Hitachi Data Ingestor

6.4.8-00

SSH Key Exchange Algorithm Feature Supplement

This document describes and provides instructions for the SSH Key Exchange Algorithm feature of the Hitachi Data Ingestor (HDI) software.

MK-90HDI061-01
September 2020

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

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

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

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

1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and

2) Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

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

Contents

Preface 5

Intended Audience 5
Product Version 5
Accessing Product Documentation 5
Getting Help 5
Comments 6

Purpose 7

Prerequisite 9

Applicable Version 9
Prerequisite Products 9
Prerequisite System Configuration 9
Related Manuals 9

Overview 11

Setting feature for SSH key exchange algorithm 11

Operational Notes 13

Operation Procedure 15

Procedure to refer the setting of SSH key exchange algorithm setting feature 15
Procedure to enable the setting of SSH key exchange algorithm 'diffie-hellman-group1-sha1' 17
Procedure to disable the setting of SSH key exchange algorithm 'diffie-hellman-group1-sha1' 17

Command Specification.. 19

sshconflist (Referring the setting of SSH key exchange algorithm setting feature)....19
sshconfset (Setting of SSH key exchange algorithm) 20

Message reference 22

Message ID beginning with KAQG53..22

Preface

This document describes and provides instructions for the SSH Key Exchange Algorithm feature of the Hitachi Data Ingestor (HDI) software.

Please read this document carefully to understand how to use this feature, and maintain a copy for reference purposes.

Intended Audience

This document is intended for system administrators, Hitachi Vantara representatives, and authorized service providers who are involved in installing, configuring, and using the Hitachi Data Ingestor (HDI) software.

This document assumes the user is familiar with the Hitachi Data Ingestor software.

Product Version

This document revision applies to Hitachi Data Ingestor version 6.4.7-00 or later.

Accessing Product Documentation

Product user documentation is available on Hitachi Vantara Support Connect: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting Help

Hitachi 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 Hitachi Vantara 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.

Comments

Please send us your comments on this document: doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you!

1

Purpose

The setting feature for SSH key exchange algorithm is a function to set key exchange algorithm to be available between the HDI and clients when the client accesses to the HDI using SSH protocol.

2

Prerequisite

Applicable Version

This feature is applicable for Hitachi Data Ingestor 6.4.7-00 or later.

Prerequisite Products

No prerequisite products are required to use this feature.

Prerequisite System Configuration

This feature is executable on the physical node in cluster and single node configuration.

Related Manuals

Related Manuals are listed as follows. Please refer to them as needed.

#	Category	Manual Name
1	User's Guide	Hitachi Data Ingestor Installation and Configuration Guide
2		Hitachi Data Ingestor Cluster Administrator's Guide / Single Node Administrator's Guide
3		Hitachi Data Ingestor CLI Administrator's Guide
4		Hitachi Data Ingestor Error Codes
5		Hitachi Data Ingestor Cluster Troubleshooting Guide / Single Node Troubleshooting Guide

3

Overview

This chapter describes the summary of the setting feature for SSH key exchange algorithm.

Setting feature for SSH key exchange algorithm

This feature is a function to set SSH key exchange algorithm to be used in the SSH communication between HDI and clients.
In versions HDI6.4.8-00 or later, the editable setting by this feature is as follows.

- SSH key exchange algorithm 'diffie-hellman-group1-sha1' to be set enable or disable
- SSH key exchange algorithm 'diffie-hellman-group-exchange-sha1' to be set enable or disable

In versions earlier than HDI6.4.8-00, the editable setting by this feature is as follows.

- SSH key exchange algorithm 'diffie-hellman-group1-sha1' to be set enable or disable

In versions earlier than HDI6.4.8-00, the SSH key exchange algorithm 'diffie-hellman-group1-sha1' and 'diffie-hellman-group-exchange-sha1' are set to enable as default.

If you want to change the setting to disable, refer '5. Operation Procedure', and perform the setting change.

4

Operational Notes

1. In versions earlier than HDI6.4.8-00, the SSH key exchange algorithm setting updated by this feature only applies for the SSH communication that had been started after setting change is completed. It does not apply for the SSH communication already connected before setting change is completed.
2. The SSH key exchange algorithm setting changed by this feature only applies for the SSH communication targeted to the node the setting change is performed on. If you want to set the same setting to both of the nodes, perform the setting change on both nodes.

5

Operation Procedure

This chapter describes how to set and refer the settings of SSH key exchange algorithm.

Procedure to refer the setting of SSH key exchange algorithm setting feature

This section explains how to refer the setting of SSH key exchange algorithm.

(1) Log in targeted to the management IP address of the node that settings to be referred by using nasroot account and ssh protocol.

(2) Execute the sshconflist command to refer the settings.
In case of versions HDI6.4.8-00 or later

```
(a) Result in the case key exchange algorithm 'diffie-hellman-group1-sha1’
    and ’diffie-hellman-group-exchange-sha1’ are enable
$ sudo sshconflist
SSH key exchange algorithm
  diffie-hellman-group1-sha1 : on
  diffie-hellman-group-exchange-sha1 : on
$


(b) Result in the case key exchange algorithm 'diffie-hellman-group1-sha1’
    and ’diffie-hellman-group-exchange-sha1’ are disable
$ sudo sshconflist
SSH key exchange algorithm
  diffie-hellman-group1-sha1 : off
  diffie-hellman-group-exchange-sha1 : off
$
```

In case of versions earlier than HDI6.4.8-00

```
(a) Result in the case key exchange algorithm 'diffie-hellman-group1-sha1’ is
    enable
$ sudo sshconflist
SSH key exchange algorithm
  diffie-hellman-group1-sha1 : on
$

(b) Result in the case key exchange algorithm 'diffie-hellman-group1-sha1’ is
    disable
$ sudo sshconflist
SSH key exchange algorithm
  diffie-hellman-group1-sha1 : off
$
```

(3) Log out from the node.

