

# bullx S6000 Remote Hardware Management CLI

Reference Guide

extreme computing





# bullx S6000

# Remote Hardware

# Management CLI

## Reference Guide

Hardware

December2011

Bull Cedoc  
357 avenue Patton  
BP 20845  
49008 Angers Cedex 01  
FRANCE

REFERENCE  
86 A1 50FG 02

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright ©Bull SAS 2011

Printed in France

## Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark misuse.

*The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.*

# Table of Contents

<b>Preface</b> .....	<b>vii</b>
Intended Readers .....	vii
Highlighting .....	vii
Related Publications .....	viii
<b>Chapter 1. Introduction</b> .....	<b>1-1</b>
1.1. Installation .....	1-2
1.2. Target host connection .....	1-3
1.3. Model requirements .....	1-4
1.3.1. lanplus model .....	1-4
1.3.2. ipmidrv model .....	1-4
1.4. Password specification .....	1-4
1.5. IPMITOOL Configuration .....	1-5
<b>Chapter 2. CLI command for bullx super-node</b> .....	<b>2-1</b>
2.1. bsmevent .....	2-2
2.1.1. Options .....	2-2
2.1.2. Usage: Server using lanplus model .....	2-3
2.2. bsmfru .....	2-4
2.2.1. Options .....	2-4
2.2.2. Usage: Server using lanplus model .....	2-5
2.2.3. Usage: Server using ipmidrv model .....	2-8
2.3. bsmFWcmd .....	2-9
2.3.1. Options .....	2-9
2.3.2. Usage .....	2-9
2.4. bsmFWupg .....	2-11
2.4.1. Options .....	2-11
2.4.2. Usage: NovaScale servers updated via kiratool .....	2-12
2.4.3. Usage: Bull servers updated via ipmitool bulloem extension .....	2-13
2.5. bsmGetConfParam .....	2-15
2.5.1. Options .....	2-15
2.5.2. Usage .....	2-15
2.6. bsmGetFunctionalProfile .....	2-17
2.6.1. Options .....	2-17
2.6.2. Usage .....	2-17
2.7. bsmGetHardwareExclusion .....	2-18
2.7.1. Options .....	2-18
2.7.2. Usage .....	2-18
2.8. bsmGetModuleLevelInfo .....	2-19
2.8.1. Options .....	2-19
2.8.2. Usage .....	2-19
2.9. bsmGetPartitionLevelInfo .....	2-20
2.9.1. Options .....	2-20
2.9.2. Usage .....	2-20

2.10.	bsmGetPlatformLevelInfo .....	2-22
	2.10.1. Options .....	2-22
	2.10.2. Usage .....	2-23
2.11.	bsmHWInfocmd .....	2-24
	2.11.1. Options .....	2-24
	2.11.2. Usage .....	2-25
2.12.	bsmHWpm .....	2-31
	2.12.1. Options .....	2-31
	2.12.2. Usage .....	2-32
2.13.	bsmidentify .....	2-44
	2.13.1. Options .....	2-44
	2.13.2. Usage: Server using lanplus model .....	2-44
	2.13.3. Usage: Server using ipmidrv model .....	2-44
2.14.	bsminfo .....	2-45
	2.14.1. Options .....	2-45
	2.14.2. Usage .....	2-45
2.15.	bsmlog .....	2-47
	2.15.1. Options .....	2-47
	2.15.2. Usage: Server using lanplus model .....	2-48
	2.15.3. Usage: Server using ipmidrv model .....	2-48
2.16.	bsmOSpm .....	2-49
	2.16.1. Options .....	2-49
	2.16.2. Usage .....	2-49
2.17.	bsmPDUpower .....	2-54
	2.17.1. Options .....	2-54
	2.17.2. Usage .....	2-55
2.18.	bsmpower .....	2-58
	2.18.1. Options .....	2-59
	2.18.2. Usage: Server using lanplus model .....	2-60
	2.18.3. Usage: Server using ipmidrv model .....	2-62
2.19.	bsmreset .....	2-63
	2.19.1. Options .....	2-63
	2.19.2. Usage .....	2-63
2.20.	bsmResetALLEMMPartition .....	2-64
	2.20.1. Options .....	2-64
	2.20.2. Usage .....	2-64
2.21.	bsmsensor .....	2-65
	2.21.1. Options .....	2-65
	2.21.2. Usage: Server using lanplus model .....	2-66
	2.21.3. Usage: Server using ipmidrv model .....	2-68
2.22.	bsmSetConfParam .....	2-69
	2.22.1. Options .....	2-69
	2.22.2. Usage .....	2-69
2.23.	bsmSetPartition .....	2-72
	2.23.1. Options .....	2-72
	2.23.2. Usage .....	2-72
2.24.	bsmSetPlatformLevelParam .....	2-73
	2.24.1. Options .....	2-73
	2.24.2. Usage .....	2-73

2.25.	bsmsol .....	2-74
2.25.1.	Options .....	2-74
2.25.2.	Usage .....	2-74
<b>Appendix A.</b>	<b>Server ON / OFF Status Codes .....</b>	<b>A-1</b>
<b>Appendix B.</b>	<b>User/Password Internal Authentication File .....</b>	<b>B-1</b>
B.1.	User/Password Authentication .....	B-1
B.2.	bsmcfg_auth_cmd command .....	B-2
B.2.1.	Options .....	B-2
B.2.2.	Usage .....	B-3
<b>Glossary</b> .....		<b>g-1</b>





## Preface

This guide describes the Hardware Management CLI (Command Line Interface) for bullx S6000 series servers.

---

**Note** The Bull Support Web site may be consulted for product information, documentation, updates and service offers:

<http://support.bull.com>

---

## Intended Readers

This guide is intended for System Administrators and Operators in charge of managing systems locally and remotely and of writing server management batch scripts.

## Highlighting

The following highlighting conventions are used in this guide:

<b>Bold</b>	Identifies the following: <ul style="list-style-type: none"><li>• Interface objects such as menu names, labels, buttons and icons.</li><li>• File, directory and path names.</li><li>• Keywords to which particular attention must be paid.</li></ul>
<i>Italics</i>	Identifies references such as manuals or URLs.
<code>monospace</code>	Identifies portions of program codes, command lines, or messages displayed in command windows.
< >	Identifies parameters to be supplied by the user.

Commands entered by the user

-----  
System messages displayed on the screen  
-----



### **WARNING**

A *Warning* notice indicates an action that could cause damage to a program, device, system, or data.

## Related Publications

This list is not exhaustive. Useful documentation is supplied on the Resource & Documentation CD(s) delivered with your system. You are strongly advised to refer carefully to this documentation before proceeding to configure, use, maintain, or update your system.

- *Site Preparation Guide, 86 A1 40FA*  
explains how to prepare a Data Processing Center for Bull Systems, in compliance with the standards in force. This guide is intended for use by all personnel and trade representatives involved in the site preparation process.
- *bullx S6010-S6030 mono-module Server Hardware Console User's Guide, 86 A1 50FD*  
explains how to use the console to manage your mono-module server. This guide is intended for use by server administrators, operators and qualified support personnel.
- *bullx S6030 mono-module Installation Guide, 86 A1 26FE*  
explains how to install and start the mono-module server for the first time. This guide is intended for use by qualified support personnel.
- *bullx S6030 mono-module Service Guide, 86 A7 85FB*  
explains how to service the mono-module server. This guide is intended for use by qualified support personnel.
- *bullx S6010 mono-module Installation Guide, 86 A1 86FB*  
explains how to install and start the mono-module server for the first time. This guide is intended for use by qualified support personnel.
- *bullx S6010 mono-module Service Guide, 86 A7 87FB*  
explains how to service the mono-module server. This guide is intended for use by qualified support personnel.
- *Resource and Documentation CD*  
contains the tools and documentation required to configure, operate and maintain the system.

# Chapter 1. Introduction

The Hardware Management CLI is delivered on the *Resource and Documentation CD*. The Hardware Management CLI provides an easy Command Line Interface (CLI) for local or remote hardware management and automation scripts. It is designed for:

- bullx S6000 series servers
- A32 or IA64 architectures,
- Linux systems ONLY.

This guide describes the Hardware Management CLI (Command Line Interface) for bullx S6000 series servers.

## 1.1. Installation

Install the BSM Hardware CLI RPM package provided on the Resource and Documentation CD:

1. Insert the CD in the drive and browse to the directory containing the RPM package:

**Resources > Software > Linux > BSMHW<release>.i386.rpm**

2. Copy the RPM package and install by launching:

```
rpm -i BSMHW<release>.i386.rpm
```

## 1.2. Target host connection

The Hardware Management CLI uses both Out-of-Band and In-Band connections to the server.

The Out-Of-Band network protocols used for these connections are based on IPMIoverLAN, SNMP:

- IPMIoverLAN for bullx series using the ipmilan or lanplus model.
- SNMP requests to the SNMP agent of Power Distribution Units (PDU).

Most of the commands may also use an InBand connection for local Hardware Management of NovaScale servers running Linux and managed via IPMI using the ipmidrv model.

Most of the commands may also use authentication file. This is why the following packages have to be installed:

- perl-XML-LibXML,
- perl-XML-LibXML-Common,
- perl-XML-SAX,
- perl-XML-Namespacesupport.

There are installed in the the bin subdirectory of the BSMHW package install directory (Default: /opt/BSMHW/bin).

## 1.3. Model requirements

The Hardware Management CLI is designed for range of server types. The protocol used to connect the target hosts is given via `-m model` parameter.

Although very similar, the some models have some mandatory arguments.

### 1.3.1. lanplus model

- Model used for Cool Cabinet Door and the novascale server that uses IPMI.
- The `user` argument is mandatory.
- If `-p password` is not specified, the password (that may be found or not) is searched in the internal authentication file.
- IPMI connection is established with the lanplus interface using cipher suite IDs for authentication, integrity, and encryption algorithms. The default cipher suite ID is 3 and specifies the RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.

### 1.3.2. ipmidrv model

- Model used for the server with the ipmidrv driver.
- IPMI management of a local system requires the installation and configuration of the Linux OpenIPMI driver and the installation of the OpenIPMI library.
- The `user`, `password` and `host` arguments MUST NOT be specified for local hardware management via IPMI.

## 1.4. Password specification

All password arguments may be either specified by `-p password` or extracted from the internal authentication file. This file is created with the `bsmcfg_auth_cmd.sh` command, detailed in Appendix B.

## 1.5. IPMITOOL Configuration

It is possible to change some IPMITOOL configuration parameters:

- CYPHER\_SUITE\_ID: this parameter specifies the authentication, integrity and confidentiality algorithms used when connecting via the lanplus interface. The default value is 3.
- ME\_CHANNEL: this parameter specifies the destination channel for IPMI requests. The default value is 0x06.
- ME\_ADDRESS: this parameter specifies the IPMB address for ipmi requests. The default value is 0x2c.

The parameters to change are in the `bsmcli.cfg.custom.sh.tmpl` file.

1. Rename the file, as shown, so that it can be called by the BSM CLI scripts.

```
$ cd /opt/BSMHW/bin  
$ mv bsmcli.cfg.custom.sh.tmpl bsmcli.cfg.custom.sh
```

2. Edit the `bsmcli.cfg.custom.sh` file, modifying the values you want to change.
3. Save the file.





## Chapter 2. CLI command for bullx super-node

This chapter describes Hardware Management CLI available for bullx super-node:

- `bsmevent`, on page 2-2
- `bsmfru`, on page 2-4
- `bsmFWcmd`, on page 2-9
- `bsmFWupg`, on page 2-11
- `bsmGetConfParam`, on page 2-15
- `bsmGetFunctionalProfile`, on page 2-17
- `bsmGetHardwareExclusion`, on page 2-18
- `bsmGetModuleLevelInfo`, on page 2-19
- `bsmGetPartitionLevelInfo`, on page 2-20
- `bsmGetPlatformLevelInfo`, on page 2-22
- `bsmHWinfocmd`, on page 2-24
- `bsmHWpm`, on page 2-31
- `bsmidentify`, on page 2-44
- `bsminfo`, on page 2-45
- `bsmlog`, on page 2-47
- `bsmOSpm`, on page 2-49
- `bsmPDUpower`, on page 2-54
- `bsmpower`, on page 2-58
- `bsmreset`, on page 2-63
- `bsmResetAllEMMPartition`, on page 2-64
- `bsmsensor`, on page 2-65
- `bsmSetConfParam`, on page 2-69
- `bsmSetPartition`, on page 2-72
- `bsmSetPlatformLevelParam`, on page 2-73
- `bsmsol`, on page 2-74

## 2.1. bsmevent

bsmevent.sh is used to add the events attached to a sensor to the SEL repository.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.1.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-a action	Action: <b>setEvent</b> <b>testEvent</b>
-m model	Target server model: <b>lanplus</b>
-H host	BMC target IP address.
-u user	BMC user.
-p password	User password.
-s sensorID	Sensor identifier (put between double-quote).
-d landest	Alert destination number.
-b state	State for the sensor identifier (default is list). Possible states are: <b>list, lnr, lcr, lnc, unc, ucr, unr</b> .
-e eventDir	Direction taken by the state (default is assert).
-i i2csaAdr	Address of the device generating the event (default is the BMC address).
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which <b>stdout</b> and <b>stderr</b> outputs are redirected.

## 2.1.2. Usage: Server using lanplus model

### Syntax

```
bsmevent.sh [-h] [-l level] -a action -m model -H host [-u user]
[-p password] -s sensorID [-b state] [-e eventDir] [-i i2csaAdr]
[-Y cipher] [-o outfile]
```

### 2.1.2.1. Insert events attached to a sensor to the SEL repository

The `setEvent` action is used to insert events attached to a sensor to the SEL repository.

#### Command

```
$ bsmevent.sh -m lanplus -H X.X.X.X -u MWA -p guest -a setEvent -s "Rear Fan" -b ucr
```

#### Output

```
-----
Finding sensor Rear Fan... ok
0x0000 | Pre-Init Time-stamp | Fan #0200#40 | Upper Critical going high
#590100
-----
```

### 2.1.2.2. Test trap event

The `testEvent` action is used to test trap event sent without writing messages in the SEL repository.

The `landest` option corresponds to an alerting destination configured with an alert IP address.

#### Command

```
$ bsmevent.sh -m lanplus -H X.X.X.X -u MWA -p guest
-a testEvent -d 2
```

#### Output

```
-----
-----
```

## 2.2. bsmfru

bsmfru displays the FRU contents using the standard output.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

The FRU is displayed in stdout, as follows:

<fru tag>: <fru content>

---

**Note** Servers are identified by their DNS name or IP address (-H parameter).

---

### 2.2.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-H host	DNS name or target server IP address
-m model	Target server model: lanplus, ipmidrv.
-u user	BMC user for NovaScale target servers.
-p password	User password.
-Y cipher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name where stdout and stderr outputs are redirected.

## 2.2.2. Usage: Server using lanplus model

### Syntax

```
bsmfriu.sh [-h] -m lanplus -H host -u user [-p password]
[-o outfile] [-l level] [-Y cipher]
```

### Command

```
$ bsmfriu.sh -m lanplus -H X.X.X.X -u super -p pass -Y 0
```

### Output

```
-----
FRU Device Description : Builtin FRU Device (ID 0 on MC 0x20)
Product Manufacturer   : BULL
  Product Name         : bullx super node
  Product Part Number  : bullx S6010
  Product Version      : 1.0
  Product Serial       : XAN-S13-00021

FRU Device Description : Module (ID 1 on MC 0x80)
  Chassis Type         : Rack Mount Chassis
  Chassis Part Number  : (not used)
  Chassis Serial       : XAN-LX2-00013

FRU Device Description : PDBL_A (ID 3 on MC 0x80)
  Board Mfg Date       : Fri Feb 18 11:57:00 2011
  Board Mfg            : ASTEEL
  Board Product        : PDBL_A
  Board Serial         : H0110440
  Board Part Number    : 11012882-009
  Board Extra          : 11012882-009
  Board Extra          : 12000741-009
  Board Extra          : proto
  Board Extra          : MAP
  Board Extra          : 12000741-009
  Board Extra          : modif:6,7,8,9
  Board Extra          : BULL

FRU Device Description : ILBL (ID 7 on MC 0x80)
  Board Mfg Date       : Mon Mar 21 13:56:00 2011
  Board Mfg            : ASTEEL
  Board Product        : ILBL
  Board Serial         : HP104504S1041000
  Board Part Number    : 11008737C-004
  Board Extra          : 11008737C-004
  Board Extra          : HP104504S1041000
  Board Extra          : MAP
  Board Extra          : MAP-OK
  Board Extra          : 12000546-004
  Board Extra          : BULL

FRU Device Description : MXB (ID 8 on MC 0x80)
  Board Mfg Date       : Thu Jan 20 11:38:00 2011
  Board Mfg            : ASTEELFLASH
  Board Product        : MXB_C
  Board Serial         : H010301DS1023001
  Board Part Number    : 11008109C-009
  Board Extra          : 11008109C-009
  Board Extra          : H010301DS1023001
  Board Extra          : 10261
  Board Extra          : SFOK
  Board Extra          : 12000747-007
  Board Extra          : reop: modif 1 (4 resistances VIO)
  Board Extra          : BULL

FRU Device Description : PIROM PROC_0 (ID 9 on MC 0x80)
  Processor S-spec/QDF Number : Q3X4
  Processor Sample/Production : Sample
```

```

Number of Cores                : 8
Number of Threads per Core    : 2
System BUS Speed              : 1066 MHz
Core Processor Family         : 6
Core Processor Model          : 14
Core Processor Stepping       : 6
Maximum P1 Core Frequency     : 2266 MHz
Maximum P0 Core Frequency     : 2666 MHz
Maximum Core Voltage ID       : 1.150 V
Minimum Core Voltage ID       : 0.800 V
Core Voltage Tolerance High   : 15 mV
Core Voltage Tolerance Low    : 15 mV
Max Intel QPI Link Transfer Rate: 6400 MT/s
Min Intel QPI Link Transfer Rate: 4800 MT/s
Intel QPI Version Number      : 1.0
Memory Support flags          : LT-SX : Not Supported
Max Intel SMI Transfer Rate   : 6400 MT/s
Min Intel SMI Transfer Rate   : 4800 MT/s
Uncore Voltage ID             : 1.125 V
Uncore Voltage Tolerance High : 0 mV
Uncore Voltage Tolerance Low  : 0 mV
L2 Cache Size                 : 2048 Kb
L3 Cache Size                 : 24576 Kb
Package Revision               : 2.0
Substrate Revision Software ID : 0
Processor Family Number       : AT80604
Processor SKU Number          : 004869AA
Maximum Case Temperature      : 69 °C
Maximum Thermal Design Power  : 130 Watts
Processor Core Feature Flags   : 0x00000000
Multiprocessor Support        : 8 processors socket
Number of Devices in TAP Chain : 0
Serial Number                  : 0xb43771f19a2fcf00

```

FRU Device Description : PIROM PROC\_1 (ID 10 on MC 0x80)

```

Processor S-spec/QDF Number   : Q3X4
Processor Sample/Production    : Sample
Number of Cores                : 8
Number of Threads per Core    : 2
System BUS Speed              : 1066 MHz
Core Processor Family         : 6
Core Processor Model          : 14
Core Processor Stepping       : 6
Maximum P1 Core Frequency     : 2266 MHz
Maximum P0 Core Frequency     : 2666 MHz
Maximum Core Voltage ID       : 1.150 V
Minimum Core Voltage ID       : 0.800 V
Core Voltage Tolerance High   : 15 mV
Core Voltage Tolerance Low    : 15 mV
Max Intel QPI Link Transfer Rate: 6400 MT/s
Min Intel QPI Link Transfer Rate: 4800 MT/s
Intel QPI Version Number      : 1.0
Memory Support flags          : LT-SX : Not Supported
Max Intel SMI Transfer Rate   : 6400 MT/s
Min Intel SMI Transfer Rate   : 4800 MT/s
Uncore Voltage ID             : 1.125 V
Uncore Voltage Tolerance High : 0 mV
Uncore Voltage Tolerance Low  : 0 mV
L2 Cache Size                 : 2048 Kb
L3 Cache Size                 : 24576 Kb
Package Revision               : 2.0
Substrate Revision Software ID : 0
Processor Family Number       : AT80604
Processor SKU Number          : 004869AA
Maximum Case Temperature      : 69 °C
Maximum Thermal Design Power  : 130 Watts
Processor Core Feature Flags   : 0x00000000
Multiprocessor Support        : 8 processors socket
Number of Devices in TAP Chain : 0

```

```

Serial Number                : 0xc5749f1257a7ea00

FRU Device Description : PIROM PROC_2 (ID 11 on MC 0x80)
Processor S-spec/QDF Number : Q3X4
Processor Sample/Production : Sample
Number of Cores              : 8
Number of Threads per Core  : 2
System BUS Speed             : 1066 MHz
Core Processor Family        : 6
Core Processor Model         : 14
Core Processor Stepping      : 6
Maximum P1 Core Frequency    : 2266 MHz
Maximum P0 Core Frequency    : 2666 MHz
Maximum Core Voltage ID      : 1.150 V
Minimum Core Voltage ID      : 0.800 V
Core Voltage Tolerance High  : 15 mV
Core Voltage Tolerance Low   : 15 mV
Max Intel QPI Link Transfer Rate: 6400 MT/s
Min Intel QPI Link Transfer Rate: 4800 MT/s
Intel QPI Version Number     : 1.0
Memory Support flags         : LT-SX : Not Supported
Max Intel SMI Transfer Rate  : 6400 MT/s
Min Intel SMI Transfer Rate  : 4800 MT/s
Uncore Voltage ID           : 1.125 V
Uncore Voltage Tolerance High : 0 mV
Uncore Voltage Tolerance Low  : 0 mV
L2 Cache Size               : 2048 Kb
L3 Cache Size               : 24576 Kb
Package Revision             : 2.0
Substrate Revision Software ID : 0
Processor Family Number      : AT80604
Processor SKU Number         : 004869AA
Maximum Case Temperature     : 69 °C
Maximum Thermal Design Power : 130 Watts
Processor Core Feature Flags  : 0x00000000
Multiprocessor Support       : 8 processors socket
Number of Devices in TAP Chain : 0
Serial Number                : 0x24cefdb417ba0600

FRU Device Description : PIROM PROC_3 (ID 12 on MC 0x80)
Processor S-spec/QDF Number : Q3X4
Processor Sample/Production : Sample
Number of Cores              : 8
Number of Threads per Core  : 2
System BUS Speed             : 1066 MHz
Core Processor Family        : 6
Core Processor Model         : 14
Core Processor Stepping      : 6
Maximum P1 Core Frequency    : 2266 MHz
Maximum P0 Core Frequency    : 2666 MHz
Maximum Core Voltage ID      : 1.150 V
Minimum Core Voltage ID      : 0.800 V
Core Voltage Tolerance High  : 15 mV
Core Voltage Tolerance Low   : 15 mV
Max Intel QPI Link Transfer Rate: 6400 MT/s
Min Intel QPI Link Transfer Rate: 4800 MT/s
Intel QPI Version Number     : 1.0
Memory Support flags         : LT-SX : Not Supported
Max Intel SMI Transfer Rate  : 6400 MT/s
Min Intel SMI Transfer Rate  : 4800 MT/s
Uncore Voltage ID           : 1.125 V
Uncore Voltage Tolerance High : 0 mV
Uncore Voltage Tolerance Low  : 0 mV
L2 Cache Size               : 2048 Kb
L3 Cache Size               : 24576 Kb
Package Revision             : 2.0
Substrate Revision Software ID : 0
Processor Family Number      : AT80604
Processor SKU Number         : 004869AA

```

```
Maximum Case Temperature      : 69 °C
Maximum Thermal Design Power  : 130 Watts
Processor Core Feature Flags  : 0x00000000
Multiprocessor Support       : 8 processors socket
Number of Devices in TAP Chain : 0
Serial Number                 : 0xdac720c5ed6abf00
```

```
FRU Device Description : LCP (ID 15 on MC 0x80)
Board Mfg Date         : Thu Jul  8 10:53:00 2010
Board Mfg              : SANMINA
Board Product         : LCP
Board Serial          : KP09XXXX
Board Part Number     : 11016561-001
Board Extra           : 11016561-001
Board Extra           : KP09XXXX
Board Extra           : 12000417-001
Board Extra           : BULL
```

```
FRU Device Description : PS_0 (ID 4 on MC 0x80)  WARNING : Unknown FRU
header version 0x56
ERROR: Close Session command failed: Invalid command
-----
```

### 2.2.3. Usage: Server using ipmidrv model

#### Syntax

```
bsmfru.sh [-h] -m ipmidrv [-o outfile] [-l level]
```



## 2.3. bsmFWcmd

The **bsmFWcmd** command is used to execute some action on a component firmware.

```
bsmFWcmd -a reset
bsmFWcmd -a backupcfg
bsmFWcmd -a restorecfg
```

**reset** is used to reset a component firmware.

**backupcfg** is used to execute a backup of the BMC configuration.

**restorecfg** is used to restore the backedup BMC configuration.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.3.1. Options

-a action	Action: reset, backupcfg, restorecfg.
-h	Displays command usage.
-m model	Target server model: lanplus.
-M hwmanager	BMC target IP address.
-D directoryPath	Full directory path where backup files will be created (backupcfg) or taken (restorecfg)
-t type	Type of file to restore. Possible values are: system : restore MAC addresses of the module. pef : restore alert filters. config : restore every other configuration parameters.
-s module	Module number (between 0 and 3).
-o outfile	Output file name where <b>stdout</b> and <b>stderr</b> outputs are redirected.
-u user	BMC user.
-p password	User password.
-Y cipher	Cipher suite ID to be used by lanplus interface (default is 3).

### 2.3.2. Usage

#### Syntax

```
bsmFWcmd.sh [-h] -m model -a reset -M hwmanager [-u user -p password] [-Y cipher] [-o outfile]
```

```
bsmFWcmd.sh [-h] -m model -a backupcfg -M hwmanager -D directoryPath [-u user -p password] [-Y cipher] [-o outfile] [-s module]
```

```
bsmFWcmd.sh [-h] -m model -a restorecfg -M hwmanager -D directoryPath -t type [-u user -p password] [-Y cipher] [-o outfile] [-s module]
```

- 
- Notes**
- -D directoryPath is required and mandatory for action backupcfg and restorecfg.
  - -t type is required and mandatory for restorecfg action.
  - -s module is a specific multimodule option.
-

### 2.3.2.1. Execute firmware reset

Command

```
$ bsmFWcmd.sh -a reset -m lanplus - M X.X.X.X -u super -p pass -Y 0
```

### 2.3.2.2. Execute a backup of the BMC configuration

Command

```
$ bsmFWcmd.sh -a backupcfg -m lanplus - M X.X.X.X -u super -p pass -Y 0 -D /tmp
```

Output

-----  
-----

### 2.3.2.3. Execute a restoration of the backed up BMC configuration

Command

```
$ bsmFWcmd.sh -a restorecfg -m lanplus - M X.X.X.X -u super -p pass -Y 0 -D /tmp -t system -s 0
```

Output

-----  
-----

## 2.4. bsmFWupg

bsmFWupg is used to upgrade, using an external tool, the firmware of Remote Management Modules. Operations that can be done:

```
bsmFWupg -a bulloemver
bsmFWupg -a bulloemupg
bsmFWupg -a bulloemlisthw
```

bulloemver: display the component firmware version.

bulloemupg: upgrade the the component firmware.

bulloemlisthw: display the list of components which can be upgraded.

This command is available only for ipmilan model NovaScale servers with Raritan Remote Management Modules that can be manipulated with the KiraTool command line tool, and on Bull servers which use the `bulloem` command extension for `ipmitool`.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

---

**Note** The KiraTool software, that allows you to manipulate the module's firmware, must be installed on the system running `bsmFWupg.sh`. Refer to the *KiraTool User Manual* for the installation procedure.

---

### 2.4.1. Options

-h	Displays command usage.
-D tooldir	Installation directory of the KiraTool command line tool (full path). Default value is C:\Program files\KiraTool for Windows, and /usr/local/bin for Linux.
-F fw_binfile	Name of the firmware binary file used during the upgrade.
-d fw_bindir	Directory where the firmware binary file is (full path). Default value is /tmp.
-H host	DNS name or IP address to identify the module over the LAN.
-t tool	Command line tool: kiratool, ipmitool.
-a action	Action for a component (identified by component_id) on the module (specified by module_id): bulloemver: display the firmware version of the component bulloemupg: upgrade the firmware of the component bulloemlisthw: display the list of components which can be upgraded.
-E component_id	Component name
-M module_id	Module ID, from 0 to 3.
-m model	Target server model: lanplus, ipmidrv. If not present, kcs driver will be used.
-u user	Administration login for the Remote Management Module.
-p password	Administration password for the Remote Management Module.
-o outfile	Output file name to which stdout and stderr outputs are redirected.

## 2.4.2. Usage: NovaScale servers updated via kiratool

### Syntax

```
bsmFWupg.sh [-h] -t kiratool -H host -F fw_binfile [-u user] [-p password]
[-D tooldir] [-d fw_bindir] [-o outfile]
```

### Command to upgrade the firmware

```
$ bsmFWupg.sh -t kiratool -H X.X.X.X -u super -p pass
-F "fw-wub-MESCB_010100_0026.bin"
```

### Output

```
-----
Starting Firmware Upgrade
Uploading Firmware File
0% ----- 50% ----- 100%
*****
Upload complete.
Flashing Firmware (takes about 1min)
Successfully upgraded firmware.
-----
```

## 2.4.3. Usage: Bull servers updated via ipmitool bulloem extension

### Syntax

```
bsmFWupg.sh [-h] -t ipmitool -H host -F [fw_binfile] [-u user]
[-p password] -a action [-E component] [-M module] [-m model]
[-d fw_bindir] [-o outfile]
```

### 2.4.3.1. Display the list of the components that can be upgraded

#### Command

```
$ bsmFWupg.sh -t ipmitool -a bulloemlisthw -H X.X.X.X -u super
-p pass -m lanplus
```

#### Output

```
-----
BMC
LCP
ILBC
MXBC
ADM1069_4_A_98
ADM1069_4_A_9C
ADM1069_3_B_98
ADM1069_3_B_9A
-----
```

#### Command

```
$ bsmFWupg.sh -t ipmitool -a bulloemlisthw -H X.X.X.X
```

#### Output

```
-----
BMC
LCP
ILBC
MXBC
ADM1069_4_A_98
ADM1069_4_A_9C
ADM1069_3_B_98
ADM1069_3_B_9A
-----
```

### 2.4.3.2. Display the firmware version

#### Command

```
$ bsmFWupg.sh -t ipmitool -a bulloemver -H X.X.X.X -u super
-p pass -m lanplus -E LCP -M 1
```

#### Output

```
-----
firmware version of LCP : 20
-----
```

### 2.4.3.3. Upgrade BMC firmware

#### Command

```
$ bsmFWupg.sh -t ipmitool -a bulloemupg -H X.XX.X -u super  
-p pass -F "fw-wub-kira_bulldc_150100_1047.bin" -E BMC
```

#### Output

```
-----  
starting upgrade of BMC on module 0 with firmware in  
/BMC/fw-wub-kira_bulldc_BCE_150100_1047.bin  
->uploading /BMC/fw-wub-kira_bulldc_BCE_150100_1047.bin  
0% ----- 50% ----- 100%  
*****  
->flashing the firmware (takes a couple of minutes)  
You need to reboot the BMC. This upgrade will be active after the  
reboot.  
Upgrade of BMC on module 0 successful.  
-----
```

### 2.4.3.4. Display all firmware versions

#### Command

```
$ bsmFWupg.sh -t ipmitool -a bulloemver -H X.X.X.X -u super -p pass -E all -M 0
```

#### Output

```
-----  
firmware version of LCP : 20  
firmware version of ILBC_BOOT : A.4.4.0.01.00  
firmware version of ILBC_FUNC : B.4.5.0.F2.07  
firmware version of MXBC_FUNC : C.4.5.0.F2.00  
firmware version of ILBC : B.4.5.0.F2.07  
firmware version of MXBC : C.4.5.0.F2.00  
firmware version of ADM1069_4_A_98 : 12.01.10  
firmware version of ADM1069_4_A_9A : 12.02.10  
firmware version of ADM1069_4_A_9C : 12.03.10  
firmware version of ADM1069_4_A_9E : 12.04.10  
firmware version of ADM1069_3_B_98 : 44.01.10  
firmware version of ADM1069_3_B_9A : 44.02.10  
firmware version of ADM1069_3_A_98 : 44.05.10  
firmware version of ADM1069_3_A_9A : 44.06.10  
firmware version of ADM1069_3_A_9C : 44.07.10  
firmware version of ADM1069_3_A_9E : 44.08.10  
firmware version of ADM1069_3_B_9C : 44.03.10  
firmware version of ADM1069_3_B_9E : 44.04.10  
firmware version of ADM1062_4_A_28 : 20.01.10  
firmware version of ADM1062_4_A_2A : 20.02.10  
BMC Firmware version: 11.9.0  
Build number: 1146  
Hardware ID: 0x30  
Firmware tag: Final Edition 20110215  
OEM: bull  
-----
```

## 2.5. bsmGetConfParam

bsmGetConfParam.sh is used to obtain the values of various configuration parameters.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

---

**Note** This command includes the following actions, according to the server

```
bsmGetConfParam -a getPowerRestorePolicy
```

```
bsmGetConfParam -a getPrimaryNTP
```

```
bsmGetConfParam -a getSecondaryNTP
```

---

### 2.5.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged by syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-a action	Action: <b>getPowerRestorePolicy</b> <b>getPrimaryNTP</b> <b>getSecondaryNTP</b>
-m model	Target server model: <b>lanplus</b> .
-H host	BMC target IP address.
-u user	BMC user.
-p password	User password.
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3)
-o outfile	Output file name to which stdout and stderr outputs are redirected.

### 2.5.2. Usage

#### Syntax

```
bsmGetConfParam.sh [-h] [-l level] -a action -m model -H host [-u user] [-p password] [-Y cypher] [-o outfile]
```

### 2.5.2.1. Get the power restore policy

The `getPowerRestorePolicy` action is used to get the power restore policy (On, Off or Restore) which is applied to the system after an AC power loss.

#### Syntax

```
bsmGetConfParam.sh [-h] -a getPowerRestorePolicy -m model -H host  
[-u user] [-p password] [-Y cipher] [-o outfile] [-l level]
```

#### Command

```
$ bsmGetConfParam.sh -m lanplus -H X.X.X.X -u super -p pass  
-a getPowerRestorePolicy
```

#### Output

```
-----  
Power Restore Policy is: on  
-----
```

### 2.5.2.2. Get the primary NTP server IP address

The `getPrimaryNTP` action is used to get the primary NTP server which gives the date and time.

#### Syntax

```
bsmGetConfParam.sh [-h] -a getPrimaryNTP -m model -H host  
[-u user] [-p password] [-Y cipher] [-o outfile] [-l level]
```

#### Command

```
bsmGetConfParam.sh -m lanplus -H X.X.X.X -u super -p pass -a getPrimaryNTP
```

#### Output

```
-----  
Primary NTP server is: Y.Y.Y.Y  
-----
```

### 2.5.2.3. Get the secondary NTP server IP address

The `getSecondaryNTP` action is used to get the secondary NTP server which gives the date and time.

#### Syntax

```
bsmGetConfParam.sh [-h] -a getSecondaryNTP -m model -H host  
[-u user] [-p password] [-Y cipher] [-o outfile] [-l level]
```

#### Command

```
bsmGetConfParam.sh -m lanplus -H X.X.X.X -u super -p pass -a getSecondaryNTP
```

#### Output

```
-----  
Secondary NTP server is: Z.Z.Z.Z  
-----
```



## 2.6. bsmGetFunctionalProfile

`bsmGetFunctionalProfile.sh` is used to get some information for a functional profile of a partition. Currently, it displays the state of the functional profile identifier (active or not) and the state of its Power Restore Policy (on or off).

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.6.1. Options

<code>-h</code>	Displays command usage.
<code>-l level</code>	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
<code>-m model</code>	Target server model: lanplus.
<code>-H IPaddress</code>	BMC IP address for a module included in the platform.
<code>-u user</code>	EMM user.
<code>-p password</code>	User password.
<code>-n functionalProfileID</code>	Functional Profile identifier (0 or 1).
<code>-Y cypher</code>	Cipher suite ID to be used by lanplus interface (default is 3).
<code>-o outfile</code>	Output file name to which <code>stdout</code> and <code>stderr</code> outputs are redirected.

### 2.6.2. Usage

#### Syntax

```
bsmGetFunctionalProfile.sh [-h] [-l level] -m model -H IPaddress [-u user] [-p password] -n functionalProfileID [-Y cypher] [-o outfile]
```

#### Command

```
$ bsmGetFunctionalProfile.sh -m lanplus -H X.X.X.X -u super -p pass -n 0
```

#### Output

```
-----  
Functional profile 0 is active  
Power Restore Policy is: off  
-----
```

## 2.7. bsmGetHardwareExclusion

bsmGetHardwareExclusion is used to get hardware component exclusion list for a module of a platform.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.7.1. Options

-h	Displays command usage
-l level	Specifies the message severity to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus.
-H IPAddress	BMC IP address for a module included in the platform.
-u user	EMM user.
-p password	User password.
-Y cipher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which stdout and stderr outputs are redirected

### 2.7.2. Usage

#### Syntax

```
bsmGetHardwareExclusion.sh [-h] [-l level]-m model -H IPAddress [-u user] [-p password] [-Y cipher] [-o outfile]
```

#### Command

```
$ bsmGetHardwareExclusion.sh -m lanplus -H X.X.X.X -u super -p pass
```

#### Output

```
-----  
Processor 2 partially excluded  
Processor 3 partially excluded  
-----
```

## 2.8. bsmGetModuleLevelInfo

bsmGetModuleLevelInfo.sh is used to obtain some information about a module of a partition. When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.8.1. Options

-h	Displays command usage.
-l level	Specifies the message severity to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus.
-H IPaddress	BMC IP address for a module included in the platform.
-u user	EMM user.
-p password	User password.
-k keyname	Value to list in order to get information. Several values can be put into double quotes (") and separated with space. If this option is not set, information about the module_id is displayed. Possible values are: module_id: module identifier, model_type:model type model_name: marketing name.
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which stdout and stderr outputs are redirected.

### 2.8.2. Usage

#### Syntax

```
bsmGetModuleLevelInfo.sh [-h] [-l level] -m model -H IPaddress [-u user] [-p password] [-k keyname] [-Y cypher] [-o outfile]
```

#### Command

```
$ bsmGetModuleLevelInfo.sh -m lanplus -H X.X.X.X -u super -p pass
```

#### Output

```
-----  
Module identifier is 0  
-----
```

#### Command

```
$ bsmGetModuleLevelInfo.sh -m lanplus -H X.X.X.X -u super -p pass  
-k "module_id model_type model_name"
```

#### Output

```
-----  
Module identifier is 0  
Module model type is MESCAx_4SNL  
Module model name is bullx S6030  
-----
```

## 2.9. bsmGetPartitionLevelInfo

bsmGetPartitionLevelInfo.sh is used to obtain some information about the composition of a partition for the platform.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.9.1. Options

-h	Displays command usage
-l level	Specifies the message severity to be logged into syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus.
-H IPAddress	BMC IP address for a module included in the platform.
-u user	EMM user.
-p password	User password.
-k keyname	Value to list in order to get information. Several values can be put between double quotes (") and separated with spaces. If this option is not set, information about partition_composition and master_id are displayed. Possible values are: partition_composition: list of the modules included in the partition, master_id: current master module identifier, next_master_id: master module identifier which will be set after the next power on ip_emm_list: list of the module IP addresses for the partition partition_name: name of the partition.
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which stdout and stderr outputs are redirected.

### 2.9.2. Usage

#### Syntax

```
bsmGetPartitionLevelInfo.sh [-h] [-l level] -m model -H IPAddress [-u user] [-p password] [-k keyname] [-Y cypher] [-o outfile]
```

#### Command

```
$ bsmGetPartitionLevelInfo.sh -m lanplus -H X.X.X.X -u super -p pass
```

#### Output

```
-----  
Module 0 is in the partition  
No current master ID. - Partition is Off  
-----
```

## Command

```
$ bsmGetPartitionLevelInfo.sh -m lanplus -H X.X.X.X -u super -p pass  
-k "partition_composition master_id next_master_id ip_emm_list partition_name"
```

## Output

```
-----  
Modules 0 and 1 are in the partition  
No current master ID. Partition is Off  
Master ID for the next power on is 0  
IP address for module 0 is X.X.X.X.  
IP address for module 1 is X.X.X.X.  
Partition name is bimodules  
-----
```

## 2.10. bsmGetPlatformLevelInfo

bsmGetPlatformLevelInfo.sh is used to obtain some platforms information.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.10.1. Options

-h	Displays command usage.
-l level	Specifies the messages severity to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus.
-H IPaddress	BMC IP address for a module included in the platform.
-u user	EMM user.
-p password	User password.
-k keyname	Value to list in order to get the information. Several values can be put between double quotes (") and separated with spaces. If this option is not set, information about platform_id, platform_name and module_count are displayed. Possible values are: platform_id: platform identifier, platform_name: platform label, module_count: number of modules in the platform, prefix_ip: internal network IP address prefix, ip_emm_list : list of platform module's IP addresses, is_flexible : possibility to change the partition composition.
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which stdout and stderr outputs are redirected.

## 2.10.2. Usage

### Syntax

```
bsmGetPlatformLevelInfo.sh [-h] [-l level] -m model -H IPaddress [-u user]
[-p password] [-k keyname] [-Y cipher] [-o outfile]
```

### Command

```
$ bsmGetPlatformLevelInfo.sh -m lanplus -H X.X.X.X -u super -p pass
```

### Output

```
-----
Platform identifier is 152
Platform name is PVT-NL-4838
Module count is 01
-----
```

### Command

```
$ bsmGetPlatformLevelInfo.sh -m lanplus -H X.X.X.X -u super -p pass
-k "module_count prefix_ip platform_name platform_id"
```

### Output

```
-----
Module count is 02
IP prefix is 10.24
Platform name is PVT-NL-4837
Platform identifier is 154
-----
```

### Command

```
$ bsmGetPlatformLevelInfo.sh -m lanplus -H X.X.X.X -u super -p pass -k "is_flexible ip_emm_list"
```

### Output

```
-----
Partitions can be changed
IP address for module 0 is X.X.X.X
IP address for module 1 is X.X.X.X
IP address for module 2 is X.X.X.X
IP address for module 3 is X.X.X.X
-----
```

## 2.11. bsmHWinfocmd

bsmHWinfocmd is used to obtain various IPMI information such as BMC parameters, LAN configuration parameters, users list, and Alerting parameters:

```
bsmHWinfocmd -a bmc_info
bsmHWinfocmd -a lan_print
bsmHWinfocmd -a user_list
bsmHWinfocmd -a get_lan_alert_dest
bsmHWinfocmd -a get_pef_policy
bsmHWinfocmd -a get_pef_list
```

bmc\_info is used to get IPMI information such as the BMC Firmware revision, Manufacturer, BMC Device support

lan\_print is used to get the configuration parameters of the LAN channel used to access the BMC with an OutOfBand connection

user\_list is used to get information about the users configured for the LAN channel used to access the BMC with an OutOfBand connection

get\_lan\_alert\_dest is used to get information about the LAN alert destinations configured for the LAN channel used to access the BMC with an OutOfBand connection

get\_pef\_policy is used to get information about the Alert Policy Table used by the BMC for Alert processing.

get\_pef\_list is used to get information about the Platform Event Filter Table used by the BMC for Alert processing.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.11.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-a param	Type of information to be read: bmc_info, lan_print, user_list, get_lan_alert_dest, get_pef_list, get_pef_policy.
-H host	DNS name or IP address of the target BMC.
-m model	Target server model: lanplus.
-u user	BMC user name.
-p password	BMC user password.
-Y cipher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which stdout and stderr outputs are redirected.



## 2.11.2. Usage

### Syntax

```
bsmHWinfocmd.sh [-h] -m lanplus -H host -a param -u user [-p password]
[-o outfile] [-l level] [-Y cipher]
```

### 2.11.2.1. Get IPMI information for a server using lanplus

#### Command

```
$ bsmHWinfocmd.sh -a bmc_info -m lanplus -H X.X.X.X -u MWA -p guest
```

#### Output

```
-----
Device ID                : 48
Device Revision          : 1
Firmware Revision       : 11.10
IPMI Version             : 2.0
Manufacturer ID         : 107
Manufacturer Name       : Bull Company
Product ID              : 4 (0x0004)
Product Name            : Unknown (0x4)
Device Available        : yes
Provides Device SDRs    : no
Additional Device Support :
  Sensor Device
  SDR Repository Device
  SEL Device
  FRU Inventory Device
  Chassis Device
Aux Firmware Rev Info   :
  0x01
  0x00
  0x11
  0x74
-----
```

## 2.11.2.2. Get IPMI information for a server using lanplus

### Command

```
$ bsmHWinfocmd.sh -a bmc_info -m lanplus -H X.X.X.X -u MWA -p guest
```

### Output

```
-----  
Device ID : 48  
Device Revision : 1  
Firmware Revision : 11.9  
IPMI Version : 2.0  
Manufacturer ID : 107  
Manufacturer Name : Bull Company  
Product ID : 4 (0x0004)  
Product Name : Unknown (0x4)  
Device Available : yes  
Provides Device SDRs : no  
Additional Device Support :  
  Sensor Device  
  SDR Repository Device  
  SEL Device  
  FRU Inventory Device  
  Chassis Device  
Aux Firmware Rev Info :  
  0x05  
  0x00  
  0x11  
  0x67  
-----
```

### 2.11.2.3. Get configuration parameters of the LAN channel

#### Command

```
$ bsmHWinfocmd.sh -a lan_print -m lanplus -H X.X.X.X -u guest -p pass
```

#### Output

```
-----  
Set in Progress           : Set Complete  
Auth Type Support        : NONE MD2 MD5 PASSWORD  
Auth Type Enable        : Callback :  
                          : User      : MD5  
                          : Operator : MD5  
                          : Admin    : MD5  
                          : OEM      : MD5  
  
IP Address Source        : Unspecified  
IP Address                : X.X.X.X  
Subnet Mask              : 255.255.255.0  
MAC Address              : 08:00:38:35:73:b2  
SNMP Community String    : public  
IP Header                : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10  
BMC ARP Control          : ARP Responses Enabled, Gratuitous ARP Disabled  
Gratituous ARP Intrvl   : 2.0 seconds  
Default Gateway IP       : 172.31.50.1  
Default Gateway MAC      : 00:00:00:00:00:00  
Backup Gateway IP        : 0.0.0.0  
Backup Gateway MAC       : 00:00:00:00:00:00  
RMCP+ Cipher Suites      : 0,1,2,3,6,7,8,11,12  
Cipher Suite Priv Max    : uuuOXXuuOXXuOXX  
                          : X=Cipher Suite Unused  
                          : c=CALLBACK  
                          : u=USER  
                          : o=OPERATOR  
                          : a=ADMIN  
                          : O=OEM  
-----
```

## 2.11.2.4. Get information about users configured for the LAN channel

### Command

```
$ bsmHWinfocmd.sh -a user_list -m lanplus -H X.X.X.X -u super -p pass
```

### Output

```
-----  
Channel Number   : 0x1  
Maximum User IDs : 63  
Enabled User IDs : 1  
  
User ID          : 1  
User Name        :  
Fixed Name       : Yes  
Access Available : call-in / callback  
Link Authentication : disabled  
IPMI Messaging   : disabled  
Privilege Level  : NO ACCESS  
  
User ID          : 2  
User Name        : super  
Fixed Name       : No  
Access Available : call-in / callback  
Link Authentication : disabled  
IPMI Messaging   : enabled  
Privilege Level  : OEM  
  
User ID          : 3  
User Name        : test  
Fixed Name       : No  
Access Available : call-in / callback  
Link Authentication : disabled  
IPMI Messaging   : enabled  
Privilege Level  : NO ACCESS  
  
User ID          : 4  
User Name        :  
Fixed Name       : No  
Access Available : call-in / callback  
Link Authentication : disabled  
IPMI Messaging   : disabled  
Privilege Level  : NO ACCESS  
.  
.  
.  
-----
```

### 2.11.2.5. Get information about LAN alert destinations for the LAN channel

#### Command

```
$ bsmHWinfocmd.sh -a get_lan_alert_dest -m lanplus -H X.X.X.X -u MWA -p guest
```

#### Output

```
-----  
Alert Destination           : 0  
Alert Acknowledge          : Unacknowledged  
Destination type           : PET Trap  
Retry Interval              : 0  
Number of Retries          : 0  
Alert Gateway              : Default  
Alert IP Address           : 0.0.0.0  
Alert MAC Address          : 00:00:00:00:00:00  
  
Alert Destination           : 1  
Alert Acknowledge          : Unacknowledged  
Destination type           : PET Trap  
Retry Interval              : 5  
Number of Retries          : 3  
Alert Gateway              : Default  
Alert IP Address           : X.X.X.X  
Alert MAC Address          : 00:11:22:33:44:55  
.....  
-----
```

### 2.11.2.6. Get information about the Alert Policy Table

#### Command

```
$ bsmHWinfocmd.sh -a get_pef_policy -m lanplus -H X.X.X.X -u MWA -p guest
```

#### Output

```
-----  
Alert policy table entry   : 1  
Policy set                 : 1  
Policy entry rule          : Try-next-entry  
Channel number             : 7  
Channel medium             : 802.3 LAN  
Destination number        : 2  
Alert destination type     : PET  
ACK timeout / retry       : 5  
Retries                    : 3  
IP address                 : X.X.X.X  
MAC address                : 00:11:2:33:44:55  
Status                    : Enabled  
  
Alert policy table entry   : 2  
.....  
-----
```

## 2.11.2.7. Get information about the Platform Event Filter Table

### Command

```
$ bsmHWinfocmd.sh -a get_pec_list -m lanplus -H X.X.X.X -u MWA -p guest
```

### Output

```
-----  
PEF table entry          : 1  
Status                   : active  
Version                  : 0x11  
Sensor type              : Any  
Sensor number            : Any  
Event severity           : Warning  
Event class              : Threshold  
Event trigger(s)        : (0x01/0x0081)<LNC,<UNC  
Action                   : Alert  
Policy set               : 1
```

```
PEF table entry          : 2  
Status                   : inactive
```

```
PEF table entry          : 3  
Status                   : active  
Version                  : 0x11  
Sensor type              : Power Supply  
Sensor number            : Any  
Event severity           : Critical  
Event class              : Discrete  
Event trigger(s)        : Sensor-specific  
Action                   : Alert  
Policy set               : 1
```

```
....  
-----
```

## 2.12. bsmHWpm

This command is used to control power consumption of platform using power and thermal policies.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.12.1. Options

-a action	Action.
-h	Displays command usage.
-m model	Target server model: lanplus.
-H host	BMC target IP address.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-u user	BMC user.
-p password	User password.
-Y cipher	Cipher suite ID to be used by the lanplus interface (default is 3).
-o outfile	Output file name where <code>stdout</code> and <code>stderr</code> outputs are redirected.
-z value	Hexadecimal code of the manageability engine channel to reach (default is 0x06)
-e value	Hexadecimal code of the manageability engine address to reach (default is 0x2c)
arglist	List of arguments specific to the action.

## 2.12.2. Usage

### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host  
[-u user -p password] [-o outfile] -a action arglist
```

---

**Note** The `bsmHWpm` command is available for servers with Manageability Engine.

---

```
bsmHWpm.sh -a getPowerBudget  
bsmHWpm.sh -a setPowerBudget  
bsmHWpm.sh -a getPowerConsumption  
bsmHWpm.sh -a getNMVersion  
bsmHWpm.sh -a getNMCapabilities  
bsmHWpm.sh -a endisNMPolicyControl  
bsmHWpm.sh -a getNMPolicy  
bsmHWpm.sh -a setNMPolicy  
bsmHWpm.sh -a removeNMPolicy  
bsmHWpm.sh -a getPowerLimit  
bsmHWpm.sh -a setPowerLimit  
bsmHWpm.sh -a getTempTrigger  
bsmHWpm.sh -a setTempTrigger  
bsmHWpm.sh -a setNMPowerDrawRange  
bsmHWpm.sh -a getNMStatistics  
bsmHWpm.sh -a resetNMStatistics  
bsmHWpm.sh -a getNumberOfCPUStates  
bsmHWpm.sh -a getMaxAllowedCPUStates  
bsmHWpm.sh -a setMaxAllowedCPUPState  
bsmHWpm.sh -a setMaxAllowedCPUPState
```

### 2.12.2.1. Get the Total Power Budget

The `getPowerBudget` action is used to get the Total Power Budget (in Watts) that is maintained by the Power Budget Control Service.

### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password] [-o  
outfile] [-z ME channel] [-e ME address] -a getPowerBudget
```

### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u root -p bull -a getPowerBudget
```

### Output

```
-----  
Power Budget = 377 Watts  
-----
```



### 2.12.2.2. Set the Total Power Budget

The `setPowerBudget` action is used to set the Total Power Budget (in Watts) that should be maintained by the Power Budget Control Service.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a setPowerBudget -x value
```

#### Options

`-x value` Total Power Budget to be set. This value must be greater than the min Power Limit value and less than the max Power Limit value returned by the `getNMCcapabilities` action.

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u root -p bull -a setPowerBudget -x 350
```

#### Output

```
-----
Total Power Budget has been set
-----
```

### 2.12.2.3. Obtain global or individual policy Power Consumption Statistics

The `getPowerConsumption` action is used to get global or per policy Power Consumption Statistics.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getPowerConsumption
[-i policyID]
```

#### Options

`-i policyID` This argument is used to obtain individual policy power consumption statistics. Without this argument, global power consumption statistics are returned

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u root -p bull -a getPowerConsumption
```

#### Output

```
-----
Current consumption: 167 Watts
Minimum consumption: 135 Watts
Maximum consumption: 511 Watts
Average consumption: 203 Watts
-----
```

### 2.12.2.4 Get Node Manager and firmware version numbers

The getNMVersion action is used to get Node Manager and firmware version numbers.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getNMVersion
```

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getNMVersion
```

#### Output

```
-----
Node Manager Version:
  Manufacturers ID: 0x000157 (Intel)
  Node Manager Version: supported Node Manager 1.5
  IPMI interface version: Patch version (binary encoded) 0x00
  IPMI interface version: Major Firmware revision (binary encoded) 0x01
  IPMI interface version: Minor Firmware revision (BCD encoded) 0x04
-----
```

### 2.12.2.5 Get Node Manager Capabilities

The getNMCapabilities action is used to get Node Manager Capabilities.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getNMCapabilities
-g policyTriggerType
```

#### Options

```
-g policyTriggerType      Policy Trigger Type:
                           0: No Policy Trigger
                           1: Inlet Temperature Policy Trigger Type
```

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getNMCapabilities -g 0
```

#### Output

```
-----
Node Manager Capabilities:
  Manufacturers ID: 0x000157 (Intel)
  Max Concurrent Settings: 10
  Max Power/Thermal value to be settable as trigger or max Power Limit to be
maintained if Policy trigger type is equal to 0: 32767
  Min Power/Thermal value to be settable as trigger or min Power Limit to be
maintained if Policy trigger type is equal to 0: 1
  Min Correction time: 6000 ms
  Max Correction time: 600000 ms
  Min Statistics Reporting Period: 1 s
  Max statistics reporting Period: 3600 s
  Domain limiting scope: CPU power limiting
  IPMI interface version: Minor Firmware revision (BCD encoded) 0x04
-----
```

## 2.12.2.6 Enable/Disable Node Manager Policy Control

The endisNMPolicyControl action is used to Enable/Disable Node Manager Policy Control.

### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password] [-o  
outfile] [-z ME channel] [-e ME address] -a endisNMPolicyControl  
-f policyControl [-i policyID]
```

### Options

-f policyControl	Policy Control value: 0: Global Disable Node Manager policy control 1: Global Enable Node Manager policy control 2: Per Domain Disable Node Manager policies for the specified domain (domain 0) 3: Per Domain Enable Node Manager policies for the specified domain (domain 0) 4: Per Policy Disable Node Manager policy for the specified policy within domain (domain 0) 5: Per Policy Enable Node Manager policy for the specified policy within domain (domain 0)
-i policyID	This argument is mandatory if the policyControl argument is set to 4 or 5

### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a endisNMPolicyControl -f 5 -i 0
```

### Output

```
-----  
Node Manager Policy Control is done.  
-----
```

## 2.12.2.7. Get the Node Manager policy parameters

The getNMPolicy action is used to get the Node Manager policy parameters.

### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getNMPolicy -i policyID
```

### Options

-i policyID                      Policy ID

### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getNMPolicy -i 0
```

### Output

```
-----
Node Manager Policy:
Manufacturers ID: 0x000157 (Intel)
Domain Id: 0
Policy enabled
per Domain Node Manager policy control enabled:
Global Node Manager policy control enabled:
Policy Trigger Type: No Policy Trigger. Policy will maintain Power Limit
Policy Type: Power Control Policy
Policy Exception Actions:
    send alert disabled
    shutdown system disabled
Power Limit: 32767 [Watts]
Print Correction Time Limit: 600000 [ms]
Policy Trigger Limit: 32767
Statistics Reporting Period: 30 [s]
-----
```

## 2.12.2.8. Create or modify a Node Manager Policy

The setNMPolicy action is used to create or modify a Node Manager Policy.

### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a setNMPolicy -i policyID
-g policyTriggerType -x powerLimit [-G policyTriggerLimit]
-c exceptionAction -T correctionTimeLimit -r statisticsReportingPeriod
```

### Options

-i policyID	Policy ID
-g policyTriggerType	Policy Trigger Type: 0: No Policy Trigger 1: Inlet Temperature Policy Trigger type
-x powerLimit	Power Limit to be maintained.
-G policyTriggerLimit	Defines the Inlet temperature (in Celsius) to be used as Policy Trigger value. This argument is mandatory only if the policy trigger type is set to 1
-c exceptionAction	Defines the action to be taken if the maintained given policy power limit is exceeded over the Correction Time Limit. Possible values are: 0: no action 1: send alert 2: hard system shutdown via BMC
-T correctionTimeLimit	Defines the max time (in seconds), in which the Node Manager must take corrective actions in order to bring the platform back within the specified power limit before taking the Exception Action.
-r statisticsReportingPeriod	Defines the Statistics Reporting Period in seconds.

### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a setNMPolicy -i 0 -g 0 -x 380 -c 0 -T 500 -r 20
```

### Output

```
-----
Node Manager Policy 0 has been set
-----
```

### 2.12.2.9. Removes a Node Manager Policy

The removeNMPolicy action is used to remove a Node Manager Policy.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a removeNMPolicy
-i policyID -g policyTriggerType
```

#### Options

-i policyID	Policy ID
-g policyTriggerType	Policy Trigger Type: 0: No Policy Trigger 1: Inlet Temperature Policy Trigger type

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a removeNMPolicy -i 1 -g 0
```

#### Output

```
-----  
Node Manager Policy 1 has been removed  
-----
```

### 2.12.2.10. Get the Power Limit to be maintained on a policy ID

The getPowerLimit action is used to get the Power Limit to be maintained for a policy ID.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getPowerLimit -i policyID
```

#### Options

-i policyID	Policy ID
-------------	-----------

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getPowerLimit -i 0
```

#### Output

```
-----  
Node Manager Policy 0 Power Limit = 365 Watts  
-----
```

### 2.12.2.11. Set the Power Limit to be maintained on a policy ID

The setPowerLimit action is used to set the Power Limit to be maintained for a policy ID.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a setPowerLimit -i policyID
-x powerLimit
```

#### Options

-i policyID	Policy ID
-x powerLimit	Power Limit to be maintained.

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a setPowerLimit -i 1 -x 365
```

#### Output

```
-----
Node Manager Policy 1 Power Limit has been set
-----
```

### 2.12.2.12. Get the Inlet temperature

The getTempTrigger action is used to get the Inlet temperature (in Celsius) that defines the Policy Trigger Limit for a policy ID.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getTempTrigger
-i policyID
```

#### Options

-i policyID	Policy ID
-------------	-----------

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getTempTrigger -i 0
```

#### Output

```
-----
Policy 0 Inlet Temperature Trigger Limit = 0x0032 Celsius
-----
```

### 2.12.2.13. Set Inlet temperature

The setTempTrigger action is used to set Inlet temperature (in Celsius) that defines the Policy Trigger Limit for a policy ID.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a setTempTrigger
-i policyID -x tempLimit
```

#### Options

-i policyID	Policy ID
-x tempLimit	Temperature Limit used as Policy Trigger value

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a setTempTrigger -i 1 -x 85
```

#### Output

```
-----
Policy 1 Inlet Temperature Trigger Limit has been set
-----
```

### 2.12.2.14. Set the Min and Max power consumption range

The setNMPowerDrawrange action is used to set the Min and Max power consumption range.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a setNMPowerDrawRange
-n minPower -N maxPower
```

#### Options

-n minPower	Minimum Power Draw in Watts
-N maxPower	Maximum Power Draw in Watts

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a setNMPowerDrawRange -n 200 -N 400
```

#### Output

```
-----
Power Draw range has been set
-----
```



### 2.12.2.15. Get the Node Manager Power Statistics

The getNMStatistics action is used to get the Node Manager Power Statistics.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getNMStatistics -O mode
[-i policyID]
```

#### Options

- |             |   |
|-------------|---|
| -O mode     | Specifies the type of statistics to be collected:<br>1: global power statistics (in Watts)<br>2: global inlet temperature statistics (in Celsius)<br>17: per policy power statistics (in Watts)<br>18: per policy trigger statistics (in Celsius) |
| -i policyID | This argument is mandatory only if mode argument is set to 17 or 18   |

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getNMStatistics -O 1
```

#### Output

```
-----
Node Manager Statistics:
  Manufacturers ID: 0x000157 (Intel)
  Current: 683
  Minimum: 620
  Maximum: 752
  Average: 682
  Timestamp: 1285366705
  Statistics Reporting Period: 1 s
  domain Id: 0
  Measurement state: Measurements in progress(host CPU in S0 state)?
-----
```

### 2.12.2.16. Reset the Node Manager Power Statistics

The resetNMStatistics action is used to reset the Node Manager Power Statistics.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a resetNMStatistics -O mode
[-i policyID]
```

#### Options

- |             |  |
|-------------|--|
| -O mode     | Specifies the type of statistics to be reset:<br>0: global statistics including power statistics and inlet temperature statistics<br>1: per policy statistics including power and trigger statistics |
| -i policyID | This argument is mandatory only if mode argument is set to 1   |

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a resetNMStatistics -O 0
```

#### Output

```
-----
Node Manager Statistics have been reset
-----
```

### 2.12.2.17. Get the number of P-States and T-States available on the target platform

The `getNumberOfCPUStates` action is used to get the number of P-States and T-States available on the target platform.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getNumberOfCPUStates
```

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getNumberOfCPUStates
```

#### Output

```
-----
Number of P-States available on the platform: 9
Number of T-States available on the platform: 8
-----
```

### 2.12.2.18. Get the maximum P-State and T-State

The `getMaxAllowedCPUStates` action is used to get the maximum P-State and T-State.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a getMaxAllowedCPUStates
```

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a getMaxAllowedCPUStates
```

#### Output

```
-----
Current maximum P-State: 5
Current maximum T-State: 4
-----
```

### 2.12.2.19. Set the maximum P-State

The `setMaxAllowedCPUPState` action is used to set the current maximum P-State.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a setMaxAllowedCPUPState
-s stateNumber
```

#### Options

`-s stateNumber` P-State number to be set; from 0 to n-1, where n is the Number of P-States (returned with the `getNumberOfCPUStates` action) available on the platform.

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a setMaxAllowedCPUPState -s 3
```

#### Output

```
-----
CPU P-State/T-State has been set
-----
```

### 2.12.2.20. Set the current maximum T-State

The `setMaxAllowedCPUTState` action is used to set the current maximum T-State.

#### Syntax

```
bsmHWpm.sh [-h] [-l level] -m model -H host [-u user -p password]
[-o outfile] [-z ME channel] [-e ME address] -a setMaxAllowedCPUTState
-s stateNumber
```

#### Options

`-s stateNumber` T-State number to be set; from 0 to n-1, where n is the Number of T-States (returned with the `getNumberOfCPUStates` action) available on the platform.

#### Command

```
$ bsmHWpm.sh -m lanplus -H X.X.X.X -u ADMIN -p ADMIN -a setMaxAllowedCPUTState -s 3
```

#### Output

```
-----
CPU P-State/T-State has been set
-----
```

## 2.13. bsmidentify

The `bsmidentify` command is used to identify physically a remote host via user-visible lights or beeps for a defined interval.

### 2.13.1. Options

<code>-h</code>	Displays command usage.
<code>-l level</code>	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
<code>-m model</code>	Target server model: lanplus, ipmidrv.
<code>-H host</code>	DNS name or target server IP address.
<code>-C value</code>	Specifies the duration of identification (in seconds). This value may be set from 0 to 250. This value set to 0 stops the identification.
<code>-u user</code>	BMC user.
<code>-p password</code>	User password.
<code>-Y cipher</code>	Cipher suite ID to be used by lanplus interface (default is 3).
<code>-o outfile</code>	Output file name where <code>stdout</code> and <code>stderr</code> outputs are redirected.

### 2.13.2. Usage: Server using lanplus model

#### Syntax

```
bsmidentify.sh [-h] -m lanplus -H host -u user [-p password] [-l level] -C value [-o outfile] [-Y cipher]
```

#### Command

```
$ bsmidentify.sh -m lanplus -H X.X.X.X -u root -p root -C 10
```

#### Output

```
-----  
Chassis identify interval : 10 seconds  
-----
```

### 2.13.3. Usage: Server using ipmidrv model

#### Syntax

```
bsmidentify.sh [-h] -m ipmidrv [-l level] -C value [-o outfile]
```

## 2.14. bsminfo

bsminfo.sh is used to direct, to the standard output, the configuration information specified by the `-i` information parameter.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.14.1. Options

<code>-h</code>	Displays command usage.
<code>-l</code>	Logs in syslog the successful completion of the command (OK). By default, only FAILED completion is logged.
<code>-i information</code>	Information type. Currently, only <i>hardwarestatus</i> and <i>BMCinfo</i> information is available.
<code>-H host</code>	DNS name or target server IP address.
<code>-m model</code>	Target server model: lanplus, ipmidrv
<code>-u user</code>	BMC user.
<code>-p password</code>	User password.
<code>-Y cipher</code>	Cipher suite ID to be used by lanplus interface (default is 3).
<code>-o outfile</code>	Output file name to which <code>stdout</code> and <code>stderr</code> outputs are redirected.

<b>-i Option</b>	<b>Hardware Component Level (-e option specified)</b>
hardwarestatus	Returns the power status ON/OFF of the chassis
BMCinfo	Returns the BMC IPMI version, FW revision,...

Table 2-1. bsminfo options and parameters for NovaScale servers using ipmidrv

### 2.14.2. Usage

#### Syntax

```
bsminfo.sh [-h] -i information -m lanplus -H host -u user [-p password] [-o outfile] [-l level] [-Y cipher]
```

```
bsminfo.sh [-h] -i information -m ipmidrv [-o outfile] [-l level]
```

---

**Note** Servers are identified by their DNS name or IP address (-H parameter).

---

### 2.14.2.1. Display the chassis power status

`hardwarestatus` is used to display chassis power status info.

---

**Note** -H host parameter is not used (ignored if present).

---

#### Command

```
$ bsmfinfo.sh -i hardwarestatus -m lanplus -H nsmaster -u MWA -p guest
```

#### Output

```
-----  
Chassis Power is on  
-----
```

### 2.14.2.2. Display BMC information

`BMCinfo` is used to display BMC information such as IPMI version, firmware revision, etc.

#### Command

```
$ bsmfinfo.sh -i BMCinfo -m lanplus -H X.X.X.X -u MWA -p guest
```

#### Output

```
-----  
Device ID           : 32  
Device Revision     : 1  
Firmware Revision   : 3.26  
IPMI Version        : 2.0  
Manufacturer ID     : 116  
-----
```

## 2.15. bsmlog

bsmlog is used to direct system log contents (SEL) to the standard output.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

If `-v` option is not specified, the output format is:

```
<rank> | <record id> | <local date> | <local time> | <event target> | <severity> -  
<event description>
```

If `-v` option is specified, one record is displayed by field (over several rows according to the format):

```
<label>: <value>
```

- 
- Notes**
- Servers are identified by their DNS name or IP address (`-H` parameter).
  - `-n range` is ignored if the `-c` option is specified.
  - By default, the `-n range` parameter is set to `-n 10`.
- 

bsmlog is also used to clear the system log contents (SEL).

### 2.15.1. Options

<code>-h</code>	Displays command usage.
<code>-l level</code>	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
<code>-v</code>	Displays record details. See below.
<code>-n range</code>	Range of records to be displayed. May be specified as a number or as an interval: <code>-n n</code> : displays the <code>n</code> most recent records. <code>-n r1-r2</code> : displays records from <code>r1</code> to <code>r2</code> . Events are displayed in chronological order beginning with the most recent ones.
<code>-H host</code>	DNS name or target server IP address.
<code>-m model</code>	Target server model: lanplus, ipmidrv.
<code>-u user</code>	BMC user.
<code>-p password</code>	User password.
<code>-Y cipher</code>	Cipher suite ID to be used by lanplus interface (default is 3).
<code>-o outfile</code>	Output file to which stdout and stderr outputs are redirected.
<code>-c</code>	Clears the SEL.

## 2.15.2. Usage: Server using lanplus model

### Syntax

```
bsmlog.sh [-h] [-v] -m lanplus [-n range] -H host -u user [-p password]
[-o outfile] [-l level] [-c] [-Y cipher]
```

### 2.15.2.1. Clear SELs

#### Command

```
$ bsmlog.sh -m lanplus -H X.X.X.X -c -u admin -p admin
```

#### Output

```
-----
$
-----
```

### 2.15.2.2. Display SELs

#### Command

```
$ bsmlog.sh -n 145-140 -m lanplus -H tiger_s2 -u admin -p admin -Y 0
```

#### Output

```
-----
144 | 0x0b30 | 09/22/2004 | 15:26:51 | System Event #0x08 | OEM System boot
event
143 | 0x0b1c | 09/22/2004 | 12:46:05 | System Event #0x08 | OEM System boot
event
142 | 0x0b08 | 09/21/2004 | 19:50:31 | 0x80 | Drive Slot #0x09 | Device
Inserted/Present
141 | 0x0af4 | 09/21/2004 | 19:50:26 | 0x80 | Drive Slot #0x09 | Device
Removed/Absent
140 | 0x0ae0 | 09/21/2004 | 19:50:21 | 0x80 | Drive Slot #0x09 | Device
Inserted/Present
$
-----
```

## 2.15.3. Usage: Server using ipmidrv model

### Syntax

```
bsmlog.sh [-h] [-v] -m ipmidrv [-n range] [-o outfile] [-l level] [-c]
```



## 2.16. bsmOSpm

The `bsmOSpm` command, is used to control the CPU policy and frequency of platform via `cpufrequtils` package.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.16.1. Options

<code>-a action</code>	Action.
<code>-h</code>	Displays command usage.
<code>-m model</code>	Remote host OS: linux.
<code>-H host</code>	Remote target name or IP address.
<code>-l level</code>	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
<code>-u user</code>	Username for remote connection via ssh.
<code>-C configfile</code>	Config file used for remote connection (default is "").
<code>-I idfile</code>	Identity file used for remote connection (default is <code>id_dsa</code> ).
<code>-d cfgdir</code>	Full path directory containing config file and identity file.
<code>-D pathdir</code>	Full path directory containing script <code>bsmOSpm_local</code> on remote host.
<code>-o outfile</code>	Output file name where <code>stdout</code> and <code>stderr</code> outputs are redirected.
<code>arglist</code>	List of arguments specific to the action.

### 2.16.2. Usage

#### Syntax

```
bsmOSpm.sh [-h] [-l level] -m model -H host [-u user] [-o outfile]
[-I idfile] [-d cfgdir] [-C configfile] [-D pathdir] -a action arglist
```

## 2.16.2.1. Get the governor and the frequency range of one or all CPUs

The `getPolicy` action is used to get the governor and the frequency range for one or all CPUs.

### Syntax

```
bsmOSpm.sh [-h] [-l level] -m model -H host [-u user] [-o outfile]
[-I idfile] [-d cfgdir] [-C configfile] [-D pathdir] -a getPolicy [-c CPU]
```

### Options

`-c cpu` CPU concerned by the action (number, all, synth (default value)).

### Command to get a synthesis

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a getPolicy -c synth
```

### Output

```
-----
CPUs ( 0 to 7) 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
or
CPUs 0,1,2,4,5,6,7 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPUs 3 2560000 kHz ( 87 %) - 2940000 kHz ( 100 %) - userspace
-----
```

### Command to get results for all CPUs

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a getPolicy -c all
```

### Output

```
-----
CPU 0 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPU 1 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPU 2 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPU 3 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPU 4 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPU 5 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPU 6 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
CPU 7 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
-----
```

### Command to get results for one CPU

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a getPolicy -c 5
```

### Output

```
-----
CPU 5 2000000 kHz ( 68 %) - 2560000 kHz ( 87 %) - userspace
-----
```

## 2.16.2.2. Set the CPU governor and the frequency range

The `setPolicy` action is used to set the CPU governor and to set the frequency range for all CPUs for the `userspace` governor.

### Syntax

```
bsmOSpm.sh [-h] [-l level] -m model -H host [-u user] [-o outfile]
[-I idfile] [-d cfgdir] [-C configfile] [-D pathdir] -a setPolicy
-g governor [-y freq_min -x freq_max]
```

### Options

-g governor	cpufreq governor. Values available are <code>userspace</code> , <code>ondemand</code> , <code>performance</code> .
-y freq_min	minimum CPU frequency the governor may select (only if <code>userspace</code> governor is specified). The frequency may be specified in kHz or as a percent of the maximum frequency possible (hardware limit).
-x freq_max	maximum CPU frequency the governor may select (only if <code>userspace</code> governor is specified). The frequency may be specified in kHz or as a percent of the maximum frequency possible (hardware limit).

### Command to set the CPU frequency governor to `ondemand`

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a setPolicy -g ondemand
```

### Output

```
-----
OK CPUs (0 to 15)  ondemand
-----
```

### Command to set the CPU frequency governor to `userspace`, with frequency range in percent

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a setPolicy -g userspace -y 77% -x 87%
```

### Output

```
-----
OK CPUs (0 to 15)  77% - 87% userspace
-----
```

### Command to set the CPU frequency governor to `userspace`, with frequency range in kHz

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a setPolicy -g userspace -y 2000000 -x 2560000
```

### Output

```
-----
OK CPUs (0 to 15)  2000000 kHz (68%) - 2560000 kHz (87%)  userspace
-----
```

### 2.16.2.3. Get the current frequency of one or all CPUs

The `getCurrentFreq` action is used to get the current frequency of one or all CPUs.

#### Syntax

```
bsmOSpm.sh [-h] [-l level] -m model -H host [-u user] [-o outfile]
[-I idfile] [-d cfgdir] [-C configfile] [-D pathdir] -a getCurrentFreq [-c
CPU]
```

#### Options

`-c cpu` CPU concerned by the action (number, all, synth (default value)).

#### Command to get a synthesis

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a getCurrentFreq -c synth
```

#### Output

```
-----
CPUs ( 0 to 7) 2128000 kHz
-----
```

#### Command to get the frequency of CPU 6

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a getCurrentFreq -c 6
```

#### Output

```
-----
CPU 6 2394000 kHz
-----
```

### 2.16.2.4. Set the current frequency for one or all CPUs

The `setCurrentFreq` action is used to set the current frequency for one or all CPUs.

#### Syntax

```
bsmOSpm.sh [-h] [-l level] -m model -H host [-u user] [-o outfile]
[-I idfile] [-d cfgdir] [-C configfile] [-D pathdir] -a setCurrentFreq
[-c CPU]
```

#### Options

`-c cpu` CPU concerned by the action (number, all, synth (default value)).

`-f freq` CPU frequency to be set. The userspace governor must have been set and loaded. The frequency may be specified in kHz or as a percent of the maximum frequency possible (hardware limit).

#### Command to set the frequency for all CPUs

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a setCurrentFreq -f 2394000 -c all
```

#### Output

```
-----
OK CPUs ( 0 to 7) 2394000 kHz
-----
```

#### Command to set the frequency for CPU 6

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a setCurrentFreq -f 2394000 -c 6
```

#### Output

```
-----
OK CPU 6 2394000 kHz
-----
```

### 2.16.2.5. Get the minimum and maximum CPU frequency allowed

The `getHWlimits` action is used to obtain the minimum and maximum CPU frequency allowed.

#### Syntax

```
bsmOSpm.sh [-h] [-l level] -m model -H host [-u user] [-o outfile]
[-I idfile] [-d cfgdir] [-C configfile] [-D pathdir] -a getHWlimits
[-c CPU]
```

#### Options

`-c cpu` CPU concerned by the action (number, all, synth (default value)).

#### Command to get the frequency allowed for each CPU

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a getHWlimits -c all
```

#### Output

```
-----
CPU 0 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 1 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 2 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 3 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 4 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 5 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 6 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 7 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 8 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 9 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 10 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 11 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 12 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 13 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 14 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
CPU 15 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
-----
```

#### Command to get the frequency allowed for CPU 3

```
$ bsmOSpm.sh -m linux -H X.X.X.X -u root -a getHWlimits -c 3
```

#### Output

```
-----
CPU 3 1596000 kHz ( 54 %) - 2927000 kHz (100 %)
-----
```

## 2.17. bsmPDUpower

The `bsmPDUpower` command is used for monitoring and the administration of Power Distribution Units (PDUs). This includes obtaining the total power consumption for all the outlets of the PDU (and also the warning and critical consumption thresholds) and for a PDU, poweron/poweroff of the PDU outlets, and obtaining their status. The command uses SNMP get and set requests to the SNMP agent of the PDU:

```
bsmPDUpower.sh -a on/off
bsmPDUpower.sh -a status
bsmPDUpower.sh -a getPowerConsumption
```

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

- 
- Notes**
- Actually, only PDUs from APC are supported. For APC metered rack PDUs, only the `getPowerConsumption` action is available.
  - The Firmware Revision of APC PDUs must be equal to or higher than v3.
- 

### 2.17.1. Options

<code>-a action</code>	Action.
<code>-h</code>	Displays command usage.
<code>-m model</code>	PDU model: <code>apc</code> .
<code>-H host</code>	DNS name or IP address of the PDU.
<code>-l level</code>	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
<code>-o outfile</code>	Output file name where <code>stdout</code> and <code>stderr</code> outputs are redirected.
<code>arglist</code>	list of arguments specific to the action.

## 2.17.2. Usage

### Syntax

```
bsmPDUpower.sh [-h] [-l level] -m model -H host [-o outfile] -a action arglist
```

### 2.17.2.1. Set on or off one or all outlets of a PDU

The **on** and **off** actions are used to set on, or off, one, or all, outlets for a PDU.

### Syntax

```
bsmPDUpower.sh [-h] [-l level] -m model -H host [-o outfile] -a on/off [-p SNMP port] [-S SNMPv] [[-C community][[-u user -L secllevel -A authPass -P authPro -X privPass -x privPro]] [-c outlet] [-T timeout]
```

### Options

-p port	SNMP port (default value: 161)
-S SNMPv	SNMP version: 1 (default value), 2c, 3
-C community	SNMPv1 community (default value 'private' pour actions on and off)
-L secllevel	SNMPv3 SecurityLevel (noAuthNoPriv   authNoPriv   authPriv)
-u user	SNMPv3 user.
-A authPass	SNMPv3 authentication passphrase (15 to 32 ASCII characters)
-P authPro	SNMPv3 authentication protocol (default value 'MD5' )
-X privPass	SNMPv3 privacy passphrase (15 to 32 ASCII characters, different than -authPass)
-x privPro	SNMPv3 privacy protocol (default value 'DES' )
-c outlet	number or name of one outlet for a PDU (default value 'all': all outlets are switched on or off)
-T timeout	SNMP timeout (default value: 30 seconds)

### Command to set all outlets off

```
$ bsmPDUpower.sh -H X.X.X.X -a off -m apc -S 3 -L authPriv -u $user -A $authpass -P md5 -X $privpass -x des -c all
```

### Output

```
-----  
Outlet1 power: Off(2)  
Outlet2 power: Off(2)  
Outlet3 power: Off(2)  
Outlet4 power: Off(2)  
Outlet5 power: Off(2)  
Outlet6 power: Off(2)  
Outlet7 power: Off(2)  
Outlet8 power: Off(2)  
-----
```

### Command to set outlet 5 on

```
$ bsmPDUpower.sh -H X.X.X.X -a on -m apc -S 3 -L authPriv -u $user -A $authpass -P md5 -X $privpass -x des -c 5
```

### Output

```
-----  
Outlet5 power: On(1)  
-----
```

## 2.17.2.2. Get the status for one or all outlets of a PDU

The `status` action is used to obtain the status for one, or all outlets, of a PDU.

### Syntax

```
bsmPDUpower.sh [-h] [-l level] -m model -H host [-o outfile] -a status  
[-p SNMP port] [-S SNMPv] [[-C community] | [-u user -L seclevel  
-A authPass -P authPro -X privPass -x privPro]] [-c outlet] [-T timeout]
```

### Options

<code>-p port</code>	SNMP port (default value: 161)
<code>-S SNMPv</code>	SNMP version: 1 (default value), 2c, 3
<code>-C community</code>	SNMPv1 community (default value 'public' for status action)
<code>-L seclevel</code>	SNMPv3 SecurityLevel (noAuthNoPriv   authNoPriv   authPriv)
<code>-u user</code>	SNMPv3 user.
<code>-A authPass</code>	SNMPv3 authentication passphrase (15 to 32 ASCII characters)
<code>-P authPro</code>	SNMPv3 authentication protocol (default value 'MD5' )
<code>-X privPass</code>	SNMPv3 privacy passphrase (15 to 32 ASCII characters, different than <code>-authPass</code> )
<code>-x privPro</code>	SNMPv3 privacy protocol (default value 'DES' )
<code>-c outlet</code>	number or name of one outlet of PDU (default value 'all': all outlets are switched on or off)
<code>-T timeout</code>	SNMP timeout (default value: 30 seconds)

### Command to obtain the status for all outlets

```
$ bsmPDUpower.sh -H X.X.X.X -a status -m apc -S 3 -L authPriv -u $user -A $authpass -P md5 -X $privpass -x des -c all
```

### Output

```
-----  
Power Distribution Unit: X.X.X.X, MODEL: "AP7922", Serial Nb: "ZA0904000484",  
Firm Rev: "v3.5.7"  
Outlet1 power: Off(2)  
Outlet2 power: Off(2)  
Outlet3 power: Off(2)  
Outlet4 power: Off(2)  
Outlet5 power: On(1)  
Outlet6 power: Off(2)  
Outlet7 power: Off(2)  
Outlet8 power: Off(2)  
-----
```

### Command to obtain the status for outlet 4

```
$ bsmPDUpower.sh -H X.X.X.X -a status -m apc -S 1 -C public -c 4
```

### Output

```
-----  
Power Distribution Unit: X.X.X.X, MODEL: "AP7922", Serial Nb: "ZA0904000484",  
Firm Rev: "v3.5.7"  
Outlet4 power: Off(2)  
-----
```



### 2.17.2.3. Get the power consumption

The `getPowerConsumption` action is used to get the power consumption (in Watts) for all outlets of a PDU.

#### Syntax

```
bsmPDUpower.sh [-h] [-l level] -m model -H host [-o outfile]
-a getPowerConsumption [-p SNMP port] [-S SNMPv] [[-C community]]
[-u user -L secllevel -A authPass -P authPro -X privPass -x privPro]]
[-T timeout]
```

#### Options

<code>-p port</code>	SNMP port (default value: 161)
<code>-S SNMPv</code>	SNMP version: 1 (default value), 2c, 3
<code>-C community</code>	SNMPv1 community (default value 'public' for <code>getPowerConsumption</code> action)
<code>-L secllevel</code>	SNMPv3 SecurityLevel (noAuthNoPriv   authNoPriv   authPriv)
<code>-u user</code>	SNMPv3 user.
<code>-A authPass</code>	SNMPv3 authentication passphrase (15 to 32 ASCII characters)
<code>-P authPro</code>	SNMPv3 authentication protocol (default value 'MD5' )
<code>-X privPass</code>	SNMPv3 privacy passphrase (15 to 32 ASCII characters, different than <code>-authPass</code> )
<code>-x privPro</code>	SNMPv3 privacy protocol (default value 'DES' )
<code>-T timeout</code>	SNMP timeout (default value: 30 seconds)

#### Command

```
$ bsmPDUpower.sh -H X.X.X.X -a getPowerConsumption -m apc
```

#### Output

```
-----
Power OK: Reading 5 Watts|power=5;5520;7360;0
-----
```

Or should be:

```
power=10;5000;7000;0
```

```
power consumption:10
high power level:   5000
critical power level: 7000
minimal consumption: 0
```

Output OK:

```
Power OK: 10|power=10;5000;7000;0
```

Output WARNING:

```
Power WARNING: High power level detected: 5500|power=5500;5000;7000;0
```

Output CRITICAL:

```
Power CRITICAL: Critical power level detected: 7500|power=7500;5000;7000;0
```

## 2.18. bsmppower

`bsmppower.sh` is used to perform system POWER ON/OFF and FORCE POWER OFF operations and to check the power state:

```
bsmppower.sh -a on
bsmppower.sh -a off
bsmppower.sh -a off_force
bsmppower.sh -a status
```

This command is asynchronous and returns the prompt before the command has completed.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

A power ON command on an already powered ON system and/or a power OFF command on an already powered OFF system may return 0 (command accepted).

An acknowledgement message is displayed in `stdout` (except if the `-q` option is specified).

- 
- Notes**
- For the Power Off command to be taken into account on a remote host running Windows 2000 / 2003 Server, the **Shutdown: Allow system to be shut down without having to log on** security option must be enabled on the remote host. To configure this security option:
    - Click Start > Run.
    - In the Open box, type `gpedit.msc` and click OK.
    - In the Group Policy window, expand Computer Configuration\Windows\Settings\Security Settings\Local\Policies\Security Options\.
    - Set the Shutdown Security option to **enabled**.
  - Servers are identified by their DNS name or IP address (-H parameter).
  - In order to power on/off a chassis, the system executing `bsmppower` must be declared on the target server as a member of a SNMPv1 read-write community. The default read-write community name used by `bsmppower` is **private**.
-

## 2.18.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no messages are logged (default). 1: FAILED completion only is logged. 3: FAILED and SUCCESSFUL completion are logged.
-q	Quiet option: stops all outputs (stdout, stderr, or outfile if the -o option is specified).
-a action	Action: on, off, off_force, status or diag
-H host	DNS name or target system IP address.
-m model	Target system model: lanplus, ipmidrv.
-u user	User identification.
-Y cipher	Cipher suite ID used by the lanplus interface (default is 3).
-p password	User password or authentication key.
-o outfile	Output file name to which the stdout and stderr outputs are redirected.

## 2.18.2. Usage: Server using lanplus model

The user can force a diagnostic interrupt on Novascale servers using the lanplus model running the following command:

```
bsmpower.sh -a diag
```

This command sends a diagnostic interrupt to the processor(s). It is used to make the Operating System perform a diagnostic dump for troubleshooting purposes.

---

**Note** The `bsmpower.sh -a status` command displays the system power ON/OFF status. The system power ON/OFF status represents the electrical status and not the functional status of the system. For example, a system may be powered ON but not RUNNING, due to a BIOS initialization error.

---

### Syntax

```
bsmpower.sh [-h] [-q] -a action -m lanplus -H host -u user  
[-p password] [-o outfile] [-l level] [-Y cipher]
```

### 2.18.2.1. Power On

#### Command

```
$ bsmppower.sh -a on -m lanplus -H X.X.X.X -u admin -p pass
```

### 2.18.2.2. Power Off

#### Command

```
$ bsmppower.sh -a off -m lanplus -H X.X.X.X -u admin -p pass
```

### 2.18.2.3. Power Off\_force

#### Command

```
$ bsmppower.sh -a off_force -m lanplus -H X.X.X.X -u admin -p pass
```

#### 2.18.2.4. Display Power Status

##### Command

```
$ bsmpower.sh -a status -m lanplus -H X.X.X.X -u MWA -p guest
```

##### Output Example

```
-----  
Chassis Power is on  
-----
```

##### Command

```
$ bsmpower.sh -a status -m lanplus -H X.X.X.X -u MWA -p guest
```

##### Output Example

```
-----  
Chassis Power is on  
-----
```

##### Return Codes

0	System powered ON.
1	System powered OFF.
-1	Command failed.

#### 2.18.2.5. Send Diagnostic Interrupt

---

**Note** A diagnostic launched on a powered off server cannot be executed.

---

##### Command

```
$ bsmpower.sh -a diag -m lanplus -H X.X.X.X -u super -p pass
```

##### Output Example

```
-----  
Chassis Power Control: Diag  
-----
```

##### Return Codes

0	Command accepted.
-1	Command failed.

### 2.18.3. Usage: Server using ipmidrv model

---

**Note** The `bsmpower.sh -a status` command displays the system power ON/OFF status. The system power ON/OFF status represents the electrical status and not the functional status of the system. For example, a system may be powered ON but not RUNNING, due to a BIOS initialization error.

---

#### Syntax

```
bsmpower.sh [-h] [-q] -a action -m ipmidrv [-o outfile] [-l level]
```

#### Command

```
$ bsmpower.sh -a status -m ipmidrv
```

#### Output Example

```
-----  
Chassis Power is on  
-----
```

## 2.19. bsmreset

bsmreset.sh is used to forcibly Power Reset a server.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

If the server is not in the right state to perform the reset command, an error is displayed.

---

**Note** Servers are identified by their DNS name or IP address (-H parameter).

---

### 2.19.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-q	Quiet option: stops all outputs (stdout, stderr, or outfile if -o option is specified).
-H host	DNS name or target server IP address.
-m model	Target server model: lanplus.
-u user	BMC user for NovaScale target servers.
-p password	User password.
-Y cipher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which stdout and stderr outputs are redirected.

### 2.19.2. Usage

#### Syntax

```
bsmreset.sh [-h] [-q] -m lanplus -H host -u user [-p password]
[-o outfile] [-l level] [-Y cipher]
```

#### Command

```
$/bsmreset.sh -m lanplus -H X.X.X.X -u super -p pass
```

#### Output Example

```
-----
Chassis Power Control: Reset
-----
```

## 2.20. bsmResetAllEMMPartition

bsmResetAllEMMPartition.sh is a specific multimodule configuration tool. It is used to reset the firmware for all modules in a partition.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.20.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged into syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus
-H IPaddress	BMC IP address for a module included in the platform.
-u user	EMM user.
-p password	User password.
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which <code>stdout</code> and <code>stderr</code> outputs are redirected.

### 2.20.2. Usage

#### Syntax

```
bsmResetAllEmmPartition.sh [-h] [-l level] -m model -H IPaddress [-u user] [-p password] [-Y cypher] [-o outfile]
```

#### Command

```
$ bsmResetAllEMMPartition.sh -m lanplus -H X.X.X.X -u super -p pass
```

#### Output on a bi-modules

```
-----  
Sent cold reset command to MC  
Sent cold reset command to MC  
-----
```



## 2.21. bsm sensor

`bsmsensor` is used to direct sensor values to the standard output.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

The sensor values are displayed in `stdout`, as follows:

```
<sensor addr> | <sensor id> | <sensor value> | <sensor unit> | <status> | <lower non recoverable> | <lower critical> | <lower non critical> | <upper non critical> | <upper critical> | <supper non recoverable>
```

If the `-v` option is specified, one sensor is displayed per field, over several rows depending on the format.

`<label>: <value>`

The fields and labels display may change according to servers and to sensors.

- 
- Notes**
- Servers are identified by their DNS name or IP address (`-H` parameter).
  - Sensor type (see definition in IPMI specification) may be specified either with the sensor type code in hexadecimal (i.e. `-t 0x01` for temperature) or with the sensor type string (i.e. `-t Power Unit`).
  - `-s sensorid` and `-t type` parameters are exclusive.
- 

### 2.21.1. Options

<code>-h</code>	Displays command usage.
<code>-l level</code>	Specifies the severity of the messages to be logged in <code>syslog</code> . 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
<code>-v</code>	Displays details of each sensor. See output section below.
<code>-H host</code>	DNS name or target server IP address.
<code>-m model</code>	Target server model: <code>lanplus</code> , <code>ipmidrv</code> .
<code>-u user</code>	BMC user for NovaScale target servers.
<code>-p password</code>	User password.
<code>-Y cipher</code>	Cipher suite ID to be used by <code>lanplus</code> interface (default is 3).
<code>-c</code>	On IPMI servers, used in conjunction to <code>-v</code> in order to get sensors information in a more compact form.
<code>-o outfile</code>	Output file name to which <code>stdout</code> and <code>stderr</code> outputs are redirected.
<code>-s sensorid</code>	Specify a list of sensor(s), specified between quotes <code>""</code> and separated by comma(s), to be read.
<code>-t type</code>	Process only sensors of the specified type (as defined in IPMI specification).
<code>-a</code>	Process only analog sensors of the type specified with <code>-t type</code> .

## 2.21.2. Usage: Server using lanplus model

### Syntax

```
bsmsensor.sh [-h] [-v] -m lanplus -H host -u user [-p password] [-c] [-o outfile] [-l level] [-s sensorid_list] [-t type [-a]] [-Y cipher]
```

### 2.21.2.1. Display Power Supply sensor

#### Command

```
$ bsmsensor.sh -m lanplus -H X.X.X.X -u super -p pass -t "Power Supply"
```

#### Output

```
-----  
0x00800001 | PS_0          | 0x80    | na      | discrete | 0x0100 |  
na         | na           | na      | na      | na       | na     |  
0x0080000e | Pwr Consumption | 0x80    | 520     | Watts    | ok     |  
na         | na           | na      | na      | na       | na     |  
-----
```

### 2.21.2.2. Display temperature sensor for servers using lanplus model

#### Command

```
$ bsmsensor.sh -m lanplus -H X.X.X.X -u super -p pass -t 0x01
```

#### Output

```
-----  
0x008000be | Ambient Temp. | 0x80    | 22.0    | degrees C | ok     |  
na         | 10.0          | na      | 35.0    | 40.0      | na     |  
0x0080006b | MXB Temperature | 0x80    | 22.0    | degrees C | ok     |  
na         | 10.0          | na      | na      | 55.0      | na     |  
0x0080006c | ILB Temperature | 0x80    | 47.0    | degrees C | ok     |  
na         | 10.0          | na      | na      | 65.0      | na     |  
0x0080006d | PDB Temperature | 0x80    | 29.0    | degrees C | ok     |  
na         | 10.0          | na      | na      | 55.0      | na     |  
0x00800096 | UltraCapa Temp. | 0x80    | 29.0    | degrees C | ok     |  
na         | 10.0          | na      | na      | 55.0      | na     |  
0x0080008d | LCP Temperature | 0x80    | 32.0    | degrees C | ok     |  
na         | 10.0          | na      | na      | 55.0      | na     |  
-----
```

### 2.21.2.3. Display one sensor

#### Command

```
$ bsmsensor.sh -m lanplus -H X.X.X.X -u super -p pass -s "MXB Temperature"
```

#### Output

```
-----  
Locating sensor record...  
Sensor Addr      : 0x0080006b  
Sensor ID        : MXB Temperature (0x6b)  
Owner ID         : 0x80  
Entity ID        : 18.96 (Processor Board)  
Sensor Type (Analog) : Temperature  
Sensor Reading   : 17 (+/- 0) degrees C  
Status           : ok  
Lower Non-Recoverable : na  
Lower Critical    : 10.0  
Lower Non-Critical : na  
Upper Non-Critical : na  
Upper Critical    : 55.0  
Upper Non-Recoverable : na  
Assertion Events  : lcr+ ucr-  
Assertions Enabled : lcr- ucr+  
Deassertions Enabled : lcr- ucr+  
-----
```

#### Command

```
$ bsmsensor.sh -m lanplus -H X.X.X.X -u super -p pass -s "FAN_7 Voltage"
```

#### Output

```
-----  
Locating sensor record...  
Sensor Addr      : 0x00800085  
Sensor ID        : FAN_7 Voltage (0x85)  
Owner ID         : 0x80  
Entity ID        : 29.103 (Fan Device)  
Sensor Type (Analog) : Voltage  
Sensor Reading   : 11.3 (+/- 0) Volts  
Status           : ok  
Lower Non-Recoverable : na  
Lower Critical    : na  
Lower Non-Critical : na  
Upper Non-Critical : na  
Upper Critical    : na  
Upper Non-Recoverable : na  
-----
```

## 2.21.2.4 Display two sensors

### Command

```
$ bsmsensor.sh -m lanplus -H X.X.X.X -u super -p pass -s "PS_0","Pwr Consumption"
```

### Output

```
-----  
Locating sensor record...  
Device ID           : PS_0  
Entity ID           : 10.96 (Power Supply)  
Device Access Address : 80h  
Logical FRU Device   : 04h  
Channel Number      : 0h  
LUN.Bus             : 0h.0h  
Device Type.Modifier : 10h.2h (IPMI FRU Inventory)  
OEM                 : 00h  
  
Sensor Addr        : 0x0080000e  
Sensor ID          : Pwr Consumption (0xe)  
Owner ID           : 0x80  
Entity ID          : 19.96 (Power Unit)  
Sensor Type (Analog) : Other  
Sensor Reading     : 796 (+/- 0) Watts  
Status             : ok  
Lower Non-Recoverable : na  
Lower Critical      : na  
Lower Non-Critical   : na  
Upper Non-Critical   : na  
Upper Critical       : na  
Upper Non-Recoverable : na  
-----
```

## 2.21.3. Usage: Server using ipmidrv model

### Syntax

```
bsmsensor.sh [-h] [-v] -m ipmidrv [-o outfile] [-l level] [-s sensorid_list]  
[-t type [-a]] [-c]
```

### Command

```
$ bsmsensor.sh -m ipmidrv -t "Power Supply"
```

### Output

```
-----  
0x00800001 | PS_0           | 0x80   | na   | discrete | 0x0100 |  
na         | na            | na     | na   | na       | na     |  
0x0080000e | Pwr Consumption | 0x80   | 520  | Watts    | ok     |  
na         | na            | na     | na   | na       | na     |  
-----
```

## 2.22. bsmSetConfParam

bsmSetConfParam.sh is used to set the values of various configuration parameters.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.22.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no messages are logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-a action	Action: setPowerRestorePolicy. setPrimaryNTP setSecondaryNTP
-m model	Target server model: lanplus
-H host	BMC target IP address.
-u user	BMC user.
-p password	User password.
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3)
-o outfile	Output file name to which the stdout and stderr outputs are redirected.

### 2.22.2. Usage

#### Syntax

```
bsmSetConfParam.sh [-h] [-l level] -a action -m model -H host [-u user] [-p password] [-Y cypher] [-o outfile]
```

### 2.22.2.1. Set the power restore policy

The `setPowerRestorePolicy` action is used to set the power restore policy (On, Off or Restore) which will be apply to the system after an AC power loss.

#### Syntax

```
bsmSetConfParam.sh [-h] -a setPowerRestorePolicy -m model -H host  
-x value [-u user] [-p password] [-Y cipher] [-o outfile] [-l level]
```

#### Options

- x value
- on: chassis always powers up after AC mains electricity is switched on or returns following an interruption.
  - off: chassis always stays powered off after AC mains electricity is switched on, power pushbutton or command required to power on system.
  - restore: after AC main electricity is switched on or returns, power is restored to the state that was in effect when AC mains electricity was switched off or lost.

#### Command

```
$ bsmSetConfParam.sh -m lanplus -H X.X.X.X -u super -p pass  
-a setPowerRestorePolicy -x on
```

#### Output

None

### 2.22.2.2. Set the primary NTP server IP address

The `setPrimaryNTP` action is used to set the IP address for the primary NTP server which gives the date and time.

#### Syntax

```
bsmSetConfParam.sh [-h] -a setPrimaryNTP -m model -H host -x value  
[-u user] [-p password] [-Y cipher] [-o outfile] [-l level]
```

- x value
- NTP server IP address to be set.

#### Command

```
bsmSetConfParam.sh -m lanplus -H X.X.X.X -u super -p pass -a setPrimaryNTP -x X.X.X.X
```

#### Output

```
-----  
NTP server set successfully  
-----
```

### 2.22.2.3. Set the secondary NTP server IP address

The `setSecondaryNTP` action is used to set IP address for the secondary NTP server which gives the date and time.

#### Syntax

```
bsmSetConfParam.sh [-h] -a setSecondaryNTP -m model -H host -x value  
[-u user] [-p password] [-Y cipher] [-o outfile] [-l level]
```

#### Command

```
bsmSetConfParam.sh -m lanplus -H X.X.X.X -u super -p pass -a setSecondaryNTP -x X.X.X.X
```

#### Output

```
-----  
NTP server set successfully  
-----
```

## 2.23. bsmSetPartition

bsmSetPartition.sh is a specific multimodule configuration tool. It is used to set some partition parameters. Setting is done for all modules belonging to the partition.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

### 2.23.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged into syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus
-H module	BMC IP address for a module included in the platform.
-u user	EMM user.
-p password	User password.
-c composition	Partition composition (decimal value from 1 to 15).
-d master	Master module identifier (value from 0 to 3).
-P partition_name	Partition name
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which <code>stdout</code> and <code>stderr</code> outputs are redirected.

### 2.23.2. Usage

#### Syntax

```
bsmSetPartition.sh [-h] [-l level] -m model -H module -c composition  
[-d master] [-u user] [-p password] [-P partition_name] [-Y cypher] [-o  
outfile]
```

```
$ bsmSetPartition.sh -m lanplus -H X.X.X.X -u super -p pass -d 0 -c 3 -P mapartition
```

#### Output

```
-----  
New partition composition set on module0.  
New partition composition set on module1.  
New master ID set to 0 on module0.  
New master ID set to 0 on module1.  
Partition name set for module0.  
Partition name set for module1.  
-----
```



## 2.24. bsmSetPlatformLevelParam

bsmSetPlatformLevelParam.sh is used to set some platform parameters. If neither the platform name nor the IP prefix is set, nothing is done. Setting is done for all modules belonging to the platform.

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

---

**Note** -l prefix\_ip is a specific for multimodule parameter.

---

### 2.24.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged into syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus
-H IPaddress	BMC IP address for a module included in the platform.
-u user	EMM user.
-p password	User password.
-N name	Platform label (14 characters maximum).
-I prefix_ip	Platform IP address prefix.
-Y cypher	Cipher suite ID to be used by lanplus interface (default is 3).
-o outfile	Output file name to which stdout and stderr outputs are redirected.

### 2.24.2. Usage

#### Syntax

```
bsmSetPlatformLevelParam.sh [-h] [-l level] -m model -H IPaddress [-u user] [-p password] [-N name] [-I prefix_ip] [-Y cypher] [-o outfile]
```

#### Command to set a platform IP address prefix

```
$ bsmSetPlatformLevelParam.sh -m lanplus -H X.X.X.X -u super -p pass -l 172.32
```

#### Output

```
-----  
Address IP prefix set for module0.  
Address IP prefix set for module1.  
-----
```

## 2.25. bsmsol

The `bsmsol` command is used to establish a Serial-Over-Lan session.

- 
- Notes**
- Enter "~." to close the session.
  - Only one Serial-Over-Lan session can be opened on a given target server.
- 

### 2.25.1. Options

-h	Displays command usage.
-l level	Specifies the severity of the messages to be logged in syslog. 0: no message is logged (default). 1: only the FAILED completion of the command is logged. 3: FAILED and successful completion of the command are logged.
-m model	Target server model: lanplus.
-H host	DNS name or target server IP address.
-C cipher	Cipher suite to be used by ipmilan model for lanplus encryption (default value "0" means no encryption).
-L priv	Remote session privilege level (ADMINISTRATOR (default), OPERATOR, USER).
-u user	BMC user.
-p password	User password.
-Y cipher	Cipher suite ID to be used by lanplus interface (default is 3).

### 2.25.2. Usage

#### Syntax

```
bsmsol.sh [-h] -m lanplus -H host -u user [-p password] [-l level] [-L priv] [-Y cipher]
```

#### Command

```
$ bsmsol.sh -m lanplus -H X.X.X.X -u root -p root
```

#### Output

```
-----  
[SQL Session operational. Use ~? For help]  
Shell>  
.....  
Shell>~. [terminated ipmitool]  
-----
```

## Appendix A. Server ON / OFF Status Codes

This appendix lists the interconnection between the ON / RUNNING / TRANSIENT / OFF states returned by the `bsmpower.sh -a` status command and the server states.

OFF corresponds to server states:

INACTIVABLE

INACTIVE

TRANSIENT corresponds to server states:

POWERING ON

POWERING ON FAILED

TIMEOUT DURING POWER ON

POWERING ON SUSPENDED

POWERING DOWN

POWER DOWN FAILED

TIMEOUT DURING POWER DOWN

ON corresponds to server states:

DOMAIN HALTED

POWERED ON - LOADING BIOS

BIOS READY - STARTING EFI

BIOS LOADING TIMEOUT

RECOVERING BIOS

TIMEOUT DURING START EFI

RUNNING corresponds to server states:

EFI STARTED - BOOTING OS

RUNNING



# Appendix B. User/Password Internal Authentication File

## B.1. User/Password Authentication

Most of the Hardware Management Commands need a user/password authentication in order to access a target identified by:

- the platform manager (specified by `-H host`),

The password information used by the Hardware Management Commands may be either specified in the command, or extracted from an authentication internal file if no password is specified in the command.

This internal authentication file contains the list of targets, identified as follows:

- platform manager (role : manager, identified by its DNS name),

This file can be accessed with dedicated users/passwords.

It is created and managed using the `bsmcfg_auth_cmd` command.

The `bsmcfg_auth_cmd` command allows to:

- add an entry defined by: `user + password + target`
- delete an entry defined by: `user + target`
- get the encoded password for an entry defined by: `user + target`
- get the decoded password for an entry defined by: `user + target`
- list the entries.

The password information is stored in the authentication internal file as a base64 encoded string.

## B.2. bsmcfg\_auth\_cmd command

`bsmcfg_auth_cmd` command manages the internal authentication file:

```
bsmcfg_auth_cmd.sh -a add
bsmcfg_auth_cmd.sh -a getE
bsmcfg_auth_cmd.sh -a getD
bsmcfg_auth_cmd.sh -a del
bsmcfg_auth_cmd.sh -a list
```

### Syntax

```
bsmcfg_auth_cmd.sh [-h] [-a action] [-u user] [-p password]
-H manager
```

When the command is accepted, the return code is 0. If the command fails, the return code is -1.

---

**Notes**

- For NovaScale servers using the ipmilan model, it is possible to use the same user/password authentication for all the servers available. This can be done by setting "\*" as the manager parameter.

---

### B.2.1. Options

-h	Displays command usage.
-a action	Action on the internal authentication file: add, del, getE, getD, list.
-H manager	DNS name or platform Manager IP address
-u user	Manager user.
-p password	Manager user password.

## B.2.2. Usage

### B.2.2.1. Add a target

`add` is used to add in the internal authentication file, a target to the list of targets that can be accessed with a dedicated user/password.

#### Syntax

```
bsmcfg_auth_cmd.sh -a add -u user -p password  
-H manager
```

#### Command to add a platform Manager

```
$ bsmcfg_auth_cmd.sh -a add -u MWA -p mwapwd -H X.X.X.X
```

#### Output

```
-----  
Key entry successfully added  
-----
```

#### Command

```
$ bsmcfg_auth_cmd.sh -a add -u MWA2 -p mwa2pwd -H ""
```

### B.2.2.2. Extract the encoded password

`getE` is used to extract, from the internal authentication file, the encoded password needed to access a target with a dedicated user.

#### Syntax

```
bsmcfg_auth_cmd.sh -a getE -u user  
-H manager
```

Command to get the encoded password to access a platform Manager

```
$ bsmcfg_auth_cmd.sh -a getE -u MWA -H X.X.X.X
```

Output

```
-----  
cGFzcw==  
-----
```

```
$ bsmcfg_auth_cmd.sh -a getE -u MWA2 -H ""
```

Output

```
-----  
RfGFerv==  
-----
```



### B.2.2.3. Extract the password needed to access a target

getD is used to extract, from the internal authentication file, the password needed to access a target for a user.

#### Syntax

```
bsmcfg_auth_cmd.sh -a getD -u user  
-H manager
```

#### Command to get the password to access a platform Manager

```
$ bsmcfg_auth_cmd.sh -a getD -u MWA -H X.X.X.X
```

#### Output

```
-----  
mwapwd  
-----
```

```
$ bsmcfg_auth_cmd.sh -a getD -u MWA2 -H ""
```

#### Output

```
-----  
mwa2pwd  
-----
```

#### B.2.2.4. Delete a target

`del` is used to delete, in the internal authentication file, a target from the list of targets that can be accessed by a user.

##### Syntax

```
bsmcfg_auth_cmd.sh -a del -u user  
-H manager
```

##### Command to delete a platform Manager

```
$ bsmcfg_auth_cmd.sh -a del -u MWA -H X.X.X.X
```

##### Output

```
-----  
Key entry successfully deleted  
-----
```

##### Command to delete a generic device

```
$ bsmcfg_auth_cmd.sh -a del -u MWA2 -H ""
```

##### Output

```
-----  
Key entry successfully deleted  
-----
```

### B.2.2.5. Display the contents of the internal authentication file

list is used to display the contents of the internal authentication file, this means the list of targets that can be accessed with their user/password details.

#### Syntax

```
bsmcfg_auth_cmd.sh -a list
```

#### Command

```
$ bsmcfg_auth_cmd.sh -a list
```

#### Output

```
-----  
<?xml version="1.0"?>  
<auth_entries>  
  <auth_entry keyname="HWMGR_mgr1" password="cHdkMQ%3D%3D" user="usr1" />  
  <auth_entry keyname="HWMGR_mgr2" password="d3h5" user="usr2" />  
  <auth_entry keyname="FTPSRV_srv1" password="cHdkMQ%3D%3D" user="usr1" />  
  <auth_entry keyname="DEV_ipaddr1" password="ZGV2cHdk" user="devuser" />  
  <auth_entry keyname="HWMGR_*" password="d3h6" user="MWA2" />  
</auth_entries>  
-----
```



---

# Glossary

---

## A

### **ABR**

Automatic BIOS Recovery.

### **ACPI**

Advanced Configuration and Power Interface.

An industry specification for the efficient handling of power consumption in desktop and mobile computers. ACPI specifies how a computer's BIOS, operating system, and peripheral devices communicate with each other about power usage.

### **ADM1069**

The ADM1069 Super Sequencer® is a configurable supervisory/ sequencing device that offers a single-chip solution for supply monitoring and sequencing in multiple supply systems.

### **ARU**

Add / Removeable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. An ARU can be nested and is not necessarily separable from other ARUs. An ARU is also known as a PMU.

### **ASR**

Automatic Server Restart.

### **ASIC**

Application Specific Integrated Circuit.

---

## B

### **Base Operating System**

The Operating System that is booted at initialization.

### **BCS**

Bull Coherent Switch. This is the Bull eXternal Node Controller providing SMP upgradeability up to 16 processors. The BCS ensures global memory and cache coherence, with optimized traffic and latencies, in both IPF-preferred and XPF-preferred variants.

### **BHC**

See Blade Hardware Console.

### **BIOS**

Basic Input / Output System. A program stored in flash EPROM or ROM that controls the system startup process.

### **BIST**

Built-In Self-Test. See POST.

### **Blade Hardware Console**

Graphical user interface used to access the management software embedded in the blade module.

### **BMC**

Baseboard Management Controller. See Embedded Management Controller.

### **BOOTP**

Network protocol used by a network client to obtain an IP address from a configuration server.

**BT**

Block Transfer. One of the three standardized IPMI System interfaces used by system software for transferring IPMI messages to the BMC. A per-block handshake is used to transfer data (higher performance).

---

**C****Chassis Hardware Console**

Graphical user interface used to access the management software embedded in the Chassis Management Module.

**CHC**

See Chassis Hardware Console.

**Clipping**

An Event filter criterion. Clipping is defined on a Count / Time basis aimed at routing a pre-defined number of messages only. Identical messages are counted and when the number of messages indicated in the Count field is reached within the period of time indicated in the Time field, no other messages will be selected for routing.

**CMB**

Chassis Management Board.

**CMC**

A Corrected Memory Check condition is signaled when hardware corrects a machine check error or when a machine check abort condition is corrected by firmware. See MCA.

**CMC**

Chassis Management Controller.

**CMM**

Chassis Management Module.

**Core**

Core is the short name for the processor execution core implemented on a processor. A core contains one or more threads (logical processors).

**CRU**

Customer Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by the End User as a single entity.

**CSE**

Customer Service Engineer.

---

**D****DES**

Data Encryption Standard.

**DHCP**

Dynamic Host Configuration Protocol.

**DMA**

Direct Memory Access. Allows data to be sent directly from a component (e.g. disk drive) to the memory on the motherboard). The microprocessor does not take part in data transfer enhanced system performance.

**DNS**

Domain Name Server.

---

## E

### **EEPROM**

Electrically Erasable Programmable Read-Only Memory. A type of memory device that stores password and configuration data.

### **EFI**

Extensible Firmware Interface. A specification for a firmware-OS interface.

### **EFI Shell**

Simple, interactive user interface that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. In addition, the EFI Shell provides a set of basic commands used to manage files and the system environment variables. See Shell.

### **Embedded Management Controller**

Also known as BMC (Baseboard Management Controller). This controller, embedded on the main system board, provides out-of-band access to platform instrumentation, sensors and effectors.

### **EMM**

Embedded Management Module. Software embedded in the server module to implement management functions and accessible from the Hardware Console graphical interface.

### **EPROM**

Erasable Programmable Read-Only Memory. A type of memory device that is used to store the system BIOS code. This code is not lost when the computer is powered off.

### **ESB**

Ethernet Switch Board.

### **ESM**

Ethernet Switch Module.

---

## F

### **FC-LGA**

Flip-Chip Land Grid Array.

### **Flash EPROM**

Flash Erasable Programmable Read-Only Memory. A type of memory device that is used to store the system firmware code. This code can be replaced by an updated code from a floppy disk, but is not lost when the computer is powered off.

### **FPGA**

Field Programmable Gate Array.

### **FQDN**

Fully Qualified Domain Name.

### **FRU**

Field Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by Customer Service Engineers as a single entity.

---

## G

### **GPU**

Graphical Processing Unit.

### **GUI**

Graphical User Interface.

---

## H

### HA

High Availability. Refers to a system or component that is continuously operational for a desirably long length of time.

### Hardware

The physical parts of a system, including the keyboard, monitor, disk drives, cables and circuit cards.

### Hardware Partition

A set of hardware components that can boot and run a Base OS image.

### Hard Partitioning

Ability to split a platform into a number of independent smaller hardware partitions or to merge multiple independent hardware partitions to form a single larger hardware partition.

### HPC

High Performance Computing.

### HPC Cluster

High Performance Computing Cluster. A group of computers linked together to form a single computer.

### Host Operating System

The Operating System that is booted at initialization and that is a Virtual Machine Monitor (VMM) and a number of guest OS.

### Hot-Plugging

The operation of adding a component without interrupting system activity.

### Hot-Swapping

The operation of removing and replacing a faulty component without interrupting system activity.

### HT

HyperThreading. See Multi-Threading.

---

## I

### I2C

Intra Integrated Circuit. The I2C (Inter-IC) bus is a bi-directional two-wire serial bus that provides a communication link between integrated circuits (ICs). The I2C bus supports 7-bit and 10-bit address space devices and devices that operate under different voltages.

### IB

InfiniBand.

### iBMC

Integrated Baseboard Management Controller. See Embedded Management Controller.

### iCare

The iCare Console (insight Care) is a web-based administration application which provides tools for hardware unit maintenance.

### ICH

Input/Output Hub. Provides a connection point between various I/O components and Intel processors.

### ICMB

Intelligent Chassis Management Bus. Name for the architecture, specifications, and protocols used to interconnect intelligent chassis via an RS-485-based serial bus for the purpose of platform management.

### ILB / ILBC

I/O Legacy Board / I/O Legacy Board Controller.



**ILM**

Independent Loading Mechanism. The Independent Loading Mechanism (ILM) - comprising a load plate, load lever and four corner screws - provides the needed force to seat a CPU neatly onto the socket contacts.

**INCA**

INtegrated Cluster Architecture.

**IOH**

Input/Output Hub. An Intel QPI agent that handles I/O requests for processors.

**IPMB**

Intelligent Platform Management Bus. Abbreviation for the architecture and protocol used to interconnect intelligent controllers via an I2C based serial bus for the purpose of platform management.

**IPMI**

Intelligent Platform Management Interface. A specification owned by Intel which describes mechanisms and devices to completely offload the task of managing system hardware from the primary CPU.

---

**J****JOEM**

JTAG Over Ethernet Module.

**JTAG**

Joint Test Action Group.

---

**K**

No entries.

---

**L****LAN**

Local Area Network.

**LCD**

Liquid Crystal Display.

**LCP**

Local Control Panel. Module consisting of a controller, a LCD color display, a green and a blue LED and a Power ON button.

**LDAP**

Lightweight Directory Access Protocol.

**LED**

Light Emitting Diode.

**Logical Partition**

When the Base Operating System is a Virtual Machine Monitor, a logical partition is the software environment used to run a Guest Operating System.

**Logical Processor**

See Thread.

---

**M****MAC**

Media Access Control.

**MCA**

A Machine Check Abort exception occurs when an error condition has arisen that requires corrective action.

**MESCA**

Multiple Environments on a Scalable Csi-based Architecture.

**MIB**

Management Interface Base.

**MIMD**

Multiple Instruction Multiple Data

**MMX**

MultiMedia eXtensions.

**MTB/MTBC**

Memory and Tukwila Board / Memory and Tukwila Board Controller.

**MTBF**

Mean Time Between Failure.

**Multicore**

Presence of two or more processors on a single chip.

**Multi-Threading**

The ability of a single processor core to provide software visibility similar to that of several cores and execute several threads in apparent (to software) simultaneity while using limited additional hardware resources with respect to a core without multi-threading.

Depending on core design, the instructions issued for execution by the core at a given cycle may be either Hyper-Threading (HT) - from a single thread, switching to another thread upon occurrence of specific events (e.g. cache misses) or Simultaneous Multi-Threading (SMT) - from both threads.

**MPB/MPBC**

Memory and Poulson Board / Memory and Poulson Board Controller.

**MXB/MXBC**

Memory and Xeon Board / Memory and Xeon Board Controller.

**MWB/MWBC**

Memory and Westmere Board / Memory and Westmere Board Controller

---

**N****Nehalem**

NEHALEM Intel Xeon Processor (8 cores per die).

**NFS**

Network File System.

**NIC**

Network Interface Controller.

**NUMA**

Non Uniform Memory Access.

**NVRAM**

Non-Volatile Random Access Memory.

---

**O****Off-Lining**

See On-Lining / Off-Lining.

**On-Lining / Off-Lining**

On-lining and off-lining are dynamic logical operations. On-lining is the non-physical addition of an ARU to the running OS. The on-lined unit already exists in the configuration as an inactive unit (present and connected). Off-lining is the non-physical removal of an ARU from the running OS. The off-lined unit remains in the configuration as an inactive unit, ready to be on-lined.

**OOB**

Out Of Band. Access to system platform management that does not go through the OS or other software running on the main processors of the managed system.

**OPMA**

Open Platform Management Architecture.

---

**P****PCI**

Peripheral Component Interconnect. Bus architecture supporting high-performance peripherals.

**PCIe**

PCI Express. Latest standard in PCI expansion cards.

**PDB**

Power Distribution Board. Sub-assembly of the Power Supply Module.

**PDU**

Power Distribution Unit. Power bus used for the connection of peripheral system components.

**Platform Event**

A platform event is an event that originates directly from platform firmware (BIOS) or platform hardware, independently of the state of the Operating System or System Management Hardware.

**PEF**

Platform Event Filtering.

A feature in IPMI that enables the BMC to generate a selectable action (e.g. power on/off, reset, send Alert, etc.) when a configurable event occurs on the management system.

**PET**

The Platform Event Trap format is used for sending a platform event in an SNMP Trap. See Platform Event.

**PIROM**

The Processor Information ROM contains information about the specific processor in which it resides. This information includes robust addressing headers to allow for flexible programming and forward compatibility, core and L2 cache electrical specifications, processor part and S-spec numbers, and a 64-bit processor number.

**PMU**

Physically Manageable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. A PMU can be nested and is not necessarily separable from other PMUs. A PMU is also known as an ARU.

**POST**

Power On Self Test.

**Processor**

Each processor contains one or more dies in a single package. Each die contains one or more cores. Each core contains one or more threads (logical processors). Each processor is housed in a processor socket.

**PSMI**

Power Supply Management Interface.

**PSU**

Power Supply Unit. Sub-assembly of the Power Supply Module.

**PSWB**

PCI SWitch Board.

**PSWM**

PCI SWitch Module.

**PWM**

Pulse Width Modulation.

---

## Q

### **QDR**

Quad Data Rate. Communication signalling technique where data is transmitted at four points in the clock cycle.

### **QPI**

Quick Path Interconnect. High-speed point-to-point Intel interface, used to interconnect processors and I/O Hubs, and optionally node controllers (BCS).

### **QSB**

Quad Switch Board.

### **QSFP**

Quad Small Form-factor Pluggable. Low-power interconnect technology.

### **QSMB**

Quad Switch Module. InfiniBand Switch.

---

## R

### **RADIUS**

Remote Authentication Dial-In User Service.

### **RAS**

Reliability, Availability, Serviceability.

### **RMII**

Reduced Media Independent Interface. A standard that reduces the number of signals/pins required to connect an Ethernet chip to physical layer transceiver. See MII.

### **RTC**

Real Time Clock.

---

## S

### **SAS**

Serial Attached SCSI. A data transfer technology used to move data to and from computer storage devices such as hard drives and tape drives.

### **SATA**

Serial ATA. A computer bus technology for connecting hard disks and other devices.

### **SEL**

System Event Log. A record of system management events. The information stored includes the name of the event, the date and time the event occurred and event data. Event data may include POST error codes that reflect hardware errors or software conflicts within the system.

A non-volatile storage area into the BMC and associated interfaces for storing System platform Event information for later retrieval.

### **Server Hardware Console**

Graphical user interface used to access the management software embedded in the server module.

### **SHC**

See Server Hardware Console.

### **Simultaneous Multi-Threading**

See Multi-Threading.

### **SMBIOS**

System Management BIOS.

**SM-BUS**

System Management Bus.

**SMI**

System Management Interrupt.

**SMP**

Symmetrical Multi Processor. The processing of programs by multiple processors that share a common operating system and memory.

**SMT**

Simultaneous Multi-Threading.

**SMTP**

Simple Mail Transfer Protocol.

**SNC**

Scalable Node Controller. The processor system bus interface and memory controller for the Intel870 chipset. The SNC supports both the Itanium2 processors, DDR SDRAM main memory, a Firmware Hub Interface to support multiple Firmware hubs, and two scalability ports for access to I/O and coherent memory on other nodes, through the FSS.

**SNMP**

Simple Network Management Protocol.

**SoC**

System on Chip.

**Socket**

Central Processing Unit multicore interface.

**SOL**

Serial Over LAN. Mechanism that enables the input and output of the serial port of a managed system to be redirected via an IPMI session over IP.

**SO-DIMM**

Small Outline Dual In-line Memory.

**SR**

Scratch Register. Internal registers of both the Tukwila processor and the I/O Hub used as scratch area.

**SSH**

Secured Shell.

**SSL**

Secure Socket Layer.

---

**T****TELNET**

TELEcommunication NETwork. Protocol used on the Internet or Local Area Networks to provide a bidirectional interactive communications facility.

**Thread**

A thread or logical processor is the execution context within a single core and the software visibility of multi-threading. A single multi-threaded processor contains two or more threads (or logical processors).

**Thresholding**

An Event filter criterion. Thresholding is defined on a Count / Time basis aimed at routing significant messages only. Identical messages are counted and when the number of messages indicated in the Count field is reached within the period of time indicated in the Time field, this message is selected for routing.

**TKW**

TUKWILA Intel Itanium Processor (4 cores per socket).

---

## U

### UCM

Ultra Capacitor Module.

### UVLO

Under Voltage Latch Output.

---

## V

### VLAN

Virtual Local Area Network. A network protocol that allows systems connected to different LAN segments to behave as if they are connected to the same LAN segments.

### VMM

Virtual Machine Monitor.

---

## W

### WOL

Wake On Lan. A feature that provides the ability to remotely power on a system through a network connection.

---

## X

### XCSI

Extended Common System Interface. High-speed point-to-point Bull interface, used to interconnect servers. XCSI ports are located and managed in the BCS (node controller).

### XNC

External Node Controller. See BCS.

---

## Y

No entries.

---

## Z

No entries.

---







Bull Cedoc  
357 avenue Patton  
BP 20845  
49008 Angers Cedex 01  
FRANCE

REFERENCE  
86 A1 50FG 02