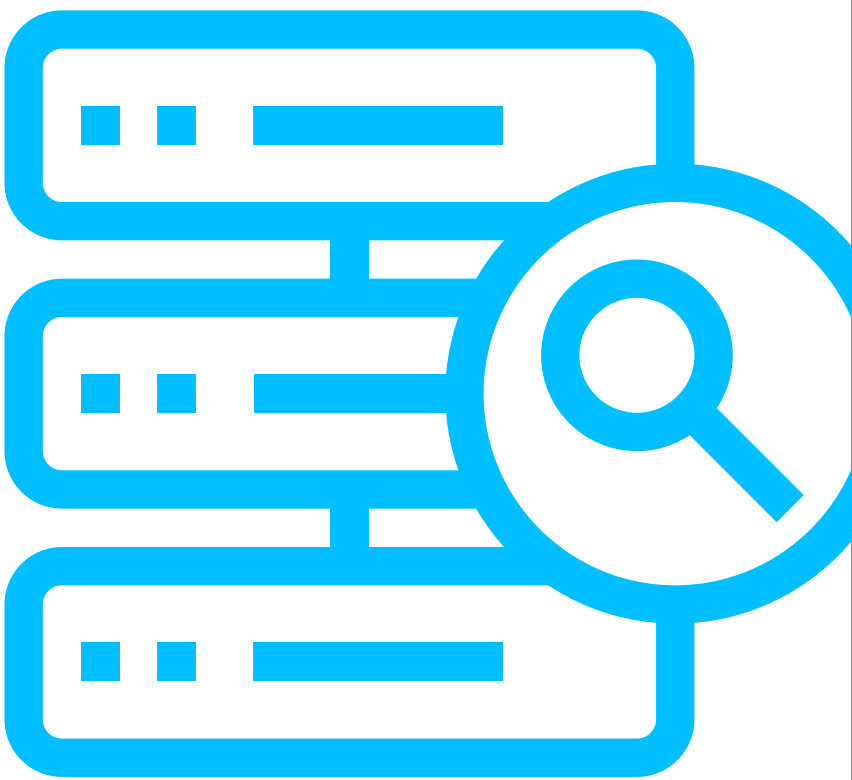
inspur

浪潮®服务器
故障诊断系统
技术白皮书

Inspur Server®
Fault Diagnosis System

ISFDS®



文档版本 1.0
发布日期 2022-09-05

尊敬的用户：

注:您购买的产品、服务或特性等应受浪潮集团商业合同和条款的约束。本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，浪潮集团对本文档内容不做任何明示或默示的声明或保证。由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

技术服务电话： 4008600011

地址： 中国济南市浪潮路1036号 浪潮电子信息产业股份有限公司

邮编： 250101

目录

1 引言

随着“新基建”、“东数西算”、“元宇宙”等数字化浪潮的推进，全社会数字化转型加速，数字化建设飞速发展，当今数字化在国家和企业层面均已上升到战略高度。通用、存储、超融合、AI服务器等作为支撑数字化计算服务的基础设施硬件，在云计算、大数据、物联网、AI等各领域的大批量部署呈指数级不断增长，并且其承载的业务也越来越多，计算压力，存储能力，网络带宽正在经受严峻的考验。

另外，服务器本身作为计算、存储、网络等新技术应用的复杂软硬件集合体，由处理器、内存、存储设备(RAID卡/HDD/SSD)、AI加速卡(GPU卡/ASIC加速卡/FPGA加速卡)、网卡(以太网卡/ Infiniband网卡/智能网卡)、主板、电源设备、散热设备、BIOS固件、BMC管理软件等组件组成，其软硬件复杂度也在不断提升；所以，在所难免会存在不可预期的故障造成宕机，影响数字化业务正常运行，特别是关键业务的宕机造成的客户损失及影响是难以估量的。

当前，海量服务器数据中心正面临着高昂的运维成本支出和维护管理复杂度的巨大挑战，所以提升服务器的维护体验，能够确保服务器连续稳定地运行，实时掌握服务器运行健康状态，即使在出现故障的情况下也可以及时修复恢复业务运行，逐步成为服务器需要具备的基础保障功能。

2 概述

浪潮服务器故障诊断系统ISFDS(Inspur Server Fault Diagnosis System)是浪潮开发的具有自主知识产权的服务器故障诊断系统，对服务器各组件软硬件设计进行深度定制融合，自主创新开发浪潮自有服务器故障诊断专家规则库，可以对服务器进行全生命周期的工作健康状态实时监测、预警，在宕机故障发生时可实现分钟级快速精准诊断、修复和恢复业务运行；提升产品硬核竞争力的同时为推进中小客户免运维的实现，以及大客户数据中心智能运维的实现，做出了实质性跨越式的贡献。

2.1 IS-FDS介绍

当前服务器运维痛点问题：

● 设备故障宕机后，定位故障的关键部件寄存器日志信息收集不完整，历史故障记录信息不健全，无法进行自动准确的故障部件定位；

● 故障诊断定位效率低下，服务器出现问题后主要基于人工分析和经验判断结果，自动化与智能化程度不高。

● 设备故障恢复上线时间长， 现场故障难以复现，需要多次手动更换部件来验证，排障效率低下，对客户的业务影响较大。

解决问题的ISFDS技术方案：

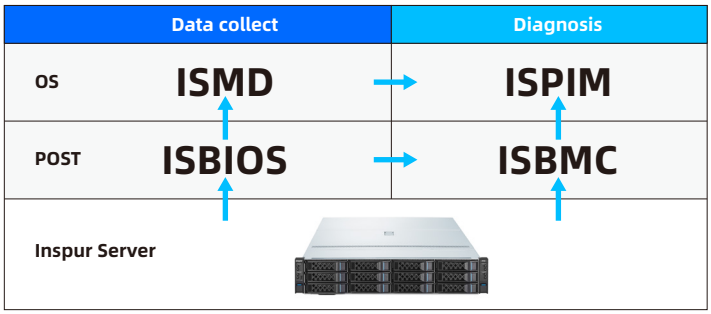


图2-1

● 服务器长久持续运行状态下，需要有健康状态的实时监控上报，ISBMC 可以在未发生故障之前，上报出是否存在异常的电压信号波动，CPU可修复错误过多，局部过多热量累积，大量内存ECC发生等。用户可提前感知这些异常的存在，关注存在预告警的服务器计划性停机维护，避免演变成致命故障或灾难性故障。

● 建立以 ISBMC 为中心的带外故障处理系统，优化对服务器各部件故障信息及使用资源的抓取逻辑，保障所有故障数据能实时完整收集，再结合服务器完整的资源拓扑，可以轻松处理各类致命故障和灾难性宕机的分析诊断定位，提升服务器故障诊断明确率与处理时效，实现分钟级诊断定位，快速更换故障部件恢复业务运行。

● 建立浪潮 ISFDS 故障诊断专家规则库，对浪潮海量客户宕机日志的深入分析学习，不断完善专家诊断规则，浪潮故障诊断专家规则库在ISBMC的落地，实现了IERR宕机诊断准确率95%的成绩。

● 研制浪潮物理基础设施管理平台ISPIM，实现ISBMC带外日志和ISMD带内日志汇总诊断,实现故障现场日志场景完整还原，实现故障监控覆盖度最大化，故障诊断准确率最大化；该平台带外硬件日志是通过ISBMC REST接口进行收集，带内系统日志是通过ISMD REST接口进行收集；也可以仅通过ISBMC进行收集带外硬件日志；ISPIM、ISBMC均具备诊断后的预告警事件直接推送到客户运维系统的能力，并且支持上报接口定制化。

● 研制浪潮服务器带内管理驱动ISMD，作为带内系统采集的代理角色，支持性能指标订阅，实现了带内系统性能、配置和日志收集等功能，支持主/被动的形式上报至ISPIM进行分析，实现了浪潮服务器带内、带外管理的能力。对于ISPIM通过ISMD进行带内日志收集的方式，需要在被管理设备系统OS下安装ISMD，ISPIM发现ISMD后即可进行带内系统日志收集。

2.2 术语

通过表2-1对本文出现的专业名词及缩略语进行解释。

术语	解释	术语	解释
ISFDS®	Inspur Server Fault Diagnosis System	PFR	Platform Firmware Resilience
ISBIOS®	Inspur Server BIOS (Basic Input/Output System)	PMBus	Power Management Bus
ISBMC®	Inspur Server BMC(Baseboard Management Controller)	SMBus	System Management Bus
ISMD™	Inspur Server Management Driver	SATA	Serial Advanced Technology Attachment
ISPIM™	Inspur Server Physical Infrastructure Manager	SMTP	Simple Mail Transfer Protocol
MCA	Machine Check Architecture	SNMP	Simple Network Management Protocol
CE	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
SRAO	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
PECI	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
AER	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	APEI	ACPI Platform Error Interfaces
RAS	Reliability、Availability、Serviceability	GHES	Generic Hardware Error Source
HBA	Host Bus Adapter	WHEA	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
NIC	Network Interface Controller		

表2-1 术语表

3 IS-FDS 整体架构

ISFDS依托浪潮自研服务器硬件开发，主要功能由ISBIOS、ISBMC、主板硬件设计联合实现；实现了服务器全生命周期的异常部件即时上报，有隐患部件智能上报，发生宕机后引发故障部件即刻准确上报；并且对非致命类故障进行实时修复，对服务器硬件固件运行状态进行实时评估，全方位监测设备的健康状态。

3.1 服务器故障分类

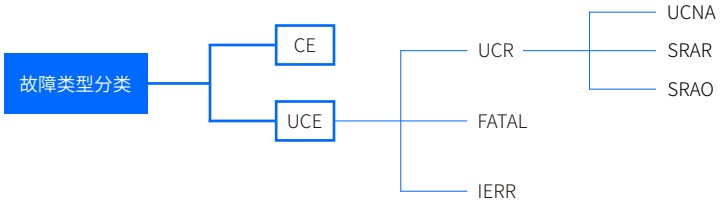


图3-1 故障类型分类

从上图可见服务器故障类型可划分为CE类故障和UCE类故障，UCE类故障包括IERR灾难性故障、FATAL致命故障、UCR不可纠正可恢复故障三种，FATAL与UCR同属于MCERR类型的故障会向OS触发MCE中断；UCR故障通常称为non-Fatal类型的UCE，包含UCNA、SRAR、SRAO三类故障。另外从故障场景划分，服务器故障可划分为宕机类故障和非宕机类故障两大类。宕机类故障主要体现在开机过程宕机及运行时宕机两部分，见图3-2。非宕机类故障包括CPU/内存/GPU/存储设备/网络设备/PCIe外插设备的可修复故障及非致命故障统计监测、部件及链路健康状态监测。另外基础硬件的监测是衡量服务器健康状态的关键指标，包括供电温度指标异常监测，主板风扇异常监测等，见图3-3。