Procedure to enable the setting of SSH key exchange algorithm 'diffie-hellman-group1-sha1'

This section explains how to enable the setting of SSH key exchange algorithm.

(1) Log in targeted to the management IP address of the node that settings to be set by using nasroot account and ssh protocol.

(2) Execute the sshconfset command to change the settings.

```
$ sudo sshconfset --kexdhgp1sha1 on
$
```

(3) Log out from the node.

(4) In versions HDI6.4.8-00 or later, reboot the OS of the target node to reflect the settings.
In versions earlier than HDI6.4.8-00, reboot is not necessary.

(5) Perform the steps from (1) to (4) on another node.

Procedure to disable the setting of SSH key exchange algorithm 'diffie-hellman-group1-sha1'

This section explains how to disable the setting of SSH key exchange algorithm.

(1) Log in targeted to the management IP address of the node that settings to be set by using nasroot account and ssh protocol.

(2) Execute the sshconfset command to change the settings.

```
$ sudo sshconfset --kexdhgp1sha1 off
$
```

(3) Log out from the node.

(4) In versions HDI6.4.8-00 or later, reboot the OS of the target node to reflect the settings.
In versions earlier than HDI6.4.8-00, reboot is not necessary.

(5) Perform the steps from (1) to (4) on another node.

Procedure to enable the setting of SSH key exchange algorithm 'diffie-hellman-group-exchange-sha1'

This section explains how to enable the setting of SSH key exchange algorithm.

(1) Log in targeted to the management IP address of the node that settings to be set by using nasroot account and ssh protocol.

(2) Execute the sshconfset command to change the settings.

```
$ sudo sshconfset --kexdhgpexcsha1 on
$
```

(3) Reboot the OS of the target node to reflect the settings.

(4) Perform the steps from (1) to (3) on another node.

Procedure to disable the setting of SSH key exchange algorithm 'diffie-hellman-group-exchange-sha1'

This section explains how to disable the setting of SSH key exchange algorithm.

(1) Log in targeted to the management IP address of the node that settings to be set by using nasroot account and ssh protocol.

(2) Execute the sshconfset command to change the settings.

```
$ sudo sshconfset --kexdhgpexcsha1 off
$
```

(3) Reboot the OS of the target node to reflect the settings.

(4) Perform the steps from (1) to (3) on another node.

6

Command Specification

sshconflist (Referring the setting of SSH key exchange algorithm setting feature)

Synopsis

```
sshconflist
sshconflist -h
```

Description

This command displays the setting of SSH key exchange algorithm set to the node.

Options and arguments

-h

Show usage of this command.

Displayed information

This command displays the setting of SSH key exchange algorithm as follows.

In versions HDI 6.4.8-00 or later
In the case key exchange algorithm 'diffie-hellman-group1-sha1' and 'diffie-hellman-group-exchange-sha1' are enable

```
SSH key exchange algorithm
   diffie-hellman-group1-sha1 : on
   diffie-hellman-group-exchange-sha1 : on
```

In the case key exchange algorithm 'diffie-hellman-group1-sha1' and 'diffie-hellman-group-exchange-sha1' are disable

```
SSH key exchange algorithm
   diffie-hellman-group1-sha1 : off
   diffie-hellman-group-exchange-sha1 : off
```

In versions earlier than HDI 6.4.8-00
In the case key exchange algorithm 'diffie-hellman-group1-sha1' is enable

```
SSH key exchange algorithm
   diffie-hellman-group1-sha1 : on
```

In the case key exchange algorithm 'diffie-hellman-group1-sha1' is disable

```
SSH key exchange algorithm
   diffie-hellman-group1-sha1 : off
```

Return values

Return value of sshconflist

Return value	Descriptions
0	Normal termination
1	The specified value might not be appropriate or the command is specified in an incorrect format. Correct the format, and then retry the operation.
99	The system error has been occurred. Collect all log data and then contact maintenance personnel.

Example

```
$ sudo sshconflist
SSH key exchange algorithm
   diffie-hellman-group1-sha1 : on
```

sshconfset (Setting of SSH key exchange algorithm)

Synopsis

```
sshconfset --kexdhgp1sha1 {on | off}
sshconfset --kexdhgpexcsha1 {on | off}
sshconfset -h
```

Description

This command set the setting of SSH key exchange algorithm to the node.

Options and arguments

--kexdhgp1sha1 {on | off}

Change the setting of SSH key exchange algorithm 'diffie-hellman-group1-sha1' into enable(on), or disable(off).

--kexdhgpexcsha1 {on | off}

Change the setting of SSH key exchange algorithm 'diffie-hellman-group-exchange-sha1' into enable(on), or disable(off).

Note: This argument can not be specified in versions earlier than HDI6.4.8-00.

-h

Show usage of this command.

Displayed information

Nothing is displayed.

Return values

Return value of sshconfset

Return value	Descriptions

0	Normal termination
1	The specified value might not be appropriate or the command is specified in an incorrect format. Correct the format, and then retry the operation.
99	The system error has been occurred. Collect all log data and then contact maintenance personnel.

Example

```
$ sudo sshconfset --kexdhgp1sha1 off
```

7

Message reference

Message ID beginning with KAQG53

Message ID	Message	Description and Action
KAQG53009-I	Usage: *command-syntax*	This message displays the syntax of a command. (O) No action is required.
KAQG53010-E	An invalid parameter is specified. (details = *details*)	An invalid parameter is specified. (O) Specify valid parameters according to the Help.
KAQG53015-E	An internal error occurred. (details = *details*)	A system error occurred. (O) Collect all log data, and then contact maintenance personnel.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact