**基于Windows平台单机版工业终端安全卫士系统需求分析**

修订记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号#** | **作者** | **检查人** | **描述** | **发布日期** |
| 0.1 | 桑安磊 |  | 新建文档 | 2020-6-18 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[1 概述 2](#_Toc43392501)

[1.1 项目背景 2](#_Toc43392502)

[1.2 适用 2](#_Toc43392503)

[1.3 参考文档 2](#_Toc43392504)

[1.4 系统兼容性 2](#_Toc43392505)

[2 系统功能 3](#_Toc43392506)

[2.1 Windows平台单机工业终端安全系统部署结构 3](#_Toc43392507)

[2.2 工业终端安全卫士功能 4](#_Toc43392508)

[2.2.1工业终端安全卫士服务端 4](#_Toc43392509)

[2.2.2 工业终端安全卫士Agent端 5](#_Toc43392510)

[2.2.3 工业终端安全卫士管理工具端 7](#_Toc43392511)

# **概述**

## 项目背景

应项目需要，要开发一款基于windows平台的单机版工业终端安全系统，因公司已有一套成熟的运行在linux平台的工业终端安全系统，linux平台的工业终端安全卫士系统采用分布式部署，基于C/S架构，服务端和客户端分布于网络的不同主机上。

所以windows平台单机版的工业终端安全卫士系统，可参考linux平台的同款产品进行软件功能移植。系统同样基于C/S架构，工业终端安全卫士server端、工业终端安全卫士Client端、管理工具均安装部署在同一台网络上。各种平台的终端agent和管理工具连接到局域网中的windows服务端。

## 适用

本文档适用于软件设计开发人员和测试人员。

## 参考文档

本文档的编写参考了 “工业终端安全卫士系统总体设计方案（Linux）”。

## 系统兼容性

|  |  |  |
| --- | --- | --- |
| 操作系统 | 内核版本 | 硬件平台 |
| Windows 7 | Windows NT 6.1 | X86\_64 |
| Windows Server 2008 R2 | Windows NT 6.1 | X86\_64 |
| Windows 8.0 | Windows NT 6.2 | X86\_64 |
| Windows Server 2012 | Windows NT 6.2 | X86\_64 |
| Windows 8.1 | Windows NT 6.3 | X86\_64 |
| Windows Server 2012 R2 | Windows NT 6.3 | X86\_64 |
| Windows 10 | Windows NT 10.0 | X86\_64 |

# ****系统功能****

## Windows平台单机工业终端安全系统部署结构

选取局域网中一台性能较好的windows主机作为工业终端安全卫士系统的服务器，局域网内各个平台（linux/windows）的客户端和管理工具（linux/windows）都可以登录到服务端，进行信息传输和交互。图2.1a展示了系统的网络结构。

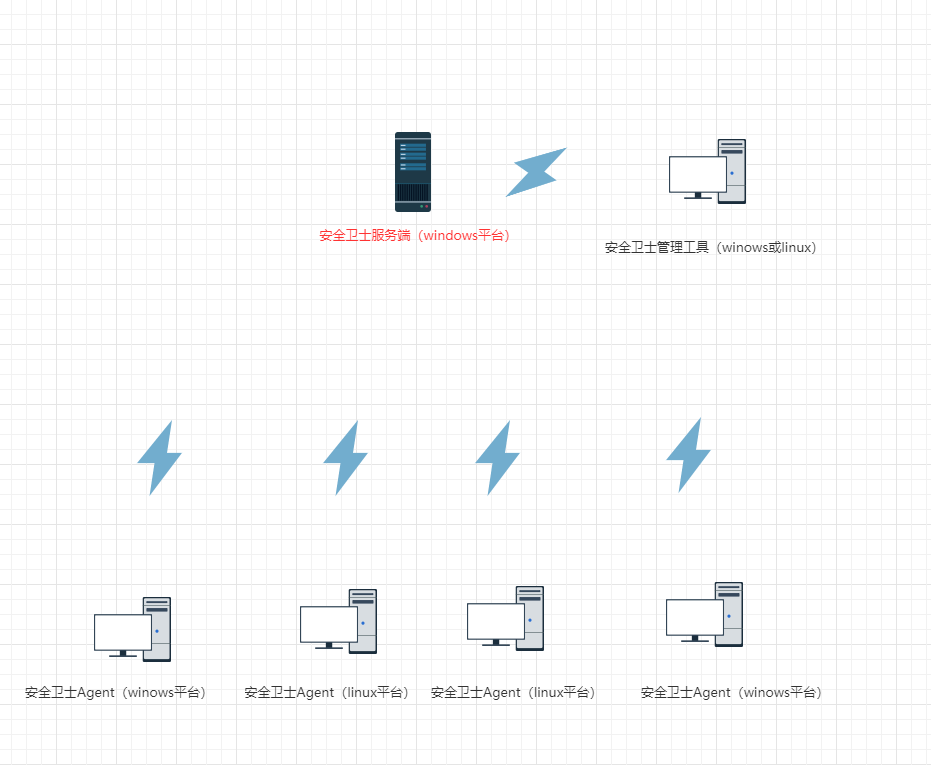


图2.1a（网络部署）

## 工业终端安全卫士功能

工业终端安全卫士软件系统包括服务端、管理端、客户端三部分， 客户端、服务端和和管理界面之间采用进程间通信方式，支持灵活部署和可扩展。



图2.2a（工业终端安全卫士软件系统）

### 2.2.1工业终端安全卫士服务端

服务端可动态分析处理来自客户端上报的事件，综合分析报警和事信息，动态分析检测安全威胁并持续评估风险状况，根据风险情况，形成安全策略下发到对应的客户端，构建持续动态的安全防护平台。服务端数主要负责协议分发，管理每个终端Agent，消息中转、消息分发、数据库管理，界面代理，配置管理等功能，参考图2.2.1a

服务端封装了windows和linux平台的原生网络 socket api，可支持高并发连接，保证数据通信的实时性。

服务端数据库管理系统支持Postgre和MySQL两种类型的数据库，可在两种数据库之间进行自由切换。目前的工业终端系统仅支持mysql，本次追加Postsql的支持，两种数据库可自由切换。



图2.2.1a

### 2.2.2 工业终端安全卫士Agent端

客户端捕获了主机的活动进程、网络连接、服务和自动运行条目、网络和安全事件等基础数据信息，采用主动式欺骗防御技术，实现主机上安全审计、访问控制、进程控制、病毒扫描、完整性监控等功能，形成主机上的可信应用环境。客户端Agent具备访问控制、双因子验证、外部设备访问控制、进程黑白名单、双因子验证、安全审计、基线审核、动态库加载黑白名单、文件完整性检查、防病毒扫描、集中授权管理、进程资源监控、主机防火墙等功能。可参考图2.2.2a



图2.2.2a（工业终端安全卫士Agent功能）

### 2.2.3 工业终端安全卫士管理工具端

管理界面主要是用于对客户端的管理，包括各种策略的配置和流量、安全事件和安全风险状况的报表查看等，是用户与卫士产品交互的主要入口。具体功能参考图2.2.3a。



图2.2.3a（工业安全终端卫士管理工具）