[2014-06-10]H3C SecCenter 2.10-E0035H01版本发布

马光彬 2014-06-25 发表

H3C SecCenter 2.10-E0035H01的版本发布

一 适用范围及配套说明

H3C SecCentr 2.10-E0035H01版本正式发布，使用范围为国内和海外市场。

1、历史版本号

历史版本号如表1所示：

表1 历史版本号

版本号	基础版本号	发布日期	发布组件	备注
E0034H01	E0034	2014-03-27	FWM UTMM ACGM IPSM	解决问题
E0035	E0034H01	2014-04-30	FWM UTMM ACGM IPSM	新增特性 解决问题
E0035H01	E0035	2014-06-10	FWM UTMM ACGM IPSM	解决问题

2、版本配套表

版本号	配套设备、软件名称及版本号	
SecCenter 2.10- E0035H01	组件	产品型号及版本
	ACGM	H3C SecPath ACG8800-S3：E6511 及以上 H3C SecPath ACG2000-M：E6113及以上 H3C SecBlade ACG插卡：E6113及以上 注：基于段的带宽策略、QoS通道策略管理、通道日志分析、丢弃流量分析功能只支持iwareB35主线版本； ACG配置文件导入导出适用于下述软件版本： ACG2000/SecBlade ACG：E6119P02 ACG8800-S3：无支持版本
	IPSM	T1000-S/T1000-M/T1000-A/T1000-C: E1218P05及以上 T200S：E1603及以上 T200、T200E:B1122及以上 T200A/M: E1204P01及以上 SecBlade IPS插卡： E2108及以上 T5000-S3：E1504及以上 注：IPS设备软件版本部署功能只支持版本号为E1222P05的版本； IPS配置文件导入导出适用于下述软件版本： T1000-A/M/S/C：E1222P06 T200-A/M：无支持版本 T200-S：无支持版本 T5000-S3：无支持版本 SecBlade IPS：E2113P04 SecBlade IPS Enhanced：R3807
	FWM	H3C SecPath F1000系列：R3166P12及以上 H3C SecBlade FW插卡:R3166P12及以上 H3C SecPath F5000-A5：R3206及以上 H3C SecBlade SSL VPN 插卡：E7110及以上 H3C SecPath F5000-C/F5000-S：R3808及以上
	UTMM	H3C SecPath U200系列：R5116及以上 H3C SecPath U200系列：R5139及以上 注： “深度防御”策略管理适用于设备软件版本为R5139及以上的UTM设备；

3、 版本使用限制

1、 安装目标文件夹名称及其路径必须为英文。

2、安装环境要专机专用，不要将SecCenter与其他公司网管产品安装在同一台计算机上。SecCenter产品卸载完成后，如果要重新安装，则必须重新启动服务器。

3、SecCenter安装完成后注意必须重新启动操作系统。

4、SecCenter WEB管理台采用80端口，请确保无其他服务使用80端口（通常，Windows 2003 Server的World Wide Web Publishing服务使用80端口，请在“服务管理器”中将该服务停止并将其启动方式设为“手动”或“已禁用”）。

