HITACHI
Inspire the Next

Hitachi Compute Blade Series

SMASH and IPMI User's Guide

FastFind Links

Getting Help

Contents

Hitachi Data Systems

MK-99COM144-01

Contents

Preface

This document describes how to use the Compute Blade series.

This preface includes the following information:

Notice: The use of Compute Blade series and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Intended Audience

This document is intended for the personnel who want to manage Compute Blade series server blades through SMASH.

This document assumes the following:

- The reader is familiar with SMASH standards and relevant CIM object model.

Product Version

This document revision applies to Compute Blade series.

Release Notes

Release notes contain requirements and more recent product information that may not be fully described in this manual. Be sure to review the release notes before installation.

Document Organization

The table below provides an overview of the contents and organization of this document. Click the chapter title in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Chapter 1, Overview on page 1-1	Overviews what SMASH is and what you can do with SMASH functions.
Chapter 2, Setting up SMASH on page 2-1	Describes how to set up SMASH before starting to use it.
Chapter 3, SMASH-CLP on page 3-1	Describes how to use SMASH-CLP.
Chapter 4, WS-Management on page 4-1	Describes how to use WS-Management.
Chapter 5, SMASH operation on page 5-1	Describes how to operate SMASH.
Chapter 6, CIM classes, properties and methods on page 6-1	Provides the list of CIM classes, properties and methods.
Chapter 7, Troubleshooting on page 7-1	Describes troubleshooting for the SMASH.
Chapter 8, IPMI Command List on page 8-1	Provides the list of supported IPMI commands.

Referenced Documents

- Hitachi Compute Blade 500 series Management Module Setup Guide, MK-91CB500014
- Hitachi Compute Blade 500 series Web Console User's Guide, MK-91CB500015
- Hitachi Compute Blade 2500 series Management Module User Guide, MK-99CB2500004

Document Conventions

This term "Compute Blade" refers to all the models of the Compute Blade, unless otherwise noted.

The Hitachi Virtualization Manager (HVM) name has been changed to Hitachi logical partitioning manager (LPAR manager, or LP). If you are using HVM based logical partitioning feature, substitute references to Hitachi logical partitioning manager (LPAR manager, or LP) with HVM.

This document uses the following typographic conventions:

Convention	Description
Regular text bold	In text: keyboard key, parameter name, property name, hardware labels, hardware button, hardware switch. In a procedure: user interface item
Italic	Variable, emphasis, reference to document title, called-out term
`Screen text`	Command name and option, drive name, file name, folder name, directory name, code, file content, system and application output, user input
< > (angled brackets)	Variable (used when italic is not enough to identify variable).
[ ] (square bracket)	Optional values
{ } braces	Required or expected value
| vertical bar	Choice between two or more options or arguments
_(underline)	Default value, for example, [a | b]

This document uses the following icons to draw attention to information:

Icon	Meaning	Description
 WARNING	**WARNING**	This indicates the presence of a potential risk that might cause death or severe injury.
 CAUTION	**CAUTION**	This indicates the presence of a potential risk that might cause relatively mild or moderate injury.
NOTICE	**NOTICE**	This indicates the presence of a potential risk that might cause severe damage to the equipment and/or damage to surrounding properties.
 NOTE	**Note**	This indicates notes not directly related to injury or severe damage to equipment.
 Tip	**Tip**	This indicates advice on how to make the best use of the equipment.

Convention for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical storage capacity values (for example, logical device capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1{,}024^2$ bytes
1 GB	1,024 MB or $1{,}024^3$ bytes
1 TB	1,024 GB or $1{,}024^4$ bytes
1 PB	1,024 TB or $1{,}024^5$ bytes
1 EB	1,024 PB or $1{,}024^6$ bytes

Getting Help

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Portal for contact information: https://portal.hds.com.

Comments

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

Thank you!

1

Overview

This chapter overviews what SMASH is and what you can do with SMASH functions.

- What SMASH is

What SMASH is

SMASH is a management standard tool for server hardware provided by DMTF.

What you can do with SMASH

You can use SMASH to perform operations including powering on or off a server blade and referring to FRU information. Both SMASH-CLP and WS-Management are supported. See DMTF web site shown below for details about SMASH-CLP and WS-Management.

http://dmtf.org/

Operations

The following operations are available for SMASH with Compute Blade series.

