



VANTAGEO Server

Log Reference (BMC V4)

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

Copyright 2024 VANTAGEO PRIVATE LIMITED.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of VANTAGEO PRIVATE LIMITED is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of VANTAGEO PRIVATE LIMITED or of their respective owners.

This document is provided as is, and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. VANTAGEO PRIVATE LIMITED and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

VANTAGEO PRIVATE LIMITED or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between VANTAGEO PRIVATE LIMITED and its licensee, the user of this document shall not acquire any license to the subject matter herein.

VANTAGEO PRIVATE LIMITED reserves the right to upgrade or make technical change to this product without further notice.

Users may visit the VANTAGEO technical support website <https://www.vantageo.com/support> to inquire for related information.

The ultimate right to interpret this product resides in VANTAGEO PRIVATE LIMITED.

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 | 2023-07-31 | First edition. |

Serial Number: VT20240305

Publishing Date: 2023-07-31 (R1.0)

Contents

| | |
|---|-----------|
| 1.BMC Diagnosis File Export | 5 |
| 1.1 Exporting a BMC Diagnosis File Through the Web Portal | 5 |
| 1.2 Exporting Logs Through the CLI (SSH) | 6 |
| 1.3 Exporting Logs Through the CLI (Serial Port) | 7 |
| 2.BMC Log Export by Category | 8 |
| 2.1 Exporting User-Related Logs..... | 8 |
| 2.2 Exporting System Logs..... | 9 |
| 3.BMC Log Parsing | 11 |
| 3.1 tmp Directory..... | 13 |
| 3.2 data Directory | 14 |
| 3.3 var Directory..... | 19 |
| 4.Reference: Configuration File Parsing | 21 |
| 4.1 conf Directory..... | 21 |
| 4.1 firmdata Directory | 21 |
| Glossary | 22 |

About This Manual

Purpose

This manual describes the procedures for exporting and parsing the log files of VANTAGEO servers.

Intended Audience

This manual is intended for:

- Commissioning engineers
- Maintenance engineers


What Is in This Manual

This manual contains the following chapters.

| | |
|--|--|
| Chapter 1, BMC Diagnosis File Export | Describes how to export a BMC diagnosis file in one click. |
| Chapter 2, BMC Log Export by Category | Describes how to export BMC logs by category. |
| Chapter 3, BMC Log Parsing | Describes the directory structures and content of BMC logs. |
| Chapter 4, Reference: Configuration File Parsing | Describes the directory structures and content of the configuration files. |

Conventions

This manual uses the following convention.

| | |
|---|--|
|  | Note: provides additional information about a topic. |
|---|--|

Chapter 1

BMC Diagnosis File Export

Table of Contents

| | |
|--|---|
| Exporting a BMC Diagnosis File Through the Web Portal..... | 5 |
| Exporting Logs Through the CLI (SSH)..... | 6 |
| Exporting Logs Through the CLI (Serial Port)..... | 7 |

To obtain **BMC** logs, you need to export a BMC diagnosis file. The BMC diagnosis file is compressed in `.tar.gz` format, and consists of BMC configuration files and BMC log files.

1.1 Exporting a BMC Diagnosis File Through the Web Portal

Abstract

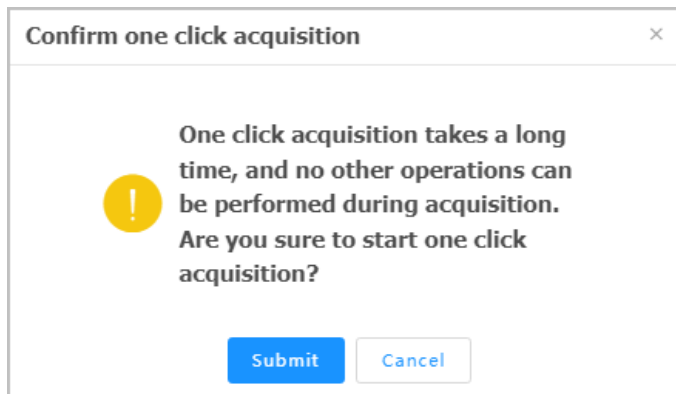
The Web portal of the **BMC** allows you to export a BMC diagnosis file in one click. The exported file is named `bmcinfo_<product serial number>.tar.gz`, and stored in the default download directory of the browser.

