网络安全智能运维方案

（轨道金融）

北京融讯光通科技有限公司

2023 年 12 月

目 录

一、业务背景

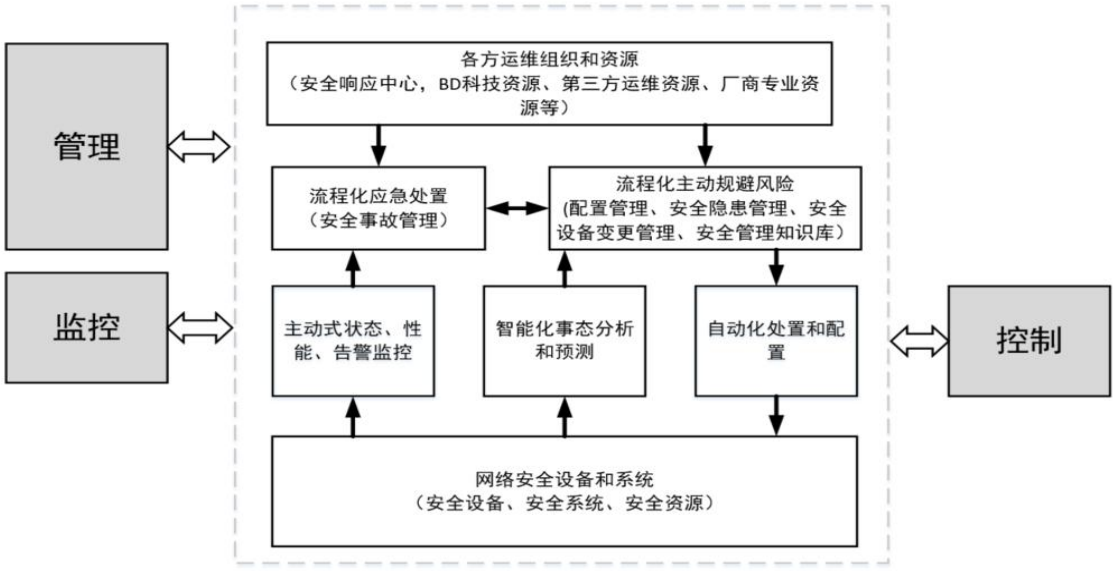
1、概述

为了应对轨道金融网络安全体系规模的不断扩大、设备和系统日趋复杂，系统和设备越来越智能化，网络安全的运营重心已不再偏重于基础设施投资，安全系统维护起来成本很高，效率有待提升。如何通过有效运营，使网络安全设备和系统更能有效运行，是迫在眉睫需要解决的问题，提高运维水平和效率成为网络安全体系建设运营的重要保障。

三分建设、七分运维。本平台针对网络安全体系的智能化运维管理，满足各类安全设备的快速有效智能运维需求。从流程规范加上智能化工具，并通过 AI 辅助人员日常工作，三管齐下，提升运维效率，保障轨道金融信息安全建设成果，并在日常工作中发挥指导价值。

融讯光通智能运维管理平台，建立在国际标准 ITIL 和 ISO20000 之上研发，同时与国家工信部发布的 ITSS 标准高度吻合，并针对网络安全设备的运维需求特点，结合了 ISO27001 的相关要素，优化了平台对安全设备的智能化运维支撑能力。

对于轨道金融信息化运维管理领域，更需要确保系统安全可控。一方面提供相关安全服务，实现网络、系统软硬件、应用、用户的安全，实现信息传输、信息处理与应用全过程的安全防护。另一方面，还需构建高效的运维系统，对安全设备和系统的运行状态、拓扑、故障、性能等进行统一监控和集中管理，通过工作流程使“监控、管理、控制”三个要素能够紧密结合，形成安全管理运营中心。



充分考虑安全设备和系统种类繁多、系统庞大、部署分散的特点，安全运行维护管理中心能够支撑对应的组织结构和管理模式，合理规划管理层次和级别，使安全管理运维系统成为各类任务保障的助力而非“阻力”。

把网络安全体系中的网络设备、安全设备、服务器、存储、机房环境、操作系统、数据库、中间件、设备资产、日常运行工作等组成统一纳管的安全对象，进行的一体化的安全监控、流程管理和调度控制，最终达到保障基础架构稳定可靠运行、降低系统和各类安全应用宕机风险，提高网络安全设备的运维支持和服务管理效率的目标。

对网络安全设备智能运维领域的业务需求，主要归纳为以下几点：

1、对系统资源进行运行信息采集、监控和告警的要求

系统具备对整个安全管理系统中使用的各类设备（防火墙、入侵检测、沙盒、行为分析、网闸等）、线路、服务器，以及操作系统、应用软件等各类组成部分，进行全面信息采集和监控，针对性制定采集监控策略，并实现主动故障告警，全面提升整体网络安全设备系统各类设施和应用的可靠性，确保各类安全应用的高可用性和高性能。

2、智能化数据采集和处理能力，满足多种运维场景对数据的需求

数据的采集和处理，应支持多种类型的监控数据、多种数据模型和处理策略，并形成统一的数据存储、数据查询等数据服务能力，支持多种运维应用的个性化开发，实现运维管理的智能化，满足现代化网络安全管理的多维度保障分析优化需求。

3、对运维组织人员和运维对象进行流程化管理，提升运维保障能力

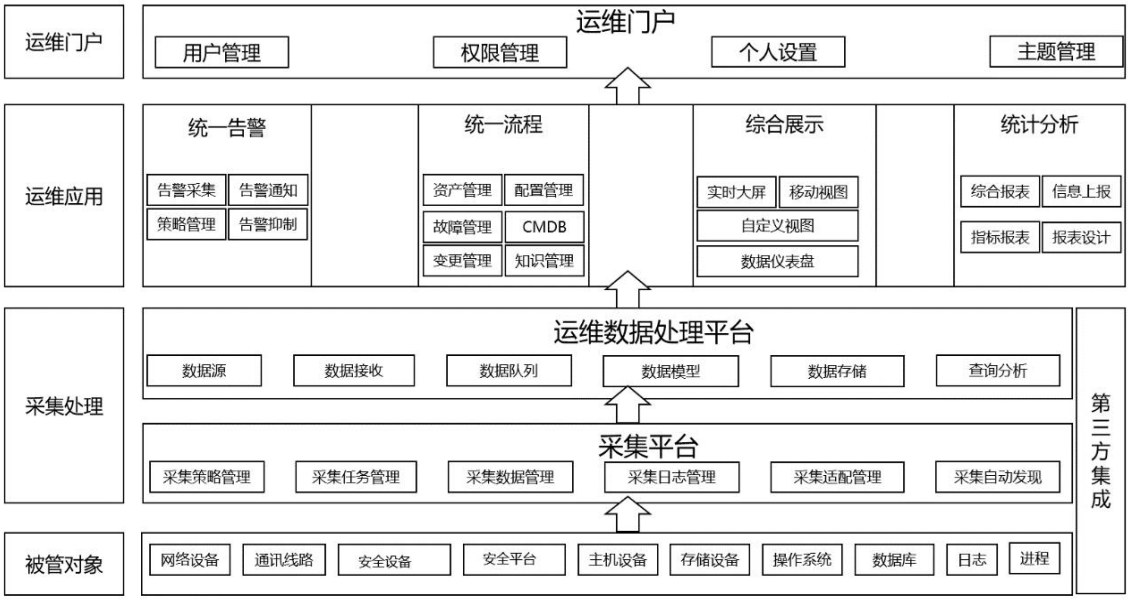
通过对网络安全设备系统中的各类对象和关系进行统一建模和精准管理，结合故障管理、变更管理、请求管理、问题管理、资产管理、知识管理等标准化运维业务流程，确保运维组

织和人员能够按照高标准的服务体系进行日常运维和服务工作。在流程和日常运营环节上，能够确保整体运维组织协同工作，整个运维体系具备精细化管理和可服务能力。

4、对运维指标和能力，进行多维度展示和分析，持续提升运维成效

通过大屏幕、数字面板、报表等多种方式，展示运维体系中的关键业务指标、关键业务信息。提供充分、易用、可视化的指标展示，使网络安全设备的运维保障工作成效清晰明了，有条不紊地保障各项业务任务，运维管理工作能够逐步实现集约化、智能化。

2、体系架构



运维分系统主要由采集处理系统、运维应用系统和运维门户系统等组成。

(1) 采集处理系统：对网络中包含的各类安全设备硬件、软件组成对象进行运行状态、性能、指标等方面信息数据进行采集和处理，通过数据模型、数据存储、和数据查询，向上层运维应用提供监控信息、指标信息、数据查询等数据支撑服务。

(2) 运维应用系统：包括统一告警、统一流程、综合展示和统计分析等四个方面的具体应用。

(3) 统一告警：对监控对象进行告警策略设置、告警收集、告警通知和处理；

(4) 统一流程：对运维相关的流程，包括告警处理、资产管理、CMDB（配置管理信息库）、变更管理、网络安全设备运维知识管理等运维流程。从运维流程角度，优化运维队伍资源，提升设备和系统的运行效率。

(5) 综合展示：通过大屏幕、数据仪表盘等方式，直观呈现系统运行宏观指标；

(6) 统计分析：通过报表统计各类运行详细指标，并按照报表要求对本级运维指标进行上报。

(7) 运维门户系统：提供四类运维应用、以及系统管理方面的访问入口，具备身份认证、分级权限管理等能力。

建设一体化、智能化、集约化的综合运管平台，为系统提供全网管理和运维支撑，实现对网络安全各个层面的一体化管理，各类网系资源的统一调度，各层级网络管理业务的统一支撑。

RXGT 智能化运维管理产品系列包括：

- **RXGT ITSM 套件：**RXGT ITSM 套件是针对网络安全设备维护的场景需求，由事件管理、问题管理、变更管理、服务请求、资产管理、配置管理、工单管理、知识库和流程引擎、开放接口组成。
- **RXGT NetManager 套件：**对网络安全设备系统中的网络设备、安全设备、操作系统等核心资源进行主动式监控，根据规则智能报警。
- **RXGT Call Center:**基于 IP 协议的 CTI 技术，融合了所有常用的呼叫中心功能，从底层硬件直到操作管理平台的统一标准化，与 RXGT ITSM 高度集成。通过多种服务接入渠道，形成 7X24 小时有人值守的安全响应热线。
- **RXGT Mobility:** RXGT Mobility 提供更快捷更便利的方式在系统中查看工单信息，并支持新建、更新、查询等日常业务操作，提供运维人员两个版本，使网络安全的智能运维日常工作效率得到极大提升。
- **RXGT KPI:** 通过大屏幕集中展示，提升整体运维管理水平。它是智能运维建设过程中关键成功要素，为智能运维可视化提供了很大的决策帮助。
- **RXGT Dashboard:** RXGT Dashboard 是一款面向日常智能运维的数据统计分析工具，以拖拽式实现各种报表、Dashboard 仪表盘、统计图、分析报告、多维分析等。
- **RXGT 智能运维生产力工具：**通过系列实用工具从文件预览到远程控制，提高智能运维服务人员的故障处置、故障针对等日常工作效率；

3、产品优势

技术特点及优势如下：

(1)全采集：满足对网络安全系统中各类资源进行信息采集、监控和告警的要求。系统具备对整个系统中使用的各类防火墙、日志审计、入侵检测、内容监控、隔离装置、其他信

息安全管理系统或者设备等各类组成部分，进行全面信息采集和监控。

(2)全处理：智能化数据采集和处理能力，满足多种运维场景对数据的需求。支持多种运维应用的个性化开发，实现运维管理的智能化，满足多维度保障分析需求。

(3)全流程：对运维人员和安全设备资产进行流程化管理，提升运维服务保障能力。确保运维组织和人员能够按照高标准的服务流程进行日常运维工作,确保运维组织的工作有章可循、具备规范化的安全作业、管理和服务能力。

(4)全分析：对运维能力指标进行多维度展示和分析，持续提升运维成效。使网络安全产品的运维管理工作，能够逐步实现集约化、智能化。

(5)全主动告警：通过信息集成，能够对接整体系统中使用的各类安全相关的设备告警、以及安全配套的专业化监控、管理或者告警平台，实现不同类型的监控信息和告警等平滑接入到智能运维管理平台。

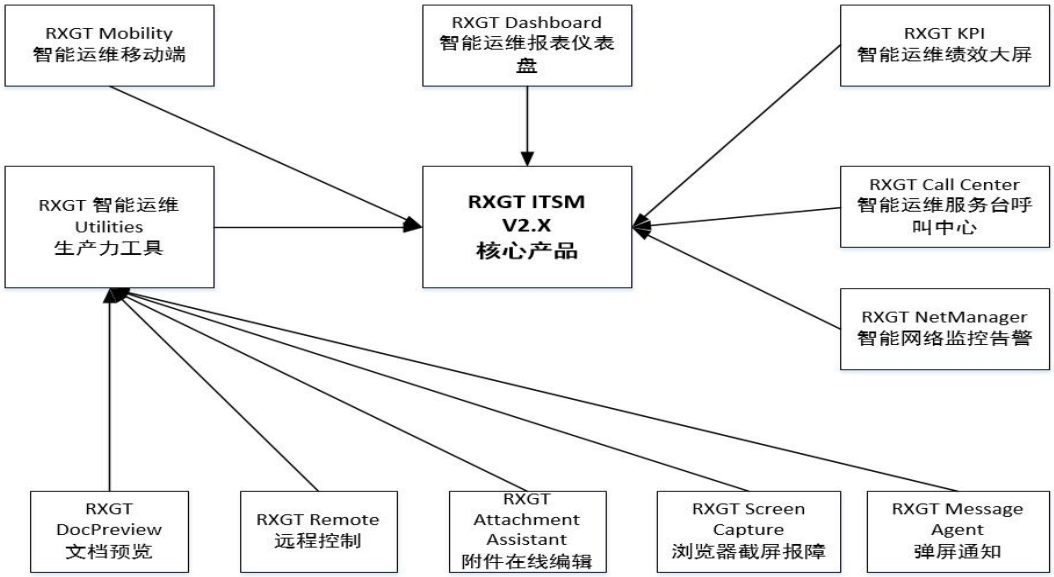
通过模拟试验，达到如下关键技术指标：

- 监控对象覆盖全系列安全设备和平台，对象覆盖率达到 95%以上；
- 监控指标包括状态指标和性能指标，90%以上的状态指标，以及 80%以上的性能指标已经完成；
- 告警接收和处理性能可达到 10000 条/秒以上。满足 90%以上的网络和安全运维范围和场景；
- 运维流程覆盖告警管理、故障管理、变更管理、配置管理、问题管理、知识库管理等，100%满足 ISO20000 和工信部 ITSS 的要求；
- 智能化预测能力正确率达到 80%以上；
- 大屏幕和智能化分析展示指标，能够简易部署在指挥大厅，满足 80%以上展示场景。

4、适用对象

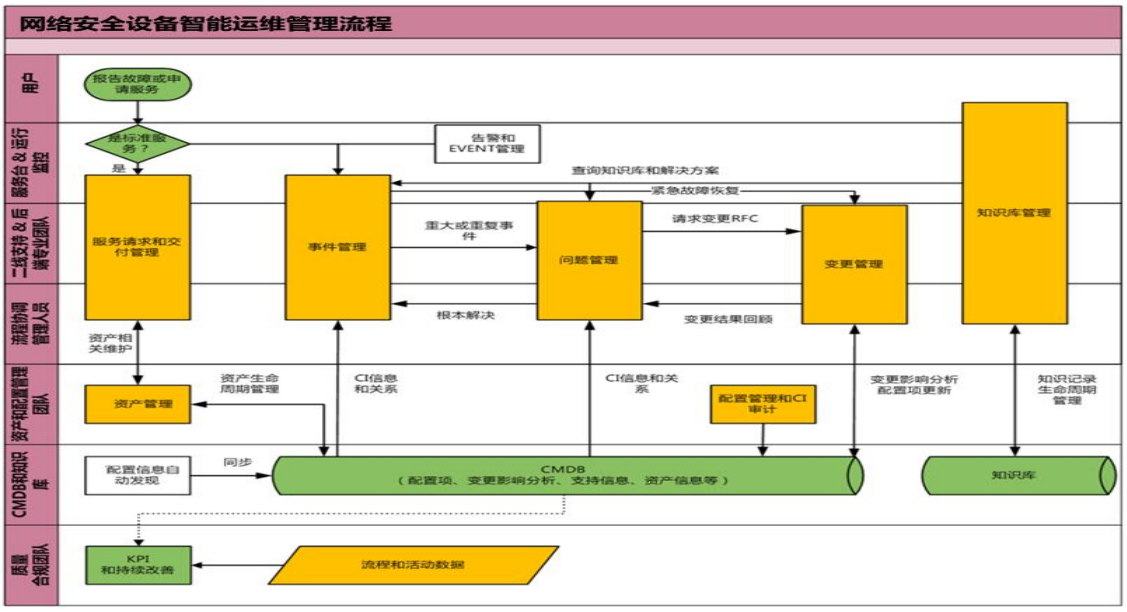
RXGT 网络安全设备的智能运维管理系列产品，在运维设备范围和规模上具有很强的适用性。适用于网络安全设备管理的不同信息化规模和不同场景。从 10 多个人的运维团队，到上千人的专业运维组织，都可以通过 RXGT 智能化运维产品来实现运维管理能力的提升。

二、系列产品组成关系


RXGT Mobility
智能运维移动端
RXGT Dashboard
智能运维报表仪表盘
RXGT KPI
智能运维绩效大屏
RXGT 智能运维
Utilities
生产力工具
RXGT ITSM
V2.X
核心产品
RXGT Call Center
智能运维服务台呼叫中心
RXGT NetManager
智能网络监控告警
RXGT
DocPreview
文档预览
RXGT Remote
远程控制
RXGT
Attachment
Assistant
附件在线编辑
RXGT Screen
Capture
浏览器截屏报障
RXGT Message
Agent
弹屏通知

三、网络安全设备智能运维流程管理

1、产品业务版块



RXGT ITSM 是基于 ITSS 等最佳实践的纯国产化产品，对标美国 BMC 公司的 Remedy ITSM、CA 公司的 CA Service Manager 等。

RXGT ITSM V2.X 一般情况下与 RXGT Mobility 产品、RXGT Dashboard、RXGT KPI 产品一起进行绑定销售和实施。

RXGT ITSM V2.X 产品和绑定产品的功能包括：

No	模块名称	业务说明
1	服务请求管理	管理网络安全设备的指战员的标准化网络安全服务内容；
2	事件管理	管理网络安全设备和应用的故障；
3	问题管理	管理网络安全设备的潜在隐患和疑难问题，找到根本原因；
4	变更管理	管理网络安全设备的软件、硬件的升级或者变更风险；
5	发布管理（可选）	管理网络安全设备的软件、硬件在生产领域的版本和发布过程，一般与变更管理配合使用；
6	服务级别管理	管理网络安全设备故障的解决以及服务请求的交付效率和质量；
7	知识管理（可选）	管理网络安全设备实用和运维过程中的常见知识，提高一线

		运维人员的解决故障的效率；
8	值班管理（可选）	管理网络安全设备的值班日常和交接班事项；
9	资产管理	管理网络安全中的各类设备的使用、备件、财务、盘点等流程；
10	配置管理 CMDB	对网络安全设备系统的被管理对象和关联关系进行管理，提供精准和完整信息
11	巡检管理（可选）	通过手机 APP，提供对网络安全设备设施等环境巡检的安排和过程进行管理，发现故障及时转换为故障进行处理；
12	服务报告	通过报表、服务仪表盘、以及大屏幕管理各个流程的服务指标；
13	移动化（可选）	通过 RXGT Mobility 实现手机 APP 接入。
14	集成模块	• 内置与监控系统的集成； • 内置与 NetManager 自动发现集成； • 内置短信集成； • 内置邮件和 LDAP 集成； • 内置 SSO 单点登录集成； • 提供服务端 REST 服务 API 开放集成服务；

2、产品特点

RXGT ITSM 产品解决方案具有以下几个特点：

- **纯国产化自主知识产品产品。**
- **流程表单灵活自定义：**RXGT ITSM 提供简单的流程设计器和表单定制器，用户可以灵活根据自身需求定制流程和表单，方便快捷；
- **集成移动 APP：**RXGT ITSM 提供功能全面的移动 APP，实现用户随时随地快速报障、技术人员快速接单处理，大大提高了运维效率；
- **部署简单，维护轻松：**RXGT ITSM 提供三种部署方式：云端部署、一体化盒子、本地部署。其中云端部署和一体化盒子不需要用户规划系统架构、采购硬件设备，安装简单，维护也轻松。
- **支持多租户和 SAAS 化模式：**产品支持云服务模式。

3、产品设计理念

基于融讯光通在智能化运维管理系统建设的经验，RXGT ITSM产品同时要保证方案整体具有系统性、实用性、高效性、可扩展性，以及技术上的先进性、规范性和安全性。具体如下：

- **产品支持“统一规划，分布部署”的整体运营能力**
  - 集中的统一安全安全响应中心服务台或者安全运营中心：规划合理的平台体系结构，对运维流程质量、运行状况、运维流程监控等实现实时监控、集中管理。
  - 服务管理流程的监控：建立一套工作流程机制，对服务流程运行情况和各阶段工作的情况进行有效地监控，保证流程服务质量。
  - 用户的可管理性：对于平台上的用户进行统一管理，根据用户身份提供严格的权限控制，实现用户统一管理模式。
  - 信息共享的可管理性：集中管理记录、配置信息、知识库等的信息访问控制规则，确保“合适的人访问合适的信息”，实现共享信息的安全访问。
- **标准性和规范性原则**

参考全球IT管理业界公认的指导性框架ITIL（Information Technology Infrastructure Library）服务管理体系，规范网络安全设备运维服务流程管理和操作，指导全体运维服务团队采用先进的规范化网络安全设备运维管理模式，建设一流的服务管理流程。

- **实用性和高效性原则**

网络安全设备运维管理系统将直接服务于日常运维支持人员及最终用户，不同用户特点决定了对该网络安全设备运维管理系统的要求：

1）最终用户（使用网络安全设备的人员）

- 简单快捷的服务：站在服务使用者的角度，简化用户与系统的交互界面，为最终用户
- 提供多种交互手段：用户可以通过电话、Email等不同手段，方便的提交各种服务请求，并接收相关服务请求的处理进展信息。

2）IT运维支持人员（对网络安全设备进行维护的组织或人员）

- 一站式个性化服务：站在IT运维支持工作者的角度，提供个性化的个人工作室服务，本系统功能繁多，但由于分工的不同，不同的使用者只涉及一部分功能和数据，为了简化使用者与系统的交互界面，需要根据使用者的身份，提供个性化的个人工

作室界面。在其个人工作室界面中，提供该用户有权限使用的所有系统功能。

- 提供多种交互手段：使用者可以以短消息(SMS)、电话、Email 等不同手段，及时接收到需要处理的事件单和工作通知。

3）管理人员（网络安全运营负责人）

- 可控的信任授权：利用信息的分级分类技术，实现对不同管理者的信息授权，保证服务信息共享的可控。
- 个性化访问界面：针对流程管理员、流程监控人员、领导决策人员等不同的角色提供个性化界面定制，方便用户使用。
- 图形化的管理工具：提供方便的流程定义、流程监控和人工干预手段。
- 提供多种交互手段：可以采用短消息(SMS)、电话、Email 等不同手段，及时将工单处理状态和预警信息自动通知到相关的管理人员。提供丰富多样、实用的流程状态监控和辅助决策手段

4、网络安全设备运营的公共服务入口和移动端

➢ **公共功能**

- 系统支持图形化的方式实现流程的自定义，模型即是应用，流程灵活自定义，非程序开发人员就能灵活自定义配置软件，持续改善不需要二次开发源代码，包括流程的模板配置、页面字段配置等；
- 所有流程图的展示，支持可视化展示当前处理状态与处理人，并随着流程阶段的不同而改变状态，在处理流程过程中，支持解决方案、日志、附件或者图片的信息记录；
- 个性化访问界面：针对流程管理员、流程监控人员、领导决策人员等不同的角色提供个性化界面定制，方便用户使用。
- 图形化的管理工具：提供方便的流程定义、流程监控和人工干预手段。
- RXGT ITSM 支持消息弹窗，邮件、短信以及 web 在线聊天等方式进行内部沟通，并可以在流程节点设置各种通知规则与通知方式；
- RXGT ITSM 使用独立的审批引擎支持并行、串行、会签、一票否决、一票通过等多种审批模式。
- 站在 IT 运维支持工作者的角度，提供个性化的个人工作服务，本系统功能繁多，但由于分工的不同，不同的使用者只涉及一部分功能和数据，为了简化使用者与系

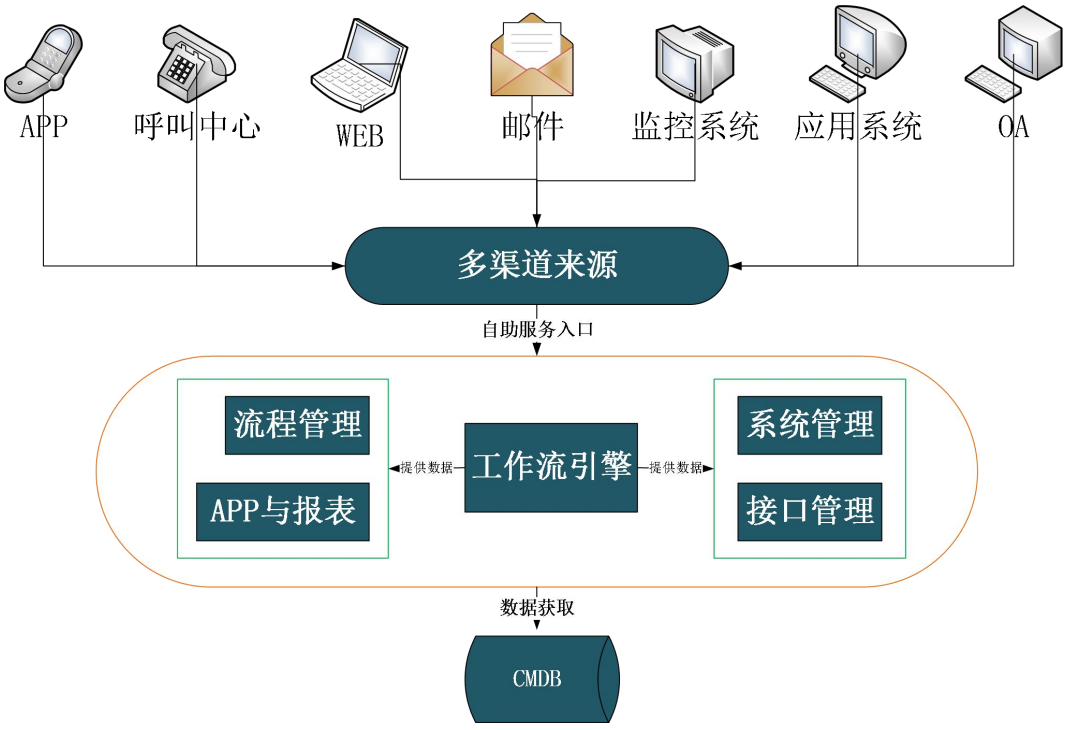
统的交互界面，需要根据使用者的身份，提供个性化的个人工作室界面。在其个人工作室界面中，提供该用户有权限使用的所有系统功能。

- 可控的信任授权：利用信息的分级分类技术，实现对不同管理者的信息授权，保证服务信息共享的可控。
- 提供多种交互手段：可以采用短消息(SMS)、电话、Email 等不同手段，及时将工单处理状态和预警信息自动通知到相关的管理人员。提供丰富多样、实用的流程状态监控和辅助决策手段。

➢ **多渠道接入**

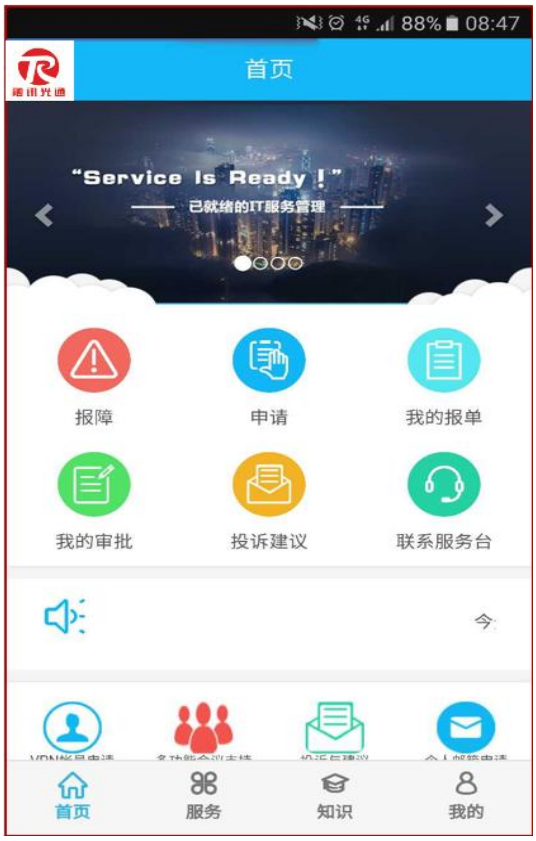
RXGT ITSM 支持多种渠道接入，目前主流的有 APP、呼叫中心、监控、实时信息沟通工具、应用系统以及邮件开单等。

APP 与 ITSM 流程与数据实现联动，与 ITSM 系统进行通讯，可以对所有的工单进行管理。包括服务申请，工单流程信息的查询与监控、工单的派发、回访、审批等功能。



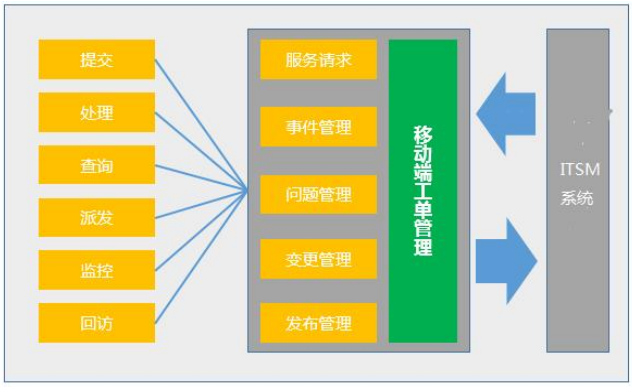
➢ **APP 移动端**

- 跨平台优势，由于服务导航台移动端需要在多平台应用（专用手机），采用 html5 开发 web app 可统一应用风格，减少移植及维护成本。
- 统一更新模式，各移动端可使用统一 UI 服务器，如 UI 服务器更新，各平台应用可统一快速更新，不需要每个客户端单独更新。
- 接口统一，移动端使用的接口同其他 web 应用一样，不需要为移动端重新开发接口。



- **工单管理**

与 ITSM 系统进行通讯，可以对所有的工单进行管理。包括服务申请，工单流程信息的查询与监控、工单的派发、回访、审批等功能。



- **首页**

- 语音报障

- 扫码报障，在专用手机上扫描安全设备条码

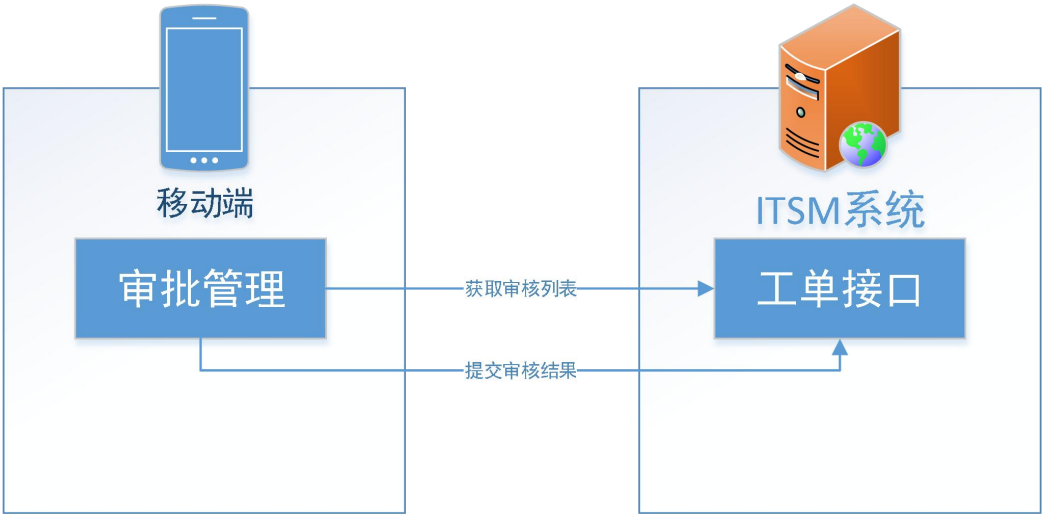
- 管理层 APP 视角

- 事件列表

- 服务请求工单详情

➢ **审批管理**

➢ **调用** ITSM 系统接口，根据当前登录人员，获取相应审批列表进行审批。业务模型如下：



审批管理具体功能点如下：

1. 审批列表

获取当前登录人员的审批列表。

2. 审批工单

查看审批工单的相关信息，提交审批结果及意见。

5、网络安全服务请求管理

➢ 流程目标与范围

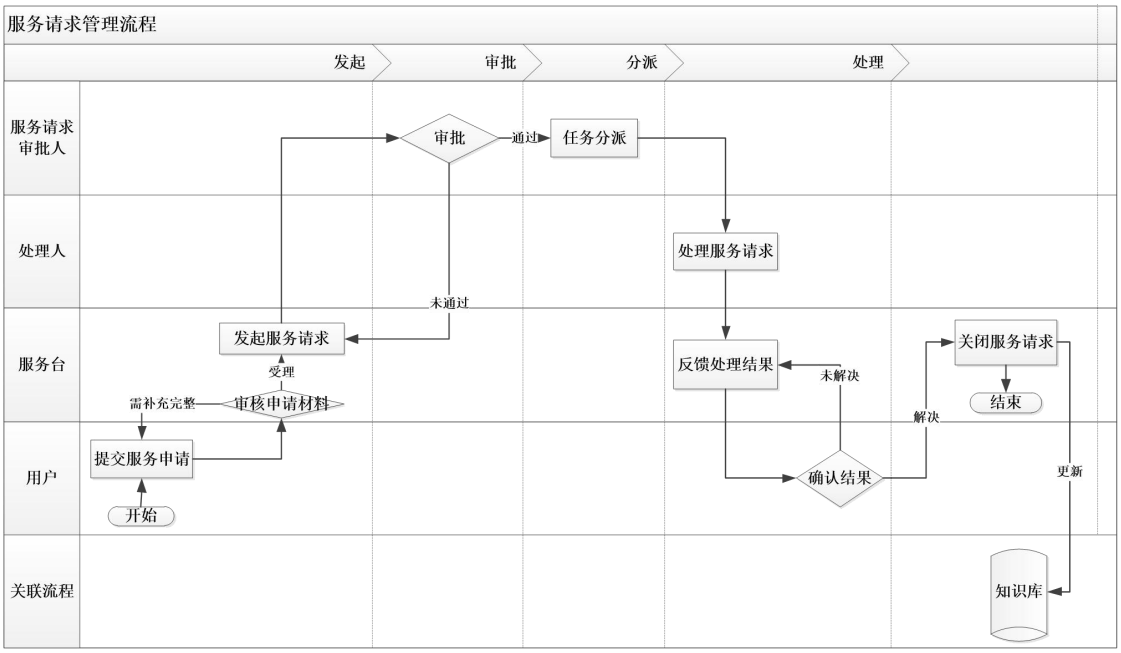
服务请求是用户想要获得网络安全设备有关的信息数据、技术支持、资源分配、文档资料、帮助建议、角色权限而提出的请求，它并不属于网络安全设备方面的事件。服务请求包括但不限于：

- 网络安全数据查询统计
- 网络安全数据提取
- 网络安全数据维护
- 网络安全业务咨询
- 网络安全技术咨询
- 网络安全资源申请（账号、标准安全配置等）
- 网络安全标准变更（网络安全规则增减等）

将用户常用的服务内容项进行梳理，形成服务目录，明确每项服务的履行过程和交付结果，可以帮助：

- 通过更加有效的规划和建设服务请求目录，向网络用户明确提出可提供的服务条目；
- 通过快速响应网络用户提出的服务请求来进一步提升网络安全设备运维服务质量及客户体验，向业务部门和最终用户提供更优质的网络安全设备运维服务；
- 通过对服务请求管理流程进行详细设计和规划，提高了服务请求处理的效率和质量，以及对业务部门提出的服务请求进行快速响应和处理；
- 通过定期对服务流程的回顾，可进一步改进向用户提供的服务水平和服务质量，确保用户对服务价值的认同和肯定；
- IT 需求管理作为一类特殊的服务请求流程，通过服务请求管理的框架流程实现。

➢ 流程关键活动



服务请求管理流程

- 发起：一种方式是安全响应中心服务台坐席人员受理用户提交的服务申请，审核申请材料的完整性，审核通过后发起服务请求流程；另一种方式是由信息科技部内部用户根据工作需要自行发起服务请求流程；
- 审批：审批人根据服务请求内容，审核服务请求的合理性。如有必要，可逐级提交上级进行审批，从而实现多级审批；
- 分派：审批通过后，进行任务分派。一种方式是自动分派，流程发起时已填写处理人，审批通过后任务自动分派给受派人；另一种方式是手工分派，服务请求发起人根据审批结果手工分派任务；

- 处理：受派人根据服务请求内容提供服务；
- 关闭：服务提供完毕，通过回访由用户对结果进行确认。如未完成，则继续提供服务；如已完成，由安全响应中心服务台关闭服务请求。

➢ 角色职责与考核 KPI

角色	职责
网络安全设备的使用用户	服务请求提交人包括用户。服务请求提交人负责服务请求的创建和提交。
服务请求审批人	服务请求审批人员由业务部门经理、主管总监担任，负责审批各部门提交的服务请求。
服务协调员	服务协调员由安全响应中心服务台一线担任，对整个服务请求的生命周期负责，即对服务请求的审批阶段，工作单处理阶段，网络用户回访阶段负责，并关注服务请求的 SLA。
处理人	服务请求执行人，由二线技术支持人员组成。需接受分派的工作单（服务请求信息），分析和处理工作单信息，提供服务。需要时协调第三方来帮助处理服务请求。
服务请求经理	服务请求经理负责协调日常的服务请求管理工作，包括对服务请求的审核、监控、所需资源的协调、编写重要服务请求报告等。服务请求经理由管理岗人员担任。其主要职责是： 1、领导服务请求管理小组，确保大家的积极性、技能水平。 2、必要时协调所需资源。 3、定期制定服务请求相关报表。 4、服务请求栏目和分类维护；

流程 KPI：

KPI 名称	实施要点
各类服务目录请求数量	1、梳理服务请求目录

服务请求处理用户满意度	设计服务请求满意度调查问卷 统计服务请求满意度问卷结果
服务请求处理 SLA 时效满足率	跟进 IT 能力设定好服务请求处理 SLA 统计服务请求处理 SLA 时效
当月服务请求动态报表	设计当月服务请求动态报表
分类统计	设定服务请求类别 报表按类别统计服务请求
请求处理用时	规范服务请求流程，缩短服务请求处理用时

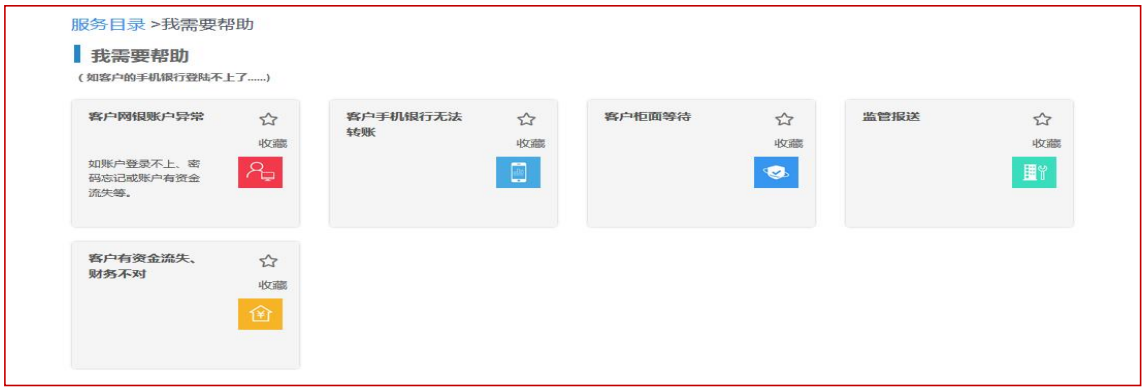
➢ 平台重点功能及示例

平台实施重点

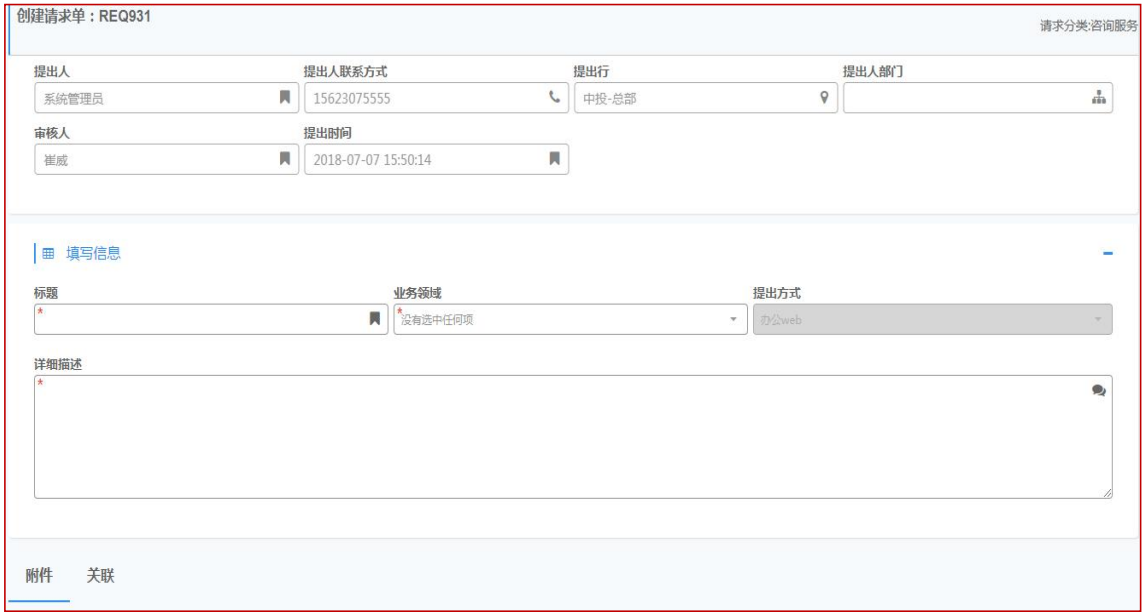
- 支持服务请求记录的新建、撤销、修改、退回、处理、转办、关闭、回访；
- 支持按照服务请求类型定义不同的输入模板及流程；
- 支持创建服务请求记录时自动记录创建日期、时间、发起人信息、请求描述等内容；
- 支持服务请求受派组内部转单；
- 支持用户查看自己提交、受理、处理等参与过的服务请求。
- 支持对服务请求工单中附件的增、删、改等功能；
- 支持服务请求处理完毕后，解决方案信息的录入；
- 支持安全响应中心服务台坐席人员或系统管理员根据解决方案一键生成知识库条目，并进行关联操作，形成知识库与服务请求可追溯的信息流。

工具示例

服务目录



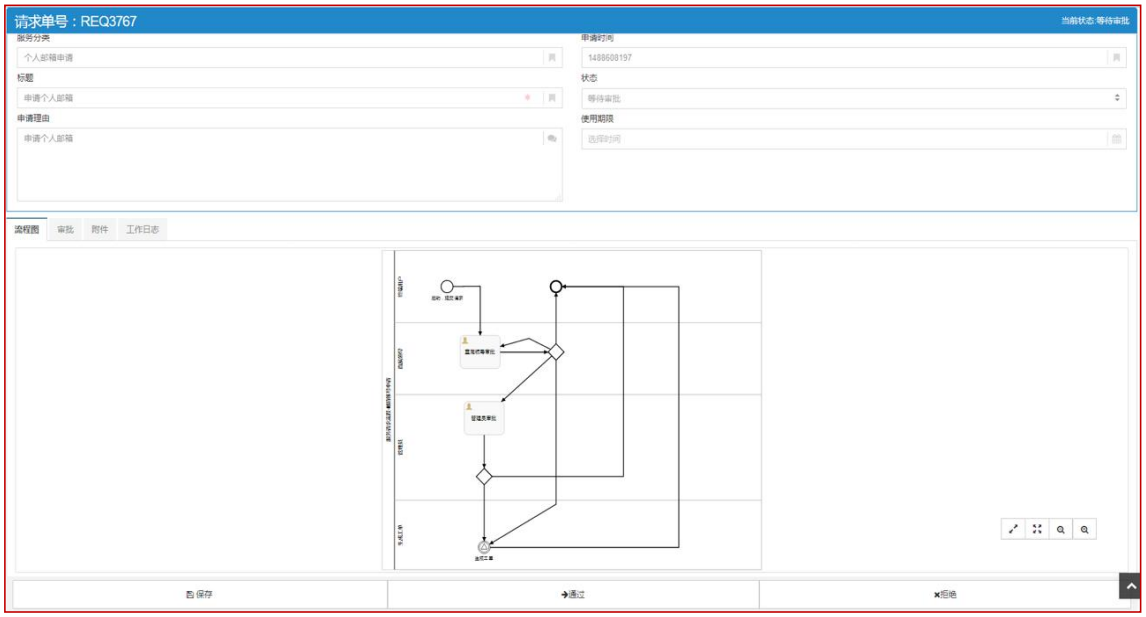
服务请求单



服务请求流程

每一个服务请求单都附带有一张流程图，显示提交该项请求后需经过的流程，并且在流

程图中标记处当前所处的状态及处理人。

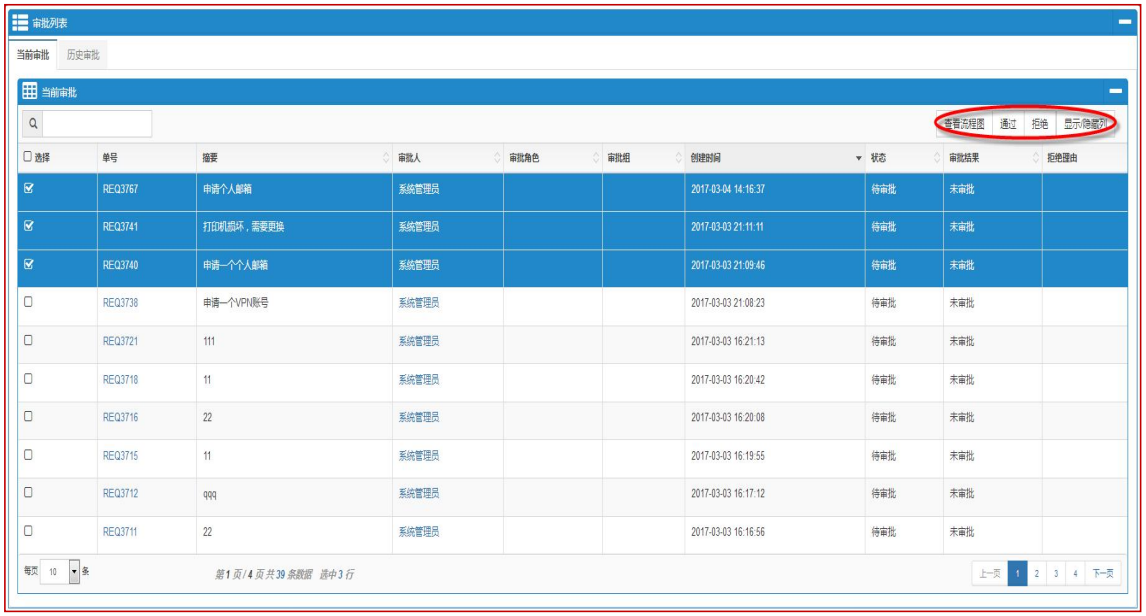


服务请求审批

查看流程图：即查看选中的请求单流程图，可了解该请求条目整个流程及当前所处的阶段。

通过：审批通过。

拒绝：审批不通过，请求流程终止。



自助请求 WEB 端：


首页
我的收藏
知识搜索
欢迎 系统管理员
客户v
最新动态
历史
2017年3月5日（周日）晚上六点，...
2017年2月19日（周日）晚上六点...
2017年2月12日（周日）晚上六点...
Ready ITSM 正式上线了
我需要帮助
（如客户的手机银行登陆不上了.....）
我有一个申请
（如我需要申请一个帐号.....）
我有一个疑问
（如我不知道新上线的网银系统如何操作.....）
我有一个需求
（如我想在手机银行APP上增加一个功能.....）
投诉与建议
商行联盟的投诉与建议服务，为用户提供入口，收集用户对IT运维服务的建议。
54
我的未解故障
86
我的所有故障
57
我的未解请求
78
我的所有请求
5
我的审批
热门请求
更多
VNP帐号申请
邮箱帐号申请
热门知识
更多
处理页面很多的必填字段红星都消失了
作者:系统管理员
点赞数:9
服务热线
邮箱：

热门请求：


Service Is Ready!
——已就绪的IT服务管理体系.——
最新动态
更多
Ready ITSM 正式上线了
2016-10-26 16:01:59
866
我的未解故障
868
我的所有故障
40
我的未解请求
6
我进行中的请求
41
我的所有请求
6
我的审批
热门请求
更多
1 资产上架
2 需求备份申请流程
3 业务数据调整(修改)
4 资产下架
5 咨询服务
6 机构调整
7 业务需求
8 数据查询统计服务
热门知识
更多
1 KM2642标题 2018-03-05 14:25:36
2 测试申请 2018-03-05 11:14:37
3 32132 2018-03-05 11:08:47
4 KM2639标题 2018-03-05 14:09:48
服务热线
邮箱
热线

热门知识：

自肋请求移动端：

我的工作台：

6、安全响应中心服务台

安全响应中心服务台（Service Desk）是网络安全设备运维管理流程组中唯一一个非流程的职能单元，也是组织向智能运维管理转型的重要环节。安全响应中心服务台是网络安全设备运维管理体系中与用户沟通和交互的单一界面，负责对用户在使用网络安全设备运维服务过程中遇到的问题和需求进行响应和处理。同时，对网络安全设备运维团队内部而言，安全响应中心服务台是网络安全设备运维组织与网络用户的官方接口和信息发布点，也是网络安全设备运维组织各个团队之间相互协作的纽带和协调者。对于网络安全设备运维而言，安全响应中心服务台对服务质量及用户体验的管理至关重要，是组织服务能力持续提升的战略单元。

安全响应中心服务台对内提供协调的战略职能单元，其主要目标应包括以下：

- 网络安全设备运维部门的统一服务窗口，通过多种途径（电话/邮件/WEB 等）提供主动或被动服务；
- 监视服务信箱收件箱，对 IT 用户的邮件咨询和请求提供恰当反馈和处理；
- 收集并记录用户上报事件、服务请求、咨询、投诉及系统监控事件；
- 基于服务目录过滤用户申告；
- 基于知识库对用户申告进行初始支持，并尝试解决事件；
- 分解用户申告，区分事件和服务请求，并路由至适当的二线人员；
- 对内部资源进行沟通与协调，加强协作效率及有效性

- 作为网络安全设备运维部门统一信息发布窗口，与 IT 用户相关的发布信息通过安全响应中心服务台系统平台发布，并有安全响应中心服务台人员进行统一沟通；
- 对用户的体验及满意度进行定期跟踪和监控，并向管理层提供相应统计信息供分析与决策

安全响应中心服务台总体上分为热线服务和安全响应中心服务台管理两个主要部分。各部分包含的具体职能描述如下：

- 热线服务

✓ 办公环境支持：负责对用户办公网络、通讯环境及桌面软硬件等方面上报的事件进行在线响应和处理；

✓ 应用系统支持：负责对用户在应用系统方面上报的事件进行响应和处理；

✓ 各类网络安全设备运维相关的咨询：负责对用户在网络安全设备运维服务方面的咨询进行记录和反馈；

✓ VIP 服务：负责对高级管理层人员提供 VIP 级服务。

✓ 热线服务也将提供办公环境和应用系统的服务请求响应服务，不在本文列出。

✓ 来电弹屏显示用户信息，并支持网络用户历史事件与所属单位历史事件的查询。

- 安全响应中心服务台管理

✓ 运营管理：负责安全响应中心服务台热线、现场团队的日常工作计划、资源协调、升级处理

✓ 投诉和满意度管理：负责接收和处理来自用户的投诉和建议，并定期发起客户满意度调研。

✓ 质量管理：负责对安全响应中心服务台日常运营 KPI 及客户满意度进行分析，并对事件记录及处理质量进行定期审查；

✓ 信息管理：负责用户信息、公告、用户端 FAQ 知识库等相关信息的维护以及网络安全设备运维部门为外的信息发布。

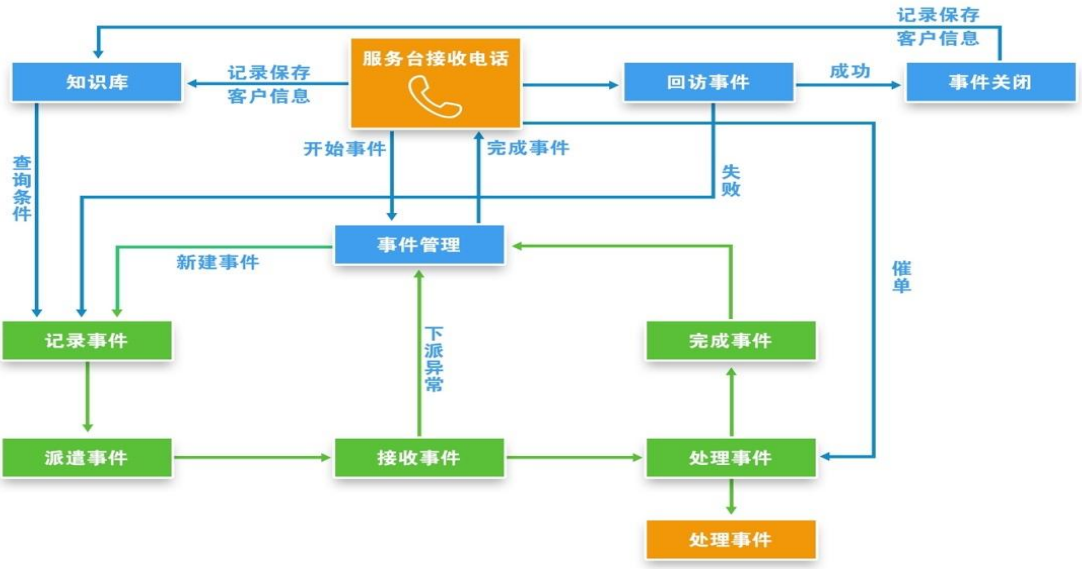
✓ 需求预受理管理：负责接收和处理用户超出服务目录之外的需求，记录并分配给需求分析受理人员，后端团队定期组织各团队对新需求进行统一梳理和分析。

✓ 知识管理：负责定期评测安全响应中心服务台人员能力、制定培训计划等；

✓ 报表管理：负责定期创建安全响应中心服务台 KPI 报表及客户服务报告；

✓ 其它各种临时提出的管理工作。

➢ 岗位职责定义



IT 安全响应中心服务台岗位涉及相关职责具体定义如下：

- 热线支持岗
  - ✓ 依照服务目录和服务级别协议向客户提供服务支持
  - ✓ 通过电话、Web 自助、邮件等方式受理用户上报事件，创建事件单并记录相关信息
  - ✓ 按照策略受理自动升级监控故障
  - ✓ 对事件进行分析和诊断，尝试提供解决方案，并进行业务恢复
  - ✓ 对事件进行分类，并指派、协调二线人员予以支持
  - ✓ 作为事件的整体责任人，跟踪、监控事件的处理过程，以确保在规定的时间内解决事件，必要时进行事件升级
  - ✓ 关闭事件前向用户进行解决结果的确认
  - ✓ 确保事件记录信息尤其是解决方案的完整性

- 服务信息岗
  - ✓ 安全响应中心服务台对外公布信息的出口，对待发布信息进行收集、格式化、确认和统一发布
  - ✓ 负责对个人用户信息、部门用户信息进行日常维护，对不完整或不准确的信息进行及时的确认和调整

