

Mate-iMonitor
机房应用服务性能综合
监控系统
产品技术白皮书



目录

1 系统简介.....	4
2 架构及方案.....	6
2.1 架构	6
2.1.1 数据采集模块.....	6
2.1.2 数据储存和分析模块.....	7
2.1.3 B/S 可视化人机界面模块	7
2.1.4 预警模块.....	7
2.1.5 扩展组件.....	7
2.2 方案	8
3 详细功能.....	9
3.2 网络设备监控.....	9
3.3 服务器监控.....	9
3.3.1 硬件状态监控和管理.....	9
3.3.2 操作系统运行状态监控.....	10
3.4 应用及业务系统监控	10
3.4.1 基础监控.....	10
3.4.2 深层次监控.....	10
3.5 数据库监控.....	11
3.6 流量分析.....	10
3.7 SYSLOG 日志分析.....	10
3.8 机房环境监控	11
3.9 预警和运维服务管理	11
4 云技术及分布式管理集中监控.....	12
4.1.1 云技术.....	12
4.1.2 分布式管理集中监控.....	13
5 B/S 可视化人机接口.....	13
5.1 “极简” 人机界面	13
5.2 自动发现和智能向导配置	17
5.3 基于角色的分级权限管理	18
5.4 网络拓扑.....	19
5.5 历史记录和性能曲线	20
5.6 报表.....	23
5.7 资产管理.....	24
6 产品特点.....	26
6.1 领先的全硬件产品方案.....	26
6.2 更高效和安全.....	26

6.3 对网络和目标影响极低.....	27
6.4 易于定制扩展.....	27

1 引言

◆ 什么是应用安全

说到安全，人们自然就会想到网络安全，但是实际情况是运营的风险更多来自于业务应用系统自身的安全性。常规安全理念往往局限于网关级别、网络边界（防火墙、IDS、漏洞扫描）等方面的防御，但是对于重要的 WebLogic、WebSphere、Jboss、Tuxedo、Tomcat 等应用系统，对 Oracle、IBM DB2、Sybase、MySql、MS SQL 等数据库，对 PHP、Apache、IIS 等 Web 服务器，对 Unix、AIX、Solaris、Linux、Windows 等操作系统的业务应用系统故障和安全威胁，没有足够的认识。而在实际中，应用安全是众多安全管理人员经常面临的棘手问题。

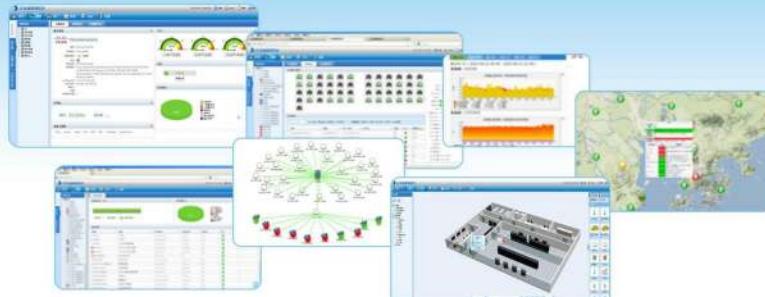
◆ 应用安全的重要性

当前，业务应用系统已成为业务运营的核心组成部分，是业务成败的决定性因素。随着业务应用系统的不断技术创新，一方面不断完善自身的体系结构和实施手段；另一方面，它引导新业务模式的产生，成为生产力提升和变革的原动力。正是由于业务应用系统对于业务模式，乃至整个社会沟通方式所产生的显著而巨大的影响，使得对业务应用系统安全的重要性，也越来越引起人们的重视。

保证业务系统的不间断稳定运行，实时对各种业务系统、应用程序、服务器运行状况的信息，能够全面显示和深入报告网络关键业务的行为，确保业务系统的正常运行，对于政府、金融、交通、能源、医疗等诸多行业的业务部门与运维部门的来说是头等大事。通过 APM 预警功能及早发现问题，将问题消灭在萌芽状态，消灭在影响到业务正常运行之前。APM 通过专业或者智能化手段辅助管理员全面及时的了解网络关键业务系统的健康状态，实现业务运维的 24 小时无人值守。

Mate-iMonitor 是创新和领先的 IT 运维管理硬件产品。“极简”的设计提供全面的应用性能监控预警解决方案。

用户体验



监控系统

cisco HUAWEI H3C Juniper ZTE 中兴 IBM hp DELL NetApp lenovo

网络设备、服务器、存储设备

Windows Linux AIX vmware SQL Server ORACLE MySQL SYBASE WebSphere.

WebLogic UNIX DB2 SOLARIS Tomcat HP-UX JBoss

操作系统、数据库、中间件



环境、市电、空调、门禁等

监测视图

监控列表	业务拓扑
物理拓扑	动环拓扑

高级模块

SYSLOG
流量分析
资产管理

报告系统

实时报表	统计报表	可用性报告	定制报表

故障处理

一般告警 | 严重告警

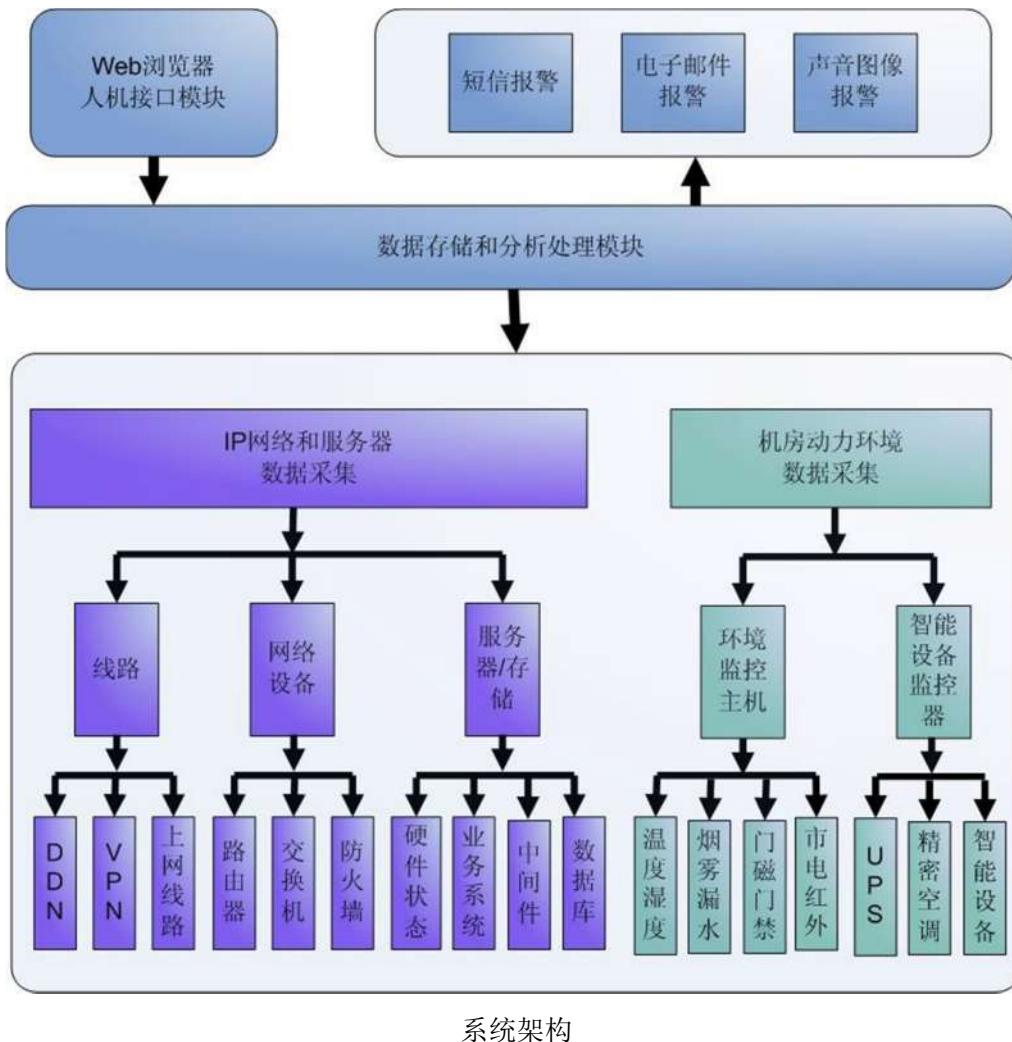
报警方式: 邮件 | 短信 | 声音 | 声光 | 颜色

2 架构及方案

2.1 架构

Mate-iMonitor 全 web 配置管理，运行更稳定可靠，监控预警 更快速准确。优化的核心程序，对网络带宽占用极低，同时对目标网络设备和服务器性能影响极低。

