# 適応型セキュリティアプライアンス (ASA)syslogの設定

内容
<u>はじめに</u>
<u>背景説明</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
基本 syslog
<u>内部バッファにログ情報を送信</u>
<u>syslog サーバにログ情報を送信</u>
<u>ログ情報を電子メールとして送信</u>
シリアル コンソールにログ情報を送信
<u>Telnet/SSH セッションにログ情報を送信</u>
ASDM 上にログ メッセージを表示
<u>SNMP 管理ステーションにログを送信</u>
<u>syslog にタイムスタンプを追加</u>
<u>例 1</u>
<u>基本 syslog を ASDM で設定</u>
<u>VPN 経由での syslog サーバへの syslog メッセージの送信</u>
<u> </u>
<u>同反な Systog</u> メッセージ リストの使用
<u>M</u> 2
ASDM の設定
<u>メッセージ クラスの使用</u>
<u>例3</u>
<u>ASDM の設定</u> ovelog サーバにデバッグ ログ桂根を送信
トラブルシュート
<u>- ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~</u>

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、『<u>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</u> <u>ド』を参照してください。</u>

## 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、『<u>ASA 8.2:ASDMを使用</u> 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 permithostdown 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、『<u>出力先を設定および管理するた</u> <u>めのコマンド』を参照してください。</u>重大度別にまとめたメッセージについては、『<u>重大度別メ</u> <u>ッセージー覧』を参照してください。</u>

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 にロ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 でロギングを有効にするには、まず基本ロギング 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。

Cisco ASEM 7.1 for ASA - 10.306.44	.164		- 0 <b>- X</b> -
File View Tools Wizards Windo	ow Help	topic to search Go.	ahaha
🕞 Hone 🦓 Cantiguration 🔀 Mon	Raina 🔚 Save 🔇 Fatesh 🔇 Bask 🔘 Farward 🧳 Hela		CISCO
Device List d* 9 ×	Configuration 2 Device Management 2 Logaing 5 Logaing Schup		
Add      Delete      Connect      Find     Go     10.2.6.2      J0.10.6.46.146      J0.106.44.146      J0.106.44.175      v	Enable logging     Enable logging     Enable logging on the fallover standby unit     Enable logging on the fallover standby unit     Enable logging as brief and avalage in EMBLEM format  Insigning to brief and avalage in EMBLEM format  Specify the size of the internal/buffer to which systogs will be saved. When the buffer fills up, it will be overwritten.		
Device Management d)	Buffer Size       1000000       bytes         You can choose to save the buffer contents before the buffer is werwitten.         Save Buffer Ter       If TP Server         Image: Term is the same for a parse of the queue for system intended for verying in ASDML.         Queue Save:       100		
By Device Management	Apply Reset		
	disco 15	3 107	28/06 7:00:00 AMUTC

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。

a Mars Tank Marsh Minds	and Male				Page topic to search	100
Hore Configuration	ikaring 🔄 Sove 🔇 Ratio	sh 🔾 Back 💭 Forward 🤗 I	elo		. The other is sense.	cisco
rvice List P = X	Configuration > Device M	lanagement > Logging > Syslog Se	EVERA.			
Add 1 Delete 💕 Connect.	Specify up to 16 syslop ser	vers. Hale sure logging is enabled in Co	nfiguration > Device Management > Logging > Logging 5	ietup.		
A 10.2.6.2 ×	Interface	IP Address	ProtoesUPort	EHBLEM	Secure	- Add
30.105.44.144						ErR
5 10.106.44.178 ×						Delete
rvice Management d' P		-				
Auto Update ·		( 1	Add Syslog Server			
I High-Availability and Scalabilit			abutan Inda			
Logging			ACTION INCOME			
E-Mail Setup			PAddrese: 172.22.1.5			
Event Lists			hotocol: 10 <sup>p</sup> e UDP			
Rate Linit			614 E14			
Sustan Servers			Log nessages in Osco EMBLEM format (UDP only)			
SMIP			Enable secure-syslog using SSUIILS			
Sout Californ						
· · · · · ·			OK. Calcel Hep			
Covice Setup		<u> </u>				
Crewal						
Remarke Access VPW						
Ste-to-Ste KPN	Specify the number of mea	rages that are allowed to be queued wh	en a sysiog server is busy. Use D to indicate unlimited que	eue eine.		
Trand Minor Contract East after	Queue Size: 512					
Dere Hoo Carwin Storky	Alos user traffic to pa	is when TCP systeg server is down				
Device Management			doole De	and the second se		
÷			Apply Me:	SPL		

