Inspur Server i24&NS5162M5 Server Acceptance Manual

Version **1.2**

Realease date **2020-01**

Honorific customer:

Note: The products, services or features you purchase should be subject to Inspur Group's commercial contracts and terms. All or part of the products, services, or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Inspur Group makes no express or implied statement or warranty on the contents of this document. The content of this document may be updated from time to time due to product version upgrades or other reasons. Unless otherwise agreed, this document is intended as a guide only, and all statements, information, and recommendations in this document do not constitute any express or implied warranty.

Technical Service： 4008600011

Address： 1036 Langchao Road, Jinan City, China
Inspur Electronic Information Industry Co., Ltd.

Postcode： 250101

Version Update

Date	Version	Prepared / Revised	Reviewer	Approver	Description
2020-01-10	1.2				

Contents

Contents...iii

1 Hardware Test...4

1.1 Hardware Test...4

1.1.1 Packaging...4

1.1.2 Chassis...5

1.1.3 PSUs...5

1.1.4 Hardware Detection...7

1.1.5 Hard Disk Controllers...8

1.1.6 Alarm, Firmware Version, and Hardware Status Detection...10

2 CMC Test...12

2.1 CMC Test...12

2.1.1 CMC Test...12

3 BMC Test...18

3.1 BMC Test...18

3.1.1 BMC Test...18

4 Hard Disk Controller Test...28

4.1 Hard Disk Controller Test...28

4.1.1 Configuring RAID1...28

4.1.2 Configuring RAID5...29

5 Network Port PXE...31

5.1.1 Network Port PXE...31

6 Customer Acceptance Sign-off Sheet...33

1 Hardware Test

1.1 Hardware Test

1.1.1 Packaging

Table 1- 1

Item	**Content**
Objective	To verify the server packaging.
Prerequisites	The structure of the mainboard and hard disk backplane is intact.
Procedure	1. Check whether the packaging is intact and not soaking. 2. Check whether the anti-shock or anti-dumping label turns red (if there is a corresponding label). The common labels are as follows: 3. Check the components in the carton against the packing list.
Expected result	1. The packaging is in good condition and has no water stain. 2. The anti-shock or anti-fall label is green. 3. All components listed in the packing list are intact.
Description	None

1.1.2 Chassis

Table 1- 2 Chassis Structure

Item	Content
Objective	To verify the server chassis structure.
Prerequisites	The structure of the mainboard and hard disk backplane is intact.
Procedure	1. Check whether there are any scratches or oxidation on the chassis surface or deformation of the chassis cover. 2. Check whether the mounting ears are in good condition and properly install. 3. Check whether the surface label and mylar label are damaged or missing.
Expected result	1. The chassis is in good condition, without scratches, oxidation, or deformation. 2. The mounting ears are in good condition and properly installed. 3. The surface label and mylar label of the case are complete and not damaged.
Description	None

1.1.3 PSUs

Table 1- 3 PSUs

Item	Content
Objective	To verify the installation and power-on status of the power supply units (PSUs).
Prerequisites	The structure of the mainboard and hard disk backplane is intact.

Procedure	1. Install PSUs into the slots. You can install one to four PSUs, and install filler modules in the vacant slots. 2. Connect power cables to the PSUs, wait for 10 seconds, and press the power button to power on the server.
Expected result	1. The PSUs and filler panel are installed smoothly and properly. 2. The PSUs fit the chassis properly. 3. The PSUs are working properly and the indicators are steady green when the server is being powered on. 4. No abnormal noise is heard during the power-on operation.
Description	None

Table 1- 4 PSU Hot Swap Function

Item	Content
Objective	To verify the PSU hot swap function.
Prerequisites	The structure of the mainboard and hard disk backplane is intact.
Procedure	1. Insert one PSU into the slot. 2. Connect the power cables and wait 10 seconds till the server is powered on. 3. Insert second PSU into another slot. Connect power cables to the PSU and check that the power status indicator is steady green. 4. Remove the first PSU from the slot. 5. Insert the first PSU into the slot. Connect power cables to the PSU and check that the power status indicator is steady green. 6. Remove the power cable from the second PSU,

Expected result	The server is operating properly during the test.
Description	None

