Dear users:

Copyright © Inspur Electronic Information Industry Co., Ltd. 2019. All rights reserved

No part of this document may be reproduced, modified or transmitted in any form or by any means without the prior written consent of the company.

Trademark statement

Inspur and the Inspur logo are trademarks or registered trademarks of Inspur Group.

All other trademarks or registered trademarks mentioned in this document are the property of their respective owners.

Remarks

The products, services or features you purchase shall be subject to the commercial contracts and terms of Inspur Electronic Information Industry Co., Ltd. All or part of the products, product safety services or features described in this document may not be covered by your purchase or use.

Unless otherwise agreed by the contract, Inspur Electronic Information Industry Co., Ltd. makes no representations or warranties, express or implied, regarding the contents of this document. The contents of this document may be updated from time to time due to product version upgrades or other reasons. Unless otherwise agreed, this document is provided as a guide only, and all statements, information, and recommendations in this document are not warranties of any kind, express or implied.

Inspur Electronic Information Industry Co., Ltd.

Website: www.inspur.com
Address: No. 1036, Langchao Road, Jinan City, Shandong Province, China
Postcode: 250101
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Introduction</td>
<td>5</td>
</tr>
<tr>
<td>1 Hardware security configuration</td>
<td>7</td>
</tr>
<tr>
<td>1.1 Power module installation</td>
<td>7</td>
</tr>
<tr>
<td>1.2 Connect network interface</td>
<td>7</td>
</tr>
<tr>
<td>1.3 Power on</td>
<td>9</td>
</tr>
<tr>
<td>1.4 Power off</td>
<td>10</td>
</tr>
<tr>
<td>2 Firmware security configuration</td>
<td>12</td>
</tr>
<tr>
<td>2.1 Security configuration of system BIOS</td>
<td>12</td>
</tr>
<tr>
<td>2.1.1 How to enter BIOS</td>
<td>14</td>
</tr>
<tr>
<td>2.1.2 BIOS system menu configuration</td>
<td>15</td>
</tr>
<tr>
<td>2.2 BMC security configuration</td>
<td>26</td>
</tr>
<tr>
<td>2.2.1 Get BMC IP</td>
<td>26</td>
</tr>
<tr>
<td>2.2.2 Remote login BMC</td>
<td>27</td>
</tr>
<tr>
<td>2.2.3 BMC Web interface settings</td>
<td>29</td>
</tr>
<tr>
<td>3 System security configuration</td>
<td>39</td>
</tr>
<tr>
<td>3.1 Server hardware maintenance</td>
<td>39</td>
</tr>
<tr>
<td>3.2 Server data backup</td>
<td>40</td>
</tr>
<tr>
<td>3.3 Server software configuration</td>
<td>40</td>
</tr>
<tr>
<td>3.4 Other</td>
<td>41</td>
</tr>
<tr>
<td>4 Conclusion</td>
<td>43</td>
</tr>
</tbody>
</table>
Purpose

This document introduces the security reinforcement methods and suggestions of Inspur server, which are applicable to almost all product models of M5 platform server (such as NF5280M5, NF8480M5, etc.). The purpose is to guide users how to configure the server to achieve the best security, eliminate potential threats and security risks brought by natural and human factors, and improve users' use experience.

Scope

The server is a device that provides services for enterprises and operators and ensures business continuity. Therefore, the security reinforcement of the server mainly involves the security configuration and management of the device, including:

- Hardware security configuration;
- Firmware security configuration;
- System security configuration.

Readers

This document applies to administrators who are responsible for configuring and managing servers. You should be familiar with the basic knowledge of Ethernet and have rich experience in server management.
## Symbols and abbreviated terms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Describe</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>PDU</td>
<td>Power Distribution Unit</td>
</tr>
<tr>
<td>BMC</td>
<td>Baseboard Management Controller</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input Output System</td>
</tr>
<tr>
<td>CMOS</td>
<td>Complementary Metal Oxide Semiconductor</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
</tbody>
</table>
0 Introduction

The security and confidentiality of the whole information in the network is a crucial issue. At present, global information technology has become a major trend of human development. However, due to the diversity of connection forms and uneven distribution of terminals in computer networks based on servers and terminals, and the vulnerability caused by various kinds of application defects, the whole network is vulnerable to hackers, malware and other attacks. Therefore, it is particularly important to guarantee the security and confidentiality of servers that carry and process information. Inspur has made great efforts to solve this problem, and has made a comprehensive and in-depth investigation and analysis of the security problems existing on the server, forming this security configuration manual.