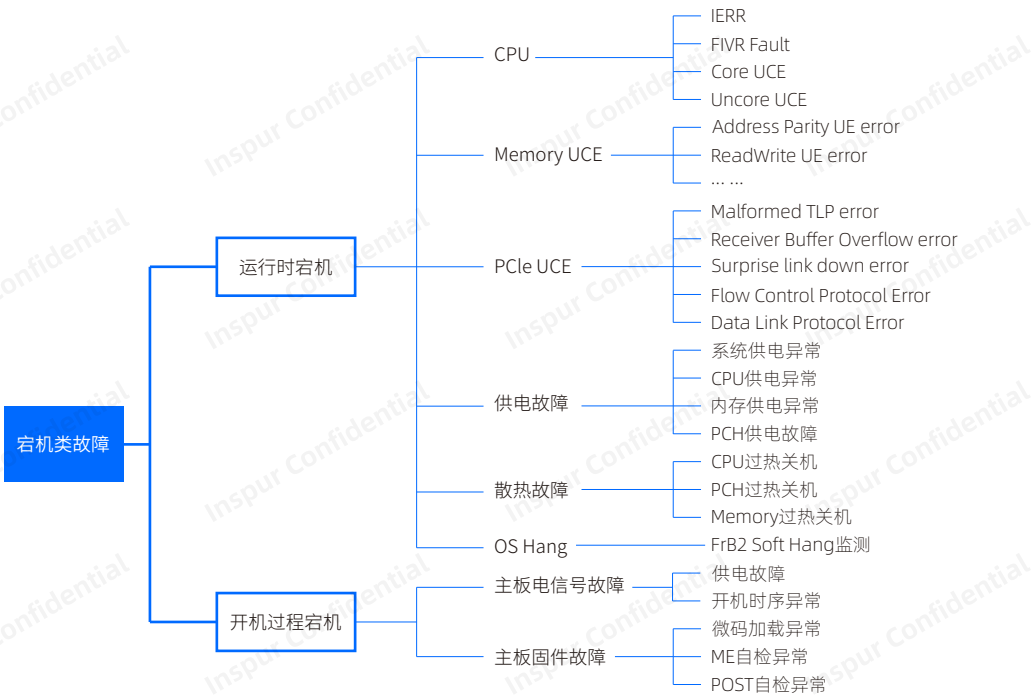


图3-2 宕机类故障分类

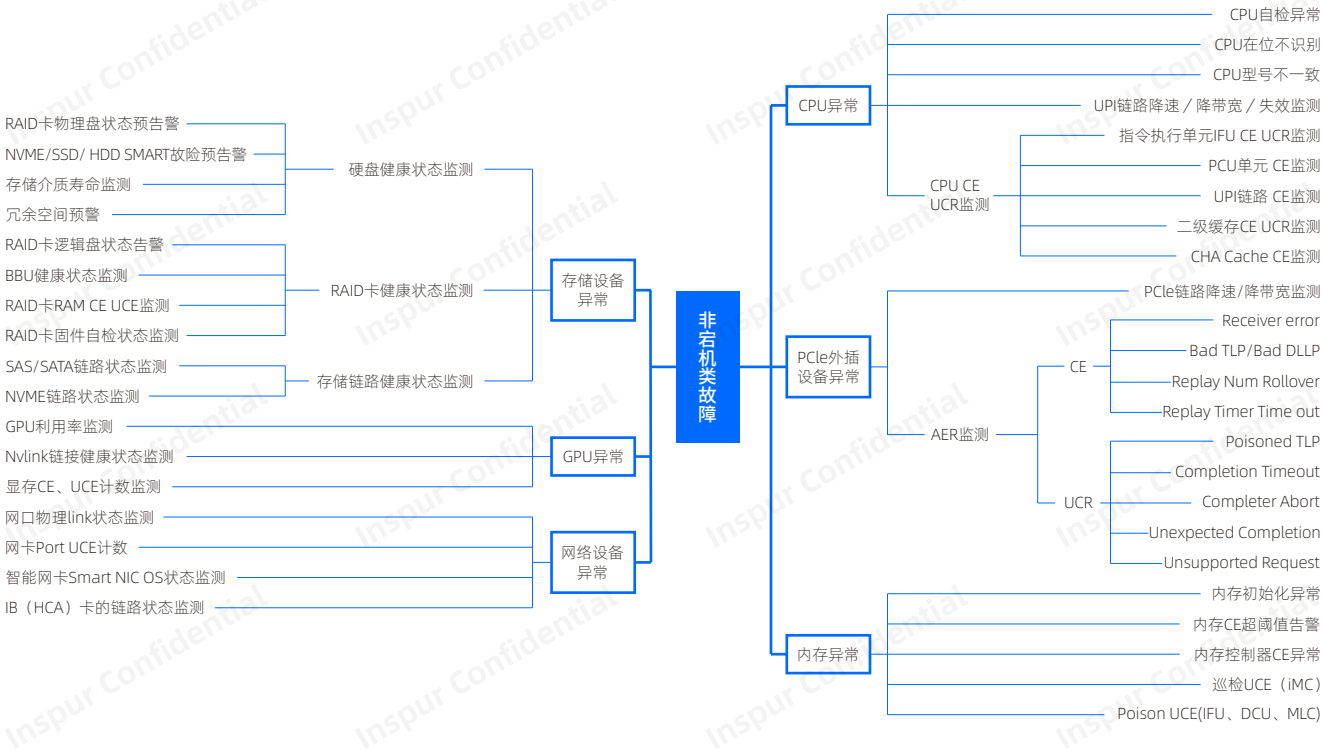


图3-3 非宕机类故障分类

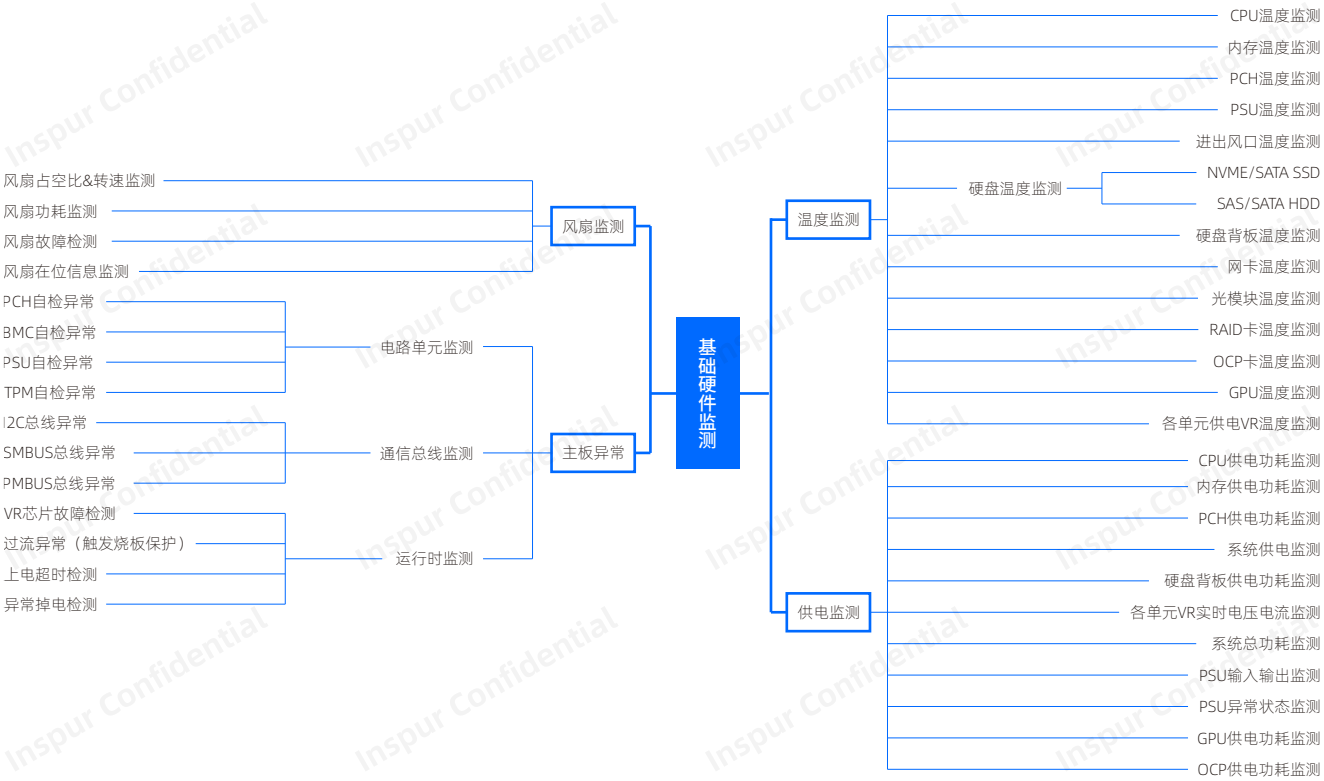


图3-4 基础硬件监测

当启动服务器后，服务器硬件和底层固件可能出现各种错误：

在OS运行过程中，随机的CE错误在硬件底层即可完成修复，通过冗余资源替换故障区域，降低运行速率、请求重传等方式修复故障，维持系统正常运行；不可预期的CE风暴会对设备性能造成持续的影响，需要对造成CE爆发的部件进行风暴中断抑制，并进行计划停机更换修复；小概率的UCE故障中，致命的UCE会导致kernel panic服务器宕机重启，非致命的UCR在系统修复的情况下OS还可以保持继续运行，例如 POST 过程内存 UCE 修复、CPU Core 故障隔离、UPI/PCIe总线链路问题降带宽、OS运行过程中内存Poison UCE Recovery修复等；灾难性的IERR故障会直接导致服务器宕机，依赖ISFDS诊断机制找出导致故障的部件进行更换维护。另外，服务器开机阶段在固件层出现问题，PFR(Platform Firmware Resilience)机制会探测到相关的异常，使用Recover动作或双镜像等措施进行开机故障即时修复。

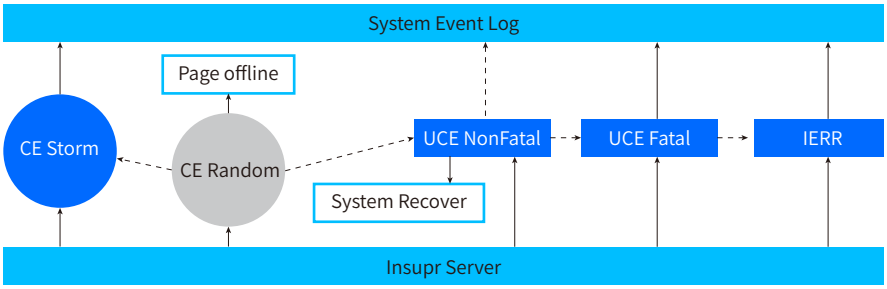


图3-5

3.2 服务器故障处理单元

浪潮服务器故障处理单元以ISBMC为主中心构建，向外部各单元延伸拓展，从基础的供电监测、温度监测、散热监测，到承载业务的关键部件CPU监测、内存监测、存储设备监测、PCIe设备监测、主板监测，实现全方位无死角的带外故障数据的实时收集、分析和诊断，并将诊断结果推送至System Event Log，同时呈现在服务器前面板故障指示灯及BMC Web界面。 另外以CPU为次中心构建故障诊断辅助系统，开机过程中CPU运行ISBIOS在带内收集CPU、内存、PCIe等设备的故障信息和资源拓扑信息，并传递给ISBMC用于辅助诊断；同时OS运行阶段ISBMC实时监测CPU CATERR/ErrorPin 信号，在 IERR/UCE/UCR/CE 发生时使用 PECI/JTAG 接口及时获取 CPU 记录的故障寄存器信息，ISBIOS可以搜集突发的异常故障信息经过CMCI、CSMI、MCE、MSMI、SMI、SCI、NMI等方式上报到ISBMC或操作系统。