Table 1- 5 PSU Backup Function

Item	Content
Objective	To verify the PSU backup function.
Prerequisites	The structure of the mainboard and hard disk backplane is intact.
Procedure	1. Insert two PSUs into the server. 2. Connect power cables to the PSUs and wait 10 seconds until the server is powered on. 3. Check that the power status indicators on the PSUs are steady on. 4. Remove the power cable from the first PSU, and remove the first PSU from the slot. Check that the other PSU and the server are operating properly. 5. Insert the first PSU into the slot. Check that the power status indicator is steady on. 6. Remove the power cable from the second PSU, and remove the second PSU from the slot. Check that the other PSU and the server are operating properly.
Expected result	The server is operating properly during the test.
Description	None

1.1.4 Hardware Detection

Table 1- 6 Hardware Detection

Item	Content

Objective	To verify that the system detects hardware properly.
Prerequisites	The structure of the mainboard and hard disk backplane is intact.
Procedure	1. Power on the system, during the system startup, press DEL to enter the BIOS setup screen. 2. View the CPU model and quantity. 3. View the total memory capacity. 4. Choose Advanced > PXE Configuration, and view the MAC addresses of the network ports. 5. View the system serial number (S/N). 6. View the basic input/output system (BIOS) version.
Expected result	1. The BIOS SETUP screen is displayed. 2. The CPU model and quantity are the same as the actual configurations. 3. The total memory capacity is consistent with actual configurations. 4. Choose Advanced > PXE Configuration, the MAC addresses of the network ports are displayed. 5. The System S/N parameter is specified. 6. The BIOS version is displayed. 7. No abnormal noise is heard during the startup.
Description	None

1.1.5 Hard Disk Controllers

Table 1- 7 Hard Disk Controllers

Item	**Content**
Objective	To verify that the RAID controller card operates properly.（LSI

	SAS 3008)
Prerequisites	The structure of the mainboard and hard disk backplane is proper, and hard disks are detected after the server is powered on.
Procedure	1. Power on the system, log in to the web interface through the management network port. Press Ctrl+C to enter controller card setup screen during the system startup.(UEFI mode needs to be viewed in the BIOS) 2. View the LSI SAS 3008 BIOS version and the firmware version on the displayed screen. 3. On the Adapter Properties screen, check the NVDATA version. 4. 。On the SAS Topology menu, expand the menu, and check the hard disk model and quantity.
Expected result	1. The SETUP screen is displayed after you press Ctrl+C. 2. The LSI SAS3008 BIOS versions, firmware versions, and NVDATA versions are displayed. 3. The hard disk model and quantity are the same as actual configurations.
Description	None

Table 1- 8 Hard Disk Controllers

Item	**Content**
Objective	To verify that the RAID controller card operates properly.（LSI SAS 3108)
Prerequisites	The structure of the mainboard and hard disk backplane is proper, and hard disks are detected after the server is powered on.

Procedure	1. Power on the system, log in to the web interface through the management network port, and access the KVM. During the LSI SAS 3108 startup, press Ctrl+C to enter controller card setup screen. (UEFI mode needs to be viewed in the BIOS) 2. Check the number, location, and capacity of hard disks in "PD Mgmt",. 3. On the Properties screen, check the Package/FW Version/BIOS Version
Expected result	1. Enter the configuration interface of the controller. 2. The Package / FW Version / BIOS Version information of the controller can be displayed normally. 3. The quantity, location, and capacity of hard disks are the same as the actual purchase configuration.
Description	None

1.1.6 Alarm, Firmware Version, and Hardware Status Detection

Table 1-9 Alarm Detection

Item	Content
Objective	To verify that the indicator has any alarms.
Prerequisites	The structure of the mainboard and hard disk backplane is proper, and hard disks are detected after the server is powered on
Procedure	1. Check the front panel indicator for any abnormalities. (Please refer to the maintenance manual for details) 2. Check the power module and network port indicators for

	abnormalities. 3. Check if the hard disk indicator is abnormal.
Expected result	1. The front panel indicator is normal. 2. The power module and network port indicators are normal. 3. The hard disk indicator is normal.
Description	None

Table 1-10 Hardware Detection

Item	**Content**
Objective	Test BMC basic functions
Prerequisites	The structure of the mainboard and hard disk backplane is proper, and hard disks are detected after the server is powered on.
Procedure	1. Whether the BMC Network Configuration can be entered normally in the BIOS. 2. Details of BMC management function acceptance, please see "2.1 BMC management function acceptance" below.
Expected result	1 . The BMC Network Configuration can be entered normally in the BIOS.
Description	None

2 CMC Test

2.1 CMC Test

2.1.1 CMC Test

Table 2- 1 Web Interface—We Interface Login

Item	Content
Objective	To verify the Web interface login function.
Prerequisites	AC power is supplied to the server. The CMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the CMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx(xxx.xxx.xxx.xxx is the static CMC ip address that has been set) 2. In the Security Alert dialog box, click Yes. 3. On the login page, select 中文（简体）, then English, and 中文（简体）. 4. Log in with the user name and the default password. 5. Enter the default user name and password again, and click Log In. 6. Wait 5 minutes without performing any operation, and click a menu in the navigation tree.