Table 1-1 SMASH Operations

#	Operation
1	Server blade operation (Retrieving status, powering on/off and rebooting)
2	Retrieving processor status
3	Retrieving memory status
4	Retrieving power supply module status
5	Retrieving fan module status
6	Retrieving sensor information
7	Retrieving FRU information
8	Changing boot device
9	Retrieving account information
10	Restarting BMC

Profiles

SMASH can perform many types of operations defined by CIM profiles. Compute Blade series support the profiles in the following table. For details, see the following DMTF web site:

http://dmtf.org/standards/profiles

Table 1-2 Supported CIM Profiles

DSP#	Profile	Organization	Version
DSP1004	Base Server	DMTF	1.0.0 or later
DSP1006	SMASH Collections	DMTF	1.0.0 or later
DSP1007	SM CLP Admin Domain	DMTF	1.0.0 or later
DSP1009	Sensors	DMTF	1.0.0 or later
DSP1011	Physical Asset	DMTF	1.0.0 or later
DSP1012	Boot Control	DMTF	1.0.0 or later
DSP1013	Fan	DMTF	1.0.0 or later
DSP1015	Power Supply	DMTF	1.0.0 or later
DSP1018	Service Processor	DMTF	1.0.0 or later
DSP1022	CPU	DMTF	1.0.0 or later
DSP1026	System Memory	DMTF	1.0.0 or later
DSP1033	Profile Registration	DMTF	1.0.0 or later
DSP1034	Simple Identity Management	DMTF	1.0.0 or later

(This page is intentionally left blank)

2

Setting up SMASH

This chapter describes how to set up SMASH before starting to use it.

- ☐ Setting user account
- ☐ Enabling ports for SMASH
- ☐ Finding IP address of BMC
- ☐ Importing digital certificate

Setting user account

Set up an IPMI/SMASH user account before starting to use SMASH. Note that SMASH cannot use an account with null user name or an account without a password. User name for IPMI/SMASH user account 1 is fixed and always null, then you cannot use the account for SMASH. In addition, the account requires Administrator privilege. For details of how to set up accounts, see the *Hitachi Compute Blade 500 series Web Console User's Guide* or *Hitachi Compute Blade 2500 series Management Module User Guide.*

Enabling ports for SMASH

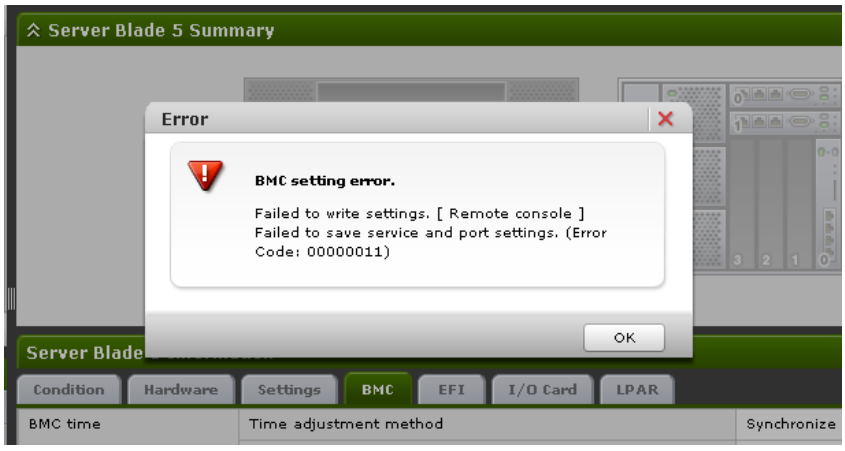
After setting up a user account, set up a port for SMASH. For details of how to enable ports, see the *Hitachi Compute Blade 500 series Web Console User's Guide* or *Hitachi Compute Blade 2500 Series Management Module User Guide.*

NOTE To downgrade an older-version server blade firmware (520HA1/B1 server blade: 01-54 or before, 520A server blade: 02-24 or before, or 540A server blade: 03-05 or before) after changing the port number for WS-Management or SMASH-CLP, change port number as follows prior to downgrade:

- SMASH (WS-Management) to its default (5986).
- SMASH (CLP) to its default (22).

Downgrading firmware without changing those ports cause disability of BMC's port filtering and can result in insecurity. In the event of downgrading firmware without the port number resumption, go back to resumption using the server blade firmware that supports SMASH.

You can check whether BMC is under secure state or not by switching the remote console enable or disable. If BMC is under insecure state, the following error appears.



Finding IP address of BMC

You need the BMC's IP address when installing the digital certificate for the BMC on the client PC or connecting the PC to SMASH. You can check the IP address by opening web console and follow the path: **Resources > Systems > Network management > Management LAN > IP address** tab. The IP addresses for the server blades 0-7 are the IP addresses for the BMC on the Compute Blade 500 series. The IP addresses for the server blades 1-15 are the IP addresses for the BMC on the Compute Blade 2500 series. The last digit in a server blade number indicates the number of the slot, in which the server blade is inserted.

Importing digital certificate

Connection via WS-Management requires installing the digital certificate on the client PC prior to the connection. For details on the how to use the digital certificate, see the *Hitachi Compute Blade 500 Series Management Module Setup Guide* or *Hitachi Compute Blade 2500 Series Management Module User Guide.*

Tip To download the digital certificate from the BMC directly, run the web browser on the client PC, and then, enter "https://<BMC's IP address>"; for example, "https://192.168.0.1/" . For details on how to download and how to install the digital certificate, see help for web browser.

