**虚拟化安全管理系统**

**T01R01P004U2B17H07测试报告**

修订历史

|  |  |  |  |
| --- | --- | --- | --- |
| 版本  | 日期 | 作者 | 更新原因 |
| V1.0 | 2020-08-10 | 赵阳 | 创建编写 |
|  |  |  |  |

目录

[一、新需求功能测试列表 4](#_Toc28337251)

[1.1测试环境 4](#_Toc28337252)

[1.2新需求测试列表 4](#_Toc28337253)

[1.3 修复的历史BUG列表 5](#_Toc28337254)

[二、基本功能回归测试 6](#_Toc28337255)

[三、安全性测试 7](#_Toc28337256)

[四、兼容性测试 7](#_Toc28337257)

[4.1 控制中心兼容性测试 7](#_Toc28337258)

[五、BUG情况统计 8](#_Toc28337259)

[5.1 BUG解决情况 8](#_Toc28337260)

[5.2 遗留bug列表 8](#_Toc28337261)

[六、测试结论 10](#_Toc28337262)

[6.1 测试结论 10](#_Toc28337263)

## 一、新需求功能测试列表

### 1.1测试环境

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | OS | CPU | 内存 |
| 服务端 | Centos 7.6 X86\_64 | 4U | 8G |
| 终端 | Windows 终端 | 4U | 4G |
| Linux终端 | 4U | 4G |

### 1.2新需求测试列表

|  |
| --- |
| P004U2B17H07新增需求和优化 |
| **功能项** | **功能检测** | **检查结果** |
| CSMP相关功能优化 | 支持CSMP获取网卡配置、静态路由、中控版本号，支持设置网卡、静态路由； | 通过 |
| 支持CSMP获取hsmp系统负载和磁盘占用率； | 通过 |
| 支持CSMP可以用ipv6访问HSMP； | 通过 |
| Linux IPS探测HTTP端口优化 | 改进之前探测TCP监听端口重复操作为记录非HTTP端口以便于下次不再探测。 | 通过 |
| 主机升级设置优化 | 系统设置->主机升级设置(4个更新时间设置为周的话，观察天数只能设置为7的倍数)。 | 通过 |
| windows升级优化 | 针对windows server 2003、XP等老版本，优化V3升级流程，实现散文件可在2003和XP等环境下不进行更新，解决低版本系统因为签名无法加载新文件签的问题。 | 通过 |

### 1.3 修复的历史BUG列表

| **Bug编号** | **Bug描述** | **测试结果** |
| --- | --- | --- |
| BUGS-2405 | kefu-【天津宁河】-【轻代理B15】-【导入平台提示未知】 | 通过 |
| BUGS-3752 | 【上海移动】-【轻代理B15H01】-【扫描任务下发不成功】 | 通过 |
| BUGS-1803 | 【中国移动】控制中心扫描存在漏洞 | 通过 |
| CSMPPROD-6643 | 【主机安全】hsmp磁盘只有50G，未自动扩容 | 通过 |
| XNHAQ-4345 | 【离线升级工具】使用离线升级工具下载特征库，某个模块下载失败后，再次下载，不管成功与否，在更新时，下载成功的模块也会更新失败 | 通过 |
| BUGS-4025 | 【嘉兴老年医疗医院】-【轻代理B17H05】-【客户端卡死】 | 通过 |
| BUGS-2820 | 【南京港集团】轻代理7.0快速扫描长时间无法完成，扫描到顽固病毒时，会弹窗提示重启 | 通过 |
| BUGS-2819 | 【南京港集团】轻代理7.0快速扫描长时间无法完成 | 通过 |
| BUGS-2756 | 【衡阳政务云】-【hsmpU2B13】-【webshell疑似后门文件确认】 | 通过 |
| BUGS-2252 | 【福建师范大学】-【轻代理 T01R01P004U2B15H01】-【部分linux客户端下发扫描任务执行失败】 | 通过 |
| BUGS-4414 | 【电科航电】-【虚拟化轻代理+B15H01】-【IE浏览器主页锁定】 | 通过 |
| BUGS-4442 | 【龙岗区中心医院】-【虚拟化安全轻代理B17H05】-【windows客户端离线故障】 | 通过 |
| BUGS-4305 | 【中铁上海工程局集团有限公司】-【虚拟化轻代理+T01R01P004U2B17H05】-【轻代理实时防护造成office文件放入网络盘中变只读】 | 通过 |
| BUGS-4255 | 【中公高科养护科技股份有限公司】-【轻代理7.0T01R01P004U2B05】-【入侵防御策略导致系统补丁安装失败】 | 通过 |
| BUGS-4074 | 【赛服(上海)网络科技有限公司】-【虚拟化轻代理】-【防暴力破解异常】 | 通过 |
| BUGS-4500 | 【重庆机场集团】-【虚拟化轻代理U2B17H05】-【虚拟机间歇性断网】 | 通过 |
| XNHAQ-3020 | 【松立集团】优先升级组配置观察两天，两天后未自动进行全网升级 | 通过 |
| CSMPPROD-7573 | 【主机安全】hsmp-p004u2b17h0711-20200617版本组件的hostname为“360hsmp” | 通过 |
| BUGS-5010 | 宁波第一医院】-【虚拟化轻代理+T01R01P004U2B17H05】-【客户端离线】 | 通过 |

## 二、基本功能回归测试

通过通用测试用例对基本功能进行回归验证，验证结果正常，基本功能列表如下：

|  |
| --- |
| P004U2B17H07回归验证 |
| **功能项** | **功能检测** | **检查结果** |
| 安装/卸载 | 控制中心安装/卸载 | 通过 |
| 客户端安装/卸载 | 通过 |
| 客户端安装后对OS影响 | 通过 |
| 客户端进程、心跳、服务等状态验证 | 通过 |
| 控制中心服务/进程状态检测 | 通过 |
| 病毒扫描 | 病毒查杀能力检测 | 通过 |
| 病毒库升级验证 | 通过 |
| 病毒查杀日志正确性 | 通过 |
| 病毒查杀对OS系统影响 | 通过 |
| 多引擎病毒检测能力验证 | 通过 |
| 实时监控 | 病毒文件监控能力验证 | 通过 |
| 病毒监控日志正确性 | 通过 |
| 监控和禁止指定文件创建 | 通过 |
| 安全基线 | 安全基线扫描验证 | 通过 |
| 安全基线自动修复功能 | 通过 |
| IPS | IPS基本功能防护能力 | 通过 |
| 特征库升级 | 通过 |
| 防火墙 | 防火墙控制能力验证 | 通过 |
| TCP、ICMP协议控制 | 通过 |
| Webshell扫描 | Webshell样本查杀能力验证 | 通过 |
| Webshell库升级 | 通过 |
| 防暴力破解 | 防爆力破解功能验证 | 通过 |
| 加白功能验证 | 通过 |
| 日志报表 | 病毒库、防火墙、IPS日志的导出 | 通过 |
| 主机升级、主机部署、日志导出 | 通过 |
| 虚拟化加固、安全扫描日志导出 | 通过 |
| 虚拟化加固 | Cloud加固功能验证 | 通过 |

## 三、安全性测试

无

## 四、兼容性测试

### 4.1 控制中心兼容性测试

控制中心兼容性测试，共测试8个OS系统，均测试通过 。

|  |  |
| --- | --- |
| **OS系统** | **测试结果** |
| Centos6.8 | 支持 |
| Centos6.9 | 支持 |
| Centos7.0 | 支持 |
| Centos7.3 | 支持 |
| Centos7.4 | 支持 |
| Centos7.5 | 支持 |
| Centos7.6 | 支持 |
| RedHat7.3 | 支持 |

## 五、BUG情况统计

### 5.1 BUG解决情况

 总Bug数17个，有效BUG数 16个；其中已解决并验证通过10个，4个属于历史问题或短期内无法解决问题。所有Later问题均经过研发、产品、二线、测试评估通过不影响版本发布。

### 5.2 遗留bug列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **关键字** | **概要** | **解决结果** | **优先级** | **提测版本** |
| [XNHAQ-4472](https://jira.qianxin-inc.cn/browse/XNHAQ-4472) | 【防暴力破解】windows防暴力破解不生效 | LATER | P2 | P004U2B17H07 |
| [XNHAQ-4544](https://jira.qianxin-inc.cn/browse/XNHAQ-4544) | 【入侵防御】centos8.0勾选301019规则，就无法访问httpd网站服务，动作即使为检测，都无法访问 | LATER | P2 | P004U2B17H07 |
| [XNHAQ-4545](https://jira.qianxin-inc.cn/browse/XNHAQ-4545) | 【入侵防御】centos8.0勾选312076、312829规则，就无法访问 http://IP:8080/st2/index.action，即使动作为检测 | LATER | P2 | P004U2B17H07 |
| [XNHAQ-4541](https://jira.qianxin-inc.cn/browse/XNHAQ-4541) | 【webshell扫描】windows自定义webshell扫描C:\，扫描出轻代理安装目录中有webshell疑似后门，文件路径c:\Program Files (x86)\360\360Safe\webshell\Quarantine | LATER | P2 | P004U2B17H07 |

## 六、测试结论

### 6.1 测试结论

上述遗留BUG均通过了产品、研发、测试、二线综合评估均属于不易复现或需要调整架构短期内不可修复的问题，版本可以正常发布，问题后续持续跟踪解决