 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。

Cisco ASEM 7.1 for ASA - 10.106.44	144	
File View Tools Wigards Winds	w Help Pype topic to search	🚳luulu
🕞 Hone 🦓 Configuration [ Mon	toring 🔚 Sove 🔇 Refresh 🔘 Bask 🔘 Forward 🧳 Help	CISCO
Device List d <sup>1</sup> P ×	Configuration > Device Hanagement > Logging > C-Hail Setup	0
Add Dots & Correct      Find     So     10.2.6.2     10.006.44.144     So     10.006.44.146     So	Enter the email address that will be used as the source address when systeps are sent as emails. Source Entel Address associated will be used as the source address when systeps are sent as emails. Enter the email address as a set of the email of the em	
Frendra Management at a	Destination 5-Pial Address Styles Severity	+00
Device Management () () The headparter (Access System Insight Configuration System Insight Co	Add E-Mail Recipient         Destination E-Hail Address:         Severity: Recupient bits recipient bits severity. The studio severity: Recuschfor this region: without the higher of the severity: recuschfor this recipient with set for all e-mail recipients in Configuration Physicies-Mogging PLogging Filters.         Systeg Severity:       Moltifications         Ook       Cancel	tali
50 Contraction	Apply Reset	
	15 100 124	1032806 7:07:10 AMUTC

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。

Cisco ASDM 7.1 for ASA - 10.106.44	4366		- 0 -X-
File View Tools Waards Windo	ow Help	Type topic to search 6	يالينان.
🚭 Hone 🦓 Cantiguration [ Mon	ntaing 🔜 Save 🔇 Refesh 🔇 Bad. 🔘 Farward 💡 Hela		CISCO
Device Link dp. 9 ×	Configuration > Device Management > Logang > SMDP		
Add Deter & Correct Find Go     Dotte:      Dotte	Configure the remote SHTP server IP address for sending-enal alerts and notifications in response to select events.  Remote SHTP Server Primary Server IP Address  IT2.22.8.10  Coptemal  Coptemal		
Chell Shup     Chell Shup     Chell Shup     Chell Shup     Chell Shup     Shup     Shup     Shup     Shup     Shup     Chell     Shup     Chell     Shup     Chell     Shup     Chell     Shup			
Control Security  Control Security  Control Security  Control Nono Content Security  Content Security			
2 Configuration-changes saved successfully.	Appr/ Meset	III III III III	5/9/64 10:46:02 AMUTC

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。

Cisco ASDM 7.1 for ASA - 10.306.44	144			_				
File View Tools Waards Windo	w Help					Type t	topic to search	🤷 սիսիս
🕤 Hore 🖧 Cantagration 💽 Mon	Raing 🔚 Save 🔇 Rahas	ih 🚺 Bask 🔘 F	Forward 🦿 Help					CISCO
Device List d <sup>1</sup> P ×	<b>Configuration &gt; Device Me</b>	magement > Mana	operated Access > 52502					0
Add Deleta & Correct      Find     So     So	Configure SMMP parameters Community String (default) Contant: ASA Location Listening Port: SSMMP Hast Access List Interface	and nonogenenit stat eneme admin office 1960 IP Address	tons. (sptionab Canhgure Traps Community String	9₩₽ Kersion	Usernares (IRMP-x-3 Crib)	Pol/Trap	uCPPort	Add Talk Delete
Participartie Antonio Frances	SMPv3 isses Configure SMPv3 users. Sp Group Name	ecfy extheritzation a Username	nd privacy options for users according to Encrypted Password	the group to which they belong. Authentication	DecyptionJ	Ugorithm .	A25.5m	Att Lik
Prevail     Bende Access VPN     Bende Access VPN     Bende Access VPN     Bende Access VPN     Dende Veno Cantent, Security     Dende Venopment								Delete
:				Apply Res	et.	Le IMA		Olivaria a constante da constante da
					ciseo	15	2	10,28,06 7:19:00 AMUTC

