ASA 8.2 : Configurez le Syslog utilisant l'ASDM

Contenu

Introduction

Ce document fournit des informations sur la façon dont configurer le Syslog sur l'appliance de sécurité adaptable Cisco (ASA) 8.x à l'aide du GUI d'Adaptive Security Device Manager (ASDM). Les messages du journal système sont les messages générés par Cisco ASA pour informer l'administrateur sur n'importe quel changement de la configuration, changements de configuration réseau, ou changements de la représentation du périphérique. En analysant les messages du journal système, un administrateur peut facilement dépanner l'erreur en exécutant une analyse de cause principale.

Des messages de Syslog sont principalement différenciés basés sur leur niveau d'importance.

1. Sévérité 0 - Messages d'urgence - La ressource est inutilisable
2. Sévérité 1 - Messages d'alerte - L'action immédiate est nécessaire

3. Sévérité 2 - Messages essentiels - États critiques
4. Sévérité 3 - Messages d'erreur - Conditions d'erreurs
5. Sévérité 4 - Messages d'avertissement - Conditions d'avertissement
6. Sévérité 5 - Messages de notification - Normale mais conditions significatives
7. Sévérité 6 - Messages d'information - Messages d'information seulement
8. Sévérité 7 - Messages de débogage - Messages de débogage seulement**Remarque:** Le niveau d'importance le plus élevé est une urgence et le niveau d'importance le plus bas met au point.

Des messages de Syslog d'échantillon générés par Cisco ASA sont affichés ici :

- %ASA-6-106012 : Refusez l'IP d'IP_address à IP_address, hexa d'options IP.
- %ASA-3-211001 : Erreur d'allocation de mémoire
- %ASA-5-335003 : ACL de par défaut NAC appliqué, ACL : Acl-nom - adresse de hôte

La valeur numérique X spécifié dans « %ASA-X-YYYYYY : », dénote la sévérité du message. Par exemple, "%ASA-6-106012" est un message d'information et "%ASA-5-335003" est un message d'erreur.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version 8.2 de Cisco ASA
- Version 6.2 de Cisco ASDM

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

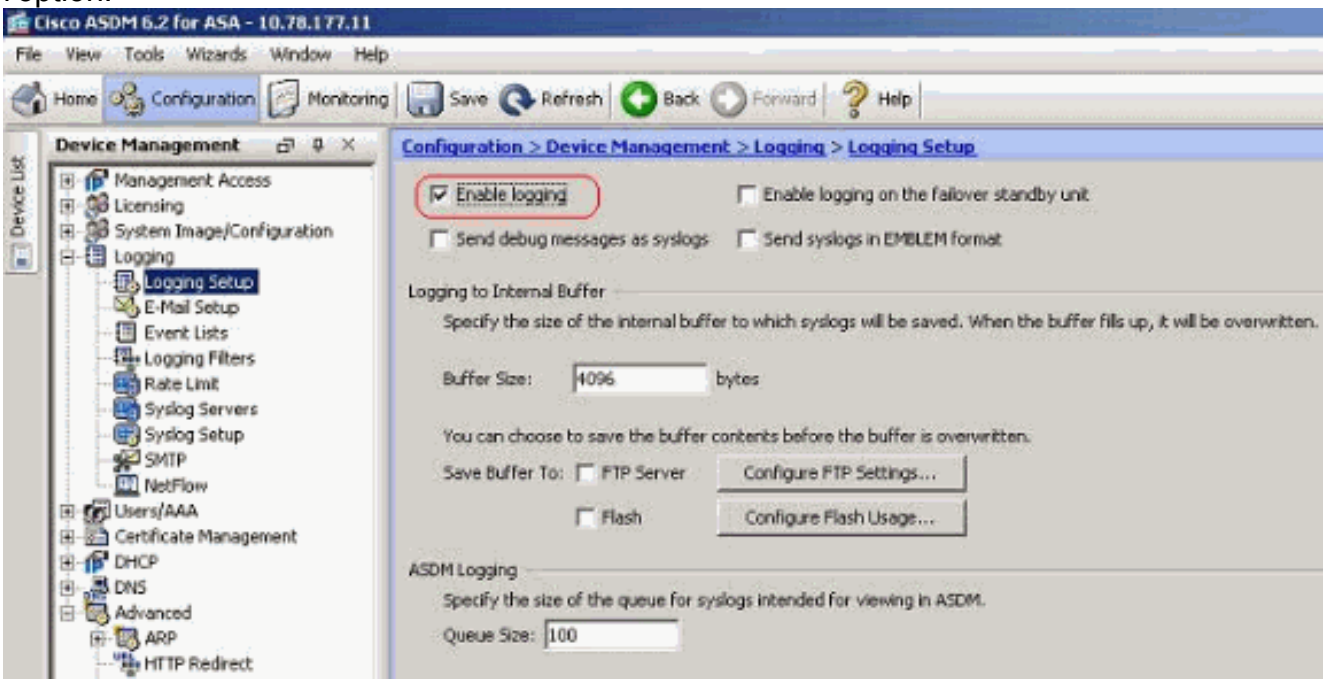
Configuration de base de Syslog à l'aide d'ASDM

Se connecter d'enable

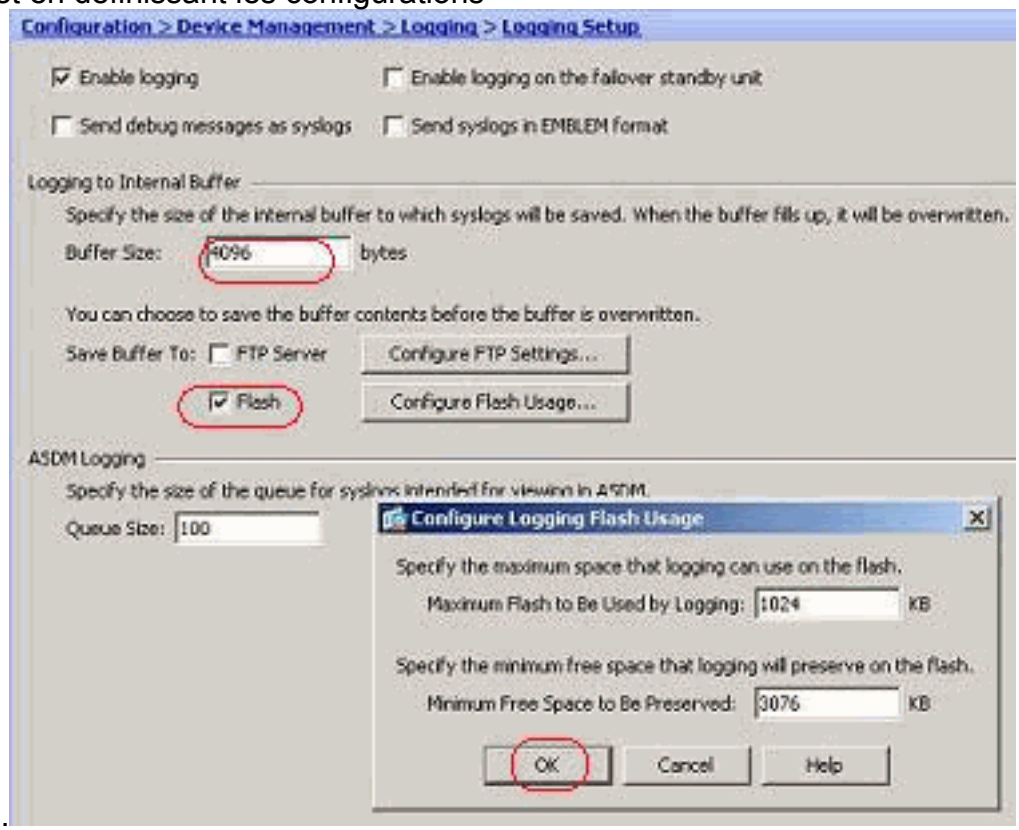
Procédez comme suit :

1. Choisissez la *configuration > la Gestion de périphériques > en se connectant > en se*

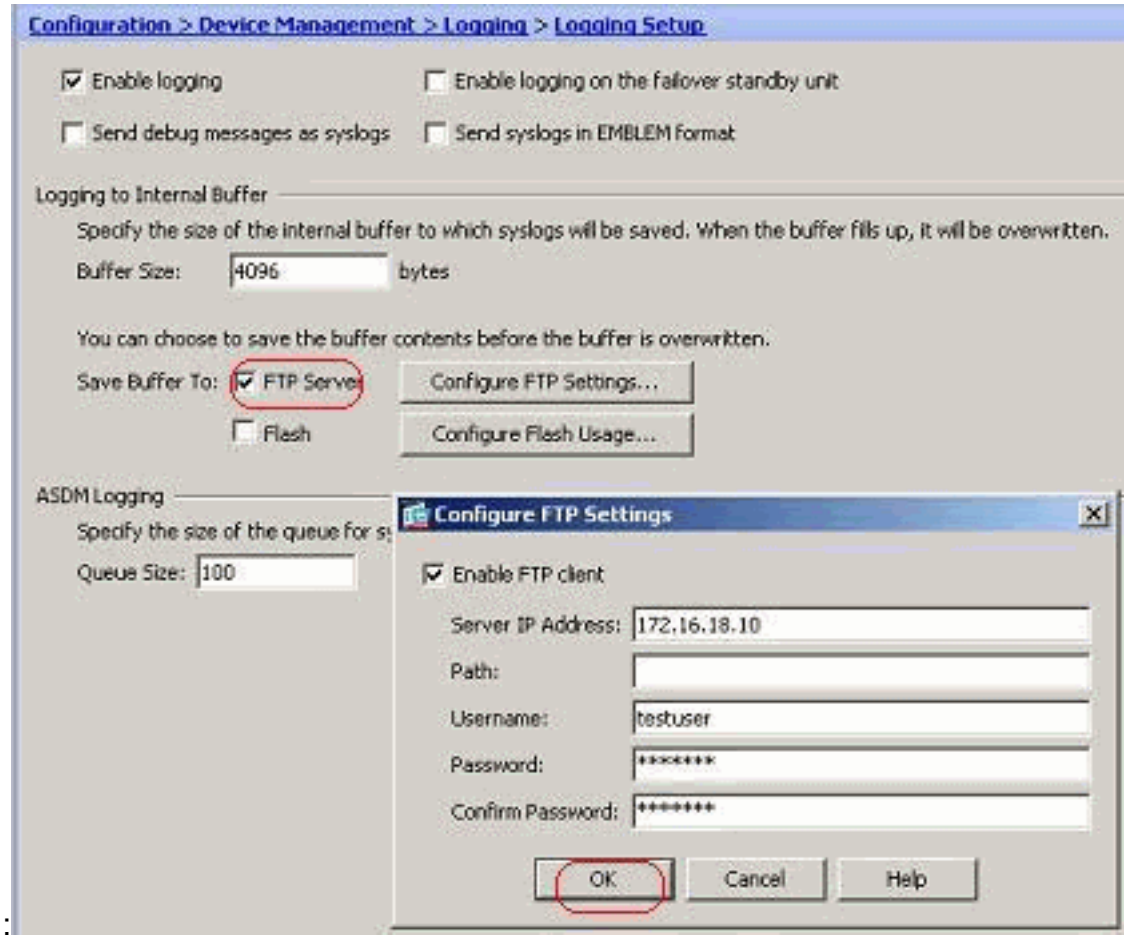
connectant l'installation et le coche l'*enable se connectant l'*option.



2. Vous pouvez se connecter les messages de Syslog à une mémoire tampon interne en spécifiant la taille de mémoire tampon. Vous pouvez également choisir de sauvegarder le contenu de mémoire tampon à la mémoire flash en cliquant sur Configure l'*utilisation instantanée* et en définissant les configurations instantanées.



