Hitachi Compute Systems Manager 8.4.1-01 Release Notes

About this document

This document (RN-91HC198-48, June 2016) provides late-breaking information about the Hitachi Compute Systems Manager Software 8.4.1-01. It includes information that was not available at the time the technical documentation for this product was published, as well as a list of known problems and solutions.

Intended audience

This document is intended for customers and Hitachi Data Systems partners who license and use the Hitachi Compute Systems Manager Software.

Getting help

Hitachi Data Systems Support Connect is the destination for technical support of products and solutions sold by Hitachi Data Systems. To contact technical support, log on to Hitachi Data Systems Support Connect for contact information: https://support.hds.com/en_us/contact-us.html.

Hitachi Data Systems Community is a global online community for HDS 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.hds.com, register, and complete your profile.

About this release

This release resolves multiple known problems.

Product package contents

Table 1 Software and Documents in Product Package

Medium	CD-ROM	Revision	Release Type	Service Pack Prerequisite
Software	Hitachi Compute Systems Manager (#1)	8.4.1-01	Full Package	-
Documents	*Hitachi Command Suite Compute Systems Manager User Guide*	MK-91HC194-15		
	Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide	MK-91HC195-18		
	Hitachi Command Suite Compute Systems Manager CLI Reference Guide	MK-91HC196-04		
	Hitachi Command Suite Compute Systems Manager Messages	MK-91HC197-17		
	Hitachi Command Suite Compute Systems Manager REST API Reference Guide	MK-92HC235-00		
	Hitachi Command Suite Messages	MK-90HC178-24		

(#1) HCSM with the HCSM Plug-in Trial Pack is installed automatically. Explore all HCSM plug-ins such as N+M Cold Standby and Logical Partitioning Manager free for 120 days. Purchase Permanent plug-in licenses to continue to use a specific plug-in or add capacity to manage additional resources.

New features and important enhancements

For 8.4.1-01

None

For 8.4.1-00

No.	New Features and Enhancements	Applied products	Applied OS
1	HCSM can now manage Chassis, Blades, and Hosts using a REST (Representational State Transfer) API.	Hitachi Compute Systems Manager	Windows Linux

2	HCSM can now manage servers as deployment resources when the server MAC address is unavailable by allowing users to specify the address manually.	Hitachi Compute Systems Manager	Windows
3	HCSM now supports Chrome for Work as a Windows client browser.	Hitachi Compute Systems Manager	Windows Linux

For 8.4.0-00

No.	New Features and Enhancements	Applied products	Applied OS
1	HCSM can manage user permissions using an external authorization server in addition to an external authentication server.	Hitachi Compute Systems Manager	Windows Linux
2	HCSM now displays the last login date and time for each user.	Hitachi Compute Systems Manager	Windows Linux
3	HCSM CLI now supports obtaining chassis information.	Hitachi Compute Systems Manager CLI	Windows Linux
4	HCSM CLI now supports obtaining blade information and controlling blade power.	Hitachi Compute Systems Manager CLI	Windows Linux
5	HCSM addresses security vulnerability HID-HCSMGUI0000019911, which relates to malicious third parties obtaining session information illegally. The prerequisite management module firmware version for Compute Blade CB500/CB2500 has been replaced and the previous firmware can no longer be used. For detailed information about upgrading the management firmware version, see Table 10 Management target requirements - Hardware Requirements.	Hitachi Compute Systems Manager	Windows Linux

System requirements

This section describes the Compute Systems Manager system requirements.

Management server requirements

This section describes the management server requirements.

Hardware Requirements

Installation of Compute Systems Manager requires a computer that satisfies the following hardware requirements.

Computer requirements

The following table describes the management server computer requirements.

Table 2 Management server computer requirements

Item	Requirements
Processor	Minimum: Dual-Core Processor Recommended: Quad-Core Processor
Physical memory	Minimum: 2 GB Recommended: 4GB Note: If Compute Systems Manager and other software products are used simultaneously, the amount of the physical memory must be equal to the total memory size of all the software products.
Disk space	Minimum: New installation(Windows): When Deployment Manager is used : 17.6 GB When Deployment Manager is not used : 11.1 GB Overwrite/Upgrade installation(Windows): When Deployment Manager is used : 0.9 GB When Deployment Manager is not used : 0.7 GB New installation(Linux): 5.0 GB Overwrite/Upgrade installation(Linux): 0.7 GB Recommended: 20.5 GB
Monitor	XGA (1024 x 768 resolution) or higher
LAN card	10/100 Ethernet LAN card If the computer and the LAN cable are compatible with Gigabit Ethernet, you can use a Gigabit-class card.
DVD drive	Required for installation.

Note: Hitachi Command Suite products, including HCSM, cannot be installed on a disk that has a logical sector size of 4,096 bytes (4K native). If you are using a disk with a logical sector size of 4,096 bytes, change the logical sector size to 512 bytes, and then install the Hitachi Command Suite products.

Virtual memory requirements

If adequate virtual memory is not allocated on the management server, the Hitachi Command Suite products and any other installed programs might become unstable or might not start. To ensure stable operation of the management server, in addition to the virtual memory required for the operating system and other programs, the management server also requires additional virtual memory.

The following table shows the virtual memory requirements for each product and Common Component in this version.

Table 3 Virtual memory requirements for each product

Product name	Virtual memory requirement (MB)
Compute Systems Manager	When Deployment Manager is used : 6,400 When Deployment Manager is not used : 5,000
Device Manager[#1] Tiered Storage Manager Replication Manager[#3]	When the memory heap size for Device Manager is Small: 7,700 When the memory heap size for Device Manager is Medium: 8,200 When the memory heap size for Device Manager is Large: 9,200
Tuning Manager[#2]	4,000
Global Link Manager	1,000
Automation Director	7,000
Hitachi NAS Manager[#4]	512
Hitachi File Services Manager[#4]	1,024
Storage Navigator Modular 2[#4]	200
Common Component	2,501

Note: If you plan to install Compute Systems Manager, and if 1,000 MB of virtual memory is already used by the operating system and other programs, you must secure more than 8,501 MB of virtual memory.

5,000 (for Compute Systems Manager) + 2,501 (for Common Component) + 1,000 (already used virtual memory) = 8,501

#1:

If the Device Manager agent is installed on the management server, you must allocate additional virtual memory for it. Specify a value for the virtual memory of the Device Manager agent in the `server.agent.maxMemorySize` property.

#2:

If the Tuning Manager agent is installed on the management server, you must allocate additional virtual memory for it. For details on virtual memory requirements, see the description of memory requirements in the *Hitachi Command Suite Tuning Manager Installation Guide*.

#3:

If Replication Manager Application Agent is installed on the management server, you must allocate additional virtual memory for it. For details on virtual memory requirements, see the *Hitachi Command Suite Replication Manager Configuration Guide*.

#4:

The virtual memory requirements listed in the table are for Hitachi NAS Manager v6.4, Hitachi File Services Manager v3.0.1 and Storage Navigator Modular 2 v11.52. For details on the latest virtual memory requirements, see the documentation for each product.

Disk space requirements

Table 4 Disk space requirements (Windows)

Install type	Item	Default installation Folder	Required disk space
New	Installation folder for Common Component	*program-files-folder*\HiCommand\Base64[#1]	When using Deployment Manager: 2,400MB Without Deployment Manager: 2,100MB
	Installation folder for Compute Systems Manager	*program-files-folder*\HiCommand\ComputeSystemsManager	
	Installation folder for Deployment Manager	*program-files-x86-folder*\HiCommand\ComputeSystemsManager	
	Storage folder for Common Component[#2] database	*program-files-folder*\HiCommand\database\x64\SYS	1,000MB
		program-files-folder\HiCommand\database\x64\BASE	
	Storage folder for Compute Systems Manager database	*program-files-folder*\HiCommand\database\x64\HCSM	1,800MB

Install type	Item	Default installation Folder	Required disk space
	Temporary folder[#3]	`Folder specified by the environment variable TMP`	6,200MB
	Installation folder for Deployment Manager	*`system-drive`*`\Deploy`	200MB
	Installation folder for Deployment Manager SQL Server	`Folder used by SQL Server`	6,000MB
Overwrite /Upgrade	Installation folder for Compute Systems Manager	*`program-files-folder`*`\HiCommand\ComputeSystemsManager`	When using Deployment Manager: 900MB Without Deployment Manager: 700MB
	Installation folder for Deployment Manager	*`program-files-x86-folder`*`\HiCommand\ComputeSystemsManager`	
	Temporary folder[#3]	Folder specified by the environment variable TMP	10MB

Table 5 Disk space requirements (Linux)

Install type	Item	Default installation Directory	Required disk space
New	Installation directory for Common Component	`/opt/HiCommand/Base64`[#1]	2,100MB
	Installation directory for Compute Systems Manager	`/opt/HiCommand/ComputeSystemsManager`	
		`/opt/HiCommand/CSMUninstall`	
	Storage directory for Common Component[#2] database	`/var/opt/HiCommand/database/x64/SYS`	1,000MB
		`/var/opt/HiCommand/database/x64/BASE`	
	Storage directory for Compute Systems Manager database	`/var/opt/HiCommand/database/x64/HCSM`	1,800MB
	Temporary directory[#3]	`/tmp`	100MB
		`/var/tmp`	
Overwrite /Upgrade	Installation directory for Compute Systems Manager	`/opt/HiCommand/ComputeSystemsManager`	700MB
		`/opt/HiCommand/CSMUninstall`	
	Temporary directory[#3]	`/tmp`	10MB
		`/var/tmp`	

⚠ ***Note:***

- Note that the *program-files-folder*`\HiCommand and` *program-files-x86-folder*`\HiCommand(Windows) or` */opt*`/HiCommand(Linux)` portion of the path can be changed.
  Read this variable as the directory specified during installation.
- In Windows, *Program-files-folder* are the folders specified in the Windows environment variable `%ProgramFiles%`. *Program-files-x86-folder* are the folders specified in the Windows environment variable `%ProgramFiles(x86)%`. *System-drive* are the drive specified in the Windows environment variable `%SystemDrive%`.

#1:

If you are installing the Hitachi Command Suite in an environment in which the Common Component is already installed, install it on the same drive.

#2:

This is not required if a Hitachi Command Suite product v4.0 or later is already installed.

#3:

This is required only during installation and is unnecessary after installation.

Required drive space for backing up when installing v8

If you are installing any Hitachi Command Suite(#) v8 software on a system that is currently running v7 or earlier software, the first installation of any v8 product requires backing up all of the data before transferring it to the v8 environment. Therefore, the free space listed here is required in addition to the space listed in Table 4 and Table 5.

(#)The following v7 or earlier products require that you back up data before installing any v8 Hitachi Command Suite product:

- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Global Link Manager

Notes:

Do not delete data back up until you upgrade all existing software to v8.

After you finish all v8 upgrades, delete the backup data by removing the following files and folders:

- Remove the file defined as the "file" item and the folder defined as the exportdir item in the following file: <Program-Files>\HiCommand\backup\exportpath.txt

- Remove the exportpath.txt file.

The formula for calculating the required free disk space is as follows:

The formula for calculating the required free space for backing up is as follows:

(<Total-database-size of H-C-S-products>+ 2.5GB) x 2

It is only necessary to preserve the free space until after the first v8 installer finishes because the backup (including HCSM) already exists.

Calculation example: If you are currently running Systems Manager, Device Manager, Tiered Storage Manager and Replication Manager software on your system, you calculate the required by accumulating the capacities of the following directories:

- Database directory of Compute Systems Manager
- Database directory of Device Manager
- Database directory of Tiered Storage Manager
- Database directory of Replication Manager
- Database directories of HCS Common component: BASE and SYS directories.

Software requirements

The Hitachi Command Suite installation requires a computer that meets the following software requirements.

Operating system requirements

Table 6 Supported management server operating systems (Windows)

OS Name	OS Version	SP	Architecture
Windows Server 2008 R2 (#1)(#3)	Standard Enterprise Datacenter	SP1	x64
Windows Server 2012 (#2) (#3)	Standard Datacenter	No SP	x64
Windows Server 2012 R2 (#2) (#3)	Standard Datacenter	No SP	x64

(#1) Server core is not supported.

(#2) Server core and Minimal Server Interface is not supported.

(#3) Only HCSM distributed by Hitachi, Ltd. , not Hitachi Data Systems, supports Japanese OS.

Table 7 Supported management server operating systems (Linux)

OS Name	OS Version	SP	Architecture	Prerequisite package(#1)
Red Hat Enterprise Linux Server(#2)	6	-	x64	-
	6.1	-	x64	-
	6.2	-	x64	-
	6.3	-	x64	-
	6.4	-	x64	-
	6.5	-	x64	- upstart-0.6.5-13.el6_5.3.x86_64.rpm
	6.6	-	x64	-
	6.7	-	x64	-
	7.0	-	x64	- tcsh-6.18.01-7.el7.x86_64.rpm - glibc-2.17-55.el7.x86_64.rpm - glibc-2.17-55.el7.i686.rpm - libgcc-4.8.2-16.el7.x86_64.rpm - libstdc++-4.8.2-16.el7.x86_64.rpm - nss-softokn-freebl-3.15.4-2.el7.x86_64.rpm - alsa-lib-1.0.27.2-3.el7.x86_64.rpm - perl-5.16.3-283.el7.x86_64.rpm - net-tools-2.0-0.17.20131004git.el7.x86_64.rpm
	7.1	-	x64	
	7.2	-	x64	
SUSE Linux Enterprise Server(#2,#3)	11	SP3	x64	-
		SP4	x64	-
	12	no SP	x64	-
		SP1	x64	-

You cannot select the Minimum package option when installing Red Hat. If you select this option, HCSM cannot function properly because there is a lack of required functionality. Note that HCSM is tested using the default OS installation packages.

(#1) The RPM package(s) shown in the table (or a later version) must be applied. You can check the latest version of the RPM package on the Web site for your operating system.

(#2) Deployment Manager Plug-in is not supported.

(#3) LXC is not supported.

Kernel parameters and shell restrictions (Linux)

Before installing HCSM, you must set the appropriate values for kernel parameters and shell restrictions on Linux.

- Red Hat Enterprise Linux 6

  Set the kernel parameters in the /etc/sysctl.conf and the restrictions in the /etc/security/limits.conf and /etc/security/limits.d/90-nproc.conf files.

- Red Hat Enterprise Linux 7

  Set the kernel parameters in the /etc/sysctl.conf and the restrictions in the /etc/security/limits.conf and /etc/security/limits.d/20-nproc.conf files.

- SUSE Linux Enterprise Server

  Set the kernel parameters in the /etc/sysctl.conf and the shell restrictions in the /etc/security/limits.conf files.

Recommended /etc/sysctl.conf values(Red Hat Enterprise Linux 6)

The kernel parameter values to be set in the /etc/sysctl.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product to be used.

The following tables show the kernel parameter values you must set. The formulas for calculating these values follow the tables.

Kernel Parameter	**HiRDB**	**Common Component**	**Operating System Initial Value**	**Compute Systems Manager**
fs.file-max	42276	42276	99483	162478
kernel.threads-max	576	142	16384	453
kernel.msgmni	44	44	1978	44
4th parameter of kernel.sem	1024	9	128	10
2nd parameter of kernel.sem	7200	80	32000	144
kernel.shmmax	200000000	24372224	4294967295	421699584
kernel.shmmni	2000	0	4096	995
kernel.shmall	24372224	23793664	268435456	458306560

These formulas are for calculating kernel parameter values:

- For kernel.shmmax:

```
kernel-parameter-value-to-be-set =
Max{
  Max{
      value-that-is-enabled-in-the-system
      ,
      initial-value-of-the-OS
    }
   ,
   value-for-Common-Component
   + value-for-Compute-Systems-Manager
   + value-for-other-HCS-products
   ,
   value-for-HiRDB
   }

- For kernel.shmall:
  kernel-parameter-value-to-be-set =
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  + value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  + value-for-HiRDB

- Other kernel parameters and shell restrictions:
  kernel-parameter-value-to-be-set =
  Max{
    Max{
      value-that-is-enabled-in-the-system
      ,
      initial-value-of-the-OS
    }
   + value-for-Common-Component
   + value-for-Compute-Systems-Manager
```

```
    + value-for-other-HCS-products
    ,
    value-for-HiRDB
}
```

Note: Max{x, y, z} indicates the maximum value among x, y, and z.

Recommended /etc/sysctl.conf values(Red Hat Enterprise Linux 7)

The kernel parameter values to be set in the /etc/sysctl.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product to be used.

