配置自适应安全设备(ASA)系统日志

目录

简介

本文档介绍的示例配置演示如何在运行代码版本8.4或更高版本的ASA上配置不同的日志记录选项。

背景信息

ASA 版本 8.4 引入了非常精细的过滤技术，支持仅显示某些指定的系统日志消息。本文档的基本 Syslog 部分说明传统的 Syslog 配置。本文档的高级系统日志部分中介绍了版本 8.4 中新增的系统日志功能。有关完整的系统日志消息指南，请参阅思科安全设备系统日志消息指南。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 采用 ASA 软件版本 8.4 的 ASA 5515
- 思科自适应安全设备管理器 (ASDM) 版本 7.1.6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意：有关ASDM 7.1版及更高版本的类似配置详细信息，请参阅ASA 8.2：使用ASDM配置系统日志。

基本 Syslog

输入下列命令以启用日志记录，以及查看日志和配置设置。

- logging enable - 允许向所有输出位置传输系统日志消息。
- no logging enable - 禁止向所有输出位置传输日志记录。
- show logging - 列出系统日志缓冲区的内容以及与当前配置相关的信息和统计信息。

ASA 可以将系统日志消息发送到各个目的地。输入下列各节中的命令可指定要将系统日志信息发送到的位置：

将日志记录信息发送到内部缓冲区

```
<#root>

logging buffered

 severity_level
```

将系统日志消息存储在 ASA 内部缓冲区中时，不需要使用外部软件或硬件。输入 show logging 命令以查看已存储的日志消息。内部缓冲区的最大大小为 1 MB（可使用 logging buffer-size 命令进行配置）。因此，可以非常快速地包装。当您为内部缓冲区选择日志记录级别时，请记住这一点，因为更详细的日志记录级别可以快速填充和包装内部缓冲区。

将日志记录信息发送到系统日志服务器

<#root>

logging host

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

logging trap

 severity_level

logging facility

 number

需要运行 Syslog 应用程序的服务器才能将 Syslog 消息发送到外部主机。默认情况下，ASA 在 UDP 端口 514 上发送系统日志，但是您可以选择协议和端口。如果选择 TCP 作为日志记录协议，这会导致 ASA 通过 TCP 连接将系统日志发送到系统日志服务器。如果服务器无法访问，或者无法与服务器建立TCP连接，默认情况下，ASA会阻止所有新连接。如果启用 logging permit-hostdown，可以禁用此行为。有关 logging permit-hostdown 命令的详细信息，请参阅配置指南。

注意：ASA仅允许范围从1025-65535的端口。使用任何其他端口都会导致此错误：
ciscoasa(config)# logging host tftp 192.168.1.1 udp/516
警告：接口Ethernet0/1的安全级别为0。
错误：端口'516'不在1025-65535范围内。

以电子邮件形式发送日志记录信息

<#root>

logging mail

 severity_level

logging recipient-address

 email_address

logging from-address

 email_address

smtp-server

 ip_address

当您在电子邮件中发送 Syslog 消息时，需要 SMTP 服务器。为了确保可以成功将邮件从 ASA 中继到指定的邮件客户端，必须在 SMTP 服务器上进行正确配置。如果此日志记录级别设置为非常详细的级别(例如debug或informational)，则您可以生成大量系统日志，因为此日志记录配置发送的每封电子邮件会导致生成多达四个或更多附加日志。

将日志记录信息发送到串行控制台

<#root>

logging console

 severity_level

控制台日志记录功能可在 ASA 控制台 (tty) 上显示系统日志消息。如果已配置了控制台日志记录，则 ASA 上的所有日志生成速率将被限制为 9800 bps（ASA 串行控制台的速度）。这会导致系统日志被丢弃到所有目标，包括内部缓冲区。因此，请勿将控制台日志记录功能用于详细系统日志。

将日志记录信息发送到 Telnet/SSH 会话

<#root>

logging monitor

 severity_level

terminal monitor

当您使用 Telnet 或 SSH 访问 ASA 控制台并从该会话中执行 terminal monitor 命令时，日志记录监控器可显示系统日志消息。要阻止将日志输出到会话，请输入 terminal no monitor 命令。

在 ASDM 上显示日志消息

<#root>

logging asdm

 severity_level

ASDM 也有一个可用来存储 Syslog 消息的缓冲区。输入 show logging asdm 命令以显示 ASDM 系统日志缓冲区的内容。

向 SNMP 管理站发送日志

<#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

用户需要具有正常工作的现有简单网络管理协议 (SNMP) 环境，才能使用 SNMP 发送系统日志消息。有关可用于设置和管理输出目的地的命令的完整参考信息，请参阅用于设置和管理输出目的地的命令。有关按严重性级别列出的消息，请参阅按严重性级别列出的消息。

向系统日志添加时间戳

为了帮助对事件进行调整和排序，可以向系统日志添加时间戳。建议执行此操作，以帮助根据时间跟踪问题。要启用时间戳，请输入 logging timestamp 命令。以下是两个系统日志示例（其中一个不带时间戳，另一个带时间戳）：

```
%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
```