- ✓ 负责收集用户对 FAQ 的反馈意见，定期召集相关技术人员对向用户公布的 FAQ 的有效性进行评价，并对 FAQ 信息进行相应维护
- ✓ 负责收集 IT 人员对知识库的反馈意见，定期召集相关技术专家对知识库的有效性进行评价，并对知识库信息进行相应维护
- ✓ 负责定期设计、发放和回收用户满意度调查表，并对反馈信息进行统计，生成用户满意度报告，提交事件经理
- ✓ 负责定期收集安全响应中心服务台及事件管理 KPI 数据，制作管理报表和服务报告。管理报表将提交给事件流程经理及管理层分析，服务报告提交事件流程经理（未来可能是客户经理或专项服务经理）审核后递交最终用户。

● 安全响应中心服务台组长

- ✓ 指导安全响应中心服务台人员按照服务目录及服务级别协议提供服务
- ✓ 制定和优化安全响应中心服务台日常工作规范和政策制度，并依照规范和制度对安全响应中心服务台进行管理
- ✓ 维护排班策略，并周期性（如每周）制定安全响应中心服务台人员的排班计划
- ✓ 对安全响应中心服务台人力资源进行日常监控、管理和调度
- ✓ 受理用户投诉，并对升级事件进行协调和处理
- ✓ 收集和整理安全响应中心服务台与客户沟通过程中存在的潜在业务机会和客户需求，并将其反馈给事件流程经理，促进组织整体的业务发展
- ✓ 在事件流程经理的授权下，对安全响应中心服务台人员及二线人员的事件记录质量进行抽查和监督；
- ✓ 协助事件流程经理，定期对事件流程管理报表和用户满意度调研报告进行分析，并就改进机会进行识别和实施

➢ 岗位技能要求

为确保安全响应中心服务台各岗位能够支撑网络安全设备运维部门服务体系，应确保各岗位配备人员满足相应岗位技能要求。安全响应中心服务台岗位作为网络安全设备运维部门对外的窗口，除需要基本的专业知识技能之外，还应具备业务和服务两方面的经验和能力。业务能力应至少包括对网络用户业务流程相关知识，以熟练使用业务语言与用户进行沟通；还应了解业务流程与网络设备架构的关联，以准确定位问题所在。服务能力应至少包括沟通能力、服务意识、运维工作认知水平和管理工具操作能力等，以提高服务质量和效率。各岗位技能要求具体如下：

领域/角色		热线	安全响应中心服务台 Team Leader	二线、内部三线
专项技术	桌面终端知识/技能	熟悉	熟悉	精通
	防火墙应用系统知识/技能	熟悉	熟悉	精通
	入侵检测管理知识/技能			
	网闸、行为检测、沙盒等其他安全知识/技能	熟悉	熟悉	精通
	操作系统安全防护知识/技能	熟悉	熟悉	精通
	综合分析诊断能力	熟悉	熟悉	精通
业务	网络相关业务流程	熟悉	熟悉	精通
	网络相关业务与网络安全设备之间的关系	熟悉	熟悉	精通
服务	沟通能力	精通	熟悉	熟悉
	服务意识	精通	熟悉	熟悉
	运维管理认知水平	熟悉	熟悉	熟悉
	管理工具使用能力	精通	熟悉	熟悉

能力级别：精通、熟悉、了解、基本了解

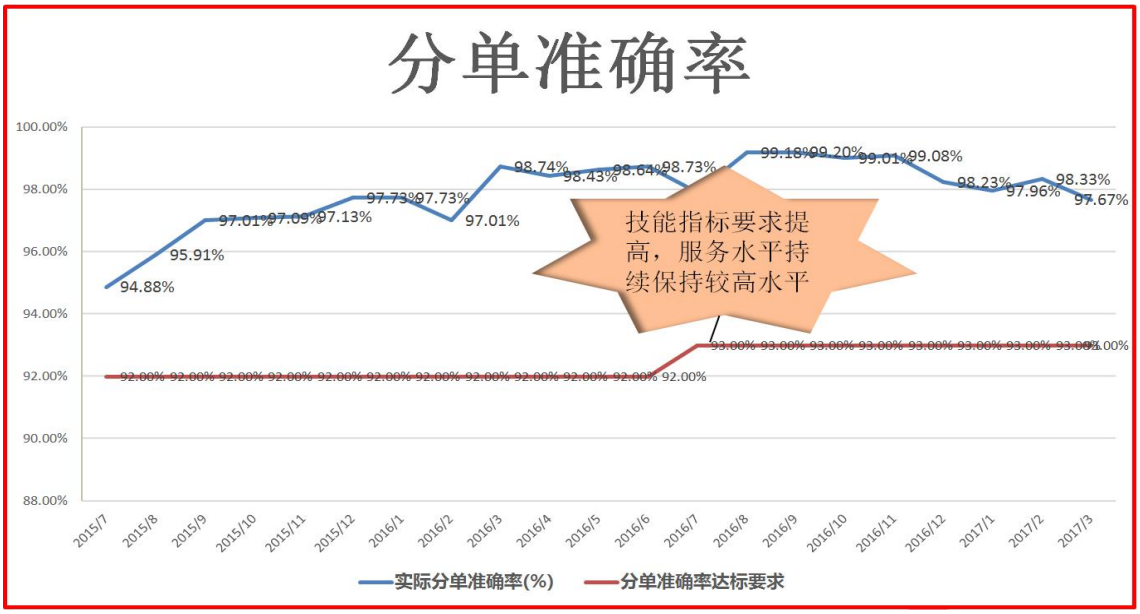
- 安全响应中心服务台服务质量度量

为确保 IT 安全响应中心服务台各岗位人员向用户提供高质量服务，事件流程经理及安全响应中心服务台值班长应针对各岗位特性制定相应绩效考核指标，并定期对人员进行评价。由于安全响应中心服务台采用外包机制，以下列举的岗位绩效，特别是安全响应中心服务台内部座席人员的绩效对 IT 而言是不需要具体掌握的。以下提供的内容供参考。

基于最佳实践，IT 安全响应中心服务台岗位考核指标定义如下：

岗位	考核指标	指标描述	统计方法
安全响应中心服务台值班长岗	客户满意度	用户对网络安全设备运维服务的总体满意度评分，体现用户对服务质量的体验状况	每季度或六个月发起一次客户满意度调研，统计满意度的平均得分
	客户投诉率	用户对安全响应中心服务台提供服务过程中对服务途径、方式、态度、效率和有效性的投诉数量和比率	每月客户对安全响应中心服务台的总体投诉数量，及其占所有投诉的比例
安全响应中心服务台一线支持岗	呼叫应答时间	座席对用户呼叫的拾取时间平均值	每月各座席对呼叫的平均拾取时间
	呼叫损失率	座席对应的呼叫未及时拾取比例	每月各座席对应呼叫损失数量及其在该座席呼叫总量中所在比例
	客户投诉率(对热线服务)	用户对热线座席的投诉比例	每月客户对各座席的投诉数量和比例
	热线解决率	座席直接解决事件的数量和比例	每月各座席直接解决的事件数量和比例
	首次派单成功率	座席派单给现场、二线人员的准确性	每月各座席重派单的数量及其占该座席所有派单数量的比例
	超期转派事件数量	当前安全响应中心服务台转派事件超过规定时间的事件数量	转派时间减去创建时间大于规定时间的事件数量。
	超期解决事件数量	当前安全响应中心服务台处理事件超过规定时间的事件数量	处理人为当前安全响应中心服务台，并且 SLA 违规的事件数量。
	平均解决时间	座席对直接解决事件的平均解决时间	每月各座席直接解决事件所花费的平均时长
	人均开单数量	座席人均登记事件的数量	每月各座席的开单数量和

			比例
	重大事件处理数量	座席参与处理重大事件的数量	每月各座席参与的最高优先级事件的数量
	用户投诉数量	用户投诉由该安全响应中心服务台处理事件的数量	事件性质为投诉，并且处理人为当前安全响应中心服务台。

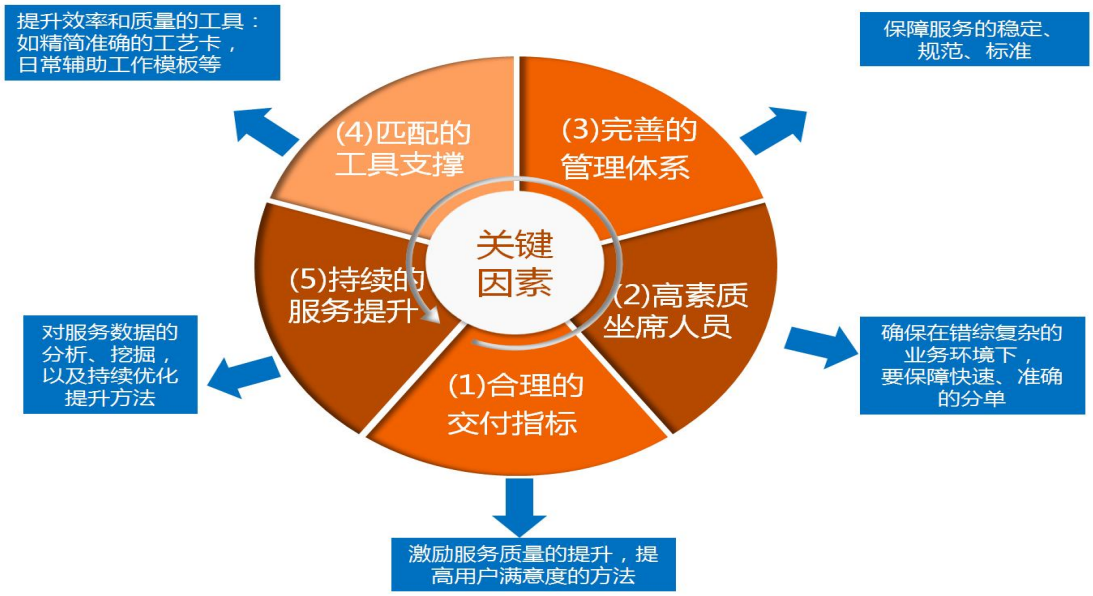


备注：

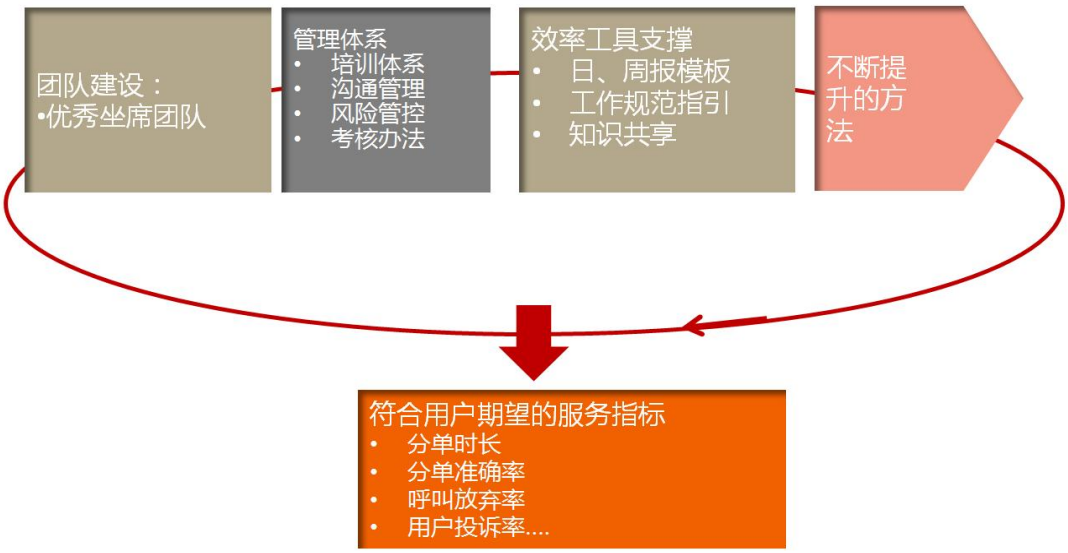
(1)部分呼叫中心的指标，由呼叫中心系统提供。例如呼叫应答时间等。

(2)安全响应中心服务台指标，包括部分事件管理指标、服务请求管理指标。请参见事件管理、服务请求流程。

➢ 安全响应中心服务台关键成功因素



➢ 安全响应中心服务台培训和运营支持管理文档



领域	名称	备注
管理制度	安全响应中心服务台日常工作规范 服务用语规范 坐席工作规范 Team Leader 工作规范	
服务报告	服务报告模板 服务改进模板 服务改进点	

	服务改进跟踪报告	
培训	沟通培训 专业技能培训 业务知识培训 组织结构培训 沟通能力考核表 技能考核表	

- 安全响应中心服务台日常工作模板示例

  - **重大安全事故发生通报模板**

尊敬的 XX 业务用户：

我们抱歉地通知您，在_____时间_____系统发生了_____现象，影响到_____。

该故障已被记录到我们的网络安全设备运维平台，事件单号为：_____。我们将采取下列措施来进行故障处理：

1._____。

2._____。

3._____。

本次故障的处理负责人是_____，联系方式：_____。预计在_____时间内，_____得以缓解或者恢复。

有关该故障的处理进展和处理结果，我们将在第一时间以电话或者邮件方式通知您。

谢谢您的理解和支持。

网络安全设备运维服务中心

服务热线：400-XXXX-XXXX

邮件地址：itservice@ rxgt.net

进入 ITSM 门户查看该事件的详细情况：http://URL。

- **重大安全事故通报规则**

由安全响应中心服务台 Team Leader 负责重大事件通报。

优先级	通报 1 专业领域 Manager	通报 2 IT Department Director	通报 3 CIO
一级	立即	30 分钟	1 小时
二级	30 分钟	1 小时没有解决方案	2 小时没有解决方案

通知列表：

Name	Location	Title	Office Number	Mobile Number	Email Address

- **重大事件进展通报模板**

示例模板如下：

尊敬的 XX 业务用户：

我们愿意及时通知您有关事件单_____的处理进展信息。该故障在_____时间_____发生导致_____现象，影响到_____。我们已经采取了下列措施来进行故障处理：

1._____。

2._____。

3._____。

取得了如下进展：

*1.*_____。

*2.*_____。

*3.*_____。

*我们预计在*_____*时间内，*_____*得以恢复。*

有关该故障的进一步处理进展和处理结果，我们将在第一时间以电话或者邮件方式通知您。

谢谢您的理解和支持。

网络安全设备运维中心

服务热线：400-XXXX-XXXX

邮件地址：itservice@ rxgt.net

进入 ITSM 门户查看该事件的详细情况：http://URL。

- **重大事故恢复通报模板**

示例模板如下：

尊敬的 XX 业务用户：

*我们高兴地通知您事件单*_____*已得到解决，服务已恢复。该故障在*_____*时间*_____*发生导致*_____*现象，影响到*_____。

有关该故障的原因分析和处理结果报告，我们将在第一时间以电话或者邮件方式通知您。

该故障导致您工作上的不便，敬请谅解。感谢您对我们工作的监督和支持。

网络安全设备运维中心

服务热线：400-XXXX-XXXX

邮件地址：itservice@ rxgt.net

进入 ITSM 门户查看该事件的详细情况：http://URL。

- **VIP 人员名单**

一般采用 EXCEL,并技术同步到 ITSM 人员信息

- **系统和服务停用通知模板**

示例模板如下：

尊敬的 XX 业务用户：

您好！由于_____原因，我们将对_____的系统进行服务停止。开始时间_____，预计结束时间_____。在此其间，_____服务部门使用。

（如果有变通或者预先准备措施）我们建议您：

_____。

该服务暂停使用导致您工作上的不便，敬请谅解。感谢您对我们工作的监督和支持。

网络安全设备运维中心

服务热线：400-XXXX-XXXX

邮件地址：itservice@ rxgt.net

进入 ITSM 门户查看该事件的详细情况：http://URL。

- **满意度调查模板**

用户填写满意度模板：

调查：	事件摘要

事件 ID：	ID
问题 1 ：	是否及时提供了服务？
等级：	（1）不满意（2）一般（3）满意
问题 2 ：	技术人员是否专业？
等级：	（1）不满意（2）一般（3）满意
问题 3 ：	是否对问题的解决感到满意？
等级：	（1）不满意（2）一般（3）满意
问题 4：	技术人员是否有礼貌？
等级：	（1）不满意（2）一般（3）满意

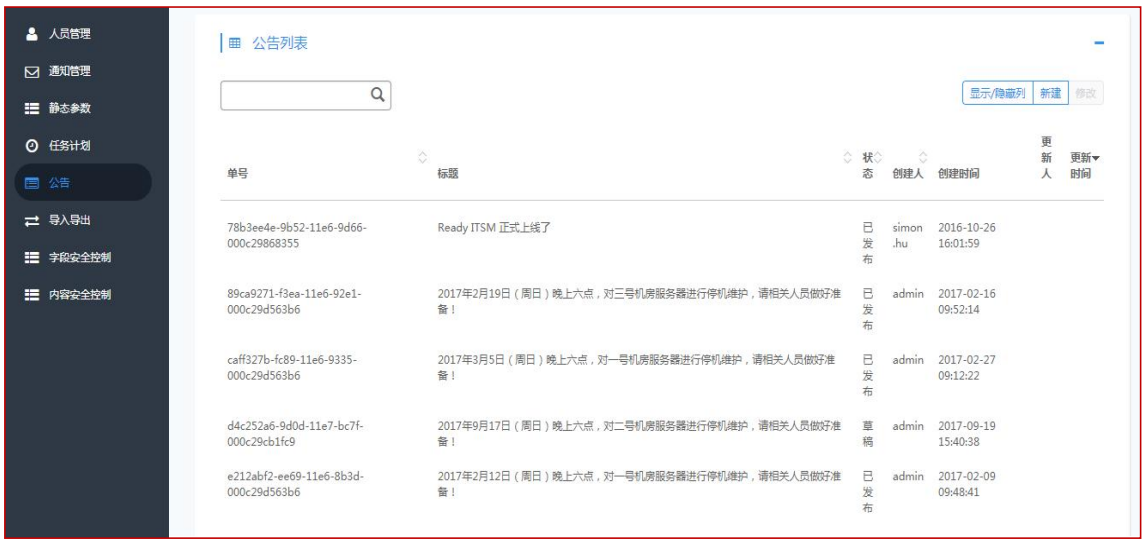
- **满意度调查结果报告模板**

内容包括：

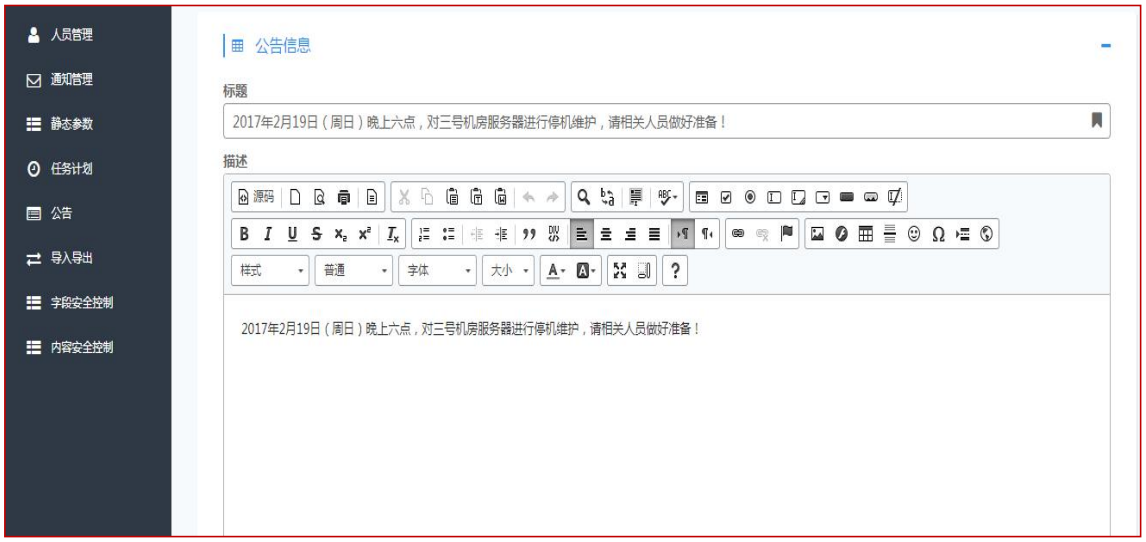
文档编写人员	
文档版本	
满意度调查时间	
满意度调查方式	
满意度调查问卷	
满意度调查结论简述	
满意度反馈数据	
满意度结果分析	
行动建议和计划	

➢ RXGT ITSM 安全响应中心服务台专项工具支持

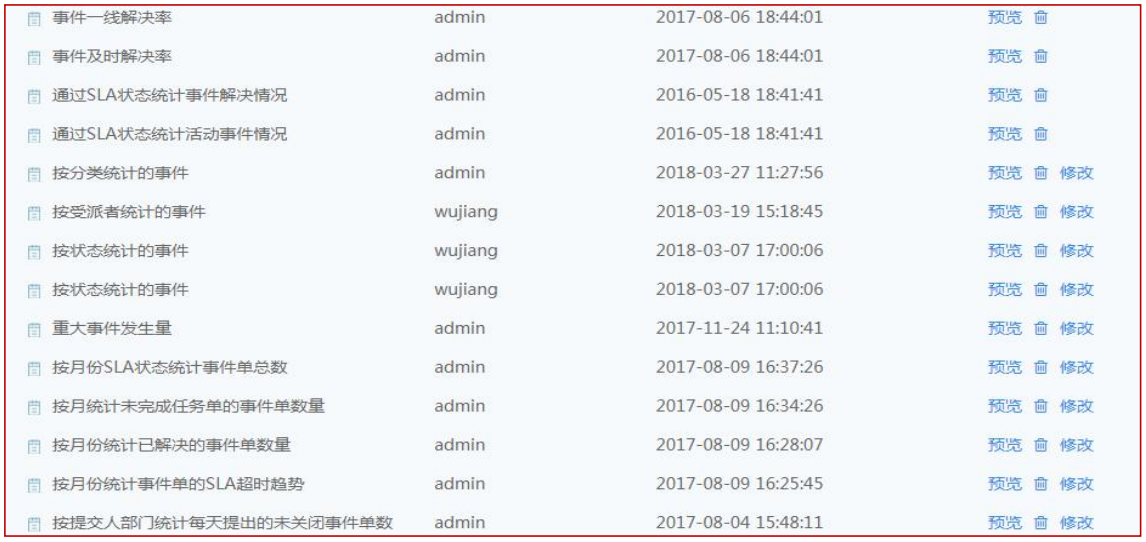
安全响应中心服务台公告显示列表设计：



发布公告：

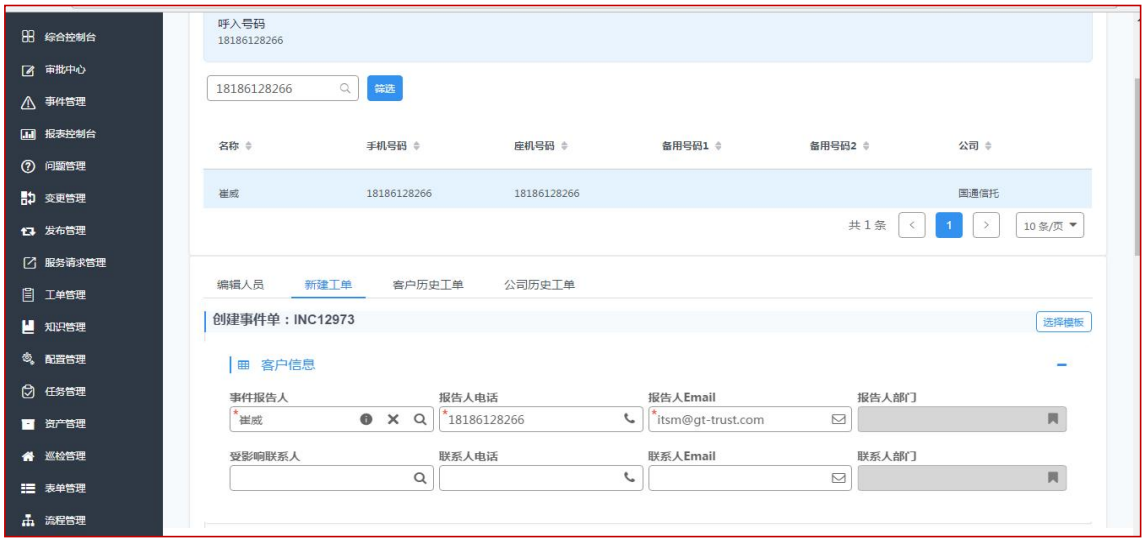


安全响应中心服务台报表管理：

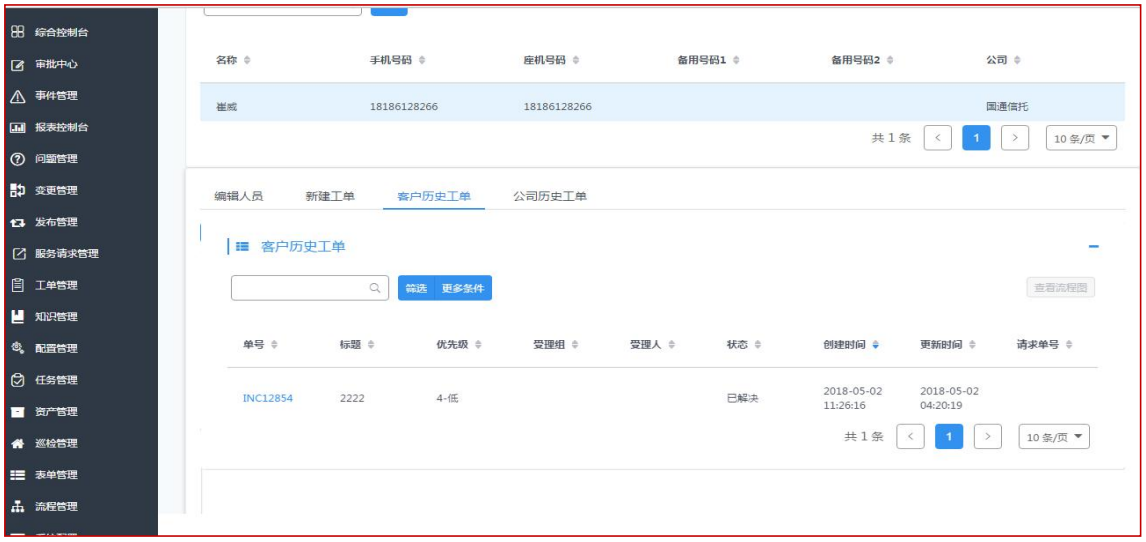


报表需要授权用户才能查看，展现已授权该用户查看的报表

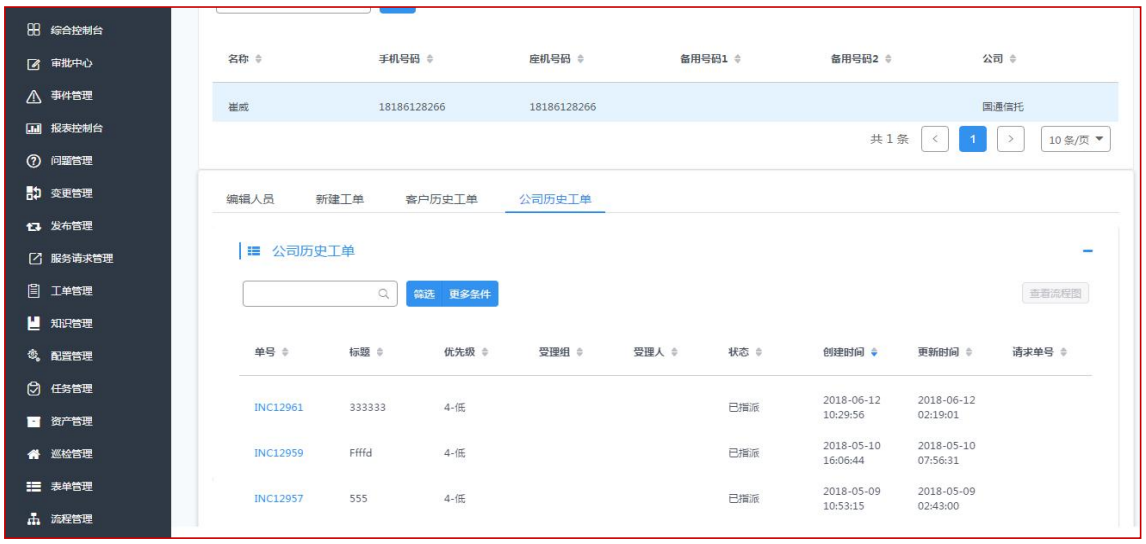
与 Callcenter 集成来电弹屏信息，如果 VIP 来电，将以红色背景来显示用户基本信息



查个人看历史工单



查看公司历史工单



安全响应中心服务台的流程与报表信息请查看事件管理的流程与 KPI 信息。

7、安全设备故障管理

➢ 流程目标与范围

事件（也称故障）是指信息系统运行中引起或可能引起服务中断或服务水平质量下降的活动及相关事件，包括以下几种：

- 系统运行事件，是指影响或可能影响业务应用、系统环境、网络通信、机器设备、机房设施等正常有效运行的事件；
- 业务处理咨询，是指咨询前端操作疑问、批量执行进度、系统备库时间、文件传输情况等内容；
- 主动运维，是指信息科技部内部用户进行健康检查以及其他例行操作；

事件管理(Incident Management)流程的主要功能是尽快解决影响应用系统正常运行的事件，保持业务支撑系统的稳定性。

其对企业的价值如下：

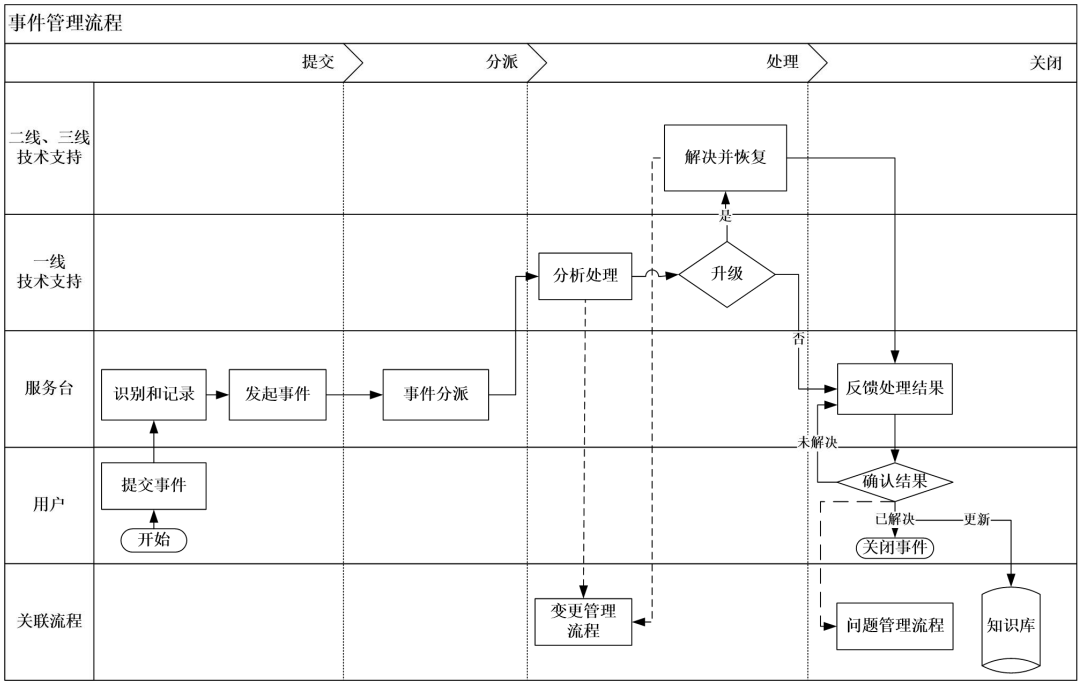
- 帮助网络用户尽快恢复网络服务
  - ✓ 快速响应服务请求（电话/Web 等）
  - ✓ 用户在线获得帮助
  - ✓ 沟通事件解决的状态

- ✓ 和客户确认事件的解决

- 帮助企业进行事件控制
  - ✓ 按规范记录事件
  - ✓ 就事件的优先级，影响度进行分类
  - ✓ 分析，诊断，必要时进行升级
  - ✓ 监视并结束事件
  - ✓ 进行定期服务流程回顾

- 为企业提供 IT 管理信息
  - ✓ 人力资源利用情况
  - ✓ 事件处理情况
  - ✓ 支持效率

➢ 流程关键活动



事件管理流程

事件是中断业务流程和降低网络服务质量的错误。事件管理模块帮助迅速解决这些事件，并最小化对于业务的不利影响。流程始于事件的接收和报告，结束于事件的解决。该模块包含下述主要功能：

- **事件接收和记录**

这个环节是事件管理流程的起点。所有用户或系统报告的 IT 事件必须由此步骤开始。此步骤的目的是在事件发生时快速准确地发现，以协助事件的诊断和解决并通知相关人员。在此步骤中将会收集创建事件记录所需的信息。

该环节的关键是信息的准确性和完整性。

- **分类和在线支持**

事件可以是一个申告/事件/告警/咨询，对于每个事件，需要确立优先级和分类。若没有现成的解决方案或临时解决措施，该事件将分配给合适的支持人员对此进行调查。

该环节的关键是必要的问题库支持和正确的事件分派。

- **调查和诊断**

若支持人员无法解决事件，可运用问题库、诊断工具等进行更加深入的分析以找到恢复服务的临时措施，必要时可调用多名支持人员以寻求解决措施。

- **解决和恢复**

支持人员实施事件的解决方案，并将解决完毕的事件转回安全响应中心服务台，由安全响应中心服务台通知用户解决的结果，并得到用户的确认。

- **优先级为紧急的事件（紧急事件）和事件升级**

对于紧急事件，安全响应中心服务台应立即提交给一线人员，由一线人员判断，上报给事件经理和相关的管理层，由事件经理决定紧急事件的处理方式，确保其得到最快速的解决。

当事件处理超过预期时限，将自动通知处理人员和相应管理层，以引起相关人员和管理人员的重视和参与。

- **结束事件**

当用户确认事件解决后，此时可结束该事件，并在必要时更新问题库

- 角色职责与考核 KPI

角色	职责
事件经理	1. 监控事件流程运行状况

	2. 负责对事件解决过程的安全响应中心服务台与二线的资源协调，保证事件的最终排除 3. 当事件超时升级或重大事件升级时，负责或参与资源协调，解决事件 4. 确保和问题管理流程的有效合作 5. 对事件管理流程运行绩效及支持人员绩效进行周期性的统计、分析，并寻找机会进行优化和改进； 6. 超时、重大事件汇总通报； 7. 主导协调重大事件的协调，作为重大事件的负责人。安排、调动应急小组人员进行具体工作。 8. 定义应急小组成员；
安全响应中心服务台一线	安全响应中心服务台一线，负责受理各类 IT 运维事件和事件的初步处理，具有以下职责： 1. 作为网络安全设备运维服务的统一入口，负责所有事件、服务诉求的记录、初步处理、分配、跟踪和关闭。 2. 24 小时值班，通过电话、邮件、Web 受理各类事件，并人工录入 IT 运维服务管理平台。IT 运维服务管理平台无法工作需手工纸面作业时安全响应中心服务台填写《事件记录单》。系统恢复起一日之内，安全响应中心服务台补录事件单。 3. 自动监控系统新建产生的事件单，也是由安全响应中心服务台统一受理和跟踪； 4. 负责跟踪事件的解决过程，及时向事件报告人通报事件的解决和进展情况。 5. 对处理完毕的事件，安全响应中心服务台应及时对事件报告人进行回访确认，并进行事件工单的关闭处理。

	6. 负责定期回访客户，跟踪客户满意度，并填报《客户满意度调查报告》。
安全响应中心服务台组长	1. 在安全响应中心服务台热线组内监控事件流程运行状况。 2. 负责对事件解决过程的安全响应中心服务台一线的资源协调。 3. 负责与事件经理进行沟通，当事件超时升级或重大事件升级时，负责或参与资源协调，解决事件。 4. 对安全响应中心服务台一线的运行绩效进行周期性的统计、分析，并寻找机会进行优化和改进。
二线支持（事件处理专家）	1. 二线支持人员实行 24 小时待命工作制，负责解决安全响应中心服务台一线支持无法处理并分派的事件。 2. 事件解决后，提交给安全响应中心服务台一线人员。对于不能解决的事件，事件受理人须将具体原因记录在 IT 运维服务管理平台中，并将事件单分派给三线支持（包括内部三线和外部三线，即第三方服务、设备提供商）。
内部三线支持	1. 负责处理二线支持升级的事件。 2. 根据专业技能制定有效解决方案或临时变通方法，并交由二线进行解决。 3. 必要时与第三方厂商或者服务商合作，确定解决方案或临时变通方法。 4. 主导制定审核应急预案。
外部三线支持	1. 外部三线支持人员为第三方服务、设备提供商，协助二线支持处理事件。对于二线支持人员无法处理的事件，提供解决方案，再由二线支持按照解决办法处理。

流程 KPI 指标：

- 用户满意度
- 用户投诉率
- 服务级别满足率
- 安全响应中心服务台电话接通率
- 安全响应中心服务台电话平均响应时间
- 安全响应中心服务台事件处理合规率
- 二线事件处理合规率
- 一线解决率
- 事件平均解决时间

➢ 平台重点功能及示例

平台实施重点

- 支持事件的新建、撤销、修改、退回、处理、转办、升级、关闭、回访；
- 支持事件受派组内部转单，支持创建事件记录时自动记录创建日期、时间、发起人信息、事件描述等内容；
- 支持事件按照影响范围、涉及系统类别、紧急程度进行分级；
- 支持查询跟踪事件处理进度，可根据处理状态、受理人、事件类别、联系人、客户等条件查询,查询结果可以导出到 EXCEL 文件；
- 支持处理过程可以随时启用“参考知识”功能，快速定位相关解决方案和案例；
- 支持调度事件单功能，安全响应中心服务台坐席人员有权调度事件单给其他人员处理，避免延误时间；
- 支持事件升级功能,如安全响应中心服务台一线无法解决用户请求时,升级至二级支持。如二级支持不能完成的，升级至三线或厂家支持，直到关闭事件；
- 支持在事件处理完毕后，由事件处理人或系统管理员一键生成知识库条目，并进行关联操作，形成知识库与事件之间可追溯的信息流；
- 支持自动生成巡检等定期任务事件并分派功能；

- 支持与 CMDB 联动集成，能通过关联分类灵活读取 CMDB CI 信息。
- 支持事件结束后自动发送邮件给客户进行满意度调查，并反馈。

工具示例

图 1：事件控制台

标记 1：事件计分板，用简单直观的数字展示当前用户最关心的事件流程指标，例如“待我处理（的事件单）”“我 SLA 预警（的事件单）”等等。

标记 2：事件单列表，选择不同计分板，列表将展示不同的事件单记录。

标记 3：导入/导出，可下载导入模板，按照模板批量导入事件单。

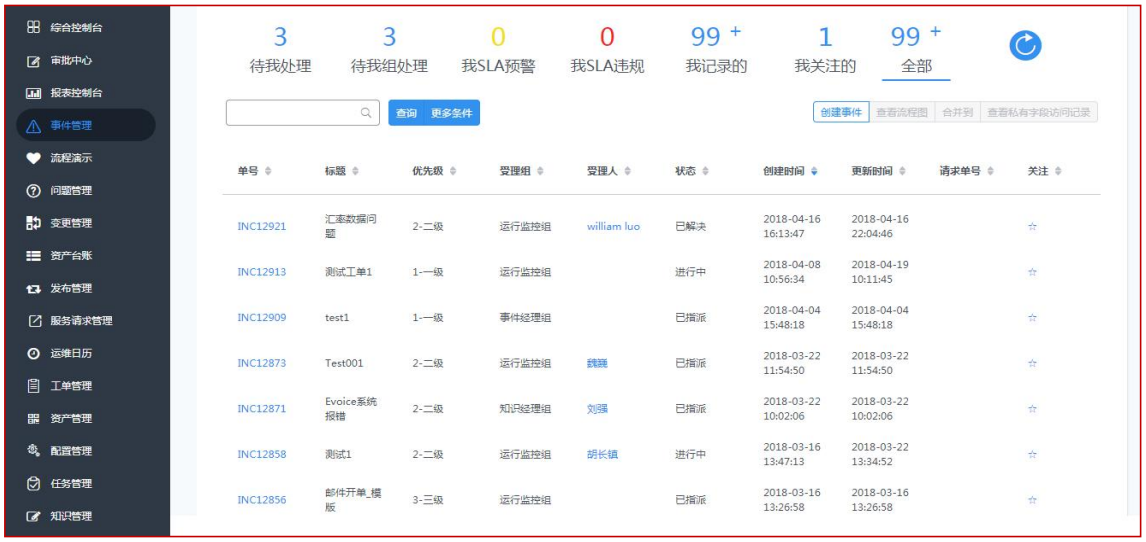


图 2：事件搜索

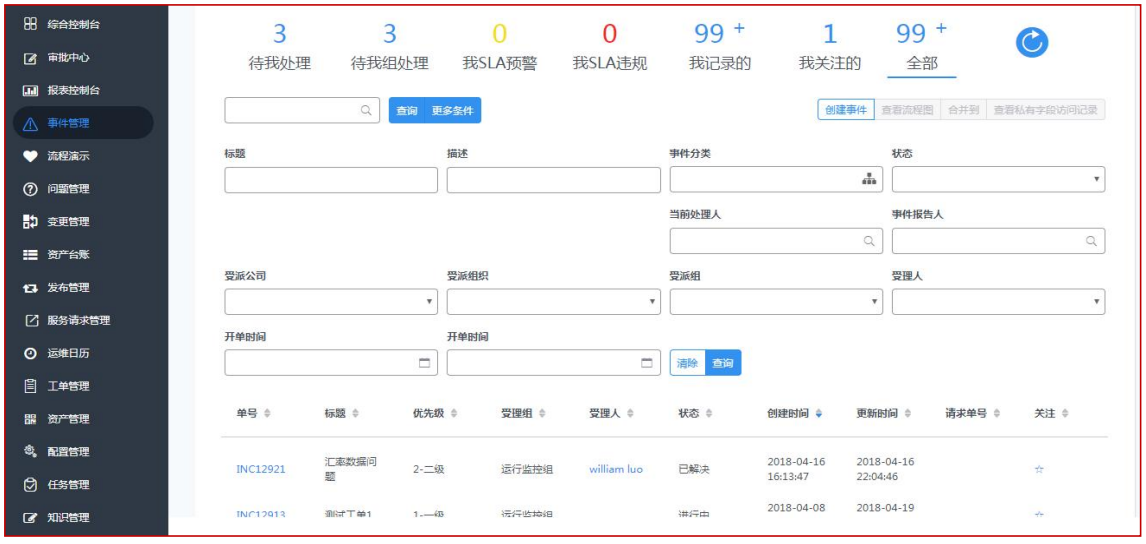


图 3：事件单详情

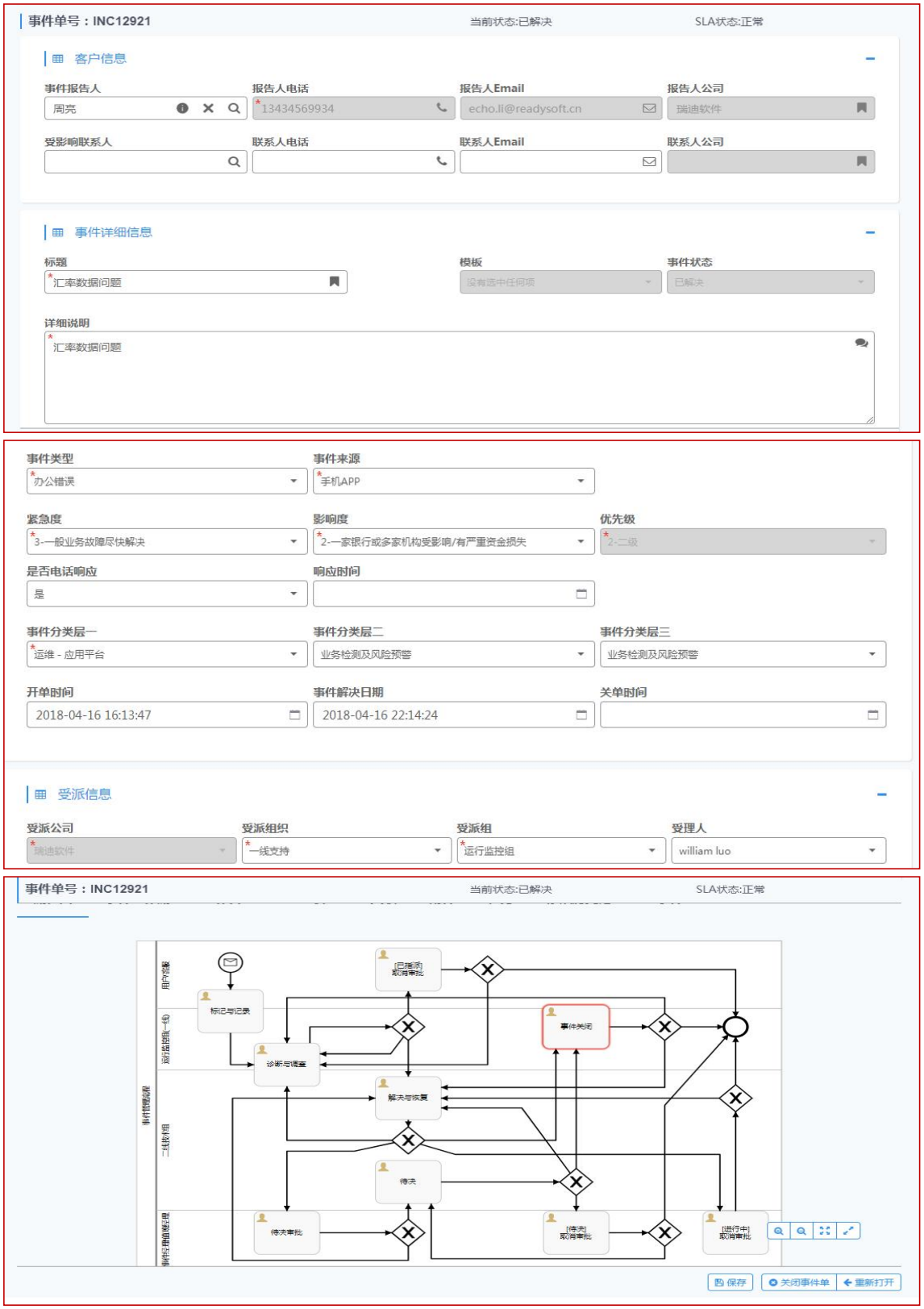
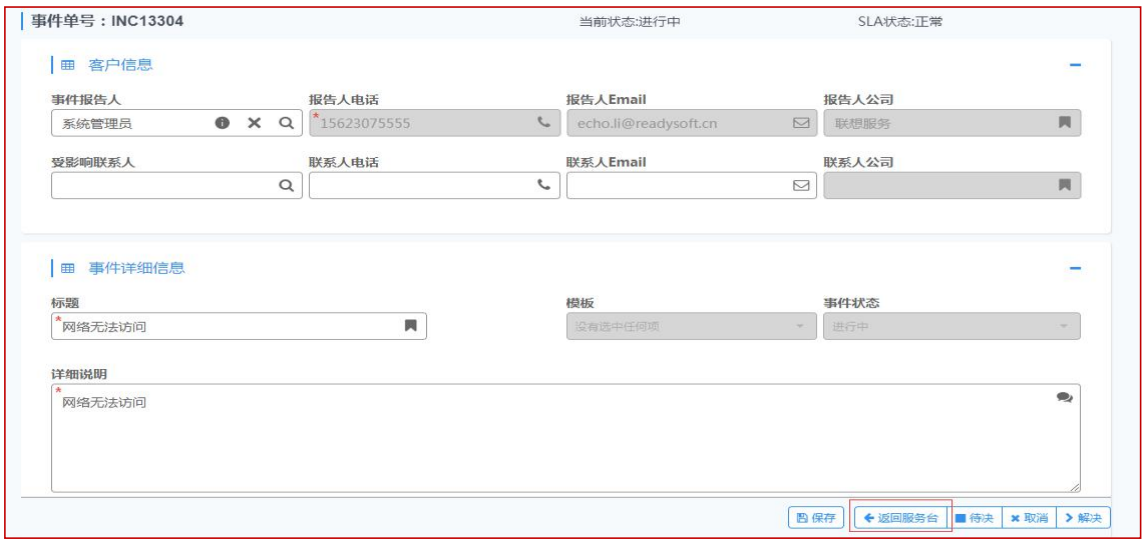
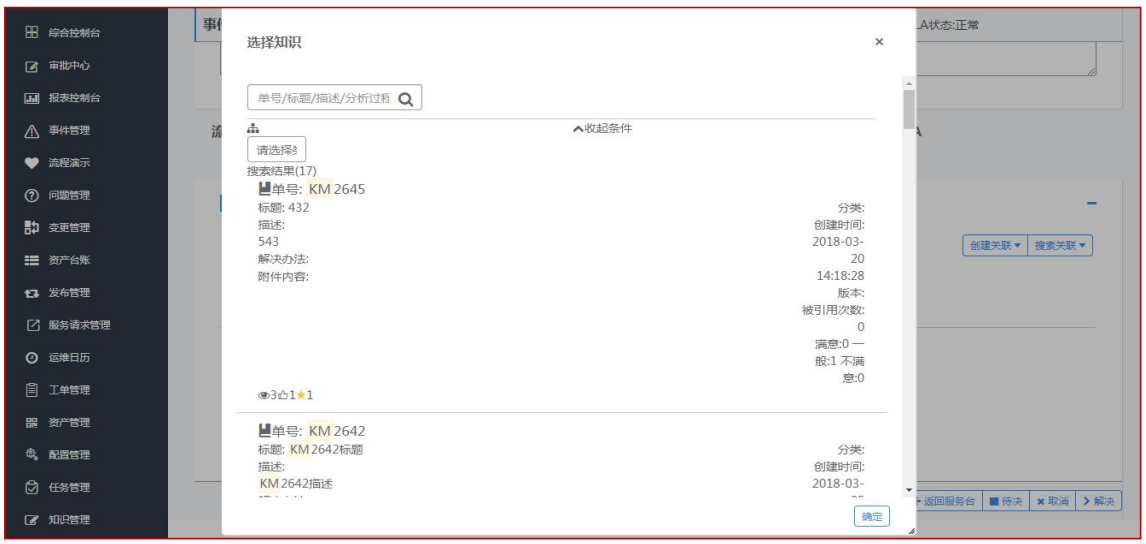


图 4：事件升级/参考知识

事件退回安全响应中心服务台重新分派或直接转派。



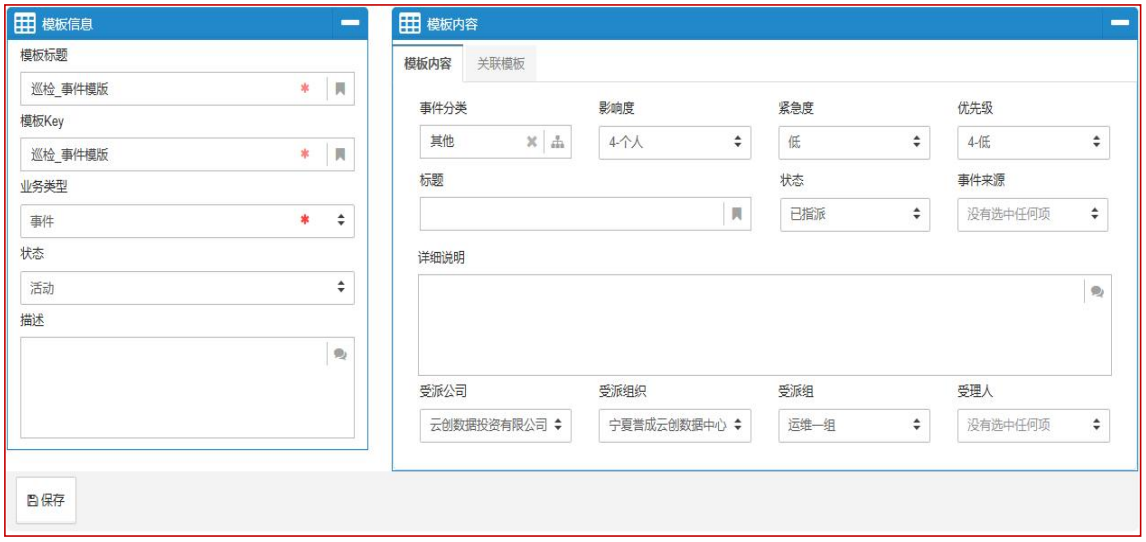
搜索关联知识库。



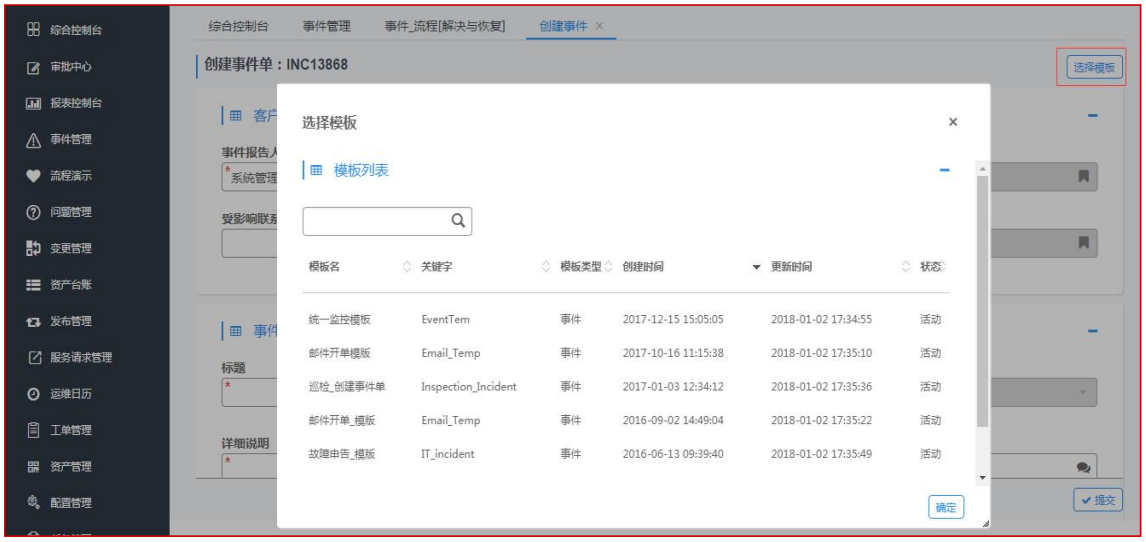
事件与问题变更等单据的关联：

事件流程报表：

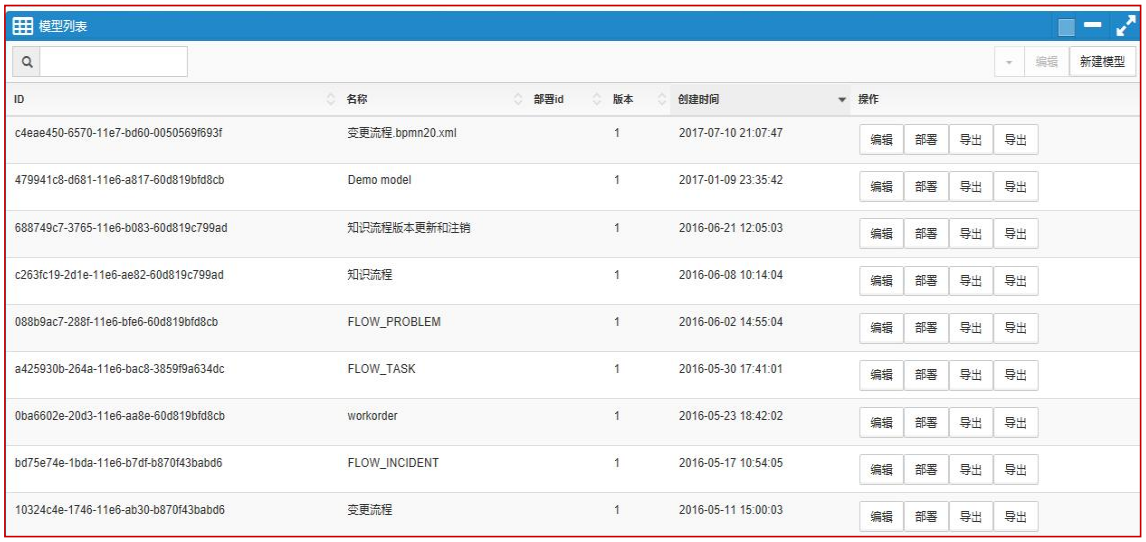
事件快速创建模板：



在事件单上选择模板



自定义修改事件流程：



事件修改历史记录功能：

事件服务评价：

8、安全设备隐患管理

➢ 流程目标与范围

问题管理（也称隐患管理）是网络安全生产环境发生各类问题的报告、受理、解决和反馈的管理过程。问题来源主要包括规避解决或未解决事件以及主动进行事件趋势分析或健康检查、巡检中发现的问题，以及由变更引发的一些问题。