The following tables show the kernel parameter values you must set. The formulas for calculating these values follow the tables.

Kernel Parameter	HiRDB	Common Component	Operating System Initial Value	Compute Systems Manager
fs.file-max	42276	42276	99483	162478
kernel.threads-max	576	142	16384	453
kernel.msgmni	44	44	1978	44
4th parameter of kernel.sem	1024	9	128	10
2nd parameter of kernel.sem	7200	80	32000	144
kernel.shmmax	200000000	24372224	4294967295	421699584
kernel.shmmni	2000	0	4096	995
kernel.shmall	24372224	23793664	268435456	458306560

These formulas are for calculating kernel parameter values:

- For kernel.shmmax:

```
kernel-parameter-value-to-be-set =
Max{
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
    }
   ,
   value-for-Common-Component
   + value-for-Compute-Systems-Manager
   + value-for-other-HCS-products
   ,
   value-for-HiRDB
   }

- For kernel.shmall:
  kernel-parameter-value-to-be-set =
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  + value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  + value-for-HiRDB

- Other kernel parameters and shell restrictions:
  kernel-parameter-value-to-be-set =
  Max{
    Max{
      value-that-is-enabled-in-the-system
      ,
      initial-value-of-the-OS
    }
   + value-for-Common-Component
   + value-for-Compute-Systems-Manager
   + value-for-other-HCS-products
   ,
   value-for-HiRDB
```

```
}
```

Note: Max{x, y, z} indicates the maximum value among x, y, and z.

Recommended /etc/security/limits.conf values(Red Hat Enterprise Linux 6)

The shell restriction values to be set in the /etc/security/limits.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product to be used. The shell restriction values must be set for both soft and hard. The value for soft must be less than the value for hard.

The following tables show the shell restriction values you must set. The formula for calculating these values follow the tables.

Shell Restriction	**HiRDB**	**Common Component**	**Operating System Initial Value**	**Compute Systems Manager**
nofile (soft/hard)	8192	1346	4096	528

The following formula is for calculating the values for the shell restriction:

```
  shell-restrictions-value-to-be-set =
  Max{
    Max{
      value-that-is-enabled-in-the-system
      ,
      initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Compute-Systems-Manager
    + value-for-other-HCS-products
    ,
    value-for-HiRDB
}
```

Recommended /etc/security/limits.conf values (Red Hat Enterprise Linux 7)

The shell restriction values to be set in the /etc/security/limits.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product to be used. The shell restriction values must be set for both soft and hard. The value for soft must be less than the value for hard.

The following tables show the shell restriction values you must set. The formula for calculating these values follow the tables.

Shell Restriction	HiRDB	Common Component	Operating System Initial Value	Compute Systems Manager
nofile (soft/hard)	8192	1346	4096	528

The following formula is for calculating the values for the shell restriction:

```
 shell-restrictions-value-to-be-set =
 Max{
   Max{
     value-that-is-enabled-in-the-system
     ,
     initial-value-of-the-OS
   }
   + value-for-Common-Component
   + value-for-Compute-Systems-Manager
   + value-for-other-HCS-products
   ,
   value-for-HiRDB
}
```

Recommended /etc/security/limits.d/90-nproc.conf (Red Hat Enterprise Linux 6)

The shell restriction values to be set in the /etc/security/limits.d/90-nproc.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product to be used. The shell restriction values must be set for both soft and hard. The value for soft must be less than the value for hard.

The following tables show the shell restriction values you must set. The formula for calculating these values follow the tables.

Shell Restriction	HiRDB	Common Component	Operating System Initial Value	Compute Systems Manager
nproc (soft/hard)	512	198	8192	50

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  + value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  ,
  value-for-HiRDB
}
```

Note: Max{x, y} indicates the larger value of x or y.

Recommended /etc/security/limits.d/20-nproc.conf (Red Hat Enterprise Linux 7)

The shell restriction values to be set in the /etc/security/limits.d/20-nproc.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product to be used. The shell restriction values must be set for both soft and hard. The value for soft must be less than the value for hard.

The following tables show the shell restriction values you must set. The formula for calculating these values follow the tables.

Shell Restriction	**HiRDB**	**Common Component**	**Operating System Initial Value**	**Compute Systems Manager**
nproc (soft/hard)	512	198	8192	50

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  + value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  ,
  value-for-HiRDB
}
```

Note: Max{x, y} indicates the larger value of x or y.

Recommended SUSE Linux Enterprise Server /etc/sysctl.conf values

The kernel parameter values to be set in the /etc/sysctl.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product to be used.

The following tables show the kernel parameter values you must set. The formulas for calculating these values follow the tables.

Kernel Parameter	HiRDB	Common Component	Operating System Initial Value	Compute Systems Manager
fs.file-max	42276	42276	50525	162478
kernel.threads-max	576	142	8192	453
kernel.msgmni	44	44	16	44
4th parameter of kernel.sem	1024	9	1024	10
2nd parameter of kernel.sem	7200	80	256000	144
kernel.shmmax	200000000	24372224	4294967295	421699584
kernel.shmmni	2000	0	4096	995
kernel.shmall	24372224	23793664	268435200	458306560

The following formulas are for calculating the values for the kernel parameters:

- For kernel.shmmax:

```
kernel-parameter-value-to-be-set =
Max{
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  ,
  value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  ,
  value-for-HiRDB
}
```

- For kernel.shmall:

```
kernel-parameter-value-to-be-set =
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  + value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  + value-for-HiRDB
```

- Other kernel parameters and shell restrictions:

```
kernel-parameter-value-to-be-set =
Max{
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  + value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  ,
  value-for-HiRDB
}
```

Note: Max{x, y, z} indicates the maximum value among x, y, and z.

Recommended SUSE Linux Enterprise Server /etc/security/limits.conf values

The shell restriction values set in the /etc/security/limits.conf file are calculated based on the default value of the operating system or the setting values of the Hitachi Command Suite product in use. The shell restriction values must be set for both soft and hard. The soft value must be less than the hard value.

The following tables show the shell restrictions values you must set. The formula for calculating these values follows the tables.

Shell Restriction	**HiRDB**	**Common Component**	**Operating System Initial Value**	**Compute Systems Manager**
nofile (soft/hard)	8192	1346	1024	528
nproc (soft/hard)	512	198	4096	50

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
  Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
  }
  + value-for-Common-Component
  + value-for-Compute-Systems-Manager
  + value-for-other-HCS-products
  ,
  value-for-HiRDB
}
```

Note: Max{x, y} indicates the larger value of x or y.

Prerequisite software for Deployment Manager

The following table lists the Deployment Manager prerequisite software.

Table 8 Deployment Manager Prerequisite Software

OS Name	Prerequisite programs
Windows Server 2008 R2	- .NET Framework 3.5.1 (#3) (#5) - .NET Framework 4.5.2, 4.6.0 or 4.6.1 (#1) (#5) - Windows Installer 5.0 (#3) - SQL Server 2014 Express x64(#2) (#6) - Internet Information Services 7.5 (#4)
Windows Server 2012	- .NET Framework 3.5.1 (#3) (#5) - .NET Framework 4.5.2, 4.6.0 or 4.6.1 (#1) (#5) - Windows Installer 5.0 (#3) - SQL Server 2014 Express x64(#2) (#6) - Internet Information Services 8 (#4)
Windows Server 2012 R2	- .NET Framework 3.5.1 (#3) (#5) - .NET Framework 4.5.2, 4.6.0 or 4.6.1 (#1) (#5) - Windows Installer 5.0 (#3) - SQL Server 2014 Express x64(#2) (#6) - Internet Information Services 8.5 (#4)

(#1) .NET Framework 4.5.2 is located on the DVD media.

(#2) This software is located on the DVD media and installed automatically during the Deployment Manager new installation.

(#3) This software is included with the operating system.

(#4) If you install Internet Information Services (IIS) 7.5, "Static Content", "ASP.NET","IIS Management Console", and "IIS 6 Metabase Compatibility" must be enabled. If you install IIS 8.0 or 8.5, "Static Content", "ASP.NET 4.5","IIS Management Console", and "IIS 6 Metabase Compatibility" must be enabled.

(#5) CCATS number G076405 is assigned for .NET Framework (Mass Market).

(#6) CCATS number G065307 is assigned for SQL Server 2014 Express (Mass Market).

Installed software

The following software is installed automatically during the HCSM installation. When you remove the HCSM software, the following software is not removed. After you remove the HCSM software, you must manually delete the following software if it is no longer required for other components.

	Software	Type	Version	Remarks
For Windows	Visual C++ 2008 SP1 Redistributable Package	x86	9.0.30729.17	
		x64	9.0.30729.17	
	Visual C++ 2010 SP1 Redistributable Package	x86	10.0.40219.1	
		x64	10.0.40219.1	
	Visual C++ 2013 Redistributable Package	X86	12.0.21005.1	Installed with Deployment Manager only.

Related Software

Oracle JDK

You can change the version of Oracle JDK that you use with HCSM after installation. HCSM supports the following Oracle JDK versions:

JDK 8 (1.8.0)

External authentication (LDAP) server

The following table lists the supported Authentication methods for using an external authentication server.

Table 9 Requirements when linking to an external authentication server

Authentication method	Requirements
LDAP	The software in use must comply with LDAP v3.

HCS Products

[Windows version of HCSM]

- When using HCSM v8.2.1 or later on a computer on which other HCS products (*) exist, you must upgrade all other HCS products to v8.1.0 or later.

(*) Other HCS products include the following:

- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Global Link Manager

[Red Hat Enterprise Linux version of HCSM]

- When using HCSM v8.2.1 or later on a computer on which other HCS products (*) exist, you must upgrade all other HCS products to v8.1.0 or later.

(*) Other HCS products include the following:

- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager

[SUSE Linux Enterprise Server version of HCSM]

If other HCS products are installed on the server on which you plan to install HCSM, you must first upgrade the HCS products to version 8.0.1 or later. For details about how to install HCSM, see the Readme.txt file included with the installation media.

Device Manager

When you install HCSM in an environment that uses HCS products, you can centrally manage and operate storage and server resources.

If you install HCSM on the same server as HCS, management operation efficiency is improved because host information for resources managed by HCSM and by the Hitachi Device Manager is automatically synchronized.
Note: Only Windows and Linux hosts can be synchronized.

In addition, HCSM can refer to storage information that is managed by Hitachi Device Manager.
However, to acquire a storage system list, Hitachi Device Manager v8.1.2 or later is required.

Management target requirements

Hardware Requirements

The following table lists the supported firmware versions for Hitachi Compute Blades and Hitachi Compute Rack servers.

Table 10 Firmware versions - Compute Blade and Rack-mounted Servers

Hardware name		Firmware version
Hitachi Compute Blade 500	management module firmware	A0280 or later (A0290 or later #5)
	LPAR manager firmware	01-80 or later (02-25 or later #3) (02-27 or later #4)
Hitachi Compute Blade 2000	management module firmware	A0365 or later (A0375 or later #1,#2)
	LPAR manager firmware	59-60 or later (59-70 or later #1,#2)
Hitachi Compute Blade 2000 MP	management module firmware	A0365 or later (A0375 or later #1,#2)
	LPAR manager firmware	79-60 or later (79-70 or later #1,#2)
Hitachi Compute Blade 2500	management module firmware	A0145 or later (A0150 or later #5)
	LPAR manager firmware	02-00 or later (02-25 or later #3) (02-27 or later #4)
Hitachi Compute Rack	CR220HM CR220SM CR210HM	09.48 or later

(#1) If you display SR-IOV, use this firmware.

(#2) If you change SR-IOV settings, use this firmware.

(#3) If you use HBA Core Dedicated Mode, use this firmware.

(#4) If you use LPAR Manager Enterprise license, use this firmware.

(#5) Use the version of firmware within the described range for using LPAR manager firmware version 02-45 or later

Software requirements

This section provides system requirements for Management targets.

Operating system requirements

The following table lists the supported operating systems for management targets.

Table 11 Supported management target OSs (Windows)

OS Name	OS Version	SP	Architecture
Windows Server 2008 (#1) (#3)	Standard 32-bit Edition Enterprise 32-bit Edition Datacenter 32-bit Edition Standard without Hyper-V 32-bit Edition Enterprise without Hyper-V 32-bit Edition Datacenter without Hyper-V 32-bit Edition	No SP	x86
		SP1	x86
		SP2	x86
	Standard Edition Enterprise Edition Datacenter Edition Standard without Hyper-V Edition Enterprise without Hyper-V Edition Datacenter without Hyper-V Edition	No SP	x64
		SP1	x64
		SP2	x64
Windows Server 2008 R2 (#1) (#3) (#4)	Standard Enterprise Datacenter	No SP	x64
		SP1	x64
Windows Server 2012 (#2) (#3) (#4)	Standard Datacenter	No SP	x64
Windows Server 2012 R2 (#2) (#3) (#4)	Standard Datacenter	No SP	x64

(#1) Server core isn't supported.

(#2) Server core and Minimal Server Interface is not supported.

(#3) Master image deploy and snapshot is not supported in Hyper-V environments.

(#4) Deployment Manager functions are not supported in native VHD boot environments.

(#5) Linux version HCSM is not supported.

Table 12 Supported management target OSs (Linux)

OS Name	OS Version	SP	Architecture	Prerequisite package
Red Hat Enterprise Linux Red Hat Enterprise Linux Advanced Platform	5	-	x86	iscsi-initiator-utils device-mapper sysstat
			x64	
	5.1	-	x86	iscsi-initiator-utils sysstat
			x64	
	5.2	-	x86	
			x64	
	5.3	-	x86	
			x64	
	5.4	-	x86	
			x64	
	5.5	-	x86	
			x64	
	5.6	-	x86	sysstat
			x64	
	5.7	-	x86	
			x64	
	5.8	-	x86	
			x64	
	5.9	-	x86	
			x64	
	5.10	-	x86	
			x64	
	5.11	-	x86	
			x64	
	6.0	-	x86	iscsi-initiator-utils pciutils device-mapper-multipath sysstat samba-common dmidecode nfs-utils smartmontools
			x64	
	6.1	-	x86	iscsi-initiator-utils pciutils device-mapper-multipath sysstat samba-common nfs-utils smartmontools
			x64	
	6.2	-	x86	
			x64	
	6.3	-	x86	
			x64	
	6.4	-	x86	
			x64	
	6.5	-	x86	
			x64	
	6.6	-	x86	
			x64	
	6.7	-	x86	

OS Name	OS Version	SP	Architecture	Prerequisite package
			x64	
	7.0	-	x64	net-tools iscsi-initiator-utils pciutils device-mapper-multipath bzip2 sysstat samba-common nfs-utils smartmontools
	7.1	-	x64	
	7.2	-	x64	net-tools iscsi-initiator-utils pciutils device-mapper-multipath bzip2 sysstat samba-common-tools nfs-utils smartmontools
SUSE Linux Enterprise Server (#1)	11	No SP	x86	open-iscsi sysstat nfs-kernel-server
			x64	
		SP1	x86	
			x64	
		SP2	x86	
			x64	
		SP3	x86	
			x64	
		SP4	x86	sysstat nfs-kernel-server
			x64	
	12	No SP	x64	sysstat
		SP1	x64	
Oracle Enterprise Linux (#2)	5.5	-	x86	iscsi-initiator-utils sysstat
			x64	
Oracle Linux (#2)	6	-	x86	iscsi-initiator-utils pciutils device-mapper-multipath sysstat samba-common dmidecode nfs-utils smartmontools
			x64	
	6.1	-	x86	
			x64	
	6.2	-	x86	
			x64	
	6.3	-	x86	
			x64	
	6.4	-	x86	
			x64	
	6.5	-	x86	
			x64	
	6.6	-	x86	
			x64	
	6.7	-	x86	
			x64	
	7.0	-	x64	net-tools iscsi-initiator-utils pciutils
	7.1	–	x64	

OS Name	OS Version	SP	Architecture	Prerequisite package
				device-mapper-multipath bzip2 sysstat samba-common nfs-utils smartmontools
	7.2	–	x64	net-tools iscsi-initiator-utils device-mapper-multipath bzip2 sysstat samba-common-tools nfs-utils smartmontools

You cannot select the Minimum package option when installing Linux. If you select this option, HCSM cannot function properly because there is a lack of required functionality. Note that HCSM is tested using the default OS installation packages.

(#1) Only Full Sector is supported for Deployment Manager System-level Backup and Snapshot.

(#2) Deployment Manager is not supported.

Table 13 Supported management target OSs (Solaris)

OS Name	OS Version	Architecture	SP
Solaris (#1)(#2)(#3)	10	x64	1/13(10.11)
	11.1	x64	-

Note that HCSM is tested using the default OS installation packages.

(#1) Master image deploy and snapshot is not supported.

(#2) Only Full Sector is supported in System-level Backup.

(#3) Deployment Manager's functions are supported only LPAR or VM environment.

Table 14 Supported management target OSs (VMware ESXi)

OS Name	OS Version	Update	Architecture
VMware ESXi (#1)	5.0	no update update1 update2 update3	-
	5.1	no update update1 update2 update3	-
	5.5	no update update1 update2 update3	
	6.0	no update update1 update2	

(#1) VMware vSphere Hypervisor (free edition) is not supported.

GUI requirements

Compute Systems Manager GUI requirements

Table 15 and Table 16 list the supported operating systems and Web browsers for using this version of the Compute Systems Manager GUI. Adobe Flash Player (latest version) is required for all browsers.

JRE 6.0 Update 29 or later is required to manage the Hitachi Compute Blade Server family. For details, refer to the following Hitachi Compute Blade Server documents:

- Hitachi Compute Blade 500 Series Web Console User's Guide

- Hitachi Compute Blade 500 Series Remote Console User's Guide

- Hitachi Compute Blade 2000 User's Guide

- Hitachi Compute Blade 2500 Series Management Module User Guide

JRE 7 (Update 2 or later) is required to manage the Hitachi Compute Rack Server family. For details, refer to the following Hitachi Compute Rack Server documents:

- Hitachi Compute Rack 210H/220H Remote Management User's Guide

- Hitachi Compute Rack 220S Remote Management User's Guide

Table 15 Supported GUI Environments (Windows)

OS Name	OS Version	SP	Architecture	Web browser
Windows Server 2008 (#1)	Standard 32-bit Edition Enterprise 32-bit Edition Datacenter 32-bit Edition Standard without Hyper-V 32-bit Edition Enterprise without Hyper-V 32-bit Edition Datacenter without Hyper-V 32-bit Edition	SP2	x86	IE9 or later
	Standard Edition Enterprise Edition Datacenter Edition Standard without Hyper-V Edition Enterprise without Hyper-V Edition Datacenter without Hyper-V Edition	SP2	x64	IE9 or later
Windows Server 2008 R2 (#1)	Standard Enterprise Datacenter	SP1	x64	IE11 or later
Windows Server 2012 (#2)	Standard Datacenter	No SP	x64	IE10 or later(#3)
Windows Server 2012 R2 (#2)	Standard Datacenter	No SP	x64	IE11 or later(#3)
Windows Vista	Business Edition Enterprise Edition Ultimate Edition	SP2	x86	IE9 or later
			x64	IE9 or later

OS Name	OS Version	SP	Architecture	Web browser
Windows 7	Professional Enterprise Ultimate	SP1	x86	IE11 or later
			x64	IE11 or later
Windows 8.1	Pro Enterprise	No SP	x86	IE11 or later (#3) Chrome for Work(#4)
			x64	IE11 or later (#3) Chrome for Work(#4)
Windows 10	Home Pro Enterprise	No SP	x86	IE11 or later (#3) Chrome for Work(#4)
			x64	IE11 or later (#3) Chrome for Work(#4)

(#1) Server core is not supported.

(#2) Server core and Minimal Server Interface is not supported.

(#3) Metro Version is not supported.

(#4) Use the latest version of Chrome for Work.

Table 16 Supported GUI Environments (Linux)

OS Name	OS Version	SP	Architecture	GUI
Red Hat Enterprise Linux	6	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	6.1	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	6.2	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	6.3	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	6.4	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	6.5	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	6.6	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	6.7	-	x86	Firefox ESR38 and ESR45
			x64	Firefox ESR38 and ESR45(#5)
	7.0	-	x64	Firefox ESR38 and ESR45(#5)
	7.1	-	x64	Firefox ESR38 and ESR45(#5)

OS Name	OS Version	SP	Architecture	GUI
	7.2	-	x64	Firefox ESR38 and ESR45(#5)
SUSE Linux Enterprise Server	11	SP2	x86	Firefox ESR38
		SP3	x86	Firefox ESR38
			x64	Firefox ESR38(#5)
		SP4	x86	Firefox ESR38
			x64	Firefox ESR38(#5)
	12	No SP	x64	Firefox ESR38 and ESR45(#5)
		SP1	x64	Firefox ESR38 and ESR45(#5)

(#5) Only the 64 bit version browser is supported.

Compute Systems Manager CLI requirements

Platforms for Compute Systems Manager CLI and the Java Runtime Environment

Table 17 and Table 18 list platforms on which the Compute Systems Manager CLI runs and the supported Java Runtime Environment (JRE) versions.

Table 17 Supported Environments for using HCSM CLI (Windows)

OS Name	OS Version	SP	Architecture	Java Runtime Environment
Windows Server 2008 (#1)	Standard 32-bit Edition Enterprise 32-bit Edition Datacenter 32-bit Edition Standard without Hyper-V 32-bit Edition Enterprise without Hyper-V 32-bit Edition Datacenter without Hyper-V 32-bit Edition	SP2	x86	JRE 8.0
	Standard Edition Enterprise Edition Datacenter Edition Standard without Hyper-V Edition Enterprise without Hyper-V Edition Datacenter without Hyper-V Edition	SP2	x64	JRE 8.0
Windows Server 2008 R2 (#1)	Standard Enterprise Datacenter	SP1	x64	JRE 8.0
Windows Server 2012 (#2)	Standard Datacenter	No SP	x64	JRE 8.0
Windows Server 2012 R2 (#2)	Standard Datacenter	No SP	x64	JRE 8.0
Windows Vista	Business Edition Enterprise Edition Ultimate Edition	SP2	x86	JRE 8.0
			x64	JRE 8.0
Windows 7	Professional Enterprise Ultimate	SP1	x86	JRE 8.0
			x64	JRE 8.0
Windows 8.1	Pro Enterprise	No SP	x86	JRE 8.0
			x64	JRE 8.0
Windows 10	Home Pro Enterprise	No SP	x86	JRE 8.0
			x64	JRE 8.0

(#1) Server core is not supported.

(#2) Server core and Minimal Server Interface is not supported.

Table 18 Supported Environments for using HCSM CLI(Linux)

OS Name	OS Version	SP	Architecture	Java Runtime Environment
Red Hat Enterprise Linux	6	-	x86	JRE 8.0
			x64	JRE 8.0
	6.1	-	x86	JRE 8.0
			x64	JRE 8.0
	6.2	-	x86	JRE 8.0
			x64	JRE 8.0
	6.3	-	x86	JRE 8.0
			x64	JRE 8.0
	6.4	-	x86	JRE 8.0
			x64	JRE 8.0
	6.5	-	x86	JRE 8.0
			x64	JRE 8.0
	6.6	-	x86	JRE 8.0
			x64	JRE 8.0
	6.7	-	x86	JRE 8.0
			x64	JRE 8.0
	7.0	-	x64	JRE 8.0
	7.1	-	x64	JRE 8.0
	7.2	-	x64	JRE 8.0
SUSE Linux Enterprise Server	11	SP3	x86	JRE 8.0
			x64	JRE 8.0
		SP4	x86	JRE 8.0
			x64	JRE 8.0
	12	No SP	x64	JRE 8.0
		SP1	x64	JRE 8.0

License keys

You must register Plug-in licenses to use specific HCSM functions.

Firmware levels

None

Resolved problems

From 8.4.1-00 to 8.4.1-01

No.	Corrected Problems	Applied products	Applied OS
1	The following problem has been corrected: Discovery or Refresh for Linux host fails with KASV30029-E	Compute Systems Manager SD-EN-HCSM-142	Windows Linux

From 8.4.0-00 to 8.4.1-00

No.	Corrected Problems	Applied products	Applied OS
11	The following problem has been corrected: Registering a refresh or power management task takes a long time.	Compute Systems Manager SD-EN-HCSM-138	Windows Linux
2	The following problem has been corrected: In an environment in which HCSM 8.x is installed, the upgrade installation from HCS 7.x products other than HCSM fails. Also, HCS products other than HCSM 8.x are removed and starting the HiRDB service fails.	Compute Systems Manager SD-EN-HICMD-181	Windows
3	The following problem has been corrected: Tasks in the "Waiting" or "In Progress" status do not end.	Compute Systems Manager SD-EN-HCSM-135	Windows Linux
4	The following problem has been corrected: Malicious third parties can get session information illegally.	Compute Systems Manager	Windows Linux
5	The following problem has been corrected: The OK button is deactivated after clicking Remove in the Add Dedicated NIC dialog box.	Compute Systems Manager SD-EN-HCSM-137	Windows Linux
6	The following problem has been corrected: In the Edit LPAR Dedicated NIC Settings Screen, after deleting any of the Dedicated NICs assigned to an LPAR, all Dedicated NICs are unintentionally deleted.	Compute Systems Manager SD-EN-HCSM-136	Windows Linux
7	The following problem has been corrected: Clicking OK on the Assign User Groups screen causes an unexpected error (KASV40001-E).	Compute Systems Manager SD-EN-HCSM-140	Windows Linux
8	The following problem has been corrected: An operation for an LPAR host fails.	Compute Systems Manager	Windows Linux

		SD-EN-HCSM-141	
9	The following problem has been corrected: After a power management task is registered, the role change for a blade is not checked, and a power task runs.	Compute Systems Manager	Windows Linux
10	The following problem has been corrected: Authorization groups are displayed in User Groups even after the external authorization server connection is terminated.	Compute Systems Manager	Windows Linux
11	The following problem has been corrected: Authorization group names that include escape characters are added and displayed	Compute Systems Manager	Windows Linux

From 8.2.1-01 to 8.4.0-00

No.	Corrected Problems	Applied products	Applied OS
12	The following problem has been corrected: When a blade in an SMP configuration is registered in an N+M cold standby group, the warning alert that lists the N+M configuration change (alert Id:0x1100) does not appear.	Compute Systems Manager SD-EN-HCSM-130	Windows Linux
13	The following problem has been corrected: When upgrading to v8.2.0 or later in an environment in which HCSM v7.x is installed in a path other than the default path, a Cluster Settings screen is incorrectly displayed and the installation cannot proceed.	Compute Systems Manager SD-EN-HCSM-131	Windows
14	The following problem has been corrected: The HCSM service stops responding when an attempt is made to register a task and register, edit, or delete a resource group at the same time	Compute Systems Manager SD-EN-HCSM-133	Windows Linux
15	The following problem has been corrected: Some Hitachi Command Suite products contain a Server-Side Request Forgery (SSRF) vulnerability (CVE-2015-5255).	Compute Systems Manager SD-EN-HICMD-171	Windows Linux
16	The following problem has been corrected: Malicious third parties can obtain session information illegally.	Compute Systems Manager	Windows Linux
17	The following problem has been corrected: Some Hitachi Command Suite products contain a vulnerability that allows unauthorized execution of commands.	Compute Systems Manager SD-EN-HICMD-182	Windows Linux
18	The following problem has been corrected: BMC initialization on a blade causes task errors or incorrect removal from deployment targets.	Compute Systems Manager SD-EN-HCSM-134	Windows Linux

19	The following problem has been corrected: Power capping tasks for multiple chassis fails.	Compute Systems Manager	Windows Linux
20	The following problem has been corrected: In the detailed information window for a virtual machine, the hypervisor IP address is incorrectly displayed as the IP address of a physical adapter. To check the IP address of the hypervisor, see the detailed information window for the host.	Compute Systems Manager	Windows Linux

Known problems

- Keyboard operations are disabled on tables with embedded radio buttons because the HCSM Server misunderstands the selected items when a keyboard is used.
- When the following conditions are met, the *Used Capacity* and *Available Capacity* values of the network drive allocated to managed Host A are not displayed correctly (SD CR#: 8181):

  (1)The folder, to which Disk Quota is set, is network-shared with Host B (Windows).

  (2) The network shared folder in (1) is allocated to the network drive in Host A (Windows).
- When the managed host is Windows and multiple IP addresses are mapped in the network adapter, the correct relationship of the Port and Alias might not be displayed in [IP Network]-[Type] of the host information. (SD CR#: 8205)
- When creating or editing a performance profile, the screen becomes gray and may not continue operation. In this case, log in to HCSM again.
- The HCSM screen might become grayed out when the following operations are performed:
  - Displaying the graph of Performance Data or Power Data multiple times.
  - Displaying the graph of Performance Data or Power Data with a long Display Time Range.

  In this case, log in to HCSM again.
- In some cases, the same host appears twice in the Resource Tab Host list. This situation can occur when you run the discovery task and specify an IP address range that includes a previously discovered host.

  When this situation occurs:
  - Each Refresh and Power-Management task can be executed from either host. However, alerts are received for the newly discovered host only.
  - Even after deleting the corresponding host, host information remains in the host list.

  - You cannot Manage, Unmanage, or Remove the hosts remaining in the host list.

  This situation occurs when all the following conditions exist:

  (1) An additional IP address is allocated to a previously discovered host.

  (2) A Refresh (including auto update) is not completed for the Host to which the IP address is added.

  (3) Discovery is run on an IP address range which includes the newly added IP address and the target criteria is set to "All."

  Therefore, when you add an IP address to a host that is already discovered in HCSM, you must also run Host Refresh (with Auto Refresh).

- The Deployment Manager process may fail if the task specifies more than 1000 Blades, Rack-mounted servers, or VMs as targets in a Deployment task.
- The restriction on modifying the LOM IP address:

  When modifying the LOM IP address that is used by the Scheduled Power Control task, the contents of the LOM IP address displayed on the Task Details screen is not updated.

  This occurs during the following operations.

  (1) When the scheduled task is any one of the following:

  - Power On task

  - Shutdown OS task

  - Reboot OS task

  - Force Power Off task

  (2) The LOM IP address currently used is changed after scheduling the task listed in step (1).

  (3) When you refer to the Task Details screen on the scheduled task of (1) or refer to the Task details screen after task execution, the displayed LOM IP address content is not updated, but the task is executed with the modified LOM IP address.

  To confirm whether the LOM IP address is updated, verify that the same LOM IP address displayed in the Hosts list of the Resource screen or the Set LOM screen.

- When a VMware High Availability (VMware HA) hypervisor is managed, the information of the virtual machine on which VMware FT is enabled is not displayed correctly. Therefore, do not use VMware FT.
- Do not run tasks other than refresh for ESXi and any virtual machine that uses vCloud, vApp. If you run other tasks, unexpected issues might occur in vCloud, vApp, and HCSM.
- The HCSM screen might be grayed out during the following tasks:
  - Displaying the View Topology dialog by clicking View Topology.
  - Displaying the View Topology dialog by selecting View Topology from the Actions menu.

  - Displaying the Detailed Alert Information dialog by clicking Respond to Alert.

  In this case, you must delete any unused virtual machines associated with Hyper-V or VMware hypervisors managed by HCSM. After deleting the unused machines, log in to HCSM again.

- When ESXi information is updated from HCSM when the VM configuration is changing, HCSM deletes the VM management information and the VM tasks fails. In this case, wait until the VM configuration information changes are complete, refresh the information, and then register the VM tasks again.
- Resource backup and restore settings are retained when backup or restore is run again. The Image file storage location and image file restoration paths are not reflected regardless of whether you changed the default image storage location path in the Deployment Setting screen. When running backup or restore after changing the image file storage location path, confirm the backup and restore settings.
- When the Deployment Manager installation is interrupted by another installation program in which you specified an installation path other than the default, the files that were installed during the first attempt remain in the path specified during the installation. This means that before you reinstall, you must delete any files that exist in the installation path specified during the original installation.
- Hyper-V management, which uses the Hyper-V Replica function of Hyper-V3.0, is not supported. When Hyper-V3.0 is set as a management target, HCSM displays the primary VM and replica VM as a single VM. In such cases, management cannot function correctly.
- The same Server is displayed multiple times in the Rack-mounted Server list on the Resource Tab.

  These symptoms may occur when all the following conditions are met:

  (1) The host that is operating on the rack-mounted server is the HCSM management target.

  (2) The rack-mounted server host IP address is modified.

  (3) The rack-mounted host is discovered by specifying the modified IP address.

  When these symptoms occur, delete the host IP address before making any address modifications.
- When the Deployment Manager installation is interrupted by other programs, the installed files remain in the path specified during the installation. In this case, run the installation again using the same path specified when the installation was interrupted.
- The number of plot data points is less than expected in the Power Monitoring Dashboard when all the following conditions are met:

  (1) The Power Monitoring Profile for Chassis/Blade or Rack-mounted server is registered.

  (2) Data Collection is enabled in the Power Monitoring Settings for Chassis/Blade or Rack-mounted servers.

(3) All Chassis is selected from the [Logical Group] drop down list in the Power Monitoring Dashboard.

- When a large amount of power data is retained, refreshing the Power Monitoring Dashboard may run slower. To resolve this problem, delete unnecessary old power data manually.
- When a large amount of power data is retained, refreshing the Power Data screen generates an error message with Message-ID: KASV50005-E. To resolve this problem, delete unnecessary old power data manually. There is no need to take the action recommended by the message displayed with this symptom.
- Deleting a large amount of performance or power data manually may generate an error with Message-ID: KASV50302-E. However, the deletion is successful. There is no need to take the action recommended by the message displayed with this symptom.
- Exporting a large amount of performance or power data may fail with a warning dialog. To resolve this problem, delete all unnecessary old performance or power data manually.
- There is incorrect message text in the following messages: KASV00222-E, KASV00223-E, KASV00224-E, and KASV00225-E. These messages may mention that shutting down an Active Blade has failed, however the target of the failed shut down is a Standby Blade.
- After running a task to turn off power on for a LPAR, the task to turn on power might successfully complete without confirming that the operating system started.
- When a Restore Assignment task is run for a blade in Failback Failed status, the status becomes Failover Successful. However, the detailed information in the balloon text displayed from the link from the status is not updated, and still shows information about the previous failure. Ignore the balloon text because the Restore Assignment task is finished.
- When HDvM coexists with HCSM on a management server and you run an Add Host task for a host running an operating system that is not supported by HCSM, HCSM fails to import the host information and the credential referred by the failed task cannot be deleted. (SD CR#: 14378)
- When a large amount of alert data is retained, clicking a pagination button to refer an alert may generate the error message with Message-ID: KASV00061-E in the All Alerts screen or the Unresolved Alerts screen. To avoid this problem, use the sort functionality or filter functionality to refer to an alert. There is no need to take the action recommended in the message.
- If you initialize a source or destination LPAR Manager configuration after LPAR migration, the hosts running on the migrated LPAR might be duplicated in the hosts list on the Resources tab. In this case, remove the chassis that is (or was) associated with the duplicated hosts on the migrated LPAR, and then rediscover the chassis to correct the hosts list. (SD CR#: 14864)
- If a CSV file is output by selecting [Export to CSV] from the following windows, the extension of the file (.csv) might not be added. (SD CR#: 15506)

- Resources list

- Performance information

- Power monitoring data

- If the location of a logical group is changed, the location of the logical group displayed in the crumb trail might not change. This problem is only associated with the display of the crumb trail. The location of the logical group is changed accurately so you can use it without modification. (SD CR#: 14778)
- If the location hierarchy of the logical group is deep, the KASV50005-E error might occur. (SD CR#: 15456)
- If the window moves after using a keyboard operation, the KASV50005-E error might occur. In this case, use a mouse when making changes in the window. It is not necessary to deal with the KASV50005-E error. (SD CR#: 14974)
- An unavailable LPAR hosted on the removed blade is incorrectly displayed in the task target list. If you select the LPAR as a target of system-level backup or restore, snapshot, master image deployment, or disk configuration check, and then attempt to register a task, the KASV40001-E error occurs. To avoid the error, verify LPAR status on the list of licensed resources of Deployment Manager, and then perform a task for an LPAR that does not have NG status. (SD CR#: 14510)
- An HCSM operation for a virtual machine may fail with the KASV00275-E or KASV10205-E message, indicating that the virtual machine has been unmanaged or deleted, even though the virtual machine exists.
  Reregister the task, and then run it again.(SD CR#: 9737)
- If the locale of the operating system installed on the management server is set to Turkish, Azerbaijani, or Lithuanian, HCSM does not operate normally. If this problem occurs, an error message, such as KASV37301-E or KASV50014-E, is displayed.
  Install HCSM on a management server running an operating system for which the locale is not set to Turkish, Azerbaijani, or Lithuanian. (SD CR#: 16759)
- The displayed tooltip may remain on the screen. In this case, log in to HCSM again. (SD CR#: 7497,15190,17268)
- If HCSM retains a large number of alerts, the following problems might occur:
  - The KASV40001-E error occurs on the alert display screen and no alerts are displayed (SD CR#: 17842). If this problem occurs, reduce the number of alerts that HCSM retains.

  - The dashboard takes a long time to display the alert status report (SD CR#: 18436). If this problem occurs, reduce the number of alerts HCSM retains.

  To delete alerts, log in as a user who has the Admin role for all resources, and do the following:

  (1) In the **Administration** tab, select **System Settings**, and then display the **Alert** window.

(2) Click **Edit Settings** to open the Edit Alert Settings dialog box.

(3) In the Edit Alert Settings dialog box, specify the following settings:

- Select the **Use custom settings** radio button.
- **Maximum number of stored alerts**: 150000
- **Number of alerts to keep after deletion**: 100000
- Select the **Delete alerts immediately** check box.

(4) Click **OK**.

After you complete these steps, when the number of alerts exceeds 150,000, the system automatically reduces the number of alerts to approximately 100,000.

Although this process takes several minutes, you can continue to use HCSM in the meantime.

If a temporary measure to change properties files has already been taken, do the following to revert the property settings:

(1) Stop the HCSM server.

(2) Delete the properties from the following file.

File:

In Windows:

<HCSM-installation-folder>\ComputeSystemsManager\

system\sysconf\system.hcsm.properties

In Linux:

<HCSM-installation-directory>/ComputeSystemsManager/

system/sysconf/system.hcsm.properties

Properties:

modifier.alert.maxCount

modifier.alert.keepCount

(3) Start the HCSM server.

- A selection in a check box list may be lost and moved to different lines when a dialog box or balloon dialog box launched from a hyper link in the list is closed. (SD CR#:18589) If this problem occurs, select the necessary lines again.
- HCSM obtains the disk capacity of the Linux file system from the result of the df command; however, the result of the df command might differ from the actual value in the btrfs file system. Therefore, HCSM might not be able to correctly obtain the size, used space, and free space of the disk. (SD CR#: 18435)
- A Hypervisor running on an LPAR is not supported. When a Hypervisor in such a configuration is a management target of HCSM, an LPAR name with a link might be

displayed in the [VM or LPAR Name] column in the [Hypervisors] list on the Resource screen, but a screen transition using the link fails with the KASV50200-E error. So, do not click the link. (SD CR#: 19084)

- ESXi, which uses Virtual Volumes, cannot be managed in HCSM.
- Do not use vMotion across vCenter Server.
- ESXi, which uses VMware vCenter Site Recovery Manager or vSphere Replication, cannot be managed in HCSM.
- When a group selected in logical group tree is moved to other location by other user, KASV50200-E error may be displayed. In that case, select a group in logical group tree once again. (SD CR#: 17483)
- Exporting a large amount of performance or power data may take a long time without an error. Although you cancel the dialog, CSV Export operation continues. During the operation, you can continue to use HCSM for other operations, but you cannot stop HCSM service process. To stop HCSM service process, stop the OS that HCSM service is installed. (SD CR#: 19111)
- In a logical group created by specifying conditions, matching resources might not be displayed or resources that do not match the conditions might be displayed. To create a logical group, create it manually - not by specifying conditions. (SD CR#: 19008)
- If filtering was performed by applying the filter condition that was selected from the drop-down list, the drop-down list might display filter conditions that have no applicable values on the window. (SD CR#: 18031, 19332)
- If you add a virtual machine before MAC address information has been obtained to the licensed resources, the task fails with the KASV00028-E message. If this problem occurs, run **Refresh VMs** for the relevant virtual machine, make sure that the MAC address information is displayed in the **Network Settings** tab, and then add the virtual machine to the licensed resources.
- If the MAC address is not displayed even after you run **Refresh VMs**, start the virtual machine, and then run **Refresh VMs** again. (SD CR#: 19860)
- When all the following conditions are met, an association between a VMware ESXi and the server is not created, and the functions that are listed after the condition do not function correctly (SD CR#: 20117):

  (1) HCSM cannot acquire the serial number from VMware ESXi.
  If you access the following URL, and there are no data items or there are multiple ServiceTag data items in HostSystemIdentificationInfo[n].identifireType.key, HCSM fails to acquire the serial number. (If there is exactly one ServiceTag data item, this problem does not occur.)

  https://<ESXi IP Address>/mob/?moid=ha-host&doPath=hardware.systemInfo.otherIdentifyingInfo

  Note: To access this URL, user authentication is required. For authentication, use the user ID and password of a user who has management permission for the applicable instance of ESXi.

(2) The MAC addresses cannot be acquired from any of the NICs installed on the server. When the system uses Intel NICs the MAC addresses of NICs cannot be acquired.

- Features that do not function correctly when the previous conditions are met: GUI display – the relationship between the server and the VMware ESX/ESXi is not displayed
- N+M Cold Standby

  - Automated N+M Cold Standby testing cannot be used.

  - During an N+M Cold Standby switching a failure, the host is always forcibly powered off.

  - Automated shutdown processes that include a Failback task for the host do not run. The host must be shut down manually before running a Failback.
- Power control by specifying a host

  - Powering on a specified host is handled by WOL.

  - Forcibly powering off a specified host is not available.

- If you specified an image file with a path that includes " in the **Edit Backup Profile** or **Edit Snapshot Profile** dialog box and the specified file exists, when you run a task, the old image file might remain without being deleted.

  Examples: C:\DeployBackup\ServerA_BK.lbr and C:\DeployBackup\ServerA.BK.lbr

  This issue does not affect functionality, but unnecessary image files will consume disk capacity. Specify an image file whose path does not include ".". (SD CR#: 20308)

- Executing tasks for a same managed resource and/or the associated resources might rarely fail with KASV10079-E. When you meet the problem, refresh the target resources, and then verify the operation that you intended is succeeded.

  When the operation is verified, ignore the error. Otherwise execute the task again. If this problem persists, collect the manual of Compute Systems Manager, and then contact customer support.

Installation precautions

Management server

- Refer to the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.
- HDvM and HCSM must reside on the same server to remain synchronized.
- To install HCSM in an environment in which Remote Desktop Session Host is installed, use the following procedure:

  (1) At the command prompt, run `CHANGE USER /INSTALL`.

  (2) Install HCSM.

(3) At the command prompt, rune `CHANGE USER /EXECUTE`.

- If Deployment Manager and Compute Systems Manager software are already installed, neither is reinstalled or upgraded through the all-in-one Installer. To install these products, you must run the Hitachi Compute Systems Manager installer.
- After an installation or removal, a shortcut folder named “programs” might be incorrectly created under the Windows Start menu. This symptom is temporary, and the shortcut folder no longer appears after you log off and log on to Windows.
- Deployment Manager cannot be installed on a domain controller.
- After installing Deployment Manager on a server, do not promote that server to a domain controller. Deployment Manager cannot be installed if the disk on the installation destination is compressed or encrypted. If DPMDBI instance exists on SQL Server, Deployment Manager will overwrite that instance. Deployment Manager should not be installed in this condition.
- The ODBC data source entitled "DPM" is added to the system on which you install Deployment Manager. Do not install Deployment Manager on a system on which the data source entitled "DPM" is already installed by an application other than DPM.
- To install Deployment Manager in an environment in which Microsoft SQL Server is installed, set the startup type for SQL Server Browser to something other than Disable, and then install Deployment Manager. After installation is complete, change the startup type back to its original value.
- If you are upgrading from HCSM v7.5.1-01 or later, the existing SNMP Trap reception port setting might be erased. If SNMP Trap reception is enabled when you upgrade, you must enter a valid SNMP Trap reception port number on the advanced settings screen during the installation. If you do not enter a valid SNMP trap port number, the HCSM service receives SNMP traps using the default port number of 162.

  To specify a different port number after finishing the installation, complete the following procedure:

  (1) Stop the HCSM service and HCS services by selecting the following:

  Select Start > All Programs > Hitachi Command Suite >

  Compute Systems Manager > Stop - HCSM

  (2) Using a text editor, open the user.properties file in the HCSM property file folder (#1) and enter the SNMP Trap reception port number. The following example shows a case in which 22601 is set as the SNMP Trap reception port number.

