Hitachi Data Ingestor v6.4.6-03 Release Notes

Contents

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

RN-90HDI011-84 (July 2019)

About this document

This document (RN-90HDI011-84, July 2019) provides late-breaking information about Hitachi Data Ingestor 6.4.6-03. 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	6.4.6-03

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

New Features and Enhancements

Table 2. New Features and Enhancements

No	Contents	Revision
1	AES256 and AES128 are supported as Kerberos encryption algorithm used by CIFS service Active Directory authentication.	6.4.6-00
2	Firmware version 24.18.0-0021 of RAID controller embedded in D51B-2U is supported.	6.4.6-00

Manual Corrections

None

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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

- 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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

License Keys

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

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:http://hdsnet.hds.com/techpub/hdi/mk-90hdicom031/hdicom0310.pdf).
- "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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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 spitting out KAQM20046-E message on HFSM screen.
  Please perform below procedure for Single Node and Cluster Models respectively, for the recovery.

  <Single Node Model>
  1. Login 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. Login 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. Login 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).

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

3) Start node0 by ndstart command.
4) Confirm node0 status is "UP" by clstatus command.

3. Login 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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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 target file systems	Content Sharing OFF	8	If file systems exceeding the recommended value are created, memory usage and CPU utilization increase, giving impact on the system performance. To create file systems exceeding the value, it is recommended to use separate systems.
2		Content Sharing ON (Read-Only)		
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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

No	Resource		Upper limit (Recommended value)	Note
				2TB.
9	Number of ACEs		700 for each file/directory	Setting over 700 ACEs causes an error.
10	Number of past version directories	Per system	4000	Tune Custom schedule so that the total sum of the number of past version directories per share does 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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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 access from Windows Server 2008 or Windows Vista

- When accessing a CIFS share from Windows Server 2008 or Windows Vista using SMB2, a measure described in Microsoft Knowledge Base 978625 is required. Check Knowledge Base and contact Microsoft Windows support.
  If the measure is not taken, Windows client becomes STOP error and error messages; "STOP: 0x00000027 (parameter1, parameter2, parameter3, parameter4)", and "mrxsmb20.sys - Address parameter1 base at parameter2, Datestamp parameter3", may appear on the blue screen.

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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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.

#	the 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)

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

- 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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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.

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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

- 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 3 in 4.2.0-00 or later.

Table 3. 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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

    - 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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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.

