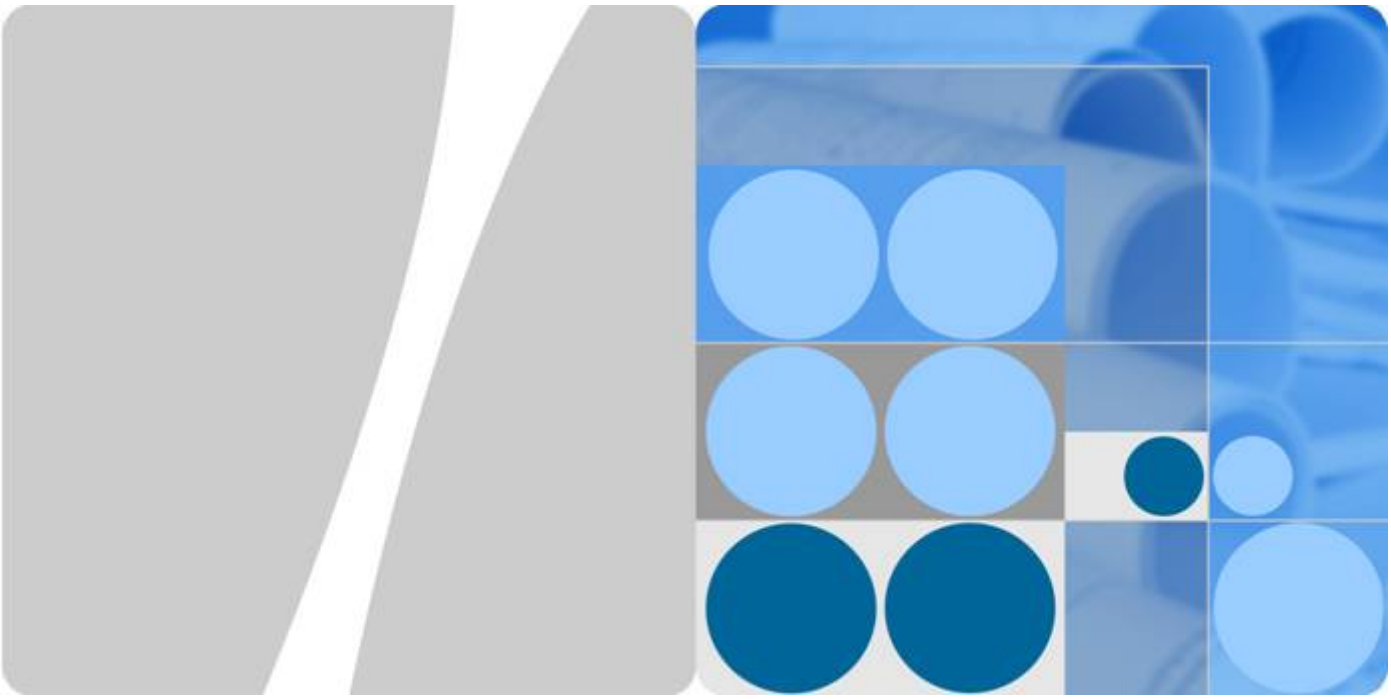


华为服务器 iMana 智能管理系统

白皮书 V1.3

文档版本 05

发布日期 2015-02-12

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司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，华为公司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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

插图目录

表格目录

1 产品简介

关于本章

1.1 概述

华为服务器iMana 200智能管理系统（以下简称iMana）是华为自主开发的具有完全自主知识产权的服务器远程管理系统。iMana兼容服务器业界管理标准IPMI 2.0、SNMP、DMTF规范、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、故障诊断、高可靠的硬件监控和管理功能。iMana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/CLI/https/SNMP/WS-MAN/SMASH-CLP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，提前发现并解决问题，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。
- 系统崩溃时临终截屏与录像

  分析系统崩溃原因不再无处下手。
- 屏幕快照和屏幕录像

  让定时巡检、操作过程记录及审计变得简单轻松。
- 支持DNS/LDAP

  域管理和目录服务，简化服务器管理网络。
- 软件双镜像备份

  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

  功率封顶技术助您轻松提高部署密度；动态节能技术助您有效降低运营成本。
- 安全管理

  从接入、账号、传输、存储四个角度保障服务器管理的安全，让您用得放心。

1.2 系统设计

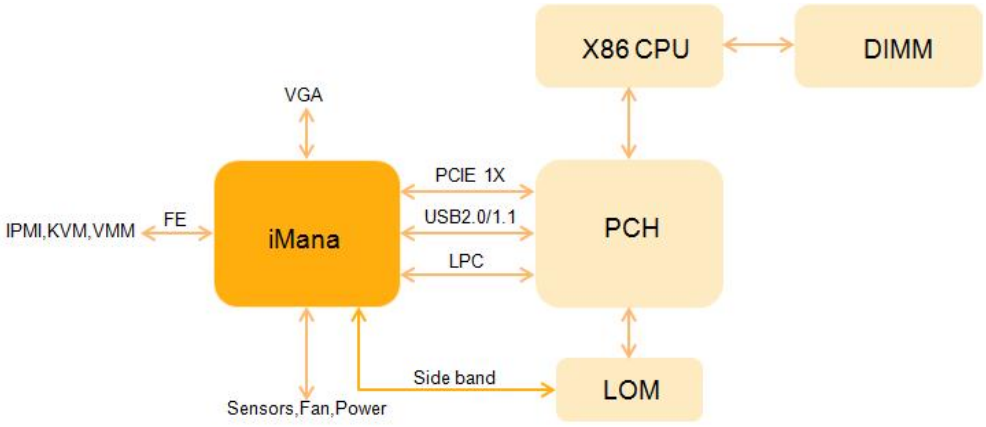
如图1-1所示，iMana主要由以下几个部分组成。

- iMana的KVM模块通过VGA接口接收来自x86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x86系统，实现远程的键盘鼠标控制。

- iMana的系统运行记录仪模块通过PCIe接口接收来自x86系统写入的运行轨迹信息（黑匣子数据），并提供记录信息的导出接口。
- iMana提供传统的LPC系统接口与x86系统通信，支持标准的IPMI管理。
- iMana对外提供FE以太网络接口，支持通过网络使用IPMI，HTTPS等协议进行远程管理操作。
- iMana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。
- iMana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。

图 1-1 iMana 系统架构



2 产品功能

关于本章

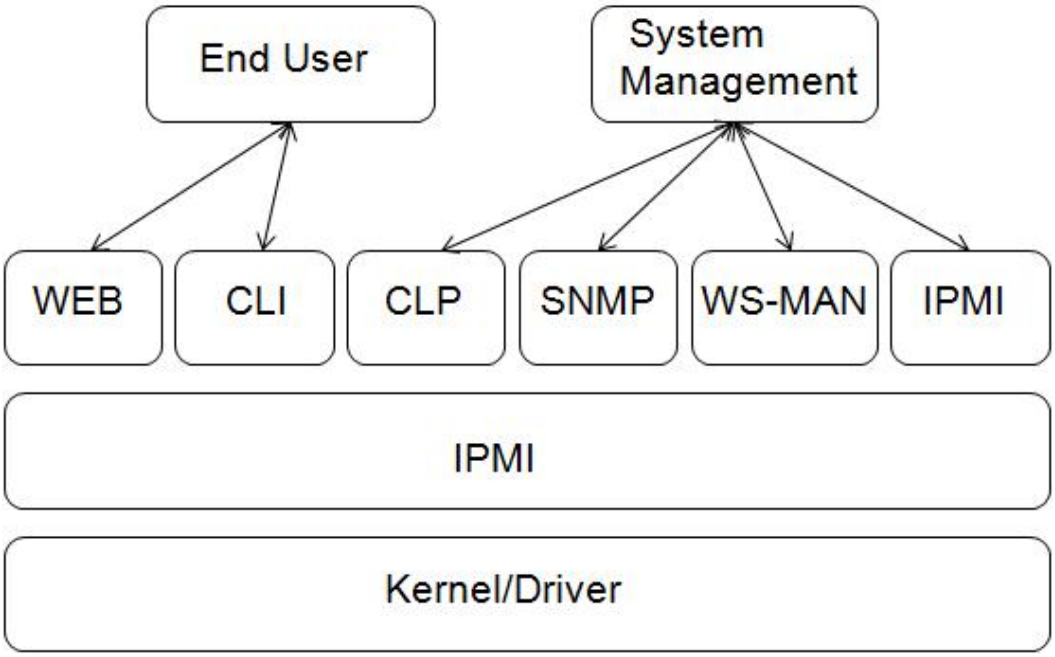
iMana以其丰富的特性支持，提升管理效率，有效降低运营成本。

- iMana是华为自主开发的具有完全自主知识产权的高级的服务器远程管理软件。它支持键盘、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、软驱、硬盘映射到服务器）和基于IPMI2.0的硬件监控和管理功能。按照电信级的可靠性要求而设计的，支持软件的双镜像备份。
- iMana提供了丰富的用户接口，如命令行、基于Web界面的用户接口、ipmitool管理接口，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。
- iMana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、电压、风扇转速、电源故障、总线故障等。同时还提供了CPU、内存和硬盘信息的查询。
- iMana能够在服务器宕机的时候保存宕机之前屏幕上输出的最后的信息，用于故障的定位。还支持实时的屏幕快照，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。

2.1 丰富的管理接口

iMana是一个遵循行业管理规范的带外单机管理系统，是数据中心管理网中的一个子节点，承载着管理、控制和诊断服务器的任务，需要对外提供各种人机接口和机机接口，以满足各种服务器管理场景的应用和集成需求。

图 2-1 iMana 管理接口图



2.1.1 标准 IPMI 1.5/IPMI 2.0 管理接口

iMana兼容IPMI 1.5/IPMI 2.0规范，通过第三方工具(如：ipmitool)基于BT或LAN通道实现对服务器的有效管理。基于BT时，ipmitool等工具必须运行在服务器本机的操作系统上；而基于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命令接口：

  Interfaces：

  open Linux OpenIPMI Interface [default]

  imb Intel IMB Interface

  lan IPMI v1.5 LAN Interface

  lanplus IPMI v2.0 RMCP+ LAN Interface
- ipmitool命令参数：

  Parameters:

  -h This help

-V Show version information
-v Verbose (can use multiple times)
-c Display output in comma separated format
-d N Specify a /dev/ipmiN device to use (default=0)
-I intf Interface to use
-H hostname Remote host name for LAN interface
-p port Remote RMCP port [default=623]
-U username Remote session username
-f file Read remote session password from file
-S sdr Use local file for remote SDR cache
-a Prompt for remote password
-e char Set SOL escape character
-C ciphersuiteCipher suite to be used by lanplus interface
-k key Use Kg key for IPMIv2 authentication
-y hex_key Use hexadecimal-encoded Kg key for IPMIv2 authentication
-L level Remote session privilege level [default=ADMINISTRATOR]
Append a '+' to use name/privilege lookup in RAKP1
-A authtype Force use of auth type NONE, PASSWORD, MD2, MD5 or OEM
-P password Remote session password
-E Read password from IPMI_PASSWORD environment variable
-K Read kgkey from IPMI_KGKEY environment variable
-m address Set local IPMB address
-b channel Set destination channel for bridged request
t address Bridge request to remote target address
-B channel Set transit channel for bridged request (dual bridge)
-T address Set transit address for bridge request (dual bridge)
-l lun Set destination lun for raw commands
-o oemtype Setup for OEM (use 'list' to see available OEM types)
-O seloem Use file for OEM SEL event descriptions

- ipmitool命令支持：

Commands：
raw Send a RAW IPMI request and print response
i2c Send an I2C Master Write-Read command and print response
spd Print SPD info from remote I2C device
lan Configure LAN Channels
chassis Get chassis status and set power state
power Shortcut to chassis power commands
event Send pre-defined events to MC
mc Management Controller status and global enables
sdr Print Sensor Data Repository entries and readings

sensor Print detailed sensor information
fru Print built-in FRU and scan SDR for FRU locators
gendev Read/Write Device associated with Generic Device locators sdr
sel Print System Event Log (SEL)
pef Configure Platform Event Filtering (PEF)
sol Configure and connect IPMIv2.0 Serial-over-LAN
tsol Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol Configure IPMIv1.5 Serial-over-LAN
user Configure Management Controller users
channel Configure Management Controller channels
session Print session information
sunoem OEM Commands for Sun servers
kontronoem OEM Commands for Kontron devices
picmg Run a PICMG/ATCA extended cmd
fwum Update IPMC using Kontron OEM Firmware Update Manager
firewall Configure Firmware Firewall
delloem OEM Commands for Dell systems
shell Launch interactive IPMI shell
exec Run list of commands from file
set Set runtime variable for shell and exec
hpm Update HPM components using PICMG HPM.1 file
ekanalyzer Run FRU-Ekeying analyzer using FRU files

- ipmitool命令举例：查询iMana上所有本地用户

  基于BT：ipmitool user list

  基于LAN：ipmitool -H *.*.*.* -I lanplus -U <用户名> -P <密码> user list 1

  - H：iMana 网口IP地址
  - I：传输协议，lan：不加密，lanplus：加密
  - U：iMana本地用户名
  - P：iMana本地用户密码

2.1.2 CLI（Command Line Inferface）管理接口

iMana提供了简单易用的命令行管理接口，包含两个基本命令程序：ipmcget和ipmcset，通过这两个命令程序就能实现对服务器的远程管理，支持通过SSH和Telnet登录后执行。

- ipmcget 查询命令格式：

  ipmcget [-t target] -d dataitem

  -t <target>

  fru0 Get the information of the fru0

  led Get led state

  sensor Print detailed sensor information

  smbios Get the information of smbios

eth0 Get the eth0 information
trap Get SNMP trap status
service Get service information

-d <dataitem>

fanmode Get fan mode

fanlevel Get the percentage of the fan speed

port80 Get the diagnose code of port 80

bootdevice Get boot device

shutdowntimeout Get graceful shutdown timeout value

health Get health status

healthevents Get health events

sel Print System Event Log (SEL)

version Get ipmc version

serialnumber Get system serial number

userlist List all user info

fruinfo Get fru information

ipmctime Get ipmc system time

macaddr Get mac address

serialdir Get front panel serial direction

rollbackstatus Get rollbackstatus

passwordcomplexity Get password complexity check enable state

remotemanageid Get Remote Manage ID

- ipmcset 设置命令格式：
  ipmcset [-t target] -d dataitem [-v value]
  -t <target>
  fru0 Operate with fru0
  led Operate with led
  eth0 Set eth0 ip address
  sensor Operate with sensor
  trap Operate SNMP trap
  service Operate with service
  user Operate with user

-d <dataitem>

fanmode Set fan mode,you can choose manual or outo

fanlevel Set fan speed percent

download Download SOL or Black box command

identify Operate identify led

pgrade Upgrade component

clearcmos Clear CMOS

bootdevice Set boot device

reset Reboot IPMC system

shutdowntimeout Set graceful shutdown timeout value

frucontrol Fru control

powerstate Set power state

sel Clear SEL

adduser Add user

password Modify user password

deluser Delete user

privilege Set user privilege

serialdir Set front panel serial direction

printscreen Print current screen to bmc

rollback Perform a manual rollback

timezone Set time zone

passwordcomplexity Set password complexity check enable state

remotemanageid Set Remote Manage ID

2.1.3 HTTPS 管理接口

iMana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iMana的网口IP地址（IPv4或IPv6）或域名称打开iMana Web的登录界面，输入本地账号或LDAP域账号登录到iMana Web。