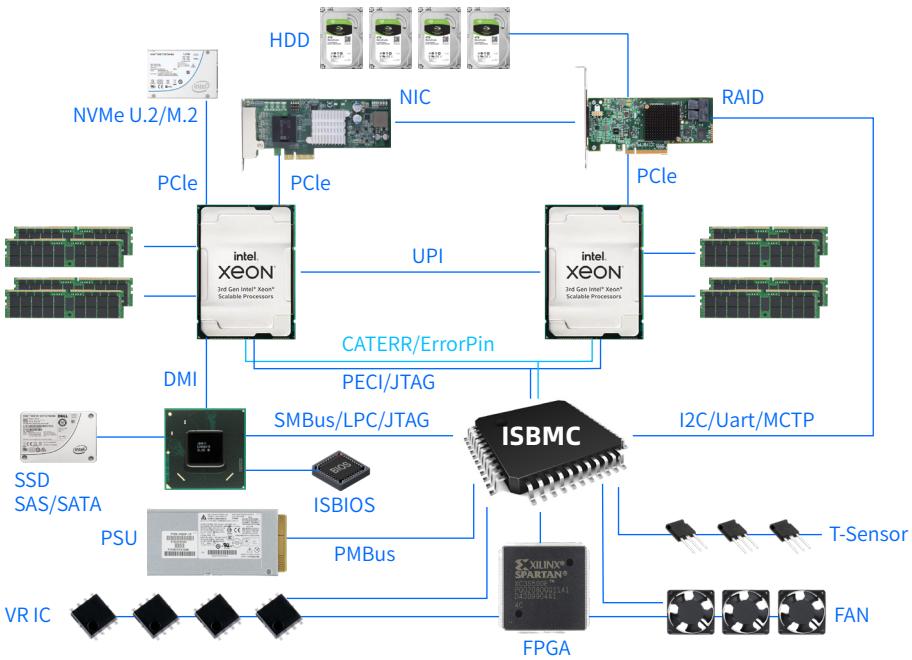


图3-6

上图列出了硬件连接拓扑示意图，其中，关键故障处理的组件有：

ISBMC: 故障检测、定位、上报的核心处理单元，提供ISFDS技术硬件层的算力算法实现。

ISBIOS: 故障隔离、预警、修复的底层代码实现，提供ISFDS平台功能实现的固件支撑。

CPU: Intel至强CPU提供了增强的RAS功能，增强了CPU内部子模块、内存、 PCIe 设备的硬件RAS特性，提供了健全的故障检测和和修复的底层硬件支持。

主板: Inspur自研主板具备支故障检测和预处理能力，供电VR发生故障立刻上报，即时硬件异常故障保护机制，过流的情况下会主动触发烧板保护功能，避免局部故障扩大化；另外还设计有上电超时、异常掉电等硬件故障检测功能。

3.3 服务器故障处理流程

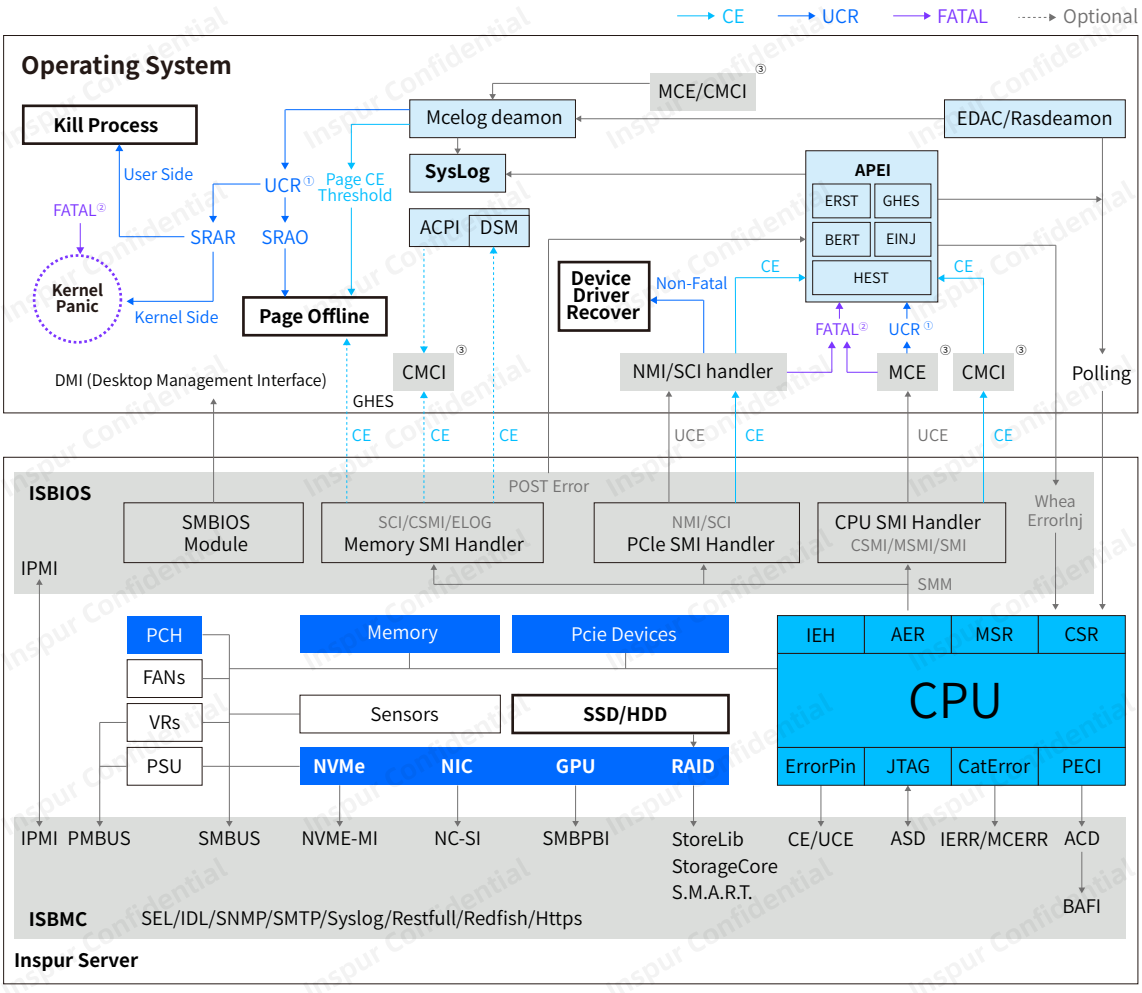


图3-7 服务器故障处理流程

如图3-7所示，服务器硬件的故障ISBMC方面可由经过各种接口协议对各PCIe部件进行主动抓取，使用CPU的ErrorPin、CatError对故障类型进行监测，使用CPU的PECI接口对CPU寄存器进行ACD收集然后进行BAFI解析，使用CPU的JTAG接口进行在线ASD调试；同时ISBMC支持SEL/IDL/SNMP/SMTP/Syslog/Restfull/Redfish/Https等各类接口推送形式将接收到的预警和故障进行上报。

ISBIOS方面可经由CPU触发各类故障的SMI中断由对应SMI Handle处理后上报给OS相应的Driver进行故障处理，同时使用IPMI上报给ISBMC；内存CE及SRAO故障使用Pageoffline机制进行修复，内存SRAR类型的故障发生在用户侧进程中可以进行进程终止修复，发生在Kernel侧则会触发Kernel Panic，CPU、Memory、PCIe产生的FATAL类型的故障同样也会触发Kernel Panic；ISBIOS会将CE及各类UCE故障记录到APEI的HEST Table供OS检索处理记入Syslog，另外OS也有RAS处理应用EDAC、Rasdeamon等可以主动抓取CPU和各部件的故障。图中具体名词释义见术语表2-1。

3.4 支持产品

功能	型号
ISFDS V2.0	NF5280M5/NF5180M5/NF8260M5/NF8480M5；
ISFDS V3.0	NF5280M6/NF5180M6/NF5260M6/NF5270M6/NF5266M6/NF5466M6/NF5468M6/NF5488M6/NF5688M6/i24M6/i48M6/SN5160FM6/SN5264FM6/NF8260M6/NF8480M6；

*具体机型实际实现功能见官方产品说明

4 IS-FDS关键技术

ISFDS整合了硬件、ISBIOS、ISBMC以及操作系统的故障处理技术，形成一整套故障处理系统，涵盖了故障检测、故障预警、故障修复、故障隔离、故障定位、故障上报，六大主要关键技术。实现了服务器各部件的实时检测及智能预警、整机性能及健康状态持续监测、系统故障全时修复与隔离、宕机故障快速诊断与精准定位；并且以ISMD、ISPIM实现带内外监控整合能力，达成了智能化运维在数据中心的进一步推进。

4.1 故障实时检测与隔离

服务器开机ISBIOS POST过程中首先BIST（Build in self test）组件会进行CPU内部各子模块的自检检测，然后进行内存和PCIe外设的初始化及故障检测，检测到Core或Dimm存在故障会隔离掉继续启动，避免单一非必要部件故障影响整机系统的运行；OS运行阶段会对内存进行实时的巡检检测，ISBIOS会主动告知OS异常的内存Page进行offline隔离；供电设计实现了主PSU故障主动隔离并启用备用PSU，主板设计监测局部过流异常及时隔离故障区域，避免硬件损坏扩大化；另外ISBMC担负整机所有的硬件及固件的故障全时的巡检监测，实时掌控各部件供电、温度情况及各种异常故障输出状态，对服务器硬件的健康状态进行整体评估。

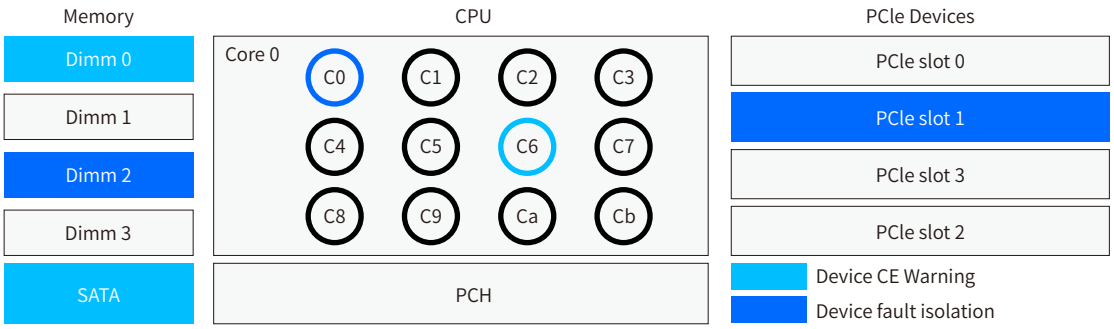


图4-1

4.2 故障精准定位与上报

ISBMC与ISBIOS直接进行灾难性故障IERR处理的流程，在灾难性故障IERR发生后第一时间感知CPU发生故障的时刻，使用优化增强的PECI交互驱动进行记录故障关键寄存器的及时抓取；ISBMC与ISBIOS在HOST系统资源拓扑构建、故障日志的收集、日志分析过程、日志上报途径(SDR、SMTP、SNMP-trap等)过程都进行了全面的代码重构，及过程可视化呈现；IERR诊断使用浪潮ISFDS故障诊断专家规则库进行故障日志的在线分析及故障部件的精准定位，并且在ISBMC诊断失败后启用ISBIOS自诊断机制，提高IERR故障诊断的准确率。