系统主要由数据采集、数据储存和分析处理、B/S 可视化人机界面、报警等模块组成，并提供多种扩展组件。



2.1.1 数据采集模块

数据采集模块通过 SNMP、WMI、SYSLOG、IPMI、各种应用层协议 (ICMP、HTTP、FTP、TELNET、SMTP、POP3 等) 及私有协议，对网络专线 (DDN、VPN)、网络设备、服务器、各种应用和数据库系统等进行各种数据采集，提交到数据储存和分析模块处理。

2.1.2 数据储存和分析模块

数据储存和分析处理模块对采集模块提交的数据进行分析，确定监控目标的状态（正常、一般告警和严重告警、错误等），向 B/S 可视化人机界面模块提交状态信息。同时，将数据储存到数据库中，提供接口供人机界面模块进行历史数据查询。

2.1.3 B/S 可视化人机界面模块

B/S 可视化人机界面模块通过 web 对用户提供配置、管理和告警接口。用户通过 web 进行系统配置、监控目标配置，查看网络拓扑图和监控目标的状态，查询历史数据生成详尽的性能曲线图、故障和告警历史记录，生成报表。

人机界面也提供完整的管理员操作日志查询、配置备份和恢复、系统手动和自动升级等多种管理功能。

2.1.4 预警模块

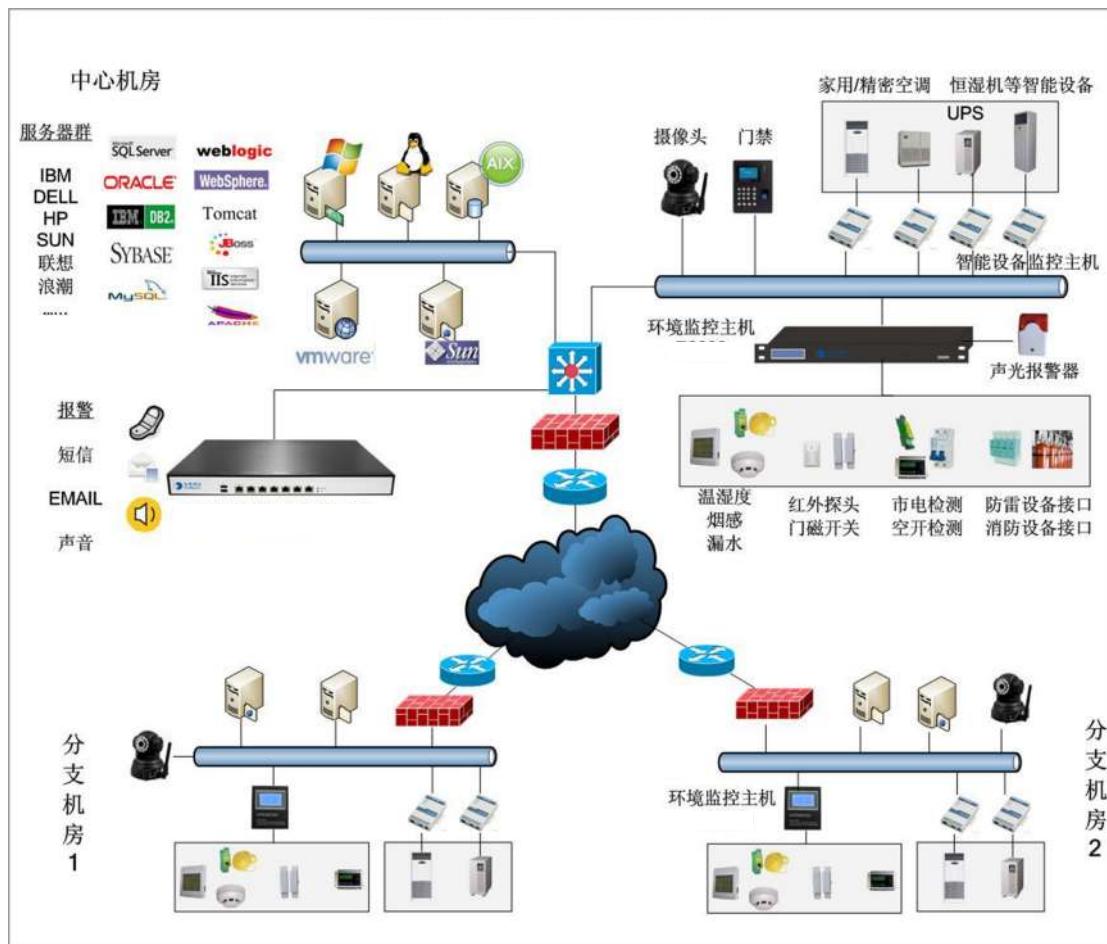
预警模块通过人机界面的弹出窗口和声音进行声光预警，同时支持通过发送电子邮件和手机短信、声光、电话通知等多种手段进行预警。

2.1.5 扩展组件

系统提供流量分析、机房动力环境、设备日志储存管理等多种组件，根据需要可灵活扩展。

- 流量分析组件通过 netflow/sflow/抓包分析等进行 IP 和应用流量统计、TOPN 列表、故障诊断、带宽容量规划决策等高级功能。
- 机房动力环境组件结合动力和环境探测设备，可以实现对机房动力（市电）、环境参数（温度、湿度、烟雾、漏水、门磁、红外）和 UPS、精密空调、家用空调、门禁等智能设备的监控预警。
- 日志储存服务组件通过 SYSLOG 协议接收和储存被监控的网络设备、服务器的日志。提供查询和管理，快速发现和定位存在的设备和服务器安全事件，设置指定关键字日志监控预警等高级功能。

2.2 方案



全面应用性能监控预警解决方案示意图

方案描述:

- 实现 DDN 专线和 VPN 隧道等通信线路监控
- 实现网络设备状态性能监控
- 实现服务器的硬件和各种操作系统状态性能监控
- 实现数据库和应用系统状态性能监控
- 实现 IP 和应用流量分析
- 实现 SYSLOG 日志分析
- 实现机房动力环境监控（需环境监控设备和各类探头支持）
- 实现多分支机房分布式部署统一监控
- 实现声光、电子邮件、短信预警和运维服务管理

3 详细功能

3.1 通信线路监控

对DDN专线、VPN隧道等网络线路的通断、丢包和延时情况进行监控，检测间隔最低可支持到1秒，提供详尽的延时和丢包性能曲线。

结合网络设备端口流量监控以及详细的IP和应用流量统计分析，实现最为全面的带宽监控、故障诊断和带宽容量规划决策。

系统以Cisco SLA（服务品质协议）为基础，针对大中型企业专网（DDN、VPN）和电信运营商的骨干网络，对不同服务等级（TOS）的延时、抖动率的进行端到端监控，并可扩展对TCP、UDP、HTTP、DNS、DHCP、FTP等应用协议的SLA支持，以保证网络的高可靠性和高品质运行。

3.2 网络设备监控

对可网管的支持SNMP协议的路由器、交换机、防火墙等网络设备进行监控。支持Cisco、Netscreen、Juniper、F5、飞塔、H3C、华为、中兴、锐捷等国内外著名厂家设备。

