ASA 8.2: تكوين Syslog باستخدام ASDM

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
تكوين syslog الأساسي باستخدام ASDM
تمكين التسجيل
تعطيل التسجيل
التسجيل إلى بريد إلكتروني
التسجيل إلى خادم syslog
تكوين syslog المتقدم باستخدام ASDM
العمل باستخدام قوائم الأحداث
العمل باستخدام عوامل تصفية التسجيل
حد المعدل
تسجيل عمليات الوصول إلى قاعدة الوصول
التكوين
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
مشكلة: فقد الاتصال — تم إنهاء اتصال syslog —
الحل
لا يمكن عرض سجلات الوقت الفعلي على Cisco ASDM
الحل
معلومات ذات صلة

المقدمة

يقدم هذا المستند معلومات حول كيفية تكوين syslog على واجهة المستخدم الرسومية (ASA 8.x) من Cisco الخاصة بتطبيق Adaptive Security Device Manager (ASDM) GUI. رسائل سجل النظام هي الرسائل التي تم إنشاؤها بواسطة Cisco ASA لإعلام المسؤول بأي تغيير في التكوين أو التغييرات في إعداد الشبكة أو التغييرات في أداء الجهاز. من خلال تحليل رسائل سجل النظام، يمكن للمسؤول أستكشاف الأخطاء وإصلاحها بسهولة عن طريق إجراء تحليل للسبب الجذري.

يتم تمييز رسائل syslog بشكل رئيسي استنادا إلى مستوى خطورتها.

1. الخطورة 0 - رسائل الطوارئ - المورد غير قابل للاستخدام
2. الخطورة 1 - رسائل التنبيه - يلزم إتخاذ إجراء فوري
3. الخطورة 2 - الرسائل الحرجة - الحالات الحرجة

4. الخطورة 3 - رسائل الخطأ - حالات الخطأ
5. الخطورة 4 - رسائل التحذير - شروط التحذير
6. الخطورة 5 - رسائل الإعلام - الظروف العادية ولكن المهمة
7. الخطورة 6 - الرسائل الإعلامية - الرسائل الإعلامية فقط
8. الخطورة 7 - رسائل تصحيح الأخطاء - رسائل تصحيح الأخطاء فقط**ملاحظة:** مستوى الخطورة الأعلى هو حالة طوارئ ويتم تصحيح الأخطاء بأقل مستوى خطورة.

يتم عرض عينة رسائل syslog التي تم إنشاؤها بواسطة Cisco ASA هنا:

- ٪ASA-6-106012: رفض IP من IP_ADDRESS إلى IP_ADDRESS، IP options hex.
- ٪ASA-3-21001: خطأ في تخصيص الذاكرة
- ٪ASA-5-335003: تطبيق قائمة التحكم في الوصول (ACL) الافتراضية، ACL:ACL-name - host-address

تشير القيمة الرقمية X المحددة في "٪ASA-X-YYYYY:" إلى خطورة الرسالة. على سبيل المثال، "٪ASA-6-106012" هي رسالة معلومات و "٪ASA-5-335003" هي رسالة خطأ.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco ASA الإصدار 8.2
- Cisco ASDM، الإصدار 6.2

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

الاصطلاحات

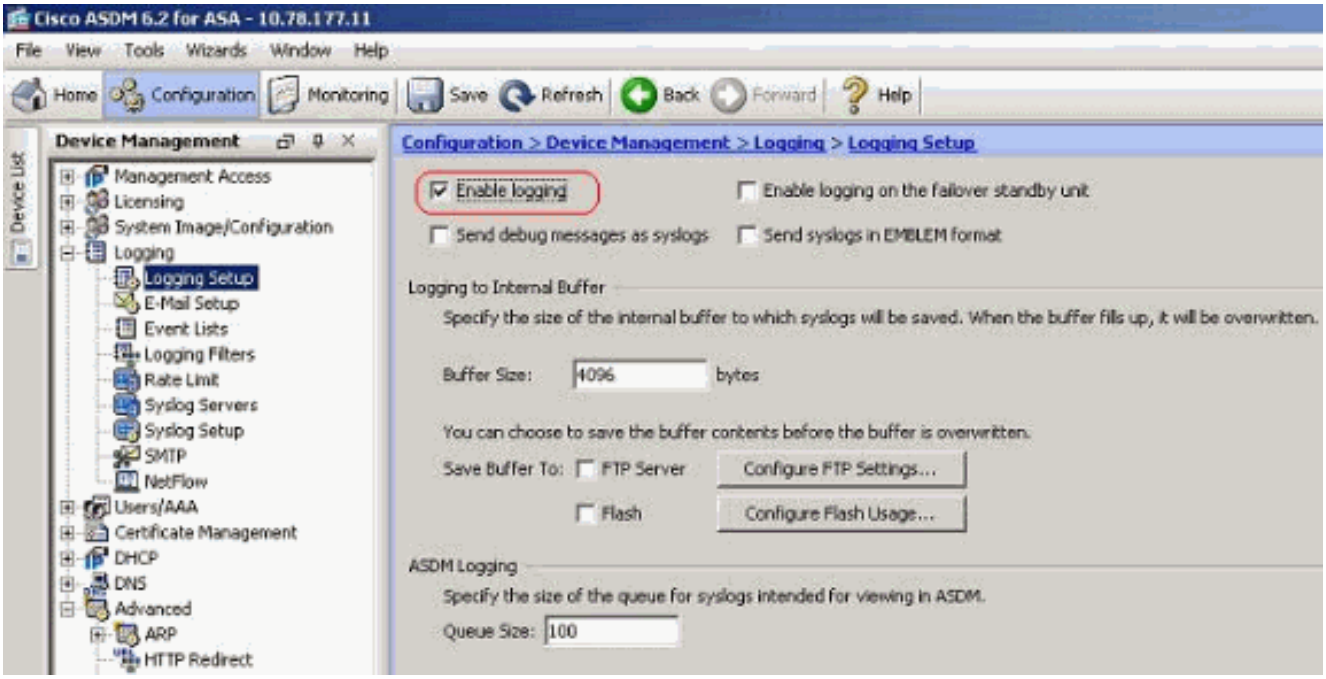
راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

تكوين syslog الأساسي باستخدام ASDM

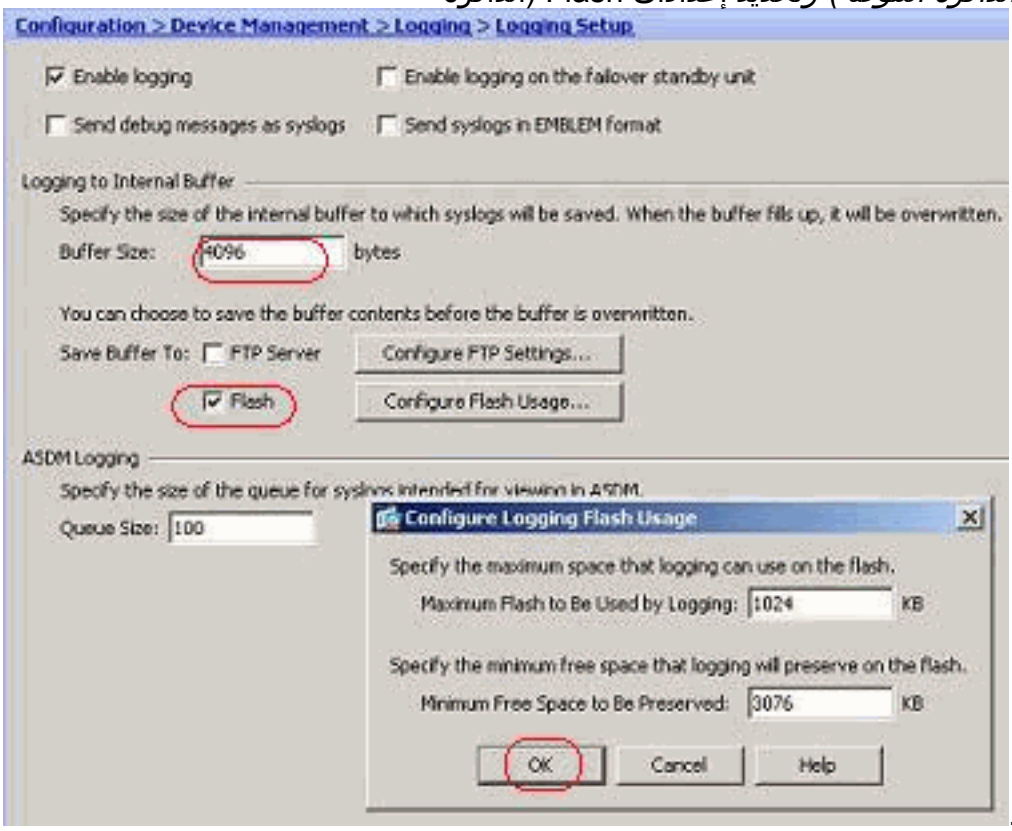
تمكين التسجيل

أكمل الخطوات التالية:

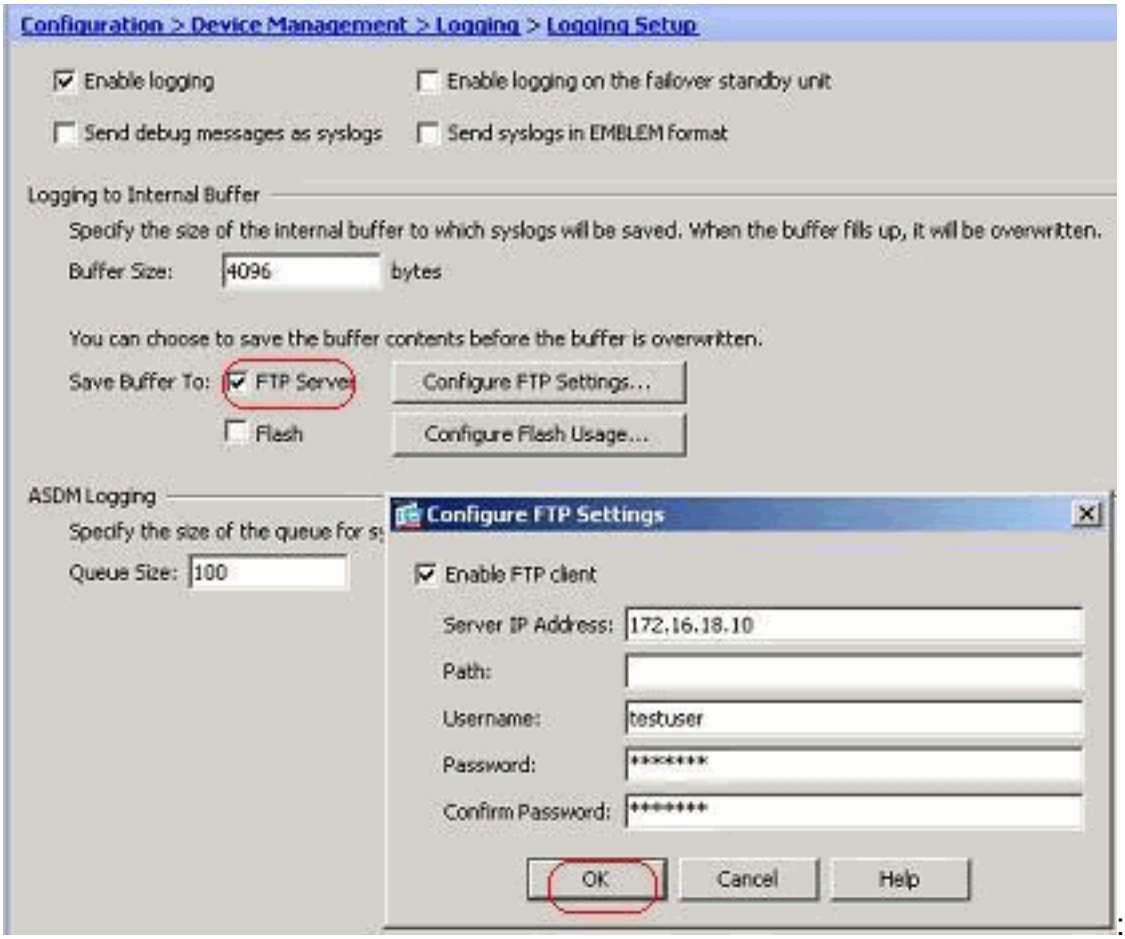
1. أخترت *تشكيل>أداة إدارة>تسجيل > تسجيل إعداد* وفحص ال *enable تسجيل* خيار.



