تكوين جهاز الأمان القابل للتكيف (ASA) Syslog

المحتويات

المقدمة

يصف هذا المستند نموذج التكوين الذي يوضح كيفية تكوين خيارات تسجيل مختلفة على ASA التي تشغل الإصدار 8.4 من الرمز أو إصدار أحدث.

معلومات أساسية

قام الإصدار 8.4 من ASA بإدخال تقنيات تصفية متعددة المستويات للغاية للسماح بعرض رسائل syslog معينة فقط. يوضح قسم syslog الأساسي في هذا المستند تكوين syslog التقليدي. يبدي ال متقدم syslog قسم من هذا وثيقة الجديد syslog سمة في صيغة syslog. 8،4. ارجع إلى أدلة رسائل سجل النظام الخاصة ب Cisco Security Appliance للحصول على دليل رسائل سجل النظام بالكامل.

المتطلبات الأساسية

المتطلبات

ال توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- ASA 5515 مع برنامج ASA، الإصدار 8.4
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 7.1.6

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.

ملاحظة: راجع ASA 8.2: تكوين syslog باستخدام ASDM للحصول على مزيد من المعلومات حول تفاصيل تكوين مماثلة باستخدام الإصدار 7.1 من ASDM والإصدارات الأحدث.

Syslog أساسي

أدخل هذه الأوامر لتمكين التسجيل وعرض السجلات وعرض إعدادات التكوين.

- logging enable - يتيح إرسال رسائل syslog إلى جميع مواقع الإخراج.
- no logging enable - يعجز التسجيل إلى جميع مواقع الإخراج.
- show logging - يسرد محتويات المخزن المؤقت syslog بالإضافة إلى المعلومات والإحصائيات المتعلقة بالتكوين الحالي.

يمكن أن يرسل ال ASA رسائل syslog إلى وجهات مختلفة. دخلت الأمر في هذا قسم in order to عينت المكان أنت تريد ال syslog معلومة أن يكون أرسلت:

إرسال معلومات التسجيل إلى المخزن المؤقت الداخلي

<#root>

logging buffered

 severity_level

ال يلزم وجود برنامج خادم أو جهاز خارجي عند تخزين رسائل syslog في المخزن المؤقت الداخلي ل ASA. أدخل الأمر show logging لعرض رسائل syslog المخزنة. يحتوي المخزن المؤقت الداخلي على حد أقصى لحجم 1 ميجابايت (قابل للتكوين باستخدام الأمر logging buffer-size). ونتيجة لذلك، يمكن أن يلتف بسرعة كبيرة. تذكر هذا عند إختيار مستوى تسجيل للمخزن المؤقت الداخلي حيث يمكن لمزيد من مستويات السرعة للتسجيل أن تعبئ المخزن المؤقت الداخلي وتلفه بسرعة.

إرسال معلومات التسجيل إلى خادم syslog

<#root>

logging host

 interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]

logging trap

 severity_level

logging facility

 number

يلزم وجود خادم يقوم بتشغيل تطبيق syslog لإرسال رسائل syslog إلى مضيف خارجي. يرسل ASA syslog على UDP ميناء 514 افتراضيا، غير أن بروتوكول وميناء يستطيع كنت إخترت. إذا تم إختيار TCP كبروتوكول التسجيل، فهذا يؤدي إلى قيام ASA بإرسال syslog عبر اتصال TCP إلى خادم syslog. إذا تعذر الوصول إلى الخادم، أو تعذر إنشاء اتصال TCP بالخادم، فيحظر ASA، بشكل افتراضي، جميع الاتصالات الجديدة. يمكن تعطيل هذا السلوك إذا قمت بتمكين إدخال تصريح التسجيل. راجع دليل التكوين للحصول على مزيد من المعلومات حول الأمر logging permit-hostdown.

ملاحظة: يسمح ال ASA فقط بالمنافذ التي تتراوح من 1025-65535. ينتج عن إستخدام أي منافذ أخرى هذا الخطأ:
ciscoASA(config)# logging host tftp 192.168.1.1 udp/516
تحذير: مستوى أمان واجهة Ethernet0/1 هو 0.
خطأ: المنفذ '516' ليس ضمن النطاق 1025-65535.

إرسال معلومات التسجيل كبريد إلكتروني

<#root>

```
logging mail
 severity_level
logging recipient-address
 email_address
logging from-address
 email_address
smtp-server
 ip_address
```

مداخ دوجو مزلي SMTP دنع لاسرإ لئاسر syslog في لئاسر البريد الإلكتروني. التكوين الصحيح على مداخ SMTP يرورض نامضل إمكانية ليحرت لئاسر البريد الإلكتروني نم ASA إلى ليمع البريد الإلكتروني المحدد حاجنب. إذا مت نييعت مستوى التسجيل اذه على مستوى ةعرس ريبك، لثم تصحيح الأخطاء أو المعلومات، فيمكنك إنشاء ددع ريبك نم syslog ارظن لأن لك ديرب إلكتروني متي لاسرإ ةطساوب نيوكت التسجيل اذه يتسبب في إنشاء ام لصي إلى أربعة تالجس إضافية أو أكثر.

إرسال معلومات التسجيل إلى وحدة التحكم التسلسلية

<#root>

```
logging console
 severity_level
```

يتيح ليجست وحدة التحكم لئاسر syslog التي متيس اهضرع على وحدة مكحت ASA (tty) دنع اهثودح. إذا مت نيوكت ليجست وحدة التحكم، فسيتم ديدحت عيمج تايلمع إنشاء السجل على ASA إلى 9800 تب في الثانية، وهي ةعرس وحدة التحكم التسلسلية ASA. اذهو دق يتسبب في إسقاط syslogs إلى كل الوجهات، والتي نمضتت نزخملا تقؤملا الداخلي. ال مدختست ليجست وحدة التحكم نقاط الوصول الظاهرية اذهل السبب.

إرسال معلومات التسجيل إلى جلسة لمع Telnet/SSH

<#root>

```
logging monitor
 severity_level
terminal monitor
```

التسجيل مدرب يمكن رسالة syslog أن يعرض بما أنها تحدث عندما تقوم بالوصول إلى وحدة terminal monitor والأمر SSH أو Telnet مع ASA تحكم. تم تنفيذ هذه من أن جلسة العمل. دخلت in order to منعت طباعة سجل إلى جلسة ك، المحطة الطرفية ما من مدرب أمر.

عرض رسائل السجل على ASDM

```
<#root>
logging asdm
 severity_level
```

يحتوي ASDM أيضا على مخزن مؤقت يمكن إستخدامه لتخزين رسائل syslog. أدخل الأمر show logging asdm لعرض محتوى المخزن المؤقت ل ASDM syslog.

إرسال السجلات إلى محطة إدارة SNMP

```
<#root>
logging history
 severity_level
snmp-server host
 [if_name] ip_addr
snmp-server location
 text
snmp-server contact
 text
snmp-server community
 key
snmp-server enable traps
```

يحتاج المستخدمون إلى بيئة بروتوكول إدارة الشبكة البسيط الوظيفي (SNMP) لإرسال رسائل syslog باستخدام SNMP. راجع أوامر الإعداد وإدارة وجهات المخرجات لمرجع كامل على الأوامر التي يمكنك إستخدامها لضبط وإدارة وجهات المخرجات. راجع الرسائل المدرجة حسب مستوى الخطورة للرسائل المدرجة حسب مستوى الخطورة.

إضافة الطوابع الزمنية إلى syslogs

للمساعدة في محاذاة الأحداث وترتيبها، يمكن إضافة الطوابع الزمنية إلى syslogs. يوصى

بذلك للمساعدة في تتبع المشكلات استنادا إلى الوقت. لتمكين الطوابع الزمنية، أدخل الأمر logging timestamp. فيما يلي مثالان ل syslog، أحدهما بدون الطابع الزمني والآخر مع:

```
%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to
 identity:172.18.124.136/161 duration 0:02:01 bytes 313

Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
 inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
 442 TCP Reset-I
```

مثال 1

يعرض هذا الإخراج نموذجا لتكوين تسجيل الدخول إلى المخزن المؤقت مع مستوى خطورة تصحيح الأخطاء.

```
<#root>

logging enable
logging buffered debugging
```

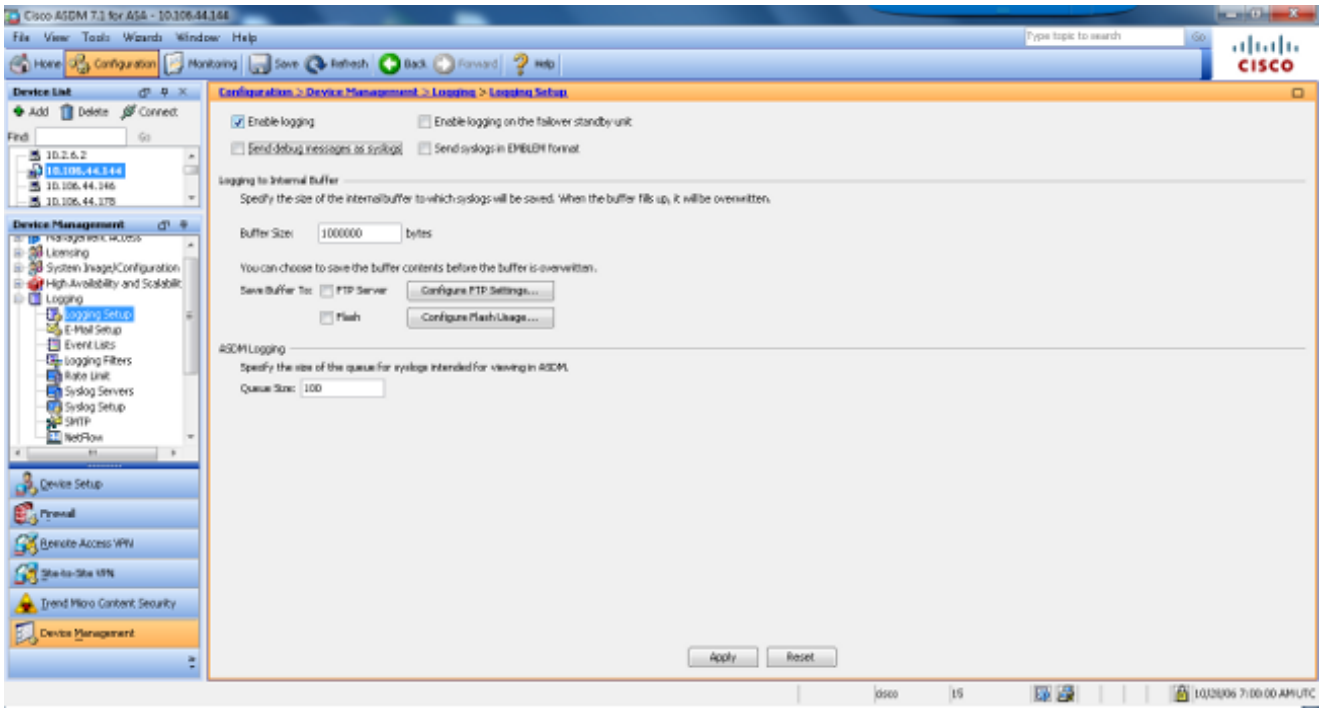
هذا نموذج للمخرجات.

```
%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

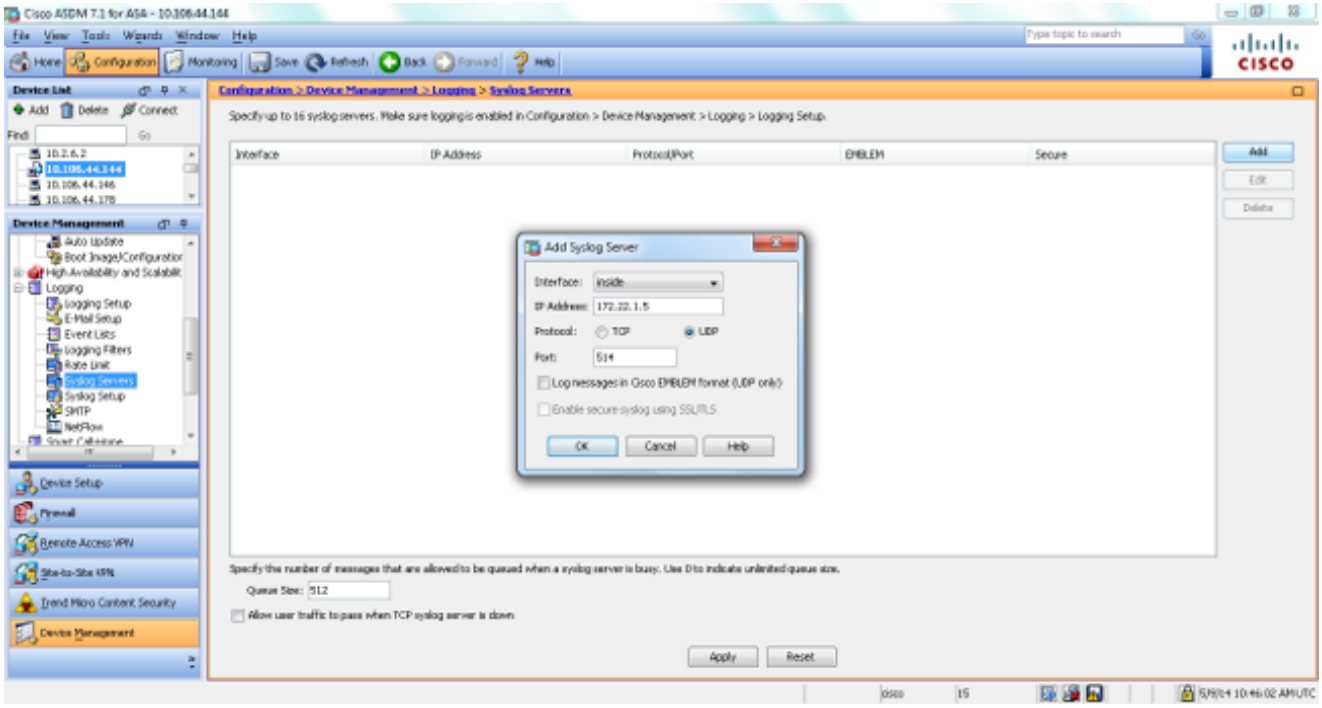
تكوين syslog الأساسي باستخدام ASDM

يوضح هذا الإجراء تكوين ASDM لجميع وجهات syslog المتاحة.

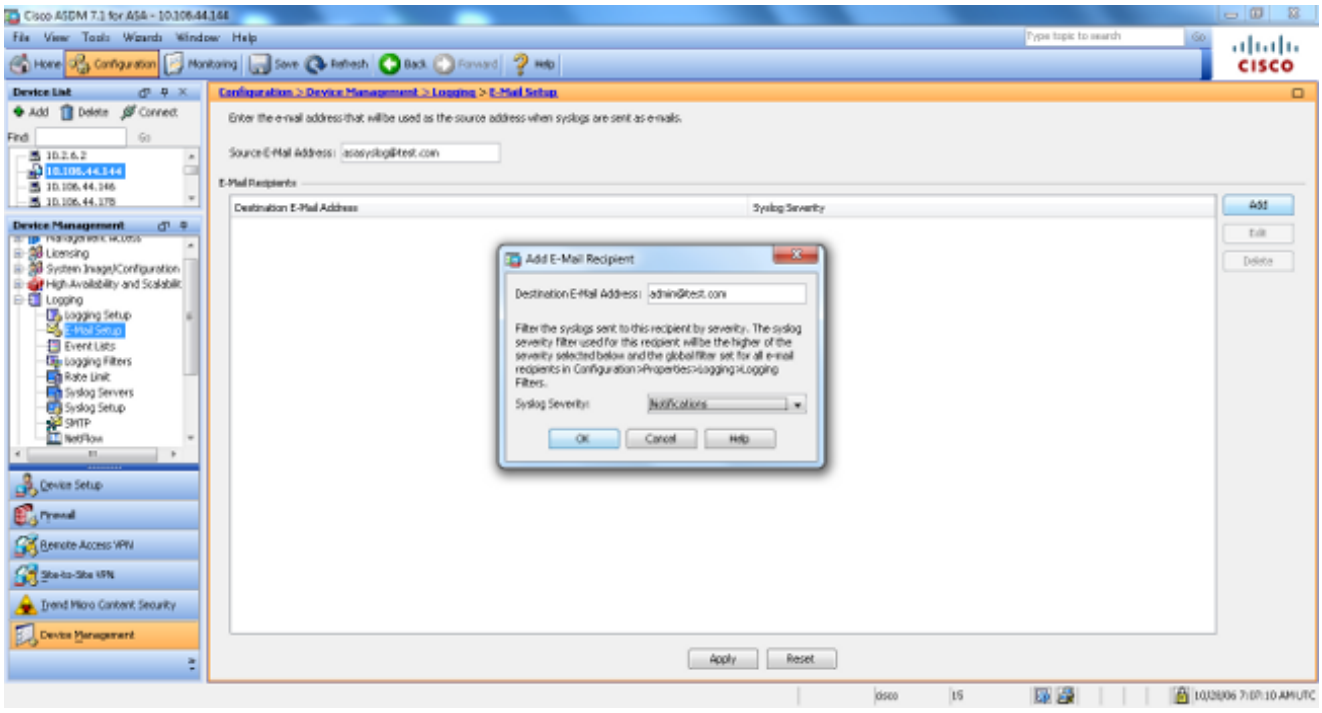
1. لتمكين تسجيل الدخول إلى ASA، قم أولا بتكوين معلمات التسجيل الأساسية. أختر التكوين > الميزات > الخصائص > التسجيل > إعداد التسجيل. حدد خانة الاختيار تمكين التسجيل لتمكين syslogs.



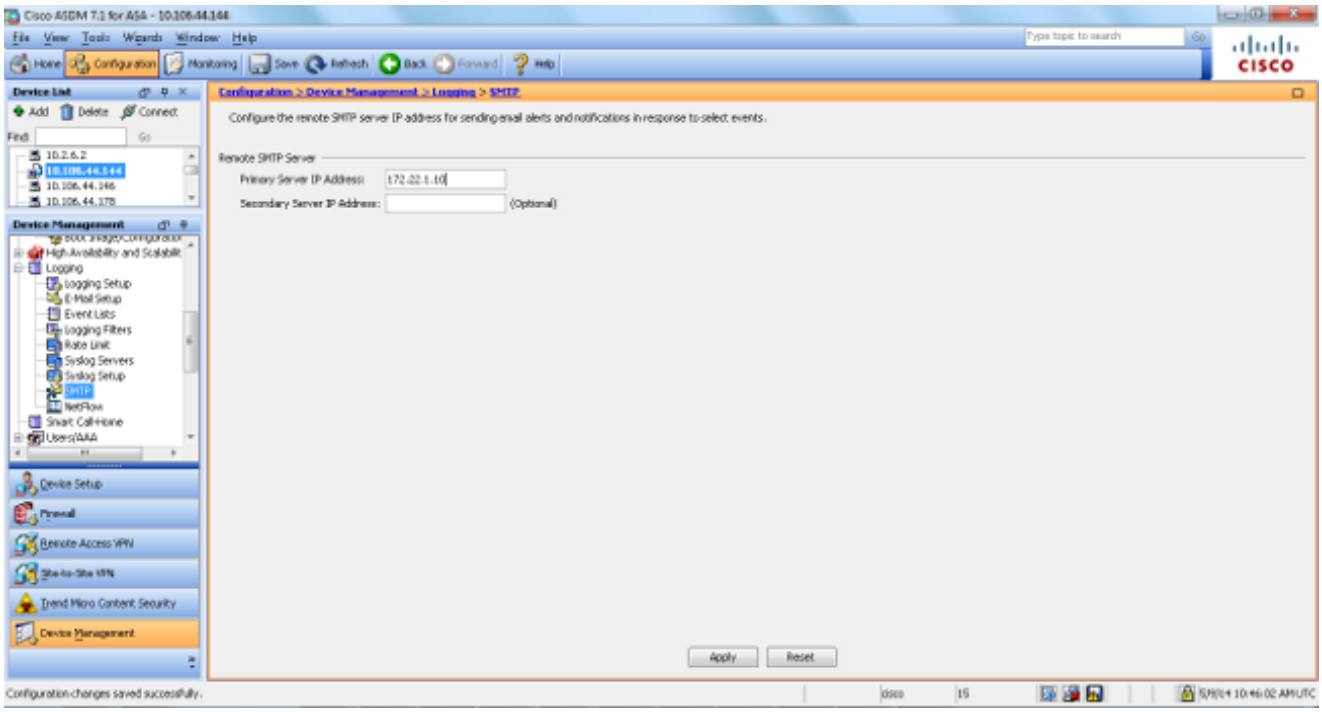
2. أخترت in order to شكلت نادل خارجي كغاية ل syslog، syslog نادل في تسجيل وطقطقة يضيف in order to أضفت syslog نادل. أدخل تفاصيل خادم syslog في المربع إضافة خادم syslog واختر موافق عند انتهائك.



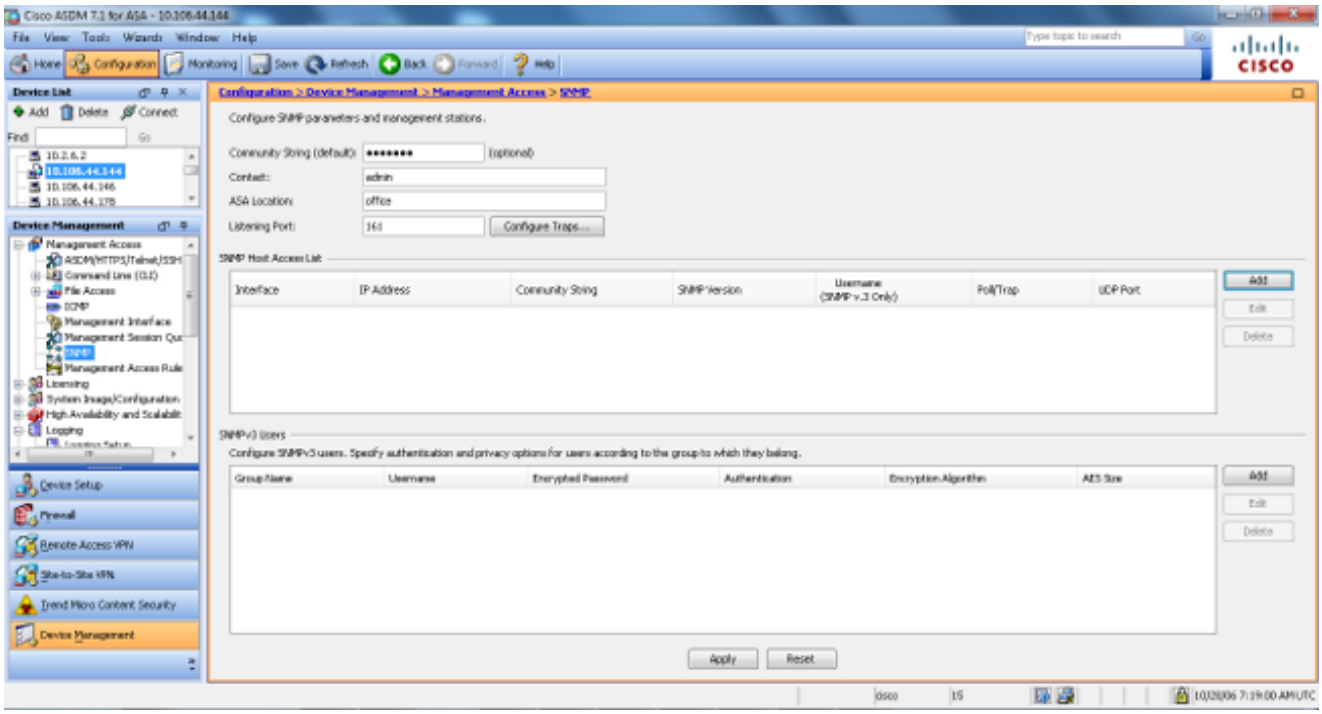
3. أختر إعداد البريد الإلكتروني في التسجيل لإرسال رسائل syslog كرسائل بريد إلكتروني إلى مستلمين معينين. حدد عنوان البريد الإلكتروني المصدر في مربع عنوان البريد الإلكتروني المصدر واختر إضافة لتكوين عنوان البريد الإلكتروني الوجهة لمستلمي البريد الإلكتروني ومستوى خطورة الرسالة. انقر فوق موافق عند الانتهاء.



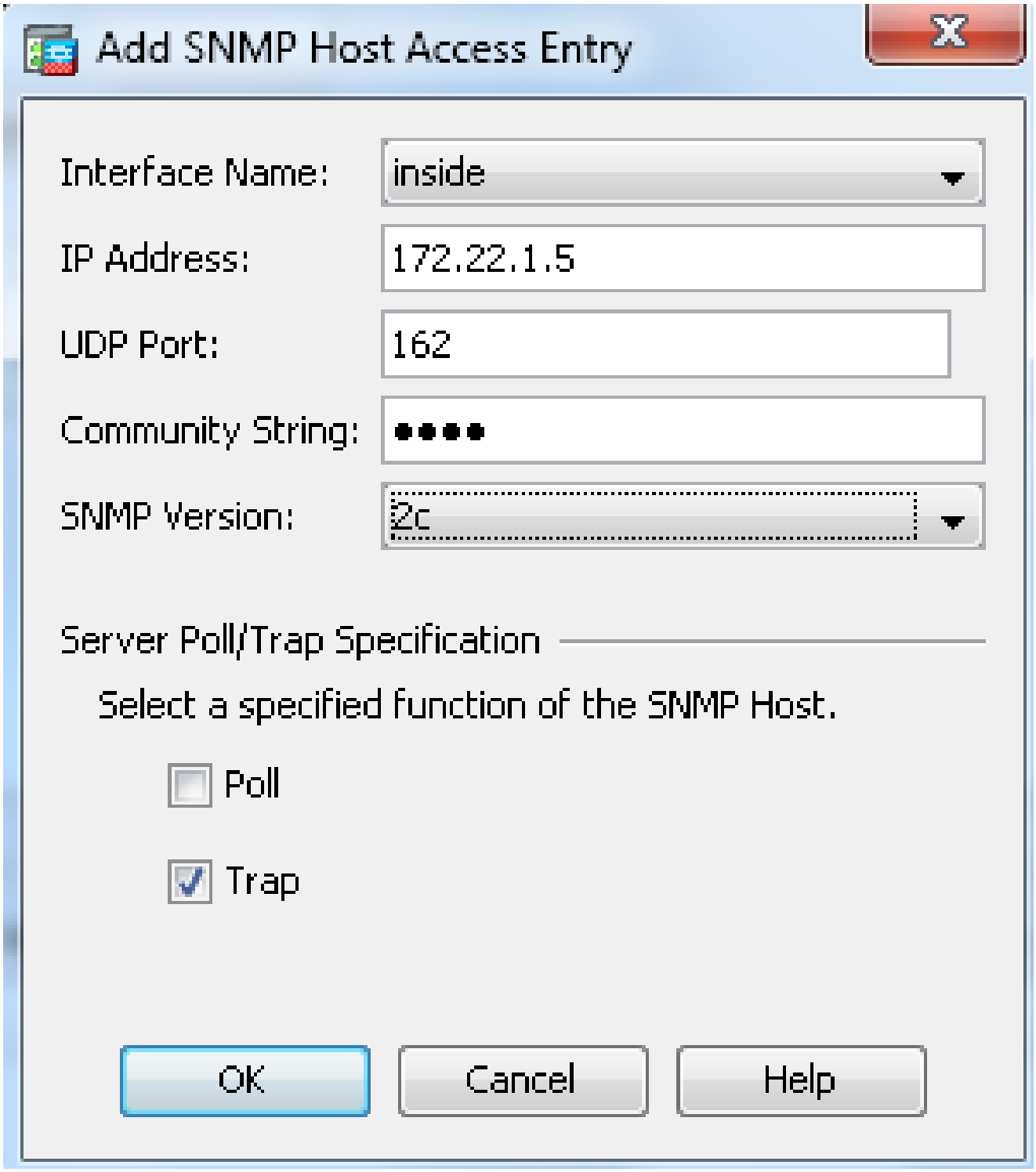
4. أخترت أداة إدارة، تسجيل، يختار SMTP، ويدخل الخادم أساسي عنوان in order to عينت ال SMTP نادل عنوان.



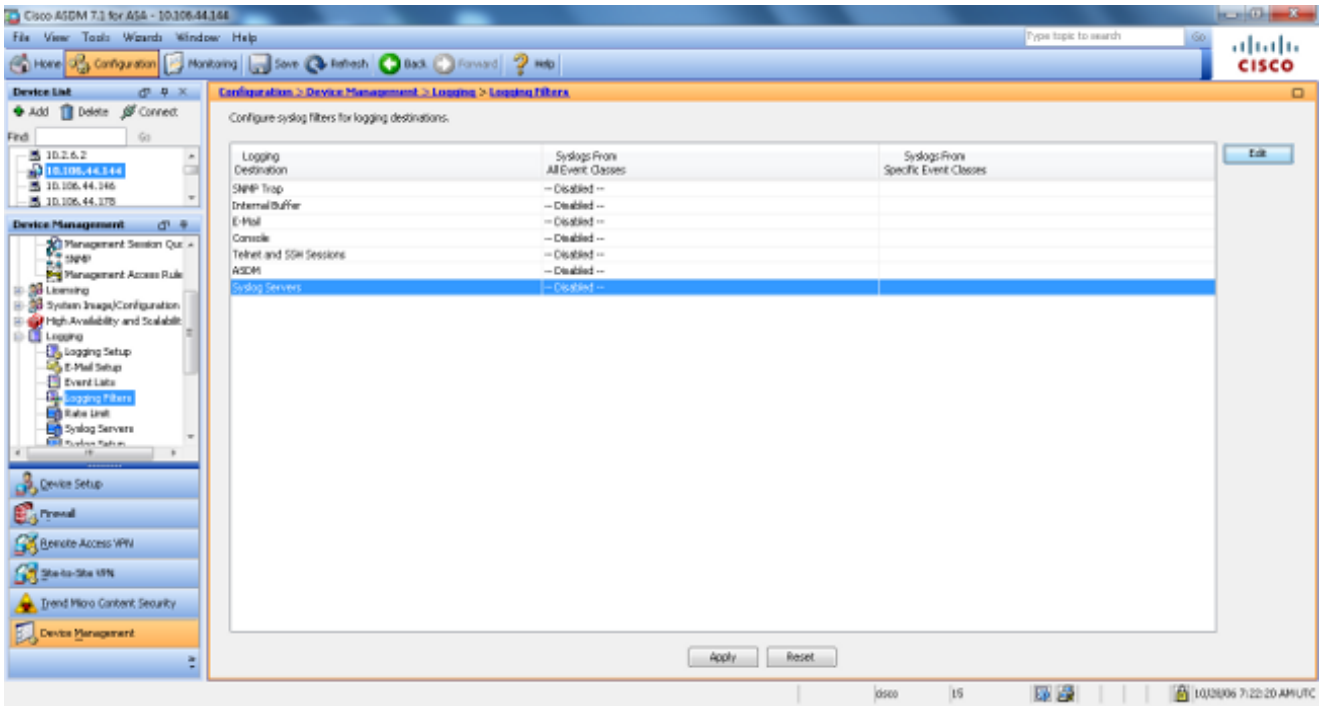
5. إذا كنت ترغب في إرسال syslogs كإختبارات SNMP، فيجب عليك أولا تحديد خادم SNMP. أختر SNMP في قائمة الوصول إلى الإدارة لتحديد عنوان محطات إدارة SNMP وخصائصها المحددة.



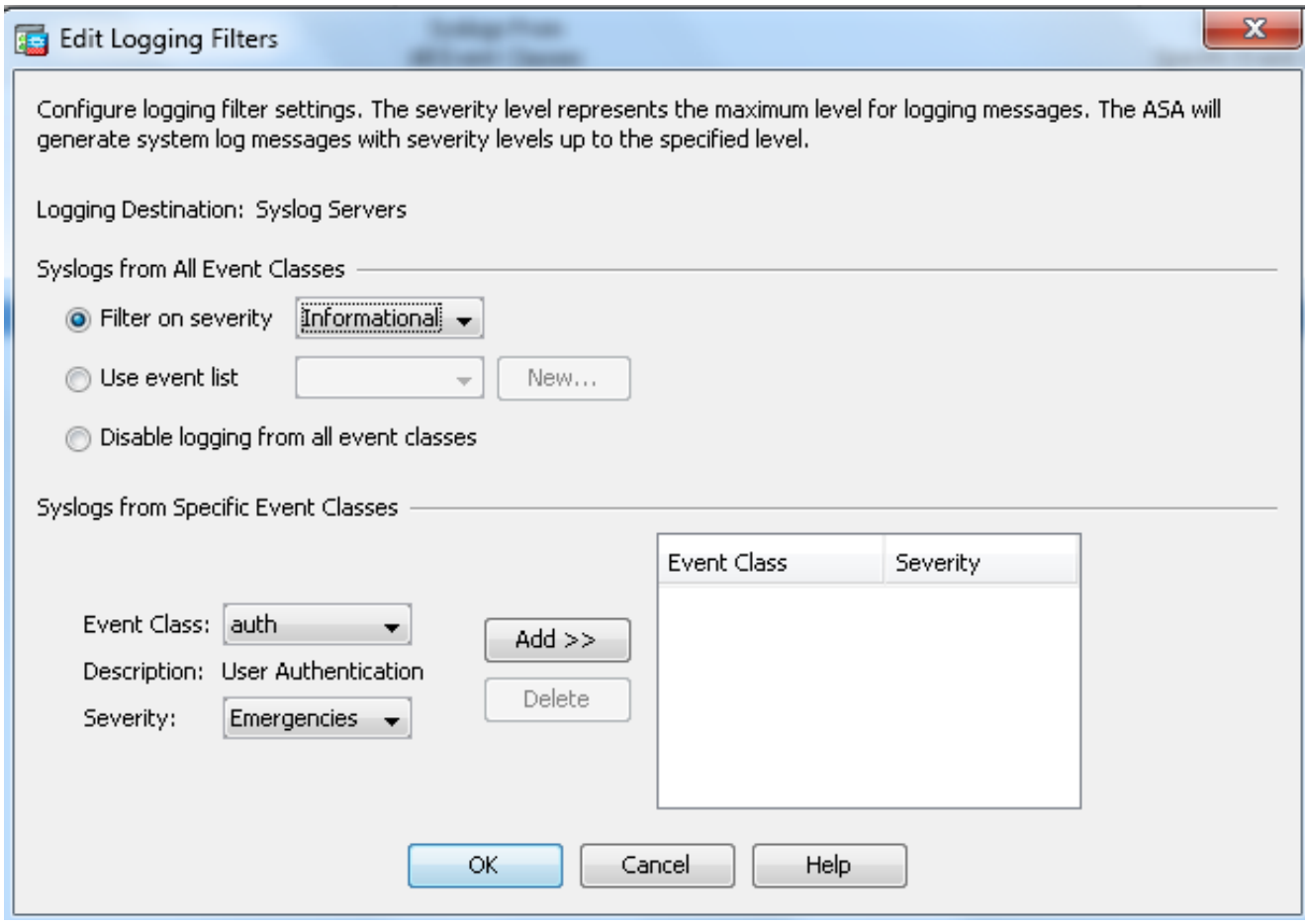
6. أختر إضافة لإضافة محطة إدارة SNMP. أدخل تفاصيل مضيف SNMP وانقر فوق موافق.



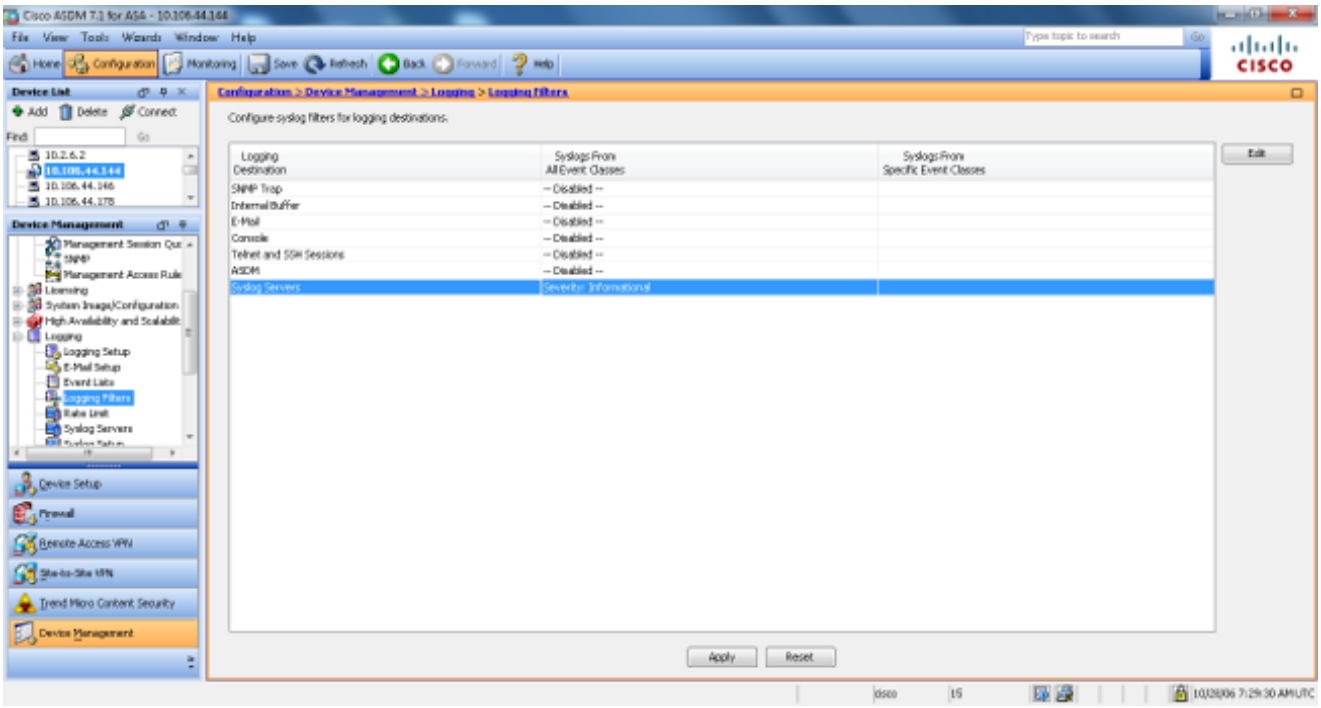
7. أخترت in order to مكنت سجل أن يكون أرسلت إلى أي من ال سابق غاية ذكر، يدون مرشح في التسجيل قسم. وهذا يقدم لك مع كل وجهة تسجيل ممكنة والمستوى الحالي من السجلات التي يتم إرسالها إلى هذه الوجهات. أختر وجهة التسجيل المطلوبة وانقر فوق تحرير. في هذا مثال، ال 'syslog دان' عدلت غاية.



8. أختر خطورة مناسبة، في هذه الحالة معلومات، من القائمة المنسدلة عامل التصفية على مستوى الخطورة. انقر فوق موافق عند الانتهاء.



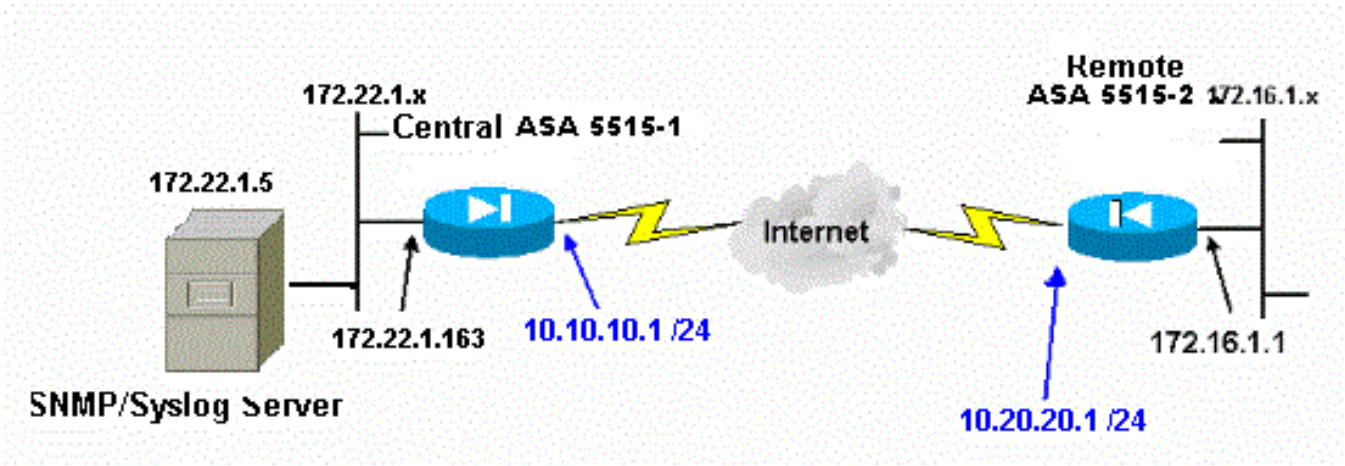
9. انقر فوق تطبيق بعد الرجوع إلى نافذة عوامل تصفية التسجيل.



أرسلت syslog رسالة عبر VPN إلى syslog نادل

في تصميم الشبكة الخاصة الظاهرية (VPN) البسيط من موقع إلى موقع أو التصميم الأكثر تعقيدا القائم على لوحة الوصل والمتكلم، قد يرغب المسؤول في مراقبة جميع جدران حماية ASA البعيدة باستخدام خادم SNMP وخادم syslog الموجود في موقع مركزي.

أحلت in order to شكلت ال IPsec VPN موقع إلى موقع، [PIX/ASA 7.x وأعلى: PIX-to-PIX VPN نفق تشكيل مثال](). بخلاف تكوين شبكة VPN، يجب تكوين بروتوكول SNMP وحركة مرور البيانات المثيرة للاهتمام لخادم syslog في كل من الموقع المركزي والمحلي.



تكوين ASA المركزي

<#root>

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
```

```
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0


!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514



logging enable
logging trap debugging

!--- Define logging host information.

logging facility 16
logging host inside 172.22.1.5


!--- Define the SNMP configuration.

snmp-server host inside 172.22.1.5 community ***** version 2c


snmp-server community *****
```

تكوين ASA البعيد

<#root>

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.

access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0


!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this ASA outside
!--- interface to the SYSLOG server.

access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
```

```
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514


!--- Define syslog server.

logging facility 23
logging host outside 172.22.1.5


!--- Define SNMP server.

snmp-server host outside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

ارجع إلى مراقبة جدار حماية Cisco Secure ASA باستخدام SNMP و Syslog من خلال نفق VPN للحصول على مزيد من المعلومات حول كيفية تكوين إصدار ASA 8.4

Syslog المتقدم

يوفر ASA الإصدار 8.4 العديد من الآليات التي تمكن من تكوين رسائل syslog وإدارتها في المجموعات. تتضمن هذه الآليات مستوى خطورة الرسالة أو فئة الرسالة أو معرف الرسالة أو قائمة رسائل مخصصة تقوم بإنشائها. باستخدام هذه الآليات، يمكنك إدخال أمر واحد يطبق عليه مجموعات صغيرة أو كبيرة من الرسائل. عند إعداد syslogs بهذه الطريقة، يمكنك التقاط الرسائل من مجموعة الرسائل المحددة ولم تعد جميع الرسائل من نفس الخطورة.

إستخدام قائمة الرسائل

أستخدم قائمة الرسائل لتضمين رسائل syslog المعنية فقط حسب مستوى الخطورة والمعرف في مجموعة، ثم أرباط قائمة الرسائل هذه بالوجهة المطلوبة.

أتمت هذا steps in order to شكلت رسالة قائمة:

1. أدخل message_list لقائمة التسجيل | أمر level severity_level [class message_class] لإنشاء قائمة رسائل تتضمن رسائل ذات مستوى خطورة محدد أو قائمة رسائل.
2. أدخل الأمر logging list message_list message syslog_id-syslog_id2 لإضافة رسائل إضافية إلى قائمة الرسائل التي تم إنشاؤها للتو.
3. أدخل الأمر logging destination message_list لتحديد وجهة قائمة الرسائل التي تم إنشاؤها.

مثال 2

أدخل هذه الأوامر لإنشاء قائمة رسائل، تتضمن جميع رسائل الخطورة 2 (الأهمة) مع إضافة الرسالة 61101 إلى 611323، ويتم إرسالها أيضا إلى وحدة التحكم:

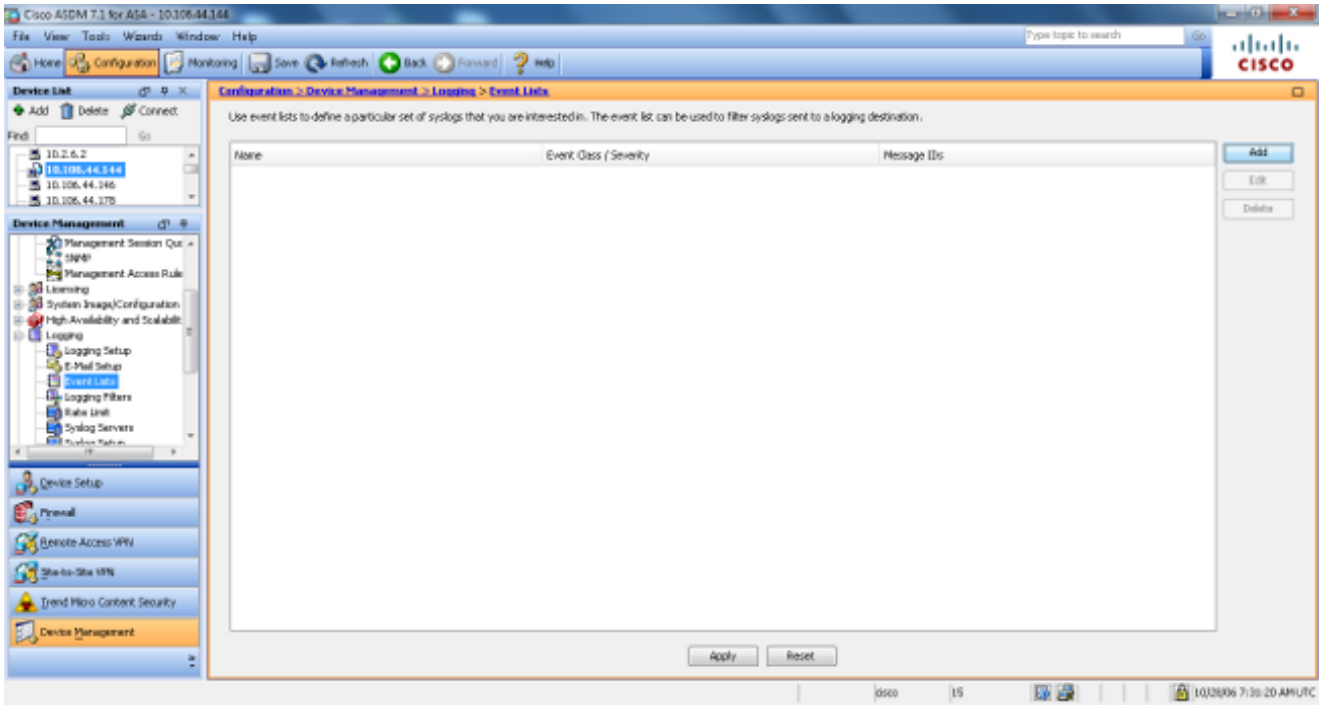
<#root>

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

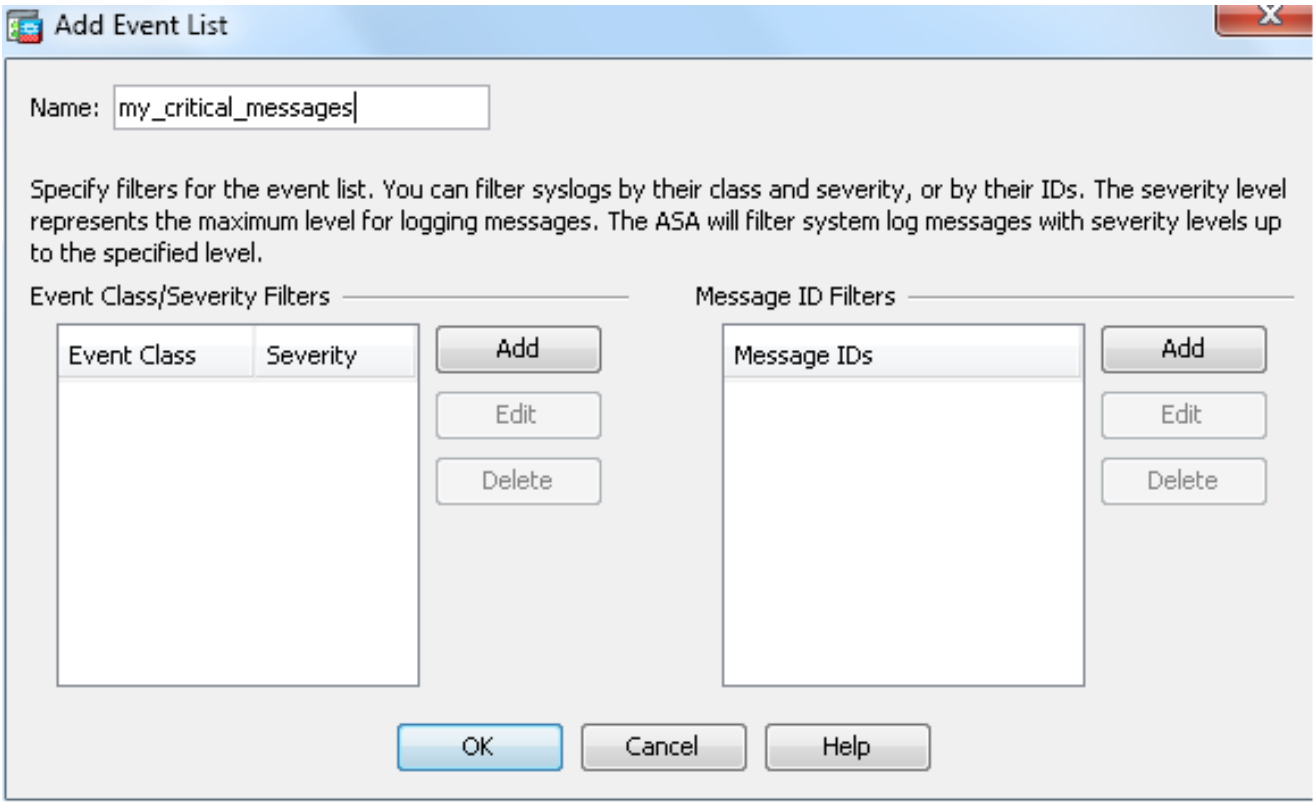
تكوين ASDM

يوضح هذا الإجراء تكوين ASDM على سبيل المثال 2 باستخدام قائمة الرسائل.

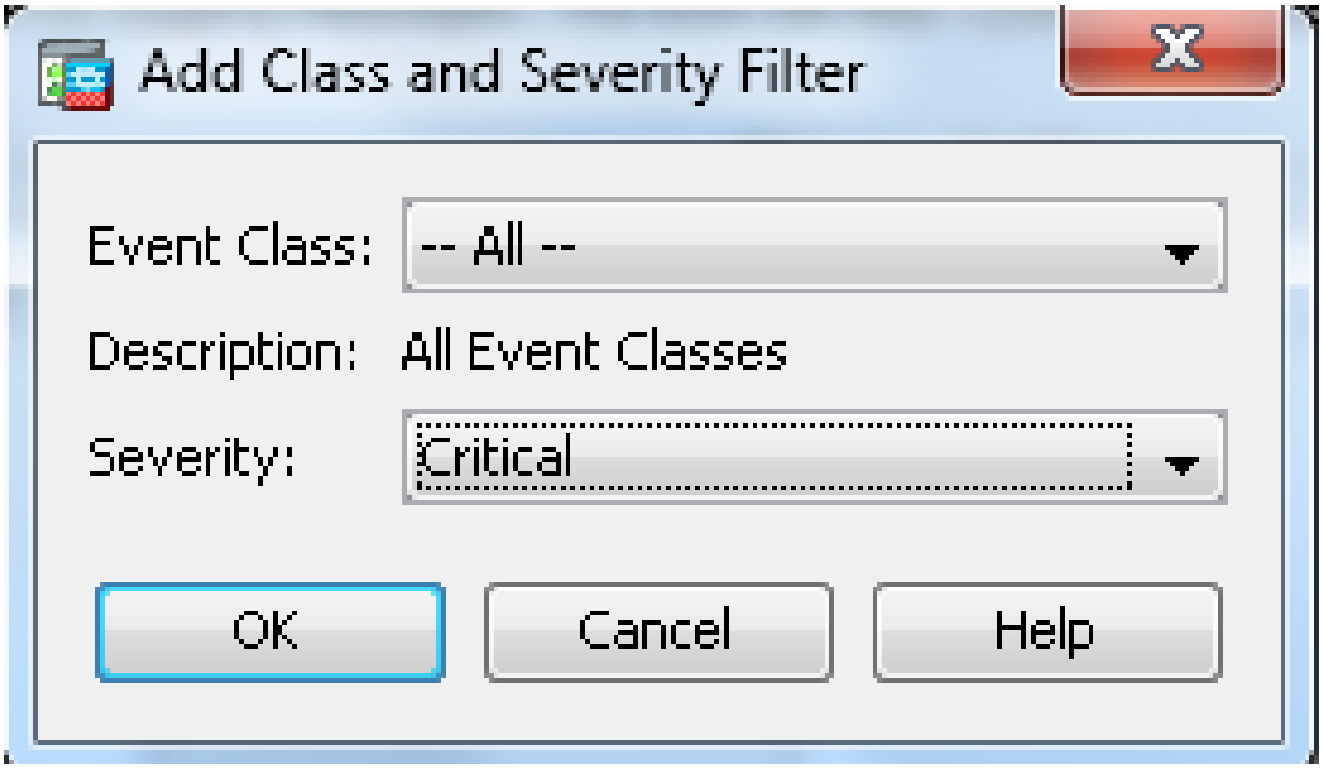
1. أختر قوائم الأحداث تحت التسجيل وانقر فوق إضافة لإنشاء قائمة رسائل.



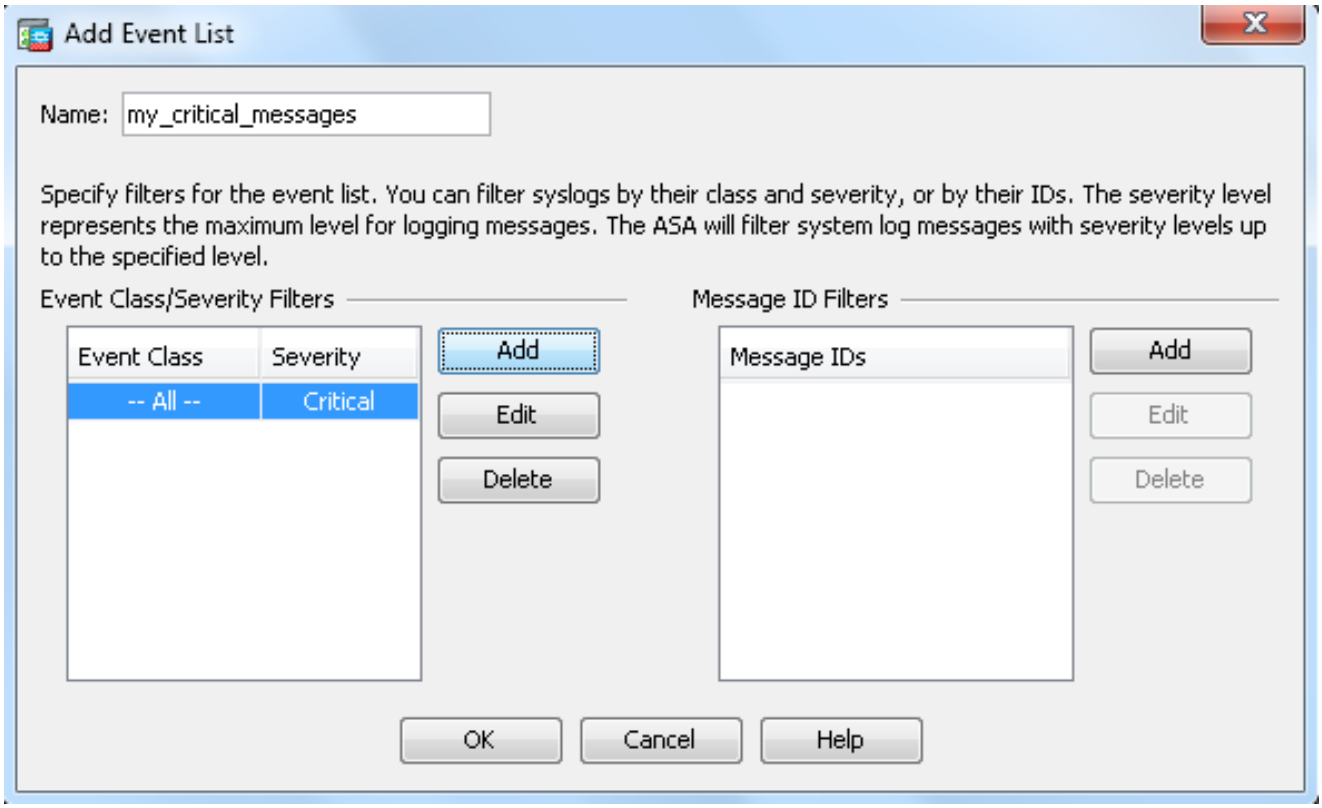
2. أدخل اسم قائمة الرسائل في مربع الاسم. في هذه الحالة يتم إستخدام my_critical_messages. انقر فوق إضافة ضمن عوامل تصفية فئة/خطورة الحدث.



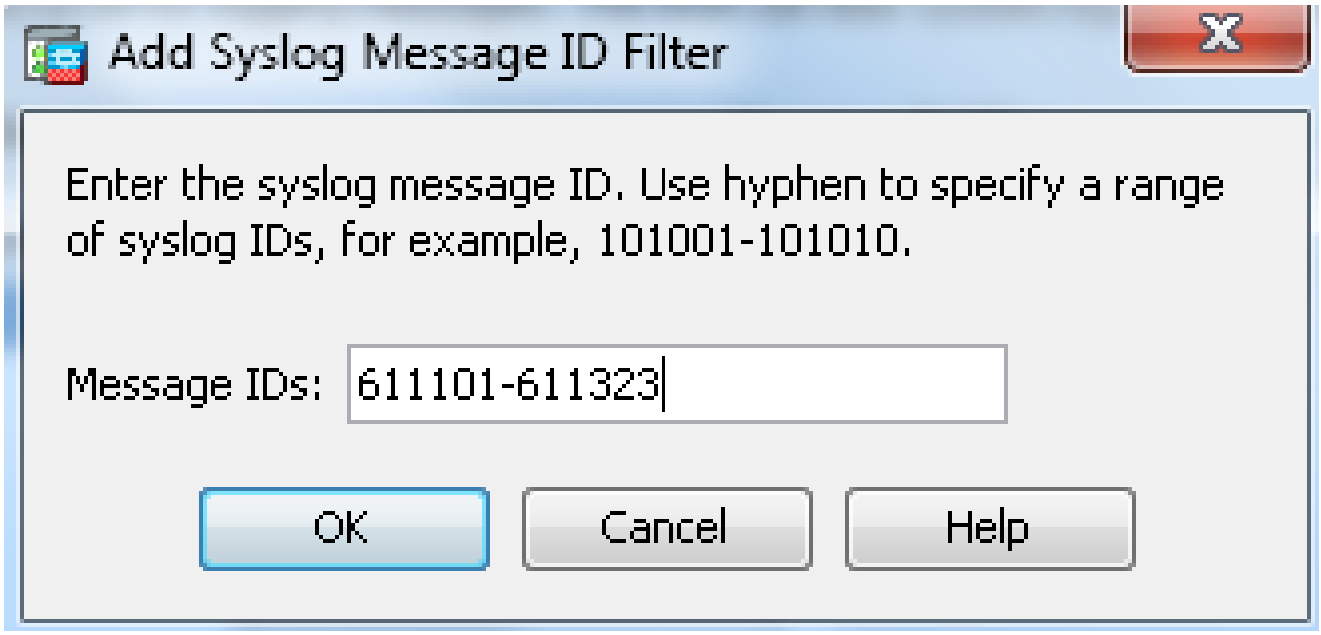
3. أختر الكل من القائمة المنسدلة لفئة الحدث. أختر اهم من القائمة المنسدلة للخطورة. انقر فوق موافق عند الانتهاء.



4. انقر فوق إضافة ضمن عوامل تصفية معرف الرسالة إذا كانت هناك حاجة إلى رسائل إضافية. في هذه الحالة، يلزمك وضع رسائل بمعرف 611101-611323.

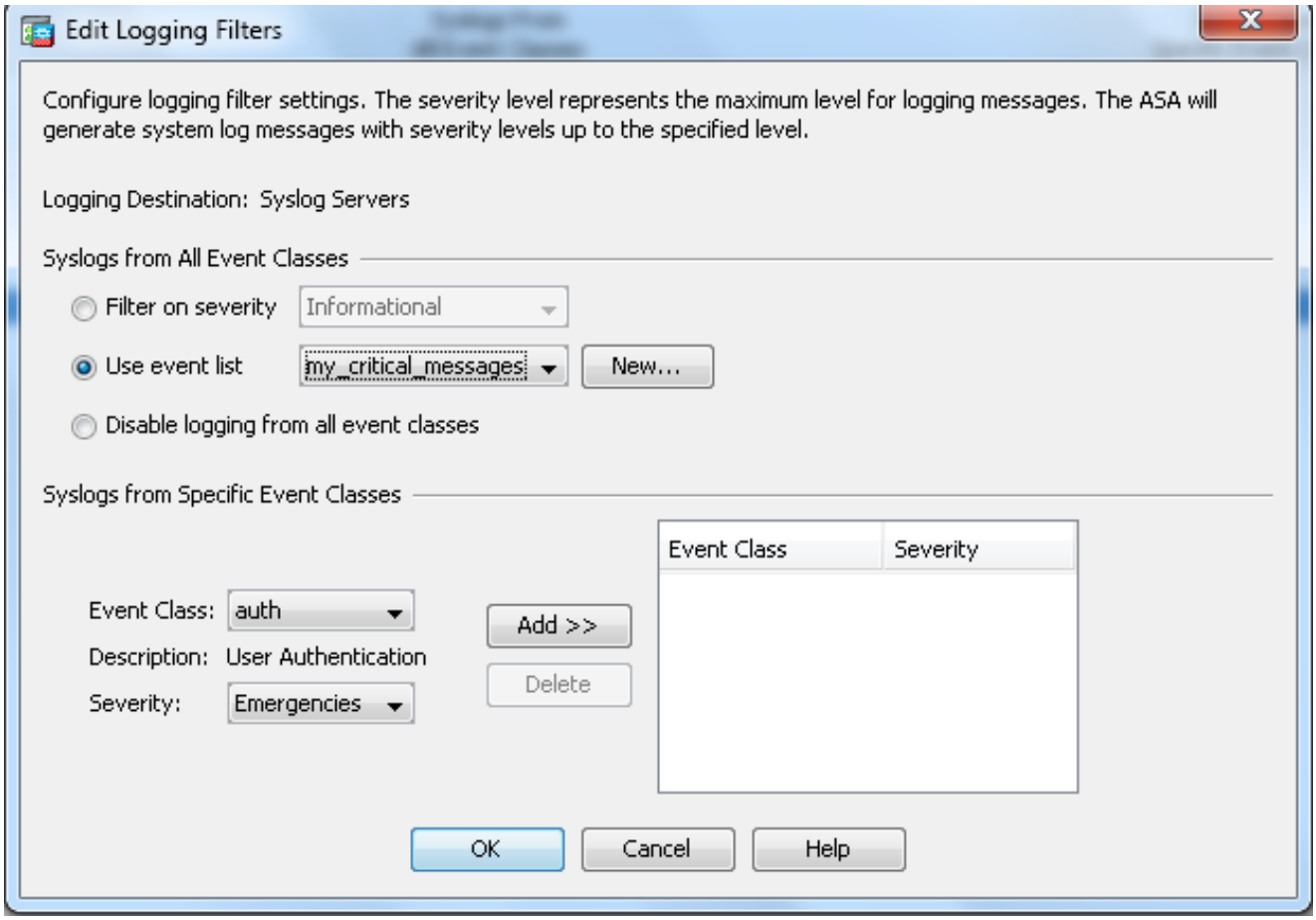


5. ضع في نطاق المعرفات في مربع معرفات الرسائل وانقر فوق موافق.

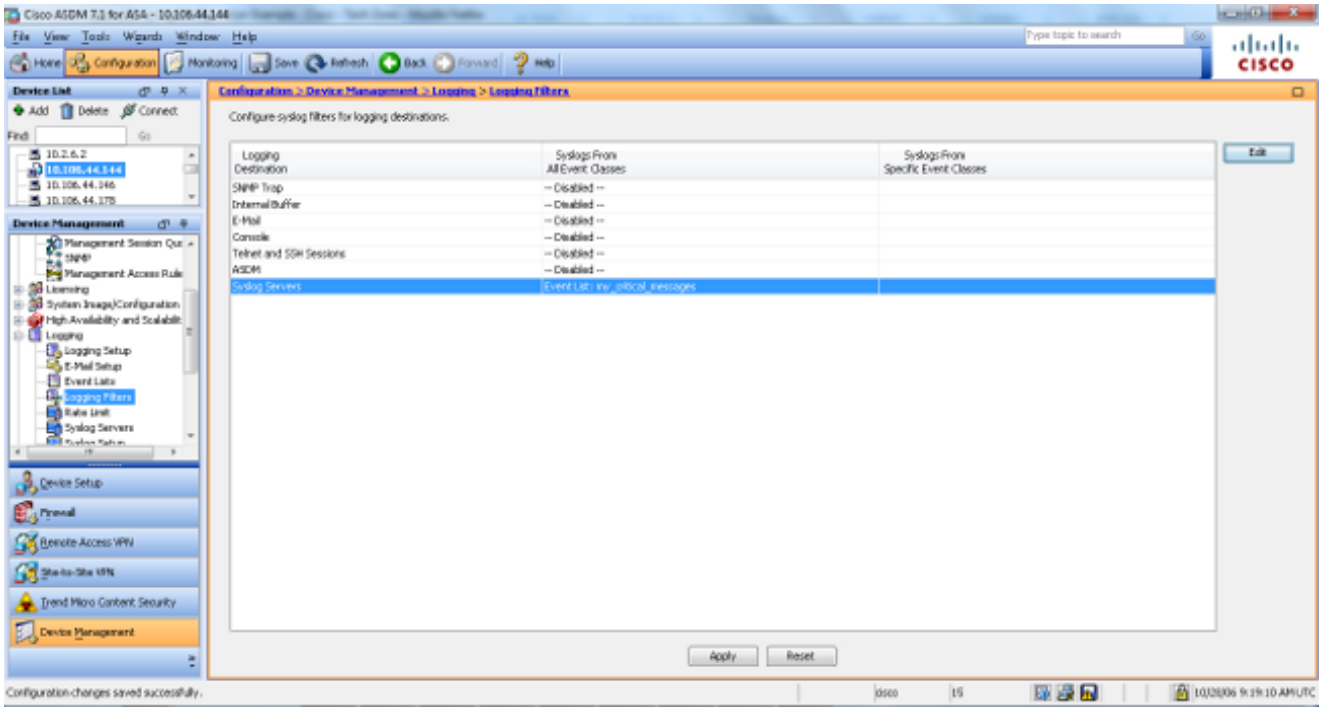


6. ارجع إلى القائمة عوامل تصفية التسجيل واختر وحدة التحكم كوجهة.

7. أختر my_critical_messages من القائمة المنسدلة إستخدام قائمة الأحداث. انقر فوق موافق عند الانتهاء.



8. انقر فوق تطبيق بعد الرجوع إلى نافذة عوامل تصفية التسجيل.



يؤدي هذا إلى اكتمال تكوينات ASDM باستخدام قائمة الرسائل كما هو موضح في المثال 2.

إستخدام فئة الرسالة

أستخدم فئة الرسالة لإرسال جميع الرسائل المرتبطة بفئة إلى موقع الإخراج المحدد. عند

تحديد حد مستوى خطورة ما، يمكنك تحديد عدد الرسائل المرسلة إلى موقع الإخراج.

```
<#root>

logging class

 message_class destination | severity_level
```

مثال 3

أدخل هذا الأمر لإرسال جميع رسائل فئة CA التي تحتوي على مستوى خطورة حالات الطوارئ أو أعلى إلى وحدة التحكم.

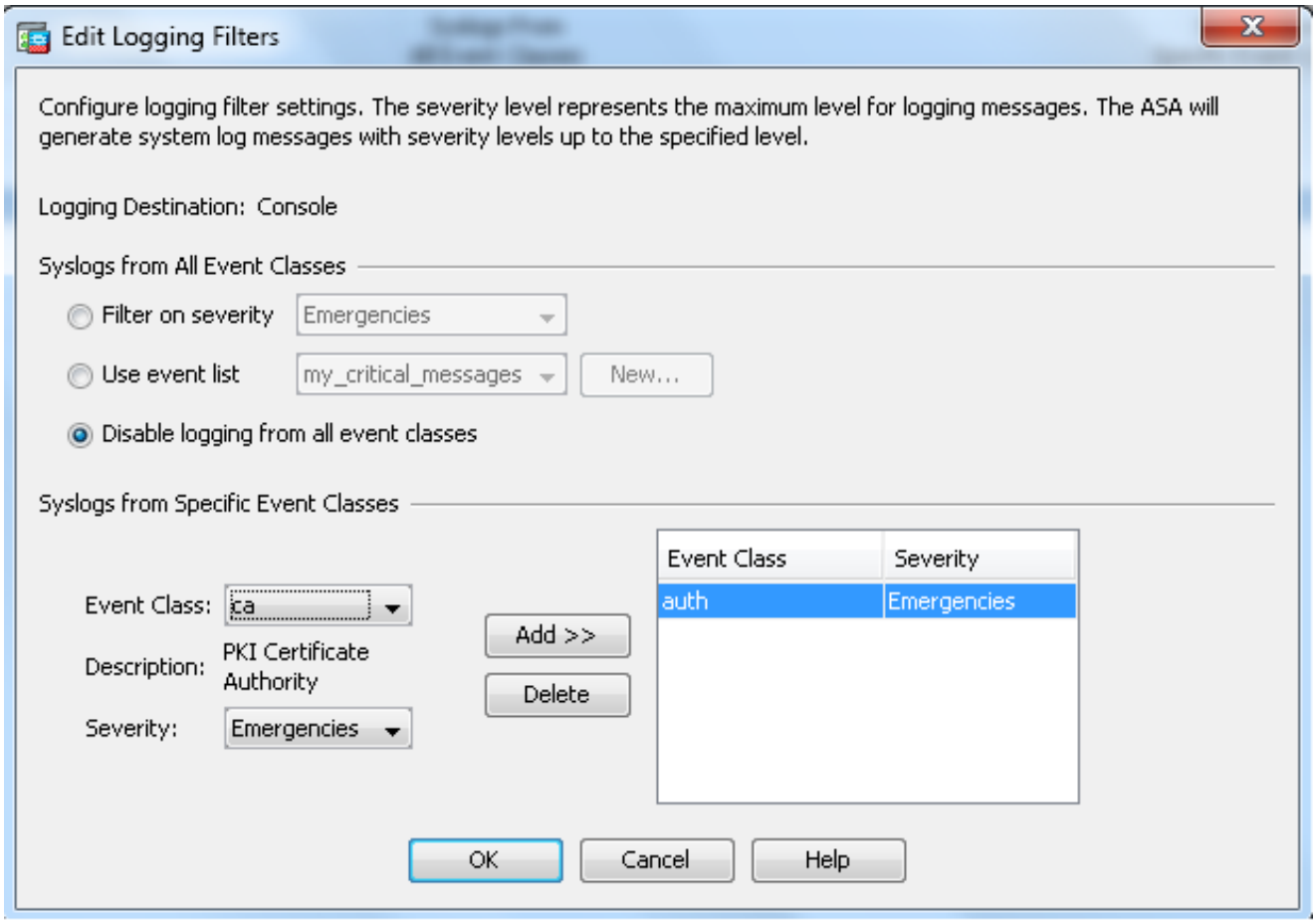
```
<#root>

logging class ca console emergencies
```

تكوين ASDM

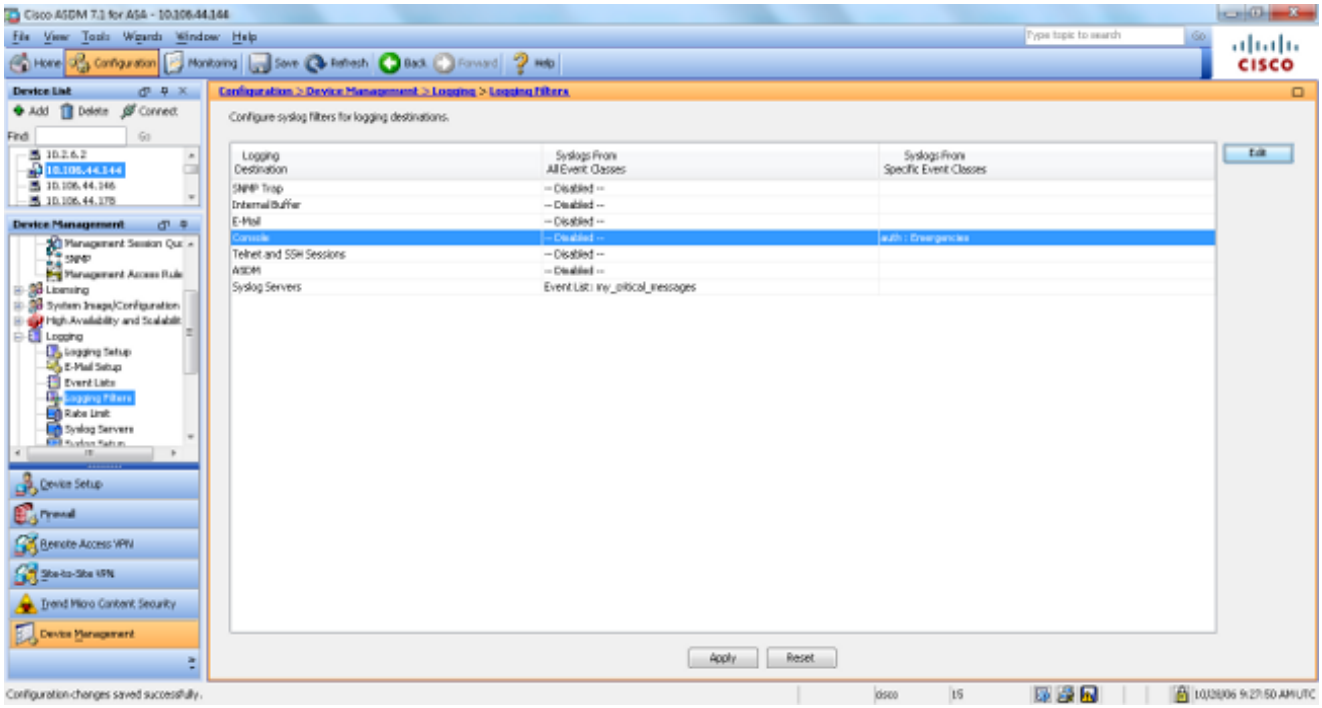
يوضح هذا الإجراء تكوينات ASDM على سبيل المثال 3 باستخدام قائمة الرسائل.

1. أختر قائمة عوامل تصفية التسجيل واختر وحدة التحكم كوجهة.
2. انقر فوق تعطيل التسجيل من جميع فئات الأحداث.
3. ضمن Syslogs من فئات أحداث محددة، أختر فئة الحدث ودرجة الخطورة التي تريد إضافتها.

   ويستخدم هذا الإجراء التوثيق والحالات الطارئة على التوالي.
4. طقطقة يضيف in order to أضف هذا إلى الرسالة صنف وطقطقة ok.



5. انقر فوق تطبيق بعد الرجوع إلى نافذة عوامل تصفية التسجيل. تقوم وحدة التحكم الآن بتجميع رسالة فئة CA ذات حالات الطوارئ من مستوى الخطورة كما هو موضح في نافذة عوامل تصفية التسجيل.



يؤدي هذا إلى اكتمال تكوين ASDM على سبيل المثال 3. ارجع إلى [الرسائل المدرجة حسب مستوى الخطورة](#) للحصول على قائمة بمستويات خطورة رسائل السجل.

إرسال رسائل سجل تصحيح الأخطاء إلى خادم syslog

السكشاف الأخطاء وإصلاحها بشكل متقدم، يلزم وجود سجلات تصحيح أخطاء خاصة بالميزة/البروتوكول. وبشكل افتراضي، يتم عرض رسائل السجل هذه على الوحدة الطرفية (SSH/Telnet). بناء على نوع تصحيح الأخطاء التي تم إنشاؤها، يمكن أن يكون إستخدام CLI صعبا إذا تم تمكين تصحيح الأخطاء. إختياريا، يمكن إعادة توجيه رسائل تصحيح الأخطاء إلى عملية syslog وتوليدها على هيئة syslogs. يمكن إرسال هذه syslog إلى أي عملية تحديد وضع ل syslog كما هو الحال مع أي syslog أخرى. دخلت in order to نقلت debugs إلى syslogs، ال logging debug-trace أمر. يرسل هذا تشكيل debug إنتاج، ك syslog، إلى syslog دان.

```
logging trap debugging
logging debug-trace
logging host inside 172.22.1.5
```

إستخدام فئات قائمة التسجيل والرسائل معا

دخلت ال logging list أمر in order to على قبض ال syslog ل lan-to-LAN واولوصول عن بعد IPsec VPN رسالة فقط. يلتقط هذا المثال جميع رسائل سجل النظام لفئة VPN (IKE و IPsec) باستخدام مستوى تصحيح الأخطاء أو أعلى.

مثال

<#root>

```
hostname(config)#
```

logging enable

```
hostname(config)#
```

logging timestamp

```
hostname(config)#
```

logging list my-list level debugging class vpn

```
hostname(config)#
```

logging trap my-list

```
hostname(config)#
```

logging host inside 192.168.1.1

تسجيل عمليات الوصول إلى قائمة التحكم في الوصول (ACL)

مق بإضافة سجل إلى كل عنصر من عناصر قائمة الوصول (ACE) الذي تريده للتسجيل عند الوصول إلى قائمة الوصول. أستخدم هذه الصياغة:

<#root>

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

مثال

<#root>

```
ASAfirewall(config)#
access-list 101 line 1 extended permit icmp any any log
```

توقم قوائم التحكم في الوصول (ACL)، بشكل افتراضي، بتسجيل كل حزمة مرفوضة. ال تحتاج إلى إضافة خيار السجل لرفض قوائم التحكم في الوصول لإنشاء syslog للحزم المرفوضة. عندما يتعين خيار السجل، فهو يحدد رسالة syslog 106100 لل ace أن يكون تطبق عليه. يتم إنشاء رسالة Syslog 106100 لكل السماح المطابق أو رفض تدفق ACE الذي يمر عبر جدار حماية ASA. تم تخزين تدفق المطابقة الأولى مؤقتا. تزيد التطابقات التالية عدد مرات الوصول المعروضة في الأمر show access-list. يكون سلوك تسجيل قائمة الوصول الافتراضي، والتي هي الكلمة الأساسية السجل غير محددة، هو أنه إذا تم رفض الحزمة، فسيتم إنشاء الرسالة 106023، وإذا تم السماح بالحزمة، فلن يتم إنشاء رسالة syslog.

يمكن تحديد مستوى syslog إختياري (0 - 7) لرسائل syslog التي تم إنشاؤها (106100). في حال عدم تحديد أي مستوى، يكون المستوى الافتراضي هو 6 (إعلامي) لأداة تحكم في الوصول (ACE) جديدة. إذا كان ACE موجودا بالفعل، فسيظل مستوى السجل الحالي الخاص به دون تغيير. في حالة تحديد خيار تعطيل السجل، يتم تعطيل تسجيل قائمة الوصول بالكامل. لم يتم إنشاء رسالة syslog، والتي تتضمن الرسالة 106023. يستعيد الخيار السجل الافتراضي سلوك تسجيل قائمة الوصول الافتراضية.

أتمت هذا steps in order to تمكن ال syslog رسالة 106100 أن يشاهد في الوحدة طرفية للتحكم إنتاج:

1. أدخل الأمر logging enable لتمكين إرسال رسائل سجل النظام إلى جميع مواقع الإخراج. يجب تعيين موقع إخراج لتسجيل عرض أي سجلات.

2. أدخل الأمر logging message <message_number> level <severity_level> لتعيين مستوى خطورة رسالة سجل نظام معينة.

   في هذه الحالة، أدخل الأمر logging message 106100 لتمكين الرسالة 106100.

3. أدخل ال logging console message_list | أمر severity_level لتمكين رسائل سجل النظام

للعرض على وحدة تحكم جهاز الأمان (tty) عند حدوثها. قم بتعيين severity_level من 1 إلى 7 أو أستخدم اسم المستوى. يمكنك أيضا تحديد الرسائل التي يتم إرسالها مع متغير message_list.

4. أدخل الأمر show logging message لعرض قائمة برسائل سجل النظام التي تم تعديلها لمستوى خطورة مختلف من الإعداد الافتراضي، وهي الرسائل التي تم تعيينها والرسائل التي تم تعطيلها.

   هذا نموذج إخراج من الأمر show logging message:

```
<#root>

ASAfirewall#

show logging message 106100


syslog 106100: default-level informational (enabled)
ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

حظر إنشاء syslog على ASA في وضع الاستعداد

ابدأ من برنامج ASA الإصدار 9.4.1 وما بعده يمكنك حظر إنشاء syslog معينة على وحدة إحتياطية واستخدام هذا الأمر:

```
no logging message syslog-id standby
```

التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

إذا كنت ترغب في منع رسالة syslog معينة ليتم إرسالها إلى خادم syslog، فيجب عليك إدخال الأمر كما هو موضح.

```
<#root>

hostname(config)#

no logging message

 <syslog_id>
```

راجع الأمر logging message للحصول على مزيد من المعلومات.

%ASA-3-20108: عدم السماح بالاتصالات الجديدة

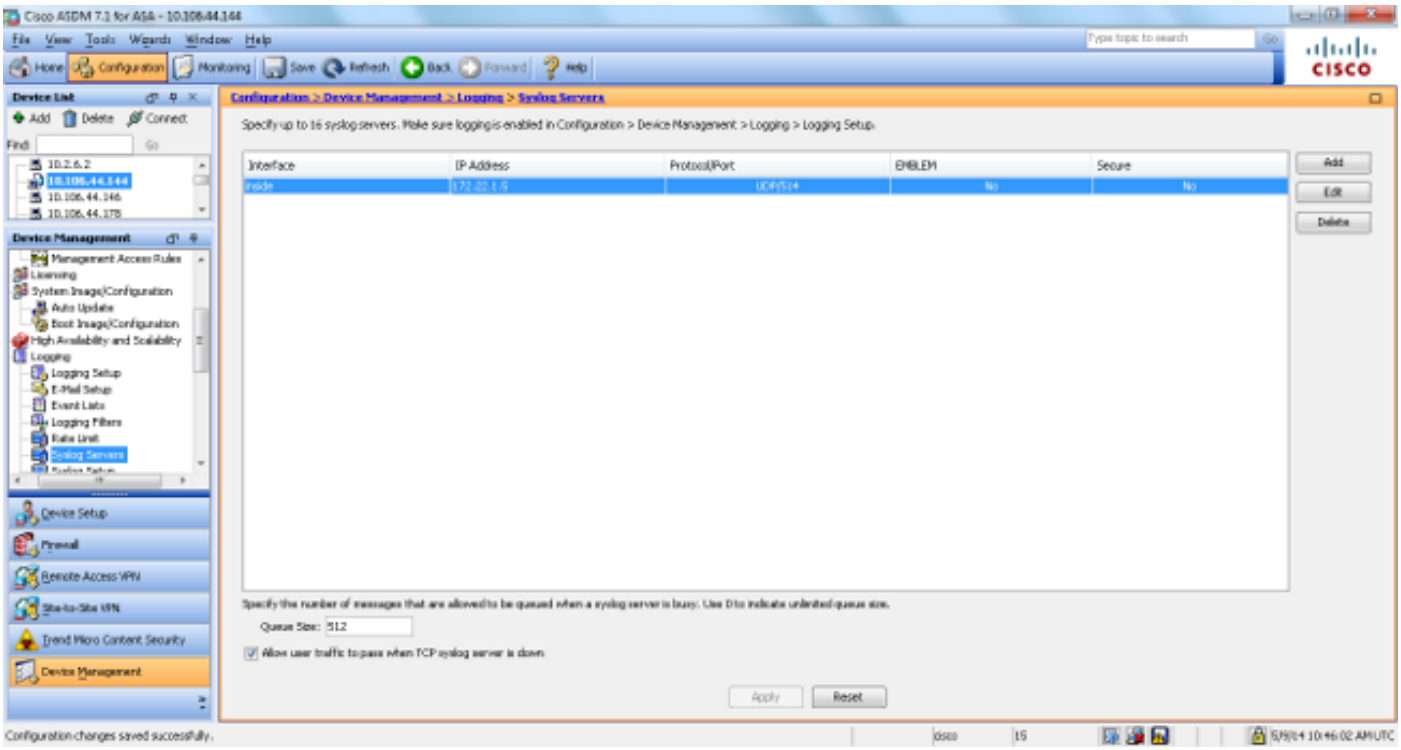
الـ %ASA-3-201008: رفض إتصالات جديدة. تظهر رسالة خطأ عندما يكون ASA غير قادر على الاتصال بخادم syslog والـ يسمح بأي إتصالات جديدة.

الحل

تظهر هذه الرسالة عند تمكين مراسلة سجل نظام TCP ويتعذر الوصول إلى خادم syslog، أو عند إستخدام خادم Cisco ASA Syslog (PFSS) والقرص الموجود على نظام Windows NT ممتلئ. أتمت هذا steps in order to حللت هذا خطأ رسالة:

- قم بتعطيل مراسلة سجل نظام TCP في حالة تمكينها.
- إذا كنت تستخدم ملفات PFSS، فقم بتحرير مساحة على نظام Windows NT حيث توجد ملفات PFSS.
- ضمنت أن الـ syslog نادل يكون فوق وأنت يستطيع أزيز المضيف من الـ cisco ASA وحدة طرفية للتحكم.
- قم بإعادة تشغيل تسجيل دخول رسائل نظام TCP للسماح بحركة المرور.

إذا تم إسقاط خادم syslog وتم تكوين تسجيل TCP، فإما أن تستخدم الأمر logging permit-hostdown أو المحول إلى تسجيل UDP.



معلومات ذات صلة

- مراجع أوامر جدار حماية PIX الآمن من Cisco

- طلبات التعليقات (RFCs)
- 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).