(This page is intentionally left blank)

3

SMASH-CLP

This chapter describes how to use SMASH-CLP.

Connecting SMASH-CLP

You can use SMASH-CLP (Command Line Protocol) using terminal software on a console terminal connected via SSH. To connect SMASH-CLP, follow these steps:

1. Start the terminal software on a console terminal, and connect to a server blade, on which you use SMASH-CLP, via SSH. For the server blade IP address, see *Finding IP address of BMC*.
2. Enter a user name and a password via SSH to connect to SMASH-CLP. Successful authentication displays the following prompt.

```
/admin1->
```

Using SMASH-CLP

With SMASH-CLP, you can operate "target" shown in a hierarchical structure using "verb". Type the following string in SMASH-CLP command line to operate an item shown in the table: SMASH Operations.

<verb> [<options>] [<target>] [<properties>]

For the SMASH-CLP, see Table 3-1 Verbs and Their Options. For the targets corresponding to items in Table 1-1 SMASH Operations, see Table 3-2 Targets for Operations. To view verb option details, enter the following command.

```
help <verb>
```

Example:

```
/admin1->help show
Description:
    The show command is used to display information about Managed
    Elements. It can be used to view information about a single
Managed
    Element, a tree of Managed Elements, or Managed Elements
matching
    a property value filter.
Syntax:
    show [{options}] [{target}] [{properties}] [{propertyname}==
    {propertyvalue}]
Options:
-a, all
    The all option instructs the Command Processor to select all
values
       :
       :
```

To view target properties, move to a target and enter the following.

```
cd <target>
show -display properties
```

Example:

```
/admin1-> cd /admin1/system1/sensors1/numericsensor1
/admin1/system1/sensors1/numericsensor1
/admin1/system1/sensors1/numericsensor1-> show -display properties
/admin1/system1/sensors1/numericsensor1
        properties
                BaseUnits = 5 (Volts)
                CurrentReading = 33264
                CurrentState = Normal
                ElementName = MB 3.3V
                EnabledState = 2 (Enabled)
                HealthState = 5 (OK)
                OperationalStatus =
                    {
                        2 (OK)
                    }
                PossibleStates =
                    {
                        Non-Critical,
                        Lower Non-Critical,
                        Upper Non-Critical,
                        Critical,
                        Lower Critical,
                        Upper Critical,
                        Fatal,
                        Lower Fatal,
                        Upper Fatal,
                        Normal,
                        Unknown
                    }
                RateUnits = 0 (None)
                RequestedState = 12 (Not Applicable)
                SensorType = 3 (Voltage)
                SettableThresholds = NULL
                SupportedThresholds =
                    {
                        3 (UpperThresholdCritical),
                        2 (LowerThresholdCritical)
                    }
                UnitModifier = -4
```

Table 3-1 Verbs and Their Options

Verb	Options	Description
cd	-default, -examine, -help, -output, -version	Changes the current default target.
show	-all, -default, -display, -examine, -help, -level, -output, -version	Views properties and verbs for a target.
exit	-help, -output, -version	Finishes SMASH-CLP.
help	-examine, -help, -output, -version	Shows help for a target.
version	-examine, -help, -output, -version	Shows a version of a target.
set	-examine, -help, -output, -version	Sets properties for a target.
start	-examine, -force, -help, -output, -version	Requests the target to start.
stop	-examine, -force, -help, -output, -state, -version, -wait	Requests the target to stop.
reset	-examine, -help, -output, -version	Requests the target to reset.

Table 3-2 Targets for Operations

Target	Object	Operation
/admin1/system1	Server blade	Displays the server blade status, powers on/off, or reboots.
/admin1/hdwr1/chassis1	Server blade	Displays FRU information.
/admin1/system1/cpu<N> /admin1/hdwr1/chassis1/card1/chip<N> /admin1/system1/capabilities1/cpucap<N>	Processor	Displays the processor status.
/admin1/system1/memory1 /admin1/hdwr1/chassis1/card1/pmem<N>	Memory	Displays the memory status.
/admin1/system1/pwrsupply<N>	Power supply module	Displays the power supply status.
/admin1/system1/fan<N>	Fan module	Displays the fan status.
/admin1/system1/sensors1/sensor<N> /admin1/system1/sensors1/numericsensor<N>	Sensor	Displays the sensor status.
/admin1/system1/sp1	BMC	Displays the BMC status or restarts BMC.
/admin1/system1/settings1/bootcfgsetting1/bootsrcsetting<N>	Boot device	Changes the boot device.
/admin1/system1/sp1/account<N>	Account	Displays account information.

4

WS-Management

This chapter describes how to use WS-Management.

Connecting WS-Management

Use software which supports WS-Management protocol. In this chapter, WinRM is used as an example.

Tip You can download Windows management framework including WinRM from Microsoft web site.

