高级网络安全报告 （版本 7.x）发行说明

发布日期： 2016 年 8 月 31 日
修订日期： 2020 年 5 月 28 日

目录

新增功能

版本 7.0 新增功能

特性	说明
AWRS 代理服务在搜索结果中显示无 WBRS 分数的事件	无 WBRS 分数 （显示 WBRS：无分数）的新过滤器已添加到**网络跟踪** > **代理服务**控制面板中。使用此过滤器，您可以查看无 WBRS 分数的代理服务的搜索结果。
部门成员报告显示 AD 组报告的详细结果	您现在可以在**用户分析** > **概述**下查看 AD 组报告的以下结果： – 按受阻事务数排名靠前的组 – 受阻事务摘要 – 按使用的带宽排名靠前的用户 – 使用的带宽摘要 – 按用户排名靠前的组 – 使用的带宽摘要 – AD 组摘要 – 每位用户的 AD 组详细信息

版本 6.6 新增功能

特性	说明
在自定义控制面板中搜索	支持在自定义控制面板中搜索数据。 • 您可以使用具有 " 提交 " 按钮的主搜索字段搜索数据。 • 您可以使用 " 结果 " 窗格中的辅助搜索字段过滤搜索结果。
从任何页面导出	您可以从任何控制面板将数据 （非图形数据）导出为逗号分隔值 (csv) 文件、 XML 文件或 JavaScript 对象表示法 (json) 文件。您必须将鼠标悬停在 " 控制面板数据显示 " 窗格上以查看此选项 ⇩ 进行下载。

版本 6.5 新增功能

此版本包含漏洞修复；请参阅已修复问题，第 7 页。

版本 6.4 新增功能

特性	说明
网络跟踪控制面板更新	• 新过滤器 - **用户**、**客户端 IP**、 **WBRS** 最低和最高分数范围以及 **SNI** 都已添加到**网络跟踪** > **代理服务**控制面板中。 • 您可以从 " 代理服务 " 控制面板查看和导出 10000 条事务。

版本 6.3 新增功能

特性	说明
Splunk 引擎升级	Splunk 引擎升级到版本 6.6.6。

版本 6.2 新增功能

特性	说明
思科 Umbrella 报告支持	您可以将高级网络安全报告应用指向包含 Umbrella 提供的日志的 AWS 存储桶。您可以在 " 合并网络安全报告 " 控制面板中查看报告。
Splunk 引擎升级	Splunk 引擎将升级到最新版本。

注意 基于角色的报告仅适用于未加速的数据模型。由于禁用加速会增加报告加载时间，因此，如果不使用基于角色的报告，请启用数据模型加速。请参阅用户手册中的 " 配置最佳实践 " 和 " 按角色限制部门报告访问权限 " 一章。

版本 6.1 新增功能

特性	说明
CEF 提取器	公共事件格式 (CEF) 提取器服务可让您将从一个或多个网络安全设备收到的访问日志转换为 CEF 格式的输出数据。
网络安全设备 AsyncOS 10.1 支持	对存档扫描访问日志更改的支持包含在网络安全设备 AsyncOS 10.1 版本中。

版本 6.0 新增功能

特性	说明
自定义过滤器	在称为 " 过滤 " 的过程中，定义可用访问、 SOCKS 和 AMP 日志数据的自定义搜索。
更新的界面	更新了应用的 " 外观 "。

系统要求

AsyncOS 版本兼容性

高级网络安全报告应用	用于网络安全设备的 AsyncOS
7.0	10.0、 10.1、 10.5、 11.0、 11.5、 11.7、 11.8
6.6	10.0、 10.1、 10.5、 11.0、 11.5、 11.7
6.5	10.0、 10.1、 10.5、 11.0、 11.5、 11.7
6.4	10.0、 10.1、 10.5、 11.0、 11.5、 11.7
6.3	8.5.3、 8.7.0、 8.8.0、 9.0.0、 9.1.0、 10.0、 10.1、 10.5、 11.0、 11.5
6.2	8.5.3、 8.7.0、 8.8.0、 9.0.0、 9.1.0、 10.0、 10.1、 10.5、 11.0。
6.1	8.5.3、 8.7.0、 8.8.0、 9.0.0、 9.1.0、 10.0、 10.1。
6.0	8.5.3、 8.7.0、 8.8.0、 9.0.0、 9.1.0、 10.0。