3. Des messages de journal en mémoire tampon peuvent être envoyés à un ftp server avant qu'ils soient remplacés. Cliquez sur Configure les *configurations de FTP* et spécifiez les détails serveurs ftp comme affiché ici



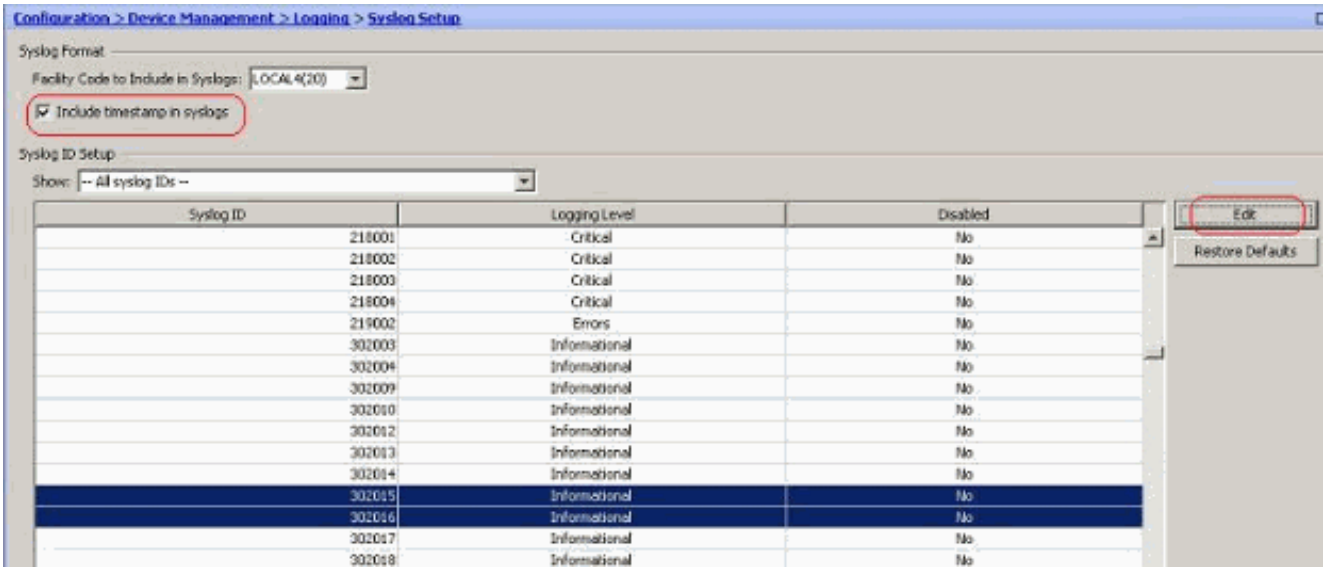
:

Se connecter de débronchement

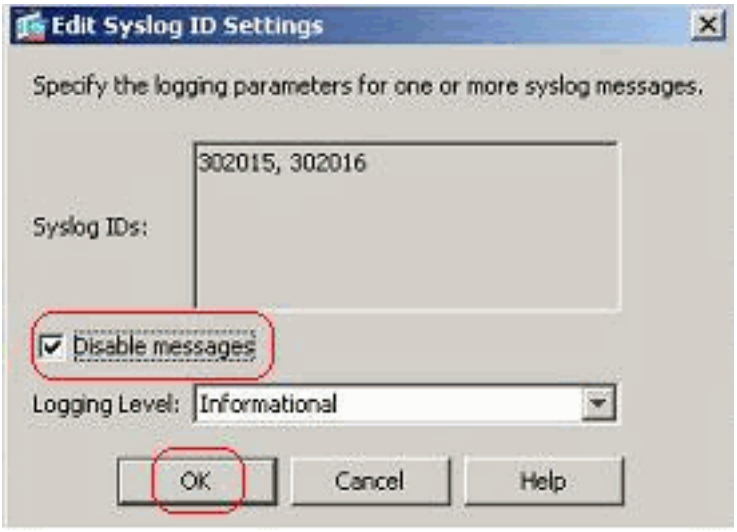
Vous pouvez désactiver des id spécifiques de Syslog basés sur votre condition requise.

Remarque: En sélectionnant le coche pour l'*horodateur d'inclusion dans l'*option de *Syslog*, vous pouvez ajouter la date et l'heure qu'elles ont été générées comme champ aux Syslog.

1. Sélectionnez les Syslog pour désactiver et cliquer sur
   Edit.

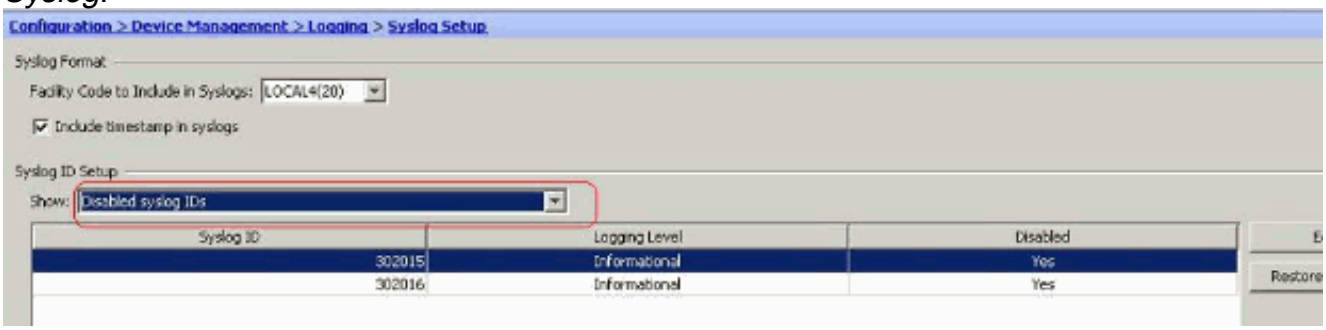


2. *Des configurations* fenêtre d'*ID de Syslog d'éditer*, le coche l'option de *messages de*



débronchement et cliquent sur OK.

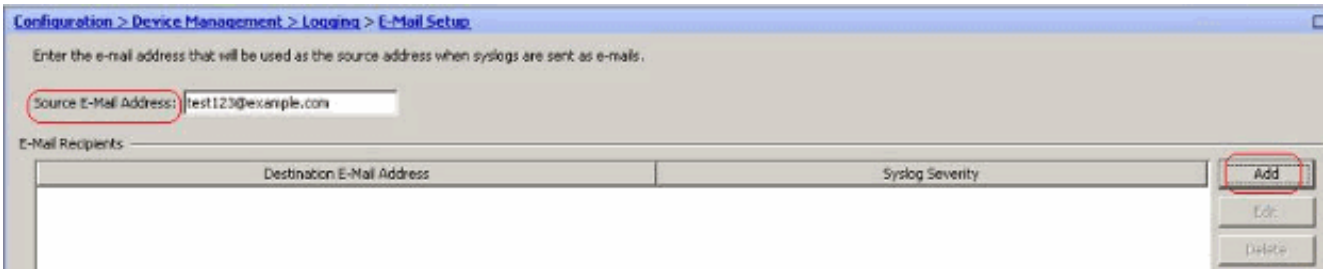
3. Les Syslog handicapés peuvent être visualisés dans un onglet distinct en sélectionnant des *id désactivés de Syslog du* menu déroulant d'*installation d'ID de Syslog*.



Se connecter à un courrier électronique

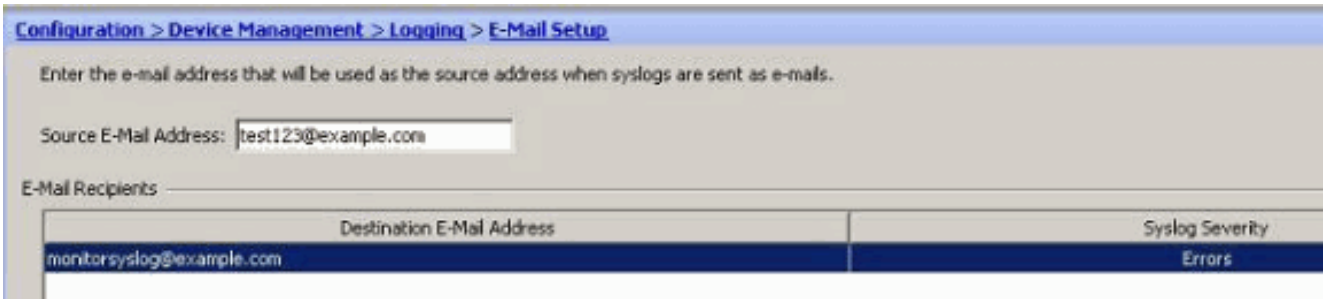
Terminez-vous ces étapes utilisant l'ASDM afin d'envoyer les Syslog à un courrier électronique :

1. Choisissez la *configuration > la Gestion de périphériques > en se connectant > installation de courrier électronique*. Le champ d'*adresse électronique de source* est utile en assignant un ID de courrier électronique comme source pour les Syslog. Spécifiez l'adresse électronique de source. Maintenant, cliquez sur Add pour ajouter les destinataires des mails.

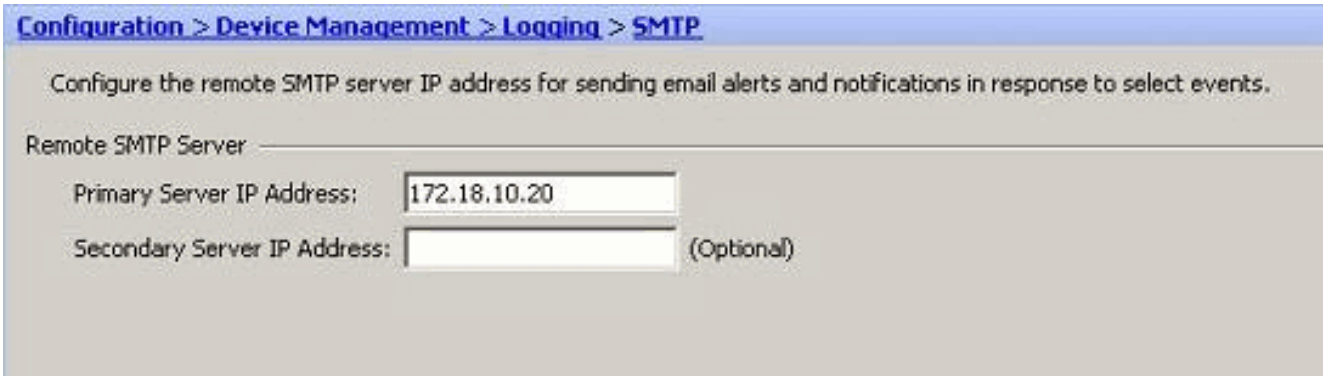


2. Spécifiez l'*adresse électronique de destination* et choisissez le *niveau d'importance*. Basé aux niveaux d'importance, vous pouvez définir différents destinataires des mails. Cliquez sur OK pour retourner de nouveau au volet d'*installation de courrier*

électronique. Ceci a comme conséquence cette configuration :



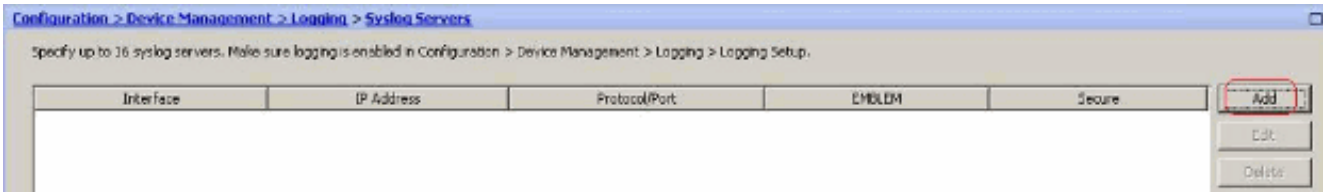
3. Choisissez la *configuration > l'installation de périphérique > en se connectant > SMTP* et spécifiez le serveur SMTP.