Web接口支持的OS和浏览器、JRE如**表2-1**所示。

表 2-1 客户端环境要求

运行环境	配置要求
操作系统	Windows XP 32位
	Windows 7 32位/64位
	Windows 8 32位/64位
	Windows Server 2008 R2 64位
	Windows Server 2012 64位
	Redhat 4.3 64位
	Redhat 6.0 64位
	Mac OS X v10.7
浏览器	Internet Explorer 8.0/10.0/11.0（仅适用于Windows操作系统），其中Internet Explorer 10.0/11.0不支持Windows XP
	Mozilla Firefox 9.0/23.0
	Chrome 13.0/31.0（仅适用于Windows操作系统）
	Safari 5.1（仅适用于MAC操作系统）
Java运行环境	JRE 1.6.0 U25/1.7.0 U40

2.1.4 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—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。

iMana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，出

厂默认只启用V3版本。SNMP V1/V2C的get/set操作可以使用不同的团体名，默认团体名分别为roHuawei12#$、rwHuawei12#$；SNMP V3的鉴权算法支持选择MD5或SHA，加密算法支持选择DES或AES，鉴权算法和加密算法默认值分别为SHA和AES，安全用户名与登录用户名相同。SNMP V3安全用户与其他接口(Web、CLI、SMASH-CLP、IPMI LAN)共用一套本地用户，但密码长度必须至少8位。

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、本地用户和域账号(LDAP)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、功率封顶、域名系统(DNS)等。

SNMP接口应用场景：

- 场景1—基于开源工具的管理

直接使用第三方开源的Mib图形工具（如MG-SOFT MIB Browser）和命令行工具基于SNMP协议对每个Mib节点进行操作，通常用于测试或临时的服务器远程管理和维护；

- 场景2—简单集成管理

网管软件将SNMP MIB定义文档编译后导入，即可通过SNMP接口管理服务器，并可对重要的信息配置触发脚本以及对TRAP事件进行重新映射；目前已跟业界常用的CA、IBM System Director、HP SIM网管软件进行了验证。

- 场景3—深度集成管理

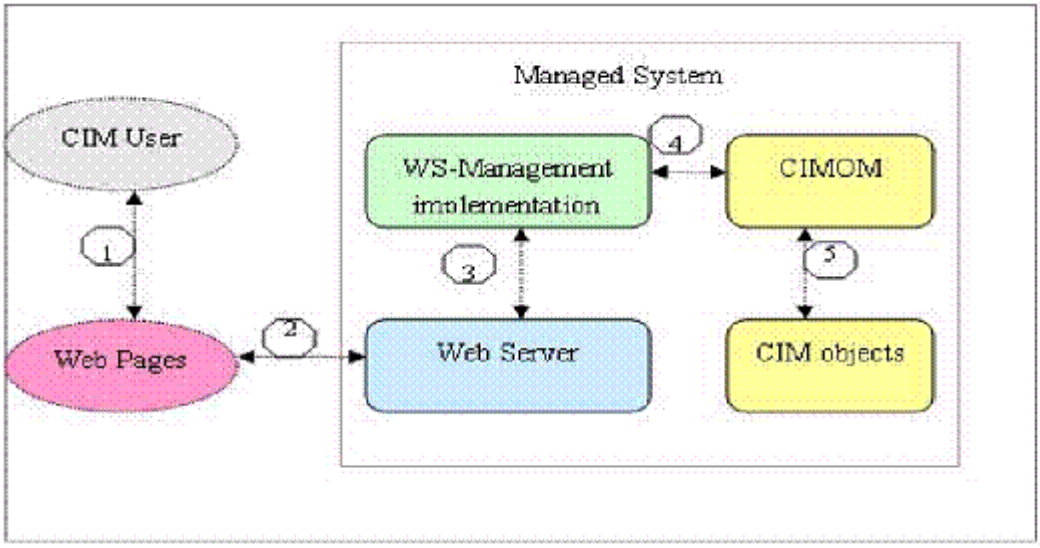
网管支持插件方式，针对不同服务器厂商开发不同的集成管理插件，插件接收网管的操作命令并通过SNMP接口与iMana交互进行查询和设置信息，然后按照网管与插件接口格式返回给网管进行展示；目前已为业界常用的Vmware Vcenter、微软System Center网管软件开发了插件。

2.1.5 WS-MAN 管理接口

WS-MAN接口是一套跨平台和OS的面向对象的编程接口；iMana通过基于SOAP（Simple Object Access Protocol）的管理协议WS-Management（Web Service Management），实现管理服务的Web化，允许系统以独立于系统类型或平台的方式使用管理信息。WS-Management 提供统一的跨整个IT 基础结构访问和交换管理信息的方法，降低IT 管理的成本和复杂性。

WS-Management基于CIM（Common Information Model）对系统进行管理，其消息流如图2-2所示。CIM提供了一种针对被管理信息的可扩展的通用定义，包括系统、网络、应用、服务等。

图 2-2 WS-Management 操作消息流



2.1.6 SMASH-CLP 管理接口

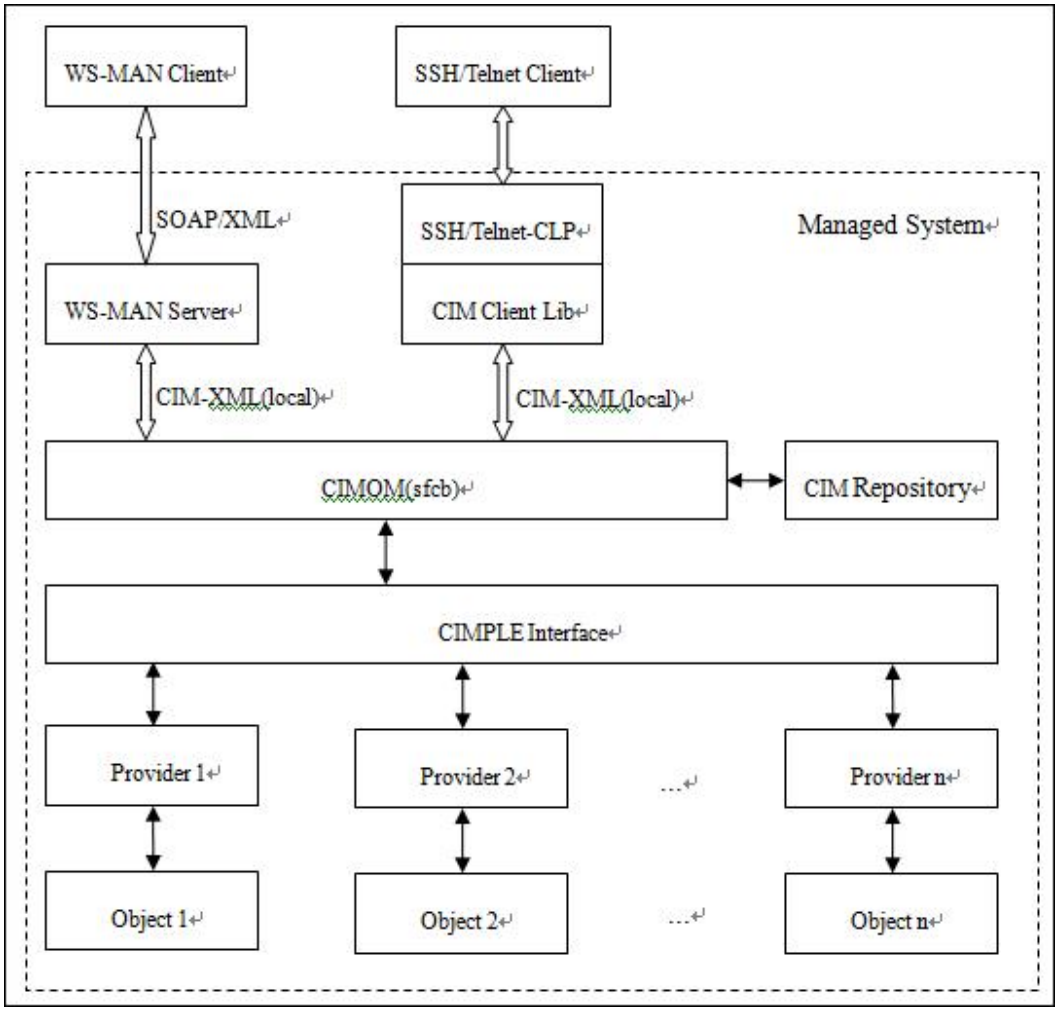
SMASH-CLP是一个命令行协议，属于DMTF的SMASH标准规范，定义了标准的操作Verbs(cd、show、set、start、stop、create、delete、load、reset、help等)，基于面向对象的CIM接口实现；易于被集成，降低了网管平台对异构服务器的管理复杂性。

通过SSH或Telnet客户端登录到iMana后，输入hwsmash并敲回车即可进入到CLP操作环境，显示如下提示符：

iMana:/->

命令格式：<verb> [<options>] [<target>] [<properties>]

图 2-3 CLP 的实现框架如下



- CLP支持具体功能如下：
  - CPU、内存、硬盘、电源、风扇属性和状态查询；
  - iMana和BIOS固件版本查询和固件升级；
  - 本地用户的用户名、密码、权限的查看和修改；
  - 服务器上下电、重启、安全重启；
  - SEL查询和清除；
  - 启动设备查询和设置；
  - DNS信息、IP地址查询和设置；
  - SNMP TRAP团体名、协议版本、上报级别、接收地址、端口配置等。

2.2 故障监控和诊断

2.2.1 故障检测

iMana对服务器进行了全面的监控，并且提供了可靠的故障检测和故障预测机制。能检测到的故障包括：

- CPU硬件故障(CAT ERROR、自检失败、配置错误)
- 超温告警(进风口、CPU、内存、系统电源)
- 主板和板卡电压故障
- 风扇故障
- 系统电源故障(AC/DC输入丢失、高温、电源风扇故障)
- 总线故障(I2C、IPMB)
- 内存故障(可纠正ECC错误超门限、高温、配置错误)
- 硬盘故障(预故障、RAID失效)
- 系统宕机故障

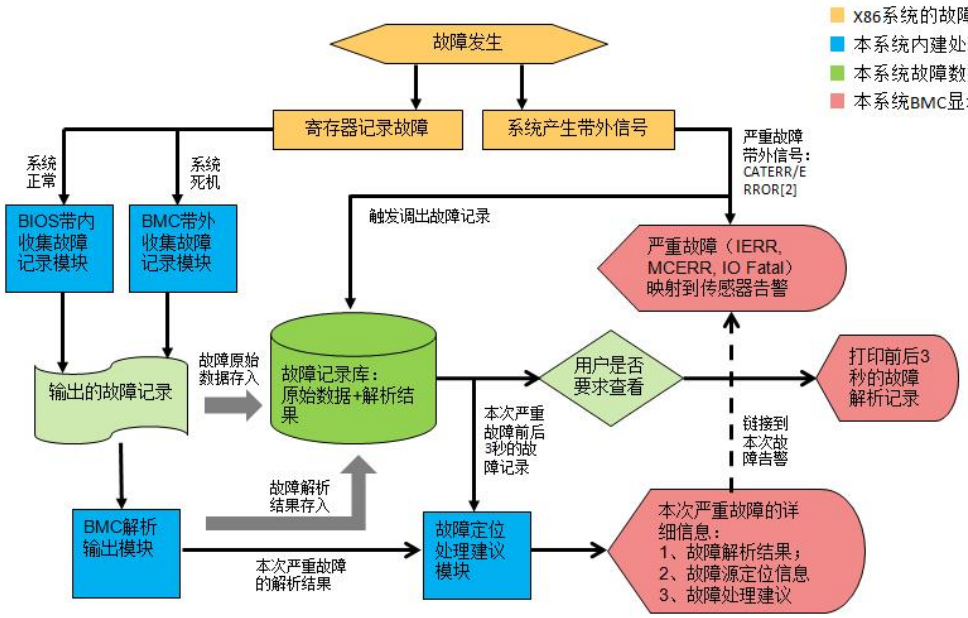
2.2.2 故障诊断

iMana集成了MCE故障处理系统(FDM)，该系统建立了一套通用的以iMana为管理中心的带外的x86系统硬件故障处理系统，实现对硬件故障进行记录、报告、定位、预报警等功能。

应用场景：

1. 数据中心服务器运行过程中突然宕机，系统黑屏/挂死，由于OS不支持等原因没有记录下产生的MCE码，只有iMana记录到CATERR事件发生，无法获取更进一步的信息判断问题所在；
2. 服务器长时间运行，整体上虽然未发生崩溃，但内部其实已经存在的大量的可恢复/纠正的故障（如ECC等）。虽然这些故障暂时不影响业务，但也需要提前发现和处理，避免发生灾难性故障；
3. 硬件故障出现概率低，难复现，主要靠人工经验判断，多次插拔/更换，效率低，对客户的影响大；
4. 故障发生后没有完整的故障记录，更不能进行故障定位、故障预报警及更深层次的处理。

图 2-4 MCE 故障处理系统模块功能图



主要技术点：

- 实现了全方位自动的故障数据的抓取

通过带内带外不同的故障数据收集技术的整合与自动切换。

- 实现一个以iMana为中心的完整可持续发展的带外故障处理系统

把所有的故障数据汇聚到iMana，由iMana在带外做更进一步的故障分析、定位、预告警等功能，克服了OS作为故障处理中心的能力不足、不可控、影响系统性能等难题。

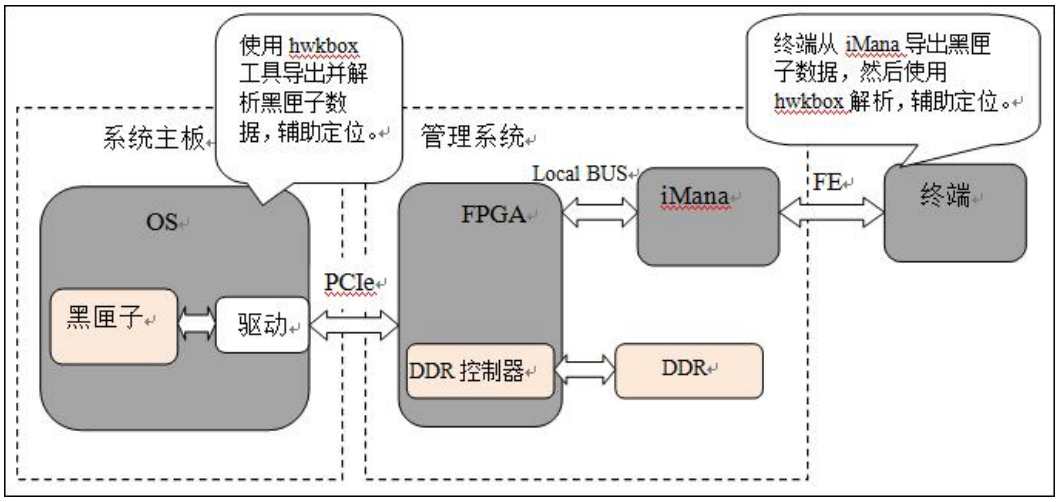
- 故障诊断专家系统 (待实现)

通过我们对MCE故障机制的深入分析理解，以及对故障样板数据的归纳总结形成的专家知识，基于iMana建立了一套故障诊断专家系统，当系统发生严重故障时可以通过已收集的故障数据来自动定位故障源并提供故障解决方案。

