在安全Web设备中配置请求调试日志

目录

简介

先决条件

- 要求
- 使用的组件

请求调试日志

配置请求调试日志

相关内容

简介

本文档介绍在安全网络设备(SWA)中请求调试日志的步骤。

先决条件

要求

建议掌握下列主题的相关知识：

- 对SWA的命令行界面(CLI)的管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

请求调试日志

SWA中的请求调试日志是一种专门日志类型，旨在捕获单个特定HTTP或HTTPS事务或客户端计算

机极为详细的端到端调试和跟踪级别信息。与记录许多请求中的汇总事件的标准代理日志不同，请求调试日志将来自处理特定请求（如身份验证、URL过滤、解密、恶意软件扫描和信誉服务）所涉及的所有Web代理模块的调试输出聚合到一个相关的日志流中。此日志类型仅用于深度诊断，只能通过CLI创建，而不能通过GUI创建。

在排除标准日志缺乏足够详细信息的复杂或间歇性代理问题时，请求调试日志至关重要。它们使管理员和Cisco TAC能够准确跟踪每个处理阶段如何处理单个请求，从而能够查明根本原因，例如意外策略匹配、扫描延迟、身份验证失败或引擎之间的不一致判定。由于日志集中于一个事务，因此它提供了最大的可视性，且不会在系统范围内跨所有代理模块启用调试日志记录对运行开销和性能造成影响。这使请求调试日志成为高级调查期间准确、高效且低风险的诊断工具。

配置请求调试日志

步骤1.登录到CLI，运行logconfig并选择new。

步骤2.选择与Request Debug Logs关联的编号，然后按Enter。

步骤3.输入日志的名称。

步骤4.选择Trace作为日志记录级别。

步骤5.选择请求收集增强日志记录的模块。可以用逗号分隔或范围列表（如1、3、4或3-7）的形式进行多个选择。

提示：如果TAC未请求特定模块，最好选择所有模块(例如：1-30）。

步骤6.指定要启用增强日志记录的请求数。捕获完此数量的请求后，日志记录将自动停止。

注意：在故障排除期间，根据流量条件选择合理值非常重要。例如，如果正在使用专用测试计算机，并且后台流量最小，则只需较低数量的请求就足够了。但是，在后台活动较高的环境中（例如操作系统更新、浏览器后台请求或Webex等应用），选择较高的值可确保捕获相关事务。

第7步：通过选择客户端IP地址、目标IP地址或目标域，定义增强日志记录的请求匹配条件。

注意：在大多数情况下，建议选择客户端IP地址，即使排除对单个网站的访问故障。此方法可确保捕获在页面加载过程中生成的所有Web请求，包括可能不可立即查看的其他URL的后台请

求。但是，当使用具有最少后台互联网流量的专用测试计算机时，此方法最有效。在客户端产生大量额外流量的环境中（例如操作系统更新、浏览器后台服务或Webex等应用），最好按Destination domain或Destination IP address进行过滤。

提示：如果确切的故障点未知，则可以收集浏览器HAR日志，以确定出现问题的特定URL或域（例如，页面加载失败或高延迟），然后可以在请求调试日志条件中配置该域。

步骤8.选择检索日志的方法。如果选择FTP Poll，则日志存储在SWA上。

步骤9.定义用于日志文件的文件名，或按Enter键接受当前生成的文件名。

步骤10.选择No进行基于时间的日志文件回滚，因为日志记录将在达到定义的请求数后停止。

步骤11.定义以字节为单位的最大文件大小，或按Enter接受当前值。

提示：定义较大的日志文件大小可能会使日志更难下载和查看。建议增加日志文件的数量，而不是增加单个日志文件的大小（下一步）。 此方法提高了可管理性，同时确保捕获所有所需的调试信息而不会创建过大的文件。

步骤12.根据在步骤5中选择用于记录的代理模块的数量和步骤7中定义的请求匹配条件，配置日志文件的最大数量。选择合理的文件限制对于确保捕获所有相关调试信息而不提前停止日志记录非常重要，因为日志记录可能导致日志不完整或丢失。

步骤13.如果提示Should a alert is sent when files removed due to the maximum number of files allowed?则选择No，这样可以防止在正常日志轮换期间出现不必要的警报，特别是当出于故障排除目的有意生成Request Debug Logs时。

步骤14.当出现Do you want to compress logs(yes/no)? 提示时，选择No（否）。这样可以保持日志文件的未压缩状态，使其在故障排除期间更易于查看和分析。

步骤15.按Enter键退出向导。

步骤16.键入commit并按Enter保存更改。

```
SWA_CLI> logconfig

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
```

```
...
[Output removed to simplify readability]
...
55. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[]> new

Choose the log file type for this subscription:
1. ADC Engine Framework Logs
2. ADC Engine Logs
...
[Output removed to simplify readability]
...
53. Request Debug Logs
...
[Output removed to simplify readability]
...
[1]> 53

Please enter the name for the log:
[]> Request_Debug_Logs

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 5

Choose modules where enhanced request logging is to be performed.
Multiple selections can be made in the form of a comma separated or range list (e.g. 1,3,4 or 3-7)
Choosing the Default Proxy will enable enhanced logging across modules:
1. Default Proxy
2. Access Control Engine
3. Proxy Configuration
4. Disk Manager
5. Memory Manager
6. McAfee Integration Framework
7. Sophos Integration Framework
8. Webroot Integration Framework
9. Webcat Integration Framework
10. Connection Management
11. Authentication Framework
12. HTTPS
13. FTP proxy
14. WCCP Module
15. License Module
16. SNMP Module
17. WBRS Integration Framework
18. Logging Framework
19. Data Security Module
20. Miscellaneous Proxy Modules
21. DCA Engine Framework
22. AVC Engine Framework
23. Cloud Connector
```

```
24. SOCKS Proxy
25. Advanced Malware Protection
26. ArchiveScan module in proxy
27. Web Traffic Tap module in proxy
28. Bandwidth Control
29. Http2 proxy
30. ADC Engine Framework
[1]> 1-30

Please enter the number of requests for which to perform enhanced logging:
[1]> 100

Choose the request criteria for logging:
1. Client IP Address
2. Destination Domain
3. Destination IP Address
[1]> 1

Specify source IP address
[]> 10.20.3.15

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 1

Filename to use for log files:
[Request_Debug_Logs.text]>

Do you want to configure time-based log files rollover? [N]>

Please enter the maximum file size:
[10485760]>

Please enter the maximum number of files:
[10]> 50

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]>

Do you want to compress logs (yes/no)
[n]>

Currently configured logs:
1. "Request_Debug_Logs" Type: "Request Debug Logs" Retrieval: FTP Poll
2. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
3. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
56. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll


SWA_LIC> commit

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
```

相关内容

- 思科安全Web设备AsyncOS 15.2用户指南
- 使用安全Web设备最佳实践
- 访问安全Web设备日志
- 使用Microsoft Server配置SWA中的SCP推送日志

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。