Configurar o Syslog do Adaptive Security Appliance (ASA)

Contents

Introdução

Este documento descreve a configuração de exemplo que demonstra como configurar diferentes opções de registro no ASA que executa o código Versão 8.4 ou posterior.

Informações de Apoio

O ASA versão 8.4 introduziu técnicas de filtragem muito granulares para permitir que apenas determinadas mensagens de syslog especificadas sejam apresentadas. A seção Syslog básico deste documento demonstra uma configuração de syslog tradicional. A seção Syslog avançado deste documento mostra os novos recursos de syslog na versão 8.4. Consulte Guias de mensagens de log do sistema do Cisco Security Appliance para obter o guia completo de mensagens de log do sistema.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5515 com software ASA versão 8.4
- Cisco Adaptive Security Device Manager (ASDM) versão 7.1.6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Observação: consulte o ASA 8.2: Configurar o Syslog usando o ASDM para obter mais informações sobre detalhes de configuração semelhantes com o ASDM versão 7.1 e posterior.

Syslog básico

Insira esses comandos para habilitar o registro em log, exibir logs e exibir definições de configuração.

- logging enable - Permite a transmissão de mensagens de syslog para todos os locais de saída.
- no logging enable - Desabilita o registro em todos os locais de saída.
- show logging - Lista o conteúdo do buffer de syslog, bem como as informações e

estatísticas que pertencem à configuração atual.

O ASA pode enviar mensagens de syslog para vários destinos. Insira os comandos nestas seções para especificar os locais para os quais você gostaria que as informações de syslog fossem enviadas:

Enviar informações de registro para o buffer interno

<#root>

```
logging buffered

 severity_level
```

Software ou hardware externo não é necessário quando você armazena as mensagens de syslog no buffer interno do ASA. Insira o comando show logging para ver as mensagens de syslog armazenadas. O buffer interno tem um tamanho máximo de 1 MB (configurável com o comando logging buffer-size). Como resultado, ele pode ser finalizado muito rapidamente. Lembre-se disso ao escolher um nível de registro para o buffer interno, já que níveis mais detalhados de registro podem preencher e empacotar rapidamente o buffer interno.

Enviar informações de registro a um servidor Syslog

<#root>

```
logging host

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

logging trap

 severity_level

logging facility

 number
```

Um servidor que executa um aplicativo syslog é necessário para enviar mensagens syslog a um host externo. O ASA envia syslog na porta UDP 514 por padrão, mas o protocolo e a porta podem ser escolhidos. Se o TCP for escolhido como o protocolo de registro, isso faz com que o ASA envie syslogs através de uma conexão TCP para o Servidor syslog. Se o servidor estiver inacessível ou a conexão TCP com o servidor não puder ser estabelecida, o ASA, por padrão, bloqueia TODAS as novas conexões. Esse comportamento pode ser desativado se você ativar o registro permit-hostdown. Consulte o guia de configuração para obter mais informações sobre o comando logging permit-hostdown.

Observação: o ASA permite apenas portas que variam de 1025 a 65535. O uso de qualquer

---

outra porta resulta neste erro:
ciscoasa(config)# logging host tftp 192.168.1.1 udp/516
AVISO: o nível de segurança da interface Ethernet0/1 é 0.
ERRO: a porta '516' não está no intervalo de 1025 a 65535.

Enviar informações de registro como e-mails

<#root>

logging mail

severity_level

logging recipient-address

email_address

logging from-address

email_address

smtp-server

ip_address

Um servidor SMTP é necessário quando você envia as mensagens de syslog em e-mails. A configuração correta no servidor SMTP é necessária para garantir que você possa retransmitir com êxito os e-mails do ASA para o cliente de e-mail especificado. Se esse nível de registro estiver definido como um nível muito detalhado, como depuração ou informativo, você poderá gerar um número significativo de syslogs, já que cada e-mail enviado por essa configuração de registro faz com que mais de quatro ou mais registros adicionais sejam gerados.

Enviar informações de registro ao console serial

<#root>

logging console

severity_level

O registro de console permite que mensagens de syslog sejam exibidas no console ASA (tty) à medida que ocorrem. Se o registro do console estiver configurado, toda a geração de registro no ASA será limitada a 9800 bps, a velocidade do console serial do ASA. Isso pode fazer com que os syslogs sejam liberados para todos os destinos, que incluem o buffer interno. Não use o registro de console para syslogs detalhados por esse motivo.

Enviar informações de registro para uma sessão Telnet/SSH

<#root>

```
logging monitor
 severity_level
terminal monitor
```

O monitor de registro permite que as mensagens de syslog sejam exibidas à medida que ocorrem quando você acessa o console ASA com Telnet ou SSH e o comando terminal monitor é executado a partir dessa sessão. Para parar a impressão de logs na sessão, insira o comando terminal no monitor.

Exibir Mensagens de Log no ASDM

<#root>

```
logging asdm
 severity_level
```

O ASDM também tem um buffer que pode ser usado para armazenar mensagens de syslog. Insira o comando show logging asdm para exibir o conteúdo do buffer de syslog do ASDM.

Enviar registros a uma estação de gerenciamento 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
```

Os usuários precisam de um ambiente funcional de Protocolo de Gerenciamento de Rede

Simples (SNMP - Simple Network Management Protocol) para enviar mensagens de syslog com SNMP. Consulte Comandos para definição e gerenciamento de destinos de saída para obter uma referência completa sobre os comandos que podem ser usados para definir e gerenciar destinos de saída. Consulte Mensagens Listadas por Nível de Severidade para obter as mensagens listadas por nível de severidade.

Adicionar Carimbos de Data/Hora a Syslogs

Para ajudar a alinhar e ordenar eventos, carimbos de data/hora podem ser adicionados aos syslogs. Isso é recomendado para ajudar a rastrear problemas com base no tempo. Para habilitar os timestamps, insira o comando logging timestamp. Aqui estão dois exemplos de syslog, um sem o timestamp e outro com:

```
%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
```

Exemplo 1

Esta saída mostra um exemplo de configuração para efetuar login no buffer com o nível de severidade de debugging.

<#root>

```
logging enable
logging buffered debugging
```

Esse é o exemplo de saída.

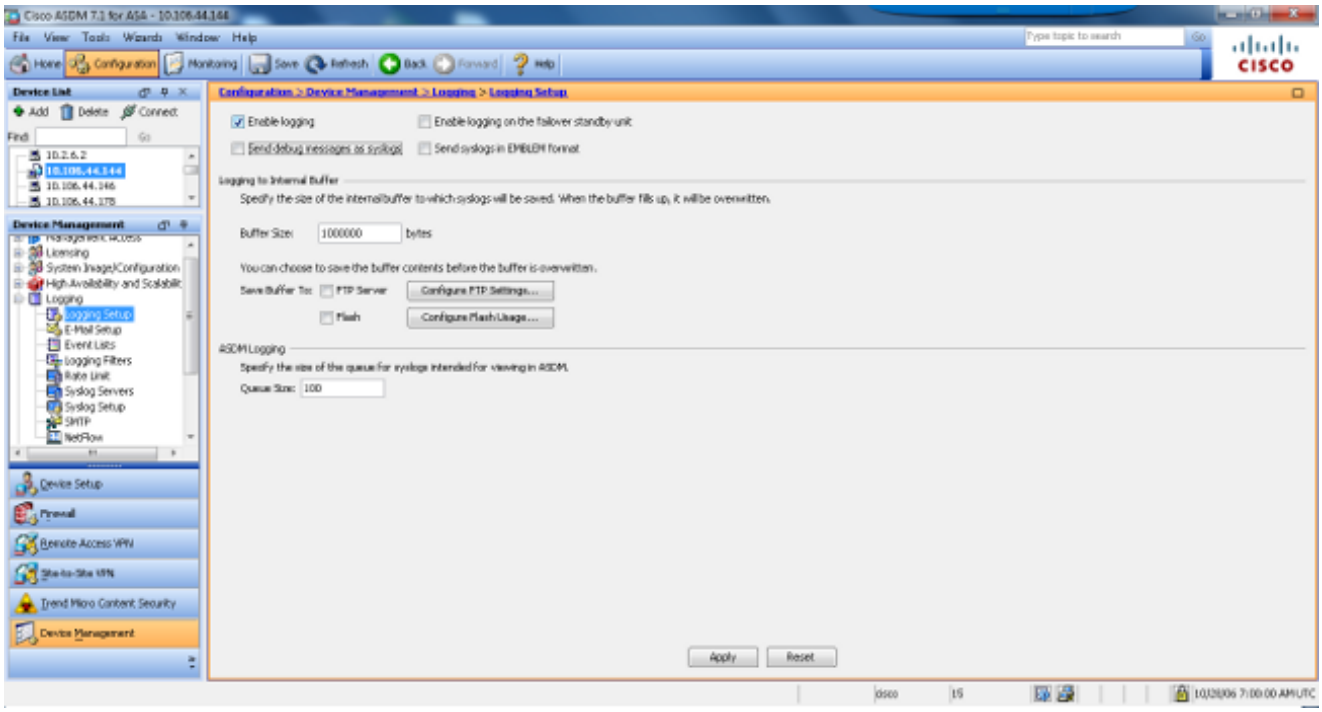
```
%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

