適応型セキュリティアプライアンス(ASA)syslogの設定

内容

はじめに

このドキュメントでは、コードバージョン8.4以降を実行するASAのさまざまなログオプションの設定方法を示す設定例について説明します。

背景説明

ASA バージョン 8.4 では、非常に詳細なフィルタリング技法が導入され、指定した特定の syslog メッセージのみを表示できるようになりました。このドキュメントの「基本的な syslog」セクションでは、従来の syslog の設定について説明しています。このドキュメントの「高度な syslog」セクションは、バージョン 8.4 での新規 syslog 機能を示しています。完全なシステム ログ メッセージ ガイドについては、『Cisco セキュリティ アプライアンス システム ログ メッセージ ガイド』を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA ソフトウェア バージョン 8.4 が稼働する ASA 5515
- Cisco Adaptive Security Device Manager（ASDM）バージョン 7.1.6

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

注：ASDMバージョン7.1以降での同様の設定の詳細については、『ASA 8.2:ASDMを使用したSyslogの設定』を参照してください。

基本 syslog

ロギングの有効化、ログの表示、および設定の表示には、次のコマンドを入力します。

- logging enable：すべての出力場所への Syslog メッセージの転送を有効にします。
- no logging enable：すべての出力場所へのログを無効にします。
- show logging：syslog バッファおよび現在の設定に関連する情報と統計の内容をリストします。

ASA では、さまざまな宛先に syslog メッセージを送信できます。syslog 情報の送信先を指定す

るには、これらのセクションで説明するコマンドを入力します。

内部バッファにログ情報を送信

<#root>

logging buffered

 severity_level

ASA の内部バッファに syslog メッセージを格納する場合は、外部のソフトウェアまたはハードウェアは必要ありません。格納されている syslog メッセージを表示するには show logging コマンドを入力します。内部バッファの最大サイズは 1 MB です（logging buffer-size コマンドで設定可能）。その結果、ラップが非常に速くなります。内部バッファのログレベルを選択する際には、冗長レベルのロギングでは内部バッファがすぐにいっぱいになり、ラップされる可能性があることに注意してください。

syslog サーバにログ情報を送信

<#root>

logging host

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

logging trap

 severity_level

logging facility

 number

syslog メッセージを外部ホストに送信するには、syslog アプリケーションを実行するサーバが必要です。デフォルトでは、ASA は UDP ポート 514 で syslog を送信しますが、プロトコルとポートは選択することができます。TCP がロギング プロトコルとして選択されている場合、ASA は TCP 接続経由で syslog サーバに syslog を送信します。サーバにアクセスできない場合、またはサーバへのTCP接続を確立できない場合、ASAはデフォルトですべての新規接続をブロックします。logging permit-hostdown を有効にすると、この動作を無効にできます。logging permit-hostdown コマンドに関する詳細については、コンフィギュレーション ガイドを参照してください。

注:ASAで許可されるポートは、1025 ~ 65535の範囲です。他のポートを使用すると、次のエラーが発生します。
ciscoasa(config)# logging host tftp 192.168.1.1 udp/516
警告：インターフェイスEthernet0/1のセキュリティレベルは0です。
エラー：ポート'516'は1025 ~ 65535の範囲内にありません。

ログ情報を電子メールとして送信

<#root>

```
logging mail
 severity_level
logging recipient-address
 email_address
logging from-address
 email_address
smtp-server
 ip_address
```

電子メールで syslog メッセージを送信する場合は、SMTP サーバが必要です。ASA から、指定した電子メール クライアントに電子メールを確実にリレーするには、SMTP サーバで正しく設定を行うことが必要です。このログレベルが、debugやinformational などの非常に冗長なレベルに設定されている場合、このログ設定から送信される各電子メールによって追加のログが4つ以上生成されるため、かなりの数のsyslogが生成される可能性があります。

シリアル コンソールにログ情報を送信

<#root>

```
logging console
 severity_level
```

コンソール ロギングを使用すると、発生した syslog メッセージを ASA コンソール（tty）に表示できます。コンソール ロギングが設定されている場合、ASA 上のすべてのログ生成は、ASA シリアル コンソールの速度である 9800 bps に制限されます。これにより、内部バッファを含むすべての宛先でsyslogがドロップされる可能性があります。このため、冗長な syslog にコンソール ロギングを使用しないでください。

Telnet/SSH セッションにログ情報を送信

<#root>

```
logging monitor
 severity_level
terminal monitor
```

ロギング モニタを使用すると、Telnet または SSH を使用して ASA コンソールにアクセスし、コマンド ターミナル モニタをそのセッションから実行する際に発生する syslog メッセージを表示できます。セッションへのログの出力を停止するには terminal no monitor コマンドを入力します。

ASDM 上にログ メッセージを表示

<#root>

```
logging asdm
 severity_level
```

ASDM には、syslog メッセージの格納に使用できるバッファも備わっています。ASDM syslog バッファの内容を表示するには、show logging asdm コマンドを入力します。

SNMP 管理ステーションにログを送信

<#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
```

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して syslog メッセージを送信するには、稼働中の SNMP 環境がすでに存在している必要があります。出力先の設定と管理に使用できるコマンドの詳細については、『出力先を設定および管理するためのコマンド』を参照してください。重大度別にまとめたメッセージについては、『重大度別メッセージ一覧』を参照してください。

syslog にタイムスタンプを追加

イベントを配置して順序付けるため、syslog にタイムスタンプを追加することができます。これは、時間に基づいて問題をトレースするために推奨されています。タイムスタンプを有効にするには、logging timestamp コマンドを入力します。次に、タイムスタンプなしとタイムスタンプ付きの 2 つの syslog の例を示します。

```
%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
```

例 1

この出力は、デバッグの重大度によりバッファ に口ギングする場合のサンプル設定を示しています。

<#root>

