



Inspur® Server **Fault** **Diagnosis System** **Technology White Paper**

Inspur Server®
Fault Diagnosis System

ISFDS®



Dear users:

Copyright © Inspur 2022. All rights reserved.

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

Note: The products, services or features you purchase are subject to the commercial contracts and terms of Inspur Group. 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 does not make any express or implied statements or warranties on the contents of this document. Due to product version upgrades or other reasons, the contents of this document will be updated from time to time. Unless otherwise agreed, this document is only used as a guide, and all statements, information and suggestions in this document do not constitute any express or implied warranty.

Inspur and "Inspur" are registered trademarks of Inspur Group.

Windows is a registered trademark of Microsoft Corporation.

Intel and Xeon are registered trademarks of Intel Corporation.

Other trademarks belong to their respective registered companies.

Technical service phone number: 4008600011

Address: Inspur Electronic Information Industry Co., Ltd., No. 1036, Inspur Road, Jinan, China

Zip code: 250101

Table of contents

1	Introduction	03
2	Overview	04
2.1	IS-FDS Introduction	04
2.2	Terminology	05
3	IS-FDS overall architecture	06
3.1	Server Failure Classification	06
3.2	Server Fault Handling Unit	08
3.3	Server Failure Handling Process	09
3.4	Supported Products	10
4	IS-FDS Key Technologies	10
4.1	Real-time fault detection and isolation	10
4.2	Accurate fault location and reporting	10
4.3	Intelligent Fault Warning and Repair	11
4.4	Internal and external fault monitoring system customized for Inspur servers	11
5	IS-FDS Function Overview	12
5.1	CPU Fault Detection and Handling	12
5.2	Memory Fault Detection and Handling	12
5.3	PCIe common component fault detection and processing	13
5.3.1	Hard disk	13
5.3.2	GPU	13
5.3.3	Memory Card	13
5.3.4	Network Card	14
5.4	Mainboard Fault Detection and Treatment	14
5.4.1	Server Fault Indicator	14
5.4.2	Mainboard VR fault detection preprocessing	16
5.4.3	Abnormal power failure handling	16

5.4.4	Power-on timeout problem handling	16
5.4.5	Mainboard anti-burn board function design	16
6	ISBMC Fault Monitoring and Diagnosis	17
6.1	System operation log records	17
6.1.1	Power-on self-check code monitoring and logging	17
6.1.2	Screenshots	18
6.1.3	Maintenance Log Introduction	18
6.2	System downtime log record	19
6.2.1	Screenshots and Video Recordings of Downtime	19
6.2.2	Log collection and download interface	20
6.2.3	Downtime Diagnosis Case	21
6.2.4	Non-downtime monitoring case	22
6.3	System Event Log Recording	22
6.3.1	System event log	22
6.3.2	Fault reporting	24
6.3.3	Log Settings	26
6.3.4	IDL log and handling suggestions	27
6.4	Whole system health status monitoring	29
6.4.1	System Overview	29
6.4.2	Sensor Summary List	30
6.4.3	Audit log records	32
6.4.4	Asset Information	34

1 Introduction

With the advancement of digitalization waves such as "new infrastructure", "Eastern Data and Western Computing", and "Metaverse", the digital transformation of the whole society has accelerated, and digital construction has developed rapidly. Today, digitalization has risen to a strategic level at both the national and corporate levels. General-purpose, storage, hyper-convergent, and AI servers, as infrastructure hardware supporting digital computing services, are being deployed in large quantities in cloud computing, big data, the Internet of Things, AI, and other fields, and the number of businesses they carry is increasing. Computing pressure, storage capacity, and network bandwidth are being severely tested.

In addition, the server itself is a complex software and hardware collection of computing, storage, network and other new technology applications, consisting of processors, memory, storage devices (RAID cards, etc.) The system is composed of components such as data center, HDD/SSD, AI acceleration card (GPU card/ASIC acceleration card/FPGA acceleration card), network card (Ethernet card/Infiniband network card/intelligent network card), motherboard, power supply equipment, cooling equipment, BIOS firmware, BMC management software, etc., and the complexity of its hardware and software is constantly increasing; therefore, it is inevitable that there will be unexpected failures that cause downtime and affect the normal operation of digital services. In particular, the customer losses and impact caused by the downtime of key services are difficult to estimate.

Currently, massive server data centers are facing huge challenges of high operation and maintenance costs and the complexity of maintenance management. Therefore, improving the server maintenance experience can ensure the continuous and stable operation of the server, grasp the health status of the server in real time, and promptly repair and restore business operations even in the event of a failure. This has gradually become a basic guarantee function that servers need to have.

2 Overview

Inspur Server Fault Diagnosis System ISFDS (Inspur Server Fault Diagnosis System) is a server fault diagnosis system developed by Inspur with independent intellectual property rights. It deeply customizes and integrates the software and hardware designs of various server components, and independently develops Inspur's own server fault diagnosis expert rule base. It can monitor and warn the working health status of the server throughout its life cycle in real time, and can achieve fast and accurate diagnosis, repair and recovery of business operations in minutes when a downtime occurs. While enhancing the core competitiveness of the product, it has made substantial leapfrog contributions to promoting the realization of free operation and maintenance for small and medium-sized customers, and the realization of intelligent operation and maintenance of large customers' data centers.

2.1 IS-FDS Introduction

Current server operation and maintenance pain points:

- After a device fails and goes down, the key component register log information for locating the fault is not fully collected, and the historical fault record information is not complete, making it impossible to automatically and accurately locate the faulty component;
- The efficiency of fault diagnosis and positioning is low. When a problem occurs on the server, the results are mainly judged based on manual analysis and experience, and the degree of automation and intelligence is not high.
- It takes a long time to restore equipment after a failure. Onsite failures are difficult to reproduce and require multiple manual replacement of parts for verification. The troubleshooting efficiency is low and has a significant impact on customer business.

ISFDS technical solutions to solve the problem:

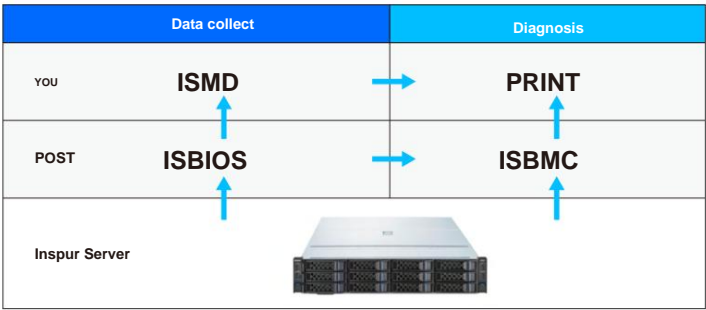


Figure 2-1

- When the server is in continuous operation for a long time, real-time monitoring and reporting of the health status is required. ISBMC can report whether there are abnormal voltage signal fluctuations, too many CPU repairable errors, excessive local heat accumulation, large amounts of memory ECC, etc. before a failure occurs. Users can perceive the existence of these anomalies in advance and pay attention to the planned downtime maintenance of servers with warnings to avoid fatal or catastrophic failures.
- Establish an out-of-band fault handling system centered on ISBMC, optimize the logic of capturing fault information and resource usage of each server component, ensure that all fault data can be collected in real time and completely, and then combined with the complete resource topology of the server, it can easily handle the analysis, diagnosis and positioning of various fatal faults and catastrophic downtimes, improve the clarity of server fault diagnosis and processing time, achieve minute-level diagnosis and positioning, and quickly replace faulty components to restore business operations.
- Established the Inspur ISFDS fault diagnosis expert rule base, conducted in-depth analysis and study of Inspur's massive customer downtime logs, and continuously improved the expert diagnosis rules. The implementation of the Inspur fault diagnosis expert rule base in ISBMC achieved an IERR downtime diagnosis accuracy rate of 95%.

- Develop Inspur's physical infrastructure management platform ISPI to realize summary diagnosis of ISBMC out-of-band logs and ISMD in-band logs, achieve complete restoration of fault site log scenarios, maximize fault monitoring coverage, and maximize fault diagnosis accuracy; the platform's out-of-band hardware logs are collected through the ISBMC REST interface, and in-band system logs are collected through the ISMD REST interface; out-of-band hardware logs can also be collected only through ISBMC; ISPI and ISBMC both have the ability to push pre-alarm events after diagnosis directly to the customer's operation and maintenance system, and support customization of reporting interfaces.
- Developed the Inspur server in-band management driver ISMD, which acts as an agent for in-band system collection, supports performance indicator subscription, realizes in-band system performance, configuration and log collection, supports active/passive reporting to ISPI for analysis, and realizes the in-band and out-of-band management capabilities of Inspur servers. For ISPI to collect in-band logs through ISMD, it is necessary to install ISMD under the OS of the managed device system. After ISPI discovers ISMD, it can collect in-band system logs.

2.2 Terminology

Table 2-1 explains the professional terms and abbreviations that appear in this article.

the term	explain	Explanation of terms	
ISFDS®	Inspur Server Fault Diagnosis System	PFR	Platform Firmware Resilience
ISBIOS®	Inspur Server BIOSBasic Input/Output System	PMBus	Power Management Bus
ISBMC®	Inspur Server BMC(Baseboard Management Controller)	SMBus	System Management Bus
ISMD™	Inspur Server Management Driver	HOURS	Serial Advanced Technology Attachment
ISPI™	Inspur Server Physical Infrastructure Manager	SMTP	Simple Mail Transfer Protocol
MCA	Machine Check Architecture	SNMP	Simple Network Management Protocol
THIS	Correctable Error	S.M.A.R.T.	Self-Monitoring Analysis and Reporting Technology
UCE	Uncorrectable Error	NVME-MI	NVM Express® Management Interface
UCR	Uncorrected Recoverable	NC-SI	Network Controller Sideband Interface
SRAR	Software Recoverable Action Request	SMBPBI	SMBus Post-Box Interface
SHIT	Software Recoverable Action Optional	IEH	Integrated Error Handler
UCNA	Uncorrected No Action required	SCI	System Control Interrupt
MCERR	Machine Check Error	SMI	System Management Interrupts
IERR	Internal Error	NMI Non	Maskable Interrupt
BAKE	Platform Environment Control Interface	MSI	Message Signal Interrupt
POST Power On Self Test		CMCI	Corrected machine-check error interrupt
MCE	Machine Check Exception	CSMI	CMCI morphed into SMI
AIR	Advanced Error Report	MSMI	MCE morphed into SMI
ASD	At-Scale Debug	ACPI	Advanced Configuration and Power Interface
ACD	Autonomous Crash Dump	DSM	Device-Specific Method
BAFI BMC Assisted FRU Isolation		WATER	ACPI Platform Error Interfaces
RAS	ReliabilityAvailabilityServiceability	Geshem	Generic Hardware Error Source
HBA	Host Bus Adapter	WHY	Windows Hardware Error Architecture
HCA	Host Channel Adapter	BERT Boot	Error Record Table
IB	InfiniBand	HEST Hardware	Error Source Table
IPMI	Intelligent Platform Management Interface	ERST Error	Record Serialization Table
JTAG	Joint Test Action Group	EINJ	Error Injection Table
NOTHING	Network Interface Controller		

Table 2-1 Glossary

3 IS-FDS Overall Architecture

ISFDS is developed based on Inspur's self-developed server hardware, and its main functions are jointly realized by ISBIOS, ISBMC, and motherboard hardware design. It realizes the instant reporting of abnormal components throughout the life cycle of the server, intelligent reporting of components with hidden dangers, and immediate and accurate reporting of faulty components after a downtime. It also performs real-time repairs on non-fatal faults, performs real-time evaluation of the running status of server hardware firmware, and monitors the health status of the equipment in all aspects.