Using WinRM

To perform operations shown in the table OPERATION below, enter the following command line at the command prompt on the WinRM-installed console terminal or in Windows PowerShell.

```
winrm <OPERATION> <RESOURCE_URI> [-SWITCH:VALUE] [@{KEY=VALUE}]
```

For available WinRM operations, see the tables below: Table 4-1 OPERATION, Table 4-2 RESOURCE_URI, and Table 4-3 -SWITCH:VALUE. For WinRM details, see help for WinRM.

Table 4-1 OPERATION

OPERATION	Description
g(et)	Retrieves management information.
s(et)	Sets management information.
c(reate)	Creates a new instance of management resources.
d(elete)	Deletes an instance of management resources.
e(numerate)	Enumerates all instances of management resources.
i(nvoke)	Invokes a method to management resources.
id(entify)	Identifies if WS-Management is executed on the server blade connected.

Table 4-2 RESOURCE_URI

RESOURCE	Description
cimv2/CIM_ComputerSystem	Powers on/off, reboots server blades, or restarts the BMC.
cimv2/CIM_Processor	Retrieves the processor status.
cimv2/CIM_Chip	
cimv2/CIM_ProcessorCapabilities	

RESOURCE	Description
cimv2/CIM_Memory	Retrieves the memory status.
cimv2/CIM_PhysicalMemory	
cimv2/CIM_PowerSupply	Retrieves the power status.
cimv2/CIM_Fan	Retrieves the fan status.
cimv2/CIM_Sensor	Retrieves sensor information.
cimv2/CIM_NumericSensor	
cimv2/CIM_Chassis	Retrieves server blade FRU information.
cimv2/CIM_BootConfigSetting	Switches boot device.
cimv2/CIM_Account	Retrieves account information.

Table 4-3 -SWITCH:VALUE

-SWITCH	VALUE	Description
-r(emote)	[TRANSPORT]	Sets a URI scheme: HTTP or HTTPS. The default value is HTTP but select HTTPS.
	HOST	Sets a host address. Valid formats: DNS name, NetBIOS name or IP address.
	[PORT]	By default, 5985 is used for HTTP; 5986 for HTTPS.
	[PREFIX]	By default, wsman is set.
-u(sername)	USERNAME	Specifies the user name for a server blade connected.
-p(assword)	PASSWORD	Specifies the user password for a server blade connected.
-a(uthentication)	VALUE	Specifies authentication mechanism used for server connection - None - Basic - Digest - Negotiate
-encoding	VALUE	Specifies the encoding for communication with a server blade connected.
-file	VALUE	Specifies an XML file read from a file when s(et), c(reate) and i(nvoke) operations are executed.

The following shows an example of command for using WinRM. The example assumes that you have created an account with user name "userA" and password "pass01". Also assumes BMC's IP address is "192.168.0.1".

To view sensor information, start WinRM by a command like the following.

```
C:\>winrm e cimv2/CIM_Sensor -r:https://192.168.0.1:5986/wsman -
u:userA -p:pass01 -a:basic -encoding:utf-8
```

Example:

```
C:\>winrm e cimv2/CIM_Sensor -r:https://192.168.0.1:5986/wsman -
u:userA -p:pass01 -a:basic -encoding:utf-8
CIM_NumericSensor
    BaseUnits = 5
    CreationClassName = CIM_NumericSensor
    CurrentReading = 33264
    CurrentState = Normal
    DeviceID = 1.22.0.32.01.99
    ElementName = MB 3.3V
    EnabledState = 2
    HealthState = 5
    LowerThresholdCritical = 29664
    LowerThresholdFatal = 0
    LowerThresholdNonCritical = 0
    OperationalStatus = 2
    OtherSensorTypeDescription = NONE
    PossibleStates = Non-Critical, Lower Non-Critical, Upper Non-
Critical, Critical, Lower Critical, Upper Critical, Fatal, Lower
Fatal, Upper Fatal, Normal, Unknown
    RateUnits = 0
    RequestedState = 12
    SensorType = 3
    SettableThresholds = null
    SupportedThresholds = 3, 2
    SystemCreationClassName = CIM_ComputerSystem
    SystemName = srv:FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    UnitModifier = -4
    UpperThresholdCritical = 36288
    UpperThresholdFatal = 0
    UpperThresholdNonCritical = 0

CIM_NumericSensor
       :
       :
```

Tip When an error message saying that the envelope is too large is displayed, enter the following command to avoid troubles.

```
C:\>winrm s winrm/config @{MaxEnvelopeSizekb="4096"}
```

5

SMASH operation

This chapter describes how to operate SMASH.

Retrieving server blade information

You can retrieve identification and status of server blades by SMASH; for example, to know the chassis serial number and the slot number where a server blade is installed. You can extract them from **OtherIdentifyingInfo** property in the instance of CIM_ComputerSystem class.

WS-Management

By using WS-Management to retrieve server blade information, you can find the information in the instance of which **Dedicated** property is 0 (Not dedicated) among the instances in the CIM_ComputerSystem class.