2. يمكنك تسجيل رسائل syslog إلى مخزن مؤقت داخلي عن طريق تحديد حجم المخزن المؤقت. يمكنك أيضا إختيار حفظ محتويات المخزن المؤقت في ذاكرة Flash (الذاكرة المؤقتة) عن طريق النقر فوق *تكوين إستخدام Flash (الذاكرة المؤقتة)* وتحديد إعدادات Flash (الذاكرة المؤقتة).



3. يمكن إرسال رسائل السجل المخزن مؤقتا إلى خادم FTP قبل الكتابة فوقها. انقر على *تكوين إعدادات FTP* وحدد تفاصيل خادم FTP كما هو موضح



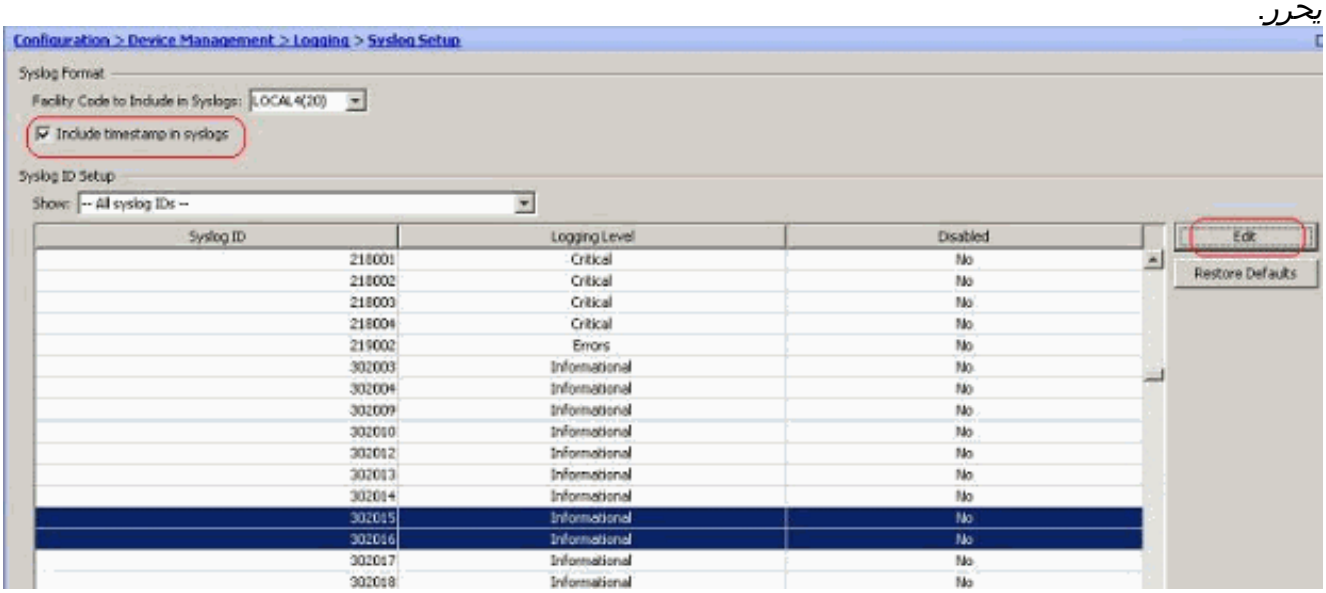
هنا:

تعطيل التسجيل

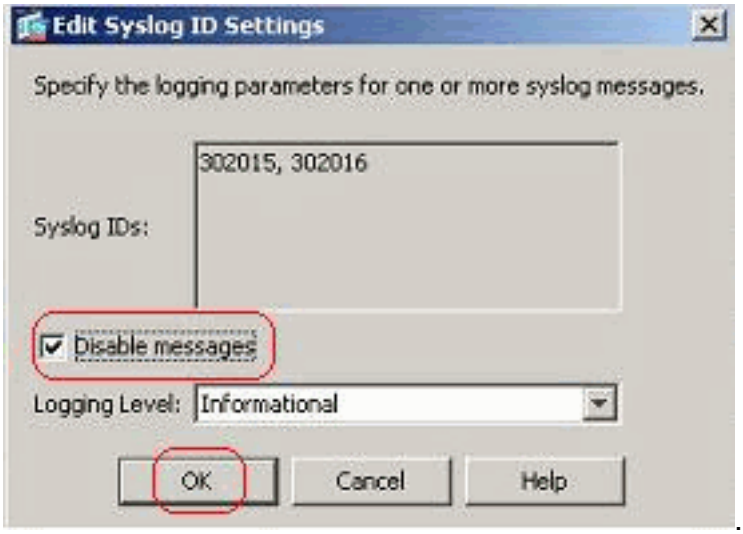
يمكنك تعطيل معرفات syslog معينة استنادا إلى متطلباتك.

ملاحظة: بتحديد علامة الاختيار لخيار *تضمين الطابع الزمني في syslogs*، يمكنك إضافة التاريخ والوقت الذي تم توليدهما كحقل إلى syslogs.

1. انتقيت ال syslogs أن يعجز وطقطقة
يحرر.

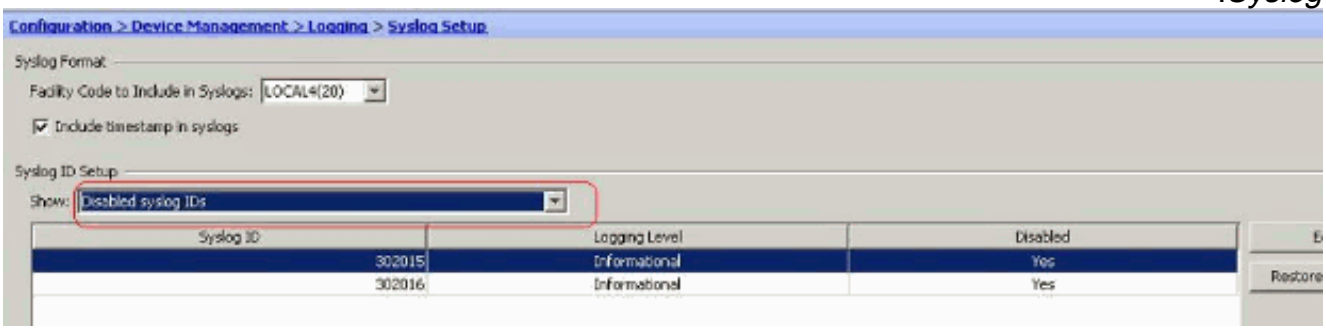


2. من نافذة *تحرير إعدادات معرف syslog*، حدد خيار *تعطيل الرسائل* وانقر على



موافق.

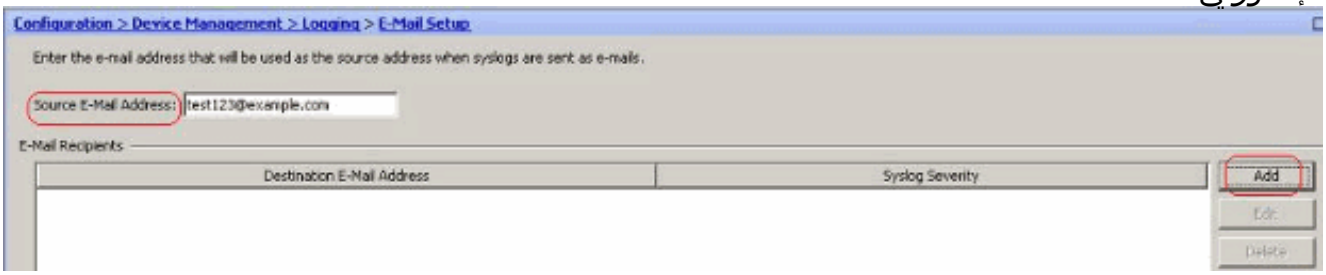
3. يمكن عرض syslog المعطلة في علامة تبويب منفصلة من خلال تحديد *معرفات syslog المعطلة* من القائمة المنسدلة *إعداد معرف Syslog*.



التسجيل إلى بريد إلكتروني

أتمت هذا steps يستعمل ASDM in order to أرسلت ال syslogs إلى بريد إلكتروني:

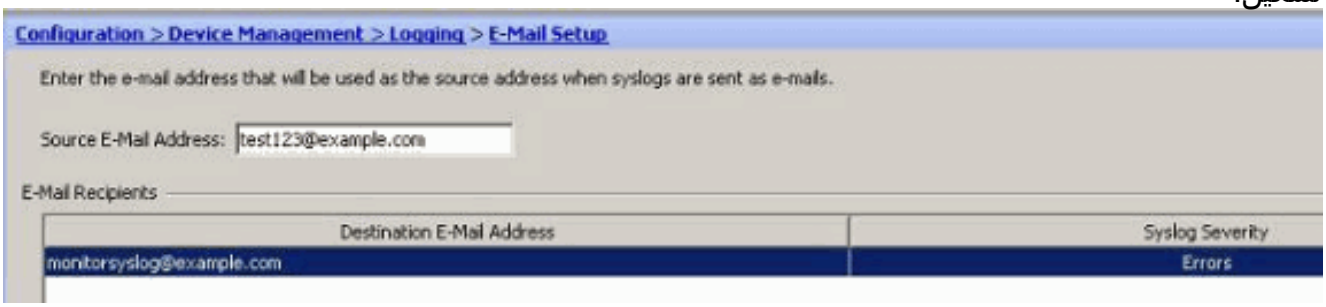
1. أختر *التكوين* > *إدارة الأجهزة* > *التسجيل* > *إعداد البريد الإلكتروني*. يفيد حقل *عنوان البريد الإلكتروني المصدر* في تعيين معرف بريد إلكتروني كمصدر ل syslogs. حدد عنوان البريد الإلكتروني المصدر. الآن، انقر فوق *إضافة* لإضافة مستلمي البريد الإلكتروني.



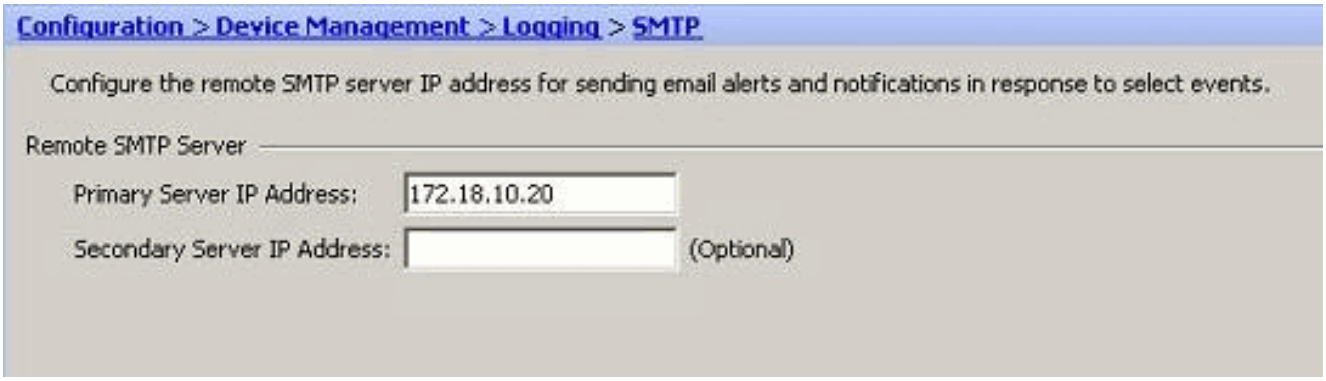
2. حدد *عنوان البريد الإلكتروني الوجهة* واختر *مستوى الخطورة*. استنادا إلى مستويات الخطورة، يمكنك تحديد مستلمي بريد إلكتروني مختلفين. انقر فوق *موافق* للعودة إلى جزء *إعداد البريد*

هذا ينتج في هذا *الإلكتروني*.

تشكيل:



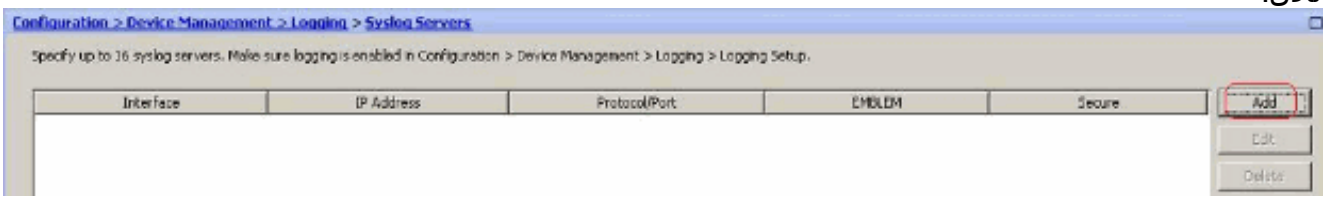
3. أختر *تكوين > إعداد الجهاز > تسجيل > SMTP* وحدد خادم SMTP.



التسجيل إلى خادم syslog

يمكنك إرسال جميع رسائل syslog إلى خادم syslog مخصص. قم بإجراء هذه الخطوات باستخدام ASDM:

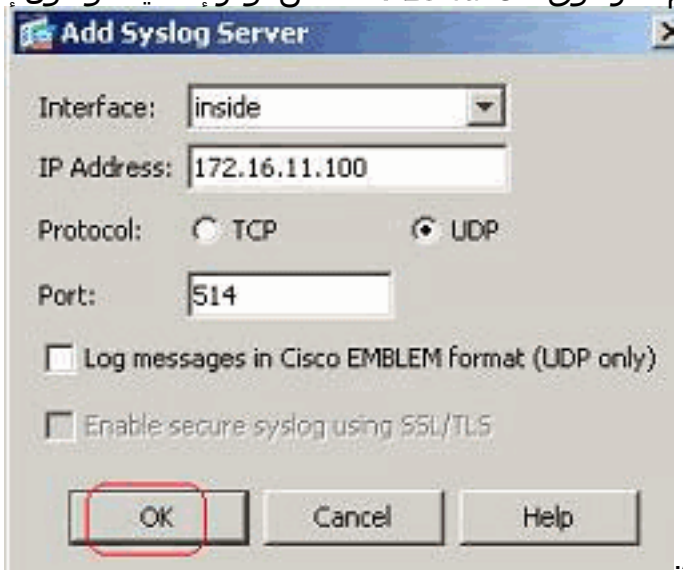
1. أخترت *تشكيل>أداة إدارة>تسجيل>syslog نادل* وطقطقة *يضيف* أن يضيف نادل.



يظهر نافذة *إضافة خادم syslog*.

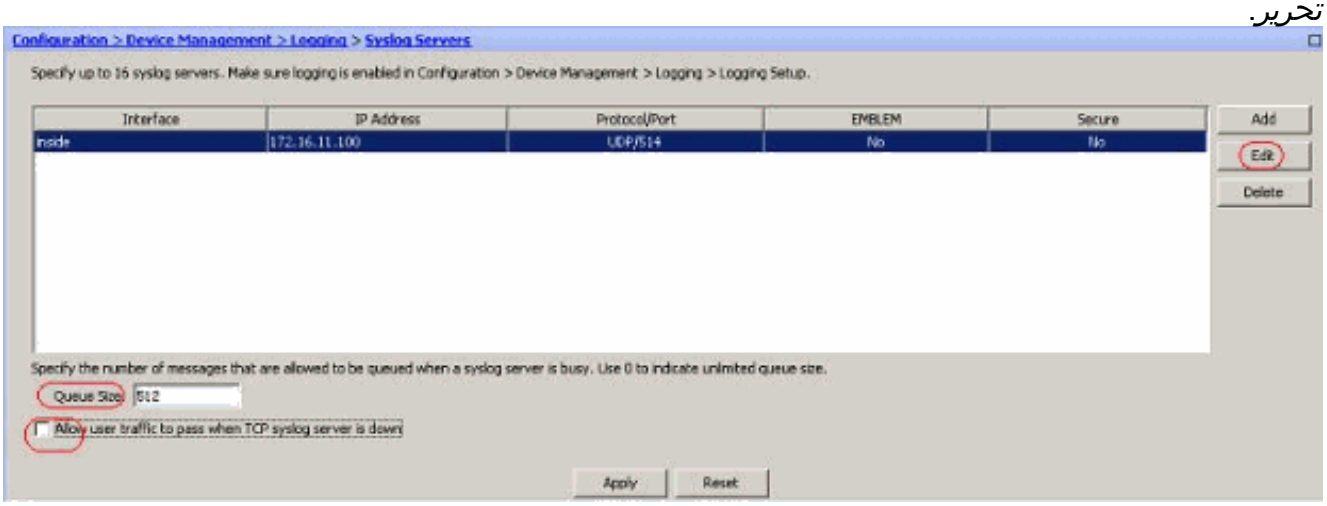
2. حدد الواجهة التي يقترن بها الخادم مع عنوان IP. حدد تفاصيل *البروتوكول والمنفذ* حسب إعداد الشبكة الخاصة

بك. ثم انقر فوق *OK*.**ملاحظة:** تأكد من توفر إمكانية الوصول إلى خادم syslog من Cisco



ASA.

3. يظهر خادم syslog الذي تم تكوينه كما هو موضح هنا. يمكن إجراء التعديلات عند تحديد هذا الخادم، ثم انقر فوق
تحرير.



ملاحظة: حدد خيار *السماح لحركة مرور المستخدم بالمرور عندما يكون خادم TCP syslog معطلا*. وإلا، يتم رفض جلسات عمل المستخدم الجديد من خلال ASA. وهذا ينطبق فقط عندما يكون بروتوكول النقل بين ASA وخادم syslog هو TCP. بشكل افتراضي، يتم رفض جلسات عمل الوصول إلى الشبكة الجديدة بواسطة Cisco ASA عندما يكون خادم syslog معطلا لأي سبب.لتحديد نوع رسائل syslog التي سيتم إرسالها إلى خادم syslog، راجع قسم عامل تصفية التسجيل.

تكوين syslog المتقدم باستخدام ASDM

العمل باستخدام قوائم الأحداث

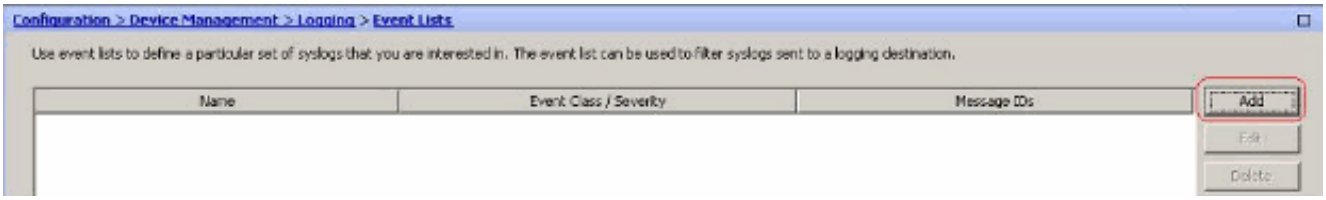
تمكننا قوائم الأحداث من إنشاء قوائم مخصصة تحتوي على مجموعة رسائل syslog التي سيتم إرسالها إلى وجهة. يمكن إنشاء قوائم الأحداث بثلاث طرق مختلفة:

- معرف الرسالة أو نطاق معرفات الرسائل
- خطورة الرسالة
- فئة الرسالة

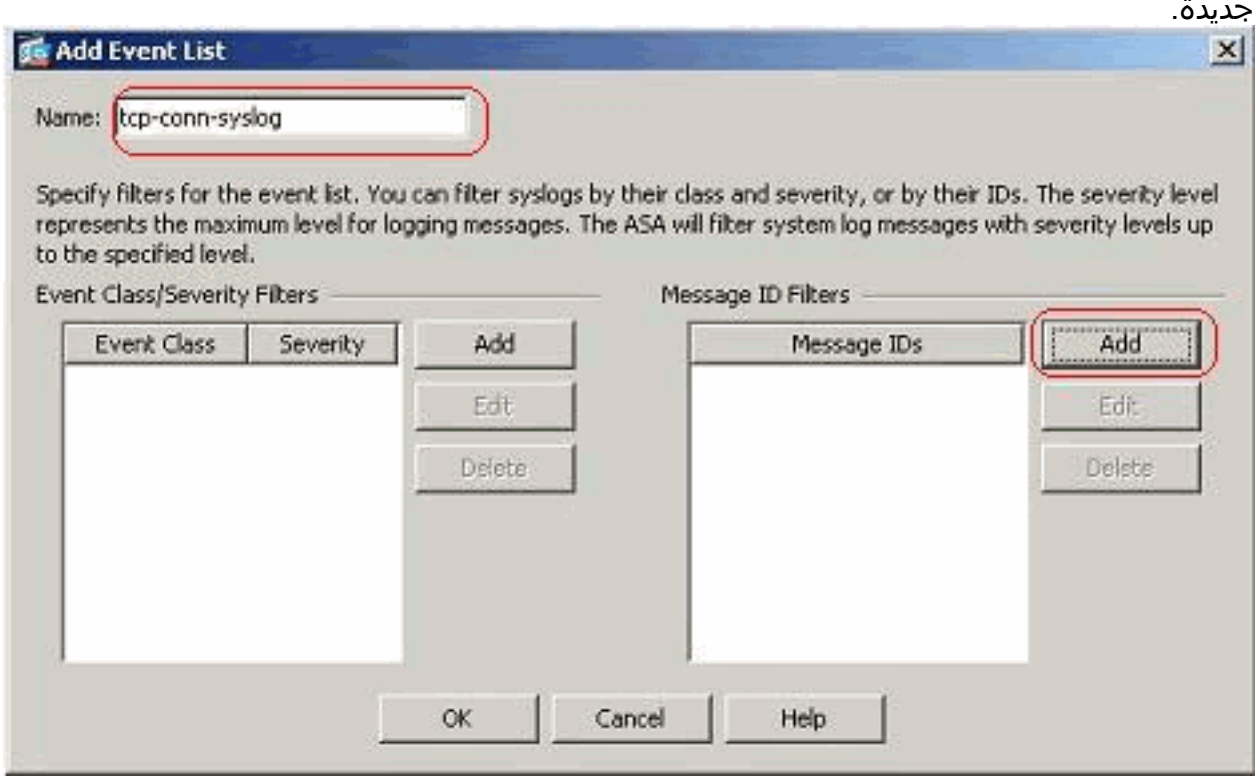
معرف الرسالة أو نطاق معرفات الرسائل

قم بإجراء هذه الخطوات:

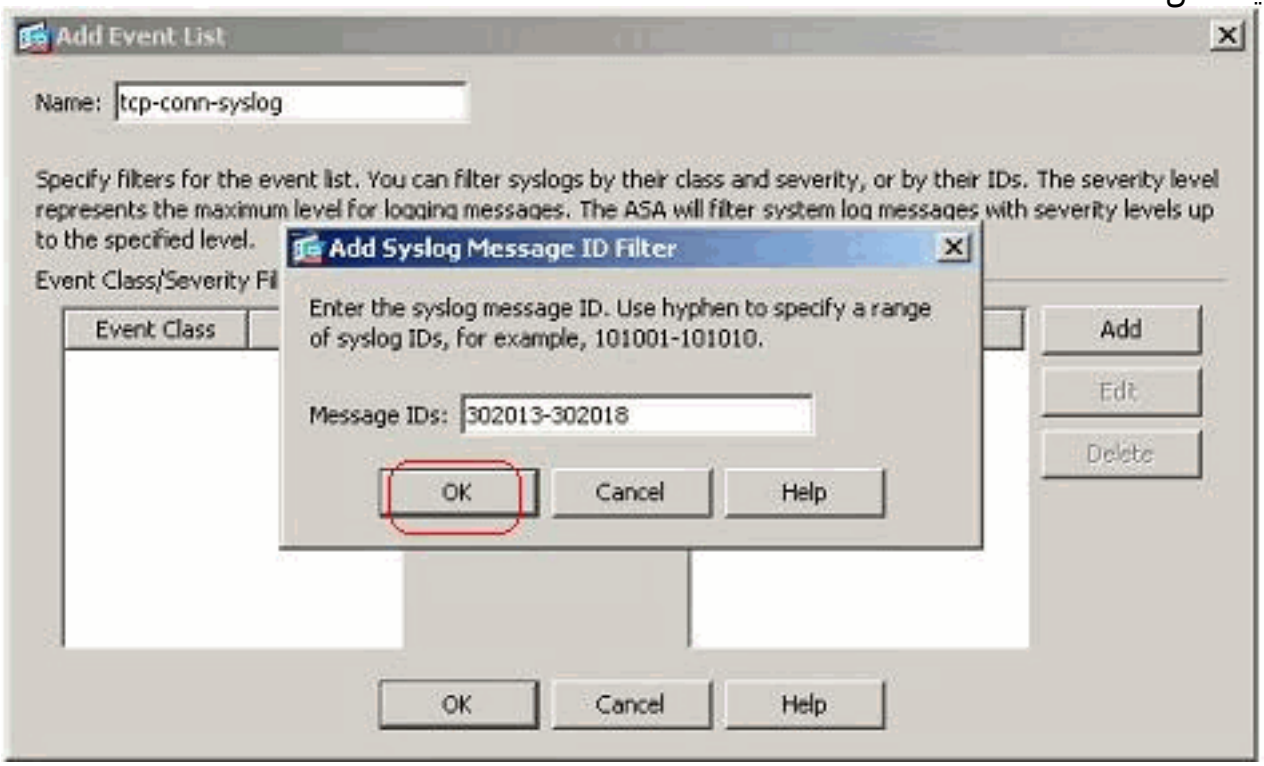
1. أخترت *تشكيل>أداة إدارة>تسجيل>حدث قائمة* وطقطقة *يضيف* أن يخلق جديد قائمة حدث.



2. حدد اسما في حقل *الاسم*. انقر فوق *إضافة* في جزء *عوامل تصفية معرف الرسالة* لإنشاء قائمة أحداث جديدة.

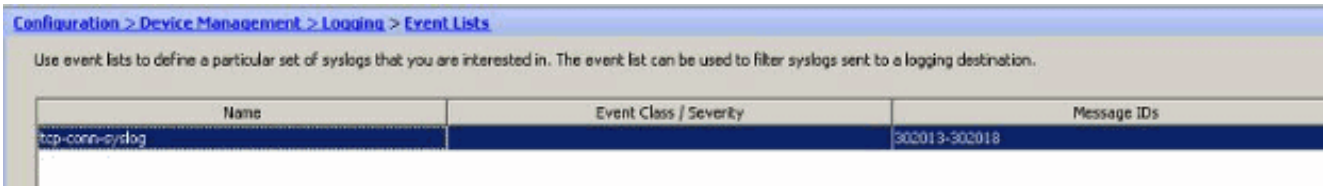


3. حدد نطاق معرفات رسائل syslog. هنا أخذت رسائل syslog ل TCP على سبيل المثال. طقطقة *ok* أن يستكمل.



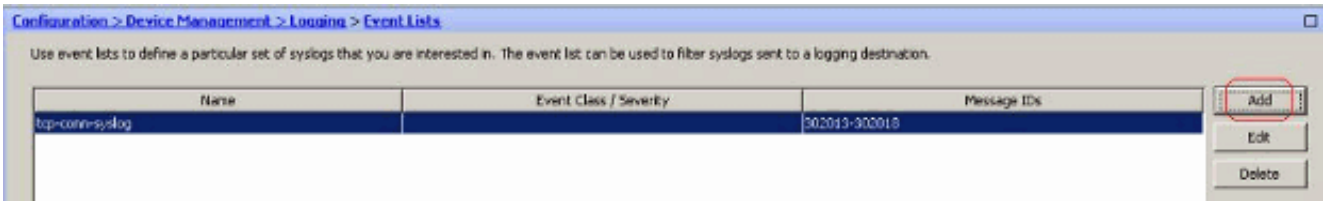
4. انقر فوق *موافق* مرة أخرى للعودة إلى نافذة *قوائم*

الأحداث.

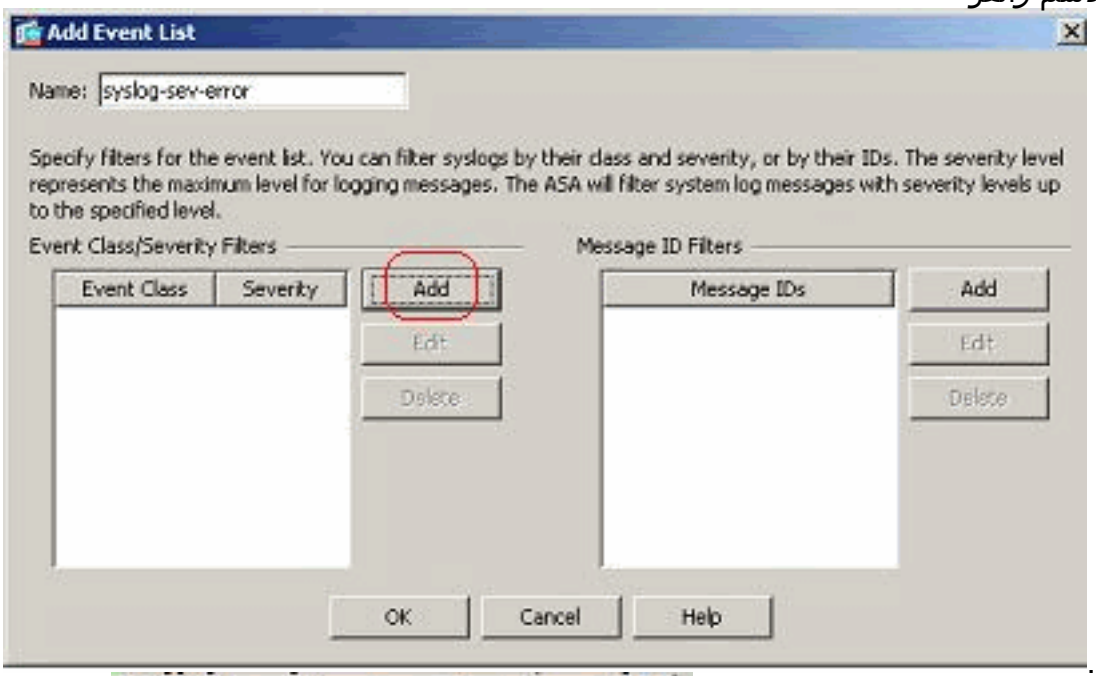


خطورة الرسالة

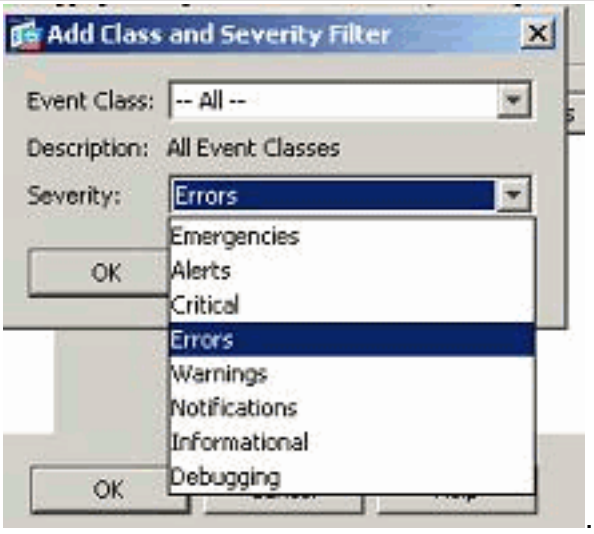
1. يمكن أيضا تحديد قوائم الأحداث استنادا إلى خطورة الرسالة. انقر فوق *إضافة* لإنشاء قائمة أحداث منفصلة.



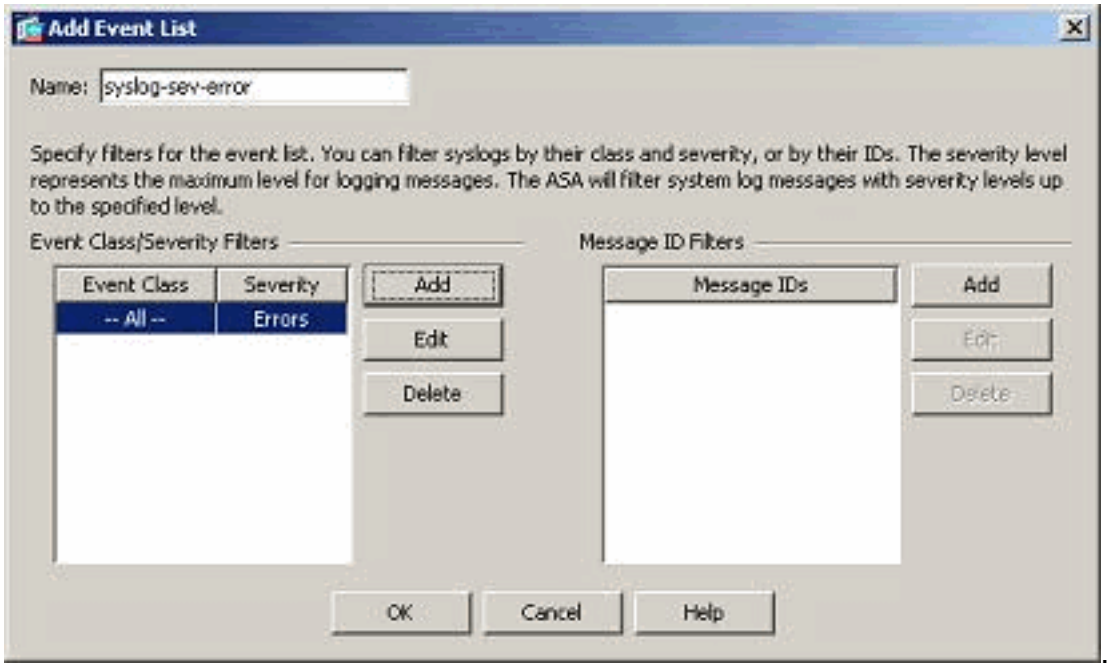
2. حدد الاسم وانقر



إضافة.



3. حدد مستوى الخطورة على هيئة *أخطاء*.



4. وانقر فوق *OK*.

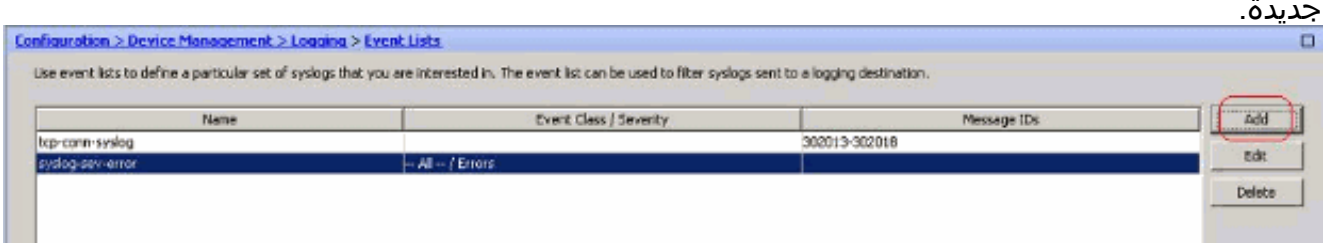
فئة الرسالة

يتم تكوين قوائم الأحداث أيضا استنادا إلى فئة الرسالة. فئة الرسالة هي مجموعة من رسائل syslog المتعلقة بميزة جهاز الأمان التي تمكنك من تحديد فئة كاملة من الرسائل بدلا من تحديد فئة لكل رسالة بشكل فردي. على سبيل المثال، أستخدم فئة المصادقة لتحديد جميع رسائل syslog المتعلقة بمصادقة المستخدم. يتم عرض بعض فئات الرسائل المتوفرة هنا:

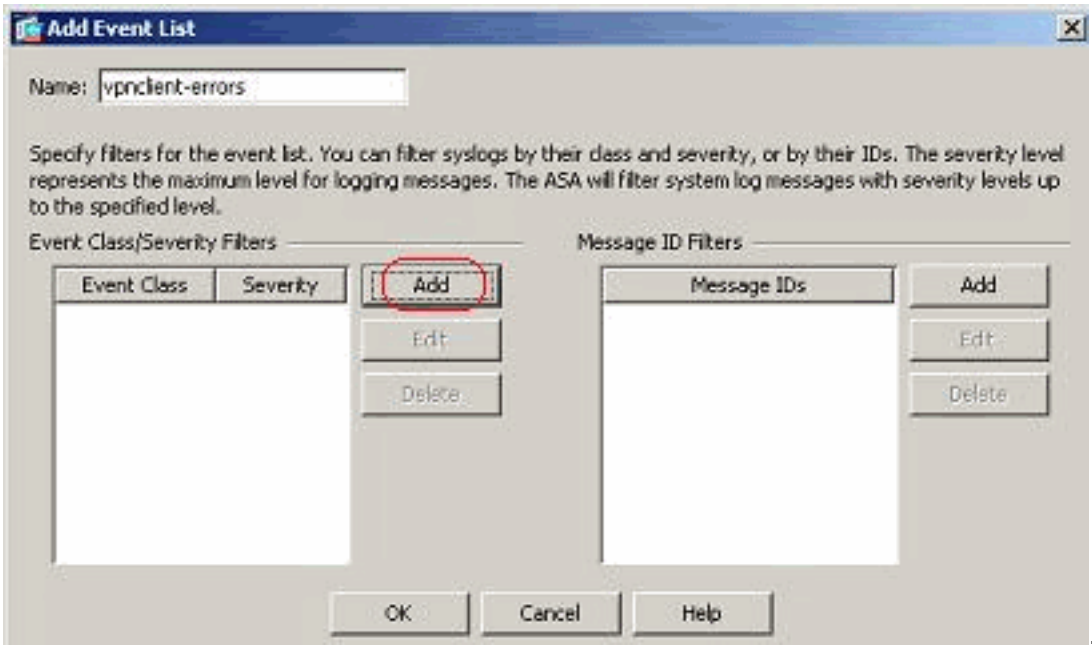
- جميع فئات الحدث
- المصادقة - مصادقة المستخدم
- جدار حماية شفاف - الجسر
- هيئة شهادة PKI—CA
- config—واجهة الأمر
- HA - تجاوز الفشل
- IPS - خدمة الحماية من التطفل
- حزمة IP—IP
- معالج الشبكة NP
- التوجيه عبر بروتوكول فتح أقصر مسار أولا (OSPF) - بروتوكول فتح أقصر مسار أولا (OSPF)
- التوجيه عبر بروتوكول معلومات التوجيه (RIP)
- جلسة مستخدم

قم بإجراء هذه الخطوات لإنشاء فئة حدث استنادا إلى فئة الرسائل *vpnClient-errors*. فئة الرسالة، *VPNC*، متوفرة لتصنيف جميع رسائل syslog المتعلقة ب vpnClient. يتم إختيار مستوى الخطورة لفئة الرسالة هذه ك "أخطاء".