监控主要内容包括：

CPU负载/内存使用量/磁盘使用量/端口状态和流量等基本运行状态。

设备电源/风扇/内部温度等硬件状态（H3C等厂家部分设备支持）。

- 接口错误包率/丢包率/广播包率等。

对F5负载均衡设备的业务性能提供更为深入的支持，包括：

- 机箱电源、温度和风扇转速等硬件环境。
- HOST、TMM CPU利用率和内存、磁盘利用率，CPU温度和风扇转速等基本运行状态。
- 全局、虚拟服务器、服务器池及成员的连接数和流量等业务性能。

3.3 服务器监控

3.3.1 硬件状态监控和管理

对支持IPMI协议的服务器，不需依赖操作系统，实现对硬件运行状态进行监控和管理。在对IPMI协议的支持上在国内处于领先地位。

目前大部分厂家的服务器，如HP、IBM、DELL和国内联想等众多的品牌服务器都支持IPMI协议。

监控和管理主要内容包括：

- 风扇转速、机箱内部和CPU温度、电源电压、电源开关、CMOS电池容量、磁盘和内存、

RAID 卡等硬件状态。

- 远程开机或重启服务器。(授权情况下)
- 定时关机或重启服务器。(授权情况下)

3.3.2 操作系统运行状态监控

通过SNMP支持对服务器中操作系统运行及性能状态进行监控。当前支持Windows、Linux、UNIX、AIX、HP-Unix、VMware、Solaris、OS/400等操作系统。

监控主要内容包括：

- CPU/内存/磁盘空间/IO 读写/网口状态和流量等。
- 接口错误包率/丢包率/广播包率等。
- 系统应用进程状态/进程负载和服务等。

3.4 应用及业务系统监控

3.4.1 基础监控

系统通过模拟访问的方式，对任意操作系统上运行的 HTTP、HTTPS、FTP、Telnet、FTP、ICMP、IMAP、Pop3、SMTP、URL 及任意TCP端口上的应用服务的可用性、访问质量等进行监控。

3.4.2 深层次监控

对广泛应用的业务系统/OA/ERP/WEB/邮件系统/中间件等服务的详细运行状态和性能参数进行监控。

服务	监测内容
Apache	Apache 对服务器的CPU 占用率、服务流量情况、服务连接数情况、每秒处理请求数等。
Nginx	Nginx 对服务器的CPU 占用率、服务流量情况、服务连接数情况等。
IIS	所有或者指定虚拟主机的接收和发送流量、总流量、当前总并发连接数、最大并发连接数、当前非匿名用户并发连接数、每秒GET请求、每秒POST请求、NotFound 错误的总数等。
Media Server	播放并发连接数、播放流带宽等。

Terminal Server	当前总会话数、活动的会话数、非活动会话数等。
Exchange Server	邮箱存储的接收队列和发送队列的邮件数、公用文件夹的接收队列和发送队列中的邮件数、发送队列中的邮件数、工作队列中未完成的邮件数等。
Tomcat	JVM 内存的使用率统计、请求信息统计，包括每秒请求数、每秒错误数、流量统计、线程统计、请求信息统计（包括请求数量、错误总数、接收和发送总流量）等。
WebSphere	WebSphere 的 CPU 和内存利用率、JDBC 连接池监控、事务监控、线程监控等
WebLogic	JMS 连接数、JRockit 监控(包括 CPU、内存、线程数监控)、JTA 回滚事务监控、SUN JVM 堆使用率、WebLogic 活动队列的空闲线程数、队列长度、吞吐量监控等。
Lotus Domino	用户会话数等。

模块化的框架设计，让系统通过扩展各种类型监测器，可以对更多应用进行深入监控。

3.5 数据库监控

数据库作为信息化系统最重要的组成部分，对业务系统的运行起到关键作用。系统主要使用模拟访问方式，对主流的数据库的性能参数进行监控。监控颗粒度非常细，为管理员提供更详尽的信息，更容易优化数据库性能。

数据库	监控内容
Oracle	<p>主要为包括：</p> <ul style="list-style-type: none"> ● Oracle 数据库表空间利用率 ● Oracle 连接用户数 ● Oracle 连接响应 ● Oracle Rollback segment 命中率 ● Oracle Redo Log IO 流量 ● Oracle 日志缓冲区重试率 ● Oracle Soft Parse 命中率 ● Oracle In-memory Sort 比率 ● Oracle 共享池重载率 ● Oracle Latches 命中率 ● Oracle Dictionary Cache 命中率

	<ul style="list-style-type: none">● Oracle Library Cache 命中率● Oracle Data Buffer Cache 命中率● Oracle 共享池内存空闲率 <p>等 20 多个重要参数。</p>	
SqlServer	主要包括： 数据库连接响应时间、已连接的用户数、CPU 占用率、占用的内存、负载、每秒的全表扫描次数、每秒批请求数、每秒的重编译数、数据缓存命中率、数据库剩余空间等 20 多个重要参数。	
Mysql	主要包括数据库连接响应时间、数据库服务已运行的时间、当前连接数、线程缓存命中率、查询命中率、表缓存命中率、数据库访问流量等 20 多个重要参数。	
DB2	主要包括数据库连接响应时间、数据库服务已运行的时间、当前连接数、线程缓存命中率、查询命中率、表缓存命中率、数据库访问流量等参数。	
Sybase	主要包括数据库连接响应时间、数据库服务已运行的时间、当前连接数、线程缓存命中率、查询命中率、表缓存命中率、数据库访问流量等参数。	
Informix	主要包括数据库表空间、数据库在线情况、数据库故障检测等参数。	
Kingbase	主要包括数据库的表空间利用率、数据库的连接用户数、数据库的 redolog 可用数、数据库的连接响应时间探测、数据库的索引使用率等参数。	

3.6 流量分析

通过 Netflow、Sflow、抓包分析等手段进行 IP 和应用流量统计，可帮助管理员发现网络中占有带宽最多的 TOPN 用户及应用。进行故障诊断、带宽容量规划决策。可设置当有 IP 流量超过阀值时进行实时报警。

3.7 SYSLOG 日志分析

集中管理网络设备和服务器等的日志信息，快速发现和定位存在的设备和服务器安全事件，并可设置指定关键字日志实现监控预警。

3.8 机房环境监控

结合环境监控主机和各类探头，可以实现对机房动力（配电柜、配电箱、空气开关）、环境参数（温度、湿度、烟雾、漏水、门磁、红外、消防、风速）和 UPS、精密空调、家用空调、门禁等智能设备的监控预警。



3.9 预警和运维服务管理

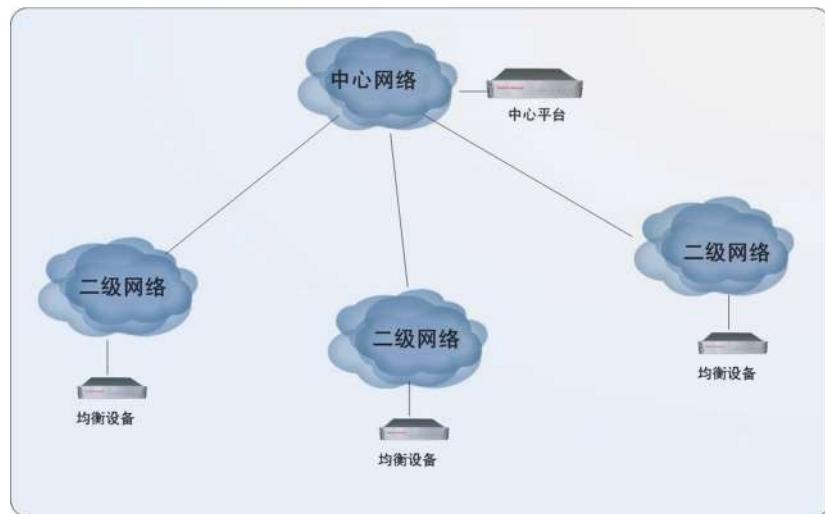
系统可设置两级报警阀值，有故障时可进行电子邮件、短信、弹出窗口、声光报警、电话等多种方式预警。管理员可进行值班表管理、人员分组和进行告警升级设置。