5、由于SecCenter是一个实时分析系统，对CPU和IO资源的占用较高，正式使用时请使用专用服务器安装。

6、SecCenter使用了不同的守候端口处理设备发送的日志信息，请注意设备侧的配置：

l 带宽管理使用了NetStream V9日志，默认端口为30010。
l 行为审计功能使用Syslog日志，默认端口为30514。
l NAT日志审计功能使用防火墙二进制日志，默认端口为30017。
7、正确配置服务器的时间和时区，由于SecCenter要进行license授权，授权后如果改动服务器时间和时区将导致SecCenter授权不可用，这时只能重装SecCenter。时区要配置为东八区（北京时间）。
8、对于在win7系统下无法停止SecCenter相关服务的情况，请使用内置Administrator账户登录后操作，或更改用户帐户控制设置为“从不通知（不推荐）”，也可先退出SecCenter监视器，后右键点击“以管理员身份运行”，即可解决问题。
9、为保证系统性能，用户名反查方式为iMC反查时，在线用户列表每两分钟增量更新一次。反查方式为CAMS时，支持历史用户行为审计。
10、若在IE10浏览器下使用本系统，请打开菜单栏中“工具”菜单，勾选“兼容性视图”选项。
11、若需使用IPS软件部署、软件自动升级功能，请配合IPS软件E1222P05版本使用。
12、对于使用Https方式访问设备，目前只支持使用设备的缺省证书；如果用户自行更新了设备的证书，请使用下述方式恢复：
恢复设备default证书的方法：
删除设备存储的hostkey，default_ca.cer，default_local.cer 文件，保存配置后重启设备即可，例如：
<H3C>dir /all
Directory of cfa0:/
0 -rw- 39012268 Apr 19 2012 16:37:32 u200s.bin
1 drw- - Apr 19 2012 15:23:14 seclog
2 -rw- 833 Apr 28 2012 10:38:42 system.xml
3 -rwh 480 Apr 28 2012 10:31:20 private-data.txt
4 -rwh 735 Apr 23 2012 07:03:20 hostkey
5 -rw- 11349 Apr 28 2012 10:31:20 config.cwmp
6 -rwh 4 Apr 28 2012 10:33:24 snmpboots
7 -rw- 23127544 Apr 19 2012 17:48:36 u200ssingle.bin
8 -rw- 891 Apr 28 2012 10:33:12 default_ca.cer
9 -rw- 39012268 Apr 19 2012 17:53:30 u200s108.bin
10 -rw- 1574 Apr 23 2012 09:16:30 https-server.p12
11 -rwh 567 Apr 26 2012 16:45:12 dsakey
12 -rw- 1411 Apr 28 2012 10:33:12 default_local.cer
二 增减特性说明
无。
三 相对前一版本解决的问题
1. ACGM，系统管理>系统配置>业务参数配置中IP组允许的最大IP数配置无效
问题现象：修改IP组允许的最大IP数后，SecCenter下发到ACG设备每个IP组里的IP数量未变，仍是修改之前的数量。
问题产生条件：无。
2. 系统管理>设备管理>设备列表，添加设备时页面中置灰的输入框中还可以输入内容
问题现象：灰色输入框可以输入内容。
问题产生条件：无。
3. SecCenter删除基于用户组的带宽策略后，再删除用户组，设备上对应的用户组未被删除
问题现象：SecCenter向设备下发基于用户组的带宽策略后，删除该策略，再删除用户组，设备上对应的用户组未被删除。
问题产生条件：无。
4. 对于插卡ACG设备，多次下发同一通道策略，只有第一次成功
问题现象：对插卡设备下发通道策略，成功后修改该策略再次下发，下发失败。
问题现象：管理设备为插卡设备。
5. 带宽管理，增加通道策略配置，输入不合法时提示语为英文
问题现象：增加通道策略，策略类型选择“带宽保证”或“带宽限制”，输入不合法时弹出英文提示。
问题产生条件：无。
6. 流量分析>用户业务分析>单用户实时流量监控，批量删除监控IP时的删除策略需优化
问题现象：SecCenter批量删除监控IP时，对设备的操作为每删除一个IP，激活保存一次配置。
这样导致删除IP较多时，需要等待较长时间才能操作设备。现已修改为：删除全部IP后，再执行一次激活、保存操作。
问题产生条件：无。

7. 流量分析>IP组业务分析>IP组峰值流量趋势描述为英文

问题现象：页面有数据时，表格下方的峰值流量及达到峰值时间显示为英文。

问题产生条件：页面有数据时。

8. 流量分析>通道流量分析，按通道查询数据，导出的excel表头没有显示查询的通道名称

问题现象：选择设备及其对应的通道，查询后导出为excel，导出文件的表头未显示所选通道名称。

问题产生条件：无。

9. ACGM，设备管理中删除ACG设备后，流量分析中多个页面仍有数据

问题现象：在系统管理>设备管理中删除ACG设备后，流量分析中“网络流量快照”、 “网络会话快照”、“TOP 用户流量列表 ”、“会话明细统计”仍然有数据。

问题产生条件：无。

10. 行为审计>审计日志备份>手动立即备份操作日志不正确，任务备份无操作日志

问题现象：手动立即备份审计日志，查看造作日志，组件一栏乱码。配置任务备份后无操作日志。

问题产生条件：无。

11. 在设备上修改IPS默认攻击策略规则后，执行SecCenter导入特征库操作， SecCenter默认攻击策略的默认状态错误

问题现象：在设备上修改IPS默认攻击策略规则后，执行SecCenter导入特征库操作，发现SecCenter默认攻击策略对应规则动作、状态和设备一致，但默认状态错误。实际上SecCenter应该和特征库保持一致。

问题产生条件：无。

12. 下发包含IP地址组的IPS策略到设备后，删除该策略及IP组，重新建相同名称的IP组，下发策略失败

问题现象：下发包含IP地址组的IPS策略到设备后，删除该策略及IP组，重新建相同名称的IP组，下发策略失败。

问题产生条件：无。

13. FWM系统管理左树缺少“设备软件库”和“部署任务”两个页面的链接

问题现象：FWM系统管理，若需查看“设备软件库”及“部署任务”，只能从设备列表>设备软件管理>备份设备软件按钮进入。目前左树菜单增加链接可直接进入。

问题产生条件：无。

14. 深度防御>防病毒策略应用，同时清空多台设备的防病毒策略及应用时，只有一台能彻底清空

问题现象：同时选择两台或两台以上设备清空防病毒策略及应用，只有一台能彻底清空。

问题产生条件：同时清空多台设备。

15. 深度防御>防病毒策略应用，修改已下发到多台设备的防病毒策略，只有一台设备能修改成功

问题现象：将防病毒策略下发到多台UTM设备后立即修改防病毒策略，只有一台能修改成功。

问题产生条件：将策略下发给多台设备后立即修改策略。

16. 配置文件中修改DDoSCache=0后重启接收器，DDoS还是以缓存方式处理,修改没有生效

问题现象：配置文件中修改DDoSCache=0后重启接收器，DDoS任然以缓存方式处理,修改没有生效。

问题产生条件：无。

如要完整的了解该版本累计解决的软件BUG，请参看配套的《H3C SecCenter2.10-E0035H01版本说明书》。