SMASH-CLP

Enter the following command.

```
cd /admin1/system1
show
```

Properties

Table 5-1 CIM_ComputerSystem class properties for server blade

Property	Description
EnabledState	Shows the power status of the server blade. 2 (Enabled) : Power is ON. 3 (Disabled) : Power is OFF.
HealthState	Shows whether a failure occurred or not. 5 (OK) : Normal 10 (Degraded/Warning) : Warning 25 (Critical error) : Failure
OperationalStatus	Shows whether a failure occurred or not. 2 (OK) : Normal 3 (Degraded) : Warning 6 (Error) : Failure
IdentifyingDescriptions	Shows the character string that represents the **OtherIdentifyingInfo** property. The order of items corresponds to that of **OtherIdentifyingInfo** property.

Property	Description
OtherIdentifyingInfo	Shows the server identifying character string. The format corresponds to **IdentifyingDescriptions** "HITACHI::LocationID" is "<Chassis serial number>:<Blade slot number>".

Powering on/off or rebooting server blade

You can power on/off and reboot server blade. Note that SMASH does NOT shut down the OS automatically in powering off or rebooting.

WS-Management

1. Find the instance of which **Dedicated** property is 0 (Not dedicated) among the instances in the CIM_ComputerSystem class.
2. Invoke **RequestStateChange()** method of the instance with appropriate **RequestedState** parameter shown below.

Table 5-2 RequestedState parameters

RequestedState parameter	Operation
2 (Enabled)	Powers on.
3 (Disabled)	Powers off.
11 (Reset)	Reboots.

SMASH-CLP

You can power on/off and reboot server blades by entering the following commands:

To power on

```
start /admin1/system1
```

To power off

```
stop /admin1/system1
```

To reboot

```
reset /admin1/system1
```

Retrieving processor status

You can retrieve the processor status.

WS-Management

You can get the status by retrieving the CIM_Processor class instances.

SMASH-CLP

You can get the status by entering the following command.

```
cd /admin1/system1/cpu<N>
show
```

Properties

Table 5-3 CIM_Processor class properties

Property	Description
ElementName	Shows the name of the processor. If the value is "Unknown", the processor is not installed.
HealthState	Shows whether a failure occurred or not. 5 (OK) : Normal 10 (Degraded/Warning) : Warning 25 (Critical error) : Failure
OperationalStatus	Shows whether a failure occurred or not. 2 (OK) : Normal 3 (Degraded) : Warning 6 (Error) : Failure

Retrieving memory status

You can retrieve the memory status.

WS-Management

You can get the status by retrieving the CIM_PhysicalMemory class instances.

SMASH-CLP

You can get the status by entering the following command.

```
cd /admin1/hdwr1/chassis1/card1/pmem<N>
show
```

Properties

Table 5-4 CIM_PhysicalMemory class properties

Property	Description
Capacity	Shows the memory capacity. If the value is "0" (zero), memory module is not installed.
HealthState	Shows whether a failure occurred or not. 5 (OK) : Normal 10 (Degraded/Warning) : Warning 25 (Critical error) : Failure
OperationalStatus	Shows whether a failure occurred or not. 2 (OK) : Normal 3 (Degraded) : Warning 6 (Error) : Failure

Retrieving power supply module status

You can retrieve the power supply module status.

WS-Management

You can get the status by retrieving the CIM_PowerSupply class instances.

SMASH-CLP

You can get the status by entering the following command.

```
cd /admin1/system1/pwrsupply<N>
show
```

Properties

Table 5-5 CIM_PowerSupply class properties

Property	Description
HealthState	Shows whether a failure occurred or not. 5 (OK) : Normal 10 (Degraded/Warning) : Warning 25 (Critical error) : Failure
OperationalStatus	Shows whether a failure occurred or not. 2 (OK) : Normal 3 (Degraded) : Warning 6 (Error) : Failure

Retrieving fan module status

You can retrieve the fan module status.

WS-Management

You can get the status by retrieving the CIM_Fan class instances.

SMASH-CLP

You can get the status by entering the following command.

```
cd /admin1/system1/fan<N>
show
```

Properties

Table 5-6 CIM_Fan class properties

Property	Description
HealthState	Shows whether a failure occurred or not. 5 (OK) : Normal 10 (Degraded/Warning) : Warning 25 (Critical error) : Failure
OperationalStatus	Shows whether a failure occurred or not. 2 (OK) : Normal 3 (Degraded) : Warning 6 (Error) : Failure

Retrieving fan rotating speed

You can retrieve the fan rotating speed.

WS-Management

You can get the information in the following steps:

1. Find the CIM_Fan class instance.
2. Extract the sensor number (<SensorNumber>) from the **DeviceID** property in the instance.
3. Find the instance corresponding to the <SensorNumber> from among the CIM_NumericSensor class instances.
4. The **CurrentReading** property in the instance found in the step 3 shows the rotating speed.

