Hitachi Ops Center Administrator

Troubleshooting Guide

**© 2024 Hitachi Vantara, Ltd. All rights reserved.**

This guide must not be used for any purposes other than those referred to in this guide. No part of the contents of this guide may be reproduced or transmitted in any form or by any means without the written permission of Hitachi Vantara, Ltd.

Preface

The Hitachi Ops Center Administrator Troubleshooting Guide describes instructions for field and support engineers to check failure status and to isolate the failure cause. We expect that this guide will lighten the burden on field and support engineers, and will assist them in taking swift troubleshooting action.

When reading the HPE OEM version, see "Appendix A-1"

Revision Level

|  |  |  |  |
| --- | --- | --- | --- |
| No | Version | Description | Date |
| 1 | 10.2.0 | Hitachi Ops Center Administrator Trouble shooting Guide first version | 2020/04/01 |
| 2 | 10.3.1 | 2.2.8 How to initialize service account password has been added. | 2020/07/01 |
| 3 | 10.5.0 | 2.2.9 How to change Java heap size of App service has been added. | 2020/09/10 |
| 4 | 10.5.1 | Following items have been added.  2.2.10 How to confirm start of CCI container  2.2.11 How to change automatic refresh interval  2.2.12 How to delete data of Elasticsearch | 2020/11/25 |
| 5 | 10.6.0 | 2.2.13 How to change the maximum number of simultaneous executable automatic refresh | 2021/1/18 |
| 6 | 10.6.1 | None | 2021/4/14 |
| 7 | 10.7.0 | 2.2.6 How to expand Root filesystem in OVF environment, when Root filesystem is full has been modified.  Following items have been added.  2.2.14 How to change the number of simultaneous executable REST API (10.6.1 or later)  2.2.15 Recovery steps for read-only status of Elasticsearch | 2021/07/13 |
| 8 | 10.8.0 | Add Podman support  Following items have been added  2.2.16 How to change the time out value of MariaDB  2.2.17 How to change the time out value of Command Control Interface command execution | 2021/09/16 |
| 9 | 10.8.1 | Restart command of podman container has been changed in 2.2.17  Following items have been added  2.2.10 Added extra parameters "-s SVP" or "-s GUM" are added to podman run command lines and podman run command lines.  2.2.18 Added new section to describe how to recover volume migration when Ops Center Administrator is restarted.  2.2.19 How to change the wait time of HORCM instance start for CLI container | 2022/01/13 |
| 10 | 10.8.2 | 2.2.9 Changed the method to change java heap memory | 2022/4/18 |
| 11 | 10.9.0 | 2.2.12 Added job data exporting/importing steps and revised overall.  2.2.15 Add an example of Grizzly log.  2.2.18 step 13 Add the note that this step is only required on Ops Center Administrator 10.7.0 or earlier. | 2022/09/22 |
| 12 | 10.9.1 | 2.2.9 Added the description of the supported version for the rainier-memory-settings command.  2.2.15 Added the description about how to check messages.  2.2.18 Added a note for searching log files on Administrator version 10.9.1 or later. | 2023/01/23 |
| 13 | 10.9.2 | None | 2023/04/18 |
| 14 | 10.9.3 | Added 2.2.21, 2.2.22 | 2023/07/07 |
| 15 | 11.0.0 | 2.2.23 How to initialize VAM sysadmin account password has been added. | 2023/12/19 |
| 16 | 11.0.1 | Added a note that file containers have been deprecated in 1.3.  Added steps 8 and 11 to 2.2.18. | 2023/03/25 |
| 17 | 11.0.2 | 2.2.24 added the steps to take when Create a migration pair fails.  2.2.25 added the steps to take when docker related files become corrupted. | 2024/05/27 |
| 18 | 11.0.3 | 2.2.25 added the steps for the podman environment.  Added 2.2.26. | 2024/10/04 |
| 19 | 11.0.4 | 2.2.10, 2.2.15, 2.2.20, 2.2.23, 2.2.25, and 2.2.26 added the steps for versions 11.0.4 and above.  2.2.10 reviewed the target storage array in step 2.  2.2.13, 2.2.14, and 2.2.17 reviewed the steps for restarting the containers.  2.2.21 reviewed the target files for deletion in step 2. | 2025/02/26 |

**Contents**

[1. Overview 7](#_Toc178929423)

[1.1 Scope of this manual 7](#_Toc178929424)

[1.2 Glossary 7](#_Toc178929425)

[1.3 Prerequisite knowledge 7](#_Toc178929426)

[1.4Related documentation 7](#_Toc178929427)

[2. Troubleshooting Procedures 8](#_Toc178929428)

[2.1 Types of troubleshooting 8](#_Toc178929429)

[2.2 Troubleshooting Procedure 8](#_Toc178929430)

[2.2.1 When a job does not progress for a while 8](#_Toc178929431)

[2.2.2 When IP address duplicates with customer environment in OVF version 8](#_Toc178929432)

[2.2.3 How to register self signed SSL certification 9](#_Toc178929433)

[2.2.4 How to delete hardware alert (In case disk alert) 10](#_Toc178929434)

[2.2.5 How to delete hardware alert (In case other than disk alert) 12](#_Toc178929435)

[2.2.6 How to expand Root filesystem in OVF environment, when Root filesystem is full 13](#_Toc178929436)

[2.2.7 How to initialize default user(sysadmin) password. 16](#_Toc178929437)

[2.2.8 How to initialize service account password 18](#_Toc178929438)

[2.2.9 How to change Java heap size of App service 19](#_Toc178929439)

[2.2.10 How to confirm start of CCI container 19](#_Toc178929440)

[2.2.11 How to change automatic refresh interval 21](#_Toc178929441)

[2.2.12 How to delete data of Elasticsearch 21](#_Toc178929442)

[2.2.13 How to change the maximum number of simultaneous executable automatic refresh 24](#_Toc178929443)

[2.2.14 How to change the number of simultaneous executable REST API (10.6.1 or later) 24](#_Toc178929444)

[2.2.15 Recovery steps for read-only status of Elasticsearch 25](#_Toc178929445)

[2.2.16 How to change the time out value of MariaDB 27](#_Toc178929446)

[2.2.17 How to change the time out value of Command Control Interface command execution 28](#_Toc178929447)

[2.2.18 How to recover volume migration when Ops Center Administrator is restarted 28](#_Toc178929448)

[2.2.19 How to change the wait time of HORCM instance start for CLI container 34](#_Toc178929449)

[2.2.20 How to delete a storage system manually when the storage system could not be deleted from the GUI 35](#_Toc178929450)

[2.2.21 How to forcibly uninstall Administrator on a Podman environment 38](#_Toc178929451)

[2.2.22 How to delete a HA replication group without changing the configuration on Protector 39](#_Toc178929452)

[2.2.23 How to initialize VAM sysadmin account password 40](#_Toc178929453)

[2.2.24 When The "Create a migration pair" fails at “The volume xx was not found.” 41](#_Toc178929454)

[2.2.25 If the " Error: .ini file does not include supervisord section " is output in the rainier log 41](#_Toc178929455)

[2.2.26 How to replace a certificate using the CLI 48](#_Toc178929456)

[3. Necessary Data for Troubleshooting 50](#_Toc178929457)

[3.1 Information required for investigation 50](#_Toc178929458)

[3.2 Information collection method 50](#_Toc178929459)

[3.2.1 When log can be collected from VAM(earlier than 10.0.0) 50](#_Toc178929460)

[3.2.2 When log cannot be collected from VAM(earlier than 10.0.0) 50](#_Toc178929461)

[3.2.3 In case 10.0.0 or later 50](#_Toc178929462)

[Appendix 51](#_Toc178929463)

[A-1 For the HPE OEM version, substitute the following terms as indicated 51](#_Toc178929464)

# Overview

## 1.1 Scope of this manual

3SC(CTSC/ESC/APSC), Hitachi Vantara, Hewlett Packard Enterprise

## 1.2 Glossary

Acronyms and abbreviations used in this manual are shown below.

|  |  |
| --- | --- |
| Acronyms and Abbreviations | Formal Nomenclature |
| Administrator | Hitachi Ops Center Administrator |
| GUI | Graphical User Interface |
| HAS | Hitachi Storage Advisor |
| OS | Operating System |
| OVF | Open Virtualization Format |
| VAM | Virtual Appliance Manager |

## 1.3 Prerequisite knowledge

- Knowledge of Administrator

- Knowledge of Docker or Podman

- Knowledge of OS(Linux)

- Knowledge of Web browser

- Knowledge of SAN

- Knowledge of storage

Note: From version 11.0.1, the file container has been deprecated, and the GUI and API for file storage management are no longer supported.

## 1.4Related documentation

- Hitachi Ops Center Administrator Getting Started Guide

- Hitachi Ops Center Administrator User Guide

- Hitachi Ops Center Administrator High Availability User Guide

- Hitachi Ops Center Administrator REST API Reference Guide

# 2. Troubleshooting Procedures

## 2.1 Types of troubleshooting

Troubleshooting flow

See Hitachi Ops Center Administrator LogAnalysisGuide 3.1 Log analysis flow of troubleshooting.

## 2.2 Troubleshooting Procedure

### 2.2.1 When a job does not progress for a while

When storage cannot be locked in the task, task does not progress. Retry of lock is executed as below.

1Minutes/time \* 720 times=720Minutes(12hour)

You can identify lock waiting by following log. "xyz times so far" is retry number.

Block | 2019-10-22T23:30:12,699 WARN [REST\_API:5nYukU:WJgXjw][http-nio-8082-exec-7104] c.h.b.s.d.b.s.c.c.CciLockingCommand --- CciLockingCommand:Resource [50343-]: The resource that you specified to lock or unlock has already been used by another user., Tried 392 times so far.

Log of lock execution and failure output in cli\_xyz.log as below.

2019/10/22 23:28:12 [Start] command:[ [echo | read-lock raidcom lock resource -time 60 -IM0] ]

2019/10/22 23:29:12 [error] command [echo | read-lock raidcom lock resource -time 60 -IM0] failed!

2019/10/22 23:29:12 [End] command:[ [echo | read-lock raidcom lock resource -time 60 -IM0] ],Took : 1m0.224737984s

When you identify lock, release storage lock, then task retry succeeds and ends normally.

### 2.2.2 When IP address duplicates with customer environment in OVF version

Default network address is below.

3.4.0, 3.4.1 : 192.168.50.0/16

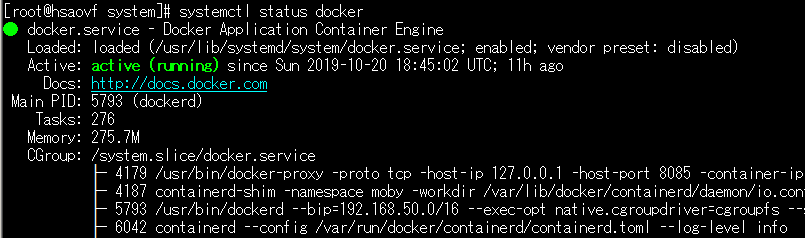
10.0.0 : 192.168.50.0/22

10.0.0-01 or later: 192.168.50.1/25

When above network address duplicates with customer network address, change network address of docker by steps below.

1. Login to the machine by root user that is installed administator
2. Verify IP address of docker

#systemctl status docker



1. Stop docker service

#systemctl stop docker

1. Change IP address of Docker

Open following file by text editor

/usr/lib/systemd/system/docker.service

Change following part of IP address

ExecStart=/usr/bin/dockerd --bip=192.168.50.0/16 \

1. Reload setting file

# systemctl daemon-reload

1. Restart docker service

#systemctl start docker

1. Check setting

#systemctl status docker

### 2.2.3 How to register self signed SSL certification

1. Execute step1 to step6 of "Generating and installing a signed SSL certificate" in Getting Started Guide.
2. Instead of Step7, execute following command to create self signed certification.

