

H3C HDM 技术白皮书

Copyright © 2019 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 概述.....	1
2 系统设计.....	2
3 产品功能.....	3
3.1 丰富的管理接口.....	3
3.1.1 IPMI管理接口.....	3
3.1.2 HTTPS管理接口.....	3
3.1.3 RESTful管理接口.....	4
3.1.4 SNMP管理接口.....	4
3.1.5 Redfish管理接口.....	4
3.2 基于WEB的可视化管理.....	7
3.2.1 系统健康状态.....	7
3.2.2 3D温度海洋.....	8
3.2.3 系统资源监控.....	9
3.3 管理接入.....	10
3.3.1 边带管理及NCSI技术.....	10
3.3.2 IPv6.....	12
3.3.3 Bonding.....	13
3.3.4 共享网口切换.....	14
3.4 HDM网络管理.....	15
3.4.1 NTP 及时间管理.....	15
3.4.2 DNS.....	15
3.5 故障告警.....	17
3.5.1 故障告警.....	17
3.5.2 SHD简介.....	18
3.5.3 SHD故障诊断.....	19
3.5.4 存储可维护.....	21
3.5.5 故障诊断辅助功能.....	21
3.5.6 故障上报.....	22
3.6 虚拟KVM和虚拟媒体.....	22
3.6.1 虚拟KVM.....	22
3.6.2 H5 KVM.....	22
3.6.3 虚拟媒体.....	23

3.7 VNC会话	24
3.7.1 VNC介绍	24
3.7.2 VNC支持共享模式和独占模式	24
3.7.3 VNC配置页面	24
3.7.4 建立非安全VNC会话	25
3.7.5 修改VNC 密码	26
3.8 主机管理	27
3.8.1 FRU及资产信息管理	27
3.8.2 系统启动项	27
3.8.3 风扇调速	27
3.9 智能电源和能耗管理	29
3.9.1 电源控制	29
3.9.2 功率封顶	30
3.9.3 电源主备	31
3.9.4 历史功率统计	31
3.9.5 设置电源性能模式	31
3.9.6 设置节能	32
3.9.7 AC恢复配置	32
3.10 RAID带外配置	33
3.11 截屏和录像回放	35
3.11.1 截屏	35
3.11.2 录像回放	36
3.12 可维护性	37
3.12.1 串口切换	37
3.12.2 一键收集	38
3.12.3 操作日志	39
3.12.4 事件日志	40
3.12.5 远程Syslog	41
3.12.6 电子邮件告警	41
3.12.7 Remote XDP	42
3.12.8 诊断面板	43
3.13 域管理和目录服务	44
3.13.1 域管理	44
3.13.2 目录服务	44
3.14 安全管理	45
3.14.1 防火墙	45

3.14.2 账号安全	45
3.14.3 SSL证书管理.....	47
3.14.4 硬件加密	47
3.14.5 服务管理	47
3.14.6 用户定义	48
3.15 固件管理	49
3.15.1 固件双镜像	50
3.15.2 固件升级	50
3.15.3 BIOS的自升级	51
3.16 配置管理	51
3.16.1 配置文件导入导出	51

1 概述

H3C 设备管理系统（Hardware Device Management，以下简称 HDM）是 H3C 自主研发的服务器远程管理系统。HDM 兼容服务器业界管理标准 IPMI、SNMP、Redfish，支持键盘、鼠标和视频的重定向，文本控制台的重定向，远程虚拟媒体，高可靠的硬件监控和管理功能。HDM 提供了丰富的特性支持。其主要特性有：

- 丰富的管理接口

提供 IPMI/HTTPS/SNMP/Redfish/RESTful 管理接口，满足多种方式的系统集成需求。

- 兼容 IPMI1.5/IPMI2.0

提供标准的管理接口，可被标准管理系统集成。

- 故障监控和诊断

故障监控和诊断，通过精准定位与诊断，指导运维人员快速解决问题，保障设备 7*24 小时高可靠运行。

- 虚拟 KVM 和虚拟媒体

提供方便的远程维护手段。

- 基于 Web 界面的用户接口

可以通过简单的界面操作快速完成设置和查询任务。

- 支持 RESTful 管理接口

简洁方便，有层次实现远程命令管理。

- 支持 Redfish 管理接口

降低开发复杂性，易于实施、易于使用、易于扩展。

- 截屏与录像

通过截屏和录像可以快速分析系统崩溃的原因。

- 屏幕录像

操作过程记录变得简单轻松。

- 支持 SHD

支持基于部件的精准故障诊断，方便部件故障定位和更换。

- 支持 DNS/LDAP

域管理和目录服务，简化服务器管理网络。

- RAID 带外管理

支持 RAID 的带外监控和配置，提升了 RAID 配置效率和管理能力。

- 双镜像备份

提高系统的安全性，即使当前运行的软件完全崩溃，也可以从备份镜像启动。

- 设备资产管理

让资产盘点不再困难。

- 支持智能电源管理

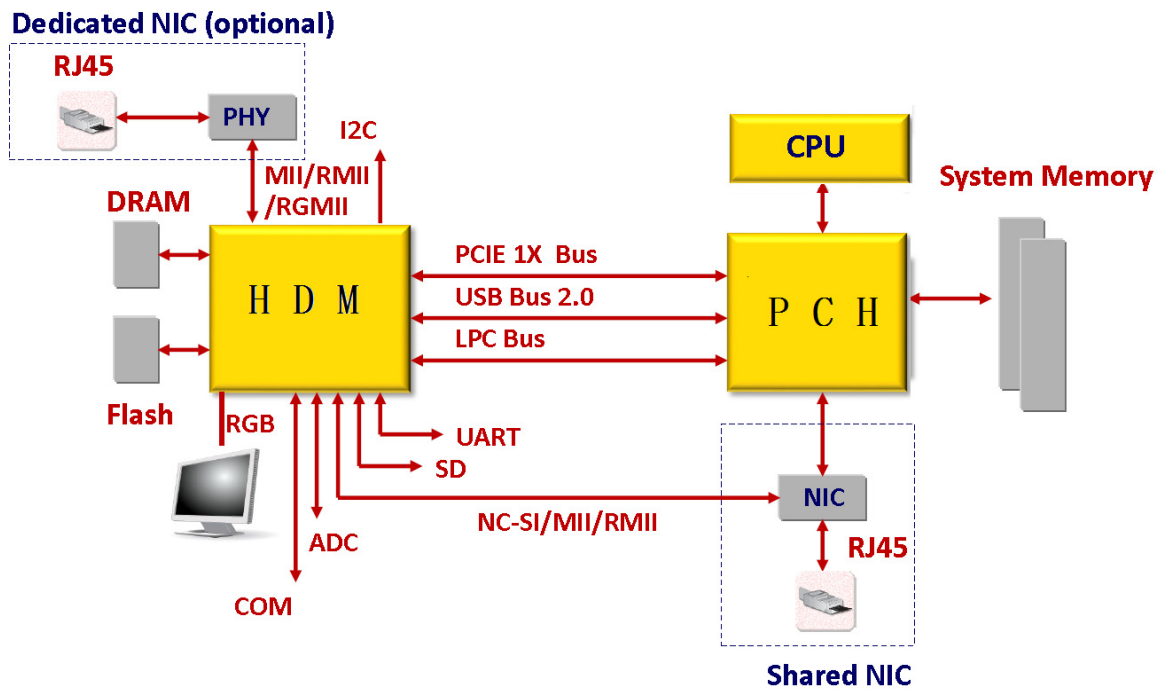
功率封顶技术帮助管理员轻松提高部署密度；动态节能技术帮助您有效降低运营成本。

- 安全管理
从接入、账号、传输、存储四个维度保障服务器管理的安全。

2 系统设计

如图所示，HDM 硬件芯片采用服务器专用 SOC 芯片，有效管理服务器硬件设备。SOC 芯片支持远程 KVM 和本地 VGA 显示，支持专用和共享网口，以及其它丰富的板级管理和外设接口。具体如下：

图1 HDM 系统结构



- HDM 的 KVM 模块通过 VGA 接口接收来自主机系统的视频信息，经过压缩后再通过网络将压缩数据传输到远程 KVM 客户端进行解压还原。此外 KVM 模块接收远程 KVM 客户端的键盘鼠标数据，通过模拟的 USB 键盘鼠标设备将数据传输到主机系统，实现远程的键盘鼠标控制。
- HDM 提供传统的 LPC 系统接口与主机系统通信，支持标准的 IPMI 管理。
- HDM 对外提供 GE 以太网网络接口，支持通过网络使用 IPMI、HTTPS、Redfish 等协议进行远程管理操作。
- HDM 通过传感器实现了对服务器的温度、电压状态全面监控，并且提供对服务器的风扇和电源的智能管理。
- HDM 支持最新的边带网络技术（NCSI）以及 VLAN 网络功能，通过边带网络可以支持更加灵活的管理组网。
- HDM 是支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体（可将终端的光驱、硬盘、文件夹映射到服务器）和基于 IPMI2.0 的硬件监控和管理功能。
- 支持 HDM 软件的双镜像备份和主备切换。

- HDM 提供了丰富的用户接口,如命令行、基于 Web 界面的用户接口、IPMI 集成接口、Redfish、SNMP 集成接口, 并且所有用户接口都采用了认证机制和高度安全的加密算法, 保证接入和传输的安全性。
- HDM 对服务器进行了全面精细的监控, 并且提供了丰富的告警和详细的日志。如 CPU 的内核温度、内存故障、硬盘故障、电压、风扇转速、电源故障等。同时还提供了 CPU、内存和硬盘信息的查询。
- HDM 能够在服务器宕机的时候自动保存宕机之前屏幕上输出的最后的信息,用于故障的定位。还支持即时的屏幕快照, 第三程序可以设置定时或周期性的进行屏幕截屏, 不需要手工定时去查看服务器, 为维护人员节省大量时间。

3 产品功能

3.1 丰富的管理接口

3.1.1 IPMI管理接口

HDM 兼容 IPMI 1.5/IPMI 2.0 规范, 支持数据中心管理接口 (DCMI, Data Center Manageability Interface), 通过第三方工具 (如: ipmitool)基于 LPC 通道的 KCS 协议或 LAN 通道的 UDP/IP 协议实现对服务器的有效管理。

- 基于 KCS 时, ipmitool 等工具必须运行在服务器本机的操作系统上;
- 基于 LAN 时, ipmitool 等工具可以远程管理服务器。

第三方工具支持 Windows 和 Linux 系统。

以下以 ipmitool 工具详细说明:

- ipmitool 命令格式: ipmitool [interface] [parameter] <command>
- ipmitool 命令举例: 查询 HDM 的传感器列表
 - 基于 KCS: ipmitool sensor list
 - 基于 LAN: ipmitool -H *.*.* -I lanplus -U <用户名> -P <密码> sensor list
 - H: HDM 网口 IP 地址
 - I: 传输协议, lan: 不加密, lanplus: 加密
 - U: HDM 本地用户名
 - P: HDM 本地用户密码
 - L: 指定用户使用权限。对于 user 和 operator 用户需要使用。

3.1.2 HTTPS管理接口

HDM 提供了基于 HTTPS 的 Web 可视化管理接口。

- 通过简单的界面操作快速完成设置和查询任务。
- 通过远程控制台可以对服务器进行 OS 启动全程监控、OS 操作、以及光驱/软驱映射等。

可以在浏览器地址栏输入 HDM 的网口 IP 地址 (IPv4 或 IPv6) 或域名地址打开 HDM Web 的登录界面, 输入账号登录到 HDM Web。

3.1.3 RESTful管理接口

HDM 支持服务器通过 RESTful API 进行管理，实现简化服务器配置过程、查看服务器组件信息、监控服务器运行状况以及远程控制服务器等功能。

RESTful 接口具有以下技术优点：

- 轻量：直接基于 HTTP，不再需要任何别的消息协议。
- 面向资源：一目了然，具有自解释性。
- 数据描述简单：一般以 xml, json 做数据交换。
- 无状态：在调用一个接口（访问、操作资源）的时候，可以不用考虑上下文，不用考虑当前状态，极大的降低了复杂度。
- 简单、低耦合。

3.1.4 SNMP管理接口

基于简单网络管理协议（以下简称 SNMP）是管理进程（NMS）和代理进程（Agent）之间的通信协议。它规定了在网络环境中对设备进行监视和管理的标准化管理框架、通信的公共语言、相应的安全和访问控制机制。

SNMP 具有以下技术优点：

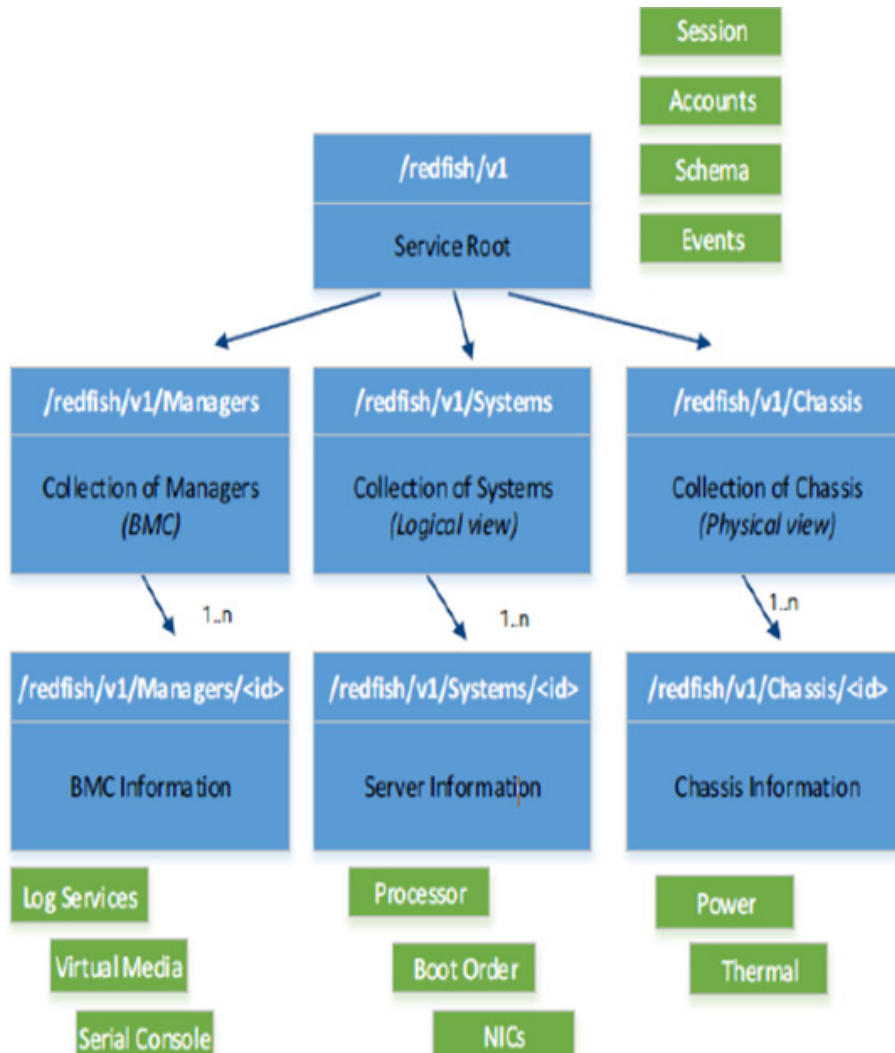
- 基于 TCP/IP 互联网的标准协议，传输层协议一般采用 UDP。
- 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。
- 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务与被管设备的物理特性和实际网络类型相对独立，从而实现对不同厂商设备的管理。
- 简单的请求一应答方式和主动通告方式相结合，并有超时和重传机制。
- 报文种类少，报文格式简单，方便解析，易于实现。
- SNMPv3 版本提供了认证和加密安全机制，以及基于用户和视图的访问控制功能，增强了安全性。
 - HDM 提供了基于 SNMP 的编程接口，支持 SNMP Get/Set/Trap 操作，第三方管理软件通过调用 SNMP 接口可以方便地对服务器集成管理。SNMP 代理支持 V1/V2C/V3 版本。
 - SNMP 代理提供接口查询系统健康状态、系统健康事件、硬件状态、内存和 CPU 型号、告警上报配置、功率统计数据、资产信息、散热管理、固件版本信息、网络管理等。

3.1.5 Redfish管理接口

Redfish 是一种基于 HTTPs 服务的管理标准，利用 RESTful 接口实现设备管理。每个 HTTPs 操作都以 UTF-8 编码的 JSON 格式（JSON 是一种 key-value 对的数据格式）提交或返回一个资源或结果，就像 Web 应用程序向浏览器返回 HTML 一样。该技术具有降低开发复杂性，易于实施、易于使用而且提供了可扩展性优势，为设计灵活性预留了空间。目前我们利用 Redfish 管理接口可以实现包括用户管理、获取服务器信息、管理模块信息等常用 HDM 和 BIOS 配置。

Redfish=REST API+软件定义的服务器(数据模型)，当前由标准组织DMTF(www.dmtf.org)负责维护。Redfish框架如图所示。

图2 Redfish 框架



Redfish 流程图如图所示，当客户端发出 HTTP(s)请求后，会去 Redis DB 读取最新数据并返回读取结果。同时 Redis DB 通过 SEL 和 IPMI 实时更新数据库内容。