Configurar Syslog Básico com ASDM

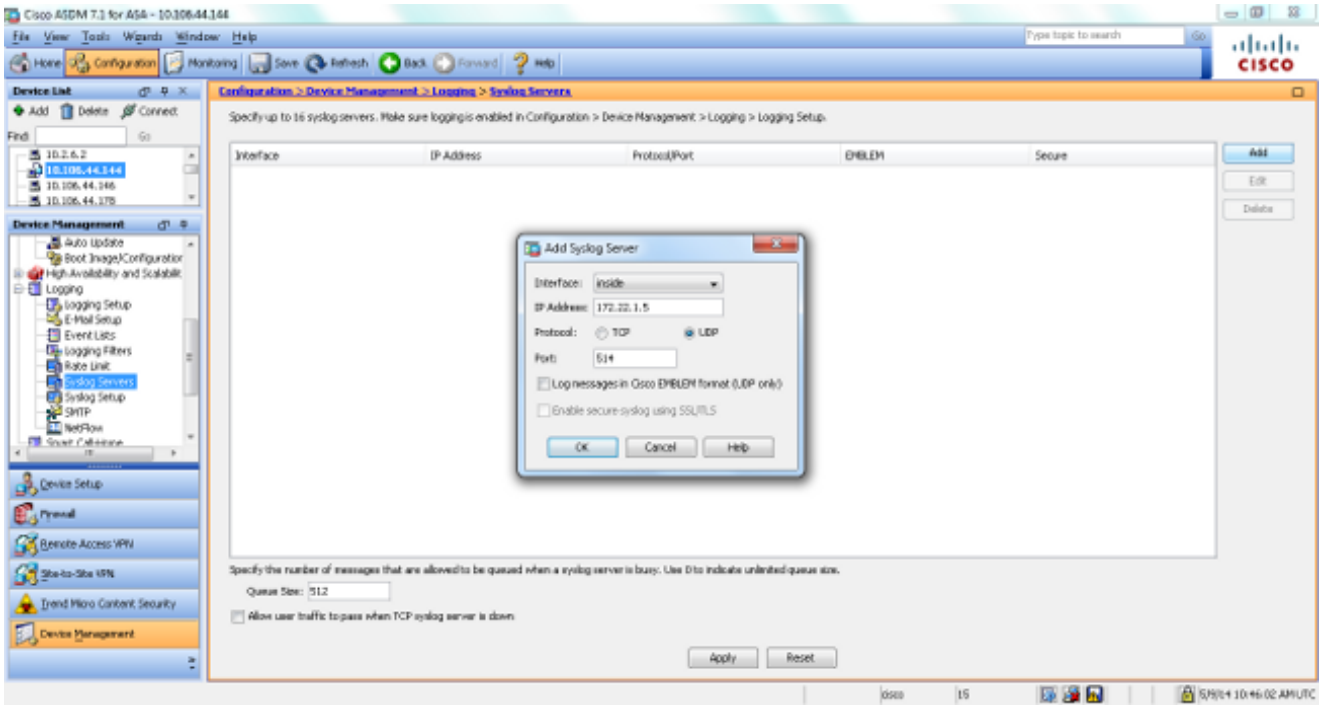
Este procedimento demonstra a configuração do ASDM para todos os destinos de syslog disponíveis.

1. Para habilitar o registro no ASA, primeiro configure os parâmetros básicos de registro. Escolha Configuration > Features > Properties > Logging > Logging Setup. Marque a caixa

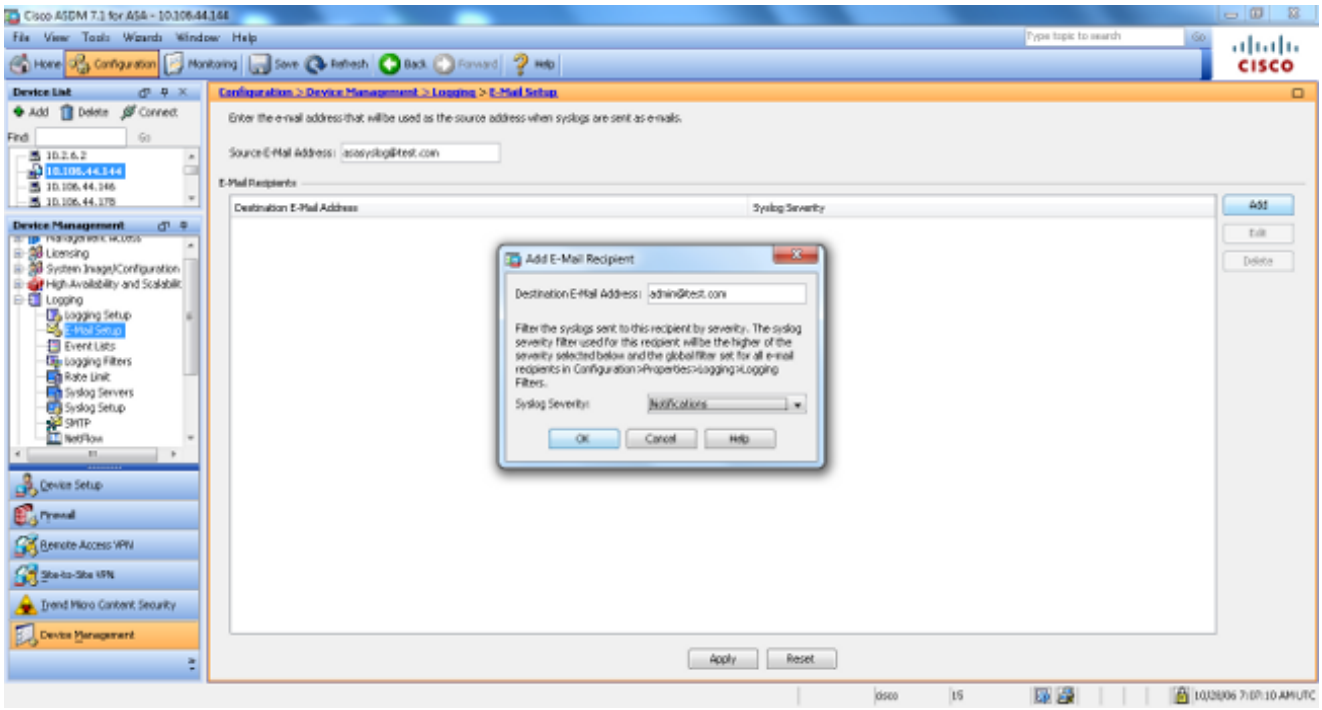
de seleção Enable logging para habilitar syslogs.



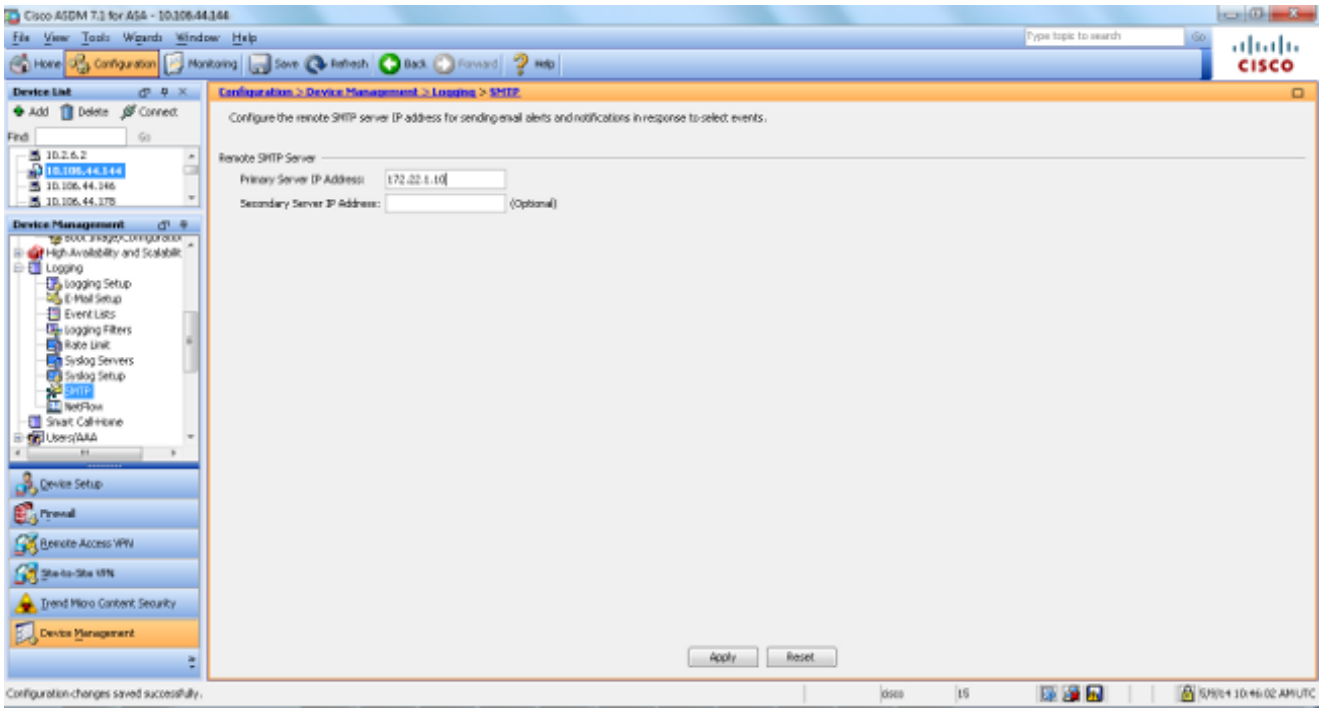
2. Para configurar um servidor externo como o destino de syslogs, escolha Syslog Servers em Logging e clique em Add para adicionar um Servidor syslog. Insira os detalhes do Servidor syslog na caixa Adicionar Servidor Syslog e escolha OK quando terminar.



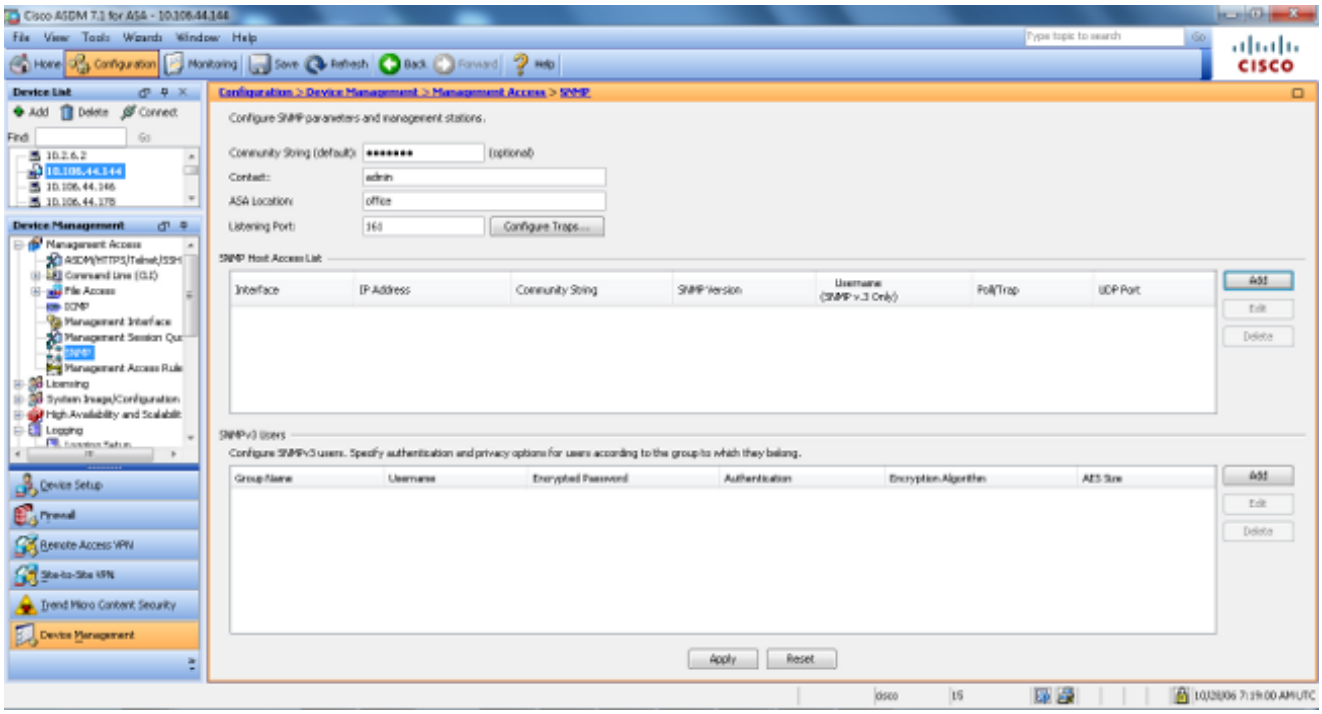
3. Escolha E-Mail Setup em Logging para enviar mensagens de syslog como e-mails a destinatários específicos. Especifique o endereço de e-mail de origem na caixa Endereço de E-mail de Origem e escolha Adicionar para configurar o endereço de e-mail de destino dos destinatários de e-mail e o nível de gravidade da mensagem. Clique em OK quando terminar.



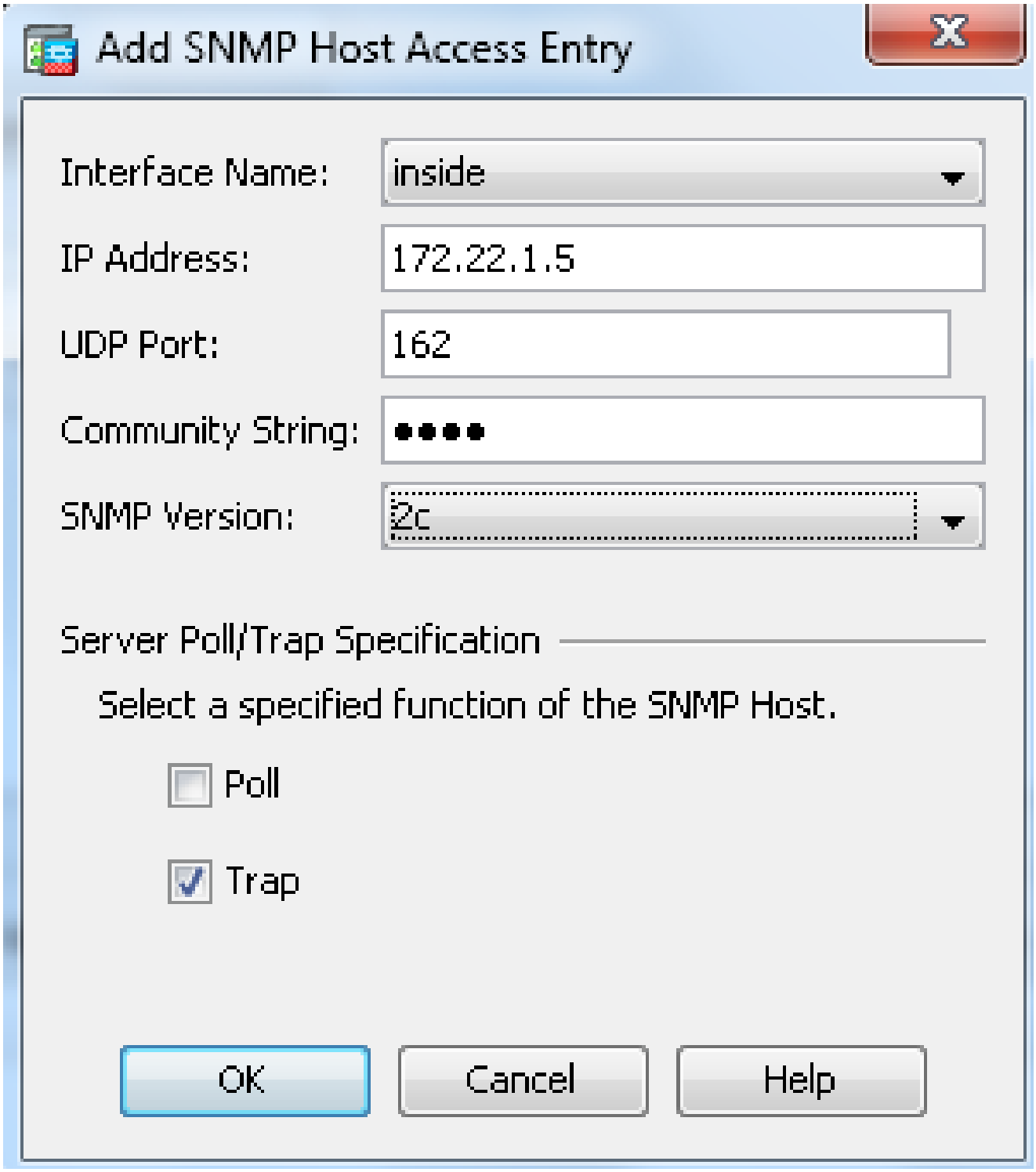
4. Selecione Device Administration, Logging, escolha SMTP e insira o Primary Server IP Address para especificar o endereço IP do servidor SMTP.



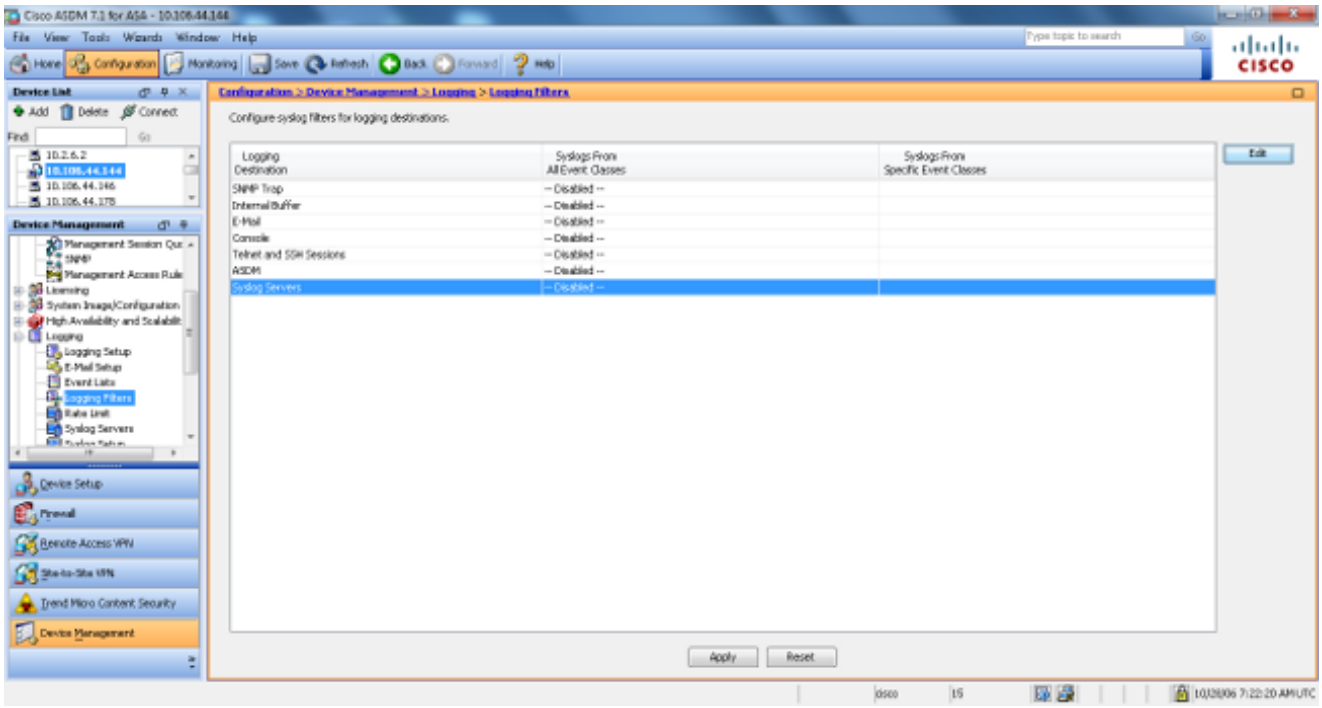
5. Para enviar syslogs como interceptações SNMP (traps), primeiro defina um servidor SNMP. Escolha SNMP no menu Acesso de gerenciamento para especificar o endereço das estações de gerenciamento SNMP e suas propriedades específicas.



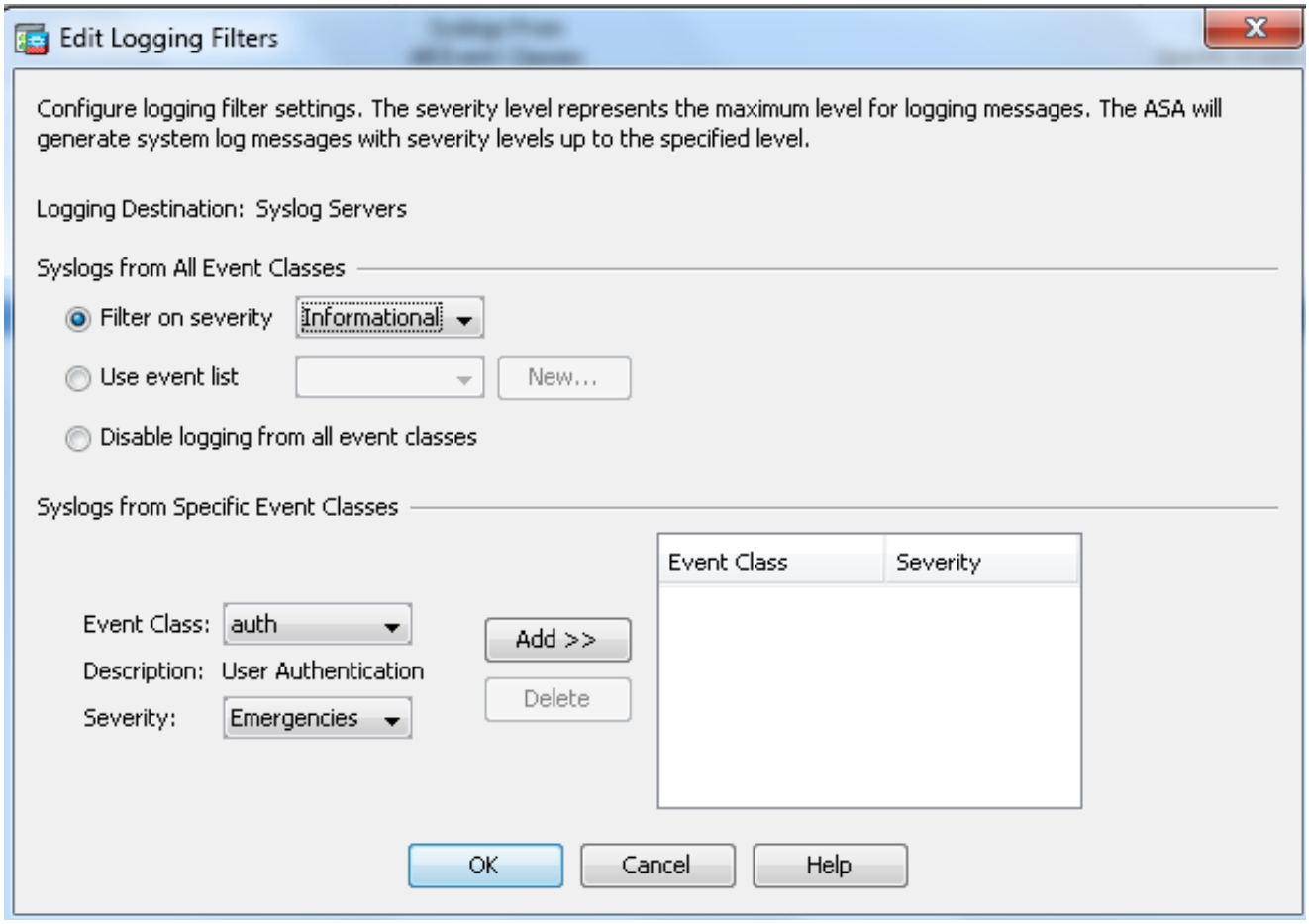
6. Escolha Add para adicionar uma estação de gerenciamento SNMP. Insira os detalhes do host SNMP e clique em OK.



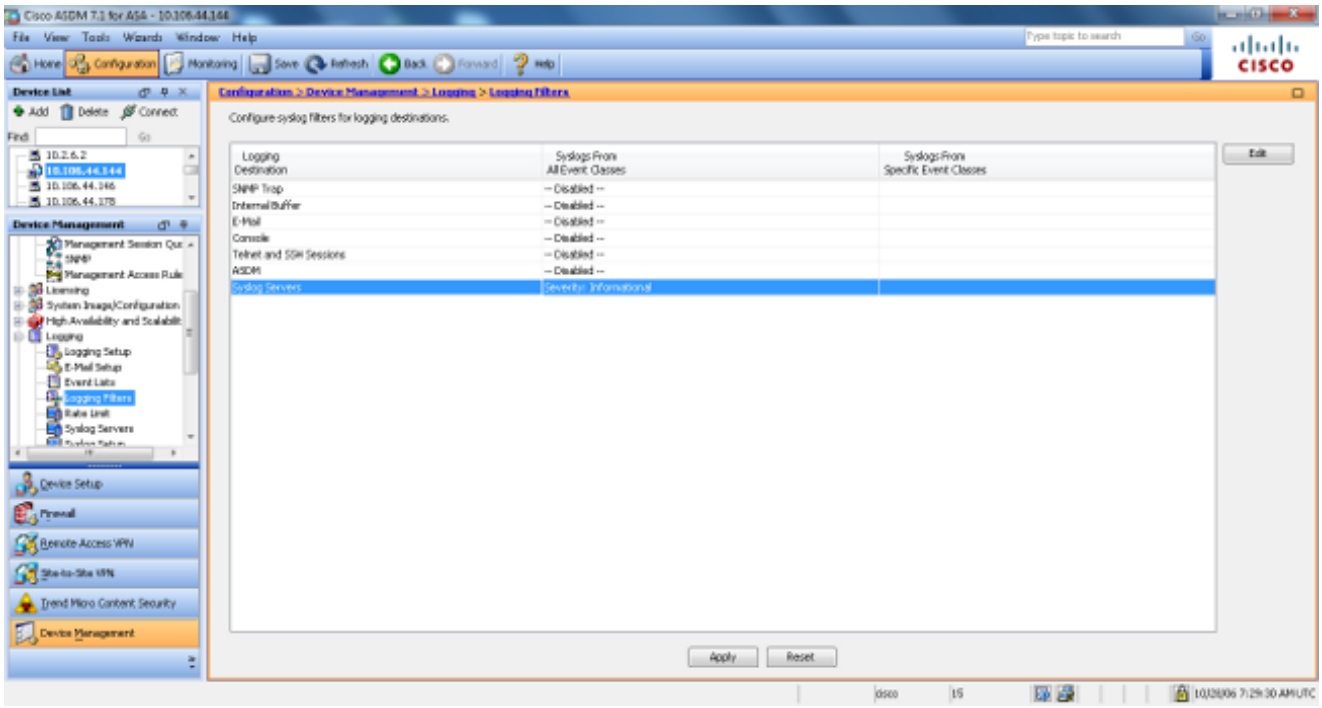
7. Para permitir que os logs sejam enviados a qualquer um dos destinos mencionados anteriormente, escolha Logging Filters na seção logging. Isso apresenta cada destino de registro possível e o nível atual de registros que são enviados a esses destinos. Escolha o destino de registro desejado e clique em Editar. Neste exemplo, o destino 'Servidores Syslog' é modificado.



8. Escolha uma severidade apropriada, neste caso Informativa, na lista suspensa Filtrar na severidade. Clique em OK quando terminar.



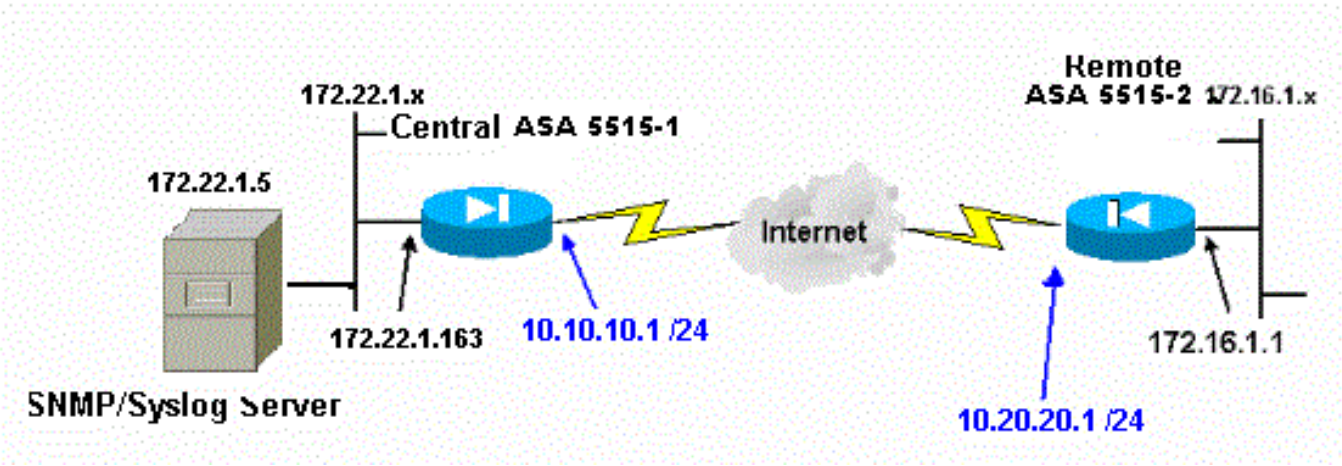
9. Clique em Apply depois de voltar à janela Logging Filters.



Enviar mensagens de syslog em uma VPN para um Servidor Syslog

No design de VPN site a site simples ou no design hub-and-spoke mais complicado, o administrador pode querer monitorar todos os firewalls ASA remotos com o servidor SNMP e o servidor syslog localizados em um site central.

Para configurar a configuração da VPN IPsec site a site, consulte PIX/ASA 7.x e posterior: Exemplo de Configuração de Túnel VPN PIX a PIX. Além da configuração da VPN, você precisa configurar o SNMP e o tráfego interessante para o Servidor syslog no site central e local.



Configuração do ASA Central

<#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 *****
```

Configuração do ASA remoto

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

Consulte Monitoring Cisco Secure ASA Firewall Using SNMP and Syslog Through VPN Tunnel para obter mais informações sobre como configurar o ASA versão 8.4

Syslog avançado

O ASA versão 8.4 fornece vários mecanismos que permitem configurar e gerenciar mensagens de syslog em grupos. Esses mecanismos incluem o nível de severidade da mensagem, a classe da mensagem, o ID da mensagem ou uma lista de mensagens personalizada criada por você. Com o uso desses mecanismos, você pode inserir um único comando que se aplica a pequenos ou grandes grupos de mensagens. Quando você configura syslogs dessa forma, é possível capturar as mensagens do grupo de mensagens especificado e não mais todas as mensagens da mesma gravidade.

Usar a lista de mensagens

Use a lista de mensagens para incluir somente as mensagens de syslog interessadas por nível de gravidade e ID em um grupo e, em seguida, associe essa lista de mensagens ao destino desejado.

Conclua estas etapas para configurar uma lista de mensagens:

1. Digite a lista de registro message_list | level severity_level [class message_class] para criar uma lista de mensagens que inclua mensagens com um nível de gravidade ou uma lista de mensagens especificados.
2. Insira o comando logging list message_list message syslog_id-syslog_id2 para adicionar mais mensagens à lista de mensagens recém-criada.
3. Insira o comando logging destination message_list para especificar o destino da lista de mensagens criada.

Exemplo 2

Digite estes comandos para criar uma lista de mensagens, que inclui todas as mensagens de gravidade 2 (críticas) com a adição de 611101 de mensagem para 611323, e também para que sejam enviadas ao console:

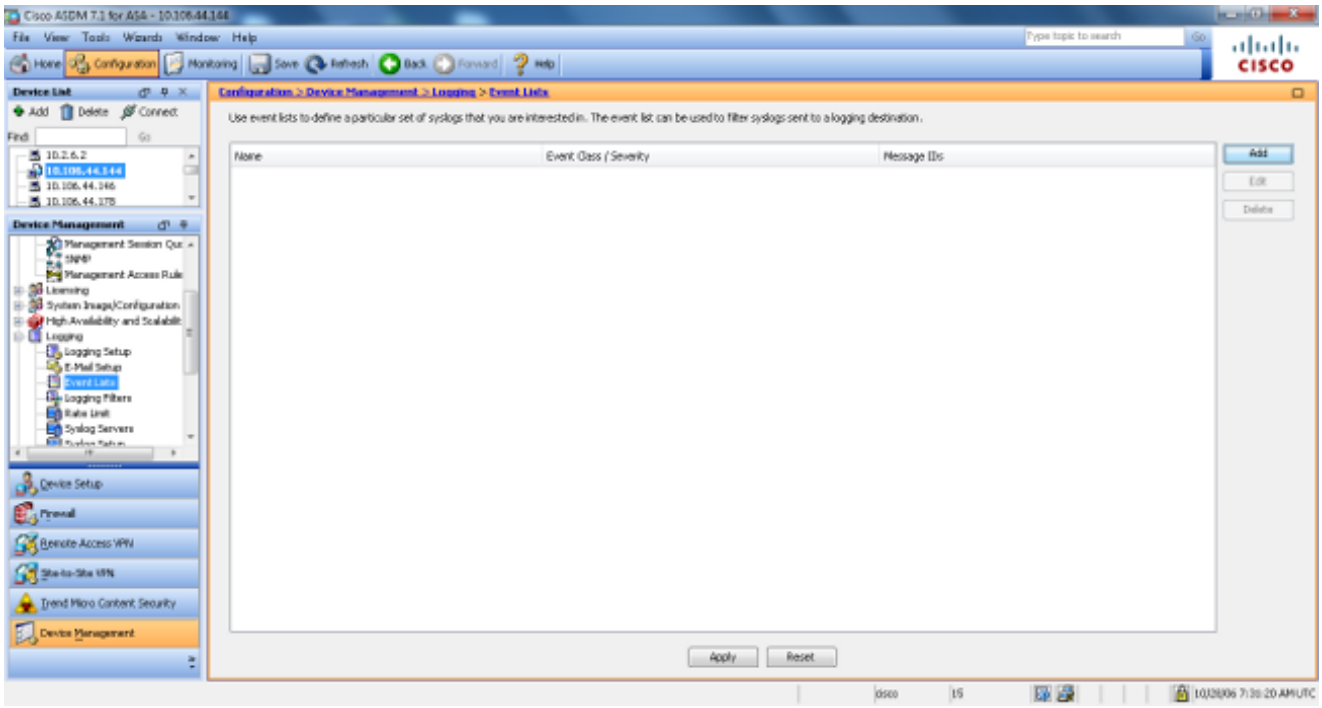
<#root>

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

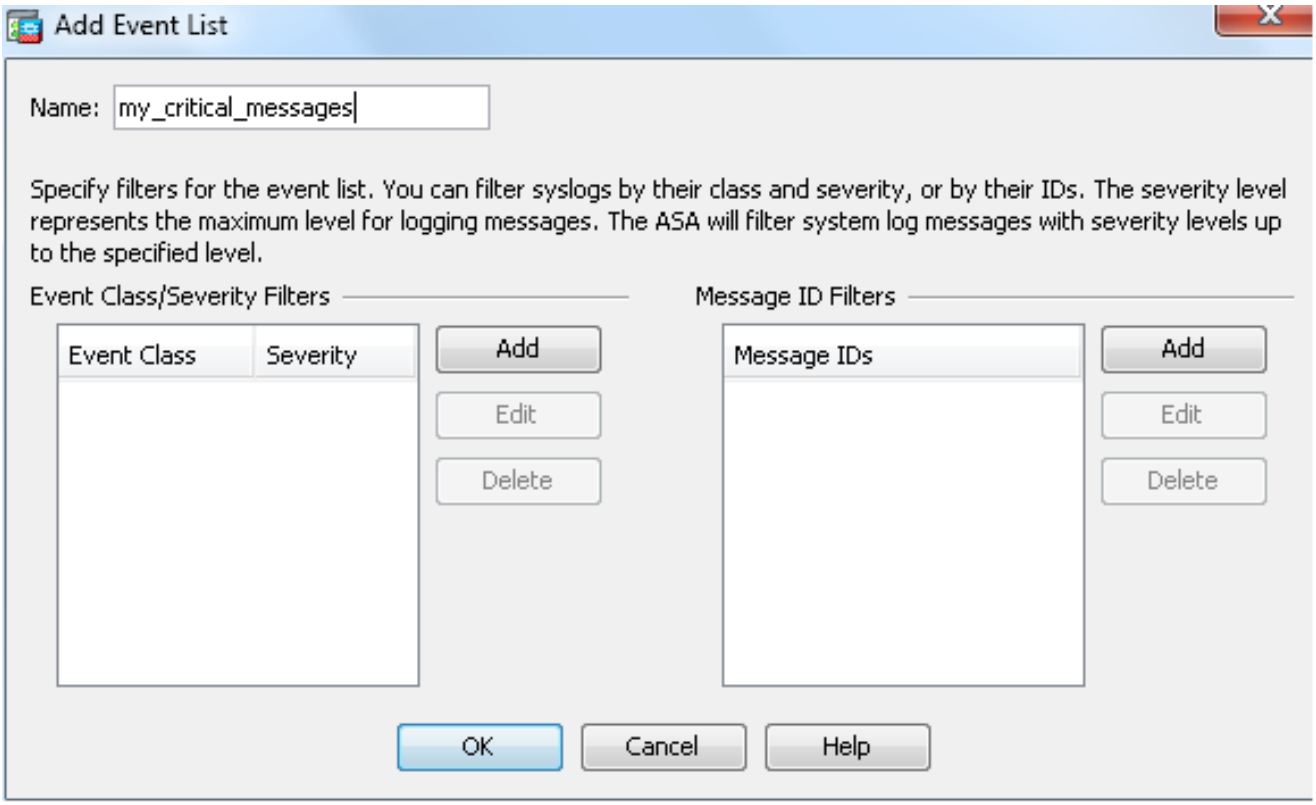
Configuração do ASDM

Este procedimento mostra uma configuração do ASDM para o Exemplo 2 com o uso da lista de mensagens.

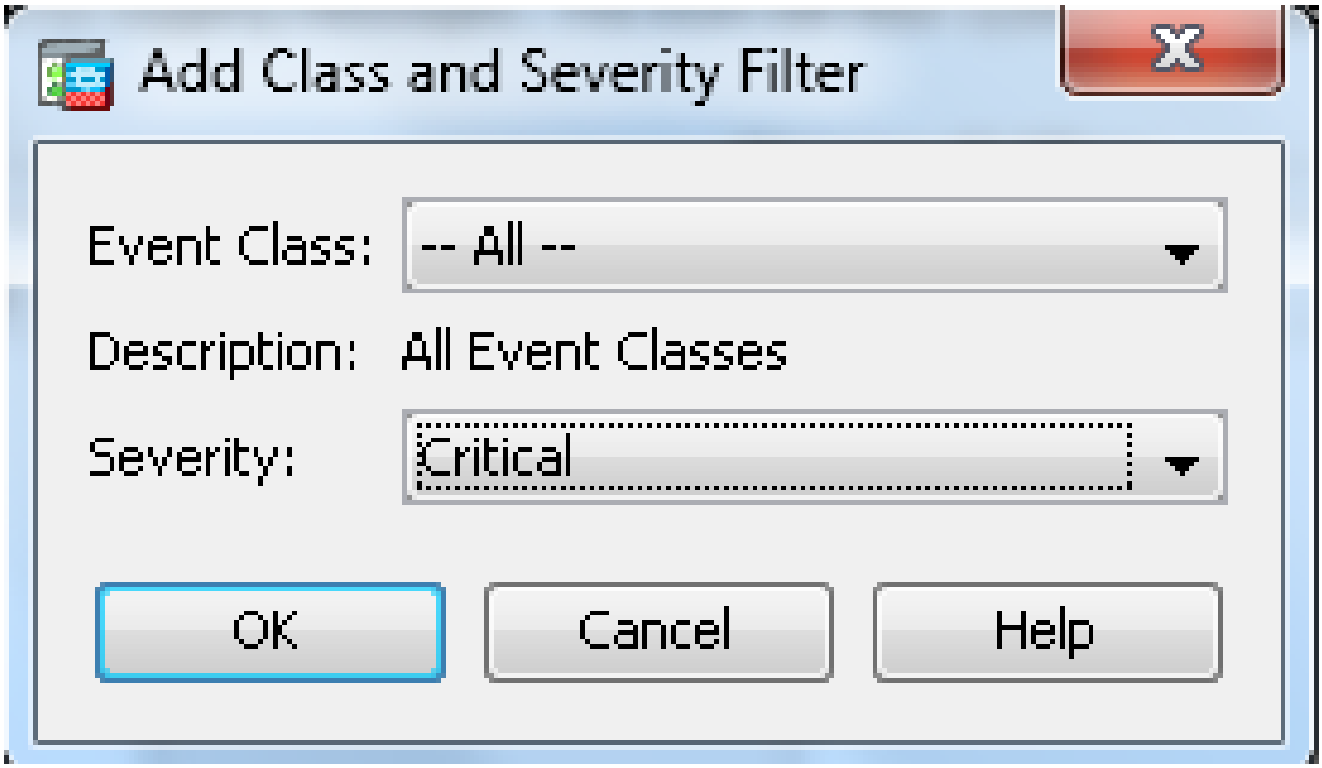
1. Selecione Event Lists em Logging e clique em Add para criar uma lista de mensagens.



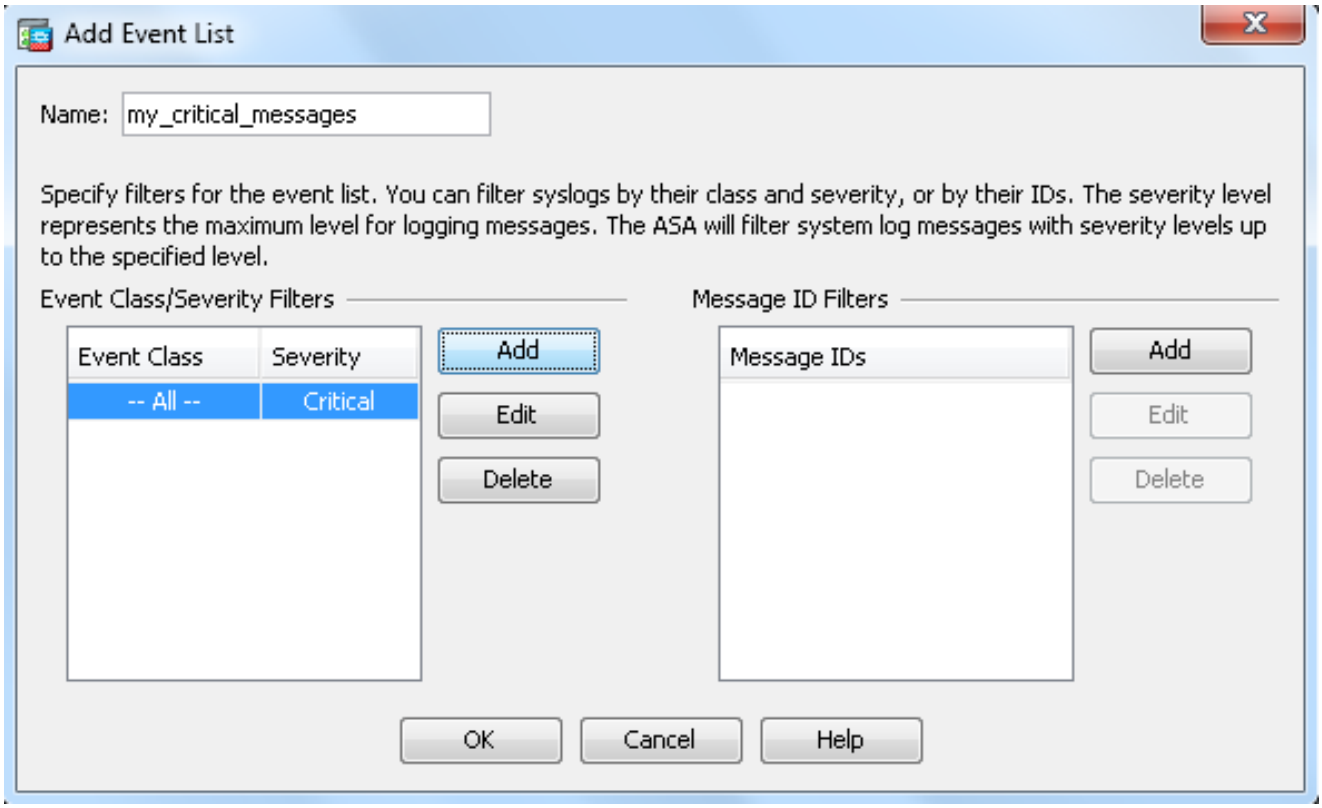
2. Digite o nome da lista de mensagens na caixa Nome. Nesse caso, my_critical_messages é usado. Clique em Add em Event Class/Severity Filters.



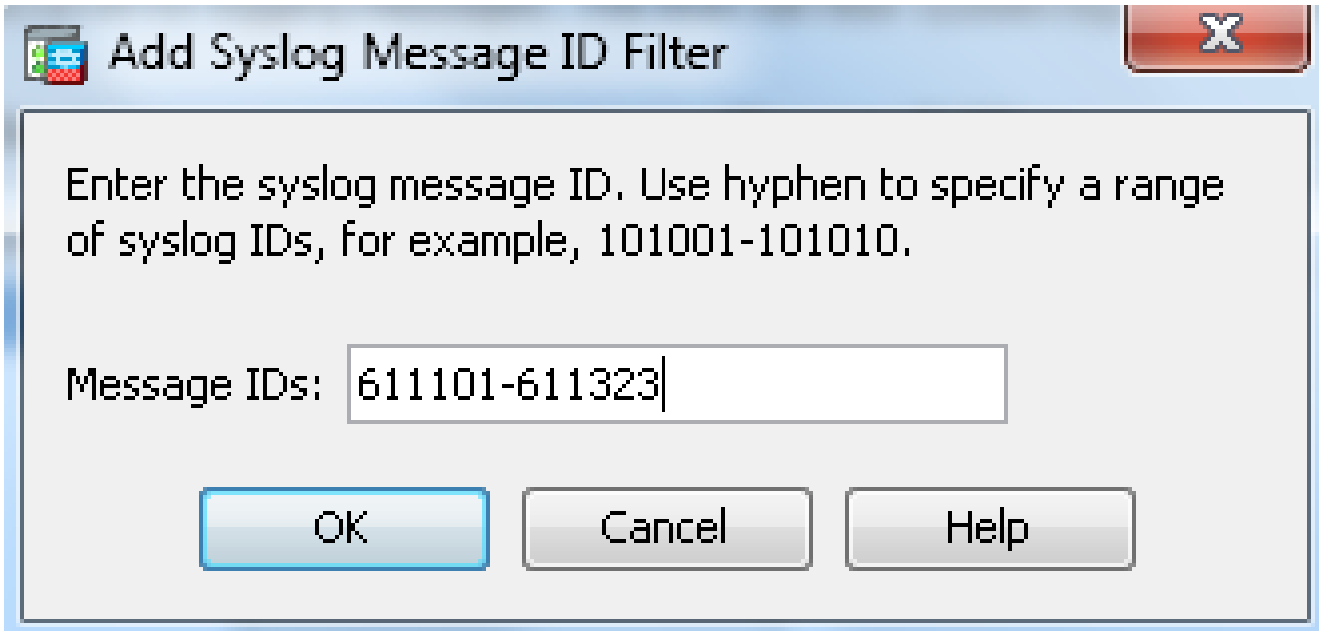
3. Escolha All na lista suspensa Event Class. Escolha Crítico na lista suspensa Severidade. Clique em OK quando terminar.



4. Clique em Adicionar em Filtros de ID de mensagem se mensagens adicionais forem necessárias. Nesse caso, você precisa colocar mensagens com a ID 611101-611323.

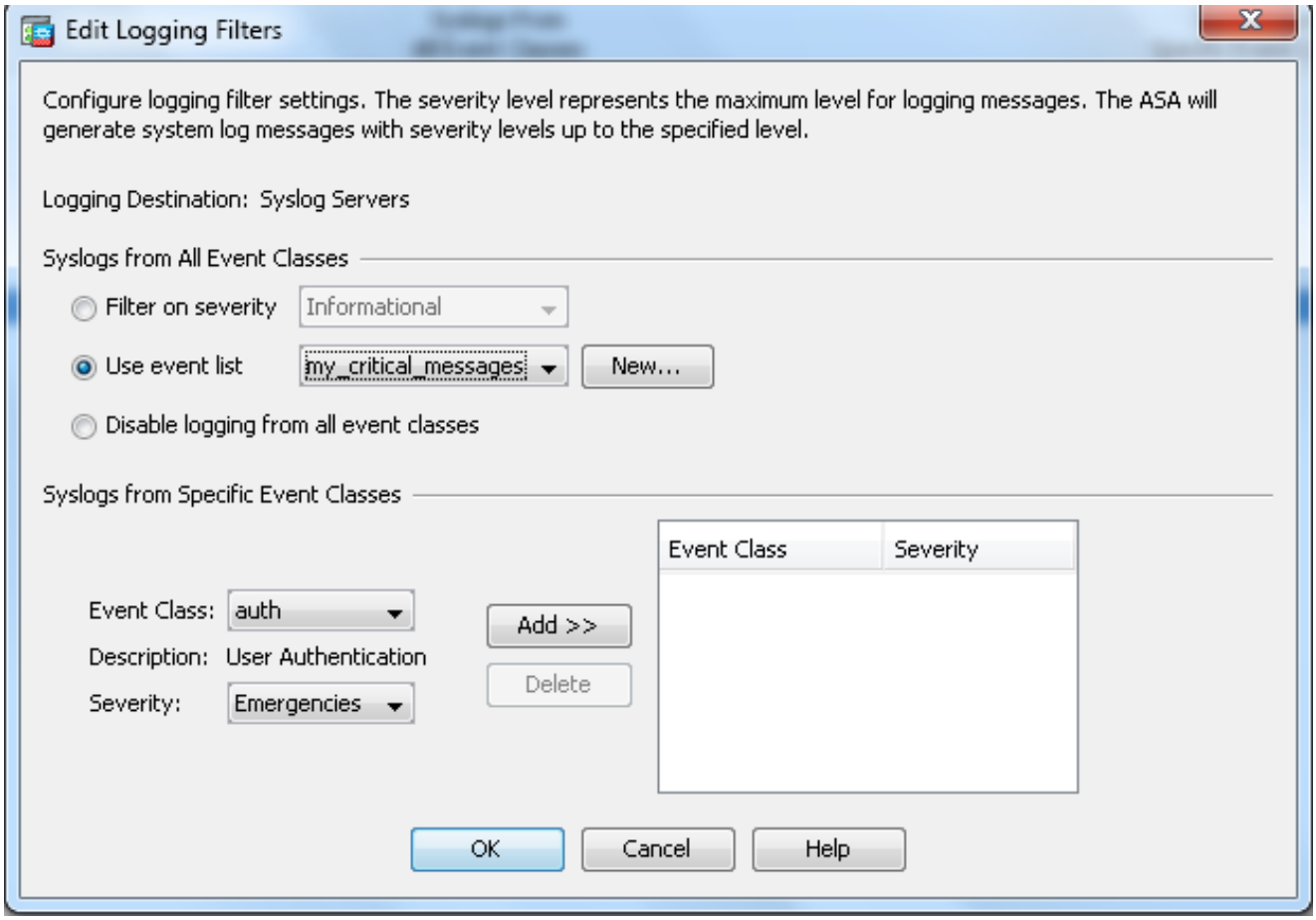


5. Coloque o intervalo de IDs na caixa IDs de mensagem e clique em OK.

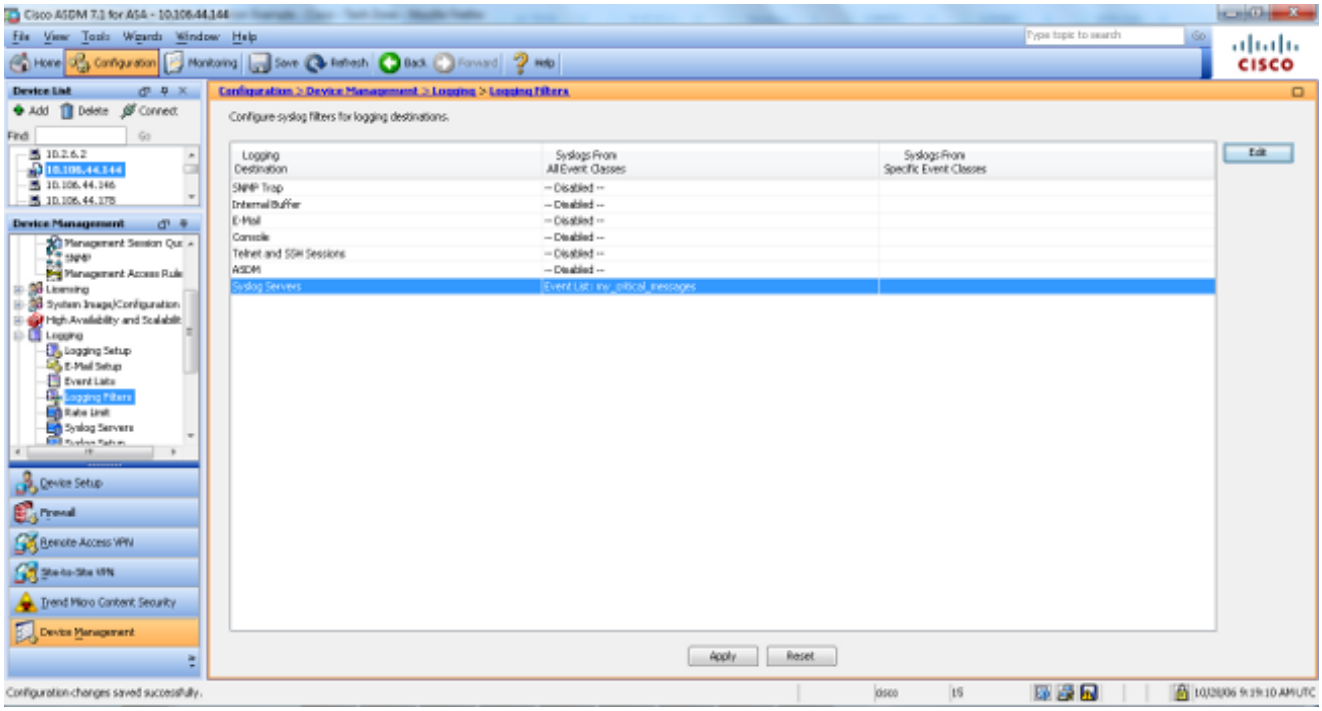


6. Volte para o menu Logging Filters e escolha Console como o destino.

7. Escolha my_critical_messages na lista suspensa Use event list. Clique em OK quando terminar.



8. Clique em Apply depois de voltar à janela Logging Filters.



Isso conclui as configurações do ASDM com o uso de uma lista de mensagens, como mostrado no Exemplo 2.

Usar a classe Mensagem

Use a classe de mensagem para enviar todas as mensagens associadas a uma classe para o local de saída especificado. Ao especificar um limite de nível de severidade, você pode limitar o número de mensagens enviadas ao local de saída.

<#root>

logging class

message_class destination | severity_level

Exemplo 3

Insira este comando para enviar todas as mensagens de classe de CA com um nível de gravidade de emergências ou superior para o console.

<#root>

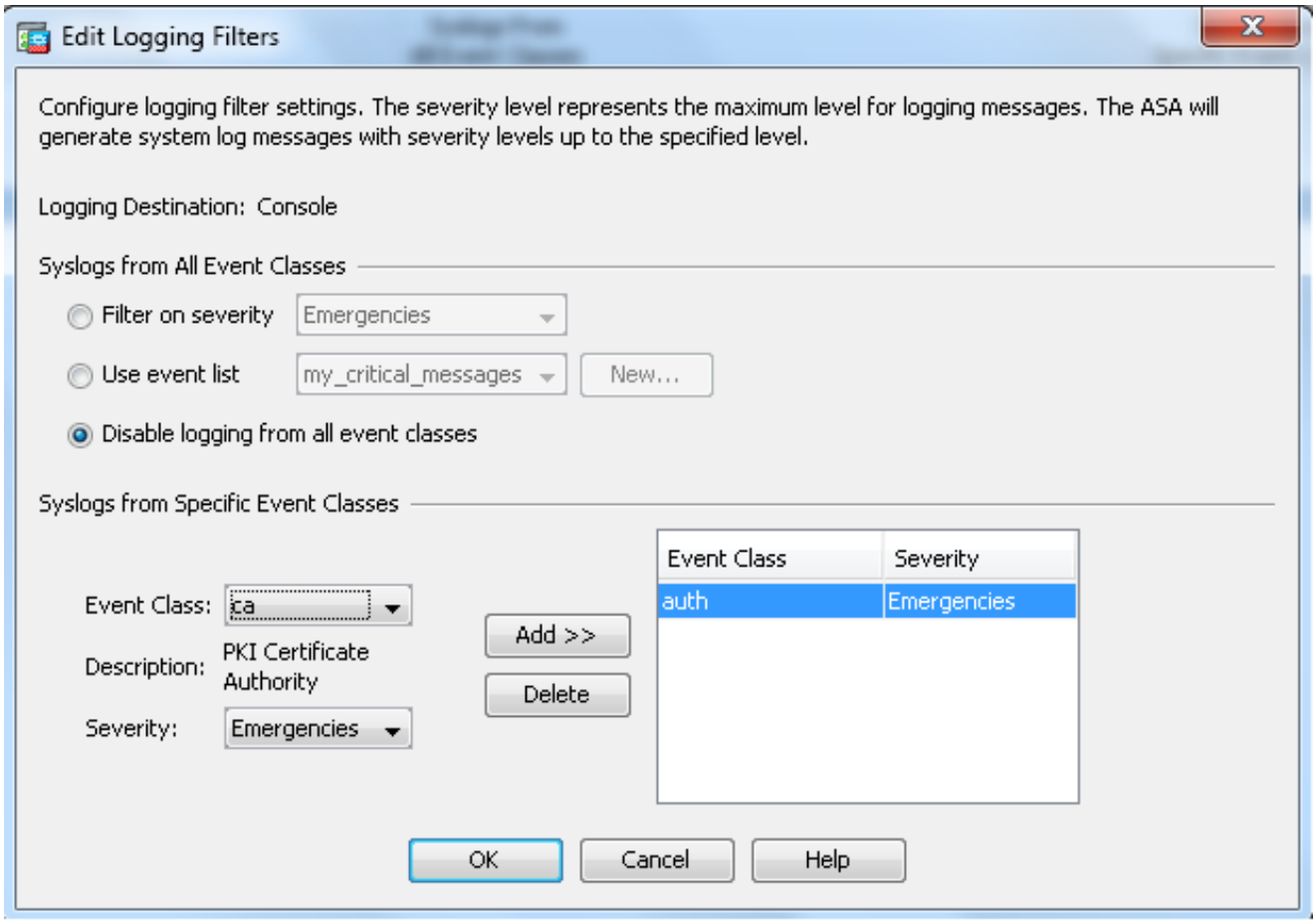
logging class ca console emergencies

Configuração do ASDM

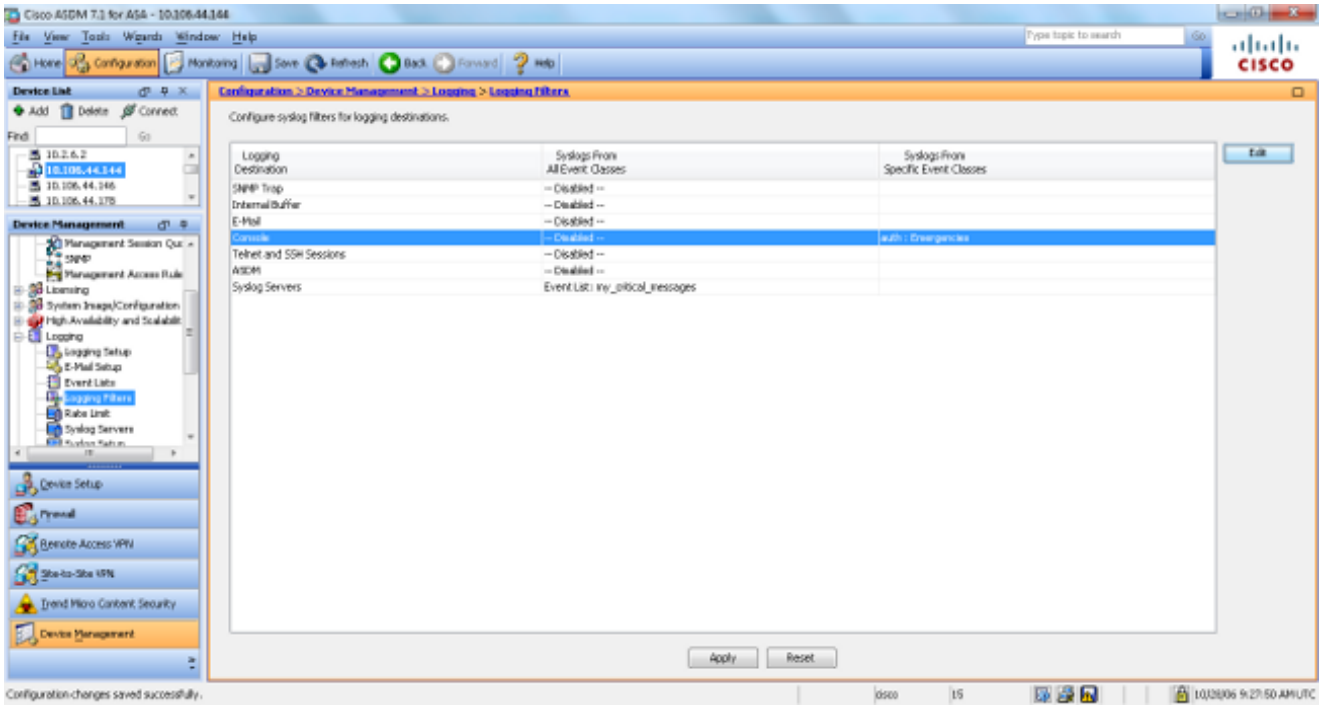
Este procedimento mostra as configurações do ASDM para o Exemplo 3 com o uso da lista de mensagens.

1. Escolha o menu Logging Filters e escolha Console como o destino.
2. Clique em Desativar registro de todas as classes de evento.
3. Nos Syslogs de Classes de Evento Específicas, escolha a Classe de Evento e a Severidade que deseja adicionar.

   Este procedimento usa ca e Emergências, respectivamente.
4. Clique em Add para adicioná-lo à classe de mensagem e clique em OK.



5. Clique em Apply depois de voltar à janela Logging Filters. O console agora coleta a mensagem da classe ca com Emergências de nível de gravidade, conforme mostrado na janela Filtros de registro.



Isso conclui a configuração do ASDM para o Exemplo 3. Consulte Mensagens Listadas por Nível de Severidade para obter uma lista dos níveis de severidade da mensagem de log.

Enviar mensagens de log de depuração para um servidor Syslog

Para a solução avançada de problemas, são necessários logs de depuração específicos de recurso/protocolo. Por padrão, essas mensagens de registro são exibidas no terminal (SSH/Telnet). Dependendo do tipo de depuração e da taxa de mensagens de depuração geradas, o uso da CLI poderá ser difícil se as depurações forem ativadas. Opcionalmente, as mensagens de depuração podem ser redirecionadas para o processo syslog e geradas como syslogs. Esses syslogs podem ser enviados para qualquer destino de syslog como faria com qualquer outro syslog. Para desviar depurações para syslogs, insira o comando logging debug-trace. Essa configuração envia saída de depuração, como syslogs, para um Servidor syslog.

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

Uso conjunto da lista de registro e das classes de mensagem

Insira o comando logging list para capturar o syslog de mensagens VPN IPsec de LAN para LAN e acesso remoto sozinho. Este exemplo captura todas as mensagens de log do sistema de classe VPN (IKE e IPsec) com nível de depuração ou superior.

Exemplo

<#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
```

Registrar Acertos da ACL

Adicione log a cada elemento da lista de acesso (ACE) desejado para registrar quando uma lista de acesso for atingida. Use esta sintaxe:

<#root>

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

Exemplo

<#root>

```
ASAfirewall(config)#

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

As ACLs, por padrão, registram cada pacote negado. Não há necessidade de adicionar a opção de log para negar ACLs para gerar syslogs para pacotes negados. Quando a opção log é especificada, ela gera a mensagem de syslog 106100 para a ACE à qual é aplicada. A mensagem de Syslog 106100 é gerada para cada fluxo de permissão ou negação de entrada correspondente que passa pelo firewall ASA. O fluxo de primeira correspondência é armazenado em cache. As correspondências subsequentes incrementam a contagem de ocorrências exibida no comando show access-list. O comportamento de registro de lista de acesso padrão, que é a palavra-chave log não especificada, é que se um pacote for negado, a mensagem 106023 será gerada e, se um pacote for permitido, nenhuma mensagem de syslog será gerada.

Um nível de syslog opcional (0 - 7) pode ser especificado para as mensagens de syslog geradas (106100). Se nenhum nível for especificado, o nível padrão será 6 (informativo) para uma nova ACE. Se a ACE já existir, seu nível de log atual permanecerá inalterado. Se a opção log disable for especificada, o registro em log da lista de acesso será completamente desabilitado. Nenhuma mensagem de syslog, que inclui a mensagem 106023, é gerada. A opção log default restaura o comportamento de log padrão da lista de acesso.

Conclua estes passos para permitir que a mensagem de syslog 106100 seja exibida na saída do console:

1. Insira o comando logging enable para habilitar a transmissão de mensagens de log do sistema para todos os locais de saída. Você deve definir um local de saída de registro para exibir todos os registros.
2. Insira o comando logging message <message_number> level <severity_level> para definir o nível de gravidade de uma mensagem de log de sistema específica.

Nesse caso, insira o comando logging message 106100 para habilitar a mensagem `106100`.

3. Insira a message_list do console de registro | severity_level para permitir que as mensagens de log do sistema sejam exibidas no console do Security Appliance (tty) à medida que ocorrem. Defina o `severity_level` de 1 a 7 ou use o nome do nível. Você também pode especificar quais mensagens são enviadas com a variável `message_list`.

4. Insira o comando show logging message para exibir uma lista de mensagens de mensagens de log do sistema que foram modificadas da configuração padrão, que são mensagens que receberam um nível de gravidade diferente e mensagens que foram desabilitadas.

   Este é um exemplo de saída do comando 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
```

Bloqueio da geração de syslog em um ASA em espera

Inicie a partir do software ASA versão 9.4.1 e você pode bloquear a geração de syslogs específicos em uma unidade em standby e use este comando:

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

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Se quiser suprimir uma mensagem de syslog específica a ser enviada ao Servidor syslog, você deverá inserir o comando como mostrado.

```
<#root>

hostname(config)#

no logging message
```

<syslog_id>

Consulte o comando logging message para obter mais informações.

%ASA-3-201008: Não Permitir Novas Conexões

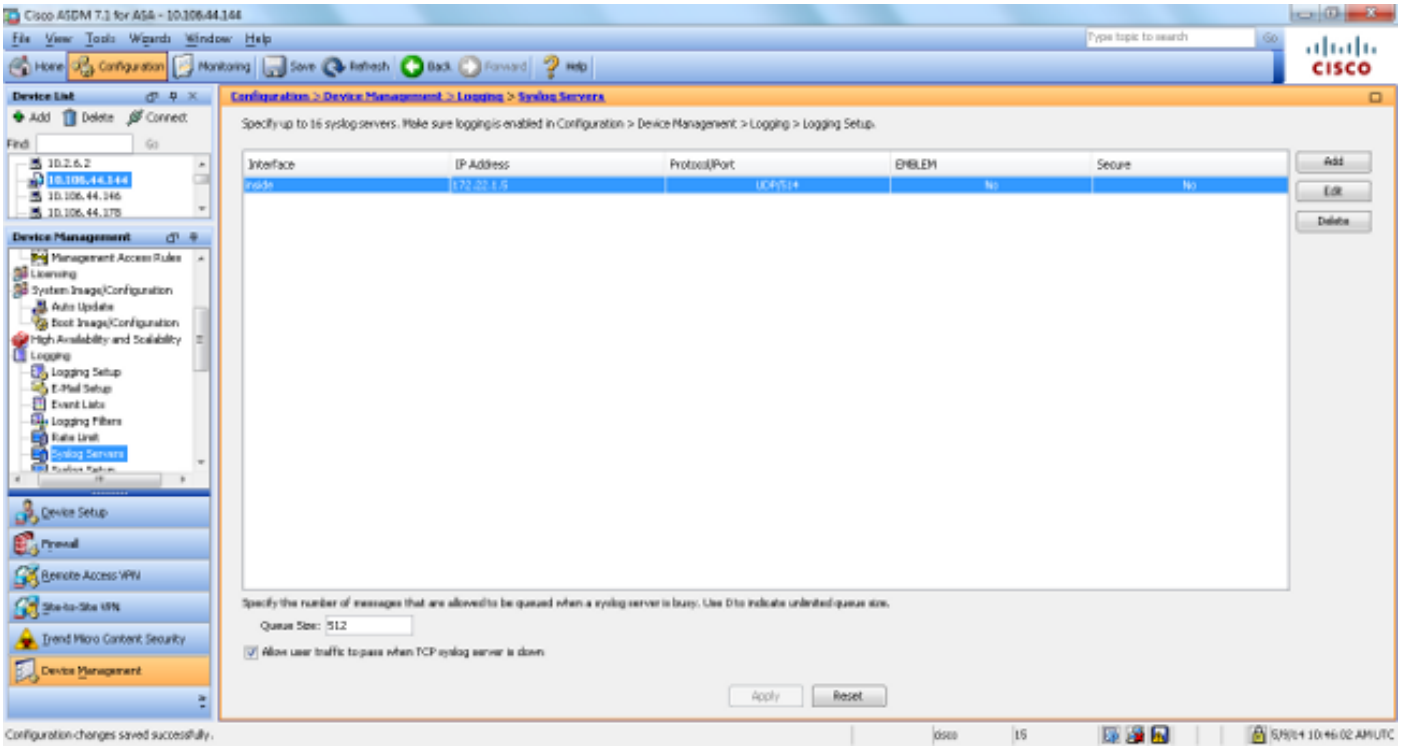
A mensagem de erro `%ASA-3-201008: Não permitindo novas conexões.` é vista quando um ASA não consegue entrar em contato com o Servidor syslog e nenhuma conexão nova é permitida.

Solução

Esta mensagem aparece quando você ativou o sistema de mensagens de log TCP e o servidor syslog não pode ser alcançado, ou quando você usa o Cisco ASA Syslog Server (PFSS) e o disco no sistema Windows NT está cheio. Conclua estas etapas para resolver esta mensagem de erro:

- Desative o sistema de mensagens de log do sistema TCP se ele estiver ativado.
- Se você usar o PFSS, libere espaço no sistema Windows NT onde o PFSS reside.
- Certifique-se de que o Servidor syslog esteja ativo e que você possa fazer ping no host a partir do console Cisco ASA.
- Reinicie o registro de mensagens do sistema TCP para permitir o tráfego.

Se o Servidor syslog for desativado e o registro de TCP estiver configurado, use o comando logging permit-hostdown ou mude para o registro de UDP.



Informações Relacionadas

- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.