浪潮物理基础设施管理平台(ISPIM)技术白皮书

文档版本 V1.3

发布日期 2021-12-30

环境保护

请将我方产品的包装物交废品收购站回收利用，以利于污染预防，共同营造绿色家园。

商标说明

Inspur 浪潮、Inspur、浪潮、英信是浪潮集团有限公司的注册商标。
本手册中提及的其他所有商标或注册商标，由各自的所有人拥有。

安全声明

账户密码的声明

产品支持不同物理设备的集中管理，会使用到物理设备的账户密码，相关密码已经在数据库中加密存储。密码支持文件格式导出，导出文件中的密码未加密，建议您导出后进行必要的安全措施，防止密码被泄露。

个人数据的声明

出于您方便运维的目的，在使用过程中可按需采集个人数据，例如：运维人员信息、驻场人员信息、告警邮箱等。对于这部分信息，本产品提供了如下保护途径

- 加密存储，个人数据信息在数据库中加密存储。
- 权限控制，Web界面上个人数据查看等功能仅提供给具有对应权限的管理员使用。

建议您根据所适用国家或地区的法律法规制定必要的用户隐私政策并采取足够的措施以确保用到的个人数据受到充分的保护。

协议使用的声明

- 本产品支持通过LDAP认证。LDAP支持LDAP over SSL（LDAPS），进行加密

传输，建议您使用636端口，使用LDAPS安全认证。

- 本产品支持通过syslog协议转储日志。syslog支持syslog over SSL，进行加密传输，建议您使用syslog over SSL方式进行日志转储，保证日志数据传输安全。
- 本产品支持通过SNMP协议发现设备。SNMP协议共有三个版本SNMPv1、SNMPv2c和SNMPv3。使用SNMPv1、SNMPv2c版本存在安全风险，建议您使用SNMPv3方式进行设备发现。

升级、打补丁的声明

本产品进行版本升级或补丁安装前，建议您核对产品哈希值或数字签名，校验升级软件的合法性，避免软件被非法篡改或替换，给您带来安全风险。

安全响应的声明

浪潮已全面建立产品安全漏洞应急和处理机制，确保第一时间处理产品安全问题。若您在本产品使用过程中发现安全问题，或者寻求有关产品安全漏洞的必要支持，请直接联系浪潮客户服务人员。

浪潮将一如既往的严密关注产品与解决方案的安全性，为客户提供更满意的服务。

内容声明

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，浪潮集团对本文档的所有内容不做任何明示或默示的声明或保证。文档中的示意图与产品实物可能有差别，请以实物为准。本文档仅作为使用指导，不对使用我们产品之前、期间或之后发生的任何损害负责，包括但不限于利益损失、信息丢失、业务中断、人身伤害，或其他任何间接损失。本文档默认读者对服务器产品有足够的认识，获得了足够的培训，在操作、维护过程中不会造成个人伤害或产品损坏。文档所含内容如有升级或更新，恕不另行通知。

技术支持

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

前言

摘要

本文档主要介绍浪潮服务器运维软件/工具的产品主要功能、基础操作、常见问题等相关内容

目标受众

本手册主要适用于以下人员：

- 技术支持工程师
- 产品维护工程师

建议由具备服务器知识的专业工程师参考本手册进行服务器运维操作。

注意

- 如您未采购装机服务，请在设备开箱前自行检查外包装箱。如发现包装箱严重损坏、水浸、封条或压敏胶带已开封，请视购机方式进行问题反馈。供应商渠道购入设备，请直接与您的供应商联系；浪潮直营渠道购入设备，请直接拨打服务电话4008600011，联系浪潮技术支持处理。
- 请不要随意拆装服务器组件、请不要随意扩配及外接其它设备。如需操作，请务必在浪潮的官方授权和指导下进行。
- 在拆装服务器组件前，请务必断开服务器连接的所有电缆。
- 请使用浪潮认证的驱动程序进行 OS 环境搭建。您可访问浪潮官网进行驱动下载，进入浪潮官网首页，顶部导航栏选择支持下载 > 产品支持 > 驱动下载，根据页面提示查找产品对应的驱动程序。如使用非浪潮认证的驱动程序，可能会引起兼容性问题并影响产品的正常使用，对此浪潮将不承担任何责任或义务。
- BIOS、BMC 的设置对配置您的服务器至关重要，如果没有特殊的需求，请您使用系统出厂时的默认值，请勿随意更改参数设置。首次登录时，请及时修改 BMC 用户密码。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

图标	说明
 危险	如不当操作，可能会导致死亡或严重的人身伤害。
 警告	如不当操作，可能会导致人员损伤。
 注意	如不当操作，可能会导致设备损坏或数据丢失。
 提示	为确保设备成功安装或配置，而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。

变更记录

文档版本	发布日期	修改说明
V1.3	2021-12-30	● 第三次正式发布 ● 合入 V6.2.0 新增/优化功能
V1.2	2021-03-30	● 第二次正式发布 ● 合入 V6.1 新增/优化功能
V1.1	2020-10-30	● 新增“边缘盒子”、“一体机”、“安全设备”等相关内容 ● 新增浪潮服务器全生命周期固件变更、故障状态追溯 ● 新增物理链路自动拓扑、支持手动自定义网络拓扑 ● 新增带内秒级性能监控及高性能 HPC 集群监控 ● 新增服务器宕机、部件故障后的根因定位及修复建议 ● 支持分布式数据分析框架，支持横向平滑扩展 ● 优化其他功能描述 ● 更新部分规格
V1.0	2020-03-30	第一次正式发布

目录

1 文档指南.....1
2 产品简介.....2
2.1 产品定位.....2
2.2 关键技术特性.....3
3 系统架构.....5
3.1 软件架构.....5
3.2 上下文对接方式.....6
4 功能特性.....8
4.1 快速灵活的纳管方式.....8
4.1.1 全网设备纳管.....8
4.1.2 SR 机柜纳管.....8
4.1.3 一体机纳管.....9
4.1.4 刀箱纳管.....9
4.1.5 边缘盒子纳管.....9
4.1.6 网络设备纳管.....9
4.1.7 安全设备纳管.....9
4.1.8 存储纳管.....9
4.2 智能资产管理.....9
4.2.1 用户场景问题.....10
4.2.2 方案介绍.....10
4.2.3 特性介绍.....11

4.3 设备全方位监控 13
4.3.1 设备信息及告警多维度呈现 14
4.3.2 设备告警管理 18
4.3.3 设备性能监控 19
4.3.4 设备故障诊断 20
4.3.5 智能告警对接 21
4.4 智能的能耗管理 21
4.4.1 用户场景问题 22
4.4.2 功耗性能历史曲线 22
4.4.3 功耗策略 23
4.4.4 能耗优化 23
4.5 高效的无状态管理 26
4.5.1 标准化的基线管理 26
4.5.2 高效快捷的固件管理 27
4.5.3 简便易用的部署管理 33
4.5.4 统一的镜像文件管理 34
4.5.5 便捷的自动上线规划 34
4.6 可视化拓扑管理 35
4.6.1 3D 拓扑 35
4.6.2 网络拓扑 36
4.7 智能容灾分布式管理 37
4.7.1 采集器 38

4.7.2 分析器 38
4.7.3 负载均衡器 39
4.8 至关重要的安全管理 39
4.8.1 用户管理 39
4.8.2 鉴权管理 39
4.8.3 安全配置 40
4.8.4 证书管理 40
4.9 标准的北向接口 40
4.9.1 用户场景问题 40
4.9.2 方案介绍 40
4.9.3 客户价值 41
5 部署方案 42
5.1 部署方式 42
5.1.1 单节点部署 42
5.1.2 高可用部署 42
5.1.3 采集分析集群部署 42
5.2 升级方式 43
6 安全性 44
6.1 组网约束 44
6.2 系统安全 46
6.3 应用安全 46
7 可靠性 48

7.1 集群可靠性.....48
7.2 数据可靠性.....48
8 配置要求.....49
A 如何获取帮助.....1
A.1 收集必要的故障信息.....1
A.2 如何使用文档.....1
A.3 获取技术支持.....1
B 术语和缩略语.....2

1 文档指南

本章节主要介绍 ISPIM 产品相关文档及内容说明。

表 1-1 文档指南

类型	文档名称	内容介绍	手册获取
了解产品	技术白皮书	描述 ISPIM 的产品定位，技术架构及各项规格参数。	《浪潮物理基础设施管理平台(ISPIM) V6.2.0 白皮书》
安装与测试	部署手册	描述 ISPIM 的安装操作、初始化配置，并给出常用操作和故障处理方法。	《浪潮物理基础设施管理平台(ISPIM) V6.2.0 部署手册》
操作类	用户手册	描述 ISPIM 的功能特性和操作指导。	《浪潮物理基础设施管理平台(ISPIM) V6.2.0 用户手册》

2 产品简介

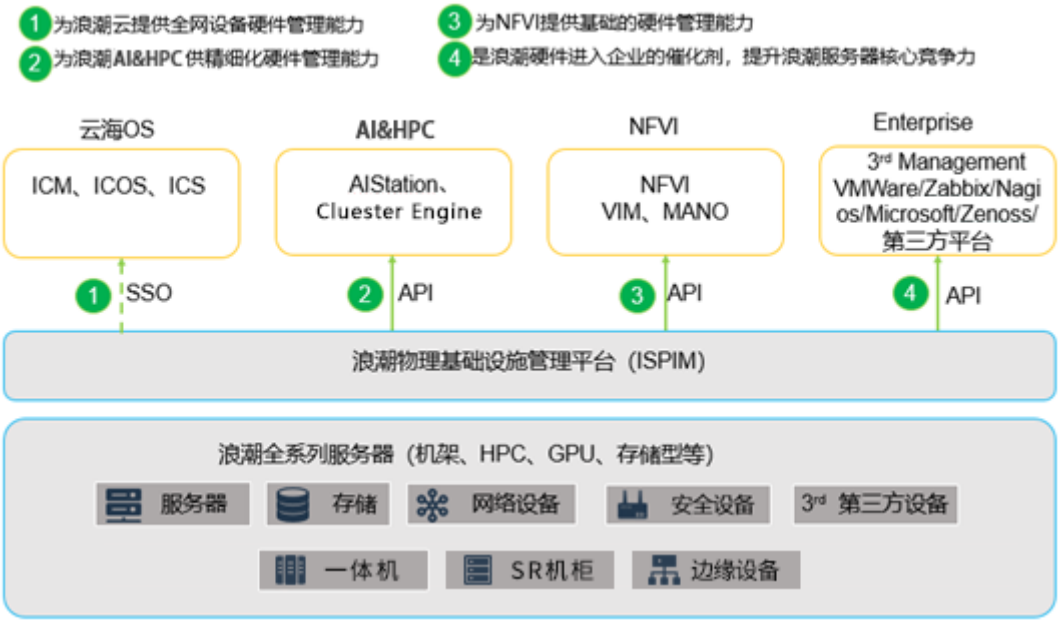
2.1 产品定位

浪潮物理基础设施管理平台（Inspur Physical Infrastructure Manager，以下简称“ISPIM”），是浪潮根据市场需求，遵循 NFV 标准，自主研发的一款高可用、高性能、高可扩展、高可维护的行业数据中心物理基础设施管理平台。

ISPIM 定位为行业数据中心运维管理软件，是新一代数据中心物理基础设施的全生命周期运维管理平台。该平台覆盖市面多品牌 IT 设备，具备资源管理、故障监控、性能监控、能耗管理、报表统计、拓扑展示、服务器故障诊断、自动报修、固件升级/配置、OS 部署等功能。ISPIM 可统一管理服务器、存储、网络、安全等异构设备，真正促进了数据中心智能化管理，可帮助客户打造无人值守数据中心，提高运维效率、降低运维成本，保障数据中心安全、可靠、稳定的运行。

ISPIM 可广泛应用于公有云、私有云、数据中心、运营商和企业客户，在 AI、HPC、互联网、智慧城市等多场景下部署，同时提供 Restful、SNMP 等接口，便于用户集成与对接。