Note

If the product serial number is not programmed, the file name is `bmcinfo_UnknownProductSN.tar.gz`.

Steps

1. Launch the Google Chrome browser on the **PC**, and enter the address of the Web portal of the **BMC**.
2. Log in to the Web portal of the **BMC**. The **Homepage** is displayed.
3. In the **Shortcuts** area, click **One-Click Collection**. The **Confirm one click acquisition** dialog box is displayed, see [Figure 1-1](#).

Figure 1-1 Confirm One Click Acquisition Dialog Box

4. Click **Submit**.

Note

During the collection process, all Web interfaces of the BMC cannot be operated. If you close the browser by mistake, log in to the BMC Web portal again. The **One click acquisition is being processed, please try again later** message is displayed. Wait for about five minutes before re-collecting logs.

1.2 Exporting Logs Through the CLI (SSH)

Abstract

If the Web portal of the [BMC](#) fails, you can log in to the BMC through [SSH](#) and export logs in one click through the [CLI](#).

Steps

1. Connect to the BMC by using an SSH tool.
2. Run the following commands in the CLI to export logs:

```
# cd /etc/init.d/  
# ./export_bmcdata.sh
```

Note

After the logs are exported, they are stored in the `/var/bmcdata/bmcinfo_.tar.gz` directory.

3. Download the log file to the local PC through [SFTP](#).
4. (Optional) Run the following commands in the CLI to delete the BMC log file:

```
# cd /var/bmcdata  
# rm bmcinfo_.tar.gz
```

1.3 Exporting Logs Through the CLI (Serial Port)

Abstract

If the [BMC](#) cannot be accessed due to a network error, you can export logs in one click through the serial port.

Steps

1. Connect the serial port of the BMC to a debugging PC by using an audio serial port cable.
2. Press and hold the [UID](#) button on the server panel for six seconds until the indicator flashes blue.
3. Use the serial port tool on the debugging PC to connect to the serial port of the BMC.
4. Log in to the serial port with the corresponding username and password.
5. Run the following commands in the CLI to export logs:

```
# cd /etc/init.d/  
# ./export_bmcdata.sh
```

Note

After the logs are exported, they are stored in the `/var/bmcdata/bmcinfo_.tar.gz` directory.

6. Run the following command to back up the log file to the `/data` directory:

```
# cp /var/video/bmcinfo_.tar.gz /data/
```

Note

After the network is recovered, you can download the log file to the local PC through [SFTP](#).

Chapter 2

BMC Log Export by Category

Table of Contents

| | |
|----------------------------------|---|
| Exporting User-Related Logs..... | 8 |
| Exporting System Logs..... | 9 |

2.1 Exporting User-Related Logs

Abstract

The user-related logs in the [BMC](#) include:

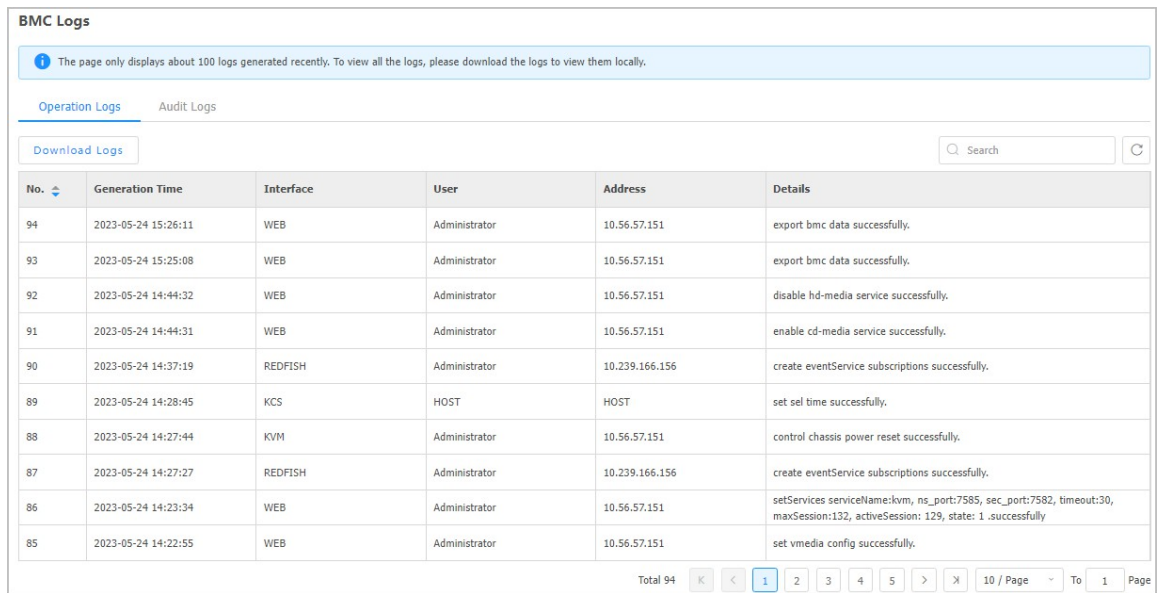
- **Operation Logs:** record user operations.
- **Audit Logs:** record user logins and logouts.