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。

🔄 Add SNMP Hos	t Access Entry
Interface Name:	inside 👻
IP Address:	172.22.1.5
UDP Port:	162
Community String:	••••
SNMP Version:	<b>2</b> c
Server Poll/Trap Sp Select a specified Poll I Trap	ecification ————————————————————————————————————
ОК	Cancel Help

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 されるロ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。

Cisco ASDM 7.3 for ASA - 10.306.44.	144					- 0 -X-
File View Tools Waards Windo	w Help				Type topic to search GO	ababa
🕤 Hone 🖓 Configuration 🔀 Moni	toring 🔚 Sove 🔇 Refresh 🔇 Bad	A 🚫 Forward 🧳 Help			_	CISCO
Device List d1 9 ×	<b>Configuration &gt; Device Management</b>	> Logging > Logging filters				
🗣 Add 📋 Delete 🖉 Correct.	Configure syslog filters for logging destina	tions.				
Find Go						
	Logging Destination	Syslogs From All Event: Classes		Syslogs From Specific Event Classes		La
- 5 10.106.44.146	SNMP Trap	- Disabled				
	Internal Buffer	Disabled				
Device Management d' +	Constin	- Codobit				
- Planagement Sension Quz +	Telnet and SSH Sessions	- Disabled				
Paragement Access Rule	ASDM	- Deabled				
a ge Liversing	Systog Servers	- Osabled				
🐵 🐉 System Inage/Configuration						
Pligh Availability and Scalabilit						
-B. Logging Setup						
-St-Mail Setup						
The Supervised and						
Synlog Servers						
Carlos Salar *						
💑 Device Setup						
🕄 Frend						
Remarke Access VPN						
Stela-StellN						
🚖 Irend Micro Cantent Security						
Device Management						1
:			Apply Reset			
				disto 15	🔯 🎒 🛛 👸 10,0	98/06 7122120 AMUTC

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。

Edit Logging Filters
Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.
Logging Destination: Syslog Servers
Syslogs from All Event Classes
Filter on severity     Informational:      New
O Disable logging from all event classes
Syslogs from Specific Event Classes
Event Class Severity
Event Class: auth  Add >>
Description: User Authentication Delete
Severity: Emergencies -
OK Cancel Help

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

Cisco ASDM 7.1 for ASA - 10.106-44.	144	-			0.	х
File View Tools Wizards Window	w Help			Pype topic to search	·	1.
🕤 Hore 🖧 Cantauration 🔀 Moni	toring 🔚 Sove 🔇 Refresh 🔇 Back 🤇	Forward 💡 Help			CISC	0
Device List d1 0 ×	Configuration > Device Management > Lo	ading > Logging filters				
🗢 Add 📋 Delete 🖉 Connect.	Configure syslog filters for logging destinations	5				
Find Go						
10.2.6.2	Logging Destination	Syslogs From All Event Classes		Syslogs From Specific Event Classes	Eak	
- 5 10.106.44.146	SNMP Trap	- Disabled				
10.100.44.0/0	Internal Buffer	Disabled				
Device Management d' +	Constitu	- Cedalar				
- Planagement Senson Quz +	Telnet and SSH Sessions	- Citabled				
Management Access Rule	ASDM	- Deabled				
10-36 Lioming	Syslog Servers	Severity: Informational				
B 35 System Inage/Configuration						
🗄 👷 High Availability and Scalabilit						
- De Longing Setup						
- Stellarbar						
- Divert Lata						
- Balangging Filters						
Solor Severa						
Turbon Tables						
* *						
🔒 Device Setup						
🕄 Frend						
Remote Access VPN						
Statu-Statin						
🚖 Trend Micro Cantent Security						
Device Management						
:			Apply Reset			
				disco 16 🔯 🚰	10,28006 7129 30	MUT