1. انقر فوق إضافة لإنشاء قائمة أحداث جديدة.

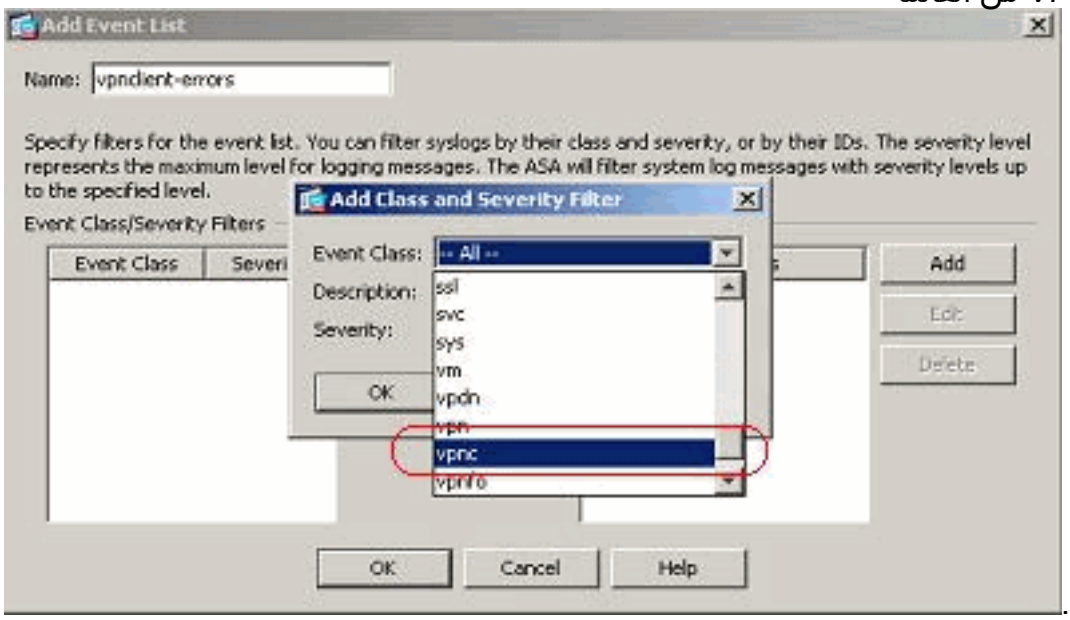


2. حدد الاسم ليكون مناسبا لفئة الرسالة التي تقوم بإنشائها وانقر فوق



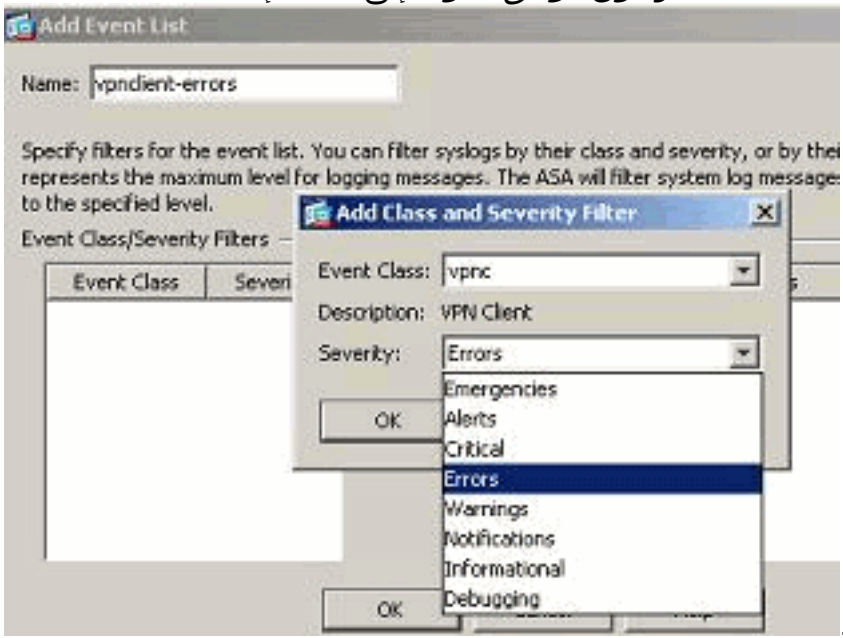
إضافة.

3. حدد *VPNC* من القائمة



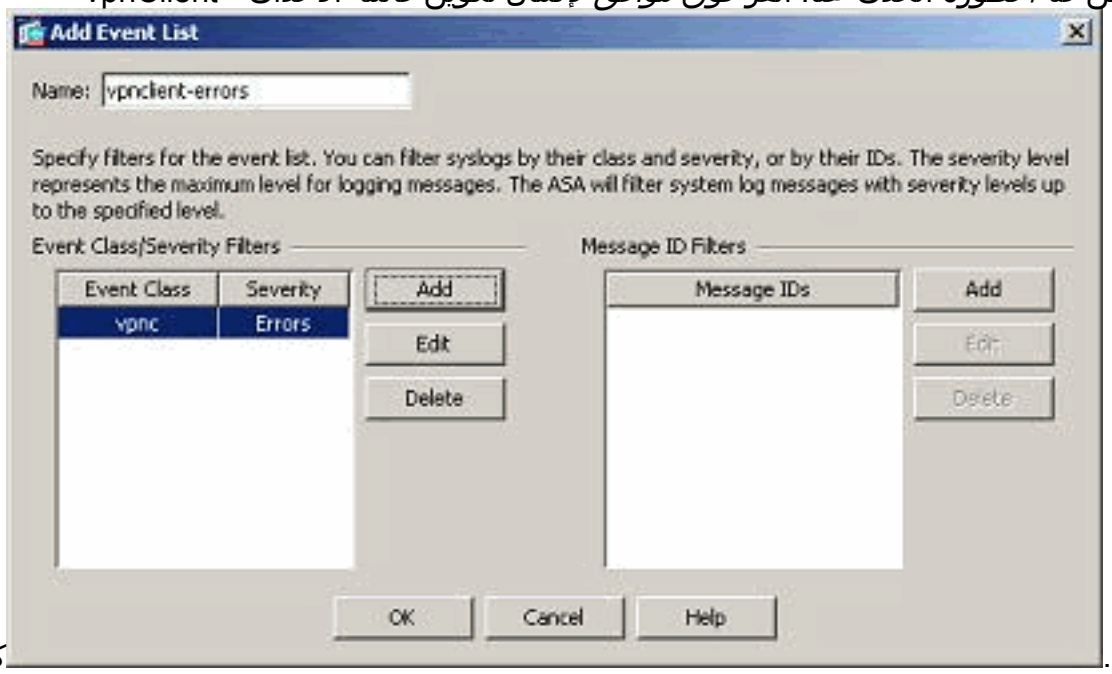
المنسدلة.

4. حدد مستوى الخطورة على هيئة *أخطاء*. مستوى الخطورة هذا قابل للتطبيق على الرسائل التي تم تسجيلها لفئة الرسالة هذه فقط. انقر فوق *موافق* للعودة إلى نافذة "إضافة قائمة

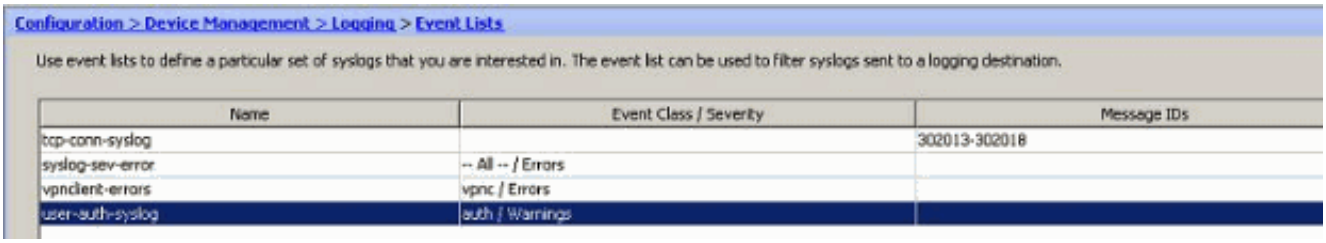


أحداث".

5. يتم عرض فئة/خطورة الحدث هنا. انقر فوق *موافق* لإكمال تكوين قائمة الأحداث "vpnClient-errors".



كما يظهر أيضا في لقطة الشاشة التالية أنه يتم إنشاء قائمة أحداث جديدة، "user-auth-syslog"، بفئة رسالة ك "auth" ومستوى الخطورة للsyslog لفئة الرسالة المحددة هذه ك "Warning". من خلال تكوين هذا الإجراء، تحدد قائمة الأحداث جميع رسائل syslog المتعلقة بفئة رسالة "المصادقة"، **التي** تصل مستويات الخطورة **إلى** مستوى "التحذيرات". **ملاحظة:** هنا، للمصطلح "حتى" أهمية. عند الإشارة إلى مستوى الخطورة، تذكر أنه سيتم تسجيل جميع رسائل syslog حتى هذا المستوى. **ملاحظة:** يمكن أن تحتوي قائمة الأحداث على فئات أحداث متعددة. يتم تعديل قائمة الأحداث "vpnClient-errors" بالنقر فوق **Edit (تحرير)** وتعريف فئة حدث جديدة "ssl/error".



العمل باستخدام عوامل تصفية التسجيل

يتم إستخدام عوامل تصفية التسجيل لإرسال رسائل syslog إلى وجهة محددة. يمكن أن تستند رسائل syslog هذه إلى "الخطورة" أو "القوائم الزوجية".

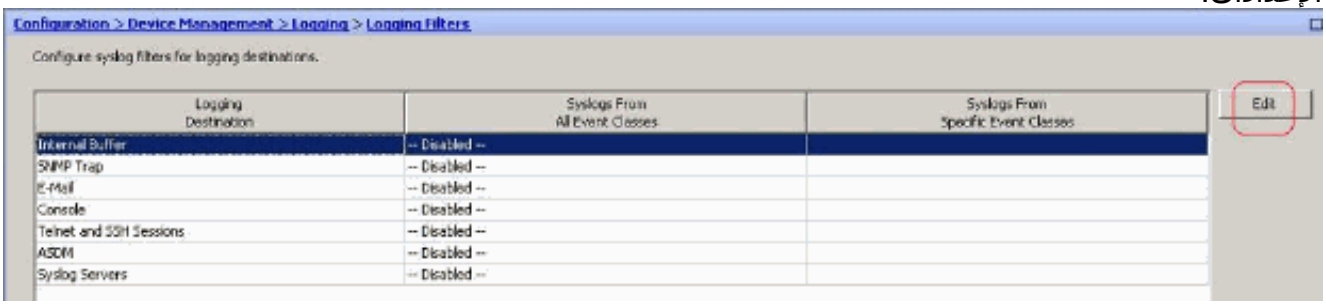
هذه هي أنواع الوجهات التي تنطبق عليها هذه عوامل التصفية:

- مخزن مؤقت داخلي
- رسائل تنبيه SNMP
- البريد الإلكتروني
- وحدة التحكم
- جلسات برنامج Telnet
- ASDM
- خوادم Syslog

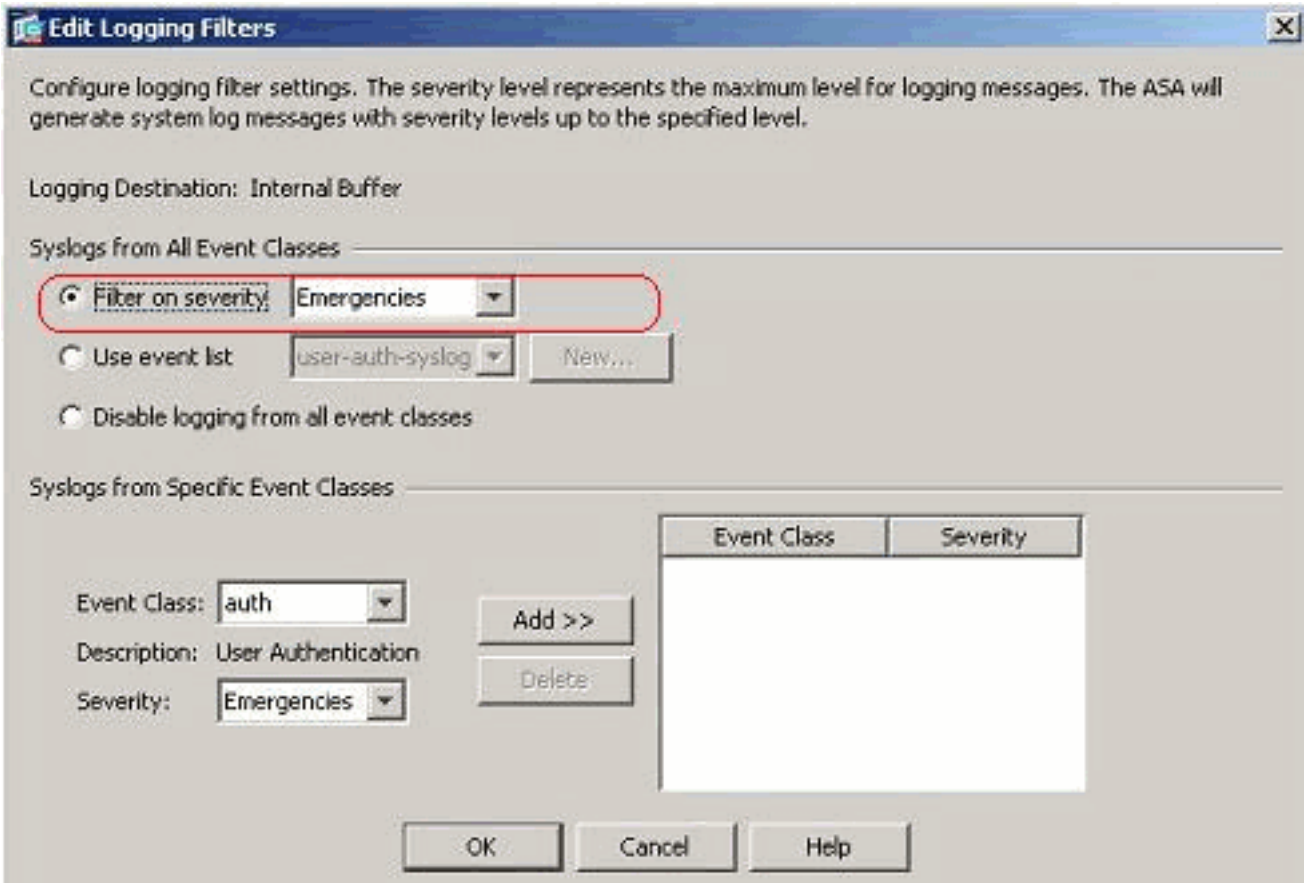
قم بإجراء هذه الخطوات:

1. أختر **التكوين > إدارة الجهاز > التسجيل > عوامل تصفية التسجيل** وحدد وجهة التسجيل. بعد ذلك، انقر **تحرير** لتعديل

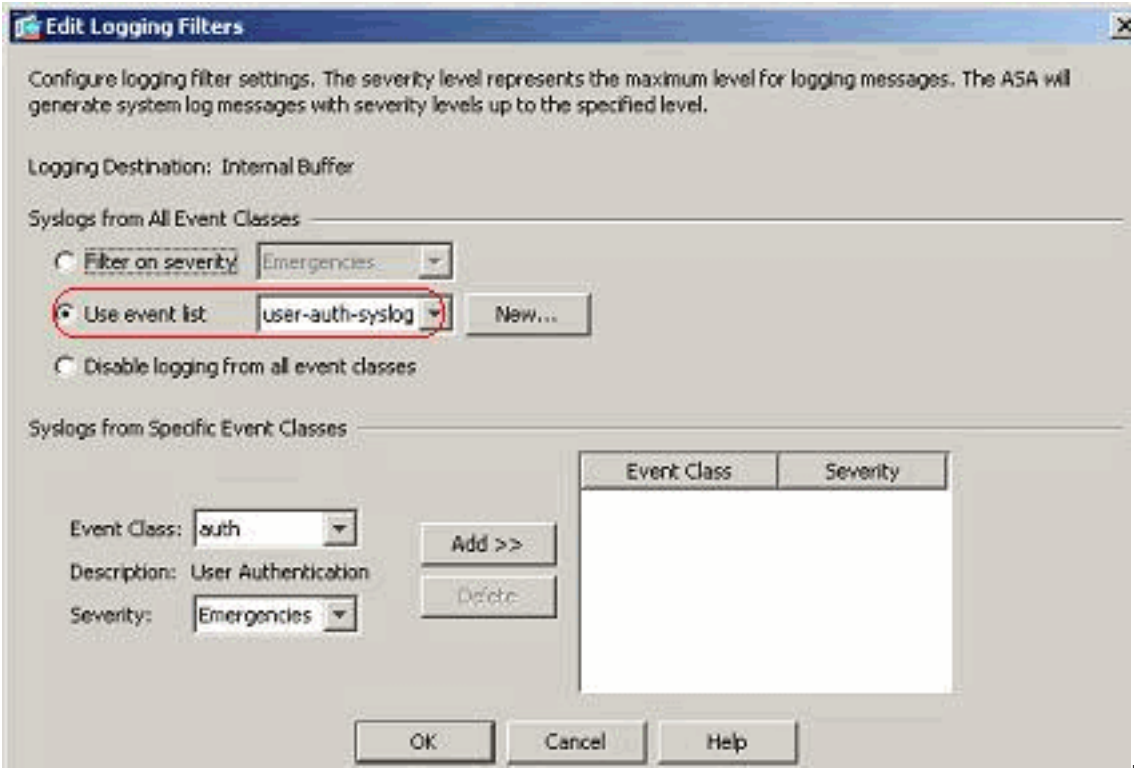
الإعدادات.



2. يمكنك إرسال رسائل syslog استنادا إلى الخطورة. وهنا تم إختيار **حالات الطوارئ** لكي تظهر كمثال.

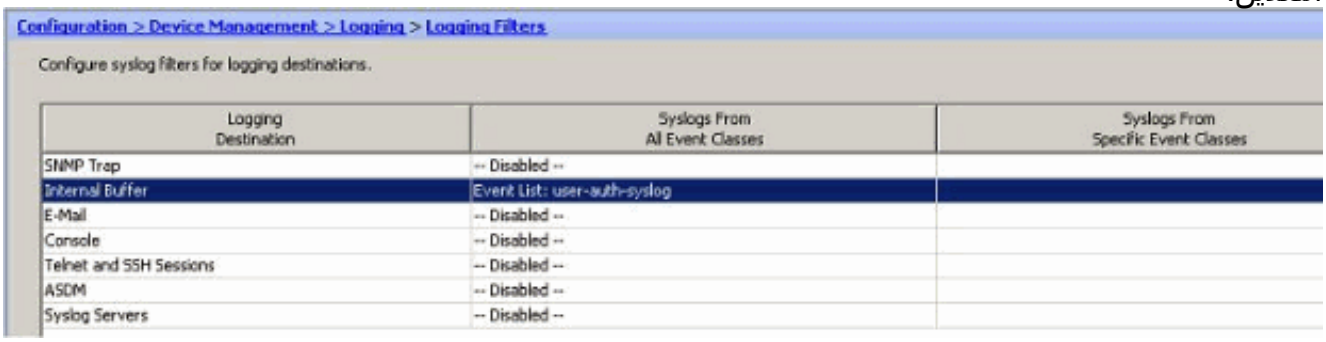


3. كما يمكن تحديد قائمة أحداث لتحديد نوع الرسائل التي سيتم إرسالها إلى وجهة معينة. وانقر فوق



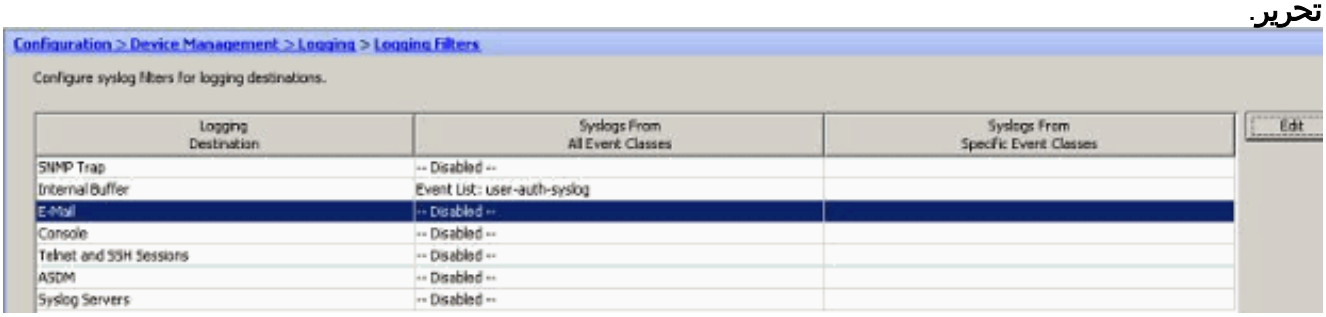
OK.

4. تحقق من التعديل.

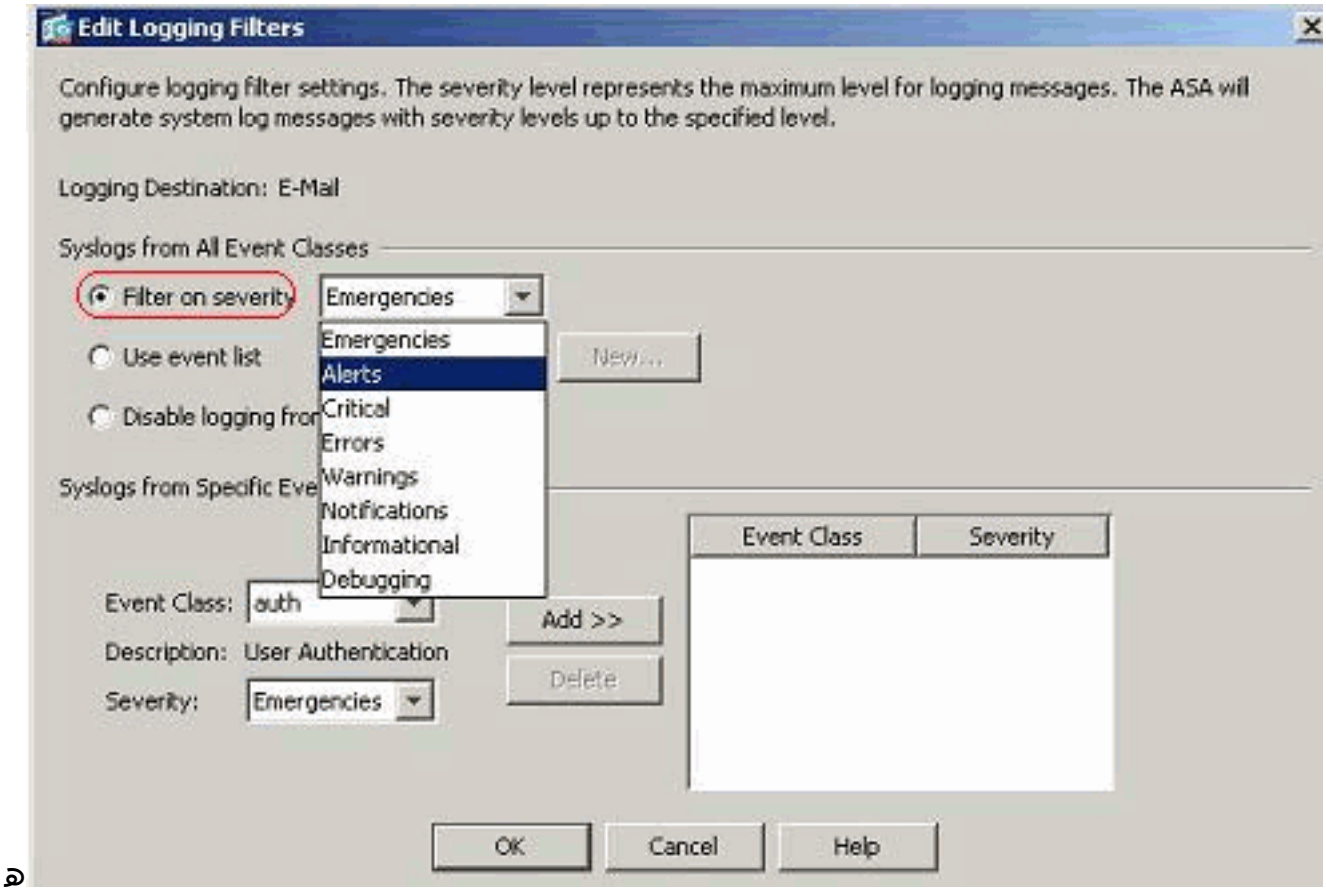


هذه هي الخطوات المتعلقة بكيفية إرسال مجموعة من الرسائل (استنادا إلى مستوى الخطورة) إلى خادم البريد الإلكتروني.

1. حدد **البريد الإلكتروني** في حقل وجهة التسجيل. بعد ذلك، انقر **تحرير**.

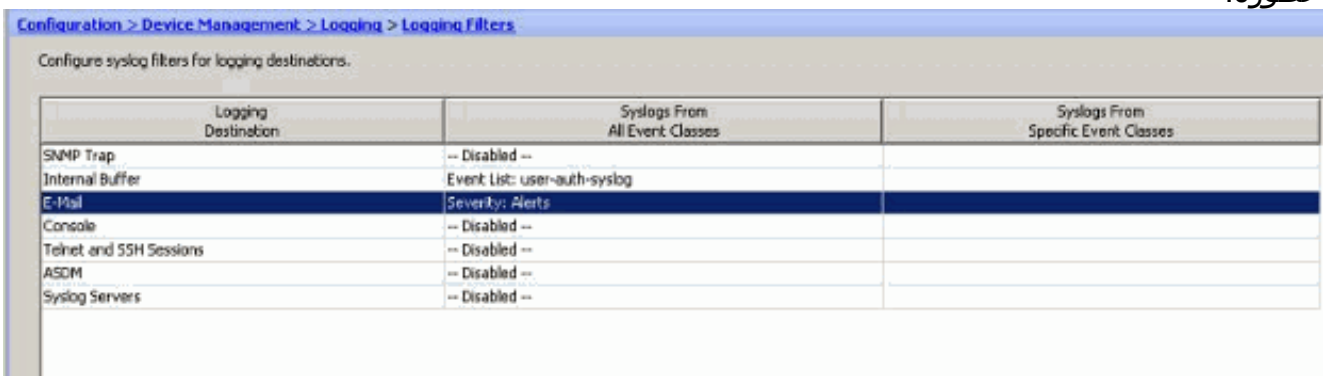


2. أختر خيار **التصفية على مستوى الخطورة** وحدد مستوى الخطورة المطلوب.

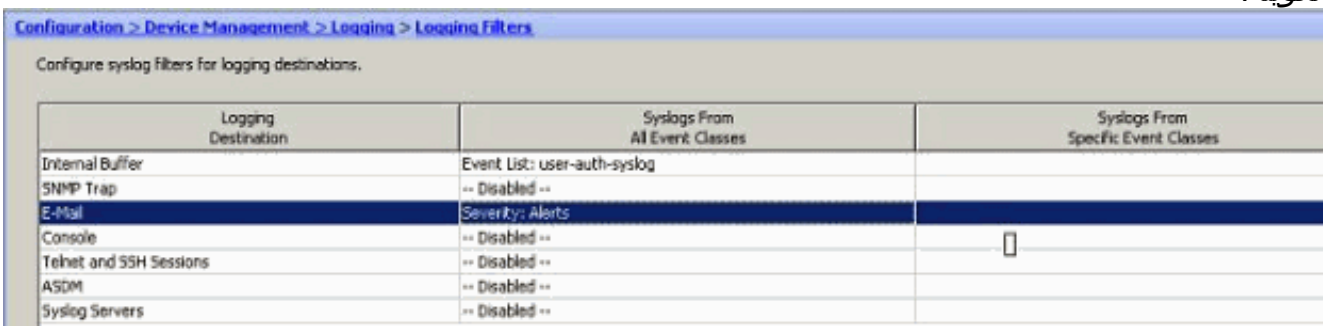


ه

نا، تم تحديد **التنبيهات** كمستوى خطورة.



يمكنك أن ترى أن كل رسائل syslog للتنبيه سيتم إرسالها إلى البريد الإلكتروني الذي تم تكوينه.

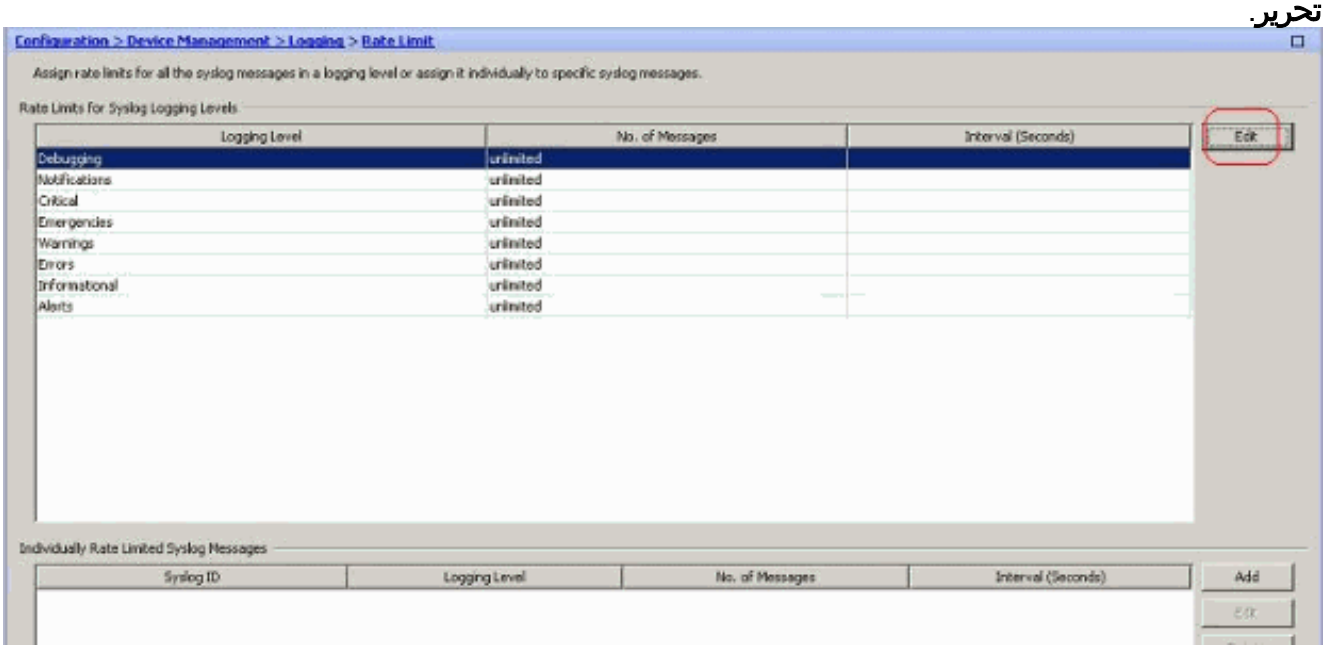


حد المعدل

هذا يحدد عدد رسائل syslog التي يرسلها Cisco ASA إلى وجهة في فترة زمنية محددة. ويتم تعريفه عادة لمستوى الخطورة.

1. أختر **التكوين > إدارة الجهاز > التسجيل > حد المعدل** وحدد مستوى الخطورة المطلوب. بعد ذلك، انقر

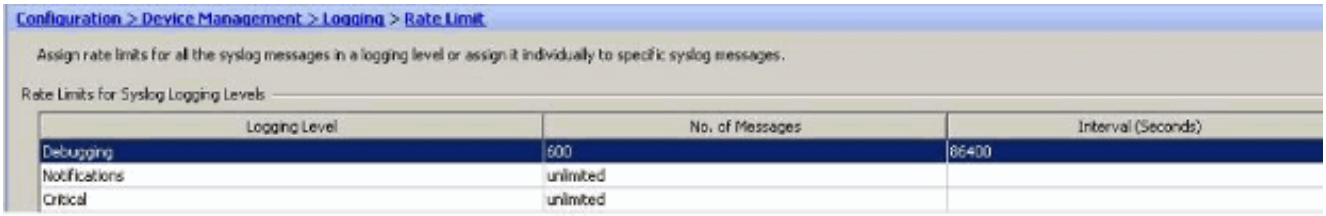
تحرير.



2. حدد عدد الرسائل التي سيتم إرسالها مع الفاصل الزمني. وانقر فوق

OK. **ملاحظة:** تعطى هذه الأرقام كمثال.

وتختلف هذه العناصر حسب نوع بيئة الشبكة.تظهر هنا القيم المعدلة:

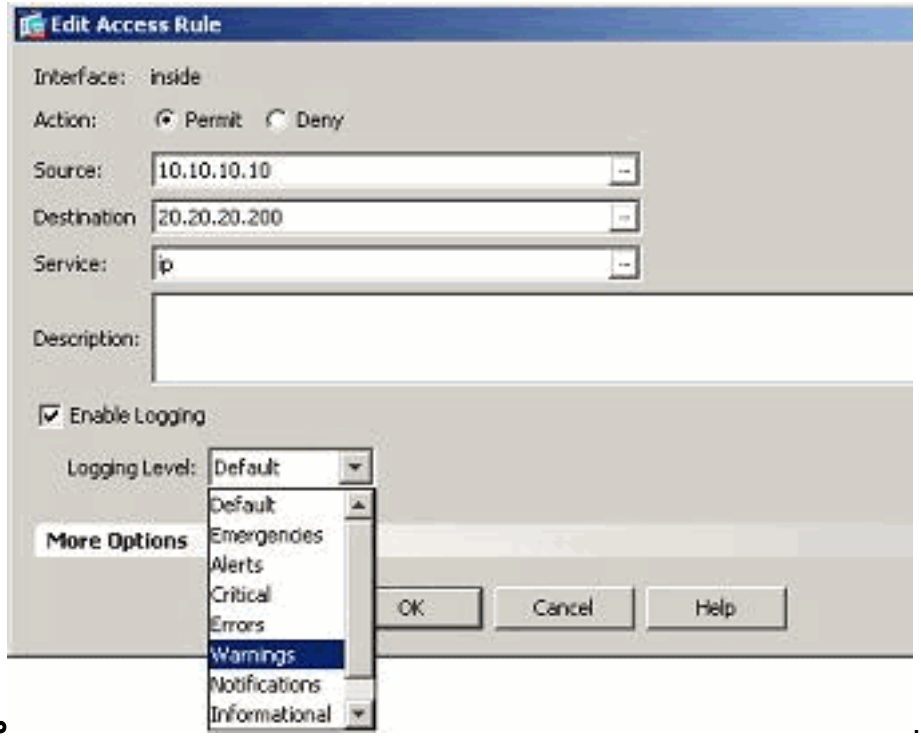


تسجيل عمليات الوصول إلى قاعدة الوصول

يمكنك تسجيل عمليات الوصول الناجحة لقاعدة الوصول باستخدام ASDM. سلوك التسجيل الافتراضي هو إرسال رسالة syslog لجميع الحزم المرفوضة. لن تكون هناك أي رسالة syslog للحزم المسموح بها ولن يتم تسجيل هذه الرسائل. ومع ذلك، يمكنك تحديد مستوى خطورة تسجيل مخصص لقاعدة الوصول لتعقب عدد الحزم التي تصل إلى قاعدة الوصول هذه.

