**虚拟化安全管理系统**

**无代理**

**7.0.3 Patch3**

**版本发布更新说明**

|  |  |  |  |
| --- | --- | --- | --- |
| █文档编号 |  | █密级 | 内部使用 |
| █版本编号 | 7.0.3 Patch3（7.0.3.1705） | █日期 | 2020-08-17 |

* **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

| **版本** | **状态** | **修订理由和内容摘要** | **修订人** | **批准人** | **修订日期** |
| --- | --- | --- | --- | --- | --- |
| V1.0 | C-创建 | 新建文档 | 张英礼 |  | 2020-08-17 |
| V1.1 | M | 修改 | 马权 |  | 2020-08-17 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

状态：C-创建，A-增加，M-修改，D-删除

目录

[1 版本统计 4](#_Toc48587493)

[2 新增功能及修复历史问题列表 4](#_Toc48587494)

[2.1 新增云平台 4](#_Toc48587495)

[2.2 新增客户端操作系统 4](#_Toc48587496)

[2.3 客户问题 4](#_Toc48587497)

[2.4 南瑞继保 5](#_Toc48587498)

[2.5 应急管理部 6](#_Toc48587499)

[2.6 其他 6](#_Toc48587500)

[2.7 内部问题 6](#_Toc48587501)

[3 已解决问题 7](#_Toc48587502)

[4 已经去除的功能 9](#_Toc48587503)

[5 版本兼容性 9](#_Toc48587504)

[6 版本特别备注 9](#_Toc48587505)

[7 升级说明 9](#_Toc48587506)

# 版本统计

|  |  |
| --- | --- |
| **发行日期** | **版本编码** |
| 2020.08.17 | 7.0.3 Patch3（7.0.3.1705） |

# 新增功能及修复历史问题列表

## **新增云平台**

SVS（杰瑞服务器虚拟化系统）0602

OVirt兼容升腾KVM版本

平高云 8.0

H3C CAS V7.0 E0705

浪潮云管平台ICM 5.6.2

## **新增客户端操作系统**

欧拉 2.2 （仅文件模块）

CentOS 7.7

中兴新支点 v3.3.2

Ubuntu-16.04.6

Oracle linux 6.9

## **客户问题**

[BUGS-3546](https://jira.qianxin-inc.cn/browse/BUGS-3546) - 【河南省信息中心】-【虚拟化无代理+7.0.0.3046】-【版本升级+授权扩容】

[BUGS-3601](https://jira.qianxin-inc.cn/browse/BUGS-3601) - 【中华人民共和国应急管理部】-【7.0.3.1650】-【控制中心升级后无法访问】

[BUGS-3544](https://jira.qianxin-inc.cn/browse/BUGS-3544) - 【中华人民共和国应急管理部】-【无代理+7.0.3.1650】-【网络模块崩溃】

[BUGS-3599](https://jira.qianxin-inc.cn/browse/BUGS-3599) - 【中华人民共和国应急管理部】-【无代理+7.0.3.1650】-【icsfilesec进程CPU占用率高达800%，系统卡死】

[BUGS-3026](https://jira.qianxin-inc.cn/browse/BUGS-3026) - 【南瑞继保】-【无代理7.0.3.1650】-【防火墙策略不生效】

[BUGS-3659](https://jira.qianxin-inc.cn/browse/BUGS-3659) - 【中华人民共和国江苏海事局】-【无代理7.0.3.1650】-【vshield NSVM安装失败】

[BUGS-3682](https://jira.qianxin-inc.cn/browse/BUGS-3682) - 【中华人民共和国应急管理部】-【无代理7.0.3.1659】-【导入入侵防御日志规则说明不准确无法使用】

[BUGS-3129](https://jira.qianxin-inc.cn/browse/BUGS-3129) - 【咸阳网信办】-【虚拟化无代理+7.0.3-1600】-【vmsec\_nfq导致虚机卡死】

[BUGS-3781](https://jira.qianxin-inc.cn/browse/BUGS-3781) - 【中华人民共和国应急管理部】-【无代理+7.0.3.1659】-【替换walnut文件后网络模块再次崩溃】

