

ASA 8.2: Syslog de la configuración usando el ASDM

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración de syslog básica usando el ASDM](#)

[Registro del permiso](#)

[Registro de la neutralización](#)

[Registro a un email](#)

[Registro a un servidor de Syslog](#)

[Configuración de syslog avanzada usando el ASDM](#)

[Trabajo con las Listas de eventos](#)

[Trabajo con los filtros del registro](#)

[Límite de velocidad](#)

[Registración de los golpes de una regla de acceso](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Problema: Conexión perdida -- Conexión del Syslog terminada --](#)

[Solución](#)

[No puede ver el tiempo real abre una sesión el ASDM de Cisco](#)

[Solución](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona la información sobre cómo configurar el Syslog en el dispositivo de seguridad adaptante de Cisco (ASA) 8.x usando el Administrador de dispositivos de seguridad adaptante (ASDM) GUI. Los mensajes del registro del sistema son los mensajes generados por Cisco ASA para notificar al administrador en cualquier cambio en la configuración, los cambios en configuración de la red, o los cambios en el funcionamiento del dispositivo. Analizando los mensajes del registro del sistema, un administrador puede resolver problemas fácilmente el error realizando una Análisis de la causa de raíz.

Los mensajes de Syslog principalmente se distinguen basados en su nivel de gravedad.

1. Gravedad 0 - Mensajes de emergencia - El recurso está inutilizable
 2. Gravedad 1 - Mensajes de alerta - La acción inmediata es necesaria
 3. Gravedad 2 - Mensajes críticos - Condiciones críticas
 4. Gravedad 3 - Mensajes de error - Condiciones de error
 5. Gravedad 4 - Mensajes de advertencia - Condiciones de advertencia
 6. Gravedad 5 - Mensajes de notificación - Normal pero estados significativos
 7. Gravedad 6 - Mensajes de información - Mensajes de información solamente
 8. Gravedad 7 - Mensajes de debugging - Mensajes de debugging solamente
- Nota:** El nivel de gravedad más alto es una emergencia y el nivel de gravedad más bajo está haciendo el debug de.

Los mensajes de Syslog de la muestra generados por Cisco ASA se muestran aquí:

- %ASA-6-106012: Niegue el IP de IP_address a IP_address, maleficio de las opciones IP.
- %ASA-3-211001: Error de asignación de memoria
- %ASA-5-335003: ACL predeterminado del NAC aplicado, ACL: ACL-nombre - host address

El valor numérico X especificado en "%ASA-X-YYYYYY: ", denota la gravedad del mensaje. Por ejemplo, el "%ASA-6-106012" es un mensaje de información y el "%ASA-5-335003" es un mensaje de error.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de ASA 8.2 de Cisco
- Cisco ASDM versión 6.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

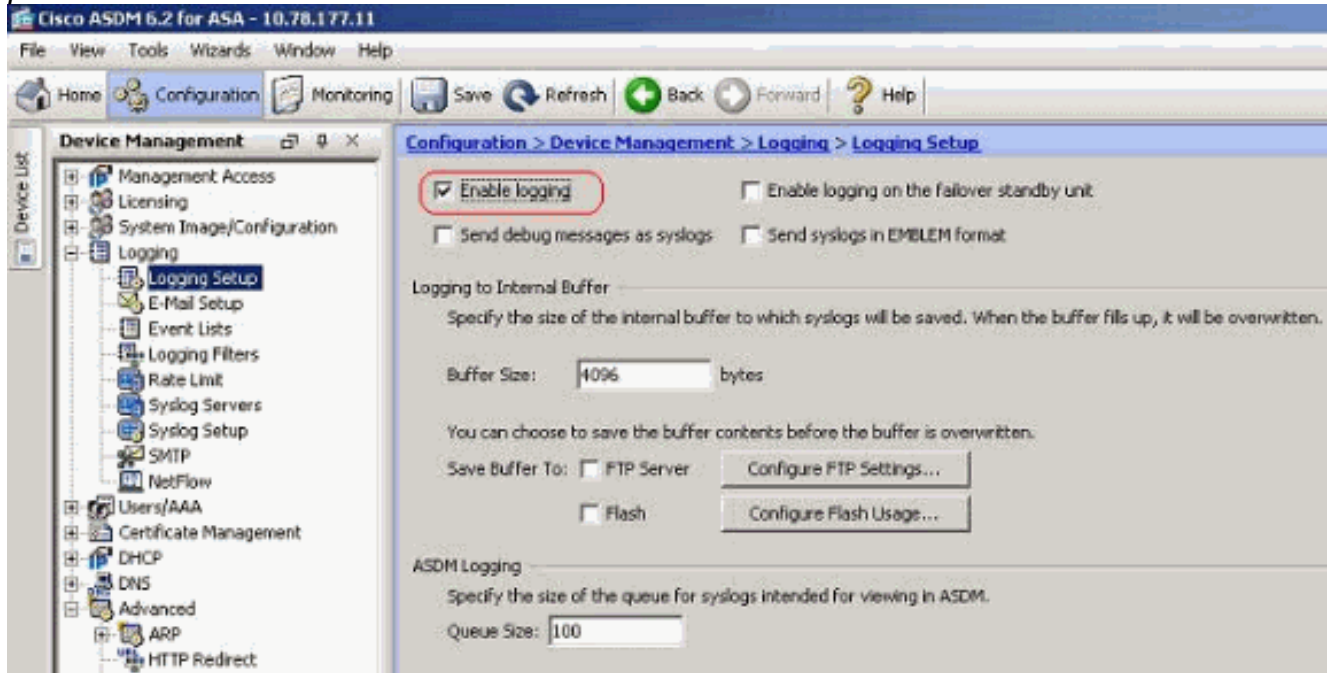
Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Configuración de syslog básica usando el ASDM

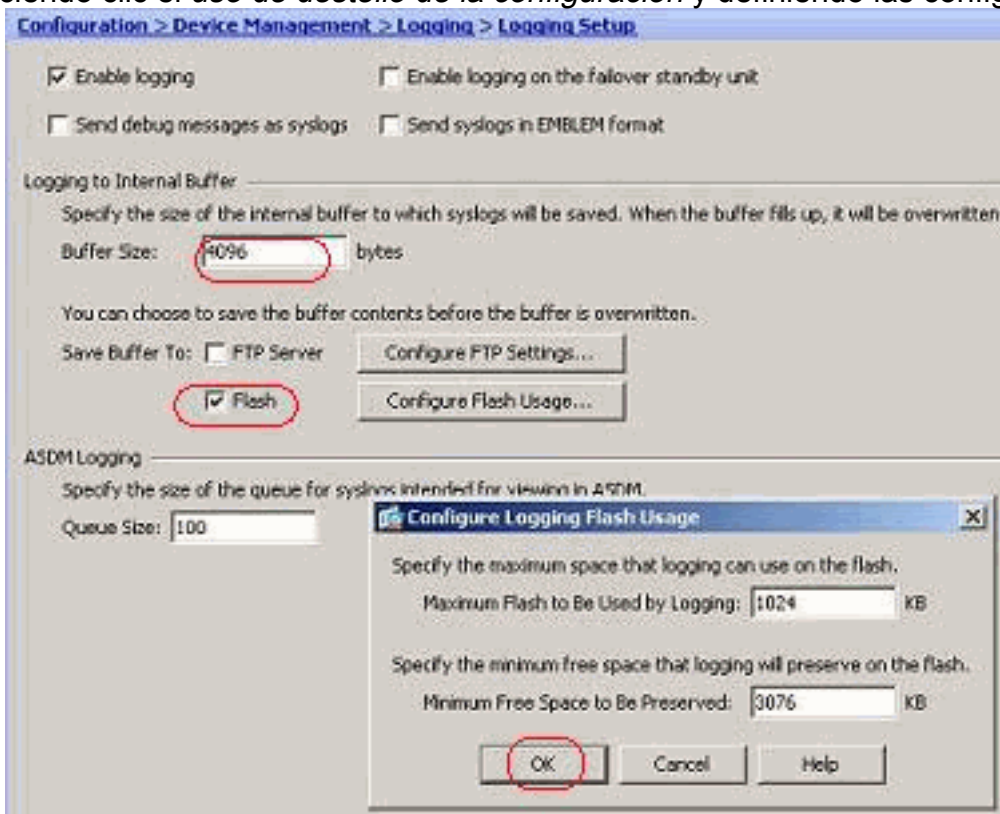
Registro del permiso

Complete estos pasos:

1. Elija la *configuración* > la *Administración de dispositivos* > el *registro* > el *registro puesto* y la marca de tilde la *opción de registro del permiso*.

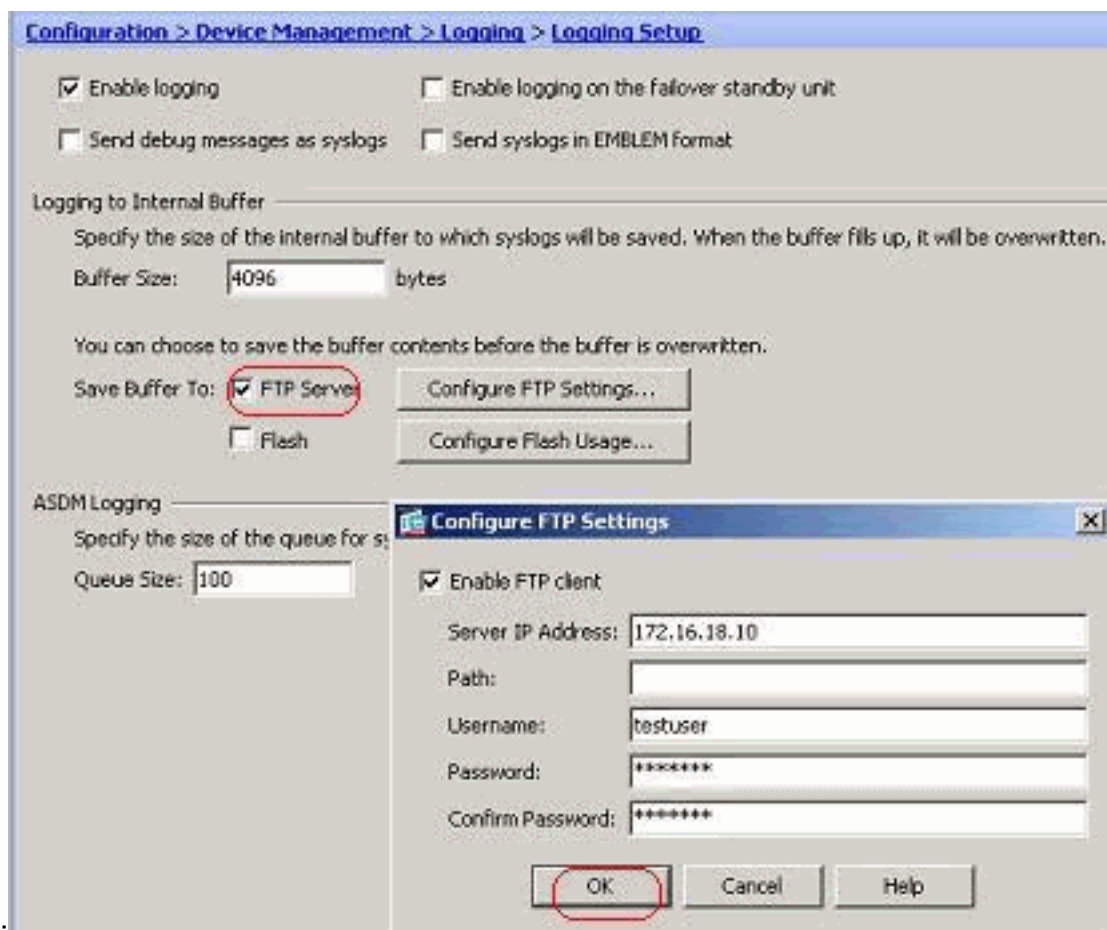


2. Usted puede registrar los mensajes de Syslog a un búfer interno especificando el tamaño de almacén intermedio. Usted puede también elegir salvar el contenido del buffer a memoria flash haciendo clic el *uso de destello de la configuración* y definiendo las configuraciones de



destello.

