华汇数据中心运维管理平台 8.3

技术白皮书

HUAHUI DATA SERVICES

深圳市华汇数据服务有限公司

网址：http://wwww.hhdata.net.cn 电话：0755-88917993

目录

1 前言

随着企业业务信息化程度的不断提高，IT 基础设施规模变得日益庞大，涉及技术也日趋繁杂，故障诊断和恢复变得越来越困难，一般企业难以配备更多专业技术人员来应对这一局面。因此，提高 IT 基础设施运行维护自动化程度，实现 IT 基础设施自动巡检和实时监控已经变得非常迫切。

数据中心运维管理平台（以后简称 DCOM）是一款高效实用的 IT 基础设施监控管理产品。它通过对企业 IT 基础设施定期自动巡检，帮助企业轻松应对 IT 基础设施运维面临的压力和挑战，有效保障企业 IT 系统稳定可靠的运行。

本白皮书主要介绍 DCOM 产品架构、功能特性、关键技术和客户价值。

2 产品概述

IT 基础设施包括网络、硬件设备和基础软件，是企业所有信息系统的基础，它为组织业务系统正常运行提供可靠的支撑服务，IT 基础设施能力与健康是决定企业业务能否能够保持持续可用的关键所在。

DCOM 通过对企业 IT 基础设施的全面自动化巡检和监控，帮助 IT 运维人员实时了解 IT 基础设施健康状况，提前发现故障隐患，真正做到防患于未然，从而保障企业业务系统持续健康稳定运行。

DCOM 监控范围包括网络、服务器、存储以及操作系统、数据库和中间件等基础软件。通过实施 DCOM，可有效提高了企业 IT 运维自动化水平，降低 IT 运营成本，帮助 IT 运维人员从日常繁重事务性中解脱出来，有利于企业将资源集中到组织核心业务服务上，从而增强企业核心竞争力和对环境应变能力。

3 产品架构

3.1 功能架构

系统功能架构如 1 图所示，分为监控对象、采集层、分析处理层和综合展现层。各层功能和目标描述如下：

- **监控对象**

  系统支持网络设备、基础硬件、系统、应用和用户端。

- **数据采集层**

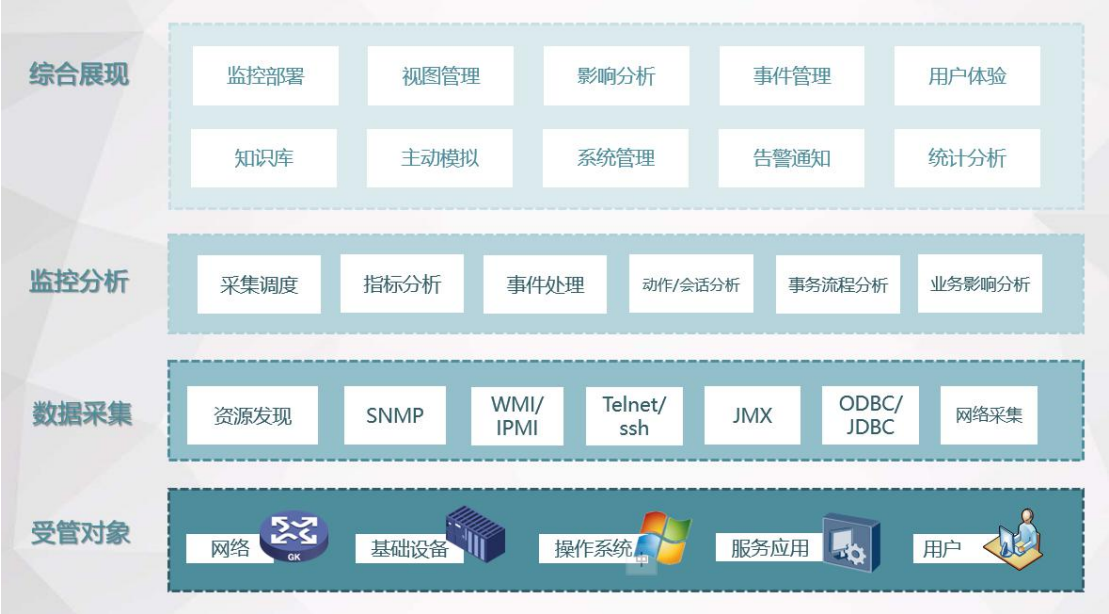
采集分析层主要通过多种协议，对监控对象进行数据采集和初步的信息处理，然后将规范化的信息上报到分析处理层。

- **分析处理层**

实现受管对象的信息采集、分析和告警等功能，目标是能够全面及时地发现各种 IT 故障和问题隐患。事件处理主要实现事件的汇聚，过滤、压制和处理，并且提供事件处理“微流程”，对没有实施流程管理的组织，运维人员可在事件控制台对事件进行确认、派工、处理和关闭等操作。

- **结果展现层**

结果展现层主要实现监控结果的统计分析和展现，其目标是帮助运维部门能够实时了解企业业务和其所依赖 IT 资源的运行状况，以及提供系统运维和优化的指示和依据。



图表 1 系统功能架构

3.2 技术架构

DCOM 采用 B/S 技术架构，操作系统采用 Linux，WEB 服务器采用 Apache，数据库采用 Mysql。

3.3 部署架构

系统部署架构如图 2 所示，下面分别说明。

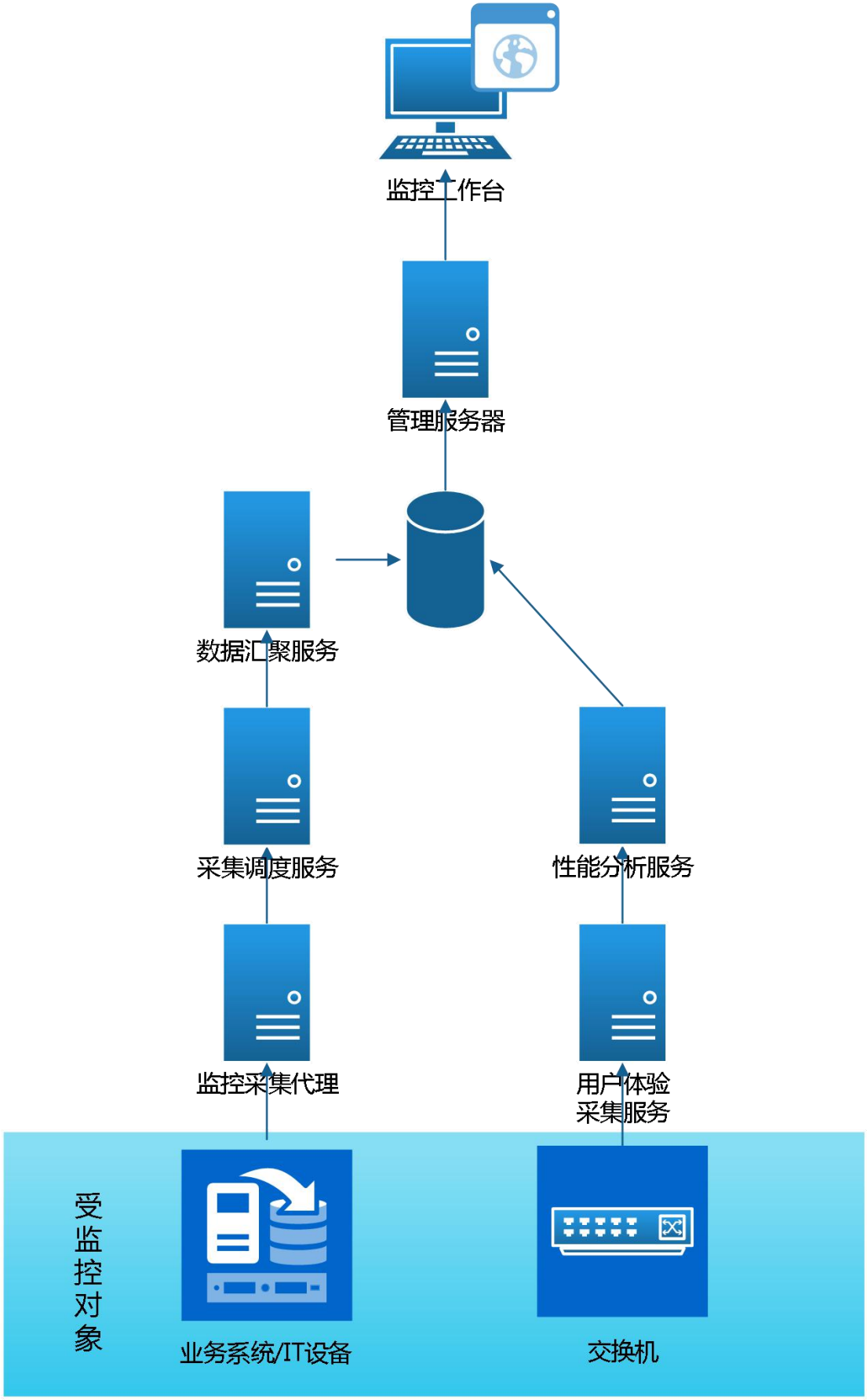
代理（Agent）:Agent 位于被监控对象宿主机上，它负责接收监控服务器（MON）发出的采集调度命令，执行采集插件，并将采集结果返回给 MON。系统也支持无代理方式，通过通用的接口进行数据采集。

监控服务器（MON）：MON 负责采集任务调度和采集结果分析，并将分析结果（指标）上报给汇聚服务器。

汇聚服务器（DAS）：汇聚服务器承担指标和事件（包括第三方监控系统输出的事件）汇聚和入库、事件分析处理、服务影响计算和告警信息推送等功能。

数据库（DB）：MYSQL 8。

管理服务器（MS）：主要负责系统统一认证与权限管理、资源模型管理、监控部署与监控策略下发、监控结果呈现和分析。


监控工作台
管理服务器
数据汇聚服务
采集调度服务
性能分析服务
监控采集代理
用户体验
采集服务
受监控对象
业务系统/IT设备
交换机

图表 2 系统部署架构

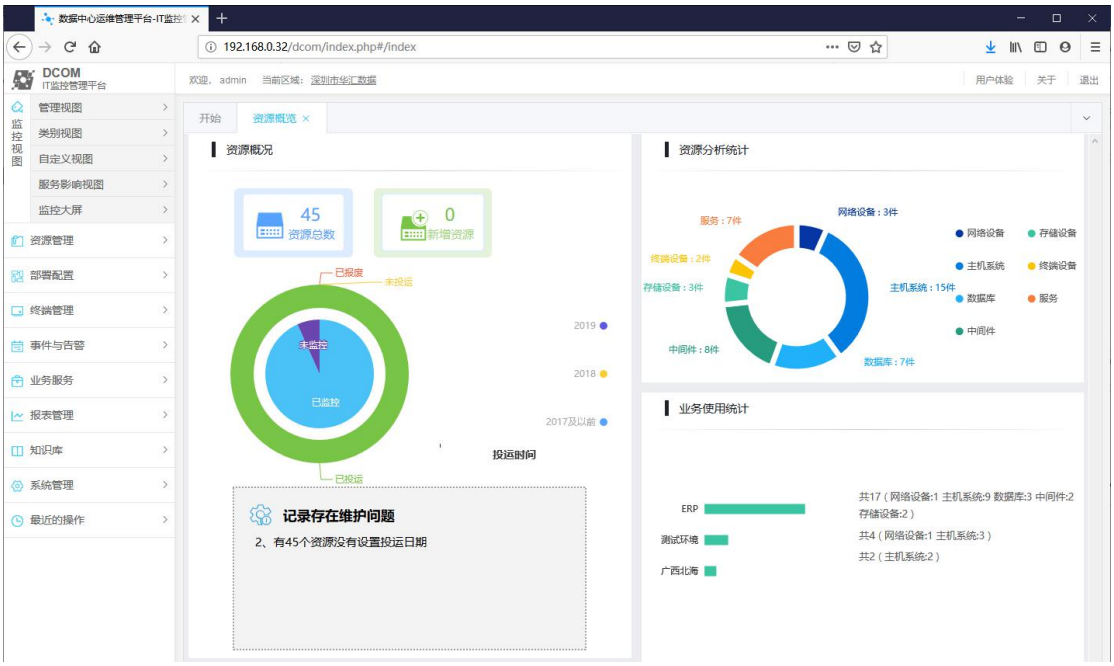
系统部署架构具有高度灵活性和可扩展性，对中小监控规模情形，管理服务器（MS）、数据存储服务器（DBS）、汇聚服务器（DAS）和监控服务器（MON）可以集中部署在一台物理服务器中。对大规模监控情形，可通过部署多个监控服务器（MON）和汇聚服务器（DAS）来满足需要。通过采用合适的部署策略，可实现跨网段监控，并且支持总部-分支机构企业集中监控和分布式部署要求。