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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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
  ```

Requirement for use Management Console for Single Node Configuration

- Operating system requirement for management console

Table 4. Supported platforms for management console

Operating Systems
Windows® 7 Service Pack 1 • Windows 7 Professional • Windows 7 Ultimate • Windows 7 Enterprise

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

Operating Systems
Windows 7 x64 Editions Service Pack 1 • Windows 7 Professional • Windows 7 Ultimate • Windows 7 Enterprise
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 2008 x64 Editions Service Pack 2 [#1] • Windows Server 2008, Standard x64 Edition • Windows Server 2008, Enterprise x64 Edition • Windows Server 2008, Datacenter x64 Edition
Windows Server 2008 Service Pack 2 [#1] • Windows Server 2008, Standard Edition • Windows Server 2008, Enterprise Edition • Windows Server 2008, Datacenter Edition
Windows Server 2008 R2 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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

Operating Systems
• 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 5. Supported Web browsers for management console

Web browser	Remark
Internet Explorer 10.0 #4	32-bit version
Internet Explorer 11.0 #3	32-bit version
Mozilla Firefox ESR 38.0.x #1, #2	x86 version
Mozilla Firefox ESR 45.x #1, #5	x86 version
Mozilla Firefox ESR 52.x #1, #5	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: By changing the option setting of browser, TLS1.1 and TLS1.2 can be supported.
#5: Supported platforms for management console is only Windows.

- Required programs for management console

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

Table 6. 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
    - Windows Server 2008 R2 SP1
    - Windows Server 2008 SP2

Known Problems

Not Applicable for this release.

Fixed Problems

1) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-00

Affected version: 02-01-00-00

The phenomenon: When a host name of HDI is changed, a computer account of HDI before the change wrongly remains on Active Directory.

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

(a) Active Directory is used as a CIFS service authentication.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

(b) Either of the following operations is performed.

(b-1) A host name of a node is changed on the [Modify Host Name] page of the [Cluster Management] dialog, and then a resource group is started after OS is restarted.

(b-2) A host name of a node is changed with the System Configuration Wizard.

The evasion plan: None.

The recovery plan: By an operation of Active Directory, delete the computer account of HDI before the change that remains on Active Directory.

2) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-00

Affected version: 02-01-00-00

The phenomenon: A computer account of HDI wrongly remains on Active Directory.

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

(a) Either of the following operations is performed.

(a-1) On the CIFS Service Management page, CIFS service authentication mode is changed from the one other than Active Directory Authentication to Active Directory Authentication, and then the CIFS service is started or re-started.

(a-2) On the CIFS Service Maintenance page, Rejoin Active Directory Domain is performed.

(b) Kerberos authentication for Active Directory fails.

The Kerberos authentication fails in a case, for example, the encryption algorithm that Kerberos authentication uses is not admitted by Active Directory policy.

The evasion plan: None.

The recovery plan: By an operation of Active Directory, delete the HDI computer account created by joining in a domain.

3) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-00

Affected version: 02-01-00-00

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

The phenomenon: When CIFS service creates or updates a computer object of Active Directory, values in Service Principal Name (SPN) list used for Kerberos authentication are overwritten and the existing values are deleted, so that NFS clients cannot be authenticated.

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

(a) NFS service and CIFS service are used.

(b) Active Directory is used on CIFS.

(c) NFS authentication is Kerberos authentication in which Active Directory is used as Key Distribution Center (KDC).

(d) Both of the following are not applicable to Service Principal Name (SPN) that NFS clients use for authentication.

- HOST/<Node host name (FQDN)>@<Realm>
- HOST/<Node NetBIOS name>@<Realm>

(e) One of the following CIFS operations is performed.

- CIFS service is started for the first time.
- A change that requires restarting CIFS service is performed, and then the service is started or restarted.
- The GUI CIFS setting page, Rejoin is performed manually.

The evasion plan: Change the Kerberos authentication setting of NFS so that SPN used by the NFS service is one of the following.

- HOST/<Node host name (FQDN)>@<Realm>

  Example: HOST/node1.customer.com@CUSTOMER.COM
- HOST/<Node NetBIOS name>@<Realm>

  Example: HOST/NODE1@CUSTOMER.COM

The recovery plan: Define deleted Service Principal Name (SPN) on Active Directory again.

4) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-00

Affected version: 5.7.0-00

The phenomenon: A CIFS service setting change fails and CPU load rises.

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

(a) Active Directory is used as a CIFS authentication.

(b) The password of a domain user used for domain joining

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

needs to be changed because of password expiration or password change request by administrator.

(c) One of the following conditions is met.

(c-1) On the CIFS Service Management page, the CIFS service authentication mode is changed from the one other than Active Directory Authentication to Active Directory Authentication, and then the CIFS service is started or restarted.

(c-2) On the CIFS Service Management page, the CIFS service authentication mode is changed from Active Directory Authentication to the one other than Active Directory Authentication, and then the CIFS service is started or restarted.

(c-3) On the CIFS Service Management page, the domain name or the NetBIOS name of the domain is changed, and then the CIFS service is started or restarted.

The evasion plan: Remove the expiration date for the password of domain user used for domain joining so that the password does not need to be changed.

The recovery plan: Restart the node where the problem occurs.

5) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-00

Affected version: 4.2.1-00

The phenomenon: Winbindd does not reuse ldap connection.

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

(a) With versions 5.2.0-00 and later, the setting of using signed ldap communication with domain controller (client_ldap_sasl_wrapping = sign) has not been changed.

Or versions earlier than 5.2.0-00, the setting of ldap communication with domain controller is changed to "client_ldap_sasl_wrapping = sign".

(b) Active Directory is set as CIFS authentication.

(c) User mapping is used.

(d) Multiple CIFS connections are made from CIFS clients.

The evasion plan: None.

The recovery plan: None.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

6) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-00

Affected version: 02-01-00-00

The phenomenon: When the cache behavior in normal circumstance is the write through, the write back can be wrongly set for the cache behavior when the battery charge remaining of super capacitor is low by running cachedbadbbuset command.

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

(a) A single node model is used.

(b) The write through is set for the behavior of cache in an internal RAID controller for user disks in normal circumstance.