图 2-1 ISPIM 所在位置



2.2 关键技术特性

多场景轻量化部署，全生命周期管理

ISPIM 提供多种场景部署能力，从多类型虚机（KVM/VMware）到裸机场景部署，可满足小型企业、大中型企业对于全网设备特别是服务器全生命周期管理的要求。

具备高可靠能力，1-N 的数据采集、分析节点按需扩展

ISPIM 可满足多业务场景需求，提供高可靠能力，并具备采集、分析节点数从 1 到 N 的平滑扩展能力，以应对用户扩容及多数据中心的场景且不影响原有监控业务。

智能资产管理功能，资产变更实时跟踪

ISPIM 提供全自动、端到端的资产管理能力，包括：设备上架、位置识别、配置核查、资产位置变更、部件变更、设备下架等，实现了资产全生命周期的变更追溯。

全方位监控，把控业务全局

ISPIM 提供全网设备硬件状态监控、性能指标实时监控的能力，可帮助运维人员快速发现故障并及时处理故障。

智能故障诊断，缩短维修周期

ISPIM 基于浪潮故障专家库，打通浪潮 360°专家服务，实现了浪潮服务器智能故障诊断、故障根因定位、专家维修建议，设备自动报修等功能。

秒级性能监控，掌握设备实时状况

ISPIM 对接带内驱动 ISMD 可实现实时性能采集，实时接收设备运行性能指标，并凭借自研性能分析核心组件，可支撑上万台服务器同时进行秒级性能数据的监控与告警，帮助运维人员实时掌握设备的性能状况。

批量化升级、配置与部署，缩短上线周期

ISPIM 提供批量固件升级、硬件配置、系统部署、运维软件部署等功能，可显著提升服务器上线运维效率。

版本管理，提升版本管理效率

ISPIM 提供固件及 OS 镜像本地管理与远程官网自动同步的能力，提升数据中心设备

软硬件版本管理效率。

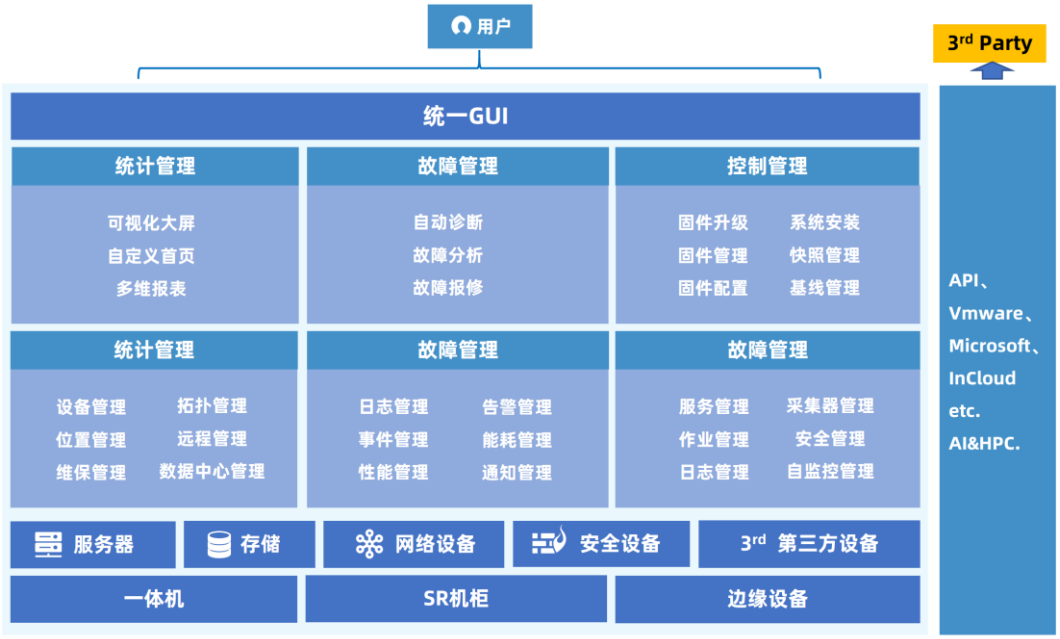
标准化的北向接口，方便用户集成对接

ISPIM 提供标准 Redfish、SNMP 接口，在此基础上可扩展功能，便于用户集成对接。

3 系统架构

3.1 软件架构

图 3-1 ISPIM 软件架构



集中管理调度中心

- 基础特性：监控、告警、升级、安全、DFX 等。
- 五大功能：资产管理、故障管理、能耗管理、无状态管理、拓扑管理。

支持全网设备管理

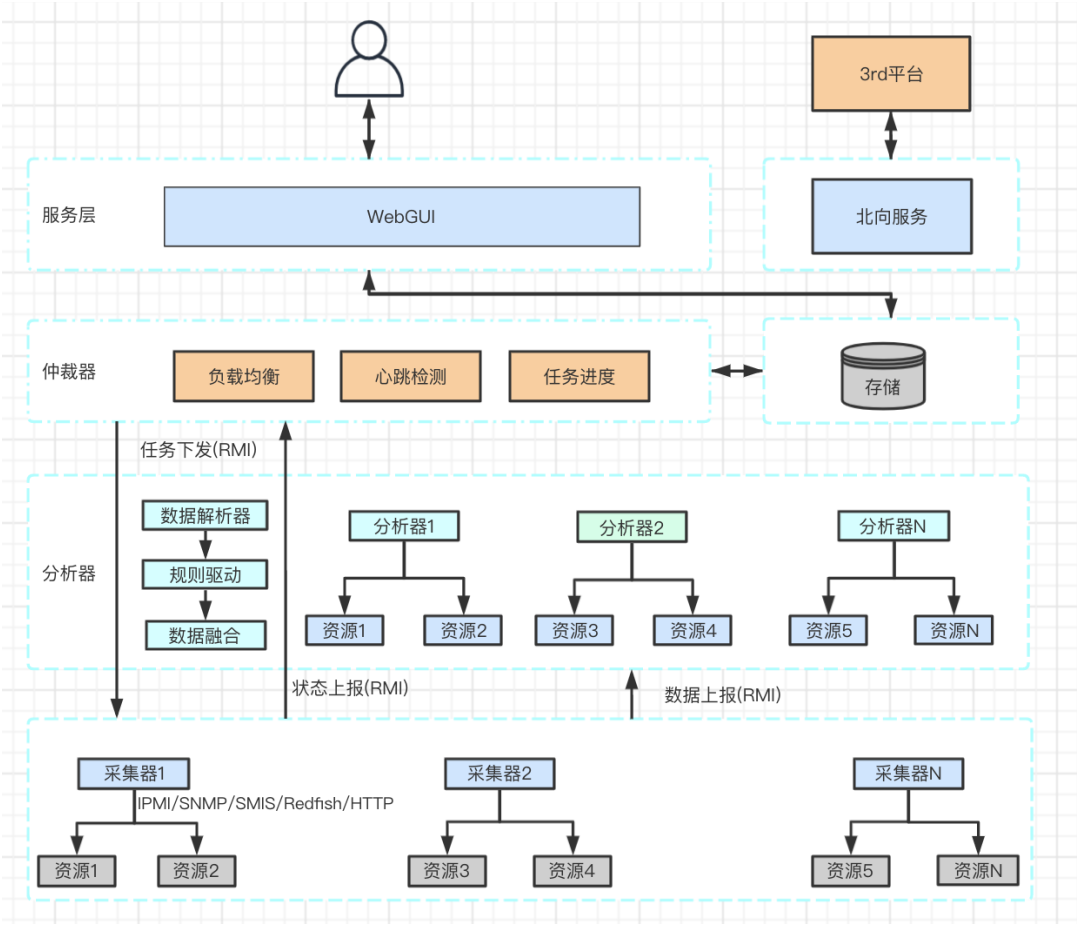
- 浪潮全系列产品，包括通用机架服务器、AI 服务器、刀片服务器、边缘设备、一体机及其它高端服务器产品，详细型号请参见《ISPIM 规格清单》。
- 支持存储、网络设备、安全设备等多种异构设备混合管理。

高可用、高扩展能力

- 主控节点 HA 主/备高可用。
- 分布式架构，提供水平在线扩展能力。

- “探针式”采集，多数据中心统一管理。
- 管理规模从百台、千台、万台灵活支持。

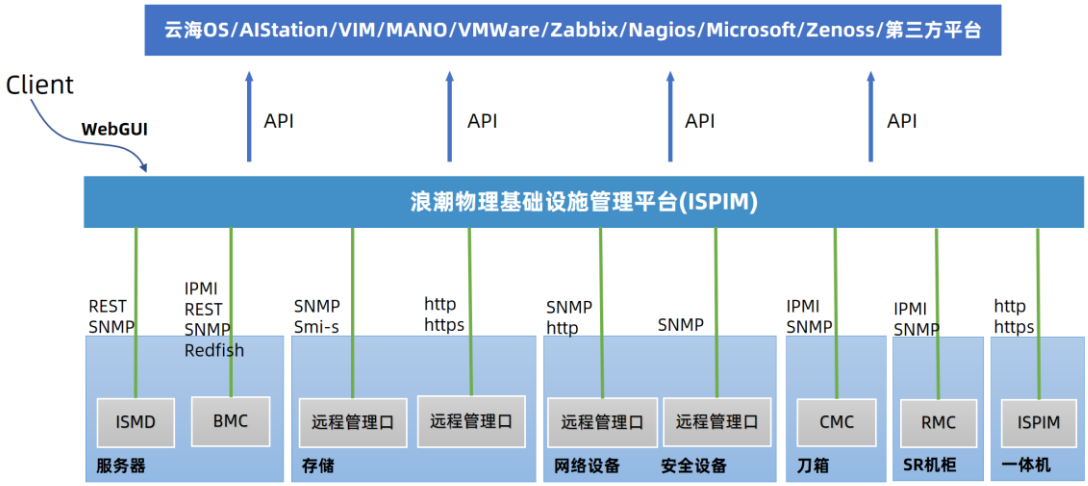
图 3-2 ISPIM 技术架构



3.2 上下文对接方式

- 服务器南向对接 BMC 与 Teye，接口为 IPMI、SNMP、Redfish 等。
- 存储南向对接管理 Controller，接口为 SNMP、SMI-S。
- 网络设备、安全设备南向对接远程管理口，接口为 SNMP。
- 北向接口对接上一级管理软件、第三方管理系统。
- 提供 WebGUI，面向运维管理员。

图 3-3 ISPIM 上下文对接图



4 功能特性

ISPIM(InspurPhysical Infrastructure Manager) 是面向互联网、金融、通信等行业数据中心的一体化基础设施管理平台（DCIM），实现云边数据中心服务器、存储、网络设备等物理设备的统一智能化管理。

图 4-1 ISPIM 功能特性

4.1 快速灵活的纳管方式

ISPIM 支持批量导入、自动发现等多种纳管方式，可以满足多种业务需要。

- 批量导入方式：适用于设备已配置管理 IP，且认证信息已知的情况下的精准纳管，一次支持导入 1000+台设备。

自动发现方式：强大的跨网段、跨域设备发现功能，实现多个数据中心设备的自动纳管。

4.1.1 全网设备纳管

ISPIM 支持物理设备资源的集中管理，支持批量导入、自动发现两种纳管方式。

纳管范围包括：服务器（浪潮、华为、中兴、惠普、戴尔、H3C、曙光等）、存储、网络设备、SR 机柜、一体机、安全设备等，详情请参见《ISPIM 规格清单》。

4.1.2 SR 机柜纳管

ISPIM 支持对 SR 整机柜的集中管理，节点管理协议支持 IPMI、SNMP、Redfish、RMC，SSH 管理协议支持 IPMI、CLI、SNMP。

4.1.3 一体机纳管

ISPIM 支持对浪潮一体机纳管，发现协议支持 http 和 https，实现对一体机内部服务器、交换机、存储设备的统一管理，同时支持对一体机环境温湿度、烟感等传感器的检测。纳管一体机前，用户需要预先在一体机“平板盒子”部署 ISPIM-XX - SR-A1 管理平台。

4.1.4 刀箱纳管

ISPIM 支持浪潮多节点服务器的统一纳管，包括高密均衡型、高密计算型、高密模块化、四子星等多种类型的刀箱及刀片多节点服务器的统一监控、管理；

4.1.5 边缘盒子纳管

ISPIM 采用 http 协议集中管理浪潮边缘盒子。在纳管边缘盒子前，用户需要先在边缘设备上部署好边缘管理系统，设定好边缘系统 IP 及用户名和密码，通过人工或者自动的方式在 ISPIM 端进行扫描，实现对边缘盒子的纳管。

4.1.6 网络设备纳管

ISPIM 支持交换机、路由器、SDN 等设备的管理，通过 SNMP 协议纳管交换机、路由器设备，通过 http 协议纳管 SDN 设备，具体支持型号详细列表请参见《ISPIM 规格清单》。

