VANTAGEO Server

BMC Log Reference (BMC V3)

Version: R1.0

VANTAGEO PRIVATE LIMITED
Corporate Address: 617, Lodha Supremus II,
Road No. 22, Wagle Estate,
Thane - 400604
URL: https://vantageo.com
E-mail: support@vantageo.com
Helpdesk - +91 18002669898

LEGAL INFORMATION

Statement on the Use of Third-Party Embedded Software:

If third-party embedded software such as Oracle, Sybase/SAP, Veritas, Microsoft, VMware, and Redhat is delivered together with this product of VANTAGEO, the embedded software must be used as only a component of this product. If this product is discarded, the licenses for the embedded software must be void either and must not be transferred. VANTAGEO will provide technical support for the embedded software of this product.

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2023-12-27	First edition.

Serial Number: VT20230310

Publishing Date: 2023-12-27 (R1.0)

Contents

About This Manual

Purpose

This manual describes the logs of the VANTAGEO server in detail.

Intended Audience

This manual is intended for:

- Maintenance engineers
- Commissioning engineers

What Is in This Manual

This manual contains the following chapters.

Chapter 1, BMC Log Export	Describes how to export the BMC logs.
Chapter 2, BMC Log Analysis	Describes the directory structure and content of the BMC logs.
Chapter 3, BMC User Rights	Describes how to configure the BMC user rights.

Conventions

This manual uses the following conventions.

	Notice: indicates equipment or environment safety information. Failure to comply can result in equipment damage, data loss, equipment performance degradation, environmental contamination, or other unpredictable results.

Chapter 1
BMC Log Export

Table of Contents

1.1 Exporting BMC Logs in One Click

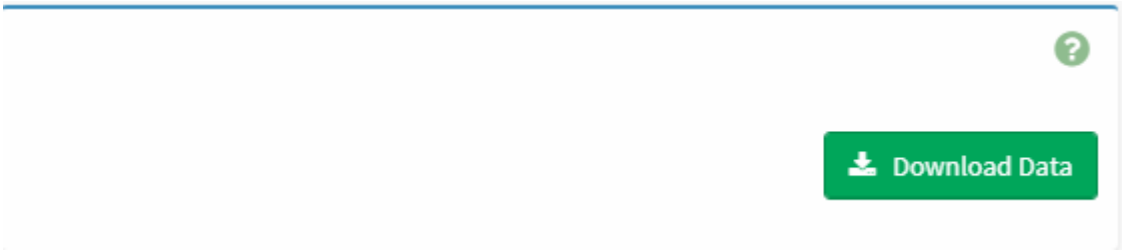
Abstract

The BMC Web portal provides the function of exporting logs in one click. The exported log file is named *bmcinfo.tar.gz* and saved in the default download directory of the browser.

Steps

1. Open the Chrome browser on your PC. In the address bar, enter the address of the BMC Web portal to access the BMC system.
2. From the menu bar in the left pane on the home page of the BMC Web portal, select **Maintenance**. The **Maintenance** page is displayed.
3. Click **Download Data**. The **Downloading Data in One Click** page is displayed, see Figure 1-1.

Figure 1-1 Downloading Data in One Click



4. Click the **Download Data** button.
   If the download is in **Processing** status, it indicates that the data is being downloaded.

Note

If the download is blocked by the browser, turn on the download permission, and click **Download Data** again. If the system prompts that "**Data is being cleared on the back end**", wait for a few minutes and try it again.

1.2 Exporting BMC Logs by Type

Abstract

BMC logs include:

- **Login log**: records user logins and logouts.
- **Operation log**: records user operations.
- **System log**: records logs and historical alarms generated during the operation of the server.