2.2.3 系统运行记录仪

iMana提供了系统运行记录仪功能，该功能由黑匣子（KBox）模块、FPGA、iMana、解析工具（hwkbox）四个模块协同完成，默认关闭。按照如图2-5所示原理，系统运行记录仪主要实现了linux系统内核panic时的内核栈信息记录和导出，以及提供给第三方应用的读写接口，便于第三方应用记录自定义信息；记录的系统故障数据（也称黑匣子数据）不会因系统重启和上下电而丢失，但AC掉电会丢失。

图 2-5 系统运行记录仪原理



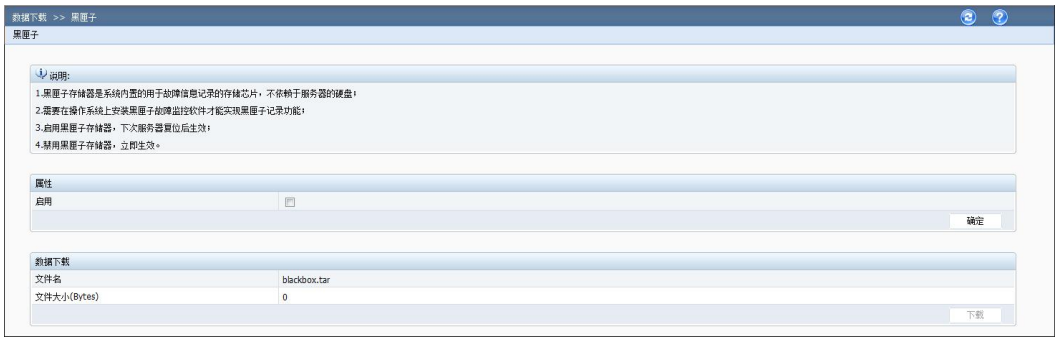
应用场景一：

在内核panic触发时，注册的黑匣子模块自动抓取内核栈信息，并写PCIe设备，通过DDR控制器将定位信息保存到DDR中，最多16M字节数据。待系统重启后， 通过对PCIe设备读操作，系统侧定位工具把保存在DDR中的定位信息读取并解析，辅助定位。 即使系统无法正常启动， DDR内的信息，也可以通过iMana（如图2-6）导出并使用专门工具解析(目前只能导入到系统OS下使用hwkbox工具解析)。

应用场景二：

系统第三方应用调用黑匣子模块写接口将运行日志记录到FPGA的DDR中，最多2M字节数据；当应用异常时，系统侧调用黑匣子模块读接口或通过iMana将运行日志读取并解析以辅助问题定位。

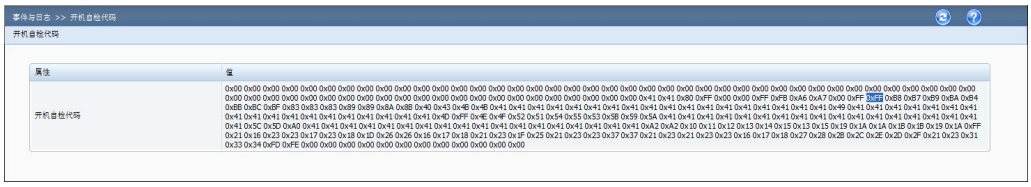
图 2-6 黑匣子数据下载界面



2.2.4 开机自检代码

开机自检代码记录系统开机自检结果信息，表示当前自检通过还是发生具体故障，不同的代码表示不同故障含义，通过查询故障代码表可定位到系统启动具体故障，如图2-7所示。

图 2-7 开机自检代码界面



2.2.5 系统事件管理

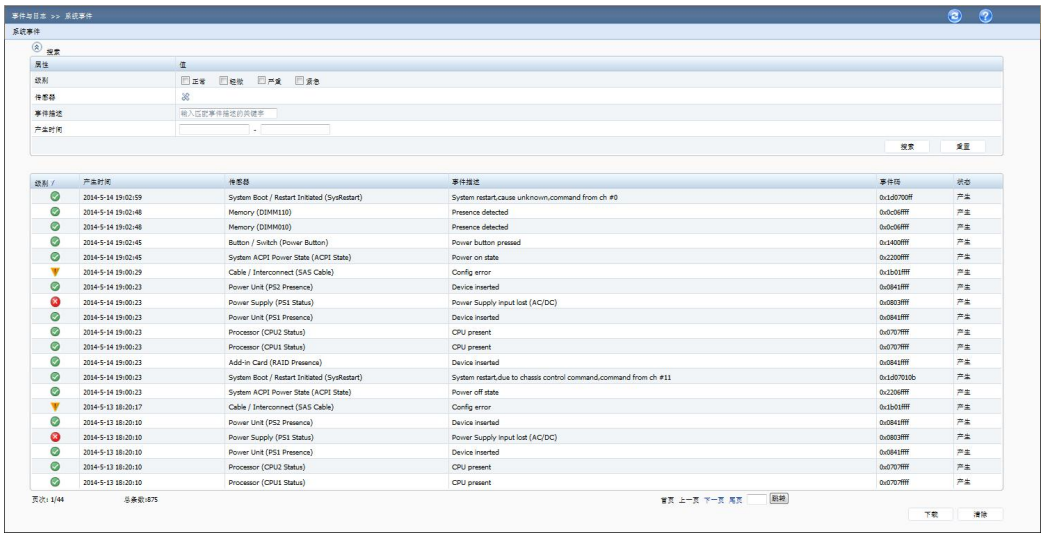
在可靠的故障检测基础上，iMana智能管理控制器还实现了丰富的告警管理功能。

- 告警监控覆盖全部硬件
- 日志描述详细
- 支持本地存储和归档
- 支持人性化的日志管理：可视化、过滤、排序、下载
- 支持多种方式(SNMP TRAP和电子邮件)远程上报告警
- 支持多目的地上报告警

系统事件实时写文件，当达到1000条事件记录后自动备份，最多备份3份文件，超过3份后自动将最早的备份文件删除。

系统事件界面可以查询所有系统事件并可以对其进行排序，过滤，清空等操作，如图2-8所示。

图 2-8 系统事件界面



系统事件参数说明如表2-2所示。

表 2-2 系统事件各参数说明

参数	说明
级别	事件的健康状态级别，包括：正常、轻微、严重、紧急。
产生时间	事件产生的时间。
传感器	产生事件的传感器。
事件描述	事件的描述。
事件码	事件的编码。
状态	事件的当前结果，包括：产生、恢复。

2.2.6 故障上报

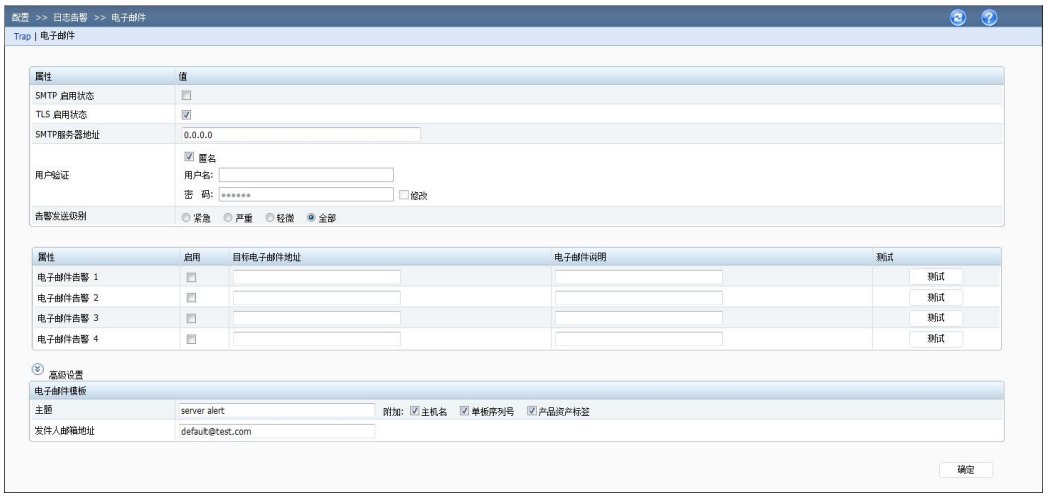
iMana支持实时监测硬件、系统的故障状态并通过SNMP （Simple Network Management Protocol）TRAP和电子邮件方式上报到远程接收服务器。

如图2-9所示，SNMP Trap支持4个接收目标，每个接收目标可配置接收地址、端口号、启用状态和告警格式；支持根据严重性级别对事件上报过滤；支持V1/V2C/V3版本，默认为V1版本，选择V3安全版本时需要从本地用户中选择一个Trap V3安全用户以及配置V3鉴权和加密算法；Trap消息中会携带主机标识和位置信息，主机标识可指定单板序列号、产品资产标签、主机名中任意一个；支持对接收目标发送测试信息。

如图2-10所示，SMTP（Simple Mail Transfer Protocol）支持4个接收目标，每个接收目标可配置接收邮箱、邮箱描述和启用状态，支持对接收目标发送测试信息，支持匿名或用户验证登录SMTP服务器，支持启用TLS对邮件加密，支持邮件模板主题和发件人定制。

图 2-9 SNMP TRAP 配置界面

图 2-10 SMTP 配置界面



2.3 虚拟 KVM 和虚拟媒体

通过远程控制台界面可以使用虚拟KVM、虚拟媒体和手动录像功能以及对电源的上下电、重启操作，控制台界面如图2-11所示。

远程控制台支持工作在窗口模式和全屏模式，当处于全屏或分屏模式下，同时按下Ctrl Alt Shift组合键可弹出工具栏。

图 2-11 远程控制台

2.3.1 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；主要特点如下：

- 分辨率：最高分辨率为1280*1024，最低分辨率为400*400。
- 鼠标同步：支持鼠标同步，该功能需要远端服务器OS支持，见**表2-3**。
- 鼠标模式：支持绝对、相对和单鼠标三种模式。
- 工作模式：支持独占和共享模式，共享模式下，协同双方可以同时操作远端服务器；若是安全考虑，请使用独占模式。
- 运行环境：使用虚拟KVM功能，客户端需具备相应版本的浏览器、OS和Java运行环境，如**表2-1**所示。
- 色彩位：支持8bit色，最多255种色彩。
- 组合键：提供了可发送任意6个键的组合键的方式。
- 加密：视频、键盘和控制命令数据支持AES 128 CBC算法加密传输。

由于鼠标同步功能取决于OS是否支持提供绝对鼠标位置信息，所以对于不能提供绝对鼠标位置信息的OS，KVM不支持鼠标同步功能。

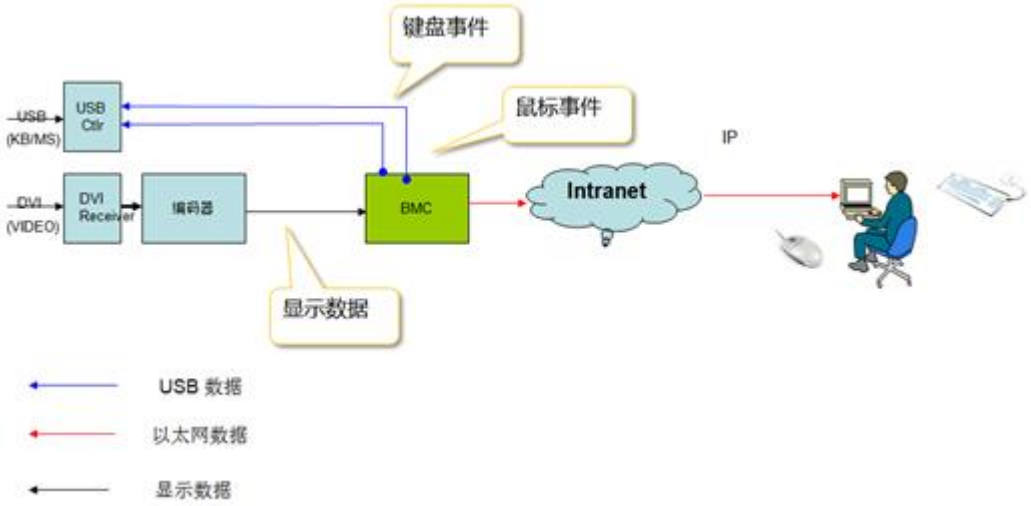
表 2-3 不支持鼠标同步功能的 OS 列表(包括但不限于)

不支持鼠标同步功能的OS列表
SUSE Linux Enterprise Server 11 Service Pack 1 for x86(32Bit)
SUSE Linux Enterprise Server 11 Service Pack 1 for Intel EM64T(64Bit)

虚拟KVM的实现原理如图2-12所示：

- iMana将远端的显示数据压缩编码后通过网络传输到用户所在的客户端主机，由客户端主机控制台解码解压缩后恢复显示。
- 虚拟KVM的控制台会将用户所在的客户端主机的鼠标事件和键盘事件捕获，通过网络传输到远端，由iMana智能管理控制器模拟远端的键盘鼠标将事件经由USB通道输入到远端服务器业务系统上。

图 2-12 虚拟 KVM 实现原理



2.3.2 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，硬盘文件夹和USB Key）的远程访问方式；虚拟媒体数据支持AES 128 CBC算法加密传输。使用虚拟媒体功能，客户端需具备相应版本的操作系统和Java运行环境如表2-1所示。

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，如图2-13所示。

图 2-13 虚拟媒体实现原理

iMana与服务器主机的数据通道采用USB2.0。目前iMana的虚拟媒体具有以下功能特性：

- 虚拟设备

  虚拟设备即将客户端的PC设备或者镜像文件映射到建立连接的服务器上，使得该服务器检测到一个USB设备。

  虚拟设备包括如下多种情况：

  虚拟一个软驱设备

  虚拟一个光驱设备

  虚拟一个USB Key

  虚拟一个文件夹

  虚拟软驱可以和其它虚拟设备同时进行

- 虚拟媒体性能

  虚拟光驱支持最大传输速率32 Mbit/s，VLAN时支持最大传输速率24 Mbit/s

  虚拟软驱支持最大传输速率4M bit/s

- 制作镜像文件

  将软盘或者光盘的内容制作成镜像文件并保存在硬盘上。

2.4 基于 HTTPS 的可视化管理接口

iMana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，支持的浏览器有IE、Firefox、Chrome、Safari，支持的具体浏览器版本详如表2-1所示。

可按照如下方式登录iMana Web：

步骤1 在浏览器URL地址栏输入http:// iMana IP[:port] 或 https:// iMana IP[:sslport]，如图2-14所示。

说明

端口号是可选的，若port不为80或sslport不为443则IP地址后面必须要带上端口号，端口号修改方法参考2.11.4 服务管理。

图 2-14 输入 iMana 地址

步骤2 在用户登录界面中输入用户名和密码，若是域账号登录则选择登录到具体的域，然后单击下方的“登录”按钮登录，如图2-15所示。

图 2-15 登录 iMana Web

说明

登录界面的“摘要信息”页签展示了系统的一些重要信息，包括设备名称、设备序列号、产品资产标签、iMana固件版本、BIOS版本、系统状态和设备状态，如图2-16所示。