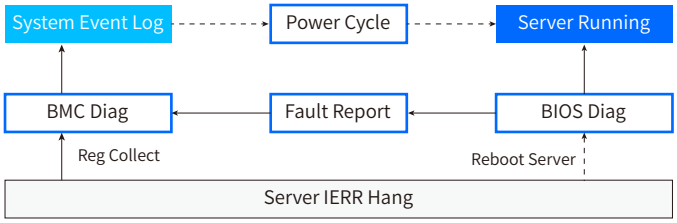


图4-2

4.3 故障智能预警与修复

ISFDS故障预警功能，采用浪潮服务器海量客户的非宕机类故障日志汇总，基于浪潮云海Insight大数据平台进行数据挖掘分析；学习数据行为模式生成预警规则，落地到浪潮故障诊断专家规则库，再由ISBMC、ISPIM进行规则应用，对服务器内所有部件进行全生命周期的运行状态进行跟踪监测，进行实时数据的行为模式识别，识别潜在隐患部件及高风险部件进行提前预警，降低服务器在高负荷运行状态下的突然失效。

ISFDS具备对于某些偶发的非致命的UCE故障的基础修复能力，做到故障的即时恢复，降低演变成致命UCE导致宕机的发生。例如CPU DCU巡检Parity故障修复、内存Poison UCE 进行Recovery、内存读写CE及巡检CE/UCE的实时修复、内存读写CE进行softPPR、内存SMbus故障自修复、PCIe UCR故障Recovery等。

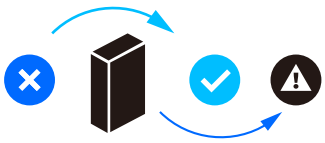


图4-3

4.4 为浪潮服务器定制的带内外故障监管系统

浪潮服务器带内管理驱动ISMD采用C语言编程，通过读取系统文件、系统函数、系统工具等手段，从监控、性能、日志等方面进行全面的监控，性能监控支持秒级监控，日志支持增量采集，依赖系统最小化，安装包10M，单核cpu利用率<10%，内存占用<100M.。

浪潮物理基础设施管理平台ISPIM基于30000+专家经验，建立了492个故障模型，实现了快速故障根因诊断，输出解决方案。该平台通过收集ISBMC带外日志和ISMD带内日志进行汇总后进行诊断，实现故障现场日志场景完整还原，完成故障数据全方位的收集分析处理，实现故障监控覆盖度最大化，故障诊断准确率最大化；

主动巡检，含492个故障模型、30，000＋专家经验，快速诊断故障根因，自动提供解决方案

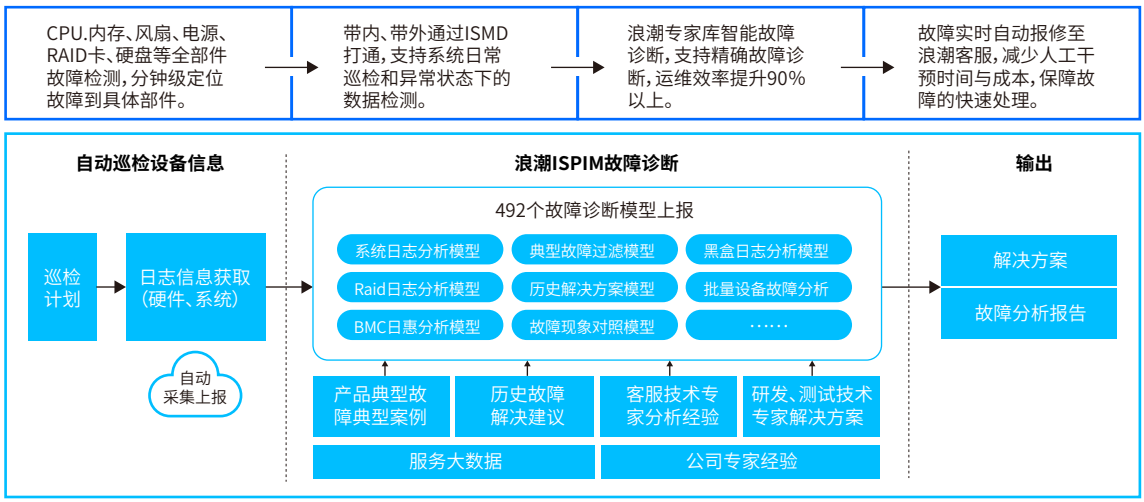


图4-4

5 IS-FDS功能简介

ISFDS功能依赖浪潮服务器整机系统、功能部件及主板硬件的RAS设计实现，在各机型的硬件基础设计及固件底层设计层面实现强壮的可靠性、可用性、可维护性；具体功能设计实现涉及CPU故障检测与处理、内存故障检测与处理、PCIe通用部件故障检测与处理、主板故障检测与处理四大主要部分。

5.1 CPU 故障检测与处理

以intel为例，CPU由Core Uncore两部分构成，Core由指令预取单元（IFU）、数据缓存单元（DCU）、数据传输缓冲单元（DTLB）、二级缓存单元（MLC）四部分构成；Uncore部分由CHA、M2M、iMC、Intel ®UPI、FIVR、PCU、UBOX、M2IOSF、IIO等单元构成；CPU运行过程中每个单元发生故障都会详细记录在每个单元所属的MCA Bank当中，并且将故障现场的故障数据记录存储在每个单元相关的掉电易失CSR寄存器（Control and Status Registers）中。Core部分会记录CPU本体或内存的故障，Uncore部分会记录各单元对应的CPU外围部件的故障，如内存、主板、PCIe部件等。

ISBMC做到了对CPU记录故障的关键寄存器进行增强抓取，对CSR及MCA Bank记录数据的深度关联解析，精确锁定真实故障源，在发生故障的现场快速精准定位到导致该故障发生的部件。

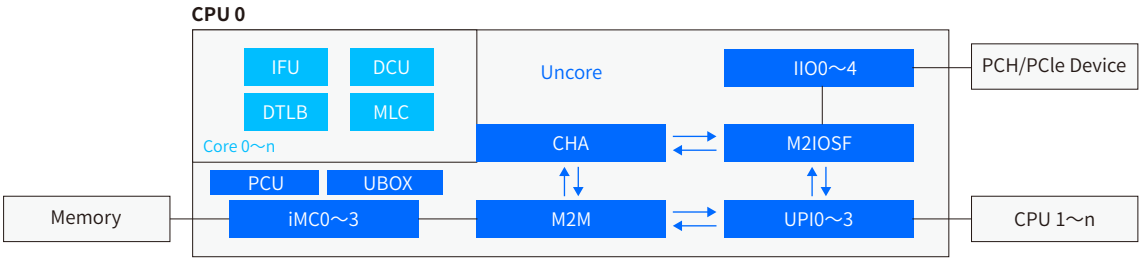


图5-1 CPU寄存器拓扑

5.2 内存故障检测与处理

随着服务器支持的内存通道数量、单体内存容量以及内存运行频率的不断提升， 内存错误发生的概率也随之升高，为避免内存故障导致的宕机频发，浪潮服务器ISBIOS固件RAS设计启用了大量的内存故障防护机制，SDDC、PostPPR、PCLS、内存增强压测及修复 (AdvancedMemoryTest)、内存Poison UCE Recovery、读写CE及巡检CE/UCE的实时修复、内存UCE进行故障Dimm隔离等；尽管如此，服务器在长久运行或大负荷运行下也会发生一些不可预期的内存故障，列举常见的内存故障如下：

常见的内存故障	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

表5-1常见内存故障列表

ISFDS可以准确识别内存故障的来源是CPU内的内存控制模块故障还是实际内存条Dimm故障，并且支持各种内存工作模式下的故障地址解析，精确定位故障 Dimm位置，并且支持在线地址解析。另外，对于Intel 傲腾持久内存PMEM的故障定位进行了专项优化支持，诊断规则覆盖各类内存导致的疑难宕机案例。

5.3 PCIe通用部件故障检测与处理

PCIe通用部件的故障一般由AER机制记录上报，AER故障有如下分类，分别对应Corrected、Non-Fatal、Fatal：

CE	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

表5-2 PCIe AER故障列表

CE类的故障一般由链路层修复；UCR类的故障上报到OS进行Recovery处理；致命的UCE类型的故障会引起系统宕机，一部分直接由AER机制进行上报定位，另外一部分造成灾难性宕机的PCIe故障会由ISFDS故障处理机制进行诊断分析，将IIO模块记录的详细AER信息与CPU CSR及MCA Bank数据融合，使用浪潮故障诊断专家规则，结合构建好的PCIe资源拓扑，精确定位到发生故障的PCIe slot上的外插部件。

5.3.1 硬盘

浪潮ISFDS技术可以实现硬盘红灯告警、博通RAID卡Media error记录、SSD擦写寿命监控等功能。

针对NVME盘可获取在位状态、槽位号、厂商型号、容量、厂商序列号、带宽速率等信息，支持剩余空间低于阈值告警、超温告警、Read Only模式告警、易失性内存备份系统失效告警和Thermal Sensor读取失败等告警功能。

5.3.2 GPU

浪潮ISFDS技术可以实现GPU卡的超温告警，ECC故障告警，PCIe CE/UCE错误上报等功能。通过读取GPU卡自身的寄存器信息，可以获取温度告警阈值，当系统检测到板卡上的芯片温度超过阈值时，会自动触发告警。当SRAM或者DRAM出现ECC错误时，系统会对其数量进行计数统计，当超过允许的范围后，会将该信息进行显示，提示用户及时更换。当PCIe CE数量超过阈值或者出现UCE时，系统能够打印出错的总线位置，方便运维人员快速定位和处理。

5.3.3 存储卡

浪潮ISFDS技术可以实现存储卡本体故障告警、掉盘告警、超温告警等功能，也可以支持获取硬盘预测故障信息、SSD寿命监控等功能。

5.3.4 网卡

随着服务器性能的提升，数据传输的能力要求也越来越高，网卡作为数据传出的通道，对网卡状态的监控显得尤为重要，浪潮ISFDS技术可以实现对网卡静态信息和动态信息的监控，可以实时监控网卡的状态。

静态信息监控，可以在BMC界面直观的监控网卡支持的NCSI版本，FW名称版本，MAC地址等静态信息，便于对网卡的运维管理。

动态信息进行监控，可以在BMC界面直观的监控网卡每个网口的link状态，网卡芯片的温度，网口搭配光模块的温度和光模块电流超阈值的告警等动态信息，可以针对出现的告警信息进行相应的问题排查。

动态信息进行监控，可以在BMC界面直观的监控网卡每个网口的link状态，网卡芯片的温度，网口搭配光模块的温度和光模块电流超阈值的告警等动态信息，可以针对出现的告警信息进行相应的问题排查。