可将监控预警、资产以及运维服务整合，更有效的提升 IT 管理水平、服务 质量和效率。运维服务管理包括资产管理，事故管理、流程管理和问题管理等。

4 云技术及分布式管理集中监控

4.1.1 云技术

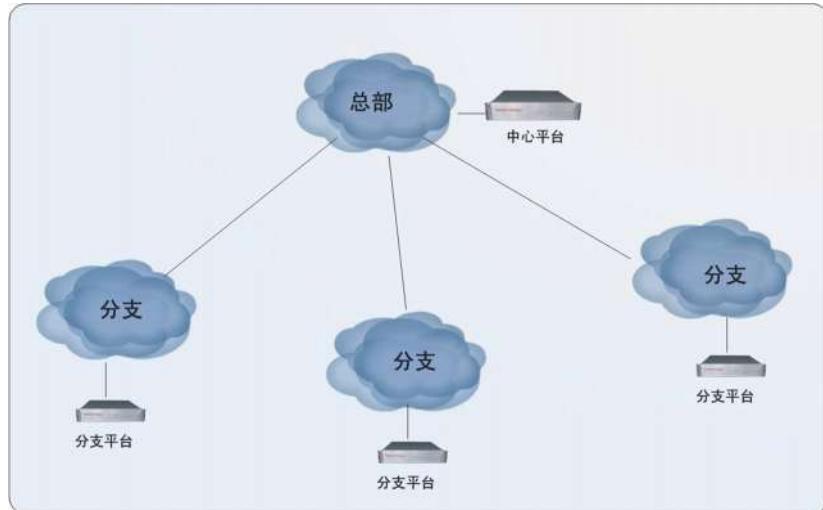
系统通过创新的“云技术”，在网络不同节点部署“监测均衡设备”，实现大规模或超大规模的监测，轻松超越 10000 个以上参数的监控，并最低支持 10 秒以下的数据采集间隔。



云技术示意图

4.1.2 分布式管理集中监控

对于多级网络，可在中心和各级机房单独部署独立的系统，各自管理。同时可将下级系统产生的故障信息上报到上级系统，实现集中监控。



分布式示意图

5 B/S 可视化人机接口

5.1 “极简” 人机界面

通过模块化的监测器类型扩展，具有丰富而强大的功能。

1. B/S 模式，只需要浏览器而不需要安装专用的客户端程序，是最方便和直接的管理方式。
2. 采用任意分级的资源树和表格的统一风格，配以使用直观的饼状图、柱状图和曲线图，以及多种颜色来表示监控目标的各种状态，一目了然，专业且人性化。
3. 提供自由和灵活的可定义 Portal 以及强大的在线帮助系统。

首页 视图 资产 报表 日志 设置

监测器状态概览

电信出口流量曲线

FastEthernet0_1

2013-08-28 12:22 - 2013-08-28 16:22

参数	值
入流量	最大 1.19 M
出流量	最大 461.18 k
	平均 258.23 k
	最小 29.02 k
	最近 935.36 k
	总量 3.68 Gb
	总计 3.32 Gb

关注设备组

组名	描述	设备数	监测器数	状态
安全设备	安全设备	2	4	正常
动力环境	动力环境	2	16	正常
服务器	服务器	8	56	异常
交换机	交换机	6	56	正常
路由器	路由器	1	4	正常
其他设备	其他设备	2	7	正常
网络设备	网络设备	0	0	正常
虚拟化	虚拟化	1	8	异常

关注设备列表

设备名	描述	IP或域名	响应时间	丢包率	状态
FreeSMonitor	FreeSMonitor	192.168.88.252	95.71ms	--	正常
FSCenterSwitchA	FSCenterSwitchA	192.168.88.1	4.67ms	0%	正常
FSCenterSwitchB	FSCenterSwitchB	46.46.46.2	89.96ms	--	正常
FSROUTE1	FSROUTE1	45.45.45.1	5.74ms	--	正常
Linux服务器	Linux服务器	192.168.88.26	6.54ms	0%	正常
VMwareESXi	VMwareESXi	192.168.88.199	24.54ms	0%	异常

今日故障日志

监测器名	所属设备	时间	状态	快照信息
存储检测	fs.com.bbbs	2013-08-28 15:46:38	异常	二级警告 - 184.22.219.6:延时 2006.183毫秒,丢包率 50%
存储检测	fs.com.bbbs	2013-08-28 15:43:38	异常	一级警告 - 184.22.219.6:延时 1190.733毫秒,丢包率 20%
存储检测	fs.com	2013-08-28 15:42:40	异常	二级警告 - 69.172.213.167:延时 2122.156毫秒,丢包率 60%

可自定义的 Portal 人机界面

首页 视图 资产 报表 日志 设置

状态列表

- 资源信息
- 拓扑图
- 流量分析
- 可用性分析

设备组概况

设备组名称: ALL

设备总数: 22 正常设备数: 18 异常设备数: 4

监测器总览

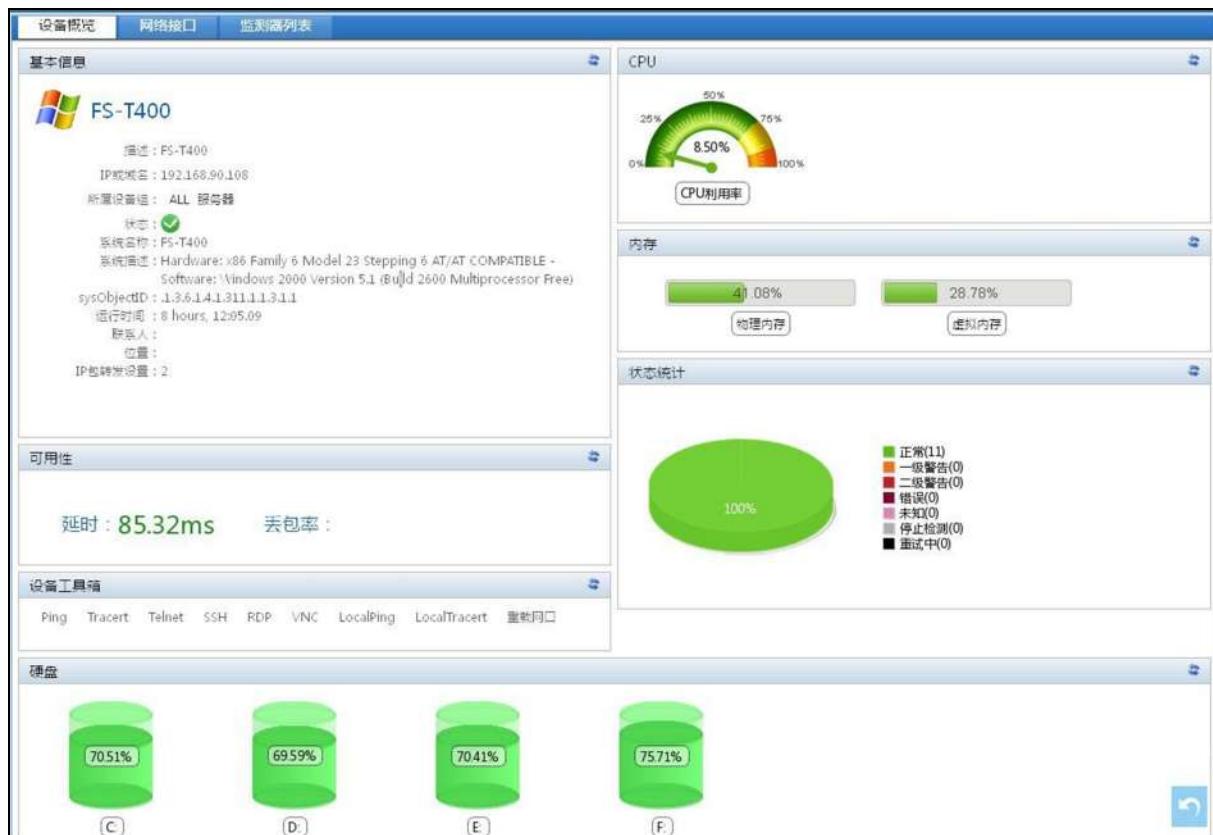
正常(129)
一级警告(1)
二级警告(2)
错误(1)
未知(4)
停止检测(14)
配置中(0)