In order to maintain the security of the whole server system, you need to build security measures from multiple levels to discover and deal with various possible security problems in advance. Therefore, how to configure the server safely is particularly important.

In order to improve the security of the server, you need to configure the security of the server system from several aspects:

1. Hardware security configuration

It mainly includes power on and power off of server, network and interface
configuration.

2. Firmware security configuration

It is mainly about the security configuration and use of BIOS and BMC, which are the bottom firmware and start before the server system. Only BIOS and BMC are secure enough can the security of the server system be guaranteed fundamentally.

3. System security configuration

It mainly includes server data backup and server software configuration. These are also critical to server security.

Before you perform any operation on the server, make sure that you have read all the operation instructions of the device, especially the instructions such as danger, warning and attention that may endanger personal and device safety, so as to minimize the probability of accidents.

It is strongly recommended that you make basic security configuration for server to avoid most security problems.

Note: The recommended configuration in this document is not applicable to all Inspur server product models. Please refer to the user manual of the corresponding product model for details.
1 Hardware security configuration

Hardware security configuration includes power on and power off of server, network and interface configuration, including how to install the power module, how to access the network safely, how to ensure the safe power on and power off, and how to check the system information through the serial port in case of system startup problems.

1.1 Power module installation

Generally, the server has multiple power modules. Please ensure that all the power modules are inserted in the power slots of the server. If one of the power modules fails, the other power modules can still maintain the operation of the server and ensure that the business of the server will not be interrupted.

1.2 Connect network interface

There are multiple network interfaces on the server. For the sake of server security, it is recommended not to connect the BMC network to the Internet, but to connect to the enterprise intranet. For how to configure the network parameters of the BMC, please refer to section 2.1.2.

The network port on the back of the server is shown in Figure 1.1, and the description is shown in Table 1.1.
Figure 1.1 schematic diagram of server network port distribution

Table 1.1 interface function description

<table>
<thead>
<tr>
<th>Name</th>
<th>Function and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interface 0/1/2/3</td>
<td>4 gigabit network interfaces per IO riser;</td>
</tr>
<tr>
<td></td>
<td>The indicator LED of the network card is green when the speed is 100MB;</td>
</tr>
<tr>
<td></td>
<td>The indicator LED of the network card is orange at Gigabit rate.</td>
</tr>
<tr>
<td>USB interface 1/2</td>
<td>Connect USB device.</td>
</tr>
<tr>
<td>VGA interface</td>
<td>Connect standard VGA interface display device.</td>
</tr>
<tr>
<td>Management interface</td>
<td>Independent RJ45 Gigabit management interface;</td>
</tr>
<tr>
<td></td>
<td>The system can be monitored and managed through integrated BMC.</td>
</tr>
</tbody>
</table>

Network interface 0/1/2/3 is the public network interface of the server. It can access the operating system and BMC simultaneously by connecting one of the network interfaces. The management interface is a dedicated network interface of BMC, which only allows access to BMC, but not to the server.
1.3 Power on

When powering up the server, pay attention to the status LED, ID LED, and power button on the front control panel of the server. The descriptions of various indicators are in Table 1.2.

Table 1.2 description of indicator light

<table>
<thead>
<tr>
<th>Name</th>
<th>Explain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status indicator LED</td>
<td>Green is always on: the system operates normally after power on; Light off: the system is not powered up normally; Red is always on: the system is abnormal.</td>
</tr>
<tr>
<td>ID indicator LED</td>
<td>When confirming the system ID, the indicator light is always on; This function needs to be realized by management software.</td>
</tr>
<tr>
<td>Power button</td>
<td>System on/off button; After the system is powered on, the button is green and bright.</td>
</tr>
</tbody>
</table>

If you need to view the startup information during the startup process of the server through the server serial port, please connect one end of the serial port line to the client (ordinary PC) and the other end to the serial port on the front of the server. You also need to install a remote login tool (such as putty) on your client computer. The putty interface is shown in Figure 1.2.
Press the switch button on the front control panel of the server, the fan runs, and the system starts self-test.