Se connecter à un serveur de Syslog

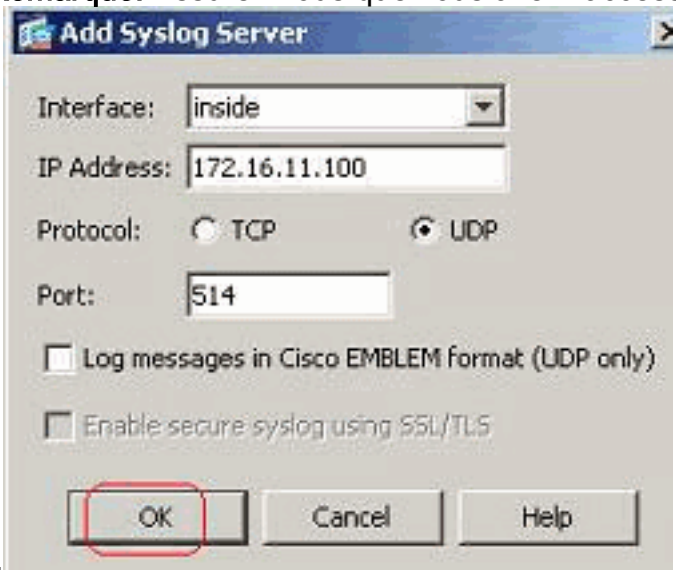
Vous pouvez envoyer tous les messages de Syslog à un serveur dédié de Syslog. Exécutez ces étapes à l'aide de l'ASDM :

1. Choisissez la *configuration > la Gestion de périphériques > en se connectant > des serveurs de Syslog* et cliquez sur Add pour ajouter un serveur de Syslog.

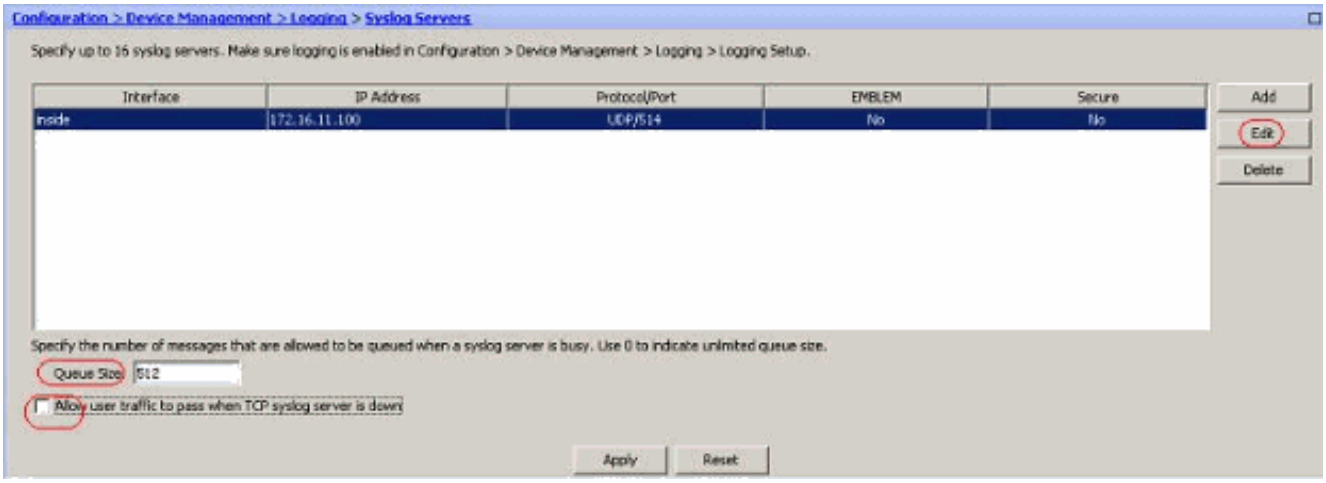


La fenêtre de *serveur de Syslog d'ajouter* apparaît.

2. Spécifiez l'interface que le serveur est associé avec avec l'adresse IP. Spécifiez *Protocol* et *mettez en communication les* détails selon votre configuration réseau. Puis, cliquez sur OK.**Remarque:** Assurez-vous que vous avez l'accessibilité au serveur de Syslog de Cisco ASA.



3. Le serveur configuré de Syslog est vu comme affiché ici. Des modifications peuvent être faites quand vous sélectionnez ce serveur, alors cliquent sur Edit.



Remarque: Coche le *trafic d'utilisateur d'autoriser à passer quand le serveur de Syslog de TCP est en bas de l'*option. Autrement, les nouvelles sessions d'utilisateur sont refusées par l'ASA. Ce s'applique seulement quand le protocole de transport entre l'ASA et le serveur de Syslog est TCP. Par défaut, de nouvelles sessions d'accès au réseau sont refusées par Cisco ASA quand un serveur de Syslog est en panne pour une raison quelconque.Afin de définir le type de messages de Syslog qui doivent être envoyés au serveur de Syslog, voyez la section se connectante de filtre.

Configuration avancée de Syslog à l'aide d'ASDM

Fonctionner avec des listes d'événements

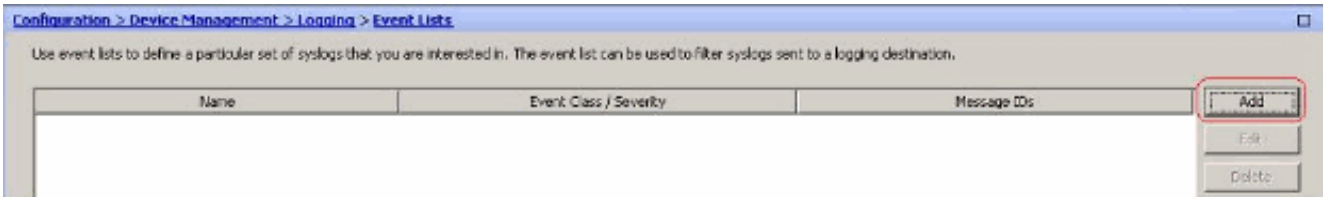
Les listes d'événements nous permettent de créer les listes personnalisées qui contiennent le groupe de messages de Syslog qui doivent être envoyés à une destination. Des listes d'événements peuvent être créées de trois manières différentes :

- ID de message ou plage des id de message
- Sévérité de message
- Classe de message

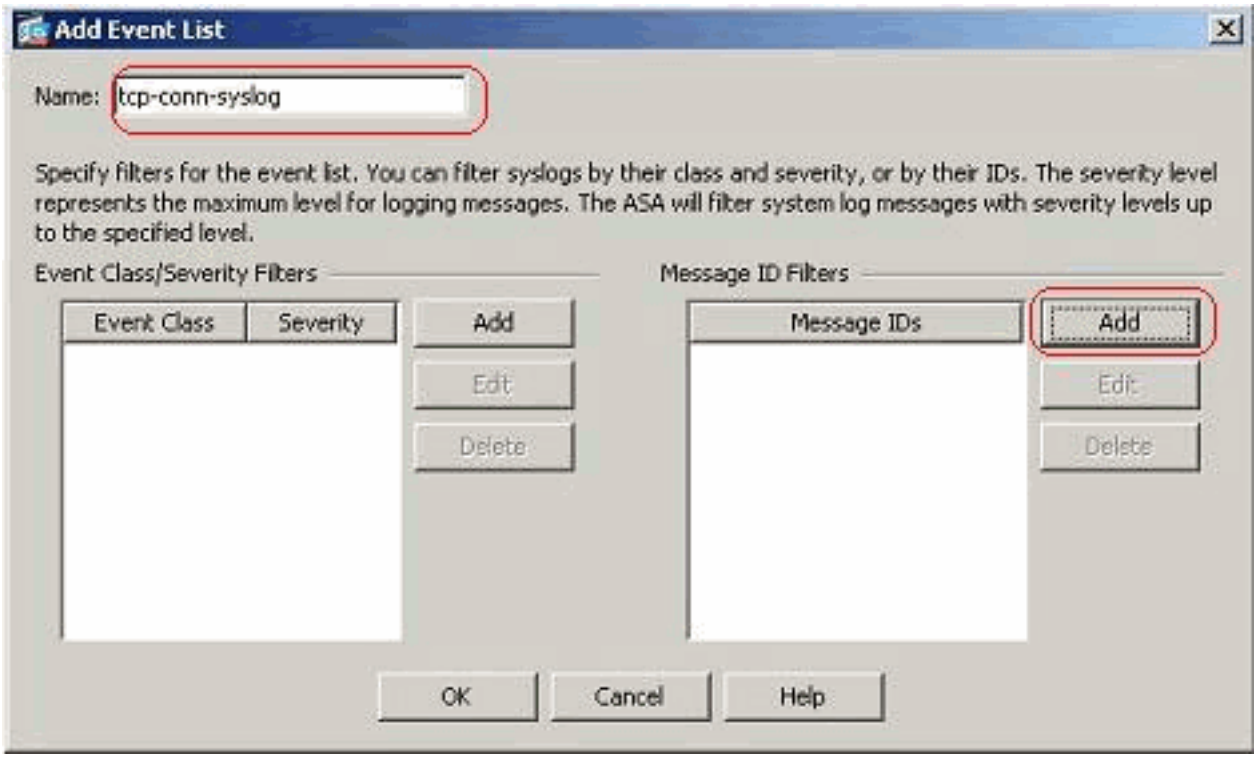
ID de message ou plage des id de message

Effectuez les étapes suivantes :

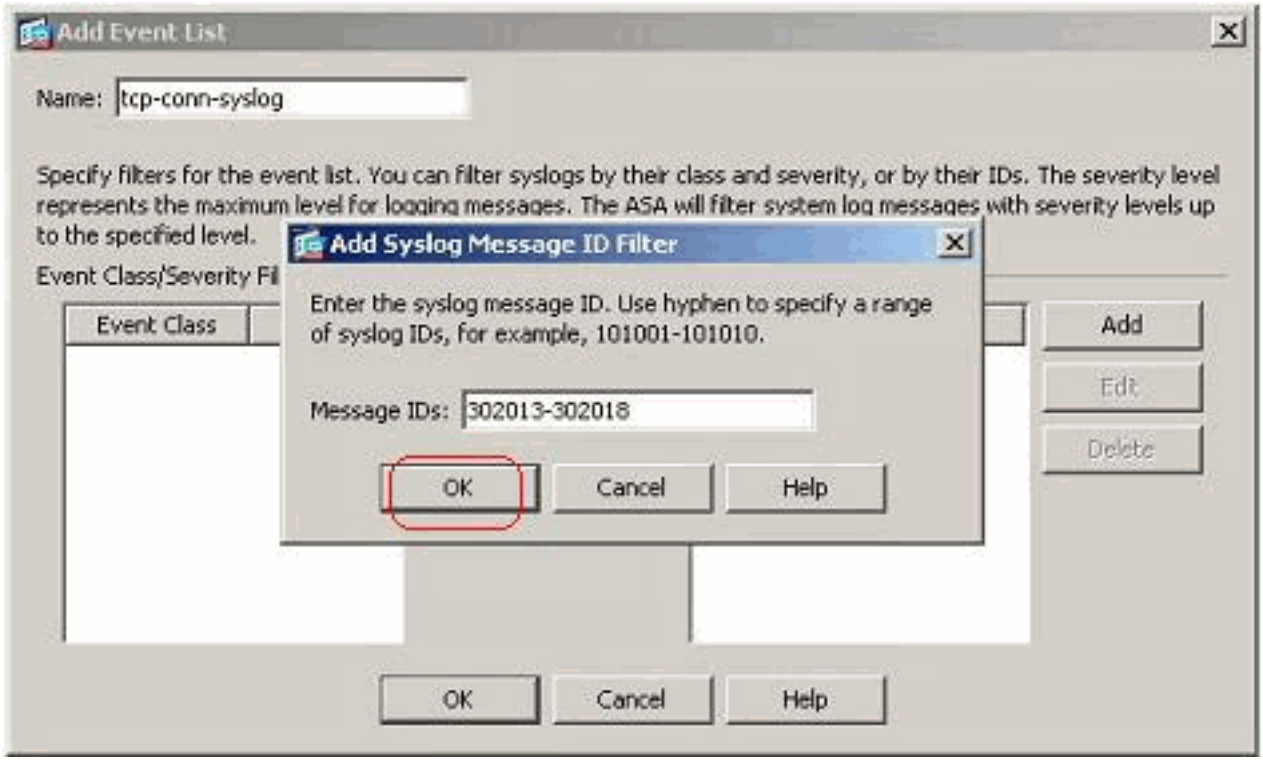
1. Choisissez la *configuration > la Gestion de périphériques > en se connectant > des listes d'événements* et cliquez sur Add pour créer une nouvelle liste d'événements.



