**新版TRMSMonitor功能实现概要设计**

[一、系统管理 2](#_Toc13999)

[组织机构管理 3](#_Toc7798)

[（1）子公司维护 3](#_Toc27725)

[（2） 部门/班组维护 3](#_Toc23732)

[（3） 岗位维护 3](#_Toc360)

[人员管理 3](#_Toc26244)

[（1） 人员维护 3](#_Toc24251)

[权限管理 4](#_Toc23520)

[（1） 权限维护 4](#_Toc24000)

[准入数据导入 4](#_Toc11299)

[（1） 准入数据导入 4](#_Toc17698)

[一、 资产管理 4](#_Toc11546)

[资产基本信息 4](#_Toc24069)

[（1） 桌面终端信息 4](#_Toc19390)

[（2） 移动设备信息 4](#_Toc4180)

[实现方案：通过设备采集的插件调用windows WMI API或Print Spooler API 来获取打印机的相关信息。 5](#_Toc11198)

[资产历史 5](#_Toc9905)

[（1） 资产历史信息管理 5](#_Toc29748)

[二、 运行管理 5](#_Toc7873)

[设备运行管理 5](#_Toc15175)

[（1） 在线设备管理 5](#_Toc20706)

[（2） 设备运行时状态 5](#_Toc20350)

[应用运行管理 6](#_Toc21136)

[（1） 应用信息查询 6](#_Toc21780)

[（2） 进程信息查询 6](#_Toc20746)

[三、 终端安全管理 6](#_Toc7826)

[应用安全管理 6](#_Toc19951)

[（1） 黑白名单维护 6](#_Toc9069)

[（2） 必备软件维护 7](#_Toc13800)

[（3） 必备软件检测 7](#_Toc19591)

[（4） 应用策略管理 7](#_Toc18855)

[（5） 软件合规性检查 7](#_Toc19905)

[信息安全管理 8](#_Toc21431)

[（1） 安全策略库维护 8](#_Toc15609)

[（2） 网络应用白名单管理 8](#_Toc14835)

[（3） 网络应用合规性检查 8](#_Toc23089)

[（4） 网络共享检测 8](#_Toc12197)

[（5） 默认用户检测 8](#_Toc22959)

[网络安全管理 9](#_Toc13714)

[（1） 终端网络流量监控 9](#_Toc18515)

[（2） 网络拓扑发现 9](#_Toc16262)

[（3） 应用/功能可用性检测 9](#_Toc9083)

[系统安全 10](#_Toc21275)

[（1） 终端硬件检测 10](#_Toc18735)

[（2） 业务环境监测 10](#_Toc20938)

[四、 运维管理 10](#_Toc19042)

[文件推送 10](#_Toc28817)

[（1） 推送计划定制 10](#_Toc14478)

[（2） 推送计划审批 11](#_Toc12716)

[（3） 推送结果查询 11](#_Toc4349)

[消息推送 11](#_Toc6455)

[（1） 推送计划定制 11](#_Toc15221)

[（2） 推送计划审批 11](#_Toc23469)

[（3） 推送结果查询 12](#_Toc32543)

[终端策略维护 12](#_Toc32165)

[（1） 终端分组管理 12](#_Toc10220)

[（2） 终端及配置策略维护 12](#_Toc22081)

[（3） 终端分组策略维护 12](#_Toc10169)

[远程协助 13](#_Toc12828)

[（1） 远程协助管理 13](#_Toc6659)

[（2） 远程协助客户端开发 13](#_Toc712)

[软件仓库 13](#_Toc1530)

[（1） 必备软件库管理 13](#_Toc10007)

[（2） 办公软件库管理 13](#_Toc23063)

[（3） 常用软件库管理 13](#_Toc31423)

[（4） 软件配置管理 14](#_Toc13754)

[共享管理 14](#_Toc4130)

[（1） 文件共享配置管理 14](#_Toc30802)

[辅助工具管理 14](#_Toc19768)

[（1） 业务系统一键安装修复管理 14](#_Toc2840)

[五、 统计分析 14](#_Toc11503)

[统计分析 15](#_Toc16753)

[（1） 统计分析 15](#_Toc12423)

# 一、系统管理

## 组织机构管理

### （1）子公司维护

功能说明：维护楚雄供电局及下属现公司的组织机构。

实现进度：已完成

实现方案：终端通过读取上来的UKEY信息，里面的ID在后端数据库反差员工归属表，就可以得到员工的归属子公司，也知道了该子公司的员工和IP信息。

### 部门/班组维护

功能说明：部门和班组维护。

实现进度：已完成

实现方案：同子公司维护功能类似，可以通过UKEY读取上来的信息进行班组和部门维护。

### 岗位维护

功能说明：岗位维护，通过岗位可确定岗位职责，通过岗位进行应用策略管理或必备软件检测。

实现进度：未完成

实现方案：同子公司维护功能类似，可以通过UKEY读取上来的信息在后端反查与之ID关联的岗位表实现岗位与员工的维护，为之后的应用策略或必备软件检测提供管理基础。

## 人员管理

### 人员维护

功能说明：维护系统操作员及桌面终端使用人员信息，将人员信息与UKEY信息进行关联。

实现进度：已完成

实现方案：维护系统操作员有管理终端的账号密码，终端使用人员的信息会被终端软件读取发送到管理端的服务器

## 权限管理

### 权限维护

功能说明：对系统操作员进行权限维护

实现进度：已完成

实现方案：由服务端后台根据数据库表设计管理员角色权限分配，有些只有读权限，有些写权限

## 准入数据导入

### 准入数据导入

功能说明：为简化人员维护工作量，可通过从准入系统或4A系统中导出人员及组织机构数据，导入系统后在进行维护。

实现进度：已完成

实现方案：通过程序导入员工数据到数据库表中

# 资产管理

## 资产基本信息

### 桌面终端信息

功能说明：查询所有已部署安全管控平台客户端的桌面终端资产类信息，包括设备厂家、型号，核心配件参数等基础数据。

实现进度：已完成

实现方案：通过设备采集的插件调用windows API以读取注册表，读取Wmi配置以及其他的方式采集到了主板，CPU，内存等硬件配置的信息。

### 移动设备信息

功能说明：查询曾经在已部署安全管控平台客户端的桌面终端上曾经使用的移动设备信息（移动硬盘，连接的打印机等）

实现进度：未完成

# 实现方案：通过设备采集的插件调用[windows WMI API](https://stackoverflow.com/questions/3997177/how-to-get-printer-information-using-command-line-on-windows-machine)或[Print Spooler API](https://msdn.microsoft.com/en-us/library/windows/desktop/dd162861(v=vs.85).aspx) 来获取打印机的相关信息。

## 资产历史

### 资产历史信息管理

功能说明：当桌面终端设备属性或责任人发生变化时，进行记录，通过次功能可查询到桌面终端全生命周期信息

实现进度：已完成

实现方案：服务端数据库维护一张与设备指纹关联的责任人变更的历史表，以及配置变更的历史表

# 运行管理

## 设备运行管理

### 在线设备管理

功能说明：查看当前在线终端的相关信息

实现进度：已完成

实现方案：安全终端每间隔一段时间回送资产的动态运行信息，该信息可以充当心跳包，来保证管理服务端能获取安全终端的运行状态，查看是否掉线。

### 设备运行时状态

功能说明：获取桌面终端的运行时状态，包括CPU、内存、网络、磁盘空间等

实现进度：已完成

实现方案：安全终端每间隔一段时间回送资产的动态运行信息，该信息包括CPU的使用率，内存使用率，网络上下行流量等，大部分都可以通过windows API来做到。

## 应用运行管理

### 应用信息查询

功能说明：获取桌面终端已安装应用信息、正在运行的应用信息。

实现进度：已完成

实现方案：安全终端每间隔一段时间回送资产的动态运行信息（包含正在运行的应用），并且在启动的时候会随着静态资产信息送回已安装的应用列表，最后存储入数据库，管理Web端就可查询出应用信息列表。

### 进程信息查询

功能说明：获取桌面终端已安装应用信息、正在运行的应用信息。

实现进度：已完成

实现方案：安全终端每间隔一段时间回送资产的动态运行信息（包含正在运行的进程），最后存储入数据库，管理Web端就可查询出进程信息列表。

# 终端安全管理

## 应用安全管理

### 黑白名单维护

功能说明：信息中心根据对岗位或终端使用人的工作性质梳理应用的黑白名单，黑名单为禁止安装类软件，白名单为允许安装类软件。

实现进度：未完成

实现方案：

1. 维持现有服务端的前提下，因为与服务端是http协议进行通讯，服务端不能主动发起连接，都是被动方式响应http请求，那么黑白名单可以在服务端配置完成并存入数据库，客户终端以一定时间间隔来请求黑白名单配置的http接口，并根据所返回的内容判断是否在分组，分部门，分IP段范围内提示用户卸载或安装必须的软件应用。这样的实现方案缺点是服务端压力会增大，有不必要的冗余请求。优点是简单直接，开发成本不大，现有服务端架构不变。
2. 改变服务端架构，引入MQ Server（比如，ActiveMQ，Kafka），通过MQ的topic的发布/订阅语义来实现推送黑白名单的配置，所有终端都订阅白名单的topic和黑名单的topic，服务端就把配置好的信息存入数据库，并推送给MQ Server，MQ Server会自动下发到订阅相关topic的订阅者客户端。这样就不会有冗余请求，服务端压力减小，传统的MQ Server支持高并发。把压力转移到MQ Server上。

### 必备软件维护

功能说明：根据管控要求桌面终端必须要安装的软件维护，可细分到岗位或终端，或终端组。

实现进度：未完成

实现方案：可根据黑白名单维护的实现方案推送必备的软件维护信息，客户终端根据信息内容执行方案，比如PhotoShop在某PC机器上版本过低，提示用户必须升级到详细的版本号上去，或者大于某个版本号。

### 必备软件检测

功能说明：根据必备软件维护通过客户端软件进行检测并上报结果。

实现进度：未完成

实现方案：可根据黑白名单维护的实现方案推送必备的软件信息，客户终端根据信息内容执行方案，比如某PC电脑或班组必须安装PhotoShop，那么就提示用户下载该软件并把结果上报给服务端，或者通过TRMSMonitor的应用仓库下载该应用（把应用ID和版本号传回服务器，服务器通过json返回必备应用的下载URL，客户端再开始下载必备软件）。

### 应用策略管理

功能说明：根据岗位、人员或终端设置软件应用策略，允许指定的人或指定的设备在指定的时间运行或禁止某些应用的使用。

实现进度：未完成

实现方案：可根据黑白名单维护的实现方案推送应用策略信息，客户终端根据信息内容执行方案，比如某PC电脑禁止运行QQ，那么终端会提示责任人卸载QQ或者强行终止QQ进程）。

### 软件合规性检查

功能说明：根据黑白名单对桌面终端安装的应用进行合规性检测并上报检测结果。

实现进度：未完成

实现方案：该功能基本属于应用黑白名单的功能，实现方案参考黑白名单维护。

## 信息安全管理

### 安全策略库维护

功能说明：根据岗位、人员或终端设置桌面终端的安全策略，如复杂口令等具有普遍性的安全策略，客户端根据终端使用人自动下发并更新相关策略，实现自动运维。

实现进度：未完成

实现方案：待定，目前暂时没在网络上搜索到策略文件通过命令行或API导入windows组策略管理器的解决方案，暂时只实现了特定的几个windows策略的修改。

### 网络应用白名单管理

功能说明：根据对必备应用和业务相关应用的梳理，可以明确存在网络应用的进程名称及相关端口和协议类型，并建立存在网络应用的进程黑白名单。

实现进度：未完成

实现方案：可根据黑白名单维护的实现方案推送应用策略信息，客户终端根据信息内容执行方案，比如某PC电脑禁止FoxReader链接网络，那么终端会通过windows 7或以上内置的[防火墙API](https://msdn.microsoft.com/en-us/library/windows/desktop/aa366418(v=vs.85).aspx)实现禁止某应用在某特定端口下网络数据收发（禁止该应用上网）。

### 网络应用合规性检查

功能说明：根据网络应用黑白名单对桌面终端存在网络应用的进程进行检测，并上报检测结果。

实现进度：未完成

实现方案：可根据黑白名单维护的实现方案推送应用策略信息，客户终端根据信息内容执行方案对比进程列表中是否有违规的进程，最后汇总并上报结果。

### 网络共享检测

功能说明：根据信息安全合规性要求对桌面终端的共享目录进行检测并上报结果。

实现进度：已完成

实现方案：已通过读取注册表检测局域网共享路径的列表并向服务端上报结果。

### 默认用户检测

功能说明：根据信息安全合规性要求对桌面终端的操作系统默认用户进行检测并上报结果。

实现进度：未完成

实现方案：客户终端能读取UKEY检测当前PC的使用者，并与指纹信息发送给客户端，指纹信息与该PC责任人相关联，若当前用户与责任人不符，那么服务端Web页面可以标记出来。

## 网络安全管理

### 终端网络流量监控

功能说明：监控桌面终端的上下行数据流量。

实现进度：已完成

实现方案：该实现方案与设备运行管理中的实现方案一致，通过API可以得到网络上下行流量。

### 网络拓扑发现

功能说明：根据管理终端下发目标IP，桌面终端客户端软件发起对目标IP的路由追踪，根据追踪结果实时绘制网络拓扑图。

实现进度：未完成

实现方案：待定，尚未发现该类命令行工具与编程接口。发现了几个如下有待进一步研究的项目

<https://lantopolog.com/> （免费GUI 网络拓扑发现工具，非命令行，闭源项目）

<https://github.com/svigneux/network.topology> （用Shell实现的非常简单的项目）

<https://github.com/verbosemode/cdpwalker> （Python实现，依赖于SNMP和Cisco Discovery Protocol 协议，不知是否可行）

<https://github.com/vijaykeswani/Network-Topology-Discovery> （Web项目）

<https://github.com/mounirLtaief/Icinga2-Faraday> （Python实现，用了Neo4j存储拓扑图模型）

<https://metacpan.org/pod/App::Netdisco> （非开源软件）

<http://www.sourcecodeonline.com/details/calia.html> （非windows 可运行软件）

<https://www.ibm.com/developerworks/cn/opensource/os-cn-nmap/>

<https://nmap.org/zenmap/> （Linux下的nmap有个叫zenmap的GUI工具，可以发现网络拓扑）

### 应用/功能可用性检测

功能说明：根据管理终端下发的请求信息，桌面终端客户端发起相应请求，并记录请求路由，响应时间的信息，实现业务系统全局可用性追踪，提高系统维护效率和故障提前预警。

实现进度：未完成

实现方案：可以直接读取tracert命令行（相当于Linux下的route trace）返回后的信息整理上报路由信息和响应时间

## 系统安全

### 终端硬件检测

功能说明：对桌面终端进行硬件设备检测，包括驱动程序安装等信息，桌面终端用户可手工检测，系统管理员也可以通过管理终端远程发起检测

实现进度：未完成

实现方案：上一版本已经实现硬件设备的信息采集，但是没有包含驱动安装的列表信息，可以通过这些信息进行检测。至于获取驱动安装列表可以通过E[numDeviceDrivers](https://msdn.microsoft.com/en-us/library/windows/desktop/ms682619(v=vs.85).aspx)该API来达到目的。另外还有[其他的方案](https://www.codeproject.com/articles/38275/getting-the-list-of-drivers-running-on-windows-os)。

### 业务环境监测

功能说明：根据业务系统制定和完善相应业务系统的运行环境检测，为业务系统终端运维提供数据支撑

实现进度：未完成

实现方案：待定，暂不清楚需求描述。

# 运维管理

## 文件推送

### 推送计划定制

功能说明：完成文件推送计划的制定、包括推送时间、对象等信息制定

实现进度：未完成

实现方案：文件推送在服务Web端进行编辑（时间段）并保存。最后通过黑白名单维护的推送方案推送消息。

### 推送计划审批

功能说明：文件推送管理人员对相应的推送计划进行审批，审批通过后系统按推送计划进行文件推送。

实现进度：未完成

实现方案：文件推送计划由系统管理员编制保存，文件推送管理人员登陆后，就能看到文件推送计划，并且点击审批按钮后才能下发文件。只要数据库表的字段增加相应的权限段即可。

### 推送结果查询

功能说明：对推送结果进行查看，可提供成功与失败清单及相关原因。

实现进度：未完成

实现方案：客户端收到文件，并以对话框的形式提示用户消息，用户确认后，客户端立即返回相应的json串通知服务器。

## 消息推送

### 推送计划定制

功能说明：完成消息推送计划的制定、包括推送时间、对象等信息制定

实现进度：未完成

实现方案：消息推送在服务Web端进行编辑（时间段）并保存。最后通过黑白名单维护的推送方案推送消息。

### 推送计划审批

功能说明：消息推送管理人员对相应的推送计划进行审批，审批通过后系统按推送计划进行文件推送。

实现进度：未完成

实现方案：消息推送计划由系统管理员编制保存，消息推送管理人员登陆后，就能看到文件推送计划，并且点击审批按钮后才能下发消息。只要数据库表的字段增加相应的权限段即可。

### 推送结果查询

功能说明：对推送结果进行查看，可提供成功与失败清单及相关原因。

实现进度：未完成

实现方案：客户端收到消息，并以对话框的形式提示用户消息，用户确认后，客户端立即返回相应的json串通知服务器。

## 终端策略维护

### 终端分组管理

功能说明：对所有在线终端可根据组织机构或岗位及相关工作性质对桌面终端进行分组管理

实现进度：未完成

实现方案：分组管理的通信机制可根据黑白名单维护管理中的方案执行，根据定制的分组信息写入MQ Server相关的topic，客户端根据topic的分类执行相应命令。

### 终端及配置策略维护

功能说明：根据不同的管控需求，制定不同的终端配置及相应策略维护。

实现进度：未完成

实现方案：待定，暂不清楚需求描述。

### 终端分组策略维护

功能说明：对终端分组和终端及配置策略进行关联，实现终端配置及配置策略和终端分组的关联。

实现进度：未完成

实现方案：待定，暂不清楚需求描述。

## 远程协助

### 远程协助管理

功能说明：实现对远程协助的配置管理，包括身份二次验证，远程协助的权限管理功能

实现进度：未完成

实现方案：远程协助采用了开源的RealVNC方案，远程客户端通过相应配置打开客户端的RealVNC Server命令行，服务端通过RealVNC客户端连接远程。

### 远程协助客户端开发

功能说明：桌面终端安全管理管控平台客户端实现远程管理模块相应功能。

实现进度：未完成

实现方案：远程协助采用了开源的RealVNC方案，远程客户端通过相应配置打开客户端的RealVNC Server命令行，服务端通过RealVNC客户端连接远程。。

## 软件仓库

### 必备软件库管理

功能说明：对网省公司要求必须安装的软件进行管理。

实现进度：未完成

实现方案：内网软件库暂时由Ftp服务器代替，服务器端数据库维护必备软件的列表表格，必备软件的ID，必备软件的版本号，必备软件在Ftp服务器下载URL。

### 办公软件库管理

功能说明：对常用办公软件进行管理

实现进度：未完成

实现方案：内网软件库暂时由Ftp服务器代替，服务器端数据库维护办公软件的列表表格，办公软件的ID，办公软件的版本号，办公软件在Ftp服务器下载URL。

### 常用软件库管理

功能说明：对常用软件进行管理

实现进度：未完成

实现方案：内网软件库暂时由Ftp服务器代替，服务器端数据库维护常用软件的列表表格常用软件的ID，常用软件的版本号，常用软件在Ftp服务器下载URL。

### 软件配置管理

功能说明：对所有入库软件进行配置管理，包括软件说明，测试人、上传人等信息进行维护

实现进度：未完成

实现方案：通过Web端上传软件到Ftp服务器，并且与软件下载URL，上传人，测试人，软件说明，版本等可编辑修改的信息关联出一张表格。

## 共享管理

### 文件共享配置管理

功能说明：设置本地共享的目录和文件并设置相应的权限，共享权限包括访问对象及操作权限

实现进度：未完成

实现方案：局域网，文件共享 ，[win32 API](https://msdn.microsoft.com/en-us/library/bb525392(v=vs.85).aspx)提供这一系列的管理功能，还有另外的叫[D-Lan](http://www.d-lan.net/features.html)的共享文件的免费软件，支持很多功能，有共享文件查找等。

## 辅助工具管理

### 业务系统一键安装修复管理

功能说明：CSGII业务系统一键安装及修复工具

实现进度：未完成

实现方案：待定，暂不清楚需求描述。

# 统计分析

## 统计分析

### 统计分析

功能说明：根据系统采集的相关数据，形成相应的统计分析报表，辅助管理人员进行终端安全管理或运维。

实现进度：未完成

实现方案：JEECG内置的highCharts实现图表绘制。