图3 Redfish 流程图

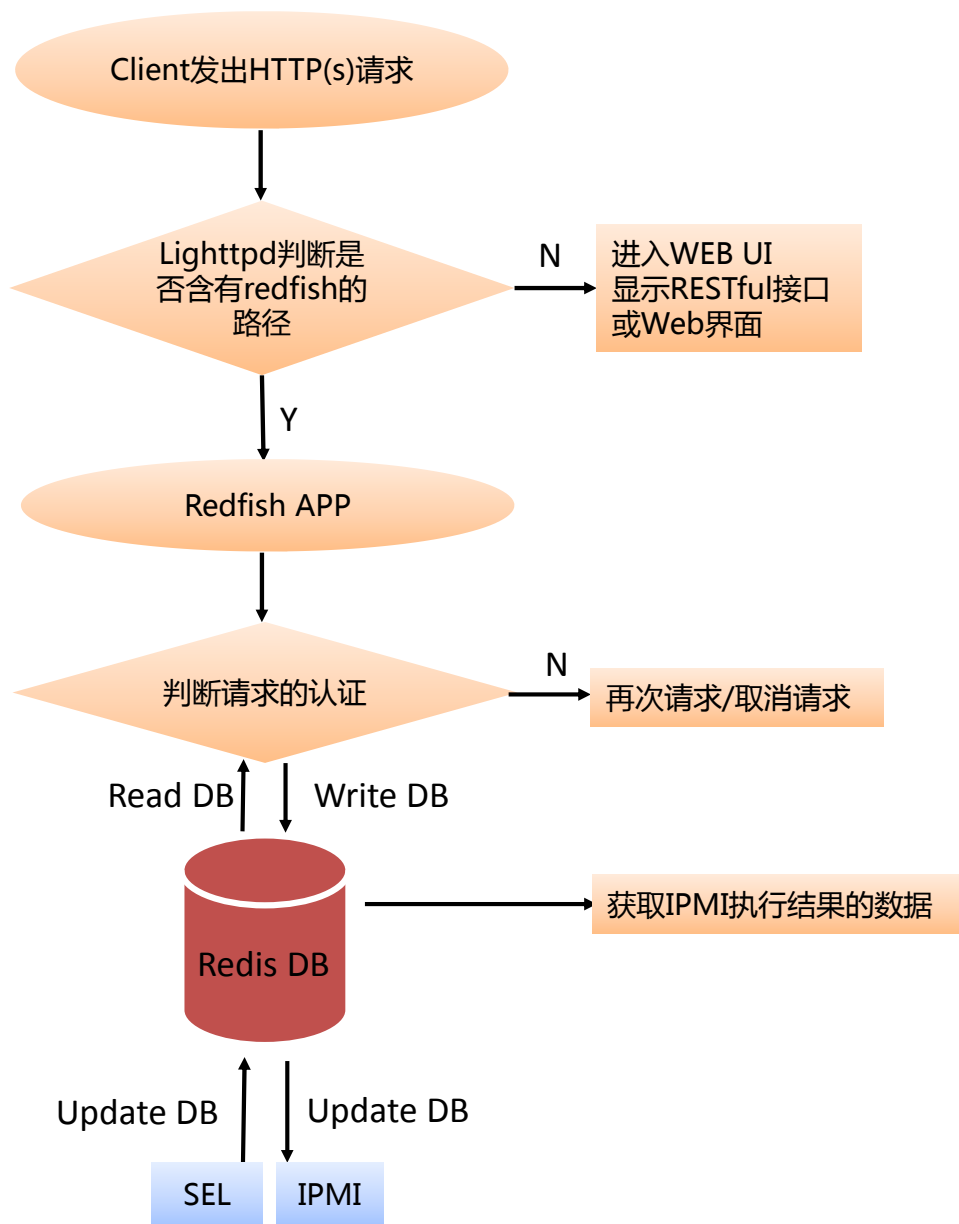


图4 Redfish 接口操作示例(查询电源信息)

The screenshot displays a REST client interface with a request and response pane. The request pane shows a GET request to the URL `https://192.168.12.36/redfish/v1/Chassis/Self/Power`. The response pane shows a 200 OK status and a JSON response. The JSON response is as follows:

```
GET on https://192.168.12.36/redfish/v1/Chassis/Self/Power
Status: 200 OK

{
  "@odata.context": "/redfish/v1/$metadata#Power.Power(PowerControl,Voltages,Id,Name,Power)",
  "@odata.etag": "W/\"1525835570\"",
  "@odata.id": "/redfish/v1/Chassis/Self/Power",
  "@odata.type": "#Power.v1_2_1.Power",
  "Id": "Power",
  "Name": "Power",
  "PowerControl": {
    "0": {
      "@odata.id": "/redfish/v1/Chassis/Self/Power#/PowerControl/1",
      "Name": "System Power Control 1",
      "PowerCapacityWatts": 800,
      "PowerMetrics": {
        "MaxConsumedWatts": 800,
        "MinConsumedWatts": 150,
        "PowerRequestedWatts": 500,
        "Status": {
          "Health": "OK",
          "State": "Disabled"
        }
      }
    }
  },
  "PowerSupplies": {
    "0": {
      "@odata.id": "/redfish/v1/Chassis/Self/Power#/PowerSupplies/1"
    }
  }
}
```

图5 Redfish 接口操作示例(查询用户信息)

The screenshot displays a REST client interface with a request and response pane. The request pane shows a GET request to the URL `https://192.168.12.36/redfish/v1/AccountService/Accounts/2`. The response pane shows a 200 OK status and a JSON response. The JSON response is as follows:

```
GET on https://192.168.12.36/redfish/v1/AccountService/Accounts/2
Status: 200 OK

{
  "@odata.context": "/redfish/v1/$metadata#ManagerAccount.ManagerAccount(Id,Links,Name,Oem,RoleId,Description)",
  "@odata.etag": "W/\"1525494885\"",
  "@odata.id": "/redfish/v1/AccountService/Accounts/2",
  "@odata.type": "#ManagerAccount.v1_0_3.ManagerAccount",
  "Description": "Default Account",
  "Enabled": true,
  "Id": "2",
  "Links": {
    "Roles": {
      "@odata.id": "/redfish/v1/AccountService/Roles/Administrator",
      "Locked": false,
      "Name": "Default Account",
      "Oem": {
        "H3C": {
          "KvmEnable": "true",
          "VmediaEnable": "true",
          "RoleId": "Administrator",
          "UserName": "admin"
        }
      }
    }
  }
}
```

3.2 基于WEB的可视化管理

HDM 提供了基于 HTTPS 的 Web 可视化管理接口，可以实现通过简单的界面点击快速完成设置和查询任务。

3.2.1 系统健康状态

在【整体概况】页面可以看到服务器整体的健康状态，其状态和服务器的健康指示灯保持一致。

整体健康状态由服务器相关部件健康状态决定，支持的部件有：CPU、DIMM、风扇、电源、温感、硬盘等。

点击页面上显示的故障部件的状态链接，可直接跳转到对应的传感器页面。

图6 HDM Web 界面



3.2.2 3D温度海洋

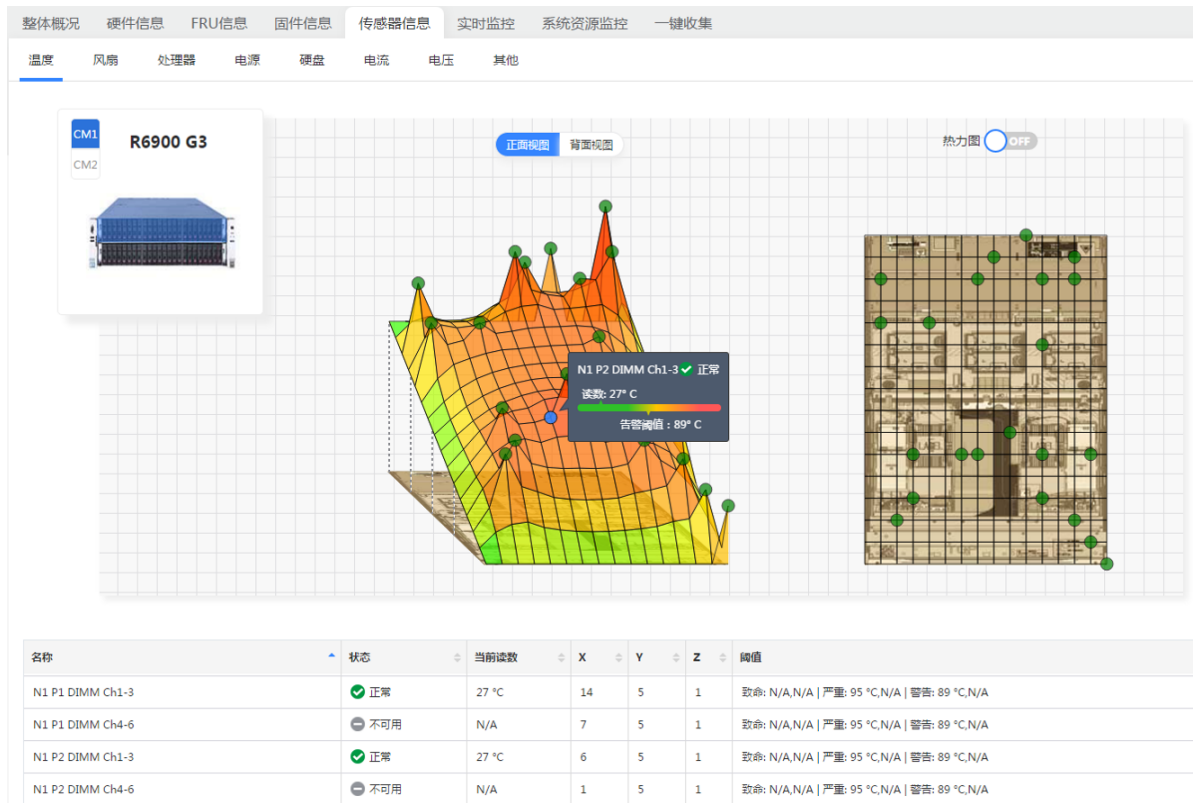
3D 温度海洋用于显示服务器机箱中各组件温度传感器的分布图及数值，同时提供了实际物理结构图作为参考。温度海洋上的圆圈与表中可用的传感器相对应，将鼠标移到温度海洋上的圆圈上可查看传感器名称、状态、温度读数和阈值。温度海洋的颜色从绿色逐渐变为红色，绿色表示温度为 0°C ，红色表示温度较高。坐标含义如下：

X: 传感器在 X 轴上的坐标信息。

Y: 传感器在 Y 轴上的坐标信息。

Z: 传感器所属的服务器信息，0 表示该传感器属于当前服务器。

图7 温度传感器信息查询



3.2.3 系统资源监控

HDM 可以查看监控带内的 CPU、内存、磁盘的资源占用率资源。使用本功能时需要在 OS 侧安装并运行 FIST SMS(Server Management Service, 运行在 OS 下的代理软件, 当前支持的操作系统有: Redhat6.8 7.3 以及 Windows Server 2012 R2)。

当监控带内的 CPU、内存、磁盘的占用率资源超过阈值时, 系统会记录事件日志。



3.3 管理接入

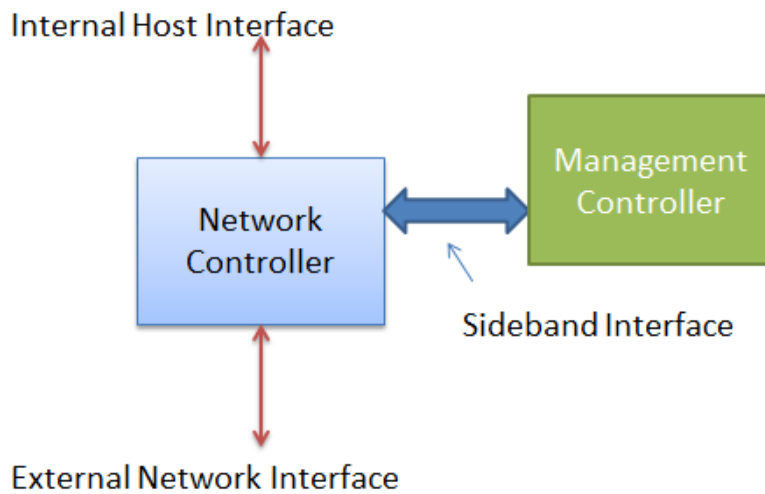
3.3.1 边带管理及NCSI技术

边带管理（共享网口）就是利用边带（NCSI Network Controller Sideband Interface）技术使管理系统与主机系统共用主机物理网口，通过一个网口就可以同时做管理操作和业务处理，简化组网，节省交换机端口；从安全考虑，利用 VLAN 技术将管理与业务划分在不同网段。

NCSI 是基于物理总线 RMII 的带外管理总线协议。普通的网络管理总线是 MDC/MDIO 总线，这种管理总线需要额外的引脚作为物理总线，但是 NCSI 总线是与网络通信总线 RMII 复用总线，在 RMII 总线基础之上定义一个 NCSI 协议，这样就可以达到减少物理引脚的目的。

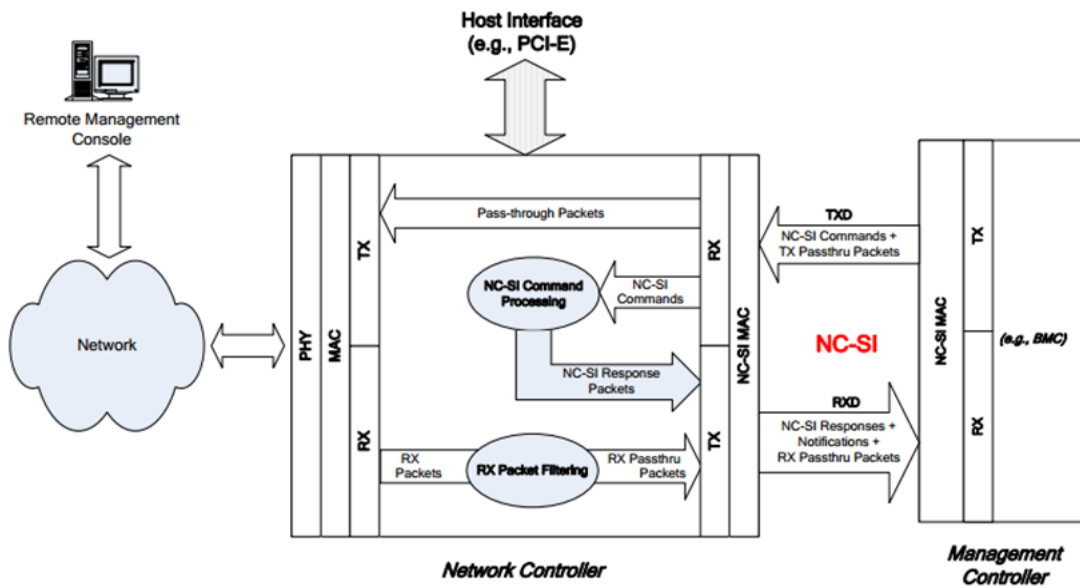
NC (Network Controller: 网络控制器)在与对外通信上分为内部网络接口：Internal Host Interface，外部网络接口：External Network Interface，以及带外接口：Sideband Interface。其用途分别是：向外部网络发送数据，与 HDM 进行网络通信（包括 NCSI 协议）。HDM 通过 NCSI 协议进行网络配置，网络配置成功之后，HDM 就可以向 NC 发送正常的网络报文。从链路上看，NCSI 报文与网络通信报文在物理链路上共用一个物理总线：RMII，该 RMII 物理总线连接的另外一端是 HDM，那么这条总线在 NC 看来就是一个带外接口（Sideband Interface）。

图8 边带管理框图



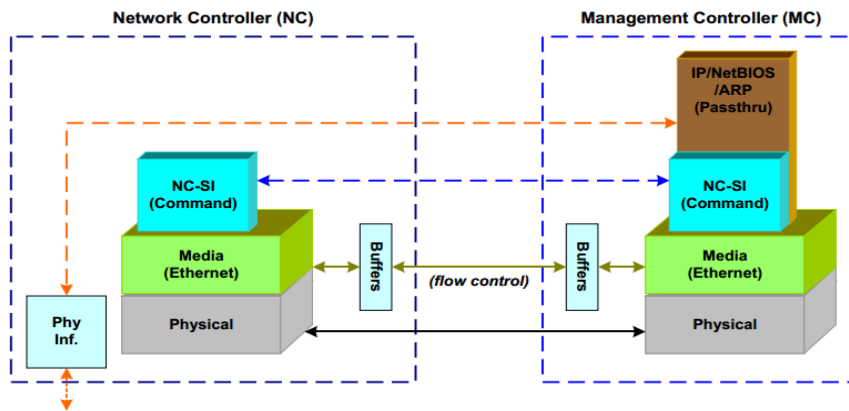
从数据流程来看，HDM 通过 MAC 向物理总线 RMII 发送一个网络报文，NC 通过 RMII 接收到网络报文后，对网络报文进行解析。解析后，如果是 NCSI 报文（判断的条件是：ether type 为 0x88F8），则进行 NCSI 响应；如果是对外发送数据的网络报文（ether type 为非 0x88F8）则将数据转发到 External Interface。

图9 边带管理数据流图



从协议层面上看，NCSI 协议是一个网络层协议，其网络类型码为 0x88F8。

图10 NCSI 协议



3.3.2 IPv6

HDM 全面支持 IPv6。专用管理网口和共享网口（NCSI）的物理通道都支持 IPv6 地址访问。

图11 HDM 支持 IPv6 地址功能

专用网口 共享网口 DNS 网口模式

概况 配置 网卡选择

HDM共享网络接口与专用网络接口的IPv6地址处于同一网段，可能导致网络不通

概况

LAN接口	共享网口
LAN设置	<input checked="" type="checkbox"/> 启用
MAC地址	74:EA:CB:5A:5D:7D

保存

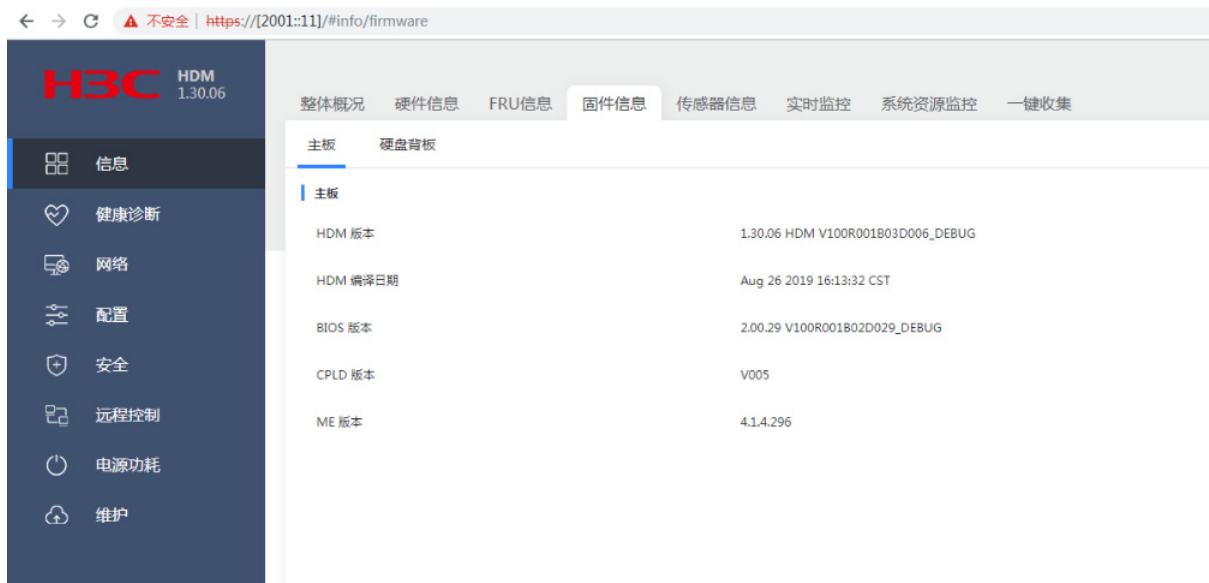
IPv4概况

IPv4地址	192.168.50.166
子网掩码	255.255.0.0
默认网关	0.0.0.0

IPv6概况

IPv6地址1	8001::c:1932
IPv6地址2	3ffe:501:2:ffff:76ea:cbff:fe5a:5d7d
本地链路地址	fe80::76ea:cbff:fe5a:5d7d

图12 支持 IPv6 登录 HDM Web



3.3.3 Bonding

使用 Bonding 功能可以提高 HDM 接入的可靠性。切换为 Bonding 后，系统会将 HDM 共享网络接口和 HDM 专用网络接口作为一个逻辑上的网络接口使用。切换后，Bonding 接口将继承 HDM 专用网络接口的 IP 地址和 MAC 地址。HDM 共享网络接口和 HDM 专用网络接口中的任意一个接口 UP 状态，管理员仍然能通过 HDM Bonding 网络接口的 IP 地址访问 HDM。

图13 Bonding 切换

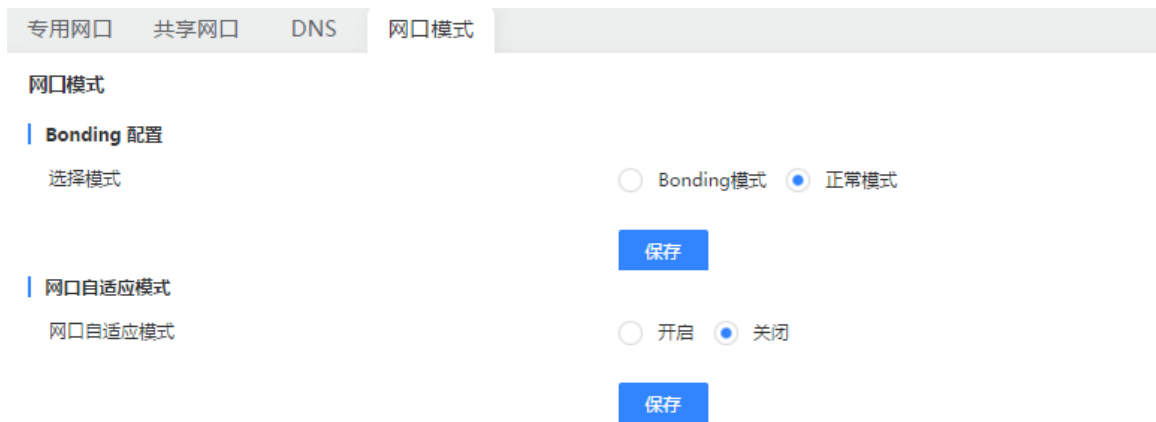


图14 Bonding 切换前后概览页面的网络配置

正常模式		Bond模式																																									
概况 > 整体概况		概况 > 整体概况																																									
<table border="1"> <tr><th colspan="2">基本信息</th></tr> <tr><td>产品厂商</td><td>Unis Huashan Technologies Co., Ltd.</td></tr> <tr><td>产品名称</td><td>UniServer R2700 G3</td></tr> <tr><td>主机名</td><td>HDM210200A00TH177000017</td></tr> <tr><td>维保序列号</td><td>210235A2DBH177000014</td></tr> <tr><td>IPv4地址</td><td>共享网口 : 172.16.47.5 ; 专用网口 : 192.168.18.169</td></tr> <tr><td>MAC地址</td><td>共享网口 : 74:EA:C8:5A:5D:7D ; 专用网口 : 74:EA:C8:5A:5D:7C</td></tr> <tr><td>HDM固件版本</td><td>1.10.37 HDM V100R001B01D037</td></tr> <tr><td>BIOS固件版本</td><td>1.00.36 V100R001B01D036</td></tr> <tr><td>CPLD固件版本</td><td>V003</td></tr> </table>		基本信息		产品厂商	Unis Huashan Technologies Co., Ltd.	产品名称	UniServer R2700 G3	主机名	HDM210200A00TH177000017	维保序列号	210235A2DBH177000014	IPv4地址	共享网口 : 172.16.47.5 ; 专用网口 : 192.168.18.169	MAC地址	共享网口 : 74:EA:C8:5A:5D:7D ; 专用网口 : 74:EA:C8:5A:5D:7C	HDM固件版本	1.10.37 HDM V100R001B01D037	BIOS固件版本	1.00.36 V100R001B01D036	CPLD固件版本	V003	<table border="1"> <tr><th colspan="2">基本信息</th></tr> <tr><td>产品厂商</td><td>Unis Huashan Technologies Co., Ltd.</td></tr> <tr><td>产品名称</td><td>UniServer R2700 G3</td></tr> <tr><td>主机名</td><td>HDM210200A00TH177000017</td></tr> <tr><td>维保序列号</td><td>210235A2DBH177000014</td></tr> <tr><td>IPv4地址</td><td>bond0 : 192.168.18.169</td></tr> <tr><td>MAC地址</td><td>bond0 : 74:EA:C8:5A:5D:7C</td></tr> <tr><td>HDM固件版本</td><td>1.10.37 HDM V100R001B01D037</td></tr> <tr><td>BIOS固件版本</td><td>1.00.36 V100R001B01D036</td></tr> <tr><td>CPLD固件版本</td><td>V003</td></tr> </table>		基本信息		产品厂商	Unis Huashan Technologies Co., Ltd.	产品名称	UniServer R2700 G3	主机名	HDM210200A00TH177000017	维保序列号	210235A2DBH177000014	IPv4地址	bond0 : 192.168.18.169	MAC地址	bond0 : 74:EA:C8:5A:5D:7C	HDM固件版本	1.10.37 HDM V100R001B01D037	BIOS固件版本	1.00.36 V100R001B01D036	CPLD固件版本	V003
基本信息																																											
产品厂商	Unis Huashan Technologies Co., Ltd.																																										
产品名称	UniServer R2700 G3																																										
主机名	HDM210200A00TH177000017																																										
维保序列号	210235A2DBH177000014																																										
IPv4地址	共享网口 : 172.16.47.5 ; 专用网口 : 192.168.18.169																																										
MAC地址	共享网口 : 74:EA:C8:5A:5D:7D ; 专用网口 : 74:EA:C8:5A:5D:7C																																										
HDM固件版本	1.10.37 HDM V100R001B01D037																																										
BIOS固件版本	1.00.36 V100R001B01D036																																										
CPLD固件版本	V003																																										
基本信息																																											
产品厂商	Unis Huashan Technologies Co., Ltd.																																										
产品名称	UniServer R2700 G3																																										
主机名	HDM210200A00TH177000017																																										
维保序列号	210235A2DBH177000014																																										
IPv4地址	bond0 : 192.168.18.169																																										
MAC地址	bond0 : 74:EA:C8:5A:5D:7C																																										
HDM固件版本	1.10.37 HDM V100R001B01D037																																										
BIOS固件版本	1.00.36 V100R001B01D036																																										
CPLD固件版本	V003																																										

3.3.4 共享网口切换

共享网口切换指的是切换HDM共享网口后,管理员只要重新接入切换后的共享网口即可访问HDM,该特性具有以下优点:

- 不用更改服务器在整网中的网络信息,实现平滑切换。
- 不需要重新配置切换后共享网口的网络信息(包括IP地址、VLAN等),提高维护效率。

图15 共享网口切换

专用网口
共享网口
DNS
网口模式

概况
配置
网卡选择

HDM共享网络接口与专用网络接口的IPv6地址处于同一网段,可能导致网络不通

端口自适应模式

端口自适应模式 开启 关闭

[保存](#)

选择网卡

mLOM 端口0 端口1 端口2 端口3

PCIe扩展网卡 (不在位) 端口0 端口1

[保存](#)

3.4 HDM网络管理

3.4.1 NTP 及时间管理

网络时间协议 NTP (Network Time Protocol) 是 TCP/IP 协议族里的一个应用层协议, 用于在一系列分布式时间服务器与客户端之间同步时钟。服务器的 HDM 支持配置服务器所在的时区, 并通过手动或自动获取首选和备用 NTP 服务器(支持 IPv4 和 IPv6), 手动设置 NTP 服务器地址支持 FQDN 域名。

图16 NTP 页面

用户配置	LDAP配置	NTP	SNMP	PEF
NTP				
HDM时间	2019-9-27 10:20:05			
时区	UTC+8:00			
与NTP服务器自动同步日期和时间 (同时开启DHCP时间同步机制)	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭			
主NTP服务器	1.cn.pool.ntp.org			
二级NTP服务器	2.cn.pool.ntp.org			
<input type="button" value="保存"/>				

HDM 可以从多种时钟源获取时间信息, 其时间同步的优先级如下:

主 NTP 服务器> 二级 NTP 服务器> DHCP Server 兼任的 NTP Server > 主机 ME> BMC 上的 RTC;

3.4.2 DNS

DNS 是一种用于 TCP/IP 应用程序的分布式数据库, 提供域名与 IP 地址之间的转换服务。完整的域名由主机名和上级域名组合而成。HDM 中, 主机名可以手动配置, 也可以根据服务器的 SN 号自动生成; 上级域名可以手动配置, 也可以通过 DHCP 自动获取。

HDM 支持将共享网口和专用网口的 IP 地址与域名建立映射关系, 并将该映射关系向网络中的 IP DNS 服务器进行注册。

注册方式分为 nsupdate 以及 FQDN\主机名方式：nsupdate 方式为客户端直接通过 nsupdate 命令更新 DNS 服务器的区文件；FQDN\主机名方式为 DHCP 服务器在确认客户端的网络地址分配后，将客户端的信息动态注册到 DNS 服务器。

用户后续可以直接使用便于记忆的、有意义的域名访问 HDM。

图17 DNS 注册流程



图18 IPv6 DNS 解析

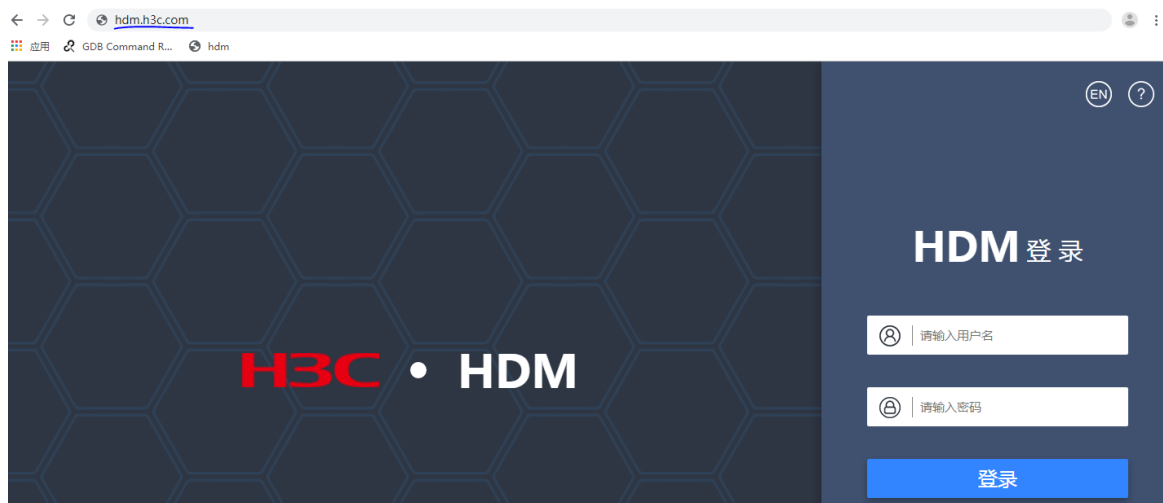
```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\H3C>ping hdm.h3c.com

正在 Ping hdm.h3c.com [3ffe:501:eeee:0:76ea:cbff:fe5a:5d7d] 具有 32 字节的数据:
来自 3ffe:501:eeee:0:76ea:cbff:fe5a:5d7d 的回复: 时间=113ms
来自 3ffe:501:eeee:0:76ea:cbff:fe5a:5d7d 的回复: 时间=381ms
来自 3ffe:501:eeee:0:76ea:cbff:fe5a:5d7d 的回复: 时间<1ms
来自 3ffe:501:eeee:0:76ea:cbff:fe5a:5d7d 的回复: 时间=80ms

3ffe:501:eeee:0:76ea:cbff:fe5a:5d7d 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 381ms, 平均 = 143ms
```

图19 通过域名访问 HDM



3.5 故障告警

3.5.1 故障告警

当服务器部件发生故障或某些原因导致系统处于不正常的工作状态时，系统能够根据不同类型及不同模块出现的故障产生告警信息，同时生成日志信息。若配置了网管系统，则该告警信息会通过 **SNMP**（Simple Network Management Protocol）Trap 协议向网管系统发送。若配置了邮件系统，则该告警信息会通过 **SMTP** 协议向外发送。

服务器产品的告警可分四个级别，按告警严重性分为：

- 正常(Info)

事件提示级别用于表示对系统不会产生影响的事件，例如正常的状态变化，告警事件解除。

- 一般告告警(Minor)

一般告警不会对系统产生大的影响，需要尽快采取相应的措施，防止故障升级。

- 严重告警(Major)

严重告警将会对系统产生较大的影响，有可能中断部分系统的正常运行，导致业务中断。

- 致命告警(Critical)

致命告警可能会使单板下电，系统中断。需要马上采取相应的措施进行处理。

能够检测的故障信息如下：

- 处理器：能够检测 CPU 的 CAT ERROR，自检错误，配置错误(包括 CPU UPI errors, IOH UPI errors, CPU core errors, IOH core errors)。
- 内存：能够检测内存的可纠正、不可纠正错误、高温、Training 错误。
- 电源：包括电源在位，AC/DC 输入丢失，电源预告警，PSU 自检失败等故障。
- 风扇：能够检测到风扇的在位，故障，降级故障。
- 存储：能够检测到硬盘在位、故障、预故障、关键阵列、故障阵列故障。
- 超温报警：包括对 CPU、内存、进风口，电源，硬盘等部件进行超温报警。
- 主板和相关板卡电压故障。

3.5.2 SHD简介

HDM 集成了智能硬件诊断系统（Smart Hardware Diagnosis，以下简称 SHD），能够对服务器主要硬件发生的故障进行快速、精准的检测与诊断。如图所示，SHD 通过收集服务器硬件发生故障时的基础数据，包括传感器、CPLD、寄存器、事件日志等，基于历史硬件故障诊断经验库，对硬件故障的发生原因进行分析定位，最终给出故障诊断结果报告。故障诊断结果报告的内容包括故障模块、故障时间、故障类型、现象描述、可能原因、故障判据以及处理措施。SHD 可以根据今后出现的新故障不断扩展优化，增强服务器的硬件故障诊断功能。