示例 1

此输出信息显示了一个示例配置，用于登录严重性级别为调试的缓冲区。

<#root>

logging enable
logging buffered debugging

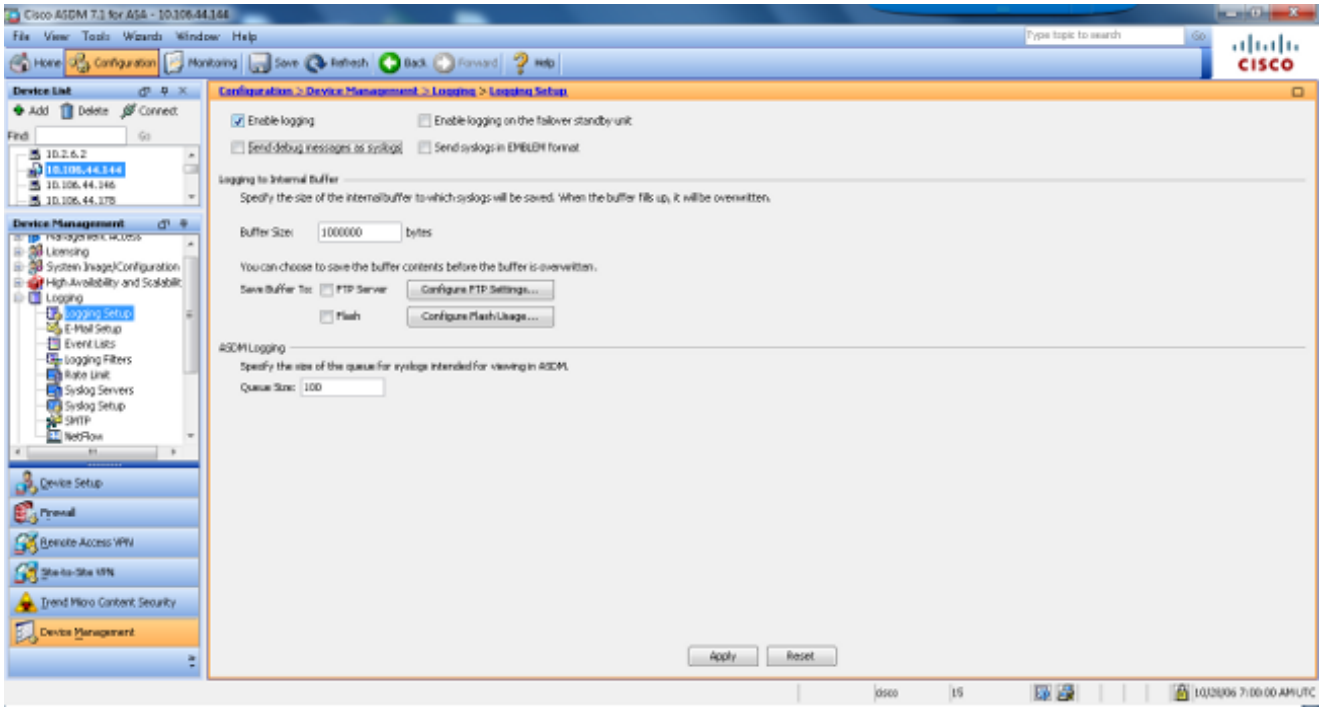
以下是示例输出。

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

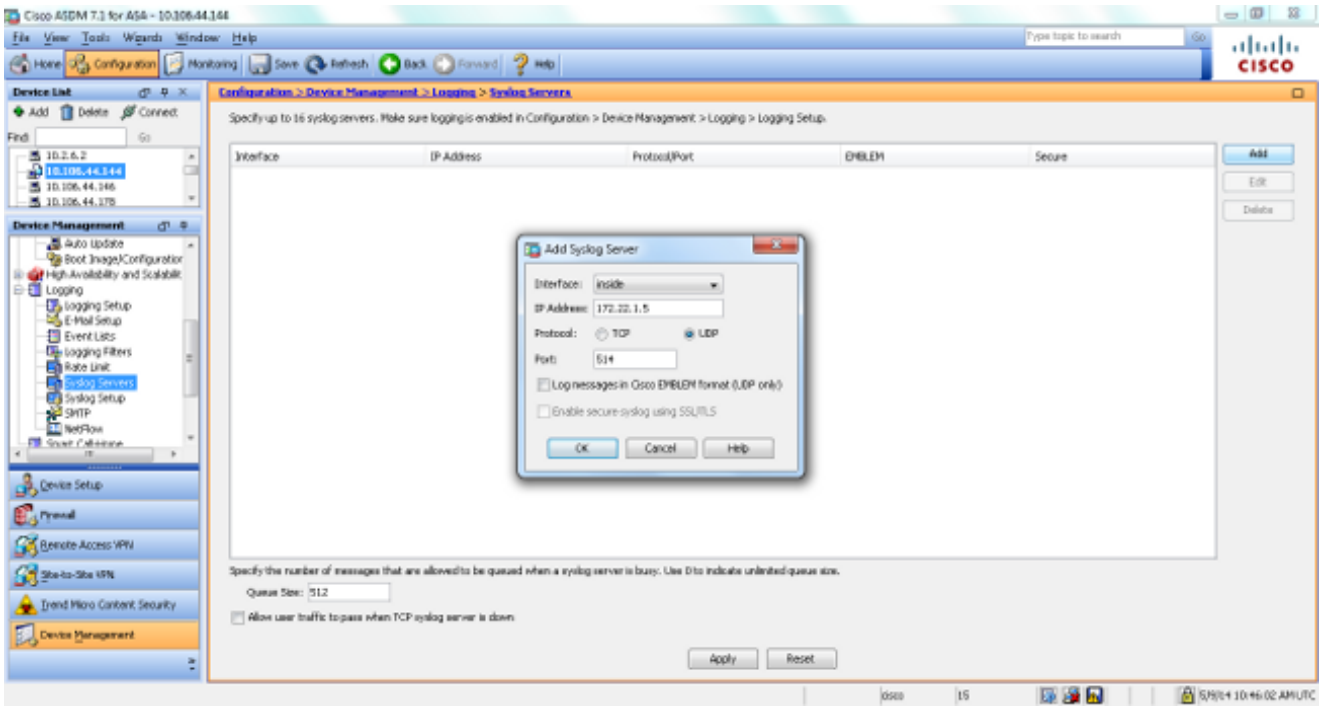
使用 ASDM 配置基本系统日志

此程序演示了针对所有可用系统日志目的地的 ASDM 配置。

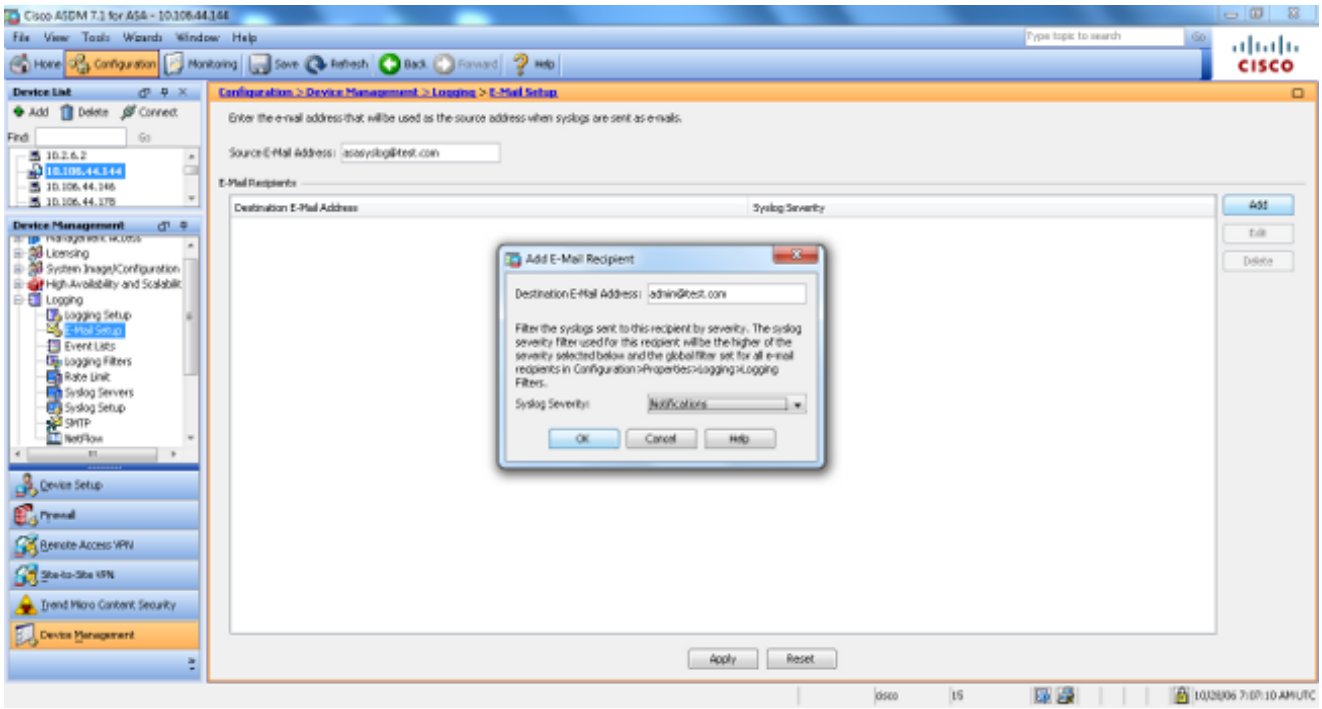
1. 要在 ASA 上启用日志记录，请先配置基本日志记录参数。选择 Configuration > Features > Properties > Logging > Logging Setup。选中启用日志记录复选框以启用系统日志。



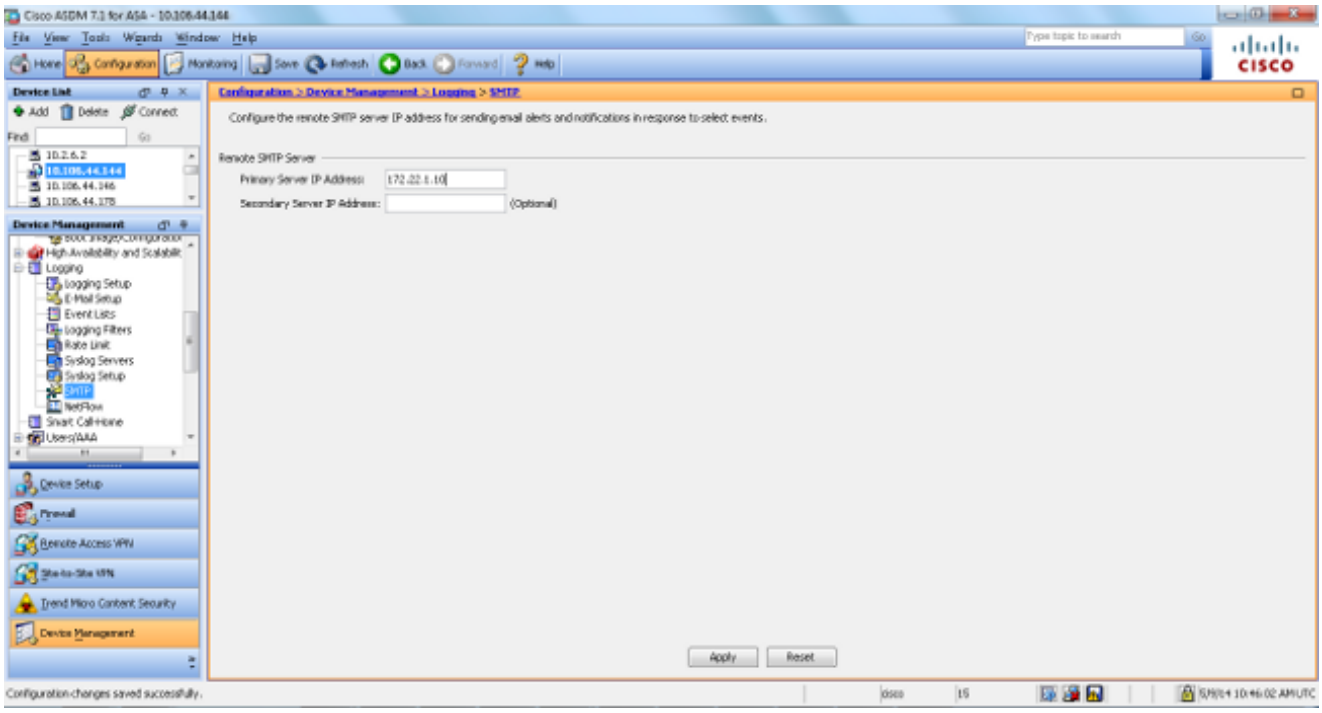
2. 要将外部服务器配置为系统日志的目的地，请在“日志记录”中选择系统日志服务器，然后点击添加以添加系统日志服务器。在 Add Syslog Server 框中输入 Syslog 服务器详细信息，并在完成后选择 OK。



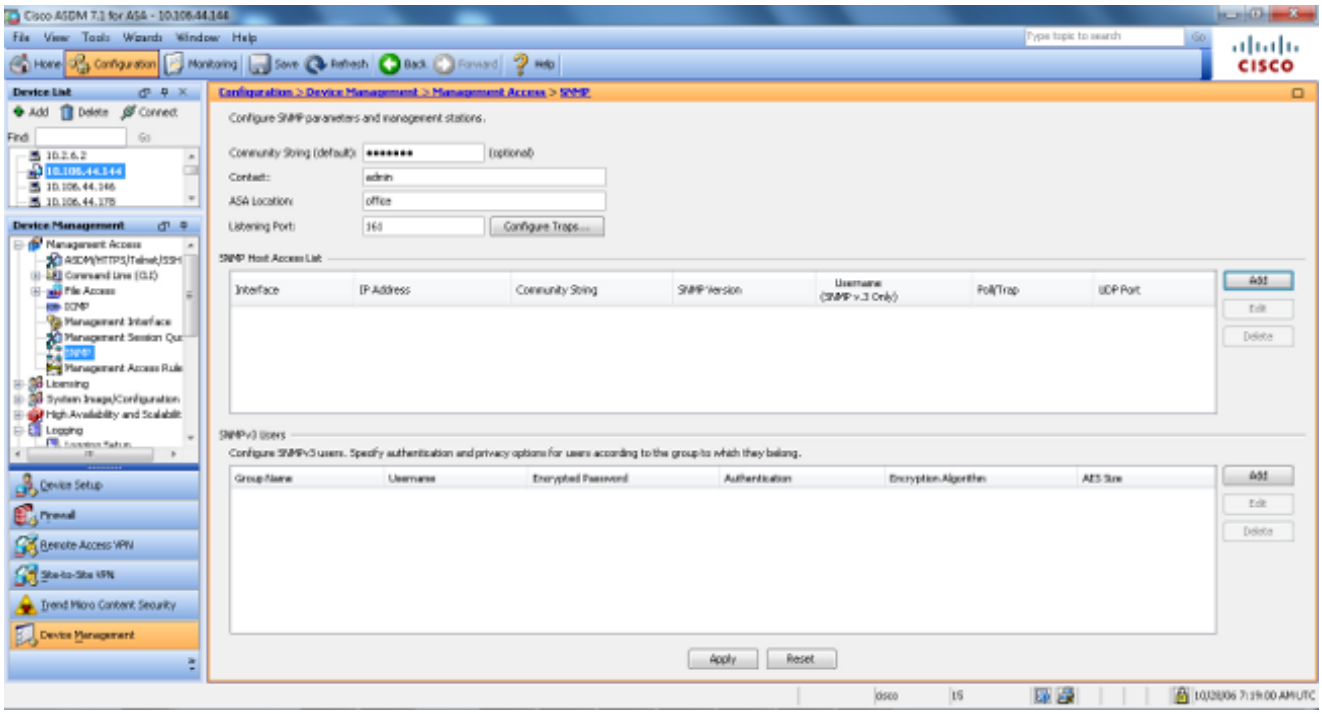
3. 在“日志记录”中选择邮件设置，以便将系统日志消息作为邮件发送给特定收件人。在 Source E-Mail Address 框中指定源电子邮件地址，并选择 Add 以配置电子邮件收件人的目标电子邮件地址和消息严重性级别。完成后单击 OK。



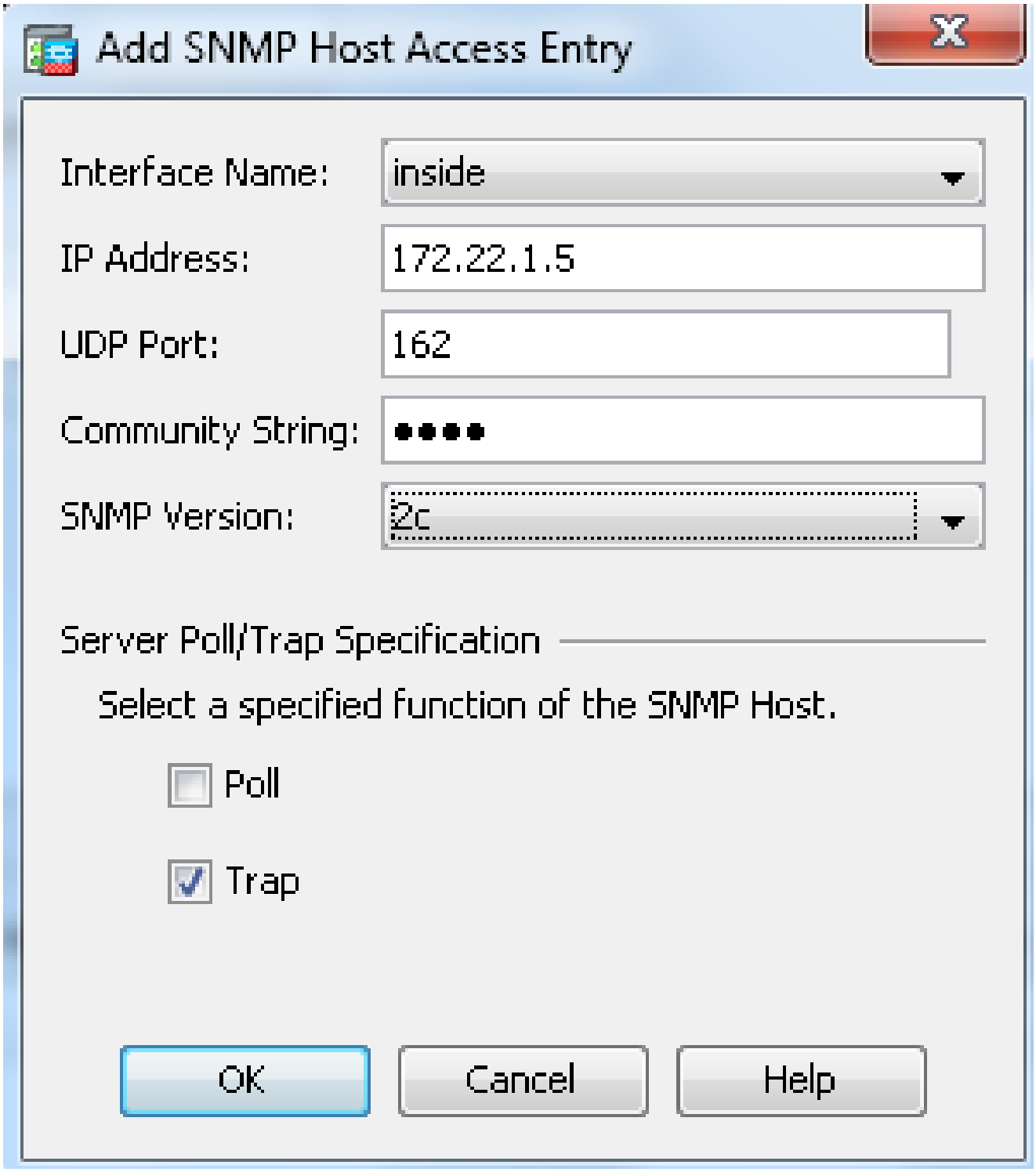
4. 依次选择设备管理、日志记录、SMTP，然后输入主服务器 IP 地址以指定 SMTP 服务器 IP 地址。



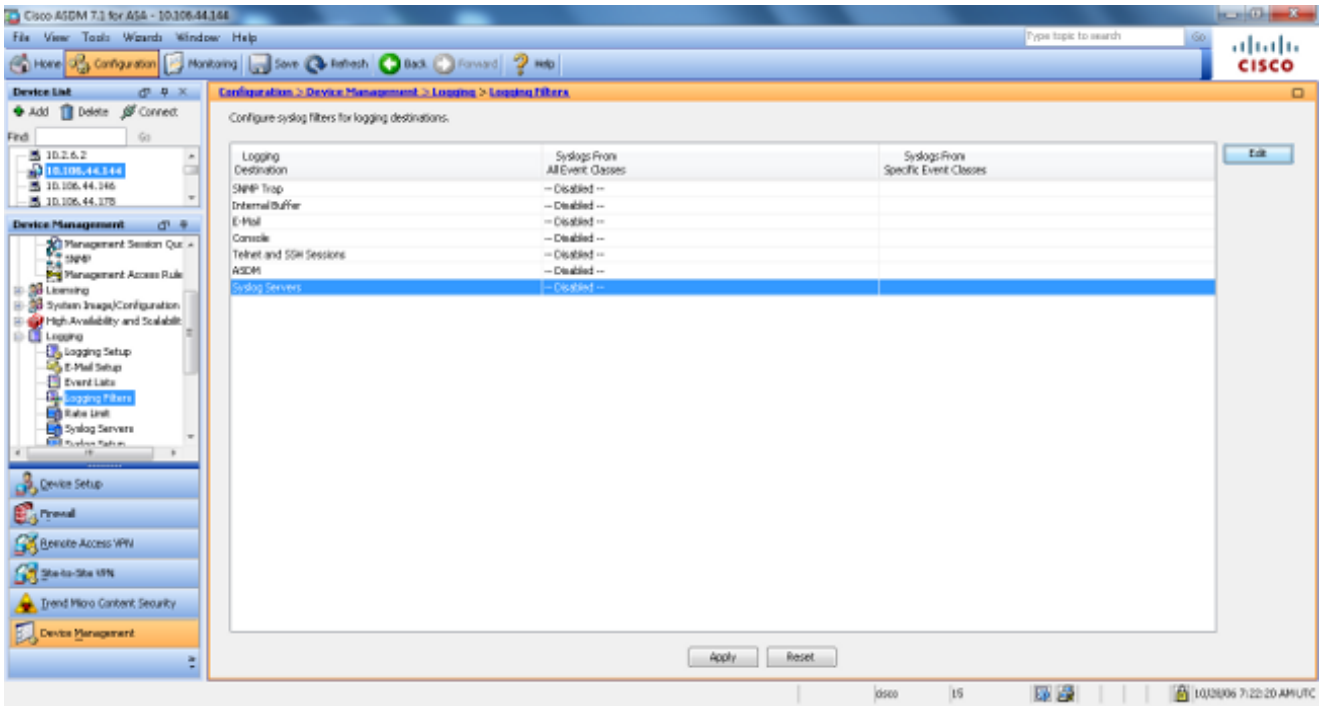
5. 如果要将系统日志作为 SNMP 陷阱发送，必须先定义 SNMP 服务器。在访问管理菜单中选择 SNMP，以指定 SNMP 管理站的地址及其具体属性。



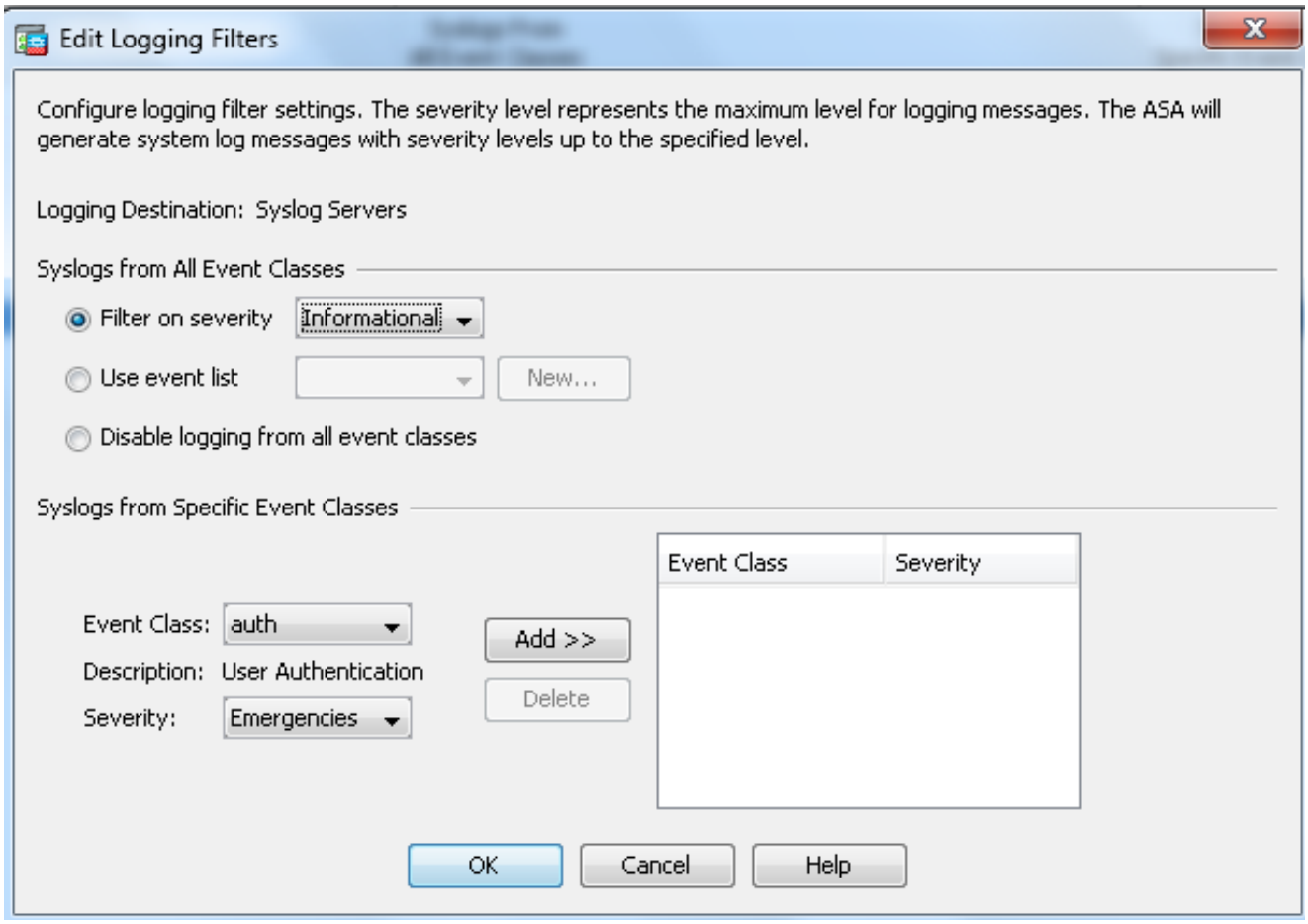
6. 选择 Add 以添加 SNMP 管理站。输入 SNMP 主机详细信息并单击 OK。



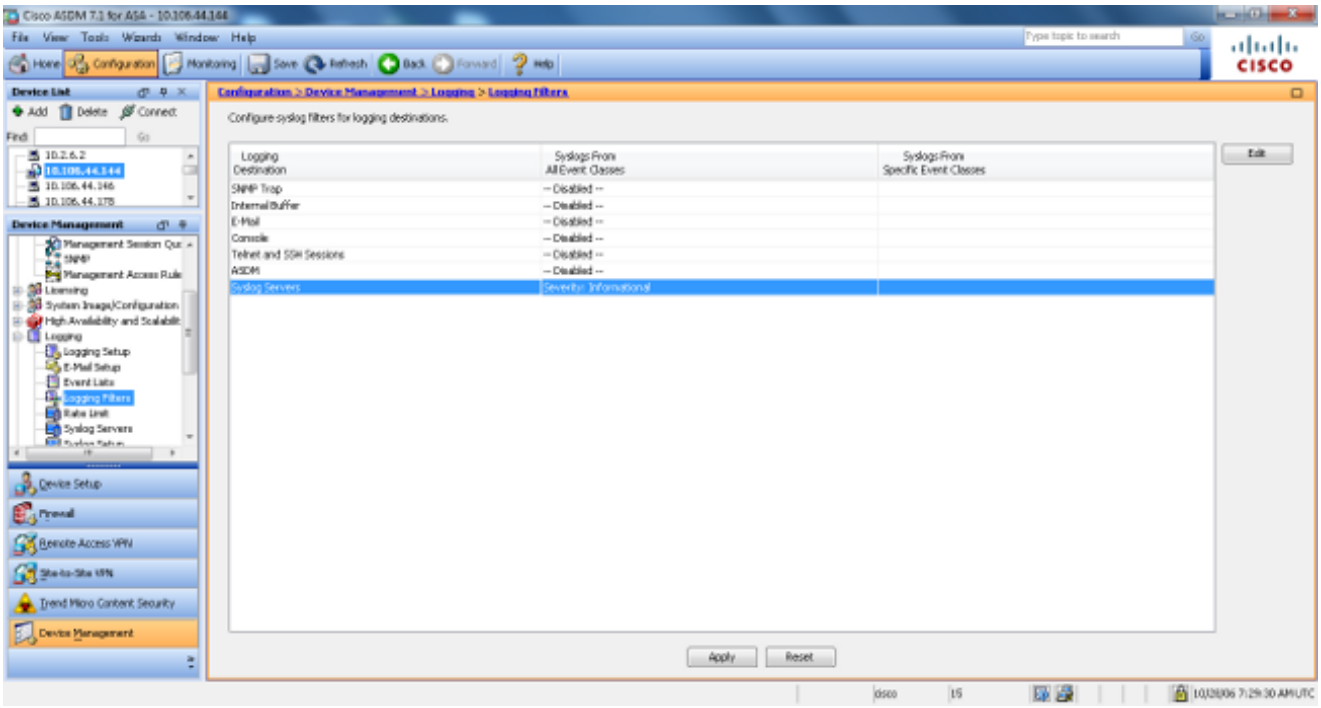
7. 要能够将日志发送到任何上述目的地，请在日志记录部分选择日志记录过滤器。这将为您提供每个可能的日志记录目的地，以及发送到这些目的地的当前级别日志。选择所需的日志记录目标并单击 Edit。在本示例中，修改了“系统日志服务器”的目的地。



8. 从按严重性筛选下拉列表中选择适当的严重性，本例中使用的严重性级别为说明性。完成后单击 OK。



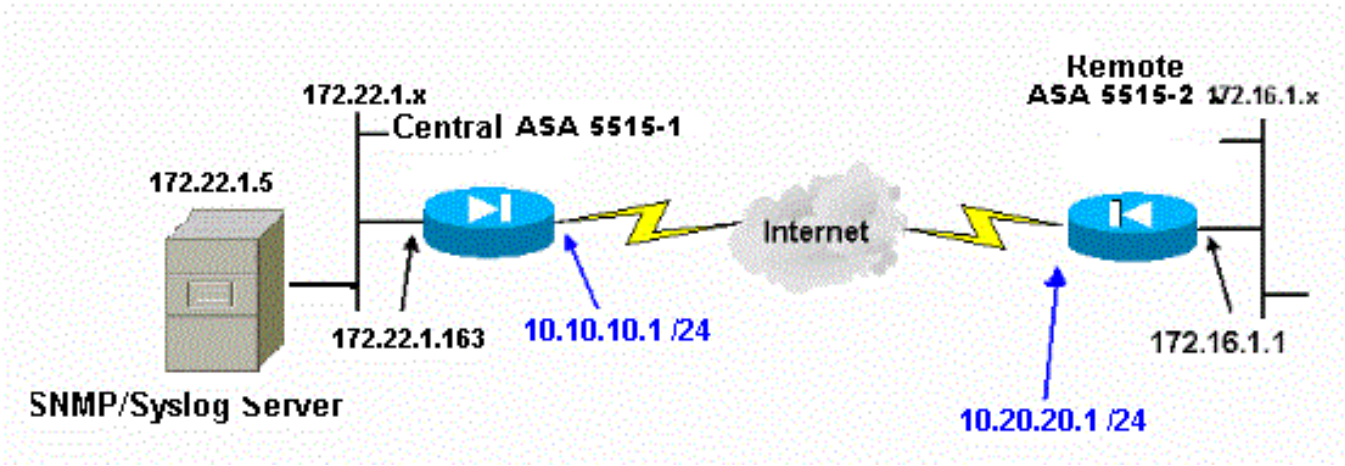
9. 返回 Logging Filters 窗口后，单击 Apply。



通过 VPN 将 Syslog 消息发送到 Syslog 服务器

在简单的站点到站点VPN设计或更复杂的中心辐射型设计中，管理员可能希望使用SNMP服务器和位于中心站点的syslog服务器监控所有远程ASA防火墙。

要配置站点到站点IPsec VPN配置，请参阅PIX/ASA 7.x及更高版本：PIX到PIX VPN隧道配置示例。除 VPN 配置外，还必须在中心和本地站点上都配置 SNMP 和 Syslog 服务器的相关数据流。



集中 ASA 配置

<#root>

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.
```

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


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


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



logging enable
logging trap debugging


!--- Define logging host information.

logging facility 16
logging host inside 172.22.1.5



!--- Define the SNMP configuration.

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


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

远程 ASA 配置

<#root>

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.

access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0


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

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

```
!--- Define syslog server.

logging facility 23
logging host outside 172.22.1.5


!--- Define SNMP server.

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

有关如何配置 ASA 版本 8.4 的详细信息，请参阅使用 SNMP 和系统日志通过 VPN 隧道监控思科安全 ASA 防火墙

高级 Syslog

ASA 版本 8.4 提供了多种机制，使您能够分组配置和管理系统日志消息。这些机制包括消息严重性级别、消息类、消息 ID 或您创建的自定义消息列表。通过使用这些机制，您可以输入应用于小或大组消息的单一命令。通过这种方式设置 Syslog 后，您可以捕获指定消息组中的消息而不再是同一严重性级别的所有消息。

使用消息列表

使用消息列表可以按严重性级别和 ID，仅将感兴趣 Syslog 消息包含在某个组中，然后将此消息列表与所需目标关联。

要配置消息列表，请完成以下步骤：

1. 输入 logging list message_list | level severity_level [class message_class] 命令以创建包括具有指定严重性级别或消息列表的消息的消息列表。
2. 输入 logging list message_list message syslog_id-syslog_id2 命令以向刚创建的消息列表中添加另外的消息。
3. 输入 logging destination message_list 命令以指定创建的消息列表的目标。

示例 2

输入以下命令以创建消息列表，其中包括所有严重性为 2（严重）的消息以及编号为 611101 至 611323 的消息，并将它们发送到控制台：

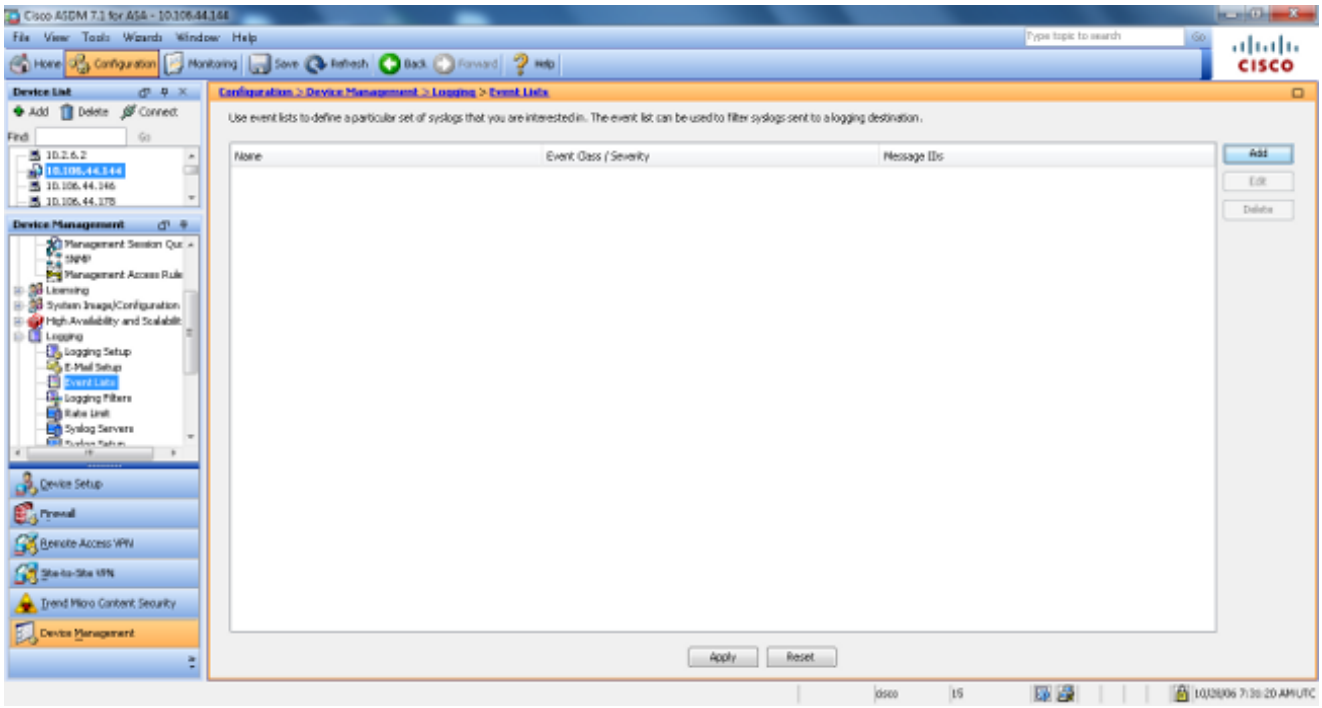
<#root>

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

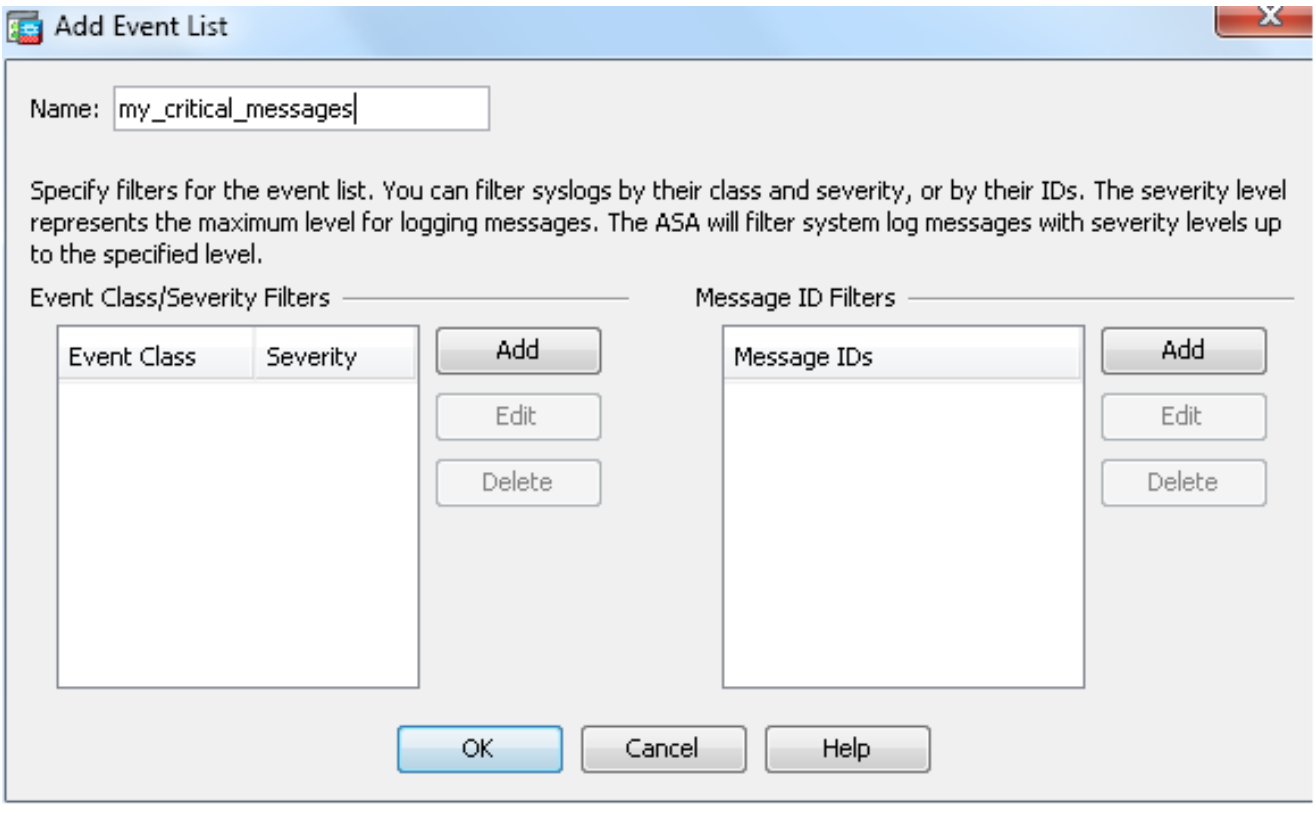
ASDM 配置

此过程显示使用消息列表的示例 2 的 ASDM 配置。

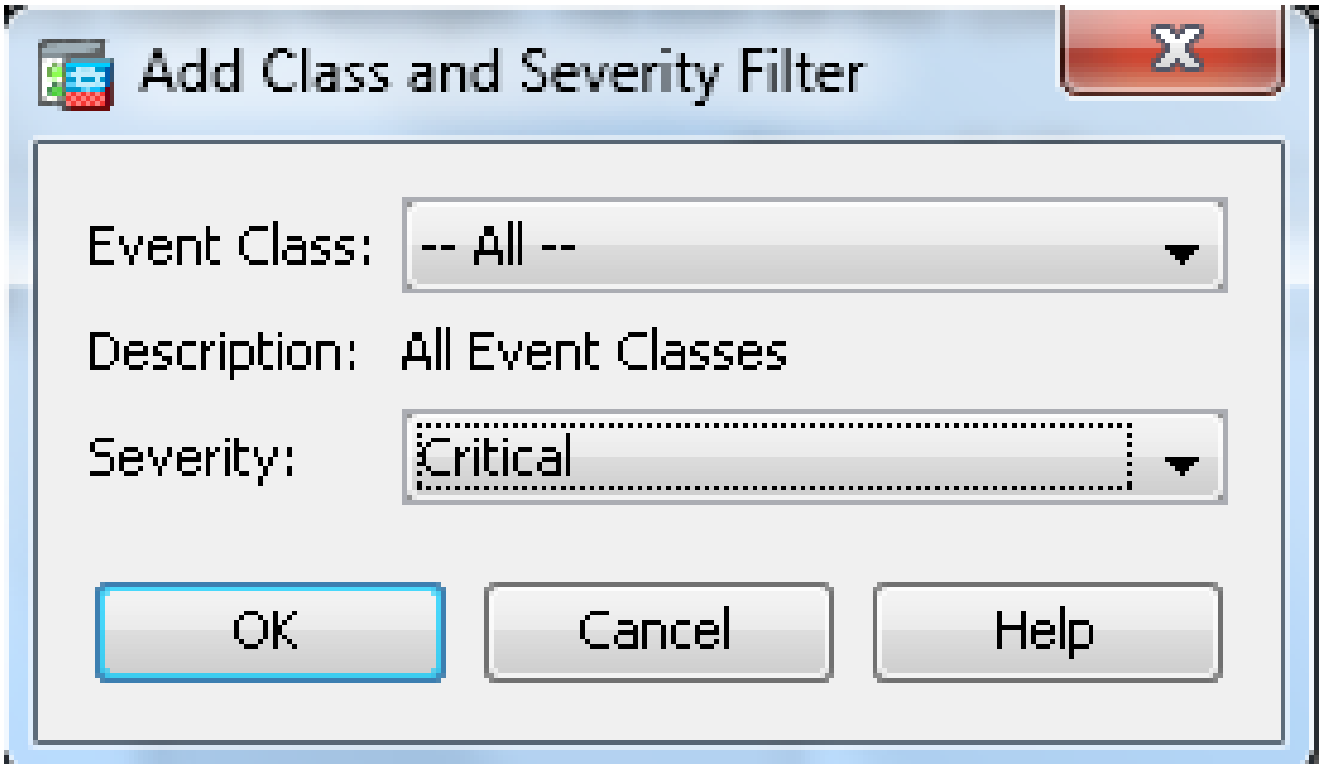
1. 选择 Logging 下的 Event Lists，并单击 Add 以创建消息列表。



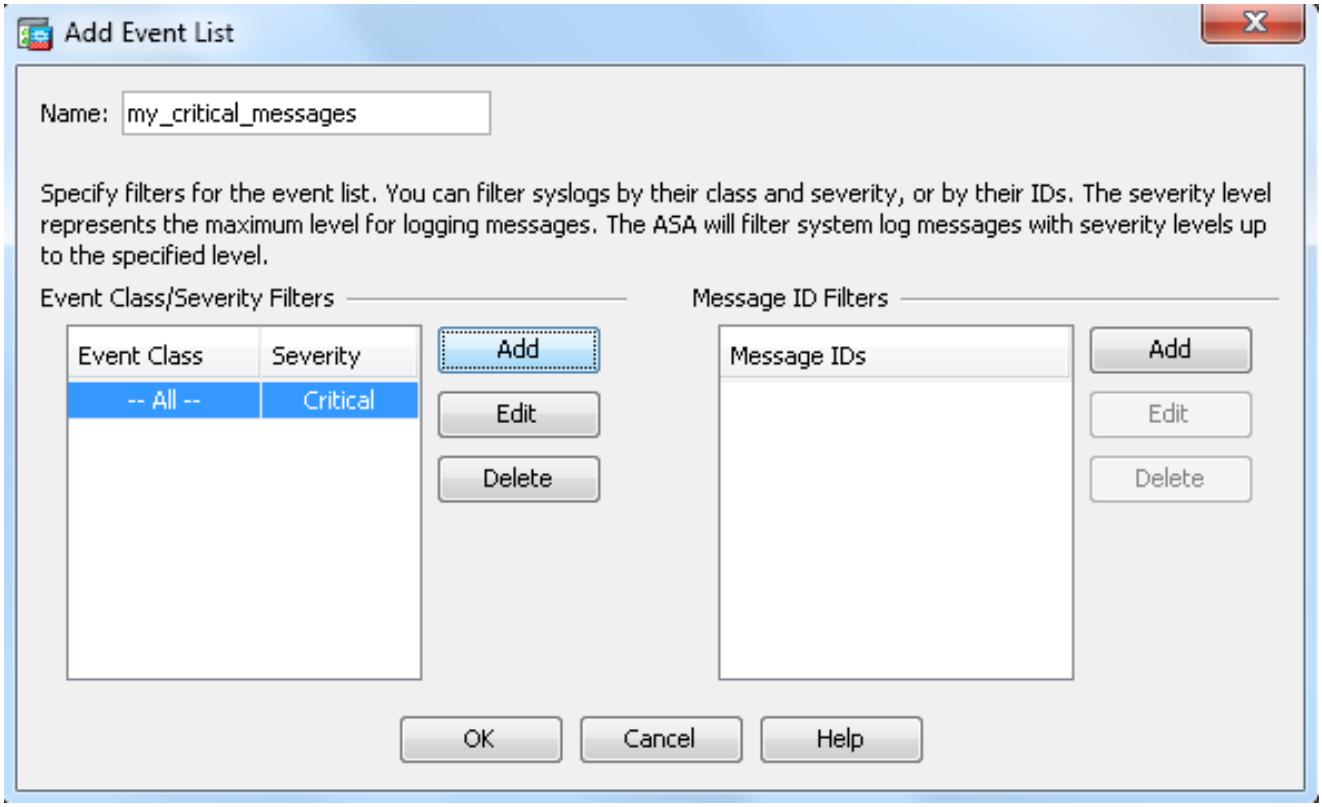
2. 在 Name 框中输入消息列表的名称。在本例中，使用 my_critical_messages。单击 Event Class/Severity Filters 下的 Add。



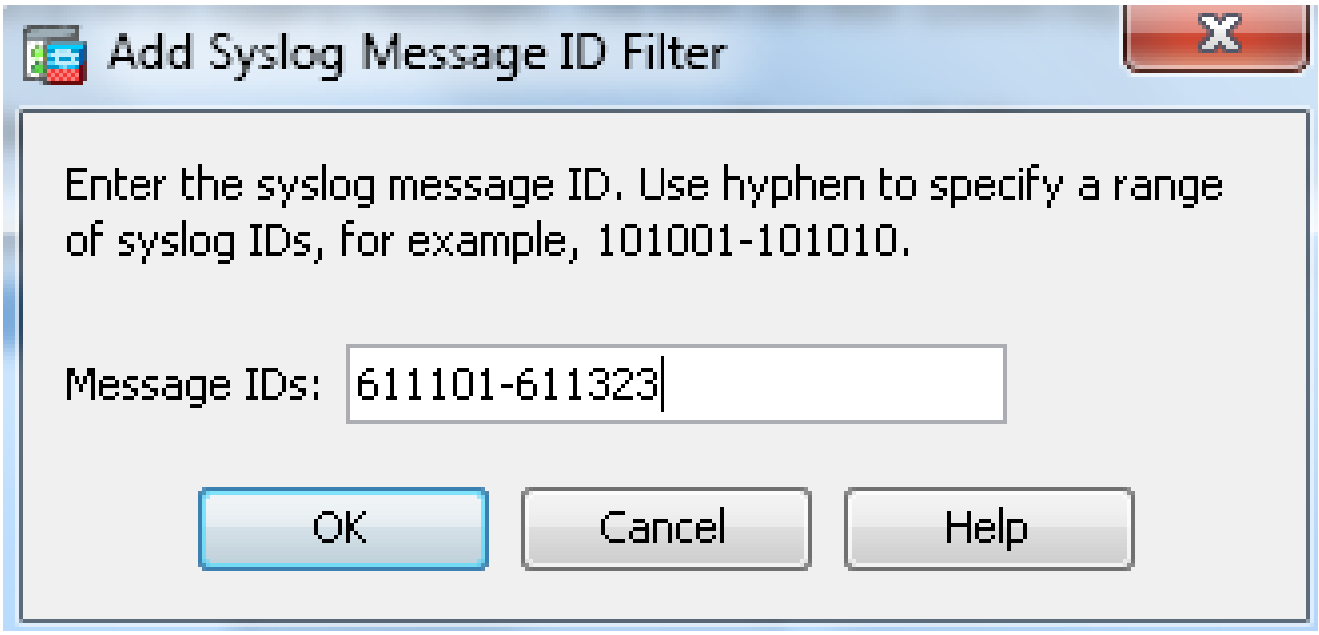
3. 从“事件类”下拉列表中选择全部。从“严重性”下拉列表中选择严重。完成后单击 OK。



4. 如果需要另外的消息，请单击 Message ID Filters 下的 Add。在本例中，您需要输入 ID 介于 611101-611323 之间的消息。

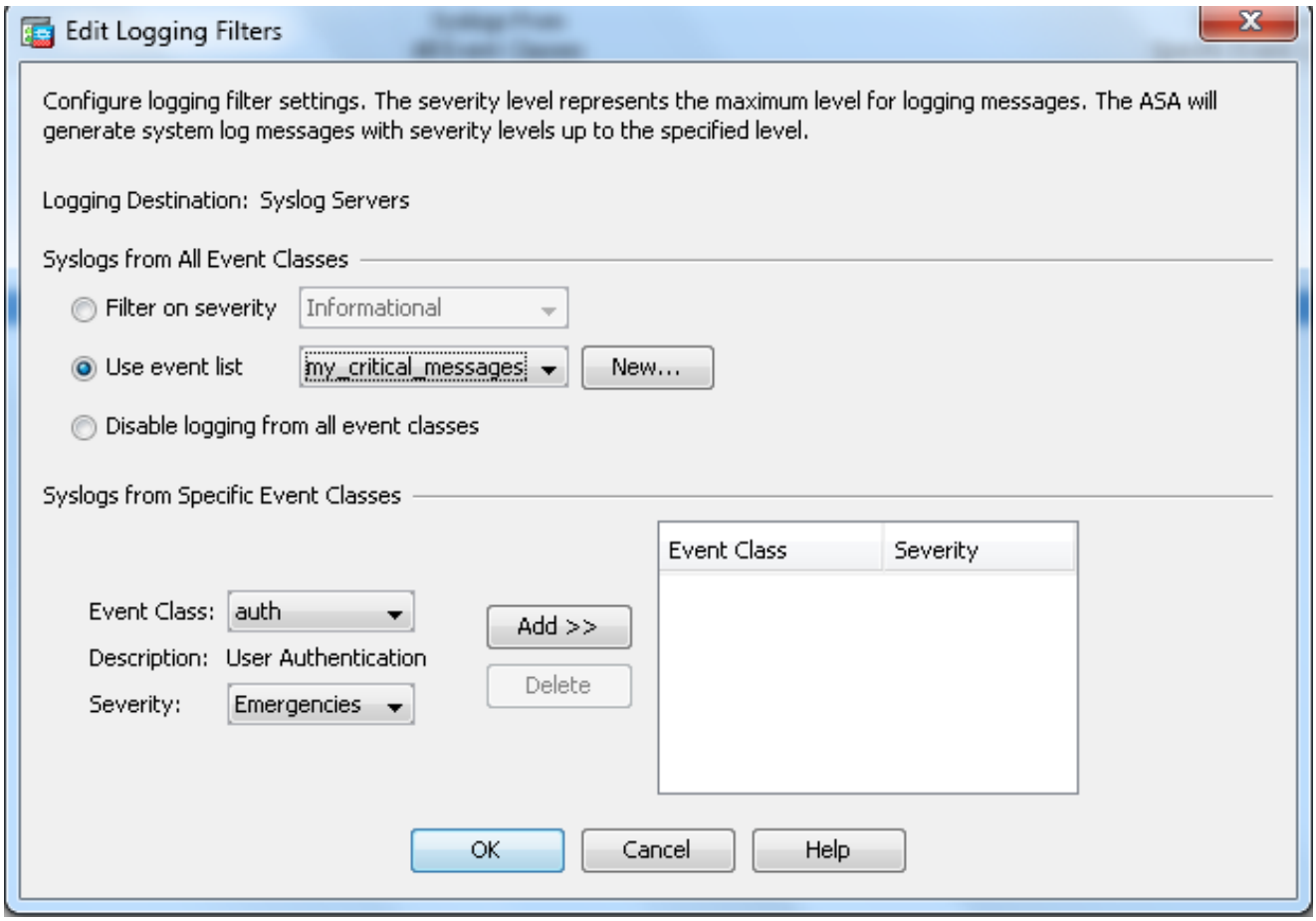


5. 在 Message IDs 框中输入 ID 范围并单击 OK。

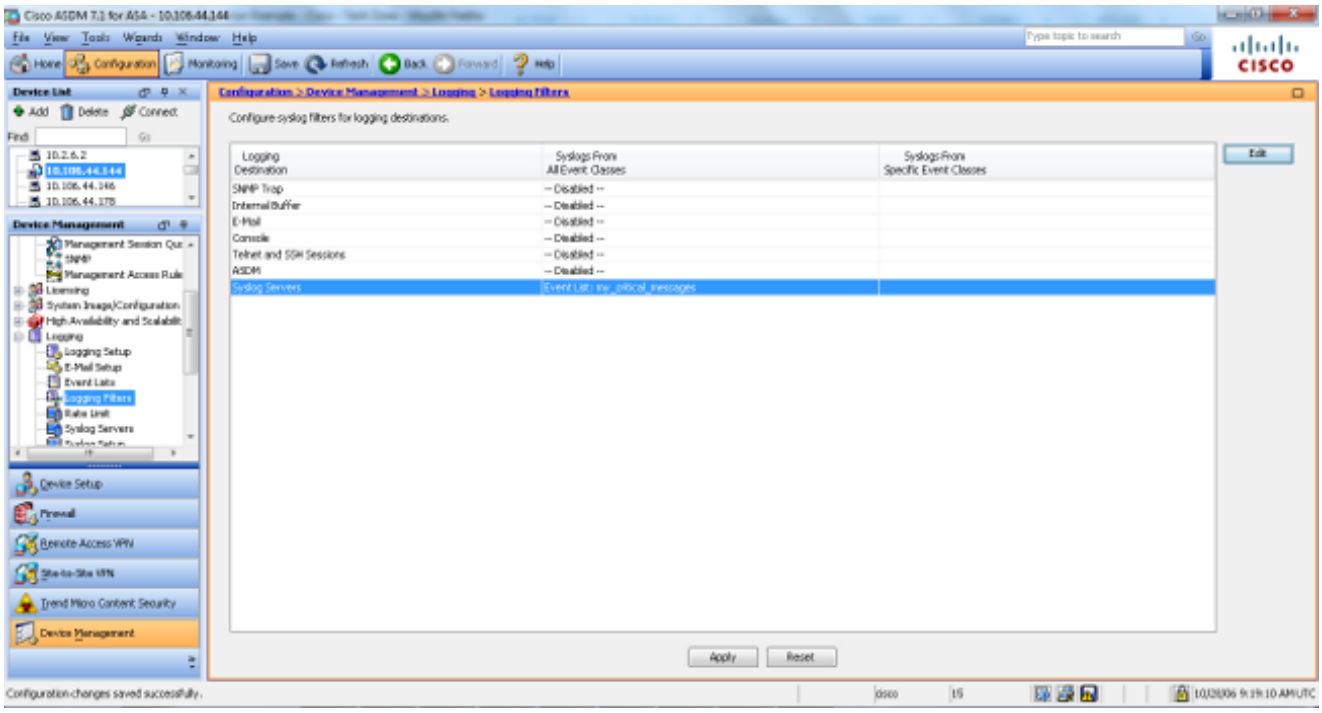


6. 返回 Logging Filters 菜单并选择 Console 作为目标。

7. 从使用事件列表下拉列表中选择 my_critical_messages。完成后单击 OK。



8. 返回 Logging Filters 窗口后，单击 Apply。



这将通过使用示例 2 中所示的消息列表完成 ASDM 配置。

使用消息类

使用消息类可以将与一个类关联的所有消息发送到指定的输出位置。指定严重性级别阈值时，可以限制发送到输出位置的消息数。

<#root>

logging class

 message_class destination | severity_level

示例 3

输入以下命令以将严重性级别为“紧急”或更高级别的所有 ca 类消息发送到控制台。

<#root>

logging class ca console emergencies

ASDM 配置

此程序显示了对应于使用消息列表的示例 3 的 ASDM 配置。

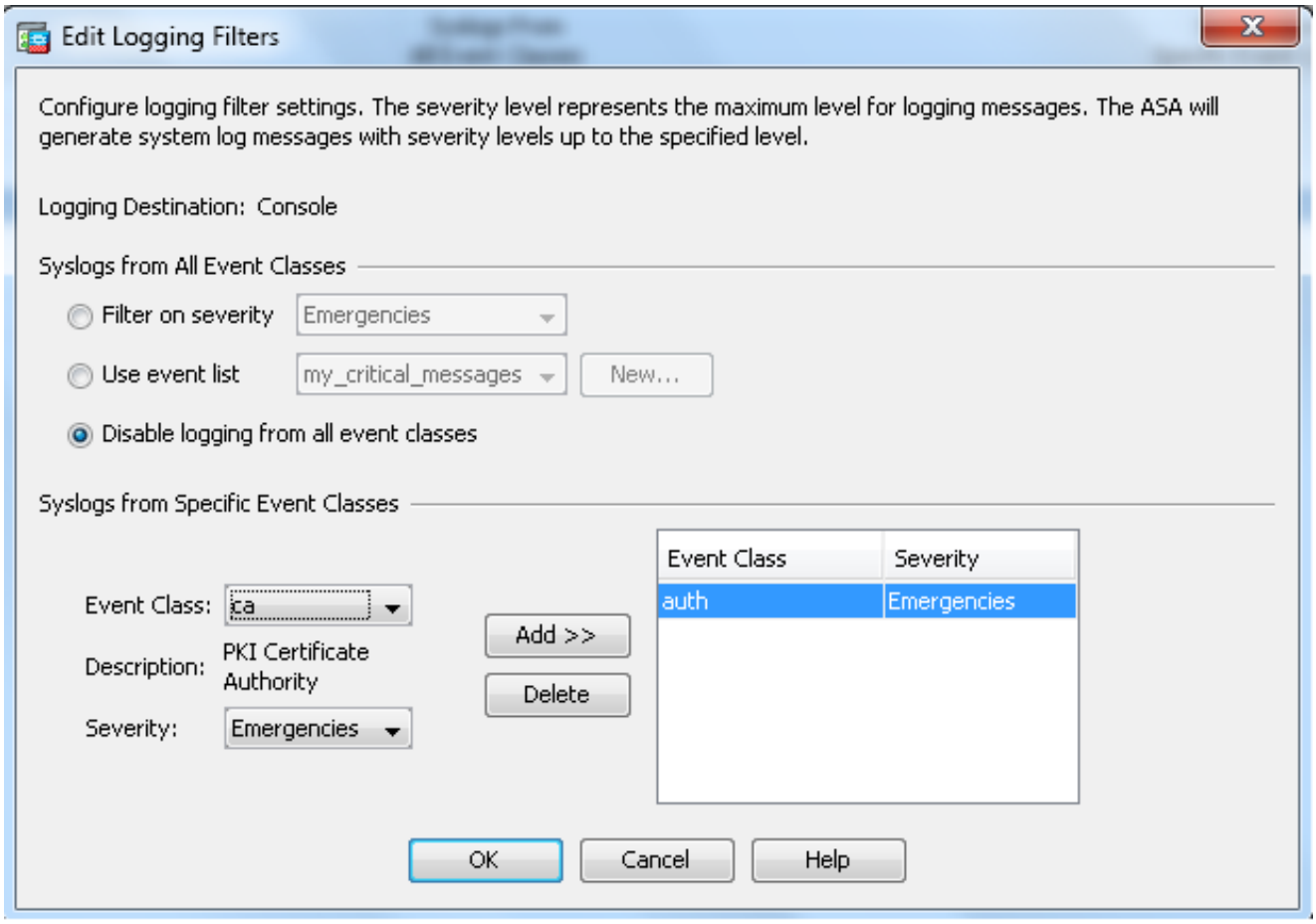
1. 选择 Logging Filters 菜单并选择 Console 作为目标。

2. 单击 Disable logging from all event classes。

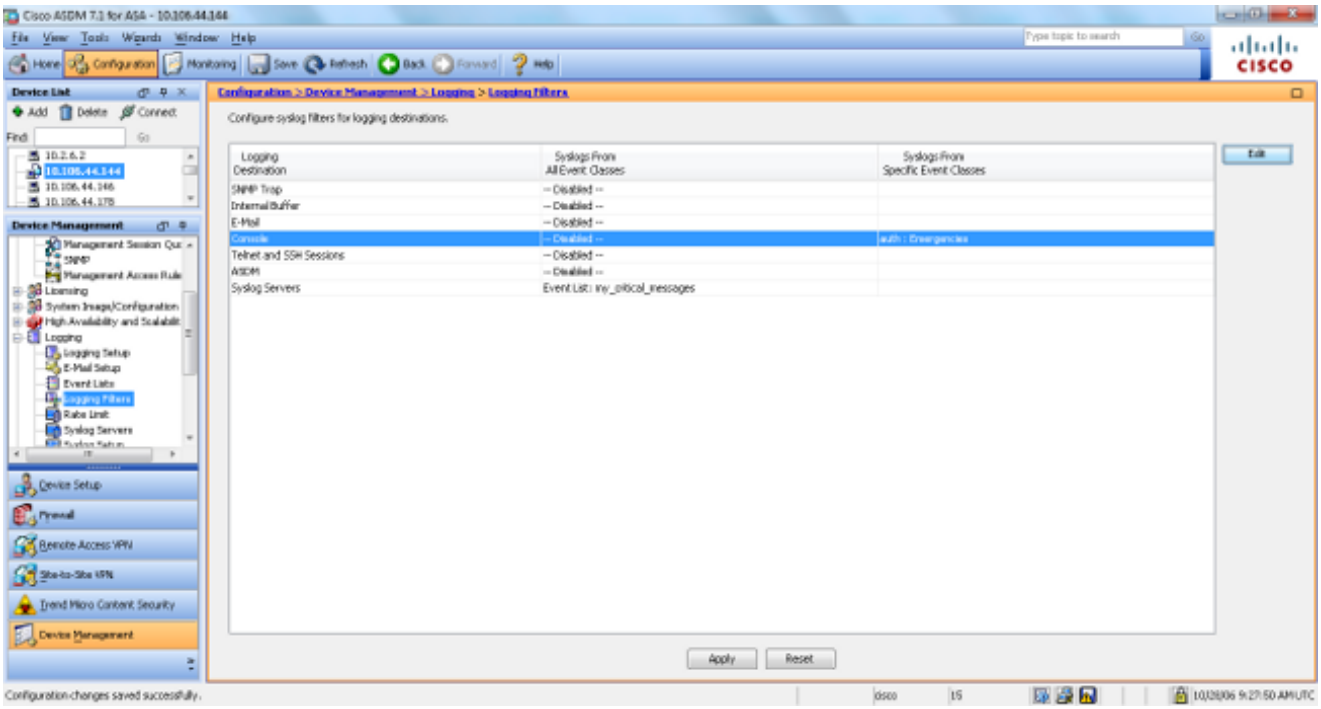
3. 在 Syslogs from Specific Event Classes 下，选择要添加的事件类和严重性。

   此过程分别使用 ca 和 Emergencies。

4. 单击 Add 以将此添加到消息类中并单击 OK。



5. 返回 Logging Filters 窗口后，单击 Apply。控制台现在将收集严重性级别为“紧急”的 ca 类消息，如“日志记录过滤器”窗口中所示。



这将完成示例 3 的 ASDM 配置。有关日志消息严重性级别的列表，请参阅[按严重性级别列出的消息。](#)

将调试日志消息发送到系统日志服务器

要执行高级故障排除，需要使用特定于功能/协议的调试日志。默认情况下，这些日志消息将显示在终端 (SSH/Telnet) 上。根据调试类型和调试消息生成速率，如果启用调试，使用CLI可能会比较困难。或者，可以将调试消息重定向到系统日志进程并生成为系统日志。像其他系统日志一样，这些系统日志也可以发送到任何系统日志目标。要将调试转移到系统日志，请输入 logging debug-trace 命令。此配置会将调试输出作为系统日志发送到系统日志服务器。

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

同时使用日志记录列表和消息类

输入 logging list 命令，以便仅捕获 LAN 对 LAN 和远程访问 IPsec VPN 消息的系统日志。本示例捕获具有“调试”级别或更高级别的所有 VPN（IKE 和 IPsec）类系统日志消息。

示例

```
<#root>

hostname(config)#

logging enable
```

```
hostname(config)#
logging timestamp

hostname(config)#
logging list my-list level debugging class vpn

hostname(config)#
logging trap my-list

hostname(config)#
logging host inside 192.168.1.1
```

记录 ACL 命中数

将日志添加到您需要的每个访问列表元素 (ACE) 中，以便在命中访问列表时进行记录。使用以下语法：

<#root>

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

示例

<#root>

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

默认情况下，ACL 会记录每个被拒绝的数据包。无需向 deny ACL 中添加日志选项即可为被拒绝的数据包生成系统日志。当指定 log 选项时，它将为其应用到的 ACE 生成 Syslog 消息 106100。系统会为通过 ASA 防火墙的每个匹配的允许或拒绝 ACE 流生成 106100 系统日志消息。将缓存第一个匹配流。后续匹配会增加 show access-list 命令中显示的命中计数。默认访问列表日志记录行为（未指定 log 关键字）是：如果数据包被拒绝，则生成消息 106023，如果数据包被允许，则不生成任何 Syslog 消息。

可以为生成的 Syslog 消息 (106100) 指定可选 Syslog 级别 (0 - 7)。如果未指定级别，则为新 ACE 使用默认级别 6（信息性）。如果 ACE 已存在，则其当前日志级别保持不变。如果指定 log disable 选项，则将完全禁用访问列表日志记录。不生成任何Syslog消息，包括消息106023。log default 选项将还原默认访问列表日志记录行为。

要使 Syslog 消息 106100 可以显示在控制台输出中，请完成以下步骤：

1. 输入 logging enable 命令以将系统日志消息传输到所有输出位置。必须设置日志记录输出位置才能查看任何日志。
2. 输入 logging message<message_number> level <severity_level> 命令，以设置特定系统日志消息的严重性级别。

   在此示例中，输入 logging message 106100 命令以启用 106100 消息。
3. 输入 logging console message_list | severity_level 命令以使系统日志消息可以在发生时显示在安全设备控制台 (tty) 上。将 severity_level 设置为从 1 到 7 的值或使用级别名称。还可以使用 message_list 变量指定要发送的消息。
4. 输入 show logging message 命令，以显示已从默认设置修改为其他设置的系统日志消息列表，这些消息是已分配了不同严重性级别的消息和已禁用的消息。

   以下是 show logging message 命令的示例输出：

```
<#root>

ASAfirewall#

show logging message 106100


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

阻止在备用 ASA 上生成系统日志

从ASA软件版本9.4.1开始，您可以阻止在备用设备上生成特定系统日志，然后使用以下命令：

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

验证

当前没有可用于此配置的验证过程。

故障排除

如果要禁止将特定系统日志消息发送到系统日志服务器，则必须输入所示命令。

<#root>

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

有关详细信息，请参阅 logging message 命令。

%ASA-3-201008：禁止新连接

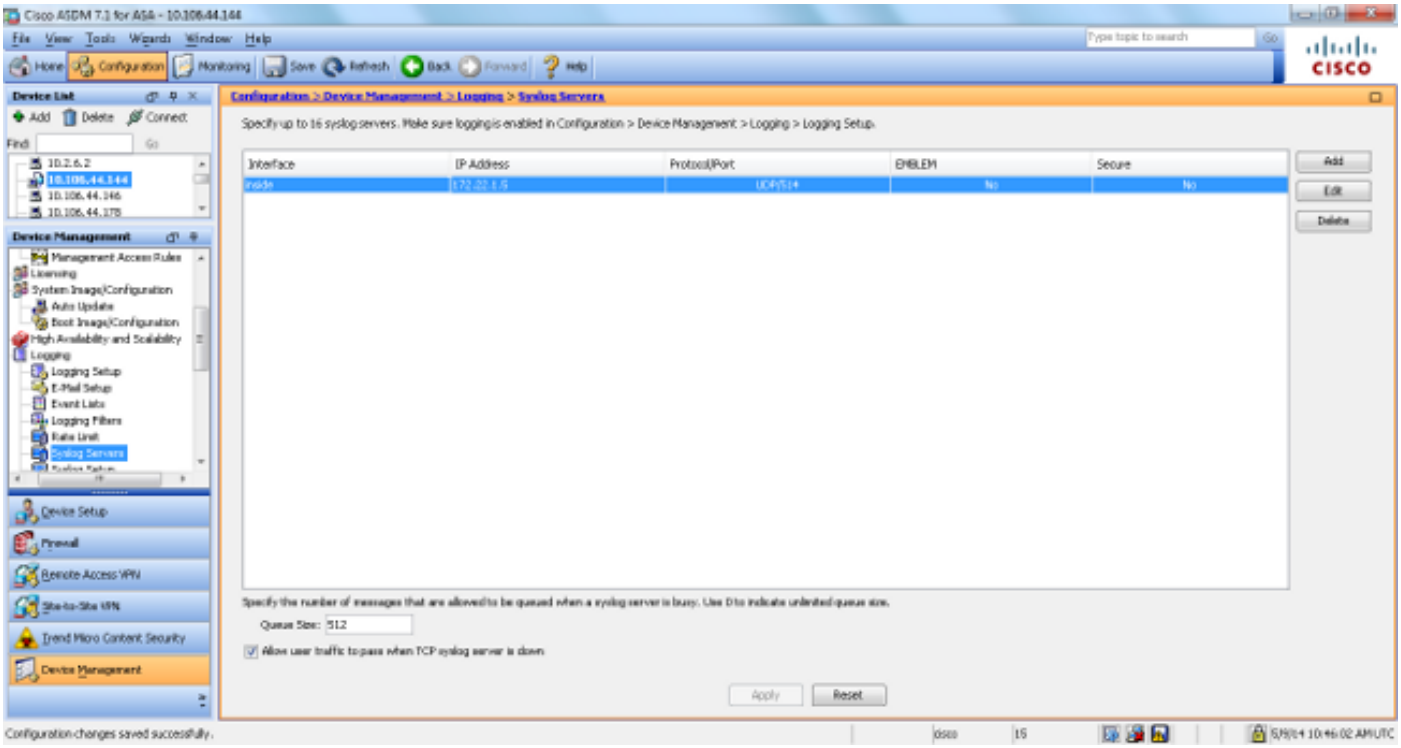
当ASA无法联系系统日志服务器并且不允许新连接时，会显示%ASA-3-201008：禁止新连接。错误消息。

解决方案

当您已启用 TCP 系统日志消息但无法到达 Syslog 服务器时，或当您使用 Cisco ASA Syslog 服务器 (PFSS) 并且 Windows NT 系统上的磁盘已满时，将显示此消息。要解决此错误消息，请完成以下步骤：

- 如果已启用 TCP 系统日志消息，请禁用它。
- 如果使用 PFSS，请释放 Windows NT 系统上 PFSS 所在的空间。
- 确保系统日志服务器已启动并且您可以从 ASA 控制台 Ping 通主机。
- 重新启动 TCP 系统消息日志记录以允许数据流。

如果系统日志服务器关闭并且已配置了 TCP 日志记录，请使用 logging permit-hostdown 命令或者切换到 UDP 日志记录。



相关信息

- Cisco Secure PIX 防火墙命令参考
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。