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、『<u>PIX/ASA 7.x以降:PIX間VPNトンネルの設定例</u>』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、『<u>VPN トンネルを通過する SNMP と syslog を使用し</u> 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

0

<#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。

Cisco ASDM 7.1 for ASA - 10.106.44	166					- 0 - X -
File View Tools Waards Winds	aar Help				Type topic to search	🤷 սևսևս
🕞 Hore 🦓 Cantiguissian 🔀 Mar	Roning 🔚 Sove 🔇 Rohesh 🔇 Bac	k 🔘 Forward 💡 Help				CISCO
Device List d <sup>a</sup> 4 ×	Configuration > Device Management	> Logging > Event Lists				0
Add      Delete      Groved:	Use event lists to define a particular set of	f syslogs that you are interested in. The event list can	te used to filter syslogs sent to a loggi	ng destination.		
- 5 10.2.6.2 *	None	Event Class (Sevenity		Message IDs		Add
10.105.44.144						1.9
- 5 10.106.44.178 *						Tables
Device Management (1 +						Tranca
- Planagement Sension Qut +						
Paragement Access Rule						
B 3 System Snage/Configuration						
High Availability and Scalabilit Locative						
Logging Setup						
Every Late						
- Logging Filters						
Syslog Servers						
d 10 salar taken						
🔏 Device Setup						
C Preval						
Benate Access VPN						
Statu-Station						
🚖 Irend Micro Content Security						
Device Management	· · · · · · · · · · · · · · · · · · ·					
:			Apply Reset			
				disco 15	1 🖓 🖓 👘 👘	10,0806 7:38:20 AMUTC

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。

t Class/Sever	ity Filters ——		Message ID Filters	
vent Class	Severity	Add	Message IDs	Add
		Edit		Edit
		Delete		Delete
		Delete		

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。

Add Class and Severity Filter
Event Class: 🛛 All 🗸
Description: All Event Classes
Severity:
OK Cancel Help

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。

<b>E</b>	Add Event List				×				
Name: my_critical_messages									
Specify filters for the event list. You can filter syslogs by their class and severity, or by their IDs. The severity level represents the maximum level for logging messages. The ASA will filter system log messages with severity levels up to the specified level.									
Ev	ent Class/Severity	y Filters ———		Message ID Filters					
	Event Class	Severity	Add	Message IDs	Add				
	All	Critical	Edit		Edit				
			Delete		Delete				
OK Cancel Help									

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。

🔂 Add Syslog Message ID Filter
Enter the syslog message ID. Use hyphen to specify a range of syslog IDs, for example, 101001-101010.
Message IDs: 611101-611323
OK Cancel Help

- 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。

	Edit Logging Filters							
	Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.							
	Logging Destination: Syslog Servers							
	Syslogs from All Event Classes							
	Filter on severity Informational							
	O Use event list my_critical_messagesi    New							
	Disable logging from all event classes							
	Syslogs from Specific Event Classes							
	Event Class Severity							
	Event Class: auth							
	Description: User Authentication							
	Severity: Emergencies -							
	OK Cancel Help							
L								

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

Cisco ASDM 7.1 for ASA - 10.106.44.1	64 Thereads Class. Test lines 10	addrived a read of the				- 0 - X
File View Tools Woards Window	er Help				Pype topic to search	60 alsola
🚯 Hore 🦓 Cartige atom 🔯 More	oring 🔄 Sove 🔇 Refresh 🔇 Bac	A 🔘 Forward 💡 Help				cisco
Device List d1 4 ×	<b>Configuration &gt; Device Management</b>	> Logging > Logging filters				0
Add      Delete      Second Connect      Find     Go	Configure syslog filters for logging destine	itons.				
10.2.6.2	Logging Destination	Syslogs From All Event: Classes		Syslogs From Specific Event Classes		Edit
- 5 10.106.44.146 - 5 10.106.44.178	SNMP Trop Internal Buffer	- Disabled				
Device Management d +	E-Hol	- Oissted				
Management Sension Qut +	Telet and SSH Sessions	- Deated - Deated				
Planagement Access Rule	Systep Servers	Event List: ny_pitical_ne	scopes			_
High Availability and Scalabilit League Classify Statup Chall Statup The League The League The League The League The League The League The League The League The League						
🔒 Device Setup 🛃 Proval						
Remote Access VPN						
Statu-Statin						
🚖 Irend Micro Content Security						
Devis Management			Apply Reset			
Configuration-changes saved successfully.				disco 15	III III III III III III III III III II	10/28/06 9:19:10 AMUTO