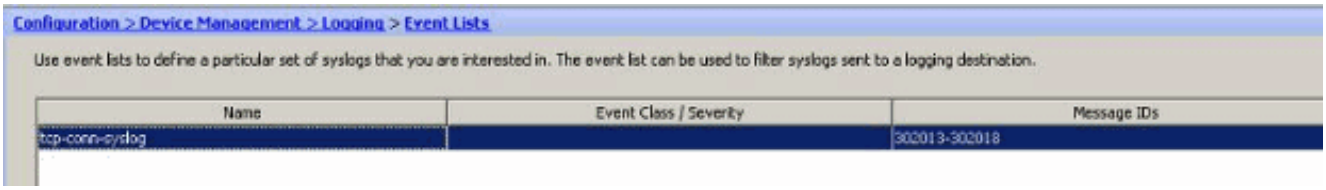
2. Spécifiez un nom dans la zone d'*identification*. Cliquez sur Add dans le volet de *filtres d'ID de message* pour créer une nouvelle liste d'événements.



3. Spécifiez la plage des id de message de Syslog. Ici les messages de Syslog de TCP ont pris par exemple. Cliquez sur **OK** pour terminer.

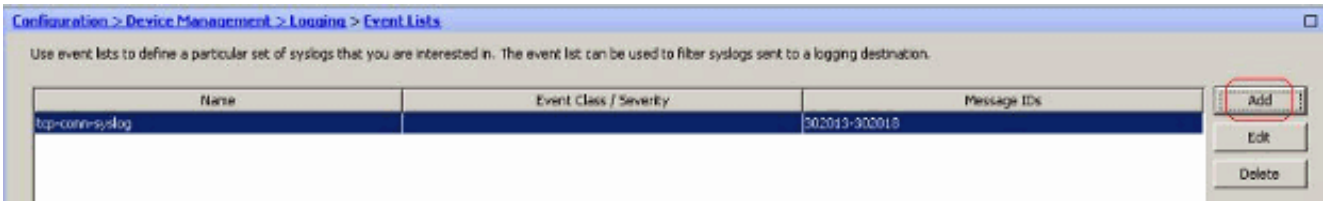


4. Cliquez sur OK de nouveau afin de revenir à la fenêtre de *listes d'événements*.

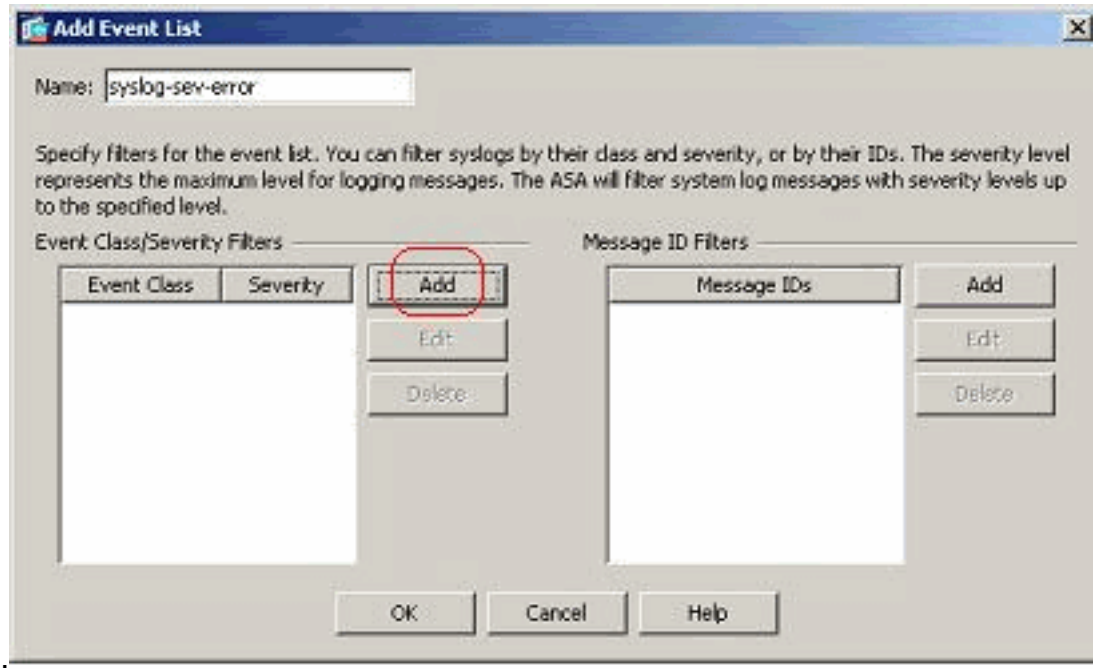


Sévérité de message

1. Des listes d'événements peuvent également être définies ont basé sur la sévérité de message. Cliquez sur Add pour créer une liste d'événements distincte.

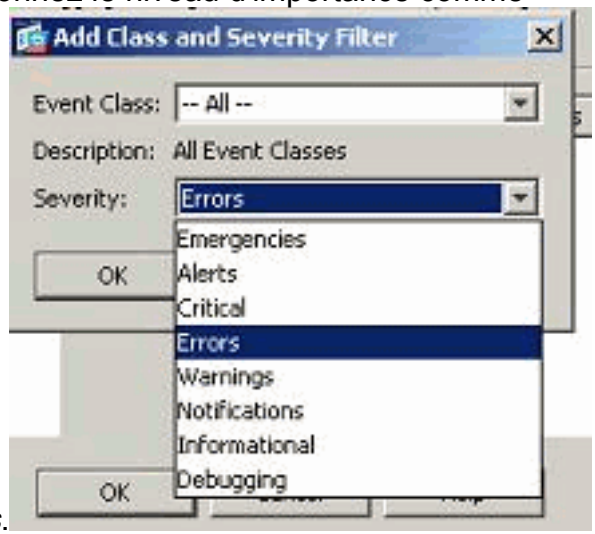


2. Spécifiez le nom et cliquez sur



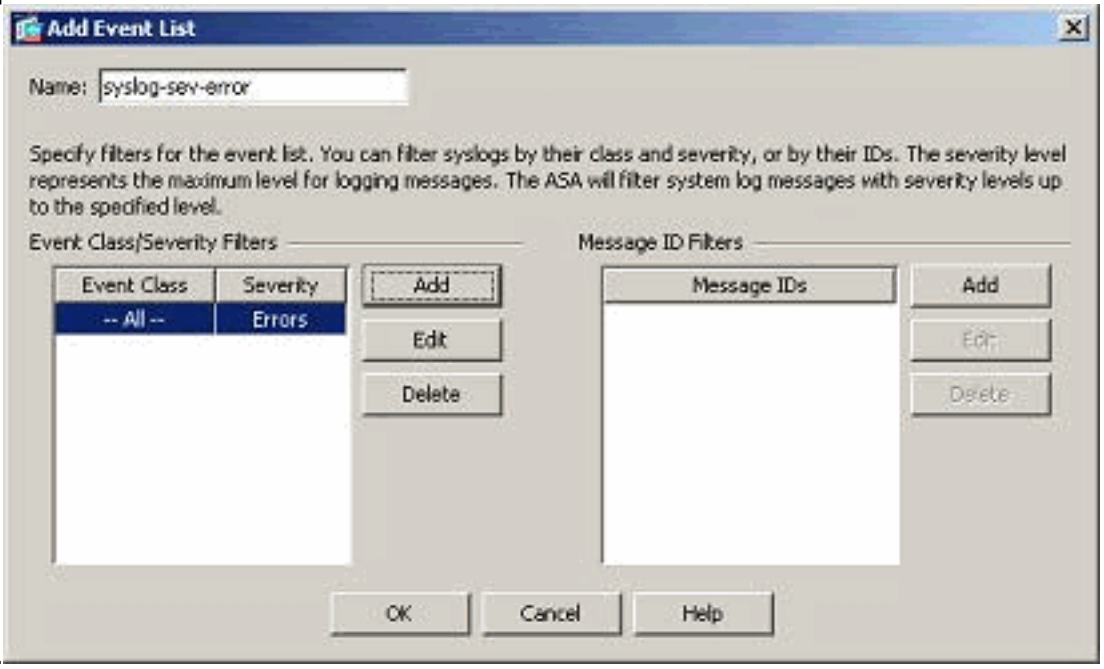
Add.

3. Sélectionnez le niveau d'importance comme



erreurs.

4. Cliquez sur



OK.

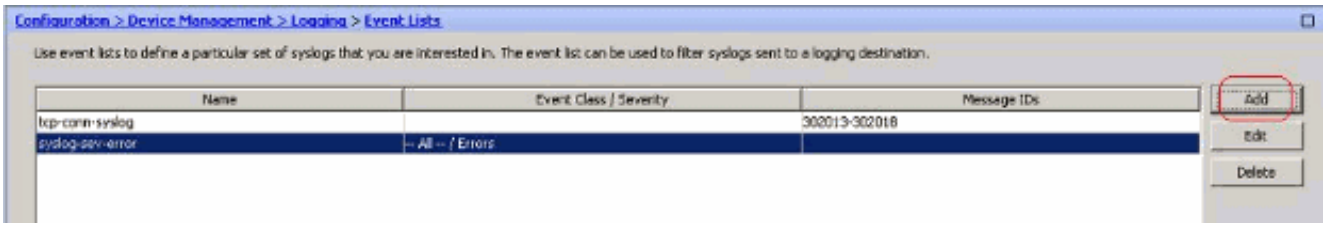
Classe de message

Des listes d'événements sont également configurées basées sur la classe de message. Une classe de message est un groupe de messages de Syslog liés à une caractéristique de dispositifs de sécurité qui te permet de spécifier une classe entière des messages au lieu de spécifier une classe pour chaque message individuellement. Par exemple, employez la classe authentique pour sélectionner tous les messages de Syslog qui sont liés à l'authentification de l'utilisateur. Quelques classes de messages disponibles sont affichées ici :

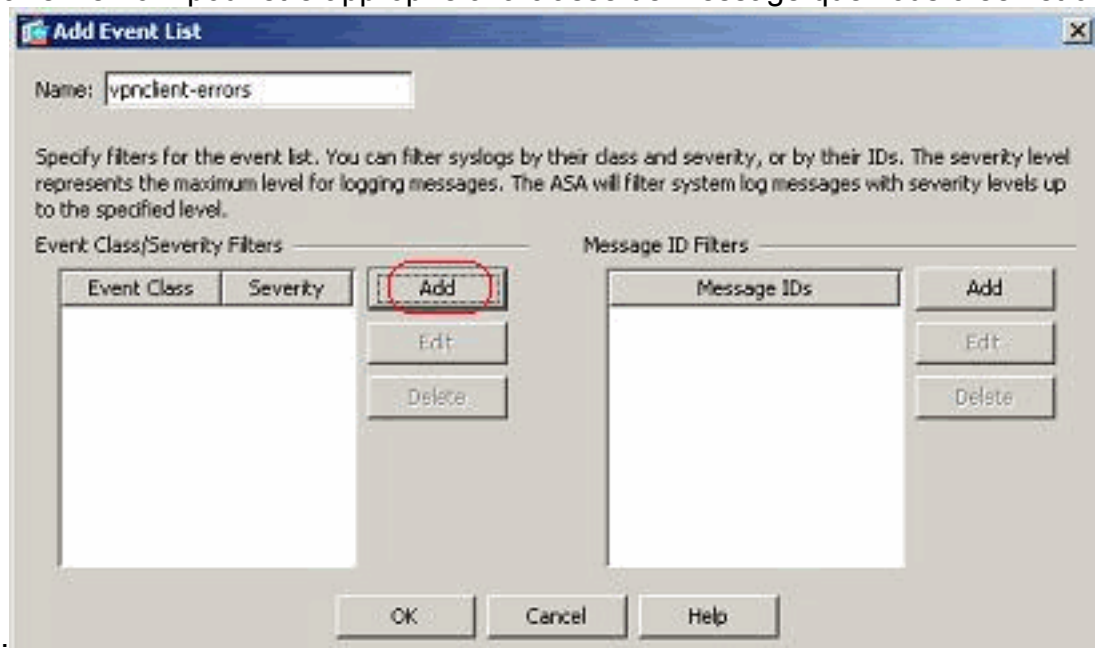
- Entièrement toutes les classes d'événement
- authentique — Authentification de l'utilisateur
- passerelle — Pare-feu transparent
- Ca — Autorité de certification de PKI
- config — Commande interface
- ha — Basculement
- IPS — Service de protection contre les intrusions
- IP — Pile IP
- le NP — Processeur de réseau
- OSPF — Routage OSPF
- déchirure — Routage de RIP
- session — Session d'utilisateur

Exécutez ces étapes pour créer une classe d'événement basée sur la classe de message de vpnclient-*erreurs*. La classe de message, *vpnc*, est disponible pour classer tous les messages par catégorie de Syslog liés au vpnclient. Le niveau d'importance pour cette classe de message est choisi en tant que « erreurs ».

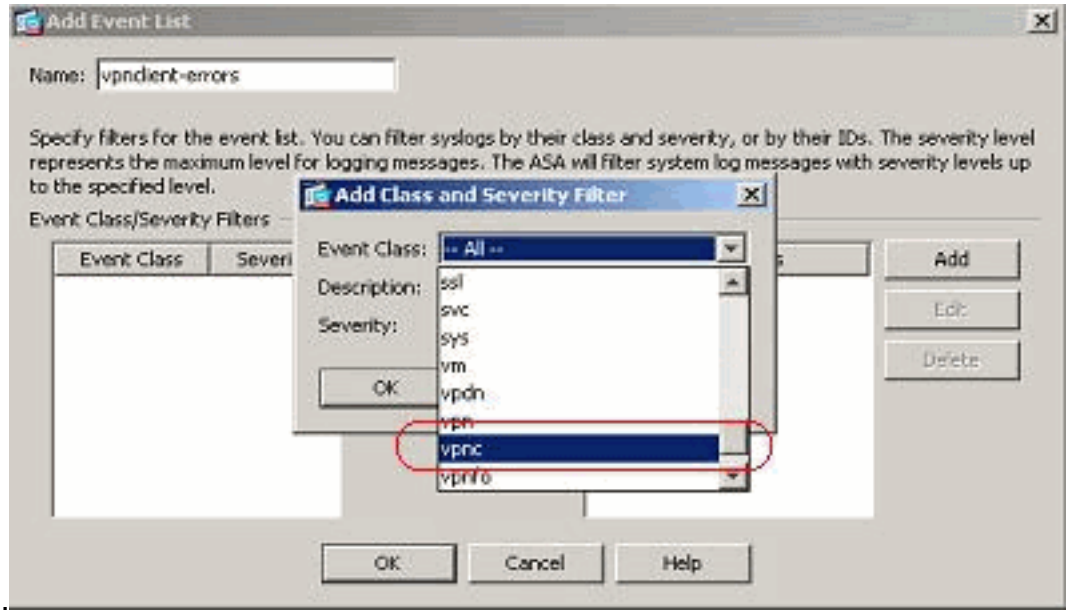
1. Cliquez sur Add pour créer une nouvelle liste d'événements.



2. Spécifiez le nom pour être approprié à la classe de message que vous créez et cliquez sur Add.

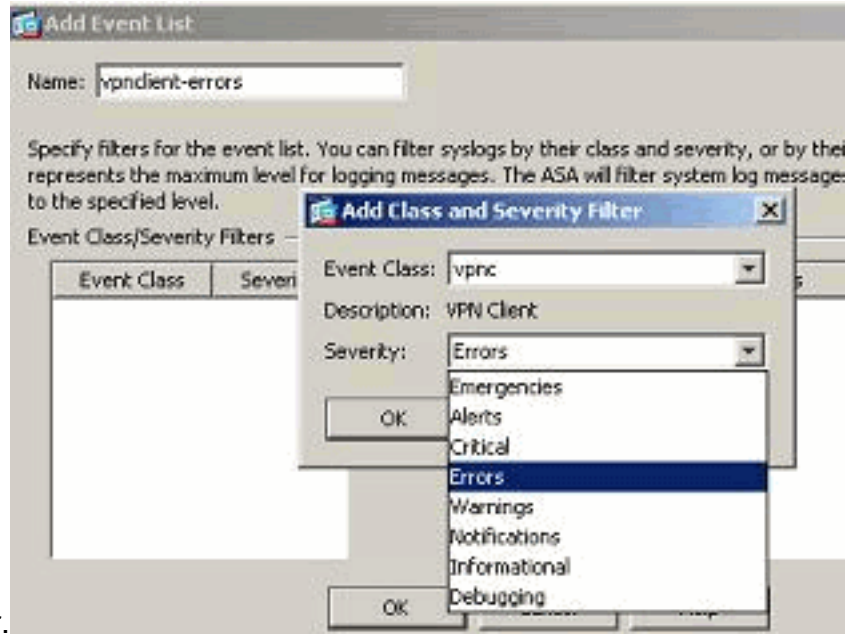


3. *Vpnc* choisi de la liste



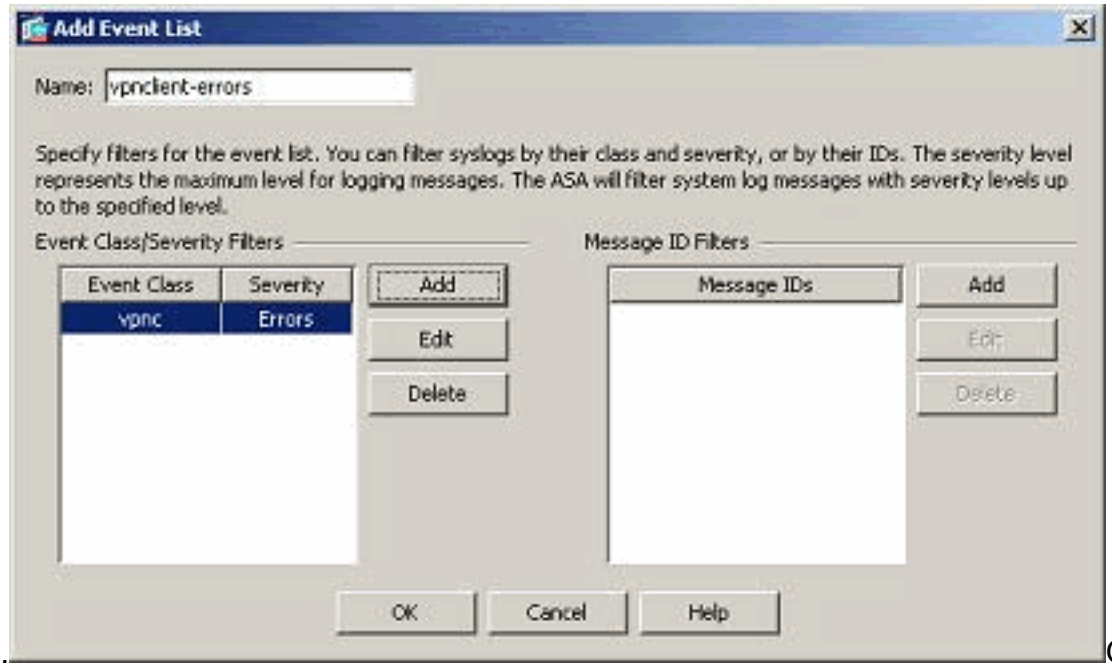
déroulante.

4. Sélectionnez le niveau d'importance comme *erreurs*. Ce niveau d'importance s'applique pour ces messages qui sont enregistré pour cette classe de message seulement. Cliquez sur OK pour revenir à la fenêtre de liste d'événements

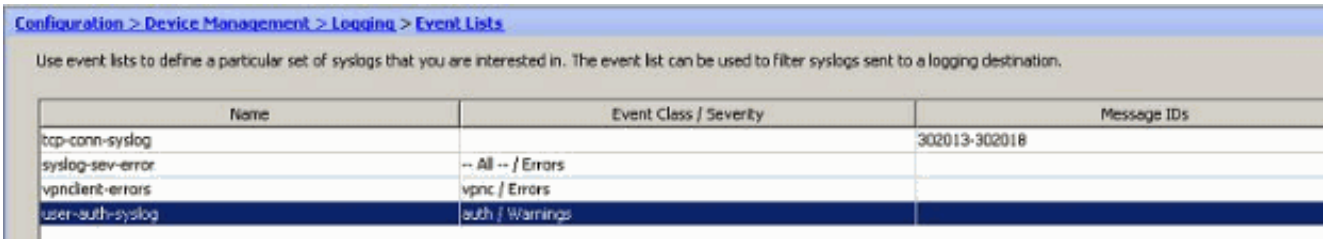


d'ajouter.

5. La classe d'événement/sévérité est affichée ici. Cliquez sur OK pour se terminer en configurant la liste d'événements de « vpnclient-



erreurs ».On lui affiche également au tir d'écran suivant qu'une nouvelle liste d'événements, le « utilisateur-auth-Syslog », est créé avec une classe de message en tant que « authentique » et au niveau d'importance pour les Syslog de cette classe de message spécifique en tant que « avertissements ». En configurant ceci, la liste d'événements spécifie tous les messages de Syslog qui sont liés à la classe de message « authentique », avec des niveaux d'importance **jusqu'aux** « avertissements » de niveau.**Remarque:** Ici, le terme « jusqu'à » est d'importance. En dénotant le niveau d'importance, maintenez dans l'esprit que tous les messages de Syslog veulent sont enregistré jusqu'à ce niveau.**Remarque:** Une liste d'événements peut contenir de plusieurs classes d'événement. La liste d'événements de « vpnclient-erreurs » est modifiée en cliquant sur Edit et en définissant une nouvelle classe d'événement « SSL/erreur ».



Fonctionner avec le Logging Filters

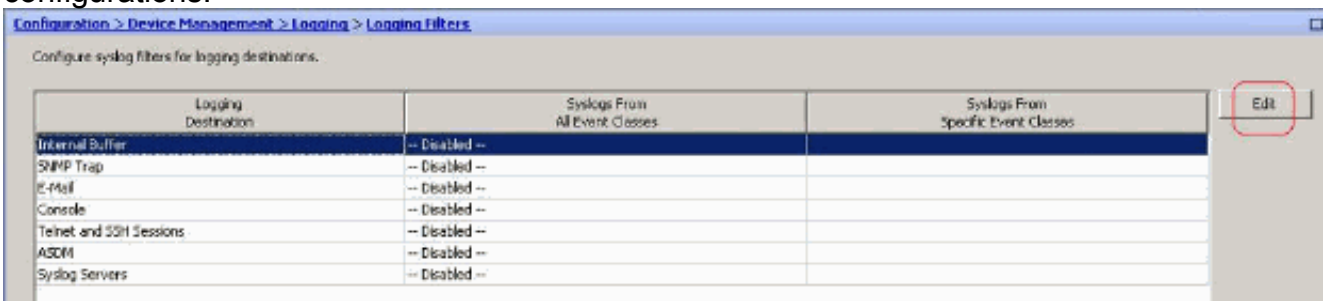
Se connectant des filtres sont utilisés pour envoyer les messages de Syslog à une destination spécifiée. Ces messages de Syslog peuvent être basés sur la « sévérité » ou « le répertorie même ».

Ce sont les types de destinations auxquelles ces filtres s'appliquent :

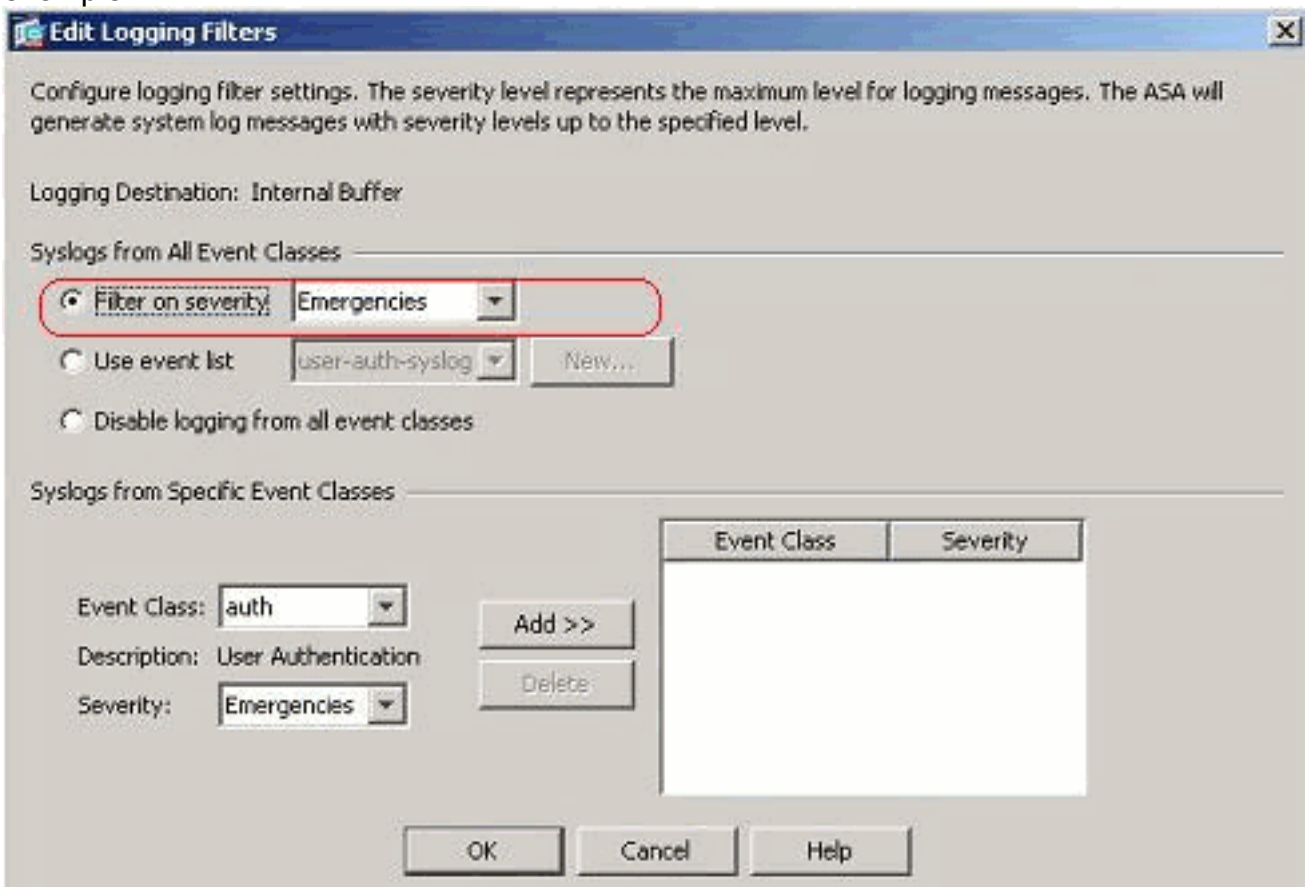
- Tampon interne
- Déroutement SNMP
- Courrier électronique
- Console
- Sessions de telnet
- ASDM
- Serveurs de Syslog

Effectuez les étapes suivantes :

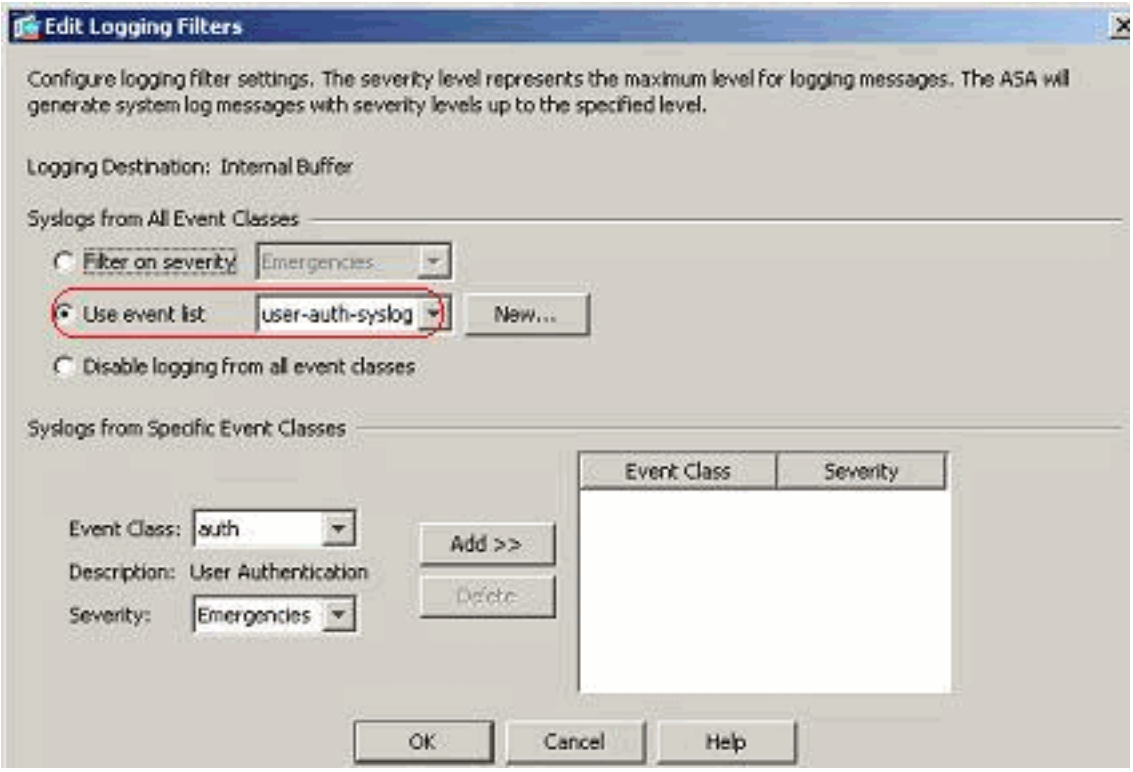
1. Choisissez la **configuration > la Gestion de périphériques > en se connectant > Logging Filters** et sélectionnez la destination de journalisation. Puis, cliquez sur Edit pour modifier les configurations.



2. Vous pouvez envoyer les messages de Syslog basés sur la sévérité. Ici, des **urgences** a été sélectionnées pour afficher comme exemple.

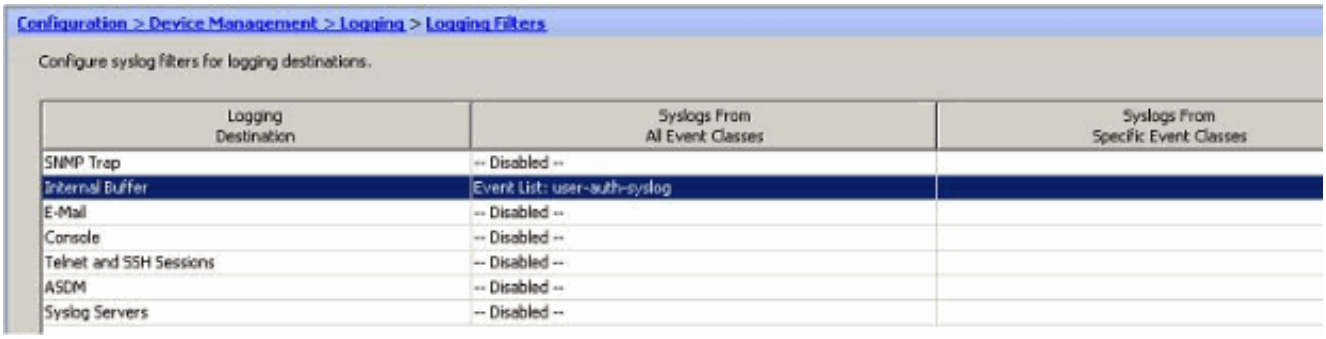


3. Une liste d'événements peut également être sélectionnée pour spécifier que le type de messages doivent être envoyé à une destination particulière. Cliquez sur



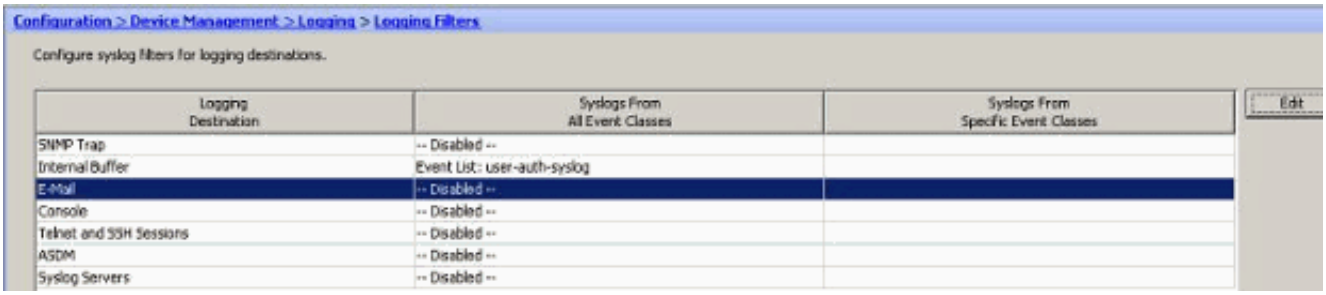
OK.

4. Vérifiez la modification.

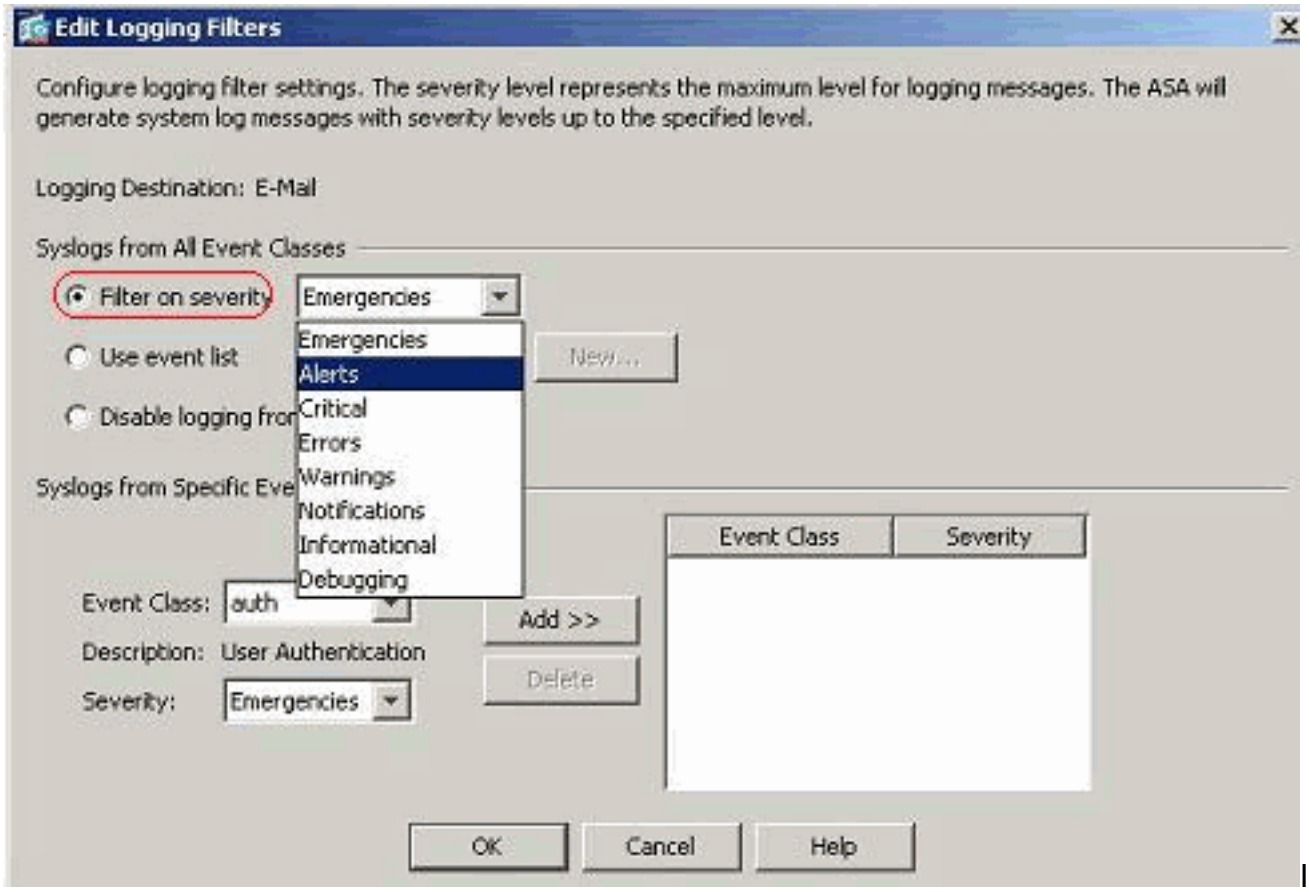


Ce sont les étapes sur la façon dont envoyer un groupe de messages (basés sur leur niveau d'importance) au serveur de mail.

