ASA 8.2:使用ASDM配置系統日誌

目錄

簡介

本文提供有關如何使用自適應安全裝置管理器(ASDM)GUI在思科自適應安全裝置(ASA)8.x上配置系統日誌的資訊。系統日誌消息是由Cisco ASA生成的消息，用於通知管理員配置的任何更改、網路設定更改或裝置效能更改。通過分析系統日誌消息，管理員可以通過執行根本原因分析輕鬆排除錯誤。

系統日誌消息主要根據其嚴重性級別來區分。

1. 嚴重性0 — 緊急消息 — 資源不可用
2. 嚴重性1 — 警報消息 — 需要立即採取行動
3. 嚴重級別2 — 嚴重消息 — 嚴重情況
4. 嚴重性3 — 錯誤消息 — 錯誤條件

5. 嚴重性4 — 警告消息 — 警告條件
6. 嚴重性5 — 通知消息 — 正常但重要的情況
7. 嚴重性6 — 資訊性消息 — 僅資訊性消息
8. 嚴重性7 — 調試消息 — 僅調試消息**注意：**最高嚴重性級別為緊急，最低嚴重性級別為調試。

Cisco ASA生成的示例系統日誌消息如下所示：

- %ASA-6-106012:拒絕從IP_address到IP_address的IP，IP選項十六進位制。
- %ASA-3-211001:記憶體分配錯誤
- %ASA-5-335003:NAC應用預設ACL，ACL:ACL-name - host-address

在「%ASA-X-YYYY：」中指定的數值X表示消息的嚴重性。例如，「%ASA-6-106012」是資訊性消息，「%ASA-5-335003」是錯誤消息。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA版本8.2
- Cisco ASDM版本6.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

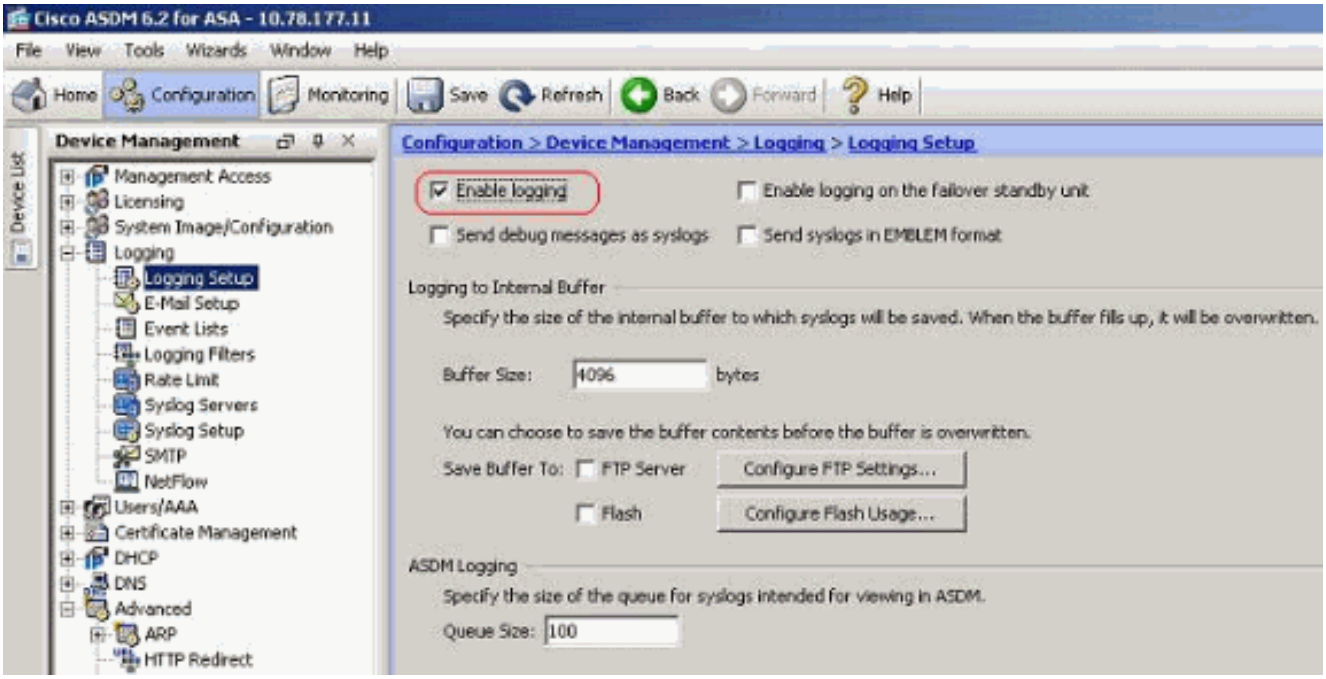
請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

使用ASDM進行基本系統日誌配置

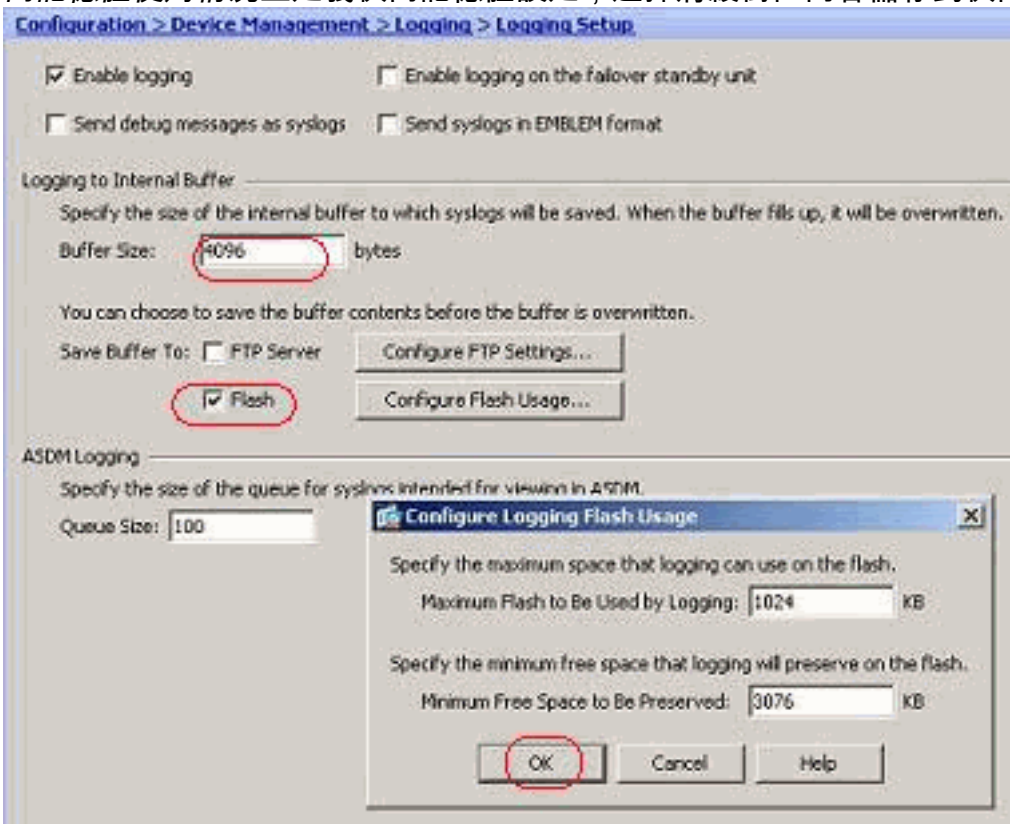
啟用日誌記錄

請完成以下步驟：

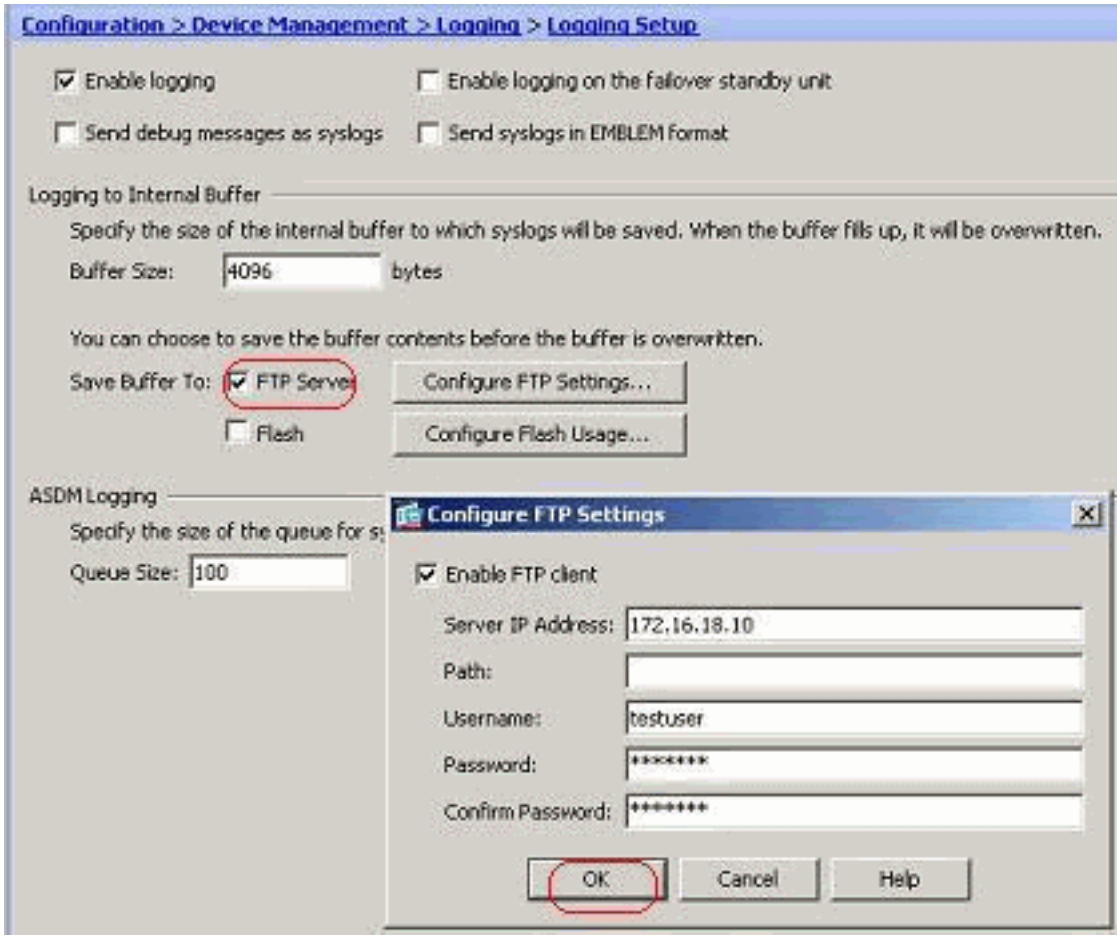
1. 選擇*Configuration > Device Management > Logging > Logging Setup*，然後選中*Enable logging*選項。



2. 您可以通過指定緩衝區大小，將系統日誌消息記錄到內部緩衝區。您也可以通過按一下*配置快閃記憶體使用情況*並定義快閃記憶體設定，選擇將緩衝區內容儲存到快閃記憶體。