3. Los mensajes de registro guardado en memoria intermedia se pueden enviar a un servidor FTP antes de que estén sobregabados. Haga clic las *configuraciones de la configuración FTP* y especifique a los detalles del servidor FTP como se muestra



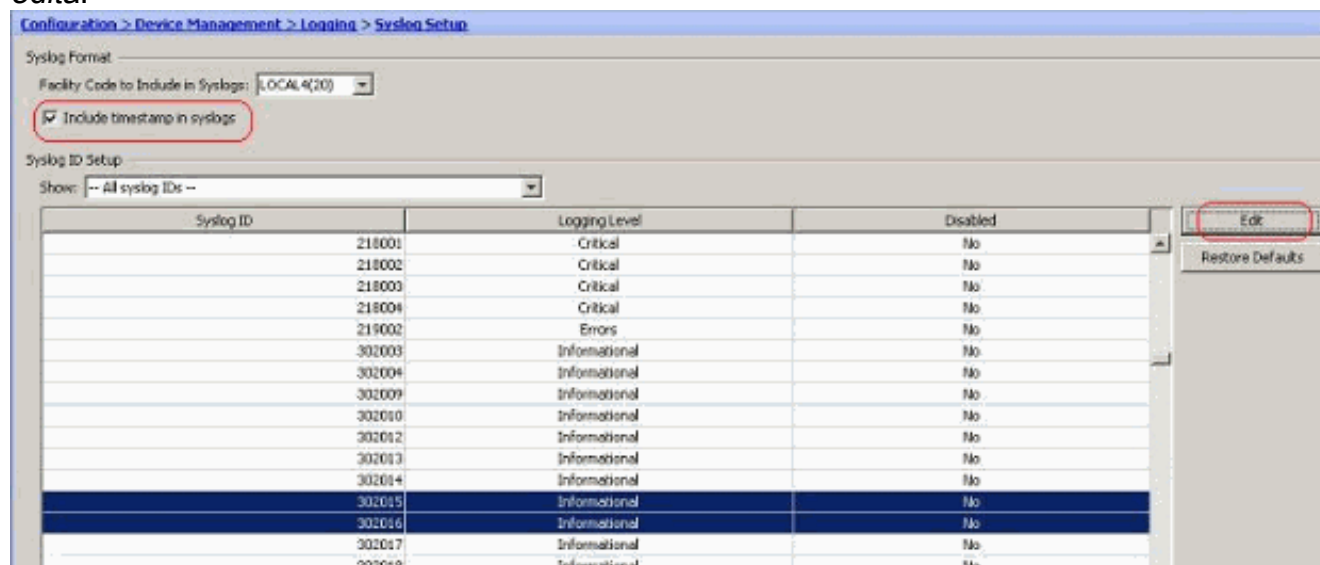
aquí:

Inhabilite el registro

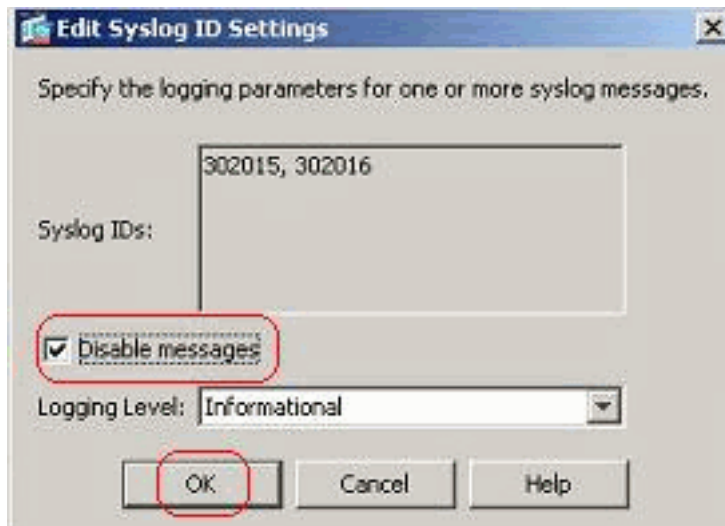
Usted puede inhabilitar los ID de syslogs específicos basados en su requisito.

Nota: Seleccionando la marca de tilde para el *grupo fecha/hora del incluido en la opción de los Syslog*, usted puede agregar la fecha y hora que fueron generados como campo a los Syslog.

1. Seleccione los Syslog para inhabilitar y el tecleo *edita*.

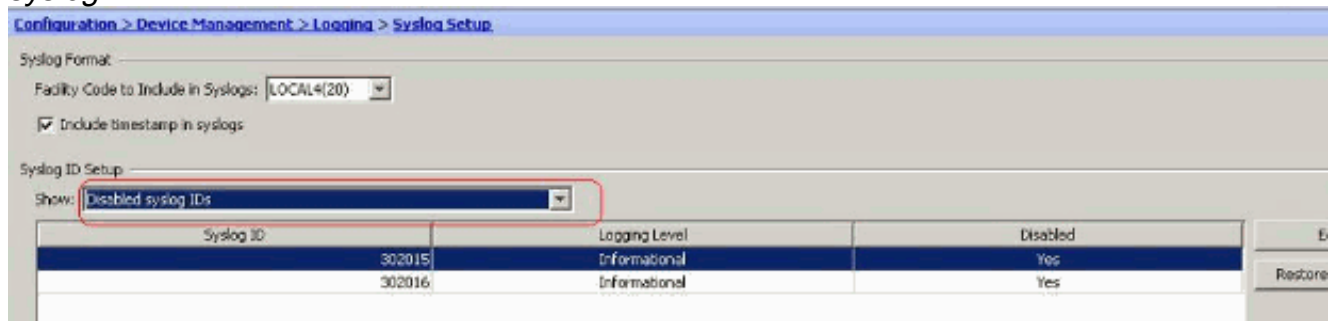


2. De la ventana de configuración del ID de syslog del editar, marca de tilde la **AUTORIZACIÓN** de la opción y del tecleo de los mensajes de la



neutralización.

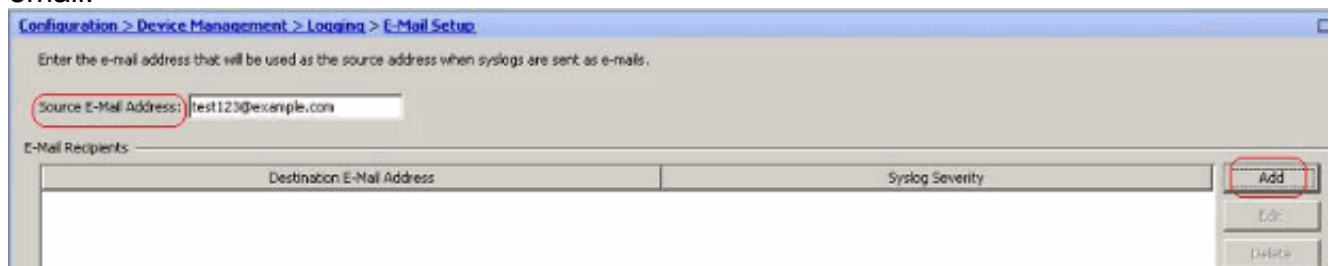
- Los Syslog discapacitados se pueden ver en una lengüeta separada seleccionando los *ID de syslogs inhabilitados* del menú desplegable de la configuración del ID de syslog.



Registro a un email

Complete estos pasos usando el ASDM para enviar los Syslog a un email:

- Elija la *configuración > la Administración de dispositivos > la configuración del registro > del email*. El campo de la *dirección de correo electrónico de la fuente* es útil en la asignación de un email ID como la fuente para los Syslog. Especifique la dirección de correo electrónico de la fuente. Ahora, el tecleo *agrega* para agregar a los beneficiarios del email.



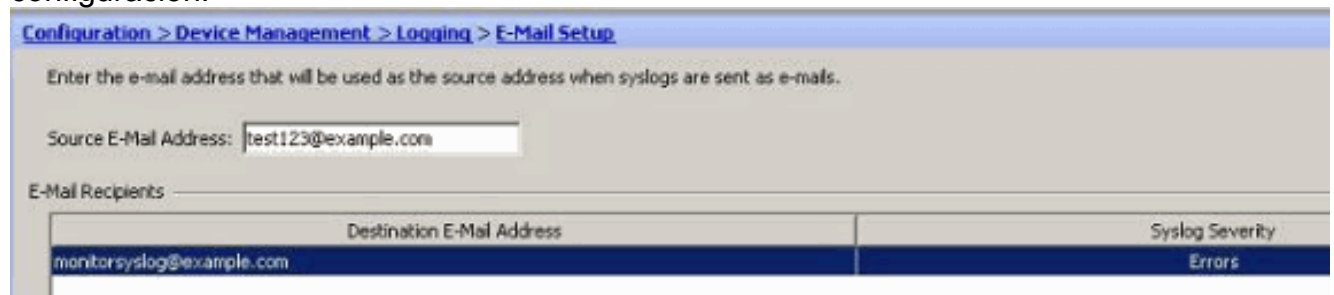
- Especifique la *dirección de correo electrónico del destino* y elija el *nivel de gravedad*. De acuerdo con los niveles de gravedad, usted puede definir a diversos beneficiarios del email. El Haga Click en OK a volver de nuevo al *email puso el*



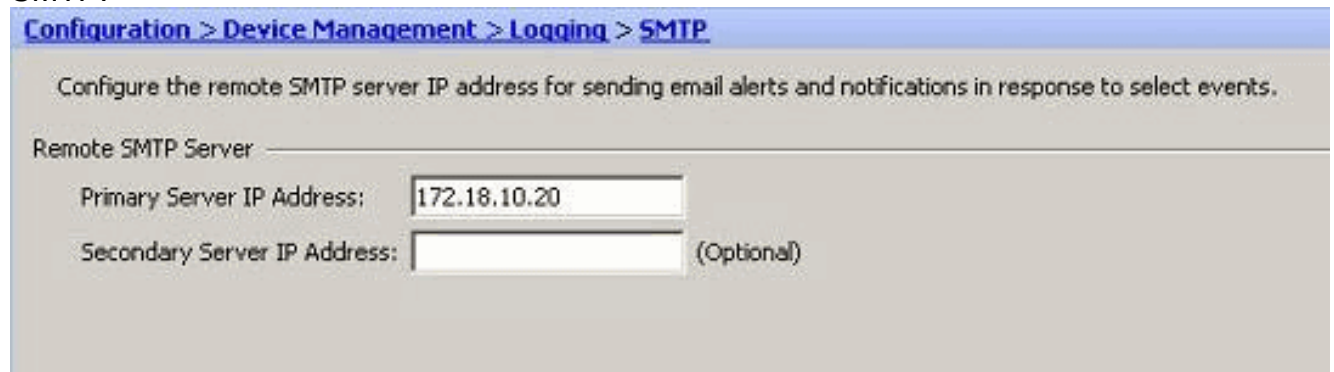
cristal.

configuración:

Esto da lugar a esta



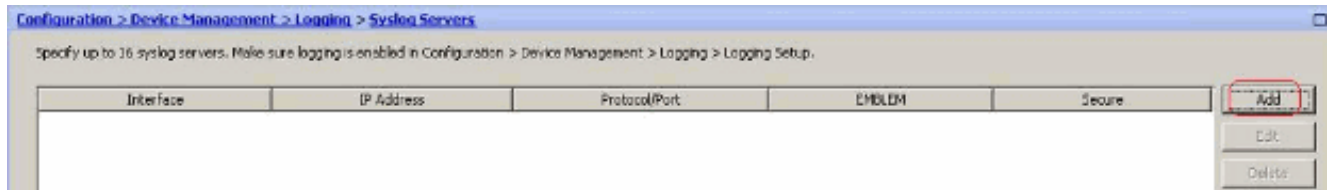
3. Elija la *configuración > la configuración > el registro > el SMTP de dispositivo* y especifique al servidor SMTP.