قم بإجراء هذه الخطوات:

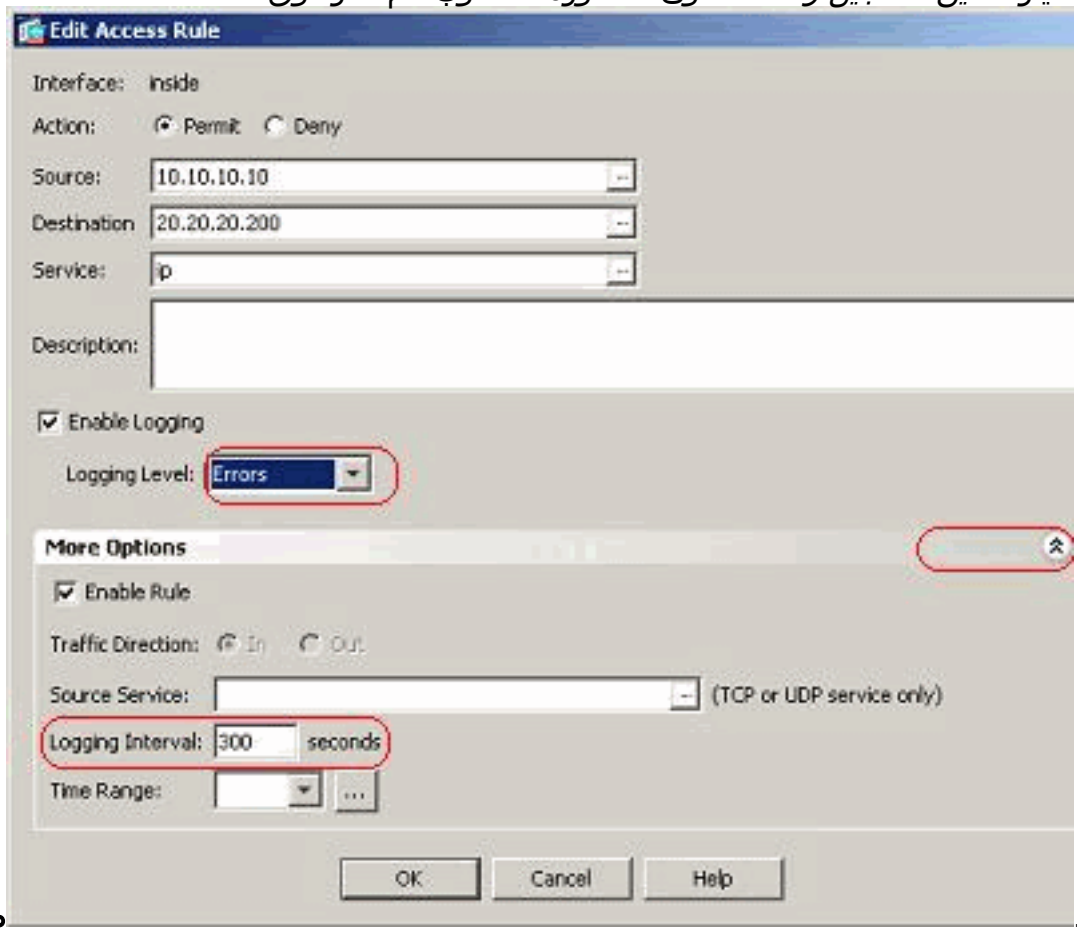
1. حدد قاعدة الوصول المطلوبة وانقر فوق *تحرير*.تظهر نافذة *تحرير قاعدة*



الوصول.

ملاحظة: في هذه الصورة، يشير الخيار *الافتراضي* في حقل *مستوى التسجيل* إلى سلوك التسجيل الافتراضي ل Cisco ASA. للحصول على مزيد من المعلومات حول هذا الأمر، ارجع إلى قسم نشاط قائمة الوصول إلى التسجيل.

2. حدد خيار *تمكين التسجيل* وحدد مستوى الخطورة المطلوب. ثم انقر فوق

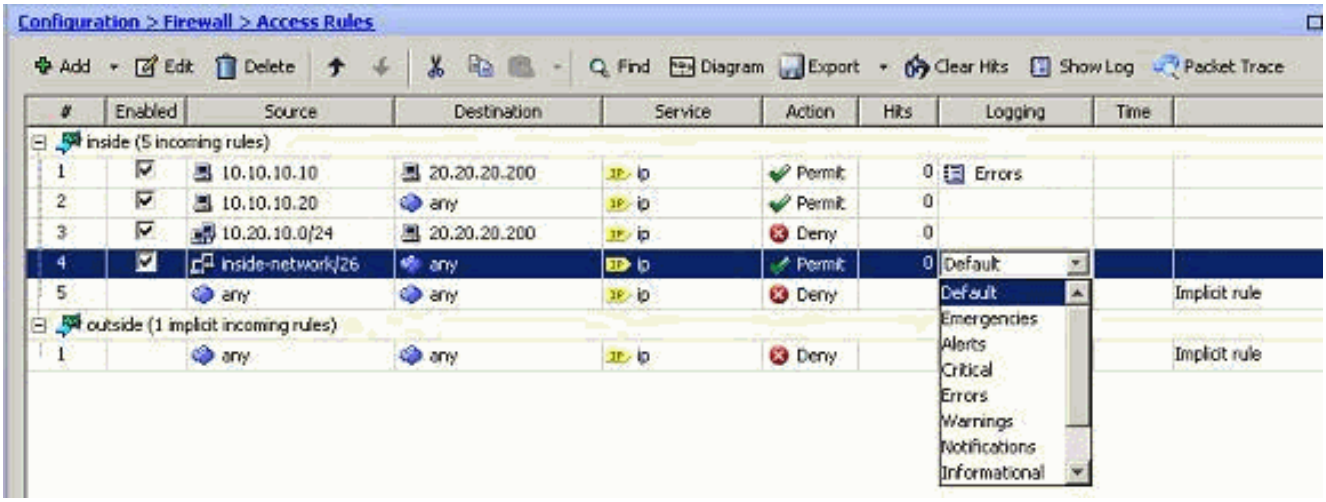


OK.

ملاحظة: بالنقر على علامة التبويب المنسدلة *المزيد من الخيارات*، يمكنك الاطلاع على خيار *الفاصل الزمني للتسجيل*. يتم إبراز هذا الخيار فقط عندما يكون خيار *تمكين التسجيل* المذكور أعلاه محددا. قيمة هذا المؤقت الافتراضية هي 300 ثانية. يكون هذا الإعداد مفيدا في تحديد قيمة المهلة الزمنية لإحصائيات التدفق التي سيتم حذفها عندما لا يكون هناك تطابق لقاعدة الوصول تلك. إذا كانت هناك أي عمليات وصول، فعندئذ ينتظر ASA حتى وقت فاصل التسجيل ويرسل ذلك إلى syslog.

3. يتم عرض التعديلات هنا. بدلا من ذلك، يمكنك النقر المزدوج فوق حقل *التسجيل* لقاعدة الوصول المحددة

وتعيين مستوى الخطورة
هناك.



ملاحظة: يعمل هذا الأسلوب البديل لتحديد *مستوى التسجيل* في نفس *جزء قواعد الوصول* بالنقر المزدوج على إدخالات قاعدة الوصول التي تم إنشاؤها يدويا فقط، وليس على القواعد الضمنية.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

التكوينات

يستخدم هذا المستند التكوينات التالية:

Cisco ASA

```
Saved :
:
(ASA Version 8.2(1
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/1
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.0
!
interface Ethernet0/2
nameif inside
security-level 100
ip address 10.78.177.11 255.255.255.192
```

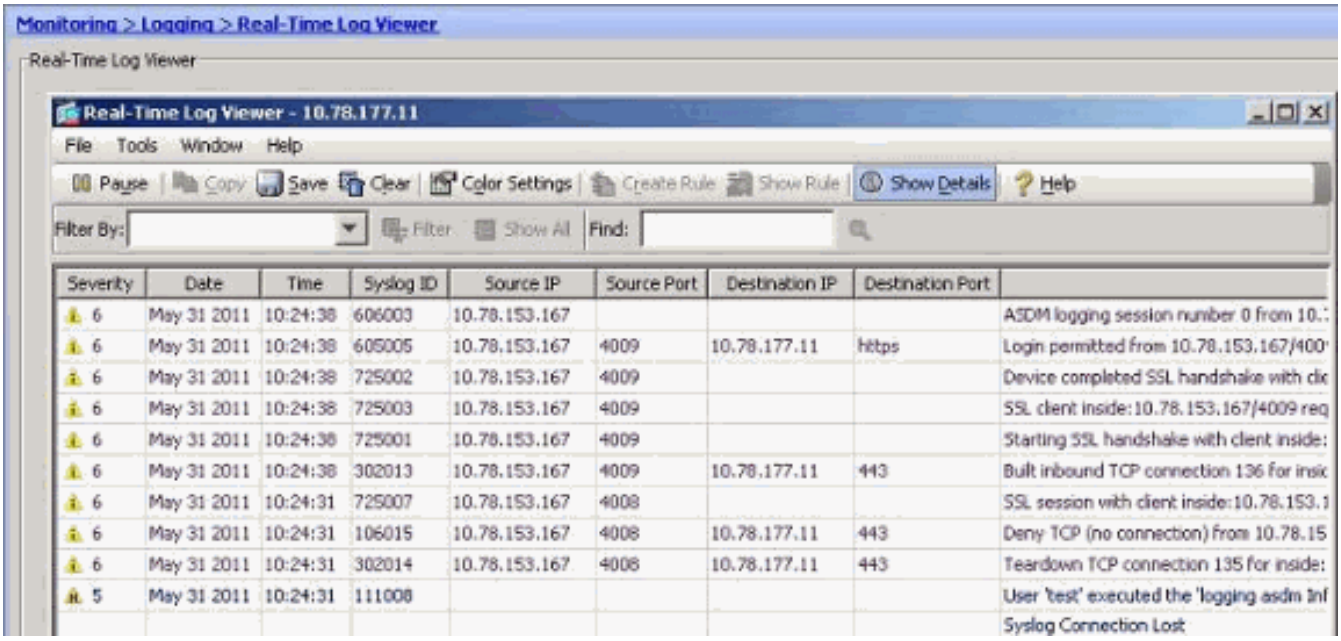
```
!
Output Suppressed ! access-list inside_access_in ---!!
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors
access-list inside_access_in extended permit ip host
10.10.10.20 any
access-list inside_access_in extended deny ip 10.20.10.0
255.255.255.0 host 20.20.20.200
access-list inside_access_in extended permit ip
10.78.177.0 255.255.255.192 any log emergencies
pager lines 24
logging enable
logging list user-auth-syslog level warnings class auth
logging list TCP-conn-syslog message 302013-302018
logging list syslog-sev-error level errors
logging list vpnclient-errors level errors class vpnc
logging list vpnclient-errors level errors class ssl
logging buffered user-auth-syslog
logging mail alerts
logging from-address test123@example.com
logging recipient-address monitorsyslog@example.com
level errors
logging queue 1024
logging host inside 172.16.11.100
logging ftp-bufferwrap
**** logging ftp-server 172.16.18.10 syslog testuser
logging permit-hostdown
no logging message 302015
no logging message 302016
logging rate-limit 600 86400 level 7
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-623.bin
asdm history enable
arp timeout 14400
Output Suppressed ! timeout xlate 3:00:00 timeout ---!!
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00 timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute timeout TCP-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy ! !---
Output Suppressed ! ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list no threat-detection
statistics TCP-intercept ! !--- Output Suppressed !
username test password /FzQ9W6s1KjC0YQ7 encrypted
privilege 15 ! ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global smtp-server 172.18.10.20
prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4
end :
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- أنت يستطيع شاهدت ال syslogs من ال ASDM. أختر **مراقبة > تسجيل > عارض سجل الوقت الحقيقي**. يتم عرض نموذج للمخرجات
هنا:



استكشاف الأخطاء وإصلاحها

مشكلة: فقد الاتصال — تم إنهاء اتصال syslog —

يتم تلقي هذا الخطأ عند محاولة تمكين تسجيل ASDM في لوحة معلومات الجهاز لأي سياق.

```
"— syslog    — "
```

عند إستخدام ASDM للاتصال مباشرة بسياق الإدارة وتعطيل تسجيل ADSM هناك، قم بالتبديل إلى سياق فرعي وتمكين تسجيل ASDM. يتم تلقي الأخطاء، ولكن رسائل syslog تصل إلى Fine إلى خادم syslog.

الحل

هذا سلوك معروف مع Cisco ASDM وموثق في معرف تصحيح الأخطاء من CSCsd10699 Cisco (العملاء المسجلون فقط). كحل بديل، قم بتمكين تسجيل ASDM عند تسجيل الدخول إلى سياق الإدارة.

لا يمكن عرض سجلات الوقت الفعلي على Cisco ASDM

توجد مشكلة في عدم إمكانية عرض سجلات الوقت الفعلي على ASDM. كيف يتم تكوين هذا؟

الحل

شكلت التالي على ال cisco ASA:

```
ciscoasa(config)#logging monitor 6
ciscoasa(config)#terminal monitor
ciscoasa(config)#logging on
ciscoasa(config)#logging trap 6
```

معلومات ذات صلة

- دعم أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- الدعم التقني والمستندات - Cisco Systems

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).