4.1.7 安全设备纳管

ISPIM 支持通过 SNMP 协议，管理防火墙、IDS、IPS、负载均衡器等设备，具体支持型号详细列表请参见《ISPIM 规格清单》。

4.1.8 存储纳管

ISPIM 支持浪潮的通用磁阵产品、分布式存储及第三方厂商存储设备集中管理，支持的管理协议为： SNMP 协议、SMI-S 协议、RESTful 协议，具体支持型号详细列表请参见《ISPIM 规格清单》。

4.2 智能资产管理

- ISPIM 支持浪潮服务器部件级的资产管理，资产数据更加丰富；支持第三方设备的资产管理。

- ISPIM 通过机柜 RMC，能够自动获取机柜设备的物理位置与资产信息。

4.2.1 用户场景问题

随着 IT 设备需求的增长，数据中心设备规模越来越大。面对数据中心大量的资产，传统 IT 资产管理系统不仅耗时耗力，而且变更流程长、效率低下。

传统资产管理的典型的问题如下：

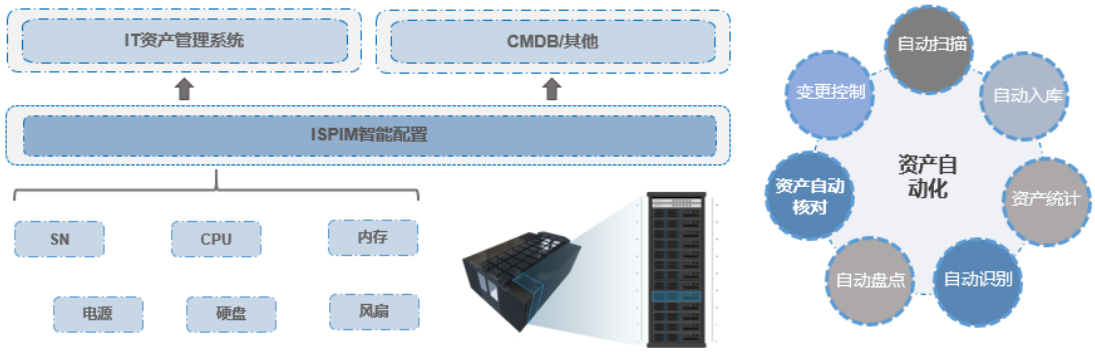
- 人工维护效率低下：设备入库和上线操作需要手动录入，效率低下。
- 设备规格查验困难：对于最新采购的设备，无法确定是否与订单规格一致。
- 设备变更风险：设备变更需要人工管理，无法自动跟踪。一旦人工操作出现偏差，无法立刻发现，存在遗失风险。
- 安全风险：设备的关键部件可能被人为更换，数据存在恶意获取或者破坏风险。
- 数据中心规划困难：对数据中心的空间缺乏直观的呈现，新增设备难以规划空间。
- 资产盘点困难：每次资产盘点都需要花费大量的人力和时间，效率低下。

以上是 IT 资产管理中的常见问题，解决这些问题的关键点在于实现资产与 CMDB 系统的自动同步，避免人工干预。

4.2.2 方案介绍

ISPIM 实现了全自动的资产端到端管理，从设备上线、位置识别、配置核查、资产位置变更、部件变更、机柜空间管理，到跟客户 CMDB 系统的整合，都提供了完善的解决方案。

图 4-2 资产管理解决方案



ISPIM 配合 SR 智能机柜 RMC、刀箱 CMC 实现了设备自动发现和位置识别。

- 机柜 RMC 或 CMC 系统通过内部直连获取节点 U 位信息，节点 SN、型号、MAC 地址、IP 地址、CPU、内存信息。
- RMC 作为机柜的智能控制系统，提供基于工业标准的 Redfish 管理协议，实时监控机柜设备的变更，采用订阅的方式将所有的资产和位置信息通过 Redfish 标准接口同步到 ISPIM。RMC 系统记录了机柜的物理位置信息，ISPIM 也可通过 RMC 采用主动抓取方式获取节点资产信息。
- ISPIM 通过服务器的 BMC，能够主动监控部件的变化，从而实现了部件级的资产管理。典型场景包括：硬盘和内存的插拔与更换事件。
- ISPIM 支持北向的 Redfish 管理接口，可以对接第三方的 CMDB。ISPIM 支持主动上报变更事件，实现实时的资产变化跟踪。

4.2.3 特性介绍

ISPIM 部件级的资产管理，可实现资产管理自动化与可视化，管理效率大幅提升。特性包括：

- 资产自动扫描、秒级盘点，资产信息全景多维度展示。
- 部件级资产管理，数据中心资产组件信息一目了然，支持报表导出；支持实时追踪资产变更，可查可控；支持资产利用效率分析，提升资产利用率。
- 数据中心 3D 可视化管理，多维度呈现数据中心资产分布、温度、能耗、警信息。机柜位置、设备槽位、部件状态信息一目了然。
- ISPIM 提供 REST 接口，支持与第三方 CMDB 系统对接，便于资产管理系统集成。

1. 资产全景统计

ISPIM 支持按数据中心维度的资产全景统计，包括：

- 服务器、存储、网络、刀箱、机柜等设备的统计。
- 数据中心资产总数和空间使用率。

2. 资产明细展示

ISPIM 支持以设备和部件维度展示详细的统计信息，包括：

- 按照服务器、存储、网络、刀箱、机柜、防火墙维度分类展示设备的不同型号统

计。

- 展示设备名称、序列号、IP、位置、厂商、型号、占用空间、上架时间。
- 展示服务器设备的硬盘、内存、CPU、主板等部件数量统计。
- 展示详细部件的名称、类型、厂商、型号、序列号等信息。

3. 服务器全生命周期管理

ISPIM 对数据中心 IT 基础设施进行监测、管理运营，记录了服务器上架至下架整个生命周期的设备和部件的详细变更事件，包含：设备上架、下架、部件增加、部件删除、部件状态变化、固件版本更新等，变更事件记录了变更时间、变更类型、设备型号、序列号、资产类型、位置及详细的资产变更描述。

ISPIM 为设备提供全生命周期管理，包括：

- **提供设备每个阶段的变化趋势**，发现设备和部件存在的潜在风险。同时支持以文件的形式存储变更信息，为服务器部件故障分析提供有效数据源。
- 提供按照数据中心分类展示变更、详细的变更事件信息。
- **提供有效、准确、及时的“部件级”IT 资产信息**。系统支持自动采集设备的硬件配置信息，可有效解决人工录入信息准确性较低的问题。资产数据定时自动更新，解决了资产信息不能及时同步的问题。自动采集的“部件级”资产数据，实现了设备“配置”变更记录，确保每一次变更自动记录系统中，且记录不可修改、删除，实现资产变更的可审计、可追踪。

4. 服务器密码托管

服务器密码托管是 ISPIM 对服务器 IPMI 远程管理账户提供的一项重要功能，可帮助用户安全、轻松地访问具有合规资质的服务器硬件资源。

待托管的服务器通过 ISPIM 双层加密运算，可安全生成硬件设备密钥。通过将密钥托管在高安全等级的系统中，可以保护用户在 ISPIM 上敏感的计算任务和资产数据，让运维管理人员更加聚焦运维。

5. 机柜视图

ISPIM 对机柜展示的内容包括：

- 机柜基本信息：包括机柜位置、编号、尺寸、高度。
- 资产管理 RMC 的基本 IP、型号和版本信息。

- 机柜 2D 视图：支持展示设备的详细信息，包括型号尺寸、高度、自身告警、节点告警。
- 机柜设备列表：包含设备名称、类型、型号、厂商、U 位、序列号、告警状态。
- 通过机柜视图，客户可直观查看机柜布局、功耗及气流分布，便于用户直观了解机柜的空间、节点健康状态等信息，从而进一步规划机柜的使用。

6. 对接第三方 CMDB

ISPIM 提供了完善的资产信息展示与资产可视化操作界面，同时支持通过 RESTful 接口或插件方式对接第三方 CMDB 系统。其中，采用插件方式时，第三方系统无需进行任何开发与配置， ISPIM 插件框架会加载第三方系统定制的插件进行资产信息自动同步，并具备定时同步资产信息的功能，便于与客户的资产管理系统对接。当前版本内置 ISIB 资产对接插件，直接同步 ISIB 资产信息。

4.3 设备全方位监控

ISPIM 通过多种标准管理协议，以主被动结合的方式，提供设备全天候实时监控与故障分析，减少业务隐患。特性包括：

- 全天候主动巡检+被动接收。实时发现告警。

- 主动轮询支持数据采集频率设置与采集项的自定义，结合用户实际关注点，进行实时精准采集，提升监控效率。
- 被动接收支持 Trap OID 集中管理，接收解析设置及南向转发。确保设备的告警推送能够被准确解析，没有遗漏。

- 支持万余设备带内秒级性能监控。

- ISPIM 可搭配浪潮管理驱动软件 ISMD，实现对设备带内性能指标的秒级采集及历史汇聚。
- 支持采集器、分析器与存储数据库的水平扩容与负载均衡，保障万余设备的稳定监控。

- 带内+带外部件状态、性能指标、维保、网络状态等全方位监控。

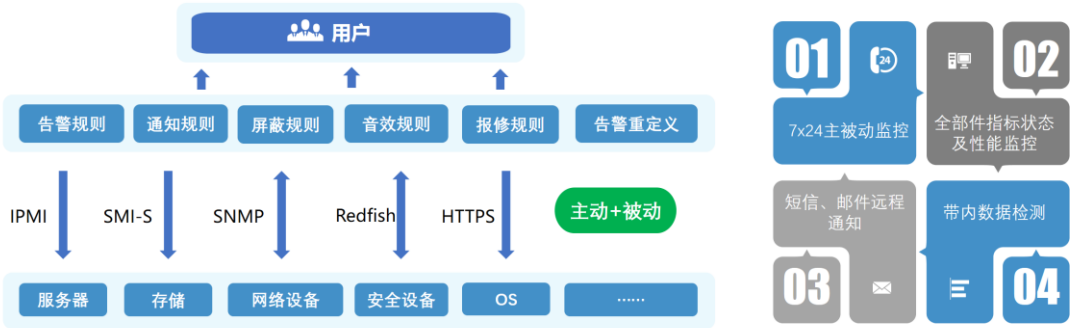
- 带外监控的同时，提供可选的带内浪潮管理驱动软件 ISMD，实现对设备性能数据的采集。实现更全面的设备信息采集与监控。
- 支持维保到期告警，满足维保需求。

- 告警规则、屏蔽规则、报修规则、通知内容模板、告警音效规则、重定义规则、通知规则等模板灵活定义告警。

- 支持数据采集项与告警阈值的自定义。
- 支持屏蔽规则的一键创建。规则涵盖屏蔽源，按告警位置屏蔽，按具体告警屏蔽等多种自定义规则，实现屏蔽粒度的自定义。
- 支持通知规则的自定义。内容涵盖：通知时间、通知方式、告警类型、系人。支持通知内容格式的自定义。
- 支持告警名称及告警级别的重定义。内容涵盖：所有告警类型的名称自定义及针对特定资源的告警级别自定义。
- 支持自定义自动报修相关规则。包括：报修告警类型设置、驻场联系人信息设置、报修客户相关信息设置。
- 支持自定义邮件及短信通知内容模板。包括：告警名称、告警位置、告警描述、告警级别、告警类型、清除方式、资产名称、资产序列号、可能原因、修复建议、首次发生时间、最后发生时间、恢复时间、资源归属、业务归属、资产 IP、资产位置、资产机型、资产厂商、部件名称、部件序列号等。

- 邮件、短信、第三方平台等多方式告警提醒。

图 4-3 ISPIM 全方位设备监控



4.3.1 设备信息及告警多维度呈现

ISPIM 将数据中心管理的设备按照不同视图的方式呈现监控信息，更准确快捷地找到客户关注的内容。

- 数据中心 3D 视图展示：支持按照数据中心、机房、机柜维度查看资源的监控及

状态信息。

- 硬件设备信息展示：支持按照设备所属类型进行查看。
- 告警信息统计：支持不同维度的告警信息展示。

表 4-1 多维度告警呈现

维度	描述
服务器告警统计	按照不同的告警级别，呈现服务器告警的数量分布
告警分类统计	按照不同的告警类型，呈现设备告警的数量分布
部件告警数量统计	显示所有资产部件的告警数量分布
设备类别告警数量统计	按照不同的设备类别，呈现告警的数量分布及级别比例

1. 设备信息展示

ISPIM 支持对已纳管的服务器设备部件信息进行 360 度呈现和管理：

- 统一 Portal

- 提供视图的定制功能，根据用户角色自定义视图，展现关键设备告警、资源状态统计等信息。
- 支持首页定制化、实时呈现最新的业务状态，帮助用户快速锁定关键业务指标。

- 可视化大屏：支持屏幕分辨率定制，适应各种大屏幕监控需求。
- 服务器部件信息

- 电源信息：名称、状态、槽位、型号、模式等。
- 风扇信息：名称、状态、槽位、转速百分比、模式、转速、槽位等。
- 处理器信息：名称、厂商、型号、主频、槽位、核数/线程数、一级缓存、二级缓存、三级缓存等。
- 内存信息：名称、厂商、容量、序列号、类型、状态和频率、槽位等。
- 物理磁盘：名称、设备 ID、槽位、容量、接口类型、固件状态等。

- 逻辑磁盘：设备 ID、名称、容量、状态等。
- 网络信息：其中 BMC 适配器（名称、MAC 地址、IP 等信息）；系统网络适配器（在位状态、位置、厂商、型号、端口、端口状态、端口 MAC 地址等信息）。
- RAID 卡：名称、序列号、资源归属、固件版本、状态、型号、厂商 ID 等。
- 逻辑磁盘：名称、状态、容量。
- PCIE 卡：名称、状态、厂商、槽位、描述等。

● 交换机部件信息

- 单板：端口、风扇、电源等。
- 端口：名称、描述、速率、类型、状态、所连设备 IP、VLAN、绑定的 MAC、所连设备 MAC、对端端口唯一标识等。
- 风扇：名称、状态等。
- 电源：名称、型号、模式、状态等。

● 存储部件信息

- BBU：名称、状态等。
- 控制器：名称、容量、状态等。
- 风扇：名称、状态等。
- ISCSI：名称、ID、索引、速率、状态、IP、MAC、子网掩码等。
- LUN：名称、WWN、LUN ID、块大小、块数量、未使用的快数、总容量、未用容量、状态等。
- 电源：名称、状态等。
- RAID：名称、池 ID、总容量、已用容量、未用容量、状态等
- 磁盘：ID、名称、型号、厂商、微码版本、容量、状态、块大小、块数量、类型、槽位等。
- FC：端口索引、端口 ID、端口速率、端口类型、状态等。

● 分布式存储信息

- 集群信息：名称、型号、厂商、软件版本、资源重构间隔、卷清理间隔、自动精简配置、运行状态、集群流控模式、NTP 服务器、LICENSE、总容量、已用容量。

- 存储池信息：名称、数据策略、安全策略、运行状态、总容量、已用容量。
- 卷信息：名称、卷容量、QOS 列表、状态、创建时间。
- 快照信息：名称、脏数据容量、创建时间。
- 节点信息：名称、管理 IP、序列号、系统类型、RAID 固件版本、资产名称、状态、网口信息、CPU、内存容量。

2. 设备分组管理

ISPIM 支持对已纳管的服务器进行分组管理，方便运维人员根据实际的业务场景对设备进行分组。分组提供了用户所关注设备信息及告警信息查看的快速入口。

- 手动分组：支持用户创建分组，并手动添加设备到分组。
- 自动分组：支持用户创建条件分组，设备被纳管后自动添加设备到分组。

3. 设备信息报表

ISPIM 提供报表功能，可以将关心的设备信息导出，支持 Excel 格式。

表 4-2 设备信息报表

类别	描述
资产	支持以机房、厂商、型号、部件四种维度生成资产信息报表。
告警	内容包括告警级别分布统计，告警级别百分比统计，实时告警与历史告警详细条目。支持自定义查询，以导出筛选后的告警条目。
维保	设备维保信息报表，涵盖采购时间，过保时间，剩余天数等信息。
性能	支持以资产、指标项、开始时间、结束时间四个维度生成资产性能信息报表，并支持导出性能信息报表。
硬件	支持导出机架、刀箱或 SR 整机柜设备的硬件资产指标信息。

4. 设备信息搜索

ISPIM 提供快速检索设备信息的功能，方便在海量数据中找到特定的设备，支持按照设备名称、IP 地址、厂商、型号、设备状态、资产状态、维保状态等条件搜索。

4.3.2 设备告警管理

ISPIM 支持设备告警的多维度展示（数据中心/机房/机柜设备统计、告警集中展示，单台设备告警详细展示），支持告警搜索、屏蔽、重定义、通知和转储功能，方便运维人员根据自身需要从不同维度进行告警管理。

表 4-3 告警管理功能

功能类型	描述
主动告警	ISPIM 内置主动监控轮询功能，同时用户可自定义设置设备的告警规则和通知规则。从而保障系统对设备的实时监控管理。
被动告警	ISPIM 提供被动接收不同厂商、不同类型设备告警并对其解析的能力，实现设备故障预警。
告警屏蔽	用户可以通过创建告警屏蔽规则，对某些不重要的告警进行屏蔽，避免冗余信息。
告警显示	通过告警面板、告警列表，按照告警级别或者设备分类展示告警信息，实时掌握全网设备的运行状况。同时提供数据中心、机房、机柜与单设备多维度的告警信息统计与分类功能，方便运维人员从多种维度进行告警管理。
告警搜索	用户可以根据告警名称、告警源、IP、级别、告警状态、逻辑分组、告警清除方式等对当前和历史告警进行组合过滤搜索，快速锁定告警。
告警通知	ISPIM 提供邮件和短信，可自定义通知模板个性化通知内容。通过邮件和短信可以实时将告警信息按照客户制定的规则通知到运维人员。
告警重定义	支持各类告警与事件的灵活转换。
南向设置	支持 OID 导入，南向 trap 解析配置。
告警转储	ISPIM 提供自动历史告警转储及转储数据检索的功能，客户无需关

功能类型	描述
	注大量的历史冗余信息。
告警音效	支持按照告警级别设定是否开启告警提示音。
告警转发	ISPIM 支持通过 SNMP Trap 的方式将告警转发至第三方网管系统。

4.3.3 设备性能监控

性能监控是将设备的 CPU、GPU、硬盘、风扇、内存、电源、网卡等关键部件的性能数据进行统计分析，并以趋势图的形式展现，方便运维人员对设备性能进行监控管理。

表 4-4 性能统计类型

统计类型	描述
CPU 统计	CPU 利用率、空闲时间百分比、用户态占用时长百分比、系统态占用时长百分比、IO 等待占用时长百分比、CPU 温度统计
GPU 统计	GPU 利用率、显存利用率、显存容量、已用显存大小、显存剩余空间大小、显存时钟频率、核心时钟频率、GPU 功耗、GPU 温度、 GPU 风扇转速
硬盘统计	硬盘利用率、读写速率、读写次数、IOPS、剩余寿命、温度统计
内存统计	内存利用率、内存大小、已用内存大小、缓冲区内存大小、缓存使用内存空间大小、交换分区使用空间大小统计
电源统计	当前功率、总功率
风扇统计	风扇读数、风扇转速百分比
网络统计	发送速率、接收速率、发送包数、接收包数
NFS 统计	客户端读写速率、服务端读写速率

统计类型	描述
系统负载	一分钟、五分钟及十五分钟系统负载
微架构	单精度浮点运算总和、双精度浮点运算总和、x87 指令集双精度浮点运算、单精度浮点运算、双精度浮点运算、CPI、总内存带宽、内存读写带宽、PCIe 设备读写速率
其他统计	电压、电流、温度

4.3.4 设备故障诊断

ISPIM 能够基于告警引擎、日志等分析结果自动触发对浪潮服务器的故障诊断。故障诊断是指 ISPIM 通过带外方式收集服务器日志（可选的通过带内浪潮管理驱动软件 ISMD 收集带内系统日志、存储等类型日志），并对日志进行智能分析，以判断服务器是否存在故障隐患。

对于采集到的设备日志，ISPIM 通过内置的故障诊断流程检测及智能故障库进行精准的分析，形成设备告警并给出用户建议方案，同时支持自动报修。

图 4-4 ISPIM 故障诊断

当 ISPIM 监控到设备告警时，能够自动触发故障诊断。ISPIM 内置的浪潮专家智能故障诊断系统，包含全面的故障诊断模型与规则，涵盖的范围包括：

- 产品典型故障，典型案例。
- 历史故障解决建议。
- 客服技术专家分析经验。
- 研发、测试技术专家解决方案。
- 为故障分析提供强大的数据支持，并给出故障维修建议。

- 故障库会随着 ISPIM 版本持续更新。

4.3.5 智能告警对接

ISPIM 支持通过 SMTP、SMPP、CMPP、SMGP、SGIP、短信猫或 HTTP/HTTPS 协议的方式，将自身告警及纳管设备的告警，按照可定制化格式实时发送给用户。

表 4-5 告警对接

功能类	描述
短消息服务器	提供运营商短消息服务器的配置方式。
邮件服务器	提供对接的 SMTP 服务器配置功能，可配置项包括：邮件服务器地址、端口、认证方式、启用开关等。
短信猫服务器	支持配置短信猫的网络制式、串口名称、波特率、号码、开关等。
短信网关服务器	提供短信网关服务的通用配置及定制化属性配置。
通知内容模板	提供自定义的通知模板，方便用户对接。

4.4 智能的能耗管理

ISPIM 能够基于数据中心所有设备的能耗、温度、气流、CUPS 等数据，通过 AI 算法进行数据的过滤、聚合与分析，提供智能的功耗管理与优化建议。内容包括：

- 数据中心多维度功耗统计：以数据中心、机房、机柜、设备维度，对资源的进风口/出风口温度、功耗、气流、CUPS 利用率进行统计。
- 灵活服务器功耗策略：服务器是数据中心功耗的最小维度，ISPIM 支持浪潮服务器的功耗策略设置，包括最低功耗策略，动态功耗策略，支持策略生效时间的灵活定义。

- 能耗优化：支持多种智能功耗优化功能。

- 制冷分析：展示机房维度的设备温度分布曲线图，以三种标准制冷规范为依据，对机房制冷提供评估建议。
- 服务器使用率分析：基于 Intel 标准的服务器使用率评估算法，检查数据中心是否存在使用率较低的服务器，通过整合低使用率的服务器的工作负载，进一步对能耗进行优化。
- 服务器功耗特征：在设备型号维度，呈现设备的功耗上限与下限分布区间，为用户提供依据，以检查是否能够升级或淘汰某些服务器以提高数据中心的能效。
- 能耗优化：根据服务器的 CUPS 数据，智能分析其对指定负载的承载能力，以帮助用户进行负载的分配与迁移。
- 高级功耗模型：通过服务器历史 CUPS 数据与功耗曲线，生成智能功耗模型，用户可根据模型预测服务器在指定利用率下的功耗。

4.4.1 用户场景问题

每个数据中心可提供的总功率是一定的，当机房设备较多、功率较大，设备所需总功率超过机房供电上限时，可能会导致部分设备随机断电或由于功率不足而出现性能降低等问题。

在数据中心运维过程中，客户常见的功耗管理的场景与诉求如下：

- 查看数据中心/机房/机柜的整体能耗 。
- 发现机房高温设备，优化制冷方案。
- 发现僵尸服务器，优化、调整业务。
- 预测服务器运行功耗。
- 限制异常高功耗设备。
- 评估服务器业务上线、业务迁移的承载能力。
- 分析设备使用率，优化系统部署方式，提高服务器使用率。

4.4.2 功耗性能历史曲线

ISPIM 建立数据中心、机房、机柜到设备的树状列表，用户可以在每一层级查看功耗性能数据，包括温度、功耗、气流和 CUPS 等数据。数据以图表形式展示，提供

近一小时、近一天、近一周直至近一年等时间范围展示功耗性能数据变化信息。

表 4-6 功耗资源维度

资源	温度	气流	功耗	计算利用率
数据中心	是	是	是	否
机房	是	是	是	否
机柜	是	是	是	否
设备	是	是	是	是

4.4.3 功耗策略

1. 功能介绍

ISPIM 允许用户针对单台设备制定相应的功耗限制策略，以限制服务器的最大功耗。策略的内容包括：

- 是否启用：建立策略后，可以随时单独关停或启用某条策略
- 时间周期：策略启用后，会在设定的时间周期内生效
- 功耗上限：策略的主要作用是通过降低 CPU 频率等手段限制设备的功耗，当策略启用并生效时，设备的功耗会被限制在设定的功耗上限附近。

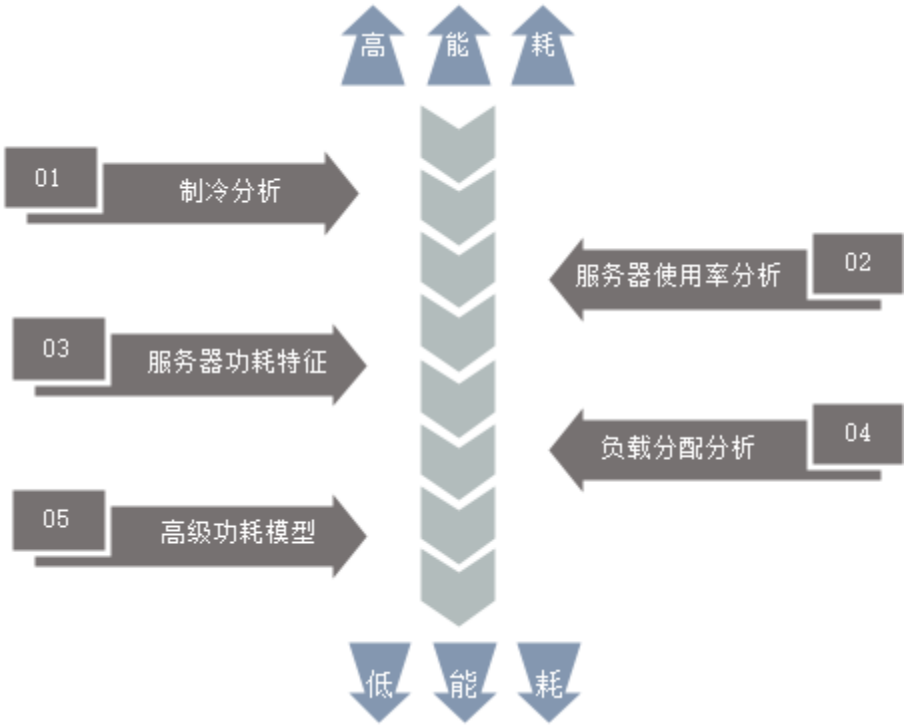
2. 兼容机型

ISPIM 的功耗策略功能当前兼容的机型包括：浪潮 M4、M5、M6 系列服务器。

4.4.4 能耗优化

ISPIM 通过五大功能辅助运维人员全面降低机房能耗。

图 4-5 ISPIM 能耗优化功能



1. 制冷分析

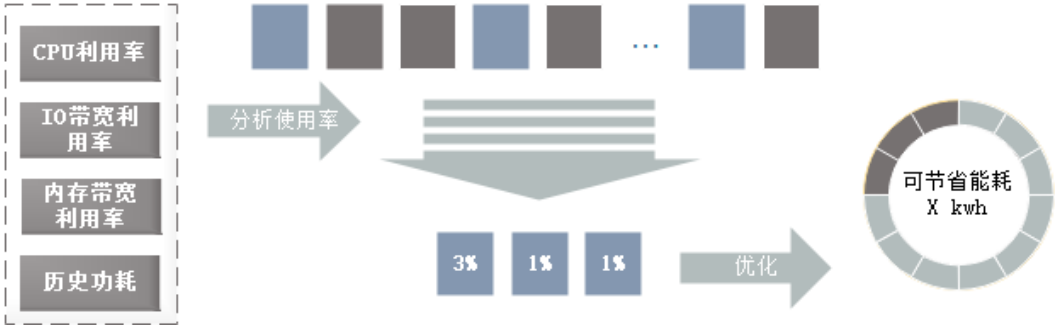
制冷分析是对机房内的设备入风口温度进行分析，展示机房内的温度分布情况，列出机房内的高温热点并给出合理制冷建议。用户可以根据使用场景，在三种不同的规范中选择其中一个，包括：

- ASHRAE 推荐温度 18℃-27℃。
- ASHRAE 一级许可温度 15℃-32℃。
- ASHRAE 二级许可温度 10℃-35℃。

2. 服务器使用率分析

服务器使用率分析是采用功耗数据或者 CUPS 对服务器的使用率进行评估，发现使用较低的僵尸设备，展示平均使用率和 99%的时间使用率，并预测优化节省能耗；使用 AI 算法，分析服务器使用规律，总结设备日使用率分布情况。

图 4-6 服务器使用率分析



3. 服务器功耗特征

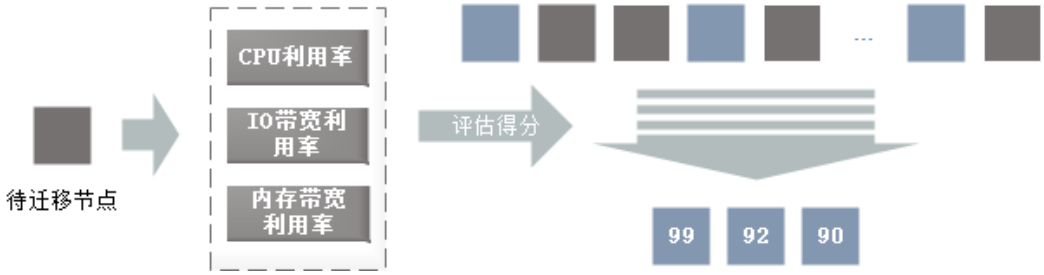
功耗特征是根据功耗进行分析，展示每种型号服务器在托管时间里的功耗上限和下限，并统计每种型号服务器功耗上限和下限的分布情况。通过该方式，展示每种型号服务器的功耗波动范围，可以及时发现高功耗设备型号。

4. 负载分配分析

ISPIM 提供方便易用的负载分配和负载迁移方法。

- 负载分配：根据用户所需的计算利用率（CPU、IO 和内存的带宽利用率），对服务器的承载能力进行评估，列出服务器承载能力评分。
- 负载迁移：根据用户选择的所需迁出负载的设备，对其他服务器进行承载能力评估，列出服务器承载能力评分。

图 4-7 负载分配&迁移



5. 高级功耗模型

高级功耗模型是根据设备资源的使用情况通过 AI 算法对设备功耗进行分析，建立高级功耗模型。模型支持从三个维度（CPU 利用率、IO 带宽利用率和内存带宽利用率）进行设备功耗的预测。

图 4-8 功耗模型

4.5 高效的无状态管理

ISPIM 基于服务器 BMC 带外管理接口实现了 BIOS 和 BMC 配置与升级、操作系统部署、带内运维软件安装、网卡、RAID 卡、HBA 卡固件升级等功能。同时，支持固件配置文件的导入和导出，在 M6 机型还支持了快照的管理。实现了设备的无状态管理。

ISPIM 提供的不间断监控能够实时侦测设备的状态变更，提供告警与自动还原功能，保证设备的合规性。

图 4-9 设备无状态管理

4.5.1 标准化的基线管理

ISPIM 提供标准的统一基线管理，包含基线模板和基线策略两大功能。

- 通过基线模板，用户可将具体型号的浪潮服务器的最优固件版本设置成基线模板，基线模板中设置了服务器最合理的固件搭配。
- 通过基线策略，用户可以对偏离基线模板的设备进行处理，例如：是否按照基线模板进行固件更新，是否产生偏离基线的告警。基线管理模块会定时采集机型的固件版本、与基线模板进行匹配，对于偏离基线的设备进行自动化的基线校准，为设备的稳定运行提供保障。

1. 用户场景问题

不同型号的设备都有满足用户业务需求的最优固件版本，设备在运行过程中存在主板更换及新上架服务器，导致固件版本与最优固件版本不一致的问题。基线管理模块提供完整的解决方案，实现了自动化基线对比、基线告警与自动较准。

2. 基线模板

基线模板提供浪潮服务器固件版本基线的设置功能，用户可以将具体型号的浪潮服务器最优固件版本设置成模板，模板信息主要包括机型、固件版本、刷新策略。基线模板是服务器设置基线标准，为自动化矫正提供基础。

3. 基线策略

基线策略设置能够针对于偏离基线的设备进行处理，例如是否按照基线模板进行固件更新，是否对偏离基线的设备产生相应的告警。基线策略包括：固件变更策略、告警产生策略。

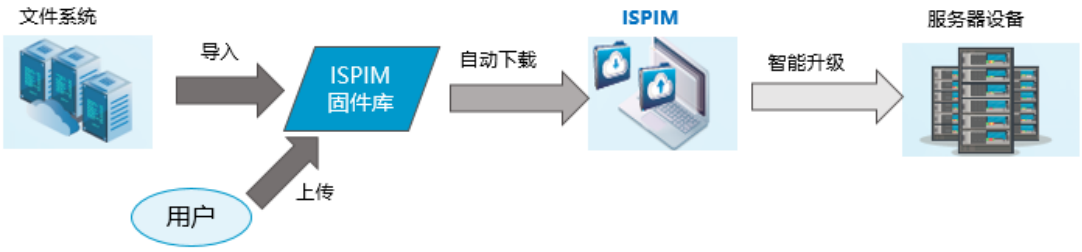
4.5.2 高效快捷的固件管理

1. 固件升级

ISPIM 实现了浪潮机架、机柜服务器生命周期内全固件升级管理。用户可以选择连接官方镜像库，通过机器序列号自动同步服务器固件，或者手动上传固件至本地镜像库（手动上传的固件需要用户预先从浪潮服务器固件管理系统或官网下载）。

固件升级主要提供带内带外两种方式，带外可以通过 RESTFUL 接口实现 BIOS 和 BMC 固件升级，带内可以结合 BMC、内存 OS 完成 BIOS、BMC、网卡、RAID 卡、HBA 卡、硬盘的固件刷新。针对 M5、M6 系列服务器的 BMC 升级，支持升级和生效分离，保证升级流程对客户业务系统无影响。

图 4-10 升级流程



1. 用户场景问题

①场景一、多节点（仅固件）远程更新，实现方案 ISPIM

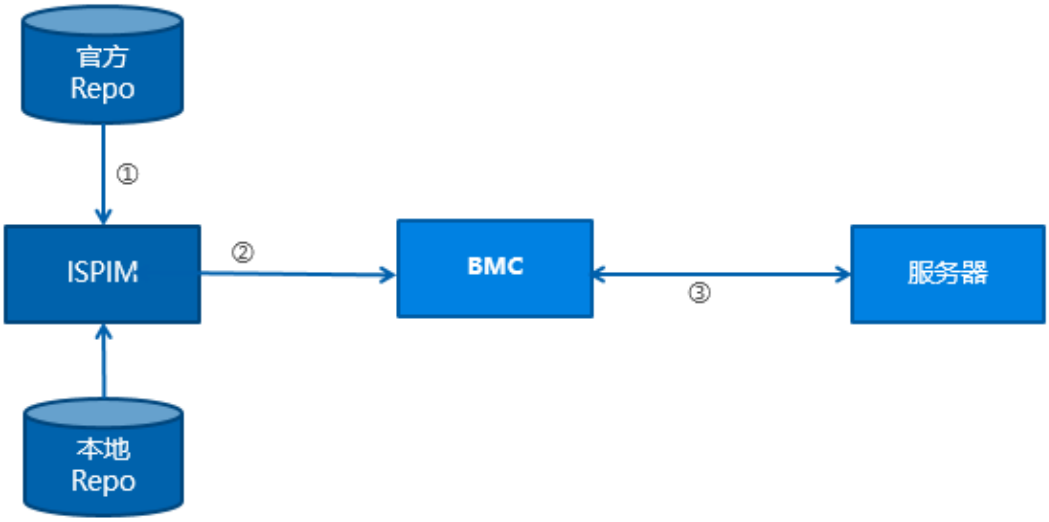
- 数据中心创建，大批量服务器需要上架，需要进行 BIOS 和 BMC 升级。
- 设备运行一段时间，固件版本问题需要修复，需要进行固件升级。
- 机器较多，固件版本较多，人工升级容易造成失误。
- 大批量的固件升级，如果采用人工作业方式，效率很低。

②场景二、多节点（含板卡）远程更新，实现方案 ISPIM+BMC+内存 OS

- 数据中心创建，大批量服务器需要上架，需要进行 BIOS、BMC、网卡、RAID 卡、HBA 卡、硬盘等部件的固件升级。
- 设备运行一段时间，固件版本问题需要修复，需要进行固件升级。
- 机器较多，固件版本较多，人工升级容易造成失误。
- 大批量的固件升级，如果采用人工作业方式，效率很低。

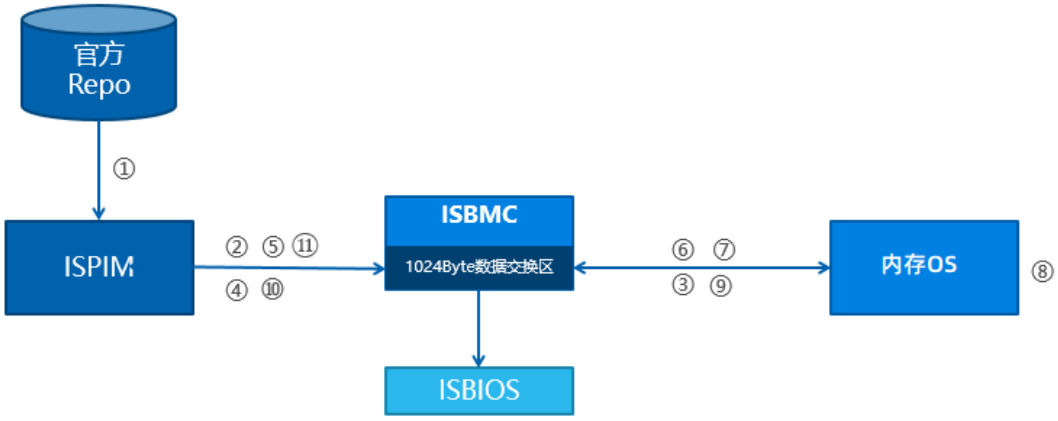
2. 升级流程

- **ISPIM 方式**



用户可以选择从官方镜像库或从本地直接上传镜像文件，ISPIM 通过 BMC 的 RESTFUL 接口，完成 BIOS 和 BMC 固件升级

- **ISPIM+BMC+内存 OS 方式**



用户可以从官方镜像库同步需要升级的固件包，ISPIM 通过指令将需要升级的固件包及内存 OS 通过 BMC 虚拟介质挂载到需要升级的服务器，并通过指令，引导内存 OS 启动，待内存 OS 启动完成后自动完成全固件的刷新。

3. 兼容性列表

表 4-7 固件升级兼容性列表

分类	型号
BIOS/BMC	浪潮 M4、M5、M6 系列服务器，i24、I48 机柜服务器

分类	型号
网卡	1、网卡_BROADCM_25G_57414_LC_PCIEx8_2_XR_OCP 2、网卡_BROADCM_25G_5741_LC_PCIEx8_XR_OCP_BD 3、网卡_BROADCM_25G_57_LC_OCP2x8_2_XR_BD 4、网卡_I_10G_X540-T2_RJ_PCIEx8_2_XR 5、网卡_M_25G_MCX4121A-ACAT_LC_PCIEx8_2_XR 6、网卡_M_25G_MCX4421ACQN_LC_PCIEx8_2_XR_OCP 7、网卡_M_25G_MCX4121ACAT_LC_PCIEx8_2_XR_T 8、网卡_M_25G_MCX4411ACQ_LC_OCP2x8_XR_BD 9、网卡_M_25G_MCX442_LC_PCIEx8_2_XR_OCPali1 10、网卡_M_25G_MCX4121ACA_LC_PCIEx8_2_XR_ali1 11、网卡_M_100G_MCX516C06_LC_PCIEx16_2_XR_ali 12、网卡_I_10G_X540-T2_RJ_PCIEx8_2_XR 13、网卡_Inspur_Fortville_X710_10G_LC_PCIEx8_2
RAID 卡	1、SAS 卡_INSPUR_SAS3008+IR+PCIE3.0 2、SAS 卡_INSPUR_SAS3008+IT+PCIE3.0 3、RAID 卡_L_8R0_9271-8i_1G_MSAS600_PCIE3_V2 4、SAS 卡_L_24R0_9305-24i_HDM12G_PCIE3 5、RAID 卡_L_8R0_9361-8i_1G_HDM12G_PCIE3 6、RAID 卡_L_8R0_9361-8i_2G_HDM12G_PCIE3 7、RAID 卡_L_8R0_9460-8i_2GB_HDM12G_PCIE3 8、RAID 卡_INSPUR_PM8060_2GB_SAS12G_PCIE3.0 9、RAID 卡_INSPUR_SAS3108_4GB_SAS12G_PCIE3
HBA 卡	1、HBA 卡_E_0R1_LPE1250_FC8G_PCIE

分类	型号
	2、HBA 卡_E_0R1_LPE16000B_FC16G_PCIE 3、HCA 卡_M_1-EDR4X25_MCX455A-ECAT_PCIE_QSFP 4、HBA 卡_QL_0R1_QLE2670_FC16G_PCIE 5、HBA 卡_QL_4R1_QLE2690-ISR-BK_FC16G_PCIE
硬盘	1、HXM7904Q_20200711NF

2. 固件配置

ISPIM 根据资产信息会自动生成固件配置模型，用户可根据机型批量选择设备，进行 BMC/BIOS/RAID 选项的自定义配置，实现固件的快速配置，提升服务器运维效率。

3. 设备配置项

对运维场景下常见的配置，基于资产配置，生成配置模板，实现图形化操作，操作简单、便捷。

表 4-8 设备配置项

部件类型	配置类型	描述
BIOS	BIOS 配置	提供对服务器设备 BIOS 的配置功能，主要配置项如下：Boot 配置、系统启动顺序、处理器配置、内存配置、硬盘配置、VMX。
RAID	RAID 配置	通过用户参数需求，自适应选择带外或者挂载 ISO 的方式，提供服务器的 RAID 创建配置功能。
BMC	SNMP 设置	支持 SNMP Trap 告警设置、告警策略设置。
	NTP 设置	提供对服务器 NTP 模式、NTP 服务器地址的配置功能。

部件类型	配置类型	描述
	SMTP 设置	提供对服务器的 SMTP 服务设置功能。
	用户设置	提供对服务器用户名的新增、修改功能。
	服务设置	提供对服务器 KVM/CD-Media/HD-Media/SSH 服务的状态、端口、和超时时间设置功能。
	DNS 设置	提供对服务器的域名、主机、域名服务器配置功能。
	SNMP 请求设置	提供对服务器的 SNMP Get/Set 配置的功能。
	BMC 日志设置	提供对服务器的 BMC 日志启用状态、记录类型、服务器地址、端口、协议类型的配置功能。

表 4-9 RAID 配置兼容性列表

序号	型号
1	9460-8i
2	9271-8i
3	9361-24i
4	9361-8i
5	SAS3108
6	9305-24i
7	PM8060
8	PM8204

4.5.3 简便易用的部署管理

1. 用户场景问题

操作系统部署与配置操作繁琐，人工作业耗时耗力。

- 数据中心业务上线，大批量服务器需要部署操作系统，如何减少人工操作，提升效率。
- PXE 方式 OS 部署，需要配置 DHCP、FTP 服务，还需要划分网络配置，网络配置复杂。
- 设备上线一段时间需要重新部署，PXE 方式会破坏已有网络，如何快速重装系统。

2. 部署管理

ISPIM 的操作系统批量部署功能，相比传统的网络（PXE）OS 部署，不需要配置 DHCP、FTP 服务，不需要进行网络划分与配置等复杂操作，部署过程仅依赖 BMC 带外网络，支持带有自定义 KS 文件的 OS 镜像，支持默认配置修改，支持手动分区，支持系统盘设置，支持 IP 配置，同时支持安装完成时状态的自动获取。

- 部署前，设备需先配置好 RAID，并且需要设置 RAID 启动盘。
- 操作系统部署支持的设备类型为浪潮 M5、M6 系列服务器。

表 4-10 操作系统兼容性列表

镜像类型	镜像版本号
RedHat	Redhat 7.3/7.4/7.5/7.6/7.7/7.8/7.9/8.1/8.2/8.3/8.4
VMware	ESXi 6.7/7.0
CentOS	**CentOS 7.3/7.4/7.5/7.6/7.7/7.8/7.9/8.1/8.2/8.3/8.4**
Ubuntu	**Ubuntu-18.04-Server、Ubuntu_20.04-Server**
UOS	**UOS20**

4.5.4 统一的镜像文件管理

1. 用户场景

在无状态管理中，用户需要面对种类繁多的镜像文件，对于固件升级文件，需要按照镜像类型(BIOS、BMC、网卡、RAID 卡、HBA 卡、硬盘)对固件的版本进行统一的管理。

对于操作系统镜像，需要按照镜像类型，系统类型，操作系统版本，是否包含自定义 KS 文件等多种维度对镜像文件进行管理。

2. 仓库

ISPIM 仓库主要针对于固件升级文件和系统安装 OS 介质进行统一管理。

操作系统镜像仅支持本地文件上传方式，按照系统类型、版本进行分类管理，系统安装 OS 介质包括 ESXI、CentOS、Redhat、Ubuntu、UOS。

固件支持自动同步和手动上传两种方式，其中：

- 自动同步：ISPIM 可以连接官方镜像库网站情况下，支持从官方镜像库自动同步固件。
- 手动管理：ISPIM 无法连接官方镜像库网站情况下，支持从其他可连接官方镜像库网站的设备下载固件，通过 ISPIM 导入固件。

4.5.5 便捷的自动上线规划

1. 传统设备上线流程

传统的设备上线，需要设备上架后才能创建设备上线任务，手动操作较多，效率较低。传统操作步骤如下：

步骤 1 设备安装人员按照手动维护的规划模板，完成设备上架。

步骤 2 运维人员手动连接每台设备完成初始 IP 的配置。

步骤 3 在网管上创建纳管任务，将设备纳管到网管。

步骤 4 人工核查上架的设备是否是客户购买的设备。

步骤 5 在网管平台中创建配置、部署任务。

步骤 6 手动启动相关任务，完成设备的上线。

2. 便捷的自动上线规划

基于 ISPIM 的自动规划上线，用户可根据预先规划的设备 IP 地址、配置文件以及 OS 部署模板等配置信息，设备安装人员按照规划的模型完成设备的上架。设备上架后支持自动配置 IP、自动纳管以及配置部署。

- 创建固件配置文件

  在上线规划策略创建之前，用户需要提前创建固件配置文件。固件配置文件以资产硬件信息为模型，自动生成服务器固件配置模板，根据模板自定义配置项。

- 创建系统安装模板

  在上线规划策略创建之前，用户需要提前创建系统部署模板。在系统部署模板中，指定系统部署的镜像类型及系统安装的各项参数配置。

- 添加规划设备

  为节约设备上线时间，提高设备上线效率，用户需提前规划待上线设备的设备系统名称、IP 地址、子网掩码、网关、用户名以及 BMC 的 IP、网关、子网掩码等信息。ISPIM 支持手动设置或通过模板文件批量导入。

- 执行上线规划

  上线规划支持“立即执行”和“定时执行”，在执行过程中，用户可以实时查看每台设备的详细执行进度和执行过程中的执行日志。

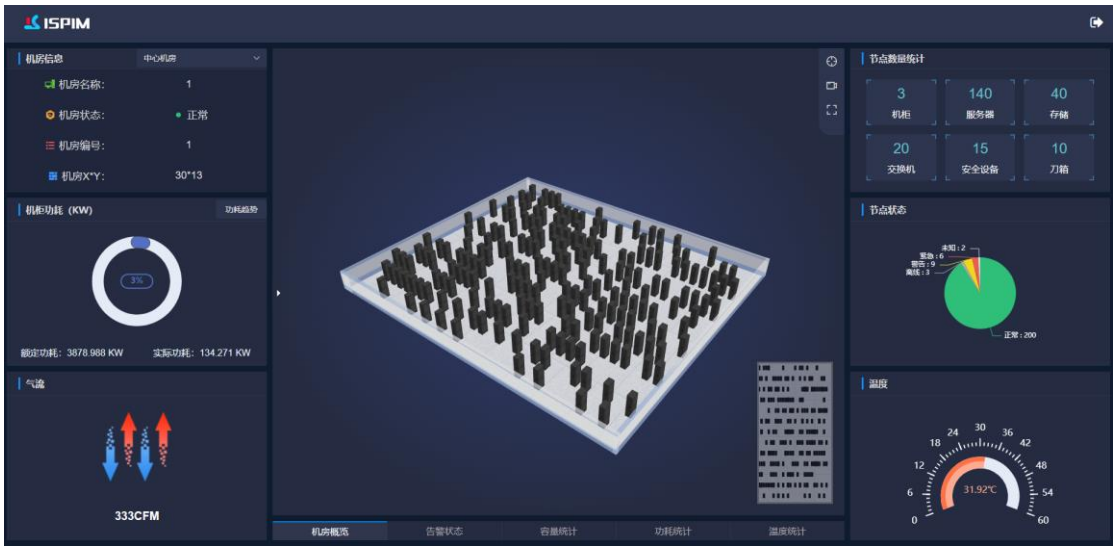
4.6 可视化拓扑管理

4.6.1 3D 拓扑

ISPIM 支持 3D 机房功能，通过三种视图（温度视图、功耗视图、状态视图）展示机房内机柜位置、功耗、温度状态信息，内容包括：

- 机房基本信息：机房内设备数量统计、状态统计和机房温度、功耗。
- 机房温度信息：通过 3D 视图呈现机房内温度分布情况，便于用户调整机房制冷。
- 机房功耗信息：通过 3D 视图呈现机房内各个机柜的功耗分布。
- 机房状态信息：通过 3D 视图呈现机房内异常状态设备所在的机柜。