(c) cachedbadbbuset --wb command is run.

The evasion plan: None.

The recovery plan: Run cachedbadbbuset --wt command and change the cache behavior setting when the battery charge remaining of super capacitor is low to the write through.

7) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-00

Affected version: 02-01-00-00

The phenomenon: A computer account of HDI wrongly remains on Active Directory.

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

(a) Active Directory is used as an authentication of CIFS service.

(b) Multiple domain controllers are specified for HDI.

(c) A domain controller that cannot communicate with HDI is set at the forefront.

(d) One of the following operations is performed.

(d-1) On the CIFS Service Management page, the CIFS service authentication mode is changed from Active Directory Authentication to the one other than Active Directory Authentication, and then the CIFS service is started or restarted.

(d-2) On the CIFS Service Management page, the domain name or the NetBIOS name of the domain is changed,

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

and then the CIFS service is started or restarted.

The evasion plan: None.

The recovery plan: By an operation of Active Directory, delete the HDI computer account that remains on Active Directory.

8) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-01

Affected version: 02-01-00-00

The phenomenon: The data in a file becomes invalid.

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

(a) HCP is combined, or data has been imported from another file server.

(b) A rename operation is performed for a file or directory from a client.

(c) On the path of the rename destination, a migrated file or migrated directory exists, or a file or directory for which importing all data is not complete exist.

(d) The file of (c) is not a regular file. (symbolic link, directory, pipe file, character device, block device)

The evasion plan: When performing a rename operation from a client, first delete files and directories of the rename destination.

The recovery plan: Restore the file using the external backup or past version directory.

9) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 6.3.0-00

The phenomenon: A file under a renamed or moved directory cannot be migrated.

The condition: When the following operations are performed, a file under the directory renamed or moved in (b) is not migrated.

(a) arccorrection command is run.

(b) After (a), a directory is renamed or moved before migration.

(c) Migration is performed.

The evasion plan: To prevent rename or move from being performed for the directory, first delete the share, run arccorrection command,

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

and then perform migration. After the migration is complete, create the share again.

The recovery plan: To prevent rename or move from being performed for the directory, first delete the share, run arccorrection command, and then perform migration. After the migration is complete, create the share again.

10) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 6.1.0-00

The phenomenon: For a file system used to refer other HDI data in read-only, an unnecessary restore operation is repeatedly performed once every hour.

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

(a) Other HDI data is referred in read-only.

(b) A namespace is assigned per file system.

(c) In an HDI that shows the data, 128 or more migration operations are performed for the past 10 days.

(d) One of the following conditions is met.

(d-1) A file system for referring the data of (c) in read-only is created.

(d-2) Data synchronization of the file system used to refer the data of (c) in read-only fails due to a failure, such as communication error.

The evasion plan: For HDI that shows the data, perform migration at intervals of 2 hours or longer.
(If migration is performed every 2 hours, the number of migration operations is 120 in 10 days)

The recovery plan: Delete old generation number directories (files in the directories as well) so that the number of generation number directories is 127 or less on the HCP. The path of generation number directories on HCP is as follows.

/management/mig_results/<generation number>

11) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

Affected version: 5.3.0-00/6.0.0-00

The phenomenon: When other HDI data is referred in read-only using a file system, the latest data cannot be referred.

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

(a) Other HDI data is referred in read-only.

(b) There is a directory under a subdirectory of a file system used to refer other HDI data in read-only.

(Example: /mnt/fs01/dir1/dir2)

(c) The data in the file system used to refer other HDI data is restored using the data from HCP.
If data synchronization fails due to a failure, such as an error in communication with HCP, the data may be restored from HCP at the next synchronization.

The evasion plan: None.

The recovery plan: If directories whose latest data cannot be referred are identified, create or delete a file under the directories in the HDI that shows data.
In other cases, delete the file system used to refer other HDI data, and then create it again.

12) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 6.1.1-00

The phenomenon: KAQM16204-E appears and starting CIFS service fails.

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

(a) Active Directory is employed for CIFS service authentication.

(b) User mapping is used for CIFS service.

(c) There is no domain that has trust relationship with a domain where the HDI joins.

(d) A user account of the domain set to the CIFS service is deleted, or the password is changed or disabled.

The evasion plan: When a user account of the domain set to the CIFS service is deleted, or the password is changed or deleted on the domain controller side, change the CIFS service setting too.

The recovery plan: Confirm available domain user account, and then add it to the

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

CIFS service.

13) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 5.7.0-00

The phenomenon: A user mapping error occurs and connecting to a CIFS share fails.

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

(a) Active Directory is employed for CIFS service authentication.

(b) Active Directory Schema is employed for user mapping.

(c) "client_ldap_sasl_wrapping = plain" is set for LDAP communication with a domain controller. *1

(d) One of the following events takes place. *2

(d-1) Regular collection of the status of connection with an external server

(d-2) [Server check] with [List of RAS Information]

(d-3) [CIFS Service Maintenance] display

(d-4) All log collection

*1: It is not applicable to versions 6.4.6-00 and later.

*2: The status of connection with domain controller is checked.

The evasion plan: None.

The recovery plan: Restart the CIFS service.

14) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 02-01-00-00

The phenomenon: An access to a folder and file that the user does not have permission to access may be enabled.

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

(a) Active Directory is employed for CIFS service authentication.

(b) User mapping is used for CIFS service.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

(c) An access to a file or folder is attempted from Domain Admins of a domain where the HDI joins, or a user belongs to Domain Users.

(d) The ACL of files and folders that the user accesses contains ACE of access permission for root group.

The evasion plan: None.

The recovery plan:

a) Procedure for confirming BUILTIN\Administrators and BUILTIN\Users mapping

Verify that BUILTIN\Administrators (displayed as "Administrators (S-1-5-32-544)"), or BUILTIN\Users (displayed as "Users (S-1-5-32-545)") are mapped with a root group by running cifsgrpedit command.