设备列表

设备名	描述	IP或域名	响应时间	丢包率	状态	操作
FCCOMPUTER	FCCOMPUTER	192.168.88.99	102.53ms	--	异常	
FreeSMonitor	FreeSMonitor	192.168.88.252	95.71ms	--	正常	
FS-T400	FS-T400	192.168.90.108	9.16ms	--	正常	
fs.com	fs.com	69.172.213.167	2366.56ms	70%	异常	
fs.com.bbbs	fs.com.bbbs	184.22.219.6	1494.22ms	30%	异常	
FSCenterSwitchA	FSCenterSwitchA	192.168.88.1	1.25ms	0%	正常	
FSCenterSwitchB	FSCenterSwitchB	46.46.46.2	53.92ms	--	正常	
FSpC2	FSpC2	192.168.88.98	4.14ms	--	正常	
FSROUTE1	FSROUTE1	45.45.45.1	6.24ms	--	正常	
Linux服务器	Linux服务器	192.168.88.26	1.17ms	0%	正常	
Lswitch1	Lswitch1	192.168.88.3	13.96ms	--	正常	
Lswitch2	Lswitch2	192.168.90.4	8.84ms	--	正常	
H3CLswitch3	H3CLswitch3	192.168.90.5	209.43ms	--	正常	
H3CLswitch4	H3CLswitch4	192.168.90.6	165.65ms	--	正常	

直观的资源树和分组表格

14



服务器实时信息展示界面



资源信息

设备概览 网络接口 监测器列表

网络接口面板

192.168.90.134	apache	C2000	FSpC2	fs.com	FCOMPUTER	FSCenterSwitchA	Lswitch1	Lswitch3	Lswitch4	localV3TEST1	Linux服务器	mysql监控系统	ORACLE	SQL-SERVER	VMwareESXi	weblogic
测试设备1	出口防火墙	视频摄像机	安全设备	动力环境	服务器	交换机	路由器	其他设备	虚拟化							

网络接口

加入监控 | 删除监控 | 启用端口 | 关闭端口 实时信息：路由表 | A

接口类型: ethernetCsmacd 确定

别名(ifDescr)	别名(ifName)	别名(ifAlias)	类型
FastEthernet0/1	Fa0/1	abc	ether
FastEthernet0/2	Fa0/2	jiekou2	ether
FastEthernet0/3	Fa0/3		ether
FastEthernet0/4	Fa0/4		ether

接口别名(ifDescr): FastEthernet0/18
接口别名(ifName): Fa0/18
接口别名(ifAlias):
管理状态:

连接状态:
类型: ethernetCsmacd
MAC地址: 00:12:43:E3:11:12
IP地址:
MTU: 1500
速率: 100Mbps
实时流量: --/--
总流量: 2.8Gb/0.07Gb
总丢包: 0/0
总单播包: 1733794/258083
总广播包: 19925887/692327

监控	状态	速率	上行/下行	操作
是		100Mbps	0.08Mbps/0.35Mbps	
否		100Mbps	--/--	
是		100Mbps	0Mbps/0Mbps	
否		10Mbps	--/--	

详尽和直观的网络设备实时信息展示界面

设备概览 网络接口 监测器列表

监测器状态

监测器总数: 18 正常: 18 一级警告: 0 二级警告: 0 错误: 0 未知: 0 停止检测: 0

监测器名	描述	状态	状态信息	操作
/			磁盘/挂载点48%(总大小: 14.89GB),	
/boot			磁盘/boot挂载点13%(总大小: 0.10GB),	
/dev/shm			磁盘/dev/shm挂载点0%(总大小: 0.25GB),	
/opt/fsm/tmpfs			磁盘/opt/fsm/tmpfs挂载点9%(总大小: 0.50GB),	
CMOS电池			CMOS_Battery:2.80Volts	
CPU风扇转速	CPU风扇转速		CPU风扇转速4275.00RPM	
CPU使用率			CPU空闲率: 95.00%	
DIMM风扇转速	DIMM风扇转速		DIMM风扇转速4425.00RPM	
eth0			流入流量为0.00Mbps 流出流量0.00Mbps	
HTTP服务	HTTP服务		正常: HTTP/1.1 200 OK - 页面大小: 7888 字节 响应时间: 0.740 秒	
Linux系统进程数统计			总进程数: 87	
Linux系统资源			最近系统Load:一分种 0.16,五分钟 0.08,十五分钟 0.02 内存利用:至5.69%(总大小:503.26MB) Sswap利用:至56.53%(总大小:511.99MB)	
PCI风扇转速	PCI风扇转速		PCI风扇转速1350.00RPM	
sda磁盘IO	sda磁盘IO		每秒读字节:0.00Bps 每秒写字节:19.00KBps 每秒读IO:0.00 每秒写IO:0.98	
sshd进程	sshd进程		正常:所有进程运行正常	
存活检测			正常 - 192.168.88.26:延时 4.122毫秒,丢包率 0%	
机箱内部温度	服务器内部温度		服务器内部温度:38.00摄氏度	
系统资源			最近系统Load:一分种 0.07,五分钟 0.07,十五分钟 0.01 内存利用:至6.14%(总大小:503.26MB) Sswap利用:至56.53%(总大小:511.99MB)	

直观的服务器硬件/资源/应用监控界面



The screenshot shows a network monitoring interface for IP flow analysis. At the top, there are tabs for '流量概况' (Traffic Overview) and '流量列表' (Traffic List). Below the tabs are filter options: '列表类型' (List Type: IP列表), '流向' (Direction: 目的), '列表排名' (List Ranking: 前20), '时间类型' (Time Type: 最近一分钟), and a '刷新' (Refresh) button. A '数据过滤器' (Data Filter: any) field is also present.

The main area displays a table of IP flows. The columns are: Flows, Bytes (总字节数), Packets (总包数), avg_bps (平均每秒流量), avg_pps (平均每秒包数), and avg_bpp (平均每秒流里). The data shows various IP addresses and their traffic metrics. For example, the top flow is 192.168.88.25 with 573.72K bytes and 3.13K packets.

Flows	Bytes (总字节数)	Packets (总包数)	avg_bps (平均每秒流量)	avg_pps (平均每秒包数)	avg_bpp (平均每秒流里)
484	573.72K	3.13K	106.59K	71	187
IP	Flows	Bytes (总字节数)	Packets (总包数)	avg_pps (平均每秒包数)	avg_bps (平均每秒流里)
192.168.88.25	146 30.2%	230.02K 40.1%	1.02K 32.4%	31.41K	
192.168.88.14	11 2.3%	120.55K 21.0%	192 6.1%	16.46K	
192.168.88.5	110 22.7%	45.16K 7.9%	536 17.1%	6.17K	
183.60.1.149	6 1.2%	44.23K 7.7%	152 4.9%	6.04K	
192.168.88.36	50 10.3%	36.65K 6.4%	294 9.4%	5K	
192.168.88.26	29 6.0%	21.85K 3.8%	303 9.7%	2.98K	
192.168.88.37	31 6.4%	20.93K 3.6%	165 5.3%	2.86K	
192.168.88.7	12 2.5%	9.85K 1.7%	82 2.6%	1.34K	
192.168.88.28	6 1.2%	9.8K 1.7%	92 2.9%	1.34K	
192.168.1.252	6 1.2%	6.09K 1.1%	36 1.1%	832	
192.168.18.2	5 1.0%	4.48K 0.8%	58 1.9%	612	
38.105.23.21	2 0.4%	3.45K 0.6%	32 1.0%	470.93	

IP 流量分析 TOPN 列表

5.2 自动发现和智能向导配置

支持自动发现和扫描、智能向导、批量处理工具等方式，配置管理轻松自在。



The screenshot shows a configuration interface for automatic discovery and scanning. It consists of three steps: '第一步: 选择参数' (Step 1: Select Parameters), '第二步: 扫描' (Step 2: Scan), and '第三步: 保存结果' (Step 3: Save Results). The current step is Step 1.

IP地址列表： (IP Address List)

- 192.168.88.1-20
- 192.168.88.111
- 172.16.1.100-120

通用选项： (General Options)

- PING存活检测：
- 连接超时时间： 1

SNMP资源： (SNMP Resource)

- SNMP版本： 2
- 团体名称(只读)： *****
- 团体名称(读写)： *****

TCP端口： (TCP Port)

- 80
- 25
- 110
- 1433
- 3389

网络应用： (Network Application)

下一步 < 上一步

精确的自动发现和扫描功能

第一步: 选择类型 第二步: 基本信息 第三步: 检测参数 第四步: 报警参数

操作	名称	方式	描述
C	SNMP Informant系统资源	SNMP	通过SNMP Informant检测Windows系统的CPU、内存资源状态
C	\Windows磁盘IO	SNMP	\Windows系统的磁盘IO状态探测
C	\Windows磁盘利用率	WMI	通过Windows的WMI协议探测系统的磁盘资源情况
C	\Windows磁盘资源	SNMP	\Windows系统的磁盘资源状态探测
C	\Windows系统CPU利用率	WMI	通过Windows的WMI协议探测系统的CPU资源情况
C	\Windows系统服务	SNMP	\Windows系统服务状态监控
C	\Windows系统服务数统计	SNMP	\Windows活动的系统服务总数的统计与监控
C	\Windows系统进程	SNMP	\Windows系统进程状态监控
C	\Windows系统进程数统计	SNMP	\Windows系统进程总数的统计与监控
C	\Windows系统进程资源检测	WMI	通过Windows的WMI协议探测系统指定进程的CPU和内存资源情况
C	\Windows系统内存利用率	WMI	通过Windows的WMI协议探测系统的内存资源情况
C	\Windows系统资源	SNMP	\Windows系统的CPU、内存、虚拟内存资源状态探测
C	\Windows指定系统进程数统计	SNMP	\Windows指定系统进程数的统计与监控

< 上一步 下一步 >

丰富的智能向导

5.3 基于角色的分级权限管理

系统具有运营级别的基于角色分级权限管理能力，主要体现在：

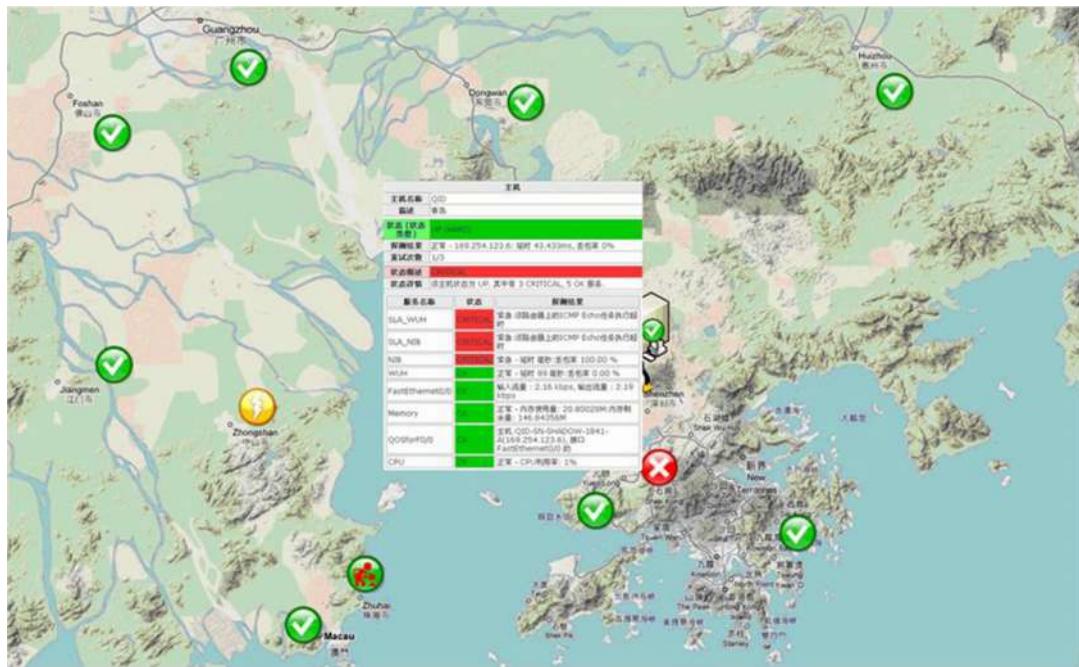
1. 可深入控制各帐号使用每个功能模块的读和写的能力，这些功能模块包括“设备和监测器 状态”、“拓扑图”、“日志”、“报表”、“帐号管理”、“设备和监测器管理”和“系统管理” 等。
2. 各帐号可关联到每个受监控管理的设备、监测器。
3. 各帐号均和设定独立的工作时间表，以及独立的告警设定。



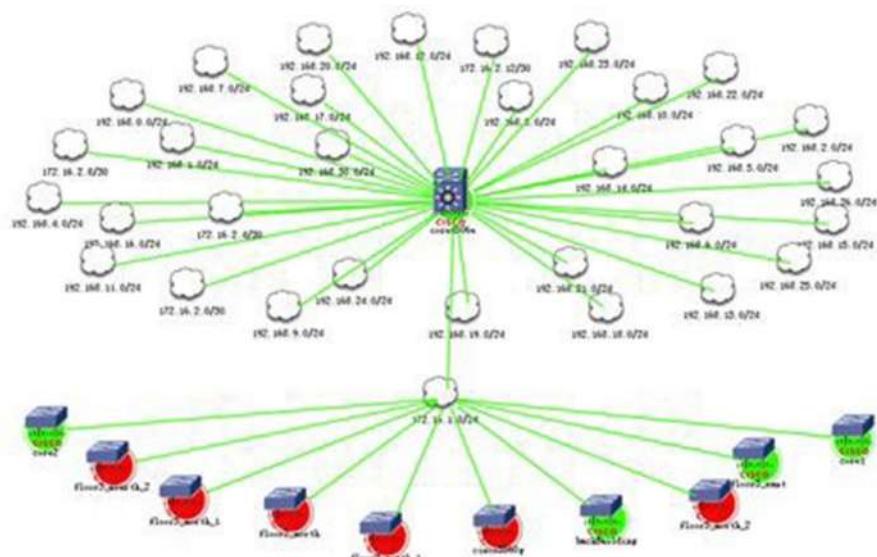
基于角色的权限定义

5.4 网络拓扑

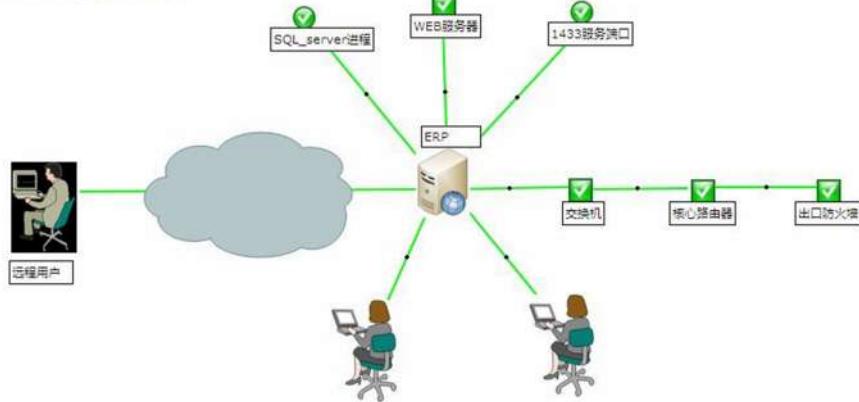
系统提供自由定义和绘制的网络拓扑功能，可进行无限的拓扑图分层，可导入 visio 生成的详细拓扑图或者真实的机房、机柜照片等。



企业网络区域监控图



ERP业务视图



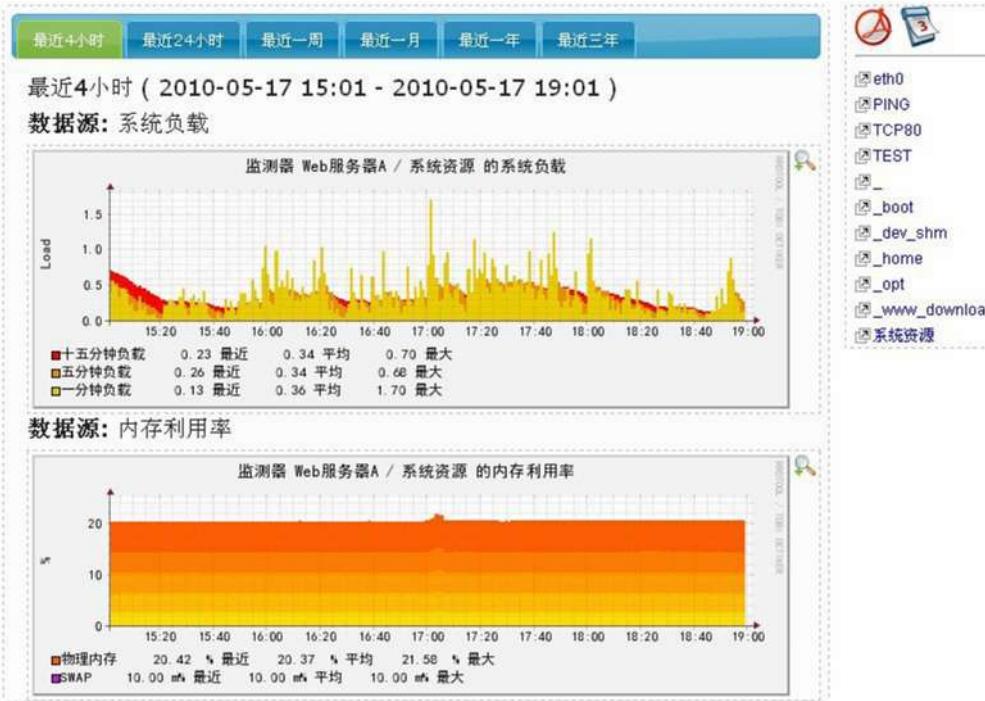
手动灵活定义拓扑



机柜真实照片监控图

5.5 历史记录和性能曲线

系统可提供每个监测器最长 10 年的监控历史性能曲线图，并可查询放大任意时间区间的历史曲线。管理员也可查询任意时刻的系统操作日志、监测器故障日志和告警日志。



性能曲线图

用户操作日志 故障日志 通知日志

时间范围: 2010-05-01 ~ 2010-05-17 刷新 清除

类型	用户IP地址	记录时间	描述
认证	192.168.88.4	2010-05-13 16:51:53	用户"admin"的活动会话十分钟超时, 强制注销
修改	192.168.88.5	2010-05-13 16:50:53	用户admin对监控系统的配置进行了激活保存
修改	192.168.88.5	2010-05-13 16:46:43	用户admin对监控系统的配置进行了激活保存
修改	192.168.88.5	2010-05-13 16:42:46	用户admin对监控系统的配置进行了激活保存
认证	192.168.88.4	2010-05-13 16:41:21	用户admin登录成功
修改	192.168.88.5	2010-05-13 16:41:08	用户admin对监控系统的配置进行了激活保存
添加	192.168.88.5	2010-05-13 16:40:54	用户admin添加了监测器"SMTP_SSL"
认证	192.168.88.4	2010-05-13 16:35:15	用户"admin"的活动会话十分钟超时, 强制注销
认证	192.168.88.4	2010-05-13 16:24:37	用户admin登录成功
认证	192.168.88.4	2010-05-13 16:21:59	用户"admin"的活动会话十分钟超时, 强制注销
类型	用户IP地址	记录时间	描述

用户操作日志查询结果

时间范围： 2010-05-01 - 2010-05-17 | 故障状态： 故障恢复(红色), 一级 | 刷新

监测器名	所属设备	时间	状态	状态信息
PING	R1-Cisco7200	2010-05-17 14:42:36	故障恢复(红色)	正常 - 192.168.88.31: 延时 189.275毫秒, 丢包率 0%
FastEthernet1/0	R1-Cisco7200	2010-05-17 14:42:36	故障恢复(绿色)	输入流量为0.14Mbps, 输出流量为0.14Mbps
FastEthernet0/0	R1-Cisco7200	2010-05-17 14:42:36	故障恢复(红色)	输入流量为0.14Mbps, 输出流量为0.14Mbps
系统资源	R1-Cisco7200	2010-05-17 14:42:36	故障恢复(红色)	最近CPU利用率: 五秒 0%, 一分钟 0%, 五分钟 0%, 内存利用率: 32.31%(总大小: 69.52MB)
系统资源	R1-Cisco7200	2010-05-15 14:11:39	一级警告	错误: 连接30秒超时
FastEthernet1/0	R1-Cisco7200	2010-05-15 14:11:29	一级警告	错误: 连接30秒超时
FastEthernet0/0	R1-Cisco7200	2010-05-15 14:10:59	一级警告	错误: 连接30秒超时
FastEthernet0/0	R1-Cisco7200	2010-05-14 19:22:39	错误	错误: 目标主机无响应
FastEthernet1/0	R1-Cisco7200	2010-05-14 19:22:39	错误	错误: 目标主机无响应
系统资源	R1-Cisco7200	2010-05-14 19:22:09	错误	错误: 目标主机无响应
监测器名	所属设备	时间	状态	状态信息

1/18 10

指定设备的监测器故障日志查询结果

时间范围： 2010-05-01 - 2010-05-17 | 联系人： 123123(asdf), admin(管) | 通知方式： 邮件, 短信 | 状态： 发送成功, 发送 | 刷新

发送成功： 62

通知方式	联系人	状态	时间	监测器名	所属设备	信息内容
邮件	李某某	发送成功	2010-05-13 10:11:04	PING	R1-Cisco7200	监测器 R1-Cisco7200 PING 故障恢复 正常 监测器：PING 设备：R1-Cisco7200 设备IP：192.168.88.31 状态：正常 状态信息：正常 - 192.168.88.31: 主机不可达 @ 192.168.88.36. 丢包率 100% 时间：2010-05-13 10:11:04 备注：
邮件	李某某	发送成功	2010-05-10 11:27:30	PING	R1-Cisco7200	监测器 R1-Cisco7200 PING 故障恢复 正常 监测器：PING 设备：R1-Cisco7200 设备IP：192.168.88.31 状态：正常 状态信息：正常 - 192.168.88.31: 延时 149.231毫秒, 丢包率 0% 时间：2010-05-10 11:27:30 备注：
邮件	李某某	发送成功	2010-05-10 11:18:32	PING	R1-Cisco7200	监测器 R1-Cisco7200 PING 故障恢复 正常 监测器：PING 设备：R1-Cisco7200 设备IP：192.168.88.31 状态：正常 状态信息：正常 - 192.168.88.31: 主机不可达 @ 192.168.88.36. 丢包率 100% 时间：2010-05-10 11:18:32 备注：