图 4-11 3D 机房



4.6.2 网络拓扑

ISPIM 为用户提供了一个简单实用的可视化网络拓扑管理功能，具有易操作、实用的特点，能够帮助数据中心管理人员维护好网络。

1. 用户场景问题

随着互联网的蓬勃发展，数据中心基础设施也在不断地发展和扩大，数据中心网络的管理也越来越复杂，如何提供一个稳定、可靠、安全的网络运作环境成为首要解决的问题。只有采用行之有效的网络管理机制，才能保障网络能够充分发挥其独特优势。同时管理人员需要的是简单化、自动化、智能化的管理工具。能够简化管理人员日常的维护工作，将管理人员从机械、重复的手动监管中解放出来。同时能够清晰地呈现数据中心网络拓扑结构，标记网络中不同状态的设备类型，自动发现并更新网络中拓扑变化，支持手动编辑网络设备和链路信息，并提供简单易用的操作界面。

2. 方案介绍

ISPIM 基于中国移动 NFV 规范，通过网络资源端口信息从三方面自动生成网络拓扑结构。

1.网络设备之间链路

ISPIM 通过获取交换机、路由器的 LLDP mib 表的数据，能够获取到交换机、路由器的对端设备 Chassis ID 以及对端端口 Port ID，通过与资源数据中的所有交换机、路由器的 ChassisID 字段进行比较，匹配成功后，再将对端的 PortID 与匹配上

的交换机或路由器下的所有端口的 Name 进行比较，如果相同即这 2 个端口有链路连接。

2.服务器业务口与交换机之间链路绘制

服务器业务口的链路绘制依赖服务器带内操作系统向交换机定时发送 LLDP 报文，此报文的 Chassis ID 填写服务器的序列号，Port ID 填写服务器的端口 Mac 地址。

交换机收到 LLDP 报文后，将信息存放在 LLDP 的 mib 表中，ISPIM 用 Chassis ID 对比服务器序列号，Port ID 对比服务器端口 MAC（忽略大小写），计算出对端设备连接的是哪个服务器的哪个端口，从而绘制链路。

3.服务器硬件管理口与交换机之间链路绘制

由于部分服务器的硬件管理口不支持发送 LLDP 报文，这部分的服务器硬件管理口的链路通过 Mac 转发表的数据进行绘制，链路生成算法为：在 ISPIM 上手动设置交换机的类型是硬件管理交换机，并正确设置其端口连接类型：上行端口/下行端口/平行端口。ISPIM 获取硬件管理 TOR 交换机的 Mac 转发表，并将 Mac 转发表中的下行端口所对应的 Mac 地址找到，去服务器配置信息表中匹配服务器的 MAC 地址，匹配成功后，绘制该交换机端口到该服务器端口的链路，即服务器管理口链路。

3. 客户价值

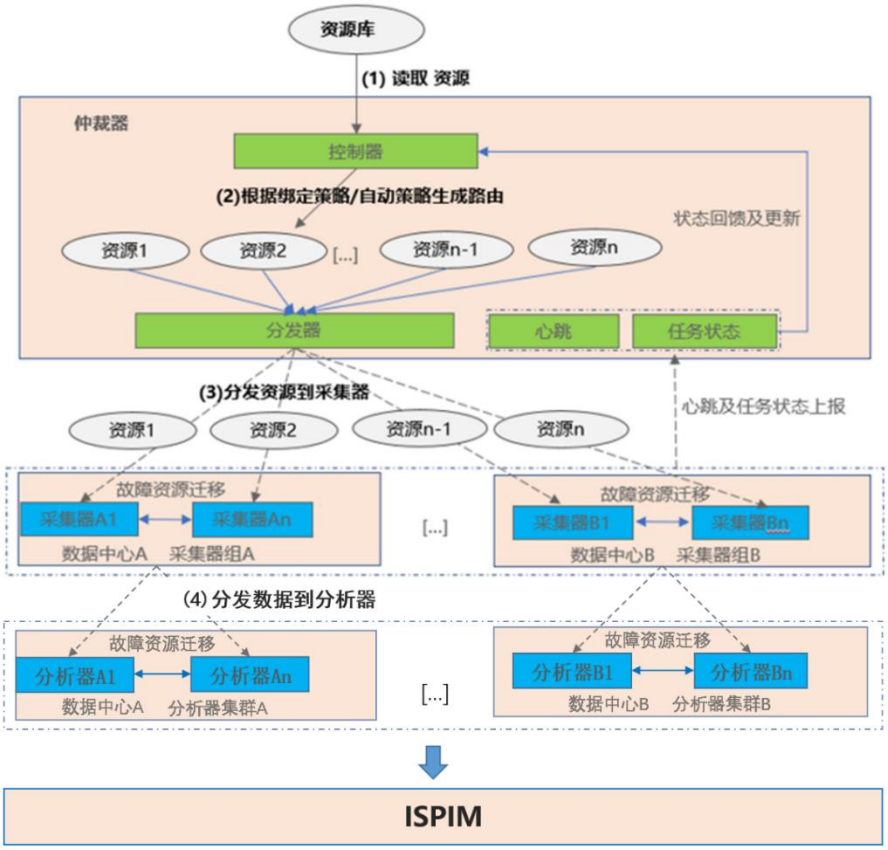
网络拓扑管理能够直观地给用户反映服务器、交换机、路由器等网络基础架构的运行状况和网络结构，能够给客户带来的主要价值如下：

- 自动发现网络中设备之间的关系并生成网络拓扑结构图
- 分层浏览网络拓扑，支持不同颜色直观展示网络设备和链路状态，清晰直观
- 兼容主流厂商、主流协议的网络设备
- 支持网络设备、网络链路手动编辑管理

4.7 智能容灾分布式管理

ISPIM 提供异地多数据中心、多机房的统一监控管理，将运行的系统任务按照资源的绑定信息负载均衡到不同的代理器执行，不同的采集器又可以把采集到的数据上报给分析器集群，保证了 ISPIM 监控节点的上限是可以横向扩展的。同时，ISPIM 为任务代理器与代理组提供了容灾策略，保证系统的高可用。另外，应对集中式场景，ISPIM 内置了集中式代理器与代理组，保障了 ISPIM 的拆箱即用。

图 4-12 智能容灾



4.7.1 采集器

ISPIM 采集器提供自动和手动绑定资源的策略，保证系统的高可用性。同时，ISPIM 提供了采集器所在设备的运行情况可视化管理，方便用户查看 ISPIM 采集器的运行状态。

- 自动绑定：提供按照负载均衡器方式绑定，根据用户录入资源时绑定的负载均衡器，系统自动做负载均衡与容灾迁移。
- 手动绑定：用户可手动绑定与解绑资源至采集器，从而实现资源的监控管理任务下发。
- 自动告警：当采集器离线时 IOPS 自监控模块会检测到集群状态发出告警

4.7.2 分析器

ISPIM 分析器提供了自动绑定资源的策略，无需在页面上做任何配置。使用自动

化脚本部署完成分析器集群后，不同的采集器就会自动的把数据上报给绑定的分析器。

- 自动绑定：不同采集器会自动上报数据给分析器，当分析器集群中有离线节点时，系统自动做负载均衡与容灾迁移。
- 自动告警：当分析器离线时 IOPS 自监控模块会检测到集群状态并发出告警。

4.7.3 负载均衡器

ISPIM 内置负载均衡器为资源绑定采集器的分组策略，同组内的采集器可认为有资源任务负载均衡的能力。

4.8 至关重要的安全管理

通过对用户管理、用户登录管理和证书管理等一系列安全策略，实现对 ISPIM 本身的安全控制，保证 ISPIM 系统的安全。

4.8.1 用户管理

ISPIM 缺省提供 admin 用户作为超级管理员，用户密码使用不可逆算法，MD5 加盐方式加密存储保障安全性。

- 支持用户的查看、增加、删除、修改。通过设定权限角色来决定用户管理权限。
- 支持用户的加锁/解锁用户功能，以限制某个指定用户的登录权限。
- 支持双认证（本地认证+LDAP 认证）登录认证：ISPIM 支持作用域管理，对用户的不同角色绑定不同的作用域，分别限制不同角色可操作的资源范围。
- 支持作用域的查看、增加、删除、修改。

4.8.2 鉴权管理

ISPIM 共有两种鉴权方式：本地认证、LDAP 认证。

- 本地认证：由 ISPIM 提供用户管理、登录鉴权、安全策略等功能，为默认的鉴权管理方式。
- LDAP 认证：支持使用域控制器中的用户域、组域、隶属于用户域的 LDAP 用户名及其密码登录，可以提高 ISPIM 系统安全性。

4.8.3 安全配置

ISPIM Web 默认为 HTTPS 安全访问模式。在用户密码连续错误的情况下（默认为 5 次），将会锁定用户一段时间，不允许登录，防止暴力破解。锁定时间默认 20 分钟，超级管理员可对锁定用户进行解锁。

4.8.4 证书管理

ISPIM 默认采用超文本传输安全协议（HTTPS） 进行数据的安全传输，且提供了一个默认证书。

- 支持证书信息的查看，包含序列号，剩余天数，颁发者，颁发给，开始时间和失效时间。
- 支持证书的上传，可以上传自己的证书文件（PFX 格式文件加证书密码）。
- 证书上传解析成功后，可以确定替换掉当前的证书，系统将重启加载最新证书。

4.9 标准的北向接口

ISPIM 以资源为中心，对外提供资产、告警、固件配置、固件升级等标准丰富的 REST 北向接口，便于第三方平台集成。

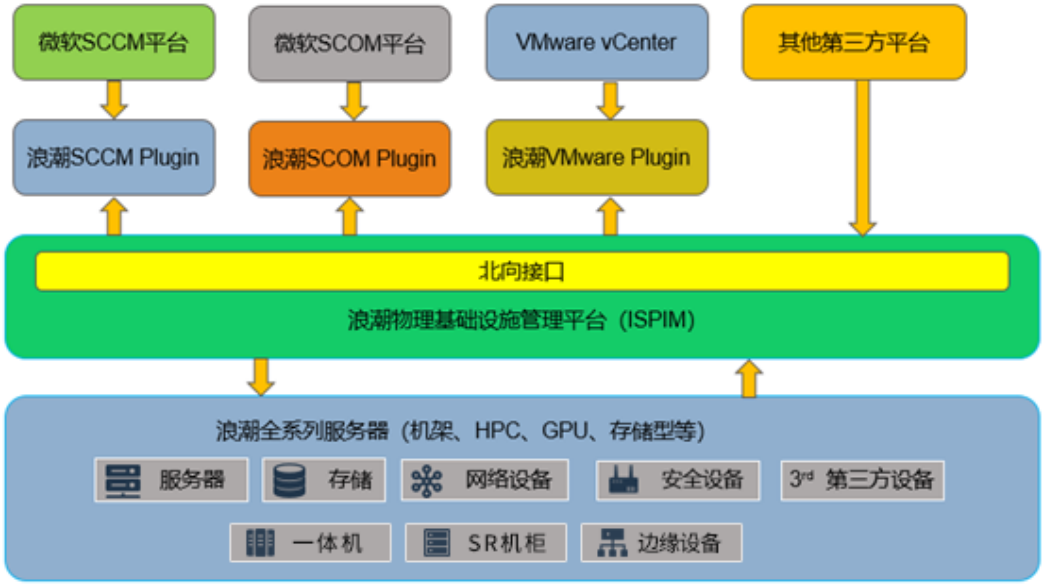
4.9.1 用户场景问题

对于大型数据中心，一般需要采购多个厂商的服务器、存储和网络设备，而普通管理软件无法完成设备的统一纳管，只能使用多套管理软件进行管理。对于多套管理软件，无法对所有设备进行资产、性能、告警等统一的呈现。用户只能依赖第三方平台对各个管理平台复杂的且不规范接口进行集成，以达到设备统一管理的目的，而不规范的北向接口会给集成带来不便。

