

Configuration du Syslog ASA (Adaptive Security Appliance)

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration Syslog de base](#)

[Envoyer les informations de journalisation à la mémoire tampon interne](#)

[Envoyer les informations de journalisation à un serveur Syslog](#)

[Envoyer les informations de journalisation sous forme de courriers électroniques](#)

[Envoyer les informations de journalisation à la console série](#)

[Envoyer les informations de journalisation à une session Telnet/SSH](#)

[Afficher les messages du journal sur l'ASDM](#)

[Envoi de journaux à une station de gestion SNMP](#)

[Ajout d'horodatages aux Syslogs](#)

[Exemple 1](#)

[Configuration de Syslog de base avec ASDM](#)

[Envoi de messages Syslog par un VPN à un serveur Syslog](#)

[Configuration ASA centrale](#)

[Configuration ASA à distance](#)

[Configuration Syslog avancée](#)

[Utilisation de la liste de messages](#)

[Exemple 2](#)

[Configuration ASDM](#)

[Utilisation de la catégorie de message](#)

[Exemple 3](#)

[Configuration ASDM](#)

[Envoyer les messages du journal de débogage à un serveur Syslog](#)

[Utilisation conjointe de la liste de journalisation et des classes de message](#)

[Journaliser les occurrences ACL](#)

[Blocage de la génération Syslog sur un ASA de secours](#)

[Vérifier](#)

[Dépannage](#)

[%ASA-3-201008 : Interdiction de nouvelles connexions](#)

[Solution](#)

[Informations connexes](#)

Introduction

Ce document décrit un exemple de configuration qui montre comment configurer différentes options de journalisation sur ASA qui exécute le code version 8.4 ou ultérieure.

Informations générales

La version 8.4 d'ASA a introduit des techniques de filtrage très granulaires afin de ne permettre que la présentation de certains messages Syslog spécifiés. La section Configuration Syslog de base de ce document explique une configuration Syslog traditionnelle. La section Advanced Syslog de ce document présente les nouvelles fonctionnalités Syslog de la version 8.4. Reportez-vous aux [Guides des messages du journal système des dispositifs de sécurité Cisco](#) pour le guide complet des messages du journal système.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5515 avec logiciel ASA version 8.4
- Cisco Adaptive Security Device Manager (ASDM) version 7.1.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.



Remarque : reportez-vous à [ASA 8.2 : Configurer Syslog à l'aide d'ASDM](#) pour plus d'informations sur des détails de configuration similaires avec ASDM version 7.1 et ultérieure.

Configuration Syslog de base

Entrez ces commandes afin d'activer la journalisation, d'afficher les journaux et d'afficher les paramètres de configuration.

- logging enable - Active la transmission des messages syslog à tous les emplacements de sortie.
- no logging enable - Désactive la journalisation vers tous les emplacements de sortie.
- show logging - Répertorie le contenu de la mémoire tampon syslog ainsi que les

informations et les statistiques relatives à la configuration actuelle.

L'ASA peut envoyer des messages syslog à diverses destinations. Entrez les commandes dans ces sections afin de spécifier les emplacements où vous souhaitez que les informations Syslog soient envoyées :

Envoyer les informations de journalisation à la mémoire tampon interne

```
<#root>
```

```
logging buffered
```

```
severity_level
```

Aucun logiciel ou matériel externe n'est requis lorsque vous stockez les messages syslog dans la mémoire tampon interne ASA. Entrez la commande `show logging` afin d'afficher les messages syslog stockés. La taille maximale de la mémoire tampon interne est de 1 Mo (configurable avec la commande `logging buffer-size`). Par conséquent, il peut s'emballer très rapidement. Gardez cela à l'esprit lorsque vous choisissez un niveau de journalisation pour la mémoire tampon interne, car des niveaux de journalisation plus détaillés peuvent rapidement remplir et envelopper la mémoire tampon interne.

Envoyer les informations de journalisation à un serveur Syslog

```
<#root>
```

```
logging host
```

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


```
logging trap
```

```
severity_level
```

```
logging facility
```

```
number
```

Un serveur qui exécute une application Syslog est requis afin d'envoyer des messages Syslog à un hôte externe. ASA envoie le syslog sur le port UDP 514 par défaut, mais le protocole et le port peuvent être choisis. Si le protocole TCP est choisi comme protocole de journalisation, l'ASA envoie les syslogs via une connexion TCP au serveur syslog. Si le serveur est inaccessible, ou si la connexion TCP au serveur ne peut pas être établie, l'ASA, par défaut, bloque TOUTES les nouvelles connexions. Ce comportement peut être désactivé si vous activez `logging permit-hostdown`. Consultez le guide de configuration pour plus d'informations sur la commande `logging permit-hostdown`.

 Remarque : l'ASA autorise uniquement les ports compris entre 1025 et 65535. L'utilisation de tout autre port entraîne cette erreur :

```
ciscoasa(config)# logging host tftp 192.168.1.1 udp/516
```

AVERTISSEMENT : le niveau de sécurité de l'interface Ethernet0/1 est 0.
ERREUR : Le port « 516 » n'est pas compris entre 1025 et 65535.

Envoyer les informations de journalisation sous forme de courriers électroniques

```
<#root>

logging mail

  severity_level

logging recipient-address

  email_address

logging from-address

  email_address

smtp-server

  ip_address
```

Un serveur SMTP est requis quand vous envoyez les messages Syslog dans les messages électroniques. Une configuration correcte sur le serveur SMTP est nécessaire afin de vous assurer que vous pouvez relayer correctement les courriers électroniques de l'ASA vers le client de messagerie spécifié. Si ce niveau de journalisation est défini sur un niveau très détaillé, tel que debug ou informational, vous pouvez générer un nombre significatif de syslogs puisque chaque e-mail envoyé par cette configuration de journalisation entraîne la génération de quatre journaux supplémentaires ou plus.

Envoyer les informations de journalisation à la console série

```
<#root>

logging console

  severity_level
```

La journalisation de la console permet aux messages syslog de s'afficher sur la console ASA (tty) au fur et à mesure qu'ils se produisent. Si la journalisation de la console est configurée, toute la génération de journaux sur l'ASA est limitée à un débit de 9 800 bits/s, soit la vitesse de la console série ASA. Cela peut entraîner l'abandon des syslogs vers toutes les destinations, y compris la mémoire tampon interne. Pour cette raison, n'utilisez pas la journalisation de console pour les syslogs explicites.

Envoyer les informations de journalisation à une session Telnet/SSH

```
<#root>  
logging monitor  
    severity_level  
terminal monitor
```

Logging monitor permet aux messages syslog de s'afficher tels qu'ils se produisent lorsque vous accédez à la console ASA avec Telnet ou SSH et que la commande terminal monitor est exécutée à partir de cette session. Afin d'arrêter l'impression des journaux à votre session, entrez la commande terminal no monitor.

Afficher les messages du journal sur l'ASDM

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

ASDM a également une mémoire tampon qui peut être utilisée pour enregistrer les messages Syslog. Entrez la commande show logging asdm afin d'afficher le contenu de la mémoire tampon syslog ASDM.

Envoi de journaux à une station de gestion SNMP

```
<#root>  
logging history  
    severity_level  
snmp-server host  
    [if_name] ip_addr  
snmp-server location  
    text  
snmp-server contact  
    text  
snmp-server community  
    key  
snmp-server enable traps
```

Les utilisateurs ont besoin d'un environnement SNMP (Simple Network Management Protocol) fonctionnel pour envoyer des messages syslog avec SNMP. Reportez-vous à la section [Commandes de définition et de gestion des destinations de sortie](#) pour une référence complète sur les commandes que vous pouvez utiliser pour définir et gérer les destinations de sortie. Consultez la section [Messages listés par niveau de gravité](#) pour les messages listés par niveau de gravité.

Ajout d'horodatages aux Syslogs

Afin de faciliter l'alignement et l'ordre des événements, des horodatages peuvent être ajoutés aux syslogs. Ceci est recommandé afin d'aider à tracer les problèmes en fonction du temps. Afin d'activer les horodatages, entrez la commande logging timestamp. Voici deux exemples Syslog, l'un sans l'horodatage et l'autre avec :

```
%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
```

Exemple 1

Ce résultat montre un exemple de configuration pour la connexion à la mémoire tampon avec le niveau de gravité du débogage.

```
<#root>
```

```
logging enable  
logging buffered debugging
```

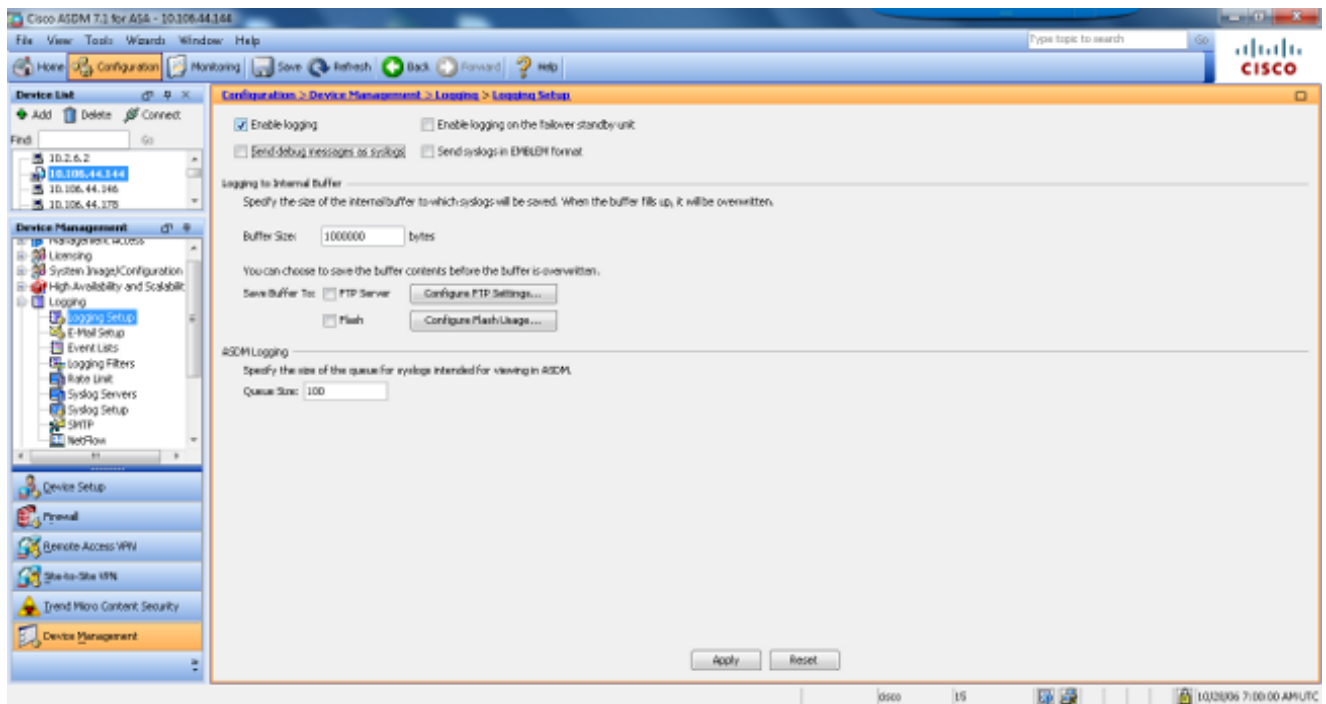
Voici un exemple de sortie.

