ASA 8.2: Configurazione di Syslog mediante ASDM

Sommario

Introduzione

In questo documento viene spiegato come configurare syslog su Cisco Adaptive Security Appliance (ASA) 8.x usando l'interfaccia utente di Adaptive Security Device Manager (ASDM). I messaggi del registro di sistema sono i messaggi generati dall'appliance Cisco ASA per notificare all'amministratore qualsiasi modifica apportata alla configurazione, alle impostazioni di rete o alle prestazioni del dispositivo. Analizzando i messaggi del registro eventi di sistema, un amministratore può risolvere facilmente l'errore eseguendo un'analisi della causa principale.

I messaggi Syslog vengono differenziati principalmente in base al livello di gravità.

1. Gravità 0 - Messaggi di emergenza - Risorsa inutilizzabile

2. Gravità 1 - Messaggi di avviso - È necessaria un'azione immediata
3. Gravità 2 - Messaggi critici - Condizioni critiche
4. Gravità 3 - Messaggi di errore - Condizioni di errore
5. Gravità 4 - Messaggi di avviso - Condizioni di avviso
6. Gravità 5 - Messaggi di notifica - Condizioni normali ma significative
7. Gravità 6 - Messaggi informativi - Solo messaggi informativi
8. Gravità 7 - Messaggi di debug - Solo messaggi di debug**Nota:** il livello di gravità più alto è quello di emergenza, mentre il livello più basso è quello di debug.

Di seguito sono riportati alcuni messaggi di syslog di esempio generati dall'appliance Cisco ASA:

- %ASA-6-106012: Nega IP da indirizzo_IP a indirizzo_IP, opzioni IP esadecimali.
- %ASA-3-211001: Errore di allocazione della memoria
- %ASA-5-35003: ACL predefinito NAC applicato, ACL:nome-ACL - indirizzo-host

Il valore numerico X specificato in "%ASA-X-YYYY:" indica la gravità del messaggio. Ad esempio, "%ASA-6-106012" è un messaggio informativo e "%ASA-5-35003" è un messaggio di errore.

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:

- Cisco ASA versione 8.2
- Cisco ASDM versione 6.2

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.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

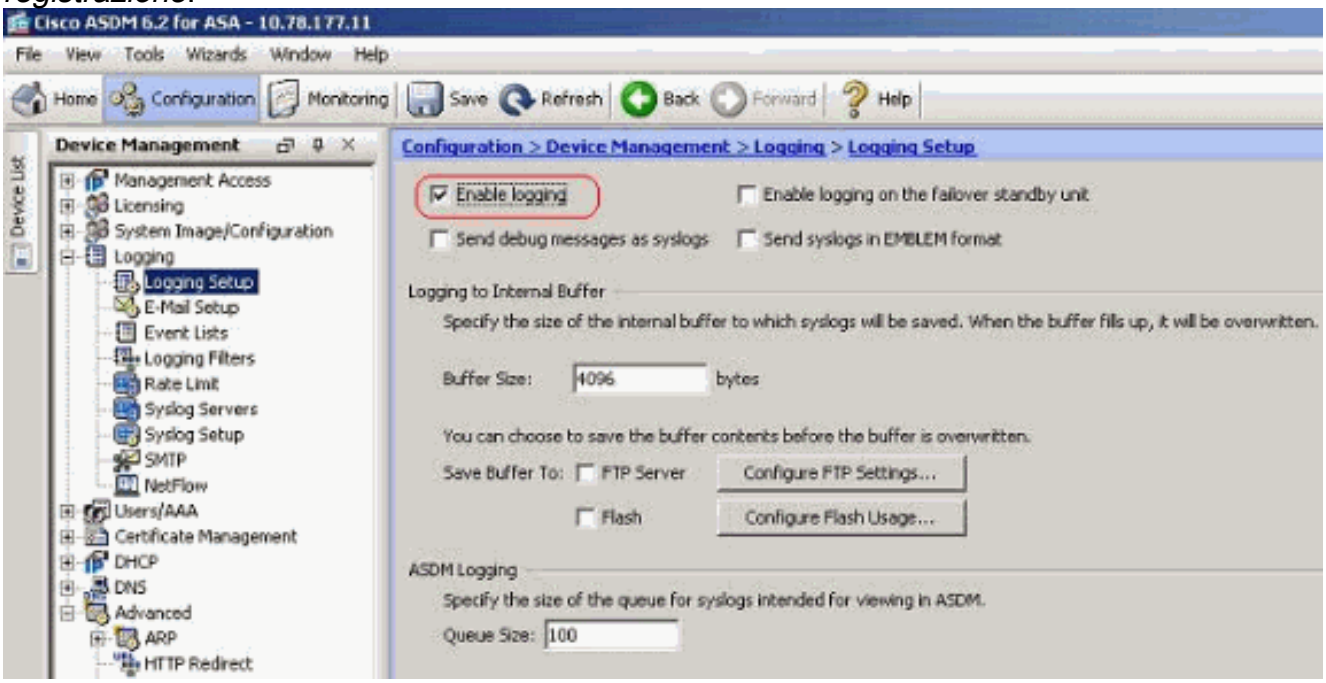
Configurazione di syslog di base con ASDM

Abilita registrazione

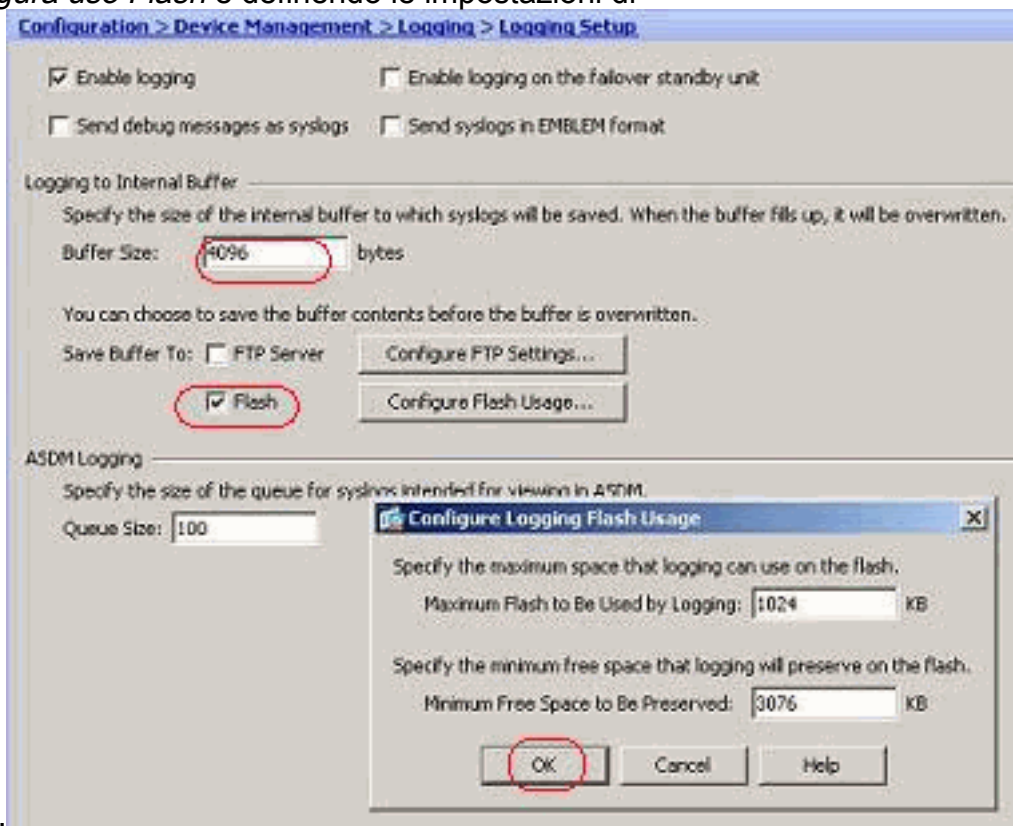
Attenersi alla seguente procedura:

1. Scegliere *Configurazione > Gestione periferiche > Registrazione > Impostazione registrazione* e selezionare l'opzione *Abilita*

registrazione.



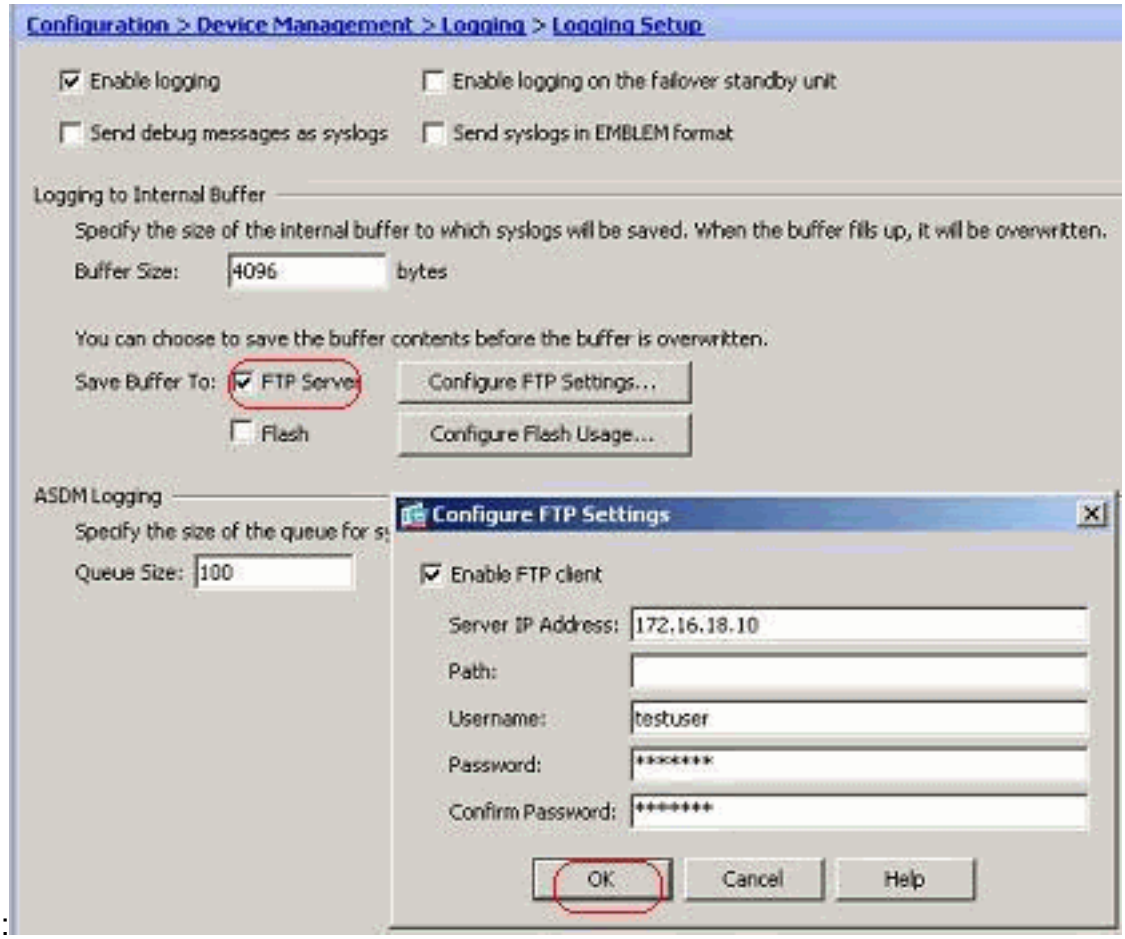
2. Èpossibile registrare i messaggi syslog in un buffer interno specificandone le dimensioni. Potete anche scegliere di salvare il contenuto del buffer nella memoria flash facendo clic su *Configura uso Flash* e definendo le impostazioni di



Flash.

3. I messaggi di log nel buffer possono essere inviati a un server FTP prima di essere sovrascritti. Fare clic su *Configure FTP Settings* (Configura impostazioni FTP) e specificare i dettagli del server FTP, come mostrato di

seguito:

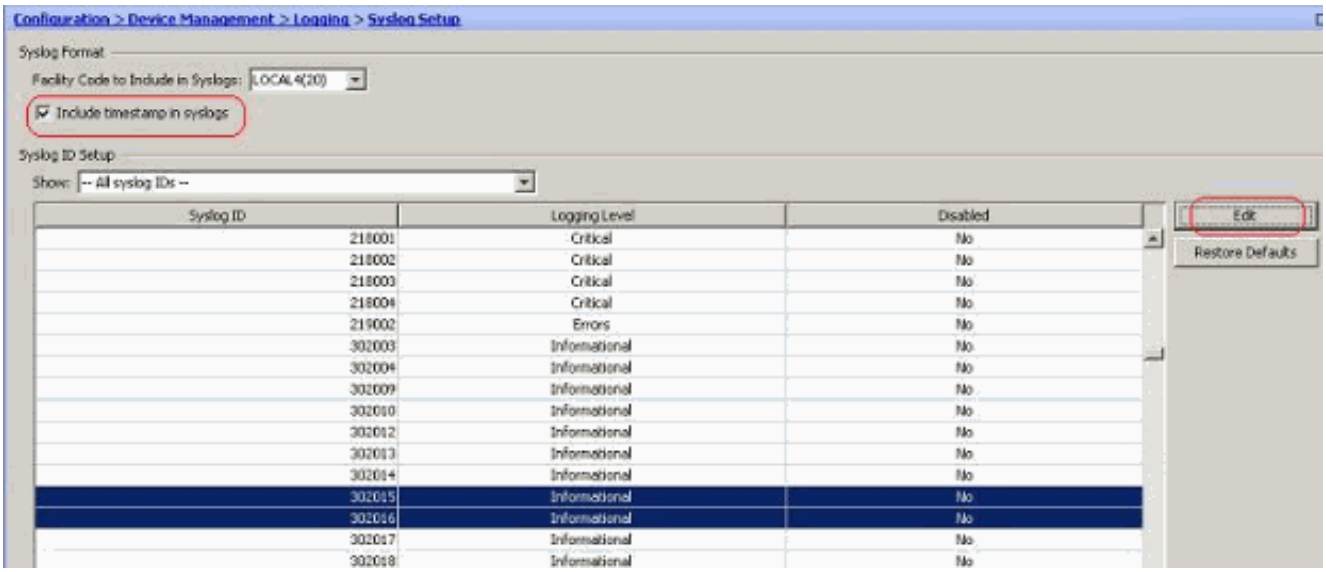


Disabilita registrazione

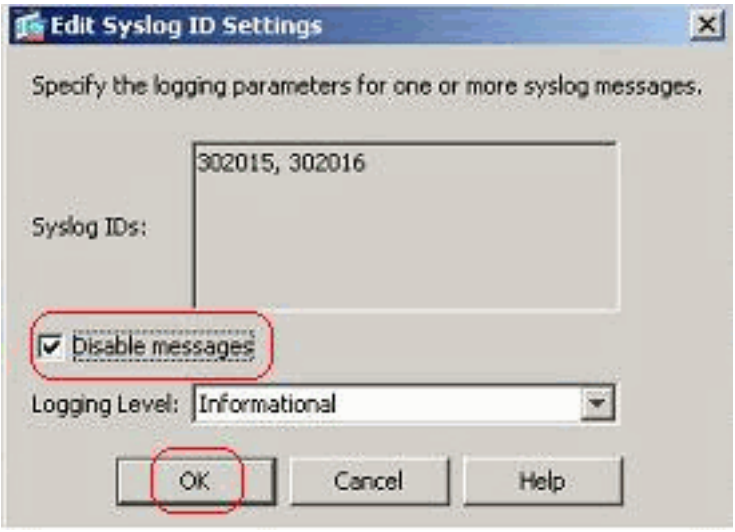
Èpossibile disabilitare gli ID syslog specifici in base alle proprie esigenze.

Nota: selezionando il segno di spunta per l'opzione *Includi indicatore orario nei syslog*, è possibile aggiungere la data e l'ora in cui sono stati generati come campo nei syslog.

1. Selezionare i syslog da disabilitare e fare clic su *Modifica*.

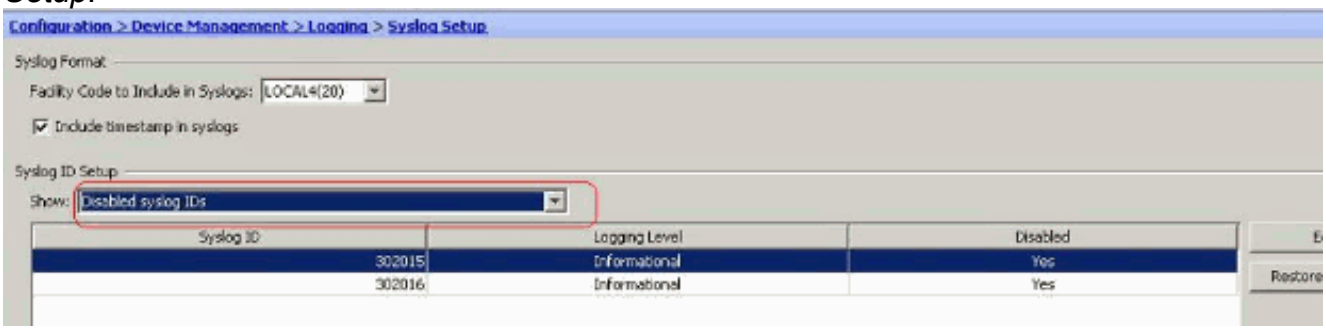


2. Dalla finestra *Edit Syslog ID Settings*, selezionare l'opzione *Disable messages* e fare clic su



OK.

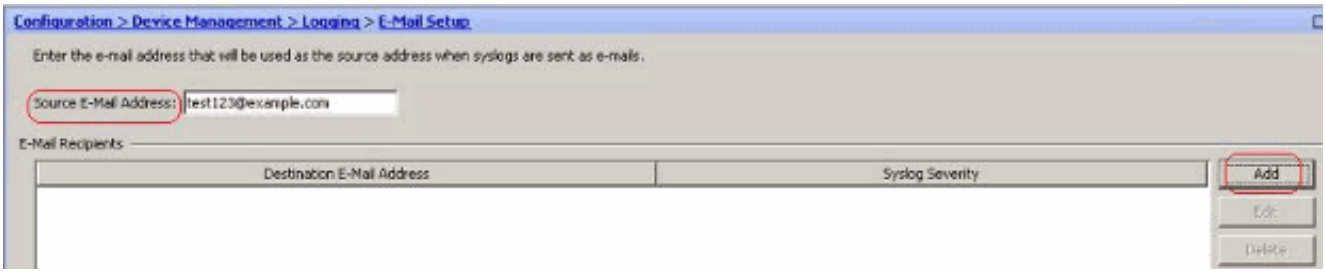
3. I syslog disattivati possono essere visualizzati in una scheda separata selezionando *ID syslog disattivati* dal menu a discesa *Syslog ID Setup*.



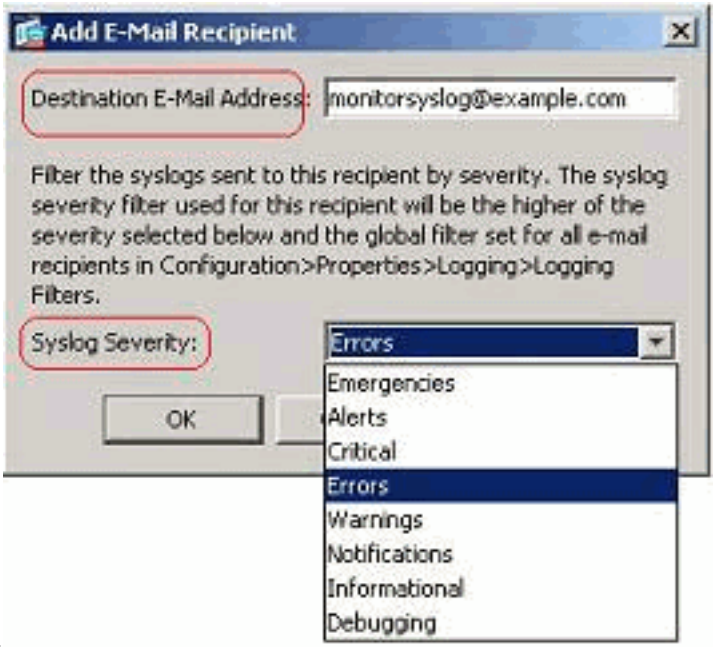
Accesso a un messaggio di posta elettronica

Per inviare i syslog a un messaggio di posta elettronica, completare la procedura seguente utilizzando ASDM:

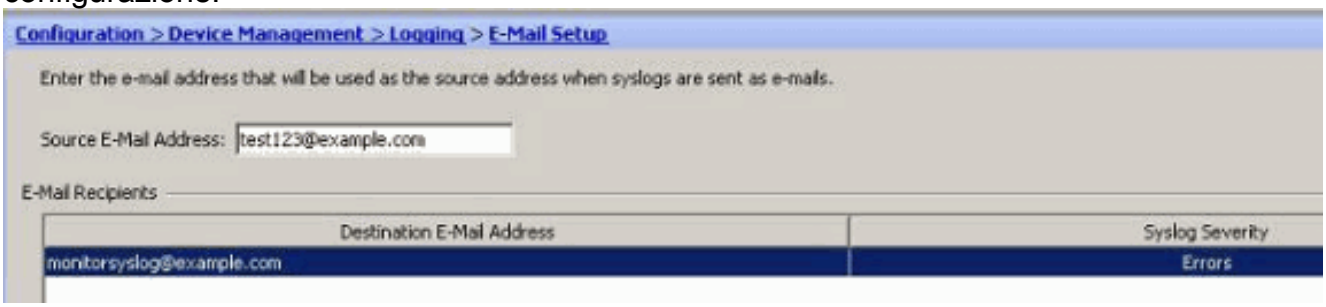
1. Scegliere *Configurazione > Gestione dispositivi > Registrazione > Configurazione posta elettronica*. Il campo *Indirizzo di posta elettronica di origine* è utile per assegnare un ID di posta elettronica come origine per i syslog. Specificare l'indirizzo di posta elettronica di origine. Fare clic su *Aggiungi* per aggiungere i destinatari di posta elettronica.



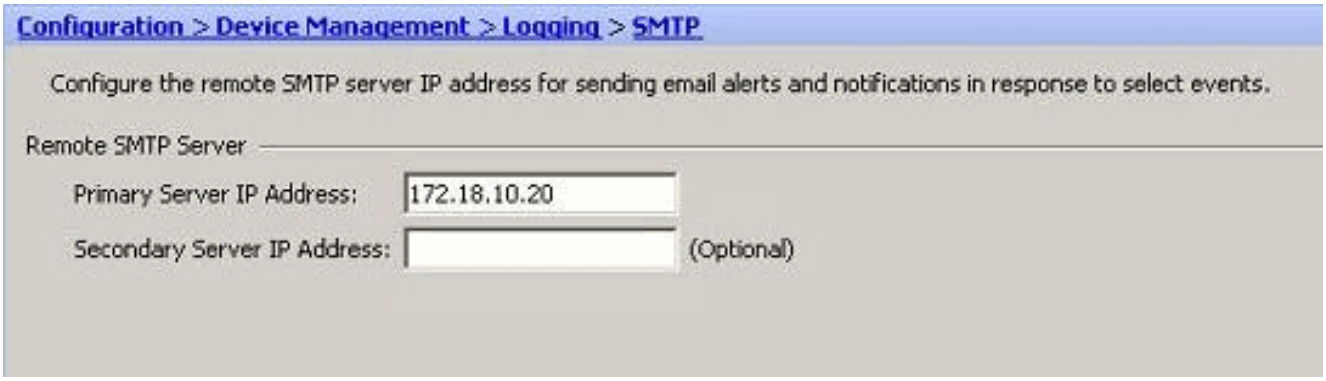
2. Specificare l'*indirizzo e-mail di destinazione* e scegliere il *livello di gravità*. In base ai livelli di gravità, è possibile definire destinatari di posta elettronica diversi. Fare clic su *OK* per tornare al riquadro *Configurazione posta*



elettronica. Il risultato è la seguente configurazione:



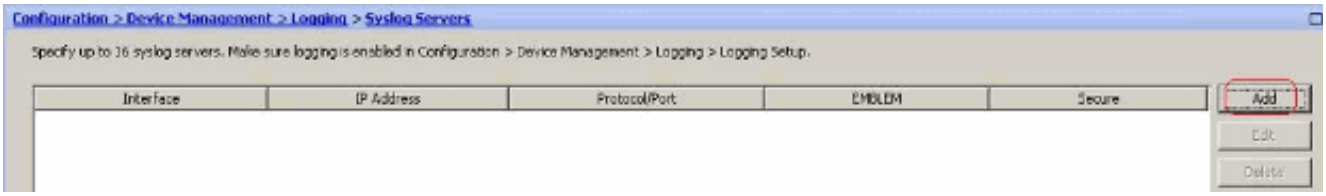
3. Scegliete *Configurazione > Configurazione dispositivo > Registrazione > SMTP* e specificate il server SMTP.



Accesso a un server Syslog

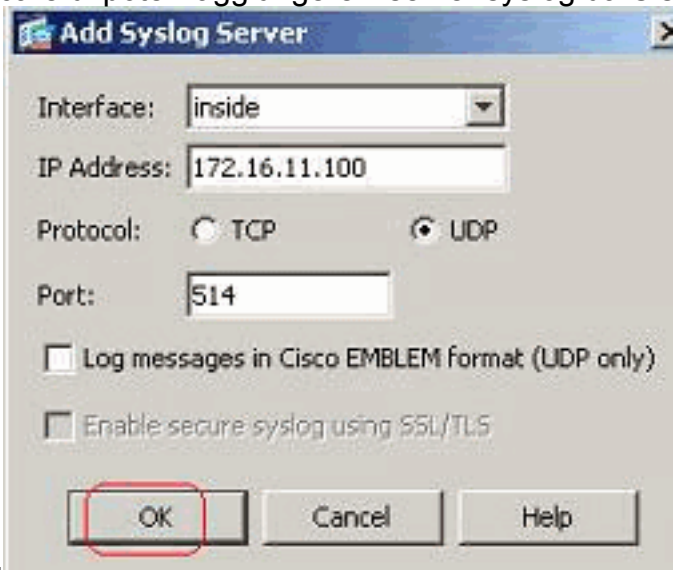
Èpossibile inviare tutti i messaggi syslog a un server syslog dedicato. Eseguire i seguenti passaggi utilizzando ASDM:

1. Scegliere *Configurazione > Gestione dispositivi > Registrazione > Server syslog* e fare clic su *Aggiungi* per aggiungere un server syslog.

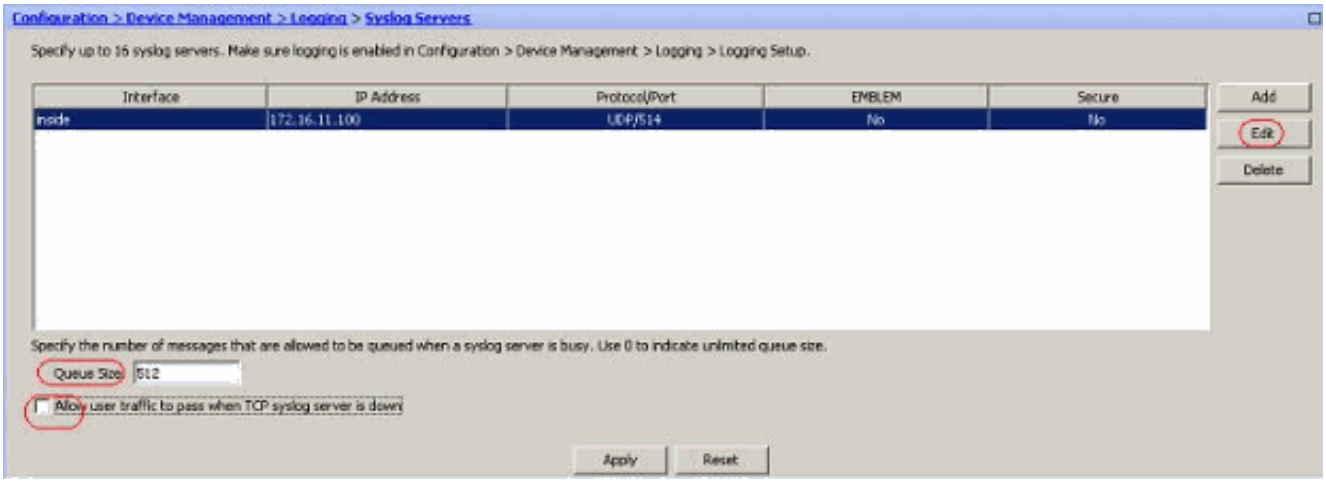


Viene visualizzata la finestra *Add Syslog Server*.

2. Specificare l'interfaccia a cui è associato il server e l'indirizzo IP. Specificare i dettagli *Protocollo* e *Porta* a seconda dell'impostazione della rete. Quindi fare clic su *OK*.**Nota:** verificare di poter raggiungere il server syslog da Cisco ASA.



3. Il server syslog configurato viene visualizzato come mostrato di seguito. Per apportare modifiche, selezionare il server e fare clic su *Modifica*.



Nota: selezionare l'opzione *Consenti passaggio traffico utente quando il server syslog TCP è inattivo*. In caso contrario, le nuove sessioni utente vengono negate tramite l'appliance ASA. Questa opzione è applicabile solo quando il protocollo di trasporto tra l'ASA e il server syslog è TCP. Per impostazione predefinita, le nuove sessioni di accesso alla rete vengono negate da Cisco ASA quando un server syslog non è attivo per qualsiasi motivo.Per definire il tipo di messaggi syslog da inviare al server syslog, vedere la sezione Filtro di registrazione.

Configurazione syslog avanzata con ASDM

Utilizzo degli elenchi di eventi

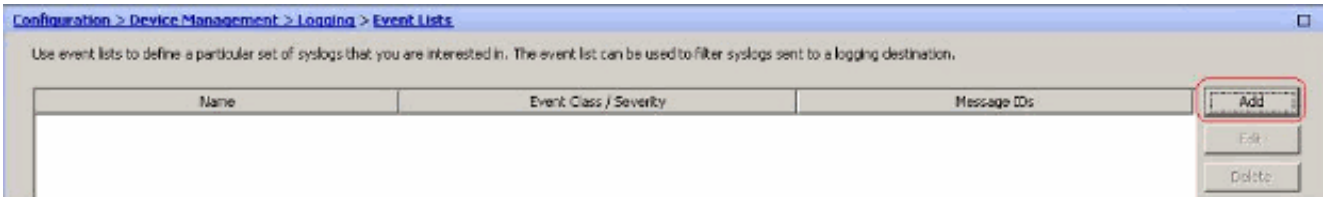
Gli elenchi di eventi consentono di creare elenchi personalizzati contenenti il gruppo di messaggi syslog da inviare a una destinazione. Gli elenchi di eventi possono essere creati in tre modi diversi:

- ID messaggio o intervallo di ID messaggio
- Gravità messaggio
- Classe messaggio

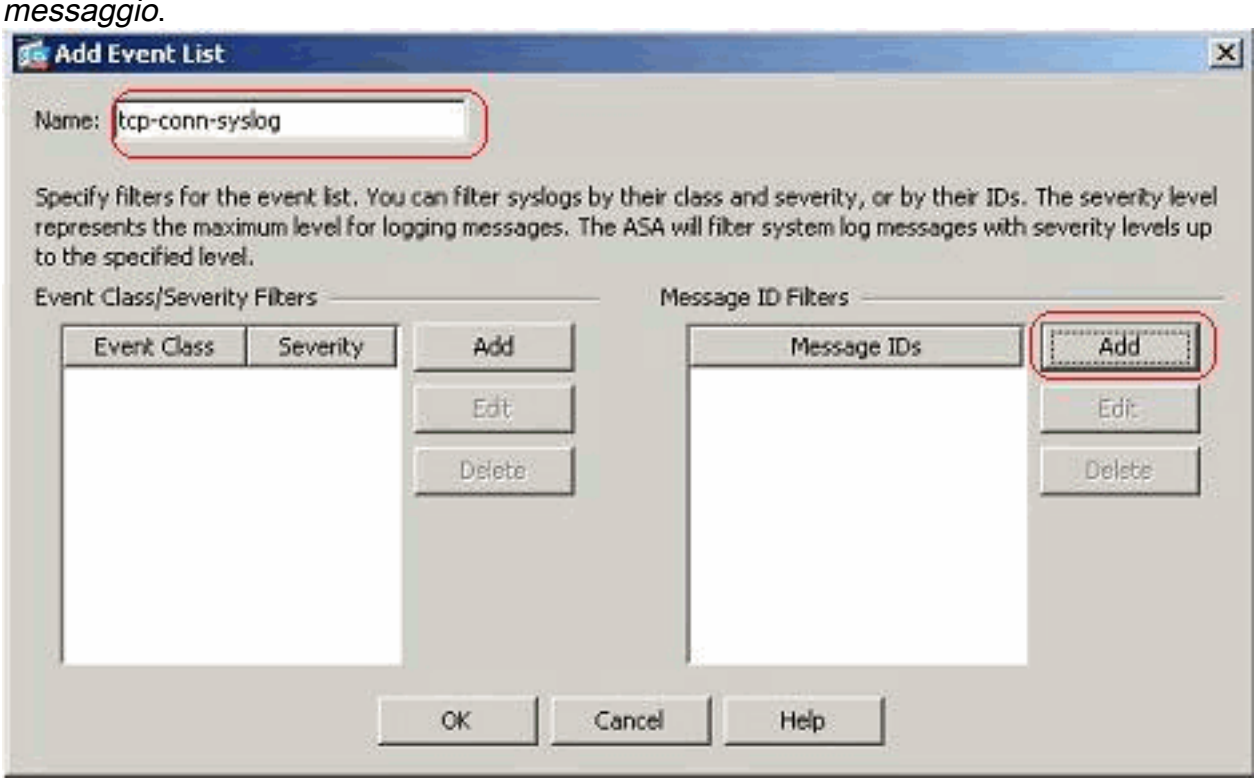
ID messaggio o intervallo di ID messaggio

Attenersi alla procedura seguente:

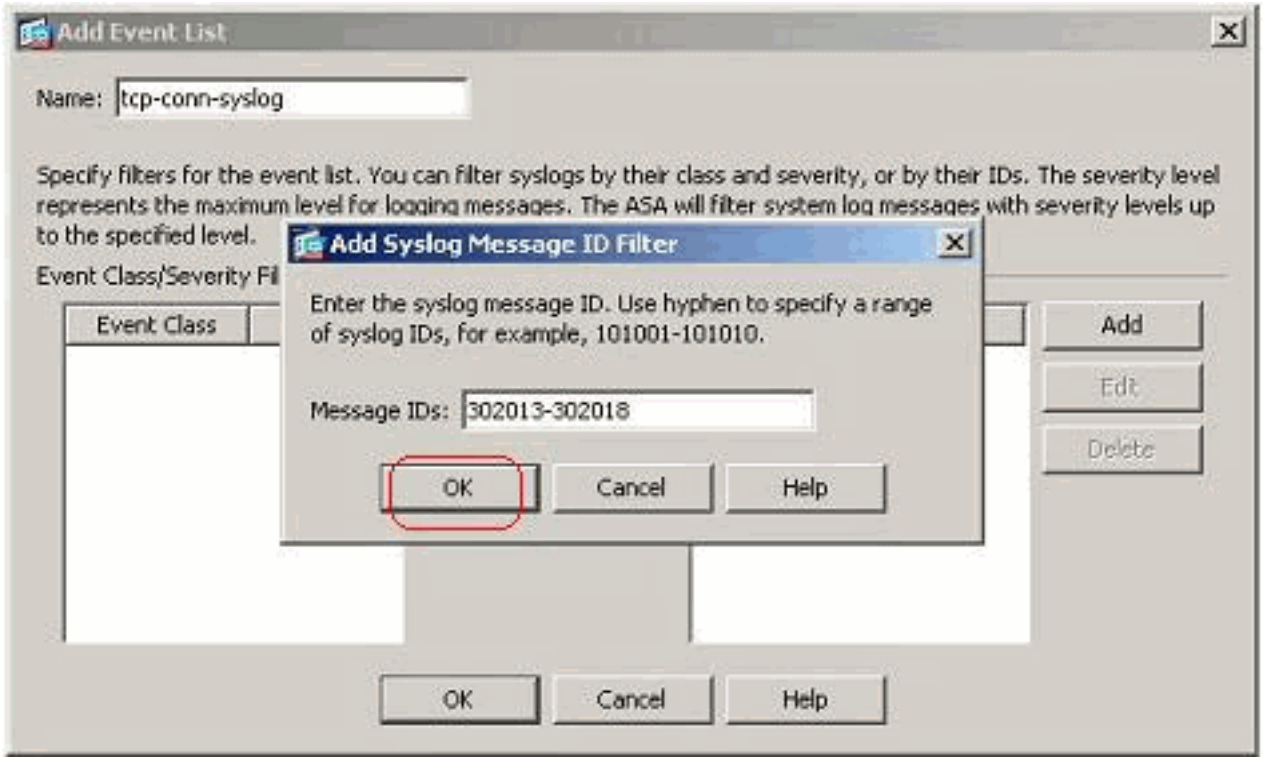
1. Scegliere *Configurazione > Gestione dispositivi > Registrazione > Elenchi eventi* e fare clic su *Aggiungi* per creare un nuovo elenco di eventi.



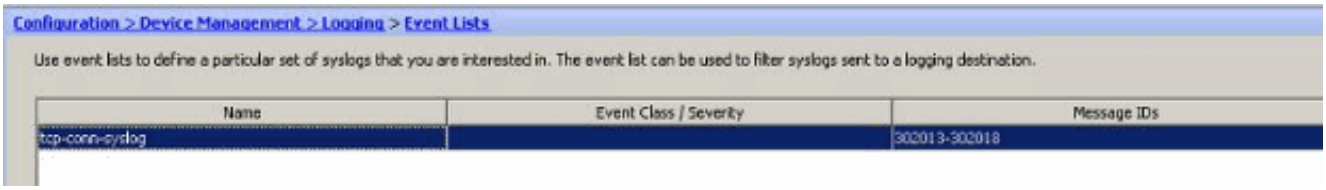
2. Specificare un nome nel campo *Nome*. Per creare un nuovo elenco di eventi, fare clic su *Aggiungi* nel riquadro *Filtri ID messaggio*.



3. Specificare l'intervallo degli ID dei messaggi syslog. Qui i messaggi syslog TCP hanno preso per esempio. Fare clic su *OK* per completare l'operazione.

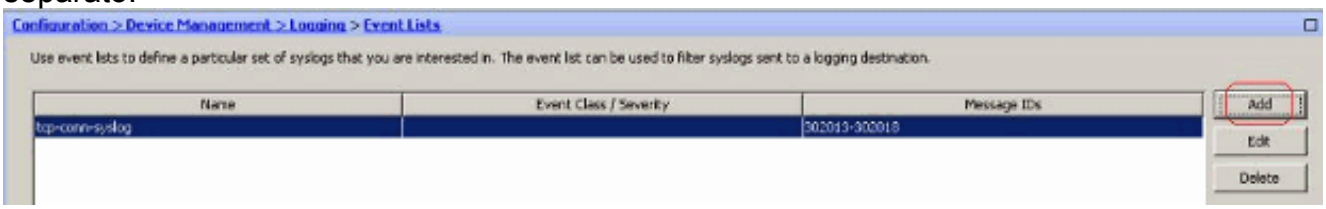


4. Fare di nuovo clic su *OK* per tornare alla finestra *Elenchi eventi*.



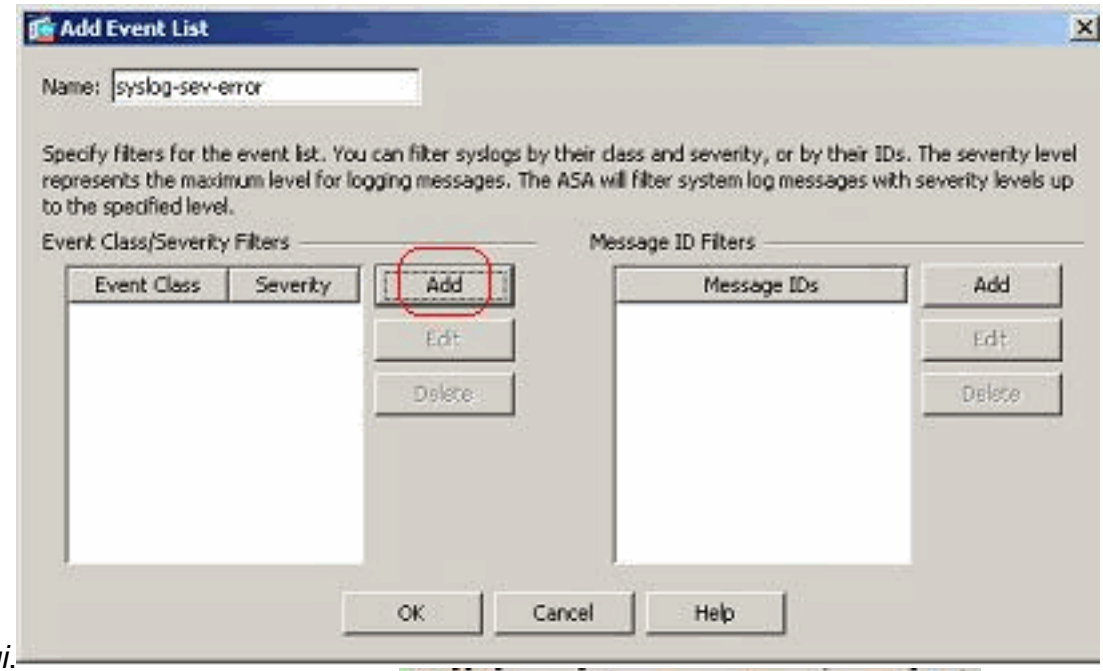
Gravità messaggio

1. Èinoltre possibile definire gli elenchi di eventi in base alla gravità del messaggio. Fare clic su *Add* per creare un elenco di eventi separato.

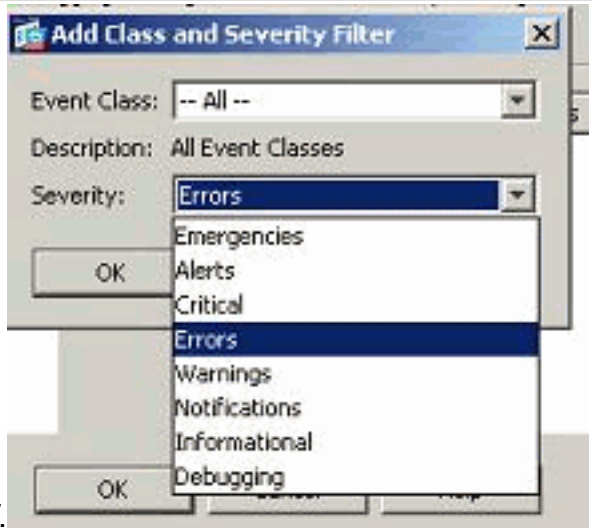


2. Specificare il nome e fare clic su

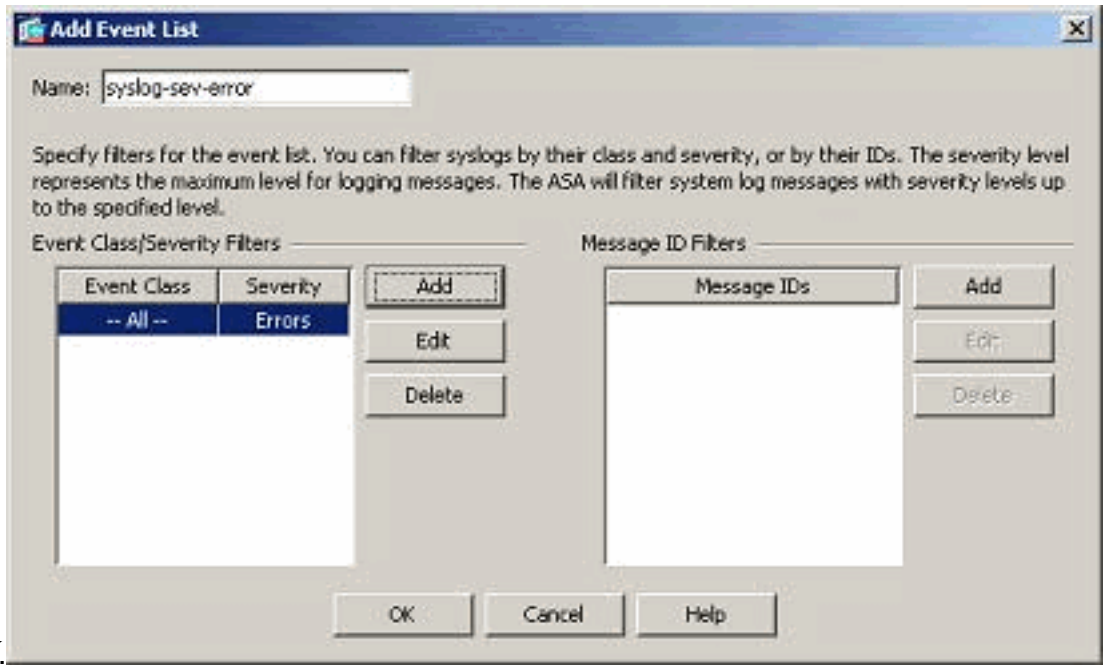
Aggiungi.



3. Selezionare il livello di gravità *Errori*.



4. Fare clic su *OK*.



Classe messaggio

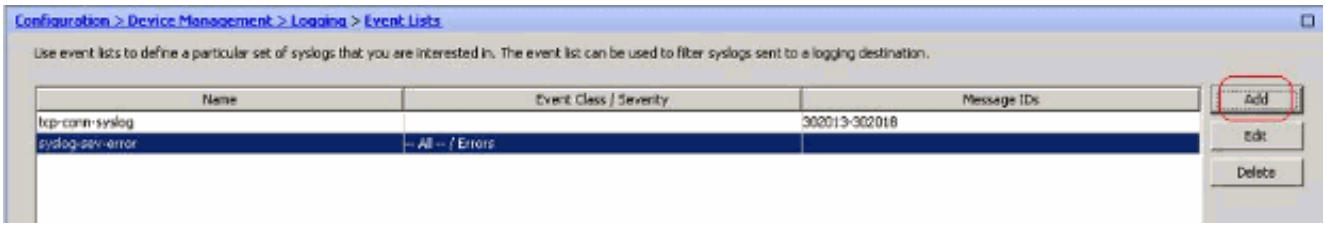
Anche gli elenchi di eventi vengono configurati in base alla classe messaggio. Una classe

messaggio è un gruppo di messaggi syslog correlati a un accessorio di protezione che consente di specificare un'intera classe di messaggi anziché una classe per ogni singolo messaggio. Ad esempio, utilizzare la classe auth per selezionare tutti i messaggi syslog relativi all'autenticazione utente. Di seguito sono elencate alcune classi di messaggi disponibili:

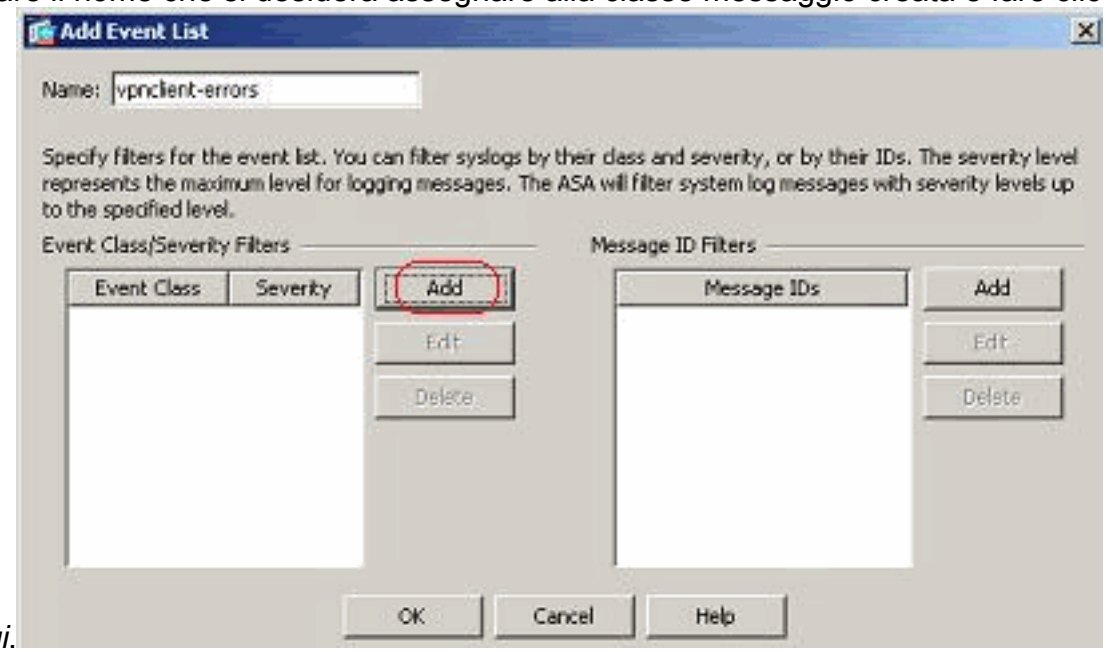
- Tutte: tutte le classi di eventi
- auth - Autenticazione utente
- bridge: firewall trasparente
- ca - Autorità di certificazione PKI
- config—Command Interface
- ha - Failover
- ips - Servizio Intrusion Protection
- ip—Stack IP
- np—Network Processor
- ospf—Routing OSPF
- rip - Routing RIP
- session - Sessione utente

Eseguire la procedura seguente per creare una classe di evento basata sulla classe messaggio *vpnclient-errors*. La classe messaggio, *vpnc*, è disponibile per classificare tutti i messaggi syslog relativi al client vpnc. Il livello di gravità per questa classe messaggio è impostato su "errors".

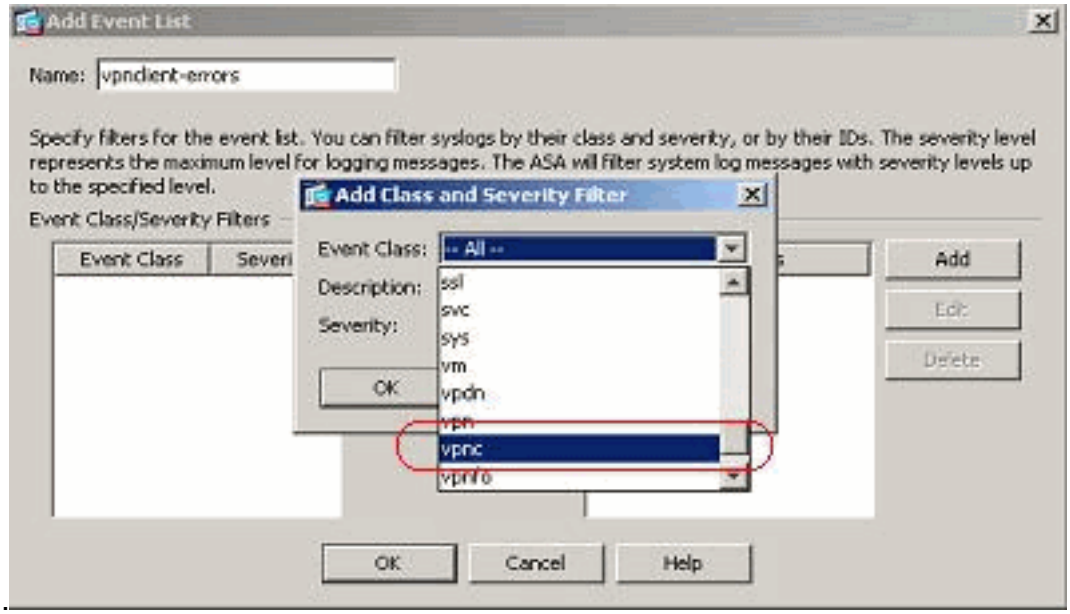
1. Fare clic su Aggiungi per creare un nuovo elenco di eventi.



2. Specificare il nome che si desidera assegnare alla classe messaggio creata e fare clic su *Aggiungi*.

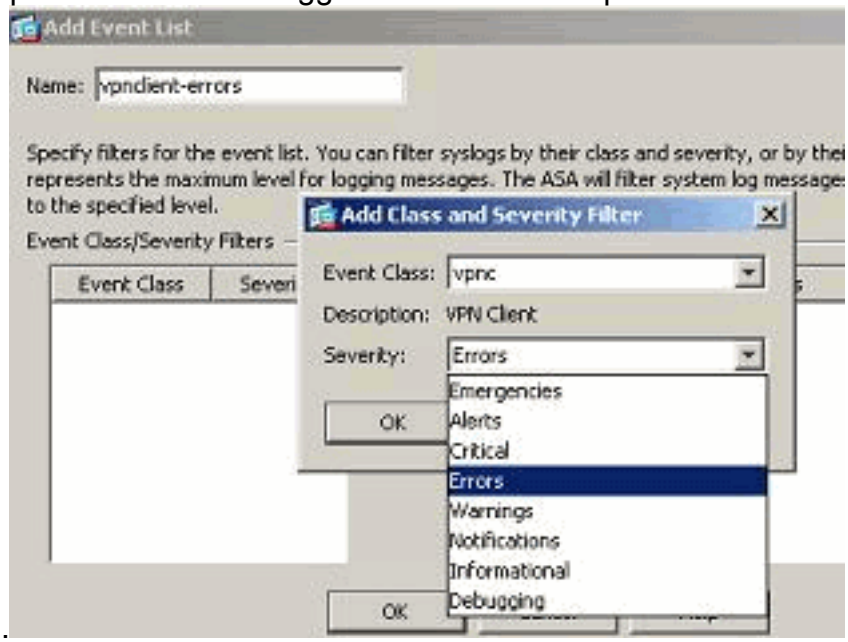


3. Selezionare *vpnc* dall'elenco a



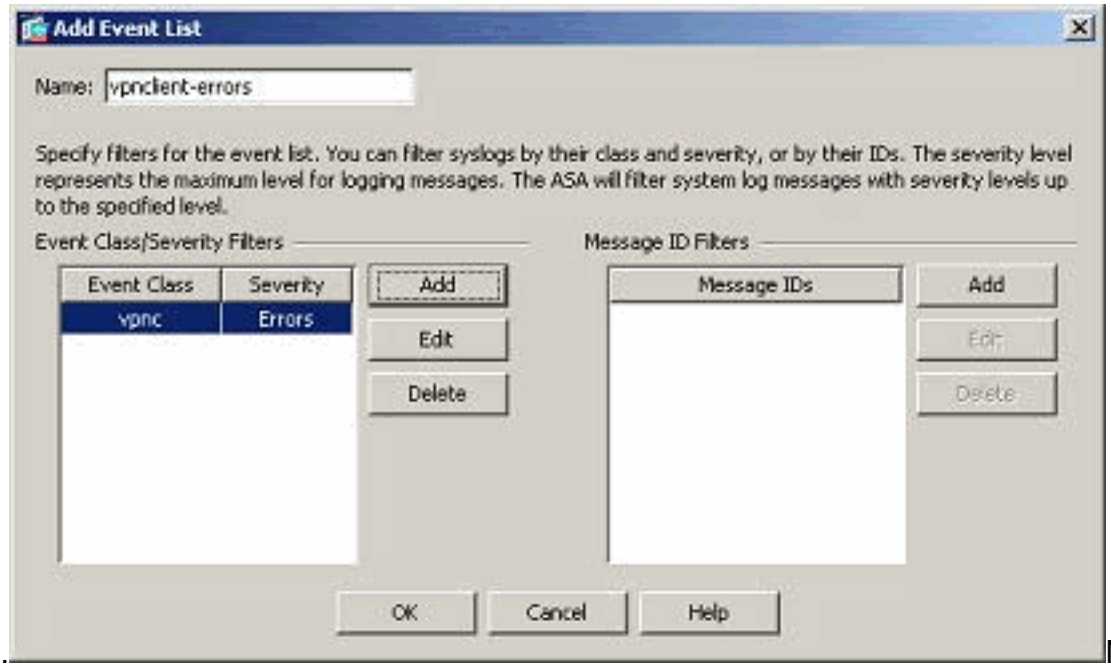
discesa.

4. Selezionare il livello di gravità *Errori*. Questo livello di gravità è applicabile solo ai messaggi registrati per questa classe messaggio. Fare clic su *OK* per tornare alla finestra Aggiungi

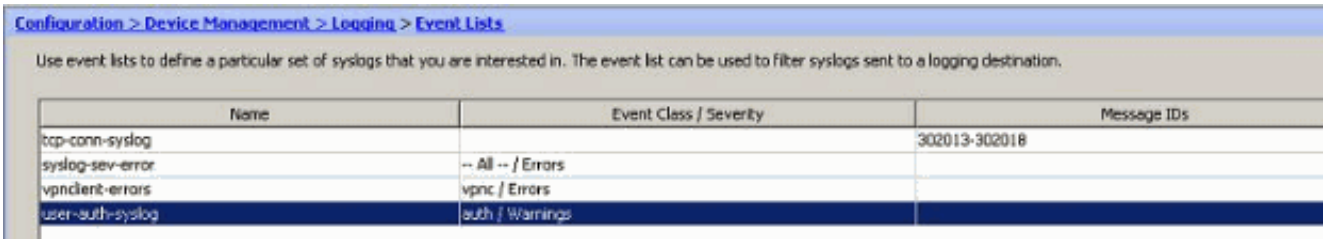


elenco eventi.

5. Di seguito viene riportata la classe/gravità dell'evento. Fare clic su *OK* per completare la configurazione dell'elenco di eventi "vpnclient-



errors".Nello screenshot successivo viene inoltre mostrato come creare un nuovo elenco di eventi, "user-auth-syslog", con una classe messaggio come "auth" e il livello di gravità per i syslog di questa classe messaggio specifica come "Warnings". Configurando questa opzione, l'elenco degli eventi specifica tutti i messaggi syslog correlati alla classe messaggio "auth", con livelli di gravità **fino al** livello "Warnings".**Nota:** qui, il termine "fino a" è di significato. Nel definire il livello di gravità, tenere presente che tutti i messaggi syslog verranno registrati fino a quel livello.**Nota:** un elenco di eventi può contenere più classi di eventi. L'elenco di eventi "vpnclient-errors" viene modificato facendo clic su **Edit** e definendo una nuova classe di eventi
"ssl/error".



Utilizzo dei filtri di registrazione

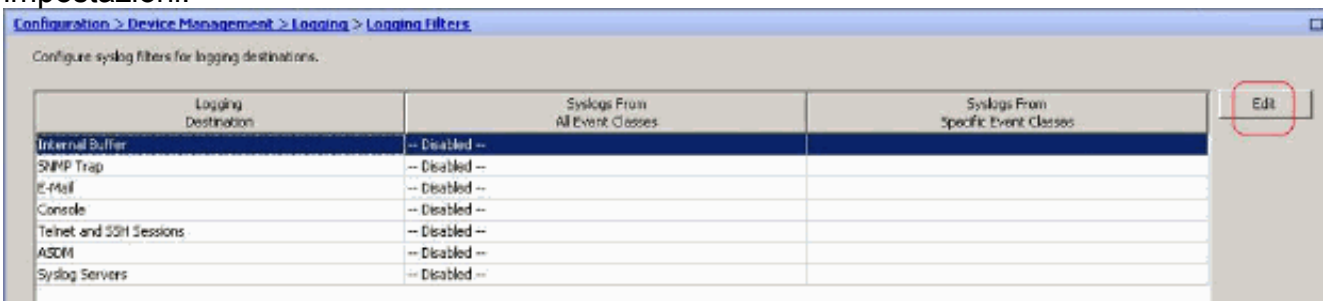
I filtri di registrazione vengono utilizzati per inviare i messaggi syslog a una destinazione specificata. I messaggi syslog possono essere basati sulla "gravità" o sugli "elenchi pari".

Di seguito sono riportati i tipi di destinazione a cui i filtri sono applicabili:

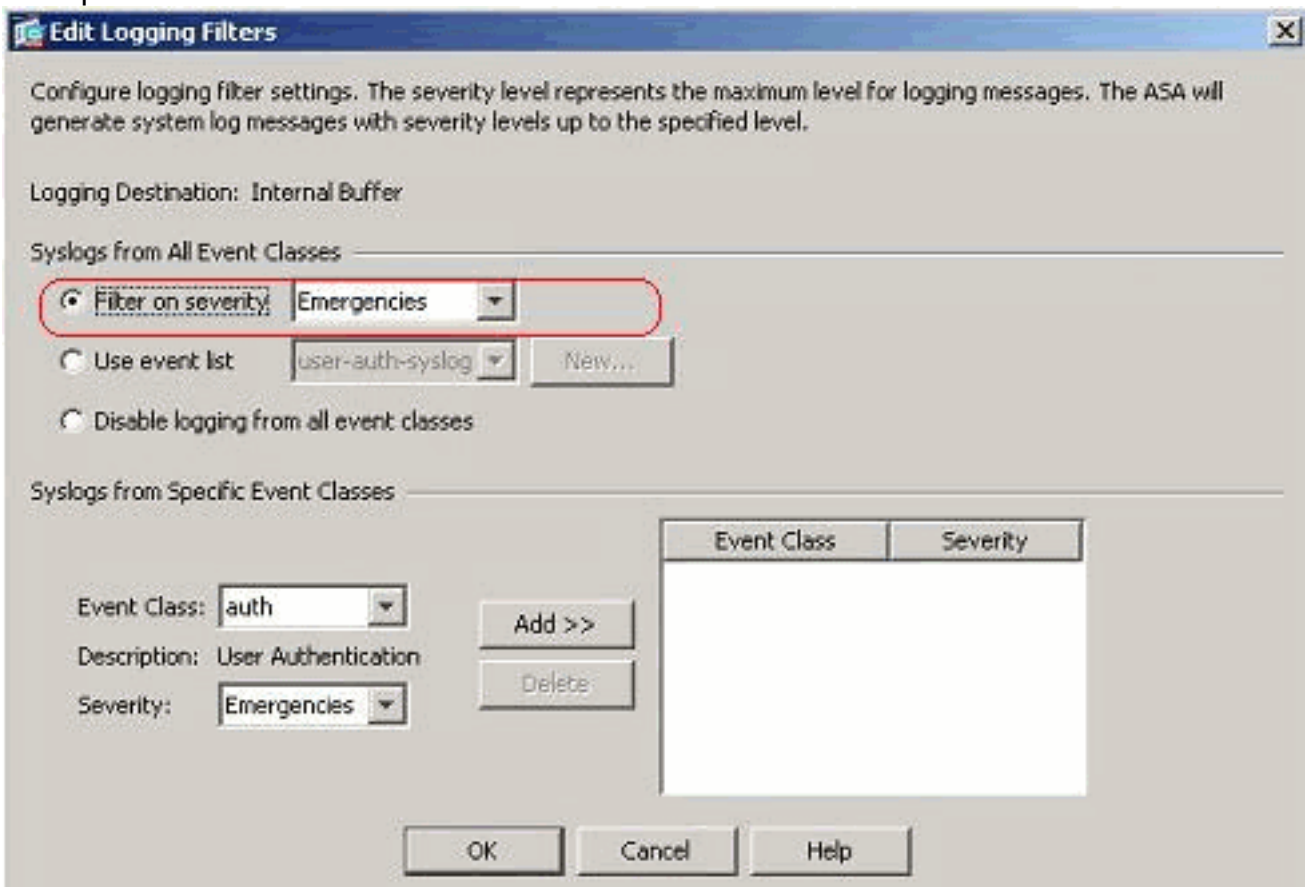
- Buffer interno
- Trap SNMP
- E-mail
- Console
- Sessioni Telnet
- ASDM
- Server Syslog

Attenersi alla procedura seguente:

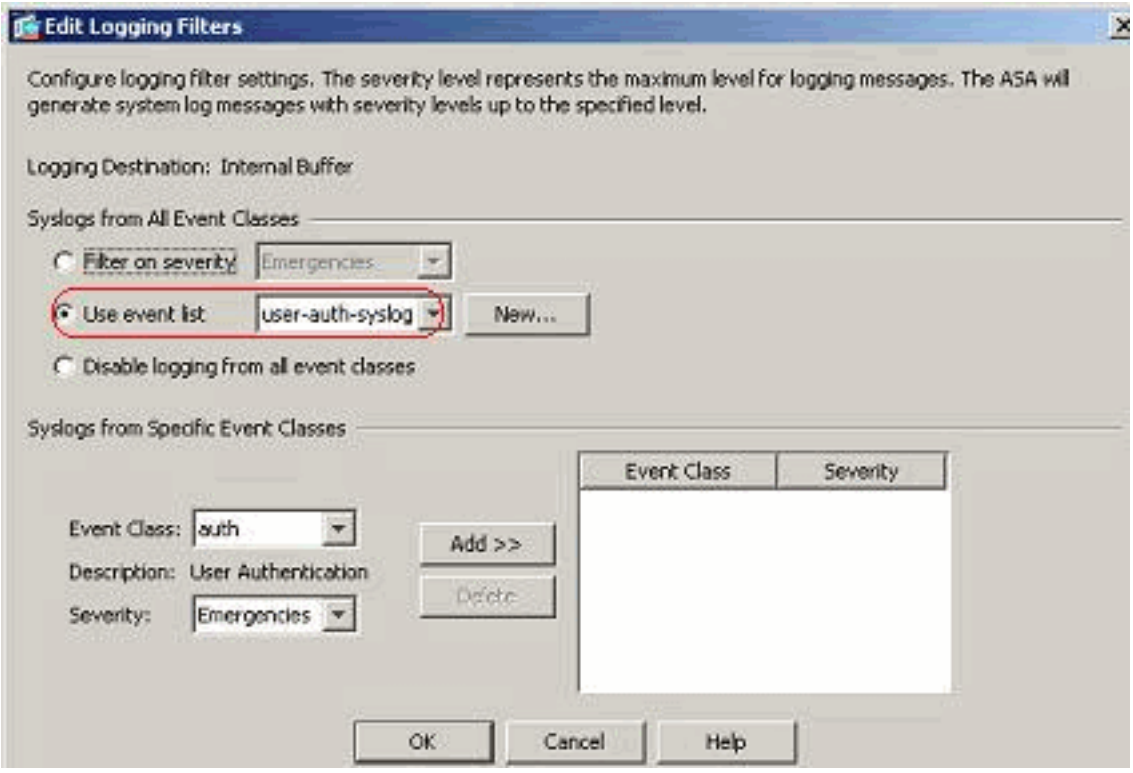
1. Scegliere **Configurazione > Gestione dispositivi > Registrazione > Filtri di registrazione** e selezionare la destinazione di registrazione. Fare quindi clic su **Modifica** per modificare le impostazioni.



2. Èpossibile inviare i messaggi syslog in base alla gravità. In questo caso, **Emergenze** è stato selezionato come
esempio.

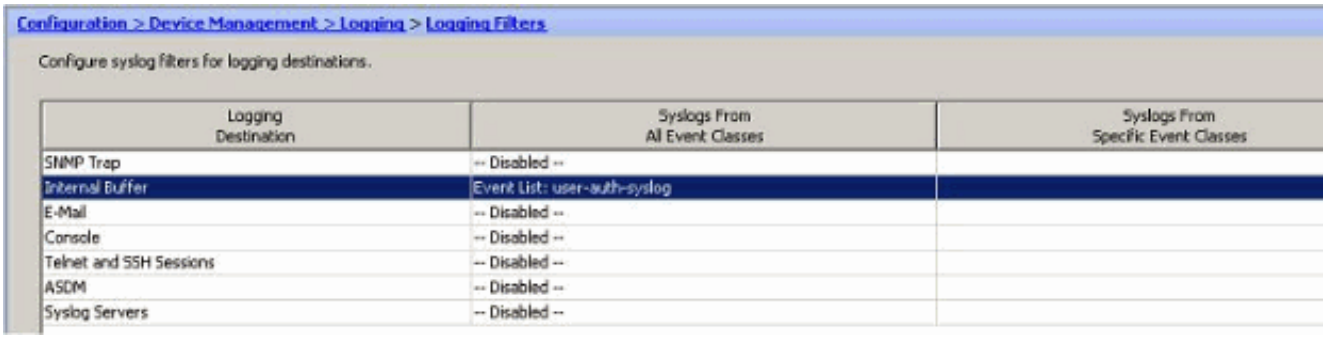


3. Èinoltre possibile selezionare un elenco di eventi per specificare il tipo di messaggi da inviare a una particolare destinazione. Fare clic su



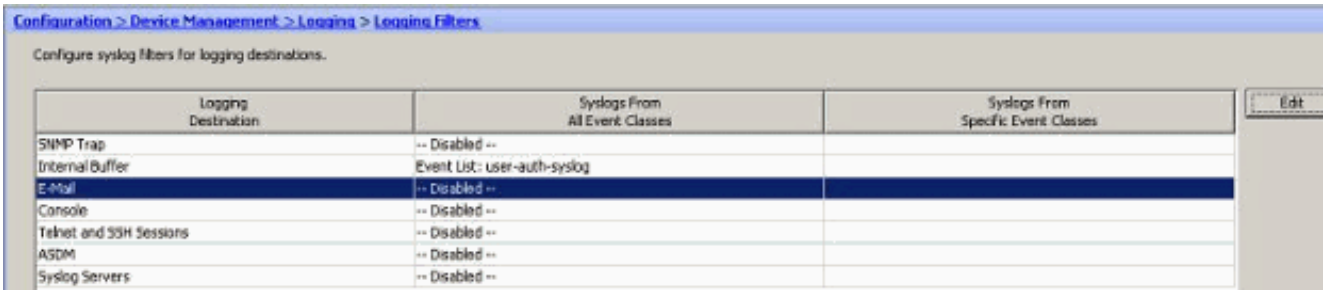
OK.

4. Verificare la modifica.

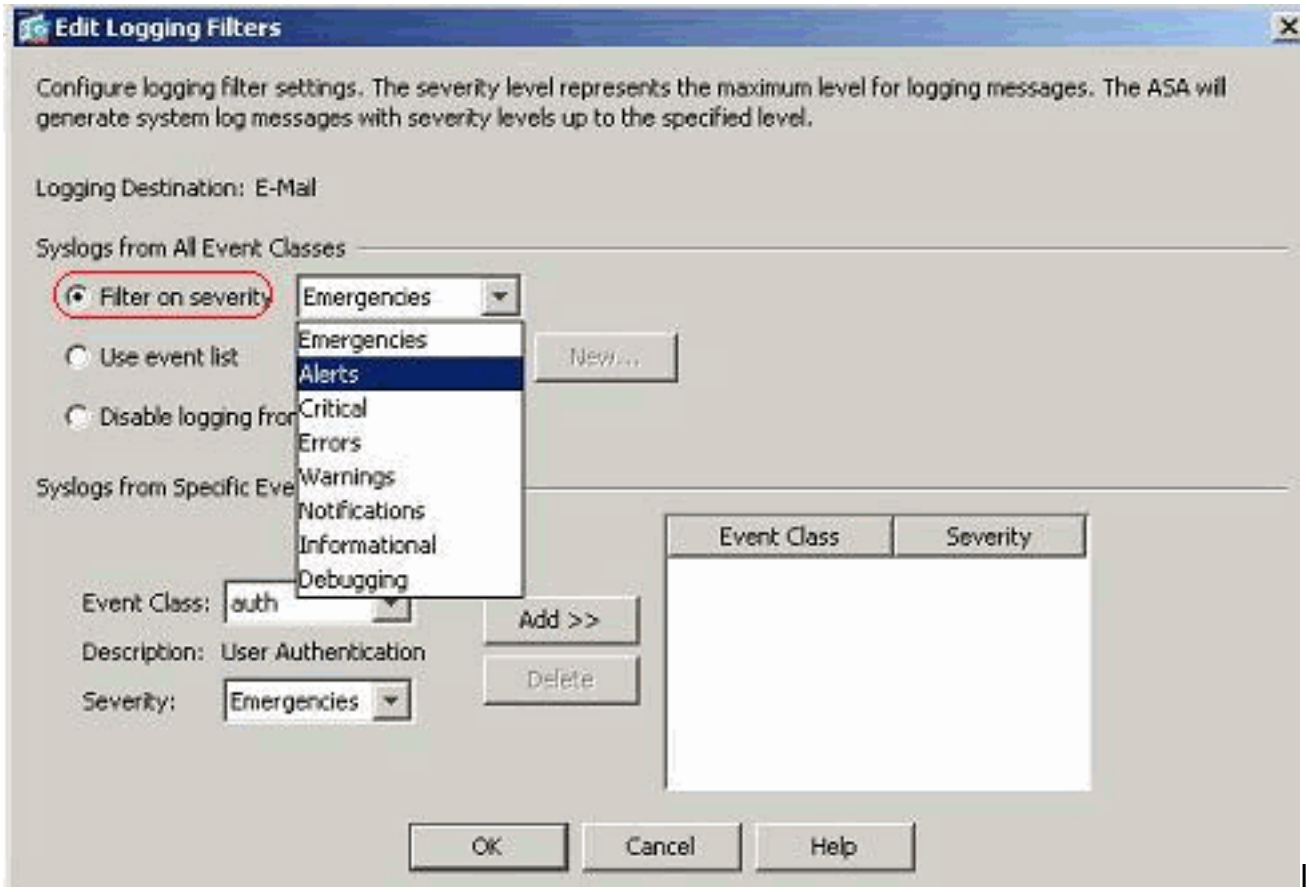


Di seguito viene descritto come inviare un gruppo di messaggi al server di posta elettronica in base al livello di gravità.

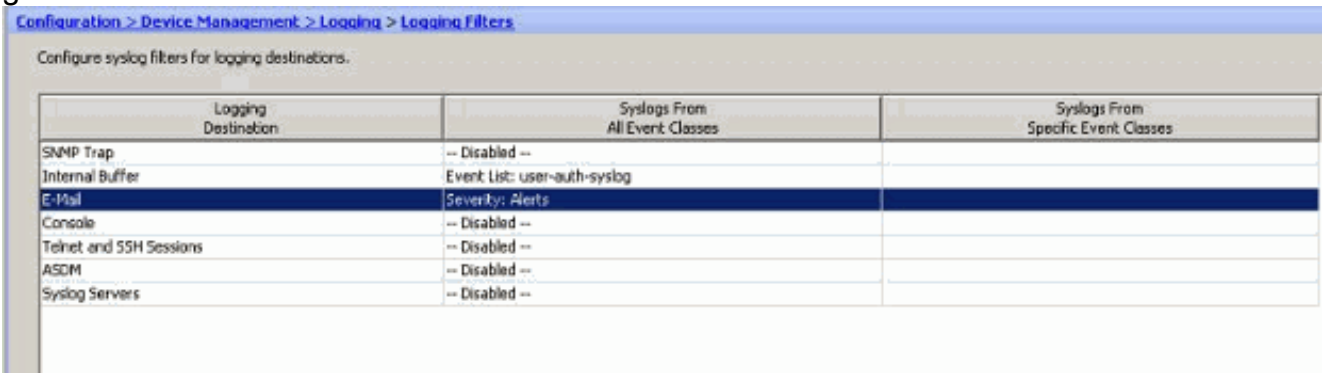
1. Selezionare **E-mail** nel campo Destinazione registrazione. Fare quindi clic su **Modifica**.



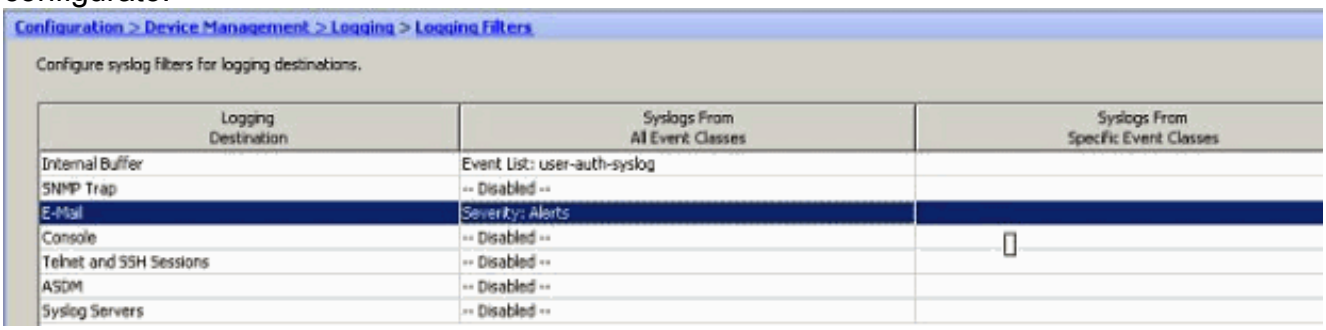
2. Scegliere l'opzione **Filtra in base alla gravità** e selezionare il livello di gravità richiesto.



n questo caso, **Alert** è stato selezionato come livello di gravità.



Tutti i messaggi del syslog di avviso devono essere inviati al messaggio di posta elettronica configurato.

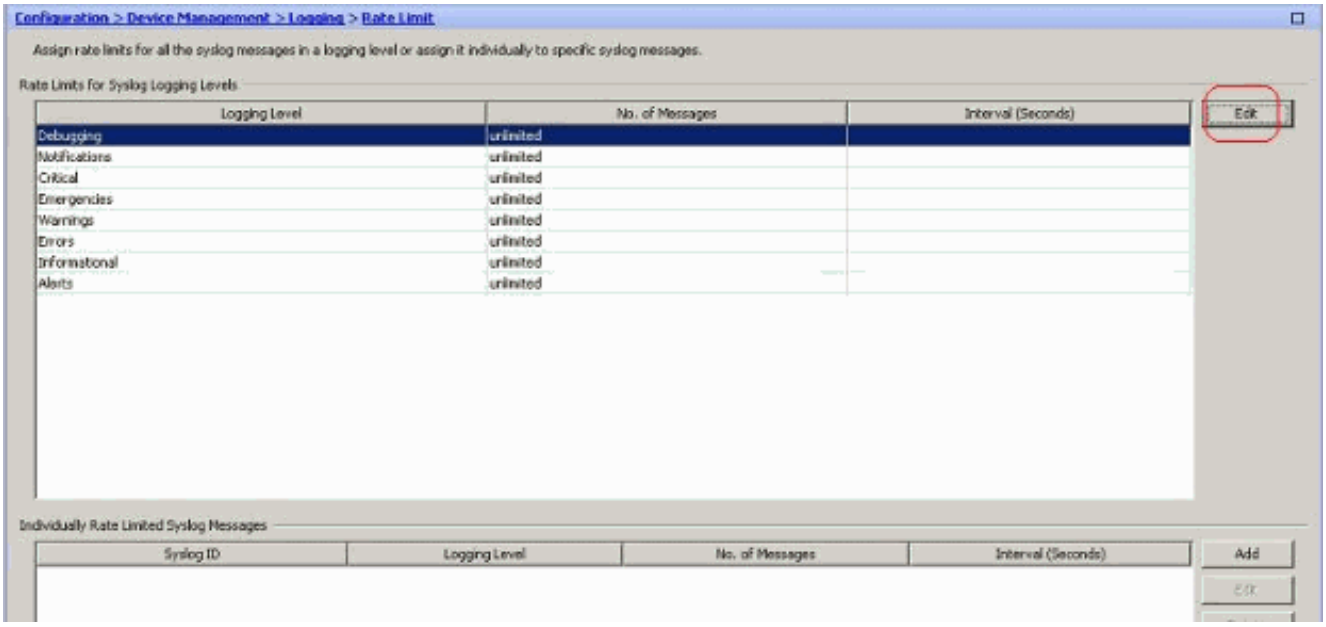


Limite di velocità

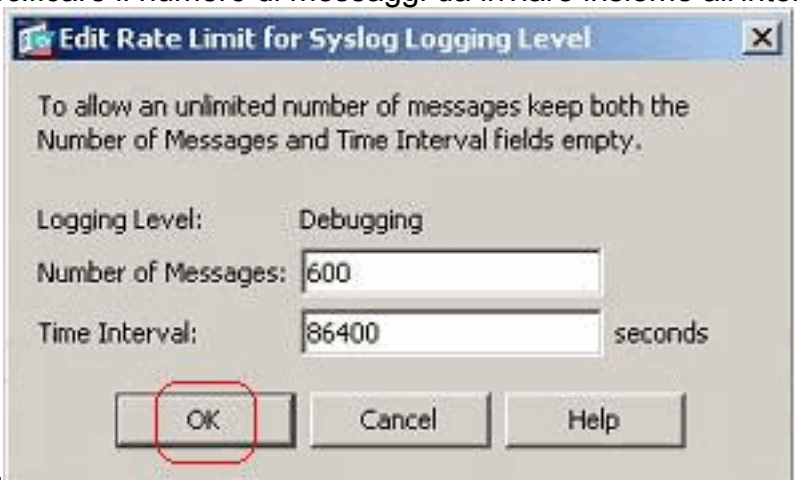
Questo valore specifica il numero di messaggi syslog che un'appliance Cisco ASA invia a una destinazione in un periodo di tempo specificato. In genere è definito per il livello di gravità.

1. Scegliere **Configurazione > Gestione dispositivi > Registrazione > Limite velocità** e

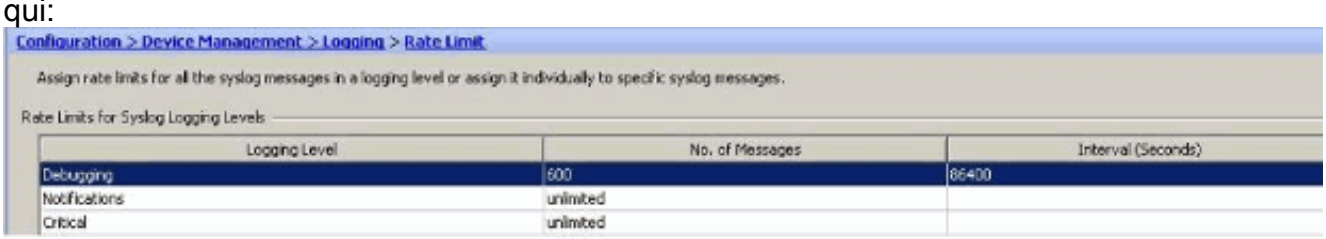
selezionare il livello di gravità richiesto. Fare quindi clic su **Modifica**.



2. Specificare il numero di messaggi da inviare insieme all'intervallo di tempo. Fare clic su **OK**.



Nota: questi numeri sono riportati a titolo di esempio. Queste variano a seconda del tipo di ambiente di rete.I valori modificati sono visualizzati qui:

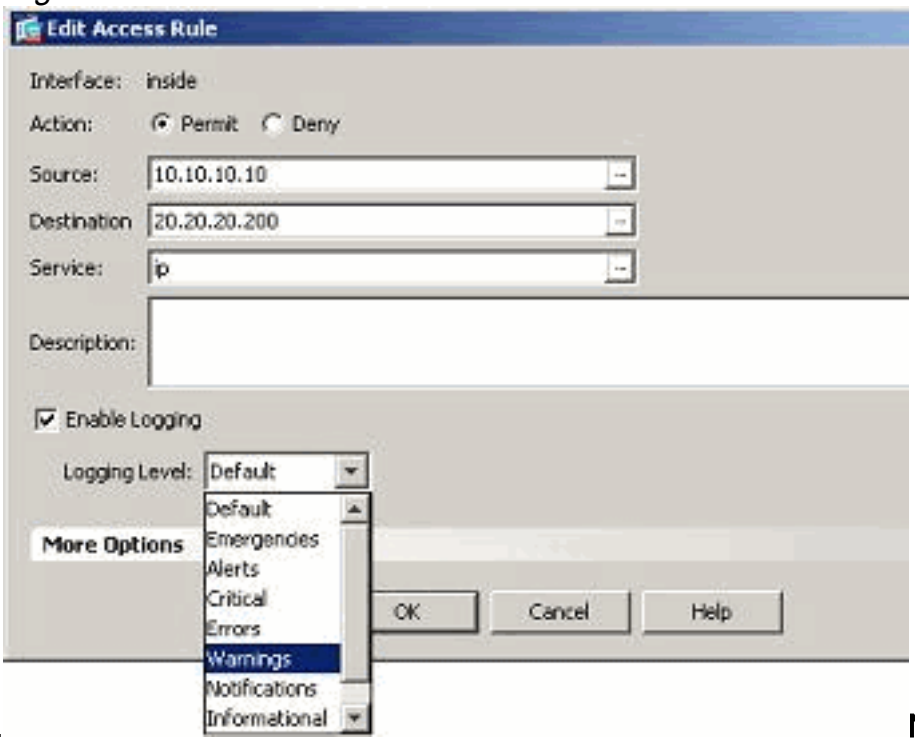


Registrazione dei riscontri di una regola di accesso

Èpossibile registrare i risultati della regola di accesso utilizzando ASDM. Il comportamento predefinito della registrazione consiste nell'inviare un messaggio syslog per tutti i pacchetti negati. Non verrà visualizzato alcun messaggio di syslog per i pacchetti consentiti che non verranno registrati. Tuttavia, è possibile definire un livello di gravità di registrazione personalizzato per la regola di accesso, in modo da tenere traccia del numero di pacchetti che raggiungono questa regola di accesso.

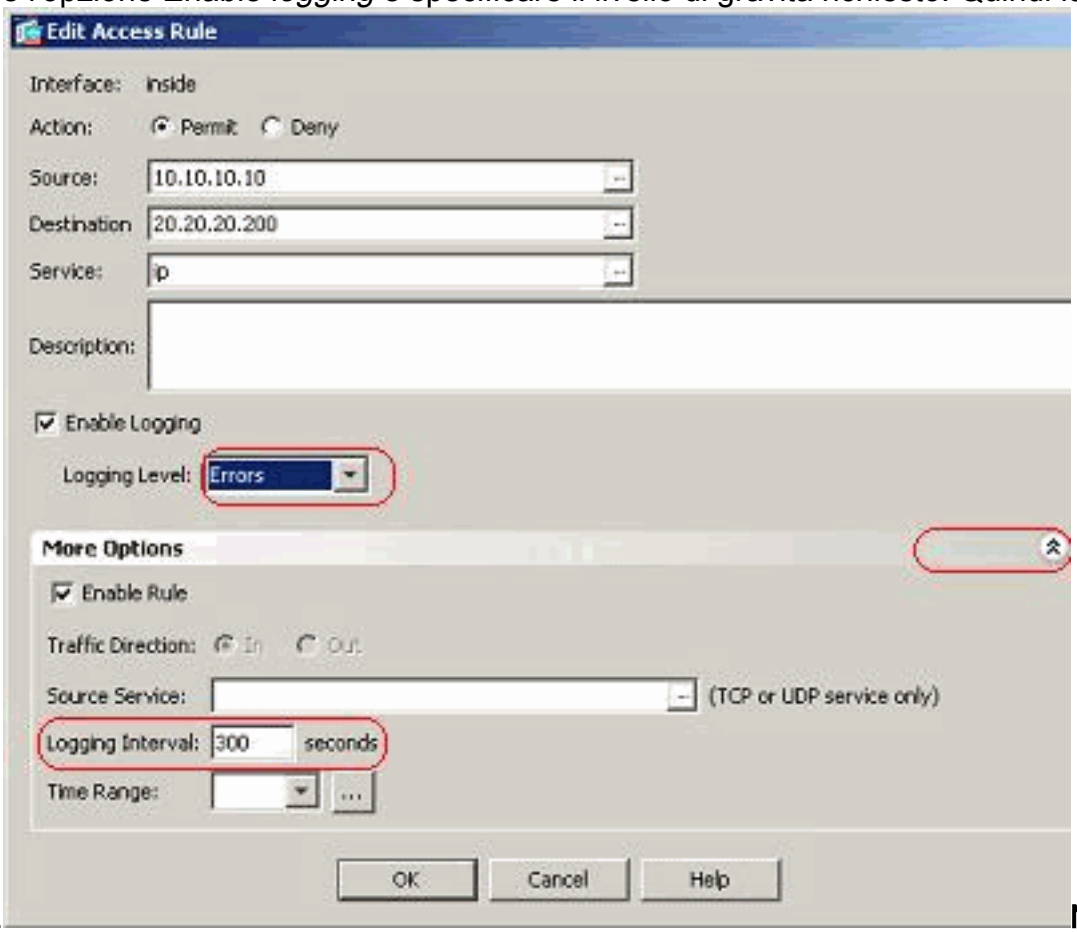
Attenersi alla procedura seguente:

1. Selezionare la regola di accesso richiesta e fare clic su *Modifica*.Verrà visualizzata la finestra *Modifica regola di accesso*.



Nota: in questa immagine, l'opzione *Default* nel campo *Logging Level (Livello di registrazione)* indica il comportamento di registrazione predefinito di Cisco ASA. Per ulteriori informazioni su questo argomento, fare riferimento alla sezione Attività dell'elenco accessi alla registrazione.

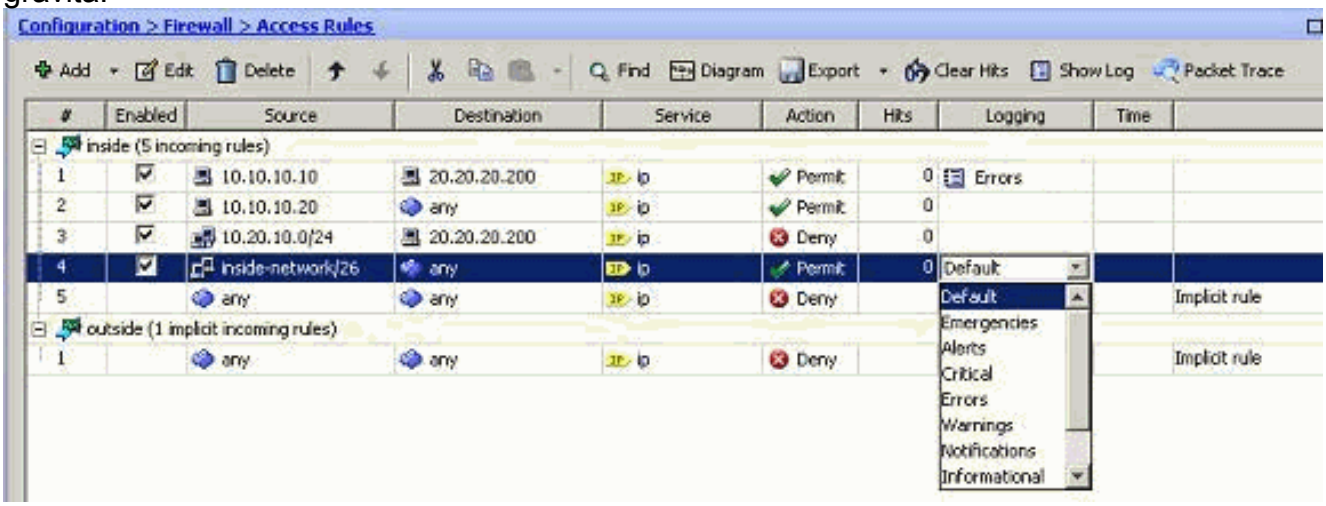
2. Selezionare l'opzione *Enable logging* e specificare il livello di gravità richiesto. Quindi fare clic su *OK*.



Nota: facendo clic sulla scheda a discesa *Altre opzioni*, è possibile visualizzare l'opzione *Intervallo di registrazione*. Questa opzione è evidenziata solo quando l'opzione *Abilita log* sopra riportata è selezionata. Il valore predefinito del timer è 300 secondi. Questa impostazione è

utile per specificare il valore di timeout per le statistiche di flusso da eliminare quando non esiste una corrispondenza per la regola di accesso. In caso di riscontri, l'ASA attende l'intervallo di registrazione e lo invia al syslog.

3. Le modifiche sono illustrate di seguito. In alternativa, è possibile fare doppio clic sul campo *Registrazione* della regola di accesso specifica e impostare il livello di gravità.



Nota: questo metodo alternativo per specificare il *livello di log* nello stesso riquadro *Regole di accesso* facendo doppio clic funziona solo per le voci delle regole di accesso create manualmente, ma non per le regole implicite.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Configurazioni

Nel documento vengono usate queste configurazioni:

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
```

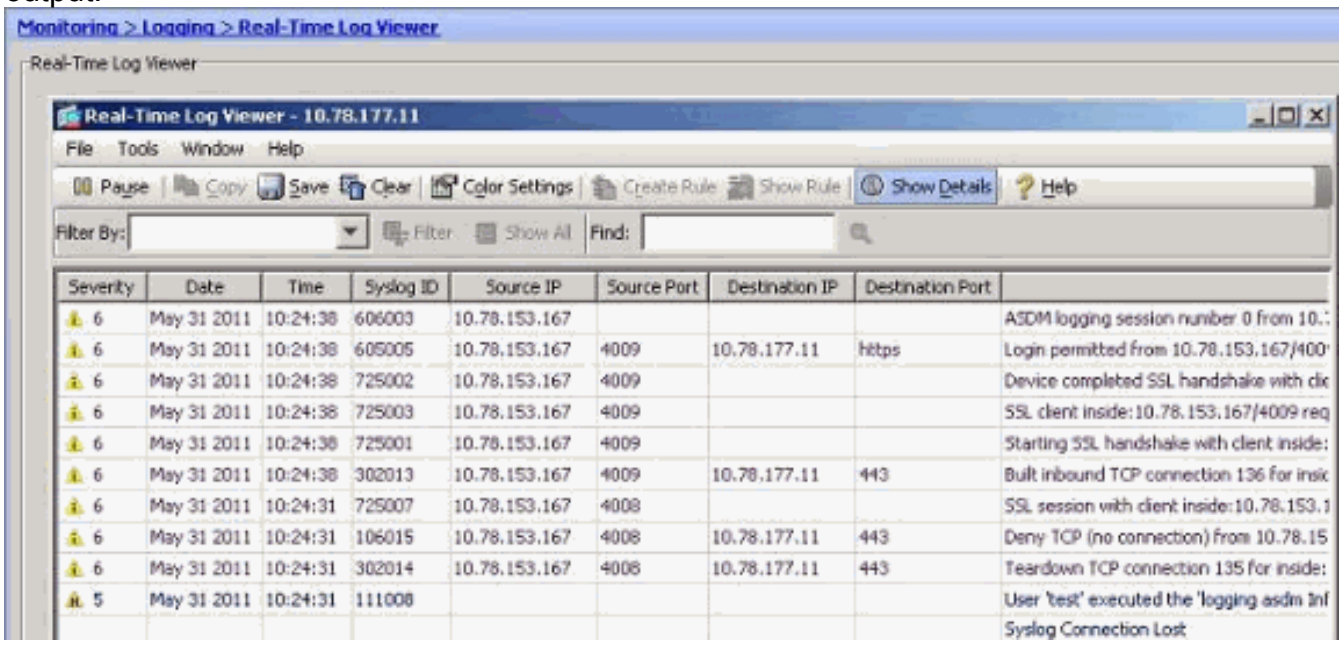
```
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global smtp-server 172.18.10.20
prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4
: end
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- Èpossibile visualizzare i syslog da ASDM. Scegliere **Monitoraggio > Log > Visualizzatore log in tempo reale**. Di seguito è riportato un esempio di output:



Risoluzione dei problemi

Problema: Connessione interrotta — Connessione syslog terminata —

Questo errore viene visualizzato quando si tenta di abilitare la registrazione ASDM nel dashboard dei dispositivi per uno qualsiasi dei contesti.

```
"Connessione interrotta – Connessione syslog terminata –"
```

Quando ASDM viene utilizzato per connettersi direttamente al contesto di amministrazione e la registrazione ADSM è disabilitata in questo contesto, passare a un sottocontesto e abilitare la registrazione ASDM. Gli errori vengono ricevuti, ma i messaggi syslog stanno raggiungendo il server syslog.

Soluzione

Questo è un comportamento noto di Cisco ASDM e documentato nell'ID bug Cisco CSCsd10699

(solo utenti registrati). Per risolvere il problema, abilitare la registrazione asdm quando si è connessi al contesto di amministrazione.

Impossibile visualizzare i log in tempo reale su Cisco ASDM

Il problema è che i log in tempo reale non possono essere visualizzati su ASDM. Come viene configurato?

Soluzione

Configurare quanto segue sull'appliance Cisco ASA:

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

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance Support
- Documentazione e supporto tecnico – Cisco Systems