(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114244676 A
(43)申请公布日 2022.03.25

(21)申请号 202111273144.0

(22)申请日 2021.10.29

(71)申请人 四川天翼网络服务有限公司
地址 610041 四川省成都市高新区九兴大道10号三楼

(72)发明人 巫明金 邓雄

(74)专利代理机构 成都金英专利代理事务所(普通合伙) 51218
代理人 袁英

(51)Int.Cl.
H04L 41/0213(2022.01)
H04L 41/0604(2022.01)
H04L 41/14(2022.01)
H04L 41/28(2022.01)
H04L 43/045(2022.01)
H04L 43/0817(2022.01)
H04L 12/66(2006.01)
H04L 9/40(2022.01)

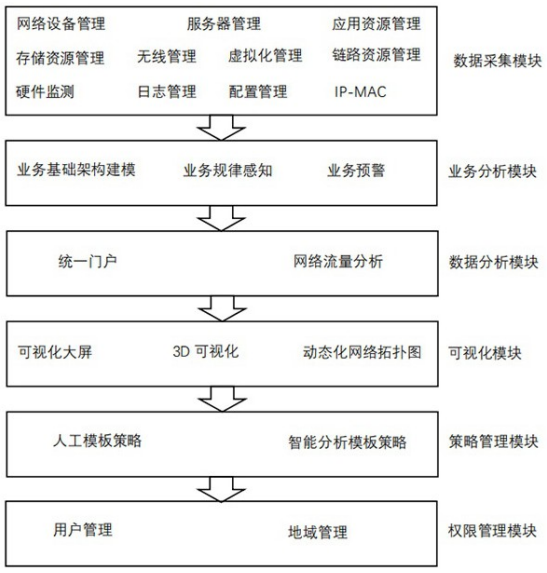
权利要求书1页 说明书9页 附图1页

(54)发明名称

一种智能IT综合网关系统

(57)摘要

本发明公开了一种智能IT综合网关系统，包括：数据采集模块：用以采集远程监测设备数据信息；业务分析模块：用以帮助用户实现业务监控，辅助用户执行业务管理；数据分析模块：将采集到的远程监测设备数据信息进行环比分析或图形趋势分析；可视化模块：用以对远程监测设备、运行情况和故障情况进行可视化展示；策略管理模块：用以控制远程监测设备的取值方式、取值周期、取值指标、阈值和告警方式；权限管理模块：用以提供各种角色的权限管理，至少包括运维管理员、一般用户、值班人员、技术人员、领导及系统管理员。本发明可对用户系统中的各部件各环节进行无漏洞的全方位监测，提高系统可利用率，优化系统配置，节省投资成本。



CN 114244676 A

1.一种智能IT综合网关系统,其特征在于,包括:

数据采集模块:用以采集远程监测设备数据信息;

业务分析模块:用以帮助用户实现业务监控,辅助用户执行业务管理;

数据分析模块:将采集到的远程监测设备数据信息进行环比分析或图形趋势分析;

可视化模块:用以对远程监测设备、运行情况和故障情况进行可视化展示;

策略管理模块:用以控制远程监测设备的取值方式、取值周期、取值指标、阈值和告警方式;

权限管理模块:用以提供各种角色的权限管理,至少包括运维管理员、一般用户、值班人员、技术人员、领导及系统管理员。

2. 如权利要求1所述的一种智能IT综合网关系统,其特征在于,所述数据采集模块包括网络设备管理、服务器管理、应用资源管理、存储资源管理、无线管理、虚拟化管理和链路资源管理,所述网络设备管理对符合SNMP标准协议的交换机、路由器、防火墙和均衡负载的网络设备进行监控和管理;所述服务器管理实现对服务器性能的监控以及性能分析;所述应用资源管理对数据库进行监控和管理;所述存储资源管理兼容不同厂商设备,实现集中式管理;所述无线管理实现对网络中AC、FAT AP、FIT AP和移动终端的一体化集中管理;所述虚拟化管理全面展示虚拟主机的整体运行情况、实时信息、异常信息、日志管理、硬件状态信息、资源分配以及子虚拟机服务器的运行指标的监控;所述链路资源管理通过多种告警方式及时通知运维管理人员。

3.如权利要求1或2所述的一种智能IT综合网关系统,其特征在于,所述数据采集模块还包括硬件监测、日志管理和配置管理,所述硬件监测通过IPMI、SSH、TELNET和/或ILO实现服务器的硬件底层监测;所述日志管理通过syslog、trap和文件的方式对网络设备、服务器和应用的日志信息进行统一收集并展示;所述配置管理通过TFTP、SNMP、TELNET或SSH协议进行配置取值。

4.如权利要求1所述的一种智能IT综合网关系统,其特征在于,所述业务分析模块包括业务基础架构建模、业务规律感知和业务预警,所述业务基础架构建模将业务服务及承载业务的IT基础设施构建成真实的业务模型,立体化监控与分析;所述业务规律感知实现自动判断业务系统接口的通信端口和通信规律,支持滑动窗口式规律自适应,智能过滤噪点数据,定制多套学习规律,自动调节最优发现方式;业务预警根据流量特性,进行网络上ARP风暴、DOS攻击行为、网络扫描行为或蠕虫病毒发散的常见异常行为检测,发现问题时,可至少通过email、短信和微信发出通知。