```
$ sudo cifsgrpedit list
   :
Administrators (S-1-5-32-544) -> root                (*1)
   :
Administrators (xxxxxxx) -> Group_name_1             (*2)
   :
Users (S-1-5-32-545) -> root                         (*3)
   :
Users (yyyyyyy) -> Group_name_2                      (*4)
```

Note: When mappings (*1) and (*3) are displayed, a rood group is mapped with BUILTIN\Administrators or BUILTIN\Users.
When mappings (*2) and (*4) are displayed, take a note of them if these mappings are required. They will be used in "(b) Procedure for deleting BUILTIN\Administrators and BUILTIN\Users mapping

b) Procedure for deleting BUILTIN\Administrators and BUILTIN\Users mapping

If "Procedure for confirming BUILTIN\Administrators and BUILTIN\Users mapping" is performed and then "Administrators (S-1-5-32-544)" or "Users (S-1-5-32-545)" is displayed, delete the user group mapped with the root group by taking the actions below. This operation requires a client that can log in to the HDI system with ssh and terminal software that has the scp file transfer function.

i) Create a file for deleting mapping. Create also a file for re-creating mapping, if necessary.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

- If a root group is mapped with BUILTIN\Administrators:

File for deleting mapping=dellist1.txt

< Content of the file >
Administrators,Administrators

File for re-creating mapping=addlist1.txt

< Content of the file >
[Group name 1],Administrators

Note: Specify Group name: (*2) that is mapped to Administrators, of which you took a note in "(a) Procedure for confirming BUILTIN\Administrators and BUILTIN\Users mapping", for Group name 1.

- If a root group is mapped with BUILTIN\Users:

File for deleting mapping=dellist2.txt

< Content of the file >
Users,Users

File for re-creating mapping=addlist2.txt

< Content of the file >
[Group name 2], Users

Note: Specify Group name: (*4) that is mapped to Users, of which you took a note in "(a) Procedure for confirming BUILTIN\Administrators and BUILTIN\Users mapping", for Group name 2.

ii) Transfer the file that is created in (i) to the home directory for nasroot.

Log in with nasroot and transfer the file that is created in (i) by using the scp function of the terminal software to the home directory for nasroot (/home/nasroot).

iii) Delete mapping.

Delete a group mapped with the root group by running cifsgrpedit command.

Example: If a root group is mapped with Administrators (S-1-5-32-544)

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

