تكوين معلمة الأداء في سجلات الوصول

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

إنشاء سجل وصول إضافي

إنشاء سجل وصول جديد من واجهة المستخدم الرسومية

تكوين سجل الوصول الجديد من CLI

إضافة حقول مخصصة لمعلمة الأداء إلى سجلات الوصول

التحقق من التغييرات

وصف الحقول في الحقول المخصصة

المحتويات ذات الصلة

المقدمة

يصف هذا المستند الخطوات اللازمة لإضافة حقل مخصص لمعلمة الأداء إلى سجل الوصول الخاص بـ Secure Web Appliance (SWA).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وصول بروتوكول طبقة الأمان (SSH) إلى واجهة إدارة SWA.
- وصول واجهة المستخدم الرسومية (GUI) إلى واجهة إدارة SWA.

تلميح: من الأفضل أن تكون لديك مساحة قرص حرة تزيد عن 20٪ على قسم بيانات SWA. يمكنك التحقق من استخدام القرص من واجهة سطر الأوامر (CLI) في أمر إخراج تفاصيل الحالة.

المكونات المستخدمة

.ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة

.تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

عندما تكون هناك مشكلة خاصة بزمن الوصول ويتم وكيل حركة المرور من خلال شبكة SWA، يمكن أن تكون سجلات الوصول مفيدة لاستكشاف أخطاء السبب الجذري لزمن الوصول وإصلاحها. يمكنك تغيير إعدادات سجلات الوصول الحالية أو إنشاء سجلات وصول جديدة بمعلمات أداء مضافة إلى حقل مخصص.

إنشاء سجل وصول إضافي

في بعض الحالات، ال يمكن إجراء تغيير في سجل الوصول الحالي بسبب السياسات الداخلية أو بعض عمليات التكوين الأخرى. وللتغلب على هذا التحدي، يمكنك إنشاء سجلات وصول أخرى وإضافة معلمة الأداء المخصصة في سجلات الوصول الجديدة.

إنشاء سجل وصول جديد من واجهة المستخدم الرسومية

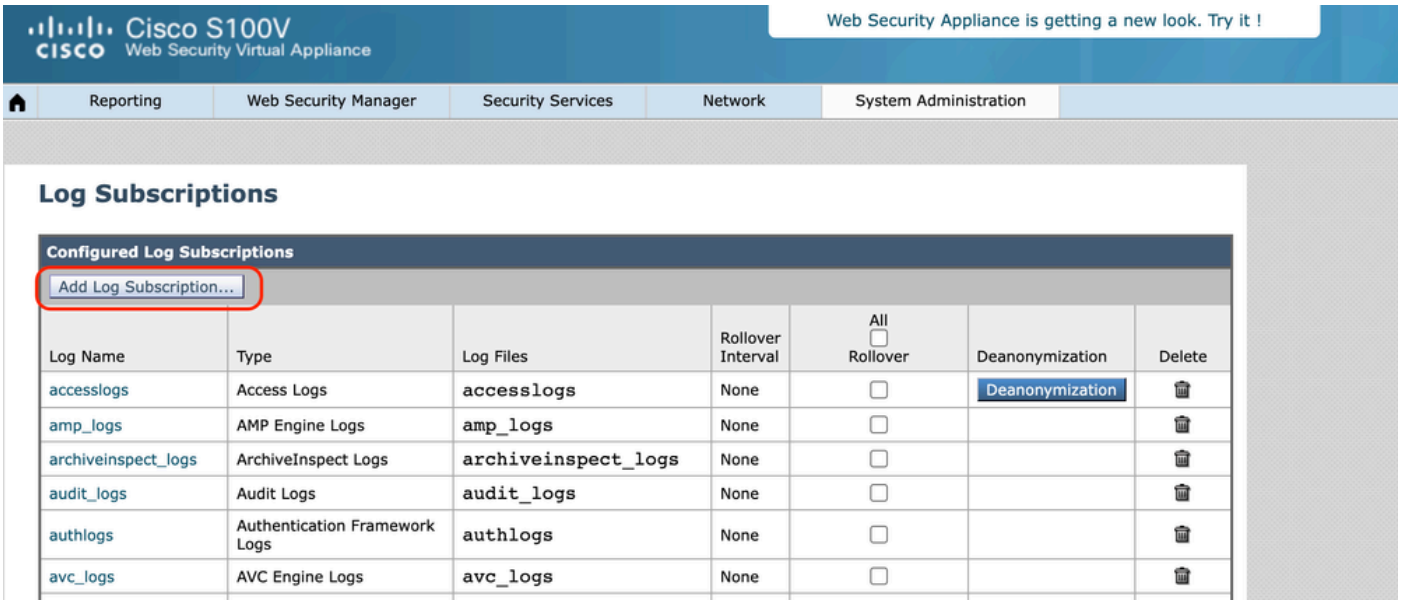
الخطوة 1. سجل الدخول إلى واجهة المستخدم الرسومية.

الخطوة 2. من قائمة إدارة النظام أختر اشتراكات السجل.

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

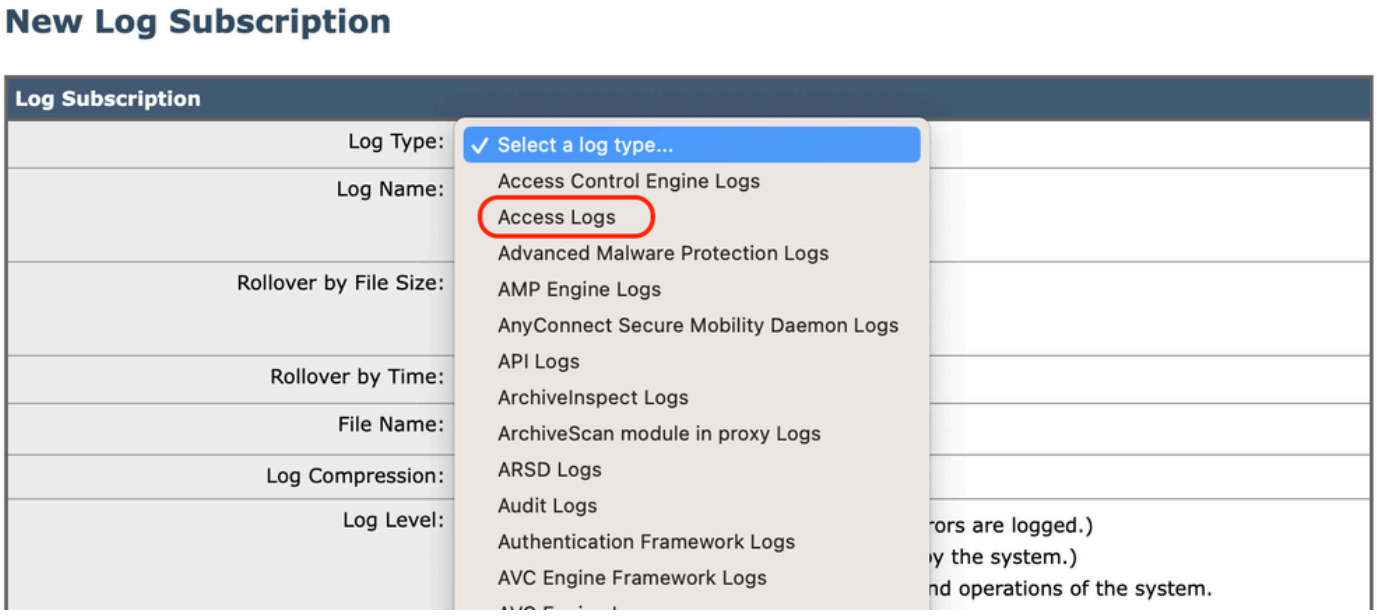
إختيار اشتراك السجل

الخطوة 3. أختر إضافة اشتراك السجل ...



أختر إضافة اشتراك سجل

الخطوة 4. من قسم نوع السجل أختر سجلات الوصول وانتظر الصفحة حتى يتم تحديثها.



أختر سجلات الوصول من نوع السجل

الخطوة 5. أدخل اسم لقسم اسم السجل الجديد. في هذا المثال، TAC_ACCESS_LOG.

الخطوة 6. أدخل قيمة تتراوح بين 102400 (100 كيلوبايت) إلى 10737418240 (10 غيغابايت)

لحجم الملف (في البايت) قبل أن تقوم SWA بتمرير السجل إلى ملف جديد. يجب أن يكون الرقم عددا صحيحا، ويمكنك إضافة M للإشارة إلى الحجم في ميغابايت، K للإشارة إلى حجم الملف بالكيلوبايت وG للغيغابايت.

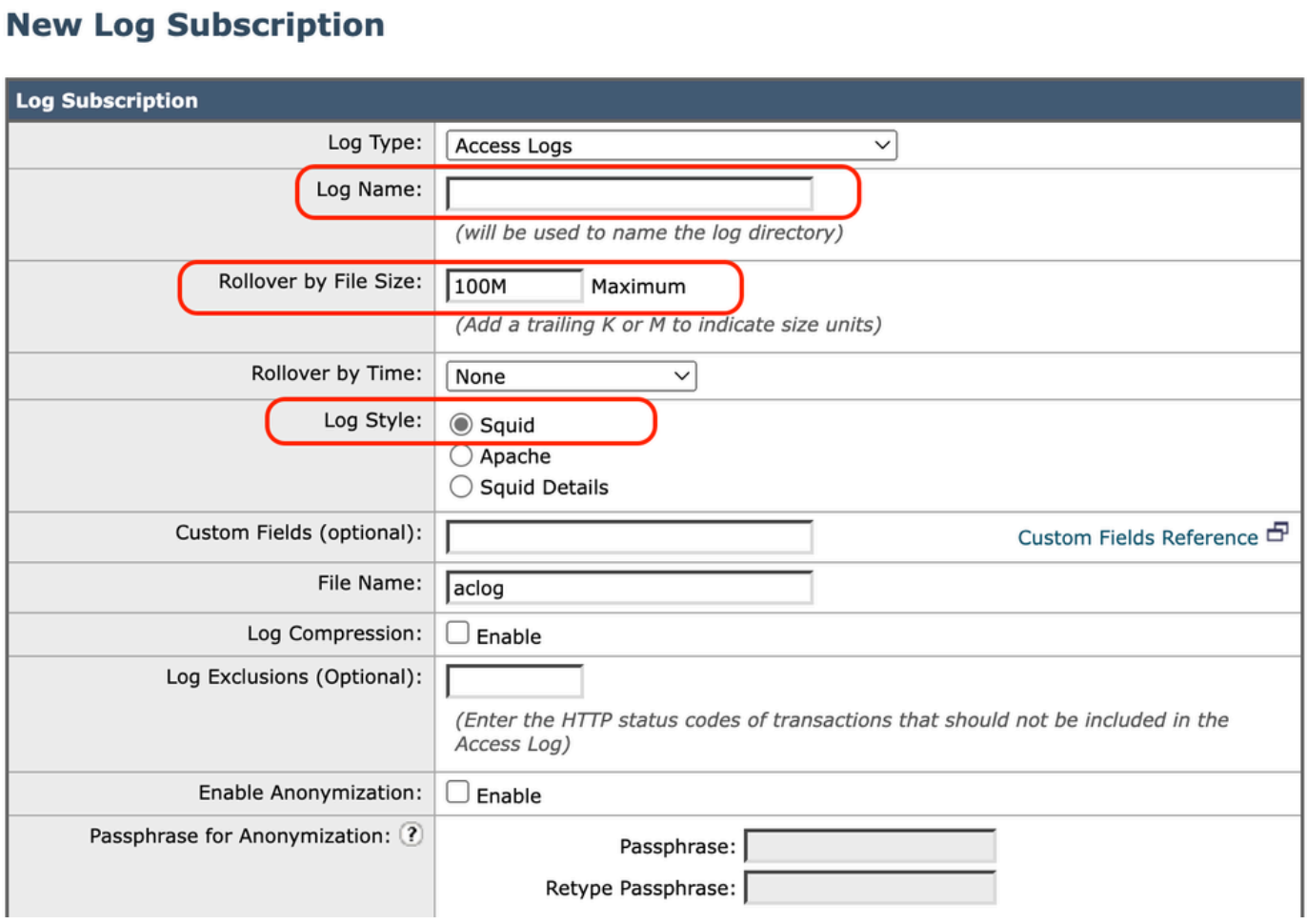
ملاحظة: تقوم أرشيفات SWA (المرور فوقه) بتسجيل الاشتراكات عندما يصل ملف السجل الحالي إلى حد أقصى يحدده المستخدم لحجم الملف، أو الحد الأقصى للوقت منذ آخر إعادة توجيه.

الخطوة 7. أختر سكويد لنمط السجل.

الخطوة 8. اسم الملف هو تعريف اسم المجلد واسم ملف السجل لهذا السجل الجديد. ينصح بأن يكون هو نفسه اسم السجل، والذي كان في هذا المثال، TAC_ACCESS_LOG.

الخطوة 9. يمكنك تمكين ضغط السجل لضغط ملف السجل، أو الحفاظ على السجلات كملف نصي.

الخطوة 10. إستثناء السجل هو تصفية رمز الاستجابة لبروتوكول نقل النص التشعبي (HTTP). عدم تصفية أكواد حالة HTTP.



الخطوة 11. أختر إستطلاع FTP للاحتفاظ بالسجلات في SWA. اكتب 1 ثم اضغط على المفتاح Enter.

الخطوة 12. إرسال التغييرات وتنفيذها.

تكوين سجل الوصول الجديد من CLI

الخطوة 1. سجل الدخول إلى CLI.

الخطوة 2. شغل logconfig.

الخطوة 3. لإنشاء سجل جديد، اكتب جديد واضغط يدخل.

الخطوة 4. ابحث عن سجلات الوصول في القائمة، اكتب الرقم المرتبط بذلك واضغط على Enter.

الخطوة 5. أدخل اسم للسجل الجديد.

الخطوة 6. اكتب 1 لاختيار Squid لنمط السجل لهذا الاشتراك، واضغط على Enter.

الخطوة 7. ال تقم بتصفية رموز حالة خطأ HTTP. اضغط على Enter للتنقل إلى الخطوة التالية.

الخطوة 8. أختر إستطلاع FTP للاحتفاظ بالسجلات في SWA. اكتب 1 ثم اضغط على المفتاح Enter.

ملاحظة: لدفع السجلات إلى خادم بروتوكول نقل الملفات (FTP) أو خادم بروتوكول النسخ الآمن (SCP) أو خادم syslog. يمكنك إختيار الخيارات المتعلقة بهم.

الخطوة 9. هذه الخطوة هي تعريف اسم المجلد واسم الملف للسجل الجديد. من الأفضل أن تكون نفس اسم السجل، واضغط على مفتاح الإدخال.

الخطوة 10. أدخل قيمة تتراوح بين 102400 (100 كيلوبايت) إلى 10737418240 (10 غيغابايت) لحجم الملف (في البايت) قبل أن تقوم SWA بتمرير السجل إلى ملف جديد.

ملاحظة: تقوم أرشيفات SWA (المرور فوقه) بتسجيل الاشتراكات عندما يصل ملف السجل الحالي إلى حد أقصى يحدده المستخدم لحجم الملف، أو الحد الأقصى للوقت منذ آخر إعادة توجيه.

الخطوة 11. يشير الحد الأقصى لعدد الملفات إلى عدد ملفات السجل المخزنة في الجهاز. إذا وصل العدد الإجمالي لملفات السجل إلى هذه القيمة، فسيتم حذف السجلات الأقدم من SWA. القيمة الافتراضية هي 10 ملفات ويمكنك كتابة عدد السجلات، نظرا لمساحة القرص المتوفرة وتكوين السجلات الأخرى، ثم اضغط على مفتاح Enter.

الخطوة 12. في هذه الخطوة، يمكنك إختيار ضغط السجلات، أو الاحتفاظ بها كملف نصي. اكتب Y لنعم وN لNO واضغط Enter.

ملاحظة: بعد أن يصل حجم الملف إلى الحد الأقصى لحجم الملف، ثم يضغط. تعتمد نسبة الضغط على سلوك حركة مرور الشبكة، ويمكن أن تختلف بين ملفات السجل.

الخطوة 13. اضغط على Enter للخروج من معالج تكوين السجل.

الخطوة 14. اكتب الالتزام بحفظ التغييرات.

```
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
```

إضافة حقول مخصصة لمعلمة الأداء إلى سجلات الوصول

الخطوة 1. سجل الدخول إلى واجهة المستخدم الرسومية.

الخطوة 2. من قائمة إدارة النظام، أختر اشتراكات السجل.

الخطوة 3. من عمود اسم السجل، حدد مدخلات، أو اسم المنشأة حديثا. في هذا المثال، TAC_ACCESS_LOG.

الخطوة 4. في قسم "الحقول المخصصة"، الصق هذه السلسلة:

```
[ 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
```

الخطوة 5. إرسال التغييرات وتنفيذها.

التحقق من التغييرات

الخطوة 1. سجل الدخول إلى CLI.

الخطوة 2. اكتب tail واضغط enter.

الخطوة 3. ابحث عن الرقم المرتبط بسجلات الوصول التي أضافت معلمة الأداء. اكتب الرقم ثم اضغط على مفتاح Enter.

يمكنك ملاحظة إضافة معلومات إضافية إلى سجلات الوصول، كما هو الحال في هذه العينة.

```
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/
```

تلميح: يمكنك إنهاء الأمر الذيل عند الضغط على مفتاح التحكم والضغط على C. إذا لم يتم إنهاء الأمر tail، اكتب q.

وصف الحقول في الحقول المخصصة

القيم المستخدمة في تعيين حقل معلمات الأداء المخصصة لهذه المعلومات:

تلميح: زمن الوصول = إجمالي AMP + إجمالي برامج مكافحة التجسس + إجمالي WBRS + إجمالي AVC + إجمالي McAfee + إجمالي Sophos + إجمالي Webroot + المصادقة

اسم الحقل المخصص	حقل مخصص	الوصف
رأس الطلب	%:<h	وقت الانتظار لكتابة رأس الطلب إلى الخادم بعد البايت الأول.
طلب إلى الخادم	%:<b	وقت الانتظار لكتابة نص الطلب إلى الخادم بعد الرأس.
البايت الأول للعميل	%:1>	وقت الانتظار للبايت الأول الذي تمت كتابته إلى العميل.
نص العميل	%:b>	وقت الانتظار حتى تتم كتابة النص بالكامل إلى العميل.

أوقات انتظار Rx (بالمللي ثانية): بايت الطلب الأول	%:1<	الوقت المستغرق من اللحظة التي يبدأ فيها وكيل الويب في الاتصال بالخادم إلى الوقت الذي يكون فيه قادرا على الكتابة إلى الخادم. إذا كان يجب على وكيل ويب الاتصال بالعديد من الخوادم لإكمال المعاملة، فهذا هو مجموع هذه الأوقات.
رأس الطلب	%:h<	وقت الانتظار لرأس العميل الكامل بعد البايت الأول.
نص العميل	%:b<	وقت الانتظار لإكمال نص العميل.
بايت الاستجابة الأولى	%:>1	وقت الانتظار لأول بايت إستجابة من الخادم.
رأس الاستجابة	%:>h	وقت الانتظار لرأس الخادم بعد بايت الاستجابة الأولى.
إستجابة الخادم	%:>ب	هذا يعني أن SWA تلقت رؤوس HTTP من الخادم، ولكن SWA تنتظر وحدات بايت الاستجابة بعد ذلك وأي المحتوى الفعلي من الخادم.
ذاكرة التخزين المؤقت للقرص	%:>ج	الوقت المطلوب لوكيل ويب لقراءة إستجابة من ذاكرة التخزين المؤقت للقرص.
إستجابة المصادقة	%:<a	وقت الانتظار لتلقي الاستجابة من عملية مصادقة وكيل الويب، بعد أن قام وكيل الويب بإرسال الطلب.
إجمالي المصادقة	%:>a	وقت الانتظار لتلقي الاستجابة من عملية مصادقة وكيل الويب، يتضمن الوقت المطلوب لوكيل الويب لإرسال الطلب.
إستجابة DNS	%:<d	الوقت المستغرق من قبل وكيل ويب لإرسال طلب اسم المجال (DNS) إلى عملية DNS الخاصة بوكيل الويب.
إجمالي DNS	%:>d	الوقت المستغرق من قبل عملية DNS الخاصة بوكيل الويب لإعادة نتيجة DNS إلى وكيل الويب.
إستجابة WBRS	%:<r	وقت الانتظار لتلقي الاستجابة من عوامل تصفية سمات الويب، بعد أن قام وكيل ويب بإرسال الطلب.

إجمالي WBRS	%:>r	وقت الانتظار لتلقي الحكم من "عوامل تصفية سمعة الويب"، يتضمن الوقت المطلوب لـ "وكيل ويب" لإرسال الطلب.
إجابة AVC	%:a>	وقت الانتظار لتلقي الاستجابة من عملية رؤية التطبيقات والتحكم فيها (AVC) بعد أن قام وكيل الويب بإرسال الطلب.
إجمالي AVC	%:a<	وقت الانتظار لتلقي الاستجابة من عملية AVC، يتضمن الوقت المطلوب لـ "وكيل ويب" لإرسال الطلب.
إستجابة DCA	%:C>	وقت الانتظار لتلقي الاستجابة من محرك تحليل المحتوى الديناميكي، بعد أن قام وكيل ويب بإرسال الطلب.
إجمالي DCA	%:C<	وقت الانتظار لتلقي الحكم من محرك تحليل المحتوى الديناميكي، يتضمن الوقت المطلوب لـ "وكيل ويب" لإرسال الطلب.
إستجابة McAfee	%:m>	وقت الانتظار لتلقي الاستجابة من محرك المسح الضوئي McAfee، بعد أن قام وكيل الويب بإرسال الطلب.
إجمالي McAfee	%:m<	وقت الانتظار لتلقي الحكم من محرك المسح الضوئي McAfee، يتضمن الوقت المطلوب لـ Web Proxy لإرسال الطلب.
در سوفوس	%:p>	وقت الانتظار لتلقي الاستجابة من محرك المسح الضوئي Sophos، بعد أن قام وكيل الويب بإرسال الطلب.
مجموع سوفوس	%:p<	وقت الانتظار لتلقي الحكم من محرك المسح الضوئي Sophos، يتضمن الوقت المطلوب لـ Web Proxy لإرسال الطلب.
إستجابة AMP	%:e>	وقت الانتظار لتلقي الاستجابة من محرك AMP، بعد أن قام وكيل الويب بإرسال الطلب.

إجمالي AMP	٪:e<	وقت الانتظار لتلقي الحكم من محرك AMP، يتضمن الوقت المطلوب لـ "وكيل ويب" لإرسال الطلب.
زمن التأخير	٪x؛ ٪l	زمن الوصول وطلب الوقت المحلي بتنسيق يمكن قراءته من قبل الإنسان: dd/mmm/yyyy : hh:mm:ss +nnn. تمت كتابة هذه الحقل باستخدام علامات اقتباس مزدوجة في سجلات الوصول. يتيح لك هذا الحقل ربط السجلات بالمشكلات دون الحاجة إلى حساب الوقت المحلي من وقت الحدث لكل إدخال سجل.
منفذ العميل	٪f	رقم المنفذ المستخدم من جانب العميل.
عنوان IP للخادم	٪k	عنوان IP لخادم الويب.
رقم منفذ الخادم	٪p	رقم منفذ خادم الويب.

المحتوى ذي الصلة

- [دليل المستخدم لـ AsyncOS 14.5 لـ Cisco Secure Web Appliance - GD (النشر العام) - Cisco]
- [إرشادات أفضل ممارسات أجهزة أمان الويب من Cisco - Cisco]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).