SCA 1.0 (E0503)版本说明书

|  |  |
| --- | --- |
| Copyright © 2017新华三技术有限公司版权所有，保留一切权利。  非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，  并不得以任何形式传播。本文档中的信息可能变动，恕不另行通知。 | H3C_彩色.emf |

目 录

[1 版本信息 1](#_Toc494374055)

[1.1 版本号 1](#_Toc494374056)

[1.2 历史版本信息 1](#_Toc494374057)

[2 软件运行环境 1](#_Toc494374058)

[2.1 硬件配置表 1](#_Toc494374059)

[2.2 客户端配置要求 2](#_Toc494374060)

[3 版本使用限制及注意事项 2](#_Toc494374061)

[4 版本特性说明 4](#_Toc494374062)

[4.1 首页 4](#_Toc494374063)

[4.2 拓扑 4](#_Toc494374064)

[4.3 综合监控 4](#_Toc494374065)

[4.4 安全策略管理 5](#_Toc494374066)

[4.5 事件分析 6](#_Toc494374067)

[4.6 行为审计 7](#_Toc494374068)

[4.7 安全评估 7](#_Toc494374069)

[4.8 安全响应 7](#_Toc494374070)

[4.9 风险分析 8](#_Toc494374071)

[4.10 安全运维 8](#_Toc494374072)

[4.11 资产管理 8](#_Toc494374073)

[4.12 转储配置 9](#_Toc494374074)

[4.13 大屏展示 9](#_Toc494374075)

[4.14 系统管理 9](#_Toc494374076)

[5 版本变更说明 10](#_Toc494374077)

[5.1 特性变更说明 10](#_Toc494374078)

[5.1.1 SCA 1.0 (E0503) 10](#_Toc494374079)

[5.1.2 SCA 1.0 (E0501) 10](#_Toc494374080)

[5.1.3 SCA 1.0 (E0202) 11](#_Toc494374081)

[5.2 操作方式变更说明 11](#_Toc494374082)

[6 存在问题与规避措施 11](#_Toc494374083)

[7 解决问题列表 11](#_Toc494374084)

[7.1 SCA 1.0 (E0503)版本解决问题列表 11](#_Toc494374085)

[7.2 SCA 1.0 (E0501)版本解决问题列表 12](#_Toc494374086)

[7.3 SCA 1.0 (E0202)版本解决问题列表 13](#_Toc494374087)

[8 相关资料 13](#_Toc494374088)

[8.1 相关资料清单 13](#_Toc494374089)

[8.2 资料获取方法 13](#_Toc494374090)

[9 技术支持 13](#_Toc494374091)

[10 版本升级操作指导 14](#_Toc494374092)

[10.1 前提 14](#_Toc494374093)

[10.2 备份SecCenter A2000 14](#_Toc494374094)

[10.3 升级SecCenter A2000 14](#_Toc494374095)

[10.4 恢复SecCenter A2000 20](#_Toc494374096)

[11 软件注册说明 21](#_Toc494374097)

[11.1 获取SecCenter A2000设备信息文件 21](#_Toc494374098)

[11.2 获取License 22](#_Toc494374099)

[11.3 SecCenter A2000注册 23](#_Toc494374100)

表目录

[表1 历史版本信息表 1](#_Toc494374101)

[表2 硬件预装配置表 1](#_Toc494374102)

[表3 客户端配置表 2](#_Toc494374103)

[表4 首页特性列表 4](#_Toc494374104)

[表5 拓扑特性列表 4](#_Toc494374105)

[表6 综合监控特性列表 4](#_Toc494374106)

[表7 安全策略管理特性列表 5](#_Toc494374107)

[表8 事件分析特性列表 6](#_Toc494374108)

[表9 行为审计特性列表 7](#_Toc494374109)

[表10 安全评估特性列表 7](#_Toc494374110)

[表11 安全响应特性列表 7](#_Toc494374111)

[表12 风险分析特性列表 8](#_Toc494374112)

[表13 安全运维特性列表 8](#_Toc494374113)

[表14 资产管理特性列表 8](#_Toc494374114)

[表15 转储配置特性列表 9](#_Toc494374115)

[表16 大屏展示特性列表 9](#_Toc494374116)

[表17 系统管理特性列表 9](#_Toc494374117)

[表18 SecCenter A2000组件版本列表 15](#_Toc494374118)

# 版本信息

## 版本号

全称：H3C安全管理中心, Version 1.0, ESS 0503

简称：SCA 1.0 (E0503)

**[注]：**在安全管理中心首页右上角下拉菜单中选择“关于”，进入产品信息页面查看版本号。

## 历史版本信息

历史版本信息表

| 版本号 | 基础版本号 | 发布日期 | 备注 |
| --- | --- | --- | --- |
| SCA 1.0 (E0503) | SCA 1.0 (E0501) | 2017-09-30 | 无 |
| SCA 1.0 (E0501) | SCA 1.0 (E0202) | 2017-04-28 | 受限研发确认局点 |
| SCA 1.0 (E0202) | SCA 1.0 (E0201) | 2016-11-21 | 无 |
| SCA 1.0 (E0201) | SCA 1.0 (E0101) | 2016-09-29 | 无 |
| SCA 1.0 (E0101) | 首次发布 | 2016-04-05 | 无 |

# 软件运行环境

## 硬件配置表

表2列出了SecCenter A2000的出厂硬件配置。

硬件预装配置表

| 产品系列 | SecCenter 系列 |
| --- | --- |
| 型号 | SecCenter A2000 |
| CPU | 2\*6核处理器，主频2.4GHz |
| 内存 | 标配64G，满配128G |
| 硬盘 | 标配2\*500G系统盘，RAID 1模式  提供12个数据盘位，可根据需要选配2T/4T容量的硬盘，数据盘推荐按照RAID 10模式配置 |
| Console口 | 1\*RJ45，RS232，9600~115200bps |
| USB | 1\*USB2.0+2\*USB3.0 |
| VGA | 1个VGA接口 |
| 网口（标配） | 6\*GE（10/100/1000 BASE-T） |
| 扩展槽 | 2 |
| 接口卡（选配） | 2端口10GE光接口网卡  2端口10GE电接口网卡  4端口GE电接口网卡 |
| 电源 | 标配1个900W电源，满配2个900W电源（1+1冗余） |
| 环境温度 | 工作：5～35℃  非工作：-40～65℃ |
| 环境湿度 | 工作时：10%~80%  非工作：5～95%，无冷凝 |
| 机箱尺寸（H×W×L） | 87.5mm（2U） x 446mm x 650mm |
| 重量范围（Kg） | 12～27kg |
| 配件 | 2U导轨组件（选配）  2U挂耳组件（选配）  2U走线管理支架（选配） |
| 备注 | 无 |