```
logging enable
logging buffered debugging
```

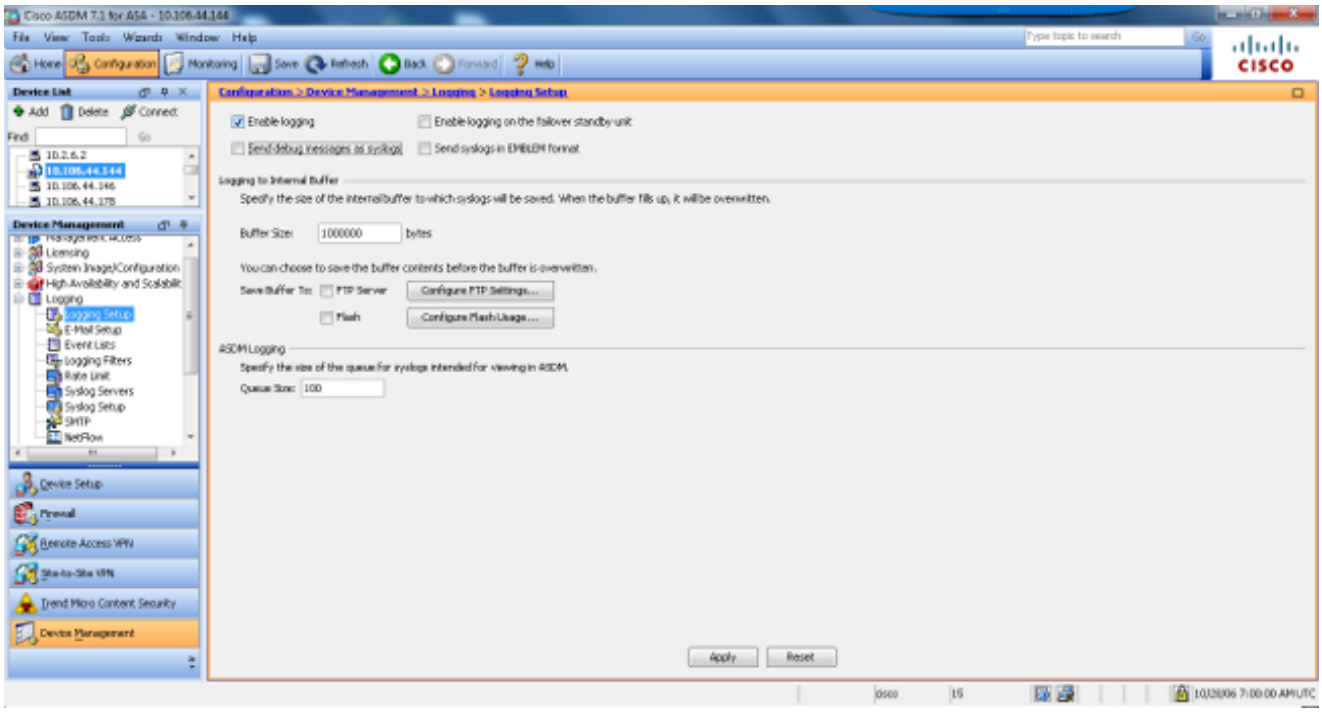
次に、出力例を示します。

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

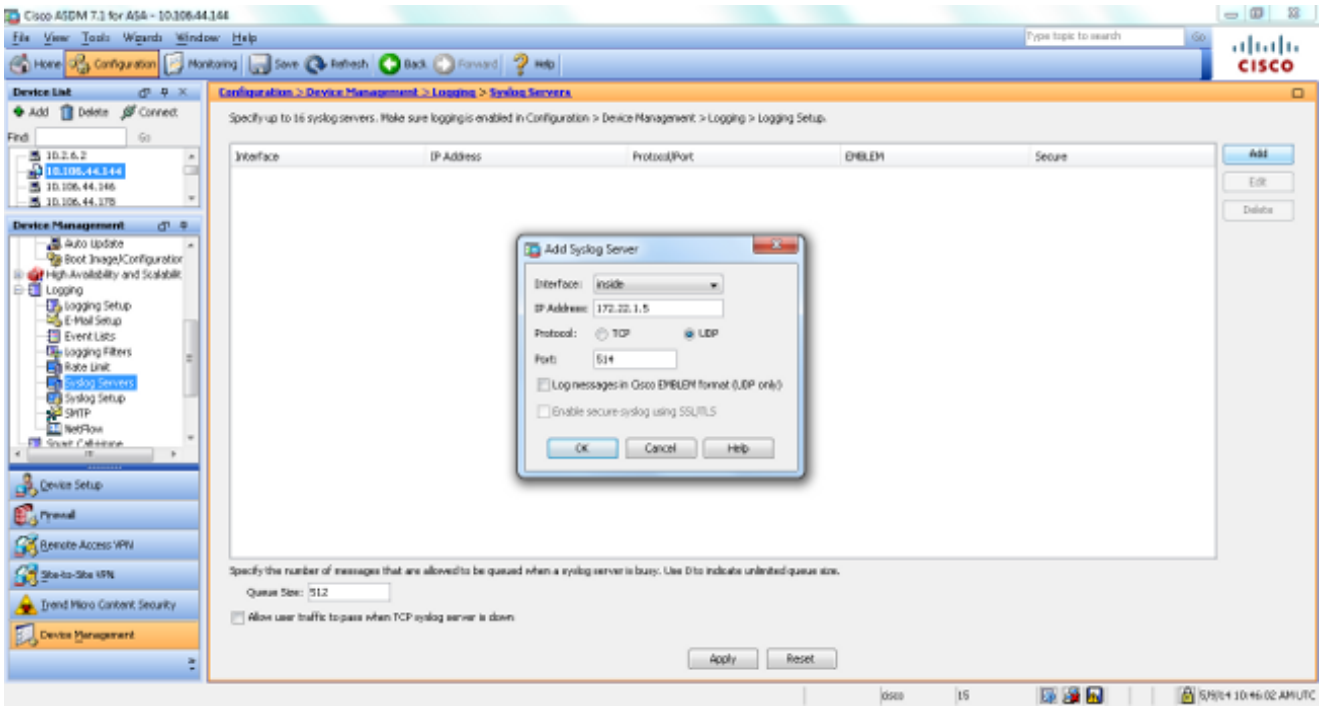
基本 syslog を ASDM で設定

次に示すのは、すべての使用可能な syslog 宛先を ASDM で設定する例です。

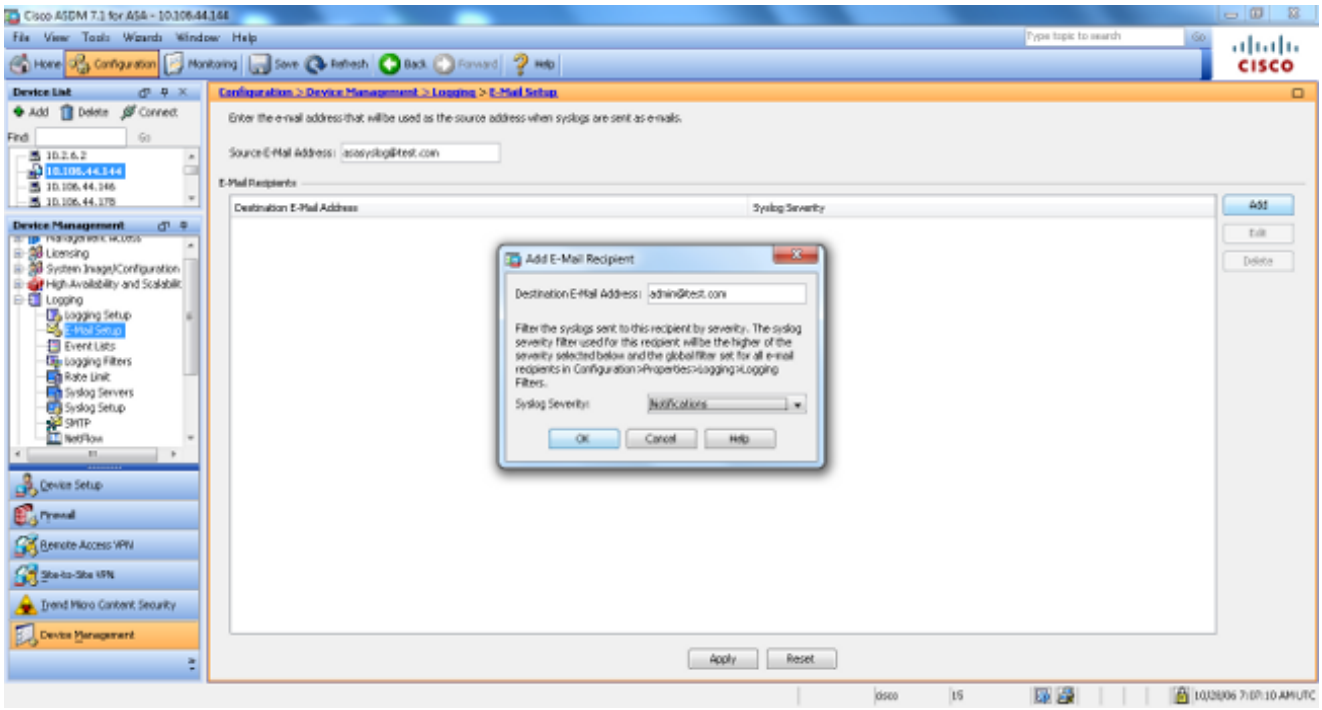
1. ASA で口ギングを有効にするには、まず基本口ギング パラメータを設定します。[Configuration] > [Features] > [Properties] > [Logging] > [Logging Setup] を選択します。[Enable logging] チェックボックスをオンにして syslog を有効にします。



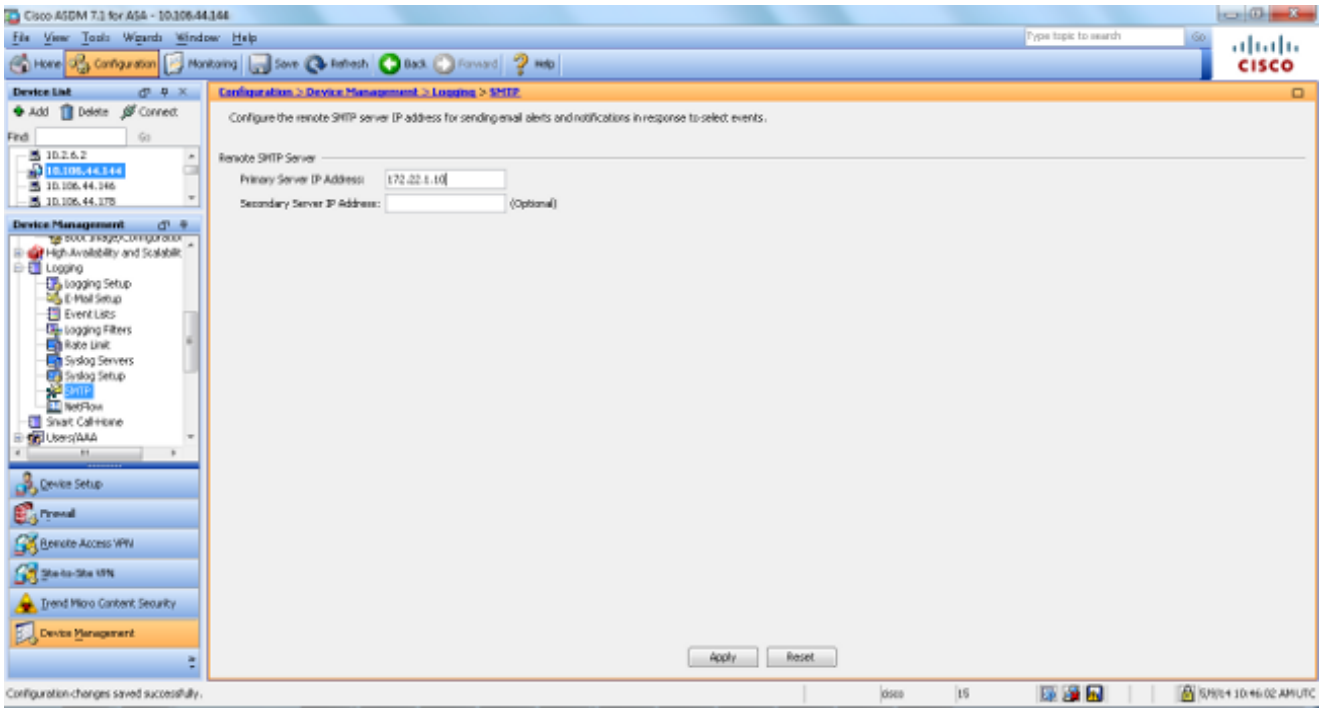
2. 外部サーバを syslog の宛先として設定するには、[Logging] で [Syslog Servers] を選択し、[Add] をクリックして syslog サーバを追加します。[Add Syslog Server] ボックスで syslog サーバの詳細を入力してから、[OK] をクリックします。



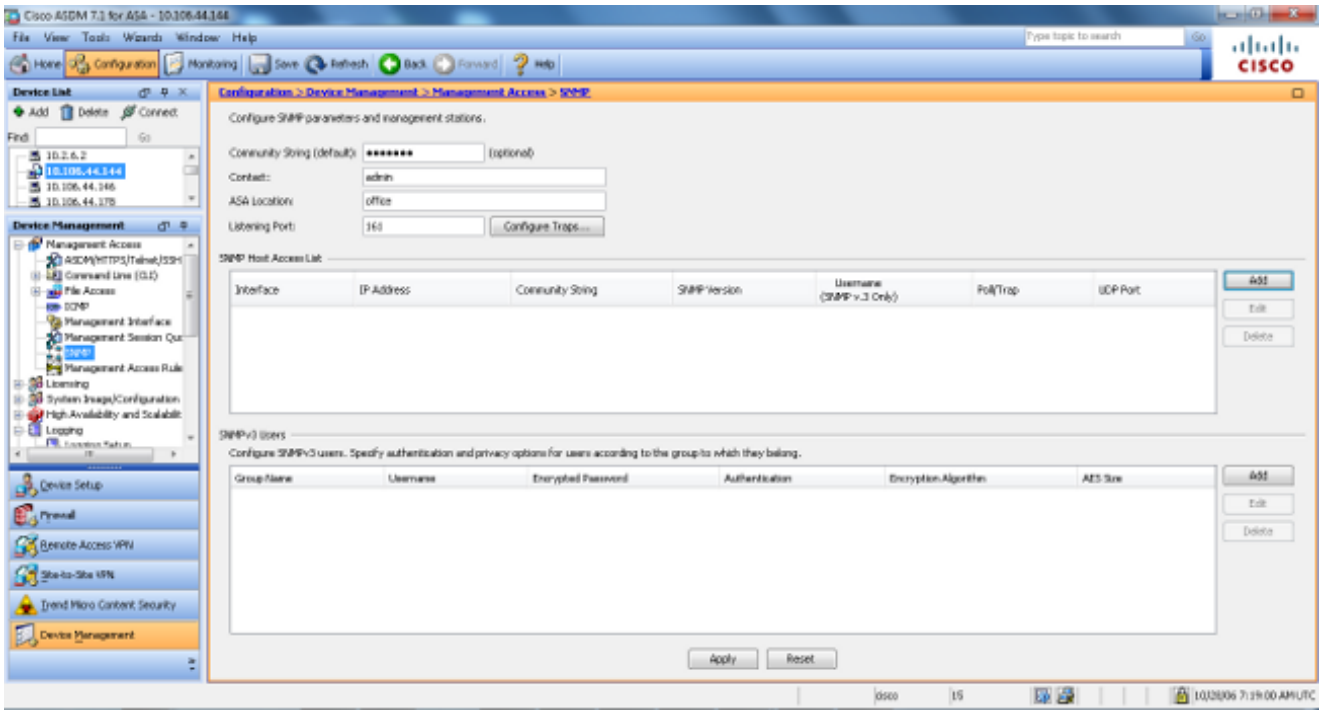