3.1 Server Failure Classification

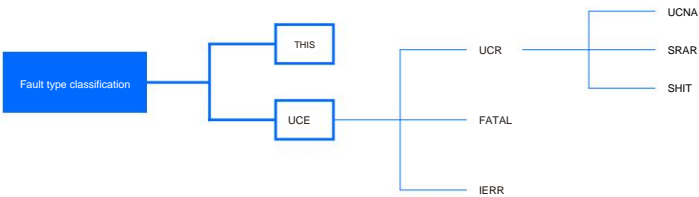


Figure 3-1 Fault type classification

From the above figure, we can see that server failure types can be divided into CE failures and UCE failures. UCE failures include IERR catastrophic failures, FATAL fatal failures, There are three types of UCR uncorrectable and recoverable faults. FATAL and UCR belong to the same MCERR type faults and will trigger an MCE interrupt to the OS. UCR faults are usually called non-Fatal type UCE, including UCNA, SRAR, and SRAO. In addition, based on the fault scenario, server faults can be divided into two categories: downtime faults and non-downtime faults. Downtime faults are mainly reflected in downtime during the boot process and downtime during operation, as shown in Figure 3-2. Non-downtime faults include statistical monitoring of repairable faults and non-fatal faults of CPU/memory/GPU/storage devices/ network devices/PCIe external devices, and monitoring of component and link health status. In addition, monitoring of basic hardware is a key indicator for measuring the health status of the server, including abnormal monitoring of power supply temperature indicators and abnormal monitoring of motherboard fans, as shown in Figure 3-3.

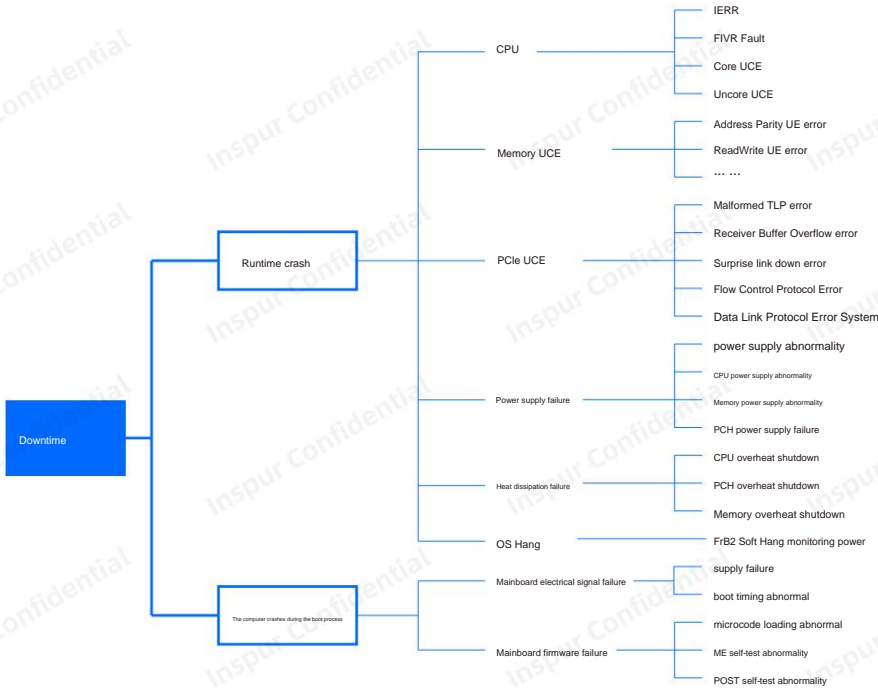


Figure 3-2 Classification of downtime faults

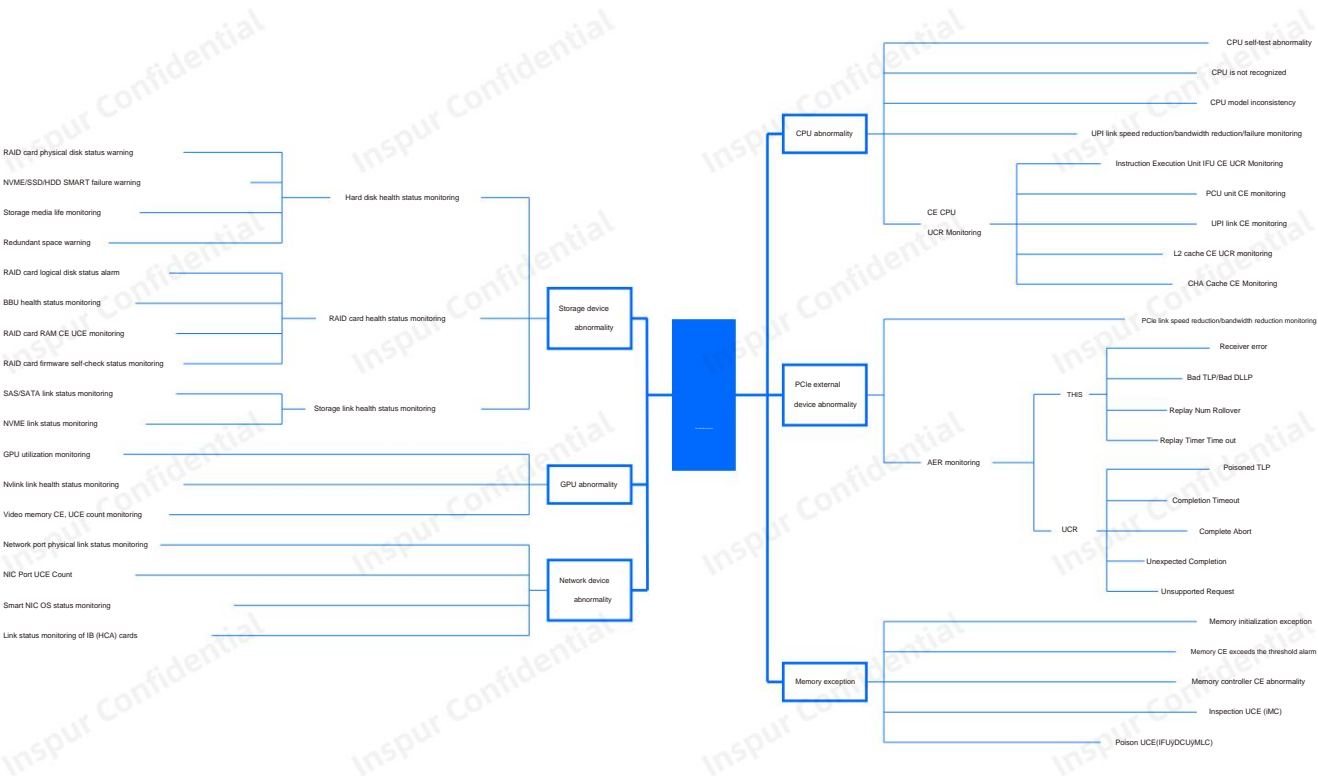


Figure 3-3 Classification of non-downtime faults

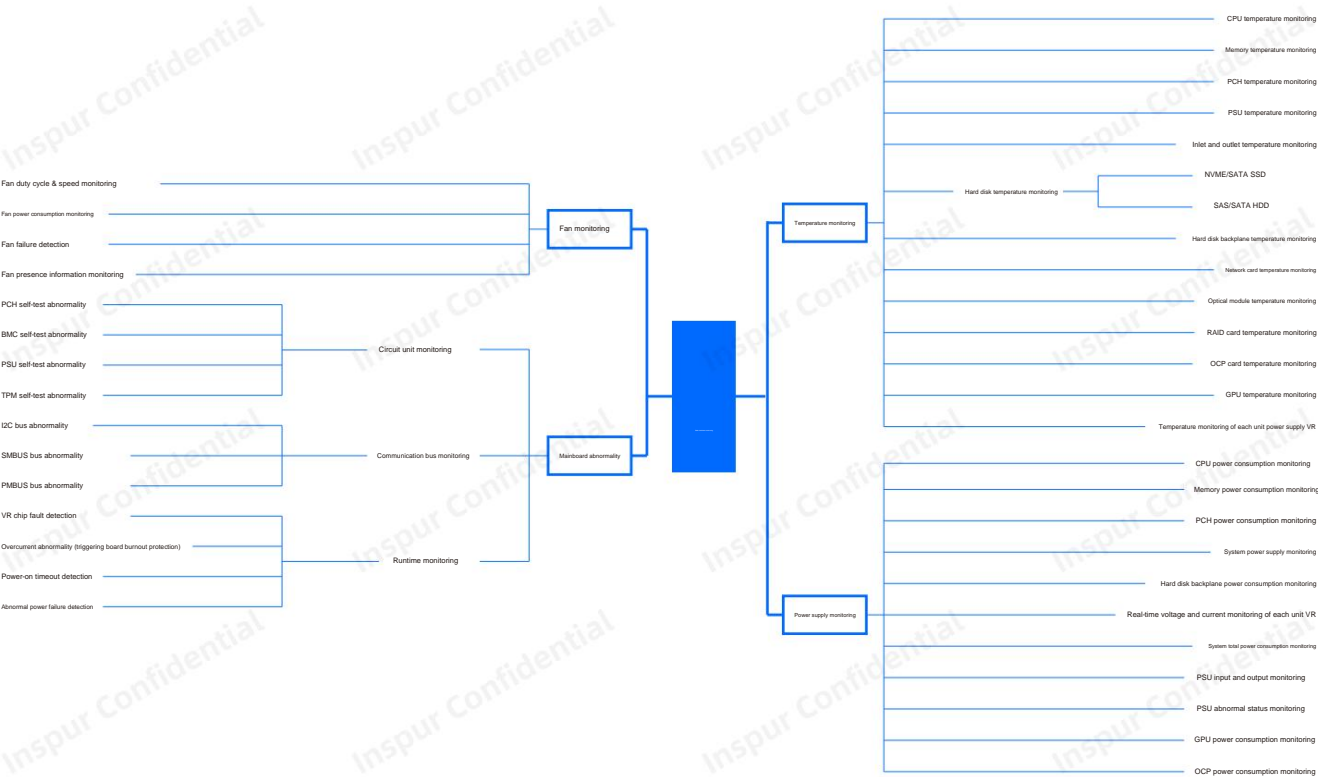


Figure 3-4 Basic hardware monitoring

When you boot up a server, various errors can occur in the server hardware and underlying firmware:

During OS operation, random CE errors can be repaired at the hardware bottom layer. The fault area can be replaced by redundant resources, the operation rate can be reduced, and the request can be retransmitted to repair the fault and maintain the normal operation of the system. Unexpected CE storms will have a lasting impact on device performance. The components that cause CE storms need to be interrupted and suppressed, and planned downtime replacement and repair should be performed. In the case of low-probability UCE failures, fatal UCE will cause kernel panic and server downtime and restart. Non-fatal UCR can continue to run when the system is repaired, such as memory UCE repair during POST process, CPU Core fault isolation, UPI/PCIe bus link problem bandwidth reduction, memory Poison UCE Recovery repair during OS operation, etc. Catastrophic IERR failures will directly cause server downtime, and the ISFDS diagnostic mechanism is relied on to find the components that cause the fault and replace and maintain them. In addition, if there is a problem at the firmware layer during the server startup phase, the PFR (Platform Firmware Resilience) mechanism will detect the relevant anomalies and use Recover actions or dual mirroring to perform immediate repair of the startup failure.

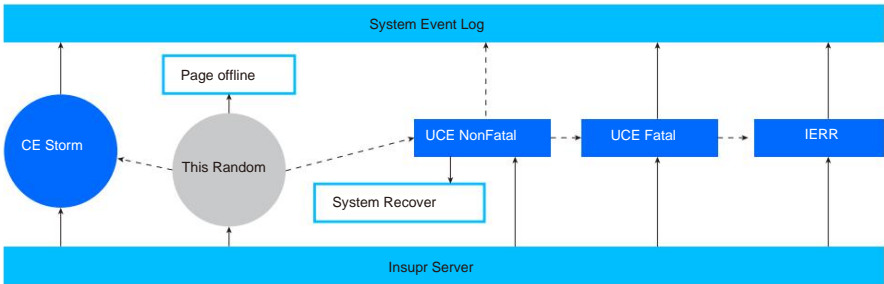


Figure 3-5

3.2 Server Fault Handling Unit

The fault handling unit of Inspur servers is built with ISBMC as the main center and extends to various external units, from basic power supply monitoring, temperature monitoring, and heat dissipation monitoring to key business-carrying components CPU monitoring, memory monitoring, storage device monitoring, PCIe device monitoring, and motherboard monitoring, to achieve all-round and no-dead-angle real-time collection, analysis, and diagnosis of out-of-band fault data, and push the diagnosis results to the System Event Log, and present them on the server front panel fault indicator and BMC Web interface. In addition, a fault diagnosis auxiliary system is built with the CPU as the secondary center. During the boot process, the CPU runs ISBIOS to collect the fault information and resource topology information of the CPU, memory, PCIe and other devices in the band, and pass it to ISBMC for auxiliary diagnosis; at the same time, during the OS running stage, ISBMC monitors the CPU CATERR/ErrorPin signal in real time, and uses the PECCI/JTAG interface to obtain the fault register information recorded by the CPU in time when IERR/UCE/UCR/CE occurs. ISBIOS can collect sudden abnormal fault information and report it to ISBMC or the operating system through CMCI, CSMI, MCE, MSMI, SMI, SCI, NMI, etc.

