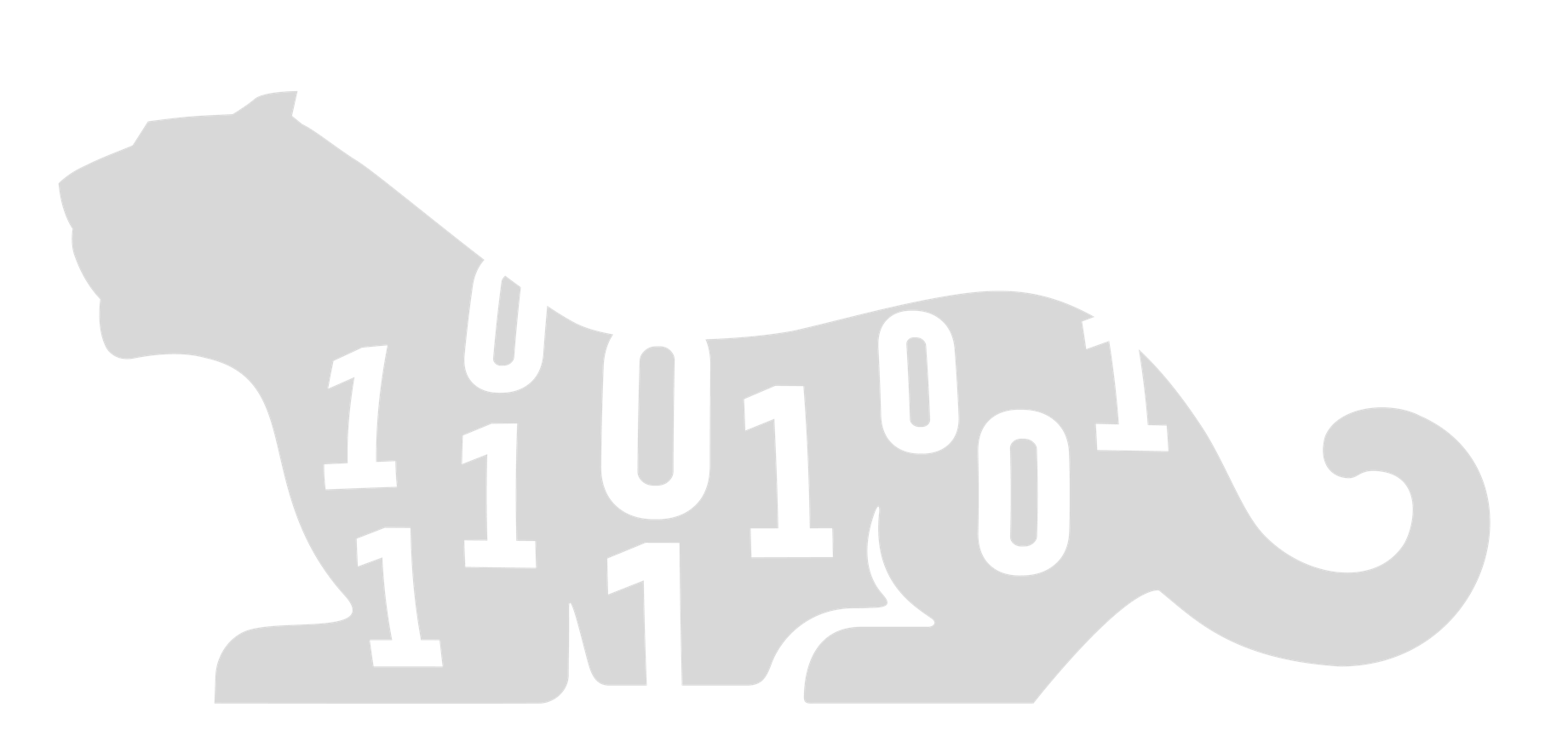
**奇安信网神统一服务器安全管理系统V8.0.0（有代理）**

**通用测试指南**



地址：北京市西城区西直门外南路26号院1号

邮编：100044

* **版权声明**

本文中出现的任何文字叙述、文档格式、插图、图片、方法、过程等内容，除另有特别注明，版权均为**奇安信集团（指包括但不限于奇安信科技集团股份有限公司、网神信息技术（北京）股份有限公司、北京网康科技有限公司）**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段。

修订记录

|  |  |  |
| --- | --- | --- |
| **修订日期** | **修订内容** | **修订人** |
| 20200616 | 修改用例 | 云安全事业部 |
|  |  |  |
|  |  |  |

目录

[1. 概述 7](#_Toc43215759)

[1.1. 测试背景 7](#_Toc43215760)

[1.2. 测试环境 7](#_Toc43215761)

[1.3. 测试安排 7](#_Toc43215762)

[1.3.1. 测试人员 7](#_Toc43215763)

[1.3.2. 测试时间及安排 7](#_Toc43215764)

[2. 安装部署 8](#_Toc43215765)

[2.1. 轻代理计算机安装安全组件 8](#_Toc43215766)

[2.1.1. 轻代理Windows安装安全组件 8](#_Toc43215767)

[2.1.2. 轻代理Linux安装安全组件（root或sudo免密） 8](#_Toc43215768)

[2.1.3. 轻代理Linux安装安全组件（sudo且需要免密） 9](#_Toc43215769)

[2.1.4. 轻代理Linux安装安全组件（su切换到root） 10](#_Toc43215770)

[2.1.5. 轻代理Linux安装安全组件（不使用ssh默认端口） 11](#_Toc43215771)

[3. 功能测试 12](#_Toc43215772)

[3.1. 防病毒增强 12](#_Toc43215773)

[3.1.1. 快速扫描 12](#_Toc43215774)

[3.1.2. 全盘扫描 13](#_Toc43215775)

[3.1.3. 防病毒监控 14](#_Toc43215776)

[3.1.4. 防病毒隔离 14](#_Toc43215777)

[3.1.5. 防病毒修复 15](#_Toc43215778)

[3.1.6. 防病毒删除 16](#_Toc43215779)

[3.1.7. 指定虚拟机目录扫描 17](#_Toc43215780)

[3.1.8. 实时防护 18](#_Toc43215781)

[3.1.9. 定期扫描 18](#_Toc43215782)

[3.1.10. 文件白名单 19](#_Toc43215783)

[3.1.11. 目录白名单 20](#_Toc43215784)

[3.1.12. 文件后缀名白名单 21](#_Toc43215785)

[3.1.13. 仅扫描目录 21](#_Toc43215786)

[3.1.14. 仅扫描指定后缀名文件 22](#_Toc43215787)

[3.1.15. 压缩文件扫描 23](#_Toc43215788)

[3.1.16. 多引擎测试(AVE引擎) 23](#_Toc43215789)

[3.1.17. 多引擎测试(QEX引擎) 24](#_Toc43215790)

[3.1.18. 多引擎测试(BD引擎) 25](#_Toc43215791)

[3.1.19. 云查测试 26](#_Toc43215792)

[3.1.20. 自保护(文件保护) 27](#_Toc43215793)

[3.1.21. 自保护(进程保护) 27](#_Toc43215794)

[3.1.22. 扫描资源占用 28](#_Toc43215795)

[3.1.23. Powershell扫描-计划任务 28](#_Toc43215796)

[3.1.24. Powershell扫描-注册表 30](#_Toc43215797)

[3.1.25. 内存扫描-1 31](#_Toc43215798)

[3.1.26. 内存扫描-2 31](#_Toc43215799)

[3.2. Webshell扫描 32](#_Toc43215800)

[3.2.1. 轻代理Windows虚拟机webshell扫描 33](#_Toc43215801)

[3.2.2. 轻代理Linux虚拟机webshell扫描 34](#_Toc43215802)

[3.2.3. 定期扫描 35](#_Toc43215803)

[3.2.4. Webshell手动扫描自定义目录 36](#_Toc43215804)

[3.2.5. Webshell白名单手动扫描 37](#_Toc43215805)

[3.3. 应用程序控制 39](#_Toc43215806)

[3.3.1. 阻止应用程序路径 39](#_Toc43215807)

[3.3.2. 阻止应用程序名 40](#_Toc43215808)

[3.3.3. 例外应用程序路径-1 41](#_Toc43215809)

[3.3.4. 例外应用程序路径-2 42](#_Toc43215810)

[3.3.5. 监控应用程序路径 43](#_Toc43215811)

[3.3.6. 监控应用程序名 44](#_Toc43215812)

[3.4. 完整性监控 45](#_Toc43215813)

[3.4.1. 实时监控轻代理Windows文件的删除 45](#_Toc43215814)

[3.4.2. 手动扫描监控文件的增加 46](#_Toc43215815)

[3.4.3. 手动扫描监控文件的删除 47](#_Toc43215816)

[3.4.4. 手动扫描监控注册表的增加 48](#_Toc43215817)

[3.4.5. 手动扫描监控轻代理Windows进程的创建 49](#_Toc43215818)

[3.4.6. 手动扫描监控轻代理Windows服务的创建 50](#_Toc43215819)

[3.4.7. 手动扫描监控轻代理Windows端口的添加 51](#_Toc43215820)

[3.5. 漏洞管理 52](#_Toc43215821)

[3.5.1. 轻代理Windows虚拟机漏洞扫描 53](#_Toc43215822)

[3.5.2. 轻代理Linux虚拟机漏洞扫描 53](#_Toc43215823)

[3.5.3. 定期扫描 54](#_Toc43215824)

[3.6. 安全基线 55](#_Toc43215825)

[3.6.1. 轻代理Windows虚拟机安全基线扫描 55](#_Toc43215826)

[3.6.2. 轻代理Linux虚拟机安全基线扫描 56](#_Toc43215827)

[3.6.3. 定期扫描 57](#_Toc43215828)

[3.7. 防暴力破解 58](#_Toc43215829)

[3.7.1. 轻代理Windows虚机rdp协议测试 58](#_Toc43215830)

[3.7.2. 轻代理Linux虚机ssh协议测试 59](#_Toc43215831)

[3.7.3. 轻代理Linux虚机telnet协议测试 60](#_Toc43215832)

[3.7.4. 防暴力破解白名单测试 61](#_Toc43215833)

[3.7.5. 防暴力破解黑名单测试 62](#_Toc43215834)

[3.8. 防火墙功能 63](#_Toc43215835)

[3.8.1. 防火墙规则ICMP出站 63](#_Toc43215836)

[3.8.2. 防火墙规则ICMP入站 63](#_Toc43215837)

[3.8.3. 防火墙TCP入站 64](#_Toc43215838)

[3.8.4. 防火墙TCP出站 65](#_Toc43215839)

[3.8.5. 防火墙UDP入站 66](#_Toc43215840)

[3.8.6. 防火墙UDP出站 66](#_Toc43215841)

[3.8.7. 修改防火墙规则状态 67](#_Toc43215842)

[3.9. 失陷检测 68](#_Toc43215843)

[3.9.1. 失陷主机隔离 68](#_Toc43215844)

[3.9.2. 失陷主机监控 69](#_Toc43215845)

[3.9.3. 威胁情报-隔离 71](#_Toc43215846)

[3.9.4. 威胁情报-监控 72](#_Toc43215847)

[3.10. 入侵防御 73](#_Toc43215848)

[3.10.1. 入侵防御阻止测试-1 73](#_Toc43215849)

[3.10.2. 入侵防御阻止测试-2 74](#_Toc43215850)

[3.10.3. 入侵防御检测测试 75](#_Toc43215851)

[3.10.4. 入侵防御白名单 76](#_Toc43215852)

[3.11. 网络可视化及管理 77](#_Toc43215853)

[3.11.1. 网络可视化及管理（网站） 78](#_Toc43215854)

[3.11.2. 网络可视化及管理（网络基础服务）-1 79](#_Toc43215855)

[3.11.3. 网络可视化及管理（网络基础服务）-2 80](#_Toc43215856)

[3.12. 虚拟机/终端策略 81](#_Toc43215857)

[3.12.1. 防恶意软件 81](#_Toc43215858)

[3.12.2. Webshell扫描 82](#_Toc43215859)

[3.12.3. 应用程序控制 83](#_Toc43215860)

[3.12.4. 完整性监控 84](#_Toc43215861)

[3.12.5. 漏洞管理 85](#_Toc43215862)

[3.12.6. 安全基线 86](#_Toc43215863)