[Registro a un servidor de Syslog](#)

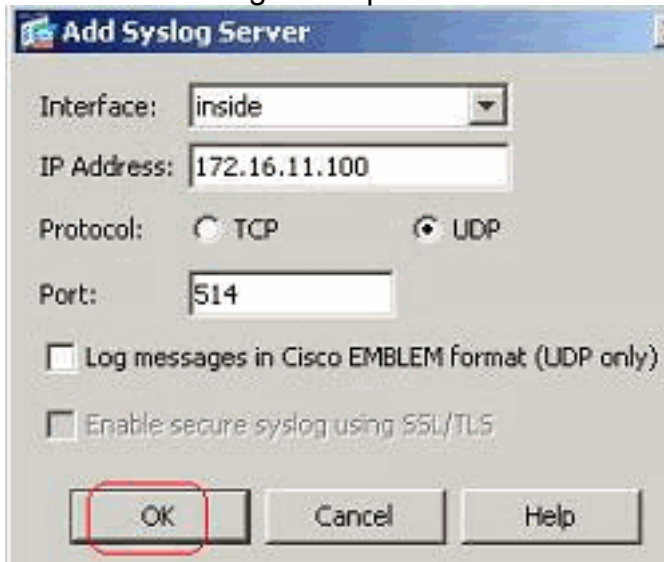
Usted puede enviar todos los mensajes de Syslog a un servidor de Syslog dedicado. Realice estos pasos usando el ASDM:

1. Elija la *configuración > la Administración de dispositivos > el registro > a los servidores de Syslog* y el tecleo *agrega* para agregar a un servidor de Syslog.



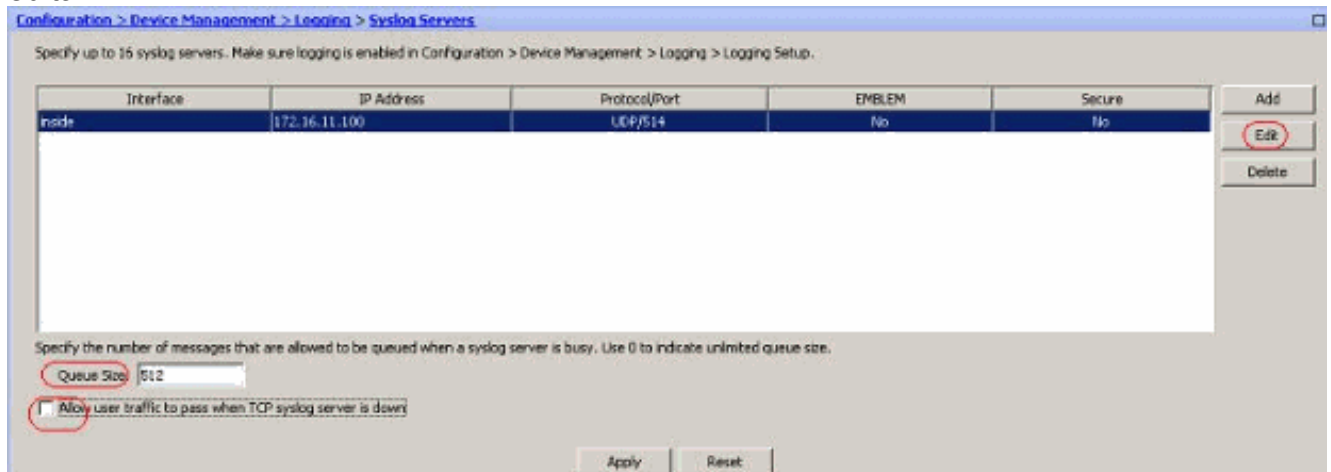
La ventana del servidor de Syslog del agregar aparece.

2. Especifique la interfaz que el servidor está asociado junto con a la dirección IP. Especifique el protocolo y a los puertos detalles dependiendo de su configuración de la red. Entonces, **AUTORIZACIÓN** del teclado. **Nota:** Asegúrese que usted tiene accesibilidad al servidor de



Syslog de Cisco ASA.

3. Ven al servidor de Syslog configurado como se muestra aquí. Las modificaciones se pueden hacer cuando usted selecciona este servidor, después hacen clic *editan*.



Nota: Marca de tilde el tráfico de usuarios de la permit a pasar cuando el servidor de Syslog TCP está abajo de opción. Si no, las sesiones de usuario nuevo se niegan con el ASA. Esto es aplicable solamente cuando el Transport Protocol entre el ASA y el servidor de Syslog es TCP. Por abandono, las nuevas sesiones del acceso a la red son negadas por Cisco ASA cuando un servidor de Syslog está abajo por cualquier motivo. Para definir el tipo de mensajes de Syslog que deban ser enviados al servidor de Syslog, vea la sección del [filtro del registro](#).

[Configuración de syslog avanzada usando el ASDM](#)

[Trabajo con las Listas de eventos](#)

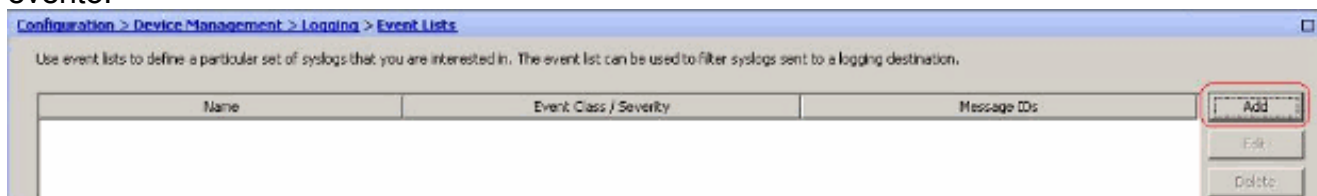
Las Listas de eventos nos permiten para crear las listas personalizadas que contienen el grupo de mensajes de Syslog que deban ser enviados a un destino. Las Listas de eventos se pueden crear en tres maneras diferentes:

- ID del mensaje o rango de los ID del mensaje
- Gravedad del mensaje
- Clase de mensaje

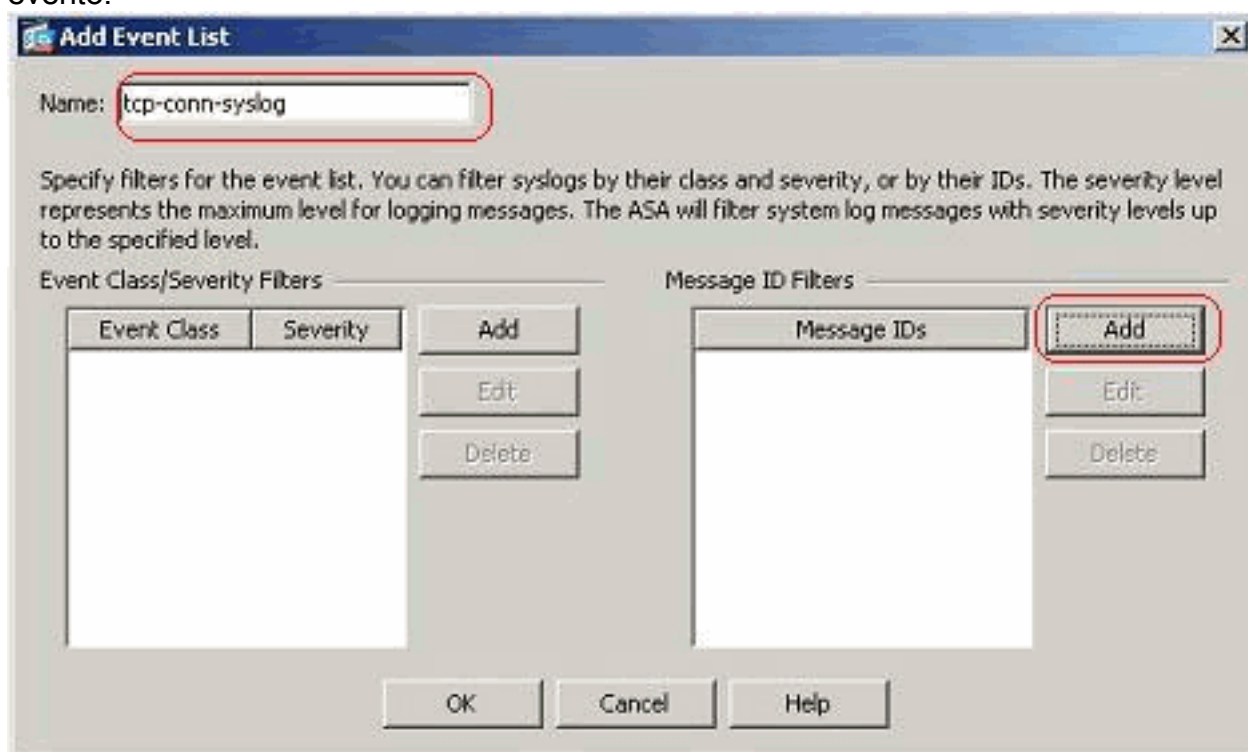
ID del mensaje o rango de los ID del mensaje

Siga estos pasos:

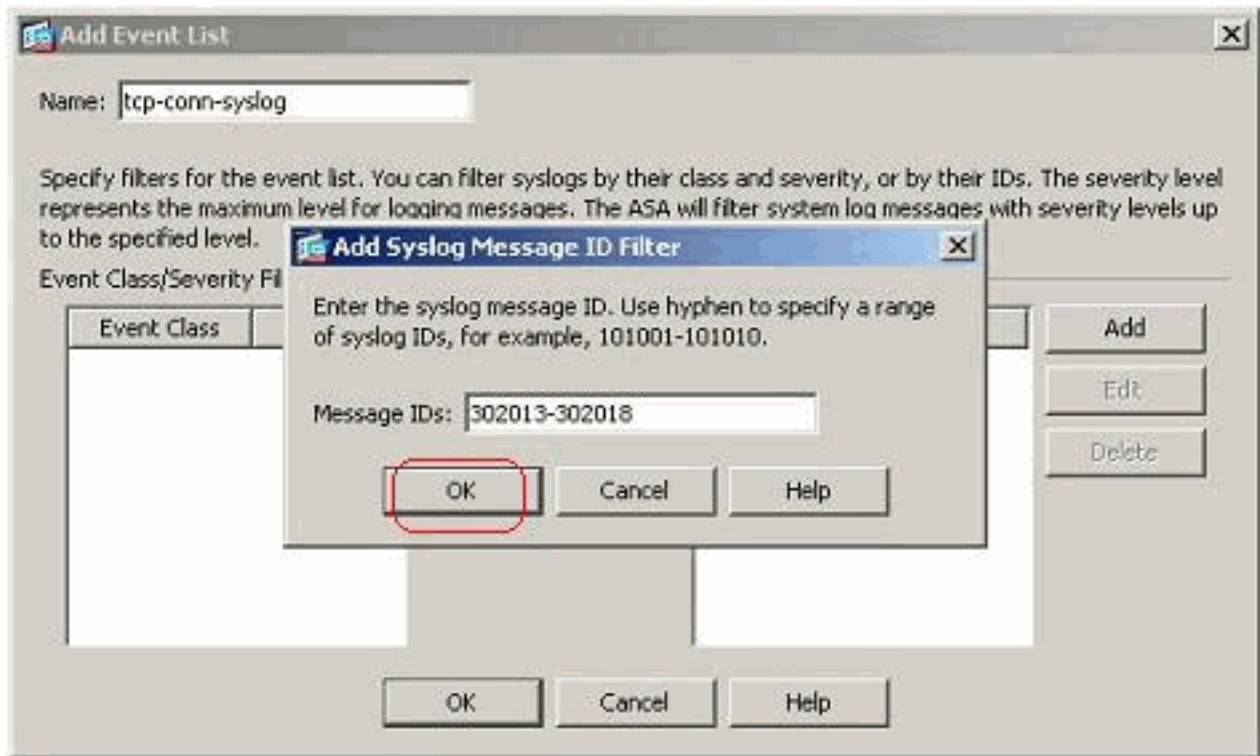
1. Elija la *configuración > la Administración de dispositivos > el registro > las Listas de eventos* y el tecleo *agrega* para crear una lista del nuevo evento.