1.4 Power off

There are two ways to shut down the server system:

1. The server can be shut down through the operation under the operating system;

2. The server can be shut down by manually long pressing the switch button on the front control panel.

After the above two ways of operation, although the server is no longer running, some voltages are still available. At this time, the system can be powered on through remote management. To achieve a complete shutdown, you need to disconnect the AC power supply of the system (that is, unplug
the power cord or turn off the power supply plug).
2 Firmware security configuration

2.1 Security configuration of system BIOS

The purpose of this section is to guide the user how to configure the system BIOS safely. The specific operations include how to restore the BIOS to the default settings when the system crashes, how to enter the BIOS and configure various security parameters.

Generally, the factory default settings of the system are optimization settings. Before understanding the meaning of each parameter, if there is no special need, it is recommended that you use the default value, and do not change the parameter settings at will. Because BIOS has a significant impact on the operation and startup of the system, setting improper parameters may cause conflicts between hardware resources, or reduce the performance of the system. In addition, the content of BIOS will change according to the different configuration of the product or the update of BIOS version.

Before changing the BIOS settings of the server, please record the corresponding initial settings, so that when the system is abnormal due to the modification of options, it can be restored according to the recorded initial settings.

If you modify some options during the use process and cause the system to
crash, you can restore the BIOS to the default settings through the clear CMOS function, which can be realized in two ways:

1. Unplug CMOS battery
   1) Power down the server AC;
   2) Unplug CMOS battery and wait for two minutes;
   3) Replace CMOS battery and power on the AC.

The CMOS battery and its removal method are shown in Figure 2.1.

![Figure 2.1 step of removing COMS battery](image)

2. CMOS Jumper
   1) Power off the server AC;
   2) Change the main board CMOS jumper from 1, 2 pin short circuit to 2, 3 pin short circuit;
   3) Restore the CMOS jumper to its original position and power on the AC.

The location of CMOS jumper on the server motherboard is shown in Figure 2.2.
Figure 2.2 location of CMOS jumper on main board

(Note: the system time will be reset if the CMOS battery is removed, so the jumper mode is recommended.)

You can also restore the BIOS function through ‘load default’ option. When BIOS cannot be started normally due to BIOS configuration error, an error prompt window will pop up on the screen during BIOS startup, indicating that you can restore BIOS function by clicking ‘load default’ option.

2.1.1 How to enter BIOS

Power on and start the server. When the logo screen is displayed, the bottom of the screen will prompt ‘press <del> to setup or <tab> to post or <F11> to boot menu or <F12> to PXE boot’. Press the <del> key quickly, and the system will enter the BIOS setting interface.

If the above operations do not enter the setting interface, press <Ctrl> +
<ALT> + <del> at the same time to restart the system and repeat the above operations.

According to the above operations, enter the BIOS main interface, as shown in Figure 2.3.

![BIOS Startup Interface](image)

Figure 2.3 BIOS startup interface

2.1.2 BIOS system menu configuration

The BIOS Setup program includes the following main function menus, among which the security related options are shown in Table 2.1.
Table 2.1 safety related menu description

<table>
<thead>
<tr>
<th>Menu name</th>
<th>Menu function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>Set basic system time, system date, display BIOS version, CPU model, system memory capacity and other information.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Set advanced features of CPU, integrated SATA controller, etc.</td>
</tr>
<tr>
<td>Chipset</td>
<td>Configure processor, QPI, memory, IIO, PCH, ME and some general configurations.</td>
</tr>
<tr>
<td>Server Mgmt</td>
<td>Configure server management features.</td>
</tr>
<tr>
<td>Security</td>
<td>Configure the super user and user password of the system.</td>
</tr>
<tr>
<td>Boot</td>
<td>Set the boot order of system devices.</td>
</tr>
<tr>
<td>Save &amp; Exit</td>
<td>Save BIOS settings, exit BIOS settings, etc.</td>
</tr>
</tbody>
</table>

1. Advanced menu

Figure 2.4 Advanced menu
Advanced menu (Figure 2.4) is mainly used to set the enhanced features. If it is not set properly, it may cause abnormal operation of the system. It is recommended to use the default settings.