The format of the **DeviceID** property in the CIM_Fan class is:

```
<EntityID> ":" <EntityInstance> ":" <SensorNumber> ":Fan"
```

<SensorNumber> is surrounded by second and third colons(":").

The format of the **DeviceID** property in the CIM_NumericSensor class is:

```
<1 or 2>.<SensorNumber>.<OwnerLUN>.<Event/Reading Type
Code>.<Sensor Specific Offset or 99>
```

<SensorNumber> is surrounded by first and second periods(".").

SMASH-CLP

You can get the rotating speed from the target **/admin1/system1/sensors1/numericsensor<N>** of which **ElementName** property begins with "FAN".

Retrieving server blade FRU information

You can retrieve server blade FRU information.

WS-Management

You can get server blade FRU information by retrieving the CIM_Chassis class instance.

SMASH-CLP

You can get server blade FRU information by entering the following command.

```
cd /admin1/hdwr1/chassis1
show
```

Properties

Table 5-7 CIM_Chassis class properties

Property	Description
Manufacturer	Shows manufacturer of the server blade.
Model	Shows model name of the server blade.
PartNumber	Shows part number of the server blade.
SerialNumber	Shows serial number of the server blade

Changing boot device

You can change boot device for next single boot.

WS-Management

You can change the boot device in the following steps:

1. Find the CIM_BootSourceSetting class instance that containing the **StructuredBootString** property for the boot device you want to use.
2. Find the CIM_BootConfigSetting class instance and invoke **ChangeBootOrder()** method, designating the CIM_BootSourceSetting class instance found above as a parameter.

To use WinRM, execute the following command:

```
C:\>winrm i ChangeBootOrder cimv2/CIM_BootConfigSetting?InstanceID
=CIM:bcs1 -r:https://192.168.0.1:5968/wsman -a:basic -u:userA -p:p
ass01 -encoding:utf-8 -file:input-ChangeBootOrder.xml
```

The contents of the input-ChangeBootOrder.xml is shown below:

```
<n1:ChangeBootOrder_INPUT
  xmlns:n1="http://schemas.dmtf.ofg/wbem/wscim/1/cim-schema/2/CIM_
BootConfigSetting"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd">
  <n1:Source>
    <wsa:ReferenceParameters>
       <wsman:ResourceURI>http://schemas.dmtf.org/wbem/wscim/1/cim
-schema/2/CIM_BootSourceSetting</wsman:ResourceURI>
      <wsman:SelectorSet>
        <wsman:Selector Name="InstanceID">BootSource</wsman:Selec
tor>
      </wsman:SelectorSet>
    </wsa:ReferenceParameters>
  </n1:Source>
</n1:ChangeBootOrder_INPUT>
```

Replace **BootSource** in the file by **InstanceID** property value of the CIM_BootSourceSetting instance which you want to use.

SMASH-CLP

You can change the boot device in the following steps:

1. Find the target **bootsrcsetting<N>** under **/admin1/system1/settings1/ bootcfgsetting1**, which **StructuredBootString** property is the device you want to boot from.
2. Execute the following command.

```
cd /admin1/system1/settings1/bootcfgsetting1
set bootorder="/admin1/system1/settings1/bootcfgsetting1/bootsrcse
tting<N>"
```

The following table shows the relationship between **StructuredBootString** property values and the boot device.

Table 5-8 StructuredBootString property values

StructuredBootString property	Boot device
HITACHI:None:1	None. Cancels the boot device designation.
CIM:Network:1	PXE boot
CIM:Hard-Disk:1	Hard disk
CIM:CD/DVD:1	CD/DVD ROM

Restarting BMC

You can restart BMC. Note that this operation terminates current SMASH session immediately.

WS-Management

You can restart BMC in the following steps:

1. Find the instance of which **Dedicated** property is 28 (Management Controller) among the instances in the CIM_ComputerSystem class.
2. Execute the **RequestStateChange()** method in the instance, designating 11 (Reset) as a **RequestedState** parameter.

SMASH-CLP

You can restart BMC by entering the following command.

```
reset /admin1/system1/sp1
```

(This page is intentionally left blank)

6

CIM classes, properties and methods

This chapter provides the list of CIM classes, properties and methods.

- List of CIM classes, properties and methods

List of CIM classes, properties and methods

Table 6-1 shows supported CIM classes, properties and methods. This list covers only major ones.