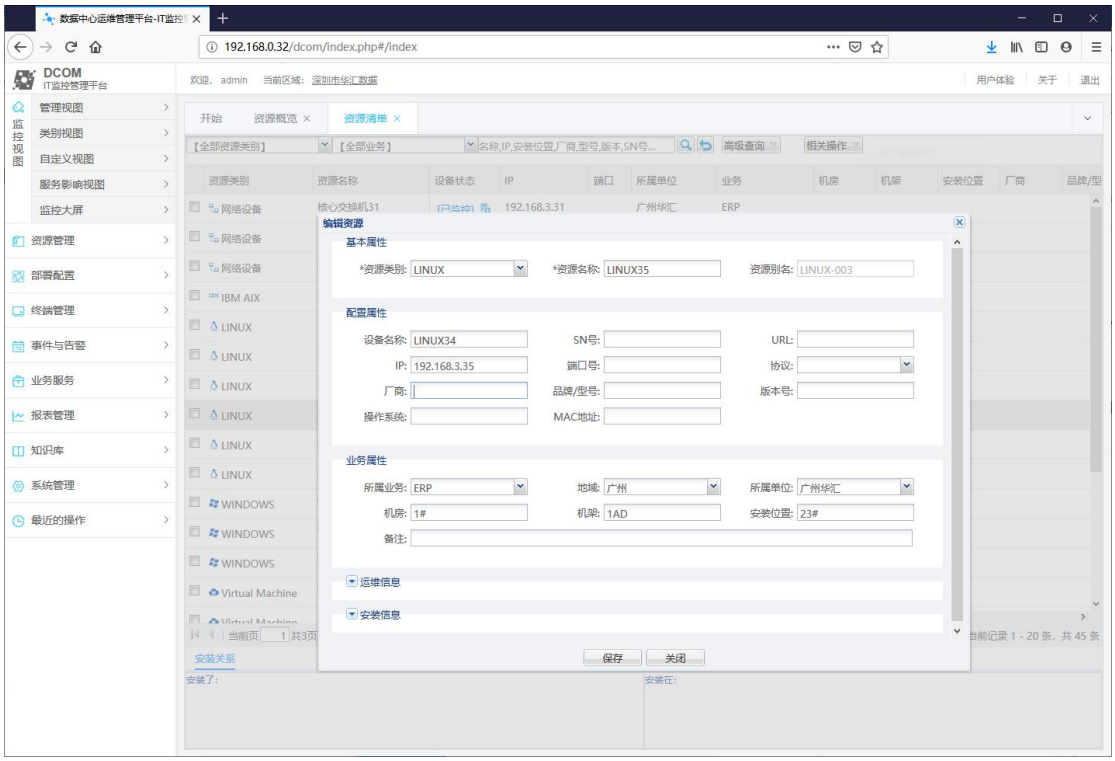
4 产品功能

4.1 资源管理

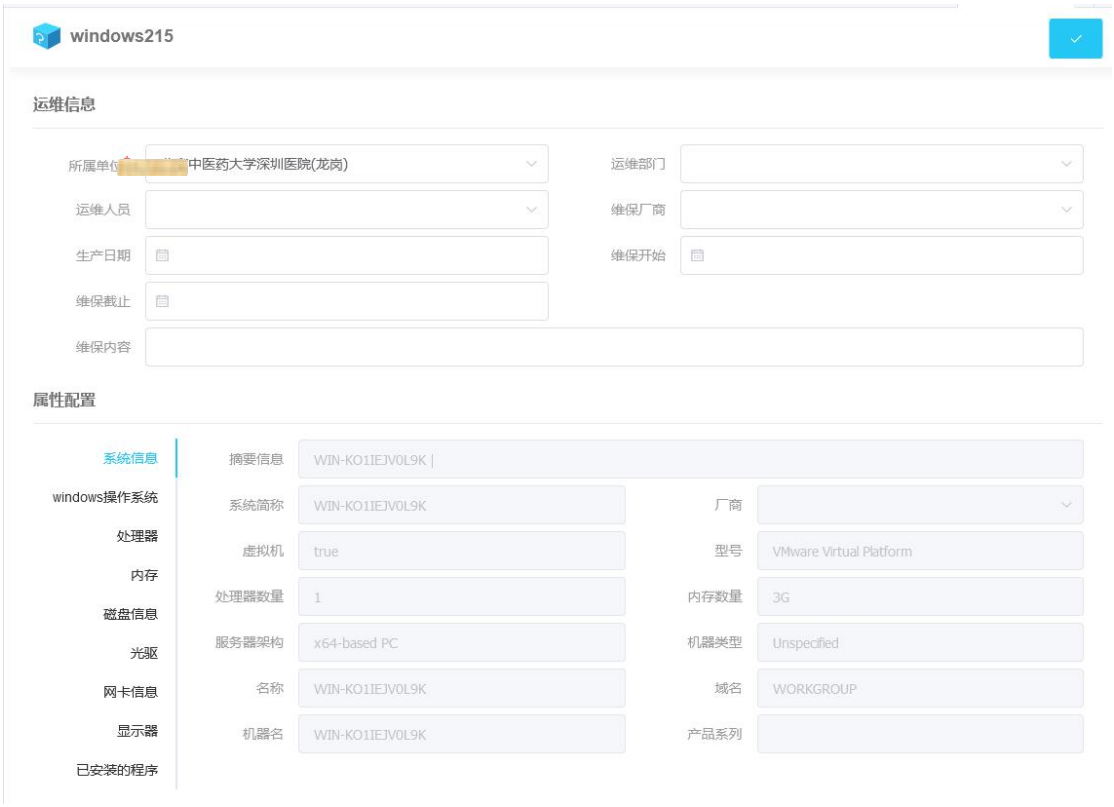
据 Gartner 研究显示，目前全球只有不到 25%的公司具有适当的 IT 资产管理规划。大多数公司都使用复杂的人工跟踪监测方式，或者根本不清楚自己的硬件资产基础。由于不了解自己 IT 资产的基础，从而导致了时间、资金以及系统性能上的损失。

DCOM 提供资产自动发现、资产跟踪、维护信息、使用监控等功能，从而帮助企业全面掌握资产的分布以及运行状况，达到降低成本和提高运营效率的目的。IT 资源管理的核心是“数据”的管理，可以总结为：数据采集、数据维护、数据展现、数据分析。





平台可以对在监控的服务器、终端的配置进行检测，检测的内容包括 CPU，内存，磁盘，网卡，操作系统，已经安装的程序等，配置变更后，能够及时自动更新，减少运维人员信息维护的工作量。



4.2 资源监控

在企业业务信息化之后，企业业务依赖于各种应用系统，应用系统又依赖于各种 IT 资源。当 IT 资源出现故障或性能下降时，会导致应用宕机或性能下降，进而影响企业业务产出。资源监控就是对哪些可能影响 IT 资源服务能力的各种技术性能参数进行全面监控，以便提前发现问题隐患并预警，帮助企业将故障消灭于萌芽状态之中。

DCOM 出厂时已经内置了大部分常见的资源监控模型，用户也可定义满足自身特殊需要的资源监控模型，具体如下表所示：

序号	类别	资源类型
1	网络设备	交换机、路由器、防火墙、负载均衡、网络链路和拓扑…
2	服务器硬件	IBM、DELL、HP、联想、浪潮…

3	虚拟化平台	VMware EXS 、 Wmware EXSI 、 华为 FusionCompute, Hyper-V…
4	主机/操作系统	WINDOWS、IBM AIX、HP-UX、Linux(包括国产基于 Linux 的各类操作系统)…
5	数据库	ORACLE、Sybase、MongoDB、SQL SERVER、Mysql、达梦 KingbaseES（人大金仓）、神通…
6	WEB 服务器	IIS、Apache、Java…
7	中间件	WebLogic、Tomcat, WebSphere, TUXEDO、Apusic（金蝶）、TongLINK/Q（东方通）…
8	存储设备	华为 OceanStor, EMC CX、EMC DX、HP 3PAR、日立 AMS200..

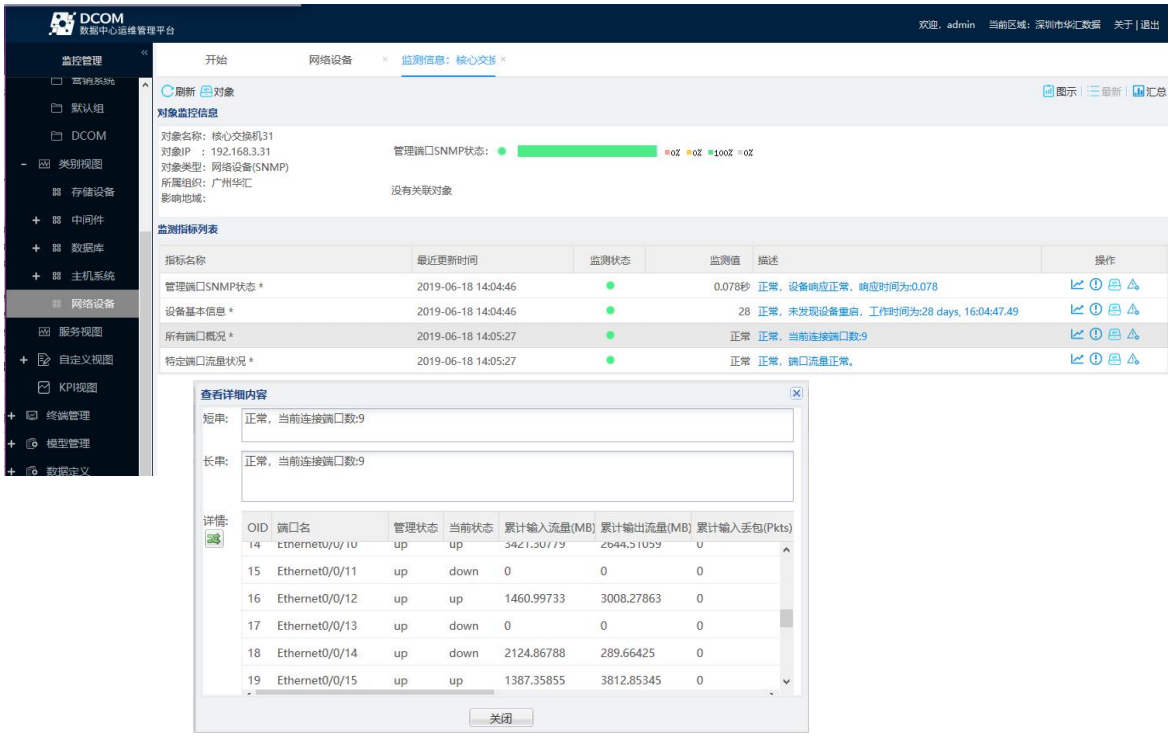
资源监控模型是否有效的关键在于科学和合理地规划监控内容，监控内容应该能全面覆盖可能导致该资源可能出现可用性和性能问题潜在隐患点。DCOM 对每类 IT 资源都参考故障树分析(Fault Tree Analysis，FTA)方法自上而下仔细梳理可能导致资源不可用或性能下降的各种隐患点，然后再据此设计监控指标和参数，最大限度地保证监控全面和有效性。

资源监控是否有效的关键在于科学和合理地规划监控内容，监控内容应该能全面覆盖可能导致该资源可能出现可用性和性能问题潜在隐患点。监控平台对每类 IT 资源都参考故障树分析(Fault Tree Analysis，FTA)方法自上而下仔细梳理可能导致资源不可用或性能下降的各种隐患点，然后再据此设计监控指标和参数，最大限度地保证监控全面和有效性。

系统内置网络设备、服务器、数据库、中间件等常见 IT 资源监控模板，如图 3 所示，并提供向导式监控对象部署方式，用户只需输入对象实例名称、IP 等必要信息就能轻松地实现对 IT 资源的监控。在实际运行过程中可根据实际情况增加监控指标，对采集频率、采集时段、告警阀值等监控参数进行调优，以使系统达到最佳监控效果。

1. 网络

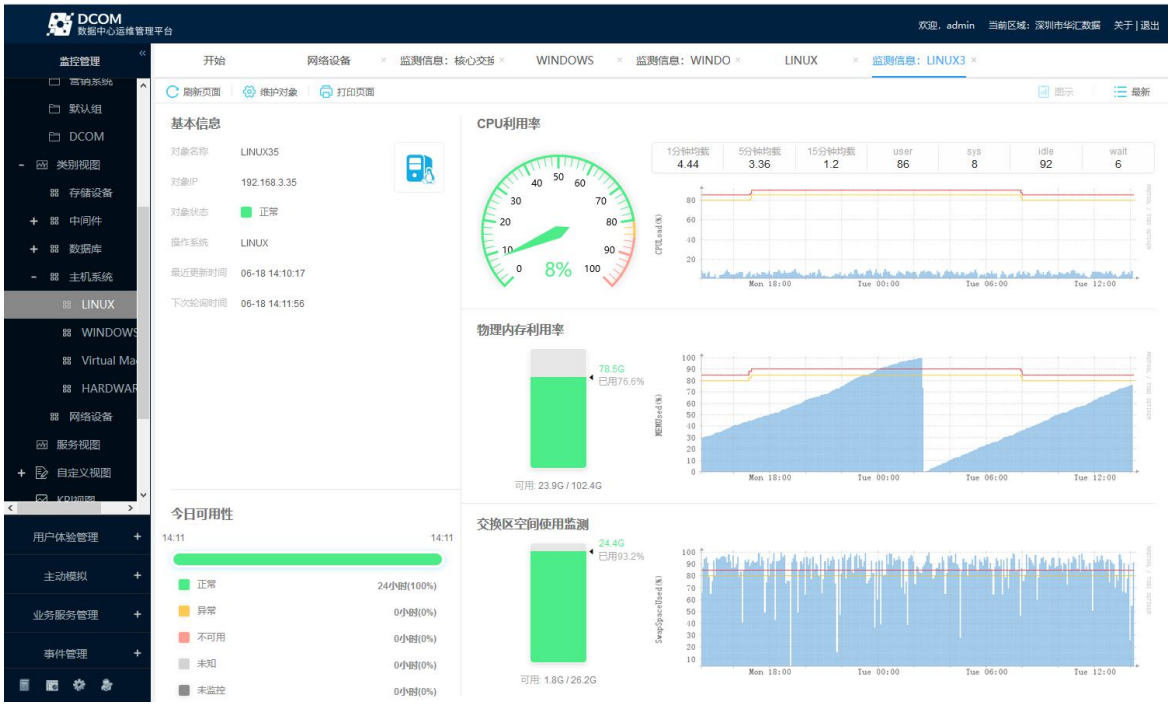
系统的网络监控是基于 SNMP 管理协议开发的跨厂商、跨平台的通用网络管理模块，能全面管理支持 SNMP 协议各个网络设备厂商的产品，监控设备类型包括交换机、路由器、防火墙、负载均衡等设备，监控内容包括设备可用性（ping）、端口流量、端口使用率、内存使用率、CPU 使用率等。



网络设备

2. 服务器

系统的服务器监控从多个方面对服务器硬件资源和操作系统进行监控管理，监控内容包括非法登录监测、存储空间监测、CPU 负载监测、物理内存监测、交换区空间监测、IO 负载监测、集群状态监测、指定进程监测和系统日志监测等。支持 IBM AIX、HP-UX、Solaris、Windows、Linux、Red Hat、CentOS 等多种操作系统及 IBM、HP、Lenovo 等服务器设备。



主机监控

3. 数据库

系统的数据库监控从可用性、性能、占用资源、安全事件和异常错误等多个方面对数据库进行全面监控，如响应时间监测、连接进程数监测、连接客户端监测、指定进程监测、长事务监测、锁监测、进程回滚监测、数据库空间监测和数据日志监测等。支持 ORACLE、Sybase、DB2 、SQL Server、Informix、MySQL 等多种数据库。

下表是 ORACLE 数据库监控内容示例。

监控资源	监控内容	说明
一、可能导致 ORACLE 数据库不可用监测点		
ORACLE 实例状态	监控 ORACLE 实例运行状态	连接到数据库运行 SQL 语句以确定 ORACLE 实例运行状态
ORACLE 监听器	监控 Oracle 网络监听器进程是否正常运行	监听器主要用于监听客户端向数据库服务器端提出的连接请求，如果宕掉会导致客户端访问不了

		数据库
ORACLE 进程	监控 ORACLE 进程是否正常运行	Oracle 进程包括服务器进程和后台进程。服务器进程在用户和 Oracle 服务器之间通信，以处理用户请求。后台进程执行 I/O 并监控其它 Oracle 进程以保障系统性能和可靠性。每个 ORACLE 实例至少运行 4 个后台进程（DBWR、LGWR、SMON 和 PMON），但可能有许多附加后台进程
表空间	监测表空间大小以及剩余可用空间是否足够	在表空间未设置为自动扩展情形下，表空间耗尽会导致数据库无法创建新对象；另外也需关注临时表空间和回滚表空间大小，如果长期增长不释放会占用大量磁盘空间
扩展数据块	监测数据库对象可用扩展数据块是否不足	适合哪些设置 MAXEXTENTS 值的对象，在可用扩展数据块耗尽时将导致该对象数据操作失败
归档目的地空间	监控归档目的地空间是否耗尽	仅适用数据库运行在 ARCHIVELOG 方式下。如果归档目的地空间耗尽数据库会被挂起直到有空间可用为止
转储目的地空间	监控转储目的地空间是否耗尽	包括后台转储目的地（BACKGROUND_DUMP_DEST）、核心转储目的地（CORE_DUMP_DEST）、用户转储

		目的地（USER_DUMP_DEST），如果指定的转储目的地空间已满会导致进程失败
会话	监控数据库会话数是否接近允许的最大会话数	当数据库连接会话数达到最大允许会话数时，会导致后续数据库连接失败

二、可能导致 ORACLE 数据库性能下降的监测点

SGA	监控 SGA 中数据高速缓存、库高速缓存和字典高速缓存命中率	高速缓存命中率应该保持在一个合适范围，较低命中率会导致 I/O 增大，造成数据库性能降低。一般数据高速缓存命中率不应低于 0.9，库高速缓存命中率不应低于 0.99，字典高速缓存命中率不应低于 0.85
PGA	监控 PGA 内存使用情况，例如 over allocation count 、mutipassExecutions 、cache hit percentage 、extra bytes read/written 以判断系统是否工作在最佳状态	PGA 相关信息可从 V$PGASTAT 等相关视图中获取，设置 PGA_AGGREGATE_TARGET 以使 ORACLE 工作最佳状态
事务	监控活动事务数、长时间运行事务、被阻塞事务	事务是包含由单个用户执行的一个或多个 SQL 语句的逻辑工作单元。监控事务可发现应用程序中可能出现的问题
锁	监控活动锁数量、死锁、长时间占用资源锁和排	Oracle 使用不同的锁来控制对数据的并发访问以及防止用户

	队超时锁	之间的破坏性交互作用，太多锁或出现长时间占用资源的锁影响系统性能，需要查找原因进行优化
回滚段	监控回滚段的等待和争用	回滚段争用会降低数据库性能，一般视图 v$rollstat 中 waits/gets 比值应该小于 1%
I/O	监控 ORACLE 数据文件 I/O 物理读取写入数	如果存在过高物理读出写入数表明存在 I/O 瓶颈，需要优化存储
游标	监控会话打开游标数目	如果会话打开游标数超出设置的最大游标数，程序会报 ORA-01000 错误
存储碎片	监控 ORACLE 存储碎片情况，包括表空间碎片、表碎片和索引碎片	过多的碎片导致在数据访问时需要更多的磁盘Ｉ/Ｏ ,增加了数据库读的数量和磁盘查找时间 ,从而引起性能下降
重做日志	监控重做日志切换和等待情况	重装日志切换频繁或发生过多等待次数，可适当增大重做日志文件大小
全表扫描	监控出现全表扫描的大表，以提供优化线索	大表一般建议通过索引以提高数据查询性能，如果出现全表扫描的大表，则考虑重新设计索引或优化应用程序
三、其他		
作业队列	监控 ORACLE 执行未成功或规定时间未执行	Oracle 作业是自动的标准和重复任务，例如执行操作系统命

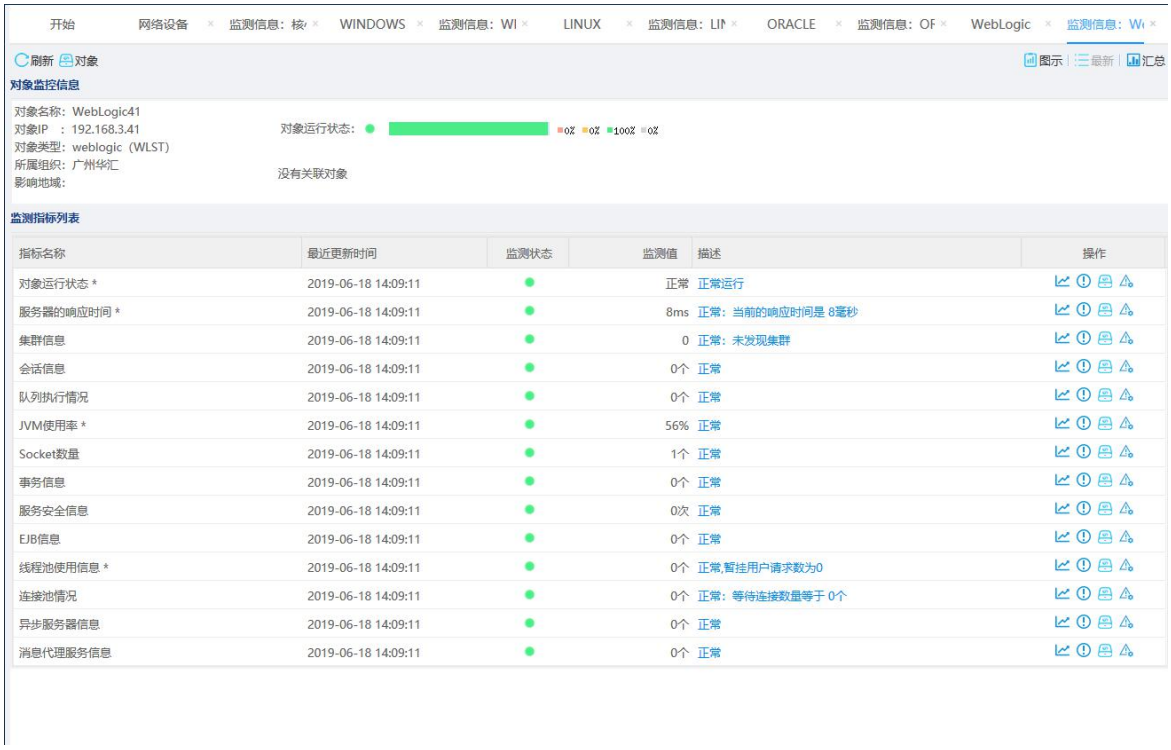
的作业	令或备份数据库

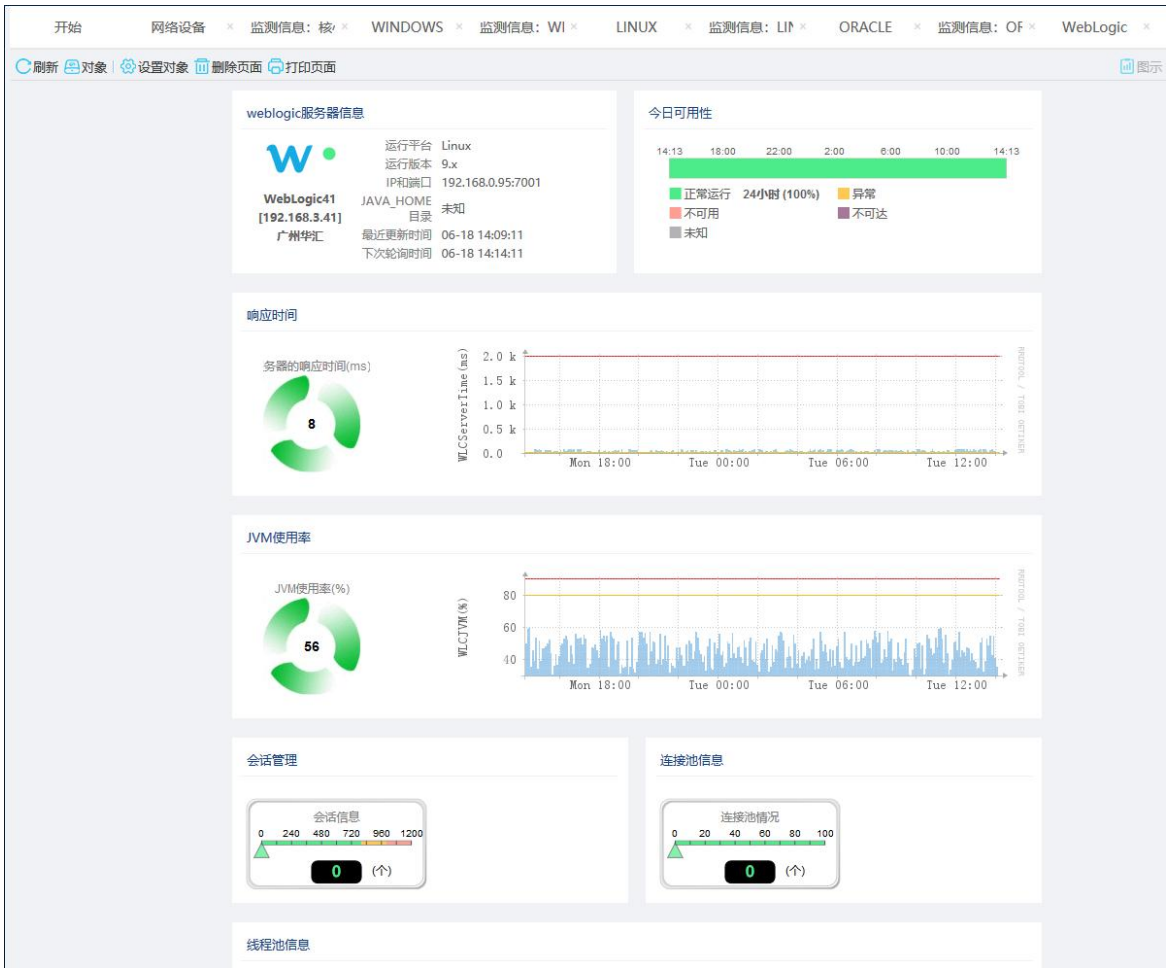
Oracle 监控

4. 中间件

中间件是位于网络、操作系统和数据库之上和应用系统之下的一种独立的系统软件或服务程序，常见的中间件类型有交易中间件、消息中间件、RPC 中间件、应用服务器和 WEB 服务器等。系统的中间件监控支持各种常用的中间件软件监控，如 Tuxedo 、WebLogic、WebSphere、JBoss、Tomcat、Apache、IIS、Exchange Server、Lotus Notes and Domino 等。系统的中间件监控从可用性、性能、占用资源、安全事件和异常错误等几个方面对中间件进行全方位

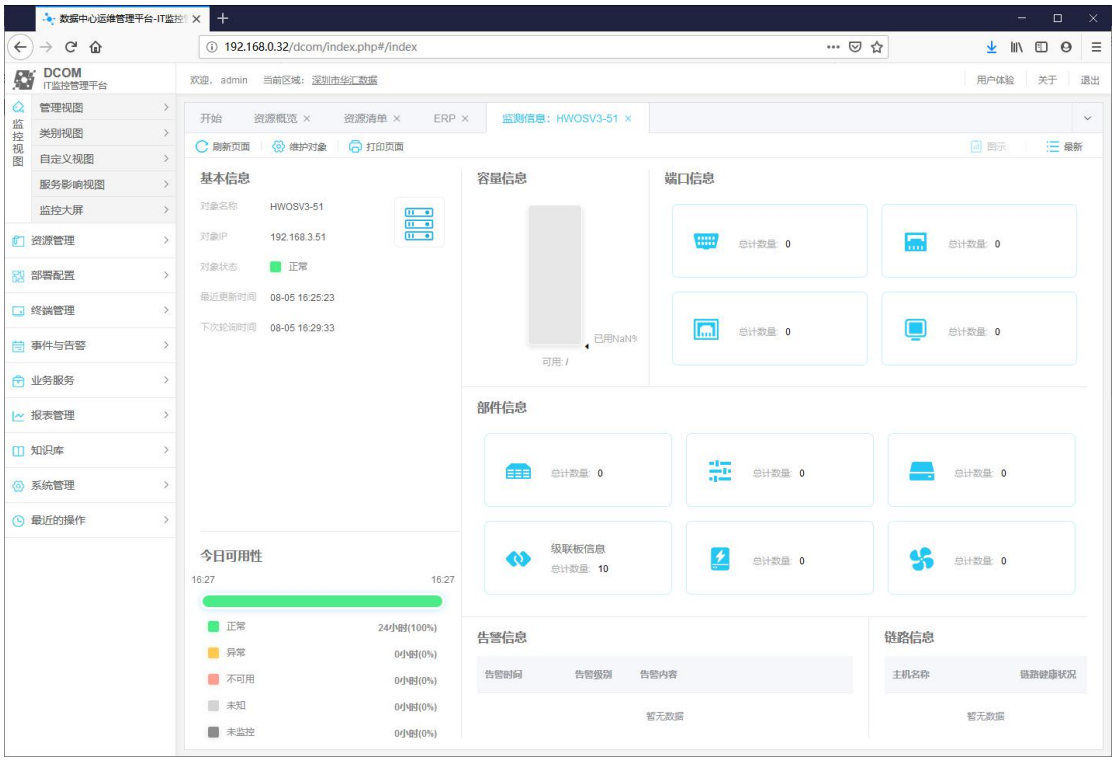
监测，如 Apache 监测内容包括服务进程监测、负载监测、请求监测、闲置监测、内存使用情况监测和数据库连接监测等信息。





中间件监控

资源监控结果除了列表展现之外，还提供可视化展现界面，可帮助运维人员更直观了解资源健康状况和关键指标信息，下面是 ORACLE 监控可视化界面：



资源可视化展现

4.3 日志管理

主机、数据库、路由器、交换机、防火墙等网络设备，以及其他应用系统，在运行期间会产生各种日志，日志信息普遍存在以下几方面的问题：

1. 生产、灾备系统服务面临着超级复杂的可用性挑战

日志分散，采集管理难度大；日志数据来源各异，且格式不一，采集配置难度大。

2. 业务异常时，难以快速定位分析故障

海量数据，全量合规存储成本高；满足安全合规条件下的全量留存，数据量巨大存储成本较高。

3. 业务运行风险增加，运维工作压力大

异地机构管理难度大；多个数据中心需要为多个分支机构提供服务，需耗费大量的资源做好异地多级单位的日志数据统一管理工作。

4. 灾难恢复后，缺少系统性评估和验证

监控工具繁多，缺少统一管理平台；运维部门、安全部门、运营部门等对日志数据查询调用需求不一， 存在误操作引起的安全隐患，缺乏统一监管。

ITOM 日志管理模块提供了统一日志管理的功能，支持对多种来源和格式的日志数据的采集、分析、导出。 支持指标、日志、事件等多种类型数据的统一存储和分析；实现对 IT 环境各个资源及设备运行情况的综合分析，提升现有 IT 运维管理水平。

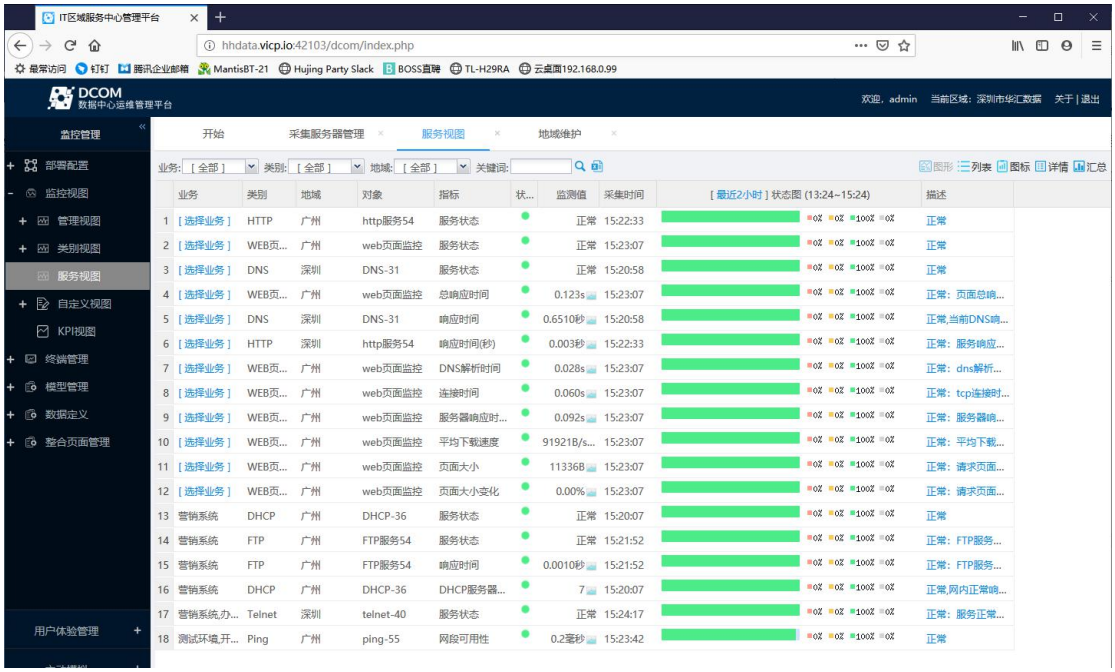
日志功能拓扑图

4.4 服务监控

在业务信息化之后，企业业务应用的可靠稳定运行依赖于 IT 基础设施提供的各种服务。除了对可能影响 IT 基础设施服务能力的各种技术性能参数进行全面监控外，DCOM 还提供对 IT 资源提供的各种服务进行直接监控，例如基础网络服务、数据库服务、WEB 服务等，以帮助 IT 运维人员实时了解不同位置下服务的可用性和性能问题。

DCOM 支持对如下服务进行监控：

序号	类别	服务类型
1	网络服务	ping、fping、ftp、dhcp、dns、telnet
2	数据库服务	jdbc、odbc
3	WEB 服务	http、https
4	邮箱服务	pop、smtp



4.5 终端管理

可以简便地管理和更新终端的程序和插件，对终端进行监控；监控内容包括：终端在线、状态查看，终端运行概要监控；

终端程序除了采集运行信息以外，还提供自助服务、消息推送等功能。

4.5.1 客户端扫描更新

可以通过管理平台进行终端扫描，浏览扫描结果，对新发现的终端进行集中操作，对某个或一批终端远程更新客户端插件或程序。

可以从客户端下载程序，安装后自动注册到监控平台上。

4.5.2 终端监控和信息维护

可以对终端（PC 机、打印机、无人值守终端）进行监控，对终端的设置信息进行管理。可展示 1 个小时内的运行情况：

1.查询当前终端故障类的事件（由用户报告的事件，类型是终端问题）；

2.显示对应终端当前的状态，如果是在线，技术人员可以查看终端的运行信息，登录用户、IP 等等，可以对终端的插件进行远程更新；

3.通过 IP 段或 IP 查询终端，对查询出的设备进行监控：查看状态、更新客户端。

4.终端运行错误；

4.5.3 终端概览

展示终端的统计信息，包括：

1）PC 机和打印机的数量，在线数量、故障数量；

2）终端能耗的趋势。能耗根据每天 PC 机的开机时间和 PC 机的额定功率进行估算；

4.6 服务影响管理

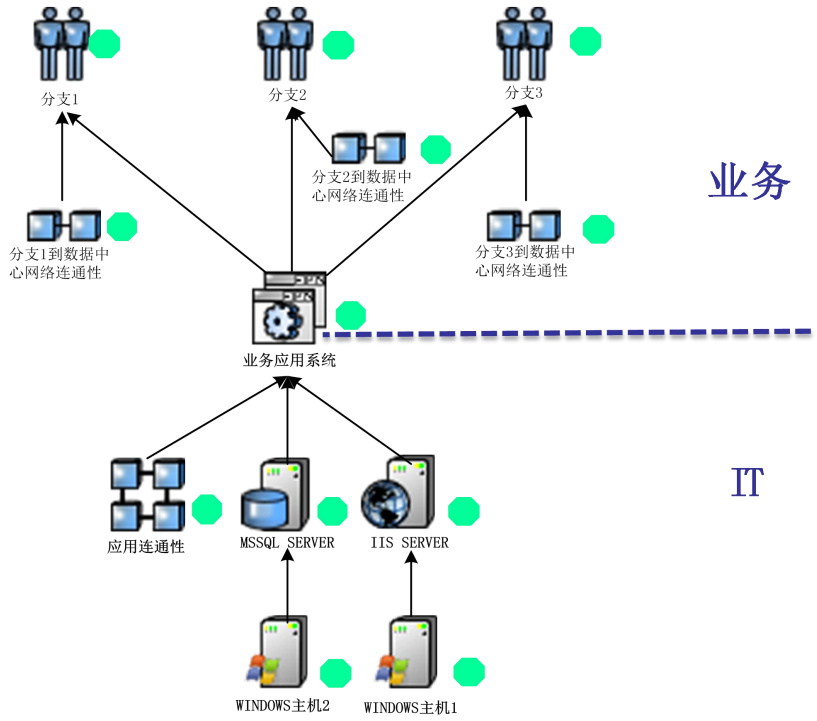
在对资源、服务和日志进行监控之后，我们能够收集企业范围内所有事件，帮助运维人员了解什么地方发生了什么事情。而基于规则的事件处理引擎则通过对事件进行过滤、压制和关联分析，极大减少了运维人员需要直接面对的事件数量，提高了运维工作效率和质量。但由于缺乏将业务服务与 IT 关联起来的能力，使运维基本还停留在以资源为中心的状况，运维人员在 IT 资源出现问题时无法确定问题对业务的影响，而在用户报告业务问题时又不能很快定位问题组件，导致对业务中断反映迟缓，运维经常处于被动局面。

服务影响管理则致力于解决上述问题，通过创建服务模型实现业务与 IT 之间关联，并能够自动计算资源问题对服务造成的影响，可帮助运维人员将注意力集中到企业主要业务上，并从业务角度来管理 IT。服务影响管理模块主要提供如下功能：

4.6.1 服务建模

监控平台应提供服务建模工具，通过创建业务服务模型将业务与 IT 资源关联起来，同时借助服务模型，使我们关注的不再是单个资源的健康状况，而是整个服务的可用性和性能，这更符合 IT 运维的本质目标。

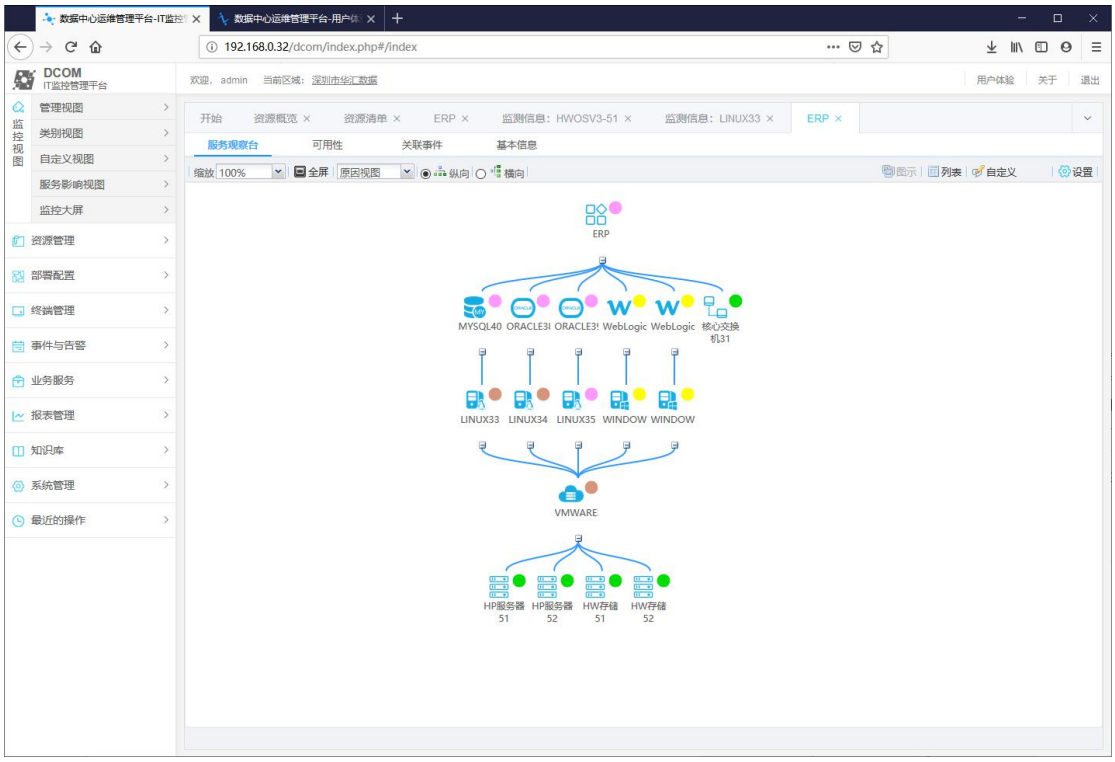
图 6 是一个服务模型示例，业务元素可以是地域、用户群或业务流程，而应用系统做为衔接业务与 IT 基础设施的桥梁。

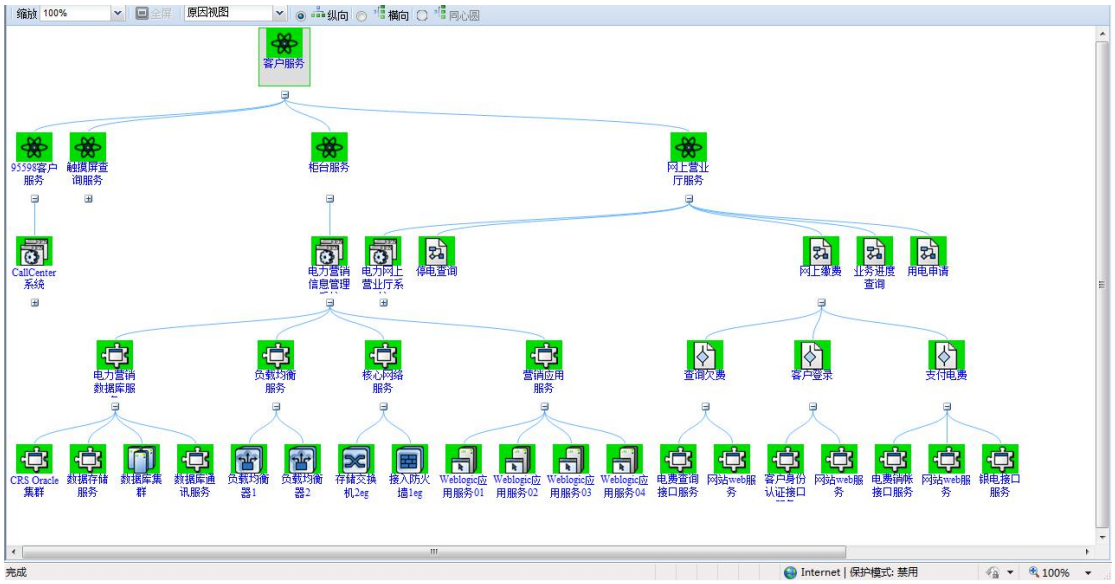


服务模型示例

4.6.2 业务视图

业务视图是一种从业务角度来组织监控对象并展现的方式。通过建立业务视图把 IT 和业务关联起来，从而帮助客户直观了解企业业务的健康状况，快速定位故障节点，清晰故障影响范围，确定故障处理优先级别，增强 IT 部门和业务部门的沟通。业务视图提供一种从整体到局部再到细节的展现方式，运维人员首先可从业务视图一览表中查看企业整体业务健康状况，然后可选择某个特定业务视图查看业务相关 IT 资源健康状况、最近告警事件和关联客户情况，如果还需进一步了解细节则可选择具体的 IT 资源了解详细指标监控状态。





4.6.3 服务影响与根源分析

监控平台支持多种服务组件状态计算方法和状态传播策略，可自动准确计算在 IT 资源故障对服务的影响。如图 5，当系统监测到分支机构 3 到数据中心网络中断时，在服务视图中会自动将分支 3 组件状态标红，标识分支机构 3 用户群服务访问中断。因此，借助服务视图运维人员可准确了解 IT 事件对

业务影响，反之在接到用户报告业务问题时通过服务视图能很快确定问题根源所在。

4.6.4 服务可用性报告

服务影响模块提供服务可用性计算，包括可用率、平均修复时间、平均故障间隔时间等 KPI 指标，为企业对 IT 运维服务水平提供基础数据。

4.7 运维自动化

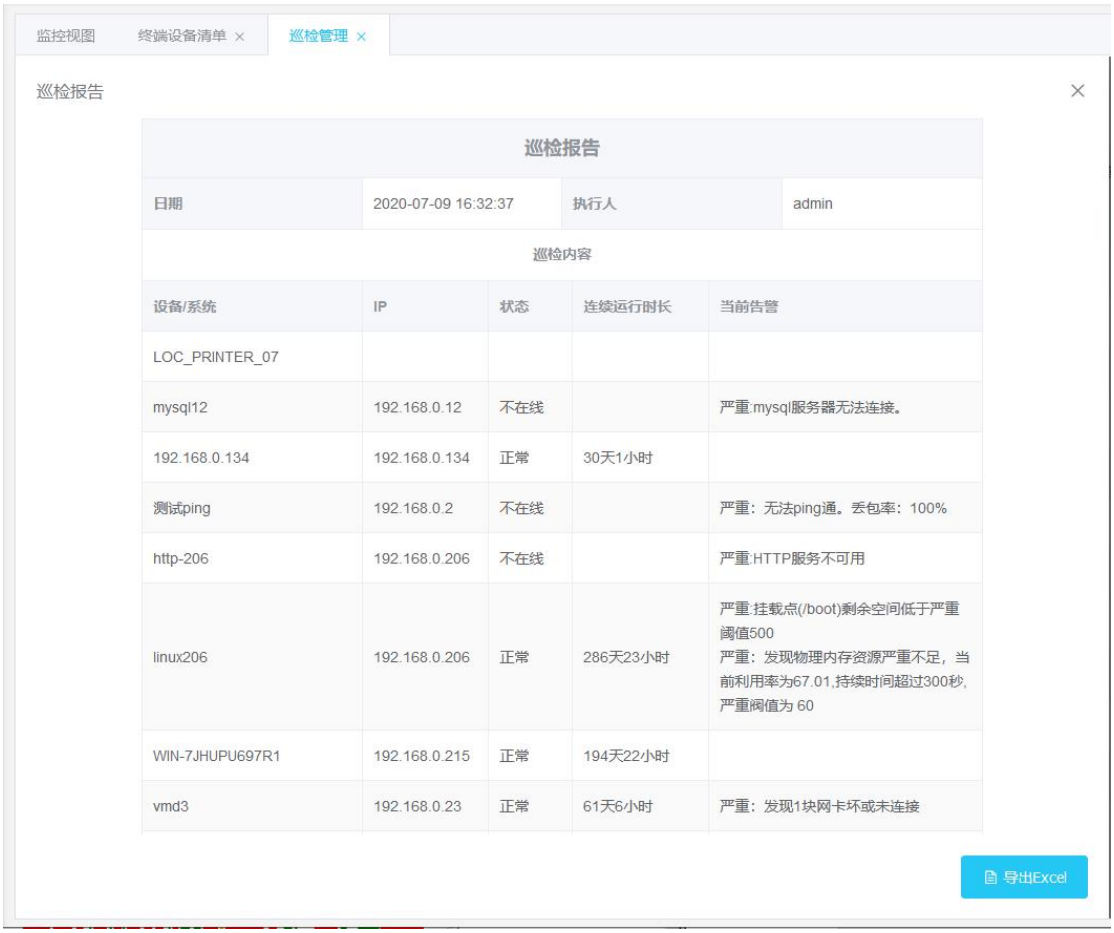
4.7.1 自动巡检

所谓 IT 运维自动化是指通过将日常 IT 运维中大量的重复性工作，由以往的手工执行转为自动化操作，从而减少乃至消除运维中的延迟，实现“零延时”的 IT 运维。IT 运维人员可以在业务系统的监控对象中选择需要关注的指标，或由系统提供定制检查脚本，对日志、接口、服务进行常规检查或者特别的测试。也可以将一些分散的脚本或编写新的指令由 DCOM 平台进行调度执行，最后自动出具运维巡检的明细报告。

运维自动化可以大大提高运维的主动性和准确性，减少技术人员的工作强度，将精力转到运维策略规划、问题分析等有价值的工作中。

4.7.2 巡检报告

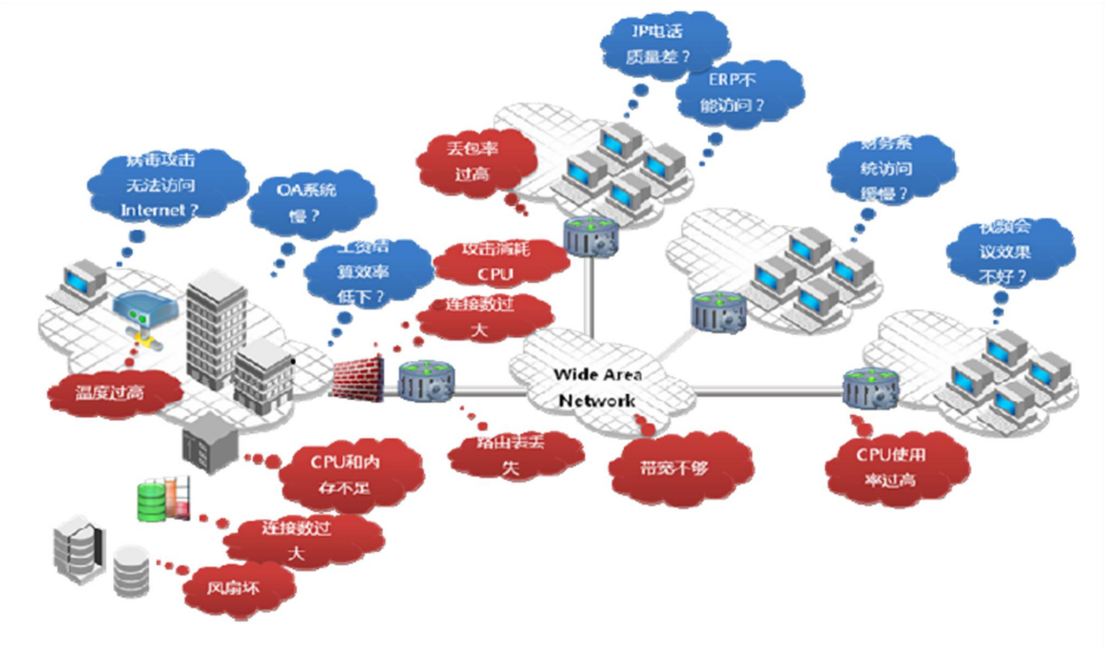
可以在定时执行系统检查后自动生成巡检报告，针对运维人员和管理人员提供不同的报告，可导出为 Word 和 PDF。



自动运维巡检报告

4.8 事件管理

如图 5 所示，在企业 IT 环境，每天都会发生成千上万各种各样事件，例如 ERP 不能访问了、磁盘空间不足、网络丢包率过高等等，如果所有事件不经处理就由运维人员直接面对，哪势必给运维人员带来繁重的工作量，影响运维工作效率和质量，这也是很多企业感觉监控系统不好用的原因之一。



IT 环境事件示例

4.8.1 事件处理引擎

DCOM 内置基于规则的事件处理引擎，能够对事件进行过滤和压制等预处理，使运维人员最终面对的都是有意义和必须处理的事件，这样就大大减轻了运维人员工作量。图 6 是系统内置的部分规则，用户也可创建自己的规则来处理事件。

开始 | 压制规则管理

刷新 | 增加 | 删除 | 修改 | 上调 | 下调

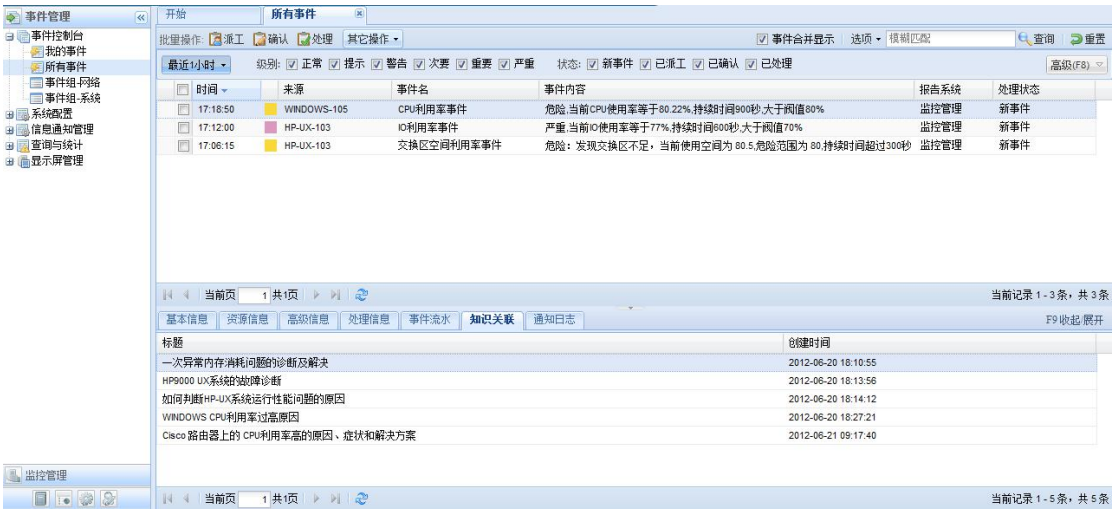
	规则名称	启用	维续标记	级别条件	规则描述	内置规则
1	收到n次连续的告警事件后才认为告警有效	✗	–	警告	一段时间内连续收到n次告警事件才发送告警通知，告警事件中间出现恢复事件将需要重新计…	是
2	根据一段时间收到的告警事件的比例来判定告警…	✗	–	警告	在一段较长的事件内统计告警事件次数，忽略其中的恢复事件，当告警事件次数大于一定数…	是
3	忽略偶发告警	✓	–	警告	SIM组件由于事件到来的顺序和传播关系的骤响，可能会导致组件状态出现短时和快速的变化…	是
4	压制当天的重复报警	✗	–	警告	压缩当天的所有相同的报警，即一天内同一告警事件只会保留1条，发送告警通知1次。	是
5	压制用户体验实例重复事件	✓	–	警告	用户体验的实例事件类似挥发性事件，每一次达到告警条件，都会产生事件，用户不希望每…	是
6	压制重复事件	✓	–	警告	AM/SLM的指标默认每小时会发送重复的告警，UXM会根据统计周期重复发送事件。这些重复…	是

DCOM 部分内置规则

如图 7 所示，DCOM 提供事件控制台，可根据需要对事件进行任意分组，以满足不同运维角色权限管理需要。同时提供一个简单事件处理微流程，操作人员可在事件控制台对事件进行确认、派工和处理等操作。对已经实施流程管理系统的企业，DCOM 可以直接与流程管理系统进行衔接。

在事件派工之后，用户登陆到系统之后，可看到事件汇总界面，如图 8

所示。用户在这里可了解自己所负责事件概况，包括按事件组、事件严重级别统计，最近一段时间告警数量变化趋势，不同资源告警发生情况，以及分配给我的事件处理情况等。用户可根据实际情况转到事件控制台对事件进行确认和处理。



事件控制台

我的事件汇总界面

4.8.2 告警信息发送

平台可以通过邮件、短信猫、短信网关、桌面终端，将告警发送给运维人

员。

4.9 监控数据可视化

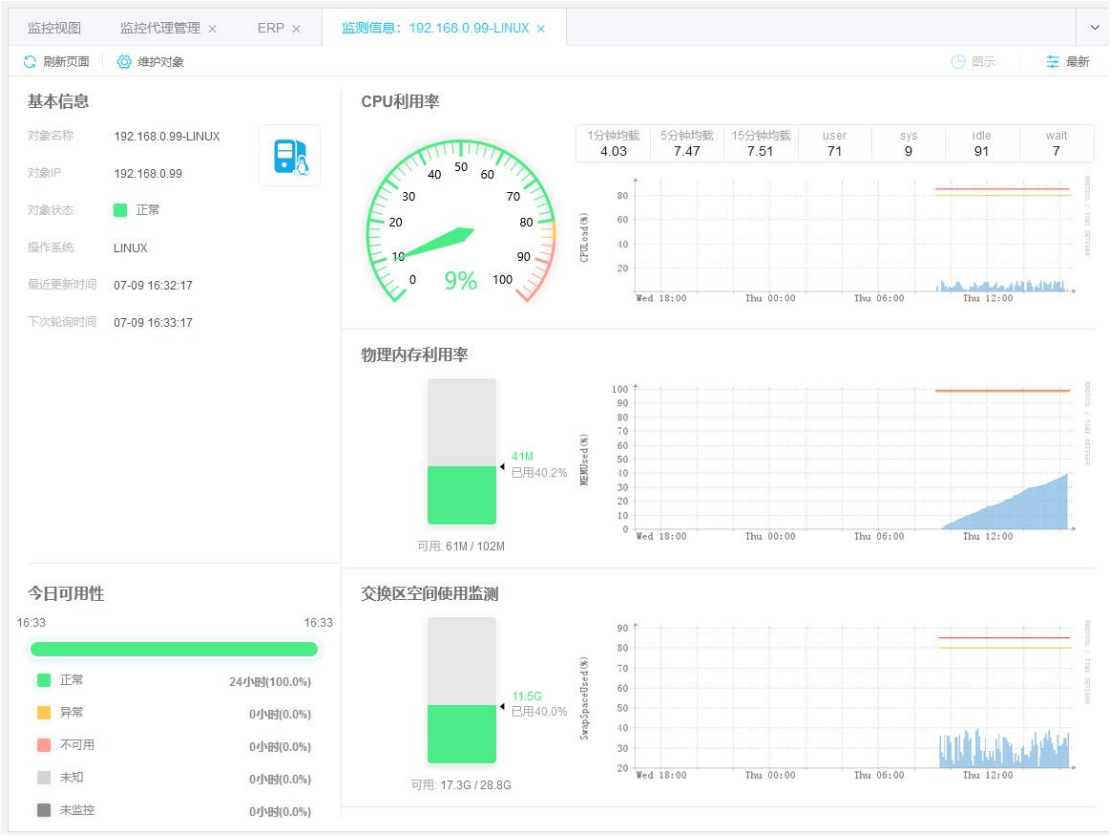
结果展现层主要实现监控结果的统计分析和展现，其目标是帮助运维部门能够实时了解企业业务和其所依赖 IT 资源的运行状况，以及提供系统运维和优化的指示和依据。

4.9.1 资源监控视图

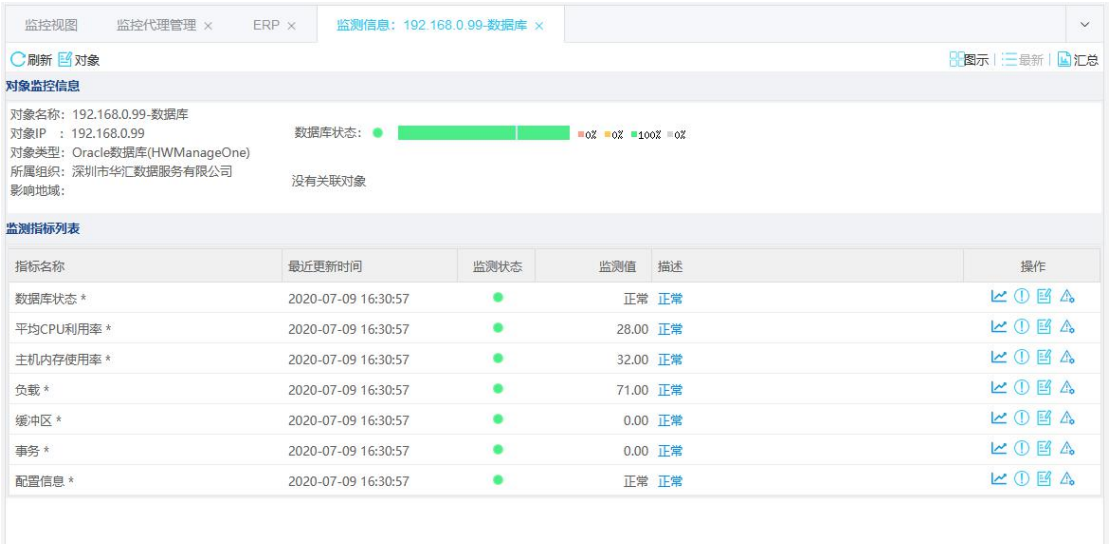
为了改变被动运维的局面，运维人员对监控系统的需求不再满足于简单的监控与告警，他们更倾向于事先在海量监控数据中去寻找故障症兆的蛛丝马迹，系统对监控信息提供多视角多层次的组织与展现方式，很好地满足了用户需求。

首先从横向角度系统提供管理视图、设备视图、业务视图和拓扑视图等多种视角来组织对象方式，使运维能真正做到分权限、分设备和分业务进行管理；其次从纵向角度提供全局、按组、按对象和按指标等多层次展现视图，满足从全局到局部再到细节等不同层次的运维管理人员需要。

对象指标列表展现



Linux 主机可视化监控图

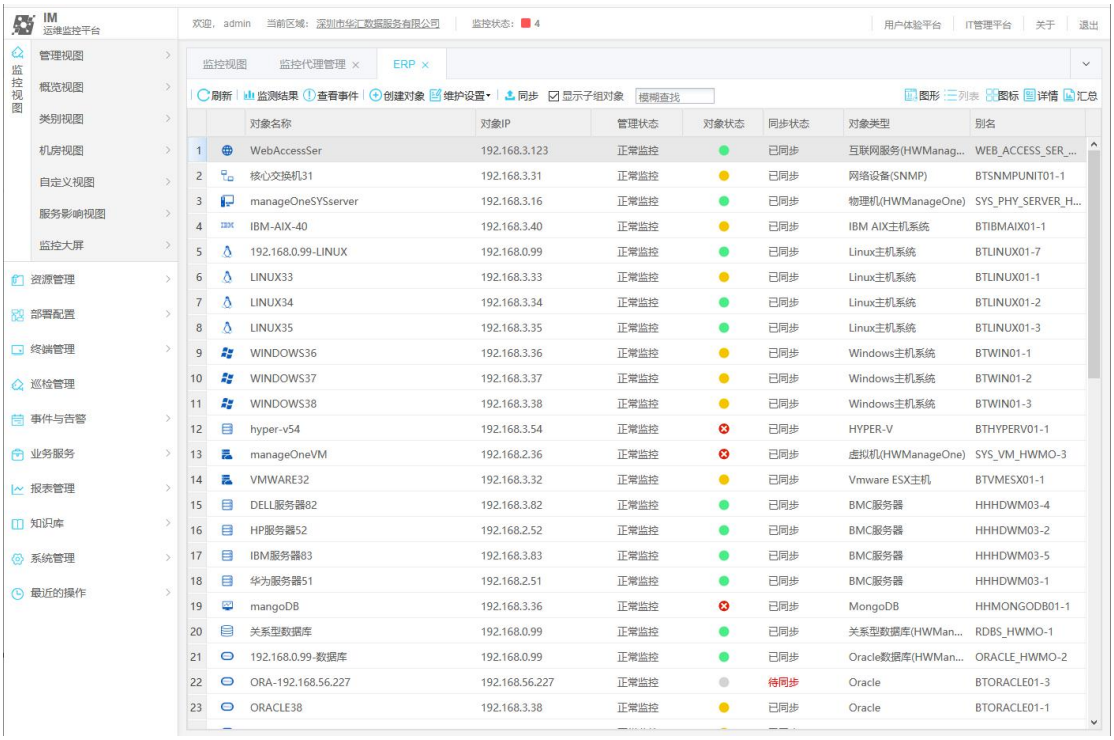


ORALCE 数据库监控图

4.9.2 管理视图

管理视图是一种按管理职责来组织监控对象并展现的方式。通过管理视图，领导能一目了然了解下属各个管理组 IT 资源健康状况，具体负责人则可通过组概览图轻松查看本组总体运行情况、关键指标运行情况和最近告警情

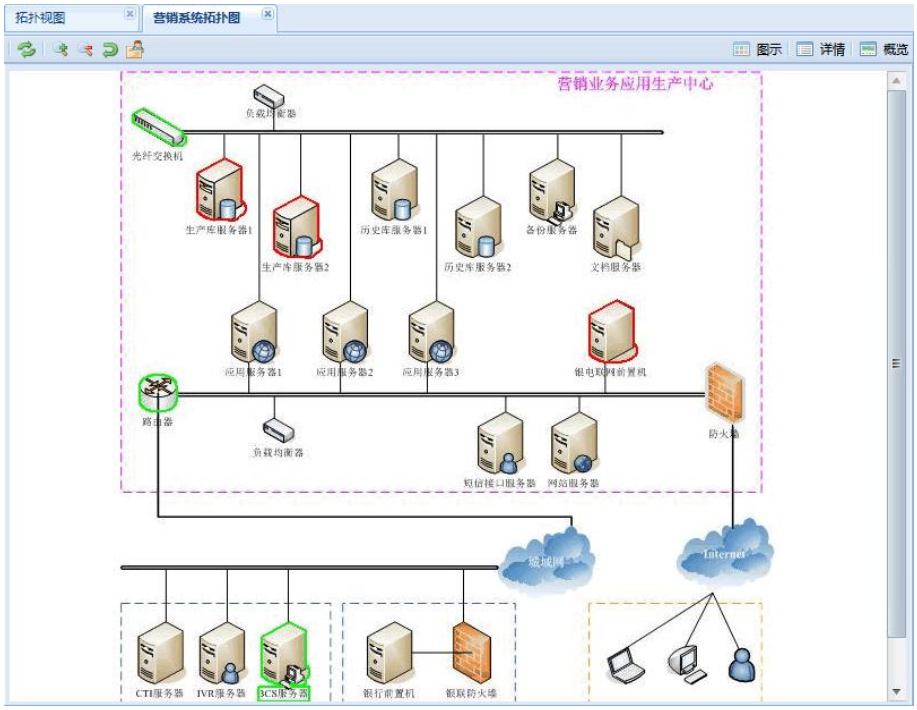
况等，如有需要还可进一步深入到对象和指标视图进行查看和分析。



管理视图

4.9.3 拓扑视图

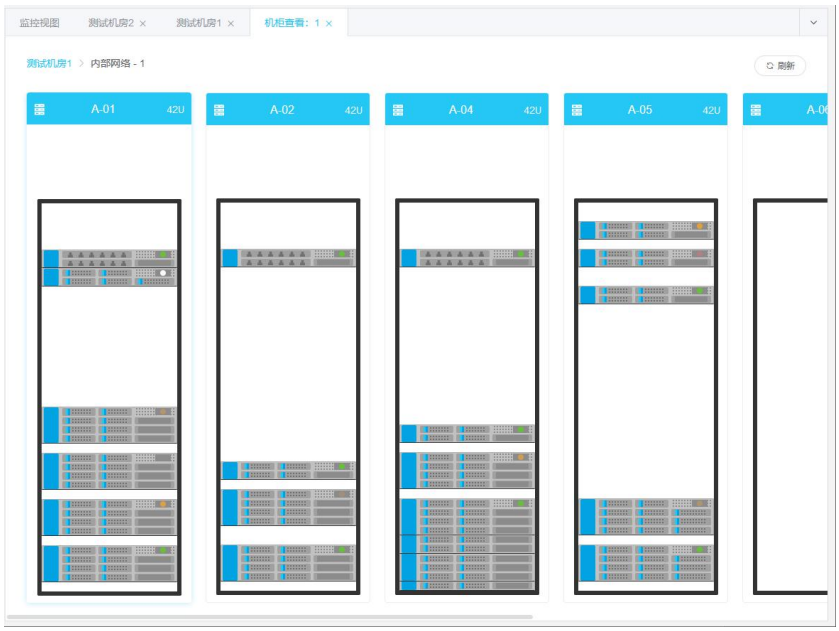
拓扑视图是讲监控结果以拓扑图形式展现，便于运维人员确定故障网络位置。



拓扑视图

4.9.4 机柜视图

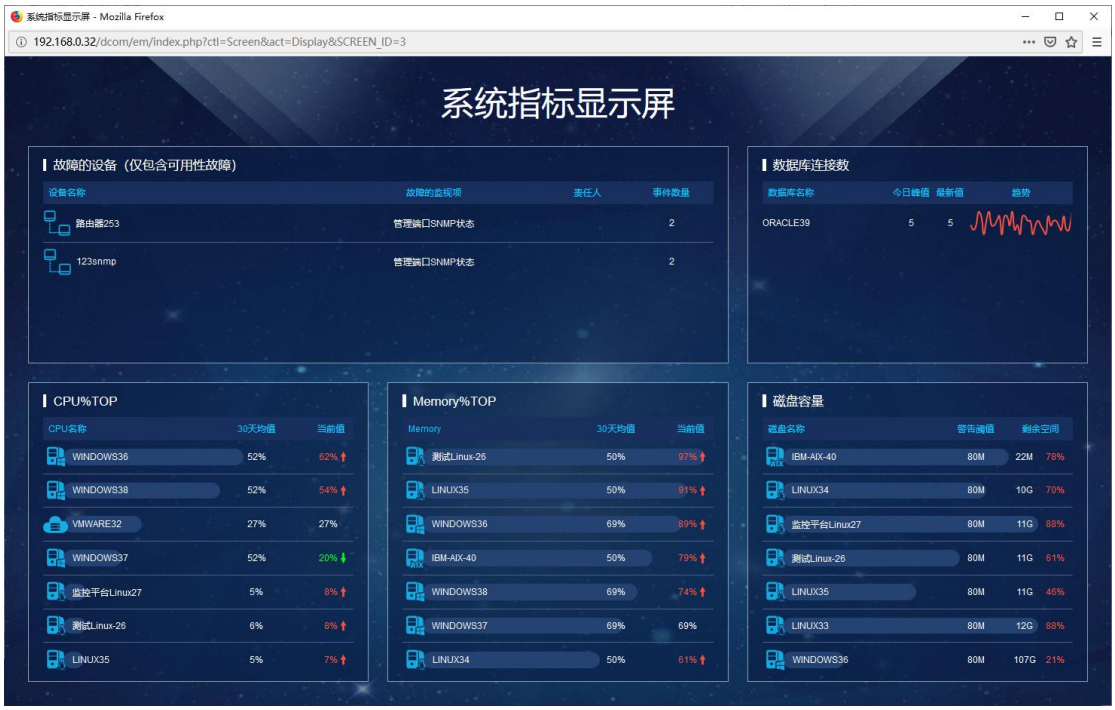
为了能够直观地了解 IT 资源的位置、安装、运行情况，系统提供以机柜视角的可视化展现。可以从机房的总体状态，快速定位到机柜、设备，再到具体的监控指标。



机柜视图

4.9.5 监控大屏

在大屏上可显示系统监控的概要信息，包括资源和系统的总体情况、当前事件和告警，直观、简洁美观。



4.10 报表管理

DCOM 提供各种监控统计分析，包括 TopN 排名分析、指标趋势分析、统计分析、时段对比分析、资源对比分析等，帮助运维人员准确评估 IT 环境运行情况，及早发现故障隐患和变化趋势，为 IT 运维决策提供参考依据。

4.10.1综合统计分析

系统提供对象运行状态、资源使用情况、告警事件分类情况、告警处理情况等各种综合统计分析报表，下图是对象运行状态统计报表界面截图，从图中可了解每个监控对象的一段时间的宕机次数、平均宕机间隔时间、平均宕机恢复时间、宕机总时长、在线率等信息。

对象名称	当前状态	宕机次数	平均宕机间隔时间	平均宕机恢复时间	宕机总时长（小时）	计划停机总时长	不可达总时长	在线率
一、网络								
路由器	正常	2	96.35	8.26	16.51	0	0	94.6%
温湿度监测器	正常	1	117.6	70.28	70.28	0	0	76.99%
防火墙_1	正常	1	33.14	150.08	150.08	0	0	30.63%
二、主机								
linux_164	正常	0	309.27	0	0	0	0	100%
windows_109	正常	1	143.23	0.16	0.16	0	0	99.94%
aix_50	正常	1	142.43	0.04	0.04	0	0	99.99%
windows_119	正常	5	47.42	0.11	0.54	0	0	99.81%
linux_1.13	正常	0	120.35	0	0	0	0	100%
linux_90	正常	0	120.01	0	0	0	0	100%
windows_12	正常	1	58.5	0.17	0.17	0	0	99.86%
windows_71	正常	0	116.56	0	0	0	0	100%
linux_1.11	正常	17	6.47	0.18	3.13	0	0	97.38%
windows-73	正常	0	115.68	0	0	0	0	100%
三、数据库								

图表 18 对象运行状态统计报表

4.10.2TOPN 排名分析

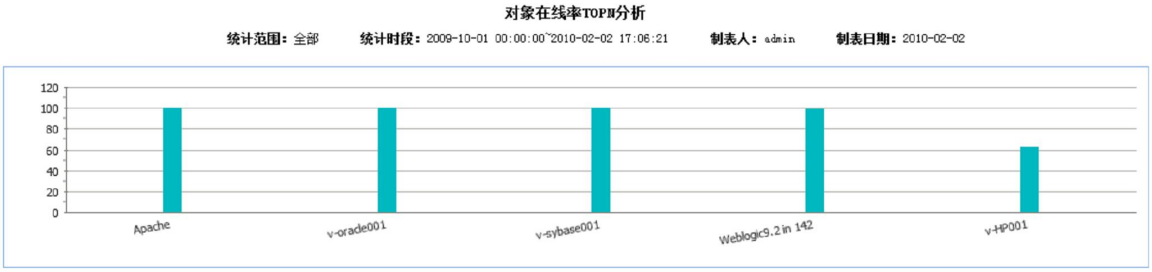
对监控对象运行状态及告警情况进行统计和比较，帮助运维人员分析 IT 环境存在问题，如哪些对象容易频繁出现告警事件？哪些对象在线率差强人意？哪些故障经常出现？图 19 是对象告警 TOPN 分析截图，图 20 是对象在线率 TOPN 分析。

	对象名称	告警次数
1	v-oracle001	97
2	Ubuntu95	7
3	linux_test	6
4	hpux-13	2
5	NetScreen25-T25	1

	对象名称	告警次数
1	NetScreen25-T25	0
2	hpux-13	0
3	linux_test	0
4	Ubuntu95	0
5	v-oracle001	0

	对象名称	告警次数
1	NetScreen25-T25	0

图表 19 对象告警 TOPN 分析

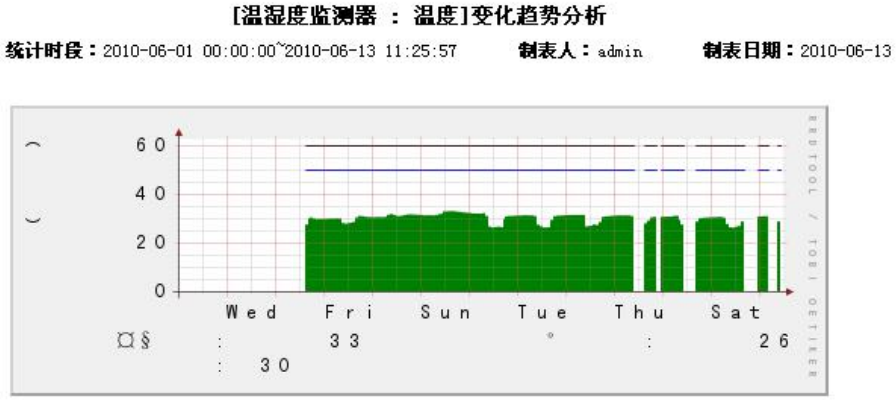


序	对象名称	统计时长	宕机次数	平均宕机间隔时间	平均宕机恢复时间	宕机总时长	计划停机总时长	不可达总时长	在线率
1	Apache	459.39	0	459.39	0	0	0	0	100%
2	v-oracle001	458.28	0	458.28	0	0	0	0	100%
3	v-sybase001	458.28	0	458.28	0	0	0	0	100%
4	Weblogic9.2 in 142	456.46	42	10.48	0.13	5.64	0	0	98.76%
5	v-HP001	458.28	4	71.14	43.43	173.73	0	0	62.09%

图表 20 对象在线率 TOPN 分析

4.10.3指标趋势分析

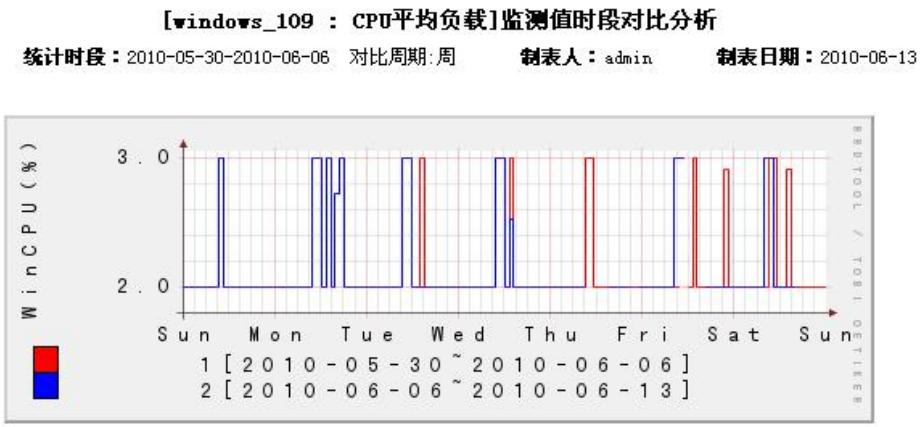
系统提供各种可用、性能和资源指标变化趋势分析功能，帮助运维人员了解各种指标变化趋势。下图是机房温度变化趋势分析。



图表 21 机房温度变化趋势分析

4.10.4时段对比分析

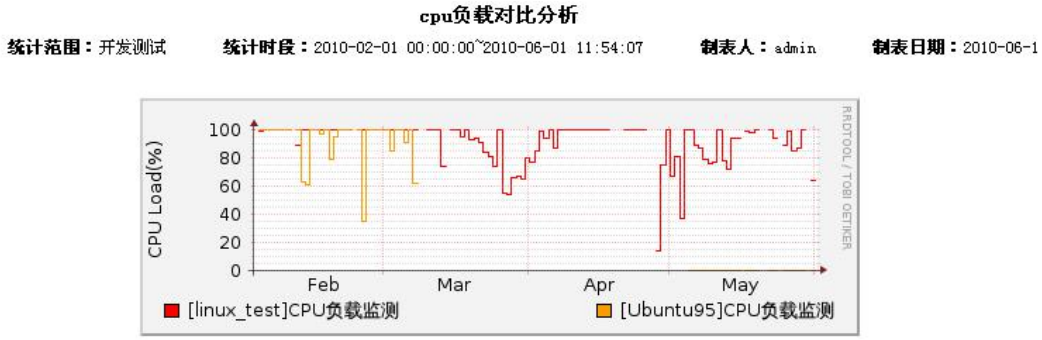
系统提供监控指标任意时段对比分析，下图是某主机 CPU 负载时段对比分析。



图表 22 某主机 CPU 负载时段对比分析

4.10.5资源对比分析

系统提供 IT 资源之间某种指标对比分析，下图是不同主机 CPU 资源利用率对比分析。



图表 23 不同资源 Cpu 利用率对比分析

4.11 安全管理

4.11.1支持 https 安全连接

平台可以根据需要开启 https 访问服务，增强客户端和服务器之间的数据通讯安全性。

4.11.2安全审计

平台对重要的数据维护和修改操作，进行日志记录，便于在数据异常时查找原因，确定是否出现越权和非法的操作。

4.11.3基于角色的人员管理

系统提供基于角色的安全管理策略，也可以从数据权限的维度，对人员和角色设置修改、查看的访问权限，极大地满足不同安全场景下的需要，比如管理、操作和审计等角色分开等等。

5 产品特点

- **监测全面,不留监控死角**

DCOM 监控平台涵盖了网络、服务器硬件、虚拟化平台、操作系统、数据库、WEB 服务器和中间件等各种 IT 基础设施的监控，除了对 IT 资源内部组件的可用和性能进行监控外，还通过主动模拟方式对资源提供的服务能力进行直接监控，并且还可以对 IT 资源的各种运行日志进行采集和分析，使监控真正做到不留死角。

- **面向预警，防患与未然**

一个好的监控产品，其价值不在于故障发生后如何告警，而是在故障发生前如何能及时预警，使 IT 运维工作真正做到“防患于未然”。DCOM 对每类 IT 资源都参考故障树分析(Fault Tree Analysis，FTA)方法自上而下仔细梳理可能导致资源不可用或性能下降的各种隐患点，然后再据此设计监控指标和参数，能够及时对可能出现的故障做出预警。

- **精确告警，避免告警风暴**

告警是监控产品最基本功能之一，但如何做到精确和智能告警并非易事。如果运维人员要经常面对大量、重复的告警事件，反而会因为监控工具引人导致运维人员工作负担加重和工作效率降低，就很难发挥监控产品应有的价值。DCOM 主要从 2 个方面解决这个问题：在告警产生层面，支持复杂告警逻辑，包括支持浮动阈值告警、事件相关告警、防抖动告警等，从源头上提高告警的精确性；例如对波动性指标，可通过设置合理持续时间去掉指标波动性

来避免误报；另外在事件处理层面，通过事件过滤、压制和关联分析功能，可以自动过滤不重要告警，压制重复告警和梳理告警之间关系，从而避免告警风暴发生。

- **高开放性与易集成性**

产品的开放性决定了产品的生命力，平台具有高度开放性和易集成能力，在数据采集、模型创建、事件转换、事件处理、可视化展现和统计分析等环节都提供用户接口或工具来帮助客户实现自己的个性化监控需求。

- **运维知识自动关联**

在事件处理时可根据事件内容自动关联运维知识库，可以极大地提高运维工作响应速度和质量。

- **丰富多样的告警通知方式**

系统提供短信、邮件、声光、桌面告警等多种告警通知方式，使告警信息及时准确地送达接受人。

- **模板化报表管理**

基于模板的统计报表，更容易满足用户个性化统计需求。

6 客户价值

1) 为客户提供一款 IT 基础设施自动巡检和监控工具，帮助运维人员从日常繁重的重复劳动中解脱出来，以便集中精力做更有价值的事情；
2) 帮助客户提高故障预警能力，真正做到防患于未然。有效的指标体系设计、复杂告警条件支持、准确有效趋势分析等有助于用户提前发现故障隐患并将之消灭在萌芽状态；
3) 帮助客户提高故障响应速度，提升系统可用率。系统强大的关联分析能力和自动 IT 运维知识关联等技术可帮助运维人员快速定位问题原因和获取问题解决方法，大大降低了故障恢复所需时间；
4) 帮助客户避免告警风暴，提高运维工作效率。基于规则的事件处理引擎可有效地对事件进行过滤、压缩和关联，可帮助用户从海量事件中自动寻找有意义的事件，极大地减少运维人员需要面对的事件数量。

关注公众号了解更多资讯