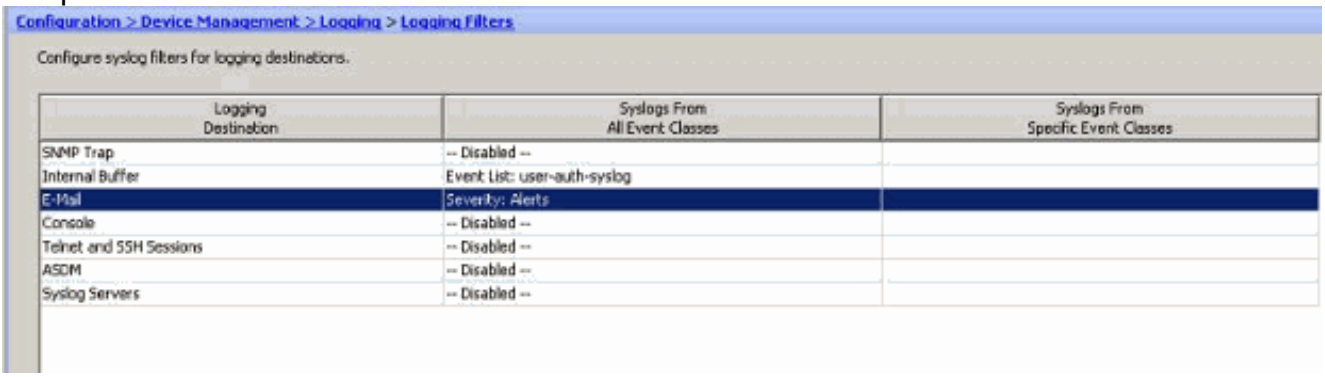
1. **Courrier électronique** choisi dans la zone réceptrice de destination de journalisation. Puis, cliquez sur Edit.



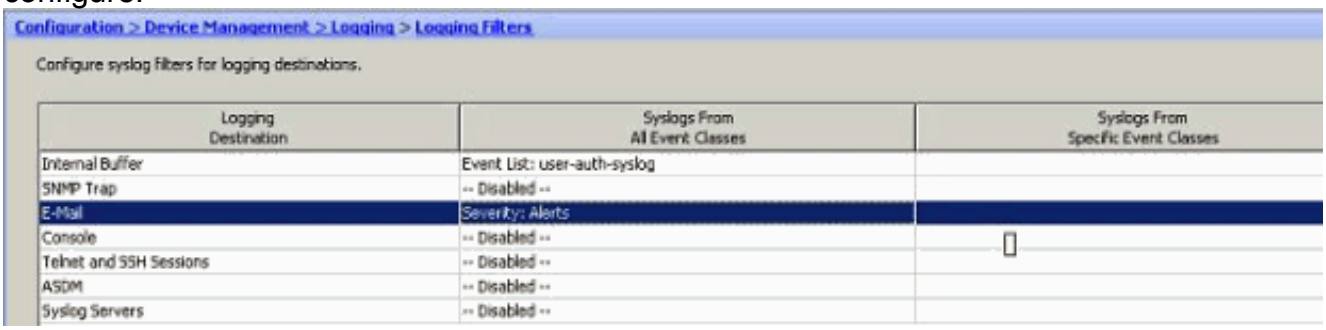
2. Choisissez le **filtre en l'**option de **sévérité** et sélectionnez le niveau d'importance exigé.



ci, des **alertes** a été sélectionnées comme niveau d'importance.



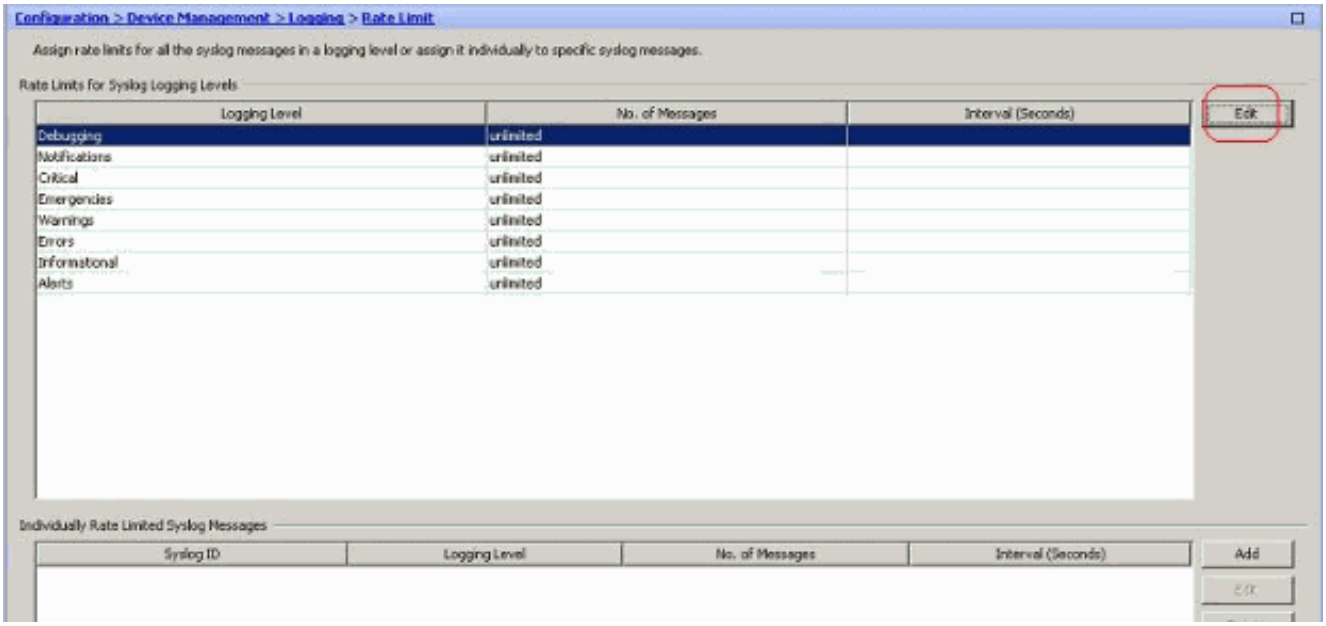
Vous pouvez voir que tous les messages vigilants de Syslog doivent être envoyés au courrier électronique configuré.



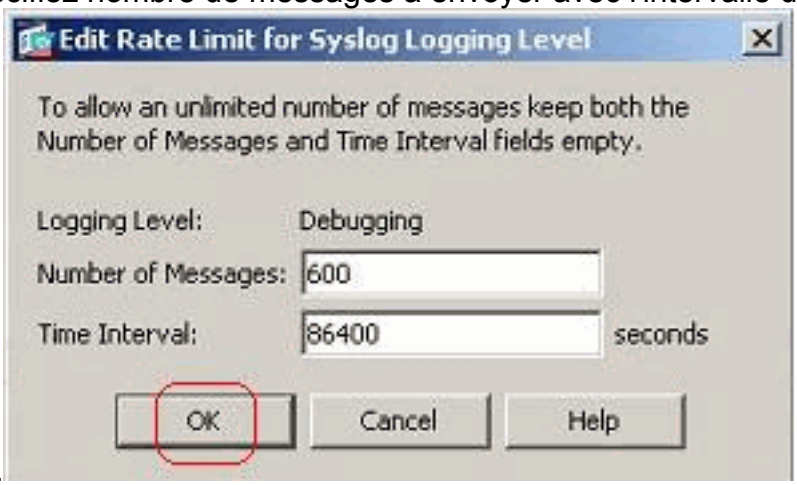
Raté limit

Ceci spécifie le nombre de messages de Syslog que Cisco ASA envoie à un destination in par période indiquée. Il est habituellement défini pour le niveau d'importance.

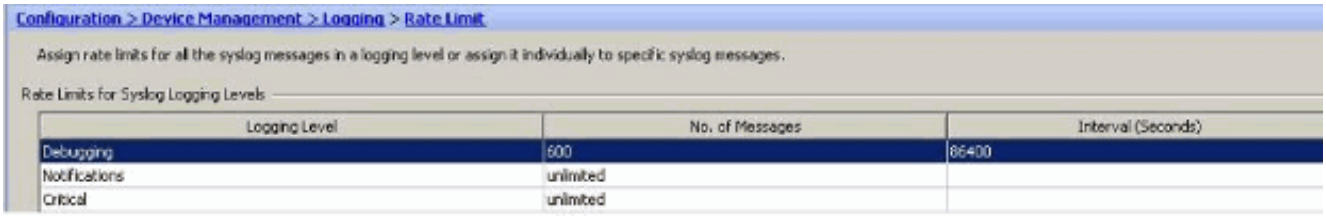
1. Choisissez la **configuration > la Gestion de périphériques > en se connectant > raté limit** et sélectionnez le niveau d'importance exigé. Puis, cliquez sur Edit.



2. Spécifiez nombre de messages à envoyer avec l'intervalle de temps. Cliquez sur **OK**.



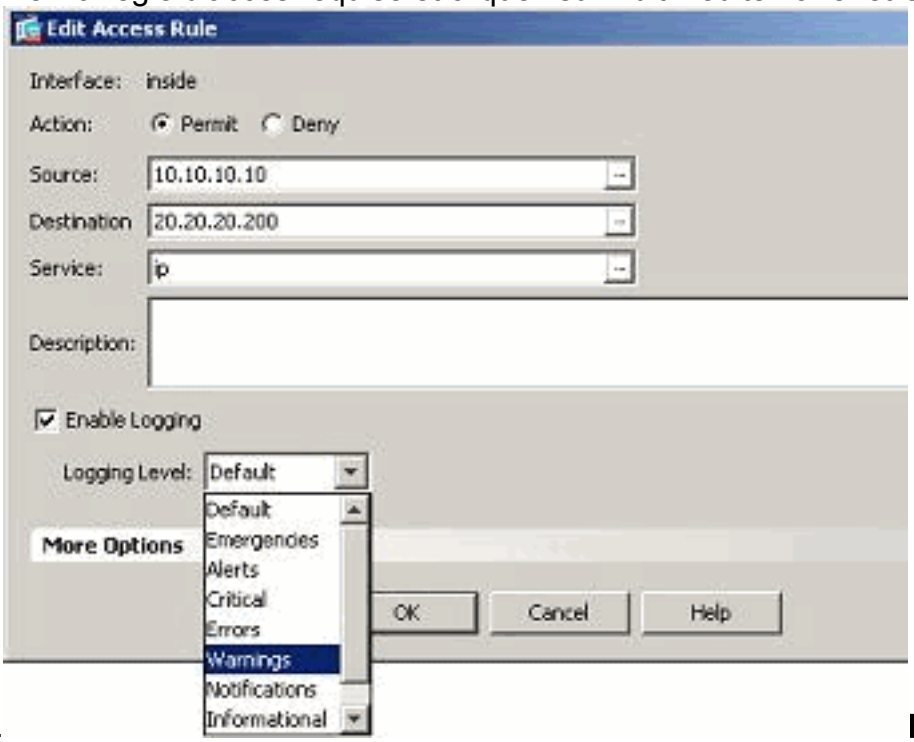
Remarque: Ces nombres sont indiqués comme exemple. Ceux-ci diffèrent selon le type d'environnement de réseau.Des valeurs modifiées sont vues ici :