```
$ sudo cifsgrpedit delete dellist1.txt
delete groupmap 'Administrators' success
result: success is 1, failure is 0.
```

iv) Verify that the group mapped with the root group is deleted.

```
$ sudo cifsgrpedit list
```

v) Repeat actions (iii) and (iv) until groups mapped with the root group are deleted.

vi) The mappings of Administrators and Users groups that are created by the user are deleted. If the mapping information is required, re-create it.

Example: Mapping of Administrators that is created by the user is required.

```
$ sudo cifsgrpedit add addlist1.txt
```

vii) Confirm that the mapping is re-created.

```
$ sudo cifsgrpedit list
```

viii) Delete the user mapping cache file.

In the [CIFS Service Maintenance] window, click the [Clear User Map Cache File] button.
If HDI joins or rejoins to the domain after deletion of user groups mapped to the root group, the built-in user may be mapped to the root group again. Therefor, if joining or rejoining to the domain is performed, perform "(a) Procedure for confirming BUILTIN\Administrators and BUILTIN\Users mapping", and then verify that the built-in user is not mapped to the root group. If it is mapped to the root group, delete it again.

15) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 03-00-00-00

The phenomenon: Memory leak occurs in a CIFS service process (winbindd for authentication).

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

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

(a) Active Directory is used.

(b) User mapping is used.

When all the following conditions are met while the HDI version is 6.4.6-00 or earlier, the amount of memory leak increases.

(a) Active Directory is used.

(b) User mapping is used.

(c) Active Directory Schema is employed for user mapping.

(d) For LDAP communication with a domain controller, set "sign" to "client_ldap_sasl_wrapping".
At new installation of 6.1.1-00 or later, the default value is "sign".
In the case of update installation from a version earlier than 6.1.1-00 to a version of 6.1.1-00 or later, if the value is already defined, it is taken over. If the value is not yet defined, the default value is "sign".

The evasion plan: HDI Version earlier than 6.4.6-00:

If "Domain controller: LDAP server signing requirements" of the domain controller policy is "None", the occurrence frequency can be decreased by setting "plain" to "client_ldap_sasl_wrapping" for the LDAP communication with the domain controller. The value can be set by running cifsoptset command.
If the setting cannot be changed, prevent the problem by periodical restart of the CIFS service. (approximately once every 3 weeks)

HDI version 6.4.6-00 or later:

None

The recovery plan: Restart the CIFS service.

16) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 6.3.1-00

The phenomenon: The information of LUs whose numbers are 0200 (hexadecimal) and greater is not displayed by Hitachi Command Suite Tuning Manager.

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

(a) A file system is mounted using LUs whose numbers are

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

0200 (hexadecimal) and greater.

(b) Device status is verified using Hitachi Command Suite Tuning Manager.

The evasion plan: None.

The recovery plan: None.

17) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 02-02-00-00

The phenomenon: During data writing from an NFS share to a file system, the OS is rebooted.

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

(a) "1" is set for wan_optimization by nfsoptset command.

(b) Data is written from a NFS share to file system.

(c) An NFS client cuts a TCP session.

The evasion plan: Set "0" for wan_optimization by running nfsoptset command.

The recovery plan: Cluster model:

Perform failover for the resource group or Virtual Server.

Single node or VM appliance model:

No action is necessary.

18) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 03-01-00-00

The phenomenon: OS is rebooted.

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

(a) NFS protocol version 4 is enabled on HDI.

(b) From a client, NFS share is mounted with NFS protocol version 4.

(c) The above client performs an operation with an operation number exceeding the range specified by NFS protocol version 4.

The evasion plan: Do not use NFS protocol version 4.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

The recovery plan: None.

19) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 02-01-00-00

The phenomenon: If a device, such as a repeater, is attacked by a malicious third party, an arbitrary file is edited on the [Edit System File] page.

The condition: It occurs when a path to a system file selected on the [Edit System File] page is edited in the communication path from a management console to HDI.

The evasion plan: There is no temporary circumvention available.
To prevent files from being edited during communication, do GUI operations of HDI in a closed network (LAN) as much as possible.

The recovery plan: If a system setting information file stored before the system file is edited is available, newly install the OS, and then restore the system setting information.
If the system setting information file stored before the system file is edited is not available, newly install the OS, set all items again. For the user data, create a file system, and then restore the data from a backup.

20) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 3.2.1-00

The phenomenon: Files on HDI cannot be read.

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

(a) The cache residency function is enabled.

(b) The size of cache residency target files exceeds 2,147,483,647 bytes.

(c) The cache residency target files are stubbed.

