be displayed correctly on single node GUI.
Restore the failure condition, perform refresh processing, and then refer the file system setting information.

Caution for ACL setting for Authenticated Users and Network accounts

Access control by ACL setting for Authenticated Users and Network accounts which are Windows built-in accounts is not supported for Classic ACL type file system.
The function can be applied to Advanced ACL type file systems only.

Caution when using [Previous Versions] of Windows

When past versions are displayed on the [Previous Versions] tab, if available past versions are not displayed, close the tab, wait for a while, and then open the tab again. The above phenomenon may occur when the [Previous Versions] tab is displayed while a migration operation is in process.

Caution about filesystem

Do not mount filesystem as Read-Only.

Caution when connecting Mac OSX 10.10/10.11 as CIFS client

The following notes applies when connecting Mac OSX 10.10 and 10.11 as a CIFS client because only SMB2.0 is supported.

1) Specify SMB2.0 for SMB protocol that is used for accesses from the CIFS client on HDI.
   For detailed settings, refer to "Hitachi Data Ingestor Cluster Administrator's Guide" or "Hitachi Data Ingestor Single Node Administrator's Guide".
   On the setting of the client with Mac OSX 10.10/10.11, minor versions, such as SMB2.0/2.1, cannot be specified. In this case, make the setting on HDI.
2) With Mac OSX 10.9 or earlier, only SMB1.0 is supported as a CIFS client. To have both versions; Mac OSX 10.9 or earlier and Mac OSX 10.10/10.11, as CIFS clients, confine the connecting SMB version for the client with Mac OSX 10.9 or earlier to 1.0 by the setting on each client.
   For detailed settings, refer to "Hitachi Data Ingestor File System Protocols (CIFS/NFS) Administrator's Guide".
   If the Mac OSX is upgraded from a version 10.9 or earlier to 10.10/10.11, apply the setting of (1) and then release the restriction of (2) (to confine the SMB version to 1.0).
3) If any multi-byte characters are used for CIFS share name with Mac OSX 10.11, because of a matter of Mac client, connection from the Mac client to CIFS may be disabled.
   Avoid the use of multi-byte characters for share names.

Caution when connecting Mac OSX as CIFS client

Notes applied to Mac OSX regardless of version are as follows.

1) Even when having write permission, an operation to write on a file may fail with Mac OSX depending on the behavior of application running on the Mac OSX.
   For this, make sure to apply the settings below in advance when performing an operation with file update on Mac OSX.

a) For users who operate or groups to which the users belong, set Full control permission for folders with extension of .TemporaryItems and all files and folders in the folders directly under a CIFS share.

b) For users, set "Delete" permission for the operation target files or "Delete subfolders and files" permission for parent folders of the operation target files.

c) Set access permission for the upper folder of operation target files for users who operate and groups to which the users belong so that the access permission can be inherited from the upper folder.

2) While only the user who is operating a file has access permission for the file, if access permission for the file is set for a different user on "Sharing & Permissions" panel of Mac OSX Finder, all ACLs may be deleted.
To avoid the above, set access permission for the upper folder of the file for both users who operate and groups to which the users belong so that the access permission can be inherited from the upper folder.
3) When writing on a read-only file from Mac OSX standard TextEdit, an error for having no permission is displayed and the writing may fail.
For users who release the read-only attribute of the file, add "Change Permissions" permission for the file.

Caution for SMB signing

If you use SMB signing for communication with a CIFS client, you can prevent man-in-the-middle attacks that tamper with SMB packets being transferred. Note, however, that the security improvements granted by SMB signing will also degrade file access performance.

Before you can use SMB signing, the necessary settings must be specified for both the client and the HDI system. The HDI system always uses SMB signing when the client requests SMB signing for communication via the SMB 2.0, SMB 2.1, or SMB 3.0 protocol. In addition, you can use the `cifsoptset` command to specify whether to use SMB signing for SMB 1.0 communication. With the initial settings, the HDI system does not use SMB signing for SMB 1.0 communication.

Caution when selecting time zone

If you choose a time zone where daylight-saving time is introduced or abolished in 2009 or later, time on HDI may differ from current local time.
To use such a time zone, use Greenwich Mean Time (GMT).

Caution when using offline files with Guest account

When CIFS Client that HDI treats as a guest account accesses a file in the offline state, it may not be accessible.
When referring to a file in the offline state, do not perform CIFS access with the guest

account.
As for the guest account, see the Hitachi Data Ingestor Cluster Administrator's Guide or the Hitachi Data Ingestor Single Node Administrator's Guide.

Caution for WWW browser security setting

On the security setting in the Advanced tab on WWW browser connected to HDI or management server, clear check boxes for Use SSL2.0 and Use SSL3.0.

Caution for disabling SMB1.0 of domain controller

If the maximum version of the SMB protocol used for the communication with a domain controller (client_ipc_max_protocol) is SMB1.0, consider changing to SMB2.0 or later prior to adding or changing a domain controller of Active Directory domain including trusted domains. If SMB is not changed to 2.0 or later, communication with domain controllers with Windows Server 2016 or later for which SMB1.0 is disabled as default (Windows Server version 1709) and domain controllers with SMB1.0 disabled is disabled, and starting a CIFS service, starting a resource group, and user authentication from a CIFS client may fail.

To confirm client_ipc_max_protocol, run a `cifsoptlist` command. To change SMB to 2.0 or later, run a `cifsoptset` command.

Usage precautions

Usage Precautions for Migration Management

- Please configure the same time zone of HDI and the Management console. If these time zones are different, the different time zone is applied the configuration and display of the migration management time.

Usage Precautions for NFS Service

- When stopping or restarting NFS service, please request the administrator using service of a client to suspend access to File Sharing.
- When using the `nfscacheflush` command, please do not access from an NFS client to a file system. If the `nfscacheflush` command is used during accessing, an EIO error may occur.
- When the file system is used and a file lock demand competes by the NFS protocol version 2 or the version 3, and the TCP protocol from the NFS client using a version higher than Red Hat software Enterprise Linux Advanced Platform v5.2 (Linux version 2.6.18-92.e15), file lock operation may become slow.

Usage Precautions for CIFS Service

- The first CIFS access after failover or failback may fail. In this case, retry the operation.
- When CIFS clients display a shortcut file with the offline attribute, the file's icon might not be displayed.
  You can confirm whether the file is shortcut file or not from the line of type on the details expression of Explorer.

Usage Precautions for KAQG72016-E Message

- Check the status of the cluster. If the status is DISABLE, contact maintenance personnel.

Usage Precautions for "CIFS bypass traverse checking" function

- The default setting of "CIFS bypass traverse checking" when creating a file system has been changed as Table 6 in 4.2.0-00 or later.

Table 6. Default operation of creating a file system

No	Function	before 4.2.0-00	4.2.0-00 or later
1	CIFS bypass traverse checking function	Disable (Not supported)	Enable

- CIFS bypass traverse checking function has been setup as disable if the update installation from a version former than 4.2.0-00 is performed. Please change the setting when you use CIFS bypass traverse checking function

Usage Precautions when integrating HCP

- If the update installation from a version former than 3.2.1-00 is performed, then replica HCP setting is deactivated. Configure replica HCP again as necessary. If the file system refers to data in a file system on another HDI system, configure replica system again as necessary.
- When update installation is performed from a version earlier than 3.2.0-00, perform one of the following operations.
    - Create a user account of tenant administrator with the name same as data access account in HCP.
    - After update installation of Hitachi File Services Manager, perform the setting of tenant administrator using HCP Settings of Configuration Wizard.

- When a file of 200MB or larger is migrated with the HTTP compression enabled while other than "0" is set to the period for monitoring the transfer speed and the lowest transfer speed to the HCP system, the average speed of transfer may be lower than the limit and the migration may fail with time-out. Set "0" to the period for monitoring the transfer speed and the lowest transfer speed, so that a time-out does not occur until the time set to time-out of communication to HCP has passed even when the transfer speed to HCP is low.
- When the priority of file stubbing is changed by `arcconfedit` command, if the priority of stubbing is high, the processing time of data reading/writing from a client and migration/recall may get longer. Do not keep the stubbing priority high but change it in the case that an increase in data writing from clients is expected.
- When a failure occurs in the network between HDI and HCP or in HCP, a wait for a response from HCP continues, which may affect the performance of accesses from file share clients to HDI. In order to mitigate the effect on the access performance, set the wait time until reconnecting to HCP by `arcconfedit` command to be larger than `--low-speed-time` option. However, if a temporary communication errors frequently occur, such as a case where HDI is combined with HCP via network, as the wait status can be solved by the temporary communication error, set 60 or lower value. When an operation with communication to HCP, such as migration and recall, is performed under the condition that the communication error is detected but the wait time has not yet passed, a communication error is returned instead of connecting to HCP. If the wait time has passed, connecting to HCP is tried. Note that access to HCP is disabled until the wait time passes even when the error has been solved. Therefore, set the wait time to "0" and see if accesses to HCP are enabled. If the user can successfully access, restore the setting to the previous.
- By the default setting, 5% (upper limit 40GB) of total capacity of the file system are secured as the reserved space that a system uses when creating a file system in 5.2.0-00 or later which links to HCP. This reserved space prevents that migration process and stubbing process are affected when the file system lacked the capacity. Because user cannot use reserved space, design total capacity of file system as total of user capacity and reserved space.
- If the update installation from a version former than 5.2.0-00 is performed, reserved space is set as 0% to existing file systems. If necessary, set reserved space using `arcresvset` command.
- When the reserved space is set in 5.2.0-00 or later, update management information process starts at 0:07 a.m. for stubbing process. This updating process takes up to an hour. While this process is running, the load of the system increases.
- If KAQM55019-E message is reported at policy or schedule setting, the file system may be full. In this case, run `arcresvget` command and check the reservation capacity of the file system combined with HCP. If reservation capacity is not set, check the free capacity of the file system. If there is no free capacity, delete unnecessary files.
- When user's operation to unmount the file system coincides with the migration event on the file system, there may be a case that KAQM04045-E displayed and the

unmount operation fails. In above case is observed, please make sure that the migration completes and try to unmount the file system.