#openssl x509 -in server.csr -days <duration> -req -signkey server.key > server.crt

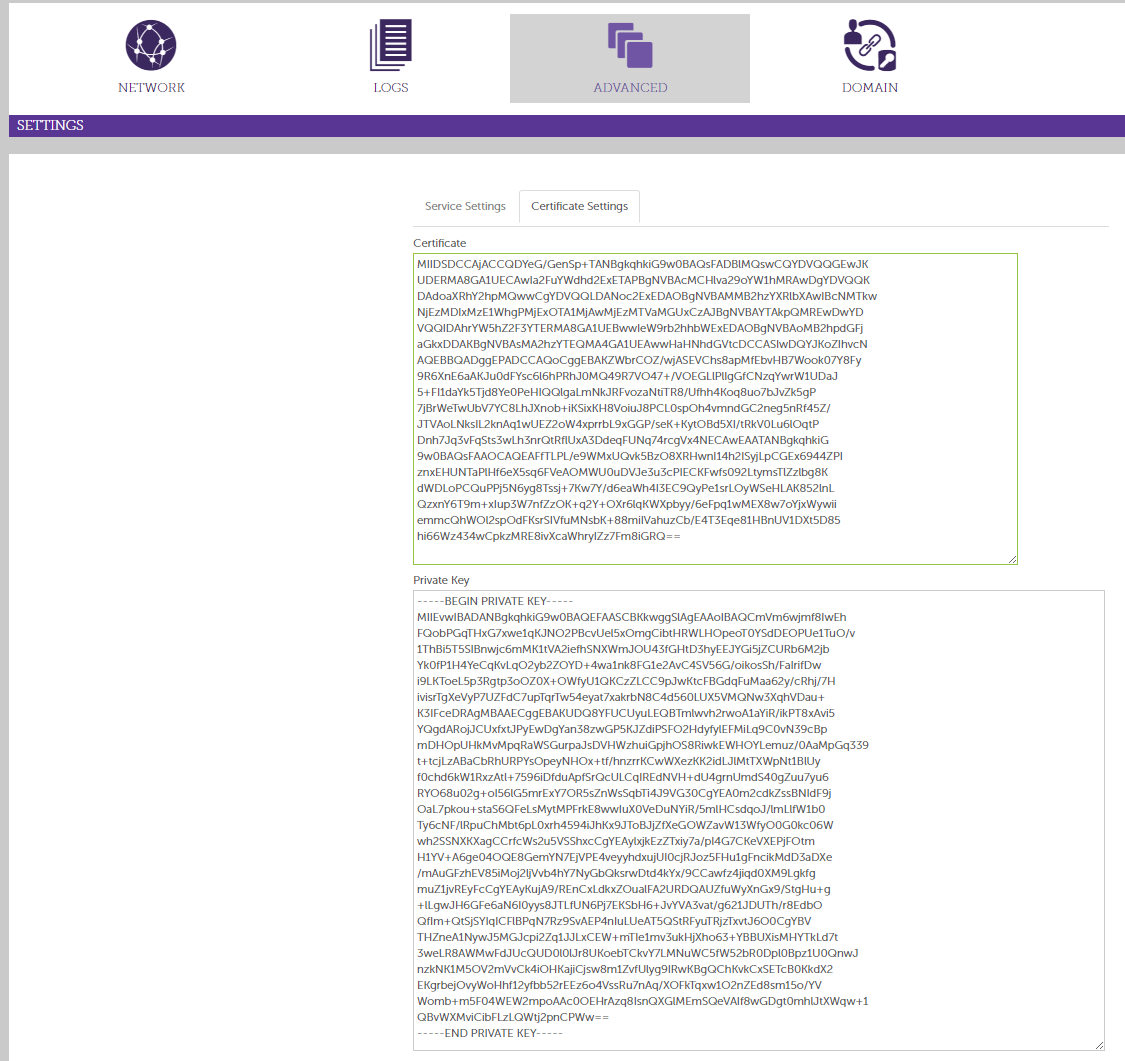
Note : For <duration>, specify number of days to expire.

1. Open VAM GUI

3-1 Copy server.crt content into "Certificate" area without delimiter.

3-2 Copy server.key content into "Private Key" area with delimiter.

Example is below.



1. Click on "submit" and wait for 5 minutes.

Note : If no message is shown after submit, registration is success.

1. Launch Hitachi Ops Center Administrator UI and verify ssl certificate from browser.

### 2.2.4 How to delete hardware alert (In case disk alert)

1. Collect information of alert

* 1. Login to Administrator and check alert that you would like to delete
  2. Collect log information (This is investigation of cause)
  3. Take backup from VAM
  4. Check container ID of mariadb

[For a Docker environment]

#docker ps | grep mariadb

[For a Podman environment]

#podman ps | grep mariadb

* 1. Connect mariadb container that is verified in Step1-4

[For a Docker environment]

#docker exec -it <container id of mariadb> bash

[For a Podman environment]

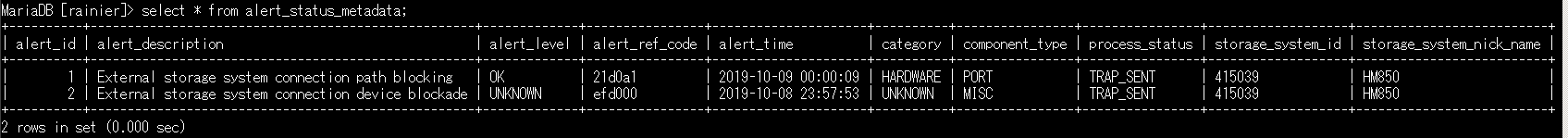
#podman exec -it <container id of mariadb> bash

* 1. After connecting to Mariadb, get alert information by steps below

#mysql

1. MariaDB[(none)]>use rainier
2. MariaDB[(rainier)]>select \* from alert\_status\_metadata;
3. MariaDB[(rainier)]>select \* from alert\_drive\_mapping;
4. MariaDB[(rainier)]>select \* from disk\_alert\_status\_metadata;

Result example of select \* from alert\_status\_metadata;



2. Find deletion target

* 1. Find alert\_id of deletion target from result of Step1-6 step b
  2. Check alert\_id that is find Step2-1 from result of Step1-6 step c, if there is matching alert\_id, notes drive\_alert\_id of matched data.

2-3 Check whether drive\_alert\_id is related to other than deletion target alert\_id or not from result of Step1-6 step c.

3. Delete alert

* 1. Execute following command to delete alert from Mariadb. (You can specify all alert\_id in ID\_x part)

MariaDB[(rainier)]>delete from alert\_status\_metadata where alert\_id IN('ID\_1', 'ID\_2', ..);

MariaDB[(rainier)]>delete from alert\_drive\_mapping where alert\_id IN('ID\_1', 'ID\_2', ..);

* 1. If the result of Step2-3 is not related to any alert\_id, execute following. (You can specify all alert\_id in ID\_x part)

MariaDB[(rainier)]>delete from disk\_alert\_status\_metadata where drive\_alert\_id IN('ID\_1', 'ID\_2',..)

### 2.2.5 How to delete hardware alert (In case other than disk alert)

1. Collect information of alert

* 1. Login to Administrator and check alert that you would like to delete
  2. Collect log information (This is investigation of cause)
  3. Take backup from VAM
  4. Check container ID of mariadb

[For a Docker environment]

#docker ps | grep mariadb

[For a Podman environment]

#podman ps | grep mariadb

* 1. Connect mariadb container that is verified in Step1-4

[For a Docker environment]

#docker exec -it <container id of mariadb> bash

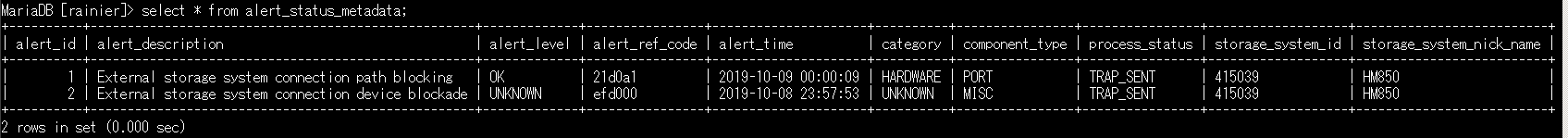
[For a Podman environment]

#podman exec -it <container id of mariadb> bash

* 1. After connecting to Mariadb, get alert information by steps below

#mysql

1. MariaDB[(none)]>use rainier
2. MariaDB[(rainier)]>select \* from alert\_status\_metadata;
3. MariaDB[(rainier)]>select \* from alert\_component\_mapping;
4. MariaDB[(rainier)]>select \* from component\_alert\_status\_metadata;

Result example of select \* from alert\_status\_metadata;

2. Find deletion target

* 1. Find alert\_id of deletion target from result of Step1-6 step b
  2. Check alert\_id that is find Step2-1 from result of Step1-6 step c, if there is matching alert\_id, notes component\_alert\_id of matched data

3. Delete alert

* 1. Execute following command to delete alert from Mariadb. (You can specify all alert\_id in ID\_x part)

MariaDB[(rainier)]>delete from alert\_status\_metadata where alert\_id IN('ID\_1', 'ID\_2',..);

MariaDB[(rainier)]>delete from alert\_component\_mapping where alert\_id IN('ID\_1', 'ID\_2',..);

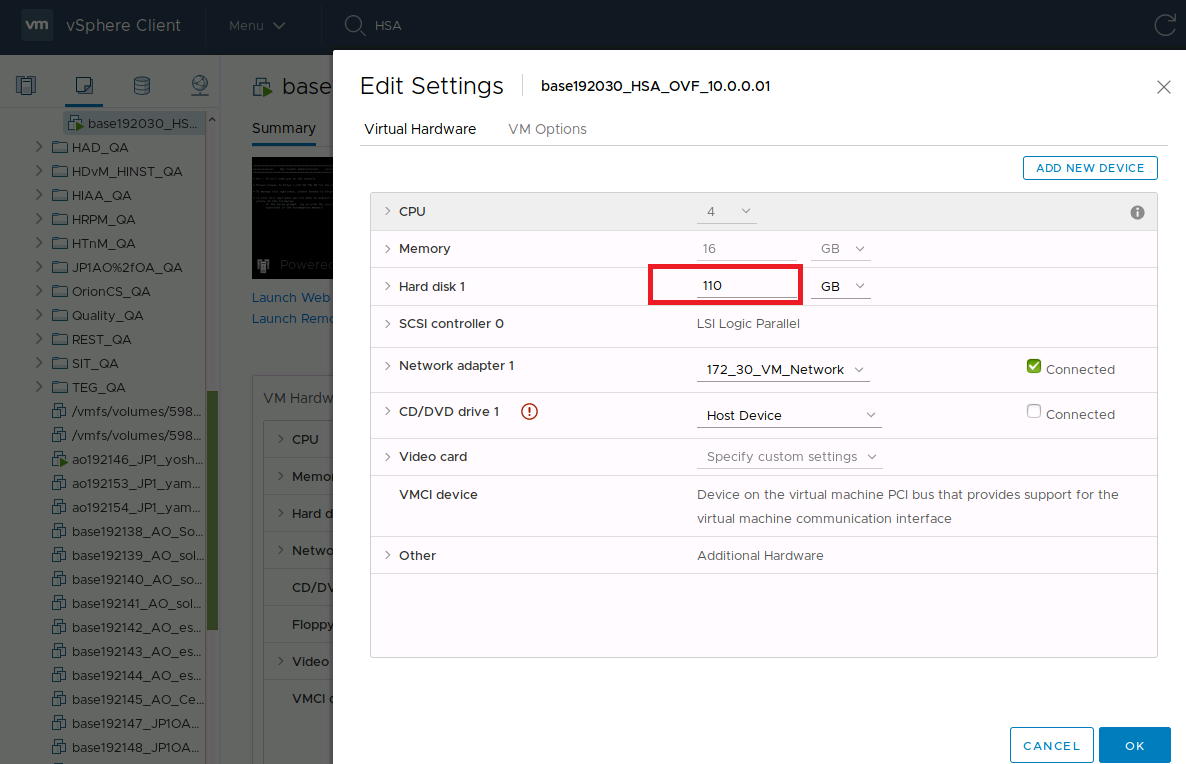
* 1. If the result of Step2-2 is related to alert\_id, execute following. (You can specify all alert\_id in ID\_x part)

MariaDB[(rainier)]>delete from component\_alert\_status\_metadata where component\_alert\_id IN('ID\_1', 'ID\_2',..)