## 客户端配置要求

表3列出了客户端配置要求。

客户端配置表

| 项目 | 描述 |
| --- | --- |
| 操作系统 | Windows（简体中文版） |
| 硬件要求 | 主频2.0G Hz（以上）  内存2GB（以上）  硬盘50GB（以上）  100M网卡（以上）  声卡 |
| 浏览器配置要求 | 关闭浏览器的弹出窗口阻塞设置  必须使能浏览器的Cookies  将SecCenter A2000站点加入受信任站点  桌面分辨率显示宽度至少为1280  推荐使用IE 10或IE 11  推荐使用Firefox 30及以上版本  推荐使用Chrome 35及以上版本 |

# 版本使用限制及注意事项

#### 浏览器类

* + - * 1. 对Firefox浏览器支持不完善，个别页面可能存在显示问题，但不影响正常使用。
        2. 缩小浏览器窗口登录SecCenter A2000，最大化浏览器后页面不能自动调整大小，手动刷新页面即可恢复正常。

#### 数据库类

* + - * 1. 在数据库发生重启的情况下，必须重新启动SecCenter A2000。

#### 分布式部署类

* + - * 1. 在SecCenter A2000主服务器启动之前，请不要启动SecCenter A2000从服务器，否则会导致某些进程启动失败。分布式部署完成后，主服务器和从服务器的启动与停止将由主服务器统一控制。
        2. 主从分布式环境升级时，每个从机的平台升级至E0504版本之后，执行“/opt/iMC/deploy/instInfoMgr.sh -motify dbAddr=主机数据库的IP地址”。通过“/opt/iMC/deploy/instInfoMgr.sh -query”查看修改是否成功。

#### 设备版本兼容性

* + - * 1. 对于V7设备，SCA 1.0 (E0202)版本只支持Comware V700R001B64D014至Comware V700R001B64D021之前版本。
        2. 对于V7设备，SCA 1.0 (E0501)及其后续版本只支持Comware V700R001B64D022及其以上版本。

#### 设备配置类

* + - * 1. 当系统中的应用较多时，如大于500个，应用监视页面显示时间需要10秒左右。
        2. 试用版本默认支持最多添加5个安全设备。
        3. 由于IPS策略功能发生变化，升级该版本后会清空旧的IPS策略，升级后需要重新配置。
        4. 同步安全设备时，需要在设备详细信息页面配置正确的NetConf参数，否则会导致安全设备列表中的设备同步失败。
        5. 同一安全设备的“同步”和“配置”操作，不宜同时进行，否则会导致SecCenter A2000中该安全设备下业务配置信息混乱。
        6. 物理安全设备配置Telnet用户名、密码，需要对该设备的Telnet参数进行相应配置，否则会导致该物理安全设备下创建虚拟安全设备失败。

#### 操作系统类

* + - * 1. 如果运行一段时间后发现系统CPU占有率持续保持在90%以上，且占用CPU的进程名称为“ora\_j0xx\_xxxx”，则使用“kill -9 ora\_j0xx\_xxxx”关闭此进程即可，对SecCenter A2000运行不会产生影响。

#### 监控代理类

* + - * 1. 如果在运行过程中，部署监控代理对进程状态的监控异常，出现“监控”界面中“启动”和“停止”按钮均不可用时，可通过以下方法解决：

退出部署监控代理，停止“H3C iMC Server”服务，然后重新启动。

如果通过部署监控代理无法启动或停止iMC各进程：

* + - 通过“安装目录/server/bin/start\_server.sh”、“安装目录/client/bin/startup.sh”脚本来手工启动进程；
    - 通过“安装目录/server/bin/stop\_server.sh”、“安装目录/client/bin/shutdown.sh”脚本来手工停止进程。
      * 1. 如果启动SecCenter A2000后，发现无法登录，请尝试重新启动jserver进程。

# 版本特性说明

## 首页

首页特性列表

| 特性 | 描述 |
| --- | --- |
| 风险业务雷达图展示 | 统计安全业务和不安全业务的个数和级别（如存在业务数过多的极端情况，为保证展示效果，只取其中需要重点关注且安全度较低的Top40业务）。 |
| 风险资产雷达图展示 | 分别统计安全资产和不安全资产的个数和级别（如存在资产数过多的情况，为保证展示效果，只取其中需要重点关注且安全度较低的Top40资产）。 |
| 攻击地图和攻击事件展示 | 攻击地图和实际攻击事件列表显示。 |
| 安全信息统计 | 对全网安全评分、高风险资产统计、安全告警（未确认的自定义事件数）统计、设备网络告警。 |
| 攻击分析展示 | 对全网资产攻击情况进行全面分析，包括受攻击资产攻击级别统计、资产攻击源、受攻击资产Top10。 |
| 漏洞分析展示 | 支持对全网最近一个月内的漏洞分析。 |
| 业务展示 | 业务卡片，针对每个业务给出业务的安全度、告警级别数量、业务组成部分（业务由三部分组成，分别为主机、网络、应用）。 |

## 拓扑

拓扑特性列表

| 特性 | 描述 |
| --- | --- |
| 拓扑 | 展示网络设备（路由器、交换机）、安全设备（FW/IPS）、LB设备、服务器、PC等资源节点的拓扑连接关系、链路状态、设备状态等网络结构和状态信息。 |