- If user run `arcmigstatus` command while HDI runs migration, there might be chance to get KAQM37764-I message in output of the command. In the case, please re-run the command after a while.
- If migration is performed using the Large File Transfer function during data import, the Large File Transfer processing fails and normal migration takes place. Set the Large File Transfer function to be disabled during data import.
- If synchronization fails due to a failure, such as an error in communication with HCP, the data might be restored from the HCP at the next synchronization.
  If the data is restored from the HCP while an NFS share is created in a subdirectory other than mount point of a file system, a share directory is created again so that an NFS access turns to ESTALE error. In this case, KAQM37782-W or KAQM37783-W is reported in SNMP trap when a restore operation is performed. In accordance with the message, mount the share directory again from an NFS client.
- If communication with HCP fails when the Dashboard tab is opened on the single node GUI, message [The set up account does not have the permissions required to access the namespace. Ask the HCP administrator to set the proper permissions for the account.] is displayed. In this case, remove the cause for the failure of communication with HCP, and then refresh the single node GUI.
- When a file in a past version is referred from a CIFS client using Volume Shadow Copy Service, other CIFS accesses may be disabled. In this case, reduce the number of read-ahead threads by using the `--cloud-vss-thread-max` option of the `arcconfedit` command. Setting around five for the number of read-ahead threads is recommended.
- If the commit mode of Auto commit of a worm file system is auto, a worm file restored by arcrestore with expired retention period cannot be deleted. In this case, delete the file by taking the following actions.
  (1) Verify that if the Max retention is “infinite” by running a `fslist` command (with `-v` option specified).
  (2) If the Max retention is “infinite”, change it to other than “infinite” by running a `fsedit` command (`-w -M` option specified).
  (3) Set read-only for the target file.
    (a) In the case of CIFS share file
      Change the file attribute setting to read-only instead of ACL setting.
    (b) In the case of NFS share file
      Cancel the write permission (w) for users, groups, and others so that the file becomes read-only.
  (4) Allow writing to the target file.
    (a) In the case of CIFS share file
      Cancel the read-only setting for the file.
    (b) In the case of NFS share file
      Set the writing permission (w) for any of users, groups, or others so that the read-only setting is canceled for the file.
  (5) Delete the target file.

Usage Precautions for CIFS Access Log

- If the update installation from a version former than 4.0.0-03 is performed, "Rename items" (renaming files or folders) event of CIFS access log is not set in the Setting Events Logged to the CIFS Access Log page in GUI. If necessary, set the CIFS access log setting.

Usage Precautions for Negotiation Mode (4.1.0-02 or later)

- With the negotiation mode having been added in 4.1.0-02, when the update installation from a version former than that is performed, the following negotiation mode name is changed. However, no action is required because the setting is not changed.

  Before the change
  (1) 1000Base Full Duplex
  After the change
  (1) 1000Base Full Duplex(Auto Negotiation)

- In addition, when the update installation from a version former than 3.2.3-00 is performed, the following negotiation mode names are changed. However, no action is required because the settings are not changed.

  Before the change
  (1) 100Base Full Duplex
  (2) 100Base Half Duplex
  After the change
  (1) 100Base Full Duplex(Auto Negotiation)
  (2) 100Base Half Duplex(Auto Negotiation)

Usage precaution for Internet Explorer 11.0 as Management console

- An operation to open different window or tab by a click of anchor or button on the window may cause an unnecessary window (such as blank or in transition window) to be opened concurrently. In this case, close the unnecessary window. If this problem persists, create a new Windows user account and then operate the browser with the new user.

Usage precaution for "subfolder monitoring" function

- When the setting of subfolder monitoring function (a function to report any change in response to a request for "monitoring all files and folders under the specified folder" from a CIFS client) is changed from "Disable" to "Enable", if many CIFS clients are

connected, HDI may be highly loaded. In this case, setting the subfolder monitoring function to "disable" can solve the high load status.

Usage precautions for SNMP manager

- Hitachi-specific MIB object definition file is changed with the version 3.2.0-00. When update installation is performed from a version earlier than 3.2.0-00 to this version, the MIB definition file loaded in SNMP manager needs to be updated too. Load the MIB definition file from the following path of provided media.

```
\etc\snmp\STD-EX-MIB.txt
```

Documentation corrections

Table 7. Corrections for "Hitachi Data Ingestor Error Codes"

No	Location to be corrected	Corrections	
1	KAQM37 messages Table 5-25 KAQM37 messages Message ID: KAQM37228-E	Before	Message: Restoration of a data-referencing file system failed. (reason = {insufficient memory|no disk space|HCP communication error|authentication error|some other error}, file system name = file-system-name)
		After	Message: Restoration of a data-referencing file system failed. (reason = {insufficient memory|no disk space|HCP communication error|authentication error|lock timeout|some other error}, file system name = file-system-name)
2	Table 3-1 KAQG messages	Add	Message ID: KAQG52069-E Message: Acquisition of a lock failed during execution of a command. Wait a while, and then execute the command again. Description and Action: Acquisition of a lock failed during execution of a command. (O) Wait a while, and then execute the command again. If the error persists, acquire all the log data, and then contact maintenance personnel.

No	Location to be corrected	Corrections	
3	KAQM26 messages Table 5-19 KAQM26 messages	Add	Message ID: KAQM26053-W Message: Failed to load migration task. Description and Action: The migration task could not be loaded because the file system name could not be acquired. (O) Collect all log data, and then contact maintenance personnel.
4	KAQM26 messages Table 5-19 KAQM26 messages	Add	Message ID: KAQM26154-E Message: The node to connect to is not supported. Make sure the node to be connected is correct. Description and Action: The connected node is not supported. (O) Check the node to connect to. If the destination node is correct, download a program of HDI Single Node GUI from the node, and perform the installation of the HDI Single Node GUI.
5	KAQM26 messages Table 5-19 KAQM26 messages	Add	Message ID: KAQM26155-E Message: The node to connect to is not supported. Perform update installation to the node. In the case you cannot perform update installation, use command for management or use GUI via browser. Description and Action: The node cannot be connected because the version of the connected node is old. (O) Perform update installation to the node. In the case you cannot perform update installation, use command for management or check the version of the node and use the corresponding GUI.

No	Location to be corrected	Corrections	
6	KAQM26 messages Table 5-19 KAQM26 messages	Add	Message ID: KAQM26156-E Message: As the version of the node to connect to is new, the node cannot be connected. Download the program of Single Node GUI from the following URL and perform the update installation. Description and Action: The node cannot be connected because the version of the connected node is new. (O) Download a program of HDI Single Node GUI from the node, and perform the installation of the HDI Single Node GUI.
7	Table 3-1 KAQG messages Message ID: KAQG52058-E	Before	Description and Action: (O) To discard the Kerberos tickets that are cached by the CIFS client, log out from the CIFS client, and then log in to the CIFS client again. For details, see the File System Protocols (CIFS/NFS) Administrator's Guide.
		After	Description and Action: (O) To discard the Kerberos tickets that are cached by the CIFS client, log out from the CIFS client, and then log in to the CIFS client again. For details, see the File System Protocols (CIFS/NFS) Administrator's Guide. If no end users are reporting access issues, no action is required.
8	Messages sent by using SNMP traps or emails Messages sent from File Services Manager (KAQK, KAQM messages) Table 1-4 List of messages sent from File Services Manager	Add	Message ID: KAQM37799-E Severity level: Error Corresponding MIB object: stdEventTrapError Available notification methods: SNMP and E-mail

No	Location to be corrected	Corrections	
9	KAQM37 messages Table 5-25 KAQM37 messages	Add	Message ID: KAQM37799-E Message: There are some directories that are not targeted to be migrated because they were renamed from the migration excluded directory name to the migration target directory name. (file system name = file-system-name) Description and Action: There are some directories that are not targeted to be migrated because they were renamed from the migration excluded directory name to the migration target directory name. (O) Using the `arccorrection` command, rebuild the management information for the file system.
10	KAQM26 messages Table 5-19 KAQM26 messages KAQM26154-E	Before	Description and Action: The connected node is not supported. (O) Check the node to connect to. If the destination node is correct, download a program of HDI Single Node GUI from the node, and perform the installation of the HDI Single Node GUI.
		After	Description and Action: The connected node is not supported. (O) Check the node to connect to. If the destination node is correct, install the HDI Single Node GUI with either way of the following. (1) Download the program from the node and perform the installation. (2) Perform the installation from the installation media if you have them. For details of installing Single Node GUI, see "Configuring an environment" in the Hitachi Data Ingestor Single Node Getting Started Guide.
11	KAQM26 messages Table 5-19 KAQM26 messages	Before	Message: As the version of the node to connect to is new, the node cannot be connected. Download the program of Single Node GUI from the following URL and perform the update installation. Description and Action:

No	Location to be corrected	Corrections	
	KAQM26156-E		The node cannot be connected because the version of the connected node is new. (O) Download a program of HDI Single Node GUI from the node, and perform the installation of the HDI Single Node GUI.
		After	Message: As the version of the node to connect to is new, the node cannot be connected. Install the latest program of the single node GUI. Description and Action: The node cannot be connected because the version of the connected node is new. (O) Install the HDI single node GUI with either way of the following. (1) Download the program from the node and perform the installation. (2) Perform the installation from the installation media if you have them. For details of installing Single Node GUI, see "Configuring an environment" in the Hitachi Data Ingestor Single Node Getting Started Guide.
12	KAQM20 messages Table 5-14 KAQM20 messages KAQM20046-E	Before	Description and Action: The system software installation timed out. (O) Wait a while, perform refresh processing, and then confirm that the system software has been updated. If node information could not be acquired, check the boot status of the OS. If the OS is not running, start the OS and then retry the installation of the system software. If the problem cannot be resolved, acquire all the log files and the management server log files, and then contact maintenance personnel. See online Help for a list of the log files.
		After	Description and Action: The system software installation timed out. (O) Wait a while, perform refresh processing, and then confirm that the system software has been updated. If node information could not be acquired, check the boot status of the OS. If the OS is running, communication with the node may have failed because the certificate was not imported correctly. Import the certificate according to the manual, and then perform the refresh process again. If the OS is not running, start the OS and then

No	Location to be corrected	Corrections	
			retry the installation of the system software. If the problem cannot be resolved, acquire all the log files and the management server log files, and then contact maintenance personnel. See online Help for a list of the log files.
13	Messages sent by using SNMP traps or emails Messages sent from File Sharing (KAQG messages) Table 1-3 List of messages sent from File Sharing	Add	Message ID: KAQG52074-W Severity level: Warning Corresponding MIB object: stdEventTrapWarning Available notification methods: SNMP and E-mail
14	Messages sent by using SNMP traps or emails Messages sent from File Sharing (KAQG messages) Table 1-3 List of messages sent from File Sharing	Add	Message ID: KAQG52075-E Severity level: Error Corresponding MIB object: stdEventTrapError Available notification methods: SNMP and E-mail
15	KAQG52 messages Table 3-1 KAQM52 messages	Add	Message ID: KAQG52074-W Message: Winbindd will now restart to apply the new configuration of the system file (CIFS.conf). Description and Action: Winbindd will now restart because it was detected as running with the old settings of the system file (CIFS.conf). (O) No action is required.
16	KAQG52 messages	Add	Message ID: KAQG52075-E

