Configuración del registro del sistema del dispositivo de seguridad adaptable (ASA)

Contenido

Introducción
Antecedentes
Prerequisites
Requirements
Componentes Utilizados
Syslog básico
Enviar información de registro al búfer interno
Enviar información de registro a un servidor Syslog
Enviar información de registro como correos electrónicos
Enviar información de registro a la consola serie
Enviar información de registro a una sesión Telnet/SSH
Visualización de mensajes de registro en el ASDM
Enviar registros a una estación de administración SNMP
Agregar marcas de tiempo a registros del sistema
Ejemplo 1
Configuración de Syslog Básico con ASDM
Enviar mensajes Syslog a través de una VPN a un servidor Syslog
Configuración de ASA central
Contiguracion de ASA remoto
Sysiog avanzado
Utilizar la lista de mensajes
Configuración de ASDM
Utilizar la clase de mensaje
Ejemplo 3
Configuración de ASDM
Enviar mensajes de registro de depuración a un servidor Syslog
Uso conjunto de listas de registro y clases de mensajes
Registro de Aciertos de ACL
Bloqueo de la generación de syslog en un ASA en espera
Verificación
Troubleshoot
%ASA-3-201008: no permitir nuevas conexiones
Solución
Información Relacionada

Introducción

Este documento describe una configuración de ejemplo que muestra cómo configurar diferentes opciones de registro en ASA que ejecuta código versión 8.4 o posterior.

Antecedentes

La versión 8.4 de ASA ha introducido técnicas de filtrado muy granulares para permitir que sólo se presenten determinados mensajes de syslog especificados. La sección Syslog Básico de este documento muestra una configuración de syslog tradicional. La sección Syslog avanzado de este documento muestra las nuevas funciones de syslog en la versión 8.4. Consulte <u>Cisco Security</u> <u>Appliance System Log Messages Guides</u> para obtener la guía completa de mensajes de registro del sistema.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5515 con software ASA versión 8.4
- Versión 7.1.6 de Cisco Adaptive Security Device Manager (ASDM)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Nota: Refiérase a <u>ASA 8.2: Configure Syslog usando ASDM</u> para obtener más información para obtener detalles de configuración similares con ASDM versión 7.1 y posteriores.

Syslog básico

Ingrese estos comandos para habilitar el registro, ver los registros y ver las configuraciones.

- logging enable Habilita la transmisión de mensajes syslog a todas las ubicaciones de salida.
- no logging enable Deshabilita el registro en todas las ubicaciones de salida.
- show logging Enumera el contenido del buffer de syslog así como la información y las estadísticas que pertenecen a la configuración actual.

El ASA puede enviar mensajes de syslog a varios destinos. Ingrese los comandos en estas secciones para especificar las ubicaciones a las que desea que se envíe la información de syslog:

Enviar información de registro al búfer interno

```
<#root>
logging buffered
severity_level
```

No se requiere software o hardware externo cuando almacena los mensajes de syslog en el buffer interno de ASA. Ingrese el comando show logging para ver los mensajes syslog almacenados. El búfer interno tiene un tamaño máximo de 1 MB (configurable con el comando logging buffer-size). Como resultado, se puede envolver muy rápidamente. Tenga esto en cuenta cuando elija un nivel de registro para el búfer interno, ya que los niveles más detallados de registro pueden llenar y ajustar rápidamente el búfer interno.

Enviar información de registro a un servidor Syslog

```
<#root>
logging host
interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
logging trap
severity_level
logging facility
number
```

Se requiere un servidor que ejecute una aplicación syslog para enviar mensajes syslog a un host externo. ASA envía syslog en el puerto UDP 514 de forma predeterminada, pero se puede elegir el protocolo y el puerto. Si se elige TCP como protocolo de registro, esto hace que ASA envíe syslogs a través de una conexión TCP al servidor syslog. Si no se puede acceder al servidor o no se puede establecer la conexión TCP con el servidor, el ASA, de forma predeterminada, bloquea TODAS las conexiones nuevas. Este comportamiento se puede inhabilitar si habilita logging permit-hostdown. Vea la guía de configuración para obtener más información sobre el comando logging permit-hostdown.