3. 緩衝日誌消息可以在被覆蓋之前傳送到FTP伺服器。按一下「*Configure FTP Settings*」，然後指定FTP伺服器詳細資訊，如下所示



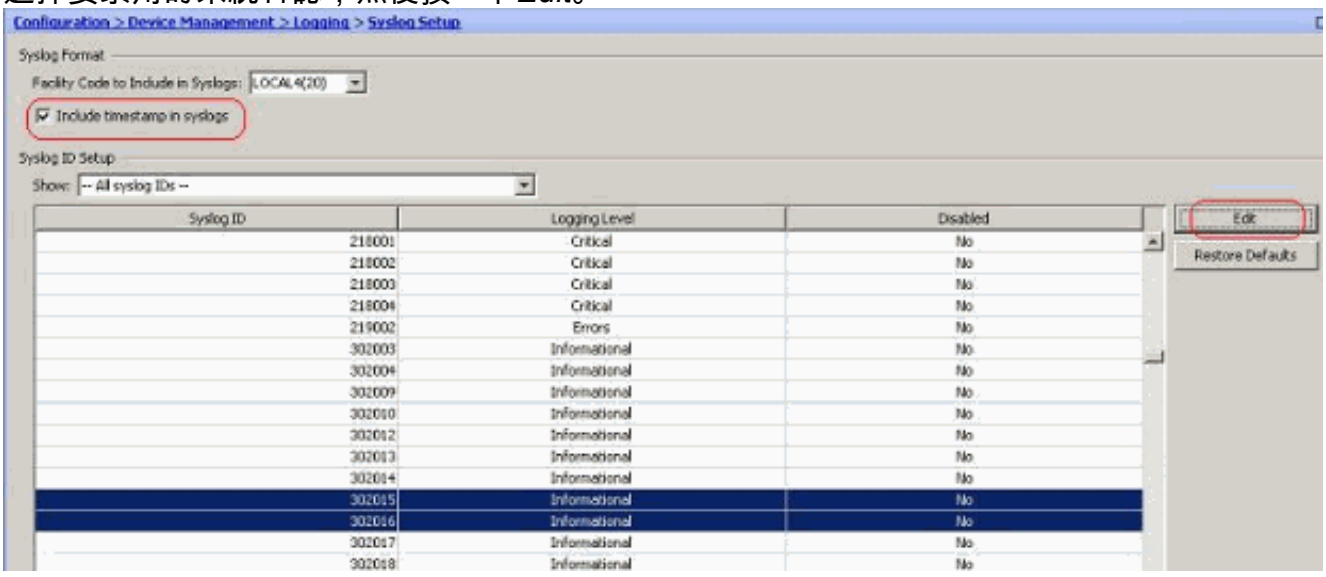
:

禁用日誌記錄

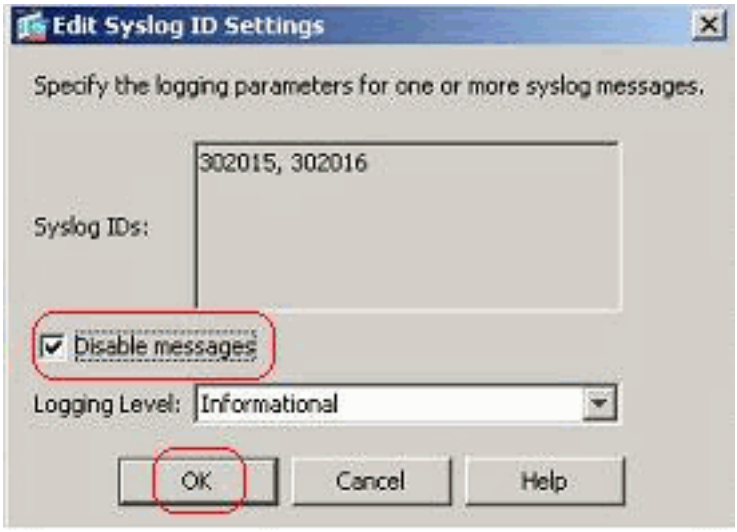
您可以根據要求禁用特定系統日誌ID。

注意：通過為*Include timestamp in syslogs*選項選擇複選標籤，可以將作為欄位生成的日期和時間新增到syslogs中。

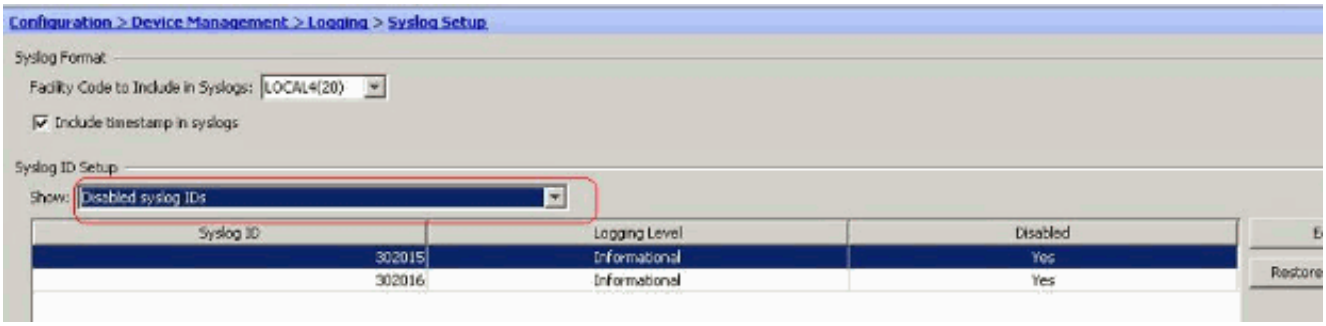
1. 選擇要禁用的系統日誌，然後按一下*Edit*。



2. 在*Edit Syslog ID Settings*視窗中，選中*Disable messages*選項，然後按一下*OK*。



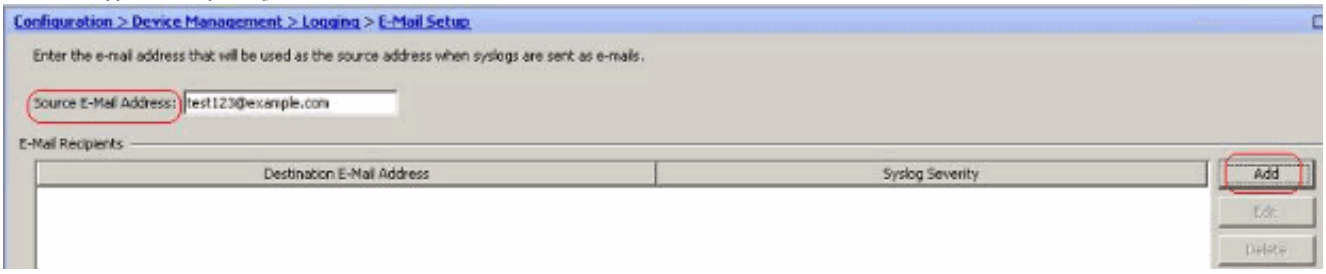
3. 通過在*Syslog ID Setup*下拉選單中選擇*Disabled syslog IDs*，可以在單獨的頁籤中檢視禁用的系統日誌。



登入到電子郵件

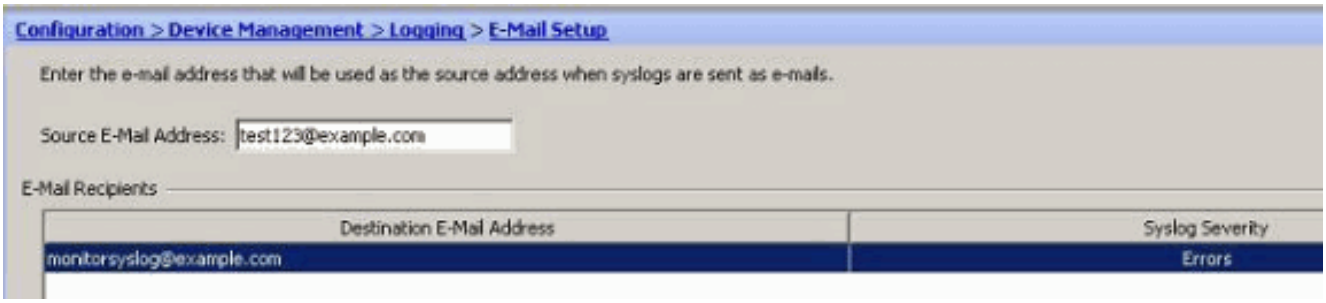
使用ASDM完成以下步驟，以便將系統日誌傳送到電子郵件：

1. 選擇*Configuration > Device Management > Logging > E-Mail Setup*。*Source E-Mail Address*欄位有助於將電子郵件ID指定為系統日誌的源。指定源電子郵件地址。現在，按一下*Add*新增電子郵件收件人。

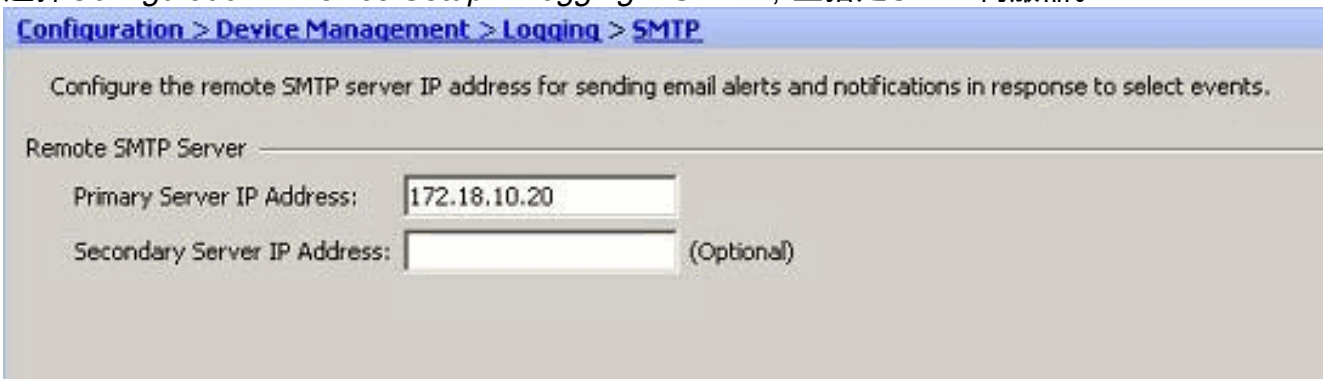


2. 指定目*的地電子郵件地址*並選擇嚴重*性級別*。根據嚴重性級別，您可以定義不同的電子郵件收件人。按一下*OK*返回到*E-Mail Setup*窗格。

這會導致以下設定：



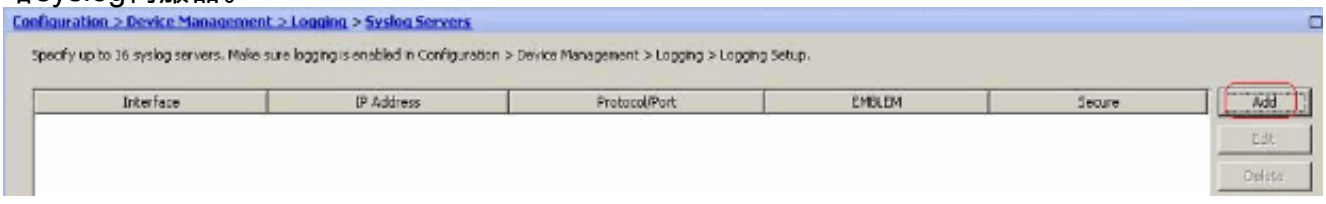
3. 選擇*Configuration > Device Setup > Logging > SMTP*，並指定SMTP伺服器。



登入到系統日誌伺服器

可以將所有系統日誌消息傳送到專用系統日誌伺服器。使用ASDM執行以下步驟：

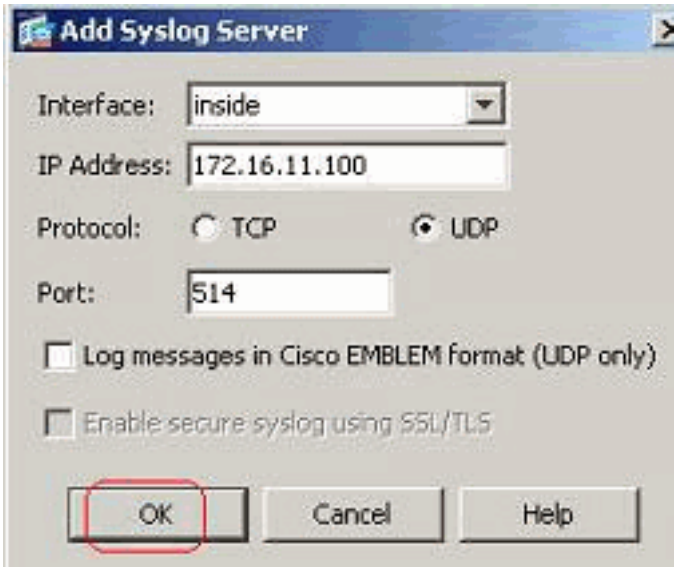
1. 選擇*Configuration > Device Management > Logging > Syslog Servers*，然後按一下*Add*以新增syslog伺服器。



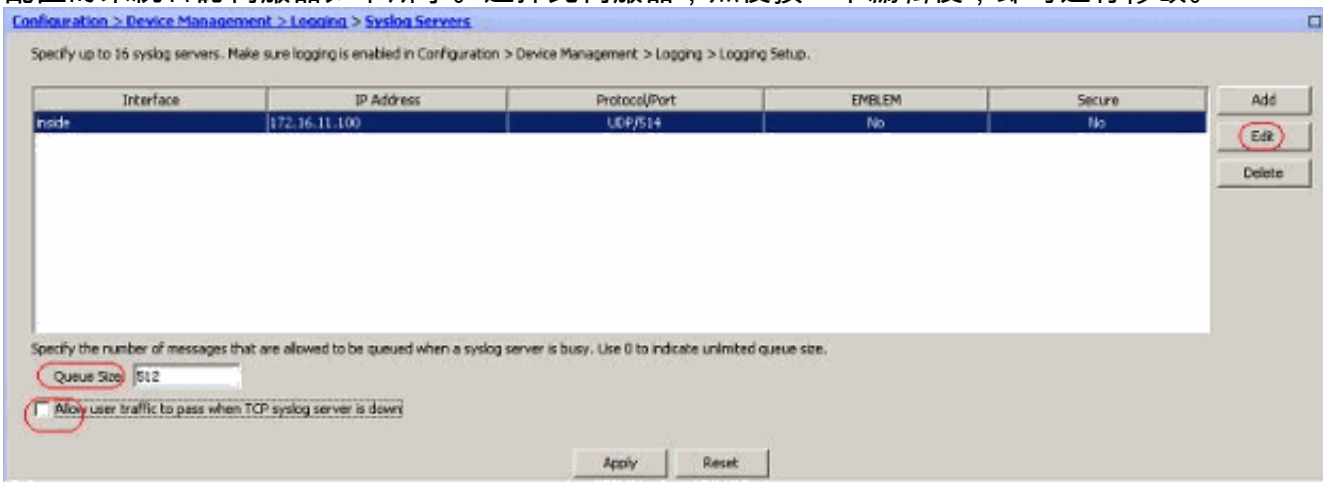
出現*Add Syslog Server*視窗。

2. 指定伺服器與IP地址關聯的介面。根據網路設定指定*協定*和*埠*詳細資訊。然後，按一下*OK*。

注意：確保可以從Cisco ASA訪問系統日誌伺服器。



3. 配置的系統日誌伺服器如下所示。選擇此伺服器，然後按一下*編輯*後，即可進行修改。



注意：選中*Allow user traffic to pass when TCP syslog server is down*選項。否則，新使用者會話將通過ASA被拒絕。僅當ASA和syslog伺服器之間的傳輸協定為TCP時適用。預設情況下，Cisco ASA會在系統日誌伺服器因任何原因關閉時拒絕新的網路訪問會話。要定義要傳送到系統日誌伺服器的系統日誌消息的型別，請參閱日誌記錄過濾器部分。

使用ASDM進行高級系統日誌配置

使用事件清單

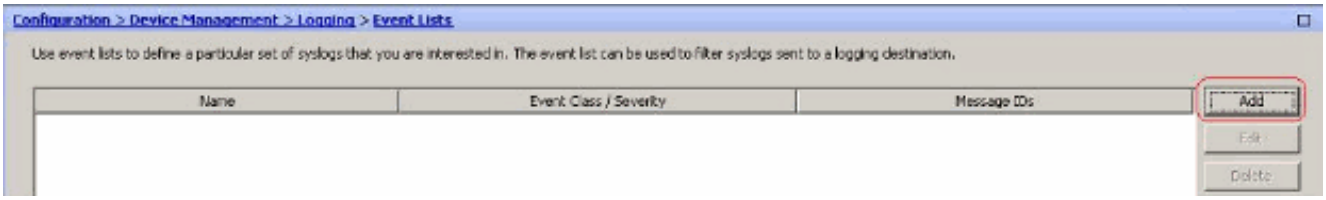
事件清單使我們能夠建立自定義清單，其中包含要傳送到目標的系統日誌消息組。可以通過三種不同的方法建立事件清單：

- 消息ID或消息ID的範圍
- 消息嚴重性
- 消息類

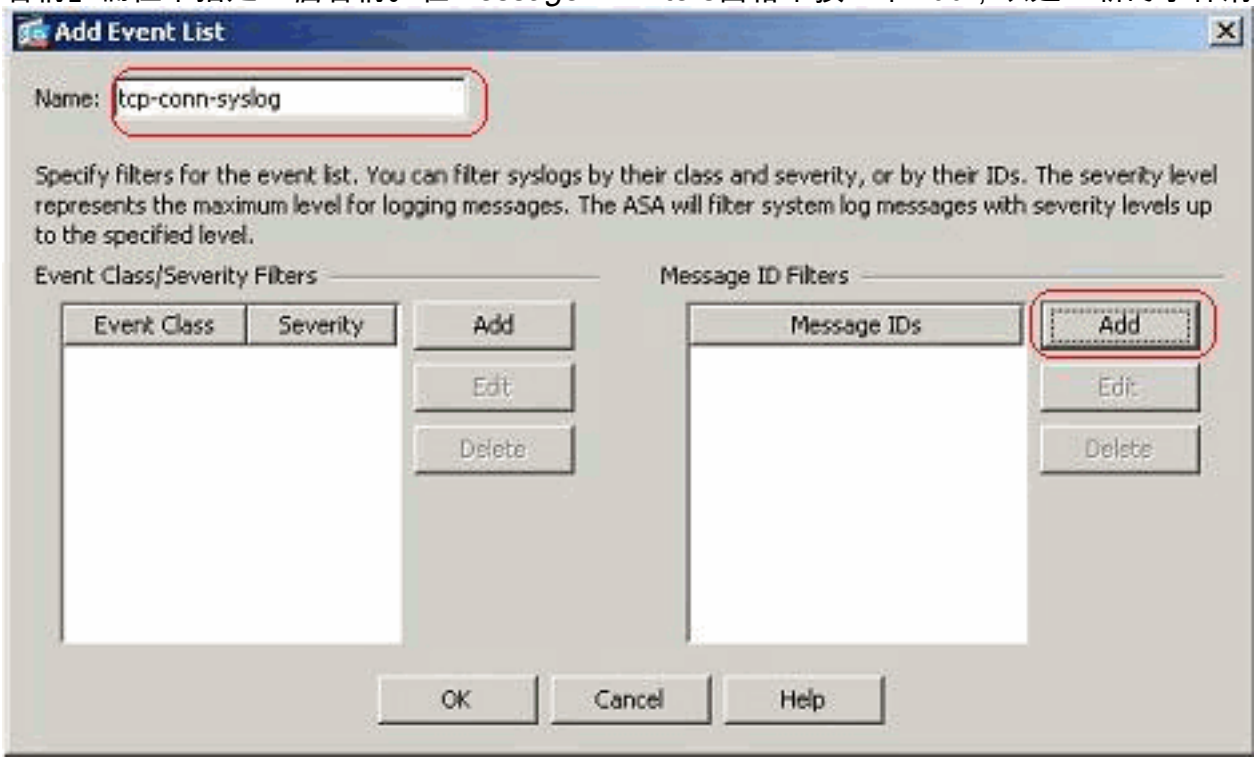
消息ID或消息ID的範圍

請執行以下步驟：

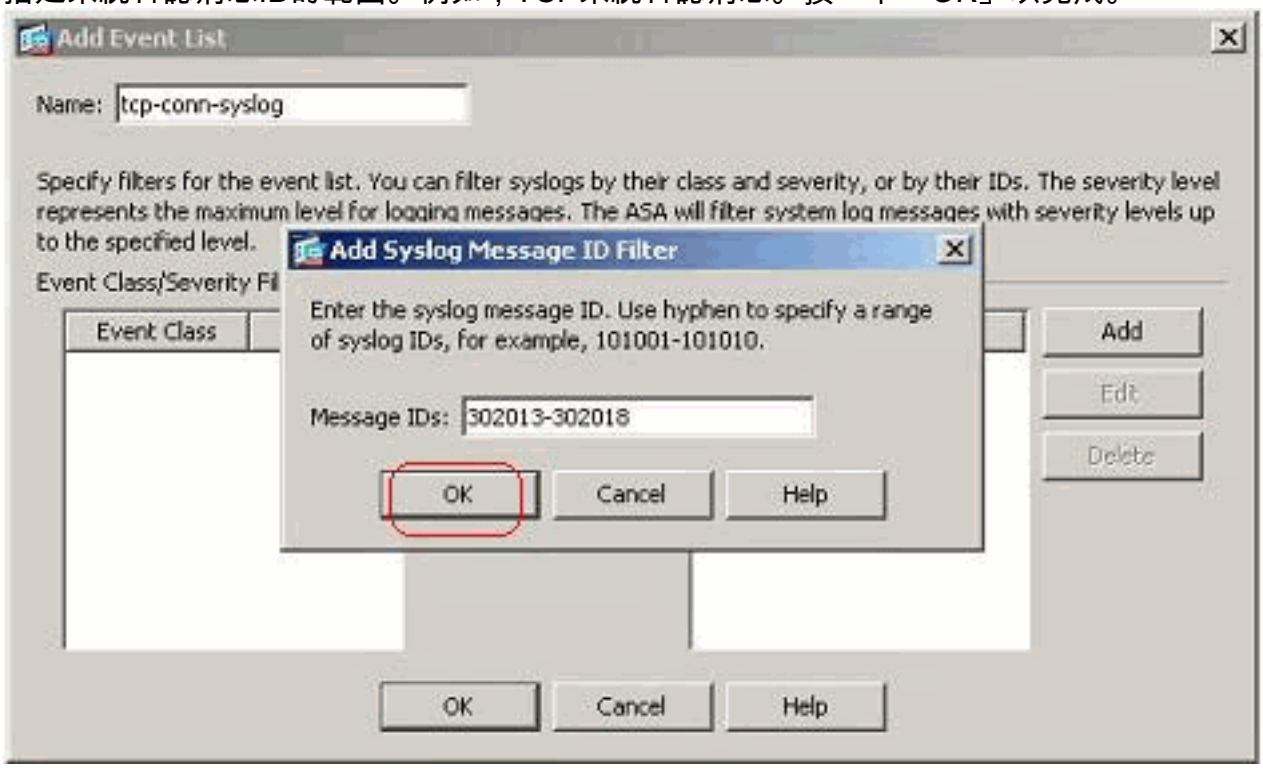
1. 選擇*Configuration > Device Management > Logging > Event Lists*，然後按一下*Add*以建立新的事件清單。



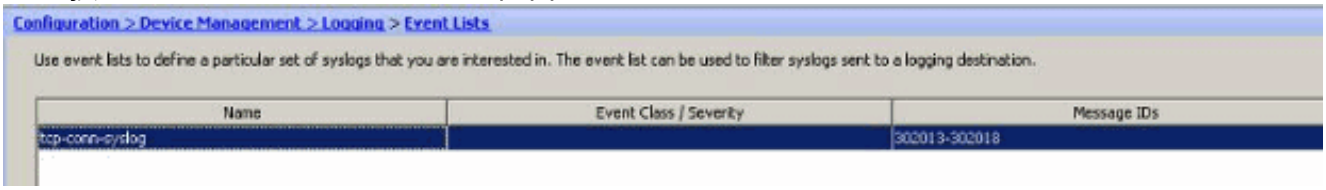
2. 在「名稱」欄位中指定一*個*名稱。在*Message ID Filters*窗格中按一下*Add*，以建立新的事件清單。



3. 指定系統日誌消息ID的範圍。例如，TCP系統日誌消息。按一下「*OK*」以完成。

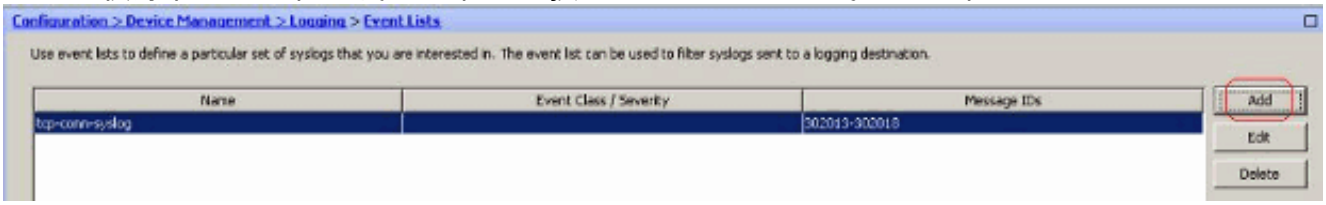


4. 再次按一下*OK*以恢復到*Event Lists*視窗。

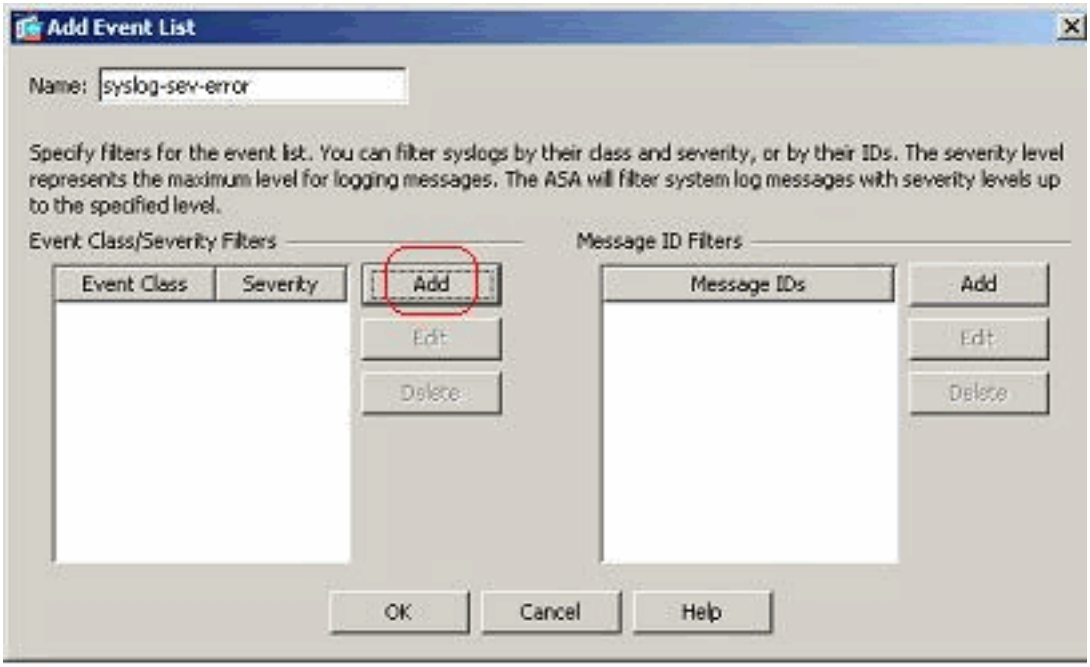


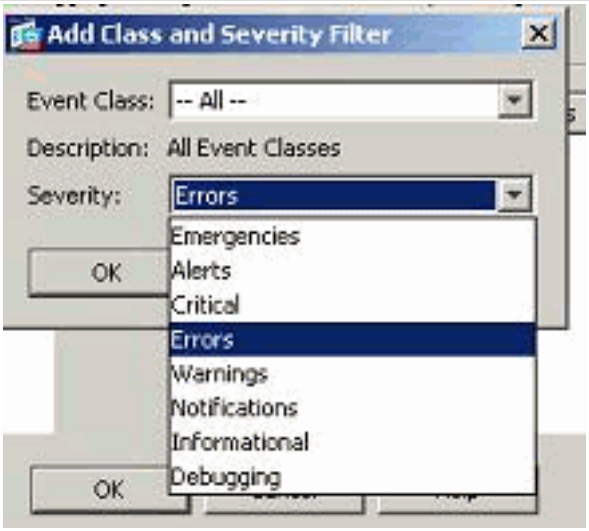
消息嚴重性

1. 還可以根據消息嚴重性定義事件清單。按一下*Add*以建立單獨的事件清單。

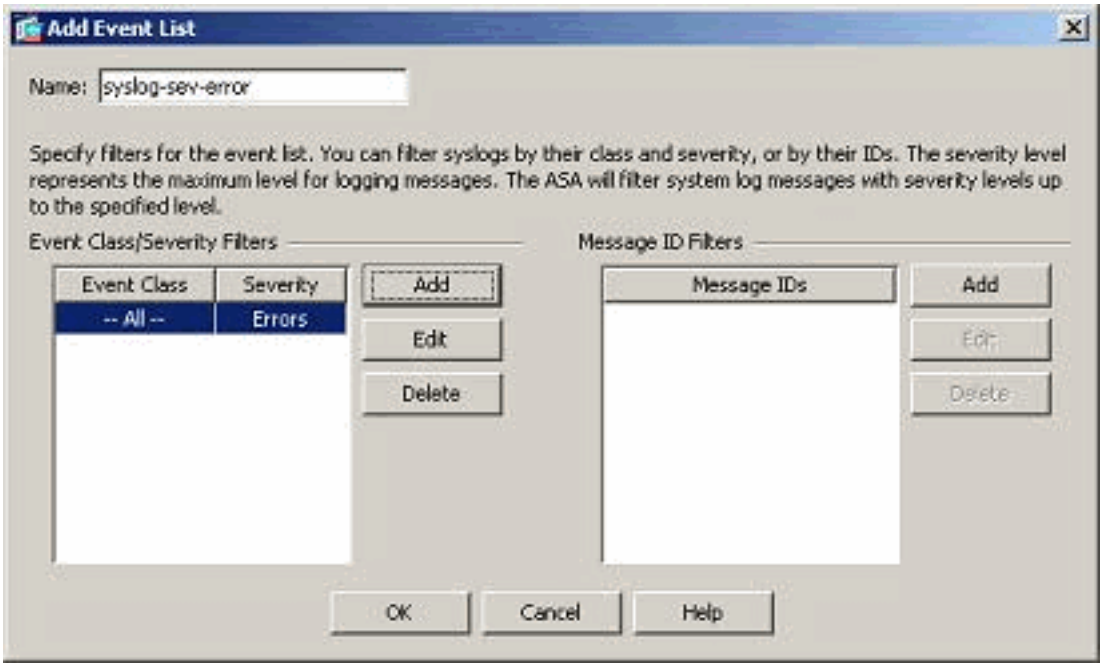


2. 指定名稱並按一下*Add*。





3. 選擇嚴重性級別為*錯誤*。
4. 按一下「*OK*」（確定）。



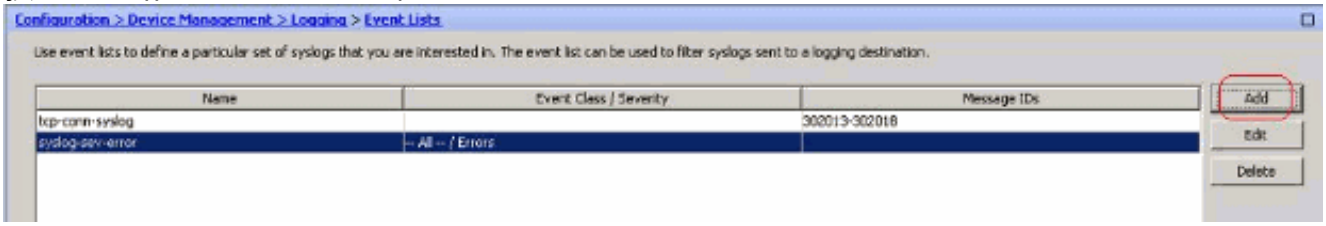
消息類

事件清單也會根據消息類進行配置。消息類是一組與安全裝置功能相關的系統日誌消息，通過該功能，您可以指定整個消息類，而不是為每個消息單獨指定類。例如，使用auth類選擇與使用者身份驗證相關的所有系統日誌消息。下面顯示了一些可用的消息類：

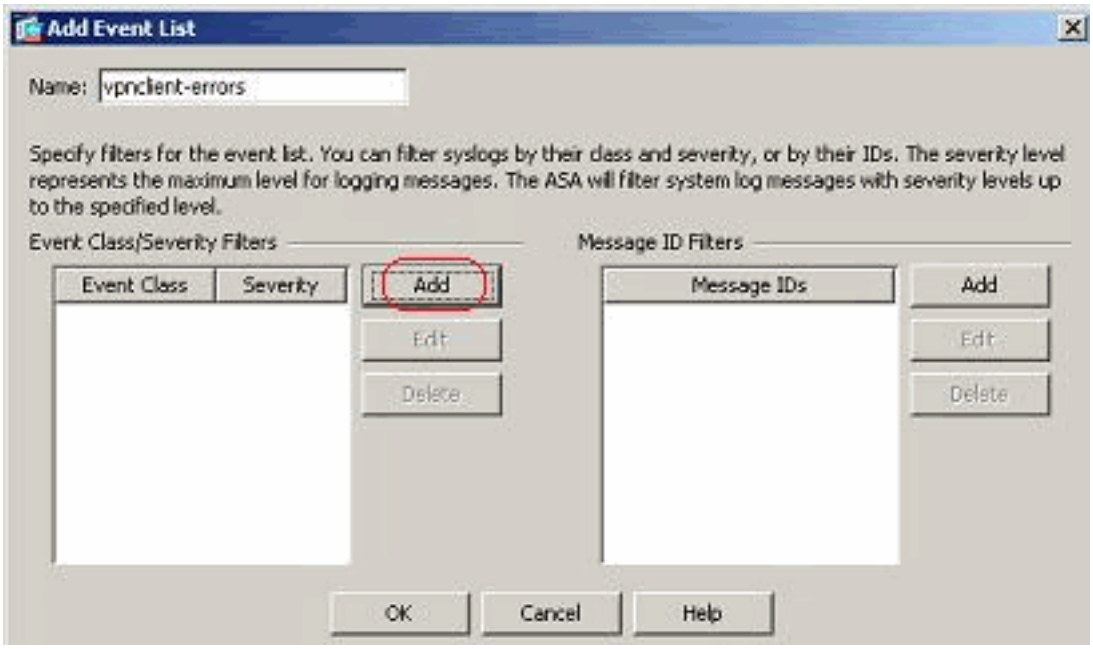
- All — 所有事件類
- auth — 使用者身份驗證
- bridge — 透明防火牆
- ca - PKI證書頒發機構
- config — 命令介面
- ha — 故障轉移
- ips — 入侵防護服務
- ip - IP堆疊
- np — 網路處理器
- ospf - OSPF路由
- rip - RIP路由
- session — 使用者會話

執行以下步驟，根據*vpnclient-errors*消息類建立事件類。消息類*vpnc*可用於對與vpnclient相關的所有系統日誌消息進行分類。此消息類的嚴重性級別選擇為「錯誤」。

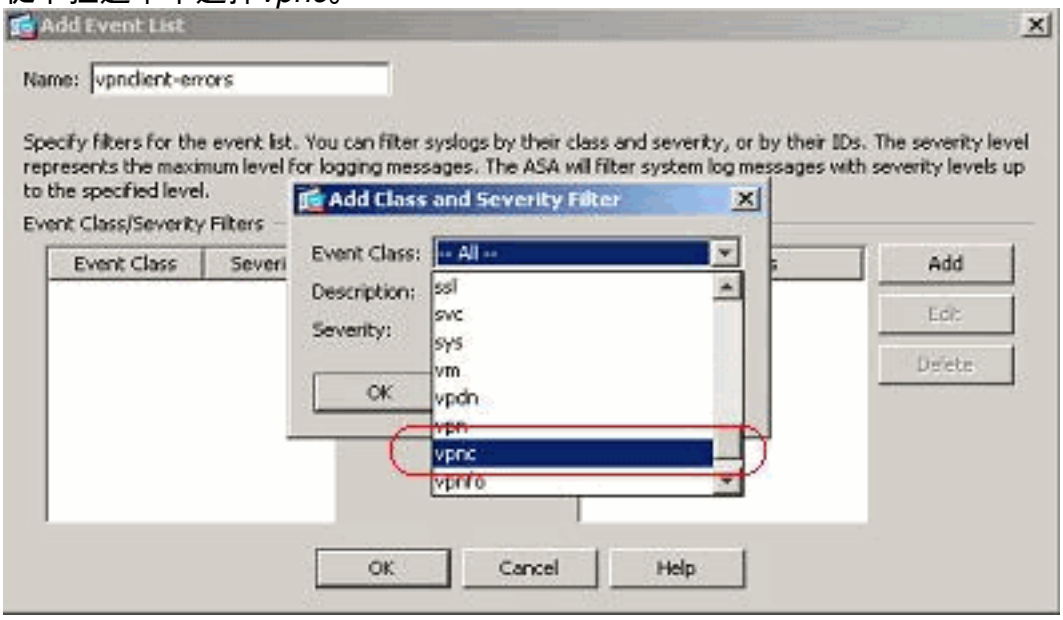
1. 按一下新增以建立新的事件清單。



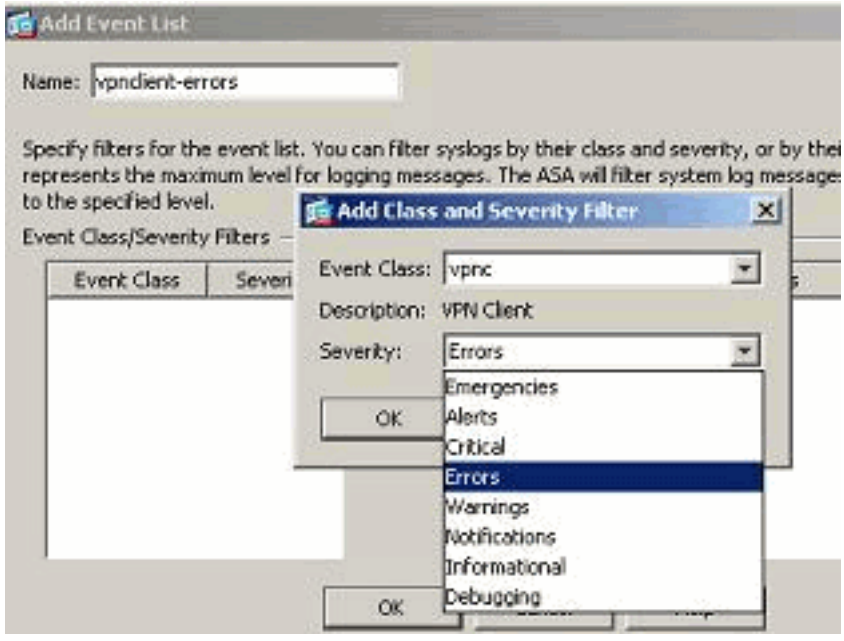
2. 指定要與所建立的消息類相關的名稱，然後按一下*Add*。



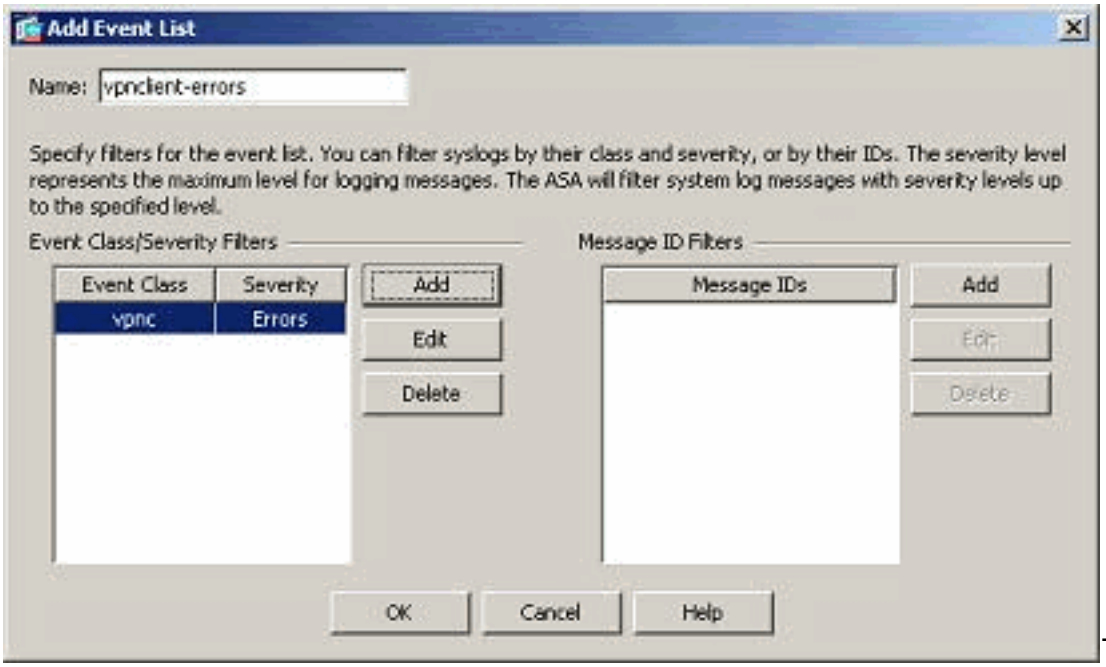
3. 從下拉選單中選擇*vpnc*。



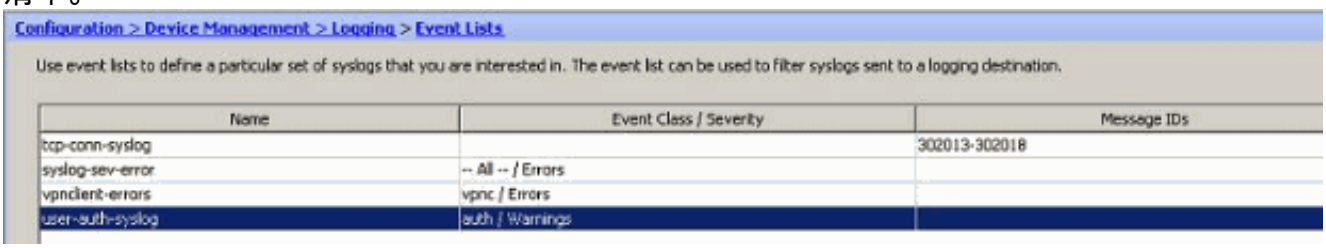
4. 選擇嚴重性級別為*錯誤*。此嚴重性級別僅適用於為此消息類記錄的消息。按一下*OK*以恢復到「新增事件清單」視窗。



5. 此處顯示事件類別/嚴重性。按一下*OK*完成配置「vpnclient-errors」事件清單。



下一個螢幕截圖還顯示，建立了一個新的事件清單「user-auth-syslog」，其中消息類為「auth」，此特定消息類系統日誌的嚴重性級別為「警告」。 通過配置此項，事件清單指定所有與「auth」消息類相關的系統日誌消息，其嚴重性級別最**高**「警告」級別。**註：**在此處，「up」一詞非常重要。指示嚴重性級別時，請記住，在該級別之前將記錄所有系統日誌消息。**註：事**件清單可以包含多個事件類。通過按一下**Edit**並定義新的事件類「ssl/error」來修改「vpnclient-errors」事件清單。



使用日誌記錄過濾器

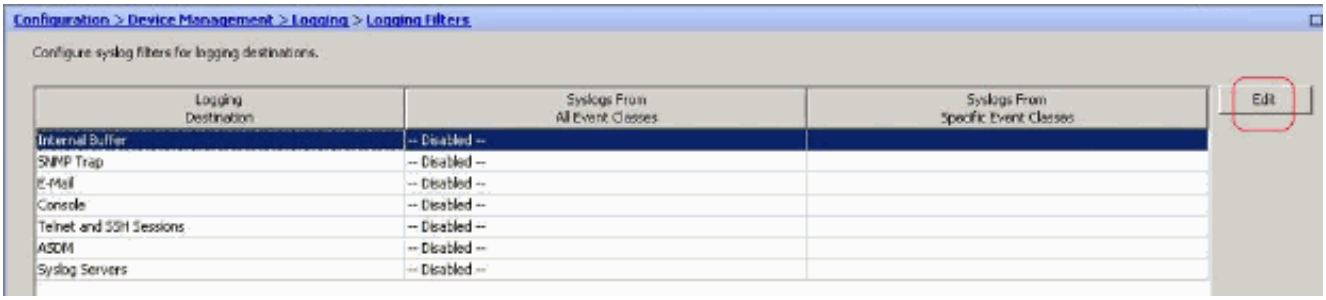
日誌過濾器用於將系統日誌消息傳送到指定的目標。這些系統日誌消息可以基於「嚴重性」或「偶數清單」。

以下是這些篩選條件適用的目的地型別：

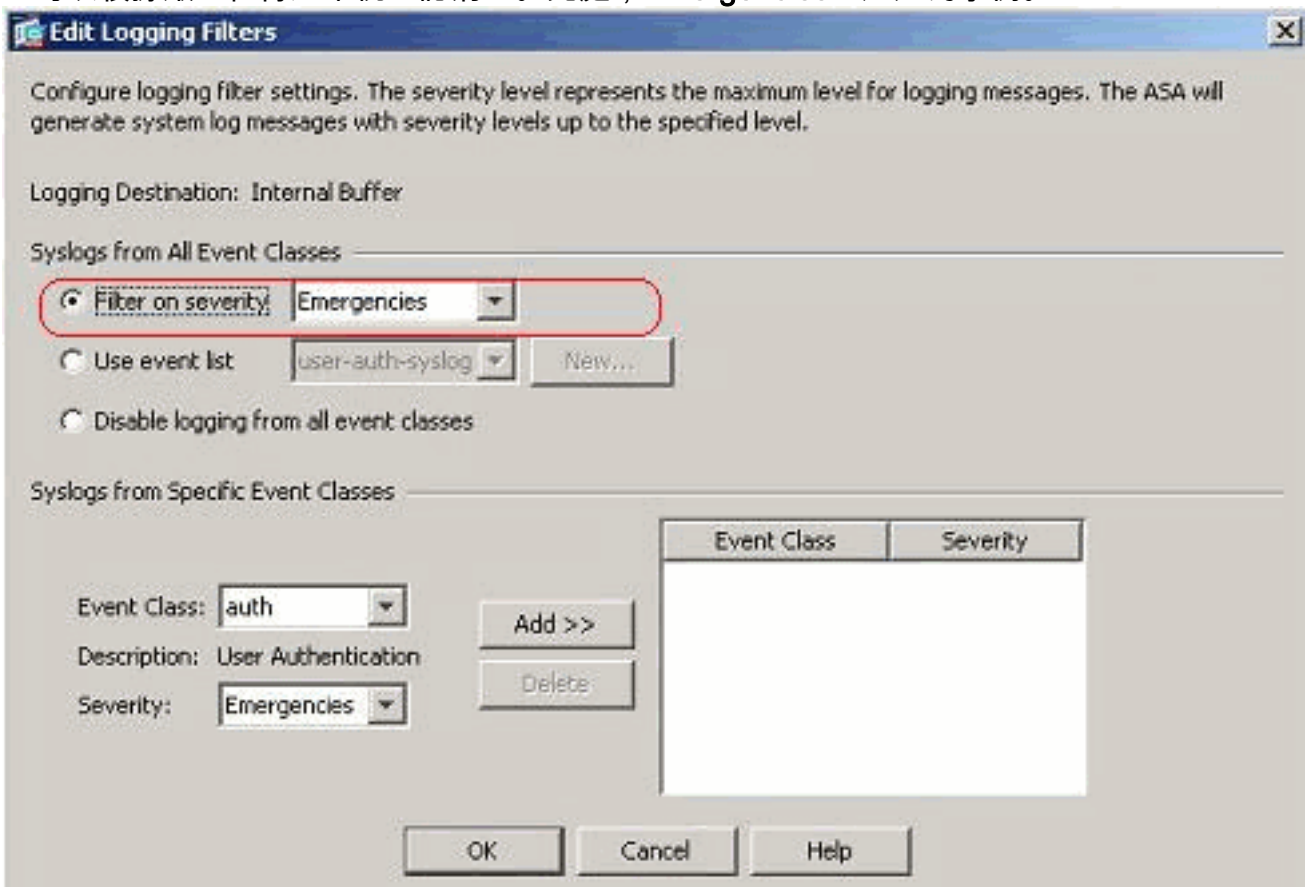
- 內部緩衝區
- SNMP陷阱
- 電子郵件
- 主控台
- Telnet作業階段
- ASDM
- 系統日誌伺服器

請執行以下步驟：

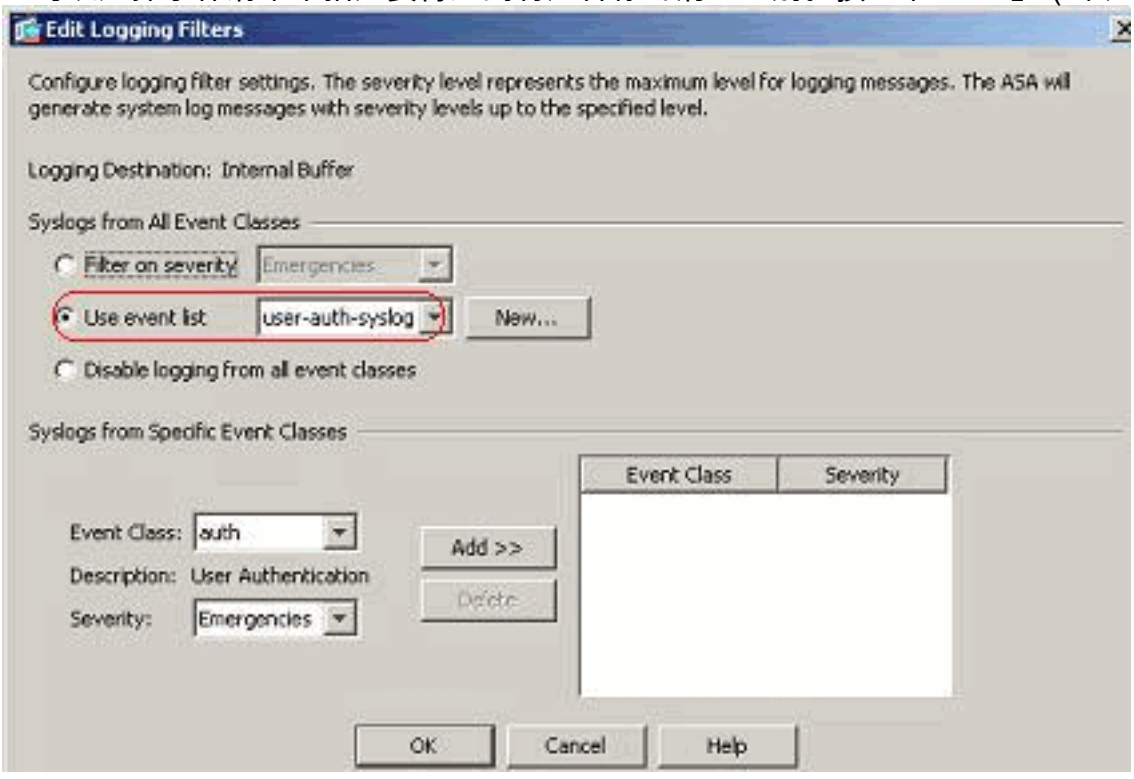
1. 選擇**Configuration > Device Management > Logging > Logging Filters**，然後選擇日誌記錄目標。然後，按一下**Edit**修改設定。



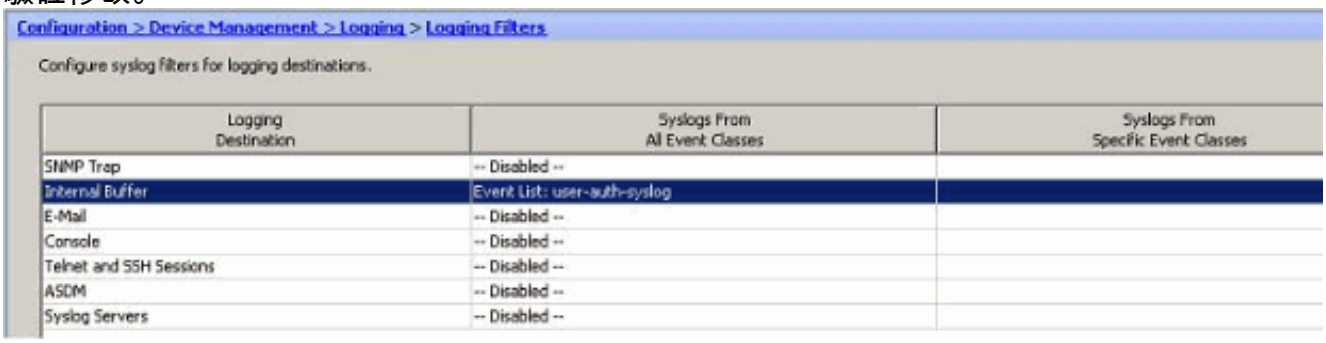
2. 您可以根據嚴重性傳送系統日誌消息。此處，**Emergencies**已選定為示例。



3. 也可以選擇事件清單來指定要傳送到特定目標的消息型別。按一下「**OK**」（確定）。

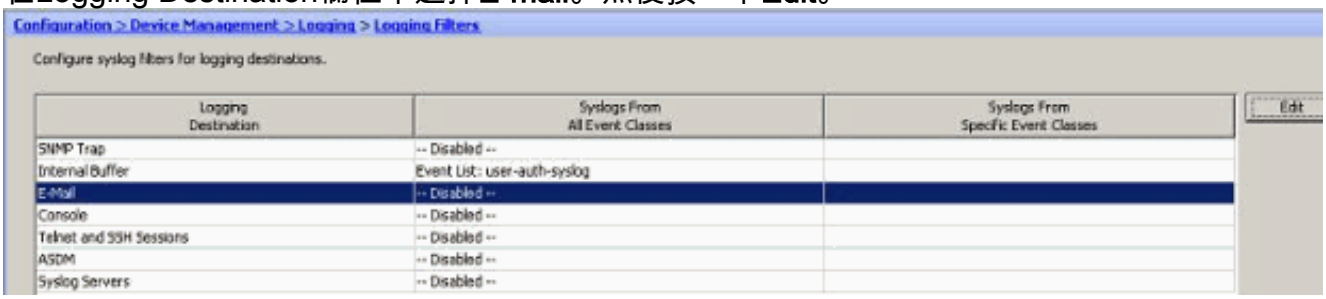


4. 驗證修改。

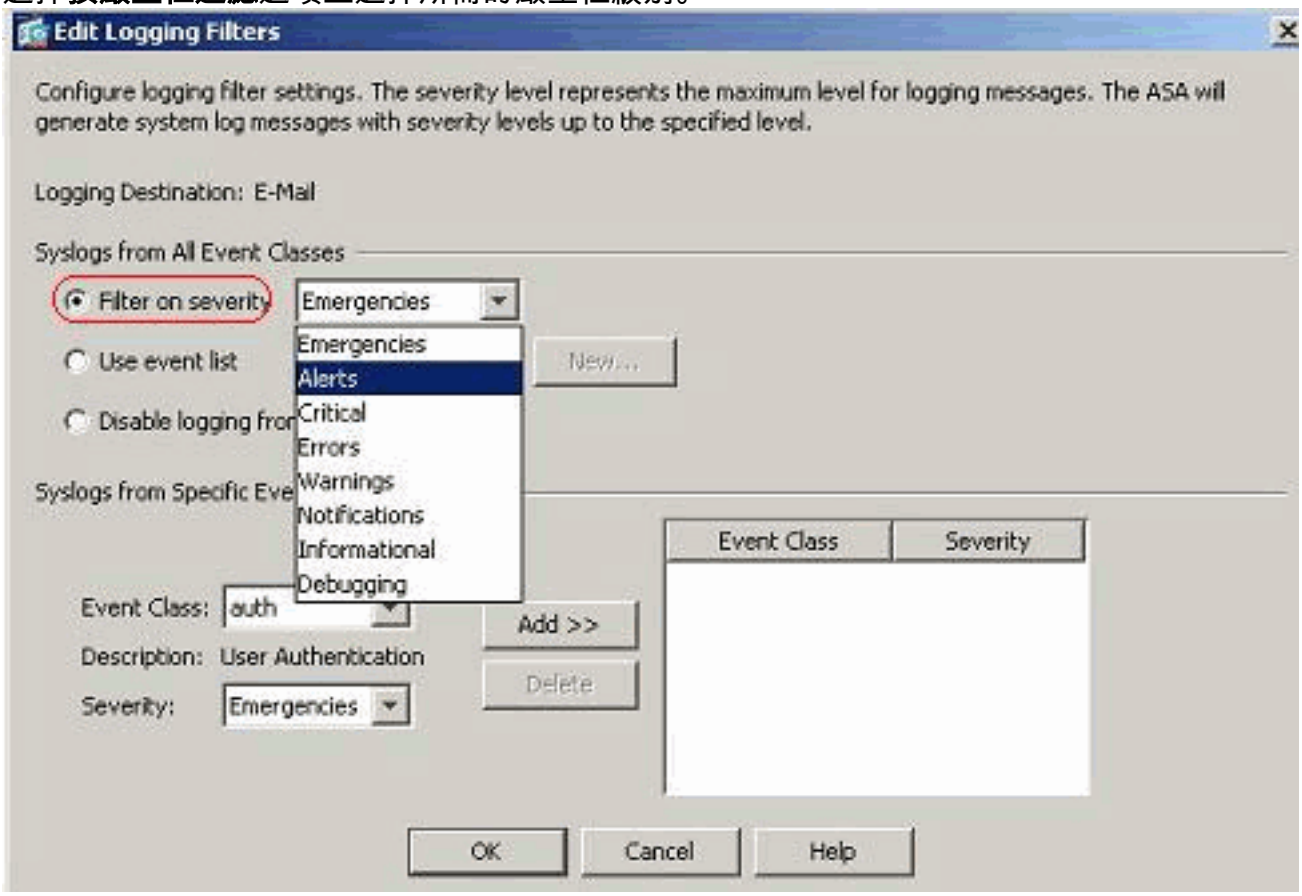


以下是有關如何將一組郵件（根據其嚴重性級別）傳送到電子郵件伺服器的步驟。

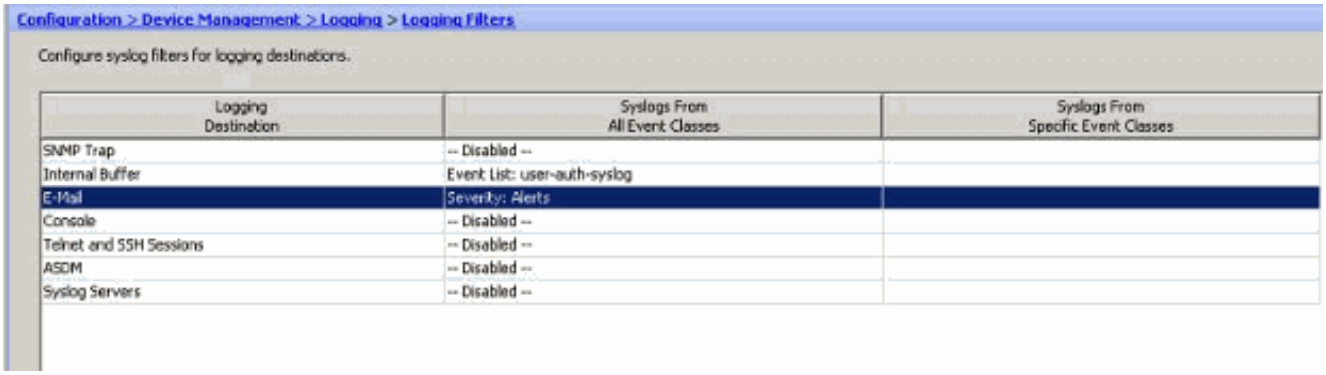
1. 在Logging Destination欄位中選擇**E-mail**。然後按一下**Edit**。



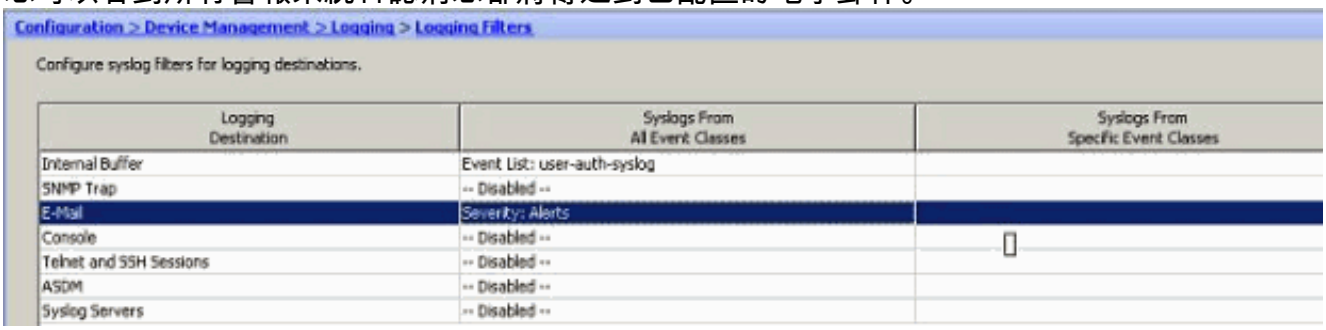
2. 選擇**按嚴重性過濾**選項並選擇所需的嚴重性級別。



此處，已選擇**Alerts**作為嚴重性級別。



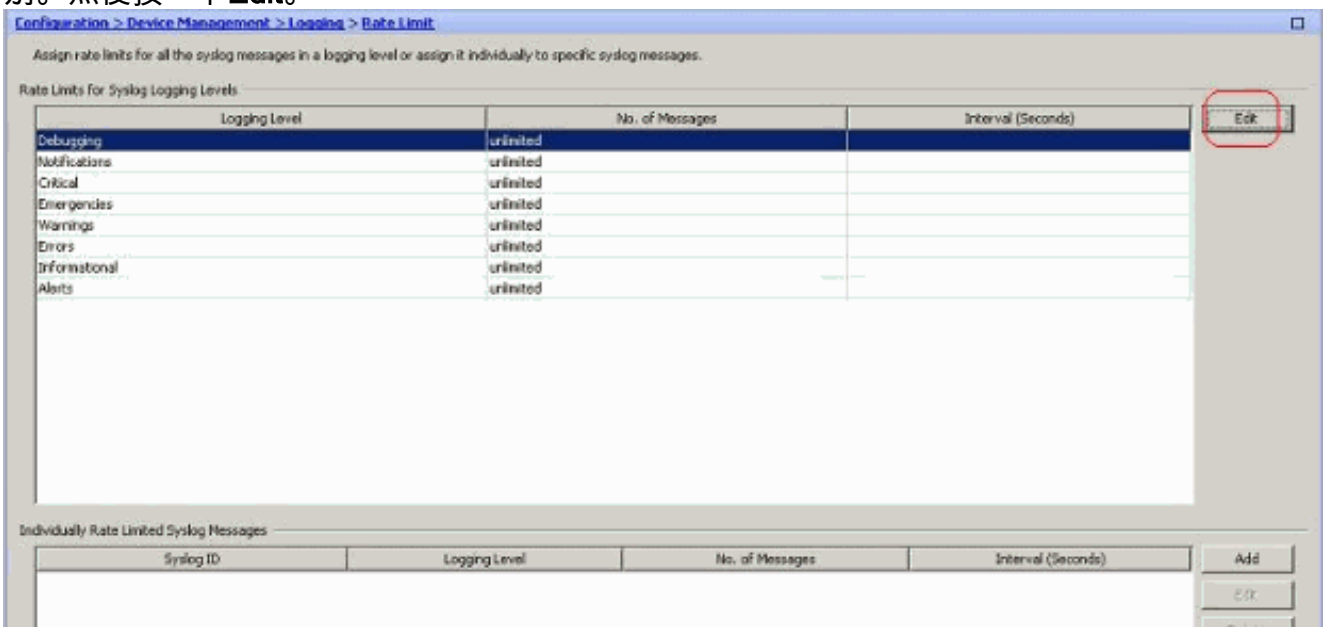
您可以看到所有警報系統日誌消息都將傳送到已配置的電子郵件。



速率限制

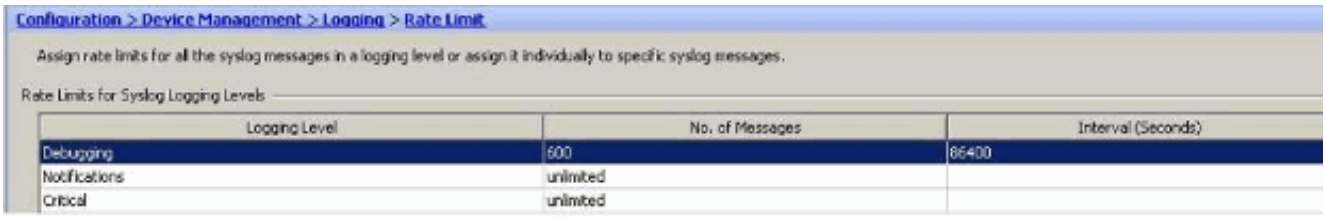
這指定Cisco ASA在指定時間段內傳送到目標的系統日誌消息數。通常針對嚴重性級別進行定義。

1. 選擇**Configuration > Device Management > Logging > Rate Limit**，然後選擇所需的嚴重性級別。然後按一下**Edit**。



2. 指定隨時間間隔一起傳送的消息數。按一下「**OK**」（確定）。

註：以下數字為例。它們因網路環境的型別而異。修改的值如下所示：

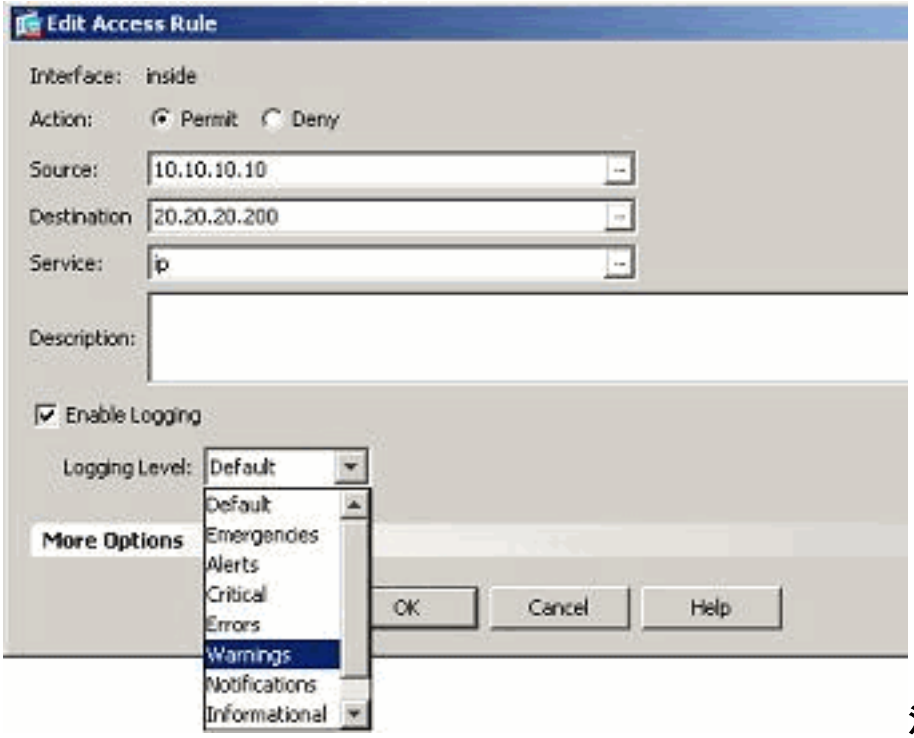


記錄訪問規則的命中數

您可以使用ASDM記錄訪問規則命中數。預設日誌記錄行為是向所有被拒絕的資料包傳送系統日誌消息。對於允許的資料包，不會出現任何系統日誌消息，並且不會記錄這些消息。但是，您可以為訪問規則定義自定義日誌記錄嚴重性級別，以跟蹤達到此訪問規則的資料包計數。

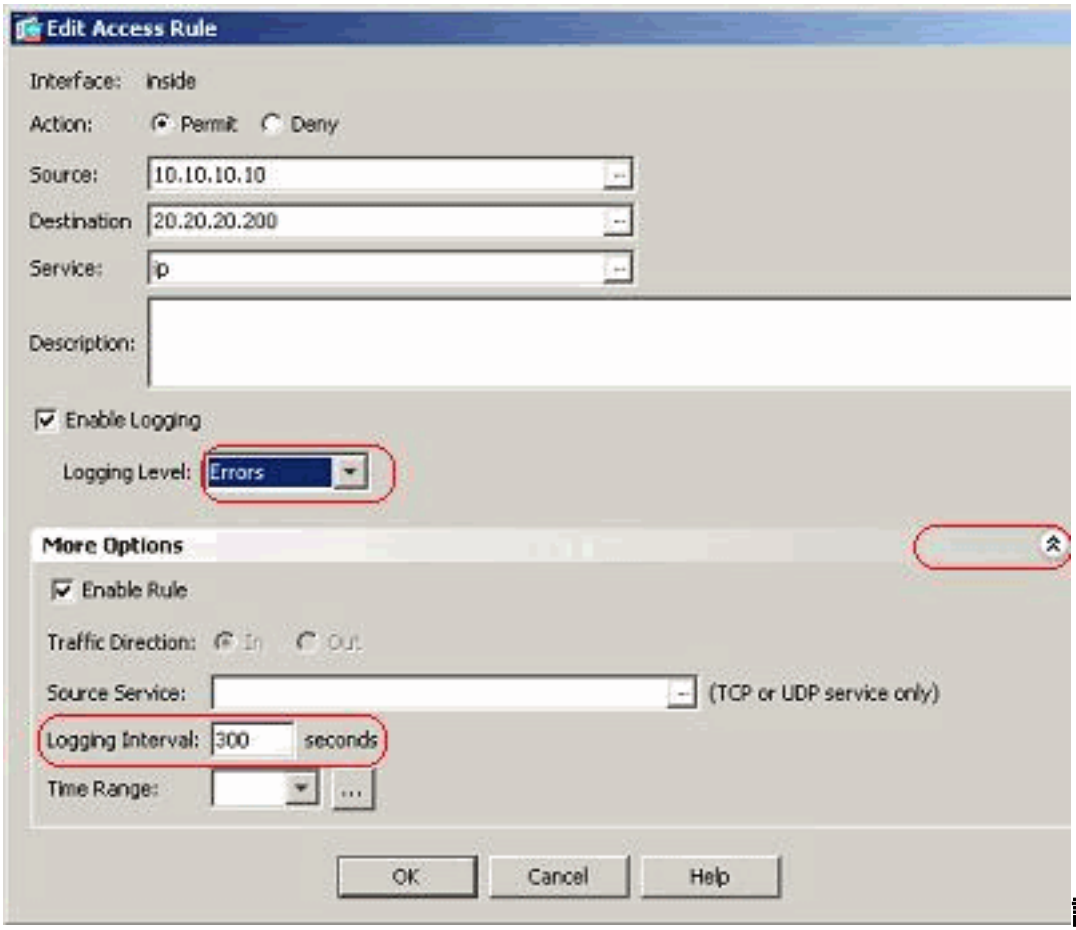
請執行以下步驟：

1. 選擇所需的訪問規則，然後按一下*Edit*。出現*Edit the Access Rule*視窗。



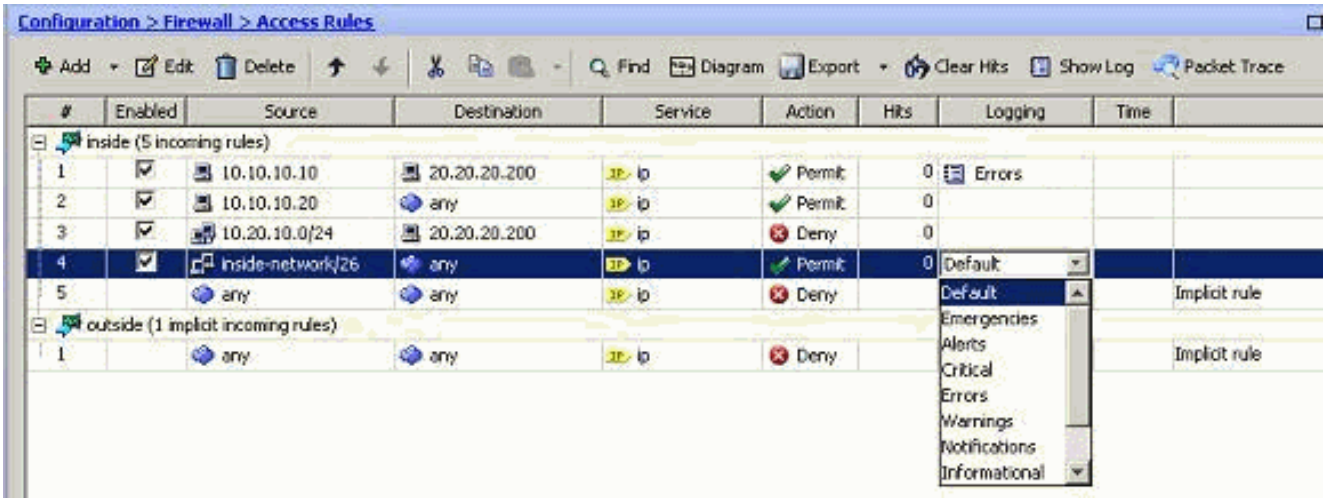
注意：在此映像中，*Logging Level***欄位中的***Default*選項表示Cisco ASA的預設日誌記錄行為。有關此問題的詳細資訊，請參閱日誌記錄訪問清單活動部分。

2. 選中標籤*Enable logging*選項並指定所需的嚴重性級別。然後，按一下*OK*。



註：通過按一下「*更多*選項」下拉標籤，您可以看到「記錄*間隔*」選項。僅當勾選上面的*Enable Logging*選項時，才會突出顯示此選項。此計時器的預設值為300秒。此設定可用於指定當該訪問規則沒有匹配項時要刪除的流統計資訊的超時值。如果有任何命中，則ASA將等待「日誌記錄間隔」時間，並將其傳送到系統日誌。

3. 此處顯示修改內容。或者，您可以按兩下特定訪問規則的*Logging*欄位，並在其中設定嚴重性級別。



注意：通過按兩下在同一*Access Rules***窗格中指定***Logging Level*的此替代方法僅適用於手動建立的訪問規則條目，不適用於隱式規則。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

組態

本檔案會使用以下設定：

CiscoASA

```
: 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
```

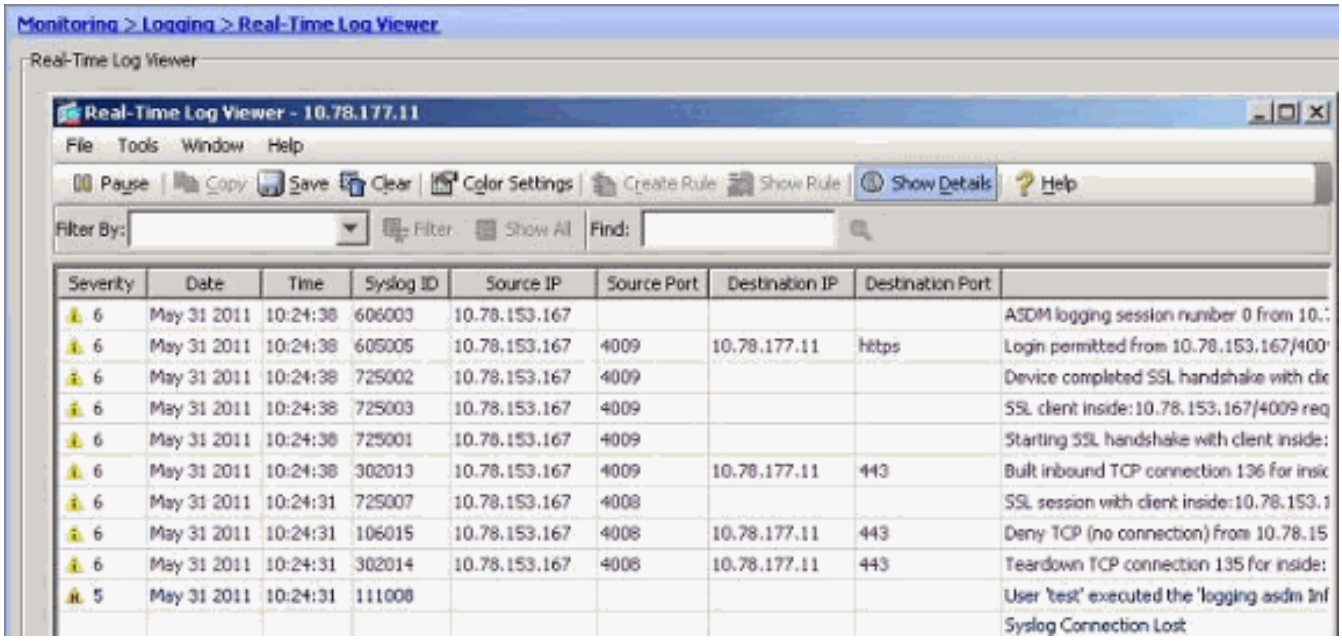
```
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-623.bin
asdm history enable
arp timeout 14400
!!--- Output Suppressed ! timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- 您可以從ASDM檢視系統日誌。選擇Monitoring > Logging > Real Time Log Viewer。輸出示例如下所示
  :



疑難排解

問題：連線丟失 — 系統日誌連線已終止 —

當嘗試在裝置控制面板上為任何情景啟用ASDM日誌記錄時，會收到此錯誤。

```
" — Syslog — "
```

當使用ASDM直接連線到管理情景並且那裡禁用了ADSM日誌記錄時，請切換到子情景並啟用ASDM日誌記錄。收到錯誤，但syslog消息到達syslog伺服器時正常。

解決方案

這是Cisco ASDM的已知行為，記錄在Cisco錯誤ID CSCsd1069(僅限註冊客戶)。 作為解決方法，請在登入到管理情景時啟用asdm日誌記錄。

無法檢視Cisco ASDM上的即時日誌

一個問題是，無法在ASDM上檢視即時日誌。此配置如何？

解決方案

在Cisco ASA上配置以下內容：

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

相關資訊

- Cisco ASA 5500系列自適應安全裝置支援
- 技術支援與文件 - Cisco Systems