Table 6-1 CIM classes, properties, and methods table

Profile Name	CIM class	Property or method
Base Server	CIM_ComputerSystem	Name
		CreationClassName
		EnabledState
		RequrestedState
		OperationalState
		HealthState
		ElementName
		Dedicated
		IdentifyingDescriptions
		OtherIdentifyingInfo
		RequestedStateChange()
	CIM_ComputerSystemPackage	PlatformGUID
	CIM_ElementCapabilities	
	CIM_EnabledLogicalElementCapabilities	RequestedStatesSupported
	CIM_Chassis	
SMASH Collection	CIM_ConcreteCollection	
	CIM_MemberOfCollection	
	CIM_OwningCollectionElement	
SM CLP Admin Domain	CIM_AdminDomain	
	CIM_ConcreteCollection	
	CIM_MemberOfCollection	
	CIM_OwningCollectionElement	
	CIM_SystemComponent	
Sensors	CIM_Sensor	SystemCreationClassName
		SystemName
		CreationClassName
		DeviceID
		SensorType
		PossibleStates
		CurrentStates
		ElementName

Profile Name	CIM class	Property or method
		OtherSensorTypeDescription
	CIM_NumericSensor	SystemCreationClassName
		SystemName
		CreationClassName
		DeviceID
		SensorType
		PossibleStates
		CurrentStates
		ElementName
		OtherSensorTypeDescription
		BaseUnits
		UnitModifier
		RateUnits
		CurrentReading
		LowerThresholdNonCritical
		UpperThresholdNonCritical
		LowerThresholdCritical
		UpperThresholdCritical
		LowerThresholdFatal
		UpperThresholdFatal
		SupportedThresholds
	CIM_SystemDevice	
Physical Asset	CIM_Card	
	CIM_Chassis	Tag
		CreationClassName
		PackageType
		ChassisPackageType
		Manufacturer
		Model
		SerialNumber
		PartNumber
		ElementName
	CIM_Chip	
	CIM_ComputerSystemPackage	PlatformGUID
	CIM_Container	
	CIM_ElementCapabilities	
	CIM_PhysicalAssetCapabilities	FRUInfoSupported
	CIM_PhysicalMemory	Tag

Profile Name	CIM class	Property or method
		CreationClassName
		FormFactor
		MemoryType
		Speed
		Capacity
		BankLabel
		ElementName
		HealthState
		OperationalStatus
	CIM_PhysicalPackage	CreationClassName
		PackageType
		CanBeFRUed
		ElementName
	CIM_Realizes	
Boot Control	CIM_BootService	
	CIM_BootConfigSetting	InstanceID
		ElementName
		ChangeBootOrder()
	CIM_BootSourceSetting	StructuredBootString
	CIM_ElementCapabilities	
	CIM_ElementSettingData	
	CIM_HostedService	
	CIM_OrderedComponent	
	CIM_ServiceAffectsElement	
Fan	CIM_Fan	SystemCreationClassName
		SystemName
		CreationClassName
		DeviceID
		OperationalStatus
		HealthState
		EnabledState
		ElementName
	CIM_SystemDevice	
Power Supply	CIM_PowerSupply	SystemCreationClassName
		SystemName
		CreationClassName
		DeviceID
		ElementName

Profile Name	CIM class	Property or method
		OperationalStatus
		HealthState
	CIM_SystemDevice	
Service Processor	CIM_ComputerSystem	CreationClassName
		Dedicated
		ElementName
		IdentifyingDescriptions
		Name
		OtherIdentifyingInfo
		RequestStateChange()
	CIM_ElementCapabilities	
	CIM_EnabledLogicalElementCapabilities	RequestedStatesSupported
CPU	CIM_ElementCapabilities	
	CIM_Processor	SystemCreationClassName
		SystemName
		CreationClassName
		DeviceID
		Family
		CurrentClockSpeed
		MaxClockSpeed
		ExternalBusClockSpeed
		CPUStatus
		EnabledState
		OperationalStatus
		HealthState
		ElementName
		Stepping
	CIM_ProcessorCapabilities	InstanceID
		NumberOfProcessorCore
		NumberOfHardwareThreads
	CIM_SystemDevice	
System Memory	CIM_Memory	SystemCreationClassName
		SystemName
		CreationClassName
		DeviceID
		Volatile
		Access
		BlockSize

Profile Name	CIM class	Property or method
		NumberOfBlocks
		OperationalStatus
		HealthState
		ElementName
	CIM_SystemDevice	
Profile Registration	CIM_RegisteredProfile	InstanceID
		RegisteredOrganization
		RegisteredName
		RegisteredVersion
	CIM_ElementConformsToProfile	
	CIM_ReferencedProfile	
Simple Identity Management	CIM_Account	SystemCreationClassName
		SystemName
		CreationClassName
		Name
		UserID
		UserPassword
		ElementName
		EnabledState
	CIM_AccountManagementCapabilities	
	CIM_AccountManagementService	
	CIM_AccountOnSystem	
	CIM_AssignedIdentity	
	CIM_ElementCapabilities	
	CIM_HostedService	
	CIM_Identity	
	CIM_ServiceAffectsElement	

7

Troubleshooting

This chapter describes troubleshooting for the SMASH.

- Troubleshooting problems

Troubleshooting problems

This section describes examples of basic troubleshooting with the SMASH.