问题管理的目标是将由网络安全业务系统错误引起的事件和问题对业务的影响减少到最低程度；查明事件或问题产生的根本原因，制定解决方案和防止事件再次发生的预防措施；实施主动问题管理，在事件发生之前发现和解决可能导致事件产生的问题。从问题申报、归类、分派、处理到最后结束，所有的过程均在问题管理中进行了严格合理的定义。从而保证问题处理的所有环节有条不紊，并具有最优效率。

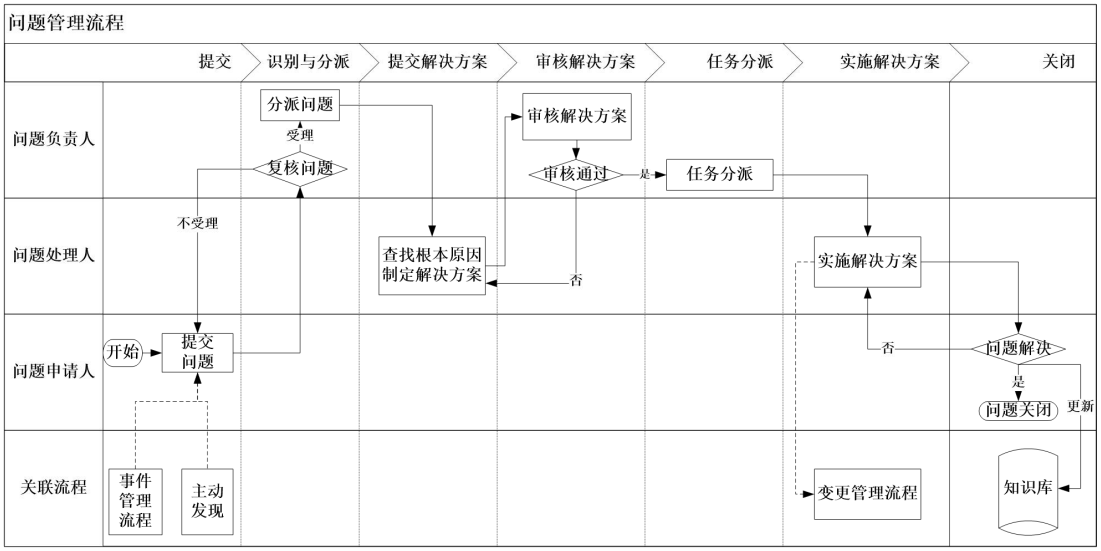
问题管理模块应提供如下功能：

- 支持多种问题申报方式如：通过事件创建和手工创建，并支持各类附件形式的问题描述。
- 提供问题的分类（严重等级、影响程度、紧急程度的分类）和优先级的设置。
- 可以和其他流程管理模块进行无缝集成，如：关联与相关的事件、从问题创建并关联变更、关联与问题有关的 CI 配置等。
- 支持不同的角色和权限对问题进行管理与审核，提供自动分派和手工分派，并

支持重新分派。

- 提供问题的升级机制，比如根据处理时间和目标时间升级到不同的组或者人。
- 支持问题的各种通知，通知的方式包括邮件、短信。
- 问题单的关闭可以通过手工关闭或自动关闭。
- 对已经找到根本原因但暂时无法根本解决的，通过独立的已知错误管理流程进行管理，要求提供临时解决方案。
- 对于已经找到根本原因且有解决方案的问题，可以提交知识条目给知识管理，同时过程中可方便地查询检索知识库。
- 问题审计：能够记录数据变化前后的修改人、时间进行记录保证数据的安全性。
- 支持重复问题或相似问题的关联。
- 提供对问题的任务进行拆分，把一个问题拆分成 N 个子任务来进行，并且每个子任务可以有不同的负责人，以更好的管理和执行问题调查任务。
- 支持在问题管理流程中查找和创建知识，问题支持人员可以建议一个新的解决方案提到知识库里，作为问题处理预案保存在问题管理中。
- 提供问题计数器，可以直接在控制台中显示不同状态的问题数量。
- 提供开箱即用的关键流程衡量指标（KPI），以有效地对问题管理流程的运行情况进行监控和改进。
- 提供图形化的问题管理流程设计功能。

➢ 流程关键活动



问题管理流程

- **分析事件**

定期分析事件，找出潜在问题。

- **生成问题记录**

在系统中生成问题记录并把所有相关事件与此记录关联起来

- **分派**

根据问题内容将问题记录分派给适当的技术小组。

- **根本原因分析**

被分派的小组人员将调查问题以期找出其原因，提出解决方案、变通方法或预防性措施，以消除产生原因，或在重发时使其影响力最小化。 记录必须被更新以反映它是已定位原因状态，并且把任何变通方法、避免或最小化负面影响的动作行为也记录下来。

- **开发、确认、提出实施解决方案**

对问题的解决方案进行评估、测试，提出变更请求（RFC）或实施具体的解决方案。

- **回顾及关闭**

对问题的解决方案进行回顾，确认解决方案达到了预期的效果。

确认问题的信息记录填写完整，提交知识库，并关闭问题记录。

➢ 角色职责与考核 KPI

角色	职责
问题经理	问题经理负责协调日常的问题管理工作，包括对问题的审核、监控、所需资源的协调、编写重要问题报告等。问题经理由技术管理岗和客服管理岗人员担任。其主要职责是： ✓ 负责受理问题单的申请。通过审核问题申请判断是否需要处理该问题。 ✓ 负责指派问题单的具体处理人。 ✓ 负责协调和监控问题单的处理和资源的调配
问题提交人	问题提交人仅包括 IT 的二线支持人员、事件经理、问题经理。 ✓ 问题提交人负责问题的创建和提交。

问题处理专家	问题处理专家由 IT 各技术岗人员和第三方服务提供商技术专家组成。 ✓ 问题处理专家负责为问题的诊断及解决提供技术支持。

考核 KPI：

- 问题单按时完成率
- 问题分析任务的及时完成率
- 已找到根本原因的问题数量及占比
- 未根本解决问题数量及占比

➢ 平台重点功能及示例

平台实施重点

- 支持问题的新建、撤销、修改、退回、处理、关闭、回访。支持创建问题记录时自动记录创建日期、时间、发起人信息、问题描述等内容；
- 支持符合一定规则的重点事件升级为问题，进行进一步的分析处理；
- 提供自动分派和手工分派，并支持重新分派，支持在流程每一环节都应该可以按照事先设置的要求进行人员的指派，并通过邮件或短信方式进行通知；
- 支持文字、图片、附件等记录方式，完整记录问题处理过程中的修改内容、修改人、修改时间，并可提供问题管理多视角展现功能；
- 支持问题设置不同紧急程度，并根据紧急程度设置不同超时时间。
- 支持问题处理过程中，处理人对问题的影响范围、涉及系统、影响时间等相关信息进行补充；
- 支持与 CMDB 联动集成，能通过关联分类灵活读取 CMDB CI 信息。
- 支持处理问题的过程可以参考知识，快速检索与问题有关的案例知识；
- 支持有价值的问题解决方案归档到知识库。

工具示例

图 1：事件升级问题

打开事件单页面，可直接创建问题。

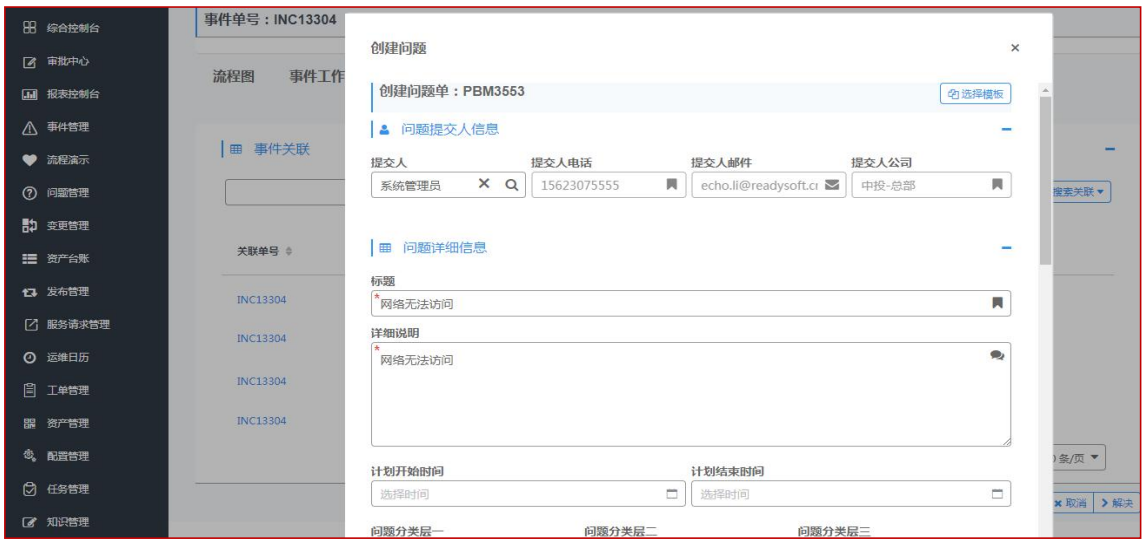
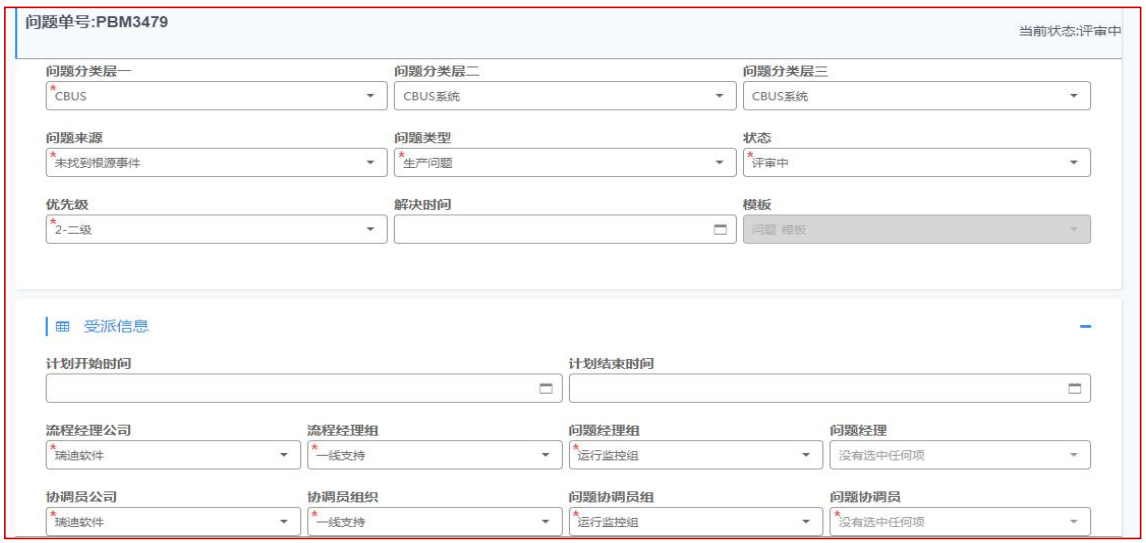


图 2：问题单详情页面

英文版示例



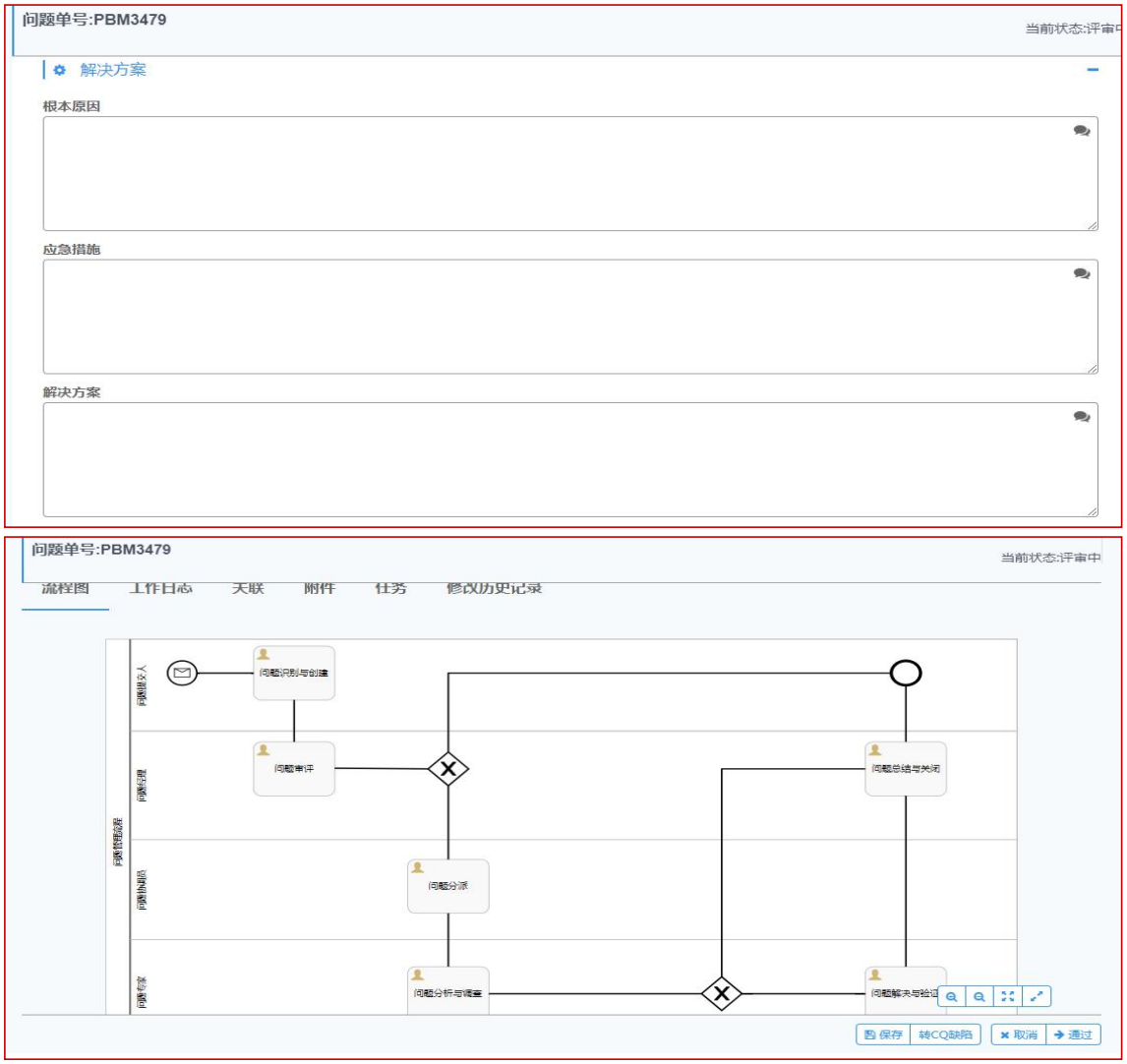


图 3：问题分派

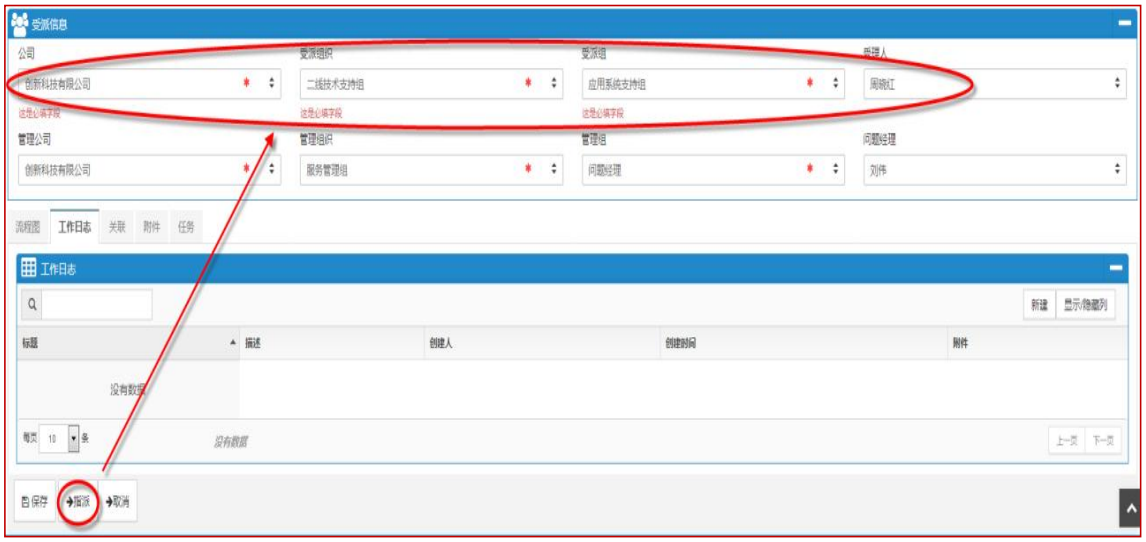
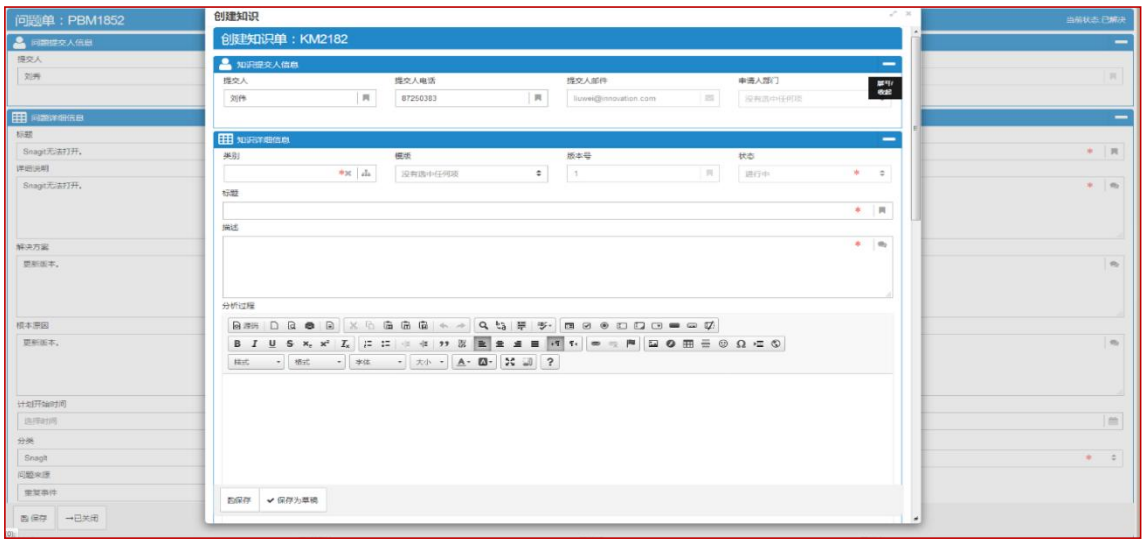


图 4：问题方案转化为知识库

问题被解决后，问题单解决方案可直接提炼成知识文章，进入到知识库中。



9、网络安全变更管理

变更管理对象是对生产环境发生变更的申请、受理、审批、实施、反馈与评价的管理过程，变更管理包括标准变更、一般变更和紧急变更，变更按类型分为生产变更、生产环境变更（包括网络维护）、数据维护。生产变更因涉及程序版本的变更，流程节点较多，故将版本变更单独作为生产验证流程来处理。

新系统上线作为一种特殊的变更，准备周期长，需要协调开发，运行，维护等多个部门，涉及生产环境、网络环境、生产变更等多个变更类型。新系统上线涉及上线准备部分纳入项目管理进行管理，涉及维护的生产变更确认表，包括基础环境确认表、主机环境确认表、网络环境确认表、应用环境确认表、配置管理确认表、安全管理确认表等目前是通过线下沟通、实施，计划在项目二阶段结合发布管理纳入网络安全设备运维管理进行流程固化。

➢ 流程目标和范围

变更管理的目标是确保在变更实施过程中使用标准的方法和步骤，尽快地实施变更，以将由变更所导致的业务中断对业务的影响减小到最低，重要控制点在于风险控制。

变更管理模块应提供如下功能：

- 为简化变更创建过程，提供变更创建向导功能，引导变更请求人通过模板、一步一步提供变更信息，保证变更请求提交的准确性。
- 支持人工直接录入变更或由服务请求、事件和问题自动产生变更请求(RFC)功能；支持在事件和问题记录上直接创建变更记录内容，系统可根据自动填写分类、解决期限等信息。
- 变更关联：支持配置记录、配置工作单与配置管理 CI 项关联，提供在 CMDB 内根据类别、所属业务等条件检索符合要求的 CI 项并批量建立关联

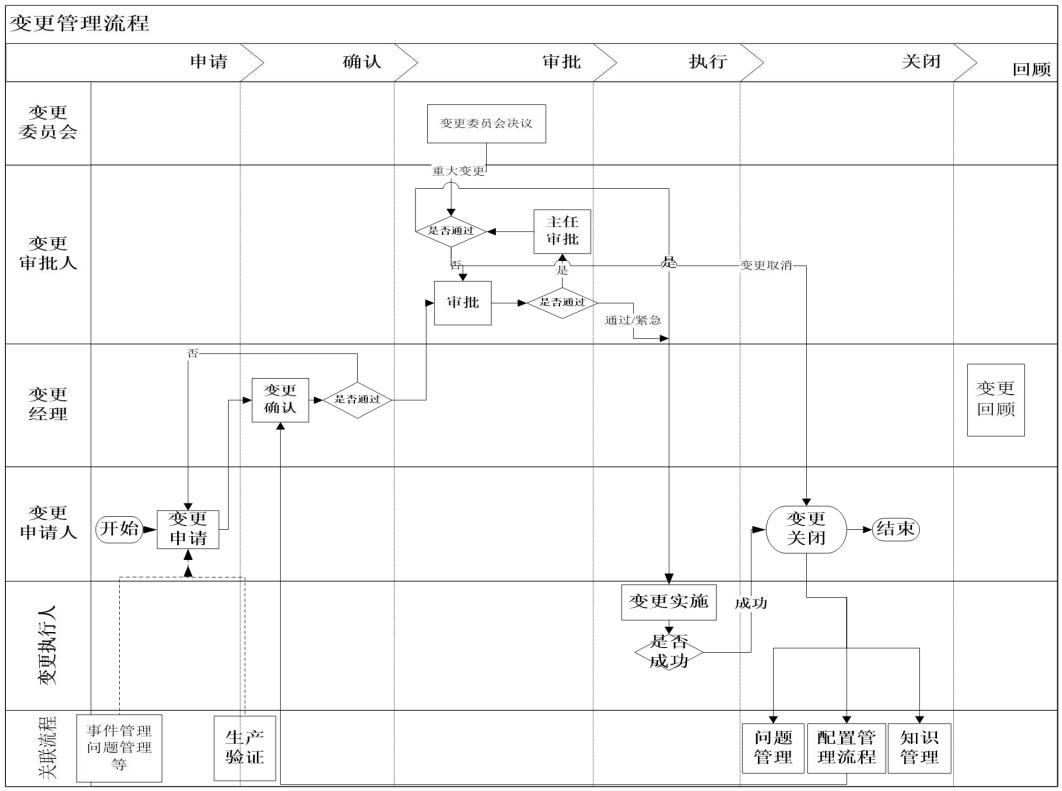
- 提供变更的风险评估、影响评估和冲突分析工具包括变更日历，帮助变更人员进行变更的处理。
- 要求具备变更影响分析和影响模拟功能，变更流程通过与 CMDB 的整合，可以对变更的 CI 项进行影响模拟，模拟该 CI 不可用时，所影响到所有相关 CI。通过影响模拟功能可以提高变更影响分析的完整性和准确性，降低变更风险。
- 要求具备变更冲突检查功能，变更流程可以检查是否存在同一时间段内对同一配置项的多变更请求的情况，如果存在上述情况，则提醒有变更冲突，避免变更失败的产生。
- 支持多人、不同内容的审批策略管理；支持审批人通过移动 APP 客户端随时随地进行变更审批；支持审批表自动化生成，可根据审批任务类型生成审批业务规则，自动确定审批者和审批表内容，支持审批表和工作单的自动派发功能。
- 要求具备成熟的审批引擎，变更流程提供审批引擎，可以实现串并行审批和多级审批，系统采用一票否决制的变更审批规则。变更审批引擎同时提供审批替代人功能，变更审批人不在岗的时候，可以由预置的审批替代人进行代审批。
- 要求具备灵活的变更路径配置功能，变更流程能提供变更请求审批、变更影响分析、变更实施前审批和变更实施后回顾四个控制点，可以根据变更类型（标准变更、例行变更、紧急变更）的不同灵活定义每个类型的变更路径，从上述四个控制点中选择适合的控制点，实现变更控制与效率的平衡。
- 变更任务：在变更管理中可以创建变更任务，支持利用计划工具交互式的分析和显示工作管理和维护信息。
- 在变更单中可以输入、查看、修改或删除变更任务，在变更任务中需要能够管理员工、物料、服务和工具的信息。用以记录员工小时数和成本、物料数量、服务成本和工具成本。
- 变更沟通：提供移动 APP、公告板、电子邮件等方式与 ITSM 管理操作人员和维护人员进行变更管理操作的协调和沟通。
- 变更关闭：提供与变更关闭相关的事件、问题和配置的自动关闭功能，变更记录状态为关闭时可自动修改与之关联的事件、问题、配置状态。支持变更关闭时，撰写变更完毕通知单到事件管理模块，并以 WEB 公告或电话等方式向用户回馈。
- 变更核实：可以和其他自动化工具集成，提供对实际配置情况和系统内的配置信息对比核对，并可以触发响应动作（包括但不限于：邮件、告警，变更自动回退，配

置自动校正等）。

- 变更流程控制：提供变更管理全程的操作跟踪和监控功能，支持变更测试和变更后的检查、操作评估功能。
- 支持与发布管理流程的无缝集成，并提供与发布打包与部署自动化管理工具集成的完整变更流程。
- 提供组合条件的变更请求记录、变更工作单、审批单包括历史记录在内的查询和统计功能，提供精确和模糊查询。可生成变更记录报告和统计报表，支持表格、饼图、柱状图等各种方式显示，具有打印功能。可定制变更管理报表。
- 提供变更与相关事件/问题相关联的功能。能够自动查询出与特定变更相关联的事件和问题，并统计出相关的影响。

➢ 流程关键活动

变更管理流程



变更管理流程始于变更的接收，结束于变更的实施和回顾。该流程包含下述主要内容：

- 提出 RFC、评估、分类

变更申请人提出 RFC，由变更主管负责检查和完善其内容，通过查询配置管理数据库，进行风险等级的初步评估；并尽量提出可能与业务发生的关联的影响，已供决策参考。变更主管并对变更进行分类；如为紧急变更，则按照紧急变更子流程执行；如

为简单变更，直接制定变更计划，并安排实施。

- 变更主管负责组织制定变更计划、测试

变更主管安排并协调相应资源制定变更计划，包括实施计划、测试计划、回退计划、配置项更新计划等。应安排对实施计划和回退计划进行测试，随后将测试结果、实施计划、回退计划、配置项更新计划等提交给变更经理审核。

- 变更经理评估、审批

变更经理接受 RFC，如果确定是紧急变更，则快速完成评估、审批。对标准变更，确定变更风险等级，审阅变更实施计划、测试报告、回退计划和配置项更新计划，批准或驳回变更申请，如需要更高级别管理层的审批，则根据不同风险级别报批。

- 变更委员会（CAB）/紧急变更委员会（ECAB）评估、审批

变更经理将根据特定的变更请求成立特定的 CAB/ECAB，成员包括对该变更的评估和批准提供应有附加价值的技术人员和管理人员，审阅工作包括变更的风险、对现有服务的影响、实施计划、回退计划和配置项更新计划等，并做出批准与否的决定。如为紧急变更，则快速完成以上评估、审批。

- 管理层审批

对于风险等级为“重大”的变更，在变更委员会审批通过后，必须再由变更经理报请至管理层审批。

- 协调变更实施

变更主管负责协调资源，准备实施前相关工作，组织人员按计划实施变更，变更主管监控实施过程和结果，并在必要时进行协调或做出决定 。在这阶段可能需要变更经理和变更委员会成员的帮助。

- 回顾和关闭

实施变更后，变更主管确保配置项及时得到更新，并协同变更经理负责从技术、管理、业务角度去回顾变更，确保 RFC 得到了预期效果，并寻找改进机会或行动计划，在回顾过程中可能会需要得到变更委员会中相关领域的技术人员的帮助，随后更新变更记录并关闭 RFC。

➢ 角色职责与考核 KPI

变更管理流程

角色	职责与权限
变更管理流程负责人	1. 全面负责流程的建设和授权，包括流程过程、考核指标和策略 2. 审阅流程报表，评估变更管理管理流程并持续改进；
变更经理	1. 评估变更管理管理流程并持续改进 2. 负责审批变更 3. 负责审批紧急变更 4. 负责变更实施后评估 5. 负责变更管理流程 6. 减少紧急变更和非标注变更，优化标准变更 7. 影响分析和资源评估 8. 对紧急变更进行授权 9. 审批变更计划 10. 确保变更管理流程正确，并被遵循 11. 提供变更管理报告 12. 管理变更请求单的互相依赖关系 13. 评估变更管理管理流程并持续改进 14. 与其他流程负责人进行协作
变更协调员	1. 检查由变更请求者提交的变更请求 RFC，提出完善建议，必要时拒绝无关或无法实施或没有必要的变更请求 2. 判断变更请求者的风险分析结果，提出评估意见 3. 作为具体变更的项目实施经理，负责领导变更的构建 / 测试，实

	施和参与回顾 4. 制定变更项目计划和时间规划等 5. 确保变更在预定的时间，资源和成本内完成 6. 在必要时，确保回退计划（Fallback Plan）得以正确实施 7. 对变更实施结果进行评审
变更审批人	1. 回顾所有已执行的变更，确保满足变更目的。 2. 参加 CAB 会议和紧急 CAB 会议。 3. 变更经理审批变更。 4. 一般根据不同变更内容有不同人员组成
变更请求者	1. 发现或获取变更需求。 2. 确定并分析变更需求和内容。 3. 填写变更请求单并提交给相关相应变更协调员。

流程考核 KPI:

- 变更成功率
- 变更影响分析准确率；
- 由变更引发事件的数量；
- 变更 Outage 通报合规率
- 变更方案正确率；
- 非授权变更数量和比率；
- 紧急变更的比率
- 变更回退失败率
- 变更引起 CI 更新正确率；

- 变更单流程执行合格率

➢ 平台重点功能及示例

平台实施重点

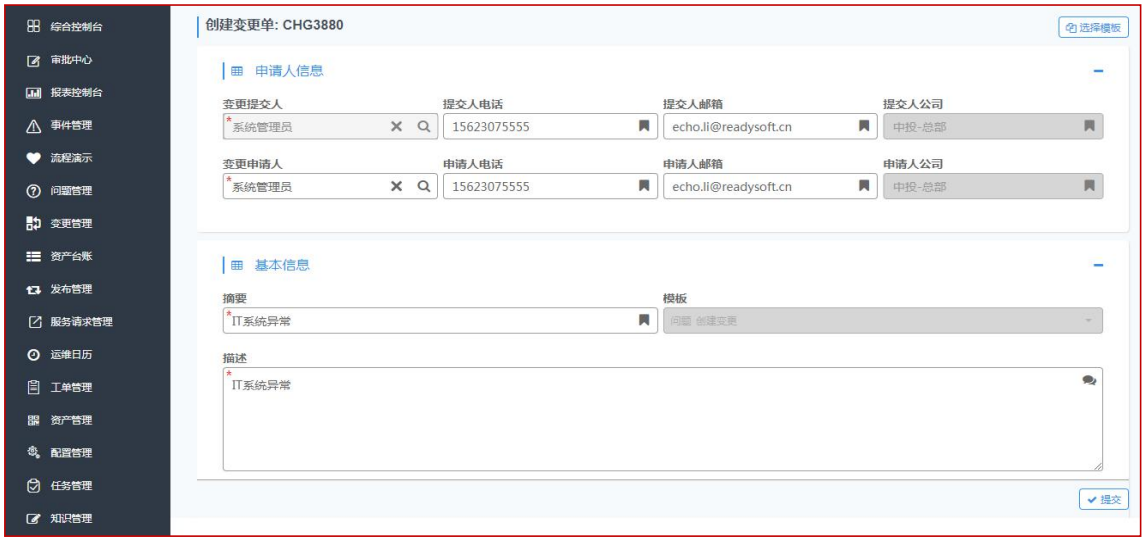
- 支持变更单可由客户自行按照模板填写提交；
- 支持灵活设定变更单的指派与审批；
- 支持退回，交接，回收，并且交接支持人员搜索功能；
- 支持实时关联工单管理，并形成相应记录，实现变更资源关联；
- 支持一次申请多个变更工单；
- 支持变更资产配置时可以方便查看资产变更的基线；
- 支持变更管理与 CMDB 的联动，具有基于配置项和计划时间进行变更冲突分析的能力；
- 支持与 UOSP 系统进行数据交互过程；
- 可以展现变更日历，进行变更冲突检查，并进行变更影响分析，提供丰富的变更风险评估功能。

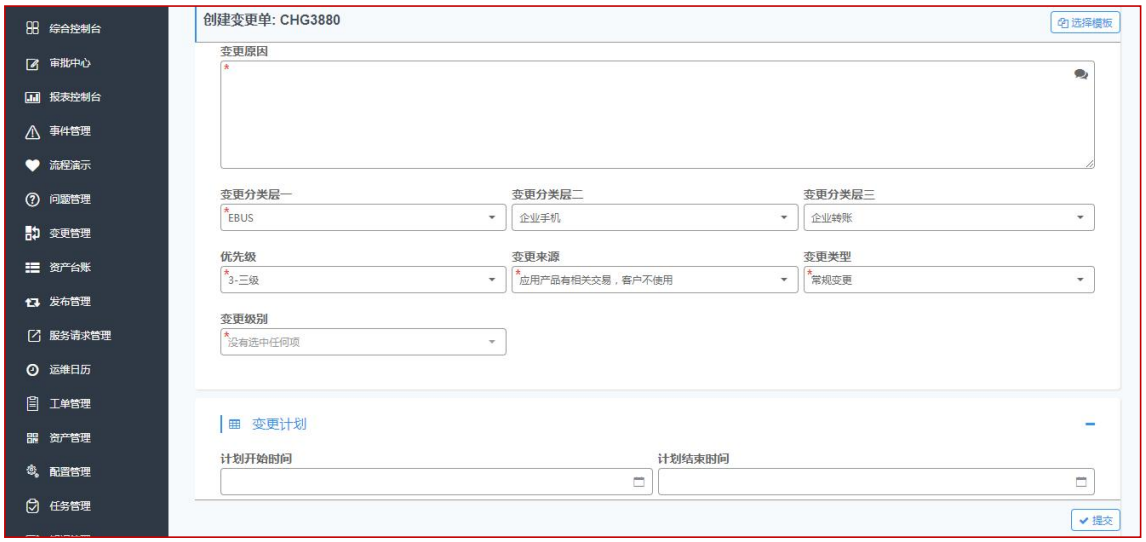
工具示例

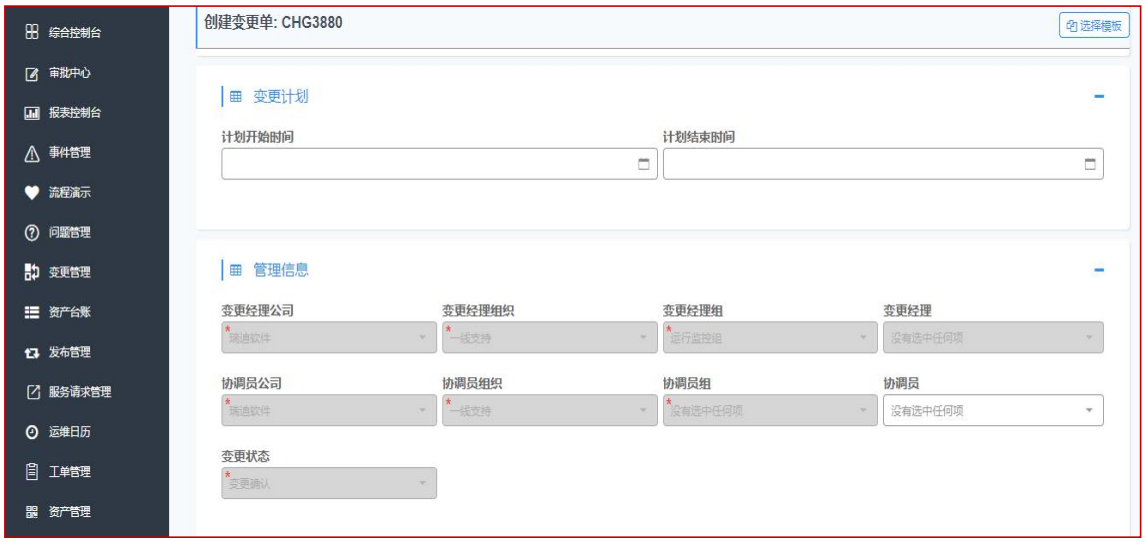
创建变更时，选择变更模板：

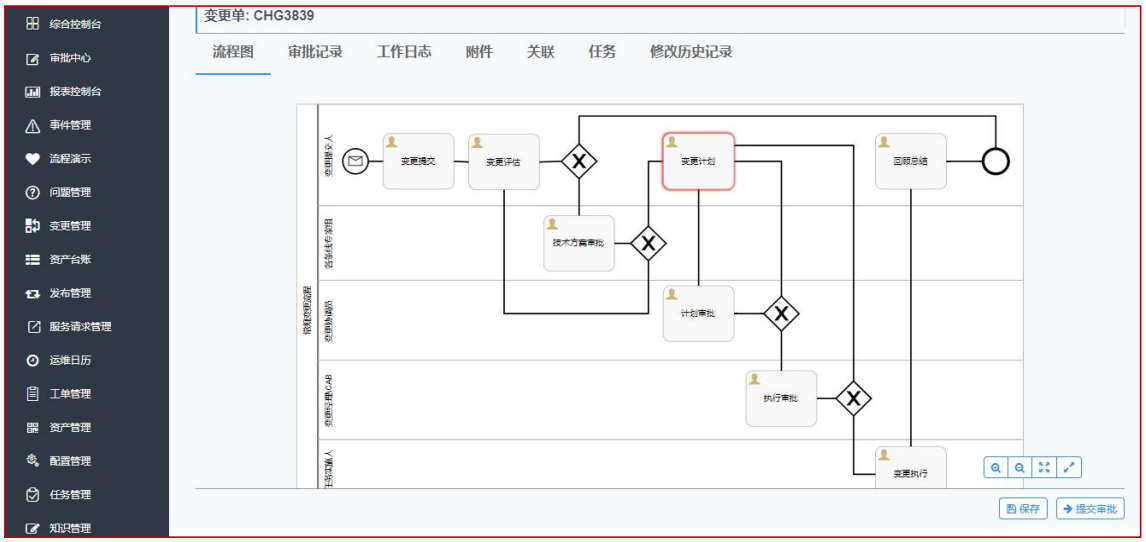
用户创建变更单时，可选择已设定好的变更模板，快速创建。变更模板上，变更分类、变更优先级、变更协调员、变更经理等信息，都可预先设定好。

变更单详情页面：


综合控制台
审批中心
报表控制台
事件管理
流程演示
问题管理
变更管理
资产台账
发布管理
服务请求管理
运维日历
工单管理
资产管理
配置管理
任务管理
知识管理
创建变更单: CHG3880
选择模板
申请人信息
变更提交人
系统管理员
提交人电话
15623075555
提交人邮箱
echo.li@readysoft.cn
提交人公司
中投-总部
变更申请人
系统管理员
申请人电话
15623075555
申请人邮箱
echo.li@readysoft.cn
申请人公司
中投-总部
基本信息
摘要
IT系统异常
模板
问题 创建变更
描述
IT系统异常
提交

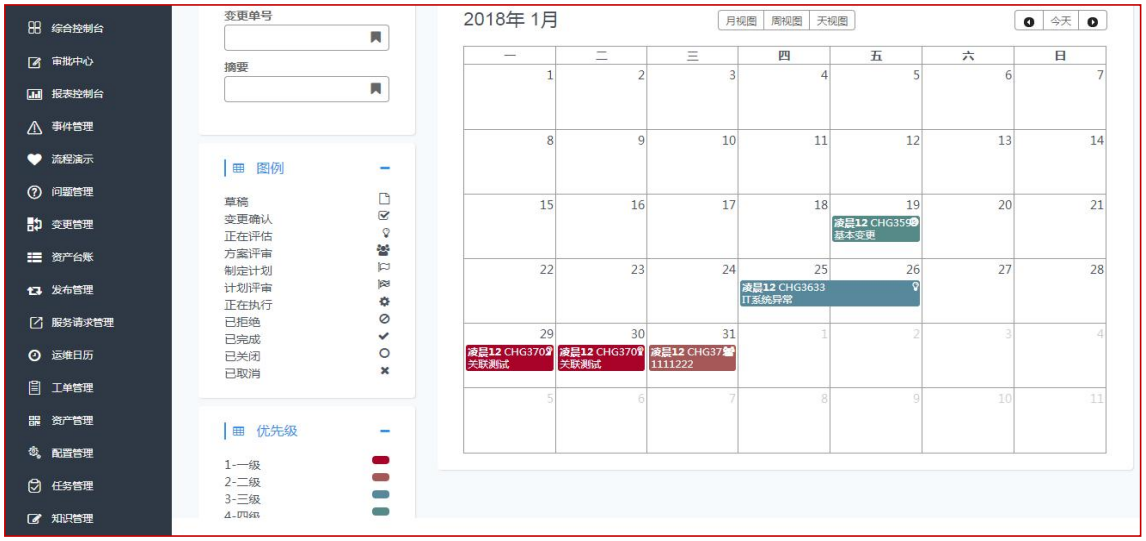

综合控制台
审批中心
报表控制台
事件管理
流程演示
问题管理
变更管理
资产台账
发布管理
服务请求管理
运维日历
工单管理
资产管理
配置管理
任务管理
创建变更单: CHG3880
选择模板
变更原因
变更分类层一
EBUS
变更分类层二
企业手机
变更分类层三
企业转账
优先级
3-三级
变更来源
应用产品有相关交易，客户不使用
变更类型
常规变更
变更级别
没有选中任何项
变更计划
计划开始时间
计划结束时间
提交


综合控制台
审批中心
报表控制台
事件管理
流程演示
问题管理
变更管理
资产台账
发布管理
服务请求管理
运维日历
工单管理
资产管理
创建变更单: CHG3880
选择模板
变更计划
计划开始时间
计划结束时间
管理信息
变更经理公司
瑞迪软件
变更经理组织
一线支持
变更经理组
运行监控组
变更经理
没有选中任何项
协调员公司
瑞迪软件
协调员组织
一线支持
协调员组
没有选中任何项
协调员
没有选中任何项
变更状态
变更确认

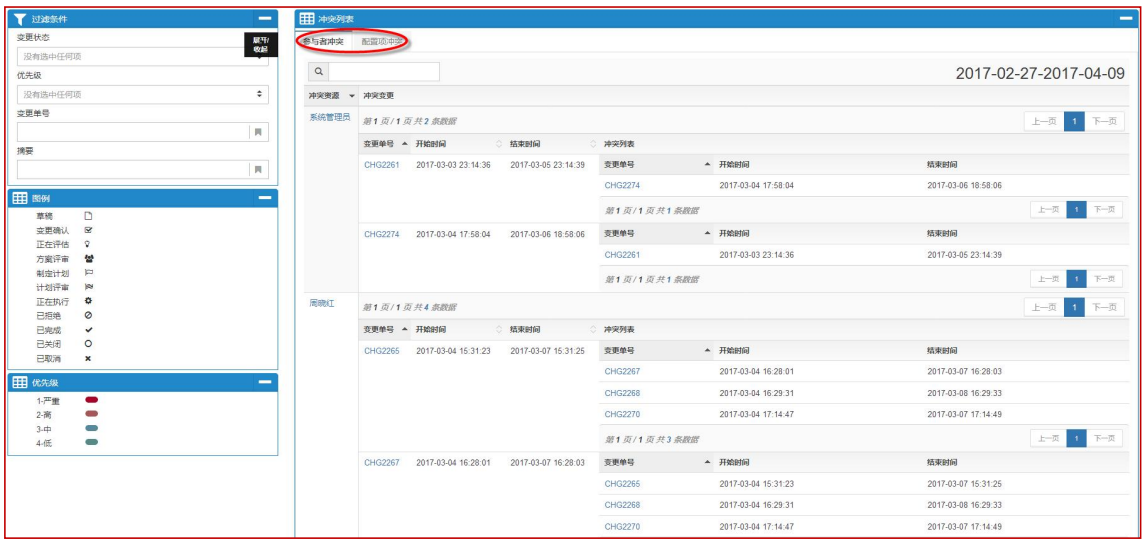


变更单日历:

以日历的形式展示每天、每周和每月计划实施的变更单。

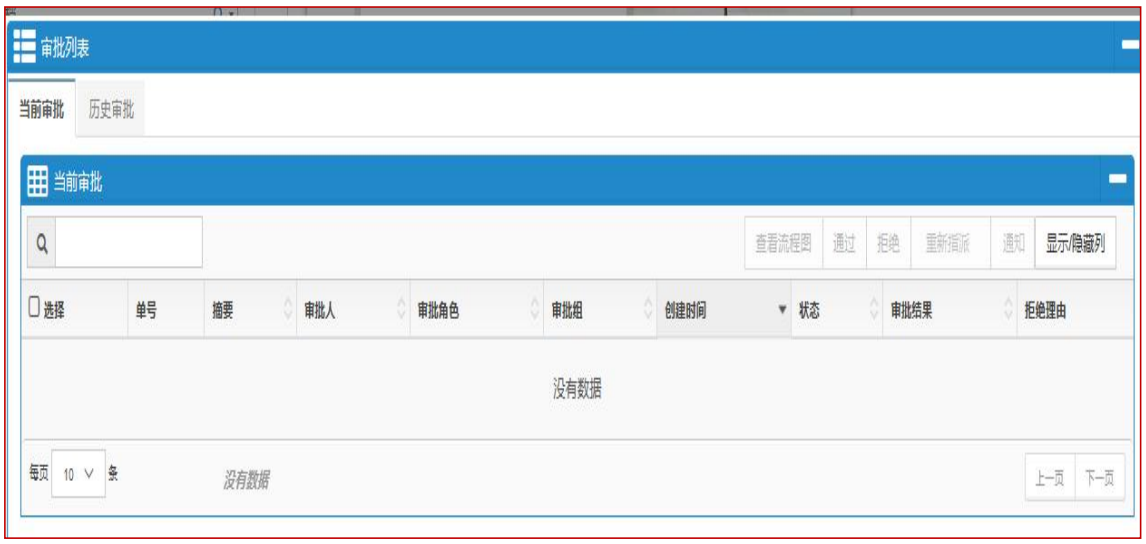


变更冲突检测：可自动检测出资源安排、变更配置项相冲突的变更单，便于变更经理及时作出规避措施。



变更审批在定义：可根据多种条件灵活定义多个审批环节及不同角色的审批人，主要功能设计如下：

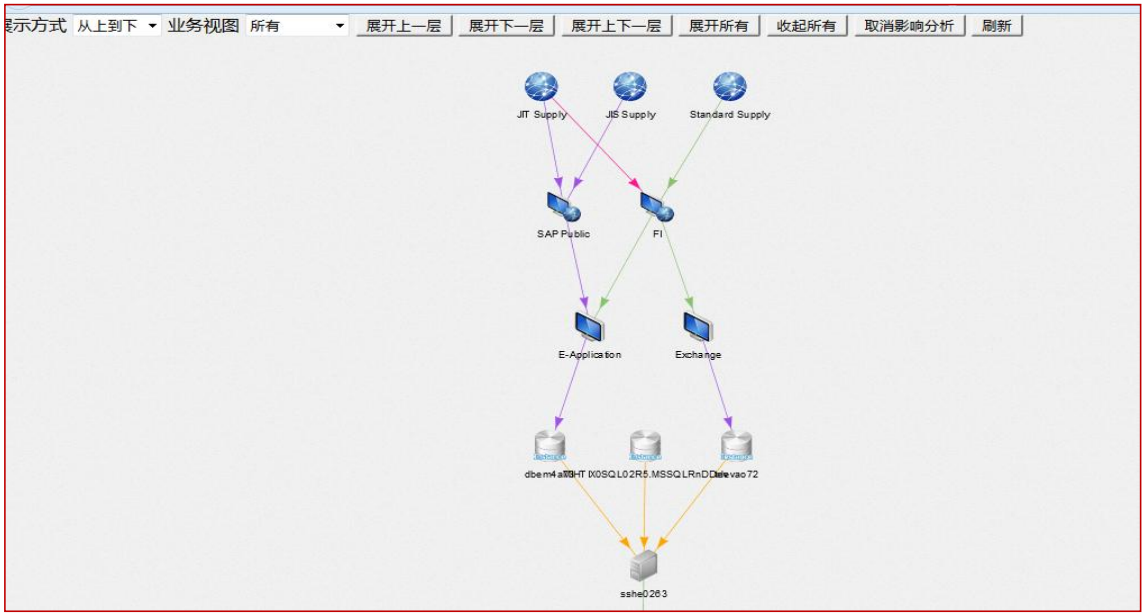
变更审批中心支持将变更审批请求重新指派或通知给其他人，详细设计如下：


审批列表
当前审批
历史审批
当前审批
查看流程图
通过
拒绝
重新指派
通知
显示/隐藏列
选择
单号
摘要
审批人
审批角色
审批组
创建时间
状态
审批结果
拒绝理由
没有数据
每页 10 条
没有数据
上一页
下一页

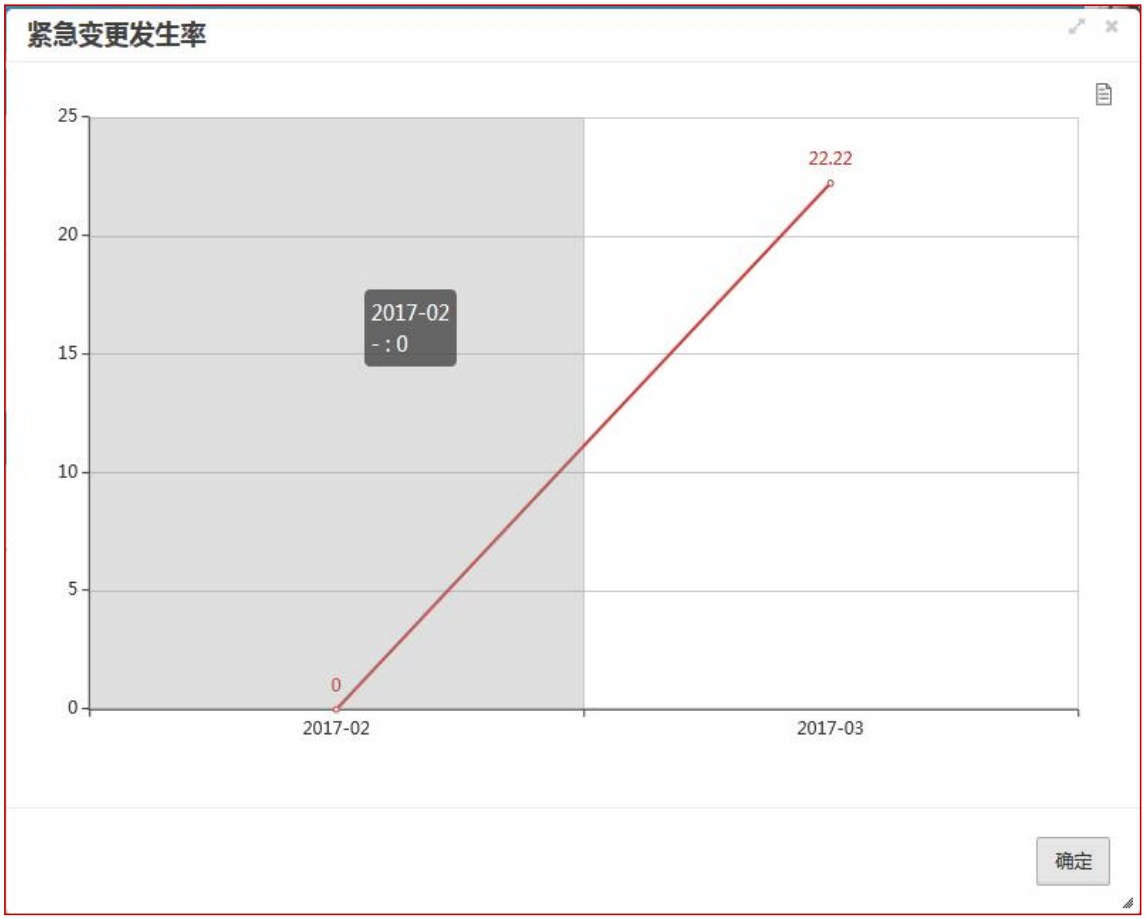
变更与配置管理的关联：


流程图
审批记录
工作日志
附件
关联
任务
修改历史记录
关联
查询
创建关联
搜索关联
事件
问题
变更
知识
配置项
资产
关联单号
被关联单号
关联类型
CHG3839
POC-13
配置项
共 1 条
1
保存
提交审批

变更影响分析：



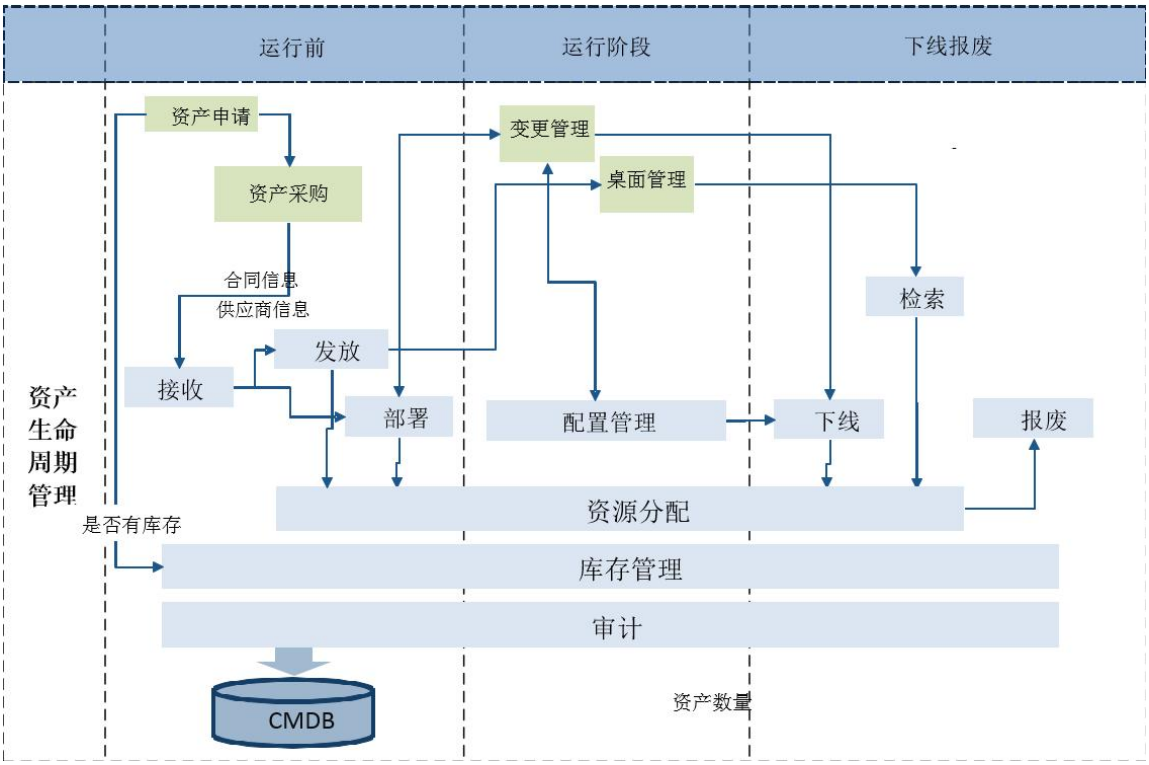
变更管理流程报表设计：



10、安全设备资产管理

➢ 流程目标与范围

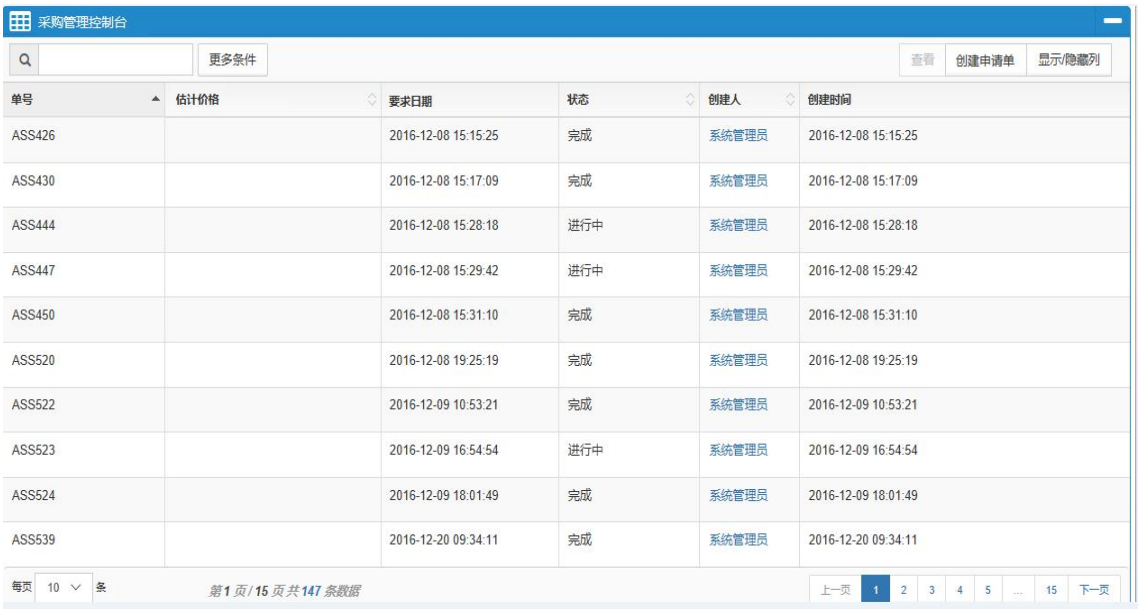
根据业务需求设计资产生命周期管理流程概要图如下：



整个生命周期分为三个阶段：运行前，运行中和资产下线报废阶段，三个阶段中涵盖了资产的采购, 接收, 入库, 发放, 上架, 归还和报废等流程，详细设计如下:

- 采购管理

根据资产库存情况和使用者的需求创建采购单，进行资产的采购，采购管理控制台设计如下：



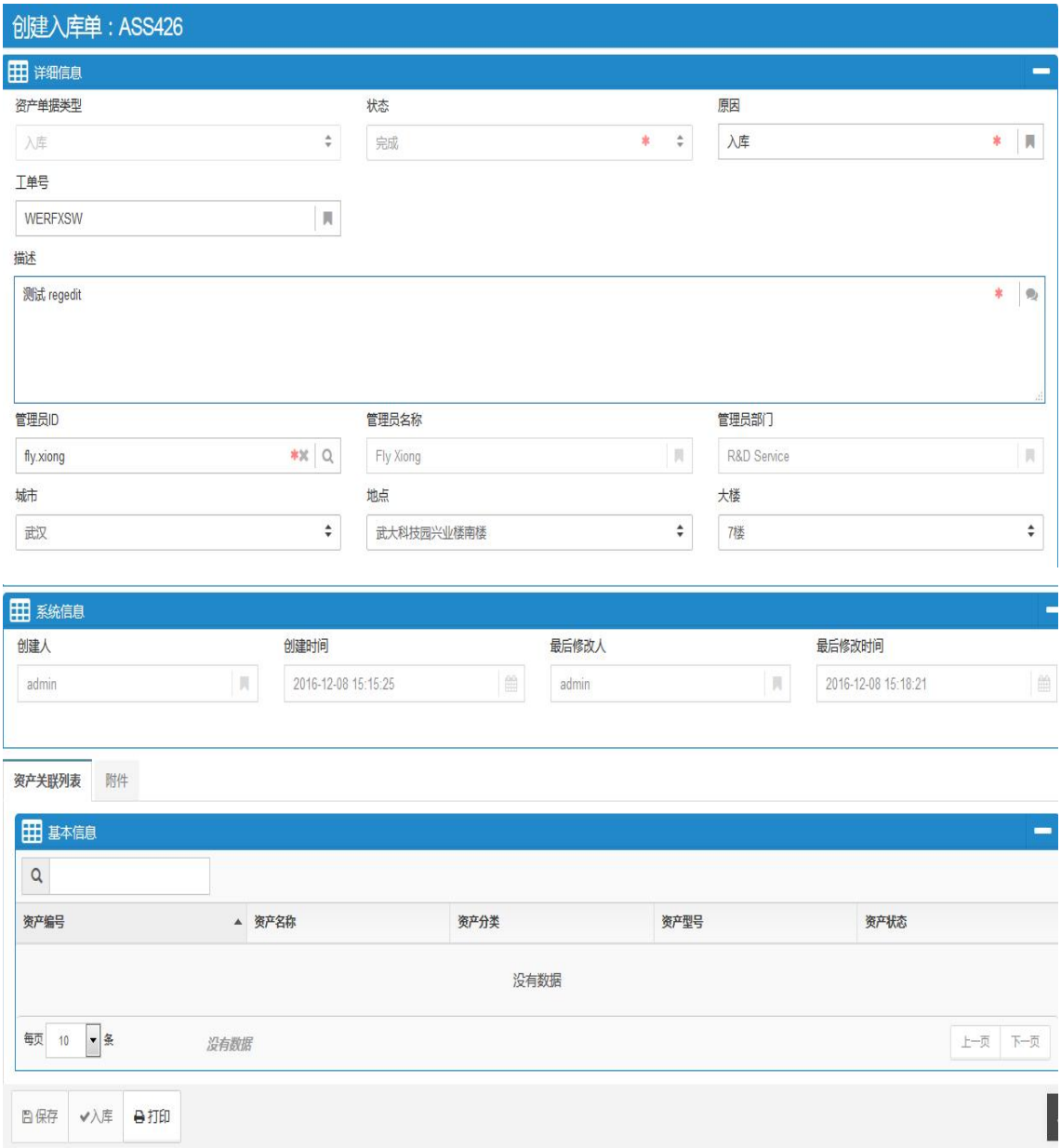
创建资产采购申请单

➢ 入库出库管理

入库管理指资产管理员在接收采购的资产后创建入库单进行资产设备的登记入库，此功能在资产流程控制台创建入库单即可，资产管理控制台设计如下：

单号	资产流程单据类型	状态	创建人	创建时间
ASS426	入库	完成	系统管理员	2016-12-08 15:15:25
ASS430	入库	完成	系统管理员	2016-12-08 15:17:09
ASS444	出库	进行中	系统管理员	2016-12-08 15:28:18
ASS447	发放	进行中	系统管理员	2016-12-08 15:29:42
ASS450	报废	完成	系统管理员	2016-12-08 15:31:10
ASS520	入库	完成	系统管理员	2016-12-08 19:25:19
ASS522	入库	完成	系统管理员	2016-12-09 10:53:21
ASS523	入库	进行中	系统管理员	2016-12-09 16:54:54
ASS524	入库	完成	系统管理员	2016-12-09 18:01:49
ASS539	入库	完成	系统管理员	2016-12-20 09:34:11

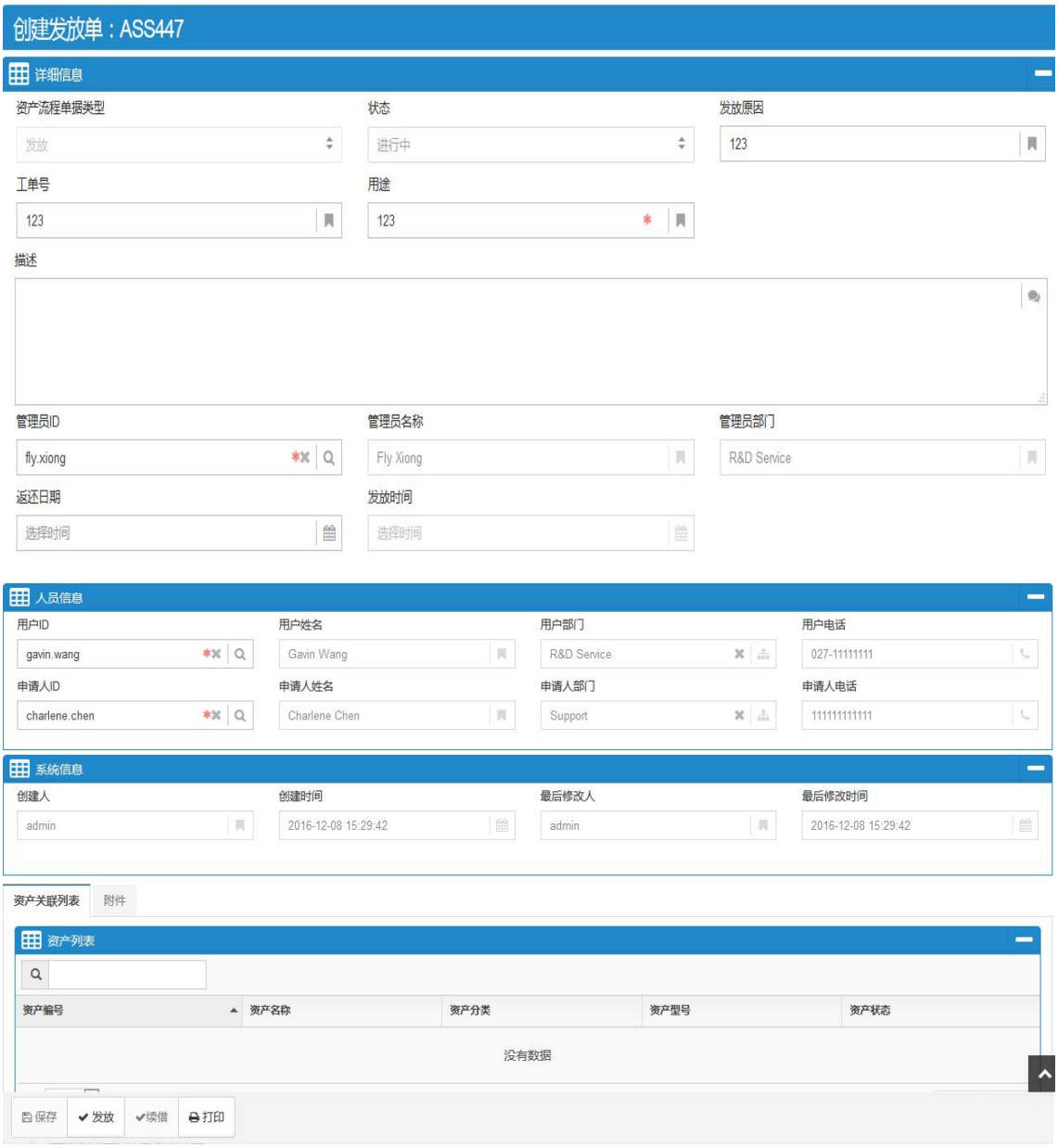
新建入库单详细信息：


创建入库单 : ASS426
详细信息
资产单据类型
入库
状态
完成
原因
入库
工单号
WERFXSW
描述
测试 regedit
管理员ID
fly.xiong
管理员名称
Fly Xiong
管理员部门
R&D Service
城市
武汉
地点
武大科技园兴业楼南楼
大楼
7楼
系统信息
创建人
admin
创建时间
2016-12-08 15:15:25
最后修改人
admin
最后修改时间
2016-12-08 15:18:21
资产关联列表
附件
基本信息
资产编号
资产名称
资产分类
资产型号
资产状态
没有数据
每页
10
条
没有数据
上一页
下一页
保存
入库
打印

新建出库单详细信息：

➢ 发放上架管理

资产在被领用后提交使用者提交变更上架流程进行资产上架，上架后更新资产信息，发放单据详细信息设计如下图：

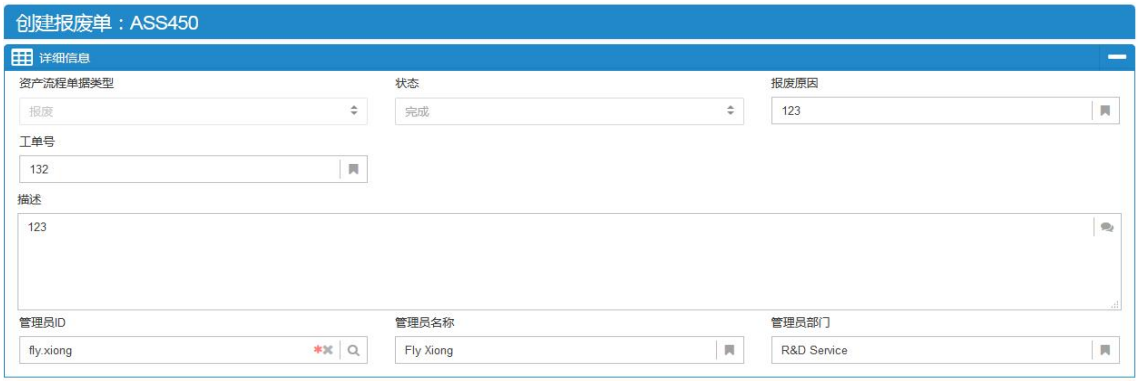


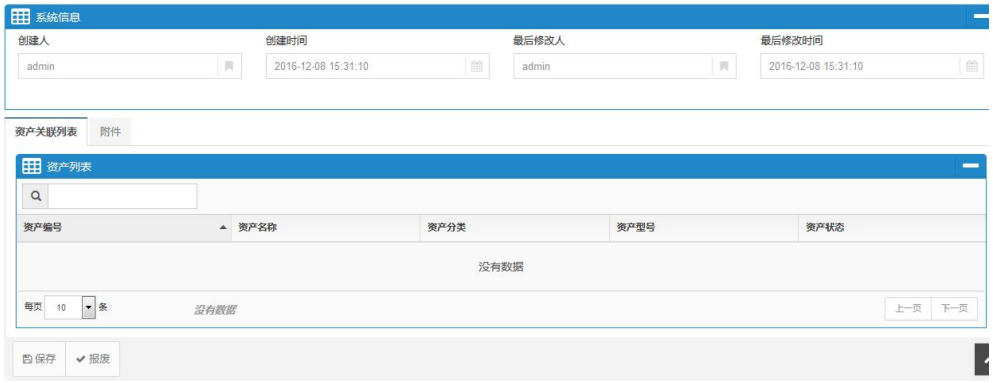
➢ 归还管理

资产使用者在借用完资产后资产管理员会在系统中创建资产归还单据进行资产归还登记处理，归还单据详细信息设计如下：

➢ 报废管理

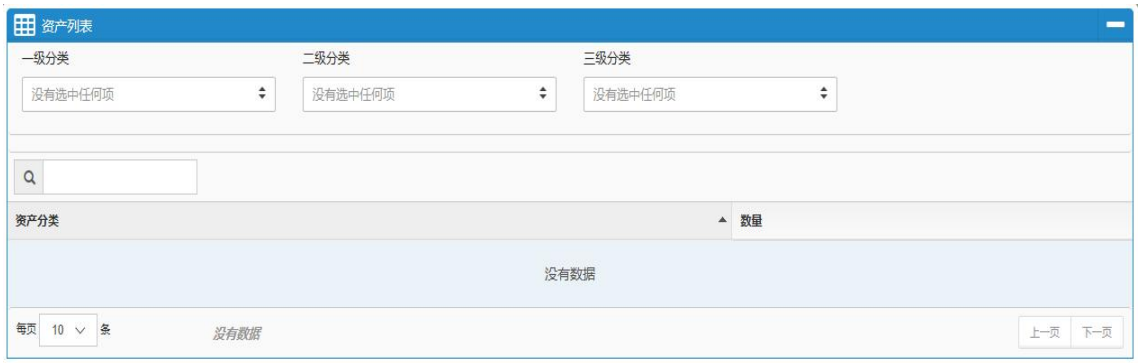
资产在经过定期盘点后有部分确认无用的资产资产管理员在系统中创建报废单，报废单详细信息设计如下：





➢ 盘点管理

资产管理员通过盘点功能查询现有资产情况与使用情况进行对比后调整资产分配，盘点查询功能设计如下：



11、安全设备配置管理

➢ 流程目标与范围

配置管理实现的目标为：

- 设计配置管理数据库（CMDB），建立相关系统的 CMDB 资源模型，支持模型的方便

扩展；

- 对现有各流程提供有效的支持。结合现有各流程的调整改造，实现“在流程中维护资源信息、在流程中使用资源信息”；
- 提供有效的资源统计报表和机房拓扑图、网络拓扑图、存储拓扑图、设备业务关联拓扑、应用服务关联拓扑等界面呈现；
- 定期产生配置信息报表，报表包括各个配置项生命周期的现存和历史数据，使得配置项的变更历史能够被追踪；
- 通过 CMDB 向管理层提供准确全面地维护信息，为其做出正确决策提供数据支撑。

➢ 配置管理核心概念

➢ **配置项 (Configuration Items)**为提供 IT 服务而需要进行管理的任何组件。每个配置项的有关信息记入配置管理系统内的配置记录，并由配置管理在信息的整个生命周期内维护。配置项受变更管理的控制。配置项通常包括 IT 服务、软硬件、建筑、人员和正式文档，例如流程文档和服务级别协议。

➢ **配置管理系统 (Configuration Management System)**一套工具和数据库，用于管理 IT 服务提供商的配置数据。CMS 还包括关于事件、问题、已知错误、变更和发布的信息；并且可以包含关于雇员、供应商、地点、业务部门、客户和用户的信息。CMS 包括收集、保存、管理、更新和显示所有配置项及其关系相关数据的工具。CMS 由配置管理维护，为所有 IT 服务管理流程所用。

➢ **配置基准 (Configuration Baseline)** 已经正式约定并由变更管理流程进行管理的配置的基准。配置基准用作未来构建、发布和变更的基础。

➢ **配置模型 (Configuration Model)** 配置管理通过记录配置项之间的关系，交付服务、资产和基础设施的模型。

➢ 配置管理数据库

- 融讯光通 CMDB 具有基于 ITIL 理念的 CMDB，并能够与网络安全设备运维管理流程无缝集成。
- 融讯光通配置管理数据库（CMDB）：是一个数据集合，存储所有配置管理的数据和信息。配置管理数据库是配置管理流程的核心，也为事件管理、问题管理、变更管理提供了查询、诊断、记录的基础。

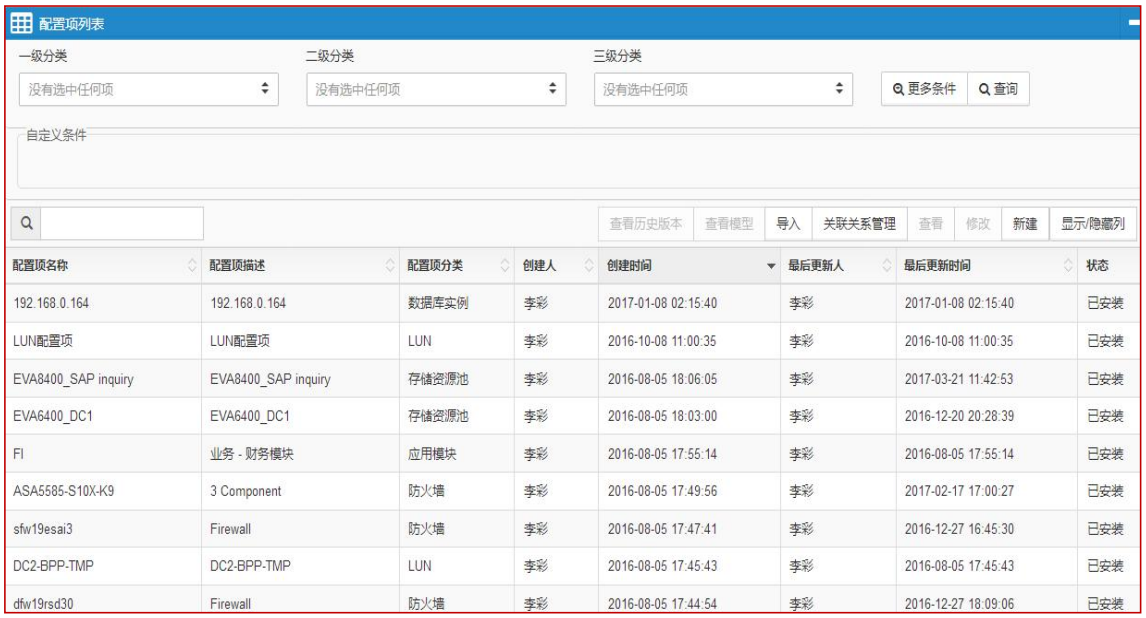
- 配置项（CI）：生产环境中需要被管理的软件、硬件、文档、人员等。
- 配置管理数据库：包含了配置项的信息以及各元素之间的关系。
- 服务管理系统应能建立、维护配置管理数据库。

➢ 识别配置项

配置项详情界面

- 支持配置项的层次化结构

配置项结构的细分程度取决于组织中配置项的使用情况。例如：将服务器整体看作一个配置项，则可将 CPU 看作服务器的一个配置属性；进一步细分，可将 CPU 看作是一个配置项。



配置项名称	配置项描述	配置项分类	创建人	创建时间	最后更新人	最后更新时间	状态
192.168.0.164	192.168.0.164	数据库实例	李彩	2017-01-08 02:15:40	李彩	2017-01-08 02:15:40	已安装
LUN配置项	LUN配置项	LUN	李彩	2016-10-08 11:00:35	李彩	2016-10-08 11:00:35	已安装
EVA8400_SAP inquiry	EVA8400_SAP inquiry	存储资源池	李彩	2016-08-05 18:06:05	李彩	2017-03-21 11:42:53	已安装
EVA6400_DC1	EVA6400_DC1	存储资源池	李彩	2016-08-05 18:03:00	李彩	2016-12-20 20:28:39	已安装
FI	业务 - 财务模块	应用模块	李彩	2016-08-05 17:55:14	李彩	2016-08-05 17:55:14	已安装
ASA5585-S10X-K9	3 Component	防火墙	李彩	2016-08-05 17:49:56	李彩	2017-02-17 17:00:27	已安装
sfw19esai3	Firewall	防火墙	李彩	2016-08-05 17:47:41	李彩	2016-12-27 16:45:30	已安装
DC2-BPP-TMP	DC2-BPP-TMP	LUN	李彩	2016-08-05 17:45:43	李彩	2016-08-05 17:45:43	已安装
dfw19rsd30	Firewall	防火墙	李彩	2016-08-05 17:44:54	李彩	2016-12-27 18:09:06	已安装

CMDB 主控制界面

- 配置项属性

配置项属性表示配置项 CI 的一项信息，如序列号、版本等。

配置项要求具有唯一标识（有唯一性检查）的对象编码，编码规则满足甲方管理要求。

- 支持附件功能

为了使 CI 的信息更加全面，可以采用附件的方式记录 CI 的相关额外信息：手册、维护合同、配置文件、图片等。

- 配置项字段

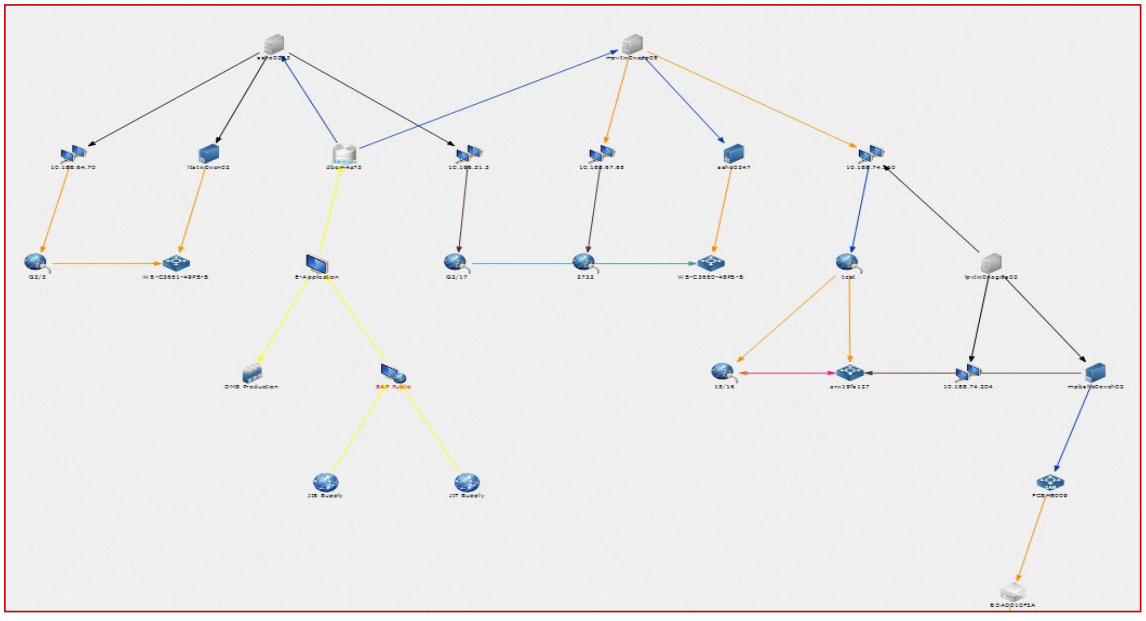
不同配置项之间的字段是不尽相同的，所以服务管理实现工具需要能够灵活地增加新的字段，以满足对各种配置项信息的记录。

- 配置项状态代码

配置项状态代码反映了配置项在其生命周期中的不同状态。

- 配置项关系

配置管理模块能够提供反映配置项之间关系的功能。



- 配置信息的收集

融讯光通 CMDB 支持以下三种信息收集方式：

- 使用模板来手工创建配置项，创建一个或多个配置项。

- 通过 Excel 批量导入配置项；
- 与外部自动发现工具集成，完成 CI 自动发现

➢ 配置控制

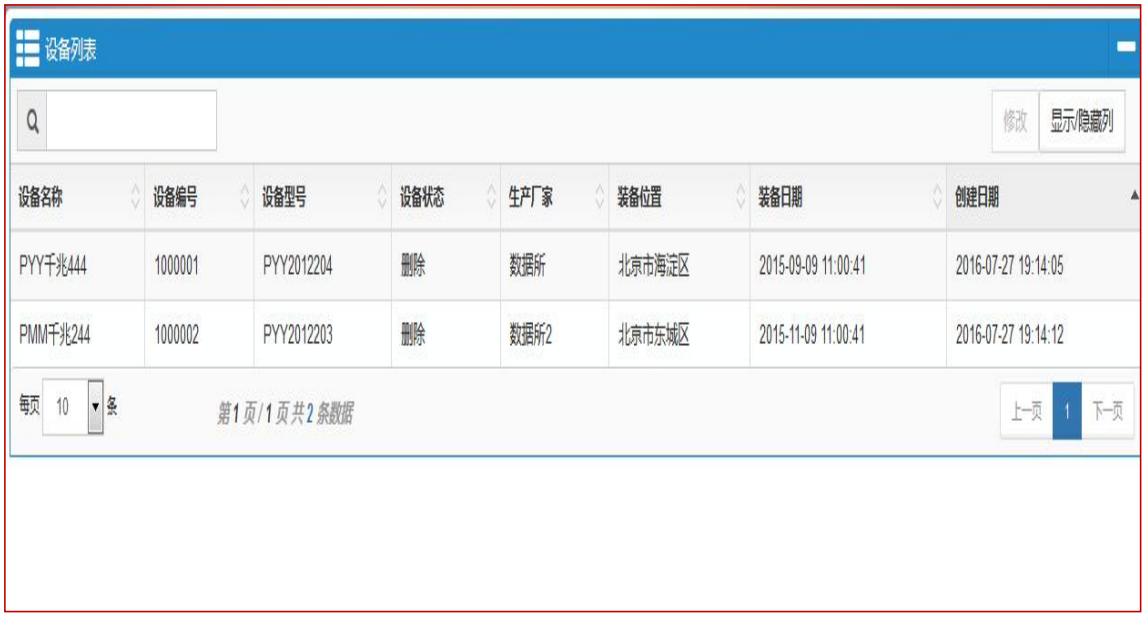
- 能够在 CI 的整个生命周期内跟踪 CI 的状态，确保只有被认可的和被标识的配置项及其配置信息才能输入 CMDB 或更新 CMDB。
- CI 记录中特定字段的变化，应被记录在 CI 的历史记录中，对一个 CI 中一系列的配置变化过程在数据库中应有日志记录，并可被浏览和审核。
- 在配置模型逻辑图中可直接选中某个配置项查看其相关的事件、问题；配置项目清单可按用户需求将配置项的编码、名称、版本、属性信息导出。

➢ 汇报和状态汇总

- 根据需要，定期产生配置管理报表，并能使相关人员进行选择、抓取、分类和返回所查询的 CMDB 数据。定期产生配置项的状态报告，并能反映配置项的版本和变动历史。

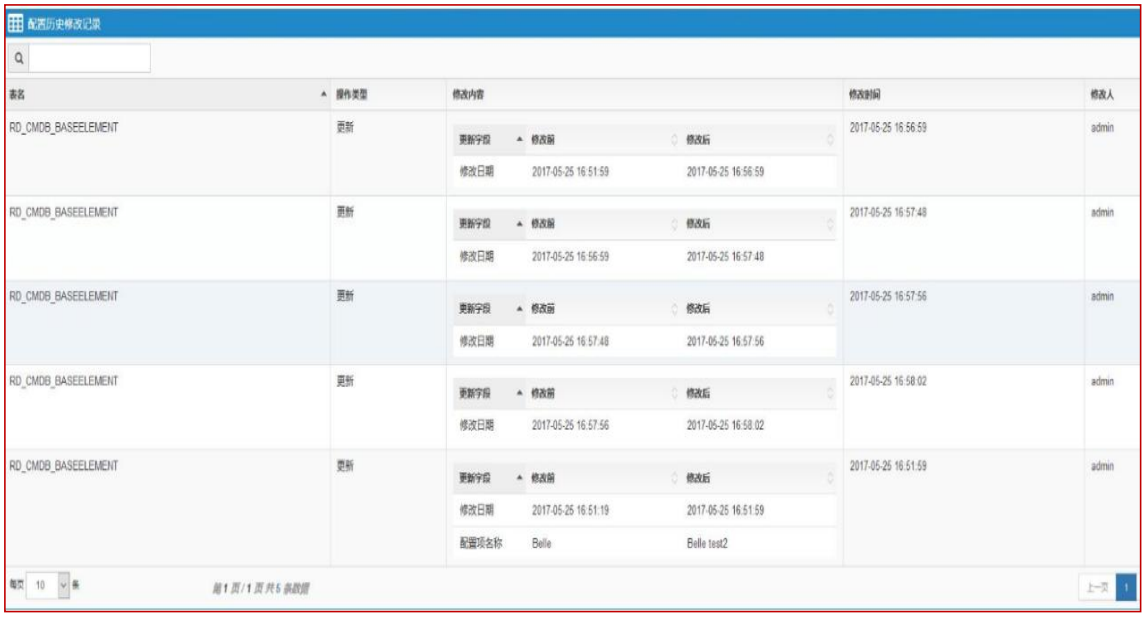
- 提供与服务管理平台其它管理模块的信息关联，如：某个 CI 所发生的历史事件记录。

备件 CI 管理：



配置关联关系管理：

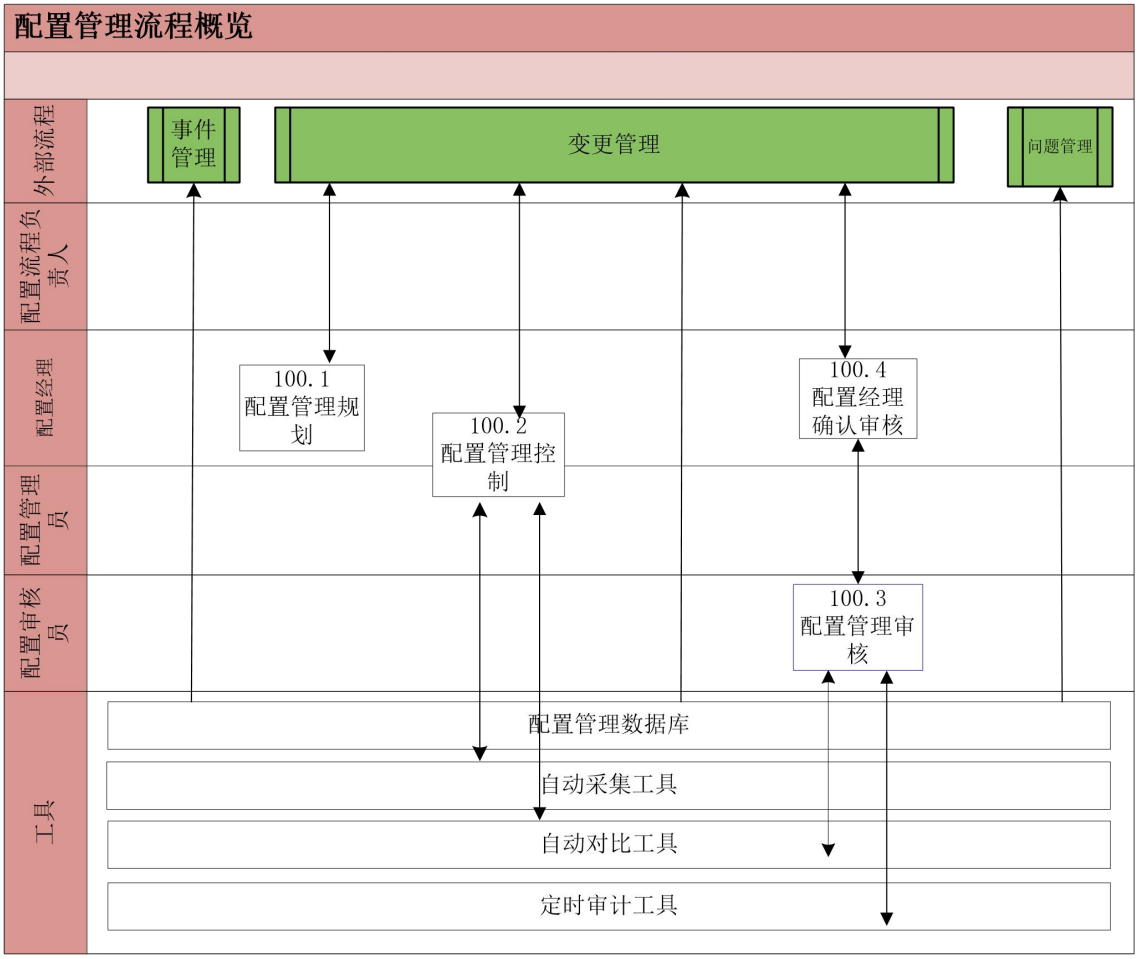
配置项历史审计记录：


配置历史修改记录
表名
操作类型
修改内容
修改时间
修改人
RD_CMDB_BASEELEMENT
更新
更新字段
修改前
修改后
修改日期
2017-05-25 16:51:59
2017-05-25 16:56:59
2017-05-25 16:56:59
2017-05-25 16:57:48
2017-05-25 16:57:48
2017-05-25 16:57:56
2017-05-25 16:57:56
2017-05-25 16:58:02
2017-05-25 16:51:19
2017-05-25 16:51:59
配置项名称
Belle
Belle test2
每页 10 条
第 1 页 / 1 页 共 5 条数据
上一页
1

配置项自定义属性维护：

➢ 配置管理流程和角色

配置管理总体流程如下：



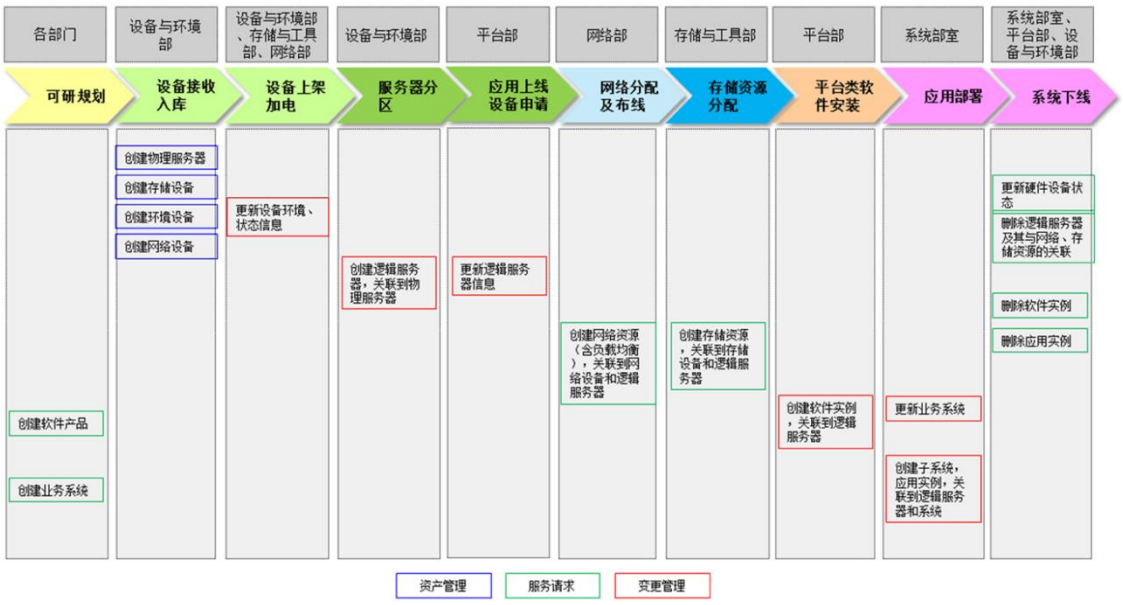
配置管理角色要求：

流程名称	角色	职责
配置管理-CI 管理	**配置管理流程经理**	➢ 制定和管理配置管理流程、人员岗位角色。 ➢ 设立配置项管理指标，持续改进配置管理流程。 ➢ 规划配置项管理范围和规则。
	配置经理	➢ 参与和审核配置项信息的准确性。 ➢ 协调配置项管理资源。

	配置管理员	➢ 负责维护和核对配置项信息。 ➢ 负责维护和核对配置项之间的关系。
	配置审计员	➢ 制定、跟踪配置审计计划； ➢ 完成配置审计报告。

➢ 配置管理和其他流程关系

配置管理生命周期示意图：



配置管理实践关系图

- 与事件管理流程的关系

事件记录与 CMDB 中的配置项相关联，此外配置管理流程为事件分析员在诊断原因提供应急预案，同时在解决的时候，如果涉及到配置项，还要通过变更流程对配置项进行相应的修改。

- 与问题管理流程的关系

问题记录与 CMDB 中的配置项相关联，配置管理同时为问题管理的根本原因分析提供参考信息；同时如果在解决的时候涉及到配置项，还要通过变更流程对配置项进行相应的修改。

- 与发布管理流程的关系

发布管理与配置管理是紧密结合的，此外配置管理为发布管理提供信息帮助发布审核员的评估分析。

- 与变更管理流程的关系

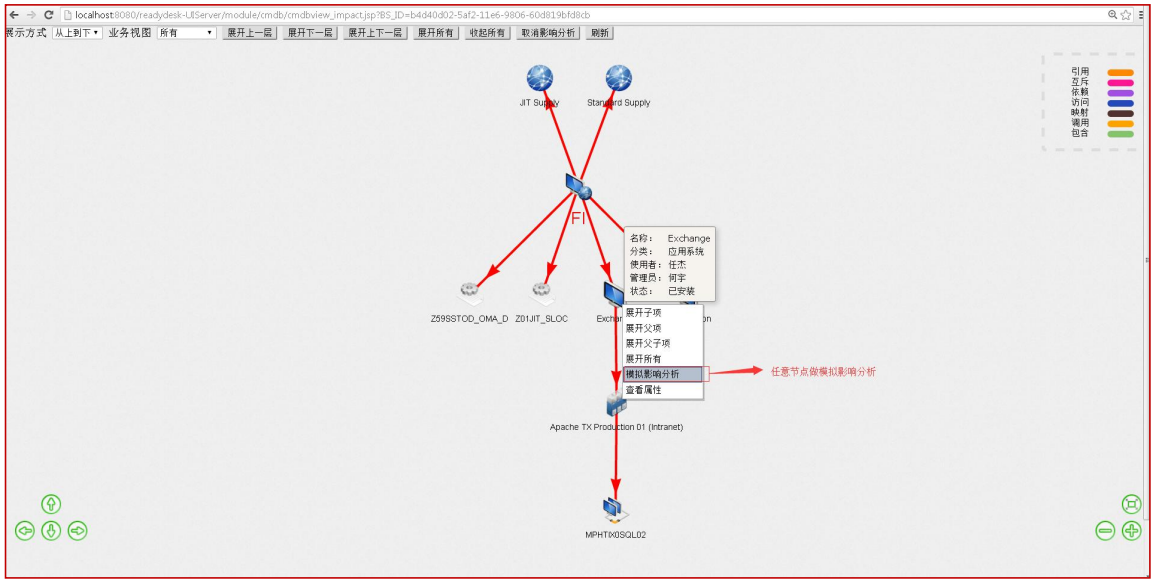
变更管理与配置管理相关联，同时在评估审批过程中，可以对配置项进行查询，配置项的改变以变更管理为入口。

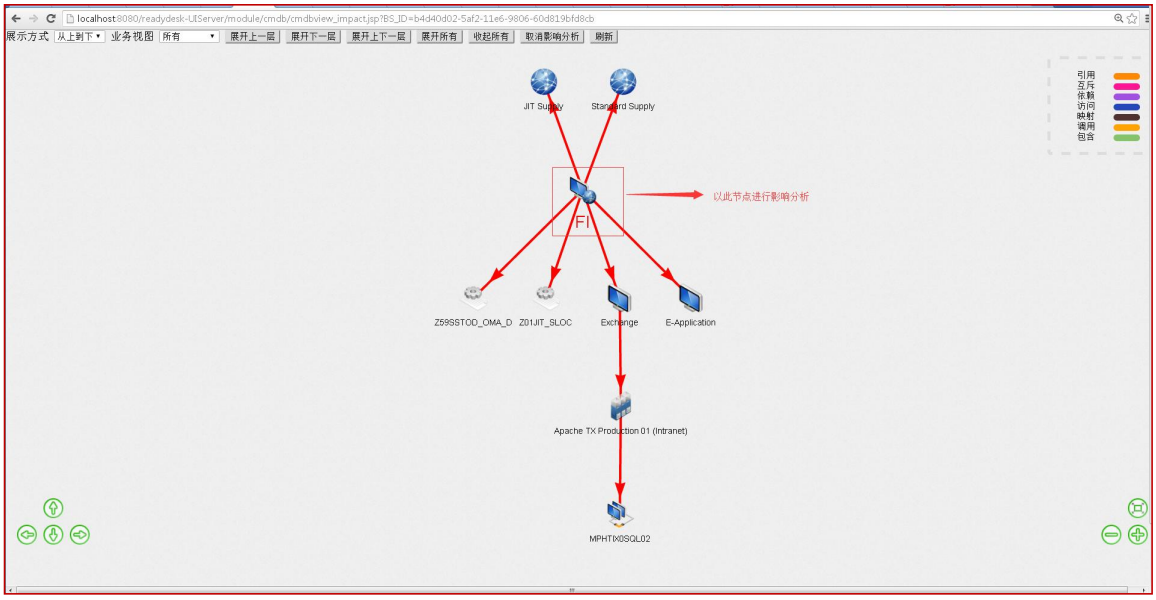
- 与服务请求流程的关系

服务请求流程与配置管理紧密结合，配置管理为服务请求提供配置项的查询

➢ 影响分析

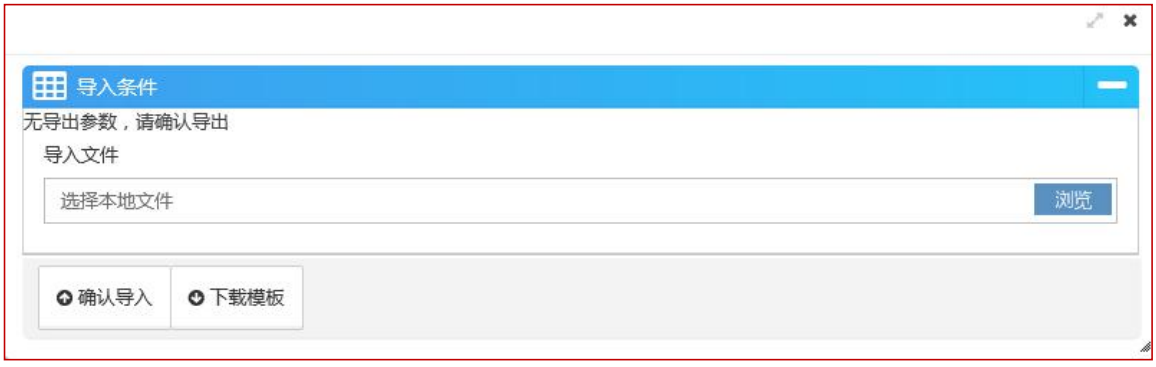
具备变更影响分析和影响模拟功能，可以对变更的配置项进行影响模拟，模拟该配置项不可用时，所影响到所有相关配置项。通过影响模拟功能可以提高变更影响分析的完整性和准确性，降低变更风险。



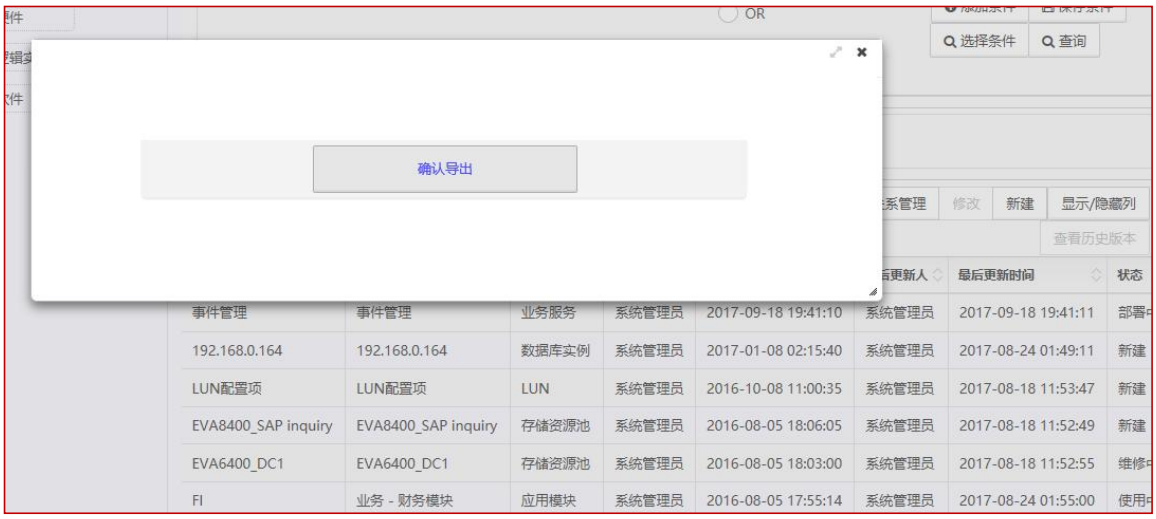


➢ 导入导出

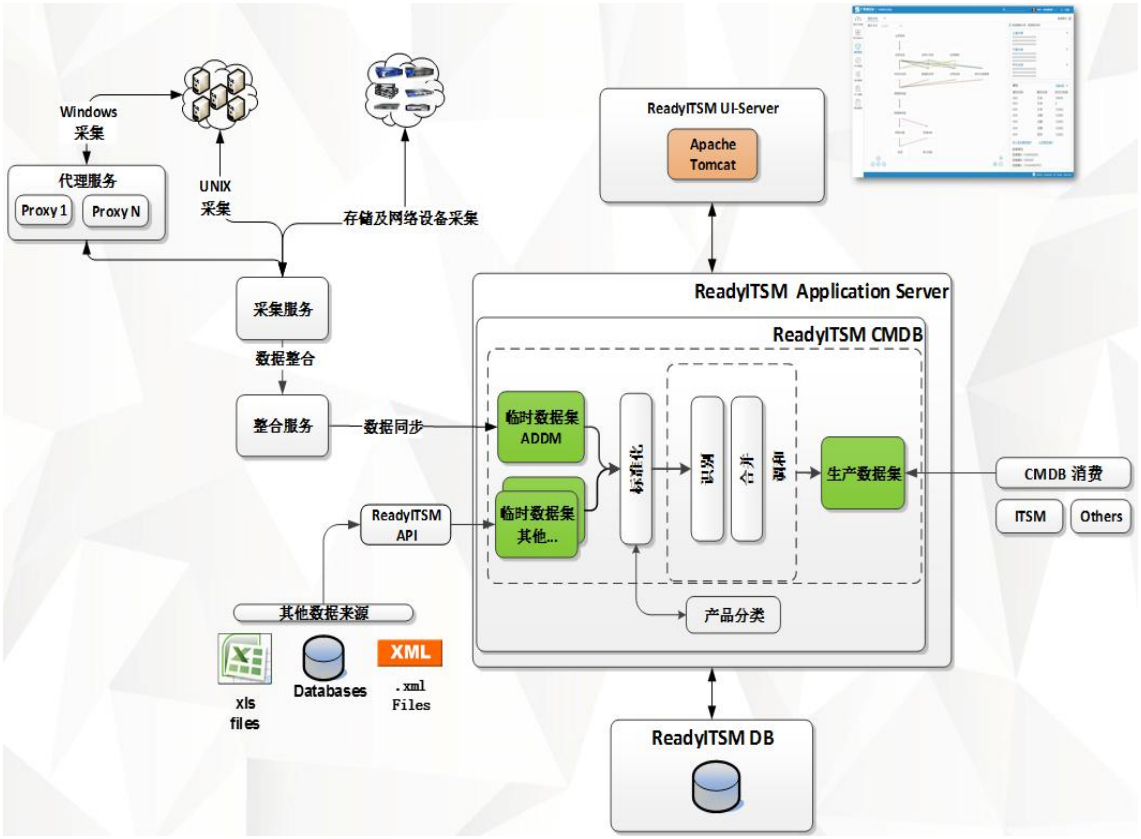
配置项管理控制台提供配置项数据的导入导出功能，方便数据的迁移。



导出：



➢ 与自动扫描工具集成方案



上图为与某厂商自动发现工具集成方案

➢ 与其它数据源的同步

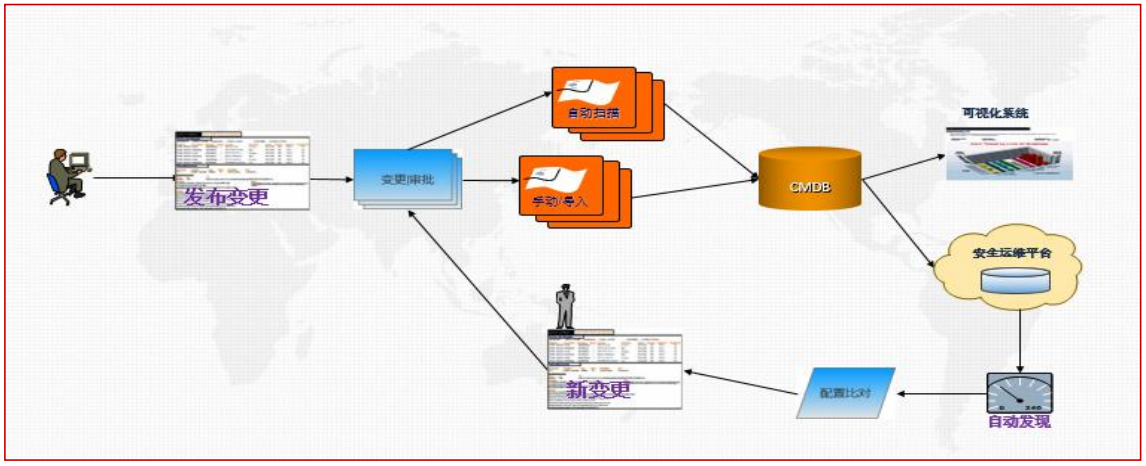
变更的来源：发布和常规运维

数据来源：自动扫描和手动/导入

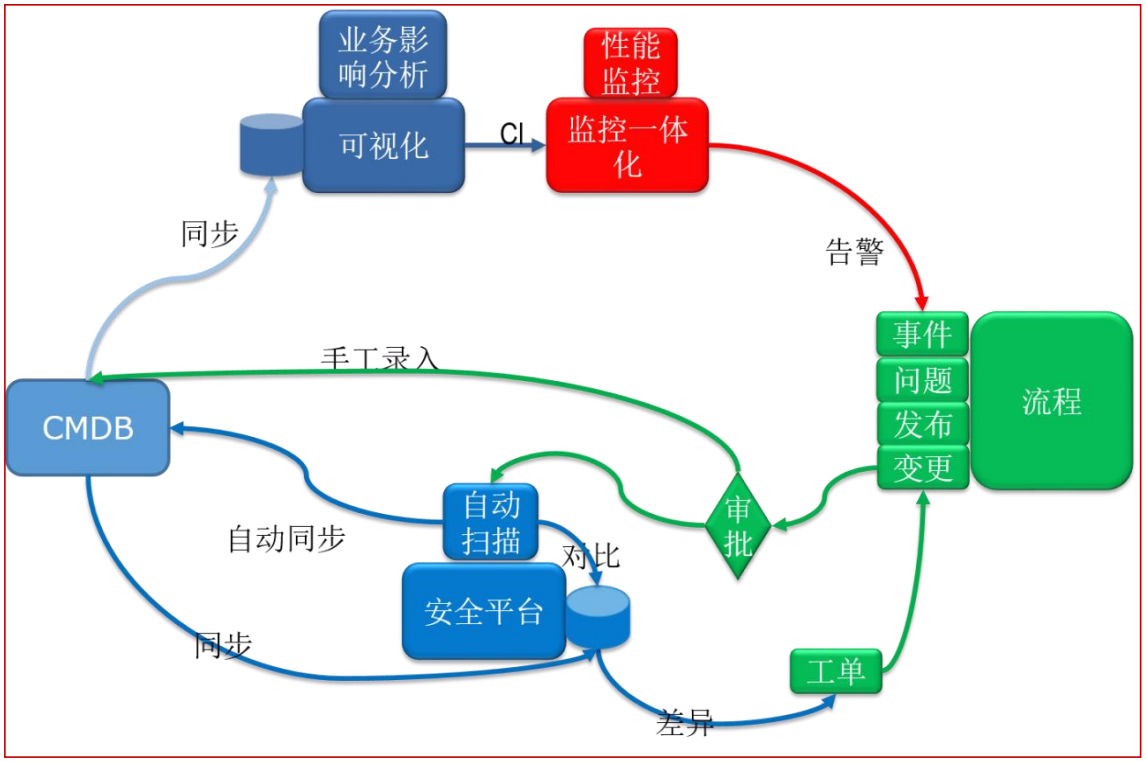
场景 1：新的应用发布>>提交 CMDB 变更请求>>审批通过>>一部分属性数据手动维护，一部分扫描调和同步>>在变更单关联 CI>>检查 CMDB 库>>CMDB 推送消费平台

场景 2:常规运维过程中发现 CMDB 数据异常>>提交变更>>在变更单关联 CI>>审批通过>>

一部分属性数据手动维护，一部分扫描调和同步>>检查 CMDB 库>>CMDB 推送消费平台



CMDB 与其它数据源的关系图：



提供 api 接口，与其他 CMDB 数据源同步数据

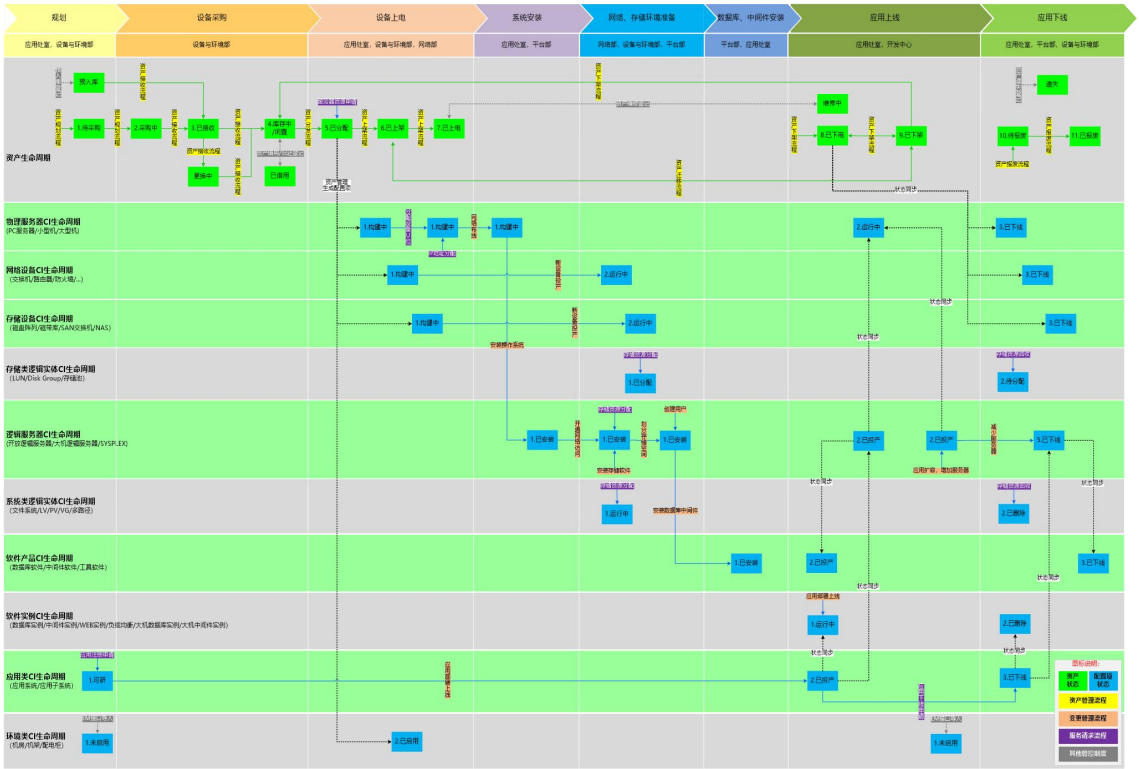
系统 rest 后台服务：

Class 类/包路径：RXGTdesk-restServer/src/com/RXGT/rest/service/api		
CmdbRestService　系统 CMDB 相关接口		
	/cmdb/data	CMDB 数据查询
	/cmdbRelation/{cmdbId}/dataByType	CMDB 根据关联关

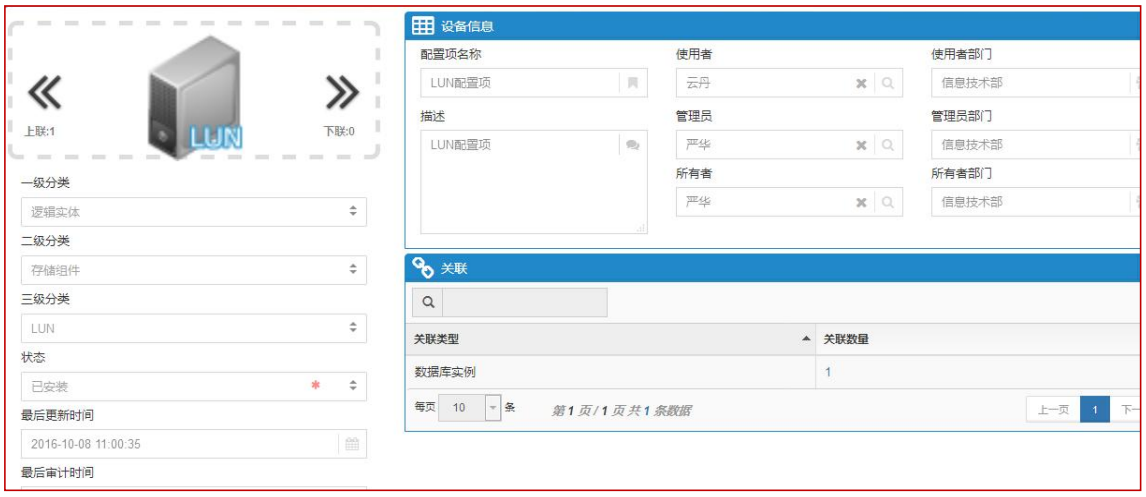
Rest 接口名		系根据数据类
	/cmdbRelation/dataWithClass	根据分类查询
	/cmdbRelation/data	CMDB 关联关系查询
	/cmdbRelation/add	CMDB 关联关系添加
	/assets/data	资产数据
CmdbviewRestService.java CMDB 模型展示接口		
Rest 接口名	/queryCmdbview/data	展示数据查询
	/queryColorview/data	展示图形颜色

➢ 实施方案

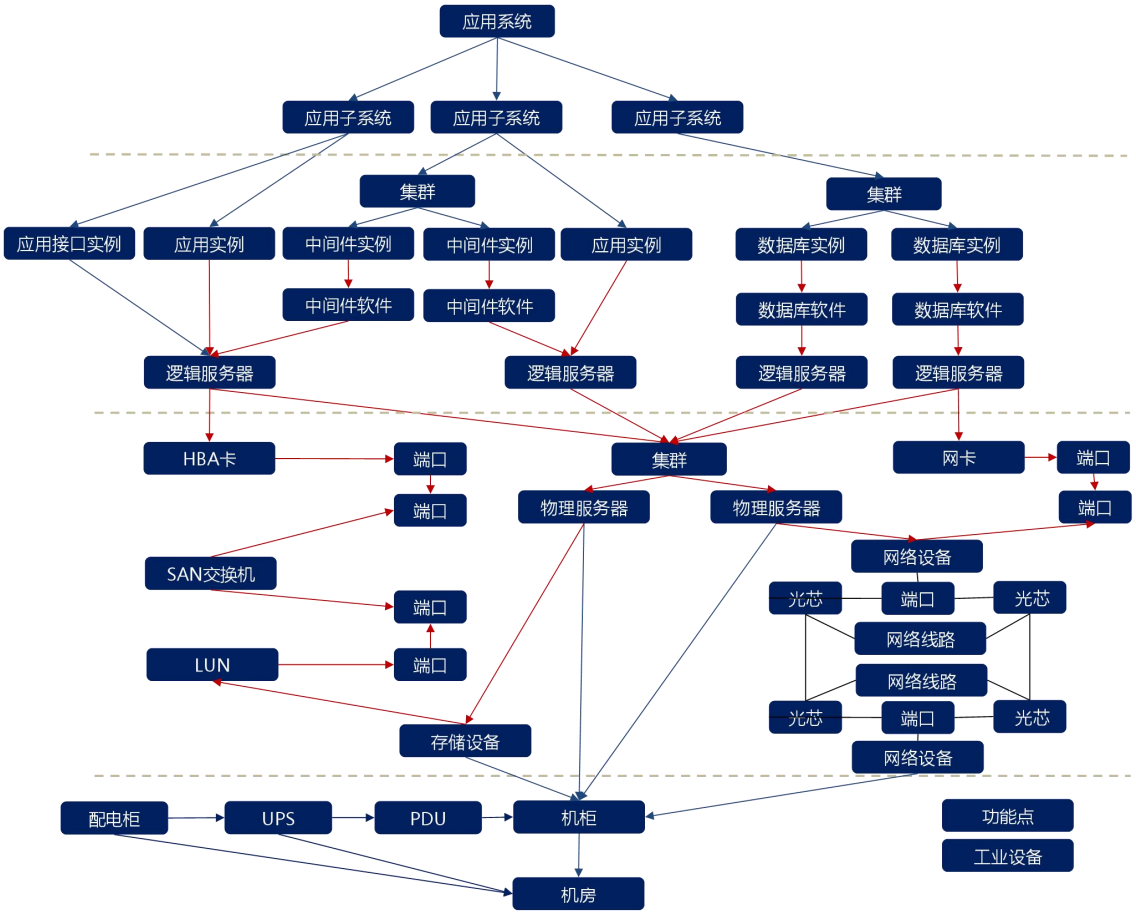
1. CMDB 全生命周期流程图



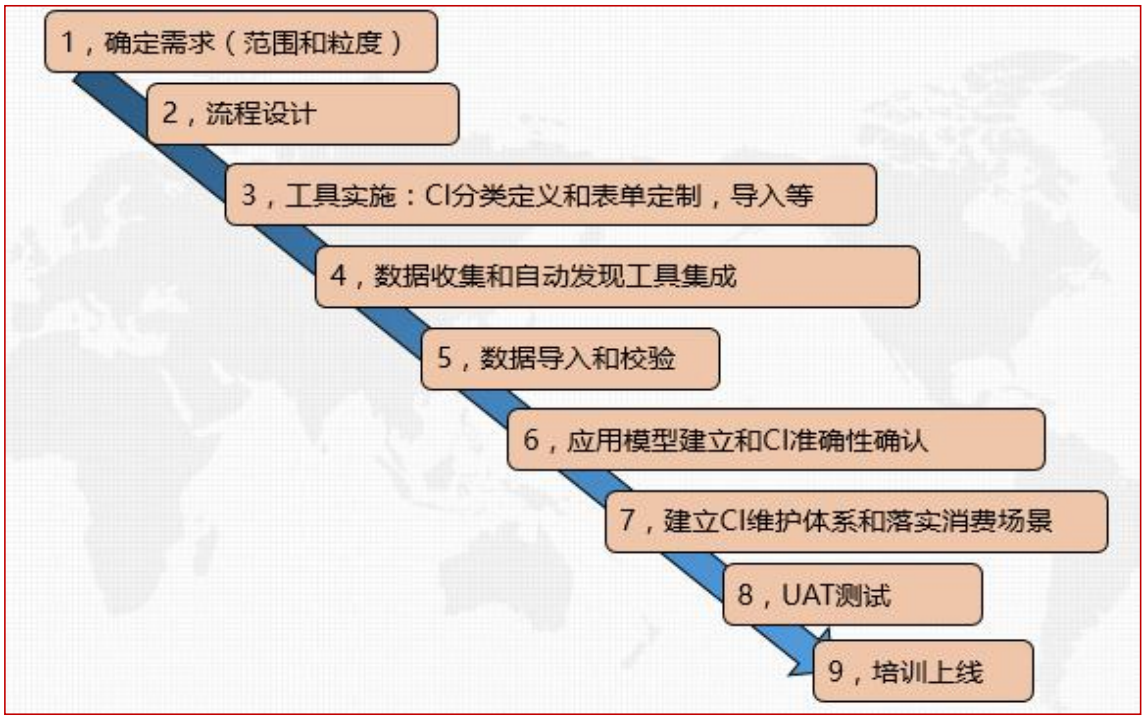
2. 实施方案



实施过的案例：



3. 建设步骤



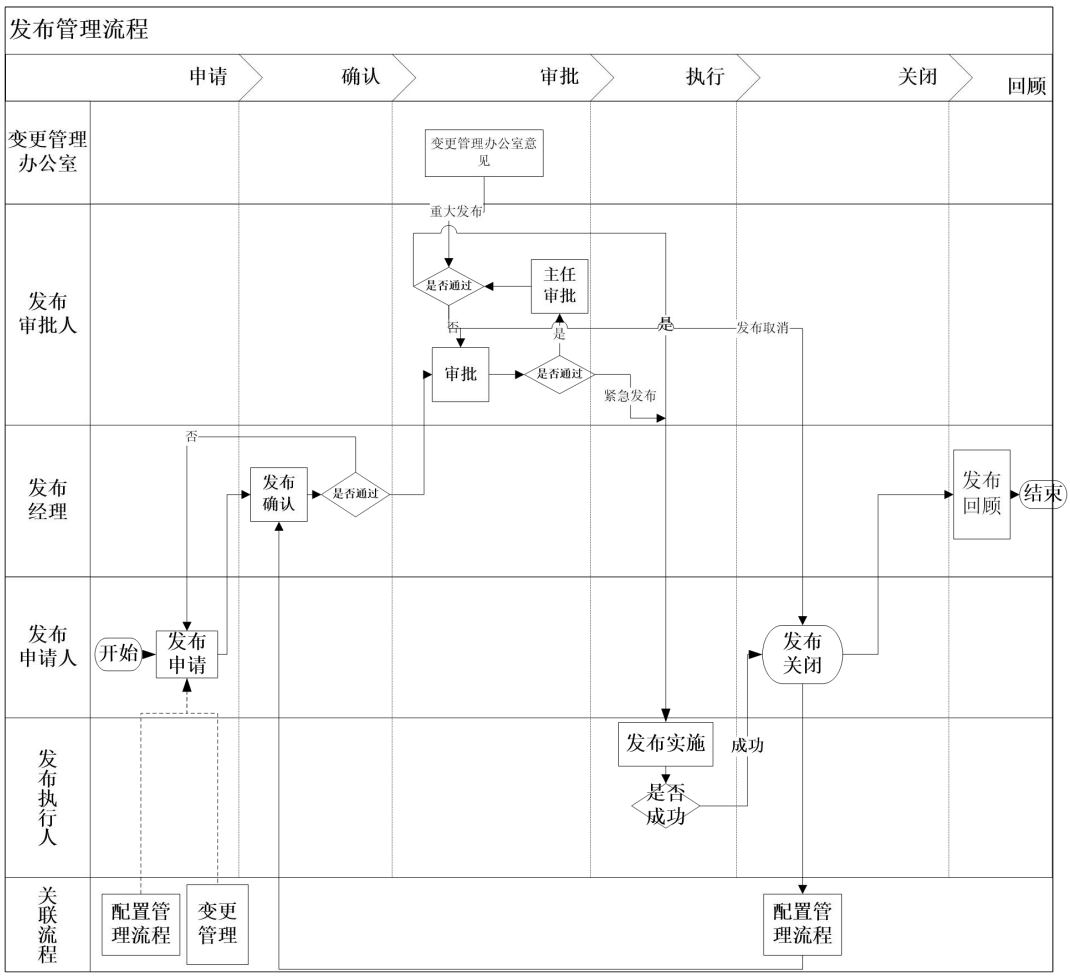
12、安全版本发布管理(可选)

➢ 流程目标与范围

发布管理是使用经过测试的软件与硬件以实施变更的流程，目的是通过正式的流程确保只有经过完整性测试与得到授权的软件与硬件才能够进入正式生产环境，以确保变更后生产环境的质量。具体分为：

- 计划和协调软件、硬件组件的发布；
- 设计和实施有效的程序（系统）来分发（push & pull）和安装（Auto & manual）IT系统的变更；
- 结合变更管理，准备发布确切内容和首次发布计划。
- 发布是由一项或多项经过批准的变更所组成。由重大发布、小型软件发布、紧急修复组成。

➢ 流程关键活动



发布管理流程

- 发布申请:维护科指定人员负责填写发布申请单，上传发布相关的附件，包括发布计划、测试报告、实施方案,风险分析等，并检查支持文档的完整性、合规性；
- 发布确认：发布经理负责对发布单进行确认；
- 发布审批:审核通过的发布计划或发布信息，如果发现发布计划或发布内容有问题，停止发布，退回发布申请人；
- 发布测试：对发布计划进行测试，并形成发布测试报告。测试仅对发布动作进行测试，如发现发布内容有问题，停止发布，退回变更申请人；
- 发布实施：发布执行人按照发布计划实施发布；
- 发布验证：在发布实施后进行，验证发布任务实施是否达到预期目的，也包括对业务功能的恢复验证等；
- 发布关闭：发布关闭由发布申请人操作，发布关闭后，可自动更新相应配置项，对一个时期以来的发布进行回顾，并形成发布管理报告,其内容包括但不限于：检查发布的增

长程度、呈现的趋势和其他相关信息，发现是否有些发布可以打包发布；对发布实施过程中出现的事件、问题进行总结，总结发布的优点和不足，提出改进建议。

➢ 角色指责与考核 KPI

角色	职责描述
发布经理	1. 设计和改进发布管理流程； 2. 设定发布管理的绩效指标并考核指标完成程度； 3. 对发布请求内容进行打包和计划，创建发布记录单； 4. 收集汇总流程信息，编制管理报告，反映存在问题，提出改进建议，制定改进计划。
发布执行人	1. 执行发布； 2. 执行发布回退或补救措施； 3. 验证发布结果； 4. 通知配置管理员修改配置项； 5. 关闭发布。
发布监督人	1. 监督发布执行人是否按照发布方案有效执行。
现场支持人员	1. 制定发布回退或补救措施。

发布管理 KPI 指标：

- 紧急发布的数量
- 发布引起的事件数量
- 按时发布的百分比

➢ 平台重点功能及示例

平台实施重点

- 支持发布的增、删、改以及相应权限分配
- 支持发布管理可手动设定审批人员
- 支持发布工单邮件及短信提醒功能
- 支持退回，交接，催办，回收。并且交接支持人员搜索功能
- 支持关联变更工单，并形成相应记录

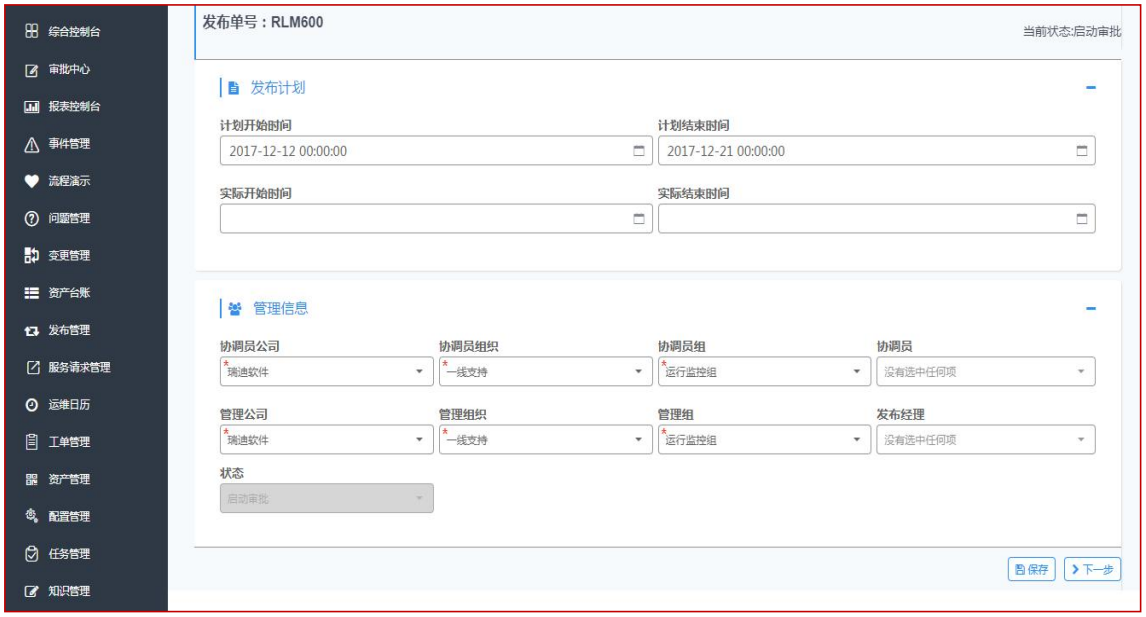
- 支持发布的处理过程进行详细的记录
- 支持一次关联多个变更单；

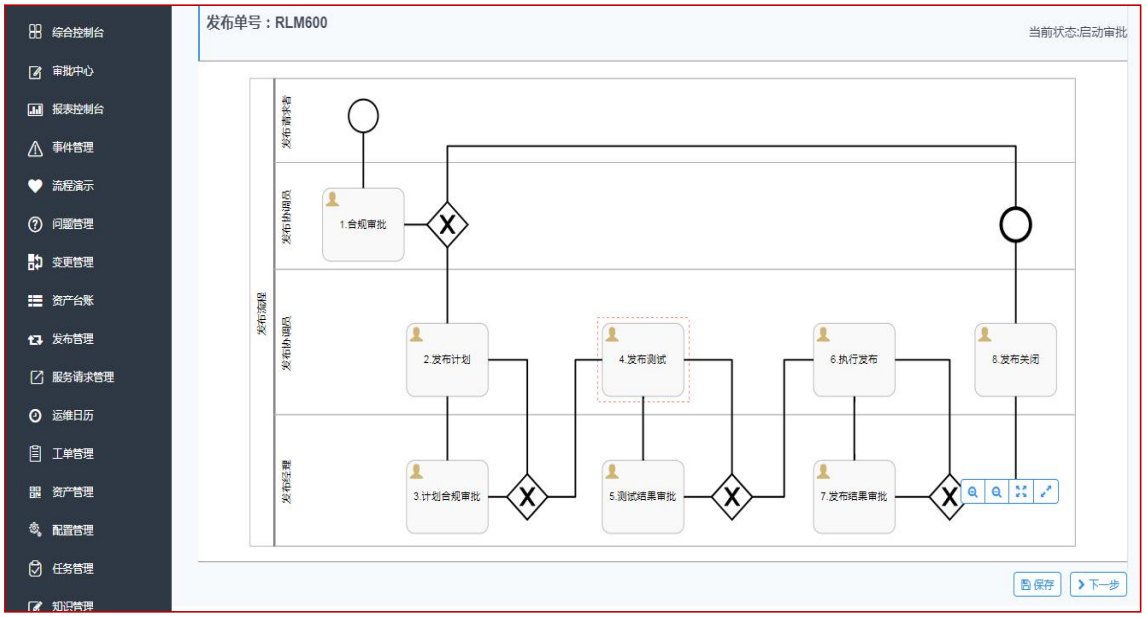
工具示例

图 1：发布管理入口

图 2： 发布单详情界面

发布单提交成功后，在单据页面上，会附带有发布流程。





13、运维知识管理

➢ 流程目标与范围

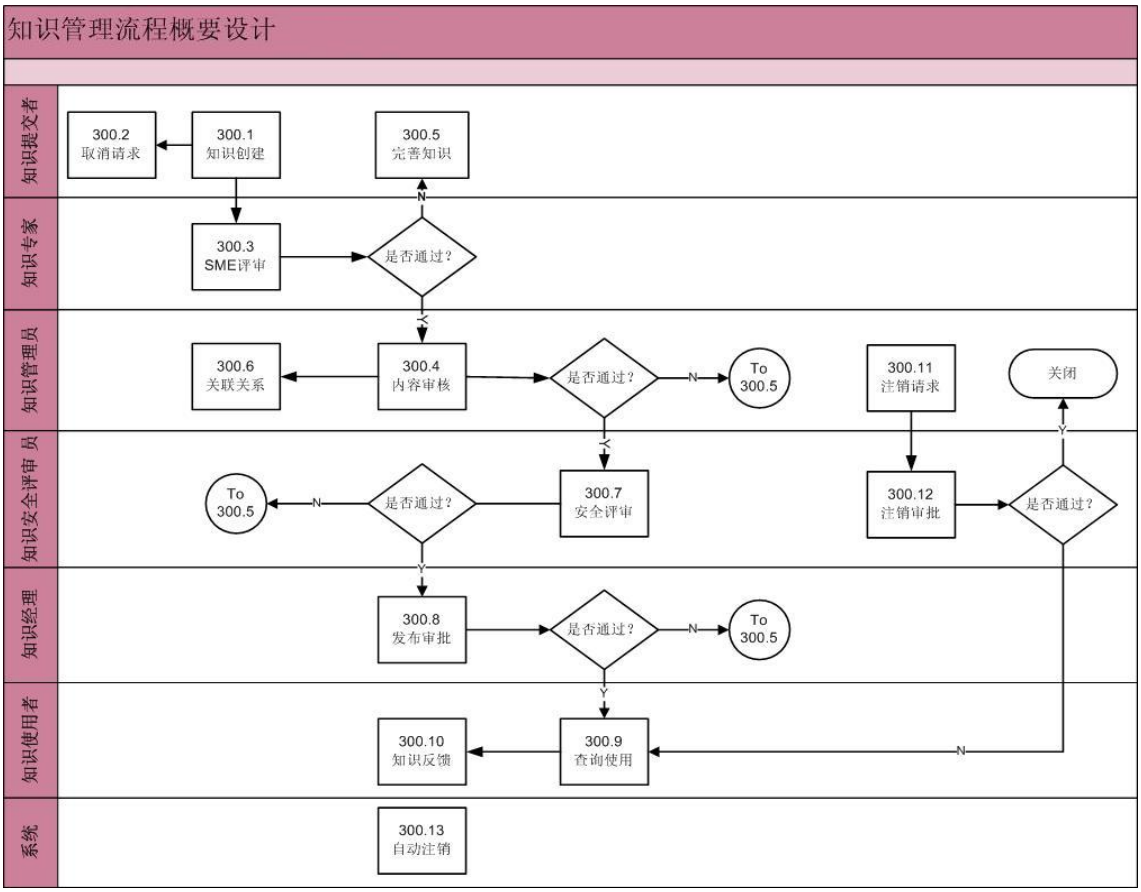
知识库提高安全响应中心服务台和一线支持的工作效率和客户满意度水平。知识库管理的目标：

- 创造知识价值：营造有序和高效的知识管理体系，通过知识的创建、共享、积累、分析，以及知识的快速检索与获取，利用知识创造价值，从而提高组织能力和个人能力。
- 实现知识共享：将 IT 支持人员从重复性的工作中解放出来，着手解决其他新的问

题，从而达到提升工作效率，降低 IT 维护成本的目的。

- 实现知识转化：知识库的建立极大地促进了知识转化，有利于提高网络安全设备运维部门的整体水平。
- 避免知识流失：有效避免由于人员流失造成的信息孤岛和知识流失。
- 提高运维响应速度和质量：作为 IT 运维的强大储备库，无疑是快速响应网络安全设备运维服务需求的捷径；同时快速、高质量的解决事件意味着提升客户满意度，而这无疑是 IT 运维的最终目的。
- 挖掘、分析 IT 应用信息：从知识条目、IT 运维解决案例、知识的生命周期等等统计数据中，不难挖掘出许多有用的信息。

➢ 流程关键活动



➢ 角色职责与考核 KPI

角色名称	关键职责	技能要求
知识提交者	1） 编写知识库草案	1） 了解相关领域的知识

	2) 提交知识库审核 3) 更新知识库内容	
知识使用者	1) 查询使用知识 2) 知识反馈	1) 了解知识的使用
知识专家	1) 对提交审核的知识进行专业技术性审核	1) 熟练掌握所属领域的专业技能
知识管理员	1) 维护知识管理流程 2) 完善知识条目 3) 分配知识查看权限 4) 确认知识生命周期	1) 了解相关 IT 技能 2) 了解用户业务流程及系统环境 3) 团队管理能力
知识安全员	1) 对提交审核的知识条目进行信息安全方面的审核	1) 对于信息安全方面的内容有一定的了解
知识经理	1) 定期考察事件，发现新的知识条目 2) 监控知识库流程运行状况 3) 当知识库超时升级时，负责或参与资源协调，完成知识库 4) 对知识库管理流程运行绩效及支持人员绩效进行周期性的统计、分析，并寻找机会进行优化和改进	1) 充分理解相关 IT 政策、操作过程和标准 2) 了解用户业务流程及系统环境 3) 用户关系管理能力 4) 资源协调和组织能力 5) 团队管理能力

流程 KPI 指标：

序号	统计指标	统计方法
1	知识库条目数量	每月知识库新增数量
2	知识库发布率	每月发布的新的知识库条目占运维人员提交的知识条目的数量比例
3	知识条目使用效	知识条目被使用次数最多的 10 条

	率	
4	安全响应中心服务台知识提交率	每月各安全响应中心服务台人员提交的知识库数量和解决事件数量比例
5	安全响应中心服务台知识采纳率	每月各安全响应中心服务台人员提交的知识库数量和被采纳知识条目数量比例
6	二线支持人员知识提交率	每月各支持组二线支持人员提交的已知错误的知识数量和解决事件数量比例
7	二线支持人员知识采纳率	每月各支持组二线支持人员提交的已知错误知识数量和被采纳知识条目数量比

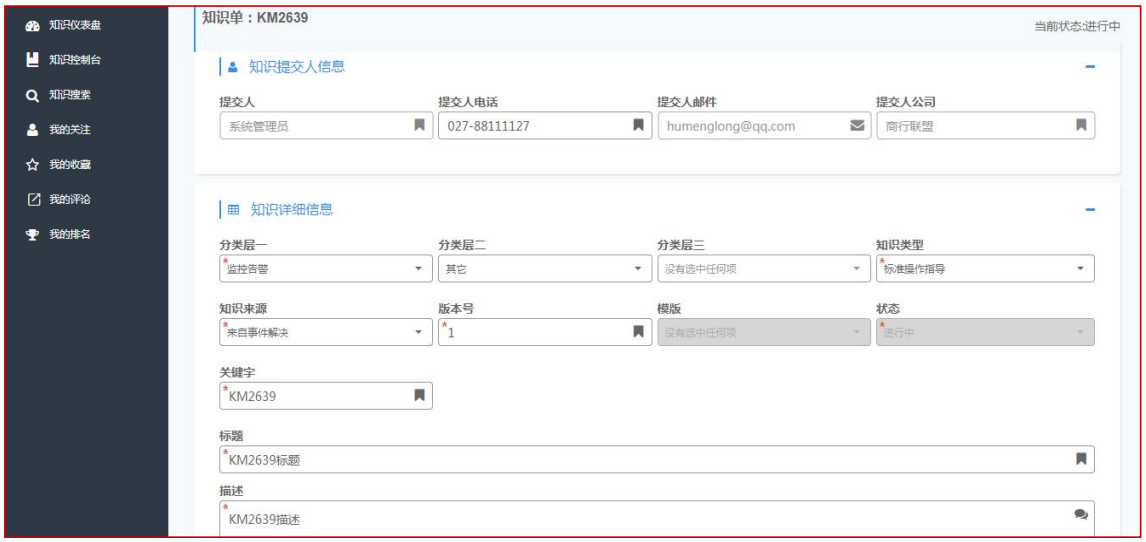
➢ 平台重点功能及示例

- 维护管理
  - 支持知识模块划分和权限划分，不同权限用户可以增加、修改、删除、查看不同模块的知识内容；
  - 可以上传各类知识文档，系统应该能够支持知识的分类存放；
  - 支持知识属性定义，知识管理输入数据项可以定制，包括日期、信息系统、负责人、关键字等；
  - 支持多种格式文件上传(特定的文档格式)和手工录入等方式。

1） 创建知识文章

知识流程的目标是为了创建积累知识，避免知识流失；共享使用知识，提高运维效率。

流程平台汇总了运维工作中知识的种类，如问题解决方案、操作指导手册、功能说明手册等。不同种类的知识有不同的模板，方便技术人员规范填写，并且可支持多种格式的知识上传，如 word、Excel、PDF 或图片或视频等。



2） 搜索知识文章

- 知识检索

在知识变为正式的发布状态之后，可以供各类用户随时检索引用。用户可以研究学习这

些知识，也可以在解决问题的过程中有目的地检索。知识记录维护用户阅读次数和用户引用解决问题次数的计数器，引用和阅读次数越多，该知识的价值越大。

为了使支持人员迅速找到所需知识，使积累的知识经验更好地发挥作用，需要实现如下检索和自动维护过程：

- 分类列表检索：

提供按照知识类别排序的树状知识结构，允许支持人员分级浏览各类知识。

关键字检索：为每条知识手工指定检索关键字的方式虽然对知识的提交带来了稍许麻烦，但是对于检索的命中率、检索性能带来极大提高。经验证明，基于关键字的检索是知识检索最有效的方式。本系统需要提供按照多个关键字组合（与/或）检索方式。

- 全文模糊匹配检索：

对知识的标题、优先级、事件现象、告警信息、原因分析、处理过程、解决方案等字段进行模糊匹配，组合检索。例如：检索事件现象中包含“HP DL580 服务器”、告警信息中包含“-6”的经验记录。

- 附件内容检索

可以对知识库的附件内容进行检索，检索内容支持中文字符。检索的附件类型支持 WORD、EXCEL、PPT、TXT 等

- 使用情况检索：

系统维护知识的阅读次数和有效次数。可以根据阅读次数和有效次数的范围进行检索，并且需要查看该知识解决过的问题的详细情况。

- 其他条件检索：

根据知识的类别、状态、提交时间段、审核时间段、提交人、审核人等属性进行检索。

支持细粒度权限划分，能够根据不同级别查看不同内容，低权限用户不允许下载知识附件等。

- 知识库类别定制

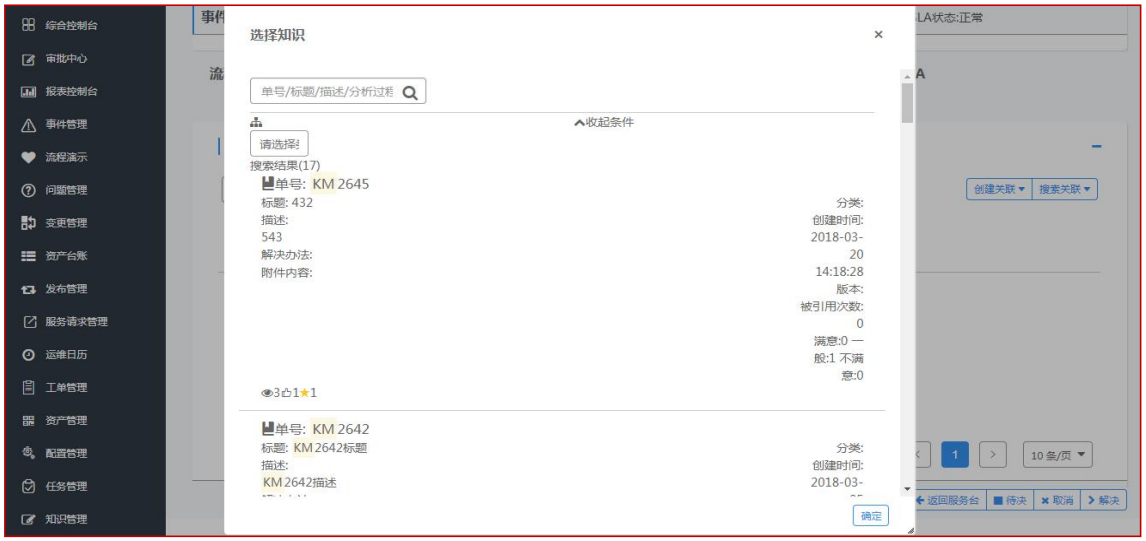
支持灵活的、多层的知识类别定制。系统提供树状级联显示知识类别功能。授权用户可

以根据实际需求，任意对其进行修改、增加、删除等设置操作。

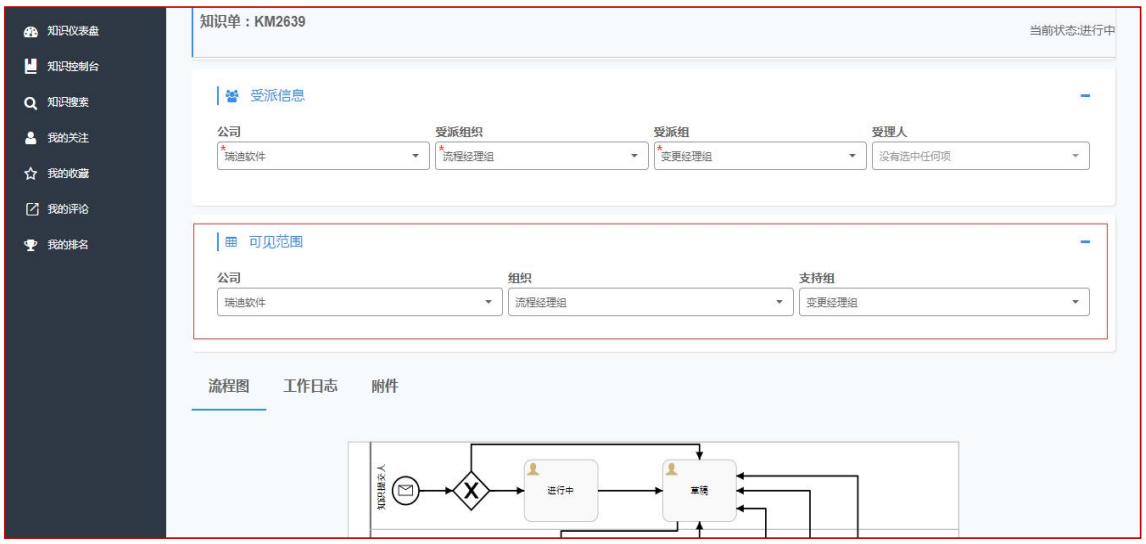
- 实现知识库和安全响应中心服务台的关联
    - 在安全响应中心服务台系统中可以实现直接对知识库的查询。
    - 用户可以在任何时间，将安全响应中心服务台中解决问题的过程和信息提交到知识库。
    - 知识库的内容和附件可以直接被安全响应中心服务台所引用。
    - 系统能自动记录和查询到：知识提交人、知识审批人、知识提交时间、知识发布时间、知识访问次数、最近访问时间等，并能生成报表进行打印。
    - 知识提交后，在未审核发布之前，知识提交者可以修改或收回知识；知识管理员有权利对未发布的知识进行修改，知识一经发布，只有审批本条知识的知识管理员可以对其进行修改

      支持从事件、问题等模块导入相应解决方案成为知识项

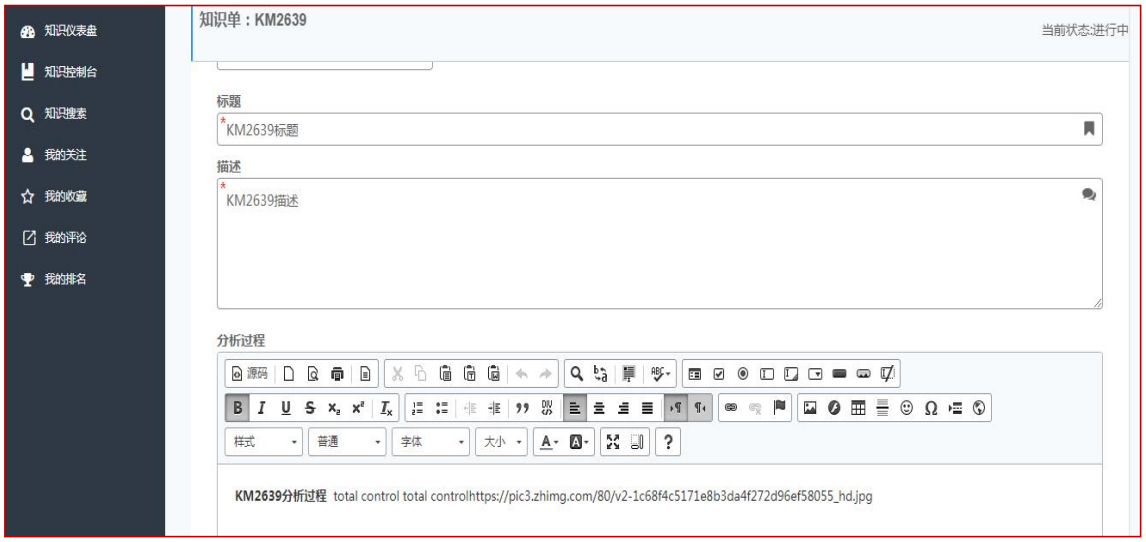
事件快速匹配使用知识：



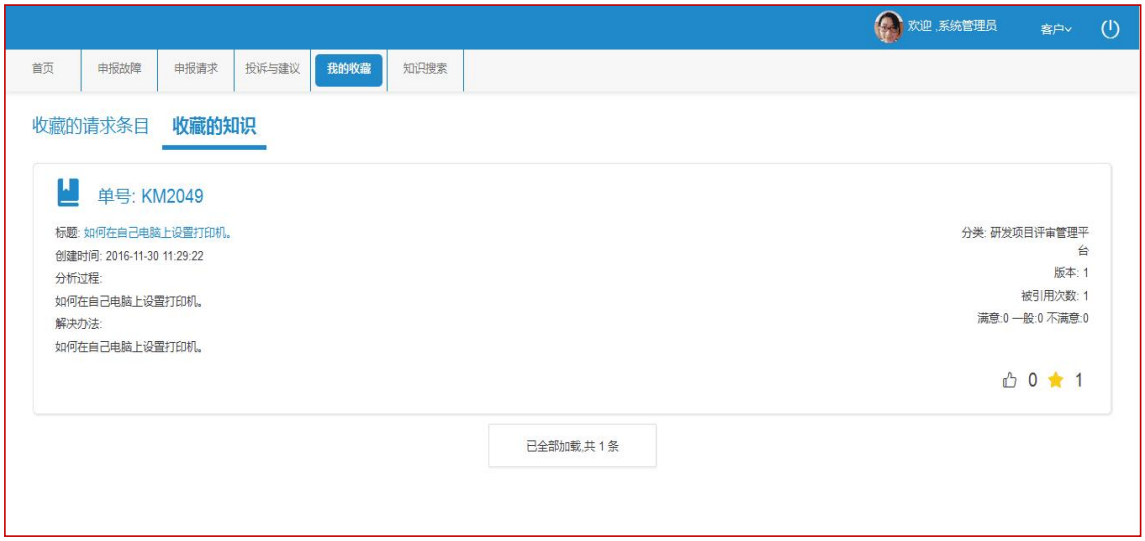
知识可见范围：

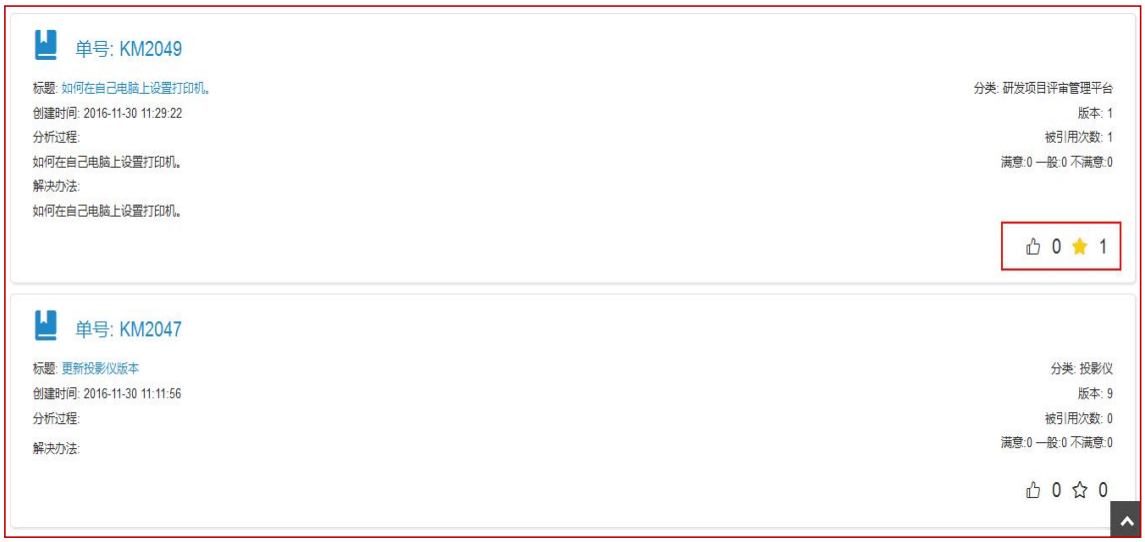

知识仪表盘
知识控制台
知识搜索
我的关注
我的收藏
我的评论
我的排名
知识单：KM2639
当前状态:进行中
受派信息
公司
瑞迪软件
受派组织
流程经理组
受派组
变更经理组
受理人
没有选中任何项
可见范围
公司
瑞迪软件
组织
流程经理组
支持组
变更经理组
流程图
工作日志
附件
进行中
重骑


笔记本
搜索结果(1)
单号: KM2174
标题: 笔记本电脑无法正常开机
创建时间: 2017-03-01 10:08:25
分析过程:
笔记本电脑无法正常开机，经常自动关机，之后就无法开机，初步诊断为系统崩溃，具体原因是杀毒软件导致的，解决方案是卸载杀毒软件，重新安装系统！
解决办法:
笔记本电脑无法正常开机，经常自动关机，之后就无法开机，初步诊断为系统崩溃，具体原因是杀毒软件导致的，解决方案是卸载杀毒软件，重新安装系统！


知识仪表盘
知识控制台
知识搜索
我的关注
我的收藏
我的评论
我的排名
知识单：KM2639
当前状态:进行中
标题
KM2639标题
描述
KM2639描述
分析过程
源码
样式
普通
字体
大小
KM2639分析过程 total control total controlhttps://pic3.zhimg.com/80/v2-1c68f4c5171e8b3da4f272d96ef58055_hd.jpg

知识的使用点赞与评价：





知识库统计平台：

14、运维任务管理

- 流程目标与范围

任务管理不是流程，是运维过程中，细分出来的最小单元（单据）。常与其他流程配合使用，如事件流程中的任务协同处理、变更流程中的实施任务、服务请求流程中的工单细分不同的请求履行任务等等。

任务管理流程是负责管理所有生产运维工作计划的流程。任务日历管理的主要目标是避免遗漏日常性运维工作，有效规划工作，提高维护窗口的使用效率，提高生产系统的运行时间，减少不必要的额外停机时间，保障 SLA 的有效的达成。

管理范围包括下面两种：

例行重复性工作:

计划性工作：

任务根据影响范围、影响时间来分为 4 级（重大、中等、一般、关注）根据不同的级别，设定不同的提醒时间和方式。

➢ 流程关键活动

提交任务申请：

任务提交人，提交相应的运维日历

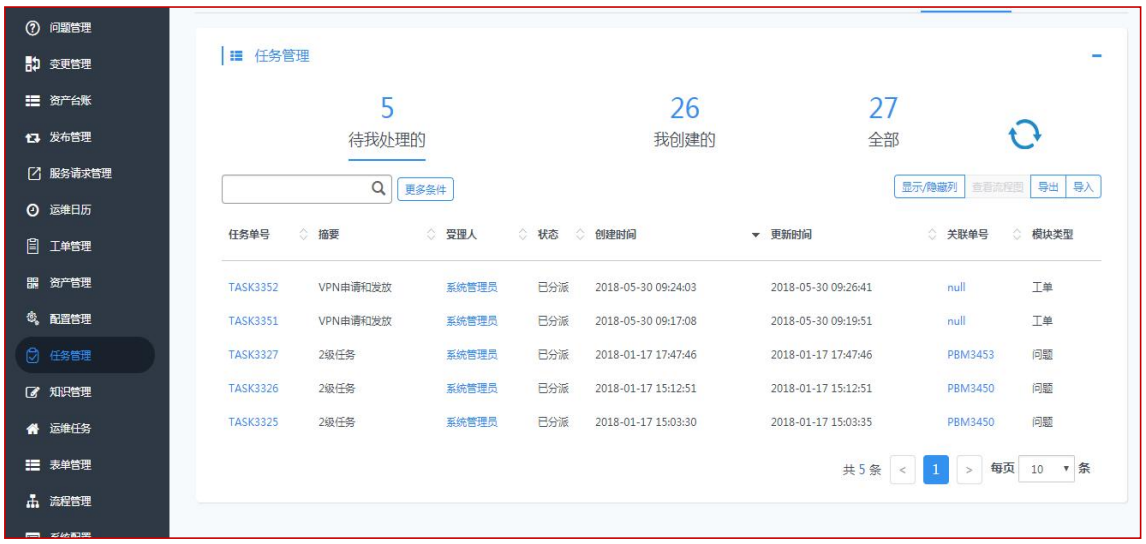
分级和设置提醒：

根据提交的任务日历需求进行分等级，然后根据不同的等级指定不同的提醒频率和相关的运维日历负责人

关联流程：任务日历流程可以从事件、问题、变更流程进行发起

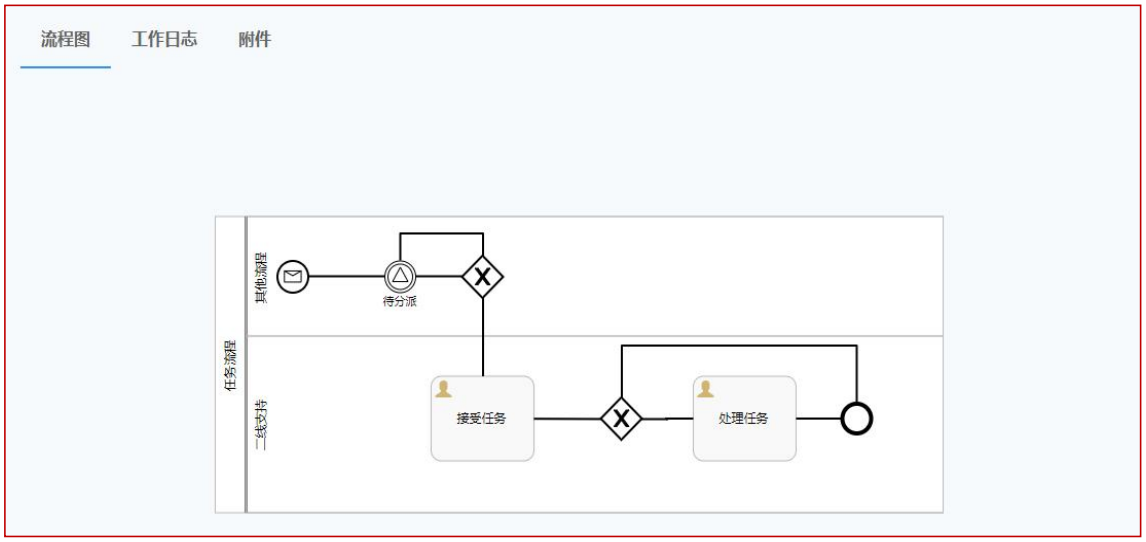
➢ 重点功能

- 提醒管理：根据任务日历不同级别，设定不同的提醒时间，提醒任务日历负责人
- 实现任务日历统计分析：周报、月报等
- 支持自定义任务日历表单和字段
- 支持自定义任务日历管理流程
- 支持处理流程的附件上传功能
- 支持与事件、变更、问题管理流程的关联，
- 支持多种主动通知方式（短信、EMAIL、界面提醒），通知节点可根据用户实际需求自定制；
- 支持自定义提醒时间阈值设置。
- 支持任务日历在安全响应中心服务台界面的自定义展示



任务管理控制台

任务详情



任务详情

TASK3352	VPN申请和发放	系统管理员	已分派	2018-05-30 09:24:03	2018-05-30 09:26:41	null	工单
TASK3351	VPN申请和发放	系统管理员	已分派	2018-05-30 09:17:08	2018-05-30 09:19:51	null	工单
TASK3327	2级任务	系统管理员	已分派	2018-01-17 17:47:46	2018-01-17 17:47:46	PBM3453	问题
TASK3326	2级任务	系统管理员	已分派	2018-01-17 15:12:51	2018-01-17 15:12:51	PBM3450	问题
TASK3325	2级任务	系统管理员	已分派	2018-01-17 15:03:30	2018-01-17 15:03:35	PBM3450	问题

15、运维服务级别管理

➢ 流程目标与范围

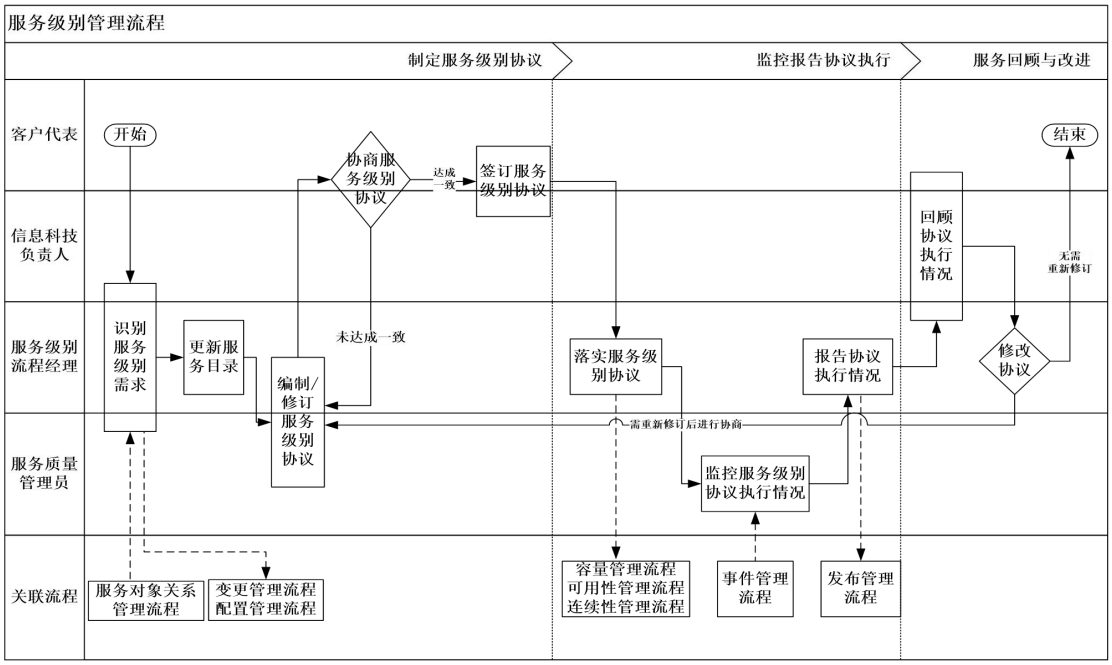
服务级别管理（Service Level Management）属于 ITIL 中服务交付范畴，它的目标是要与客户就所要提供的网络安全设备运维服务的类型和质量签订清晰的协议，并确保这些协议得以实施。

服务级别管理是定义、协商、订约、检测和评审提供给客户的服务质量水准的流程。有关所提供的服务和这些服务的质量水准记录在服务级别协议中。服务级别协议规定了服务双方各自的责任、权利和义务，是网络安全设备运维服务成功运作的重要保障。

- 服务级别协议（SLA）是网络安全设备运维服务提供方和客户之间就服务提供中关键的服务目标及双方责任等有关问题签订的协议。
- 服务级别需求（SLR）是指有关客户业务需求的详细定义，通常作为设计服务和制定服务级别协议的一个蓝本。
- 服务目录是从用户角度描述的服务项目以及有关服务级别的概要说明。例如：宕机时间、应用中断时间等。
- 支持合同（UC）是指网络安全设备运维服务提供方与外部供应商就某一特定服务项目的提供与支持所签订的协议。
- 运营级别协议（OLA）是指网络安全设备运维服务提供方与组织内部 IT 部门就某个具体服务项目的提供而达成的协议，如：网络的可用性、打印机的可用性等。
- 服务说明书（SP）描述了为客户提供的功能和 IT 部门内部实施的技术之间的关系，并为服务提供了一个详细的说明。

- 服务改进方案（SIP）通常作为一个项目来实施，定义了改进一项网络安全设备运维服务相关的活动、阶段和相应的里程碑。
- 服务质量计划（SQP）定义了服务管理流程和运营管理的流程参数，服务级别协议说明了网络安全设备运维服务提供方应该提供什么服务，服务质量计划说明网络安全设备运维服务提供方应该怎样提供服务。

➢ 流程关键活动



服务级别管理流程

- 识别服务级别需求:服务质量管理员接收来自客户的网络安全设备运维服务需求，整理后提交服务级别流程经理，服务级别流程经理审核后提交信息科技负责人，信息科技负责人根据信息技术服务交付能力以及监管要求，与客户代表就服务级别需求达成共识。
- 更新服务目录：服务级别流程经理根据客户服务级别需求，以及新增或变更服务的要求，依据变更管理和配置管理流程的管理要求，更新服务目录，并作为服务级别协议的附件。
- 编制/修订服务级别协议：服务质量管理员和服务级别流程经理根据服务目录以及服务级别需求编制或修订服务级别协议，提交信息科技负责人对服务目录、服务级别协议进行审核。
- 协商、签订服务级别协议：信息科技负责人与客户就服务级别协议内容进行沟通、

协商，如达成一致则签订服务级别协议，未达成一致则修订服务级别协议。

- 落实服务级别协议：服务级别流程经理在信息科技部公开发布已签订的服务级别协议，并组织各流程经理将服务级别协议各项要求分解并落实到可用性管理、连续性管理、容量管理等流程中，调整各流程及相关文件的关键指标及目标，确保所有的流程工作能够支撑服务级别协议的指标要求。
- 监控服务级别协议执行情况：服务质量管理员负责监控信息科技部全体员工严格按照服务级别协议执行，按照各流程要求监督、协调流程运行，整理日常工作记录和相关数据，以用于服务级别实际情况的计算。
- 报告服务级别协议执行情况：服务级别流程经理负责根据服务级别协议中的相关指标规定监控日常工作，汇总各流程经理生成的服务报告或提供的数据，编制服务级别管理报告提交至信息科技负责人，并进行发布。
- 服务回顾与改进：服务级别流程经理按照服务对象关系管理的要求，定期与客户就服务级别协议内容和执行情况进行回顾总结，根据服务回顾会议结果，确定是否需要修订服务级别协议。

➢ 角色指责与考核 KPI

角色	职责描述
客户代表	1. 参与商定服务级别内容定制；
信息科技负责人	1. 与客户代表协商服务级别内容； 2. 参与回顾服务级别协议履行情况；
服务级别流程经理	1. 负责流程直接的、日常运作的活动，流程主要的交付物都是服务级别经理的直接职责。 2. 配合服务规划人员建立和维护组织目前为客户提供服务的服务目录； 3. 描述、协商和维护组织的服务级别管理架构，包括： a) 建立 SLA 结构 b) OLA c) UC 4. 调研业务部门对服务级别的需求，识别和确定服务级别需求 5. 磋商和签订 SLA、OLA、UC 等

角色	职责描述
	6. 分析与比较实际服务水平与 SLA 约定的水平，提出服务改进计划需求 7. 制作定期报告，报告服务水平 8. 发起、组织和实施定期回顾检查报告会 9. 收集整理并分析业务部门、内部科技信息部、外部供应商的反馈和意见，制定行动计划 10. 处理流程开发中出现的问题，把不能解决的问题及时上报给管理层 11. 根据流程衡量指标生成报告，提供给流程负责人分析，并参与流程改进会议。
服务质量管理员	1. 参与编制/修订服务级别协议； 2. 监督服务级别协议履行情况。

服务级别管理流程 KPI 指标：

- 与用户签订的服务级别协议数量；
- 服务级别协议完全履行比率；
- 已具备 SLA 的客户占总客户数的百分比
- SLA 已覆盖的服务占总服务数的百分比
- 过期的、需要更新的 SLA、OLA 和 UC 占各自总数的百分比

➢ 平台重点功能及示例

平台实施重点

- 支持对网络安全设备运维服务提供方与客户签订的服务级别协议、网络安全设备运维服务提供方与供应商签订的支持合同进行规则定义和集中管理，部署标准格式的 SLA 数据，并通过流程进行实时跟踪和历史审计；
- 支持创建、变更和删除 SLA 中有关网络安全设备运维服务提供方、客户、特定服务的信息以及指定服务的效用信息。
- 支持 SLA 与事件管理进行关联，自动识别、跟踪和统计事件管理的执行效果，落实面向客户的服务质量承诺，加强面向 IT 部门的流程内控管理；
- 支持 SLA 与事件类别相关联，设置与服务目录、问题类别、变更类别相关联的 SLA，

由该 SLA 跟踪与之关联的事件、问题、变更管理流程的运行；

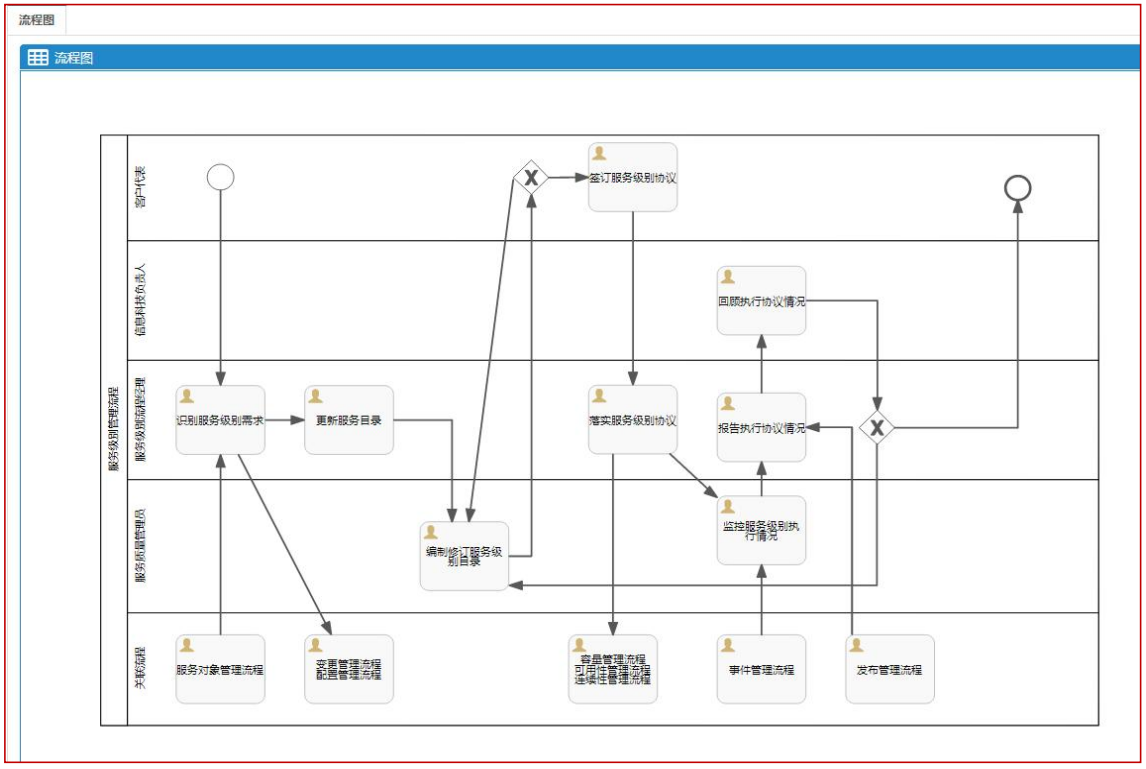
- 支持面向不同部门部署不同内容的 SLA；
- 提供面向不同优先级别部署不同内容的 SLA；
- 支持对 SLA 的响应时间、解决时间进行设定，并以此作为流程运行目标和服务监视点。对 SLA 的自动转交时间的设定，防止服务超时违反 SLA；
- 支持图形化方式设定 OLA 升级预警时间阀值，在流程运行时在已设定时间点向相关人员或管理层预警报告，防止服务超时违反 SLA；
- 支持对 SLA 进行审计追踪，自动记录 SLA 的变更情况；
- 支持对 SLA 进行制订、审批、部署、修订、废止全生命周期管理和控制；
- 支持通过集成的界面显示各种 SLA 的实时状况；
- 支持生成报表显示网络安全设备运维服务在与服务水平协议相比之下的完成情况。

工具示例

图 1：服务级别管理入口

图 2： 服务级别需求单详情界面

服务级别需求单提交成功后，在单据页面上，会附带有发布流程。



根据报表统计分析服务水平达成情况：

16、网络安全值班管理（可选）

➢ 流程目标与范围

- 系统通过对人员进行一个排班计划，将值班信息录入系统中，根据周，月形式展现在控制台界面。充分计算机应用技术和手段，提高办公效率、改善质量的高效管理信息系统。
- 对工作任务进行管理，自动进行交接并提醒下一位值班人员

➢ 平台重点功能及示例

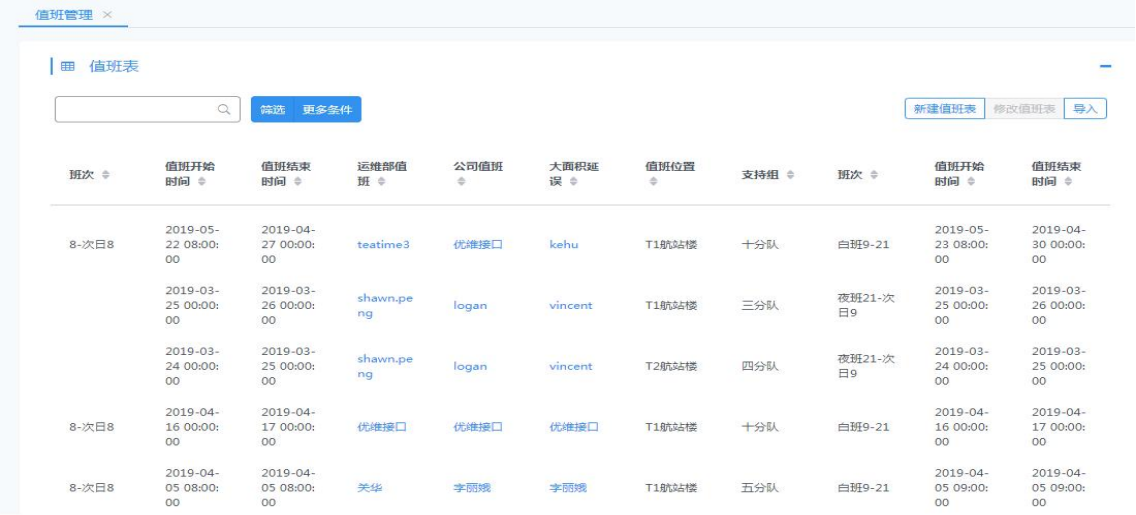
值班管理描述：

系统通过管理人员的排班计划，根据当前的日期时间，根据排班表的计划，给对应的值班人员一个值班任务。值班人员接受值班任务后，对当前值班的情况记录在值班记录中，下班即处理完成值班任务提交。

排班表展示：

添加排班计划：

值班记录：



班次	值班开始时间	值班结束时间	运维部值班	公司值班	大面积延误	值班位置	支持组	班次	值班开始时间	值班结束时间
8-次日8	2019-05-22 08:00:00	2019-04-27 00:00:00	teatime3	优维接口	kehu	T1航站楼	十分队	白班9-21	2019-05-23 08:00:00	2019-04-30 00:00:00
	2019-03-25 00:00:00	2019-03-26 00:00:00	shawn.peng	logan	vincent	T1航站楼	三分队	夜班21-次日9	2019-03-25 00:00:00	2019-03-26 00:00:00
	2019-03-24 00:00:00	2019-03-25 00:00:00	shawn.peng	logan	vincent	T2航站楼	四分队	夜班21-次日9	2019-03-24 00:00:00	2019-03-25 00:00:00
8-次日8	2019-04-16 00:00:00	2019-04-17 00:00:00	优维接口	优维接口	优维接口	T1航站楼	十分队	白班9-21	2019-04-16 00:00:00	2019-04-17 00:00:00
8-次日8	2019-04-05 08:00:00	2019-04-05 08:00:00	关华	李丽娥	李丽娥	T1航站楼	五分队	白班9-21	2019-04-05 09:00:00	2019-04-05 09:00:00

17、网络安全巡检管理（可选）

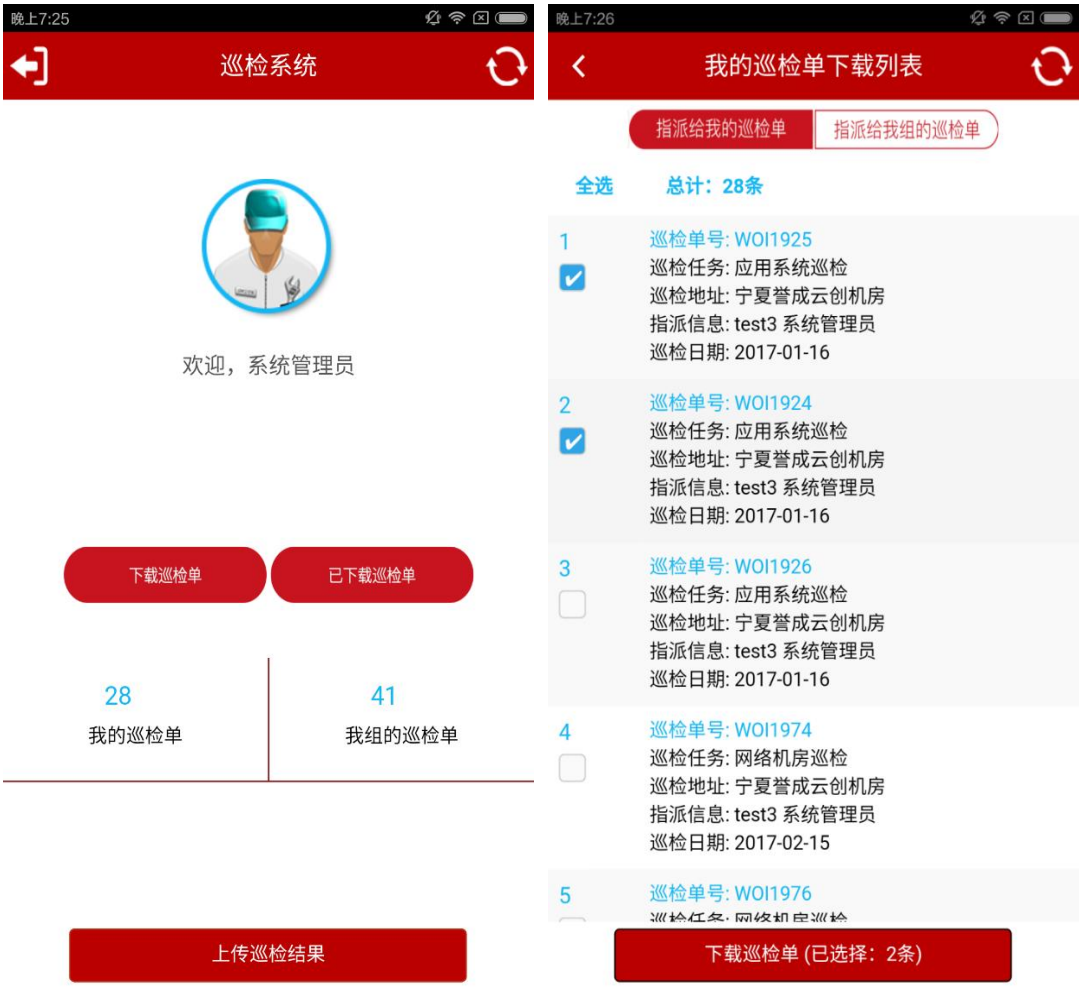
RXGT ITSM 通过了解客户实际需求，推出了人工巡检模块，主要帮助企业更好的实施资产设备的日常维护，提高维护的便捷性，提升工作效率。

日常运维巡检工作，通常情况下，先设定好巡检计划表，规划巡检范围、巡检内容、巡检时间与周期以及巡检执行人员。如下图所示：

- **人工巡检过程**

当制定好巡检计划，预设定了巡检任务后，在正式巡检之前，运维人员可通过手机 APP 下载巡检任务，查看当天要做的具体事项，开始巡检；巡检过程中，如发现设备故障，可直接扫描设备上的二维码，申报故障；最后巡检结束，提交巡检报告。

- **巡检人员接受巡检任务，在手机 APP 上实施巡检**



18、智能运维服务报告和 KPI 指标

➢ 报表管理概述

报表对于监控流程运作十分重要，通过报表可以对流程的性能和价值进行评估，可以告诉管理人员流程的执行情况和结果，反映用户对流程的满意程度。同时，通过报表监控，对管理流程的运作情况进行统计分析，可以充分了解流程的现状，为流程的改进提供帮助。

RXGT ITSM 报表系统简要说明如下：

实现方式	RXGT ITSM 自带 echarts 与 Birt 引擎，直接使用报表工具开发
访问方式	C/S、B/S 结构，通过 WEB 客户端工具访问
主要特点	1. 报表引擎免费； 2. RXGT ITSM 已经优化，开发效率高； 3. 格式展示支持：Excel/Word/PDF 等等；

	4. 无法访问其他数据源；

➢ 开箱自带报表功能

RXGT ITSM 根据不同的运维管理需求，整理了大量流程报表模板，用户可以直接使用。报表的展示形式有两种：图形化展示报表和统计型报表。

图形化报表，也就是以丰富的图表方式展示各种运维报表及 KPI，例如事件解决率、事件 SLA 状态、用户满意度等报表。这类报表的特点是直观、形象，便于 IT 管理层快速掌握运维流程单据的处理情况及用户反馈。

统计型报表，即事后统计流程单据数据，例如每周事件发生量、每月事件解决量等。这类报表的特点是以列表、简单图形的方式给运维报告提供可靠数据素材。

RXGTITSM 内置的报表模板：

模块	报表名称
网络安全设备变更管理	在计划时间内按时完成的变更比率
网络安全设备变更管理	统计未通过审批就执行的变更比率
网络安全设备变更管理	变更成功率
网络安全设备变更管理	变更积压数
网络安全设备变更管理	统计每月紧急变更的比例
网络安全设备变更管理	统计每月紧急变更的比例
网络安全设备变更管理	已批准但实施失败的变更请求
网络安全设备变更管理	按变更分类统计变更数量
网络安全设备配置管理	按状态分类层 1 统计
网络安全设备配置管理	按状态分类层 2 统计
网络安全设备配置管理	按状态分类层 3 统计
网络安全设备配置管理	CI 关联变更单量统计
网络安全设备配置管理	CI 关联事件单量统计
网络安全设备配置管理	CI 关联问题单量统计
网络安全设备配置管理	按分类层 2 统计
网络安全设备配置管理	按分类层 3 统计
网络安全设备知识管理	通过状态统计知识百分比

网络安全设备知识管理	通过知识解决的事件百分比
网络安全设备知识管理	知识反馈
网络安全设备知识管理	知识使用情况统计
网络安全设备知识管理	按月统计新增知识
网络安全设备其它	审批拒绝率
网络安全设备问题管理	问题平均解决时间
网络安全设备问题管理	根本解决数量统计问题单
网络安全设备问题管理	已创建解决方案的问题数量
网络安全设备问题管理	问题关联变更的比率
网络安全设备问题管理	创建了解决方案的问题百分比
网络安全设备问题管理	问题平均解决时间(分钟)
网络安全设备问题管理	根本解决数量统计问题单
网络安全设备问题管理	已创建解决方案的问题数量
网络安全设备问题管理	问题关联变更的问题数量
网络安全设备问题管理	创建了解决方案的问题百分比
网络安全设备问题管理	按月统计新增问题数量
网络安全设备问题管理	按受派组、受派者统计问题单
网络安全设备问题管理	按状态统计问题单
网络安全设备问题管理	按状态和分类分组的问题的总数
网络安全设备问题管理	所有已创建的问题数量
网络安全设备问题管理	问题成功解决率
网络安全设备服务请求管理	已完成的工单满足 SLA 的比率
网络安全设备服务请求管理	排名前 10 的频繁使用的服务请求类别
网络安全设备服务请求管理	统计各分类服务请求的状态
网络安全设备服务请求管理	按月统计已创建工作单的数量
网络安全设备服务请求管理	按状态和优先级统计已创建工作单的数量
网络安全设备服务请求管理	未完成的服务请求任务单数量
网络安全设备事件管理	通过 SLA 状态统计事件解决情况
网络安全设备事件管理	通过 SLA 状态统计活动事件情况

网络安全设备事件管理	事件一线解决率
网络安全设备事件管理	事件二线解决率
网络安全设备事件管理	从事件创建到事件解决的分钟数
网络安全设备事件管理	事件平均解决时间（分钟）
网络安全设备事件管理	按事件优先级统计已创建事件数量
网络安全设备事件管理	按事件来源统计已创建事件的数量
网络安全设备事件管理	按事件状态统计已创建事件的数量
网络安全设备事件管理	事件信息汇总 1
网络安全设备事件管理	事件信息汇总 2
网络安全设备事件管理	在 SLA 规定的目标时间内解决的事件
网络安全设备事件管理	在 OLA 规定的目标时间内解决的事件
网络安全设备事件管理	事件及时解决率

报表控制台：多展示图形化报表。

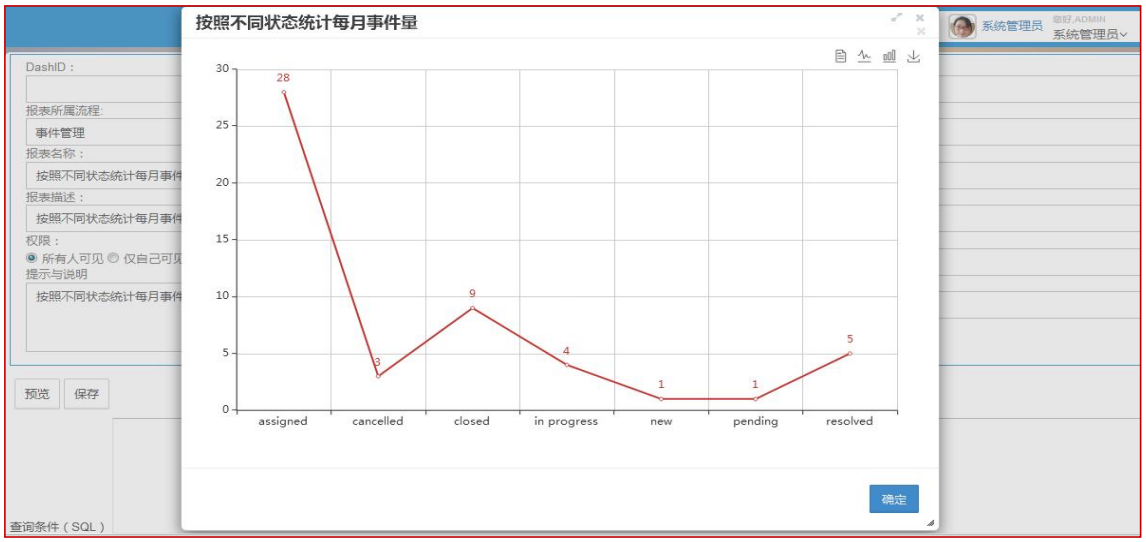

全部
单据数量统计
2195
事件数量
刷新 编辑
2
问题数量
刷新 编辑
26
发布数量
刷新 编辑
196
工单数量
刷新 编辑
事件
事件报告用户分布
事件数量
High
Low
事件满意度反馈
不满意
满意
不满意: 7.69%
满意: 92.31%
INC_INCIDENT_NUMBER
事件实时积压数量统计
事件实时积压
3263
事件报告类型统计
事件数量
12k
10k
8k
6k
4k
2k
0
6683
11092
2679
2557
1398
其它
咨询
故障
服务请求
需求


事件周创建量及周环比统计_应用系统
周报事量
周环比%
事件周解决量及解决率统计_应用系统
周报事量
周解决量
周解决率

驾驶舱报表

➢ 扩充和定制新报表

如下图所示，RXGTITSM 报表体系从定制开发到用户查看使用，主要包含以下几个方面：



- 定制开发：RXGTITSM 提供 JDBC 数据源，报表开发人员可以使用 Birt 报表开发程序访问该 JDBC 数据源，抽取、处理相应的数据字段，并定义好报表的呈现格式；
- 报表格式导入：定义好的水晶报表文件（rpt 文件）通过 RXGTITSM 表单导入 RXGTITSM 系统，并定义好报表的相关属性；
- 报表查看：RXGTITSM 客户端程序内置 Birt 查看引擎，用户可以通过 RXGTITSM 报表控制台应用分类查看运行相关报表。

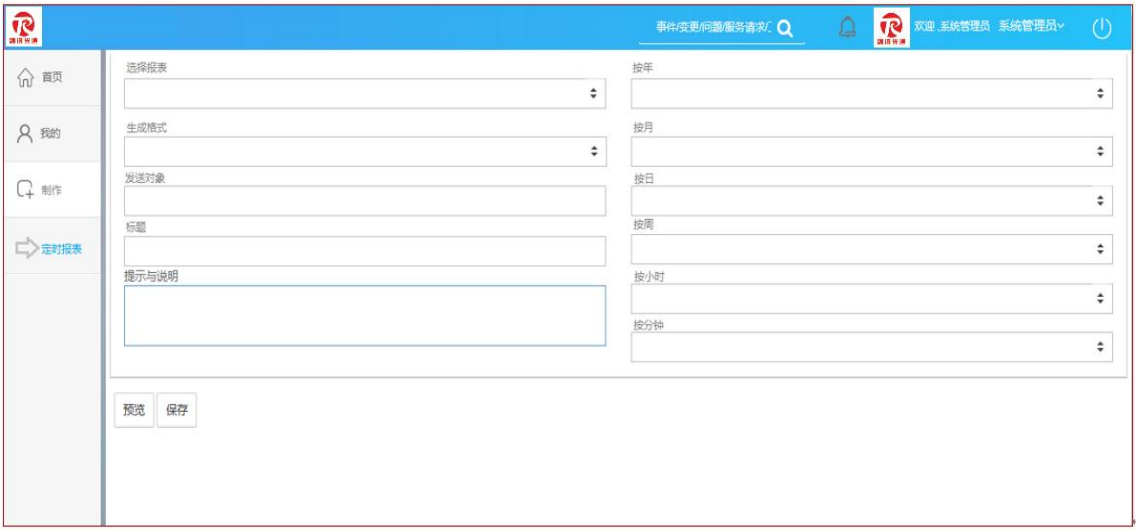
➢ 自定义仪表盘

能够自定义自己的仪表盘，实时展示数据，支持在 SLA 及 KPI 指标即将违反时进行警示。

可编辑仪表盘展示的样式和展示的报表

➢ 定时报表

可选择报表，按特定时间或者周期导出报表，并发送给选则的人员。

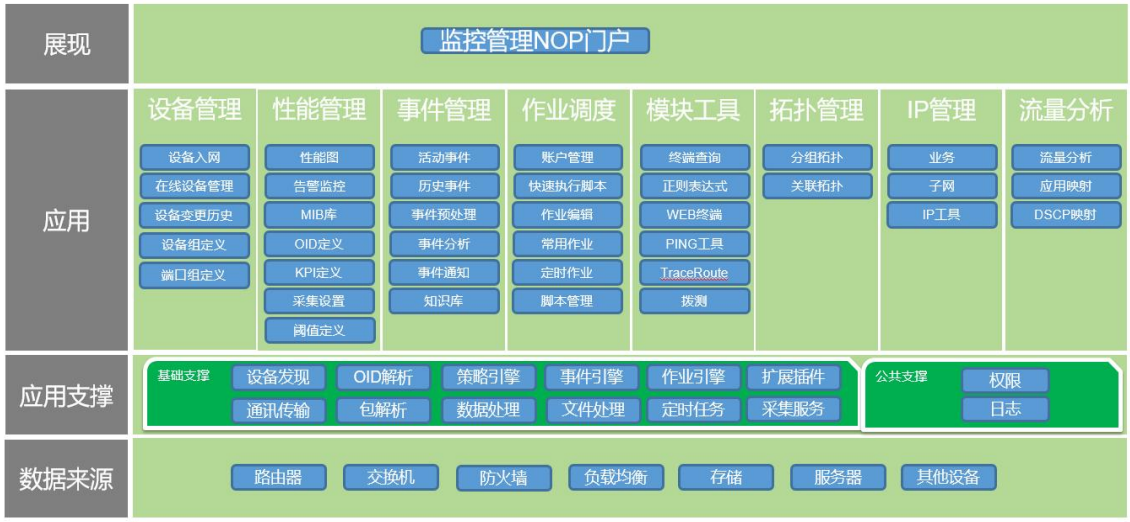


四、网络安全设备智能监控

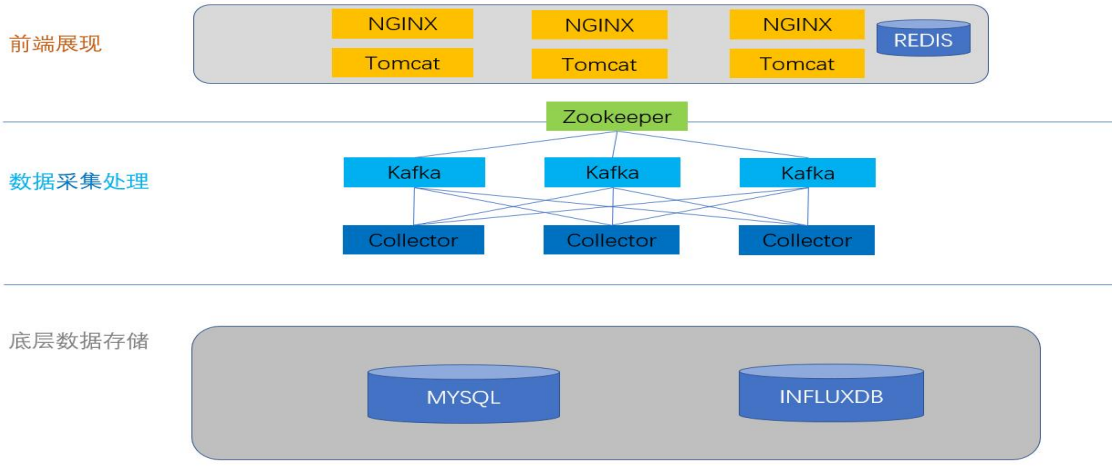
网络质量和网络安全被越来越多的用户所关注。针对企业级网络监控运维管理的现状，企业中使用的网络设备品类繁多，设备数量也很庞大。依赖于设备厂商自己的网管系统往往只能覆盖各厂商自己品牌的设备，对其他厂商的设备纳管监控往往很不方便。这就为企业网络管理人员的日常巡检和配置变更带来相当巨大且重复的工作量，降低了工作效率。针对目前企业中存在的网络设备的管理痛点和难点，融讯光通深耕网络监控优化与自动化领域，提供了一套相对完善的网络可视化监控解决方案以覆盖市场上绝大部分的网络设备。在行业内融讯光通也积累了丰富的经验和案例场景，也得到了用户的一致好评。

1、产品架构

融讯光通运维自动化监控平台目前主要包含 9 个系统功能模块：资产配置管理、性能管理、Portal 管理、事件管理、拓扑管理、自动化作业管理、IP 地址管理、流量分析和集成管理。系统架构中功能架构图如下：



网络监控平台使用的软件技术架构图如下：



网管平台产品架构图

前端展现上网络监控平台采用展现层通过开源组件实现 WEB 服务器的负载均衡，采集处理层利用 Zookeeper 实现消息和采集器的集群，保障高可用性以及处理效率，底层数据存储由 Mysql 负责存储事件 Influxdb 负责存储时序性能数据。

2、优势

1、稳定灵活的架构设计

产品在设计上从数据库、队列管理、缓存管理及中间件、负载均衡等全部采用主流的开源软件平台。其平台的稳定性和可靠性均得到广泛的验证且平台的升级与持续支持能力均有活跃的社区支持。

为适应企业级的应用要求，产品架构在各组件的设计上均实现了高可用集群的能力。灵活可伸缩部署架构也充分考虑了企业级应用的灵活适应业务扩展需求。

对于具有多级分支机构的大型企业集团或总部总行，我们实现了统一部署分级管理。通过支持多租户、数据隔离、分权分域等设计，满足集团用户的多种分级管理需求。

2、优异的处理性能

经过多年的耕耘，产品从部署实施到支撑运维均经受过大型企业网络规模的考验。

网络设备日志采集与告警过滤模块达到了日处理十亿级日志条目告警过滤压缩策略无延迟的能力。

吻合用户场景的使用体验

产品前端框架采用 VUE 架构，界面风格符合主流互联网应用交互体验。

多年专注的挖掘与行业客户场景积累，使各功能模块更吻合行业用户的应用场景。

3、开放的集成接口

前后台的设计分离及各功能模块的松耦合集成设计，既满足各模块的统一协作要求，

又具备灵活裁剪与扩展的能力。

标准开放的 API 接口可以快速与第三方管理平台或工具集成。

3、运维信息采集和处理

采集处理系统，实现对信息系统各个组成部分的性能数据及事件数据的采集，并根据设定的阈值及事件处理规则对采集数据进行处理，以达到及时了解安全管理运行环境中各组件状况的目的。

采集对象具体分类：

（1） 网络设备和线路：包括通讯线路、接入设备、交换机和路由器等；

（2） 服务器设备：Linux 和国产化服务器系统；

（3） 安全设备：防护墙、入侵防护等系列安全设备；

（4） 数据库：各类数据库；

（5） 中间件：网络安全使用到的中间件，包括 MQ/Redis 等。

（6） 机房设备：使用既有的机房软件监控，将告警事件转发到集中告警平台。

（7） 存储设备：将通过 SNMP 将告警送往集中事件管理平台进行集成。

（8） 核心业务监控：通过进行用户模拟测试业务情况的实现应用监控。

运维平台数据采集和处理，主要包括以下两类：

（1）性能数据流：对于性能的实时数据，由 Agent 进行采集后，直接送往运维门户界

面上可以直接查看。这部分实时的性能数据保存在虚拟内存中，不进入数据库。对于性能的历史数据，由 Agent 进行采集后，通过定时导入数据库。这部分历史数据可以通过运维的门户界面直接查看，也可以通过报表系统生成报表后进行查看。

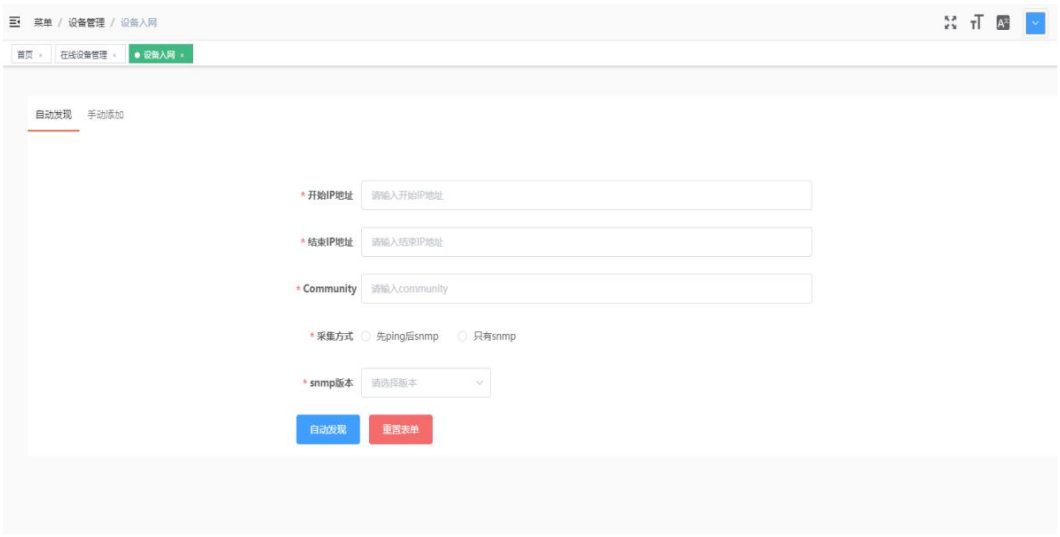
（2）告警数据流：对于监控对象，包括网络安全设备、网络安全应用中的操作系统、数据库、中间件、机房设备、存储设备等对象发出的事件告警，通过设置阀值生成性能告警数据。这部分告警事件将展示在运维门户界面中，也可以通过报表系统生成报表后进行查看。事件告警由三部分构成:1）通过收集网络设备的 syslog 告警数据;2）通过 snmp trap 收集网络设备的 snmp trap 告警数据;3）通过设定阀值生成性能告警数据。

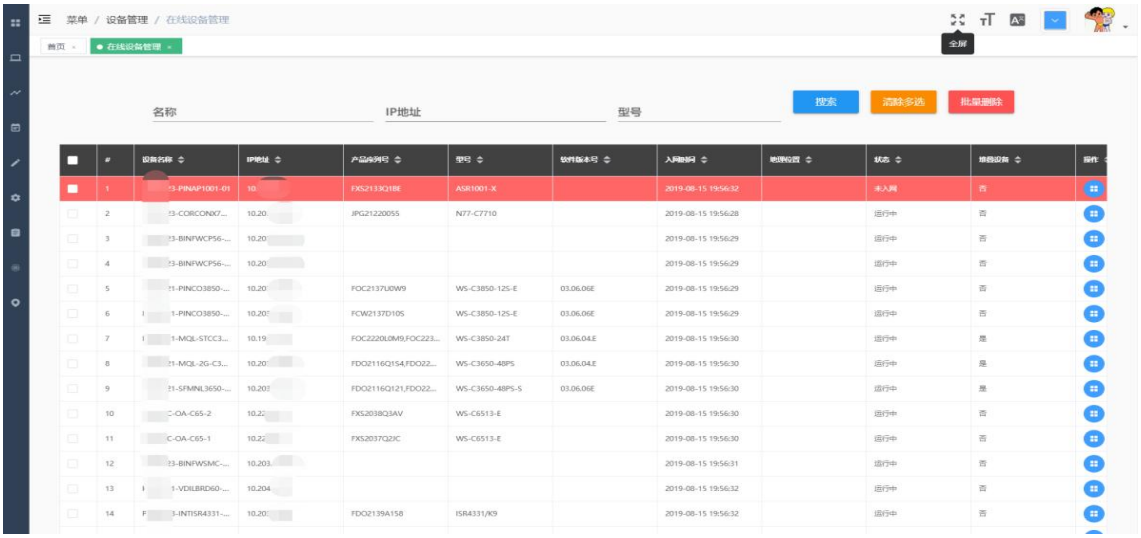
4、网络安全设备资产自动发现

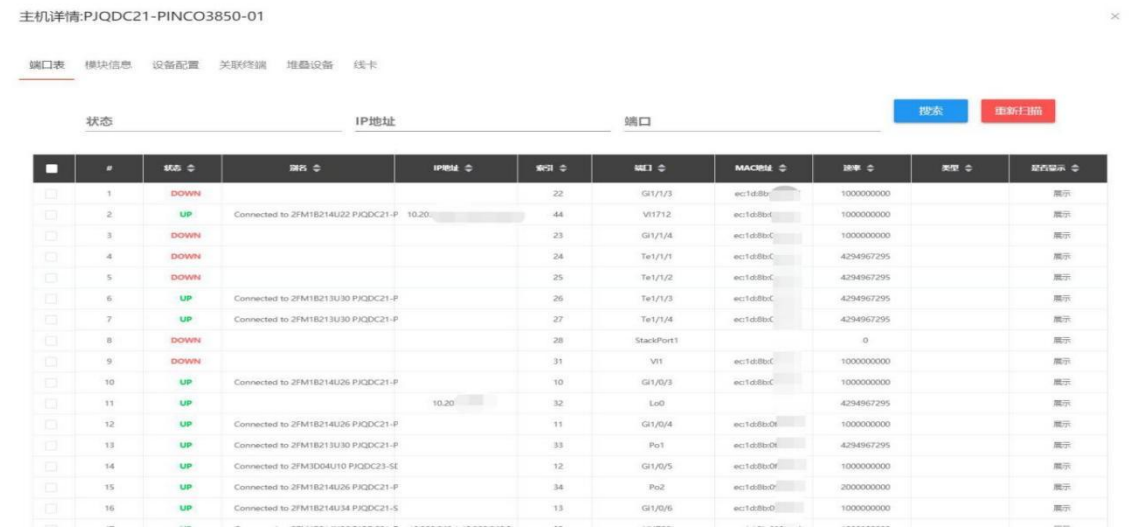
通过自动发现被管设备，自动实时发现资产变化；自动实时轮询设备状态；将新发现的设备置于待入网状态，由管理员确认后进入运行中状态；当设备在预设的时间段内离线时，自动将设备置于维护中状态；当设备在更长的预设时间段内离线时，自动将设备置于待拆除状态。每种状态都以不同颜色标识以提醒管理员关注。

同时，作为网络管理域的设备、链路、配置等资产信息的统一数据库，资产信息库还作为网络管理域的 CMDB，供各种网络管理场景（如事件告警、性能管理、拓扑展示、自动化巡检、批量下发配置等）消费资产配置信息来便捷准确地完成各种运维任务。

在发现方式上，用户可选择根据管理 IP 网段或指定种子节点（如核心设备 IP）等方式自动发现各种在线设备。设备自动发现功能支持用户自定义厂商的 snmp oid 等参数，可以支持各厂商的设备。设备自动发现入网的设备，可同时将设备序列号，型号，软件版本等基础数据自动采集至资产库。用户还可通过外部文件批量导入或收到输入的形式关联资产入库线下数据（如供应商、服务起止日期、到货日期等信息）。

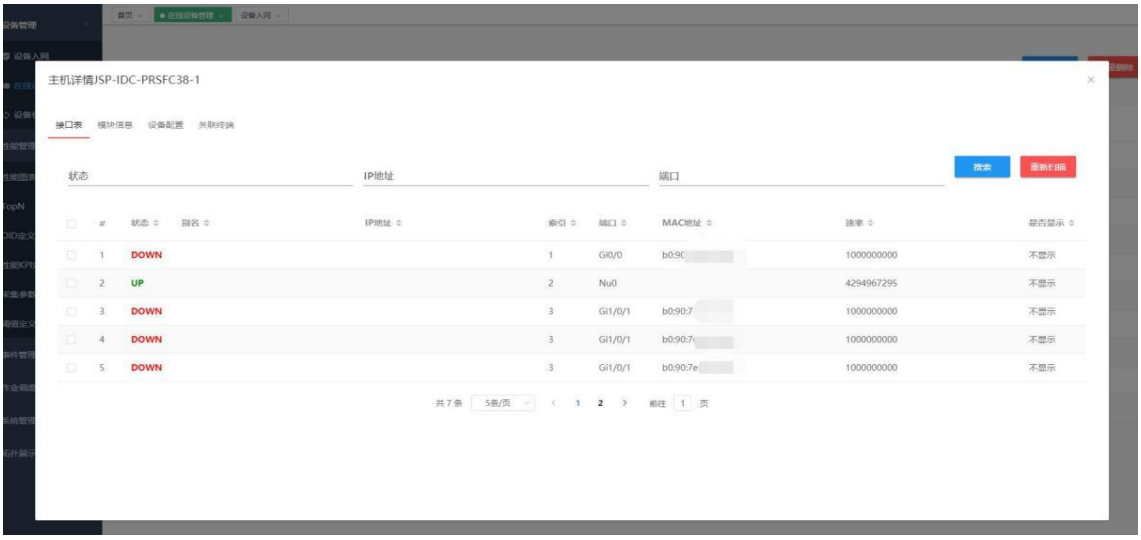




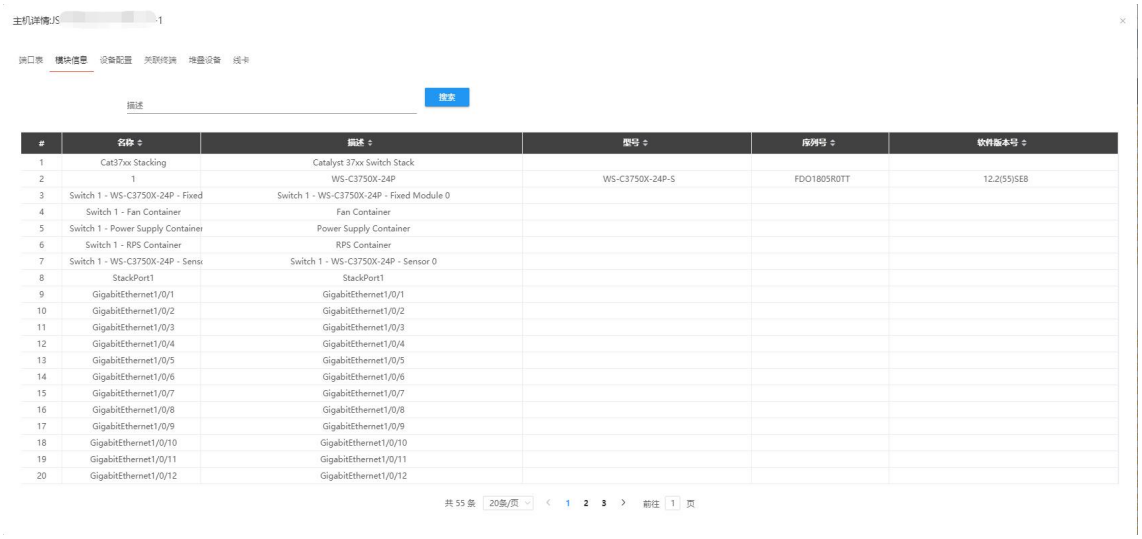


通过设备自动发现，设备入网，在线设备管理，维护中、待拆除等设备状态的管理实现了设备生命周期管理的流程闭环。目前系统可以管理的设备类型囊括了路由器、交换机、防火墙、负载均衡设备、无线控制器、无线 AP 以及其他支持 snmp 协议或是 ssh/telnet 协议的设备。通过后台扫描网络设备的管理 IP 自动更新网络设备信息。

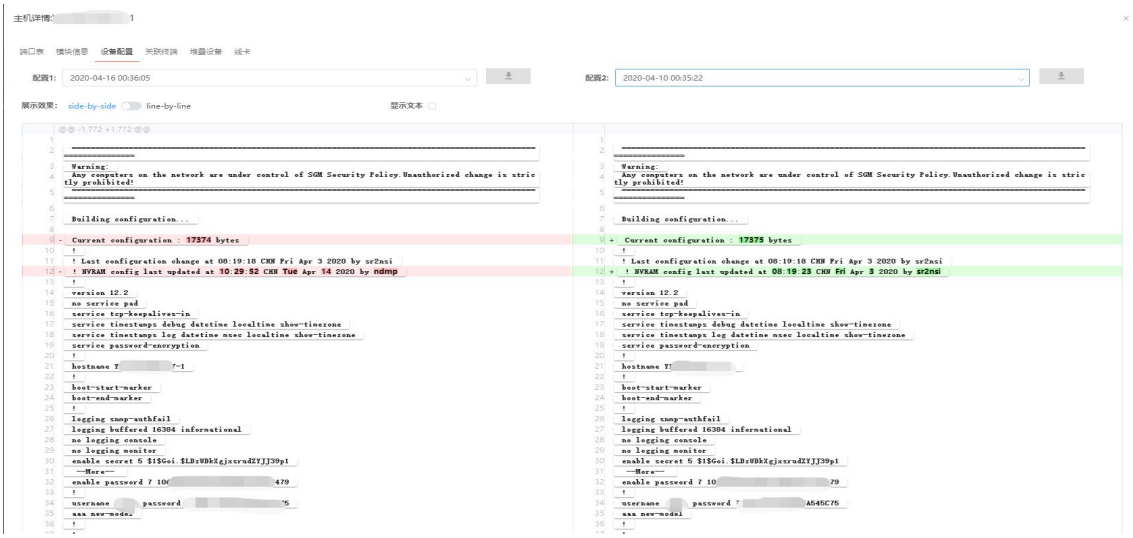
能够自动获取设备下的端口信息：



设备的模块信息：



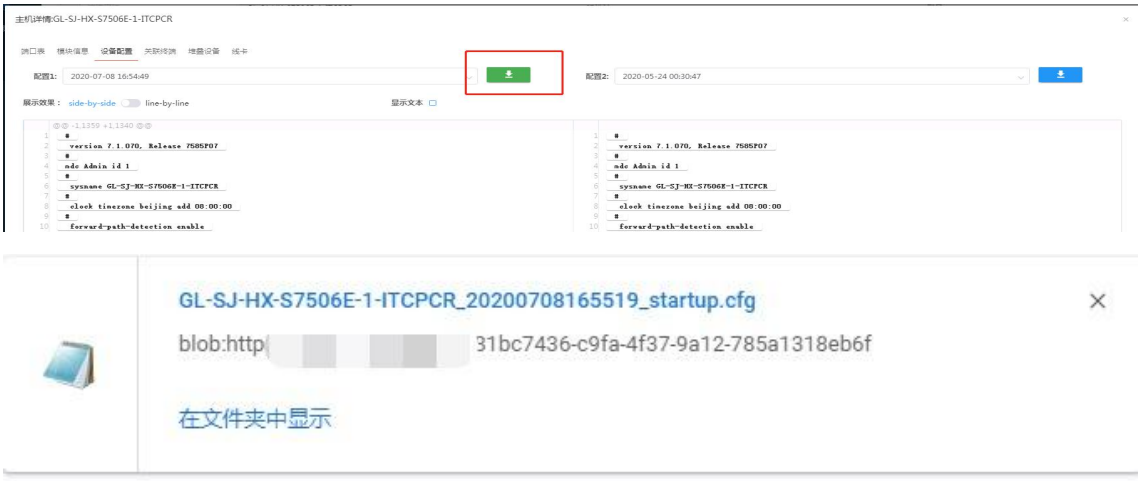
在设备管理中，我们还整合了设备配置的定时自动化备份，在设备详情的设备配置页，管理员可以选择任意时间（以天为单位）的备份版本进行浏览。不仅如此，系统还提供了不同版本间配置备份比对的能力，如下图：



如果两个版本的某行配置信息不一致，系统会以高亮的形式展示差异。差异的展示形式可以是上图的左右高亮比对，也可以是下图的合并展示：

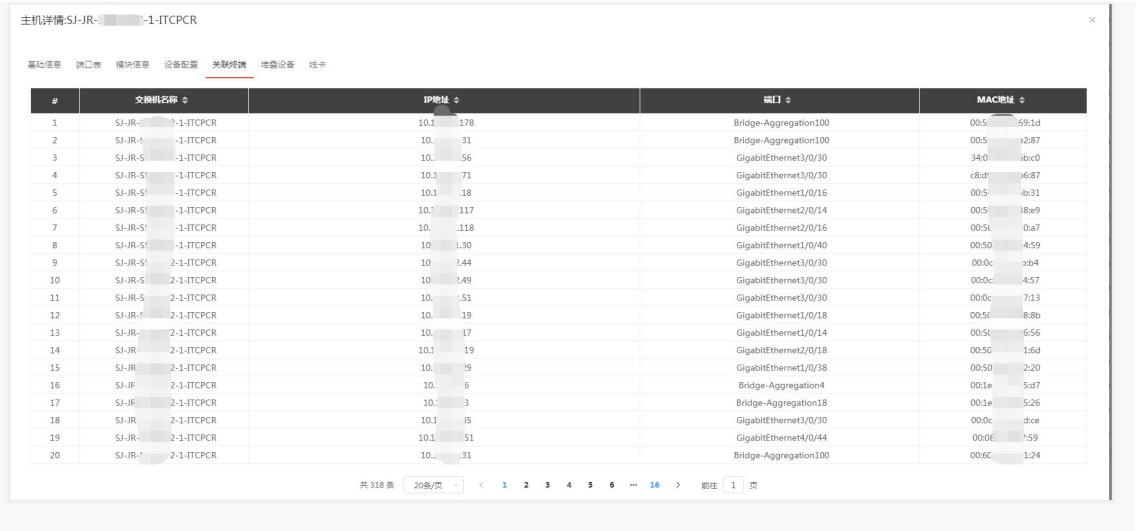
当某台设备的配置备份任务失败时，系统会在告警平台产生一条告警日志，及时通知管理员进行问题排查或处理。

如果用户选择的是 TFTP 配置文件备份的方式，系统还提供了文件下载的功能让管理员方便从配置文件服务器上拉取备份配置文件选择直接 scp 回滚：



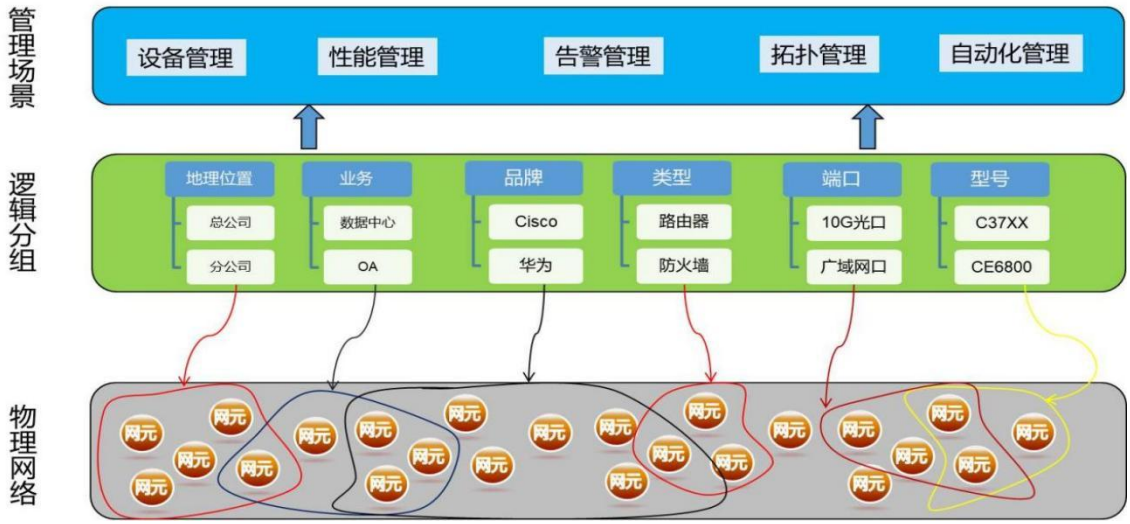
此外，如果属于接入设备，NETMANAGER 的设备“关联终端”页会展示与该接入交换机直连的服务器/终端的 IP 地址、MAC 地址及对应的物理端口。NETMANAGER 通过获取的网络拓扑

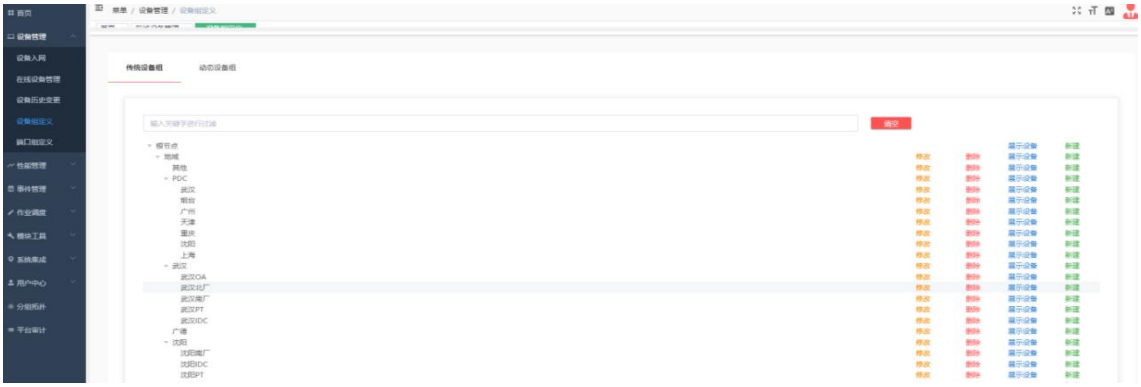
信息、各设备的 MAC 地址表及 RIP 表等信息经过一系列的算法获取接入交换机与服务器/终端的连接信息。可以帮助网络管理员快速定位与系统的关联关系，提高排障效率。



除了设备自动添加，NETMANAGER 还支持设备的手动添加，可以设置设备的权重、供电方式和资产编号等离线的资产信息。

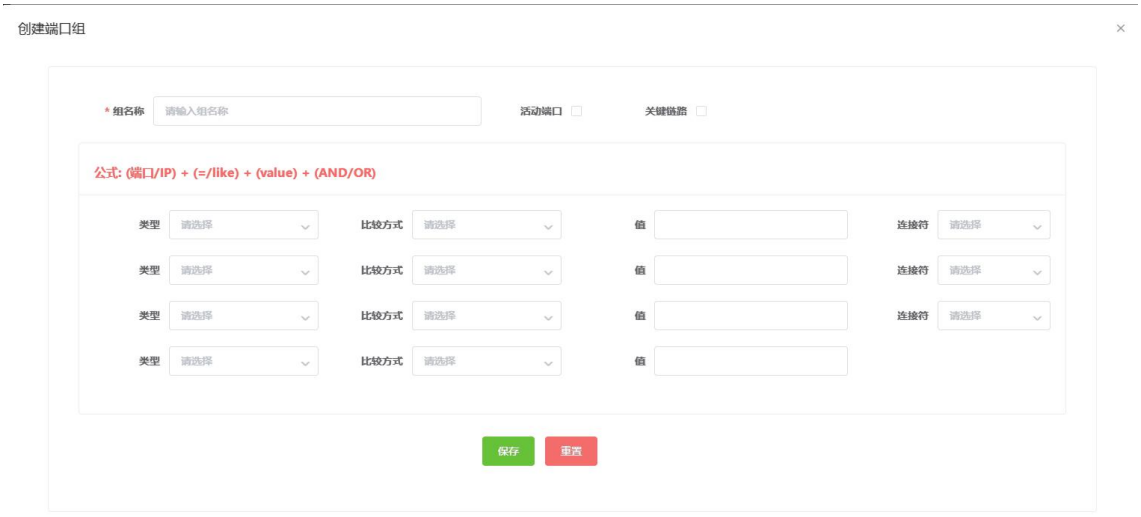
某些大型企业网络规模巨大（设备数量甚至超过万台），种类繁多（路由器、交换机、防火墙、负载均衡、无线接入设备等等），厂家众多。为方便网络运维人员对大规模数量的设备及端口进行管理，平台支持将网元节点、端口按照逻辑关系分组，易于分类分批管理，同时方便性能管理模块、自动化作业模块或报表模块等的个性化统计与展示。



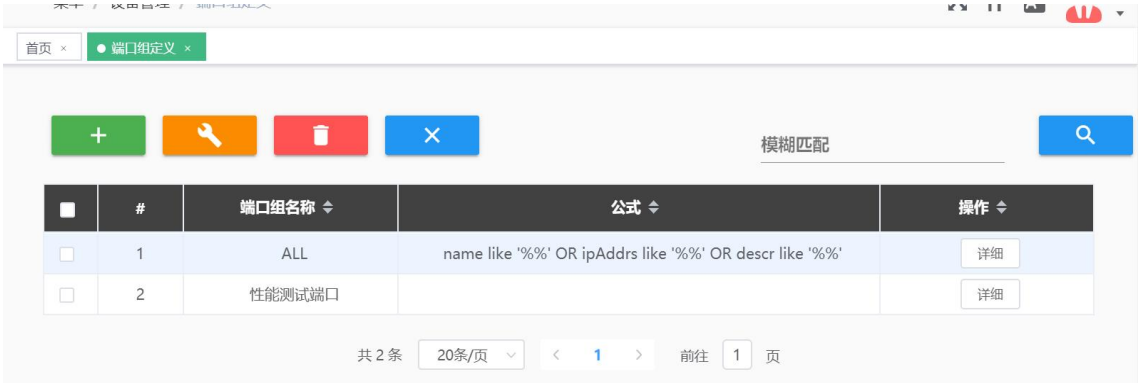


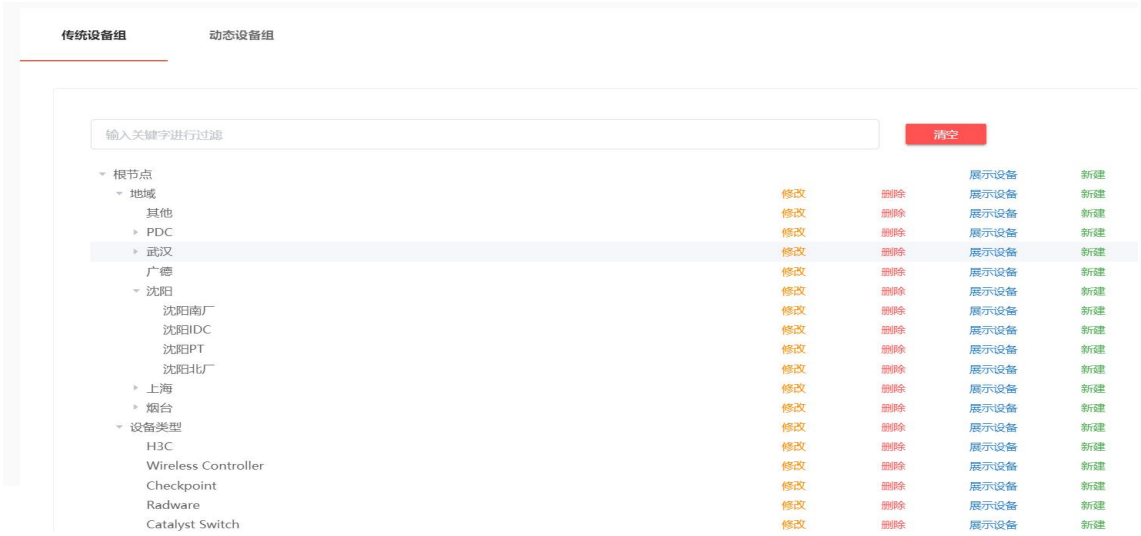
节点组新增操作如下：

端口组新增操作如下：



NETMANAGER 系统提供节点树操作，可方便查看节点组、节点、端口各层级关系，并支持在树节点上的快捷操作。





在资产管理模块，如前所述，NETMANAGER 系统通过提供和蓝鲸 CMDB 配置平台的同步接口，支持将数据同步至蓝鲸 CMDB，为在蓝鲸平台上实现更上层的运维管理闭环或统一运维管理

等需求提供网络域的配置信息。

5、网络安全设备性能管理

性能管理也是网络管理领域的重要部分。设备的运行性能及端口、链路的流量、带宽利用率、丢包、延时等等与网络各环节运行状态相关的性能数据复杂而多样。及时而全面的性能数据采集与展示是性能管理部分的关键要素。

考虑到性能数据采集的量级大，对并发以及吞吐的效率要求较高，处理中采用分布式集群 KAFKA，Kafka 集群在运行期间可以轻松地扩展或收缩（可以添加或删除代理），而不会宕机，能够以超快的速度有效地存储和检索数据。

数据库采用开源时序数据库 InfluxDB，特别适合用于处理和分析资源监控数据这种时序相关数据。而 InfluxDB 自带的各种特殊函数如求标准差，随机取样数据，统计数据变化比等，使数据统计和实时分析变得十分方便。

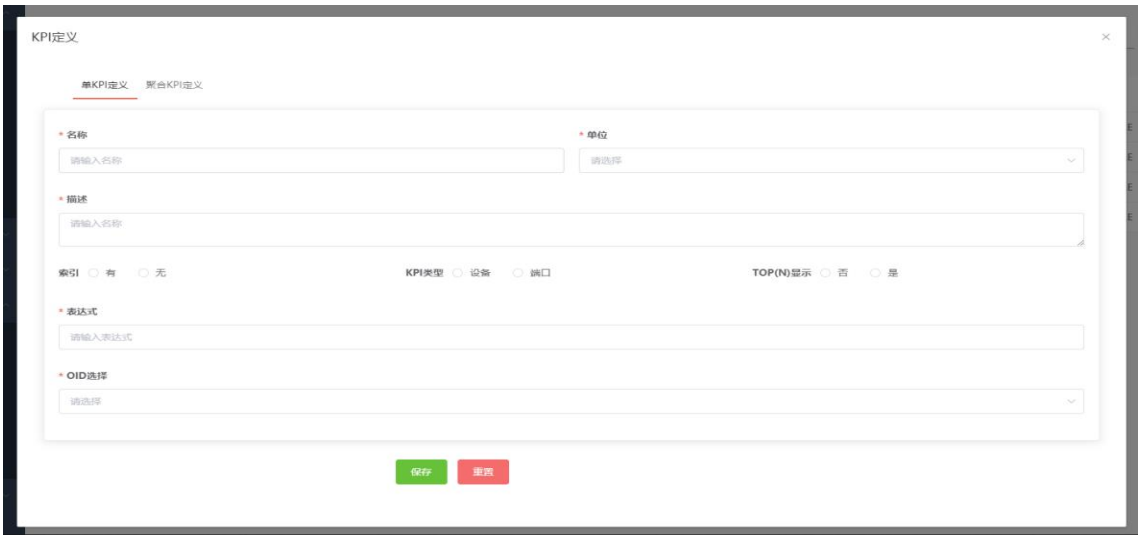
除提供了分布式高并发的数据采集支持海量设备管控外，NETMANAGER 开放的可自定义的 KPI 指标体系帮助性能指标的灵活扩展；灵活的多级性能阈值定义及告警。性能管理模块目前具备的优势有以下四点。

1. 采用分布式的性能数据采集方式，能大规模同一时间采集数以万计的性能数据，并且易于扩展。
2. KPI、采集时间间隔完全客户化自定义配置，支持 KPI 动态表达式计算，可对设定的节点组、端口组进行统一配置。
3. 使用 HTML5 技术对性能数据进行展现，支持柱状图、折线图、饼图等多种图表，并提供

RealTime 实时图表。

4. 灵活的阀值报警策略，支持二级阀值并可自定义报警消息正文。

系统中通过完全自定义的 KPI，动态表达式让网管人员能更轻松自如配置各复杂指标。

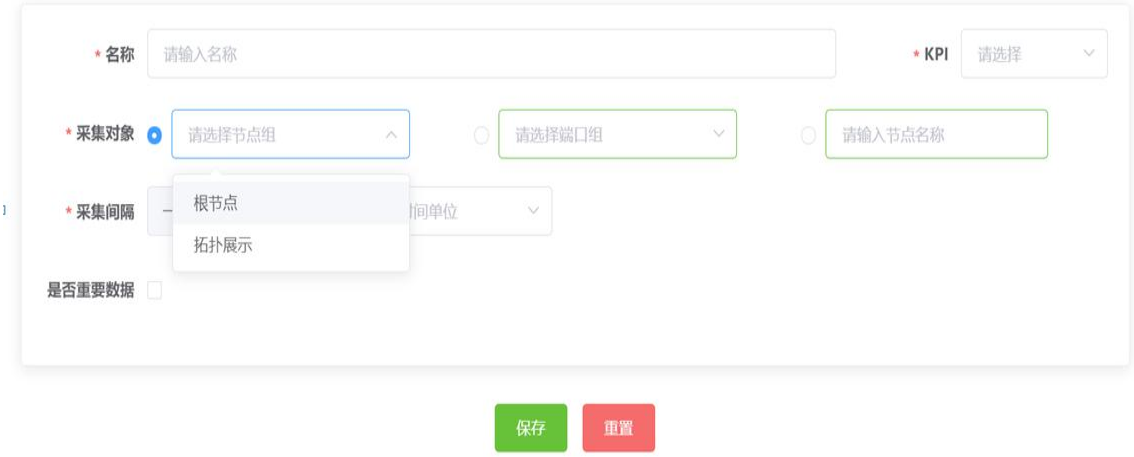


KPI 定义列表展示页面效果如图：

#	名称	描述	表达式/聚合	单位	ID	KPI类型
1	inbound	入流量	÷inbound*8	bps	1	0
2	outbound	出流量	÷outbound*8	bps	2	0
3	PortMIN	端口流量	÷inbound*8+÷outbound*8	bps	5	0
4	InPacketNum	入包数	÷InPacketNum	packet	6	0
5	OutPacketNum	出包数	÷OutPacketNum	packet	7	0
6	OutErrorPacketNum	出错包数	÷OutErrorPacketNum	packet	8	0
7	InErrorPacketNum	入错包数	÷InErrorPacketNum	packet	9	0
8	OutLossPacketNum	出丢包数	÷OutLossPacketNum	packet	10	0
9	InLossPacketNum	入丢包数	÷InLossPacketNum	packet	11	0
10	PortLossPacket	端口丢包率	((÷InLossPacketNum+÷OutLossPacke	%	12	0
11	PortErrorCode	端口误码率	((÷InErrorPacketNum+÷OutErrorPack	%	13	0
12	PortLoad	端口利用率	(÷inbound*8/$PortSetMbpsAll)*100+	%	14	0

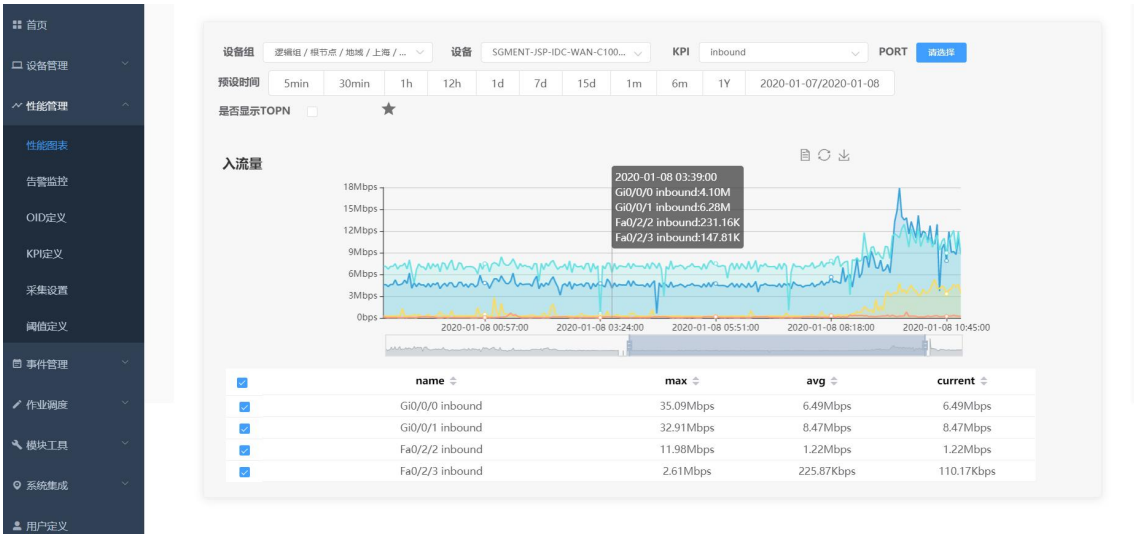
共 12 条 20条/页 1 前往 1 页

网络管理人员可根据业务需要，方便的自定义采集时间间隔，并以组的形式对节点、端口的性能数据进行采集。采集参数定义如下：



关键链路的网络质量性能视图：

也可以按照节点选择一定时间段内的流量情况：

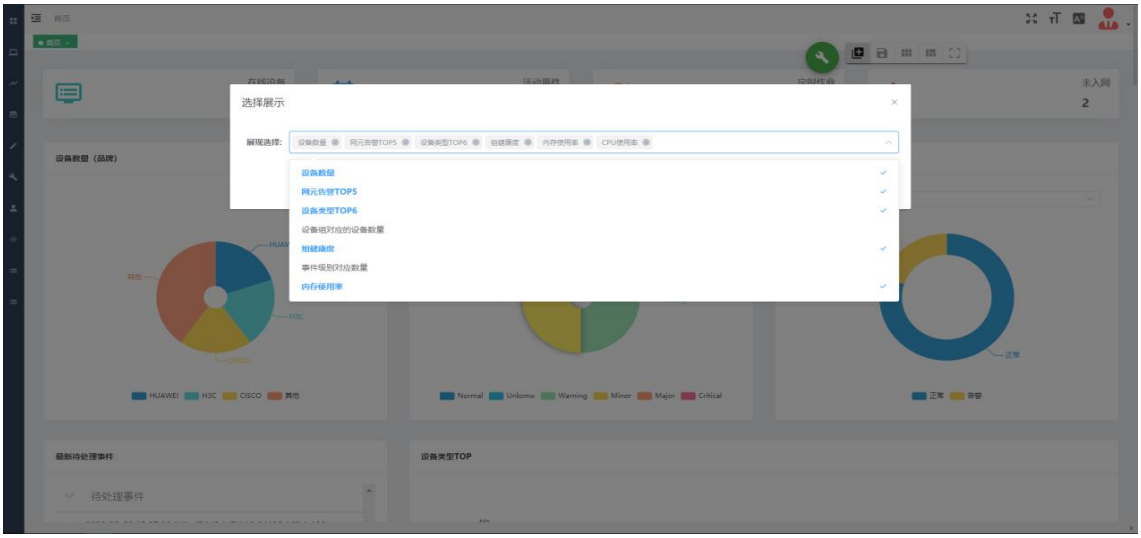


6、网络安全设备监控门户管理

为网络管理人员提供更为便捷直观的管理视图，本系统提供了可灵活定制的主页数据展示功能。如下图示例：

- 页面最上部分展示关注的汇总数据指标。如在线设备数，当前活动事件数，代办事项数，系统告警数等，每个 Tab 可以点击进入专项页面查看数据明细等详情；

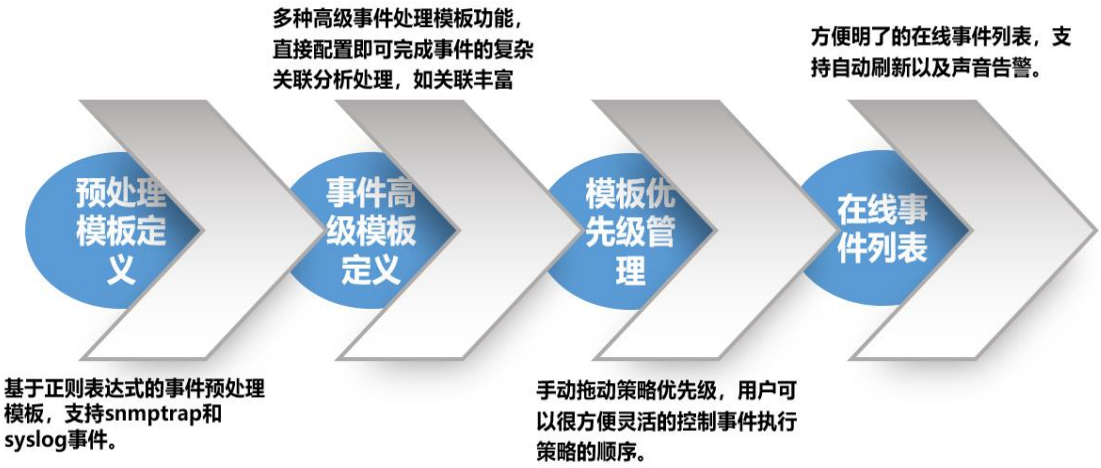
- 页面图形展示区域可以由管理员自行定义，这里分四个区域展示了关键端口流量，按客户的流量及占比排名图形。这两个是在性能管理模块里定义好性能监控组合后直接在页面选择加入 Portal 主页即可生效。资产占用汇总图在统计报表模板中选择加入 Portal 主页；待处理事项列表在流程管理页面定义选择加入 Portal 主页。



7、设备事件告警管理

告警事件处理是网络管理中几乎最为重要的工作。告警的准确性、及时性直接影响

到网络管理的效率和用户服务水平。简单来说，告警事件处理需要做到不错报，不漏报，及时报。对于告警事件的产生判断流程如下图所示：



告警处理流程示意图

网络告警事件的数据来源有四个方面：

- 网络设备的 Syslog，
- 网络设备主动上报的 SnmpTrap，
- 网管平台主动发起的 ICMP 报文检测连通性反馈，
- 性能 KPI 触发了阈值产生的健康度告警

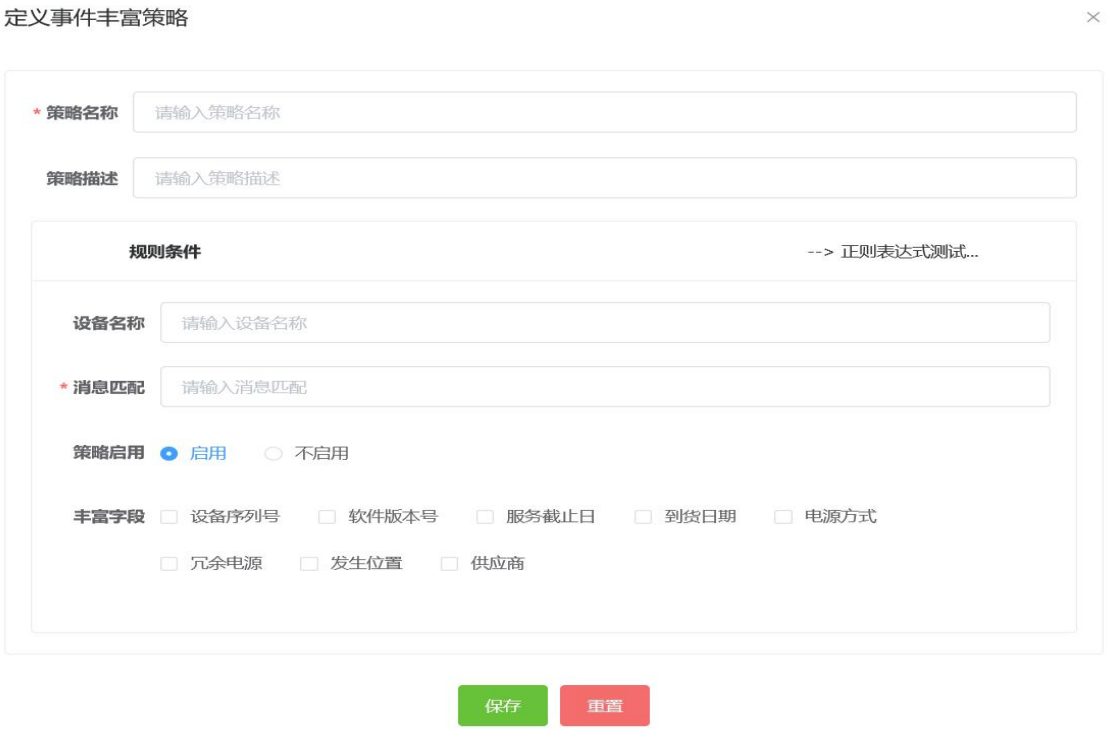
对于前两种来源产生的原始数据，事件处理平台通过预处理模板定义对原始的 Syslog 和 SNMPTrap 执行过滤策略，格式化策略。

事件过滤：如果不是用户关心的事件或不能通过事件过滤器，则该事件会被丢弃，从而节省大量的处理时间和存储空间。用户可在管理控制台上建立过滤规则、修改过滤规则以及删除过滤规则等。

#	模板名称	关联组	描述	设备名称匹配	消息匹配	消息正文	对冲类型
1	Minor	根节点	minor *-1-2-3	.*	%(.*)-([1|2|3])-(.*):(.*)		DOWN
2	Warning	根节点	warning *-4-5	.*	%(.*)-([4|5])-(.*):(.*)		DOWN
3	Normal	根节点	Normal -6|7	.*	%(.*)-([6|7])-(.*):(.*)		DOWN
4	RPS FAIL	根节点	RPS FAIL	.*	%(.*)PLATFORM_ENV-1-PWR_RPS		DOWN
5	DROP_ASA-5	根节点	DROP_ASA-5	.*	ASA-5.*		DOWN
6	DROP_ASA-4-1061	根节点	DROP_ASA-4-1061	.*	ASA-4.*		DOWN
7	DROP_ILPOWER-5	根节点	DROP_ILPOWER-5	.*	ILPOWER-5.*		DOWN
8	DROP_ETHPORT-5-	根节点	DROP_ETHPORT-5-	.*	ETHPORT-5.*		DOWN
9	Drop_10.203.252.16	根节点		10.203.252.161	.*		DOWN
10	Drop_10.127.0.97	根节点	Drop_10.127.0.97	10.127.0.97	.*		DOWN
11	denied udp	根节点	denied udp		.*denied udp.*		DOWN

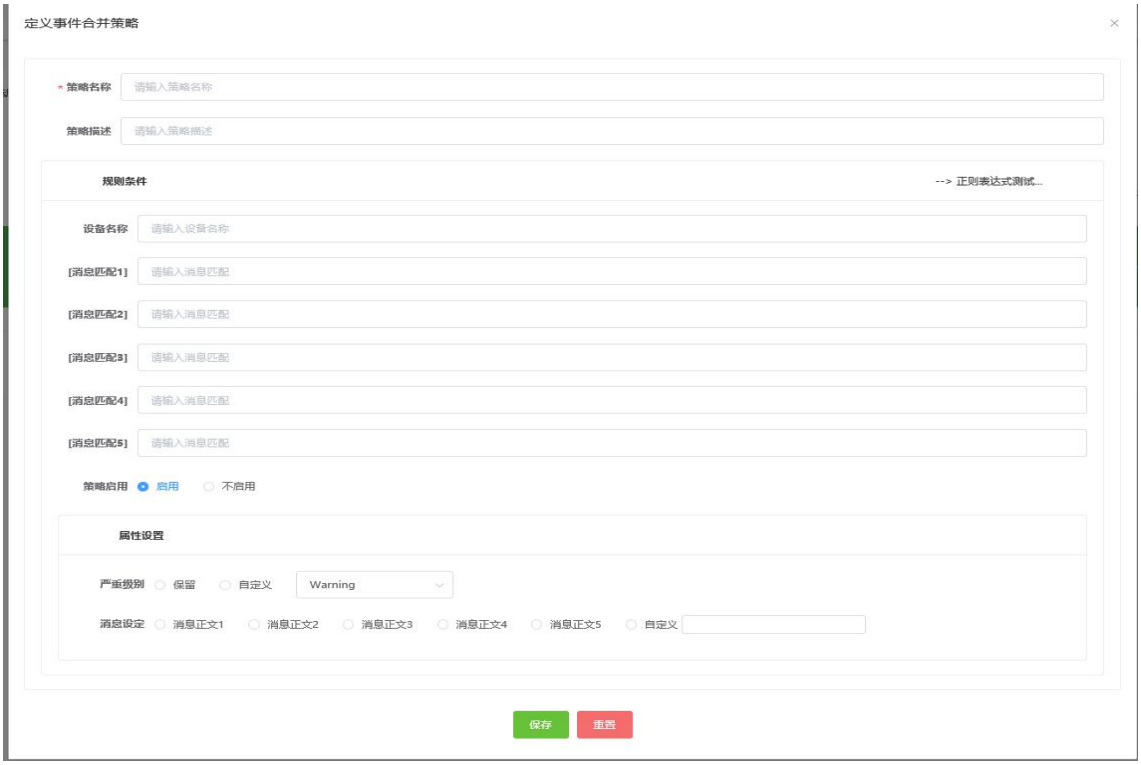
事件匹配处理规则列表

事件管理平台具有丰富事件管理功能，可自定义将 CMDB 属性字段与告警事件进行关联，为后续高级的事件处理策略提供关联信息。



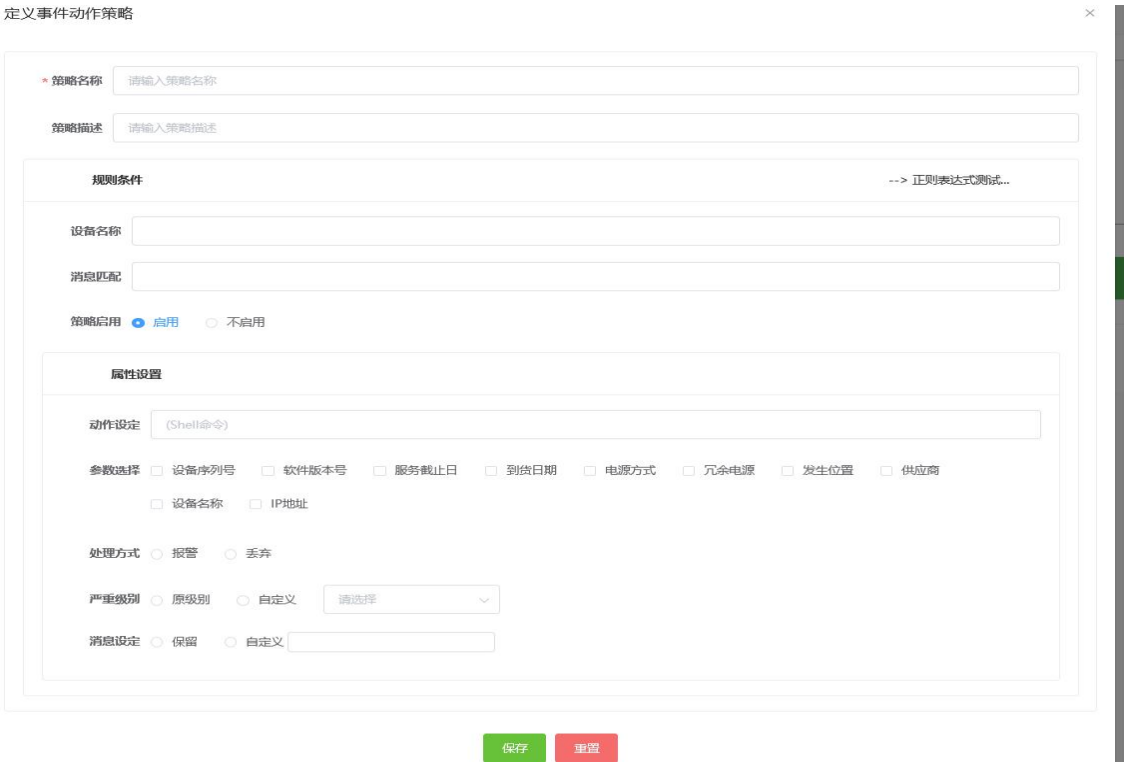
事件丰富策略表单

规则化处理：在该阶段确定同一事件是否已发生多次、是否是重复事件、重复事件发生多少次才可以进入下一个处理过程、事件优先级别设定等。



事件合并/收敛策略表单

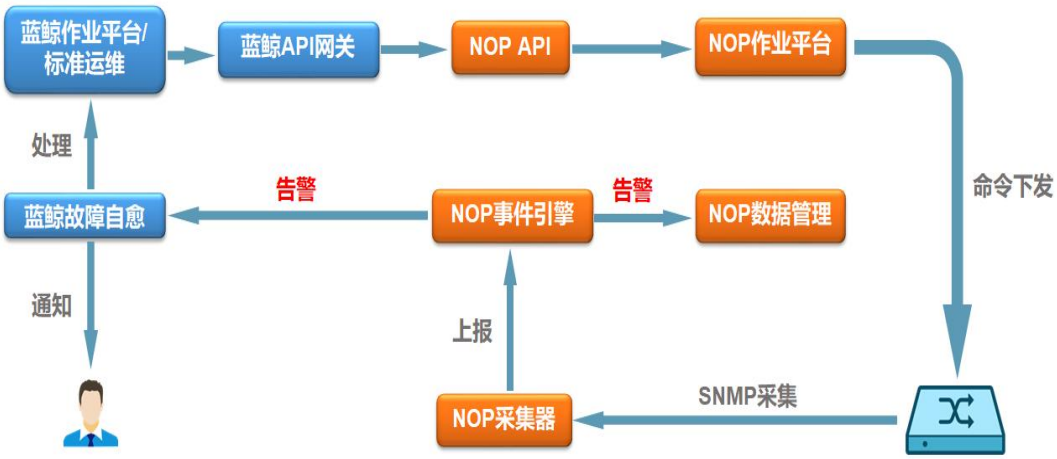
动作策略：对应该事件是否有告警级别调整，或驱动外部程序动作与外系统做相应关联。



事件动作策略表单

NETMANAGER 平台已经预先包含有关联逻辑的模版，对于最常见的关联逻辑都可以在这些模版上作适当的修改快速实现，为关联逻辑的开发、调整、部署提供了基础。可以丰富增加额外的事件属性，对重复事件进行处理，压缩满足某种条件的事件等。除了上述预先定义的关联模版，用户还能够通过用户关联定义模版配置自己的关联逻辑。

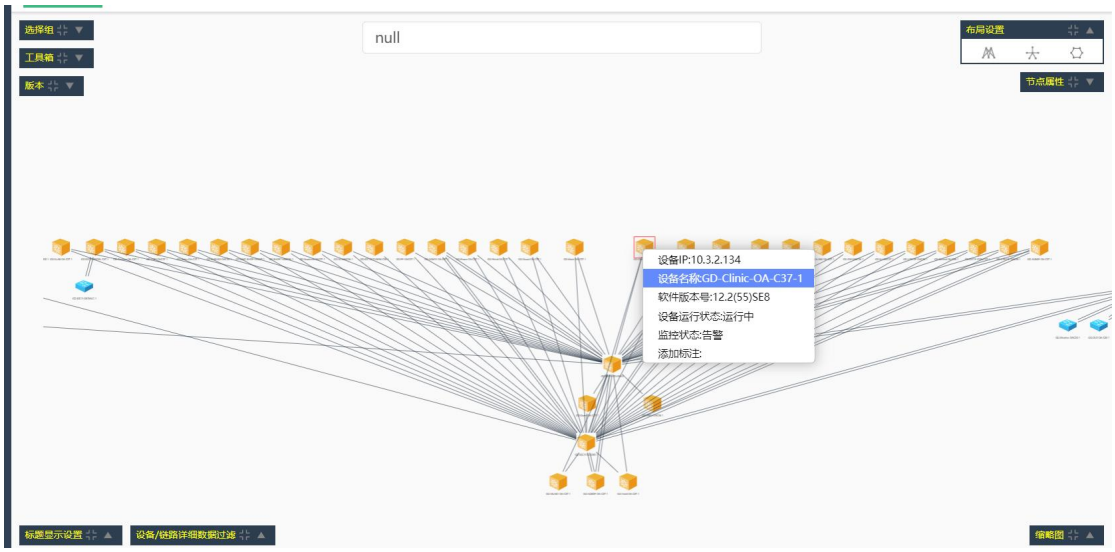
NETMANAGER 产生的事件告警可以作为故障信息主动推送给蓝鲸的故障自愈。管理员可在故障自愈中定义故障排查判断树，并通过标准运维调用 NETMANAGER 作业原子帮助快速定位故障根源，并可最终执行适当的指令恢复故障。具体集成流程如下图所示：



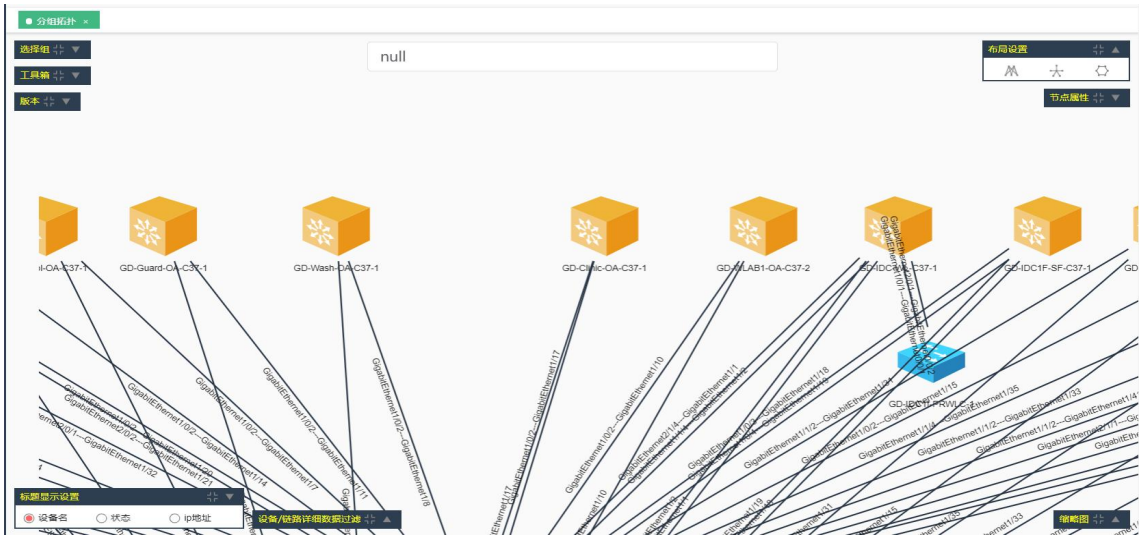
8、网络安全设备拓扑管理

网络设备间的链路关系可以直观地反应网络的拓扑架构。通过 CDP、LLDP 协议自动发现网络设备间的链路层关系并能直观简洁地绘制出来会帮助网络管理人员快速定位设备在网络中的位置，了解设备间的互连关系；通过拓扑图上的实时告警展示快速定位网络故障根源。

NETMANAGER 提供了基于 CDP、LLDP 的链路自动发现功能，并通过 2D/3D 引擎自动绘制网络拓扑结构，结合内置的网络布局算法提供多种视角的网络布局展示。管理员也可以通过拖拽的方式调整设备布局来更吻合自己的管理视角，并保持调整结果。如下图所示：

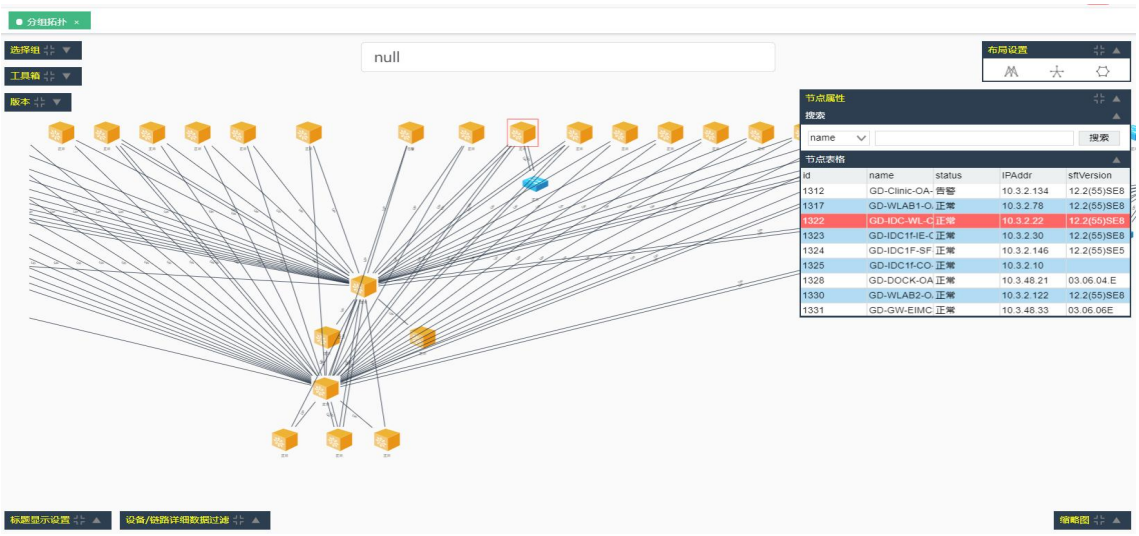


通过将鼠标移至设备可显示设备的基本配置信息及状态概要。

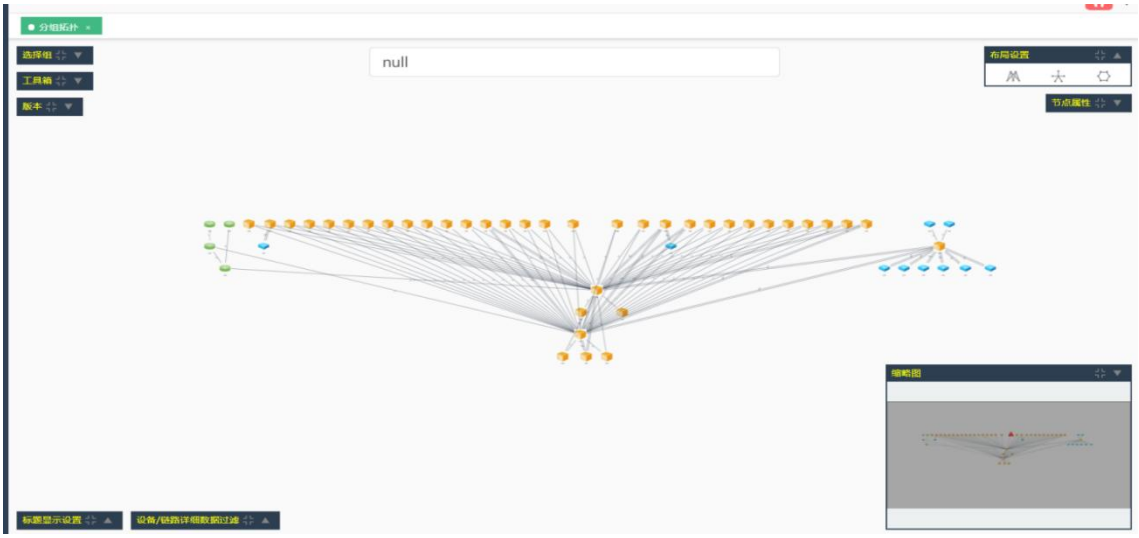


通过将鼠标移至链路可显示链路的基本配置信息及状态概要。

根据管理员的管理需要，设备标签的显示信息也可在“节点名”、“设备名”、“状态”、“IP 地址”间进行切换。



当网络中设备数量庞大的情况下，管理员可通过快速检索窗口通过设备名称的模糊检索快速定位设备或链路。



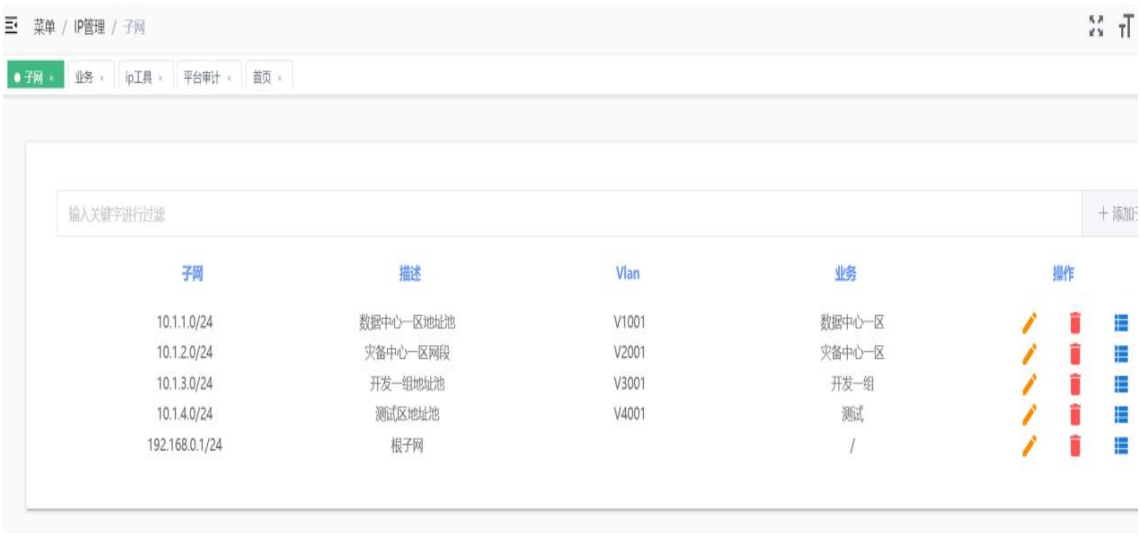
当网络规模庞大的时候，NETMANAGER 还可支持逻辑分组展示管理员关心的局部网络拓扑，并在右下角的全局缩略图中显示局部拓扑在整个网络结构中的位置。

9、网络安全设备 IP 地址管理

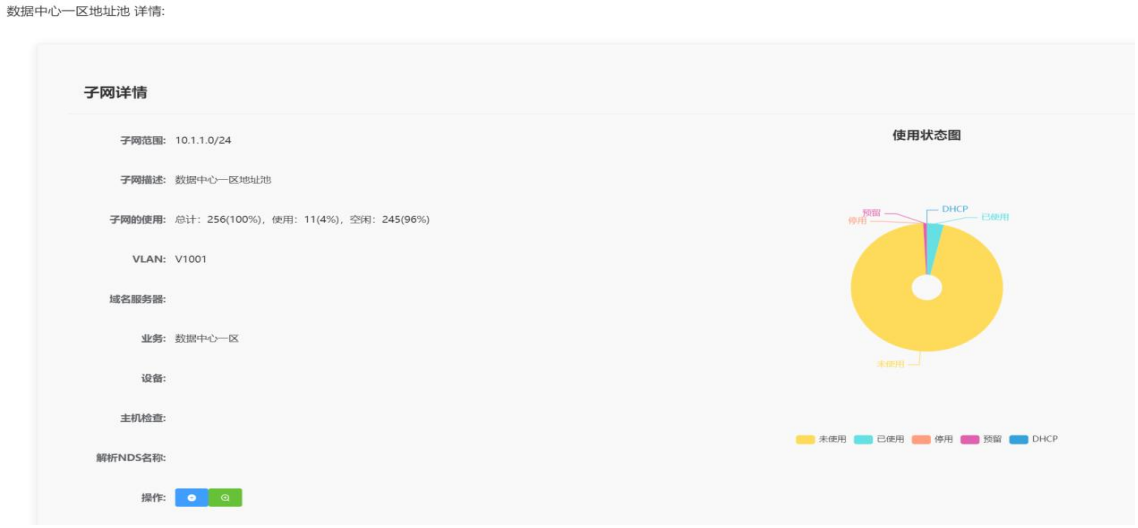
IP 地址资源是企业网络资源的重要组成部分。合理的网络地址规划及对 IP 地址使用情况的搜集与管理也是网络管理中必不可少的环节。

NETMANAGER 的 IP 地址管理模块允许管理员按照业务维度定义业务名称及相关联的属性信息。

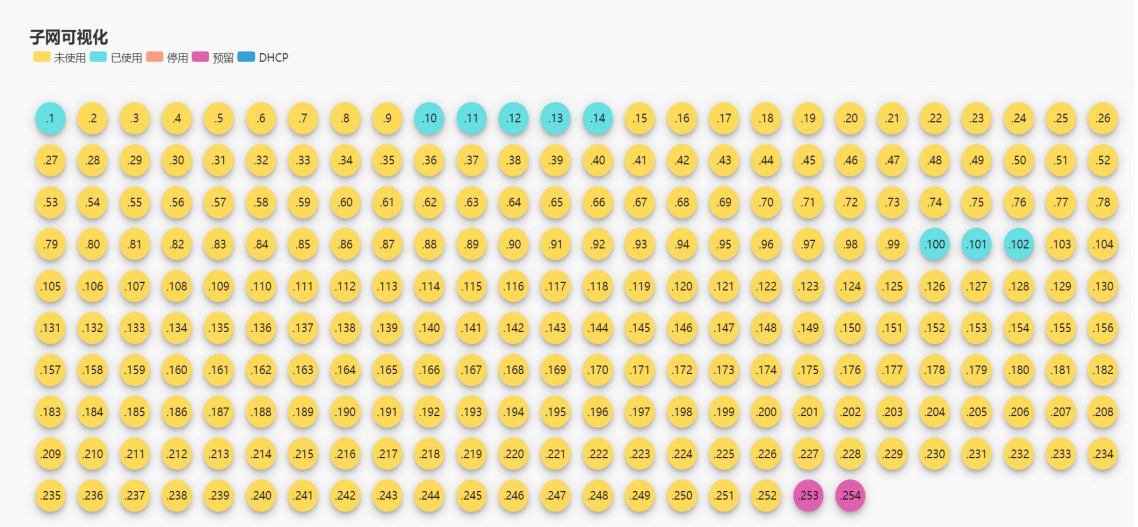
再通过规划的子网与定义的业务相关联。



展开每个子网可以展现该网段对应的分配详情。



进一步展开可显示子网内各 IP 地址的具体分配情况。



结合 NETMANAGER 平台的自动发现和自动采集以及拓扑发现、关联终端等算法自动获取的 IP 地址使得 IP 地址占用情况的数据基本通过自动化维护实现。大大减轻了网络管理人员

的维护工作量。

10、网络安全设备流量分析

NETMANAGER 的流量分析模块通过网络设备所支持的 NetFlow/SFlow/NetStream 协议收集指定设备端口的通信数据流，分析 IP 数据包的二-四层属性，快速区分网络中传送的各种不同类型业务的数据流。通过单独跟踪和准确计量，记录其传送方向和目的地等流向特性，统计其起始和结束时间、服务类型、包含的数据包数量和字节数量等流量信息。主要通过 IP 数据包的以下 7 个属性来实现：

a）源 IP 地址；

b）目标 IP 地址；

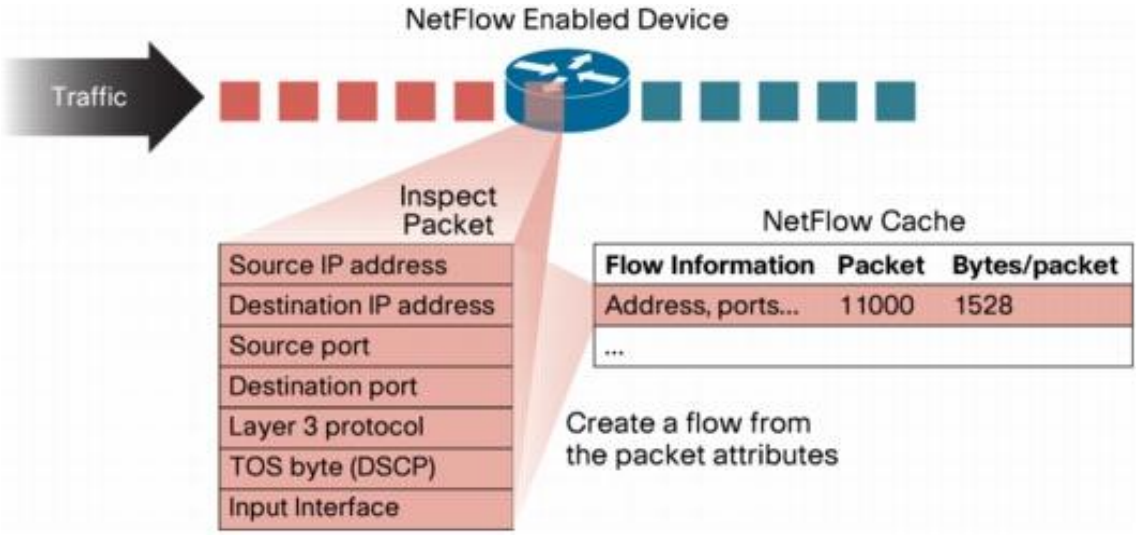
c）源通信端口号；

d）目标通信端口号；

e）第三层协议类型；

f）服务类型（TOS）字节；

g）网络设备输入或输出的逻辑网络端口（iflndex）。

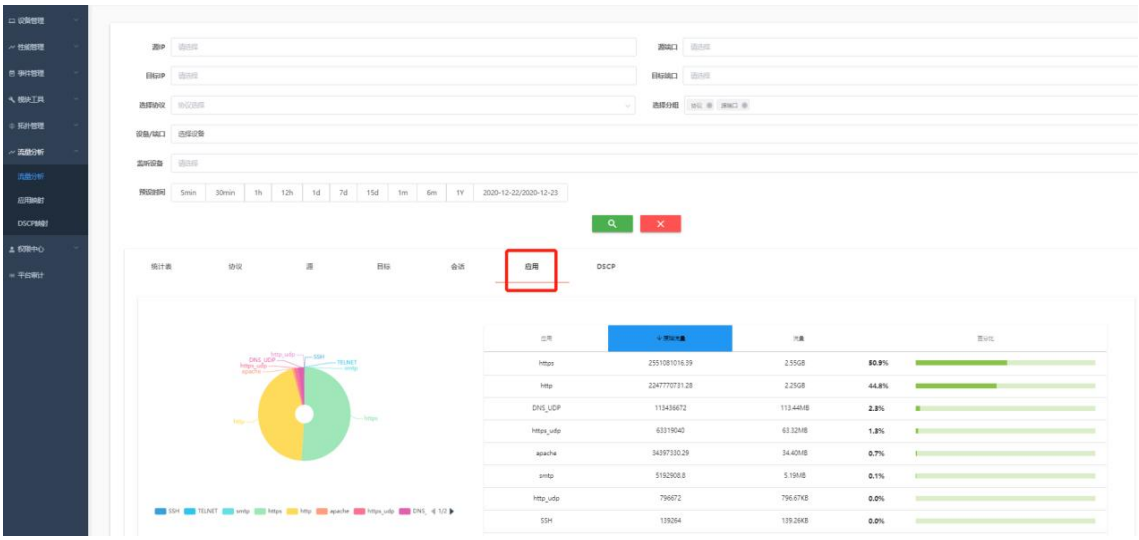


相对于镜像分流或物理探针式采集数据流进行分析的方案，NETMANAGER 的流量分析模块给用户提供了一个廉价、灵活且可快速部署的 IP 数据流量分析的选择。通过流量分析模块获取的数据，可以帮助网络管理员快速定位网络攻击异常；统计分析应用的流量占比；为 QoS 策略提供数据依据并监控实施效果等等。

根据不同厂家支持的协议，目前 NETMANAGER 支持的协议格式种类及厂家列表如下：

设备/厂家	Flow 格式
Cisco,3COM, RiverBed, Exteme Networks, Palo Alto,BroCade, Fortinet, F5	NetFlow
Huwaei,H3C	Netstream
Huawei，H3C	sFlow

NETMANAGER 将收集来的流量数据统一存放在 InfluxDB 数据库中，让管理员按照 7 元素的不同组合结合时间维度查询流量统计数据。同时，为管理员预置了常用的汇总统计排名场景。如按通信协议查询流量占比；按源 IP 地址查询流量占比及排名；按目的 IP 地址查询流量占比及排名;按应用查询流量占比及排名;按会话查询流量占比及排名;按服务类型(DSCP)查询流量占比及排名等等。



11、网络安全设备自动化管理

网络运维中会涉及大量如配置比对、下发配置、状态巡检等对设备的批量操作。很多操作还需定期执行。这些操作既费时又容易出错。为此，一个自动化下发命令脚本并对输出结果进行检查或处理，同时还能管理这些脚本的平台成为网络运维中必不可少的内容。

NETMANAGER 设计的网络自动化作业平台可以让管理员自定义作业执行网络配置的批量操作。对复杂的任务可以分解成若干作业步骤顺序执行。作业执行时可灵活选择节点或

配置平台预先定义好的节点组。

下面我们以一个案例来阐述作业平台的具体工作形式。

案例：用户业务访问控制案例演示

- 配置说明：为每一组共性用户配置一个 user-group，并创建策略，在策略视图下针对不同类型的用户关联不同的动作，从而实现不同类型用户业务的访问需求。
- 规范要求：

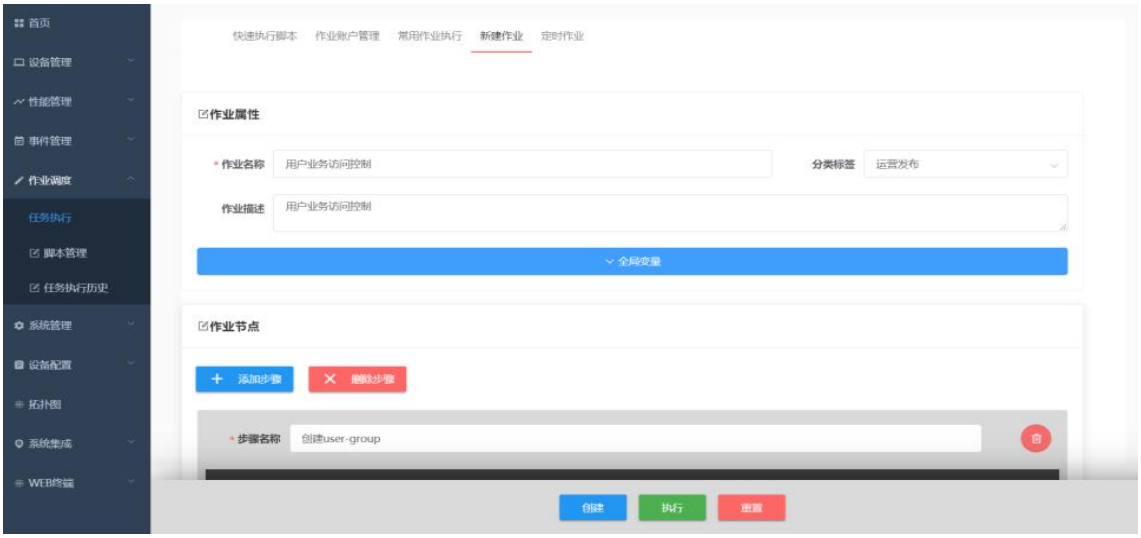
  创建 user-group，创建 acl，起始 rule 为 10，步长为 10，在 acl 中设置 sourc 绑定 user-group，即源地址为 user-group 所应用的 domain 中所有用户。

  创建 classifier，匹配 acl，并创建 behavior，制定动作。

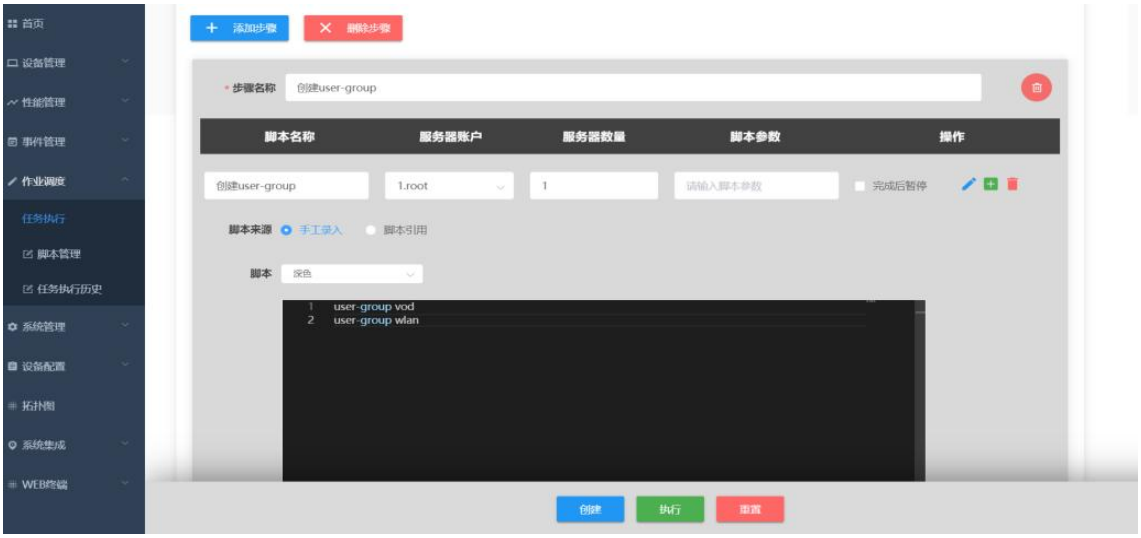
  创建 policy，将业务流和动作关联，并在全局下应用。

操作步骤详解：

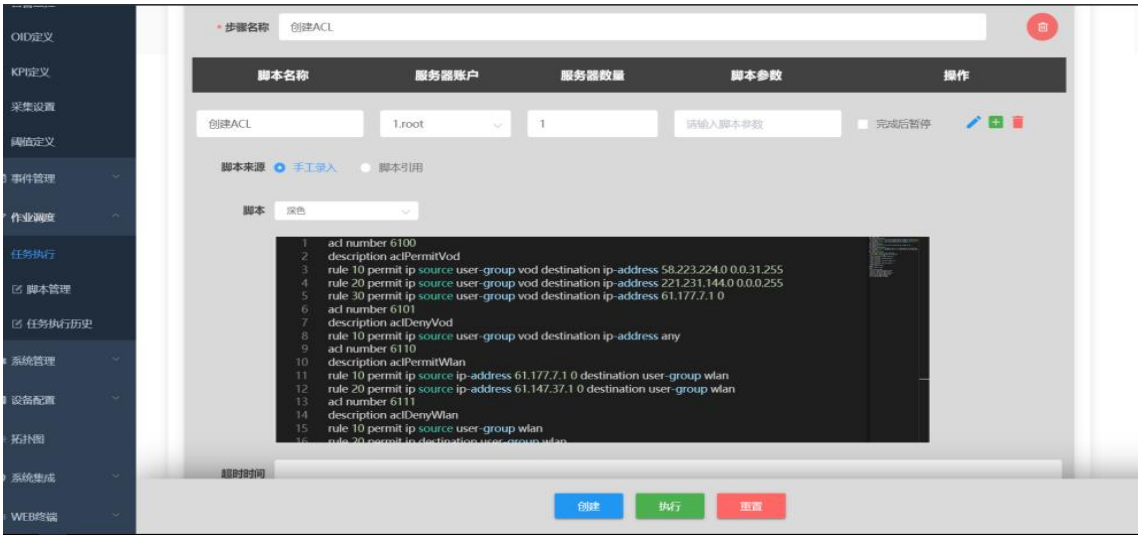
- 在作业调度页面新建作业，填写业务名称等基本信息



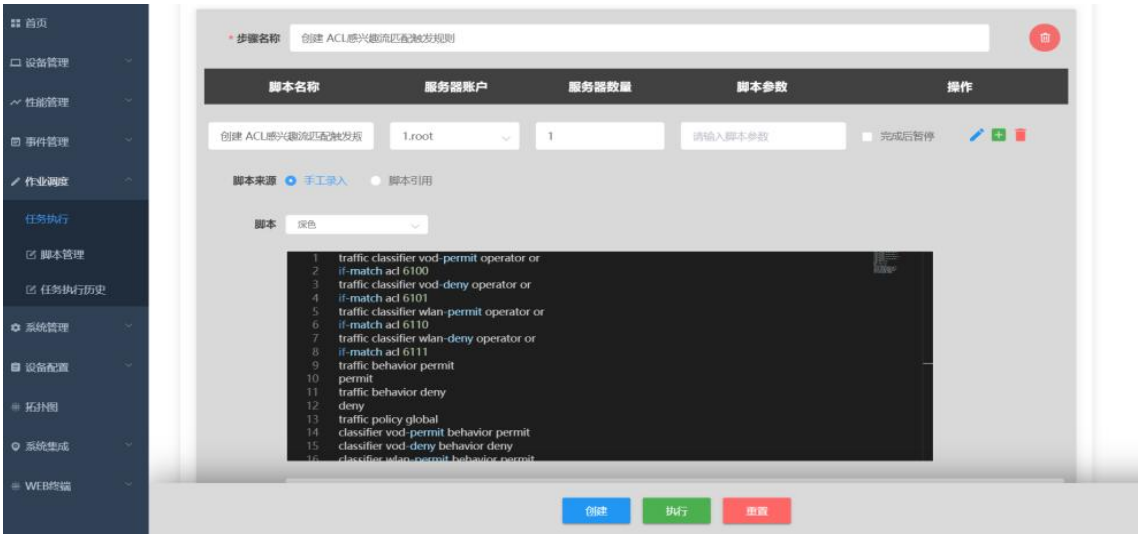
- 根据业务需求编写创建用户组脚本



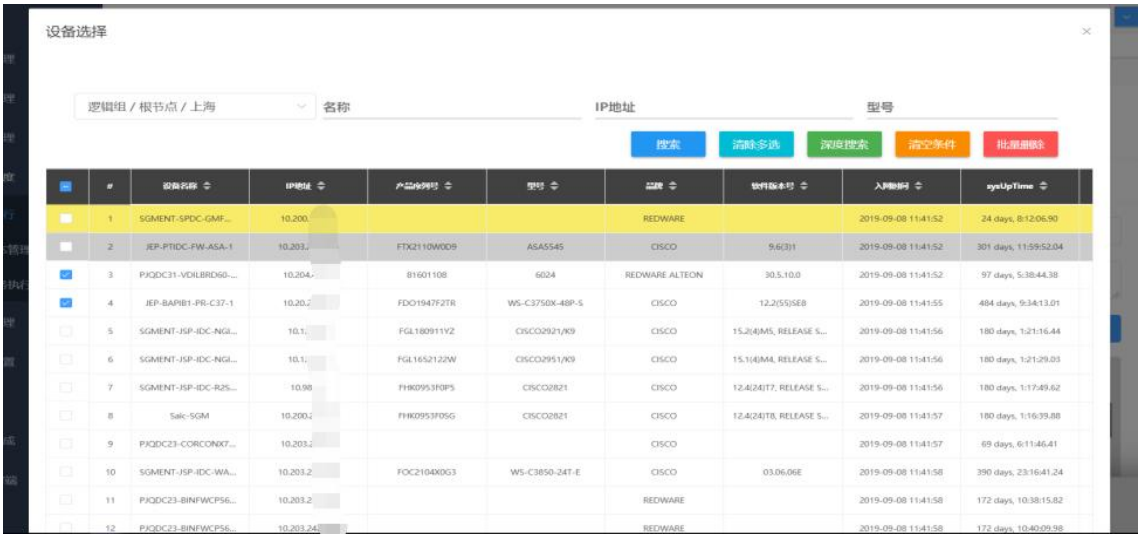
- 根据业务需求编写 ACL 创建脚本



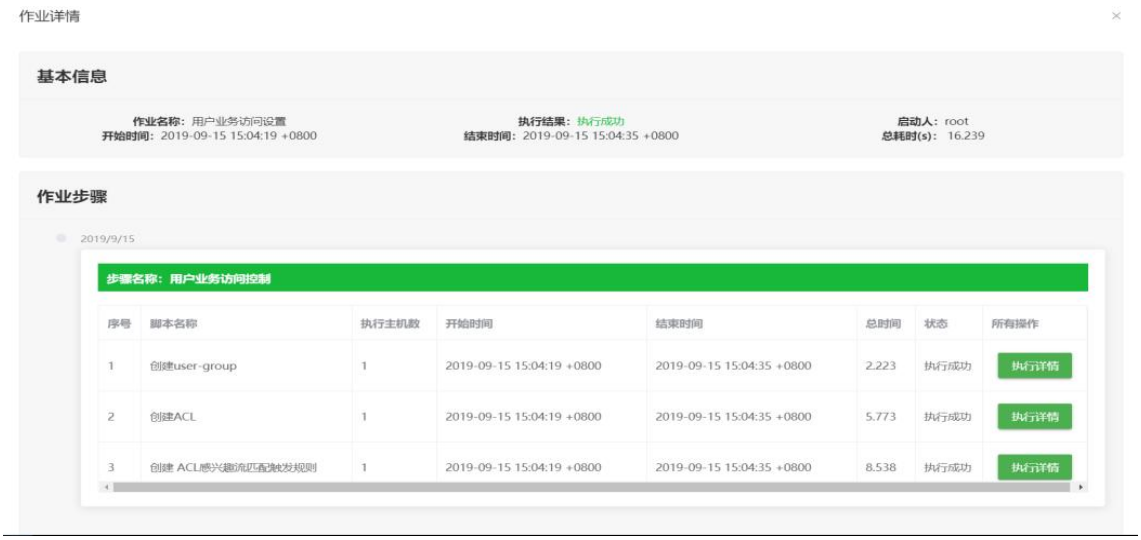
- 根据业务场景编写业务感兴趣流和动作关联脚本



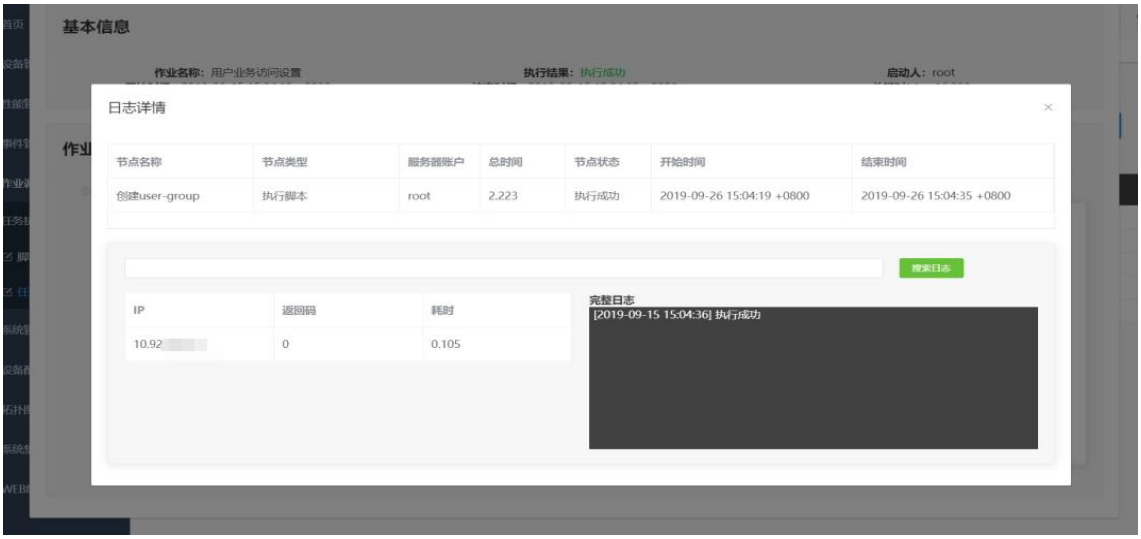
- 作业编写完成后选择需要操作的网元设备或者设备组下发作业执行操作



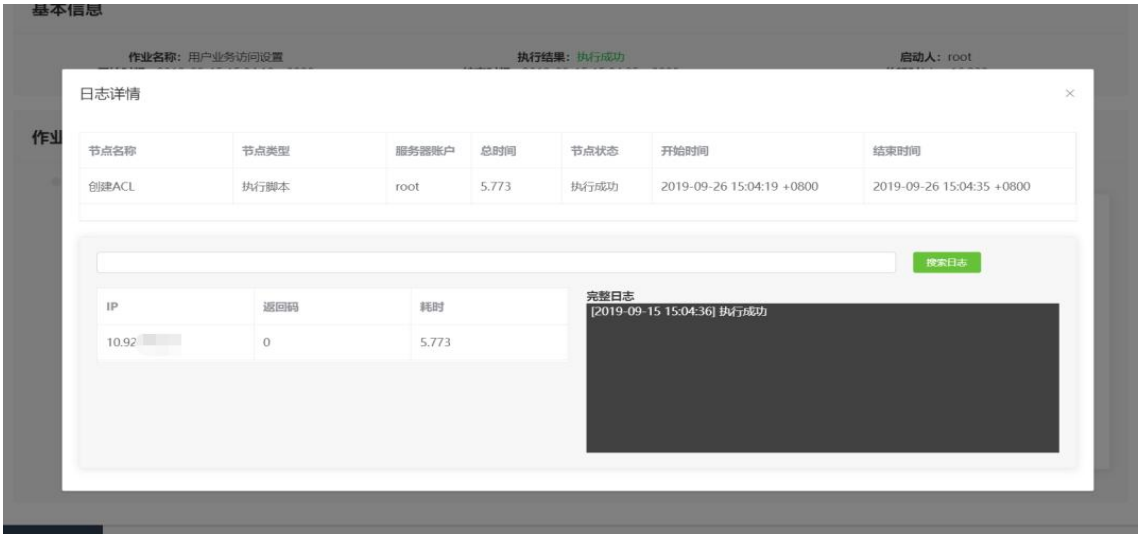
- 设备或者设备组选择好后，便可以执行该作业，完成自动化网络设备变更配置，作业执行完成后可以查看作业执行结果反馈，以便判断作业是否执行成功



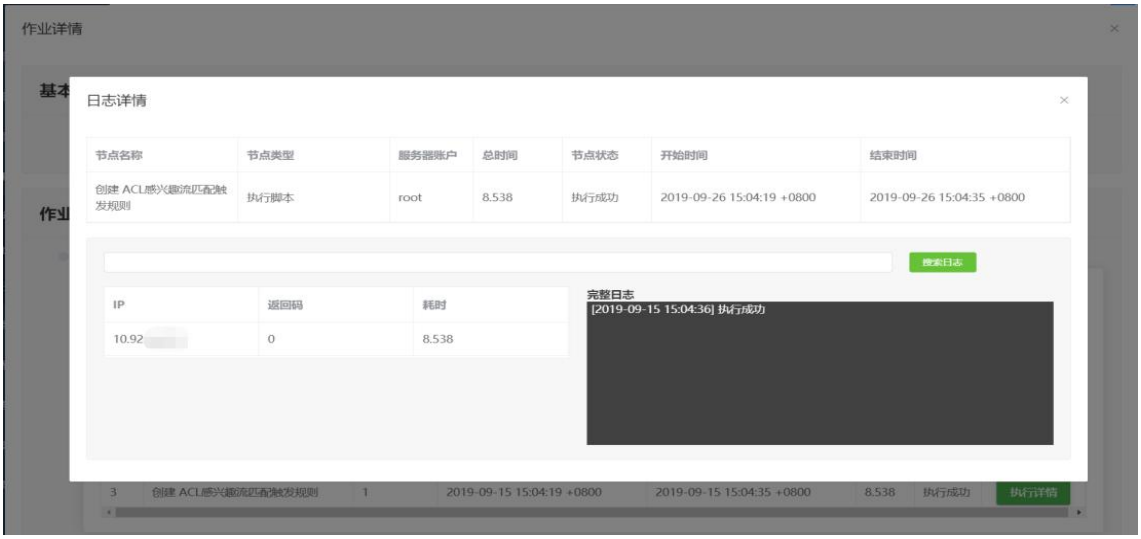
点开执行详情可以查看作业中每个脚本执行的返回状态，和执行耗时



脚本 1 执行详情



脚本 2 执行详情

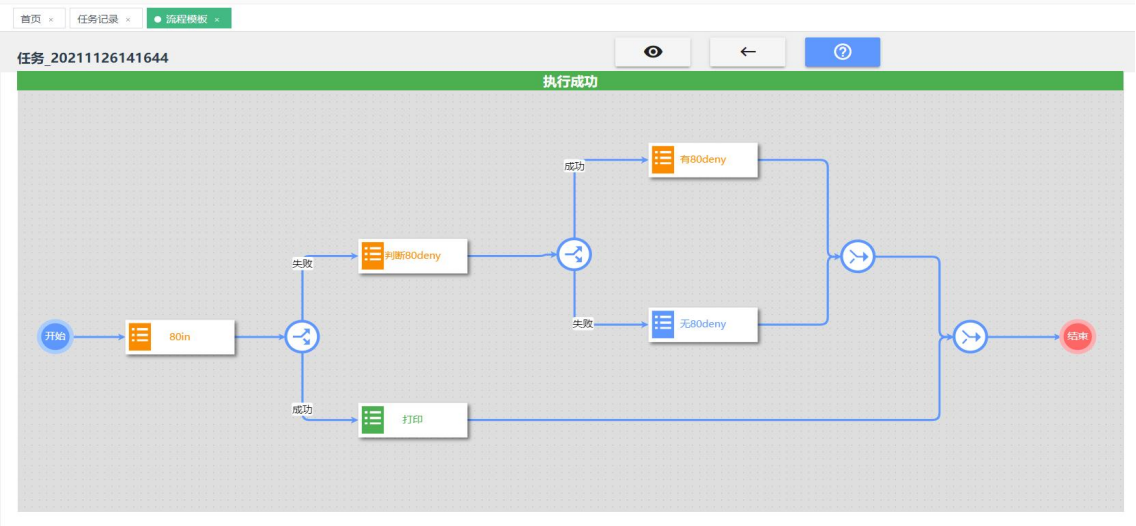


脚本 3 执行详情

通过作业平台脚本批量执行可以大大减少管理员的重复工作量并减少人为出错概率以提高工作效率。

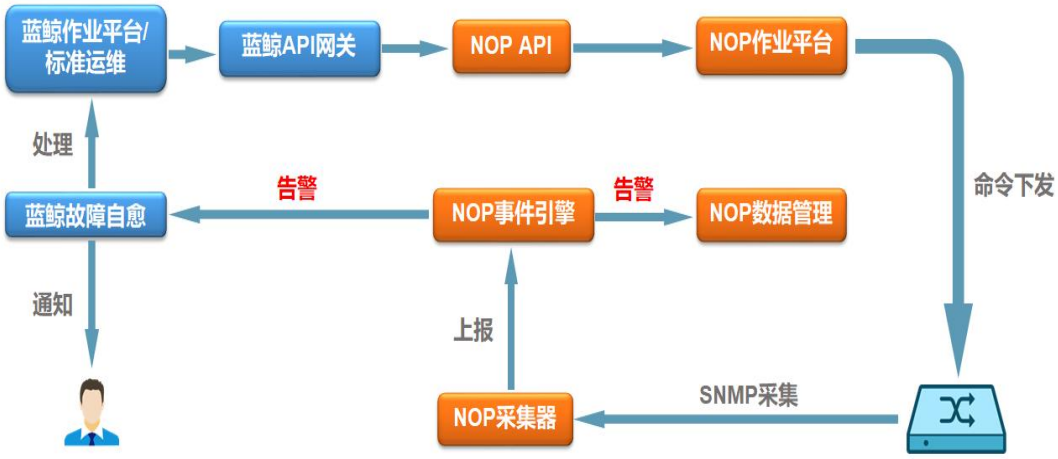
经过众多客户场景的积累，我们已有覆盖 Cisco、H3C、华为等品牌的典型日常巡检场景作业脚本；常用的 SNMP、ACL 等配置变更的批量操作脚本等。

对于需要进行条件判断及分支处理的自动化场景，NETMANAGER 还设计了【流程编排】功能模块，让管理员以作业平台的自动化作业作为动作原子，通过流程编排功能组合出更为复杂的自动化网络运维操作。例如，基于已有的 ACL 配置信息来批量增加新的访问控制策略的运维场景。

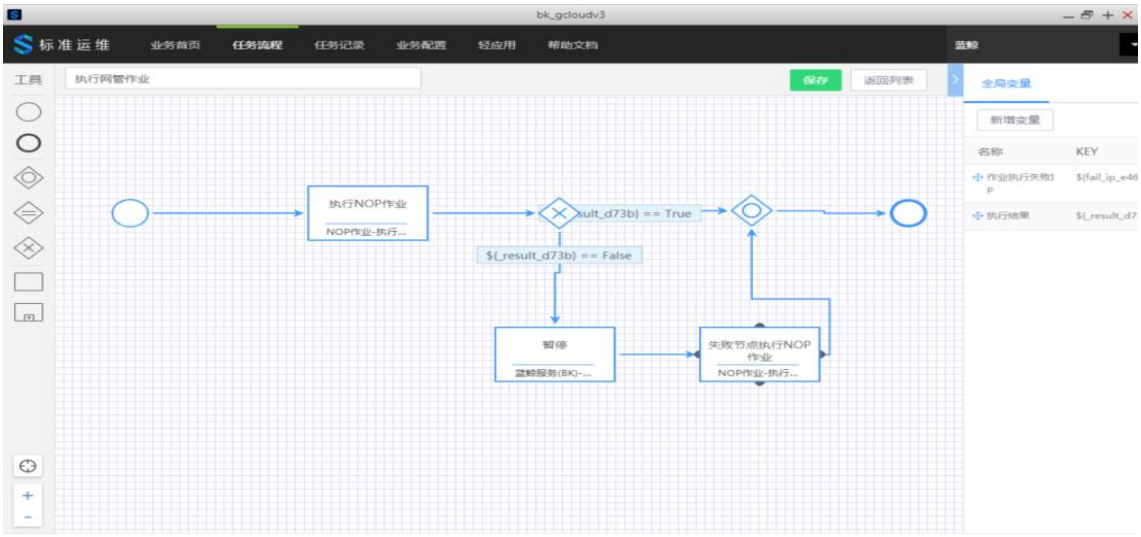


如上图所示，执行的过程可以实时展示，每个执行环境的结果也可以下钻追溯。

对于更为复杂的自动化运维操作场景或为应用运维团队提供网络标准化服务，可结合蓝鲸平台的标准运维，将网络作业原子化实现在标准运维中编排涉及网络操作的任务，或在故障自愈中实现网络设备故障告警与故障处理流程化自动处理。

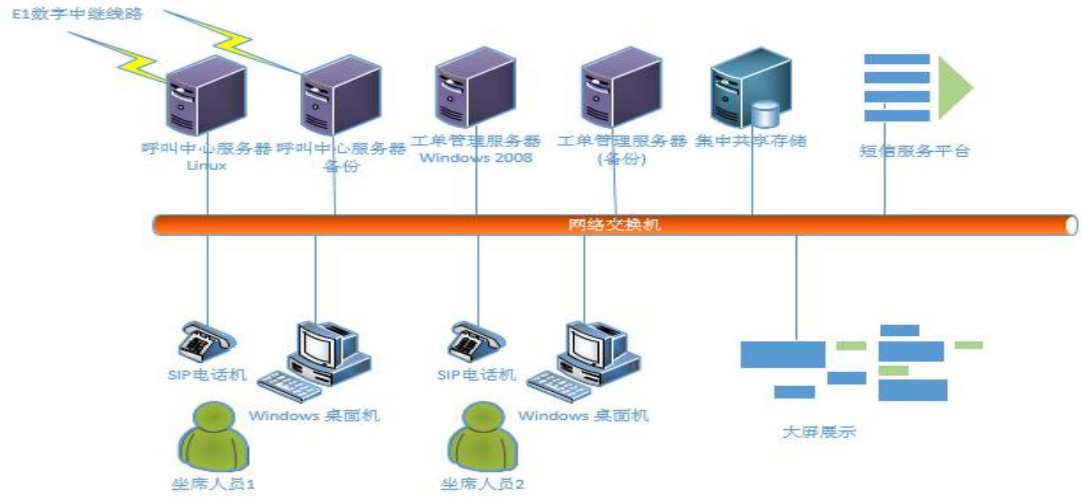


将 NETMANAGER 平台的作业原子对接为标准运维中的原子，供标准运维流程编排中调用。


bk_gcloudv3
标准运维
业务首页
任务流程
任务记录
业务配置
轻应用
帮助文档
蓝鲸
工具
执行网管作业
保存
返回列表
全局变量
新增变量
名称
KEY
执行NOP作业
NOP作业-执行...
sult_d73b} == True
${_result_d73b} == False
暂停
蓝鲸服务(BK)-...
失败节点执行NOP作业
NOP作业-执行...

五、智能运维响应中心服务台

1、RXGT Call Center 产品简介



RXGT Callcenter 是一款纯 IP PBX 系统。配合 RXGT CTI Agent 接续控制软件，可以实现从 10 人到 100 人的 IT 安全响应中心服务台呼叫中心能力。

PBX/ACD 中心主要功能

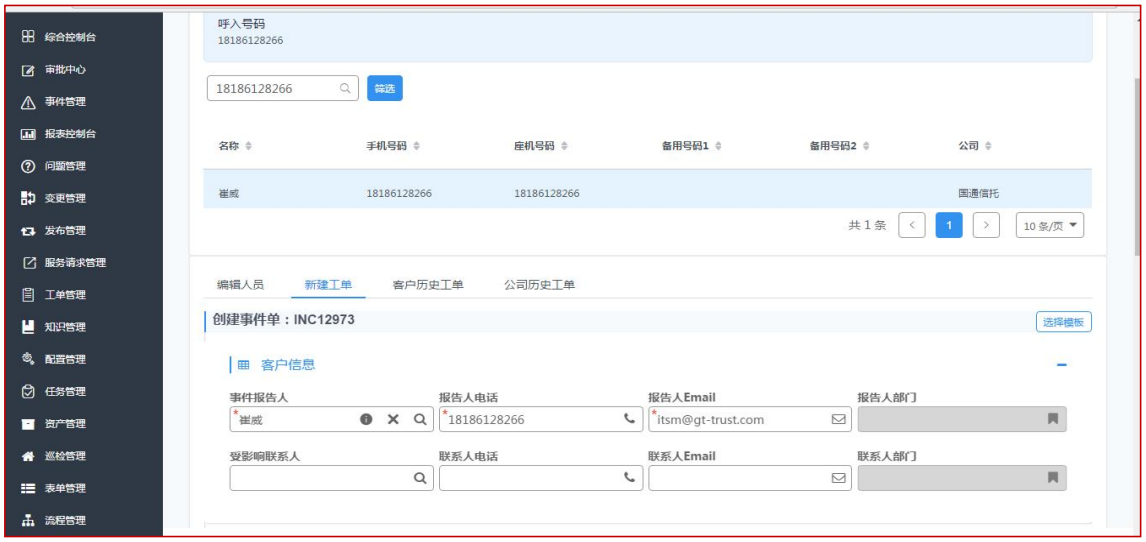
- 电信 E1 线路，支持最大 30 路语音同时呼叫；
- IVR 语音导航；
- ACD 呼叫等待；
- 按键选择；
- 对列轮循；
- 呼入、呼出自动录音系统；
- 多账号签入签出；
- 示忙、示闲；
- 会议功能；
- 邮件功能；
- 短信功能；

CTI Agent 坐席软件：

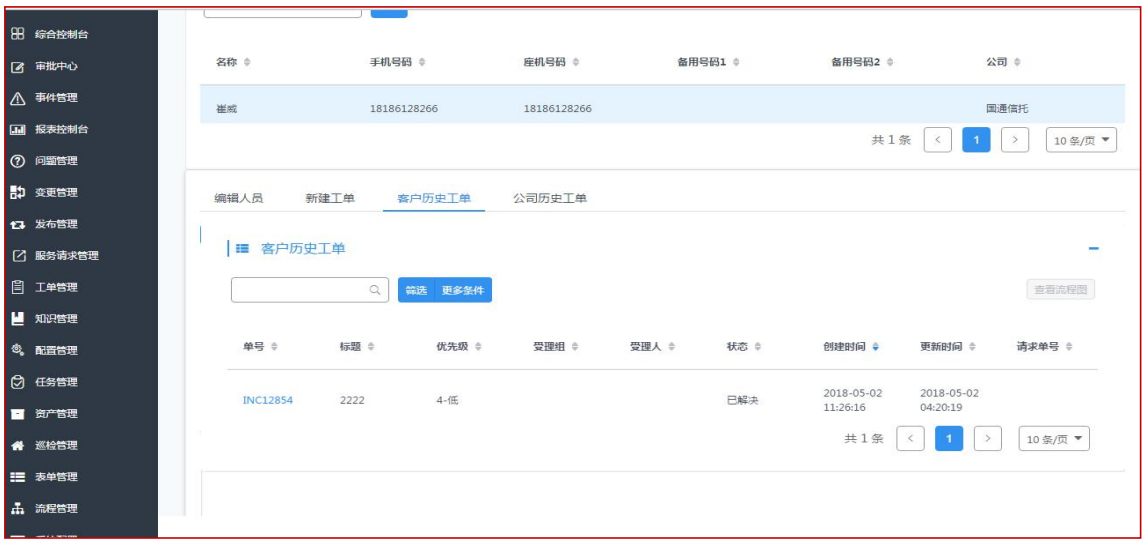
- CTI 签入、签出；

- CTI 功能模块与 SIP 话机功能同步；
- CTI 所有坐席状态查询；
- CTI 历史呼叫查询；
- CTI 接听电话话机自动示忙；
- 系统呼入溢出显示；

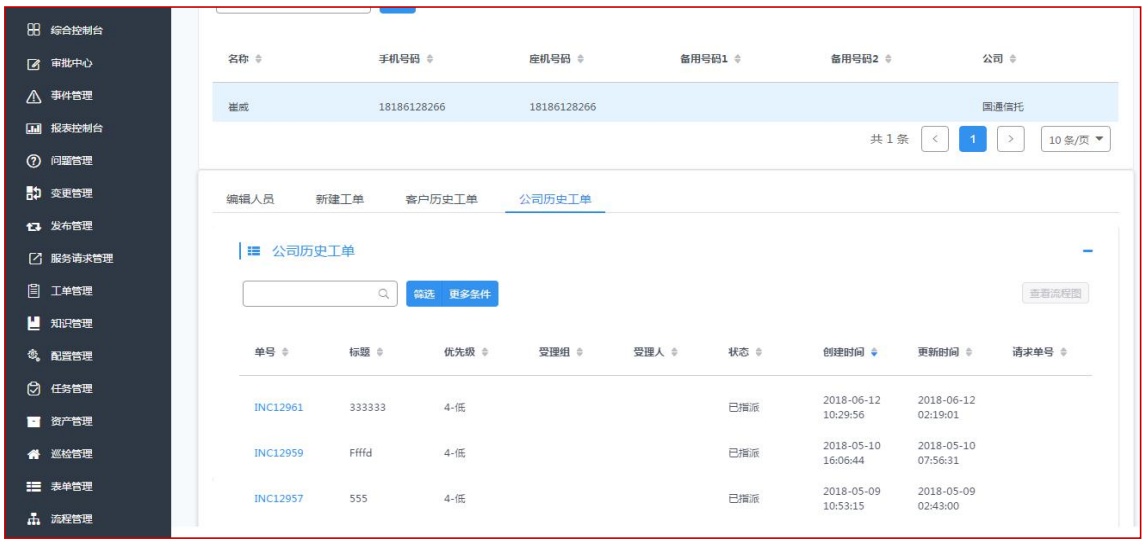
RXGT ITSM V2.X 与 Call Center 集成来电弹屏信息，如果 VIP 来电，将以红色背景来显示用户基本信息



查个人看历史工单



查看用户单位历史工单



2、RXGT EasyCTI Agent 产品简介

RXGT Call Center 解决方案是基于 IP、IPPBX 等先进技术形成的全方位呼叫中心解决方案。具有完整 IVR、PBX 等各项专业功能。

本软件 EasyCTI Agent，是为了满足客户对简易型呼叫中的要求而专门定制的，该软件对现有的硬件环境依赖最小，不需要专业 Call Center，通过简易普通电话线路，就可以实现来电识别、录音、工单弹屏等关键功能。小型规模的 ITSM 机构可以把它作为简易安全响应中心服务台使用，迅速提高客户服务体验，从而深受广大小型运维服务组织所喜爱。

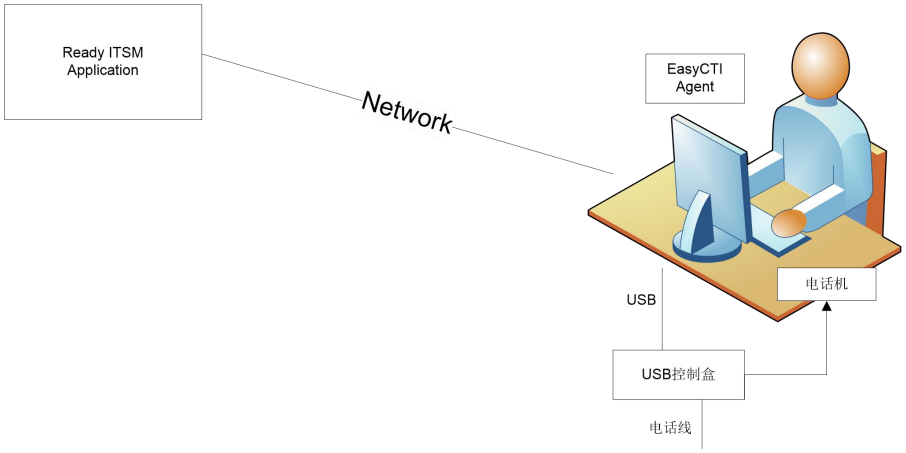
RXGT EasyCTI 是为 IT 安全响应中心服务台设计的简易型电话坐席软件。具备以下特点：

- 设备简单。通过 USB 电话语音控制盒，与普通电话线路和电话机进行协同工作。
- 内置与 RXGT ITSM 软件集成系统工作。
- 录音文件可以上传到服务器，并与工单进行关联。
- 适用于国产化操作系统换。

- 无需安装任何驱动程序。

RXGT EasyCTI 软件具有以下功能：

- 通过 USB 控制盒子，与普通电话线路和电话机协同工作。
- 来电识别，并弹出 RXGT ITSM 浏览器页面，匹配主叫号码到用户。快速识别用户身份和历史工单；
- 后台呼入呼出录音；在本地、SFTP 或者 ITSM 服务器上进行同步存储。
- 录音与工单进行关联，便于后期服务质量检查；
- 记录和管理通话记录；
- 通话记录可以转出为 Excel。来电自动匹配通话历史。
- 通话历史可以被简易查询。
- 直观显示当前话机状态。
- 对通话进行备注，记录跟踪事项。
- 在 ITSM 页面上直接呼出拨打电话，避免手工按键。
- 工作可以在前台或者后台，并可以通过快捷按键进行迅速切换。

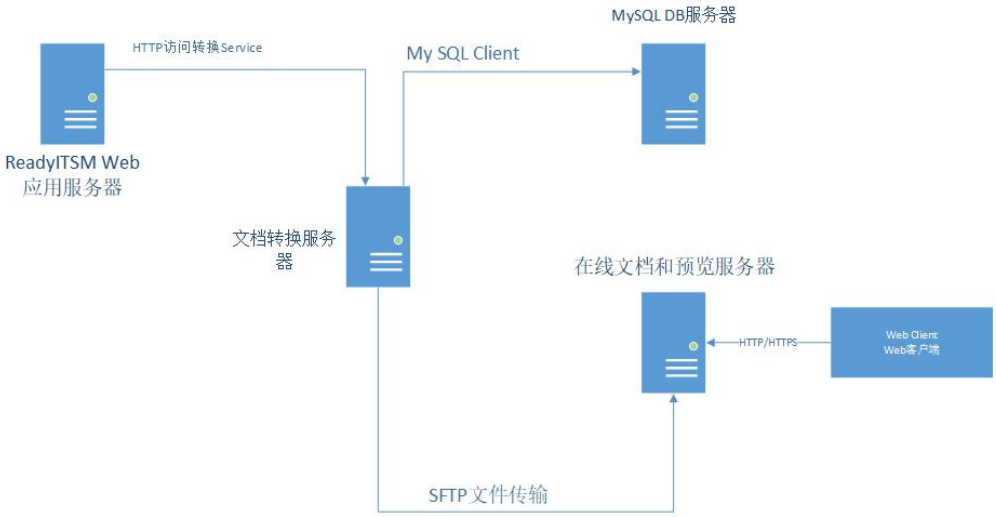


六、智能运维个人辅助工具

1、RXGT DocPreview 文档转换预览服务器

文档预览服务器软件的目标是不需要用户下载附件，直接在系统内通过浏览器预览查询附件的内容。支持 Office 文件类型、多媒体文件类型等附件。技术目标为：

- 当用户上载附件后，服务器自动准实时进行转换；
- 把数据库中的附件，从数据表 rd_sys_attachment 中的 BLOB 字段，自动提取成独立为文件；
- 能够把提取的文档，自动归档或者转存到专门的文档服务器；
- 后台自动进行转换，能够把常见的 Office 文档包括 Word、PPT、Excel 等转换为在线预览何所，通过 Web 和手机进行在线预览文档内容，而不需要下载；
- 提供基于文件的高级运用能力，例如未来的全文检索；
- 提供 HTTP Web 服务，提供及时转换服务，而不需要插入的 ITSM 附件。



2、RXGT Attachment Assistant 附件助手

附件助手是安装在用户桌面机上的软件，能够与 RXGT ITSM 系统协同工作。可以在页面上点击“在线编辑”后，自动下载附件到本地，打开相应的 Office/WPS 软件进行附件编辑，用户保存后，附件助手自动上载更新后的文件。

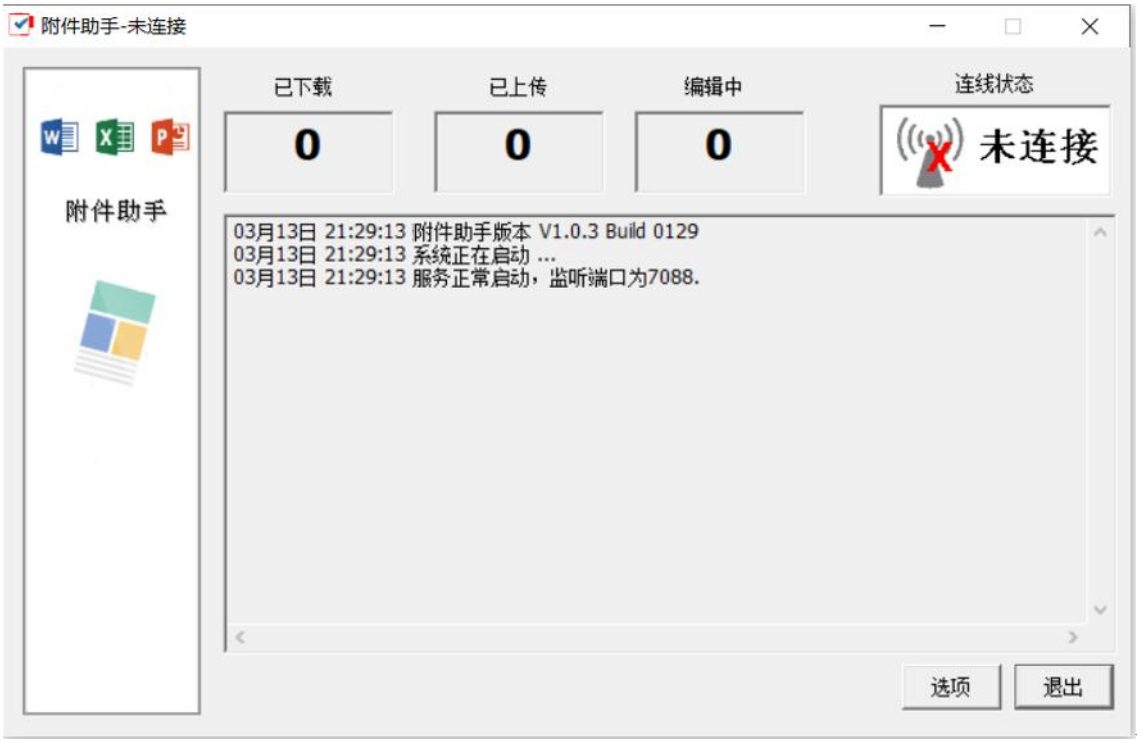
对业务的优势如下：

（1） 与浏览器类型无关，无浏览器插件，安全可靠；

（2） 同时支持 Microsoft Office 以及 WPS 文档编辑器；

（3） 常驻后台，保持用户本地编辑文档软件的操作习惯；

（4） 灵活小巧，用户操作流程，用户体验好。

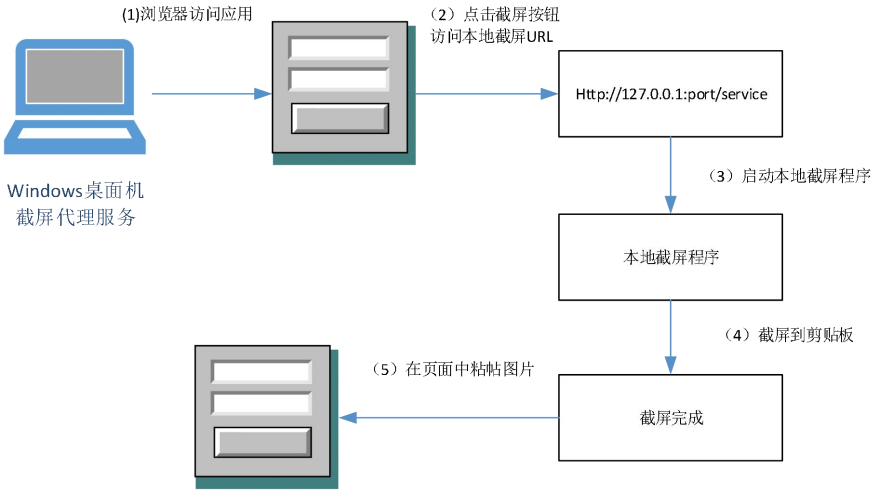


3、RXGT Screen Capture Web 截屏

融讯光通 Web 截屏代理，是一套用户在 Web 界面上直接点击按钮进行截屏的软件。与目前常见的 QQ、微信客户端截屏不同之处是：直接在 Web 页面上点击截屏，而且不需要在浏览器上安装任何插件。它可以帮助您实现下列功能：

1. 在 Web 应用上直接点击截屏按钮发起截屏动作；
2. 可以选择不同的截屏区域，并可以进行箭头标示关键屏幕信息；
3. 截取的屏幕直接拷贝到客户机剪贴板，在 Web 页面的富文本编辑框内 Control+V 剪贴到页面；
4. 系统不包含任何 ActiveX 等类似扩展插件，因此广泛支持多种浏览器；
5. 目前该软件支持麒麟、统信等国产化操作系统。

3.1、融讯光通 Web 截屏系统结构



整个 Web 截屏服务由以下三个部分组成：

- Web 截屏服务：本地服务形式。以 HTTP 服务器的形式监听在本地 127.0.0.1 端口，支持浏览器通过约定的 URL 检测、启动截屏程序；
- 截屏程序：由 Web 截屏服务调用，完成屏幕截屏并保存到系统剪贴板；
- 配套 Web 页面：在 Web 上由富文本编辑页面和截屏按钮组成。支持 Web 截屏服务提供的服务命令和格式。

3.2、融讯光通 Web 截屏适用范围

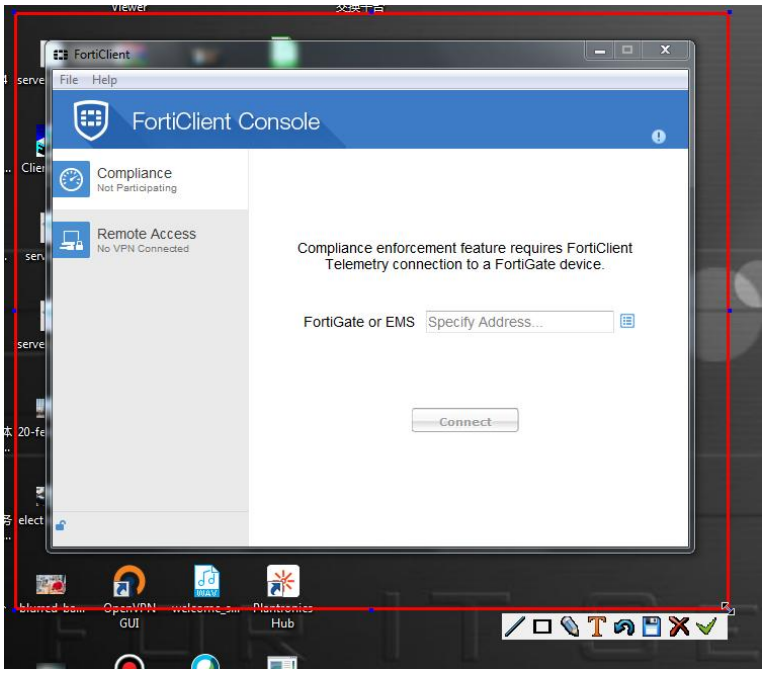
Web 截屏代理可以适用于需要在页面上进行截屏的场景，便于提高截屏的易用性和效率。典型的运用场景如下：

1. RXGT ITSM 上故障申告。当出现应用软件、Web 页面等各类 IT 故障时，可以在页面上直接截屏，并保存到事件单；

2. OA、ERP 等应用。需要在业务环境进行截屏的时候，例如某个应用提供的凭证页面，

也可以使用 Web 截屏代理系统。

3. 对浏览器安全性高的场合。例如有些高安全性的场合不能安装浏览器第三方插件，可以通过 Web 截屏代理来满足这方面的特殊要求；

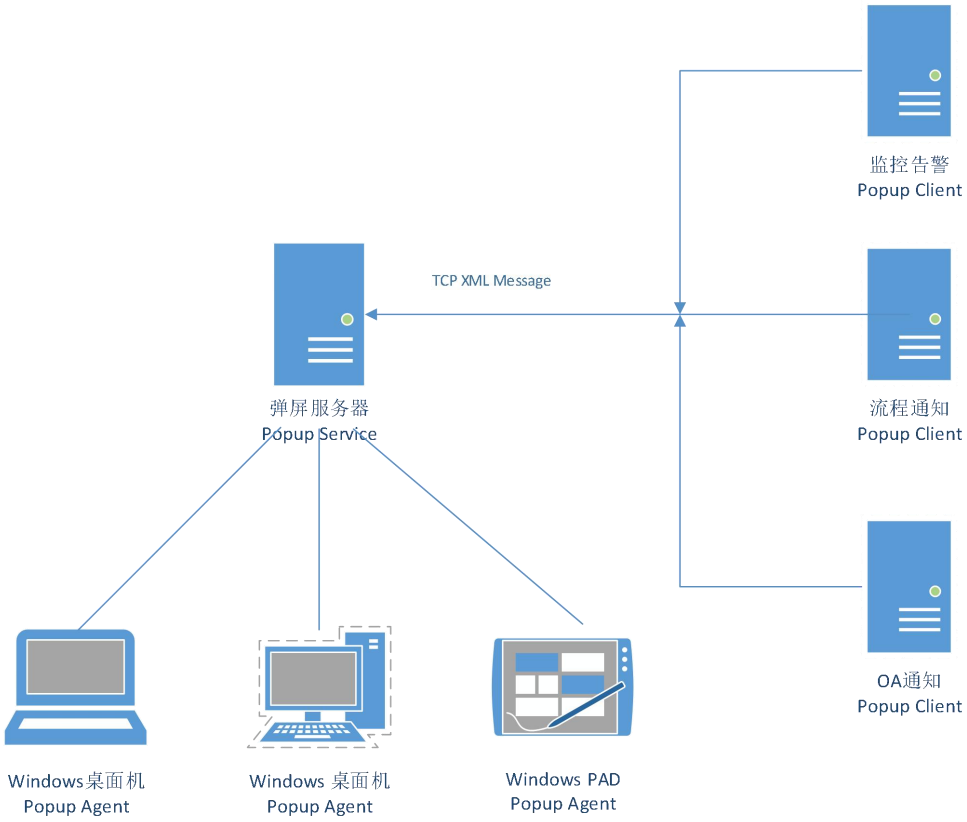


4、RXGT Message Agent 消息弹屏服务

融讯光通弹屏服务系统，是一套在 TCP/IP 网络环境下的及时消息通知系统。当需要向被通知对象的弹屏客户机发送及时通知消息时，融讯光通弹屏服务系统可以帮助您实现下列功能：

1. 在网络安全设备运维工程师的桌面终端，及时弹出消息屏幕，零延迟；
2. 可播放定制的音乐或者声音提醒；
3. 基于 Client/Server 模式，支持异构网络和 NAT 协议；
4. 提供基于 XML 的标准协议，可以灵活地与 ITSM、监控、事件告警等应用系统进行集成；
5. 支持消息暂存和重发，完整的传输控制确保消息不丢失；
6. 专属的私密通知渠道和形式，与社交软件如微信相不同，确保工作信息的严谨性；

4.1、融讯光通弹屏服务系统结构



整个弹屏服务系统由以下三个部分组成：

- 弹屏服务器：在国产化操作系统环境下运行 Popup Service 服务，接收来自告警系统发出的推送消息请求，并按照目标对象，推送到指定的国产化操作系统桌面机。作为服务端，它还需要完成客户端的注册、状态跟踪、退出等管理工作，同时也需要完成消息的存储和转发等传输控制工作。

- 弹屏坐席端：在国产化操作系统环境下安装 Popup Agent 软件，并配置好相关参数，注册到 Popup 服务器，接收并弹出消息，并完成历史消息存储查看和 URL 一键点开等功能。

- 弹屏消息发送客户端：基于 XML 的 TCP 消息格式，向服务器发送需要通知的消息，包括消息发送对象和消息体内容。产品提供 JAVA 代码和国产化操作系统客户端代码，便于在不同的应用场景进行集成和灵活运用。

4.2、融讯光通弹屏服务系统适用范围

弹屏服务可以适用于需要及时通知的各类场景。典型的运用场景如下：

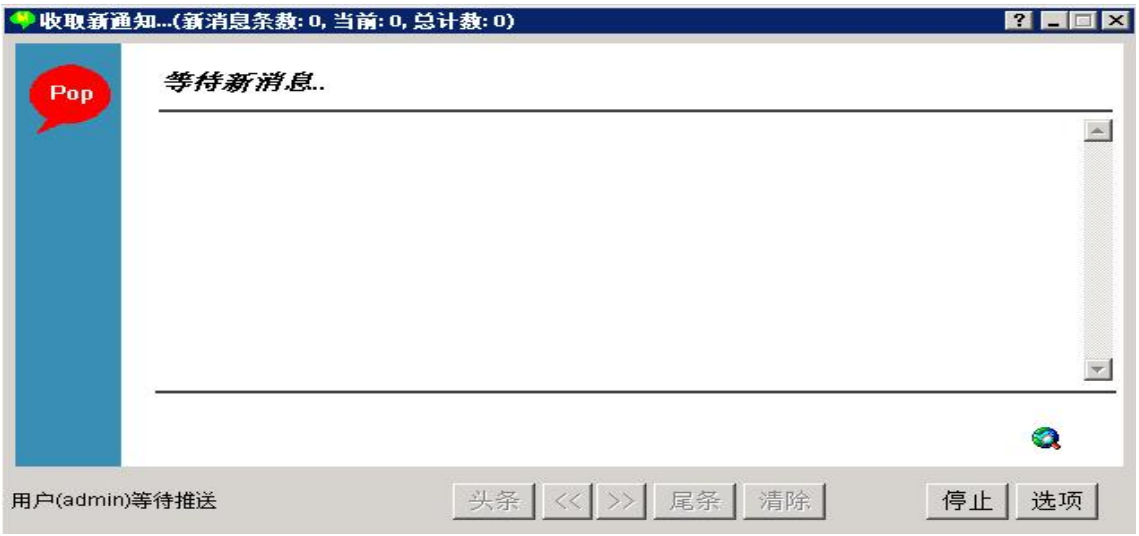
1. RXGT ITSM 通知。当有工单分配到工程师时，能够在工程师国产化操作系统机器上弹出通知消息；

2. 监控告警。监控系统发现重大故障时，能够通过弹屏消息通知到值班人员，并播放告警的声音；

3. OA、ERP 等企业应用。当业务流程需要指定人员进行快速处理时，弹屏服务系统可及时通知到相关人员。

4.3、运行环境

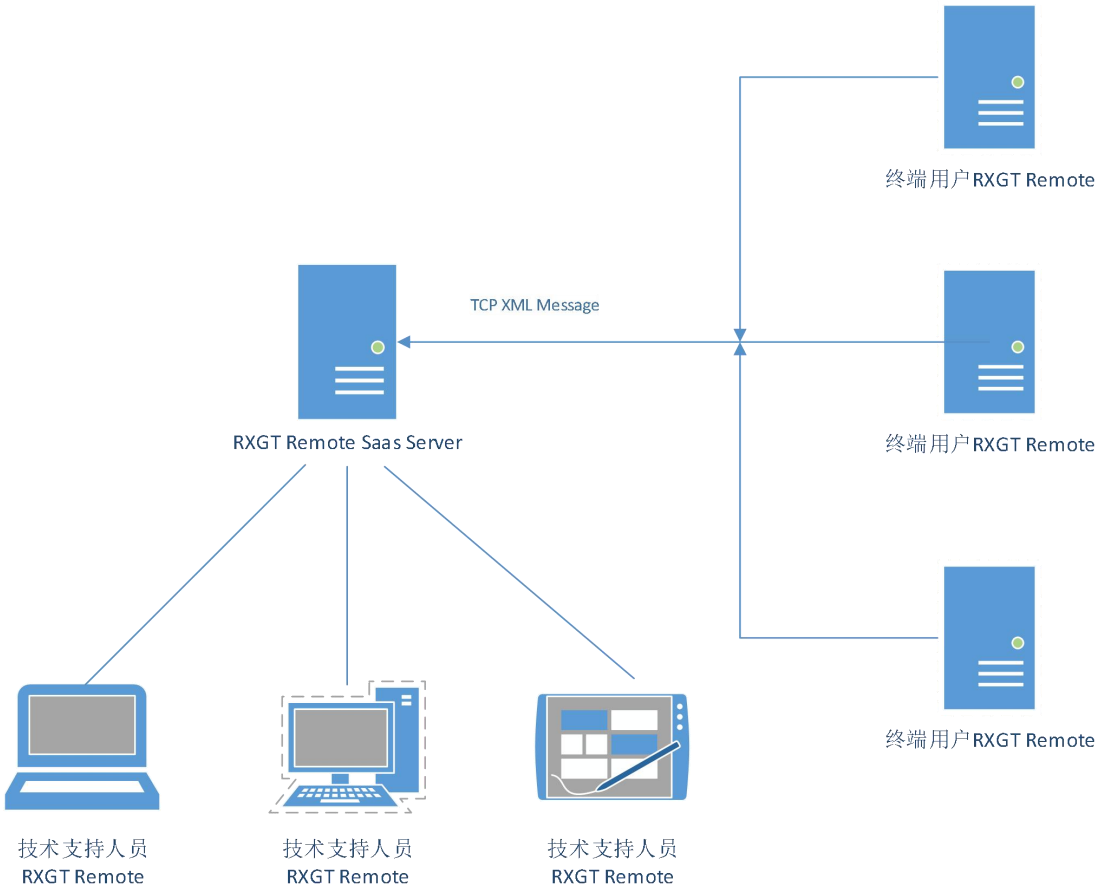
No	部件	版本	运行环境
1	弹屏服务器	1.0.1	国产化操作系统 32Bits or 64Bits
2	弹屏座席端	1.0.1	国产化操作系统 32Bits or 64Bits
3	弹屏消息发送端	1.0.1	国产化操作系统 2008, 32Bits or 64Bits Linux Java JRE/JDK 1.8 or Higher



5、RXGT Remote 云端远程控制

融讯光通远程控制，是一款运行在国产化操作系统环境下的，基于云服务的远程控制产品。与 ITSM 系统相结合，可以当终端用户出现 IT 故障时，网络安全设备运维服务人员及时通过远程控制，共享用户桌面和输入设备，及时解决问题。

5.1、RXGT Remote 系统结构



整个远程控制服务系统由以下二个部分组成：

- Remote Saas 服务器：在国产化操作系统/Linux 环境下运行 Saas 化 Remote Proxy Service 服务，位于公网或者内网公共区域，作为管道处理远程控制的各种通讯。
- Remote Server/Client：在国产化操作系统环境下安装 Remedy Remote 软件，并配置好相关参数，注册到 Saas 服务器，通过唯一 ID 进行远程控制。

5.2、融讯光通远程控制系统适用范围

远程控制运用场景如下：

1. 远程控制客户机，直接处理客户 IT 故障，提高故障处理效率和客户满意度；
2. 远程培训；
3. 协同工作。不同的网络安全设备运维服务团队，通过远程控制共享客户屏幕，协同解决问题。