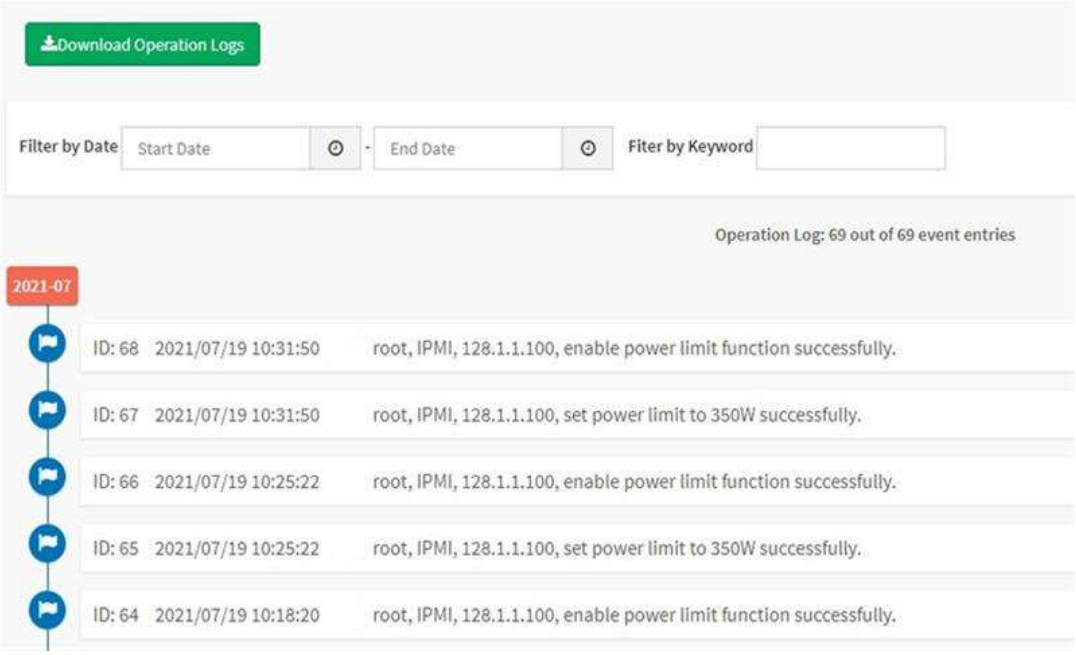
Note

This procedure describes how to export operation logs. The operations for exporting other types of logs are similar.

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > Operation Log**. The **Operation Log** page is displayed, see Figure 1-2.

Figure 1-2 Operation Log Page



2. Perform the following operations as required.

To ...	Do...
Filter logs by date	Click  in the **Filter by Date** area, and set the start date and end date to query operation logs during this period.
Filter logs by keyword	a. In the **Filter by Keyword** text box, enter a keyword. b. Press **Enter**. The query result is displayed at the bottom of the page.
Save logs to the local PC	Click **Download Operation Logs** and save the operation logs to the local PC.

1.3 Exporting Logs Through the Command Line (SSH)

Abstract

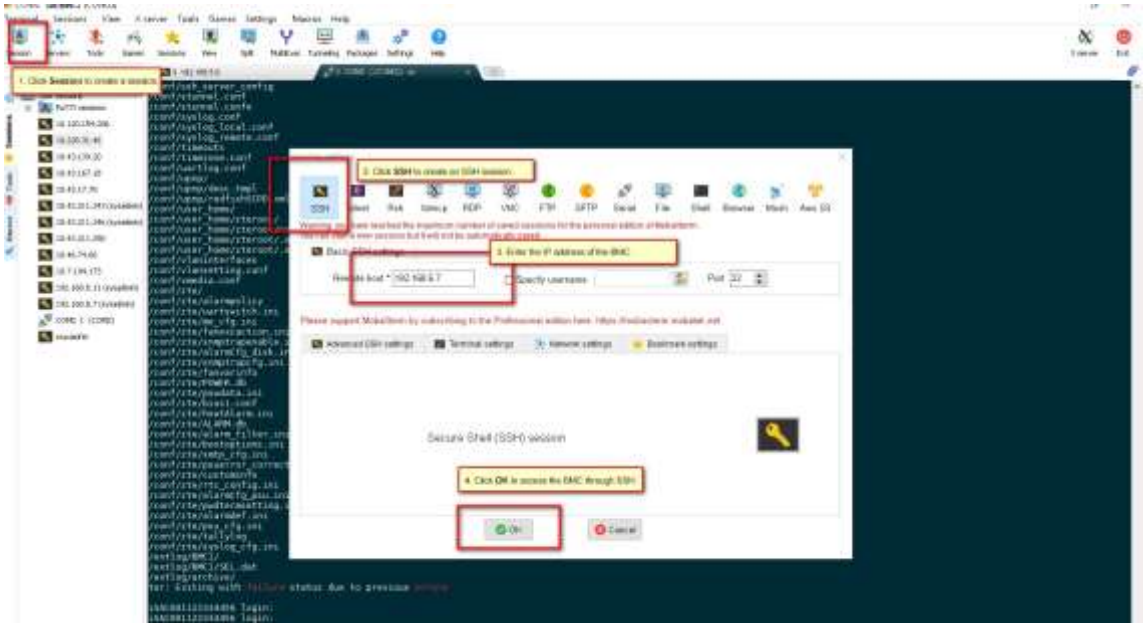
If the BMC Web portal is faulty, you can connect to the BMC remotely through SSH and export logs through the command line.

Steps

1. Connect to the BMC by using the SSH tool.

   Use the MobaXterm toolbox as an example, see Figure 1-3.

Figure 1-3 Connecting to the BMC Through SSH



2. Click **OK**. In the displayed dialog box, enter the SSH password of the BMC.
3. Enter the following commands in the command line to export logs:

   # cd /etc/init.d/

   # ./expert_data.sh

Note

The logs are exported to the */var/video/bmcinfo.tar.gz* directory.

4. Download the log file to the local PC.
5. (Optional) Enter the following commands in the command line to delete the BMC log file:

   # cd /var/video

   # rm bmcinfo_.tar.gz

1.4 Exporting Logs Through the Command Line (Serial Port)

Abstract

If you cannot connect to the BMC due to a network error, you can export logs through the serial port.

Steps

1. Connect to the serial port of the BMC by using a DB9 serial port cable.
2. Press and hold the UID button on the server panel for about six seconds until the indicator flashes blue.
3. Use a serial port tool to connect to the serial port of the BMC.
4. After the connection is established, log in to the serial port with the account and password.
5. Enter the following commands in the command line to export logs:

   # cd /etc/init.d/

   # ./expert_data.sh

Note

The logs are exported to the */var/video/bmcinfo.tar.gz* directory.