3. syslog メッセージを特定の受信者に電子メールとして送信するには、[Logging] で [E-Mail Setup] を選択します。[Source E-Mail Address] ボックスで送信元の電子メール アドレスを指定し、[Add] をクリックして、電子メール受信者の宛先アドレスとメッセージの重大度を設定します。完了したら、[OK] をクリックします。



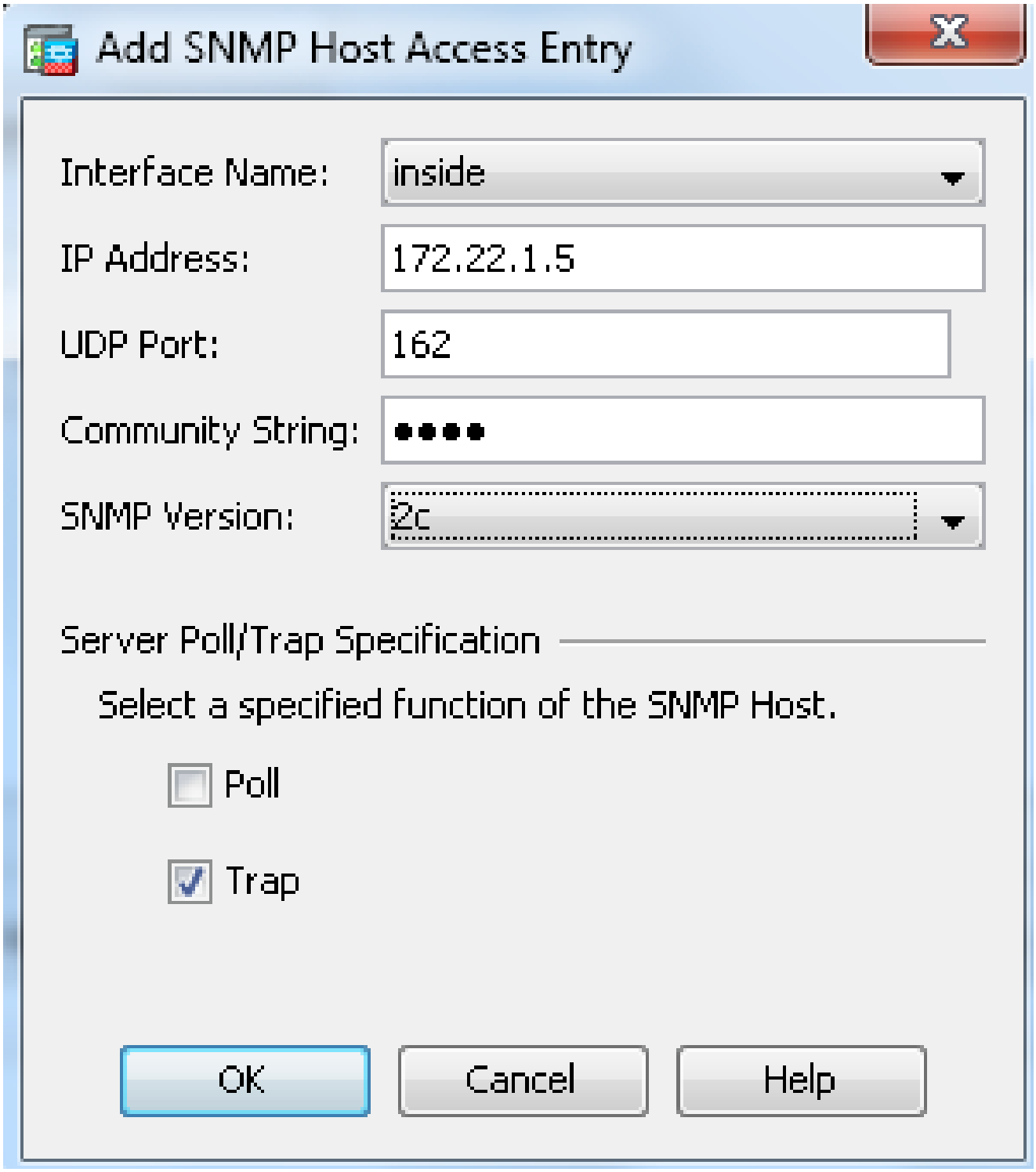
4. [Device Administration]、[Logging]、[choose SMTP] を選択し、プライマリ サーバ IP アドレスを入力して、SMTP サーバ IP アドレスを指定します。



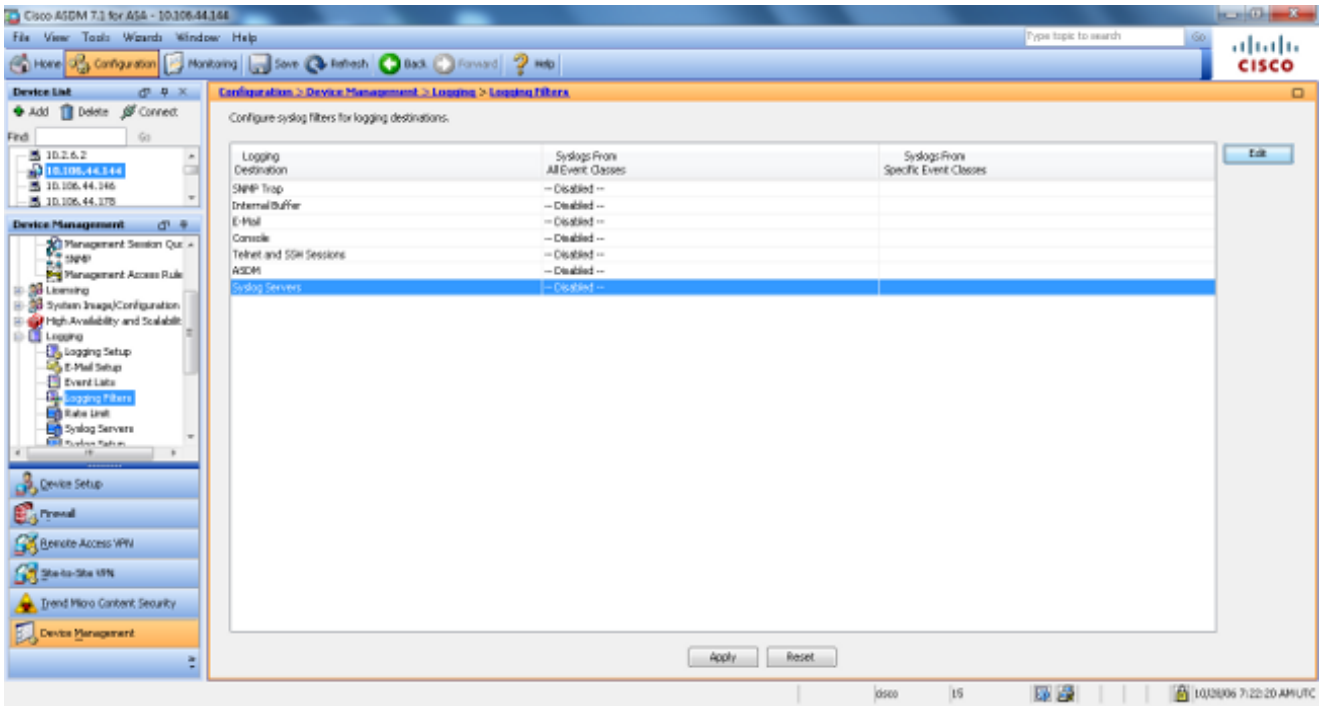
5. SNMP トラップとして syslog を送信するには、まず SNMP サーバを定義する必要があります。SNMP 管理ステーションとその特定のプロパティのアドレスを指定するには、[Management Access] メニューで [SNMP] を選択します。



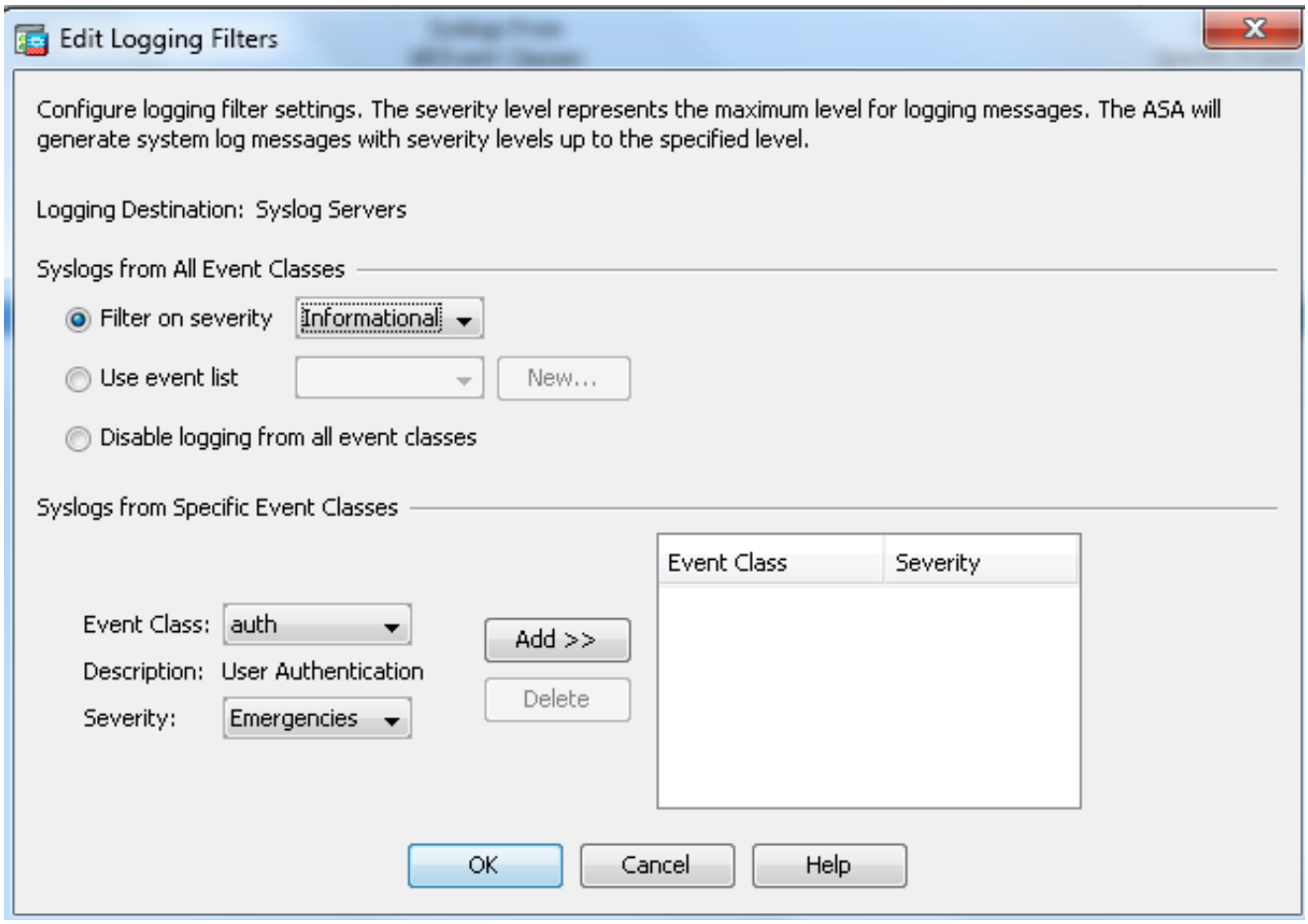
6. SNMP 管理ステーションを追加するには、[Add] をクリックします。SNMP ホストの詳細を入力して、[OK] .をクリックします。



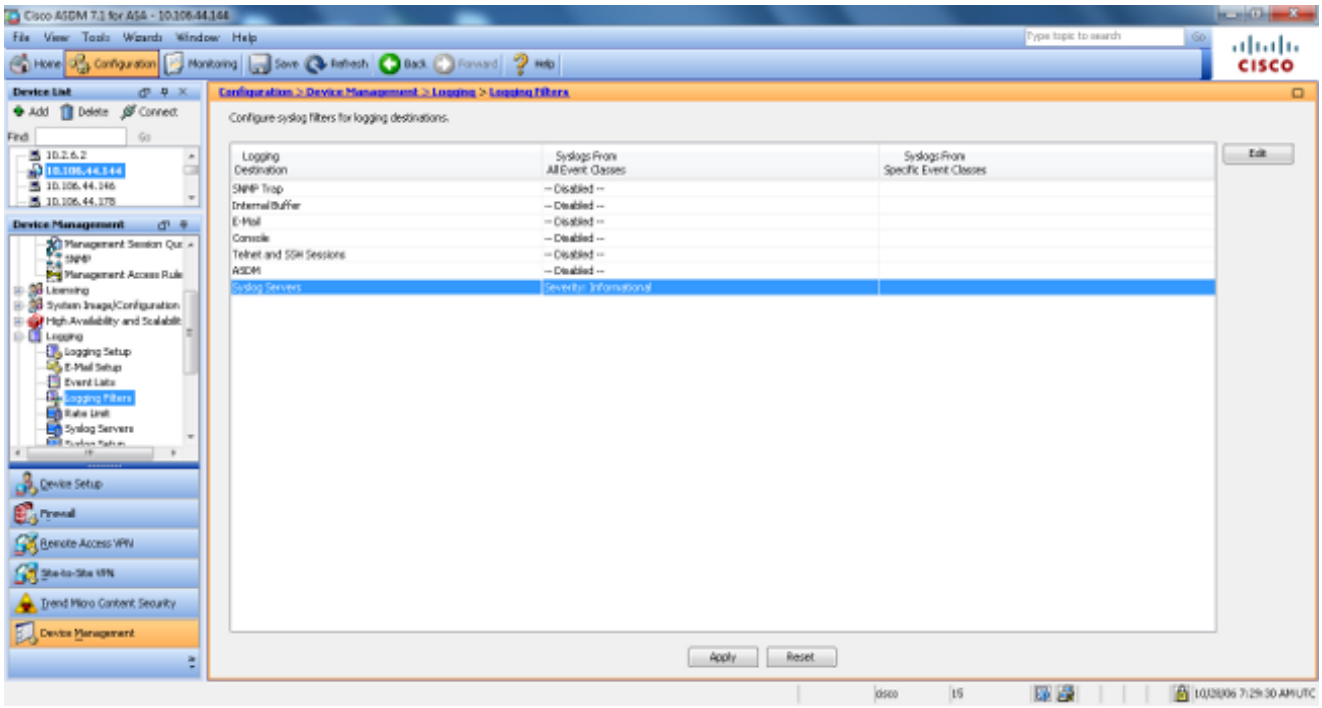
