|  |
| --- |
| 360虚拟化安全管理系统 |

**部署环境要求手册**

|  |
| --- |
| ©2020 奇安信集团 |

|  |  |
| --- | --- |
| ■版权声明 | |
| 本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，所有版权均属奇安信集团所有，受到有关产权及版权法保护。任何个人、机构未经奇安信集团的书面授权许可，不得以任何方式复制或引用本文的任何片断。 | |
| 文档修订历史 | Revision History | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **编号** | **修订说明** | **修订日期** | **版本号** | **修订人** | **备注** |
| 1 | 创建 | 2020-08-10 | V1.0 |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| 目 录 | Contents |

[前言 4](#_Toc47955604)

[一、系统介绍 5](#_Toc47955605)

[1.1 产品概述 5](#_Toc47955606)

[1.2 设计理念 5](#_Toc47955607)

[1.3 产品架构 5](#_Toc47955608)

[二. 安装部署环境要求 7](#_Toc47955609)

[2.1服务器准备 7](#_Toc47955610)

[2.2访问控制中心管理平台浏览器要求 8](#_Toc47955611)

[2.3访问控制中心管理平台系统分辨率要求 8](#_Toc47955612)

[2.4终端硬件配置 8](#_Toc47955613)

[2.5终端适配OS及云平台 8](#_Toc47955614)

[2.6网络环境准备 13](#_Toc47955615)

# 前言

* 文档范围

本文档主要介绍360虚拟化终端安全管理系统V7.0T01R01P004U2B17H07的安装和初始化配置，主要包括系统简介、安装环境的准备、360虚拟化控制中心的安装与卸载、客户端的安装与卸载、系统基本配置。

* 文档对象

本文档主要适合希望了解360虚拟化终端安全管理系统安装和部署的用户、系统管理员、工程师进行阅读。

* 获取帮助

您可以访问 “<https://www.qianxin.com/>” 获取360虚拟化安全的最新动态和360虚拟化终端安全管理系统相关的资料，同时您可以通过下面的联系方式与我们联系。

|  |
| --- |
| 地址：北京市朝阳区酒仙桥6号电子城国际电子总部B座  电话：+86（10）57836300  传真：+86（10）57836303  奇安信客服热线：4008-136-360 / 400-678-3600  奇安信服务邮箱：[kefu@qianxin.com](mailto:kefu@qianxin.com) |

一、系统介绍

## 产品概述

360虚拟化安全系统是一个能够为虚拟化环境提供安全能力的软件系统。该系统采用轻代理模式，并融合了私有云技术，使得产品能够支持多种虚拟化平台。

360虚拟化安全系统能够满足虚拟化终端的安全需要，提高虚拟化环境下安全软件的运行效率，有效降低虚拟化环境下安全软件对虚拟化平台的资源占用。

360虚拟化安全系统具有终端管理、杀毒管理、日志报告和终端配置等主要功能。

## 设计理念

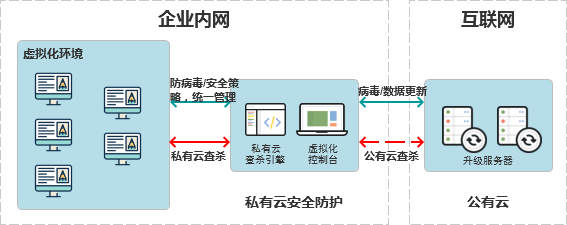
* **立体防护**

360虚拟化终端具有病毒木马查杀、黑白名单等多样化的防护手段，为用户构建立体防护网，确保企业终端安全。

* **安全管控**

360虚拟化控制中心为管理员提供了统一杀毒、统一升级、流量管理、终端安全策略管理等多种管理功能，管理员可以通过控制台直接对网内所有终端进行统一管控。

## 产品架构



*图：360虚拟化产品架构图*

360虚拟化终端安全管理系统包括安全控制中心和客户端两部分。

* **控制中心**

安全控制中心是360虚拟化终端安全管理系统的核心，部署在服务器端，主要包括安全管控和安全事件收集告警两大功能。

安全控制中心采用B/S架构，管理员可以随时随地的通过浏览器打开访问，对360虚拟化终端进行管理和控制。主要有分组管理、策略制定下发、全网健康状况监测、统一杀毒、网络流量管理等。安全此外安全控制中心还提供了系统运维的基础服务，如：云查杀服务、终端升级服务、数据服务、通讯服务等。

安全事件收集告警，通过管控中心，管理员可以了解全网终端的告警信息，通过报表分析，掌握全网威胁状况。

* **客户端**

客户端部署在需要被保护的终端或服务器上，执行最终的木马病毒查杀、安全防护等安全操作。并与安全控制中心通信，提供控制中心管理所需的相关安全告警信息。

# 安装部署环境要求

### 2.1服务器准备

360虚拟化安全管理系统安全控制中心支持部署在硬件服务器和虚拟化服务器上，在对安全控制中心进行安装时需要提前根据如下要求准备对应的服务器环境。

建议的服务器配置为：

|  |  |  |
| --- | --- | --- |
| **所需配置类型** | | **配置内容** |
| 硬件 | CPU  (类型:不支持sse4\_2指令集) | 500终端最低8核2.4Ghz；  1000终端最低16核2.4Ghz；  5000及以上终端最低32核2.4Ghz(没有实际数据支撑，可能存在误差) |
| 内存 | 500终端最低8GB；  1000终端最低16GB；  5000及以上终端最低32GB(没有实际数据支撑，可能存在误差) |
| 硬盘 | 最低500GB可用空间，推荐1T |
| 网卡 | 一块千兆以太网卡 |
| 鼠标、键盘、显示器 | 普通 |
| 软件 | 操作系统 | 安全控制中心支持安装在如下操作系统平台：  CentOS 6.8 x86\_64、  CentOS 6.9 x86\_64、  CentOS 7.0 x86\_64、  CentOS 7.1 x86\_64、  CentOS 7.2 x86\_64、  CentOS 7.3 x86\_64、  CentOS 7.4 x86\_64、  CentOS 7.5 x86\_64、  CentOS 7.6 x86\_64、  Red Hat 7.3 x86\_64 |

用iso包安装的时候，创建虚拟机时，空间分配必须大于20G 否则会安装失败！

说明

|  |
| --- |
| 1）虚拟化安全控制中心安装程序自带高性能数据库，因此不需要单独准备数据库软件；  2）实际环境中的服务器配置请根据实际需求和环境进行规划； |

### 2.2访问控制中心管理平台浏览器要求

要正常使用控制中心的所有功能，推荐使用chrome 43.0及以上版本的Web浏览器来访问控制中心的Web管理平台。

### 2.3访问控制中心管理平台系统分辨率要求

要正常使用控制中心的所有功能，推荐将系统分辨率设置在1366\*768及以上。

### 2.4终端硬件配置

|  |  |  |
| --- | --- | --- |
| **所需配置类型** | | **配置内容** |
| 硬件 | CPU | 最低2核2.4Ghz； |
| 内存 | 4GB； |
| 硬盘 | 最低40GB可用空间 |
| 网卡 | 一块千兆以太网卡 |
| 鼠标、键盘、显示器 | 普通 |

### 2.5终端适配OS及云平台

360虚拟化安全管理客户端支持部署在如下操作系统类型上：

|  |  |  |
| --- | --- | --- |
| 系统类型 | 操作系统 | 是否支持 |
| Windows服务器版 | Windows 2003 Server R2 SP2 x64 | 支持 |
| Windows 2003 Server R2 SP2 x86 | 支持 |
| Windows 2003 Server SP1 x86 | 支持 |
| Windows 2003 Server SP2 x64 | 支持 |
| Windows 2003 Server SP2 x86 | 支持 |
| Windows 2008 Server R2 x64 | 支持 |
| Windows 2008 Server x64 | 支持 |
| Windows 2012 Server R2 x64 | 支持 |
| Windows 2012 Server x64 | 支持 |
| Windows 2016 Server x64 | 支持 |
| Windows 2019 Server x64 | 支持 |
| Windows XP SP3 x86 | 支持 |
| Windows 7 SP1 x64 | 支持 |
| Windows 7 SP1 x86 | 支持 |
| Windows 7 x64 | 支持 |
| Windows 8 x64 | 支持 |
| Windows 10 x64 | 支持 |
| Linux服务器版 | CentOS(5.3、5.5、5.11、6.1、6.2、6.3、6.5、6.6、6.7、6.8、6.9、6.10、7.0、7.1、7.2、7.3、7.4、7.5、7.6、7.7) x86\_64 | 支持 |
| RedHat Enterprise(5.3、5.4、5.5、5.8、5.9、5.11、6.1、6.2、6.3、6.4、6.5、6.6、6.7、6.8、6.9、7.1、7.2、7.3、7.4、7.5) x86\_64 | 支持 |
| Ubuntu (10.04 LTS、12.04 LTS、14.04 LTS、16.04 LTS、18.04 LTS) x86\_64 | 支持 |
| SUSE(11 SP1、11 SP2、11 SP3、11 SP4、12 SP1、12 SP2) x86\_64 | 支持 |
| Debian(7、8、9) x86\_64 | 支持 |
| Oracle Linux(5、5.8、6.3、7.0) x86\_64 | 支持 |
| Asianux (3、4) x86\_64 | 支持 |
| Deepin(14、15) x86\_64 | 支持 |
| 麒麟Kylin(3.2.8、4.0.2、4.0.2 SP1) x86\_64 | 支持 |
| 中标麒麟NeoKylin(6.5、6.7、7.0、7.2、7.4 adv) x86\_64 | 支持 |
| Citrix XenServer | Citrix XenServer 6.5(build 6.5.2.2510)64位 | 支持 |
| VMware | VMware vSphere5.0、5.1、5.5、6.0、6.5、6.7 | 支持 |
| H3C | H3CV2.0 D0218、H3CAS E0306、 H3C CAS2.0 E0218H07、H3C CAS3.0 E0306H06 H3C CAS5.0 E0503 | 支持 |
| Hyper-V | Hyper-V 2008、Hyper-V 2012、Hyper-V 2016 | 支持 |
| EasyStack | OpenStack L | 支持 |
| 九州云 | 九州云 | 支持 |
| 浪潮 | Incloud OpenStack 云海服务器虚拟化系统 Incloud Sphere V5 浪潮超融合一体机 Incloud Rail | 支持 |
| 航盾 | 航盾BAOMI\_HDVE\_V3.6.2.1 | 支持 |
| OpenStack | OpenStack Liberty K、L、M、N、O、P | 支持 |
| 深信服超融合Sangfor | VMP 5.3.8R2 | 支持 |
| openstack rocky | openstack rocky | 支持 |
| 烽火云 | OpenStack pike | 支持 |
| Huawei | FusionCompute V100R005C10SPC700 基础版 FusionCompute V100R003C10SPC600 FusionCompute V100R006C10 基础版 FusionSphere OpenStack V100R006C10SPC500 FusionCompute V100R006C00U1高级版本 FusionCompute 6.3.0  FusionCompute 6.5.0  FusionCompute 6.5.1  FusionSphere OpenStack V100R006C30SPC200 | 支持 |
| Huawei ManageOne | ManageOne 6.3.0、6.3.1 | 支持 |
| 云联万维 | Yunion OneCloud 2.0.0 企业版、2.0.15企业版 | 支持 |
| 航天云宏 | WinCenter 7.1 | 支持 |
| 中标麒麟云平台 | Kylin 7.0 | 支持 |

产品功能支持：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 功能模块  操作系统 | 病毒扫描 | Webshell | 安全基线 | 防火墙 | 入侵防御 | 防暴力破解 | 虚拟化加固 | 网卡流量统计 |
| Asianux 3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Asianux 4 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 5.11 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 5.3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 5.5 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.0 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.1 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.2 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.5 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.6 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.7 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.8 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.9 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 6.10 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.0 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.1 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.2 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.4 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.5 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.6 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| CentOS 7.7 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Debian 7 x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| Debian 8 x86\_64 | √ | × | √ | √ | × | × | √ | √ |
| Debian 9 x86\_64 | √ | × | √ | √ | × | √ | √ | √ |
| Deepin 14 x86\_64 | √ | × | √ | √ | × | × | × | √ |
| Deepin 15 x86\_64 | √ | × | √ | √ | × | √ | √ | √ |
| 麒麟Kylin 3.2.8 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| 麒麟Kylin 4.0.2 x86\_64 | √ | × | √ | √ | × | √ | × | √ |
| 麒麟Kylin 4.0.2 sp1 x86\_64 | √ | √ | √ | √ | × | × | × | √ |
| 中标麒麟Neokylin 6.5 adv x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| 中标麒麟NeoKylin 6.7 adv x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| 中标麒麟Neokylin 7.0 x86\_64 | √ | √ | √ | × | × | √ | √ | √ |
| 中标麒麟Neokylin 7.2 adv x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| 中标麒麟Neokylin 7.4 adv x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| 功能模块  操作系统 | 病毒扫描 | Webshell | 安全基线 | 防火墙 | 入侵防御 | 防暴力破解 | 虚拟化加固 | 网卡流量统计 |
| Oracle Linux 5 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Oracle Linux 5.8 x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| Oracle Linux 6.3 x86\_64 | √ | √ | √ | √ | × | √ | √ | √ |
| Oracle Linux 7.0 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 5.11 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 5.3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 5.4 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 5.5 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 5.8 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 5.9 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.1 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.2 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.4 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.5 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.6 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.7 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.8 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 6.9 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 7.1 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 7.2 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 7.3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 7.4 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| RedHat Enterprise 7.5 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| SUSE 11 SP1 x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| SUSE 11 SP2 x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| SUSE 11 SP3 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| SUSE 11 SP4 x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| SUSE 12 SP1 x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| SUSE 12 SP2 x86\_64 | √ | √ | √ | √ | √ | √ | √ | √ |
| EulerOS V2.0 SP5 | √ | √ | √ | √ | √ | √ | √ | √ |
| Ubuntu 10.04 LTS x86\_64 | √ | √ | √ | √ | × | √ | √ | √ |
| Ubuntu 12.04 LTS x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| Ubuntu 14.04 LTS x86\_64 | √ | × | √ | √ | √ | √ | √ | √ |
| Ubuntu 16.04 LTS x86\_64 | √ | √ | √ | √ | × | √ | × | √ |
| Ubuntu 18.04 LTS x86\_64 | √ | √ | √ | √ | × | √ | √ | √ |
| Windows 2003 Server R2 SP2 x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2003 Server R2 SP2 x86 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2003 Server SP1 x86 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2003 Server SP2 x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2003 Server SP2 x86 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2008 Server R2 x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2008 Server x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2012 Server R2 x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2012 Server x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2016 Server x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2019 server x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows XP SP3 x86 | √ | √ | √ | √ | √ | × | √ | √ |
| Windows 7 SP1 x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 7 SP1 x86 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 7 x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 8 x64 | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 10 x64 | √ | √ | √ | √ | √ | √ | √ | √ |

备注: x86\_64 指的是64位系统

### 2.6网络环境准备

* IP地址准备

需要为虚拟化安全控制中心服务器准备一个固定IP地址，同时为了保证360虚拟化安全管理系统安全控制中心服务器能够正常的对客户端进行管理，需要保证客户端网络到服务器网络全局路由可达。

* 网络权限

如果在网络中间存在访问控制策略（如防火墙策略、ACL等）则需要按照如下表格对相关端口进行放行：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 类型 | 源IP | 源端口 | 目的IP | 目的端口 | 协议 | 功能 |
| 服务器 | any(需要访问web页面的所有地址) | any | 控制中心 | 8443 | TCP | 用户操作web控制台 |
| 服务器 | any(部署终端的所有地址) | any | 控制中心 | 8090  8080 | TCP | 终端与控制中心通信 |
| 服务器 | 控制中心 | any | 私有云鉴定中心IP(可配置) | 私有云鉴定中心(可配置) | TCP | 鉴定中心连接测试 |

说明

|  |
| --- |
| 以上均为系统默认端口，如果实施过程中对默认端口进行了修改，则应该按照实际的端口进行放行。 |