

# ASA 8.2 : 使用ASDM , 配置Syslog

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[通过使用ASDM的基本Syslog配置](#)

[启用日志](#)

[禁用记录](#)

[对电子邮件的记录日志](#)

[对系统日志服务器的记录日志](#)

[通过使用ASDM的先进的Syslog配置](#)

[工作与事件列表](#)

[工作用记录日志过滤器](#)

[丢包率限制](#)

[记录访问规则的命中数](#)

[配置](#)

[配置](#)

[验证](#)

[故障排除](#)

[问题：丢失的连接--终止的Syslog连接--](#)

[解决方案](#)

[不能查看实时注册思科ASDM](#)

[解决方案](#)

[相关信息](#)

## 简介

本文提供信息关于怎样配置在思科可适应安全工具(ASA)通过使用可适应安全设备管理器(ASDM) GUI , 8.x的Syslog。系统日志信息是思科ASA生成的消息通知所有变化的管理员在配置、变化在网络设置上或者变化上在设备的性能上。通过分析系统日志信息 , 管理员能容易地排除故障错误由执行根本原因分析。

系统消息主要被区分根据他们的严重级别。

1. 严重性0-Emergency消息-资源是不可用的
2. 严重性1-警报消息-即时动作是需要的
3. 严重性2-Critical消息-严重情况
4. 严重性3-Error Messages错误情况

5. 严重性4-Warning消息-警告情况
6. 严重性5-通知消息-正常，但是重要状况
7. 严重性6-Informational消息-仅供参考消息
8. 严重性7-调试消息-仅调试消息**注意**：最高的严重级别是紧急，并且最低的严重级别调试。

思科ASA生成的示例系统消息表示此处：

- %ASA-6-106012 : 拒绝IP从Ip\_address到Ip\_address , Ip options十六进制。
- %ASA-3-211001 : 内存分配错误
- %ASA-5-335003 : 应用的美洲台默认ACL , ACL : ACL名称-主机地址

数值在"%ASA-X-YYYYYY指定的x："，表示消息的严重性。例如，"%ASA-6-106012"是供参考消息，并且"%ASA-5-335003"是错误消息。

## 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：

- Cisco ASA版本8.2
- Cisco ASDM版本6.2

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

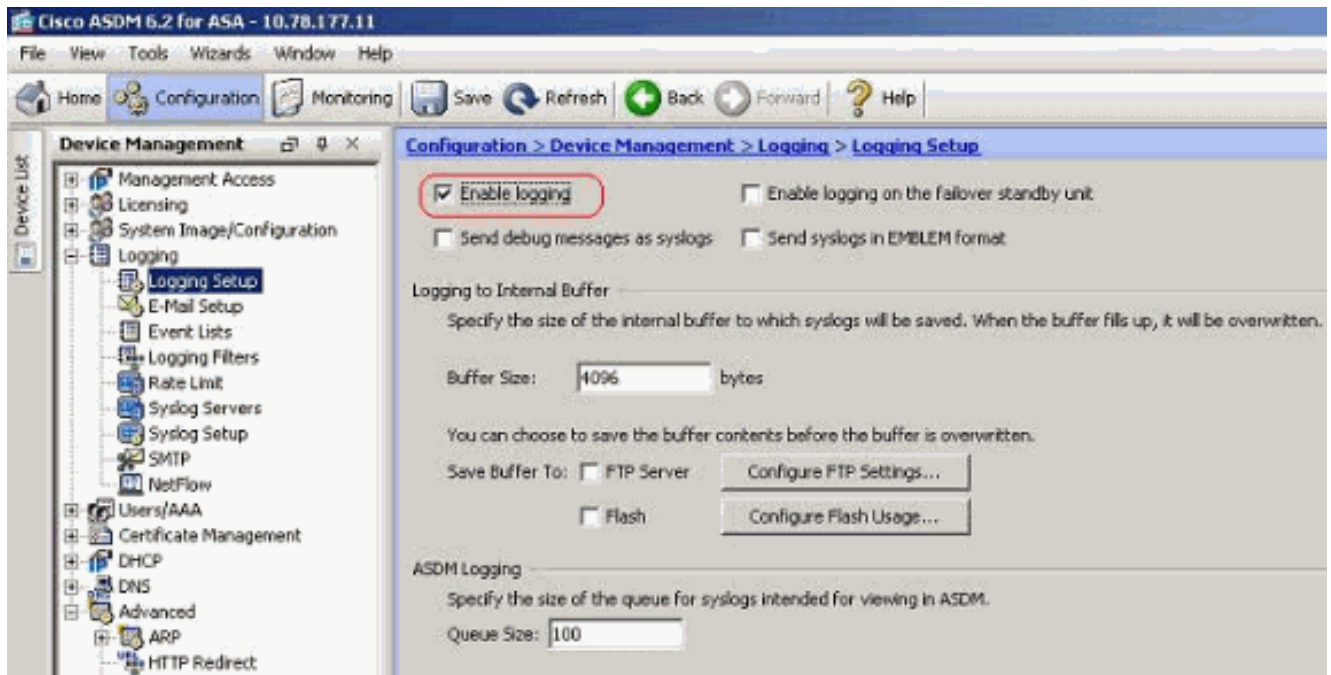
有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 通过使用ASDM的基本Syslog配置

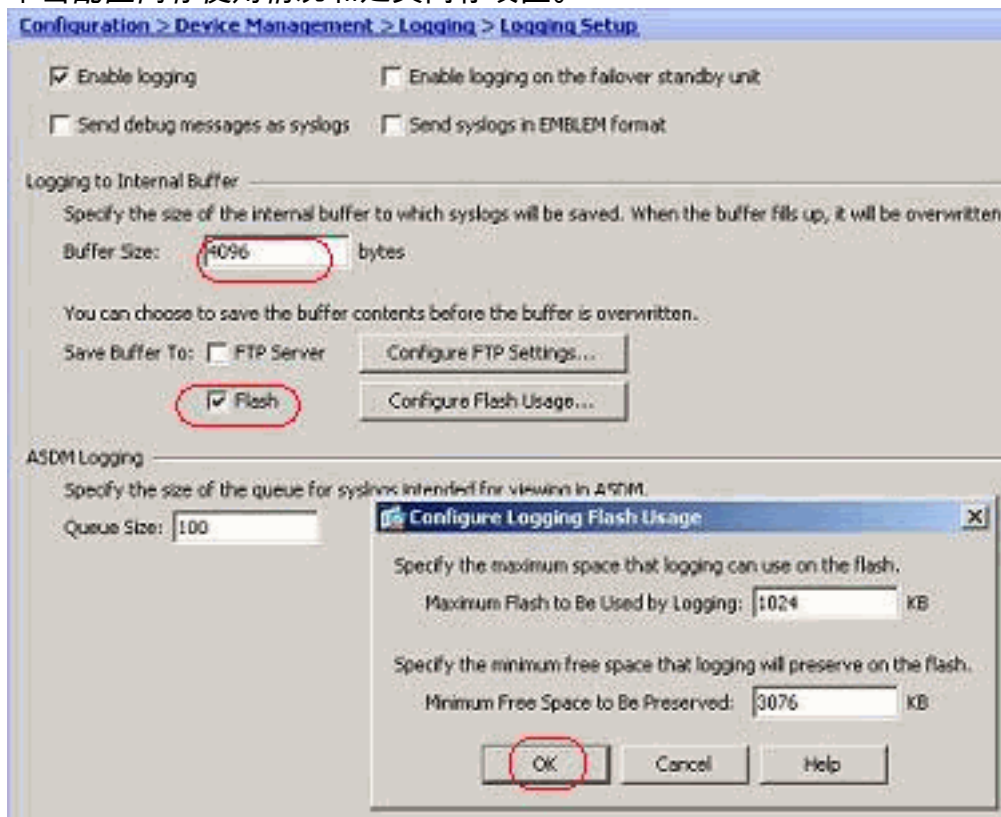
### 启用日志

完成这些步骤：

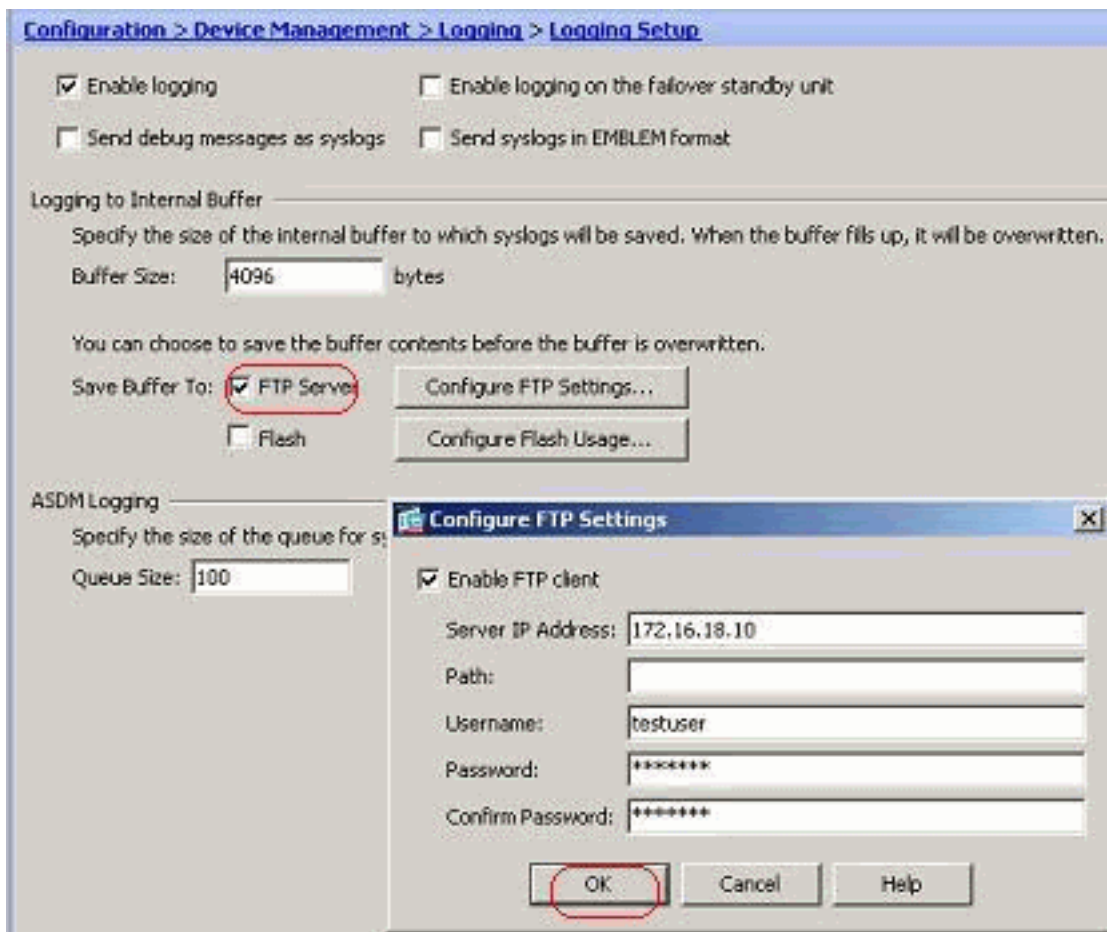
1. 选择 *Configuration*>设备管理>记录日志>记录日志设置的和复选标记启用日志选项。



2. 您能记录系统消息到内部缓冲器通过指定缓冲区大小。您能也选择保存缓冲区内容到闪存通过单击配置闪存使用情况和定义闪存设置。



3. 在他们覆盖前，缓冲日志消息可以传送到FTP服务器。单击配置FTP设置并且指定FTP服务器详细信息如显示此处

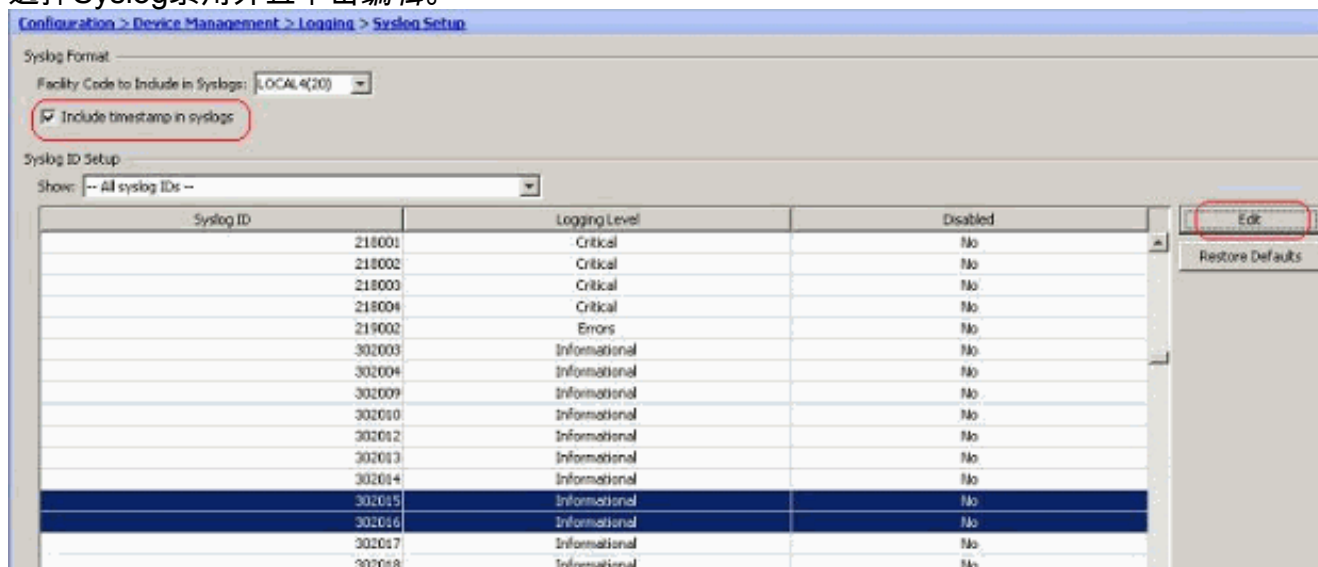


## 禁用记录日志

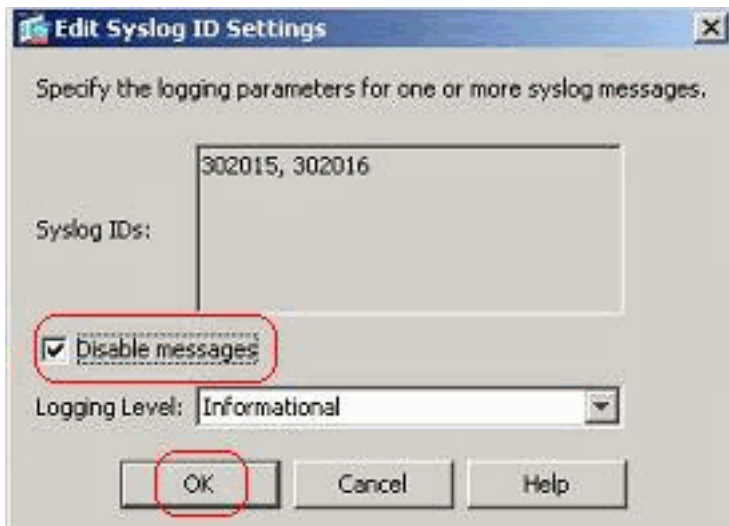
您能禁用根据您的需求的特定Syslog ID。

**注意：** 通过选择包括时间戳的复选标记在Syslog选项，您能添加日期和时间他们生成作为Syslog的一个字段。

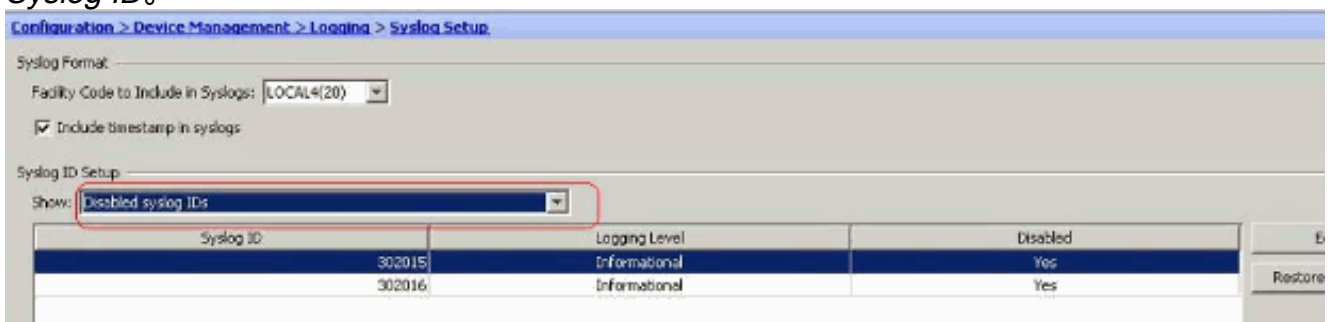
1. 选择Syslog禁用并且单击编辑。



2. 从Settings窗口编辑Syslog的ID，复选标记禁用消息选项和点击OK键。



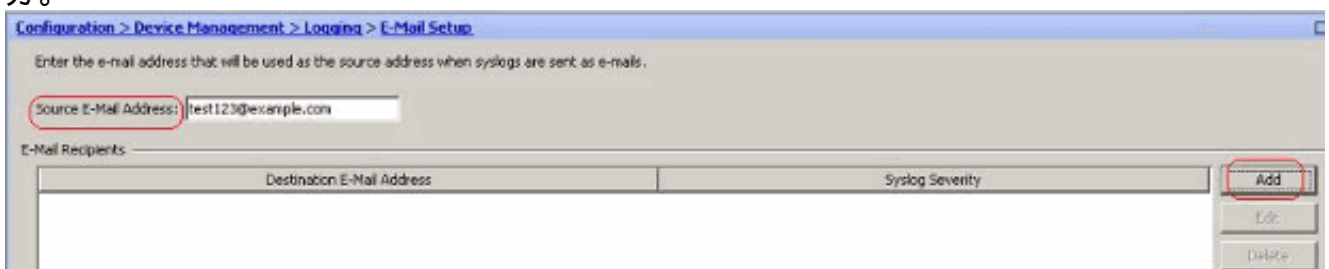
3. 已禁用Syslog在一分开的选项卡可以查看通过选择从Syslog ID设置的下拉菜单的已禁用 Syslog ID。



## 对电子邮件的记录日志

完成这些步骤使用ASDM为了发送系统日志到电子邮件：

1. 选择 *Configuration* > 设备管理 > 记录日志 > 电子邮件设置。来源电子邮件地址字段是有用在分配电子邮件ID作为来源Syslog的。指定来源电子邮件地址。现在，请单击添加添加电子邮件接收方。

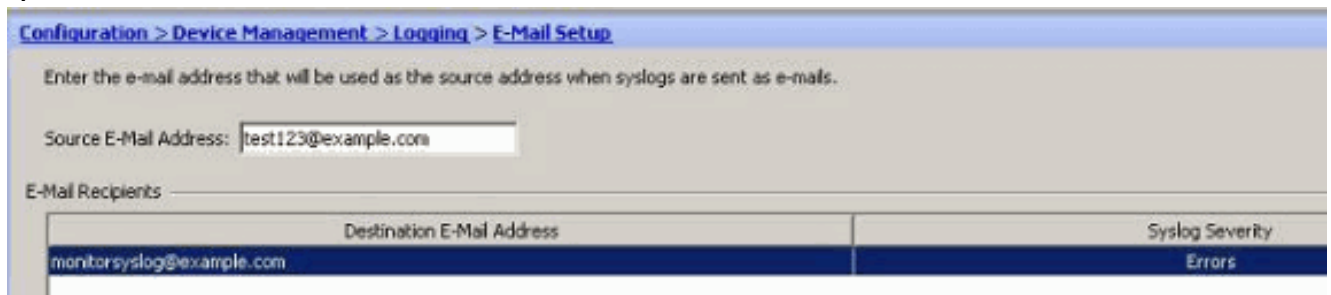


2. 指定目的地电子邮件地址并且选择严重级别。凭在严重级别上，您能定义不同的电子邮件接收方。点击OK键返回返回电子邮件设置窗格。

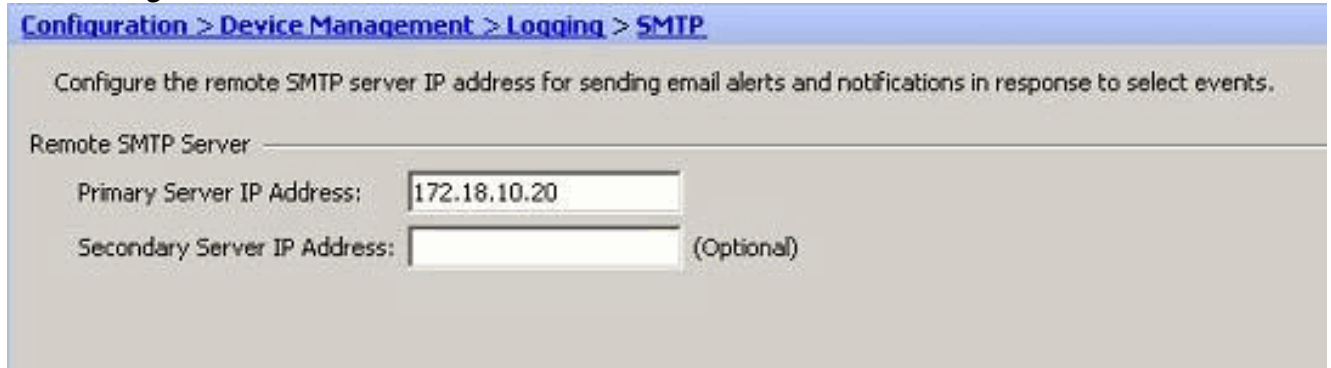




这导致此配置



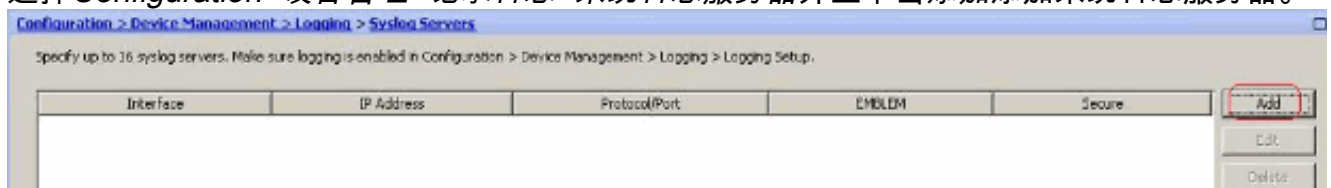
3. 选择 *Configuration*>设备设置>记录日志>SMTP并且指定SMTP服务器。



## 对系统日志服务器的记录日志

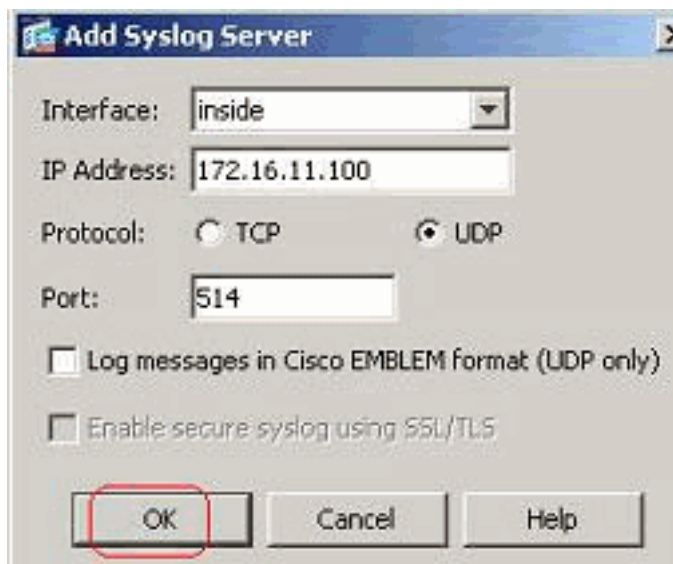
您能传送所有系统消息到一个专用的系统日志服务器。通过使用ASDM，执行这些步骤：

1. 选择 *Configuration*>设备管理>记录日志>系统日志服务器并且单击添加添加系统日志服务器。

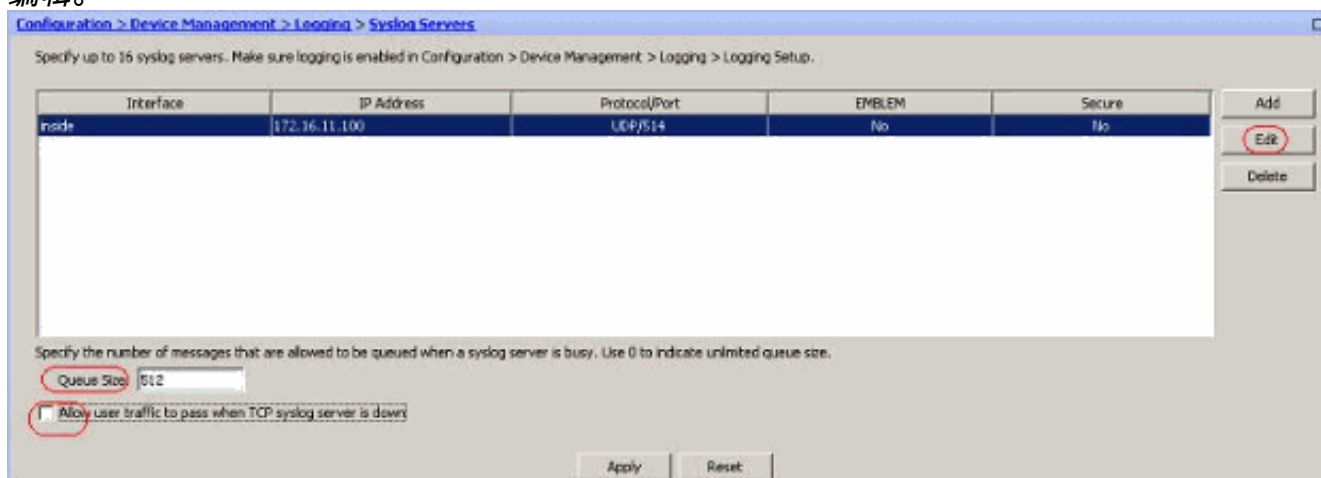


添加系统日志服务器窗口出现。

2. 指定接口服务器关联与与IP地址一起。根据您的网络设置指定协议和端口详细资料。然后，单击OK。**注意：** 确保您有可接通性到从思科ASA的系统日志服务器。



3. 已配置的系统日志服务器被看到如显示此处。修改可以完成，当您选择此服务器时，然后单击编辑。



**注意：** 复选标记通过的允许用户数据流，当Tcp syslog服务器是在选项下。否则，新用户会话通过ASA拒绝。只有当在ASA和系统日志服务器之间的传输协议是TCP时，这是可适用的。默认情况下，当系统日志服务器因故时，发生故障新建的网络访问会话由思科ASA拒绝。为了定义将发送到系统日志服务器系统消息的种类，请参阅[记录日志过滤器](#)部分。

## 通过使用ASDM的先进的Syslog配置

### 工作与事件列表

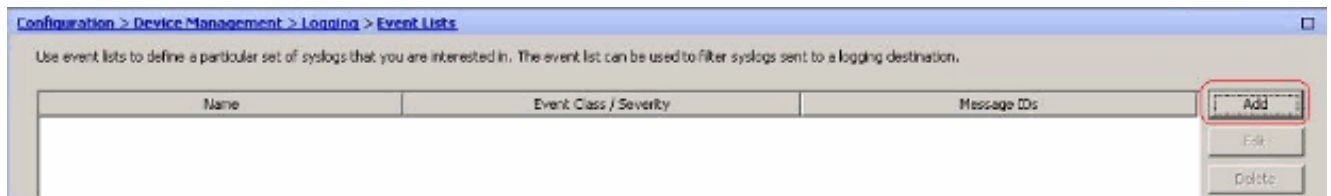
事件列表使我们建立包含系统消息组将发送到目的地的定制列表。事件列表可以创建用三个不同的方式：

- 消息ID或范围消息ID
- 消息重要性
- 邮件类别

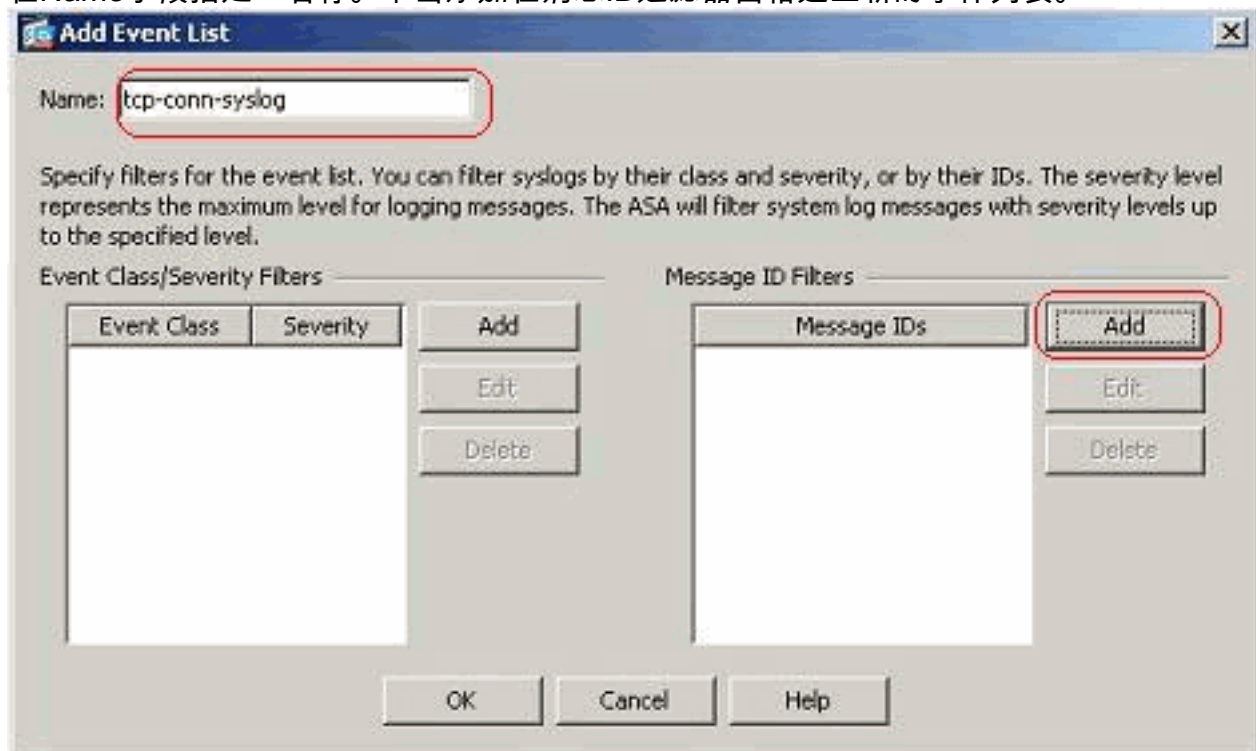
#### 消息ID或范围消息ID

请执行以下步骤：

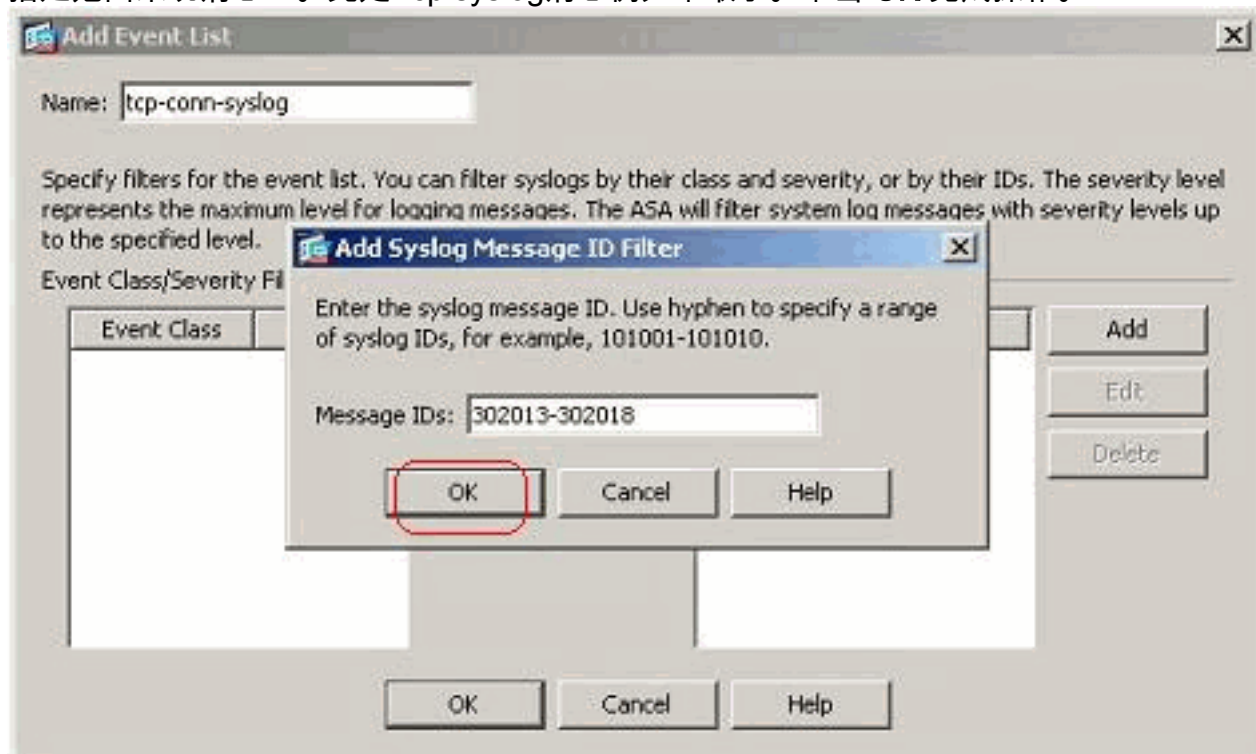
1. 选择 *Configuration*>设备管理>记录日志>事件列表并且单击添加建立新的事件列表。



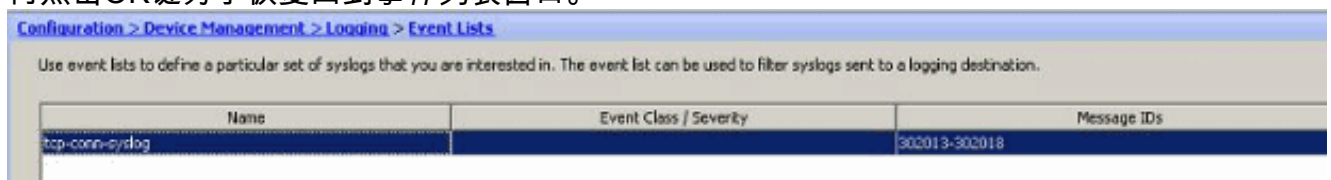
2. 在Name字段指定一名称。单击添加在消息ID过滤器窗格建立新的事件列表。



3. 指定范围系统消息ID。此处Tcp syslog消息例如采取了。单击 OK 完成操作。



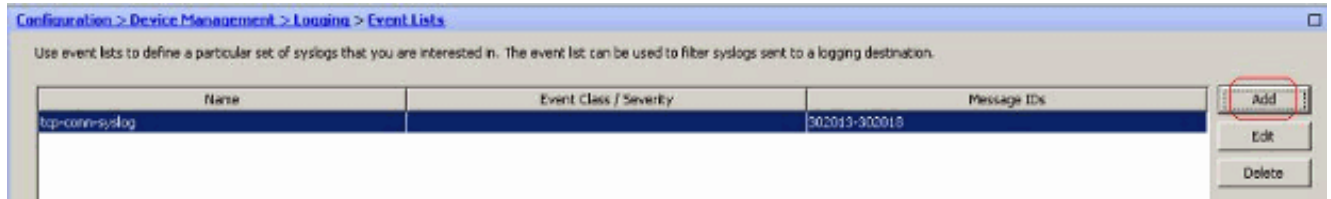
4. 再点击OK键为了恢复回到事件列表窗口。



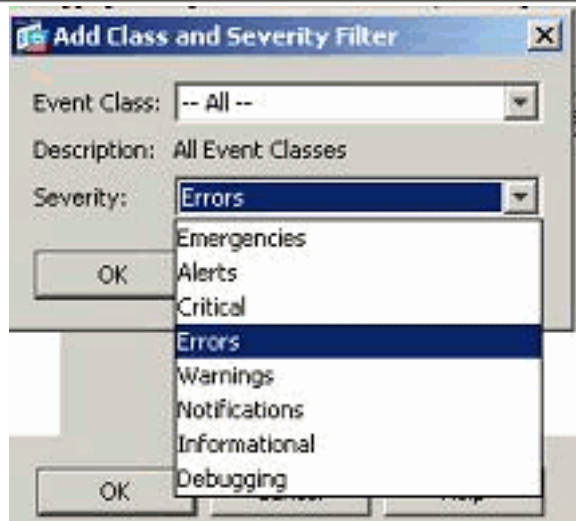
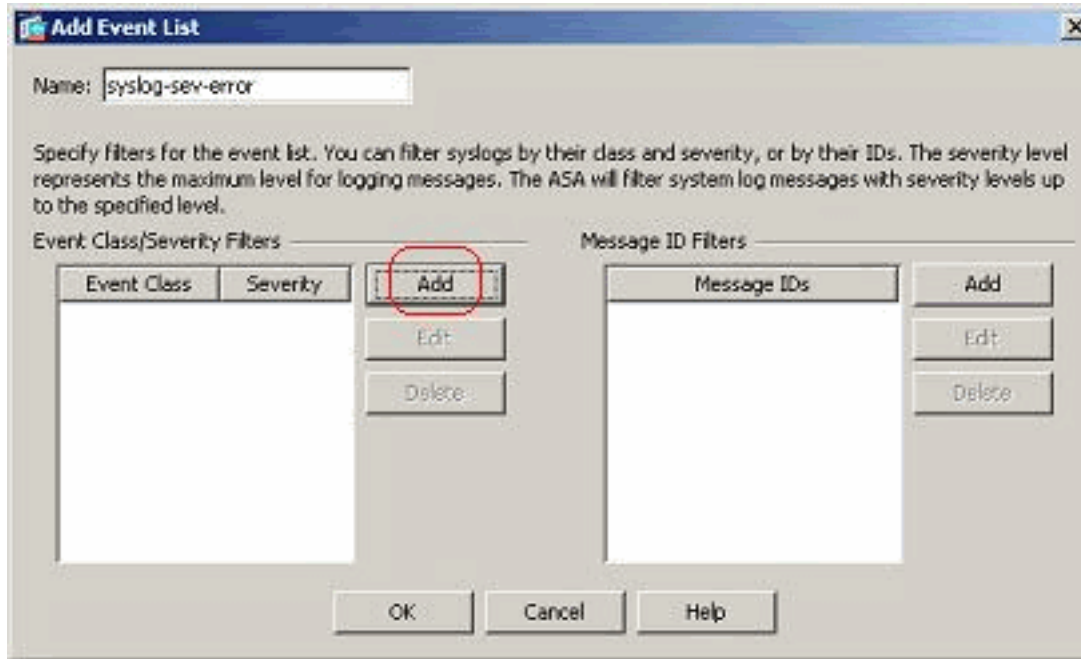


## 消息重要性

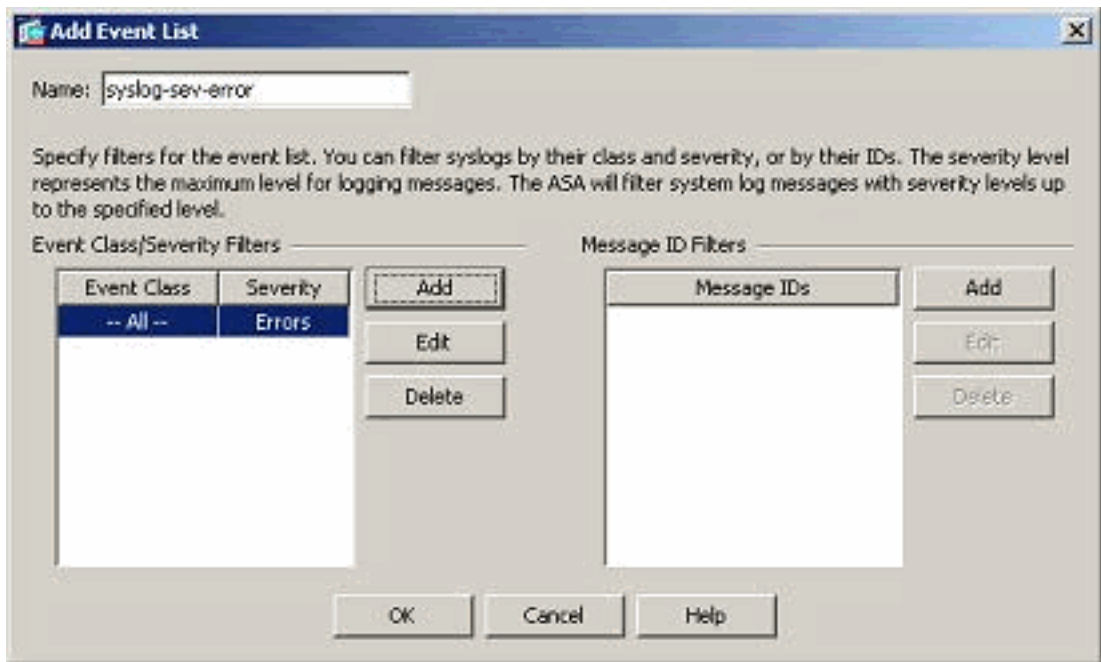
1. 事件列表可能根据消息重要性也定义。单击添加建立分开的事件列表。



2. 指定名称并且单击添加。



3. 选择严重级别作为错误。



4. 单击OK。

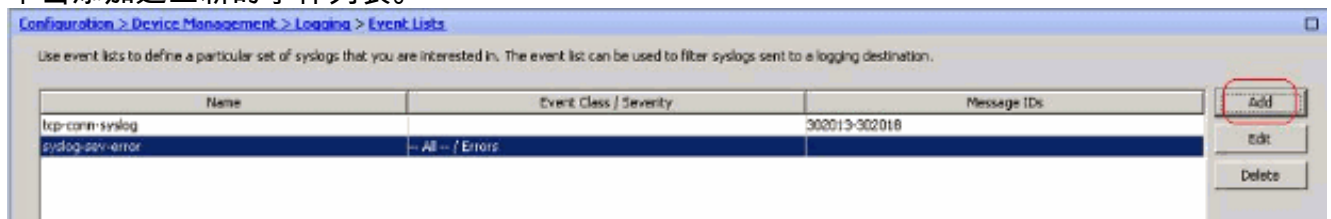
## 邮件类别

事件列表根据信息分类也配置。信息分类是与使您指定消息一整个类而不是单个指定每个消息的一类的安全工具功能涉及的系统消息的一组。例如，请使用验证类选择与用户认证涉及的所有系统消息。一些联机信息分类显示此处：

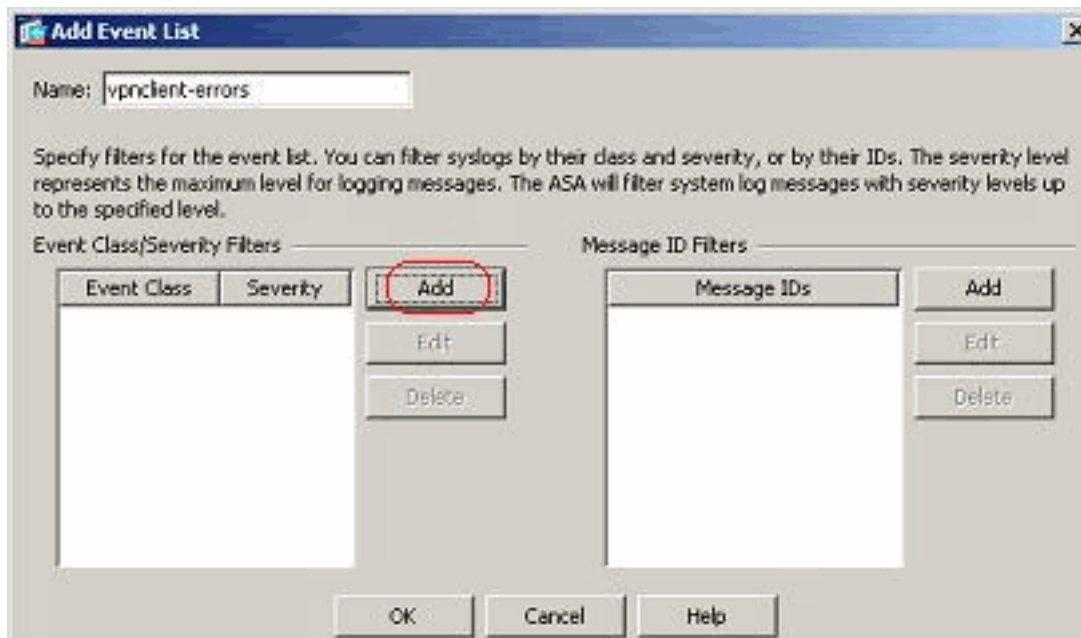
- 全所有事件类
- 验证—用户认证
- 网桥—透明防火墙
- 加州— PKI证书颁发机构
- config命令接口
- ha —故障切换
- ips —入侵保护服务
- ip — IP协议栈
- np —网络处理器
- ospf — OSPF路由
- RIP — RIP路由
- 会话—用户会话

执行这些步骤创建根据vpncient错误信息分类的事件类。信息分类， *vpnc*，是可用分类与vpncient涉及的所有系统消息。此信息分类的严重级别选择作为“错误”。

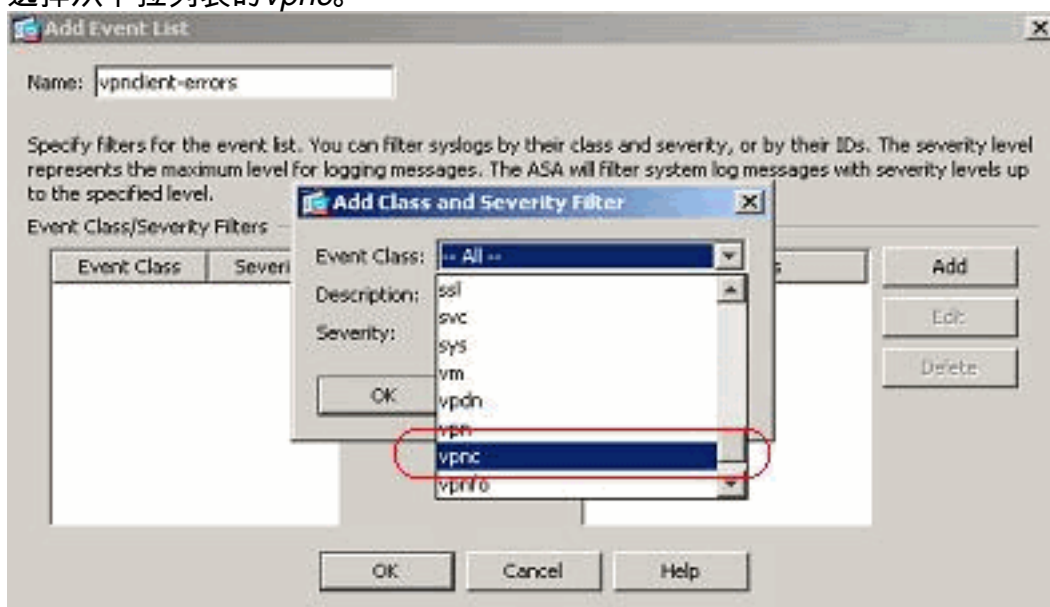
1. 单击添加建立新的事件列表。



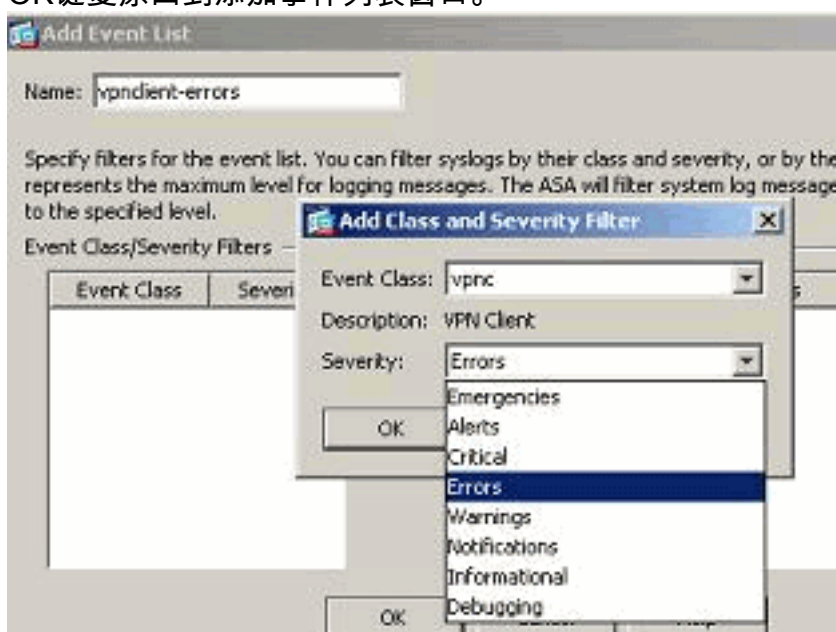
2. 指定名称是相关的与您创建的信息分类并且单击添加。



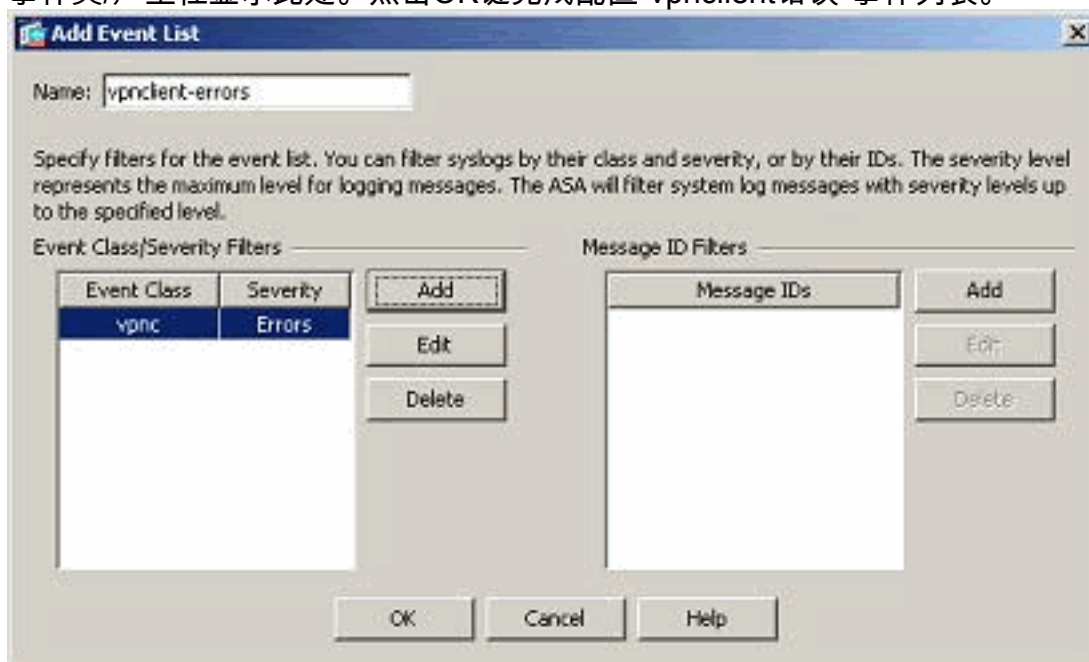
3. 选择从下拉列表的 *vpnc*。



4. 选择严重级别作为 *错误*。此严重级别为为仅此信息分类被记录的那些消息是可适用的。点击 *OK* 键复原回到添加事件列表窗口。

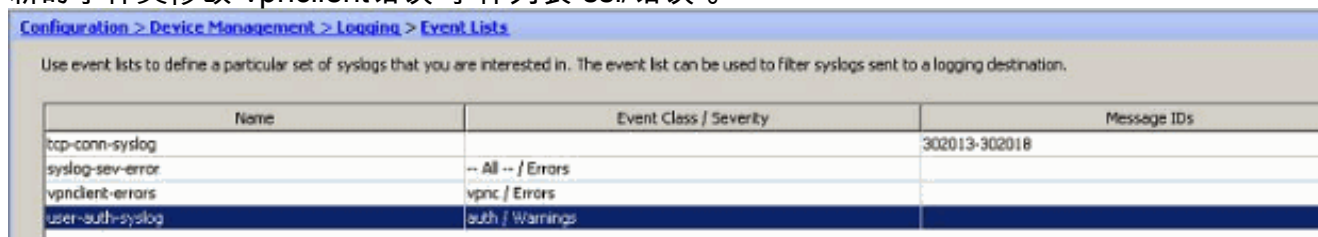


5. 事件类/严重性显示此处。点击OK键完成配置“vpnclient错误”事件列表。



在下张屏幕画

面新的事件列表，“用户验证Syslog”，创建与信息分类作为“验证”和此特定留言类Syslog的严重级别也显示作为“警告”。通过配置此，事件列表指定与“验证”信息分类涉及的所有系统消息，与严重级别至“警告”级别。**注意：**这里，期限“至”是意义。当表示严重级别时，请记住所有系统消息将被记录，直到该级别。**注意：**事件列表能包含多个事件类。单击**编辑**和定义一个新的事件类修改“vpnclient错误”事件列表“ssl/错误”。



## 工作用记录日志过滤器

记录的过滤器用于传送系统消息到指定的目的地。这些系统消息可以根据“严重性”或“列表”。

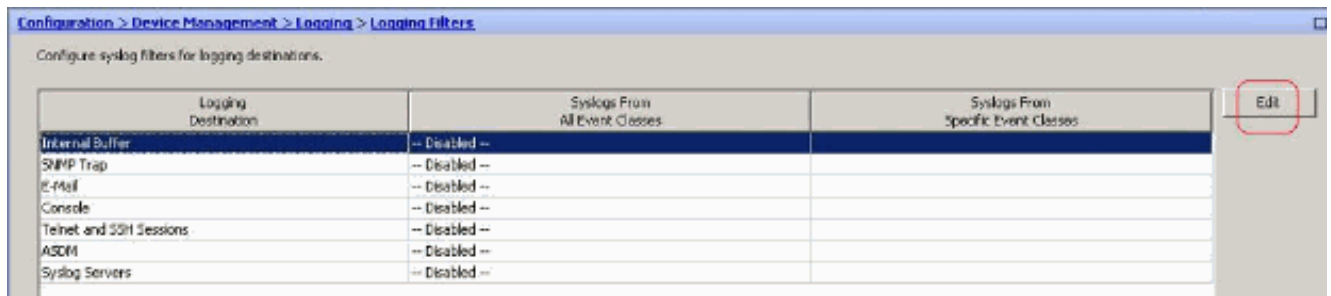
这些是这些过滤器是可适用的种类的位置：

- 内部缓冲区
- SNMP 陷阱
- 电子邮件
- 控制台
- Telnet 会话
- ASDM
- 系统日志服务器

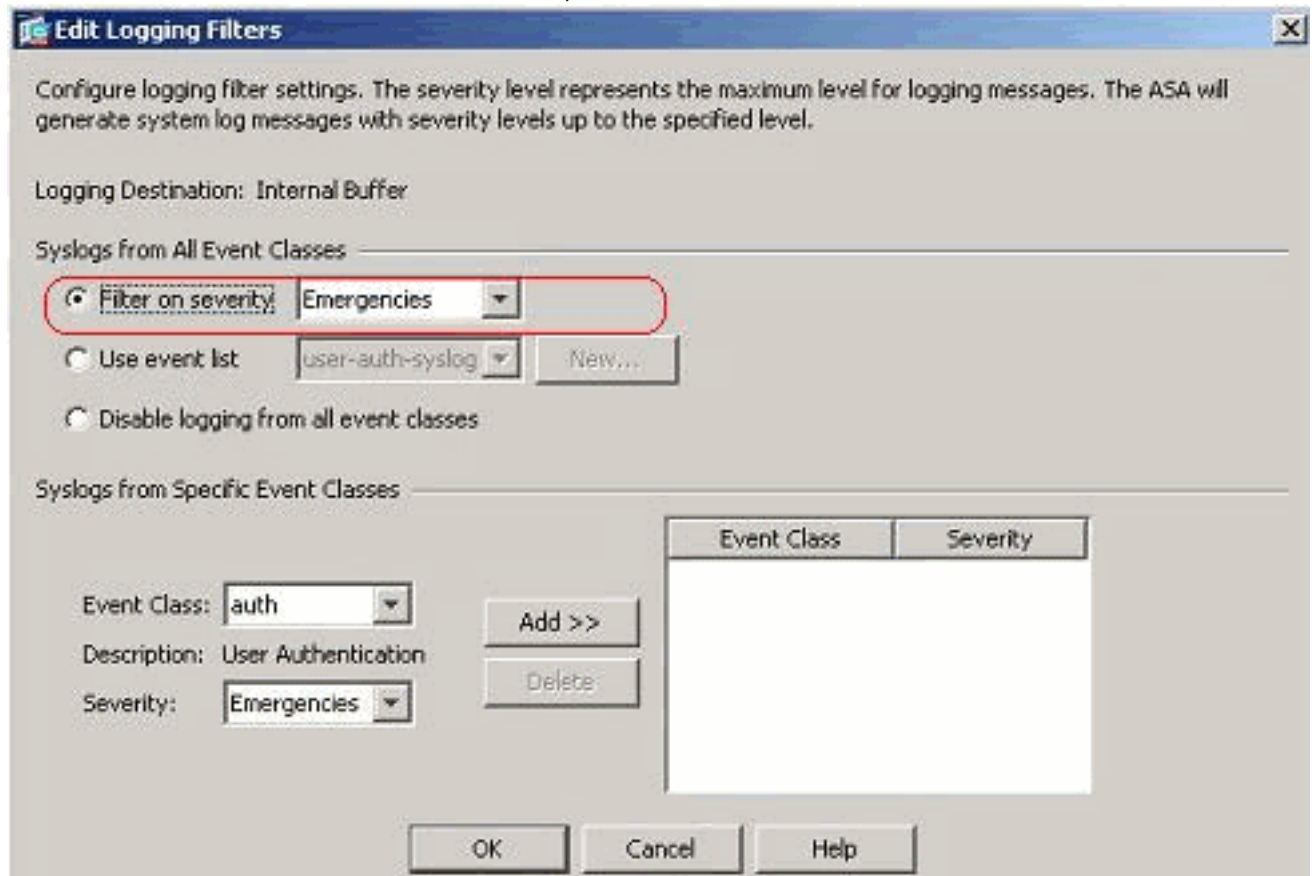
请执行以下步骤：

1. 选择**Configuration>设备管理>记录日志>记录日志过滤器**并且选择操作日志目的地。然后，请单击**编辑**修改设置。

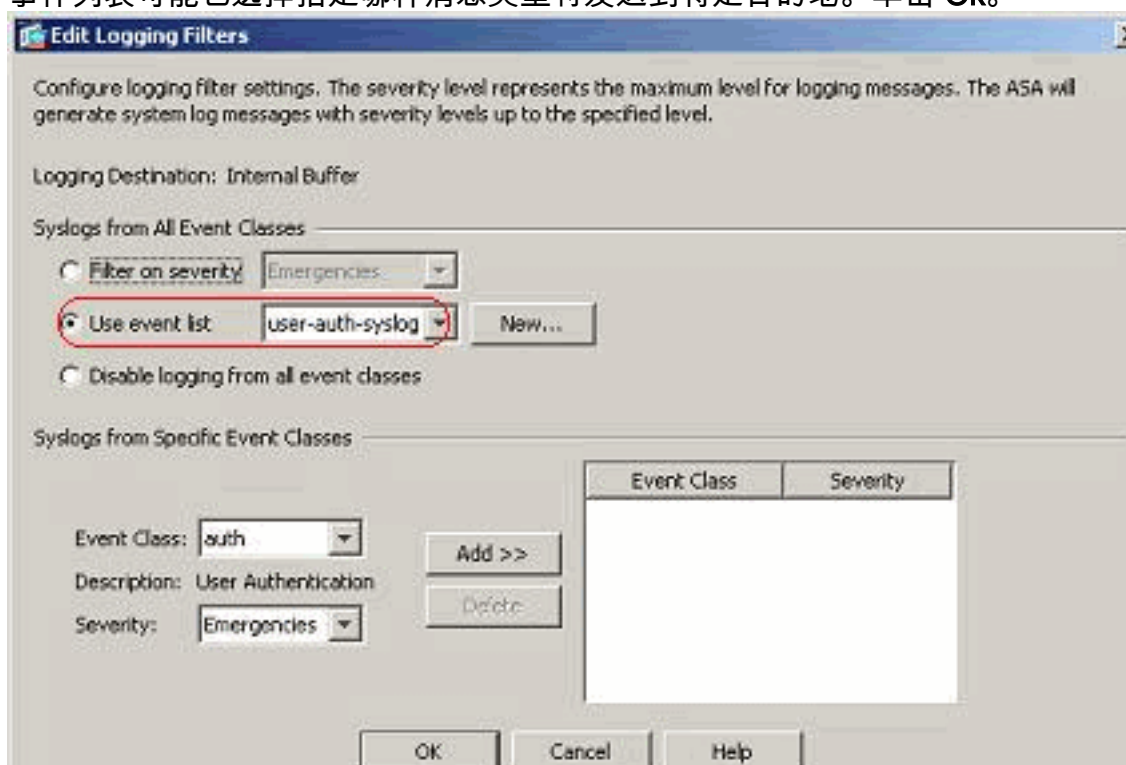




2. 您能传送根据严重性的系统消息。这里，紧急状态选择显示为例。

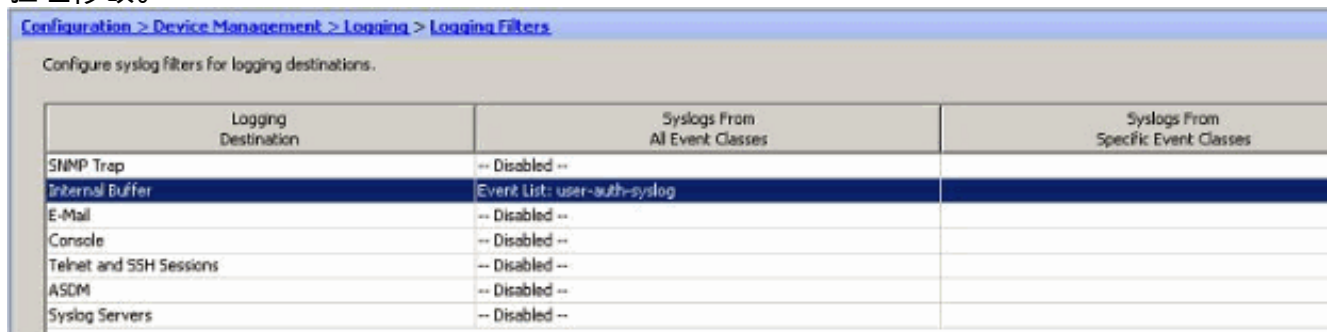


3. 事件列表可能也选择指定哪种消息类型将发送到特定目的地。单击 Ok。



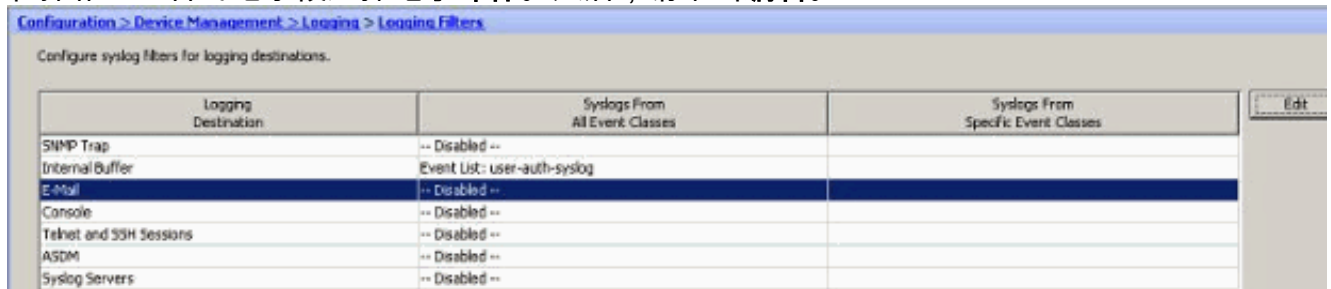


#### 4. 验证修改。

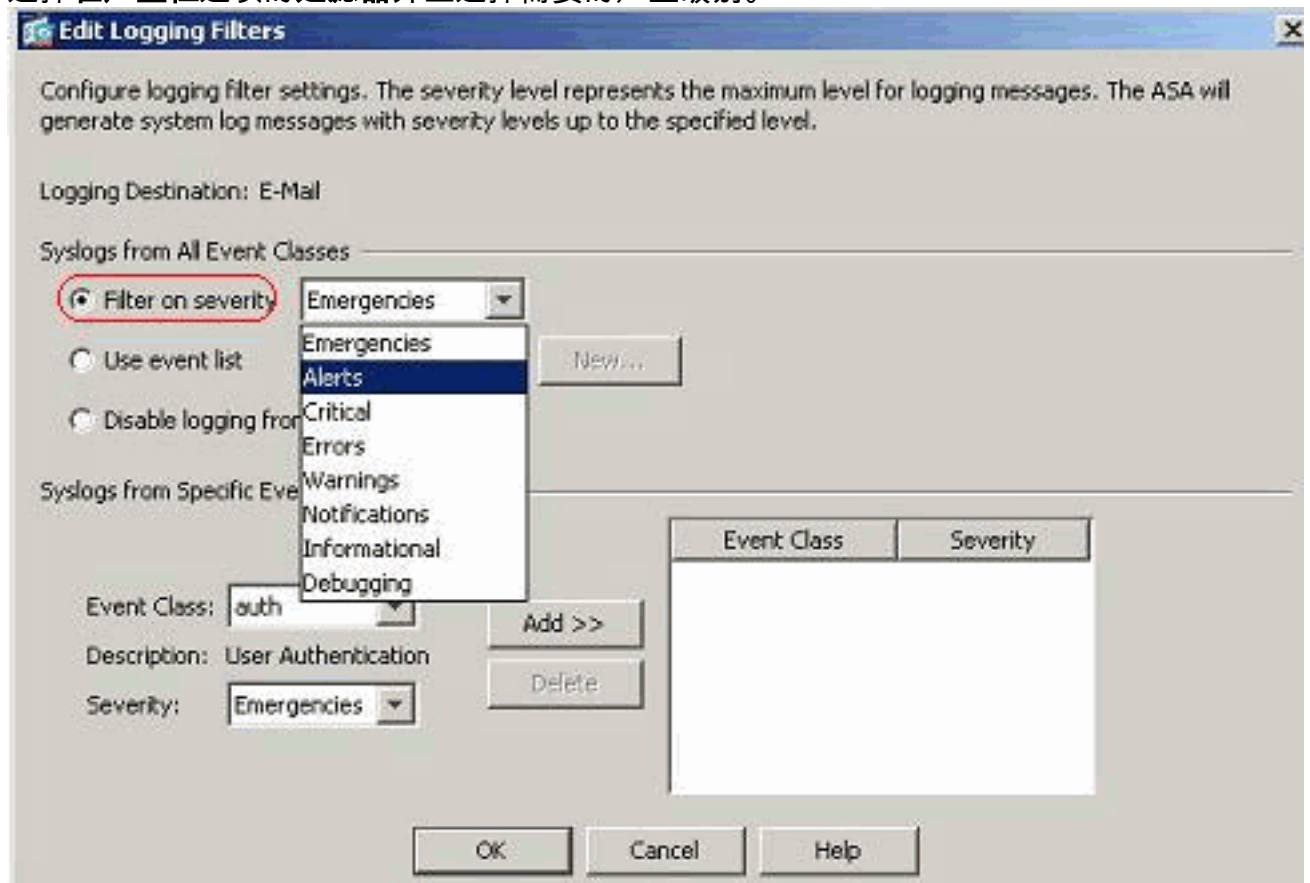


这些是关于怎样的步骤传送信息的一组(根据他们的严重级别)到电子邮件服务器。

#### 1. 在操作日志目的地字段选择**电子邮件**。然后，请单击**编辑**。



#### 2. 选择在**严重性**选项的过滤器并且选择需要的严重级别。



这里，**警报**选择作为严重级别。

Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

| Logging Destination     | Syslogs From All Event Classes | Syslogs From Specific Event Classes |
|-------------------------|--------------------------------|-------------------------------------|
| SNMP Trap               | -- Disabled --                 |                                     |
| Internal Buffer         | Event List: user-auth-syslog   |                                     |
| E-Mail                  | Severity: Alerts               |                                     |
| Console                 | -- Disabled --                 |                                     |
| Telnet and SSH Sessions | -- Disabled --                 |                                     |
| ASDM                    | -- Disabled --                 |                                     |
| Syslog Servers          | -- Disabled --                 |                                     |

您能看到所有提醒的系统消息将发送到配置的电子邮件。

Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

| Logging Destination     | Syslogs From All Event Classes | Syslogs From Specific Event Classes |
|-------------------------|--------------------------------|-------------------------------------|
| Internal Buffer         | Event List: user-auth-syslog   |                                     |
| SNMP Trap               | -- Disabled --                 |                                     |
| E-Mail                  | Severity: Alerts               |                                     |
| Console                 | -- Disabled --                 |                                     |
| Telnet and SSH Sessions | -- Disabled --                 |                                     |
| ASDM                    | -- Disabled --                 |                                     |
| Syslog Servers          | -- Disabled --                 |                                     |

## 丢包率限制

这指定思科ASA传送对在指定的时间段的一个目的地系统消息的数量。它为严重级别通常定义。

1. 选择Configuration>设备管理>记录日志>速率限制并且选择需要的严重级别。然后，请单击编辑。

Configuration > Device Management > Logging > Rate Limit

Assign rate limits for all the syslog messages in a logging level or assign it individually to specific syslog messages.

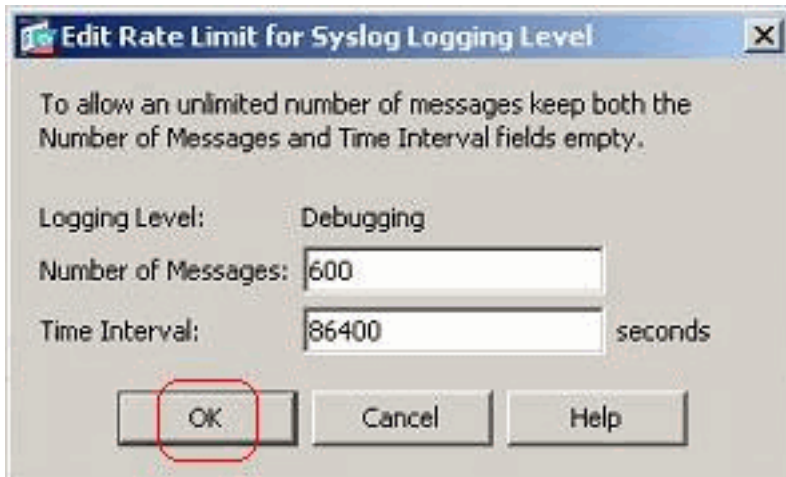
Rate Limits for Syslog Logging Levels

| Logging Level | No. of Messages | Interval (Seconds) | Edit |
|---------------|-----------------|--------------------|------|
| Debugging     | unlimited       |                    |      |
| Notifications | unlimited       |                    |      |
| Critical      | unlimited       |                    |      |
| Emergencies   | unlimited       |                    |      |
| Warnings      | unlimited       |                    |      |
| Errors        | unlimited       |                    |      |
| Informational | unlimited       |                    |      |
| Alerts        | unlimited       |                    |      |

Individually Rate Limited Syslog Messages

| Syslog ID | Logging Level | No. of Messages | Interval (Seconds) | Add  |
|-----------|---------------|-----------------|--------------------|------|
|           |               |                 |                    | Edit |

2. 指定与时间间隔一起将发送通讯数量。单击 Ok。



注意：这些编号给为例。这些根据网络类型环境有所不同。已修改值被看到此处

：

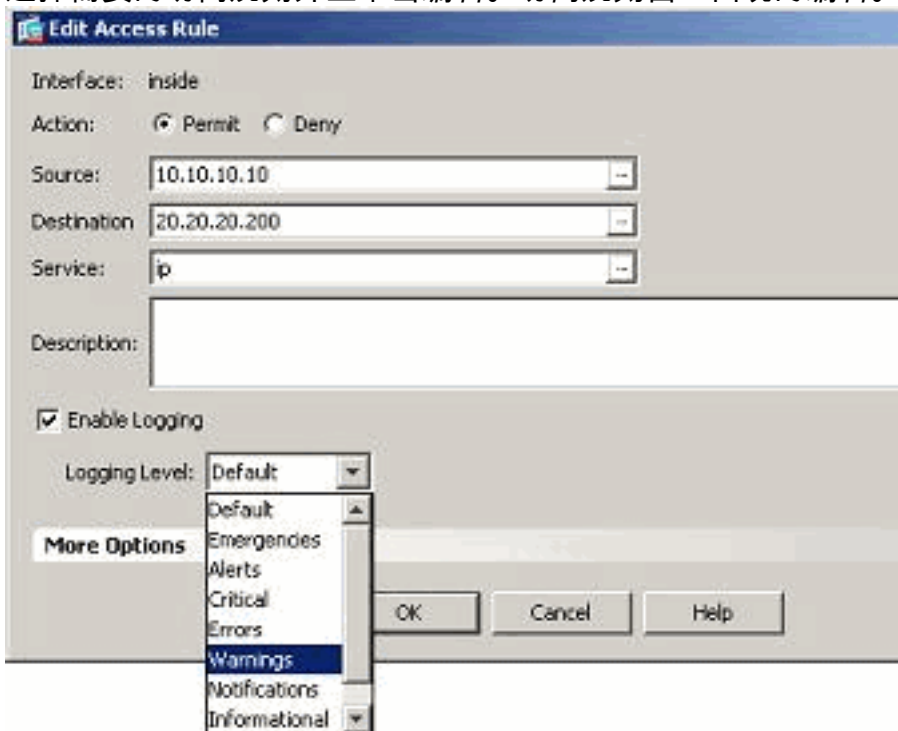
| Logging Level | No. of Messages | Interval (Seconds) |
|---------------|-----------------|--------------------|
| Debugging     | 600             | 86400              |
| Notifications | unlimited       |                    |
| Critical      | unlimited       |                    |

## 记录访问规则的命中数

使用ASDM，您能记录访问规则命中数。默认日志行为是传送所有已拒绝数据包的一系统消息。将没有允许的数据包的所有系统消息，并且这些不会被记录。然而，您能定义一自定义记录日志严重级别到访问规则跟踪点击此访问规则数据包的计数。

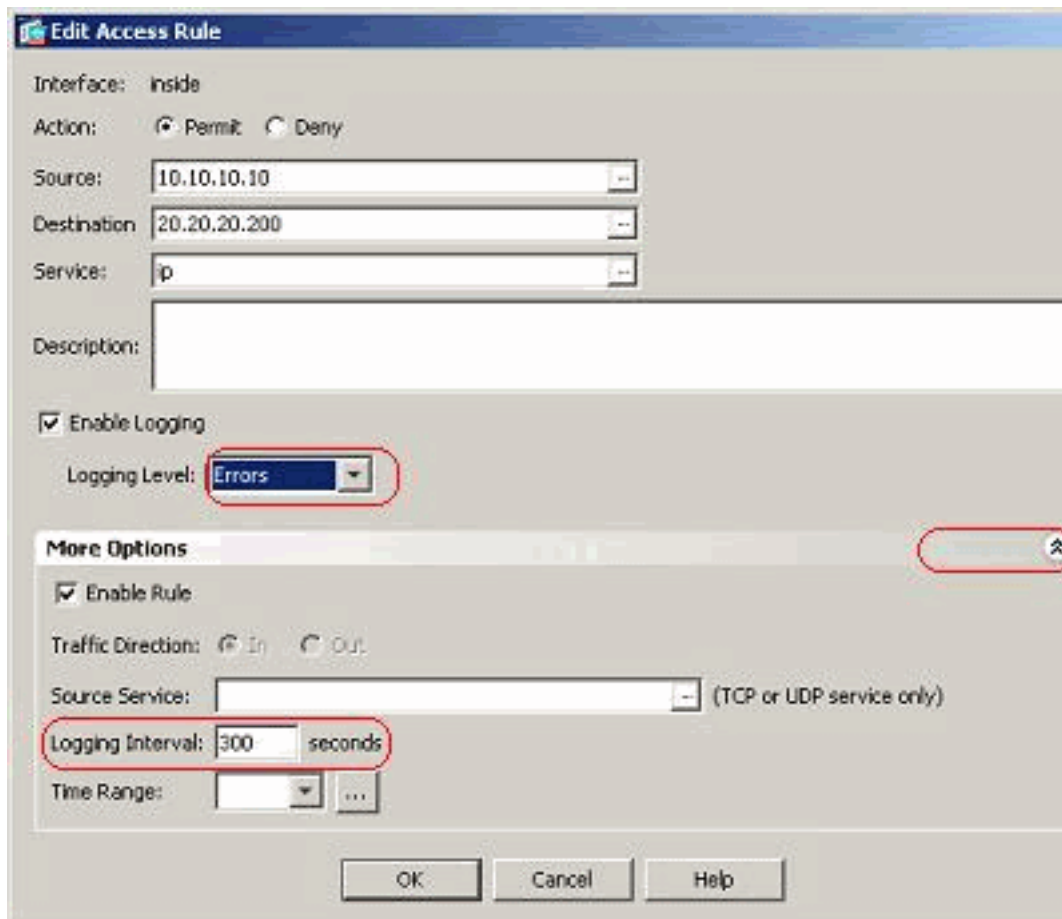
请执行以下步骤：

1. 选择需要的访问规则并且单击编辑。访问规则窗口出现的编辑。



注意：在此镜像，默认选项在日志级别字段指示思科ASA的默认日志行为。关于此的更多信息，参考[记录日志访问列表活动](#)部分。

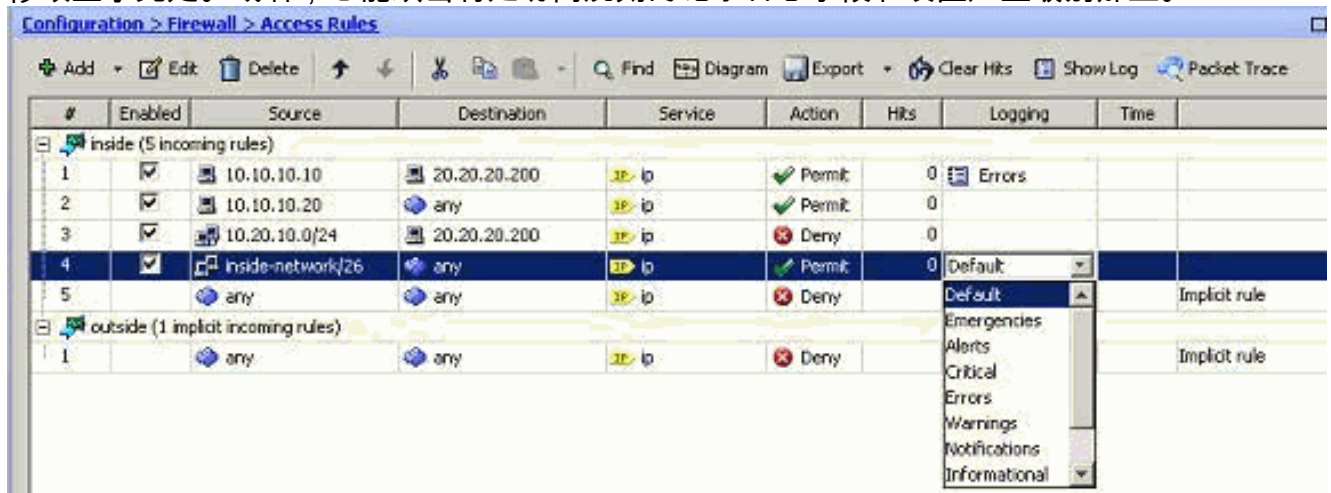
2. 复选标记启用日志选项和指定需要的严重级别。然后，单击OK。



**注意：** 通过单击

更多选项下拉式选项卡，您能看到记录日志间隔选项。只有当上述启用日志选项做标记时，此选项突出显示。默认值此计时器是300秒。此设置是有用的在指定能将删除的流统计信息的超时值，当没有对手对于该访问规则时。如果有任何命中数，则ASA等待直到对Syslog的记录日志间隔时间和发送。

3. 修改显示此处。或者，您能双击特定访问规则的记录日志字段和设置严重级别那里。



**注意：** 指定在同样的日志级别此替代方法访问窗格在双击旁边为手工仅创建的访问规则条目工作的规则，但是不对隐式规则。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：** 使用[命令查找工具](#) (仅限注册用户) 可获取有关本部分所使用命令的详细信息。

## 配置

本文档使用以下配置：

```
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

```

## 验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \( 仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- 您能查看从ASDM的Syslog。选择记录的Monitoring> >实时日志查看器。输出示例:显示此处

The screenshot shows the 'Real-Time Log Viewer' window with a table of log entries. The table has columns for 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 insic |
| 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                     |

## 故障排除

### 问题：丢失的连接--终止的Syslog连接--

当尝试启用记录在的设备控制板的ASDM任何上下文时，此错误接收。

“--Syslog--”

当ASDM用于连接直接地到admin上下文，并且ADSM记录禁用那里，然后对subcontext和enable (event) ASDM记录的交换机。错误接收，但是系统消息优良到达到系统日志服务器。

## [解决方案](#)

这是与思科ASDM的一种认为的行为并且描述了在Cisco Bug ID [CSCsd10699](#) ([仅限注册用户](#))。作为应急方案，enable (event) asdm记录日志，当登录的admin上下文。

## [不能查看实时注册思科ASDM](#)

问题是实时日志在ASDM不可能查看。这如何配置？

## [解决方案](#)

配置以下在思科ASA：

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

## [相关信息](#)

- [Cisco ASA 5500 系列自适应安全设备支持](#)
- [技术支持和文档 - Cisco Systems](#)