Nota: ASA solo permite puertos que oscilan entre 1025-65535. El uso de cualquier otro puerto produce este error: ciscoasa(config)# logging host tftp 192.168.1.1 udp/516 ADVERTENCIA: el nivel de seguridad de la interfaz Ethernet0/1 es 0.

Enviar información de registro como correos electrónicos

<#root>
logging mail
severity_level
logging recipient-address
email_address
logging from-address
email_address
smtp-server
ip_address

Se requiere un servidor SMTP cuando envía los mensajes de syslog en correos electrónicos. Es necesaria una configuración correcta en el servidor SMTP para garantizar que pueda retransmitir correctamente los correos electrónicos del ASA al cliente de correo electrónico especificado. Si este nivel de registro se establece en un nivel muy detallado, como debug o informational, puede generar un número significativo de registros del sistema ya que cada correo electrónico enviado por esta configuración de registro hace que se generen hasta cuatro o más registros adicionales.

Enviar información de registro a la consola serie

<#root>
logging console
severity_level

El registro de la consola permite que los mensajes de syslog se muestren en la consola ASA (tty) a medida que se producen. Si se configura el registro de la consola, toda la generación de registro en el ASA se limita a una velocidad de 9800 bps, la velocidad de la consola serial del ASA. Esto puede hacer que los syslogs se descarten en todos los destinos, que incluyen el buffer interno. No utilice el registro de la consola para los syslogs detallados por esta razón.

Enviar información de registro a una sesión Telnet/SSH

<#root>

logging monitor

severity_level
terminal monitor

El monitor de registro permite que los mensajes de syslog se muestren cuando se accede a la consola ASA con Telnet o SSH y el comando terminal monitor se ejecuta desde esa sesión. Para detener la impresión de registros en su sesión, ingrese el comando terminal no monitor.

Visualización de mensajes de registro en el ASDM

<#root>
logging asdm
severity_level

ASDM también tiene un buffer que se puede utilizar para almacenar mensajes de syslog. Ingrese el comando show logging asdm para visualizar el contenido del buffer syslog ASDM.

Enviar registros a una estación de administración 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
```

Los usuarios necesitan un entorno SNMP (Simple Network Management Protocol) funcional existente para enviar mensajes syslog con SNMP. Consulte <u>Comandos para configurar y</u> <u>administrar destinos de salida</u> para obtener una referencia completa de los comandos que puede utilizar para establecer y administrar destinos de salida. Consulte <u>Mensajes enumerados por nivel</u>

de gravedad para ver los mensajes enumerados por nivel de gravedad.

Agregar marcas de tiempo a registros del sistema

Para ayudar a alinear y ordenar los eventos, se pueden agregar marcas de tiempo a los syslogs. Esto se recomienda para ayudar a rastrear los problemas en función del tiempo. Para habilitar las marcas de tiempo, ingrese el comando logging timestamp. Aquí hay dos ejemplos de syslog, uno sin la marca de tiempo y otro con:

```
%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
```

Ejemplo 1

Este resultado muestra una configuración de ejemplo para iniciar sesión en el buffer con el nivel de gravedad de debugging.

<#root>

logging enable logging buffered debugging

Ésta es una salida de ejemplo.

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

Configuración de Syslog Básico con ASDM

Este procedimiento muestra la configuración de ASDM para todos los destinos syslog disponibles.

 Para habilitar el registro en el ASA, primero configure los parámetros de registro básicos. Elija Configuration > Features > Properties > Logging > Logging Setup. Marque la casilla de verificación Enable logging para habilitar syslogs.



2. Para configurar un servidor externo como destino para syslogs, elija Syslog Servers en Logging y haga clic en Add para agregar un servidor syslog. Ingrese los detalles del servidor syslog en el cuadro Add Syslog Server (Agregar servidor Syslog) y elija OK cuando termine.

ie View Tools Wizards Winds	w Help				Type topic to search	60
hore 🖧 Cantagentan 🛐 Mar	Roing 🔚 Sove 🔇 Retre	sh 🔿 Back. 🕥 Forward 🤗 H	fo			cisco
evice List d ^{p.} P.X.	Configuration > Device M	magement > Logging > Syring Ser	YARA.			
Add 👔 Delete 💕 Connect.	Specify up to 16 syslog serv	ers. Make sure logging is enabled in Con	Rguration > Device Management > Logging > Logging S	etup		
- 10.2.6.2 ×	Interface	IP Address	Protocul/Port	D18.EM	Secure	444
10.105.44.144						Edit
10.106.44.176 v						Delete
nice Management d' P		-				
Auto Update *		(B)	Add Syslog Server	1		
High Availability and Scalabilit			autors [auto			
Logging			errore ersee •			
E-Mail Setup			Address: 172.22.1.5			
Event Lists		P	otocol: 10 @ UDP			
Rate Linit		~	xti 514			
- Sustan Servers		E	Log nessages in Gsco EMBLEM format ().0P only)			
SMTP		1	Enable secure-syslog using SSU/ILS			
Sout Californ						
18 +			Carcar resp			
Cevice Setup		· · · · · · · · · · · · · · · · · · ·				
C Typesal						
Bemake Access VPW						
Ste-to-Ste KFN	Specify the number of mean	ages that are allowed to be queued whe	n a nyelog server is busy. Use D to indicate unlimited que	nae sizm.		
Trend Micro Content Security	Queue Ster: 512					
a sea caro convert severy	Alon user traffic to pas	e when TCP systing server is down				
Device Management						

3. Elija E-Mail Setup in Logging para enviar mensajes syslog como correos electrónicos a destinatarios específicos. Especifique la dirección de correo electrónico de origen en el cuadro Dirección de correo electrónico de origen y elija Agregar para configurar la dirección de correo electrónico de destino de los destinatarios de correo electrónico y el nivel de gravedad del mensaje. Haga clic en Aceptar cuando haya terminado.

Cisco ASEM 7.1 for ASA - 10.106.44	144	- 0 8
File View Tools Wigards Winds	w: Help Pype topic to earth	🚳 ahaha
🕞 Hone 🦓 Configuration [Mon	taring 🔜 Save 🔇 Refresh 🔇 Bast 🔘 Forward 💡 Heb	CISCO
Device List d ¹ P ×	Configuration > Device Honogenent > Logging > E-Had Setup	
Add Dots & Connect Find So 10.2.6.2 10.2.6.4 10.006.44.144 So 10.006.44.146 So 10.006.44.176 So	Enter the e-mail address that will be used as the source address when syskips are sent as e-mails. Source E-Hail Address assaysing@test.com E-Hail Registerts	
Denire Management (7) 8	Leadonadori z-hasi Addesai Sylatig Sirvercy	
	Add E-Mail Recipient Destination E-Mail Address: Effer the systeps sent to this recipient by serverity. The systep serverity lifer used for their recipient by serverity. The systep serverity is setted babas and the globality for their and e- recipients in Configuration Physics Hosping Filters. Systep Serverity: Math Colors OK Cancel	tuit
5 POLINI THE REAL	Apply Reset	
	0500 15 24 25	1002806 7 07 10 AMUTC

4. Elija Device Administration, Logging, elija SMTP, e ingrese la dirección IP del servidor primario para especificar la dirección IP del servidor SMTP.

Cisco ASDM 7.3 for ASA - 10.306.44	344		- 0 - X-
File View Tools Wgards Winds	aw Hsb	Pype topic to search 60	ababa
🕞 Hore 🥰 Carrige star	Roma 🔜 Sove 🔇 Rohesh 🔇 Boxk 🔘 Forward 💡 Heb		CISCO
Device List d ¹ P ×	Configuration > Device Hanagement > Longing > \$2072		
Add Deter Correct Find Go	Configure the remote SHIP server IP address for sending enall alerts and notifications in response to select events. Remote SHIP Server Primary Server IP Address: (22.2.1.10) Secondary Server IP Address: (Optional)		
Device Management of 9 Spoot Anapycourse High Anable bit y and Sodabilt Looping Sodabilt Course Looping Setup Sodabilt	Áçdiy Reset		
Configuration changes saved successfully.	dista 15	📓 🎜 🔝 👔 🖓	27UMA 50/6#/01 #/5/R

5. Si desea enviar registros del sistema como capturas SNMP, primero debe definir un servidor SNMP. Elija SNMP en el menú Management Access para especificar la dirección de las estaciones de administración SNMP y sus propiedades específicas.

Cisco ASDM 7.3 for ASA - 10.306.44	144		-					- 0 -X
File View Tools Waards Winds	ow Help					Тури	topic to search	🔍 սիսիս
🕤 Hore 🖧 Configuration 🔀 Mor	itoing 🔄 Sove 🔇 Ratio	ih 🚺 Bask 🔘 F	Forward 🦿 Help					CISCO
Device List d1 4 ×	Configuration > Device Me	magement > Mana	operated Access > 52502					0
Add Deleta & Connect Find So 10.2.6.2 10.2.6.4 10.0.6.4.146 10.0.44.170 Connect To 100.44.146 Connect Connec	Configure SMMP parameters Community String (default) Contant: ASA Location Listening Port: SMMP Heat Access List	and nonogenent stat eneme admin office 360 IP Address	tons. (optional) Configure Traps Comunity String	9##Piersion	Username (2009 v.3 Orije)	Pol(Trap	UCPPort	Add Talk Delate
Phragement Access Rule	SMPv3 Isses Configure SMPv3 users. Sp Group Name	edfy extheritation a Username	nd privacy options for users according to Encrypted Password	othe group to which they belong. Authenticetors	Decyption	Ngoetten	AES Same	401
Prevail See See See See See See See See See								Dditta
:				Apply Res	et lism	hs IW		Ribonana tuta oo amuto

6. Elija Add para agregar una estación de administración SNMP. Ingrese los detalles del host SNMP y haga clic en Aceptar.

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

7. Para permitir que los registros se envíen a cualquiera de los destinos mencionados anteriormente, elija Logging Filters en la sección logging. Esto le presenta cada posible destino de registro y el nivel actual de registros que se envían a esos destinos. Elija el destino de registro que desee y haga clic en Editar. En este ejemplo, se modifica el destino 'Servidores Syslog'.

Cisco ASDM 7.1 for ASA - 10.306.44	144					
File View Tools Winds Winds	w Help				Type topic to search 6	հ տիտիս
🕞 Hone 🖓 Configuration [Mon	Rong 🔚 Sove 🔇 Refresh 🔇 Bad	s. 🕐 Forward 💡 Help				CISCO
Device List d1 9 ×	Configuration > Device Management	> Logging > Logging Filters				0
🗣 Add 🃋 Delete 🖋 Connect	Configure system filters for logging destina	etions.				
Find Go						
10.2.6.2 ·	Logging Destination	Syslogs From All Event: Classes		Syslogs From Specific Event Classes		Eak
- 5 30.106.44.146	SNMP Trap	- Disabled				
10.106.44.178	Internal Buffer	Dinabled				
Device Management d +	E-Piol	- Osated				_
- Management Sension Que +	Taket and CSI Sections	Deather				-
17 Sterer	ASDM	- Disibility				
2 St Linesing	Systop Servers	- Disabled				
🖶 😹 System Image/Configuration						
🗄 🙀 High Availability and Scalabilit						
D Loging						
S E-Mail Setup						
- Event Lata						
Logang Filtere						
Rate Lint						
Sylling Safryaria						
4 10 9						
💦 Device Setup						
🕄 Frend						
Remote Access VPN						
🚰 Statu-Statist						
🚖 Irend Micro Content Security						
Device Management						_
:			Apply Reset.			
				disto 15	🐺 🎜 🔰 🙆 t	0,0806 7122:20 AMUTC

8. Elija una gravedad adecuada, en este caso Informativa, en la lista desplegable Filtrar por gravedad. Haga clic en Aceptar cuando haya terminado.

Edit Logging Filters			×
Configure logging filter settings. The severity level represents t generate system log messages with severity levels up to the sp	he maximum level fo ecified level.	r logging messages.	The ASA will
Logging Destination: Syslog Servers			
Syslogs from All Event Classes			
O Use event list			
Disable logging from all event classes			
Syslogs from Specific Event Classes			
E	vent Class	Severity	
Event Class: auth			
Description: User Authentication			
Severity: Emergencies 👻			
OK Cance	Help		

9. Haga clic en Apply después de volver a la ventana Logging Filters.

Cisco ASDM 7.1 for ASA - 10.306.44	164					- 0 - X -