如果插的是智能网卡，除了可以在BMC界面监控静态和动态信息，还可以提供SoC、FPGA的状态信息，收集相关的日志。并可以进行SoC系统的断电、上电等操作。

5.4 主板故障检测与处理

5.4.1 服务器故障指示灯

服务器前面板设有整机故障提示指示灯，以NF5280M6为例，详细定义如下：

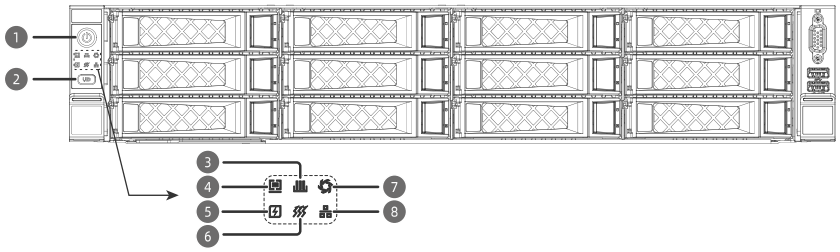


图5-2 NF5280M6前面板指示灯示意图

序号	名称	序号	名称
1	电源开关按键/指示灯	2	UID|BMC RST按键/指示灯
3	内存故障指示灯	4	系统故障指示灯
5	电源故障指示灯	6	系统过热指示灯
7	风扇故障指示灯	8	网络状态指示灯

表5-3 前面板指示灯序号与名称对照表

符号	指示灯和按键	状态说明
	电源开关按键/指示灯	**电源指示灯说明：** ·熄灭：设备未上电。 ·绿色常亮：设备正常上电。 ·橙色常亮：设备待机（Standby）状态。 **电源按键说明：** ·上电状态下长按4s电源按键，强制关机。 **说明：** ·不同OS可能需要根据操作系统界面提示信息关闭操作系统。 ·待机（Standby）状态下短按电源按键，可以进行上电。
UID	UID|BMC RST按键/指示灯	**UID指示灯用于定位待操作的设备：** · 熄灭：设备未被定位。 · 蓝色常亮：设备被定位。 · 蓝色闪亮：设备被远程操作。 **说明：** ·可通过手动按UID按键或者ISBMC远程控制使灯熄灭或灯亮。 ·长按UID按键超过6s复位BMC。
	内存故障指示灯	· 熄灭：设备正常状态。 · 红色闪烁（1Hz）：系统有一般告警。 · 红色常亮：系统有严重告警。
	系统故障指示灯	· 熄灭：设备正常状态。 · 红色闪烁（1Hz）：系统有一般告警。 · 红色常亮：系统有严重告警。
	电源故障指示灯	· 熄灭：设备正常状态。 · 红色闪烁（1Hz）：系统有一般告警。 · 红色常亮：系统有严重告警。
	系统过热指示灯	· 熄灭：设备正常状态。 · 红色闪烁（1Hz）：系统有一般告警。 · 红色常亮：系统有严重告警。
	风扇故障指示灯	· 熄灭：设备正常状态。 · 红色闪烁（1Hz）：系统有一般告警。 · 红色常亮：系统有严重告警。
	网络状态指示灯	·熄灭：没有网络连接或处于异常状态。 ·绿色闪烁：数据传输中。 **说明：** ·仅指示板载网络工作状态。

表5-4 前面板指示灯说明标识对照表

5.4.2 主板VR故障检测预处理

主板VR的故障检测及预处理涉及CPU、内存、PCH芯片供电状态监测，同时可实现对风扇、硬盘、GPU及OCP外插卡等部件供电状态的实时监控（具体是BMC通过I2C总线访问相应的VR、EFUSE、CPLD单元，读取VR或EFUSE内部的工作状态寄存器的故障位或是CPLD的GPIO的故障状态，以此来判断故障类型及具体原因）。以下是以NF5280M6主板为例的供电故障检测诊断示意图，通过ISBMC对以上主板功能单元及部件的供电异常进行判断，能快速定位供电故障原因。

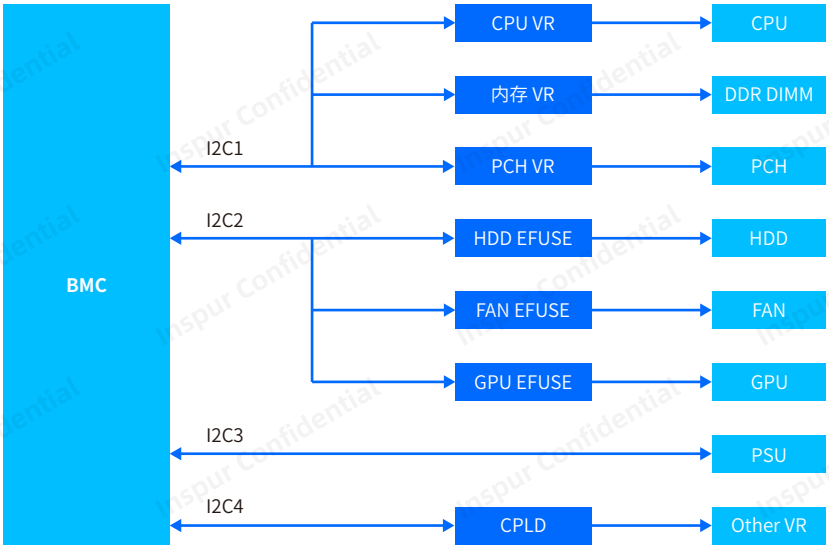


图5-3 常见服务器VR & Efuse错误定位拓扑

5.4.3 异常掉电问题处理

主板支持板卡电源的异常监控及预处理功能，在主板运行过程中，当出现异常掉电时，主板会记录异常掉电原因，并及时关闭板卡电源，避免出现烧板问题。

当服务器出现异常掉电时，查看BMC IDL日志中会打印PWR_Drop等日志记录。

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

5.4.4 上电超时问题处理

当主板各电源模块正常时，按电源按键后主板应正常上电开机；但是当主板某一电源模块存在异常时，会存在无法正常上电开机的问题。该故障发生时BMC IDL日志中会存在PWR_On_TMOUT等日志记录。

Power Supply PWR_On_TMOUT | Failure detected | Asserted|

5.4.5 主板防烧板功能设计

主板硬件支持功耗监控，主板12V电流超过设定阈值时，会触发主板的自动断电功能。

当主板某一电路模块发生了损坏引发过流异常，便会触发该防护机制，BMC的IDL日志会记录如下相关日志：

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

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

6 ISBMC故障监测与诊断

ISBMC作为故障检测、定位、上报的核心处理单元，担负着服务器系统日常运行日志的监测记录、系统异常事件的监测记录、系统宕机日志的记录和故障根因分析等重要任务，并实时输出整机系统的健康监测状态。

6.1 系统运行日志记录

6.1.1 开机自检码监测及日志记录

ISBMC web界面支持开机自检代码，界面记录了服务器开关机状态、当前自检代码、当前自检代码描述以及历史自检代码。开机自检代码描述了系统开机自检结果信息，反映了当前自检是否发生具体故障，并采用代码的形式体现，通过当前自检代码和当前自检代码描述定位系统启动的具体故障。

在ISBMC Web页面导航栏中选择“故障诊断>开机自检代码”打开如图6-1所示。

图6-1 开机自检代码web界面

服务器开关机状态：主要检测当前系统的开关机状态。

当前自检代码：采用代码形式表示系统开机各设备部件的具体运行状况。

当前自检代码描述：对当前自检代码的具体描述。

历史自检代码：历史自检代码。

当前自检代码及当前自检代码描述如表6-1所示;另外历史自检代码还记录在inspur_debug.log，日志文件会记录开机时BIOS记录的具体故障码来定位故障发生阶段及故障类型，同时对应的故障会记录到BMC System Event Log，以便遇到开机异常的故障进行故障原因追溯。

当前自检代码	当前自检代码描述	当前自检代码	当前自检代码描述
11	CPU初始化	15	NB初始化
19	SB初始化	2B	MEM初始化读SPD
2C	初始化检测MEM	2F	MEM初始化设定初值
31	内存安装完成	32	CPUPOST -MEM初始化
……	……	……	……

表6-1 开机自检代码参数表

6.1.2 屏幕快照

屏幕快照是ISBMC提供的一项方便系统巡检的功能，用户可以通过Web界面对当前系统的屏幕输出进行截取并保存，在OS唤醒状态及关闭KVM状态下使用手动截屏，随时对系统当前画面进行屏幕截图，当用户需要查看时可以通过网络将文件获取至本地使用图片查看软件浏览屏幕截图，不需要时则删除截图即可。

在ISBMC Web页面导航栏中选择“故障诊断>屏幕截图>手动截屏”，如图6-2所示。

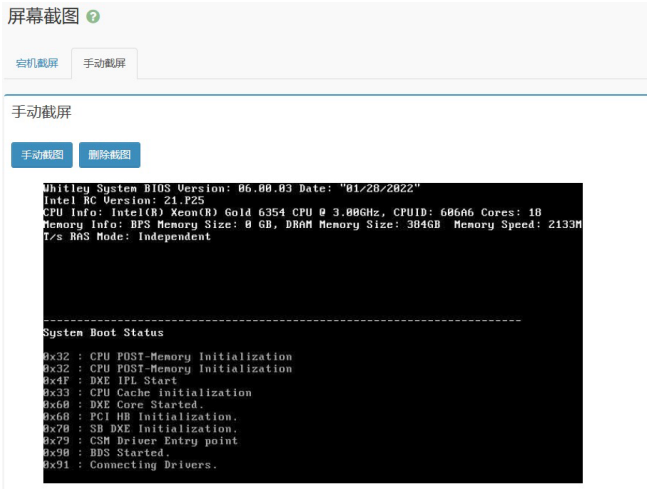


图6-2 手动截屏

6.1.3 Mainteance Log介绍

在导航栏中选择“日志和告警>一键收集日志”下载压缩包dump_0__20000102-0243.tar.gz并解压为onekeylog，Maintenance Log位于文件夹Log内，打开如图6-3所示界面。具体参数见表6-2

```
<182> 2000-01-01T08:20:19.970000+08:00 [Diagnose Lag]【MCAProgressTask】McaTriggerType:9
<182> 2000-01-01T08:20:19.990000+08:00 [Diagnose Log]【MCAProgressTask】Collect Reg Data and Analyse, phaseName:First
<182> 2000-01-01T08:20:19.990000+08:00 [Diagnose Log]【MCAProgressTask】Get register start time:2000-01-01T08:20:19(First)
<182> 2000-01-01108:20:20.370000+08:00 [Diagnose Log]【MCAProgressTask】PciconfigRegLocal Get CSR register(global,csr) data Done,expend 0s
<182> 2000-01-01T08:20:20.560000+08:00 [Diagnose Log]【MCAProgressTask】PciconfigRegLocal Get CSR register(dmi) data Done,expend 0s
<182> 2000-01-01T08:20:27.520000+08:00 [Diagnose Log]【MCAProgressTask】PciConfigReg Get PCIe RootPort register data Done,expend 7s
<182> 2000-01-01T08:20:28.760000+08:00 [Diagnose Log]【MCAProgressTask】PciConfigReg Get PCIe Device register data Done,expend 1s
<182> 2000-01-01T08:20:29.060000+08:00 [Diagnose Log]【MCAProgressTask】PciConfigRegLocal Get CSR register(iio) data Done,expend 1s
<182> 2000-01-01T08:20:32.730000+08:00 [Diagnose Log]【MCAProgressTask】Get Msr register data Done,expend 3s
```

图6-3 维护日志

维护日志Maintenance.Log主要记录了程序运行过程的重要数据，常用于分析软件的具体执行情况。如图7-4所示，日志记录了Oem命令触发收集register data的开始时间、收集Csr 和PCIe RootPort register data的花费时间以及收集register data的结束时间。

参数	描述
2000-01-01T08:20:19.990000+08:00	系统记录日志的时间
Get Msr register data Done, expend 3s	程序记录在日志的数据