6. Run the following command to back up the log file to the */mnt/nandflash0/* directory:

   # cp /var/video/bmcinfo_.tar.gz /mnt/nandflash0/

Note

You can download the log file to the local PC by using the SFTP function after the network is restored.

Chapter 2
BMC Log Analysis

Table of Contents

Log Overview

BMC logs are exported as the bmcinfo.tar.gz compressed file.

After the file is decompressed, there are four directories:

- **Conf**: stores BMC configuration files.
- **Mnt**: stores key BMC NAND flash partition logs. The logs are be lost in case of power supply failure.
- **Tmp**: stores BMC logs that record the system operation status during log download.
- **Var**: stores the BMC system log that records system function errors. The logs are lost in case of power supply failure.

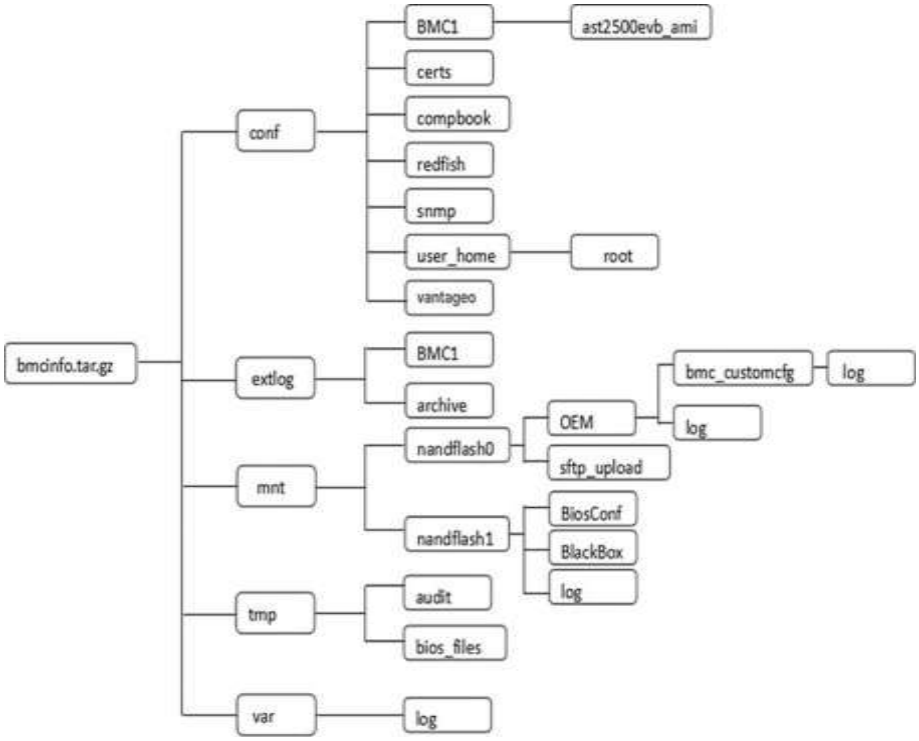
Note

A log rotation mechanism is used to prevent log files from being too big and thus occupying too much system storage space. A log file (using system.log as an example) is rotated every 30 minutes. When the size of the log file exceeds 1 Megabyte, it will be rotated without any regard for the time interval of rotation. After rotation, the log file becomes system.log.1, and a new log file named system.log is created.

Log File Structure

Figure 2-1 shows the structure of the *bmcinfo.tar.gz* log file.

Figure 2-1 Structure of the BMC Log File



2.1 Conf Directory

The Conf directory stores BMC configuration files. For the Conf directory structure, refer to Table 2-1.

Table 2-1 Conf Directory

Level-1 Directory	Level-2 Directory
BMC1	ast2500evb_ami
certs	–
compbook	–
redfish	–
root.ssh	–
snmp	–
user_home	root
Vantageo	–

Configuration files of the BMC system are stored in the Conf root directory and BMC1 sub-directory.

The vantageo directory stores configuration files of the OEM devices.

Notice

Do not change any configuration file of the BMC. Failure to comply can result in system operation failures.

2.2 Tmp Directory

The Tmp directory stores logs that record the current system operation status. For the Tmp directory structure, refer to Table 2-2.

Table 2-2 Tmp Directory

Level-1 Directory	Level-2 Directory
audit	-
bios_files	-
rmedia	Rpipe
_cmdline.txt	-
_cpuinfo.txt	-
_date.txt	-
_devices.txt	-
_ifconfig.txt	-
_interfaces.txt	-
_interrupts.txt	-
_iomem.txt	-
_ioports.txt	-
_loadavg.txt	-
_mctpapp.txt	-
_meminfo.txt	-
_modules.txt	-
_mounts.txt	-
_netstat.txt	-
_ps-elf.txt	-
_ps-elL.txt	-
_route.txt	-
_softirqs.txt	-

Level-1 Directory	Level-2 Directory
_stat.txt	-
_top.txt	-
_upname.txt	-
_uptime.txt	-
auto_video_record_status	-

The files contain information about CPU, memory, operating process, network, account and important system services.

