配置自適應安全裝置(ASA)系統日誌

目錄

簡介

本文檔介紹的示例配置演示如何在運行代碼版本8.4或更高版本的ASA上配置不同的日誌記錄選項。

背景資訊

ASA版本8.4引入了非常精細的過濾技術，以便僅允許顯示某些指定的系統日誌消息。本文檔的基本系統日誌部分演示了傳統的系統日誌配置。本文檔的「高級Syslog」部分顯示8.4版中的新Syslog功能。有關完整的系統日誌消息指南，請參閱Cisco安全裝置系統日誌消息指南。

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：

- 具備ASA軟體版本8.4的ASA 5515
- 思科調適型安全裝置管理員(ASDM)版本7.1.6

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

註：有關ASDM版本7.1及更高版本的類似配置詳細資訊，請參閱ASA 8.2：使用ASDM配置系統日誌。

基本系統日誌

輸入以下命令以啟用日誌記錄、檢視日誌和檢視配置設定。

- logging enable -允許將Syslog消息傳輸到所有輸出位置。
- no logging enable - 禁止記錄到所有輸出位置。
- show logging - 列出Syslog緩衝區的內容，以及與當前配置相關的資訊和統計資訊。

ASA可以將系統日誌消息傳送到各種目的地。在這些部分輸入命令以指定希望傳送系統日誌資訊的位置：

將日誌記錄資訊傳送到內部緩衝區

```
<#root>

logging buffered

 severity_level
```

將系統日誌消息儲存在ASA內部緩衝區中時，不需要外部軟體或硬體。輸入show logging命令以檢視儲存的Syslog消息。內部緩衝區的最大大小為1 MB(可透過logging buffer-size命令進行配置)。因此，可以非常快速地將其包覆。在為內部緩衝區選擇日誌記錄級別時，請記住這一點，因為更詳細的日誌記錄級別可以快速填充和包裝內部緩衝區。

將日誌記錄資訊傳送到系統日誌伺服器

```
<#root>

logging host

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

logging trap

 severity_level

logging facility

 number
```

需要運行系統日誌應用程式的伺服器才能將系統日誌消息傳送到外部主機。預設情況下，ASA在UDP埠514上傳送syslog，但可以選擇協定和埠。如果選擇TCP作為日誌記錄協定，則這會導致ASA透過到系統日誌伺服器的TCP連線傳送系統日誌。如果伺服器無法訪問，或者無法與伺服器建立TCP連線，預設情況下，ASA會阻止所有新連線。如果啟用logging permit-hostdown，則可以停用此行為。有關logging permit-hostdown命令的詳細資訊，請參閱配置指南。

注意：ASA僅允許範圍從1025-65535的埠。使用任何其他連線埠都會導致以下錯誤：
ciscoasa(config)# logging host tftp 192.168.1.1 udp/516
警告：介面Ethernet0/1安全級別為0。
錯誤：埠「516」不在1025-65535範圍內。

以電子郵件傳送記錄資訊

```
<#root>

logging mail

 severity_level

logging recipient-address

 email_address

logging from-address

 email_address

smtp-server

 ip_address
```

在電子郵件中傳送系統日誌消息時需要SMTP伺服器。為了確保可以成功將電子郵件從ASA中繼到指定的電子郵件客戶端，必須在SMTP伺服器上進行正確的配置。如果此日誌記錄級別設定為非常詳細的級別(如調試或資訊性)，則您可以生成大量系統日誌，因為此日誌記錄配置傳送的每封電子郵件都會導致生成多達四個或更多附加日誌。

將記錄資訊傳送至序列主控台

<#root>

```
logging console
 severity_level
```

控制檯日誌記錄使系統日誌消息可以在發生時顯示在ASA控制檯(tty)上。如果配置了控制檯日誌記錄，則ASA上的所有日誌生成速率限制為9800 bps，即ASA串列控制檯的速度。這可能導致系統日誌被丟棄到所有目標，包括內部緩衝區。因此，請勿對詳細系統日誌使用控制檯日誌記錄。

將日誌記錄資訊傳送到Telnet/SSH會話

<#root>

```
logging monitor
 severity_level
terminal monitor
```

日誌記錄監控器允許您在透過Telnet或SSH訪問ASA控制檯時立即顯示系統日誌消息，並從該會話執行terminal monitor命令。要停止將日誌列印到會話中，請輸入terminal no monitor命令。

顯示ASDM上的日誌消息

<#root>

```
logging asdm
 severity_level
```

ASDM還具有可用於儲存系統日誌消息的緩衝區。輸入show logging asdm命令以顯示ASDM Syslog緩衝區的內容。

將日誌傳送到SNMP管理站

<#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

使用者需要一個現有的功能簡單網路管理協定(SNMP)環境，以便使用SNMP傳送系統日誌消息。有關可以用來設定和管理輸出目標的命令的完整參考，請參閱用於設定和管理輸出目標的命令。有關按嚴重性級別列出的消息，請參閱按嚴重性級別列出的消息。

將時間戳增加到系統日誌

為了幫助協調和排序事件，可以將時間戳增加到syslog。建議使用此選項，以便幫助根據時間跟蹤問題。要啟用時間戳，請輸入logging timestamp命令。以下是兩個系統日誌示例，一個沒有時間戳，另一個帶有：

```
%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
```