[3.12.7. 防暴力破解 87](#_Toc43215864)

[3.12.8. 防火墙 88](#_Toc43215865)

[3.12.9. 失陷检测 89](#_Toc43215866)

[3.12.10. 入侵防御 90](#_Toc43215867)

[3.12.11. 网络可视化及管理 91](#_Toc43215868)

[4. 产品管理功能 92](#_Toc43215869)

[4.1. 分组管理 92](#_Toc43215870)

[4.1.1. 分组及规则 92](#_Toc43215871)

[4.1.2. 匹配规则 93](#_Toc43215872)

[4.2. 配置维护 93](#_Toc43215873)

[4.3. 域名解析 95](#_Toc43215874)

[4.3.1. 新增域名解析记录 95](#_Toc43215875)

[4.3.2. 删除域名解析记录 95](#_Toc43215876)

[4.3.3. 修改主机名 96](#_Toc43215877)

[4.4. 通用设置 96](#_Toc43215878)

[4.4.1. 配置NTP服务器 96](#_Toc43215879)

[5. 性能测试 97](#_Toc43215880)

[6. 测试总结 98](#_Toc43215881)

# 概述

## 测试背景

因业务发展需要，*[添加客户名称]*为内部员工提供虚拟化资源池，以此优化现有硬件资源，降低硬件采购成本，提高资源使用率。与此同时，虚拟化环境面临的杀毒问题，无法采用传统杀毒软件有效解决。虚拟化环境下的安全防护，需要考虑保障原有资源的高效利用，同时不影响现有虚拟机系统里正在运行的系统。奇安信集团为*[添加客户名称] [添加客户虚拟化环境]*环境下有代理防护需求，提供奇安信网神虚拟化安全作为产品功能测试和验证。

## 测试环境

*[添加客户实际搭建测试环境]*

## 测试安排

### 测试人员

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 部门 | 姓名 | 角色 | 联系方式 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 测试时间及安排

*[添加客户测试安排计划时间]*

# 安装部署

## 轻代理计算机安装安全组件

### 轻代理Windows安装安全组件

|  |  |
| --- | --- |
| **测试项目** | **轻代理Windows安装安全组件** |
| 测试步骤 | * 进入 管理中心 资产管理-主机 页面，勾选一个轻代理windows主机，点击“安装安全组件”按钮 * 在安装安全组件页面，操作系统选择Windows，主机用户名填写管理员用户名Administrator及对应的密码 * 许可类型根据Windows系统选择桌面版或者服务器版（例如Win7就选择桌面版，Windows2012R2就选择服务器版） * 点击 确定 按钮提交，等待大约2分钟后查看安装结果 |
| 预期结果 | * 1. 安装安全组件页面能正常弹出，各选择框、输入框功能正常 * 2. 能正常提交成功 * 3. 安装成功，状态显示 安装成功 * 4. 再等待2分钟后，会显示系统信息和特征库信息 |

### 轻代理Linux安装安全组件（root或sudo免密）

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux安装安全组件（root或sudo免密）** |
| 测试步骤 | * 进入 管理中心 资产管理-主机 页面，勾选一个轻代理linux主机，点击“安装安全组件”按钮 * 在 主机用户名 输入框输入 linux服务器上已存在的用户名（比如testsec）以及对应的密码 * 获取管理员权限选择“root或sudo免密”（需要在主机文件/etc/sudoers中添加<username> ALL=(ALL) NOPASSWD:ALL） * 点击 确定 按钮提交，等待大约2分钟后查看安装结果 |
| 预期结果 | * 1. 安装安全组件页面能正常弹出，各选择框、输入框功能正常 * 2. 能正常提交成功 * 3. 安装成功，状态显示 安装成功 * 4. 再等待2分钟后，会显示系统信息和特征库信息 |

### 轻代理Linux安装安全组件（sudo且需要免密）

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux安装安全组件（sudo且需要免密）** |
| 测试步骤 | * 进入 管理中心 资产管理-主机 页面，勾选一个轻代理linux主机，点击“安装安全组件”按钮 * 在 主机用户名 输入框输入linux服务器上已存在的用户名（比如testsec）以及对应的密码 * 获取管理员权限选择“sudo且需要密码”（需要在主机文件/etc/sudoers中添加<username> ALL=(ALL) ALL） * 点击 确定 按钮提交，等待大约2分钟后查看安装结果 |
| 预期结果 | * 1. 安装安全组件页面能正常弹出，各选择框、输入框功能正常 * 2. 能正常提交成功 * 3. 安装成功，状态显示 安装成功 * 4. 再等待2分钟后，会显示系统信息和特征库信息 |

### 轻代理Linux安装安全组件（su切换到root）

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux安装安全组件（su切换到root）** |
| 测试步骤 | * 进入 管理中心 资产管理-主机 页面，勾选一个轻代理linux主机，点击“安装安全组件”按钮 * 在 主机用户名 输入框输入linux服务器上已存在的用户名（比如testsec）以及对应的密码 * 获取管理员权限选择“su切换到root” * 弹出的ROOT密码输入框填入主机root密码 * 点击 确定 按钮提交，等待大约2分钟后查看安装结果 |
| 预期结果 | * 1. 安装安全组件页面能正常弹出，各选择框、输入框功能正常 * 2. 能正常提交成功 * 3. 安装成功，状态显示 安装成功 * 4. 再等待2分钟后，会显示系统信息和特征库信息 |

### 轻代理Linux安装安全组件（不使用ssh默认端口）

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux安装安全组件（不使用ssh默认端口）** |
| 测试步骤 | * 进入 管理中心 资产管理-主机 页面，勾选一个轻代理linux主机，点击“安装安全组件”按钮 * 在 主机用户名 输入框输入linux服务器上已存在的用户名（比如testsec）以及对应的密码 * 获取管理员权限选择“su切换到root” * 弹出的ROOT密码输入框填入主机root密码 * SSH端口填写6000   （需要修改/etc/ssh/sshd\_config，把要使用的端口添加进去，Port 22前的#去掉，新增Port 6000保存，重启sshd服务）   * 点击 确定 按钮提交，等待大约2分钟后查看安装结果 |
| 预期结果 | * 1. 安装安全组件页面能正常弹出，各选择框、输入框功能正常 * 2. 能正常提交成功 * 3. 安装成功，状态显示 安装成功 * 4. 再等待2分钟后，会显示系统信息和特征库信息 |

# 功能测试

## 防病毒增强

本类用例主要测试奇安信网神统一服务器安全管理系统（有代理）的防病毒增强相关功能。

### 快速扫描

|  |  |
| --- | --- |
| **测试项目** | **快速扫描测试** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态关闭，手动/定期扫描的恶意软件处理选择删除 * 拷贝测试病毒至虚拟机中 * 在虚拟机页面，选择对应的虚拟机，点击 安全操作->快速扫描 * 查看虚拟机中病毒文件是否被系统检测并删除 * 管理中心是否会产生病毒删除日志 |
| 预期结果 | * 1. 安全配置编辑成功 * 2. 病毒文件拷贝成功 * 3.系统开始对虚拟机进行全盘扫描,虚拟机右侧的“防恶意软件状态”栏会显示扫描进度和扫描结果 * 4.虚拟机中病毒文件被成功删除 * 5.分析-防恶意软件页面中显示了病毒查杀的日志，被删除的文件不可恢复 |

### 全盘扫描

|  |  |
| --- | --- |
| **测试项目** | **全盘扫描测试** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态关闭，手动/定期扫描的恶意软件处理选择隔离 * 拷贝测试病毒至虚拟机中 * 在虚拟机页面，选择对应的虚拟机，点击 安全操作->全盘扫描 * 查看虚拟机中病毒文件是否被系统检测并隔离 * 管理中心是否会产生病毒隔离日志 |
| 预期结果 | * 安全配置编辑成功 * 病毒文件拷贝成功 * 系统开始对虚拟机进行全盘扫描,虚拟机右侧的“防恶意软件状态”栏会显示扫描进度和扫描结果 * 虚拟机中病毒文件被成功隔离 * 分析-防恶意软件页面中显示了病毒隔离的日志，被隔离的文件在虚拟机中可以手动恢复 |

### 防病毒监控

|  |  |
| --- | --- |
| **测试项目** | **恶意软件处理动作为监控** |
| 测试步骤 | * 1. 进入 管理中心 资产管理-虚拟机/终端 页面，将虚拟机安全配置中的实时防护状态打开，恶意软件处理配置为监控 * 2. 拷贝测试病毒至虚拟机/root/virus/目录中 * 3. 查看病毒文件是否被删除或隔离 * 4. 系统是否有病毒文件的监控日志 |
| 预期结果 | * 安全配置编辑成功 * N/A * 病毒文件仍然在/root/virus/中 * 管理中心记录了病毒文件的监控日志 |

### 防病毒隔离

|  |  |
| --- | --- |
| **测试项目** | **恶意软件处理动作为隔离** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将虚拟机安全配置中的实时防护状态打开，恶意软件处理配置为隔离 * 拷贝测试病毒至虚拟机/root/virus/目录中 * 查看病毒文件是否被隔离 * 系统是否有病毒文件的隔离日志 |
| 预期结果 | * 病毒文件被隔离 * N/A * 病毒文件被成功隔离 * 分析-防恶意软件页面中显示了病毒隔离的日志，被隔离的文件在虚拟机中可以手动恢复 |

### 防病毒修复

|  |  |
| --- | --- |
| **测试项目** | **恶意软件处理动作为修复** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将虚拟机安全配置中的实时防护状态打开，恶意软件处理配置为修复 * 拷贝测试病毒至虚拟机/root/virus/目录中 * 查看病毒文件是否被修复 * 系统是否有病毒文件的修复日志，如果文件修复不了，是否采取隔离处理 |
| 预期结果 | * N/A * 病毒文件被成功修复，没有被修复的文件做隔离处理 * 分析-防恶意软件页面中显示了病毒修复的日志，没有被修复的文件做隔离处理，被隔离的文件在虚拟机中可以手动恢复 |

### 防病毒删除

|  |  |
| --- | --- |
| **测试项目** | **恶意软件处理动作为删除** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将虚拟机安全配置中的实时防护状态打开，恶意软件处理配置为删除 * 拷贝测试病毒至虚拟机/root/virus/目录中 * 查看病毒文件是否被删除 * 系统是否有病毒文件的删除日志 |
| 预期结果 | * 策略下发成功 * N/A * 病毒文件被成功删除 * 分析-防恶意软件页面中显示了病毒被删除的日志 |

### 指定虚拟机目录扫描

|  |  |
| --- | --- |
| **测试项目** | **扫描指定目录** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态关闭，手动/定期扫描的恶意软件处理配置为删除 * 拷贝测试病毒分别至虚拟机的/root/virus/目录和/root/normal/目录中 * 在虚拟机页面，选择对应的虚拟机，点击 安全操作->扫描指定目录 * 在打开的对话框中配置需要扫描的目录为/root/virus/ * 查看虚拟机/root/virus/和/root/normal/目录中的病毒文件是否被系统检测并删除，并有病毒查杀日志 |
| 预期结果 | * 安全配置编辑成功 * N/A * N/A * 系统开始对指定的虚拟机目录进行扫描,虚拟机右侧的“防恶意软件状态”栏会显示扫描进度和扫描结果 * /root/virus/目录中的病毒文件被成功删除，分析-防恶意软件页面中显示了病毒查杀的日志，/root/normal/目录中的病毒文件没有被删除 |

### 实时防护

|  |  |
| --- | --- |
| **测试项目** | **实时防护** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理为删除 * 拷贝测试病毒至虚拟机中 * 查看病毒文件能否被检测并删除 |
| 预期结果 | * N/A * N/A * 病毒被成功检测并删除，管理中心能够看到病毒查杀日志 |

### 定期扫描

|  |  |
| --- | --- |
| **测试项目** | **定期扫描** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要定期扫描的虚拟机的安全配置中的实时防护状态关闭，手动/定期扫描的恶意软件处理为删除，配置定期扫描时间为每天12:00 * 拷贝测试病毒至虚拟机 * 12:00时进入管理中心 资产管理-虚拟机/终端 页面查看系统是否开始对虚拟机进行扫描 * 查看病毒文件是否被删除并产生病毒查杀日志 |
| 预期结果 | * N/A * N/A * 12:00后，系统开始对使用对应安全配置的虚拟机进行扫描，右侧会显示扫描进度 * 虚拟机中的病毒文件被成功删除，且管理中心能够看到病毒查杀的日志 |

### 文件白名单

|  |  |
| --- | --- |
| **测试项目** | **文件白名单** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，目录/文件白名单配置为/root/white/virus.a * 拷贝测试病毒文件virus.a和virus.b到虚拟机/root/white/目录，拷贝测试病毒文件virus.a到/root/normal/目录 * 查看测试病毒文件能否保存成功 |
| 预期结果 | * N/A * N/A * /root/white/目录中的病毒文件virus.a仍然存在，/root/white/目录病毒文件virus.b和/root/normal/目录中的病毒文件virus.a被删除 |

### 目录白名单

|  |  |
| --- | --- |
| **测试项目** | **目录白名单** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，目录/文件白名单配置为/root/white/ * 拷贝测试病毒文件到虚拟机/root/white/目录和/root/normal/目录 * 查看测试病毒文件能否保存成功 |
| 预期结果 | * N/A * N/A * /root/white/目录中的病毒文件仍然存在，/root/normal/目录中的病毒文件被删除 |

### 文件后缀名白名单

|  |  |
| --- | --- |
| **测试项目** | **文件名后缀白名单** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，文件后缀名白名单配置为a * 拷贝测试病毒文件virus.a和virus.b到虚拟机/root/virus/目录中 * 查看测试病毒文件能否保存成功 |
| 预期结果 | * N/A * N/A * /root/virus/目录中病毒文件virus.a没有被删除，/root/virus/目录中病毒文件virus.b被删除 |

### 仅扫描目录

|  |  |
| --- | --- |
| **测试项目** | **仅扫描下列目录** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，仅扫描下列目录配置为/root/black/ * 拷贝测试病毒文件到虚拟机/root/black/和/root/normal/目录中 * 查看测试病毒文件能否保存成功 |
| 预期结果 | * N/A * N/A * /root/black/目录中病毒文件被删除，管理中心产生病毒删除日志，/root/normal/目录中病毒文件没有被删除 |

### 仅扫描指定后缀名文件

|  |  |
| --- | --- |
| **测试项目** | **扫描指定后缀名文件** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将需要扫描的虚拟机的安全配置中的实时防护状态打开，恶意软件处理配置为删除，仅扫描包含下列后缀名的文件配置为b * 拷贝测试病毒文件virus.a和virus.b到Linux虚拟机中 * 查看能否测试病毒文件能否保存成功 |
| 预期结果 | * N/A * N/A * 病毒文件virus.b被删除，管理中心产生病毒文件查杀日志，病毒文件virus.a没有被删除 |

### 压缩文件扫描

|  |  |
| --- | --- |
| **测试项目** | **压缩文件实时防护测试** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将测试虚拟机的安全配置中的实时防护状态打开，默认开启监控压缩包文件，采取默认勾选配置。 * 拷贝带病毒的压缩包文件到测试虚拟机中 * 查看压缩病毒文件是否能够进行解压缩扫描，并且文件被隔离 * 进入分析日志模块，查看查杀日志中是否带有“==>”日志，如果存在，说明压缩文件经过解压后进行查杀； |
| 预期结果 | * N/A * N/A * 带病毒的压缩文件被隔离，管理中心产生病毒文件查杀日志。 * 防恶意软件分析日志中产生了带“==>”的压缩文件扫描日志 |

### 多引擎测试(AVE引擎)

|  |  |
| --- | --- |
| **测试项目** | **AVE引擎测试** |
| 测试步骤 | * 导入license：在“管理-使用许可”中导入360引擎license； * 设置安全策略：在安全配置中设置安全策略：实时防护打开，恶意软件处理为“隔离”； * 在虚拟机任意目录下放入AVE病毒文件； * 进入分析日志模块，查看查杀是否产生隔离日志，文件是否被做隔离处理 |
| 预期结果 | * License导入成功，引擎加载成功； * 策略下发成功； * AVE病毒文件被隔离查杀； * 产生AVE病毒被查杀的日志，且病毒被成功隔离； |

### 多引擎测试(QEX引擎)

|  |  |
| --- | --- |
| **测试项目** | **QEX引擎测试** |
| 测试步骤 | * 导入license：在“管理-使用许可”中导入360引擎license； * 设置安全策略：在安全配置中设置安全策略：实时防护打开，恶意软件处理为“隔离”； * 在虚拟机任意目录下放入QEX病毒文件； * 进入分析日志模块，查看查杀是否产生隔离日志，文件是否被做隔离处理 |
| 预期结果 | * License导入成功，引擎加载成功； * 策略下发成功； * QEX病毒文件被隔离查杀； * 产生QEX病毒被查杀的日志，且病毒被成功隔离； |

### 多引擎测试(BD引擎)

|  |  |
| --- | --- |
| **测试项目** | **BD引擎测试** |
| 测试步骤 | * 导入license：在“管理-使用许可”中导入BD引擎license； * 设置安全策略：在安全配置中设置安全策略：实时防护打开，恶意软件处理为“隔离”； * 在虚拟机任意目录下放入BD病毒文件； * 进入分析日志模块，查看查杀是否产生隔离日志，文件是否被做隔离处理 |
| 预期结果 | * License导入成功，引擎加载成功； * 策略下发成功； * BD病毒文件被隔离查杀； * 产生BD病毒被查杀的日志，且病毒被成功隔离； |

### 云查测试

|  |  |
| --- | --- |
| **测试项目** | **云查测试** |
| 测试步骤 | * 导入license：在“管理-使用许可”中导入360引擎license； * 设置安全策略：在安全配置中设置安全策略：实时防护打开，恶意软件处理为“隔离”； * 检查云查功能是否正常，网络是否畅通； * 在虚拟机任意目录下放入超过50条病毒病毒文件； * 进入分析日志模块，查看查杀是否产生隔离日志，文件是否被做隔离处理，查看文件模块日志，查看病毒文件被云查查杀； |
| 预期结果 | * License导入成功，引擎加载成功； * 策略下发成功； * 云查功能正常； * 病毒文件被云查隔离查杀； * 产生病毒被查杀的日志，且病毒被成功隔离； |

### 自保护(文件保护)

|  |  |
| --- | --- |
| **测试项目** | **自保护-文件保护测试** |
| 测试步骤 | * 在概括页面或者安全配置中打开自保护功能，保存使得配置生效； * 进入windows虚拟机C:\Program Files\Nubosh目录中，对文件/目录进行创建、修改、删除操作，查看文件是否被阻止进行上述操作； |
| 预期结果 | * 策略下发成功，自保功能打开； * Nubosh目录下的文件或者目录被阻止做任何写入操作； |

### 自保护(进程保护)

|  |  |
| --- | --- |
| **测试项目** | **自保护-进程保护测试** |
| 测试步骤 | * 在概括页面或者安全配置中打开自保护功能，保存使得配置生效； * 进入windows虚拟机录中，查看“进程”、“详细信息”窗口中文件进程或者网络进程能否被停止； * 查看 “服务”窗口中文件服务或者网络服务能否被停止； |
| 预期结果 | * 策略下发成功，自保功能打开； * 进程”、“详细信息”窗口中文件进程或者网络进程无法被停止； * “服务”窗口中文件服务或者网络服务无法被停止； |

### 扫描资源占用

|  |  |
| --- | --- |
| **测试项目** | **扫描资源占用测试** |
| 测试步骤 | * 在“管理中心-安全配置-防恶意软件-手动/定期扫描”中设置“扫描资源占用”为“平衡型”，保存使得配置生效； * 对windows虚拟机进行全盘扫描操作，通过任务管理器查看文件进程使用CPU是否始终不超过50%； |
| 预期结果 | * 策略下发成功，扫描资源占用功能设置成功； * 对windows虚拟机进行全盘扫描操作，通过任务管理器查看文件进程使用CPU始终不超过50%； |

### Powershell扫描-计划任务

|  |  |
| --- | --- |
| **测试项目** | **扫描powershell计划任务** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将准备扫描的windows有代理虚拟机的安全配置中的实时防护状态关闭，恶意软件处理配置为删除 * 在测试虚机中创建powershell计划任务：  1. 在控制面板-系统和安全-管理工具中，打开任务计划程序； 2. 点击创建任务，输入任务名称，在“操作”选项中，点击新建，在设置中输入powershell脚本，点击确定，任务创建  * 在虚拟机/终端页面选择该虚机，点击快速扫描，查看文件是否被删除 * 查看分析>防恶意软件日志信息 |
| 预期结果 | * N/A * 创建成功 * 计划任何成功被删除 * 在分析日志页面可以正常查看到计划任务被删除的信息 |

### Powershell扫描-注册表

|  |  |
| --- | --- |
| **测试项目** | **扫描powershell注册表** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将准备扫描的windows有代理虚拟机的安全配置中的实时防护状态关闭，恶意软件处理配置为删除 * 在测试虚机中创建powershell注册表：  1. 在运行中输入regedit，打开注册表编辑器 2. 在HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVerion\Run项中，在右侧空白位置右击新建-字符串值，输入名称，如test 3. 选中新建的键值，右击修改，在数值数据中输入powershell脚本，点击确定  * 在虚拟机/终端页面选择该虚机，点击快速扫描，查看文件是否被删除 * 查看分析>防恶意软件日志信息 |
| 预期结果 | * N/A * 创建成功 * 注册表成功被删除 * 在分析日志页面可以正常查看到注册表被删除的信息 |

### 内存扫描-1

|  |  |
| --- | --- |
| **测试项目** | **扫描正在运行的powershell进程** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将准备扫描的windows有代理虚拟机的安全配置中的实时防护状态关闭，恶意软件处理配置为删除 * 在该虚拟机的快速扫描目录下（如：Windows User）配置powershell关联进程文件并启动 * 选择该虚机，点击快速扫描按钮，查看扫描结果 * 查看分析->防恶意软件日志信息 |
| 预期结果 | * N/A * N/A * Powershell进程被删除，弹框提示处理动作为删除 * 分析->防恶意软件的日志页面显示进程删除信息 |

### 内存扫描-2

|  |  |
| --- | --- |
| **测试项目** | **执行病毒文件扫描** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将准备扫描的windows有代理虚拟机的安全配置中的实时防护状态关闭，恶意软件处理配置为隔离 * 在测试虚机的快速扫描目录（如：Windows User）下配置可执行病毒文件（例如exe）并启动（如没有可执行病毒文件，可通过将exe先添加到自定义恶意软件黑名单中） * 选择该虚机，点击快速扫描，查看扫描结果 * 查看分析->防恶意软件日志信息 |
| 预期结果 | * N/A * N/A * 快扫目录下的病毒文件被隔离，已运行的对应可执行文件的程序，被清除，客户端弹框提示处理状态为：隔离； * 分析->防恶意软件页面显示该文件隔离处理信息 |

## Webshell扫描

本类用例主要测试奇安信网神统一服务器安全管理系统（轻代理）的webshell扫描相关功能。

### 轻代理Windows虚拟机webshell扫描

|  |  |
| --- | --- |
| **测试项目** | **轻代理Windows虚机webshell扫描测试** |
| 测试步骤 | * 开启Windows虚机的web服务（nginx，apache等） * 将后门文件拷贝至Windows虚机web服务对应的目录中 * 在管理中心选择资产管理--虚拟机/终端，勾选所要扫描的轻代理Windows虚拟机，点击安全操作->webshell扫描 * 等待一两分钟，查看虚机概况界面能否显示扫描状态，时间及结果 * 查看管理中心的分析-webshell扫描页面是否有对应日志 |
| 预期结果 | * N/A * N/A * 扫描能够正常结束 * 虚拟机概况界面能够显示扫描状态，上次扫描时间，后门文件数量 * 日志分析的webshell扫描中有对应Windows虚拟机的webshell后门统计信息，且能对后门文件进行下载，隔离，加白操作 |

### 轻代理Linux虚拟机webshell扫描

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux虚机webshell扫描测试** |
| 测试步骤 | * 开启Linux虚机的web服务（nginx，apache等） * 将后门文件拷贝至Linux虚机web服务对应的目录中 * 在管理中心选择资产管理--虚拟机/终端，勾选所要扫描的轻代理Linux虚拟机，点击安全操作->webshell扫描 * 等待一两分钟，查看虚机概况界面能否显示扫描状态，时间及结果 * 查看管理中心的分析-webshell扫描页面是否有对应日志 |
| 预期结果 | * N/A * N/A * 扫描能够正常结束 * 虚拟机概况界面能够显示扫描状态，上次扫描时间，后门文件数量 * 日志分析的webshell扫描中有对应Linux虚拟机的webshell后门统计信息，且能对后门文件进行下载，隔离，加白操作 |

### 定期扫描

|  |  |
| --- | --- |
| **测试项目** | **Webshell定期扫描测试** |
| 测试步骤 | * 开启Linux虚机的web服务（nginx，apache等） * 将后门文件拷贝至Linux虚机web服务对应的目录中 * 在管理中心选择资产管理--虚拟机/终端，点击测试虚拟机使用的安全配置，进入webshell标签页，配置webshell定期扫描时间为每天12：00，点击保存按钮 * 12点后，查看系统是否对测试虚拟机进行了webshell扫描 * 查看管理中心的分析-webshell扫描页面是否有对应日志 |
| 预期结果 | * N/A * N/A * 安全配置修改成功 * 到达指定时间后，系统会对测试虚拟机进行webshell扫描，扫描完成后，虚拟机概况界面能够显示扫描状态，上次扫描时间，后门文件数量 * 日志分析的webshell扫描中有对应虚拟机的webshell后门统计信息，且能对后门文件进行下载，隔离，加白操作 |

### Webshell手动扫描自定义目录

|  |  |
| --- | --- |
| **测试项目** | **Webshell新增非自动检测目录为自定义扫描目录并手动扫描** |
| 测试步骤 | * 管理中心新增安全配置，webshell自定义扫描目录新增一条非自动检测扫描目录，保存 * 安全配置应用到测试虚机中 * 拷贝后门文件到自动检测目录及自定义扫描目录 * 在管理中心 资产管理-虚拟机/终端页面，选择测试虚拟机，点击“安全操作-webshell扫描” * 查看自动检测目录及自定义扫描目录后门文件是否被检测到，自定义目录是否优先被执行扫描 * 验证系统检测到的后门文件数量是否正确 * 在资产管理-实时监控页面中webshell后门计数器的值 * 进入分析-webshell页面，点击原始日志图标 |
| 预期结果 | * 保存成功，后台配置文件包括自定义扫描目录 * 安全配置应用成功 * 拷贝成功 * 系统开始对测试虚拟机进行webshell扫描，虚拟机详情页面中会显示扫描进度；扫描完成后，扫描状态会显示为“已完成”；会显示上次扫描完成的时间及检测到的后门数量 * 原始日志会显示扫描到的自动检测目录及自定义扫描目录后门文件，自定义扫描目录优先被扫到 * 系统检测到的后门文件计数器的值=实际后门文件数量 * Webshell后门文件计数器的值=实际后门文件数量 * 点击原始日志图标后，页面中会显示检测到的后门文件的具体信息，包括首次发现时间、虚拟机/终端、分组、安全配置、后门类型、文件路径、状态、操作，日志内容均正确，其中状态默认为未处理，可选操作为“下载 隔离 加白” |

### Webshell白名单手动扫描

|  |  |
| --- | --- |
| **测试项目** | **上传webshell白名单并手动扫描** |
| 测试步骤 | * 进入管理中心 管理-系统设置-特征库页面 * 进入“webshell白名单”标签页，点击“新增”按钮，在打开的“新增”对话框中点击“上传”按钮 * 在打开的对话框中选择要加入白名单的后门文件，如后门文件A * 将后门文件A拷贝至测试虚机web服务对应的目录中 * 在管理中心 虚拟机自定义安全配置，打开定制安全配置，保存 * 在管理中心资产管理-虚拟机/终端页面，选择测试虚机，点击“安全操作-webshell扫描” * 验证系统检测到的后门文件数量是否比实际的后门数量少一个 * 在资产管理-实时监控页面中是否会有统计webshell后门数量的计数器 * 进入分析-webshell页面，点击原始日志图标 |
| 预期结果 | * N/A * N/A * 选择要添加至白名单的后门文件，点击打开后，会自动上传该文件，白名单列表“备注文件名”栏中能正确显示该后门文件的名称、“文件指纹”栏中会显示自动为该后门文件计算出的md5值 * 拷贝成功 * 保存成功 * 系统定时开始对测试虚拟机进行webshell扫描，虚拟机详情页面中会显示扫描进度；扫描完成后，扫描状态会显示为“已完成”；会显示上传扫描完成的时间及检测到的后门的数量 * 系统检测到的后门数量比实际后门数量少1 * 实时监控页面能看到webshell后门文件的计数器，且计数器的值正确 * 点击原始日志图标后，页面中会显示检测到的后门文件的具体信息，包括首次发现时间、虚拟机/终端、分组、安全配置、后门类型、文件路径、状态、操作，日志内容均正确，其中状态默认为未处理。日志中不包括白名单中的后门文件A的信息 |

## 应用程序控制

本类用例主要测试奇安信网神统一服务器安全管理系统（有代理）的应用程序控制相关功能。

### 阻止应用程序路径

|  |  |
| --- | --- |
| **测试项目** | **阻止应用程序路径** |
| 测试步骤 | * 1. 进入管理中心 安全策略 > 安全配置页面 * 2. 点击“Windows安全配置，进入”应用程序控制“标签页 * 3. 开启实时管控功能、动作配为阻止、在应用程序路径列表中输入C:\Windows\System32\cmd.exe，其他应用程序启动时采取动作为允许 * 4. 点击保存按钮 * 5. 在测试虚拟机中运行cmd * 6. 等一二分钟，进入管理中心 分析-应用程序控制页面查看阻止日志 |
| 预期结果 | * N/A * N/A * N/A * 安全配置保存成功 * 在测试虚拟机中打开cmd程序失败，其他应用程序打开成功 * 管理中心能够正确显示应用程序控制的阻止日志 |

### 阻止应用程序名

|  |  |
| --- | --- |
| **测试项目** | **阻止应用程序名** |
| 测试步骤 | * 1. 进入管理中心 安全策略 > 安全配置页面 * 2. 点击“Windows安全配置，进入”应用程序控制“标签页 * 3. 开启实时管控功能、动作配为阻止、在应用程序名列表中输入cmd.exe，其他应用程序启动时采取动作为允许 * 4. 点击保存按钮 * 5. 在测试虚拟机中运行cmd，在虚拟机中打开其他应用程序 * 6. 等一二分钟，进入管理中心 分析-应用程序控制页面查看阻止日志 |
| 预期结果 | * N/A * N/A * N/A * 安全配置保存成功 * 在测试虚拟机中打开cmd程序失败，其他应用程序打开成功 * 管理中心能够正确显示应用程序控制的阻止日志 |

### 例外应用程序路径-1

|  |  |
| --- | --- |
| **测试项目** | **阻止例外应用程序路径** |
| 测试步骤 | * 1. 进入管理中心 安全策略 > 安全配置页面 * 2. 点击“Windows安全配置，进入”应用程序控制“标签页 * 3. 开启实时管控功能、动作配为允许、点击“添加系统应用程序”，添加windows系统应用程序，在例外应用程序路径中输入C:\Windows\System32\cmd.exe，其他应用程序启动时采取动作为阻止 * 4. 点击保存按钮 * 5. 在测试虚拟机中打开cmd * 6. 在测试虚拟机中打开IE * 7. 等一二分钟，进入管理中心 分析-应用程序控制页面查看阻止日志 |
| 预期结果 | * N/A * N/A * N/A * 安全配置保存成功 * 在测试虚拟机中打开cmd程序失败 * 在测试虚拟机中能够成功打IE * 管理中心能够正确显示测试虚拟机中cmd被阻止的日志 |

### 例外应用程序路径-2

|  |  |
| --- | --- |
| **测试项目** | **监控例外应用程序路径** |
| 测试步骤 | * 1. 进入管理中心 安全策略 > 安全配置页面 * 2. 点击“Windows安全配置，进入”应用程序控制“标签页 * 3. 开启实时管控功能、动作配为允许、点击“添加系统应用程序”，添加windows系统应用程序，在例外应用程序路径中输入C:\Windows\System32\cmd.exe，其他应用程序启动时采取动作为监控 * 4. 点击保存按钮 * 5. 在测试虚拟机中打开cmd * 6. 在测试虚拟机中打开IE * 7. 等一二分钟，进入管理中心 分析-应用程序控制页面查看监控日志 |
| 预期结果 | * N/A * N/A * N/A * 安全配置保存成功 * 在测试虚拟机中打开cmd成功 * 在测试虚拟机中能够成功打IE * 管理中心能够正确显示测试虚拟机中cmd被监控的日志，属于windows系统应用程序中的应用程序不会被监控 |

### 监控应用程序路径

|  |  |
| --- | --- |
| **测试项目** | **监控应用程序路径** |
| 测试步骤 | * 1. 进入管理中心 安全策略 > 安全配置页面 * 2. 点击“Windows安全配置，进入”应用程序控制“标签页 * 3. 开启实时管控功能、动作配为监控、在应用程序路径列表中输入C:\Windows\System32\cmd.exe * 4. 点击保存按钮 * 5. 在测试虚拟机中运行cmd * 6. 等一二分钟，进入管理中心 分析-应用程序控制页面查看监控日志 |
| 预期结果 | * N/A * N/A * N/A * 安全配置保存成功 * 在测试虚拟机中打开cmd成功 * 管理中心能够正确显示测试虚拟机中cmd的监控日志 |

### 监控应用程序名

|  |  |
| --- | --- |
| **测试项目** | **监控应用程序名** |
| 测试步骤 | * 1. 进入管理中心 安全策略 > 安全配置页面 * 2. 点击“Windows安全配置，进入”应用程序控制“标签页 * 3. 开启实时管控功能、动作配为监控、在应用程序名列表中输入cmd.exe * 4. 点击保存按钮 * 5. 在测试虚拟机中运行cmd * 6. 等一二分钟，进入管理中心 分析-应用程序控制页面查看监控日志 |
| 预期结果 | * N/A * N/A * N/A * 安全配置保存成功 * 在测试虚拟机中打开cmd成功 * 管理中心能够正确显示应用程序控制的监控日志 |

## 完整性监控

本类用例主要测试奇安信网神统一服务器安全管理系统的完整性监控相关功能。

### 实时监控轻代理Windows文件的删除

|  |  |
| --- | --- |
| **测试项目** | **实时监控轻代理Windows文件的删除测试** |
| 测试步骤 | * 1、登录管理中心界面，选择安全策略--安全配置-点击或新增Windows安全配置进入配置界面 * 2、点击系统加固下拉箭头选择完整性监控，开启实时扫描、定期扫描关闭，监控等级设置为严格，勾选编号为20105的规则，点击保存 * 3、在被测虚拟路径为C:\Windows\SysWOW64\drivers下建立test文件 * 4、主界面选择资产管理--虚拟机/终端，勾选所要扫描的虚拟机，点击安全操作->重新生成完整性基线 * 5、根据20105规则，在所选虚拟机路径为C:\Windows\SysWOW64\drivers上删除test文件，查看管理中心实时监控、分析日志是否报对应的提示信息或日志 |
| 预期结果 | * N/A * N/A * N/A * 基线生成成功，在虚机概况界面可以看到基线重置时间 * 管理中心的分析->完整性监控页面能够正确显示虚机删除test文件的日志 |

### 手动扫描监控文件的增加

|  |  |
| --- | --- |
| **测试项目** | **完整性监控手动扫描文件的增加测试** |
| 测试步骤 | * 1、登录管理中心界面，选择安全策略--安全配置-点击或新增Windows安全配置进入配置界面 * 2、点击系统加固下拉箭头，选择完整性监控，关闭实时扫描、定期扫描，监控等级设置为严格，勾选编号为20111，“监控IE浏览器目录的任何变化”这条规则，点击保存 * 3、主界面选择资产管理--虚拟机/终端，勾选所要扫描的虚拟机，点击安全操作->重新生成完整性基线 * 4、根据20111这条规则，在所测虚拟机上在所监控C:\Program Files\Internet Explorer目录下建立test文件； * 5、在管理中心上选择此虚拟机点击安全操作->完整性扫描，扫描完成后查看管理中心实时监控、分析日志是否报对应的提示信息或日志 |
| 预期结果 | * N/A * N/A * 基线生成成功，在虚机概况界面可以看到基线重置时间 * N/A * 管理中心的分析->完整性监控页面能够正确显示虚机新增test文件的日志 |

### 手动扫描监控文件的删除

|  |  |
| --- | --- |
| **测试项目** | **完整性监控手动扫描文件的删除测试** |
| 测试步骤 | * 1、登录管理中心界面，选择安全策略--安全配置-点击或新增Windows安全配置进入配置界面 * 2、点击系统加固下拉箭头，选择完整性监控，关闭实时扫描、定期扫描，监控等级设置为严格，勾选编号为20111，“监控IE浏览器目录的任何变化”这条规则，点击保存 * 3、在所测虚拟机上C:\Program Files\Internet Explorer目录下建立test文件 * 4、主界面选择资产管理--虚拟机/终端，勾选所要扫描的虚拟机，点击安全操作->重新生成完整性基线 * 5、根据20111这条规则，在所测虚拟机上对所监控C:\Program Files\Internet Explorer目录下删除test文件； * 6、在管理中心上选择此虚拟机点击安全操作->完整性扫描，扫描完成后查看管理中心实时监控、分析日志是否报对应的提示信息或日志 |
| 预期结果 | * N/A * N/A * N/A * 基线生成成功，在虚机概况界面可以看到基线重置时间 * N/A * 管理中心的分析->完整性监控页面能够正确显示虚机删除test文件的日志 |

### 手动扫描监控注册表的增加

|  |  |
| --- | --- |
| **测试项目** | **完整性监控手动扫描注册表的增加测试** |
| 测试步骤 | * 1、登录管理中心界面，选择安全策略--安全配置-点击或新增Windows安全配置进入配置界面 * 2、点击系统加固下拉箭头选择完整性监控，关闭实时扫描、定期扫描，监控等级设置为严格，勾选编号为20026的注册表规则，点击保存 * 3、主界面选择资产管理--虚拟机/终端，勾选所要扫描的虚拟机，点击安全操作->重新生成完整性基线 * 4、根据编号为20026规则，在所选虚拟机上监控的注册表路径为 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer中新增一张test表 * 5、在管理中心上选择此虚拟机点击安全操作->完整性扫描，扫描完成后查看管理中心实时监控、分析日志是否报对应的提示信息或日志 |
| 预期结果 | * N/A * N/A * 基线生成成功，在虚机概况界面可以看到基线重置时间 * N/A * 管理中心的分析->完整性监控页面能够正确显示虚机注册表被改变的日志 |

### 手动扫描监控轻代理Windows进程的创建

|  |  |
| --- | --- |
| **测试项目** | **完整性监控手动扫描进程的创建测试** |
| 测试步骤 | * 1、登录管理中心界面，选择安全策略--安全配置-点击Windows安全配置进入配置界面 * 2、点击完整性监控，关闭实时扫描、定期扫描，监控等级设置为严格，勾选22001，“监控Windows进程变化“规则 * 3、主界面选择资产管理--虚拟机/终端，勾选所要扫描的虚拟机，点击安全操作->重新生成完整性基线， * 4、在所选虚拟机任务管理器中创建新的进程，在管理中心上选择此虚拟机点击安全操作->完整性扫描，扫描完成后查看管理中心实时监控、分析日志是否报对应的提示信息或日志 |
| 预期结果 | * N/A * N/A * 基线生成成功，在虚机概况界面可以看到基线重置时间 * 管理中心的分析->完整性监控页面能够显示对应的日志 |

### 手动扫描监控轻代理Windows服务的创建

|  |  |
| --- | --- |
| **测试项目** | **完整性监控手动扫描服务的创建测试** |
| 测试步骤 | * 1、登录管理中心界面，选择安全策略--安全配置-点击Windows安全配置进入配置界面 * 2、点击完整性监控，关闭实时扫描、定期扫描，监控等级设置为严格，勾选22003，“监控Windows服务变化”规则 * 3、主界面选择资产管理--虚拟机/终端，勾选所要扫描的虚拟机，点击安全操作->重新生成完整性基线， * 4、在所选虚拟机上服务中添加新的服务（Windows进入cmd执行sc create DBManage binPath= "C:/Program Files/TsingHua/DBManageService.exe" DisplayName= "DBManage" start= auto；） * 5、在管理中心上选择此虚拟机点击安全操作->完整性扫描，扫描完成后查看管理中心实时监控、分析日志是否报对应的提示信息或日志 |
| 预期结果 | * N/A * N/A * 基线生成成功，在虚机概况界面可以看到基线重置时间 * N/A * 管理中心的分析->完整性监控页面能够显示对应的日志，创建了服务DBManage |

### 手动扫描监控轻代理Windows端口的添加

|  |  |
| --- | --- |
| **测试项目** | **完整性监控手动扫描端口的添加测试** |
| 测试步骤 | * 1、登录管理中心界面，选择安全策略--安全配置-点击Windows安全配置进入配置界面 * 2、点击完整性监控，关闭实时扫描、定期扫描，监控等级设置为严格，勾选22002，“监控Windows监听端口变化“规则 * 3、主界面选择资产管理--虚拟机/终端，勾选所要扫描的虚拟机，点击安全操作->重新生成完整性基线， * 4、在所选虚拟机中添加某udp端口，在管理中心上选择此虚拟机点击安全操作->完整性扫描，扫描完成后查看管理中心实时监控、分析日志是否报对应的提示信息或日志 |
| 预期结果 | * N/A * N/A * 基线生成成功，在虚机概况界面可以看到基线重置时间 * 管理中心的分析->完整性监控页面能够显示对应的日志 |

## 漏洞管理

本类用例主要测试奇安信网神统一服务器安全管理系统（轻代理）的漏洞管理相关功能。

### 轻代理Windows虚拟机漏洞扫描

|  |  |
| --- | --- |
| **测试项目** | **轻代理Windows虚机漏洞扫描测试** |
| 测试步骤 | * 在管理中心选择资产管理--虚拟机/终端，勾选所要扫描的轻代理Windows虚拟机，点击安全操作->漏洞扫描 * 等待一两分钟，查看虚机概况界面能否显示扫描状态，时间及结果 * 查看管理中心的分析-漏洞管理页面是否有对应日志 |
| 预期结果 | * 1、扫描能够正常结束 * 2、虚拟机概况界面能够显示扫描状态，上次扫描时间、漏洞数量、漏洞严重程度、漏洞详细信息 * 3、日志分析的漏洞管理中有对应Windows虚拟机的漏洞信息 |

### 轻代理Linux虚拟机漏洞扫描

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux虚机漏洞扫描测试** |
| 测试步骤 | * 在管理中心选择资产管理--虚拟机/终端，勾选所要扫描的轻代理Linux虚拟机，点击安全操作->漏洞扫描 * 等待一两分钟，查看虚机概况界面能否显示扫描状态，时间及结果 * 查看管理中心的分析-漏洞管理页面是否有对应日志 |
| 预期结果 | * 1、扫描能够正常结束 * 2、虚拟机概况界面能够显示扫描状态，上次扫描时间、漏洞数量、漏洞严重程度、漏洞详细信息 * 3、日志分析的漏洞管理中有对应Linux虚拟机的漏洞信息 |

### 定期扫描

|  |  |
| --- | --- |
| **测试项目** | **漏洞管理定期扫描测试** |
| 测试步骤 | * 在管理中心选择资产管理--虚拟机/终端，点击测试虚拟机使用的安全配置，进入漏洞管理标签页，配置定期扫描时间为每天12：00，点击保存按钮 * 12点后，查看系统是否对测试虚拟机进行了漏洞扫描 * 查看管理中心的分析-漏洞管理页面是否有对应日志 |
| 预期结果 | * 安全配置修改成功 * 到达指定时间后，系统会对测试虚拟机进行漏洞扫描，扫描完成后，虚拟机概况界面能够显示扫描状态，上次扫描时间、漏洞数量、漏洞严重程度、漏洞详细信息 * 日志分析的漏洞管理中有对应虚拟机的漏洞信息 |

## 安全基线

本类用例主要测试奇安信网神统一服务器安全管理系统（轻代理）的安全基线相关功能。

### 轻代理Windows虚拟机安全基线扫描

|  |  |
| --- | --- |
| **测试项目** | **轻代理Windows虚机安全基线扫描测试** |
| 测试步骤 | * 在管理中心选择资产管理--虚拟机/终端，勾选所要扫描的轻代理Windows虚拟机，点击安全操作->安全基线扫描 * 等待一两分钟，查看虚机概况界面能否显示扫描状态，时间及结果 * 查看管理中心的分析-安全基线页面是否有对应日志 * 点击虚机概况界面的扫描得分，勾选可自动修复的安全基线规则，点击修复，再次进行安全基线扫描，查看扫描得分 |
| 预期结果 | * 1、扫描能够正常结束 * 2、虚拟机概况界面能够显示扫描状态，上次扫描时间，扫描得分 * 3、日志分析的安全基线中有对应Windows虚拟机的安全基线信息，且能对可自动修复的扫描项进行自动修复 * 4、自动修复成功，再次扫描后扫描得分提高，且已修复的扫描项不再出现 |

### 轻代理Linux虚拟机安全基线扫描

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux虚机安全基线扫描测试** |
| 测试步骤 | * 在管理中心选择资产管理--虚拟机/终端，勾选所要扫描的轻代理Linux虚拟机，点击安全操作->安全基线扫描 * 等待一两分钟，查看虚机概况界面能否显示扫描状态，时间及结果 * 查看管理中心的分析-安全基线页面是否有对应日志 * 点击虚机概况界面的扫描得分，勾选可自动修复的安全基线规则，点击修复，再次进行安全基线扫描，查看扫描得分 |
| 预期结果 | * 1、扫描能够正常结束 * 2、虚拟机概况界面能够显示扫描状态，上次扫描时间，扫描得分 * 3、日志分析的安全基线中有对应Linux虚拟机的安全基线信息，且能对可自动修复的扫描项进行自动修复 * 4、自动修复成功，再次扫描后扫描得分提高，且已修复的扫描项不再出现 |

### 定期扫描

|  |  |
| --- | --- |
| **测试项目** | **安全基线定期扫描测试** |
| 测试步骤 | * 在管理中心选择资产管理--虚拟机/终端，点击测试虚拟机使用的安全配置，进入安全基线标签页，配置定期扫描时间为每天12：00，点击保存按钮 * 12点后，查看系统是否对测试虚拟机进行了安全基线扫描 * 查看管理中心的分析-安全基线页面是否有对应日志 * 点击虚机概况界面的扫描得分，勾选可自动修复的安全基线规则，点击修复，再次进行安全基线扫描，查看扫描得分 |
| 预期结果 | * 安全配置修改成功 * 到达指定时间后，系统会对测试虚拟机进行安全基线扫描，扫描完成后，虚拟机概况界面能够显示扫描状态，上次扫描时间，扫描得分 * 日志分析的安全基线中有对应虚拟机的安全基线信息 * 自动修复成功，再次扫描后扫描得分提高，且已修复的扫描项不再出现 |

## 防暴力破解

本类用例主要测试奇安信网神统一服务器安全管理系统（轻代理）的防暴力破解相关功能。

### 轻代理Windows虚机rdp协议测试

|  |  |
| --- | --- |
| **测试项目** | **轻代理Windows虚机rdp协议测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中开启防暴力破解，设置防暴力破解规则，60秒内尝试登录超过10次，拦截10分钟 * 将新增的安全配置A指定给Windows虚机 * 使用远程登录连接被防护的Windows虚机 * 在60秒内尝试登录10次，验证是否拒绝连接，且拦截时间为10分钟 * 查看管理中心的分析-防暴力破解页面是否有对应日志 * 查看虚机详情界面能否显示被攻击时间 |
| 预期结果 | * 1、N/A * 2、N/A * 3、攻击机器能够远程连接被防护的Windows虚机 * 4、触发防暴力规则后，防暴力破解程序开始拦截操作，被拦截机器10分钟之后才能访问 * 5、日志分析的防暴力破解中有对应Windows虚拟机的阻止暴力破解次数统计信息 * 6、虚机详情界面能够显示最近被攻击时间 |

