Hitachi Data Ingestor
5.2.1-00 Release Notes

Table of Contents

About This Document

These release notes provide late-breaking information about Hitachi Data Ingestor. They include 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 Hitachi Data Systems customers and authorized service partners who license and use the Hitachi Data Ingestor.

Getting Help

If you purchased this product from an authorized reseller, contact that reseller for support. For the name of your nearest authorized reseller, refer to the Hitachi Data Systems Support Web site for locations and contact information. To contact the Hitachi Data Systems Support Center, please visit the HDS Web site for current telephone numbers and other contact information: http://www.hds.com/services/support/.

About This Release

These release notes cover version 5.2.1-00 of the Hitachi Data Ingestor.

Product Package Contents

The following table lists the contents of the Hitachi Data Ingestor.

Table 1. Package Contents

Medium	Product Name	Revision
DVD-R	Hitachi Data Ingestor	5.2.1-00

New Features and Enhancements

None

Manual Corrections

Table 2. Corrections to "Hitachi Data Ingestor Administrator's Guide"

No	Location to be corrected	Corrections	
1	Table C-180 Information specified in the Edit File Capacity page Item: Capacity	Before	Select a value from 1 to 6 for the maximum size of the log file before it is switched to the next generation (units: MB). When the logged data exceeds the specified size, the log file is switched to the next generation. When you specify 5 MB or 6 MB for the CIFS log file size, the log file might be switched before the logged data exceeds the specified size.
		After	Select a value from 1 to 6 for the maximum size of the log file (units: MB). When the logged data exceeds the specified size, the log file is switched to the next generation.
2	Table G-6 ip (4) group	Add	ID Object name Type Meaning 24.4.1 ipCidrRouteEntry (1) - An ipCidrRoute entry
3	Table G-6 ip (4) group	Before	ID Object name Type 22.1.2 ipNetToMediaPhysAddress (2) INTEGER 22.1.3 ipNetToMediaNetAddress (3) PhysAddress 31.1.1.7 ipSystemStatsInHdrErrors (7) Counter64
		After	ID Object name Type 22.1.2 ipNetToMediaPhysAddress (2) PhysAddress 22.1.3 ipNetToMediaNetAddress (3) IpAddress 31.1.1.7 ipSystemStatsInHdrErrors (7) Counter32
4	Table G-6 ip (4) group	Before	ID Object name 24.4.1 ipCidrRouteDest (1) 24.4.2 ipCidrRouteMask (2) 24.4.3 ipCidrRouteTos (3) 24.4.4 ipCidrRouteNextHop (4) 24.4.5 ipCidrRouteIfIndex (5) 24.4.6 ipCidrRouteType (6) 24.4.7 ipCidrRouteProto (7) 24.4.9 ipCidrRouteInfo (9) 24.4.10 ipCidrRouteNextHopAS(10) 24.4.11 ipCidrRouteMetric1 (11) 24.4.12 ipCidrRouteMetric2 (12) 24.4.13 ipCidrRouteMetric3 (13) 24.4.14 ipCidrRouteMetric4 (14) 24.4.15 ipCidrRouteMetric5 (15) 24.4.16 ipCidrRouteStatus (16)

		After	ID Object name 24.4.1.1 ipCidrRouteDest (1) 24.4.1.2 ipCidrRouteMask (2) 24.4.1.3 ipCidrRouteTos (3) 24.4.1.4 ipCidrRouteNextHop (4) 24.4.1.5 ipCidrRouteIfIndex (5) 24.4.1.6 ipCidrRouteType (6) 24.4.1.7 ipCidrRouteProto (7) 24.4.1.9 ipCidrRouteInfo (9) 24.4.1.10 ipCidrRouteNextHopAS(10) 24.4.1.11 ipCidrRouteMetric1 (11) 24.4.1.12 ipCidrRouteMetric2 (12) 24.4.1.13 ipCidrRouteMetric3 (13) 24.4.1.14 ipCidrRouteMetric4 (14) 24.4.1.15 ipCidrRouteMetric5 (15) 24.4.1.16 ipCidrRouteStatus (16)
5	Table G-14 ucdavis (2021) group	Before	ID Object name Type 8.1.100 extResult (100) DisplayString
		After	ID Object name Type 8.1.100 extResult (100) Integer32

Table 3. The corrections of "Hitachi Data Ingestor API References"

No	Location to be corrected	Corrections	
1	Table 3-13 XML structure when the PUT method is used to send a request to the CIFSShare resource Table 3-103 XML structure when a PUT method request is sent to the NFSShare resource DirectorySetup property - userName property/groupName property - Number of items that can be specified	Before	1
		After	0 or 1
2	Table 3-14 Properties used to send a PUT method request to the CIFSShare resource Table 3-104 Properties	Before	None

	used to send a PUT method request to the NFSShare resource DirectorySetup property - userName property/groupName property - Description	After	Added below. "If userName property or groupName property is omitted, root is set."
3	Table 3-14 Properties used to send a PUT method request to the CIFSShare resource Table 3-104 Properties used to send a PUT method request to the NFSShare resource DirectorySetup property - userName property/groupName property - Specification	Before	Required if the DirectorySetup property is set.
		After	Can bespecified when the DirectorySetup property is set.
4	Table 3-14 Properties used to send a PUT method request to the CIFSShare resource Table 3-104 Properties used to send a PUT method request to the NFSShare resource DirectorySetup property - isStickyBit property/groupPermission property/ownerPermission property/otherPermission property – Description	Before	None
		After	Added below. "If userName property or groupName property is omitted, the specified sticky bit and permission to access share directory is ignored."

Table 4 Corrections to "Hitachi Data Ingestor CLI Administrator's Guide"

No	Location to be corrected	Corrections	
1	arcresvset (Setting the reserved space for file systems that link to the HCP system) Options and arguments --resv-space reserved-space	Before	Percentages will be specified in the form n%. The letter n refers to a whole number in the range from 1 to 10.
		After	Percentages will be specified in the form n%. The letter n refers to a whole number in the range from 0 to 10. The following is added. When 0%, 0g, or 0G is specified, the capacity used by the system is not reserved.

Table 5. Corrections to "Hitachi Data Ingestor Single Node Administrator's Guide"

No	Location to be corrected	Corrections	
1	Table F-6 ip (4) group	Add	ID Object name Type Meaning 24.4.1 ipCidrRouteEntry (1) - An ipCidrRoute entry
2	Table F-6 ip (4) group	Before	ID Object name Type 22.1.2 ipNetToMediaPhysAddress (2) INTEGER 22.1.3 ipNetToMediaNetAddress (3) PhysAddress 31.1.1.7 ipSystemStatsInHdrErrors (7) Counter64
		After	ID Object name Type 22.1.2 ipNetToMediaPhysAddress (2) PhysAddress 22.1.3 ipNetToMediaNetAddress (3) IpAddress 31.1.1.7 ipSystemStatsInHdrErrors (7) Counter32

3	Table F-6 ip (4) group	Before	ID Object name 24.4.1 ipCidrRouteDest (1) 24.4.2 ipCidrRouteMask (2) 24.4.3 ipCidrRouteTos (3) 24.4.4 ipCidrRouteNextHop (4) 24.4.5 ipCidrRouteIfIndex (5) 24.4.6 ipCidrRouteType (6) 24.4.7 ipCidrRouteProto (7) 24.4.9 ipCidrRouteInfo (9) 24.4.10 ipCidrRouteNextHopAS(10) 24.4.11 ipCidrRouteMetric1 (11) 24.4.12 ipCidrRouteMetric2 (12) 24.4.13 ipCidrRouteMetric3 (13) 24.4.14 ipCidrRouteMetric4 (14) 24.4.15 ipCidrRouteMetric5 (15) 24.4.16 ipCidrRouteStatus (16)
		After	ID Object name 24.4.1.1 ipCidrRouteDest (1) 24.4.1.2 ipCidrRouteMask (2) 24.4.1.3 ipCidrRouteTos (3) 24.4.1.4 ipCidrRouteNextHop (4) 24.4.1.5 ipCidrRouteIfIndex (5) 24.4.1.6 ipCidrRouteType (6) 24.4.1.7 ipCidrRouteProto (7) 24.4.1.9 ipCidrRouteInfo (9) 24.4.1.10 ipCidrRouteNextHopAS(10) 24.4.1.11 ipCidrRouteMetric1 (11) 24.4.1.12 ipCidrRouteMetric2 (12) 24.4.1.13 ipCidrRouteMetric3 (13) 24.4.1.14 ipCidrRouteMetric4 (14) 24.4.1.15 ipCidrRouteMetric5 (15) 24.4.1.16 ipCidrRouteStatus (16)
4	Table F-14 ucdavis (2021) group	Before	ID Object name Type 8.1.100 extResult (100) DisplayString
		After	ID Object name Type 8.1.100 extResult (100) Integer32

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.