表6-2 维护日志参数表

6.2 系统宕机日志记录

6.2.1 宕机截屏及宕机录像

当服务器操作系统发生宕机时，宕机截屏可以获取系统宕机的最后一屏画面并以指定的格式保存在ISBMC的存储空间内。用户发现系统宕机后，可以通过网络登录至ISBMC内查看宕机屏幕，进而对故障进行快速定位和分析。

在导航栏中选择“故障诊断>屏幕截图>宕机截屏”。

如图6-4所示，在系统宕机时获取系统宕机的最后一屏画面。

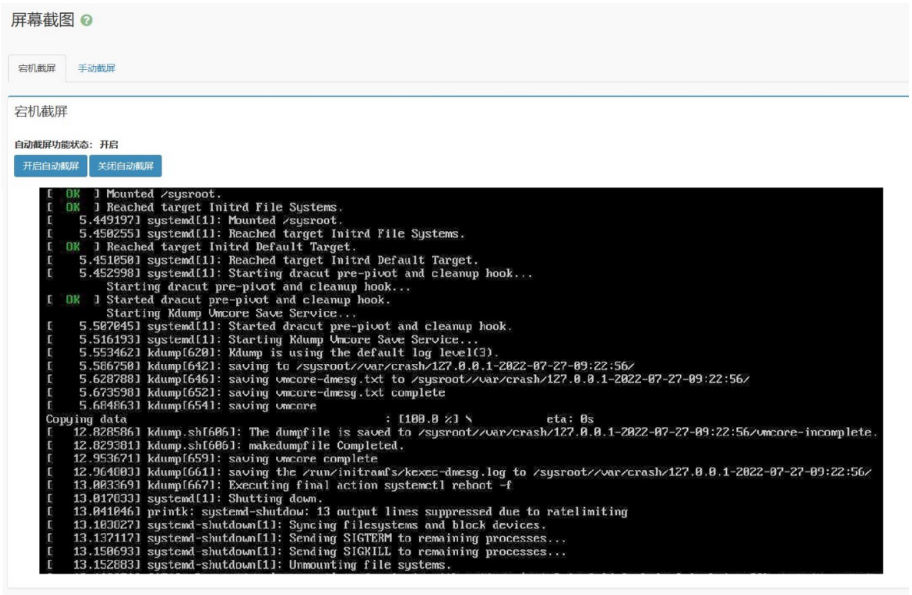


图6-4 系统宕机截屏

开启宕机录像功能，当服务器操作系统触发宕机时，系统会自动录制一段宕机前的视频并以压缩的格式保存至ISBMC存储空间。用户可以通过“一键收集日志”下载录制的宕机视频（.dat 格式），并在“解析视频”处将ISBMC下载到本地的.dat文件转为.avi文件，然后在“宕机视频”显示录像，技术人员可以通过录制的视频信息辅助定位系统故障。该功能必须先关闭KVM服务才会生效。

在导航栏中选择“故障诊断>屏幕录像>宕机录像”，打开如图6-5所示界面。

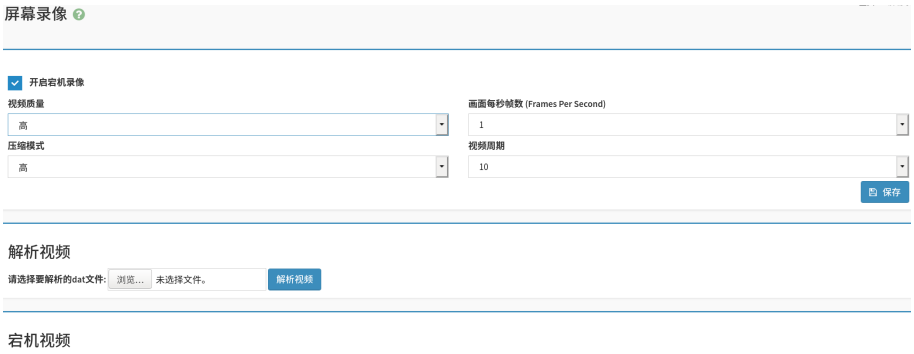


图6-5 宕机录像web界面

6.2.2 日志收集下载界面

在ISBMC Web页面导航栏中选择“日志和告警>一键收集日志”下载压缩包dump_0__20000102-024.tar.gz并解压为onekeylog，日志文件均位于Log文件夹，界面如图6-6所示，参数见表6-3。

图6-6 日志收集界面

日志收集下载路径	信息项	用途
Onekeylog/log/InspurCpuRegisterRawData.json	CPU寄存器	记录获取寄存器数据的时间、触发方式、CPU的类型、CPU寄存器的数据等。
Onekeylog/log/InspurIerrAnalyResultReport.json	故障诊断解析日志	记录寄存器解析结果、信息采集时间、CPU类型、收集诊断数据的方式等。
Onekeylog/log/AnalyProcess.log	故障诊断分析流程日志	记录IERR故障诊断的具体过程，及诊断分析结果（诊断结果会推送至SEL日志）。
Onekeylog/log/audit.log	审计日志	记录用户登录、注销、用户管理、固件更新和恢复等。
Onekeylog/log/idl.log	IDL日志	记录实体部件的事件描述并显示错误等级。
Onekeylog/log/inspur_debug.log	调试日志	存储调试过程的相关信息并显示信息的等级。
Onekeylog/log/maintenance.log	维护日志	记录用户需求或技术人员调试的重要信息。
Onekeylog/log/selelist.csv	SEL日志	记录系统内传感器名称，传感器类型、触发事件的详细描述。

表6-3 日志文件参数表

6.2.3 宕机诊断案例

服务器发生IERR灾难性故障后，ISBMC会立刻执行IERR故障精准定位流程，故障的详细诊断报告会记录在“故障诊断分析流程日志”中，用户可以查看发生故障的精确时间、发生故障的模块及故障类型、故障现象描述、导致故障的具体设备、故障定位的详细判据以及处理建议等，如图6-7所示，另外对于疑难复杂宕机案例ISBMC还支持ASD、ACD、BAFI等技术实现疑难案例的快速分析及诊断定位根因。

图6-7展示了由CPU0访问PCIe设备MMIO资源异常，发生的Tor Timeout导致3-Strick Timeout，进一步引发了CPU IERR故障的发生。由图例可以看到，故障定位先找到发生故障的CPU CPU0，再找到记录故障现场数据的MCA Bank MC10，由该Bank解析出详细的故障类型 Tor_Timeout，由该Bank记录的地址追溯到使用该MMIO地址空间的PCIe设备 Mellanox ConnectX-5网卡，并详细打印了该设备名称、BDF、槽位信息等。

```
[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]",
                                       } ]
```

图6-7 故障诊断分析流程日志

6.2.4 非宕机监测案例

ISBMC可以实现对NVME SSD常见SMART故障的监测，可以做到剩余（冗余）空间异常、盘体超温、只读模式、易失性内存失效、预故障提醒，详细见下表6-4。

SMART字段	ISBMC记录	建议动作
NVME SSD剩余空间低于阈值告警	[DiagNVME]:SN:S63SNE0R509578 , available spare space has fallen below the threshold!	此告警发生时，说明NVME SSD的冗余空间不足， 已达到冗余空间的阈值，建议更换全新的NVME SSD
NVME SSD温度超过阈值告警	[DiagNVME]:SN:S63SNE0R509578, Tempperature is above an over temperature threshold or below an under temperature threshold!	此告警发生时，说明服务器整机或机房散热异常， 建议提升系统风扇转速或降低机房环境温度
NVME SSD系统可靠性降级	[DiagNVME]:SN:S63SNE0R509578, NVM Subsysterm reliablility has been degraded!	若是存在温度超标，建议检查散热情况； 非超温情况，建议进行换盘操作
NVME SSD介质为只读模式告警	[Diag NVME]:SN:S63SNE0R509578, The media has been placed in read only mode!	此告警发生时，说明NVME SSD进入“只读”模式， 无法进行数据写入，避免发生数据丢失的风险， 请尽快更换全新的NVME SSD
NVME SSD易失性内存备份系统失效告警	[Diag NVME]:SN:S63SNE0R509578, The volatile memory backup device has failed!	此告警发生时，说明NVME SSD内部DRAM器件损坏， 盘无法正常工作，请尽快更换全新的NVME SSD
NVMe SSD PDLU寿命监测（Percentage Drive Life Used）超过阈值进行Warning级别告警	[DiagNVME]:SN:S63SNE0R509578, life used warning level alert!	此告警发生时，说明NVME SSD的寿命将要耗尽， 请尽快更换全新的NVME SSD。
	[DiagNVME]:SN:S63SNE0R509578, life used critical level alert!	
NVME SSD 读取温度sensor失败	[DiagNVME]:SN:S63SNE0R509578, Read temp sensor failed assert!	此告警发生时，说明NVME SSD的温度传感器发生异常， 建议更换全新的NVME SSD。

表6-4

6.3 系统事件日志

通过“系统事件日志”界面的功能，用户可以查看ISBMC系统事件日志，下载系统事件日志和清除系统事件日志。系统事件日志特性如下：

（1） 最多支持3639个条目。

（2） 支持人性化日志管理：可视化、筛选、下载、清空。

（3） 支持本地存储和归档。

（4） 支持循环模式。当SEL已满时，旧日志将被丢弃，新日志被保留。

（5） 操作清除SEL时，1条“SEL被清除”的日志将被记录在SEL中。

（6） 支持通过Web或IPMI CMD导出SEL。

（7） 支持通过SNMP Trap、Syslog通知事件至远程客户端。

6.3.1 系统事件记录

在ISBMC Web页面导航栏中选择“日志和告警>系统事件日志”，打开如图6-8所示界面。参数说明见表6-5，日志操作说明见表6-6。

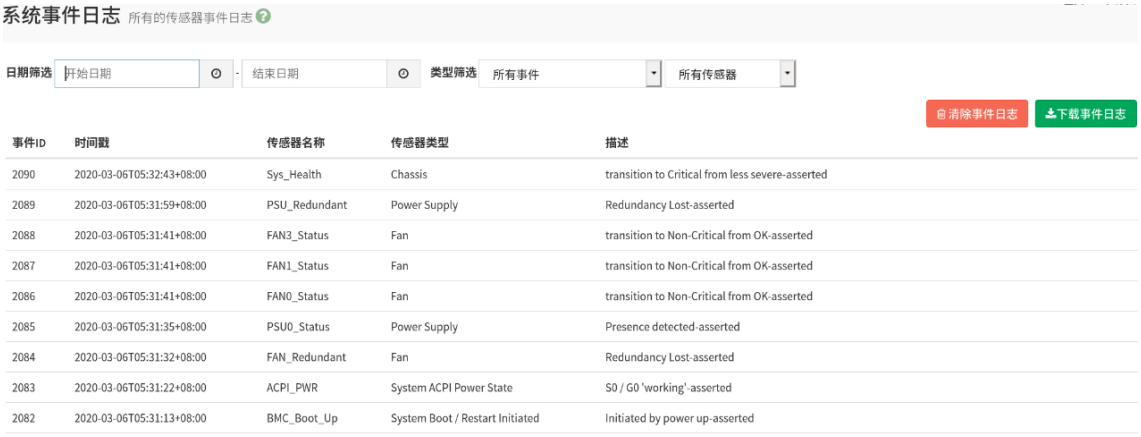


图6-8 系统事件web界面

参数	描述
事件ID	SEL中的事件ID
时间戳	事件日志生成时间
传感器名称	传感器名称，用户可通过ipmitool sdr elist 查看设备所有传感器名称
传感器类型	IPMI 2.0中定义的传感器类型： Temperature //温度传感器 Voltage //电压传感器 Processor //CPU状态传感器 Power Unit //PSU状态传感器 Memory //内存状态传感器 Drive Slot //硬盘状态传感器 Critical Interrupt //Pcie状态传感器
描述	事件详细信息