## 综合监控

综合监控特性列表

| 特性 | 描述 |
| --- | --- |
| 设备监控 | 支持对设备的自动发现和手工增加、删除、修改等操作。支持添加设备时自动同步设备信息到资产管理的功能。 |
| 支持对网络设备、安全设备和服务器的监控。 |
| 支持备份和部署安全设备配置文件和安全设备软件。 |
| 应用监控 | 支持对应用的增加、删除、修改操作。 |
| 提供应用监视列表，用于展示应用详情，包括应用名称、应用类型、健康状况、根因分析、告警等信息。 |
| 业务监控 | 支持业务建模管理，将网络设备、应用，根据企业实际情况组合成业务。提供对业务的增加、删除、修改操作。 |
| 提供业务监视列表，展示业务健康度、繁忙度、风险级别、拓扑的信息。 |
| 告警管理 | 提供告警列表，显示告警级别、告警来源、类型、所属资产、业务、告警信息、恢复状态、确认状态、告警时间、持续时间等信息。 |
| 支持对告警的确认、恢复、删除、列表表格定制、导出操作。 |
| 报表 | 预定义报表：攻击事件报表。 |
| 提供可视化的报表设计功能，基于SOC开放的数据源，用户可自定义新的报表模板。 |
| 支持自动周期报表，可以按照天、周、月、年的周期生成报表。 |
| 支持手工立即生成报表，按照选择的时间段生成报表。 |
| 下级监视 | 支持分布式下，从机安全评分、安全告警、服务数量和应用数量的展示。支持增加、删除、修改和查询功能。 |

## 安全策略管理

安全策略管理特性列表

|  |  |
| --- | --- |
| 特性 | 描述 |
| FW策略 | 提供配置防火墙策略并下发的功能。支持对防火墙规则的增加、删除、修改和查询功能。 |
| 以列表的形式显示规则详情，包括域、IP、服务、时间段、动作、日志功能。支持对规则的匹配统计，给出规则匹配次数。 |
| IPS策略 | 提供配置下发IPS策略功能，支持删除、修改、查询操作。 |
| 支持对IPS规则的动作调整、使能、禁用功能。 |
| 策略调优 | 以列表的形式显示FW规则的触发情况，包括源域、目的域、源IP、目的IP地址、最后匹配时间、匹配次数等信息，使管理员可以对长期未触发的策略进行优化调整。 |
| 全局资源 | 安全域管理用于提供对FW、IPS策略的支持。支持增加、删除、修改、查询功能。 |
| IP管理用于提供对防火墙规则的支持，创建规则需要该参数。支持包含对主机IP、范围IP、子网IP、IP组的增加、删除、修改和查询操作。 |
| 服务管理用于提供对防火墙规则的支持，创建规则需要该参数。支持包含对预定义服务（预定义为系统默认服务，不支持修改操作），自定义服务、服务组的增加、删除、修改和查询操作。 |
| 时间段管理用来配置域间规则生效的时间段。 |
| 域间规则管理用于配置防火墙和IPS的域间规则，包含源域、目的域、源IP组、目的IP组、时间段、过滤动作等。 |
| IPS规则列表用来展示IPS特征库的内容，包含规则的名称、默认动作等。 |
| 动作管理用于提供对IPS策略的支持，包含对四种动作（阻断动作、重定向动作、捕获动作和日志动作）的增加、删除和修改操作。 |

## 事件分析

事件分析特性列表

| 特性 | 描述 |
| --- | --- |
| 实时事件 | 以列表的形式展示最近一小时内事件详情。包含的事件详情有：事件级别、攻击时间、源IP、源国家/地区、目的IP、目的国家/地区、协议、事件、事件数、资产名称、业务、动作等信息。支持高级查询，支持区域反查功能。 |
| 支持主机日志实时展示功能，以列表的形式给出最近一小时内主机事件详情。 |
| 以拓扑的形式对事件攻击路径的展示。 |
| 支持对攻击事件的攻击详情说明。 |
| 支持针对事件知识库说明。 |
| 事件明细 | 以列表的形式展示历史事件详情，包含的事件详情有：事件级别、攻击时间、源IP、源国家/地区、目的IP、目的国家/地区、协议、事件、事件数、业务、动作等信息。支持高级查询和区域反查。 |
| 支持事件导出功能。 |
| 支持对主机日志的分析展示。 |
| 支持在指定时间段内对攻击源IP Top5、目的IP Top5、产生最多事件的设备Top5、产生最多事件Top5的图形展示。 |
| 以拓扑的形式提供对事件攻击路径的展示。 |
| 支持对攻击事件详情说明。 |
| 支持下发限制规则功能（只能与Comware V7安全设备配合）。 |
| 支持针对事件知识库说明。 |
| 支持IPS事件着色审计分析。 |
| 支持对iMC-EIA及安恒认证事件展示。 |
| 事件概览 | 对最近一小时的事件进行汇总分析和展现。支持按设备名称、Top个数、业务等作为分析条件的统计分析。 |
| 提供攻击源TopN、攻击目的TopN、产生事件最多的设备TopN、产生最多的事件TopN、事件趋势、攻击协议TopN等分析图表。 |
| 支持对TopN的明细展示，点击饼图上的IP、事件等，界面支持跳转到事件明细列表，显示对应的事件详情。 |
| 多维度分析 | 支持根据时间段、周期、事件类别、业务类型、设备名、IP地址对事件的查询分析。 |
| 安全设备事件分析支持对攻击类型事件数、攻击源IP事件数、攻击目的IP事件数、攻击端口的事件数、攻击级别事件数、攻击协议事件数、源和目的IP事件数的统计分析。 |
| 设备运行状况分析支持对告警TopN、CPU使用率TopN、内存使用率TopN的统计分析。 |
| 威胁活动分类分析 |
| 关联分析 | 支持多种类型或者同种类型事件之间的关联分析，生成新的自定义事件。 |
| 支持关联事件导入功能。 |
| 支持对关联事件的禁用和启用功能。 |
| 提供关联明细展示功能，以列表的形式展示新事件的属性，包括源IP、目的IP、触发时间、级别、所属业务、触发规则。根据聚合规则数，可以得知原始事件详情。 |