5.如权利要求1所述的一种智能IT综合网关系统,其特征在于,所述可视化模块包括可视化大屏、3D可视化和动态化网络拓扑图,所述可视化大屏基于H5实现大屏展示功能,支持将监控到的设备通过自定义的方式展示到大屏页面上,通过仪表盘和/或进度条的方式实现对设备的可视化展示;所述3D可视化至少提供三维可视化漫游、展示和操作;所述动态化网络拓扑图通过H5技术实现。

6.如权利要求1所述的一种智能IT综合网关系统,其特征在于,所述策略管理模块包括人工模板策略和智能分析模板策略。

7.如权利要求1所述的一种智能IT综合网关系统,其特征在于,所述权限管理模块包括用户管理和地域管理。

一种智能IT综合网关系统

技术领域

[0001] 本发明涉及远程监控技术领域，尤其涉及一种智能IT综合网关系统。

背景技术

[0002] 随着社会的快速发展，视频监控已深入各个领域，城市视频监控系统具有设备与资源规模巨大、设备种类庞杂、参与维护的人员众多的特点，单纯依靠传统的人工作业方式来进行日常巡检和维护管理，将难以保证整个系统的高可用性，如类似摄像机损坏、停电或电路故障、传输网络阻断、视频图像丢失、服务器故障、存储设备部件损坏、网络不稳定等，完全靠人工检测发现，不仅工作量巨大，技术上也是非常困难的。上述监测和控制通过中心平台软件方式无法实现，需要在前端现场加装智能硬件设备，远程维护机器人(Smart Diagnostic Terminal，以下简称SDT)，能够实现这些诉求，它自带电源与网络，独立于监控系统运行，支持RJ45有线传输，同时可选配运营商的4G/物联网无线通讯功能模块与后端平台进行数据链接，可用于对前端硬件设备的实时检测。

[0003] 视频监控系统往往包含成千上万个监控前端设备、大量的接入和分发节点、平台服务器群组、以及大量显示设备。视频监控的故障可能会由于任意的设备引起。当前端设备出现故障时虽然不会影响全局，但在实战中由故障引起的证据缺失往往会造成重大损失，而在传统的视频监控系统中采用的人工巡检方式在面对大量监控设备时显得力不从心，不仅对人员和设备的数量要求高，而且实时性、准确率也不能满足实战需求，因此前端设备故障的主动识别对于大型网络视频监控系统尤为重要。当平台设备出现故障时如果不能及时发现和处理将会影响整个系统的运行，严重时可能导致系统瘫痪，因此对故障识别的预防、主动识别、故障处理机制的能力都提出了非常高的要求。

发明内容

[0004] 为了解决上述问题，本发明提供了一种智能IT综合网关系统，旨在为客户提供全面IT运维整合服务，本系统集网络设备、服务器、数据库、中间件、安全设备、虚拟机集群、存储、视频设备、业务应用等各种软硬件实现一体化IT网络监控方案，打造IT网管软件产品的智能化运维、自动化管理的网管需求，提供全方面多纬度的IT网络运维管理平台整合服务。同时遵循ITIL标准，便捷的IT运维流程处理模式简化事件处理流程，提高IT运维管理水平。

[0005] 本发明所提供的一种智能IT综合网关系统包括：

数据采集模块：用以采集远程监测设备数据信息；

业务分析模块：用以帮助用户实现业务监控，辅助用户执行业务管理；

数据分析模块：将采集到的远程监测设备数据信息进行环比分析或图形趋势分析；

可视化模块：用以对远程监测设备、运行情况和故障情况进行可视化展示；

策略管理模块：用以控制远程监测设备的取值方式、取值周期、取值指标、阈值和告警方式；

权限管理模块:用以提供各种角色的权限管理,至少包括运维管理员、一般用户、值班人员、技术人员、领导及系统管理员。

[0006] 进一步的,所述数据采集模块包括网络设备管理、服务器管理、应用资源管理、存储资源管理、无线管理、虚拟化管理和链路资源管理,所述网络设备管理对符合SNMP标准协议的交换机、路由器、防火墙和均衡负载的网络设备进行监控和管理;所述服务器管理实现对服务器性能的监控以及性能分析;所述应用资源管理对数据库进行监控和管理;所述存储资源管理兼容不同厂商设备,实现集中式管理;所述无线管理实现对网络中AC、FAT AP、FIT AP和移动终端的一体化集中管理;所述虚拟化管理全面展示虚拟主机的整体运行情况、实时信息、异常信息、日志管理、硬件状态信息、资源分配以及子虚拟机服务器的运行指标的监控;所述链路资源管理通过多种告警方式及时通知运维管理人员。

[0007] 进一步的,所述数据采集模块还包括硬件监测、日志管理和配置管理,所述硬件监测通过IPMI、SSH、TELNET和/或ILO实现服务器的硬件底层监测;所述日志管理通过syslog、trap和文件的方式对网络设备、服务器和应用的日志信息进行统一收集并展示;所述配置管理通过TFTP、SNMP、TELNET或SSH协议进行配置取值。