No	Location to be corrected	Corrections	
	Table 3-1 KAQM52 messages		Message: An attempt to restart winbindd failed. Description and Action: An attempt to restart winbindd failed. (O) Check the CIFS service settings of the node that this message was output, and then restart the CIFS service. If the error still occurs, collect all the log files, and then contact maintenance personnel. For details about all the log files, see online Help.
17	KAQG23 messages Table 5-16 KAQM23 messages	Add	Message ID: KAQM23038-E Message: The operation has not executed because an error occurred during refresh operation. (Processing node name or physical node name or virtual server name = processing-node-name-or-Physical-node-name-or-virtual-server-name) Description and Action: The operation cannot be executed because an error occurred during refresh operation. (O) Restart File Services Manager server, and then try again. If the error continues to occur after restarting File Services Manager server, acquire all the log files and then contact maintenance personnel.
18	KAQG messages Table 3-1 KAQG messages KAQG52020-E	Before	Description and Action: The new user or group ID could not be assigned because the upper limit specified for user and group IDs assigned by user mapping has been reached. (O) Increase the range of the user or group IDs that can be used for user mapping.
		After	Description and Action: The new user or group ID could not be assigned because the upper limit specified for user and group IDs assigned by user mapping has been reached. This error might prevent some users from logging in. (O)

No	Location to be corrected	Corrections	
			Increase the range of the user or group IDs that can be used for user mapping. After that, execute `cifscachectl` with the resolved_negative_cache option specified.
19	KAQG messages Table 3-1 KAQG messages KAQG52021-W	Before	Description and Action: A user or group ID used to access a CIFS share was outside the acceptable range (200-2147483147). (O) Specify a value for the user or group ID registered on the LDAP server or external authentication server that is within the range 200-2147483147.
		After	Description and Action: A user or group ID used to access a CIFS share was outside the acceptable range (200-2147483147). This error might prevent some users from logging in. (O) Specify a value for the user or group ID registered on the LDAP server or external authentication server that is within the range 200-2147483147. After that, execute `cifscachectl` with the resolved_negative_cache option specified.
20	KAQG messages Table 3-1 KAQG messages	Add	Message ID: KAQG52059-I Message: Usage: `cifscachectl --purge {all_negative_cache|resolved_negative_cache|unresolved_negative_cache}` `cifscachectl -h` Description and Action: No action is required.
21	KAQG messages Table 3-1 KAQG messages	Add	Message ID: KAQG52060-Q Message: Are you sure you want to purge the cached user mapping information? (y/n) Description and Action: This confirmation message is output before the cached user mapping information is purged.

No	Location to be corrected	Corrections	
			(O) Enter y or n.
22	KAQG messages Table 3-1 KAQG messages	Add	Message ID: KAQG52061-E Message: The cached user mapping information file might be corrupted. Description and Action: The cached user mapping information file might be corrupted. (O) Restart the CIFS service.
23	KAQG messages Table 3-1 KAQG messages Add	Add	Message ID: KAQG52062-W Message: The cached user mapping information was repaired. Description and Action: The cached user mapping information was repaired. Note that, the first time you access a CIFS share after information is repaired, a query for your user ID and group ID is performed, which might affect access performance. (O) No action is required.
24	KAQG messages Table 3-1 KAQG messages	Add	Message ID: KAQG52063-E Message: Processing of the specified command has already been executed. Description and Action: The specified command has already been executed. (O) No action is required.
25	KAQG messages Table 3-1 KAQG messages	Add	Message ID: KAQG52064-E

No	Location to be corrected	Corrections	
			Message: A system error occurred. Description and Action: A system error occurred during processing to purge the cache. (O) Re-execute the command. If an error occurs again, acquire all the log data, and then contact maintenance personnel.

Table 8. Corrections for "Hitachi Data Ingestor CLI Administrator's Guide"

No	Location to be corrected	Corrections	
1	Table 2-107 Return values of the `cifsoptlist` command	Add	Return value: 65 Description: Acquisition of a lock failed during execution of a command. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
2	Table 2-108 Return values of the `cifsoptset` command	Add	Return value: 65 Description: Acquisition of a lock failed during execution of a command. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
3	Table 2-100 Return values of the `cifsinfogetctl` command	Add	Return value: 65 Description: Acquisition of a lock failed during execution of a command. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
4	2.65	Add	Item

No	Location to be corrected	Corrections	
	cifsoptlist (Display the configuration definition for the CIFS service) Table 2-106 Information displayed when executing the `cifsoptlist` command		idmap_cache_time Description: Displays the validity period of the user mapping information that is cached when mapping is successfully complete at an inquiry to a domain controller or LDAP server for user mapping. (Unit: second)
5	2.65 cifsoptlist (Display the configuration definition for the CIFS service) Table 2-106 Information displayed when executing the `cifsoptlist` command	Add	Item idmap_resolved_negative_cache_time Description Displays the validity period of resolved_negative_cache. (Unit: second) resolved_negative_cache is the user mapping information to be cached when mapping fails at an inquiry to a domain controller or LDAP server for user mapping. The information is cached in the following cases. - The account is deleted from the domain. - When user mapping of the RID or LDAP method is used (at automatic allocation of user ID and group ID), a user ID or group ID to be allocated is outside the specified range. - When user mapping of Active Directory schema method is used, no user ID or no group ID is set to the Active Directory.
6	2.65 cifsoptlist (Display the configuration definition for the CIFS service) Table 2-106 Information displayed when executing the `cifsoptlist` command	Add	Item idmap_unresolved_negative_cache_time Description Displays the validity period of unresolved_negative_cache. (Unit: second) unresolved_negative_cache is the user mapping information to be cached when an inquiry to a domain controller or LDAP server for user mapping fails. The information is cached when the communication with the domain controller or LDAP server for user mapping is disabled due to disconnection of the communication path or a failure on an external server.
7	2.65 cifsoptlist (Display the configuration	Add	Item winbind_cache_time Description

No	Location to be corrected	Corrections	
	definition for the CIFS service) Table 2-106 Information displayed when executing the `cifsoptlist` command		Displays the validity period of the cache regarding the result of an inquiry to a domain controller. (Unit: second)
8	2.66 cifsoptset (Change the configuration definition of the CIFS service) Synopsis	Add	Expansion option: idmap_cache_time {validity period|default} idmap_resolved_negative_cache_time {validity period|default} idmap_unresolved_negative_cache_time {validity period|default} winbind_cache_time {validity period|default}
9	2.66 cifsoptset (Change the configuration definition of the CIFS service) Options and arguments Expansion option	Add	idmap_cache_time {validity period|default} This option is to specify the validity period of the user mapping information to be cached when mapping is successfully complete at an inquiry to a domain controller or LDAP server for user mapping. Specify it together with the `-s` option. If the command is run with the option specified while the CIFS service is running, restart the CIFS service after the command is complete. Validity period Specify the validity period of the cache within the range from 0 to 2,147,483,647. (unit: second) The initial setting is [604,800]. default Specify it to apply the default setting. If this argument is specified, 604,800 is set.
10	2.66 cifsoptset (Change the configuration definition of the CIFS service) Options and arguments Expansion option	Add	idmap_resolved_negative_cache_time {validity period|default} This option is to specify the validity period of resolved_negative_cache. resolved_negative_cache is the user mapping information to be cached when mapping fails at an inquiry to a domain controller or LDAP server for user mapping. The information is cached in the following cases. - The account is deleted from the domain. - When user mapping of the RID or LDAP method is used (at automatic allocation of user ID and group ID), a user ID or group ID to be allocated is outside the specified range. - When user mapping of Active Directory schema method is used, no user ID or no group ID is set to the Active Directory.

No	Location to be corrected	Corrections	
			Specify it together with the -s option. If the command is run with the option specified while the CIFS service is running, restart the CIFS service after the command is complete. Validity period Specify the validity period of the cache within the range from 0 to 2,147,483,647. (Unit: second) The initial setting is [120]. default Specify it to apply the default setting. If this argument is specified, 120 is set.
11	2.66 cifsoptset (Change the configuration definition of the CIFS service) Options and arguments Expansion option	Add	idmap_unresolved_negative_cache_time {validity period|default} This option is to specify the validity period of unresolved_negative_cache. unresolved_negative_cache is the user mapping information to be cached when an inquiry to a domain controller or LDAP server for user mapping fails. The information is cached when the communication with the domain controller or LDAP server for user mapping is disabled due to disconnection of the communication path or a failure on an external server. Specify it together with the -s option. If the command is run with the option specified while the CIFS service is running, restart the CIFS service after the command is complete. Validity period Specify the validity period of the cache within the range from 0 to 2,147,483,647. (Unit: second) The initial setting is [120]. default Specify it to apply the default setting. If this argument is specified, 120 is set.
12	2.66 cifsoptset (Change the configuration definition of the CIFS service) Options and arguments Expansion option	Add	winbind_cache_time {validity period|default} This option is to specify the validity period of the cache regarding the result of an inquiry to a domain controller. (Unit: second) Specify it together with the -s option. If the command is run with the option specified while the CIFS service is running, restart the CIFS service after the command is complete. Validity period Specify the validity period of the cache within the range from 0 to 2,147,483,647. (Unit: second) The initial setting is [300]. default

No	Location to be corrected	Corrections	
			Specify it to apply the default setting. If this argument is specified, 300 is specified.
13	2 Command Reference	Add	`cifscachectl` (CIFS service cache management) Synopsis `cifscachectl --purge` {all_negative_cache|resolved_negative_cache|unresolved_negative _cache} [-y] `cifscachectl -h` Description This command is to manage CIFS service cache. The command is applied to a node on which the command is run. In a cluster configuration, run the command on both nodes. Options and arguments `--purge` {all_negative_cache|resolved_negative_cache|unresolved_negative _cache} Specify it to discard CIFS service cache, such as resolved_negative_cache and unresolved_negative_cache. resolved_negative_cache is the user mapping information to be cached when mapping fails at an inquiry to a domain controller or LDAP server for user mapping. The information is cached in the following cases. - The account is deleted from the domain. - When user mapping of the RID or LDAP method is used (at automatic allocation of user ID and group ID), a user ID or group ID to be allocated is outside the specified range. - When user mapping of Active Directory schema method is used, no user ID or no group ID is set to the Active Directory. unresolved_negative_cache is the user mapping information to be cached when an inquiry to a domain controller or LDAP server for user mapping fails. The information is cached when the communication with the domain controller or LDAP server for user mapping is disabled due to disconnection of the communication path or a failure an external server. If the command is run with the option specified, a confirmation message and a message indicating the discarding processing progress are displayed. all_negative_cache

<table>
<tr><th>No</th><th>Location to be corrected</th><th colspan="2">Corrections</th></tr>
<tr><td></td><td></td><td></td><td>
Specify it to discard resolved_negative_cache, unresolved_negative_cache, and cache of the result of an inquiry regarding users and groups to a domain controller.

resolved_negative_cache

Specify it to discard resolved_negative_cache and cache of the result of an inquiry regarding users and groups to a domain controller.

unresolved_negative_cache

Specify it to discard unresolved_negative_cache and cache of the result of an inquiry regarding users and groups to a domain controller.

Notes:

When a user accesses a CIFS share for the first time after CIFS service cache discarding, an inquiry to a domain controller or LDAP server for user mapping takes place and it might affect the access performance. Therefore, discard the CIFS service cache when necessary.

