文档编号：20180814-DLK-001

**XX省医保管理局**

**医疗保险省级安全体系建设项目需求规格说明书**

**(版本号:1.0)**

目录

[1 平台功能 3](#_Toc522005819)

[1.1 功能整体说明 3](#_Toc522005820)

[1.2 系统功能架构 3](#_Toc522005821)

[1.2.1 省局功能模块 3](#_Toc522005822)

[1.2.2 地市局功能模块 4](#_Toc522005823)

[1.3 部署架构 4](#_Toc522005824)

[1.3.1 省局部署服务器 5](#_Toc522005825)

[1.3.2 地市局部署服务器 5](#_Toc522005826)

[1.4 平台功能点 6](#_Toc522005827)

[1.4.1 基础设施监控 6](#_Toc522005828)

[1.4.2 资产配置管理 12](#_Toc522005829)

[1.4.3 安全合规管理 16](#_Toc522005830)

[1.4.4 云和虚拟化管理 19](#_Toc522005831)

[1.4.5 运维流程管理 25](#_Toc522005832)

[1.4.6 大屏展示 29](#_Toc522005833)

[1.4.7 统计分析 30](#_Toc522005834)

# 平台功能

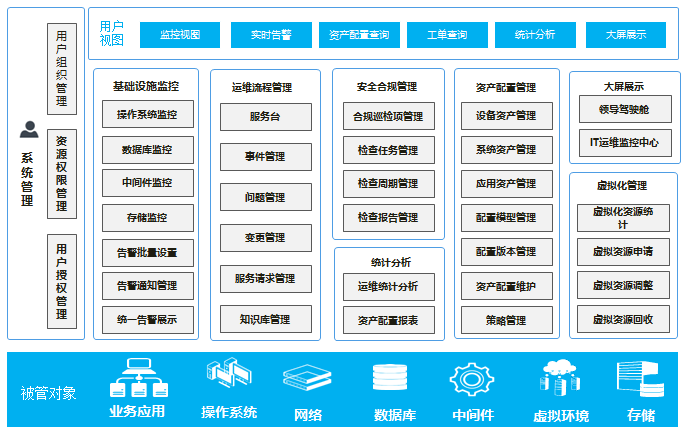
## 功能整体说明

建立集中的基础设施监控管理，全面覆盖服务器、数据库、中间件、网络、存储等IT基础资源，将网络设备、服务器、数据库、中间件、存储等告警信息进行统一整合，以最直观的方式统一显示相关告警信息；全方位的配置信息管理，实现配置模型、属性、关系的灵活定义，以及配置信息批量导入功能；安全合规巡检管理模块实现重要系统服务器的安全合规检查；通过运维流程管理构建标准化IT服务管理体系，促进贵局运维工作高效展开。推动运维工作流程规范化，提升工作效率。建立知识共享机制和主动查询、关联，为系统管理人员开展运维工作提供便利。

## 系统功能架构

### 省局功能模块

信息安全集中管控系统由不同管理模块组成。系统将功能进行模块化拆分，可根据用户需要、灵活选择业务实际所需服务，本项目根据实际需要，省局功能：基础设施监控管理、资产配置管理、安全合规管理、虚拟化管理、运维流程管理、大屏展示、统计分析。



### 地市局功能模块

地市局功能包含：基础设施监控管理。

## 部署架构

信息安全集中管控系统，既实现对省级数据中心的监控，也实现了各市级数据中心的监控管理。采用省级集中管理、地市分布式部署的二级架构，实现全省集中监控告警和地市告警处置的功能。在覆盖领域上，要对医保管理服务信息系统所依赖的所有IT资源进行监控，包括网络设备、服务器、操作系统、数据库、中间件和存储、虚拟化等监控告警。



### 省局部署服务器

省局一级机构部署服务器包含应用服务器、数据库服务器、采集服务器、代理采集agent服务器。

### 地市局部署服务器

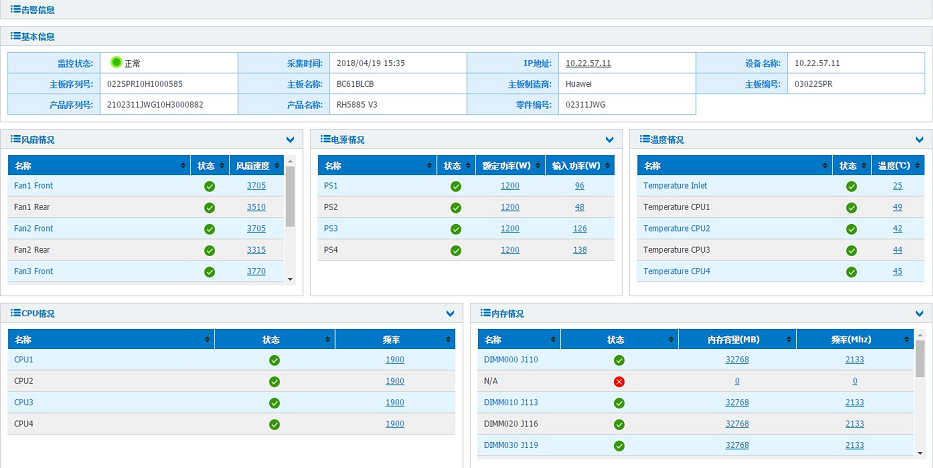
地市局二级机构部署服务器包含采集服务器、代理采集agent服务器，数据统一上传省局数据库服务器，统一访问省局应用服务器。

## 平台功能点

### 基础设施监控

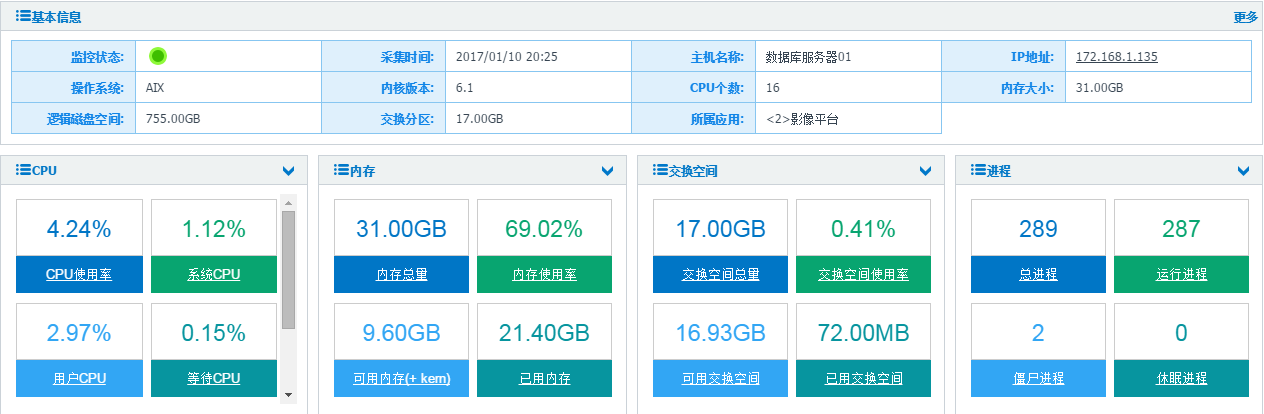
#### 硬件监控

平台支持对X86服务器硬件的远程监控，包括H3C、浪潮品牌，指标包括电源、风扇、CPU、内存。



#### 操作系统监控

系统支持本地Agent模式监控，支持Linux、Window系统监控。监控指标包含CPU使用率、内存使用率，磁盘使用率、文件系统使用情况、网卡流量、进程状态、进程使用CPU情况、进程占用内存大小、僵尸进程等；



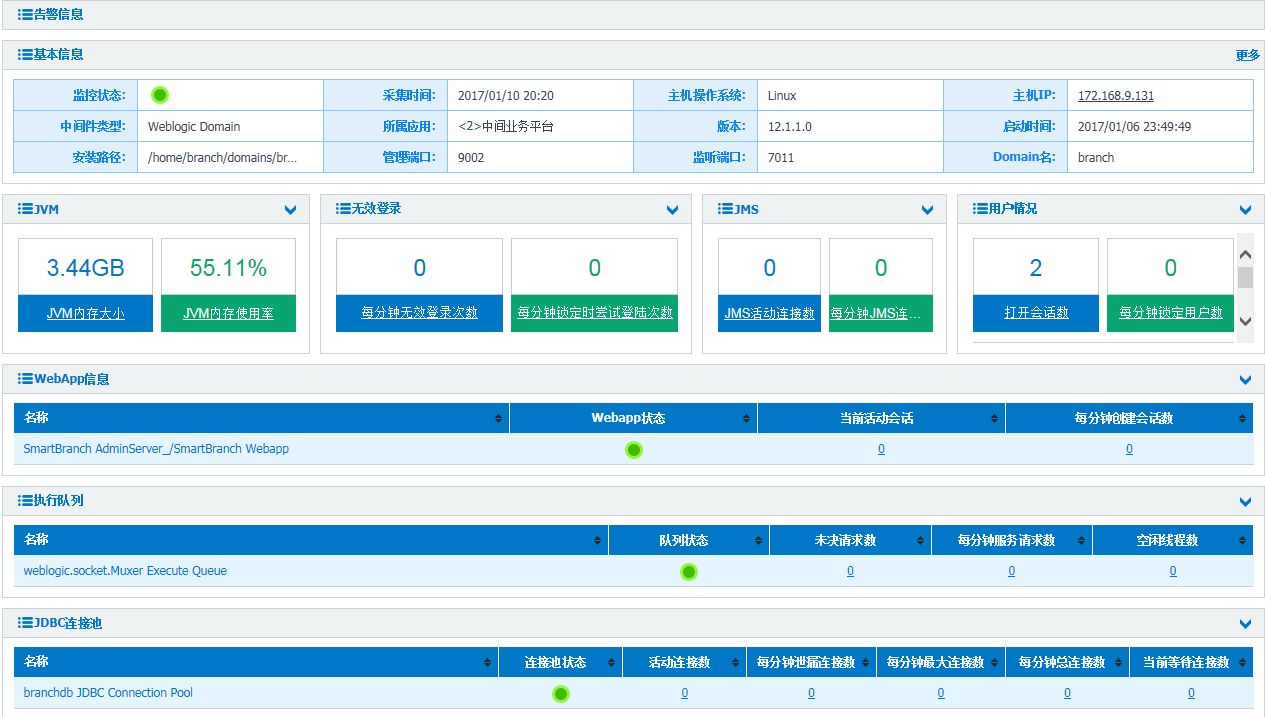
#### 数据库监控

支持数据库类型包括Oracle、SQL Server、MySQL，监控指标包括：数据库连通性、SQL执行耗时TOP5、SQL耗CPU最高TOP5、SQL耗内存TOP5、表空间利用率排名、每分钟用户提交数、表空间运行状态、表空间使用率、磁盘使用大小、实例可用性、当前登录的活动数等。



#### 中间件监控

支持中间件类型包括Weblogic、Tomcat，监控指标包括：服务可用性、JVM总大小、JVM已用大小、应用可用性、连接池可用性、连接池大小、活动连接数、等待连接数、创建连接数、活动线程数量、会话创建数、无效会话数等。



#### 光纤交换机监控

支持对博科、IBM品牌光纤交换机监控，主要监控指标包含硬件风扇、温度、电源状态，以及各个端口状态、传输情况。



#### 网络设备监控

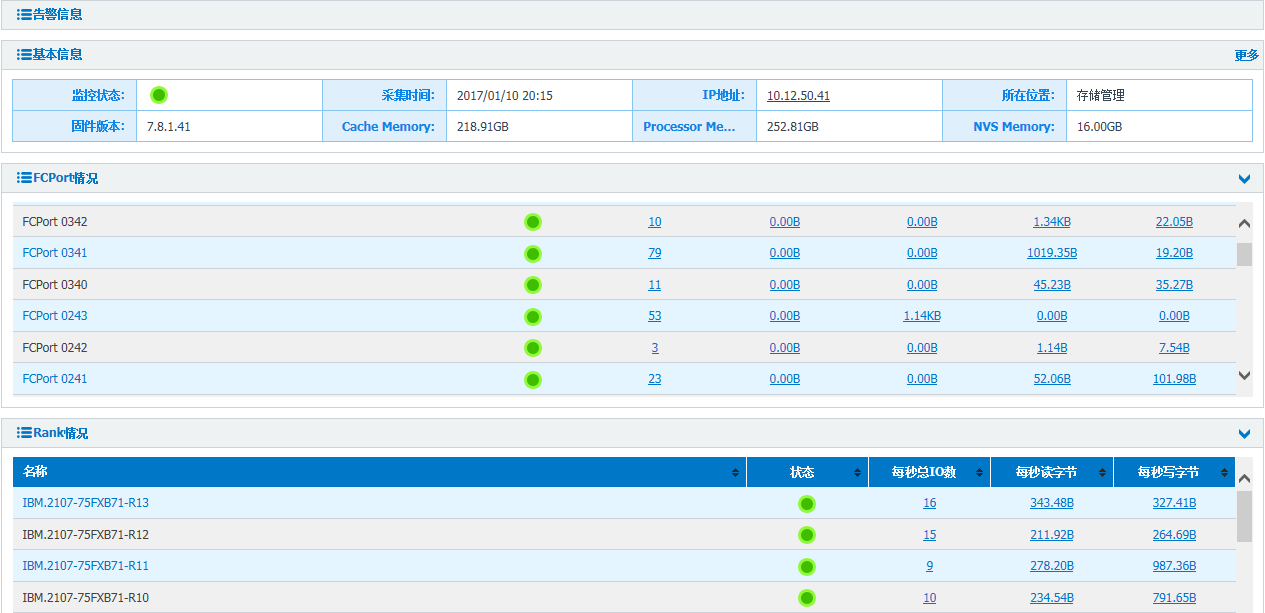
网络设备监控支持路由器/交换机监控类型包括：思科、华为、华三等。

主要监控内容包括：

设备的CPU负载、内存利用率、内存总大小、端口状态、端口速率、接口流量、入带宽利用率、出带宽利用率、端口丢包数、入流量、出流量、输入丢包数、输出丢包数、输入错包率、输出错包率、设备的端口速率、设备各接口的I/O流量，区分入流量及出流量。

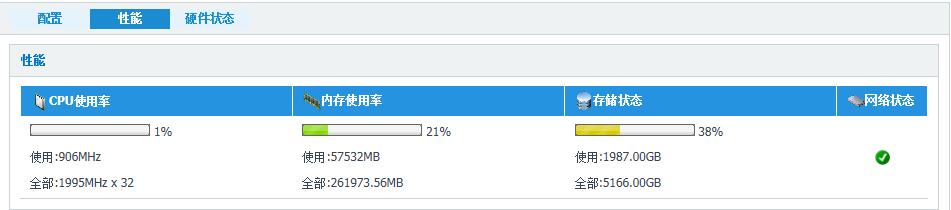
#### 存储监控

支持存储设备监控，包括HP、IBM品牌存储设备，支持的监控指标包括：容量情况、Volume性能、前端口性能、DISK性能等。



#### 虚拟化监控

支持VMware虚拟化监控，支持监控Host的运行状况、网络状态、CPU使用率、内存使用率、存储容量；支持监控Host硬件状态，包括处理器、内存、风扇、温度、电源等。



支持虚拟机运行状况、网络状况监控，包括：CPU使用率、内存使用率、分区文件系统使用情况、存储使用率、虚拟磁盘读写速度、网络性能、僵尸虚机等。



#### 统一告警管理

建立统一的告警平台，支持通过告警平台整合所有监控的告警信息。实现告警信息的统一展示、告警通知方式的统一设置以及告警通知方式的统一实现。



#### 告警规则定义

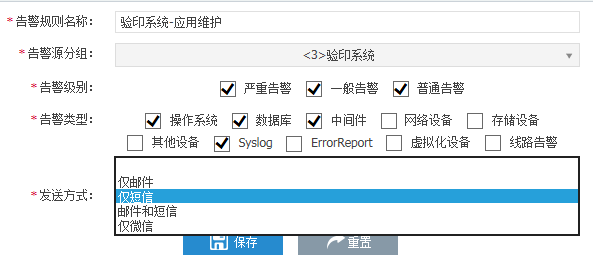
在采集到监控指标后，系统可根据运维实际需要，在平台中对采集指标进行告警设定。平台能够提供对告警规则灵活的增、删、改、查功能，告警的标题、正文、级别、阈值、分类可以灵活定制，告警规则有重复告警的过滤和计数机制。



#### 告警通知设定

支持告警通过多种方式通知给相关人员，包括短信、邮件等方式。

支持告警通知根据相应监控设备的管理权限发送给相关人员，支持根据不同的告警级别发给不同的管理人，需要支持不同时段的不同通知方式。



### 资产配置管理

#### 配置模型管理

##### 配置模型定义

配置模型管理为IT资产提供配置项类型和属性的定义管理，能够可视化的定义配置项类型、属性和配置项之间的关系。



##### 配置属性定义

配置项属性定义支持文本框、文本域、下拉列表、多选、日期、数字控件、附件、其他配置模型；配置项属性支持多种类别，实现类型化管理。以根据业内经验进行分类，包括：基本属性、配置属性、运维属性、机房属性、维保属性多种属性类别；能够结构化管理配置项属性。



#### 配置信息维护

配置信息维护为IT基础设施及组件、应用及服务提供统一的配置信息维护功能，包括配置信息录入、配置信息导入和配置权限的管理，同时支持维护配置项信息、配置项属性信息及配置项关系信息。



#### 配置版本管理

系统支持配置版本管理功能：

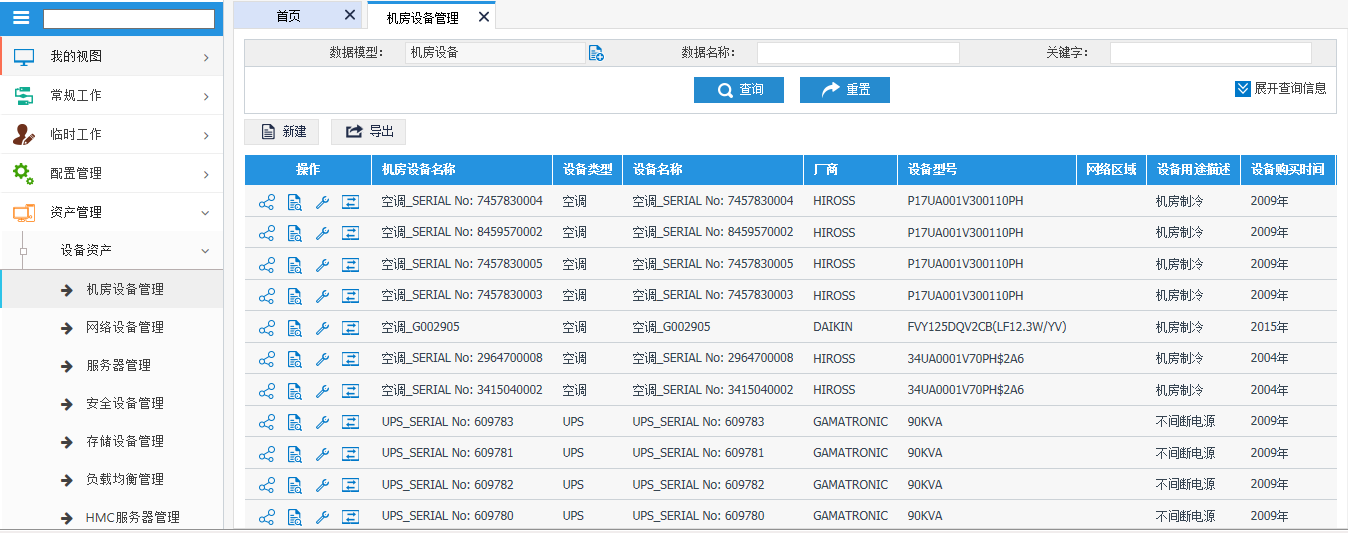
* 配置信息具有版本号，系统需要能够对配置信息进行版本管理；
* 历史版本查看，能够查看或回溯配置历史版本，能够查看历史版本的详细配置及其属性信息；
* 历史版本比较，支持比较不同版本之间的差异，列出配置属性信息的差异性。



#### 设备资产管理

设备资产管理对大型机、小型机、服务器、PC、机房设备以及其他终端设备及其配置属性、运维属性、机房属性、维保属性等进行全面的管理。主要功能包括：

* 支持对设备详细信息进行登记，同时可管理其基本属性信息、配置属性信息及运维属性信息等；
* 支持建立及维护设备与其他资产之间的关联关系；
* 支持历史版本比对功能，支持查看资产各版本信息变更对比情况。



#### 系统资产管理

系统资产管理，支持对安装后形成的系统资源，如操作系统、数据库、中间件等系统的维护信息、使用信息、详细配置信息及与关联信息等进行统一管理。主要功能包括：

* 支持对系统资产详细信息进行登记，同时可管理其基本属性信息、配置属性信息及维保属性信息等；
* 支持建立及维护系统资产与其他资产之间的关联关系；
* 支持历史版本比对功能，支持查看资产各版本信息变更对比情况。



#### 应用资产管理

运维人员需要准确掌握各种不同应用资产的具体情况，以便对应用系统进行有效管理。

应用资产管理支持对业务应用系统的开发信息、维护信息、使用信息、配置信息以及其他关键信息进行统一记录与管理，满足日常工作和业务管理的需要。主要功能包括：

* 支持对应用资产详细信息进行登记，同时可管理其基本属性信息、配置属性信息及维保属性信息等；
* 支持建立及维护应用资产与其他资产之间的关联关系；
* 支持历史版本比对功能，支持查看资产各版本信息变更对比情况。



#### 策略管理

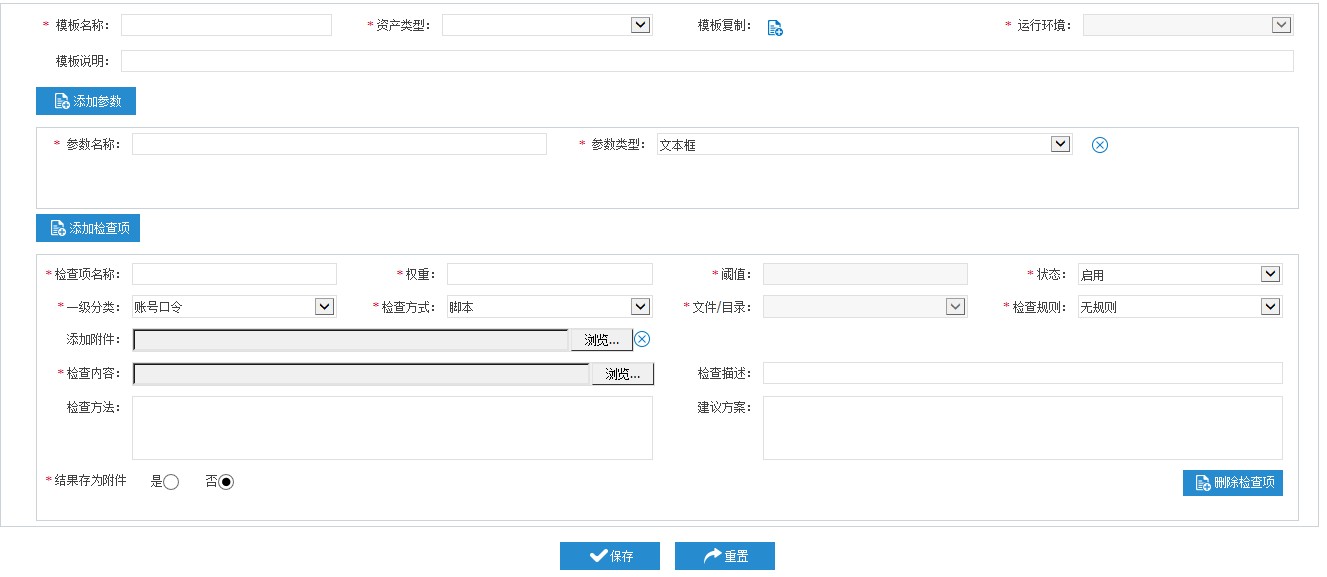
防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。吉林医疗保险管理局、地市局因业务需求，下属各自的定点药房、定点医院需要访问医保的应用系统，需频繁的对防火墙策略进行调整，为提升工作效率，我司将根据业务特点和不同防火墙命令集，将已通过审批的请求进行自动化调整。

### 安全合规管理

信息安全集中管控系统各功能模块采用均为同一个数据采集代理agent来实现监控、合规巡检，针对不同类型对象的巡检要求提供多种检查模板，通过检查模板可批量设置检查对象。在确定检查对象基础上，可帮助运维人员建立并管理巡检任务，同时支持同一任务设定多个对象，并提供自动化检查任务周期管理，可对运维人员进行工作提醒。

#### 合规模板管理

针对不同类型对象的安全合规要求提供多种检查模板，通过检查模板可批量设置检查对象。

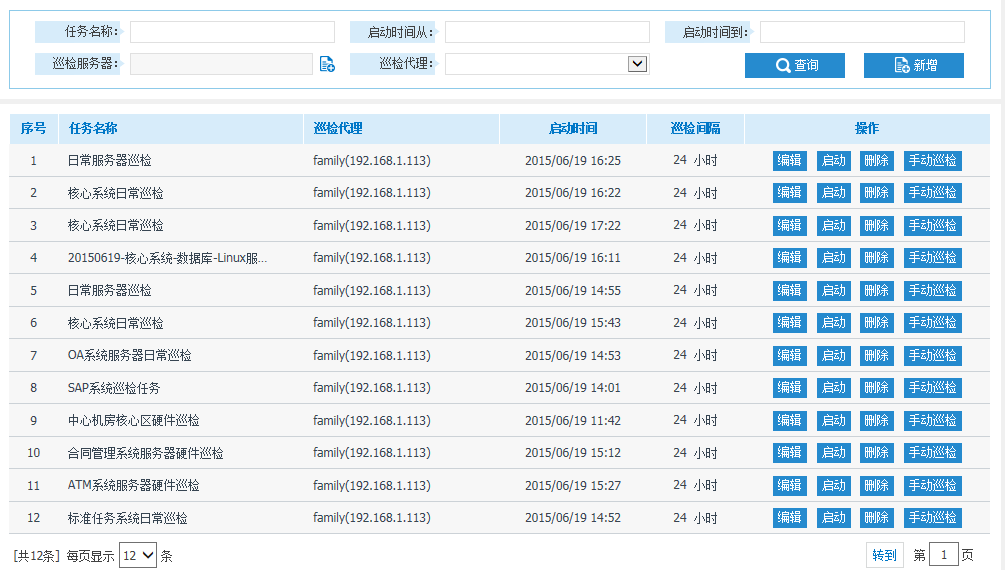


#### 检查对象管理

将主机划定为检查对象，设定检查项，统一管理检查对象及其相应的检查项。

#### 检查任务管理

确定检查对象，在此基础上，可帮助运维人员建立并管理检查任务，同时支持同一任务设定多个对象，并提供自动化检查任务周期管理，可对运维人员进行工作提醒。



#### 安全检查执行

根据检查计划对检查对象进行安全合规巡检，自动执行检查任务，对检查结果情况进行集中管理，可追溯巡检任务历史执行情况。



#### 检查结果查看

支持检查结果查看功能。当安全合规巡检任务完毕后，系统发现巡检对象不符合检查要求时，会进行检查结果预警。支持查看检查预警明细信息及历史预警信息。



### 云和虚拟化管理

虚拟化管理整合多Vcenter进行统一管理，支持对宿主机、虚拟机监控，同时根据所收集数据对虚拟化资源进行统计，提供虚拟资源申请、调整、回收流程，用户在虚拟资源申请流程审批通过后实现虚拟机自动部署及资源调整，从而极大的提升工作效率。

#### 虚拟机管理

支持用户通过虚拟机管理页面来查询当前所有虚拟机配置与管理信息。

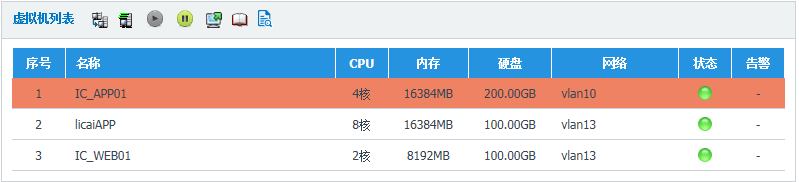
支持资源配置过程中，用户的信息随资源的创建、分配、变更记录到对应的资源属性中。



支持用户通过虚机管理页面对虚拟机的配置信息进行维护。包括使用者、机构、隶属项目信息、所在主机、操作系统、操作系统版本、IP地址等等。（隶属信息用于部门、项目统计使用，如没有登记，将不对此虚机进行统计）。



支持用户对所拥有的虚拟机可进行完全控制，包括：虚机的开关机、重启、删除、快照操作；



#### 资源申请

支持用户发起资源申请，在资源或配额足够的前提下，能够获得所需求的虚拟机资源，流程完成审批后进行虚拟机自动部署。

#### 资源调整

用户在使用虚机过程中可以发起虚机资源调整流程，调整内容包括虚机的CPU、内存、硬盘、网络等资源配置信息。

#### 资源回收

用户在使用虚机过程中可以发起虚机资源回收流程，将不再使用的虚机资源交还给资源池。

#### 资源统计

云平台提供完整的综合报表管理，支持序列排序，可在线查看和导出文档，平台能够保证数据的严谨性和正确性。

支持僵尸虚机、申请资源与实际使用差距等统计信息，提高资源使用效率。并可以定期生成报告，持续优化整体资源配置。

平台预制资源使用情况统计报表、资源性能分析报表、部门使用情况报表、项目使用情况报表、监控资源统计报表、僵尸资源统计报表、关机资源统计报表、虚拟化资源统计报表、资源综合统计报表等。

##### 监控资源统计

支持虚拟资源监控统计报表，对于虚拟机名称、IP地址、用户名称、部门名称、CPU平均使用、磁盘 I/O平均使用速率、网络 I/O平均使用速率、性能查看等信息进行统计。



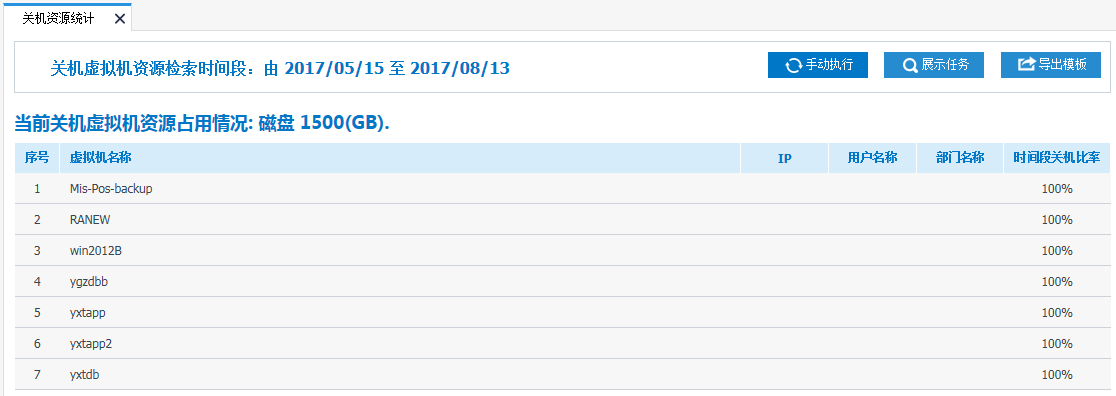
##### 僵尸资源统计

支持僵尸资源统计报表，对于虚拟机名称、IP地址、用户名称、部门名称、应用名称、CPU平均使用、磁盘 I/O平均使用速率、网络 I/O平均使用速率等信息进行统计。



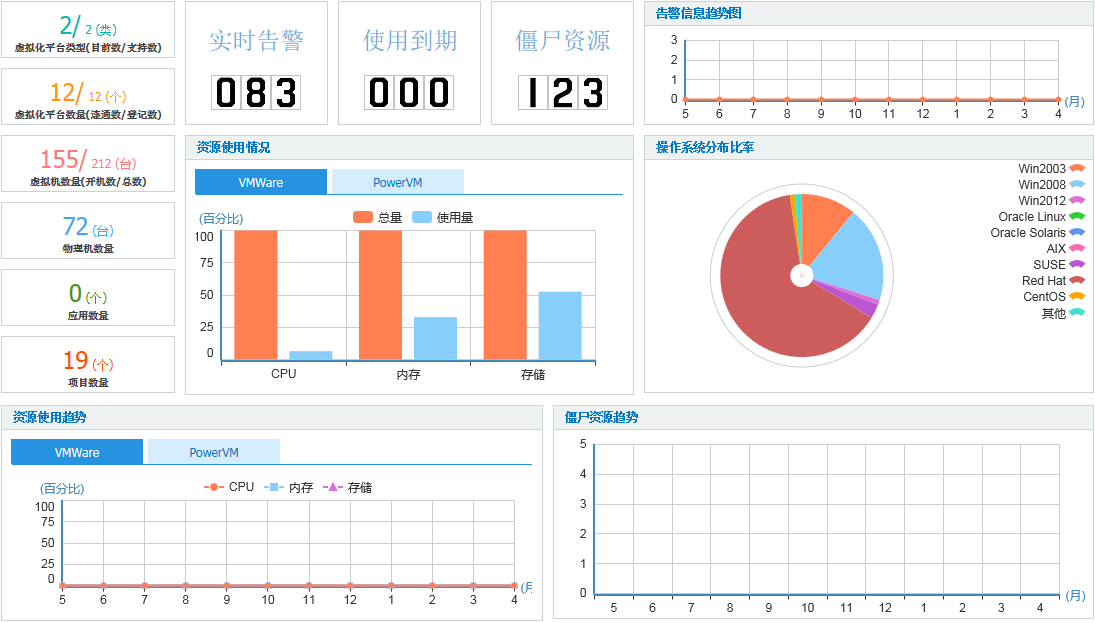
##### 关机资源统计

支持关机资源统计报表，对于虚拟机名称、IP、用户名称、部门名称、时间段关机比率等信息进行统计。



##### 资源综合统计

资源综合统计报表，支持虚拟化资源综合统计，对于告警信息统计、告警趋势分析、资源使用情况、操作系统分布比例、资源使用趋势、僵尸资源趋势等信息进行统计。



### 运维流程管理

信息安全集中管控系统满足全省一体化运维服务管理功能需求，支持总分一体化管理。通过建立IT服务管理平台构建标准化IT服务管理体系，促进贵局运维工作高效展开。推动运维工作流程规范化，提升工作效率。建立知识共享机制和主动查询、关联，为系统管理人员开展运维工作提供便利。

一体化运维管理平台为使用人员提供统一的平台入口，采取B/S架构，并且具备用户、角色、权限、组织机构的管理功能，通过不同的用户、不同的角色进行管理功能的划分。

系统支持个人门户管理功能，针对不同角色可提供不同的功能模块，从而达到每个用户有不同的角色、组织机构和展现内容，实现集中运维管理。同时按照运维人员的不同职责，划分运维人员所关注的重点，达到职责有别、关注有别。

#### 服务台

提供给业务人员的自助服务台界面，业务部门通过自助服务台直接提交故障申报、服务申请、业务咨询等需求；业务人员参考自助服务台中的FAQ，可以快速进行问题的自查，减轻了IT服务人员的工作压力。

服务台主要功能包括：

* 提供的知识库检索和查询功能，可以快速进行知识库查询。
* 提供统一的控制台界面，对所有未关闭的事件进行跟踪。
* 通过客户端或浏览器方式对用户请求进行查询，了解请求的状态。
* 提供接收，登记，记录用户提出的投诉/建议功能。
* 提供服务工单功能，以便记录信息报告人姓名、联系电话、所属机构、报告事由等信息。
* 提供多种主动通知方式，通过手机短信、电子邮件、界面提醒获得通知消息。
* 服务台支持列出所有被指派到当前用户的待处理工作列表。
* 服务台支持列出当前用户所发起的所有流程。

#### 事件管理

事件管理作为负责解决IT服务中事件、监控告警事件的运维管理流程，它的目的是尽快恢复被中断或受到影响的IT服务。

事件管理主要功能包括：

* 根据以往项目案例及经验积累，预置事件分类信息。
* 事件发起：发起事件，选择事件类型，选择事件报告人、事件影响人，填写事件名称。事件单记录来源、用户、时间、现象、影响度等内容。
* 事件查询：按事件的类型、事件状态、事件紧急程度、发起人员、事件的时间段等条件进行事件查询。
* 事件的分类和优先级确定：事件的分类应当可以由管理员根据事件的属性、级别、内容预先设定。
* 事件分派：事件经理将事件分派给处理人员进行处理，并给相关人发送通知和提醒。
* 事件处理：被分派的事件处理人记录处理过程；支持记录事件超时时间。
* 事件升级：支持按照预设的规则，对事件进行升级处理，并通知相应人员。
* 知识查询：事件处理过程中可以查询知识库寻求支持。
* 事件状态或事件指派发生变化时，系统能够自动以邮件或短信等方式及时通知到相关人员。
* 事件处理过程中的关键点和操作完整记录到系统中。

#### 问题管理

问题管理指通过找到事件发生的根本原因，或采取预防性行为，对运维管理工作进行主动支持，它的目的是发现事件的根本原因。

问题管理主要功能包括：

* 提供对问题工单内容进行填写，包括问题名称、描述、问题分类、影响程度、紧急程度等。
* 提供通过手工录入问题工单信息。
* 提供问题工单同事件工单的关联。
* 提供分配问题单后，通知相关处理人。
* 问题处理过程中的关键点和操作完整记录到系统中。

#### 变更管理

变更管理用以确保对信息技术资产所做的所有更改都是以计划和授权的方式实施的，以规避实施过程中操作风险。

变更管理主要功能包括：

* 提供变更管理的全过程：如新建、审批、处理、评估、关闭、取消等状态变化。
* 变更工单记录工单的发起人、计划执行时间、变更描述和变更执行、恢复、验证计划等信息。
* 提供多级审批，对于不切实际、不合要求的变更可视情况进行驳回和关闭处理。
* 变更状态发生变化时，系统能够自动以邮件或短信等方式及时通知到相关人员。
* 提供根据查询条件对变更进行精确查询。
* 变更可按医保局需求，定制、增加各种变更选项、要素选择等。

#### 服务请求管理

IT服务请求主要用于处理其他部门向运维部门提出的与信息科技相关的服务请求。

服务请求管理主要功能包括：

* 提供对服务请求表单信息的灵活定义。
* 提供对服务请求流程查看实时跟踪处理状态，可以通过服务请求名称、服务请求描述、服务请求处理状态等对服务请求流程进行查询。
* 提供流程处理提醒机制，支持提醒方式包括：短信、邮箱提醒，可实时通知科技部人员及时处理工单，确保日常运维工作的及时、有效处理；
* 提供灵活定义流程跃迁规则及节点信息等。
* 服务请求处理过程信息可记录在日志中。

#### 知识库管理

通过完善的知识库管理功能，使得运维人员可以方便、快捷地获得问题的解决方案，以快速解决问题，提高IT服务效率和质量。

知识库管理主要功能包括：

* 支持自定义知识分类。
* 提供通过手工录入问题单创建知识。
* 提供将事件、问题和变更流程处理记录引入知识库，作为知识案例。
* 提供对知识进行审核，实现只有审核通过的知识才可以对外发布。
* 能通过关键字迅速在知识库中寻找到解决方案，支持关键字查找功能。
* 支持添加图像、文档等不同格式的附件。
* 提供多种搜索方法，针对任意字段进行查询、过滤、排序等操作，支持对知识条目的检索功能。
* 知识库内容的更新要有相关记录，对关键的知识的修改需要重新审核。对知识库的操作由系统自动记录。
* 知识库应支持知识引用、知识评价、评分的功能。

### 大屏展示

本次大屏展示告警清单、告警分类饼图、告警量趋势图、BSM视图等内容。在本次项目建设中，提供大屏展示设计与开发数量为2张大屏以内。

展示方式：支持列表、饼图、柱图、折线等展示多种展示方式，不对统计结果数据进行钻取。

根据领导决策需要设计符合实际情况的领导视图大屏。领导视图可以纵览全局，领导可通过领导驾驶舱掌握运维部门的整体情况，如：运维平台的使用情况、IT资源的运行情况、运维人员日常工作信息等。主要包括资源运行状况、监控告警情况、运维工单的数量、系统运行状态等信息。通过对运维团队运营情况的了解与掌握，可适时的对工作进行分派处理。



IT运维监控中心：展示省医保IT基础设施（含操作系统、数据库、中间件、网络设备、存储、虚拟化等）健康情况，实时显示监控告警信息。



### 统计分析

#### 运维统计分析

提供报表服务，对IT运维流程进行全方位的KPI统计报告，并可为不同角色的用户提供个性化的功能丰富的仪表盘（Dashboard）。

流程报表包括：运维报告、基础设施运行状况、重要应用系统运行状况、IT服务流程统计、故障告警统计、运维流程趋势分析，各类流程的详细分析，包括工单关闭情况、各类型占比情况、数量趋势情况等。

最终形成的报表包括但不限于以上报表，具体需求以最后交付为准。

#### 资产配置报表

可自定义资产配置明细报表，包含操作系统报表、硬件设备报表、网络设备报表等，为科技领导及相关管理人员提供全面的资产配置信息。