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

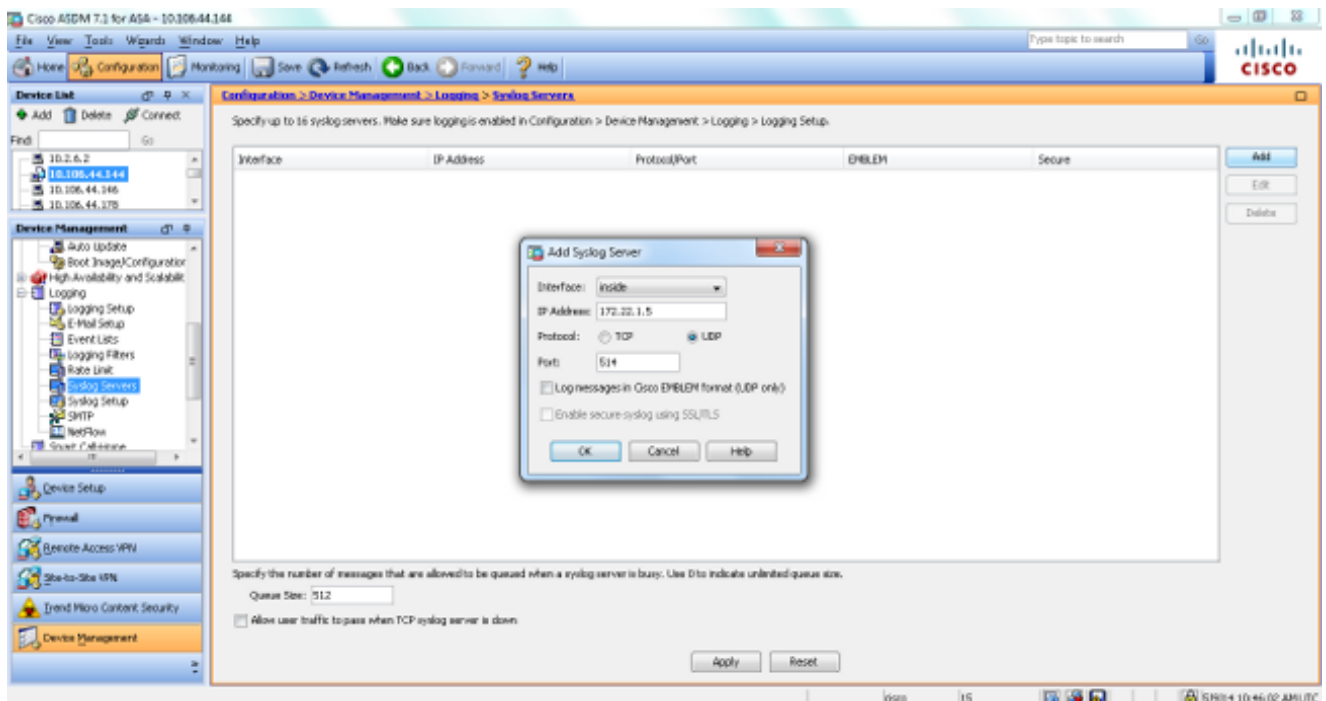
Configuration de Syslog de base avec ASDM

Cette procédure illustre la configuration ASDM pour toutes les destinations syslog disponibles.

1. Afin d'activer la journalisation sur l'ASA, configurez d'abord les paramètres de journalisation de base. Choisissez Configuration > Features > Properties > Logging > Logging Setup. Cochez la case Enable logging afin d'activer syslogs.

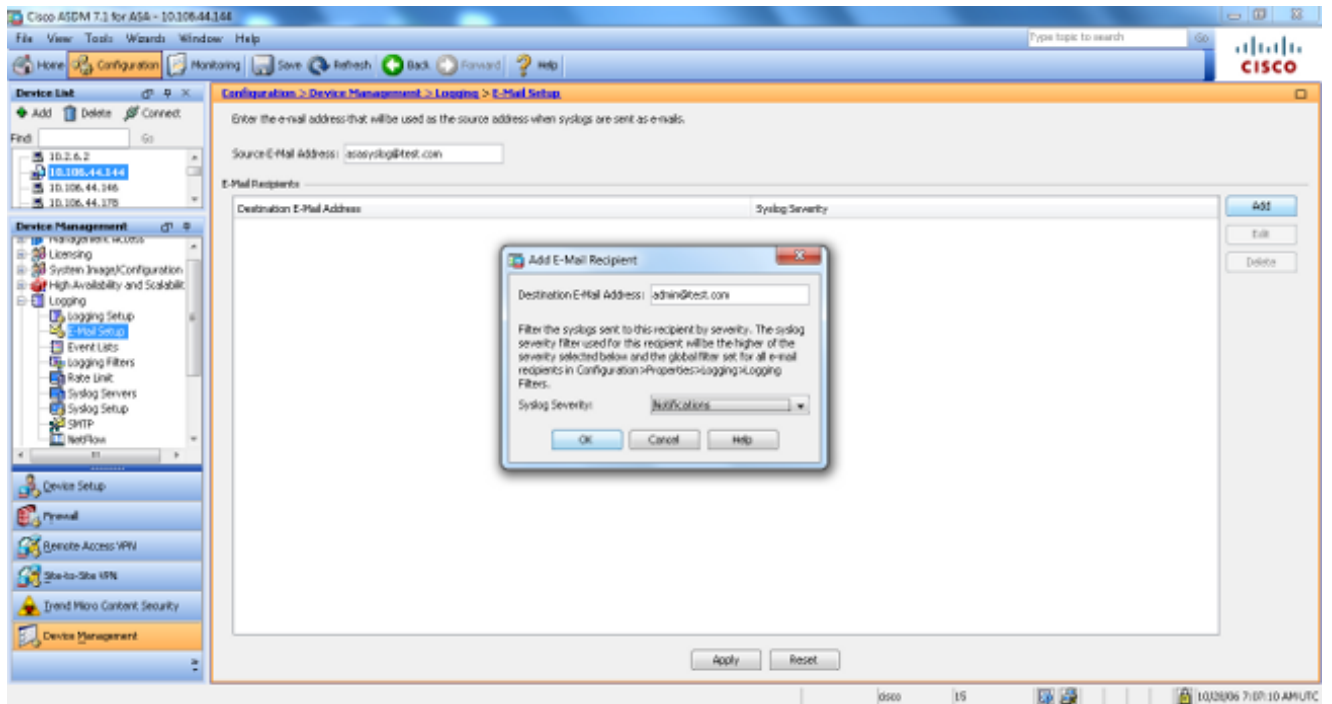


2. Afin de configurer un serveur externe comme destination pour syslog, choisissez Syslog Servers dans Logging et cliquez sur Add afin d'ajouter un serveur syslog. Saisissez les détails du serveur syslog dans la zone Add Syslog Server (Ajouter un serveur Syslog) et choisissez OK lorsque vous avez terminé.

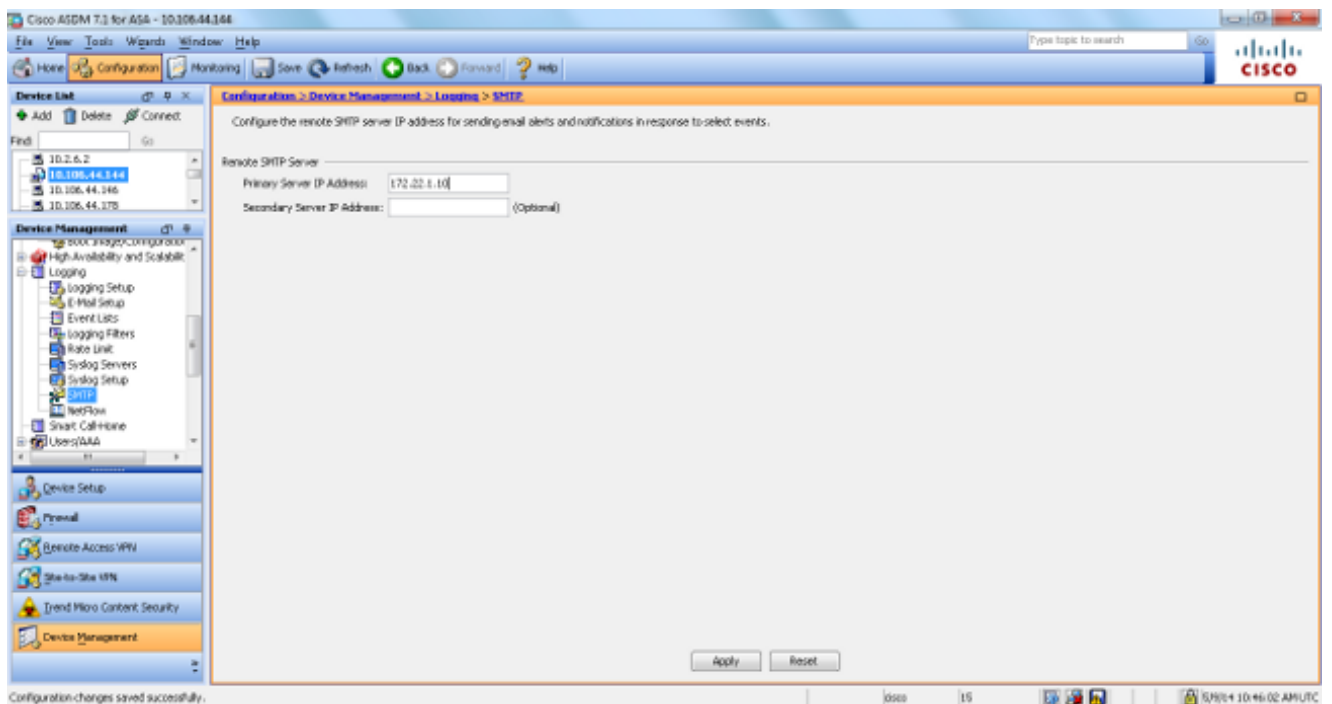


3. Choisissez E-Mail Setup in Logging afin d'envoyer des messages syslog comme des courriels à des destinataires spécifiques. Précisez l'adresse électronique source dans la zone de l'adresse électronique source et choisissez Add afin de configurer l'adresse