Return values

<table>
<tr><td>Return value</td><td>Description</td></tr>
<tr><td>0</td><td>Normal termination</td></tr>
<tr><td>1, 2, 3</td><td>The command is specified in an incorrect format. Verify the format and then retry the command.</td></tr>
<tr><td>4</td><td>The CIFS service cache might be corrupted. Restart the CIFS service.</td></tr>
<tr><td>5</td><td>The same command has already been run.</td></tr>
<tr><td>99</td><td>The error cannot be handled by the system administrator. Contact maintenance personnel.</td></tr>
</table>
Examples

To discard unresolved_negative_cache and cache of the result of an inquiry regarding users and groups to a domain controller:

<pre>$ sudo cifscachectl --purge
unresolved_negative_cache</pre>
KAQG52060-Q Are you sure you want to purge the cached user mapping information? (y/n) y

Purging cache...(0%)

Purging cache...(100%)
</td></tr>
</table>

Table 9. Corrections for "Hitachi Data Ingestor Cluster Administrator's Guide"

No	Location to be corrected	Corrections	
1	Table C-295 Task Status	Add	Policy Inconsistency The policy of the migration task is inconsistent. The migration task cannot be executed. Delete the migration task and add a migration task again.

Table 10. Corrections for "Hitachi Data Ingestor Single Node Administrator's Guide"

No	Location to be corrected	Corrections	
1	Table C-1 Task Status	Add	Policy Inconsistency The policy of the migration task is inconsistent. The migration task cannot be executed. Delete the migration task and add a migration task again.
2	Logging on to the system	Before	A system administrator can operate and manage a Hitachi Data Ingestor (HDI) system from a Web browser by logging on to the system.
		After	A system administrator can operate and manage a Hitachi Data Ingestor (HDI) system from a HDI Single Node GUI by logging on to the system.
3	Logging on to the system To log on to the system	Before	1. If you are using UPnP, click the HDI icon in Other Devices, which appears in the network list in the management console. If you are not using UPnP, enter the URL in your web browser's address bar, in the following format: https://HDI-IP-address-or-host-name/admin/ The Login window appears. 2. Specify a user ID and the password in the Login window, and then click Login. The main window is displayed.
		After	1. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser. https://HDI-IP-address-or-host-name/admin/download.html 2. Start the installation program to install a HDI single node GUI. For details on the prerequisites for installing the single-node GUI, see "Prerequisites for installing the Hitachi Data Ingestor (HDI) single-node GUI" in the Hitachi Data Ingestor Single Node Getting Started Guide.

No	Location to be corrected	Corrections	
			3. Start the installed HDI single node GUI. The login window is displayed. 4. Enter IP address or host name of HDI to be managed, user ID, and password, and then click the Login. The main window is displayed.
4	Adding internal hard disks to a node	Before	6. From a browser, log on to the system.
		After	6. From a HDI Single Node GUI, log on to the system.
5	Adding LUs to a running storage system	Before	3. From a browser, log on to the system.
		After	3. From a HDI Single Node GUI, log on to the system.
6	Updating software	Delete	•If you update the software in an environment where the OS or web browser of the management console is not configured to support SHA-2, you will no longer be able to communicate with the node. Ensure that the OS or web browser is configured to support SHA-2 before you update the software.
7	Updating software (using the installation file registered in an HCP system)	Add	10. After updating the node software, you may need to update the HDI single node GUI. If update is necessary, the following message will be displayed when you log on using the HDI single node GUI. As the version of the node to connect to is new, the node cannot be connected. Download the program of single node GUI from the following URL and perform the update installation. URL=xxx If this message is displayed, update the HDI single node GUI. For updating the HDI single node GUI, refer to "Updating Hitachi Data Ingestor single node GUI".
8	Updating software (using an installation media)	Before	14. Confirm that the login window is displayed on the monitor that is connected to the node. If the node is restarted and the login window is displayed on the monitor, the installation is complete.
		After	14. After updating the node software, you may need to update the HDI single node GUI. If update is necessary, the following message will be displayed when you log on using the HDI single node GUI. As the version of the node to connect to is new, the node cannot be connected.

No	Location to be corrected	Corrections	
			Download the program of single node GUI from the following URL and perform the update installation. URL=xxx If this message is displayed, update the HDI single node GUI. For updating the HDI single node GUI, refer to "Updating Hitachi Data Ingestor single node GUI".
9	Window configuration Table B-1 Items displayed in the global taskbar area File	Before	Logout
		After	Exit
10	Notes on using the GUI	Before	•If a window is closed while a page is loading, an error sometimes occurs the next time a window is opened, and no operations can be performed. If this happens, close all open Web browsers, and then start over from the beginning.
		After	•If a window is closed while a page is loading, an error sometimes occurs the next time a window is opened, and no operations can be performed. If this happens, close all open window, and then start over from the beginning.
11	Updating Hitachi Data Ingestor (HDI) Single Node GUI	Add	The following describes how to perform the update installation for the software running on the management console. 1. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser. https://HDI-IP-address-or-host-name/admin/download.html 2. Start the installation program to install a HDI single node GUI. For details on the prerequisites for installing the single-node GUI, see "Prerequisites for installing the Hitachi Virtual File Platform / Hitachi Data Ingestor (HVFP/HDI) single-node GUI" in the Hitachi Data Ingestor Single Node Getting Started Guide.
12	Logging on to the system To log on to the system	Before	1. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser. https://HDI-IP-address-or-host-name/admin/download.html
		After	1. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser.

No	Location to be corrected	Corrections	
			https://HDI-IP-address-or-host-name/admin/download.html Alternatively, you can install from the installation media. Use the installer located in the "SingleNodeGUI" folder on the installation media.
13	Updating software (using the installation file registered in an HCP system)	Before	10. After updating the node software, you may need to update the HDI single node GUI. If update is necessary, the following message will be displayed when you log on using the HDI single node GUI. As the version of the node to connect to is new, the node cannot be connected. Download the program of single node GUI from the following URL and perform the update installation. URL=xxx If this message is displayed, update the HDI single node GUI. For updating the HDI single node GUI, refer to "Updating Hitachi Data Ingestor single node GUI".
		After	10. After updating the node software, you may need to update the HDI single node GUI. If update is necessary, the following message will be displayed when you log on using the HDI single node GUI. As the version of the node to connect to is new, the node cannot be connected. Install the latest program of the single node GUI. If this message is displayed, update the HDI single node GUI. For updating the HDI single node GUI, refer to "Updating Hitachi Data Ingestor single node GUI".
14	Updating software (using an installation media)	Before	14. After updating the node software, you may need to update the HDI single node GUI. If update is necessary, the following message will be displayed when you log on using the HDI single node GUI. As the version of the node to connect to is new, the node cannot be connected. Download the program of single node GUI from the following URL and perform the update installation. URL=xxx If this message is displayed, update the HDI single node GUI. For updating the HDI single node GUI, refer to "Updating Hitachi Data Ingestor single node GUI".

No	Location to be corrected	Corrections	
		After	14. After updating the node software, you may need to update the HDI single node GUI. If update is necessary, the following message will be displayed when you log on using the HDI single node GUI. As the version of the node to connect to is new, the node cannot be connected. Install the latest program of the single node GUI. If this message is displayed, update the HDI single node GUI. For updating the HDI single node GUI, refer to "Updating Hitachi Data Ingestor single node GUI".
15	Updating Hitachi Data Ingestor (HDI) Single Node GUI	Before	1. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser. https://HDI-IP-address-or-host-name/admin/download.html
		After	1. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser. https://HDI-IP-address-or-host-name/admin/download.html Alternatively, you can install from the installation media. Use the installer located in the "SingleNodeGUI" folder on the installation media.

Table 11. Corrections for "Hitachi Data Ingestor File System Protocols (CIFS/NFS) Administrator's Guide"

No	Location to be corrected	Corrections	
1	Notes on accessing file shares	Before	•Because the character code used by an NFS share depends on the NFS client environment, a file or directory name might not be displayed correctly if the NFS client has used other character codes, such as EUC or JIS, to create a file or directory.
		After	•Character codes used by NFS share depend on the environment of NFS client. If a file or directory created by an NFS client that uses character codes, such as EUC and JIS, or control codes (*1) is used on the CIFS share side, the file or the directory is displayed in a name different from that stored in the file system, Also CIFS clients cannot access the file or the directory, or cannot access an intended file or directory, Therefore, to share files and directories with CIFS clients, use character codes of UTF-8 for file and directory names created by NFS clients. *1: Control code: 0x01~0x1f, 0x22, 0x2a, 0x2f, 0x3a, 0x3c, 0x3e, 0x3f, 0x5c, 0x7c

<table>
<tr><th>No</th><th>Location to be corrected</th><th colspan="2">Corrections</th></tr>
<tr><td></td><td></td><td></td><td>
The tables below show differences between versions.
Table: Names displayed on explorer for CIFS client
<table>
<tr><td>Character code other than UTF-8</td><td>Control code</td><td>Earlier than 5.7.0-00</td><td>5.7.0-00 and later</td></tr>
<tr><td>Not contained</td><td>Contained</td><td>Different name (*2)</td><td>Different name (*2)</td></tr>
<tr><td rowspan="2">Contained</td><td>Contained</td><td>Different name (*2)</td><td>Different name (*2)</td></tr>
<tr><td>Not contained</td><td>Different name (*2)</td><td>None</td></tr>
</table>
*2: Displayed in names different from those on file system
Table: File open/accessibility from CIFS client
<table>
<tr><td>Character code other than UTF-8</td><td>Control code</td><td>Earlier than 5.7.0-00</td><td>5.7.0-00 and later</td></tr>
<tr><td>Not contained</td><td>Contained</td><td>Enable</td><td>Enable</td></tr>
<tr><td rowspan="2">Contained</td><td>Contained</td><td>Enable</td><td>Disable</td></tr>
<tr><td>Not contained</td><td>Enable</td><td>Disable</td></tr>
</table>
</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">5.4 Authentication when user mapping is being used</td><td>Before</td><td>Whenever a connection to the LDAP server used for user mapping fails, the LDAP serer cannot be accessed again for at least five minutes. Users (such as anew domain user or a domain user who has deleted cache files) who usually access the LDAP server by using the CIFS service will not be able to access the LDAP server. Correct the problem that is preventing connections to the LDAP server, either wait five minutes or restart the CIFS service, and then attempt to access the CIFS service again, If the LDAP server is restarted after the problem is corrected, restart the LDAP server, and then restart the CIFS service.</td></tr>
<tr><td>After</td><td>If accesses to the LDAP server are disabled when the user mapping with LDAP method is used, an access to the CIFS service might fail. In this case, remove the problem that is preventing connections to the LDAP server, either wait for two minutes (*) or discard unresolved_negative_cache by running a <code>cifscachectl</code> command, and</td></tr>
</table>

No	Location to be corrected	Corrections	
			then access the CIFS service again. For the procedure to discard unresolved_negative_cache, see Table8 No.13. *: It is after the specified validity period of unresolved_negative_cache is passed if it has been changed by a `cifsoptset` command. The validity period of unresolved_negative_cache can be confirmed by a `cifsoptlist` command.
3	5.4 Authentication when user mapping is being used	Before	When an error occurs on a network with a domain controller, and when you receive CIFS-service-related error information using SNMP or email notification from a node, the node cannot acquire user and group information from the domain controller for five minutes after failure detection. Accordingly, the node fails to authenticate users during this five-minute period. If this problem occurs, correct the error that is preventing a connection to the domain controller, and then either wait five minutes or restart the CIFS service. After that, access the CIFS service.
		After	When an error occurs on a network with a domain controller, and when you receive CIFS-service-related error information using SNMP or email notification from a node, the node cannot acquire user and group information from the domain controller for five minutes after failure detection. Accordingly, the node fails to authenticate users during this five-minute period. If this problem occurs, remove the error that is preventing a connection to the domain controller, verify that the connection with the domain controller is recovered by using SNMP or email notification, either wait for five minutes (*) or discard unresolved_negative_cache by running a `cifscachectl` command, and then access the CIFS service. For the procedure to discard unresolved_negative_cache, see Table 8 No.13. *: If the validity period of unresolved_negative_cache and that of cache regarding the result of an inquiry to a domain controller have been changed by a `cifsoptset` command, it is after the longer validity period is passed. The validity periods can be confirmed by a `cifsoptlist` command.