2.3 Mnt Directory

The Mnt directory stores key system logs which are not lost in case of power supply failure. For the Mnt directory structure, refer to Table 2-3.

Table 2-3 Mnt Directory

Level-1 Directory	Level-2 Directory	Level-3 Directory	Level-4 Directory	Level-5 Directory
nandflash0	a.txt	–		
	bootimage.ini	–		
	exclude.txt	–		
	OEM	bmc_customcfg	log	bmc_oem_config.log
		log	bios_oem_config.log	–
			bmc_oem_config.log	–
	sftp_upload	–		
	snmpdengineboots.conf	–		
	tmp.txt	–		
nandflash1	BiosConf	bioscfg_current.xml	–	–
		bioscfg.xml	–	–
	BlackBox	BIOS_LOG	–	–
	log	audit.log	–	–
		bios_asset.log	–	–
		cron_dbg.log	–	–
		execdaemon.log	–	–

Level-1 Directory	Level-2 Directory	Level-3 Directory	Level-4 Directory	Level-5 Directory
		execdaemon.log.1	–	–
		fanctl.log	–	–
		hbLed.log	–	–
		http.log	–	–
		kcs_log.bak	–	–
		keepalive.log	–	–
		kern.log	–	–
		lifecycle.log	–	–
		lighttpd.log	–	–
		lighttpd.log.1	–	-
		mcExc.log	–	-
		mcReset.log	–	–
		me.log	–	–
		nand_mount_check.log	–	–
		netconf.log	–	–
		operation.log	–	–
		partfault.log	–	–
		pem.log	–	–
		procmonitor.log	–	–
		rest.log	–	–
		startup.log	–	–
		system.log	–	–
		trace.log	–	–
		update.log	–	–
		up.log	–	–
		wdt.log	–	–

An operation log is used as an example to describe the log format.

```
2021-04-07T17:44:39.980937+08:00 [BoardSN:]: root, WEB, 192.168.5.10, set snmp
trap community name(public) successfully.
```

A log is composed of two parts:

- **Part 1**: time when the log is recorded. The format is time + time zone, which is the same for all logs.
- **Part 2**: content of the log. It is determined as required.

Important logs under this directory are described as follows:

audit.log

Log format:

```
2022-04-07T17:19:16.411038+08:00 [BoardSN:]: HTTPS login from IP: 192.168.5.10
user: root successfully.
```

This log records the login mode (HTTPS, that is, through a web browser), IP address (*192.168.5.10*), account (root) and operation result (successfully).

The audit.log file records the information about the logins to the BMC through SERIAL, SSH or HTTPS.

For any incorrect operations, you can first find the login information about the operator in accordance with the login log.

operation.log

Log format:

```
2022-04-07T17:24:35.930803+08:00 [BoardSN:]: root, WEB, 192.168.5.10, enable
power limit alarm successfully.
```

This log records the login mode (Web), account (root), IP address (*192.168.5.10*) and specific operation (enable power limit alarm successfully).

The operation.log file records all BMC settings. Query operations are not recorded. If the configuration of the BMC is changed, you need to check the operation log and login log to see whether the operation is proper.

system.log

Log format:

```
2021-04-07T17:24:38.700803+08:00 [BoardSN:]: Major(30776) 2021-04-07 17:24:38
System power is more than threshold. Deasserted.
```

This log records the alarm severity (Major), time when the alarm was generated (2021-04-07 17:24:38), alarm content (System power is more than threshold) and alarm status (Deasserted).

The system.log file records alarms or notifications generated during the operation of the server. An administrator can determine whether the server is faulty in accordance with the system log.

kern.log

Log format:

```
2022-01-01T08:00:33.790000+08:00 [35.450000] Helper Module Driver Version 1.2.
```

This log records the print and output of system kernel information, including the driver information and kernel errors.
You can check the kernel log when the system is not operating properly. Key kernel printings are recorded to help locate the fault.

mcReset.log

Log format:

```
2022-04-02 15:20:19 [2213] : ResetStatus[SCU3C] is 00000008(HEX), last reset type is RebootCommand-WDT#2.
```

This log records the status value (00000008) of the SCU3C register and the cause of the last BMC reset (RebootCommand).
Common reset causes include the server power loss (PowerOnReset), BMC watchdog reset (WatchDogTimeOut), BMC controller pin reset (EXTERN-PIN), and the reboot through the command line (RebootCommand).
The mcReset.log file is used to determine the cause of the last BMC reset.

wdt.log

Log format:

```
2022-03-31T15:17:55.963917+08:00 [SetWDT 696]set watchdog timer, timer use: FRB2, initial countdown value: 9000count(100ms/count).
```

This log records the set watchdog timer (FRB2) and watchdog timeout (9000count). The types of watchdog timers include FRB2, POST, OSload and OS.
The wdt.log file records the operating status of the watchdog timer and the kicking conditions. The watchdog log is used to recover from the system hang.

keepalive.log

Log format:

```
2022-06-28T21:16:07.220000+08:00 Failed to create IPMI Session wRet(0x3) 0 times!!!
```

This log records the failure to connect to the IPMI and the BMC reset or process.

The keepalive.log records the keepalive settings in the BMC system, including the IPMIMain, lighttpd and MCTP keepalive settings.