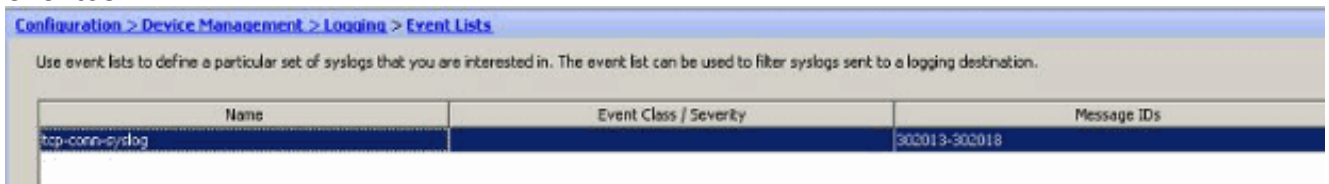
2. Especifique un nombre en el *campo de nombre*. El tecleo *agrega* en el cristal de los *filtros del ID del mensaje* para crear una lista del nuevo evento.



3. Especifique el rango del mensaje de Syslog ID. Aquí los mensajes de Syslog TCP han tomado por ejemplo. Haga Click en OK a completar.

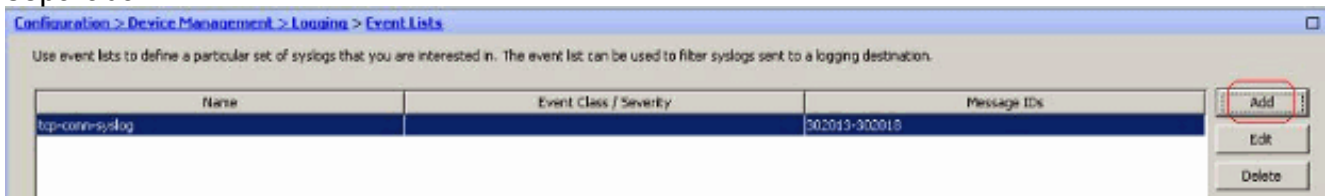


4. Haga Click en OK otra vez para invertir de nuevo a la ventana de las *Listas de eventos*.

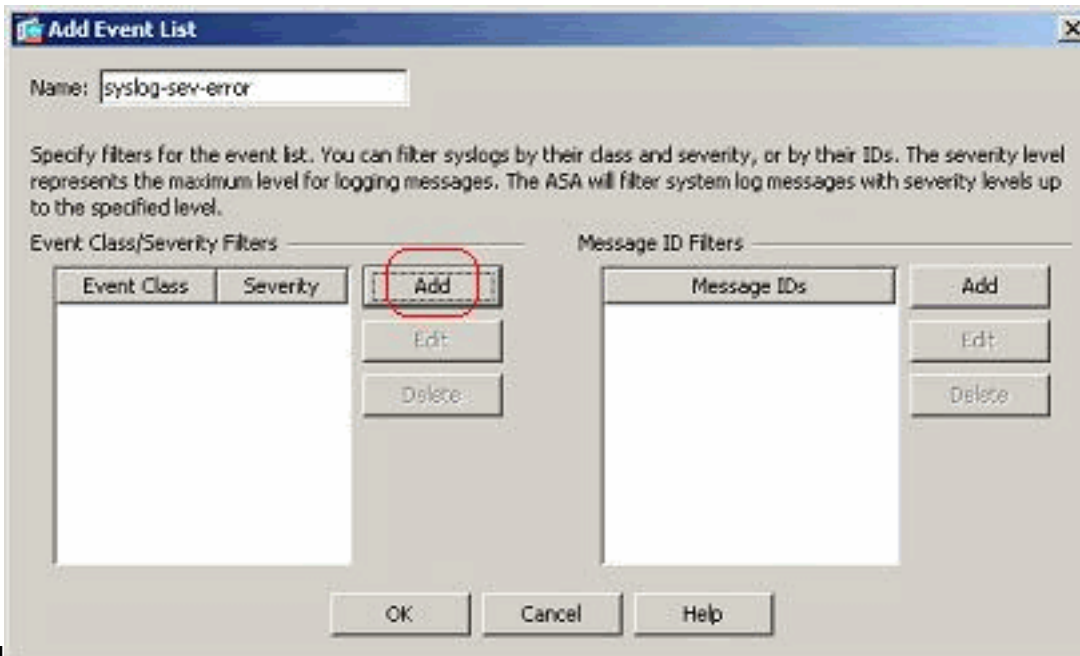


Gravedad del mensaje

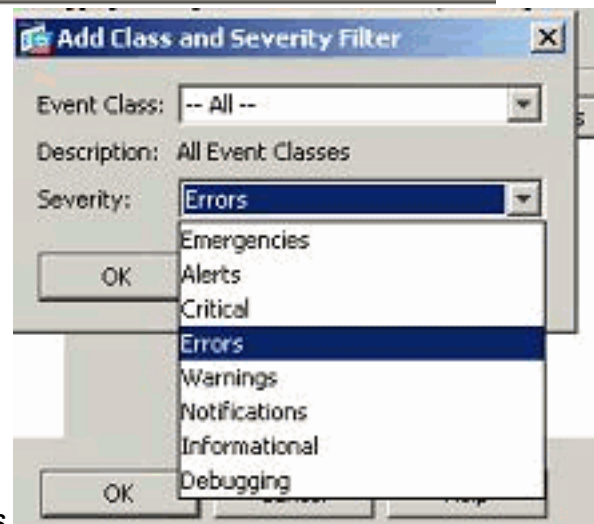
1. Las Listas de eventos se pueden también definir sobre la base de la gravedad del mensaje. El teclado *agrega* para crear una Lista de eventos separada.



2. Especifique el nombre y el haga click en

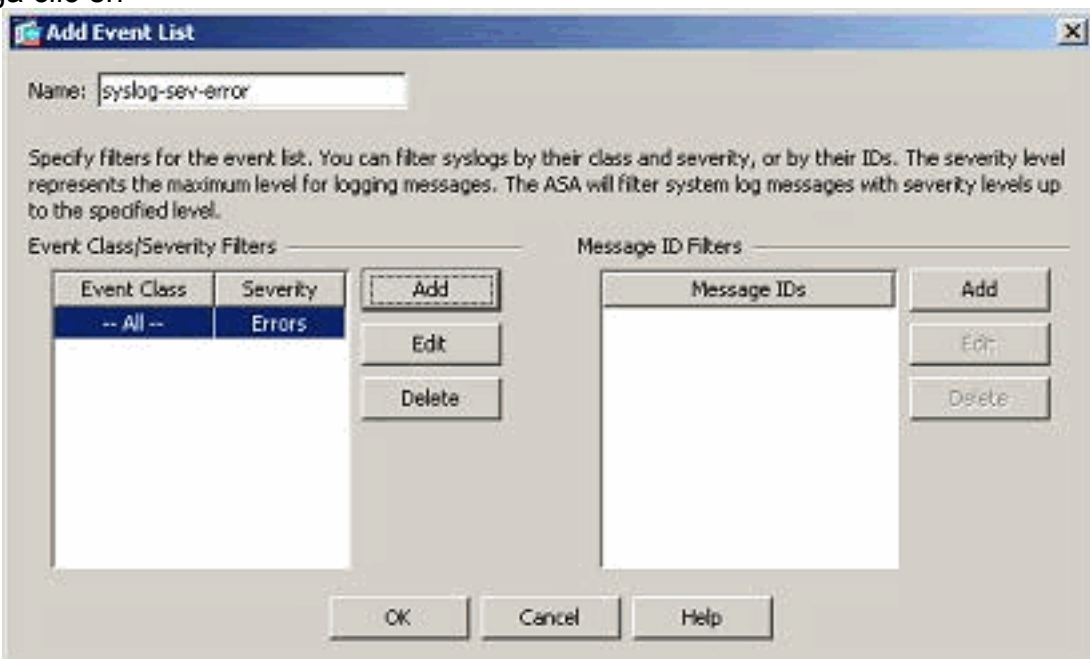


Add



3. Seleccione el nivel de gravedad como *errores*.

4. Haga clic en



OK.

Clase de mensaje

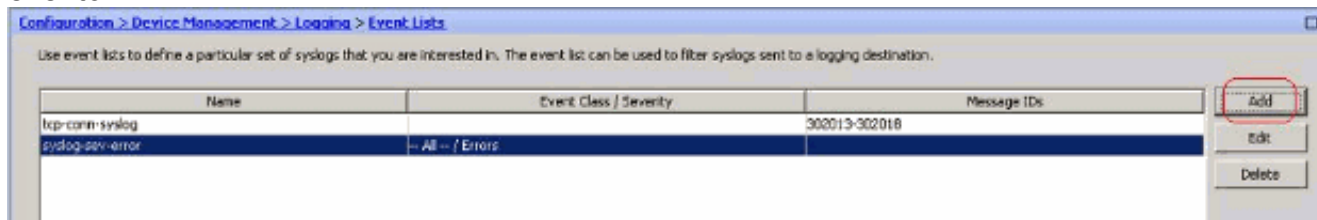
Las Listas de eventos también se configuran sobre la base de la clase de mensaje. Una clase de

mensaje es un grupo de mensajes de Syslog relacionados con una característica del dispositivo de seguridad que le permita para especificar una clase entera de mensajes en vez de especificar una clase para cada mensaje individualmente. Por ejemplo, utilice la clase del auth para seleccionar todos los mensajes de Syslog que se relacionen con la autenticación de usuario. Algunas clases de mensajes disponibles se muestran aquí:

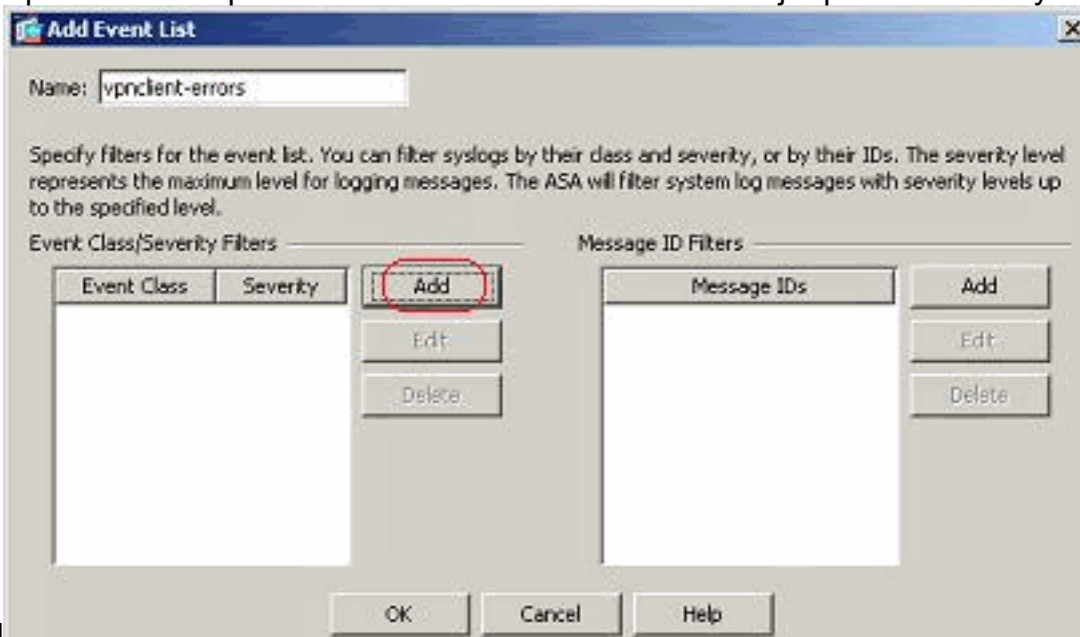
- Todos — Todas las clases de evento
- auth — Autenticación de usuario
- Bridge — Firewall transparente
- Ca — Autoridades de certificación PKI
- interfaz del comando config
- ha — Conmutación por falla
- IPS — Servicio de protección contra intrusos
- IP — Pila IP
- NP — Procesador de red
- OSPF — OSPF Routing
- RIP — El rutear del RIP
- sesión de usuario de sesión

Realice estos pasos para crear una clase de evento basada en la clase de mensaje de los *vpnclient-errores*. La clase de mensaje, *vpnc*, está disponible categorizar todos los mensajes de Syslog relacionados con el *vpnclient*. El nivel de gravedad para esta clase de mensaje se elige como “errores”.