Table 12. Corrections for "Hitachi Data Ingestor Single Node Troubleshooting Guide"

No	Location to be corrected	Corrections	
1	Collecting node log files	Before	3. In the Web browser download dialog box, specify where to download the files.
		After	3. In the download dialog box, specify where to download the files.

No	Location to be corrected	Corrections	
2	Collecting node log files	Before	1. Display the Check for Errors dialog box by using either of the following methods: • Click the Action menu in the top-left corner of the GUI, choose Launch, and then Check for Errors. • In the Settings area of the host-name window, select Check for Errors. 2. In the Info. type drop-down list, select Batch-download, and then click the Display button. 3. Select the radio button for the log group you want to download in batch, and then click the Download button. Note: If you select a PSB log group, a dialog box asking you whether to perform a batch download is displayed before the download dialog box appears. 4. In the Web browser download dialog box, specify where to download the files. The log files that belong to the selected log group are archived in tar format, compressed in gzip format, and then downloaded to the specified destination. 5. Click the Close button in the download dialog box.
		After	a. Display the Check for Errors dialog box by using either of the following methods: • Click the Action menu in the top-left corner of the GUI, choose Launch, and then Check for Errors. • In the Settings area of the host-name window, select Check for Errors. b. In the Info. type drop-down list, select Batch-download, and then click the Display button. c. Select the radio button for the log group you want to download in batch, and then click the Download button. Note: If you select a PSB log group, a dialog box asking you whether to perform a batch download is displayed before the download dialog box appears. d. In the Web browser download dialog box, specify where to download the files. The log files that belong to the selected log group are archived in tar format, compressed in gzip format, and then downloaded to the specified destination. e. Click the Close button in the download dialog box.

<table>
<tr><th>No</th><th>Location to be corrected</th><th colspan="2">Corrections</th></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Batch restoration of system configuration information and user data</td><td>Before</td><td>1. Make sure the restored files do not have any inconsistencies by executing the <code>hcporphanrestore</code> command without the <code>--display</code> option.
2. If inconsistencies exist in any recovered files, copy the recovered files to an appropriate location.</td></tr>
<tr><td>After</td><td>a. Make sure the restored files do not have any inconsistencies by executing the <code>hcporphanrestore</code> command without the <code>--display</code> option.
b. If inconsistencies exist in any recovered files, copy the recovered files to an appropriate location.</td></tr>
<tr><td rowspan="2">4</td><td rowspan="2">GUI-related troubleshooting examples
Table C-1 GUI-related troubleshooting examples
Non-specific
You cannot use the GUI when you configure network information about nodes using DHCP.</td><td>Before</td><td>• Specify the host name in your Web browser's address bar.</td></tr>
<tr><td>After</td><td>•Specify the host name as the IP address on the login window of HDI Single Node GUI.</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">GUI-related troubleshooting examples
Table C-1 GUI-related troubleshooting examples
Non-specific
You attempted to use UPnP, but the GUI did not start even though you clicked the HDI icon, or right-clicked the icon and then selected</td><td>Before</td><td><table><tr><th>Cause</th><th>Action</th></tr><tr><td>If the management console runs on Windows 8 or Windows Server 2012, a problem might occur if the https communication stops between the HDI node and the management console.</td><td>Click the address displayed in Device webpage in the properties dialog box for the HDI icon.</td></tr></table></td></tr>
<tr><td>After</td><td><table><tr><th>Cause</th><th>Action</th></tr><tr><td>Flash Player is not installed.</td><td>Use HDI Single Node GUI after downloading the program from the node and performing the installation of HDI Single Node GUI. For IP</td></tr></table></td></tr>
</table>

<table>
<tr><th>No</th><th>Location to be corrected</th><th colspan="3">Corrections</th></tr>
<tr><td></td><td>View device web page.</td><td></td><td colspan="2"><table><tr><td></td><td>address on the login window of Single Node GUI, input the IP address displayed in the URL of "Device Webpage"that is in the property window of the icon indicating HDI. For details of downloading Single Node GUI, see "Configuring an environment" in the Hitachi Data Ingestor Single Node Getting Started Guide.</td></tr></table></td></tr>
<tr><td>6</td><td>GUI-related troubleshooting examples
Table C-1 GUI-related troubleshooting examples
Non-specific</td><td>Add</td><td colspan="2"><table><tr><td>Type of problem</td><td>Cause</td><td>Action</td></tr><tr><td>HDI Single Node GUI does not start.</td><td>This may be caused by the files that make up the application being damaged for some reason.</td><td>Download the HDI Single Node GUI again and re-install.</td></tr></table></td></tr>
<tr><td rowspan="2">10</td><td rowspan="2">GUI-related troubleshooting examples
Table C-1 GUI-related troubleshooting examples
Non-specific
You attempted to use UPnP, but the GUI did not start even though you clicked the HDI icon, or right-clicked the icon and then selected View device web page.
Action</td><td>Before</td><td colspan="2">Use HDI Single Node GUI after downloading the program from the node and performing the installation of HDI Single Node GUI. For IP address on the login window of Single Node GUI, input the IP address displayed in the URL of "Device Webpage" that is in the property window of the icon indicating HDI. For details of downloading Single Node GUI, see "Configuring an environment" in the Hitachi Data Ingestor Single Node Getting Started Guide.</td></tr>
<tr><td>After</td><td colspan="2">Install and use the HDI Single Node GUI with either way of the following.
(1) Download the program from the node and perform the installation.
(2) Perform the installation from the installation media if you have them.
For IP address on the login window of Single Node GUI, input the IP address displayed in the URL of "Device Webpage" that is in the property window of the icon indicating HDI. For details of downloading Single Node GUI, see "Configuring an environment" in the Hitachi Data Ingestor Single Node Getting Started Guide.</td></tr>
<tr><td>11</td><td></td><td>Before</td><td colspan="2">Download the HDI Single Node GUI again and re-install.</td></tr>
</table>

No	Location to be corrected	Corrections	
	GUI-related troubleshooting examples Table C-1 GUI-related troubleshooting examples Non-specific HDI Single Node GUI does not start. Action	After	Re-install and use the HDI Single Node GUI with either way of the following. (1) Download the program from the node and perform the installation. (2) Perform the installation from the installation media if you have them.
12	2.6 Checking user mapping information	Before	• The latest user information has been applied If an end user accesses a CIFS share immediately after the user or the group information managed by a domain controller is changed, old user mapping information that has been cached might be applied. If you modify the user or group information managed by a domain controller (such as by re-creating a user or changing a user group), the system administrator restart the CIFS service or inform the end users to reconnect to the CIFS share after five minutes, in order for the information to be refreshed. If an end user is already connected to the CIFS share, they must disconnect and then reconnect the CIFS share.
		After	• The latest user information has been applied If an end user accesses a CIFS share immediately after the user or the group information managed by a domain controller is changed, old user mapping information that has been cached might be applied. If the user or group information managed by a domain controller is modified (such as by re-creating a user or changing a user group), the system administrator discards resolved_negative_cache by a `cifscachectl` command or informs the end user to reconnect to the CIFS share (if already connected, disconnect and then connect) after five minutes (*), and then access the CIFS share to update the information. For the procedure to discard resolved_negative_cache, see Table 8 No.13. *: If is after the validity period of resolved_negative_cache or that of cache regarding the result of an inquiry to a domain controller, whichever is longer, is passed. The validity periods can be confirmed by a `cifsoptlist` command.

No	Location to be corrected	Corrections	
13	2.6 Checking user mapping information	Before	If no particular problems are found, the system administrator must perform either of the following tasks: •Delete the cached user mapping information in the CIFS Service Maintenance page of the Access Protocol Configuration dialog box. •Inform end users that the CIFS share must not be accessed for five minutes
		After	If no particular problems are found, the system administrator must perform either of the following tasks: • Delete the cached user mapping information in the CIFS Service Maintenance page of the Access Protocol Configuration dialog box. • Discard resolved_negative_cache and unresolved_negative_cache by a `cifscachectl` command. For the procedure to discard resolved_negative_cache and unresolved_negative_cache, see Table 8 No.13. • Inform end users to wait for around five minutes (*) and then access the CIFS share again. *: It is after the longest validity period among resolved_negative_cache, unresolved_negative_cache, and cache regarding the result of an inquiry to a domain controller is passed. The validity periods can be confirmed by a `cifsoptlist` command.

Table 13. Corrections for "Hitachi Data Ingestor Single Node Getting Started Guide"

No	Location to be corrected	Corrections	
1	Configuring an environment	Before	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!