- In **Cache Resident** tab on **File Systems** window of GUI, Cache resident information is not displayed. Also **Download List of Pinned Files** button is not available.
- 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.
- Even when the encryption license is set, Encryption Settings may not be displayed in the System Information panel on the Dashboard tab on single node GUI. If the setting is not displayed, confirm Encryption Settings on the *host-name* window.
- 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.

License Keys

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

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.
- With versions 4.0.0-00 and later, there is a change in cache residency function. To perform update installation from versions earlier than 4.0.0-00, note that;
  - If a file has been stubbed before policy setting, the entity of the file is not returned to HDI immediately after policy setting even if the file is a cache residency target.
  - The following functions are not available.
    - · Displaying files with cache residency
    - · Displaying result of cache residency processing

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 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

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 4 in 4.2.0-00 or later.

Table 6 The 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.
- When a file system linked to the HCP is deleted and then a file system with the same name is created, both policies of before deletion and after creation may be displayed on the [Task Management] dialog box. In this case, Present Status of policies after creation and before deletion are [Scheduled] and [Standby] respectively. As the policy of after deletion is not scheduled, it does not affect the behavior.

- 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.

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

Usage precautions for update installation

- "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.

Caution when deny setting of ACL is prioritized

- With versions earlier than 5.0.1-00, due to the problem that has been fixed with 5.0.1-00, a deny setting of ACL that is not intended to be prioritized in ACL order of directory/file may be prioritized. After update installation, as the ACL order of directory/file created with the version earlier than 5.0.1-00 does not change, set the ACL order again if necessary.

  To reset, perform one of the following operations.

・Resetting procedure from Windows command.

(1) Run icacls command for the most superior directory of the resetting target file.

Record all of ACLs under the specified directories displayed.

(2) Make the setting from the most superior directory 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 most superior directories 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 most superior directory 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).

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 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.

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.

Requirement for use Management Console for Single Node Configuration

- Operating system requirement for management console

Table 7 Supported platforms for management console

Operating Systems
Windows® 7, no service pack or Service Pack 1 Windows 7 Professional Windows 7 Ultimate Windows 7 Enterprise
Windows 7 x64 Editions, no service pack or Service Pack 1 Windows 7 Professional Windows 7 Ultimate Windows 7 Enterprise
Windows® 8 Windows 8 Enterprise Windows 8 Pro
Windows 8 x64 Editions Windows 8 Enterprise Windows 8 Pro
Windows® 8.1 Windows 8.1 Enterprise Windows 8.1 Pro
Windows 8.1 x64 Editions Windows 8.1 Enterprise Windows 8.1 Pro
Windows Vista®, Service Pack 1 or Service Pack 2 Windows Vista Ultimate Windows Vista Business Windows Vista Enterprise
Windows Vista x64 Editions, Service Pack 1 or Service Pack 2 Windows Vista Ultimate Windows Vista Business Windows Vista Enterprise
Windows Server® 2003, Service Pack 1 or Service Pack 2 Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition Windows Server 2003, Datacenter Edition

Operating Systems
Windows Server 2003 x64 Editions, Service Pack 1 or Service Pack 2 Windows Server 2003, Standard x64 Edition Windows Server 2003, Enterprise x64 Edition Windows Server 2003, Datacenter x64 Edition
Windows Server 2003 R2, no service pack or Service Pack 2 Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition Windows Server 2003 R2, Datacenter Edition
Windows Server 2003 R2, x64 Editions, no service pack or Service Pack 2 Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Enterprise x64 Edition Windows Server 2003 R2, Datacenter x64 Edition
Windows Server 2008 x64 Editions, Service Pack 1 or Service Pack 2 Windows Server 2008, Standard x64 Edition Windows Server 2008, Enterprise x64 Edition Windows Server 2008, Datacenter x64 Edition
Windows Server 2008, Service Pack 1 or Service Pack 2 Windows Server 2008, Standard Edition Windows Server 2008, Enterprise Edition Windows Server 2008, Datacenter Edition
Windows Server 2008 R2, no service pack or Service Pack 1 Windows Server 2008 R2, Standard Edition Windows Server 2008 R2, Enterprise Edition Windows Server 2008 R2, Datacenter Edition
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
Red Hat Enterprise Linux 5.6 Red Hat Enterprise Linux 5.6 Advanced Platform
Red Hat Enterprise Linux 6.4

- Required Web browser for management console

Table 8 Supported Web browsers for management console

Web browser	Remark
Internet Explorer® 7.0	32-bit version
Internet Explorer 8.0	32-bit version

Web browser	Remark
Internet Explorer 9.0	32-bit version
Internet Explorer 10.0	32-bit version
Internet Explorer 11.0[#3]	32-bit version
Mozilla Firefox 3.6.x[#1#2]	x86 version
Mozilla Firefox ESR 10.0.x[#1#2]	x86 version
Mozilla Firefox ESR 17.0.x[#1#2]	x86 version
Mozilla Firefox ESR 24.1.x[#1#2]	x86 version
Mozilla Firefox ESR 31.0.x[#1#2]	x86 version

[#1]: x means that it does not depend on the version x.

[#2]: Supported platforms for Hitachi File Services Manager 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.

- Required programs for management console

Table 9 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 Backup Restore function with Symantec NetBackup(TM), the following programs is required:

- Symantec NetBackup(TM) Enterprise Server 7.0.
- Symantec NetBackup(TM) for NDMP.

To use Backup Restore function with Hitachi Data Protection Suite, powered by CommVault®, the following program is required:

- Hitachi Data Protection Suite, powered by CommVault® 8.0.

Known Problems

Not Applicable for this release.

Fixed Problems

(1) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 4.2.3-01

The phenomenon: After turning a file to a WORM file, read-only attribute of the WORM file whose retention period expires cannot be released by an operation from a CIFS client. As a result, the file cannot be deleted manually.

The condition: It occurs when a file is turned to a WORM file by the auto commit function of wormctl command.

The evasion plan: None.

The recovery plan: Delete the WORM file whose retention period expires by one of the following operations.

(a) Enable the auto-dispose function by wormctl command to automatically delete the file.

(b) From a root user, access NFS share to which anonymous mapping is not applied, set the write (w) permission of the file, and then delete the file.

(2) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 5.2.0-00

The phenomenon: When the reserved space used by a system is set in a file system combined with HCP, stubbing processing concentrates in the time period where the impact on operations is large (around UTC 00:07), so that the system workload increases.

The condition: It occurs when the conditions below are all combined.

(a) Other than 0 is set to the reserved space of file system that is combined with HCP.

(b) Other than 0 is set to the threshold for stubbing initiation of file system.

The evasion plan: None.

The recovery plan: None.

(3) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 02-01-00-00

The phenomenon: A file access from a CIFS client is hung up.

The condition: It might occur when the conditions below are all combined.

(a) A file system to which recording the last access time (atime) is enabled.

(b) For the file system of (a), differential-data snapshot creation or release of unused area in virtual LU is performed.

(c) For the same file in the file system of (a), accesses from CIFS clients in one of the following combinations conflict.

(c-1) Reading and writing

(c-2) Reading and file attribute change

(d) The last access time (atime) of the file of (c) applies to one of the following.

(d-1) Before the last edit time (*1)(mtime) of the file.

(d-2) Before the last update time (*2)(ctime) of the file.

(d-3) More than 24 hours before the current time.

*1: The time when the file content is changed.

*2: The time when the file attribute or content is changed.

The evasion plan: None.

The recovery plan: None.

(4) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 02-01-00-00

The phenomenon: Log information output when a message of KAQG62001-W for abnormal end of process is reported is enhanced.

The condition: The enhanced log information is output when the system workload increases and response degradation of system continues for 20 seconds or longer.

The evasion plan: None.

The recovery plan: None.

(5) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 03-00-00-00

The phenomenon: Values of MIB objects may not be obtained.

The condition: It might occur when the following MIB objects are obtained.

ipCidrRouteDest.

ipCidrRouteMask.

ipCidrRouteNextHop.

The evasion plan: None.

The recovery plan: None.

(6) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 03-00-00-00

The phenomenon: The value of MIB object that indicates netmask is not correct.

The condition: It occurs when the following MIB object is obtained.

ipCidrRouteMask.

The evasion plan: None.

The recovery plan: None.

(7) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 02-01-00-00

The phenomenon: When the OS is terminated abnormally or a node is reset, an inconsistency may occur in OS LU. If the OS detects the inconsistency after reboot, it is terminated abnormally.

The condition: It might occur when the conditions below are all combined.