```
#Hitachi Compute Systems Manager User Configuration File


snmp.trap.receive.port=22601
```

```
...
```

(3) If you stopped the services in the step 1, start the HCSM service and HCS services by selecting the following:

Select Start > All Programs > Hitachi Command Suite >

Compute Systems Manager > Start - HCSM

(#1) The location of the HCSM properties file folder depends on your environment.

The default folder on a system with C: as a system drive:

"C:\Program Files\HiCommand\ComputeSystemsManager\conf"

- Never stop the HiRDB/EmbeddedEdition _HD0 and HiRDB/EmbeddedEdition _HD1 services if the services are on the Windows [Service] window because these services must remain running.
- An installation of Hitachi Command Suite product v8 or later may take few hours in an environment that is running v7 or earlier products because backup data is processed for the existing products before the v8 upgrade process begins.
- To perform operations for a Tuning Manager server by remotely connecting to Device Manager in an environment in which Computes Systems Manager and Device Manager are installed on the same Linux machine, use Device Manager v8.1.1 or later. If you use a Device Manager earlier than v8.1.1, Tuning Manager server fails to start services with the KATN15014-E message.
- After installing HCSM in Red Hat Enterprise Linux 6.x, you cannot upgrade to Red Hat Enterprise Linux 7.x. Use the following procedure to upgrade the operating system.

  (1) Back up HCSM.

  (2) Uninstall HCSM.

  (3) Upgrade the operating system.

  (4) Install HCSM.

  (5) Restore the backed up settings and database.
- Before starting Automation Director in a cluster environment, complete the following tasks:

  - In the cluster management software, right-click to select the resource script and set its dependence on the [property]-[Dependencies] tab.

  - Specify [HAutomation Engine HCSclustergroup-name] to the resources that must be brought online before bringing the script online.
- If you used a version earlier than 8.4.0 linked with an external authorization server, use the following procedure to upgrade HCSM.

  (1) Before starting the upgrade, delete all tasks that are waiting to run.

  After the upgrade, you must re-register the tasks you deleted that were registered by external authorized users and waiting to run.. If not re-registered, the tasks do not run normally.

Note that the tasks that need re-registration are as follows:

- Powering ON, powering OFF, or restarting

  Hosts, virtual machines, servers, HVMs, and LPARs
- Updating information about managed objects

  Hosts, hypervisors, virtual machines, chassis, servers, and LPARs
- Updating performance information and power information

  Hosts, chassis, and servers

(2) Upgrade HCSM to the latest version

(3) After the upgrade, re-register the tasks that you deleted in Step (1).

(4) Log in to HCSM.

Use the external authorized HCSM user accounts to log in to HCSM. Logging in applies the account information of the external authorized users to HCSM. If you do not log in using the accounts, email notifications are not properly sent to the users.

You can check the list of the external authorized users who logged in to HCSM by selecting the **Administration** tab > **User Groups** > **External Authorized Users** tab.

- Before you start a new installation or upgrade installation on a machine that is also running Hitachi Replication Manager, you must complete the following tasks:
  - Verify the software versions running on the machine:

    Hitachi Replication Manager v8.0.0-00 to v8.4.0-00

    Hitachi Device Manager v8.0.0-00 to v8.4.0-00.
  - Complete one of the following procedures based on the server operating system:

    - For Linux servers, go to Linux Procedure.

    - For Windows servers, complete the following:

    Windows Procedure:

    1. If Device Manager is remotely linked with Tuning Manager, shut down the Tuning Manager server.
    2. Log in to Windows as the administrator.
    3. When installing Hitachi Command Suite in a cluster environment, take Hitachi Command Suite services offline. Then suppress failover of the resource group as described in the following section of the *Hitachi Command Suite Installation and Configuration Guide* depending on the version from which you are upgrading.

       - For v8.0.0-00 to v8.1.4-xx: “Suppressing failover when upgrading or overwriting Hitachi Command Suite (Windows)”

- For v8.2.0-00 or later: “Taking Hitachi Command Suite services offline (Windows)”

4. As administrator, access the Command Prompt and run the following commands in the order listed:

```
cd /d <Hitachi-Command-Suite-installation-folder>\Base64\bin
hcmds64srv /stop
hcmds64srv /statusall
hcmds64dbsrv /start
cd <Hitachi-Command-Suite-installation-folder>\Base64\sbin
hcmdsdbreclaim -k index -a -c dic
hcmdsdbreclaim -k index -j -c dic
hcmdsdbreclaim -k table -a -c dic
hcmdsdbreclaim -k table -j -c dic
```

Linux Procedure:

1. If Device Manager is remotely linked with Tuning Manager, shut down the Tuning Manager server.
2. Log in as root.
3. When installing Hitachi Command Suite in a cluster environment, delete the HCS product services from the Red Hat High Availability service group as described in the section "Deleting HCS product services from the service group (Red Hat Enterprise Linux)" in the *Hitachi Command Suite Installation and Configuration Guide*.
4. Start the terminal window and run the following commands in the order listed:

```
cd <Hitachi-Command-Suite-installation-directory>/Base64/bin
./hcmds64srv -stop
./hcmds64srv -statusall
./hcmds64dbsrv -start
cd <Hitachi-Command-Suite-installation-directory>/Base64/sbin
./hcmdsdbreclaim -k index -a -c dic
./hcmdsdbreclaim -k index -j -c dic
./hcmdsdbreclaim -k table -a -c dic
./hcmdsdbreclaim -k table -j -c dic
```

- To apply a service pack to an SQL Server used by Deployment Manager, use the following procedure:

Note: Before applying the service pack, visit Microsoft's download site for service pack installers to check the system requirements and other precautions.

(1) Confirm that no Deployment Manager tasks are running.

If a task is running, wait for the task to finish.

(2) Log in to the management server using an account with Administrator privileges.

(3) Stop the following services:

DeploymentManager API Service

DeploymentManager Backup/Restore Management

DeploymentManager Get Client Information

DeploymentManager PXE Management

DeploymentManager PXE Mtftp

DeploymentManager Remote Update Service

DeploymentManager Schedule Management

DeploymentManager Transfer Management

(4) Download a service pack installer from the Microsoft website, and run the installer to apply the service pack.

Note: Download and run a service pack installer, not an SQL Server Express main program installer.

Example: Installing SQL Server 2014 SP1

Installer for SQL Server 2014 SP1 (run either of these programs):

-> SQLServer2014SP1-KB3058865-x64-ENU.exe or

SQLServer2014SP1-KB3058865-x86-ENU.exe

Installer for SQL Server 2014 SP1 Express main program

(do not apply these programs):

-> SQLEXPR_x64_ENU.exe or SQLEXPR_x86_ENU.exe

(5) Start the services that you stopped in Step (3).

- To upgrade the SQL Server used by Deployment Manager to SQL Server 2014, use the following procedure:

  Note: Before upgrading, visit the following Microsoft page to check the system requirements and other precautions:

  https://technet.microsoft.com/en-us/library/ms144267%28v=sql.120%29.aspx

Note: If your current SQL Server Service Pack is not the latest version, upgrading to SQL Server 2014 might not be supported. In this case, apply the latest service pack before upgrading to SQL Server 2014.

(1) Confirm that no Deployment Manager tasks are running.

If a task is running, wait for the task to finish.

(2) Log in to the management server using an account with Administrator privileges.

(3) Stop the following services:

DeploymentManager API Service

DeploymentManager Backup/Restore Management

DeploymentManager Get Client Information

DeploymentManager PXE Management

DeploymentManager PXE Mtftp

DeploymentManager Remote Update Service

DeploymentManager Schedule Management

DeploymentManager Transfer Management

(4) When performing an upgrade, refer to the following Microsoft page:

http://technet.microsoft.com/ja-jp/library/ms144267.aspx

Note: To upgrade SQL Server Express (x86) running on an x64 OS to SQL Server 2014 Express, download SQLEXPR_x86 (which can be used for installation to either an x86 or x64 OS) from the Microsoft Download Center.

Note: When configuring the SQL Server installation center settings, take the following precaution:

- In the Select Instance window, select the instance of DPM (DPMDBI).

(5) Start the services that you stopped in Step (3).

CLI

Refer to the Hitachi Command Suite Compute Systems Manager CLI Reference Guide

Usage precautions

Note on registering multiple licenses

If multiple licenses are registered for a single plug-in, the system might display an error in the license information or on the dashboard. Ignore this error because the licenses are valid.

Note on the SNMP Trap version

HCSM supports SNMP Trap version v1/v2c only. V3 is not supported.

Note on changing the access port number of the HBase 64 Storage Mgmt Web Service

To change the access port number of the HBase 64 Storage Mgmt Web Service, do not specify the following ports:

1(tcpmux)

7(echo)

9(discard)

11(systat)

13(daytime)

15(netstat)

17(qotd)

19(chargen)

20(FTP Data)

21(FTP Control)

22(ssh)

23(telnet)

25(smtp)

37(time)

42(name)

43(nicname)

53(domain)

77(privrjs)

79(finger)

87(ttylink)

95(supdup)

101(hostriame)

102(iso-tsap)

103(gppitnp)

104(acrnema)

109(pop2)

110(pop3)

111(sunrpc)

113(auth)

115(sftp)

117(uucp-path)

119(nntp)

123(ntp)

135(loc-srv / epmap)

139(netbios)

143(imap2)

179(bgp)

389(ldap)

465(smtp+ssl)

512(print / exec)

513(login)

514(shell)

515(printer)

526(tempo)

530(courier)

531(chat)

532(netnews)

540(uucp)

556(remotefs)

563(nntp+ssl)

587(smtp)

601(syslog)

636(ldap+ssl)

993(ldap+ssl)

995(pop3+ssl)

2049(nfs)

4045(lockd)

6000(x11)

Note on Port Number change

If you change the port number, make sure that the new port number is not included in the range of dynamic port numbers or is not used by other applications.

The default range of dynamic port numbers is as follows:

For Windows Server 2008: 49152 – 65535

For Windows Server 2012: 49152 – 65535

Note on installing HDvM on an HCSM Management Server

When installing HDvM on an HCSM management server, you must use v8.0 or later.

Note on unexpected errors

If you receive an Unexpected Error message while using the user interface or while running a task, retry the action.

Note on the locale settings of the CLI

The output data when using the CLI may not be correct when the locale settings of the machine running the CLI and Managed Host are different. In this case, set the CLI output format to UTF-8 and redirect the output result into a file.

To set the format to UTF-8, access a command prompt or use the batch file used for running CLI commands and implement the following:

```
set _JAVA_OPTIONS=-Dfile.encoding=UTF-8
```

Automatic processing and notification is not performed when an alert is generated

If an alert is generated during a network failure or while HCSM is stopped, the following automatic processing and notifications might be skipped even if they are set to be triggered by alerts:

- Failover for N+M cold standby
- Running of a scripted command
- Notification of alert reception by email

After starting (or restarting) HCSM or after recovery from a network failure, use the following procedure to check whether automatic processing or a failure alert notification has been skipped, and take action as needed:

(1) See the Tasks & Alerts tab to check if any of the following alerts are recorded during the HCSM startup or during resolution of a network failure:

- Alert of failover from the active blade (alert ID: 0xFF2A or 0xFF2B)
- Alert with an ID that is specified in the scripted command settings and which corresponds to the managed resource specified by the component that generated the alert
- Alert with an alert level that is specified in the email notification settings

(2) If any of the above alerts is recorded, check the HCSM screen for any applicable N+N Cold Standby failover tasks or for scripted commands that were run. Check, at the notification destinations, whether email notifications were sent.

Note that there are two types of triggers that cause HCSM to receive an alert:

(a) Alert sent spontaneously by a hardware component

This is an alert notification sent to HCSM by a hardware component on its own initiative. This category includes alerts sent when a hardware component retries an alert transmission.

(b) Alert that has not been sent and that is obtained through communication from HCSM

HCSM obtains the unsent alert in its first communication* with the hardware component as soon as this communication becomes possible after a failure is resolved or when HCSM is started.

The alerts described in (b) might be obtained by HCSM significantly later than when they were generated, and HCSM cannot determine whether action is required at the time an alert is obtained. Therefore, HCSM does not perform the automatic processing, and the customer must take action as necessary. Even if an alert is sent while alert transmission is being retried as in (a), the alert might be sent as a category (b) alert depending on the timing.

* When HCSM communicates with a hardware component and obtains unsent alerts

- Startup of HCSM
- Discovery of resources
- Refreshing the host and server information (if the host is associated with the server, the server is also accessed when the host information is refreshed)
- Obtaining detailed server information using the HCSM GUI
- Starting Web remote KVM using the HCSM (Access KVM) GUI

- Starting Web Console using the HCSM GUI
- Operation of LID on the front panel, blades, management modules, switch module, management LAN modules, and IOBD
- Power operations on a blade (including those performed after selecting a host)
- Operation of LPAR manager/LPAR
- Operation of DPM (excluding operation on a VM)
- Failover, failback, and testing for N+M cold standby
- Firmware updates
- Enabling/disabling power capping
- Changes to credentials
- Changes to SSL settings (and HCSM GUI operations that are required when the SSL key is changed)
- Alert reception
- Automatic refreshing of host and server information (configuration refresh and status refresh)

(Select Administration - System Settings - Refresh Intervals to specify the interval.)

- Acquisition of power information (if enabled)
- Automatic re-login to SVP (about once every 10 minutes)

Note on forcing server power OFF

When a server is forcibly Powered OFF, the Power Status displayed in the following screens may not match for a temporary period of time:

- Select Resource tab > Chassis & Servers > All Chassis and select Chassis from the Chassis list. The Power Status is displayed in the Condition tab of the Server Blades tab.

- Select Resource tab > Chassis & Servers > All Servers and then click Blade. The Power Status is displayed in the Blade list.

When the above situation occurs, select the corresponding server and refresh the information by using the Refresh Server option. (SD CR#: 7956)

Note on the timing of information collection

Depending on the timing of information collection, it may not be possible to acquire some information from the management target host. In such cases, you must use the refresh option for the relevant management target host.

Note on the virtualization platform environment

- Virtual machine migration

If you operate HCSM using virtual machine migration, note the following:

(1) If you control access to virtual machines:

Do not register the virtual machine to be migrated to the resource group. The virtual machine might disappear from the resource group after migration. Always perform access control for the host that operates on the virtual machine.

(2) If you control the power or refresh the information of the virtual machine:

- Register the tasks for the host that operates on the virtual machine.

- After migrating the virtual machine, refresh the information for the destination hypervisor by using HCSM. The tasks will fail until the information update is complete.

(3) If you add the virtual machine to the logical group:

- Create the logical group not by direct specification but by condition specification.

- After migrating the virtual machine, refresh the information for the destination hypervisor by using HCSM. The virtual machine cannot be displayed in the logical group correctly until the information update is complete.

- Maintenance mode

Do not operate Hypervisors and virtual machines when the Hypervisor is in maintenance mode. In maintenance mode, any HCSM operations for virtual machines might result in failure. In such cases, cancel the maintenance mode and run the operation.

- Hypervisor using a shared disk

When multiple hypervisors share the same disk, the total value of the shared disk capacity identified by each hypervisor is displayed on the Storage of All VMware Summary, All Hyper-V Summary. This means that a value more than the actual capacity may be displayed.

- Resource names in Topology View

The wrong resource name is sometimes displayed in Topology View. You can display the correct resource name by clicking the resource name link. (SD CR#: 17783)

- Obtain the performance information of the host.

If the host is a VMware ESXi host, the disk queue length in the performance data cannot be obtained.

If the host is a Linux host that is configured with a virtual machine on VMware ESXi or Windows Hyper-V, the disk load and the disk queue length in the performance data cannot be obtained.

Notes on a VMware environment

- Lock down mode

ESXi, which uses the lock down mode, cannot be managed in HCSM.

- VM name encoding

If a VM name includes particular characters, the characters are encoded before they are displayed. The following table shows the characters and associated encoded string:

Table 19 Map of characters and displayed strings

No.	Character	Displayed string
1	%	%25
2	/	%2f
3	\	%5c

- SNMP traps

ESXi SNMP traps are not recognized as alerts.

Notes on N+M cold standby

When configuring N+M Standby in a virtualized platform environment, note the following:

VMware environments

- Auto-start settings

When HSCM must start a virtual machine after the failover of the Standby system blade and failback of the Active system blade, the virtual machine must be configured to start automatically when the associated hypervisor starts. You configure Auto-start settings using the vSphere Client.

- UUID settings

To maintain the virtual machine UUID after a failover and failback, you must set the UUID settings as “Always Keep”. You configure UUID settings using the vSphere Client. Ensure that the virtual machine configuration parameter [uuid.action] is set as “keep”. If you cannot find this configuration parameter, add it. If the UUID cannot be inherited, the confirmation dialog UUID change opens during virtual machine startup, and the startup is not completed.

- VMware High Availability (VMware HA)

You cannot use VMware High Availability (VMware HA) in the same virtualization platform in which you plan to use N+M cold standby. After the standby system failover, it may not be possible to start the virtual machine.

- Storage vMotion

You cannot use any Storage vMotion functions if you are using N+M cold standby.

- Blade MAC type setting

When the blade on which VMware runs is set as an active blade, select **Optional Physical** as the blade MAC type. If you do not plan to select **Optional Physical**, implement the workaround described in VMware Knowledge Base 1031111 beforehand. If the MAC type is not Optional Physical, the MAC address is not inherited from the active blade to the standby blade. Depending on the settings, VMware uses the physical machine MAC address as the virtual NIC MAC address. As a result, the MAC addresses of the active blade and the VMware virtual NIC overlap each other after an N+M cold standby failover or failback.

When such duplication occurs, complete the procedures described in 1031111 to eliminate the overlapping of the MAC addresses.

Hyper-V environments

- Auto-start action setting

When HSCM must start a virtual machine after the failover of the Standby system blade and failback of the Active system blade, the virtual machine must be configured to start automatically. You configure the Auto-start action settings using the Hyper-V manager.

Notes on the BIOS/EFI time

In an N+M Cold Standby failover, the BIOS/EFI time on the active server blade is not inherited by the standby server blade. In addition, the handling of the BIOS/EFI time differs depending on the OS and virtualization platform. Therefore, if server blades that belong to a single N+M group run on two different platforms, A and B, the OS or virtualization platform time might differ before and after an N+M Cold Standby failover or failback.

Platform A: OSs and virtualization platforms that handle the BIOS/EFI time as the local time

- Windows (including Hyper-V)
- Logical partitioning
- Red Hat Enterprise Linux (when the local time is specified)

Platform B: OSs and virtualization platforms that handle the BIOS/EFI time as the UTC (Coordinated Universal Time)

- VMware ESXi
- Red Hat Enterprise Linux (when UTC is specified)

To prevent such a time difference, take the actions below according to your environment. Note that the location for specifying BIOS/EFI time settings in the actions below is different for standby server blades and server blades other than standby server blades. For standby server blades, specify the settings in the BIOS/EFI window. For server blades other than standby server blades, specify the settings in the OS or virtualization platform. Then, apply the settings to the BIOS/EFI time.

In the N+M Cold Standby configuration, if you power on a standby server blade to check or specify BIOS/EFI time settings, the blade state of the standby server blade is switched, and it cannot be failed over. Then, a warning alert 0x1100 is sent from the server. After you check and specify BIOS/EFI time settings, perform the following actions:

- Power off the server blade, and then update the chassis information. The blade state of the standby server blade is switched and it can be failed over.
- Change the state of the warning alert 0x1100 to the resolved state.
-

For details on how to check the time, see the server blade manual.

(1) If platform A (which handles the BIOS/EFI time as the local time) can be used throughout the N+M group:

(a) During creation of the system:

Set the local time in the BIOS/EFI time settings for all server blades (including standby server blades) in the N+M group.

(b) During replacement of server blades:

When you replace server blades, before starting the platform, confirm that the local time is specified in the BIOS/EFI time settings for the new server blade.

(2) If platform B (which handles the BIOS/EFI time as the UTC) can be used throughout the N+M group:

(a) During creation of the system:

Set the UTC in the BIOS/EFI time settings for all server blades (including standby server blades) in the N+M group.

(b) During replacement of server blades:

When you replace server blades, before starting the platform, specify the UTC in the BIOS/EFI time settings for the new server blade.

(3) If the same BIOS/EFI time cannot be used throughout the N+M group (#1)

(a) During creation of the system:

- If VMware ESXi exists in the N+M group, enable the NTP (time synchronization mechanism) for VMware ESXi, and then specify settings to obtain time information from the NTP server (#2). To avoid a time synchronization failure due to an NTP server failure, we recommend that you specify at least two NTP servers.

- If Red Hat Enterprise Linux exists in the N+M group, specify settings so that the BIOS/EFI time is handled as the local time.

- Set the local time in the BIOS/EFI time settings for standby server blades.

(b) During system operation:

If VMware ESXi is failed over to a standby server blade, the BIOS/EFI time setting for the standby server blade is changed to UTC by NTP. Therefore, after N+M failback, change to the local time in the BIOS/EFI time settings for the standby server blade.

(c) During replacement of server blades:

- If VMware ESXi runs, confirm that UTC is specified in the BIOS/EFI time settings for the new server blade.
- If an OS or virtualization platform other than VMware ESXi ran, confirm that the local time is set in the BIOS/EFI time settings for the new server blade.

#1: This is the case when either Windows (including Hyper-V) or the logical partitioning and VMware ESXi exist together.

#2: By separating platform A and platform B into different groups, you can eliminate the need for an NTP server.

Notes on displaying the HCSM GUI after an upgrade

Before accessing the HCSM GUI after an upgrade, restart the browser, clear the browser temporary cache and log in to HCSM again. If you do not complete these actions, the GUI may not operate.

Notes on Deployment Manager

Notes on managing a VM on Hyper-V with Deployment Manager

The Hardware Driver Group is updated in v7.6.1-01.

You cannot use system-level backup images or snapshot images that you collected using a version previous to 7.6.1-01. Apply the new version, and then complete the following tasks:

1. Delete the system-level backup images and snapshot images that were collected in the previous version.

2. Remove all of the VMs on Hyper-V that are registered with Hardware Driver Group 1 from the license targets for deployment.
3. After applying the new version, specify Hardware Driver Group 4 for the VMs on Hyper-V, and then register the VMs as license targets for deployment.
4. After completing step 3, collect system-level backup images and snapshot images again as necessary.

- Supported Virtual Disk

When using v7.6.1-01 or later, Disk Configuration Check Results include SCSI Disk information. However, deployment features only support the IDE Disk. Therefore, you cannot specify SCSI Disk to a deployment target disk.

Notes on managing an LPAR with Deployment Manager

Because the system detects only shared NICs for use during a Deployment Manager PXE boot operation, you must ensure that virtual or dedicated NICs on the LPAR are not configured to run PXE boot using the following procedures:

1. Boot an LPAR with a shared NIC that is enabled with PXE boot.
2. Add the LPAR as a licensed resource of Deployment Manager.
3. Verify that the LPAR MAC address of the shared NIC is listed in the Deployment Resources screen on the Management Tab.
4. If the other LPAR MAC address is detected, disable PXE boot on the shared and dedicated NICs on the LPAR, and complete the procedure again.

Notes on PXE Boot Settings

Set the managed LPAR to be registered to the deployment target so that the PXE boot is performed from only one MAC address. If you use an expansion LAN card for CB500/CB2500(*), the PXE boot might be performed from multiple ports (MAC addresses) on the card. In an environment where the PXE boot is requested from multiple MAC addresses of an identical managed LPAR, errors might occur in the tasks of the deployment functionality.

(*): The applicable expansion LAN cards are as follows (as of the end of March 2015):

- GG-CN3M1G2X1-Y

- GG-CN3M1G3X1-Y

System-level Backup and Snapshot

- Restrictions for hardware and operating systems

The applications, which are affected by hardware specific values (such as MAC address) and operating system specific settings, may not work when Restore or

Deploy is run after hardware replacement. In this case, uninstall the application before taking a Snapshot and reinstall it after using the Deploy task.

The following environments are not supported.

- Dynamic disks changed from Windows RE or a maintenance partition which made 2 or more numbered partitions
- Operating system or application level RAID environment (hardware or firmware level is supported)
- A logical disk/volume/partition consisting of multiple storage regions (such as spanning volume) is not supported.
- Encryption technology (such as BitLocker or Trusted Boot)
- Disks used in a storage pool function on Windows Server 2012
- Red Hat Enterprise Linux environments in which the boot loader is not installed in MBR in the BIOS boot environment
- Windows environment in which the VHD is configured for native boot
- Two or more machines with the same BI GUID (GUID used during PXE boot) cannot be set as Deployment Manager targets.

  For example, this situation occurs when the VM of Hyper-V is exported or imported and a copy is created.

- Snapshot and master image deployment, which targets the Windows environment where Hyper-V is installed, is not supported.

- Specifying Entire or Full sector

You must specify Entire or Full sector based on the target disk file system type and disk type.

No.	Target File System	Specify Entire(#1)	Specify Full sector(#2)
1	FAT16	(#3)	-
2	FAT32	(#3)	-
3	NTFS	(#3)	-
4	ReFS	Yes	Yes
5	ext2	-	-
6	ext3	-	-
7	ext4	Yes	Yes
8	Linux-swap	-	-
9	LVM1	Yes	Yes
10	LVM2	Yes	Yes
11	ReiserFS	Yes	Yes
12	JFS	Yes	Yes
13	XFS (#4, #5)	Yes	Yes

14	other	Yes	Yes

(#1) For snapshot, Entire must be specified regardless of this list.

For a dynamic disk and GPT disk environments, Entire must be specified regardless of this list.

(#2) For SuSE Linux or Solaris environment, Full sector must be specified regardless of this list.

(#3) Basic disk on Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2 is not supported for partitions. Entire must be specified for this environment.

(#4) When creating the XFS file system, we recommend choosing a target partition or disk that can run a System-level Backup/System-level Restore task for a journal by using HCSM. The storage location of the journal is indicated as "Linux XFS Journal".

(#5) When running a System-level Backup/System-level Restore task of the XFS file system, back up or restore "Linux XFS Journal" at the same time in order to maintain the integrity of information between the XFS file system and the journal.

- Image Path for System-level Backup or Snapshot

The System-level Backup and Snapshot image paths support only single-byte characters.

- If the target host of a System-level Backup/Snapshot task is unmanaged or removed from the list of licensed resources, the task is able to run. However, the image generated by the task cannot be used in a System-level Restore/Deployment task.

Deployment Templates

- Host Name setting

The Deployment Template host name setting supports only single-byte characters.

- Network settings

Set one or more static IP address that can communicate with HCSM in Specify Network Parameters. When the IP address is not specified, the Deploy Master Image task fails. In addition, ensure that you set an IP address that is different from the IP address assigned in DHCP.

- Language in Create Deployment Template for Windows

While creating Deployment Templates for Windows Server 2008 or later versions, specify the same value as the operating system language for the Master Image that you plan to use for the Deploy Master Image task. When an incorrect language is specified, the IP address and Administrator password settings fail, and the Deploy Master Image task may fail.

Master Image Deployment

- SSH port number

While performing disk duplication for a Linux server, set the SSH port number of the management target server as 22. If the port number is anything other than 22, the Deploy Master Image task fails.

- Windows account name

When running the Windows snapshot task, change the account name (Administrator or other) back to the default built-in account name, activate the account, and then run the Snapshot task. If the snapshot is run when the account name is different than the default or while the account is disabled, the Deploy Master Image task fails.

- Notes on Deployment Manager settings

When configuring Deployment Manager settings, ensure that you set the Maximum Simultaneous Connection value by measuring the performance monitor parameter while running a backup task.

No.	Group	Counter	Recommended Value
1	PhysicalDisk	Current Disk Queue Length	[Maximum] (Number of disks for which physical disk is configured+2) x Number of CPU threads or less

Installation and removal of Deployment Manager

- Notes on upgrading from v7.4.1-00 to v7.4.1-01 or later

If you created Deployment Templates using v7.4.1-00 and then you upgrade to 7.4.1-01, you must reset the Deploy Template settings and the language settings before running the Deploy Master Image task. When the language is not set, the IP address and Administrator password settings fail, and Deploy Master Image task may fail.

- Removing Deployment Manager

Do not remove Microsoft SQL Server before you remove Deployment Manager. Removal of SQL Server before Deployment Manager may cause a reinstallation to fail. If you plan to reinstall the database, ensure that the following folders do not exist. If the folders exist, delete them before reinstalling the database.

[Target folder]

In Microsoft SQL Server 2008 R2:

C:\Program Files\Microsoft SQL Server\MSSQL10_50.DPMDBI

In Microsoft SQL Server 2012:

C:\Program Files\Microsoft SQL Server\MSSQL11.DPMDBI

In Microsoft SQL Server 2014:

C:\Program Files\Microsoft SQL Server\MSSQL12.DPMDBI

If the following files exist in the target folder used by Deployment Manager, delete the files and the target folder:

- \MSSQL\Data\DPM_DATA.MDF
- \MSSQL\Data\DPM_LOG.LDF

Deployment Manager disk number limitation

In an environment in which Deployment Manager runs, the maximum number of disks that can be connected to monitoring targets is as follows:

(When connecting to external storage by using a multi-path configuration, the maximum number of disks can be obtained by multiplying the number of LUs by the number of paths.)

Earlier than v8.2.1: Up to 256 disks

v8.2.1 or later: Up to 2,000 disks

If the specified number of disks exceeds the maximum, Deployment Manager does not work properly.

No.	Type of disk	Upper limit of disk number
1	IDE	4
2	SCSI, FC	16(#1)(#2)(#4)
3	RAID	16(#3)

(#1) This number is the upper limit of total number of SCSI and FC disks.

(#2) When you configure a multi-path FC, the detected and an actual number might differ.

(#3) This number is the upper limit of logical disks on a controller.

(#4) For FC, Deployment Manager can manage disks with a logical disk number from 0 to 255. Even if the maximum number of disks is not exceeded, disks with a logical disk number of 256 or later cannot be backed up.

The maximum number of disks with disk information that can be obtained by the disk configuration check is 128 disks when using Hardware Driver Group 1, and 256 disks when using other hardware driver groups.

Limitation on the number of partitions on a licensed resource

When either of the following limitations is exceeded, a Deployment Manager task fails.

- A dynamic disk has more than 1000 partitions.

- A basic disk has more than the following number of partitions.

When you configure a disk using an extended partition, the limitation on logical drives on the disk is 3 units fewer than listed in the following table.

No.	Type of disk	Upper limit of partitions on a disk
1	IDE	15
2	SCSI, FC	14
3	RAID	14

Notes on the maximum disk size and partition size

The following table lists the maximum disk size and partition size for each Hardware Driver Group on which system-level backup, system-level restore, snapshot, and master image deployment can be run.

Hardware Driver Group	Maximum disk size	Maximum partition size
Hardware Driver Group 1	2TB	2TB
Hardware Driver Group 2	2TB	2TB
Hardware Driver Group 3	2TB	2TB
Hardware Driver Group 4	8TB	2TB
Hardware Driver Group 5	8TB	2TB

About the disk capacity

From HCSM 7.6.1 onward, the value for [Capacity] of a disk that is displayed in each dialog box of the deployment function has changed.

- Versions prior to 7.6.1: The sum of the recognized sizes of partitions
- Versions 7.6.1 and later: The recognized size of the disk

Example:

If a 20-GB disk has 10 GB for Partition 1 and 5 GB for Partition 2, the disk size is displayed as follows depending on the version:

- Versions prior to 7.6.1: 15 GB
- Versions 7.6.1 and later: 20 GB

This information changes if the disk configuration check is executed in v7.6.1 or a later version. Only the display is changed. The operation is not affected.

About the attribute values of the partition information

From HCSM v7.6.1 onward, the value for [Attribute] that is displayed in each window of the deployment function has changed. The table below shows a list of the changes.

The information changes if the disk configuration check task runs in v7.6.1 or a later version. The operations is not affected; only the display changes.

Versions prior to 7.6.1	**Version 7.6.1 to earlier than 8.0.0-00**	**Version 8.0.0 to earlier than 8.2.1-00**	**Version 8.2.1 or later**
Unknown EFI Linux RAID	Unknown	Unknown	Unknown
hidden partition	hidden partition	hidden partition	hidden partition
NTFS(#1)	NTFS Unknown(#1)	NTFS Unknown(#1)	NTFS Unknown(#1)
FAT12 FAT12/16	FAT12	FAT12	FAT12
FAT32	FAT32	FAT32	FAT32
Linux Unknown	Linux	Linux Native Linux ext2/3/4 Linux ext4	Linux Native Linux ext2/3/4 Linux ext4
Linux-swap	Linux-swap	Linux-swap	Linux-swap
Linux LVM LVM	Linux LVM	Linux LVM	Linux LVM
EFI system	EFI system	EFI system	EFI system
Microsoft reserved	Microsoft reserved	Microsoft reserved	Microsoft reserved
Unknown	Dynamic Volume	Dynamic Volume	Dynamic Volume
Maintenance partition	Maintenance partition	Maintenance partition	Maintenance partition
Unknown	Unknown	Unknown XFS(#2)	Unknown XFS(#3)

#1: If using v7.6.1 or earlier, ReFS is displayed as NTFS. If using v7.6.1 or later, ReFS is displayed as Unknown.

#2: If using v8.1.1 or earlier, XFS is displayed as Unknown. If using v8.1.1 or later, XFS is displayed as XFS.

#3: If using v8.2.1 or earlier, Linux XFS Journal is displayed as Unknown. If using v8.2.1 or later, Linux XFS Journal is displayed as Linux XFS Journal.

Notes on setting a Windows Server 2012 R2 Hyper-V virtual machine as a management target

Specify Generation 1 as the Generation of the virtual machine when you create it.

Notes on master image deployment in v7.6.1 and later

Master image deployment will fail if you use a master image acquired from a version prior to 7.6.1 and all the following conditions are met:

(1) The HSCM and DHCP servers coexist.

(2) For the master image acquired from a version prior to 7.6.1, one of the following conditions is satisfied:

(a) When Sysprep is executed, the IP address of the management server is not entered.

(b) When Sysprep is executed, the IP address of the management server is entered, but it is different from the IP address of the management server in which HCSM 7.6.1 or a later version of HCSM is running.

Notes on master image deployment

If you use the master image that was obtained from a Windows Server 2012 or later master host to execute a master image deployment task, wait at least 90 seconds after the task is complete, and then use the destination resource.

Note on errors during Disk Configuration Check

There is a possibility that the managed resource is stopped during the processing when errors occur in Disk Configuration Check. Power off the managed resources before using them. (SD CR#: 14925)

Notes on an error occurring for a task to change deployment settings

If a task to change deployment settings terminates due to a KASV31422-E error, run the task again. (SD CR#: 15748)

Notes on UEFI boot order setting for Deployment Manager targets

Do not add an UEFI-based computer which has a boot order setting bound with a hardware ID (such as MAC address) as a licensed resource of Deployment Manager. This setting may prevent system-level restore tasks, master image deployment tasks, or restarting the target after finishing Deployment Manager tasks.

Notes on elapsed time of PXE boot for Deployment Manager targets

If a Deployment Manager licensed resource takes more than 10 minutes to complete a PXE boot after the resource turns on, the deployment task fails.

In this case, adjust the [Maximum allotted time for Servers, LPARs or VMs to power on successfully] setting to a higher number to allow for completing the PXE boot.

Notes on the Local Security Policy

After installing Deployment Manager, do not remove the following account information from the "Log on as a Service" list in the Local Security Policy.

- In Windows Server 2008 R2 (IIS7.5)
  - NT SERVICE\ALL SERVICES
  - Classic .NET AppPool
  - NETWORK SERVICE
  - NT SERVICE\MSSQL$DPMDBI
  - NT SERVICE\SQLAgent$DPMDBI

  - SQLServer2005SQLBrowserUser$*computer-name*
  - ASP.NET v4.0 DeploymentManagerPool

- In Windows Server 2012 (IIS 8.0)
  - NT SERVICE\ALL SERVICES
  - IIS APPPOOL\.NET v4.5
  - IIS APPPOOL\.NET v4.5 Classic
  - NETWORK SERVICE
  - NT SERVICE\MSSQL$DPMDBI
  - NT SERVICE\SQLAgent$DPMDBI
  - SQLServer2005SQLBrowserUser$*computer-name*
  - IIS APPPOOL\DeploymentManagerPool

- In Windows Server 2012 R2 (IIS 8.5)
  - NT SERVICE\ALL SERVICES
  - IIS APPPOOL\.NET v4.5
  - IIS APPPOOL\.NET v4.5 Classic
  - NETWORK SERVICE
  - NT SERVICE\MSSQL$DPMDBI
  - NT SERVICE\SQLAgent$DPMDBI
  - SQLServer2005SQLBrowserUser$*computer-name*

- IIS APPPOOL\DefaultAppPool
- IIS APPPOOL\DeploymentManagerPool

If System-level Restore or Master Image Deployment wizard displays multiple images of the same backup image or snapshot image

If you change the Logical Partitioning (enable or disable LPAR Manager) without deleting the information of hosts managed by HCSM, the backup images or snapshot images of the hosts might be shown redundantly. (SD CR#: 18212)

In this case, cancel the wizard, and then remove the hosts existed before changing the Logical Partitioning from the HCSM management targets.

Note on registering a Deployment Manager Plug-in license in a cluster environment.

If you changed the number of Deployment Manager Plug-in licenses registered in HCSM, restart the HCSM service. If the service is already registered in the cluster management software, take the service offline and then bring it back online. (SD CR#: 18875)

#: This includes entering the number of licenses when the environment was newly built.

Notes when the image file path of a system backup or snapshot image contains a semicolon (;)

From HCSM 8.1.1, semicolons (;) can no longer be used in the path to an image file used by Deployment Manager. If an image file is stored in a path that contains a semicolon (;) in a version earlier than HCSM 8.1.1, or if a deployment functionality task to which a path that contains a semicolon is specified exists, follow the procedure below to change the path to the image files.

(1) Write down the information of a task whose path to an image file to be acquired or used contains a semicolon (;).

(2) Move or copy a system backup image or snapshot image whose path contains a semicolon (;) to a path that does not contain a semicolon.

(3) In the **Administration** tab, go to **Deployment** and **Image File Management**, and then import the information of the file moved or copied in (2).

(4) Re-register the task in (1). For a System-level Restore or Master Image Deployment task, specify the file imported in (3) as the image file to be used. For a system backup or snapshot task, specify a path that does not use a semicolon (;) as the image storage destination.

(5) Delete the task in (1).

(6) In the **Administration** tab, go to **Deployment** and then **Image File Management**, and then delete the information of the original file moved or copied in (2).

(7) In the **Administration** tab, select **Deployment** and then **Settings**. If a path that contains a semicolon (;) is specified for **Default Path**, change the path to a path that does not contain a semicolon.

Precautions about the deployment template for Linux

In the deployment template for Linux targets, associations of MAC addresses and devices (eth0, eth1, ..., eth6) are ignored. For this reason, select "Auto Detect" for MAC addresses. (SD CR#: 18628)

Notes on rescheduling a System Level Backup task

Do not reschedule an existing System Level Backup task from "Later" to "Repeat". If a task having such modification is executed, irrespective of the successful backing up operation, it ends with the KASV00028-E that indicates an unexpected error.(SD CR#: 19113)

Also the backup image file might be saved as an erroneous file name:

- When the "Add sequence number for repeated tasks to image file name" setting is selected, the sequence number part is set to "null". (e.g. VM_BK_D1E_C_null.lbr)

- When the setting is not selected, the file is saved as the correct file name.

Notes on using an extended partition in a Linux environment

When you run the fdisk command with the f subcommand for Linux, the EBR (Extended Boot Record) of the extended partition might become invalid. When you run a deployment function for disks or partitions that contain an invalid EBR, tasks might fail or might not run correctly.

Example problems:

- Tasks for system-level backup and system-level restoration fail.# 1

- Tasks for taking a snapshot and deploying a master image fail.#1

- Results of disk configuration checks are incorrect.

#1: When images that were obtained by specifying [Back up entire disk] are used, the tasks run successfully.

Corrective actions:

This problem is caused by an error in the Linux fdisk command.

If the machine operating system is any of the following, do not run the fdisk command with the f subcommand on the disk containing the extended partition: Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server 11, or SUSE Linux Enterprise Server 12.

Notes on using LPAR Migration

When using LPAR migration in the Deployment Manager, ensure that the migration source and migration destination server blades have the same settings for the following:

- Boot order of EFI drivers
- Optional parameters of HBA EFI drivers

For details about configuring these settings, see the Compute Blade User's Guide, which comes with the hardware component.

Notes on managing a Deployment Manager target in UEFI boot environments

When managing a Deployment Manager target that is in UEFI boot environment, perform the following instructions:

(1) When registering a Red Hat Enterprise Linux 7.0 system as a Deployment Manager target in UEFI boot environments

When registering a Red Hat Enterprise Linux 7.0 system as a Deployment Manager target in UEFI boot environments, after installing Red Hat Enterprise Linux 7.0, change the boot file setting from shim.efi to grubx64.efi.

(2) When registering a Windows system as a Deployment Manager target in UEFI boot environments

Windows system possibly insert the “Windows Boot Manager” at top of boot orders by design when the OS starts after either of the following occasions: A system level restore, a master image deployment task, and modifying EFI menu.

When a Deployment Manager task fails with KASV31431-E, and the Windows OS starts on the target, resume the priority of network boot to the top.

Also, use the “Windows Boot Manager” that is appended by the Windows OS as a boot order item for starting OS.

Notes for modifying a Host IP address

When you modify a Host IP address after deleting the host information (containing the original IP address) from HCSM, specify the modified IP address and then run Discovery.

Notes on the Hitachi Compute Rack maintenance mode

When in maintenance mode, Hitachi Compute Rack-mounted systems cannot be managed in HCSM. (SD CR#: 10963)

Notes on performance monitoring

CPU usage

When monitoring the performance of a host that is running the following software, there is a possibility that the CPU usage may not be acquired correctly:

- Operating system is Windows Server 2008.
- Hyper-V is installed.

Therefore, if you have managed hosts in your environment that meet this criteria, disable the acquisition of CPU usage performance data in the performance monitoring settings.

Physical disk read/write

When displaying ESXi performance data, instance names that are displayed in the read/write of a physical disk differ from that of the object names displayed on a vSphere Client. (SD CR#: 11631)

Notes on the management server hostname

The management server hostname must adhere to the following rules:

- Maximum length: 128 bytes
- Valid characters: A-Z a-z 0-9 - .
- A dash (-) cannot be used at the beginning and at the end of the host name.

Notes on the properties files during an overwrite/upgrade installation

When running an overwrite/upgrade installation, the HCSM properties file is replaced with a new property file. However, the existing settings of the properties files are carried forward to the new file. If, however, you modified or added parameters other than the standard setting values, those changes are not inherited from the original file and must be made again.

Notes for management targets logged in as general user in Linux

When the following conditions are met, the Timeout error (KASV10029-E, KASV30036-E) may occur:

- Connect to a Linux host.

- For credentials, specify General user set to use the sudo command.

- The sudoers setting required to use the sudo command are not set.

Refer to the Hitachi Compute Systems Manager Installation and Configuration Guide for information on how to add or correct the sudoers settings.

Notes about the information for volumes mounted on a network drive

In the following situations, the same network drive information is displayed for the file system in the host information more than once. (SD CR#: 13396)

- For Windows Server 2008 with UAC disabled:

If there are sessions connected to the management target, the number of login sessions is displayed regardless of the account.

- For Windows Server 2008 with UAC enabled:

The number of volumes mounted by the Administrator account is displayed according to the number of login sessions of the Administrator.

Notes on time synchronization

If the following time-adjustment programs are run, the operating system time might be changed to a past date, which may cause HCS to run improperly:

- Time synchronization using NTP (Network Time Protocol)

- Time synchronization function of a guest OS in Hyper-V

In such cases, refer to the Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide and adjust the time of the management server.

Notes on server blade firmware updates

If the firmware of server blade is updated when the server blade power is OFF, the process to reflect the updated firmware in the server blade is run. During that time, the server blade power control is restricted by the management module. You must monitor this process closely so that there is no overlap between the firmware update processes when registering the task that manages the power control of the server blade.

The reflection time to the firmware server blade is approximately 20 minutes.

Notes on exporting CSV

BOM (Byte Order Mark)

CSV export data is output in UTF-8 code and BOM (Byte Order Mark) is added to the beginning of the file.

Corruption of UTF-8 text

Because exported CSV data is output in UTF-8 format, output text may be corrupted by software that is not compatible with UTF-8.

Notes when modifying MAC address on management target OS

If a MAC address is modified on the operating system typically according to network driver settings, hosts cannot be correctly managed using associated VM or LPAR information.

To change the MAC address, change the VM or LPAR settings instead of OS or network driver settings.

If you modified the MAC address using the operating system or network driver settings, change the operating system or network driver settings again to use the same MAC address used in the VM or LPAR setting.

Notes on EFI settings and enabling/disabling LPAR Manager

When LPAR Manager on Hitachi Compute Blade 2000 is enabled or disabled, the EFI settings for the applicable blade are overwritten with initial values for each LPAR Manager status.

Notes on LPAR Management

Solaris Support

LPARs for Solaris cannot be created using HCSM. However, you can manage LPARs for Solaris that already exist.

Supported LPAR NICs

HCSM Server does not support LPARs with only dedicated NICs. Ensure LPARs are assigned shared NICs so that the HCSM Server can manage the LPARs.

LPAR migration error

HCSM Logical Partitioning Manager differs with HVM Navigator in how LPAR migration status information is displayed. HCSM LPAR Manager requires approximately 10 minutes before notifying a user that an LPAR migration task failed, whereas HVM Navigator notifies a user immediately.

The delay is caused by the way HCSM Logical Partitioning Manager manages maintenance information, and occurs regardless of whether the LPAR migration tasks succeed. Although there is a delay in displaying the information, the expected time for HCSM to collect maintenance information included in an LPAR migration task is equivalent to HVM Navigator.

LPAR Manager operation

Do not operate an LPAR Manager simultaneously by using HCSM and logical partitioning manager software such as HVM screen or Element Manager.

Supported LPAR Manager

HCSM Server only supports LPAR Managers in "Expansion" mode. Do not change the mode to "Standard".

Notes on encrypted communication

If HCSM is configured to verify a certificate for communications between HCSM and a TLS supported LPAR Manager, the HCSM server must import the certificate of the certificate authority or intermediate certificate authority that is the issuer of the LPAR Manager certificate. If the valid certificate is not imported, managing the LPAR Manager fails due to communication errors.

Notes on changing the Logical Partitioning of a server blade

To enable or disable the Logical Partitioning of a blade server, remove hosts that are operating on the target server blade and the Logical Partitioning from HCSM management targets, and then change the Logical Partitioning.

Notes on the IPv6 specifications

If you use IPv6 to manage Compute Blade, HCSM does not support LPAR Management.

To use LPAR Management with HCSM, you must use IPv4 to manage Compute Blade. (SD CR#: 19864)

Notes on FC boot settings

If you use a non-Hitachi FC board, the Boot Availability of private and shared FCs cannot be changed by using the LPAR create/edit function.

Notes on user account

Do not use a user account with a user ID containing one or more single quotation marks.

Notes on memory usage of browser

If a browser connecting to the HCSM server slows down or displays incorrectly, the memory usage of the browser might be extremely high. To recover from the symptom, close the browser window, and then log in to the HCSM Server again.

Notes on the status of the managed resources

When a managed resource is not able to respond to HCSM while the managed resource is starting or shutting down, HCSM displays the status of the managed resource as "Unknown" or "Unconnect".

Notes on blade power operation

To reduce the duration of a power control operation for a blade that runs LPAR Manager, the following operations are effective.

- Disable “Verify LPAR Manager startup” setting, and then execute power on or reboot for LPAR Manager.

- Power OFF LPARs that runs on a target LPAR Manager, and then execute power off or reboot for LPAR Manager.

Notes on using LPAR Migration and N+M Cold Standby

If LPAR Migration and N+M Cold Standby are used in a system, an LPAR Migration task might fail with a WWN conflict error with ID KASV00566-E. This symptom might occur when all of the following conditions are met:

(1) An LPAR Migration was run using HVM Navigator or HCSM Server, and the associated blades are managed by the HCSM Server.

(2) The blades were added to an N+M Cold Standby group.

(3) An LPAR Migration task was run for one or more managed blades in the system.

To resolve the problem that occurred in (3), complete the following procedures to correct the conflict:

(i) On each blade with a conflict, access the HVM menu screen and run "Save Configuration" or press the F9 key.

(ii)Turn on or restart the LPAR Manager.

If the problem persists, collect the relevant maintenance information by referring to the Hitachi Compute Systems Manager Installation and Configuration Guide or the Hitachi Compute Systems Manager Users Guide and then contact the Customer Support.

Notes on using HCSM LPAR Management and HVM Navigator on the same system

When HCSM runs LPAR Management and HVM Navigator on the same system, follow the basic policy, which is always using HCSM to modify LPAR manager and LPAR configuration and settings. However, you must use HVM Navigator for the following tasks:

- Showing boot orders
- Changing boot orders
- Saving configuration
- Monitoring LPAR manager and LPAR
- Rehearsal of LPAR migration

If an error occurs on HCSM after an HVM Navigator tasks run, refresh the LPAR manager information using HCSM. If the error persists, remove the LPAR manager, the chassis mounting the LPAR manager, and the hosts on the LPAR from managed resources. Then re-discover them, and re-register the task as needed.

Notes on managed resources in a multiboot environment

If the managed resources are in a multiboot environment, the resources cannot be managed by HCSM.

Notes on memory usage if using ZFS with Solaris

If ZFS is used with Solaris, when the ZFS cache is allocated, the value displayed in HCSM performance information that shows memory usage will decrease. If the cache is UFS, the value that shows memory usage does not decrease. Memory allocated as a cache is automatically released by the operating system when there is a memory shortage.

Note on performance data collection for VMware ESXi

Although this version fixes an issue that caused the sent and received packets of performance data of VMware ESXi to swap display values, incorrectly stored data is not corrected and is displayed incorrectly. Therefore the affected sent and received packets values must be swapped when they are read.

Notes on the variables specified in the argument of Scripted Command

The value of the following variables might include a meta character (such as a space, &, `, <, >, |, ^, \, ;, $, or "):

%M: The name of the resource on which the alert was issued.

%S: The alert content.

%P: The failure location for the alert.

%H: The ID of the LPAR Manager which the alert was issued.

%V: The name of the LPAR on which the alert was issued.

Enclose the argument in double quotation marks (") in the command path setting of the script command. (For example: D:\tools\ShutdownOS.bat %D %T "%M" %L %I "%S")

Even if the argument is enclosed in double quotation marks ("), the scripted command does not operate properly when the variable includes ", \, or $.

Do not use ", \, or $ in the values for the following settings:

- Host Name
- Chassis Name
- Server Name
- LPAR Manager ID
- LPAR Name
- "Failure Location" and "Alert Content" of the SNMP settings

Notes on the registration of repetitive tasks

If the KASV10066-E error occurs when registering a repetitive task, there might be a mistake in the schedule settings. Confirm that there are no mistakes in the cycle, start time, and end time. (SD CR#: 14751)

Notes on using SSL communication or changing the port number for Hitachi Command Suite Common Component

If HCSM is installed in an environment in which SSL communication is enabled or the port number for Hitachi Command Suite Common Component has been changed, the GUI might not start, even if the " Start Hitachi Command Suite GUI" check box is selected in the Install Complete window.

If this problem occurs, check the changed management server information, and then enter the URL for Compute Systems Manager in the web browser's address bar to start the GUI.

Notes on using Internet Explorer 11.0

When you click a button or anchor on the screen to open a new tab or new window, an extra blank window or transitional window might be displayed at the same time. In such a case, please close the unnecessary window.

If such problems occur repeatedly, create a new Windows user account, and then use the new user account to operate the browser.

Notes on specifying user-defined asset tags for servers

You can specify a user-defined asset tag for server managed resources using Element Manager. After you define the asset tag, you can view it along with the other server information in the server list.

(1) On the Resources tab, select Chassis & Servers.

(2) Select All Servers.

(3) Expand the tree and select the type of server for which you want to view information.

(4) From the list of servers, locate the server for which you want to specify an asset tag and click the associated Chassis Name link. The chassis summary screen opens.

(5) From the More Actions menu, select Launch Element Manager. The Element Manager application opens.

(6) Log in to Element Manager. The Element Manager interface opens.

(7) On the Element Manager Resources tab, select Server Blades and then expand the tree and select the Server blade for which you want to specify an asset tag.

(8) Select the BMC tab.

(9) On the BMC tab, select Edit --> Asset information.

(10) In the Asset information window, enter a unique asset tag for this server and click Confirm. You can enter a maximum of 63 alphanumeric characters and symbols. The new asset tag appears in the Asset tag field on the BMC tab.

(11) When you finish adding asset tags, you can close Element Manager. When you return to the HCSM screen, the new asset tag now appears as the server name in the Server list.

Notes on creating LPARs

When you upgrade HCSM from v7.6.1-00 or an earlier version to this version, refresh server information for the target blade before creating or editing LPARs. The error message with Message-ID: KASV50005-E might occur, if the server information is not refreshed. (SD CR#: 15039)

Notes on the decimal point in the CLI output

If a decimal point is included in the CLI output when the version of HCSM which CLI has connected to is later than v7.6.1-01, the decimal point is always displayed as "." regardless of the OS language settings.

Notes on HCS installation failure due to a Common Component error

If the following message is recorded in the Common Component installation log file, the installation file may be scheduled for update during the next startup. Restart the management server, and then start the installer again.

[Windows]

Log file location: Root directory of the <system-drive>

File name: hcmds64ist.log

[Linux]

Log file location: /tmp

File name: hcmds64inst.log