要求 高级网络安全报告

虚拟设备上的操作系统要求

- Linux （64 位）
- Windows （64 位） - Windows Server 2008 R2、 Windows Server 2012、 Windows Server 2012 R2、 Server 2016、 Windows 8、 Windows 8.1、 Windows 10

平台要求。参考硬件可以是商品级的，并且必须具有以下最低规格才能获得思科支持:

- Intel x86 64 位芯片架构，具有两个 CPU，每个 CPU 12 个内核，每个内核 2.0 GHz 或更高（最低配置）
- 16 GB RAM
- RAID1+0 （800 IOPS 或更高）中的四个 300-GB SAS 硬盘，每个硬盘转速 10,000 rpm
- 标准 1 Gb 以太网 NIC，用于管理网络的可选第二个 NIC

假定条件:

- 安装具有根权限或管理权限的操作系统。
- 当前版本不支持配置为 IPV6 的 IPV4。
- 通过应用所有必需的补丁，可以解决与操作系统 / 内核相关的漏洞。

注意 高级网络安全报告 121/5000 通常首先要受磁盘 I/O 的约束，因此在选择存储硬件时始终要首先考虑磁盘基础结构。

应根据行业最佳实践创建单独的操作系统卷。企业安装应尽可能驻留在其自己的逻辑卷上。

支持的文件系统:

平台	文件系统
Linux	ext2、 ext3、 ext4、 btrfs、 XFS、 NFS 3/4
Windows 的 ISE 安全评估代理	NTFS、 FAT32

基于 Unix 的系统范围的资源限制

下表显示了软件使用的系统范围的资源。它为非转发器 （例如索引器、搜索头、集群管理器、许可管理器、部署服务器和监控控制台 (MC)）的实例提供了这些资源的最低建议设置。

系统范围的资源	ulimit 调用	建议的最小值
打开文件	ulimit -n	64000
用户进程	ulimit -u	16000
数据段大小	ulimit -d	1073741824

此注意事项不适用于基于 Windows 的系统。

规模和扩展建议

- 基本配置是一个单层架构，其中一台服务器提供典型高级网络安全报告部署的全部三个部分的核心功能：
  - 搜索实例
  - 索引器
  - 数据源监控器
- 通过添加另一个高级网络安全报告实例并调整配置，新的基础设施将提高总体索引和搜索性能 （一旦数据负载平衡），并提高存储和保留容量。
- 还将向基础设施添加一个专用的转发器服务器，并对其进行配置，以监控 Web 安全设备日志文件，并使用负载平衡跨多个索引器转发日志数据。
- 为便于实施和配置每日索引量巨大的环境，请参阅表 1 基于每日索引量的基础设施建议，第 6 页。建议使用 Splunk 专业服务来设置分布式部署的基础设施。

注意　扩展需要分布式部署设置的基础设施，必须通过 Splunk 专业服务将其合并。此基础设施未经 AWSR 测试 / 验证，因为其仅通过 Splunk 专业服务在客户现场进行设置 / 配置和验证。

基于针对拥有 1 万用户的 Web 安全设备的日志量估计，收集的未压缩数据量是 10 GB/ 天。一旦建立索引，数据将压缩到所使用的估计为 2.5 GB/ 天的索引存储库。该高级网络安全报告实例会根据 500 GB 的卷大小，将索引数据保留 200 天左右。

Web 安全设备用户	预计日志量 （每用户每天 2500 起事务）	预计索引量	预计保留量 (500 GB)
10 K	10 GB/ 天	2.5 GB	200 天
50 K	50 GB/ 天	13 GB	40 天
100 K	100 GB/ 天	25 GB	20 天

注意　基于阵列中的估计日志量和中等容量驱动器的指导原则。

每日使用量	77 GB/ 天	140 GB/ 天	180 GB/ 天
总事务数	1.72 亿	3.25 亿	4.17 亿
预定义报告加载时间	< 5 秒	< 10 秒	< 15 秒