7. 前述の宛先のいずれかにログが送信されるようにするには、ロギング セクションで [Logging Filters] を選択します。これにより、可能なログの宛先およびこれらの宛先に送信される口グの現在のレベルがそれぞれ提示されます。目的の [Logging Destination] を選択して、[Edit] をクリックします。この例では、「syslog サーバ」の宛先が変更されます。



8. [Filter on severity] ドロップダウン リストから、適切な重大度（この場合は [Informational]）を選択します。完了したら、[OK] をクリックします。



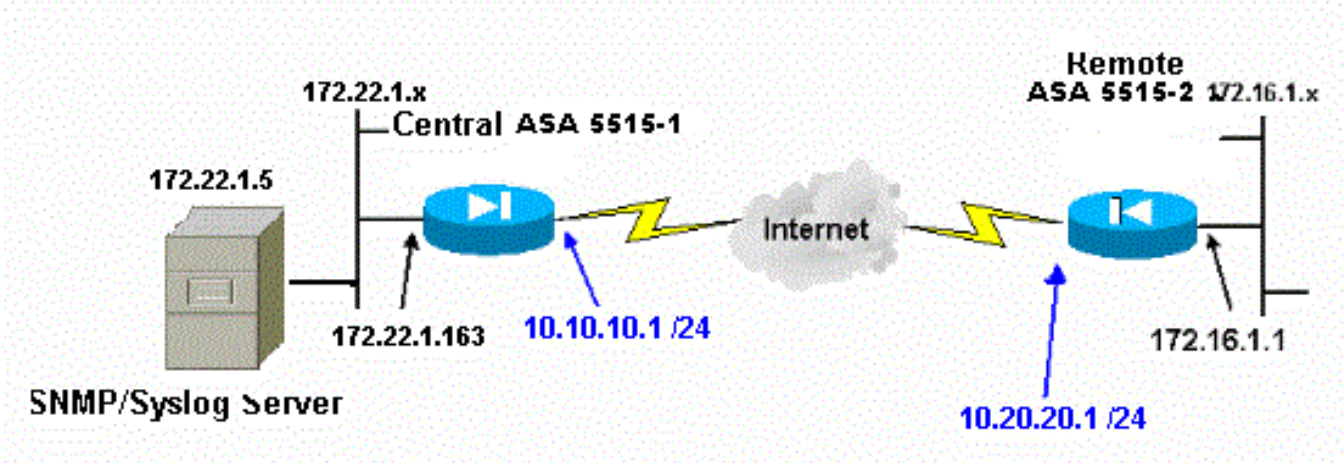
9. [Logging Filters] ウィンドウに戻ったら、[Apply] をクリックします。



VPN 経由での syslog サーバへの syslog メッセージの送信

単純なサイト間VPN設計でも、複雑なハブアンドスポーク設計でも、管理者は中央サイトに配置されたSNMPサーバとsyslogサーバですべてのリモートASAファイアウォールを監視できます。

サイト間のIPsec VPNの設定については、『PIX/ASA 7.x以降：PIX間VPNトンネルの設定例』を参照してください。VPN の設定とは別に、SNMP、および、syslog サーバの対象のトラフィックを、中央サイトとローカル サイトの両方で設定する必要があります。



中央 ASA 設定

<#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 *****
```