4.9.2 方案介绍

ISPIM 不仅具有管理不同厂商的服务器、存储和网络设备的能力，还具有标准的 Restful、SNMP 等北向接口，供第三方管理平台进行集成。同时，ISPIM 可以通过浪潮 SCCM Plugin 与微软 SCCM 进行整合，实现浪潮服务器的配置；通过浪潮 SCOM Plugin 与微软 SCOM 进行整合，实现浪潮服务器的监控管理；通过浪潮 VMware Plugin 与 VMware vCenter 进行整合，实现浪潮服务器的监控管理。

图 4-13 北向实施方案



通过如上方案，第三方平台可以通过 ISPIM 北向接口或者浪潮 SCCM/SCOM/VMware Plugin，实现对浪潮服务器的资产、告警、固件配置、固件升级等功能，从而实现对浪潮服务器的全面管理，便于用户对所有设备进行统一管理。

4.9.3 客户价值

第三方平台通过标准丰富的北向接口实现对浪潮服务器的统一管理，从而实现对所有设备的统一的呈现、告警与配置。

SCCM/SCOM/VMware 管理平台,通过浪潮 SCCM/SCOM/VMware Plugin 实现对浪潮服务器的统一管理，实现对浪潮服务器的资产、告警与配置的管理。

5 部署方案

5.1 部署方式

ISPIM 根据纳管的节点数量、业务场景，提供单节点部署、高可用部署等方案。

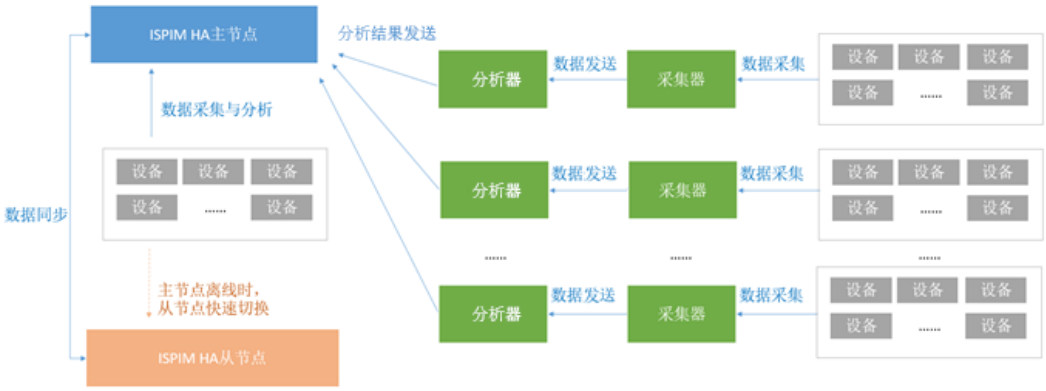
5.1.1 单节点部署

ISPIM 单节点部署具备“拆箱即用”（out-of-the-box）的特性，省去传统部署的繁琐步骤。

5.1.2 高可用部署

ISPIM 支持完备的 1+1+N 高可用部署方案,仲裁器采用主备部署方案。采集器，分析器采用集群式部署方案，可根据部署节点数灵活调整分析器及采集器个数。保证仲裁器高可用的同时如果采集器，或者分析器集群中有节点出现故障，资源可平均分配给其他采集器或者分析器上。单数据中心万级节点规模主备 1 分钟内完成全部切换，多数据中心万级规模 5 分钟内完成切换。

图 5-1 高可用部署示意图



5.1.3 采集分析集群部署

ISPIM 采集器与分析器支持横向扩容，对原有集群无任何影响。部署时只需要把扩容节点的 IP 及用户名密码在配置文件填写后即可完成一键化部署。

5.2 升级方式

ISPIM 提供版本升级包，一键升级，安全可靠。新版本生效需要重启 ISPIM 服务时，时间大约 10 分钟。

6 安全性

6.1 组网约束

由于 ISPIM 内部已经占用了 3306、8086、32314、32315、32316、32317、32318、32319、32320、32321、32322、32323、32324、32325、32326、32327、32229、161、162、623 端口，在规划端口时，和 ISPIM 业务相关的设备的其他业务需要避开这些端口。

表 6-1 组网约束

源端口	目的设备	目的地址	端口	协议	端口类型	是否可修改	认证方式	加密方式
随机	硬件设备	硬件管理口	80	TCP	采集服务器信息	不涉及	用户名、密码	HTTP 协议无加密
随机	硬件设备	硬件管理口	161	TCP/UDP	采集服务器信息	不涉及	v1/v2c: 团体名 v3: 用户名/密码	加密算法: MD5/SHA 隐私算法: AES/DES
随机	硬件设备	硬件管理口	443	TCP	采集服务器信息	不涉及	用户名、密码	HTTPS 使用 TLS
随机	硬件设备	硬件管理口	623	TCP/UDP	采集服务器信息	不涉及	用户名、密码	
随机	采集器部署设备	采集器	162	TCP/UDP	服务器客户端告警上报至服务端（snmp）	是	v1/v2c: 团体名 v3: 用户名/密码	加密算法: MD5/SHA 隐私算法: AES/DES

源端口	目的设备	目的地址	端口	协议	端口类型	是否可修改	认证方式	加密方式
随机	分析器部署设备	分析器	32325	TCP	上报采集到的数据（http）	是	Token 认证	HTTP 协议无加密
随机	采集器部署设备	采集器	32320	TCP	仲裁器下发采集任务（http）	是	Token 认证	HTTP 协议无加密
随机	仲裁器部署设备	用户服务	32324	TCP	监控软件（http）	是	Token 认证	HTTP 协议无加密
随机	北向服务部署设备	北向服务	32321、32322	TCP	ISPIM 北向接口(http 、https)	是	Token 认证	HTTP 协议无加密 HTTPS 使用 TLS
随机	采集器部署设备	采集器	32314、32315	TCP	采集器接收指令（RMI）	是	证书认证	RMI 协议 TLS 加密
随机	分析器部署设备	分析器	32318、32319	TCP	分析器接收数据（RMI）	是	证书认证	RMI 协议 TLS 加密
随机	仲裁器部署设备	仲裁器	32316、32317	TCP	仲裁器接收任务状态	是	证书认证	RMI 协议 TLS 加密
随机	北向服务部署设备	北向服务	32230、32231	TCP	北向服务接收数据（RMI）	是	证书认证	RMI 协议 TLS 加密

6.2 系统安全

用户可以从操作系统加固来了解 ISPIM 的系统安全。

操作系统加固

- ISPIM 基于 CentOS7.9 操作系统，并经过安全加固，确保应用程序运行在安全的环境中。
- ISPIM 操作系统镜像仅保留了 CentOS7.9 需的核心服务，通过操作系统最小化安装，确保只安装和启用系统必须的服务，减少被黑客攻击的风险。
- ISPIM 选用安全稳定的数据库版本和其他中间件版本，以解决最基本的安全问题。

6.3 应用安全

ISPIM 的应用安全体现在访问安全、数据安全、通信安全、编码安全和日志审计安全五个方面。

访问安全

- 应用程序并不是单独存在的。它们不仅能访问其他系统和应用程序，而且能够被系统管理员、用户、业务支撑系统、其他系统和其他应用程序等访问。因此，应用程序中必须设计适当的访问安全方案。在 ISPIM 的应用程序中，访问安全措施通过帐号管理、身份验证、密码管理方面执行。

数据安全

应用系统中最重要的数据包括：系统数据、数据库数据、机密数据、用户私有数据等。ISPIM 应用程序通过加密技术、访问控制措施来保护数据的安全。加密技术是保护数据最重要也是最普遍的方法。为了确保加密的效果和性能，ISPIM 应用程序遵守如下加密规范：

- 不使用有缺陷的算法，例如 SHA-0/SHA-1/DES 等，尤其是一些被破解的算法。
- 采用 SHA-256/HMAC-SHA-256/AES/PBKDF2 等算法。

通信安全

- 应用程序必须与其他系统和组件通信，相互之间交互信号与数据。如果通信存在漏洞，不仅会威胁通信的信息，而且还会威胁到应用程序和整个系统。所以通信安全是应用层安全的重要组成部分。
- 采用身份验证、加密协议、完整性保护等技术确保通信安全。在建立一个通信连接之前必须执行严格的身份验证。
- 使用 TLS/HTTPS 协议代替不安全的协议。

编码安全

编码安全是系统安全的基础。许多攻击利用系统编码的漏洞，如缓冲区溢出、拒绝服务、SQL 注入等。ISPIM 应用程序遵循编码安全规范，如下：

- 最小化受攻击面：即最小化或者加强应用程序暴露的功能，尤其是网页和通信接口。
- 最小特权原则：越多特权会产生越多风险，因此应用只能拥有最少的特权。
- 故障保护：避免不合理的故障产生的漏洞。
- 不受信服务：所有的外部系统都需要经过不受信处理。
- 职责分离：不同职责不同的角色能够避免在职者集中的系统中权限滥用。
- 消除编码中的不安全因素：必须加强关键系统和应用程序源码的安全性。
- 保持简单的安全措施：开发中应避免使用双重否定和复杂的结构而使用更简单的方法将会更快和更简单。

7 可靠性

7.1 集群可靠性

ISPIM 支持集群管理，多个 ISPIM 节点加入一个集群后，可由其中一个节点对整个集群系统进行管理。当管理节点出现故障，另外一个节点会自动接管，不会影响业务运行。

7.2 数据可靠性

备份与恢复功能是保证系统在出现异常情况时，能够快速恢复正常运行的重要保证。

ISPIM 支持数据库的备份与恢复，可根据系统情况设置备份策略为自动备份或手动备份。可以设置定期备份的周期和备份的路径。

8 配置要求

为保障 ISPIM 正常运行，所属设备的的硬件配置必须满足一定的要求。

表 8-1 ISPIM 主服务配置要求

项目	要求
CPU	500 节点以下>=8 核 2000 节点以下>=16 核
内存	500 节点以下>=16GB 2000 节点以下>=32GB
硬盘	>=300GB (当管理规模大于 1000 节点时，建议每 1000 节点增加 100GB)
网卡	>=1 个

采集分析集群节点建议每 2000 个节点增加一个节点要求配置如下表所示。

表 8-2 ISPIM 采集分析集群节点配置要求

项目	要求
操作系统	Centos7.9 最小化安装
CPU	8 核
内存	32 GB
硬盘	>=200GB

网卡	>=1 个

A 如何获取帮助

A.1 收集必要的故障信息

在进行故障处理前，需要收集必要的故障信息。

收集的信息包括：

- 客户详细名称、地址
- 联系人姓名、电话号码
- 故障发生的具体时间
- 故障现象的详细描述
- 设备类型及软件版本
- 故障后已采取的措施和结果
- 问题的级别及希望解决的时间

A.2 如何使用文档

浪潮电子信息产业股份有限公司提供全面的随设备发货的指导文档。指导文档能解决您在日常维护或故障处理过程中遇到的常见问题。为了更好的解决故障，在寻求浪潮技术支持前，建议充分使用指导文档。

A.3 获取技术支持

浪潮电子信息产业股份有限公司通过办事处、电话技术指导、远程支持及现场技术支持等方式向用户提供及时有效的技术支持。

浪潮电子信息产业股份有限公司技术支持体系包括：

- 客户服务中心：(+86)400-860-0011; (+86)800-860-0011
- 企业业务网站（https://www.inspur.com）

B 术语和缩略语

术语	说明性定义
ISPIM	Inspur Physical Infrastructure Manager，浪潮物理基础设施管理平台
BMC	Baseboard Management Controller，基板管理控制器
BIOS	Basic Input Output System，基本输入输出系统
RAID	Redundant Arrays of Independent Drives，磁盘阵列
DHCP	Dynamic Host Configuration Protocol，动态主机设置协议
DNS	Domain Name System，域名系统
IPMI	Intelligent Platform Management Interface，智能平台管理接口
SNMP	Simple Network Management Protocol，简单网络管理协议