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。

Edit Logging Filters	Long-Top			×				
Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.								
Logging Destination: Cor	nsole							
Syslogs from All Event Cl	asses							
🔘 Filter on severity	Emergencies 🚽							
🔘 Use event list	O Use event list my_critical_messages → New							
Oisable logging fro	m all event classes							
Syslogs from Specific Eve	ent Classes							
		Event Class	Severity					
Event Class: ca		auth	Emergencies					
Description: PKI Certificate Add >> Add >> Delete								
Severity: Emergencies -								

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。

Cisco ASDM 7.3 for ASA - 10.306.44	166			- 0 - X
File View Tools Wgards Windo	er Help		Type topic to rearch	© de de
🕤 Hone 🦓 Cantiguestian 📝 Mon	koring 🔚 Sove 🔇 Refresh 🔇 Back 🤅	Farward 🦻 Help		CISCO
Device List d <sup>1</sup> P ×	Configuration > Device Management > Lo	nation > Longing filters		0
Add      Delete      Correct      Find     Go	Configure syslog filters for logging destination	6		
10.2.6.2	Logging Destination	Systops From All Event: Classes	Syslags From Specific Event Classes	t a
- 5 10.106.44.146 - 5 10.106.44.175 *	SNMP Trop Internal Buffer	- Cisisted		
Device Management	E-Mail	- Disabled		
Management Sension Qut +	Conscie	- Disabled	auth : Energencies	
54 5940	Telnet and SSH Sessions	- Osabled		
Paragement Access Rule	System Servers	Event List: nv: pitical nessages		
Styten Inage/Configuration Figh.Available Configuration Figh.Available Fightspace Fight		Apply Reset		
•				
Configuration changes saved successfully.			oiseo 15 🔛 🚰 🖬	10,028/06 9127.50 AMUT

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、『<u>重大度</u> <u>別メッセージー覧</u>』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 <br/> <b

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。

Cisco ASDM 7.1 for ASA - 10.106.44	164					- 0 - X-
File View Tools Wgards Windo	ev <u>H</u> elp				Type topic to search	© alate
🕞 Hone 🧏 Cantagration [ Mon	Raing 🔚 Save 🔇 Rah	esh 🔇 Back 🜔 Forward 🧳 Help				CISCO
Device List d <sup>1</sup> 4 ×	Configuration > Device ?	Sanagement > Logging > Syslog Servers				
🗣 Add 📋 Delete 🖉 Connect	Specify up to 16 syslop se	rvers. Hale sure logging is enabled in Configurati	on > Device Management > Logging > Loggi	ig Setupi		
Find Go	[	10 4 4 4 4 4	Real and Market	2 C D I		
- 102.6.2	Interface	IP Address	Protocil/Port	EVELEM	Secure	H21
- 3 30.106.44.146	1001	172-22-1.6	0.045514	N)	No	£.0R
10.106.44.178 *						Delete
Device Management d +						
Management Access Rules A						
Storning						
Ante Update						
Boot Image/Configuration						
Pigh Availability and Scalability 🗉						
La Logono						
- 1 Evant Lata						
- By Logging Filters						
- Fit Solat Servers						
Tarles Sales *						
🔒 Device Setup						
🕄 Frend						
Benate Access VPN						
🚱 Statu-Station	Specify the number of mes	mages that are allowed to be queued when a eye	ing server is busy. Use D to indicate orderited	queue size.		
A Trend Micro Content Security	Queue Ster: 512					
	V Alove user traffic to pa	as when TCP systing server is down				
Device Management						
-			Apply	Reset.		
				1		100
Configuration-changes saved successfully.				(Cisto)	15	5/9/04 10:46:02 AMUTC



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

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。