[BUGS-3782](https://jira.qianxin-inc.cn/browse/BUGS-3782) - 【中华人民共和国应急管理部】-【无代理+7.0.3.1659】-【icsfilesec服务关闭后自启】

[BUGS-3958](https://jira.qianxin-inc.cn/browse/BUGS-3958) - 【甘肃省环保厅】-【虚拟化无代理+7.0.3-1500】linux虚拟机安装消息中心后cpu占用过高问题

[BUGS-3993](https://jira.qianxin-inc.cn/browse/BUGS-3993) - 【中国电信】-【虚拟化无代理+7.0.3.1600】-【客户端安装问题】

[BUGS-4331](https://jira.qianxin-inc.cn/browse/BUGS-4331) - 【中华人民共和国应急管理部】-【无代理+7.0.3.1659】-【云内虚机存在主动访问小红伞病毒库】

[BUGS-3821](https://jira.qianxin-inc.cn/browse/BUGS-3821) - 【国家开发银行】-【无代理7.0.3.1600】-【无法手动停止全盘扫描任务】

## 南瑞继保

1. 小红伞license不对导致文件模块起不来（客户端直接从中控下载license，中控增加了license的校验）
2. Windows有代理实时防护导致客户应用启动非常慢
3. Windows有代理增加针对计划任务为恶意可执行文件的清理
4. 以模板启动的虚拟机且vmid与同步到的vmid不一致，在同步脚本未同步到之前会注册成新注册主机，最终导致出现两个虚拟机
5. Windows有代理计划任务支持策略配置白名单

## 应急管理部

1. 有代理客户端小红伞特征库升级只从管理中心升级，升级配置注释掉从小红伞官网升级的链接
2. 有代理客户端及无代理主机端升级脚本，根据当前服务的启停状态来决定升级后是否需要启停服务

## 其他

1. 浪潮新增主机池时，部分虚机vmid为空时，虚机策略初始化插入数据库异常，导致页面看不到主机虚机列表，一直在同步中
2. ManageOne运营面接口调整：接口添加composedName字段显示租户名称，防止重名租户
3. easystack网络双栈同步到ipv6地址，导致虚机详情页面异常
4. 【铁四院】-【虚拟化安全无代理+7.0.3\_1650】-【防火墙规则不生效】

## **内部问题**

1. 特征库升级时去除license中小红伞引擎检测，默认更新小红伞特征库：windows有代理只支持小红伞引擎
2. CSMP单租户授权创建不成功
3. XNHAQ-4049 失陷检测日志发生部分丢失，总数与详情中日志数量不匹配
4. OpenStack有代理非多租部署时，主机端获取不到groupid，漏洞扫描失败
5. CSMPDZ-204:【第三方组件】无代理主机安全组件在授权足够的情况下授权过期
6. 【LTS】【urgent\_hotfix】老版的ip失陷检测生成的日志，只能看到原始日志，无法显示数量及柱状图和折线图，威胁情报集成的失陷检测日志是正常的
7. 修复系统诊断下载权限错误
8. CSMPPROD-6814:【VSMS】【第三方组件】无代理dhcp获取不到ipv6地址
9. 【LTS】【urgent\_hotfix】在703-1650或者升级后的1670环境上部署HA后，发现备机/opt/nubosh/vmsec-ctrl/patch/cluster目录缺少文件，此问题会导致管理中心升级失败
10. XNHAQ-4423【LTS】【1674】管理中心点击产品诊断“开始诊断”后，点击“结束诊断”，界面报406错误