This procedure uses how to export operation logs as an example to describe how to export user-related logs.


Steps

1. From the menu bar on the Web portal of the BMC, select **Maintenance > BMC Logs**. The **BMC Logs** page is displayed, see [Figure 2-1](#).

Figure 2-1 BMC Logs Page—Operation Logs Tab



2. Click **Download Logs**. An operation log file is downloaded to the local PC.
The name of the log file contains the log type and date (year/month/day/hour/minute/second), for example, *operate_log_20221029110815.log*.
3. (Optional) Perform the following operations as needed.

| To... | Do... |
|------------------------|--|
| Filter logs by keyword | In the Search box, enter a keyword. |
| Refresh logs | Click  . The latest logs are displayed on the page. |

2.2 Exporting System Logs

Abstract

The system logs in the **BMC** include:

- **Current Alarms:** record the active alarms of the server.
- **System Events:** record the events that occur during the operation of the server.

This procedure uses exporting active alarms as an example to describe how to export system logs.

Steps

1. From the menu bar on the Web portal of the BMC, select **Maintenance > Alarm & Event**.
The **Alarm & Event** page is displayed, see [Figure 2-2](#).

Figure 2-2 Alarm & Event Page—Current Alarms Tab

| Alarm & Event | | | | | | | | |
|-----------------|----------|---|---|---------------------|-------------|----------|----------------|-------------------------|
| Current Alarms | | System Events | | | | | | |
| Download Alarms | | Total: 4 ● 2 ● 1 ● 1 | | | Search | | Advanced Query | |
| No. | Severity | Alarm Name | Description | Generation Time | Object Type | Position | Event Code | Handling Suggestions |
| 4 | Critical | Hard disk RAID array is offline | Raid Card(RM243B(Embedded1)) logical driver(id:1, name:54645) is offline assert. | 2023-05-24 22:16:56 | Disk | LD_1 | 0x1a000083 | Details |
| 3 | Major | Hard disk is missing | Disk19 is missing(SN:unknown). | 2023-05-23 16:48:55 | Disk | DISK_19 | 0x1a000016 | Details |
| 2 | Critical | Hard disk RAID array is offline | Raid Card(RM243B(Embedded1)) logical driver(id:0, name:osredhat75) is offline assert. | 2023-05-23 16:38:36 | Disk | LD_0 | 0x1a000083 | Details |
| 1 | Minor | Redundancy Lost | PS_Redundant Redundancy Lost assert. | 2023-05-23 16:37:18 | PSU | PSU_0 | 0x0a0b0801 | Details |

Total 4 1 / Page To 1 Page

2. Click **Download Alarms**. An active alarm file is downloaded to the local PC.

Note

The name of the alarm file contains the alarm type and date (year/month/day/hour/minute/second), for example, *alarminfo_20221029201628.csv*.