图 2-16 摘要信息界面

----结束

2.4.1 查看系统总体概况

总体概况界面显示系统当前基本情况，包括系统状态、iMana信息、系统配置信息和当前告警信息，并提供常见操作接口链接，如图2-17所示。

图 2-17 总体概况界面

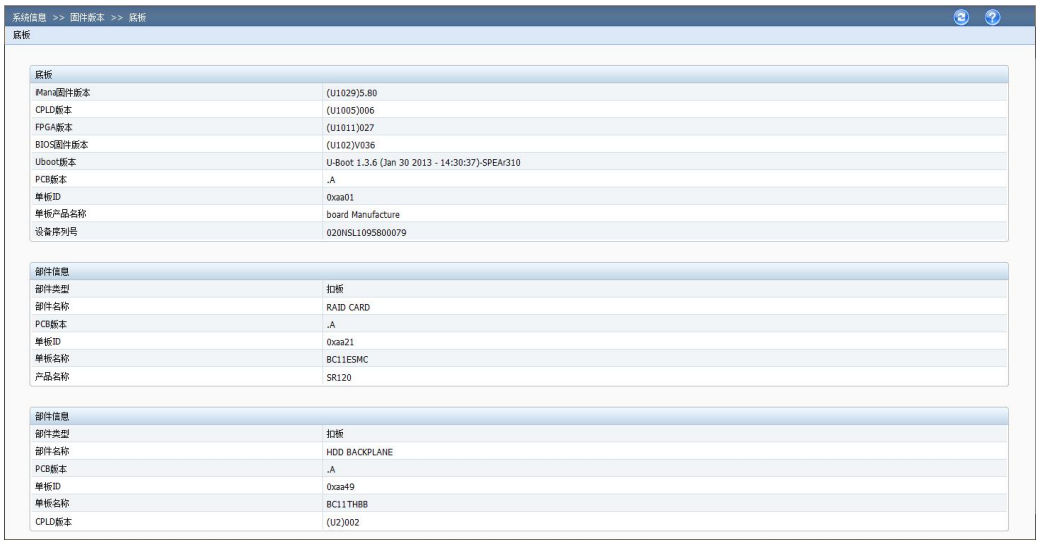
2.4.2 查看系统信息

系统信息界面详细显示当前系统的固件版本、资产信息和整机硬件信息。

固件版本

固件版本包括iMana固件、BIOS、FPGA、UBOOT、CPLD的版本，以及底板、各种扣卡（如：RAID卡、Mezz卡、硬盘背板等）的PCB和单板ID，如图2-18所示。

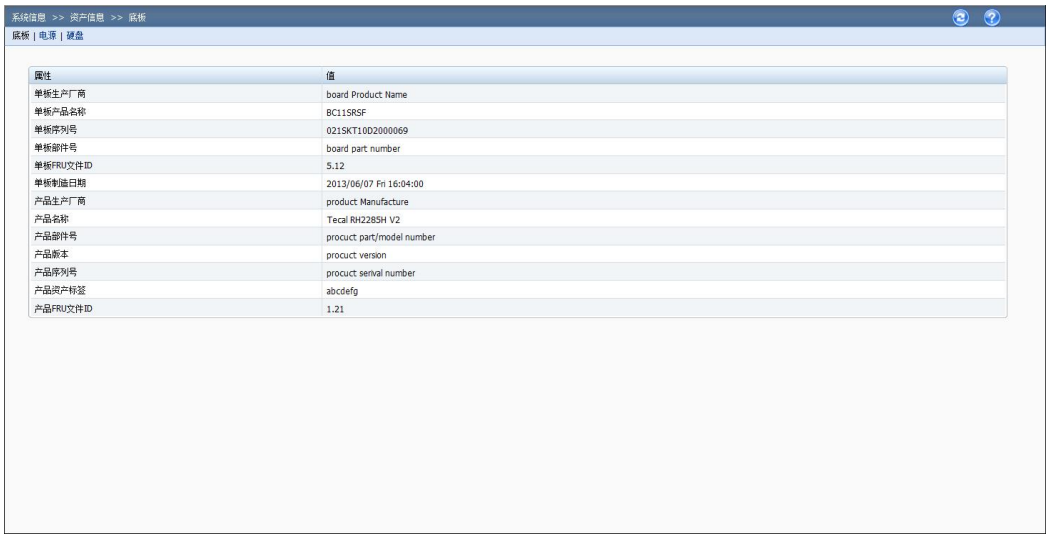
图 2-18 固件版本界面

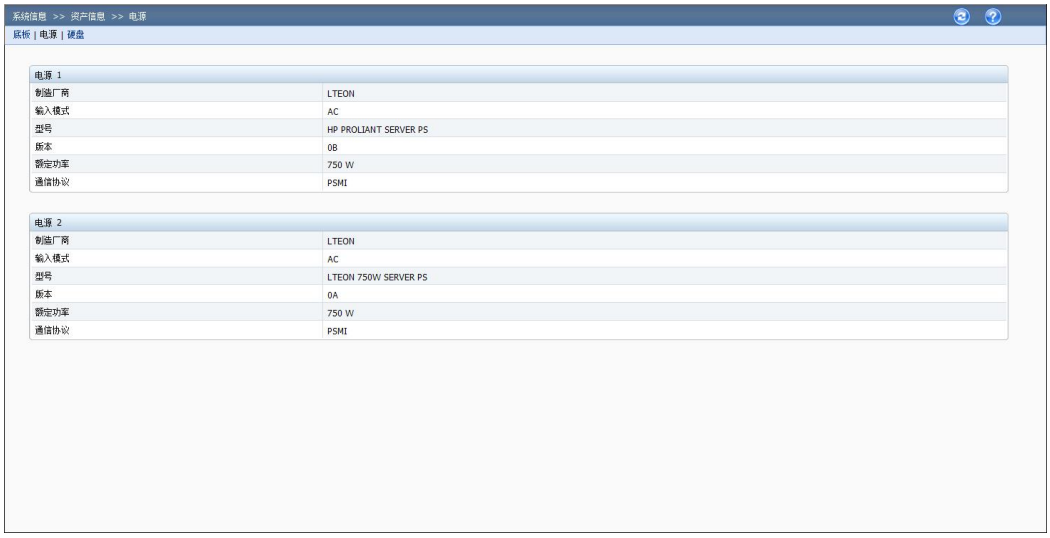


资产信息

资产信息包括底板及所有FRU的资产信息，如图2-19所示。

图 2-19 资产信息界面



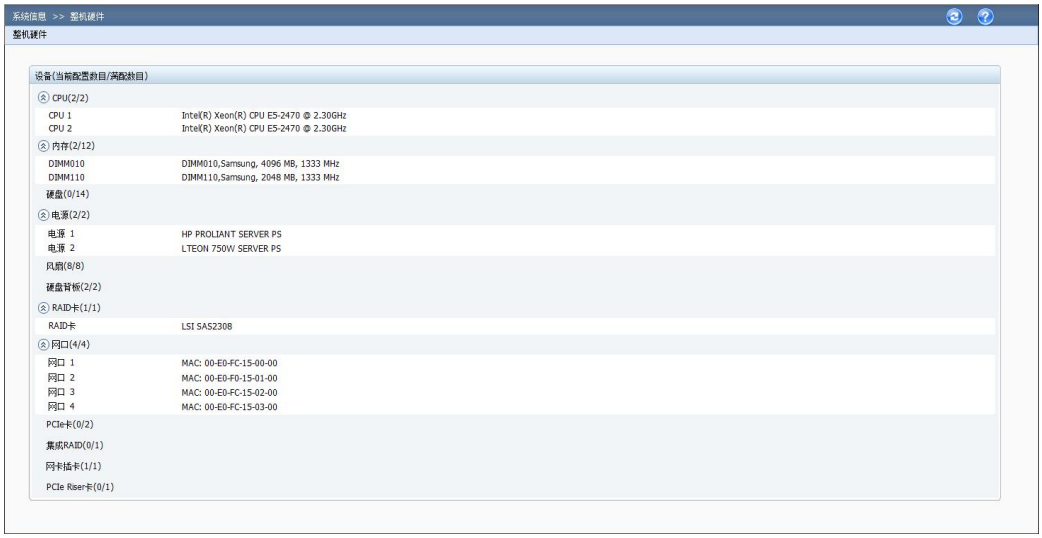


与带内BMA(Board Management Agent)模块配合，还支持查看物理硬盘信息：制造厂商、最大转速、容量、总线协议类型、序列号、联机状态、RAID重构进度、型号、firmware版本；当前版本不支持对连接到RAID标卡和PCH SCU接口的硬盘信息查看。关于BMA模块的详细介绍，请登录http://support.huawei.com/enterprise/productsupport，搜索《服务器 BMA V100R002 用户指南》。

整机硬件

整机硬件信息包括系统主要部件的最大配置数、当前配置数和型号，如图2-20所示。

图 2-20 整机硬件界面



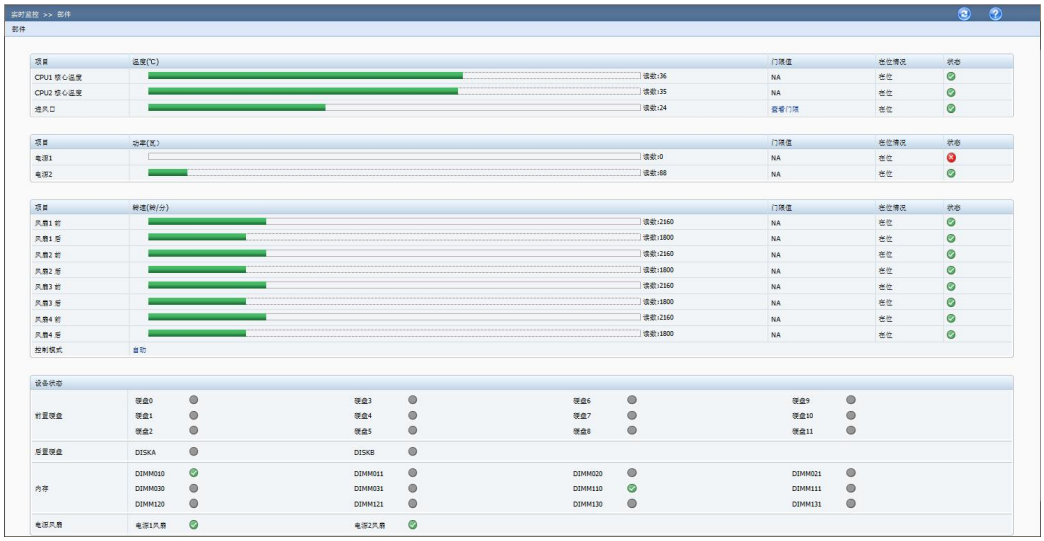
2.4.3 实时监控

实时监控包含部件、传感器、指示灯三个方面的信息和操作接口。

部件

如图2-21所示，部件界面显示设备重要项目的监控信息，包括：CPU和进风口温度、系统电源功率、风扇的实时读数和状态，硬盘、内存、PCIe设备状态。

图 2-21 部件界面



传感器

传感器界面显示设备所有传感器信息，如图2-22所示，相关的参数如表2-4所示。

图 2-22 传感器界面

传感器	当前值	单位	紧急下门限	严重下门限	轻微下门限	轻微上门限	严重上门限	紧急上门限
CPU1 Core Rem	36.00	℃	NA	NA	NA	NA	NA	NA
CPU2 Core Rem	36.00	℃	NA	NA	NA	NA	NA	NA
CPU1 DTS	-59.00	NA	NA	NA	NA	NA	-1.00	NA
CPU2 DTS	-59.00	NA	NA	NA	NA	NA	-1.00	NA
Inlet Temp	24.00	℃	NA	NA	NA	NA	44.00	46.00
Rear Disk Temp	25.00	℃	NA	NA	NA	NA	52.00	NA
CPU1 Prochot	30.00	℃	NA	NA	NA	NA	90.00	NA
CPU2 Prochot	30.00	℃	NA	NA	NA	NA	90.00	NA
Power1	0.00	W	NA	NA	NA	NA	NA	NA
Power2	88.00	W	NA	NA	NA	NA	NA	NA
FAN1 F Speed	2160.00	RPM	NA	NA	NA	NA	NA	NA
FAN1 R Speed	1800.00	RPM	NA	NA	NA	NA	NA	NA
FAN2 F Speed	2160.00	RPM	NA	NA	NA	NA	NA	NA
FAN2 R Speed	1920.00	RPM	NA	NA	NA	NA	NA	NA
FAN3 F Speed	2160.00	RPM	NA	NA	NA	NA	NA	NA
FAN3 R Speed	1800.00	RPM	NA	NA	NA	NA	NA	NA
FAN4 F Speed	2160.00	RPM	NA	NA	NA	NA	NA	NA
FAN4 R Speed	1920.00	RPM	NA	NA	NA	NA	NA	NA
CPU1 Status	0x8080	NA	NA	NA	NA	NA	NA	NA
CPU2 Status	0x8080	NA	NA	NA	NA	NA	NA	NA
CPU1 Memory	0x8000	NA	NA	NA	NA	NA	NA	NA
CPU2 Memory	0x8000	NA	NA	NA	NA	NA	NA	NA
PwrOk Sig. Drop	0x8000	NA	NA	NA	NA	NA	NA	NA
PS1 Presence	0x8002	NA	NA	NA	NA	NA	NA	NA
PS1 Status	0x8008	NA	NA	NA	NA	NA	NA	NA

表 2-4 传感器界面各参数说明

参数	说明
传感器	传感器的名称。
当前值	传感器的当前值。
单位	传感器的取值单位。
紧急下门限	传感器值低于此下限值时，系统会产生紧急告警。
严重下门限	传感器值低于此下限值时，系统会产生严重告警。
轻微下门限	传感器值低于此下限值时，系统会产生轻微告警。
轻微上门限	传感器值高于此上限值时，系统会产生轻微告警。
严重上门限	传感器值高于此上限值时，系统会产生严重告警。
紧急上门限	传感器值高于此上限值时，系统会产生紧急告警。

指示灯

如图2-23所示，指示灯信息包括：指示灯名称、状态、支持颜色、本地控制默认颜色和逾越状态默认颜色。

指示灯状态包括：控制状态、点亮情况、当前颜色。

- 控制状态包括：本地控制状态、逾越状态。
  - 本地控制状态：由系统根据设备健康状态设定指示灯状态。
  - 逾越状态：由用户配置的指示灯状态。
- 点亮情况包括：亮、灭。

单击指示灯名称，可以设置指示灯状态信息，包括闪烁的时间、测试的持续时间、颜色、开/关状态。详细的参数说明如表2-5所示。

图 2-23 指示灯界面

表 2-5 指示灯设置参数说明

参数	说明
状态	指示灯的当前状态。

参数	说明
闪烁	指示灯的开启和关闭时间段。单击“指示灯颜色”下拉框选择指示灯闪烁时的颜色。 **说明** 闪烁时间取值范围:10毫秒～2500毫秒。
测试	指示灯持续的时间。单击“颜色”下拉框选择指示灯持续时的颜色。 **说明** 闪烁时间取值范围:100毫秒～12700毫秒。
开/关	点亮或关闭指示灯。
恢复正常模式	恢复指示灯当前模式为正常模式。

2.4.4 设备定位

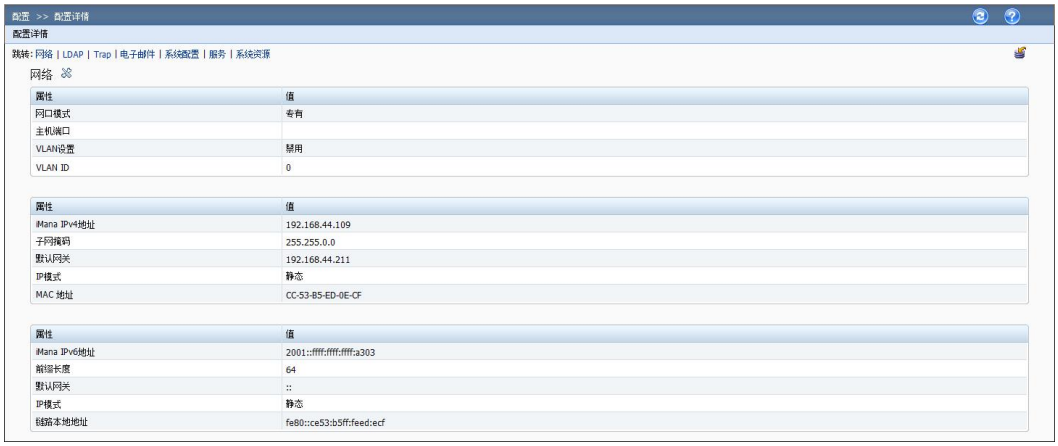
如图2-24所示，在设备定位界面，可以根据实际需要设置定位指示灯状态，通过点亮定位指示灯，使用户可以在机房的大量设备中，快速定位到需要执行现场操作的设备。