# 已解决问题

|  |  |
| --- | --- |
| **关键字** | **概要** |
| [XNHAQ-4574](https://jira.qianxin-inc.cn/browse/XNHAQ-4574) | 【资产管理】新增主机池后，主机页面同步不到华为云平台的主机列表 |
| [XNHAQ-4468](https://jira.qianxin-inc.cn/browse/XNHAQ-4468) | 【性能测试】管理中心3500台虚机长时间压力下日志处理积压及tomcat日志报错问题 |
| [XNHAQ-4583](https://jira.qianxin-inc.cn/browse/XNHAQ-4583) | 【主机端升级】有代理linux和无代理主机均升级失败 |
| [XNHAQ-4580](https://jira.qianxin-inc.cn/browse/XNHAQ-4580) | 【网络模块】有代理Linux网络模块启动时打印异常 |
| [XNHAQ-4532](https://jira.qianxin-inc.cn/browse/XNHAQ-4532) | 【主机端升级】NSX6.7升级文件信息对比问题汇总 |
| [XNHAQ-4558](https://jira.qianxin-inc.cn/browse/XNHAQ-4558) | 【主机端升级】主机升级后未清除commsrv pid文件 |
| [XNHAQ-4530](https://jira.qianxin-inc.cn/browse/XNHAQ-4530) | 【主机端升级】有代理linux升级文件信息对比问题汇总 |
| [XNHAQ-4571](https://jira.qianxin-inc.cn/browse/XNHAQ-4571) | 【管理中心升级】升级包中带的老版本威胁情报库覆盖了已有的最新版本特征库文件，但未修改版本号，导致无法再升级至最新 |
| [XNHAQ-4533](https://jira.qianxin-inc.cn/browse/XNHAQ-4533) | 【主机端升级】Xen升级文件信息对比问题汇总 |
| [XNHAQ-4500](https://jira.qianxin-inc.cn/browse/XNHAQ-4500) | 【云查杀】ISO及升级包内带的云查引擎未更新导致云查失效 |
| [XNHAQ-4528](https://jira.qianxin-inc.cn/browse/XNHAQ-4528) | 【管理中心升级】7.0.2.3366管理中心升级到7.0.3.1697后没有完整性监控规则 |
| [XNHAQ-4570](https://jira.qianxin-inc.cn/browse/XNHAQ-4570) | 【安全配置】新建或者编辑任意防火墙规则时，光标停留在【名称】输入框时，输入回车，页面却跳转至新建安全配置页面 |
| [XNHAQ-4474](https://jira.qianxin-inc.cn/browse/XNHAQ-4474) | 【网络模块】有代理CentOS8网络模块3:40停止后未能自动拉起 |
| [XNHAQ-4510](https://jira.qianxin-inc.cn/browse/XNHAQ-4510) | 【防恶意软件】病毒文件缓存7天超时后仍可查杀，需重启文件模块过滤超时病毒文件缓存后才不再查杀 |
| [XNHAQ-4508](https://jira.qianxin-inc.cn/browse/XNHAQ-4508) | 【稳定性】openstack云平台，siege压测1小时，walnut进程挂掉，segfault at 14 ip 00000000005d0210 sp 00007f1fc77f5620 error 4 in walnut[400000+32c000] |
| [XNHAQ-4460](https://jira.qianxin-inc.cn/browse/XNHAQ-4460) | 【系统更新】openstack有代理部署，在虚机页面点击更新指定虚机和更新指定虚机特征库均无反应，在主机页面点击才有效 |
| [XNHAQ-4531](https://jira.qianxin-inc.cn/browse/XNHAQ-4531) | 【主机端升级】H3C升级文件信息对比问题汇总 |
| [XNHAQ-4549](https://jira.qianxin-inc.cn/browse/XNHAQ-4549) | 【分析-日志】【patch升级】失陷检测原始日志详情点击无反应 |
| [XNHAQ-4547](https://jira.qianxin-inc.cn/browse/XNHAQ-4547) | 【主机升级】NSX从3366升级到1650再升级到1701时未更新文件模块和网络模块 |
| [XNHAQ-4473](https://jira.qianxin-inc.cn/browse/XNHAQ-4473) | 【完整性监控】无代理CentOS8和ubuntu16.04.6完整性监控扫描不到结果 |