指定设备的监测器告警记录日志查询结果

5.6 报表

内置强大的报表功能，能够基于设备、监测器、接口流量、设备存活率、设备性能、线路运行率进行灵活的自定义报表。自动生成日报、周报、月报、年报的历史报表，并可定时自动发送报表邮件。

系统可根据设备组、监测器组、设备所包含的监测器生成任意时间范围的可用性分析表，并针对每个监测器，生成详尽的可用性报告，包括故障趋势图、可用性列表和饼状图、历史曲线图、故障日志和告警记录日志。

可输出 HTML 和 EXCEL 格式报表，并可按用户要求定制报表内容。



The screenshot shows the Mate reporting interface. On the left, there's a sidebar with a tree view under '报表' (Reports) containing categories like '统计报表', '设备', '监测器' (selected), '接口流量', '设备存活率', '设备性能', and '线路运行率'. The main area has tabs at the top: '添加' (Add), '删除' (Delete), '应用' (Apply), '禁用' (Disable), '刷新' (Refresh), and '生成' (Generate). Below these tabs are two sections: '监测器统计报表' (Monitor Statistics Report) and '已生成的报表' (Generated Reports). The '监测器统计报表' section lists three items: '名称' (Name), '描述' (Description), '监测器数' (Number of Monitors), '时间段' (Time Range), '格式' (Format), '状态' (Status), and '操作' (Operations). The '已生成的报表' section lists 14 generated reports with columns for '格式' (Format), '标题' (Title), '时间段' (Time Range), '生成时间' (Generation Time), and '状态' (Status). Each report entry includes a small preview icon.

自动生成指定多个设备或设备组报表

LINUX日报						
2012-08-13 00:00:00至2012-08-14 00:00:00						
LINUX日报						
设备存活率						
设备名(IP)	正常(%)	一级警告(%)	二级警告(%)	错误(%)	未知(%)	总时长
Linux服务器 (192.168.88.26)	100%	0%	0%	0%	0%	24小时
localhost (localhost)	100%	0%	0%	0%	0%	24小时
Linux/Solaris系统资源						
设备名(IP)	类型	最大值	平均值	最小值	最近值	
Linux服务器 (192.168.88.26)	1分钟负载	0.79	0.20	0.00	0.04	
	5分钟负载	0.48	0.17	0.02	0.12	
	15分钟负载	0.31	0.14	0.07	0.12	
	内存利用率(%)	56.50	55.14	53.53	0.02	
	SWAP利用率(%)	6.78	6.78	6.78	6.78	
localhost (localhost)	1分钟负载	1.67	0.65	0.07	0.65	
	5分钟负载	1.06	0.61	0.22	0.65	
	15分钟负载	0.92	0.57	0.24	0.63	
	内存利用率(%)	53.28	49.33	47.25	0.22	
	SWAP利用率(%)	0.94	0.92	0.90	0.94	

报表部分详细内容

监测器名	所属设备	正常(%)	一级警告(%)	二级警告(%)	错误(%)	未知(%)	总时长
Q_boot	localhost	100%	0%	0%	0%	0%	16时7分52秒
Q_Mysql数据库流量	localhost	100%	0%	0%	0%	0%	16时7分5秒
Q_Mysql内存空间利用率	localhost	100%	0%	0%	0%	0%	16时7分48秒
Q_Mysql连接数	localhost	100%	0%	0%	0%	0%	16时6分36秒
Q_PING	localhost	100%	0%	0%	0%	0%	16时6分38秒
Q_TCP80	localhost	100%	0%	0%	0%	0%	16时8分22秒
Q_eth0	localhost	100%	0%	0%	0%	0%	16时7分52秒
Q_http	localhost	100%	0%	0%	0%	0%	16时7分58秒
Q_http连接数	localhost	100%	0%	0%	0%	0%	16时6分30秒
Q_早八点开机	Develop1	100%	0%	0%	0%	0%	88时30分0秒
Q_系统资源	localhost	100%	0%	0%	0%	0%	16时7分34秒
Q_PING	Develop1	49.72%	0%	100.00%	0%	0%	16时8分18秒
Q_TCP80	Develop1	49.71%	0%	100.00%	0%	0%	16时8分27秒
Q_eth0	WEB服务器B	49.69%	0%	100.00%	0%	0%	16时7分43秒
Q_http	Develop1	49.68%	0%	100.00%	0%	0%	16时8分13秒

指定设备包含的监测器可用性分析表

5.7 资产管理

资产管理功能，可以对公司固定资产、无形资产、合同管理等进行手动添加建立资产档案。 并可对需要进行定时提醒的任务，设置短信或邮件进行提醒。

资产列表										
ID	名称	类型	负责人	位置	供应商	型号	序列号	资产编号	备注	操作
1	联想服务器	固定资产	admin (管理员1)	深圳	集成商	联想-万全R520	123	456	联想万全R520 G7 S5606 4G/1TSN	
4	电信专线	合同管理	admin (管理员1)	深圳	中国电信	none	10000	10000	中国电信专线	
5	飞思网巡	固定资产	admin (管理员1)	深圳	飞思安诺	飞思网巡-1000型	008	1000	IT运维网管系统。	
6	格力空调	固定资产	admin (管理员1)	深圳	集成商	none	SNFS009	1001	格力机房专用空调，5P。	

资产列表

资产列表								
ID	名称	状态	通知时间	联系组	关联资产	备注	操作	
1	专线到期	未完成	2013-07-01 10:00:00	admins (管理员组)	电信专线	专线到期		
2	空调定期检查	未完成	2013-08-01 10:00:00	admins (管理员组)	格力空调	空调定期检查		
3	软件升级	未完成	2012-12-01 10:00:00	admins (管理员组)	飞思网巡	统一版本升级。		

自动提醒任务

6 产品特点

6.1 领先的全硬件产品方案

硬件产品与软件产品的比较：

	硬件产品	软件
安装	旁路接入交换机，“即插即用”。	需要比较复杂的过程： 1. 准备好服务器及 windows 操作系统、数据库软件光盘； 2. 安装操作系统； 3. 安装数据库软件； 4. 安装网管程序。 安装过程中可能会碰到兼容性问题。
维护	网络安全设备级别的可靠性，故障率低。出现故障时直接使用备机或由厂家维修更换硬件设备即可。	1. 一两个月要重启一次。网管系统本身是用来监控关键设备和服务器的，但自身不具有足够的可靠性保证报警准确和及时。 2. 出现故障时，要先判断是网管程序、数据库软件、操作系统那方面出现问题，然后找对应的厂家。故障点不容易判断时更无从入手； 3. 系统极易感染病毒，要重新安装一遍。

6.2 更高效和安全

高效和模块化的核心程序：

	本产品	其他产品
采集间隔	秒级。最低为 1 秒的数据采集间隔。	最小采集间隔为 1 分钟或以上。一般把缺省值设定在 5 分钟或更高。
预警	快而准。对要求严格的监控目标，通过进行秒级的采集间隔设定，能迅速对故障进行反应，执行预警动作。	慢。不适用于要求严格的环境。

6.3 对网络和目标影响极低

系统以对带宽占用低、目标网络设备、服务器等性能占用接近零为设计原则，数据采集程序进行特别优化。在满足监控所需数据的情况下，不占用任何额外的带宽，以及对目标的访问。

这差别于以追求最大限度展示图形和实时面板的软件系统，这些都牺牲网络中大量的带宽以及服务器性能。

6.4 易于定制扩展

模块化的系统框架，让系统定制支持能力更强，对个性化的需求快速响应。