(a) A system deletes a file on OS LU in HDI.

(b) The OS ends abnormally or a node is rebooted.

The evasion plan: None.

The recovery plan: None.

(8) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 4.2.3-00

The phenomenon: When communicating with HCP via a proxy server that requires user authentication, the connecting to HCP fails with a message of KAQM37037-E (communication with HCP fails) reported.

The condition: It occurs when the conditions below are all combined.

(a) A proxy server that requires user authentication is set to HDI.

(b) The proxy server of (a) supports Negotiate authentication.

The evasion plan: None.

The recovery plan: None.

(9) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 4.2.3-00

The phenomenon: When a proxy server that requires user authentication and HTTP protocol are used for communication with HCP, data transfer to HCP fails with a message of KAQM37037-E (Communication with HCP fails) reported.

The condition: It occurs when the conditions below are all combined.

(a) A proxy server that requires user authentication is set in HDI.

(b) For a protocol used to communicate with HCP, HTTP is set instead of HTTPS.

(c) One of the following operations to transfer the data to HCP is performed.

- Migration
- Cache resident policy setting or setting change
- System LU saving

The evasion plan: None.

The recovery plan: None.

(10) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 4.2.3-00

The phenomenon: When setting a wrong user name or password as the information of proxy server that requires user authentication and then communicating with HCP via the proxy server, an inadequate message of KAQM37021-E (internal error) is output and the connection to HCP fails.

The condition: It occurs when the conditions below are all combined.

(a) A proxy server that requires user authentication is set to HDI.

(b) A user name or password set in (a) is incorrect.

(c) One of the following operations is performed.

- Migration
- Cache resident policy setting or setting release
- System LU restoring
- Restoring file system from which the data is migrated to HCP

The evasion plan: None.

The recovery plan: None.

(11) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 3.2.0-00

The phenomenon: When a proxy server is used for communication with HCP, capacity expansion of system name space (system-backup-data, rwcs-system) fails.

The condition: It occurs when the conditions below are all combined.

(a) A proxy server is set to HDI.

(b) The capacity used by system name space (system-backup-data) exceeds the value of hard Quota.

(c) One of the following operations is performed.

- System LU saving or restoring
- Restoring file system from which the data is migrated to HCP
- Cache resident policy setting or setting release for a sub-tree file system

- Migration

The evasion plan: None.

The recovery plan: None.

(12) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 02-01-00-00

The phenomenon: Migration fails.

The condition: It might occur when the conditions below are all combined.

(a) HCP is combined.

(b) The system is highly loaded.

The evasion plan: None.

The recovery plan: If migration schedule is set, no action is required because migration is done for the file whose migration fails at the next schedule.

If migration schedule is not set, perform migration manually.

(13) Following defect has been fixed by Hitachi Data Ingestor 5.2.1-00

Affected version: 5.2.0-00

The phenomenon: When renaming or deleting a read-write-content sharing file, OS is rebooted.

The condition: It might occur when the conditions below are all combined.

(a) A read-write-content sharing is used.

(b) A file that is updated in HDI at a different site is accessed.

(c) Renaming or deleting is performed for the file of (b) at the same time of (b).

The evasion plan: None.

The recovery plan: None.

Documents

In addition to the help system, Hitachi Data Ingestor ships with the following:

- *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 Backup Restore Features Supplement for Hitachi Data Protection Suite*

- *Hitachi Data Ingestor Backup Restore Features Supplement for IBM® Tivoli® Storage Manager*
- *Hitachi Data Ingestor Backup Restore Features Supplement for Symantec NetBackup*
- *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*

Port numbers

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

Table 10 Port numbers used by the product

Port numbers	Model		Service	Note
	Single	Cluster		
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	
4045(TCP/UDP)	X	X	Region lock on file share for NFS	
2049(TCP/UDP)	X	X	File share for NFS	
8005(TCP)	X	X	Management for HCP data migration	
8006(TCP)		X	Management for HCP data migration	
8443(TCP)	X	X	Management for HCP data migration	
8444(TCP)		X	Management for HCP data migration	
9090(TCP)	X	X	Management API	

Port numbers	Model		Service	Note
	Single	Cluster		
10000(TCP)	X	X	NDMP	
15000~15019, 19012(TCP/UDP)	X	X	Management for HCP data migration	
15020~15039, 19032(TCP/UDP)		X	Management for HCP data migration	
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 11. Destination port numbers which 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