### 轻代理Linux虚机ssh协议测试

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux虚机ssh协议测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中开启防暴力破解，设置防暴力破解规则，60秒内尝试登录超过10次，拦截10分钟 * 将新增的安全配置A指定给Linux虚机 * 使用ssh连接被防护的Linux虚机 * 在60秒内尝试登录10次，验证是否拒绝连接，且拦截时间为10分钟 * 查看管理中心的分析-防暴力破解页面是否有对应日志 * 查看虚机详情界面能否显示被攻击时间 |
| 预期结果 | * 1、N/A * 2、N/A * 3、攻击机器能够远程连接被防护的Linux虚机 * 4、触发防暴力规则后，防暴力破解程序开始拦截操作，被拦截机器10分钟之后才能访问 * 5、日志分析的防暴力破解中有对应Linux虚拟机的阻止暴力破解次数统计信息 * 6、虚机详情界面能够显示最近被攻击时间 |

### 轻代理Linux虚机telnet协议测试

|  |  |
| --- | --- |
| **测试项目** | **轻代理Linux虚机telet协议测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中开启防暴力破解，设置防暴力破解规则，60秒内尝试登录超过10次，拦截10分钟 * 将新增的安全配置A指定给Linux虚机 * 使用telnet连接被防护的Linux虚机 * 在60秒内尝试登录10次，验证是否拒绝连接，且拦截时间为10分钟 * 查看管理中心的分析-防暴力破解页面是否有对应日志 * 查看虚机详情界面能否显示被攻击时间 |
| 预期结果 | * 1、N/A * 2、N/A * 3、攻击机器能够远程连接被防护的Linux虚机 * 4、触发防暴力规则后，防暴力破解程序开始拦截操作，被拦截机器10分钟之后才能访问 * 5、日志分析的防暴力破解中有对应Linux虚拟机的阻止暴力破解次数统计信息 * 6、虚机详情界面能够显示最近被攻击时间 |

### 防暴力破解白名单测试

|  |  |
| --- | --- |
| **测试项目** | **防暴力破解黑名单测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中开启防暴力破解，设置防暴力破解规则，100秒内尝试登录超过2次，拦截2分钟 * 将新增的安全配置A指定给Linux虚机 * 使用ssh连接被防护的Linux虚机 * 在60秒内尝试登录10次，验证是否拒绝连接，且拦截时间为10分钟 * 查看管理中心的分析-防暴力破解页面是否有对应日志 * 在“安全配置-系统加固-防暴力破解-黑白名单”中设置防暴力破解白名单为被拦截机器 * 查看被拦截中的加白机器能否成功连接被防护机器； |
| 预期结果 | * 1、N/A * 2、N/A * 3、攻击机器能够远程连接被防护的Linux虚机 * 4、触发防暴力规则后，防暴力破解程序开始拦截操作，被拦截机器10分钟之后才能访问 * 5、日志分析的防暴力破解中有对应Linux虚拟机的阻止暴力破解次数统计信息 * 设置防暴力破解白名单成功； * 6、拦截过程中进行加白，被拦截机器可以成功连接防护机器； |

### 防暴力破解黑名单测试

|  |  |
| --- | --- |
| **测试项目** | **防暴力破解黑名单测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中开启防暴力破解，设置防暴力破解规则，100秒内尝试登录超过2次，拦截2分钟 * 将新增的安全配置A指定给Linux虚机 * 在“安全配置-系统加固-防暴力破解-黑白名单”中设置防暴力破解黑名单； * 查看加黑机器能否始终被拦截； * 查看管理中心的分析-防暴力破解页面是否有对应日志； |
| 预期结果 | * 1、N/A * 2、N/A * 3、设置防暴力破解黑名单生效 * 4、加黑机器始终被拦截； * 5、日志分析的防暴力破解中有对应Linux虚拟机的阻止暴力破解次数统计信息； |

## 防火墙功能

本类用例主要测试奇安信网神统一服务器安全管理系统（有代理）的防火墙相关功能。

### 防火墙规则ICMP出站

|  |  |
| --- | --- |
| **测试项目** | **防火墙规则ICMP出站测试** |
| 测试步骤 | * 1. 在管理中心新增安全配置A，在配置A中新增防火墙规则，动作阻止，方向出站，协议ICMP，本地信息选择所有IP地址，远程信息填写10.128.0.111 * 2. 将新增安全配置A指定给测试虚拟机 * 3.在测试虚拟机中ping 地址 10.128.0.111，10.128.0.1 ,www.baidu.com * 4. 等一二分钟，进入管理中心 分析-防火墙/网络管理页面查看日志 |
| 预期结果 | * N/A * N/A * 除了10.128.0.111，其他地址都能Ping通 * 管理中心能够正确显示防火墙的阻止日志 |

### 防火墙规则ICMP入站

|  |  |
| --- | --- |
| **测试项目** | **防火墙规则ICMP入站测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中新增防火墙规则，动作阻止，方向入站，协议ICMP，本地信息选择所有IP地址，远程信息填写10.128.0.111 * 将新增安全配置A指定给测试虚拟机 * 从10.128.0.111 ping测试虚拟机 * 从其他机器 ping测试虚拟机 * 等一二分钟，进入管理中心 分析-防火墙/网络管理页面查看日志 |
| 预期结果 | * N/A * N/A * 从10.128.0.111 ping测试虚拟机失败 * 从其他机器 ping测试虚拟机成功 * 管理中心能够正确显示防火墙的阻止日志 |

### 防火墙TCP入站

|  |  |
| --- | --- |
| **测试项目** | **防火墙规则TCP入站测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中新增防火墙规则，动作阻止，方向入站，协议TCP，本地信息选择所有IP地址，端口为3389，远程信息选择所有IP和端口 * 将新增安全配置A指定给测试虚拟机 * 远程连接至测试虚拟机 * 等一二分钟，进入管理中心 分析-防火墙/网络管理页面查看日志 |
| 预期结果 | * N/A * N/A * 远程连接失败 * 管理中心能够正确显示测试虚拟机TCP入站的阻止日志 |

### 防火墙TCP出站

|  |  |
| --- | --- |
| **测试项目** | **防火墙规则TCP出站测试** |
| 测试步骤 | * 在管理中心新增安全配置A，在配置A中新增防火墙规则，动作阻止，方向出站，协议TCP，本地信息选择所有IP地址和端口，远程信息选择所有IP，端口选择20，21 * 将新增安全配置A指定给测试虚拟机 * 在测试虚拟机中通过cmd访问某个ftp服务器 * 等一二分钟，进入管理中心 分析-防火墙/网络管理页面查看日志 |
| 预期结果 | * N/A * N/A * 3. 在测试虚拟机中访问Ftp服务器失败 * 4. 管理中心能够正确显示测试虚拟机TCP出站的阻止日志 |

### 防火墙UDP入站

|  |  |
| --- | --- |
| **测试项目** | **防火墙规则UDP入站测试** |
| 测试步骤 | * 1. 在管理中心新增安全配置A，在配置A中新增防火墙规则，动作阻止，方向入站，协议UDP，本地信息选择所有IP地址，远程信息填写装有iperf的虚拟机B的IP * 2. 将新增安全配置A指定给测试虚拟机 * 3. 虚拟机B做为客户端，测试虚拟机做为服务端，虚拟机B向测试虚拟机发送UDP报文 * 4. 等一二分钟，进入管理中心 分析-防火墙/网络管理页面查看日志 |
| 预期结果 | * N/A * N/A * 测试虚拟机没有收到虚拟机B发送的UDP报文 * 管理中心能够正确显示测试虚拟机UDP入站的阻止日志 |

### 防火墙UDP出站

|  |  |
| --- | --- |
| **测试项目** | **防火墙规则UDP出站测试** |
| 测试步骤 | * 1. 在管理中心新增安全配置A，在配置A中新增防火墙规则，动作阻止，方向出站，协议UDP，本地信息选择所有IP地址和端口，远程信息选择所有IP，远程端口配置为53 * 2. 将新增安全配置A指定给测试虚拟机 * 3. 在测试虚拟机打开浏览器，访问网页 * 4. 等一二分钟，进入管理中心 分析-防火墙/网络管理页面查看日志 |
| 预期结果 | * N/A * N/A * 访问失败 * 管理中心能够正确显示测试虚拟机UDP出站的阻止日志 |

### 修改防火墙规则状态

|  |  |
| --- | --- |
| **测试项目** | **修改防火墙状态测试** |
| 测试步骤 | * 1. 在管理中心新增安全配置A，在配置A中新增防火墙规则，动作阻止，方向出站，协议ICMP，本地信息选择所有IP地址，远程信息填写10.128.0.111 * 2. 将新增安全配置A指定给测试虚拟机 * 3.在测试虚拟机中ping 地址 10.128.0.111，10.128.0.1, www.baidu.com * 4. 等一二分钟，进入管理中心 分析-防火墙/网络管理页面查看日志 * 5.修改安全配置A，打开防火墙标签页，将第一步新增的防火墙规则状态改为关闭，点击保存 * 6.在测试虚拟机中ping 地址 10.128.0.111，10.128.0.1, www.baidu.com |
| 预期结果 | * N/A * N/A * 除了10.128.0.111，其他地址都能Ping通 * 管理中心能够正确显示防火墙的阻止日志 * 防火墙规则状态修改成功 * 10.128.0.111，10.128.0.1, www.baidu.com都能ping通 |

## 失陷检测

本类用例主要测试奇安信网神统一服务器安全管理系统（有代理）的失陷检测相关功能。

### 失陷主机隔离

|  |  |
| --- | --- |
| **测试项目** | **失陷主机隔离测试** |
| 测试步骤 | * 1. 进入管理中心，新增安全配置A，开启防火墙，开启失陷检测，失陷处理选择隔离，保存安全配置 * 2. 将安全配置A指定给测试虚拟机 * 3. 在指定的虚机上，产生与失陷检测匹配的攻击流量 * 4. 等一两分钟，进入管理中心 分析-失陷检测页面查看日志 * 5. 查看虚机概况界面的失陷检测状态 * 6. 查看虚机详情的防火墙页面 * 7. 再次产生相同的攻击流量，查看分析—防火墙/网络管理日志 |
| 预期结果 | * 1. 安全配置A创建成功 * 2. N/A * 3. N/A * 4. 在分析-失陷检测页面中，可以看到与虚机产生攻击流量匹配的日志 * 5. 虚机名称变为绿色，在此虚机概况中的“失陷检测”，显示：已失陷，隔离状态：已隔离 * 6. 在虚机详情中的防火墙中，可以看到自动生成的隔离规则 * 7. 攻击失败，在分析—防火墙界面可以看到阻止日志，对应的规则正是刚刚自动生成的隔离规则 |

### 失陷主机监控

|  |  |
| --- | --- |
| **测试项目** | **失陷主机监控测试** |
| 测试步骤 | * 1. 进入管理中心，新增安全配置A，开启防火墙，开启失陷检测，失陷处理选择监控，保存安全配置 * 2. 将安全配置A指定给测试虚拟机 * 3. 在指定的虚机上，产生与失陷检测匹配的攻击流量 * 4. 等一二分钟，进入管理中心 分析-失陷检测页面查看日志 * 5. 查看虚机概况界面的失陷检测状态 * 6. 查看虚机详情的防火墙页面 * 7. 再次产生相同的攻击流量 * 8. 点击虚机概况界面失陷检测状态中隔离状态的未隔离，勾选刚刚攻击的恶意流量，点击隔离，再查看虚机详情的防火墙页面和失陷检测状态中的隔离状态 * 9. 再次产生相同的攻击流量，查看分析-防火墙/网络管理日志 |
| 预期结果 | * 1. 安全配置A创建成功 * 2. N/A * 3. N/A * 4. 在分析-失陷检测页面中，可以看到与虚机产生攻击流量匹配的日志 * 5. 虚机名称变为红色，在此虚机概况中的“失陷检测”，显示：已失陷，隔离状态：未隔离 * 6. 在虚机详情中的防火墙中，没有自动生成的隔离规则 * 7. 攻击仍能成功 * 8. 失陷检测状态中的隔离状态变为已隔离，虚机名称变为绿色，防火墙页面出现自动生成的隔离规则 * 9. 攻击失败，在分析-防火墙/网络管理界面可以看到阻止日志，对应的规则正是刚刚生成的隔离规则 |

### 威胁情报-隔离

|  |  |
| --- | --- |
| **测试项目** | **威胁情报隔离** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将Linux有代理虚拟机的安全配置中的失陷检测开启，行为选为隔离 * 在被测虚拟机上访问挖矿网站（可以通过ping挖矿域名模拟），产生对应挖矿域名的解析流量 * 查看挖矿网站的访问结果 * 查看分析>失陷检测日志信息 |
| 预期结果 | * N/A * N/A * N/A * 挖矿网站的访问被阻止 * 分析>失陷检测中生成对应的失陷日志，且日志记录的访问方式为阻止 |

### 威胁情报-监控

|  |  |
| --- | --- |
| **测试项目** | **威胁情报监控** |
| 测试步骤 | * 进入 管理中心 资产管理-虚拟机/终端 页面，将Linux有代理虚拟机的安全配置中的失陷检测开启，行为选为监控 * 在被测虚拟机上访问挖矿网站（可以通过ping挖矿域名模拟），产生对应挖矿域名的解析流量 * 查看挖矿网站的访问结果 * 查看分析>失陷检测日志信息 |
| 预期结果 | * N/A * N/A * 挖矿网站可以正常访问 * 分析>失陷检测中生成对应的失陷日志，且日志记录的访问方式为监控 |

## 入侵防御

本类用例主要测试奇安信网神统一服务器安全管理系统（有代理）的入侵防御相关功能。

### 入侵防御阻止测试-1

|  |  |
| --- | --- |
| **测试项目** | **入侵防御阻止测试1** |
| 测试步骤 | * 在被测虚拟机上开启远程连接 * 进入管理中心 安全策略-安全配置页面 * 点击“windows安全配置”，进入“入侵防御规则“页面 * 在“入侵防御规则“标签页中点击规则列表中第一列的，勾选”所有“，在右侧的搜索框中输入“CVE-2019-0708“，去勾选搜索结果中所有规则前的复选框，动作为阻止，点击保存 * 将0708detector.exe拷贝到本地任意目录， * 运行cmd.exe，输入命令0708detector.exe -t 192.168.91.138(要测试的目标IP) -p 3389(目标端口，一般都是3389)，查看输出结果 * 查看管理中心是否产生了入侵防御的日志 |
| 预期结果 | * 成功开启 * N/A * N/A * 保存成功 * N/A * 攻击失败，入侵防御功能生效，会输出Detect NLA enable！Server likely NOT vulnerable * 分析-入侵防御页面能看到入侵防御阻止的日志 |

### 入侵防御阻止测试-2

|  |  |
| --- | --- |
| **测试项目** | **入侵防御阻止测试2** |
| 测试步骤 | * 在被攻击虚拟机上开启远程连接 * 进入管理中心 安全策略-安全配置页面 * 点击“windows安全配置”，进入“入侵防御规则”页面 * 在“入侵防御规则“标签页中点击规则列表中第一列的，勾选”所有“，在右侧的搜索框中输入“8uc.linux1.cc”， 去勾选规则前的复选框，动作为阻止，点击保存 * 在所测试的虚拟机上打开cmd或者使用命令，进行ping 8uc.linux1.cc * 查看管理中心是否产生了入侵防御阻止的日志 |
| 预期结果 | * N/A * N/A * N/A * 保存成功 * Ping挖矿网站，解析挖矿网站DNS失败，被阻止 * 分析-入侵防御页面能看到入侵防御的日志 |

### 入侵防御检测测试

|  |  |
| --- | --- |
| **测试项目** | **入侵防御检测测试** |
| 测试步骤 | * 进入管理中心 安全策略-安全配置页面 * 点击“windows安全配置”，进入“入侵防御规则”页面 * 在“入侵防御规则“标签页中点击规则列表中第一列的，勾选”所有“，在右侧的搜索框中输入“8uc.linux1.cc”，确认该规则前复选框为勾选状态，实时防护打开，修改动作为检测，点击保存 * 在所测试的虚拟机上打开cmd或者使用命令，进行ping 8uc.linux1.cc * 查看分析页面是否产生了入侵防御的日志 |
| 预期结果 | * N/A * N/A * 安全配置保存成功 * ping挖矿网站，解析挖矿网站DNS成功，不会被阻止 * 分析-入侵防御页面能看到入侵防御检测的日志，记录为检测 |

### 3.10.4. 入侵防御白名单

|  |  |
| --- | --- |
| **测试项目** | **入侵防御白名单测试** |
| 测试步骤 | * 在被攻击虚拟机上开启远程连接 * 进入管理中心 安全策略-安全配置页面 * 点击“windows安全配置”，进入“入侵防御“页面 * 在“入侵防御规则“标签页中点击规则列表中第一列的，勾选”所有“，在右侧的搜索框中输入“CVE-2019-0708“，去勾选搜索结果中所有规则前的复选框 * 在“白名单“标签页中，源IP地址，地址列表填写运行0708detector.exe的机器IP，目的端口选择所有端口，点击保存 * 将0708detector.exe拷贝到需要执行0708规则的机器的任意目录 * 运行cmd.exe，输入命令0708detector.exe -t 192.168.91.138(要测试的目标IP) -p 3389(目标端口，一般都是3389)，查看输出结果 * 查看管理中心是否产生了入侵防御的日志 |
| 预期结果 | * N/A * N/A * N/A * N/A * 安全配置保存成功 * N/A * 攻击成功，入侵防御未能生效 * 分析-入侵防御页面没有对应的入侵防御日志 |

## 网络可视化及管理

本类用例主要测试奇安信网神统一服务器安全管理系统（有代理）的网络可视化及管理相关功能。

### 网络可视化及管理（网站）

|  |  |
| --- | --- |
| **测试项目** | **网络可视化及管理（网站）** |
| 测试步骤 | * 进入管理中心 安全策略-安全配置页面 * 点击“windows安全配置”，进入“网络可视化及管理”标签页 * 在左侧的“选择网络协议”栏中选择“商城/在线购物”，点击确定按钮 * 点击保存按钮，保存该安全配置 * 在测试虚拟机上访问商城或购物类网站，查看能否访问成功 * 在管理中心上是否能看网络管理阻止的日志 |
| 预期结果 | * N/A * N/A * N/A * 安全配置保存成功 * 5 在测试机上无法访问购物类网站 * 6 管理中心的分析-防火墙/网络管理页面有网络协议被阻止日志 |

### 网络可视化及管理（网络基础服务）-1

|  |  |
| --- | --- |
| **测试项目** | **网络可视化及管理（网络基础服务- ICMP）** |
| 测试步骤 | * 进入管理中心 安全策略-安全配置页面 * 点击“windows安全配置”，进入“网络可视化及管理”标签页 * 在搜索栏中输入”ICMP“ * 选择ICMP协议，点击”阻止“按钮，点击保存 * 在测试虚拟机上ping同一网段内的机器，查看能否ping成功 * 在管理中心上是否能看到ICMP被阻止的日志 |
| 预期结果 | * N/A * N/A * 输入ICMP后，下方的应用程序框中会显示名称中包含ICMP的网络基础服务 * 安全配置保存成功 * Ping不通其他机器 * 分析-防火墙/网络管理页面能够看到ICMP被阻止的日志 |

### 网络可视化及管理（网络基础服务）-2

|  |  |
| --- | --- |
| **测试项目** | **网络可视化及管理（网络基础服务- DNS）** |
| 测试步骤 | * 进入管理中心 安全策略-安全配置页面 * 点击“windows安全配置”，进入“网络可视化及管理”标签页 * 在搜索栏中输入” DNS “ * 选择DNS协议，点击”阻止“按钮，点击保存 * 在测试虚拟机上ping百度（www.baidu.com），查看能否ping成功 * 在管理中心上是否能看到DNS被阻止的日志 |
| 预期结果 | * N/A * N/A * 输入DNS后，下方的应用程序框中会显示名称中包含DNS的网络基础服务 * 安全配置保存成功 * 百度ping不通 * 分析-防火墙/网络管理页面能够看到DNS（114.114.114.114）被阻止的日志 |

## 虚拟机/终端策略

本类用例主要测试奇安信网神统一服务器安全管理系统（有代理）的虚机策略相关功能。

以下只是针对每个功能举了一个自定义虚拟机策略的例子，实际上安全配置中可以调整的配置均可以进行自定义。

### 防恶意软件

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机防恶意软件策略** |
| 测试步骤 | * 1. 测试虚拟机使用的是默认的windows安全配置，安全配置中恶意软件处理方式为隔离 * 2. 在 资产管理-虚拟机/终端页面，点击测试虚拟机名称，打开虚拟机策略页面，进入防恶意软件标签页，打开定制安全配置，配置恶意软件处理动作为删除，点击保存 * 3. 拷贝病毒文件至测试虚拟机中，查看病毒文件能否被查杀，查杀动作是删除还是隔离 |
| 预期结果 | * 1. N/A * 2. 点击保存后，虚拟机页面该测试虚拟机的安全配置名称后会出现一个标记，表示是自定义的配置 * 3. 病毒文件拷贝失败，被系统删除。分析-防恶意软件页面能看到杀毒日志，病毒文件状态为删除 |

### Webshell扫描

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机webshell扫描策略** |
| 测试步骤 | * 1. 测试虚拟机使用的安全配置中webshell扫描的定期扫描功能未开启 * 2. 在“资产管理”-“虚拟机/终端”，点击测试虚拟机名称，打开自定义虚拟机策略页面 * 3. 进入 webshell应用防护-webshell扫描页面，打开定制安全配置，配置定期扫描时间为每天某个时间点，点击保存 * 4. 到达指定时间点后，查看系统是否正常对测试虚拟机进行webshell扫描 |
| 预期结果 | * 1. N/A * 2. N/A * 3. webshell应用防护-webshell扫描页面中定制安全配置功能默认为关闭状态，修改保存后，测试虚拟机安全配置名称后带有“已定制”标记 * 4. 到达指定时间后，系统开始对测试虚拟机进行webshell扫描 ，扫描过程中，显示扫描正在进行，扫描能够正常结束；   能够正确显示扫描结果，包括上次扫描时间、后门文件数量；  日志分析的webshell扫描中能够正确显示测试虚拟机的后门文件信息 |

### 应用程序控制

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机应用程序控制策略** |
| 测试步骤 | * 1. 测试虚拟机使用的安全配置中，应用程序控制的实时管控功能默认为关闭 * 2. 进入测试虚拟机的虚拟策略-应用程序控制标签页，打开定制安全配置，打开实时管控 * 3. 配置允许系统应用程序，其他均为阻止，点击保存 * 4. 在测试虚拟机上访问应用程序路径列表中的应用，查看能否访问成功 * 5. 在测试虚拟机上访问应用程序路径列表之外的应用，查看能否访问成功 |
| 预期结果 | * 1. N/A * 2. N/A * 3. 点击保存后，测试虚拟机安全配置名称后会出现自定义标记 * 4. 在测试虚拟机上访问应用程序路径列表中的应用成功 * 5. 在测试虚拟机上访问应用程序路径列表外的应用失败，分析-应用程序控制页面能看到阻止日志 |

### 完整性监控

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机完整性监控策略** |
| 测试步骤 | * 1. 测试虚拟机使用默认的安全配置 * 2. 在资产管理-虚拟机/终端页面，点击测试虚拟机名称，打开自定义虚拟机策略页面 * 3. 进入虚拟机加固-完整性监控标签页，打开定制安全配置，开启实时监控，去勾选某条规则，点击保存 * 4. 在资产管理--虚拟机/终端，选择测试虚拟机，点击 安全操作-重新生成完整性基线 * 5. 根据去勾选的规则内容，在测试虚拟机进行相关操作 |
| 预期结果 | * 1. N/A * 2. N/A * 3. 点击保存后，测试虚拟机的安全配置名称后带有自定义标记 * 4. 生成完整性基线成功，虚拟机概况页面能看到扫描完成的时间 * 5. 系统不会监控该规则中的操作 |

### 漏洞管理

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机漏洞管理策略** |
| 测试步骤 | * 1. 测试虚拟机使用的安全配置中漏洞管理的定期扫描功能未开启 * 2. 在“资产管理”-“虚拟机/终端”，点击测试虚拟机名称，打开自定义虚拟机策略页面 * 3. 进入 虚拟机加固-漏洞管理页面，打开定制安全配置，配置定期扫描时间为每天某个时间点，点击保存 * 4. 到达指定时间点后，查看系统是否正常对测试虚拟机进行漏洞扫描 |
| 预期结果 | * 1. N/A * 2. N/A * 3. 虚拟机加固-漏洞管理页面中定制安全配置功能默认为关闭状态，页面中能够正确展示漏洞库的内容。点击保存后，测试虚拟机安全配置名称后带有自定义标记 * 4. 到达指定时间后，系统开始对测试虚拟机进行漏洞扫描 ，扫描过程中，显示扫描正在进行，扫描能够正常结束；   能够正确显示扫描结果，包括上次扫描时间、漏洞数量、漏洞详细信息  日志分析的漏洞管理中能够正确显示测试虚拟机的漏洞信息 |

### 安全基线

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机安全基线扫描策略** |
| 测试步骤 | * 1. 测试虚拟机使用的安全配置中安全基线扫描的定期扫描功能未开启 * 2. 在“资产管理”-“虚拟机/终端”，点击测试虚拟机名称，打开自定义虚拟机策略页面 * 3. 进入 系统加固-安全基线页面，打开定制安全配置，配置定期扫描时间为每天某个时间点，点击保存 * 4. 到达指定时间点后，查看系统是否正常对测试虚拟机进行安全基线扫描 |
| 预期结果 | * 1. N/A * 2. N/A * 3. 系统加固-安全基线页面中定制安全配置功能默认为关闭状态，修改保存后，测试虚拟机安全配置名称后带有“已定制”标记 * 4. 到达指定时间后，系统开始对测试虚拟机进行安全基线扫描 ，扫描过程中，显示扫描正在进行，扫描能够正常结束；   能够正确显示扫描结果，包括上次扫描时间、扫描得分；  日志分析的安全基线中能够正确显示测试虚拟机的安全基线信息 |

### 防暴力破解

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机防暴力破解扫描策略** |
| 测试步骤 | * 1. 测试虚拟机使用的安全配置中防暴力破解功能未开启 * 2. 在“资产管理”-“虚拟机/终端”，点击测试虚拟机名称，打开自定义虚拟机策略页面 * 3. 进入系统加固-防暴力破解页面，打开定制安全配置，打开防暴力破解功能，新增防暴力破解规则：60秒内，尝试登录超过10次，拦截10分钟，点击保存 * 4. 在攻击虚拟机上，60内尝试登录10次测试虚拟机，验证是否拒绝连接，且拦截时间为10分钟 * 5. 查看管理中心的分析-防暴力破解页面是否有对应日志 * 6. 查看虚机详情界面能否显示被攻击时间 |
| 预期结果 | * 1. N/A * 2. N/A * 3.系统加固-防暴力破解页面中定制安全配置功能默认为关闭状态，修改保存后，测试虚拟机安全配置名称后带有“已定制”标记 * 4. 触发防暴力规则后，防暴力破解程序开始拦截操作，被拦截机器10分钟之后才能访问 * 5、日志分析的防暴力破解中有对应虚拟机的阻止暴力破解次数统计信息 * 6、虚机详情界面能够显示最近被攻击时间 |

### 防火墙

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机防火墙策略-阻止ICMP出站** |
| 测试步骤 | * 1. 测试虚拟机使用默认的安全配置，安全配置中防火墙规则为空 * 2. 点击测试虚拟机名称，进入自定义虚拟机策略-防火墙页面，点击新增按钮，新增防火墙规则rule1, 阻止ICMP出站，配置远程IP为x.x.x.x，其他均为默认，点击确定后再点击保存 * 3. 在测试虚拟机上ping x.x.x.x这个地址 * 4. 在测试虚拟机上ping其他地址 |
| 预期结果 | * 1. N/A * 2. 防火墙规则rule1创建成功，点击保存后，测试虚拟机的安全配置名称后带有自定义标记 * 3. 在测试虚拟机上ping x.x.x.x失败，分析-应用防火墙页面能看到阻止日志，日志中安全配置名称后带有自定义标记 * 4. 在测试虚拟机上ping其他地址成功 |

### 失陷检测

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机失陷检测策略** |
| 测试步骤 | * 1. 测试虚拟机使用的是默认的windows安全配置，安全配置中失陷主机检测功能默认未开启 * 2. 在“资产管理-虚拟机/终端”页面，点击测试虚拟机名称，打开虚拟机策略页面 * 3. 进入“失陷检测”标签页，打开定制安全配置，开启“失陷检测”功能，点击保存 * 4. 在测试虚拟机上产生与失陷检测匹配的攻击流量 * 5. 在测试虚拟机概况页面中查看虚拟机的失陷情况 |
| 预期结果 | * 1. N/A * 2. N/A * 3. 测试虚拟机的安全配置名称后会出现自定义的标记 * 4. 在分析-失陷主机检测中，能够看到与测试虚机产生攻击流量匹配的日志 * 5. 测试虚拟机概况页面中显示虚拟机已失陷，未隔离 |

### 入侵防御

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机入侵防御策略** |
| 测试步骤 | * 1. 测试虚拟机使用默认的windows安全配置，安全配置中适用操作系统为windows，安全等级为高 * 2. 在资产管理-虚拟机/终端页面，点击测试虚拟机名称，进入自定义虚拟机策略页面 * 3. 进入入侵防御标签页，去勾选某个规则，点击保存 * 4. 进入windows安全配置-入侵防御页面，搜索该规则，查看该规则的勾选情况 * 5. 针对该规则构造对应的攻击，查看能否攻击成功 |
| 预期结果 | * 1. N/A * 2. N/A * 3. 点击保存后，测试虚拟机安全配置名称后带有自定义标记 * 4. windows安全配置中，该规则仍然是勾选状态 * 5. 针对去勾选的规则攻击成功 |

### 网络可视化及管理

|  |  |
| --- | --- |
| **测试项目** | **自定义虚拟机网络可视化及管理策略-阻止DNS** |
| 测试步骤 | * 1. 测试虚拟机使用默认的windows安全配置，安全配置中网络可视化及管理阻止和允许的协议均为空 * 2. 点击测试虚拟机的名称，打开虚拟机策略-概况页面，进入网络可视化及管理页面 * 3. 在网络可视化及管理页面，打开定制安全配置，配置阻止DNS，点击保存 * 4. 在测试虚拟机上ping百度（www.baidu.com），查看能否ping通 |
| 预期结果 | * 1. N/A * 2. N/A * 3. 该测试虚拟机安全配置名称后带有自定义标记 * 4. 在测试虚拟机上ping不通百度，分析-应用防火墙中能显示DNS被阻止的日志 |

# 产品管理功能

## 分组管理

### 分组及规则

|  |  |
| --- | --- |
| **测试项目** | **根据多个条件组件进行分组** |
| 测试步骤 | * 在管理中心虚拟机/终端页面，点击 分组管理-新增 * 在打开的 新增分组 对话框中输入分组的名称A，点击确定 * 在虚拟机/终端页面，点击 分组管理-分组规则 * 在分组规则页面点击 规则管理-新增 * 在分组规则对话框中输入规则名称、选择分组A、配置匹配条件为多个条件的组合，点击确定 * 返回虚拟机/终端页面，查看虚拟机/终端的分组情况 * 在实时监控和分析模块分别查看分组A下的统计信息 |
| 预期结果 | * N/A * 分组A创建成功 * N/A * N/A * 分组规则创建成功 * 匹配成功的虚拟机/终端全部被自动分配至分组A中 * 实时监控和分析模块能够正确显示分组A中的统计信息 |

### 匹配规则

|  |  |
| --- | --- |
| **测试项目** | **根据分组名称进行匹配** |
| 测试步骤 | * 1. 在安全策略-安全配置页面，创建安全配置A * 2. 创建匹配规则，输入名称、选择安全配置A，配置匹配条件为虚拟机/终端组B，点击确定 * 3. 查看虚拟机/终端组B中的虚拟机/终端所使用的安全配置 |
| 预期结果 | * 安全配置A创建成功 * 匹配规则创建成功 * 虚拟机/终端组B中的虚拟机/终端都自动匹配上了安全配置A，且该配置能够正常生效 |

## 配置维护

|  |  |
| --- | --- |
| **测试项目** | **配置导入导出** |
| 测试步骤 | * 在管理中心A中添加并部署云平台 * 添加相关配置 * 进入 管理-系统设置-备份恢复页面，点击“备份”，备份当前配置文件并下载 * 关闭管理中心A，创建新的管理中心B，IP配置为管理中心A的IP * 进入管理中心B的备份恢复页面，点击“恢复”，上传备份文件并恢复配置，将从管理中心A上导出的配置上传管理中心B * 测试系统基本功能是否正常 |
| 预期结果 | * 部署成功 * N/A * 配置导出成功 * N/A * 配置上传成功 * 系统基本功能均正常 |

## 域名解析

### 新增域名解析记录

|  |  |
| --- | --- |
| **测试项目** | **快速扫描测试** |
| 测试步骤 | * 进入 管理中心 点击 管理->系统设置->通用设置，滚动到最下方域名解析输入框 * 添加一条域名解析记录 10.1.1.1 www.test1.com，然后保存 * 按F5刷新页面 |
| 预期结果 | * 1. 能正常保存成功 * 2. 刷新后上面添加的记录依然存在 |

### 删除域名解析记录

|  |  |
| --- | --- |
| **测试项目** | **快速扫描测试** |
| 测试步骤 | * 进入 管理中心 点击 管理->系统设置->通用设置，滚动到最下方域名解析输入框 * 删除一条域名解析记录 10.1.1.1 www.test1.com，然后保存 * 按F5刷新页面 |
| 预期结果 | * 1. 能正常保存成功 * 2. 刷新后删除的域名解析记录不存在了 |

### 修改主机名

|  |  |
| --- | --- |
| **测试项目** | **快速扫描测试** |
| 测试步骤 | * 进入 管理中心 点击 管理->系统设置->通用设置 * 在通用设置->主机名中修改主机名为hosttest1，点击右侧保存 * 按F5刷新页面 * 滚动到最下方查看域名解析框里内容 |
| 预期结果 | * 1. 能正常保存成功 * 2. 刷新页面后仍然能展示修改后的主机名 * 3. 域名解析框新增 127.0.0.1 hosttest1和::1 hosttest1两条记录 |

## 通用设置

### 配置NTP服务器

|  |  |
| --- | --- |
| **测试项目** | **快速扫描测试** |
| 测试步骤 | * 进入 管理中心 点击 管理->系统设置->通用设置 * 在通用设置->NTP服务器中修改地址为ntp.ntsc.ac.cn，点击右侧保存 * 按F5刷新页面 |
| 预期结果 | * 1. 能正常保存成功 * 2. 刷新页面后仍然能展示修改后的NTP服务器地址 * 3. 管理中心本地时间展示正常，为最新时间 |

# 性能测试

|  |  |
| --- | --- |
| **测试项目** | **防病毒性能测试1：全盘扫描对虚机性能影响** |
| 测试步骤 | * 选择测试虚拟机 * 记录虚拟机资源占用情况：CPU、内存 * 进入管理中心虚拟机页面，选择 资产管理 =》 虚拟机/终端 * 选择测试虚拟机，点击全盘扫描 * 记录虚拟机资源占用情况：CPU、内存，并进行查杀前后资源占用对比 |
| 预期结果 | * 对比扫描前后虚拟机资源占用情况 |

|  |  |
| --- | --- |
| **测试项目** | **防病毒性能测试2：拷贝大量小文件** |
| 测试步骤 | * 大量小文件拷贝是最影响杀毒软件性能的一个特征，所以我们选择这个场景来做测试 * 在没部署防病毒或者关闭实时防护的情况下，拷贝文件并记录拷贝时间，CPU、内存占用情况 * 部署防病毒并开启实时防护，然后测试拷贝相同文件，记录拷贝时间以及CPU、内存占用情况 * 选择测试虚拟机，点击全盘扫描 * 记录虚拟机资源占用情况：CPU、内存，并进行查杀前后资源占用对比 |
| 预期结果 | * 对比前后两次拷贝文件时间、以及资源占用情况 |

# 测试总结

|  |  |  |  |
| --- | --- | --- | --- |
| *[添加客户测试小结]* | | | |
| 测  试  工  程  师 | 单位：  签名：  时间： | 审核人员 | 单位：  签名：  时间： |
| 测  试  用  户 | 单位：  签名：  时间： | | |

奇安信科技集团股份有限公司（简称：奇安信集团）