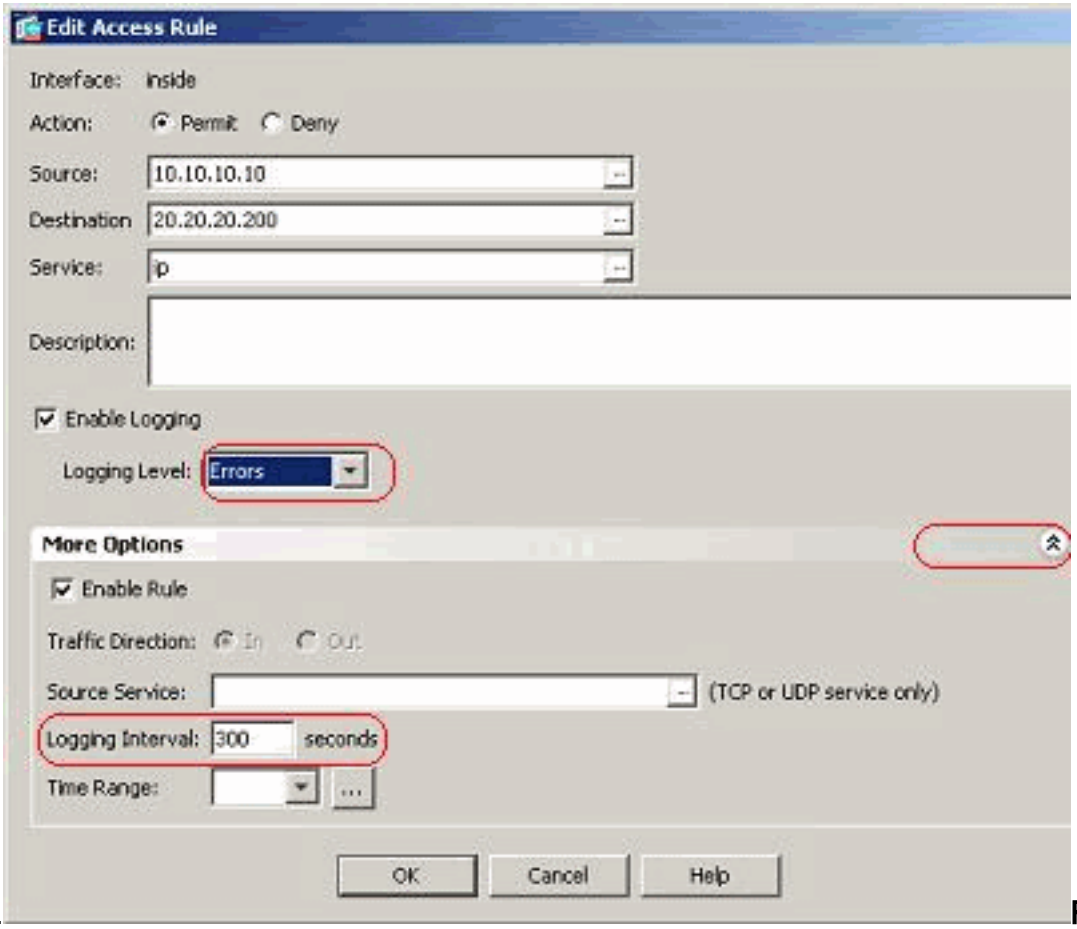


Se connecter les hit d'une règle d'accès

Vous pouvez se connecter les hit de règle d'accès utilisant l'ASDM. Le comportement se connectant par défaut est d'envoyer un message de Syslog pour tous les paquets refusés. Il n'y aura pas aucun message de Syslog pour les paquets permis et ceux-ci pas sont enregistré. Cependant, vous pouvez définir un niveau d'importance se connectant fait sur commande à la règle d'accès de dépister le compte des paquets qui frappe cette règle d'accès.

Effectuez les étapes suivantes :

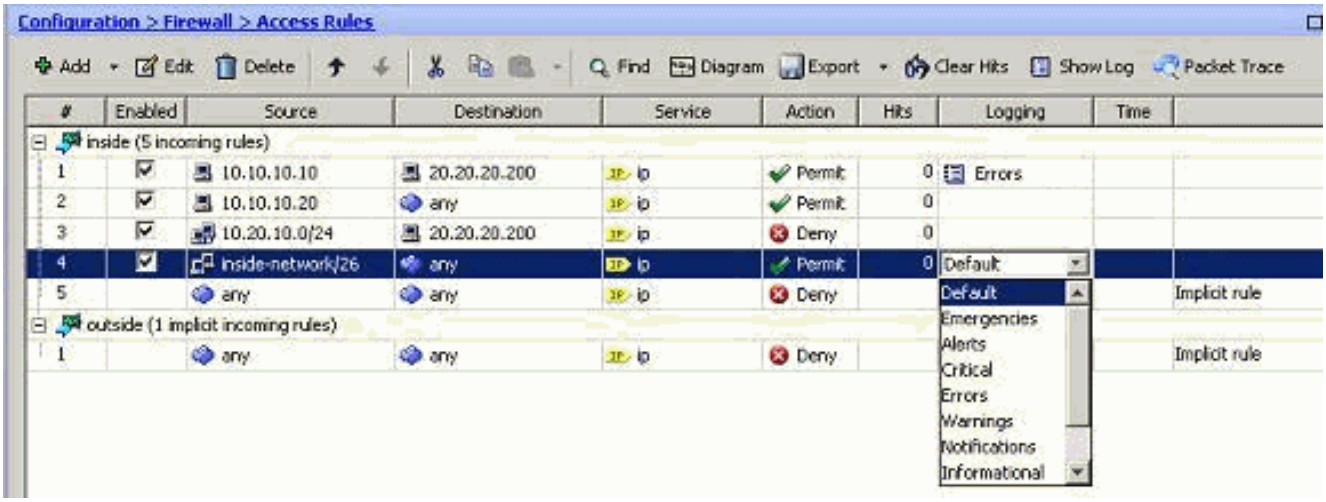
1. Sélectionnez la règle d'accès requise et cliquez sur Edit.*L'éditer la* fenêtre de *règle d'accès* apparaît. 

Remarque: Dans cette image, l'*option par défaut* dans le domaine *de niveau se connectant* indique le comportement se connectant par défaut de Cisco ASA. Pour plus d'informations sur ceci, référez-vous à la section [se connectante d'activité de liste d'accès].
2. Le coche l'*enable se connectant l'*option et spécifient le niveau d'importance exigé. Puis, cliquez sur OK. 

Remarque: En cliquant sur *plus d'*onglet de déroulant d'*options*, vous pouvez voir l'option *se connectante d'intervalle*. Cette option est mise en valeur seulement quand l'*enable* ci-dessus *se connectant l'*option est fait tic tac. La valeur par défaut de ce temporisateur est de 300

secondes. Cette configuration est utile en spécifiant la valeur du dépassement de durée pour que les écoulement-statistiques soient supprimées quand il n'y a aucune correspondance pour cette règle d'accès. S'il y a des hit, alors l'ASA attend jusqu'à l'intervalle se connectant et envoie cela au Syslog.

3. Les modifications sont affichées ici. Alternativement, vous pouvez double-cliquer le champ *se connectant de la* règle d'accès spécifique et placer le niveau d'importance là.



Remarque: Cette autre méthode de spécifier le *niveau se connectant* dans le même volet de *règles d'accès* en double-cliquer fonctionne pour seulement les entrées manuellement créées de règle d'accès, mais pas aux règles implicites.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

Ce document utilise les configurations suivantes :

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
```

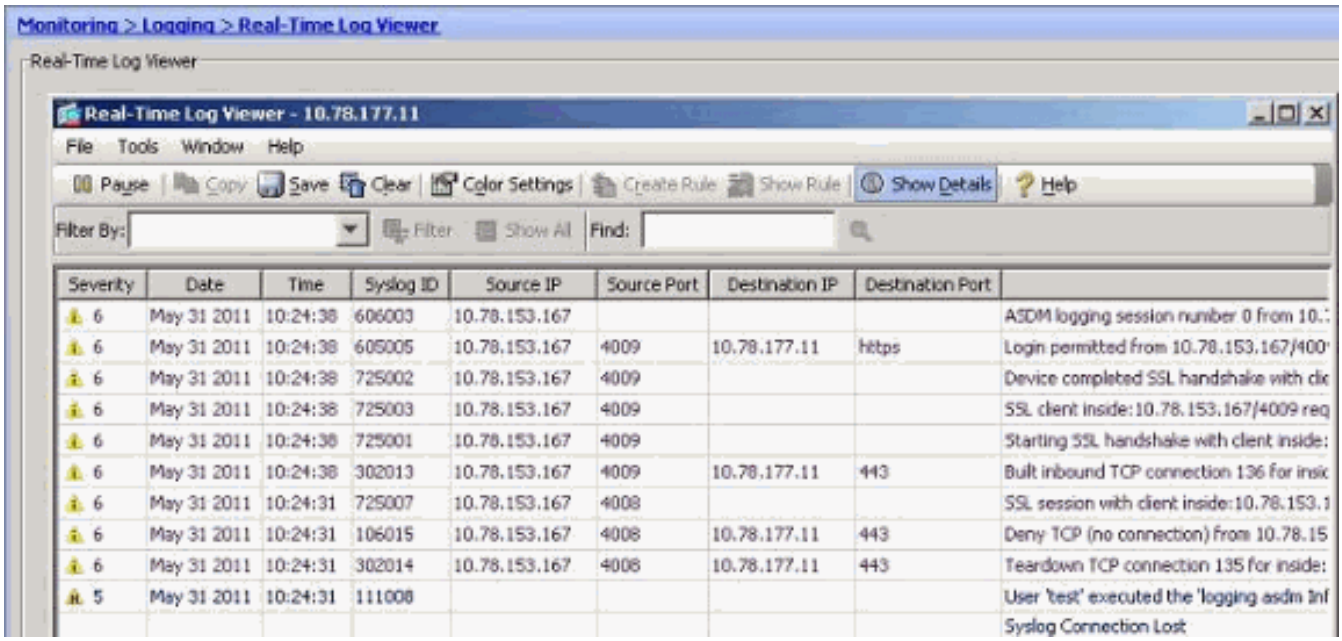
```
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.0
!
interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.78.177.11 255.255.255.192
!
!!--- Output Suppressed ! access-list inside_access_in
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors access-list 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
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- Vous pouvez visualiser les Syslog de l'ASDM. Choisissez le **Monitoring > Logging > Real-time Log Viewer**. Un résultat témoin est affiché ici
  :



Dépannez

Problème : Connexion perdue -- Connexion de Syslog terminée --

Cette erreur est reçue en tentant d'activer l'ASDM se connectant au tableau de bord de périphérique pour des contextes l'uns des.

```
« Connexion perdue -- Connexion de Syslog terminée --"
```

Quand l'ASDM est utilisé pour se connecter directement au contexte d'admin et se connecter ADSM est désactivé là, alors commutateur à se connecter de subcontext et d'enable ASDM. Les erreurs sont reçues, mais les messages de Syslog atteignent bien au serveur de Syslog.

Solution

C'est un comportement connu avec Cisco ASDM et a documenté dans l'ID de bogue Cisco CSCsd10699 (clients enregistrés seulement). Comme contournement, asdm d'enable se connectant une fois connecté dans le contexte d'admin.

Ne peut pas visualiser les logins Cisco ASDM de temps réel

Une question est que les logs en temps réel ne peuvent pas être visualisés sur l'ASDM. Comment est-ce que ceci est configuré ?

Solution

Configurez le suivant sur Cisco ASA :

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

Informations connexes

- Assistance des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems