**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](#_Toc43383402)

[1.1 项目背景 2](#_Toc43383403)

[1.2 适用 2](#_Toc43383404)

[1.3 参考文档 2](#_Toc43383405)

[1.4 系统兼容性 2](#_Toc43383406)

[2 详细需求 3](#_Toc43383407)

[2.1 Windows平台单机环境下工业终端安全系统 3](#_Toc43383408)

[2.2 工业终端安全卫士功能 4](#_Toc43383409)

# **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 |

# ****详细需求****

## Windows平台单机环境下工业终端安全系统

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。

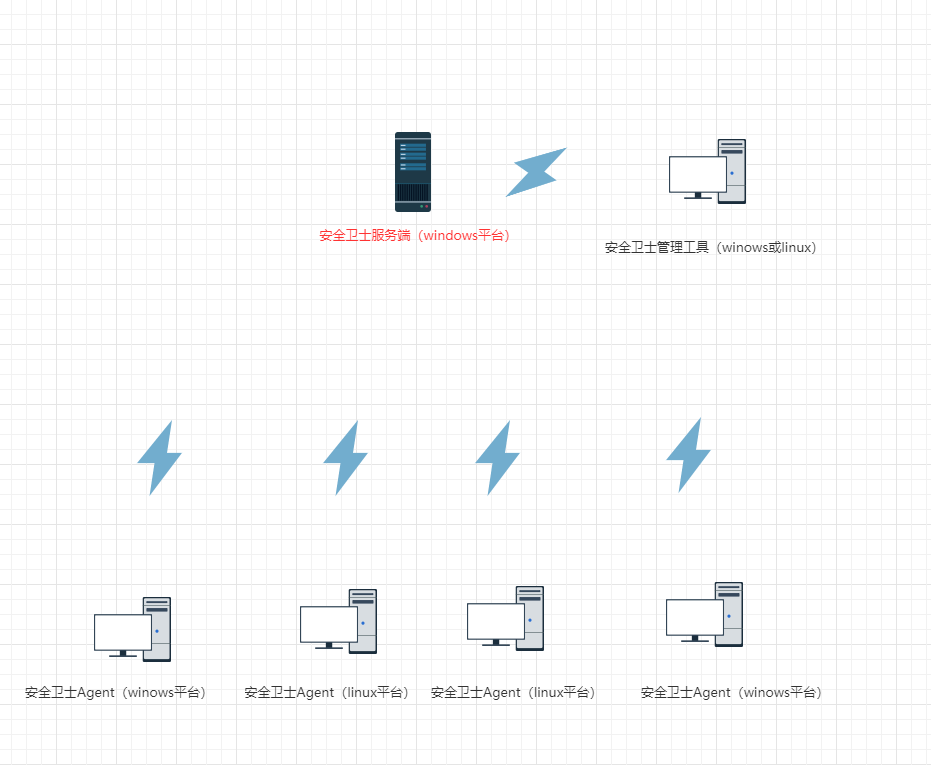


图2.1a（网络部署）

## 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。

1. 服务端要具备消息转发、事件入库，数据库管理，界面代理，配置管理功能。
2. 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。
3. 管理工具实现了配置管理、设备告警管理、事件管理、日志管理、账号管理等功能。



图2.2a（服务端职责功能）