### 2.2.6 How to expand Root filesystem in OVF environment, when Root filesystem is full

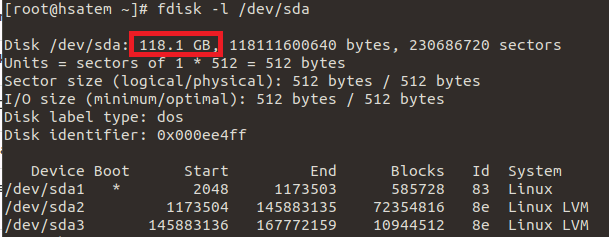
1. Shut down target machine

2. Change capacity of Hard disk 1 from vSphere client, Power on



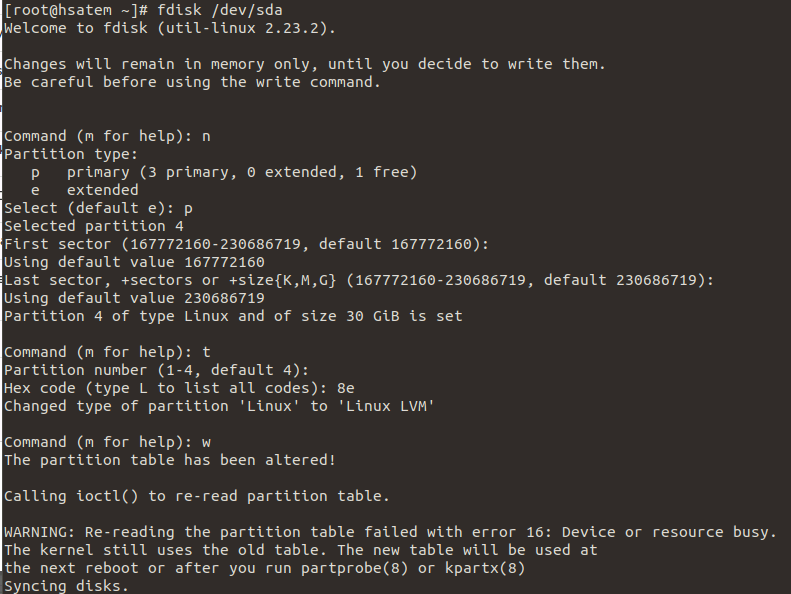
1. Login to server by ssh, then check disk size

#fdisk -l /dev/sda



1. Create partition in expanded part byfdisk /dev/sda of LVM(8e)

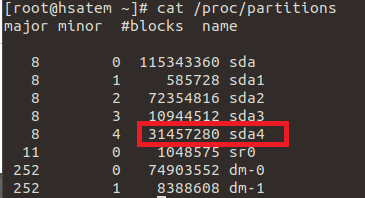
Example of command execution is as below



1. Recognize created partition

#partprobe

Verify result from /proc/partitions file



1. Create PV(Physical Volume) of LVM in created partition



1. Expand VG(Volume Group) by using PV created in Step6

[In case 10.0.0 or later]



[In case 3.4.0/3.4.1]



1. Expand current LV(Logical Volume)

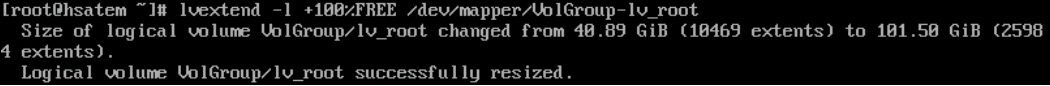
[In case 10.1.2 or later]



[In case 10.0.0 to 10.1.0]

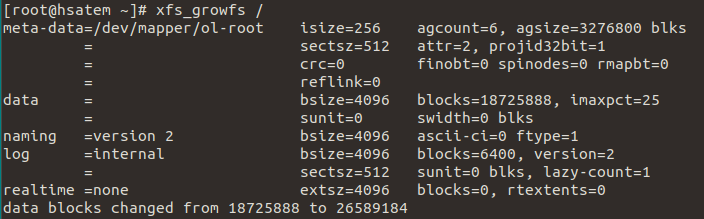


[In case 3.4.0/3.4.1]

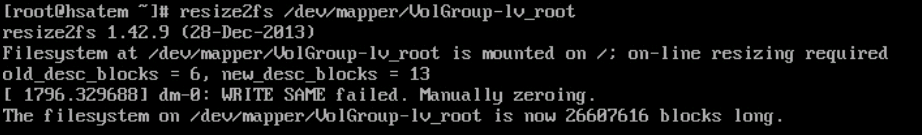


1. Expand filesystem

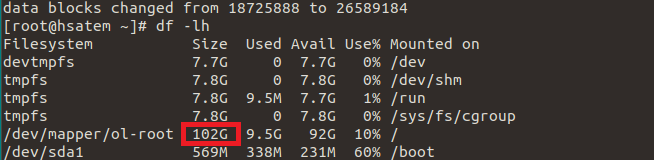
[In case 10.0.0 or later]



[In case 3.4.0/3.4.1]



1. Verify expanded filesystem



### 2.2.7 How to initialize default user(sysadmin) password.

Execute following steps to initialize password.

1. Login to Administrator server by root account
2. Create work directory and change current directory.

# mkdir /change\_password

# cd /change\_password

1. Copy the script for initialization to directory that is created in step 2.

-Script is different between Hitachi Vantara edition and HPE edition. See description below.

-File name : change\_password.sh

4. Change permission of script.

# chmod 755 change\_password.sh

# ./change\_password.sh

[Password initialization script for Hitachi Vantara edition]

[For a Docker environment]

#!/bin/bash

matchApp=$(docker ps --filter="name="mariadb"" -q | xargs)

docker exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

echo "Updating theuser\_tao table with the password change"

docker exec -it $matchApp bash -c "mysql rainier -e \"update account\_domain\_user set password=\\\"sysadmin\\\" where login\_name=\\\"sysadmin\\\"\""

echo "Get the updated output for Account Domain User"

docker exec -it $matchApp bash -c "mysql rainier -e \"select \* from account\_domain\_user\""

echo "Updating the password value to default - sysadmin"

docker exec -it $matchApp bash -c "mysql si -e \"update user\_dao set password=\\\"\\\$2a\\\$10\\\$n59Ltnj2ZaHtSdwzC.WYBe6wr3l2SPtkDS/kA0r87A5MFjZQsCUea\\\" where name IN(\\\"sysadmin\\\")\""

echo "Get User table info"

docker exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

[For a Podman environment]

#!/bin/bash

matchApp=$(podman ps --filter="name="mariadb"" -q | xargs)

podman exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

echo "Updating theuser\_tao table with the password change"

podman exec -it $matchApp bash -c "mysql rainier -e \"update account\_domain\_user set password=\\\"sysadmin\\\" where login\_name=\\\"sysadmin\\\"\""

echo "Get the updated output for Account Domain User"

podman exec -it $matchApp bash -c "mysql rainier -e \"select \* from account\_domain\_user\""

echo "Updating the password value to default - sysadmin"

podman exec -it $matchApp bash -c "mysql si -e \"update user\_dao set password=\\\"\\\$2a\\\$10\\\$n59Ltnj2ZaHtSdwzC.WYBe6wr3l2SPtkDS/kA0r87A5MFjZQsCUea\\\" where name IN(\\\"sysadmin\\\")\""

echo "Get User table info"

podman exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

[Password initialization script for HPE edition]

[For a Docker environment]

#!/bin/bash

matchApp=$(docker ps --filter="name="mariadb"" -q | xargs)

docker exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

echo "Updating theuser\_tao table with the password change"

docker exec -it $matchApp bash -c "mysql rainier -e \"update account\_domain\_user set password=\\\"manager\\\" where login\_name=\\\"system\\\"\""

echo "Get the updated output for Account Domain User"

docker exec -it $matchApp bash -c "mysql rainier -e \"select \* from account\_domain\_user\""

echo "Updating the password value to default - system"

docker exec -it $matchApp bash -c "mysql si -e \"update user\_dao set password=\\\"\\\$2a\\\$10\\\$gpfEKQhwODXicCL2mrhvruhUgJujs/B8IwbE5fzDEYMJ4ane.dSNS\\\" where name IN(\\\"system\\\")\""

echo "Get User table info"

docker exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

[For a Podman environment]

#!/bin/bash

matchApp=$(podman ps --filter="name="mariadb"" -q | xargs)

podman exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

echo "Updating theuser\_tao table with the password change"

podman exec -it $matchApp bash -c "mysql rainier -e \"update account\_domain\_user set password=\\\"manager\\\" where login\_name=\\\"system\\\"\""

echo "Get the updated output for Account Domain User"

podman exec -it $matchApp bash -c "mysql rainier -e \"select \* from account\_domain\_user\""

echo "Updating the password value to default - system"

podman exec -it $matchApp bash -c "mysql si -e \"update user\_dao set password=\\\"\\\$2a\\\$10\\\$gpfEKQhwODXicCL2mrhvruhUgJujs/B8IwbE5fzDEYMJ4ane.dSNS\\\" where name IN(\\\"system\\\")\""

echo "Get User table info"

podman exec -it $matchApp bash -c "mysql si -e \"select \* from user\_dao\""

### 2.2.8 How to initialize service account password

Execute following steps to initialize password.

1. Login to Administrator server by root account
2. Execute following command.

#usermod -p '$6$Nf4KsSiA$GncxHqSVf7a1HWZar1X6cTTv7Qaht0SrM1mcbYJ40hUPENaeVpZkmmDYTi2oqBjBlLGDx5hk4LWRCBT/ybWdP1' service

## 2.2.9 How to change Java heap size of App service

From version 10.8.2 to earlier than 10.9.1, the user can use the rainier-memory-settings command to change the Java heap size. See chapter "Changing the heap memory setting of the java process" for detail.

### 2.2.10 How to confirm start of CCI container

When CCI container takes time to start for onboard, storage onboard fails. In this case, it is possible to check start of CCI container takes time or not by following steps.

1. Do ssh to Administrator (HSA) server with root account.

2. Create CCI container manually with following command.

[VSP G1000, VSP G1500, VSP F1500 and VSP 5000 series]

[For a Docker environment]

#docker run --name cli\_<Serial number>\_2 -e "START\_CCI\_ARGS=-i <SVPip,SVPip> -b HV -s SVP" -d `docker images | grep rdocker:6000/cli | awk '{print $3}'`

example)

#docker run --name cli\_39304\_2 -e "START\_CCI\_ARGS=-i 192.168.0.2,192.168.0.2 -b HV -s SVP" -d `docker images | grep rdocker:6000/cli | awk '{print $3}'

[For a Podman environment and the version is earlier than 11.0.4]

#podman run --name cli\_<Serial number>\_2 -e "START\_CCI\_ARGS=-i <SVPip,SVPip> -b HV -s SVP" -d ` podman images | grep rdocker:6000/cli | awk '{print $3}'`

example)

#podman run --name cli\_39304\_2 -e "START\_CCI\_ARGS=-i 192.168.0.2,192.168.0.2 -b HV -s SVP" -d `podman images | grep rdocker:6000/cli | awk '{print $3}'`

[For a Podman environment and the version is 11.0.4 or later]

#podman run --name cli\_<Serial number>\_2 -e "START\_CCI\_ARGS=-i <SVPip,SVPip> -b HV -s SVP -n <index>" -e "NETWORK\_MODE=<mode>" -v /opt/rainier/settings/port.properties:/opt/config/port.properties:z -v /opt/rainier/container-shared/cli/:/opt/container-shared/cli/:z -d `podman images | grep rdocker:6000/cli | awk '{print $3}'`

Note: For <index> specify the number of storage arrays onboarded to the Administrator.

For <mode> specify the network mode when installing Administrator. Use "host" for host mode and "podman" for bridge mode.

example)

#podman run --name cli\_39304\_2 -e "START\_CCI\_ARGS=-i 192.168.0.2,192.168.0.2 -b HV -s SVP -n 2" -e "NETWORK\_MODE=host" -v /opt/rainier/settings/port.properties:/opt/config/port.properties:z -v /opt/rainier/container-shared/cli/:/opt/container-shared/cli/:z -d `podman images | grep rdocker:6000/cli | awk '{print $3}'`

[VSP E series, VSP Fx00 models, VSP Gx00 models, VSP One Block 20]

[For a Docker environment]

#docker run --name cli\_<Serial number>\_2 -e "START\_CCI\_ARGS=-i <GUMip1,GUMip2> -b HV -s GUM" -d `docker images | grep rdocker:6000/cli | awk '{print $3}'`

example)

#docker run --name cli\_415249\_2 -e "START\_CCI\_ARGS=-i 192.168.0.5,192.168.0.6 -b HV -s GUM" -d `docker images | grep rdocker:6000/cli | awk '{print $3}'

[For a Podman environment and the version is earlier than 11.0.4]

#podman run --name cli\_<Serial number>\_2 -e "START\_CCI\_ARGS=-i <GUMip1,GUMip2> -b HV -s GUM" -d `podman images | grep rdocker:6000/cli | awk '{print $3}'`

example)

#podman run --name cli\_415249\_2 -e "START\_CCI\_ARGS=-i 192.168.0.5,192.168.0.6 -b HV -s GUM" -d `podman images | grep rdocker:6000/cli | awk '{print $3}'`

[For a Podman environment and the version is 11.0.4 or later]

#podman run --name cli\_<Serial number>\_2 -e "START\_CCI\_ARGS=-i <GUMip1,GUMip2> -b HV -s GUM -n <index>" -e "NETWORK\_MODE=<mode>" -v /opt/rainier/settings/port.properties:/opt/config/port.properties:z -v /opt/rainier/container-shared/cli/:/opt/container-shared/cli/:z -d `podman images | grep rdocker:6000/cli | awk '{print $3}'`

Note: For <index> specify the number of storage arrays onboarded to the Administrator.

For <mode> specify the network mode when installing Administrator. Use "host" for host mode and "podman" for bridge mode.

example)

#podman run --name cli\_415249\_2 -e "START\_CCI\_ARGS=-i 192.168.0.5,192.168.0.6 -b HV -s GUM -n 2" -e "NETWORK\_MODE=host" -v /opt/rainier/settings/port.properties:/opt/config/port.properties:z -v /opt/rainier/container-shared/cli/:/opt/container-shared/cli/:z -d `podman images | grep rdocker:6000/cli | awk '{print $3}'`

3. Wait for CCI container starts for 5-10 minutes.

4. Login to CCI container.

[For a Docker environment]

#docker exec -it cli\_<Serial number>\_2 bash

[For a Podman environment]

#podman exec -it cli\_<Serial number>\_2 bash

5. Run following command to collect data.

#raidcom get resource -IM0

This will ask for storage credentials. Please enter and continue. If command succeed, connection is fine and CCI is running.

Note: It may take time to start CCI, so please retry step 5 after 60min.

6. Exit from CCI container.

#exit

7. Collect log files of CCI from following /HORCM/log0 in CCI container

[For a Docker environment]

#docker cp cli\_<Serial number>\_2:HORCM/log0 <destination>

example)

#docker cp cli\_415249\_2:/HORCM/log0 /tmp

[For a Podman environment]

#podman cp cli\_<Serial number>\_2:HORCM/log0 <destination>

example)

#podman cp cli\_415249\_2:/HORCM/log0 /tmp

Note: Collect all logs available in HORCM directory including sub directories.

8. Delete CCI container which is manually created.

[For a Docker environment]

#docker stop cli\_415249\_2

#docker rm cli\_415249\_2

[For a Podman environment]

#podman stop cli\_415249\_2

#podman rm cli\_415249\_2

### 2.2.11 How to change automatic refresh interval

Automatic refresh interval is set 10 minutes as default, but you can change interval by following steps. If user want to decrease load of Administrator server, these steps can be used.

Following example sets 120 minutes for the interval, change value 120 if you would like to set another value. The unit is minute.

1. Do ssh to Administrator (HSA) server with root account.
2. Execute following command.

[For a Docker environment]

#docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '120' where name = 'CacheRefreshDelay';"

[For a Podman environment]

#podman exec -it $(podman ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '120' where name = 'CacheRefreshDelay';"

### 2.2.12 How to delete data of Elasticsearch

When data of Elasticsearch becomes abnormal, it is possible to delete data of Elasticsearch by following steps. Follow an instruction of each support case for execution of this steps.

1. Using the root user account, log in to the Hitachi Storage Advisor server or the Ops Center Administrator server.

2. Export the job data.

If you are using Docker:

# docker exec $(docker ps -aqf "name=hid-grizzly\_1") /infraScripts/export.sh

If you are using Podman:

# podman exec $(podman ps -aqf "name=hid-grizzly\_1") /infraScripts/export.sh

3. Check that the job data files were created.

If you are using Docker:

# docker exec $(docker ps -aqf "name=hid-grizzly\_1") ls /infraScripts/export

If you are using Podman:

# podman exec $(podman ps -aqf "name=hid-grizzly\_1") ls /infraScripts/export

As a result of running the command, if the following three file names are output, the files were created.

- grizzly.properties

- jobs.json

- metadata.json

4. Stop all services.

If you are using Docker:

# docker stop $(docker ps -a | grep rdocker:6000 | awk '{print $1}')

If you are using Podman:

# systemctl stop rainier

5. Delete the data directory of Elasticsearch.

If you are using Docker:

# rm -rf $(docker inspect $(docker ps -aqf "name=data-elasticsearch\_1") | grep -E \"Source\".\*\_data\"\, | sed -e 's/^.\*\/var/\/var/' -e 's/\",/\/nodes/')

If you are using Podman:

# rm -rf $(podman inspect $(podman ps -aqf "name=data-elasticsearch\_1") | grep -E \"Source\".\*\_data\"\, | sed -e 's/^.\*\/var/\/var/' -e 's/\",/\/nodes/')

6. Restart all services.

If you are using Docker:

# docker restart $(docker ps -a | grep rdocker:6000 | awk '{print $1}')

If you are using Podman:

# systemctl restart rainier

7. Wait for the job list to be displayed on the Hitachi Storage Advisor GUI or the Ops Center Administrator GUI.

8. Create a directory for storing the job data files.

If you are using Docker:

# docker exec $(docker ps -aqf "name=hid-grizzly\_1") mkdir -p /infraScripts/import/infra

If you are using Podman:

# podman exec $(podman ps -aqf "name=hid-grizzly\_1") mkdir -p /infraScripts/import/infra

9. Move the job data files.

If you are using Docker:

# docker exec $(docker ps -aqf "name=hid-grizzly\_1") mv /infraScripts/export /infraScripts/import/infra/hid-grizzly

If you are using Podman:

# podman exec $(podman ps -aqf "name=hid-grizzly\_1") mv /infraScripts/export /infraScripts/import/infra/hid-grizzly

10. Import the job data.

If you are using Docker:

# docker exec $(docker ps -aqf "name=hid-grizzly\_1") /infraScripts/import.sh

If you are using Podman:

# podman exec $(podman ps -aqf "name=hid-grizzly\_1") /infraScripts/import.sh

11. Remove the job data files.

If you are using Docker:

# docker exec $(docker ps -aqf "name=hid-grizzly\_1") rm -rf /infraScripts/import

If you are using Podman:

# podman exec $(podman ps -aqf "name=hid-grizzly\_1") rm -rf /infraScripts/import

### 2.2.13 How to change the maximum number of simultaneous executable automatic refresh

The maximum number of simultaneous executable automatic refresh is set 4 as default, but you can decrease the number by following steps. If user want to decrease load of Administrator server, these steps can be used.

Following example sets 2 for the maximum number, change value 2 if you would like to set another value.

1. Do ssh to Administrator (HSA) server with root account.

2. Run the following command:

[For a Docker environment]

docker exec -it $(docker ps -qf "name=mariadb\_1") mysql -D rainier -e "update application\_property set value = '2' where name = 'ThreadsForRefreshingCache';"

[For a Podman environment]

podman exec -it $(podman ps -qf "name=mariadb\_1") mysql -D rainier -e "update application\_property set value = '2' where name = 'ThreadsForRefreshingCache';"

3.Restart all Docker containers on the Ops Center Administrator server.

[For a Docker environment]

docker ps -a | grep rdocker:6000 | docker restart `awk '{print $1}'`

[For a Podman environment]

systemctl restart rainier

### 2.2.14 How to change the number of simultaneous executable REST API (10.6.1 or later)

The default number of simultaneous REST API executions is 8 if the version is below 10.8.2, and 2 if the version is 10.8.2 or above. However, you can decrease the number of simultaneous REST API executions by following these steps. If a user wants to decrease the load on the REST API server, these steps can be used.

Following example sets 2 for the simultaneous number, change value 2 if you would like to set another value.

1. Do ssh to Administrator server with root account.

2. Run the following command.

[For a Docker environment]

docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '2' where name = 'BlockRestApiParallelSize';"

[For a Podman environment]

podman exec -it $(podman ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '2' where name = 'BlockRestApiParallelSize';"

3. Restart all containers on the Ops Center Administrator server.

[For a Docker environment]

docker ps -a | grep rdocker:6000 | docker restart `awk '{print $1}'`

[For a Podman environment]

systemctl restart rainier

### 2.2.15 Recovery steps for read-only status of Elasticsearch

When the usage rate of the file system reaches nearly 100% utilization, all indexes in the Elasticsearch service will be set to read-only and the Administrator server will stop working properly.

(1) If the problem occurred, certain messages appear in some logs.

a) A message that includes "flood stage disk watermark" is output to the Elasticsearch service log.

Example of the log:

[2021-07-13T01:28:50,786][WARN ][o.e.c.r.a.DiskThresholdMonitor] [HID-Production] flood stage disk watermark [95%] exceeded on [jhXPCphNRhuyTLVZNYjQ1Q][HID-Production][/usr/share/elasticsearch/data/nodes/0] free: 1.1gb[3.8%], all indices on this node will be marked read-only

How to find the message: Run one of the following commands. If a message that includes "flood stage disk watermark" is output, the message in quotation was output to the log.

[For a Docker environment]

# docker exec -it $(docker ps -a | grep rdocker:6000/logspout: | awk '{print $1}') /bin/bash -c 'grep " flood stage disk watermark" /var/logs/infra-hid-elasticsearch/\*.log'

[For a Podman environment]

# \_odman exec -it $(\_odman ps -a | grep rdocker:6000/logspout: | awk '{print $1}') /bin/bash -c 'grep " flood stage disk watermark" /var/logs/infra-hid-elasticsearch/\*.log'

b) A message that includes "ClusterBlockException: Blocked by: [FORBIDDEN/*<number>*/index read-only / allow delete (api)]" is output in the Grizzly service log.   
Note: This message might be output for a reason other than this problem.

Example of the log:

2022/07/13 10:07:00.500 Grizzly ERROR at com.hds.hid.infrastructure.jobs.common.aspect.TraceAspect:27 - Exception in com.hds.hid.infrastructure.jobs.service.JobServiceImpl.createJob() with cause = com.hds.hid.infrastructure.common.elasticsearch.exceptions.GeneralElasticSearchException

*(omitted)*

Caused by: org.elasticsearch.cluster.block.ClusterBlockException: blocked by: [FORBIDDEN/12/index read-only / allow delete (api)];

How to find the message: Run one of the following commands. If a message that includes "ClusterBlockException" is output, the message in quotation was output to the log.

[For a Docker environment]

# docker exec -it $(docker ps -a | grep rdocker:6000/logspout: | awk '{print $1}') /bin/bash -c 'grep -E "ClusterBlockException: blocked by: \[FORBIDDEN/[0-9]+/index read-only / allow delete \(api\)\]" /var/logs/infra-hid-grizzly/\*.log'

[For a Podman environment]

# podman exec -it $(podman ps -a | grep rdocker:6000/logspout: | awk '{print $1}') /bin/bash -c 'grep -E "ClusterBlockException: blocked by: \[FORBIDDEN/[0-9]+/index read-only / allow delete \(api\)\]" /var/logs/infra-hid-grizzly/\*.log'

(2) If the problem occurred, perform following steps.

Steps to recover:

1. Do ssh to Administrator server with root account.

2. Decrease filesystem usage by deleting unnecessary files or expansion of filesystem.

3. Unset the read-only status by following command.

[For a Docker environment]

docker ps -a | grep rdocker:6000/elasticsearch | docker exec `awk '{print $1}'` curl -XPUT -H "Content-Type: application/json" http://localhost:9200/\_all/\_settings -d '{"index.blocks.read\_only\_allow\_delete": null}'

[For a Podman environment and the version is earlier than 11.0.4]

podman ps -a | grep rdocker:6000/elasticsearch | podman exec `awk '{print $1}'` curl -XPUT -H "Content-Type: application/json" http://localhost:9200/\_all/\_settings -d '{"index.blocks.read\_only\_allow\_delete": null}'

[For a Podman environment and the version is 11.0.4 or later]

podman ps -a | grep rdocker:6000/elasticsearch | podman exec `awk '{print $1}'` curl -XPUT -H "Content-Type: application/json" http://localhost:$(cat /opt/rainier/settings/port.properties| grep ^port.internal.tcp.es.http= |awk -F "=" '{ print $2 }')/\_all/\_settings -d '{"index.blocks.read\_only\_allow\_delete": null}'

4.Refresh all storage systems.

### 2.2.16 How to change the time out value of MariaDB

1. Do ssh to Administrator server with root account.

2. Run the following command to open console of mariadb container.

[For a Docker environment]

docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') bash

[For a Podman environment]

podman exec -it $(podman ps -a | grep 6000/mariadb | awk '{print $1}') bash

1. Create the following file under "/etc/my.cnf.d"

* Name : mariadb.cnf
* Permission : 644
* Contents :

[mariadb]

wait\_timeout=604800

1. Run the following command to exit from mariadb container

exit

1. Run the following command to restart mariadb container

[For a Docker environment]

docker restart $(docker ps -a | grep 6000/mariadb | awk '{print $1}')

[For a Podman environment]

podman restart $(podman ps -a | grep 6000/mariadb | awk '{print $1}')

1. Verify the set value, if wait\_timeout is not 604800, execute step again from step 2.
2. Run the following command

[For a Docker environment]

docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') mysql -e "show global variables like 'wait\_timeout';"

[For a Podman environment]

podman exec -it $(podman ps -a | grep 6000/mariadb | awk '{print $1}') mysql -e "show global variables like 'wait\_timeout';"

1. Verify the following contents are output.

+---------------+--------+

| Variable\_name | Value |

+---------------+--------+

| wait\_timeout | 604800 |

+---------------+--------+

### 2.2.17 How to change the time out value of Command Control Interface command execution

Command execution timeout of Command Control Interface is set as 7 minutes in 10.6.1 or later, but Command Control Interface command times out when network environment between storage and Ops Center Administrator tends to lost UDP packet. In this case, change the time out value by the following steps.

1. Do ssh to Administrator server with root account.
2. Run the following command.

Following example sets 120 minutes, change value 120 if you would like to set another value.

[For a Docker environment]

docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '120' where name = 'CciCallTimeoutMin'";

[For a Podman environment]

podman exec -it $(podman ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '120' where name = 'CciCallTimeoutMin'";

1. Restart all containers on the Ops Center Administrator server

[For a Docker environment]

docker ps -a | grep rdocker:6000 | docker restart `awk '{print $1}'`

[For a Podman environment]

systemctl restart rainier

### 2.2.18 How to recover volume migration when Ops Center Administrator is restarted

As described in Figure 1, monitoring of migration pairs is performed after migration pairs are created in Migrate volumes task. The monitoring processing waits for the completion of replication, and it takes relatively long time. Therefore, Ops Center Administrator may be restarted for some reason while waiting. This section describes the recovery procedure below.

1. Get the log files of Ops Center Administrator and job ID of the volume migration from your customer.

The job ID can be found on the **Job details** page. Figure 1 shows an example of the page, and the job ID is "c8c35008-bf5c-498e-83e6-39e56f9e5af9".

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション, メール

自動的に生成された説明

Figure 1 An example of Job details page - Migrate volumes

2. Identify the NDC ID from the Job ID.

Extract log files of Ops Center Administrator and run grep command for files under the /logs/application-logs/rainier-rainier directory with the job ID as the key. The following is the example, and it indicates the NDC ID is "MIGRATION:nnilfl".

rainier-2021-12-09T08-26-45.127.log(36531): App | 2021-12-09T08:17:11,579 INFO [**MIGRATION:nnilfl**][RainierScheduler\_Worker-3] c.h.b.s.c.j.e.JobRunnerBase --- Created job JOB\_ID: **c8c35008-bf5c-498e-83e6-39e56f9e5af9**, Title: Migrate volumes

Note: On Ops Center Administrator version 10.9.1 or later versions, old log files are saved with gz format. Use the zgrep command as well as the grep command, or unzip the gz files and run the grep command.

3. Filter logs with the NDC ID.

Run grep command for files under the rainier-rainier directory with the NDC ID as a key to extract logs.

4. Identify the migration task ID.

Search " Starting a migration task with ID" from the logs extracted results on 3. The migration task ID is output after the message and make a note of that value. The value is 4 in the following example.

App | 2021-12-09T08:17:11,810 INFO [MIGRATION:nnilfl][pool-4-thread-30] c.h.b.s.c.j.e.JobStepReporter --- JOB\_ID: c8c35008-bf5c-498e-83e6-39e56f9e5af9, SEVERITY: Information, MESSAGE: Storage System 417707. **Starting a migration task with ID 4**.

5. Confirm the job progress.

Search "Created job" from the extracted log on 3. The output is like the following when terminated at monitoring migration pairs. In addition, if "Monitor migration pairs" does not appear or "Delete a migration pair" is output, other recovery procedure is required.

App | 2021-12-09T08:17:11,579 INFO [MIGRATION:nnilfl][RainierScheduler\_Worker-3] c.h.b.s.c.j.e.JobRunnerBase --- Created job JOB\_ID: c8c35008-bf5c-498e-83e6-39e56f9e5af9, Title: Migrate volumes  
App | 2021-12-09T08:19:23,993 INFO [MIGRATION:nnilfl][pool-4-thread-30] c.h.b.s.c.j.e.JobRunnerBase --- Created job JOB\_ID: 39011480-c8b0-4881-9302-a22431f47e82, Title: Create a migration pair  
App | 2021-12-09T08:22:02,581 INFO [MIGRATION:nnilfl][pool-4-thread-30] c.h.b.s.c.j.e.JobRunnerBase --- Created job JOB\_ID: 04361bfa-8d8a-412e-9310-0a65ee3489a1, Title: Create a migration pair  
App | 2021-12-09T08:24:29,309 INFO [MIGRATION:nnilfl][pool-4-thread-30] c.h.b.s.c.j.e.JobRunnerBase --- Created job JOB\_ID: d4edf19b-bdb6-4fb7-b3a6-92158b48cf64, Title: **Monitor migration pairs**

6. Get the migration task information.

Open the **Migration Tasks** page, and find the source volume IDs, the destination volume IDs and the copy progress for the migration task that is identified on 4. An example in Figure 2 indicates:

- Source volume IDs: 929, 930

- Destination volume IDs: 935, 936

- Copy progress: Both pair are 100%

If there is a pair whose processing is not 100%, you need to wait until the progress reaches 100%.

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション, メール

自動的に生成された説明

Figure 2 An example of Migrate Tasks page

If you want to find the above information on the log, search for the character string "MigrationStatusCalculator.calc() with argument[s]". Refer the line in which the migration task ID identified in 4. and the time stamp is latest. If the copy progress in the line is 100, it means the replication is completed. Since these lines are output for each migration pair, it is necessary to check multiple lines if there are multiple pairs. The following is an example for two migration pairs.

These lines contain the source and destination volume IDs, so make a note of those IDs.

App | 2021-12-09T08:42:00,912 INFO [REFRESH:iLJBP0, REFRESH:iLJBP0, REFRESH:iLJBP0, REFRESH:iLJBP0][pool-7-thread-36] c.h.b.s.c.c.a.BusinessLogicLoggingAspect --- Enter: com.hds.bel.storage.orchestrator.provider.block.data.migration.MigrationStatusCalculator.calc() with argument[s] = [MigrationPair{migrationPairId=MigrationPairIdentifier{migrationPairId=11, migrationTaskId=MigrationTaskIdentifier{**migrationTaskId=4**, storageSystemId=417707}}, **sourceVolumeId=VolumeIdentifier{volumeId=929**, storageSystemId=417707}, sourcePoolId=StoragePoolIdentifier{storagePoolId=0, storageSystemId=417707}, sourceParityGroupId=null, **targetVolumeId=VolumeIdentifier{volumeId=935**, storageSystemId=417707}, reservedVolumeId=null, targetPoolId=StoragePoolIdentifier{storagePoolId=11, storageSystemId=417707}, dkcDataSavingType=null, volumeIdRange=null, sourceLunPathAdded=false}, VolumePair{type=MIGRATION, volumePairGroup=hsa-test-pool\_1639037991091, primaryVolume=VolumeSpec{id=929, storageSystemId=417707, status=PSUS}, secondaryVolume=VolumeSpec{id=935, storageSystemId=417707, status=SSUS}, mirrorId=0, poolId=null, splitTime=null, consistent=false, consistencyId=null, state=HEALTHY, deviceName=929\_935, **copyProgress=100**, quorumId=null},...  
App | 2021-12-09T08:42:00,919 INFO [REFRESH:iLJBP0, REFRESH:iLJBP0, REFRESH:iLJBP0, REFRESH:iLJBP0][pool-7-thread-36] c.h.b.s.c.c.a.BusinessLogicLoggingAspect --- Enter: com.hds.bel.storage.orchestrator.provider.block.data.migration.MigrationStatusCalculator.calc() with argument[s] = [MigrationPair{migrationPairId=MigrationPairIdentifier{migrationPairId=12, migrationTaskId=MigrationTaskIdentifier{**migrationTaskId=4**, storageSystemId=417707}}, **sourceVolumeId=VolumeIdentifier{volumeId=930**, storageSystemId=417707}, sourcePoolId=StoragePoolIdentifier{storagePoolId=7, storageSystemId=417707}, sourceParityGroupId=null, **targetVolumeId=VolumeIdentifier{volumeId=936**, storageSystemId=417707}, reservedVolumeId=null, targetPoolId=StoragePoolIdentifier{storagePoolId=11, storageSystemId=417707}, dkcDataSavingType=null, volumeIdRange=null, sourceLunPathAdded=false}, VolumePair{type=MIGRATION, volumePairGroup=hsa-test-pool\_1639037991091, primaryVolume=VolumeSpec{id=930, storageSystemId=417707, status=PSUS}, secondaryVolume=VolumeSpec{id=936, storageSystemId=417707, status=SSUS}, mirrorId=0, poolId=null, splitTime=null, consistent=false, consistencyId=null, state=HEALTHY, deviceName=930\_936, **copyProgress=100**, quorumId=null}, ...

7. Identify the copy group name.

Extract "raidcom add copy\_grp" from the result of 3. A character string after "-copy\_grp\_name" is the copy group name. It is "hsa-test- pool\_1639037991091" in the following example.

Block | 2021-12-09T08:20:05,349 INFO [MIGRATION:nnilfl:uCi7Gq][pool-6-thread-4] c.h.b.s.d.b.s.c.c.CciCommandBase --- [417707] Running Command: echo | read-lock raidcom add copy\_grp   
**-copy\_grp\_name hsa-test-pool\_1639037991091** hsa-test-pool\_1639037991091\_P hsa-test-pool\_1639037991091\_S   
-mirror\_id 0 -IM0, attempt #0

8. Identify the device group information.

Extract " Running Command: ... raidcom add device\_grp " from the result of 3. A character string after "-device\_grp\_name” and “-ldev\_id” is the device group information. The combination of "DpPool\_001\_1711350718949\_P" and "250" and the combination of "DpPool\_001\_1711350718949\_S" and "251" are as in the following example.

rainier.log:Block | 2024-03-25T07:11:59,312 INFO [MIGRATION:sNxoyn:c5wJrc][pool-1411-thread-6] c.h.b.s.d.b.s.c.c.CciCommandBase --- [700183] Running Command: echo | read-lock raidcom add device\_grp -device\_grp\_name **DpPool\_001\_1711350718949\_P** 250\_251 -ldev\_id **250** -IM0, attempt #0

rainier.log:Block | 2024-03-25T07:11:59,643 INFO [MIGRATION:sNxoyn:c5wJrc][pool-1411-thread-4] c.h.b.s.d.b.s.c.c.CciCommandBase --- [700183] Running Command: echo | read-lock raidcom add device\_grp -device\_grp\_name **DpPool\_001\_1711350718949\_S** 250\_251 -ldev\_id **251** -IM0, attempt #0

9. Identify LUN paths for the replication.

Extract "Running Command: ... raidcom add lun" from the result of 3. Character strings after "-port" and "-ldev\_id" is the LUN path information. In the example below, the combination of CL1-A-4 and 936 and the combination of CL1-A4 and 935 correspond to it.

Block | 2021-12-09T08:19:30,783 INFO [MIGRATION:nnilfl:yLHtaE][pool-6-thread-1] c.h.b.s.d.b.s.c.c.CciCommandBase --- [417707] Running Command: echo | read-lock raidcom add lun **-port CL1-A-4 -ldev\_id 936** -IM0, attempt #0  
Block | 2021-12-09T08:22:08,900 INFO [MIGRATION:nnilfl:bKJaH4][pool-6-thread-8] c.h.b.s.d.b.s.c.c.CciCommandBase --- [417707] Running Command: echo | read-lock raidcom add lun **-port CL1-A-4 -ldev\_id 935** -IM0, attempt #0

10. Delete the pairs.

Log in to the Ops Center Administrator server as a user with root privileges. And then, enter the CLI container corresponding to the storage system ID. If the storage system ID is 417707, run the following command:

docker exec -it **cli\_417707** bash

In addition, run commands for deleting pairs with specifying the copy group name. The copy group name is identified in 7.

pairsplit **-g hsa-test-pool\_1639037991091** -S -IM0

11. Delete the device group

Run commands for deleting device group. The device group information is identified in 8.

raidcom delete device\_grp -device\_grp\_name **DpPool\_001\_1711350718949\_P** -ldev\_id **250** -IM0

raidcom delete device\_grp -device\_grp\_name **DpPool\_001\_1711350718949\_S** -ldev\_id **251** -IM0

12. Remove LUN paths for replication.

Run commands to remove LUN paths. The LUN paths added on the 9 are removed.

raidcom delete lun **-port CLI1-A-4 -ldev\_id 936** -IM0

raidcom delete lun **-port CLI1-A-4 -ldev\_id 935** -IM0

13. Discard zero pages in the destination volumes.

Perform discarding zero page with specifying the destination volume ID that is identified in 6.

raidcom modify ldev **-ldev\_id 929** -status discard\_zero\_page -IM0

raidcom modify ldev **-ldev\_id 930** -status discard\_zero\_page -IM0

And then, exit from the CLI container.

exit

14. Remove the migration task information from Mariadb.

In the following way, remove migration pair information and migration task information in the Mariadb with specifying migration task ID that is identified in 4.

docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "delete from migration\_pair where **migration\_task\_id=4**;"  
docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "delete from migration\_task where **migration\_task\_id=4**;"

15. Delete the cached data stored in the Elasticsearch service.

See 2.2.12 for details.

Note: This step is only required on Ops Center Administrator version 10.7.0 or earlier.

16. Remove the source volumes before migration by using the Administrator's function if necessary.

### 2.2.19 How to change the wait time of HORCM instance start for CLI container

Wait time of HORCM instance start for CLI container is 25 minutes in 10.8.1 or later. When a lot of pairs are included in copy group, there is a case that HORCM instance start time exceeds wait time. In this case, it is possible to change wait time by following steps.

1. Do ssh to Administrator server with root account.

2. Run the following command.

[For a Docker environment]

docker exec -it $(docker ps | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '1800' where name = 'CliWaitContainerAvailableTimeoutInSeconds';"

[For a Podman environment]

podman exec -it $(docker ps | grep 6000/mariadb | awk '{print $1}') mysql -D rainier -e "update application\_property set value = '1800' where name = 'CliWaitContainerAvailableTimeoutInSeconds';"

3. Restart all containers on the Ops Center Administrator server.

[For a Docker environment]

docker ps -a | grep rdocker:6000 | docker restart `awk '{print $1}'`

[For a Podman environment]

systemctl restart rainier

### 2.2.20 How to delete a storage system manually when the storage system could not be deleted from the GUI

By some reason, a storage system could not be deleted from the GUI. In this case, you can remove the storage system manually by running some commands. The following steps shows the commands when the storage system ID is 20055. Replace 2055 with the target ID when running the commands.

1. By using the root user account, log in to the Ops Center Administrator server.

2. Stop the rainier container.

If Docker is used:

# docker stop $(docker ps -aqf "name=\_rainier\_1")

If Podman is used:

# podman stop $(podman ps -aqf "name=\_rainier\_1")

3. Stop and remove the CLI container.

If Docker is used:

# docker stop cli\_20055

# docker rm cli\_20055

If Podman is used:

# podman stop cli\_20055

# podman rm cli\_20055

4. Open the MariaDB console.

If Docker is used:

# docker exec -it $(docker ps -aqf "name=\_mariadb\_1") mysql rainier

If Podman is used:

# podman exec -it $(podman ps -aqf "name=\_mariadb\_1") mysql rainier

5. Check if any migration tasks exist.

select migration\_task\_id from migration\_task where storage\_system\_id='20055';

If any id is output as below, perform the following step 6 and 7.

+-------------------+

| migration\_task\_id |

+-------------------+

| 2 |

+-------------------+

1 row in set (0.001 sec)

If no id is output as below, skip the following step 6 and 7.

Empty set (0.000 sec)

6. Delete records related to scheduled tasks for volume migration.

Run this step for each ID output in 5. The following commands are examples when migration\_task\_id is 2, and replace the ID with the target ID.

delete from QRTZ\_SIMPLE\_TRIGGERS where trigger\_name='migrationTaskId:2';

delete from QRTZ\_TRIGGERS where job\_name='migrationTaskId:2';

delete from QRTZ\_JOB\_DETAILS where job\_name='migrationTaskId:2';

7. Delete migration task records.

delete from migration\_pair where storage\_system\_id='20055';

delete from migration\_task where storage\_system\_id='20055';

Note: This step is not mandatory. When you remove a storage system from the GUI, these records are not removed.

8. Delete records related to scheduled task for creating snapshots.

delete from QRTZ\_CRON\_TRIGGERS where trigger\_name like 'SNAP\_JOB\_20055\_%';

delete from QRTZ\_TRIGGERS where job\_name like 'SNAP\_JOB\_20055\_%';

delete from QRTZ\_JOB\_DETAILS where job\_name like 'SNAP\_JOB\_20055\_%';

9. Delete replication policy records.

delete from replication\_policy\_primary\_volume where replication\_policy\_model\_id IN (select id from replication\_policy where storage\_system\_id='20055');

delete from replication\_policy\_group where replication\_policy\_id IN (select id from replication\_policy where storage\_system\_id='20055');

delete from replication\_policy where storage\_system\_id='20055';

Note: This step is not mandatory. When you remove a storage system from the GUI, these records are not removed.

10. Delete the storage system record.

delete from storage\_system\_metadata where storage\_system\_id='20055';

11. Close the MariaDB console.

exit

12. de Elasticsearch indexes for the storage system.

If Docker is used:

# docker exec -it $(docker ps -aqf "name=hid-elasticsearch\_1") curl -X DELETE localhost:9200/20055-com.hds\*

If Podman is used and the version is earlier than 11.0.4:

# podman exec -it $(podman ps -aqf "name=hid-elasticsearch\_1") curl -X DELETE localhost:9200/20055-com.hds\*

If Podman is used and the version is 11.0.4 or later:

# podman exec -it $(podman ps -aqf "name=hid-elasticsearch\_1") curl -X DELETE localhost:$(cat /opt/rainier/settings/port.properties| grep ^port.internal.tcp.es.http= |awk -F "=" '{ print $2 }')/20055-com.hds\*

13. Restart all containers of Administrator server.

If Docker is used:

# docker ps -a | grep rdocker:6000 | docker restart $(awk '{print $1}')

If Podman is used:

# systemctl restart rainier

### 2.2.21 How to forcibly uninstall Administrator on a Podman environment

The procedure to uninstall Administrator is described in *Chapter 6: Removing Ops Center Administrator* of *Hitachi Ops Center Administrator Getting Started Guide*. However, sometimes the procedure does not work when the Podman is unstable. In that case, perform the following steps.

Note: All Podman resources such as containers and images are removed.

Steps for force uninstall:

(1) Login to the Administrator server by using a user having the root permission.

(2) Initialize the Podman environment.

# podman system reset

Specify 'y' for the following message:

WARNING! This will remove:

- all containers

- all pods

- all images

- all networks

- all build cache

- all machines

Are you sure you want to continue? [y/N]

If (2) is succeeds, remove files created by Administrator:

# sh /opt/rainier/bin/rainier-config-remove

(For 10.9.3 or later execute above)

# rm -rf /opt/rainier

# rm -rf /var/log/rainier-audit-log

# rm -rf /var/logs/rainier-tool

# rm -rf /var/logs/rainier-elastic-store

# rm -rf /var/run/host-manager.sock

# rm -rf /var/logs/rainier-logs

# rm -rf /var/logs/rainier-ubi

# rm -rf /var/opt/rainier-ubi

# rm -f /etc/systemd/system/rainier.service

# rm -f /etc/systemd/system/rainier-pipe.service

# rm -f /etc/containers/containers.conf.d/rainier.conf

If (2) fails, perform the following steps:

(3) Stop the Administrator service:

# systemctl stop rainier

(4) Disable the Administrator service

# systemctl disable rainier

(5) Restart OS

(6) Remove resources of Podman:

# rm -rf /var/lib/containers/storage

(7) Remove files created by Administrator

# sh /opt/rainier/bin/rainier-config-remove

(For 10.9.3 or later execute above)

# rm -rf /opt/rainier

# rm -rf /var/log/rainier-audit-log

# rm -rf /var/logs/rainier-tool

# rm -rf /var/logs/rainier-elastic-store

# rm -rf /var/run/host-manager.sock

# rm -f /etc/systemd/system/rainier.service

------------------------------------------------------------

### 2.2.22 How to delete a HA replication group without changing the configuration on Protector

To delete a High Availability replication group without removing resources on the Ops Center Protector server, perform the following steps (in the steps below, the replication group name is RG1):

(1) Login to the Administrator server by using a user having the root permission.

(2) Open the mysql console in the mariadb container.

For Docker environment:

# docker exec -it $(docker ps -a | grep 6000/mariadb | awk '{print $1}') mysql rainier

For Podman environment:

# podman exec -it $(podman ps -a | grep 6000/mariadb | awk '{print $1}') mysql rainier

(3) Search the ID of the hdid\_data\_flow\_operation.

MariaDB [rainier]> select hdid\_data\_flow\_operation from replication\_policy where name='RG1';

Output example:

+--------------------------+

| hdid\_data\_flow\_operation |

+--------------------------+

| 3 |

+--------------------------+

1 row in set (0.001 sec)

(4) Delete the replication\_policy record.

MariaDB [rainier]> delete from replication\_policy where name='RG1';

Query OK, 1 row affected (0.001 sec)

(5) Delete the hdid\_data\_flow\_operaion record. Specify the ID in the following where clause that was found in step (3).

MariaDB [rainier]> delete from hdid\_data\_flow\_operation where id=3;

Query OK, 1 row affected (0.001 sec)

(6) Close the mysql console.

MariaDB [rainier]> exit

Bye

(7) Restart the Administrator server.

For Docker environment:

# docker ps -a | grep rdocker:6000 | docker restart $(awk '{print $1}')

For Podman environment:

# systemctl restart rainier

### 2.2.23 How to initialize VAM sysadmin account password

Execute following steps to initialize password.

1. Login to Administrator server with root account.
2. Get into infra-app-manager container.

[For a Docker environment]

# docker exec -it $(docker ps -a | grep 6000/infra-app-manager | awk '{print $1}') bash

[For a Podman environment]

# podman exec -it $(podman ps -a | grep 6000/infra-app-manager | awk '{print $1}') bash

1. Execute following command.

[For the version is earlier than 11.0.4]

# etcdctl set /hid-instances/$APP\_MANAGER\_INSTANCE\_ID/user-accounts/sysadmin '{"username":"sysadmin","passwordHash":"d577adc54e95f42f15de2e7c134669888b7d6fb74df97bd62cb4f5b73c281db4"}'

[For the version is 11.0.4 or later]

# etcdctl --endpoints http://127.0.0.1:$(cat /opt/config/port.properties| grep ^port.internal.tcp.etcd= |awk -F "=" '{ print $2 }') set /hid-instances/$APP\_MANAGER\_INSTANCE\_ID/user-accounts/sysadmin '{"username":"sysadmin","passwordHash":"d577adc54e95f42f15de2e7c134669888b7d6fb74df97bd62cb4f5b73c281db4"}'

### 2.2.24 When The "Create a migration pair" fails at “The volume xx was not found.”

When “Migrate volumes” fails at child job “Create a migration pair”, with “The volume xx was not found.” output in the job report, there is a possibility that a software lock conflict occurred in storage system.

Therefore, in such case, wait for a certain period of time and retry it again. Confirm that "Create a migration pair" is completed successfully.

### 2.2.25 If the " Error: .ini file does not include supervisord section " is output in the rainier log

If you are unable to log in to the Administrator, and the " Error: .ini file does not include supervisord section " is output in the rainier log, docker related files may be corrupted.

In such cases, you can recovery by following the steps below.

1. Rebuilding the rainier container

Because the rainier container is not working properly, rebuild the rainier container

1. Stop the rainier container

[For a Docker environment]

# docker stop $(docker ps -a | grep 6000/rainier: | awk '{print $1}')

[For a Podman environment]

# podman stop $(podman ps -a | grep 6000/rainier: | awk '{print $1}')

1. Remove the rainier container

[For a Docker environment]

# docker rm $(docker ps -a | grep 6000/rainier: | awk '{print $1}')

[For a Podman environment]

# podman rm $(podman ps -a | grep 6000/rainier: | awk '{print $1}')

1. Open console the infra-app-manager container

[For a Docker environment]

# docker exec -it $(docker ps -a | grep 6000/infra-app-manager: | awk '{print $1}') bash

[For a Podman environment]

# podman exec -it $(podman ps -a | grep 6000/infra-app-manager: | awk '{print $1}') bash

(4) Search the docker-compose file

# grep -r 6000/rainier: ./docker-compose-projects

Output example:

./docker-compose-projects/73a41927-f956-433e-b15d-b8e01e265933/docker-compose.yml: image: rdocker:6000/rainier:zebra\_default\_e6004026cf5dfaaaf3becab2e16ff3ea760f255f

(5) Move to the directory where docker-compose.yml is stored

# cd ./docker-compose-projects/73a41927-f956-433e-b15d-b8e01e265933

(6) Execute the “docker compose”

# docker-compose up

Once a certain number of logs are output, stop with CTRL+C

(7) Close console the infra-app-manager container

# exit

(8) Restart the Administrator

[For a Docker environment]

# systemctl restart docker

[For a Podman environment]

# systemctl restart rainier

(9) Check operating status of the rainier container

[For a Docker environment]

# docker exec -it $(docker ps -a | grep 6000/logspout: | awk '{print $1}') tail -f /var/logs/rainier-rainier/rainier.log

[For a Podman environment]

# podman exec -it $(podman ps -a | grep 6000/logspout: | awk '{print $1}') tail -f /var/logs/rainier-rainier/rainier.log

Check that logs starting with “app” or “block” are output.

Note:If logs starting with “app” or "block” are not output even after about 10 minutes, it is highly likely that recovery is not possible.

Consider to re-install Administrator without backup.

2. Obtain backup data

(1) Obtain Authentication token

[For the version is earlier than 11.0.4]

# curl --noproxy '\*' -u "sysadmin:password" --silent -w "%{http\_code}" --output /dev/null -D - -X POST <http://127.0.0.1:8085/v1/security/tokens>

[For the version is 11.0.4 or later]

# curl --noproxy '\*' -u "sysadmin:password" --silent -w "%{http\_code}" --output /dev/null -D - -X POST http://127.0.0.1:$(cat /opt/rainier/settings/port.properties| grep ^port.internal.tcp.appmanager= |awk -F "=" '{ print $2 }')/v1/security/tokens

Note:Change the password to the password to login to the Virtual Appliance Manager GUI for sysadmin user.

Output example:

HTTP/1.1 200

X-Auth-Token: aa4a718a-b7a8-4341-a156-a440c1b340af

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: DENY

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

Pragma: no-cache

Expires: 0

Content-Length: 0

Date: Tue, 08 Nov 2022 06:51:56 GMT

(2) Confirm the following two points regarding the result of step (1) .

・“HTTP/1.1 200” is output.

・”X-Auth-Token:…” is output

If either one is No, the password in step (1) might not be correct. Please return to step (1) and retry again.

(3) Obtain backup data by specifying the authentication token

[For the version is earlier than 11.0.4]

# curl --noproxy '\*' -H "X-Auth-Token: aa4a718a-b7a8-4341-a156-a440c1b340af" -H "Content-Type: application/json" -w "%{http\_code}" -X POST -d '{}' --output "backup.tar.gz" <http://127.0.0.1:8085/v1/applications/export-data>

[For the version is 11.0.4 or later]

# curl --noproxy '\*' -H "X-Auth-Token: aa4a718a-b7a8-4341-a156-a440c1b340af" -H "Content-Type: application/json" -w "%{http\_code}" -X POST -d '{}' --output "backup.tar.gz" http://127.0.0.1: $(cat /opt/rainier/settings/port.properties| grep ^port.internal.tcp.appmanager= |awk -F "=" '{ print $2 }') /v1/applications/export-data

Note: Replace "X-Auth-Token: ..." with the content in (2) above.

(4) Check backup data just in case

# tar -tvf backup.tar.gz

Note:If content is not output correctly, backup data was not be obtained correctly.

Consider re-install Administrator without backup.

Output example:

drwxr-xr-x root/root 0 2022-11-08 06:53 appManager/

-rw-r--r-- root/root 3004 2022-11-08 06:53 appManager/certificateData

-rw-r--r-- root/root 122 2022-11-08 06:53 appManager/logSettings.json

-rw-r--r-- root/root 92 2022-11-08 06:53 appManager/ldapSettings.json

-rw-r--r-- root/root 71 2022-11-08 06:53 appManager/hostSettings.json

-rw-r--r-- root/root 33 2022-11-08 06:53 appManager/rainierMemorySettings.json

-rw-r--r-- root/root 17 2022-11-08 06:53 appManager/metadata.json

drwxr-xr-x root/root 0 2022-11-08 06:55 infra/

drwxr-xr-x root/root 0 2022-11-08 06:55 infra/si/

-rw-r--r-- root/root 1654 2022-11-08 06:55 infra/si/account\_domain.json

-rw-r--r-- root/root 0 2022-11-08 06:55 infra/si/common\_services\_config.json

-rw-r--r-- root/root 0 2022-11-08 06:55 infra/si/common\_services\_group\_mapping.json

-rw-r--r-- root/root 0 2022-11-08 06:55 infra/si/ldab\_auth\_provider.json

-rw-r--r-- root/root 18 2022-11-08 06:55 infra/si/metadata.json

-rw-r--r-- root/root 367 2022-11-08 06:55 infra/si/si.properties

-rw-r--r-- root/root 1031 2022-11-08 06:55 infra/si/user.json

drwxr-xr-x root/root 0 2022-11-08 07:00 infra/hid-grizzly/

-rw-r--r-- root/root 1 2022-11-08 06:57 infra/hid-grizzly/grizzly.properties

-rw-r--r-- root/root 332712 2022-11-08 06:57 infra/hid-grizzly/jobs.json

-rw-r--r-- root/root 18 2022-11-08 06:57 infra/hid-grizzly/metadata.json

drwxr-xr-x root/root 0 2022-11-08 06:58 rainier/

drwxr-xr-x root/root 0 2022-11-08 06:57 rainier/file/

-rw-r--r-- root/root 0 2022-11-08 06:57 rainier/file/bellerophonData

-rw-r--r-- root/root 44 2022-11-08 06:57 rainier/file/encryptionKey.json

-rw-r--r-- root/root 19 2022-11-08 06:57 rainier/file/metadata.json

drwxr-xr-x root/root 0 2022-11-08 06:58 rainier/cinder-brocade/

drwxr-xr-x root/root 0 2022-11-08 06:58 rainier/cinder-brocade/data/

-rw-r--r-- root/root 9216 2022-11-08 06:58 rainier/cinder-brocade/data/whistlerCinder.db

-rw-r--r-- root/root 14 2022-11-08 06:58 rainier/cinder-brocade/metadata

drwxr-xr-x root/root 0 2022-11-08 06:58 rainier/cinder-cisco/

drwxr-xr-x root/root 0 2022-11-08 06:58 rainier/cinder-cisco/data/

-rw-r--r-- root/root 9216 2022-11-08 06:58 rainier/cinder-cisco/data/whistlerCinder.db

-rw-r--r-- root/root 14 2022-11-08 06:58 rainier/cinder-cisco/metadata

drwxr-xr-x root/root 0 2022-11-08 06:58 rainier/whistler/

drwxr-xr-x root/root 0 2022-11-08 06:58 rainier/whistler/data/

-rw-r--r-- root/root 20480 2022-11-08 06:58 rainier/whistler/data/whistler.mv.db

-rw-r--r-- root/root 14 2022-11-08 06:58 rainier/whistler/metadata

drwxr-xr-x root/root 0 2022-11-08 07:00 rainier/rainier/

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/AlertStatusRepository.json

-rw-r--r-- root/root 526 2022-11-08 07:00 rainier/rainier/ApplicationProperties.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/ChapUserRepository.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/ComponentAlertStatusRepository.json

-rw-r--r-- root/root 24 2022-11-08 07:00 rainier/rainier/CopyGroupSequenceIdRepository.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/DiskAlertStatusRepository.json

-rw-r--r-- root/root 181 2022-11-08 07:00 rainier/rainier/HdidMetadataRepository.json

-rw-r--r-- root/root 509 2022-11-08 07:00 rainier/rainier/HotSpareDiskRatioRepository.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/MigrationPairRepository.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/MigrationTaskRepository.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/ProtectionSetupStatusRepository.json

-rw-r--r-- root/root 1048 2022-11-08 07:00 rainier/rainier/RaidConfigurationRepository.json

-rw-r--r-- root/root 574 2022-11-08 07:00 rainier/rainier/RaidLayoutRepository.json

-rw-r--r-- root/root 229 2022-11-08 07:00 rainier/rainier/RaidLevelRepository.json

-rw-r--r-- root/root 2426 2022-11-08 07:00 rainier/rainier/ReplicationPolicyRepository.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/ServerGroupRepository.json

-rw-r--r-- root/root 4300 2022-11-08 07:00 rainier/rainier/ServerRepository.json

-rw-r--r-- root/root 0 2022-11-08 07:00 rainier/rainier/SnmpManagerMetadataRepository.json

-rw-r--r-- root/root 1257 2022-11-08 07:00 rainier/rainier/StorageArrayRepository.json

-rw-r--r-- root/root 64 2022-11-08 07:00 rainier/rainier/StorageLaunchSettings.json

-rw-r--r-- root/root 1428 2022-11-08 07:00 rainier/rainier/StorageSystemMetadataRepository.json

-rw-r--r-- root/root 3937 2022-11-08 07:00 rainier/rainier/SubTierRepository.json

-rw-r--r-- root/root 1987 2022-11-08 07:00 rainier/rainier/TierRepository.json

-rw-r--r-- root/root 778 2022-11-08 07:00 rainier/rainier/WarningBannerSettings.json

-rw-r--r-- root/root 67 2022-11-08 07:00 rainier/rainier/encryptionKey

-rw-r--r-- root/root 19 2022-11-08 07:00 rainier/rainier/metadata.json

-rw-r--r-- root/root 32 2022-11-08 07:00 rainier/rainier/rainier\_cacerts

(5) Move the backup data(backup.tar.gz) to a location that is accessible to Administrator client (the host that can display Administrator GUI)

3. Remove the Administrator

Refer to “Removing Ops Center Administrator” section in the Ops Center Administrator Getting Started Guide for removal step.

4. Reinstall the Docker/Podman

Uninstall and reinstall docker/podman

5. Install

Prepare the Administrator media and install it.

Refer to “Installing Ops Center Administrator” section in the Ops Center Administrator Getting Started Guide for install step.

6. Restore

Click Restore button in the Virtual Appliance Manager GUI and specify the backup data file (backup.tar.gz) in step 2 above.

### 2.2.26 How to replace a certificate using the CLI

Please follow the steps below to replace the certificate when access to VAM is restricted.

1. Get the ID of the app-manager container

【For the version is earlier than 11.0.4】

[For a Docker environment]

# APP\_IP=$(docker inspect --format='{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' `docker ps --filter 'label=APP\_MANAGER\_CONTAINER\_LABEL=app-manager' --format='{{ .ID }}' --latest`)

[For a Podman environment]

# APP\_IP=$(podman inspect --format='{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' `podman ps --filter 'label=APP\_MANAGER\_CONTAINER\_LABEL=app-manager' --format='{{ .ID }}' --latest`)

【For the version is 11.0.4 or later】

[For the Network Mode is bridge]

# APP\_IP=$(podman inspect --format='{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' `podman ps --filter 'label=APP\_MANAGER\_CONTAINER\_LABEL=app-manager' --format='{{ .ID }}' --latest`)

[For the Network Mode is host]

# APP\_IP=127.0.0.1

1. Check the obtained container ID

# echo $APP\_IP

Output example:

10.88.0.25

1. Get the instance ID from the app-manager container

[For a Docker environment]

# INST=$(docker inspect --format='{{.Config.Env }}' `docker ps -qf 'label=APP\_MANAGER\_CONTAINER\_LABEL=app-manager'` | sed 's/ /\n/g' | grep APP\_MANAGER\_INSTANCE\_ID | sed -e "s/APP\_MANAGER\_INSTANCE\_ID=/\/hid-instances\//g")

[For a Podman environment]

# INST=$(podman inspect --format='{{.Config.Env }}' `podman ps -qf 'label=APP\_MANAGER\_CONTAINER\_LABEL=app-manager'` | sed 's/ /\n/g' | grep APP\_MANAGER\_INSTANCE\_ID | sed -e "s/APP\_MANAGER\_INSTANCE\_ID=/\/hid-instances\//g")

1. Check the obtained instance ID

# echo $INST

Output example:

/hid-instances/1a06500d-8bdb-4fb8-8d73-0908098ca0ee

1. Set the server certificate in the environment variable

# CRT=$(cat <server certificate>)

# CRT=${CRT//[+]/%2B}

1. Set the private key in the environment variable

# KEY=$(cat <private key>)

# KEY=${KEY//[+]/%2B}

1. Replace the server certificate

[For the version is earlier than 11.0.4]

# curl -L --noproxy '\*' http://${APP\_IP}:2379/v2/keys${INST}/nginx/server-certificate -X PUT -d value="${CRT}"

[For the version is 11.0.4 or later]

# curl -L --noproxy '\*' http://${APP\_IP}:$(cat /opt/rainier/settings/port.properties| grep ^port.internal.tcp.etcd= |awk -F "=" '{ print $2 }')/v2/keys${INST}/nginx/server-certificate -X PUT -d value="${CRT}"

1. Replace the private key

[For the version is earlier than 11.0.4]

# curl -L --noproxy '\*' http://${APP\_IP}:2379/v2/keys${INST}/nginx/server-key -X PUT -d value="${KEY}"

[For the version is 11.0.4 or later]

# curl -L --noproxy '\*' http://${APP\_IP}:$(cat /opt/rainier/settings/port.properties| grep ^port.internal.tcp.etcd= |awk -F "=" '{ print $2 }')/v2/keys${INST}/nginx/server-key -X PUT -d value="${KEY}"

# 3. Necessary Data for Troubleshooting

## 3.1 Information required for investigation

Table 3-1 Information required for investigation

|  |  |  |
| --- | --- | --- |
| # | Collect information | Detail |
| 1 | Operation information | * Steps before failure * Reproducible or not * Occurred symptoms (error message, etc.) |
| 2 | Time of failure occurred | * Time of failure occurred * When symptom started(There is success case or not) |
| 3 | Log of administrator/Environment information | * In case 10.0.0 or later, result of rainier-getlogs * In case earlier than 10.0.0, application-log from VAM and HSA version |
| 4 | Storage information | * Type of storage (like VSP G1000, G370), version of micro code |

## 3.2 Information collection method

### 3.2.1 When log can be collected from VAM(earlier than 10.0.0)

Login to VAM and push "DOWNLOAD LOGS" that is displayed in upper left, then download Application logs.

### When log cannot be collected from VAM(earlier than 10.0.0)

1. Check container ID of logspout

Docker ps | grep logspout

1. Execute copy

Docker cp <Container ID that is checked in step 1>:/var/logs <any directory>

Example

[root@hsaauto235 ~]# docker ps | grep logspout

f0949f26a855 rdocker:6000/logspout:infiniti\_default\_e8f21f6eaafaec91ac950bc792af428e55e8e737 "/opt/start.sh" 22 hours ago Up 22 hours 59923e9b97694a629bdb287449f1ee01\_logspout\_1

[root@hsaauto235 ~]# docker cp f0949f26a855:/var/logs /tmp/hsaLog/

[root@hsaauto235 ~]# tar -zcvf hsalog.tar.gz /tmp/hsaLog/logs

### 3.2.3 In case 10.0.0 or later

Collect rainier-logs.tar.gz after executing following command.

/opt/rainier/bin/rainier-getlogs -dir <Output location>

# Appendix

## A-1 For the HPE OEM version, substitute the following terms as indicated

When reading, replace the terms in the text according to the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Item | Hitachi version | HPE OEM version |
| 1 | Product Names | Hitachi Ops Center Administrator | HPE XP Intelligent Storage Manager |
| 2 | Hitachi Data Instance Director | Data Protection Manager |
| 3 | Storage Navigator | Remote Web Console |
| 4 | Related documents | Hitachi Ops Center Administrator Getting Started Guide | HPE XP Intelligent Storage Manager |
| 5 | Hitachi Ops Center Administrator User Guide | HPE XP Intelligent Storage Manager User Guide |
| 6 | Hitachi Ops Center Administrator REST API Reference Guide | None |
| 7 | Subsystem Names  (RAID) | "Hitachi Virtual Storage Platform" or "VSP G1000/1500, F1500" or RAID800 | XP7 |
| 8 | "Hitachi Virtual Storage Platform" or "VSP G5000 series" or RAID900 | XP8 |
| 9 | Subsystem Names(HM) | "Hitachi Virtual Storage Platform" or "VSP G200/400/600/800, F400/600/800" or HM800 | None(HITACHI only) |
| 10 | "Hitachi Virtual Storage Platform" or "VSP G350/370/700/900, F350/370/700/900" or HM850 | None(HITACHI only) |
| 11 | "Hitachi Virtual Storage Platform" or "VSP GX00" or HM900 | None(HITACHI only) |
| 12 | Copy Pair names | Clone | Business Copy(BC) |
| 13 | Snap | Fast Snap |
| 14 | HA | HA |
| 15 | Pool names | Dynamic Tiering(TIRED) | Smat Tiers(SMART) |
| 16 |  | Dynamic Provisioning(THIN) | Thin Provisioning(THP) |
| 17 |  | Thin Image(SNAP) | Fast Snap |