| [XNHAQ-4517](https://jira.qianxin-inc.cn/browse/XNHAQ-4517) | 【防恶意软件】NSX全盘扫描有漏扫现象，第二次扫描才能扫描到病毒文件 |
| [XNHAQ-4525](https://jira.qianxin-inc.cn/browse/XNHAQ-4525) | 【网络模块】有代理Windows使用安全配置适用操作系统为所有操作系统时，入侵防御功能失效，walnut占用内存仅90M |
| [XNHAQ-4543](https://jira.qianxin-inc.cn/browse/XNHAQ-4543) | 【完整性监控】有代理Linux手动停止完整性监控服务后仍会被守护进程拉起 |
| [XNHAQ-4498](https://jira.qianxin-inc.cn/browse/XNHAQ-4498) | 【应用程序控制】Windows有代理阻止其他应用程序时会阻止完整性监控进程 |
| [XNHAQ-4550](https://jira.qianxin-inc.cn/browse/XNHAQ-4550) | 【syslog】【patch升级】租户下syslog配置默认端口号为空 |
| [XNHAQ-4563](https://jira.qianxin-inc.cn/browse/XNHAQ-4563) | 【特征库】漏洞特征库显示为漏洞库特征库 |
| [XNHAQ-4562](https://jira.qianxin-inc.cn/browse/XNHAQ-4562) | 【安装部署】【patch升级】有代理欧拉2.2安装部署注册到管理中心失败，且卸载common模块失败 |
| [XNHAQ-4527](https://jira.qianxin-inc.cn/browse/XNHAQ-4527) | 【管理中心升级】7.0.2.3366管理中心升级到7.0.3.1697后安装CentOS8失败 |
| [XNHAQ-4509](https://jira.qianxin-inc.cn/browse/XNHAQ-4509) | 【安装部署】安装VShield安全虚机后管理中心显示连接中断 |
| [XNHAQ-4493](https://jira.qianxin-inc.cn/browse/XNHAQ-4493) | 【安装部署】vcenter修改端口后VShield安装部署安全虚机失败 |
| [XNHAQ-4496](https://jira.qianxin-inc.cn/browse/XNHAQ-4496) | 【安装部署】浪潮云管平台添加界面地址栏提示信息未添加端口 |
| [XNHAQ-4463](https://jira.qianxin-inc.cn/browse/XNHAQ-4463) | 【分析日志】一分钟内的原始日志乱序 |
| [XNHAQ-4454](https://jira.qianxin-inc.cn/browse/XNHAQ-4454) | 【特征库升级】管理中心小红伞特征库文件权限为root导致有代理Windows特征库升级下载文件error |
| [XNHAQ-4490](https://jira.qianxin-inc.cn/browse/XNHAQ-4490) | 【安装部署】手动安装deb/rpm包运行注册脚本部署有代理Linux会注册两次 |
| [XNHAQ-4471](https://jira.qianxin-inc.cn/browse/XNHAQ-4471) | 【云查升级】CentOS8云查引擎升级时报错，日志显示升级成功，但动态库文件未替换 |
| [XNHAQ-4461](https://jira.qianxin-inc.cn/browse/XNHAQ-4461) | 【云查】有代理linux无代理的云查引擎升级均失败，显示No module named numpy |
| [XNHAQ-4450](https://jira.qianxin-inc.cn/browse/XNHAQ-4450) | 【安装部署】CentOS8.0安装部署失败，手动安装网络模块提示没有python |
| [XNHAQ-4459](https://jira.qianxin-inc.cn/browse/XNHAQ-4459) | 【安装部署】ubuntu16.04.6安装完安全组件或消息中心后linux命令失效，提示No such file or directory |

# 已经去除的功能

无

# 版本兼容性

7.0.2，7.0.3可平滑升级至7.0.3.1705版本

# 版本特别备注

无

# 升级说明

与之前版本升级方法相同，下面是升级步骤：

升级控制中心

提前准备好升级更新包。从控制中心的“资产管理”->“主机”页面，选择“系统更新”菜单下的“上传更新包”，上传升级更新包。

升级主机安全组件和有代理组件

在“主机”页面选择要升级的无代理或有代理主机，然后选择“系统更新”菜单下的“更新指定主机”；或者选择菜单下的“更新全部主机”。