Only the main and common submenus or options are described below.

1) Trusted Computing

This item displays TPM related information (Figure 2.5). If your server does not have a TPM chip, ignore this submenu.

![Figure 2.5 security device support](image)

If you need to use the TPM feature, set the ‘Security Device Support’ option to ‘Enable’. If you have trusted software business on your server, please turn on trusted related devices through options such as ‘Storage Devices’, or turn off trusted devices.
2. Server Mgmt menu

Server Mgmt menu (Figure 2.6) provides setting function items and FRU related information for system management.

Only the main and common submenus or options are described below.

1) FRB-2 Timer

This item is used to set whether to start the timing function of FRB-2. There are two options: [enabled] \ [disabled].

2) FRB-2 Timer timeout

This item is used to set the time for starting FRB-2. The default setting is 6 minutes.

3) FRB-2 Timer Policy

<table>
<thead>
<tr>
<th>BMC Self Test Status</th>
<th>FRB-2 Timer</th>
<th>FRB-2 Timer Timeout</th>
<th>FRB-2 Timer Policy</th>
<th>OS Watchdog Timer</th>
<th>OS Htd Timer Timeout</th>
<th>OS Htd Timer Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passed</td>
<td>[Enabled]</td>
<td>[6 minutes]</td>
<td>[Power Cycle]</td>
<td>[Disabled]</td>
<td>[10 minutes]</td>
<td>[Reset]</td>
</tr>
</tbody>
</table>

Figure 2.6 Server Mgmt menu
This item is used to set the actions that the system will perform after the arrival of the time. There are four options: "restart", "reset (default)", "shut down" and "do nothing".

4) BMC network configuration

This item is used to view the configuration information of BMC network interface, as shown in Figure 2.7.

![BMC network configuration](image-url)

Figure 2.7 BMC network configuration
Figure 2.8 shared network settings

① Sharelink Network

This is used to enable/disable the shared network (Figure 2.8). If enable is selected, the public network interface of the server can access the server and BMC at the same time. If this item is disabled, the public network interface of the server can only be used to access the server. For your data security, it is recommended that you do not connect the BMC to the Internet.

Do nothing: to use the last configuration without change.

Auto: indicates the IP address obtained automatically.

Manual: which means to manually configure the BMC's IP, gateway and other information.

If you select ‘Manual’ in ‘Get BMC Sharelink Parameters’, you can select ‘Configuration Address source’, which also has three options: ‘Unspecified’, ‘Static’ and ‘Dynamicbmcdhcp’.

Unspecified: indicates that no specific parameters are specified for this network configuration, and the system will use the last configuration;

Static: which means ‘Station IP address’, ‘Subnet mask’ and ‘Router IP address’ can be configured by yourself.

Dynamicbmcdhcp: indicates that the system will automatically assign dynamic BMC network parameters.

The configuration steps of ‘BMC dedicated management channel’ are the same as above.

5）BMC User Settings

This item is used to add, delete, and configure BMC user permission levels, as shown in Figure 2.9.

① Add User
Here you need to set the user password according to the following requirements:

1. The password must be within the range of 8-64 characters;
2. The password must start with English letters, at least three combinations of uppercase letters, lowercase letters, numbers and special characters (except for spaces), and the user name cannot be a part of the password;
3. Spaces are not allowed;
4. When you modify the password, the new password cannot be the same as the password before modification;
5. The password shall not be set in simple numerical arrangement or obvious English words, and the password shall be changed regularly;
There are 5 options for ‘User Privilege Limit’:

- No Access
- User
- Operator
- Administrator
- OEM Proprietary

Only administrator account has ‘Administrator’ operation permission. Other users can be assigned one of the remaining four operation permissions as required.

② Delete User

The user account can only be deleted with administrator permission.

③ Change User Settings

Only with administrator's permission can the password and operation permission of user account be changed.

