Configurazione del syslog di Adaptive Security Appliance (ASA)

Sommario

Introduzione

In questo documento viene descritto un esempio di configurazione che mostra come configurare diverse opzioni di registrazione su un'appliance ASA con codice versione 8.4 o successive.

Premesse

ASA versione 8.4 ha introdotto tecniche di filtraggio molto granulari per permettere di presentare solo alcuni messaggi syslog specifici. La sezione Syslog di base di questo documento mostra una configurazione syslog tradizionale. La sezione Advanced Syslog di questo documento mostra le nuove funzioni del syslog nella versione 8.4. Per la guida completa ai messaggi del log di sistema, consultare la guida ai messaggi del log di sistema di Cisco Security Appliance.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA 5515 con software ASA versione 8.4
- Cisco Adaptive Security Device Manager (ASDM) versione 7.1.6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nota: per ulteriori informazioni sulla configurazione di ASDM con versione 7.1 e successive, consultare il documento ASA 8.2: Configure Syslog using ASDM.

Syslog base

Immettere questi comandi per abilitare la registrazione, visualizzare i log e visualizzare le impostazioni di configurazione.

- logging enable - Abilita la trasmissione dei messaggi syslog in tutti i percorsi di output.
- no logging enable: disattiva la registrazione in tutti i percorsi di output.
- show logging: visualizza il contenuto del buffer syslog e le informazioni e le statistiche relative alla configurazione corrente.

L'ASA può inviare messaggi syslog a diverse destinazioni. Immettere i comandi nelle sezioni seguenti per specificare le posizioni in cui si desidera inviare le informazioni di syslog:

Invia informazioni di registrazione al buffer interno

<#root>

logging buffered

 severity_level

Quando si memorizzano i messaggi syslog nel buffer interno dell'ASA, non è necessario disporre di software o hardware esterni. Immettere il comando show logging per visualizzare i messaggi syslog archiviati. Il buffer interno ha una dimensione massima di 1 MB (configurabile con il comando logging buffer-size). Di conseguenza, può andare a capo molto rapidamente. Tenere presente questo aspetto quando si sceglie un livello di log per il buffer interno, in quanto livelli di log più dettagliati possono riempire e mandare a capo rapidamente il buffer interno.

Invia informazioni di registrazione a un server Syslog

<#root>

logging host

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

logging trap

 severity_level

logging facility

 number

Per inviare messaggi syslog a un host esterno, è necessario un server che esegue un'applicazione syslog. Per impostazione predefinita, ASA invia syslog sulla porta UDP 514, ma è possibile scegliere tra protocollo e porta. Se si sceglie TCP come protocollo di log, l'ASA invierà i syslog al server syslog tramite una connessione TCP. Se il server non è accessibile o non è possibile stabilire la connessione TCP con il server, per impostazione predefinita l'ASA blocca TUTTE le nuove connessioni. Questo comportamento può essere disabilitato se si abilita la registrazione di allow-hostdown. Per ulteriori informazioni sul comando logging allow-hostdown, consultare la guida alla configurazione.

Nota: l'appliance ASA può essere abilitata solo sulle porte con intervallo 1025-65535. L'uso di qualsiasi altra porta genera questo errore:
cisco(config)# logging host tftp 192.168.1.1 udp/516
AVVISO: il livello di sicurezza dell'interfaccia Ethernet 0/1 è 0.

ERRORE: la porta '516' non è compresa nell'intervallo 1025-65535.

Invia informazioni di registrazione come messaggi di posta elettronica

<#root>

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

Quando si inviano i messaggi syslog nei messaggi di posta elettronica, è necessario un server SMTP. Per essere certi di poter inoltrare correttamente i messaggi dall'ASA al client di posta elettronica specificato, è necessario configurare correttamente il server SMTP. Se questo livello di registrazione è impostato su un livello molto dettagliato, ad esempio debug o informativo, è possibile generare un numero significativo di syslog poiché ogni messaggio di posta elettronica inviato da questa configurazione di registrazione determina la generazione di quattro o più log aggiuntivi.

Invio delle informazioni di registrazione alla console seriale

<#root>

```
logging console
 severity_level
```

La registrazione della console consente la visualizzazione dei messaggi syslog sulla console ASA (tty) non appena vengono visualizzati. Se è stata configurata la registrazione sulla console, tutta la generazione del registro sull'appliance ASA è limitata a 9800 bps, ossia alla velocità della console seriale ASA. In questo modo, i syslog possono essere eliminati in tutte le destinazioni, incluso il buffer interno. Non utilizzare la registrazione da console per syslog dettagliati per questo motivo.

Invio di informazioni di registrazione a una sessione Telnet/SSH

<#root>

```
logging monitor
 severity_level
terminal monitor
```

Il monitor di log consente di visualizzare i messaggi syslog man mano che si verificano quando si accede alla console ASA con Telnet o SSH e il comando terminal monitor viene eseguito da quella sessione. Per interrompere la stampa dei log nella sessione, immettere il comando terminal no monitor.

Visualizzazione dei messaggi di log su ASDM

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

ASDM ha anche un buffer che può essere usato per memorizzare i messaggi syslog. Immettere il comando show logging asdm per visualizzare il contenuto del buffer syslog di ASDM.

Invio di registri a una stazione di gestione 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
```

Per inviare messaggi syslog con SNMP, gli utenti devono disporre di un ambiente SNMP (Simple Network Management Protocol) funzionale esistente. Per un riferimento completo sui comandi che

è possibile utilizzare per impostare e gestire le destinazioni di output, vedere Comandi per l'impostazione e la gestione delle destinazioni di output. Per i messaggi elencati per livello di gravità, vedere Messaggi elencati per livello di gravità.

Aggiungi timestamp ai syslog

Per facilitare l'allineamento e l'ordinamento degli eventi, è possibile aggiungere timestamp ai syslog. Questa opzione è consigliata per consentire la traccia dei problemi in base al tempo. Per abilitare i timestamp, immettere il comando logging timestamp. Di seguito sono riportati due esempi di syslog, uno senza timestamp e uno con:

```
%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
```

Esempio 1

Questo output mostra una configurazione di esempio per l'accesso al buffer con il livello di gravità del debug.

<#root>

```
logging enable
logging buffered debugging
```

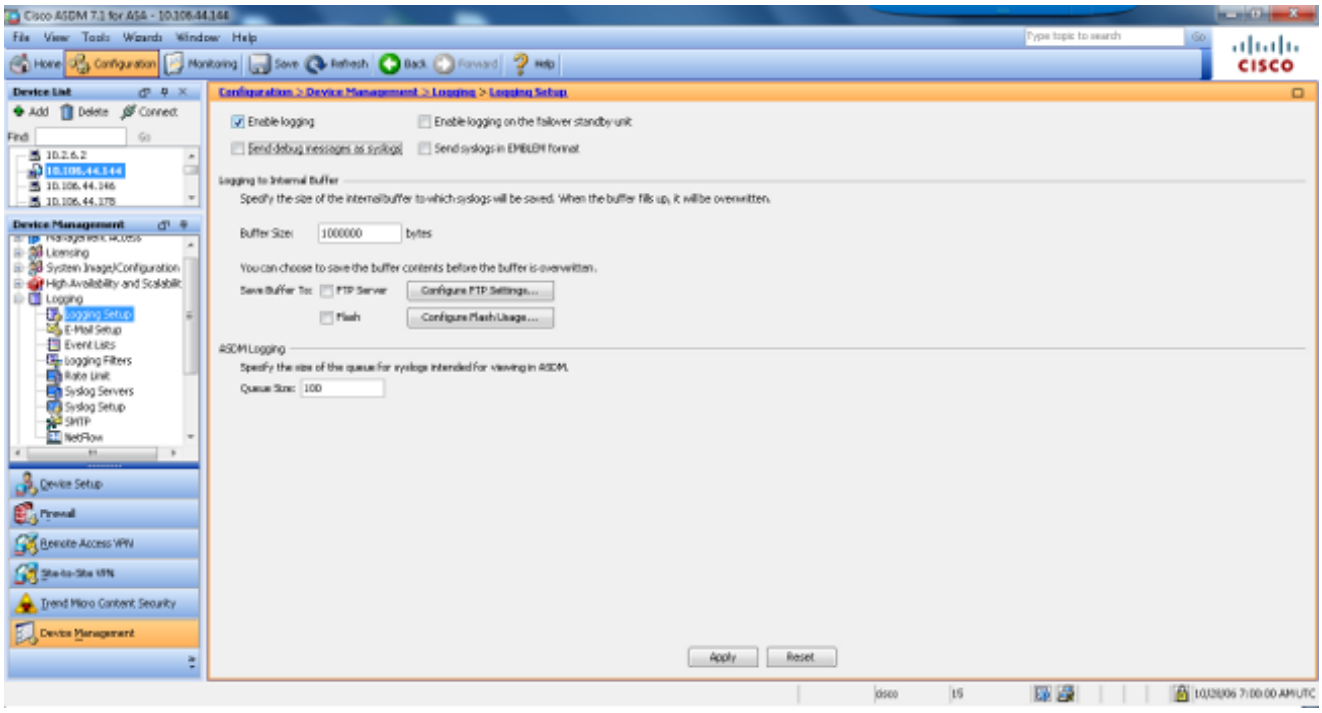
Questo è l'output di esempio.

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

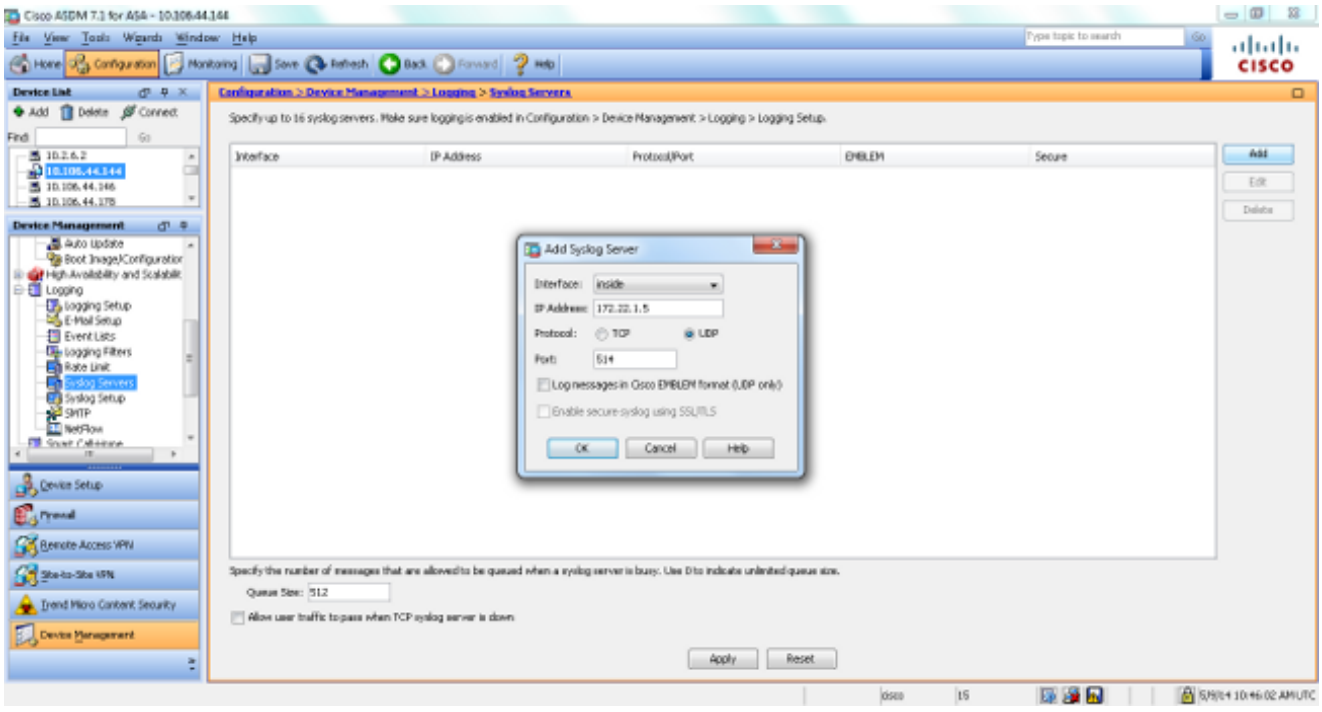
Configurazione del syslog di base con ASDM

In questa procedura viene mostrata la configurazione ASDM per tutte le destinazioni syslog disponibili.

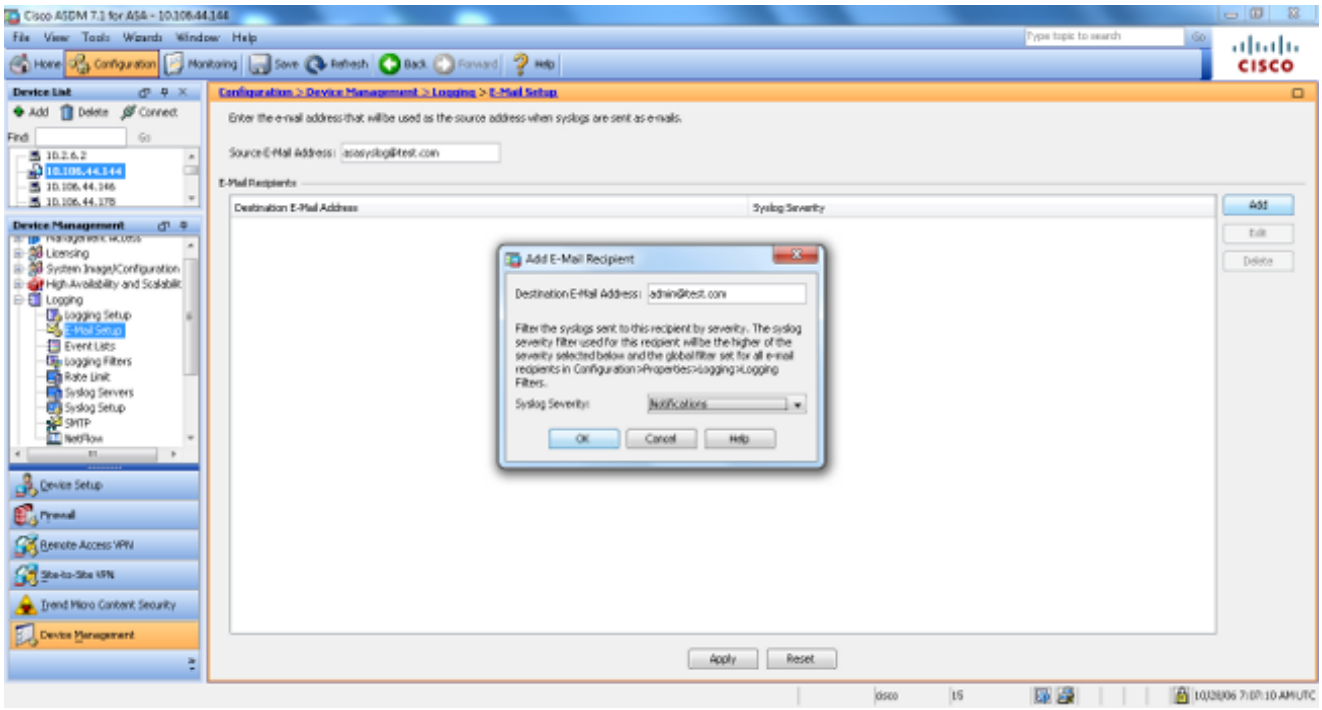
1. Per abilitare la registrazione sull'appliance ASA, configurare prima i parametri di registrazione di base. Scegliete Configurazione > Funzionalità > Proprietà > Registrazione > Impostazione registrazione. Per abilitare i syslog, selezionare la casella di controllo Abilita log.



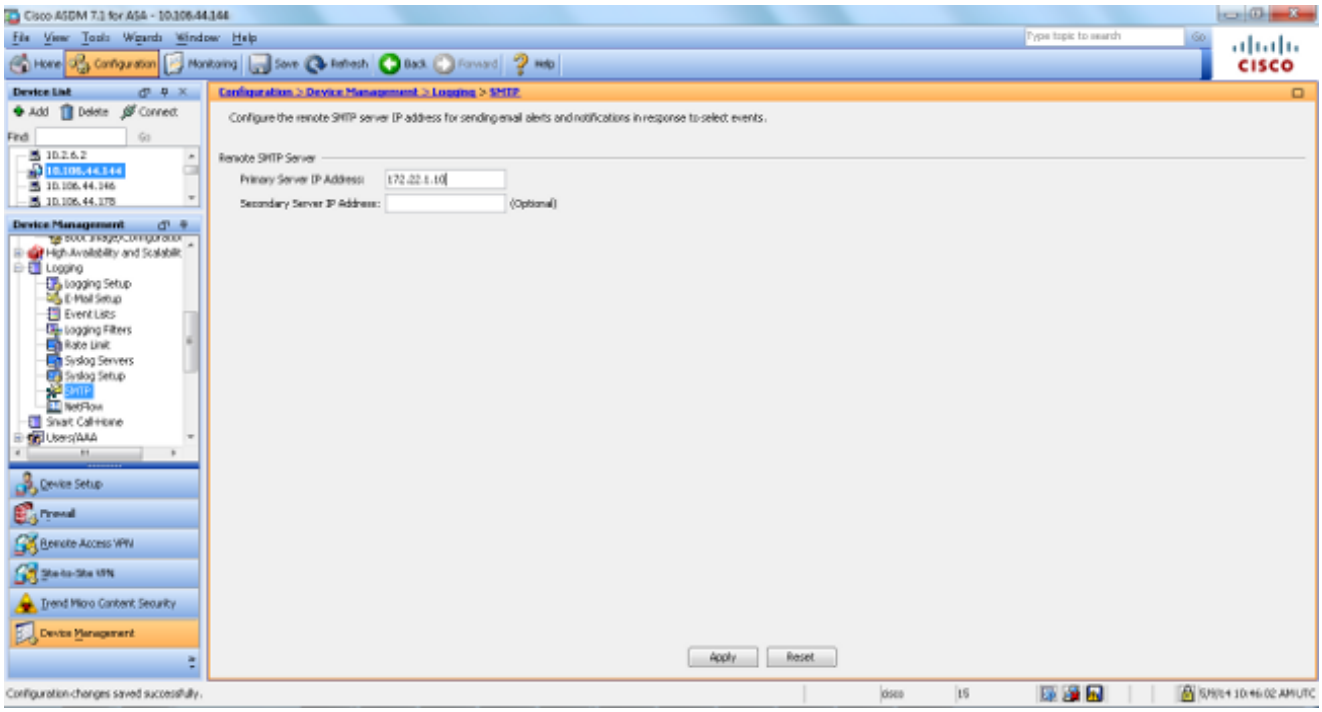
2. Per configurare un server esterno come destinazione per i syslog, scegliere Syslog Server in Log e fare clic su Aggiungi per aggiungere un server syslog. Immettere i dettagli del server syslog nella casella Add Syslog Server (Aggiungi server syslog) e al termine scegliere OK.



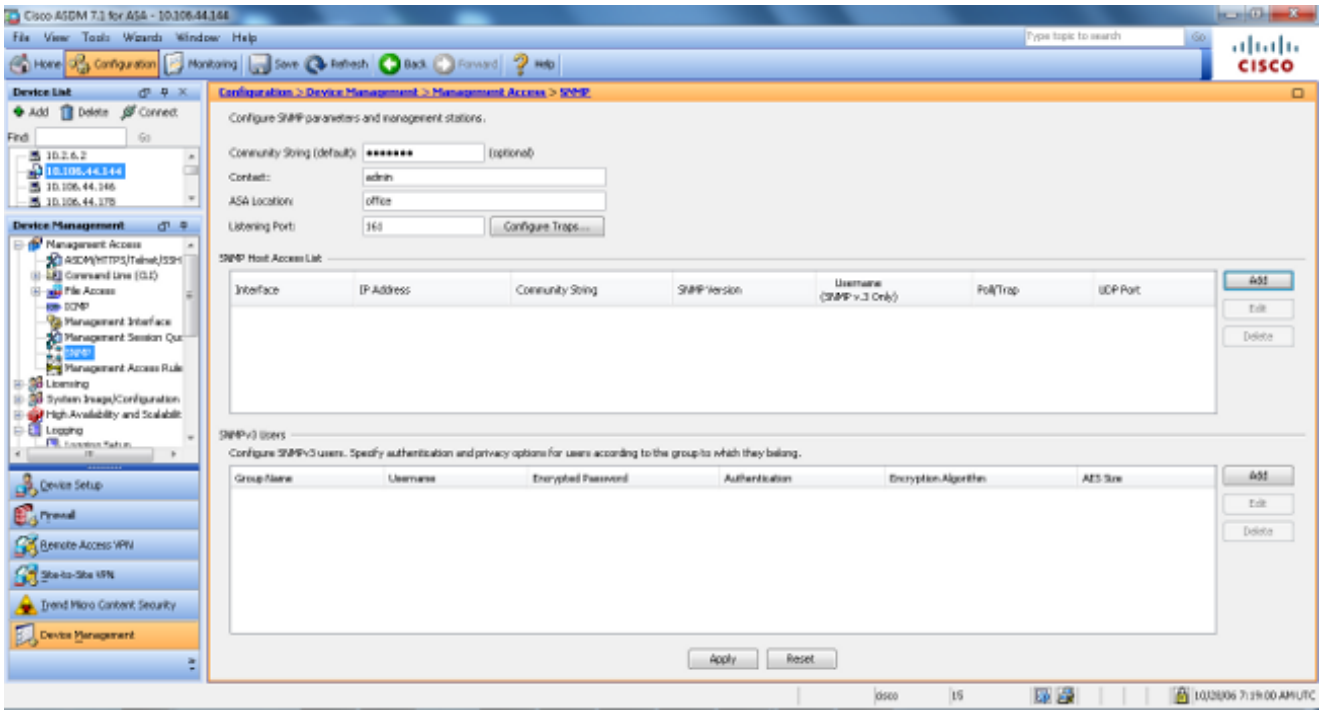
3. Scegliere Configurazione posta elettronica in Registrazione per inviare messaggi syslog come messaggi di posta elettronica a destinatari specifici. Specificare l'indirizzo di posta elettronica di origine nella casella Indirizzo di posta elettronica di origine e scegliere Aggiungi per configurare l'indirizzo di posta elettronica di destinazione dei destinatari di posta elettronica e il livello di gravità del messaggio. Al termine, fare clic su OK.



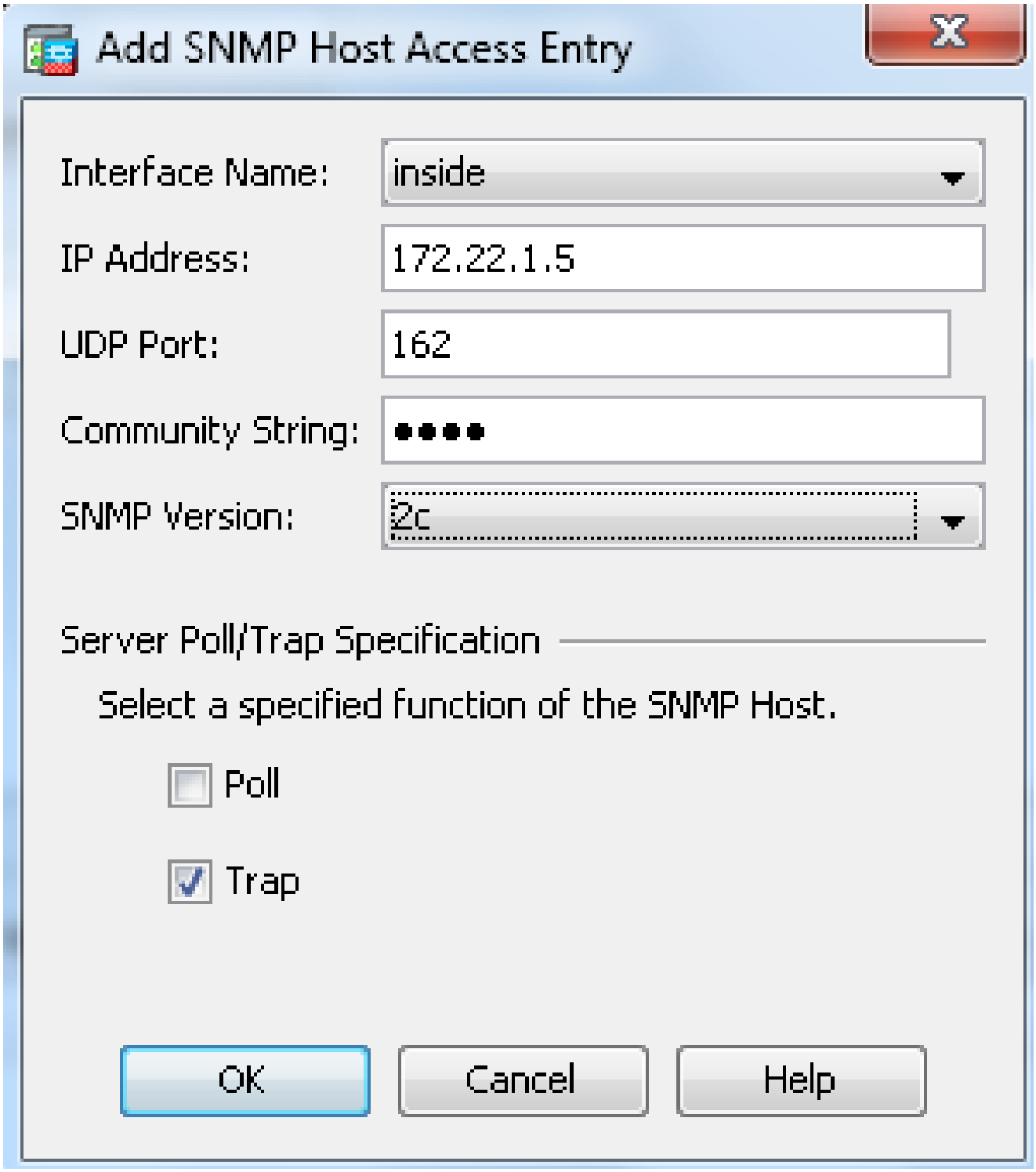
4. Scegliere Amministrazione periferica, Registrazione, SMTP e immettere l'indirizzo IP del server primario per specificare l'indirizzo IP del server SMTP.



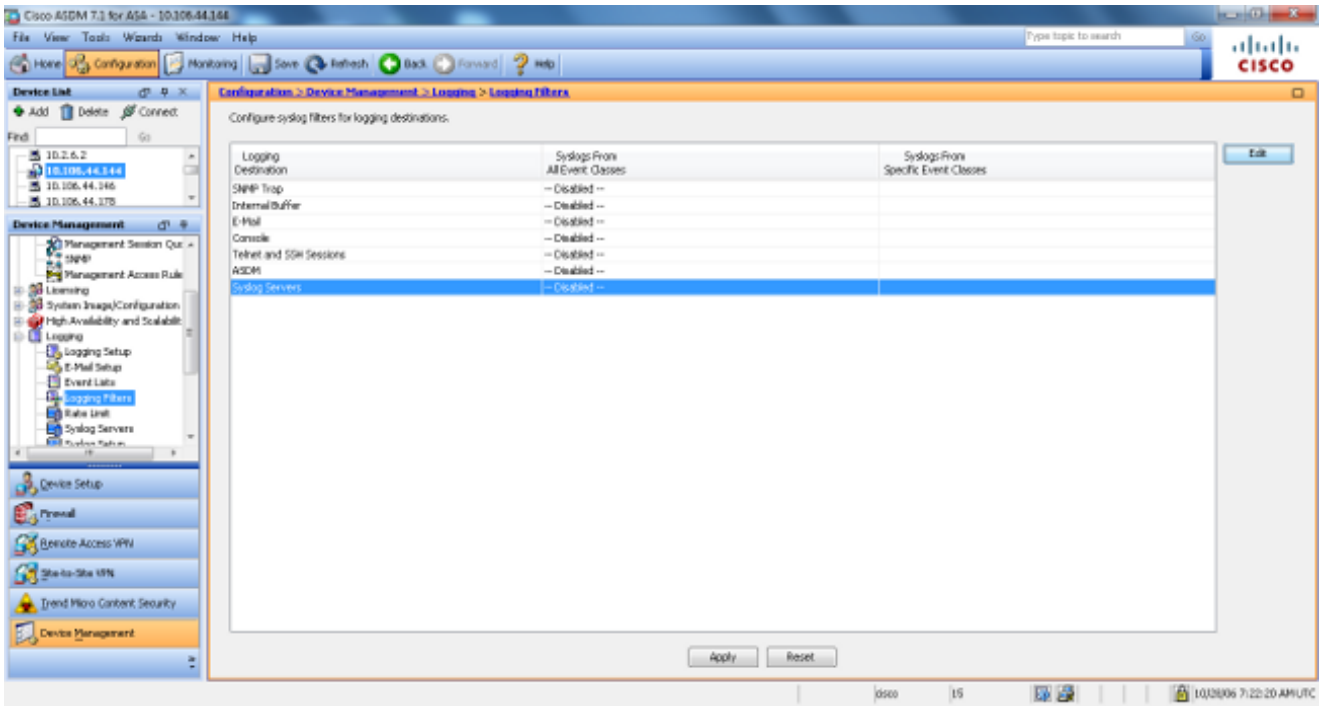
5. Se si desidera inviare syslog come trap SNMP, è innanzitutto necessario definire un server SNMP. Scegliere SNMP nel menu Management Access per specificare l'indirizzo delle stazioni di gestione SNMP e le relative proprietà specifiche.



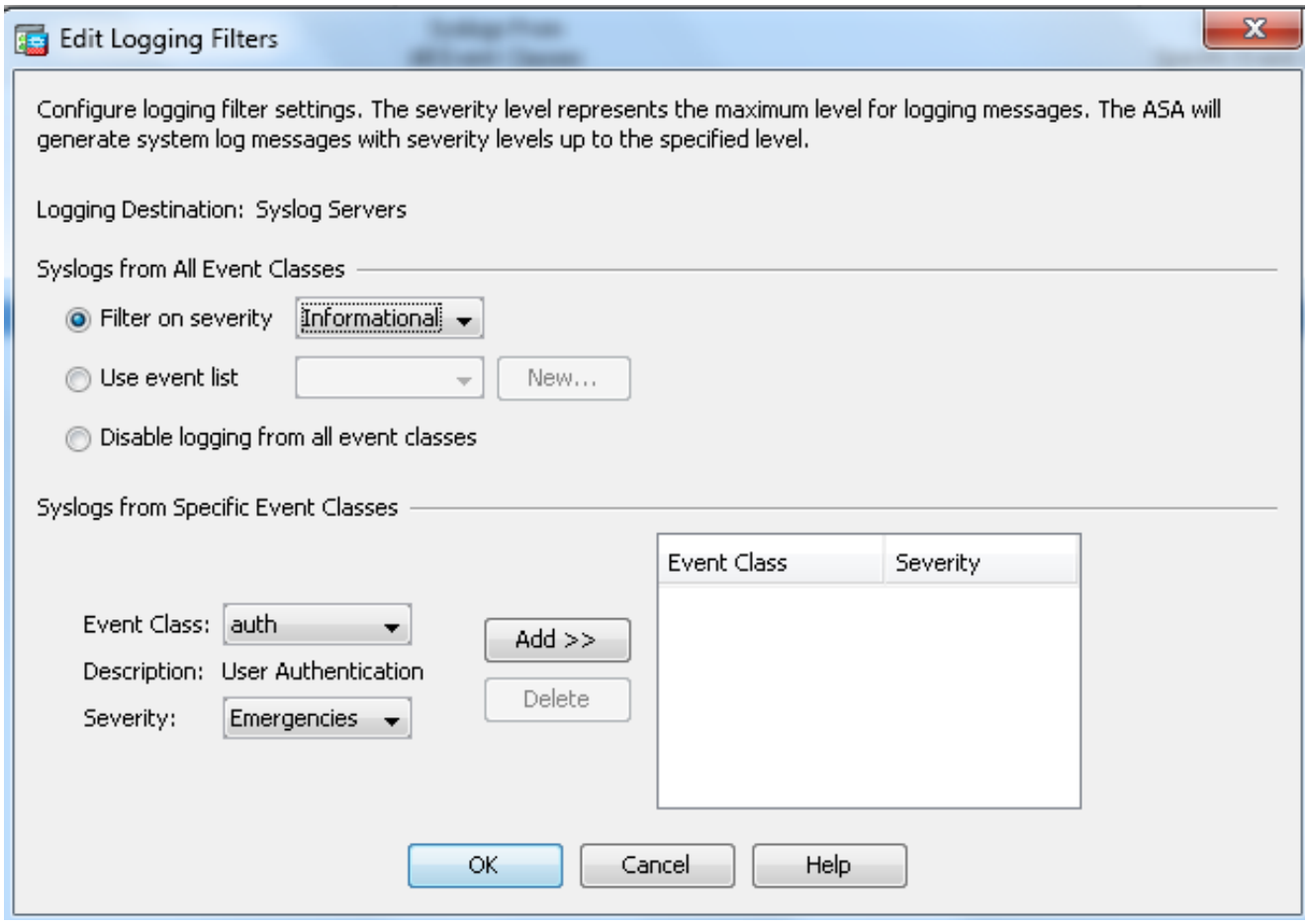
6. Per aggiungere una stazione di gestione SNMP, scegliere Add (Aggiungi). Immettere i dettagli dell'host SNMP e fare clic su OK.



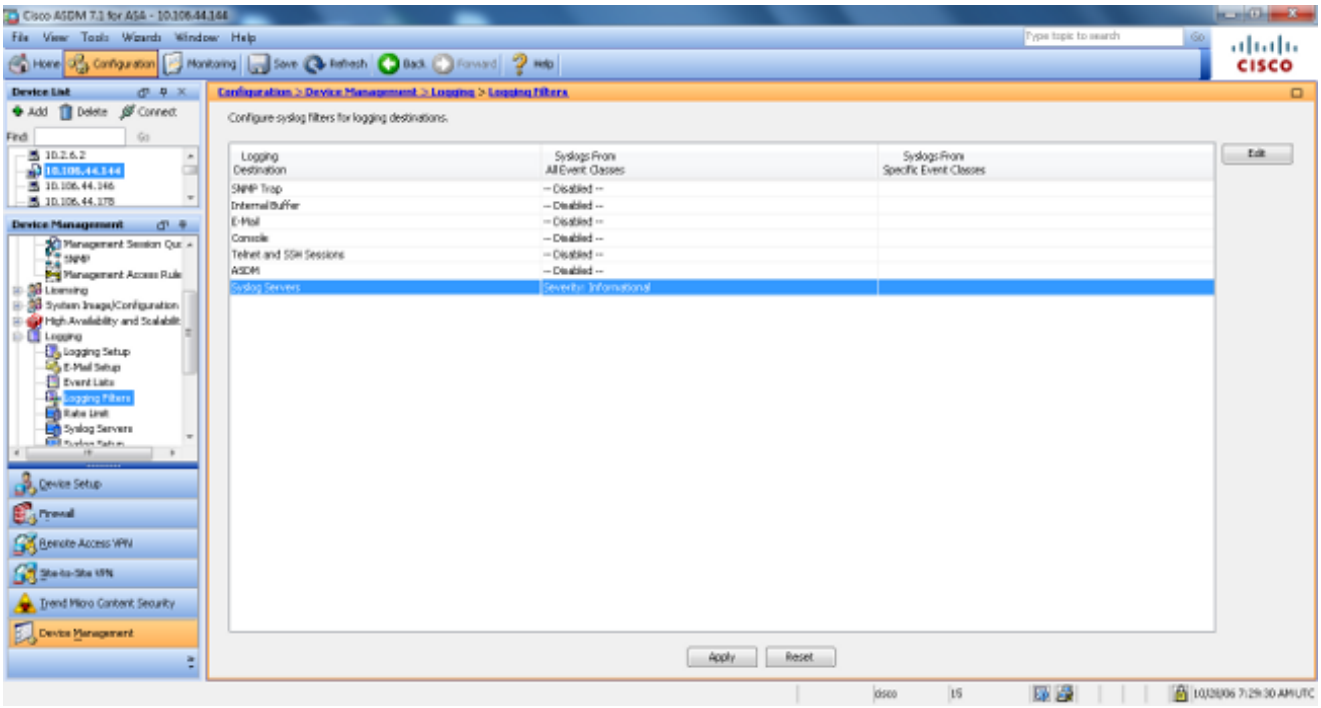
7. Per abilitare l'invio dei log a una delle destinazioni indicate in precedenza, scegliere Filtri di log nella sezione di log. In questo documento vengono indicate tutte le possibili destinazioni di registrazione e il livello corrente dei log inviati a tali destinazioni. Scegliere la destinazione di logging desiderata e fare clic su Modifica. In questo esempio viene modificata la destinazione 'Syslog Server'.



8. Selezionare il livello di gravità desiderato, in questo caso Informativo, dall'elenco a discesa Filtra in base alla gravità. Al termine, fare clic su OK.



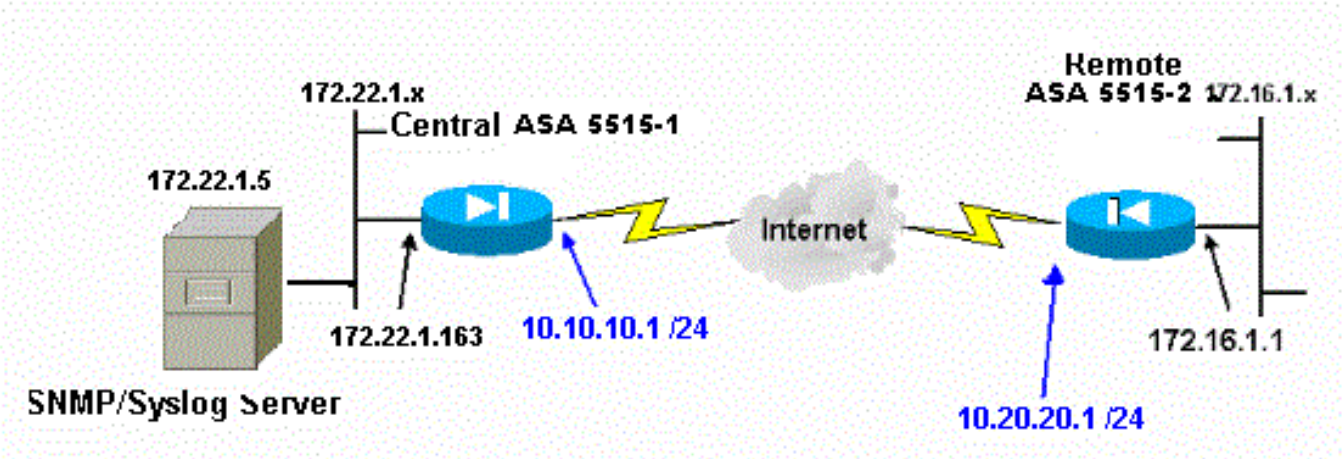
9. Fare clic su Applica dopo essere tornati alla finestra Filtri di registrazione.



Invio di messaggi syslog su una VPN a un server syslog

Con il semplice design VPN da sito a sito o con il design più complesso hub e spoke, gli amministratori potrebbero voler monitorare tutti i firewall ASA remoti con il server SNMP e il server syslog situati in un sito centrale.

Per configurare la VPN IPsec da sito a sito, fare riferimento a PIX/ASA 7.x e versioni successive: esempio di configurazione del tunnel VPN da PIX a PIX. A parte la configurazione VPN, è necessario configurare il protocollo SNMP e il traffico interessante per il server syslog sia sul sito centrale che su quello locale.



Configurazione ASA centrale

<#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 *****
```

Configurazione ASA remota

<#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 *****
```

Per ulteriori informazioni su come configurare l'ASA versione 8.4, fare riferimento a Monitoraggio di Cisco Secure ASA Firewall con SNMP e Syslog through VPN Tunnel

Syslog avanzato

ASA versione 8.4 fornisce diversi meccanismi che consentono di configurare e gestire i messaggi syslog in gruppi. Tali meccanismi includono il livello di gravità del messaggio, la classe del messaggio, l'ID del messaggio o un elenco di messaggi personalizzato creato dall'utente. Tramite questi meccanismi è possibile immettere un singolo comando applicabile a gruppi di messaggi piccoli o grandi. Quando si configura il syslog in questo modo, è possibile acquisire i messaggi dal gruppo di messaggi specificato e non tutti i messaggi con la stessa gravità.

Utilizzare l'elenco dei messaggi

Utilizzare l'elenco dei messaggi per includere in un gruppo solo i messaggi syslog interessati in base al livello di gravità e all'ID, quindi associare l'elenco alla destinazione desiderata.

Per configurare un elenco di messaggi, completare la procedura seguente:

1. Immettere l'elenco di registrazione elenco_messaggi | level severity_level [class_message_class] per creare un elenco di messaggi che includa i messaggi con un livello di gravità o un elenco di messaggi specificato.
2. Immettere il comando logging list message_list message syslog_id-syslog_id2 per aggiungere altri messaggi all'elenco appena creato.
3. Immettere il comando logging destination_list per specificare la destinazione dell'elenco di messaggi creato.

Esempio 2

Immettere questi comandi per creare un elenco di messaggi, che includa tutti i messaggi di gravità

2 (critici) con l'aggiunta dei messaggi da 611101 a 611323, e inviarli anche alla console:

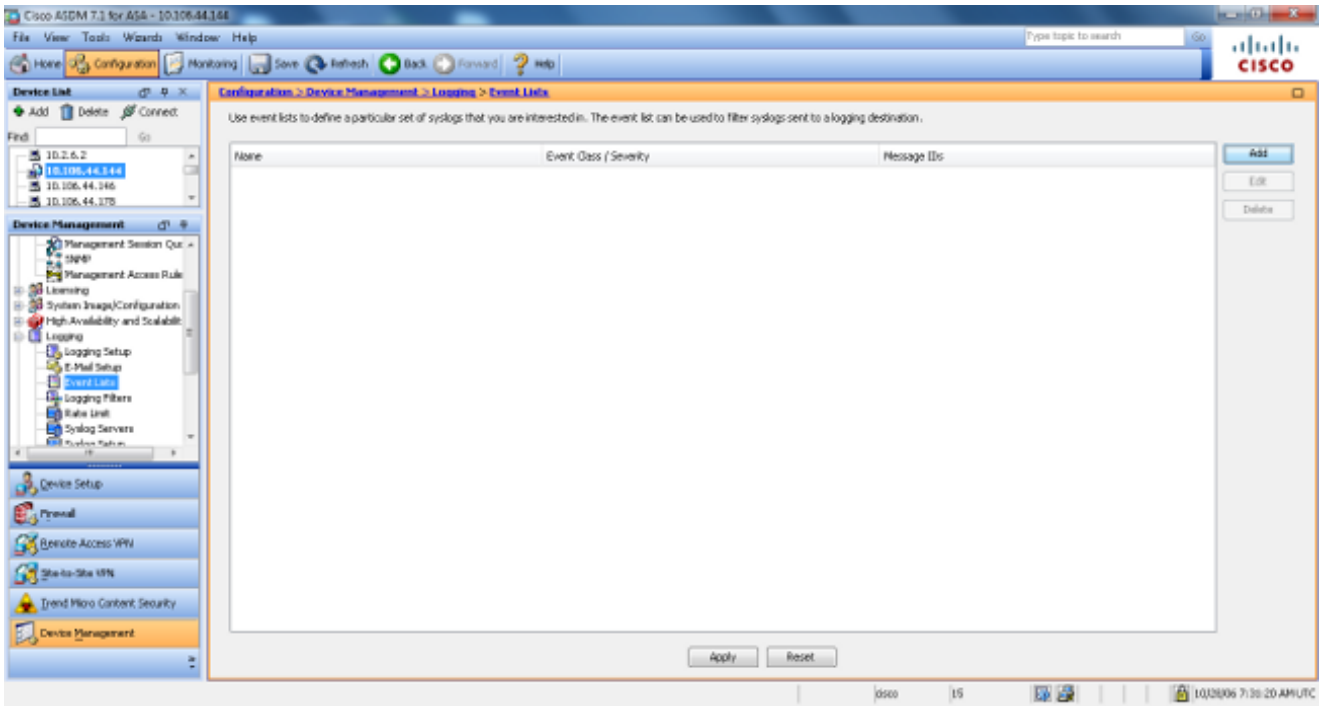
<#root>

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

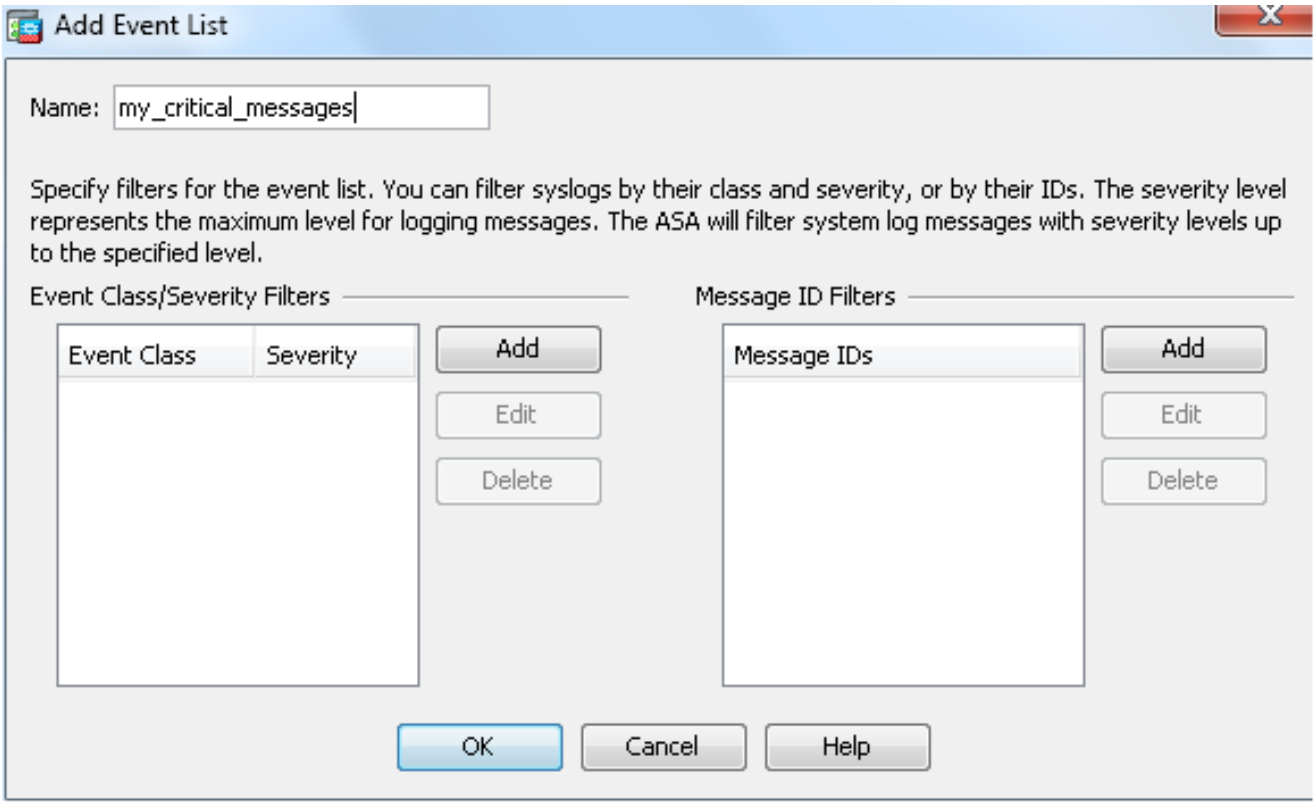
Configurazione ASDM

In questa procedura viene illustrata una configurazione ASDM per l'esempio 2 con l'uso dell'elenco dei messaggi.

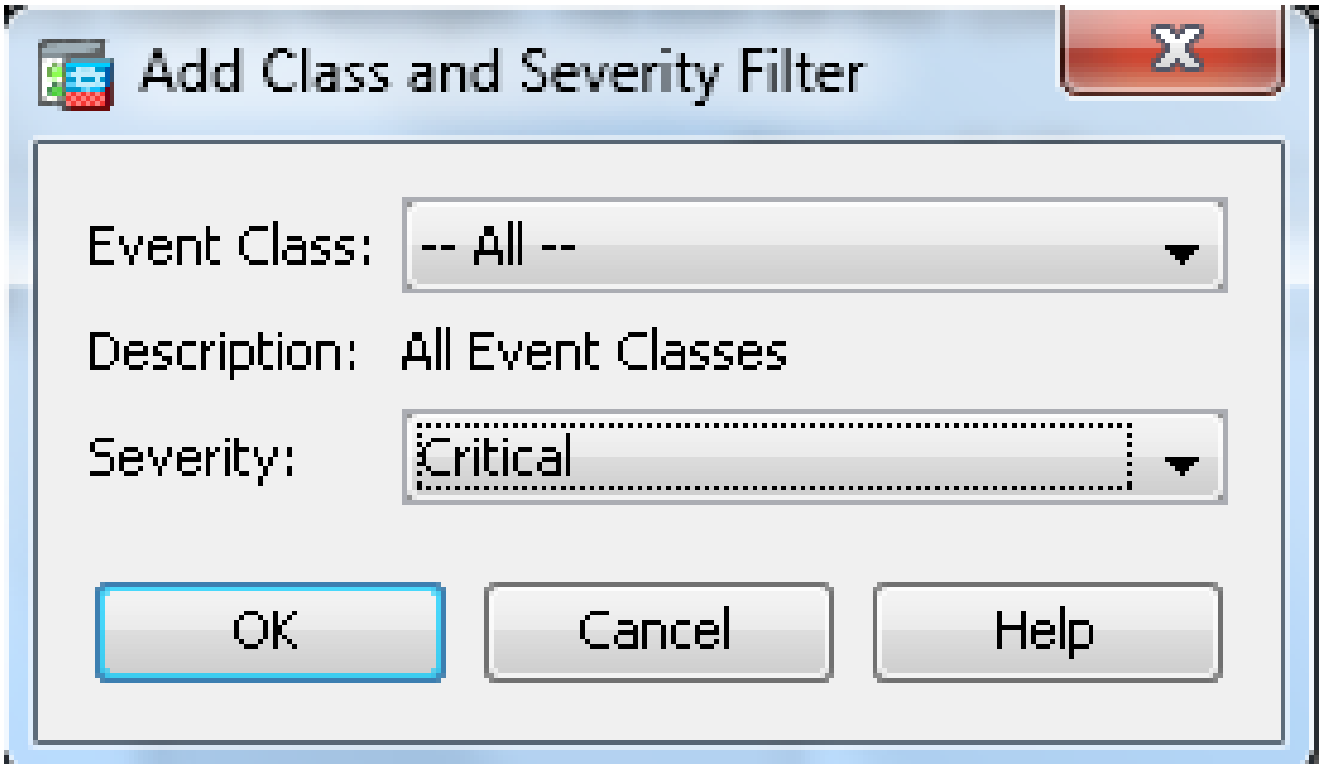
1. Per creare un elenco di messaggi, scegliere Elenchi eventi in Registrazione e fare clic su Aggiungi.



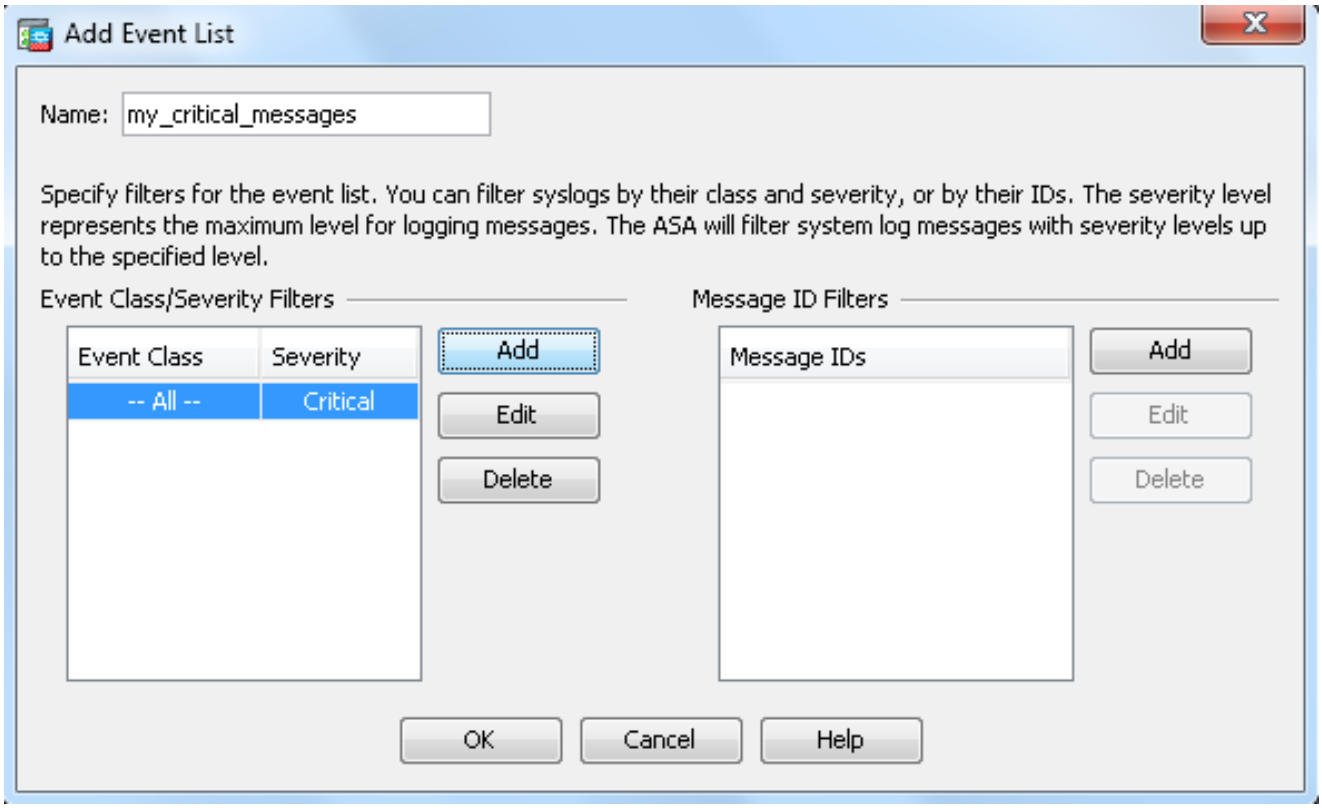
2. Immettere il nome dell'elenco dei messaggi nella casella Nome. In questo caso viene utilizzato my_critical_messages. Fare clic su Add (Aggiungi) in Event Class/Severity Filters (Filtri classi evento/gravità).



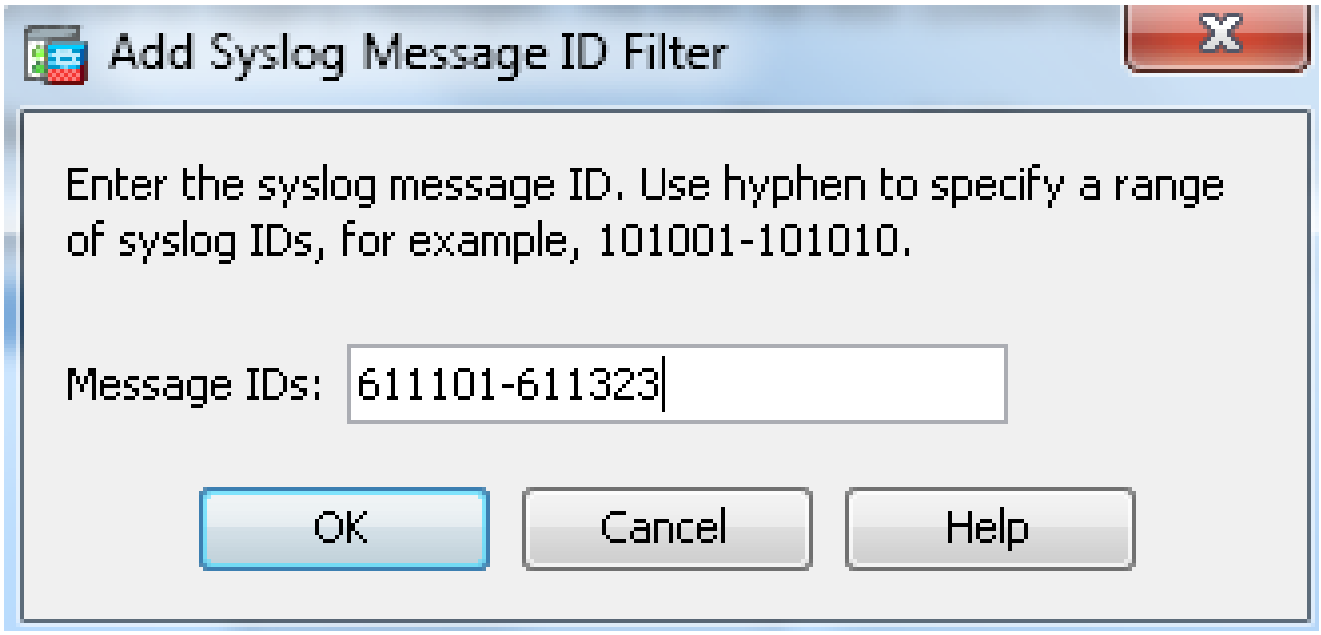
3. Selezionare Tutto dall'elenco a discesa Classe evento. Selezionare Critico dall'elenco a discesa Gravità. Al termine, fare clic su OK.



4. Se sono necessari messaggi aggiuntivi, fare clic su Add (Aggiungi) in Message ID Filters (Filtri ID messaggi). In questo caso, è necessario inserire messaggi con ID 611101-611323.

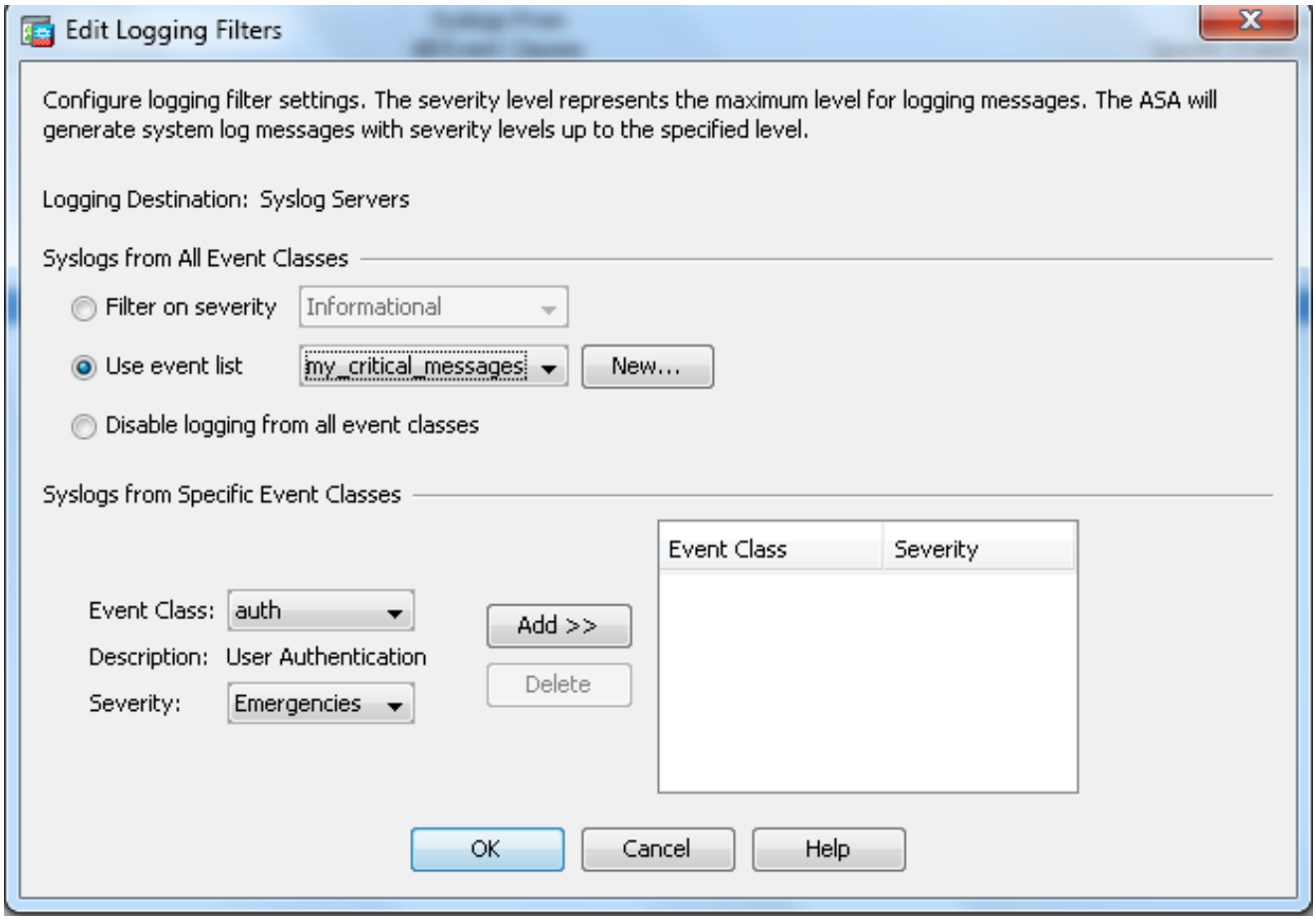


5. Inserire l'intervallo di ID nella casella ID messaggio e fare clic su OK.

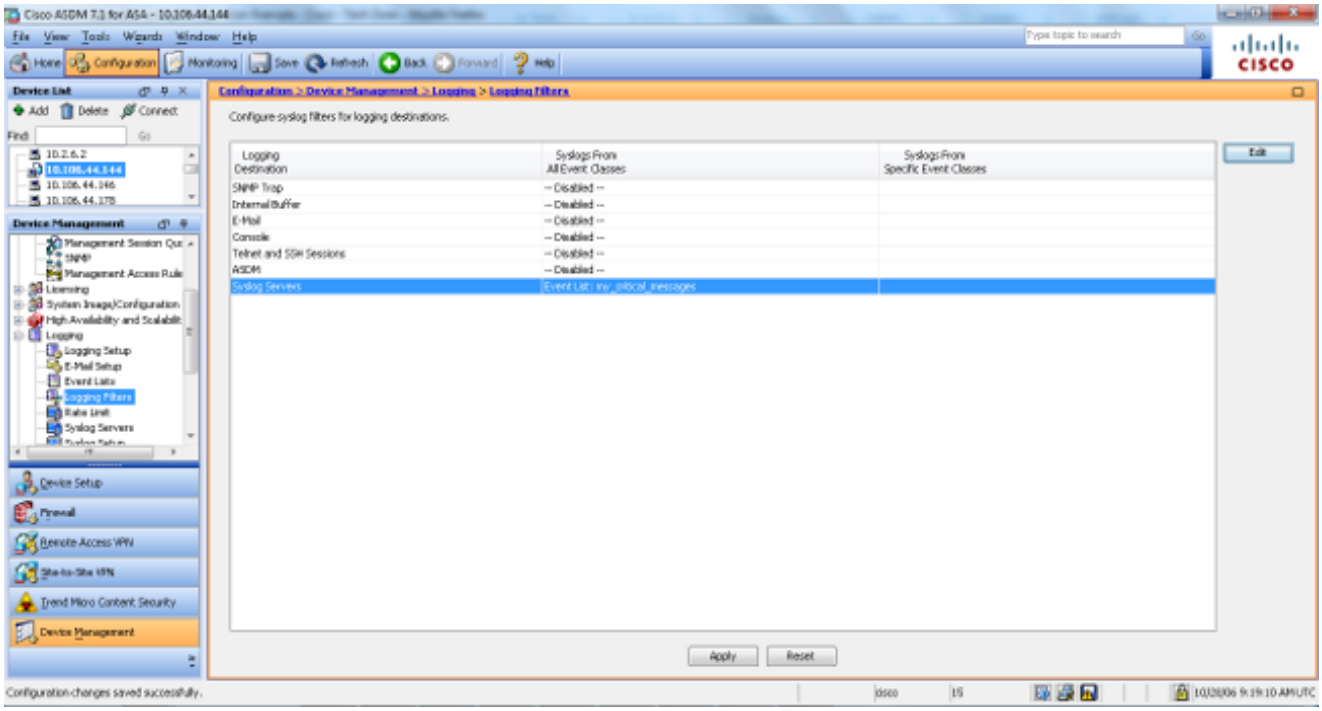


6. Tornare al menu Logging Filters e scegliere Console come destinazione.

7. Scegliere my_critical_messages dall'elenco a discesa Utilizza evento. Al termine, fare clic su OK.



8. Fare clic su Applica dopo essere tornati alla finestra Filtri di registrazione.



Le configurazioni ASDM vengono completate con l'uso di un elenco di messaggi, come mostrato nell'esempio 2.

Utilizzare la classe Message

Utilizzare la classe messaggio per inviare tutti i messaggi associati a una classe nel percorso di output specificato. Quando si specifica una soglia del livello di gravità, è possibile limitare il numero di messaggi inviati al percorso di output.

<#root>

logging class

message_class destination | severity_level

Esempio 3

Immettere questo comando per inviare alla console tutti i messaggi di classe ca con un livello di gravità pari o superiore alle emergenze.

<#root>

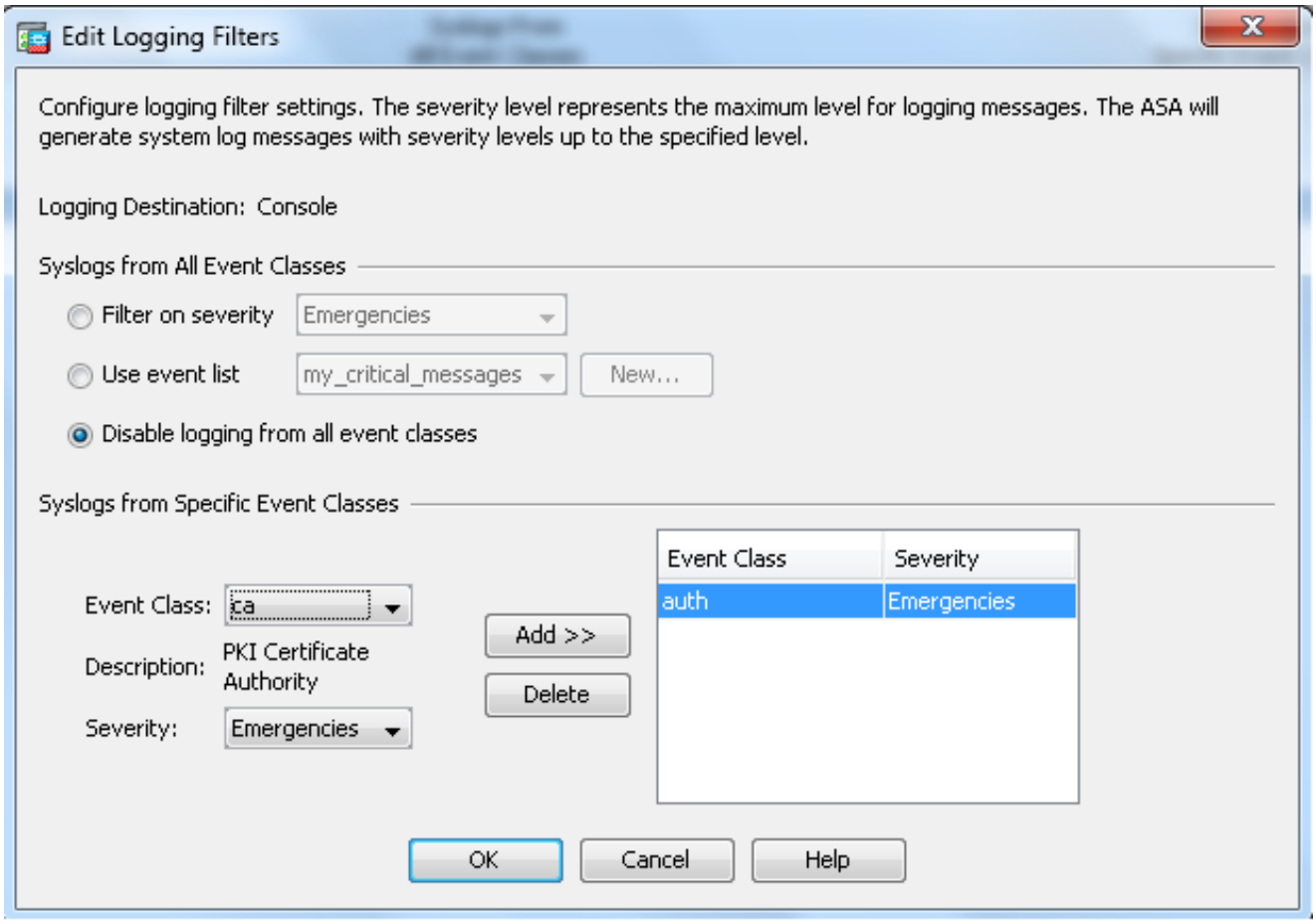
logging class ca console emergencies

Configurazione ASDM

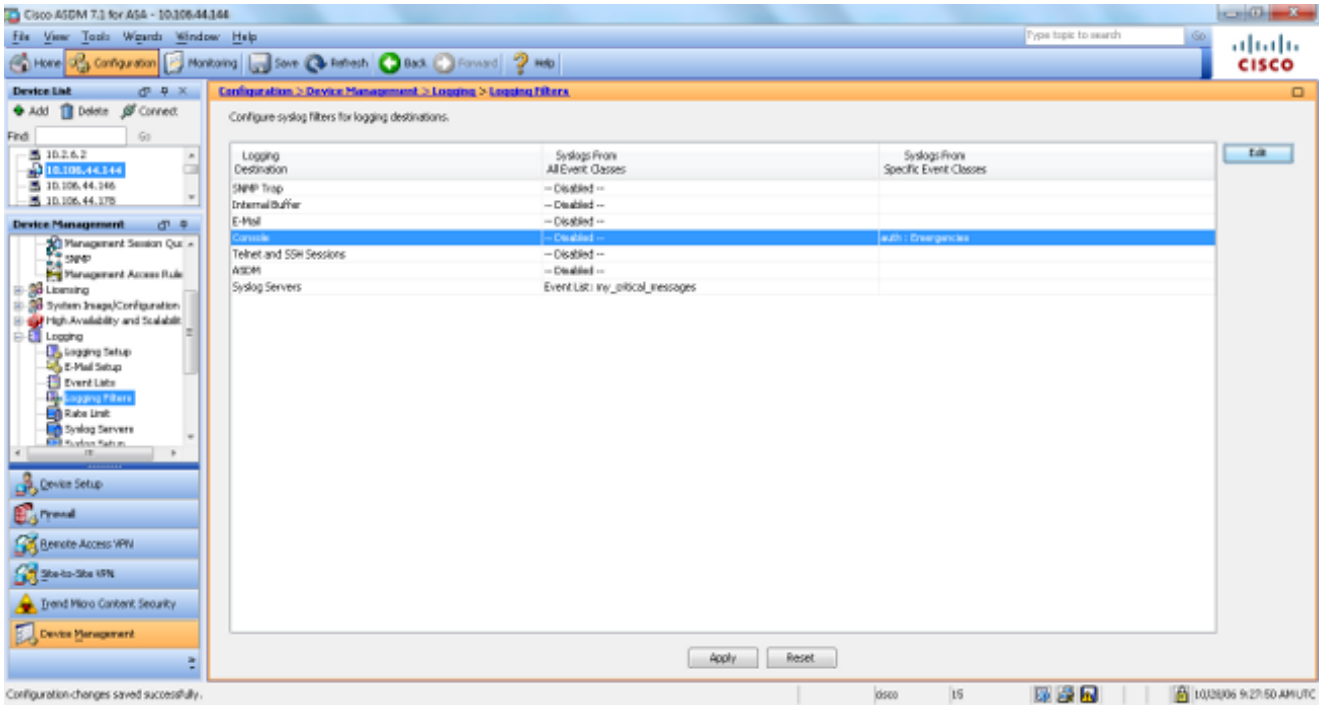
In questa procedura vengono mostrate le configurazioni ASDM per l'esempio 3 con l'uso dell'elenco dei messaggi.

1. Scegliere il menu Filtri di logging e scegliere Console come destinazione.
2. Fare clic su Disabilita registrazione da tutte le classi di eventi.
3. In Registri di sistema da classi di evento specifiche scegliere la classe di evento e la gravità da aggiungere.

   Questa procedura utilizza rispettivamente ca e Emergency.
4. Per aggiungere il messaggio alla classe, fare clic su Add (Aggiungi), quindi su OK.



5. Fare clic su Applica dopo essere tornati alla finestra Filtri di registrazione. La console raccoglie ora il messaggio della classe CA con il livello di gravità Emergenze, come mostrato nella finestra Filtri di registrazione.



La configurazione ASDM dell'esempio 3 è completata. Per un elenco dei livelli di gravità dei messaggi di log, fare riferimento a Messaggi elencati per livello di gravità.

Invio dei messaggi del log di debug a un server syslog

Per una risoluzione avanzata dei problemi, sono necessari registri di debug specifici per funzionalità/protocollo. Per impostazione predefinita, questi messaggi log vengono visualizzati sul terminale (SSH/Telnet). A seconda del tipo di debug e della frequenza dei messaggi di debug generati, l'uso della CLI può risultare difficile se i debug sono abilitati. Facoltativamente, i messaggi di debug possono essere reindirizzati al processo syslog e generati come syslog. Questi syslog possono essere inviati a qualsiasi destinazione syslog come qualsiasi altro syslog. Per deviare i debug ai syslog, immettere il comando log debug-trace. Questa configurazione invia l'output di debug, come syslog, a un server syslog.

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

Utilizzo congiunto di elenchi di registrazione e classi di messaggi

Immettere il comando log list per acquisire il syslog solo per i messaggi VPN da LAN a LAN e ad accesso remoto con IPsec. In questo esempio vengono acquisiti tutti i messaggi di registro di sistema della classe VPN (IKE e IPsec) con livello di debug o superiore.

Esempio

<#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
```

Registra riscontri ACL

Aggiungere il log a ciascun elemento dell'elenco di accesso (ACE) che si desidera registrare quando viene raggiunto un elenco di accesso. Utilizzare la seguente sintassi:

<#root>

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

Esempio

<#root>

```
ASAfirewall(config)#

access-list 101 line 1 extended permit icmp any any log
```

Per impostazione predefinita, gli ACL registrano tutti i pacchetti negati. Non è necessario aggiungere l'opzione log per negare gli ACL e generare syslog per i pacchetti negati. Quando si specifica l'opzione log, viene generato il messaggio syslog 106100 per la voce di controllo di accesso a cui viene applicata. Il messaggio Syslog 106100 viene generato per ogni licenza o negazione del flusso ACE corrispondente che passa attraverso il firewall ASA. Il flusso della prima corrispondenza viene memorizzato nella cache. Le corrispondenze successive incrementano il numero di passaggi visualizzato nel comando show access-list. Il comportamento predefinito della registrazione dell'elenco degli accessi, ovvero la parola chiave log non specificata, prevede che se un pacchetto viene rifiutato, venga generato il messaggio 106023 e che, se un pacchetto è autorizzato, non venga generato alcun messaggio syslog.

È possibile specificare un livello syslog opzionale (0 - 7) per i messaggi syslog generati (106100). Se non viene specificato alcun livello, il livello predefinito è 6 (informativo) per una nuova voce ACE. Se la voce di controllo di accesso esiste già, il relativo livello di registro corrente rimane invariato. Se si specifica l'opzione log disable, la registrazione dell'elenco degli accessi è completamente disabilitata. Non viene generato alcun messaggio syslog, che include il messaggio 106023. L'opzione log default ripristina il comportamento di registrazione predefinito dell'elenco degli accessi.

Completare questa procedura per abilitare il messaggio syslog 106100 da visualizzare nell'output della console:

1. Immettere il comando logging enable per abilitare la trasmissione dei messaggi del registro di sistema in tutti i percorsi di output. Per visualizzare i registri, è necessario impostare un percorso di output di registrazione.

2. Immettere il comando logging message <message_number> level <severity_level> per

impostare il livello di gravità di un messaggio di registro di sistema specifico.

In questo caso, immettere il comando logging message 106100 per abilitare il messaggio `106100`.

3. Immettere il message_list della console di registrazione | comando severity_level per consentire la visualizzazione dei messaggi del registro di sistema sulla console dell'appliance di sicurezza (tty) non appena vengono visualizzati. Impostare `severity_level` su un valore compreso tra 1 e 7 oppure utilizzare il nome del livello. È inoltre possibile specificare i messaggi da inviare con la variabile `message_list`.

4. Immettere il comando show logging message per visualizzare un elenco di messaggi del registro di sistema modificati dall'impostazione predefinita, ossia messaggi a cui è stato assegnato un livello di gravità diverso e messaggi disabilitati.

   Di seguito viene riportato un esempio di output del comando 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
```

Blocco della generazione del syslog su un'appliance ASA in standby

Partire dal software ASA versione 9.4.1 in poi e bloccare la generazione di syslog specifici su un'unità di standby, quindi usare questo comando:

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

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Se si desidera eliminare un messaggio syslog specifico da inviare al server syslog, è necessario immettere il comando come mostrato.

<#root>

```
hostname(config)#
```

no logging message

<syslog_id>

Per ulteriori informazioni, consultare il comando logging message.

%ASA-3-20108: disattivazione nuove connessioni

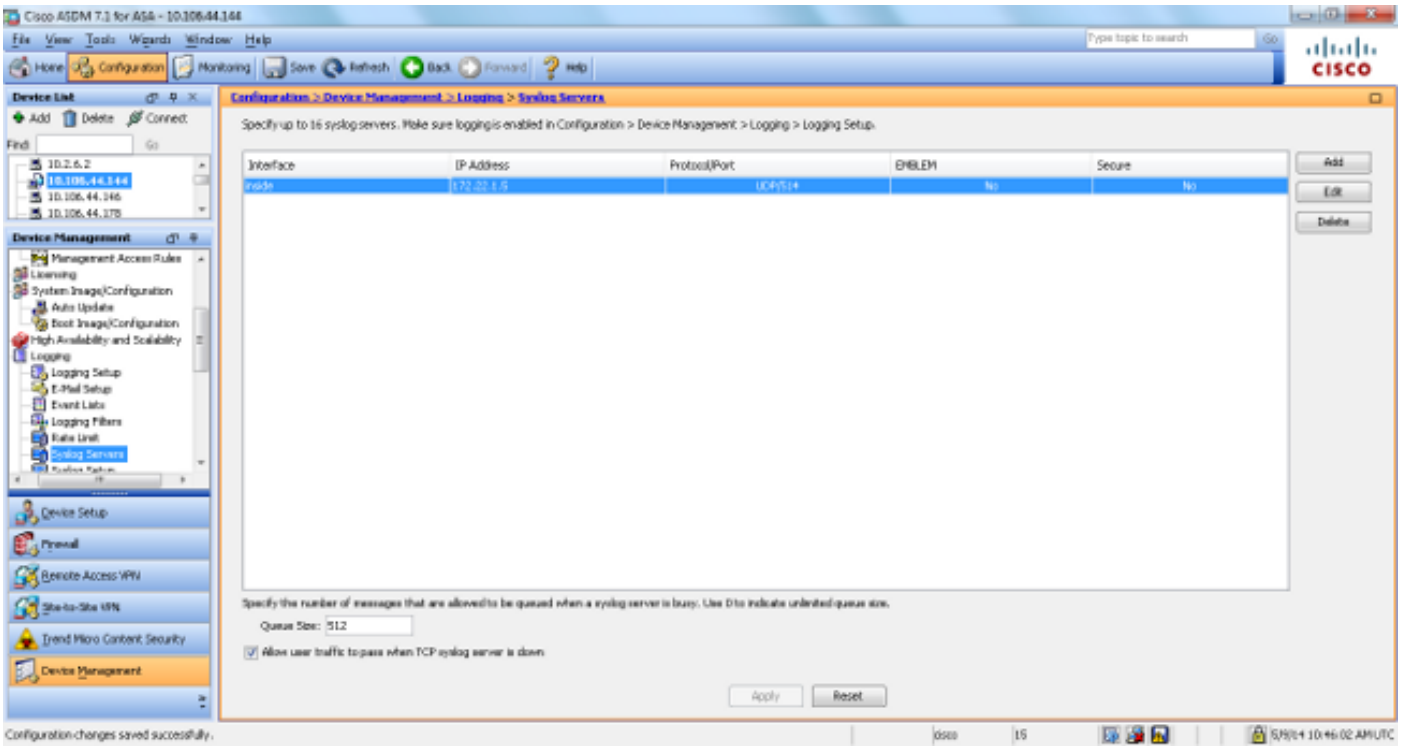
In `%ASA-3-20108: non sono consentite nuove connessioni.` Viene visualizzato il messaggio di errore quando un'ASA non è in grado di contattare il server syslog e non sono consentite nuove connessioni.

Soluzione

Questo messaggio viene visualizzato quando è stata abilitata la messaggistica del registro di sistema TCP e non è possibile raggiungere il server syslog oppure quando si usa Cisco ASA Syslog Server (PFSS) e il disco nel sistema Windows NT è pieno. Per risolvere questo messaggio di errore, completare la procedura seguente:

- Disabilitare la messaggistica del registro di sistema TCP, se abilitata.
- Se si utilizza PFSS, liberare spazio nel sistema Windows NT in cui risiede PFSS.
- Verificare che il server syslog sia attivo e poter eseguire il ping sull'host dalla console Cisco ASA.
- Riavviare la registrazione dei messaggi di sistema TCP per consentire il traffico.

Se il server syslog non funziona e la registrazione TCP è configurata, usare il comando logging allow-hostdown o passare alla registrazione UDP.



Informazioni correlate

- [Riferimenti per i comandi di Cisco Secure PIX Firewall]
- [RFC (Requests for Comments)]
- [Documentazione e supporto tecnico – Cisco Systems]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).