配置访问日志中的性能参数

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

创建额外的访问日志

- 从GUI创建新访问日志
- 从CLI配置新的访问日志

将性能参数的自定义字段添加到访问日志

- 检验更改

自定义字段中的字段说明

相关内容

简介

本文档介绍将性能参数自定义字段添加到安全网络设备(SWA)访问日志的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全外壳协议(SSH)访问SWA管理接口。
- 图形用户界面(GUI)访问SWA管理界面。



提示：最好在SWA数据分区上具有超过20%的可用磁盘空间。您可以在status detail命令的输出中通过命令行界面(CLI)检查磁盘使用情况。

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。

背景信息

当出现延迟问题且流量通过SWA代理时，访问日志有助于排除延迟的根本原因。您可以更改当前的访问日志设置，或使用添加到自定义字段的性能参数创建新的访问日志。

创建额外的访问日志

在某些情况下，由于内部策略或其他配置，无法更改当前访问日志。要克服此限制，您可以创建另一个访问日志并在新的访问日志中添加自定义性能参数。

从GUI创建新访问日志

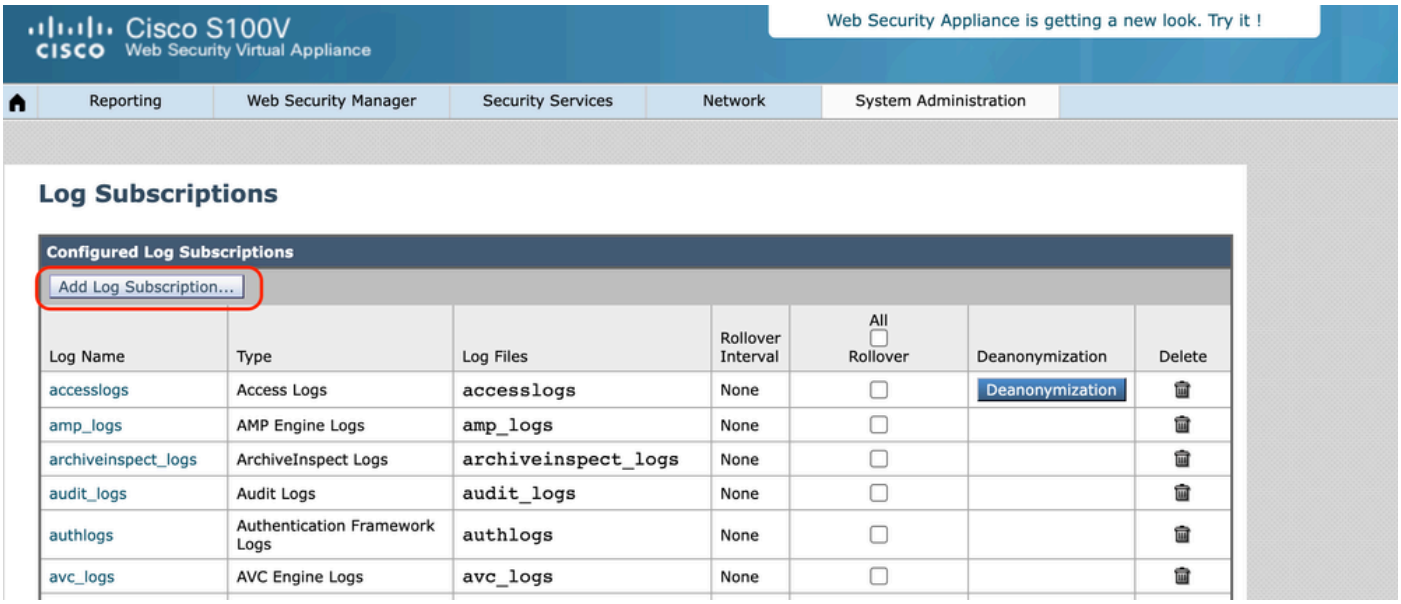
步骤1.登录GUI。

步骤2.从System Administration菜单中选择Log Subscriptions。


System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary
Configuration File
Feature Key Settings
Feature Keys
Smart Software Licensing
Upgrade and Updates
Upgrade and Update Settings
System Upgrade
System Setup
System Setup Wizard
FIPS Mode
Cisco Success Network
Next Steps