Table 7-1 Troubleshooting

#	Problem	Description
1	Cannot connect to BMC	Check the following from web console. 1) BMC's IP address and ports are properly configured. 2) IPMI/SMASH user account is properly configured. 3) Secure transport protocol (HTTPS or SSH) is used. HTTP and telnet are not supported. 4) Connection from your client PC's IP address is allowed.

2	An error message displayed when "`show /admin1/hdwr1/chassis1`" is executed in CLP.	The error message is below.
		`cmdstat`
		`status : 2`
		`status_tag : COMMAND PROCESSING FAILED`
		`error : 246`
		`error_tag : INVALID TARGET`
		
		This message appears when asset tag contains non-ASCII characters. Compute Blade series only support ASCII encoding for asset tag.
		Set asset tag containing only ASCII characters from web console.

8

IPMI Command List

This chapter provides the list of supported IPMI commands.

- IPMI Command List

IPMI Command List

Table 8-1 shows the list of supported IPMI commands.

Table 8-1 Supported IPMI commands

Command	NetFn	CMD
IPMI Device "Global" Commands		
Get Device ID	App(06h,07h)	01h
Get ACPI Power State	App(06h,07h)	07h
BMC Watchdog Timer Commands		
Reset Watchdog Timer	App(06h,07h)	22h
Set Watchdog Timer	App(06h,07h)	24h
Get Watchdog Timer	App(06h,07h)	25h
BMC Device and Messaging Commands		
Get System GUID	App(06h,07h)	37h
Get Channel Authentication Capabilities	App(06h,07h)	38h
Set Session Privilege Level	App(06h,07h)	3Bh
Close Session	App(06h,07h)	3Ch
Get Session Info	App(06h,07h)	3Dh
Set Channel Access	App(06h,07h)	40h
Get Channel Access	App(06h,07h)	41h
Set User Access	App(06h,07h)	43h
Get User Access	App(06h,07h)	44h
Set User Name	App(06h,07h)	45h
Get User Name	App(06h,07h)	46h
Set User Password	App(06h,07h)	47h
Activate Payload	App(06h,07h)	48h
Deactivate Payload	App(06h,07h)	49h
Get Payload Activation Status	App(06h,07h)	4Ah
Get Payload Instance Info	App(06h,07h)	4Bh
Set User Payload Access	App(06h,07h)	4Ch
Get User Payload Access	App(06h,07h)	4Dh
Get Channel Cipher Suites	App(06h,07h)	54h
Chassis Device Commands		
Get Chassis Capabilities	Chassis(00h,01h)	00h
Get Chassis Status	Chassis(00h,01h)	01h
Chassis Control	Chassis(00h,01h)	02h
Chassis Identify[1]	Chassis(00h,01h)	04h
Set System Boot Options[2]	Chassis(00h,01h)	08h

Command	NetFn	CMD
Get System Boot Options	Chassis(00h,01h)	09h
Sensor Device Commands		
Get Sensor Threshold	Sensor/Event(04h,05h)	27h
Get Sensor Reading	Sensor/Event(04h,05h)	2Dh
FRU Device Commands		
Get FRU Inventory Area Info	Storage(0Ah,0Bh)	10h
Read FRU Data	Storage(0Ah,0Bh)	11h
SDR Device Commands		
Get SDR Repository Info	Storage(0Ah,0Bh)	20h
Reserve SDR Repository	Storage(0Ah,0Bh)	22h
Get SDR	Storage(0Ah,0Bh)	23h
SEL Device Commands		
Get SEL Info	Storage(0Ah,0Bh)	40h
Reserve SEL	Storage(0Ah,0Bh)	42h
Get SEL Entry	Storage(0Ah,0Bh)	43h
Clear SEL	Storage(0Ah,0Bh)	47h
Get SEL Time	Storage(0Ah,0Bh)	48h
Set SEL Time	Storage(0Ah,0Bh)	49h
LAN Device Commands		
Set LAN Configuration Parameters[3]	Transport(0Ch,0Dh)	01h
Get LAN Configuration Parameters	Transport(0Ch,0Dh)	02h
Serial/Modem Device Commands		
Set SOL Configuration Parameters[4]	Transport(0Ch,0Dh)	21h
Get SOL Configuration Parameters	Transport(0Ch,0Dh)	22h
DCMI Commands		
Get Asset Tag	DCGRP(2Ch,2Dh)	06h
Set Asset Tag	DCGRP(2Ch,2Dh)	08h

Notes:

1. This command makes Identify LED turn on or turn off. Identify LED blinks when Pre-configure is executed. If this command and Pre-configure operate simultaneously, the LED will be in a blink state.
2. Only Boot Device Selector is supported. Selectable Options are "No override" and "Force PXE".
3. Configurable parameters are "IPv4 Header Parameters" and "RMCP+ Messaging Cipher Suite Privilege Levels".
4. Configurable parameters are "SOL Enable", "SOL Authentication", "Character Accumulate Interval", "Character Send Threshold" and "SOL Retry".

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

MK-99COM144-01