图20 智能硬件诊断系统



SHD 支持对服务器主要硬件的全面监控，提供了精准可靠的故障检测与诊断机制，可以检测和诊断的硬件故障包括：

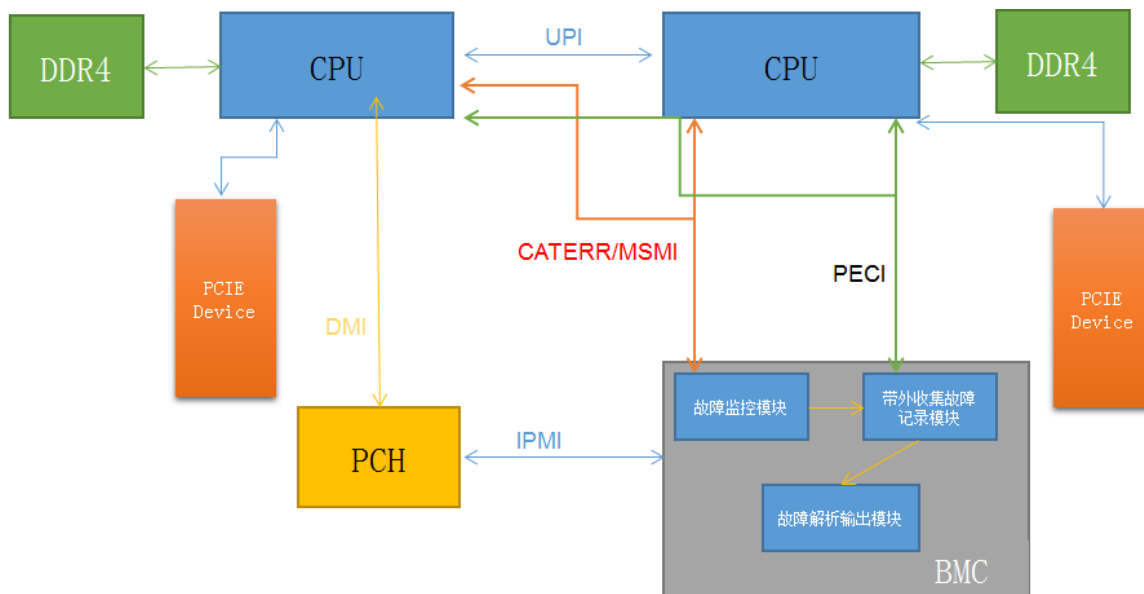
- MCA 故障（CPU、内存和 PCIe 故障）
- 电源故障（电流、电压、温度、电源风扇、IIC、均流）
- 主板故障（二次电源、风扇、网卡、电流、电压、温感）
- PCIe 卡故障（网卡、RISER 卡、NCSI 通道）
- 阵列卡故障（RAID 卡、线缆、扩展板、缓存、电池、硬盘）

3.5.3 SHD故障诊断

1. MCA故障诊断

MCA（Machine Check Architecture，以下简称 MCA）故障诊断是 SHD 的重要组成部分，MCA 故障诊断支持 CPU、内存、PCIe 故障的检测和诊断。SHD 采用轮询检测机制对 MCA 故障进行监控和诊断，即 SHD 在轮询过程中检测到 CATERR/MSMI 信号后，能够通过 PECE 通道进行带外收集硬件故障现场的基础数据，主要是错误相关的 Banks 寄存器和 CSRs 寄存器。结合收集的故障现场基础数据，基于历史硬件故障诊断经验库，对硬件故障进行分析定位给出诊断报告。如图，从总体上展现了 MCA 故障诊断的流程。

图21 MCA 故障诊断总体概览图



(1) CPU 故障检测

CPU 故障来源有两种，一种是 CPU 本身内部的故障，另一种是 CPU 外部部件（内存和 PCIe 设备）故障引起的。MCA 故障诊断能够检测 CPU 内部主要模块的故障，包括：取指单元（IFU），数据缓存单元（DCU），数据传输缓冲单元（DTLB）等。MCA 故障诊断能够分析出故障类型，在多个疑似故障源中进行综合分析，筛选定位到具体故障部件。常见的 CPU 故障类型有：

- 缓存不可纠正故障，包括数据读取错误、数据写入错误、数据预取错误
- 看门狗超时故障，3-strike timeout
- UPI 不可纠正故障
- CPU 内部电源控制模块故障
- CPU 访存超时

(2) 内存故障检测

内存故障总体上可划分为可纠正内存故障和不可纠正内存故障。服务器系统一旦发生内存不可纠正故障将会对客户业务的运行造成严重影响。MCA 故障诊断专注于内存不可纠正故障的检测与诊断，可以对收集故障记录模块记录的内存故障地址进行解析，在服务器系统搭载的大量内存条中识别出故障的内存条，精准定位到具体的 CPU-Channel-DIMM。常见的内存不可纠正故障类型有：

- 访存地址/命令错误

- 内存读取/写入错误
- 内存缓存控制错误
- 内存超时错误

(3) PCIe 故障检测

MCA 故障诊断能够对收集故障记录模块记录的 PCIe 故障地址进行解析,在服务器系统诸多的 PCIe 设备中识别出故障的 PCIe 设备,精准定位到具体的 CPU-Slot。常见的 PCIe 故障类型有:

- Received an Unsupported Request 故障
- Malformed TLP 故障
- Completer Abort 故障
- Completion Timeout 故障
- Poisoned TLP 故障
- ACS Violation 故障
- Flow Control Protocol Error 故障
- Data Link Protocol Error 故障
- Surprise Down Error 故障

2. 电源故障诊断

电源是服务器工作的动力来源,电源故障的检测和诊断是基本要求,SHD 采用中断上报和轮询检测的机制对电源故障进行监控,能够支持 11 类共计 24 种电源故障,基本涵盖了电源的主要故障类型,实现电源故障的全面监控和诊断。

- 电源不在位故障;
- 电源输入电压故障,包括输入欠压告警和保护,机房输入掉电或输入电源线接触不良;
- 电源风扇故障;
- 电源入风口温度故障,温度过高告警和保护,温度过低告警和保护;
- 电源输出电压故障,包括输出电压过低告警和保护,输出电压过高告警和保护;
- 电源输出电流故障,输出电流过高告警和保护;
- 电源 1Hz 闪烁,不供电故障;
- 电源 IIC 通讯异常;
- 电源 EEPROM 信息错误,包括 FRU 信息不正确和非我司认证电源;
- 电源型号不匹配;
- 电源负载不均衡。

3. 主板故障诊断

主板是连接服务器其他硬件的枢纽,SHD 针对服务器不同机型进行个性化故障检测和诊断,最多能够支持 70+种主板故障类型。

- 二次电源故障,涵盖了服务器各类二次电源模块,包括 CPU 和板卡电源模块等;
- 外部风扇不在位故障和 PWM 转速异常;
- 温度异常,包括整机、CPU 和各类板卡温度异常;
- 电压和电流异常。

4. PCIe卡故障诊断

PCIe 卡是对服务器功能的扩展，SHD 主要针对网卡和 RISER 卡进行故障检测和诊断，根据机型差异最多能够支持 40+种 PCIe 卡故障类型。

- 网卡故障，包括自研 mLOM 卡和 25G 自研 FLOM 卡的电源、温感和在位异常；
- RISER 卡在位异常；
- NCSI 通道切换异常。

5. 阵列卡故障诊断

SHD 支持 PMC 和 LSI 阵列卡的故障检测和诊断，通过分析阵列卡上报的事件日志，能够支持 100 种阵列卡故障类型。

- RAID 卡启动异常；
- 线缆异常；
- 内存异常；
- 电池异常；
- 硬盘异常；
- 掉电保护模块异常。

3.5.4 存储可维护

1. 故障告警

能够检测到硬盘在位、故障、预故障、关键阵列、故障阵列故障。

2. SDS日志

通过 PBSI 通道，SDS 能够获取 PMC 卡相关日志信息，包括 60+种硬盘故障。(两代 RAID/HBA 卡均支持)

通过 MCTP(over i2c)通道，能够获取 LSI 卡相关日志信息，约 200+条关于 RAID 卡、BBU、硬盘、逻辑盘、背板相关故障信息日志。

3. SHD诊断

SHD(智能硬件诊断)模块，支持对 PMC/LSI 的 RAID/HBA 卡的日志信息进行诊断，诊断出相应的错误原因，并给出了相关处理措施。支持的模块有：RAID 卡、连接线缆、BBU、存储介质。共计有 100 条故障判据。诊断结果信息在 SD 卡中的\dump\shd\init\xxxx_RAID 目录下。

4. 其它

获取 SAS/SATA HDD 硬盘 SMART 信息。保存周期 30 天(1 天 1 次)。

带外 NVMe 信息获取，包括剩余(擦写)寿命。

硬盘定位点灯。

RAID 扣卡的串口日志保存。

3.5.5 故障诊断辅助功能

SHD 系统提供了一些辅助诊断功能，包括故障发生时的服务器系统截屏，BMC 设备的串口日志，IPMI 进程的调试日志，通过这些故障诊断辅助功能，能够更加清楚地知道故障发生时的现场情况。

3.5.6 故障上报

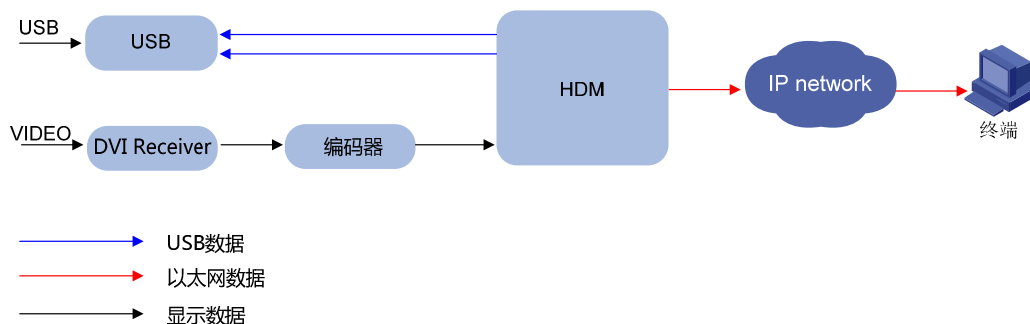
HDM 支持实时监测硬件和系统的故障状态，能够实时上报故障 SEL 日志，并通过 SNMP Trap 方式上报到远程接收服务器。通过 HDM 的一键收集功能，可以查看 SDS 日志中的/user/result.rst 诊断报告文件获取硬件故障的详细信息。

3.6 虚拟KVM和虚拟媒体

3.6.1 虚拟KVM

虚拟 KVM 是指用户在客户端利用本地的视频、键盘、鼠标对远程的设备进行监视和控制，提供实时操作异地设备的管理方式。

图22 虚拟 KVM



3.6.2 H5 KVM

H5 KVM 相对于 KVM 优势在于无需任何插件,通过浏览器 https 访问即可实现对服务器的远程管理。

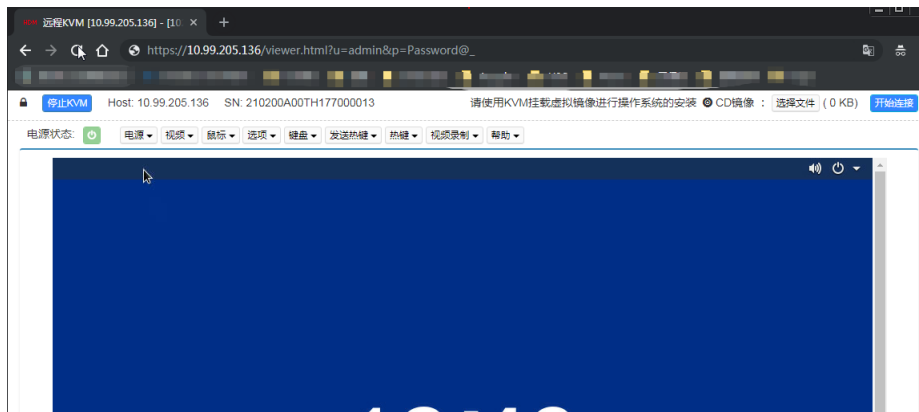
图23 H5 KVM



HDM 支持通过 IP 地址和账号密码来直接访问 H5 KVM。

输入格式如下：http://ip_addr/viewer.html?u=user_name&p=user_password。示例如下：

图24 H5 KVM 的直接访问的示例



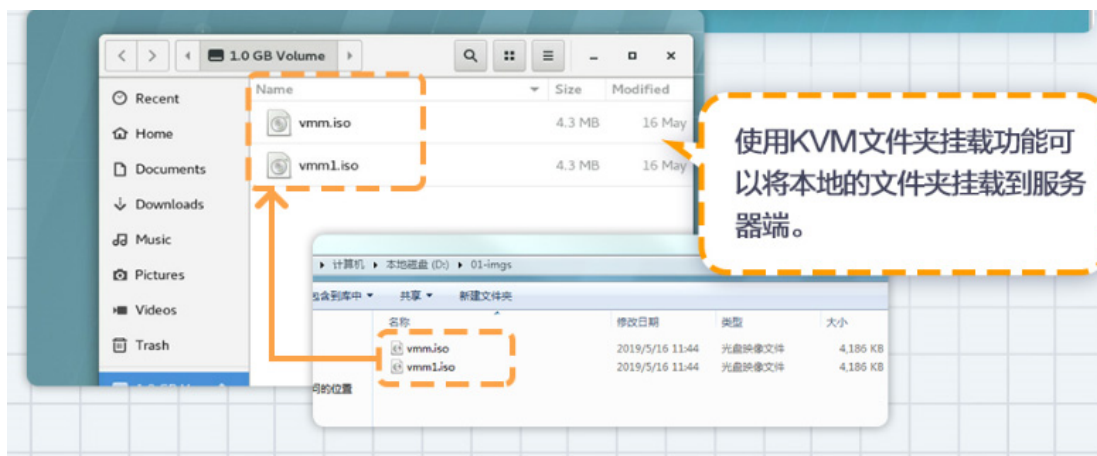
3.6.3 虚拟媒体

虚拟媒体即通过网络在服务器上以虚拟 USB 光盘驱动器和软盘驱动器的形式提供对本地媒体（光盘驱动器、软盘驱动器或光/软盘的镜像文件，硬盘文件夹）的远程访问方式；虚拟媒体数据支持 AES 128 CBC 算法加密传输。虚拟媒体的实现原理是将客户所在的本地主机的媒体设备通过网络虚拟为远端服务器主机的媒体设备。

支持的虚拟媒介有：

- DVD、CD 光驱
- ISO、IMG 文件
- 虚拟文件夹：将本地的文件夹挂载到服务器端。
- USB key

图25 虚拟文件夹实现效果



3.7 VNC会话

3.7.1 VNC介绍

VNC (Virtual Network Computing, [虚拟网络 计算机](#)) 用于传送服务端的原始图像到客户端, 该协议提供一种不用登录HDM即可访问控制服务器的方法, 即用本地主机的显示器、输入设备远程控制服务器。

VNC 系统由客户端, 服务端和 VNC 协议组成。

- VNC 服务端 VNCServer: 在 HDM 端运行, 其作用是捕获并共享服务器屏幕, 并且与系统运行状态无关。
- VNC 客户端即 VNCViewer (PC 端本地应用程序): 用于与服务器交互, 远程连接运行 VNCServer 的计算机。第三方 VNC 客户端有 RealVNC、TightVNC、NoVNC 等。

HDM 支持 IPv4、IPv6 VNC 会话, 为用户提供更为灵活的 KVM 操作方式。

3.7.2 VNC支持共享模式和独占模式

HDM 同时最多支持 2 个 VNC 会话, 且支持两种会话模式。

- (1) 共享模式: 支持打开 2 个 VNC 会话, 2 个 VNC 会话均有权限控制鼠标和键盘, 可控制 OS;
- (2) 独占模式: 当独占模式的会话连接时, 如果存在共享模式的会话, 该会话将被强制断开; 独占模式的会话存在时, 下一个会话的连接请求将被拒绝。

共享模式与独占模式由客户端指定。

3.7.3 VNC配置页面

VNC 在线会话使能默认关闭。配置页面为: 单击[安全/服务配置]菜单项, 进入服务配置页面。

The screenshot shows the HDM 1.30.06 web interface. The left sidebar contains navigation options: 信息, 健康诊断, 网络, 配置, 安全, 远程控制, 电源功耗, 维护. The main content area is titled '服务配置' and contains a table of services. A modal dialog titled '修改服务' is open over the VNC service row, showing the following configuration:

名称	非安全端口	超时	最大会话	活动会话
VNC	5900	10	2	0

3.7.4 建立非安全VNC会话

1. 在HDM上的操作

开启 VNC 服务。

2. 在VNC viewer客户端进行登录操作

通过 VNC viewer 建立 VNC 会话；打开 VNC viewer：输入<HDM_IP:非安全端口>，并输入 VNC 密码打开 VNC 会话。

(3) 对于 IPv4 地址：直接输入地址即可；

(4) 对于 IPv6 地址：需要加上[]，即[IPv6]:port。

图26 建立 IPv4 非安全 VNC 会话

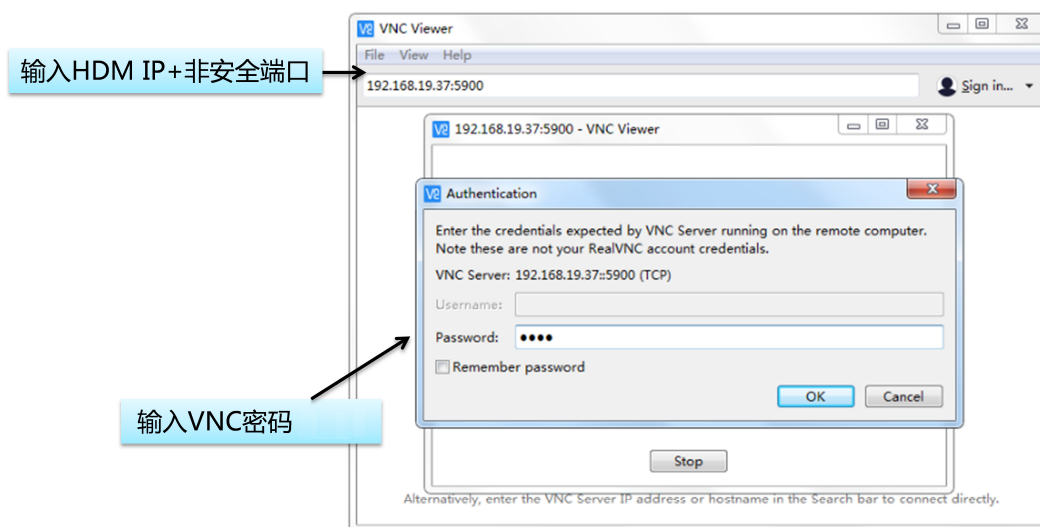
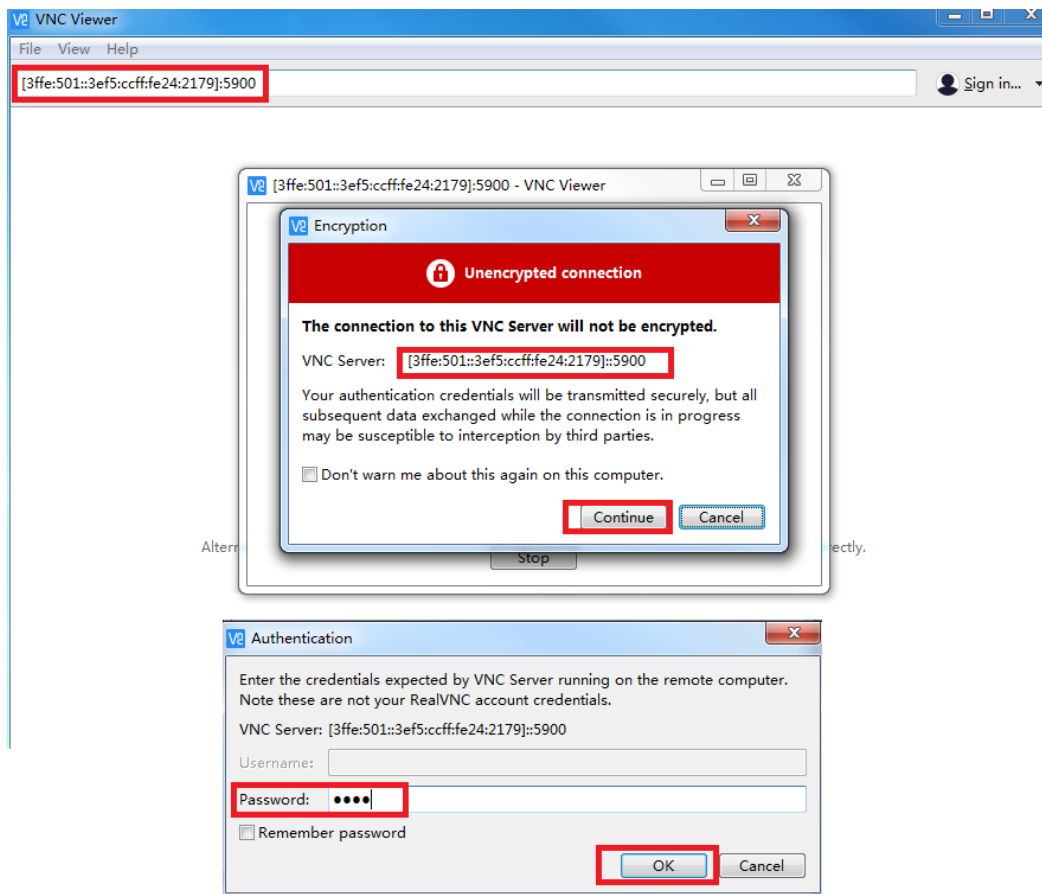


图27 建立 IPv6 非安全 VNC 会话



3. 查看会话

成功建立非安全会话后，可以在[安全/服务配置]查看到会话类型为 VNC，IP 地址为客户端 IP，且支持 IPv4 和 IPv6。

图28 查看会话

服务会话 ×

会话ID	会话类型	用户编号	用户名	IP地址	用户权限	操作
3	VNC	N/A	NA	192.168.0.235*	Administrator	删除
5	VNC	N/A	NA	3ffe:501:eeee:2:f82b:8ca1:89b6:3b9f	Administrator	删除

关闭

3.7.5 修改VNC 密码

IPMI 命令修改 VNC 密码。

```
E:\JNC>
E:\JNC>ipmitool -I lanplus -U admin -P Password@_ -H 172.16.20.19 raw 0x36 0x09 0x20 0x14 0x00 0x31 0x00 0x33 0x33 0x33
a2 63 00
```

3.8 主机管理

3.8.1 FRU及资产管理

FRU 信息指整机或部件制造过程中写入到部件存储器件中的相关信息，包括：制造商，产品名称，部件号，序列号等信息。

资产信息管理的核心是采集部件的唯一编码，HDM 支持采集服务器上相关部件的唯一编码，包括自研板卡和外购部件。

- 自研板卡从 FRU 中获取部件信息，包括唯一编码信息。
- 外购卡，HDM 从 BIOS 或其它带外方法获取相关信息。

不同部件唯一编码信息获取方法不一样，下表列出了相关部件唯一编码信息的确定策略

部件名称	可获取唯一编码
CPU	PPIN
DIMM	SN
网卡	Mac
电源	SN
主板	Board Serial Number
GPU	SN
NVMe	SN
硬盘	SN

3.8.2 系统启动项

系统启动项用于配置服务器的下一次启动模式和启动设备，以及设置的有效期。

3.8.3 风扇调速

HDM 支持风扇线性调速和更为精确的 PID 调速两种调速方法。

1. MS线性调速

MS 调速算法简单，直接根据温度以及 xml 配置文件来决定出风扇的转速。下图为示例的 xml 配置文件。

```

<algorithm1>
  <enable>true</enable>
  <type>ms</type>
  <args>
    <10>80</10>           //10° 时风扇为 80PWM
    <20>80</20>           //20° 时风扇为 80PWM
    <25>95</25>           //25° 时风扇为 95PWM
    <27>100</27>          //27° 时风扇为 100PWM
    <28>110</28>          //28° 时风扇为 110PWM
    <30>120</30>          //类推直到 high 的限制点
    <35>170</35>
    <40>230</40>
    <45>255</45>
    <128>255</128>
  </args>
  <setp>40</setp>
  <limit>
    <low>16</low>
    <high>255</high>
  </limit>
/algorithm1

```

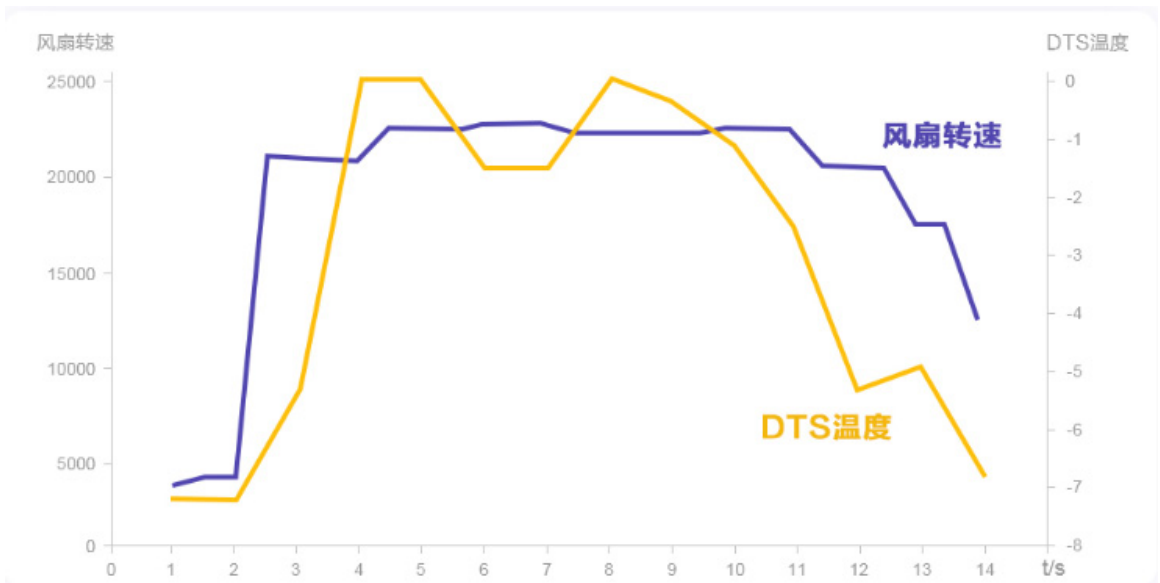
2. PID调速

PID 风扇调速通过调速参数配置 XML 文件中传感器调速参数以及传感器温度, 实时计算出风扇转速。其优点是能够更加精准的进行风扇转速控制。

PID 算法如下:

$$u(t) = kP \left(e(t) + \frac{1}{TI} \int e(t) dt + TD * \frac{de(t)}{dt} \right)$$

下图为 PID 算法调速效果仿真图。从中可以看到随着 DTS 温度的升高, 风扇转速也会相应的增加, 温度降低风扇转速也会相应的降低。

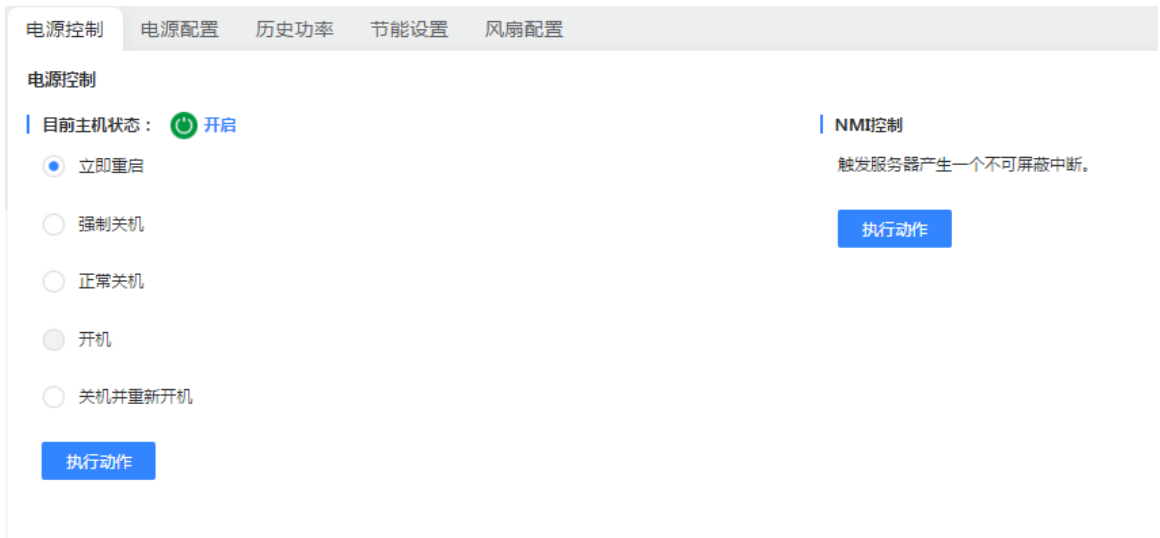


3.9 智能电源和能耗管理

3.9.1 电源控制

电源控制界面提供对服务器的电源控制方式，如图所示。

图29 电源控制页面



服务器电源控制方式包括：立即重启、强制关机、正常关机、开机、关机并重新开机。

- 立即重启：表示对服务器进行冷复位，即：HDM 直接拉 PCH 使系统复位，绕过正常的操作系统关闭流程。
- 强制关机：表示对服务器进行关机，无需等待 OS 响应，绕过正常的操作系统关闭流程，效果相当于长按服务器面板上的电源按钮。
- 正常关机：表示对服务器进行安全关机，HDM 向 OS 发送 ACPI 中断，若 OS 支持 ACPI 服务，则先走正常的操作系统关闭(将所有运行进程关闭)后下电，否则，只能等到超过下电超时时间后，HDM 将系统强制关机；效果相当于短按服务器面板上的电源按钮。
- 开机：表示对服务器进行上电。
- 关机并重新开机：表示对服务器先安全关机再开机，即：先走正常的操作系统关闭流程并关机，若设置的安全关机超时时间内不能完成关机则强制关机，最后再开机。
- NMI：表示向 OS 触发一个 NMI 中断，以收集内核堆栈信息并输出到控制台，便于系统异常时定位。

3.9.2 功率封顶

现代数据中心一直面临的一项挑战是企业正在消耗大量的电源、空间和冷却成本。而随着能源需求以及能源和冷却成本的大幅度上涨，日益增长的可用能源的容量预计在未来几年里将跟不上需求的增长。对于当前的数据中心来说，最急需解决的问题就是通过技术创新实现节能降耗。在传统的数据中心中，客户为保证数据中心无间断运行，往往要耗费巨资来建设一套额外的电力基础设施。此外，IT 管理员通常会以过度能源供应，来确保电力供应。HDM 提供的功率封顶技术可以通过有效地对每一台服务器能耗的准确控制，避免了能源的过度供应，有效地将能源中过度供应的部分能源用于数据中心扩容。

功率封顶功能通过设置系统的功率预期上限，当系统功率超过此上限值后，引导特定动作发生，从而保证机箱整体功率的合理分配。

封顶失败进一步动作包括：

- 记录事件：封顶失败后在系统事件文件中记录一条日志，默认执行。
- 关机（可选）：封顶失败后，系统将执行强制下电操作。

图30 电源配置-功率配置

The screenshot shows the 'Power Configuration' (功率配置) tab within the 'Power Control' (电源控制) section. It features three main settings:

- 功率封顶启用 (Power Capping Enabled):** A radio button interface with '关闭' (Off) selected and '开启' (On) unselected.
- 功率封顶值(W) (Power Capping Value (W)):** A text input field containing '500', with a note indicating the range is '范围为150-800整数' (Range is 150-800 integers).
- 功率封顶失效是否关机 (Power Capping Failure to Shut Down):** A radio button interface with '是' (Yes) selected and '否' (No) unselected.

A blue '保存' (Save) button is located at the bottom of the configuration area.

3.9.3 电源主备

在满足业务功耗前提下，将部分电源设置为热备用，提升电源功率转换效率。

在满足业务功耗情况下，将部分电源的输出电压降低 0.3V，通过电压差抑制备用电源电流输出，由主用电源提供系统供电；使电源处于热备用状态，一旦有主用电源异常时，备用电源平滑切换为主用电源投入供电，不影响业务。

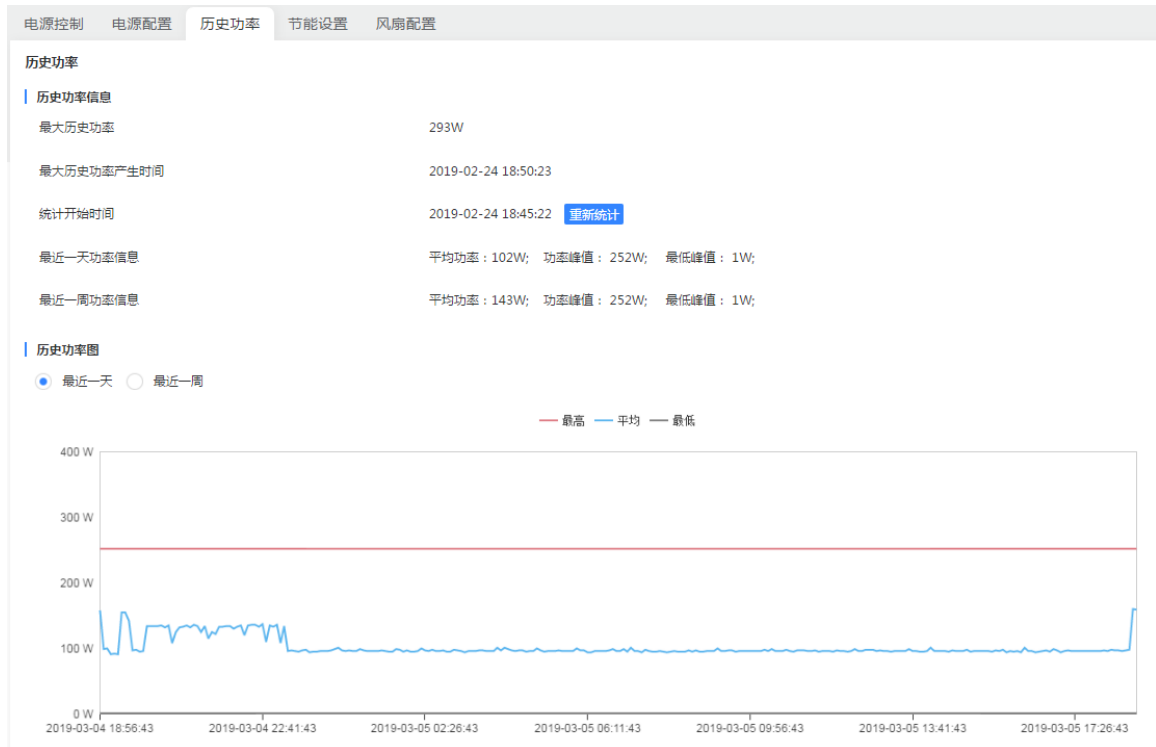
图31 主备配置

电源序号	当前状态	型号	序列号	最大功率(W)	电源输入模式	主备情况	操作
1	在位	PSR800-12A	210213A05PH17B000017	800	No input	主电源	设为备用
2	在位	PSR800-12A	210213A05PN164000068	800	AC	主电源	设为备用

3.9.4 历史功率统计

HDM 可以提供准确的能耗监测并且能通过曲线提供统计，从而使管理员能够通过能耗监测装置深入了解实际电力及散热资源的使用情况。用户可以根据历史数据对服务器节能进行优化。

图32 查看历史功率



3.9.5 设置电源性能模式

一键设置电源性能模式，节能优先或性能优先。满足不同客户或不同场景对服务器的性能、功耗、噪声等有不同需求。

图33 设置电源性能模式



3.9.6 设置节能

通过调节 CPU 的最高工作频率（P-state）和空闲工作时间（T-state）可以降低系统能耗。支持多种调节等级，操作灵活，满足不同产品需求。

图34 设置节能



3.9.7 AC恢复配置

AC 恢复配置用于配置服务器通电后系统的启动策略。包括：

- 总是开启：通电后，服务器系统会自动启动。

- 总是关闭：通电后，服务器系统保持关闭状态。
- 上一次电源状态：通电后，服务器系统会恢复到上次断电前的状态。服务器缺省处于此模式。

开机延迟：开机延迟时间。可以配置：0，15s，30s，45s，60s，以及随机(0~120s)。开机延迟可以用于服务器的错峰上电，降低机房开机过程中的瞬时功耗。

3.10 RAID带外配置

HDM 支持存储控制卡的状态查看，并可以对 LSI 卡(9300 9310 除外)存储卡进行创建逻辑盘操作。RAID 带外配置管理依赖 RAID 控制器 firmware 的能力。带外配置原理如下图所示。

图35 带外配置原理

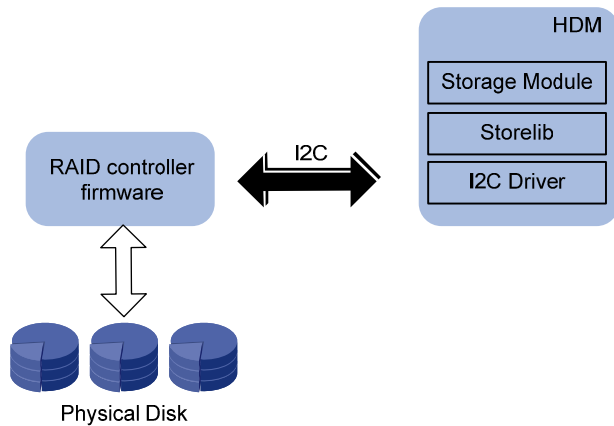


图36 硬盘信息查询

远程控制台 UID灯控制 系统启动项 远程镜像挂载 RAID配置

RAID信息 物理盘管理 逻辑盘管理

RAID-LSI-9361-8i(1G)-A1-X (SLOT 3)

槽位号	BIOS下编号	状态	属性	容量	操作
Front 2	2	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	Unconfigured Good Unconfigured Bad
Front 3	3	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	Unconfigured Good Unconfigured Bad
Front 4	4	Unconfigured Good	6.0 Gbps SATA HDD	931.51GiB	Unconfigured Good Unconfigured Bad
Front 5	5	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	Unconfigured Good Unconfigured Bad
Front 6	6	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	Unconfigured Good Unconfigured Bad
Front 7	7	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	Unconfigured Good Unconfigured Bad

图37 逻辑盘配置页面

The screenshot shows the RAID configuration interface. At the top, there are navigation tabs: 远程控制台, UID灯控制, 系统启动项, 远程镜像挂载, and RAID配置. The RAID配置 tab is active. Below it, there are sub-tabs: RAID信息, 物理盘管理, and 逻辑盘管理. The 逻辑盘管理 tab is selected.

Under 逻辑盘管理, there is a section for creating a logical disk: RAID-LSI-9361-8i(1G)-A1-X (SLOT 3). The settings are as follows:

- 名称: [Empty text box]
- RAID级别: 0
- 条带大小: 256 KB
- 初始化类型: No
- 组个数: 1
- 每个Span的成员盘数: [Empty text box]
- 读策略: Read ahead
- 写策略: Write back
- IO策略: Direct
- 物理盘缓存策略: Unchanged
- 访问策略: Read/Write
- 容量: [Empty text box] Mi

Below the settings is a section for selecting physical disks: 选择物理盘. It contains a table with the following data:

<input type="checkbox"/>	槽位号	BIOS下编号	状态	属性	容量	组ID
<input type="checkbox"/>	Front 2	2	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	选项为空 -
<input type="checkbox"/>	Front 3	3	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	选项为空 -
<input type="checkbox"/>	Front 4	4	Unconfigured Good	6.0 Gbps SATA HDD	931.51GiB	选项为空 -
<input type="checkbox"/>	Front 5	5	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	选项为空 -
<input type="checkbox"/>	Front 6	6	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	选项为空 -
<input type="checkbox"/>	Front 7	7	Unconfigured Good	12 Gbps SAS HDD	5.46TiB	选项为空 -

At the bottom left of the page, there is a 保存 (Save) button.

创建逻辑盘后，在 RAID 信息页面查看信息。点击<查看>按钮跳转到[系统信息/硬件信息]的存储页签查看更为详尽的信息。

图38 逻辑盘信息查询

The screenshot shows the RAID configuration interface, specifically the RAID information page. The RAID配置 tab is active, and the RAID信息 sub-tab is selected.

Under RAID信息, there is a section for RAID-LSI-9361-8i(1G)-A1-X (SLOT 3). It contains a table with the following data:

ID	状态	RAID级别	容量	成员盘数	成员盘槽位号	操作
0	Optimal	RAID 1	5.457TiB	2	Front 0, Front 1	查看 删除

图39 存储信息页面

The screenshot displays the storage information page with the following components:

- Navigation Bar:** Includes tabs for 整体概况, 硬件信息 (selected), FRU信息, 固件信息, 传感器信息, 实时监控, 系统资源监控, and 一键收集. Below these are sub-tabs for CUPS, 处理器, 内存, 存储 (selected), 风扇, 电源, 网卡, PCIe卡, and NVMe.
- RAID Card Section:**
 - 逻辑视图 (Logical View):**

型号	RAID-LSI-9361-8i(1G)-A1-X
固件版本	4.680.00-8292
序列号	SK71181307
缓存容量	1GB
支持RAID级别	0/1/5/6/10/50/60
Flash卡	不在位
超级电容	不在位
 - 物理视图 (Physical View):**

型号	RAID-LSI-9361-8i(1G)-A1-X
固件版本	4.680.00-8292
序列号	SK71181307
缓存容量	1GB
支持RAID级别	0/1/5/6/10/50/60
Flash卡	不在位
超级电容	不在位
- 逻辑驱动器 0 (Logical Drive 0):**

状态	正常
级别	RAID 1
容量	5.457TiB
启动盘	是
物理盘缓存策略	关闭
- 前部 物理驱动器 0 (Front Physical Drive 0):**

槽位号	Front 0
BIOS下编号	0
主机下编号	0
状态	已配置
厂商型号	HGST HUS726060AL5210
固件版本	A907
序列号	K1H33AHD
属性	12 Gbps SAS HDD
- 前部 物理驱动器 1 (Front Physical Drive 1):**

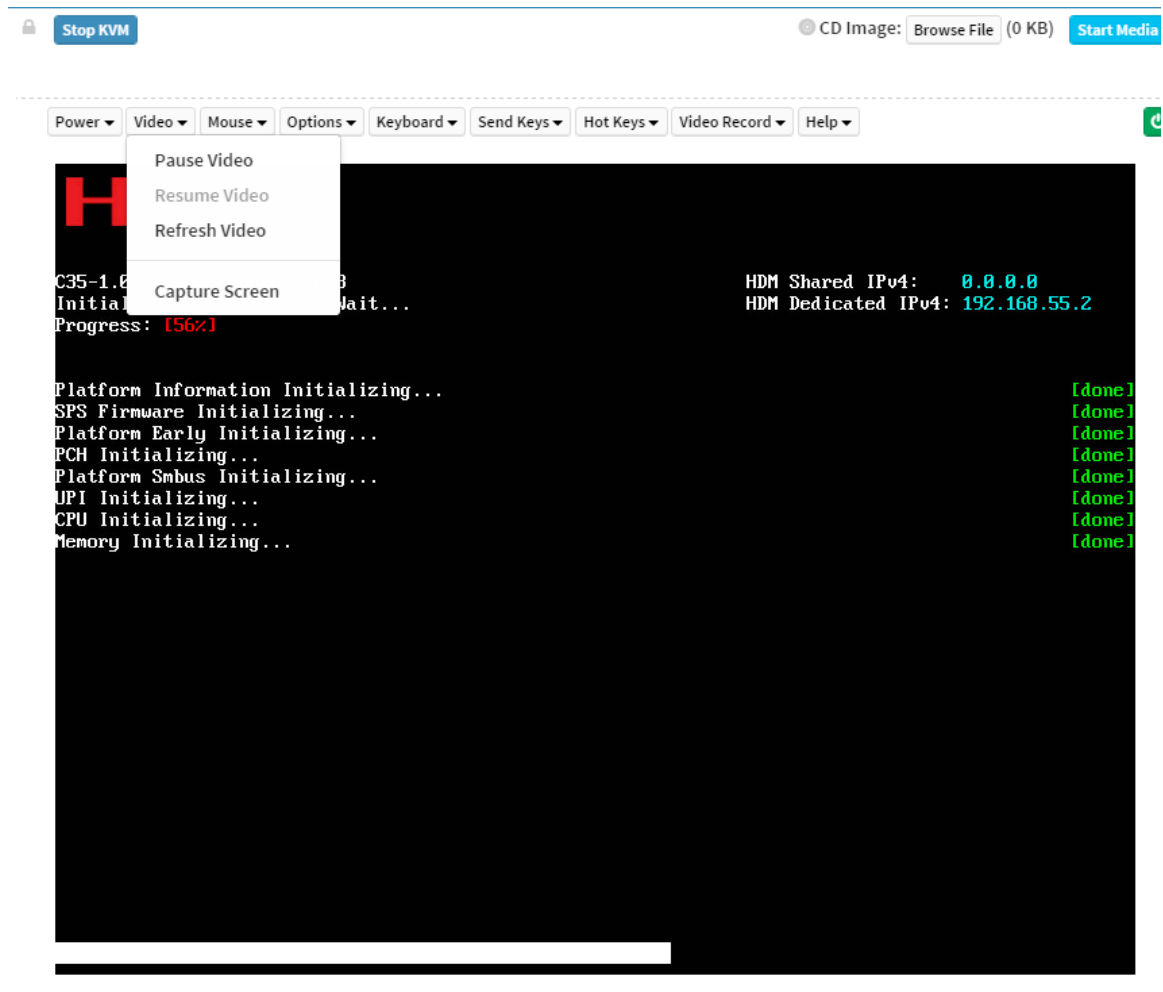
槽位号	Front 1
BIOS下编号	1
主机下编号	1
状态	已配置

3.11 截屏和录像回放

3.11.1 截屏

在 KVM 界面可以开启截屏功能，截屏图像格式为 JPEG 格式，录像文件保存在本地 PC（打开 KVM 的 PC）。如图所示。

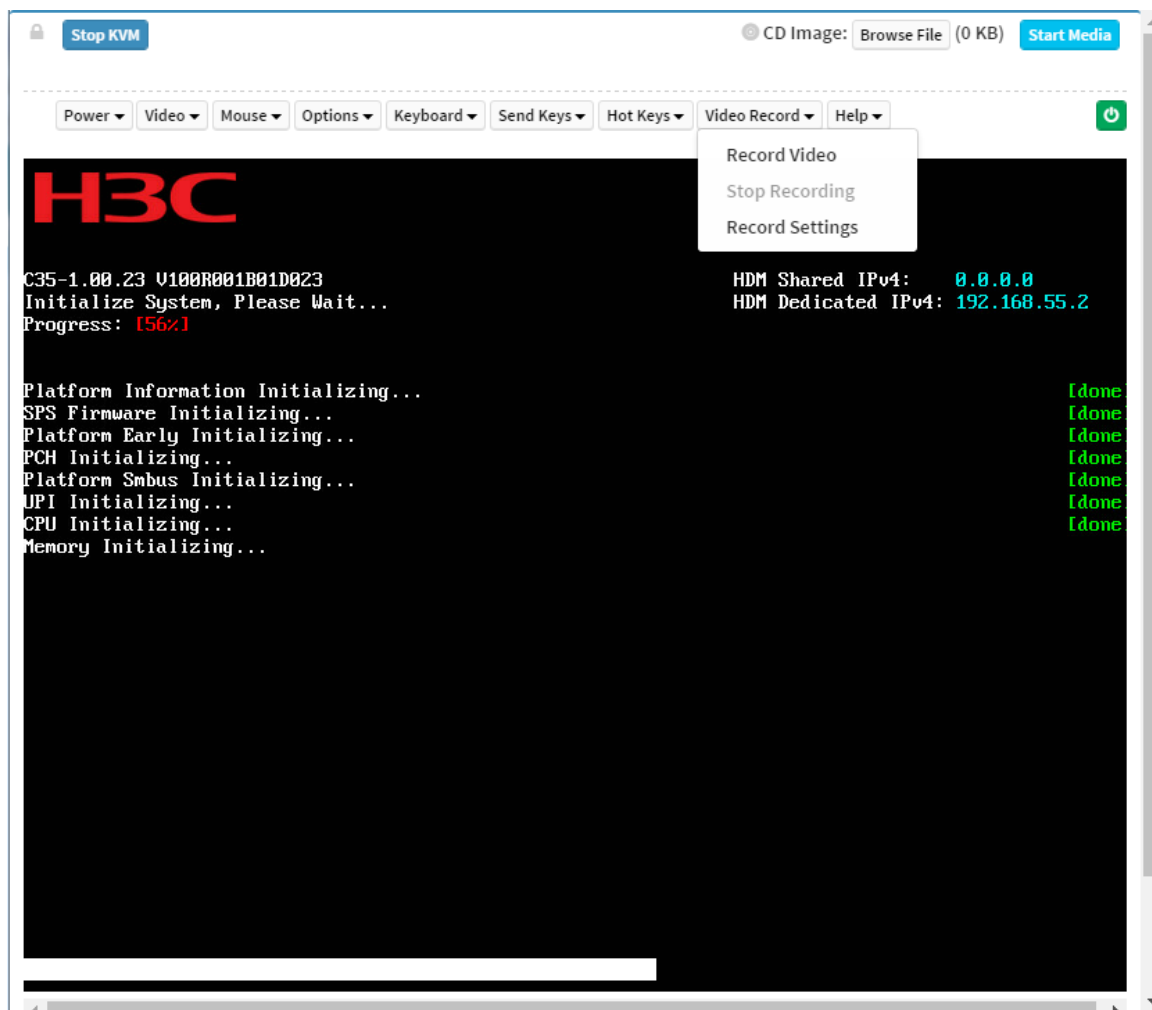
图40 KVM 界面的截屏功能



3.11.2 录像回放

在 KVM 界面可以开启录像功能,录像格式为 AVI 格式,录像文件保存在本地 PC(打开 KVM 的 PC)。如图所示。当用户出于安全或者其他需要,要将虚拟 KVM 操作过程记录下来时,可以通过启动屏幕录像功能来实现。屏幕录像功能启动后,虚拟 KVM 控制台会自动将屏幕上的所有显示和操作都记录到自定义视频格式文件中。录像文件在本地可以通过播放器来播放。

图41 KVM 界面的视频录制



3.12 可维护性

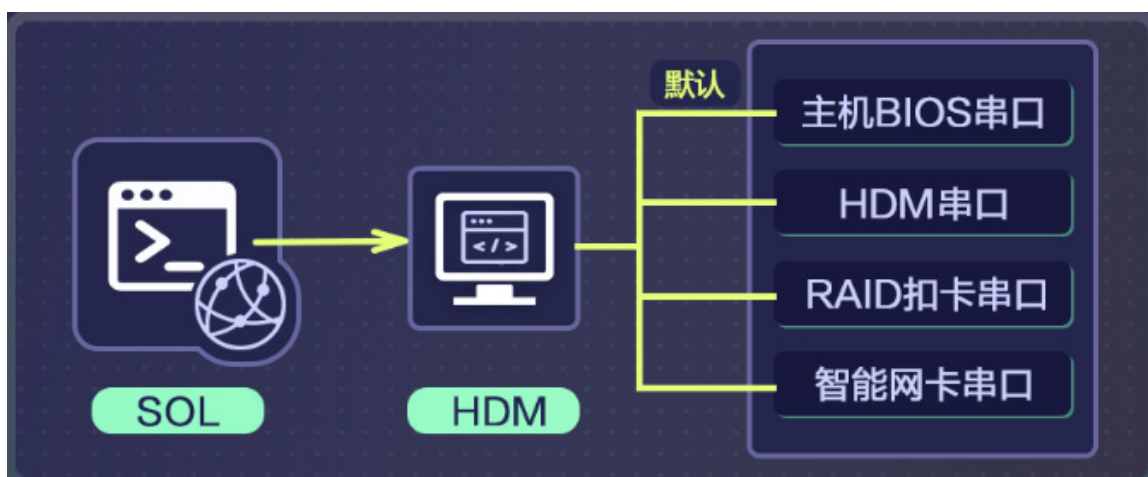
3.12.1 串口切换

串口切换功能允许选择面板串口/SOL 和内部主机相关部件连接，以对内部指定部件进行监控。

1. 基于SOL的串口切换

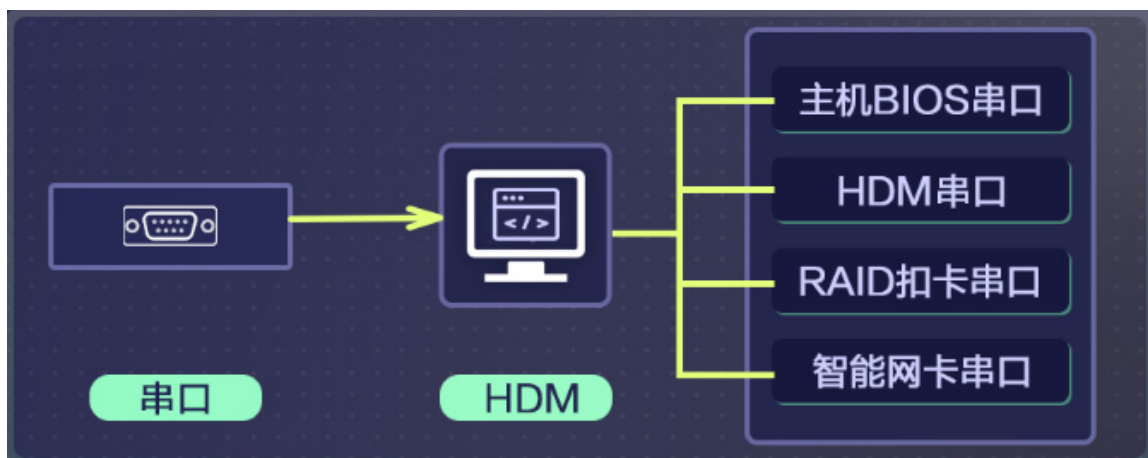
HDM 提供系统串口重定向（SOL: Serial Over LAN）功能，即将原本只能从本地串口线输出的系统串口数据重定向到网络设备输出，并能接受远程网络设备的输入。如图所示原理，网管人员在远程通过网络终端就可以轻松的查看系统串口实时输出数据，并能对系统进行操作干预，跟在近端使用系统串口效果一样。

图42 SOL 串口切换



2. 面板串口的串口切换

通过 IPMI 命令可以配置本地的面板串口任意连接到相关部件串口，节省了服务器的面板空间。



3. 串口信息记录

HDM 可以提供串口信息记录功能，该功能将部件的实时串口数据记录到内部存储介质中。当部件发生故障时，可以通过一键导出功能导出串口日志信息进行分析。

目前 HDM 支持对 BIOS 日志、RAID 扣卡日志进行日志保存。

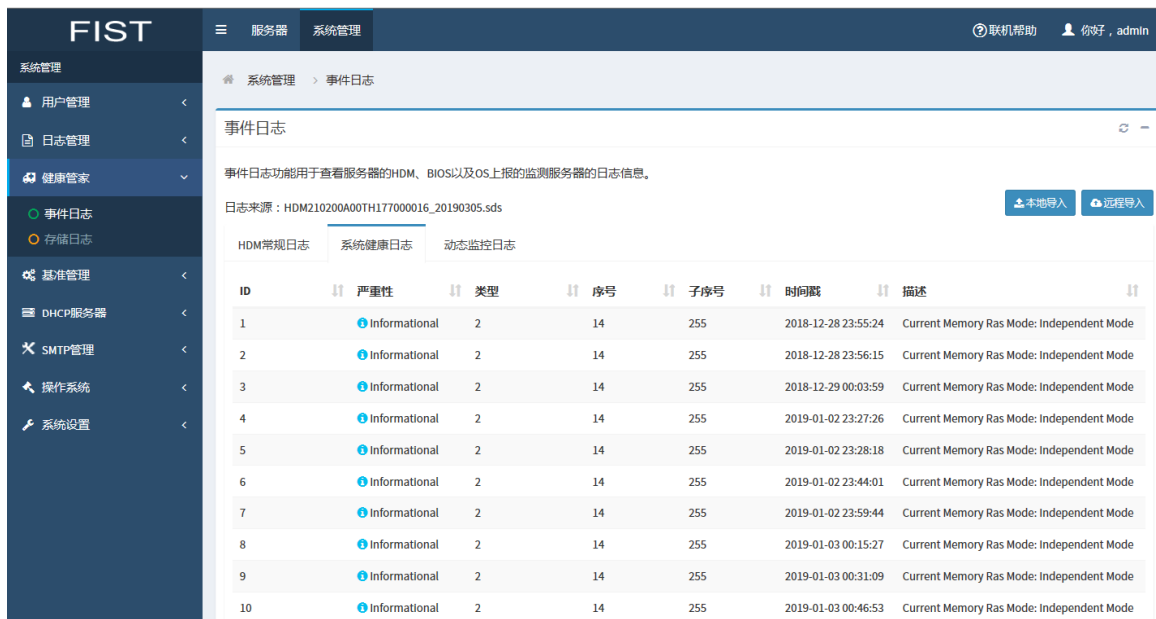
3.12.2 一键收集

本功能用于收集服务器的日志信息、硬件信息、故障诊断信息。通过 FIST 可以解析事件日志和存储日志，也可以查看 CSV 格式日志，了解服务器运行状态。可以添加联系人信息，用于日志解析问题咨询，方便信息对接，提高运维工作效率。

图43 一键收集



图44 FIST 健康管家解析 SDS 日志



3.12.3 操作日志

操作日志包含审计日志、固件更新日志、硬件更新日志和配置日志。

- 审计日志记录访问 HDM 的操作信息，包括：通过浏览器登录 HDM、启动远程控制台等信息。
- 固件更新日志记录固件更新的操作信息及操作结果。
- 硬件更新日志：记录硬件更新的操作信息及操作结果。
- 配置日志记录用户的配置操作及操作结果。

日志包含时间，主机名和详细信息描述。操作日志界面如图所示。

图45 操作日志界面

事件日志	操作日志	蓝屏快照	录像回放	开机自检码		
日志列表						
所有类型	所有等级	高级设置 查看CSV				
所有类型	时间	用户名	接口类型	IP地址	主机名	描述
审计日志						
固件更新日志	3-05 20:03:25:50.770	admin	WEB	192.168.50.37	HDM210200A00TH177000016	Performed graceful power-off successfully.
配置日志						
硬件更新日志						
	998 2019-03-05 20:22:37.205	admin	WEB	192.168.50.37	HDM210200A00TH177000016	HDM flash successfully
	997 2019-03-05 20:20:32.801	admin	WEB	192.168.50.37	HDM210200A00TH177000016	From 1.11.22 to 1.11.23
	996 2019-03-05 20:20:32.800	admin	WEB	192.168.50.37	HDM210200A00TH177000016	HDM verify image successfully
	995 2019-03-05 20:20:03.277	admin	WEB	192.168.50.37	HDM210200A00TH177000016	HDM prepare successfully
	994 2019-03-05 20:20:01.602	admin	WEB	192.168.50.37	HDM210200A00TH177000016	HDM set flash type successfully
	993 2019-03-05 20:20:01.438	admin	WEB	192.168.50.37	HDM210200A00TH177000016	Set transfer protocol for firmware update to HTTP/HTTPS successfully.
	992 2019-03-05 20:02:18.557	admin	LAN	192.168.50.37	HDM210200A00TH177000016	HTTPS login from IP:192.168.50.37 user:admin
	991 2019-03-05 19:58:22.412	admin	LAN	192.168.50.37	HDM210200A00TH177000016	HTTPS session timeout from IP:192.168.50.37 user:admin
	990 2019-03-05 19:40:56.014	op123	LAN	192.168.0.91	HDM210200A00TH177000016	HTTPS session timeout from IP:192.168.0.91 user:op123

3.12.4 事件日志

事件日志用于记录、查看服务器传感器产生的各种事件。事件按严重性分成如下 4 个等级：

- 通知：表示对系统不会产生影响的事件，例如正常的状态变化，告警事件解除。
- 次要：表示对系统不会产生大的影响，需要尽快采取相应的措施，防止故障升级。
- 重要：表示对系统产生较大的影响，有可能中断部分系统的正常运行，导致业务中断。
- 紧急：表示可能会使服务器下电，系统中断。需要马上采取相应的措施进行处理。

在事件日志页面可以通过传感器名称，事件等级，时间参数来快速筛选查询到所需要的事件日志。

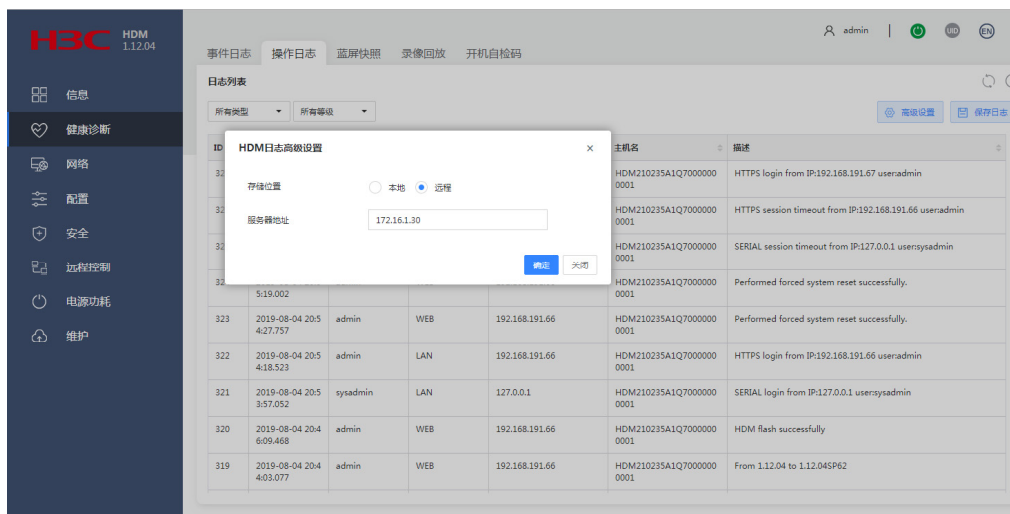
图46 事件日志界面

ID	时间戳	传感器名称	传感器类型	状态	级别	描述
1462	2018-09-20 22:51:37	Microcontroller	Microcontroller / Coprocessor	触发	通知	Transition to running
1461	2018-09-20 22:51:30	ACPI_State	system_acpi_power_state	触发	通知	S5/G2 soft-off
1460	2018-09-20 22:51:30	ACPI_State	system_acpi_power_state	触发	通知	LPC Reset occurred
1459	2018-09-20 22:51:29	Button	Button / Switch	触发	通知	Power button pressed---Virtual button---Power off command
1458	2018-09-20 22:51:03	Button	Button / Switch	触发	通知	Power button pressed---Virtual button---Soft off command
1457	2018-09-20 22:50:59	Button	Button / Switch	触发	通知	Power button pressed---Virtual button---Soft off command
1456	2018-09-20 22:50:59	System	system_event	解除	通知	Transition to power off
1455	2018-09-20 22:50:58	System	system_event	解除	通知	Transition to power off
1454	2018-09-20 22:50:58	Power	power_unit	触发	次要	Power limit is exceeded over correction time limit
1453	2018-09-20 22:50:58	Power	power_unit	触发	次要	Power limit is exceeded over correction time limit
1452	2018-09-20 22:50:42	System	OEM Record	触发	通知	POST Info---Current Memory Ras Mode: Independent Mode
1451	2018-09-20 22:50:24	ACPI_State	system_acpi_power_state	触发	通知	LPC Reset occurred
1450	2018-09-20 22:50:14	ACPI_State	system_acpi_power_state	触发	通知	S0/G0 working
1449	2018-09-20 22:50:08	Button	Button / Switch	触发	通知	Power button pressed---Virtual button---Power on command
1448	2018-09-20 20:25:57	Microcontroller	Microcontroller / Coprocessor	触发	通知	Transition to running

3.12.5 远程Syslog

HDM 支持远程 syslog 服务器获取操作日志和事件日志。远程 syslog 服务器地址支持 IPv4 和 IPv6 格式。

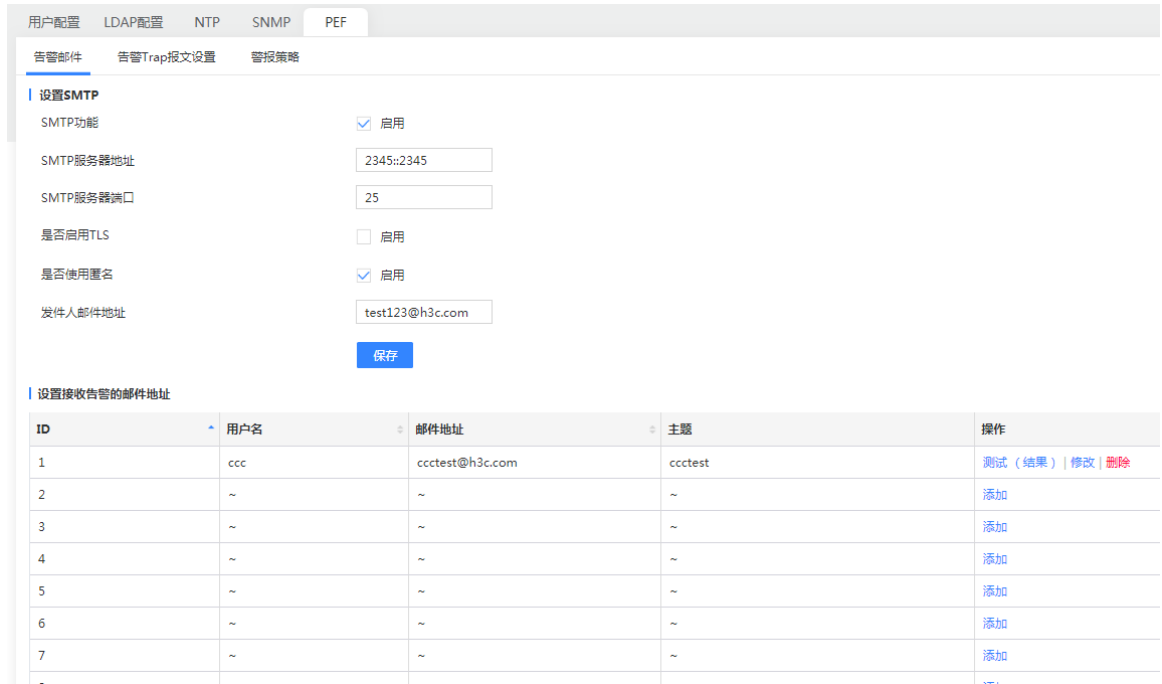
图47 远程 syslog 服务器配置



3.12.6 电子邮件告警

HDM 可设置将服务器产生的事件日志通过“电子邮件警报”发送给指定用户，帮助用户监控服务器的运行状态。SMTP 服务器地址支持 IPV4 和 IPV6 地址。支持匿名/认证用户发送，告警信息最多支持发送给 15 个用户用于服务器监控。

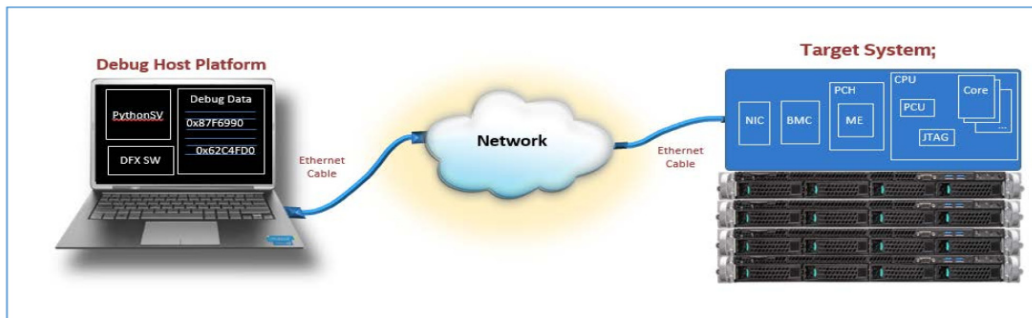
图48 SMTP 配置



3.12.7 Remote XDP

针对 Intel CPU, 用户无需购买 Intel 专用调试器进入机房和服务器连接, 远程即可对 CPU 进行 JTAG 调试, 收集服务器的 CPU、内存、PCIE、USB 等部件的寄存器信息, 以协助定位到底层硬件疑难问题。(仅 1、2 路的 Skylake 机型支持)

图49 Remote XDP 原理



使用介绍:

- (1) 开启 HDM 的 RemoteXDP 服务。
- (2) 在远程 PC 上安装 Intel 提供的 openIPC。
- (3) 安装 python, 下载 Intel 提供的 Cscripts。
- (4) 打开 CMD 窗口, 在 cscripts 目录下执行如下图命令即可完成调试环境的建立。

```

SKX_Cscripts
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

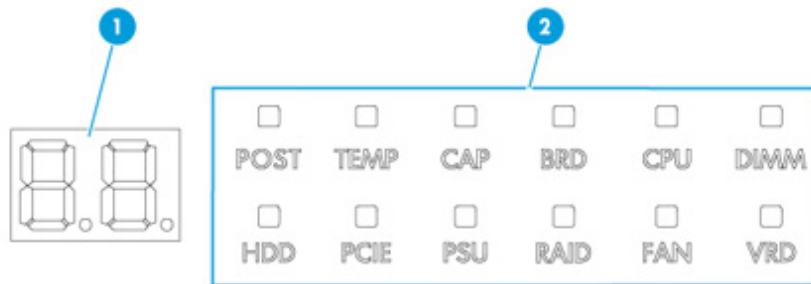
F:\557704_CScripts_SKX_Server.1.18.Rev.609586\cscripts>startCscripts.py
Using Intel Restricted Secret and Confidential commands
Target Configuration: SKX_renodedebugging
Note: Target reset has occurred
Note: Clock Restore occurred
Note: Power Loss occurred
Warn: No CPU power detected on pod 0, skip detecting tap devices on th
is pod!
[SKX_C27_T0] HLI Instruction break at 0x38:0000000000E526A
[SKX_C27_T1] HLI Instruction break at 0x38:0000000000E526A
[SKX_C26_T0] HLI Instruction break at 0x38:0000000000E526A
[SKX_C26_T1] HLI Instruction break at 0x38:0000000000E526A
[SKX_C25_T0] HLI Instruction break at 0x38:0000000000E526A
[SKX_C25_T1] HLI Instruction break at 0x38:0000000000E526A
[SKX_C24_T0] HLI Instruction break at 0x38:0000000000E526A
[SKX_C24_T1] HLI Instruction break at 0x38:0000000000E526A
[SKX_C22_T0] HLI Instruction break at 0x38:0000000000E526A
[SKX_C22_T1] HLI Instruction break at 0x38:0000000000E526A
[SKX_C21_T0] HLI Instruction break at 0x38:0000000000E526A
[SKX_C21_T1] HLI Instruction break at 0x38:0000000000E526A

```

3.12.8 诊断面板

诊断面板可以直接的显示出服务器异常，并能直接指示到具体故障设备，其故障显示与 HDM 的事件日志记录同步。

图50 诊断面板示意图



(1):故障代码 (2):故障指示灯

面板功能介绍：

- 颜色指示：橙灯/红灯则表示对应组件有故障告警，绿灯表示组件状态正常。
- 故障数码管：一般用于指示具体是哪个部件。
- 支持设备：支持 POST/TEMP/CAP/BRD/CPU/DIMM/HDD/PCIE/PSU/RAID/FAN/VRD 大类的故障。
- 多种故障：若多个组件同时出现故障时，诊断面板以 4 秒为周期循环显示全部故障。

故障组件信息说明：

- POST：表示系统 POST 期间有错误发生，POST 异常中止。
- TEMP：表示对应组件温度超过设定阈值。
- CAP：表示系统功率超出当设置的功率封顶限额。
- BRD：表示设备上对应的 SMC/PDB/Node/mLOM 出现故障。
- CPU：表示对应的 CPU 上出现错误告警。

- DIMM:表示对应的通道上内存条出现告警。
- HDD: 表示对应背板上硬盘出现错误告警。
- PCIE: 表示对应的槽位上 PCIE 卡出现错误告警。
- PSU: 表示对应的哪个电源模块出现错误告警。
- RAID: 表示相应的 RAID 卡插槽上 RAID 卡状态提示。
- FAN: 表示对应的风扇出现错误告警。
- VRD: 表示对应的 SMC/PDB/CPU 等模块出现电源错误告警。

3.13 域管理和目录服务

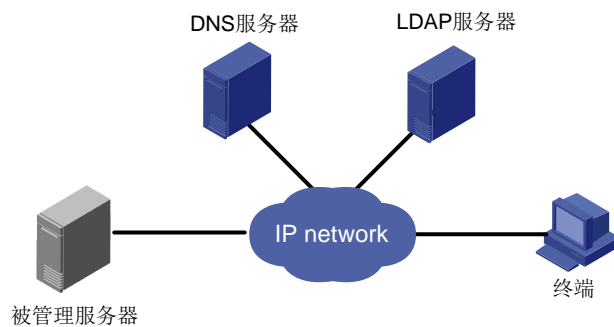
3.13.1 域管理

用户可以将所有被管理服务器加入一个统一的管理域并使用域名来访问被管服务器的 HDM。

3.13.2 目录服务

LDAP（Lightweight Directory Access Protocol）是一个访问在线目录服务的协议。LDAP 目录中可以存储例如电子邮件地址、邮件路由信息等各种类型的数据，为用户提供更集中、更便捷的查询。按照如图所示原理，启用 HDM 的目录服务，可以将所有 HDM 的用户管理，权限分配，有效期管理都集中到目录服务器上，避免大量的重复性用户配置任务，提高管理效率。另外将用户集中到目录服务器上，也能大大提高 HDM 智能管理系统的安全性。

图51 LDAP 服务器原理图



LDAP 标准优点：

- 可扩展性：可以在所有 HDM 上同时动态支持 LDAP 服务器上新增账户的管理。
- 安全性：用户密码策略都在 LDAP 服务器上实施。
- 实时性：LDAP 服务器上账户的任何更新都将立即应用到所有的 HDM。
- 高效性：可以将所有 HDM 智能管理系统的用户管理，权限分配，有效期管理都集中到目录服务器上，避免大量的重复性用户配置任务，提高管理效率。

支持性：支持 SSL 加密机制。

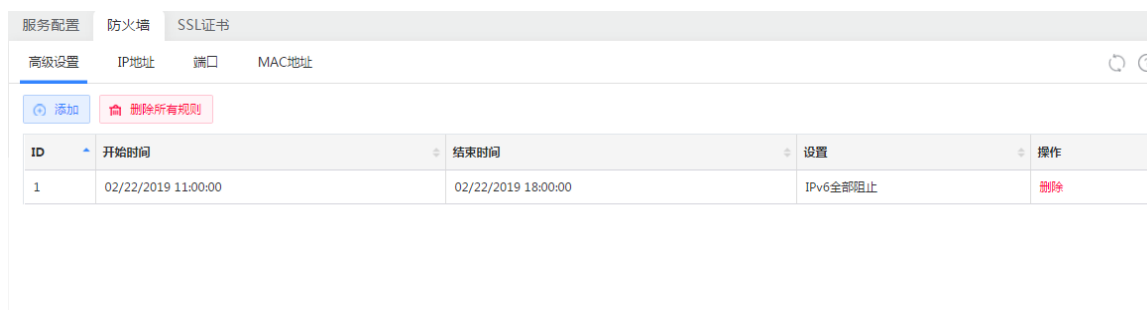
3.14 安全管理

3.14.1 防火墙

基于安全考虑，HDM 提供防火墙特性以实现基于场景的登录管理。HDM 可以从时间、IP 地址和 IP 版本（IPV4/IPV6）、MAC、端口、协议（TCP/UDP）五个维度将服务器管理接口访问控制在最小范围；目前该特性适用于 WEB、SSH、SNMP V1/V2C/V3、IPMI LAN 接口的登录限制。

由用户根据需要设置登录规则的白名单，登录时只要匹配上任意一条登录规则，即可登录，否则拒绝登录；登录规则可应用于所有本地用户和 LDAP 用户组。

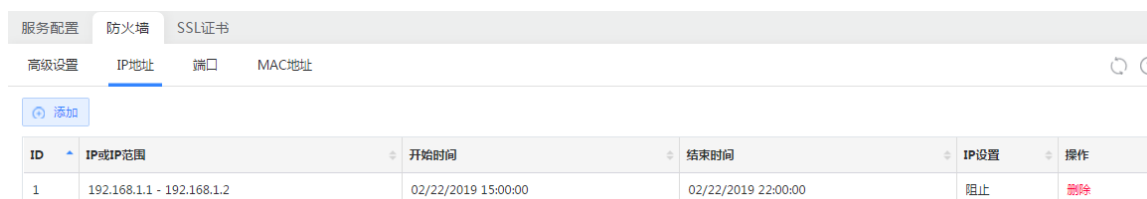
图52 高级设置



The screenshot shows the '高级设置' (Advanced Settings) tab for the Firewall configuration. It displays a table with one rule:

ID	开始时间	结束时间	设置	操作
1	02/22/2019 11:00:00	02/22/2019 18:00:00	IPv6全部阻止	删除

图53 阻止指定 IP 地址登录



The screenshot shows the '高级设置' (Advanced Settings) tab for the Firewall configuration. It displays a table with one rule:

ID	IP或IP范围	开始时间	结束时间	IP设置	操作
1	192.168.1.1 - 192.168.1.2	02/22/2019 15:00:00	02/22/2019 22:00:00	阻止	删除

3.14.2 账号安全

账号安全包括：密码复杂度检查、密码有效期、禁用历史密码重复次数、登录失败锁定、密码锁定时长，提示修改初始密码。在“配置->用户配置”的“高级设置”里可配置。如图所示。

图54 账户安全设置

密码规则

密码复杂度检查 开启 关闭

密码有效期 天
取值范围0~365 (整数), 0表示密码无使用期限限制

禁用历史密码 个
取值范围0~5, 1~5表示不能和前1~5次密码重复, 0表示不禁用历史密码

登录失败锁定 次
取值范围1~5, 登录失败到达次数后锁定

登录失败锁定时长 分
取值范围1~5, 锁定登录的时间

确定 关闭

- 密码复杂度检查：开启该功能后，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。
 - 密码长度为 8~16 个字符，仅支持字母、数字、空格和特殊字符 `~!@#\$%^&*()_+~=[\|};:~./<>?`，区分大小写；
 - 至少包含大写字母、小写字母和数字中的两种字符；
 - 至少包含一个空格或特殊字符；
 - 不能与用户名或用户名的倒序相同；
 - 需符合“禁用历史密码”要求。
- 密码有效期：用户密码的使用期限，临近使用期限前，HDM 会提醒用户更换密码。默认管理员不受密码有效期配置影响。
- 禁用历史密码：用户修改密码时，禁止使用设置次数内的历史密码。
- 登录失败锁定：用户登录失败的次数达到设定的次数后，系统会锁定该用户的登录。
- 登录失败锁定时长：用户由于登录失败达到登录失败锁定次数后，被系统锁定的时长。用户被锁定后，在失败锁定时长内不能登录 HDM。

3.14.3 SSL证书管理

SSL 证书管理包括上传 SSL、生成 SSL、查看 SSL。

SSL 证书信息包括：使用者、颁布者、有效时间、序列号等信息。

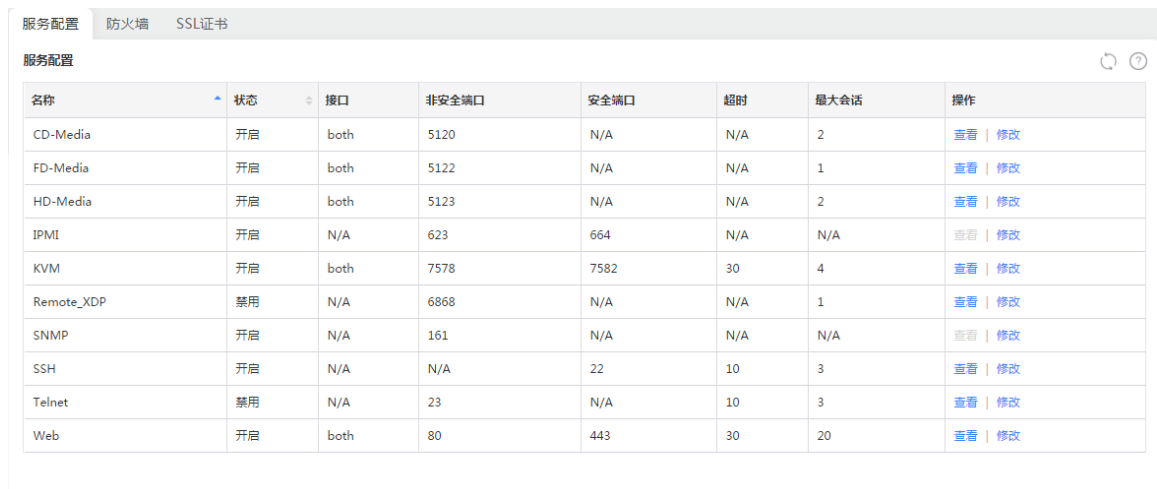
3.14.4 硬件加密

HDM 的 SOC 芯片支持硬件安全加速模块，用来加强 HDM 的安全相关功能。主要应用在认证、数据加解密等安全应用中。实现了 AES、DES、3DES、RC4、MD5、SHA1、SHA224、SHA256、HMAC-MD5、HMAC-SHA1、HMAC-SHA224 和 HMAC-SHA256 算法。

3.14.5 服务管理

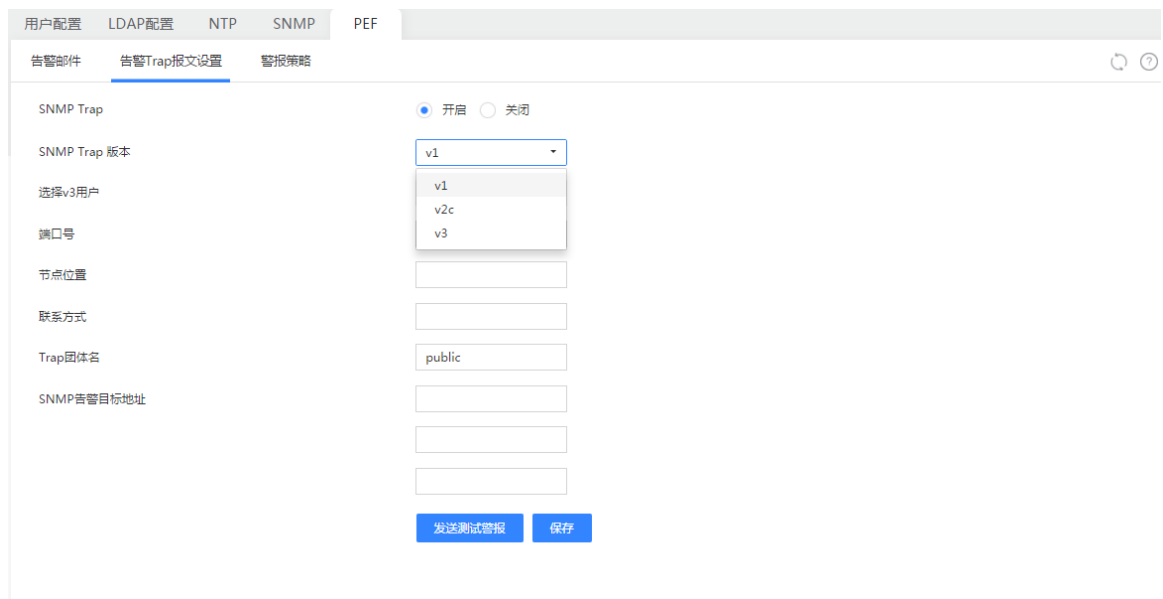
为了满足客户的业务和安全需要，HDM 提供开关来控制是否提供服务端口。HDM 支持修改的服务为：CD-Media、FD-Media、HD-Media、IPMI、KVM、Remote_XDP、SNMP、SSH、Telnet 和 Web，如图所示。

图55 HDM 服务配置



名称	状态	接口	非安全端口	安全端口	超时	最大会话	操作
CD-Media	开启	both	5120	N/A	N/A	2	查看 修改
FD-Media	开启	both	5122	N/A	N/A	1	查看 修改
HD-Media	开启	both	5123	N/A	N/A	2	查看 修改
IPMI	开启	N/A	623	664	N/A	N/A	查看 修改
KVM	开启	both	7578	7582	30	4	查看 修改
Remote_XDP	禁用	N/A	6868	N/A	N/A	1	查看 修改
SNMP	开启	N/A	161	N/A	N/A	N/A	查看 修改
SSH	开启	N/A	N/A	22	10	3	查看 修改
Telnet	禁用	N/A	23	N/A	10	3	查看 修改
Web	开启	both	80	443	30	20	查看 修改

图56 SNMP trap 配置界面



3.14.6 用户定义

随着客户对安全的重视，不同客户对管理权限的需求各异，不仅需要支持管理员、操作员和普通用户三个角色，还需要定义不同功能的权限。所以，HDM 还增加了 KVM、VMedia 和 SNMP 的权限分配。权限分配如图所示。

图57 网络权限

修改用户 ×

用户名

修改密码

密码

确认密码

用户访问 启用

网络权限

扩展权限 KVM VMedia WEB IPMI

SNMP扩展权限 开启

SNMP v3读写权限 读取 读/写

SNMP v3鉴权算法

SNMP v3加密算法

电子邮件ID

上传的SSH密钥

新的SSH密钥

3.15 固件管理

HDM 可管理的固件包括：

- 支持查询 HDM、BIOS、CPLD 固件版本；
- 支持不断电不中断业务升级 HDM 固件版本；
- 支持固件升级，且升级时 HDM、BIOS、CPLD 固件都已经进行过签名，确保镜像是完整的；
- 支持双镜像切换。

3.15.1 固件双镜像

为了提升系统可靠性，HDM 使用了固件双镜像备份技术。当在运行过程中出现 flash 误操作或者存储块损坏时，可以切换到备份镜像运行。

图58 固件双镜像

主备切换

主分区镜像版本	1.11.22
备分区镜像版本	1.11.22

[主备切换](#)

3.15.2 固件升级

支持对 HDM、BIOS、CPLD 固件升级。从兼容性考虑，建议用户将 HDM 主备镜像更新到同一个版本。

图59 固件升级页面（支持 HDM、BIOS、CPLD 固件升级）

固件升级

警告：请注意，在固件更新过程中，部分网页和服务将无法使用。请勿刷新页面。

1 更新准备 2 固件信息 3 固件更新

上传方式

固件类型

请选择固件镜像

HDM更新配置

更新后手动重置

覆盖所有配置

[下一步](#)

HDM 固件升级时支持两种生效方式（手动和自动），BIOS 固件升级支持三种生效方式（手动、自动和设置重启时间），且支持 HDM、BIOS 升级后的配置保留。

图60 固件升级页面

导入/导出配置 固件更新 重置HDM

固件更新

警告：请注意，在固件更新过程中，部分网页和服务将无法使用。请勿刷新页面。

1 更新准备 2 固件信息 3 固件更新

上传方式 本地上传

固件类型 BIOS

请选择固件镜像 浏览

BIOS更新配置

更新后立即重启

更新后 0 小时 10 分钟后重启

更新后手动重启

覆盖所有配置

配置保留 配置覆盖 强制覆盖

下一步

3.15.3 BIOS的自升级

当 BIOS 升级选择“配置保留”和“配置覆盖时”，HDM 仅上传 BIOS 的固件文件到 SD 卡，后续主机重启时，BIOS 会通过 HDM 从 SD 卡中获取固件文件，自行升级固件，以实现相关的配置策略。

3.16 配置管理

3.16.1 配置文件导入导出

配置导入导出就是指把 HDM、BIOS、RAID 的所有配置能以配置文件的方式导出和导入，实现管理员可以轻松远程配置服务器。

配置文件导入导出具有以下技术优势：

- 通过 HDM 的配置导入导出功能实现带外批量配置 HDM、BIOS、RAID 三大模块的配置选项，覆盖选项全。
- 配置可阅读、可编辑、可保存。可并行配置多台服务器。
- 操作便捷，灵活使用将大幅提升管理运维效率。
- 配置导入速度快：配置单个文件仅需 2 分钟，HDM+BIOS+RAID 全配置仅需 6 分钟。
- 可配置参数多：其中 HDM 支持 100+选项、BIOS 支持 1000+选项、支持修改 RAID 级别覆盖 0/1/5/6/10。

图61 配置文件导入导出页面



配置文件支持如下使用场景：

- 导出配置文件，完成修改再导入 = 批量修改设置选项。
- 配置文件在同型号服务器上通用，即针对同一类型机器快速完成大规模设备的配置和部署。
- 更换主板或者恢复出厂默认设置后，可以快捷的恢复自定义设置。

图62 配置文件导入导出使用场景示意图