If the system is not operating properly, you can check the keepalive log.

mcExc.log

Log format:

```
********** Begin of BMC Exc Record **********
Record Time:2031-06-28 21:16:06
PID: 2195 (IPMIMain) is terminating because of SIG !!!!!
TaskId: 2514 (RecvUDSPkt) Segmentation fault
Signal :11(SIGSEGV),signal code:1,error address:0xb7666d8
Function Calling Trace:
/usr/local/lib/libunix.so.2(+0x9298)[0xb5f45298]
/lib/arm-linux-gnueabi/libc.so.6(__default_rt_sa_restorer_v2+0x0)[0xb5a03db0]
/usr/local/lib/libipmilocal.so.3.18.0(RecvUDSPkt+0x264)[0xb47b3638]
Exception Registers:
R0:0x0000000e, R1:0x5b30002e, R2:0x5b30002e, R3: 0x02daaf17
R4:0x0040249e, R5:0x001066d4, R6:0x00000002, R7: 0x000baa78
R8:0x0011aa78, R9:0x00000001, R10:0x00009b48, FP: 0x00046f48
IP:0x00000000, SP:0xac4efca0, LR :0x0b7666d4, PC: 0xb47b3638, CPSR:0x20000010
```

This log records the time when the failure occurred (Record Time:2031-06-28 21:16:06), abnormal PID and signal type, incorrect address, invocation chain, and address mapping information.

The **mcExc.log** log records the logout failure occurring when the BMC process receives abnormal signals. You can locate the failure in accordance with the recorded process information.

Other Logs

In addition to the above logs, there are other logs:

- **log/pem.log**: PSU log.
- **Log/rest.log**: Web request log.
- **log/hbLed.log**: BMC heartbeat indicator log.
- **BiosConf/bioscfg.xml**: configuration files of the current BIOS.
- **BlackBox/BIOS_LOG**: log recording hardware failures detected by the BIOS.

2.4 Var Directory

The Var directory stores key system logs. They are lost in case of power supply failure. Therefore, you must back up the logs before restarting the system to recover from a failure.

For the Var directory structure, refer to Table 2-4.

Table 2-4 Var Directory

Level-1 Directory	Level-2 Directory
log	adviser.log
	alarm.log
	authpriv.log
	btmp
	crit.log
	cron.log
	daemon.log
	debug
	debug.log
	dmesg
	emerg.log
	info.log
	info.log.1
	messages
	oemsys.log
	redfish.log
	redfish-rest.log
	redfish-rest.log.1
	redis-server.log
	slpd.log
	storage.log
	storage.log.1
	syslog
	warning.log
	wtmp

adviser.log

Log format:

```
2021-08-01 21:39:17.070000 [3013.3013] : Enter register adviserd process!
```

This log records the KVM application, which contains the time (2021-08-01 21:39:17.07000) and content (Enter register adviser process!). You can check this log to solve KVM failures.

alarm.log

Log format:

```
2021-04-07T17:24:39.040803+08:00 alarm11 PerformActionAlert 3:RetVal=0x0
```

This log records the handling process of the BMC system alarm (alarm11). When an alarm fault occurs (for example, an alarm is not reported), you can check this log to see whether the system alarm is reported and analyze the log if so.

crit.log/info.log/emerg.log/warning.log

Log format:

```
2021-04-08T10:12:08.840818+08:00[2213:2585CRITICAL][vantageo_nic.c:6334]NIC_GetPowerGoodState.
```

This log records operation errors of BMC function modules. It contains the time, the line number of the error code (vantageo_nic.c:6334), and failure cause. These logs are for developers to locate the error code that results in the abnormal operation of the BMC service modules.

dmesg

Log format:

```
[3047262.341377] nfsd: last server has exited, flushing export cache
```

This log is a system kernel log, which is similar to the kernel log. You do not need to pay attention to this type of logs.

storage.log

Log format:

```
2021-04-08T10:19:26.700894+08:00  StoragePrepare:host  offline
```

This log records the operation status of the storage module, which contains the time and content (StoragePrepare:host offline). It can be used to locate storage failures.

Chapter 3
BMC User Rights

Table of Contents

The BMC provides different rights for the following three type of users:

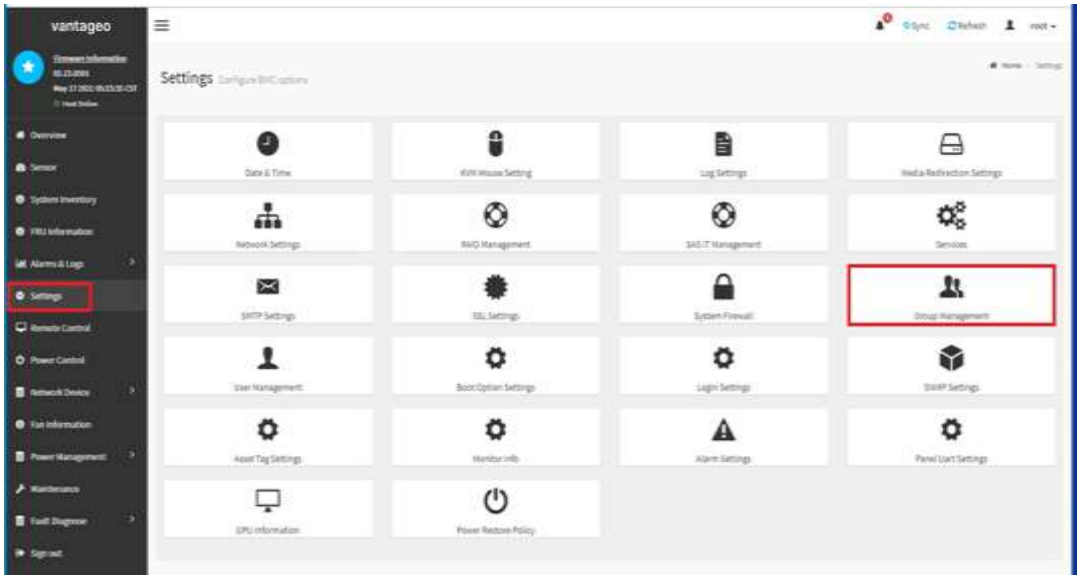
- **Administrator**: can use all the functions provided by the BMC.
- **Operator**: can use parts of functions provided by the BMC.
- **Viewer**: can only query the information on the BMC Web portal.

3.1 Right Configuration on the Web Portal

The BMC provides the group management configuration. You can configure the rights by creating a group.

1. Log in to the BMC Web portal. Select **Settings** from the menu bar in the left pane. The **Settings** page is displayed, see Figure 3-1.

Figure 3-1 Settings Page



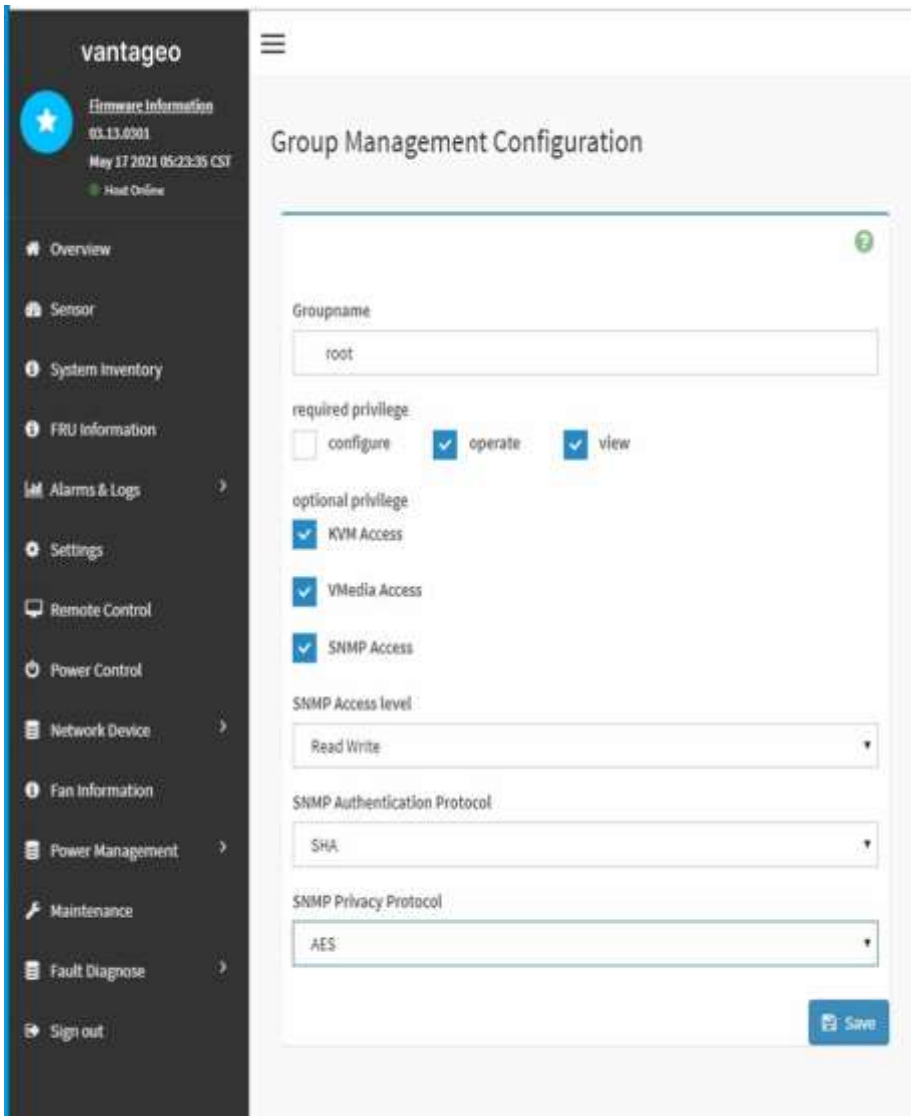
2. In the right pane, select **Group Management**.

3. The first three are default groups, corresponding to the administrator, operator and viewer, and the others are groups that are not configured, see Figure 3-2. Select a group that is not configured.