## 行为审计

行为审计特性列表

| 特性 | 描述 |
| --- | --- |
| 多维度分析 | 提供流量分析及行为日志分析功能，以趋势图及饼图的形式展示网络使用状况。 |
| 行为明细 | 以列表形式展示用户网络使用行为。 |
| NAT审计 | 以列表形式展示NAT日志。 |
| NAT444审计 | 支持九种NAT444日志类型的审计展示功能。 |

## 安全评估

安全评估特性列表

| 特性 | 描述 |
| --- | --- |
| WEB漏扫任务管理 | 支持添加Web网站漏扫任务，通过定时、周期、立即三种执行方式对网站漏洞进行监测和分析，支持评估结果展示。 |
| 支持删除Web网站漏扫任务。 |
| 数据库漏扫任务管理 | 支持添加数据库漏扫任务，通过定时、周期、立即三种执行方式对数据库漏洞等进行监测和分析，支持评估结果展示。 |
| 支持删除漏扫任务。 |
| 主机漏扫任务管理 | 支持添加主机漏扫任务，通过定时、周期、立即三种执行方式对主机漏洞数据进行监测和分析，支持评估结果展示。 |
| 支持删除主机漏扫任务。 |
| 评估历史 | 记录每次漏洞扫描任务的执行详情，以列表的形式给出任务执行状态、任务名称、启动时间、完成时间、扫描类型等信息。 |
| 以列表的形式展示扫描结果和解决办法。 |

## 安全响应

安全响应特性列表

| 特性 | 描述 |
| --- | --- |
| 响应策略 | 支持基于事件的防护策略定制。通过选择自定义事件名称、保护时间段、触发事件后的执行动作完成对策略的配置下发。支持对策略的增加、删除、修改和查询功能，点击策略对应图标，可以跳转到自定义事件响应明细列表，查看命中历史。 |
| 支持手动重新下发。 |
| 支持交换机接口阻断、安全响应脚本等响应动作。 |
| 支持响铃、邮件、短信等报警方式。 |
| 响应明细 | 以列表的形式展示每次触发策略明细，包括触发时间、策略名称、响应动作，响应结果等。 |

## 风险分析

风险分析特性列表

| 特性 | 描述 |
| --- | --- |
| 业务风险分析 | 提供业务风险卡片，集中在一张卡片上展示一个业务的业务构成、风险情况，支持将业务风险卡片以更精简化的形式一屏展现。 |
| 资产风险评估 | 资产风险分析，体现资产名、责任人、当前风险值、IP、告警数量等明细信息以及从风险概览、威胁信息、脆弱性信息三个维度进行资产风险统计并以图表形式展现结果。 |
| 业务建模管理 | 显示业务详情列表，主要包括安全度等信息，并支持对阈值配置、权重分配进行调整。 |
| 支持业务的增加、删除、修改和查询。 |
| 支持业务拓扑展示。 |

## 安全运维

安全运维特性列表

| 特性 | 描述 |
| --- | --- |
| 事件流程 | 支持对关联事件告警创建工单，查看当前用户名下的待办任务，管理工单流程。 |
| 知识库 | 预定义一万多种事件的详细说明和解决方案，支持按事件类型查询功能。 |
| 支持用户自定义知识，允许增加、删除、修改自定义知识。 |

## 资产管理

资产管理特性列表

| 特性 | 描述 |
| --- | --- |
| 服务器管理 | 支持对服务器资产的增加、删除、修改以及导入导出操作。 |
| 网络管理 | 支持对网络设备资产的增加、删除、修改以及导入导出操作。 |
| 安全管理 | 支持对安全设备资产的增加、删除、修改以及导入导出操作。 |
| 应用管理 | 支持对应用的增加、删除、修改以及导入导出操作。 |
| 资产类型 | 支持对资产类型的增加、删除操作。 |

## 转储配置

转储配置特性列表

| 特性 | 描述 |
| --- | --- |
| NAT444日志转储 | 支持对NAT444日志周期转储和定时清理原始日志。 |
| 安全事件转储 | 支持对主机磁盘空间监控，显示最近30天磁盘使用情况。 |
| 支持对安全事件执行本地转储、远程转储、本地恢复、远程恢复、以及删除本地转储和在线数据的功能。 |
| 支持周期执行转储功能。 |
| 支持在线数据保留时长限制和定时清理在线数据功能。 |
| 支持日志备份到nfs服务器功能。 |

## 大屏展示

大屏展示特性列表

| 特性 | 描述 |
| --- | --- |
| 大屏展示 | 提供针对下级和区域两种方式的日志分析和图形展示功能。支持最近一小时、最近一天、最近一星期、最近一月的数据统计。  默认统计显示今日累计事件数、事件类别、24小时事件数、24小时攻击事件数、实时攻击检测、攻击类型标签云、攻击来源、下级攻击事件以及区域事件专题图。 |
| 区域事件专题图 | 在区域事件专题图设置页面，自定义区域节点位置。数据来源选择“区域”，分别显示区域上报攻击事件数量和区域攻击地图；数据来源选择“下级监视”，显示下级监视上报攻击事件数量。 |
| 市IP管理 | 市IP管理提供了对各个市IP地址的便捷管理，可以增加市IP地址、删除市IP地址和修改市IP地址。通过对市IP的管理，可以在攻击地图中准确看到省范围内的攻击分布。 |
| 数据板 | 分为配置自定义大屏和设置大屏展示两个模块。数据板主要用于设置大屏展示页面。操作员可以配置自定义大屏，也可以选择默认大屏。 |

## 系统管理

系统管理特性列表

| 特性 | 描述 |
| --- | --- |
| 分布式 | 支持分布式管理。 |
| 系统安全 | 防暴力破解，输错用户名或密码超过三次锁定一分钟才允许下一次登录。 |
| 提供闲置超时机制，闲置时长可以配置。 |
| 支持操作日志功能。 |
| 全局管理 | 支持对操作员的增加、删除、修改操作以及操作员分组、分权操作。 |
| 提供配置国家/地区IP地址的功能，配置IP后，攻击事件即可显示源、目的国家/地区信息。 |
| 提供日志参数配置功能，用于配置日志接收端口。 |
| 提供应用配置管理功能，用于配置应用基线、阈值等参数。 |
| 支持对邮件服务器、短信业务的配置以及日志级别设置、数据收集操作。 |
| 提供应用联系人和模板配置功能。 |
| 提供针对IPS日志的黑白名单配置。 |
| 提供安全日志过滤器配置，用于过滤IPS日志以及报表数据过滤使用。 |

