**桌面终端安全管控平台设计方案**

[**版本信息** 2](#_Toc491551646)

[**1. 产品框架** 3](#_Toc491551647)

[**1.1.** **总框架** 3](#_Toc491551648)

[**1.1.1. ICE** 3](#_Toc491551649)

[**1.1.2. 数据传输规范** 3](#_Toc491551650)

[**1.2.** **客户端** 4](#_Toc491551651)

[**1.3.** **服务端** 5](#_Toc491551652)

[**1.3.1. 应用服务器** 5](#_Toc491551653)

[**1.3.2. 数据库服务器** 5](#_Toc491551654)

[**1.3.3. 文件服务器** 5](#_Toc491551655)

[**2. 技术规格** 5](#_Toc491551656)

[**3. 功能定义** 5](#_Toc491551657)

[**3.1.** **客户端** 5](#_Toc491551658)

[**3.1.1. 桌面安全终端管控平台** 5](#_Toc491551659)

[**3.1.2. 守护进程** 19](#_Toc491551660)

[**3.2.** **服务器** 19](#_Toc491551661)

[**3.2.1. 接入适配层服务器** 19](#_Toc491551662)

[**3.2.2. 应用服务器** 19](#_Toc491551663)

[**3.2.3. 数据库服务器** 19](#_Toc491551664)

[**3.2.4. 文件服务器** 19](#_Toc491551665)

**版本信息**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 编写/修改 | 时间 | 审阅 | 说明 |
| 1.0.3 | 肖正龙 | 2017-9-6 |  | 定义客户端和服务器端的ICE接口 |
| 1.0.2 | 肖正龙 | 2017-8-26 |  | 补充完善客户端界面的页面设计，设计深度仅到3级，其余部分有待完善 |
| 1.0.1 | 肖正龙 | 2017-8-25 |  | 根据需求文档完成部分技术设计和规范 |

1. **产品框架**
   1. **总框架**



* + 1. **ICE**

ICE(Internet Communication Engine):实现负载均衡和网络数据的传输

* + 1. **数据传输规范**

所有的数据传输采用zeroC技术框架

* 1. **客户端**



1. **终端客户端程序**：桌面终端安全管控平台操作入口
2. **守护进程**：遵循Fail-Safe原理，一直不间断的监视主程序运行状况，主程序容器一旦意外终止，它会重新启动主程序。以windows 服务的形式提供。
   1. **服务端**



* + 1. **应用服务器**

处理终端应用的应用请求，并根据请求对数据可服务器和文件服务器进行相应的存储和查询

* + 1. **数据库服务器**

存储终端设备信息，用户信息

* + 1. **文件服务器**

作为文件资源服务器，存储应用程序，服务端程序，客户端程序和插件等资源

1. **技术规格**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 设备 | CPU | 内存 | 硬盘 | 操作系统 | 备注 |
| 接入适配层服务器 | CPU1\*4core | >=8G | >=150G | CentOS64 | 按照500并发量设计 |
| 应用层服务器 | CPU2\*4core | >=8G | >=1T | CentOS64 | 按照1500并发量设计 |
| 数据库服务器 | CPU1\*4core | >=8G | >=2T | CentOS64 |  |
| 文件服务器 | CPU1\*4core | >=8G | >=2T | CentOS64 |  |

1. **功能定义**
   1. **客户端**
      1. **桌面安全终端管控平台**

**默认约定**

* 所有的页面是否显示以及是否具备权限均与UKEY的权限挂钩
  + - 1. **终端状态**
         1. **默认信息**

|  |  |
| --- | --- |
| **项目** | **定义** |
| **标识信息** | 终端ID，所属机构信息 |
| **在线情况** | 终端在线情况，UKEY用户在线情况 |
| **流量状态** | 当前实时网速显示 |
| **设备状态** | CPU(当前CPU使用率)/内存(使用率)/磁盘状态(使用率) |



* + - * 1. **进程状态**

|  |  |
| --- | --- |
| **项目** | **定义** |
| **镜像名称** | 进程的名称 |
| **用户名** |  |
| **CPU** | CPU使用率 |
| **内存** | 内存使用率 |
| **描述** | 基本信息描述 |



* + - * 1. **合规报告**

如果存在不合规的软件，列出不合规的软件清单。如果全部正常，则给出当前终端合所有安装软件均合规的信息说明。



* + - * 1. **网络拓扑**

需要和网关系统接通，然后获取当前终端到目标设备的网络拓扑信息，在当前页面显示



* + - * 1. **统计分析**



* + - 1. **系统管理**
         1. **组织机构**

组织机构目前按照总公司，分公司，部门，组4个层级设计，其中组可定义也可以不定义



在该页面的所有操作均与操作权限挂钩，右键点击相应级别的机构，可以对该级别的机构进行[新增/修改/删除]操作

* + - * 1. **人员**



**操作说明**

选中整行，右键单击，则可以进行[修改/删除]的操作

* + - * 1. **数据导入**



* + - 1. **运行管理**
         1. **已安装程序**



* + - * 1. **安全管理**



**使用策略**



**安装策略**



**网络黑白名单**



**共享检测**



**功能可用性检测**



* + - * 1. **系统安全**



**漏洞管理**



**业务环境检测**



* + - 1. **运维管理**
         1. **远程协助**



* + - * 1. **文件消息推送**



**发送**



**查询**



* + - * 1. **终端分组管理**



* + - * 1. **终端及配置策略维护**



* + - * 1. **软件仓库**



* + - * 1. **共享管理**



* + - * 1. **辅助管理**



* + - 1. **资产管理**



* + 1. **守护进程**
  1. **服务器**



* + 1. **ICE**

ICE使用RPC的调用机制，接口定义在ICEDesktopTerm.h文档中

* + - 1. **组织结构**

int OrgGet(SFilterOrg t\_filter,std::vector<SCompany> &t\_lstOrg);//获取组织机构信息

bool OrgMod(int t\_nopt,SObject t\_obj); //增删改组织信息

* + - 1. **人员信息**

int ManGet(SFilterMan t\_filter,std::vector<SMan> &t\_lstOrg);//获取组织机构信息

bool ManMod(int t\_nopt, SObject t\_obj);//增删改组织信息

* + - 1. **设备信息**

int DevGet(SFilterDev t\_filter,std::vector<SDev> &t\_lstDev);//获取设备信息

bool DevMod(int t\_nopt, SMan t\_dev);//增删改设备信息

* + - 1. **策略信息**

int StraGet(SFilerStra t\_filter, std::vector<SStragegy> &t\_lstStra);//获取策略信息

bool StraMod(int t\_nopt, SStragegy t\_stra);//增删改策略信息

* + - 1. **运行信息**

bool RunSave(SRunSoft t\_run);//存储当前运行信息

* + - 1. **软件仓库**

int SoftGet(SFilterSoft t\_filter, std::vector<SRunSoftHouse> &t\_lstOrg);//获取软件信息

bool SoftMod(int t\_nopt, SSoftMsg t\_obj);//增删改软件信息

* + - 1. **报告信息**

int ReportGet(SFilterReport t\_filter, std::vector<SReport> &t\_lstReport);//获取报告信息

* + - 1. **消息**

bool MessageUpdate(SMessage t\_msg); //更新消息

bool MessageAsk(); //订阅消息，消息机制未定参数暂时留空

* + 1. **微服务**
       1. **存储服务**
       2. **查询服务**
       3. **分发服务**
    2. **数据服务**
       1. **数据存储服务器**
       2. **文件服务器**