範例 1

此輸出顯示了使用debugging的嚴重性級別登入緩衝區的示例配置。

<#root>

logging enable
logging buffered debugging

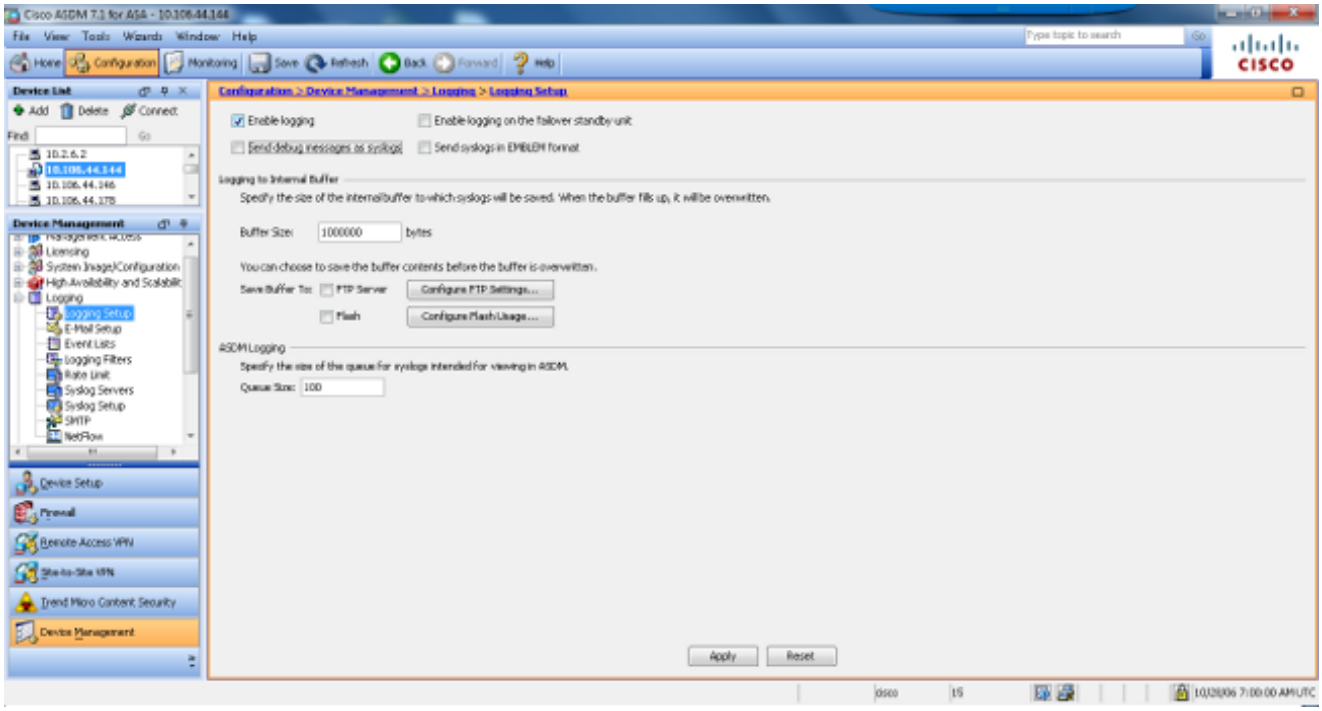
以下是輸出示例。

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

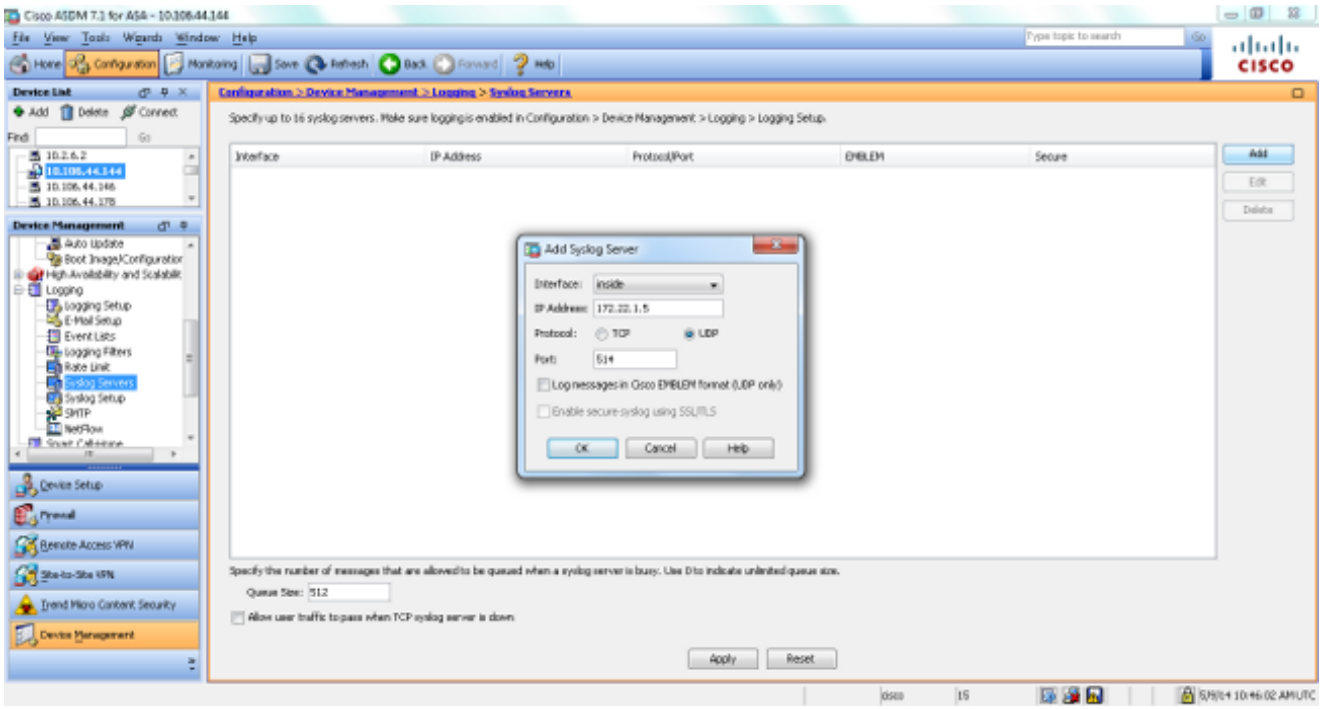
使用ASDM配置基本系統日誌

此過程演示所有可用系統日誌目標的ASDM配置。

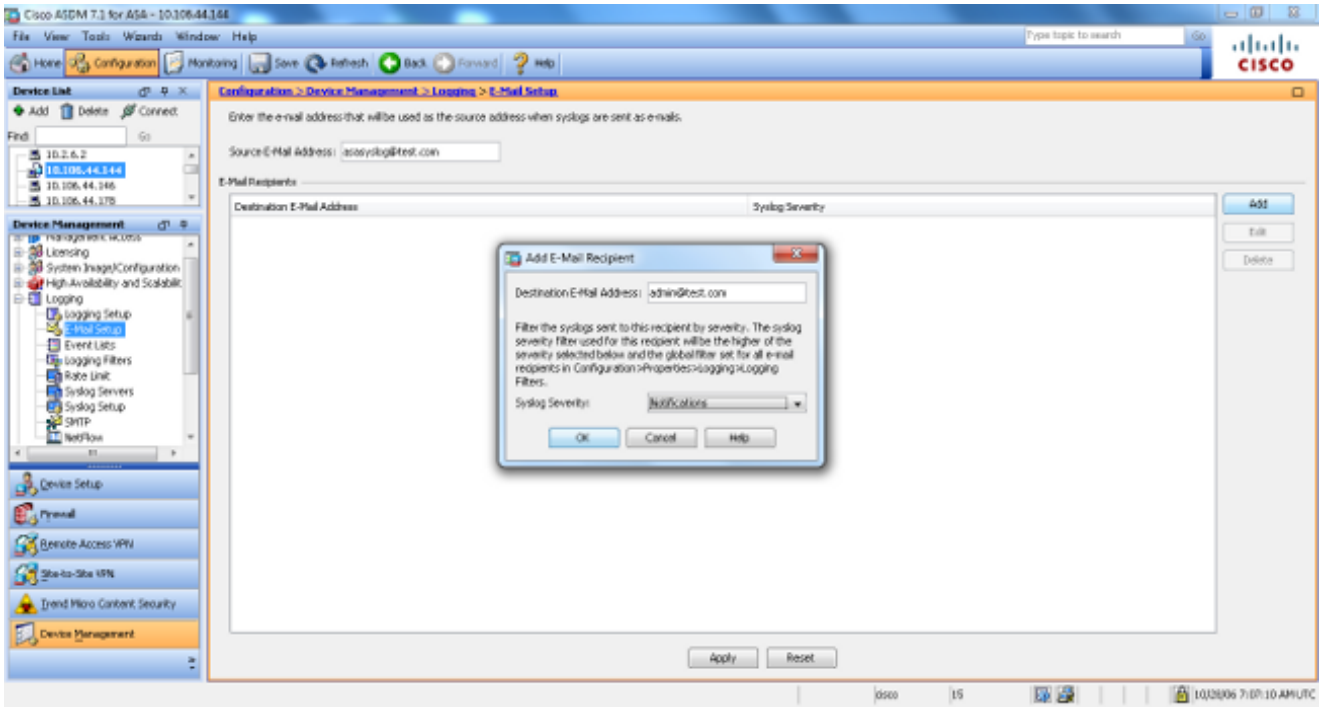
1. 要在ASA上啟用日誌記錄，首先配置基本日誌記錄引數。選擇Configuration > Features > Properties > Logging > Logging Setup。選中Enable logging覈取方塊以啟用Syslog。



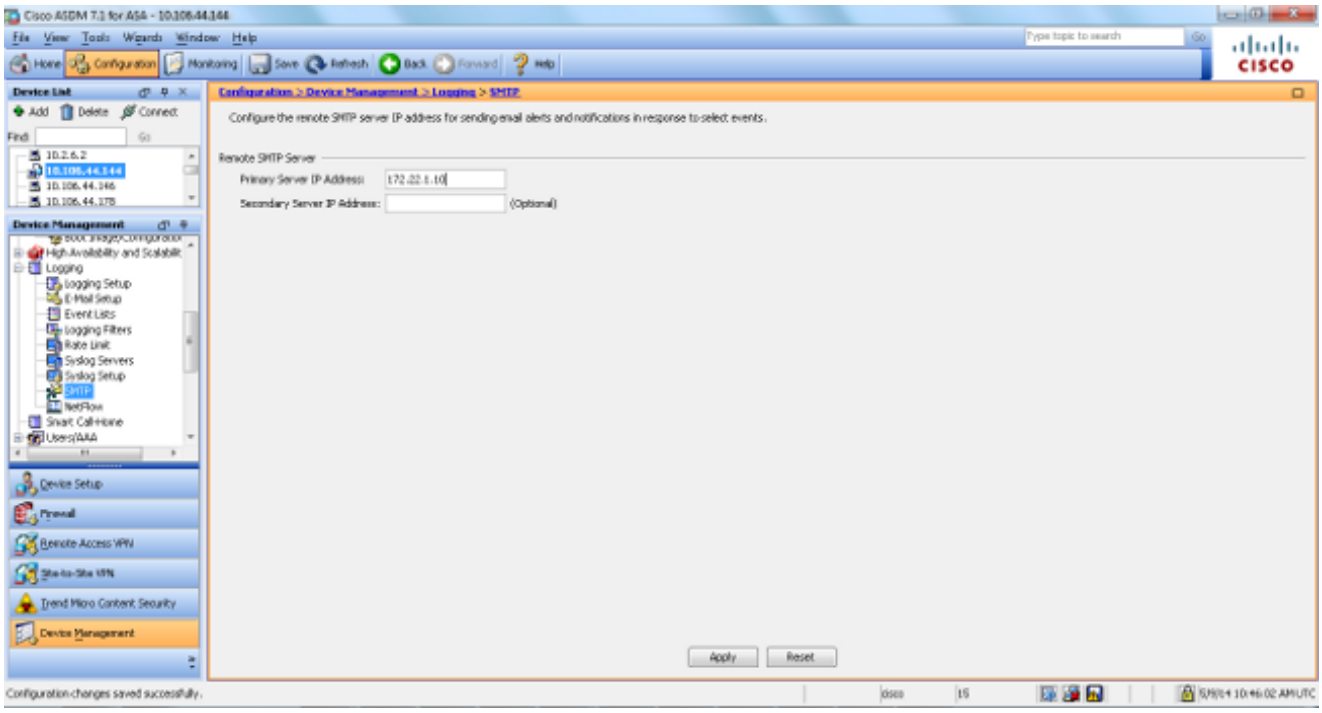
2. 要將外部伺服器配置為系統日誌的目標，請在Logging中選擇Syslog Servers並按一下Add以增加Syslog伺服器。在Add Syslog Server框中輸入Syslog伺服器詳細資訊，並在完成後選擇OK。



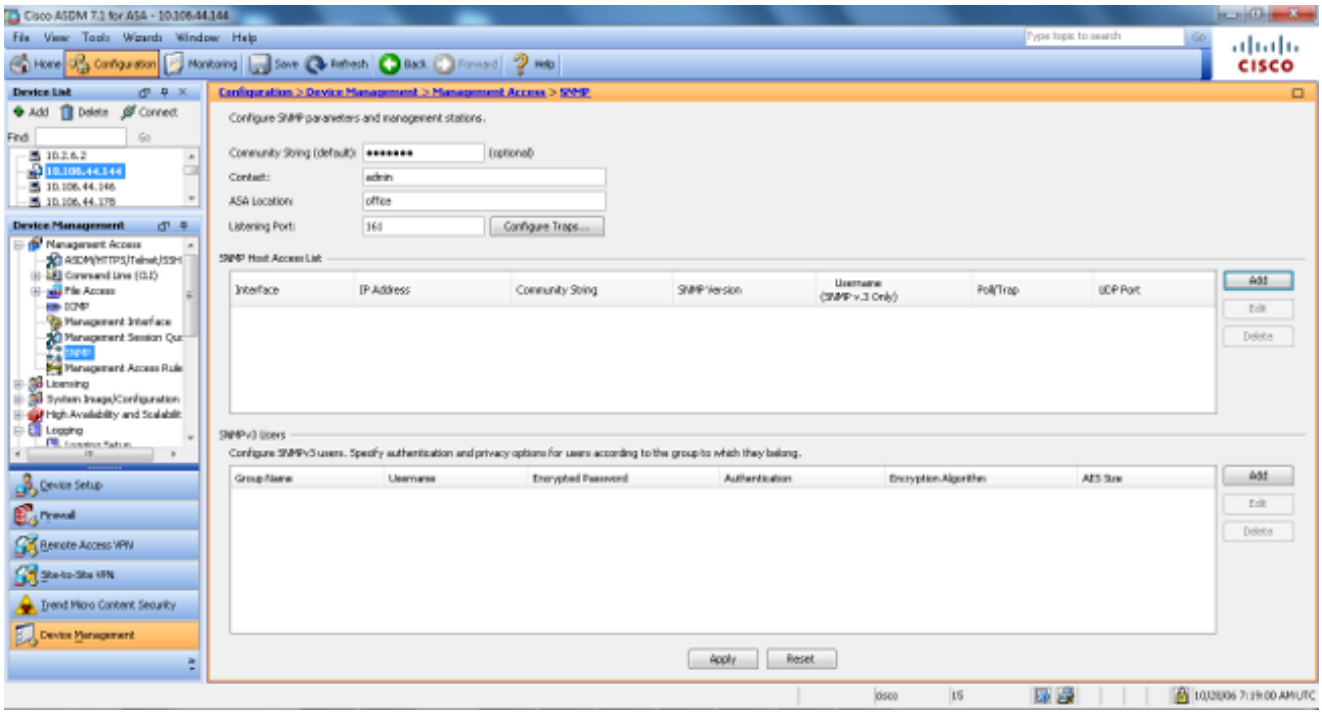
3. 選擇Logging中的E-Mail Setup 以將Syslog消息作為電子郵件傳送給特定收件人。在Source E-Mail Address框中指定源電子郵件地址，並選擇Add 以配置電子郵件收件人的目標電子郵件地址和消息嚴重性級別。完成後按一下OK。