1. El teclado agrega para crear una lista del nuevo evento.

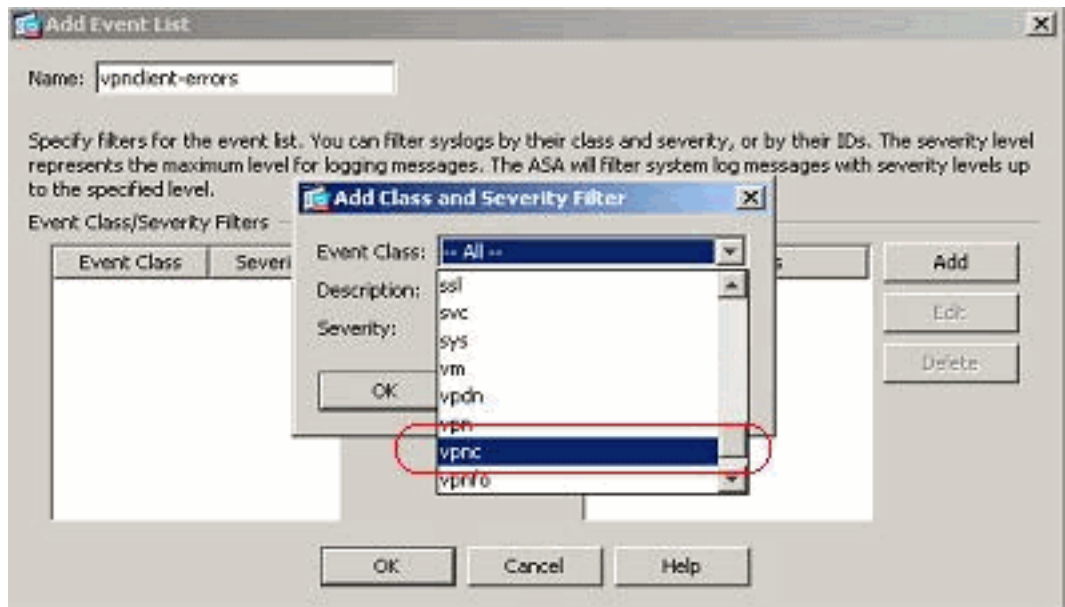


2. Especifique el nombre para ser relevante a la clase de mensaje que usted crea y haga click



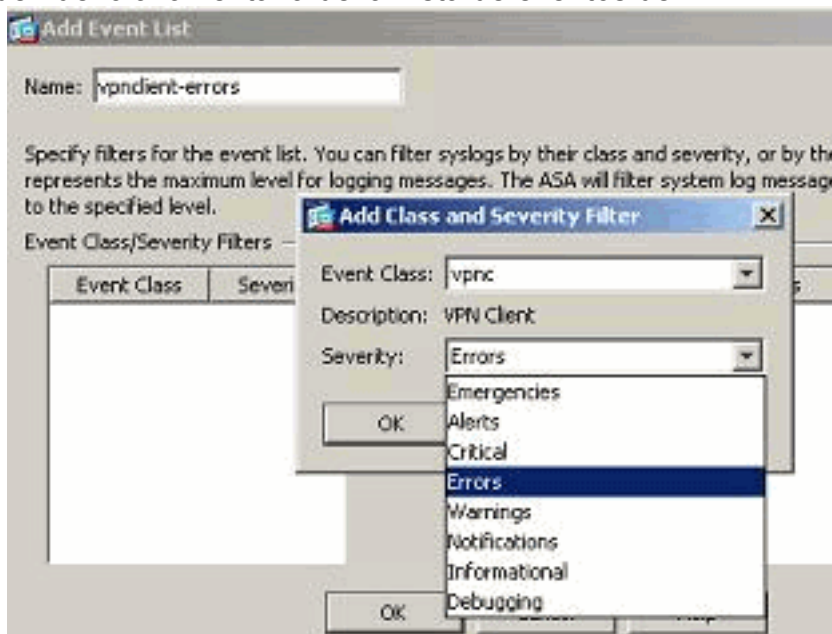
en Add

3. Seleccione el *vpnc* de la lista



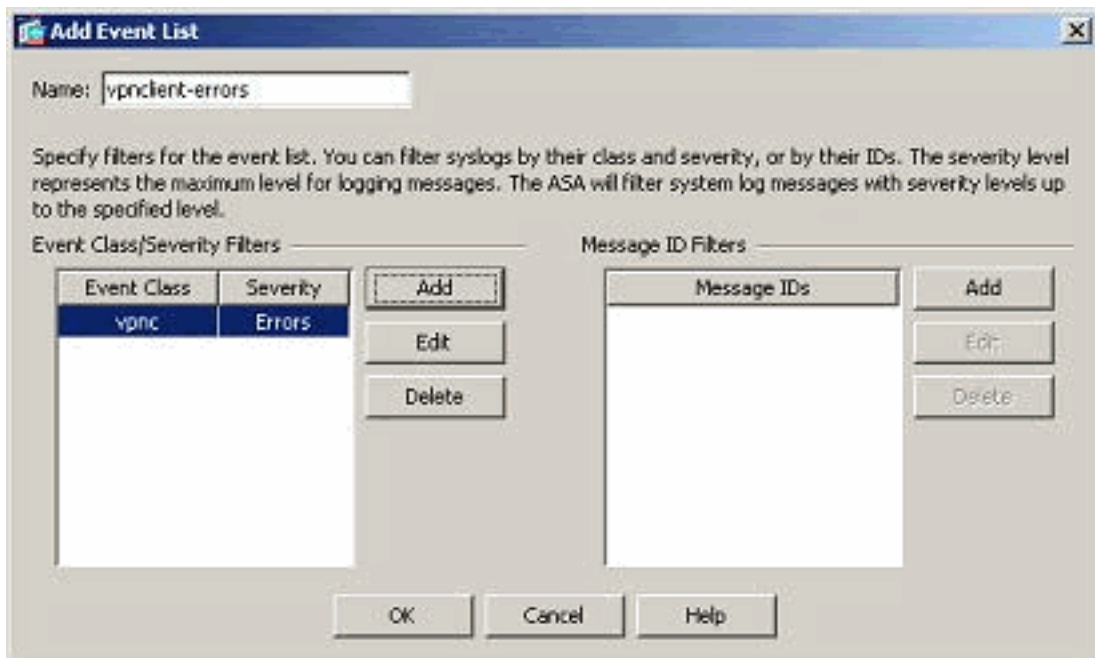
desplegable.

4. Seleccione el nivel de gravedad como *errores*. Este nivel de gravedad es aplicable para esos mensajes que se registren para esta clase de mensaje solamente. Haga Click en OK a invertir de nuevo a la ventana de la Lista de eventos del



agregar.

5. La clase de evento/la gravedad se muestra aquí. Haga Click en OK a completar configurando la Lista de eventos de los "vpnclient-



errores”.

Tambi

én se muestra en el tiro de siguiente pantalla que una lista del nuevo evento, el “usuario-auth-Syslog”, se crea con una clase de mensaje como “auth” y el nivel de gravedad para los Syslog de esta clase de mensaje específica como “advertencias”. Configurando esto, la Lista de eventos especifica todos los mensajes de Syslog que se relacionan con la clase de mensaje del “auth”, con los niveles de gravedad **hasta el** nivel de las “advertencias”. **Nota:** Aquí, el término “hasta” está de significación. Al denotar el nivel de gravedad, tenga presente que todos los mensajes de Syslog serán registrados hasta que ese nivel. **Nota:** Una Lista de eventos puede contener las clases de eventos múltiples. La Lista de eventos de los “vpncient-errores” es modificada haciendo clic **edita** y definiendo una clase de nuevo evento “SSL/error”.

Configuration > Device Management > Logging > Event Lists

Use event lists to define a particular set of syslogs that you are interested in. The event list can be used to filter syslogs sent to a logging destination.

Name	Event Class / Severity	Message IDs
tcp-conn-syslog		302013-302018
syslog-sev-error	-- All -- / Errors	
vpncient-errors	vpnc / Errors	
user-auth-syslog	auth / Warnings	

Trabajo con los filtros del registro

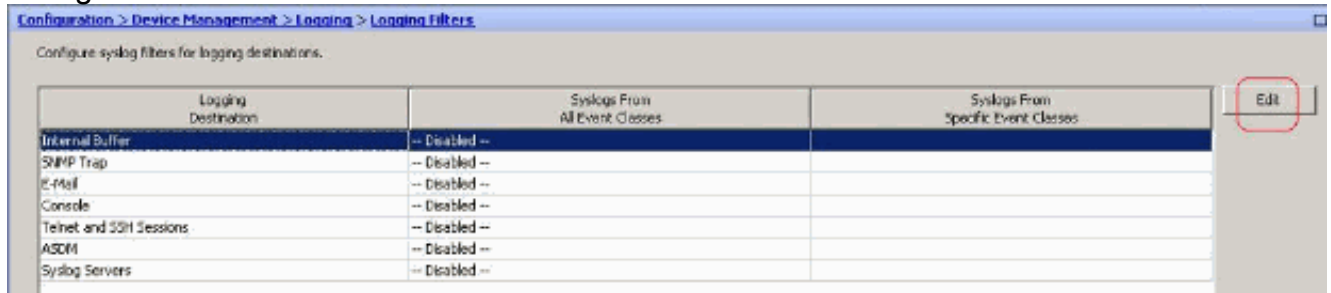
Los filtros de registración se utilizan para enviar los mensajes de Syslog a un destino especificado. Estos mensajes de Syslog se pueden basar en la “gravedad” o “incluso enumera”.

Éstos son los tipos de destinos a los cuales estos filtros sean aplicables:

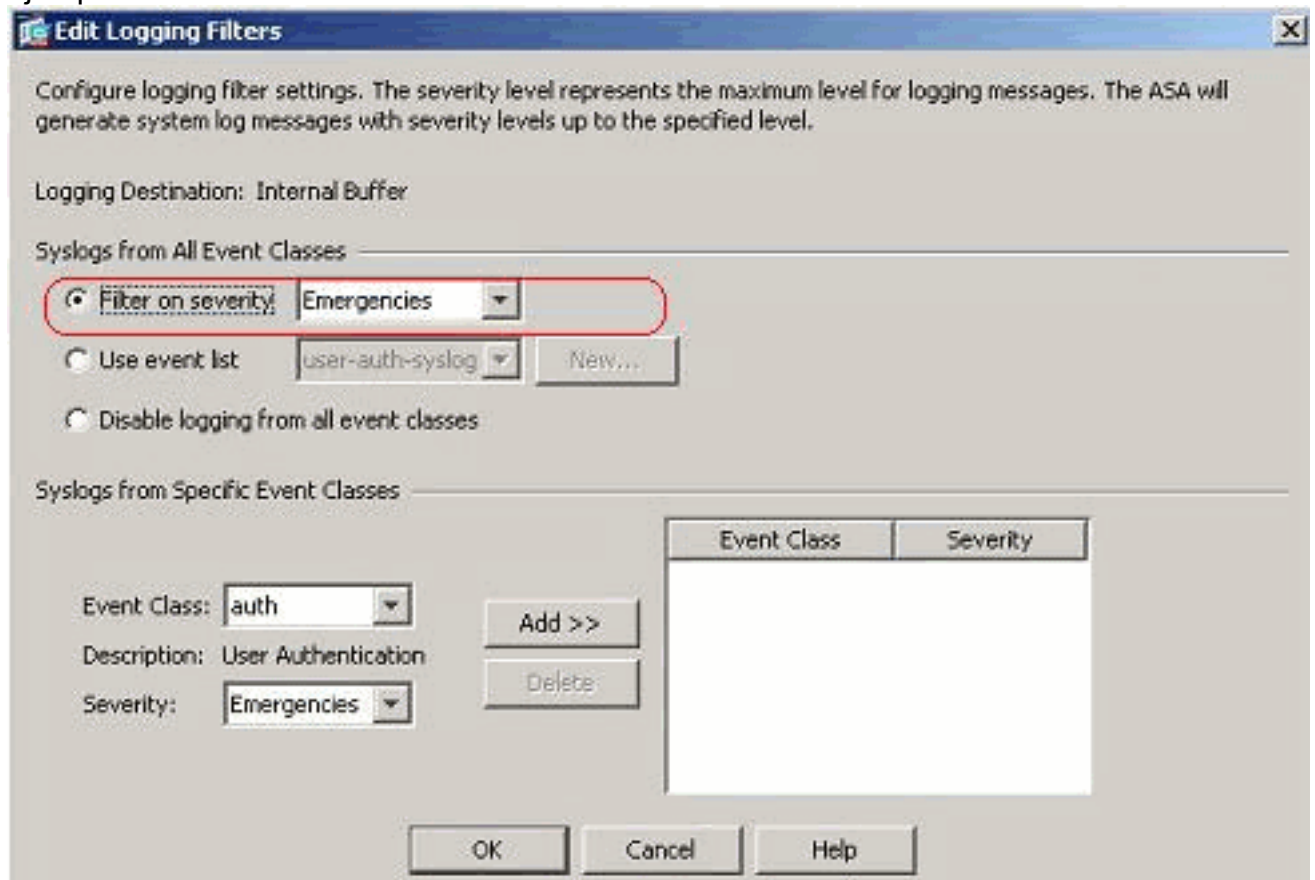
- Búfer interno
- SNMP trap
- Correo electrónico
- Consola
- Sesiones telnets
- ASDM
- Servidores de Syslog

Siga estos pasos:

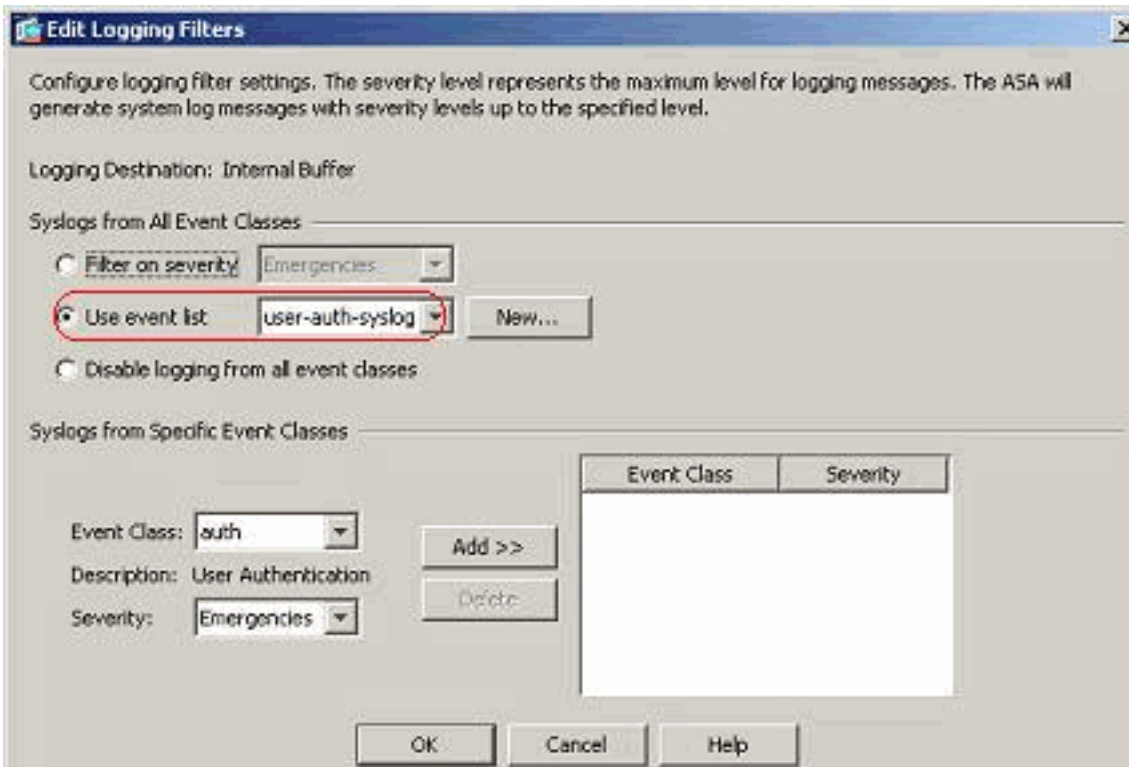
1. Elija la configuración > la Administración de dispositivos > el registro > los filtros del registro y seleccione el destino de registro. Entonces, el tecleo **edita** para modificar las configuraciones.



2. Usted puede enviar los mensajes de Syslog basados en la gravedad. Aquí, las **emergencias** se han seleccionado para mostrar como un ejemplo.

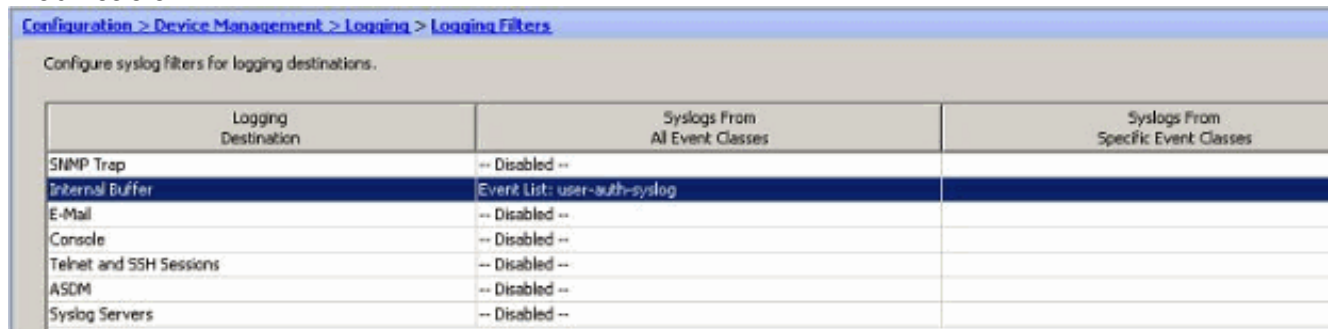


3. Una Lista de eventos se puede también seleccionar especificar qué tipo de mensaje debe ser enviado a un destino determinado. Haga clic en



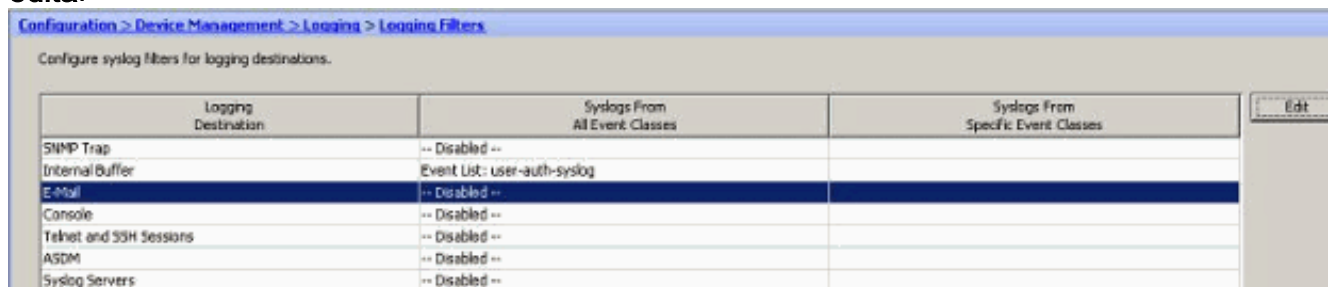
OK.

4. Verifique la modificación.

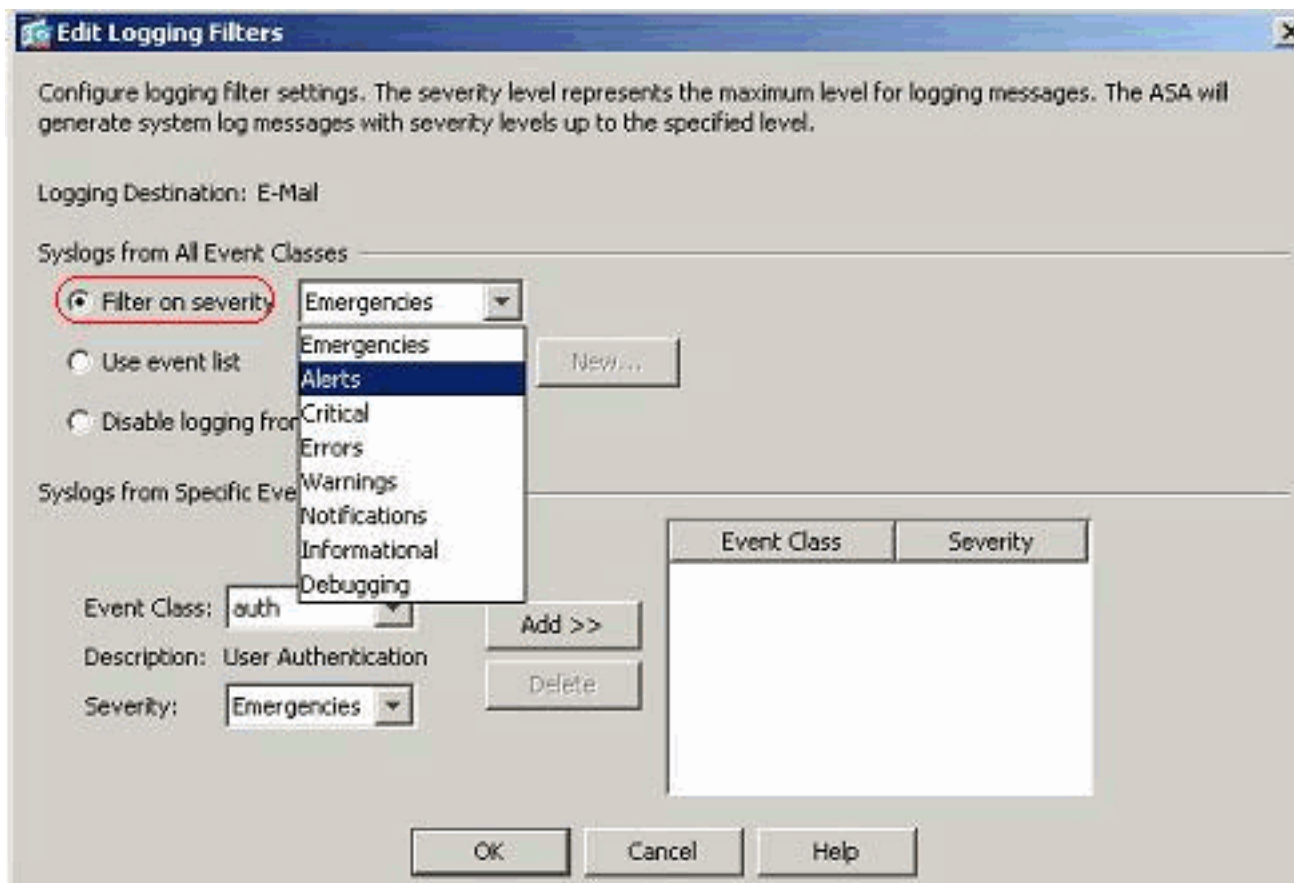


Éstos son los pasos en cómo enviar un grupo de mensajes (basados en su nivel de gravedad) al servidor del email.

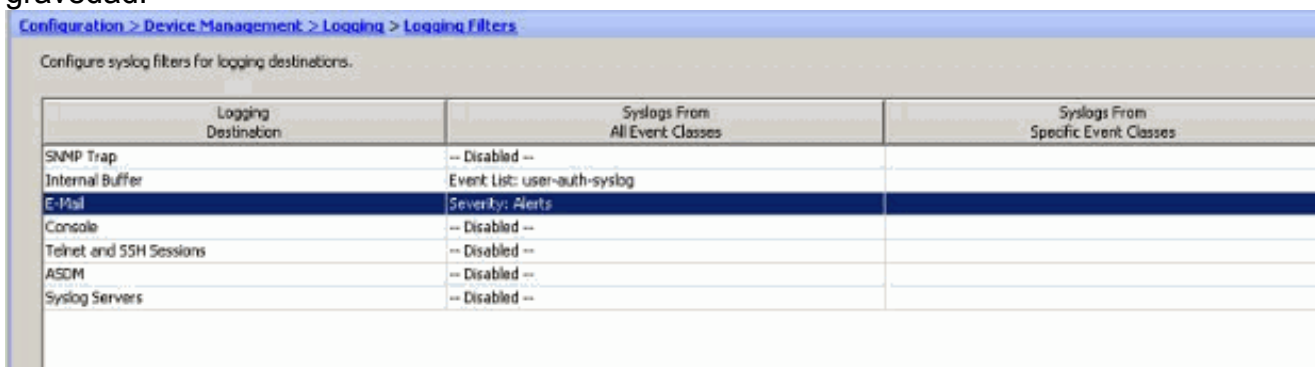
1. Seleccione el **email** en el campo de destino de registro. Entonces, el tecleo **edita**.



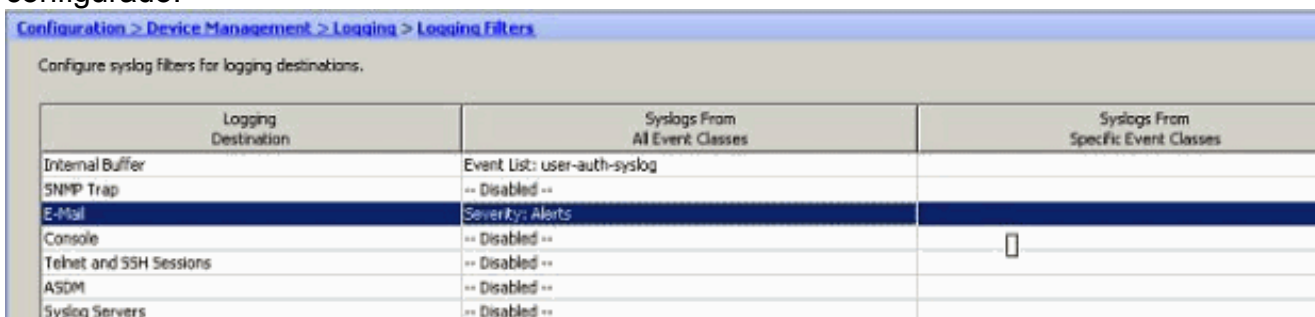
2. Elija el **filtro** en la opción de la **gravedad** y seleccione el nivel de gravedad requerido.



quí, las **alertas** se han seleccionado como el nivel de gravedad.



Usted puede ver que todos los mensajes de Syslog alertas deben ser enviados al email configurado.

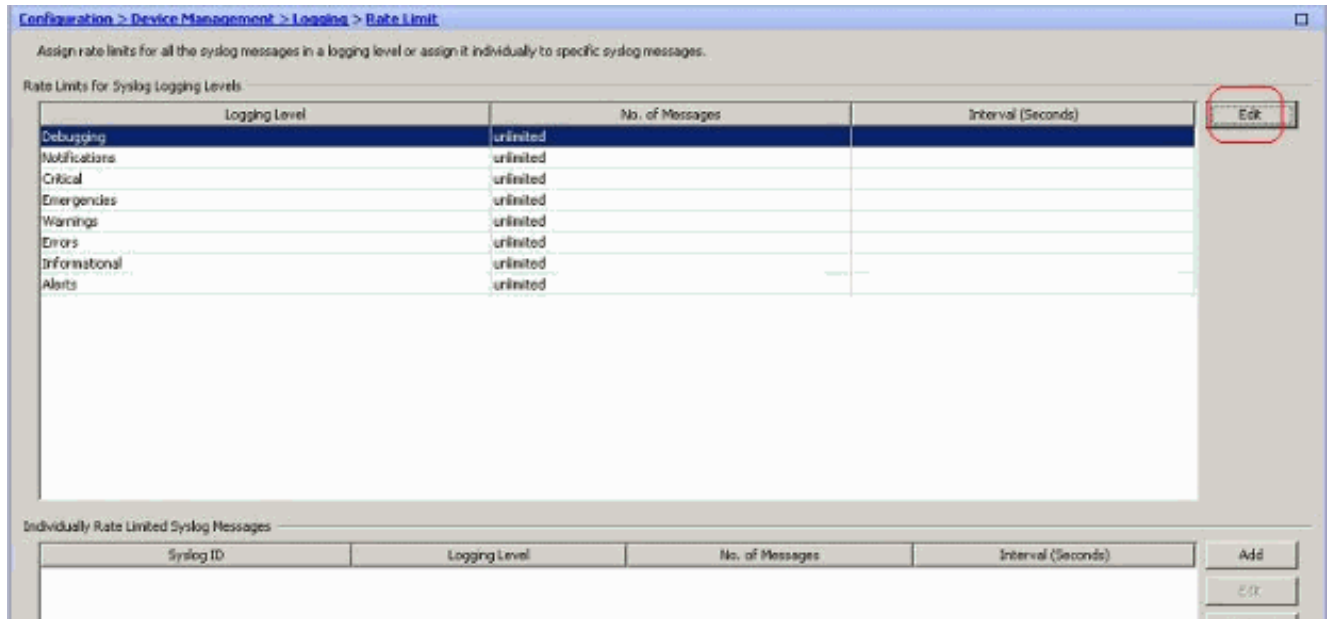


Límite de velocidad

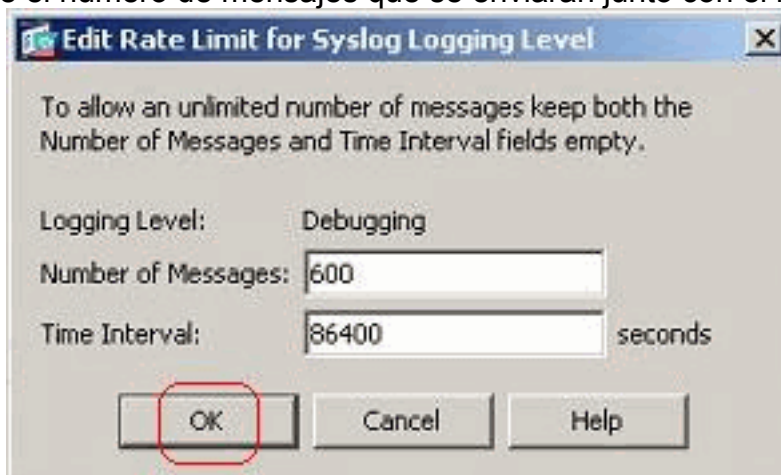
Esto especifica el número de mensajes de Syslog que Cisco ASA envíe a un destino en un periodo de tiempo especificado. Se define generalmente para el nivel de gravedad.

1. Elija la configuración > la Administración de dispositivos > el registro > el límite de velocidad

y seleccione el nivel de gravedad requerido. Entonces, el tecleo edita.



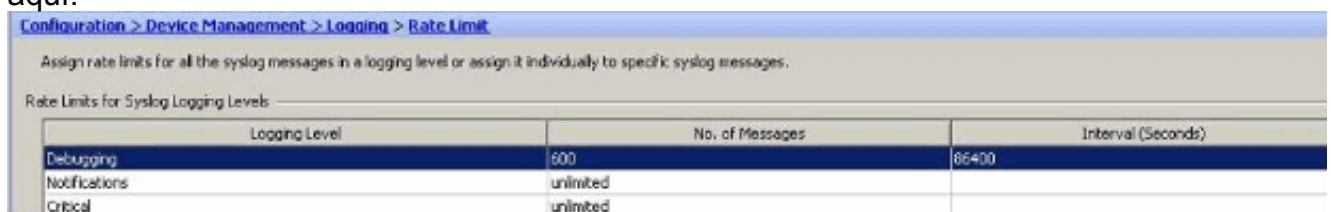
2. Especifique el número de mensajes que se enviarán junto con el intervalo de tiempo. Haga



clic en OK.

Nota: Estos números se dan como un ejemplo. Éstos diferencian dependiendo del entorno del tipo de red. Los valores modificados se consideran

aquí:

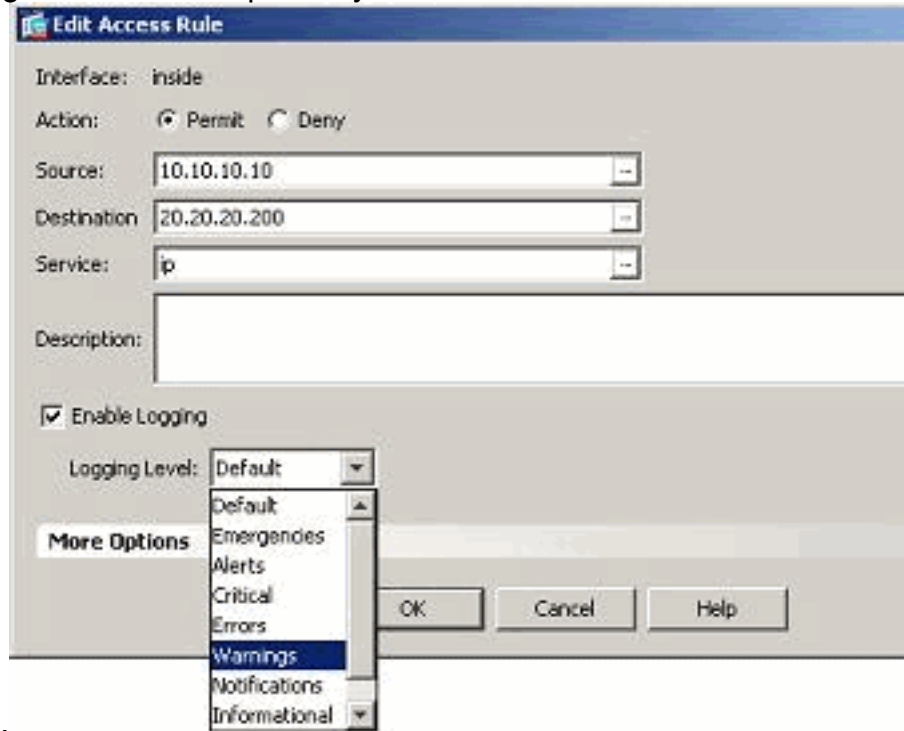


Registración de los golpes de una regla de acceso

Usted puede registrar los golpes de la regla de acceso usando el ASDM. El comportamiento predeterminado del registro es enviar un mensaje de Syslog para todos los paquetes negados. No habrá ningún mensaje de Syslog para los paquetes permitidos y éstos no serán registrados. Sin embargo, usted puede definir un nivel de gravedad de encargo del registro a la regla de acceso para seguir la cuenta de los paquetes que golpea esta regla de acceso.

Siga estos pasos:

1. Seleccione la regla de acceso requerida y el tecleo *edita*. El *editar* la ventana de la regla de

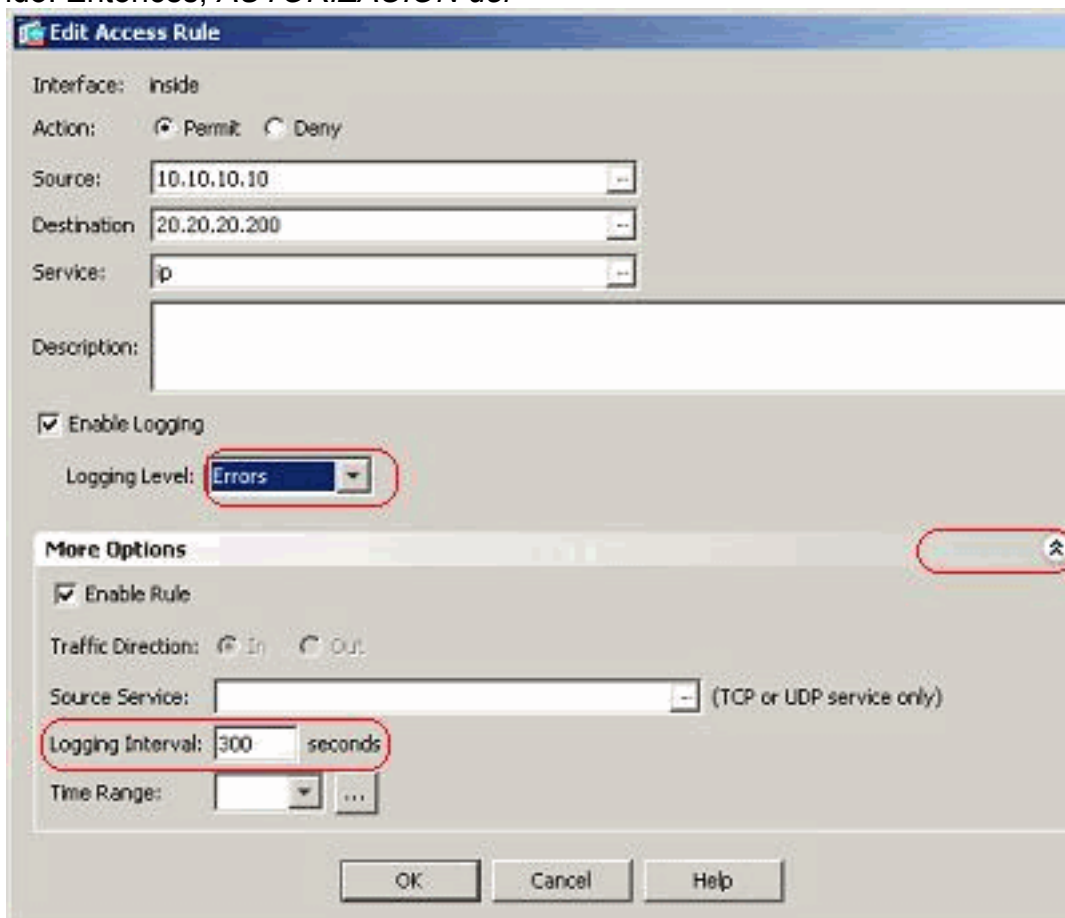


acceso aparece.

Nota: En

esta imagen, la *opción predeterminada* en el campo del *nivel de registro* indica el comportamiento predeterminado del registro de Cisco ASA. Para más información sobre esto, refiera a la sección de la [actividad de la lista de acceso del registro](#).

2. La marca de tilde la *opción de registro del permiso* y especifica el nivel de gravedad requerido. Entonces, *AUTORIZACIÓN del*



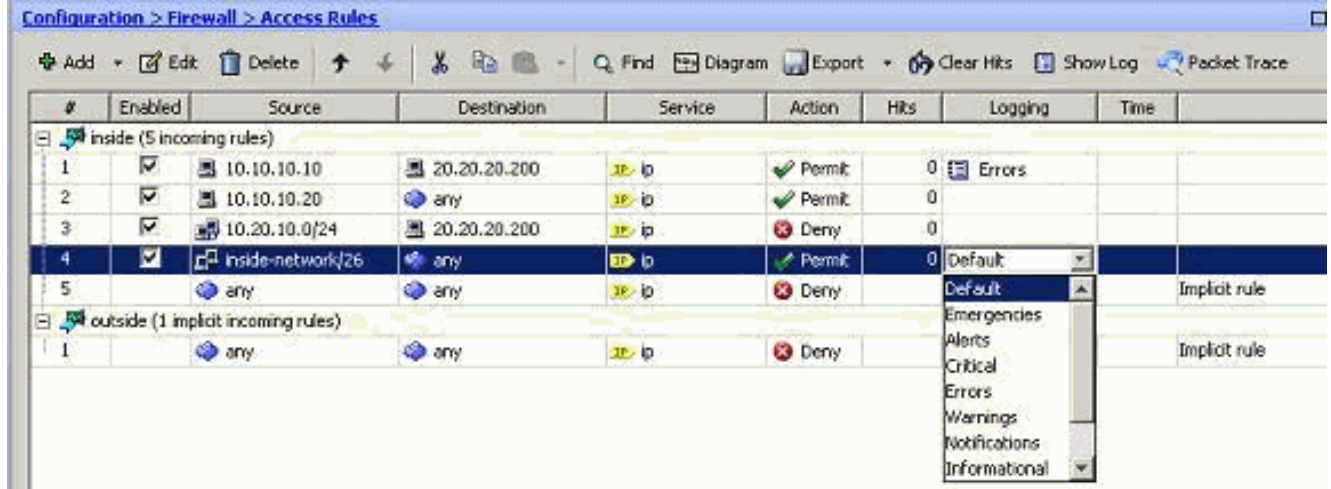
tecleo.

Nota: Haci

endo clic la *más* lengüeta del descenso-abajo de las *opciones*, usted puede ver la *opción del intervalo del registro*. Se resalta esta opción solamente cuando se hace tictac la *opción de registro* antedicha del *permiso*. El valor predeterminado de este temporizador es 300

segundos. Esta configuración es útil en especificar el valor del time out para que las flujos estadísticas sean borradas cuando no hay coincidencia para esa regla de acceso. Si hay algunos golpes, después el ASA espera hasta la duración del intervalo del registro y envía eso al Syslog.

3. Las modificaciones se muestran aquí. Alternativamente, usted puede hacer doble clic el campo del *registro de la* regla de acceso específica y fijar el nivel de gravedad allí.



Nota: Este Método alternativo de especificar el *nivel de registro* en el mismo cristal de las *reglas de acceso* haciendo doble clic trabaja para solamente las entradas manualmente creadas de la regla de acceso, pero no a las reglas implícitas.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos utilizados en esta sección.

Configuraciones

En este documento, se utilizan estas configuraciones:

```
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
```

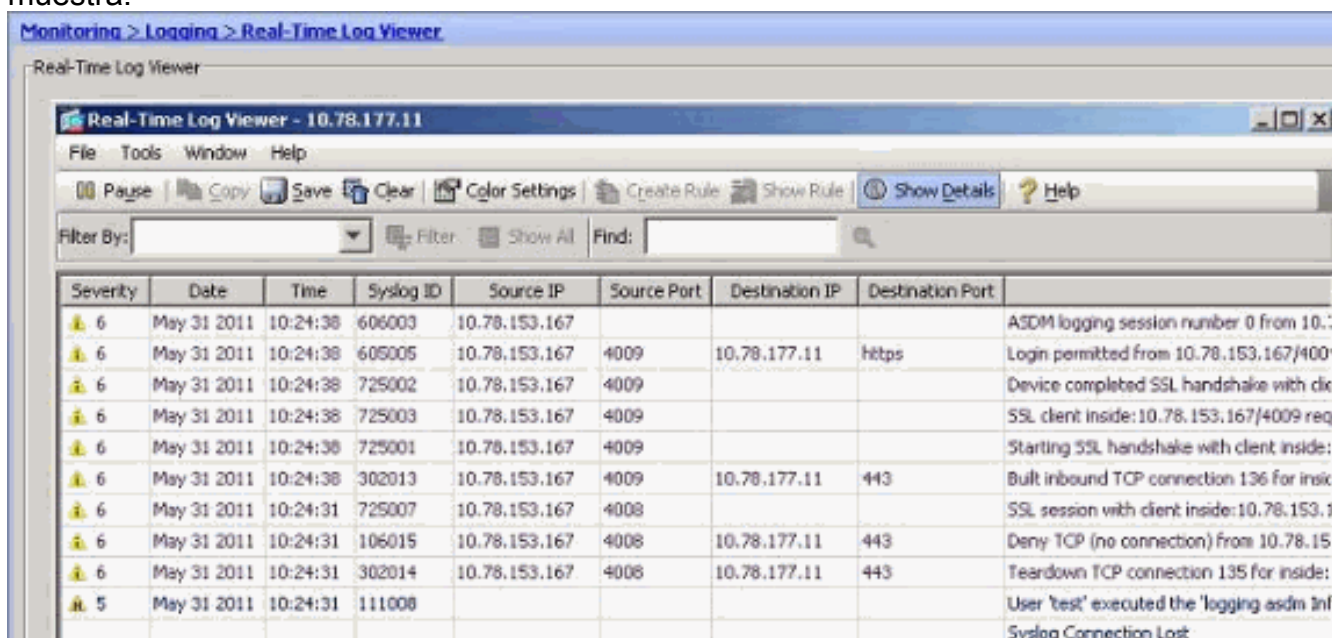
```
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global smtp-server 172.18.10.20
prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4
: end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- Usted puede ver los Syslog del ASDM. Elija la **supervisión > el registro > Log Viewer en tiempo real**. Aquí se muestra la salida de muestra:



The screenshot shows the 'Real-Time Log Viewer' window for IP 10.78.177.11. The interface includes a menu bar (File, Tools, Window, Help), a toolbar with icons for Pause, Copy, Save, Clear, Color Settings, Create Rule, Show Rule, Show Details, and Help. Below the toolbar is a 'Filter By:' dropdown and a 'Find:' search box. The main area contains a table with the following columns: Severity, Date, Time, Syslog ID, Source IP, Source Port, Destination IP, Destination Port, and a description of the event.

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
6	May 31 2011	10:24:38	606003	10.78.153.167				ASDM logging session number 0 from 10.:
6	May 31 2011	10:24:38	605005	10.78.153.167	4009	10.78.177.11	https	Login permitted from 10.78.153.167/400
6	May 31 2011	10:24:38	725002	10.78.153.167	4009			Device completed SSL handshake with cli
6	May 31 2011	10:24:38	725003	10.78.153.167	4009			SSL client inside:10.78.153.167/4009 req
6	May 31 2011	10:24:38	725001	10.78.153.167	4009			Starting SSL handshake with client inside:
6	May 31 2011	10:24:38	302013	10.78.153.167	4009	10.78.177.11	443	Built inbound TCP connection 136 for insi
6	May 31 2011	10:24:31	725007	10.78.153.167	4008			SSL session with client inside:10.78.153.1
6	May 31 2011	10:24:31	106015	10.78.153.167	4008	10.78.177.11	443	Deny TCP (no connection) from 10.78.15
6	May 31 2011	10:24:31	302014	10.78.153.167	4008	10.78.177.11	443	Teardown TCP connection 135 for inside:
5	May 31 2011	10:24:31	111008					User 'test' executed the 'logging asdm inf Syslog Connection Lost

Troubleshooting

Problema: Conexión perdida -- Conexión del Syslog terminada --

Se recibe este error al intentar habilitar el ASDM que registra en el panel del dispositivo para los contextos uces de los.

"Conexión perdida -- Conexión del Syslog terminada --"

Cuando el ASDM se utiliza para conectar directamente con el contexto admin y registro ASDM se inhabilita allí, después Switch a una registraci3n del ASDM del subcontext y del permiso. Se reciben los errores, pero los mensajes de Syslog est1n alcanzando muy bien al servidor de Syslog.

Soluci3n

Esto es un comportamiento sabido con el ASDM de Cisco y documentó en el Id. de bug Cisco [CSCsd10699](#) ([clientes registrados solamente](#)). Como solución alternativa, registro del asdm del permiso cuando está registrado en el contexto admin.

[No puede ver el tiempo real abre una sesión el ASDM de Cisco](#)

Un problema es que los registros en tiempo real no se pueden ver en el ASDM. ¿Cómo se configura esto?

[Solución](#)

Configure el siguiente en Cisco ASA:

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

[Información Relacionada](#)

- [Soporte del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)