ASA 8.2: Configureren met ASDM

Inhoud

Inleiding

Dit document bevat informatie over de manier waarop u inline voeding op Cisco adaptieve security applicatie (ASA) 8.x kunt configureren door gebruik te maken van de ASDM GUI (Adaptieve Security Devices Manager). De logberichten van het systeem zijn de berichten die door Cisco ASA worden gegenereerd om de beheerder op de hoogte te stellen van elke verandering in de configuratie, veranderingen in netwerkinstelling of veranderingen in de prestaties van het apparaat. Door de systeemmeldingen te analyseren, kan een beheerder de fout eenvoudig oplossen door een analyse van de basisoorzaak uit te voeren.

De syslogberichten zijn voornamelijk gedifferentieerd op basis van hun ernst.

1. Ernst 0 - Noodberichten - hulpbron is niet bruikbaar
2. Ernst 1 - waarschuwingsberichten - Er is onmiddellijke actie nodig

3. Severity 2 - Critical Messaging - Critici ervan
4. Severity 3 - foutmeldingen - foutenvoorwaarden
5. Ernst 4 - Waarschuwingsberichten - Waarschuwingsvoorwaarden
6. Ernst 5 - Meldingsberichten - Normale maar belangrijke voorwaarden
7. Ernst 6 - Informatieberichten - Alleen informatieve berichten
8. Ernst 7 - Afluisterberichten - alleen afluisterberichten**Opmerking:** Het hoogste ernst niveau is een noodgeval en het laagste ernst niveau is het fouilleren.

De voorbeeldsignalen die door Cisco ASA zijn gegenereerd worden hier weergegeven:

- %ASA-6-106012: Ontken IP van IP_adres naar IP_adres, IP opties hex.
- %ASA-3-21001: Geheugentoewijzingsfout
- %ASA-5-33503: Standaard NAC-ACL-toepassing: ACL-naam - host-adres

De numerieke waarde X gespecificeerd in "%ASA-X-YYYYY:", geeft de ernst van het bericht aan. Bijvoorbeeld, "%ASA-6-106012" is een Informatief bericht en "%ASA-5-35003" is een foutbericht.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA versie 8.2
- Cisco ASDM versie 6.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

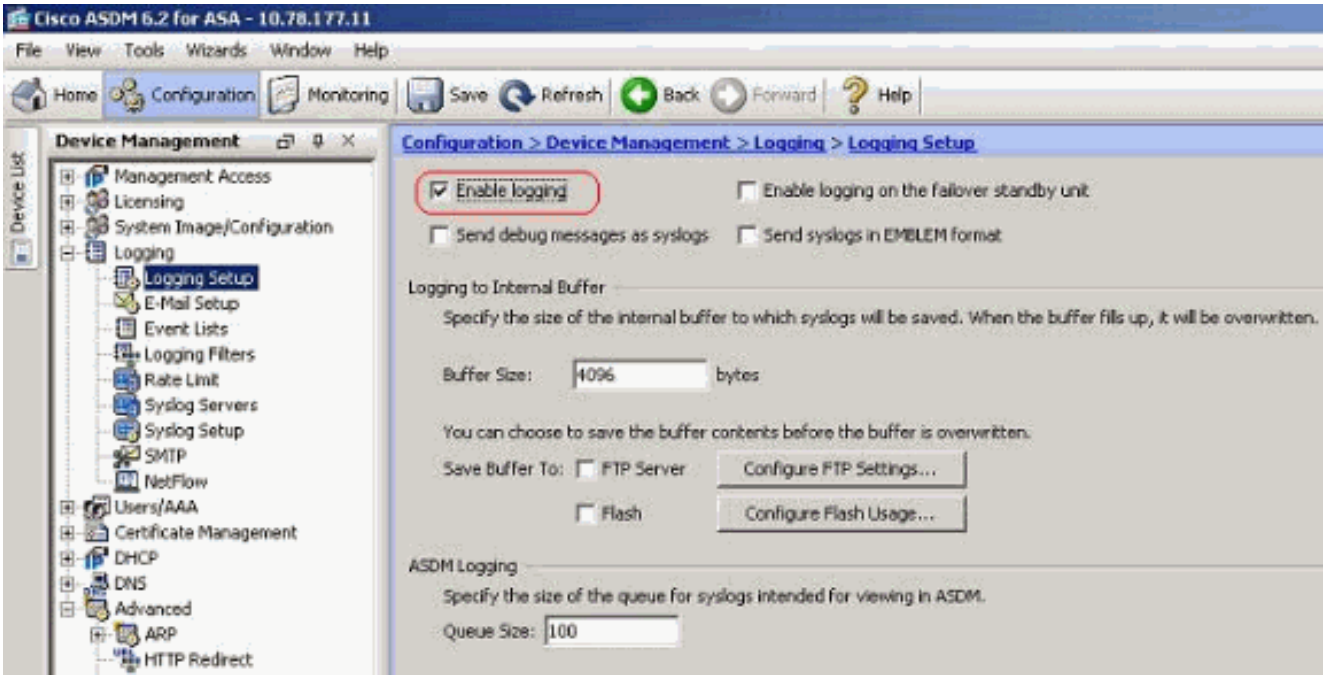
Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Basisconfiguratie van het systeem via ASDM

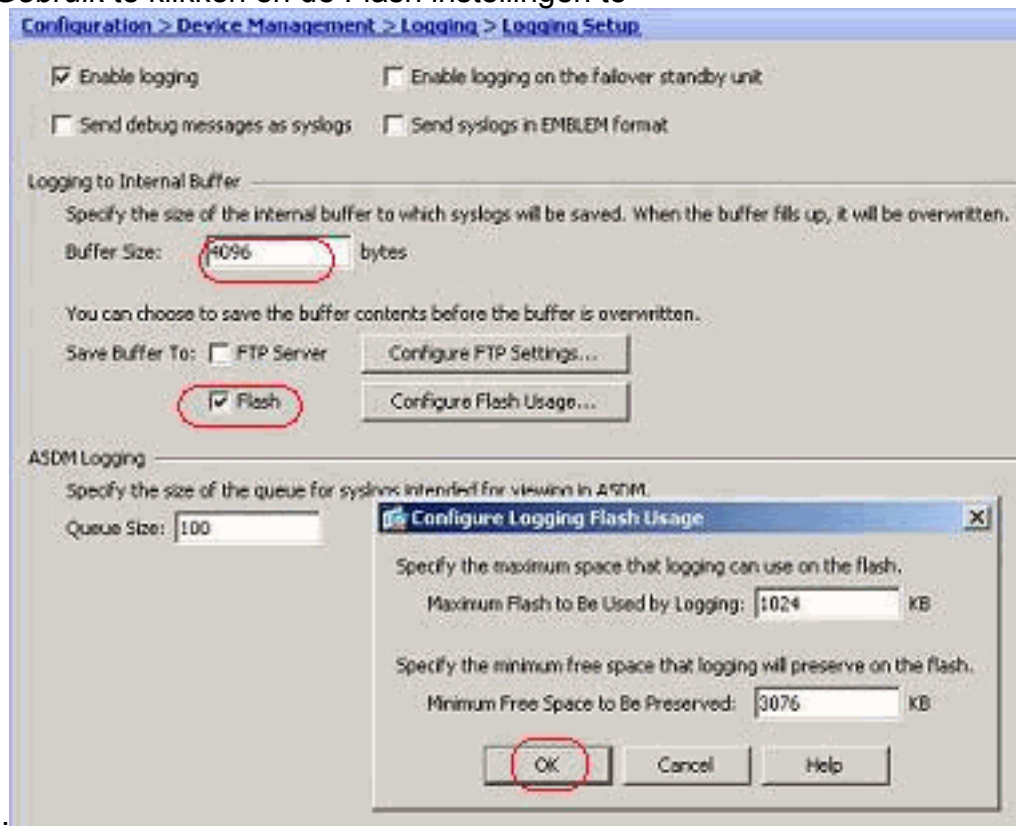
Vastlegging inschakelen

Voer de volgende stappen uit:

1. Kies *Configuratie > Apparaatbeheer > Vastlegging > Instellen vastlegging* en controleer de optie *houtkap inschakelen*.

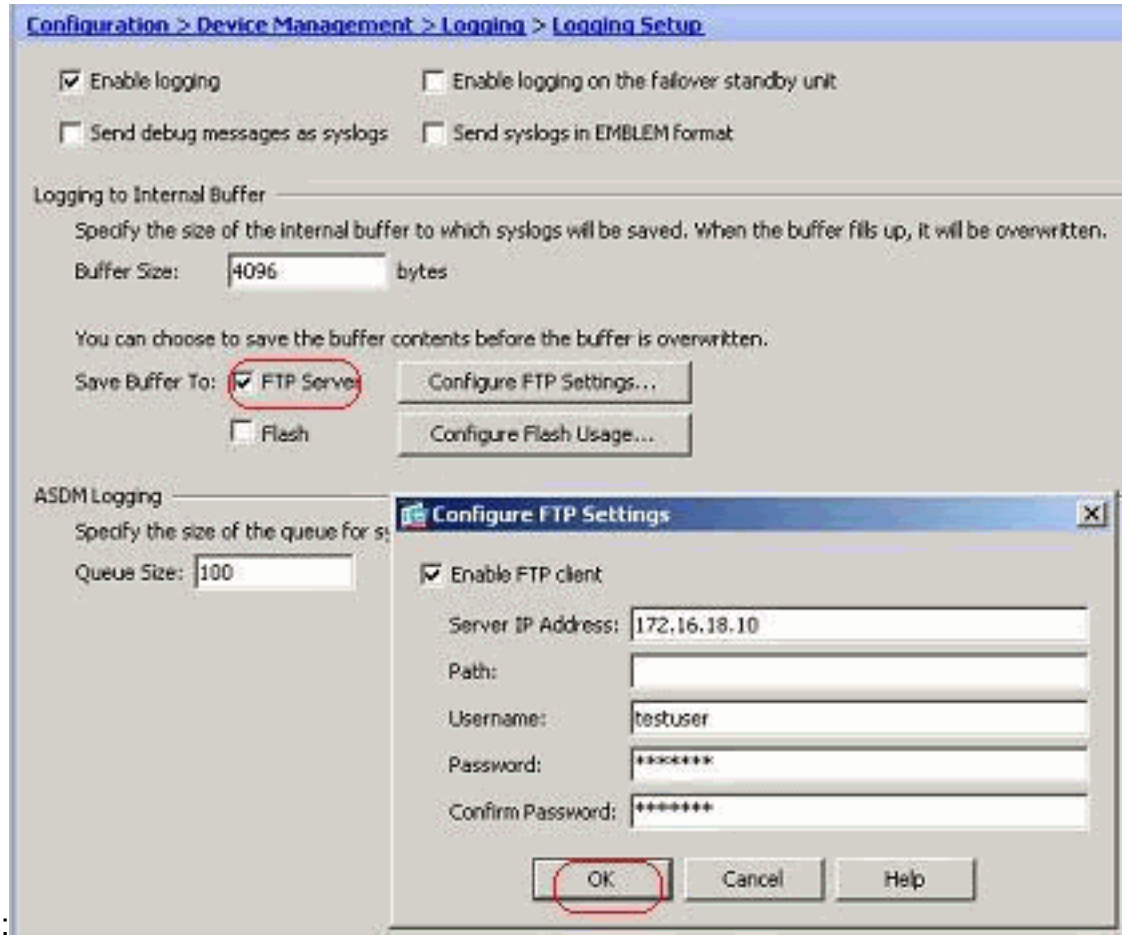


2. U kunt de syslogberichten aan een interne buffer registreren door de buffergrootte te specificeren. U kunt ook kiezen om de bufferinhoud op te slaan naar Flash geheugen door op *Flash Gebruik* te klikken en de Flash instellingen te definiëren.



3. De gebufferde logberichten kunnen naar een FTP server worden verzonden voordat ze worden overschreven. Klik op *Instellen FTP-instellingen* en specificeer de FTP-serverdetails zoals hieronder wordt

weergegeven:

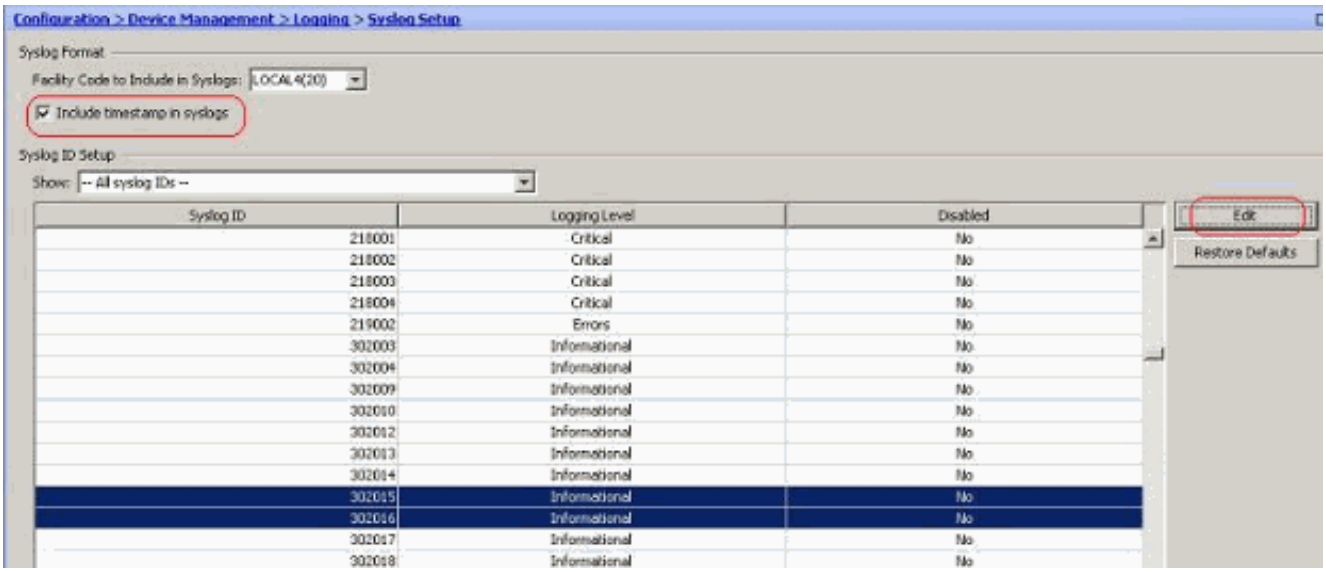


Vastlegging uitschakelen

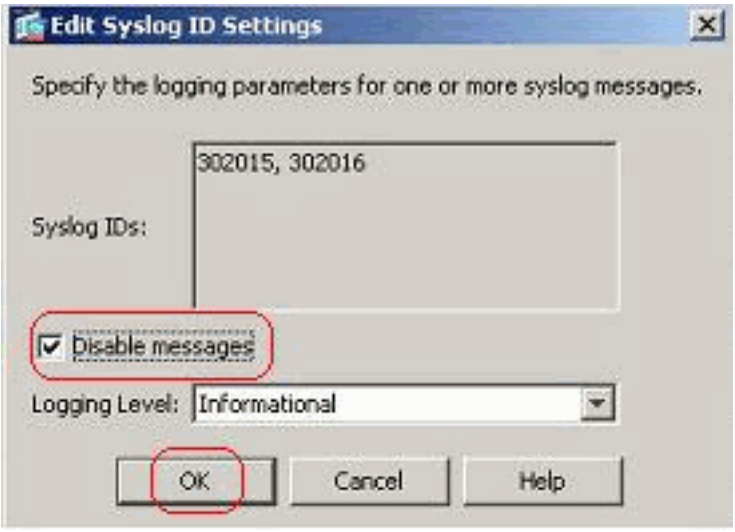
U kunt specifieke syslg-ID's op basis van uw vereisten uitschakelen.

Opmerking: door de selectieteken voor de optie *timestamp in syslogs* toe te voegen, kunt u de datum en de tijd toevoegen dat ze als een veld aan de syslogs gegenereerd zijn.

1. Selecteer de systemen om uit te schakelen en klik op *Bewerken*.

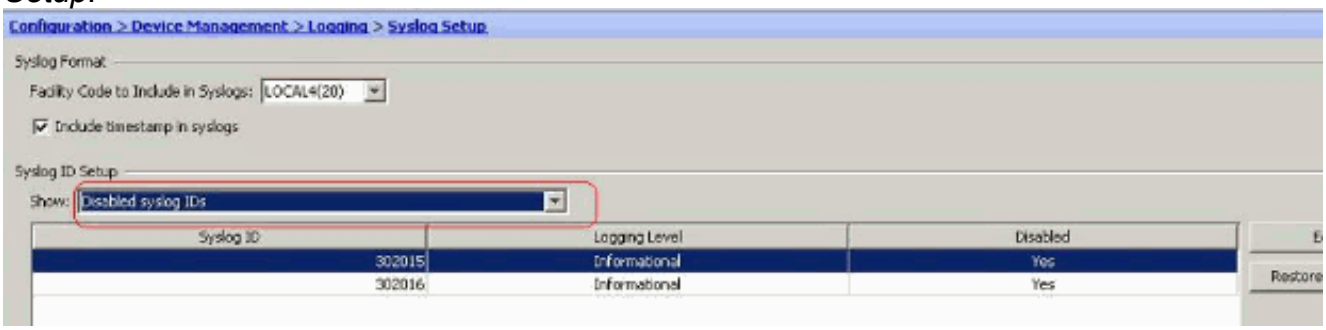


2. Selecteer in het venster *Instellingen* syslogan *bewerken* de optie *Geluid uit* en klik op



OK.

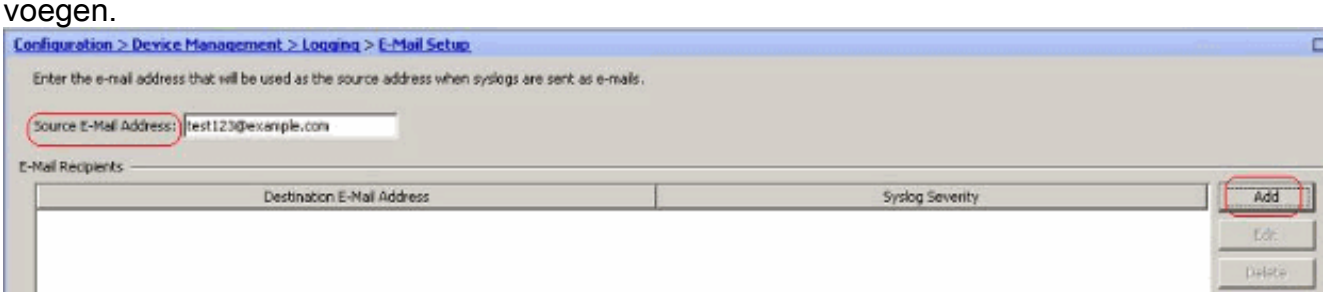
3. De gehandicapte syslogs kunnen in een afzonderlijk tabblad worden bekeken door de *Gehandicapte syslog ID's* te selecteren in het vervolgkeuzemenu *Syslog ID Setup*.



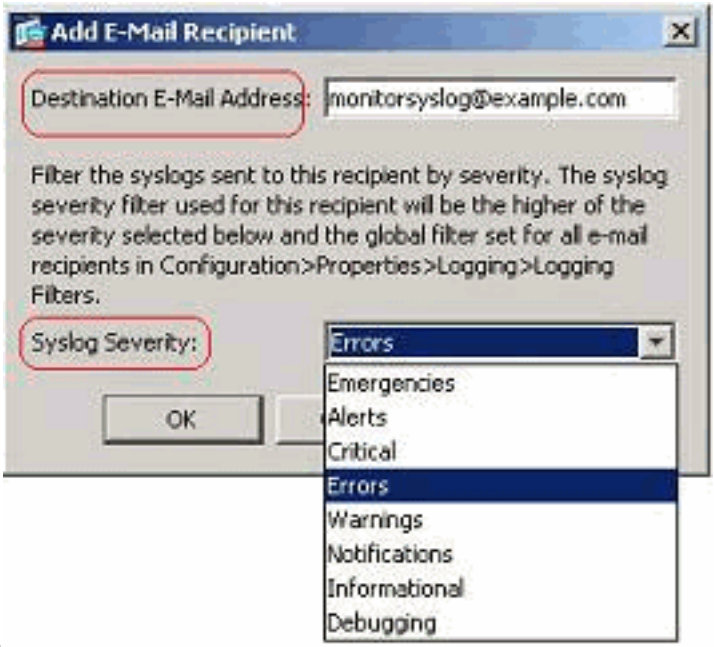
Aanmelden bij een e-mail

Voltooi deze stappen met ASDM om de systemen naar een e-mail te sturen:

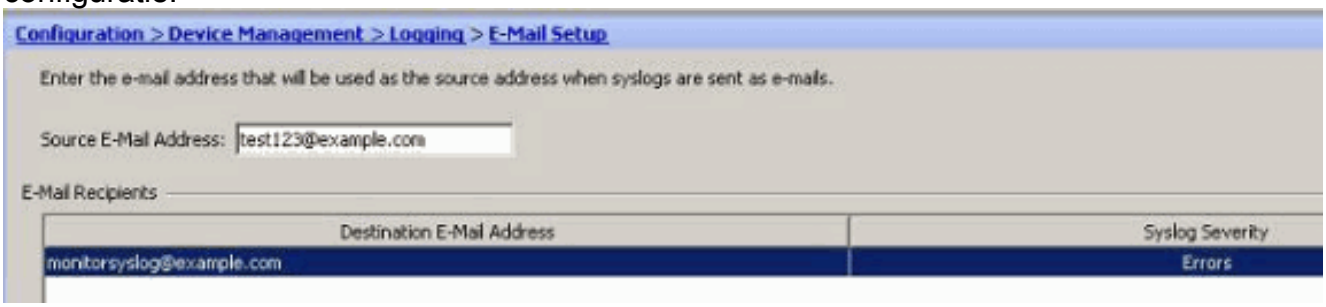
1. Kies *Configuratie > Apparaatbeheer > Vastlegging > E-mailinstelling*. Het veld *E-mailadres* is handig om een e-mailid als bron voor de syslogs toe te wijzen. Specificeer het e-mailadres van de bron. Klik nu op *Toevoegen* om de e-mailontvangers toe te voegen.



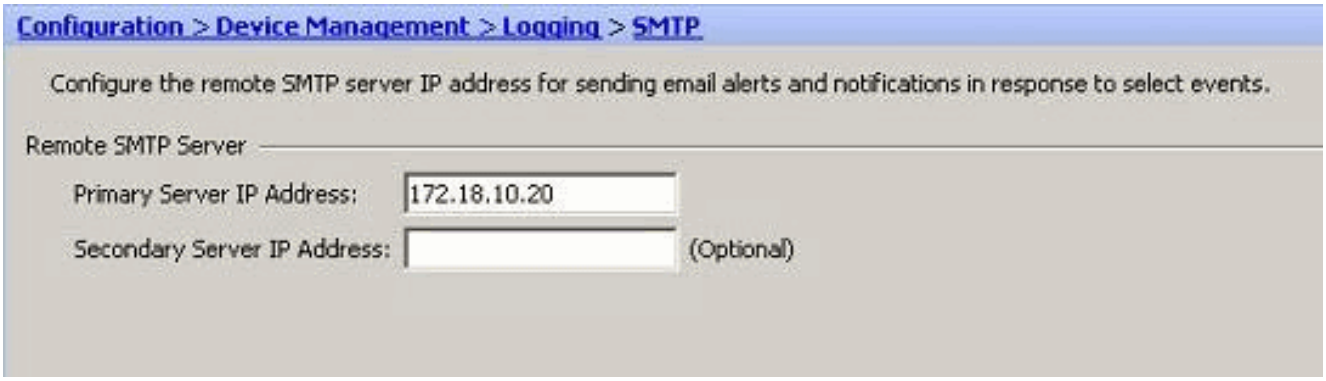
2. Specificeer het *E-mailadres* van de *bestemming* en kies het *ernst-niveau*. Op basis van de ernst van de vervuiling kunt u verschillende e-mailontvangers definiëren. Klik op *OK* om terug te keren naar het *deelvenster* met *e-*



mails. Dit resulteert in de volgende configuratie:



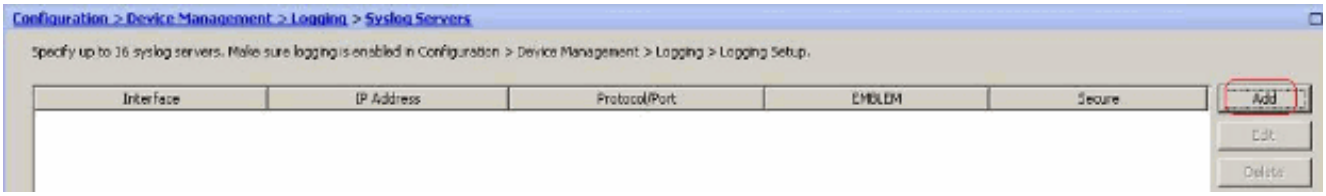
3. Kies *Configuratie > de Instellen van het apparaat > het Vastleggen > MTP* en specificeer de server
MTP.



Aanmelden bij een snelserver

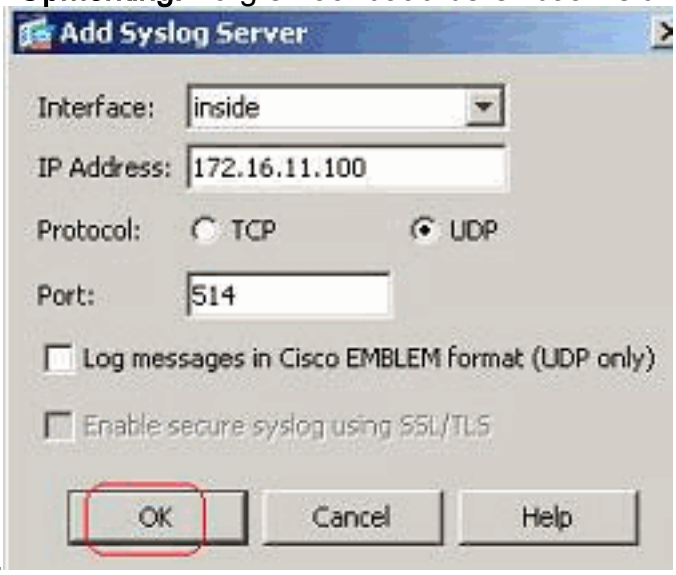
U kunt alle syslogberichten naar een speciale syslogserver verzenden. Voer deze stappen uit door ASDM te gebruiken:

1. Kies *Configuratie > Apparaatbeheer > Vastlegging > Syrische servers* en klik op *Add* om een syslogserver toe te
voegen.

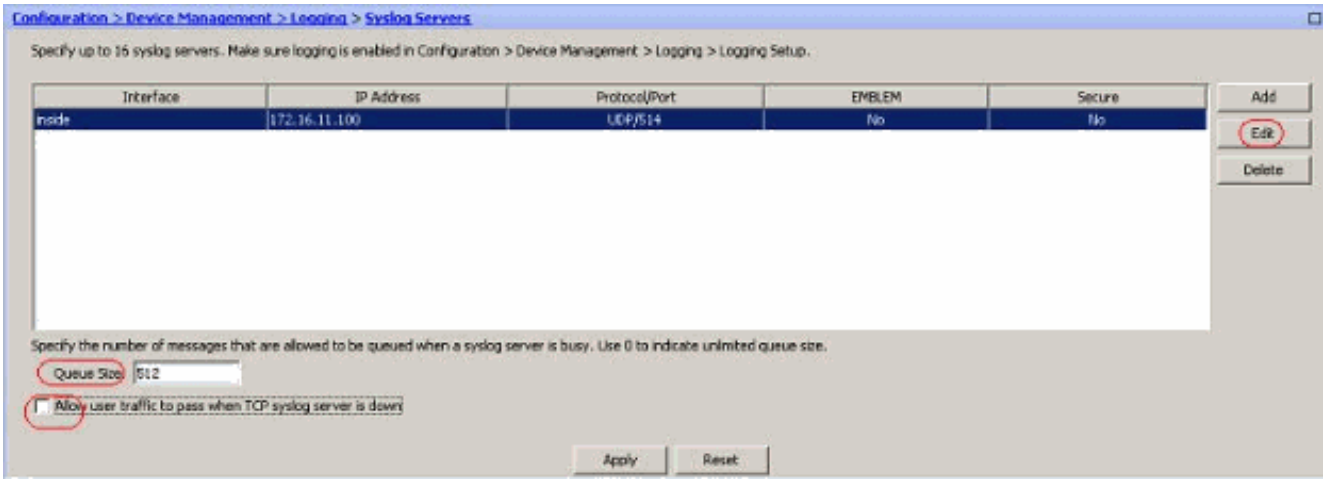


Het venster *Add Sspreker Server* verschijnt.

2. Specificeer de interface waarmee de server samen met het IP-adres wordt geassocieerd. Specificeer de details van *het protocol* en de *poort*, afhankelijk van uw netwerkinstelling. Klik vervolgens op *OK*.**Opmerking:** Zorg ervoor dat u bereikbaarheid hebt voor de syslogserver vanaf Cisco ASA.



3. De geconfigureerde syslogserver wordt hier weergegeven. U kunt wijzigingen uitvoeren wanneer u deze server selecteert en vervolgens op *Bewerken* klikt.



Opmerking: Controleer of *u gebruikersverkeer toestaat om door te geven wanneer TCP syslogserver* optie *is*. Anders worden de nieuwe gebruikerssessies ontkend door de ASA. Dit is alleen van toepassing wanneer het transportprotocol tussen de ASA en de syslogserver TCP is. De standaardinstelling is dat nieuwe sessies van netwerktoegang door Cisco ASA worden ontkend wanneer een syslogserver om welke reden dan ook is uitgezet.Zie het gedeelte Logging Filter om het type syslogberichten te definiëren dat naar de syslogserver moet worden verzonden.

Geavanceerde configuratie door gebruik van ASDM

Werken met lijst van gebeurtenissen

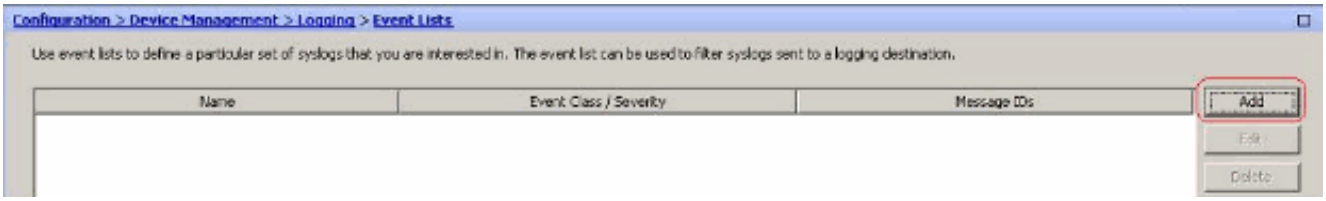
De lijsten van de gebeurtenis maken het mogelijk om aangepaste lijsten te maken die de groep syslogberichten bevatten die naar een bestemming moeten worden verzonden. De lijsten van gebeurtenissen kunnen op drie verschillende manieren worden gemaakt:

- Bericht ID of bereik van bericht-ID's
- Berichternst
- Berichtenklasse

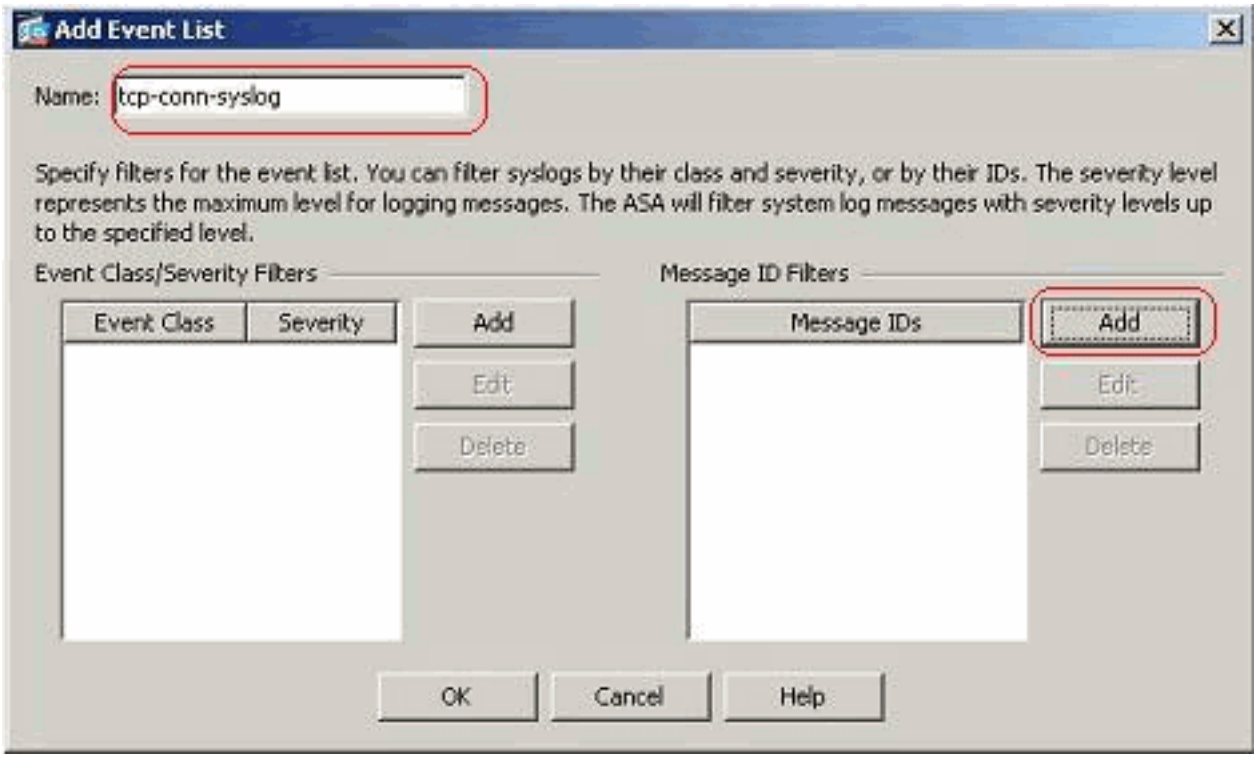
Bericht ID of bereik van bericht-ID's

Volg deze stappen:

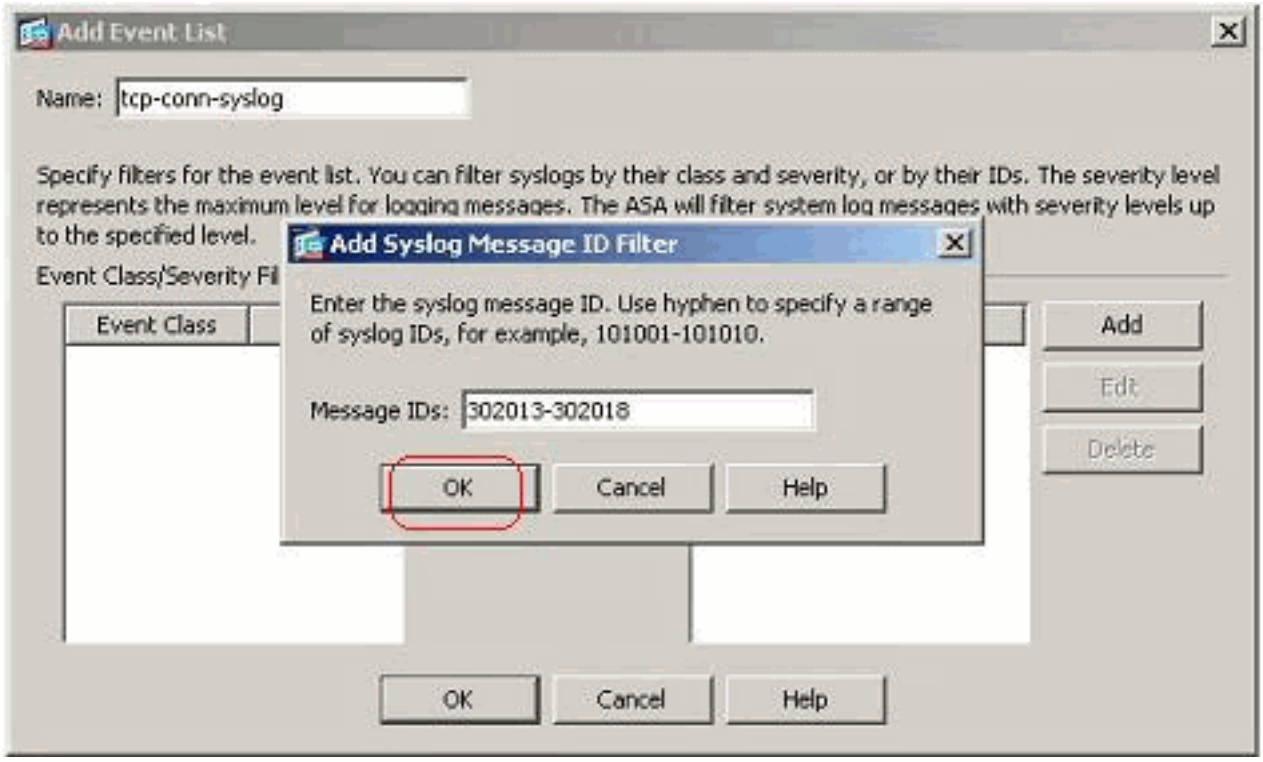
1. Kies *Configuratie > Apparaatbeheer > Vastlegging > Event Lists* en klik op *Add* om een nieuwe lijst met gebeurtenissen te maken.



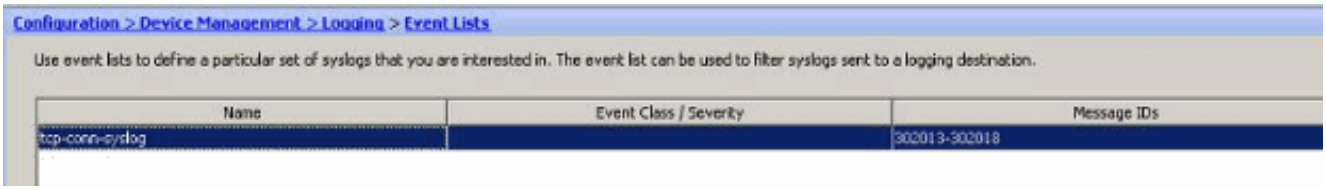
2. Specificeer een naam in het veld *Naam*. Klik op *Add* in het venster *Message ID Filters* om een nieuwe eventlijst te maken.



3. Specificeer het bereik van de syslogbericht-ID's. Hier hebben de TCP syslog berichten genomen. Klik op *OK* om dit te voltooien.

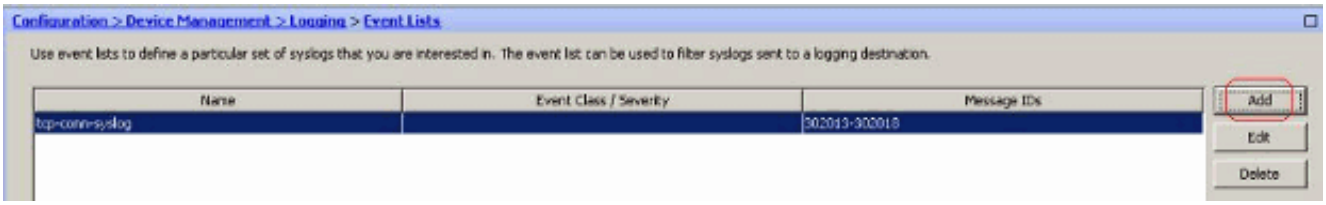


4. Klik nogmaals op *OK* om terug te keren naar het venster *Event Lists*.



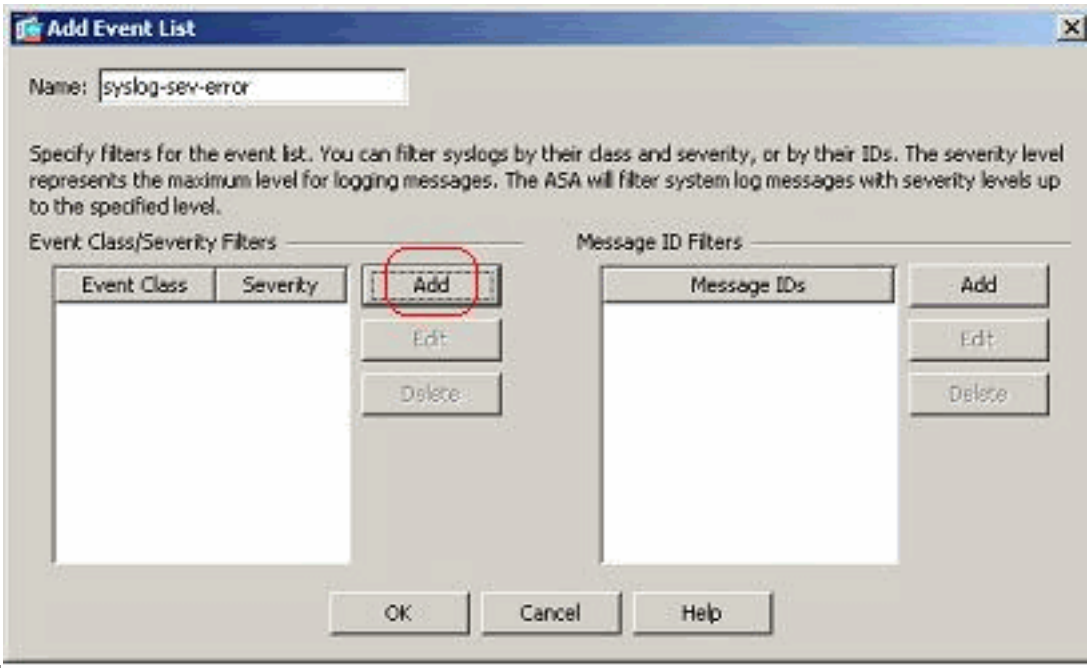
Berichternst

1. De lijst met gebeurtenissen kan ook worden gedefinieerd op basis van de ernst van het bericht. Klik op *Add* om een aparte eventlijst te maken.

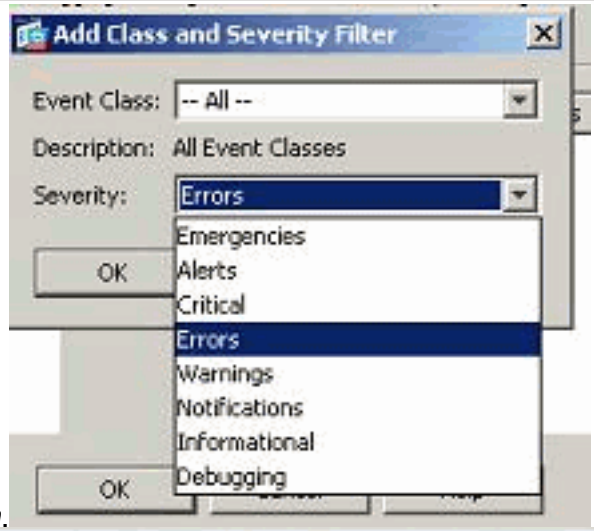


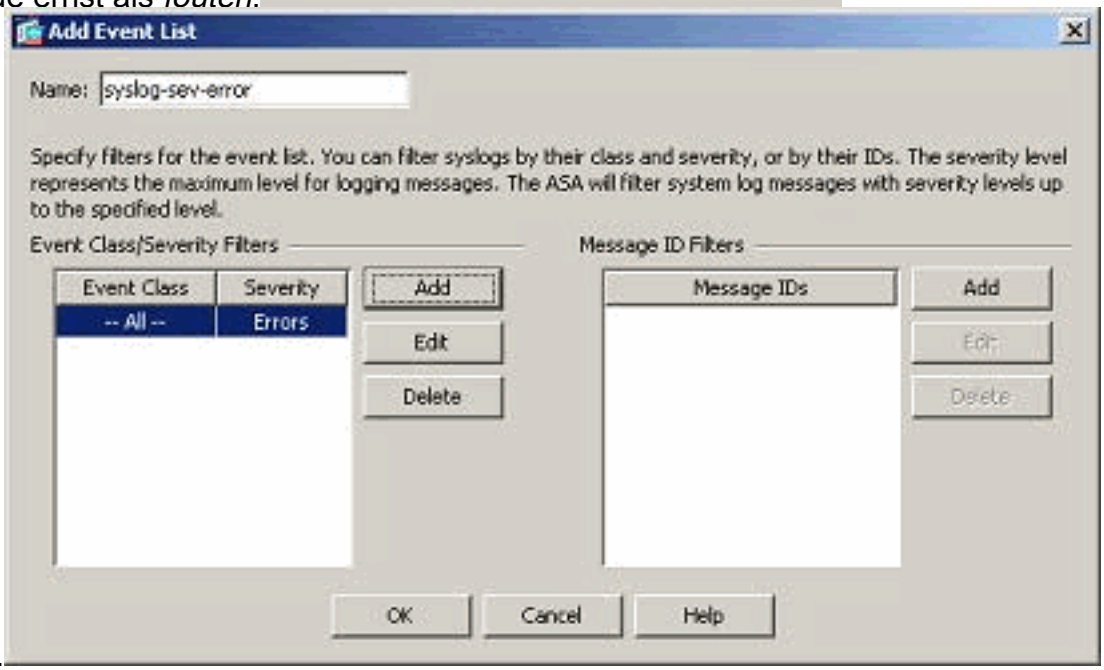
2. Specificeer de naam en klik op

Toevoegen.



3. Selecteer de ernst als *fouten*.





4. Klik op *OK*.

Berichtenklasse

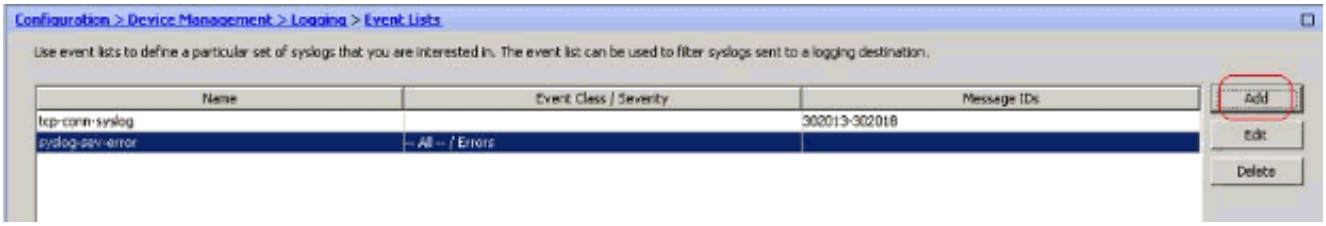
De lijst met gebeurtenissen is ook op basis van de berichtklasse ingesteld. Een berichtklasse is een groep syslogberichten gerelateerd aan een veiligheidsapparaat die u in staat stelt om een volledige klasse van berichten te specificeren in plaats van een klasse voor elk bericht afzonderlijk

te specificeren. Gebruik bijvoorbeeld de autclass om alle syslogberichten te selecteren die betrekking hebben op gebruikersverificatie. Sommige beschikbare berichtklassen worden hier weergegeven:

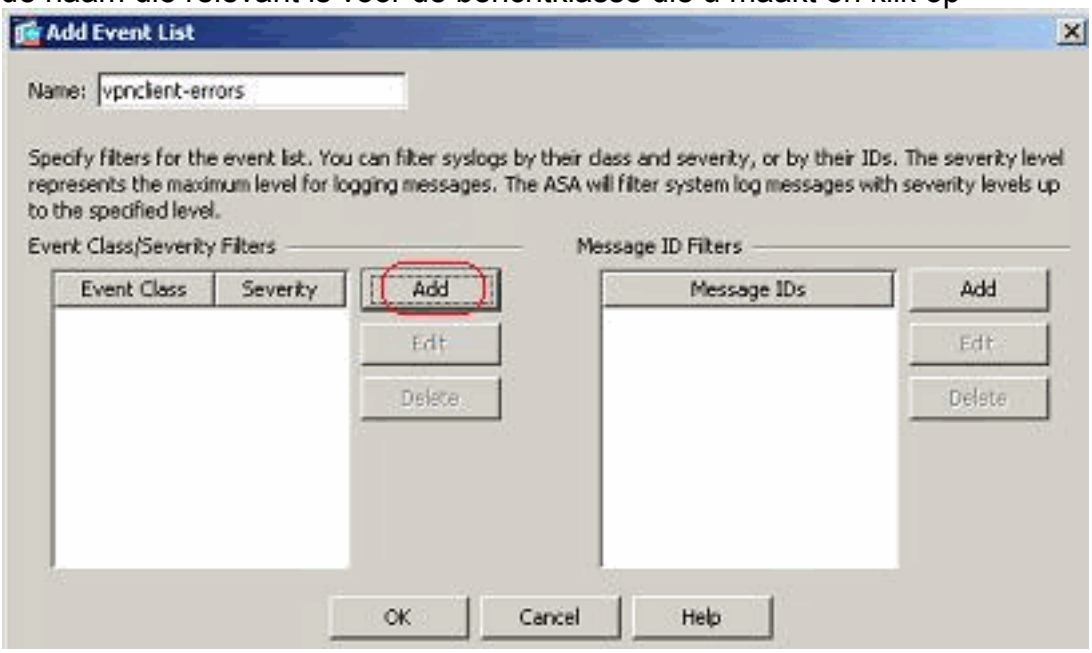
- Alle—alle eventklassen
- verificatie van auth en gebruiker
- bridge-transparante firewall
- A—PKI-certificeringsinstantie
- configuratie—Opdracht interface
- ha—failover
- IPS—Inbraakbeschermingsservice
- IP-stack
- NP-netwerkprocessor
- OSPF-routing
- rip-RIP routing
- sessie—gebruikerssessie

Voer deze stappen uit om een gebeurtenis class te maken die is gebaseerd op de berichtklasse *van VPN-fouten*. De berichtklasse, *vpnc*, is beschikbaar om alle syslogberichten met betrekking tot de client te categoriseren. De ernst van deze berichtklasse wordt geselecteerd als "fouten".

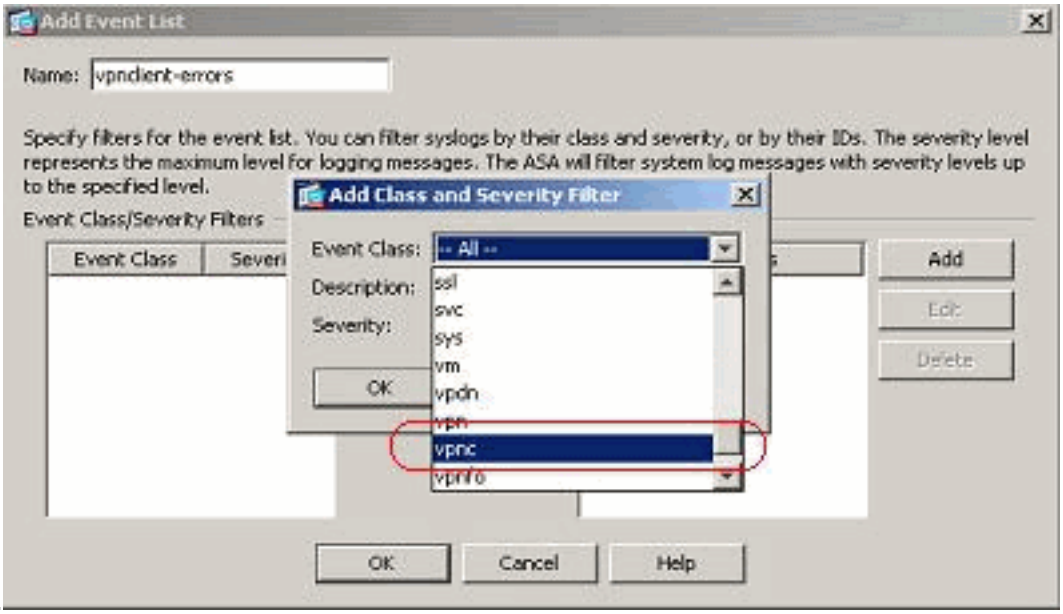
1. Klik op Toevoegen om een nieuwe eventlijst te maken.



2. Specificeer de naam die relevant is voor de berichtklasse die u maakt en klik op *Toevoegen*.

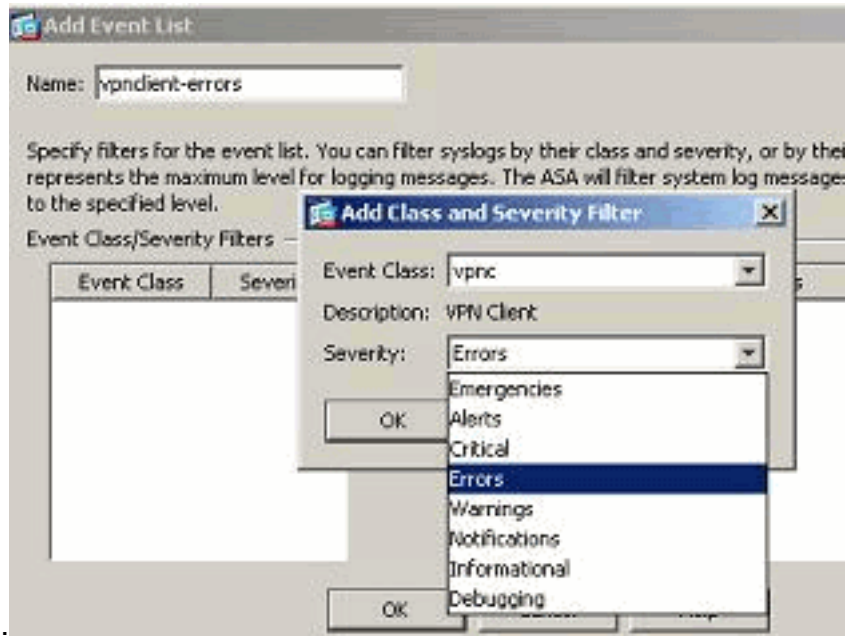


3. Selecteer *VPN* in de



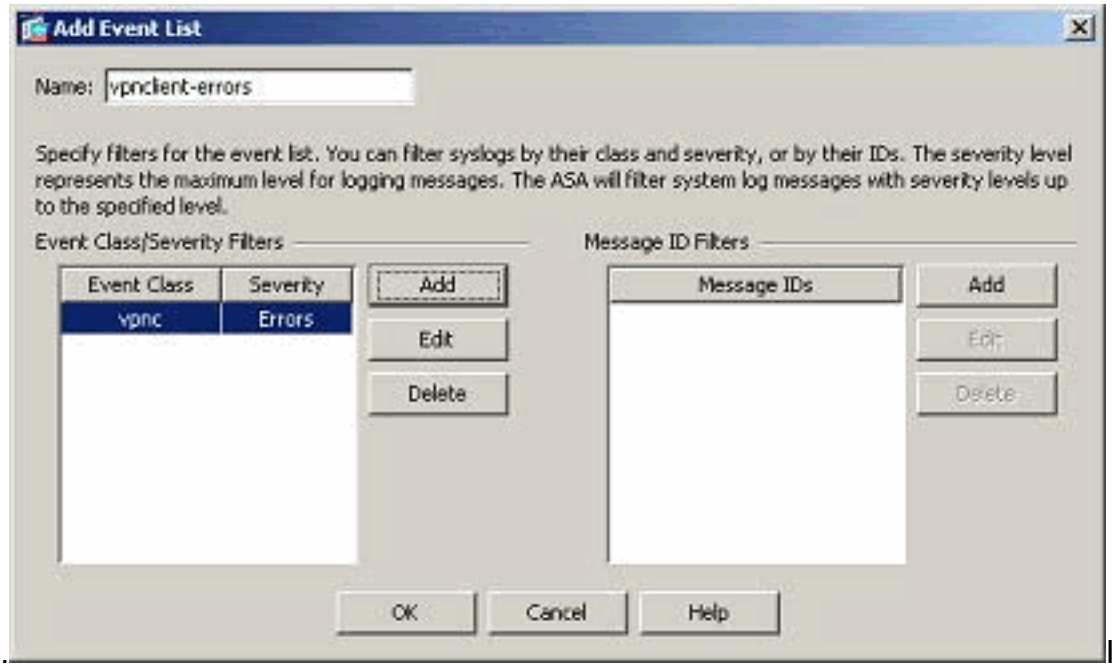
vervolgkeuzelijst.

4. Selecteer de ernst als *fouten*. Dit ernst niveau is van toepassing voor de berichten die voor deze berichtklasse worden ingelogd. Klik op *OK* om terug te keren naar het venster Bijvoegen lijst van

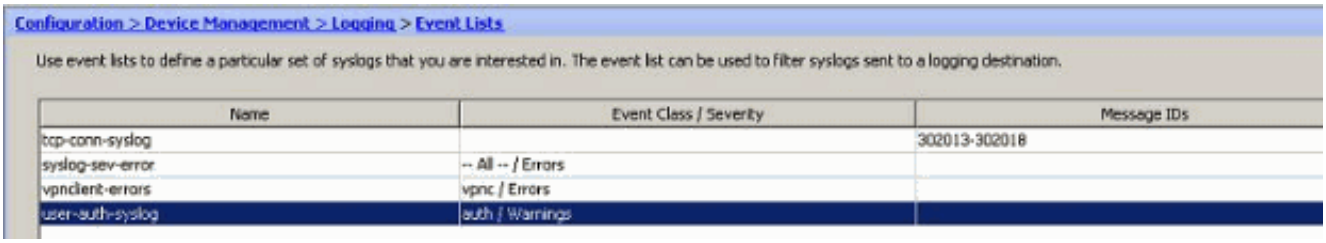


gebeurtenissen.

5. De gebeurtenissen class/ernst wordt hier weergegeven. Klik op *OK* om het configureren van de vervolgkeuzelijst "VPN-client-fouten" te



voltooien. In het volgende screenshot is ook te zien dat er een nieuwe eventlijst, "user-auth-syslog", wordt aangemaakt met een berichtklasse als "auth" en het ernst-niveau voor de symbolen van deze specifieke berichtklasse als "Waarschuwingen". Door dit te configureren specificeert de eventlijst alle syslogberichten die gerelateerd zijn aan de "auth" berichtklasse, met niveaus van ernst **tot** "Waarschuwingen" niveau.**Opmerking:** hier is de term "tot" van belang. Wanneer u het ernst-niveau aanduidt, bedenk dan dat alle syslogberichten tot dat niveau zullen worden ingelogd.**Opmerking:** een eventlijst kan meerdere eventklassen bevatten. De vervolgkeuzelijst "VPN-client-error" wordt gewijzigd door op **Bewerken** te klikken en een nieuwe eventklasse "ssl/error" te definiëren.



Werken met logfilters

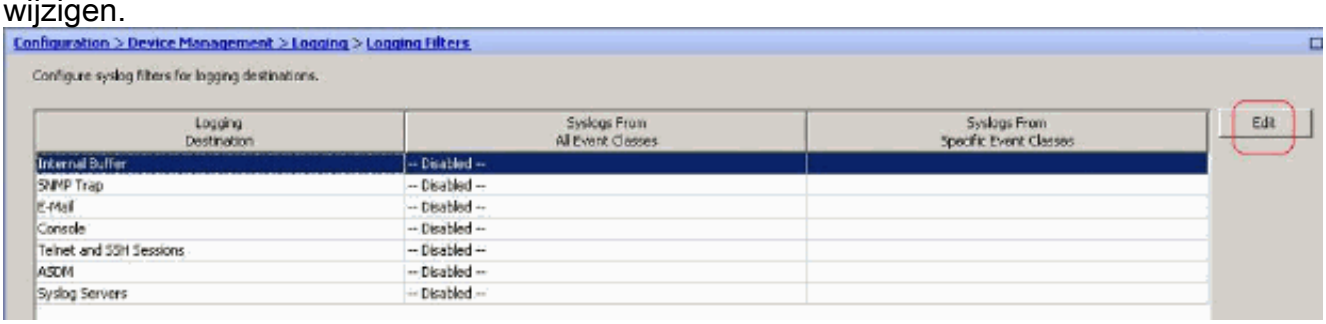
Loging filters worden gebruikt om de boodschappen naar een bepaalde bestemming te sturen. Deze slogan-berichten kunnen zijn gebaseerd op de "Ernst" of de "Zelfs lijsten".

Dit zijn de soorten bestemmingen waarop deze filters van toepassing zijn:

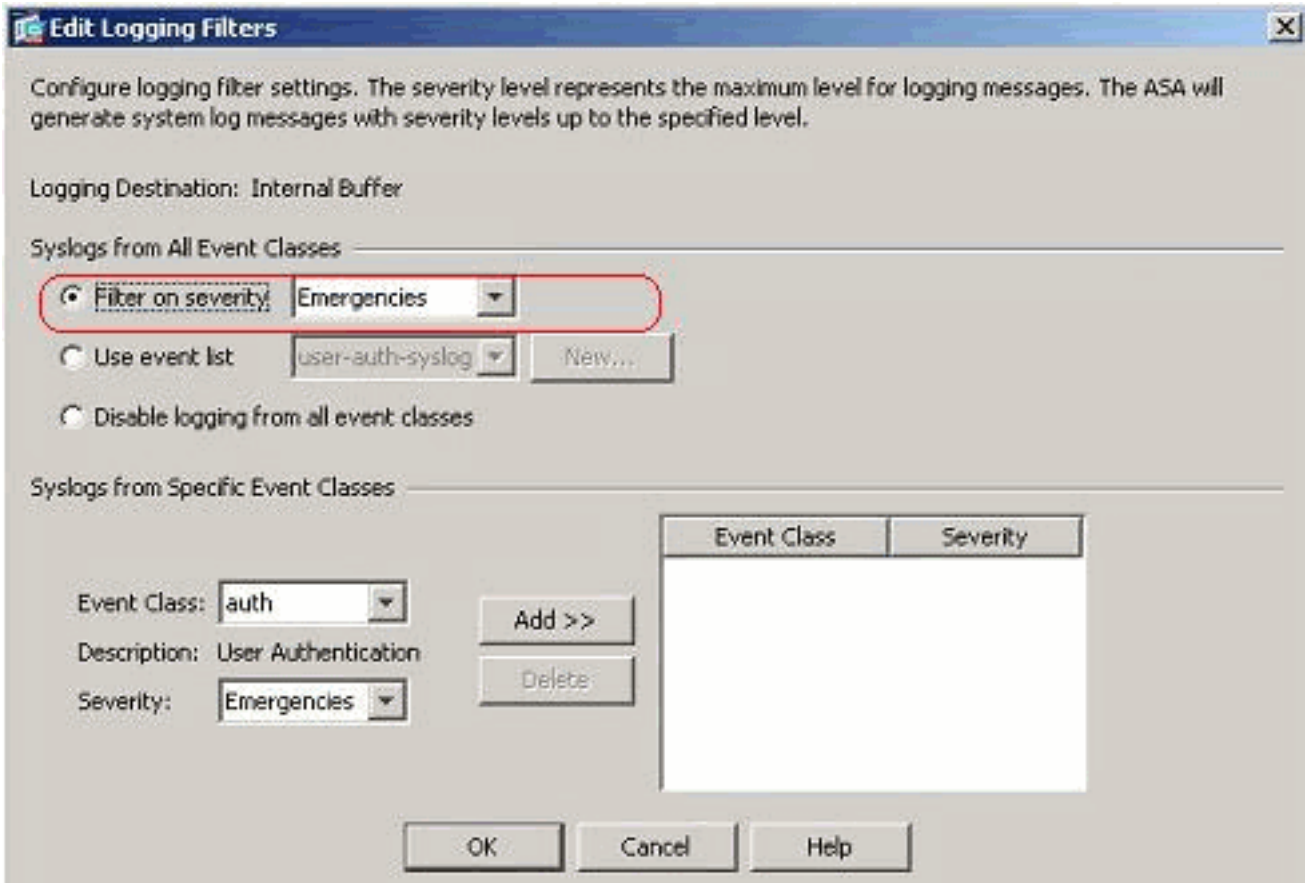
- Interne buffer
- SNMP-trap
- e-mail
- console
- Telnet-sessies
- ASDM
- Syrische servers

Volg deze stappen:

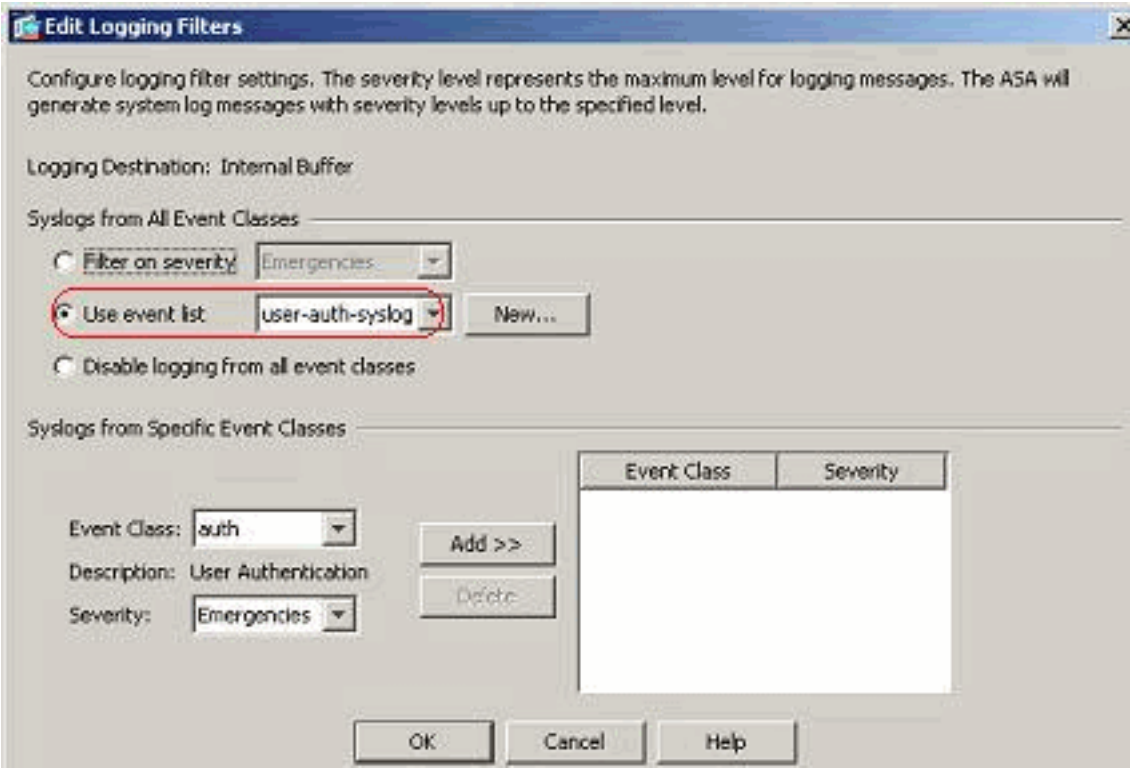
1. Kies **Configuratie > Apparaatbeheer > Vastlegging > Logging Filters** en selecteer de logbestemming. Klik vervolgens op **Bewerken** om de instellingen te wijzigen.



2. U kunt de syslog-berichten verzenden op basis van de ernst. Hierin is geselecteerd dat **noodsituaties** als voorbeeld dienen.

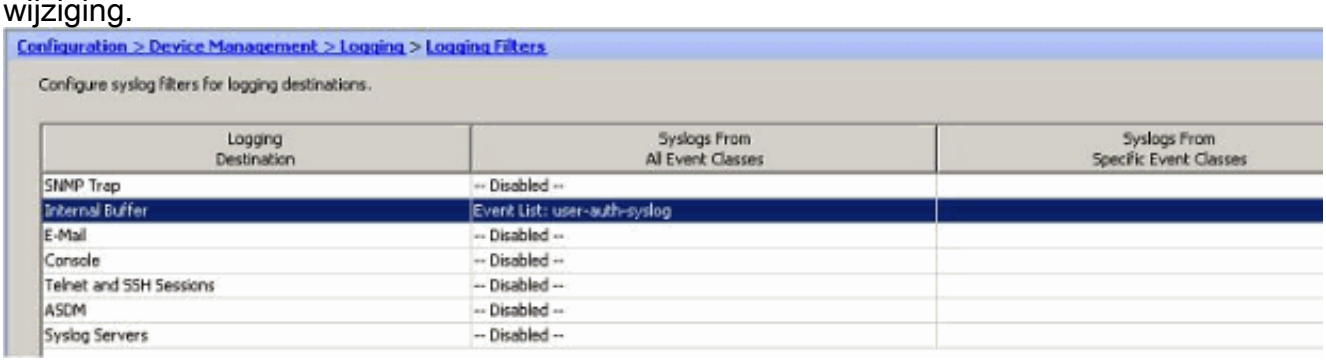


3. Een eventlijst kan ook worden geselecteerd om te specificeren welk type van berichten naar een bepaalde bestemming moet worden verzonden. Klik op



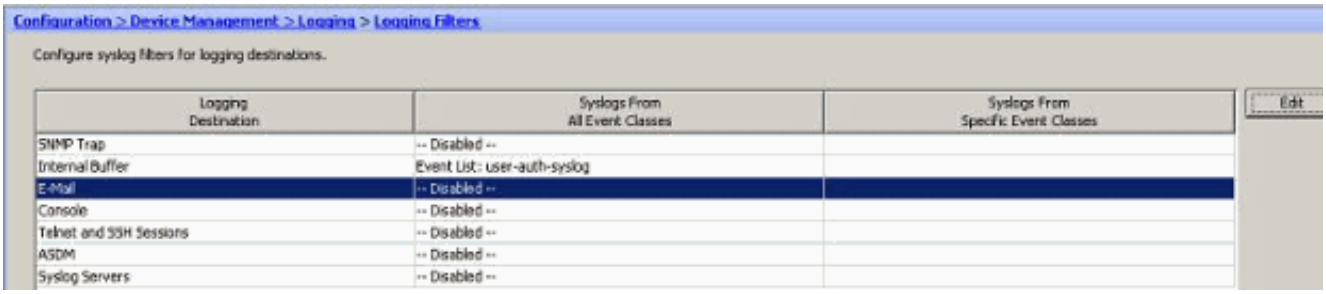
OK.

4. Controleer de wijziging.

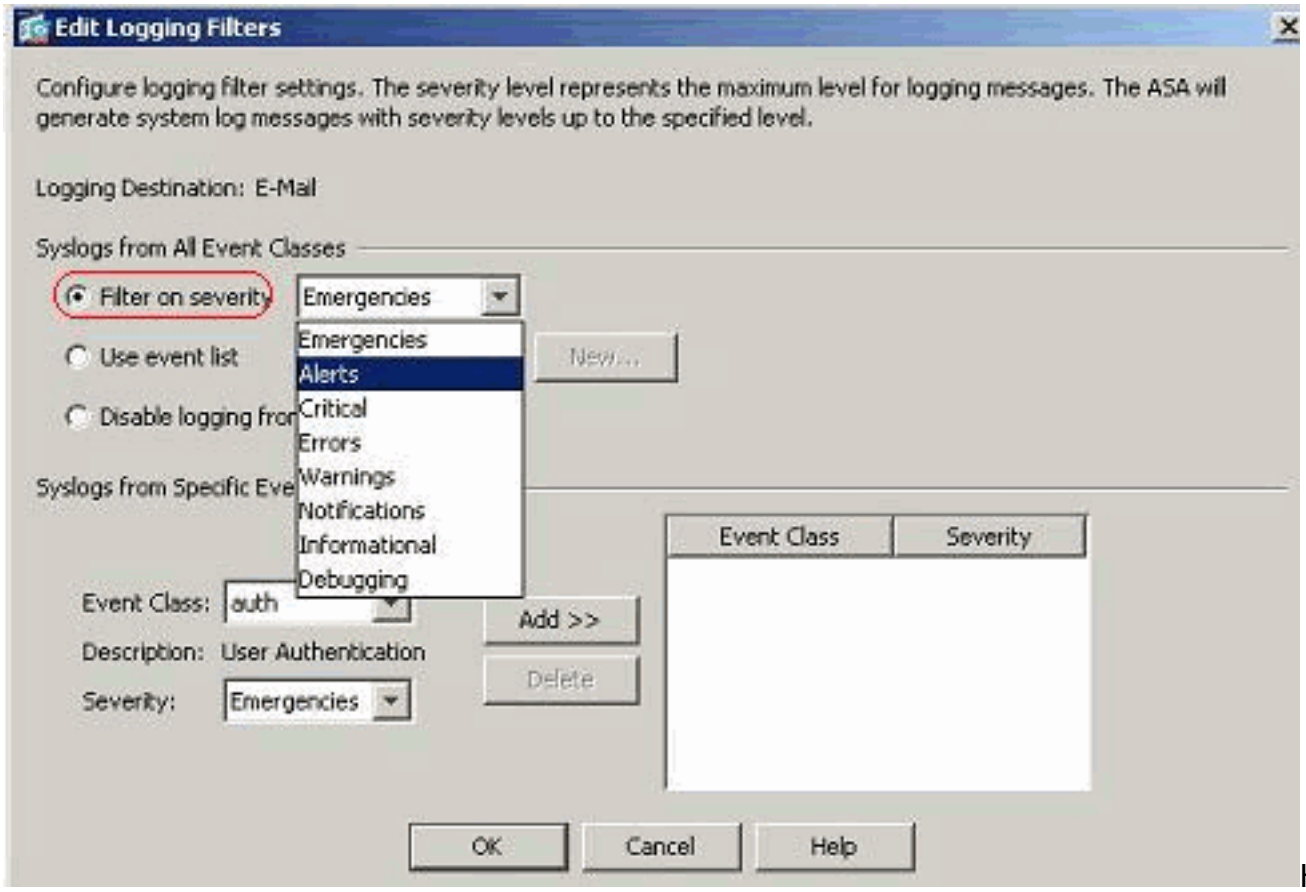


Dit zijn de stappen hoe u een groep berichten (gebaseerd op hun ernst) naar de e-mailserver kunt sturen.

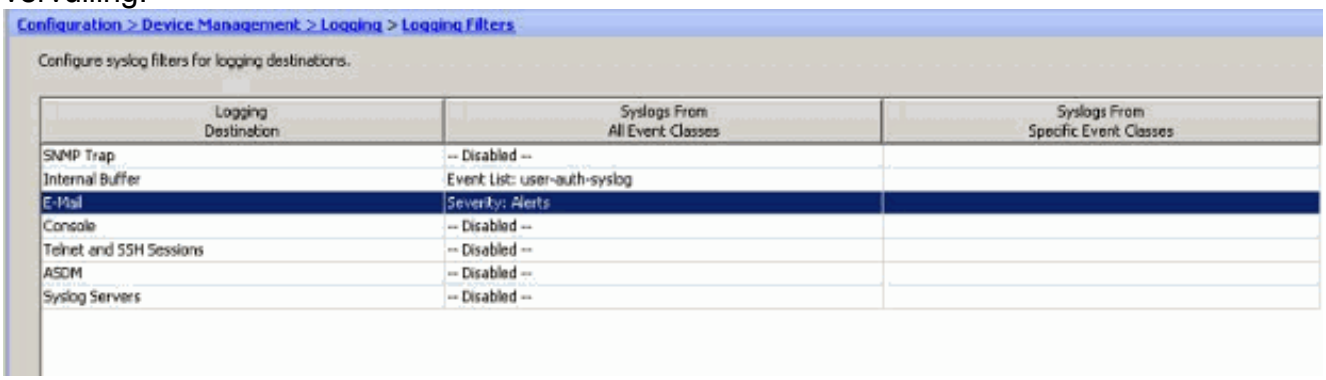
1. Selecteer **E-mail** in het veld Logging Destination. Klik vervolgens op **Bewerken**.



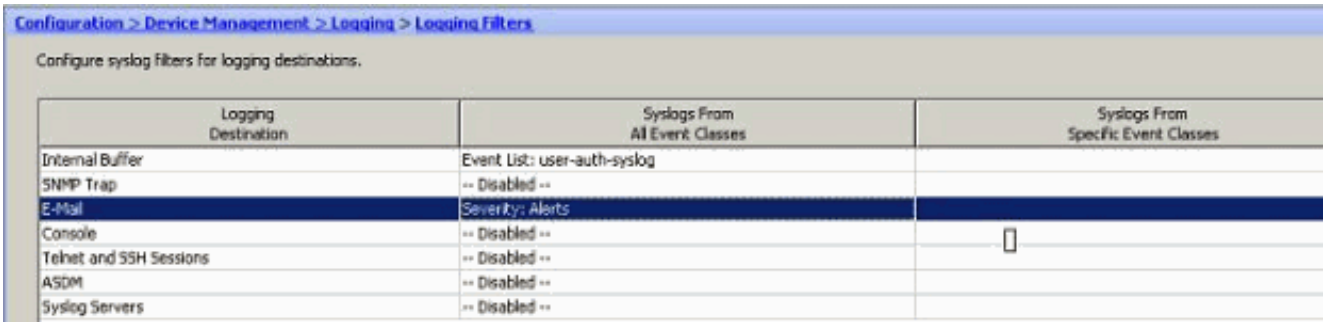
2. Kies het **filter op** ernst en selecteer het gewenste ernst niveau.



Hier zijn **waarschuwingen** geselecteerd als de ernst van de vervuiling.



U kunt zien dat alle waarschuwingssignalen worden verzonden naar de geconfigureerde e-mail.

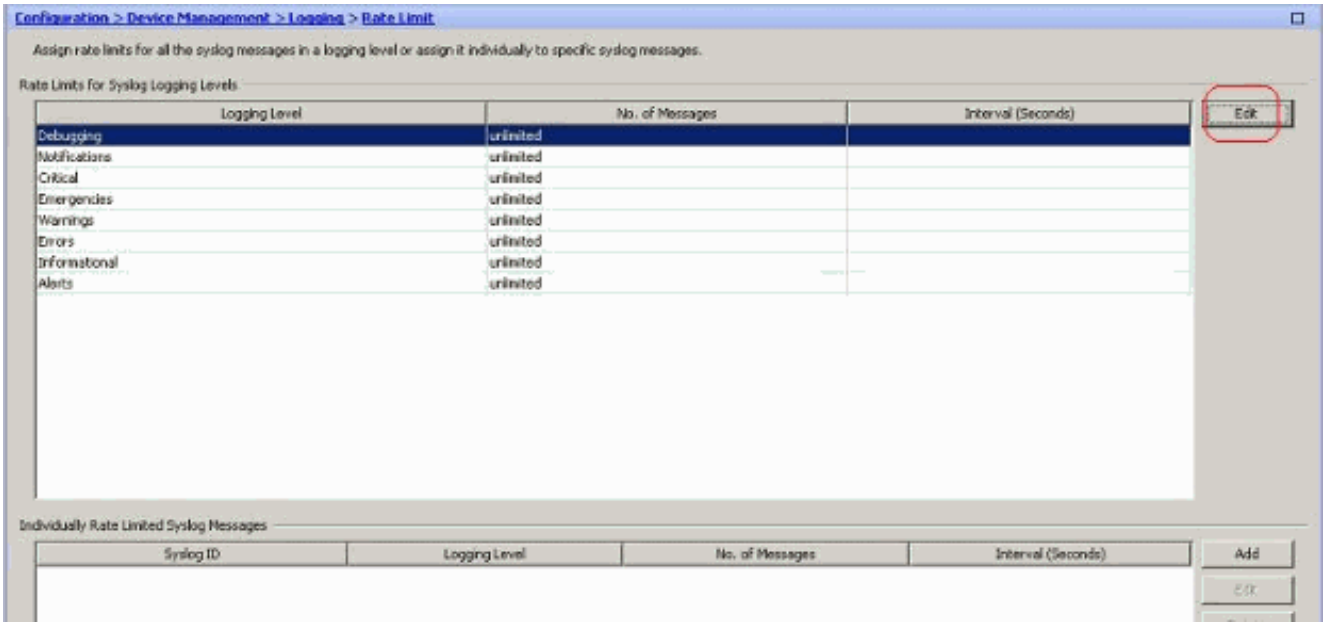


Snelheidsbeperking

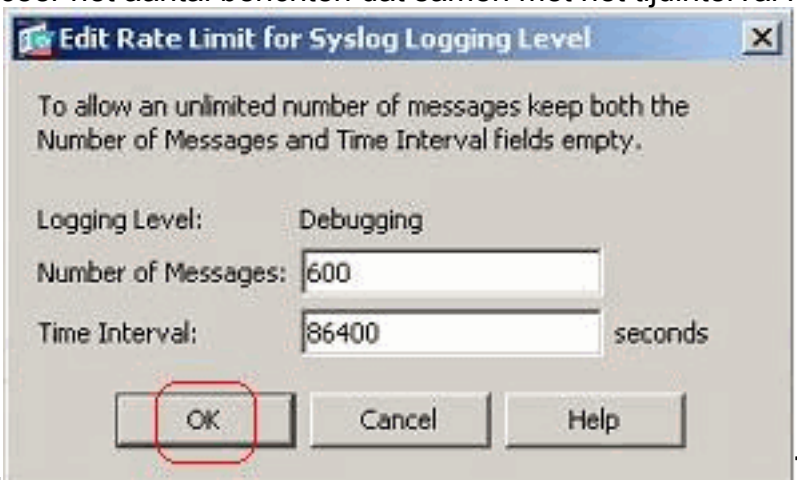
Dit specificeert het aantal syslogberichten dat een Cisco ASA naar een bestemming in een gespecificeerde tijdsperiode stuurt. Het wordt meestal gedefinieerd voor de ernst.

1. Kies **Configuratie > Apparaatbeheer > Vastlegging > Snelheidsbeperking** en selecteer het

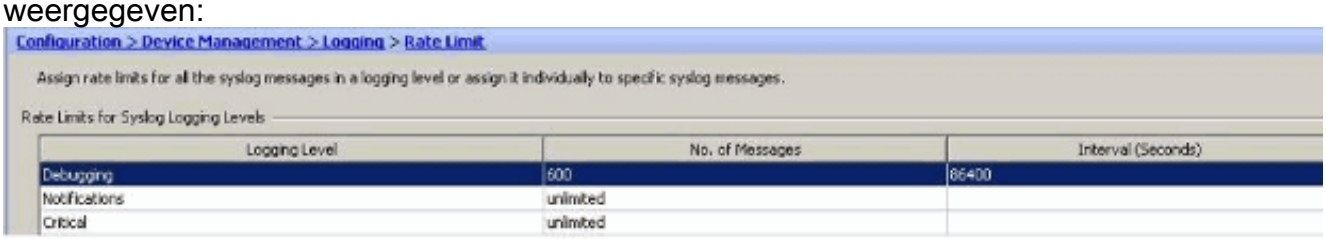
gewenste ernst-niveau. Klik vervolgens op **Bewerken**.



2. Specificeer het aantal berichten dat samen met het tijdinterval moet worden verzonden. Klik op **OK**.



Toelichting: Deze getallen worden als voorbeeld gegeven. Deze verschillen afhankelijk van het type netwerkomgeving.Hier worden aangepaste waarden weergegeven:

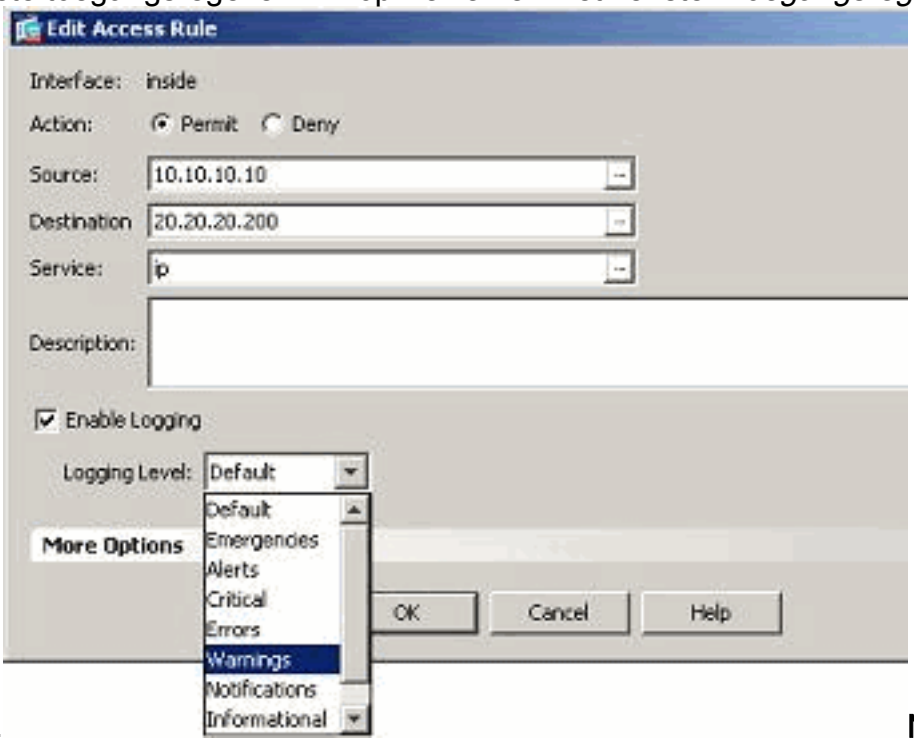


De hits van een toegangsregel registreren

U kunt de toetsen van de toegangsregel registreren met de ASDM. Het standaardloggedrag is om een syslog bericht voor alle ontkende pakketten te verzenden. Er is geen waarschuwingsbericht voor de toegestane pakketten en deze worden niet geregistreerd. U kunt echter wel een prioriteitsniveau voor het registreren van de aangepaste rechten definiëren op basis van de toegangsregel om de telling van de pakketten te volgen die deze toegangsregel raakt.

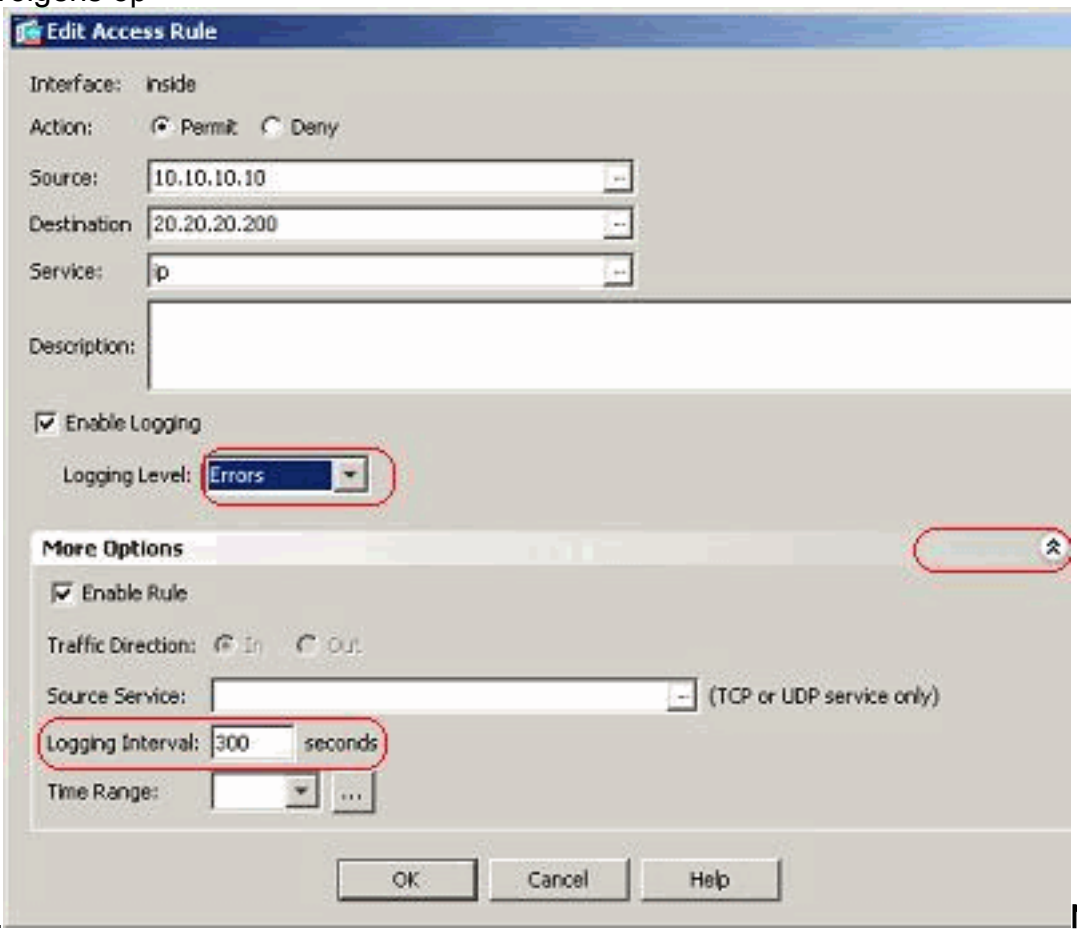
Volg deze stappen:

1. Selecteer de gewenste toegangsregel en klik op *Bewerken*.Het venster *Toegangsregel bewerken* verschijnt.



N.B.: In deze afbeelding geeft de *standaardoptie* in het veld *Logging Level* het standaardloggedrag van de Cisco ASA aan. Raadpleeg voor meer informatie hierover het gedeelte Toegangslijst registreren.

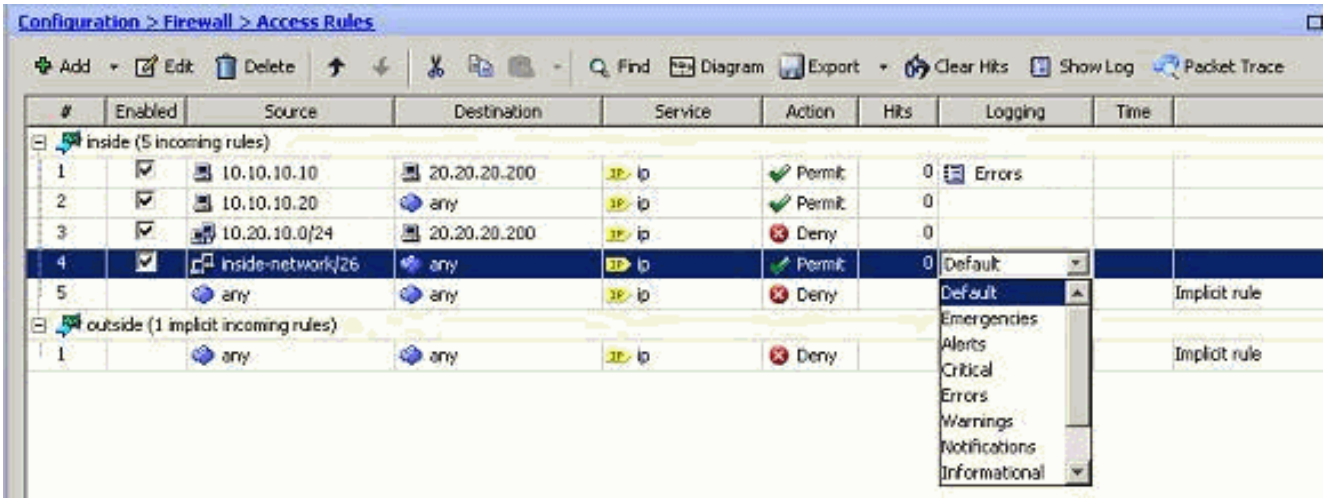
2. Controleer de optie *houtkap inschakelen* en specificeer het gewenste ernst-niveau. Klik vervolgens op *OK*.



N.B.: Door op het tabblad *Meer opties* te klikken, kunt u de optie *Inloggen* bekijken. Deze optie wordt alleen gemarkeerd als de bovenstaande optie *Vastlegging inschakelen* is ingeschakeld. Standaard waarde van deze timer is 300 seconden. Deze instelling is handig bij het specificeren van de

time-out waarde voor de flow-statistics die moet worden verwijderd wanneer er geen match voor die toegangsregel is. Als er hits zijn, wacht ASA tot de tijd van Logging Interval en stuurt dat naar de syslog.

3. De wijzigingen zijn hier weergegeven. In plaats hiervan kunt u ook dubbelklikken op het veld *Vastlegging* van de specifieke toegangsregel en het ernst-niveau instellen.



N.B.: Deze alternatieve methode om het *Logging Level* in hetzelfde deelvenster met toegangsregels op te geven door te dubbelklikken werkt alleen voor handmatig gemaakte toegangsregels, maar niet voor de Impliciete regels.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Configuraties

Dit document gebruikt deze configuraties:

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
```

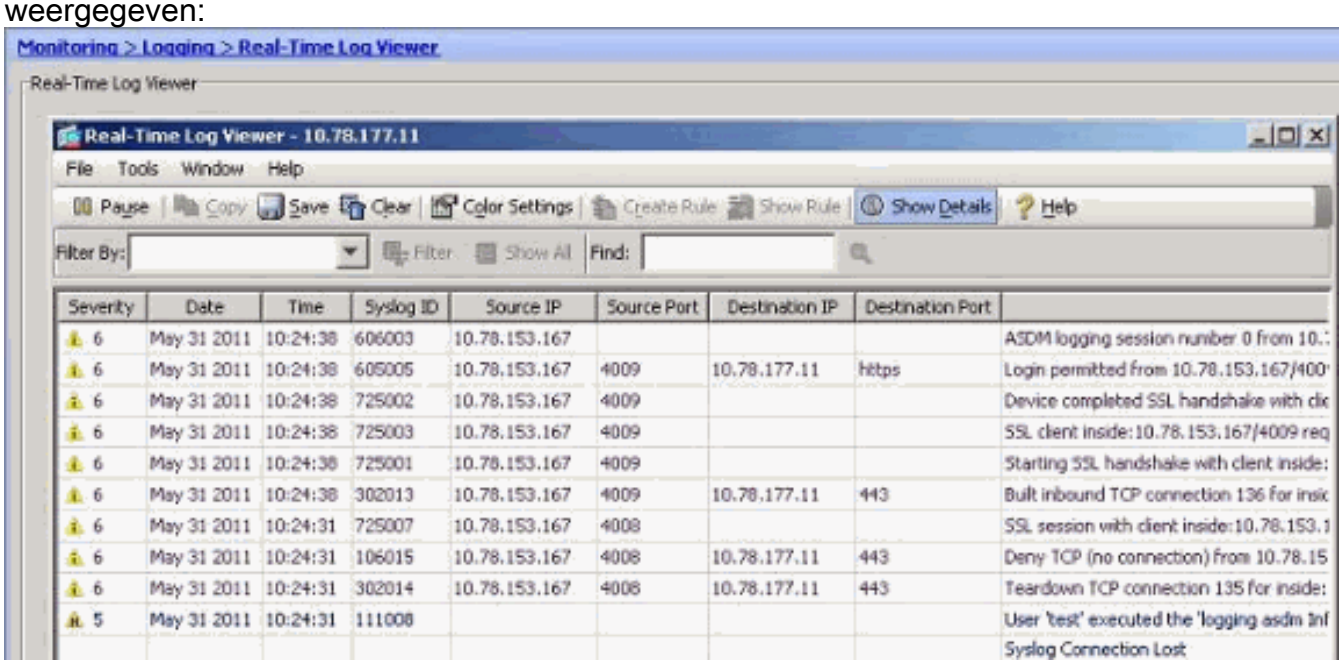
```
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global smtp-server 172.18.10.20
prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4
: end
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- U kunt de symbolen vanuit de ASDM bekijken. Kies **Bewaking > Vastlegging > Realtime logvenster**. Hier wordt een voorbeelduitvoer weergegeven:



Problemen oplossen

Probleem: Verbinding verloren — SLOGverbinding beëindigd —

Deze fout wordt ontvangen wanneer u ASDM-vastlegging op het Dashboard van het apparaat voor een van de contexten wilt inschakelen.

```
"Verbinding verloren – verbinding met het platform afgesloten –"
```

Wanneer ASDM wordt gebruikt om direct verbinding te maken met de admin-context en ADSM-vastlegging is uitgeschakeld, schakelt u vervolgens over naar een subcontext en maakt u ASDM-vastlegging mogelijk. De fouten worden ontvangen, maar de slogberichten bereiken fijn aan de syslogserver.

Oplossing

Dit is een bekend gedrag met Cisco ASDM en gedocumenteerd in Cisco bug-ID CSCsd10699

(alleen geregistreerde klanten). Als tijdelijke oplossing kunt u ASDM loggen inschakelen bij inloggen in admin-context.

Kan de realtime-vastlegging niet op Cisco ASDM weergeven

Een probleem is dat de real-time logs niet op ASDM kunnen worden bekeken. Hoe wordt dit ingesteld?

Oplossing

Configureer het volgende op Cisco ASA:

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

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Technische ondersteuning en documentatie – Cisco Systems