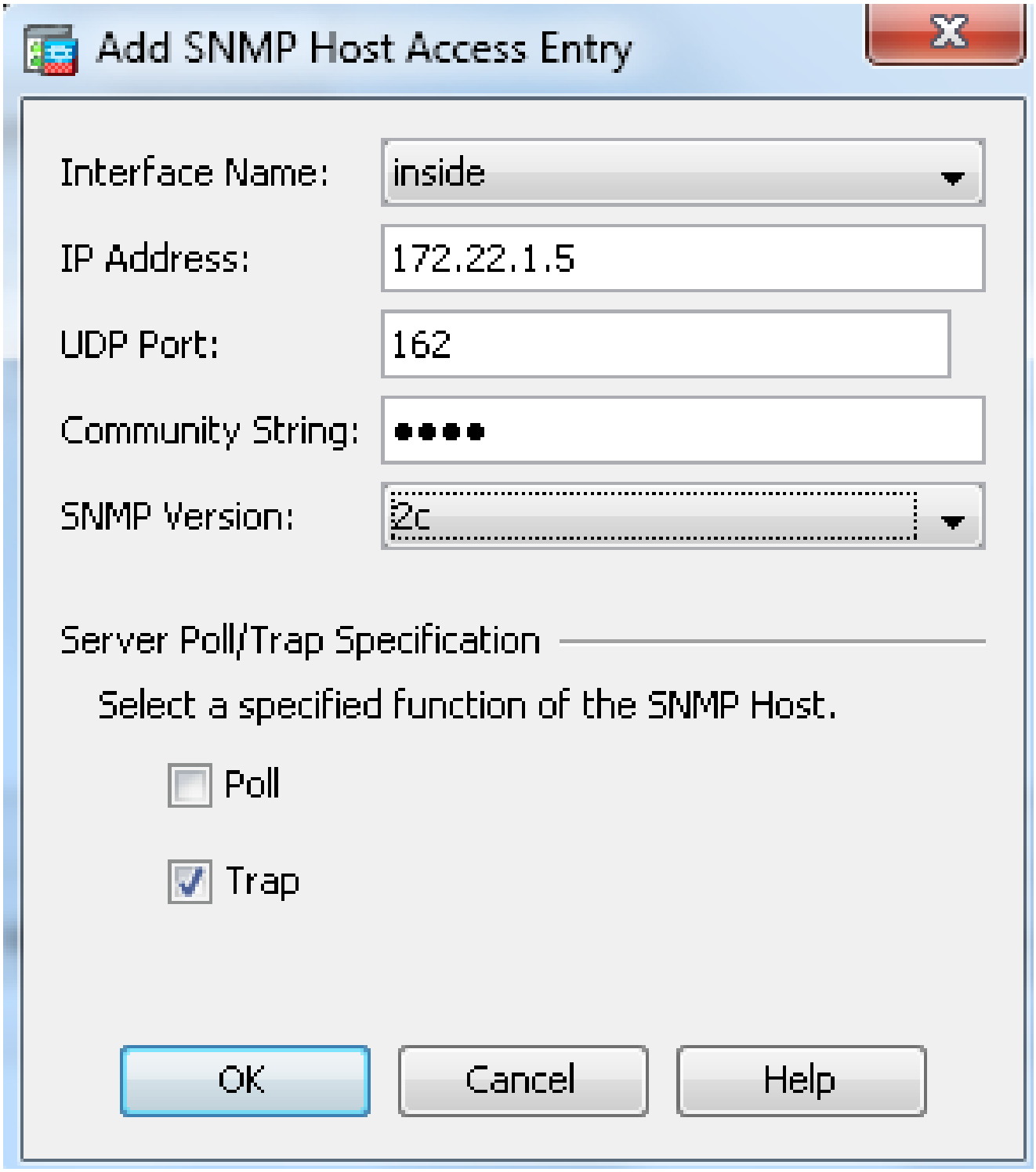
4. 選擇Device Administration、Logging、選擇SMTP，然後輸入主伺服器IP地址以指定SMTP伺服器IP地址。



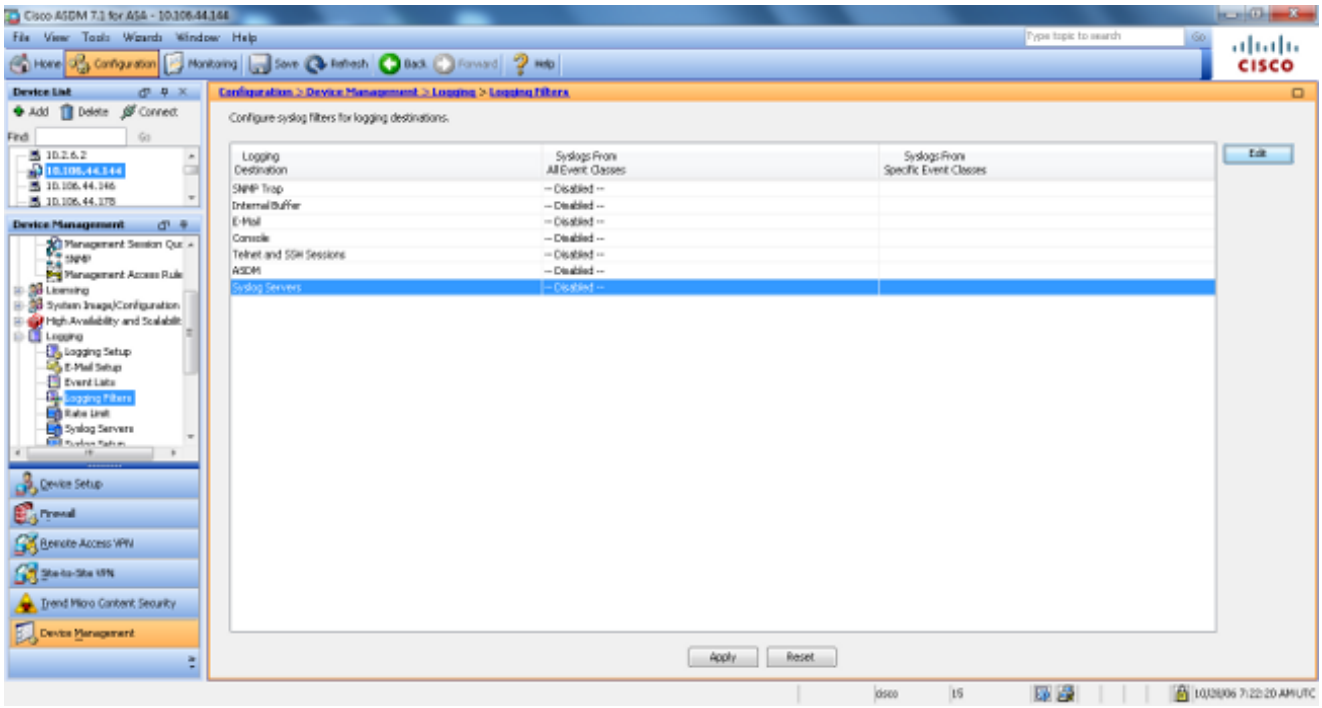
5. 如果要將系統日誌作為SNMP陷阱傳送，則必須首先定義SNMP伺服器。在Management Access 選單中選擇SNMP以指定SNMP管理站的地址及其特定屬性。