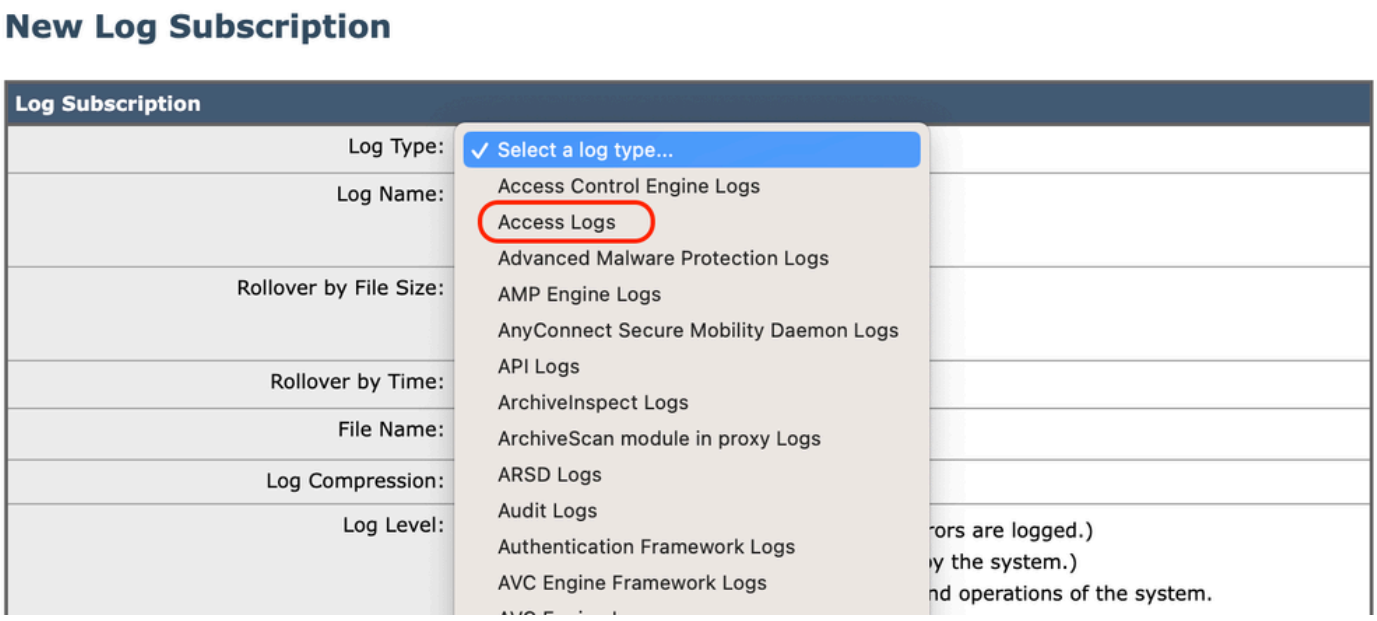
选择日志订阅

步骤3.选择添加日志订阅……



选择Add Log Subscription

步骤4.从日志类型部分选择Access Logs，然后等待刷新页面。



从日志类型选择访问日志

步骤5.在“日志名称”部分输入新日志的名称。在本示例中，TAC_access_logs。

步骤6.在SWA将日志滚动到新文件之前，输入介于102400(100 KB)到10737418240(10 GB)之间的

文件大小（以字节为单位）值。Number必须为整数，您可以添加M以表示文件大小（以兆字节为单位），添加K以表示文件大小（以千字节为单位），添加G以表示千兆字节。

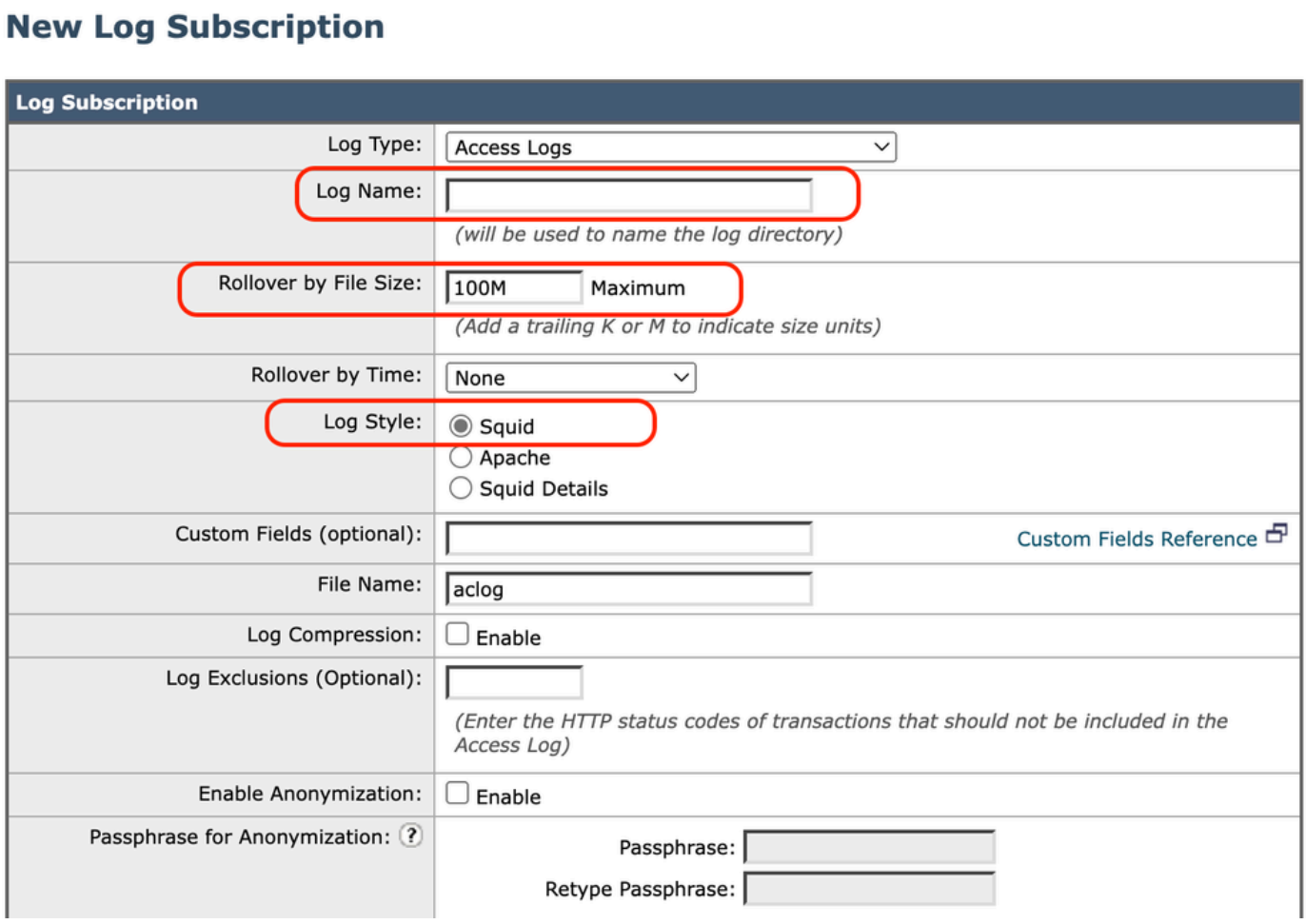
注意：当当前日志文件达到用户指定的最大文件大小限制或自上次滚动后的最长时间时，SWA存档（回滚）日志订阅。

步骤7.选择Squid作为日志样式。

步骤8.“文件名”用于定义此新日志的文件夹名称和日志文件名。建议与日志名称相同，在本例中为TAC_access_logs。

步骤9.可以启用日志压缩以压缩日志文件，或将日志保留为文本文件。

步骤10.日志排除用于过滤超文本传输协议(HTTP)响应代码。请勿过滤HTTP状态代码。



填写必填字段

步骤11.选择FTP轮询以在SWA中保留日志。键入1并按Enter。

步骤12.提交并提交更改。

从CLI配置新的访问日志

步骤1.登录到CLI。

步骤2.运行logconfig。

步骤3.要创建新日志，请键入New并按Enter键。

步骤4.在列表中查找访问日志，键入与其相关的数字并按Enter键。

步骤5.输入新日志的名称。

步骤6.键入1为此订用的日志样式选择Squid，然后按Enter。

步骤7.不过滤HTTP错误状态代码。按Enter导航到下一步。

步骤8.选择FTP轮询以在SWA中保留日志。键入1并按Enter。



注意：要将日志推送到文件传输协议(FTP)服务器、安全复制协议(SCP)服务器或系统日志服务器。您可以选择与它们相关的选项。

步骤9.此步骤是为新日志定义文件夹名称和文件名。最好与日志名称相同，然后按Enter。

步骤10.在102400(100 KB)到10737418240(10 GB)之间输入一个值，表示文件大小（以字节为单位），然后SWA将日志滚动到新文件。



注意：当当前日志文件达到用户指定的最大文件大小限制或自上次滚动后的最长时间时，SWA存档（回滚）日志订阅。

步骤11.最大文件数表示设备中存储的日志文件数。如果日志文件总数达到此值，则会从SWA中删

除较旧的日志。默认值为10个文件，由于可用磁盘空间和其他日志配置，您可以键入日志数，然后按Enter。

步骤12.在此步骤中，您可以选择压缩日志或将其保留为文本文件。在Yes中键入Y，在No中键入N，然后单击Enter。

注意：文件大小达到最大文件大小后，再进行压缩。压缩比率取决于网络流量行为，并且可能因日志文件而异。

步骤13.按Enter退出日志配置向导。

步骤14.键入commit以保存更改。

```
SWA_CLI> logconfig
...
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.
[]> NEW

Choose the log file type for this subscription:
1. AVC Engine Framework Logs
2. AVC Engine Logs
3. Access Control Engine Logs
4. Access Logs
....
58. Webroot Logs
59. Welcome Page Acknowledgement Logs
[1]> <=== type the number associated with Access Logs and press Enter

Please enter the name for the log:
[]> <=== Choose desired name, in this example, TAC_access_logs

Choose the log style for this subscription:
1. Squid
2. Apache
3. Squid Details
[1]> <=== Press Enter to keep the default value

Enter the HTTP Error Status codes (comma separated list of 4xx and 5xx codes) you want to filter out fr
[]> <=== Press Enter to keep the default value

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> <=== Choose FTP poll to keep the logs in the SWA
```

```
Filename to use for log files:
[aclog]> <=== It is better to have the same file name as the log, in this example, TAC_access_logs

Do you want to configure time-based log files rollover? [N]> <=== Enter the desired answer

Please enter the maximum file size:
[104857600]> <=== Enter the desired answer, or you can leave as default

Please enter the maximum number of files:
[100]> <=== Enter the desired answer, it depends on free disk space and log file size

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

Do you want to compress logs (yes/no)
[n]> <=== Enter the desired answer

Currently configured logs:
1. "Splunk Logs" Type: "Access Logs" Retrieval: FTP Push - Host 10.0.0.1
2. "TAC_access_logs" Type: "Access Logs" Retrieval: FTP Poll
3. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
....
40. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
41. "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.
[]> <=== Press Enter to exit the log configuration wizard

SWA_CLI> commit
Please enter some comments describing your changes:
[]> <=== Type the change description and press Enter
```

将性能参数的自定义字段添加到访问日志

步骤1.登录GUI。

第2步：从“系统管理”(System Administration)菜单中，选择“日志订阅”(Log Subscriptions)。

步骤3.从“日志名称”列中，选择访问日志或新创建的名称。在本示例中，TAC_access_logs。

步骤4.在自定义字段(Custom Fields)部分，粘贴以下字符串：

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)


     , Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<, R
```

```
a; DNS response = %:

 d, WBRS response = %:

  r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respons

   s; AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ] [Client Port = %F, Server IP = %k
```

步骤5.提交并提交更改。

检验更改

步骤1.登录到CLI。

步骤2.键入tail并按Enter键。

步骤3.查找与添加性能参数的访问日志关联的编号。键入编号并按Enter。

您可以看到访问日志中添加了额外的信息，与本示例中相同。

```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa/

      - " [ Request Details: ID = 104, User Agent = "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/
```

提示：在按住Control键并按C时，可以退出tail命令。如果未退出tail命令，请键入q。

自定义字段中的字段说明

自定义性能参数字段中使用的值映射到以下信息：

提示：延迟= AMP总计+反间谍软件总计+ Webroot总计+ Sophos总计+ McAfee总计+ AVC总计+ WBRS总计+身份验证总计

自定义字段名称	自定义字段	描述
请求报头	%:<h	第一个字节之后将请求报头写入服务器的等待时间。
请求服务器	%:<b	在报头之后将请求正文写入服务器的等待时间。
第1个字节到客户端	%:1>	写入客户端的第一个字节的等待时间。
客户端正文	%:b>	写入客户端的完整正文的等待时间。
Rx等待时间（毫秒）：第1个请求字节	%:1<	从Web代理开始连接到服务器到它首次能够写入服务器所用的时间。如果Web代理必须连接到多台服务器才能完成事务，则是这些时间之和。
请求报头	%:h<	第一个字节后完成客户端报头的等待时间。
客户端正文	%:b<	完成客户端正文的等待时间。
第1个响应字节	%:>1	服务器第一个响应字节的等待时间。
响应报头	%:>h	第一个响应字节之后的服务器报头的等待时间。
服务器响应	%:>b	这表示SWA从服务器收到HTTP报头，但SWA会等待响应字节，然后响应字节将是来自服务器的实际内容。

磁盘缓存	%:>c	Web代理从磁盘缓存读取响应所需的时间。
身份验证响应	%:<a	Web代理发送请求后，从Web代理身份验证进程接收响应的等待时间。
身份验证总计	%:>a	从Web代理身份验证进程接收响应的等待时间，包括Web代理发送请求所需的时间。
DNS响应	%:<d	Web代理向Web代理DNS进程发送域名请求(DNS)请求所用的时间。
DNS总计	%:>d	Web代理DNS进程将DNS结果发送回Web代理所用的时间。
WBRS响应	%:<r	Web代理发送请求后，从Web信誉过滤器接收响应的等待时间。
WBRS总计	%:>r	从Web信誉过滤器接收裁决的等待时间，包括Web代理发送请求所需的时间。
AVC响应	%:A>	Web代理发送请求后，从应用可视性与可控性(AVC)进程接收响应的等待时间。
AVC总计	%:A<	从AVC进程接收响应的等待时间，包括Web代理发送请求所需的时间。
DCA响应	%:C>	Web代理发送请求后，从动态内容分析引擎接收响应的等待时间。
DCA总计	%:C<	从动态内容分析引擎接收裁决的等待时间，包括Web代理发送请求所需的时间。
McAfee响应	%:m>	Web代理发送请求后，从McAfee扫描引擎接收响应的等待时间。
McAfee总计	%:m<	从McAfee扫描引擎接收裁决的等待时间，包括Web代理发送请求所需的时间。
Sophos响应	%:p>	Web代理发送请求后，从Sophos扫描引擎接收响应的等待时

		间。
Sophos总计	%:p<	从Sophos扫描引擎接收裁决的等待时间，包括Web代理发送请求所需的时间。
AMP响应	%:e>	Web代理发送请求后，从AMP引擎接收响应的等待时间。
AMP总计	%:e<	从AMP引擎接收判定的等待时间，包括Web代理发送请求所需的时间。
延迟	%x;%L	延迟和请求本地时间（采用人工可读格式）：DD/MMM/YYYY :hh:mm:ss +nnnn。此字段在访问日志中使用双引号书写。 此字段允许您将日志与问题关联起来，而无需为每个日志条目计算从纪元时间开始的本地时间。
客户端端口	%F	从客户端使用的端口号。
服务器 IP 地址	%k	Web 服务器 IP 地址.
服务器端口号	%p	Web 服务器端口号.

相关内容

- 思科安全网络设备AsyncOS 14.5用户指南 — GD（通用部署）— 思科
- 思科网络安全设备最佳实践指南 — 思科

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）。