リモート ASA 設定

<#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 *****
```

ASA バージョン 8.4 の設定方法の詳細は、『VPN トンネルを通過する SNMP と syslog を使用した Cisco Secure ASA Firewall のモニタリング』を参照してください。

高度な syslog

ASA バージョン 8.4 が備えるメカニズムを使用すると、syslog メッセージのグループを設定して管理できます。このメカニズムには、メッセージの重大度、メッセージのクラス、メッセージの ID、またはユーザが作成するカスタム メッセージ リストが含まれます。このメカニズムを使用することで、単一のコマンドを入力して大小のメッセージ グループに適用できます。この方法で syslog を設定すると、指定したメッセージ グループからのメッセージをキャプチャでき、同じ重大度のメッセージをすべてキャプチャする必要はなくなります。

メッセージ リストの使用

メッセージ リストを使用して、関心のある syslog メッセージだけを重大度と ID でグループ化し、このメッセージ リストを目的の宛先と関連付けます。

メッセージ リストを設定するには、次の手順を実行します。

1. logging list message_list | level severity_level [class message_class] コマンドを入力して、指定された重大度レベルまたはメッセージ リストを持つメッセージが含まれるメッセージ リストを作成します。
2. 作成したばかりのメッセージ リストにメッセージをさらに追加するには、logging list message_list message syslog_id-syslog_id2 コマンドを入力します。
3. 作成したメッセージ リストの宛先を指定するには、logging destination message_list コマンドを入力します。

例 2

すべての重大度 2（クリティカル）メッセージと 611101 ～ 611323 の追加メッセージを含むメッセージ リストを作成し、メッセージをコンソールに送信するには、次のコマンドを入力します。

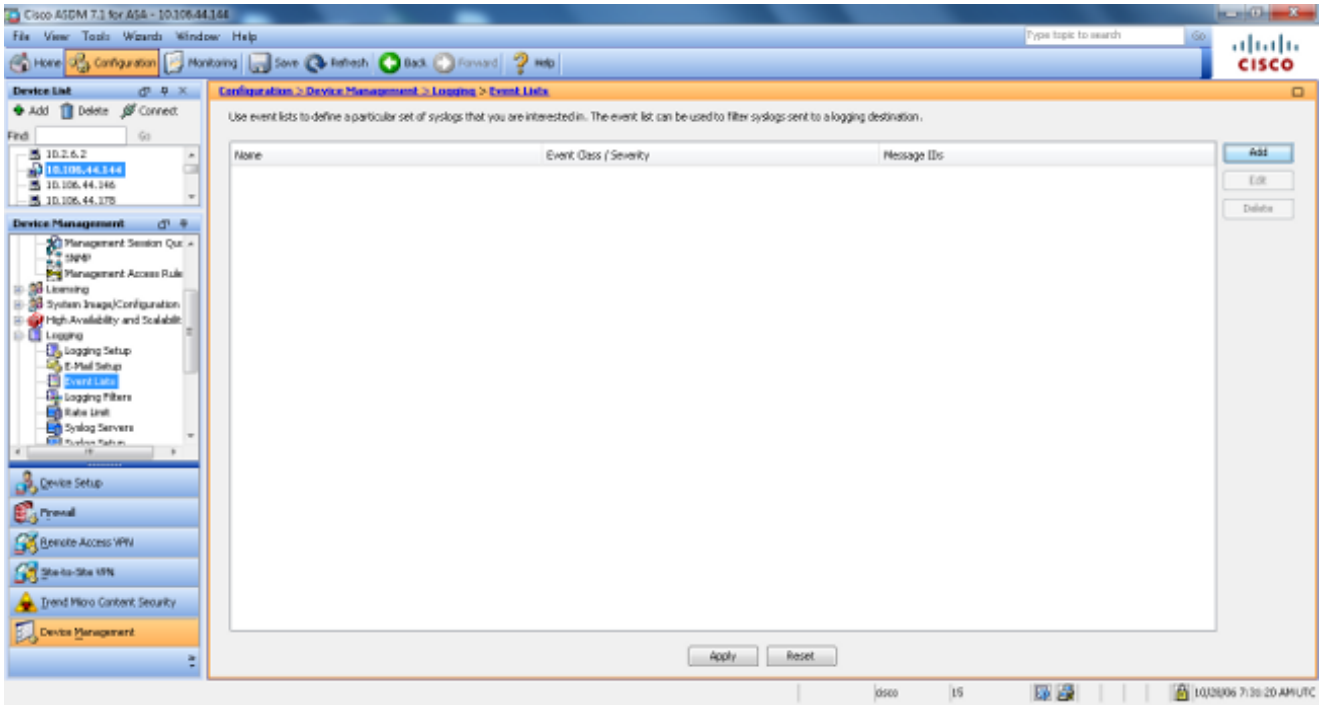
<#root>

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

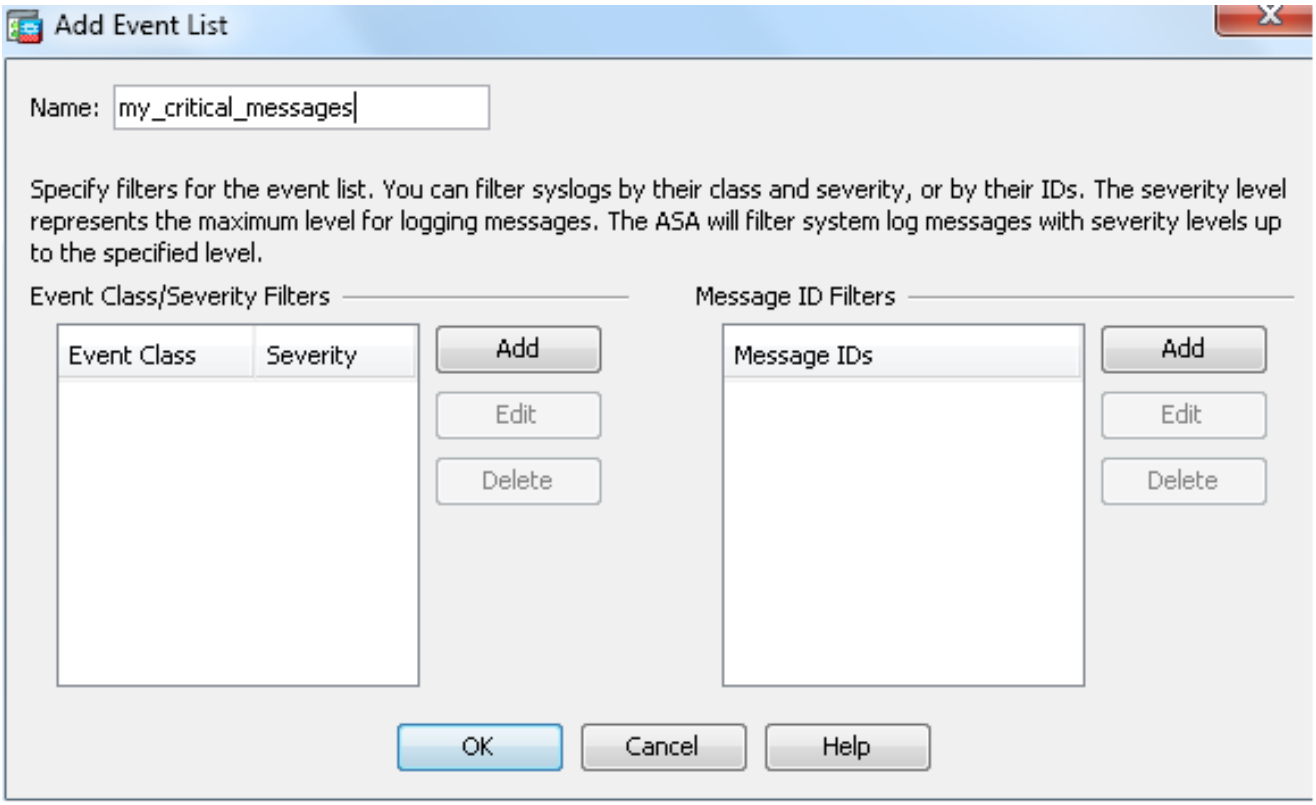
ASDM の設定

この手順は、メッセージ リストを使用する 例 2 に対する ASDM 設定を示しています。

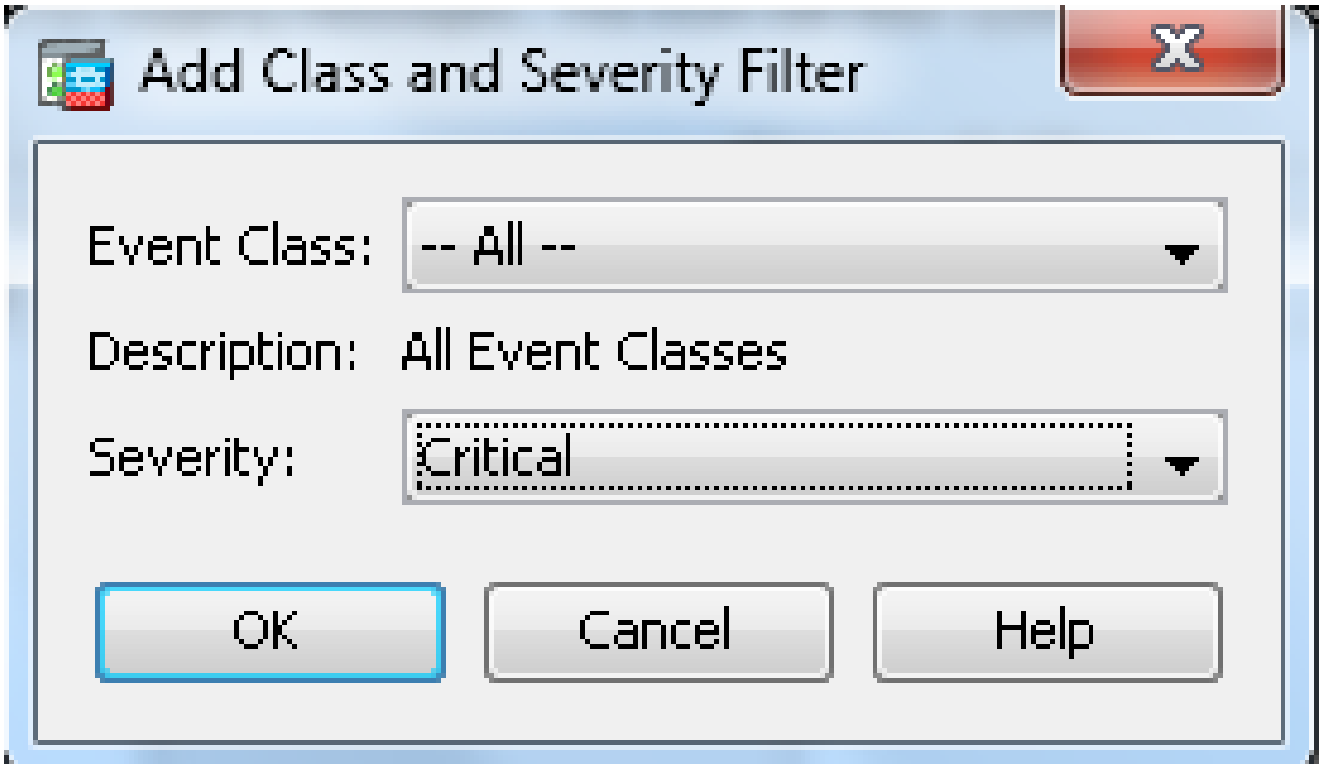
1. メッセージ リストを作成するには、[Logging] で [Event Lists] を選択して [Add] をクリックします。



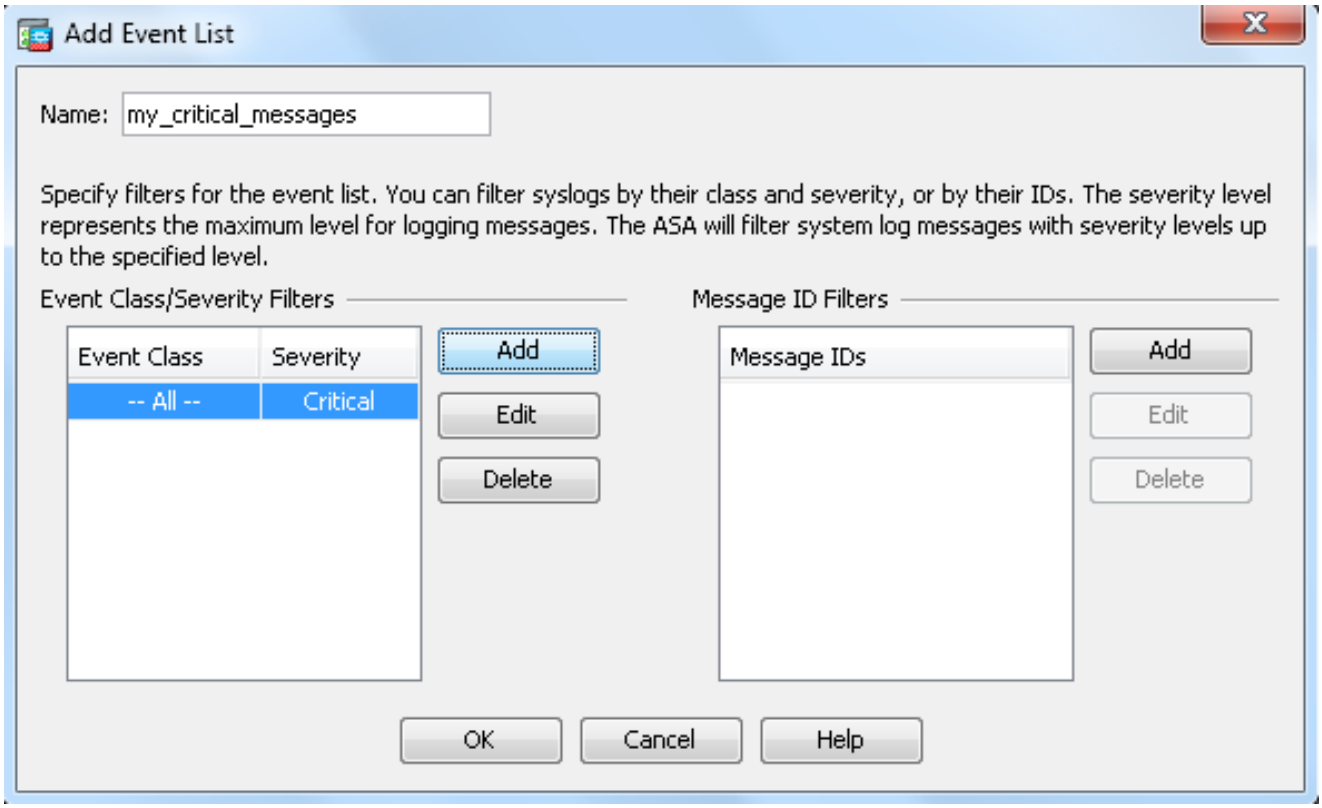
2. Name ボックスにメッセージ リストの名前を入力します。この場合は、my_critical_messages が使用されています。[Event Class/Severity Filters] の [Add] をクリックします。



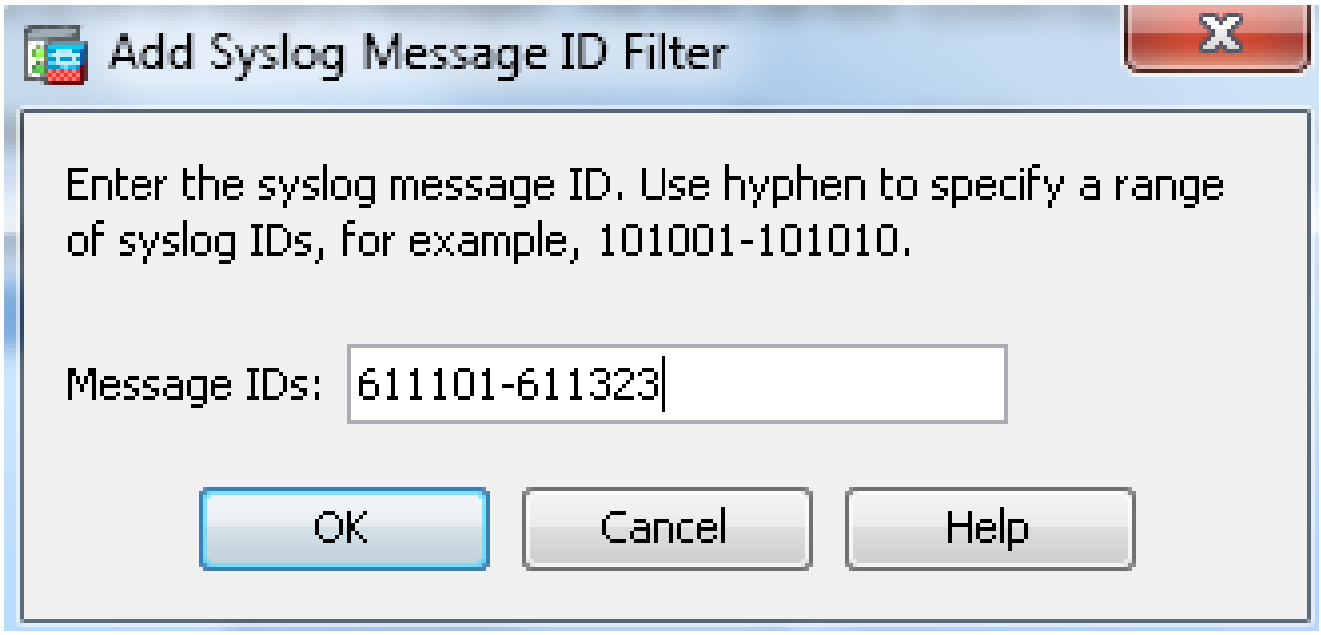
3. [Event Class] ドロップダウン リストから [All] を選択します。[Severity] ドロップダウン リストから [Critical] を選択します。完了したら、[OK] をクリックします。



4. さらにメッセージが必要な場合は、[Message ID Filters] の [Add] をクリックします。この場合は、ID が 611101 ～ 611323 のメッセージを指定する必要があります。

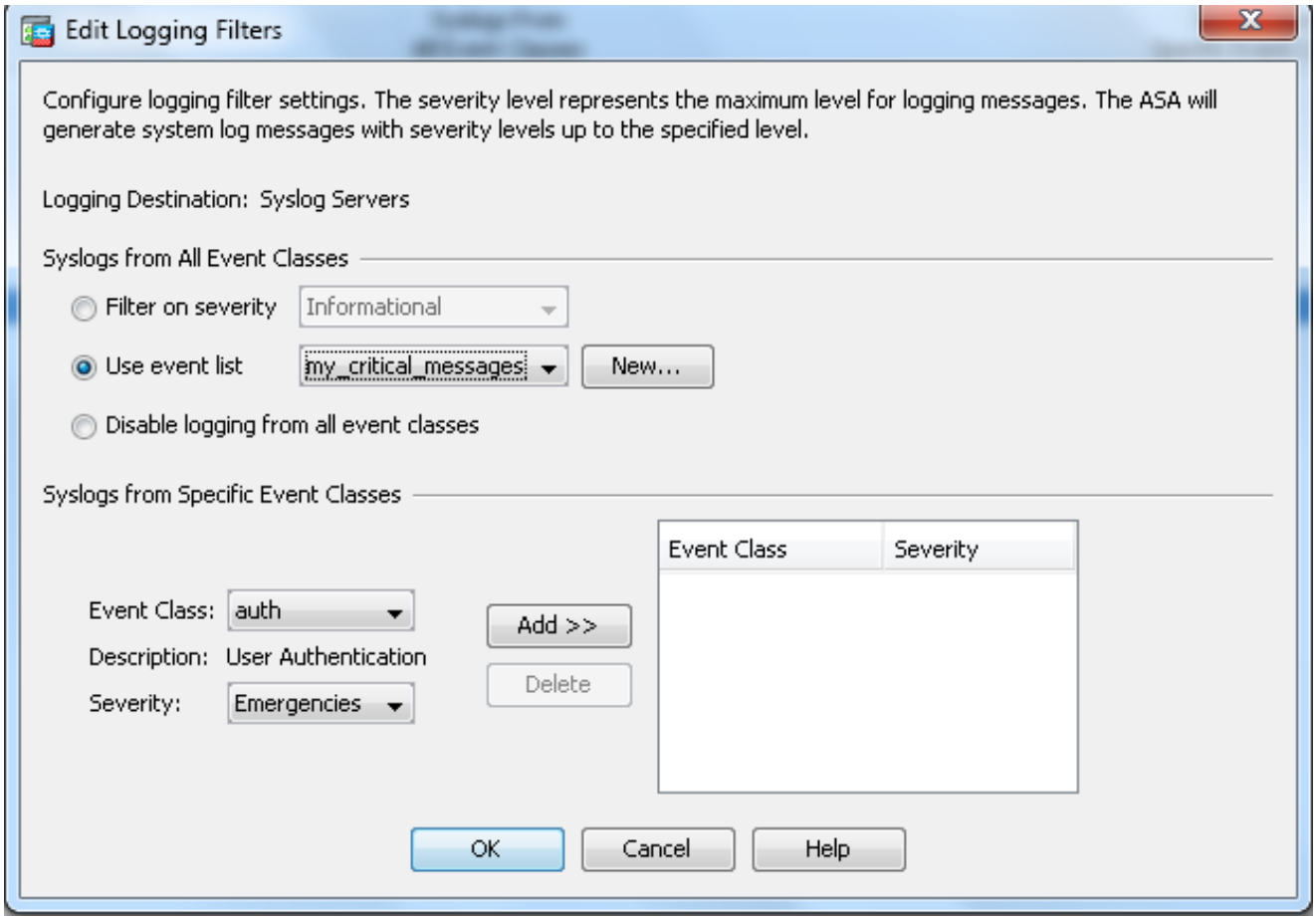


5. [Message IDs] ボックスに ID の範囲を入力し、[OK]をクリックします。

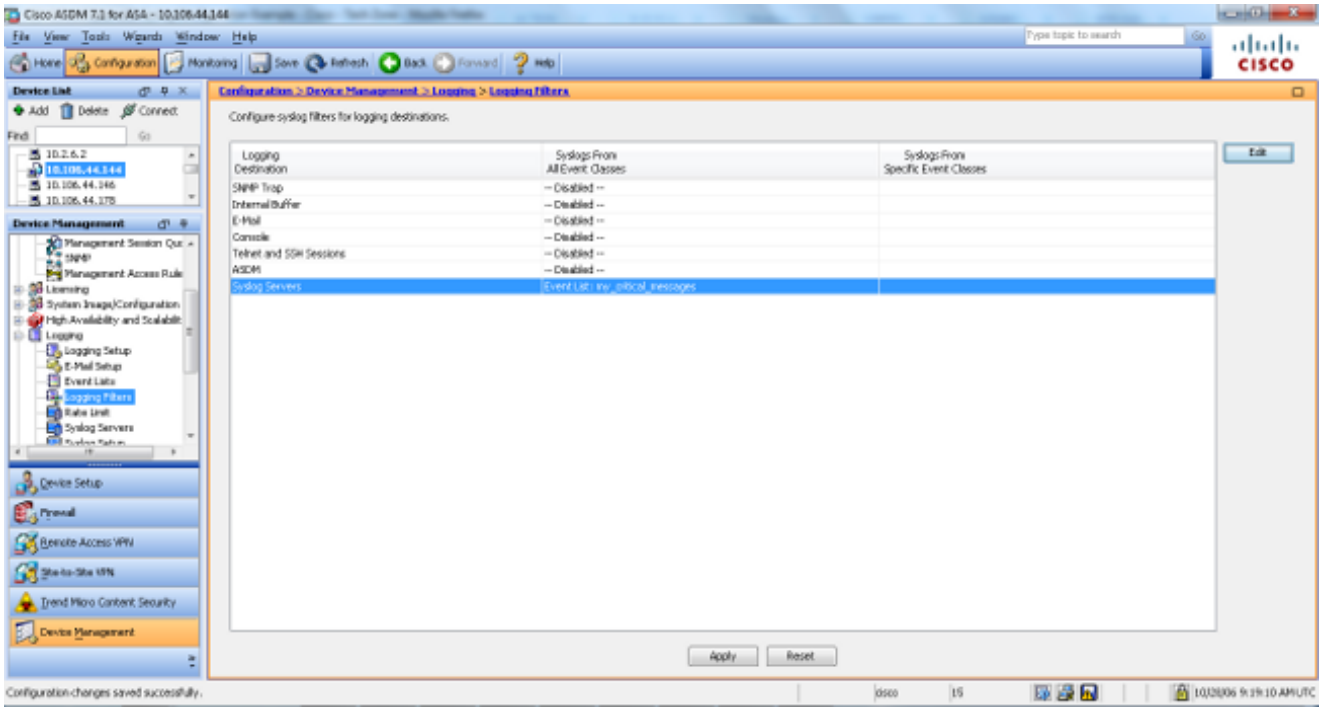


6. [Logging Filters] メニューに戻り、宛先として [Console] を選択します。

7. [Use event list] ドロップダウン リストから [my_critical_messages] を選択します。完了したら、[OK] をクリックします。



8. [Logging Filters] ウィンドウに戻ったら、[Apply] をクリックします。



これで、例 2 に示すように、メッセージ リストを使用する ASDM 設定が完了します。

メッセージ クラスの使用

特定のクラスに関連するすべてのメッセージを指定した出力場所に送信するには、メッセージ ク

ラスを使用します。重大度しきい値を指定すると、出力場所に送信されるメッセージの数を制限できます。

<#root>

logging class

 message_class destination | severity_level

例 3

重大度が緊急（Emergencies）以上のすべての ca クラス メッセージをコンソールに送信するには、次のコマンドを入力します。

<#root>

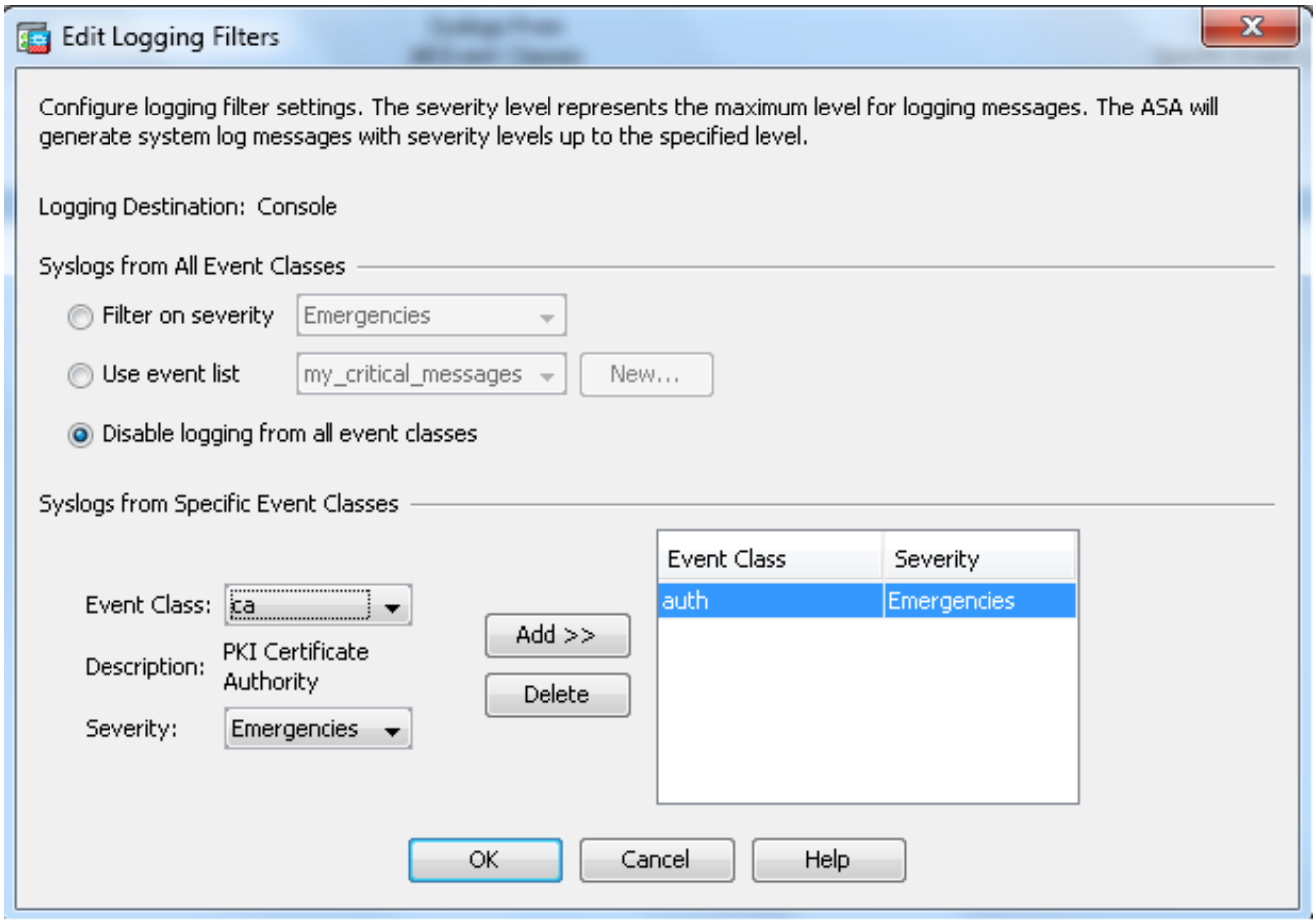
logging class ca console emergencies

ASDM の設定

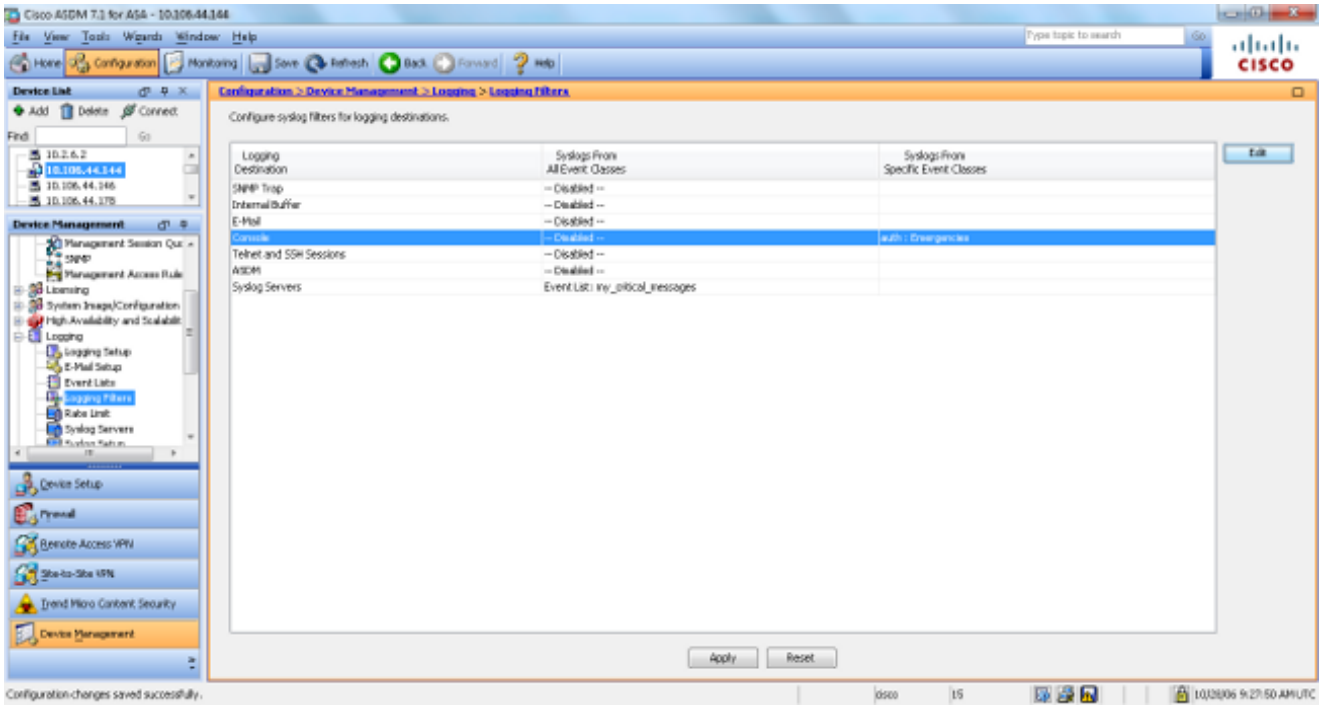
この手順は、メッセージ リストを使用する例 3 に対する ASDM 設定を示しています。

1. [Logging Filters] メニューを選択し、宛先として [Console] を選択します。
2. [Disable logging from all event classes] をクリックします。
3. Syslogs from Specific Event Classes で、追加する Event Class と Severity を選択します。

   この手順は [ca] および [Emergencies] をそれぞれ使用します。
4. [Add] をクリックしてこれをメッセージ クラスに追加し、[OK] をクリックします。



5. [Logging Filters] ウィンドウに戻ったら、[Apply] をクリックします。[Logging Filters] ウィンドウで示されるように、コンソールは ca クラスのメッセージで重大度が緊急（Emergencies）のものを収集するようになります。



これで、ASDM による「例 3」の設定は終了です。ログ メッセージの重大度の一覧は、『重大度別メッセージ一覧』を参照してください。

syslog サーバにデバッグ ログ情報を送信

高度なトラブルシューティングの場合、機能およびプロトコル固有のデバッグ ログが必要です。デフォルトでは、これらのログ メッセージは端末（SSH/Telnet）に表示されます。デバッグのタイプと生成されるデバッグメッセージのレートによっては、デバッグが有効になっている場合、CLIの使用が困難になる場合があります。オプションで、デバッグ メッセージを syslog プロセスにリダイレクトし、syslog として生成することができます。これらの syslog は、他の syslog と同様、任意の syslog 宛先に送信することができます。syslog にデバッグを転送するには、logging debug-trace コマンドを入力します。この設定は、syslog と同様に syslog サーバにデバッグ出力を送信します。

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

ロギング リストとメッセージ クラスの併用

LAN 間メッセージおよびリモート アクセス IPsec VPN メッセージのみの syslog をキャプチャするには、logging list コマンドを入力します。次の例では、すべての VPN（IKE および IPsec）クラスの syslog メッセージでデバッグ レベル以上のものがキャプチャされます。

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
```

ACL ヒットのログ

必要な各アクセス リスト エレメント（ACE）にログを追加して、アクセス リストがヒットしたときにログに記録します。次の構文を使用します。

<#root>

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

例

<#root>

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

ACL は、デフォルトでは拒否されたパケットをすべてログに記録します。拒否されたパケットに対して syslog を生成するために ACL を拒否するログ オプションを追加する必要はありません。[log] オプションを指定すると、適用される ACE に sylog メッセージ 106100 が生成されます。syslog メッセージ 106100 は、ASA ファイアウォールを通過するすべての一致する許可または拒否 ACE フローに対して生成されます。最初に一致したフローがキャッシュされます。以降の一致では、show access-list コマンドで表示されるヒット カウントが増分されます。[log] キーワードが指定されていないアクセス リストのデフォルトのロギング動作では、パケットが拒否されるとメッセージ 106023 が生成され、パケットが許可されると syslog メッセージは生成されません。

生成される syslog メッセージ（106100）に対しては、オプションの syslog レベル（0 ～ 7）を指定できます。レベルを指定しないと、新しい ACE はデフォルトのレベル 6（情報提供）になります。ACE がすでに存在する場合、現在のログ レベルは変更されません。[log disable] オプションが指定された場合、アクセス リスト ログは完全に無効になります。syslogメッセージ(メッセージ106023を含む)は生成されません。[log] デフォルト オプションは、デフォルトのアクセス リスト ログ動作を復元します。

syslog メッセージ 106100 をコンソール出力で表示するには、次の手順を実行します。

1. すべての出力場所への syslog メッセージの送信を有効にするには、logging enable コマンドを入力します。ログを表示するには、ロギング出力場所を設定する必要があります。
2. 特定のシステム ログ メッセージの重大度レベルを設定するには、logging message <message_number> level <severity_level> コマンドを入力します。

   この場合、logging message 106100 コマンドを入力して、メッセージ 106100 を有効にします。
3. logging console message_list | severity_level コマンドを入力して、発生した system log メ

ッセージをセキュリティ アプライアンス コンソール（tty）に表示できるようにします。severity_level を 1 ～ 7 に設定するか、レベル名を使用します。message_list 変数で送信されるメッセージを指定することもできます。

4. デフォルトの設定から変更された syslog メッセージの一覧、つまり異なる重大度が割り当てられたメッセージおよび無効にされたメッセージの一覧を表示するには、show logging message コマンドを発行します。

   show logging message コマンドの出力例を次に示します。

```
<#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
```

スタンバイ ASA での syslog 生成のブロック

ASAソフトウェアリリース9.4.1以降では、特定のsyslogがスタンバイユニットで生成されないようにし、次のコマンドを使用できます。

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

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

特定の syslog メッセージが syslog サーバに送信されないようにするには、次に示すようにコマンドを入力する必要があります。

```
<#root>

hostname(config)#

no logging message

 <syslog_id>
```

詳細は、logging message コマンドを確認してください。

%ASA-3-201008：新しい接続の拒否

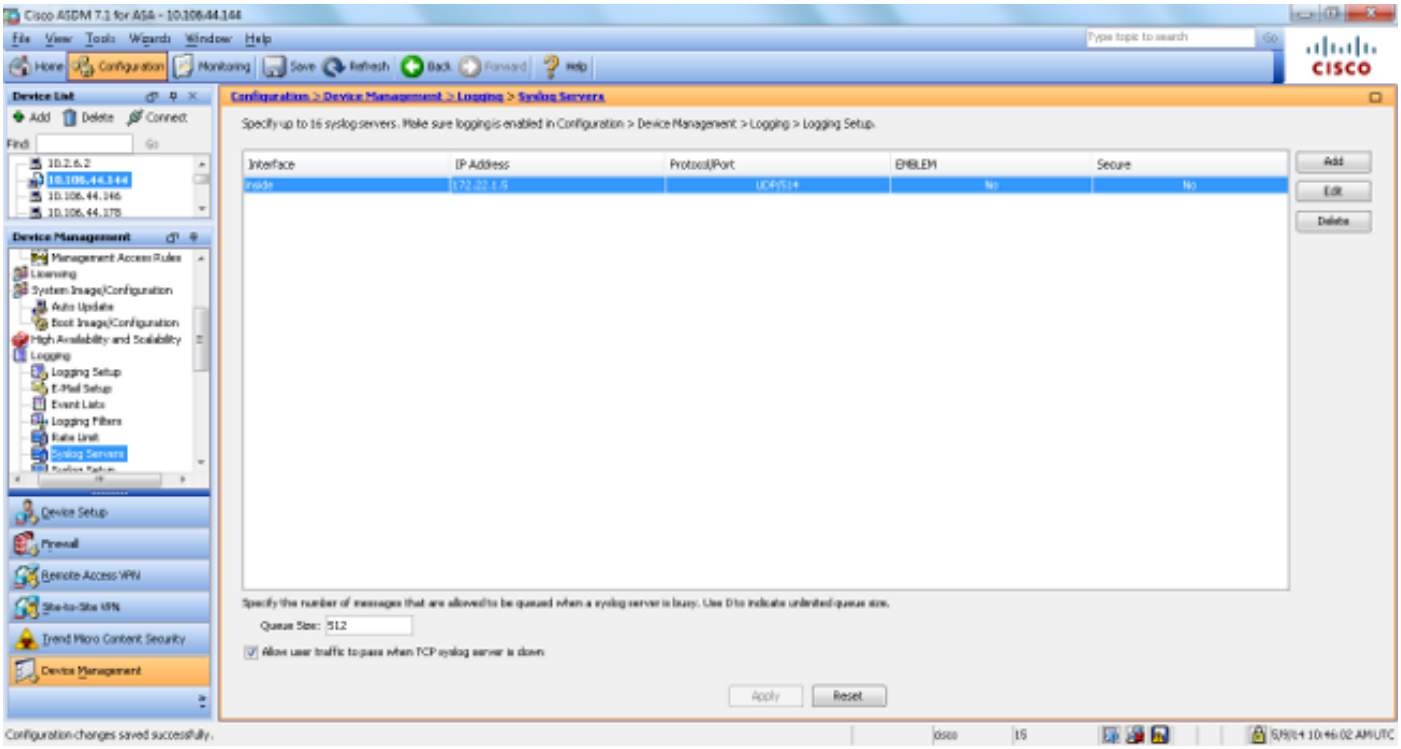
ASAがsyslogサーバに接続できず、新しい接続が許可されない場合、「`%ASA-3-201008: Disallowing new connections.`」エラーメッセージが表示されます。

解決方法

このメッセージは、TCP システム ログ メッセージングを有効にしても syslog サーバに到達できない場合、または Cisco ASA syslog サーバ（PFSS）を使用しており Windows NT システムのディスクが満杯になっている場合に表示されます。このエラー メッセージを解決するには、次の手順を実行してください。

- TCP のシステム ログ メッセージが有効になっている場合は無効にします。
- PFSS を使用している場合は、PFSS が常駐する Windows NT システム上のスペースを解放します。
- syslog サーバが動作しており、Cisco ASA コンソールからそのホストに ping できることを確認します。
- 次に、TCP システム メッセージ ロギングを再開してトラフィックを許可します。

syslog サーバがダウンし、TCP ログが設定される場合、logging permit-hostdown コマンドを使用するか、UDP ログに切り替えます。



関連情報

- Cisco Secure PIX ファイアウォール コマンド リファレンス
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。