3. (Optional) Perform the following operations as needed.

| To... | Do... |
|---|---|
| Filter alarms by keyword | In the Search box, enter a keyword. |
| Query alarms based on the advanced parameters | <ul style="list-style-type: none"> a. Click Advanced Query. Advanced query conditions are displayed. b. Set the query parameters. c. Click Query. d. (Optional) If the selected query conditions are incorrect, click Reset, and re-execute Step b through Step c. |
| View the handling suggestions for an alarm | Click Details for the alarm. |
| Refresh alarms | Click . The latest alarms are displayed on the page. |

Chapter 3

BMC Log Parsing

Table of Contents

| | |
|----------------------|----|
| tmp Directory | 13 |
| data Directory | 14 |
| var Directory..... | 19 |

A **BMC** diagnosis file consists of BMC configuration files and BMC log files.

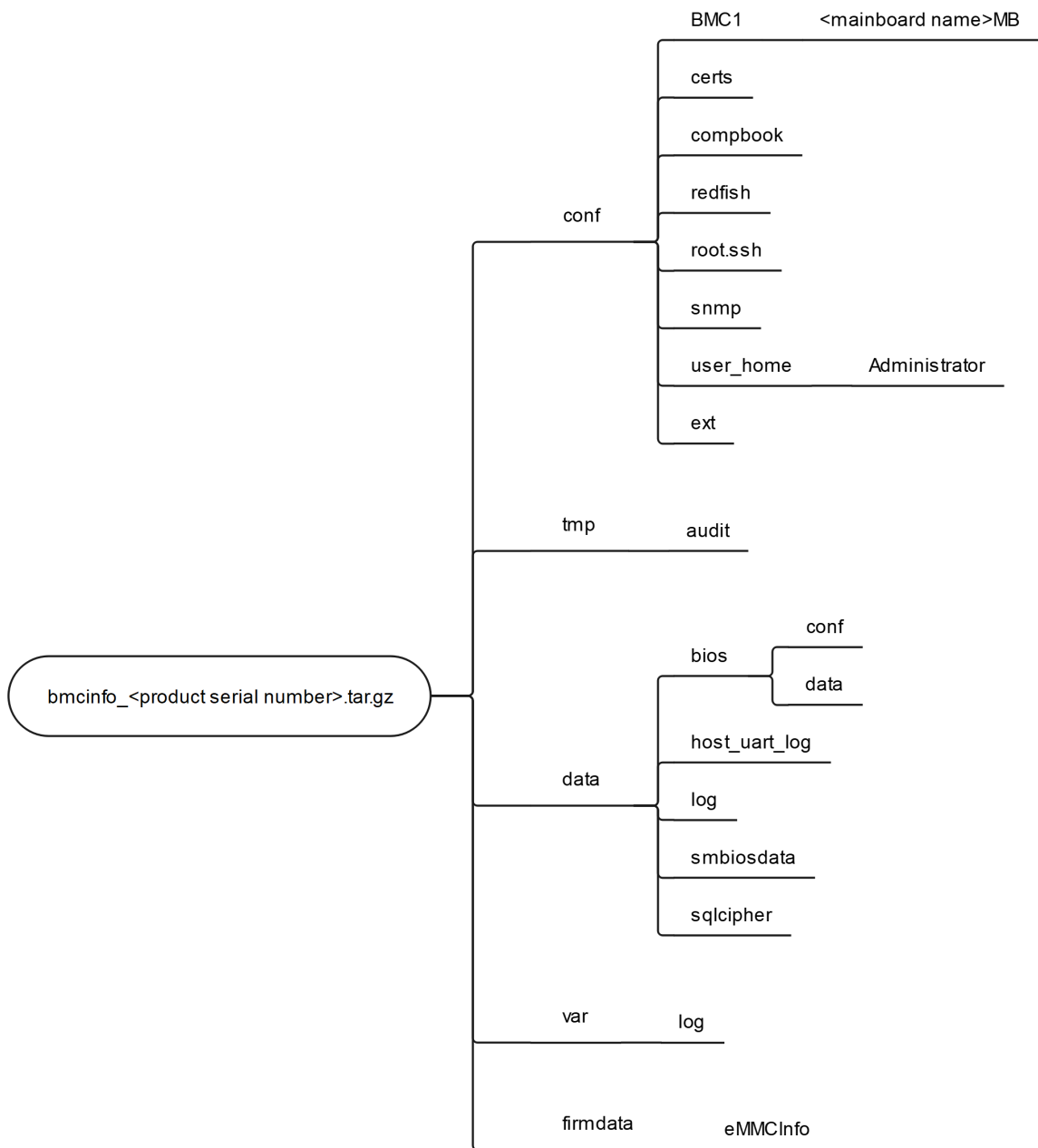
When you export a diagnosis file in one-click mode to obtain logs, the exported diagnosis file is compressed into `.tar.gz` format and the file name is `bmcinfo.tar.gz`.