[0008] 进一步的,所述业务分析模块包括业务基础架构建模、业务规律感知和业务预警,所述业务基础架构建模将业务服务及承载业务的IT基础设施构建成真实的业务模型,立体化监控与分析;所述业务规律感知实现自动判断业务系统接口的通信端口和通信规律,支持滑动窗口式规律自适应,智能过滤噪点数据,定制多套学习规律,自动调节最优发现方式;业务预警根据流量特性,进行网络上ARP风暴、DOS攻击行为、网络扫描行为或蠕虫病毒发散的常见异常行为检测,发现问题时,可至少通过email、短信和微信发出通知。

[0009] 进一步的,所述可视化模块包括可视化大屏、3D可视化和动态化网络拓扑图,所述可视化大屏基于H5实现大屏展示功能,支持将监控到的设备通过自定义的方式展示到大屏页面上,通过仪表盘和/或进度条的方式实现对设备的可视化展示;所述3D可视化至少提供三维可视化漫游、展示和操作;所述动态化网络拓扑图通过H5技术实现。

[0010] 进一步的,所述策略管理模块包括人工模板策略和智能分析模板策略。

[0011] 进一步的,所述权限管理模块包括用户管理和地域管理。

[0012] 本发明的有益效果在于:对用户系统中的各部件各环节进行无漏洞的全方位监测,对监测数据进行智能分析及可视化,提高系统可利用率,优化系统配置,节省投资成本。

附图说明

[0013] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图示出的结构获得其他的附图。

[0014] 图1为本发明系统框图。

具体实施方式

[0015] 应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0016] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完

整地描述，显然，所描述的实施例仅是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0017] 参阅图1，本发明提出了一种实施例：

一种智能IT综合网关系统，包括：

数据采集模块：用以采集远程监测设备数据信息；

业务分析模块：用以帮助用户实现业务监控，辅助用户执行业务管理；

数据分析模块：将采集到的远程监测设备数据信息进行环比分析或图形趋势分析；

可视化模块：用以对远程监测设备、运行情况和故障情况进行可视化展示；

策略管理模块：用以控制远程监测设备的取值方式、取值周期、取值指标、阈值和告警方式；

权限管理模块：用以提供各种角色的权限管理，至少包括运维管理员、一般用户、值班人员、技术人员、领导及系统管理员。

[0018] 具体的，所述远程监测设备采用远程维护机器人(Smart Diagnostic Terminal，以下简称SDT)，其自带电源与网络，独立于监控系统运行，支持RJ45有线传输，同时可选配运营商的4G/物联网无线通讯功能模块与后端平台进行数据链接，可用于对前端硬件设备的实时检测。该设备可实时监测电网设备箱等的多种电路、网络参数，判断故障点和远程控制，并能与维护平台进行通讯。同时预留多组GPIO接口，具有很强的扩展性，能满足不同环境下各种不同的需求。

[0019] 本发明所提出的一种智能IT综合网关系统专注于为客户提供全面IT运维整合服务。集网络设备、服务器、数据库、中间件、安全设备、虚拟机集群、存储、视频设备、业务应用等各种软硬件实现一体化IT网络监控方案，打造IT网管软件产品的智能化运维、自动化管理的网管需求，提供全方面多纬度的IT网络运维管理平台整合服务。同时遵循ITIL标准，便捷的IT运维流程处理模式简化事件处理流程，提高IT运维管理水平。

[0020] 具体的，所述数据采集模块包括网络设备管理、服务器管理、应用资源管理、存储资源管理、无线管理、虚拟化管理、链路资源管理、硬件监测、日志管理、配置管理和IP-MAC。

[0021] 具体的，所述网络设备管理能够对符合 SNMP 标准协议的交换机、路由器、防火墙、均衡负载等网络设备进行监控和管理，并能够自动发现网络设备间的链路和网络设备与计算机间的链路，能监测链路的上行、下行带宽利用率和速率、上行和下行的丢包率、错包率、链路连通状况。当进入某台网络设备可以查看到该设备的监控信息(基本信息、通断信息、其他指标、CMDB(基本信息、网络设备信息、配置信息、物理信息)、体验化(系统简况、CPU 信息、内存信息、背板、健康度折线图)等。可对网络设备的接口进行管理，自动区分并过滤 vlan 等虚拟接口。接口指标监控主要为接口名称、接口别名、连接设备、接口类型、、所属vlan、接口状态、接口容量、接口流出/流入速率、流入/流出利用率、流入/流出广播包等。可对网络设备的背版在系统中展现出来，对设备的网络接口和运行状况进行管理，并可实时分析接口流量、接口连接设备。

[0022] 具体的，所述服务器管理能够支持监控多种主流操作系统，包括linux 全系列版本、Windows Server 2003/2008/2012/2016 全系列版本、AIX、Solaris、HP unix、ScoUnix

等。监控服务器各种详细信息，如文件系统信息、系统日志信息、系统进程、系统版本信息；服务器运行指标：包括多个 CPU 中每个 CPU 的实时负载情况；物理内存、虚拟内存及页面文件的实时使用率；磁盘每个逻辑分区的分区容量；进程运行状态等；网卡实时连接及流量、网络端口的丢包率、利用率、发送速率等指标；系统支持通过自定义 SNMP OID 脚本，采集特殊的服务器特殊指标项。采用仪表盘图形方式实时显示主机服务器的CPU利用率、CPU使用情况、内存利用率、磁盘信息、进程信息的情况。提供对当前服务器各个性能的监控，并根据当前系统的运行情况，提供深入的性能分析。

[0023] 具体的，所述应用资源管理对用户的核心业务系统，包括运行在上述各种数据库进行有效的监控和管理，而且系统具有良好的可扩展性，能方便的支持其他数据库的管理。数据库管理的功能至少包括对数据库的表空间进行容量规划，并能够对表空间的使用情况进行定期分析和预警；实时监控当前数据库连接、监听器的管理并能够在连接数据库出现问题时发送消息到管理平台；对数据库的碎片情况进行监测；对 SQL 的执行效率进行分析；告警记录信息的采集和显示；数据库表空间和数据文件、回滚文件的管理、配置和监控；分类、环冲、共享池和事务处理性能的分析、监控和管理；索引性能和数据库锁的管理。

[0024] 在本实施例当中，对SQL Server 数据库的管理和监控，其中包括配置对 SQL Server 数据库的连接监控，配置对 SQL Server 数据库的 sql 语句的执行情况的监控，配置对 SQL Server 数据库的性能及其阀值的监控。一个SQL Server 数据库监视器实例能对数据库连接失败、执行 sql 语句失败、性能阀值越界产生报警事件。SQL Server监视器部分监视指标包括登录次数/秒：每秒登录 SQL Server 的次数的阀值；CPU 运算占用资源：SQL Server 数据库用于 CPU 运算占用资源的百分比的阀值；I/O 操作占用资源：SQL Server 数据库用于 I/O 操作占用资源的百分比的阀值；空闲资源：SQL Server 数据库空闲百分比的阀值。

[0025] 对Oracle 数据库的监控和管理，其中包括配置对 Oracle 数据库的连接监控，配置对 Oracle 数据库的 sql 语句的执行情况的监控，配置对 Oracle 数据库的性能及其阀值的监控。一个Oracle数据库监视器实例能对数据库连接失败、执行 sql 语句失败、性能阀值越界产生报警事件。

[0026] 在本实施例当中，J2EE 应用服务至少包括JBoss和/或Weblogic和/或WebSphere和/或Sun One和/或Oracle AS和/或Lotus Domino。

[0027] 具体的，所述存储资源管理兼容不同厂商的设备，实现集中式管理；使用拓扑、一体化页面等图形展现方式使运维工作简单化；深入监管各个关键对象，配合多种告警方式，实现主动式告警。有效提高存储管理运维的效率，保证业务数据的安全存储。支持通过SMI-S、SNMP协议、接口等多种方式，实现监控不同厂商的存储设备，实现集中式、可视化的管理，有效提高存储管理运维的效率，保证业务数据的安全存储。同时，存储监控能够全面覆盖FC-SAN网络中的不同设备类型，管理对象包括磁盘阵列、FC-交换机、HBA、线路等。这完全满足了对异构存储系统监控的需要。同时，对于现有的超融合、分布式等存储，也具备监测能力，实现对HP、Hitachi、IBM、SUN、EMC、DDN、昆腾等主流厂商型号存储设备的监控。通过图形化展现各类存储设备实时状态、对磁盘阵列、控制器、物理磁盘、主机、虚拟磁盘等详细信息各类KPI指标以及存储架构和其他IT基础架构的关联的关系。可深度支持磁盘阵列的各个组件，包括风扇、电源、电池、控制器、硬盘的状态、实时性能，以及交换机的各温度、电池、电

源传感器的状态监控，同时，提供二次开发服务，对于特殊的存储架构进行二次开发以满足用户对存储的监测需求，保障存储稳定安全运行。

[0028] 具体的，所述无线管理可以实现对于网络中的AC、FAT AP、FIT AP、移动终端等无线设备与有线设备进行一体化集中管理，解决无线网络环境复杂的情况下故障定位困难的问题，在网络拓扑中将有线、无线设备的统一展现，让管理人员直观看到网络故障点、性能负载、AP与POE交换机的流量信息等，使整网的运行状态一目了然。AP分布星图帮助工程师快速定位故障点，改变随机性的故障处理方式，计算地理位置的故障AP分布，有计划的进行设备维护。

[0029] 具体的，所述虚拟化管理支持vSphereAPI管理方式，即通过vCenter进行虚拟化的统一管理。全面展示虚拟主机的整体运行情况、实时信息、异常信息、日志管理、硬件状态信息、资源分配以及子虚拟机服务器的运行指标的监控。实现实时虚拟机监控、故障及时告警、性能数据分析，实现简单化管理，一个界面集中统一管理，包括虚拟机的CPU、MEM、磁盘使用率、流量使用情况等。

[0030] 具体的，所述链路资源管理：运维管理系统可以监控链路资源，并根据链路资源的属性设置阈值，判断当前链路状态等，并通过多种告警的方式及时通知运维管理人员。具体指标包括链路的容量、链路的上联和下联设备接口、链路状态、链路上/下行速率、链路上/下行利用率、链路的丢包率、链路的错报率、链路的包长和链路的总包数和丢包数。

[0031] 具体的，所述硬件监测通过IPMI、SSH、TELNET、ILO等方式实现服务器的硬件底层监测，同时包含刀片、刀箱的节点底层信息，包含风扇、内存、电源、温度、硬盘状态等指标，并可进行统一的预警。

[0032] 具体的，所述日志管理通过syslog、trap和文件的方式，对网络设备、服务器、应用的日志信息做统一收集并展示在系统里，且可根据关键字或者模型进行预警。

[0033] 具体的，所述配置管理通过TFTP、SNMP/TELNET/SSH等协议进行配置取值，配置管理是对网络设备的配置文件的自动管理。不仅可以自动定时的对配置文件进行备份以恢复到良好的网络环境，更能提供可靠的配置文件变动告警。当配置文件发生变化时，即使不在公司的网络管理人员都可以收到相应的告警来明确自己公司网络环境中可能面临的变化或危机。用天翼综合运维管理系统的配置管理功能能够为用户在灾难发生之前，对网络设备的配置文件进行备份、监控、预警，并支持在天翼界面中对网络设备配置文件进行修改保存恢复，极大地提高运维管理人员的工作效率，减少运维部门的经济损失和成本。

[0034] 具体的，所述IP-MAC：通过可以查看IP-MAC-PORT 3者之间的绑定关系，如 IP 地址与MAC 地址的关系，MAC 地域与交换机端口的关系，同时还能由 IP 地址查找到该 IP 的 MAC地域及该 IP 所连接的交换机端口。通过 IP-MAC-PORT3 者的绑定，可以查看基准表信息、实时表信息、实时表与基准表信息比较后的差异信息、差异处理信息等，并可以通过差异告警配置，对网络环境中出现的 IP 变更、新增终端及终端变更等异常进行告警，有助于用户及时掌握网络环境动态。

[0035] 具体的，所述业务分析模块包括业务基础架构建模、业务规律感知和业务预警。

[0036] 具体的，所述业务基础架构建模将业务服务及承载业务的IT基础设施构建成真实的业务模型；立体化监控与分析：下属资源、系统API及用户模拟。支持将监控到所有资源进行业务建模，根据相应的业务模型和相关的算法计算业务的健康度和繁忙度。面向业务服

务管理层面，立体化监控与分析以用户业务为导向，从IT管理更高的水平高度上，以直观、便捷的方式帮助用户实现对业务监控，辅助用户执行高效率、高质量的业务管理。业务建模系统可自动学习业务之间的规律与关系，也提供手动干预功能，可以人为指定。从而综合评价业务健康、繁忙度、可用性、资源占用，系统可将各个管理对象的指标作为评价基础，可以根据各个管理对象对于业务的影响，设置权重。支持评价基础指标作为预警阈值，在界面中以不同颜色图标显示，以示对业务的影响；支持业务健康度的实时动态更新；支持业务健康度低分原因的及时显示。提供手动创建业务架构图功能，也可根据业务架构自动构建的业务接口拓扑图，反映业务接口之间的关联关系，业务架构出现变更自动更新，无需手动调整，通过物理架构、逻辑架构、物理与逻辑结合架构方式真实反映出业务系统整体架构图。

[0037] 具体的，所述业务规律感知，配置有多套智能学习算法，主要实现自动判断业务系统接口的通信端口和通信规律，支持滑动窗口式规律自适应，智能过滤噪点数据，定制多套学习规律，自动调节最优发现方式。基于实时和历史数据的上下文快速关联分析，采用大数据提供智能化在线分析和模式匹配，实现业务周期规律性、内部指标之间关联性分析，使用统计学工具，和行为学知算法，揭示业务指标间的数学关系，核心算法包括行为学知和预测分析机制帮助诊断并规避服务中断；使用先进的沃森分析算法，针对单指标以及多指标分析；从整体观出发，通过自学习了解各IT元素是如何相互关联的；利用实时流分析技术，对异常情况提出预先报警提示。通过自动学习进行适配，无差别适用多类业务系统，覆盖全业务对象，提供整体性接口管理方案，支持评估业务的影响范围和重要性。

[0038] 以医院的PACS业务为例，当系统学习到，“业务响应时间”与“用户请求”有正相关因果关系，且随着用户负载增加而变慢。如果这一正常历史规律被破坏，比如说由于内存泄漏，造成即便用户请求数下降了，业务响应时间还很高，异常预警信号将立即发出。问题被发现，尽管这时业务服务质量仍处于“好”的区间。业务异常多种规律都可自学习与感知，除开上面举的例子之外，还有比较典型的业务的流量规律性异常、业务访问终端化异常等，都是常见的例子。业务流量规律性预测与监测，从每天的在不同时间轴的规律周期性、每周、每月、每年不同时间为周期进行分析与预警，同时可根据天到周，周到月的变化学习，去判断业务流量的异常情况，可提前预知告警，并且便于对业务流量整体的分析与预测。同时也让用户的业务模型更具有数据说服了，从不同的方面去评估整个业务的健康度与可用性，也是业务升级扩容的依据之一。

[0039] 具体的，所述业务预警以业务为视角进行业务预警，同时也可根据流量特性，进行网络上ARP风暴、DOS攻击行为、网络扫描行为、蠕虫病毒发散等常见异常行为检测，发现问题时，可至少通过email、短信、微信等多种方式发出通知。异常行为检测的规则库可持续更新，根据管理经验添加新规则。发现各通信规律的异常，智能判断规律异常。异常上报数量可控，异常数据准确偏差小，支持自适应弹性阈值，异常数据同时推动规律更新。

[0040] 具体的，所述数据分析模块包括统一门户和网络流量分析。

[0041] 具体的，所述统一门户可自定义门户组件内容、组件位置、组件大小，组件标题文字可编辑等，具备多门户界面，门户界面按用户及权限来区分，同一用户可创建多个门户界面，通过鼠标拖拽和移动即可实现门户的自由编辑。可为运维人员提供当前网络中的个人所关注的相关资源负载最高或最低的指标，如服务器 CPU、ICMP 响应时间、设备内存利用率、CPU 利用率、链路上行速率等 Top N排序的集中列表展现，并可对此 Top N 排序的资

源及指标进行自定义。通过此 Top N 列表可以及时了解当前网络的哪些资源负载比较高、使用比较多以及哪些资源负载比较低、使用比较少。从而帮助运维人员更合理的分配网络资源，提高网络资源利用率。使得运维人员能够在使用最少的成本的前提下，最有效的利用网络资源，做到物尽其用。

[0042] 具体的，所述网络流量分析对接口状态和流量的采集，包含输入输出速率、输入输出利用率等指标的采集，并可按照日、周、月、年进行环比分析。能监测链路的上行、下行带宽利用率和速率。可以实时统计分析每次轮询数据、30分钟统计、2小时统计、日统计等多种实时统计和数据保存，并可以生成日曲线、周曲线、月曲线、年曲线进行图形趋势分析。

[0043] 具体的，所述可视化模块包括可视化大屏、3D可视化和动态化网络拓扑图。

[0044] 具体的，所述可视化大屏：基于H5实现大屏展示功能，支持将监控到的设备通过自定义的方式展示到大屏页面上，通过仪表盘、进度条等多种方式实现对设备的可视化展示。并集成全网整体运行情况、故障情况等多种信息进行统一展示。支持将拓扑图展示到大屏上，并可将其他的任何网页集成到大屏做统一展示，不限制大屏的页面个数，页面进行自动的轮播。

[0045] 具体的，所述3D可视化基于B/S架构，采用H5技术开发，无需浏览器加载插件。为各级别的数据中心/电子信息系统机房和电子信息系统机房提供了全面而直观的三维可视化漫游、展示和智控操作，包含了环境可视化、动环监控可视化、资产管理可视化、容量管理可视化、管线管理可视化、IT运维管理可视化、告警可视化等多种类的可视化模块，通过将数据中心/电子信息系统机房内分散的多种专业监控系统、资产管理系统、运维流程管理系统进行深度整合，融合在构建数据中心/电子信息系统机房的3D全息图景中；建立统一监控、统一预警、统一资产管理以及统一空间规划，并提供规范化的系统管理流程；改变监控、数据孤岛现象，并保障机房运维过程有据可依；实现对数据中心/电子信息系统机房资产设备、资源设备运行参数和状况的全面监控和管理，提高数据信息的可读性和交互效率，以最大限度降低数据中心/电子信息系统机房运营成本、提高信息化管理能力、提高运维管理效率，让数据中心/电子信息系统机房管理人员看到更多，理解更多，掌控更多。支持W/A/S/D方向控制与鼠标左键角度控制，实现全场景漫游操作。双击可触发开机操作，双击设备可触发设备打开操作，完全模拟人物巡检视角。具备在线编辑功能，用户可以自定义在线绘制3D机房场景，用户可自定义机柜以及机柜里面的设备。设备数据可无缝对接监测到的设备数据，并可进行提示框进行展示。

[0046] 具体的，所述动态化网络拓扑图：系统支持全网自动发现，并自动生成网络拓扑图。基于H5技术实现的拓扑图功能。通过拓扑图模块用户能了解当前生产网络的整体运行情况，能自动生成真实物理拓扑图。

[0047] 进一步的，所述动态化网络拓扑图包括物理拓扑、示意拓扑和业务拓扑，所述物理拓扑可将企业用户网络环境中的各种可管理的网络设备、服务器等通过管理软件发现出来显示成一张物理拓扑图。同时在物理拓扑图上自动生成，我们可以真实的发现设备间的真实逻辑链路，通过用户快速的发现问题解决问题。当网络发现异常网管并用不同颜色来表示每个资源的异常等级状况，从而帮助判断异常的轻重缓急。真正帮助整体感知整个网络的健康状况，实时监测网络资源的性能，将最复杂的网络状况清晰展现。根据发现的网原能够自动构建的拓扑图，当然也可以手动添加或修改拓扑图及策略。所述示意拓扑可将个人

所关注或需要监控的实际网络环境与应用通过增加示意图元、示意链路的方式。所述业务拓扑可将企业用户各项业务以及承载这些业务的各种网络设备、服务器、应用等有机的组织在一起，同时对于每个业务系统能自定义各项业务拓扑图。不仅真实准确的反映实际物理链接、逻辑链接，于业务拓扑上实时动态展现业务系统及其各个下属资源健康度、平均CPU利用率、内存利用率及 ICMP 响应时间等运行情况，并用不同颜色来表示每个资源的异常等级状况。真正帮助您整体感知个人所关心业务的健康状况，实时监测业务组成部分的性能，全局上帮助您实时掌握整体网络运行状况，将最复杂的网络状况以最简明、直观的方式呈现。

[0048] 具体的，所述策略管理模块包括人工模板策略和智能分析模板策略。

[0049] 具体的，所述人工模板策略是资源对象的开关，控制资源的取值方式、取值周期、取值指标、阈值、告警方式等系统的控制层面都可由模板完成。

[0050] 具体的，智能分析模板策略：由于配置多种智能模板，阈值动态调整，无需人为调整，包括故障周期分析：实时汇总分析历史上指标告警发生的分钟、小时、每周和每月中隐藏的规律。例如某应用端口Down固定发生在每天早上6点到6点半之间，且每周、每月内发生频率均衡分布；例如某Web容器线程池使用率在下午3-4点通常会到达99%，早上9点前及晚上8点后从未发生，且每周一到周三发生频率最高，周四到周日负载逐级下降。故障根源分析：指标告警发生时，可以实时分析影响它的相关软硬件及性能指标，并找出与其同时告警的指标关联关系，故障根源一目了然。指标相关性分析：实时分析指标告警发生前后，与它运行趋势相同的强相关指标对比的轨迹变化。指标关联组分析：实时分析并展示历史上多次出现同时告警的成组关联指标。

[0051] 本发明还包括巡检管理模块，智能巡检是一个综合的智能巡检应用平台，实现了无纸化数据采集、实时上传，任务自动激活，实现了巡检管理的数字化、信息化、规范化、智能化，有效的降低人为因素带来的漏检或错检等问题，最大程度提高工作效率，为巡检管理工作提供了科学的手段。

[0052] 具体的，权限管理模块提供各种角色的权限管理，如运维管理员、一般用户、值班人员、技术人员、领导及系统管理员等，可以通过系统的各个管理模块对 IT 资源进行哪些操作，即规定了不同角色对视频资源的操作权限。系统可以把不同资源分为不同管理域，对不同的功能，给不同的角色分配不同的权限；同时给不同用户分配不同的角色以及不同的地域。通过立体化多维化的地域和权限管理，构建智能化的权限和视图管理，并保证高效管理和严密权限相结合。同时，系统建立独立redis用户中心，方便和其他系统的用户密码统一管理。包括用户管理和地域管理。

[0053] 具体的，所述用户管理提供用户对登陆系统账号的设备操作，用户可以对账号进行部门分组、查看用户账号、修改用户账号的信息，配置使用模块的权限以区别用户身份。对于不同的用户可以设置不同的用户地域权限和用户角色的权限，确保了整套系统的安全。

[0054] 具体的，所述地域管理帮助用户筛选设备，并可以做到管理域。地域管理和角色管理结合起来，可以实现立体的权限管理。系统将不同的IT资源按照不同的地域进行划分，地域权限管理功能可以让不同角色的人登陆到系统后只能看到与其地域有关的关联信息，并约束以上不同角色能够管理到哪些区域或范围内的资源，即规定了不同角色对地域的管理

权限。通过角色与地域权限立体化的管理，能够帮助企业用户对各种角色的运维人员做到责权分明。

[0055] 本发明还包括运维工具，本系统集成了常用的网络诊断和分析工具，其中包括ping 、telnet、ssh、TraceRoute、IP在线检测、SNMP 连接测试、实时表查询、Mibbrowser，使管理员无需脱离本系统的操作界面，即可对一些常见的网络故障进行诊断和排除，并更加方便的分析网络运行情况。另外，系统还提供简单易用的 MIB 查看工具，通过这个工具可以便于查看设备的 MIB 信息，并可以设置 TRAP，对关心的数据进行采集整理。

[0056] 本发明还可包括报表和分析模块，提供网络设备、链路、服务器、应用及业务等多种类型的日、周、月、季及年报表，并可以根据不同的关注点和时间段将所关注的各种类型的资源项及其指标项灵活添加至报表内容中。用户可以自定义报表模板，并提供一系列内建模板供用户选择。用户也可以自定义报表周期，如：日/周/月/年报表。系统通过手动或自动定时的方式发布，对于发布所形成报表的具体内容可以进行查看与配置，报表以柱状图、表格等形式灵活展现，且支持打印，以EXCEL 和 PDF 格式的导出便于发布和提交。

[0057] 本发明还可包括故障管理模块，显示网络中所有资源的异常信息，用户在该模块中可以查看、确认、删除异常信息。对所有的异常还可以按时间和关键字进行查询。

[0058] 本发明还可包括云预警平台，用户只需关注预警云平台，在系统规则库与预警云平台后端做数据绑定，严格控制平台权限，精确推荐预警，不增加用户成本，实现随时随地接受预警通知。同时支持客户端、短信、邮件等其它告警方式。

[0059] 本发明还可包括移动端运维模块，支持手机浏览器即可访问系统，并能够自动适应手屏幕，包括首页和告警模块，首页需要展示资源的运行情况，包含网络设备、服务器、存储、虚拟化的整体运行情况，以不同颜色区分、健康、亚健康、不可用设备。展开资源类型，以列表形式展现资源，并可点击查看资源的具体运行情况。通过故障页面即可接收到所有的故障信息。即不需要在安装APP的情况下即可实现手机端运维。

[0060] 需要说明的是，对于前述的实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某一些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本申请所必须的。

[0061] 上述实施例中，描述了本发明的基本原理和主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的只是说明本发明的原理，在不脱离本发明精神和范围的前提下，本领域人员所进行的改动和变化不脱离本发明的精神和范围，则都应在本发明所附权利要求的保护范围内。

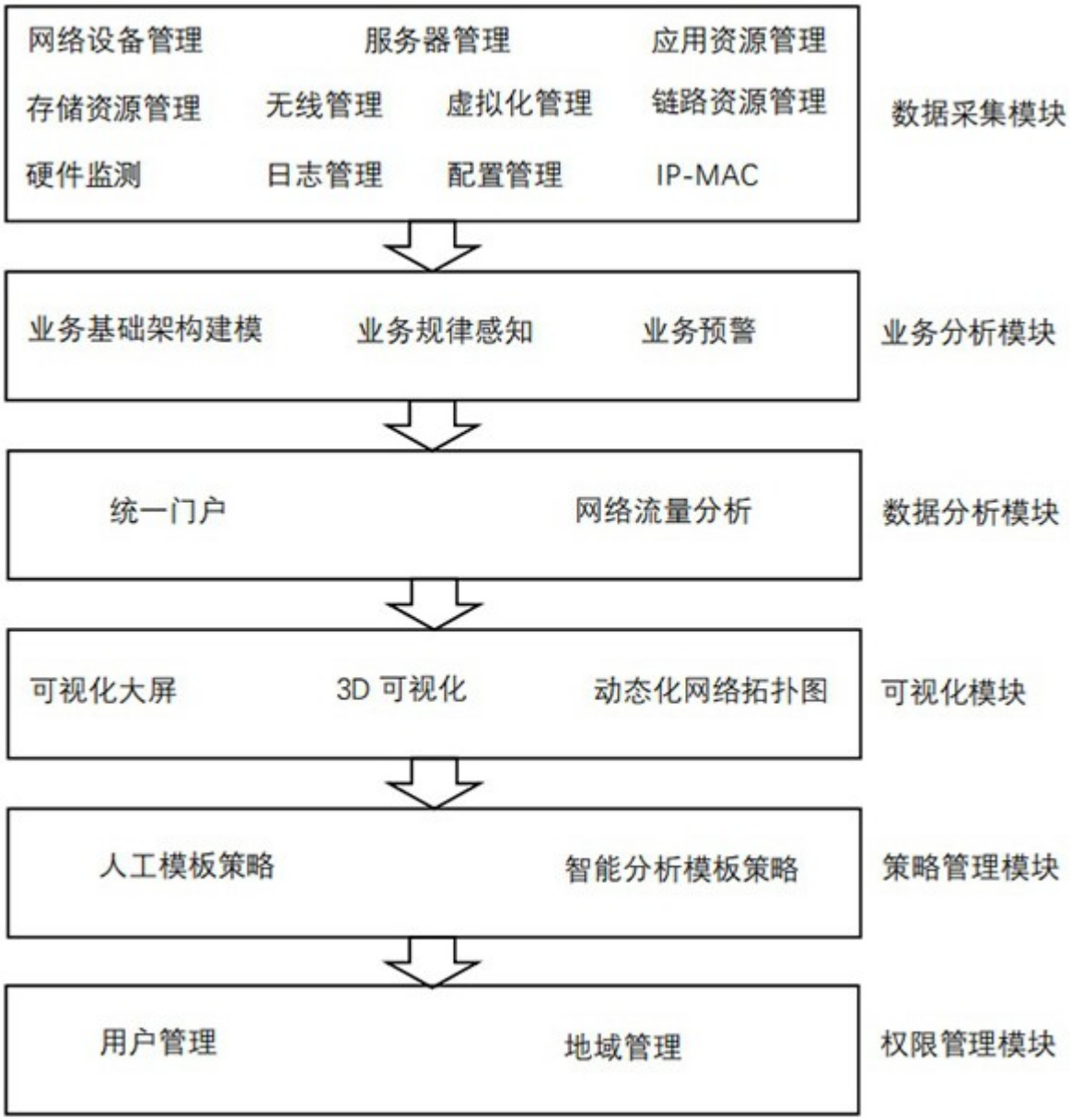

网络设备管理
服务器管理
应用资源管理
存储资源管理
无线管理
虚拟化管理
链路资源管理
硬件监测
日志管理
配置管理
IP-MAC
数据采集模块
业务基础架构建模
业务规律感知
业务预警
业务分析模块
统一门户
网络流量分析
数据分析模块
可视化大屏
3D 可视化
动态化网络拓扑图
可视化模块
人工模板策略
智能分析模板策略
策略管理模块
用户管理
地域管理
权限管理模块

图1