表6-5 系统事件日志参数表

参数	描述
过滤	选择事件类型、传感器和起止日期进行过滤搜索。 **动作：** 您可以采用过滤器选项（事件类型、传感器名称、起止时间）， 查看设备中记录的特定事件。
下载事件日志	点击该按钮可下载日志到本地
清除事件日志	点击该按钮将删除所有现有传感器日志记录

表6-6 日志操作说明表

6.3.2 故障上报

ISBMC支持实时监测系统告警事件，并通过SNMP（Simple Network Management Protocol）TRAP、邮箱、syslog等方式上报至远程接收服务器。

通过“SNMP TRAP设置”界面的功能，用户可以

（1）启用SNMP TRAP

（2）设置告警策略

在ISBMC Web页面导航栏中选择“日志和告警>SNMP TRAP”，打开如图7-12和图7-13所示界面。

图6-9 SNMP TRAP web界面

勾选启用 SNMP TRAP展开页面，SNMP TRAP支持TRAP版本选择，默认版本号V1，选择V3版本时需要增加用户名、认证密码、加密协议以及加密密码。支持根据告警事件严重性级别进行上报过滤。Trap消息会携带主机标识符，主机标识可指定主机名、单板序列号、产品资产标签中任意一个。

图6-10 告警策略web界面

告警策略支持设置4个syslog服务器的IP为目的地、端口，点击保存。支持对接收目标发送测试信息。

通过“邮箱告警”界面的功能，用户可以

（1）启用或关闭SMTP邮件告警。

（2）设置接收告警的邮件地址。

在导航栏中选择“日志和告警>邮箱告警”，打开如图6-11和图6-12所示界面。

图6-11 邮箱告警web界面

勾选启动SMTP邮件告警展开页面，SMTP支持选择SMTP服务器地址、SMTP服务器端口、SMTP服务器安全端口、是否启用发件人身份证、发件人电子邮件ID、发件人用户名、发件人密码、是否启用SMTP SSLTLS、是否启用SMTP STARTTLS、邮件主题、主题附加、告警发送级别等信息。

图6-12 接收告警邮件地址web界面

接收告警的邮件地址最多支持4个接收目标，每个接收目标均可配置邮件地址以及对邮件地址的描述信息，支持对接收目标发送测试信息。

6.3.3 日志设置

BMC支持“日志设置“功能，通过配置Syslog 日志设置，使 BMC 系统向第三方服务器以 Syslog 报文方式发送日志。

在导航栏中选择“日志和告警>日志设置”，打开如图6-13 所示界面，点击“Syslog日志设置”，打开如图6-14所示界面，具体参数见表6-7 和表6-8。

图6-13 日志设置界面

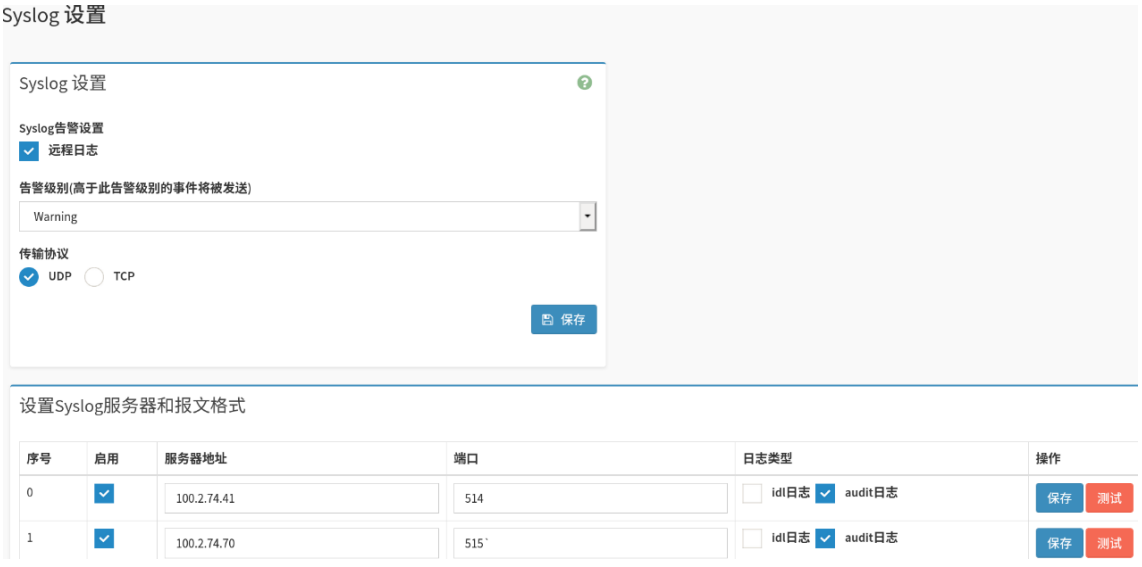


图6-14 Syslog设置

参数	描述
远程日志	Syslog告警日志存储位置，可选择是否存储远程日志。 使用远程日志时，BMC将日志存放在远程Syslog服务器中和本地日志文件中。 不使用远程日志时，仅会存放在本地日志文件中。
告警级别	高于此告警级别的时间将被发送，可选为： Info：发送Info、Warning和Critical级别的告警信息。 Warning：发送Warning，Critical级别的告警信息。 Critical：仅发送Critical级别的告警信息。
传输协议	Syslog报文在BMC系统和Syslog服务器之间传输时使用的传输协 议，可选为： UDP：面向非连接的协议，在正式收发数据前，收发方不建 立连接，直接传输正式的数据。 TCP：面向连接的协议，在正式收发数据前，必须在收发方 建立可靠的连接。

表6-7 Syslog设置

参数	描述
序号	序号。
启用	启用或关闭自动上报Syslog报文功能。
服务器地址	Syslog服务器地址信息。
端口	Syslog服务器端口号。
日志类型	需要使用Syslog报文上报的日志类型。可选为：Idl日志、audit日志中的一项或两项。
操作	保存：保存该Syslog服务器和报文相关信息。测试：测试已设置的Syslog通道是否可以成功发送报文。

表6-8 Syslog服务器和报文格式

6.3.4 IDL日志及处理建议

浪潮故障诊断IDL是浪潮ISBMC独有的日志类型，用于记录BMC设备上基于IPMI传感器的事件历史记录。与系统事件日志信息相比，IDL日志信息提供的信息更多更全，并且每条日志均有相应的处理建议，能更有效的帮助用户进行日志诊断和分析。日志可根据日期、严重性、设备、关键字等方式进行过滤，可执行日志下载和日志清除操作，点击每条日志后侧按钮 可获取关于本条日志的处理建议以及相应的操作步骤。

通过“IDL日志”界面功能，您可以查看此设备上的BMC IDL日志列表。通过点击相应告警事件右侧的处理建议按钮，可以查看对告警事件的处理建议。

在ISBMC Web页面导航栏中选择“日志和告警>IDL日志”，打开如图6-15所示界面。具体参数说明见表6-9，IDL日志操作说明见表6-10。

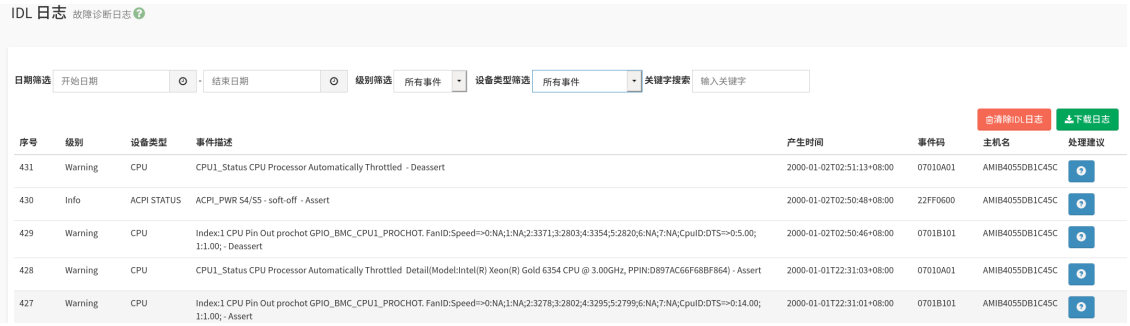


图6-15 IDL日志web界面

参数	描述
序号	IDL日志中的事件ID
级别	事件错误等级，包括信息、告警和严重。
设备类型	FAN、INTRUSION、CPU、PSU、MEMORY、DISK、PCIe、BMC…...
事件描述	告警事件的详细描述
产生时间	IDL日志生成时间
事件码	告警事件的唯一故障编码，长度8字节
主机名	服务器系统主机名
处理建议	针对此告警事件的处理建议

表6-9 IDL日志参数说明表

参数	描述
过滤	选择严重性和起止日期以进行过滤搜索 动作：用户可以使用过滤选项（事件严重性级别、时间、关键字），查看设备中记录的特定事件。
下载日志	下载IDL日志到本地
清除日志	点击清除日志按钮将清除BMC上所有IDL日志信息

表6-10 IDL日志操作说明表

IDL日志支持告警事件处理建议，用户可根据IDL日志的处理建议和相应操作步骤清除告警事件。如图6-16所示。

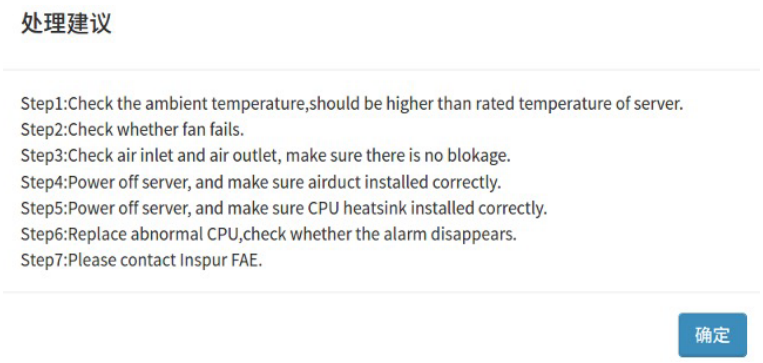


图6-16 IDL日志告警事件处理建议

6.4 整机系统健康状态监测

6.4.1 系统概要

在浏览器登录BMC远程页面之前，地址栏输入https://BMC_IP/#dashboard，并按“Enter”，打开如图6-17所示页面，该页面在未输入用户名密码之前会有一个整机健康状态提示的图标，用户可根据该图标，在未登录之前确定是否该服务器存在异常问题。

在登录BMC远程页面后，通过主页“系统概要”界面，用户可以查看服务器信息、服务器运行状况信息、固件版本信息、在线用户信息等，了解整机系统的健康状态。如图6-18所示。具体参数见表6-11。

图6-17 BMC 登录界面

图6-18 系统概要web界面

区域	展示的信息
服务器信息	**提供服务器的基本信息，包括：** 产品类型：服务器的产品类型。 产品名称：服务器的产品名称。 制造商：服务器的制造商。 产品序列：服务器的产品序号。 资产编号：服务器的资产编号。 System UUID：服务器的System UUID 信息。 Device UUID：服务器的Device UUID 信息。 绑定管理接口：服务器的绑定管理口IP地址。
服务器运行状况	**提供服务器的运行状况，包括：** 服务器开关机状态：开机或关机。 UID状态：UID指示灯打开或关闭。 整体状态：服务器整体状态。 处理器：CPU健康状态。 内存：内存健康状态。 硬盘：硬盘健康状态。 风扇健康状态。 网络：网络健康状态。 电源：电源健康状态。 **说明：各模块健康状态可包含为：** 正常/在位 警告 严重 不在位/灯灭
固件版本信息	**固件版本信息，包括：** BMC 版本。 BIOS版本。 ME版本。 PSU版本。 CPLD版本。 **说明：** 因机型差异，此区域显示的固件类型会有所不同。
在线用户信息	**当前登录本BMC Web的用户信息，包括：** 类型：登录类型，如HTTPS、CTL等。 用户名：登录BMC的用户名。 用户权限：登录BMC的用户对应的用户组信息。 IP：登录BMC的用户所在机器IP地址信息。

表6-11 IDL系统概要说明表

6.4.2 Sensor 汇总列表

通过“传感器”界面的功能，用户可以查看当前系统支持的所有传感器的相关信息，并可以通过双击门限传感器界面中的传感器行跳到修改传感器阈值界面进行设置。传感器界面包含门限传感器页签和离散传感器页签。

在ISBMC Web页面导航栏中选择“传感器>门限传感器”， 打开如图6-19界面，具体监控的门限传感器见表6-12，其范围包含但不限于表6-12。参数说明见表6-14。

图6-19 门限传感器web界面

名称	当前值	严重低阈	严重高阈	单位
Inlet_Temp	25	N/A	55	deg_c
Outlet_Temp	30	N/A	N/A	deg_c
CPU0_Temp	Disable	N/A	N/A	deg_c
CPU1_Temp	Disable	N/A	N/A	deg_c
CPU0_NVDIMM_T	Disable	N/A	83	deg_c
CPU1_NVDIMM_T	Disable	N/A	83	deg_c
PCH_Temp	Disable	N/A	107	deg_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_VIN	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

表6-12 门限传感器

在导航栏中选择“传感器>离散传感器”，打开如图6-20界面，具体监控的离散传感器见表6-13，其范围包含但不限于表6-13。参数说明见表6-15。

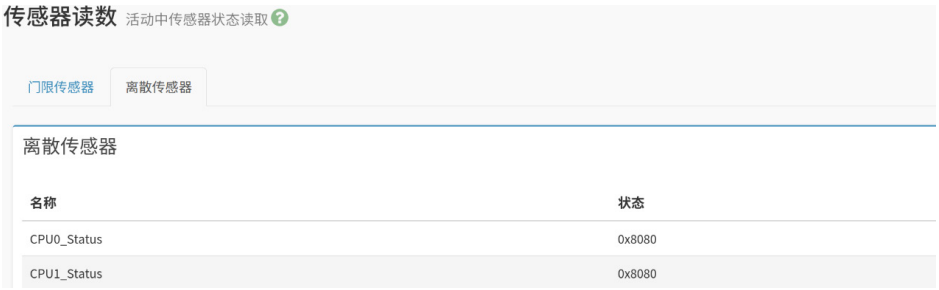


图6-20 离散传感器web界面

名称	状态
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

表6-13 离散传感器

参数	描述	参数	描述
名称	传感器名称	非严重低阈	传感器非严重低阈值
当前值	传感器当前读值	非严重高阈	传感器非严重高阈值
状态	传感器状态	严重高阈	传感器严重高阈值
不可逆低阈值	传感器不可逆低阈值	不可逆高阈	传感器不可逆高阈值
严重低阈	传感器严重低阈值	单位	传感器读值单位

表6-14 门限传感器参数表

参数	描述
名称	传感器名称
状态	传感器状态

表6-15 离散传感器参数表

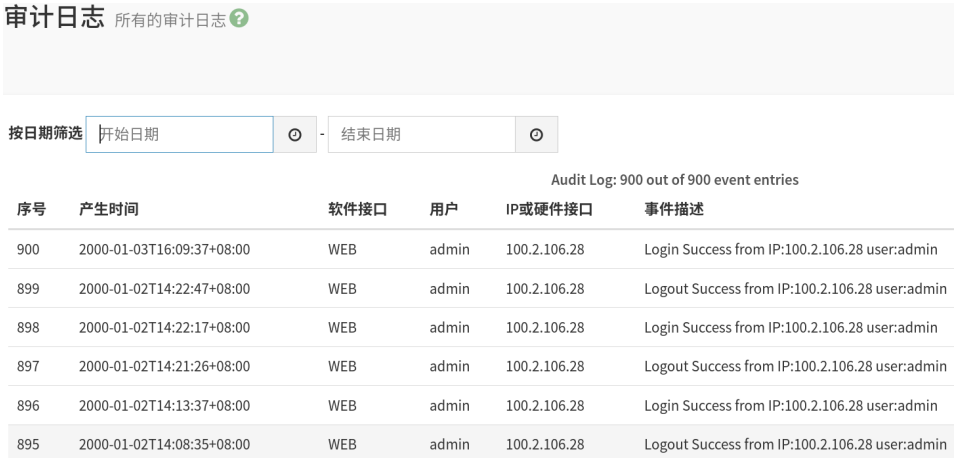
6.4.3 审计日志记录

通过“审计日志”界面的功能，用户可以查看系统的审计日志，BMC审计日志特性如下：

（1）通过SSH、Redfish、IPMI、Web接口登录系统进行管理的关键行为将会被记录，其范围包括但不限于登录、注销、用户管理、密码管理、授权管理、核心安全配置（如访问控制策略、自动更新策略、安全监控策略、审计功能）的变更、固件更新和恢复等。

（2）审计日志支持的大小是200K，如果超过200K，较老的日志将会备份到BMC中。当前的审计日志可通过Web进行查看，较老的审计日志可通过一键收集日志功能下载。

在ISBMC Web页面导航栏中选择“日志和告警>审计日志”，打开如图6-21所示界面，参数说明见表6-16。



序号	产生时间	软件接口	用户	IP或硬件接口	事件描述
900	2000-01-03T16:09:37+08:00	WEB	admin	100.2.106.28	Login Success from IP:100.2.106.28 user:admin
899	2000-01-02T14:22:47+08:00	WEB	admin	100.2.106.28	Logout Success from IP:100.2.106.28 user:admin
898	2000-01-02T14:22:17+08:00	WEB	admin	100.2.106.28	Login Success from IP:100.2.106.28 user:admin
897	2000-01-02T14:21:26+08:00	WEB	admin	100.2.106.28	Logout Success from IP:100.2.106.28 user:admin
896	2000-01-02T14:13:37+08:00	WEB	admin	100.2.106.28	Login Success from IP:100.2.106.28 user:admin
895	2000-01-02T14:08:35+08:00	WEB	admin	100.2.106.28	Logout Success from IP:100.2.106.28 user:admin

图6-21 审计日志web界面

参数	描述
序号	审计日志序号，序号越小的操作发生越早
产生时间	审计日志产生时间
软件接口	软件接口，包括： Web CLI IPMI KVM VMEDIA_CD VMEDIS_HD
用户	用户，记录日志事件操作用户，如admin，sysadmin或者NA等
IP或硬件接口	IP或硬件接口，硬件接口包括SERIAL、HOST、IPMB、USB和SSIF
事件描述	事件详细信息

表6-16 审计日志参数表

6.4.4 资产信息

通过“系统信息”界面的功能，用户可以查看系统的资产信息详情，在该界面下有 CPU、内存、电源、设备清单、硬盘、网卡、安全芯片，七个子页面，分别展示各种类别设备的详情信息。以CPU子页面为例，会展示CPU的在位状态、处理器ID、具体型号、当前速率、核数、线程数、TDP、各级缓存大小、PPIN等。内存、电源、PCIe设备的具体详细信息见图6-22的示例所示。

在ISBMC Web页面导航栏中选择“信息>系统信息”，打开如图6-22所示界面。

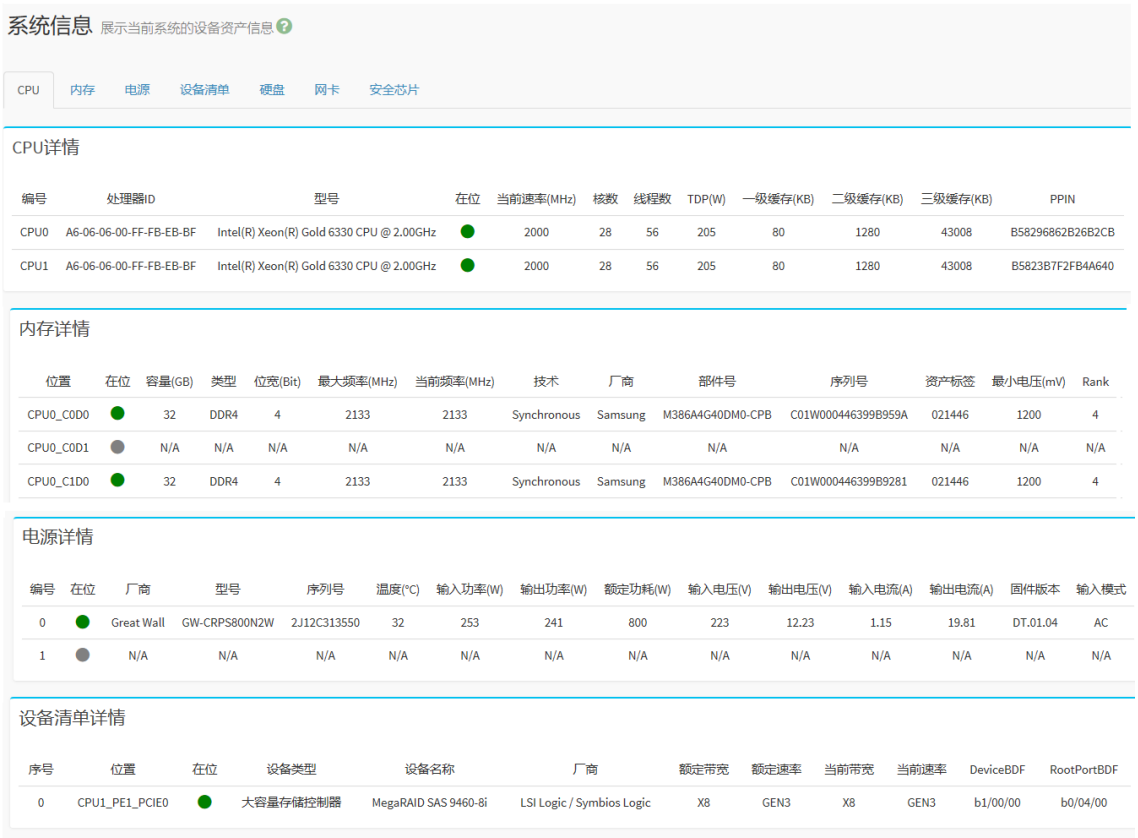


图6-22 资产信息web界面

浪潮信息 www.inspur.com

浪潮®技术支持与服务热线 400-860-0011

购买咨询热线 400-860-6708 / 800-860-6708

浪潮服务器

浪潮存储