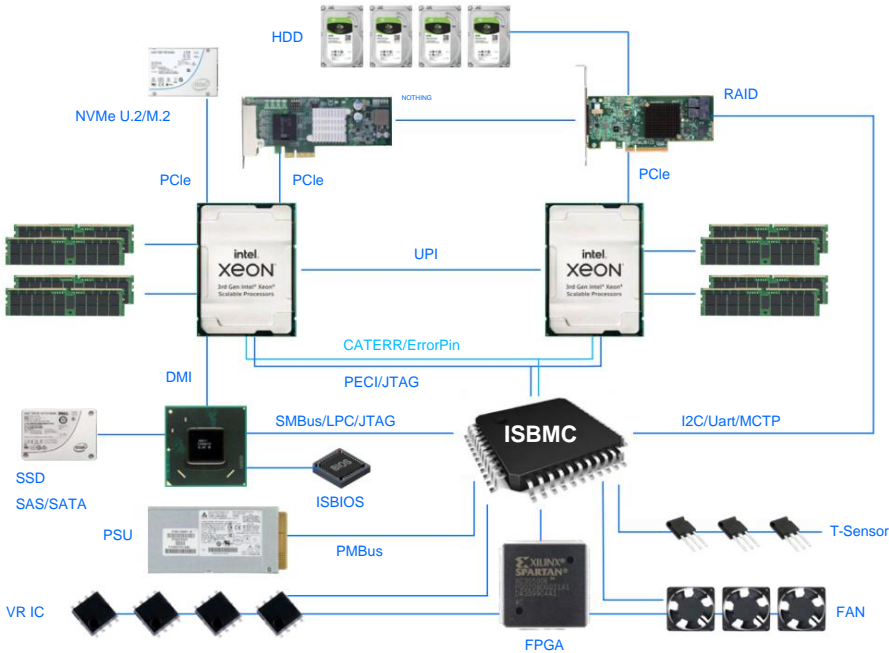


Figure 3-6

The figure above lists the hardware connection topology diagram, among which the key fault handling components are:

ISBMC: The core processing unit for fault detection, location, and reporting, providing the computing power algorithm implementation of the ISFDS technology hardware layer.

ISBIOS: The underlying code implementation of fault isolation, early warning, and repair, providing firmware support for the implementation of ISFDS platform functions.

CPU: Intel Xeon CPU provides enhanced RAS function, enhances the hardware RAS characteristics of CPU internal submodules, memory, PCIe devices, and provides a sound

The underlying hardware supports fault detection and repair.

Motherboard: Inspur self-developed motherboard has the ability to detect and pre-process faults. It will immediately report any faults in the power supply VR, and has an instant hardware abnormality fault protection mechanism.

In the event of a fault, the board burnout protection function will be triggered to prevent the expansion of local faults. In addition, hardware fault detection functions such as power-on timeout and abnormal power failure are also designed.

3.3 Server Failure Handling Process

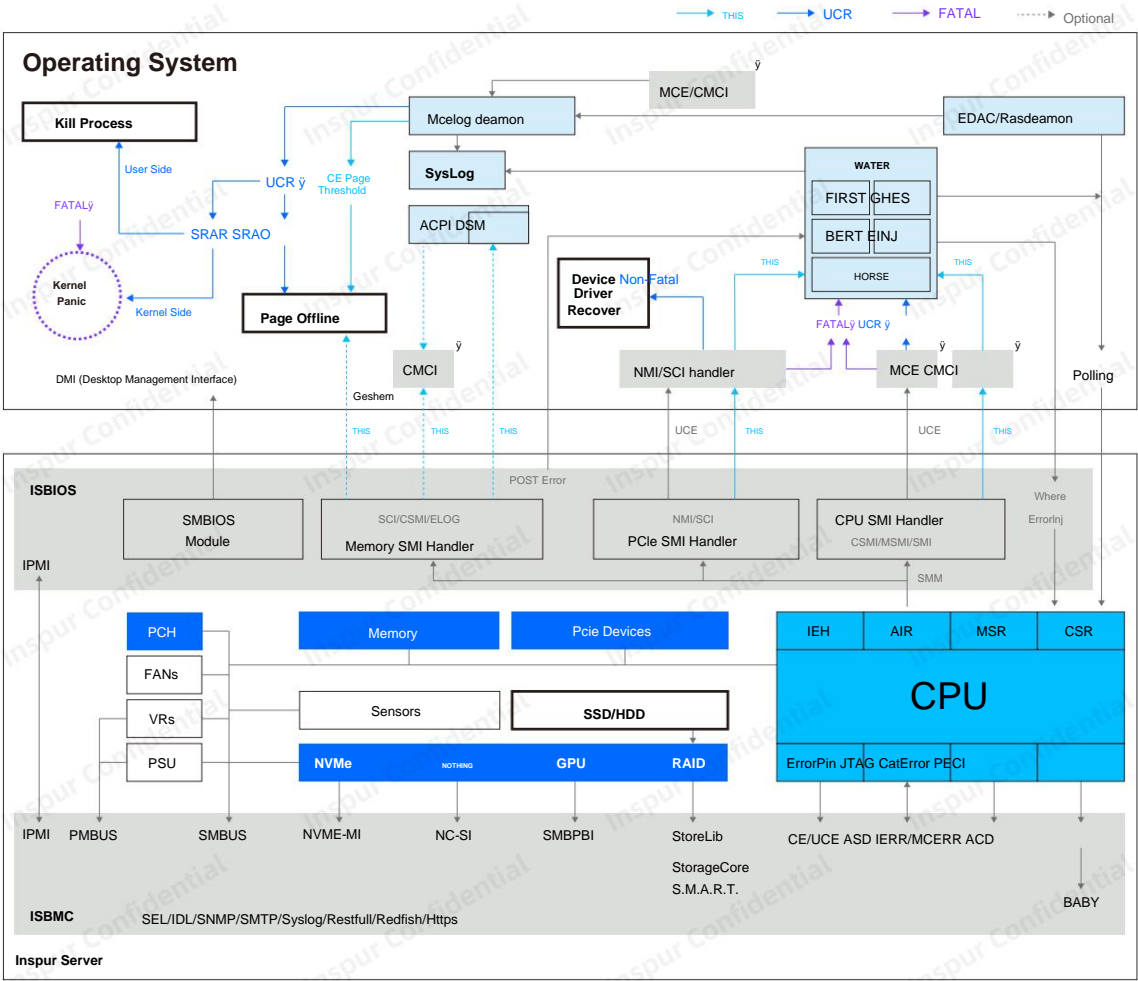


Figure 3-7 Server fault handling process

As shown in Figure 3-7, the server hardware fault ISBMC can actively capture each PCIe component through various interface protocols and use the CPU ErrorPin and CatError monitor the fault type, use the CPU's PECCI interface to collect ACD on the CPU registers and then perform BAFI analysis, use the JTAG interface of the CPU is used for online ASD debugging; at the same time, ISBMC supports various types of SEL/IDL/SNMP/SMTP/Syslog/Restfull/Redfish/Https, etc. The interface pushes the received warnings and faults to the upper level.

ISBIOS can trigger SMI interrupts of various faults through the CPU, which are processed by the corresponding SMI Handler and reported to the corresponding OS Driver for fault processing.

IPMI is used to report to ISBMC; memory CE and SRAO faults are repaired using the Pageoffline mechanism, and memory SRAR type faults occur on the user side

Process termination repair can be performed during the process. If it occurs on the kernel side, it will trigger kernel panic, FATAL type errors generated by CPU, Memory, and PCIe.

Failures will also trigger Kernel Panic; ISBIOS will record CE and various UCE failures to the HEST Table of APEI for OS retrieval and processing.

Syslog, in addition, OS also has RAS processing applications such as EDAC and Rasdeamon, which can actively capture CPU and component failures.

Glossary 2-1.

3.4 Supported Products

Function	model
ISFDS V2.0	NF5280M5/NF5180M5/NF8260M5/NF8480M5y
ISFDS V3.0	NF5280M6/NF5180M6/NF5260M6/NF5270M6/NF5266M6/NF5466M6/NF5468M6/NF5488M6/ NF5688M6/i24M6/i48M6/SN5160FM6/SN5264FM6/NF8260M6/NF8480M6y

*For specific models, please refer to the official product description for actual functions.

4 IS-FDS Key Technologies

ISFDS integrates the fault handling technologies of hardware, ISBIOS, ISBMC and operating system to form a complete fault handling system, covering fault detection, fault

The six key technologies are fault warning, fault repair, fault isolation, fault location, and fault reporting. Real-time detection and intelligent control of each component of the server are achieved.

Early warning, continuous monitoring of machine performance and health status, full-time repair and isolation of system failures, rapid diagnosis and precise location of downtime failures; and ISMD,

ISPIIM realizes the ability to integrate internal and external monitoring, and further promotes intelligent operation and maintenance in data centers.

4.1 Real-time fault detection and isolation

During the server startup ISBIOS POST process, the BIST (Build in self test) component will first perform a self-test of each submodule inside the CPU, and then

Initialization and fault detection of memory and PCIe peripherals. If a Core or Dimm fault is detected, it will be isolated and continue to boot, avoiding single non-essential component failure

Affects the operation of the entire system; during the OS running phase, the memory will be inspected in real time, and ISBIOS will actively inform the OS of abnormal memory pages for

Offline isolation; the power supply design realizes active isolation of the main PSU fault and enables the backup PSU, and the motherboard design monitors local overcurrent anomalies and isolates the fault area in time

domain, to prevent the expansion of hardware damage; in addition, ISBMC is responsible for the full-time inspection and monitoring of all hardware and firmware failures of the entire machine, and real-time control of the power supply,

Temperature conditions and various abnormal fault output states, to conduct an overall assessment of the health status of server hardware.

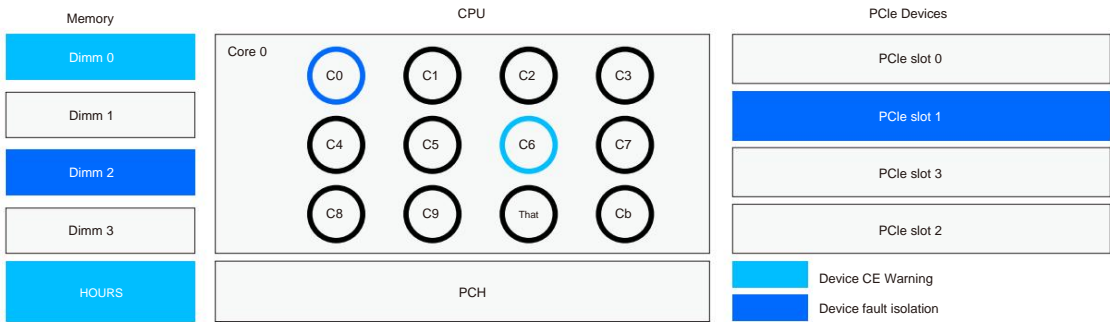


Figure 4-1

4.2 Accurate fault location and reporting

The ISBMC and ISBIOS directly handle the catastrophic fault IERR process, and detect the CPU failure immediately after the catastrophic fault IERR occurs.

At this moment, the optimized and enhanced PECI interactive driver is used to timely capture the key registers of the fault record; ISBMC and ISBIOS are in the HOST system resource topology structure

The code of the process of fault log collection, log analysis, and log reporting channels (SDR, SMTP, SNMP-trap, etc.) has been completely refactored.

and process visualization; IERR diagnosis uses Inspur ISFDS fault diagnosis expert rule base to perform online analysis of fault logs and accurate positioning of faulty components.

And after the ISBMC diagnosis fails, the ISBIOS self-diagnosis mechanism is enabled to improve the accuracy of IERR fault diagnosis.