# 版本变更说明

## 特性变更说明

### SCA 1.0 (E0503)

#### 特性变更

* 新增特性
  + EIA认证事件明细展示
  + 威胁活动分类分析
  + 行为审计-多维度分析
  + 行为审计-行为明细
  + 行为审计-NAT审计
* 删除特性

无。

* 修改特性

无。

### SCA 1.0 (E0501)

#### 特性变更

* 新增特性
  + 大屏展示
  + IPS日志黑白名单配置
  + IPS事件着色审计
  + 安全事件明细报表过滤功能
* 删除特性

无。

* 修改特性

无。

### SCA 1.0 (E0202)

#### 特性变更

* 新增特性

无。

* 删除特性

无。

* 修改特性

无。

## 操作方式变更说明

无。

# 存在问题与规避措施

#### 201610310398

* 问题现象：数据库漏扫结果信息中会有一些地方有乱码。
* 问题产生条件：执行Oracle类型的数据库漏洞扫描。
* 规避措施：无。

#### 201709210544

* 问题现象：操作日志显示乱码。
* 问题产生条件：执行设备同步时间配置，并批量选择设备。
* 规避措施：无。

#### 201709050597

* 问题现象：列表显示为空。
* 问题产生条件：应用监视中有数据，在修改业务页面中选择应用。
* 规避措施：先手动查询再重置，可查询出数据。

# 解决问题列表

## SCA 1.0 (E0503)版本解决问题列表

#### [201706200502](javascript:openTab('../DefectDetail/Default/8d2d8e90-e495-4687-b150-1957fdfcea14',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201706200502');)

* **[严重]**问题现象：立即执行操作只执行了新增的Web漏扫任务。
* 问题产生条件：增加一个Web漏扫任务，选择其它已存在的Web漏扫任务，单击<立即执行>按钮。

#### [201706190724](javascript:openTab('../DefectDetail/Default/c298b08f-145c-45ae-95c7-fa6ec9ef112e',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201706190724');)

* **[严重]**问题现象：报表管理中预定义报表不显示。
* 问题产生条件：点击修改预定义报表，修改模板名称后，单击<确定>按钮。

#### [201706190509](javascript:openTab('../DefectDetail/Default/c3304170-3896-4860-b39b-5233cc8733ca',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201706190509');)

* **[严重]**问题现象：策略部署的功能页面显示异常。
* 问题产生条件：在IP地址管理创建多个IP地址组，并且IP地址组之间出现相互引用。

#### [201706240124](javascript:openTab('../DefectDetail/Default/090c3d88-080b-45ea-918d-6fe2914576fa',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201706240124');)

* **[严重]**问题现象：虚拟设备无法创建。
* 问题产生条件：增加虚拟设备时，物理设备选择仅含有40GE口的安全设备。

#### [2](javascript:openTab('../DefectDetail/Default/090c3d88-080b-45ea-918d-6fe2914576fa',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201706240124');)01706260435

* **[严重]**问题现象：日志信息无法显示。
* 问题产生条件：SOC接收设备发送的电信和联通NAT444审计日志。

#### 201706200746

* **[一般]**问题现象：页面提示“未获得服务器扫描ID，扫描失败”。
* 问题产生条件：Web漏扫任务执行成功后，操作员重新登录SOC，选择执行成功的Web漏扫任务，单击<立即执行>按钮。

#### 201706230227

* **[一般]**问题现象：查询结果仍是上次正确查询的结果。
* 问题产生条件：进入多维度分析>攻击>按攻击级别页面，输入不合法IP地址，单击<查询>按钮。

#### 201706230633

* **[一般]**问题现象：图表显示异常。
* 问题产生条件：进入策略优化管理页面，点击匹配次数非0次的历史记录。

#### 201706300497

* **[一般]**问题现象：名称显示错误。
* 问题产生条件：进入多维度分析>应用>按应用分类页面，查看应用的详细分析。

## SCA 1.0 (E0501)版本解决问题列表

#### 201611190133

* **[严重]**问题现象：分布式部署环境下，配置完NAT日志自定义转储后，从机会立即转储，主机不转储。
* 问题产生条件：分布式部署成功后，进入NAT日志转储配置页面，转储任务选择为“开启”，设置每天12点执行任务，转储1天之前的数据，单击<确认>按钮后，在未到12点的情况下，从机会立即转储，主机不转储。

#### 201611240377

* **[严重]**问题现象：首页攻击地图攻击类型Top5部分数据丢失。
* 问题产生条件：进入首页，在攻击地图右下角点击向上的箭头，进入到大屏攻击地图页面。

#### 201703160404

* **[严重]**问题现象：事件明细页面日志级别显示错误，界面和实际级别展示相反。
* 问题产生条件：进入事件明细页面，查询日志级别展示。

#### 201611040140

* **[严重]**问题现象：NAT日志转储，自定义转储时间与实际执行时间不一致。
* 问题产生条件：进入NAT日志转储配置页面，修改自定义转储事件为非当前时间，单击<确定>按钮后，NAT日志会立即执行转储。

#### 201611020717

* **[严重]**问题现象：策略调优页面，最后匹配时间与实际不符。
* 问题产生条件：进入策略调优页面，查看最后匹配时间。

## SCA 1.0 (E0202)版本解决问题列表

#### [201611010283](javascript:openTab('../DefectDetail/Default/4d010ad4-10ea-42df-8e89-4c6c8d134519',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201611010283');)

* **[严重]**问题现象：分布式部署环境下，主机预定义知识显示为0个。
* 问题产生条件：分布式部署成功后，进入主机知识库页面，选择“攻击”或“漏洞”单选按钮。

#### [201611010279](javascript:openTab('../DefectDetail/Default/8e462078-0268-4005-8d53-50da0c214ae9',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201611010279');)

* **[一般]**问题现象：NAT444审计按协议查询日志，页面报错。
* 问题产生条件：进入NAT444审计页面，选择任意一种日志类型，点击高级查询并按协议查询。

#### 201611040095

* **[提示]**问题现象：从创建新知识页面返回知识库列表，批量删除按钮不显示。
* 问题产生条件：进入知识库页面，单击<创建新知识>按钮，进入创建新知识页面，在创建新知识页面单击<确定>或<取消>按钮。

#### 201610290311

* **[一般]**问题现象：首页攻击类型Top5的攻击类型名称重复。
* 问题产生条件：进入首页，点击攻击地图上拉图标，进入最大化地图界面。

#### 201611010521

* **[一般]**问题现象：远程恢复数据执行成功后，所占磁盘空间大小显示为0。
* 问题产生条件：进入转储配置页面，选择日期执行远程恢复。

# 相关资料

## 相关资料清单

* H3C SecCenter A2000安全管理中心 快速安装指南-5PW101

## 资料获取方法

用户可以通过H3C官网了解SecCenter A2000的相关资料：

<http://www.h3c.com/cn/Technical_Documents>

# 技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：<http://www.h3c.com>

# 版本升级操作指导

该版本只能从旧版本升级，可参考下面的步骤。

## 前提

该版本支持升级操作，可以基于如下版本升级：

* SCA 1.0 (E0501)

升级包应拷贝到服务器本地使用，避免通过远程共享等方式使用升级包。

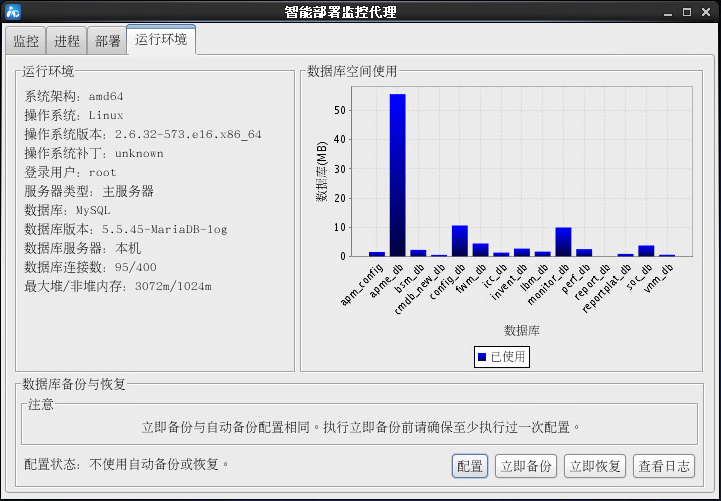
## 备份SecCenter A2000

在执行SecCenter A2000的升级操作前，依据以下步骤，对原有的SecCenter A2000进行备份，以便于在升级失败时，能够快速恢复到之前的状态。

* + - * 1. 备份数据库

打开部署监控代理，并使用监控代理“运行环境”选项卡中的“立即备份”功能，备份当前服务器上的SecCenter A2000数据库。

备份SecCenter A2000的数据库



* + - * 1. 备份SecCenter A2000安装目录

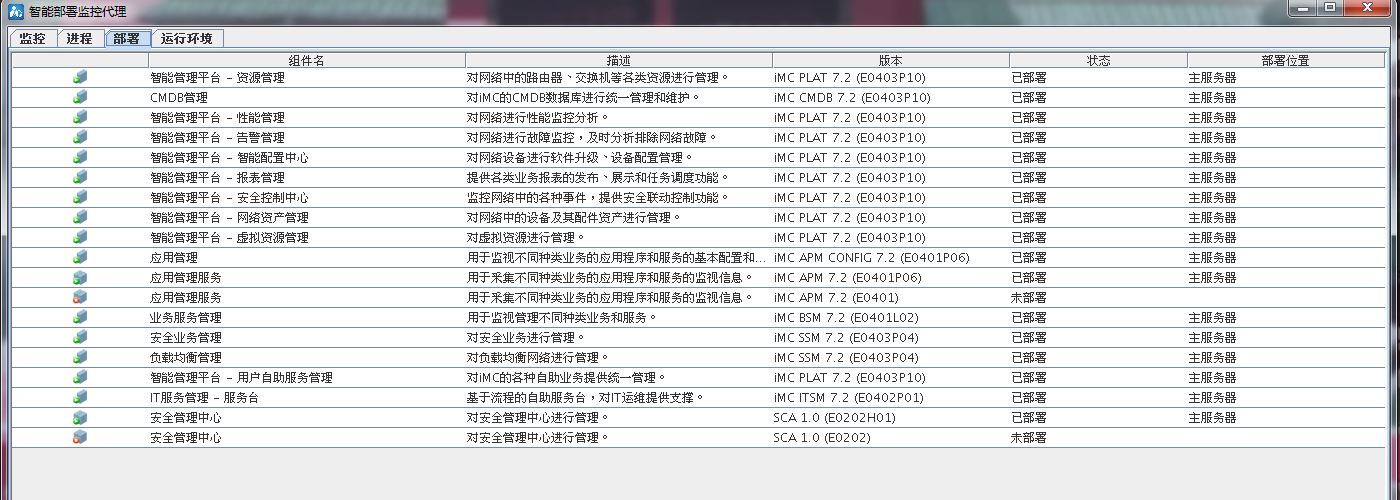
将整个SecCenter A2000安装目录拷贝到另一个文件夹中。如果升级过程中出现问题，可以将备份的SecCenter A2000覆盖到原有的目录下快速恢复到升级前的状态。

## 升级SecCenter A2000

升级步骤如下：

* + - * 1. 在智能部署监控代理窗口的“部署”选项卡中查看SecCenter A2000各组件的版本信息。

SecCenter A2000各组件的版本信息



* + - * 1. 如果某个组件的版本信息与表18中所列版本一致，则该组件不需要升级；如果某个组件的版本信息与表18中所列版本不一致，则需要将该组件版本升级为与表18所列版本一致。

SecCenter A2000组件版本列表

| 组件名称 | 版本号 | 备注 |
| --- | --- | --- |
| PLAT | iMC PLAT 7.2 (E0403P10) | 首先升级该组件。 |
| APM | iMC APM CONFIG7.2 (E0401P06) | 无。 |
| BSM | iMC BSM 7.2 (E0401L02) | 无。 |
| ITSM | iMC ITSM 7.2 (E0402P01) | 无。 |
| SSM | iMC SSM 7.2 (E0403P04) | 无。 |
| SOC | SCA 1.0 (E0202H01) | 在升级完其他所有组件之后才能升级该组件。 |

* + - * 1. 在智能部署监控代理中，单击“监控”界面中的<停止iMC>按钮，停止所有SecCenter A2000进程。
        2. 单击“监控”界面中<安装新组件>按钮，系统将会弹出选择文件夹窗口。

安装新组件



选择文件夹窗口



* + - * 1. 使用<浏览>按钮，在SecCenter A2000升级包所在路径下找到PLAT所在的文件夹（如果升级的是其他组件，则选择该路径下其他组件所在的文件夹，此处以PLAT为例），并单击<确定>按钮，进入安装向导窗口。

安装向导窗口



* + - * 1. 单击<下一步>按钮进入许可协议窗口。

许可协议窗口



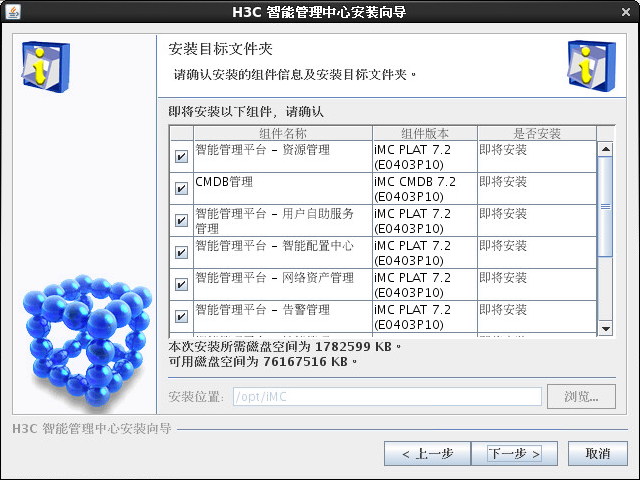
* + - * 1. 认真阅读许可协议后，选择“我同意”，单击<下一步>按钮，系统会弹出升级公共组件确认窗口并自动升级公共组件，公共组件包括部署监控代理和后端通用服务等。

升级公共组件窗口



* + - * 1. 待升级公共组件完成后，系统将会显示安装目标文件夹窗口。

选择安装目标文件夹窗口



* + - * 1. 选择安装目标文件夹窗口中显示了即将升级的组件信息。升级文件的安装位置为SecCenter A2000的安装位置。确认信息后，单击<下一步>按钮，弹出操作确认窗口。
        2. 单击<是>按钮，进入部署和升级配置窗口。

部署和升级配置窗口



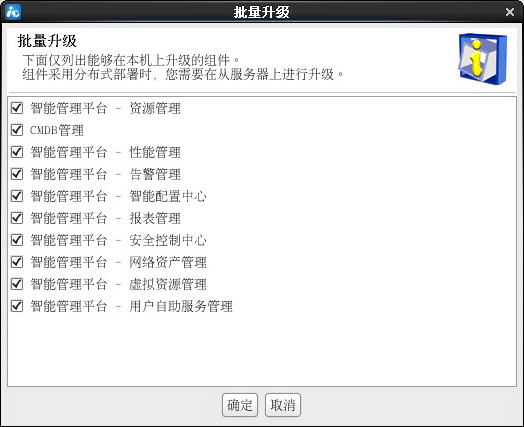
* + - * 1. 选择“立即部署或升级”，单击<下一步>按钮，进入安装摘要信息窗口。

安装摘要信息窗口



* + - * 1. 确认相关安装信息后，单击<开始安装>按钮执行安装操作。安装完成后自动进入批量升级窗口。

批量升级窗口



* + - * 1. 选择需要升级的组件后，单击<确定>按钮开始批量升级操作，待升级完成后，系统将会弹出批量升级结果窗口。

批量升级结果窗口



* + - * 1. 单击<确定>按钮关闭该界面，完成升级操作。
        2. 完成PLAT所有版本的升级后，按照步骤(4)-步骤(14)操作升级其他组件。
        3. 升级完所有组件后，单击智能部署监控代理“监控”界面中的<启动>按钮，启动所有SecCenter A2000服务进程的运行。

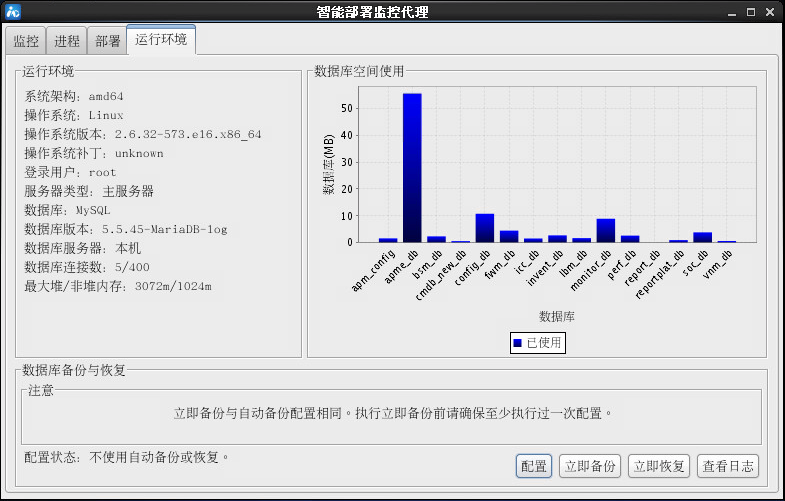
如果 SecCenter A2000使用分布式部署方式运行，在主服务器端公共组件升级完成后，需要重新启动从服务器端部署监控代理和“H3C iMC Server”服务。重启完成后，监控代理将提示是否需要升级从服务器端公共组件，选择“是”即可执行从服务器端公共组件的升级操作，操作过程和主服务器完全相同。

## 恢复SecCenter A2000

如果SecCenter A2000在升级过程中出现错误，需要恢复到升级前的环境，可参照如下步骤执行。

* + - * 1. 打开部署监控代理，并使用监控代理“运行环境”选项卡中的“立即恢复”功能。
        2. 根据数据备份文件的存储位置选择恢复类型，单击<本地恢复>或<远程恢复>按钮，在弹出的对话框中选择升级前备份的所有数据库备份文件，并执行恢复操作。

数据库备份与恢复操作界面



* + - * 1. 将SecCenter A2000所有进程停止（包括监控代理和H3C iMC Server服务）。
        2. 手工删除SecCenter A2000安装路径。
        3. 手工将升级前备份的SecCenter A2000目录拷贝到原来的SecCenter A2000安装路径下。
        4. 重新启动SecCenter A2000相关进程（包括H3C iMC Server服务和部署监控代理）。

# 软件注册说明

## 获取SecCenter A2000设备信息文件

未注册的SecCenter A2000试用版可以试用45天，从第一次启动SecCenter A2000开始计算，用户可以通过获取License并注册为正式版解除试用时间限制。试用版在功能上与正式版完全相同。

设备信息文件获取方法如下：

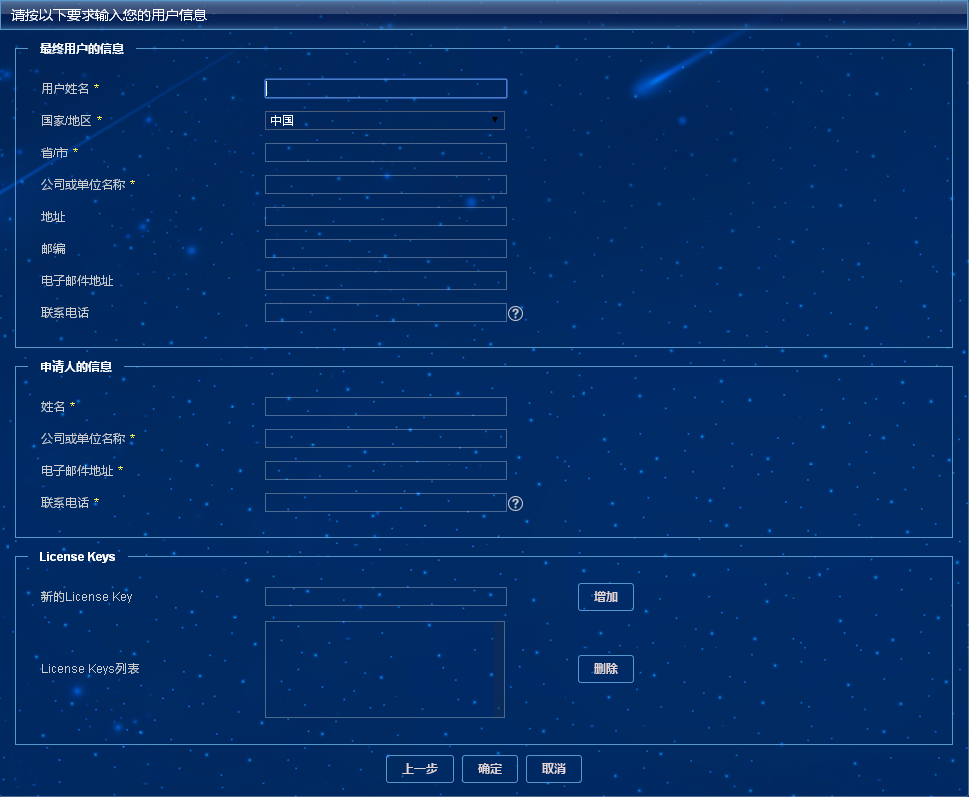
* + - * 1. 首先，在SecCenter A2000登录界面中点击“产品注册”链接，进入注册操作选择窗口。

注册操作选择窗口



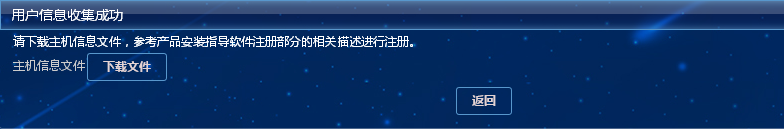
* + - * 1. 输入admin用户的登录密码，并将“选择您要执行的操作”设置为“申请新的License或升级现有的License”，单击<下一步>按钮，进入用户信息输入窗口。

用户信息输入窗口



* + - * 1. 按照要求输入最终用户信息、申请人信息和License Keys数据后，单击<确定>按钮，进入用户信息收集成功提示窗口。

成功提示



* + - * 1. 点击上图中的下载文件链接，将主机信息文件下载到本地。系统将主机信息文件备份保存在SecCenter A2000的安装目录下：opt/iMC/license/，主机信息文件的名称为hostid.txt。但是当SecCenter A2000服务器重新启动后，该文件将会被自动删除。

## 获取License

待主机文件下载完成后，登录到<http://www.h3c.com.cn/Service/Authorize_License/Achieve_License>上，填写相关信息并上传主机信息文件，即可获取SecCenter A2000 License，然后请参见11.3 SecCenter A2000注册中描述的步骤进行注册即可。

## SecCenter A2000注册

当获取SecCenter A2000许可文件后，可以通过SecCenter A2000登录界面中的“产品注册”功能进行注册。

* + - * 1. 在SecCenter A2000登录界面中点击“产品注册”链接，进入注册操作选择窗口。输入admin用户的登录密码，并将“选择您要执行的操作”设置为“使用License文件对产品进行注册”，单击<下一步>按钮，进入注册您的产品窗口。
        2. 单击<选择文件>按钮，选择License文件（后缀名为.txt）。

选择License文件



* + - * 1. 在“注册为”下拉框中，选择“主机”或者“从机”，然后单击<确定>按钮，进入注册成功窗口。
        2. 单击<确定>按钮，完成注册操作。
        3. 注册完成后，重启SecCenter A2000，使修改后的注册信息生效，即可访问SecCenter A2000系统。