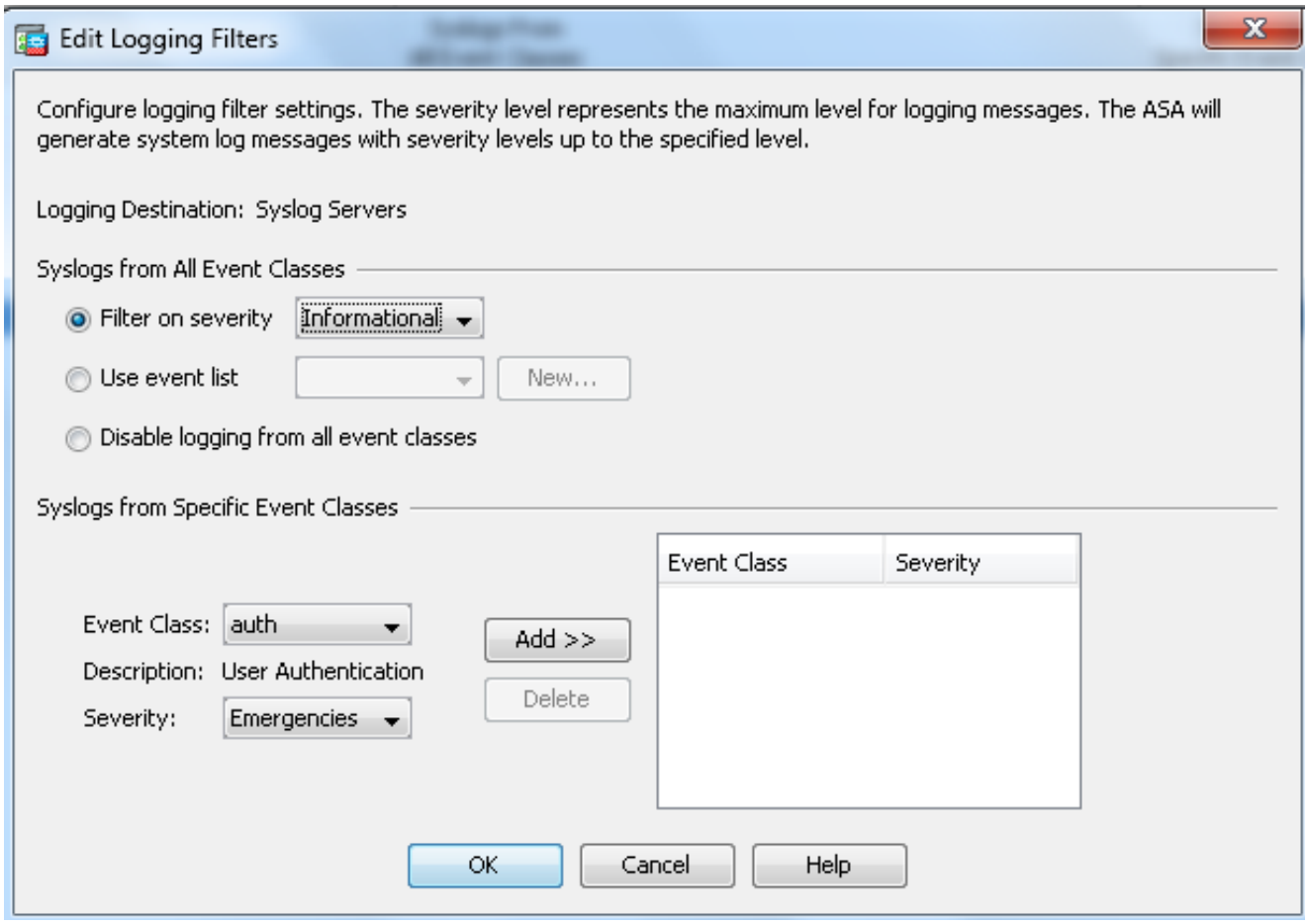
6. 選擇Add以增加SNMP管理站。輸入SNMP主機詳細資訊並按一下OK。



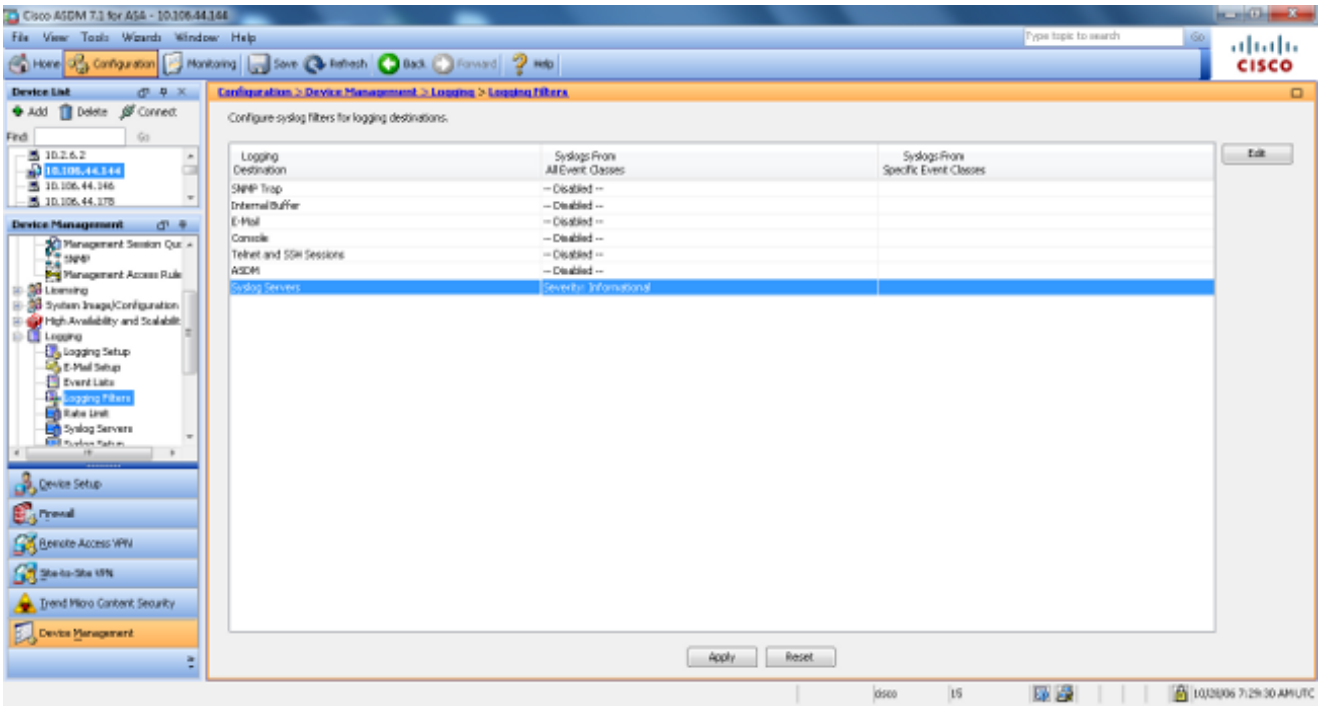
7. 要允許將日誌傳送到前面提到的任何目標，請在logging部分中選擇Logging Filters。這會顯示每個可能的日誌記錄目標和傳送到這些目標的當前日誌級別。選擇所需的日誌記錄目標並按一下Edit。在本例中，「Syslog Servers」目標被修改。



8. 從Filter on severity下拉選單中選擇適當的嚴重性(在本例中為Informational)。完成後按一下OK。



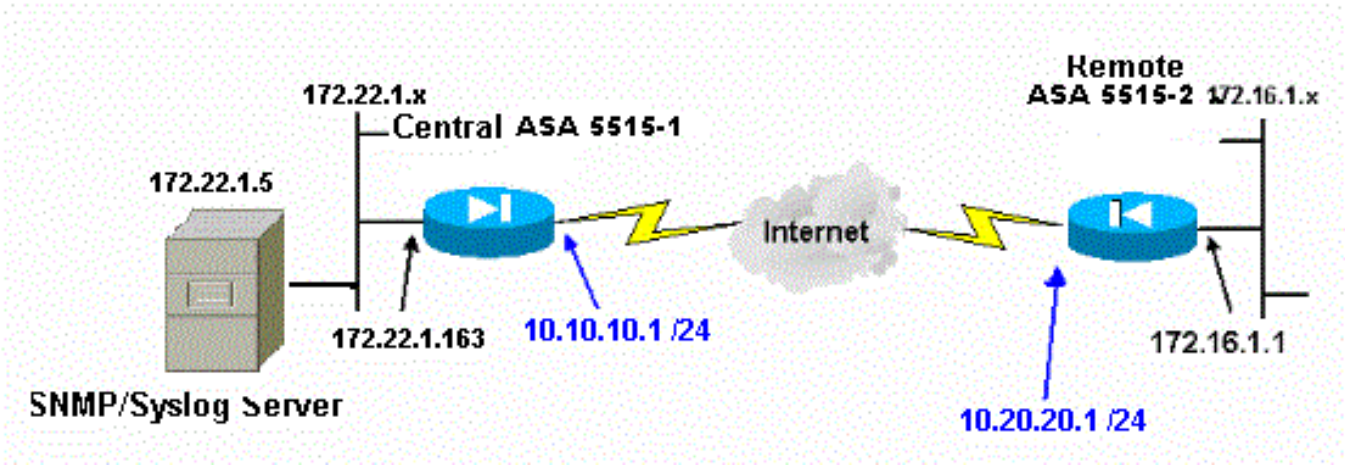
9. 返回Logging Filters窗口後，按一下Apply。



透過VPN將系統日誌消息傳送到系統日誌伺服器

在簡單的站點到站點VPN設計或更加複雜的集中星型設計中，管理員可能希望使用SNMP伺服器和位於中心站點的syslog伺服器監控所有遠端ASA防火牆。

要配置站點到站點IPsec VPN配置，請參閱PIX/ASA 7.x及更高版本： PIX到PIX VPN隧道配置示例。除了VPN配置之外，您還需要為中央站點和本地站點中的syslog伺服器配置SNMP和相關流量。



中央ASA配置

<#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 *****
```

遠端ASA配置

<#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 *****
```

有關如何配置ASA版本8.4的詳細資訊，請參閱使用SNMP和Syslog透過VPN隧道監控Cisco Secure ASA防火牆

高級系統日誌

ASA版本8.4提供多種機制，使您能夠在組中配置和管理系統日誌消息。這些機制包括消息嚴重性級別、消息類別、消息ID或您建立的自定義消息清單。使用這些機制，您可以輸入適用於小型或大型消息組的單個命令。透過這種方式設定syslog時，您可以捕獲來自指定消息組的消息，而不再捕獲來自同一嚴重性的所有消息。

使用訊息清單

使用消息清單可以按嚴重性級別和ID僅將相關的系統日誌消息包括到組中，然後將此消息清單與所需目標相關聯。

完成以下步驟以配置消息清單：

1. 輸入logging list message_list | level severity_level [class message_class]命令以建立包括具有指定嚴重性級別或消息清單的消息的消息清單。
2. 輸入logging list message_list message syslog_id-syslog_id2命令以向剛建立的消息清單中增加另外的消息。
3. 輸入logging destination message_list命令以指定建立的消息清單的目標。

範例 2

輸入以下命令可建立消息清單，其中包括所有嚴重性為2（嚴重）的消息，並增加了611101 to 611323的消息，同時還可將這些消息傳送到控制檯：

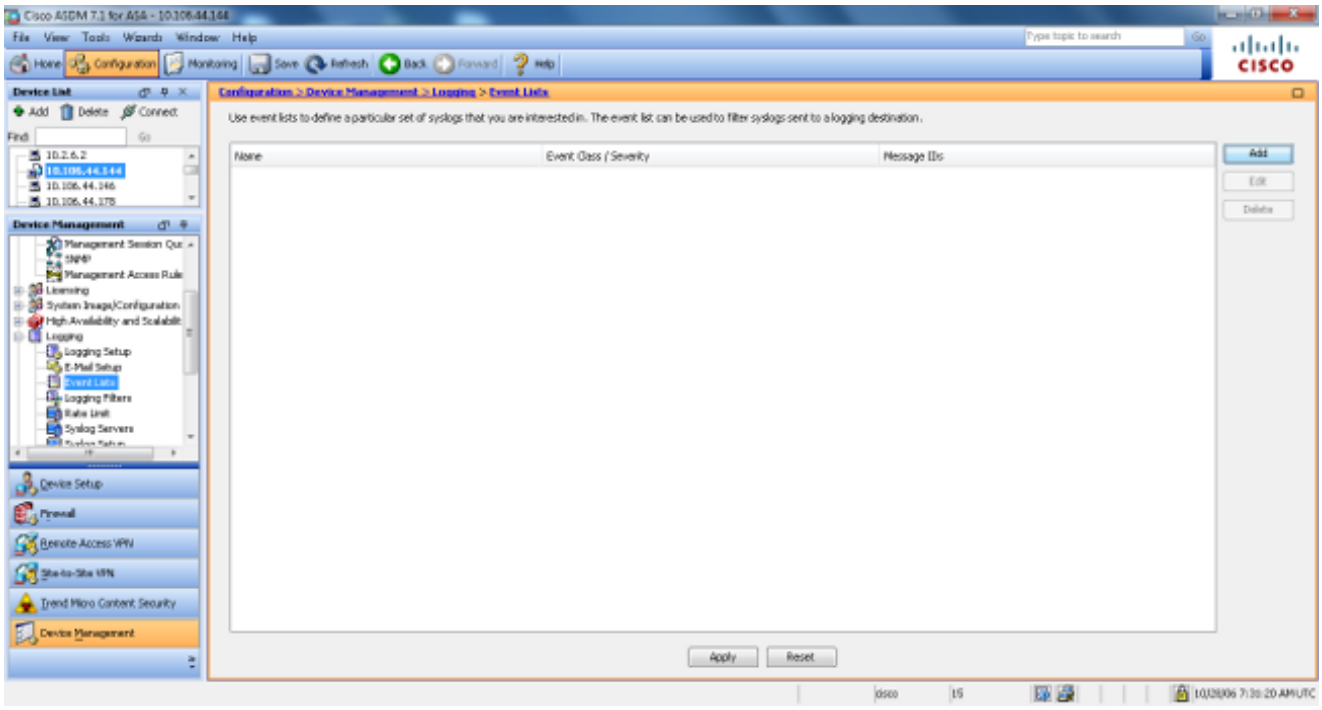
<#root>

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

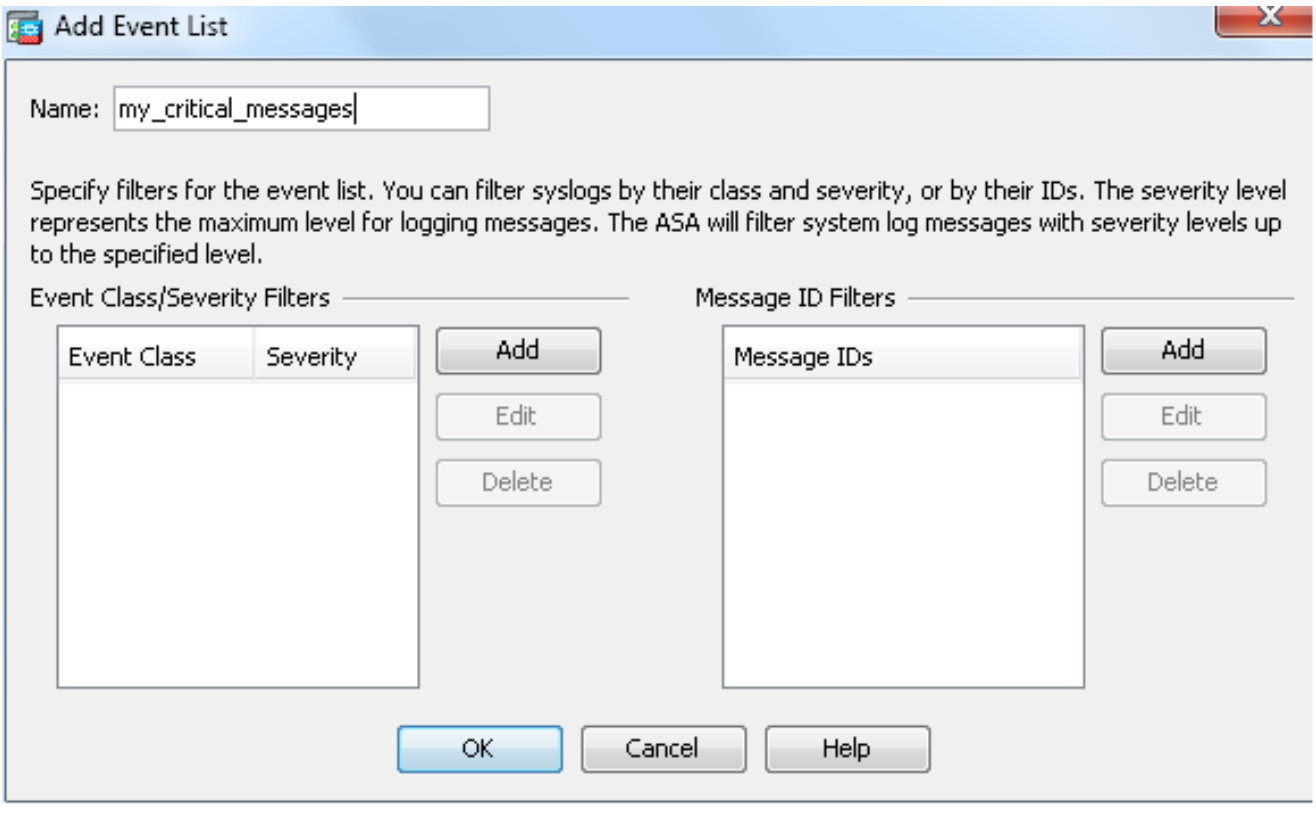
ASDM配置

此過程顯示使用消息清單的示例2的ASDM配置。

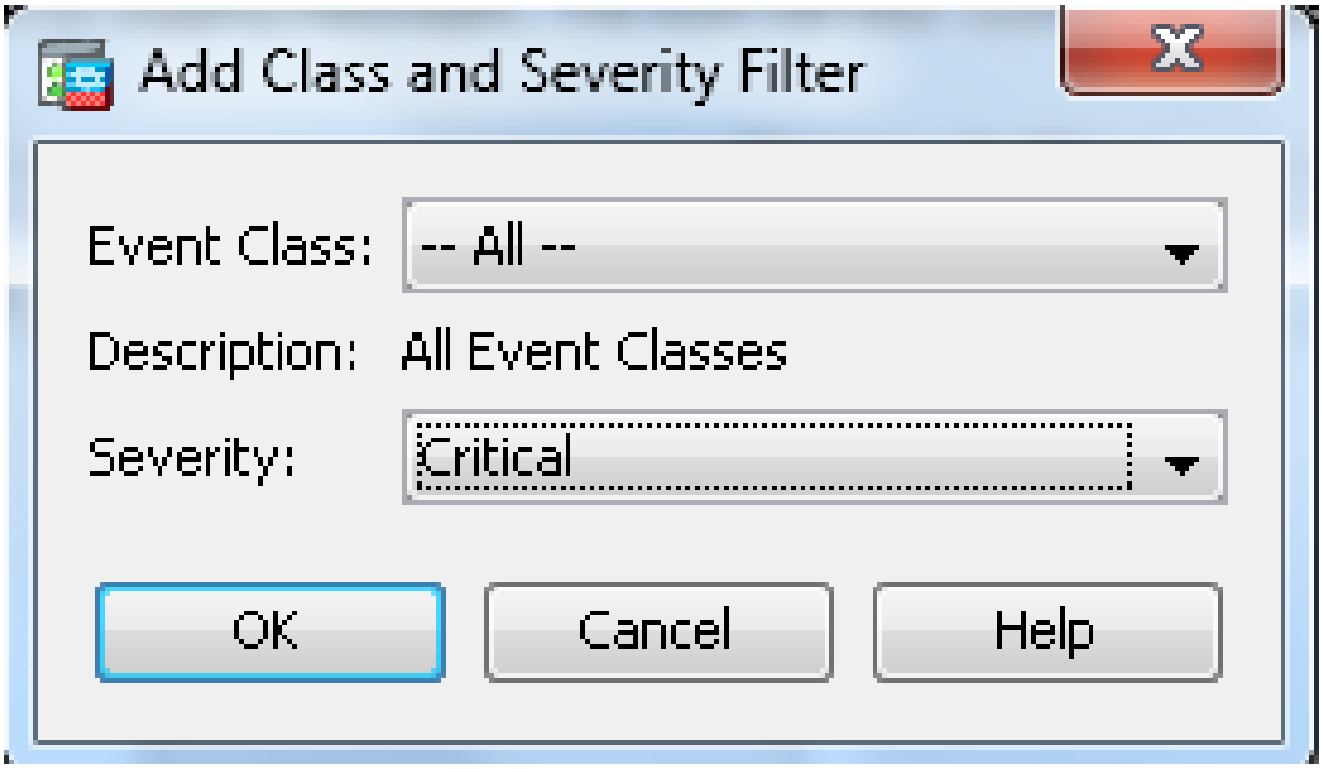
1. 選擇Logging下的Event Lists，並按一下Add以建立消息清單。



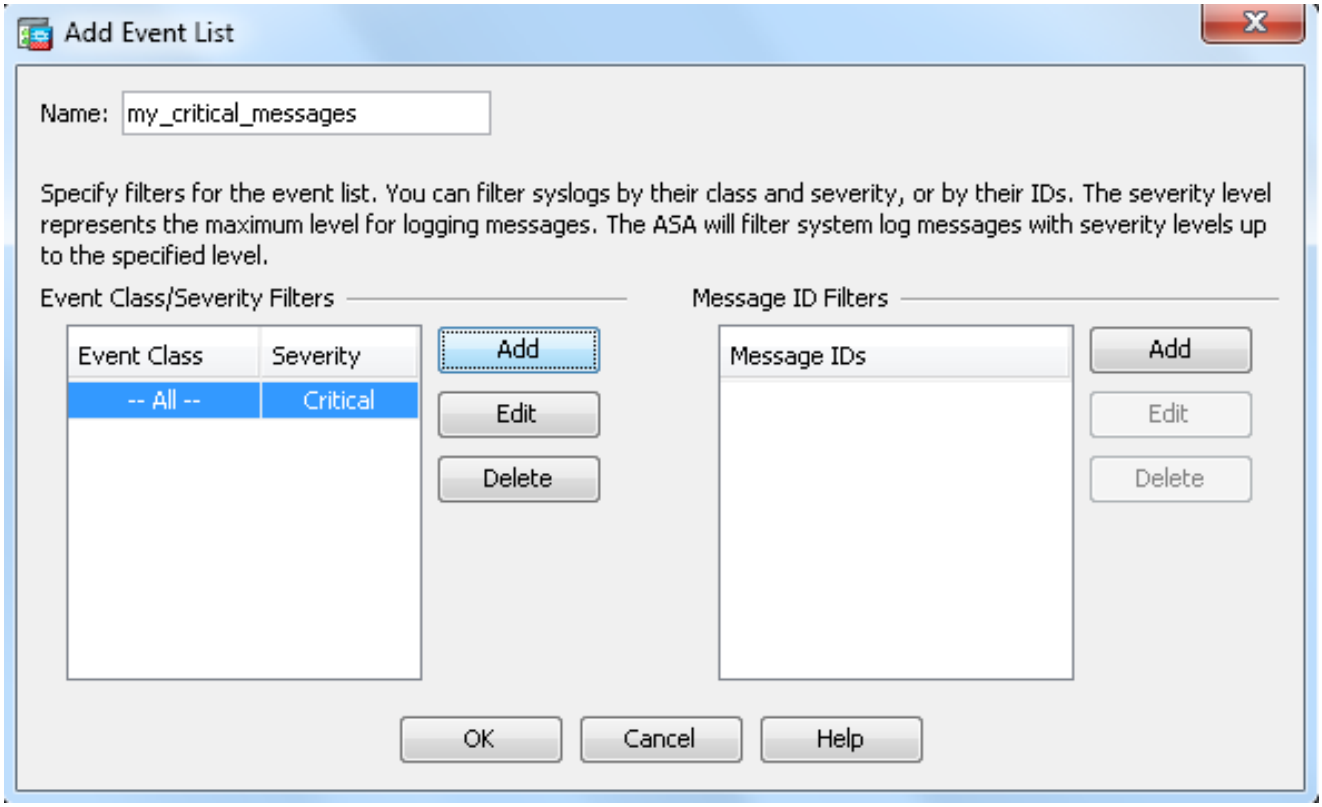
2. 在「名稱」方塊中輸入訊息清單的名稱。在本例中，使用my_critical_messages。按一下Event Class/Severity Filters下的Add。



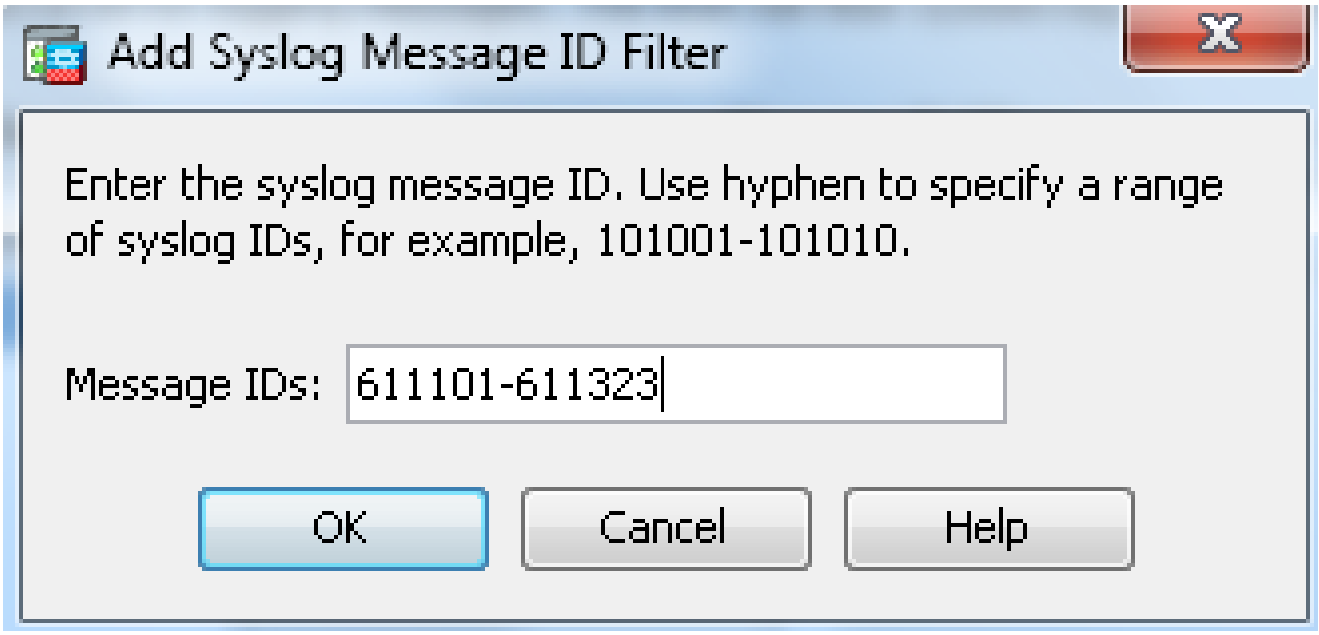
3. 從Event Class下拉選單中選擇All。從Severity下拉選單中選擇Critical。完成後按一下OK。



4. 如果需要另外的消息，請按一下Message ID Filters下的Add。這種情況下，您需要輸入ID為611101-611323的消息。

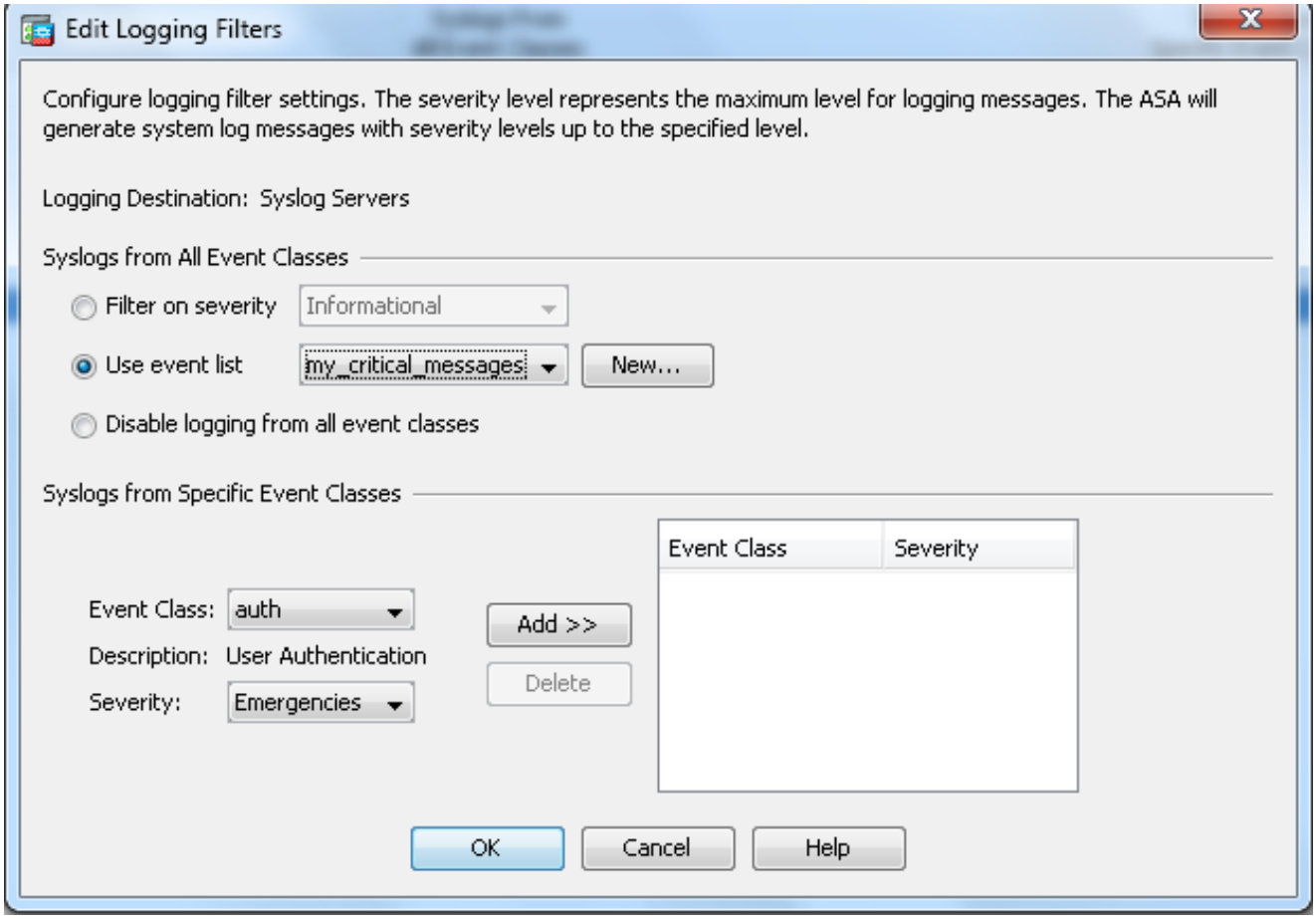


5. 在Message IDs框中輸入ID範圍並按一下OK。

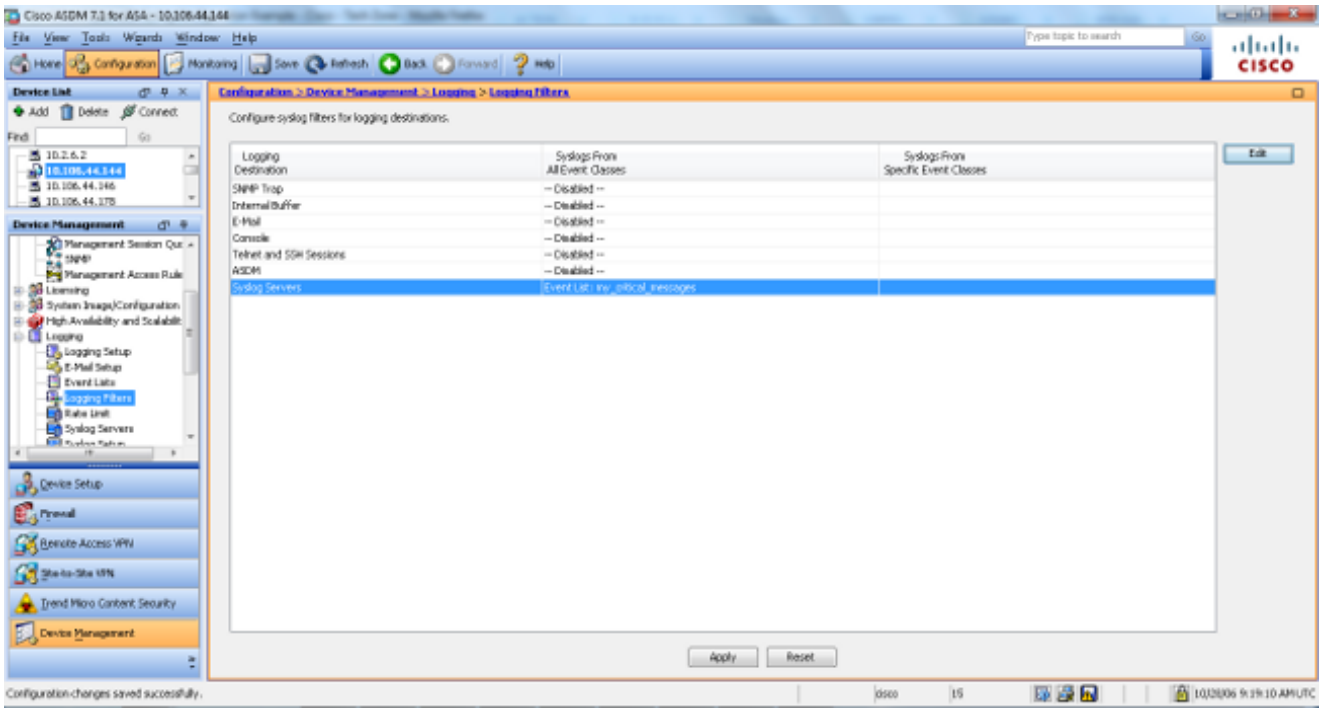


6. 返回Logging Filters 選單並選擇Console作為目標。

7. 從Use event list下拉選單中選擇my_critical_messages。完成後按一下OK。



8. 返回Logging Filters窗口後，按一下Apply。



這將完成使用消息清單的ASDM配置，如示例2所示。

使用訊息類別

使用message類將與該類關聯的所有消息傳送到指定的輸出位置。指定嚴重性級別閾值時，可以限制傳送到輸出位置的消息數。

<#root>

logging class

 message_class destination | severity_level

範例 3

輸入以下命令將嚴重性級別為緊急或更高的所有類別類別消息傳送到控制檯。

<#root>

logging class ca console emergencies

ASDM配置

此過程顯示使用消息清單的示例3的ASDM配置。

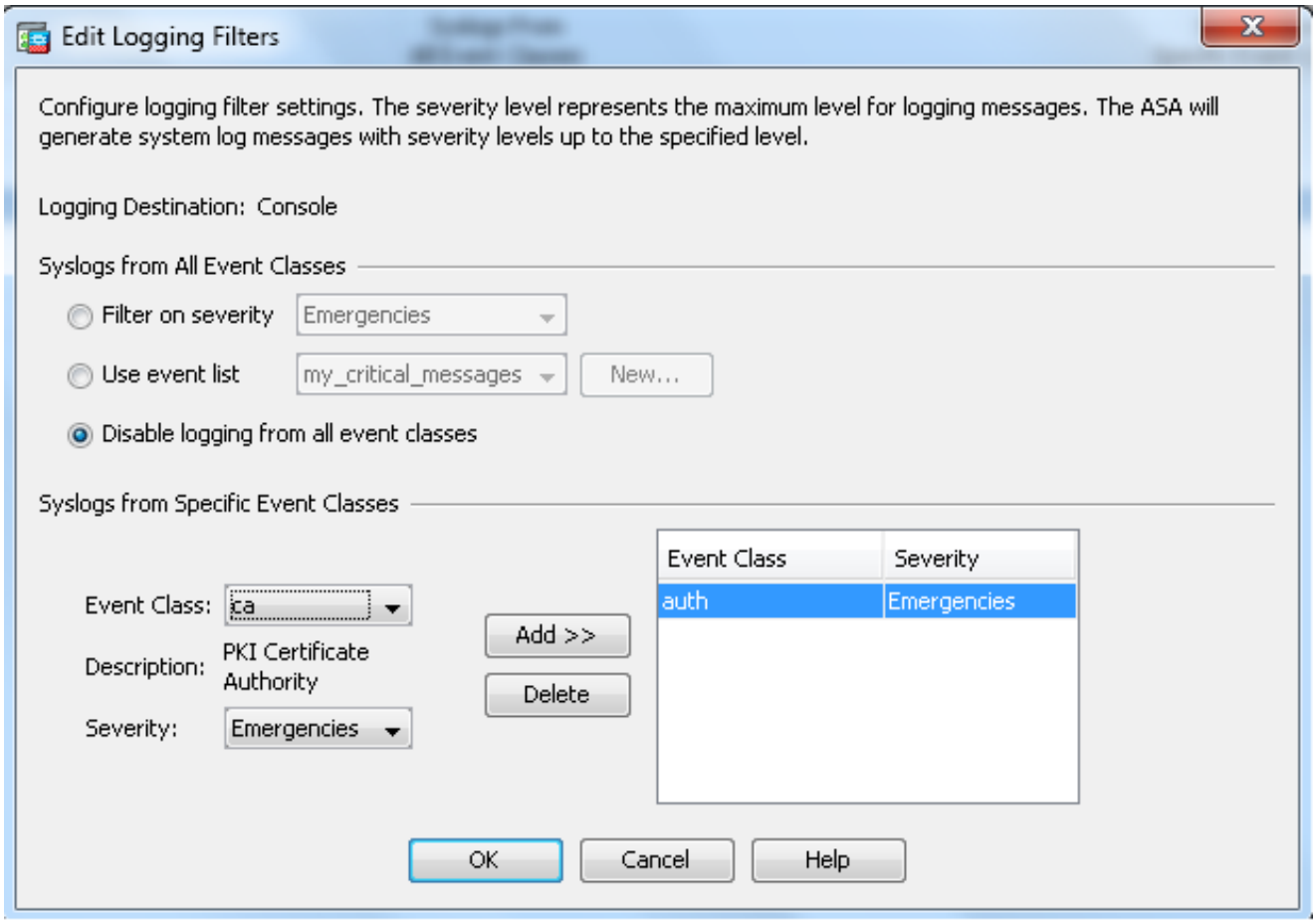
1. 選擇Logging Filters 選單並選擇Console作為目標。

2. 按一下Disable logging from all event classes。

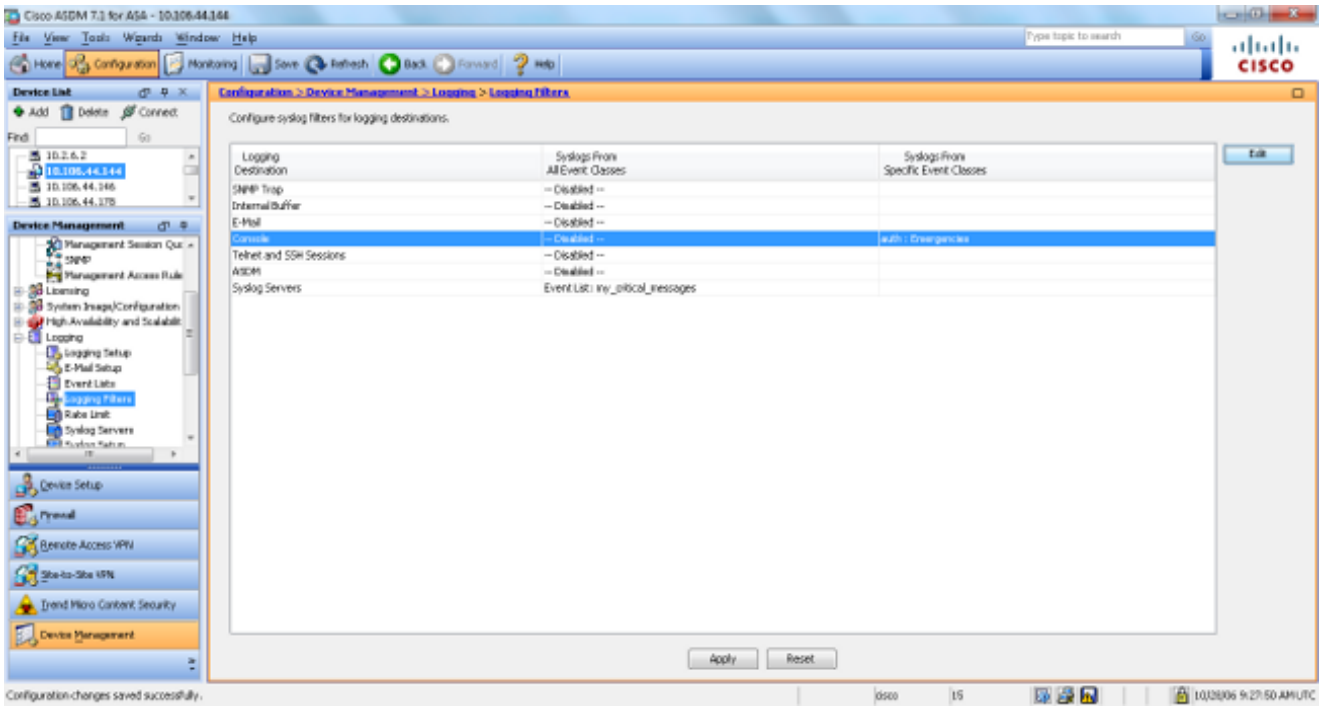
3. 在Syslog from Specific Event Classes下，選擇要增加的事件類和嚴重性。

   此過程分別使用ca和Emergencies。

4. 按一下Add以將此增加到消息類中並按一下OK。



5. 返回Logging Filters窗口後，按一下Apply。現在，控制檯將收集嚴重性級別為「Emergencies」的ca類消息，如Logging Filters窗口中所示。



這將完成示例3的ASDM配置。有關日誌消息嚴重性級別的清單，請參閱按嚴重性級別列出的消息。

將調試日誌消息傳送到系統日誌伺服器

對於高級故障排除，需要特定功能/協定的調試日誌。預設情況下，這些日誌消息顯示在終端(SSH/Telnet)上。根據調試型別和生成調試消息的速率，如果啟用了調試，使用CLI可能會比較困難。或者，調試消息可以重定向到syslog進程並生成為syslog。這些系統日誌可以像任何其他系統日誌一樣傳送到任何系統日誌目的地。要將調試轉移到syslog，請輸入logging debug-trace命令。此配置以syslogs形式將調試輸出傳送到系統日誌伺服器。

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

同時使用記錄清單和訊息類別

輸入logging list命令以僅捕獲LAN到LAN和遠端訪問IPsec VPN消息的Syslog。此示例捕獲調試級別或更高級別的所有VPN （IKE和IPsec）類系統日誌消息。

範例

```
<#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
```

記錄ACL命中

向您需要的每個訪問清單元素(ACE)增加log，以便在命中訪問清單時記錄。使用以下語法：

<#root>

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

範例

<#root>

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

預設情況下，ACL會記錄每個被拒絕的資料包。無需為deny ACL增加日誌選項即可為拒絕的資料包生成系統日誌。當指定log選項時，它將為其應用的ACE生成Syslog消息106100。將為透過ASA防火牆的每個匹配的允許或拒絕ACE流生成Syslog消息106100。第一個匹配流被快取。後續匹配會增加show access-list命令中顯示的命中計數。預設訪問清單日誌記錄行為(未指定log關鍵字)是：如果資料包被拒絕，則生成消息106023，如果資料包被允許，則不生成任何syslog消息。

可以為生成的系統日誌消息(106100)指定可選的系統日誌級別(0 – 7)。如果未指定級別，則新ACE的預設級別為6（資訊性）。如果ACE已存在，則其當前日誌級別保持不變。如果指定log disable選項，則將完全停用訪問清單日誌記錄。不生成任何Syslog消息，包括消息106023。log default選項將還原預設訪問清單日誌記錄行為。

完成以下步驟以便使Syslog消息106100能夠在控制檯輸出中檢視：

1. 輸入logging enable命令以允許將系統日誌消息傳輸到所有輸出位置。您必須設定日誌記錄輸出位置才能檢視任何日誌。

2. 輸入logging message <message_number> level <severity_level>命令以設定特定系統日誌消息的嚴重性級別。

   在這種情況下，輸入logging message 106100命令以啟用消息106100。

3. 輸入logging console message_list | severity_level命令以使系統日誌消息可以在發生時顯示在安全裝置控制檯(tty)上。將severity_level設定為從1到7的值或使用級別名稱。還可以使用message_list變數指定要傳送的消息。

4. 輸入show logging message 命令以顯示已從預設設定更改的系統日誌消息的清單，這些消息是已被分配不同的嚴重性級別的消息和已被停用的消息。

   以下是show logging message命令的示例輸出：

```
<#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
```

阻止在備用ASA上生成系統日誌

從ASA軟體版本9.4.1開始，您可以阻止特定系統日誌在備用裝置上生成，然後使用以下命令：

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

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

如果要抑制傳送到系統日誌伺服器的特定系統日誌消息，則必須輸入如下所示的命令。

```
<#root>

hostname(config)#

no logging message

 <syslog_id>
```

有關詳細資訊，請參閱logging message 命令。

%ASA-3-201008：禁止新連線

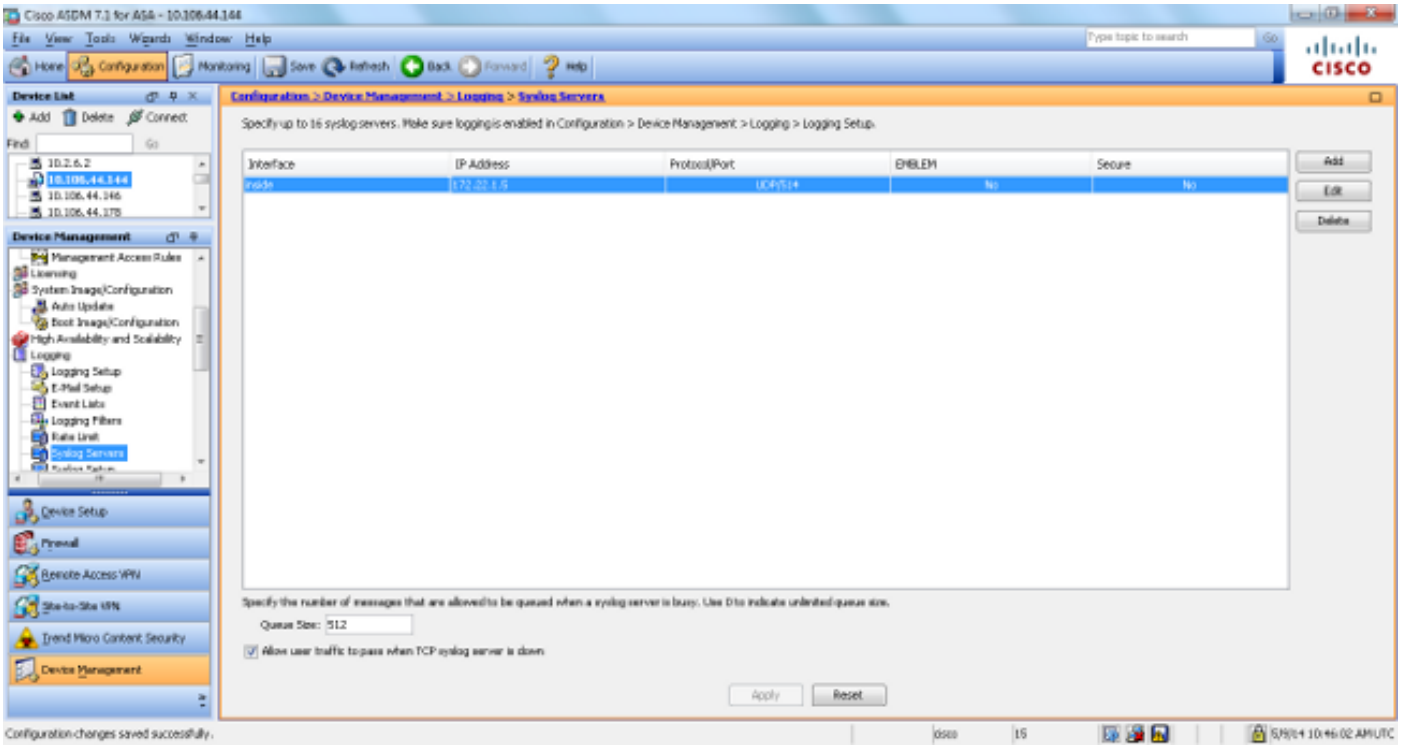
當ASA無法聯絡系統日誌伺服器並且不允許新連線時，會顯示%ASA-3-201008：禁止新連線。錯誤消息。

解決方案

當您啟用TCP系統日誌消息且無法訪問系統日誌伺服器，或者使用Cisco ASA系統日誌伺服器(PFSS)且Windows NT系統上的磁碟已滿時，會顯示此消息。完成以下步驟以解決此錯誤訊息：

- 如果已啟用TCP系統日誌消息，請將其停用。
- 如果您使用PFSS，請釋放PFSS所在的Windows NT系統上的空間。
- 確保系統日誌伺服器已啟動，並且您可以從Cisco ASA控制檯ping主機。
- 重新啟動TCP系統訊息記錄以允許流量。

如果Syslog伺服器已關閉，並且配置了TCP日誌記錄，則使用logging permit-hostdown 命令或切換到UDP日誌記錄。



相關資訊

- Cisco Secure PIX防火牆命令參考
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。