```
----------------------------------------------------
[hh:mm:ss] Installation result:
[hh:mm:ss] 02
```

Notes on the column display and the filter settings of HCSM GUI after an upgrade

When you upgrade HCSM, the order of columns, show or hide settings, sort settings, and filtering conditions that were set for each window in the previous version are reset. (SD CR#: 17618, 18026, 18473)

Notes on file transfers when upgrading

If upgrading from v8.0 or earlier, the installation directory used in v7.x is deleted. If there are any necessary files other than the data that is transferred in the upgrade, back them up before the upgrade.

Notes on the Deployment Manager port number when upgrading

If upgrading from v8 or earlier, the port number used in the Deployment Manager is overwritten with the default value or the value used in v7.x. Check the settings after the upgrade.

Notes on user scripts when upgrading

The command name to collect management server maintenance information was changed from hcmdsgetlogs for v7.x to hcmds64getlogs for v8.0.0 and later. If the hcmdsgetlogs command is used in any user scripts, you must update the scripts to use the new command name.

Notes on the uninstallation order of HCS products

To uninstall HCS products (including HCSM), uninstall the following products first:

- Hitachi Storage Navigator Modular 2

- Hitachi File Services Manager

Notes on migrating from the Windows version of HCSM to the Linux version

Take note of the following if the database in the Windows version of HCSM is exported and imported to the Linux version of HCSM.

Deployment Manager Settings

The Deployment Manager settings that are set in the Windows version of HCSM are deleted.

If the managed Host is Windows

Import the database to the Linux version of HCSM and then use the GUI to specify the port number for the Credentials of the Windows managed host. The communication method used for the Windows managed host is changed from DCOM to WinRM. See the Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide when configuring the settings.

Notes on the power consumption of power monitoring

If the times of the management server and the power monitoring target server do not match, a hyphen (-) might be displayed in the total power consumption and average power consumption. (SD CR#: 15609)

Notes on Red Hat Enterprise Linux 6.5 prerequisite libraries

The following optional package is required for Red Hat Enterprise Linux 6.5 to run HCSM server. Apply this package if you use Red Hat Enterprise Linux 6.5.

upstart-0.6.5-13.el6_5.3.x86_64 or later

Notes on using power capping for Compute Rack

Power capping setting for Compute Rack does not reject an invalid threshold value which is less than the acceptable range, and power capping function is not turned on. Instead of an error in power capping setting, you receive a 0xFF10 alert generated by the Compute Rack.

In this case, correct the threshold value. (SD CR#: 10666)

Notes on displaying a MAC address of a Compute Rack

HCSM does not show a MAC address of a NIC in a PCI slot of a Compute Rack.

Discover the OS on the Compute Rack, and access the IP Network tab to check the MAC address. (SD CR#: 11023)

Notes on users, user groups, and resource groups

Take care to design the system in such a way that the following limits on users, user groups, and resource groups are not exceeded:

(1) Limits that apply to Hitachi Command Suite

(a) Number of users: 30

(b) Number of user groups: 30

(c) Number of resource groups: 400

(2) Limits that apply to a single user group

(a) Number of users: 30

(b) Number of resource groups: 20

(3) Limits that apply to a single user

(a) Number of user groups: 3

Notes on the group definition of N+M Cold Standby Groups

If either of the following conditions is met, the controller number of an I/O card will appear blank in the group definition of an N+M Cold Standby Group: (SD CR#:17794)

(1) The N+M Cold Standby Group was created in a version of HCSM earlier than 8.1.0

(2) The chassis type of the N+M Cold Standby Group is Compute Blade CB500 and the firmware version is earlier than A0230.

Notes network interface names on a Linux managed server

HCSM supports network interface names in only the formats listed in the following table. HCSM will not display network interfaces with names that do not meet these conditions. (SD CR#: 17774)

No.	Conditions	Examples
1	Contains `eth`	eth0, seth0, veth0
2	Contains `bond`	bond0
3	Contains `:`	eth0:1
4	Starts with `ibft`	ibft0
5	Starts with `en`	eno1, ens33, enp1s0f1, enx78e7d1ea46da
6	Matches the following regular expression: `.+?\.\d{1,4}.*`	bond1.100
7	Matches the following regular expression: `vlan\d{1,4}.*`	vlan100
8	Matches the following regular expression: `br\d+.*`	br0
9	Matches the following regular expression: `virbr\d+.*`	virbr0, virbr0-nic
10	Matches the following regular expression: `p[0-9a-fA-F]+p\d+.*`	p1p1
11	Matches the following regular expression: `em\d+.*`	em1

Management servers on Red Hat Enterprise Linux 5.x or 6.x, include the following additional restriction:

- To use Deployment Manager to take a system level backup, all network interface names on the managed server must be 15 characters or less and must be named ethX or bondX (where 'X' is a digit).

Management servers on Red Hat Enterprise Linux 7.x, include the following additional restriction:

- To use Deployment Manager to take a system level backup, all network interface names on the managed server must be 15 characters or less.

Management servers on SUSE Linux Enterprise Server, include the following additional restrictions:

- All network interface names on the managed server must 9 characters or less.

- To use Deployment Manager to take a system level backup, all network interface names on the managed server must be named ethX or bondX (where 'X' is a digit).

Notes on Product values in host information

When you upgrade HCSM from a version earlier than 8.1.0, a space is sometimes added to the end of the Product value in the host information, preventing filters from working correctly. In this case, update the host information manually. (SD CR#: 17810)

Note on Filtering

The filtering may not work correctly when a criteria including a comma (,) is specified for the following items. (SD CR#: 18239)

- Credentials

- Server Slot Numbers

To filter correctly, specify the target string separately without using a comma (,).

Notes on secure communication with management targets

In HCSM version 8.4.1 or later, communication between HCSM and a managed Hitachi server is encrypted by default using TLS 1.2 only . As a result, communication with a management target using SSLv3, TLS 1.0, or TLS 1.1 fails in any HCSM version earlier than 8.4.1.

The following two management targets may be affected by this issue:

(1) Hitachi Compute Blade CB500, CB2000, and CB2500

The new firmware supports TLS1.2 communication. In the *Hardware Requirements* section in *Management target requirements*, check the firmware versions supported by HCSM. If you are using a firmware version that is not supported, update the firmware. After updating the firmware, see the manual for the server and enable communication using TLS1.2.

Note that if the firmware does not support TLS1.2, HCSM cannot receive alerts from servers.

(2) Hitachi Compute Rack

The new firmware supports TLS1.2 communication. In the *Hardware Requirements* section in *Management target requirements*, check the firmware versions supported by HCSM. If you are using a firmware version that is not supported, update the firmware. After updating the firmware, see the manual for the server and enable communication using TLS1.2.

Note that if the firmware does not support TLS1.2, HCSM cannot receive alerts from servers.

If you cannot take action on the management target side, you can enable SSL3.0, TLS1.0 or TLS1.1 communication by completing the following procedure. Note, however, that we do not recommend enabling these protocols, because they have known vulnerabilities. If SSL3.0, TLS1.0 and TLS1.1 communication are no longer necessary because of the management server firmware update, revert the settings as soon as possible.

This modification also has an effect on the communication of other HCS products on the same management server.

(1) Stop the HCSM server.

(2) Edit the property in the following file.

File:

In Windows:

<*HCS-Common-Component-installation-folder*>\

conf\user.conf

In Linux:

<*HCS-Common-Component-installation-directory*>/

conf/user.conf

Property:

ssl.protocol=TLSv1.2,TLSv1.1,TLSv1,SSLv3

Note: Hitachi Command Suite Common Component is installed in the following directory by default.

In Windows:

<*HCSM-installation-folder*>\Base64

In Linux:

<*HCSM-installation-directory*>/Base64

If you install Compute Systems Manager on a server on which other Hitachi Command Suite products are already running, Compute Systems Manager is installed in the same location as Hitachi Command Suite Common Component.

Note: If the file user.conf does not exist, create the file.

Note: In the previous example, several protocols are set in the ssl.protocol property. However, we recommend that you specify the minimum required protocols only in addition to TSL v1.2.

(3) Edit the property in the following file:

File:

In Windows:

<HCS-Common-Component-installation-folder>\

conf\ssl\java.security

In Linux:

<HCS-Common-Component-installation-directory>/

conf/ssl/java.security

Property:

Delete "SSLv3" from jdk.tls.disabledAlgorithms.

Note: If you do not specify a value in the jdk.tls.disabledAlgorithms property, keep the following property setting, without deleting the entire line.

jdk.tls.disabledAlgorithms=

(4) Start the HCSM server.

Note: If you modify the JDK to be used in the hcmds64chgjdk command, the property in (3) is overwritten. Perform the above steps (1), (3) and (4) again.

Notes on the management status of the host

Do not perform [Manage Resources] or [Unmanage Resources] for the host already discovered, which is running on the blade registered in the N+M Cold Standby Group. If you perform [Manage Resources] to change the management status from "No" to "Yes", the problems below might occur: (SD CR#: 18919)

- The relationship between the blade and the host is not displayed correctly.
- Operations for the host fail, outputting a KASV10075-E error.

If any of these problems occurs, perform discovery again for the applicable host. In this case, select "All" for Discovery Type Criteria in the Advanced Settings to Discover Resources.

Notes on importing databases

Do not import an archive file without HCSM information to the management server where HCSM exists by using the hcmds64dbtrans command. Additionally, always specify ALL for the /type option of the hcmds64dbtrans command.

If it is necessary to import an archive file without HCSM information, or to specify a setting other than ALL for the /type option of the hcmds64dbtrans command, transfer HCSM to a server other than the destination management server, and then perform those operations.

Notes on displayed volume information

For a volume whose attribute is LUSE, duplicate information might be displayed in the volume tab even though there is no problem with the storage system configuration. To check the correct information, use the HDvM window. (SD CR#: 19241)

Notes on Obtain Storage Volume information

When Obtain Storage Volume information is enabled, durations of discovering chassis and refreshing chassis/servers/LPARs tasks increase in proportion to the number of volumes managed by Device Manager. While these tasks run, other tasks for the same resources might be pended for a long period.

The following tables show approximate duration of discovery and refreshing tasks in an environment with Obtain Storage Volume information enabled.

Ensure that the duration does not affect your system, and then enable Obtain Storage Volume information function.

Table 20 Duration of discovery and refreshing chassis

		Number of volumes		
		10000	**20000**	**50000**
Number of chassis	1	3 minute	6 minute	8 minute
	5	6 minute	8 minute	16 minute
	10	8 minute	12 minute	25 minute

Table 21 Duration of discovery and refreshing servers and LPARs

		Number of volumes		
		10000	**20000**	**50000**
Number of Blades or LPARs	1	3 minute	5 minute	8 minute
	5	5 minute	8 minute	15 minute
	10	6 minute	11 minute	25 minute

Notes on display format of a Volume ID

Hex and Decimal display formats of Volume ID are used on HDvM according to models of storage systems. On the other hand, on HCSM, Volume IDs are displayed only in Hex format.

When you reference a Volume of a storage system displayed in Decimal format on HDvM, you must convert the Hex ID displayed on HCSM into Decimal format.

Example) In case of AMS1000 storage system

A Volume ID on HCSM [00:01:96] corresponds to [406] on HDvM.

Notes on changing SSL secure communication for managed servers

Use the following procedure to restore the default keystore setting of secure SSL communication for Hitachi Servers and Logical Partitioning Managers. (SD CR#: 19473)

(1) Stop the HCSM server.

(2) Edit the line of hcsm.keystore.filename in the HCSM property file as follows.

File:

In Windows:

<HCSM-installation-folder>\ComputeSystemsManager\conf
\user.properties

In Linux:

<HCSM-installation-directory>/ComputeSystemsManager/conf
/user.properties

The edited line of hcsm.keystore.filename:

```
hcsm.keystore.filename=hcsm.default.keystore
```

(3) Start the HCSM server.

(4) On the **Administration** tab, select **System Settings**.

(5) Select **SSL**.

(6) Click **Edit Setting**.

(7) Clear the **Specify the Key Password and Keystore Password** check box.

(8) Click **OK**.

Notes on credentials for searching and managing Compute Blade or Compute Rack

When registering or editing credentials used to search or manage Compute Blade and Compute Rack, be aware of the following:

For Compute Blade CB500/CB2500:

Credentials used for HCSM are accounts specified for CB500/CB2500 **HCSM**. Do not use any other accounts (such as the login account for Element Manager).

The default account specified for the Compute Blade initial settings is the **HCSM** account. No account is displayed in the **HCSM** window. In this case, check the [Default Setting] on the **Credential** window for HCSM to search and manage target system devices.

If you change HCSM credentials and the HCSM account of Compute Blade, be sure to set the same user ID and password for the Compute Blade settings and the HCSM settings.

For details on CB500/CB2500 HCSM accounts, refer to "*Hitachi Compute Blade 500 Series Management Module Setup Guide*" and "*Hitachi Compute Blade 2500 Series Management Module User Guide*".

For Compute Blade CB2000:

The credential used for HCSM is the account specified for CB2000 **HCSM setting**. Do not use any other accounts (such as the login account for Element Manager).

The default account specified for the Compute Blade initial settings is the **HCSM setting** account. No account is displayed in the **HCSM setting** window. In this case, check the [Default Setting] on the **Credential** window for HCSM to search and manage target system devices.

If you change HCSM credentials and the HCSM account of Compute Blade, make sure to set the same user ID and password for the Compute Blade settings and the HCSM settings.

For details on the CB2000 HCSM account, refer to "*Hitachi Compute Blade 2000 User's Guide*".

For Compute Rack:

The default credentials cannot be modified for Compute Rack. Therefore, select the checkbox for [Default Setting] on the credential settings for HCSM.

Notes on using power capping for Compute Blade

Even if a valid value is specified when power capping is set by using HCSM, the task might end with the error KASV30060-E (“Unable to change power capping settings. There is no selected blade for power capping, or the upper limit value is too small. Verify the power capping setting.”).

This problem occurs because the lower limit of the capping setting for the chassis fluctuates according to the capping (APC) status.

In this case, open the capping setting window again to display the current specifiable value range, and then set the new capping value. (SD CR#: 20133)

Notes on collecting maintenance information

To execute the hcmds64getlogs command in an environment where Deployment Manager is installed, use the user name that installed Deployment Manager.

Notes on running the hcsmtraptoxml command

If you run the hcsmtraptoxml command in a Windows environment, the KASV25123-W message is generated. In addition, copies of the following message might appear on multiple lines in the parse_error.txt file.

If only the following message is generated, the XML output is not affected. If another message is also listed, check the content of that message.

```
Cannot find module (XXXXX): At line 0 in (none)
```

Note: "XXXXX" refers to the module name contained in the MIB file.

Documentation

Available documents

Document name	Document number	Issue date
Hitachi Command Suite Compute Systems Manager User Guide	MK-91HC194-15	February 2016
Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide	MK-91HC195-18	April 2016
Hitachi Command Suite Compute Systems Manager CLI Reference Guide	MK-91HC196-04	February 2016
Hitachi Command Suite Compute Systems Manager Messages	MK-91HC197-17	April 2016
Hitachi Command Suite Compute Systems Manager REST API Reference Guide	MK-92HC235-00	April 2016
Hitachi Command Suite Messages	MK-90HC178-24	April 2016

Documentation errata

None

Copyrights and licenses

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

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

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems 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 employees and other individuals to access relevant data; and

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

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, BlueArc, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, RS/6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, z10, zSeries, z/VM, and z/VSE are registered trademarks and DS6000, MVS, and z10 are trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

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.

Notice:

HITACHI and HiRDB are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Windows Server®, Windows Vista®, Internet Explorer®, Hyper-V®, Visual C++® and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft .NET is software for connecting people, information, systems, and devices.

Red Hat is a trademark or a registered trademark of Red Hat, Inc. in the United States and other countries.

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

Intel Core is a trademark of Intel Corporation in the U.S. and/or other countries.

XFS is a trademark of Silicon Graphics, Inc.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

The Deployment Manager Plug-in includes software developed by NEC Corporation.

Hitachi Compute Systems Manager Software includes RSA BSAFE Cryptographic software from EMC Corporation.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel,and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/.

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).

This product includes software developed by Andy Clark.