After the diagnosis file is decompressed, there are five directories:

- **conf**: directory of BCM configuration files.
- **tmp**: directory of BMC status logs, which record the operational status of the BMC when the logs are downloaded.
- **data**: directory of the logs in the BMC NAND flash partitions, which record key system information and are not lost when the server is powered off.
- **var**: directory of BMC system logs, which record function failures and are lost when the server is powered off.
- **firmdata**: directory of customized configuration files and eMMC partition configuration information, which are not lost when the server is powered off.

[Figure 3-1](#) shows the directory structure of the diagnosis file.

Figure 3-1 Diagnosis File Directory Structure



This chapter focuses on the parsing of BMC logs in the *tmp*, *data*, and *var* directories. For the parsing of configuration files, refer to [4 Reference: Configuration File Parsing](#).

Note

Logs are regularly backed up and rotated to avoid large log file size and save storage space. The backup interval is 6 minutes, the maximum size of a log file is 1 M, and the backup file is named *.1.

3.1 tmp Directory

The current operational status information about the BMC is stored in the *tmp* directory. For the structure of the *tmp* directory, refer to [Table 3-1](#).

Table 3-1 tmp Directory

| Level-1 Directory | Level-2 Directory |
|--------------------------|-------------------|
| audit | - |
| _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 | - |
| _stat.txt | - |
| _top.txt | - |
| _uname.txt | - |
| _uptime.txt | - |
| auto_video_record_status | - |

The file content consists of the **CPU** information, memory information, currently running process information, network information, account information, and system-related important service information.

3.2 data Directory

Directory Structure

The *data* directory stores key system logs. After the server is powered off, the logs in the *data* directory are not lost. For the structure of the *data* directory, refer to [Table 3-2](#).

Table 3-2 data Directory

| Level-1 Directory | Level-2 Directory | Level-3 Directory |
|-------------------|--|-------------------|
| bios | conf | Files |
| | | static |
| | data | - |
| host_uart_log | HostSerial- Port_01_20221128_21_39_50 | - |
| | HostSerial- Port_02_20221128_21_39_50 | - |
| | HostSerial- Port_03_20221128_21_39_50 | - |
| | HostSerial- Port_04_20221128_21_39_50 | - |
| | HostSerial- Port_05_20221128_21_39_50 | - |
| log | audit.log | - |
| | cron_dbg.log | - |
| | current_check_code.log | - |
| | customdiskslot.log | - |
| | epld.log | - |
| | event.log | - |
| | execdaemon.log | - |
| | fanctl.log | - |
| | faultdiagcpu.log | - |
| | faultdiagmemory.log | - |

| Level-1 Directory | Level-2 Directory | Level-3 Directory |
|-------------------|-------------------------|-------------------|
| | faultdiagtool.log | - |
| | historyCode.log | - |
| | hostpwrcctl.log | - |
| | keepalive.log | - |
| | kern.log | - |
| | mcExc.log | - |
| | mcpmonitor.log | - |
| | mcReset.log | - |
| | me.log | - |
| | operate.log | - |
| | pciedev.log | - |
| | pcieid.log | - |
| | pem.log | - |
| | previous_check_code.log | - |
| | procmonitor.log | - |
| | rasdata.log | - |
| | reboot.log | - |
| | redfish-error.log | - |
| | redfish-hi.log | - |
| | redfish-rest.log | - |
| | rest.log | - |
| | rsvmem.log | - |
| | selevent.log | - |
| | startup.log | - |
| | storage.log | - |
| | system.log | - |
| | trace.log | - |
| | update.log | - |
| | variableinfo.log | - |

| Level-1 Directory | Level-2 Directory | Level-3 Directory |
|-------------------|-------------------------|-------------------|
| | watchdog_dump.log | - |
| | wdt.log | - |
| smbiosdata | smbios.log | - |
| sqlcipher | alarminfo.csv | - |
| | bmc_event.db | - |
| | bmc_event_bak.db | - |
| | power.db | - |
| | privilege_management.db | - |

The following uses an operation log as an example to parse the log format:

```
2022-11-28 21:14:46 [BoardSN:7022abcdefgh]: Administrator, WEB, 192.168.5.111,
begin upgrade FRU successfully.
```

The log consists of two parts:

- Part 1: recording time. The time format for all logs is the same.
- Part 2: log content, depending on the actual requirements.

The important files in this directory are parsed below.

audit.log

The *audit.log* file records logins to the BMC in any way, including through the serial port, [SSH](#), and [HTTPS](#).

The log format is as follows:

```
2022-11-30 04:56:12 [BoardSN:7022abcdefgh]: sysadmin, N/A, 192.168.5.111, login
over SSHD successfully.
```

The log content consists of the login mode ([HTTPS](#), namely Web), [IP](#) address (192.168.5.111), account information (sysadmin), and operation success or failure record (successfully).

If an operation error occurs in the system, you can locate the operator's login information in accordance with the login logs first.

operate.log

The *operate.log* file records all the configuration operations (query operations excluded) on the BMC.

The log format is as follows:


```
2022-11-28 21:14:46 [BoardSN:7022abcdefgh]: Administrator, WEB, 192.168.5.111,
begin upgrade FRU successfully.
```

The log content consists of the operation mode (Web), account (Administrator), IP address (192.168.5.111), and specific operation content (begin upgrade FRU successfully).

If configuration is changed in the BMC, you need to determine whether the operation is proper in accordance with the operation logs and login logs.

system.log

The *system.log* file records BMC-related alarms or notifications. You can determine whether the BMC is operating properly in accordance with system logs.

The log format is as follows:

```
2022-11-29 02:51:04 [BoardSN:7022abcdefgh]: Level: Major, EntityType: CPU, De-
scription: CPU_PVNN_MAIN_01 CPU Voltage (0.000 Volts) Lower Critical - Going Low
(0.802 Volts) assert, Occurtime: 2022-11-29 02:51:04, Status: Assert, Location:
CPU_1, EventCode: 0x3010202, EventName: Below lower major threshold.
```

The log content consists of alarm-related fields and their descriptions, for example, alarm level (Level: Major), alarm description (Description: CPU_PVNN_MAIN_01 CPU Voltage (0.000 Volts) Lower Critical - Going Low (0.802 Volts) assert), and alarm time (Occurtime: 2022-11-29 02:51:04).

kern.log

The *kern.log* file records key information about the system kernel.

The log format is as follows:

```
2022-11-29 02:51:04 [35.450000] Helper Module Driver Version 1.2.
```

The log content consists of the driver information and kernel errors.

In most cases, you need to check this log file for locating faults.

mcReset.log

The *mcReset.log* file records the BMC reset information.

The log format is as follows:

```
Sat Jan 1 00:00:01 UTC 2000 0x00013030 TIPS: bit24/27-WDT3(Start), bit20/23-WDT2
(Run), bit16/19-WDT1(reboot), bit1-EXTRST, bit0-PWRON.
```

The log content consists of the status value (0x00013030) of the SCU3C register and the cause (RebootCause) of the last BMC reset.

The log is used to determine the cause of the last BMC reset for locating the BMC reboot fault. Common reset causes include server power loss (PowerOnReset), CLI-based reboot (RebootCommand), BMC watchdog reset (WatchDogTimeOut), and BMC pin-based reset (EXTERNAL-PIN).

wdt.log

The *wdt.log* file records the operating status and reset status of the timer to recover the BMC from a fault.

The log format is as follows:

```
2022-11-29 02:47:30 [PlatResetTask 225] Here is going to process FRB2 watchdog.
```

The log content consists of the watchdog timer type (FRB2) and timeout period. The types of watchdog timers include FRB2, POST, OSload, and OS.

keepalive.log

The *keepalive.log* file records the keepalive information about the BMC.

The log format is as follows:

```
2022-11-29 02:47:30 Failed to create IPMI Session wRet(0x3) 0 times!!!
```

The log content consists of the [IPMI](#) connection failure and IPMI process reset records, for example, IPMIMain, lighttpd, and [MCTP](#) keepalive.

You need to check this log file when the system status is abnormal.

mcExc.log

The *mcExc.log* file records the fault indicating that the environment process receives a signal error and thus exits.

The log format is as follows:

```
***** 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
```

The log content consists of the fault occurrence time (Record Time:2031-06-2821:16:06), [PID](#) s of abnormal processes, type of abnormal signal, abnormal address, and invocation chain and address mapping information.

The process-related information recorded in this log file helps to locate faults.

Other Logs

In addition to the above logs, the *data* directory also contains the following logs:

- log/pem.log: [PSU](#) logs.
- log/rest.log: Web request logs.
- log/selevent.log: system event logs.
- log/watchdog_dump.log: BMC watchdog-related dump information, used for locating faults.
- log/faultdiag*.log: server fault diagnosis logs.

3.3 var Directory

Directory Structure

The *var* directory stores key system logs, which are lost when the server is powered off. If a failure occurs, you need to back up logs before restarting the server for recovery.

For the structure of the *var* directory, refer to [Table 3-3](#).

Table 3-3 var Directory

| Level-1 Directory | Level-2 Directory |
|-------------------|-------------------|
| log | adviser.log |
| | authpriv.log |
| | btmptmp |
| | crit.log |
| | cron.log |
| | daemon.log |
| | debug |
| | debug.log |
| | dmesg |
| | info.log |
| | kcs.log |
| | messages |

| Level-1 Directory | Level-2 Directory |
|-------------------|---------------------|
| | oemsys.log |
| | redis-server.log |
| | redis-server.log |
| | rmcp_message |
| | rsvmem.log |
| | storage.log |
| | syslog |
| | tally.log |
| | warning.log |
| | wtmp |
| | vantageonetwork.log |

The important files in this directory are parsed below.

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

The *crit.log*, *info.log*, *emerg.log*, and *warning.log* files record the operational errors of each function module of the BMC.

The log format is as follows:

```
2022-11-30 05:05:46 [2246 : 2248 CRITICAL][peminfo.c:444]PMBus read query failed!
```

The log content consists of the time, failure code line number (peminfo.c:444), and failure cause, helping to locate the code that leads to operational errors of BMC functions.

dmesg

Like the *kern.log* file, the *dmesg* file also records system kernel information, which does not need to be checked.

The log format is as follows:

```
[80.686001] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready.
```

storage.log

The *storage.log* file records the operational status of the storage module.

The log format is as follows:

```
2022-11-29 02:51:15 pmc_oob_precondition: power status is changed(form 1 to 0,1:power on,else:power off).
```

The log content consists of the time and specific log information (power status is changed(form 1 to 0,1:power on,else:power off) for locating storage errors.

Chapter 4

Reference: Configuration File Parsing

Table of Contents

| | |
|-------------------------|----|
| conf Directory..... | 21 |
| firmdata Directory..... | 21 |

4.1 conf Directory

The *conf* directory stores **BMC** configuration files. For the structure of the *conf* directory, refer to [Table 4-1](#).

Table 4-1 conf Directory

| Level-1 Directory | Level-2 Directory |
|-------------------|--------------------|
| BMC1 | <Mainboard name>MB |
| certs | – |
| compbook | – |
| redfish | – |
| root.ssh | – |
| snmp | – |
| user_home | Administrator |
| ext | – |

The *conf* root directory and the *BMC1* subdirectory store BMC configuration files.

The *ext* directory stores the **OEM** configuration files.



Note

To avoid operational errors, you must not modify these configuration files casually.

4.1 firmdata Directory

The *firmdata* directory stores the eMMCInfo files, which are used to record **eMMC** partitioning process information for analysis by **R&D** engineers.

Glossary

BMC

- Baseboard Management Controller

CLI

- Command Line Interface

CPU

- Central Processing Unit

HTTPS

- Hypertext Transfer Protocol Secure

IP

- Internet Protocol

IPMI

- Intelligent Platform Management Interface

MCTP

- Management Component Transport Protocol

OEM

- Original Equipment Manufacturer

PC

- Personal Computer

PID

- Process Identifier

PSU

- Power Supply Unit

R&D

- Research and Development

SFTP

- Secure File Transfer Protocol

SSH

- Secure Shell

UID

- Unit Identification Light

eMMC

- Embedded Multimedia Card