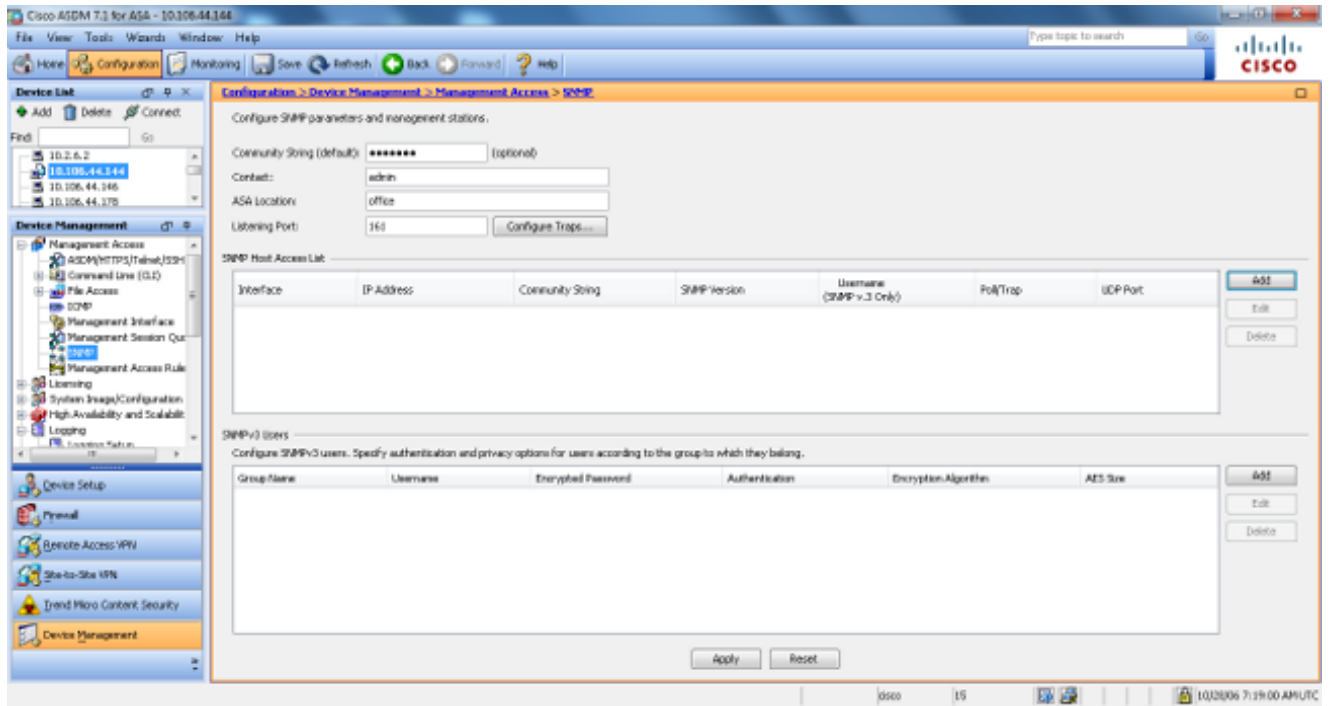
électronique de destination des destinataires des messages électroniques et le niveau de gravité du message. Cliquez sur OK lorsque vous avez terminé.



4. Choisissez Device Administration, Logging, choisissez SMTP, et entrez l'adresse IP du serveur principal afin de spécifier l'adresse IP du serveur SMTP.



5. Si vous souhaitez envoyer des syslogs en tant que dérouterments SNMP, vous devez d'abord définir un serveur SNMP. Choisissez SNMP dans le menu Management Access afin de spécifier l'adresse des stations de gestion SNMP et leurs propriétés spécifiques.



6. Choisissez Add afin d'ajouter une station de gestion SNMP. Saisissez les détails de l'hôte SNMP et cliquez sur OK.

Add SNMP Host Access Entry

Interface Name: inside

IP Address: 172.22.1.5

UDP Port: 162

Community String: ●●●●

SNMP Version: 2c

Server Poll/Trap Specification

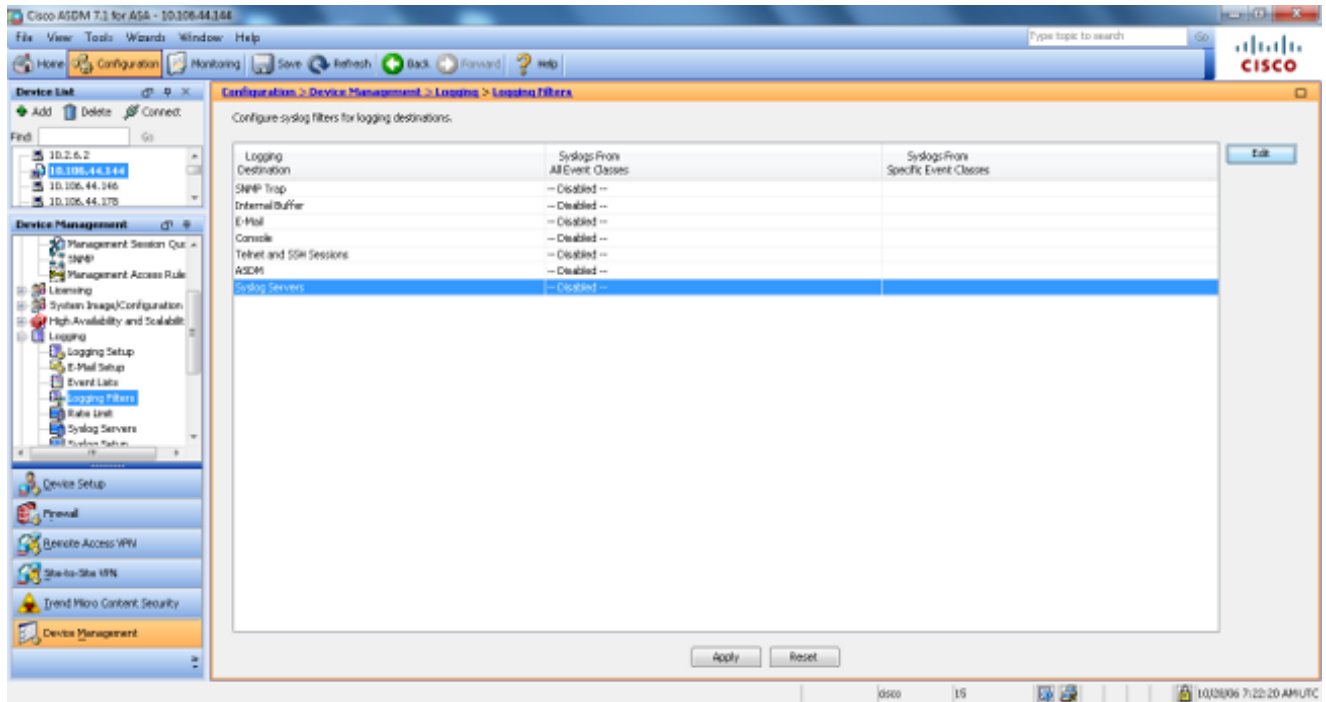
Select a specified function of the SNMP Host.