图 2-24 设备定位界面

2.4.5 配置详情

如图2-25所示，配置详情汇总了iMana智能管理控制器的所有配置，包含网络配置、LDAP、SNMP Trap、SMTP、系统配置和服务配置，便于一次性查看iMana全部配置信息，同时该界面也支持恢复出厂默认配置功能。

图 2-25 配置详情界面

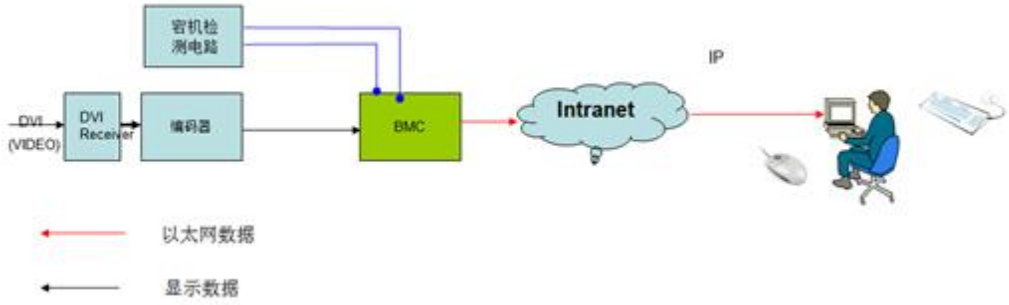


2.5 宕机截屏与宕机录像

2.5.1 宕机截屏

如图2-26所示，宕机截屏是iMana在检测到宕机发生时将系统临终时刻的屏幕以指定的格式保存在iMana的存储空间内。当用户发现系统宕机后，可以通过网络登录iMana查看宕机屏幕进行故障定位或者远程将宕机屏幕获取到本地进行查看。

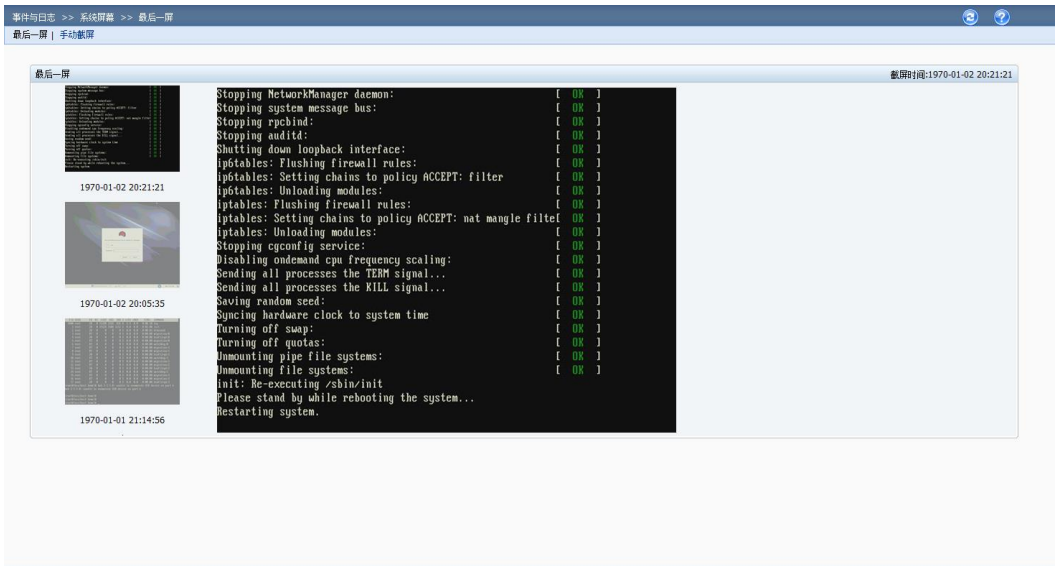
图 2-26 宕机截屏原理



iMana最多支持保存3个宕机截屏，并在下一次宕机时自动覆盖最旧的一次截屏数据。

可以参考“系统屏幕”通过Web查看宕机截屏，如图2-27所示。

图 2-27 宕机截屏界面



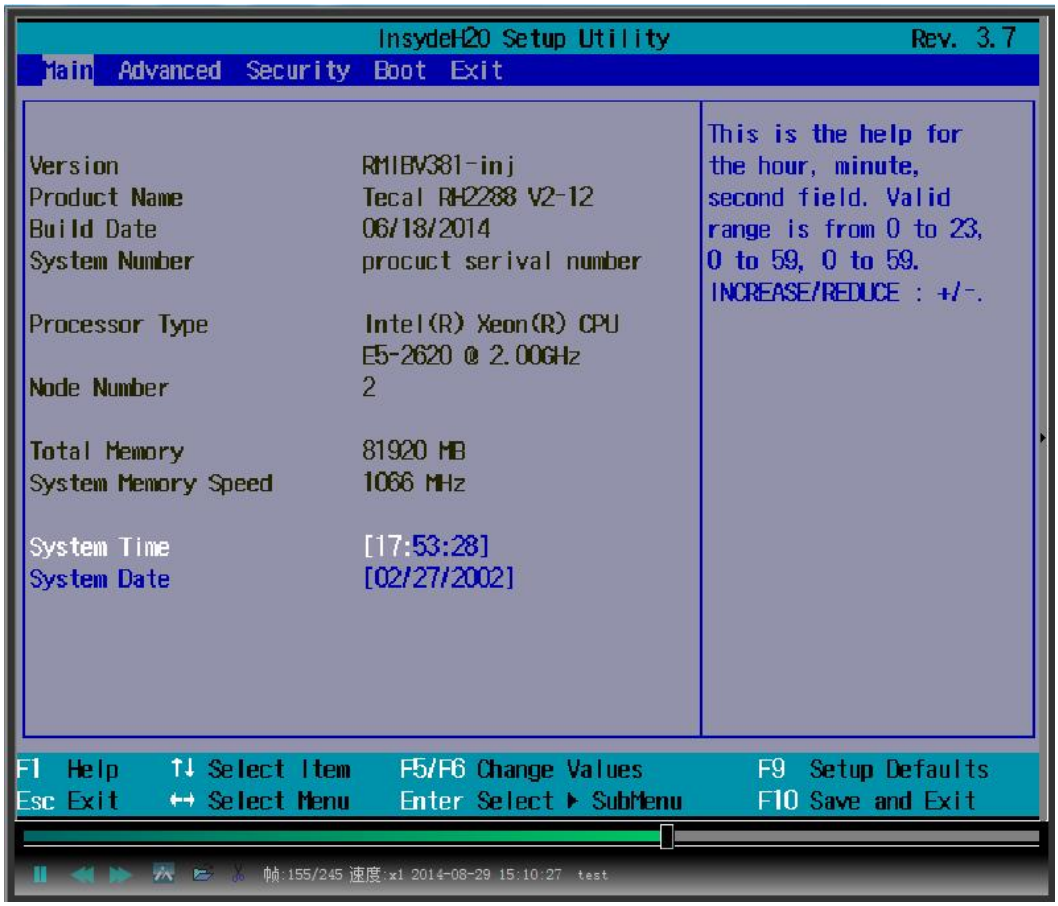
2.5.2 宕机录像

iMana在检测到系统宕机发生时会自动将宕机时刻前后各约一分钟的屏幕显示以压缩格式保存到外部存储器中，支持Host CAT Error、下电、重启场景的自动录像，其中Host

CAT Error场景的录像文件保存在iMana的FLASH，其它两种场景的录像文件保存到iMana的内存中。当用户发现系统宕机时，可以先将宕机录像文件导出到本地，然后再打开iMana的录像回放控制台在线播放，以帮助精确定位系统故障。

可以在“录像回放”页面中打开录像回放控制台，如图2-28所示。

图 2-28 录像回放控制台



2.6 屏幕快照和屏幕录像

2.6.1 屏幕快照

屏幕快照是iMana提供的一项方便系统巡检的功能，用户可以通过远程命令行（CLI）控制iMana管理软件对当前系统的屏幕输出进行截取并保存。当用户需要查看时可以通过远程将文件获取到本地使用图片查看软件浏览所有被巡检服务器的当前屏幕。

屏幕快照与虚拟KVM相比，省去了https登录过程，支持命令行接口，方便脚本集成实现服务器巡检自动化。此外通过web页面也可以获取当前系统屏幕快照。

通过命令行方式获取屏幕快照

截屏命令（printscreen）

用于截取服务器所显示的屏幕图片的printscreen命令。

命令功能

printscreen命令用于截取服务器所显示的屏幕图片。

命令格式

```
ipmcset -d printscreen -v wakeup
```

参数说明

加参数wakeup时该命令截取屏幕图片并唤醒系统屏保。

使用指南

执行printscreen命令后，iMana将自动把截图文件保存至tmp文件夹下，文件名为screen.bmp，查看此文件需要把图片文件通过FTP或TFTP传到可以查看.bmp文件的客户端中。

使用实例

```
# 截取当前服务器操作系统的屏幕。
root@BMC:/#ipmcset -d printscreen
Set printscreen successfully.
# 查询图片文件。
root@BMC:/#cd tmp
root@BMC:/tmp#ls
screen.bmp
```

通过 Web 界面获取屏幕快照

通过Web界面，可以在“系统屏幕”的手动截屏页面下进行“截屏”操作获取当前的系统屏幕快照，如图2-29所示。

图 2-29 手动截屏界面

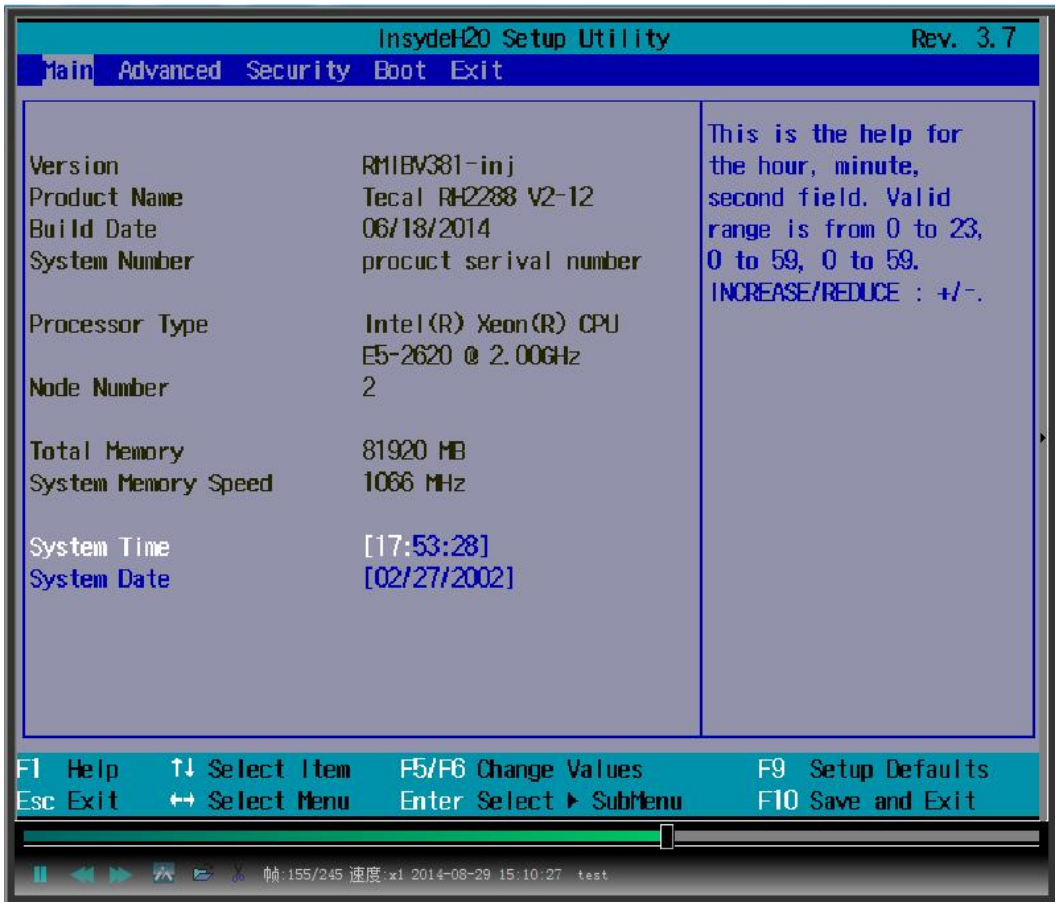
2.6.2 屏幕录像

屏幕录像是虚拟KVM控制台上提供的一项远程KVM录像功能，需手动启动，录像格式为自定义，录像数据保存在本地(打开KVM控制台的计算机)；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。

图 2-30 手动录像开启/关闭

iMana WEB界面集成了录像文件播放工具用于录像回放。

图 2-31 录像回放控制台



2.7 域管理和目录服务

随着企业应用的发展，IT基础架构的容量也越来越大，带来的资产管理和日常管理工作量也呈数量级增长。为了应对越来越繁重的IT基础架构管理工作，iMana智能管理系统提供了域管理和目录服务。

2.7.1 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iMana。如果在加入域的同时使用被管服务器的资产编号作为域名，还可以通过域控制器实现自动资产盘点，大大降低IT资产管理的成本。

步骤1 加入域。

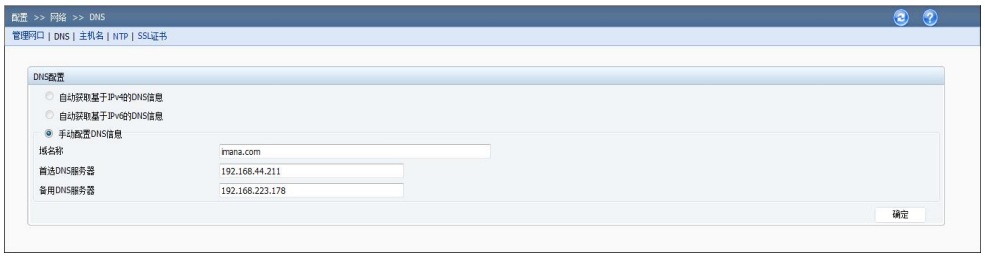
1. 在iMana的Web中打开“DNS”界面，如图2-32所示。

   说明

   DNS（Domain Name System）是因特网的一项核心服务，将域名和IP地址相互映射，使用户可以通过域名直接访问网络，而不必去记住对应的IP地址。

2. 在图2-32中，用户可以配置DNS绑定网口及DNS信息获取模式。设置完毕后单击“确定”执行操作。
3. 当用户选择“手动配置DNS信息”时，需要同时配置域名以及相应的首选、备用DNS服务器。

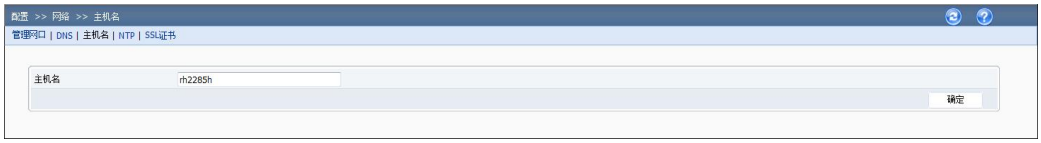
图 2-32 DNS 配置界面



步骤2 在如图2-33所示界面中设置主机名。

----结束

图 2-33 主机名配置界面



----结束

2.7.2 目录服务

按照如图2-34所示原理，启用iMana的目录服务，可以将所有iMana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iMana智能管理系统的安全性。

LDAP标准优点：

1、可扩展性：可以在所有iMana上同时动态支持LDAP服务器上新增账户的管理。

2、安全性：用户密码策略都在LDAP服务器上实施。

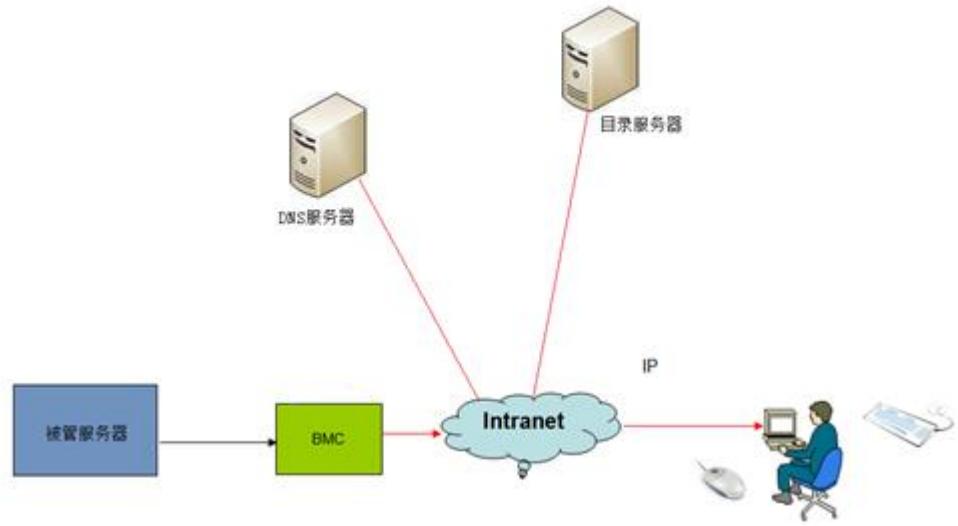
3、实时性：LDAP服务器上账户的任何更新都将立即应用到所有的iMana。

4、高效性：可以将所有iMana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。

5、支持性：支持Active Directory，支持NTLM认证机制。

从安全考虑，LDAP只支持SSL安全协议加密的LDAPS，不支持明文传输的LDAP，并且支持修改LDAPS端口；为了确保LDAP服务器的真实性，LDAP支持对服务器合法性验证功能，该功能开启后必须将LDAP服务器的根CA证书导入到iMana才能使用LDAP功能，且域控制器地址必须配置为与根CA证书里的证书使用者通用名称一致，因为在验证服务器合法性时会匹配域控制器地址与根CA证书的使用者名称是否完全一致。

图 2-34 目录服务原理



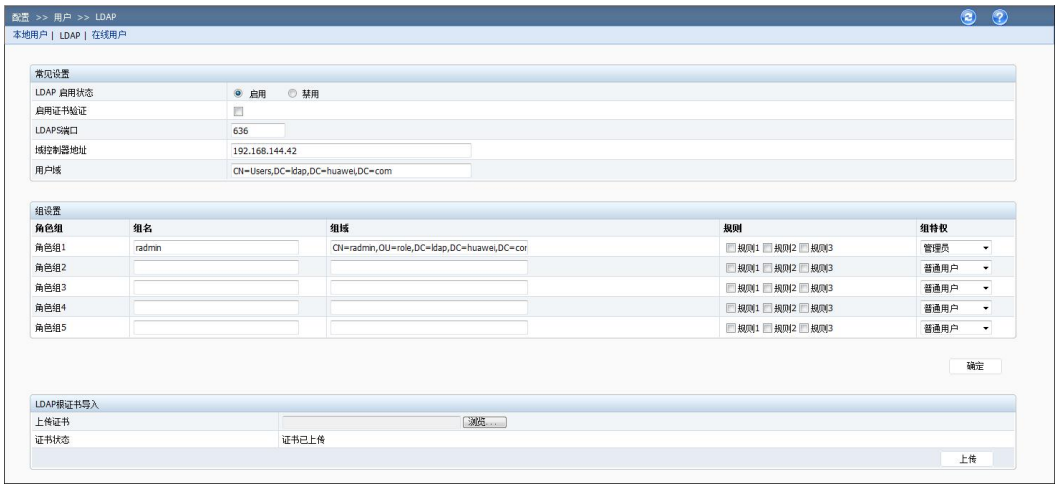
打开“LDAP用户”界面，如图2-35所示。

说明

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。

在图2-35中，可以显示或配置LDAP用户的相关信息。

图 2-35 LDAP 用户界面



通过LDAP用户界面可以完成的设置有：

- 启动或者禁止LDAP。
- 启用证书验证。
- 设置LDAPS的端口号，默认为636。

- LDAP服务器CA根证书导入。
- 设置域控制器地址。

  域控制器地址为活动目录active directory所在服务器的IP地址或域名。域控制器地址最大长度为255个字符。
- 设置用户域。

  用户域为配置活动目录active directory中登录iMana Web界面的用户的域。用户域最大长度为255个字符。
- 设置用户角色组名。

  组名为配置活动目录active directory中登录iMana Web界面的用户角色组的名称。组名最大长度为32个字符。
- 设置用户角色组域。

  组域为配置活动目录active directory中登录iMana Web界面的用户角色组的域。组域最大长度为255个字符。
- 设置用户角色组特权。

  组特权为配置活动目录active directory中登录iMana Web界面的用户角色组的特权。包括：管理员用户、操作员用户、普通用户三种权限。

2.8 固件管理

iMana可管理的固件包括iMana固件、BIOS、CPLD、LCD，支持固件版本查询、固件升级、双镜像切换。

2.8.1 固件双镜像

为了提升系统可靠性，iMana使用了固件双镜像备份技术。当在网运行过程中出现flash误操作或者存储块损坏时，系统会自动切换到备份镜像运行，并通过告警提醒镜像冗余降级。

通过命令行切换镜像

命令功能

rollback命令用来切换iMana当前和备份镜像文件。

命令格式

```
ipmcset -d rollback
```

参数说明

无

使用指南

无

使用实例

```
# 将iMana的当前镜像文件切换为备份文件。
root@BMC:/#ipmcset -d rollback
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Set rollback successfully, system will reboot soon!
```

通过 Web 切换镜像

在导航树上选择“配置与控制 > 固件升级”，打开“固件升级”界面。如图2-36所示。

在固件版本视图窗口中，显示iMana固件及BIOS固件的当前版本信息，并可进行镜像切换和重启iMana操作。

图 2-36 固件升级界面

2.8.2 固件升级

固件升级支持对iMana固件（含FPGA）、BIOS、CPLD（主板和硬盘背板）、LCD固件的升级；其中iMana固件支持版本回滚和两种生效方式（手动和自动），如图2-37所示。从兼容性考虑，建议用户将iMana主备镜像更新到同一个版本。

图 2-37 固件升级界面

2.9 智能电源管理

为了降低运营TCO，iMana智能管理系统提供了多种智能电源管理功能。

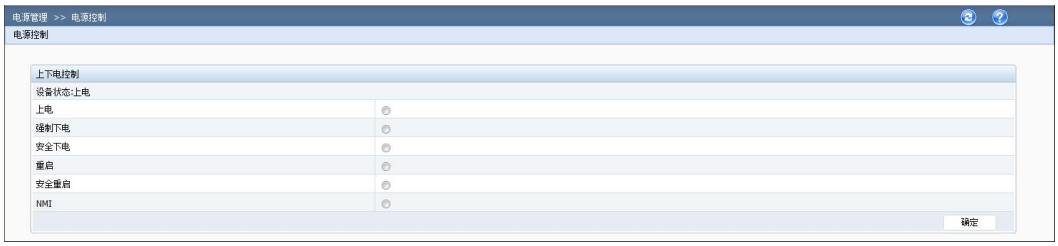
2.9.1 电源控制

电源控制功能提供对服务器的电源控制方式，如图2-38所示；支持屏蔽面板电源按钮，即:从安全和避免现场误操作考虑，支持对服务器面板电源按钮禁用功能。

服务器电源控制方式包括：上电、强制下电、安全下电、重启、安全重启。

- 上电：表示对服务器进行上电。
- 强制下电：表示对服务器进行下电，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。
- 安全下电：表示对服务器进行下电，iMana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，只能等到安全下电超时时间后，iMana将系统强制下电；效果相当于短按服务器面板上的电源按钮。
- 重启：表示对服务器进行冷复位，即：iMana直接拉南桥使系统复位，绕过正常的操作系统关闭流程。
- 安全重启：表示对服务器先安全下电再上电，即：先走正常的操作系统关闭流程并下电，若设置的安全下电超时时间内不能完成下电则强制下电，最后再上电。
- 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。

图 2-38 电源控制



2.9.2 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。iMana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。

在导航树上选择“电源管理 > 功率封顶”，打开“功率封顶”界面，如图2-50所示。

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。

在图2-39中，根据实际需要设置功率封顶使能状态、封顶功率、封顶失败进一步动作，单击“确定”按钮。设置成功后，界面将提示“操作成功”。

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。
- 关机：封顶失败后，系统将在15秒内执行强制下电操作。

图 2-39 功率封顶界面

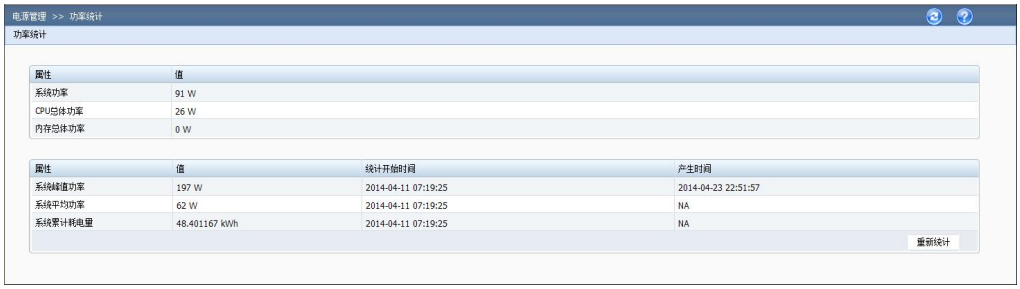
2.9.3 功率统计和历史曲线

iMana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。

在导航树上选择“电源管理 > 功率统计”，打开“功率统计”界面，如图2-40所示。在功率统计界面显示系统当前功率、CPU总功率、内存总功率以及特定时间段的峰值功率、平均功率、累计耗电量。

单击“重新统计”按钮可以对系统峰值功率、系统平均功率和系统累计耗电量重新进行统计。

图 2-40 功率统计界面

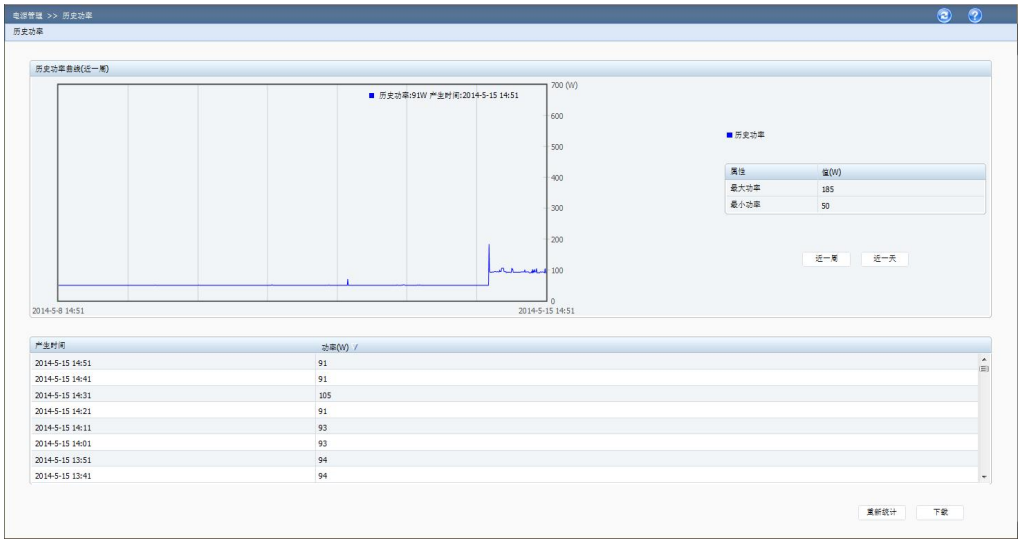


在导航树上选择“电源管理 > 历史功率”，打开“历史功率”界面，如图2-41所示。

历史功率界面中，通过曲线和表格的方式显示近期历史功率统计信息。单击“近一周”和“近一天”查看相应时间段的功率信息；单击“重新统计”可对历史功率曲线和对应表格进行刷新；单击“下载”可以下载历史功率信息。

通过此界面，用户可以更直观地观察到近期内设备的功率变化情况，更方便地了解到一段时间内设备的运行情况。

图 2-41 历史功率界面



2.9.4 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。

- 特性原理

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。

备用电源投入供电条件(主备模式切换为负载均衡模式)：

1. 主用电源拔出；
2. 主用电源输出电压低或无输出；
3. 主用电源温度过高、输入丢失、过流、过压；

4、 系统功率达到主用电源额定功率总和的75%时(注：小于65%时，用户设置的备用电源切回备用电源)。

主备供电界面如图2-42所示，提供电源供电总体工作模式、主用电源的设置接口。

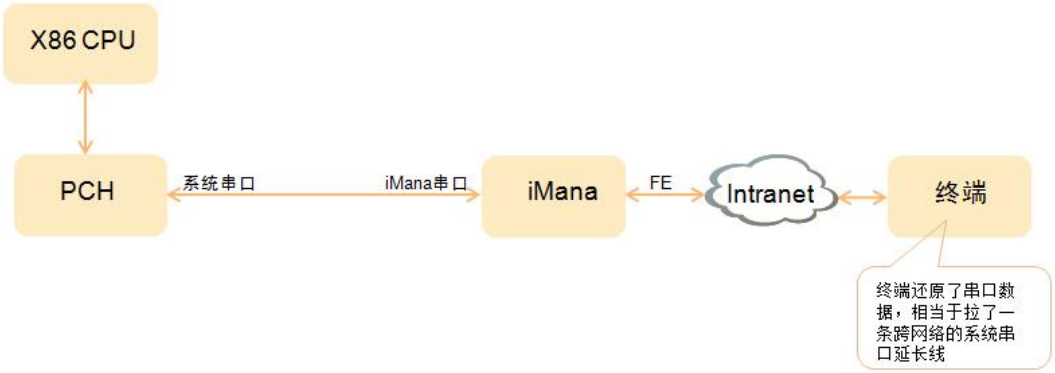
图 2-42 主备供电界面

2.10 系统串口重定向及运行记录

2.10.1 系统串口重定向

iMana提供系统串口重定向(SOL：Serial Over LAN)功能，即将原本只能从近端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2-43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一样的效果。