Expected result	1. The CMC login page is displayed, and the URL in the address box starts with https://. 2. The GUI language is correctly set, and the login pages in different languages between 中文（简体）and English are displayed correctly. 3. The user name is displayed in plaintext, and the password in ciphertext. 4. The web server automatically times out by default within 5 minutes. You need to log in again after the timeout.
Description	Required for acceptance

Table 2- 2 Web Interface—Power-On and Power-Off on the WebUI

Item	**Content**
Objective	To verify that you can power on and power off the server on the WebUI.
Prerequisites	AC power is supplied to the server. The CMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the CMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static CMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose Power on the menu bar, and choose Power Control in the navigation tree.

	4. On the Virtual Power Buttons page, click Power On and then Yes. 5. On the Virtual Power Buttons page, click Power Off and then Yes. 6. On the Virtual Power Buttons page, click Forced System Reset and then Yes. 7. Choose Alarm & SEL on the menu bar, choose System Events in the navigation tree, and view system event logs.
Expected result	1. There are interfaces for node operation on the web page, including "power on", "power off", "forced power off", "restart", "restart BMC", and "restore factory settings". 2. After you select Power Off, make sure it starts to shut down and will not turn on automatically. 3. After you select Power On, the server is powered on and the OS is started. 4. After you select Reset, the server OS restarts successfully. 5. After performing the restart BMC operation, confirm that the BMC has performed the restart operation, and the BMC can log in again after a suitable time. 6. The power-on and power-off operations are logged successfully.
Description	Required for acceptance

Table 2-3 Web Interface—IP Address Configuration on the WebUI

Item	Content
Objective	To verify that you can configure an IP address for the server on the WebUI.
Prerequisites	AC power is supplied to the server.

	The CMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the CMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx(xxx.xxx.xxx.xxx is the static CMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose Configuration > CMC Network. On the displayed page, check that the IP address obtaining mode, IP address, subnet mask, default gateway, and MAC address of the CMC are displayed. 4. Select Automatically obtain IP address and check that all parameters below are unavailable. 5. Select Manually set IP address, enter an IP address, subnet mask, and default gateway, and click Save. Ensure that the new IP address is on the same network segment as that of the terminal. 6. Use the new IP address to log in to the CMC WebUI.
Expected result	1. The IP address is properly configured. 2. The new IP address, subnet mask, and gateway are displayed on the WebUI. 3. The new IP address takes effect and can be used to log in.
Description	Acceptance options.

Table 2- 4 Web Interface—Firmware Upgrade on the WebUI

Item	Content
Objective	To verify that you can upgrade the CMC firmware on the WebUI.
Prerequisites	AC power is supplied to the server. The CMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the CMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx(xxx.xxx.xxx.xxx is the static CMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose System > CMC Firmware Upgrade, the Firmware Upgrade page is displayed. 4. Select the CMC software upgrade package and click Upgrade.
Expected result	1. Update CMC on WebUI. 2. The CMC versions is correctly displayed. The textbox for importing upgrade packages is displayed. 3. The upgrade progress bar is properly displayed.
Description	Acceptance options.

Table 2-5 Web Interface—CMC System Logs on the WebUI

Item	Content
Objective	To verify CMC system logs on the WebUI.
Prerequisites	AC power is supplied to the server.

	The CMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the CMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static CMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose Log information> CMC System Events and view CMC logs in the right pane.
Expected result	1. System logs are displayed in descending order based on the time. Each record contains the Severity, ID, Event Source, Sensor, Description, Generated, and Status. 2. Each page displays a maximum of 10 records. You can view the total number of pages or records and go to the first page, previous page, next page, last page, or a specific page.
Description	Acceptance options.

3 BMC Test

3.1 BMC Test

3.1.1 BMC Test

Table 3- 1 Web Interface—Web Interface Login

Item	Content
Objective	To verify the Web interface login function.
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. In the Security Alert dialog box, click Yes. 3. On the login page, select 中文（简体）, then English, and 中文（简体）. 4. Log in with the user name and the default password. 5. Enter the default user name and password again, and click Log In. 6. Wait 5 minutes without performing any operation, and click a menu in the navigation tree.