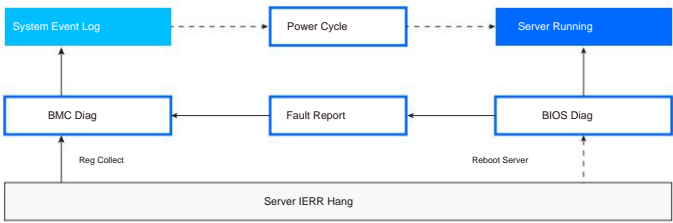


Figure 4-2

4.3 Intelligent Fault Warning and Repair

The fault warning function of ISFDS uses the non-downtime fault logs of a large number of Inspur server customers to conduct data mining and analysis based on the Inspur Yunhai Insight big data platform. It learns data behavior patterns to generate warning rules, which are implemented in the Inspur fault diagnosis expert rule base, and then ISBMC and ISPIM apply the rules to track and monitor the operating status of all components in the server throughout the life cycle, identify the behavior patterns of real-time data, identify potential hidden danger components and high-risk components, and issue early warnings to reduce sudden failures of servers under high-load operation.

ISFDS has the basic repair capability for some occasional non-fatal UCE faults, achieving instant recovery of faults and reducing the occurrence of fatal UCEs leading to downtime. For example, CPU DCU inspection Parity fault repair, memory Poison UCE recovery, memory read and write CE and inspection CE/UCE real-time repair, memory read and write CE softPPR, memory SMBus fault self-repair, PCIe UCR fault recovery, etc.



Figure 4-3

4.4 Internal and external fault monitoring system customized for Inspur servers

Inspur server in-band management driver ISMD is programmed in C language. It reads system files, system functions, system tools and other means to conduct comprehensive monitoring in terms of monitoring, performance, and logs. Performance monitoring supports second-level monitoring, logs support incremental collection, and system dependency is minimized. The installation package is 10M, single-core CPU utilization is <10%, and memory usage is <100M.

Inspur's physical infrastructure management platform ISPIM has established 492 fault models based on the experience of more than 30,000 experts, enabling rapid root cause diagnosis and output of solutions. The platform collects ISBMC out-of-band logs and ISMD in-band logs, aggregates them, and then performs diagnosis, achieving complete restoration of fault site log scenarios, completing all-round collection, analysis, and processing of fault data, maximizing fault monitoring coverage, and maximizing fault diagnosis accuracy;

Active inspection, including 492 fault models and 30,000+ expert experience, quickly diagnoses the root cause of the fault and automatically provides solutions

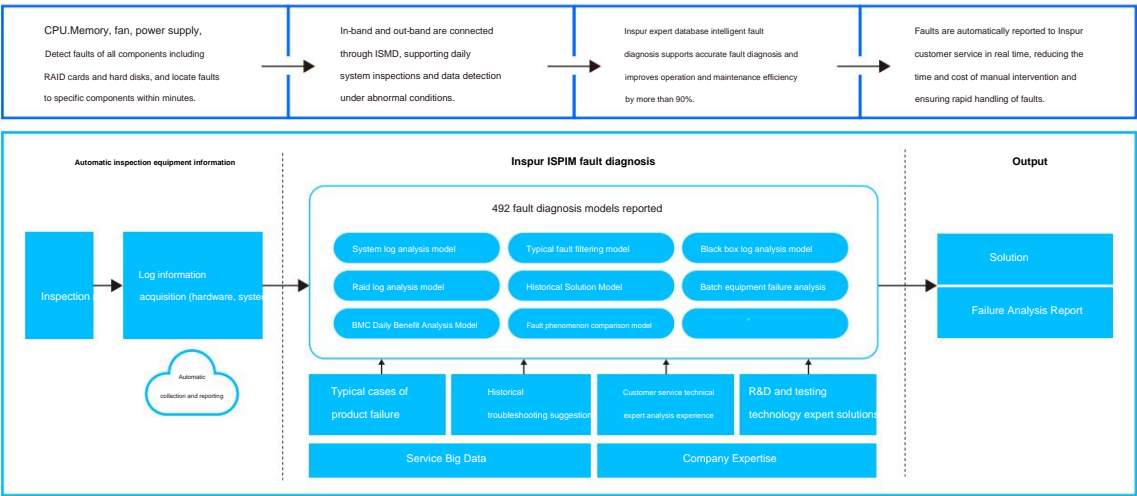


Figure 4-4

5. Introduction to IS-FDS

ISFDS functions rely on the RAS design of the Inspur server system, functional components and motherboard hardware.

The design level realizes strong reliability, availability, and maintainability; the specific functional design implementation involves CPU fault detection and processing, memory fault detection and processing

It consists of four main parts: fault detection and processing, PCIe common component fault detection and processing, and mainboard fault detection and processing.

5.1 CPU Fault Detection and Handling

Taking Intel as an example, the CPU consists of two parts: Core and Uncore. The Core consists of the instruction prefetch unit (IFU), the data cache unit (DCU), and the data transfer cache.

The Uncore consists of four parts: the DTLB unit, the L2 cache unit (MLC); the Uncore consists of CHA, M2M, iMC, Intel®UPI, FIVR, PCU, UBOX, M2IOSF, IIO and other units; when a unit fails during CPU operation, it will be recorded in detail in the MCA Bank to which each unit belongs.

The fault data of the fault site is recorded and stored in the power-off volatile CSR registers (Control and Status Registers) associated with each unit.

The Core section will record the CPU or memory failures, and the Uncore section will record the CPU peripheral component failures corresponding to each unit, such as memory, main Boards, PCIe components, etc.

ISBMC has enhanced the capture of key registers of CPU record faults, and deeply correlated and analyzed CSR and MCA Bank record data to accurately lock

The real source of the fault can be quickly and accurately located at the scene of the fault to the component that caused the fault.

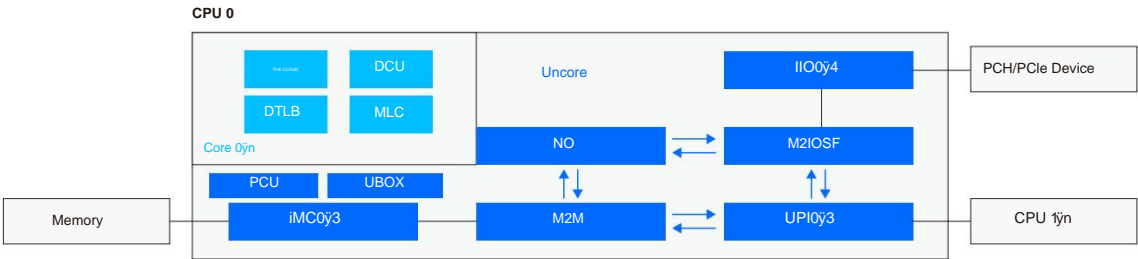


Figure 5-1 CPU register topology

5.2 Memory Fault Detection and Handling

As the number of memory channels supported by servers, the capacity of single memory, and the operating frequency of memory continue to increase, the probability of memory errors also increases.

To avoid frequent downtime caused by memory failures, Inspur server ISBIOS firmware RAS design enables a large number of memory failure protection mechanisms, SDDC, PostPPR, PCLS, memory enhanced stress testing and repair (AdvancedMemoryTest), memory Poison UCE Recovery, read and write CE and inspection

Real-time repair of CE/UCE, isolation of faulty DIMM by memory UCE, etc.; however, some problems may occur when the server is running for a long time or under heavy load.

Unexpected memory failures. Common memory failures are listed below:

common of Memory Fault	M2M Time-out error
	Last level memory controller error
	Near-Memory Cache controller error
	UnCorrectable Address Parity Error
	Memory Address/Command Error
	Memory Read/Write Corrected Error
	Memory Read/Write UnCorrectable Error
	Correctable/UnCorrectable Patrol Scrub Error

Table 5-1 Common memory failure list

ISFDS can accurately identify whether the source of memory failure is a memory control module failure in the CPU or an actual memory stick DIMM failure, and supports fault address resolution in various memory working modes, accurately locates the faulty DIMM position, and supports online address resolution. In addition, special optimization support is provided for fault location of Intel Optane persistent memory PMEM, and the diagnostic rules cover difficult downtime cases caused by various types of memory.

5.3 PCIe common component fault detection and processing

PCIe general component failures are generally recorded and reported by the AER mechanism. AER failures are classified into the following categories: Corrected, Non-Fatal, and Fatal:

THIS	Receiver error / Bad TLP / Bad DLLP / Replay Num Rollover / Replay Timer Time out
UCR	Poisoned TLP / Completion Timeout / Completer Abort /Unexpected Completion / Unsupported Request
UCE	Malformed TLP error / Receiver Buffer Overflow error / Surprise link down error / Flow Control Protocol Error / Data Link Protocol Error

Table 5-2 PCIe AER fault list

CE-type faults are generally repaired by the link layer; UCR-type faults are reported to the OS for recovery processing; fatal UCE-type faults will cause system downtime, some of which are directly reported and located by the AER mechanism, and other PCIe faults that cause catastrophic downtime will be diagnosed and analyzed by the ISFDS fault processing mechanism, which integrates the detailed AER information recorded by the IIO module with the CPU CSR and MCA Bank data, uses Inspur fault diagnosis expert rules, and combines the constructed PCIe resource topology to accurately locate the external component on the failed PCIe slot.

5.3.1 harddisk

Inspur ISFDS technology can realize functions such as hard disk red light alarm, Broadcom RAID card Media error record, and SSD erase and write life monitoring.

For NVME disks, you can obtain information such as the in-place status, slot number, manufacturer model, capacity, manufacturer serial number, bandwidth rate, etc. It supports alarm functions such as remaining space below threshold alarm, overtemperature alarm, Read Only mode alarm, volatile memory backup system failure alarm, and Thermal Sensor read failure.

5.3.2 GPU

Inspur ISFDS technology can realize functions such as GPU card over-temperature alarm, ECC fault alarm, PCIe CE/UCE error reporting, etc. By reading the register information of the GPU card itself, the temperature alarm threshold can be obtained. When the system detects that the chip temperature on the board exceeds the threshold, it will automatically trigger an alarm. When ECC errors occur in SRAM or DRAM, the system will count the number. When it exceeds the allowed range, the information will be displayed to prompt the user to replace it in time. When the number of PCIe CE exceeds the threshold or UCE occurs, the system can print the location of the wrong bus, which is convenient for operation and maintenance personnel to quickly locate and handle.

5.3.3 Memory Card

Inspur ISFDS technology can realize functions such as storage card fault alarm, disk drop alarm, over-temperature alarm, etc., and can also support obtaining hard disk prediction fault information, SSD life monitoring and other functions.

5.3.4 Network Card

With the improvement of server performance, the data transmission capability requirements are getting higher and higher. As the channel for data transmission, the monitoring of the network card status is particularly important. Inspur ISFDS technology can monitor the static and dynamic information of the network card and can monitor the status of the network card in real time.

Static information monitoring can intuitively monitor the NCSI version, FW name version, MAC address and other static information supported by the network card on the BMC interface, which is convenient for the operation and maintenance management of the network card.

Dynamic information can be monitored. The link status of each network port of the network card, the temperature of the network card chip, the temperature of the optical module matched with the network port, and the alarm of the optical module current exceeding the threshold value can be intuitively monitored on the BMC interface. Corresponding problem troubleshooting can be carried out according to the alarm information that appears.

Dynamic information can be monitored. The link status of each network port of the network card, the temperature of the network card chip, the temperature of the optical module matched with the network port, and the alarm of the optical module current exceeding the threshold value can be intuitively monitored on the BMC interface. Corresponding problem troubleshooting can be carried out according to the alarm information that appears.

If a smart network card is inserted, in addition to monitoring static and dynamic information on the BMC interface, it can also provide SoC and FPGA status information and collect related logs. It can also perform operations such as powering off and powering on the SoC system.

5.4 Mainboard Fault Detection and Treatment

5.4.1 Server fault indicator

The server front panel is equipped with a machine fault prompt indicator. Taking NF5280M6 as an example, the detailed definition is as follows:

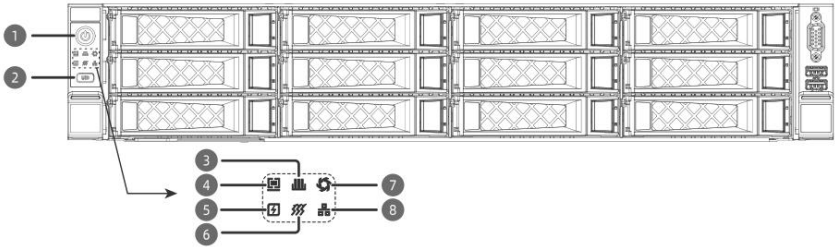


Figure 5-2 NF5280M6 front panel indicator diagram

Serial number	name	Serial number	name
1	Power switch button/indicator light	2	UID/BMC RST button/indicator
3	Memory fault indicator	4	System fault indicator
5	Power Failure Indicator	6	System overheat indicator
7	Fan fault indicator	8	Network status indicator

Table 5-3 Front panel indicator light numbers and names









Symbol indicators and buttons	Status Description
	<p>Power switch button/indicator light</p> <p>Power indicator light description: - Off: The device is not powered on. - Steady green: The device is powered on normally. - Steady orange: The device is in standby mode.</p> <p>Power button description: - Press and hold the power button for 4 seconds to force shutdown.</p> <p>Note: - Different OS may require you to shut down the OS according to the OS interface prompts. - In the Standby mode, short press the power button to power on.</p>
	<p>UID BMC RST button/indicator</p> <p>The UID indicator is used to locate the device to be operated: - Off: The device has not been located. - Steady blue: The device has been located. - Flashing blue: The device is being remotely operated.</p> <p>Note: - You can turn the light off or on by pressing the UID button manually or by remote control of the ISBMC. - Press the UID button for more than 6 seconds to reset the BMC.</p>
	<p>Memory fault indicator</p> <p>- Off: The device is in normal state. - Flashing red (1Hz): The system has a general alarm. - Steady red: The system has a serious alarm.</p>
	<p>System fault indicator</p> <p>- Off: The device is in normal state. - Flashing red (1Hz): The system has a general alarm. - Steady red: The system has a serious alarm.</p>
	<p>Power Failure Indicator</p> <p>- Off: The device is in normal state. - Flashing red (1Hz): The system has a general alarm. - Steady red: The system has a serious alarm.</p>
	<p>System overheat indicator</p> <p>- Off: The device is in normal state. - Flashing red (1Hz): The system has a general alarm. - Steady red: The system has a serious alarm.</p>
	<p>Fan fault indicator</p> <p>- Off: The device is in normal state. - Flashing red (1Hz): The system has a general alarm. - Steady red: The system has a serious alarm.</p>
	<p>Network status indicator</p> <p>- Off: No network connection or in abnormal state. - Flashing green: Data is being transmitted.</p> <p>Note: - Only indicates the working status of the onboard network.</p>

Table 5-4 Front panel indicator light description comparison table

5.4.2

Motherboard VR fault detection preprocessing

The fault detection and preprocessing of the motherboard VR involves the monitoring of the power supply status of the CPU, memory, and PCH chip. At the same time, it can realize real-time monitoring of the power supply status of components such as fans, hard disks, GPUs, and OCP plug-in cards (specifically, the BMC accesses the corresponding VR, EFUSE, and CPLD units through the I2C bus, reads the fault bit of the working status register inside the VR or EFUSE or the fault status of the GPIO of the CPLD, and judges the fault type and specific cause). The following is a schematic diagram of power supply fault detection and diagnosis using the NF5280M6 motherboard as an example. The ISBMC can judge the power supply anomalies of the above motherboard functional units and components, and quickly locate the cause of the power supply fault.

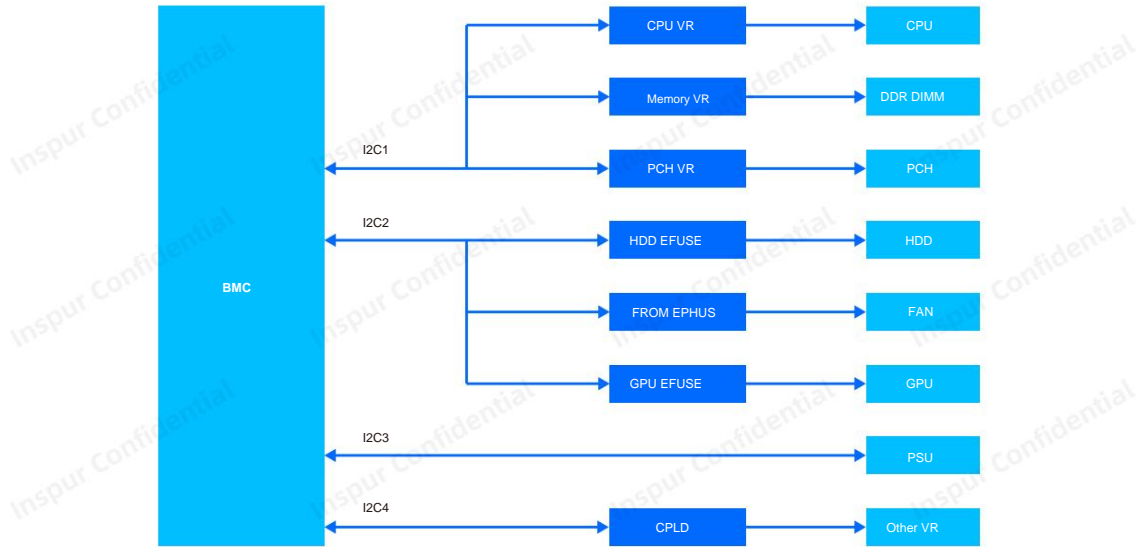


Figure 5-3 Common server VR & Efuse error location topology

5.4.3

Abnormal power failure problem handling

The motherboard supports abnormal monitoring and preprocessing of the board power supply. During the operation of the motherboard, when an abnormal power failure occurs, the motherboard will record the cause of the abnormal power failure and turn off the board power supply in time to avoid the problem of burning the board.

When the server experiences an abnormal power failure, the BMC IDL log will print log records such as PWR_Drop.

MAINBOARD|Assert|Critical|PWR_Drop Abnormal power failure|On Going State|PVCCIO_CPU3_fault|

5.4.4

Power-on timeout problem handling

When all power modules on the motherboard are normal, the motherboard should be powered on normally after pressing the power button; however, when a power module on the motherboard is abnormal, the motherboard may not be powered on normally. When this fault occurs, there will be log records such as PWR_On_TMOUT in the BMC IDL log.

Power Supply PWR_On_TMOUT | Failure detected | Asserted|

5.4.5

Mainboard anti-burn board function design

The motherboard hardware supports power consumption monitoring. When the motherboard 12V current exceeds the set threshold, the motherboard's automatic power-off function will be triggered.

When a circuit module on the motherboard is damaged and causes an overcurrent exception, the protection mechanism will be triggered, and the BMC IDL log will record the following related logs:

MAINBOARD|Assert|Critical|15FFB002|PWR_Drop Power Supply Failure detected |

MAINBOARD|Assert|Critical|15FFB002|Abnormal power failure Shutdown Reason: FAN3~5 |

6 ISBMC Fault Monitoring and Diagnosis

As the core processing unit for fault detection, location, and reporting, ISBMC is responsible for important tasks such as monitoring and recording the daily operation logs of the server system, monitoring and recording system abnormal events, recording system downtime logs, and fault root cause analysis, and outputs the health monitoring status of the entire system in real time.

6.1 System operation log records

6.1.1

POST code monitoring and logging

The ISBMC web interface supports power-on self-test codes. The interface records the server power-on and power-off status, current self-test code, current self-test code description, and historical self-test codes. The power-on self-test code describes the system power-on self-test result information, reflects whether a specific fault occurs in the current self-test, and is expressed in the form of a code. The current self-test code and the current self-test code description are used to locate the specific fault of system startup.

Select "Fault Diagnosis > POST Code" from the navigation bar of the ISBMC Web page to open the page as shown in Figure 6-1.



Figure 6-1 Power-on self-test code web interface

Server power on/off status: mainly detects the power on/off status of the current system.

Current self-test code: Use code to indicate the specific operating status of each device component when the system is turned on.

Current self-test code description: Detailed description of the current self-test code.

Historical self-check code: Historical self-check code.

The current self-test code and its description are shown in Table 6-1. In addition, the historical self-test code is also recorded in `inspur_debug.log`. The log file records the specific fault code recorded by the BIOS during startup to locate the fault stage and fault type. At the same time, the corresponding fault is recorded in the BMC System Event Log, so that the cause of the fault can be traced when an abnormal startup fault occurs.

Current self-test code	Current self-test code description	Current self-test code	Current self-test code description
11	CPU Initialization	15	NB initialization
19	SB Initialization	2B	MEM initialization read SPD
2C	Initialize detection MEM	2F	MEM initialization sets the initial value
31	Memory installation completed	32	CPUPOST -MEM initialization
-	-	-	-

Table 6-1 Power-on self-test code parameter table

6.1.2 Screen Shots

Screen snapshot is a convenient system inspection function provided by ISBMC. Users can capture and save the screen output of the current system through the Web interface.

When the OS is awake or the KVM is turned off, you can use manual screenshot to take a screenshot of the current system screen at any time.

Get the file locally via the network and use image viewing software to browse the screenshot. Delete the screenshot when you don't need it.

In the navigation bar of the ISBMC web page, select Troubleshooting > Screenshot > Manual Screenshot, as shown in Figure 6-2.

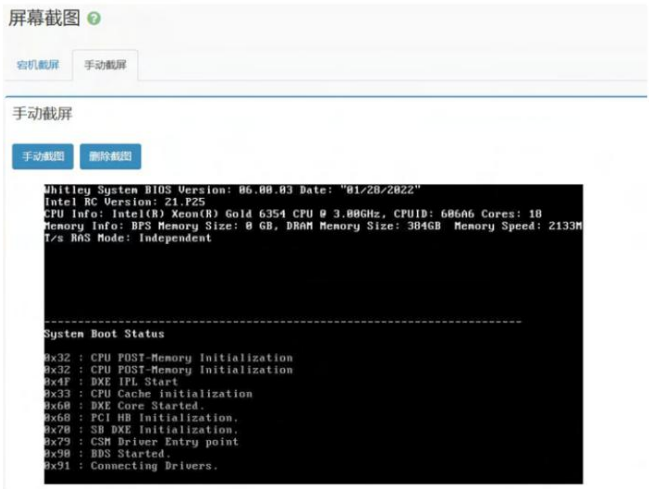


Figure 6-2 Manual screenshot

6.1.3 Maintenance Log Introduction

In the navigation bar, select "Logs and Alarms > One-click Log Collection" to download the compressed package dump_0__20000102-0243.tar.gz and decompress it.

onekeylog, Maintenance Log is located in the folder Log, open the interface shown in Figure 6-3. For specific parameters, see Table 6-2

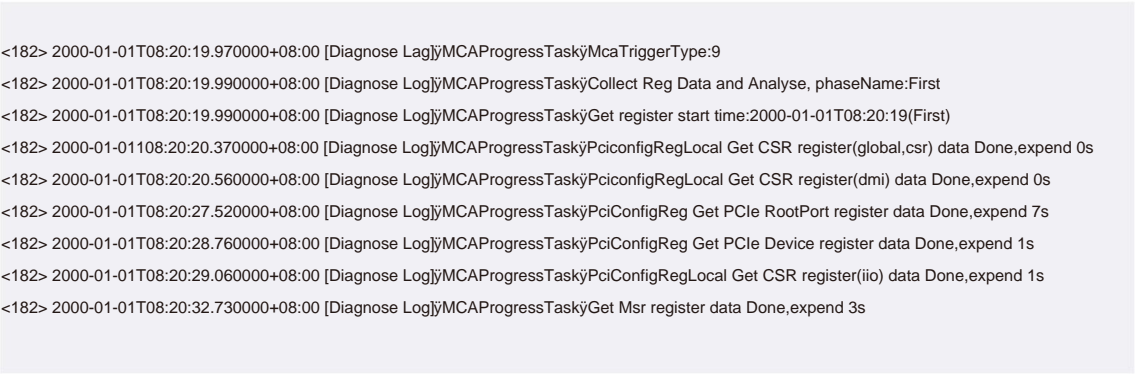


Figure 6-3 Maintenance log

The maintenance log Maintenance.Log mainly records important data during the program operation process and is often used to analyze the specific execution of the software. As shown in Figure 7-4

The log records the start time of the Oem command triggering the collection of register data, and the time spent collecting Csr and PCIe RootPort register data.

And the end time of collecting register data.

parameter	describe
2000-01-01T08:20:19.990000+08:00	Time when the system records the log
Get Msr register data Done, expend 3s	Data recorded in the log by the program

Table 6-2 Maintenance log parameter table

6.2 System downtime log record

6.2.1

Downtime screenshots and downtime videos

When the server operating system crashes, the crash screenshot can capture the last screen of the system crash and save it in the specified format in the storage space of ISBMC. After the user finds that the system crashes, he can log in to ISBMC through the network to view the crash screen and quickly locate and analyze the fault.

In the navigation bar, select Troubleshooting > Screenshot > Screenshot.

As shown in Figure 6-4, when the system crashes, the last screen image of the system crash is obtained.

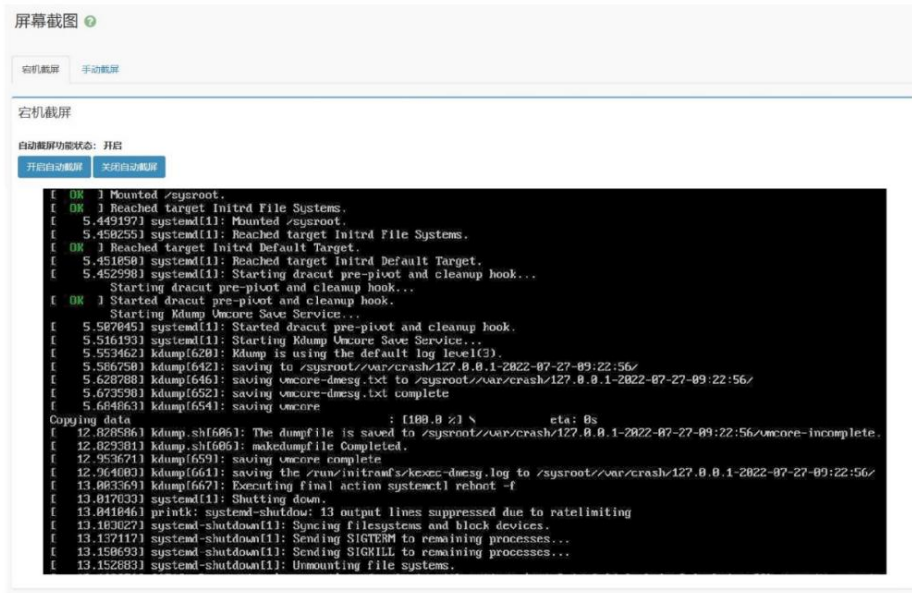


Figure 6-4 System crash screenshot

Enable the downtime recording function. When the server operating system triggers a downtime, the system will automatically record a video before the downtime and save it in a compressed format. ISBMC storage space. Users can download the recorded downtime video (.dat format) through "One-click log collection", and convert the .dat file downloaded to the local ISBMC into an .avi file in "Analyze video", and then display the video in "Downtime video". The technicians can use the recorded video information to assist in locating system failures. This function must be shut down the KVM service before it will take effect.

Select "Fault Diagnosis > Screen Recording > Downtime Recording" from the navigation bar to open the interface shown in Figure 6-5.



Figure 6-5 Downtime recording web interface

6.2.2

Log collection and download interface

In the navigation bar of the ISBMC web page, select Logs and Alarms > One-key Log Collection to download the compressed package dump_0_20000102-024.tar.gz and decompress it as onekeylog. The log files are all located in the Log folder. The interface is shown in Figure 6-6. For parameters, see Table 6-3.

名称	大小	类型 ▲	已修改
 InspurCpuRegisterRawData.json	73.4 KB	程序	2000年1月1日
 InspurIerrAnalyResultReport.json	36.7 KB	程序	2000年1月1日
 AnalyProcess.log	3.0 KB	文字	7月14日
 audit.log	147.5 KB	文字	2000年1月2日
 idl.log	85.9 KB	文字	2000年1月1日
 inspur_debug.log	1.1 MB	文字	2000年1月2日
 InspurDiagnoseComponent.log	20.9 KB	文字	2000年1月1日
 maintenance.log	170.4 KB	文字	2000年1月2日
 selelist.csv	43.4 KB	文字	2000年1月2日

Figure 6-6 Log collection interface

Log collection download path	Information Items	USE
Onekeylog/log/InspurCpuRegisterRawData.json CPU register		Record the time of obtaining register data, trigger mode, CPU type, Data of CPU registers, etc.
Onekeylog/log/InspurIerrAnalyResultReport.json	Fault diagnosis and analysis log	Record register analysis results, information collection time, CPU type, method of collecting diagnostic data, etc.
Onekeylog/log/AnalyProcess.log	Fault diagnosis and analysis process log	Record the specific process of IERR fault diagnosis and the diagnosis and analysis results (the diagnosis results will be pushed to the SEL log).
Onekeylog/log/audit.log Onekeylog/log/	Audit log	Record user login, logout, user management, firmware update and recovery, etc.
idl.log Onekeylog/log/inspur_debug.log	IDL Log	Logs the event description of the entity component and displays the error level.
Onekeylog/log/maintenance.log	Debug Log	Stores information about the debugging process and displays the level of information.
	Maintenance log	Record important information of user requirements or technical personnel debugging.
Onekeylog/log/selelist.csv	SEL Log	Record the sensor name, sensor type, and detailed description of the triggering event in the system.

Table 6-3 Log file parameters

6.2.3

Downtime diagnosis case

When a server IERR catastrophic failure occurs, ISBMC will immediately execute the IERR fault accurate location process, and the detailed fault diagnosis report will be recorded in the "Fault Diagnosis"

In the "Fault Analysis Process Log", users can view the exact time of the fault, the module where the fault occurred and the fault type, the fault phenomenon description, and the cause of the fault.

The specific equipment, detailed criteria for fault location and handling suggestions are shown in Figure 6-7. In addition, for difficult and complex downtime cases, ISBMC also supports ASD,

ACD, BAFI and other technologies enable rapid analysis and diagnosis of difficult cases and root cause location.

Figure 6-7 shows that CPU0 accesses PCIe device MMIO resources abnormally, and the Tor Timeout causes 3-Strike Timeout, which further causes CPU IERR fault. As can be seen from the legend, fault location first finds the faulty CPU CPU0, then finds MCA Bank MC10 that records the fault field data, and analyzes the detailed fault type Tor_Timeout from the Bank. The address recorded in the Bank is traced back to the PCIe that uses the MMIO address space.

The device is a Mellanox ConnectX-5 network card, and the device name, BDF, slot information, etc. are printed in detail.

```
[2020-06-08 14:16:31] =====Analysis first fault source CPU=====Start=====
[2020-06-08 14:16:31] IerrLogging: The first fault source CPU is CPU0
[2020-06-08 14:16:31] =====Analysis first fault source CPU=====End=====
[2020-06-08 14:16:31] The first fault source CPU is CPU0
[2020-06-08 14:16:31] FirstErrSrcId value 0x4a meets the conditions, Chaid = 10 Bank = 10
[2020-06-08 14:16:31] Cpu0_Cha10_MC10_STATUS 0xfe200000000c1136 0x94 is valid
[2020-06-08 14:16:31] MSCOD:MCx_Status[31:16] = 0x000c TOR_TIMEOUT
[2020-06-08 14:16:31] MCACOD:MC3_STATUS Bit[15:0] = 0x0400: 3-strike timeout
[2020-06-08 14:16:31] Mc10_Addr is valid
[2020-06-08 14:16:31] Cpu0_Cha10_MC10_ADDR 0x0000203ffa000000 0x94
[2020-06-08 14:16:31] ADDR match fault device: 0x0000203ffa000000 #CPU0_PE2(Critical)
[2020-06-08 14:16:31] TorDump Mc10Address to match fault device: 0x0000203ffa000000 #CPU0_PE2
[2020-06-08 14:16:31] Replace PCIE device location: #CPU0_PE2
[2020-06-08 14:16:31] Diagnosis result: [ {
    "DeviceType": "PCIE",
    "Location": "#CPU0_PE2",
    "ErrorType": "FATAL",
    "PcieBus": "0x4b",
    "PcieDevice": "0x0",
    "PcieFunc": "0x0",
    "Vendor": "Mellanox Technologies",
    "Device": "MT28800 Family [ConnectX-5 Ex]",
  } ]
```

Figure 6-7 Fault diagnosis and analysis process log

6.2.4 Non-downtime monitoring case

ISBMC can monitor common SMART faults of NVME SSD, including remaining (redundant) space abnormality, disk overtemperature, read-only mode, volatile memory failure, and pre-fault reminders. See Table 6-4 below for details.

SMART Fields	ISBMC Records	Suggested Action
NVME SSD remaining space is lower than the threshold alarm	[DiagNVME]:SN:S63SNE0R509578 , available spare space has fallen below the threshold!	When this alarm occurs, it means that the redundant space of the NVME SSD is insufficient and has reached the redundant space threshold. It is recommended to replace the NVME SSD with a new one.
NVME SSD temperature exceeds the threshold alarm	[DiagNVME]:SN:S63SNE0R509578, Tempperature is above an over temperature threshold or below an under temperature threshold!	When this alarm occurs, it indicates that the heat dissipation of the server or the computer room is abnormal. It is recommended to increase the system fan speed or reduce the ambient temperature of the computer room.
NVME SSD system reliability degradation	[DiagNVME]:SN:S63SNE0R509578, NVM Subsystem reliability has been degraded!	If the temperature exceeds the limit, it is recommended to check the heat dissipation. If the temperature is not excessive, it is recommended to replace the disk.
NVME SSD media is in read-only mode.	[Diag NVME]:SN:S63SNE0R509578, The media has been placed in read only mode!	When this alarm occurs, it means that the NVME SSD has entered "read-only" mode and data cannot be written. To avoid the risk of data loss, please replace it with a new NVME SSD as soon as possible.
NVME SSD volatile memory backup system failure alarm	[Diag NVME]:SN:S63SNE0R509578, The volatile memory backup device has failed!	When this alarm occurs, it means that the DRAM device inside the NVME SSD is damaged and the disk cannot work normally. Please replace it with a new NVME SSD as soon as possible.
NVMe SSD PDLU life monitoring yPercentage Drive Life Used) exceeds the threshold Warning level alarm	[DiagNVME]:SN:S63SNE0R509578, life used warning level alert!	When this alarm occurs, it means that the life of the NVME SSD is about to expire. Please replace it with a new NVME SSD as soon as possible.
	[DiagNVME]:SN:S63SNE0R509578, life used critical level alert!	
NVME SSD failed to read temperature sensor	[DiagNVME]:SN:S63SNE0R509578, Read temp sensor failed assert!	When this alarm occurs, it indicates that the temperature sensor of the NVME SSD is abnormal. It is recommended to replace the NVME SSD with a new one.

Table 6-4

6.3 System Event Log

Through the functions of the "System Event Log" interface, users can view the ISBMC system event log, download the system event log, and clear the system event log. The system event log features are as follows:

- (1) A maximum of 3639 entries are supported.
- (2) Support humanized log management: visualization, filtering, downloading, and clearing.
- (3) Support local storage and archiving.
- (4) Supports circular mode. When the SEL is full, the old logs will be discarded and the new logs will be retained.
- (5) When the SEL is cleared, a log of "SEL cleared" will be recorded in the SEL.
- (6) Support exporting SEL via Web or IPMI CMD.
- (7) Supports notification of events to remote clients via SNMP Trap and Syslog.

6.3.1 System event log

In the navigation bar of the ISBMC web page, select Logs and Alarms > System Event Log to open the interface shown in Figure 6-8. For parameter descriptions, see Table 6-5. For log operation descriptions, see Table 6-6.

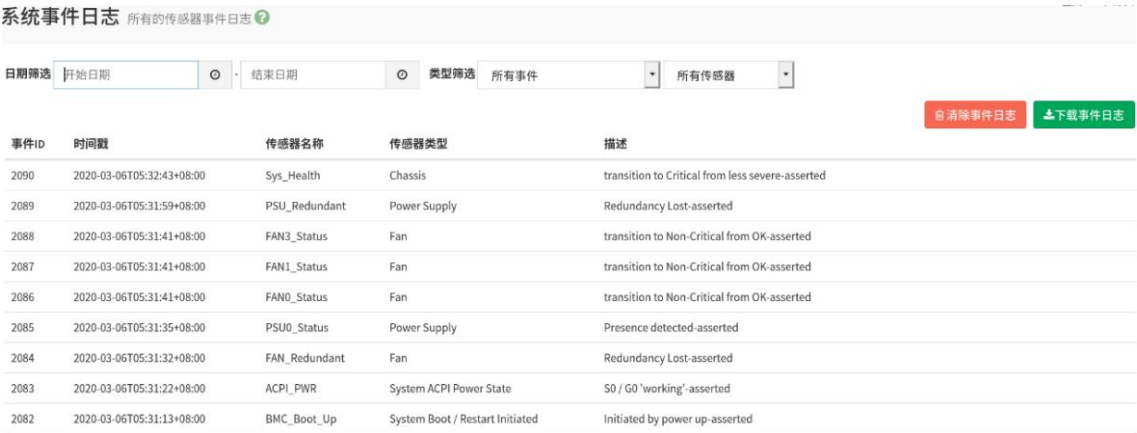


Figure 6-8 System event web interface

parameter	describe
Event ID	Event ID in SEL
Timestamp	Event log generation time
Sensor Name	Sensor name. Users can view the names of all sensors on the device through ipmitool sdr elist
Sensor Type	Sensor types defined in IPMI 2.0: Temperature //Temperature sensor Voltage // Voltage sensor Processor //CPU status sensor Power Unit //PSU status sensor Memory //Memory status sensor Drive Slot // Hard disk status sensor Critical Interrupt //Pcie status sensor
describe	Event details

Table 6-5 System event log parameter table

parameter	describe
filter	Select event type, sensor, and start and end dates to filter your search. action: You can use filter options (event type, sensor name, start and end time), View specific events logged on the device.
Download event log	Click this button to download the log to your local computer.
Clear Event Log	Clicking this button will delete all existing sensor log records.

Table 6-6 Log operation description

6.3.2

Fault reporting

ISBMC supports real-time monitoring of system alarm events and reports them to remote receiving servers through SNMP (Simple Network Management Protocol) TRAP, mailbox, syslog, etc.

Through the functions of the "SNMP TRAP Settings" interface, users can

- (1) Enable SNMP TRAP
- (2) Setting up alert strategies

In the navigation bar of the ISBMC web page, select Logs and Alarms > SNMP TRAP to open the interface shown in Figure 7-12 and Figure 7-13.

SNMP Trap

☒ 启用SNMP Trap

Trap版本

V1

告警级别（高于此告警级别的事件将被发送）

Info

团体名

主机标识

HostName

用户名

认证协议

认证密码

加密协议

加密密码

引擎号

设备类型

All

保存

Figure 6-9 SNMP TRAP web interface

Check Enable SNMP TRAP to expand the page. SNMP TRAP supports TRAP version selection. The default version is V1. When V3 is selected, you need to add the user name, authentication password, encryption protocol, and encryption password. Supports reporting filtering based on the severity level of the alarm event. The Trap message will carry a host identifier, which can specify any one of the host name, board serial number, and product asset tag.

告警策略设置

ID	启用	目的地	端口	动作
0	<input type="checkbox"/>		162	<div>保存 测试</div>
1	<input type="checkbox"/>		162	<div>保存 测试</div>
2	<input type="checkbox"/>		162	<div>保存 测试</div>
3	<input type="checkbox"/>		162	<div>保存 测试</div>

Figure 6-10 Alarm strategy web interface

The alarm policy supports setting the IP addresses of four syslog servers as the destination and port, and clicks Save. It supports sending test information to the receiving target.

Through the functions of the "Mailbox Alert" interface, users can

- (1) Enable or disable SMTP email alert.
- (2) Set the email address to receive alerts.

Select Logs and Alerts > Email Alerts from the navigation bar to open the interface shown in Figure 6-11 and Figure 6-12.

邮箱告警

SMTP 设置

☒ 启动SMTP邮件告警

SMTP服务器地址

SMTP服务器端口

SMTP服务器安全端口

☐ 发件人身份认证

发件人电子邮件 ID

发件人用户名

发件人密码

☐ 启用SMTP SSLTLS

☐ 启用SMTP STARTTLS

邮件主题

主题附加

☐ 主机名 ☐ 单板序列号 ☐ 产品资产标签

告警发送级别(高于此告警级别的事件将被发送)

Info

保存

Figure 6-11 Email Alert Web Interface

Check Enable SMTP email alert to expand the page. SMTP supports selecting SMTP server address, SMTP server port, SMTP server secure port, whether to enable sender ID, sender email ID, sender user name, sender password, whether to enable SMTP SSLTLS, whether to enable SMTP STARTTLS, email subject, subject attachments, alert sending level and other information.

设置接收告警的邮件地址

邮件地址1:	<input type="text"/>	描述:	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input type="checkbox"/>	启用
邮件地址2:	<input type="text"/>	描述:	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input type="checkbox"/>	启用
邮件地址3:	<input type="text"/>	描述:	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input type="checkbox"/>	启用
邮件地址4:	<input type="text"/>	描述:	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input type="checkbox"/>	启用

Figure 6-12 Web interface for receiving alarm email addresses

The email address for receiving alarms supports up to 4 recipients. Each recipient can be configured with an email address and description information for the email address, and supports sending test information to the recipient.

6.3.3

Log Settings

BMC supports the "Log Settings" function. By configuring the Syslog log settings, the BMC system can send logs to a third-party server in the form of Syslog messages.

Select "Log & Alarm > Log Settings" in the navigation bar to open the interface shown in Figure 6-13. Click "Syslog Log Settings" to open the interface shown in Figure 6-14. For specific parameters, see Table 6-7 and Table 6-8.



Figure 6-13 Log settings interface

Syslog 设置

Syslog 设置

Syslog告警设置

☒ 远程日志

告警级别(高于此告警级别的事件将被发送)

Warning

传输协议

☒ UDP ☐ TCP

设置Syslog服务器和报文格式

序号	启用	服务器地址	端口	日志类型	操作
0	<input checked="" type="checkbox"/>	100.2.74.41	514	<input type="checkbox"/> idt日志 <input checked="" type="checkbox"/> audit日志	<input type="button" value="保存"/> <input type="button" value="测试"/>
1	<input checked="" type="checkbox"/>	100.2.74.70	515	<input type="checkbox"/> idt日志 <input checked="" type="checkbox"/> audit日志	<input type="button" value="保存"/> <input type="button" value="测试"/>

Figure 6-14 Syslog settings

parameter	describe
Remote Log	Syslog alarm log storage location, you can choose whether to store remote logs. When using remote logs, BMC stores logs in the remote Syslog server and local log files. When not using remote logs, they are only stored in local log files.
Alarm level	Times above this alarm level will be sent, options are: Info: Sends Info, Warning, and Critical level warning information. Warning: Sends warning or critical level warning information. Critical: Only critical level alarms are sent.
Transport Protocol	The transmission protocol used when Syslog messages are transmitted between the BMC system and the Syslog server can be: UDP: A connectionless protocol. Before officially sending and receiving data, the sender and receiver do not establish a connection and directly transmit the official data. TCP: A connection-oriented protocol. Before officially sending or receiving data, a reliable connection must be established between the sender and the receiver.

Table 6-7 Syslog settings

parameter	describe
Serial number	Serial number.
Enable	Enable or disable the automatic Syslog message reporting function.
Server address	Syslog server address information.
port	Syslog server port number. The log
Log Type	type to be reported using Syslog messages. You can choose one or both of ldl log and audit log.
operate	Save: Save the Syslog server and message related information. Test: Test whether the configured Syslog channel can send messages successfully.

Table 6-8 Syslog server and message format

6.3.4

IDL log and handling suggestions

Inspur fault diagnosis IDL is a unique log type of Inspur ISBMC, which is used to record the event history based on IPMI sensors on BMC devices. Compared with system event log information, IDL log information provides more and more complete information, and each log has corresponding processing suggestions, which can more effectively help users perform log diagnosis and analysis. Logs can be filtered by date, severity, device, keyword, etc., and log download and log clearing operations can be performed. Click the button behind each log to obtain processing suggestions and corresponding operation steps for this log.

You can view the BMC IDL log list on this device through the "IDL Log" interface function. You can view the processing suggestions for the alarm event by clicking the processing suggestion button on the right side of the corresponding alarm event.

In the navigation bar of the ISBMC web page, select Logs and Alarms > IDL Logs to open the interface shown in Figure 6-15. For detailed parameter descriptions, see Table 6-9. For IDL log operation descriptions, see Table 6-10.

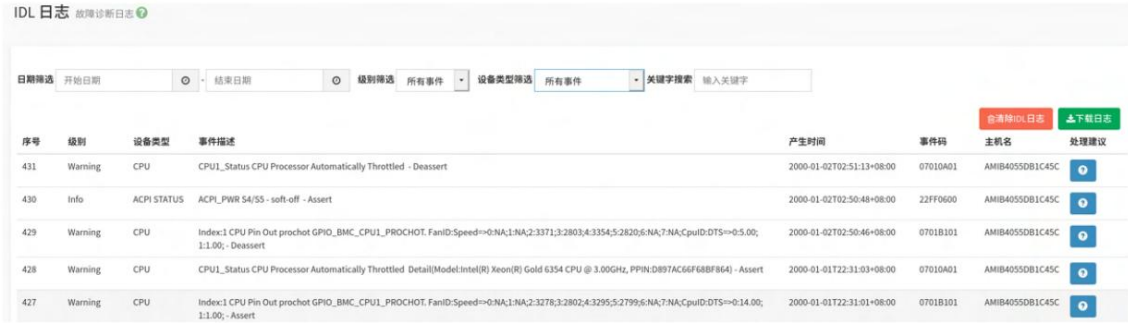


Figure 6-15 IDL log web interface

parameter	describe
Serial number	Event ID in IDL log
level	Event error levels, including information, warning, and severe.
Device Type	FANyINTRUSIONyCPUyPSUyMEMORYyDISKyPCleJBMCy...
Event Description	Detailed description of the alarm event
Generation time	IDL log generation time
Event Code	Unique fault code of the alarm event, length 8 bytes
Hostname	Server system host name
Suggestions	Suggestions for handling this alarm event

Table 6-9 IDL log parameter description table

parameter	describe
filter	Select severity and start and end dates to filter your search Action: Users can use filtering options (event severity level, time, keywords) to view specific events logged in the device.
Download log	Download IDL log to local computer
Clear Logs	Click the Clear Log button to clear all IDL log information on the BMC.

Table 6-10 IDL log operation description table

IDL logs support alarm event processing suggestions. Users can clear alarm events according to the processing suggestions and corresponding operation steps of IDL logs, as shown in Figure 6-16.

处理建议

- Step1:Check the ambient temperature,should be higher than rated temperature of server.
- Step2:Check whether fan fails.
- Step3:Check air inlet and air outlet, make sure there is no blokage.
- Step4:Power off server, and make sure airduct installed correctly.
- Step5:Power off server, and make sure CPU heatsink installed correctly.
- Step6:Replace abnormal CPU,check whether the alarm disappears.
- Step7:Please contact Inspur FAE.

确定

Figure 6-16 Suggestions for handling IDL log alarm events

6.4 Whole system health status monitoring

6.4.1 System Overview

Before logging in to the BMC remote page using a browser, enter `https://BMC_IP/#dashboard` in the address bar and press Enter to open the page shown in Figure 6-17. Before entering the user name and password, an icon indicating the health status of the entire server is displayed. Based on the icon, users can determine whether the server has any abnormal problems before logging in.

After logging in to the BMC remote page, users can view server information, server operation status information, firmware version information, online user information, etc. on the home page "System Overview" interface to understand the health status of the entire system, as shown in Figure 6-18. For specific parameters, see Table 6-11.



Figure 6-17 BMC login interface



Figure 6-18 System overview web interface

Area	Information displayed
Server Information	<p>Provide basic information about the server, including: Product Type: product type of the server.</p> <p>Product Name: The product name of the server.</p> <p>Manufacturer: The manufacturer of the server.</p> <p>Product Serial: The product serial number of the server.</p> <p>Asset ID: The asset ID of the server.</p> <p>System UUID: System UUID information of the server.</p> <p>Device UUID: Device UUID information of the server.</p> <p>Binding management interface: The IP address of the server's binding management port.</p>
Server Health	<p>Provides the operating status of the server, including: Server power on/off status: on or off.</p> <p>UID Status: The UID indicator is on or off.</p> <p>Overall Status: The overall status of the server.</p> <p>Processor: CPU health status.</p> <p>Memory: Memory health status.</p> <p>Hard disk: Hard disk health status.</p> <p>Fan health status.</p> <p>Network: Network health status.</p> <p>Power: Power health status.</p> <p>Note: The health status of each module can include:</p> <div><div></div> Normal/In-position</div> <div><div></div> warning</div> <div><div></div> serious</div> <div><div></div> Not present/light off</div>
Firmware version information	<p>Firmware version information, including: BMC version.</p> <p>BIOS version.</p> <p>ME version.</p> <p>PSU version.</p> <p>CPLD version.</p> <p>Note: The firmware type displayed in this area may vary depending on the model.</p>
Online user information	<p>Information about the user currently logged in to the BMC Web, including:Type: Login type, such as HTTPS, CTL, etc. Username: User</p> <p>name for logging into the BMC. User rights: User</p> <p>group information corresponding to the user who logs into the BMC.</p> <p>IP: The IP address of the machine where the user who logs in to the BMC is located.</p>

Table 6-11 IDL system overview

6.4.2

Sensor Summary List

Through the functions of the "Sensor" interface, users can view the relevant information of all sensors supported by the current system, and can jump to the Modify Sensor Threshold interface to set it by double-clicking the sensor line in the Threshold Sensor interface. The Sensor interface includes the Threshold Sensor tab and the Discrete Sensor tab.

Select "Sensor > Threshold Sensor" in the navigation bar of the ISBMC web page to open the interface shown in Figure 6-19. For specific threshold sensors to be monitored, see Table 6-12. The range includes but is not limited to Table 6-12. For parameter descriptions, see Table 6-14.



Figure 6-19 Threshold sensor web interface

name	Current Value	Severely low threshold	Severe high threshold	unit
Inlet_Temp	25	N/A	55	you_c
Outlet_Temp	30	N/A	N/A	you_c
CPU0_Temp	Disable	N/A	N/A	you_c
CPU1_Temp	Disable	N/A	N/A	you_c
CPU0_NVDIMM_T	Disable	N/A	83	you_c
CPU1_NVDIMM_T	Disable	N/A	83	you_c
PCH_Temp	Disable	N/A	107	you_c
CPU0_Vcore	Disable	1.206	2.223	volts
CPU1_Vcore	Disable	1.206	2.223	volts
CPU0_VCCIO	Disable	0.774	1.26	volts
CPU1_VCCIO	Disable	0.774	1.26	volts
PSU0_WIN	224	N/A	N/A	volts
PSU1_VIN	Disable	N/A	N/A	volts
SYS_12V	12.18	10.2	14.04	volts
Total_Power	32	N/A	N/A	watts
FAN_Power	8	N/A	N/A	watts
CPU_Power	Disable	N/A	N/A	watts
PSU0_PIN	36	N/A	N/A	watts
PSU1_PIN	Disable	N/A	N/A	watts
FAN1_F_Speed	8400	N/A	N/A	rpm
FAN1_R_Speed	7200	N/A	N/A	rpm
FAN2_F_Speed	8400	N/A	N/A	rpm
FAN2_R_Speed	7200	N/A	N/A	rpm
FAN3_F_Speed	Disable	N/A	N/A	rpm
FAN3_R_Speed	Disable	N/A	N/A	rpm

Table 6-12 Threshold Sensors

Select "Sensor > Discrete Sensor" in the navigation bar to open the interface shown in Figure 6-20. The specific monitored discrete sensors are shown in Table 6-13, and their range includes but is not limited to Table 6-13. The parameter description is shown in Table 6-15.

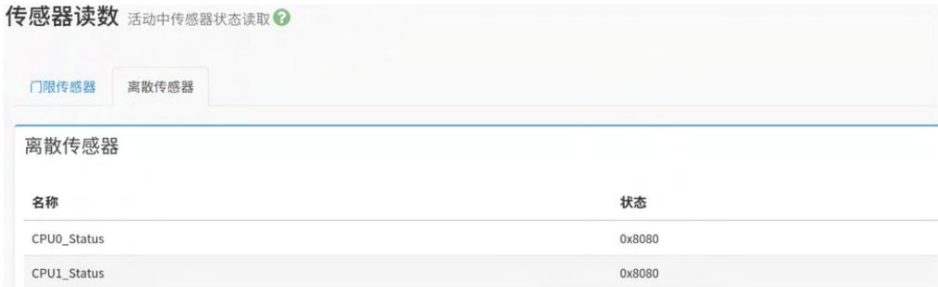


Figure 6-20 Discrete sensor web interface

name	state
CPU0_Status	0x8080
CPU1_Status	0x8080
BMC_Boot_Up	0x8000
SEL_Status	0x8000
PSU0_Status	0x8001
ACPI_PWR	0X8000
Power_Button	0X8000
UID_Button	0x8002
FAN_Redundant	0x8002
PWR_On_TMOUT	0x8000
CPU_C0D0	0x8040
CPU0_C0D1	Disabled
Disk0_Status	Disabled
PCIe_Status	0x8000
BIOS_Boot_Up	0x8002
Post_Status	0x8000
Sys_Heath	0x8004

Table 6-13 Discrete sensors

parameter	describe	parameter	describe
name	Sensor Name	Non-critical low threshold	Sensor Non-Critical Low Threshold
Current Value	Current sensor reading	Non-serious high threshold	Sensor Non-Critical High Threshold
state	Sensor Status	Severe high threshold	Sensor Critical High Threshold
Irreversible low threshold	Sensor irreversible low threshold	Irreversible high threshold	Sensor irreversible high threshold
Severely low threshold	Sensor critical low threshold	unit	Sensor reading unit

Table 6-14 Threshold sensor parameters

parameter	describe
name	Sensor Name
state	Sensor Status

Table 6-15 Discrete sensor parameter table

6.4.3

Audit logging

Through the functions of the "Audit Log" interface, users can view the system's audit log. The BMC audit log features are as follows:

(1) Key management behaviors of logging into the system through SSH, Redfish, IPMI, and Web interface will be recorded, including but not limited to login, logout, user management, password management, authorization management, changes to core security configurations (such as access control policies, automatic update policies, security monitoring policies, and audit functions), firmware updates, and recovery.

(2) The supported size of the audit log is 200K. If it exceeds 200K, the older logs will be backed up to the BMC. The current audit log can be accessed through the Web. Older audit logs can be downloaded through the one-click log collection function.

In the navigation bar of the ISBMC web page, select Logs and Alarms > Audit Logs to open the page shown in Figure 6-21. For parameter descriptions, see Table 6-16.

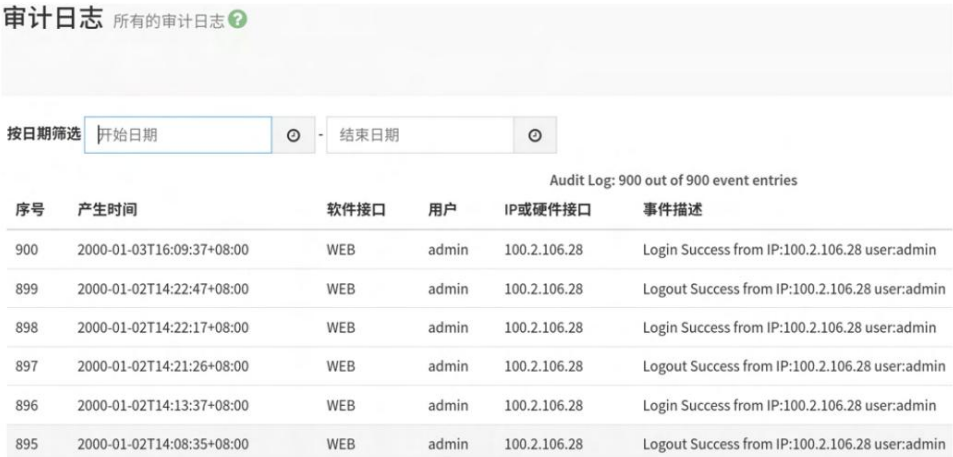


Figure 6-21 Audit log web interface

parameter	describe
Serial number	Audit log sequence number. The smaller the sequence number, the earlier the operation occurred.
Generation time	Audit log generation time
Software Interface	Software interfaces, including: Web CLI IPMI KVM VMEDIA_CD VMEDIS_HD
user	User, records the log event operation user, such as admin, sysadmin or NA, etc.
IP or hardware interface	IP or hardware interface, hardware interfaces include SERIAL, HOST, IPMB, USB and SSIF
Event Description	Event details

Table 6-16 Audit log parameter table

6.4.4

Asset Information

Through the "System Information" interface, users can view the asset information details of the system. There are seven sub-pages in this interface, including CPU, memory, power supply, device list, hard disk, network card, and security chip, which display the detailed information of various types of devices. Taking the CPU sub-page as an example, it will display the CPU's in-place status, processor ID, specific model, current speed, number of cores, number of threads, TDP, cache size at all levels, PPIN, etc. Specific detailed information of memory, power supply, and PCIe devices is shown in the example in Figure 6-22.

In the navigation bar of the ISBMC web page, select Information > System Information to open the interface shown in Figure 6-22.

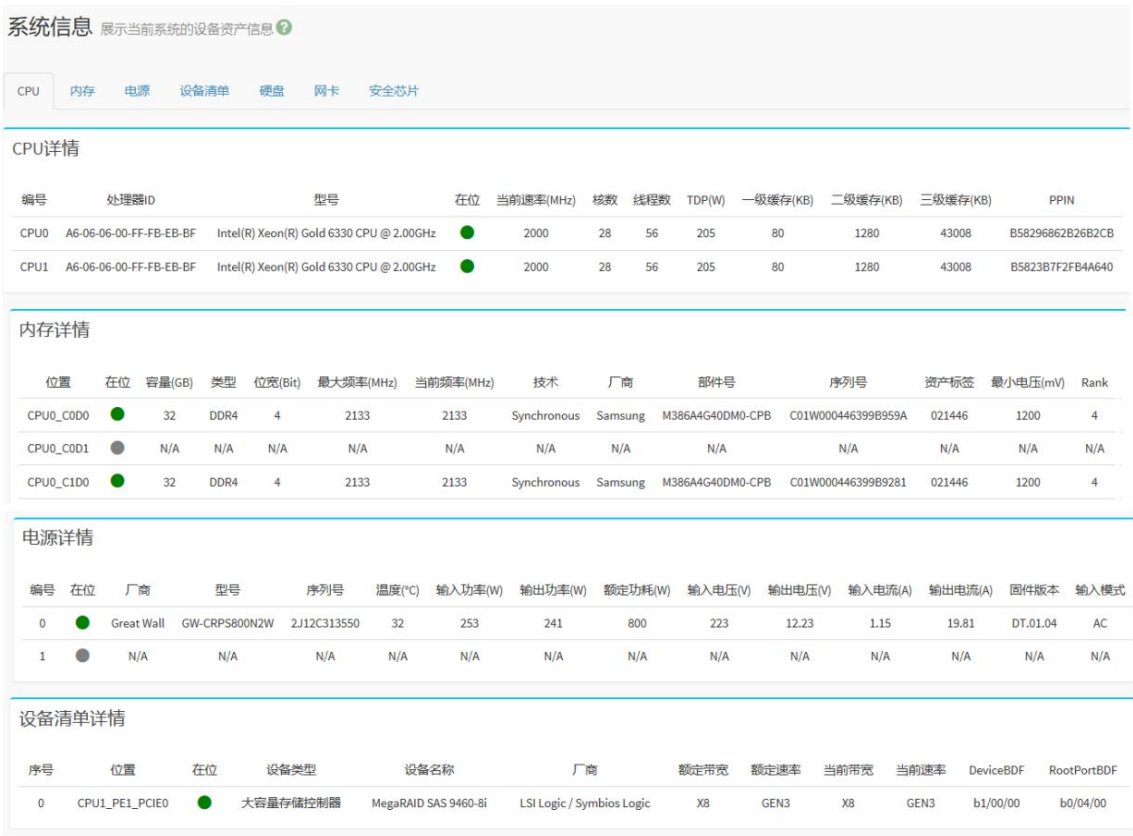


Figure 6-22 Asset information web interface

浪潮信息 www.inspur.com Inspur®
Technical Support and Service Hotline: 400-860-0011
Purchase Consultation Hotline: 400-860-6708 / 800-860-6708



Inspur Server



Inspur Storage