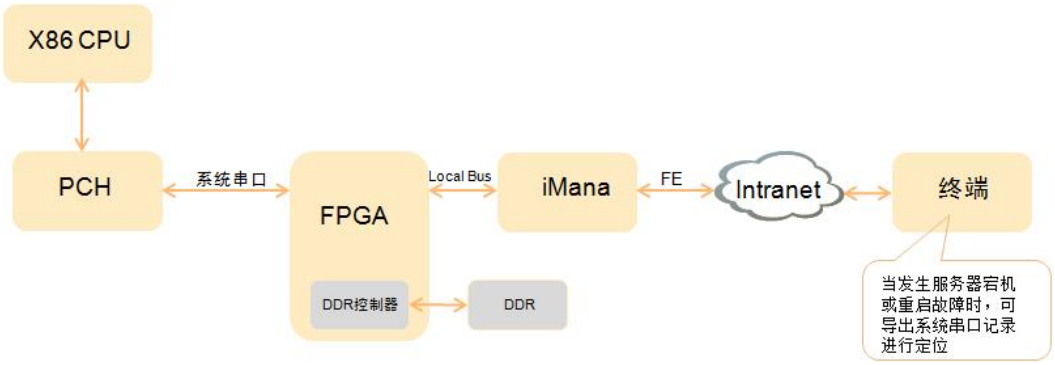
图 2-43 系统串口重定向原理



2.10.2 系统串口信息记录

iMana提供系统串口信息记录功能。如图2-44所示原理，系统串口信息记录将系统串口的实时数据记录到FPGA的DDR中，循环覆盖，最多保留最近1M字节的系统串口数据；当系统发生宕机或重启故障时，可以从iMana导出信息记录并查看详细的故障信息。

图 2-44 系统串口信息记录原理



2.11 安全管理

2.11.1 基于场景的登录限制

基于安全考虑，从时间、地点(IP/MAC)、用户三个维度将服务器管理接口访问控制在最小范围；目前该特性只针对WEB接口进行登录限制。

由用户根据需要设置登录规则的白名单，最多支持三条登录规则，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；

每条登录规则包括时间段、登录用户的源IP段和MAC段，这三个条件必须同时满足才认为匹配到一条登录规则；登录规则可应用于每个本地用户和LDAP用户组，用户默认不应用任何登录规则(即：无限制)；

访问时间到期后，用户被强制退出；支持配置一个紧急管理员用户（同密码有效期的紧急用户），该用户不应用任何登录规则，可用于在其他用户不可登录等异常情况下登录iMana管理。

三维立体象限：

时间段：包括开始时间和结束时间，时间格式必须一致，支持YYYY-MM-DD HH:MM、YYYY-MM-DD和HH:MM三种格式，允许为空；

IP段：支持单个IPv4地址或IPv4地址段，允许为空，目前不支持IPv6地址；

MAC段：支持单个MAC地址或MAC地址段(只填前三段，指定某个厂家网卡)，允许为空。

登录规则界面提供了登录规则设置和启用接口，如图2-45所示。

图 2-45 登录规则界面

2.11.2 账号安全

账号安全包括：密码复杂度、密码有效期、禁用历史密码重复次数和登录失败锁定。

密码有效期只针对所有本地用户，以天为单位，有效期内，用户可以登录并管理iMana；过期后，用户不再允许登录iMana，而已登录用户可继续访问iMana。

密码有效期范围为0~360天，0表示永久有效，从用户创建那天开始累计天数，按自然时间计算，服务器AC掉电期间的天数也计算在内，并且不受iMana时间更改的影响，iMana时间更改后，iMana会自动刷新每个用户的密码有效期开始时间。用户密码有效期天数小于10天时，登录WEB、CLI时有“密码将在xx天后过期，请及时修改密码。”的类似提示，密码过期后，会记录系统日志。

逃生通道：

1. 支持配置一个紧急管理员用户（同登录限制的紧急用户），该用户的密码有效期为永久；
2. 通过BIOS修改User ID为2的密码，该用户默认为管理员；
3. 在本机OS下通过BT通道使用ipmitool等第三方工具来修改过期用户的密码；
4. 刀片服务器还可以通过机框管理板来修改过期用户密码。

图 2-46 账号安全配置界面

2.11.3 SSL 证书管理

服务器SSL证书包括WEB服务端和WS-MAN服务端的证书，这两个服务端共用一套SSL证书。

SSL证书管理包括查看当前证书信息(证书的使用者、颁发者、有效期、序列号)、生成CSR文件、导入由CSR生成的签名证书（只有公钥，PKCS#7格式）、导入自定义证书（包含公钥和私钥，PKCS#12格式）；“证书导入匹配成功”或“恢复出厂默认配置”时，CSR文件将被删除；证书格式只支持Base 64编码的X.509格式，封装格式支持PKCS#7和PKCS#12两种，PKCS#12格式证书支持对私钥设置密码。

iMana的服务器SSL证书出厂默认使用自签名SSL证书，证书的签名算法使用SHA1和RSA(2048位)，从安全考虑，iMana提供了两种替换自签名证书的方法：

第一种方法：

1、登录到iMana Web，修改证书使用者信息；

2、生成CSR；

3、导出CSR；

4、将CSR提交给CA机构；

5、CA机构生成PKCS#7格式签名证书；

6、将签名证书导入到iMana；

7、重启iMana生效。

注意：签名证书必须与CSR配套，即：签名证书必须是通过该CSR申请的，否则导入证书失败。

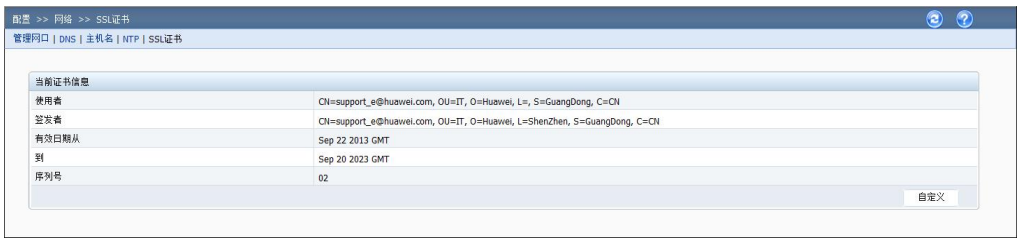
第二种方法：

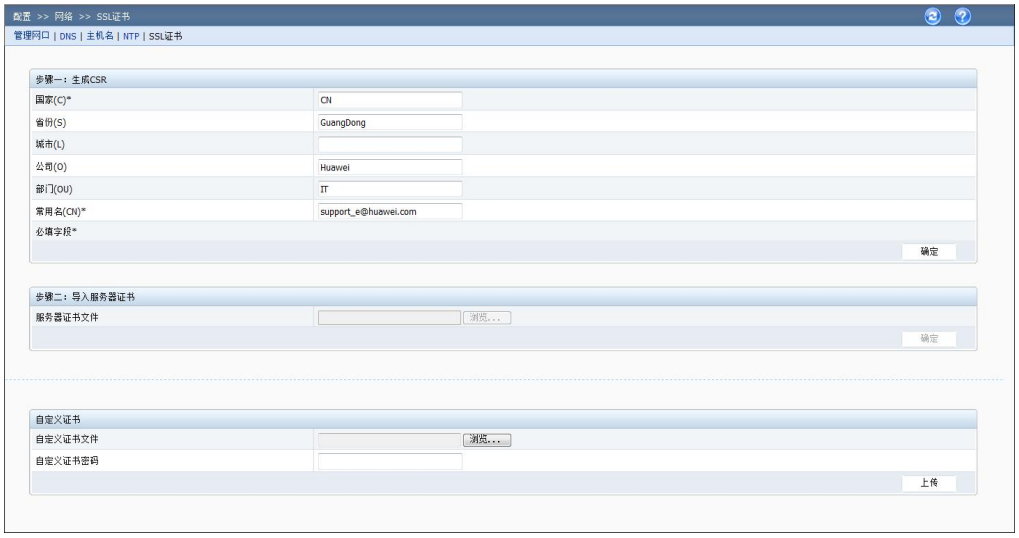
1、由客户通过自己搭建的CA服务器生成自定义证书或直接从CA购买证书；

2、登录到iMana Web，将自定义证书导入到iMana；

3、重启iMana生效。

图 2-47 SSL 证书管理界面





2.11.4 服务管理

服务的不安全协议和默认端口都是存在安全风险，需要提供接口进行开关和修改，满足客户的业务和安全需要；不安全协议(FTP/TELET/HTTP/RMCP)默认关闭。

如图2-48和图2-49所示，目前iMana主要服务包括Web、FTP、SSH、Telnet、Remote Control、WS-MAN、SNMP Agent、IPMI LAN。

图 2-48 SNMP 配置界面

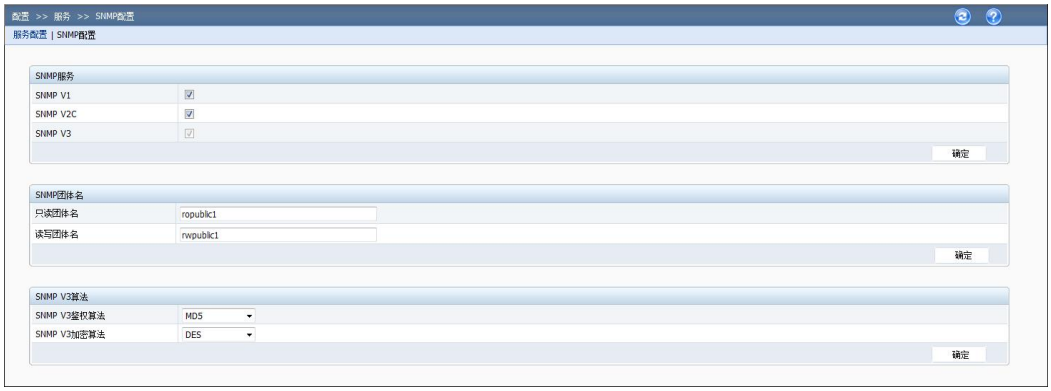


图 2-49 服务配置界面

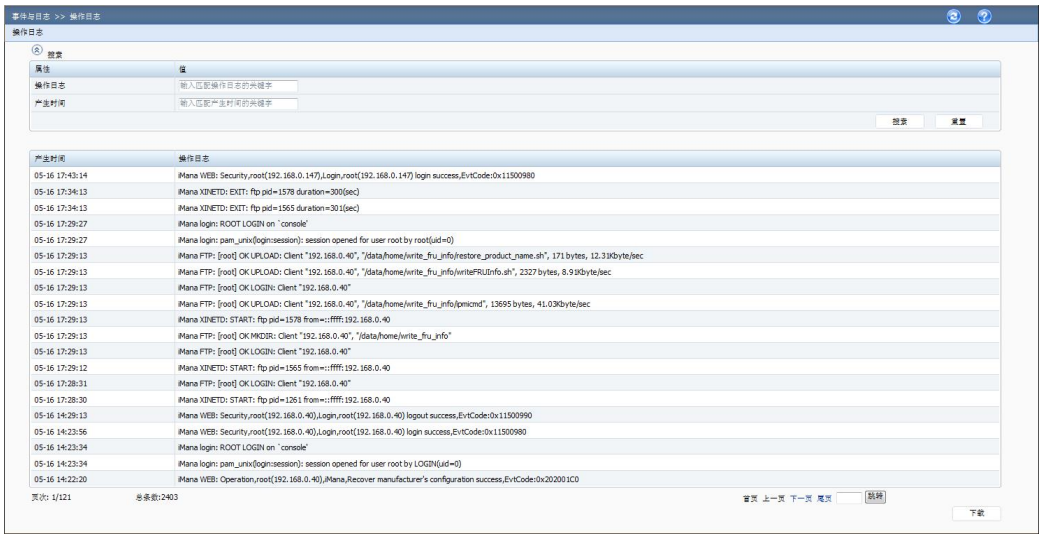
2.11.5 操作日志管理

记录了iMana所有接口的非查询操作，为防止暴力攻击(如：尝试登录)的大量日志覆盖掉正常日志，所以只记录了执行成功的操作；操作日志分两类，一类是linux系统进程的日志，另一类是用户进程的日志；用户进程记录的日志包括操作类型、操作源IP、操作源用户、执行动作、动作描述、日志码。

操作日志写文件，当达到100K字节大小后自动备份，最多备份3份日志文件，超过3份后自动将最早的备份文件删除。

操作日志支持在WEB上查看、筛选、导出。

图 2-50 操作日志查看界面



2.11.6 高强度加密算法

加密算法为交互双方提供了如下安全保障：

- 机密性(Confidentiality)：机密性也称为保密性，是指敏感信息不泄露给未经授权的实体。例如当使用口令登录或往数据库中储存机密医疗档案时，采用加密的方式能够确保只有拥有相应密钥的用户能够访问被保护的数据。
- 完整性(Integrity)：采用密码学相应手段能保证信息在储存和传输过程中不被修改。如使用哈希函数可以为数据提供校验来保证数据安全。
- 真实性(Authenticity)：使用密码算法相应方式可以确定远程用户或系统的身份。比如Web服务器提供的SSL证书能够保证用户连上的是正确的服务器。
- 不可抵赖性(Non-Repudiation)：不可抵赖性的概念在财务和电子商务应用中非常重要，它通过密码学工具或手段来证明一个唯一的用户进行了交易请求。用户是不可能对他或她的行为进行否认的。

iMana支持的加密算法如下：

表 2-6 加密算法表

加密算法	应用场景	用途
DSA/RSA 2048位	WEB/WS-MAN服务端证书、SSH主机证书	数字签名
AES 128 CBC	IPMI LAN传输加密、KVM键盘/视频/控制数据、VMM数据加密、WS-MAN HTTPS传输加密、WEB的HTTPS传输加密、SNMP V3传输加密、SSH传输加密	加密
AES 256 CBC	WS-MAN HTTPS传输加密、WEB的HTTPS传输加密、SSH传输加密	加密
DES 64	SNMP V3协议传输加密	加密
HMAC-MD5-96	SNMP V3协议认证	鉴权
HMAC-SHA1-96	SNMP V3协议认证、IPMI LAN鉴权	鉴权
SHA256	HTTPS完整性校验、linux用户密码加密	完整性、加密

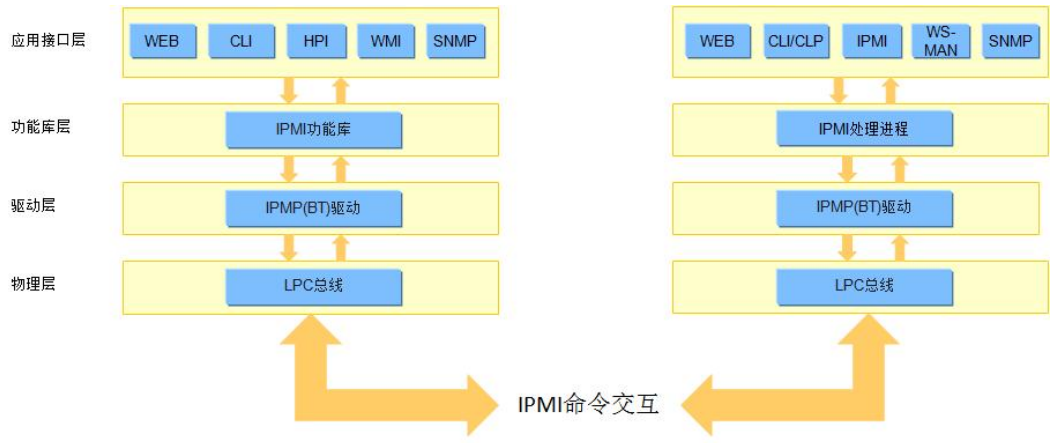
2.12 统一通信接口

服务器内存在两个独立系统：主机系统(带内)和管理小系统(带外)，分别拥有自己的CPU、内存和存储器，物理上隔离，两个系统基于内部LPC总线之上的BT协议通讯。

BMA(Board Management Agent)是一个服务器配套的运行在主机系统OS上的带内管理模块，服务器发货时不携带该模块且安装OS时也不会自动安装该模块，需要手动独立安装。关于BMA模块的详细介绍，请登录http://support.huawei.com/enterprise/productsupport，搜索《服务器 BMA V100R002 用户指南》。