3. Security settings

Security settings are shown in Figure 2.10.
Figure 2.10 Security settings

1) Account classification settings

It is necessary to set the account hierarchically. It supports two accounts, ‘Administrator’ and ‘User’. Password and permission are separated. ‘Administrator’ has the highest permission. Only through ‘Administrator’ can ‘User’ accounts be added or deleted. ‘User’ only have the minimum access rights, such as the basic options of only modifying system time and restoring factory default values.

2) Secure boot

The purpose of secure boot is to prevent malware intrusion. UEFI stipulates that when the main board leaves the factory, some reliable public keys can be built in. Any operating system or hardware driver that wants to load on
this motherboard must pass the authentication of these public keys.

In UEFI mode, you can choose to enable/disable ‘Secure boot’. In Legacy mode, ‘Secure boot’ is invalid. When ‘Secure boot’ is enabled, if you want to install other operating systems or hardware drivers other than windows on the server system, you must pass the public key authentication issued by Microsoft.

4. Boot Menu

![Boot menu](image)

Figure 2.11 Boot menu

In order to ensure the physical security of your server, you should also configure the system so that it is only allowed to boot from the hard disk and prevent the intruder from starting your server from the removable media.
Log in to the server's BIOS as an administrator before configuration. The specific configuration steps are as follows:

1) Select the ‘Boot’ menu, and its main interface is as shown in the figure above;
2) Under ‘Boot Option Priorities’, select ‘Boot Option#1’, press ‘Enter’ and then select the hard disk you want to start;
3) Select the hard disk you want to start, press ‘Enter’ to return to the ‘Boot’ interface;
4) Press F10 to save the configuration and exit the interface, then the system starts.

2.2 BMC security configuration

BMC is responsible for monitoring and managing the running status of the server, so you should pay attention to its security. The purpose of this section is to guide you to complete the security configuration of BMC and fundamentally eliminate the existence of unsafe factors. The specific operations include obtaining BMC IP, logging in BMC web remotely and configuring BMC safely.

2.2.1 Get BMC IP

BMC IP address can be viewed or set in ‘Server MGMT’ -> ‘BMC network configuration’ -> ‘Station IP address’ menu in BIOS.
If you reset the BMC IP address, you need to reboot or power down the server (unplug the power cord) after saving to use it normally.

### 2.2.2 Remote login BMC

#### 1. Remote client system requirements

The client system requirements for connecting to the server BMC GUI interface through a web browser are shown in Table 2.2.

Table 2.2 client system requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Remote web console/client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client OS</td>
<td>Windows 7.1 x64, Windows 8 x64, Windows 10 x64, Ubuntu 14.04.03 LTS x64, MAC OS X, Fedora 23 x64</td>
</tr>
<tr>
<td>Browser Versions</td>
<td>On Windows Clients: Edge, Firefox 43, Chrome 47+, IE 11+; On Linux Clients: Firefox 43, Chrome 47+; On MAC Client: Safari</td>
</tr>
<tr>
<td>Java KVM</td>
<td>User should download and open JNLP (Java Application), JRE environment should be read; Supported JRE version: jre-7u40 and above, jre-8u45 and above.</td>
</tr>
<tr>
<td>TCP/IP network protocol stack</td>
<td>Support TCP/IP network protocol stack.</td>
</tr>
</tbody>
</table>

You can use Inspur driver CD to enter the Java directory under the CD root directory and install the browser plug-in directly.

Before logging in to the remote Web interface, the client should install the browser plug-in, and set the IP of the remote client in the same network segment as that of the BMC.
2. Remote login method

Enter the IP address of BMC in the IP address column of client browser and press enter to open the management login interface, as shown in Figure 2.12.

![BMC remote login Web interface](image)

Figure 2.12 BMC remote login Web interface

Please enter the default username and password of the administrator:

Username: admin
Password: admin

The default username and password can be used to configure and set permissions for all modules. Therefore, in order to ensure system security, it is recommended that you modify the login password in time after login.

If you want to exit the current login, please click the ‘logout (or exit)’ button on the page to invalidate the session immediately.

When the system administrator logs in to BMC, the number of login attempts of the user account should be defined first, generally set as 6 times/minute, and then set the time of locking login after login failure,
which should not be less than 5 minutes and the recommended setting is 30 minutes.

2.2.3 BMC Web interface settings

After logging in to the system, the left side of the interface is the navigation tree. Through the nodes of the navigation tree, different function interfaces can be selected.

1. BMC settings


1) Service settings

This interface can be used to set up and view the services supported by BMC.
Select a service, and then modify its interface, non-security port number, security port number and other information according to your needs. It is recommended to close unnecessary ports and services, check the service operation regularly, and make sure that the prohibited and enabled services are normal.

The insecure services include SSH and SoLSSH, which are turned off by default. If you choose to turn on SSH, you will face the following risks: timing attack, denial of service attack (DoS), man in the middle attack, etc.

2) User settings

Users can be added, deleted, and modified to a maximum of 16 users.
Figure 2.14 users settings

Please refer to section 2.1.2 for user name and password settings. The length of user password can be 16 or 20 bits. Please log in with the administrator account, disable or delete all user accounts and group accounts not used.

BMC user rights include administrator, operator, user, OEM exclusive and no access rights. Different user rights support different operations, as shown in Table 2.3.
Table 2.3 user rights

<table>
<thead>
<tr>
<th>User privileges</th>
<th>Supported operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>Read/Write</td>
</tr>
<tr>
<td>operator</td>
<td>Read</td>
</tr>
<tr>
<td>user</td>
<td>Read</td>
</tr>
<tr>
<td>No authority</td>
<td>None</td>
</tr>
</tbody>
</table>

In case of any of the following circumstances, the account number shall be revoked or the password of the account number shall be changed immediately, and records shall be made:

① The account user no longer needs the original access rights due to the change of post responsibilities, resignation and other reasons;

② Temporary or phased accounts shall be used after the completion of work;

③ The account user violates the password management regulations.

3) IP access control

This item is used to set that only devices within an IP segment can access BMC, as shown in Figure 2.15.
4) Disable BMC shared network

If the BMC shared management network is enabled, the BMC can use the public network interface of the system. Based on security consideration, it is recommended to disable the BMC shared management network, and the BMC should use a private network interface.
2. Log

Select ‘log’ in the navigation tree to open the log related pages, including six pages: ‘System Event Log’, ‘BMC System Audit Log’, ‘Event Log Setting’, ‘BMC Syslog Setting’, ‘One-key collection Log’ and ‘IDL Log’. When the system prompts that the log will be full of alarm information, please log in to the system as administrator account to delete or export the logs.

![Figure 2.17 log settings](image)

3. System maintenance

System maintenance functions include: ‘(BMC) Dual Firmware Update’, ‘BIOS FW Update’, ‘User Administration’, etc.

1) BMC/BIOS firmware update
When updating the BMC version, you must check the integrity of the firmware image. The verification method is as follows:

1. Run MD5 verification tool, which is sent along with BMC image;
2. Import the BMC image file into the verification tool;
3. Start the verification and record the result at the same time;
4. Compare the verification result with the standard MD5 value issued by Inspur. If it is consistent, the BMC image is complete. Otherwise, the BMC image is incomplete.

BIOS firmware update is the same as BMC firmware, and the integrity of BIOS image needs to be verified before upgrading. Refer to BMC image
verification process for verification process.

In addition, when uploading a new BMC or BIOS image file, please use the correct file. Any image file not released by Inspur and not applicable to the server type is not allowed to be uploaded.

2) User Administration

![User Administration Settings](image)

Figure 2.19 user administration settings

This item is used to modify the system administrator password. The password setting shall meet the security requirements of password length and complexity. For details, please refer to section 2.1.2. If you use a weak password with low complexity, there will be a security risk of password brute force cracking. Please be careful.
4. IPMI safety switch

This section introduces the opening mode, application and influence of IPMI safety switch.

At present, the only security switch that is turned off by default is ASPEED chip security mechanism switch.

