

VANTAGEO Server

BMC User Guide (BMC V4)

Version: R1.3

VANTAGEO PRIVATE LIMITED Corporate Address: 617, Lodha Supremus II, Road No. 22, Wagle Estate, Thane - 400604 URL: https://vantageo.com E-mail: <u>support@vantageo.com</u> 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 <u>https://www.vantageo.com/support</u> 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
R1.3	2024-11-07	Fully updated.
R1.2	2024-07-01	Fully updated.
R1.1	2024-04-24	Fully updated.
R1.0	2023-09-07	First edition.

Serial Number: VT20240301

Publishing Date: 2024-11-07 (R1.3)

Contents

1 BMC Overview. 1.1 Operating Principle	9 9
1.2 Functions	11
1.3 Software Security	12
1.4 Operation Interfaces	15
2 Performing Client Commissioning	16
3 Logging in to the Web Portal of the BMC	21
4 Common Operations	19
4.1 Logging In to the BMC Through SSH	27
4.2 Logging In to the BMC Through a Serial Port	
4.3 Modifying the BMC Address	33
4.4 Checking Server Information	34
4.5 Managing Storage Devices	
4.6 Installing an OS Remotely	
4.7 Resetting the BMC When the Web Portal Is Unavailable	44
4.8 Querying and Configuring Services	45
4.9 Configuring an NTP Server	47
4.10 Configuring an SMTP Server	49
4.11 Configuring Trap Notification Parameters	50
4.12 BMC Log Export	52
4.12.1 Exporting Logs in One Click Through the Web Portal	53
4.12.2 Logs by Category Through the Web Portal	54
4.12.3 Exporting Logs Through the CLI (SSH)	55
4.12.3 Exporting Logs Through the CLI (Serial port)	55
4.13 Upgrading the BMC Firmware	56
4.14 Restoring Factory Defaults	57
4.15 Backing Up BMC Configurations	58
4.16Creating an SNMP User	59
5 System Management	63
5.1 Querying System Information	63
5.2 Querying Performance Data	64
5.4 Configuring the Heat Dissipation Policy	67

5.6 Managing Storage Devices	
5.8 Powering On/Off the Server	74
5.9 Configuring the Server Startup Policy	77
5.10 Configuring Power-On Delay Parameters	78
5.11 Configuring the High-Temperature Power-Off Strategy	79
5.12 Querying Power Supply Information	81
5.13 Configuring the Power Mode	82
5.14 Querying Power Statistics	84
5.15 Configuring Power Control Parameters	85
5.16 Querying Power KPIs	86
5.17 Configuring Boot Options	87
5.18 Configuring the Serial Port output Mode	89
6 Diagnosis and Maintenance	91
6.1 Querying Alarms	91
6.2 Alarm Reporting Parameter Configuration	92
6.2.1 Configuring Trap Notification Parameters	93
6.2.2 Configuring Syslog Notification Parameters	95
6.2.3 Configuring Email Notification Parameters	97
6.3 Configuring Screen Recording Parameters	99
6.3 Configuring Screen Recording Parameters 6.4 Viewing Recorded Videos	99 101
6.3 Configuring Screen Recording Parameters6.4 Viewing Recorded Videos6.5 Taking a Screenshot	99 101 102
6.3 Configuring Screen Recording Parameters6.4 Viewing Recorded Videos6.5 Taking a Screenshot6.6 Viewing POST Codes	99 101 102 103
 6.3 Configuring Screen Recording Parameters 6.4 Viewing Recorded Videos 6.5 Taking a Screenshot 6.6 Viewing POST Codes 6.7 Downloading Server Logs 	99 101 102 103 104
 6.3 Configuring Screen Recording Parameters 6.4 Viewing Recorded Videos 6.5 Taking a Screenshot 6.6 Viewing POST Codes 6.7 Downloading Server Logs 6.8 Querying BMC Logs 	99 101 102 103 104 105
 6.3 Configuring Screen Recording Parameters 6.4 Viewing Recorded Videos 6.5 Taking a Screenshot 6.6 Viewing POST Codes 6.7 Downloading Server Logs 6.8 Querying BMC Logs 6.9 Querying SEL Logs	
 6.3 Configuring Screen Recording Parameters	
 6.3 Configuring Screen Recording Parameters	
 6.3 Configuring Screen Recording Parameters	
 6.3 Configuring Screen Recording Parameters. 6.4 Viewing Recorded Videos. 6.5 Taking a Screenshot. 6.6 Viewing POST Codes. 6.7 Downloading Server Logs. 6.7 Downloading Server Logs. 6.8 Querying BMC Logs. 6.9 Querying SEL Logs. 6.10 Querying Memory Health Scores. 7 Service Management. 7.1 Configuring Port Service Parameters. 7.2 Configuring Web Service Parameters. 	
 6.3 Configuring Screen Recording Parameters	
 6.3 Configuring Screen Recording Parameters. 6.4 Viewing Recorded Videos. 6.5 Taking a Screenshot. 6.6 Viewing POST Codes. 6.7 Downloading Server Logs. 6.8 Querying BMC Logs. 6.9 Querying SEL Logs. 6.10 Querying Memory Health Scores. 7 Service Management. 7.1 Configuring Port Service Parameters. 7.2 Configuring Web Service Parameters. 7.3 Configuring KVM Service Parameters. 7.4 Starting the KVM. 	
 6.3 Configuring Screen Recording Parameters	
 6.3 Configuring Screen Recording Parameters	
 6.3 Configuring Screen Recording Parameters. 6.4 Viewing Recorded Videos. 6.5 Taking a Screenshot. 6.6 Viewing POST Codes. 6.7 Downloading Server Logs. 6.7 Downloading Server Logs. 6.8 Querying BMC Logs. 6.9 Querying SEL Logs. 6.10 Querying Memory Health Scores. 7 Service Management. 7.1 Configuring Port Service Parameters. 7.2 Configuring Web Service Parameters. 7.3 Configuring KVM Service Parameters. 7.4 Starting the KVM. 7.5 Configuring Virtual Media Parameters. 7.6 Mounting a Virtual Media Device. 7.7 Configuring VNC Parameters. 	

8 BMC Management	130
8.1 Network Parameter Configuration	130
8.1.1 Configuring the Host Name	130
8.1.2 Configuring the Network Port Mode	131
8.1.3 Configuring IP Addresses of Network Ports	133
8.1.4 Configuring the DNS	135
8.1.5 Configuring an iSAC VLAN	137
8.1.6 Configuring an NCSI VLAN	138
8.1.7 Configuring USB over LAN	139
8.2 Setting the Time of the BMC	140
8.3 Resetting the BMC on the Web Portal of the BMC	144
8.4 Upgrading Firmware	145
8.5 Switching Modes	147
8.6 Updating BMC Configurations	148
8.7 Restoring Factory Defaults	150
9 User and Security	151
9.1 Adding a Local User	151
9.2 Configuring Authentication Parameters for Domain Users	154
9.3 Querying Online Users	158
9.4 Configuring Permissions for a Customized Role	159
9.5 Configuring Security Enhancement Parameters	160
9.6 Configuring Firewall Parameters	161
9.7 Configuring Two-Factor Authentication	163
10 Reference: Default Passwords	165
11 Reference: Accessing Documents	
Glossary	169

About This Manual

Purpose

This manual describes the BMC management software of VANTAGEO servers to provide guidance on BMC configuration and management.

Intended Audience

This manual is intended for:

- Network planning engineers
- Configuration engineers
- Maintenance engineers

What Is in This Manual

This manual contains the following chapters.

Chapter 1, BMC Overview	Describes the operating principle and functions of the BMC, software security and operation interfaces.
Chapter 2, Performing Client Commissioning	Describes the debugging operations on the BMC Web portal logged in through a client.
Chapter 3, Logging In to the Web Portal of the BMC	Describes how to log in to the Web portal of the BMC.
Chapter 4, Common Operations	Describes common operations in the BMC.
Chapter 5, System Management	Describes how to perform system management operations.
Chapter 6, Diagnosis and Maintenance	Describes how to perform diagnosis and maintenance operations.
Chapter 7, Service Management	Describes how to perform service management operations.
Chapter 8, BMC Management	Describes how to perform BMC management operations.
Chapter 9, User and Security	Describes how to perform user and security management operations.
Chapter 10, Reference: Default Passwords	Describes the default passwords that are used to log in to the BMCs in VANTAGEO servers of different models.

Chapter 11, Reference: Accessing Documents

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.
Note: provides additional information about a topic.

Chapter 1 BMC Overview

Table of Contents

Operating Principle	9
Functions	11
Software Security	12
Operation Interfaces	15

The BMC is the management system of a VANTAGEO server, which monitors and manages server hardware, and provides a Web portal for operation and maintenance, achieving the purposes of software and hardware configuration, fault diagnosis, operating system installation, and operations on the server.

1.1 Operating Principle

The BMC consists of a dedicated management chip and the management software operating on the chip.

• Dedicated management chip

The server-dedicated management chip provides abundant hardware interfaces and functions. For the hardware interfaces of the BMC, see Figure 1-1.



For a description of the BMC channels, refer to Table 1-1.

Table 1-1 BMC Hardware Channel Descriptions

Channel	Typical Physical Link	Typical Management Object or Function
Service peripheral supervision channel	PCle and SMBUS	PCIe devices of a server
Host internal supervision channel	SMBUS and PECI	Internal functional units of the CPU or bridge chip
Host interaction channel	PCIe, USB, LPC, KCS, and SM- BUS	Supports KVM, virtual media function, and host serial port functions, and the IP- MI protocol
Direct supervision channel for service peripherals	SMBUS and NC-SI	PCIe devices of a server
Sensor supervision channel	SMBUS, GPIO, and A/D	Temperature sensor, voltage sensor, current sensor, and presence sensor
Fan supervision channel	PWM	Fan
Power supervision channel	SMBUS	CRPS, and PMBUS power supply
Control channel	GPIO and SGPIO	Power-on, power-off, and indicator on/off
Remote management channel	Ethernet	Accesses the BMC management server

Management software

The BMC management software communicates with hardware devices through the management channels to monitor and manage hardware. For the architecture of the BMC management software, see Figure 1-2.



1.2 Functions

The BMC is a the management system of a server. It provides abundant management functions.

- Server health status management: Checks the operational status of a server, analyzes historical data and actual monitoring data, and helps users to find and solve problems in advance, ensuring the highly reliable operation of the server.
 - → The 80-code recording function provides sufficient information for analyzing startup failures.
 - → When the system crashes, the last-screen capture function records the on-site scenario for analyzing system crashes.
 - → Screen snapshots and screen recording on preventive maintenance and operation processes facilitate follow-up audits.
 - → The alarm function supports precise fault diagnosis based on components, facilitating component fault locating and replacement.
 - \rightarrow The CrashDump function facilitates further analysis of system errors.
 - → The BMC supports the syslog, SNMP trap, email and Redfish subscription functions to report alarms, so that the NMS can collect server fault information easily.
 - → The BMC supports direct display of the server health status through the alarm indicator.
- Host system maintenance
 - → Supports virtual KVM and virtual media functions for remote maintenance of the host system.

- → Supports out-of-band monitoring and management of RAIDs, so that RAIDs can be monitored without depending on the host system, and the storage devices in the host system can be configured, which improves configuration efficiency and management capability.
- → Supports OS installation through PXE, which improves the efficiency of remote installation of operating systems in batches.
- Device firmware management → Dual BMCs are supported to ensure the reliable operation. → Dual BIOSs are supported to improve the reliability of BIOS upgrade and operation.
 - \rightarrow The firmware (for example, the FRU and EPLD) upgrade function is supported.
- System cooling → Monitors the temperature of important components on the server, and performs different cooling controls based on different hardware thermal characteristics.
 - → Supports the over-temperature power-off function to ensure that the server hardware is not damaged, extending the service life of components.
- Intelligent power consumption management → The BMC supports the power capping technology, and provides the standard DCMI for centralized control by the NMS, improving the deployment density of servers.
 - \rightarrow Energy-saving design reduces the operating costs of a server.
- BMC self-management
 - → Supports synchronizing the BMC time through the network and the host, meeting the requirements in different scenarios.
 - → Supports multiple authentication modes, which simplifies server management.
 - → Supports DHCP and DNS, which simplifies server deployment and management.
- Diversified management interfaces

The BMC meets the requirements of various system integration interfaces by providing the following:

→ Standard DCMI1.5/IPMI2.0/Redfish interfaces → Remote command line interfaces and Web management interfaces → SNMPv1, SNMPv2 and SNMPv3 interfaces

1.3 Software Security

Security Measures for Function Invocation

- Complete security design: Uses threat modeling for security design.
- Encrypted KVM access: Supports encrypted KVM access.

HTTPS access with a high encryption security level: Provides an HTTPS trusted path between the server and users to protect local or remote users when they log in to the system through the Web page and prevent communication data from being modified or leaked.

- SSH access with a high encryption security level: Provides an SSH trusted path between the server and users, and between servers and other devices to protect local or remote users when they log in to the system and prevent communication data from being modified or leaked.
- SNMPv3 protocol with a high encryption security level: Supports the SNMPv3 communication security protocol, SHA, and AES.
- IPMI 2.0 protocol with a high encryption security level: Supports the IPMI 2.0 communication protocol, and provides the encryption security technology with a higher level.
- Redfish interface with a high encryption security level: Supports the next-generation standard shelf management interface, with the encryption level higher than the IPMI protocol.
- Protocol and port anti-attack: Disables unused network services and high-risk ports as well as insecure protocols by default, including RMCP, Telnet.

Security Measures for User Permissions

- User role management: User permissions are allocated to logged-in users, and multiple management user roles can be allocated. Roles can be divided into different levels. By associating roles, the functional permissions of each user can be restricted to prevent unauthorized operations.
- User account security enhancement: Weak password detection, default strong password, password complexity configuration, password validity period configuration, and forbidding repeated use of the latest three historical passwords during password modification are supported.
- Authentication service: The BMC supports both local authentication access and remote authentication access. Remote access supports authentication through LDAP, and account locking upon login authentication failures. The number of login failures can be configured.
- User access restriction: User access can be restricted by port, source IP address, and MAC whitelist. The system supports the functions such as maximum number of sessions, forced exit after session timeout, configurable session expiration, multi-session concurrent restriction for a single user, online user management, and forced logout.
- Intrusion alarm: The BMC supports the chassis cover opening alarm to improve system security.
- Certificate service: The BMC supports certificate encryption and import services, which can only be operated by the administrator.

Security Measures for Log Management

- Log recording: All key system events can be recorded, including the date, time, user, event description, event result, and other related information. The BMC supports recording of component replacement logs.
- Log category: The BMC supports different log categories, including operation logs, maintenance logs, and login logs.
- Log query: The BMC provides log information query permissions for authorized users, and supports allocating log file read permissions by account to prevent log files from being accessed illegally.
- Log protection: Logs are saved in non-volatile storage media. Log information that has been stored cannot be deleted without authorization to prevent modifying the stored log information. Logs are saved for 90 days or longer.
- Centralized alarm management: The BMC supports centralized alarm management for the faults that occur during device operation, allows authorized users to export alarms, and supports alarm reporting through SNMP Trap in a centralized manner.
- Centralized log management: The BMC allows authorized users to export logs, and supports log through Syslog in a centralized manner.
- Reliable timestamp: The BMC supports local time modification and NTP to ensure the time accuracy of system logs and alarms.

Security Measures for Data Security

- Encrypted data storage: Supports data protection, encrypted data storage, and database password authentication.
- Encrypted data transmission: Supports communication protocols with high encryption security levels such as IPMI 2.0/SNMP V3/SSH/Redfish/HTTPS and the KVM encryption function to ensure data transmission security.
- Data integrity: Supports data integrity check to ensure data verification, storage and transmission.

Security Measures for Version Management

- Version integrity check: When the server system loads software, the BMC checks the integrity of the software to prevent version confusion or malicious modification caused by error codes during transmission.
- Software upgrade permission control: The BMC records software version and firmware version information. Only the administrator has the permission to upgrade software and firmware and record related operations in logs.

Version rollback: When an error occurs during the version upgrade process, the version can be rolled back.

- Venerability-free release of software: Before the product software is released, it passes the security scan by the security tools such as NSFOCUS, NESSUS, and WebInspect, and passes the source code scan for vulnerabilities. In addition, the product software passes several rounds of penetration tests to ensure no vulnerability.
- Redundancy: The BMC supports active/standby BMC boots, BMC versions and BMC management ports.
- Strict version release control process: The BMC supports security evaluation of the thirdparty software and plug-ins used. Before a version is released, the BMC scans it by using mainstream anti-virus software. SHA256 check codes are released to prevent version tempering.
- Secure and controllable BMC source code: The BMC source code passes the 100% code walkthrough and the Klocwork and Coverity white box security checks and tests, so that the potential security vulnerabilities are eliminated and the security is reinforced.

1.4 Operation Interfaces

The BMC supports common batch deployment operation interfaces and server management interfaces.

- The batch deployment operation interfaces include:
 - → The IPMI is a standard server interface. It is used for interconnection with the upper-layer NMS or the monitoring software at the host side to implement the functions specified by the IPMI2.0.
 - → The Redfish interface is a standard server interface. It is used for interconnection with the upper-layer NMS to monitor and manage a server.
 - → The SNMP interface is a non-standard server interface. It is used for interconnection with the upper-layer NMS to monitor and manage a server.
- The server management interfaces include:
 - → Web interface → KVM interface → Remote CLI

Chapter 2 Performing Client Commissioning

Abstract

In most cases, you can log in to the Web portal of the BMC on a client through the iSAC management network port of a server. Before logging in to the Web portal of the BMC for the first time, you need to commission the client to ensure that it is interconnected with the iSAC management network port.

Prerequisite

- All the needed tools are ready:
 - \rightarrow A PC (acting as the client)
 - → Network cable
- One of the following browsers is already installed on the PC:
 - → Google Chrome 59 or later versions
 - → Firefox 54 or later versions
 - → Microsoft IE 11 or later versions



Google Chrome 59 and later versions are recommended.

Context

The default IP address of the iSAC management network port of a server is 192.168.5.7. Figure 2-1 shows the position of the iSAC management network port on the rear panel of the server.



Figure 2-1 Position of the iSAC Management Network Port

1. iSAC management network port

Note

The network port with the **iSAC** silk screen on the rear panel of a server identifies the iSAC management network port. The locations of the iSAC management network interfaces on different servers are slightly different. This procedure uses an 2230-RE server as an example to describe the position of the iSAC management network port. For other servers, refer to the corresponding Hardware Description.

Steps

- 1. Connect the PC to the iSAC management network port on the rear panel of the server through a network cable.
- 2. On the PC, change the IP address of the PC to an IP address (for example, 192.168.5.8) in the same network segment as 192.168.5.7.
- 3. On the PC, launch the specified browser.
- 4. In the address bar of the browser, enter *https://192.168.5.7* and press Enter. The page for login is displayed, see Figure 2-2.



Figure 2-2 Login Page

If the prompt information as shown in Figure 2-3 is displayed before login, click **Advanced** and select **Proceed to** enter the login page.

Figure 2-3 Security Prompt

Your connection is not private
Attackers might be trying to steal your information from 192.168.5.7 (for example, passwords, messages, or credit cards). <u>Learn more</u>
Q To get Chrome's highest level of security, <u>turn on enhanced protection</u>
Advanced Back to safety

5. Enter your username and password.



The default username and password are as follows:

- Username: Administrator
- Password: Superuser9!

To unhide the password, you can click the 🔊 button on the right.



After you log in to the BMC Web portal by using the default password, you must change the default password immediately. It is recommended that you change the default password to a strong password.

6. Click Log In, The Homepage of the Web portal of the BMC is displayed, see Figure 2-4.

Figuro 2-4 Homonago

S VANTAGEO-BM¢	Homepage	System	Maintenance	Services	BMC Settings	User &	Security		₩ ` `	ຽ~ ∉	🖲 English 🗸	× ۸
Device Name 22	40-RE		Device Informa	tion				Short	cuts			
			Product Serial Num:	219000000000	Host Na	me:	ISAC98F0BCA45AF3					
			BMC Version:	04.24.02.00 (Feb	26 Running	Time:	143 days, 19 hrs	(Er	Firmwar	re (Log	
_		_	BIOS Version:	01.23.04.00 (Dec	27 Chip Info	ormation:	AST2600		y opgraa	· · ·		
		1	GUID:	30e72400-0000-1	00 Manufac	turer:	VANTAGEO					
HISTORICH	ON ON		IPv4 Address:	192.168.5.7	MAC Ad	dress:	98:F0:BC:A4:5A:F3	Œ	Network	k (Powe	r
			IPv6 Address:	N/A								
Alarm Statistics			Asset Tag: 🕐	219000000000				(2)	One-Cli	ck		
0 1	0								Collectio	on		
Critical 🔕 Major	Ø Minor Ø	Details										
Device List												
CPU	Memory		Stora	ige Card		Network	Adapter	Power			Fan	
Total 2 Present 2	Pre Ca	tal 3 esent 2 pacity 6400		Storage Card Logical Drive Physical Drive	2 2 12	N N	etwork Card 1 etwork Port 2	Ø	Total Present	2	P	otal 4 Present 4
System Monitoring									Virtual	Console	Operate	- Setting
21°C Air Inlet Temp									T Not re	the KVM previous commended to pro-	w is not enable enable both Ky view Preview	d. VM and

7. Set the IP address of the iSAC management network port as planned, for example, 10.235.51.202.



For how to set the IP address of the iSAC management network port, refer to 8.1.3 Configuring IP Addresses of Network Ports.

- 8. Record the IP address of the iSAC management network port.
- 9. Connect the iSAC management network port to the corresponding switch through a network cable.
- 10.On the PC, change the IP address of the PC to an IP address (for example, 10.235.51.203) in the same network segment that the iSAC management network port belongs to.
- 11.Connect the PC to the corresponding switch through a network cable, so that the PC and the iSAC management network port are in the same LAN.
- 12.Run the ping command on the CLI of the PC to make sure that the PC can communicate with the iSAC management network port properly.

Chapter 3 Logging In to the Web Portal of the BMC

Abstract

This procedure describes how to log in to the Web portal of the BMC of a server through the specified browser on your PC. You can monitor and manage the server on the portal.

Prerequisite

The IP address of the iSAC management network port is already obtained.

Steps

1. In the address bar of the browser, enter the address of the Web portal of the BMC, and press **Enter**. The page for login is displayed, see Figure 3-1.

Figure 3-1 Login Page





The address format of the Web portal of the BMC is as follows: https://IP. "IP" is the IP address of the iSAC management network port.

If the prompt information as shown in Figure 3-2 is displayed before login, click **Advanced** and select **Proceed to** to enter the login page.

Figure 3-2 Security Prompt

O To get Chror	ne's highest leve	el of security, <u>tu</u>	n on enhanced pr	otection
ET::ERR_CERT_AUTHO	RITY_INVALID			
ttackers might be t asswords, message	trying to steal yo es, or credit card	our information s). <u>Learn more</u>	from 10.235.51.2	02(for example,
our connec	tion is not	private		



- Username: Administrator
- Password: Superuser9!

To unhide the password, you can click the 🔯 button on the right.



2

After you log in to the BMC Web portal by using the default password, you must change the default password immediately. It is recommended that you change the default password to a strong password.

3 Click Log In, The Homepage of the Web portal of the BMC is displayed, see Figure 3-3.

Figure 3-3 Homepage

vice Name 2240-RE	Device Information		
m Statistics 0 1 0 Critical • Major • Minor • De	Product Serial Num: 219000000000 BMC Version: 04.24.02.00 (Feb 26 BIOS Version: 01.23.04.00 (Dec 27 GUID: 30e72400-0000-100 IP-4 Address: IP-6 Address: N/A Asset Tagl: ① 219000000000	Host Name: ISAC99F08CA45AF3 Running Time: 143 days, 19 hrs Chip Information: AST2600 Manufacturer: VANTAGEO MAC Address: 98F0.BC5A4:5AF3	Firmware B Log Upgrade D Power Image: Solution of the content
Total 2 Present 2 Total Capacity	Storage Card 32 20 640G Storage Card 2 Logical Drive 2 Physical Drive 12	Network Adapter Wetwork Card 1 Network Port 2	Power Fan Total 2 Present 2 Total 4 Present 4
em Monitoring			Virtual Console Operate - Settings

For a description of the **Homepage**, refer to Table 3-1.

Table 3-1	Homepage	Descr	iptions

No.	Name	Description
1	Device Information	 Displays the detailed information and active alarm statistics of the server. To modify the asset flag of the server, click To view alarm details, click Details.
2	Menu bar	Displays all the function menus in the format of a navigation tree in the left pane after you click any main menu on the menu bar.
3	Alarm button	 Displays the total number of active alarms. To view the number of alarms at each level, hover the mouse pointer over this button. To view alarm details, click this button.
4	UID button	 Displays the UID indicator status of the server. To change the status of the UID indicator, click this button and select the corresponding shortcut menu. The shortcut menus include: Steady on: The UID indicator is lit, helping you to identify the current server among the servers in the equipment room.

No.	Name	Description	
		• Blink: The UID indicator flashes, indicating that the BMC is being operated.	
		The UID indicator flashes automatically when the BMC, Web portal, KVM, or	
		virtual media is being used.	
		• Off: The UID indicator is off.	
		The grayed shortcut menu indicates the current status of the UID indicator. For example, if the Blink shortcut menu is grayed, the UID indicator of the server is flashing.	
5	Power button	Displays the power status of the server.	
		To change the power status, click this button and select the corresponding	
		shortcut menu.	
		The shortcut menus include:	
		• Power On : Power on the server.	
		• Normal Power Off: Power off the server.	
		• Forced Power Off: Forcibly power off the server.	
		• Power Reset : Perform a warm reboot.	
		Warm reboot means that the server is restarted when it is not shut down.	
		During the restart, the server is not offline.	
		• Power Cycle: Perform a cold reboot.	
		Cold reboot means that the server is started after it is shut down. During the	
		restart, the server is offline.	
		The grayed shortcut menu indicates the current power status of the server. For example, if the Power On shortcut menu is grayed, the server is in power-on status.	
6	Language button	Displays the current language of the Web portal of the BMC.	
		To change the language, click this button.	
7	Current user	Displays the currently logged-in user	
		 To view the details of the currently logged in user, including the IP address 	
		and login time, click this button.	
		 To log out the currently logged-in user, click this button and then click Log Out in the detailed information box displayed. 	
8	Shortcuts	Displays the shortcut operation buttons on the Web portal of the BMC, including:	
		• Firmware Upgrade: upgrades firmware. For details, refer to 8.4 Upgrading	
		Firmware.	
		• Log: queries BMC logs. For details, refer to 6.8 Querying BMC Logs.	
		• Network: configures network parameters. For details, refer to 8.1 Network	
		Parameter Configuration.	
		• Power : queries server power-on/off information, and power supply and power consumption information. For details, refer to 5.8 Powering On/Off the Server and 5.15 Configuring Power Control Parameters.	

No.	Name	Description	
		• One-Click Collection : collects all configuration files, databases, and logs for fault location, packages them, and downloads them to the PC. It takes a long time to collect the required information, and no other operations can be performed during the collection period.	
9	Device List	Displays the components in the server by category.	
		To view the details of components of a category, click the category.	
10	Virtual Console	Displays the operations related to the virtual console, including:	
		• To enable KVM preview in the Virtual Console area, click Open Preview.	
		• To disable KVM preview in the Virtual Console area, click Close Preview.	
		• To start the virtual console in HTML mode, click Operate and then select	
		Start HTML Virtual Console from the shortcut menu.	
		• To start the virtual console in Java mode, click Operate and then select Start	
		Java Virtual Console from the shortcut menu.	
		• To reset the virtual console, click Operate and then select Reset Virtual	
		Console from the shortcut menu.	
		Click Settings.	
11	System Monitoring	Displays system monitoring information.	

Chapter 4 Common Operations

Table of Contents

Logging In to the BMC Through SSH2	27
Logging In to the BMC Through a Serial Port2	29
Modifying the BMC Address	33
Checking Server Information	34
Managing Storage Devices	36
Installing an OS Remotely	38
Resetting the BMC When the Web Portal Is Unavailable4	4
Querying and Configuring Services	15
Configuring an NTP Server4	17
Configuring an SMTP Server4	9
Configuring Trap Notification Parameters	50
BMC Log Export	52
Upgrading the BMC Firmware	56
Restoring Factory Defaults	57
Backing Up BMC Configurations	58
Creating an SNMP User	59

4.1 Logging In to the BMC Through SSH

Abstract

This procedure describes how to log in to the BMC through SSH to configure the BMC.

Prerequisite

The PC is already installed with SSH software, for example, PuTTY.



The operations for different SSH software are similar. This procedure uses the PuTTY software as an example.

Steps

1. On the PC, start the *PuTTY* software. The **PuTTY Configuration** window is displayed, see Figure 4-1.

Basic options for your PuT	TY session
Specify the destination you want to o Host Name (or IP address)	Port
Connection type:	SSH OSerial
Load, save or delete a stored session Saved Sessions	n]
Default Settings	Load
	Save
	Delete
Close window on exit: Always Never Only	on clean exit
	Basic options for your PuT Specify the destination you want to of Host Name (or IP address) 10. Connection type: Raw O Telnet O Rlogin (Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: Always O Never O Only

Figure 4-1 PuTTY Configuration Window

2. Set the parameters. For a description of the parameters, refer to Table 4-1.

Table 4-1 PuTTY Configuration Parameter Descriptions

Parameter	Setting
Category	Select Session .
Host Name (or IP address)	Enter the IP address of the iSAC management network port or shared network port.

Port	Enter 22.
Parameter	Setting
Connection type	Select SSH .

- 3. Click **Open**. The CLI is displayed.
- 4. Enter the username and password of the administrator.

Note

The default administrator username is *sysadmin*. The default administrator password depends on server models and BMC versions. For details, refer to 10 Reference: Default Passwords.

5. Press Enter to log in to the BMC.

4.2 Logging in to the BMC Through a Serial Port

Abstract

When neither the iSAC management network port nor the shared network port is available for accessing the BMC, you can log in to the BMC through a serial port to configure the BMC.

Prerequisite

The PC is already installed with SSH software, for example, PuTTY.



The operations for different SSH software are similar. This procedure uses the *PuTTY* software as an example.

- If the PC needs to convert a USB port into a serial port, the corresponding driver must be installed.
- A serial cable is available.

Steps

- 1. Connect the PC to the serial port on the rear panel of the server through a serial cable.
 - Connect the PC to the audio serial port on the rear panel of a G5 server, as shown in Figure 4-2.



Figure 4-2 Position of the Audio Serial Port

The port with the server identifies the audio serial port. This procedure uses an 2230-RE server as an example to describe the position of the serial port.

 Connect the PC to the USB serial port on the rear panel of a G6 server, as shown in Figure 4-3.



1. USB Serial Port



The port with the server silk screen on the rear panel of the server identifies the USB serial port. This procedure uses an R5300 G6 server as an example to describe the position of the serial port.

2. Press and hold the UID button on the front panel of the server for six seconds. The serial port is switched to the BMC serial port commissioning mode.

For the position of the UID button on the front panel, refer to Figure 4-4.

Figure 4-4 Position of the UID Button



1. UID button



The button with the **UID** silk screen on the front panel of a server is the UID button. This procedure uses an 2230-RE server as an example to describe the position of the UID button.

- 3. In the **Device Manager** window on the PC, check the serial port connected with the serial cable.
- 4. On the PC, start the *PuTTY* software. The **PuTTY Configuration** window is displayed, see Figure 4-5.

tegory:		
- Session	Basic options for your PuTT	Y session
Logging ⊒- Terminal Keyboard Rall	Specify the destination you want to constrain the Serial line	onnect to Speed 115200
Features ⊒ Window	Connection type:	SSH
Appearance Behaviour Translation Selection	Load, save or delete a stored session Saved Sessions	
Colours	Default Settings	Load
Data		Save
 Proxy Telnet Rlogin SSH Serial 		Delete
	Close window on exit: Always Never Only	on clean exit

Figure 4-5 PuTTY Configuration Window

5. Set the parameters. For a description of the parameters, refer to Table 4-2.

Table 4-2 PuTTY Configuration Parameter Descriptions

Parameter	Setting
Category	Select Session .
Serial line	Enter the serial port obtained in Step 3.
Speed	Enter 115200.
Connection type	Select Serial .

- 6. Click **Open**. The CLI is displayed.
- 7. Enter the username and password of the administrator.

vantageo



The default administrator username is *sysadmin*. The default administrator password depends on server models and BMC versions. For details, refer to 10 Reference: Default Passwords.

8. Press Enter to log in to the BMC.

4.3 Modifying the BMC Address

Abstract

To replan the IP address of the iSAC management network port or shared network port of the server, you need to modify the address of the BMC.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see Figure 4-6.

work Protocols				
Select Network Port	O Dedicated Port	Shared Port		
Network Protocols	🗹 IPv4 💟 IPv6			
Settings	IPv4		IPv6	
	Acquisition method	O Manually set IP address	Acquisition method	O Manually set IP address
		Automatically obtain IP address		• Automatically obtain IP address
	Address	10.239.227.66	Address	
	Mask	255.255.255.0	Prefix Length	0
	Default Gateway	10.239.227.1	Default Gateway	
	MAC Address	D4:2A:24:5E:AF:51	Link Local Address	fe80::d62a:24ff:fe5e:af51

3. Set the parameters in the **Network Protocols** area. For a description of the parameters, refer to Table 4-3.

Parameter	Setting
Select Network Port	This parameter can be set only if Select Mode is set to Alone in the Network Port area
	Select the network port for which you want to configure an IP address.
	 Dedicated Port: configures the IP address of the iSAC management network port.
Parameter	Setting
	• Shared Port: configures the IP address of the shared network port.
Network Protocols	Select the network protocol(s) for the network port.
	• The IPv4 settings need to be configured if you select IPv4 only.
	• The IPv6 settings need to be configured if you select IPv6 only.
	 Both IPv4 settings and IPv6 settings need to be configured if you select IPv4 and IPv6.
Acquisition method	Select the method of obtaining the IP address.
	The parameters below do not need to be configured if Acquisition method is set to Automatically obtain IP address .
Address Enter the address of the BMC as planned.	
Mask	Enter the mask.
Default Gateway	Enter the IP address of the default gateway.

Table 4-3 Network Protocol Parameter Descriptions

4. Click Save.

4.4 Checking Server Information

Abstract

Before reporting a fault or replacing hardware, you must check the server information, including:

- Serial number
- CPU
- Memory
- NIC
- Slot that a GPU is located



For the 2230-RE 4-GPU model, the operations of removing and installing a GPU are complicated. Before removing and installing the GPU, you need to query the ID of the slot where the GPU is located to ensure that the operations are correct.

Steps

1. On the **Homepage**, check the serial number of the server, see Figure 4-7.

Figure 4-7 Homepage

S vantageo-bm¢	Homepage System	n Maintenance	Services BMC	Settings User 8	& Security	😴 😌		\oplus English \checkmark \land
Device Name 22	40-RE	Device Informat	tion			Shortcuts	;	
Alarm Statistics 0 1	0	Product Serial Num: 2 BMC Version: 0 BIOS Version: 0 GUID: 5 IPv4 Address: 1 IPv6 Address: 1 Asset Tag: ① 2	2190000000 04.24.02.00 (Feb 26 01.23.04.00 (Dec 27 30e72400-0000-100 192.168.5.7 N/A 219000000000	Host Name: Running Time: Chip Information: Manufacturer: MAC Address:	ISAC98F08CA45AF3 143 days, 19 hrs AST2600 VANTAGEO 98:F0:BC:A4:5A:F3	(F) (*) (*)	Firmware Upgrade Network One-Click Collection	Log Power
CPU Total 2 Present 2	Memory Total Present Capacity 64	Stora 32 20 06	ge Card Storage Card 2 Logical Drive 2 Physical Drive 12	Network	k Adapter Network Card 1 Network Port 2	Power Tot Pre	al 2 esent 2	Fan Total 4 Present 4
System Monitoring						V	The KVM pr Not recommende	e Operate Settings
							BMC Time: 20	24/03/07 15:24 (UTC+08:00)

- 2. Select System. The System page is displayed.
- 3. From the navigation tree in the left pane, select **System Information**. The **System Information** page is displayed, see Figure 4-8.

Figure 4-8 System Information Page

forma	ation										
CPU Information Generation				🗆 Disk Information 🛛 🖶 Network Adapter 🖒 FRU Information 🔲 Sensor 🕏 Other							
No.	Nam e	Present Status	Health Status	Manufacturer	Model	TDP(Watt	Frequency(MH z)	Maximum Frequency(MHz)	Core s	Threa ds	Architectu re
1	CPU 0	Present	Healthy	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86
2	CPU 1	Present	Healthy	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86
f	orma orma No. 1	ormation ormation No. Nam e 1 CPU 0 2 CPU 1	Arman Present No. Ram Present 1 CPU Present 2 CPU Present	Anno Present Status Health Status 1 CPU 0 Present Healthy 2 CPU 1 Present Healthy	ormation	ormation Ormation Memory Information Disk Information Metwork Adapter No. Resent e Health Status Manufacturer Model 1 CPU 0 Present Healthy Healthy Intel(R) Intel(R) Intel(R) Xeon(R) Platinum 8470Q 2 CPU 1 Present Healthy Healthy Intel(R) Intel(R) Intel(R) Xeon(R) Platinum 8470Q	ormation ormation Memory Information Disk Information Metwork Adapter PRU I No. e Present Health Manufacturer Model TDP(Watt s) 1 0 Present • Healthy Intel(R) Intel(R) Xeon(R) Platinum 8470Q 350 2 1 Present • Healthy Intel(R) Intel(R) Xeon(R) Platinum 8470Q 350	ormation ormation Memory Information Disk Information Network Adapter PRU Information Requency(MH z) No. Rev status Health Status Manufacturer Model TDP(Watt s) Frequency(MH z) 1 0 Present Healthy Intel(R) Corporation Intel(R) Xeon(R) Platinum 8470Q 350 2100 2 1 Present Healthy Intel(R) Corporation Intel(R) Xeon(R) Platinum 8470Q 350 2100	ormation ormation Memory Information Disk Information Metwork Adapter FRU Information Memory Information Software No. Revent Status Health Status Manufacturer Model Software Sof	ormation ormation P Memory Information Disk Information Network Adapter P RU Information Model S RU Information Second S	ormation ormation P Memory Information Disk Information Metwork Adapter P RU Information Meson S Other No. Name Present Healthy Manufacturer Model TDP(Watt Frequency(MH Maximum Core Threa 1 0° Present Healthy Intel(R) Intel(R) Xeon(R) Platinum 350 2100 3800 52 104 2 10 Present Healthy Intel(R) Xeon(R) Platinum 350 2100 3800 52 104

4. Perform the following operations as required.

То	Do					
Check CPU information	Click CPU Information to switch to the CPU Information tab.					
Check memory information	Click Memory Information to switch to the Memory Information tab.					
Check NIC information	Click Network Adapter to switch to the Network Adapter tab.					
Check GPU information	a. Click Other . The Other tab is displayed, as shown in Figure 4- 9.					
	b. Check the Position and Device BDF columns for each GPU.					

То	Do
	The last two digits in the Position column indicate the slot where a GPU is located. For example, mainboardPCIeCard11 indicates that the slot number of the GPU is 11.
	C. Log in to the server as the <i>root</i> user.
	d. Run the following command to view the slot number of the
	GPU, as shown in Figure 4-10.
	#lspci -s 0:98:0:0 - vvv
	In the above command, "0:98:0:0" is the BDF of the GPU.

Figure 4-9 Other Tab

System Information												
@ CPU Information 🛛 🛏 Mer	mory Information	Disk Infe	ormation	l Network Ada	pter	🖒 FRU	Information (0) Sensor	8 Other				
GPU(4) PCIe Card 11 (NVIDIA 120)	PCIe Card Information											
PCIe Card 12 (NVIDIA L20)	Position	Name	Description	Manufacturer	Туре	Status	Maximum Speed (GTps)	Negotiation Speed (GTps)	Maximum bandwidth	Negotiate bandwidth	Device BDF	Root Port BDF
PCIe Card 13 (NVIDIA L20) PCIe Card 14 (NVIDIA L20)	mainboardPCIeCard11	GPU11	NVIDIA L20	Nvidia	GPU	Active	16	16	x16	x16	0:98:0.0	0:97:1.0
PCIe Card(4)	mainboardPCIeCard12	GPU12	NVIDIA L20	Nvidia	GPU	Active	16	16	x16	x16	0:d8:0.0	0:d7:1.0
Drive Backplanes(1)	mainboardPCIeCard13	GPU13	NVIDIA L20	Nvidia	GPU	Active	16	16	x16	x16	0:38:0.0	0:37:1.0
	mainboardPCIeCard14	GPU14	NVIDIA L20	Nvidia	GPU	Active	16	16	x16	x16	0:5a:0.0	0:59:1.0
									Total 4		10 / Page 🗸	To 1 Page

Figure 4-10 Querying a Physical Slot of a GPU

```
[root@localhost Desktop]# lspci -s 0:98:0.0 -vvv
98:00.0 3D controller: NVIDIA Corporation Device 26ba (rev a1)
Subsystem: NVIDIA Corporation Device 1957
Physical Slot: 11
```

4.5 Managing Storage Devices

Abstract

The storage devices of a server refer to RAID controllers and hard disks.

The physical disks managed by a RAID controller can be created as logical disks.

On the **Storage Management** page, the **Storage Card** tab displays SAS/SATA disks, and the **NVMe** tab displays NVMe disks.

Steps

- 1. Select System. The System page is displayed.
- From the navigation tree in the left pane, select Storage Management. The Storage Management page is displayed, see Figure 4-11.
Figure 4-11 Storage Management Page

Storage Management Storage Card NVMe				
Embedded Card 1 (RM24 + E-Logical Driver 0 Logical Driver 1	Controller Information	RM2438	Location:	Embedded Slot1
- Disk 17 - Disk 22 - Disk 51	Manufacturer: Chip Type:	VANTAGEO PM8238	Chip Manufacturer: Health Status:	Microchip Normal
	Device Version: NVDATA Version:	3.22	Packaged Version: BIOS Version:	
	Serial Number: Device Interface:	5AS 12Gbps	SAS Address: Memory Size :	 128 MiB
	Temperature: Supported RAID Levels:	45 ℃ RAID0, RAID1, RAID5, RAID10	Supported Strip Size Range:	16384-1048576 K
	BBU			
	Name: Status:	absent	Health Status: Temperature:	

1.RAID controller

2.Logical disk 3.Physical disk

3. Perform the following operations as required.

То	Do
Check RAID controller and BBU information	On the Storage Card tab, click the desired RAID controller. The RAID controller and BBU information is displayed on the right.
Check logical disk information	On the Storage Card tab, click the desired logical disk. The detailed logical disk information is displayed on the right. In the logical disk information, Status includes: • Optimal • Degraded • Part Degraded • Offline
Set the UID indicator of a logical disk	 a. On the Storage Card tab, click the desired logical disk. b. Click Settings on the right. The Logical Drive Setting dialog box is displayed. c. Select Open or Close. Open: turns on the UID indicators of all member disks of the logical disk. Off: turns off the UID indicators of all member disks of the logical disk. d. Click Submit.

Check physical disk information	On the Storage Card tab, click the desired physical disk. The detailed physical disk information is displayed on the right.
То	Do
Create a logical disk	 a. On the Storage Card tab, click + next to a RAID controller. The Create Logical Drive area is displayed on the right, see Figure 4-12. b. Configure the following parameters: Logical disk name: Enter the name of the logical disk. RAID Level: Select the corresponding RAID level. Stripe Size: Select a stripe size. Physical Drive Configuration: Select the member disks that form the logical disk.
	c. Click Save.
Query NVMe hard disk information	On the Storage Management page, click NVMe to switch to the NVMe tab. The detailed NVMe disk information is displayed.
Figure 4-12 Create Logi	cal Drive Area
Create Logical Driv	e

Logical disk name	test	
RAID Level	RAID0	1
Strip Size	1MiB	2
Physical Drive Configuration	17-SSD-1920 × 22-SSD-1920 ×	
	Save Cancel	

Note

Different types of RAID controllers have different pages for creating logical disks.

4.6 Installing an OS Remotely

Abstract

When you are not on the customer site, you can install the OS for a server remotely through a PC.

The operations for remote OS installation include:

- 1. Disabling media redirection configurations
- 2. Configuring a boot mode
- 3. Installing an OS

Prerequisite

- The *iso* file of the OS is already obtained.
- The RAID configuration for the system disk of the server is already completed.
- If the KVM needs to be started in Java mode, JRE (for example, *jre-8u191*) is already installed on the PC.

Steps

Disabling Media Redirection Configurations

- 1. Select Services. The Services page is displayed.
- From the navigation tree in the left pane, select Virtual Media. The Virtual Media page is displayed, see Figure 4-13.

Figure 4-13 Virtual Media Page

Virtual Media		
Media Setting Medi	Mounting	
VMedia Entity Settings		
CD/DVD Physical Device	1	v
HD Physical Device	1	
Remote KVM CD/DVD Physical Device	1	×
Remote KVM HD Physical Device	1	Ŷ
⑦ Media Redirection Encryption	0	
	Save	

- 3. In the VMedia Entity Settings area, turn off Media Redirection Encryption, and click Save.
- 4. From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed, see Figure 4-14.

Figure	4-14	Virtual	Console	Page
A 1947				

Virtual Console			
Start KVM	HTML Virtual Console	Java Virtual Console	
Session Settings			
* ⑦ Communication Encryption	\bigcirc		
Single Port	0		
Retry Times	3		
Retry Interval	10		S
	Save		

5. In the Session Settings area, turn off Communication Encryption, and click Save.

Configuring a Boot Mode

- 6. Select System. The System page is displayed.
- From the navigation tree in the left pane, select System Settings. The System Settings page is displayed, see Figure 4-15.

Figure 4-15 System Settings Page

ystem Settings		
Boot Options Board	Panel Uart Config	
 Startup settings are valid configure. 	for permanent use and require administrator privileges to	
Boot Option	CD/DVD	
Boot Mode	UEFI	
Current Boot Mode	VEFI	
Effective	🔘 One-time 🔵 Permanent	
	Save	

8. Set the parameters. For a description of the parameters, refer to Table 4-4.

Table 4-4 Boot Option Parameter Descriptions

Parameter	Setting
Boot Medium	Select CD/DVD.
Boot Mode	Select UEFI.
Effective	Select Permanent .

9. Click Save.

Installing an OS

- 10.Select Services. The Services page is displayed.
- 11.From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed.
- 12.Perform the following operations as required.

То	Do
Start the KVM in HTML mode	 Click HTML Virtual Console. The HTML Virtual Console page is displayed, see Figure 4-16.
	b. Click Browse File next to CD Image , and select the <i>iso</i> file from the PC.
	c. Click Start Media to load the <i>iso</i> file.
	d. Select Power > Reset Server to restart the server. The page for installing the OS is displayed.

Start the KVM in Java mode	a. In the search box in the lower left corner of the PC, enter Java.
	b. In the search result, select Configure Java. The Java Control Panel
	dialog box is displayed.
	c. Click Security. The Security window is displayed.
	d. Click Edit Site List. The Exception Site List dialog box is displayed.
	e. Click Add to add the address of the Web portal of the BMC.
	f. Click OK to return to the Security window.
	g. Click OK .
	h. On the Virtual Console page of the Web portal of the BMC, click
	Java Virtual Console. A dialog box indicating whether to keep
	jviewer.jnlp is displayed.
	i. Click Keep .
	j. In the lower left corner of the browser, click $\verb"jviewer.jnlp". A dialog$
	box indicating whether to proceed is displayed.
	$k. \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
	box is displayed.
	I. Select I accept the risk and want to continue to run this app. and
	click Run . The Untrusted Connection dialog box is displayed.
	m. Click Yes . The Java Console page is displayed, see Figure 4-17.
То	Do
	n. Select Media > Virtual Media Wizard, and switch to the CD/DVD
	tab.
	o. Click Browse , and select the <i>iso</i> file from the PC.
	p. Click Connect .
	q. Select Power > Reset Server to restart the server. The page for installing the OS is displayed.



Before starting the KVM in one mode, you must disable the KVM in another mode. For example, before starting the KVM in Java mode, you must disable the KVM started in HTML mode.

Stop KVM	CD Image: Browse File (0 KB) Start Media
Video • Mouse • Options • Keyboard • Send Keys • Hot Keys • Video Record • Power • Active Users • Help •	▲ Zoem 100 % 🖵 🕑
Wed 14:51	€) - •() ♥ -
bs Not listed?	
🧐 redhat.	
	LWIN RWIN LALT LCTRL RALT RCTRL NUM CAPS SCR

Figure 4-16 HTML Console Page

Figure 4-17 Java Console Page



4.7 Resetting the BMC When the Web Portal Is Unavailable

Abstract

If you cannot log in to the Web portal of the BMC, you need reset the BMC.

You can reset the BMC through one of the following ways:

- Resetting the BMC by logging in to the server
- Resetting the BMC by using an SSH tool (for example, PuTTY)
- Resetting the BMC by using the ipmitool
- Resetting the BMC by powering off the server

Prerequisite

- If you want to reset the BMC by using the ipmitool, the **ipmi** service port number is already set to **623**.
- If you want to reset the BMC by using the ipmitool, the BMC address is successfully pinged with the ipmitool.

Steps

- Resetting the BMC by logging in to the server
 - 1. Log in to the server as the *root* user.
 - 2. Run the following commands to reset the BMC:

```
# modprobe ipmi_si
```

```
# modprobe ipmi_devintf
```

```
# ipmitool mc reset cold
```

- Resetting the BMC by using an SSH tool
 - 1. Log in to the BMC by using the SSH tool Enter the following parameters for login:
 - → Host address: address of the BMC
 - → Username: sysadmin (the default administrator username)
 - → Password: The default administrator password depends on server models and BMC versions. For details, refer to 10 Reference: Default Passwords.
 - → Port number: 22
 - 2. Run the following command to reset the BMC:

reboot

- Resetting the BMC by using the ipmitool
 - 1. In the ipmitool, run either of the following commands to reset the BMC:
 - → Warm boot: ipmitool -I lanplus -H 10.235.51.202 -U Administrator

- -P Superuser9! mc reset warm Sent warm reset command to MC
- \rightarrow Cold boot: ipmitool -I lanplus -H 10.235.51.202 -U Administrator
- P Superuser9! mc reset cold Sent cold reset command to MC

The parameters in the above commands are described as follows:

- → 10.235.51.202: address of the BMC
- → Administrator: username
- → Superuser9!: password
- Resetting the BMC by powering off the server
 - 1. Power off the server without services.
 - 2. Power on the server.

4.8 Querying and Configuring Services

Abstract

By default, the BMC provides the following services:

- web: a platform-independent, low-coupling, self-contained, programmable web-based application. You can use open XML standards for defining, publishing, discovering, coordinating, and configuring such applications, which are used to develop distributed and interoperable applications.
- **kvm**: controls, switches between, and manages multiple devices through a keyboard, display, or mouse, playing an important role in remote scheduling and monitoring.
- cd-media: a virtual media service that allows a KVM target server to access files on physical CD/DVD devices on a PC (acting as the client).
- hd-media: a virtual media service that allows a KVM target server to access files on physical HD devices on a PC (acting as the client).
- **ssh**: a protocol that provides secure remote access and other secure network services in an insecure network.
- **vnc**: a remote control tool, which consists of the application program (vncviewer) of the client and the application program (vncserver) of the server.
- snmp: a network management standard protocol widely used in TCP/IP networks. It provides unified interfaces to achieve the unified management of devices of different manufacturers.
- redfish: a server management specification. The Redfish Scalable Platforms Management API ("Redfish") uses RESTful interface semantics to access data defined in model format to perform out-of-band systems management. It is suitable for the management and deployment of large-scale server cloud environments.
- ipmi: a standard applied to server management system design.

This procedure describes how to query and modify the parameters of the services above.

Steps

- 1. Select Services. The Services page is displayed.
- 2. From the navigation tree in the left pane, select **Port Services**. The **Port Services** page is displayed, see Figure 4-18.

Figure 4-18 Port Services Page

Ports	ervices						
No.	Name	Status	Non Secure Port	Secure Port	Timeout(Min)	Maximum Sessions	Operation
1	web	Open	80	443	30	20	Edit
2	kvm	Open	7578	7582	30	4	Edit
3	cd-media	Open	5120	5124		1	Edit
4	hd-media	Open	5123	5127		1	Edit
5	ssh	Open	3 5	22	10		Edit
6	vnc	Open	5900	5901	10	2	Edit
7	snmp	Open	161	0.00			Edit
8	redfish	Open	0.57	100		127	Edit
9	ipmi	Open	222	623			

- 3. Click Edit for a service to activate the parameters.
- 4. Set the parameters. For a description of the parameters, refer to Table 4-5.

Parameter	Setting	
Status	Select whether to enable a service.	
Non Secure Port	Enter the non-secure port number of the service.	
	• Default non-secure port number of the Web service: 80.	
	• Default non-secure port number of the KVM service: 7578.	
	• Default non-secure port number of the CD media service: 5120.	
	• Default non-secure port number of the HD media service: 5123.	
	• Default non-secure port number of the VNC service: 5900.	
	• Default non-secure port number of the SNMP service: 161.	
	Other services do not support non-secure ports.	
	Range of the non-secure port numbers: 1–65535.	

Table 4-5 Port Service Parameter Descriptions

Secure Port	 Enter the secure port number of the service. Default secure port number of the Web service: 443. Default secure port number of the KVM service: 7582. Default secure port number of the CD media service: 5124. Default secure port number of the HD media service: 5127. Default secure port number of the SSH service: 22. Default secure port number of the VNC service: 5901. Default secure port number of the IPMI service: 623. Other services do not support secure ports. Range of the secure port numbers: 1–65535.
Timeout(Min)	The service exits if no operation is performed within the specified timeout period. Enter the timeout period (in minutes). Range: 5–60 (for the VNC service) or 1–60 (for other services).



You cannot configure the Maximum Sessions parameter.

5. Click Save.

Verification

 After enabling the Redfish service, you can query and configure the BMC through the Redfish interface.

For a detailed description of the Redfish interface, refer to the VANTAGEO Server Redfish Interface Description (BMC V4). For how to obtain the VANTAGEO Server Redfish Interface Description (BMC V4) file, refer to 11 Reference: Accessing Documents.

 After enabling the SNMP service and configuring a correct non-secure port, you can query and configure the BMC through the SNMP interface.

For a detailed description of the SNMP interface, refer to the VANTAGEO Server SNMP Interface Description (BMC V4). For how to obtain the VANTAGEO Server SNMP Interface Description (BMC V4) file, refer to 11 Reference: Accessing Documents.

4.9 Configuring an NTP Server

Abstract

An NTP server is a time synchronization source of the BMC. If the time of the BMC needs to be synchronized with an NTP server, you need to configure the NTP server.

To configure an NTP server, perform the following operations:

- 1. Enabling the NTP service: provides the NTP service for the devices whose time needs to be synchronized.
- 2. Modifying the registry: modifies the registry parameters related to the NTP service.
- 3. Restarting the NTP service: applies the modified registry parameters.



This procedure uses the operations on a PC with the Windows Server 2012 R2 OS as an example. The operations on PCs with other Windows Server OSs are similar.

Steps

Enabling the NTP Service

- Right-click This PC on the desktop, and then select Manage from the shortcut menu. The Computer Management window is displayed.
- From the navigation tree in the left pane, select Services and Applications > Services. The Services window is displayed.
- 3. In the service list, right-click **Windows Time** and select **Start** from the shortcut menu.

Modifying the Registry

- 4. Press Windows+R. The Run dialog box is displayed.
- 5. In the **Open** text box, enter *regedit*, and click **OK**. The **Registry Editor** window is displayed.
- 6. Modify the registry parameters. For a description of the parameters, refer to Table 4-6.

Table 4-6 Registry Parameter Descriptions

Registry Path	Parameter	Value
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	AnnounceFlag s	5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\ NtpServer	Enabled	1
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	Туре	NTP

Restarting the NTP Service

- 7. In the **Open** text box in the **Run** dialog box, enter *cmd*, and click **OK**. The command line window is displayed.
- 8. Run the following command to stop the NTP service:
 - C:\>net stop w32time

9. Run the following command to start the NTP service:

C:\>net start w32time

10.Run the following command to verify that the NTP server is configured successfully:

C:\>w32tm /stripchart /computer:127.0.0.1

If the output time is displayed after the command is executed, it indicates that the configuration is successful.

4.10 Configuring an SMTP Server

Abstract

An SMTP server receives alarm emails from the BMC.

To configure an SMTP server, perform the following operations:

- 1. Installing the SMTP server: provides the SMTP service for the BMC.
- Configuring the IP address and port number: sends alarm emails (if any) to the default path (*C:\inetpub\mailroot\Drop*) on the SMTP server after the IP address and port number of the SMTP server are configured on the Web portal of the BMC.

III Note

This procedure uses the operations on a PC with the Windows Server 2012 R2 OS as an example. The operations on PCs with other Windows Server OSs are similar.

Steps

Installing an SMTP Server

- 1. Press Windows+R. The Run dialog box is displayed.
- 2. In the **Open** text box, enter *servermanager*, and click **OK**. The **Server Manager** window is displayed.
- 3. Click Add Roles and Features. The Add Roles and Features Wizard window is displayed.
- 4. Select Role-based or feature-based installation.
- 5. Click Next.
- 6. Select Select a server from the server pool, and then select the server from Server Pool.
- 7. Click Next until the Features step in Add Roles and Features Wizard is displayed.
- 8. Select SMTP Server.
- 9. Click Install.

Configuring the IP Address and Port Number

- 10.In Control Panel > System and Security > Administrative Tools, double-click Internet Information Services (IIS) 6.0 Manager.
- 11.Right-click **SMTP Virtual Server #1**, and select **Properties** from the shortcut menu. The **[SMTP Virtual Server #1] Properties** dialog box is displayed.
- 12. From the IP address list, select the corresponding IP address.



The selected IP address is that of the server selected in Step 6.

13.Switch to the **Delivery** tab.

14.Click Outbound connections. The Outbound Connections dialog box is displayed.

15.In the TCP port text box, enter 25.

16.Click OK.

4.11 Configuring Trap Notification Parameters

Abstract

Trap notification parameters are used by the BMC to report alarms to a third-party NMS through traps.



Trap notification parameters are provided by the third-party NMS, so the values of trap notification parameters set on the Web portal of the BMC must be the same as those on the third-party NMS.

Abstract

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed, see Figure 4-19.

Alarm Set	tings					
Trap Noti	fication	vslog Notification Em	nail Notification			
Trap Funct	tion					
	Trap					
	Trap Version	V2C		~		
	Select V3 User	Administrator		*		
Co	ommunity Name	public				
Confirm Co	ommunity Name	public				
	Trap Host ID	Host Name		~		
Event Sending Level		Critical ~		~		
		Save				
Trap Serve	er Configuration					
No.	Server Ad	dress	Trap Port		Current Status	Operation
1	10.239.212	2.117	323		Disabled	Edit Test
2	10.230.19.	204	162		Enabled	Edit Test
3	10.239.211	53	53		Enabled	Edit Test

3. Set the parameters in the **Trap Function** area. For a description of the parameters, refer to Table 4-7.

Parameter	Setting	
Тгар	Turn on the Trap switch.	
Trap Version	Select the SNMP version for traps. Options: V1, V2C, and V3.	
Select V3 User	This parameter is required if Trap Version is set to V3 . Select an SNMP user as the alarm sender. For how to create an SNMP user, refer to "4.16 Creating an SNMP User".	
Community Name	This parameter is required if Trap Version is set to V1 or V2C . Enter the trap community name.	
Confirm Community Name	This parameter is required if Trap Version is set to V1 or V2C . Enter the trap community name.	
Trap Host ID	Select the identifier of the host that reports alarms.	
Event Sending Level	Select the level of events to be reported. For example, if Event Sending Level is set to Critical , only critical alarms are reported.	

Table 4-7 Trap Function Parameter Descriptions

4. Click Save.

5. Set the parameters in the **Trap Server Configuration** area. For a description of the parameters, refer to Table 4-8.

Parameter	Setting
Server Address	After you click Edit , the parameter is activated. Enter the address of the server that receives alarms. An IPv4 address, IPv6 address, or domain name is supported.
Trap Port	After you click Edit , the parameter is activated. Enter the port number of the server that receives alarms. Range: 1– 65535.
Current Status	After you click Edit , the parameter is activated. Select whether to enable the current server to receive alarms.

Table 4-8 Parameter Descriptions for Trap Server Configuration

6. Click Save.



After the Edit button is clicked, it is changed to the Save button.

7. (Optional) To send a test event to the server, click Test.



If a message indicating "sent successfully" is displayed on the page, the trap is sent successfully.

4.12 BMC Log Export

You can export BMC logs in the following ways:

- Exporting logs in one click through the Web portal
 For details, refer to 4.12.1 Exporting Logs in One Click Through the Web Portal.
- Exporting logs by category through the Web portal For details, refer to 4.12.2 Exporting Logs by Category Through the Web Portal.
- Exporting logs through SSH commands
 For details, refer to 4.12.3 Exporting Logs Through the CLI (SSH).
- Export logs through a serial port
 For details, refer to 4.12.4 Exporting Logs Through the CLI (Serial Port).

4.12.1 Exporting Logs in One Click Through the Web Portal

Abstract

The Web portal of the BMC provides the one-click log export function. The exported log file is named *bmcinfo_<product serial number>.tar.gz* and stored in the default download directory of the browser.



If the product serial number is not programmed, the filename is bmcinfo_UnknownProductSN.tar.gz.

Steps

1. In the **Shortcuts** area on the **Homepage**, click **One-Click Collection**. The **Confirm one click acquisition** dialog box is displayed, see Figure 4-20.

Figure 4-20 Confirm One Click Acquisition Dialog Box



2. Click Submit.



During the collection process, all Web interfaces of the BMC cannot be operated. If you shut down the browser by mistake and collect logs again after relogging in to the Web portal of the BMC, the **One click acquisition is being processed, please try again later.** prompt is displayed. In this case, you need to wait for about five minutes.

4.12.2 Exporting Logs by Category Through the Web Portal

Abstract

Logs of the BMC include:

- **Operation Logs**: record the information about users' operations on the server, including manual server operations and remote server operations.
- Audit Logs: record users' login to and logout of the Web portal, BMC, and KVM.

Steps

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **BMC Logs**. The **BMC Logs** page is displayed, see Figure 4-21.

MC Lo	gs				
1 The	e page only displays about 10) logs generated recently. To	o view all the logs, please downloa	d the logs to view them locally.	
Operat	tion Logs Audit Logs				
Downlo	oad Logs				Q Search(Fuzzy search only s
No. 🛊	Generation Time 💠	Interface	User	Address	Details
112	2024-03-07 14:10:27	WEB	Administrator	10.	set time zone (Asia/Shanghai) successfully.
111	2024-03-07 14:10:27	WEB	Administrator	10.	disable NTP Server successfully.
110	2024-03-07 14:10:22	WEB	Administrator	10.	set bmc time to 2024-03-07 14:10:22 successfully.
109	2021-06-29 20:54:36	WEB	Administrator	10.	set asset tag: 21900000000 successfully
108	2021-06-29 20:36:52	WEB	Administrator	10.	set asset tag: 21900000000 successfully
107	2021-06-21 03:09:55	WEB	Administrator	10.	control chassis power on successfully.
106	2021-06-20 21:07:21	REDFISH	Administrator	10.	control chassis power cycle successfully.
105	2021-06-20 21:07:07	N/A	N/A	N/A	upgrade BIOS successfully.
104	2021-06-20 20:52:48	N/A	N/A.	N/A	upgrade BIOS with preserve configuation successfully.
103	2021-06-20 20:52:47	REDFISH	N/A	N/A	begin upgrade BIOS successfully.

3. Perform the following operations as required.

То	Do
Export operation logs	 a. Click Operation Logs to switch to the Operation Logs tab. b. (Optional) In the Search box, enter a keyword. c. Click Download Logs.
Export audit logs	 a. Click Audit Logs to switch to the Audit Logs tab. b. (Optional) In the Search box, enter a keyword. c. Click Download Logs.

4.12.3 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/
# ./expert_bmcdata.sh
```

Note

After the logs are exported, they are stored in the /var/bmcdata directory.

- 3. Download the log file to the local PC by using the SFTP function.
- 4. Run the following commands in the CLI to delete the BMC log file:
 - # cd /var/bmcdata

rm bmcinfo_.tar.gz

4.12.4 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 to the serial port of the BMC by using a serial cable.
- Press and hold the UID button on the server panel for six seconds until the indicator flashes blue.
- 3. Connect to the serial port of the BMC by using a serial port tool.
- 4. After the connection is established, 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/
 - # ./expert_bmcdata.sh



After the logs are exported, they are stored in the /var/bmcdata directory.

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

```
# cp /var/bmcdata/bmcinfo_.tar.gz /mnt/nandflash0/
```

Note

After the network is restored, you can download the log file to the local PC by using the SFTP function.

4.13 Upgrading the BMC Firmware

Abstract

When the BMC firmware needs to be upgraded, you can upload the firmware online to upgrade

it.

III Note

- The Web portal of the BMC temporarily supports the upgrade of the active BMC firmware only. After the active BMC firmware is upgraded, the BMC is automatically restarted to apply it.
- If a firmware version fails to be upgraded during the upgrade process, you must upgrade it again.

Prerequisite

The BMC firmware is already obtained.



The firmware upgrade file can be downloaded on the **Software Download** page on the Web portal of the servers and storage products (<u>https://VANTAGEO.com/Enterpriseservers</u>).

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- From the navigation tree in the left pane, select Firmware Upgrade. The Firmware Upgrade page is displayed, see Figure 4-22.

Figure 4-22 Firmware Upgrade Page

```
Firmware Upgrade
   Firmware Upgrade
                                 Mode Switching
   1 After the BMC is upgraded, the BMC is automatically restarted. When the system is powered off, the BIOS upgrade takes effect directly. When the system is powered on, the BIOS is updated to the backup version and takes effect automatically after the systems is powered off. It takes a period of time to make the firmware take effect automatically, and firmware upgrade cannot be performed
         during this period.
                                              Firmware Reset BMC
                                             Operation
                                            Information
                                                               BMC Primary Partition Version 04.24.04.00 (Sep 27 2024)
                                                               BMC Standby Partition Version 04.24.04.00 (Aug 26 2024)
                                                               BIOS Primary Version
                                                                                                      04.24.03.10 (Aug 26 2024)
                                                               BIOS Standby Version
                                                                                                  04.24.03.10 (Aug 26 2024)
                                                               EPLD Version
                                                                                                      00.00.00.0107
                                        (?) Upgrade
                                                               Upload
```

3. Click Upload and select the firmware upgrade file.

III Note

After the BMC firmware is successfully uploaded, the **Don't Inherit Configuration When Upgrading BMC** check box becomes activated.

4. (Optional) To restore the factory default settings of the BMC, select Don't Inherit

Configuration When Upgrading BMC.

5. Click Upgrade.

U Notice

During the firmware upgrade process, you cannot to switch to another page. Otherwise, the upgrade process is interrupted.

4.14 Restoring Factory Defaults

Abstract

This procedure describes how to restore the server configuration items (for example, the network, user, SNMP configuration, and boot mode) to factory defaults.



Do not perform any operation during restoration. After the factory defaults are restored, the BMC will be restarted automatically.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- From the navigation tree in the left pane, select Configuration Update. The Configuration Update page is displayed, see Figure 4-23.

Configuration Update				
Configure Import				
i Supports importing BMC ar	id BIOS configurations. After importing, BMC automatically restarts and the configuration takes effect. BIOS takes effect and requires manual resetting of the hos			
Select Type	O BMC O BIOS			
Select File	Upload			
	Import			
Configure Export				
Select Type	O BMC O BIOS			
	Export			
Restore Factory Settings				
After restoring BMC factory	/ settings, you need to log in to BMC for the first time. Please use this function with caution.			
After restoring BMC factory	settings, you need to log in to BMC for the first time. Please use this function with caution.			

3. Click Restore Factory Settings.

4.15 Backing Up BMC Configurations

Abstract

Before replacing the mainboard of the server, you must export the BMC configurations. After replacing the mainboard, you need to import the BMC configurations.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- From the navigation tree in the left pane, select Configuration Update. The Configuration Update page is displayed, see Figure 4-24.

Figure 4-24 Configuration Update Page

Configuration Update	
Configure Import	
i Supports importing BMC a	nd BIOS configurations. After importing, BMC automatically restarts and the configuration takes effect. BIOS takes effect and requires manual resetting of the host
Select Type	O BMC O BIOS
Select File	Upload
	Import
Configure Export	
Select Type	O BMC O BIOS
	Export
Restore Factory Settings	
After restoring BMC factory	r settings, you need to log in to BMC for the first time. Please use this function with caution.
	Restore Factory Settings

- 3. Click **Export** to export the current BMC configurations to your local PC.
- 4. After replacing the mainboard, click **Upload**, and select the exported BMC configuration file in the displayed dialog box.
- 5. Click Import, and confirm the import in the displayed message box.



After the BMC configurations are imported, the BMC is automatically restarted to apply the configurations. Do not perform any other operations until the BMC is restarted.

4.16 Creating an SNMP User

Abstract

When configuring notification parameters for SNMPv3 trap messages, you need to select an SNMP user as the alarm sender. This procedure describes how to create an SNMP user.

Steps

- 1. Select User & Security. The User & Security page is displayed.
- 2. From the navigation tree in the left pane, select **Local Users**. The **Local Users** page is displayed, as shown in Figure 4-25.

ocal Users				(
+ Add Use	r			Q Search(Fuzzy search only.
User ID	User Name	Role	Login Interfaces	Operation
1	anonymous	Administrator	SNMP SSH Redfish	Edit Enable Delete
2	Administrator	Administrator	SNMP SSH Redfish	Edit Disable Delete

3. Click Add User. The Add User page is displayed, as shown in Figure 4-26.

ocal Users > Add User		
New User ID	3	~
New UserName	testUser	
New Password	•••••	
Confirm Password	••••••	
Role	Administrator	\$
Login Interfaces	SNMP 🕐 🗌 Redfish	
Current User Password		
	Submit	

4. Set the parameters. For a description of the parameters, refer to Table 4-9.

Parameter	Description
New User ID	Select the ID of the new user. A maximum of 16 local users are supported, so the user ID ranges from 1 to 16. User 1 is a reserved user, and user 2 is the default administrator.
New UserName	Enter the name of the new user. The name contains a maximum of 16 characters, including digits, letters (case sensitive), and special characters. The new username cannot be the same as any existing one. The following cannot be used as a username: sshd, ntp, stunnel4, sysadmin, daemon, Administrator, and anonymous. The allowed special characters include hyphens (-), underscores (_), and at symbols (@).

Table 4-9 Parameter Descriptions for Adding a Local User

Parameter	Description
New Password	Enter the password of the new user. The password contains 8–20 characters, including digits, letters (case sensitive), and special characters. It must contain one special character and characters from at least two of the following types: digits, uppercase letters, and lowercase letters. The password can contain the following special characters: `, ~, !, @, \$, %, ^, &, *, (,), -, _, =, +, , [, {, },], :, ', ", ,, <, ., >, /, ?, #, ;. The function of disabling historical passwords is disabled by default. If this function is enabled, the new password cannot be the same as any of the historical passwords. The password cannot be the same as the username in reverse order. For example, if the username is test, the password cannot be tset.
Confirm Password	Enter the password again. It must be the same as New Password .
Role	Select the role of the new user.
Login Interfaces	 Select one or more login interfaces available to the new user. SNMP is required. It indicates SNMP interface-based login. For Redfish interface-based login, select Redfish. SSH-based login is supported for all users by default.
Current User Password	Enter the password of the currently logged-in user of the Web portal of the BMC.

- 5. Click **Submit** to return to the **Local Users** page.
- 6. In the **Operation** column, click **Edit** for the new user. The **Edit** page is displayed, as shown in Figure 4-27.

Figure 4-27 Edit Page

Local Users > Edit		
User ID	3	
User Name	testUser	
Password	Please enter the password	
Confirm Password	Please enter the password again	
Role	Administrator	~
Login Interfaces	SNMP 🕐 🗌 Redfish	
⑦ SNMPv3 Authentication Algorithm	SHA256	~
③ SNMPv3 Encryption Algorithm	AES	~
Current User Password		
	Submit	

7. Set the parameters. For a description of the parameters, refer to Table 4-10.

Table 4-10 Parameter Descriptions for Editing a Local User

Parameter	Description
SNMPv3 Authentication Algorithm	Select an authentication algorithm. SHA256 , SHA384 , or SHA512 is recommended.
SNMPv3 Encryption Algorithm	Select an encryption algorithm. AES is recommended.
Current User Password	Enter the password of the currently logged-in user of the Web portal of the BMC.

8. Click Submit.

Chapter 5 System Management

Table of Contents

Querying System Information	63
Querying Performance Data	64
Querying Fan Information	67
Configuring the Heat Dissipation Policy	67
Querying Temperature KPIs	69
Managing Storage Devices	70
Configuring the Position Indicator of a Pass-Through Disk	73
Powering On/Off the Server	74
Configuring the Server Startup Policy	77
Configuring Power-On Delay Parameters	78
Configuring the High-Temperature Power-Off Strategy	79
Querying Power Supply Information	81
Configuring the Power Mode	
Querying Power Statistics	84
Configuring Power Control Parameters	
Querying Power KPIs	86
Configuring Boot Options	87
Configuring the Serial Port Output Mode	89

5.1 Querying System Information

Abstract

By querying system information, you can learn about the following information:

- CPU information
- Memory information
- Hard disk information
- NIC information, including Ethernet NIC and FC information
- FRU information
- Sensor information

 Other information, including GPU, PCIe card information, and hard disk backplane information.



The operations for querying the above information are similar. This procedure uses how to query CPU information as an example.

Steps

- 1. Select System. The System page is displayed.
- From the navigation tree in the left pane, select System Information. The System Information page is displayed, see Figure 5-1.

Figure 5-1 System Information Page

CPU	Informa	ation	I Memory	Information	🗌 Disk Informati	ion 🛛 🕀 Network Adapter	r 🖸 FRU I	nformation	(••) Sensor 🛛 😂 Other			
Details	No.	Nam e	Present Status	Health Status	Manufacturer	Model	TDP(Watt s)	Frequency(M Hz)	Maximum Frequency(MHz)	Core s	Threa ds	Architectu re
~	1	CPU 0	Present	 Healthy 	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86
~	2	CPU 1	Present	 Healthy 	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86

3. (Optional) To view the details of a CPU, click in the **Details** column for the CPU.

5.2 Querying Performance Data

Abstract

By querying performance data, you can learn about the following information:

- CPU usage
- Memory usage
- Disk usage
- Dynamic CPU load ratio: ratio of the currently used CPU resources to the total CPU resources of the server
- Dynamic memory load ratio: ratio of the currently used memory resources to the total memory resources of the server
- Dynamic I/O load ratio: ratio of the currently used I/O resources to the total I/O resources of the server

Note

The three types of performance data related to dynamic load ratio is displayed on the **CUPS** tab. The **CUPS** tab is displayed for a server whose CPU is supported by only the Intel platform.

Steps

- 1. Select System. The System page is displayed.
- From the navigation tree in the left pane, select **Performance Monitoring**. The **Performance Monitoring** page is displayed, see Figure 5-2.

Performance Monitoring		C
System Resource CU	S	
Resource Usage		Advanced Setting
 Threshold 55%	 Threshold 38%	
CPU Usage	Memory Usage	
Disk Usage		
	No Data.	
	priease check whether the disk is running normally/whether in-band monitoring	

Figure 5-2 Performance Monitoring Page

Note

The CPU usage, memory usage, and disk usage are displayed on the above page.

3. (Optional) Click CUPS. The CUPS tab is displayed, as shown in Figure 5-3.



The CUPS tab is displayed for a server whose CPU is supported by only the Intel platform.

Figure 5-3 CUPS Tab

erformance Monit	oring		
System Resource CUPS			
CUPS Overview			
0%		0%	0%
CPU		Memory	IO
CPU Utilization		Memory Utilization	IO Utilization

Note

The dynamic CPU, memory, and I/O load ratios are displayed on the above tab.

Related Tasks

To set the CPU usage, memory usage, and disk usage thresholds, perform the following operations:

1. On the **Performance Monitoring** page, click **Advanced Setting**. The **Set Alarm Threshold** dialog box is displayed, see Figure 5-4.

ed to install and run iSDMA(intelligent Server D Ins under OS) on the OS side.The alarm thresh %), otherwise it will not be reported as an alar	evice Management old cannot be lower m.
5	%
8	%
8	%
	ed to install and run iSDMA(intelligent Server D uns under OS) on the OS side.The alarm thresh %), otherwise it will not be reported as an alar 55 88

- 2. Set the alarm thresholds as required.
- 3. Click Submit.

5.3 Querying Fan Information

Abstract

By querying fan information, you can learn about the operational status and detailed information of each fan in the server.

Steps

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Fan & Heat Dissipation**. The **Fan & Heat Dissipation** page is displayed, see Figure 5-5.

Figure 5-5 Fan & Heat Dissipation Page

an & Heat Dissipation							
Fan Ir	nformation Heat	Dissipation Key Perfo	rmance Indicator				
No.	Name	Туре	Present	Speed(RPM)	Speed Ratio(%)	Health Status	
1	FAN1	8038	Present	4591	30	Normal	
2	FAN2	8038	Present	4545	30	Normal	
3	FAN3	8038	Present	4610	30	Normal	
4	4 FAN4 8038		Present	4599	30	Normal	
					Total 4 K K	> 10 / Page ~ To 1 Page	

Note

- The Speed(RPM) column indicates the current speed of each fan.
- The **Speed Ratio(%)** column indicates the ratio of the current speed of each fan to its maximum speed.

5.4 Configuring the Heat Dissipation Policy

Abstract

A heat dissipation policy is configured in accordance with the environment where the server is held to ensure the performance and stability of the server.

Steps

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Fan & Heat Dissipation**. The **Fan & Heat Dissipation** page is displayed.

3. Click Heat Dissipation. The Heat Dissipation tab is displayed, see Figure 5-6.



4. Perform the following operations as required.

lf	Then
There is space above the top surface of the server, and the server is insensitive to noise	Set Heat Dissipation to Auto and then set Select Mode to Balance .
lf	Then
Servers are stacked together, and there is no space between them	Set Heat Dissipation to Auto and then set Select Mode to Performance .
The server is placed in an office or other areas that are sensitive to noise	Set Heat Dissipation to Auto and then set Select Mode to Low Noise.
The fan speed needs to be set manually for the server	Set Heat Dissipation to Manual and then set Speed Ratio .

Note

Speed Ratio indicates the ratio of the current speed of a fan to its maximum speed.

5. Click Save.

5.5 Querying Temperature KPIs

Abstract

Air inlet temperatures, air outlet temperatures, and CPU temperatures of a server are KPIs related to fans and heat dissipation of the server. By querying these KPIs, you can learn about heat dissipation during the operation of the server.

III Note

The server supports the high-temperature power-off function. If this function is enabled, the server is powered off after the air inlet temperature reaches the preset threshold, avoiding damages to the server hardware. To ensure service operation stability, it is recommended to disable this function.

Steps

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Fan & Heat Dissipation**. The **Fan & Heat Dissipation** page is displayed.
- 3. Click **Key Performance Indicator**. The **Key Performance Indicator** tab is displayed, as shown in Figure 5-7.

Fan & Heat Dissipa	ation								
Fan Information	Heat Dissipation	Key Performance In	dicator						
Inlet Temperature	24 Hours Last Week	Last Month			Curr	ant Value 21 00	-O- Maximum	Minimum	Export Average
25 ℃					cum		Value	Value	Value
15 °C									
10 °C									
0 ℃ 2024-01-11 20 09:18:07 0	24-01-11 2024-01-1 19:24:41 09:31:15	1 2024-01-11 09:37:49	2024-01-11 09:44:23	2024-01-11 09:50:57	2024-01-11 09:57:31	2024-01-11 10:04:05	2024-01-11 10:10:39	2024-01-11 10:17:13	2024-01-11 10:23:47
Outlet Temperatur	e t 24 Hours Last Weel	Last Month			Curre	ent Value 29.00	-O- Maximum Value	-O- Minimum Value	Export O- Average Value
30 °C									
15 ℃ 10 ℃									
5 °C 2024-01-11 20 09:23:10 C	24-01-11 2024-01- 19:29:13 09:35:17	1 2024-01-11 09:41:21	2024-01-11 09:47:24	2024-01-11 09:53:28	2024-01-11 09:59:32	2024-01-11 10:05:35	2024-01-11 10:11:39	2024-01-11 10:17:43	2024-01-11 10:23:47
CPU Temperature CPU0 CPU1 Last Hour Last	24 Hours Last Week	Last Month			Curre	ent Value 40.00	-O- Maximum Value	-O- Minimum Value	Export Average Value
40 ℃									
30 °C									
10 °C									
2024-01-11 20 09:23:10 0	24-01-11 2024-01-1 19:29:13 09:35:17	1 2024-01-11 09:41:21	2024-01-11 09:47:24	2024-01-11 09:53:28	2024-01-11 09:59:32	2024-01-11 10:05:35	2024-01-11 10:11:39	2024-01-11 10:17:43	2024-01-11 10:23:47

Figure 5-7 Key Performance Indicator Tab

4. Select a granularity period for a query.

Note

The data on the tab is automatically refreshed after the granularity period is selected.

5. (Optional) To export data, click Export.

5.6 Managing Storage Devices

Abstract

The storage devices of a server refer to RAID controllers and hard disks.

The physical disks managed by a RAID controller can be created as logical disks.

On the **Storage Management** page, the **Storage Card** tab displays SAS/SATA disks, and the **NVMe** tab displays NVMe disks.

Steps

- 1. Select System. The System page is displayed.
- From the navigation tree in the left pane, select Storage Management. The Storage Management page is displayed, see Figure 5-8.

Figure 5-8 Storage Management Page

Storage Management				
Embedded Card 1 (RM24 +	Controller Information			
Logical Driver 1	Name: Manufacturer:	RM243B VANTAGEO	Location: Chip Manufacturer:	Embedded Slot1 Microchip
- Disk 22 - Disk 51	Chip Type:	PM8238	Health Status:	Normal
	Device Version: NVDATA Version:	3.22	Packaged Version: BIOS Version:	
	Serial Number:	743775500002	SAS Address:	 128 MiB
	Temperature:	45 °C	Supported Strip Size Range:	16384-1048576 K
	Supported RAID Levels:	RAIDO, RAID1, RAID5, RAID10		
	BBU Name:		Health Status:	
	Status:	absent	Temperature:	

- 1. RAID controller
- 2. Logical disk
- 3. Physical disk
- 3. Perform the following operations as required.

То	Do
Check RAID controller and BBU information	On the Storage Card tab, click the desired RAID controller. The RAID controller and BBU information is displayed on the right.
Check logical disk information	On the Storage Card tab, click the desired logical disk. The detailed logical disk information is displayed on the right. In the logical disk information, Status includes: • Optimal

То	Do		
	 Degraded Part Degraded Offline 		
Set the UID indicator of a logical disk	 a. On the Storage Card tab, click the desired logical disk. b. Click Settings on the right. The Logical Drive Setting dialog box is displayed. 		
	 c. Select Open or Close. Open: lights up the UID indicators of all member disks of the logical disk. Off: lights off the UID indicators of all member disks of the logical disk. d. Click Submit. 		
Check physical disk information	On the Storage Card tab, click the desired physical disk. The detailed physical disk information is displayed on the right.		
Create a logical disk	 a. On the Storage Card tab, click + next to a RAID controller. The Create Logical Drive area is displayed on the right, see Figure 5-9. b. Configure the following parameters: Logical disk name: Enter the name of the logical disk. RAID Level: Select the corresponding RAID level. Stripe Size: Select a stripe size. Physical Drive Configuration: Select the member disks that form the logical disk. c. Click Save. 		
Check NVMe disk information	On the Storage Management page, click NVMe to switch to the NVM tab. The detailed NVMe disk information is displayed.		
Figure 5-9 Create Logical Drive Area

Logical disk name	test	
RAID Level	RAID0	0
Strip Size	1MiB	8
Physical Drive Configuration	17-SSD-1920 × 22-SSD-1920 ×	0

Note

Different types of RAID controllers have different pages for creating logical disks.

5.7 Configuring the Position Indicator of a Pass-Through Disk

Abstract

A pass-through disk refers to a hard disk in the server that is directly connected to a network or host through a hardware interface for data processing rather than a RAID controller or other intermediate devices.

The pass-through disks of the SATA interface type are displayed on the **Direct Harddisk** tab of the **Storage Management** page.

Setting the position indicator of a pass-through disk can help you to locate the pass-through hard disk easily.

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Storage Management**. The **Storage Management** page is displayed.
- 3. Click Direct Harddisk. The Direct Harddisk tab is displayed, as shown in Figure 5-10.



4. Click **Set** in the **Operation** column for a pass-through disk whose position indicator you want to turn on.

5.8 Powering On/Off the Server

Abstract

When you are not on the customer site, you can remotely control the server on the PC to power on or off the server.

Steps

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed, see Figure 5-11.

Figure 5-11 Power Page

Power	
Power Control Power Supply Informa	ation Power Consumption Key Performance Indicator
Host	
Host Status	Off
Host Operation	Power On Normal Power Off Forced Power Off Power Reset Power Cycle
Power Restore Policy Set	
Power Restore Policy	O Always-off Always-on Previous
	Save
Power-On Delay	
Power-On Delay	
Delay Strategy	Custom O Random(1~90s)
	Save
High Temperature Power-off	
Enabling High-Temperature Power-Off	0
	5ava

3. In the Host area, check Host Status, and perform the following operations as required.

То	Do
Power on the server	Click Power On.
Power off the server	Click Normal Power Off . The prerequisite for selecting Normal Power Off to shut down the server is that When the Power Button is Pressed in the OS of the server is already set to Power Off . For details, refer to Related Tasks .
Forcibly power off the server	Click Forced Power Off.
Perform a warm reboot	Click Power Reset . Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.
Perform a cold reboot	Click Power Cycle . Cold reboot means that the server is started after it is shut down. During the restart, the server is offline.



The grayed button indicates the current power status of the server. For example, if the **Power On** button is grayed, the server is powered on.

Related Tasks

To set When the Power Button is Pressed to Power Off, perform the following operations:



This procedure uses the Red Hat OS as an example. For other OSs, the operations are similar. If an OS does not have a GUI, you need to install the ACPI service.

1. Log in to the OS through KVM.

If the screen is locked, you need to enter the password to log in to the OS.

2. Click **III**. The **Activities** screen is displayed, as shown in Figure 5-12.



3. Click **Settings**. The **Settings** screen is displayed, as shown in Figure 5-13.

🛎 Activities 🤸 Settings 👻	Jun 22 07:18		き) ひ・
🖌 Q Settings	Power		×
ଙ୍କ Wi-Fi	Power Saving		
Bluetooth	Blank screen	5 minutes 👻	
Background			
Notifications	Suspend & Power Button		
Q. Search	Automatic suspend	Off	
	When the Power Button is pressed	Suspend	
Region & Language		Power Off	
Universal Access		Nothing	
Online Accounts			
III, Privacy			
Sharing			
() Sound			
🕞 Power			
Network			
The Devices			

. .

4. Set When the Power Button is Pressed to Power Off.

5.9 Configuring the Server Startup Policy

Abstract

This procedure describes how to configure the server startup policy to specify the power status of the server after power is restored.

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select Power. The Power page is displayed, see Figure 5-14.

Figure 5-14 Power Page

Power						
Power Control	Power Supply Informa	tion Power Cons	umption Key Performar	nce Indicator		
Host						
	Host Status	Off				
	Host Operation	Power On	Normal Power Off	Forced Power Off	Power Reset	Power Cycle
Power Restore Po	licy Set					
	Power Restore Policy	O Always-off 🔘 Alv	ways-on 🔘 Previous			
		Save				
Power-On Delay						
	Power-On Delay					
	Delay Strategy	🔿 Custom 🧿 Rando	om(1~90s)			
		Save				
High Temperature	Power-off					
Enabling H	High-Temperature Power-Off	0				
		Save				
		Jave				

- 3. In the **Power Restore Policy Set** area, set the server startup policy after the power is restored.
 - Always-off: The server remains powered off after power is restored.
 - Always-on: The server is powered on automatically after power is restored.
 - **Previous**: The server goes back to the previous power status after power is restored.
- 4. Click Save.

5.10 Configuring Power-On Delay Parameters

Abstract

This procedure describes how to configure power-on delay parameters to stagger the power-on of servers.

- 1. Select System. The System page is displayed.
- From the navigation tree in the left pane, select **Power**. The **Power** page is displayed, see Figure 5-15.

Power						
Power Control	Power Supply Informat	tion Power Consu	umption Key Performa	nce Indicator		
Host						
	Host Status	Off				
	Host Operation	Power On	Normal Power Off	Forced Power Off	Power Reset	Power Cycle
Power Restore Pol	icy Set					
	Power Restore Policy	O Always-off 🔘 Alw	ays-on 🔘 Previous			
		Contraction of the				
Power-On Delay		Save				
	Power-On Delay					
	Delay Strategy	🔿 Custom 🚺 Rando	m(1~90s)			
20. 2000.		Save				
High Temperature	Power-off					
Enabling F	lign-remperature Power-Off					
		Save				

Figure 5-15 Power Page

3. Set the parameters in the **Power-On Delay** area. For a description of the parameters, refer to Table 5-1.

Parameter	Setting
Power-On Delay	 Select whether to enable the power-on delay function. To enable the power-on delay function, turn the switch on. To disable the power-on delay function, turn the switch off.
Delay Strategy	 Select the corresponding power-on delay mode. Custom: The power-on delay time is user-defined. If Custom is selected, set Custom Delay Duration. Range: 1–120, unit: seconds. Random: The power-on delay time is automatically generated by the system.

Table 5-1 Power-On Delay Parameter Descriptions

4. Click Save.

5.11 Configuring the High-Temperature Power-Off Strategy

Abstract

If the high-temperature power-off strategy is enabled, when the air inlet temperature reaches the preset threshold, an alarm prompting server power-off is triggered. If the alarm is not cleared within the preset power-off alarm duration (60 seconds by default), the server is automatically powered off for protection.

Note

To ensure service operation stability, it is recommended to disable the high-temperature power-off strategy.

You can query and modify the high-temperature power-off alarm threshold and power-off alarm duration through IPMI commands.

Context

For the default high-temperature power-off alarm thresholds set for servers of different models, refer to Table 5-2.

Server Model	Default Value
2240-RE	52 °C
2230-RE	52 °C
22G1-RE	52 °C
1240-RE	52 °C
4440-RE	47 °C

Table 5-2 High-Temperature Power-Off Alarm Thresholds

- 1. Select **System**. The **System** page is displayed.
- 2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed, as shown in Figure 5-16.

Power						
Power Control	Power Supply Informatio	n Power Consu	mption Key Performar	nce Indicator		
Host						
	Host Status 🤎	Off				
	Host Operation	Power On	Normal Power Off	Forced Power Off	Power Reset	Power Cycle
Power Restore Pol	icy Set					
	Power Restore Policy	Always-off 🔘 Alwa	ays-on 🔘 Previous			
		Save				
Power-On Delay						
	Power-On Delay					
	Delay Strategy	Custom 🚺 Randor	n(1~90s)			
		Save				
High Temperature	Power-off		1			
Enabling H	igh-Temperature Power-Off	19				
		Save				

Figure 5-16 Power Page

3. In the **High Temperature Power-off** area, set the parameters. For a description of the parameters, refer to Table 5-3.

Parameter	Setting
Enabling High-Temperature Power-Off	 Sets whether to enable or disable the high-temperature power-off strategy. If the Enabling High-Temperature Power-Off toggle switch is turned on, the high-temperature power-off strategy is enabled. If the Enabling High-Temperature Power-Off toggle switch is turned off, the high-temperature power-off strategy is disabled.

4. Click Save.

5.12 Querying Power Supply Information

Abstract

By querying power supply information, you can learn about the power supplies of the server.

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.

 Click Power Supply Information. The Power Supply Information tab is displayed, see Figure 5-17.

Power Control Powe	r Supply Information	Power Consumption	Key Performance Indicator
Power Supply Information	Power Mode Setting		
ainboard Power Supply			
PSU1 Main	Power Supply Normal	PSU2	Main Power Supply Normal
Present Status	Present	Present Status	Present
Input Mode	AC	Input Mode	AC
Output Status	On	Output Status	On
Manufacturer	Great Wall	Manufacturer	Great Wall
Model	CRP51600D2	Model	CRPS1600D2
Serial Number	22M010012057	Serial Number	22M010012059
Production Date	220108	Production Date	220108
Firmware Version	DC:1.04 PFC:1.01	Firmware Version	DC:1.04 PFC:1.01
Temperature Range(°C)	0~55	Temperature Range(°C) 0~55
Current Temperature(°C)	41	Current Temperature(*	C) 35
Max Output Power(W)	1600	Max Output Power(W)	1600
Current Input Power(W)	262	Current Input Power(W	/) 291
Current Output Power(W)	250	Current Output Power	(W) 272
Current Input Voltage(V)	233	Current Input Voltage(V) 235
Current Output Voltage(V)	12.23	Current Output Voltage	e(V) 12.23

Figure 5-17 Power Supply Information Tab



The power supply input modes include: AC, HVDC and LVDC. For the R6900 G5 model, **Power Supply Information** also includes the power supply information about the GPU module.

5.13 Configuring the Power Mode

Abstract

The server power modes include:

• Load Balancing: The power modules supply power in load-balancing mode.

• Active/Standby: The power modules supply power in active/standby mode.

A proper power mode enables the power modules to supply power to the server in a reasonable manner.

Steps

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
- 3. Click Power Supply Information. The Power Supply Information tab is displayed.
- Click Power Mode Setting. The Power Mode Setting tab is displayed, see Figure 5-18.
 Figure 5-18 Power Mode Setting Tab

Power			
Power Control	Power Supply Information	Power Consumption	Key Performance Indicator
Power Supply Inform	nation Power Mode Setting		
Mainboard Power	Supply		
	Set Work Mode O Load Balancin	g 🔿 Active/Standby	
	Save		
	- Sano		

Note

For the R6900 G5 model, **Power Mode Setting** also includes power mode setting for the GPU module.

5. Select a power mode.



The **Active/Standby** mode can be selected only when two or more power modules are present and in **Normal** state.

6. Click Save.

5.14 Querying Power Statistics

Abstract

By querying power statistics, you can learn about the current power status of the server and the power changes within the specified time period.

Steps

- 1. Select **System**. The **System** page is displayed.
- 2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
- Click Power Consumption. The Power Consumption tab is displayed, see Figure 5-19.
 Figure 5-19 Power Consumption Tab

ower Control Pow	er Supply Information	Power Consumption	Key Performance Indicator		
vstem Power Statistics	System Power Control		Reg renormance indicator		
ower Status	PTI/A				
	BIOM			2/2 1/2	
Current Power	357 W		Current CPU Power	242 W	
Peak Power	446 W Generation tin 10:17:10	ie: 2024-01-11	Current Memory Power	4 W	
Average Power	357 W		Current Fan Power	12 W	
			Current Disk Power	9 W	
wer History W	BTU/h	Aonth	-0	- Realtime Power -O- Maximum -O- Minimum -O-	Average Power
ower History W Last Hour Last 24 H	BTU/h ours Last Week Last I	Aonth	-0	Realtime Power Maximum Power	Average Power
UNACTOR OF CONTRACT OF CONTRACT.	BTU/h	Ionth	~	- Realtime Power -O- Maximum -O- Power -O-	Average Power
Last Hour Last 24 H	BTU/h	Aonth	~	- Realtime Power -O- Maximum -O- Power -O-	Average Power
Last Hour Last 24 H	BTU/h	Aonth		Realtime Power - Maximum - Minimum	Average Power
ower History W Last Hour Last 24 H 00 W Image: Comparison of the second	BTU/h	Aonth		- Realtime Power -O- Maximum -O- Power -O-	Average Power

Note

- The current power statistics of the server are displayed in the Power Status area.
- The historical power statistics of the server are displayed in the **Power History** area. You can specify a time range to query the corresponding power statistics.

5.15 Configuring Power Control Parameters

Abstract

The power control parameters include:

- **Power Capping**: The server power is limited to the power cap.
- **Power Threshold**: An alarm is raised when the server power exceeds the threshold.

This procedure describes how to configure the power control parameters.

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
- 3. Click Power Consumption. The Power Consumption tab is displayed.
- Click System Power Control. The System Power Control tab is displayed, see Figure 5-20.

Figure 5-20 System Power Cont	rol Tab
-------------------------------	---------

Power			
Power Control Pow	er Supply Information	Power Consumption	Key Performance Indicator
System Power Statistics	System Power Control		
Power Capping			
Power Capping	\bigcirc		
Power Cap Value	500		W
	Save		
Power Threshold			
Power Threshold	\bigcirc		
Power Threshold Value	500		W
	Save		

5. Perform the following operations as required.

То	Do
Set the power cap	 a. In the Power Capping area, turn on the Power Capping switch. b. In the Power Cap Value text box, set the power cap (range: 1–32767, unit: W). c. Click Save.
Set the power threshold	 a. In the Power Threshold area, turn on the Power Threshold switch. b. In the Power Threshold Value text box, enter the power threshold (range: 5–32767, unit: W). c. Click Save.

5.16 Querying Power KPIs

Abstract

Input voltage and output voltage of a server are KPIs related to power modules and energy consumption of the server. By querying these KPIs, you can learn about power supply during the operation of the server.

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
- 3. Click **Key Performance Indicator**. The **Key Performance Indicator** tab is displayed, as shown in Figure 5-21.

SU Input Vo	Itage									Export
PSU1 P	SU2					<u> </u>	225.25	Maximum	A Minimum	Average
Last Hour	Last 24 Hours	Last Week	Last Month			Curren		Value	Value	Value
50 V										_
00 V										
50 V										
V 00										
50 V								1	÷	
0.1										
2024-01-11 09:43:22	2024-01-11 09:49:56	2024-01-11 09:56:30	2024-01-11 10:03:04	2024-01-11 10:09:38	2024-01-11 10:16:12	2024-01-11 10:22:46	2024-01-11 10:29:20	2024-01-11 10:35:54	2024-01-11 10:42:28	2024-01 10:49:0
SU Output	/oltage									-
PSU1 P	SU2									Export
Last Hour	Last 24 Hours	Last Week	Last Month			Curre	ent Value 12.19	-O- Maximum Value	-O- Minimum -	- Average Value
4 V										
2 V										
2 V 0 V										
2 V 0 V 8 V										
2 V 0 V 8 V 6 V										

Figure 5-21 Key Performance Indicator Tab

4. Select a granularity period for a query.

Note

The data on the tab is automatically refreshed after the granularity period is selected.

5. (Optional) To export data, click Export.

5.17 Configuring Boot Options

Abstract

This procedure describes how to configure the boot device, boot mode, and boot option effectiveness for the server.

- 1. Select System. The System page is displayed.
- 2. From the navigation tree in the left pane, select **System Settings**. The **System Settings** page is displayed, see Figure 5-22.

Figure 5-22 System Settings Page

stem Settings		
Boot Options Board Par	el Uart Config	
 Startup settings are valid for 	permanent use and require administrator privileges to configure.	
Boot Option	Hard Drîve	0
Boot Mode	No Override	3
Current Boot Mode	UEFI	
Effective	One-time OPermanent	
	Save	

3. Set the parameters. For a description of the parameters, refer to Table 5-4.

Parameter	Setting
Boot Medium	 Select the device used to boot the server. No Override: configures no boot device and uses the default boot device configured in the BIOS. Hard Drive: forcibly boots from a hard drive. PXE: forcibly boots from the PXE. CD/DVD: forcibly boots from the CD-ROM or DVD-ROM drive. • BIOS Setup: enters the BIOS menu after the server is booted. FDD/Removable Device: forcibly boots from a floppy drive or removable device (for example, USB).
Parameter	Setting
Boot Mode	 Select a server boot mode. No Override: No server boot mode is set. The default server boot mode set in BIOS prevails. Legacy: a traditional boot mode with certain limitations, which supports the PXE boot only through a CPU-connected NIC. UEFI: a newer boot mode, which supports the PXE function in an IPv6/IPv4 network and provides the UEFI Shell environment. UEFI mode is recommended.

Table 5-4 Boot Option Parameter Descriptions

Effective	Select whether the reconfigured server boot options are applied to the current
	restart only.
	• One-time : only effective for the current restart.
	• Permanent : permanently effective.

4. Click Save.

5.18 Configuring the Serial Port Output Mode

Abstract

In common cases, the serial port output modes on the panel include:

- COM0: The recorded information in the BIOS phase is output, which can be configured in the BIOS.
- COM1: There is no output in the BIOS phase and the system hot key cannot be responded. The recorded information in the OS phase is output.



The servers of the HG4 model supports only COM0 mode.

For servers of the ARM model (such as, R5310 G3), the serial port output modes of CPUs in different power-on phases of a host are different and include UEFI/OS, ATF, CPU0SCP0, and CPU1SCP0.



This procedure uses a server of non-ARM model as an example.

- 1. Select **System**. The **System** page is displayed.
- 2. From the navigation tree in the left pane, select **System Settings**. The **System Settings** page is displayed.
- 3. Click **Board Panel Uart Config**. The **Board Panel Uart Config** tab is displayed, see Figure 5-23.

4. Figure 5-23 Board Panel Uart Config Tab

Boot Options	Board Panel Uar	t Config	
	Uart Mode	О СОМО	О сом:
		C	

- 5. Select a serial port output mode.
- 6. Click Save.

Chapter 6 Diagnosis and Maintenance

Table of Contents

Querying Alarms	91
Alarm Reporting Parameter Configuration	92
Configuring Screen Recording Parameters	99
Viewing Recorded Videos	101
Taking a Screenshot	102
Viewing POST Codes	103
Downloading Server Logs	104
Querying BMC Logs	105
Querying SEL Logs	106
Querying Memory Health Scores	107

6.1 Querying Alarms

Abstract

By querying alarms, you can learn about the active alarms and system events of the server. System events include notifications and cleared alarms.

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **Alarm & Event**. The **Alarm & Event** page is displayed, see Figure 6-1.

larm	of Event							
Curr	ent Alarms	System Events						
Dow	nioad Alarms	Total: 4 🔇 2 🔇 1 🔇 1				Search	Adva	nced Query
No.	Severity	Alarm Name	Description	Generation Time	Object Type	Position	Event Code	Handling Suggestions
4	O 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	O 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	OMinor	Redundancy Lost	PS_Redundant Redundancy Lost assert.	2023-05-23 16:37:18	PSU	PSU_0	0x0a0b0801	Details

3. Perform the following operations as required.

то	Do
Query alarms by keyword	In the Search box, enter a keyword.
Query alarms based on the advanced parameters	 a. Click Advanced Query. Advanced query conditions are displayed. b. Set the query parameters. c. Click Query.
View the handling suggestions for an alarm	Click Details for the alarm.
Save alarm information to the local PC	Click Download Alarms .
Query system events	Click System Events. The System Events tab is displayed.

6.2 Alarm Reporting Parameter Configuration

Alarms can be reported in the following ways:

- Reported through trap packets
 For how to configure trap notification parameters, refer to 6.2.1 Configuring Trap Notification
 Parameters.
- Reported through syslog packets

For how to configure syslog notification parameters, refer to 6.2.2 Configuring Syslog Notification Parameters.

Reported through emails
 For how to configure email notification parameters, refer to 6.2.3 Configuring Email
 Notification Parameters.

6.2.1 Configuring Trap Notification Parameters

Abstract

Trap notification parameters are used by the BMC to report alarms to a third-party NMS through traps.



Trap notification parameters are provided by the third-party NMS, so the values of trap notification parameters set on the Web portal of the BMC must be the same as those on the third-party NMS.

Abstract

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed, see Figure 6-2.

Figure 6-2 Alarm Settings Page

Alarm Set	tings					
Trap Noti	ification S	yslog Notification E	nail Notification			
rap Funct	tion					
	Trap					
	Trap Version	V2C		~		
	Select V3 User	Administrator		~		
C	ommunity Name	public				
Confirm C	ommunity Name	public				
	Trap Host ID	Host Name ~		~		
Eve	nt Sending Level	Critical		~		
rap Serve	er Configuration	Save				
No.	Server Ad	ldress	Trap Port		Current Status	Operation
	10.239.212	2.117	323		Disabled	Edit Test
2	10.230.19.	204	162		Enabled	Edit Test
1	10.239.21	1.53	53		Enabled	Edit Test
ŧ	10.239.166	5.158	162		Enabled	Edit Test

3. Set the parameters in the Trap Function area. For a description of the parameters, refer

to Table 6-1.

Parameter	Setting
Тгар	Turn on the Trap switch.
Trap Version	Select the SNMP version for traps. Options: V1 , V2C , and V ¹ .
Parameter	Setting
Select V3 User	This parameter is required if Trap Version is set to V3 . Select a user that has permission to send alarms through SNMP. For how to create an SNMP user, refer to "4.16 Creating an SNMP User".
Community Name	This parameter is required if Trap Version is set to V1 or V2C . Enter the trap community name.
Confirm Community Name	This parameter is required if Trap Version is set to V1 or V2C . Enter the trap community name.
Trap Host ID	Select the identifier of the host that reports alarms.
Event Sending Level	Select the level of events to be reported. For example, if Event Sending Level is set to Critical , only critical alarms are reported.

Table 6-1 Trap Function Parameter Descriptions

- 4. Click Save.
- 5. Set the parameters in the **Trap Server Configuration** area. For a description of the parameters, refer to Table 6-2.

Parameter	Setting
Server Address	After you click Edit , the parameter is activated. Enter the address of the server that receives alarms. An IPv4 address, IPv6 address, or domain name is supported.
Trap Port	After you click Edit , the parameter is activated. Enter the port number of the server that receives alarms. Range: 1– 65535.
Current Status	After you click Edit , the parameter is activated. Select whether to enable the current server to receive alarms.

Table 6-2 Parameter Descriptions for Trap Server Configuration

6. Click Save.

III Note

After the Edit button is clicked, it is changed to the Save button.

7. (Optional) To send a test event to the server, click Test.



If a message indicating "sent successfully" is displayed on the page, the trap is sent successfully.

6.2.2 Configuring Syslog Notification Parameters

Abstract

This procedure describes how to configure syslog notification parameters so that the BMC can send logs to the syslog server. The sent logs include:

- **Operation Log**: records the information about users' operations on hardware devices, including manual operations and remote operations.
- Audit Log: records users' login to and logout of the Web portal of the BMC, BMC, and KVM.
- Event Log: records log and alarm information generated during the operation of the server.

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed.
- 3. Click Syslog Notification. The Syslog Notification tab is displayed, see Figure 6-3.

Figure 6-3 Syslog Notification Tab

Alarm : Trap I	Settings Notification Syslog	Notification Email Notifi	ation			
Syslog	Function					
	Syslog					
	Syslog Server Identity	Host Name		w.		
	Transport Protocol	O TCP O UDP O TLS				
	Authentication Mode	O Unidirectional Authentication	• Two-way Authentication			
	Upload certificate	CA certificate file Certi	ficate FILE Private key			
Syslog	Server Configuration	Save				
No.	Server Address		Port	Log Type	Current Status	Operation
1	195.196.1.12		514	🕑 Operation Logs 🛃 Audit Logs	Event Logs	Save Cancel
2						Edit Test
3						Edit Test
4						Edit Test

4. Set the parameters in the Syslog Function area. For a description of the parameters, refer to Table 6-3.

Parameter	Setting
Syslog	Turn on the Syslog switch.
Syslog Server Identity	Select the identifier of the syslog server to which logs are sent.
Transport Protocol	Select a log transmission protocol.
Parameter	Setting
Authentication Mode	 When Transport Protocol is set to TLS, this parameter should be configured. You can select unidirectional authentication or two-way authentication for TLS. Unidirectional Authentication: The server sends a certificate to the Syslog server for unidirectional authentication. Two-way Authentication: The server and the Syslog server exchange certificates mutually for two-way authentication.
Upload certificate	When Transport Protocol is set to TLS , this parameter should be configured. Click the corresponding certificate button and upload the certificate.

Table 6-3 Syslog Function Parameter Descriptions

5. Click Save.

6. Set the parameters in the **Syslog Server Configuration** area. For a description of the parameters, refer to Table 6-4.

Parameter	Setting
Server Address	After you click Edit , the parameter is activated. Enter the address of the syslog server. An IPv4 address, IPv6 address, or domain name is supported.
Port	After you click Edit , the parameter is activated. Enter the port number of the syslog server. Range: 1–65535, default: 514.
Log Туре	After you click Edit , the parameter is activated. Select one or more log types.
Current Status	After you click Edit , the parameter is activated. Select whether to enable the current syslog server to receive logs.

Table 6-4 Syslog Server Parameter Descriptions

7. Click Save.



After the Edit button is clicked, it is changed to the Save button.

8. (Optional) To send a test log to the syslog server, click Test.



If a message indicating "sent successfully" is displayed on the page, the test log is sent successfully.

6.2.3 Configuring Email Notification Parameters

Abstract

This procedure describes how to configure email notification parameters so that the BMC can send emails to the specified mailbox.

Prerequisite

An SMTP server is already deployed. For details, refer to 4.10 Configuring an SMTP Server.

Abstract

1. Select Maintenance. The Maintenance page is displayed.

- 2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed.
- 3. Click Email Notification. The Email Notification tab is displayed, see Figure 6-4.

Figure	6-4	Email	Notification	Tab

Alarm Settings						
Trap Notification	Trap Notification Syslog Notification Email Notification					
SMTP Function	SMTP Function					
SMTP Ser	rver Address	10.239.212.117				
SMTP	Server Port	25				
	TLS	\bigcirc				
Mail Information						
Use	Anonymous					
Sender	r User Name	Please enter.				
Send	ler Password	Please enter.				
Sender Er	mail Address	Please enter.				
Mess	sage Subject	Server Alert				
Subje	ect Attached	Board Serial Number Product Asset Tag	Host Name			
		Save				
Email Address For	Email Address For Receiving Alarm					
No.	Mailing Add	lress	Description	Current Status	Operation	
1	test@vantage	eo.com	test	Enabled	Edit Test	
2	test01@vanta	ageo.com	123456789	Enabled	Edit Test	
3					Edit Test	
4					Edit Test	

4. Set the parameters in the **SMTP Function** area. For a description of the parameters, refer to Table 6-5.

Parameter	Setting
SMTP	Turn on the SMTP switch.
Parameter	Setting
SMTP Server Address	Enter the IP address of the SMTP server in IPv4 or IPv6 format.
SMTP Server Port	Enter the port number of the SMTP server. Range: 1–65535, default: 25.
TLS	Select whether to enable the encryption function.
Use Anonymous	Select whether emails are sent anonymously.
Sender User Name	Required if the Use Anonymous switch is turned off. Enter the username for SMTP authentication.

Table 6-5 SMTP Function Parameter Descriptions

Sender Password	Required if the Use Anonymous switch is turned off. Enter the password of the email sender.
Sender Email Address	Enter the email address of the sender.
Message Subject	Enter the subject of alarm emails.
Subject Attached	Select the information to be attached to the email subject. One or more options can be selected.

- 5. Click Save.
- 6. Set the parameters in the **Email Address For Receiving Alarm** area. For a description of the parameters, refer to Table 6-6.

Table 6-6 Mailbox Address Parameter Descriptions

Parameter	Setting
Mailing Address	After you click Edit , the parameter is activated. Enter the email address to which alarms are sent.
Description	After you click Edit , the parameter is activated. Enter the description of the email address.
Current Status	After you click Edit , the parameter is activated. Select whether to enable the current email address to receive alarms.

7. Click Save.



After the Edit button is clicked, it is changed to the Save button.

8. (Optional) To send a test alarm email to the email address, click Test.



If a message indicating "sent successfully" is displayed on the page, the alarm email is sent successfully.

6.3 Configuring Screen Recording Parameters

Abstract

By configuring screen recording parameters, you can specify the events that trigger screen recording and the recording duration.

The recorded videos can be viewed on the Screenshot&Video page.

Prerequisite

Before enabling the screen recording function, you need to enable the KVM service. For details, refer to "7.3 Configuring KVM Service Parameters".

III Note

The launch of a KVM or VNC session temporarily disables recording. After the KVM or VNC session is closed, recording is automatically resumed.

Steps

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **Screenshot&Video**. The

Screenshot&Video page is displayed, as shown in Figure 6-5.

5creenshot&Video		
Video playback		Configur
Restart recording	Restart recording	Restart recording
0	0	0
re reset video O.dat ue Apr 2 14:58:05 2024	pre reset video 1.dat Tue Apr 2 1457.45 2024	pre_reset_video_2_dat Tue Apr 2 14:57:27 2024
Auto Screenshot	Manual Screenshot Screenshot Delete	
2021-07-25 21:50:36		
2021-07-21 20:31:03		
· · · · · · · · · · · · · · · · · · ·	No Screenshot	

3. Click **Configuration** in the upper right corner. The **Video recording function configuration** dialog box is displayed, as shown in Figure 6-6.

Video recording function	configurat	ion	
Video recording fun	nction enabling		
Recording time	10		
Video type	Pre-crash	Pre-poweroff	Pre-restart
	Submit	Cancel	

Figure 6-6 Video Recording Function Configuration Dialog Box

4. Set the parameters. For a description of the parameters, refer to Table 6-7.

Parameter	Description
Video recording function enabling	Turn on the toggle switch.
Recording time	Enter the screen recording duration. Options: 10, 20, 30, 40, 50, and 60. Unit: seconds.
Video type	Select the events that trigger screen recording.

Table 6-7 Parameter Descriptions for the Screen Recording Function

5. Click Submit.

6.4 Viewing Recorded Videos

Abstract

After the screen recording function is enabled, the system automatically records the screen in accordance with the configured recording parameters before the server crashes, restarts, or powers off. You can view the recorded videos for fault diagnosis.

Prerequisite

The screen recording function is enabled. For details, refer to "6.3 Configuring Screen Recording Parameters".

Steps

1. Select Maintenance. The Maintenance page is displayed.

 From the navigation tree in the left pane, select Screenshot&Video. The Screenshot&Video page is displayed, as shown in Figure 6-7.

Screenshot&Video		
Video playback		Configuratio
Restart recording	Restart recording	Restart recording
0	0	0
pre_reset_video_0.dat Tue Apr 2 14:58:05 2024	pre_ireset_video_1_dat Tuei Apr 2 1457:45 2024 (Tueinte)	pre_reset_video_2.dat Tue Apr 2 1457:27 2024
Auto Screenshot	Manual Screenshot Screenshot Delete	
 2021-07-25 21:50:36 		
2021-07-21 20.31.03		
No Data	No Screenshot	

Note

The Video playback area displays the latest three recorded videos.

3. Click to play a recorded video.

6.5 Taking a Screenshot

Abstract

The screenshot function is used for fault diagnosis.

III Note

Before using the screenshot function, you must disable the KVM function.

Screenshots can be taken in the following ways:

Automatic

Automatic screenshot is triggered when one of the following conditions is met:

```
→ The server is restarted after a fatal error (for example, a CPU fault)
```

occurs. → The BMC triggers Power Reset. → The BMC triggers Power

Cycle. \rightarrow The BMC triggers **Forced Power Off**.

For a description of the power operations that can be triggered by the BMC, refer to 5.8 Powering On/Off the Server.

Manual

Steps

- 1. Select Maintenance. The Maintenance page is displayed.
- From the navigation tree in the left pane, select Screenshot&Video. The Screenshot&Video page is displayed, see Figure 6-8.

Screenshot&Video		
Video playback		Configure
Restart recording	Restart recording	Restart recording
0	0	0
pre_reset_video_0.dat Ture Apr 2 1458:05 2024	pre reset video 1 dat Ture Aor 2 143745 2024	pre_reset_video_2.dat Tue Apr 2 1457:27 2024 Double
Auto Screenshot	Manual Screenshot Screenshot Delete	
 2021-07-25 21:50:36 		
2021-07-21 20:31:08		
100	No Ermenter	

3. Perform the following operations as required.

То	Do
Take screenshots automatically	Turn on the Last Screen switch.
Take a screenshot manually	Click Screenshot . The screenshot of the current screen is displayed at the bottom of the page. To delete the current screenshot, click Delete .

6.6 Viewing POST Codes

Abstract

The POST code records the status of the server during power-on.

Check the POST code for fault diagnosis.

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **POST Code**. The **POST Code** page is displayed, see Figure 6-9.

POST Code	
POST Code	
POST Code	
	Save
Details	
Server Power Status	• On
Current POST Code	50 10 01 02 02 03 03 04 04 05 06 05 03 03 23 23 00 02 7f 48 0e 49 4a 4d 15 52 55 19 31 00 a1 a3 a3 a3 a3 a3 a3 a3 a7 a9 a9 a2 a2 ab ab a
	a7 a7 a7 a7 a9 a9 a9 a8 aa ae e0 e0 e0 e1 e4 e3 e5 af af b0 bf b5 b0 7e cf 7e cd b0 7e b0 c1 70 b1 b1 b1 7e b4 b4 b4 c2 7e b0 70 7e 7e b1
	c4 b1 b1 b1 b1 b6 7e b0 b4 7e b4 b4 b4 b8 c5 b2 c6 b3 b3 b6 b6 b6 b6 b6 b7 b6 b7 b6 b6 7e b0 7e 7e b1 b7 b7 b6 b6 b7 b7 b7 b7 b7 b7
	67 67 67 67 67 67 67 67 67 67 67 67 67 6
	b7 b
	7e b0 b7 b7 be be 7e 7e b0 d2 7e d2 d6 70 b9 b9 b9 b9 7e b7 b7 b7 b7 b8 b8 b8 d7 c9 da d9 db ba b9 70 70 7e 70 7e 70 7e 7e cb bb
	bb
	af af af af af af e6 e7 e9 eb ec ed ee 03 23 02 22 00 02 7f 48 0e 49 4a 4d 15 52 55 02 22 00 04 06 0b 0c 0d 15 7f 00 7f 40 41 42 47 4f 33 60 6
	68 70 79 90 91 92 94 94 94 94 94 94 94 94 94 94 94 94 94
	92 92 92 92 92 92 92 92 92 92 92 92 92 9
	98 92 a0 a2
	92 92 b6 ad
Last POST code	10 01 02 02 03 03 04 04 05 06 05 03 03 23 23 00 02 7f 48 0e 49 4a 4d 15 52 55 19 31 00 a1 a3 a3 a3 a3 a3 a3 a3 a7 a9 a9 a2 a2 ab ab ab a
	a7 a7 a7 a9 a9 a9 a8 aa ae e0 e0 e1 e4 e3 e5 af af b0 bf b5 b0 7e cf 7e 73 cd b0 7e b0 c1 70 b1 b1 b1 7e b4 b4 b4 c2 7e b0 70 7e 7e b
	b1 b1 b1 b1 b6 7e b0 b4 7e b4 b4 b4 b8 c5 b2 c6 b3 b3 b6 b6 b6 b6 b0 b7 b6 b6 7e b0 7e 7e 7e b1 b7 b7 b6 b6 b7 b7 7e 70 70 7e 70
	70 7e b7 7e b0 b7 b7 be be 7e 7e b0 d2 7e d2 d6 70 b9 7e b7 b7 b7 b7 b8 b8 b8 d7 c9 da d9 db ba b9 70 70 7e 70 70 7e 70 7e 7e cb bb
	bb
	af af af af af af e6 e7 e9 eb ec ed ee 03 23 02 22 00 02 7f 48 0e 49 4a 4d 15 55 02 22 00 04 06 0b 0c 0d 15 7f 00 7f 40 41 42 47 4f 33 60 61 6
	70 79 90 91 92 94 94 94 94 94 94 94 94 94 94 94 94 94
	92 92 92 92 92 92 92 92 92 92 92 92 92 9
	92 a0 a2 a2 a2 a2 a0 a2 99 92 92 92 a4 a6 a7 a7 a7 a7 a7 a7 a7 92 92 92 92 92 92 92 92 92 92 92 92 92
	92 b3

Figure 6-9 POST Code Page

- 3. (Optional) If the POST code is not enabled, open **POST Code** and click **Save**.
- 4. View Server Power Status, Current POST Code, and Last POST Code.

6.7 Downloading Server Logs

Abstract

When a fault occurs, the server logs are written to the serial port. You can download these logs for fault diagnosis.

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **Host Logs**. The **Host Logs** page is displayed, see Figure 6-10.

Figure 6-10 Host Log Page

Host Logs
Host Serial Port Logs
1 Please wait for the BIOS startup to complete before downloading the log, in case the data is incomplete, and the name of the downloaded file contains the 'product serial number'.
Download

3. Click Download.

6.8 Querying BMC Logs

Abstract

BMC logs include:

- **Operation Logs**: record the information about users' operations on the server, including manual operations and remote operations.
- Audit Logs: record users' login to and logout of the Web portal of the BMC, BMC, and KVM.

Steps

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **BMC Logs**. The **BMC Logs** page is displayed, see Figure 6-11.

Figure 6-11 BMC Logs Page

BMC Lo	gs					С	
1 The	page only displays about 100	0 logs generated recently. T	o view all the logs, please downloa	d the logs to view them locally.			
Operat	ion Logs Audit Logs						
Downlo	ad Logs				Q :	Search(Fuzzy search only s	
No. 🗘	Generation Time 💠	Interface	User	Address	Details		
112	2024-03-07 14:10:27	WEB	Administrator	10.	set time zone (Asia/Shanghai) successfully.		
111	2024-03-07 14:10:27	WEB	Administrator	10.	disable NTP Server successfully.		
110	2024-03-07 14:10:22	WEB	Administrator	10.	set bmc time to 2024-03-07 14:10:22 succes	isfully.	
109	2021-06-29 20:54:36	WEB	Administrator	10.	set asset tag: 21900000000 successfully		
108	2021-06-29 20:36:52	WEB	Administrator	10.	set asset tag: 21900000000 successfully		
107	2021-06-21 03:09:55	WEB	Administrator	10.	control chassis power on successfully.		
106	2021-06-20 21:07:21	REDFISH	Administrator	10.	control chassis power cycle successfully.	control chassis power cycle successfully.	
105	2021-06-20 21:07:07	N/A	N/A	N/A	upgrade BIOS successfully.		
104	2021-06-20 20:52:48	N/A	N/A	N/A	upgrade BIOS with preserve configuation su	accessfully.	
103	2021-06-20 20:52:47	REDFISH	N/A	N/A	begin upgrade BIOS successfully.		
				Total 112 K <	1 2 3 4 5 > X 10/	Page - To 1 Page	

3. Perform the following operations as required.

То	Do
Query operation logs	 a. Click Operation Logs to switch to the Operation Logs tab. b. (Optional) In the Search box, enter a keyword. c. (Optional) Click Download Logs.
Query audit logs	 a. Click Audit Logs to switch to the Audit Logs tab. b. (Optional) In the Search box, enter a keyword. c. (Optional) Click Download Logs.

6.9 Querying SEL Logs

Abstract

The SEL logs record event logs reported by sensors in the server system.

- 1. Select Maintenance. The Maintenance page is displayed.
- 2. From the navigation tree in the left pane, select **SEL Logs**. The **SEL Logs** page is displayed, see Figure 6-12.

EL Logs					
Download S	EL Logs Clear SEL Logs			Q Search	Advanced Quer
Event ID 💠	Generation Time 💠	Sensor Name	Sensor Type	Description	Status
67	2023-07-20 09:21:53	BMC_BOOT_UP	System Boot/Restart Initiated	Initiated by hard reset	Asserted
66	2023-07-20 09:21:53	ACPI_STATUS	System ACPI Power State	S0/G0 'working'	Asserted
65	2023-07-20 09:20:14	System	Version Change	Software or F/W Change detected with associated En successful.(deassertion event means 'unsuccessful')	ntity was Asserted
64	2023-07-20 09:19:00	System	Version Change	Firmware or software change detected with associate Entity.Informational. Success or failure not implied	ed Asserted
63	2023-07-19 15:59:50	SYS_RESTART	System Boot/Restart Initiated	Initiated by warm reset	Asserted
62 2023-07-19 15:59:48		ACPI_STATUS	System ACPI Power State	50/G0 'working'	Asserted
61	2023-07-19 15:59:41 OS_STOP OS Stop / Shutdown OS Graceful Shutdown		OS Graceful Shutdown	Asserted	
60	2023-07-19 15:59:41	ACPI_STATUS	System ACPI Power State	S5/G2 'soft-off'	Asserted
59	2023-07-19 15:57:30	ACPI_STATUS	System ACPI Power State	S0/G0 'working'	Asserted
58	2023-07-19 15:57:23	OS_STOP	OS Stop / Shutdown	OS Graceful Shutdown	Asserted

- 3. (Optional) Click Advanced Query, set the query conditions, and click Query.
- 4. Perform the following operations as required.

То	Do
Download SEL Logs	Click Download SEL Logs.

Clear SEL Logs

Click Clear SEL Logs.

6.10 Querying Memory Health Scores

Abstract

You can query memory health scores through the memory fault prediction function to learn about the operational status of memory.

Note

The memory fault prediction function is disabled by default. To enable this function, run the corresponding IPMI commands.

Steps

- 1. Select Maintenance. The Maintenance page is displayed.
- From the navigation tree in the left pane, select Memory Fault Prediction. The Memory Fault Prediction page is displayed, as shown in Figure 6-13.

		Memory Fault Prediction								
emory Index 🌲	CPU Slot Number 💠	Controller Number 💲	Channel Number 💲	Slot ‡	Slot Identification \ddagger	SN Number 👙	Health Score 💲			
				_						
			.0							
			The second se							

3. Check memory health scores.

Chapter 7 Service Management

Table of Contents

Configuring Port Service Parameters	108
Configuring Web Service Parameters	110
Configuring KVM Service Parameters	112
Starting the KVM	114
Configuring Virtual Media Parameters	122
Mounting a Virtual Media Device	124
Configuring VNC Parameters	125
Configuring SNMP Parameters	127

7.1 Configuring Port Service Parameters

Abstract

By configuring port service parameters, you can configure the status, secure port, non-secure port, and timeout period of each service of the BMC.

The parameters configured on the **Port Services** page are synchronized with the parameters configured on the following pages:

- Web Services page
 Virtual Console page
 Virtual Media page
- VNC page
- SNMP page

- 1. Select Services. The Services page is displayed.
- From the navigation tree in the left pane, select **Port Services**. The **Port Services** page is displayed, see Figure 7-1.
| Figure | 7-1 | Port | Servi | ces | Page | |
|--------|-----|------|-------|-----|------|--|
| | | | | | | |

Port S	'ort Services						
No.	Name	Status	Non Secure Port	Secure Port	Timeout(Min)	Maximum Sessions	Operation
1	web	Open	80	443	30	20	Edit
2	kvm	Open	7578	7582	30	4	Edit
3	cd-media	Open	5120	5124	**/	1	Edit
4	hd-media	Open	5123	5127	37 4	1	Edit
5	ssh	Open	102	22	10		Edit
6	vnc	Open	5900	5901	10	2	Edit
7	snmp	Open	161		55%	1055	Edit
8	redfish	Open	1771		274	1000	Edit
9	ipmi	Open	:02	623	225		

- 3. Click **Edit** for a service to activate the parameters.
- 4. Set the parameters. For a description of the parameters, refer to Table 7-1.

Parameter	Setting
Status	Select whether to enable a service.
Non Secure Port	 Enter the non-secure port number of the service. Default non-secure port number of the Web service: 80. Default non-secure port number of the KVM service: 7578. Default non-secure port number of the CD media service: 5120. Default non-secure port number of the HD media service: 5123. Default non-secure port number of the VNC service: 5900. Default non-secure port number of the SNMP service: 161. Other services do not support non-secure ports. Range of the non-secure port numbers: 1–65535.
Secure Port	 Enter the secure port number of the service. Default secure port number of the Web service: 443. Default secure port number of the KVM service: 7582. Default secure port number of the CD media service: 5124. Default secure port number of the HD media service: 5127. Default secure port number of the SSH service: 22. Default secure port number of the VNC service: 5901. Default secure port number of the IPMI service: 623. Other services do not support secure ports. Range of the secure port numbers: 1–65535.
Timeout(Min)	Timeout period after which the service exits if no operation is performed. Enter the timeout period (in minutes). Range: 5–60 (for the VNC service) or 1–60 (for other services).

Table 7-1 Port Service Parameter Descriptions



You cannot configure the Maximum Sessions parameter.

5. Click Save.

7.2 Configuring Web Service Parameters

Abstract

By configuring the Web service parameters, you can securely access the Web portal of the BMC through the local PC.

To configure the Web service parameters, perform the following operations:

- 1. Configuring basic parameters
- 2. Uploading the SSL certificate to the browser
- 3. Uploading the SSL certificate to the Web portal of the BMC

Prerequisite

The pem file (containing the certificate file and private key file) is already obtained.

Steps

Configuring Basic Parameters

- 1. On the Web portal of the BMC, select Services. The Services page is displayed.
- 2. From the navigation tree in the left pane, select **Web Services**. The **Web Services** page is displayed, see Figure 7-2.

Web Services			
Basic Configuration			
HTTP			
HTTP Port	80		
HTTPS			
HTTPS Port	443		
Timeout Period	20	Min	
Active Sessions	4		
	Save		
SSL Certificate			

Figure 7-2 Web Services Page

3. Set the parameters. For a description of the parameters, refer to Table 7-2.

Parameter	Setting
НТТР	Turn on the HTTP switch.
HTTP Port	Enter the non-secure port number of the Web service. Range: 1–65535, default: 80.
HTTPS	Turn on the HTTPS switch.
HTTPS Port	Enter the secure port number of the Web service. Range: 1–65535, default: 443.
Timeout Period	The Web service exits if no operation is performed within the specified timeout period. Enter the timeout period. Range: 1–60, unit: minutes.

Table 7-2 Basic Parameter Descriptions

Uploading the SSL Certificate to the Browser

4. On the **Settings** page of the browser (for example, Google Chrome) on the PC, select **Privacy and security**. The **Privacy and security** page is displayed.



Click on the right of **Manage certificates** and upload the SSL certificate.

Uploading the SSL Certificate to the Web Portal of the BMC

 On the Web Services page on the Web portal of the BMC, click Upload SSL. The Upload SSL dialog box is displayed, see Figure 7-3.

Upload SSL	
Current Certificate	Fri Dec 31 16:00:02 1999
New Certificate	Select File
Current Private Key	Fri Dec 31 16:00:02 1999
New Private Key	Select File
	Submit Cancel

- 7. Select the prepared certificate file and private key file.
- 8. Click Submit.

Verification

In the address bar of your browser, enter the address of the Web portal of the BMC, and press **Enter** to see if the login page is displayed directly and there is no "Not secure" warning displayed, see Figure 7-4.

Figure 7-4 Secure Access

https://1)/#login
11(cp3)//1	7 . logi

Figure 7-5 shows the "Not secure" warning displayed in the address bar of the browser.

Figure 7-5 Insecure Access		
▲ Not secure 1	i/#login	

7.3 Configuring KVM Service Parameters

Abstract

Before starting the KVM, you need to configure the KVM service parameters.

Steps

- 1. Select Services. The Services page is displayed.
- 2. From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed, see Figure 7-6.

Figure 7-6 Virtual Console Page

Virtual Console		
Start KVM	HTML Virtual Console Java Virtual Console	
Session Settings		
* (1) Communication Encryption	\Box	
Single Port	0	
Retry Times	3	
Retry Interval	10	5
	Save	

3. Set the parameters in the **Session Settings** area. For a description of the parameters, refer to Table 7-3.

Parameter	Setting
Communication Encryption	Select whether to encrypt KVM communication.
Single Port	 Select whether to use port 443 in a unified manner when the KVM is started in HTML mode. If the Single Port switch is turned on, port 443 is used in a unified manner. If the Single Port switch is turned off, port 443 is not used in a unified manner.
Parameter	Setting
Retry Times	Enter the number of session retires. Range: 1–20.
Retry Interval	Enter the session retry interval. Range: 5–30, unit: seconds.

Table 7-3 Session Setting Parameter Descriptions

4. Click Save.

7.4 Starting the KVM

Abstract

When you are not on the customer site, you can start the KVM to remotely control the server.

Prerequisite

If the KVM needs to be started in Java mode, JRE 8 or a later version (for example, *jre-*8u191) is already installed on the PC.

Steps

- 1. Select Services. The Services page is displayed.
- 2. From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed, see Figure 7-7.

Figure 7-7 Virtual Console Page

Virtual Console		
Start KVM	HTML Virtual Console Java Virtual Console	
Session Settings		
* Communication Encryption	00	
Single Port	0	
Retry Times	3	
Retry Interval	10	5
	Saue	

3. Perform the following operations as required.

Start the KVM in HTML mode a. Click HTML Virtual Console. The Remote KVM (HTML) page is displayed, see Figure 7-8. b. Perform the following operations as required.	то	Do
For a description of the operations, refer to Table 7-4.	Start the KVM in HTML mode	 a. Click HTML Virtual Console. The Remote KVM (HTML) page is displayed, see Figure 7-8. b. Perform the following operations as required. For a description of the operations, refer to Table 7-4.

То	Do
Start the KVM in Java mode	a. In the search box in the lower left corner of the PC, enter Java.
	b. In the search result, select Java. The Java Control Panel dialog box
	is displayed.
	c. Click Security. The Security window is displayed.
	d. Click Edit Site List. The Exception Site List dialog box is displayed.
	e. Click Add to add the address of the Web portal of the BMC.
	f. Click OK to return to the Security window.
	g. Click OK .
	h. On the Virtual Console page of the Web portal of the BMC, click
	Java Virtual Console. A dialog box indicating whether to keep
	jviewer.jnlp is displayed.
	i. Click Keep.
	j. In the lower left corner of the browser, click $\verb"jviewer.jnlp". A dialog$
	box indicating whether to proceed is displayed.
	k. Click Continue. The Do you want to run this application? dialog
	box is displayed.
	I. Select I accept the risk and want to continue to run this app. and
	click Run . The Untrusted Connection dialog box is displayed.
	m. Click Yes. The Remote KVM (JAVA) page is displayed, see Figure 7-
	9.
	n. Perform the following operations as required.
	For a description of the operations, refer to Table 7-5.

Note

Before starting the KVM in one mode, you must disable the KVM in another mode. For example, before starting the KVM in Java mode, you must disable the KVM started in HTML mode.



Table 7-4 Descriptions for the Remote KVM (HTML) Operations

Operation	Description
Stop the KVM	Click Stop KVM to exit the Remote KVM (HTML) page.
Mount a local <i>iso</i> file	 a. Click Browse File next to CD Image, and select the <i>iso</i> file from the PC. b. Click Start Media.
Display the notifications received	Click A.
Lock the display of the server	 Lock the server display through either of the following ways: Click Select Video > Display OFF. After the server display is locked, if another user wants to view a server screen, a permission request is sent to the current active user. The user can view the server screen only after being authorized by the current active user.

Unlock the server display	Unlock the server display through either of the following ways:
	• Click
	• Select Video > Display ON.
	is converted to 😐.

Operation	Description
Pause a remote control screen	Select Video > Pause Video.
Resume a remote control screen	Select Video > Resume Video.
Refresh a remote control screen	Select Video > Refresh Video.
Capture the current screen	Select Video > Capture Screen.
Display or hide the mouse pointer on the server screens	 To display the mouse pointer on the server screens, click Mouse, and select Show Client Cursor. To hide the mouse pointer on the server screens, click Mouse, and clear Show Client Cursor.
Set the mouse mode	Click Mouse , and select Absolute Mouse Mode . In absolute mouse mode, the absolute position of the local mouse is transferred to the server to make the mouse on the server move.
Set keyboard layout	 a. Select Keyboard. b. In the displayed submenu, select the keyboard layout, including English U.S, German and Japanese. English U.S is selected by default.
Set video recording time length	 a. Select Video Record > Record Settings. The Record Settings dialog box is displayed. b. Set the video recording time length with a range of 1–1800 seconds. c. Click OK.
Record videos	Select Video Record > Record Video.
Stop recording	Select Video Record > Stop Recording.
Shut down the server	 Shut down the server through either of the following ways: Select Power > Orderly shutdown. Orderly shutdown. Click

Start the server	 Start the server through either of the following ways: Select Power > Power On Server. Click
Perform a cold reboot	Select Power > Power Cycle Server . Cold reboot means that the server is started after it is shut down. During the restart, the server is offline.
Perform a warm reboot	Select Power > Reset Server . Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.
Operation	Description
View the users that are using remote control	Select Active Users.
Figure 7-9 Remote KVM (Ja	va) Page
Embedded LOM Portl (IPv6 Boot) PXE boot IPv6 boot from device : PciRoot((MAC Address : 20-20-07-09-85 Controller Driver Name : Inf Checking media	Image: Contract of the second seco
	LALT LCTRL RALT RCTRL Num Caps Scroll

Operation	Description
Pause a remote control screen	 Pause a remote control screen through one of the following ways: Select Video > Pause Redirection. Click Press Alt+P.
Resume a remote control screen	 Resume the remote control screen through one of the following ways: Select Video > Resume Redirection. Click Press Alt+R.

Table 7-5 Descriptions for the Remote KVM (JAVA) Operations

Operation	Description
Refresh a remote control screen	 Refresh the remote control screen through either of the following ways: Select Video > Refresh Video. Press Alt+E.
Switch the host screen display mode	 To display the remote screen on the host, select Video > Turn ON Host Display. To not display the remote screen on the host, select Video > Turn OFF Host Display. Note: You can use either of the following methods to rapidly switch between the remote screen display modes of the host. Click Press Alt+N.
Capture the current screen	 Capture the current screen through either of the following ways: Select Video > Capture Screen. Press Alt+S.
Set a video decoding mode	 a. Select Video > Compression Mode. b. Select a video decoding mode from the displayed submenu.
Set the video display quality	 a. Select Video > DCT Quantization Table. b. Select the video display quality from the displayed submenu. The video display quality is divided into eight levels from 0 through 7, with video quality degraded in turn.

Define a key combination	 a. Select Keyboard > Hot Keys > add Hot Keys. The User Defined Macros page is displayed.
	b. Click add. The Add Macros page is displayed.
	C. Press and then release the user-defined key combination.
	d. Click OK .
Enable full keyboard support	 To enable full keyboard support, click Keyboard, and select Full Keyboard Support. To disable full keyboard support, click Keyboard, and clear Full Keyboard Support.
Display or hide the mouse pointer	 To display the mouse pointer, click Mouse, and select Show Client Cursor. To hide the mouse pointer, click Mouse, and clear Show Client Cursor. You can use either of the following methods to rapidly change the mouse display modes on the PC. Press Alt+C. Click
Set the network bandwidth	a. Select Options > Bandwidth .

Operation	Description
	b. Select the desired network bandwidth from the displayed submenu.
Change the encryption status of the mouse/keyboard	 To enable mouse/keyboard encryption, click Options, and select Keyboard/Mouse Encryption. To disable mouse/keyboard encryption, click Options, and clear Keyboard/Mouse Encryption.
Set the scaling mode of a remote screen	 a. Select Options > Zoom. b. In the displayed submenu, set the zoom scale of the remote screen. Zoom In: zooms in the remote screen. Zoom Out: zooms out the remote screen. Actual Size: displays the remote screen in the proportion of 100%. Fit to Client Resolution: displays the remote screen in the resolution of the local client system. Fit to Host Resolution: displays the remote screen in the resolution of the remote screen.

Send an IPMI command to the server	a. Select Options > Send IPMI Command . The IPMI Command Dialog window is displayed.
	b. Enter the IPMI command.
	 C. Click Send. The IPMI command supports hex format and ASCII format.
Set the GUI language	a. Select Options > GUI Languages.
	b. Select the GUI language from the displayed submenu.
Set the privilege request	a. Select Options > Block Privilege Request.
mode	 b. Select a privilege request block mode from the displayed submenu. Allow only Video: The permission for viewing the information
	displayed on the server is automatically granted to the user who initiates a privilege request.
	• Deny Access : Privilege requests in the system are blocked.
Mount a local <i>iso</i> file	 a. Open the Virtual Media window in either of the following ways: Select Media > Virtual Media Wizard, and switch to the CD/ DVD tab. Click
	b. Click Browse and select a local <i>iso</i> file.
	c. Click Connect .
Mount a local folder	a. Create an <i>iso</i> file on the PC.
	 b. Open the Virtual Media window in either of the following ways: Select Media > Virtual Media Wizard, and switch to the Hard Disk/USB tab. Click
	C. Select physical drive > folder path.

Operation	Description
	 d. Click Browse and select a local folder path. e. Set Size and folder path. f. Click Connect. The value of Size must be 2ⁿ, such as 2, 4 and 8. The path specified by folder path needs to be the same as that of the new <i>iso</i> file.
Set keyboard layout	a. Select Keyboard Layout.b. Select the keyboard layout from the displayed submenu.
Open the soft keyboard	Click 🕮.

Configure video recording	 a. Select Video Record > Settings. The Video Record window is displayed. b. Set the video recording time length in seconds and the video storage position. c. Click OK. The video recording time length ranges from 1 through 1800 seconds.
Record videos	 a. Start recording a video in either of the following ways: Select Video Record > Start Record. Click Click Select Video Record a video in either of the following ways: Select Video Record > Stop Record. Click Select recording time length is reached or the recording is stopped manually, click OK. The recorded video file is saved to the <i>VideoCaptures</i> folder in the preset path.
Set the server power mode	 a. Select Power. b. Select a server power option from the displayed submenu. The server power options are as follows: Reset Server: restarts the system without shutting down the power supply (warm reboot). Immediate Shutdown: shuts down the server immediately by shutting down the power supply. Orderly Shutdown: shuts down the server in order through program control. Power On Server: starts the server. Power Cycle Server: shuts down the server and restarts it (cold reboot).
Check active users	Select Active Users to view the users using remote control.

7.5 Configuring Virtual Media Parameters

Abstract

Before mounting a CD/DVD or HD of the PC to the server through the KVM, you must configure virtual media parameters.

Steps

1. Select Services. The Services page is displayed.

2. From the navigation tree in the left pane, select **Virtual Media**. The **Virtual Media** page is displayed, see Figure 7-10.

Figure 7-10 Virtual Media Page

VMedia Entity Settings CD/DVD Physical Device HD Physical Device 1 Remote KVM CD/DVD Physical	. v .
CD/DVD Physical Device 1 HD Physical Device 1 Remote KVM CD/DVD Physical	. Y
HD Physical Device 1 Remote KVM CD/DVD Physical	
Remote KVM CD/DVD Physical	Ŷ
Device 1	
Remote KVM HD Physical Device 1	
Media Redirection Encryption	

3. Set the parameters. For a description of the parameters, refer to Table 7-6.

Parameter	Setting
CD/DVD Physical Device	Select the number of CD/DVD devices on the PC. Keep the default value 1 .
HD Physical Device	Select the number of HD devices on the PC. Keep the default value 1 .
Remote KVM CD/DVD Physical Device	Select the number of CD/DVD devices to be mounted through the KVM. The number cannot exceed the number of CD/DVD physical device. Keep the default value 1 .
Remote KVM HD Physical Device	Select the number of HD devices to be mounted through the KVM. The number cannot exceed the number of HD physical device.
Parameter	Setting
	Keep the default value 1 .
Media Redirection Encryption	Turn off the Media Redirection Encryption switch.

Table 7-6 Parameter Descriptions for VMedia Instance Settings

4. Click Save.

7.6 Mounting a Virtual Media Device

Abstract

This procedure describes how to enable the virtual media function and remotely mount a virtual media device.

Steps

- 1. Select Services. The Services page is displayed.
- 2. From the navigation tree in the left pane, select **Virtual Media**. The **Virtual Media** page is displayed.
- 3. Click Media Mounting. The Media Mounting tab is displayed, as shown in Figure 7-11.

Figure 7-11 Virtual Media Page—Media Mounting Tab

Media Setti	ng Media Mou	nting					
irtual Media En	able						
Start Media Type	Server Address	File Path	Shared File System	Username	Password	Status	Operation
CD/DVD	10.239.20.11	/home/mount_test/isocfg-tool-v1.iso	CIFS ~	test		Disabled	Start Moun
HD	10.320.30.11	(home/mount test/inorfe tool ut ima	NES			Disabled	Start Mount

4. Set the parameters. For a description of the parameters, refer to Table 7-7.

Table 7-7 Parameter Descriptions for Mounting a Virtual Media Device

Parameter	Description
Virtual Media Enable	Turn on the toggle switch. If the Virtual Media Enable switch is turned off, the mounted virtual media devices are cleared.
Start Media Type	The number of virtual media devices in the Start Media Type column must be the same as that of the devices set in Remote KVM CD/DVD Physical Device and Remote KVM HD Physical Device on the Media Setting tab. For example, if Remote KVM CD/DVD Physical Device is set to 1, there is only one CD/DVD entry displayed in the Start Media Type column.
Parameter	Description
Server Address	Enter the IP address of the server that provides the remote image mounting service. Domain names are not supported.

File Path	 Enter the storage path of the image file on the remote server. A maximum of 256 characters can be entered. The name of each mounted image file must be unique. If Start Media Type is CD/DVD, the suffix of the image filename must be <i>iso</i>. If Start Media Type is HD, the suffix of the image filename must be <i>img</i> or <i>ima</i>.
Shared File System	 Select a file system protocol for file sharing. Options: NFS, CIFS, and HTTPS. If Start Media Type is CD/DVD, NFS, CIFS, and HTTPS are supported. If Start Media Type is HD, NFS and CIFS are supported.
Username	Enter the username for logging in to the remote server. This parameter does not need to be set if Shared File System is set to NFS .
Password	Enter the password for logging in to the remote server. This parameter does not need to be set if Shared File System is set to NFS .

5. In the Operation column, click Start Mount for the desired virtual media device.



After the virtual media device is successfully mounted, its status in the **Status** column is changed to **Enabled**.

Related Tasks

To disable a mounted virtual media device, click End Mount in the Operation column for it.

7.7 Configuring VNC Parameters

Abstract

A server can be remotely controlled through the KVM and VNC. Before remotely controlling the server in VNC mode, you must configure the VNC parameters.



For KVM-related parameter configuration, refer to 7.3 Configuring KVM Service Parameters. For KVMbased remote server control operations, refer to 7.4 Starting the KVM. **Steps**

1. Select Services. The Services page is displayed.

2. From the navigation tree in the left pane, select **VNC**. The **VNC** page is displayed, see Figure 7-12.

Figure 7-12 VNC Page
VALC

Secure Port	5901	
Non Secure Port	5900	
Timeout Period	10	Min
Maximum Sessions	2	
Modify Password	00	
Password complexity check	\bigcirc	
Password complexity check VNC Password		
Password complexity check VNC Password Confirm VNC Password		

3. Set the parameters. For a description of the parameters, refer to Table 7-8.

Table 7-8	VNC	Parameter	Descri	ptions

Parameter	Setting
Secure Port	Enter the secure port number of the VNC service. Range: 1–65535, default: 5901.
Non Secure Port	Enter the non-secure port number of the VNC service. Range: 1–65535, default: 5900.
Timeout Period	The VNC service exits if no operation is performed within the specified timeout period. Enter the timeout period. Range: 5–60, unit: minutes.
Modify Password	 Whether to modify the VNC password. To modify the VNC password, turn on the Modify Password switch. To not modify the VNC password, turn off the Modify Password switch.
Parameter	Setting

Password complexity check	 Whether to check the complexity of the VNC password. To check the complexity of the VNC password, turn on the Password complexity check switch. To not check the complexity of the VNC password, turn off the Password complexity check switch.
VNC Password	 This parameter can be set when the Modify Password switch is turned on. Enter the new VNC password. The requirements for the VNC password are as follows: The password contains a maximum of eight characters. The password must contain at least one special character except spaces. The password must contain at least two of the following types: uppercase letters, lowercase letters, and digits. If the configuration is null, the default password is restored.
Confirm VNC Password	This parameter can be set when the Modify Password switch is turned on. Confirm the new VNC password, which must be the same as VNC Password .

4. Click Save.

7.8 Configuring SNMP Parameters

Abstract

This procedure describes how to configure SNMP parameters for communication between the BMC and a third-party NMS.

III Note

SNMP parameters are provided by the third-party NMS, so the values of SNMP parameters set on the Web portal of the BMC must be the same as those on the third-party NMS.

Steps

- 1. Select Services. The Services page is displayed.
- From the navigation tree in the left pane, select SNMP. The SNMP page is displayed, see Figure 7-13.

Figure 7-13 SNMP Page

SNMP	
SNMP	
Port	161
Complex Password	
Edit Read-only Community	\odot
Read-only Community	Please enter the community name.
Confirm Read-only Community	Please enter the group name again.
Edit Read-write Community	\odot
Read-write Community	Please enter the community name.
Confirm Read-write Community	Please enter the group name again.
Engine ID	0x80000f3e03e224a282e035
	Save

3. Set the parameters. For a description of the parameters, refer to Table 7-9.

Table 7-9 SNMP Parameter Descriptions

Parameter	Setting
SNMP	Turn on the SNMP switch.
Port	Enter the non-secure port number of the SNMP service. Range: 1– 65535, default: 161.
Complex Password	 Whether to enable the complex password function. To enable the complex password function, turn on the Complex Password switch. To disable the complex password function, turn off the Complex Password switch.



Edit Read-only Community	 Whether to edit the read-only community name. To edit the read-only community name, turn on the Edit Read-only Community switch. To not edit the read-only community name, turn off the Edit Read-only Community switch. 		
Parameter	Setting		
Read-only Community	This parameter can be set when the Edit Read-only Community switch is turned on. Enter the read-only community name (default: roAdmin9!).		
Confirm Read-only Community	This parameter can be set when the Edit Read-only Community switch is turned on. Confirm the read-only community name, which must be the same as that specified by Read-only Community .		
Edit Read-write Community	 Whether to edit the read-write community name. To edit the read-write community name, turn on the Edit Read-write Community switch. To not edit the read-only community name, turn off the Edit Readwrite Community switch. 		
Read-write Community	This parameter can be set when the Edit Read-write Community switch is turned on. Enter the read-write community name (default: rwAdmin9!).		
Confirm Read-write Community	This parameter can be set when the Edit Read-write Community switch is turned on. Confirm the read-write community name, which must be the same as that specified by Read-write Community .		

4. Click Save.

Chapter 8 BMC Management

Table of Contents

Network Parameter Configuration	130
Setting the Time of the BMC	140
Resetting the BMC on the Web Portal of the BMC	144
Upgrading Firmware	145
Switching Modes	147
Updating BMC Configurations	148
Restoring Factory Defaults	150

8.1 Network Parameter Configuration

Figure 8-1 Network Settings Page

8.1.1 Configuring the Host Name

Abstract

This procedure describes how to configure the host name to identify the server.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see Figure 8-1.

Host Name	
Host Name Settings	🔿 Automatic 🗿 Manual
Host Name	test
	Save

3. Set the parameters in the **Host Name** area. For a description of the parameters, refer to Table 8-1.

Parameter	Setting
Host Name Settings	 Select the desired host name setting mode. Automatic: A host name is automatically set by the system. Manual: A host name needs to be manually entered in the Host Name text box.
Host Name	This parameter is required if Host Name Settings is set to Manual . Enter the host name. The host name contains a maximum of 64 characters, including digits, letters, and hyphens. The host name cannot begin or end with hyphens.

Table 8-1 Host Name Parameter Descriptions

4. Click Save.

8.1.2 Configuring the Network Port Mode

Abstract

This procedure describes how to configure the network port mode to specify the management network port and shared network port.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see Figure 8-2.

Figure 8-2 Network Settings Page

Network Port	
Select Mode	🔿 Automatic 🔿 Fixed 🧿 Alone
NCSI Mode	🔘 Automatic 🔘 Manual
Specify Network Port	Dedicated Port
	O Dedicated Port
	Save

3. Set the parameters in the **Network Port** area. For a description of the parameters, refer to Table 8-2.

Parameter	Setting
Select Mode	Select the desired network port mode.
	• Automatic: The dedicated network port (namely the iSAC network
	port) is preferentially used as the management network port. If the
	dedicated network port does not operate properly, an onboard NCSI
	that is operating properly is automatically used as the management
	network port to replace the dedicated network port.
	• Fixed: A network port (the dedicated network port or an onboard
	NCSI) specified in the Dedicated Port box in the Specify Network
	Port area is used as the management network port.
	 Alone: The management network port and shared network port are configured separately. The dedicated network port is used as the management network port, and an onboard NCSI is used as the shared network port.

Table 8-2 Parameter Descriptions for Configuring a Network Port Mode

Parameter Setting	
	If Select Mode is set to Automatic , the following parameters do not need to be configured.
NCSI Mode	 This parameter is required when Alone is selected. Select the desired shared network port mode. Automatic: If the shared network port does not operate properly, an onboard NCSI that is operating properly is automatically used as the shared network port to replace the faulty shared network port. Manual: An onboard NCSI specified in the Network Card box in the Specify Network Port area is used as the shared network port. If NCSI Mode is set to Automatic, no shared network port needs to be specified.
Specify Network Port	 If Select Mode is set to Automatic, no network port needs to be specified. If Select Mode is set to Fixed, a network port (the dedicated network port or an onboard NCSI) needs to be specified as the management network port. If Select Mode is set to Alone and NCSI Mode is set to Manual, the dedicated network port is used as the management network port, and an onboard NCSI needs to be specified in the Network Card box as the shared network port.

4. Click Save.

8.1.3 Configuring IP Addresses of Network Ports

Abstract

To replan the IP address of the iSAC management network port or shared network port of the server, you must configure the IP address, subnet mask, default gateway, and other related information.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- From the navigation tree in the left pane, select Network Settings. The Network Settings page is displayed, see Figure 8-3.

Figure	8-3	Network	Settings	Page

	·			
Network Protocols	IPv4 🗹 IPv6			
Settings	IPv4		IPv6	
	Acquisition method	O Manually set IP address	Acquisition method	O Manually set IP address
		 Automatically obtain IP address 		• Automatically obtain IP address
	Address	10.	Address	
	Mask	255.255.255.0	Prefix Length	0
	Default Gateway	10.	Default Gateway	
	MAC Address	D4:2A:24:5E:AF:51	Link Local Address	fe80::d62a:24ff:fe5e:af51
	MAC Address	D4:2A:24:5E:AF:51	Link Local Address	fe80::d62a:24ff:fe5e:af51

3. Set the parameters in the **Network Protocols** area. For a description of the parameters, refer to Table 8-3.

Parameter	Setting	
Select Network Port	 This parameter can be set only if Select Mode is set to Alone in the Network Port area. Select the network port for which you want to configure an IP address. Dedicated Port: configures the IP address of the iSAC management network port. Shared Port: configures the IP address of the shared network port. 	
Network Protocols	 Select the network protocol(s) for the network port. The IPv4 settings need to be configured if you select IPv4 only. The IPv6 settings need to be configured if you select IPv6 only. Both IPv4 settings and IPv6 settings need to be configured if you select IPv4 and IPv6. 	
Acquisition method	Select the method of obtaining the IP address. The parameters below do not need to be configured if Acquisition method is set to Automatically obtain IP address .	
Address	Enter the address of the BMC as planned.	
Mask	Enter the mask.	
Default Gateway	Enter the IP address of the default gateway.	

Table 8-3 Network Protocol Parameter Descriptions

Prefix Length	Prefix is the digits of an IP address that represent the network.
	Value range: 0–128.

4. Click Save.

8.1.4 Configuring the DNS

Abstract

To access the Web portal of the BMC through a FQDN, you must configure the DNS information about the server.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see Figure 8-4.

Figure 8-4 Network Se	ettings Page
DNS	
DNS	
DNS Server Settings	O Manual O Automatically obtain DNS IPv4 address
	 Automatically obtain DNS IPv6 address
Registration Options	O Host Name O DHCP Client FQDN
Domain Name	test.vantageo.com
Preferred Server	10
Alternate Server 1	
Alternate Server 2	
	Save

3. Set the parameters in the **DNS** area. For a description of the parameters, refer to Table 8-4.

Table 8-4 DNS Parameter Descriptions

Parameter	Setting
DNS	 Select whether to enable the DNS service. To enable the DNS service, turn on the DNS switch. In this case, the following parameters need to be configured. To disable the DNS service, turn off the DNS switch. In this case, the following parameters do not need to be configured.
DNS Server Settings	Select the desired DNS setting method.

Parameter	Setting	
	 Manual: If Acquisition method is set to Manually set IP address in the Network Protocols area, this parameter must be set to Manual. When Manual is selected, you need to configure the following parameters. Automatically obtain DNS IPv4 address: If Acquisition method is set to Automatically obtain IP address and Network Protocols is set to IPv4 in the Network Protocols area, this parameter must be set to Automatically obtain DNS IPv4 address. When Automatically obtain DNS IPv4 address. Automatically obtain DNS IPv4 address is selected, you do not need to configure the following parameters. Automatically obtain DNS IPv6 address: If Acquisition method is set to Automatically obtain DNS IPv6 address. When Automatically obtain DNS IPv6 address: If Acquisition method is set to Automatically obtain DNS IPv6 address is selected, you do not need to configure the following parameters. Automatically obtain DNS IPv6 address is selected, you do not need to Automatically obtain DNS IPv6 address is set to IPv6 in the Network Protocols area, this parameter must be set to Automatically obtain DNS IPv6 address. When Automatically obtain DNS IPv6 address. When Automatically obtain DNS IPv6 address. 	
Registration Options	 Select the option used to register with the DNS. Host Name: uses DHCP option 12 to register with the DNS. DHCP Client FQDN: uses DHCP option 81 to register with the DNS. If the DHCP server does not support DHCP option 81, select Host Name. If DNS Server Settings is set to Manual, only Host Name can be selected. If DNS Server Settings is set to Automatically obtain DNS IPv4 address or Automatically obtain DNS IPv6 address, Host Name or DHCP Client FQDN can be selected. 	
Domain Name	Enter a domain name. The domain name consists of a maximum of 67 characters, including digits, letters, hyphens, and dots. It cannot start with a hyphen or dot or end with a hyphen. No more than 63 characters are allowed between any two dots.	
Preferred Server	Enter the IP address of the preferred DNS server. This parameter is required if DNS Server Settings is set to Manual .	
Alternate Server 1	Enter the IP address of alternate DNS server 1. This parameter is optional if DNS Server Settings is set to Manual .	
Alternate Server 2	Enter the IP address of alternate DNS server 2. This parameter is optional if DNS Server Settings is set to Manual .	

4. Click Save.

8.1.5 Configuring an iSAC VLAN

Abstract

This procedure describes how to configure an iSAC VLAN so that the iSAC management network port can be added to the VLAN.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see Figure 8-5.

Figure 8-5 Network Settings Page

ISAC.VLANConfiguration	
ISAC VLAN	
⑦ iSAC VLAN ID	2
③ ISAC VLAN Priority	0
	Save

3. Set the parameters in the **ISAC VLAN Configuration** area. For a description of the parameters, refer to Table 8-5.

Parameter	Setting
iSAC VLAN	 Select whether to enable the iSAC VLAN function. To enable the iSAC VLAN function, turn on the iSAC VLAN switch. In this case, the following parameters need to be configured. To disable the iSAC VLAN function, turn off the iSAC VLAN switch. In this case, the following parameters do not need to be configured. iSAC VLAN can be enabled if one of the following conditions is met: The Select Mode parameter in the Network Port area is set to Automatic, and the iSAC management network port is connected. The Select Mode parameter is set to Fixed in the Network Port area, and the iSAC management network port is specified as the management network port.
ISAC VLAN ID	Enter the iSAC VLAN ID. Range: 2–4094.

Table 8-5 iSAC VLAN Parameter Descriptions

ISAC VLAN Priority	Enter the iSAC VLAN priority. Range: 0–7. A greater value indicates a higher priority.
--------------------	--

4. Click Save.

8.1.6 Configuring an NCSI VLAN

Abstract

This procedure describes how to configure an NCSI VLAN so that an onboard NCSI can be added to the VLAN.

Steps

- 1. Select **BMC Settings**. The **BMC Settings** page is displayed.
- 2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see Figure 8-6.

NCSI.VLANConfiguration		
NCSI VLAN		
⑦ NCSI VLAN ID		
⑦ NCSI VLAN Priority		
	Save	

3. Set the parameters in the **NCSI VLAN Configuration** area. For a description of the parameters, refer to Table 8-6.

Parameter	Setting	
NCSI VLAN	 Select whether to enable the VLAN function. To enable the VLAN function, turn on the VLAN switch. In this case, the following parameters need to be configured. To disable the VLAN function, turn off the VLAN switch. In this case, the following parameters do not need to be configured. The VLAN function can be enabled if any of the following conditions is met: The Select Mode parameter is set to Automatic in the Network Port area, and an onboard NCSI is connected. The Select Mode parameter is specified as the management network port. 	
NCSI VLAN ID	Enter the VLAN ID. Range: 2–4094.	
Parameter	Setting	
NCSI VLAN Priority	Enter the VLAN priority. Range: 0–7. A greater value indicates a higher priority.	

Table 8-6 NCSI VLAN Parameter Descriptions

4. Click Save.

8.1.7 Configuring USB over LAN

Abstract

This procedure describes how to configure USB over LAN to establish a communication channel between the BMC and a host.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, as shown in Figure 8-7.

Figure 8-7 Network Settings Page

Lan Over USB Enabled				
Network Protocols	🕑 IPv4 🗌 IPv6			
Setting	IPv4		IPv6	
	Address	10.10.10.22	Address	
	Mask	255.255.255.0	Prefix Length	
	MAC Address		Link Local Address	
	mac Audress		Line Local Address	

3. In the **Lan Over USB Configuration** area, set the parameters. For a description of the parameters, refer to Table 8-7.

Table 8-7 USB over LAN Parameter Descriptions

Parameter	Setting
Lan Over USB Enabled	 Select whether to enable USB over LAN. Turn on the Lan Over USB Enabled toggle switch to enable USB over LAN and configure the following parameters. Turn off the Lan Over USB Enabled toggle switch to disable USB over LAN. The following parameters do not need to be configured.
Network Protocols	Select a network protocol and set the network parameters such as IP address.

4. Click Save.

8.2 Setting the Time of the BMC

Abstract

The time of the BMC must be correct.

This procedure describes how to set the time of the BMC in either of the following ways:

- Setting time manually
- Synchronizing time with an NTP server

To make the manually set time permanently valid, you need to disable NTP-based time synchronization.

Steps

- Setting Time Manually
 - 1. Select BMC Settings. The BMC Settings page is displayed.
 - From the navigation tree in the left pane, select Time Zone & NTP. The Time Zone & NTP page is displayed, as shown in Figure 8-8.

The expected time set by the set sel time command will take effect permanently. Please disable NTP synchronization.		
Time Zone		
Time	2024-01-11 11:07:09 🖉	
Current Timezone	UTC+08:00	
Region	INDIA / MUMBAJ	
NTP		
NTP		
Polling Interval	60	
Main Server	10.	
Secondary Server	time.nist.gov	
Tertiary Server		
	Save	

Figure 8-8 Time Zone & NTP Page

Note

The time is automatically saved on the page after being set.

- Synchronizing Time with an NTP Server
 - 1. Select **BMC Settings**. The **BMC Settings** page is displayed.
 - From the navigation tree in the left pane, select Time Zone & NTP. The Time Zone & NTP page is displayed, as shown in Figure 8-9.

The expected time set b synchronization.	y the set sel time command will take effect permanently. Please disable NTP	
Time Zone		
Time	2024-01-11 11:08:04 🖉	
Current Timezone	UTC+08:00	
Region	INDIA/ MUMBAI	6
NTP		
Polling Interval	60	s
Main Server	10	
Secondary Server	time.nist.gov	
Tertiary Server		

Figure 8-9 Time Zone & NTP Page

3. Set the parameters in the **NTP** area. For a description of the parameters, refer to Table 8-8.

Table 8-8 NTP Parameter Descriptions

Parameter	Description	
NTP	Enable NTP .	
Polling Interval	Enter the time synchronization period. Range: 60–65535, unit: seconds.	
Parameter	Description	
Main Server	Enter the IP address or FQDN of the primary NTP server. The length cannot exceed 127 characters. This parameter is required.	
Secondary Server	Enter the IP address or FQDN of the secondary NTP server. The length cannot exceed 127 characters. This parameter is optional.	

	Enter the IP address or FQDN of the tertiary NTP server. The length cannot exceed 127 characters. This parameter is optional.
Note	

The BMC first synchronizes time with the primary NTP server. If the synchronization fails, it synchronizes time with the secondary NTP server and tertiary NTP server in turn.

4. Click Save.

Verification

If NTP-based time synchronization is used, perform the following operations:

1. On the **Time Zone & NTP** page, view the date and time, as shown in Figure 8-10.

Time	2024-01-11 11:09:18 🖉	
Current Timezone	UTC+08:00	
Region	INDIA/ MUMBAI	
NTP		
Polling Interval	60	s
Main Server	10	
Main Server Secondary Server	10 time.nist.gov	

Figure 8-10 Time Zone & NTP Page

2. On the NTP server, check whether the time is the same as the time of the BMC.

8.3 Resetting the BMC on the Web Portal of the BMC

Abstract

After some configurations (for example, MAC address and chassis information programming), you must reset the BMC to apply the changes.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Firmware Upgrade**. The **Firmware Upgrade** page is displayed, see Figure 8-11.


Firmware Upgrade			
After the BMC is upgraded, the BMC is auton version and takes effect automatically after th period.	natically restarted. When the systen he systems is powered off. It takes a	n is powered off, the BIOS upgrade tak a period of time to make the firmware	kes effect directly. When the system is powered on, the BIOS is updated to the backup take effect automatically, and firmware upgrade cannot be performed during this
Firmware Operation	Reset BMC		
Version Information	BMC Primary Partition Version BMC Standby Partition Version BIOS Primary Version BIOS Standby Version EPLD Version	04.24.02.00 (Feb 26 2024) 04.24.01.00 (Jan 08 2024) 01.23.04.00 (Dec 27 2023) 01.23.04.00 (Dec 27 2023) 00.00.00.0102	
(?) Upgrađe	Don't Inherit Configuration Wh Upload	en Upgrading BMC 📃 Don't Inhe	rrit Configuration When Upgrading BIOS

3. Click Reset BMC, and confirm the reset in the displayed message box.



Relogin is allowed only after the BMC is reset.

8.4 Upgrading Firmware

Abstract

If the firmware on the mainboard of a server needs an upgrade, you can upload the firmware online for upgrade.

If multiple firmware versions need an upgrade, the following sequence is recommended:

1. FRU firmware

After the FRU firmware is upgraded, the BMC is automatically restarted to apply the new version.

2. BMC firmware

The Web portal of the BMC temporarily supports the upgrade of the active BMC firmware only. After the active BMC firmware is upgraded, the BMC is automatically restarted to apply it.

3. EPLD firmware

After the EPLD firmware is upgraded, the new version takes effect only after the server is restarted. Therefore, it is recommended that you stop the services running on the server before the upgrade.

4. BIOS firmware

After the BIOS firmware is upgraded, the new version takes effect only after the server is restarted. Therefore, it is recommended that you stop the services running on the server before the upgrade.

- If the BIOS firmware is upgraded when the server is powered off, the upgraded BIOS firmware takes effect directly.
- If the BIOS firmware is upgraded when the server is powered on, the upgraded BIOS firmware is displayed as a standby version on the Web portal and takes effect automatically after the server is powered off and restarted. It takes time for the new version to take effect automatically. During this period, firmware upgrade is not allowed.

5. VR firmware

III Note

If a firmware version fails to be upgraded during version upgrade, you must upgrade it again.

Prerequisite

The firmware to be upgraded is already obtained.

III Note

Firmware files can be obtained on the **Software Download** page on the Web portal of the servers and storage products (https://enterprise.VANTAGEO.com.cn).

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select Firmware Upgrade. The Firmware

Upgrade page is displayed, see Figure 8-12. Figure 8-12 Firmware Upgrade Page

Firmware Upgrade After the BMC is upgraded, the BMC is autor version and takes effect automatically after t	natically restarted. When the system he systems is powered off. It takes a	n is powered off, the BIOS upgrade takes effe a period of time to make the firmware take ef	ect directly. When the system is powered on, the BIOS is updated to the backup ffect automatically, and firmware upgrade cannot be performed during this period.
Firmware Operation	Reset BMC		
Version Information	BMC Primary Partition Version	04.24.01.20 (Mar 17 2024)	
	BMC Standby Partition Version	04.24.01.00 (Jan 08 2024)	
	BIOS Primary Version BIOS Standby Version	01.23.04.00 (Dec 27 2023) 01.23.04.00 (Dec 27 2023)	
	EPLD Version	00.00.00.0102	
⑦ Upgrade	Don't Inherit Configuration Wh	ien Upgrading BMC 🛛 Don't Inherit Cor	nfiguration When Upgrading BIOS
	Upload		
	Upgrade		

3. Click **Upload** and select the firmware file in the displayed dialog box.





Only one firmware file can be selected at a time. During the firmware upgrade process, the firmware file automatically matches the firmware type.

After the BMC or BIOS firmware is successfully uploaded, the **Don't Inherit Configuration When Upgrading BMC** or **Don't Inherit Configuration When Upgrading BIOS** check box becomes activated.

- 4. (Optional) Perform either of the following operations:
 - To restore the factory default settings of the BMC, select Don't Inherit Configuration When Upgrading BMC.
 - To restore the factory default settings of the BIOS, select Don't Inherit Configuration When Upgrading BIOS.
- 5. Click **Upgrade**.



During the firmware upgrade process, you cannot to switch to another page. Otherwise, the upgrade process is interrupted.

8.5 Switching Modes

Abstract

A mode refers to a working mode of a PCIe switch board. By switching modes, CPUs and GPU s can work in a proper mode.



Only R6500 G5 servers support mode switching.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- 2. From the navigation tree in the left pane, select **Firmware Upgrade**. The **Firmware Upgrade** page is displayed.
- 3. Click Mode Switching. The Mode Switching tab is displayed, as shown in Figure 8-13.

Figure 8-13 Mode Switching Tab

Firmware Upgrade		
Firmware Upgrade	Mode Switch	ing
	Firmware Mode Mode Selection	Dual uplink
		Save

4. Set the parameters. For a description of the parameters, refer to Table 8-9.

Parameter	Setting
Firmware Mode	Firmware mode is determined by the hardware topology of a PCIe switch board, including Single uplink and Dual uplink . It cannot be configured.
Mode Selection	 Select the working mode of a PCIe switch board. Cascade Mode: provides the best point-to-point communication between GPUs and the worst I/O bandwidth between CPUs and GPUs. Normal Mode: provides the suboptimal point-to-point communication between GPUs and suboptimal I/O bandwidth between CPUs and GPUs. Balancing Mode: provides the worst point-to-point communication between GPUs and the best I/O bandwidth between CPUs and GPUs. Balancing Mode: provides the worst point-to-point communication between GPUs and the best I/O bandwidth between CPUs and GPUs. Balancing Mode: provides the worst point-to-point communication between GPUs and the best I/O bandwidth between CPUs and GPUs. When Firmware Mode is set to Dual uplink, you can select only Normal Mode or Balancing Mode.

Table 8-9 Mode Switching Parameter Descriptions

5. Click Save.

8.6 Updating BMC Configurations

Abstract

This procedure describes how to update BMC/BIOS configurations online.

Before replacing the mainboard of a server, you can back up the BMC/BIOS configurations by using the configuration update function.

Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.

 From the navigation tree in the left pane, select Configuration Update. The Configuration Update page is displayed, see Figure 8-14.

Configuration Update		
Configure Import	Configure Import	
Supports importing BMC ar	d BIOS configurations. After importing, BMC automatically restarts and the configuration takes effect. BIOS takes effect and requires manual resetting of the host.	
Select Type	O BMC O BIOS	
Select File	Upload	
	Import	
Configure Export		
Select Type	O BMC O BIOS	
	Export	
Restore Factory Settings		
() After restoring BMC factory	settings, you need to log in to BMC for the first time. Please use this function with caution.	
	Restore Factory Settings	

Figure 8-14 Configuration Update Page

3. Perform the following operations as required.

If	Then
There is an existing BMC/ BIOS configuration file	 a. Click Upload, and select the BMC configuration file in the displayed dialog box. b. Click Import, and confirm the import in the displayed message box.
There is no BMC/BIOS configuration file	a. Click Export to export the current BMC configurations to your local PC.
	 b. Edit the exported BMC configuration file. c. Click Upload, and select the BMC configuration file in the displayed dialog box
	d. Click Import , and confirm the import in the displayed message box.



After the BMC configurations are imported, the BMC is automatically restarted to apply the configurations. Do not perform any other operations until the BMC is restarted. After the BIOS configuration is imported, you need to manually reset the host to validate the configuration.

Related Tasks

To back up BMC configurations, perform the following operations:

- 1. Click **Export** to export the current BMC configurations to your local PC.
- 2. After replacing the mainboard, click **Upload**, and select the exported BMC configuration file in the displayed dialog box.
- 3. Click Import, and confirm the import in the displayed message box.

8.7 Restoring Factory Defaults

Abstract

By restoring factory defaults, you can restore the server configuration items (for example, the network, user, SNMP configuration and startup mode) to factory defaults.



Do not perform any operation during restoration. After the factory defaults are restored, the BMC will be restarted automatically.

Steps

- 1. Select BMC Settings. The BMC Settings page is displayed.
- From the navigation tree in the left pane, select Configuration Update. The Configuration Update page is displayed, see Figure 8-15.

Configuration Update	
Configure Import	
 Supports importing BMC and 	d BIOS configurations. After importing, BMC automatically restarts and the configuration takes effect. BIOS takes effect and requires manual resetting of the host.
Select Type	O BMC: O BIOS
Select File	Upload
	Import
Configure Export	
Select Type	O BMC O BIOS
	Export
Restore Factory Settings	
After restoring BMC factory	settings, you need to log in to BMC for the first time. Please use this function with caution.
	Restore Factory Settings

Figure 8-15 Configuration Update Page

3. Click Restore Factory Defaults.

Chapter 9 User and Security

Table of Contents

Adding a Local User	.151
Configuring Authentication Parameters for Domain Users	154
Querying Online Users	.158
Configuring Permissions for a Customized Role	159
Configuring Security Enhancement Parameters	160
Configuring Firewall Parameters	.161
Configuring Two-Factor Authentication	163

9.1 Adding a Local User

Abstract

Local users refer to users of the BMC itself. This procedure describes how to add a local user to configure and manage the BMC.

Steps

- 1. Select User & Security. The User & Security page is displayed.
- 2. From the navigation tree in the left pane, select **Local Users**. The **Local Users** page is displayed, see Figure 9-1.

Local Users				C
+ Add Use	er			Q Search(Fuzzy search only
User ID	User Name	Role	Login Interfaces	Operation
1	anonymous	Administrator	SNMP SSH Redfish	Edit Enable Delete
2	Administrator	Administrator	SNMP SSH Redfish	Edit Disable Delete

3. Click Add User. The Add User page is displayed, see Figure 9-2.

Figure	9-2 Add	User	Page
i iguio		0001	. ugo

Local Users > Add User	
New User ID	10 ×
New UserName	test
New Password	
Confirm Password	
Role	Administrator ~
Login Interfaces	SNMP 🕐 🗹 Redfish
Current User Password	
	Submit Cancel

4. Set the parameters. For a description of the parameters, refer to Table 9-1.

Parameter	Setting
New User ID	Select the ID of the new user. A maximum of 16 local users are supported, so the user ID ranges from 1 to 16. User 1 is a reserved user, and user 2 is the default administrator.
New UserName	Enter the name of the new user. The name contains a maximum of 16 characters, including digits, letters (case sensitive), and special characters. The new username cannot be the same as another existing username. The following cannot be used as a username: sshd, ntp, stunnel4, sysadmin, daemon, Administrator, and anonymous. The allowed special characters include hyphens (-), underscores (_), and at symbols (@).
New Password	Enter the password of the new user. The password contains 5–20 characters (If Login Interfaces is set to SNMP , the password contains 8–20 characters.), including digits, letters (case sensitive), and special characters. It must contain one special character and characters from at least two of the following types: digits, uppercase letters, and lowercase letters. The allowed special characters include `, ~, !, @, \$, %, ^, &, *, (,), -, _, =, +, , [, {, },], :, ', ", ,, <, ., >, /, ?, #, ;.

Table 9-1 Parameter Descriptions for Adding a Local User

Parameter	Setting
	The function of disabling historical passwords is disabled by default. If this function is enabled, the new password cannot be the same as any of the historical passwords. The password cannot be the same as the username in reverse order. For example, if the username is test, the password cannot be tset.
Confirm Password	Enter the same password again for confirmation.
Role	Select the role that the new user belongs to, including Administrator , Operator , Common User , and Custom Role . The permissions of each role can be viewed on the Security Management page.
Login Interfaces	 Select one or more login interfaces available to the new user. For SNMP interface-based login, select SNMP. For Redfish interface-based login, select Redfish. SSH-based login is supported for all users by default.
Current User Password	Enter the password of the currently logged-in user.

- 5. Click Submit.
- (Optional) If Login Interfaces is set to SNMP, click Edit in the Operation column for the new user. The Edit page is displayed. Set SNMPv3 Authentication Algorithm and SNMPv3 Encryption Algorithm.
 - Options of SNMPv3 Authentication Algorithm include SHA, MD5, SHA256, SHA384, and SHA512. It is recommended that you select SHA256, SHA384, or SHA512
 - Options of **SNMPv3 Encryption Algorithm** include **DES**, **AES**, and **AES256**. It is recommended that you select **AES**.

Related Tasks

Perform either of the following operations as needed.

То	Do
Disable a local user	 In the Operation column, click Disable for the user. The Confirm dialog box is displayed.
	 Enter the password of the currently logged-in user. Click Submit
Delete a local user	 In the Operation column, click Delete for the user. The Confirm dialog box is displayed. Enter the password of the currently logged-in user. Click Submit.

9.2 Configuring Authentication Parameters for Domain Users

Abstract

Domain users are not the users of the BMC itself. The detailed information about domain users is stored on an LDAP server or AD server.

This procedure describes how to configure authentication parameters for domain users to authenticate them through an LDAP or AD server.

Note

If you log in to the BMC as a domain user, the current server must be interconnected with the LDAP server or AD server.

Prerequisite

The parameters of the LDAP server or AD server are already obtained.

Steps

- Configuring LDAP Server Authentication Parameters
 - 1. Select User & Security. The User & Security page is displayed.
 - 2. From the navigation tree in the left pane, select Domain Users. The Domain Users

page is displayed, see Figure 9-3. Figure 9-3 Domain Users Page

Domain U	Jsers				
LDAP	AD				
LD	AP Authentication				
Basic At	tributes				
	Server Address	1!			
	Port	389			
	Bind DN	cn=admin,dc=ladpdomain,dc=cor	n		
	Password	Please enter.			
	Search Base	dc=ladpdomain,dc=com			
Attri	bute of User Login	O cn ◯ uid			
	Encryption Type	O No encryption O SSL O Sta	rtTLS		
	ale Group	Save			
ID	Name		Search Domain	Permissions	Operation
1	test		cn=admin,ou=login,dc=ldapdomain,dc=com	🔿 Administraor 🔿 Operator 🗿 User	
					Save Cance
2					Save Cance
2 3					Edit
2 3 4					Save Cance Edit Edit Edit

- 3. Turn on the LDAP Authentication switch.
- 4. Set the parameters in the **Basic Attributes** area. For a description of the parameters, refer to Table 9-2.

Parameter	Setting					
Server Address	Enter the IP address or FQDN of the LDAP server.					
Port	Enter the port number. Range: 1–65535. Default: 389. If Encryption Type is set to SSL , enter the port number 636.					
Bind DN	Enter the DN of the LDAP server, for example, cn=admin,dc=ldapdomain,dc=com.					
Password	Enter the password for logging in to the LDAP server. It cannot be left blank. Range: 1–47 characters. Bind DN and Password are used to access the LDAP server.					
Search Base	Enter the storage location of the user information on the LDAP server, for example, <i>dc=ldapdomain</i> , <i>dc=com</i> .					
Attribute of User Login	Select the user login attribute identified by the LDAP server. \rightarrow If Bind DN contains cn, select cn . \rightarrow If Bind DN contains uid, select uid .					
Encryption Type	 Select the type of encryption used by the LDAP server. → No encryption: indicates that no encryption is used. → SSL: indicates that SSL encryption is used. 					
	→ StartTLS: indicates that StartTLS encryption is used.					
Upload certificate	Click the corresponding certificate button and upload the certificate. If Encryption Type is set to No encryption , no certificate needs to be uploaded.					

Table 9-2 Parameter Descriptions for Basic LDAP Authentication Attributes

- 5. Click Save.
- 6. In the **LDAP Role Group** area, click **Edit** in the **Operation** column for a role group to activate role group parameters.
- 7. Set the role group parameters. For a description of the parameters, refer to Table 9-3.

Parameter	Setting
Name	Enter the name of the role group that domain users belong to. The name contains a maximum of 64 characters, including digits, letters, spaces, and special characters. It cannot begin with a space. The allowed special characters include hyphens and underscores.
Parameter	Setting
Search Domain	Enter the storage location of the user group information on the LDAP server, for example, cn=admin,ou=login,dc=ldapdomain,dc=com.
Permissions	Select the permissions of the role group that domain users belong to in the BMC, including Administrator , Operator , and User . The permissions of each role can be viewed on the Security Management page.

Table 9-3 LDAP Role Group Parameter Descriptions

- 8. Click Save in the Operation column.
- Configuring AD Server Authentication Parameters
 - 1. Select User & Security. The User & Security page is displayed.
 - 2. From the navigation tree in the left pane, select **Domain Users**. The **Domain Users** page is displayed.
 - 3. Click AD. The AD tab is displayed, see Figure 9-4.

Domain U	Jsers				
LDAP	AD				
	AD Certification				
A Basic At	tributes				
	SSL Encryption				
	User Name	test			
	Password				
U	lser Domain Name	mydomain.com			
Domain Cont	trol Server Address 1	10			
Domain Cont	trol Server Address 2	Please enter.			
Domain Cont	trol Server Address 3	Please enter.			
		_			
AD Role	Group	Save			
ID	Name		Domain Name	Permissions	Operation
1	test01		mydomain.com	🔿 Administrator 🔿 Operator 🧿 User	Save Cancel
2	6786786785	5	6786786654645	User	Edit Delete
3					Edit
					Edit
4					

- 4. Turn on the **AD Authentication** switch.
- 5. Set the parameters in the **Basic Attributes** area. For a description of the parameters, refer to Table 9-4.

Parameter	Setting
SSL Encryption	 Select whether SSL encryption is used when logging in to the AD server. → To enable SSL encryption, turn on the SSL Encryption switch. → To disable SSL encryption, turn off the SSL Encryption switch.
User Name	Enter the username for logging in to the AD server. The username contains a maximum of 64 characters, including digits, letters (case sensitive), spaces, and special characters. It must begin with a letter. The allowed special characters include hyphens and underscores. If the username and password are not required, leave this parameter blank.
Password	Enter the password for logging in to the AD server. Range: 6–127 characters. If the username and password are not required, leave this parameter blank.
User Domain Name	Enter the domain name of the AD server, for example, mydomain.com, and is required.
Domain Control Server Address 1	Enter the IP address of AD server 1, which supports IPv4 and IPv6 formats, and is required.
Domain Control Server Address 2	Enter the IP address of AD server 2, which supports IPv4 and IPv6 formats, and is optional.
Domain Control Server Address 3	Enter the IP address of AD server 3, which supports IPv4 and IPv6 formats, and is optional.

Table 9-4 Parameter Descriptions for Basic AD Authentication Attributes

- 6. Click Save.
- 7. In the **AD Role Group** area, click **Edit** in the **Operation** column for a role group to activate role group parameters.
- 8. Set the role group parameters. For a description of the parameters, refer to Table 9-5.

Parameter	Setting
Name	Enter the name of the role group that domain users belong to. The name contains a maximum of 64 characters, including digits, letters, spaces, and special characters. It cannot begin with a space. The allowed special characters include hyphens and underscores.
Domain Name	Enter the domain name of the role group, for example, <i>mydomain.com</i> .
Permissions	Select the permissions of the role group that domain users belong to in the BMC, including Administrator , Operator , and User . The permissions of each role can be viewed on the Security Management page.

Table 9-5 AD Role Group Parameter Descriptions

9. Click Save in the Operation column.

9.3 Querying Online Users

Abstract

By querying online users, administrator can learn about all online users, including their IDs, usernames, login modes, login IP addresses, and login time.

III _{Note}

The ID is the serial number of a user's connection session rather than the user ID.

Steps

- 1. Select User & Security. The User & Security page is displayed.
- 2. From the navigation tree in the left pane, select **Online Users**. The **Online Users** page is displayed, see Figure 9-5.

igur Online	e 9-5 Online	Users Page			
ID	User Name	Login Method	Login IP	Login Time	Operation
12	Administrator	Web HTTPS	10.	2024-03-07 15:06:15	Delete
				Total 1 K < 1 > X 10 / Page	 To 1 Pag

 (Optional) To force a user to log out of the Web portal of the BMC, click **Delete** in the Operation column for the user, and click **Submit** in the displayed message box.

You cannot delete yourself.

9.4 Configuring Permissions for a Customized Role

Abstract

The following roles exist in the system by default:

- Common user
- Operator
- Administrator
- Customized roles 1-4

The permissions of common users, operators, and administrators cannot be configured, while the permissions of customized roles can be configured.



Only administrators can configure the permissions of customized roles.

Steps

- 1. Select User & Security. The User & Security page is displayed.
- 2. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed, see Figure 9-6.

Figure 9-6 Security Management Page

Security Man	agement									
Permission N	lanagement	Security Enhan	icements	Firewall						
Role	User Mgmt	Basic Mgmt	Remote Control	VMM	Security Mgmt	Power Control	Diagnosis	Query	Configure Itself	Operation
Common User								\checkmark	\checkmark	
Operator		\checkmark	\checkmark	~		\checkmark		\checkmark	\checkmark	
Administrator	~	~	~	~	~	~	~	~	~	
Custom Role 1								~	\checkmark	Edit Disable
Custom Role 2								\checkmark	\checkmark	Edit Disable
Custom Role 3								~	\checkmark	Edit Disable
Custom Role 4								~	~	Edit Disable

3. In the **Operation** column, click **Edit** for a customized role to activate the permission check boxes, see Figure 9-7.

Figure 9-7 Activating the Permission Check Boxes

Permission N	lanagement	Security Enhan	cements	Firewall						
Role	User Mgmt	Basic Mgmt	Remote Control	VMM	Security Mgmt	Power Control	Diagnosis	Query	Configure Itself	Operation
Common User								~	1	
Operator		\checkmark	\checkmark	\checkmark		\checkmark		\checkmark	\checkmark	
Administrator	~	\checkmark	~	~	~	~	~	~	~	
Custom Role 1								\checkmark		Save Cance
Custom Role 2								~	1	Edit Disable
Custom Role 3								\checkmark	\checkmark	Edit Disable
Custom Role 4								1	1	Edit Disable

- 4. Select the corresponding permissions.
- 5. Click Save.

Related Tasks

To disable or enable a customized role, perform the following operations:

- In the **Operation** column, click **Disable** to disable the customized role.
- In the **Operation** column, click **Enable** to enable the customized role.

III Note

You cannot disable or enable common users, operators, and administrators.

9.5 Configuring Security Enhancement Parameters

Abstract

To enhance user login security, you can configure security enhancement parameters, including:

Password Complexity Check
 Password Validity
 User Lockout Policy

Steps

- 1. Select User & Security. The User & Security page is displayed.
- 2. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed.
- Click Security Enhancements. The Security Enhancements tab is displayed, see Figure 9-8.

Figure 9-8 Security Enhancements Tab

Security Management				
Permission Management	Security	/ Enhancements	Firewall	
Password Complexi	ity Check			
Password	d Validity	1		Day
User Locko	ut Policy	Unlimited	~	
		Number of failures		
		Save		

4. Set the parameters. For a description of the parameters, refer to Table 9-6.

Table 9-6 Securi	ty Enhancemen	t Parameter Descriptions

Parameter	Setting	
Password Complexity Check	 Select whether to enable password complexity check. To enable password complexity check, turn on the Password Complexity Check switch. To disable password complexity check, turn off the Password Complexity Check switch. 	
Password Validity	Enter the password validity period. Range: 0–365, unit: days. If the password validity period is 0, there is no limit to the validity period.	
User Lockout Policy	Select the maximum number of login failures and enter the locking duration. If the maximum number is exceeded, a user is locked.	

5. Click Save.

9.6 Configuring Firewall Parameters

Abstract

By configuring firewall parameters, you can add IP or MAC addresses to the blacklist and whitelist to control access to the BMC.

- The devices in the blacklist are forbidden to access the BMC all the time or within the specified time period.
- The devices in the whitelist are allowed to access the BMC all the time or within the specified time period.

Note: When enabling the whitelist policy, you must first add the IP or MAC address of your local PC (acting as a client PC) to the whitelist to ensure that your local PC can access the Web portal of the BMC.

This procedure describes how to configure firewall parameters.

Steps

- 1. Select User & Security. The User & Security page is displayed.
- 2. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed.
- 3. Click Firewall. The Firewall tab is displayed, as shown in Figure 9-9.

Figure 9-9 Firewall Tab

Security I	/lanagement			
Permissi	on Management Security Enhancements Firewall			
i Time effec IP se singl MAC addr At le	period: supports three formats: YYYY-MM-DD HH: MM, YYYY-MM-DD and HH: MM; tive. Please select a time range before selecting Workday Only. gment: support a single IP or IP segment, support IPv4 and IPv6, and the format of the IP. segment: support a single MAC or MAC segment, support format xxxxxxxxxxxx, ref seses set one item shall be filled in for IP segment and MAC segment.	'he format of start time and end time must start IP address and end IP address must l ers to a single complete MAC address. The	t be consistent. If the time period is blank be consistent. 127.0.0.1 is not allowed to l MAC segment cannot contain more than	the rule is always be configured for 64 MAC
Blacklist				
🚺 Black	list: Only devices that meet the rules are prohibited from accessing BMC.			
No. 🌲	Time Segment	IP Segment	MAC Segment	Operation
1	Time Date > 2024-01-11 00:00 - 2024-02-1	10.239.10.10 - 10.239.10.20	Required — Optional	Save Cancel
+ Add Rul	e			
Whitelist				
() Whit Whe	elist: Only devices that meet the rules are allowed to access BMC. No address other the adding white list rules, please first add the local IP address or MAC address to ensure	an the white list can access the BMC. Please e normal access to BMC.	e operate with caution.	
No. ≑	Time Segment	IP Segment	MAC Segment	Operation
1	Time Date > 2024-01-11 00:00 - 2024-02-1	10.239.20.10 — 10.239.20.20	Required — Optional	Save Cancel
+ Add Ru	e			

4. Perform the following operations as needed.

то	Do
Add an item to the blacklist	a. In the Blacklist area, click Add Rule . The blacklist parameters are activated.
	b. Set the parameters. For a description of the parameters, refer to Table 9-7.
	c. Click Save.
Add an item to the whitelist	a. In the Whitelist area, click Add Rule . The whitelist parameters are activated.
	b. Set the parameters. For a description of the parameters, refer to Table 9-7.
	c. Click Save.

Parameter	Description	
Time Segment	From the Time Type list, select the desired time type, and set the time period accordingly. The format of the start time and end time must be the same. Before selecting Working days only , you must specify a time period. If the time period is left blank, the devices in the blacklist are permanently forbidden to access the BMC or those in the whitelist are permanently allowed to access the BMC.	
IP Segment	Enter an IP address or an IP address segment. IPv4 or IPv6 format is supported. For a single IP address, 127.0.0.1 is disallowed.	
	For an IP address segment, the format of the start address and end address must be the same.	
MAC Segment	Enter a MAC address or a MAC address segment. The format is xx:xx:xx:xx:xx. A MAC address segment can contain a maximum of 64 MAC addresses. At least one of the IP Segment and MAC Segment parameters must be set.	

Table 9-7 Blacklist/Whitelist Parameter Descriptions

9.7 Configuring Two-Factor Authentication

Abstract

Two-factor authentication requires another credential for access to the BMC in addition to a static password. It improves the security of the BMC.

Steps

- 1. Select User & Security. The User & Security page is displayed.
- 2. From the navigation tree in the left pane, select **Two-factor Authentication**. The **Two-factor Authentication** page is displayed, as shown in Figure 9-10.

wo-factor A	uthentication
Turning authent	ication on or off
Turning authenti	cation on or off 🝳 enable 🔘 disable
Mobile Phone Bi	Save
	 Use the mobile app to scan the QK code, enter the dynamic password generated by the mobile app, and complete the binding.

Figure 9-10 Two-factor Authentication Page

- 3. Select whether to enable two-factor authentication. Options:
 - enable: enables two-factor authentication.
 - disable: disables two-factor authentication.
- 4. Click Save.
- 5. (Optional) If two-factor authentication is enabled, click **Generate QR code**, and then scan the code and enter the correct token to bind your mobile number to.



The bound mobile number will be used as the other credential in addition to the static password. In addition, the BMC time must be the same as the Internet time. Otherwise, the verification fails.

Chapter 10 Reference: Default Passwords

The default administrator username for logging in to the BMC of a server is *sysadmin*. The default administrator password depends on server models and BMC versions. For details, refer to Table 10-1.

Server Model	BMC Version	Default Password
2240-RE	Versions earlier than V04.23.01.02P1	superuser
	V04.23.01.02P1 and later	Superuser@123
2230-RE	Versions earlier than V04.23.02.01	superuser
	V04.23.02.01 and later	Superuser@123
1240-RE	Versions earlier than V04.23.04.00	superuser
	V04.23.04.00 and later	Superuser@123
	V04.23.01.02 and later	Superuser@123
22G1-RE	Versions earlier than V04.23.01.01P2	superuser
	V04.23.01.01P2 and later	Superuser@123

Table 10-1 Default Password Descriptions



After logging in to the BMC by using the default password, you must change it immediately. It is recommended that you change the password to a strong password.

Chapter 11 Reference: Accessing Documents

Abstract

Documents are readily available at VANTAGEO.com Enterprise Servers, select the model and at every model page will have the document download links



This procedure uses VANTAGEO Server Redfish Interface Description (BMC V4) as an example, and other documents can be accessed by similar steps.

Prerequisite

You have registered successfully at VANTAGEO.com and select the product

Steps

- 1. In the address bar of your browser, enter *https://VANTAGEO.com* and press Enter. The home page is displayed.
- 2. Click Login in the upper right corner. The User Login page is displayed, see Figure 11-1.



- 3. Enter the username, password, and verification code.
- 4. Click Login to log in the VANTAGEO.com/partner-portal/ website.
- 5. Select **Support** on the menu. The **Support** page is displayed, see Figure 11-2.

Figure 11-2 Support Page

C 1. Vantageoun/support		200500		
i Gmail 🛄 YouTube 💡 Maps. 🎯 Sleek Bill	n ppt slide samples 🗀 Imported 🚱 MOA (9).pdf	openai		
	vantageo	Home Products v Solutions v	About Us Success Stories Support	٩
		E	nter product serial number	
		Se	arch	
			ack sustam's warranty / Suppor	
		St	atus Open a support ticket from	here
		Ser	rial number not matching or not found follow t	elow
		opt	tions	
		Cor	ntact Support@vantageo.com and a help desk	team shall
		and the Association of the second sec	t back to you	

6. Click **Document Download**. The **Document Download** page is displayed, see Figure 11-3.

Figure 11-3 Document Download Page (Select your model from Enterprise Servers and below every model you can find the download link)

Memory 32x DDRS, 8TB max, S600MT/s (Sth Gen), PMem support Storage 45x 2.5" or 20x 3.5" + 4x 2.5" hot-swap, 34 NVMe SSDs, 40 ELS/E3.5 PCIe Stots 20x PCIe 4.0 (2x OCP 3.0) Networking OCP 3.0 (1/10/25/100CbE) Power Supply 1+1 redundant S50W-2200W 80+ Platinum/Titanium Security TPM 2.0, Secure Boot, Silicon Root of Trust	M Gmail 🖸 YouTube 💡 Maps 🌀 Sleek Bill 🚵 pp	t slide samples 🗋 Imported 🧉	MOA (9).pdf 🚳 openai	
Storage 45x 2.5° or 20x 3.5° + 4x 2.5° hot-swap, 34 NVMe SSDs, 40 ELS/E3.5 PCIe Stots 20x PCIe 4.0 (2x DCP 3.0) Networking OCP 3.0 (1/10/25/100CbE) Power Supply 1+1 redundant 550W-2700W 80+ Platinum/Titanium Security TPM 2.0, Secure Boot, Silicon Root of Trust		Memory	32x DDR5, 8TB max, 5600MT/s (5th Gen), PMem support	
PCIe Slots 20x PCIe 4.0 (2x OCP 3.0) Networking OCP 3.0 (1/10/25/100CbE) Power Supply 1+1 redundant 550W-2700W 80+ Platinum/Titanium Security TPM 2.0, Secure Boot, Silicon Root of Trust		Storage	45x 2.5" or 20x 3.5" + 4x 2.5" hot-swap, 34 NVMe SSDs, 40 E1.S/E3.S	
Networking OCP 3.0 (1/10/25/100GbE) Power Supply 1+1 redundant SSOW-2700W 80+ Platinum/Titanium Security TPM 2.0, Secure Boot, Silicon Root of Trust		PCIe Slots	20x PCIe 4.0 (2x OCP 3.0)	
Power Supply 1+1 redundant 550W-2700W 80+ Platinum/Titanium Security TPM 2.0, Secure Boot, Silicon Root of Trust		Networking	OCP 3.0 (1/10/25/100GbE)	
Security TPM 2.0, Secure Boot, Silicon Root of Trust		Power Supply	1+1 redundant 550W-2700W 80+ Platinum/Titanium	
		Security	TPM 2.0, Secure Boot, Silicon Root of Trust	
OS Support Windows Server, RHEL, SLES, Ubuntu, VMware vSphere 7.0/8.0		OS Support	Windows Server, RHEL, SLES, Ubuntu, VMware vSphere 7.0/8.0	

7. On the server list of servers at the lower part of the page, click the server that the document to be accessed is about.

8. In the **document** list, select **Interface Description**, and all the documents about interface description are display on the right side of the page.

9. Click **Download** to the right of **VANTAGEO Server Redfish Interface Description (BMC**

V4), and download the document.

Glossary

A/D - Analog to Digital AC - Alternating Current ACPI - Advanced Configuration and Power Interface AD - Active Directory AES - Advanced Encryption Standard API - Application Programming Interface ASCII - American Standard Code for Information Interchange BBU - Battery Backup Unit BDF - Bus/Device/Function BIOS - Basic Input/Output System BMC - Baseboard Management Controller CD - Compact Disk CLI - Command Line Interface CPU - Central Processing Unit CRPS - Common Redundant Power Supplies DCMI - Data Center Manageability Interface DHCP - Dynamic Host Configuration Protocol DNS - Domain Name Server DVD - Digital Versatile Disc EPLD - Erasable Programmable Logic Device FC

- Fiber Channel

FQDN - Fully Qualified Domain Name FRU - Field Replaceable Unit **GPIO** - General Purpose Input Output GPU - Graphics Processing Unit GUI - Graphical User Interface HD - Hard disk HTML - HyperText Markup Language HTTP - Hypertext Transfer Protocol HTTPS - Hypertext Transfer Protocol Secure HVDC - High-Voltage Direct Current **I/O** - Input/Output ID - Identification IE - Internet Explorer IP - Internet Protocol **IPMI** - Intelligent Platform Management Interface IPv4 - Internet Protocol Version 4 IPv6 - Internet Protocol Version 6 JRE - Java Runtime Environment KPI - Key Performance Indicator KVM - Keyboard, Video and Mouse LAN - Local Area Network LDAP - Lightweight Directory Access Protocol

LPC

- Lower order Path Connection

LVDC - Low-Voltage Direct Current MAC - Media Access Control NCSI - Network Controller Sideband Interface NIC - Network Interface Card NMS - Network Management System NTP - Network Time Protocol **NVMe** - Non-Volatile Memory Express OS - Operating System PC - Personal Computer **PCle** - Peripheral Component Interconnect Express PECI - Platform Environment Control Interface POST - Power-On Self-Test **PWM** - Pulse-Width Modulation **PXE** - Preboot eXecution Environment RAID - Redundant Array of Independent Disks RMCP - Remote Management Control Protocol **RPM** - Rotations Per Minute SAS - Serial Attached SCSI SATA - Serial ATA SEL - System Event Log SFTP - Secure File Transfer Protocol **SGPIO** - Serial GPIO

SHA

- Secure Hash Algorithm

SMBUS - System Management BUS SMTP - Simple Mail Transfer Protocol SNMP - Simple Network Management Protocol SSH - Secure Shell SSL - Secure Sockets Layer TCP - Transmission Control Protocol TLS - Transport Layer Security UEFI - Unified Extensible Firmware Interface UID - Unit Identification Light USB - Universal Serial Bus iSAC - Integrated Server Administrator Controller VNC - Virtual Network Console VR - Voltage Regulator XML - Extensible Markup Language

iSAC

- Integrated Server Administrator Controller