为了简化组网，增强管理功能，带内外都需要从另一端获取一些重要的信息，比如：带外需要从带内获取系统资源使用率、硬盘信息等信息；带内需要从带外获取电源和风扇等相关信息。统一接口功能就是为了解决这些问题而实现的。

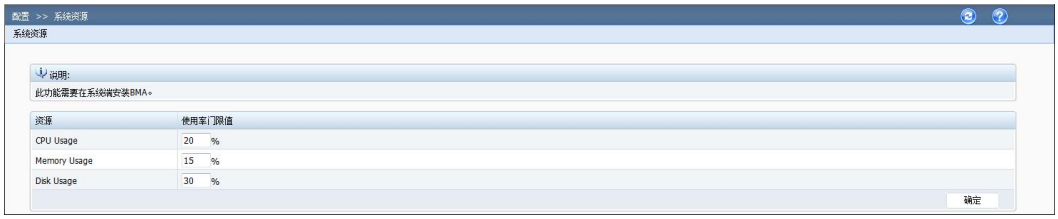
图 2-51 iMana 与 BMA 数据交互



2.12.1 系统资源监控

系统资源包括CPU、内存和磁盘，它们的使用率带外无法直接获取；系统资源使用率监控是在统一通信接口平台之上实现的一个功能，BMA负责对系统资源使用率进行实时检测和比较，一旦使用率超过门限值(连续多次检测)，则通知iMana，而iMana负责上报告警以及提供接口修改使用率门限值；目前，iMana只提供了WEB界面查看和设置系统资源使用率门限值，从影响考虑，门限值默认为100%；系统资源门限值存储在iMana的FLASH中，BMA定时从iMana读取门限值并更新。

图 2-52 系统资源使用率配置界面



2.12.2 硬盘信息

硬盘信息包括制造厂商、最大转速、容量、总线协议类型、序列号、联机状态、RAID重构进度、型号、固件版本这些物理硬盘属性；这些信息都是客户非常关心的，目前iMana在技术上很难直接从RAID卡获取，但是通过带内很容易获取到。基于统一通信接口平台，BMA在启动或发现硬盘变更或RAID重构时及时读取硬盘相关信息并更新到iMana内存，刷新iMana的资产信息WEB页面即可查看到在位硬盘的信息。目前该功能只支持RAID卡管理域的硬盘。

2.13 管理接入

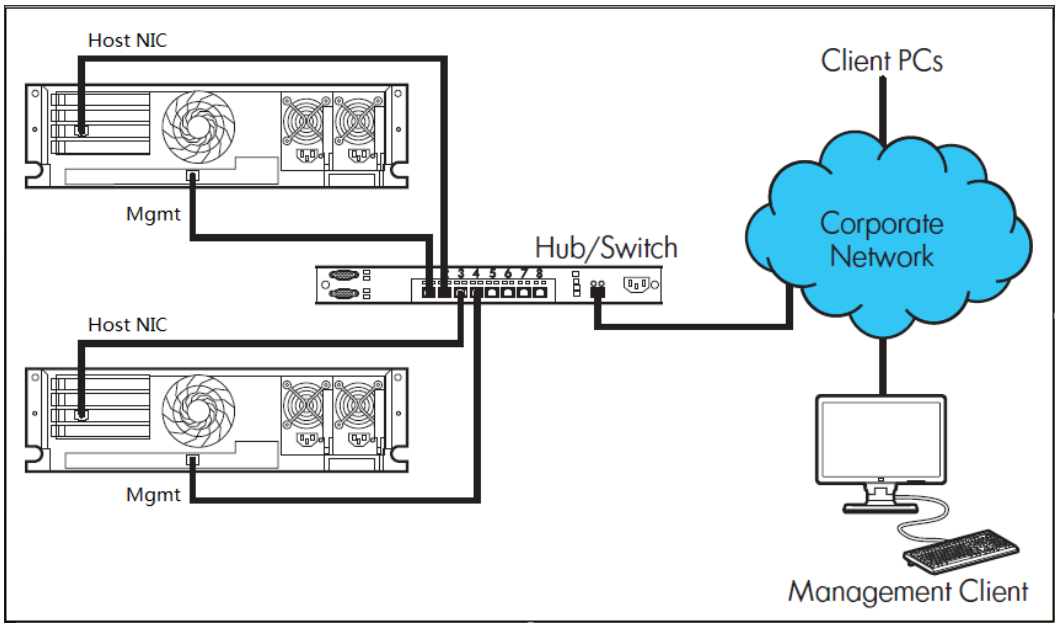
目前，iMana兼容支持了IPv4和IPv6两种协议版本地址，支持通过专用管理网口或共享网口(利用NCSI边带功能)接入，其中共享网口支持VLAN功能。

2.13.1 管理网口自适应

机架和节点服务器有两个物理管理网口：一个专用管理网口和一个边带管理网口(NCSI，与主机系统共用物理网口)，此功能是根据网口link状态，自动将逻辑网口与其中一个物理网口适配。

网口自适应启用后，服务器更换组网后只要专用管理网口或边带管理网口任一网口连接了网线即可访问管理界面，平滑切换，不需要再配置任何网络信息，省去繁杂的配置步骤，提升维护效率。

图 2-53 管理组网图



网口自适应配置界面提供了网口模式查询和设置接口，若是自适应模式，则支持配置哪个主机网口作为边带网口，默认为网口1，如图2-54所示。

图 2-54 网口自适应配置界面

2.13.2 边带管理

边带管理(iMana界面称共享网口)就是利用边带(NCSI)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；从业务数据优先角度考虑，管理数据最大带宽限制在100MB/S；从安全考虑，利用VLAN技术将管理与业务划分在不同在网段。

图 2-55 边带管理框图

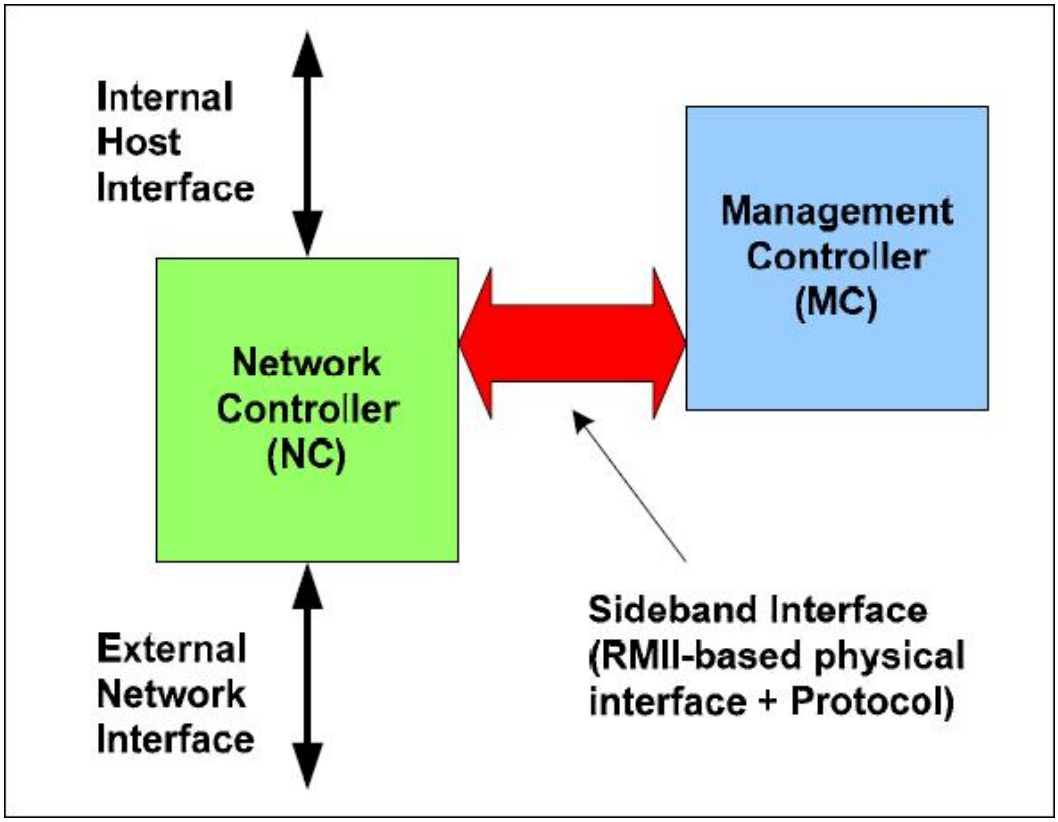
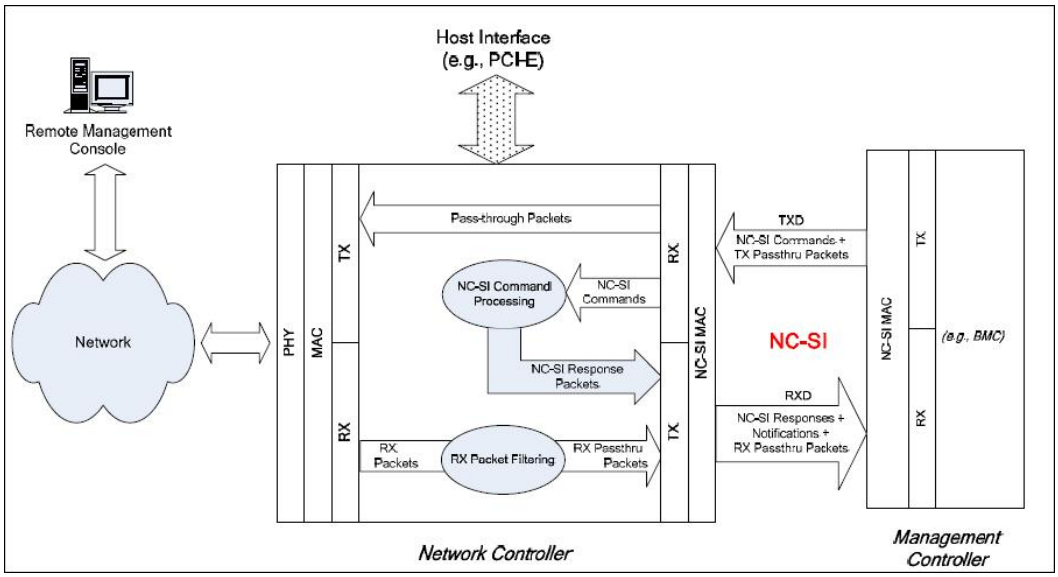


图 2-56 边带管理数据流图



2.13.3 IPv6

IPv4地址资源很快面临枯竭，解决办法是使用IPv6地址，iMana已经正式全面支持了IPv6地址功能。目前iMana的WEB、Telnet、SSH、SNMP、WS-MAN和IPMI LAN接口模块

都已支持IPv6地址访问，专用管理网口和共享网口(NCSI)的物理通道也都支持IPv6地址访问。

图 2-57 IPv6 地址配置界面

支持手动设置或DHCP获取iMana的IPv6地址。

2.14 统一用户管理

iMana是一个基于嵌入式CPU和OS的管理子系统，OS和应用对外是一个封闭的整体，只提供了固定的维护、集成接口。OS(CLI)、SNMP、IPMI LAN、WEB等这些对外接口各自都有一套独立的本地用户管理，对用户来说，要想通过这些接口都能接入，则必须重复四遍配置用户的动作，非常繁琐。因此，我们提供了统一用户管理的功能，只要在上述任一接口配置好用户，即可使用该用户登录iMana所有接口，也就是说所有接口呈现的本地用户是同一套；iMana后台自动完成了各个接口的用户同步。

本地用户最多支持17个用户(含USERID为1的匿名用户)，支持增加、修改和删除用户；所有用户划分为管理员、操作员和普通用户三个权限组，每个组的具体权限如下(以WEB为例，OS的操作员和普通用户的用户都只有普通用户权限)：

管理员：拥有iMana的所有配置和控制权限；

操作员：相对于管理员，拥有除用户管理和安全配置外的所有配置和控制权限；

普通用户：只有查看权限，除OS相关信息和操作日志查看外的所有查看权限。

图 2-58 用户管理界面

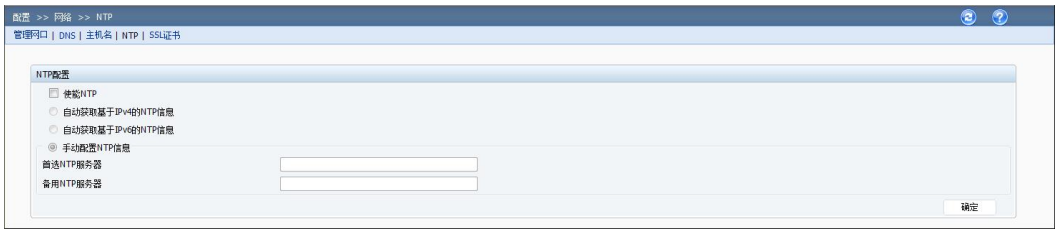
2.15 NTP

NTP(Network Time Protocol)是用来使计算机时间同步的一种协议。iMana自身没有RTC，但支持从多个时间源同步时间且同一时间只能从一个时间源同步，时间源见表2-7。NTP功能默认关闭且支持开启，支持手动设置或自动获取首选和备用NTP服务器地址(支持IP的v4和v6版本)，手动设置时NTP服务器地址还支持FQDN域名输入。

表 2-7 iMana 时间源

iMana	支持时间源	默认时间源
机架服务器	系统RTC（BIOS/OS）、NTP	系统RTC（BIOS/OS）
刀片服务器	机框管理板	机框管理板
高密度服务器	系统RTC（BIOS/OS）、NTP	系统RTC（BIOS/OS）

图 2-59 NTP 配置界面



3 产品规格

组件	规格
支持的产品	BH620 V2(JDM)、BH621 V2(JDM)、BH622 V2、BH640 V2、RH1288 V2、RH2285 V2、RH2285H V2、RH2288 V2、RH2288H V2、RH2485 V2、RH5885H V3、RH2288E V2、XH310 V2 (JDM)、XH311 V2(JDM)、XH320 V2、XH321 V2、XH621 V2、DH320 V2(X8000和X6000共用)、DH321 V2(X8000和X6000共用)、DH620 V2、DH621 V2、DH628 V2
KVM	● 支持最大分辨率：1280*1024 ● 支持最小分辨率：400*400 ● 支持255种颜色
网络接口	● 1个集成的百兆专用以太网接口。 ● 1个集成的百兆共享以太网接口。
虚拟媒体	● 虚拟光驱支持最大传输速率32 Mbit/s ● 虚拟软驱支持最大传输速率4 Mbit/s
用户接口	● HTTPS ● IPMI LAN/BT ● SNMP ● WS-MAN ● CLI ● SMASH-CLP
安全特性	● 支持用户管理 ● 支持角色鉴权 ● 支持数据加密 ● 基于场景的登录限制 ● 账号安全 ● SSL证书管理