When the chip security mechanism switch of the ASPEED chip is turned off, it allows any read-write access to the physical address space of the BMC from the host (or from the network in the special case that UART of the BMC console is connected to the serial concentrator). It can cause arbitrary reading and writing of BMC physical address space in the host; when the switch is turned on, it will affect the use of the host OS installation, BIOS option management out of band and other key functions.

The relevant commands are as follows:

1) Command to permanently close the chip security mechanism: ‘ipmitool -I lanplus -H ip address -U (user name) -P (password) raw 0x3c 0x3a 0x1e 0x00’.

2) Command to permanently open the chip security mechanism: ‘ipmitool -I lanplus -H ip address -U (user name) -P (password) raw 0x3c 0x3a 0x1e 0x01’.

3) Command to close the chip security mechanism once: ‘ipmitool -I lanplus -H ip address -U (user name) -P (password) raw 0x3c 0x3a 0x1e 0x02’.
4) Single open: note that the single open command is only valid when the chip security protection mechanism is enabled permanently. After the BMC is restarted, the command fails.

5) Query the status of chip security mechanism: ipmitool -I lanplus -H ipaddress -U(user name) -P(password) raw 0x3c 0x3b 0x1e. Return value: 0(close), 1(open), 2(single close).
3 System security configuration

This section is the system security configuration of the server. The purpose is to help users configure the server in a comprehensive and safe way. The main contents include: server hardware maintenance, server data backup, server software configuration and others.

3.1 Server hardware maintenance

When uninstalling and replacing the server, please read the instructions carefully, do not forcibly dismantle it. Before operation, you must completely cut off the power supply and conduct it under the condition that the server is well grounded to prevent static electricity from damaging the server.

When installing and replacing server parts, you also need to pay attention to the following:

1. Wear anti-static wrist strap during installation and replacement of parts to prevent electrostatic damage to you and equipment.

2. Keep the area where the parts are located clean and keep the parts away from heat generating equipment such as radiator.

3. When operating parts, make sure that the cuff is tied tightly or rolled over the elbow. For safety, it is recommended not to wear jewelry, watches, metal frame glasses or clothes with metal buttons.
4. Avoid operation such as excessive force or forced pulling and inserting, so as not to damage the physical appearance of components or lead to connector failure (such as pin bending, pin short circuit, etc.).

It is recommended that you upgrade the server at regular intervals. If you need to replace the memory or hard disk, it is recommended that you replace it with the same model.

It is recommended that you dust the server, especially the power supply and check the network of the server regularly.

3.2 Server data backup

In case of emergency, it is recommended that you back up the data on the server every day and place the backup data on different servers. And regularly organize the data stored on the server.

However, there are also huge security holes in data backup, because the backed up data may also be stolen, so the backup media should be effectively password protected during backup, and encryption software should be used to encrypt these data when necessary, so even if the data is stolen, there will be no data leakage problem.

3.3 Server software configuration

In the operating system of the server, it is recommended that you regularly check the event viewer to see if there are any exception records in the
system log, security log and application log. And regularly install the latest patches or upgrade packages for the server's operating system and anti-virus software.

It is recommended that you use vulnerability scanning and risk assessment tools to scan the server regularly to find potential security problems and ensure that normal maintenance such as upgrading or modifying the configuration will not bring security problems.

For data security reasons, it is recommended to change all partitions of the server to NTFS format.

The server administrator shall not install any software and application programs irrelevant to system security and website operation on the server, enhance the key file attribute setting and the authority control of some key files, prevent misoperation and reduce security risks.

If you use the server as an internal server, it is recommended that you configure the server firewall to block the access of external personnel.

3.4 Other

The firmware version of BMC will be upgraded irregularly to fix security problems and vulnerabilities.

The person in charge manages account and password of the server uniformly. Except for the authorization of the responsible person and no one else is allowed to have account and password of the server.
It is recommended that you establish a security incident response mechanism to deal with safety accidents, so as to ensure that production can be resumed and vulnerabilities can be solved as soon as possible after safety accidents occur, and the loss can be minimized.
4 Conclusion

This configuration manual is different from the server user manual and does not cover the complete server operation steps, but it shows you how to use the server more safely, which is very important for you. We hope that this manual can help you to configure the server safely and protect it from attacks, viruses, etc.