<table>
<tr><th>No</th><th>Location to be corrected</th><th colspan="2">Corrections</th></tr>
<tr><td></td><td></td><td>After</td><td>2. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser.
https://HDI-IP-address-or-host-name/admin/download.html
3. Start the installation program to install a HDI single node GUI.
For details on the prerequisites for installing the single-node GUI, see "Prerequisites for installing the Hitachi Data Ingestor (HDI) single-node GUI" in the Hitachi Data Ingestor Single Node Getting Started Guide.
4. Start the installed HDI single node GUI. The login window is displayed.
5. Enter IP address or host name of HDI to be managed, user ID, and password, and then click the Login.
The main window is displayed.</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Configuring an environment</td><td>Before</td><td>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.</td></tr>
<tr><td>After</td><td>9. On the 6. Completion page, check the processing results, and terminate the HDI Single Node GUI and then restart it.
10. Enter IP address or host name, user ID, and password, and then click the Login.</td></tr>
<tr><td>3</td><td>Prerequisites for installing Hitachi Data Ingestor (HDI) Single Node GUI</td><td>Add</td><td>Check the following before installing HDI Single Node GUI.
The environment of the computer on which you will install HDI Single Node GUI:
• Make sure that the computer meets the requirements for HDI Single Node GUI.
For details on the requirements, see Requirements for a management console on page 3-9.
• If you are performing a new installation of HDI Single Node GUI, make sure that the target disk drive has sufficient free space for installing the software.
The following table lists the components to be installed and the amount of free space required to install each component.
Table 2-1 Components to be installed and free space required for installation
<table><tr><td>Component</td><td>Required free space</td></tr></table></td></tr>
</table>

No	Location to be corrected	Corrections	
			<table><tr><td>HDI Single Node GUI</td><td>At least 40MB</td></tr></table> Tasks that you need to carry out before installing HDI Single Node GUI: • Log on to Windows as an Administrator or a member of the Administrators group. • If a security monitoring program has been installed, either stop it or change its settings so that it does not hamper installation of HDI Single Node GUI. • If an antivirus program has been installed, stop the program, and then install HDI Single Node GUI. You might not be able to install HDI Single Node GUI while an antivirus program is running. If an installation attempt fails, take action according to the message displayed in the error dialog box.
4	Uninstalling Hitachi Data Ingestor (HDI) Single Node GUI	Add	This section describes how to uninstall HDI Single Node GUI. 1. Select "[Hitachi Virtual File Platform Single Node GUI] / [Hitachi Data Ingestor Single Node GUI]" from [Programs and Features] of Windows, and click "Uninstall" to perform uninstallation.
5	Configuring an environment	Before	2. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser. https://HDI-IP-address-or-host-name/admin/download.html
		After	2. Download the installation program of HDI Single Node GUI. It can be downloaded from the following URL using a WWW browser. https://HDI-IP-address-or-host-name/admin/download.html Alternatively, you can install from the installation media. Use the installer located in the "SingleNodeGUI" folder on the installation media.

Table 14. Corrections for " Cluster Troubleshooting Guide "

No	Location to be corrected	Corrections	
1	2.7 Checking user mapping information	Before	•The latest user information has been applied If an end user accesses a CIFS share immediately after the user or the group information managed by a domain controller is changed, old usermapping information that has been cached might be applied. If you modify the user or group information managed by a domain controller (such as by re-creating a user or changing a user group), the

No	Location to be corrected	Corrections	
			system administrator restart the CIFS service or inform the end users to reconnect to the CIFS share after five minutes, in order for the information to be refreshed. If an end user is already connected to the CIFS share, they must disconnect and then reconnect the CIFS share.
		After	• The latest user information has been applied If an end user accesses a CIFS share immediately after the user or the group information managed by a domain controller is changed, old user mapping information that has been cached might be applied. If the user or group information managed by a domain controller is modified (such as by re-creating a user or changing a user group), the system administrator discards resolved_negative_cache by a `cifscachectl` command or informs the end user to reconnect to the CIFS share (if already connected, disconnect and then connect) after five minutes (*), and then access the CIFS share to update the information. For the procedure to discard resolved_negative_cache, see Table 8. No.13. *: It is the validity period of resolved_negative_cache or that of cache regarding the result of a inquiry to a domain controller, whichever is longer. The validity periods can be confirmed by a `cifsoptlist` command.
2	2.7 Checking user mapping information	Before	If no particular problems are found, the system administrator must perform either of the following tasks: •Delete the cached user mapping information in the CIFS Service Maintenance page of the Access Protocol Configuration dialog box. •Inform end users that the CIFS share must not be accessed for five minutes
		After	If no particular problems are found, the system administrator must perform either of the following tasks: •Delete the cached user mapping information in the CIFS Service Maintenance page of the Access Protocol Configuration dialog box. •Discard resolved_negative_cache and unresolved_negative_cache by a `cifscachectl` command. For the procedure to discard resolved_negative_cache and unresolved_negative_cache, see table 8 No.13. • Inform end users to wait for around five minutes (*), and then access the CIFS share again. *: It is the longest validity period among resolved_negative_cache, unresolved_negative_cache, and cache regarding the result of an inquiry

No	Location to be corrected	Corrections	
			to a domain controller. The validity period can be confirmed by a `cifsoptlist` command.

Fixed problems

1) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00.

Affected version: 02-01-00-00

Phenomenon: There are vulnerabilities reported with the following CVEs, and those are solved by updating base versions of HDI internal components; OpenSSH, OpenSSL, and cURL. Some of them do not affect, because HDI functions do not use them.

CVE-2010-4755, CVE-2011-4327, CVE-2011-5000, CVE-2012-0814, CVE-2014-2532, CVE-2014-2653, CVE-2015-5352, CVE-2015-5600, CVE-2015-6563, CVE-2015-6564, CVE-2015-8325, CVE-2016-1907, CVE-2016-1908, CVE-2016-3115, CVE-2016-6210, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708, CVE-2017-15906, CVE-2018-15473, CVE-2018-15919, CVE-2018-20685, CVE-2019-6109, CVE-2019-6111

CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2015-3197, CVE-2016-0702, CVE-2016-0703, CVE-2016-0704, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2842, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306, CVE-2016-7056, CVE-2016-8610

CVE-2010-0734, CVE-2011-2192, CVE-2013-1944, CVE-2013-2174, CVE-2013-4545, CVE-2014-0015, CVE-2014-0138, CVE-2014-0139, CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, CVE-2015-3148, CVE-2015-3153, CVE-2016-0754, CVE-2016-0755, CVE-2016-4802, CVE-2016-5419, CVE-2016-5420, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8621, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625, CVE-2016-9586, CVE-2017-7407, CVE-2017-1000100, CVE-2018-14618, CVE-2018-16842, CVE-2018-1000007, CVE-2018-1000120

Condition: See the information of Common Vulnerability Exposures (CVEs).

Evasion plan: None.

Recovery plan: None.

2) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 02-01-00-00

Phenomenon: A nasroot account is wrongly able to log in to the window for end users.

Condition: It occurs when nasroot is specified for user ID and then the login button is clicked on the window for end users.

Evasion plan: None.

Recovery plan: None.

3) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 02-01-00-00

Phenomenon: If a GUI parameter is falsified by a malevolent user, an arbitrary command can run with root permission. (CVE-2021-20740)

Condition: It may occur when conditions below are all combined.

(a) A user who can log in to GUI for a system administrator or end users

(b) The user of (a) logs on to GUI.

(c) A GUI parameter is falsified and then sent.

Evasion plan: None.

Recovery plan: None.

4) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 6.2.0-00

Phenomenon: The system setting file is not periodically saved in the specified directory.

Condition: It occurs when conditions below are all combined.

(a) The HDI system is not linked with an HCP system.

(b) A directory on a file system is specified as a location to periodically save the system setting file.

(c) The path of the directory in (b) contains a specific character (such as a space) that the shell deciphers.

(d) The periodic saving of the system setting file runs.

Evasion plan: Do not use specific characters (such as a space) deciphered by shell for a path to a directory to periodically save the system setting file.

Recovery plan: None.

5) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 02-01-00-00

Phenomenon: Vulnerabilities reported by the following CVEs may adversely affect operations.

CVE-2020-2754/CVE-2020-2755/CVE-2020-2756/

CVE-2020-2757/CVE-2020-2767/CVE-2020-2773/

CVE-2020-2778/CVE-2020-2781/CVE-2020-2800/

CVE-2020-2803/CVE-2020-2805/CVE-2020-2816/

CVE-2020-2830/CVE-2013-3827/CVE-2019-2973/
CVE-2019-2981/CVE-2012-0881/CVE-2013-4002

Condition: It may occur when a request from a malicious user is received.

Evasion plan: None.

Recovery plan: None.

6) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 6.1.0-00

Phenomenon: A migration task does not run periodically.

Condition: It may occur when conditions below are all combined.

(a) 6.1.0-00 or later is used.

(b) A migration task is set.

(c) HDI is restarted.

Evasion plan: None.

Recovery plan: Set the migration task schedule again.

Note: The schedule can be set by selecting the target schedule task, opening Edit Task from GUI. And then apply it as is.

7) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 6.1.0-00

Phenomenon: The setting information changed on HCP Anywhere cannot be applied.

Condition: It may occur when conditions below are all combined.

(a) HCP Anywhere is connected.

(b) The migration setting information is edited on HCP Anywhere.

(c) HDI is restarted.

Evasion plan: Edit the migration setting information on the HDI side.

Recovery plan: None.

The problem can be solved automatically within an hour after the restart.

8) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 6.1.0-00

Phenomenon: KAQM0341-E occurs on the Migration Tasks dialog box.

Condition: It occurs when conditions below are all combined.

(a) For the URL at single node GUI access, an IPv6 address is specified.

(b) The Migration Tasks dialog box is displayed.

Evasion plan: To use an IPv6 address on GUI, specify a host name instead of the IP address.

Recovery plan: None.

9) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-00

Affected version: 02-01-00-00

Phenomenon: Text of the Copyright of the single node GUI is wrong.

Condition: None.

Evasion plan: None.

Recovery plan: None.

10) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-01

Affected version: 5.0.0-00

Phenomenon: A renamed directory and file may not be migrated.

Condition: It may occur in rare cases if the following operations are performed during migration.

* A migration target directory or file is shown as A, a directory or file that is not a migration target is shown as B below.

(a) A is renamed to C. (C is migrated at the next time)

(b) B is renamed to A.

(c) A is renamed to D. (D may not be migrated)

If the problem occurs, D cannot be migrated even though it is updated.

* Rename includes moving directory and file.

Evasion plan: None.

Recovery plan: Run arccorrection and create the file system management information again.

11) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-01

Affected version: 02-01-00-00

Phenomenon: A file that is renamed during migration cannot be a migration target.

Condition: It may occur when all the following conditions are met.

(a) A file for which migration has already been performed is updated.

(b) During migration, the file of (a) is renamed or moved.

If the problem occurs, the file is updated, but not migrated.

Evasion plan: None.

Recovery plan: Run arccorrection and create the migration target list again.

12) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-01

Affected version: 5.1.1-00

Phenomenon: The following problems occur.

(a) the tasks on the dashboard tab are not displayed. (e.g. migration task is not displayed)

(b) KAQM26052-E occurs on the Service Configuration Wizard.

(c) KAQM26046-E will be logged.

Condition: It may occur when all the following conditions are met.

(a) single node configuration is used.

(b) GUI service is starting.

(c) FOS is restarted or stopped due to any reasons.

Evasion plan: None.

Recovery plan: Please follow the steps below.

1. Perform an update installation.
2. Restore system LUs.
3. Restart the node.

13) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-01

Affected version: 5.1.1-00

Phenomenon: The GUI functions are unavailable.

Condition: It may occur when all the following conditions are met.

(a) System LUs are restoring.

(b) FOS is restarted or stopped due to any reasons.

Evasion plan: None.

Recovery plan: Please follow the steps below.

1. Restore system LUs.
2. Restart the node.

14) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-01

Affected version: 5.1.1-00

Phenomenon: The API functions are unavailable.

Condition: It may occur when all the following conditions are met.

(a) Installation or update installation is executing.

(b) FOS is restarted or stopped due to any reasons.

Evasion plan: None.

Recovery plan: Please follow the steps below.

1. Perform an update installation.
2. Restore system LUs.
3. Restart the node.

15) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 02-01-00-00

Phenomenon: The folder list collection processing (FIND processing) of the CIFS service remains so that the CIFS service stop processing is delayed or system load increases.

Condition: It may occur when one of the following conditions is met.

(a) Access Based Enumeration is enabled.

(b) There are large number of CIFS connections.

(c) There are many files in a folder, or many folders on a CIFS share.

Evasion plan: None.

Recovery plan: None.

16) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 02-01-00-00

Phenomenon: When a failback takes place while the CIFS service configuration definition differs in each node in a cluster, the CIFS service configuration definition becomes invalid.

Condition: It may occur when all the following conditions are met.

(a) User mapping is used on the CIFS service.

(b) The user mapping setting of the CIFS service differs in each node of a cluster.

(c) A resource group that has been failed over is failed back to the previous node.

Evasion plan: Make the CIFS service configuration definition consistent among nodes in a cluster.

Recovery plan: If a resource group is failed over from a node to the node with failure, fail back the resource group to the previous node, and then restart the CIFS service.

17) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 6.2.0-00

Phenomenon: Migration cannot be performed.

Condition: It occurs when all the following conditions are met.

(a) A file system supporting WORM

(b) Auto commit is enabled.

(c) The file system is an Advanced ACL type file system.

(d) A CIFS administrator sets an inheritable ACE from a CIFS client to a file system mount point.

(e) Migration is performed.

(f) During migration, the auto commit period runs out.

(g) After the migration operation is complete, migration is performed again.

Evasion plan: To set an inheritable ACE for a file system mount point, run a `dirsetacl` command instead of operating from a CIFS client.

Recovery plan: None.

18) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 6.2.0-00

Phenomenon: Recreating the file system management information by running an `arccorrection` command is disabled.

Condition: It occurs when all the following conditions are met.

(a) A file system supporting WORM

(b) Auto commit is enabled.

(c) The file system is an Advanced ACL type file system.

(d) A CIFS administrator sets an inheritable ACE from a CIFS client to a file system mount point.

(e) The file system management information is recreated by running an `arccorrection` command.

(f) After (e) and before the stub processing runs, the auto commit period runs out.

(g) An `arccorrection` command is run again.

Evasion plan: To set an inheritable ACE for a file system mount point, run a `dirsetacl` command instead of operating from a CIFS client.

Recovery plan: None.

19) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 5.7.0-00

Phenomenon: When a file or folder is opened from a CIFS client, smbd outputs a core file.

Condition: It occurs when all the following conditions are met.

(a) A file or folder with a name containing both of the character and the code below is created with a client other than CIFS client (such as NFS client).

(a-1) One or more characters whose character code is not UTF-8

(a-2) A one or more-bytes control code (*)

* Control code: 0x01 to 0x1f, 0x22, 0x2a, 0x2f, 0x3a, 0x3c, 0x3e, 0x3f, 0x5c, 0x7c

(b)The file or folder that meets the above condition is opened from a CIFS client.

Evasion plan: None.

Recovery plan: Change the name of the file or folder created with an NFS client so as not to contain character codes that are not UTF-8 and control codes.

20) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 5.7.0-00

Phenomenon: Restarting the CIFS service may fail.

Condition: It may occur when all the following conditions are met.

(a) The system load is high.

(b) A CIFS client accesses a CIFS share.

(c) The CIFS service is restarted.

Evasion plan: None.

Recovery plan: Wait for a while, and then start the CIFS service.

21) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 5.7.0-00

Phenomenon: A memory leak occurs in a CIFS service process (smbd).

Condition: It may occur when all the following conditions are met.

(a) The CIFS service is used.

(b) Collecting a name from user/group identifier (SID) is requested from a CIFS client.

Evasion plan: None.

Recovery plan: Restart the CIFS service.

22) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 02-01-00-00

Phenomenon: A node goes down when a cluster or node is started or stopped.

Condition: It may occur when the following conditions (a) and (b), or (a) and (c) are met.

(a) Cluster model

(b) One of the following operations is performed immediately after the node OS start.

(b-1) Starting cluster

(b-2) Stopping cluster

(b-3) Starting node

(b-4) Stopping node

(c) The configuration wizard is started and system configuration is performed.

Evasion plan: Do not use the configuration wizard, but manually start or stop the cluster or node. Also wait for about 5 minutes after the node OS restart is complete (notification of OS ready or confirmation of BOOT COMPLETE status), and then perform the operation.

Recovery plan: Perform failback.

23) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 02-01-00-00

Phenomenon: When the database update processing after update installation fails, the management GUI is unavailable unless new installation is performed.

Condition: It may occur after update installation.

Evasion plan: Perform new installation.

Recovery plan: Perform update installation.

24) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-02

Affected version: 02-01-00-00

Phenomenon: Vulnerabilities reported by the following CVEs may adversely affect operations.

CVE-2020-14779/CVE-2020-14781/CVE-2020-14782/

CVE-2020-14792/CVE-2020-14796/CVE-2020-14797/

CVE-2020-14798

Condition: It may occur when a request from a malicious user is received.

Evasion plan: None.

Recovery plan: None.

25) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 5.7.0-00

Phenomenon: The vulnerability reported with the CVE below might affect.

CVE-2017-14746/CVE-2017-15275

Condition: It may occur when a CIFS access from a malicious user is received.

Evasion plan: None.

Recovery plan: None.

26) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 02-01-00-00

Phenomenon: The stub processing failed.

Condition: It may occur when all the following conditions are combined.

(a) The stub processing ends.

(b) The next stub processing is started.

(c) The processing in (a) and that in (b) run concurrently.

(d) While the stub processing started in (b) is running, the next stub processing is run.

Supplement:

The stub processing runs every 30 minutes. Therefore, the problem occurs if the stub processing takes 30 minutes or more.

Evasion plan: None.

Recovery plan: Create the file system management information again by using an `arccorrection` command.

27) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 02-01-00-00

Phenomenon: The stub processing failed.

Condition: It may occur when one of the following operations is performed concurrently with the stub processing.

(a) Migration (in case of files that are targets for WORM auto commit)

(b) Recall

(c) Data import from different file server

(d) New file creation

(e) File update

(f) File or directory rename

Evasion plan: None.

Recovery plan: Create the file system management information again by using an `arccorrection` command.

28) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 5.2.0-00

Phenomenon: Even though a file on an HDI has been migrated to an HCP, some files are not stubbed and the free capacity of the file system reduced.

Condition: It may occur when all the following conditions are combined.

(a) A read-write-content-sharing file system

(b) Meta data update is performed for a stub file by an operation, such as running a `touch` command.

(c) The data in the stub file is not updated or referred, and a recall does not occur.

(d) Migration is performed for the HCP.

Evasion plan: None.

Recovery plan: Create the file system management information again by using an `arccorrection` command.

29) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 02-02-01-00

Phenomenon: The vulnerability reported with the CVE below might affect.

CVE-2020-14803

Condition: It may occur when a factitious request is received from a malicious user.

Evasion plan: None.

Recovery plan: None.

30) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 6.1.0-00

Phenomenon: The number of files and the file size of the migration history were not displayed.

Condition: It occurs when either of the following conditions (a) or (b) is met.

(a) All the following conditions are met.

(a-1) A migration task ends during non-daylight saving time.

(a-2) Daylight saving time begins.

(a-3) During daylight saving time, the migration history of (a-1) is confirmed in the History tab of the migration-task page in the Migration Tasks dialog box on GUI.

(b) All the following conditions are met.

(b-1) A migration task ends during daylight saving time.

(b-2) Daylight saving time ends.

(b-3) During non-daylight saving time, the migration history of (b-1) is confirmed in the History tab of the migration-task page in the Migration Tasks dialog box on GUI.

Evasion plan: None

Recovery plan: None

31) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 6.1.0-00

Phenomenon: When an `arcmigstatus` command was run with `--day` specified, the migration history of the incorrect date is displayed.

Condition: It occurs when either of the following conditions (a) or (b) is met.

(a) All the following conditions are met.

(a-1) A migration task ends during non-daylight saving time.

(a-2) Daylight saving time begins.

(a-3) During daylight saving time, an `arcmigstatus` command is run with `--day` specified.

(a-4) The command of (a-3) is run between 00:00 to 01:00.

(a-5) The date of (a-1) is within the days specified for the `--day` option of (a-3).

(b) All the following conditions are met.

(b-1) A migration task ends during daylight saving time.

(b-2) Daylight saving time ends.

(b-3) During non-daylight saving time, an `arcmigstatus` command is run with `--day` specified.

(b-4) The command of (b-3) is run between 23:00 to 00:00.

(b-5) The date of (b-1) is within the days specified for the `--day` option of (b-3).

Evasion plan: None

Recovery plan: None

32) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-03

Affected version: 02-01-00-00

Phenomenon: After running an `arccorrection` command, files are not stubbed.

Condition: It may occur when all the following conditions are met.

(a) A time zone that is ahead of UTC is set for HDI.

(b) For some failure, the management information of a file system becomes incomplete, and taking actions for the error message is required or running an `arccorrection` command is instructed by maintenance personnel.

(c) An `arccorrection` command is run.

(d) The date of local time (*) 24 hours before the command is run in (c) is the same as the current date of UTC (*).

(e) File stubbing is performed.

*: The date of the local time and that of UTC can be confirmed by running a `timeget` command (no option specified) and a `timeget` command with `-u` specified respectively.

Evasion plan: Do not run an `arccorrection` command at a time when the date 24 hours ago in local time (*) is the same as the current date of UTC (*).

*: The date of the local time and that of UTC can be confirmed by running a `timeget` command (no option specified) and a `timeget` command with `-u` specified respectively.

Recovery plan: Run an `arccorrection` command at a time when the date 24 hours ago in local time (*) is not the same as the current date of UTC (*).

*: The date of the local time and that of UTC can be confirmed by running a `timeget` command (no option specified) and a `timeget` command with `-u` specified respectively.

33) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 6.4.0-00

Phenomenon: Old versions of temporary objects of the Large File Transfer (LFT) function remained on an HCP, so that the capacity usage of the HCP namespace increased wrongly.

Condition: It occurs when all the following conditions are combined.

(a) The migration processing using the LFT function for the same file cannot be complete within the time-out time or the migration aborting time and are stopped several times.

(b) One of the following operations is performed.

(b-1) After the file for which migration is stopped in (a) is deleted, migration is performed.

(b-2) Migration is performed without using the LFT function. (Cases that the LFT function is disabled and the capacity of work space is insufficient)

Evasion plan: None.

Recovery plan: After the versioning retention period passes over, olde versions are deleted and the problem is solved automatically.

To manually solve the problem, delete old versions of temporary objects of the LFT function (objects whose extension is tmp).

Note that even if the modified version with the fix for this problem is applied, already remained old versions of temporary objects cannot be deleted. In this case, take the recovery action where necessary.

34) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 6.0.3-00

Phenomenon: A WORM file whose retention period had expired could not be deleted.

Condition: It may occur when all the following conditions are combined.

(a) A WORM file system

(b) The Auto Commit mode is "auto".

(c) After a file is changed to the WORM status by Auto Commit and before it is accessed (before the file becomes read only), it is migrated to an HCP system.

(d) The retention period of the WORM file expires.

(e) The file system is created again and then arcrestore is run.

Evasion plan: None.

Recovery plan: (a) Verify that Max retention is "infinite" by running an `fslist` command (with `-v` option specified).

(b) If Max retention is "infinite", change Max retention to other than "infinite" by running an `fsedit` command (`-w -M` option specified)

(c) Set read only for the target file.

(c-1) In the case of CIFS share file

Change the attribute setting to read only instead of changing ACL setting.

(c-2) In the case of NFS share file

Release the write permission (w) for all of user, group, and other.

(d) Set the write permission for the target file.

(d-1) In the case of CIFS share file

Release the read only attribute.

(d-2) In the case of NFS share file

Set the write permission (w) for one of user, group, and other.

(e) Delete the target file.

35) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 6.4.6-00

Phenomenon: When starting to connect to a CIFS share from a CIFS client, Active Directory authentication failed and KAQG62001-W message (process name: smbd) was output.

Condition: It may occur when all the following conditions are combined.

(a) Active Directory authentication is used for the authentication mode used by the CIFS service.

(b) Connecting from a CIFS client with HDI IP address specified is attempted.(Authentication with NTLM)

(c) Either of the following is satisfied when smbd connects DC.

(c-1) User mapping is enabled. Then a communication from smbd to winbindd fails.

(c-2) User mapping is enabled . Then a client uses NTLMv2 to authenticate a CIFS service in a resource group that has fail-overed.

(c-3) User mapping is disabled.

Evasion plan: Connect from a CIFS client with HDI host name specified. (authentication with Kerberos)

Recovery plan: None.

36) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 02-01-00-00

Phenomenon: Downloading "User mapping info." using "Batch-download" in the List of RAS Information page failed and KAQM09039-E was output.

Condition: It may occur when all the following conditions are combined.

(a) The LDAP method is used for user mapping used by the CIFS service.

(b) "Batch-download" is displayed in the List of RAS Information page, and then "User mapping info." is downloaded.

Evasion plan: None.

Recovery plan: None.

37) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 6.1.0-00

Phenomenon: Unnecessary data remained on an HCP at a retry of migration.

Condition: It may occur when one of the following conditions is met.

(a) When a file is updated during migration, the following conditions (a-1) to (a-4) are combined.

(a-1) The number of retires of the migration if a file is updated during the migration is not 0. (it is the value in the Update retry max column of `arcconflist` command, and the default is 1.)

(a-2) The Active File Migration function is disabled.

(a-3) A new file is migrated.

(a-4) The file is updated during the migration.

(b) When a directory or a special file is updated during migration, the following conditions (b-1) to (b-3) are combined.

(b-1) The number of retries of the migration if a file is updated during the migration is not 0. (It is the value in the Update retry max column of `arcconflist` command, and the default is 1.)

(b-2) A new directory or a new special file is migrated.

(b-3) The directory or the special file is updated during the migration.

(c) When an error occurs on the communication to an HCP, the following conditions (c-1) to (c-3) are combined.

(c-1) The number of retries at an error on the communication to an HCP is not 0. (It is the value in the Retry max column of `arcconflist` command, and the default is 1.)

(c-2) A new file is migrated.

(c-3) An error occurs on the communication to the HCP during the migration.

Evasion plan: Set 0 for the number of retries by running an `arcconfedit` command with `--update-retry-max` option and `--retry-max` option.

Note that the migration is not retried by setting 0 for the number of retries so that migration tends to fails.

Recovery plan: Delete unnecessary HCP objects on the HCP side.

Once deleted then the HCP objects can be detected as Orphan object after the following operations are performed in the listed order.

(a) Retry the migration.

(b) Verify that everything ends normally.

(c) Run an `hcporphanrestore` command `--display` option.

38) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 02-01-00-00

Phenomenon: A file could not be turned into a stub file so that the free capacity of the file system could not increase.

Condition: It occurs when all the following conditions are combined.

(a) After the meta-data of a stub file is updated, the data is updated.

(b) A recall of the data is not performed.

(c) Migration is performed.

Evasion plan: None.

Recovery plan: Run an `arccorrection` command.

39) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 6.0.0-00

Phenomenon: The performance statistics information of the service on the day of daylight saving time start could not be collected.

Condition: It occurs when all the following conditions are combined.

(a) Daylight saving time is applied.

(b) The performance statistics information collection function is used.

(Directories on a file system are set by `perfmonctl` command `--setdir` option)

(c) The day of daylight saving time start passes.

Evasion plan: None.

Recovery plan: None.

40) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 6.0.0-00

Phenomenon: The data of a file system that referred the data of a different HDI as read only could not be synchronized with the data on an HCP.

Condition: It occurs when all the following conditions are combined.

(a) A file system of the sub-tree namespace.

(b) The file system refers the data of a different HDI as read only.

(c) Before setting a sub-tree namespace, a CIFS share or NFS share is created under the sub-tree.

(d) A sub-tree namespace is set.

Evasion plan: Do not create a share under the sub-tree before setting the sub-tree namespace.

Recovery plan: Take following actions on the file system that refers the data of a different HDI as read only.

(a) Delete the target sub-tree and the share under the sub-tree by running a command for deleting share (`cifsdelete`/`nfsdelete`).

(b) Delete the setting of the target sub-tree namespace by running a command for deleting namespace (`arcstdel`).

(c) Set the sub-tree namespace again.

(d) Create a share under the sub-tree.

41) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 6.1.0-00

Phenomenon: When file system editing was performed, the file system size was changed to an unintentional value.

Condition: It may occur when all the following conditions are combined.

(a) A file system that uses the Active File Migration function

(b) The work space size of the file system is different from that shown in Creating a shared directory in Single Node Administrator's Guide.

(c) The Edit File System dialog is displayed.

(d) OK is clicked in the Edit File System dialog and then the confirmation window is displayed.

(e) Apply is clicked in the confirmation window.

Evasion plan: Take the following actions.

(a) Verify that the work space size of the file system to be edited is the same as the value shown in Creating a shared directory in Single Node Administrator's Guide by running an `arcactmigctl` command.

If the size is consistent with value in the guide, no need to take the following actions.

(b) If the size is not the same as the value in the guide, delete the work space of the file system to be edited by running an `arcactmigctl` command.

(c) Set the work space using the value shown in Creating a shared directory in Single Node Administrator's Guide by running an `arcactmigctl` command.

(d) Display the Edit File System dialog, and perform an operation to edit the file system.

(e) After the operation to edit the file system is complete, set the original value for the work space size by running an `arcactmigctl` command.

Recovery plan: None.

42) Following defect has been fixed by Hitachi Data Ingestor 6.4.8-04

Affected version: 02-02-01-00

Phenomenon: Vulnerabilities reported by the following CVEs may adversely affect operations.

CVE-2021-23841/CVE-2021-3450/CVE-2021-2161/CVE-2021-2163

Condition: It may occur when a factitious request is received from a malicious user.

Evasion plan: None.

Recovery plan: None.

Known problems

Not applicable for this release.

Port numbers

- The following port numbers are used by the product as a listening port. When firewall is designed, please refer to the port numbers below.

Table 14. Port numbers used by the product

Port numbers	Single node model	Cluster model	Service	Note
20(TCP)	X	X	FTP	
21(TCP)	X	X	FTP	
22(TCP)	X	X	SSH, SFTP	
69(UDP)	X	X	TFTP	
111(TCP/UDP)	X	X	The services related to NFS	
137(UDP)	X	X	NetBIOS over TCP/IP for CIFS service	
138(UDP)	X	X	NetBIOS over TCP/IP for CIFS service	
139(TCP)	X	X	NetBIOS over TCP/IP for CIFS service	
161(UDP)	X	X	SNMP	
443(TCP)	X	X	Management server and management console	
445(TCP)	X	X	Direct Hosting of SMB for CIFS service	
450(TCP/UDP)	X	X	File share for NFS (when the port number is set to a privileged port used by NFS service)	
451(TCP/UDP)	X	X	File share for NFS (when the port number is set to a privileged port used by NFS service)	
452(TCP/UDP)	X	X	File share for NFS (when the port number is set to a privileged port used by NFS service)	
4045(TCP/UDP)	X	X	Region lock on file share for NFS	
2049(TCP/UDP)	X	X	File share for NFS	

Port numbers	Single node model	Cluster model	Service	Note
9090(TCP)	X	X	Management API	
10000(TCP)	X	X	NDMP	
17001(UDP)		X	Internal communication between nodes	
17002(UDP)		X	Internal communication between nodes	
17003(UDP)		X	Internal communication between nodes	
20048(TCP/UDP)	X	X	NFS file sharing for when fixed port is selected and NFS version is not v4	
20265(TCP)	X	X	Maintenance interface	
29997(TCP/UDP)	X	X	NFS file sharing for when fixed port is selected and NFS version is not v4	
29998(TCP/UDP)	X	X	NFS file sharing for when fixed port is selected	
Dynamically assigned	X	X	NFS file sharing for when dynamic port is selected	

- When the product is connected to HCP or HCP Anywhere, the product uses the following ports to those products.

Table 15. Destination port numbers that are used for connecting the product to external server

Port numbers	Service	Target
443(TCP)	All Communication between HDI and HCP Anywhere	HCP Anywhere
80(TCP)	Data migration to HCP	HCP
443(TCP)	Data migration to HCP	HCP
9090(TCP)	HCP MAPI communication	HCP

Documents

Hitachi Data Ingestor ships with the following documents:

- Hitachi Data Ingestor Installation and Configuration Guide
- Hitachi Data Ingestor Cluster Getting Started Guide
- Hitachi Data Ingestor Cluster Administrator's Guide
- Hitachi Data Ingestor CLI Administrator's Guide
- Hitachi Data Ingestor Error Codes
- Hitachi Data Ingestor File System Protocols (CIFS/NFS) Administrator's Guide
- Hitachi Data Ingestor Single Node Administrator's Guide
- Hitachi Data Ingestor Enterprise Array Features Administrator's Guide
- Hitachi Data Ingestor Modular Array Features Administrator's Guide
- Hitachi Data Ingestor API References
- Hitachi Data Ingestor Single Node Getting Started Guide
- Hitachi Data Ingestor Cluster Troubleshooting Guide
- Hitachi Data Ingestor Single Node Troubleshooting Guide

Copyrights and licenses

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
1) 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, IBM, Lotus, MVS, OS/390, PowerPC, RS/6000, 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, 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, and the Windows start button 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 at https://www.hitachivantara.com/en-us/company/legal.html.