Figure 3-2 Group Management Page

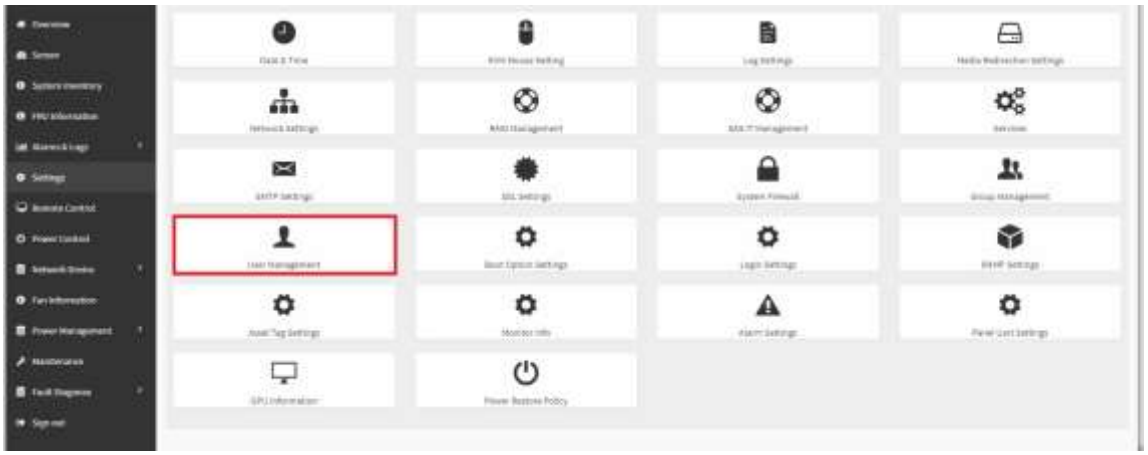
4. Set the parameters on the **Group Management Configuration** page, see Figure 3-3.

Figure 3-3 Group Management Configuration Page



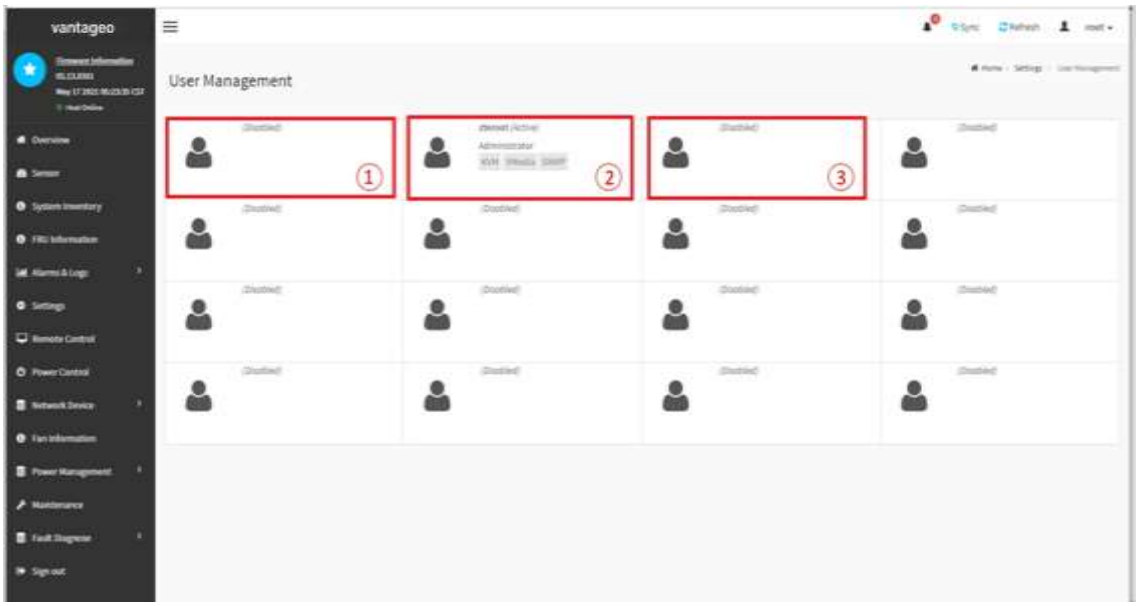
5. After the group is configured, go back to the **Settings** page. Select **User Management** in the right pane, see Figure 3-4.

Figure 3-4 Settings Page



6. On the **User Management** page, the first user is the default system user, the second user is the factory default root administrator, and the others are users that are not configured, see Figure 3-5. Select a user that is not configured.

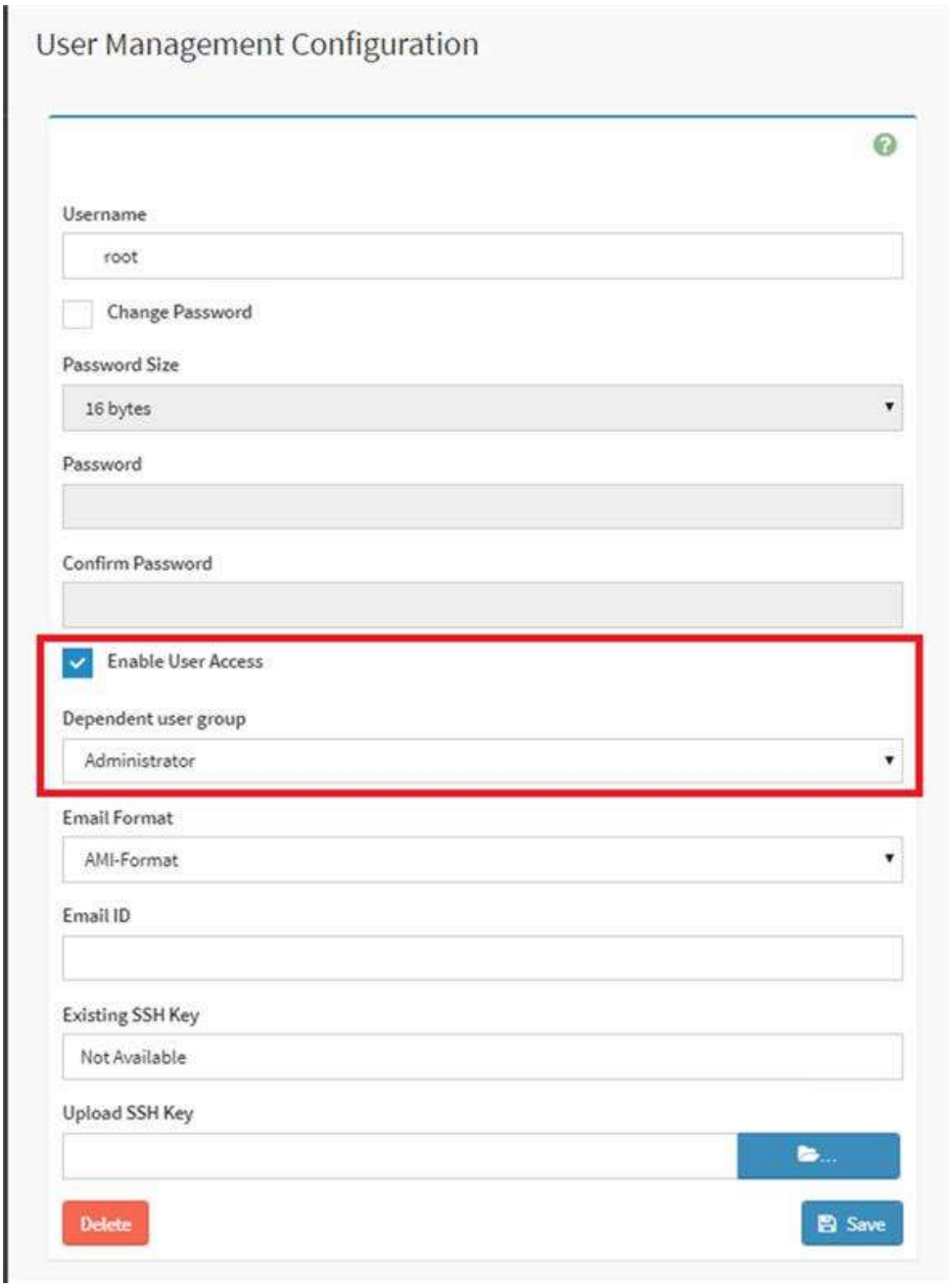
Figure 3-5 User Management Page



1. Default system user that cannot be configured.
2. Factory default administrator root.
3. User that can be configured.

7. Set the user information as required. The rights of a user are restricted by the rights of the group that the user belongs to.

Figure 3-6 User Management Configuration Page



3.2 Right Configuration Through the IPMI Commands

You can configure only IPMI-related rights for the administrator, operator and viewer through the IPMI commands. Optional rights on the Web interface including SNMP, KVM and VMedia access cannot be configured through the IPMI commands.

The commands are as follows:

```
ipmitool -I lanplus -H IP -U USER -P PASSWD user set name CHANNEL user_name
ipmitool -I lanplus -H IP -U USER -P PASSWD user set password CHANNEL user_passwd
ipmitool -I lanplus -H IP -U USER -P PASSWD user priv CHANNEL AUTH
ipmitool -I lanplus -H IP -U USER -P PASSWD user enable CHANNEL
ipmitool -I lan -H IP -U USER -P PASSWD channel setaccess 1 CHANNEL callin=on ipmi=on link=on privilege=AUTH
ipmitool -I lan -H IP -U USER -P PASSWD channel setaccess 2 CHANNEL callin=on ipmi=on link=on privilege=AUTH
```

AUTH indicates user rights:

- Administrator rights
- Operator rights
- Viewer rights

CHANNEL is the user ID ranging from 1 to 16.

Glossary

BIOS

- Basic Input/Output System

BMC

- Baseboard Management Controller

BMC

- Baseboard Management Controller

CPU

- Central Processing Unit

HTTPS

- Hypertext Transfer Protocol Secure

IPMI

- Intelligent Platform Management Interface

KVM

- Keyboard, Video and Mouse

MCTP

- Management Component Transport Protocol

OEM

- Original Equipment Manufacturer

OS

- Operating System

PC

- Personal Computer

PID

- Process Identifier

PSU

- Power Supply Unit

SFTP

- Secure File Transfer Protocol

SNMP

- Simple Network Management Protocol

SSH

- Secure Shell

UID

- User Identifier