总量	2.3 TB
工作日保留量 @70 GB/ 天	33
预定义报告加载时间	< 20 秒

表 1　　基于每日索引量的基础设施建议

用户总数	每日索引量						
	< 2 GB/ 天	2-250 GB/ 天	250-500 GB/ 天	500-750 GB/ 天	750GB-1TB/ 天	1-2 TB/ 天	2-3 TB/ 天
< 4	1 个组合实例	1 个搜索实例 1 个索引器	1 个搜索实例 2 个索引器	1 个搜索实例 3 个索引器	1 个搜索实例 4 个索引器	1 个搜索实例 8 个索引器	1 个搜索实例 12 个索引器
最多 8	1 个组合实例	1 个搜索实例 1 个索引器	1 个搜索实例 2 个索引器	1 个搜索实例 4 个索引器	1 个搜索实例 5 个索引器	1 个搜索实例 10 个索引器	1 个搜索实例 15 个索引器
最多 16	1 个搜索实例 1 个索引器	1 个搜索实例 1 个索引器	1 个搜索实例 3 个索引器	1 个搜索实例 4 个索引器	2 个搜索实例 6 个索引器	2 个搜索实例 12 个索引器	2 个搜索实例 18 个索引器
最多 24	1 个搜索实例 1 个索引器	1 个搜索实例 2 个索引器	1 个搜索实例 3 个索引器	1 个搜索实例 4 个索引器	2 个搜索实例 6 个索引器	2 个搜索实例 12 个索引器	2 个搜索实例 18 个索引器
最多 48 个		1 个搜索实例 2 个索引器	1 个搜索实例 3 个索引器	1 个搜索实例 4 个索引器	3 个搜索实例 8 个索引器	3 个搜索实例 16 个索引器	3 个搜索实例 24 个索引器

安装和升级说明

有关基本说明 （包括要运行的脚本），请参阅可从相关文档，第 7 页中的所示位置下载的*高级网络安全报告 《安装、设置和用户手册》*。

将 “ 主 ” 设置为目标索引

与早期版本不同，在设置正在进行的数据传输时，必须选择**主**作为目标索引。与此相关的说明可参见 *《高级网络安全报告安装、设置和用户手册》*。

许可

此版本提供 " 混合报告 "； 也就是说，同时支持网络安全设备和 CWS 日志报告。要使用混合报告，您必须升级许可证；但是对于现有许可证，您可以继续使用仅网络安全设备报告。有关详细详细，请参阅 *《思科高级网络安全报告安装、设置和用户手册》* 中的许可和迁移部分。

注意 为了从仅网络安全设备迁移到混合报告，您必须开启思科技术支持中心 (TAC) 支持案例来删除您现有的许可证并安装新的混合报告许可证，其中包括报告源类型的完整列表，即包括 `ciscocws` 源类型。如果您是高级网络安全报告 4.0 或更高版本的新用户，则不需要这样做。

待解决问题

- CWS 支持添加的 " 高级恶意软件保护 " 报告，但不支持 " 文件分析 " 报告。
- SPLUNK 尚未解决的问题位于 https://www.splunk.com/page/securityportal。

已修复问题

- CSCvn65880 - AWSR 未解析所有访问日志
- CSCvn97489 - 在代理服务屏幕中，由于解析 WSA 日志出错，无法查看字段策略的值。
- CSCvn97502 - Policy_type 未以某种 WSA 日志格式显示任何值，因为正则表达式中存在问题。
- CSCvo04664 - 由于 ACL 标签存在问题， AWSR 无法生成报告。
- CSCvn97441 - AWSR 无法为 full_decision 字段解析某些 WSA 日志格式。
- CSCvo24110 - AMP 判定不会更新 AWSR 6.5 中的任何结果。

相关文档

以下文档可从下列网址下载：
http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html。

- *《高级网络安全报告安装、设置和用户手册》*
- 《Web 安全设备支持的 AsyncOS 版本的用户手册》

支持

思科支持社区

思科支持社区是一个面向思科客户、合作伙伴和员工的在线论坛。它提供了一个场所，供相关人员讨论常规内容安全问题以及有关具体思科产品的技术信息。您可以向论坛发布主题咨询问题，并与其他思科用户分享信息。

通过以下 URL 访问思科支持社区来了解网络安全和相关管理：

https://community.cisco.com/t5/web-security/bd-p/5786-discussions-web-security

客户支持

国际：访问 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

支持网址：访问 http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

---

本文档需结合 " 相关文档 " 一节中列出的文档共同使用。