(files are stubbed by arcrestore command or files are stubbed before cache residency is set)

The evasion plan: Do not set the cache residency function for files whose size exceeds 2,147,483,647 bytes.
(Disable the cache residency function, or set the maximum size for the cache residency policy)

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

The recovery plan: For files that are not updated after the problem occurs, the data can be restored from HCP by taking all the actions below.

(a) Disable the cache residency function.

(a-1) Disabling the function per file system

sudo arcresidentpolicydel --file-system file system name

(a-2) Disabling the function for the entire system

sudo arcresidentctl --report disable

(b) Perform migration.

(c) Create the file system again.

(d) Run arcrestore command.

For files that are updated after the problem occurs, copy the files from the past version directory to restore them, but if the retention period of past versions expires or past versions are not kept by the setting, files cannot be restored.

21) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 6.1.1-03

The phenomenon: When a migration result list is downloaded, KAQM0341-E occurs. After that migration operations are not performed for a while.

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

(a) Downloading with [List of successful migrations] selected in [Download Report] dialog

Assuming that a file path has 256 characters, there are 50,000 or more successfully migrated files and directories.

(b) Download with [List of failed migrations] selected in [Download Report] dialog

Assuming that a file path has 256 characters, there are 18,000 or more migration failed files and directories.

The evasion plan: Redirect the output of arcmigresult command to a file.

The recovery plan: Migration operations can be performed after approximately 10 minutes after the error. To download the migration result list, take the action of temporary circumvention.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

22) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 02-01-00-00

The phenomenon: If a log file in a DB is bloated, which weighs on a system LU, accesses to the file system are disabled until the bloated log file is overwritten by a log rotate.

The condition: It may occur if the usage frequency of single node GUI or API is high.

The evasion plan: None.

The recovery plan: None.

23) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 3.2.1-00

The phenomenon: When arcresidentresult command is run, Pinned capacity is displayed smaller than the actual.

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

(a) The cache residency function is enabled.

(b) Cache residency target files are stubbed.

(For example, a file is restored by arcrestore command, or a file has been stubbed before the cache residency is set)

(c) After the cache residency processing runs, arcresidentresult command is run.

The evasion plan: None.

The recovery plan: The value is recovered at the next cache residency processing. The cache residency processing runs at 00:00 everyday. The completion date of the cache residency processing can be confirmed by "As of" that is a display item of arcresidentresult command.

24) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 6.1.1-00

The phenomenon: When some private commands are run, operations outside the functioning range of the commands are wrongly enabled.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

The condition: It occurs when some private commands are run.

The evasion plan: None.

The recovery plan: None.

25) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-02

Affected version: 02-02-01-00

The phenomenon: The common vulnerability with identifiers below may cause adverse impact.

CVE-2018-2633/CVE-2018-2582/CVE-2018-2618/

CVE-2018-2629/CVE-2018-2657/CVE-2018-2599/

CVE-2018-2678/CVE-2018-2663/CVE-2018-2579/

CVE-2017-3736

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

The evasion plan: None.

The recovery plan: None.

26) Following defect has been fixed by Hitachi Data Ingestor 6.4.6-03

Affected version: 5.0.1-00

The phenomenon: Accesses to an NFS share are disabled.

The condition: It occurs when NFS shares are mounted 1005 times or more in total from an NFS client using NFSv2 after starting the HDI OS or restarting an NFS service.

The evasion plan: Do not use NFSv2.

The recovery plan: Restart the NFS service.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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 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 7. 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	

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

Port numbers	Single node model	Cluster model	Service	Note
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	
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	

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

Port numbers	Single node model	Cluster model	Service	Note
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 8. 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

Copyrights and licenses

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.

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

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

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

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

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

27) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
28) 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, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or 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.

© 2011, 2019 Hitachi, Ltd., Hitachi Vantara Corporation. All rights reserved.