Poll

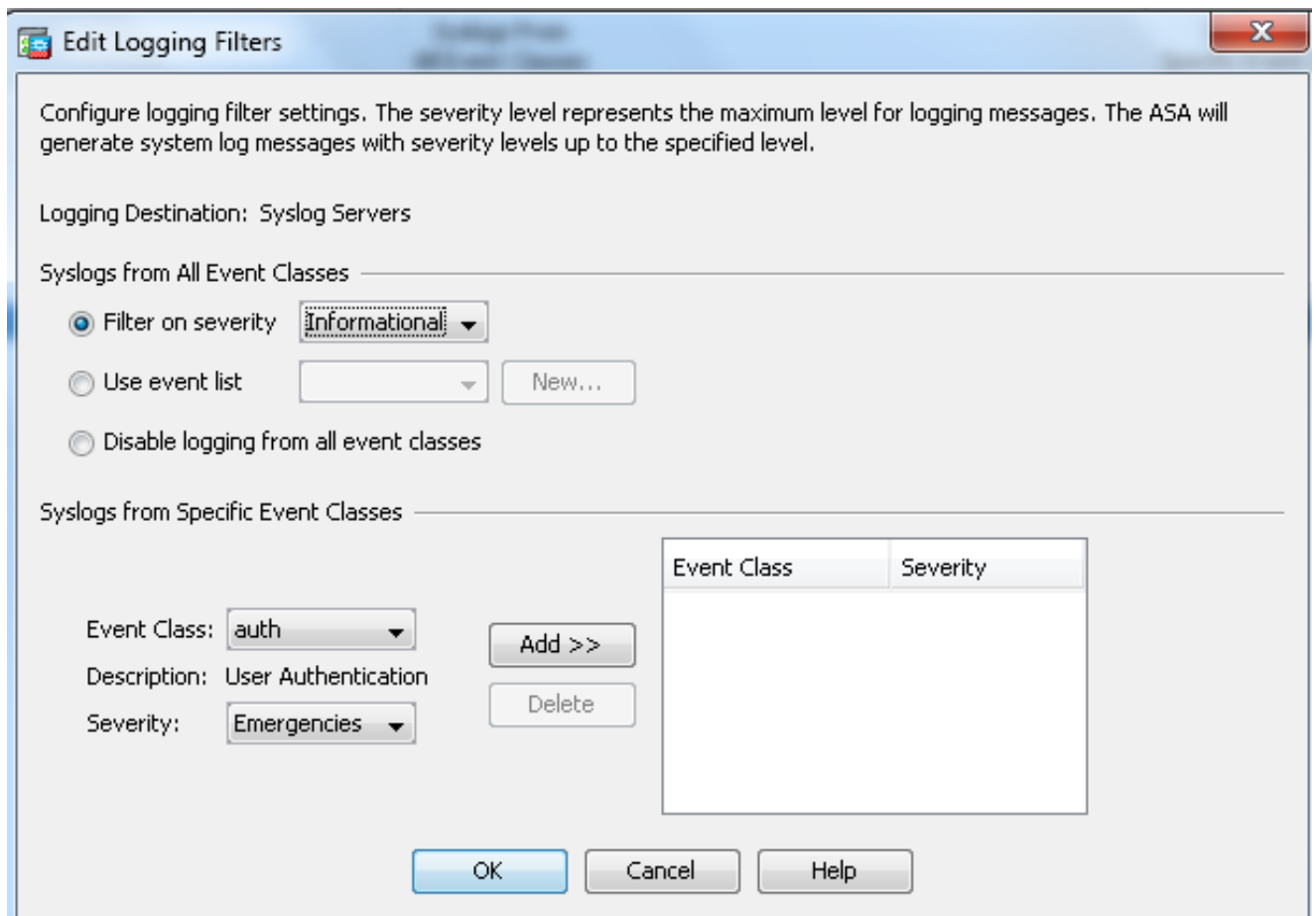
Trap

OK Cancel Help

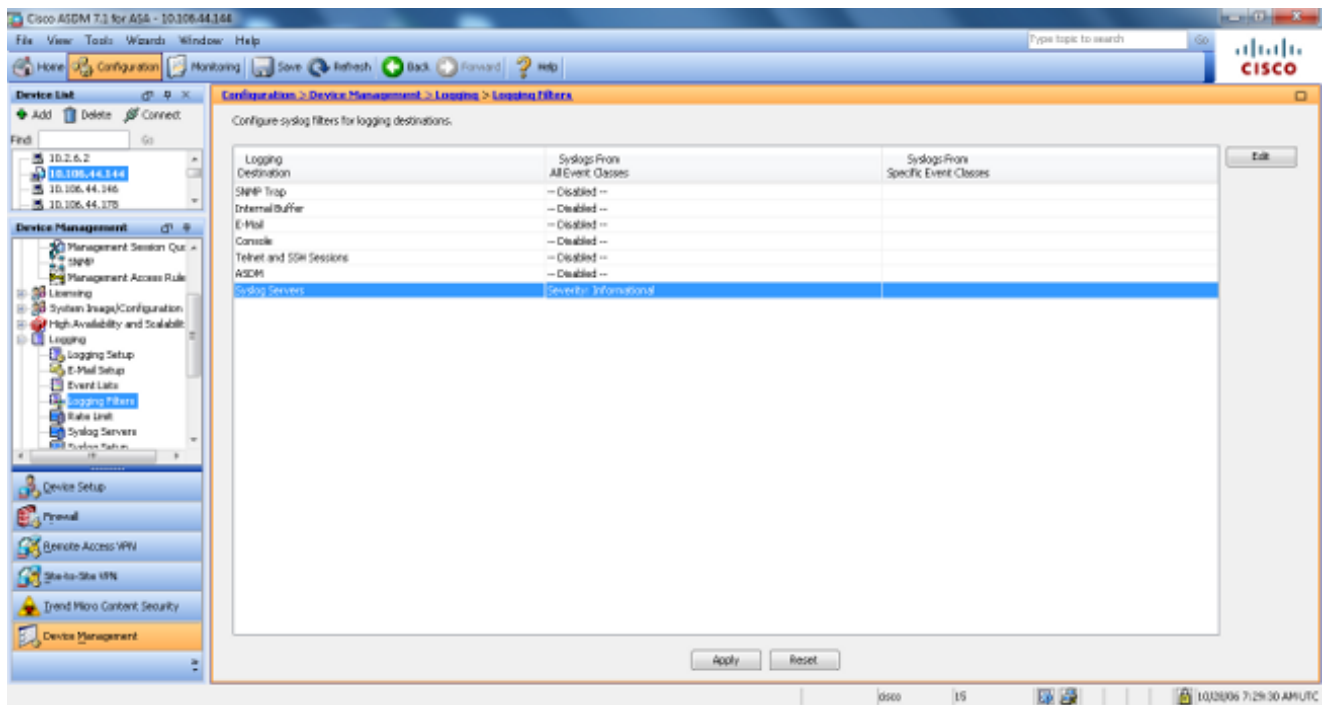
7. Afin d'activer l'envoi des journaux à l'une des destinations mentionnées précédemment, choisissez Logging Filters dans la section logging. Vous disposez ainsi de chaque destination de journalisation possible et du niveau actuel des journaux envoyés à ces destinations. Choisissez la destination de journalisation souhaitée et cliquez sur Edit. Dans cet exemple, la destination « Serveurs Syslog » est modifiée.



8. Choisissez un niveau de gravité approprié, dans ce cas, Informationnel, dans la liste déroulante Filtrer selon le niveau de gravité. Cliquez sur OK lorsque vous avez terminé.



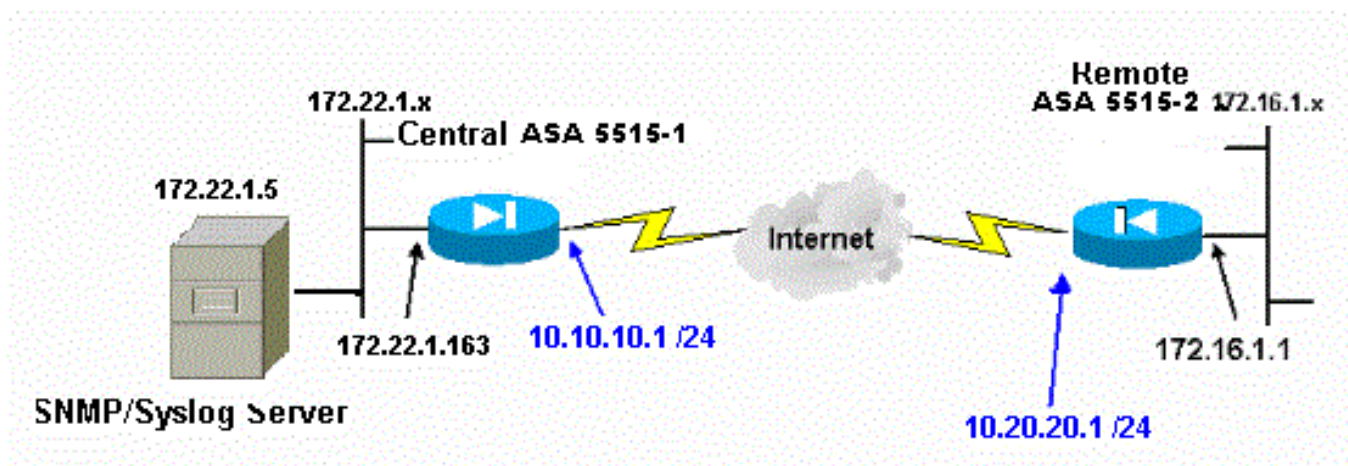
9. Cliquez sur Apply après être revenu à la fenêtre des filtres de journalisation.



Envoi de messages Syslog par un VPN à un serveur Syslog

Dans la conception VPN site à site simple ou dans la conception Hub and Spoke plus compliquée, l'administrateur peut vouloir surveiller tous les pare-feu ASA distants avec le serveur SNMP et le serveur Syslog situés sur un site central.

Afin de configurer la configuration VPN IPsec de site à site, référez-vous à [PIX/ASA 7.x et au-dessus : Exemple de configuration de tunnel VPN PIX-à-PIX](#). Indépendamment de la configuration VPN, vous devez configurer le SNMP et le trafic intéressant pour le serveur syslog dans le site central et le site local.



Configuration ASA centrale

```
<#root>
```

```
!--- This access control list (ACL) defines IPsec interesting traffic.
```

*!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.*

```
access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

*!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.*

```
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161  
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161  
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162  
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162  
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514
```

```
logging enable  
logging trap debugging
```

!--- Define logging host information.

```
logging facility 16  
logging host inside 172.22.1.5
```

!--- Define the SNMP configuration.

```
snmp-server host inside 172.22.1.5 community ***** version 2c
```

```
snmp-server community *****
```

Configuration ASA à distance

```
<#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 *****
```

Référez-vous à [Surveillance du pare-feu Cisco Secure ASA à l'aide de SNMP et Syslog via un tunnel VPN](#) pour plus d'informations sur la façon de configurer ASA Version 8.4

Configuration Syslog avancée

ASA version 8.4 fournit plusieurs mécanismes qui vous permettent de configurer et de gérer les messages Syslog dans des groupes. Ces mécanismes incluent le niveau de gravité du message, la catégorie du message, l'ID du message ou une liste de messages personnalisée que vous créez. Avec l'utilisation de ces mécanismes, vous pouvez saisir une commande unique qui s'applique à de petits ou grands groupes de messages. Quand vous configurez Syslog de cette façon, vous pouvez capturer les messages du groupe de message spécifié, non plus tous messages de la même gravité.

Utilisation de la liste de messages

Utilisez la liste de messages afin d'inclure seulement les messages syslog intéressés par le niveau de gravité et l'ID dans un groupe, puis associez cette liste de messages à la destination souhaitée.

Réalisez ces étapes afin de configurer une liste de messages:

1. Saisissez la commande `logging list message_list | level severity_level [class message_class]` afin de créer une liste de messages qui inclut des messages avec un niveau de gravité ou une liste de messages spécifiés.
2. Saisissez la commande `logging list message_list message syslog_id-syslog_id2` afin d'ajouter des messages supplémentaires à la liste de messages que vous venez de créer.
3. Saisissez la commande `logging destination message_list` afin de préciser la destination de la liste de messages créée.

Exemple 2

Entrez ces commandes afin de créer une liste de messages, qui inclut tous les messages de gravité 2 (critiques) avec l'ajout du message 611101 à 611323, et les envoyer également à la console :

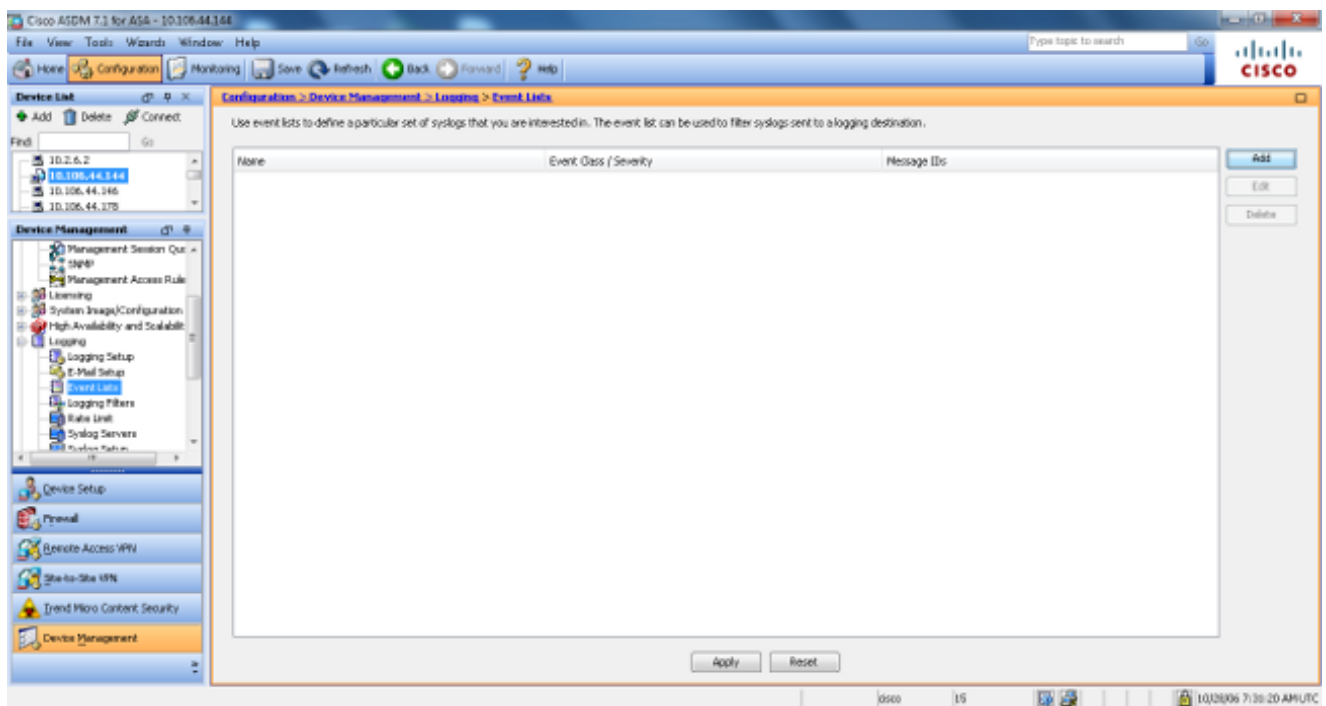
```
<#root>
```

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

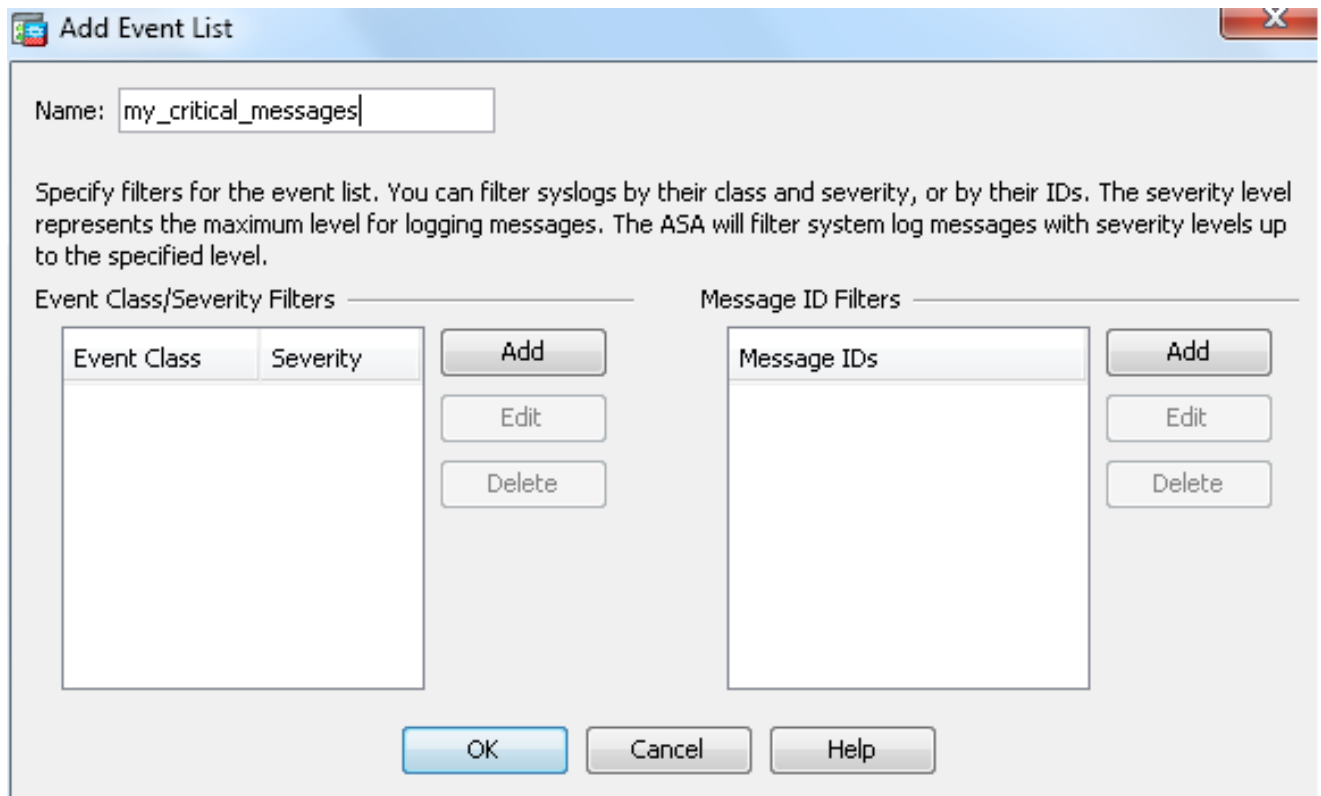
Configuration ASDM

Cette procédure montre une configuration ASDM pour l'exemple 2 avec l'utilisation de la liste de messages.

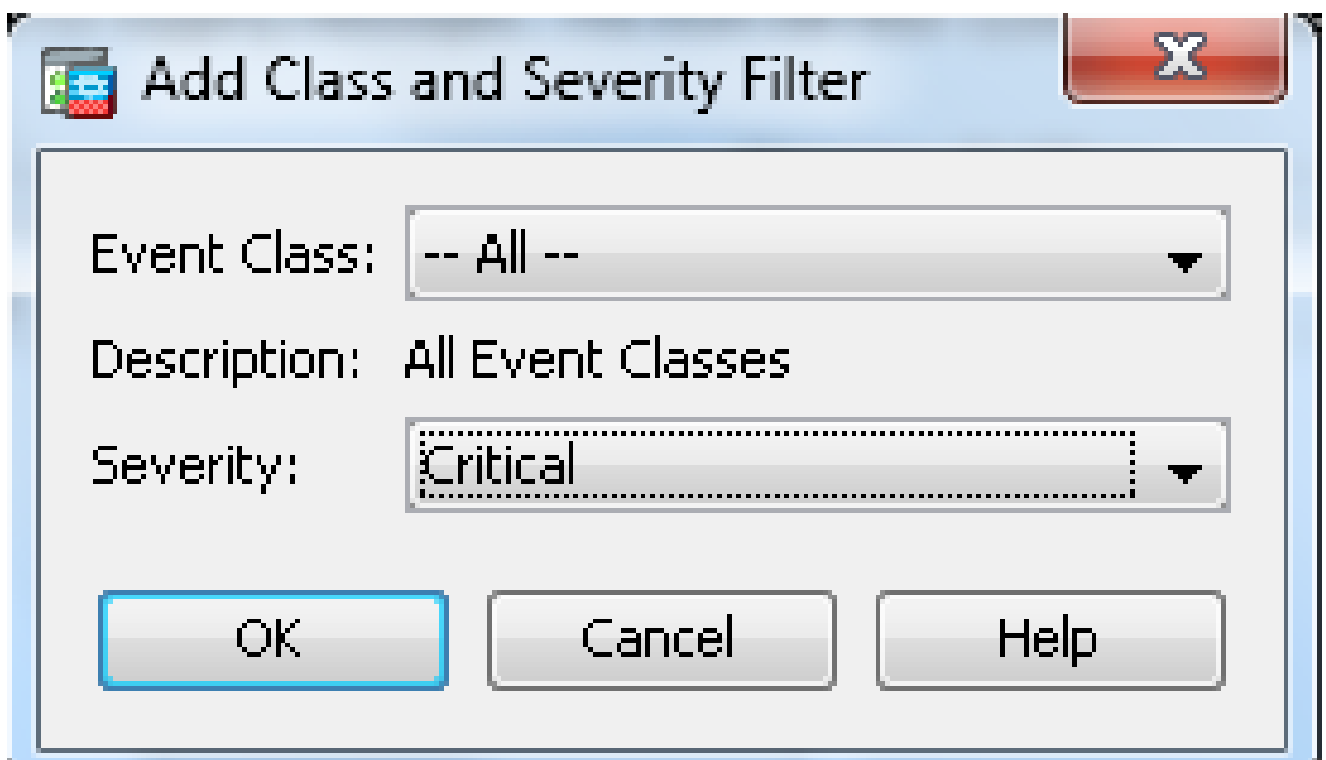
1. Choisissez Event Lists sous Logging et cliquez sur Add afin de créer une liste de messages.



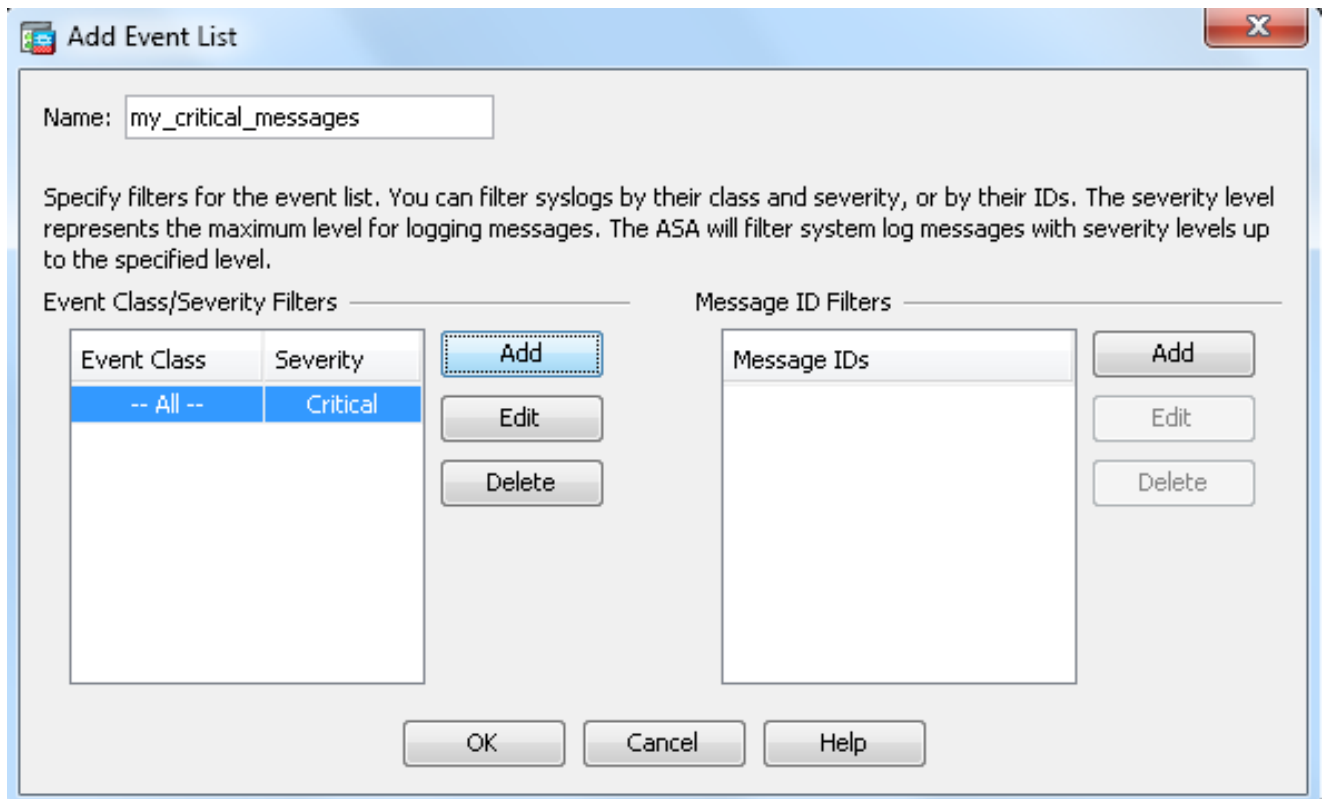
2. Saisissez le nom de la liste de messages dans la zone du nom. Dans cet exemple, my_critical_messages est utilisé. Cliquez sur Add sous Event Class/Severity Filters.



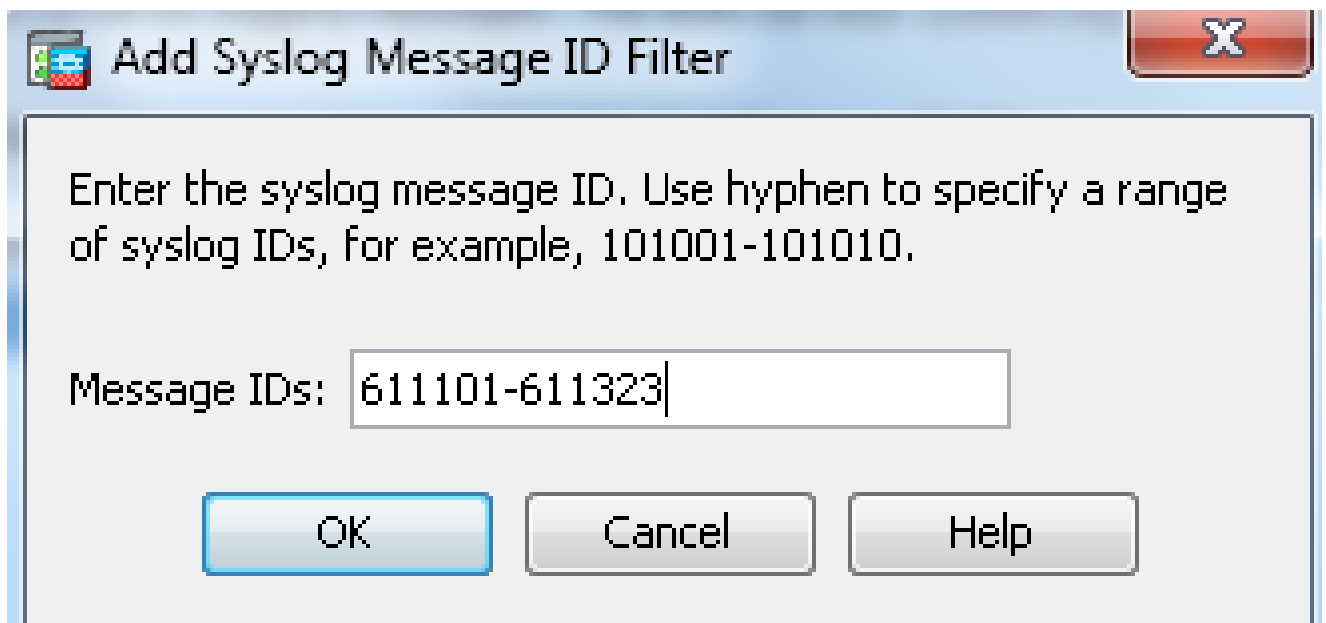
3. Choisissez All dans la liste déroulante Event Class. Choisissez Critical dans la liste déroulante Severity. Cliquez sur OK lorsque vous avez terminé.



4. Cliquez sur Add sous les filtres d'ID de message si des messages supplémentaires sont requis. Dans cet exemple, vous devez inclure les messages avec les ID 611101 à 611323.

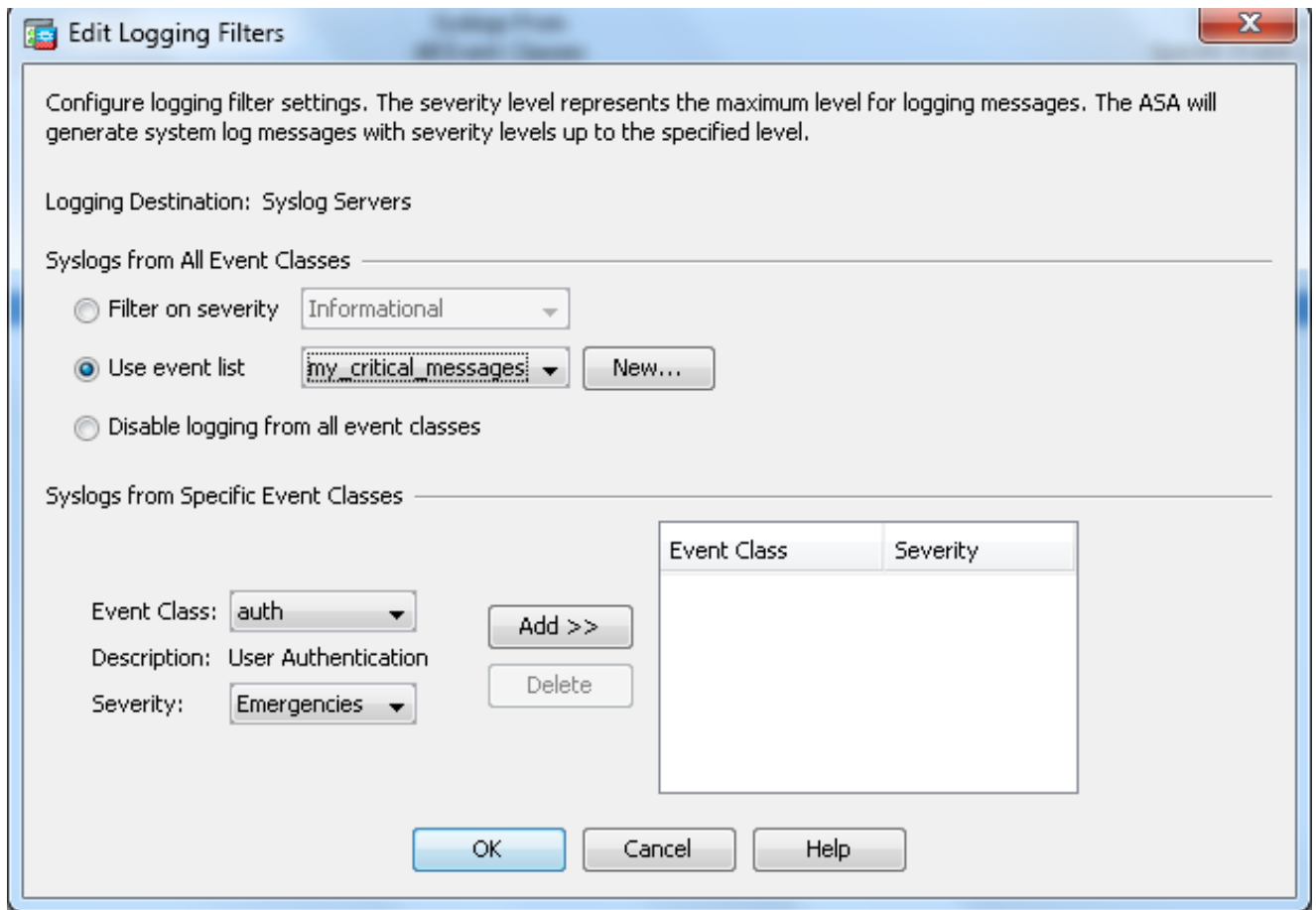


5. Indiquez la plage d'ID dans la case des ID de message et cliquez sur OK.

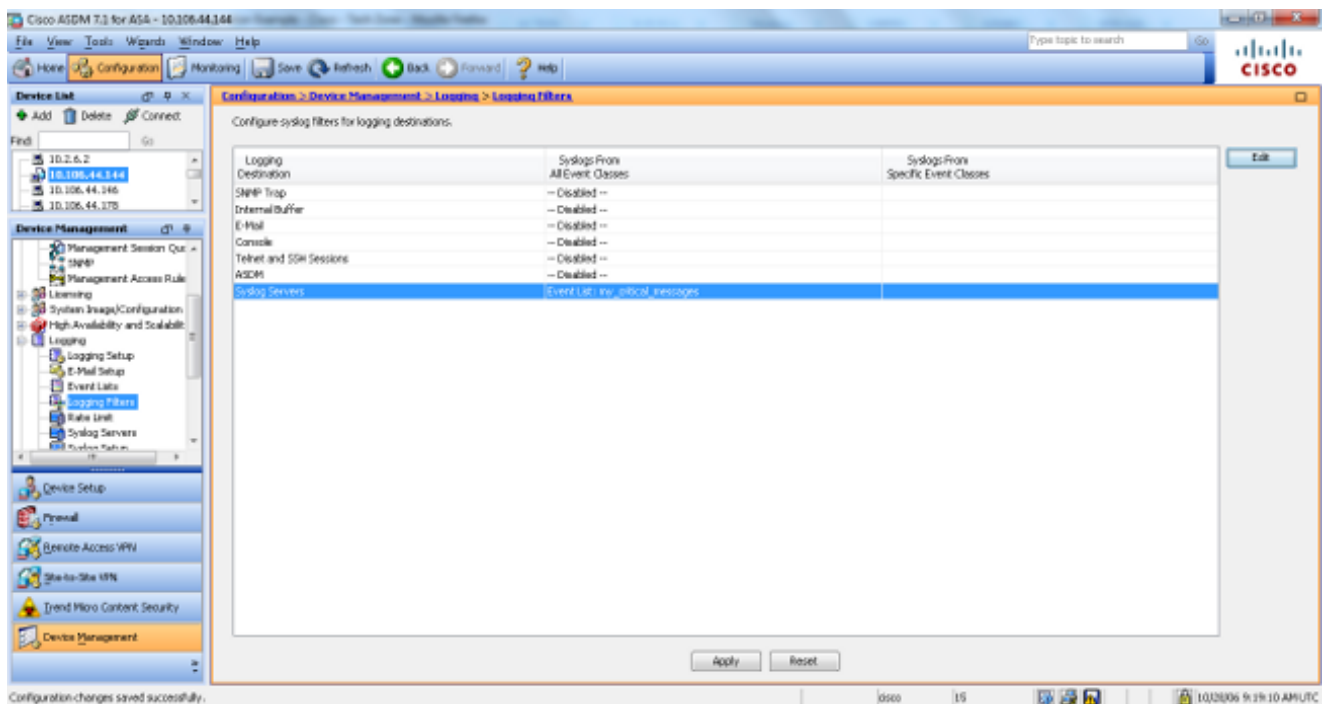


6. Retournez au menu Logging Filters et choisissez Console comme destination.

7. Sélectionnez my_critical_messages dans la liste déroulante Utiliser la liste d'événements. Cliquez sur OK lorsque vous avez terminé.



8. Cliquez sur Apply après être revenu à la fenêtre des filtres de journalisation.



Les configurations ASDM sont ainsi complétées par l'utilisation d'une liste de messages, comme illustré dans l'exemple 2.

Utilisation de la catégorie de message

Utilisez la catégorie de message afin d'envoyer tous les messages liés à une catégorie à l'emplacement de sortie indiqué. Quand vous précisez un seuil de niveau de gravité, vous pouvez limiter le nombre de messages envoyés à l'emplacement de sortie.

```
<#root>
```

```
logging class
```

```
message_class destination | severity_level
```

Exemple 3

Saisissez cette commande afin d'envoyer tous les messages de la catégorie ca avec un niveau de gravité urgent ou supérieur vers la console.

```
<#root>
```

```
logging class ca console emergencies
```

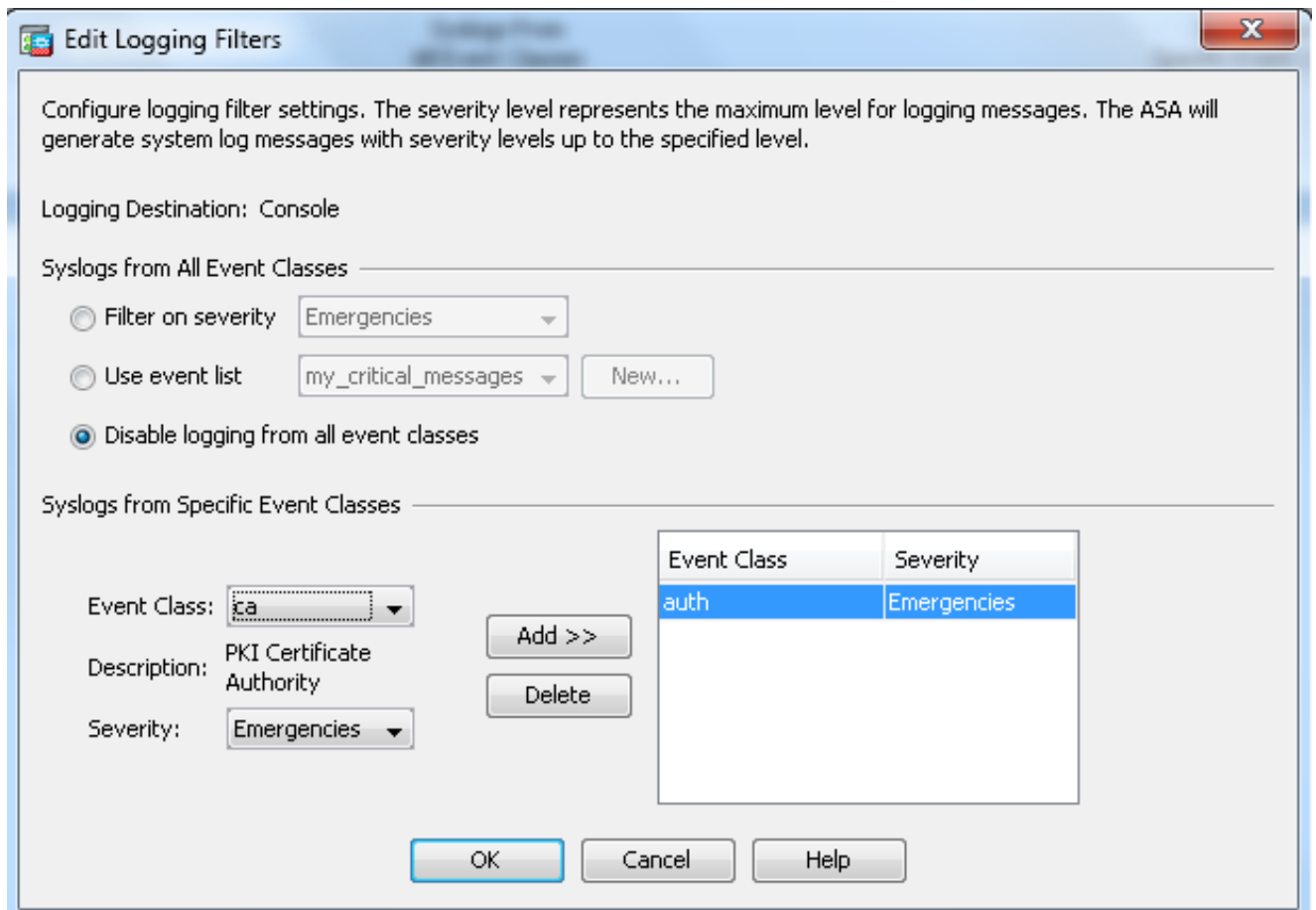
Configuration ASDM

Cette procédure montre les configurations ASDM pour l'exemple 3 avec l'utilisation de la liste de messages.

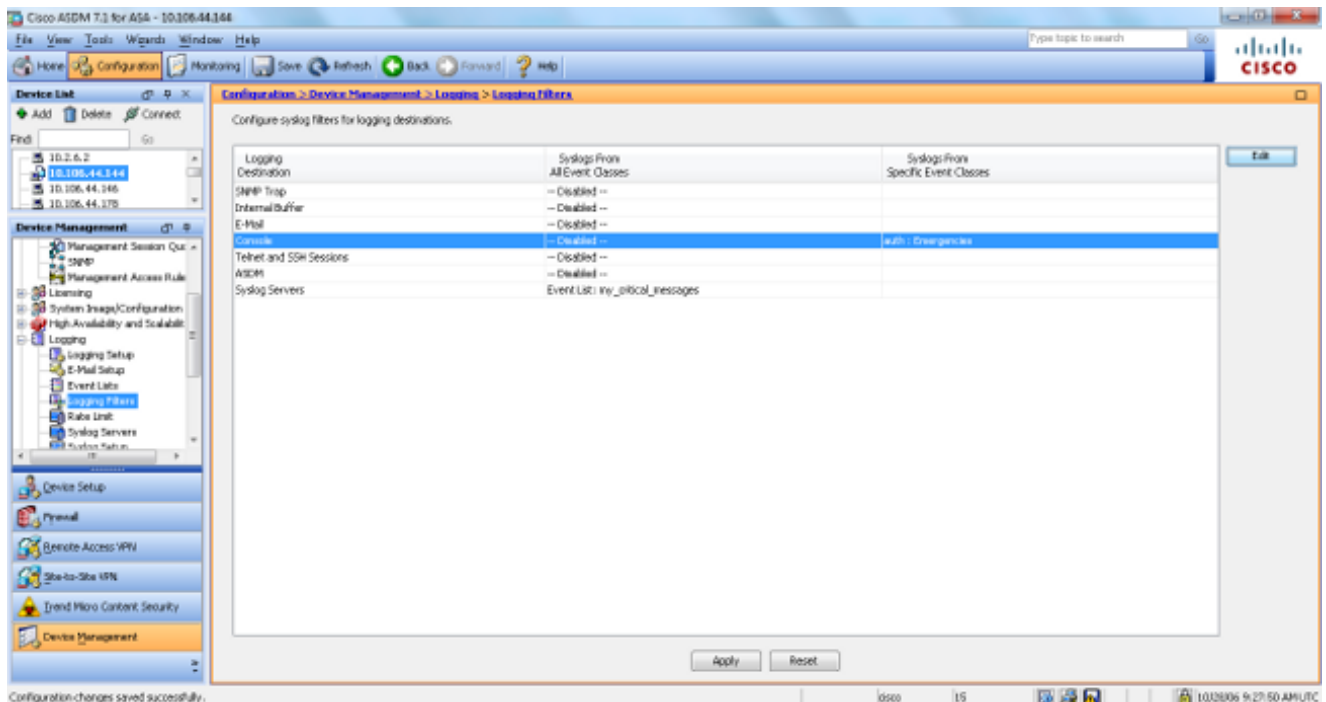
1. Choisissez le menu Logging Filters et choisissez Console comme destination.
2. Cliquez sur Disable logging from all event classes.
3. Sous les Syslog des catégories d'événement spécifiques, choisissez la catégorie d'événement et la gravité que vous souhaitez ajouter.

Cette procédure utilise ca et Emergencies respectivement.

4. Cliquez sur Add afin d'ajouter cela dans la catégorie de message et cliquez sur OK.



5. Cliquez sur Apply après être revenu à la fenêtre des filtres de journalisation. La console collecte désormais le message de classe ca avec le niveau de gravité Urgences, comme indiqué dans la fenêtre Filtres de journalisation.



Cela termine la configuration ASDM pour l'exemple 3. Consultez le document [Messages listés par niveau de gravité pour obtenir une liste des niveaux de gravité des messages du journal.](#)

Envoyer les messages du journal de débogage à un serveur Syslog

Pour un dépannage avancé, des journaux de débogage spécifiques aux fonctionnalités/protocoles sont requis. Par défaut, ces messages de journal sont affichés sur le terminal (SSH/Telnet). En fonction du type de débogage et du taux de messages de débogage générés, l'utilisation de l'interface de ligne de commande peut s'avérer difficile si les débogages sont activés. En option, les messages de débogage peuvent être redirigés vers le processus syslog et générés en tant que syslog. Ces syslog peuvent être envoyés à n'importe quelle destination syslog comme n'importe quel autre syslog. Afin de dévier les débogages vers syslogs, entrez la commande `logging debug-trace`. Cette configuration envoie la sortie de débogage, en tant que Syslog, à un serveur Syslog.

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

Utilisation conjointe de la liste de journalisation et des classes de message

Entrez la commande `logging list` afin de capturer le syslog pour les messages VPN IPsec de LAN à LAN et d'accès à distance uniquement. Cet exemple capture tous les messages du journal système de la catégorie VPN (IKE et IPsec) avec le niveau de débogage ou supérieur.

Exemple

```
<#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
```

Journaliser les occurrences ACL

Ajoutez log à chaque élément de liste d'accès (ACE) que vous souhaitez afin de consigner quand une liste d'accès est atteinte. Utilisez cette syntaxe :

<#root>

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

Exemple

<#root>

```
ASAfirewall(config)#
```

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

Par défaut, les listes de contrôle d'accès consignent chaque paquet refusé. Il n'est pas nécessaire d'ajouter l'option log pour refuser les ACL pour générer des syslogs pour les paquets refusés. Quand l'option log est précisée, elle génère le message syslog 106100 pour l'ACE auquel elle est appliquée. Le message Syslog 106100 est généré pour chaque flux ACE d'autorisation ou de refus correspondant qui passe par le pare-feu ASA. Le flux de la première correspondance est mis en cache. Les correspondances ultérieures incrémentent le nombre d'occurrences affiché dans la commande show access-list. Le comportement de journalisation de liste d'accès par défaut, qui est le mot-clé de journal non spécifié, est que si un paquet est refusé, alors le message 106023 est généré, et si le paquet est autorisé, alors aucun message syslog n'est généré.

Un niveau Syslog facultatif (0 - 7) peut être indiqué pour les messages syslog générés (106100). Si aucun niveau n'est précisé, le niveau par défaut est 6 (informatif) pour un nouvel ACE. Si l'ACE existe déjà, son niveau de journal actuel reste inchangé. Si l'option log disable est spécifiée, la journalisation de la liste d'accès est complètement désactivée. Aucun message syslog, qui inclut le message 106023, n'est généré. L'option par défaut log restaure le comportement de journalisation de liste d'accès par défaut.

Réalisez ces étapes afin de permettre au message syslog 106100 de s'afficher dans la sortie de la console :

1. Entrez la commande logging enable afin d'activer la transmission des messages du journal système à tous les emplacements de sortie. Vous devez définir un emplacement de sortie de journalisation afin d'afficher tout journal.
2. Entrez la commande logging message <message_number> level <severity_level> afin de définir le niveau de gravité d'un message de journal système spécifique.

Dans ce cas, entrez la commande logging message 106100 afin d'activer le message 106100.

3. Entrez la liste des messages de la console de journalisation | severity_level afin de permettre aux messages du journal système de s'afficher sur la console d'appliance de sécurité (TTY) à mesure qu'ils se produisent. Réglez le severity_level entre 1 et 7, ou utilisez le nom du niveau. Vous pouvez également préciser quels messages sont envoyés avec la variable message_list.
4. Entrez la commande show logging message afin d'afficher une liste des messages du journal système qui ont été modifiés par rapport au paramètre par défaut, qui sont des messages qui ont été affectés à un niveau de gravité différent et des messages qui ont été désactivés.

Voici un exemple de sortie de la commande show logging message :

```
<#root>
ASAFirewall#
show logging message 106100

syslog 106100: default-level informational (enabled)
ASAFirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Blocage de la génération Syslog sur un ASA de secours

Commencez à partir de la version 9.4.1 du logiciel ASA et vous pouvez bloquer la génération de syslog spécifiques sur une unité en veille et utiliser cette commande :

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

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Si vous souhaitez supprimer un message syslog spécifique à envoyer au serveur syslog, vous devez entrer la commande comme indiqué.

```
<#root>
```

```
hostname(config)#  
no logging message  
<syslog_id>
```

Consultez ce document sur la commande [logging message](#) pour obtenir plus d'informations.

%ASA-3-201008 : Interdiction de nouvelles connexions

%ASA-3-201008 : Interdiction de nouvelles connexions. Un message d'erreur s'affiche lorsqu'un ASA ne parvient pas à contacter le serveur Syslog et qu'aucune nouvelle connexion n'est autorisée.

Solution

Ce message apparaît quand vous avez activé les messages du journal système de TCP et le serveur syslog ne peut pas être atteint, ou quand vous utilisez le serveur syslog Cisco ASA (PFSS) et que le disque du système Windows NT est plein. Procédez comme suit pour résoudre ce message d'erreur :

- Désactivez les messages du journal système de TCP s'ils sont activés.
- Si vous utilisez PFSS, libérez de l'espace sur le système Windows NT où PFSS réside.
- Assurez-vous que le serveur syslog est actif et que vous pouvez envoyer une requête ping à l'hôte depuis la console Cisco ASA.
- Redémarrez la journalisation de messages système de TCP pour autoriser le trafic.

Si le serveur syslog tombe en panne et que la journalisation TCP est configurée, utilisez la commande [logging permit-hostdown](#) ou passez à la journalisation UDP.

The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Device Management > Logging > Service Servers". Below the title bar, there is a navigation bar with buttons for Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help. The left sidebar contains a "Device Link" section with a list of IP addresses (10.2.6.2, 10.106.44.244, 10.106.44.246, 10.106.44.275) and a "Device Management" tree with categories like Management Access Rules, Licensing, System Image/Configuration, High Availability and Scalability, Logging, and Troubleshooting. The main content area displays a table for "Service Servers" with columns: Interface, IP Address, Protocol/Port, ENABLED, and Secure. The table contains one entry for the "inside" interface with IP 172.22.1.6, Protocol/Port UDP/5, ENABLED No, and Secure No. Below the table, there is a "Queue Size" field set to 512 and a checked checkbox "Allow user traffic to pass when TCP syslog server is down". "Apply" and "Reset" buttons are at the bottom. A status bar at the bottom left shows "Configuration changes saved successfully." and the bottom right shows system information like "asa0" and "15".

Interface	IP Address	Protocol/Port	ENABLED	Secure
inside	172.22.1.6	UDP/5	No	No

Informations connexes

- [Références des commandes du pare-feu Cisco Secure PIX](#)
- [Demandes de commentaires \(RFC\)](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.