Expected result	1. The BMC login page is displayed, and the URL in the address box starts with https://. 2. The GUI language is correctly set, and the login pages in different languages between 中文（简体）and English are displayed correctly. 3. The user name is displayed in plaintext, and the password in ciphertext. 4. The web server automatically times out by default within 5 minutes. You need to log in again after the timeout.
Description	Required for acceptance

Table 3- 2 Web Interface—Power-On and Power-Off on the WebUI

Item	**Content**
Objective	To verify that you can power on and power off the server on the WebUI.
Prerequisites	The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose Power on the menu bar, and choose Power Control in the navigation tree. 4. On the Virtual Power Buttons page, click Power On and

	then Yes. 5. On the Virtual Power Buttons page, click Power Off and then Yes. 6. On the Virtual Power Buttons page, click Forced System Reset and then Yes. 7. Choose Alarm & SEL on the menu bar, choose System Events in the navigation tree, and view system event logs.
Expected result	1. The options Power On, Power Off, and Forced System Reset are displayed. 2. After you select Power Off, the OS shuts down and the server powers off. 3. After you select Power On, the server is powered on and the OS is started. 4. After you select Reset, the server OS restarts successfully. 5. The power-on and power-off operations are logged successfully.
Description	Required for acceptance

Table 3-3 Web Interface—UID Indicator on the WebUI

Item	Content
Objective	Configure positioning indicator for the server on the WebUI.
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx

	(xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Select “Information”-> “Information Overview”, and check “Location Indicator” in “Virtual Button”. 4. Select the "On". 5. Select the "Off". 6. Select the "Blink".
Expected result	1. Select "On", the positioning light is on. 2. Select "Off" and the positioning light goes out. 3. Select "Blink" and the positioning light blinks.
Description	The temporary indicator of the positioning indicator is blinking, the frequency is 1Hz, and the indicator is blue. Required for acceptance.

Table 3-4 Web Interface—Remote KVM on the WebUI

Item	Content
Objective	To verify the remote KVM over Java on the WebUI.
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set)

	2. Enter the user name root and the default password, and click Log In. 3. Choose Remote > Remote Virtual Console.
Expected result	A page is displayed, allowing you to use remote KVM
Description	Required for acceptance.

Table 3- 5 Web Interface—IP Address Configuration on the WebUI

Item	**Content**
Objective	To verify that you can configure an IP address for the server on the WebUI.
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose Configuration > Network. On the displayed page, check that the IP address obtaining mode, IP address, subnet mask, default gateway, and MAC address of the BMC are displayed. 4. Select Automatically obtain IP address and check that all parameters below are unavailable. 5. Select Manually set IP address, enter an IP address, subnet

	mask, and default gateway, and click Save. Ensure that the new IP address is on the same network segment as that of the terminal. 6. Use the new IP address to log in to the BMC WebUI.
Expected result	1. The IP address is properly configured. 2. The new IP address, subnet mask, and gateway are displayed on the WebUI. 3. The new IP address takes effect and can be used to log in.
Description	After the new IP address is configured or obtained, use the new IP address to log in again.

Table 3-6 Web Interface—Firmware Upgrade on the WebUI

Item	Content
Objective	To verify that you can upgrade the firmware on the WebUI.
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose System > Firmware Upgrade, the Firmware Upgrade page is displayed. 4. Select the BMC software upgrade package and click

	Upgrade. 5. Select the BIOS software upgrade package and click Upgrade
Expected result	1. The BIOS and BMC are upgraded. 2. The BIOS and BMC versions are correctly displayed. The textbox for importing upgrade packages is displayed. 3. The upgrade progress bar is properly displayed.
Description	Acceptance options.

Table 3- 7 Web Interface—System Boot Option on the WebUI

Item	Content
Objective	To verify that you can set the system boot option on the WebUI
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network. The DVD-ROM drive is connected to the server, and the PXE is properly configured.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose Configuration > Boot Device. 4. Select DVD-ROM and click Save. 5. Restart the server and check whether the setting takes

	effect. 6. Select PXE and click Save. 7. Restart the server and check whether the setting takes effect. 8. Select No override and click Save. 9. Restart the server and check whether the setting takes effect.
Expected result	1. The system startup options Hard Drive, DVD-ROM, FDD/Removable Device, PXE, and No Override are displayed. 2. The system boots from the DVD-ROM drive. 3. The system boots from the PXE. 4. The system boots based on the BIOS settings.
Description	Acceptance options.

Table 3- 8 Web Interface—System Logs on the WebUI

Item	Content
Objective	To verify system logs on the WebUI.
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. Enter the user name root and the default password, and

	click Log In. 3. Choose Alarm&SEL > System Events and view BMC logs in the right pane.
Expected result	1. System logs are displayed in descending order based on the time. Each record contains the Severity, ID, Event Source, Sensor, Description, Generated, and Status. 2. Each page displays a maximum of 10 records. You can view the total number of pages or records and go to the first page, previous page, next page, last page, or a specific page.
Description	Acceptance options.

Table 3-9 Web Interface—User Management Function on the WebUI

Item	**Content**
Objective	To verify the user management function on the WebUI.
Prerequisites	AC power is supplied to the server. The BMC network port IP address has been set. Internet Explorer 8.0/9.0/10.0, Firefox 9.0 has been installed on the terminal. The terminal is connected to the BMC network port on the target server over the network.
Procedure	1. In the address box, enter http://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx is the static BMC ip address that has been set) 2. Enter the user name root and the default password, and click Log In. 3. Choose Configuration > Local Users, and view user management information in the right pane.

	4. You can manage BMC users, including adding users, deleting users, and changing passwords.
Expected result	1. Use the initial admin user to manage BMC users, including adding users, deleting users, and changing passwords.
Description	Acceptance options.

4 Hard Disk Controller Test

4.1 Hard Disk Controller Test

4.1.1 Configuring RAID1

Table 4- 1 Configuring RAID1 Arrays on LSI SAS 3008

Item	Content
Objective	To verify that you can configure RAID arrays on the LSI SAS 3008
Prerequisites	The server is powered on, and the hard disks are detected (Prior to software integration and customer authorized).
Procedure	1. Power on the server and press Ctrl+C at POST. The screen for configuring the LSI SAS 3008 controller card is displayed(This is in legacy mode; UEFI mode needs to be configured in the BIOS, see the product user manual for details). 2. Select LSI SAS 3008, and press Enter. 3. Select RAID Properties and press Enter. 4. Select Create RAID1 Volume and press Enter. Press → to select RAID Disk, and press the Space key to select two hard disks for configuring RAID1 properties. RAID Disk for the two hard disks is displayed as Yes. Press C to configure RAID1 properties. On the displayed screen, select Save changes then exit this menu and press Enter to save the settings.

Expected result	RAID1 arrays properties are configured successfully.
Description	None

4.1.2 Configuring RAID5

Table 4- 2 Configuring RAID5 Arrays on LSI SAS 3108

Item	**Content**
Objective	To verify that you can configure RAID5 arrays on the LSI SAS 3108
Prerequisites	The server is powered on, and the hard disks are detected.
Procedure	1. Power on the server and press Ctrl+R at POST. The screen for configuring the LSI SAS 3108 controller card is displayed(This is in legacy mode; UEFI mode needs to be configured in the BIOS, see the product user manual for details). 2. Select“SAS3108 BIOS Configuration Utility” 3. Press F2 and select Create Virtual Drive from the pop-up list. 4. Press Enter in the RAID Level area box, and select the RAID level as RAID 5 by using ↑ and ↓. 5. Press " ↓ " to move the cursor to the "Drives" area, press " ↑ " and " ↓ " to move the cursor, and press "Enter" to select the hard disk to be added to the RAID group. 6. Press " ↓ " to move the cursor to the "Basic Settings" area. Move the cursor to the "Size" area and set the RAID capacity as required.

	When not set, the system uses the maximum capacity supported by the current RAID as the default value of "Size". 7. Move the cursor to the "Name" area and set the RAID name. 8. Select Advanced and press Enter to open the advanced RAID attribute setting interface, and set advanced RAID attribute parameters as required. Press " ↑ " and " ↓ " to move the cursor and press "Enter" to select "Initialize". When this option is selected, the initialization operation is automatically performed when the RAID is created. 9. Click OK in the pop-up advanced dialog box. 10. On the returned Create New VD screen, select OK and press Enter. The initialization confirmation dialog box appears. 11. Click “OK” in the pop-up initialization confirmation dialog box to start the initialization. 12. In the returned CU main interface, press "→" to expand the folding information to view the detailed configuration. 13. Press "ESC". A confirmation dialog box is displayed. 14. Select "OK" and press "Enter". 15. Exit the CU configuration interface and prompt to restart the system. Restart the server.
Expected result	RAID5 arrays properties are configured successfully.
Description	None

5 Network Port PXE

5.1.1 Network Port PXE

Table 5- 1 Network Port PXE

Item	Content
Objective	To verify that LOM ports on the server support PXE.
Prerequisites	1. The server is powered on. 2. The Dynamic Host Configuration Protocol (DHCP) server is configured properly. 3. The installation server is configured properly 4. The DHCP server and installation server are connected to NIC1 on the server over the network.
Procedure	Power on the server and wait until it starts. Press F12 on the first BIOS screen.
Expected result	The server starts over PXE. An IP address is obtained for the server. The server starts to install an OS over the network.
Description	None

Note:

(1) Before acceptance, the system should be properly installed, and the software and hardware debugging should pass, and the system can run normally.

(2) The acceptance project should be confirmed by relevant personnel of both Inspur and the user.

(3) During the acceptance and preliminary inspection tests, the personnel of both parties shall perform strict tests against relevant standards. Some index parameters have been

tested when leaving the factory. When acceptance is limited, the conditions may be random or exempt.

📖 Statement:

During the actual acceptance test, the acceptance is subject to the contract requirements and the agreement between the two parties. This manual is for reference only.

---

6 Customer Acceptance Sign-off Sheet

Test Category	Test Item	Test Sub-item	Result
Hardware Test	Packaging	Packaging	□Pass □Fail □N/A
	Chassis	Chassis Structure	□Pass □Fail □N/A
	PSUs	PSUs	□Pass □Fail □N/A
		PSU Hot Swap Function	□Pass □Fail □N/A
		PSU Backup Function	□Pass □Fail □N/A
	Hardware Detection	Hardware Detection	□Pass □Fail □N/A
	Hard Disk Controllers	RAID Controller Card LSI SAS 3008	□Pass □Fail □N/A
		RAID Controller Card LSI SAS 3108	□Pass □Fail □N/A
	Alarm, Firmware Version, and Hardware Status Detection	Alarm Detection	□Pass □Fail □N/A
		Hardware Detection	□Pass □Fail □N/A

Remarks:

Inspur Representative： Customer Representative：

Date:______________________ Date:______________________

Test Category	Test Item	Test Sub-item	Result
CMC Test	Web Interface	Web Interface Login	□Pass □Fail □N/A
		Power-On and Power-Off on the	□Pass □Fail □N/A

Test Category	Test Item	Test Sub-item	Result
		WebUI	
		IP Address Configuration on the WebUI	□Pass □Fail □N/A
		Firmware Upgrade on the WebUI	□Pass □Fail □N/A
		System Logs on the WebUI	□Pass □Fail □N/A

Remarks:

Inspur Representative：

Customer Representative：

Date:______________________

Date:______________________

Test Category	Test Item	Test Sub-item	Result
BMC Test	Web Interface	Web Interface Login	□Pass □Fail □N/A
		Power-On and Power-Off on the WebUI	□Pass □Fail □N/A
		UID Indicator on the WebUI	□Pass □Fail □N/A
		Remote KVM on the WebUI	□Pass □Fail □N/A
		IP Address Configuration on the WebUI	□Pass □Fail □N/A
		Firmware Upgrade on the WebUI	□Pass □Fail □N/A
		System Logs on the WebUI	□Pass □Fail □N/A
		System Logs on the WebUI	□Pass □Fail □N/A
		User Management Function on the WebUI	□Pass □Fail □N/A
Remarks:			
Inspur Representative： Date:_______________________		Customer Representative： Date:_______________________	

Test Category	Test Item	Test Sub-item	Result
Hard Disk Controller Test	Configuring RAID1	Configuring RAID1 Arrays on LSI SAS 3008	□Pass □Fail □N/A
	Configuring RAID5	Configuring RAID5 Arrays on LSI SAS 3108	□Pass □Fail □N/A
Remarks:			
Inspur Representative： Date:______________________		Customer Representative： Date:______________________	

Test Category	Test Item	Test Sub-item	Result
Network Port Test	Network Port PXE	Network Port PXE	□Pass □Fail □N/A
Remarks:			
Inspur Representative： Date:______________________		Customer Representative： Date:______________________	

Final Sign-off

Conclusion: Totally 22 items are covered in this acceptance test, in which ______ passed, ______ failed, and ______ were not applicable.

Inspur Representative：

Customer Representative：

Date:______________________

Date:______________________