概要需求说明书

**V1.0**

**2018年11月**

**目 录**

[第一章 IT监控管理详细需求 4](#_Toc10199166)

[1.1. 总体需求 4](#_Toc10199168)

[1.2. 监控能力要求 4](#_Toc10199169)

[1.2.1. 监控范围要求 4](#_Toc10199170)

[1.2.2. 网络设备监控要求 6](#_Toc10199171)

[1.2.3. 主机设备监控要求 8](#_Toc10199172)

[1.2.4. 数据库监控要求 9](#_Toc10199173)

[1.2.5. 云资源监控要求 10](#_Toc10199174)

[1.3. 系统功能需求 10](#_Toc10199175)

[1.3.1. 网元配置管理 10](#_Toc10199176)

[1.3.2. 数据采集管理 10](#_Toc10199177)

[1.3.3. 告警预警管理 10](#_Toc10199178)

[1.3.4. 阈值管理 11](#_Toc10199179)

[1.3.5. 告警分析 11](#_Toc10199180)

[1.3.6. 告警展示 11](#_Toc10199181)

[1.3.7. 告警与故障处理 11](#_Toc10199182)

[1.3.8. 告警事件通知 11](#_Toc10199183)

[1.3.9. 拓扑管理 11](#_Toc10199184)

[1.3.10. 多维监控视图 12](#_Toc10199185)

[1.3.11. 业务系统管理视图 12](#_Toc10199186)

[1.3.12. 相关性分析 12](#_Toc10199187)

[1.3.13. 丰富的监控报告 12](#_Toc10199188)

[1.4. 系统非功能性需求 15](#_Toc10199189)

[第二章 IT运维服务管理详细需求 16](#_Toc10199190)

[1.1. 总体功能 16](#_Toc10199191)

[1.2. 服务目录管理 16](#_Toc10199192)

[1.3. ★IT服务台 16](#_Toc10199193)

[1.4. ★来电弹屏管理 17](#_Toc10199194)

[1.5. 事件及故障管理 17](#_Toc10199195)

[1.6. 变更管理 18](#_Toc10199196)

[1.7. 巡检管理 18](#_Toc10199197)

[1.8. IT 资产管理 19](#_Toc10199198)

[1.9. 知识管理 19](#_Toc10199199)

[1.10. 系统通告 19](#_Toc10199200)

[1.11. ★微信集成 20](#_Toc10199201)

[1.12. 运维质量分析 20](#_Toc10199202)

[1.13. 流程引擎 20](#_Toc10199203)

[1.14. 通知机制 21](#_Toc10199204)

[1.15. 升级与备份 21](#_Toc10199205)

[1.16. 接口要求 21](#_Toc10199206)

[第三章 云资源交付管理功能需求 21](#_Toc10199207)

[1.1. 资源服务目录 22](#_Toc10199208)

[1.2. 用户自助服务 23](#_Toc10199209)

[1.3. 云资源管理 24](#_Toc10199210)

[1.1.1. 资源池管理 24](#_Toc10199211)

[1.1.2. 编排管理 24](#_Toc10199212)

[1.1.3. 资源配置 25](#_Toc10199213)

[1.1.4. 资源配额 25](#_Toc10199214)

[1.1.5. 资源池概览 25](#_Toc10199215)

[1.1.6. 资源统计 25](#_Toc10199216)

[1.4. 公有云资源纳管 26](#_Toc10199217)

[1.5. 自动化运维管理 26](#_Toc10199218)

[第四章 运维安全管理功能需求 27](#_Toc10199219)

[1.6. 运维行为监控 27](#_Toc10199220)

[1.1.7. 操作行为监控 27](#_Toc10199221)

[1.1.8. 会话过程监控 28](#_Toc10199222)

[1.1.9. 违规行为处理 29](#_Toc10199223)

[1.7. 操作安全审计 29](#_Toc10199224)

[1.1.10. 日志安全审计 29](#_Toc10199225)

[1.1.11. 数据库安全审计 31](#_Toc10199226)

[1.1.12. 网络安全审计 31](#_Toc10199227)

[1.1.13. 主机安全管理 32](#_Toc10199228)

[1.8. 运维的准入、记录 33](#_Toc10199229)

[1.1.14. 访问授权管理 33](#_Toc10199230)

[1.1.15. 运维人员身份管理 33](#_Toc10199231)

[1.9. 安全事件的集中监控、预警和分析 35](#_Toc10199232)

[1.10. 系统非功能性需求 36](#_Toc10199233)

# IT监控管理详细需求



## 监控能力要求

### 监控范围要求

系统需对WEB、Email、DNS、FTP、ERP、CRM、MIS、中间件、财务、电子商务等应用系统从应用可用性、系统资源占用和性能指标三个层面进行全面深入的监测管理。

支持成熟的监控方式，对于宿主服务器的资源消耗非常少，不会影响到宿主服务器上正常业务的运行。提供基于SNMP和ICMP等协议的轮询监控方式，此方式目前极为广泛的用于对网络设备的监测。通过该模块可以全面监测整个网络体系，例如网络的连通性（Ping）及其网络设备（交换机、路由器、防火墙）的状态，如接口状态、接口流量、接口丢包率、路由器的CPU负载等。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **采集类型** | | **采集范围** | | | **指标数量** | |
| **主机** | | | | | | |
| HP-UX主机 | | | 文件系统、进程、文件目录、消息队列、端口通信、内存、CPU、磁盘、SWAP、主机网络、日志 | | 106 | |
| AIX主机 | | | 文件系统、进程、文件目录、消息队列、端口通信、内存、CPU、磁盘、交换区、HA、主机网络、卷组、vpath、日志 | | 149 | |
| Sun主机 | | | 文件系统、进程、swap、内存、CPU、磁盘 | | 53 | |
| Linux主机 | | | 文件系统、进程、文件目录、消息队列、端口通信、内存、CPU、磁盘、主机网络 | | 119 | |
| Windows主机 | | | CPU、内存、磁盘、进程、分区 | | 148 | |
| **数据库** | | | | | | |
| Oracle数据库 | | | 可用性、健康状况、性能、SGA、表空间 | | | 110 |
| Informix数据库 | | | 可用性、健康状况、性能、DbSpace、DbSpace Chunk、临时DbSpace、临时DbSpace Chunk | | | 63 |
| DB2数据库 | | | 连接性、事务、缓存、缓冲池、日志、锁、表空间、CPU使用情况 | | | 68 |
| DB2实例 | | | 代理统计 | | | 58 |
| SQL SERVER数据库 | | | 内存、缓冲管理器、统计连接、缓存明细、锁明细、事务统计、latch明细、访问方式明细、数据库明细 | | | 55 |
| MYSQL数据库 | | | 统计连接、请求统计、线程、访问方式、表锁、键效率、缓存 | | | 47 |
| **网络设备** | | | | | | |
| 网络设备 | | 路由器、防火墙、交换机等的CPU利用率、内存利用率、设备温度、接口运行状态、接口入速度、接口入利用率、接口出速度、接口出利用率、接口接收出错包数、接口发送出错包数 | | | 17，SNMP，可迅速扩充 | |
| **存储、备份、HA** | | | | | | |
| 存储 | IBM DS系列、HP磁盘阵列等 | | | 4 | | |
| 备份 | IBM备份。可迅速扩充 | | | 8 | | |
| HA | IBM HA，HP HA。可迅速扩充 | | | 32 | | |

（监控指标一览）

### 网络设备监控要求

监控内容包括实时监控网络设备状态、网络接口状态、链路运行状态、安全设备状态、加密通道及加密流量状态、隧道通断及互联状态、网络流量信息、网络整体性能分析。

展示内容包括全网真实拓扑、节点实时状态、链路实时状态、异常及告警信息。可实现声光电等多种告警方式提示管理人员网络的异常及故障。

分级管理包括总分支机构的综合展示，分支机构告警信息的共享与上报，系统策略的下发与执行审计，总控平台对分支机构系统的直接管理与运维。

具体指标包括：

1、网络拓扑管理

网络拓扑自动发现

能够采用多种算法，进行有条件的拓扑结构自动发现。迅速搜索整个网络内的所有节点、自动勾画出设备间的冗余连接、备份连接、均衡负载连接等。

拓扑发现的条件包括：特定网段条件，被管对象类型条件等。

支持物理拓扑发现和逻辑拓扑发现。

对于已经发现的某一个或某几个子网能够进行再次发现。

拓扑管理支持分层管理、子图缩略管理。

网络浏览功能、拓扑监视功能、拓扑编辑功能、拓扑被管对象管理、图例管理功能

2、网络性能管理

性能管理功能主要面向各类网络设备的性能综合监测和分析，应具有性能监测管理、性能数据上报管理、性能数据管理、性能门限管理、性能分析等子功能。

系统必须支持分布式数据采集，可以将不同网段范围的设备的性能数据交由不同服务器上的数据采集系统进行采集，并集中提供网管系统处理和访问；

系统必须能适应不同取数间隔，自动重用已获得的性能数据，避免大量重复取数造成的网络资源浪费；

系统必须提供SNMP OID方式能够把需要的性能数据提取出来做历史记录。

性能监测管理、性能数据管理、性能分析管理、性能TopN分析

3、网络故障管理

故障管理功能应具有告警监视与分析、收集与显示、告警确认与清除、告警过滤、告警级别管理，支持单点告警、复合告警、基线告警。

单点告警：以某一个条件检测管理对象是否触发告警。

复合告警：以某几个条件检测管理对象是否触发告警。

基线告警：以管理对象小时、日、周、月的运行数据为基准，某时刻超越该基准线则触发告警。

告警收集与显示、告警确认与清除、告警过滤功能、告警级别管理、告警通知与动作

4、分级管理

总部和各下属机构的管理系统，通过层次化管理功能，在总部对全辖范围内的IT信息资源进行集中管理，各下属公司根据总部制定的管理策略得到相应的权限，在本地通过本地的管理系统进行本地化管理；

最终要求做到“集中监控、分散管理”，以符合我方的行政管理架构。避免大集中管理带来的责权不清，容易扯皮的弊端，也避免纯分布式管理带来的难以统一规划资源、难以统一进行“同业对标”的不足。

具体来说：我们要求投标方提供的系统分为总部、下属单位二级网络管理模式，总部做为整个系统的网络中枢，下属单位为二级网络管理结点，建立一个安全、高效、先进的网络监控体系，确保各业务系统安全、高效、稳定地运行，提高管理水平，满足公司日益增长的服务需要，提供最安全最周到的服务保障，将监控系统集成化，网络化。实现对全公司网络系统、应用系统的属地化管理原则，实现两级监控、二级管理的信息网络综合监测管理模式。

我们要求系统可以在上级单位直接调阅各下属单位的网络实时物理拓扑结构（如远程设备的当前负载情况，端口状态，故障日志等等），实现全网运行率统计、配置和监控数据的上传下发、告警信息发送、全网IP地址联动、报表下发等管理功能。各个层次的相对独立性，上级部门在需要时可以对下级部门进行管理，保证整个网络管理的统一性和完整性。

要求系统支持将整个管理区域分为若干拓扑子图，通过建立拓朴子图和缩略图（双击可以展开显示）的方式，可以对拓朴图进行分布或集中式的监控。支持拓扑结构图的无级缩放、区域内设备整体拖动。

### 主机设备监控要求

* 1. 支持对AS400/Windows/Linux/Unix(HPUX、AIX、Solaris…)等多平台系统主机进行的统一监控和管理。
  2. 主机视图管理：
* 提供主机、机柜的逻辑与物理视图，集中监控全部主机，能直观看到各点是否存在故障及报警。
* 提供一个管理界面，方便的监控和管理服务器的性能、告警、配置信息。
* 对于有负载均衡的机器，提供负载均衡的链路逻辑视图及各节点的配置信息、物理主机信息等。
* 支持主机面板远端图形显示。
  1. 主机连通性管理:

提供直观的图形，显示主机各部分是否存在连通性方面的故障。

* 1. 主机运行状况监视管理:
* 提供监视主机的状态、网卡状态、机器温度和性能指标越界等故障告警。
* 监测多平台上运行的系统进程和服务的运行状况。
* 提供硬件报警故障管理（硬盘、电源、电池等信息）。
* 负载均衡状态监控。
  1. 主机性能管理:
* 提供监视管理非常广泛的性能测量指标（如CPU使用率、内存使用率，磁盘空间、虚拟内存、换页空间、进程、I/O吞吐、事务响应时间、网络接口和服务端口等等），如果出现内存或CPU故障或者未识别的情况能够出现告警。支持对单个指标进行阈值设定。
* 提供主机各容量指标增长性的分析，及时预警各容量可能达95%的时间推算。
  1. 主机安全性管理:
* 提供外网对系统访问的监控管理(监控记录操作内容、操作时间、登录的用户等)信息。
* 提供异常访问记录与监控：如同个用户，多次登录不成功；对系统参数修改操作记录；并能自动记录入事件管理模块。
  1. 可以对主机的配置信息改变进行监控和管理，包括主机名、IP地址、接口数量、设备厂商、操作系统版本、CPU个数、内存大小等配置信息。
  2. 可以监测系统日志变化情况，而且对监测结果支持匹配查询、设置过滤条件等方式进行更深层次的分析，通过服务器系统日志监测功能，可以帮助管理员更为准确地掌握重要进程或操作系统的运行状况。

### 数据库监控要求

实现对Oracle、DB2、SQL Server等数据库的监控管理。实现对数据库系统关键参数进行监控及管理。数据库采集，至少需提供JDBC和脚本两种采集方式根据不同需求实现对数据库信息的采集。

* 1. 数据库运行状态管理：
* 可以监控数据库运行状态，如数据库ID、数据库状态、数据库表空间（未分配、预留、索引、未使用）、连接数、回滚段、锁定总数、连接用户数、网络读取、写入等待、完成页面读取数、可用缓存等。
  1. 数据库性能及容量管理：
* 可以对数据库的性能，包括内存、Cache、IO性能、碎片、SGA命中率、关键表空间增长情况等进行监控；能够设定相应阀值，实现相关报警。
  1. SQL语句管理：

能够监控数据库的活动进程，以及SQL语句的执行状况等。

### 云资源监控要求

★云宿主机监控：支持对云环境物理宿主机进行监控，支持集成的ESXi、vCenter监控，监控主要从下面三个层次进行：宿主机层面，对VMware宿主机（Host）的CPU、内存、磁盘和网络等项目进行监测，对宿主环境 的每个存储的使用率，剩余量、总容量指标、IO流量等进行监测。

★虚拟机监控：提供虚拟主机基本信息采集，包括虚拟机性能、设备连续运行时间、设备描述信息，如操作系统、型号、IP地址、CPU型号、内存容量、硬盘容量等。支持虚拟主机文件系统、文件目录的磁盘空间、消息队列端口信息、Swap情况、网络流量、文件分区使用率等监控。

公有云监控：通过配置公有云管理账号信息，采用共有用开放的接口协议，可以自动对云服务器等资源进行导入并同步，并能够采集资源的配置信息、运行性能信息,从而将共有云资源统一纳入到集中的实时监控中心。

★云备份系统监控: 能够对云资源的备份系统进行自动监控，包括备份进程、备份实例有效性等能够自动识别，确保虚拟机、数据库等备份的准确和可靠。

## 系统功能需求

### 网元配置管理

可在任意网元类型建模的基础上建立某种类型设备的实例，将其纳入到的管理范围进行监控，以便对其进行性能分析、故障发现、告警等。

### 数据采集管理

可以对任意网元实现单独或批量的配置和修改采集方式、采集周期等策略。

### 告警预警管理

数据的分析处理支持灵活的参数和阈值设置、通过灵活的告警公式进行复杂的告警逻辑判断、提供告警和故障的直接处理、对于关键性的故障信息支持自动升级为事件处理流程，与统一流程管理直接对接，形成告警故障的闭环处理。

### 阈值管理

支持告警公式的设计和定义功能，用逻辑表达式的方式描述对特定故障场景的定义。

告警阈值可提供对历史趋势的分析判断，以提高告警的准确性。

### 告警分析

对接收到的故障数据、性能数据、配置数据分别处理，性能数据将根据所配置的告警定义进行告警分析判断，包括简单的阀值判断、复杂的逻辑算术公式、函数运算，生成原始告警信息。

### 告警展示

系统应有非常良好的故障表达方式，可以将复杂晦涩的技术术语转化为通俗易懂的语言。

### 告警与故障处理

实现告警的确认和维护记录的管理功能，相同告警再次出现时，能够查看到以往的维护记录并以之作为参考。

### 告警事件通知

告警通知功能是将经过告警分析判断、告警关联分析后的告警信息以短信、邮件、MSN、QQ等方式通知相关的运维人员；系统监控平台能够提供各种告警通知的接口，并能够从用户管理模块中获取系统维护人员的各类信息（如手机号码、Email等）；告警通知能够灵活定义，能够通过规则的设定，实现通知时间段的控制。

### 拓扑管理

拓扑图功能完全通过浏览器操作，可在界面上实际操作各种拓扑图的情况。可手动创建示意设备、示意链路，并支持拖拽方式修改拓扑图内容。可按设备类型、名称、IP地址，管理员可以快速定位网络拓扑图中的设备。拓扑图支持导出打印功能。

### 多维监控视图

系统提供多种不同角度的全景监控视图，直观地、综合性地、全面地反映系统管理对象的运行状态和告警，包括：

地理位置视图：从地理位置角度看所有系统管理对象；

逻辑拓扑视图：各系统管理对象的逻辑链接和分布；

物理拓扑视图：各系统管理对象的物理链接和分布；

应用系统视图：各应用系统所使用到的其它系统管理对象的链接和分布；

3D机房机架视图：从模拟3D效果的机房鸟瞰视图及机架正视图，快速定位故障设备位置；

所有视图直观的、美观的、可修改的（可增加、删除、修改其中的系统管理对象及其在图中的位置、连线、需要显示的状态参数等），并动态显示各系统管理对象的主要状态参数实际值和预警、报警；同时各个视图都能够按区域、按层次、按对象进入更细节的局部视图。

### 业务系统管理视图

能够实现基于业务系统视角的IT监控视图，实现业务逻辑支撑结构呈现，并能够提供业务系统自动化巡检功能。

### 相关性分析

系统应具有相关性分析功能，通过梳理设备-功能模块-应用系统-业务之间的对应关系, 当设备发生故障时，能够快速做相关性分析，找出这个设备的故障将会影响哪些系统和业务。

### 丰富的监控报告

综合报表和分析系统能完成各类数据和运行状况的分析，自动生成系统运行状况报告、系统事件报告、系统安全报告等，可以充分反映信息系统为业务提供服务的质量。

统计分析报表均采用全中文的界面，并能根据不同的用户角色定义不同的报表，使一般运维管理员、信息主管领导等根据各自关注重点，通过浏览器查看报表系统；

针对业务应用系统，形成反映各业务系统使用情况的报表（提供模版的方式便于用户自行定制统计分析报表），同时监控报表支持在一张报表中同时展现出与业务应用系统相关的各种被管对象的性能、告警等数据统计；

报表采用门户的标准进行管理数据展现，各类统计分析报表支持直接发布到门户，并支持报表订阅、个性化展现、SSO（单点登录）等门户标准功能；

能够提供柱状图、柄图、折线图、数据列表等多种灵活、形象的分析图表。且数据组合方式能够基于业务系统、部门划分、设备、时间段、TopN等多种查询方式进行，提供多种组合条件的统计分析；

具备多维数据分析统计能力，能够以多种层面和角度对运行数据进行钻取。可根据操作人员使用要求进行性能指标检索并统计结果；

能够按照使用的要求对网络系统的端口流量、链路状况、设备运行状况、系统性能数据、故障维护数据等自动生成相应的日报、月报、年报等；

能够对服务器、数据库系统、中间件系统的运行状况、性能数据、故障维护数据、安全状况等自动生成相应的日报、月报、年报等；

报表能够导出为excel、pdf、xml等多种格式用于数据交换；

统计分析报表界面风格美观大方，生动直观展示管理数据；

* 实时性能报表

实时报表提供某一监测器最近的12小时的报表，报表提供12小时以来某监测器的统计信息和详细信息，包括12小时以来数据采样的次数；监测器正常、危险、错误运行时间的百分比；监测器返回值的最大值、平均值；12小时以来按照监测返回数据生成的曲线图；以及12小时以来所有监测返回数据的详细监测数据列表。

* TopN报表

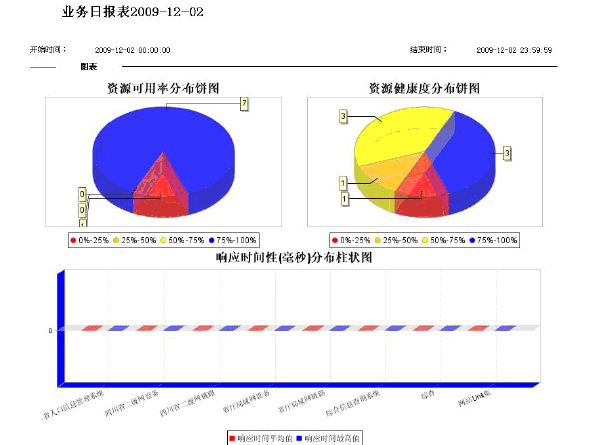
TopN报表列出同一类型监测中的前N项排序表。通过TopN报表可以很容易的将数据排序输出，根据排序方式的不同可以清楚的查看到数据的好坏情况。TopN报表是分析数据非常好的一种报表形式。

通过Top N报表，用户可以了解目前网络上运行最好或最差的网络元素,以及它们离目标的距离，为解决网络故障或升级网络提供数据支持。

* 告警报表

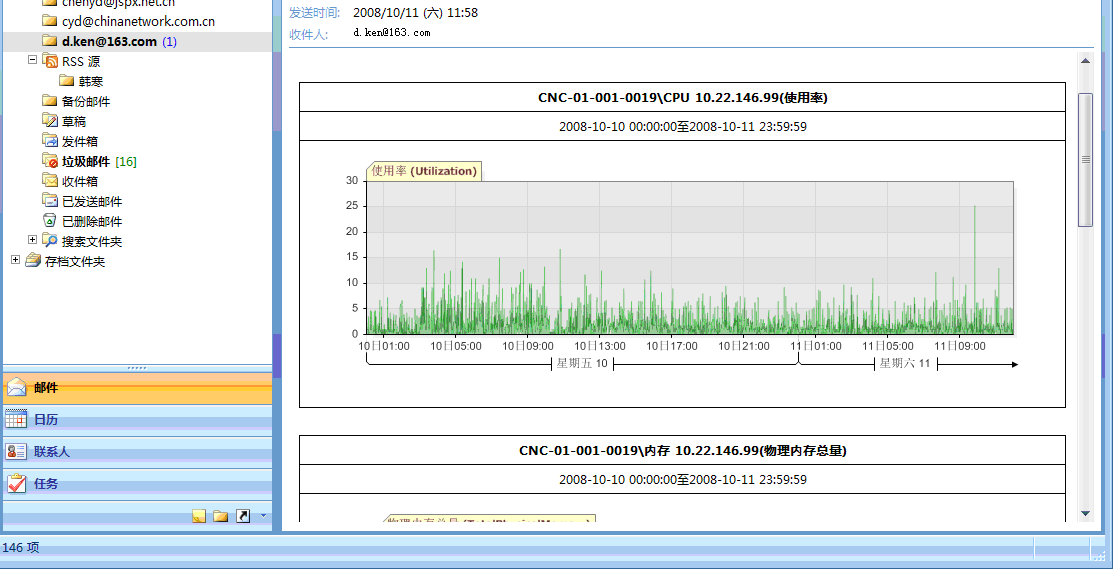
提供各种维度的告警分析功能，包括告警级别、告警设备、告警处理及时度等。便于用户对所关注范围内的设备进行整体性的审视，评估性能的瓶颈和故障的盲区，有针对性的解决和加强IT设备性能问题。

* 能力分析报表



* 邮件通知

系统包含的报表都支持用户订阅功能，系统会定时将相关报表通过邮件发送给订阅者，以图文并茂的方式进行展现：



## 系统非功能性需求

(1)符合行业标准协议，支持多种API，并针对用户提供定制化开发；(2)及时性：保证预警、警报、性能、配置信息能及时采集，实现告警信息压缩、关联定位、等级分类，采集周期可以自定义；

(3)可以自行定义各类数据的阀值及各类参数的关联关系，以便于灵活的组合和告警。

(4)准确性：保证信息采集准确可靠，采集的数据能够真实有效地反映系统管理对象真实情况；

(5)传输安全可靠：保证采集数据和故障事件信息的准确传输；

(6)采集方式的多样性：数据采集能够提供多样化的采集手段，完成对原始数据的采集；

(7)对于配置数据的采集以自动采集为主，不能自动采集的，才可以采用手工录入、批量文件导入等方式；

(8)数据采集不能对系统管理对象的稳定运行造成影响，增加新的系统管理对象时，要能方便纳入系统，不需修改系统核心功能；

(9)最少的资源占用：保证在系统管理对象上运行采集程序时，无论是硬盘占用空间、内存占用空间、网络占用带宽，还是CPU使用率都保持最小，最高不能超过系统资源的5%。

(10)能采用安全的协议和方式实现对不同安全等级区域中的系统管理对象进行监测和管理。

(11)具有自身安全性控制，包括用户访问权限、数据安全控制、通信协议安全等，用户必须具有分权管理功能。

(12)有很好的可扩展性，可以随着应用规模和管理需求的增加而不断扩展，并保证不同阶段实施的管理功能和结构的完整和统一，保护投资。

(13)需要支持J2EE架构，具有易于使用的web 使用界面，最终用户可以通过WEB登记服务请求，查看FAQ及服务处理结果等操作。

(14)必须提供灵活的服务支持权限管理功能，确保市与市、市与省中心的监控和运维管理工作彼此独立，但又能同时支持跨省市的联合服务流程操作。

（15）并发能力和响应速度：监控功能模块至少支持10个并发用户，服务流程功能模块至少支持50个并发用户，一般功能响应速度不超过1秒，复杂功能响应速度不超过3秒。

# IT运维服务管理详细需求

## 总体功能

以ITIL和ISO20000为信息化服务流程规范，统一制定我单位的信息化服务流程，并由运维流程子系统进行统一管理，对服务流程实行统一集中监控，提供直观的、美观的、图形化的监控视图，动态实时反映各项服务流程的执行情况和效率。

通过规范化的流程梳理，定义完善的服务台统一接入、服务请求及事件处理流程、以及其他信息化运维必须的流程。

系统应提供丰富多样的统计分析工具和图表展示， 以报表形式形成信息化运维管理周报及月报，用于分析和统计各项服务管理流程的执行情况及效率，为不断优化服务流程、提高运维服务效率和用户满意度提供依据。

## 服务目录管理

服务目录可进行数据配置，支持分级管理。

支持服务目录中的工作配套流程相关配置，通过配置相关配套流程，可让此服务项在配套流程的执行实例中对流程的相关数据进行考量和环节驱动。

**★**支持服务目录中的服务项的服务团队配置，通过配置服务团队，可让使用此服务项的流程实例按照服务目录的默认分配原则进行工作分配。

## ★IT服务台

服务台应作为信息中心与用户间的单点联系接口在运维工作总起着至关重要的作用。

服务台负责管理事件和服务请求，实现与用户的沟通和人员的协调调度。服务台应设计满足以下要求：

- 支持通过电话、网络、电子邮件等方式向用户提供单点联系接口；

- 支持定制工单分发策略，可以选择自动分发、手动分发等不同策略；

- 支持跟踪服务请求的处理情况，确保所有服务请求能够以闭环方式结束；

- 支持根据服务请求，自动关联出相关的知识库记录；

- 支持与短信平台对接，用邮件或短信方式将事件通知给相关人员。

提供专门的服务台操作界面，界面内容应包括：事件列表，来电列表，事件概览数据统计，事件申告趋势统计。

提供多任务窗口操作，使得服务台可在多个事件的操作间来回切换。

可直接申告事件，或通过来电弹屏等方式申告事件。

★自助服务台：提供专门针对用户的申告界面，用户可自助申告事件，页面简洁大方，功能完善（要求PC界面和手机浏览器两种界面，可通过在微信或手机第三方工具扫描二维码的方式进入手机浏览器页面。）

## ★来电弹屏管理

通过集成模拟电话识别设备（投标人提供），使电话与终端可以实时通讯，用户拨打电话到服务台座席后，系统能够自动弹出事件申告页面。

在弹出的事件申告页面中能明确展示出来电部门、电话、呼入号码、位置、姓名等信息。能展示响铃的本机号码。

能查询来电历史的相关信息，未接来电和未生成工单的来电信息，可以点击补录事件单。可使得服务台繁忙情况下分流一部分工作压力。

系统应提供来电弹屏转接功能，即电话与服务台所操作的电脑不在同一物理区域也可实现弹屏功能。

## 事件及故障管理

梳理流程，制定受理、处理、审核、关闭、通知的全流程管理，规范服务受理过程，使故障受理工作更协调，处理结果更有保证、客户满意度更高。

通过服务目录可自动分配流程流转的相关人员。具有工单通知功能，通过短信、微信或第三方平台实现工单流转后的消息通知功能，用于提醒下一环节人员及时处置。通知内容包括：事件名称、人员、电话等信息。

应满足对服务目录模糊录入。即，输入服务目录关键字，快速检索定位所需的服务项，方便服务台快速录入，提高故障受理效率。

应满足对人员以及组织结构的模糊录入。即，输入组织结构或人员的关键字，快速检索定位所需的信息。

应满足对事件标题智能录入。即，服务台录入事件标题，支持系统自学习功能，下次同类事件出现后，可以输入关键字，进行事件标题提示功能。

## 变更管理

需求变更管理：

变更管理流程：应包括以下几个环节 新建—>方案—>审批—>实施—>确认。

变更范围与内容：在一个变更单中需包括若干需求，审核人员可针对每个需求进行逐条审批。

基础设施变更：

变更管理流程：应包括以下几个环节 新建—>方案—>审批—>实施—>确认。

变更范围与内容：变更单可与配置库进行关联，通过变更单可查询配置库，并且通过配置项可查询到配置项的变更历史。

## 巡检管理

巡检计划任务管理：系统应能支持对巡检计划任务的配置，用以设置巡检的周期、巡检的类型、巡检的设备范围等信息。

巡检模板管理：对各类型资产进行巡检单配置管理功能，能够针对某个或某一类设备配置巡检项，提供可视化绘制巡检表单样式等功能。

巡检执行管理：系统应能支持安全管理工作中规定的巡检工作记录功能。巡检记录需要在巡检事件上进行提交，使巡检工作存档电子化。以便于审计、统计和管理。

巡检单归档：巡检工作结束并提交后，系统将巡检结果进行持久化保存，并能够进行打印，导出。

## IT 资产管理

围绕IT资产类型，构建符合运维工作需要的管理属性信息。通过梳理，帮助信息中心整理出一套能够时刻真实反映在线运行资产的配置情况，并对资产的部署位置、供应商、服务商、质保期、负责人进行统一的管理。

根据资产类型，可灵活扩展资产的属性，无需二次开发。

拥有资产信息版本管理功能，能够对资产信息的变动进行版本管理。能够查询出每个资产信息版本的详细信息。

**★**提供资产的二维码管理功能，微信端扫描资产二维码自动进行报障，自动关联资产信息、位置，故障现象等。

## 知识管理

提供知识类别管理，知识录入管理，知识使用管理、知识的评分管理。通过与运维流程的关联，实现运维人员随时随地可以参考知识库进行工作执行。

可通过事件进行知识的快速创建，也可单独通过知识管理进行创建。拥有知识评审流程，当知识经理审核后，知识才能正式发布。

用于区分知识的知识类别可单独维护。

知识进行查询时，系统可根据查询人所在的团体自动进行数据筛选，展示出符合此团体特性的知识。

服务台工程师可根据事件的关键字自动获得知识库匹配的知识，并进行故障解决。

工程师可在事件处理过程中查询出与该事件分类/关键字一致的相关事件及解决方案。并能通过操作直接引用知识。

## 系统通告

支持系统内的通知通告管理，通过选择部门或人员，向其发送系统内的通知。

系统应具备醒目的通知展示区域，提醒操作人员当前的待办工作和相关通知数量。

## ★微信集成

通过关注企业微信号，申告人员可通过进入事件或报障管理，进行事件的申告，工程师可进行事件的处理等操作。

在微信申告页，需要提供录音、拍照等功能进行事件申告。

拥有满意度调查功能，在事件处理完毕后申告人可对此事件进行满意度评价。

微信端能实时接受事件操作的相关提醒。

## 运维质量分析

操作视图：包括至少两个角色的操作视图（工程师以及领导视图），领导视图可对当前管理范围内的所有工单进行查询和查看详情。工程师或服务台视图可对自己管理范围内的工单进行编辑操作。

统计视图：提供服务请求分日申告趋势相关数据以及曲线视图，视图应包括事件工单的分日数量。

提供基于服务目录的整体数据对比统计，能统计时间段内的各个服务目录事件申告数量对比图，提供以处理人为维度的处理数量统计，并能以图形方式展示。

提供以服务台维度的处理数量统计，总体建单量，以及服务台人员每日的建单量，并能与来电数量进行匹配。

提供对于电话历史记录的相关统计，包括（电话有效转单数，找人电话数，无效电话数，未生成工单电话数）。

提供以巡检人为维度的巡检次数以及巡检质量统计。能够统计出没有按时完成巡检，逾期巡检积压数量的前5名人员。

大屏展示视图：支持页面的全屏展示，并能适应高分辨率大屏（高分辨率显示器终端或投影），展示当前的事件处置状态，提供对本月的还在处置中的事件统计，并根据服务目录进行分组对比。

## 流程引擎

流程引擎可支持对工单的转派，驳回，直接关闭等机制。

所有流程操作界面中，人员数据，部门数据，服务目录数据均支持模糊检索和动态下拉列表功能。

满足流程固有表单的同时，系统应支持根据不同的服务目录展示不同类型的工单。

## 通知机制

★可使用邮件、短信、微信等方式，灵活的通知相关人员

通知方式可配置，让操作人员可在工单的每步操作中选择各种通知方式。支持默认通知方式。

## 升级与备份

**★**数据备份：

系统界面应包含数据备份功能，通过操作系统后台界面对系统的数据进行备份。并能通过相关程序对系统数据进行备份数据的恢复。

系统升级：

应拥有完善的系统自身升级发布功能，能实现快速系统升级。在升级过程中拥有系统程序和数据备份功能，拥有健壮的回滚功能。

## 接口要求

★本系统能够提供其他系统对接。其他系统可通过接口向本系统进行事件变更等流程的发起；

# 云资源交付管理功能需求

实现传统物理IT设施及云IT资源的统一抽象，屏蔽底层平台技术差异及复杂度，对外能够为用户提供便捷的云资源申请开通、资源扩容、资源运维等自助服务，对内能够提供更加简洁的云资源规划、构建、分配、跟踪、回收等。

提供的自服务门户，用户可进行IT资源与服务进行自助申请、管理。用户在自服务门户上可根据需要填写资源与服务申请，包括资源类型、规格、存储、网络、使用期限等，并可对申请到的实例进行常规管理操作。

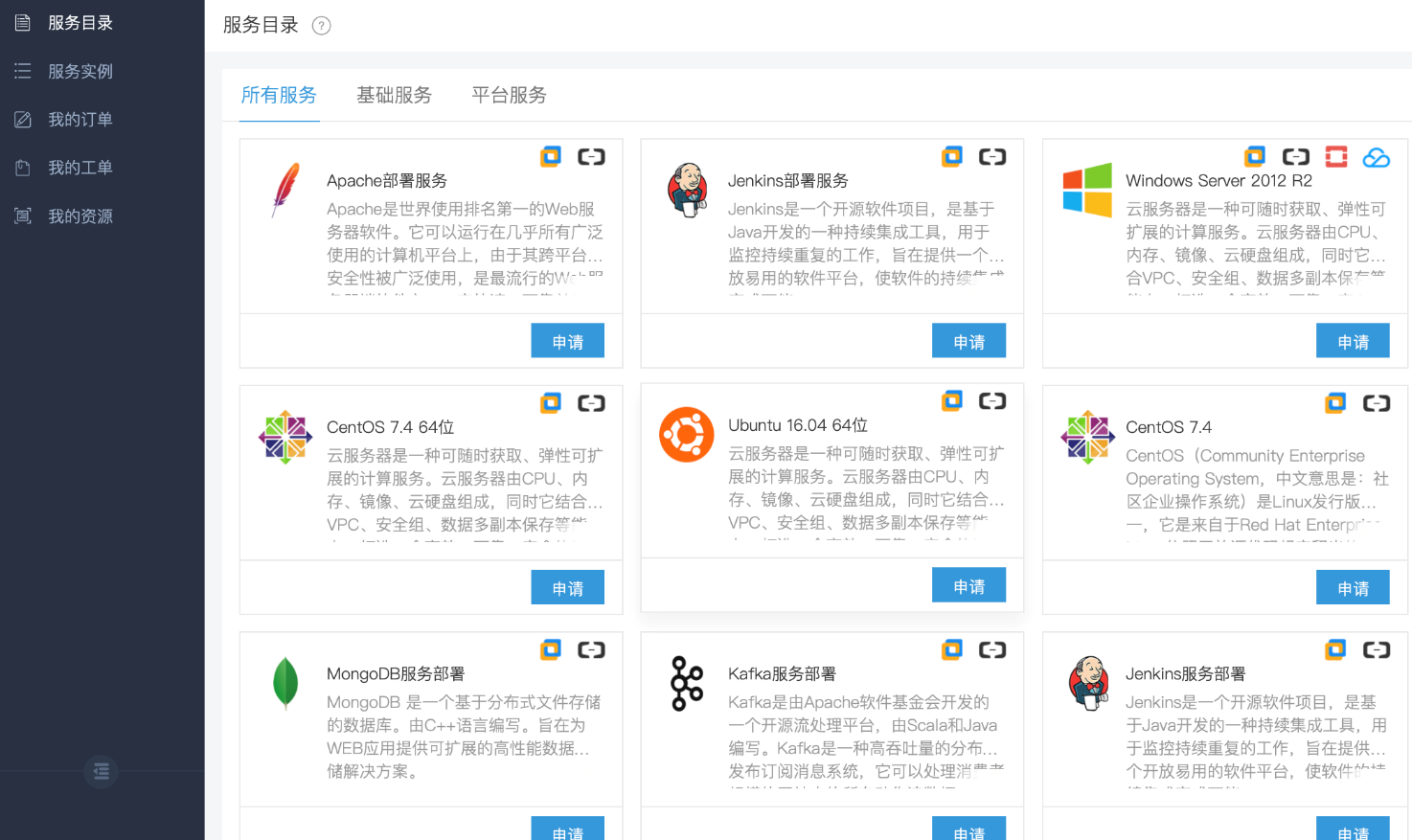
自服务门户提供工单功能，通过工单功能，用户可对IT资源与服务的申请和使用遇到的问题/需求进行提交反馈。

利用服务编排等手段大幅提升IT资源交付能力和管理能力，除了基础的虚拟机交付能力外，同时支持应用性组件交付、软件及集群的交付，甚至是应用架构的自动交付，支持将传统数据中心的一些管理职能如虚拟机快照、容灾、数据备份等作为服务提供给最终用户，全面提升云的交付能力。

## 资源服务目录

云管理平台具有强大的资源抽象和提供能力，能够将不同的云平台资源以标准服务目录方式向用户发布，便于用户申请利用，满足企业部署开发环境、生产环境、应用升级等多种应用场景，实现集中管理普遍部署的IT服务。

提供自定义多种类型、多级别的服务目录，可以对云平台中资源，如：虚拟机、数据库集群、应用集群、备份系统等提供资源服务，也可对运维类操作，如：资源编排、作业面板、软件安装等功能提供运维类服务。



平台管理员可以根据用户需要，方便的创建自助服务目录，以便用户能够顺利的实现对各类资源的使用。

## 用户自助服务

自助式服务门户为用户提供的集申请、使用和管理云资源为一体的门户。在规格化自助服务目录基础上，通过流程化服务模板和操作向导帮助用户快捷开通云业务,IT用户通过门户站点提供的各种云应用服务，可方便快捷的完成复杂资源的申请，资源的运维；运营管理人员可以方便快捷的进行云资源规划，服务发布，资源审核等；管理人员可以通过门户查看资源池的利用情况以及使用状态。

资源申请

用户通过资源服务目录，选择需要申请的资源类型（虚拟机、数据库、备份存储等）和配置信息，按照系统设置的申请流程完成资源的申请和生成过程。

用户资源申请自服务通过流程的方式进行审批，审批流程支持创建自定义审批策略和审批流程，支持配置多级审批，以确保满足各业务要求。并可以针对不同资源服务、组织、用户配置不同的审批流程。审批环节支持短信、邮件等方式通知相应责任人，申请人可查看资源申请进度，流程完成后自动生成资源实例并通知申请人资源开通信息。

资源变更

用户可以对在用的资源进行配置变更申请，按照系统设置的流程完成资源的配置的审核和生成。

资源释放

用户可以对不再使用的资源进行释放，释放的资源将自动回收到对应的资源池，供其他场景使用。

资源操作

用户在自助服务界面，可以对拥有的资源进行各种运维操作，如开机、管理、重启、远程登陆、备份、恢复等操作。

资源监视

用户在自助服务界面，可以对拥有的资源运行状态信息进行详细查看，包括虚拟机运行信息、数据库、中间件运行信息等。

同时用户也可以对所拥有资源的整体情况进行查看，按照资源分组、分类等维度掌握资源的利用情况。

## 云资源管理

云管理平台以资源服务为中心来简化资源管理，支持资源的定义、发布以及生命周期各项操作功能；支持通过资源编排定义灵活的资源模板，为IT用户提供更贴近应用的云资源交付。

### 资源池管理

平台提供虚拟资源池管理功能，虚拟资源池可将环境中的各种资源（存储、计算、网络）、物理资源、虚拟化资源、公有云资源，统一导入形成统一的虚拟化资源池。

平台能够通过不同类型资源的底层接口，配置资源池接入参数，包括VMware、Oracle数据库集群、应用集群、备份系统，读取资源池的基础信息、配置和容量信息等，为后续其他功能实现提供基础。

支持其他类型资源接入机制，如openstack、其他公有云等，为未来提供扩展的空间。基于底层云设施的接口能力，可以实现对存储池的管理，支持对SAN、NAS、分布式存储的接入和管理功能、支持网络资源池的管理，支持IP、VLAN等的分配和管理、支持IP使用情况的统计及可视化展现等。

平台支持资源的分类/分组管理，支持以配额限制的方式进行逻辑池划分、自定义命名。

平台支持资源的分配、利用管理，支持资源与项目/用户的映射关系。

平台中已存在的资源或由管理员新建归属于项目、项目用户的资源，可通过再分配、迁移的方式分配给其他的项目组或用户。

### 编排管理

基于资源类型的开放接口，实现资源模版管理功能，具备模版库管理功能，支持不同资源池内创建模版、以及基于模版创建虚拟机、基础数据库等应用环境。具备镜像库管理功能，包括镜像的导入、导出、下载等功能。

支持管理员通过编排设计、发布主机镜像模块、数据库模版、应用服务模版、脚本等，并提供版本管理。

虚拟机模版还可以支持为主机添加不同的执行脚本、设置不同的配置参数。

### 资源配置

支持按照用户申请的资源规格，经过审批后，自动依据预置模板完成资源的自动开通。系统支持多级部门的设定以满足不同类型的审批需求，同时结合角色、流程、权限组功能实现在操作、查看、审批等不同层面的合规性。

支持管理员后台手动批量创建虚拟机，并同步完成自定义主机命名及随机密码配置功能，满足企业云平台中批量大规模创建虚拟机的应用场景。提供创建时虚拟机定义“标签”功能，自定义描述归属关系，满足客户应用场景。

支持虚拟机和软件的全生命周期管理，具备到期前提醒、到期后关机、过期后回收的机制，并可设置每个区间的时间间隔，适用开发测试之类的特殊的资源回收等场景需求。

### 资源配额

平台提供资源配额管理能力，在实际应用中可以根据情况选择启用或停用。

配额管理对用户、部门、项目组、应用系统对资源使用进行配额设置，超限时自动触发告警；提供对平台下各用户户资源使用趋势图查看，并支持按周、月、年显示；对各类云资源使用率进行细粒度的统计分析，通过预测模型对容量实现未来使用预测。

### 资源池概览

以多个视角对平台中的所有的资源进行可视化展示，实时查看云环境下的资源的保有、使用水位和报警情况。资源概览可自定义展示模块，根据企业真实应用场景灵活定制。对不同云平台总体资源统计和分析；实时呈现宿主机和虚拟机资源性能及使用状态；

### 资源统计

提供完善的运营统计和资源成本计算能力，可以辅助实现各类内部统计/考核等需求。

支持各类报表的统计，便于开展各类的统计和分析工作，如闲置虚拟机、需要扩容的存储、需要扩容的资源池、部门/应用使用排名等。

实现对常规的计算资源、存储空间、网络资源、应用的统计；实现对备份服务、数据库服务等云服务的统计；实现对总资源池和各级别资源池的容量管理及各类统计；实现对各类型资源的库存统计，并具备扩容倒计时的验算；

支资云资源池的全局利用情况、各个分中心资源利用情况、各个业务和资源关系、部门和资源关系、人员和资源关系。

支持云资源账号的统计分析，生成账号的活动、静默等信息，辅助完成账号的分配、回收等管理。

## 公有云资源纳管

系统通过对各类商用公有云接口的对接集成，实现与私有云资源一致的管理接口和操作界面，从而实现对公有云资源的统一规划、配置、申请、开通、回收的全生命周期管理。

同时结合公有云资源的计费模型，核算云资源的成本支出，及时反馈云资源使用期限等能力。

## 自动化运维管理

基于DevOps运维理念，为IT资源使用者提供业务应用和基础架构的自动化能力。

(A)平台提供自动化调度引擎，内置丰富的运维操作，能够灵活编排各种资源运维场景，标准化各种操作流程，可根据企业现状按需扩展，并可以通过编写脚本，按需扩展实现特定功能，更加符合企业运维自动化需求。最大限度的节约运维成本、降低管理风险、提升运维效率和服务满意度。

(B)系统提供常规任务编排和调度能力，支持编写shell、bat、python等类型脚本，实现各类常规定时性任务的执行，用户可以针对单资源实例/或批量资源进行执行并查看跟踪执行进度。

(C)内置操作系统安装（IPMI/PXE）支持，以及资源管理、应用件部署、业务脚本调度等各个层面的运维操作，像搭积木一样设计自动化流程，满足各种运维场景，实现从底层到业务的全栈自动化交付能力，大幅提升运维管理效率。

(D)平台提供可视化编排设计器，可编排各种运维场景的自动化流程。系统内置高效的作业调度引擎，对并行作业的执行过程进行详尽记录，提供可视化跟踪和控制界面，让一切操作尽在掌控之中。

提供基于自动化管理引擎，在内部源、镜像库、脚本库、工具库的基础上实现工作流的自定义，从而提供批量化、自动化的创建虚拟机、软件、集群、应用架构的自动化部署等服务。

提供基于处理故障类型的分组，关联设备、脚本，并通过一键执行的方式来解决和处理问题（如：一键重启服务、一键清除日志、一键关闭接口、一键配置、一键备份数据、备份验证等）。用户设定规则（基于监控系统的告警），由告警触发脚本、作业等实现故障自动处理。

# 运维安全管理功能需求

运维安全审计是信息安全体系建设的重要内容，是制度执行的有效保障。

企业信息安全审计系统主要定位于安全运维的服务层，覆盖各类安全服务及流程，包括用户授权检查、安全接入，该平台也是资源层各类安全事件和安全信息的汇总，采集各种安全信息和安全事件进行分析、过滤后，筛选出需要处理的事件或问题送往现有的IT运维管理平台启动相应流程进行处理，同时根据需要结合安全事件等级程度，报送到省局现有企业信息安全审计系统。

系统通过B/S方式(https)进行管理，其主要功能为实现对运维人员操作服务器、网络设备、数据库过程的记录，以及违规操作行为的阻断与审计功能。系统采用先进的软件架构，支持对多种远程维护方式的审计功能，如字符终端方式(SSH、Telnet、Rlogin)、图形方式（RDP、X11、VNC、Radmin、PCAnywhere）、文件传输（FTP、SFTP）以及多种主流数据库的访问操作，能够满足不同用户的审计需求。

## 运维行为监控

### 操作行为监控

对所有操作行为，企业信息安全审计系统能完整记录操作过程。访问记录由操作日志和回放文件两部分组成，记录内容包括操作时间、IP地址、用户账号、服务器账号、操作指令、操作结果等信息。系统管理员即可通过操作日志查看详细操作指令，也可通过录像回放查看详细的操作过程。

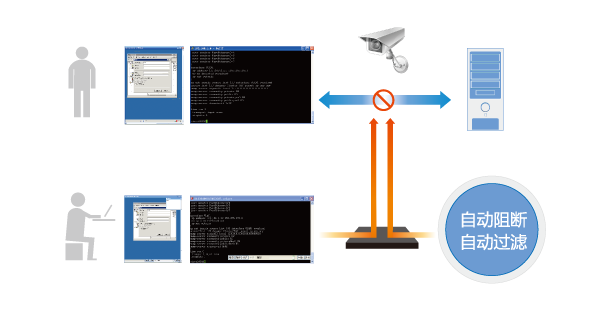
对于所有的操作记录，企业信息安全审计系统可以长时间进行保留，为日后安全审计提供客观依据。



### 会话过程监控

对于所有远程访问目标设备的会话连接，企业信息安全审计系统均可实现同步过程监视，运维人员在服务器上做的任何操作都会同步显示在系统管理员的监控画面中，包括vi、smit以及图形化的RDP、VNC、X11等操作，管理员可以根据需要随时切断违规操作会话。

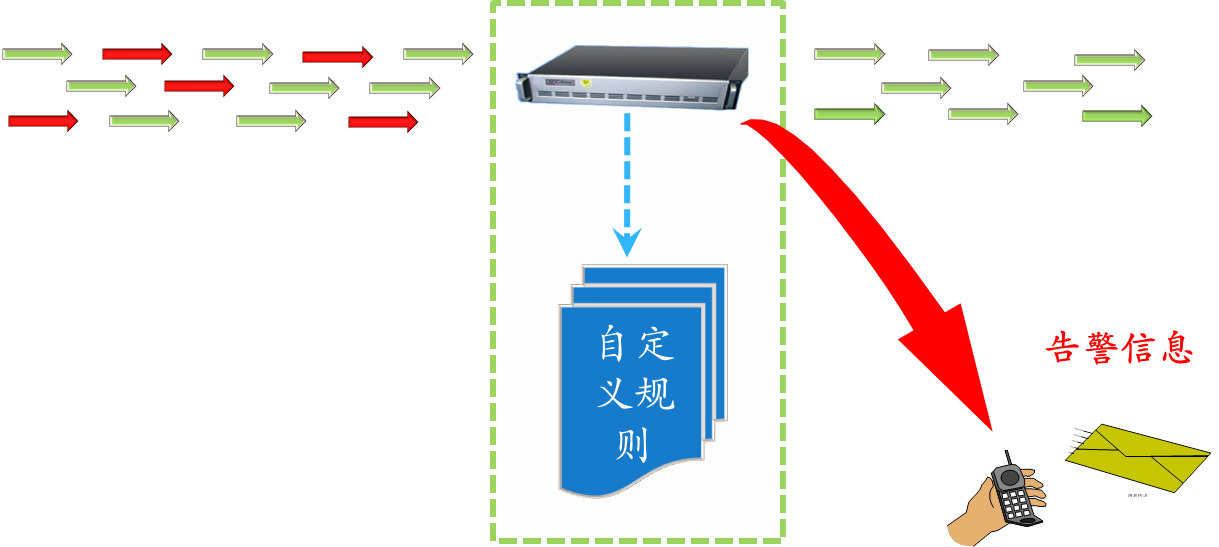
企业信息安全审计系统应能以视频回放方式，重现维护人员对服务器的所有操作过程，从而真正实现对操作行为的完全审计。



### 违规行为处理

企业信息安全审计系统应内置安全事件规则库，可实时对操作过程进行检测，安全事件规则库支持自定义扩充功能，管理员可以根据内部管理需求，灵活扩充规则库内容。

安全事件规则的设定应具有灵活性，系统管理员可对异常行为的内容、安全事件等级、安全事件分类、作用对象等条件进行配置，并设定相关处理方法（发送告警至运维系统并启动事件流程、阻断会话、忽略指令、锁定帐号）。根据配置的安全事件规则，企业信息安全审计系统发现违规操作行为后，向现有的运维管理系统发送告警，启动相应的事件处理流程（系统管理员可在系统中对每条告警信息增加批注），并通过短信、邮件等方式向系统管理员发送告警信息或自动中止操作会话。



## 操作安全审计

### 日志安全审计

全面收集安全和系统审计信息，有效地对来自异构系统的所有安全事件数据进行监控，通过归类、合并、关联、优化、直观呈现等方法，使系统管理员能够识别网络环境中潜在的恶意威胁活动。通过跨平台的集中管理，集中收集来自不同操作系统服务器、安全系统、以及第三方网络和安全设备的日志和事件信息，从海量数据库中精确识别出关键的安全事件数据，帮助降低受到来自外界和内部的恶意侵袭的风险。

日志审计系统应涵盖信息系统各个层面的支撑资源，包括网络层、主机层、应用层等各个方面，具体描述如下：

网络安全设备日志：防火墙、防病毒系统、VPN、IDS/IPS等设备，其信息源包括Syslog日志和OPSEC LEA协议日志；

操作系统日志：包括Microsoft Windows系列产生的系统事件日志（Event Log），Unix/Linux产生的SYSLOG日志；

Web服务器日志：Microsoft IIS服务产生的应用事件日志（Event Log）、Apache产生的Error Log等

应用系统平台日志：包括应用服务器（如WebSphere）、邮件服务器，FTP服务器的系统告警日志文件；

数据服务层日志： 数据库的用户访问操作等日志；

 企业信息安全审计系统要求进行日志审计分析，为此要对网络环境中的网络设备及系统平台的日志信息进行内容采集，具体要求如下：

A、安全设备的采集内容：

  安全设备系统事件记录；

  配置发生修改记录；

  规则/策略更新记录；

  动态连接记录；

  授权访问记录；

  拒绝IP连接记录；

  应用记录（FTP,HTTP等）；

  安全事件记录；

B、操作系统的采集内容：

  采集系统日志，包含由 Windows 系统组件记录的事件；

  采集应用日志，包含由应用程序或一般程序记录的事件；

  采集安全日志，诸如有效和无效的登录尝试等安全事件，以及与资源使用有关的事件，

  探测CPU、内存、磁盘、接口流量利用率；

  探测服务和TCP连接数；

  如启用DNS、域服务，还需采集DNS日志、目录服务日志、文件复制服务日志。

C、Web服务的采集内容：

 IIS WEB服务产生的启动和错误日志；

  采集Apache产生的error.log文件里的启动和错误日志；

D、应用服务平台的采集内容：

  采集应用服务系统日志；

  探测应用服务的关键进程运行情况；

 E、数据库的采集内容：

  采集数据库系统日志，启动、登录、错误；

  探测数据库的关键进程运行情况；

### 数据库安全审计

数据库系统及其数据是核心资产，各应用系统操作的本质是基于数据库的操作，数据库系统的安全性是系统安全运行的关键。为应对目前数据库和应用系统在逻辑和技术上层出不穷的安全漏洞，以及监督管理制度缺乏有效执行保障的现状，企业信息安全审计系统必须与数据库进行对接，建立完善的数据库安全审计平台，从根本上杜绝任何技术手段或违规操作对数据的非法获取和篡改。通过监听方式，实时第三方获取、保留网络中所有数据库客户端和服务器间的用户对数据库系统的访问操作，对各种违规行为或高危行为进行综合审计，并以通知、报表形式提交给安全管理人员，真正实现对数据库资源的有效管理。

### 网络安全审计

企业信息安全审计系统应提供网络安全审计，主要用于监视并记录网络中的各类操作，实时地综合分析出网络中发生的安全事件，外部事件如外部入侵行为和内部事件如内部人员的文件拷贝、信息获取、信息发布、资源变迁等，并根据设置的规则，智能地判断出违规行为，并对违规行为进行记录、报警。企业信息安全审计系统自身的数据具备防销毁、防篡改的特性，能够为网络犯罪案件的侦破和取证提供精确、宝贵的辅助数据，最终在内部局域网上建立完善的安全预警和安全应急反应体系，为信息系统的安全运行提供保障。

对系统的功能具体要求如下：

* Telnet审计：

系统能够审计Telnet应用：对于telnet应用，能够记录telnet连接的所有信息，包括输入的命令和回显的界面，并且系统能够根据vt100标准将用户操作的界面完全还原出来。

* HTTP审计：

系统能够对用户访问WEB进行审计，对于满足审计条件的HTTP应用，审计系统能够记录HTTP连接的信息，并且能够根据一定的标准将用户访问的信息还原。

* FTP审计：

系统能够通过用户设置条件，对网络中的数据包进行分析，对于满足审计条件的应用，审计系统能够记录FTP连接的所有信息，并且根据协议标准将操作命令还原。

* 专业的规则设置

企业信息安全审计系统需要提供一个功能强大的、易于升级的安全规则定制向导。这些安全规则覆盖了主机、网络、关键业务和数据库平台等各种情况下的安全规则，用户可以按需要，直接使用或者更改定制好的安全规则。用户也可以依据自身的特定安全需求，制作或是定制安全规则向导，保存后应用于安全体系中的各个设备上，达到全网安全策略统一的目的。

### 主机安全管理

###### 1）、访问方式管理

企业信息安全审计系统必须所有主机（包括小型机和PC服务器）、网络设备（交换机和路由器）、平台软件等进行对接，将主机进行细化分类，如网络设备、DB2数据库、Windows 2003服务器等，从而明确主机类型，确定对接方案，在企业信息安全审计系统的主机配置界面，系统管理员还可按协议及端口设定相关主机访问方式，并支持修改协议默认端口。

###### 2）、主机账号管理

企业信息安全审计系统支持主机帐号托管功能，可选择按协议填写相应主机帐号及密码;也可不填写帐号及密码，待连接目标设备时手工输入。

###### 3）、主机账号自动改密

企业信息安全审计系统提供主机密码管理功能，可以周期性对主机密码进行自动修改，用户还可根据需要设定密码强度策略。在每次自动改密后，企业信息安全审计系统将自动生成密码文件，密码文件可本地下载，也可自动发送到管理员指定的邮箱中。

企业信息安全审计系统可以自动对密码文件进行高强度加密，密码文件的读取需使用企业信息安全审计系统专用解密软件，并结合管理员帐号密码，从而确保密码文件的安全性。

## 运维的准入、记录

### 访问授权管理

企业信息安全审计系统应对运维人员进行访问权限管理，以黑白名单的形式严格限制运维帐号访问的主机IP地址、协议及访问时间段，支持以组形式（用户组、主机组）批量授权。同时还可设定同一时间某一运维帐号只能使用一个IP进行登录，以及设定访问无操作自动中断连接的时间阀值等功能。

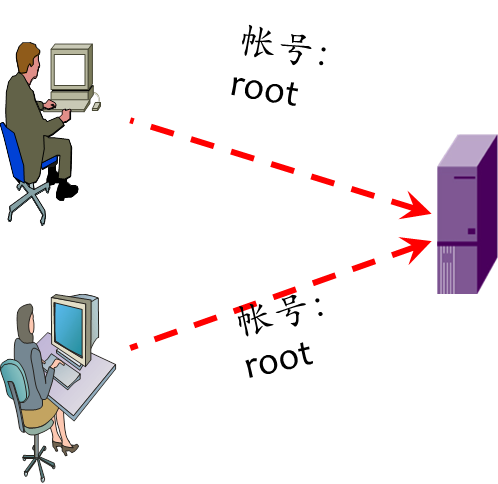
企业信息安全审计系统还可对具体的操作指令进行授权管理，以黑白名单的形式严格限制会话中某些操作指令的使用，支持以组形式（用户组、主机组）批量授权。在告警配置中，还可设定违规操作响应方式（忽略指令、阻断会话、告警），并可配置多种告警方式，如syslog、短信、邮件等。

企业信息安全审计系统还支持审批功能，对临时开放的特权用户，每次连接目标设备，必须得到管理员的审批通过方可连接目标设备，避免临时人员在管理员不知情的情况下进行访问。

### 运维人员身份管理

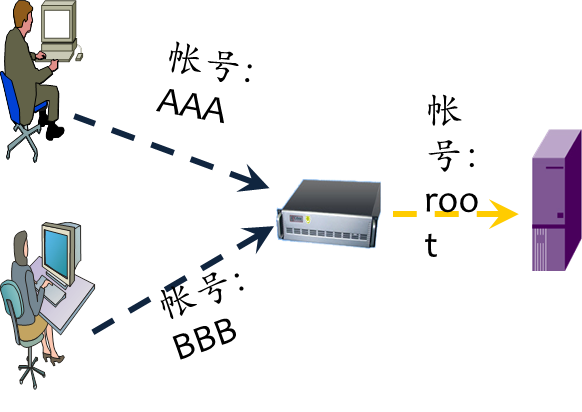
###### 1)、身份认证

为提供安全保障和防护能力，企业信息安全审计系统的安全认证和授权机制，通过身份认证、访问控制、权限管理等技术措施，进一步提升企业信息安全审计系统的身份认证能力，使其具备高强度的身份认证和责任认定机制，从而保证系统安全性、保密性和行为的不可否认性。



###### 2）、身份鉴别

为避免信息系统维护管理过程中，多名运维人员共用同一系统帐号进行登录访问，导致安全事件无法清晰定位责任人的情况。企业信息安全审计系统在设计上应通过“企业信息安全审计系统帐号”与“服务器帐号”相关联的方式，为每一个运维人员创建唯一的企业信息安全审计系统账号，运维人员先通过该帐号登录企业信息安全审计系统，再登录目标服务器，从而将登陆人员身份认证落实到“自然人”。



###### 3)、属性管理

在企业信息安全审计系统系统中，管理员可为每个运维用户填写详细的用户信息，包括姓名、部门、手机、email、密码等，并可设定运维用户帐号的有效使用期限。

###### 4)、运维帐号安全

在企业信息安全审计系统中，管理员对运维帐号可根据需要启用、停用或锁定，从而确保运维帐号的合理使用。同时管理员还可配置相关运维帐号密码策略，设定最小密码长度、密码使用期限、密码复杂度要求及帐号锁定策略等管理功能。

以上功能要求必须在企业信息安全审计系统上必须实现，为信息系统安全运行提供保障。

## 安全事件的集中监控、预警和分析

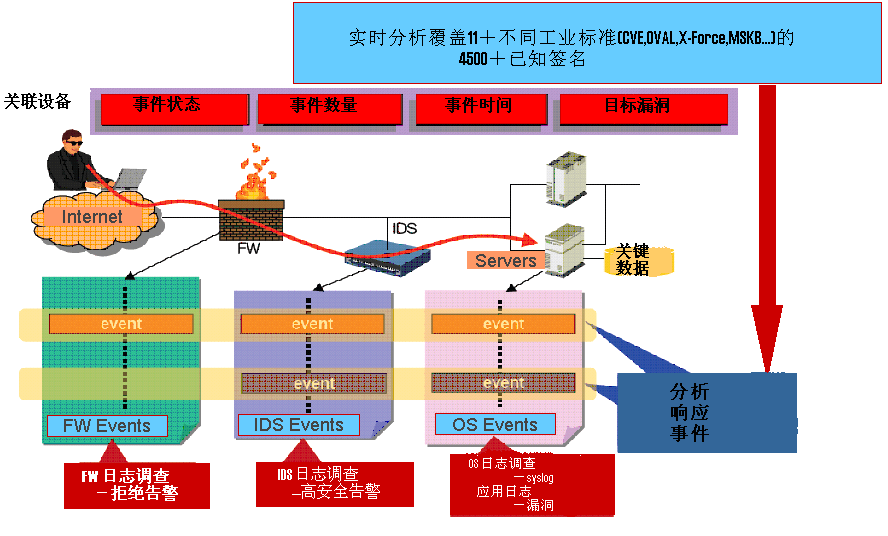
通过跨平台的集中管理，集中收集来自不同操作系统服务器、安全系统、以及第三方网络和安全设备的日志和事件信息，从海量数据库中精确识别出关键的安全事件数据，通过海量日志快速分析与检索系统，全面掌控设备的安全状态，协助管理员快速发现、关注与定位事件，从而实现安全事件的集中监控，降低受到来自外界和内部的恶意侵袭的风险。

系统应支持安全事件的预警机制，提供多种信息通知机制，如邮件/短信等，并对安全事件按照级别/资产等维度进行直观的展现。

系统应支持对海量安全日志的关联性分析，能够根据事件的类型/资产源/IP

以及资产间关系对安全事件的影响范围/根源进行分析和挖掘。

系统应在对收集的事件进行详尽的分析的基础上支持丰富的报表，实现分析结果的可视化，帮助管理员对安全事件进行深度的挖掘分析。提供多种报表模板，以支持管理员从不同方面进行安全事件的可视化分析，对于分析结果提供表格及多种图形表现形式（柱状图、饼图、曲线图），使运维人员能够一目了然。



## 系统非功能性需求

系统须在技术上达到当前的国际先进水平，采用最先进、成熟的理念、技术和产品，以达到总体建设目标。要求既满足目前的业务需要、保证系统的顺利实施和稳定运行，又充分考虑未来的发展。

选用符合国际标准的系统和产品，以保证系统具有较长的生命力和扩展能力，满足将来系统升级的需要。系统基于业界流行的三层架构设计，支持主流的应用服务器和数据库，支持多种主流的操作系统。

为了保证整个系统中模块的协同运行，且考虑到系统投资的长期效应，系统的设计预选性必须注重开放性，即构成系统的各产品必须符合国际标准和工业标准，以满足系统的可扩展性、可移植性和互操作性的要求。

采用高可靠性能的软件平台，使全系统具有高度的可靠性。采用多层次的冗余备份手段和技术，保证设备在发生故障时能在最短时间内恢复，以最大程度地保证系统的正常运转,满足7\*24小时不间断工作，系统的年可用率应大于99.9%，保证系统的可靠性和安全性。

系统要满足不断发展的业务需求。系统将随着架构的发展而发展，适应这种发展的要求，随着业务的增长和应用水平的提高，系统具备平台级开放式架构，有丰富的二次开发接口，可平滑地扩展和升级，而不需要对网络结构和设备以及软件平台进行大的改动。

系统具备很强的易用性要求，具有全中文界面，操作简便且具有良好的可管理性，具有监测、故障诊断等功能，以便于系统的管理和维护；同时尽可能选取集成度高、模块化、可通用的软件产品，便于管理和维护。

系统应在健壮性方面提供很好的支持，具备完整的数据校验、容错性及一致性指标。

系统应采用先进成熟的技术，以保证投资的有效性和延续性。

软件版本升级或改进应在不影响业务的情况下进行，保证系统可以稳定、平滑过渡。