File View Tools Waards Winds	w Help				Pype topic to search Go	alada
🕞 Hone 🦓 Cartigution 🔯 Man	Roring 🔚 Sove 🔇 Refresh 🔇 Back	🕐 Forward 💡 Help				CISCO
Device List d ¹ P ×	Configuration > Device Management >	Logaing > Logaing filters				
🗢 Add 📋 Delete 🖉 Connect	Configure system filters for logging destination	05				
Find Go						
10.2.6.2 ·	Logging Destination	Syslogs From All Event: Classes		Syslogs From Specific Event Classes		Eak
- 3 10.106.44.146	SNMP Trap	- Disabled				
10.106.44.178	Internal Buffer	Disabled				
Device Management dn +	E-Mol	- Osatsed				
- Management Sension Que +	Televit and CSai Sections	Celebert				
T Steven and Array Date	ASDM	- Disabled				
10 10 Lioming	Syslog Servers	Severity: Informational				
🐵 🐉 System Inage/Configuration						
E 👷 High Availability and Scalabilit						
- R Logging Setup						
-St-HallSetup						
- Dvent Lata						
- the copping filters						
Synlog Servers						
El Tarles Sales						
Revice Setup						
E. rrend						
Remarke Access WPW						
🚰 Statu-Statin						
🚖 Irend Micro Content Security						
Device Management						
:			Apply Reset			
				disto 15	🕼 🎉 🔰 👔 10,0	806 7129 30 AMUTC

Enviar mensajes Syslog a través de una VPN a un servidor Syslog

En el diseño VPN simple de sitio a sitio o en el diseño más complicado de hub y spoke, el administrador podría querer monitorear todos los firewalls ASA remotos con el servidor SNMP y el servidor syslog ubicados en un sitio central.

Para configurar la configuración de VPN IPsec de sitio a sitio, consulte <u>Ejemplo de Configuración</u> <u>de Túnel PIX a PIX VPN PIX/ASA 7.x y superior</u>. Aparte de la configuración VPN, debe configurar el SNMP y el tráfico interesante para el servidor syslog en el sitio central y local.



Configuración de 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 ***** Configuración de 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 <u>Monitoreo de Cisco Secure ASA Firewall Usando SNMP y Syslog a través del Túnel</u> <u>VPN</u> para obtener más información sobre cómo configurar ASA Versión 8.4

Syslog avanzado

La versión 8.4 de ASA proporciona varios mecanismos que le permiten configurar y administrar los mensajes de syslog en grupos. Estos mecanismos incluyen el nivel de gravedad del mensaje, la clase de mensaje, el ID de mensaje o una lista de mensajes personalizada que cree. Con el uso de estos mecanismos, puede escribir un solo comando que se aplique a grupos pequeños o grandes de mensajes. Cuando configura syslogs de esta manera, puede capturar los mensajes del grupo de mensajes especificado y ya no todos los mensajes de la misma gravedad.

Utilizar la lista de mensajes

Utilice la lista de mensajes para incluir solamente los mensajes syslog interesados por nivel de gravedad e ID en un grupo, luego asocie esta lista de mensajes con el destino deseado.

Complete estos pasos para configurar una lista de mensajes:

- Ingrese la lista de registro message_list | level severity_level [class message_class] para crear una lista de mensajes que incluya mensajes con un nivel de gravedad o una lista de mensajes especificados.
- 2. Ingrese el comando logging list message_list message syslog_id-syslog_id2 para agregar mensajes adicionales a la lista de mensajes recién creada.
- 3. Ingrese el comando logging destination message_list para especificar el destino de la lista de mensajes creada.

Ejemplo 2

Ingrese estos comandos para crear una lista de mensajes, que incluya todos los mensajes de gravedad 2 (críticos) con la adición del mensaje 611101 a 611323, y también para que se envíen

a la consola:

<#root>

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

Configuración de ASDM

Este procedimiento muestra una configuración ASDM para el Ejemplo 2 con el uso de la lista de mensajes.

1. Elija Listas de Eventos bajo Registro y haga clic en Agregar para crear una lista de mensajes.



2. Introduzca el nombre de la lista de mensajes en el cuadro Nombre. En este caso se utiliza my_critical_messages. Haga clic en Agregar bajo Filtros de Clase de Evento/Gravedad.

ent Class Severity Add Message IDs		Message ID Filters ——		ity Filters	nt Class/Severi
Edit	Add	Message IDs	Add	Severity	Event Class
	Edit		Edit		
Delete	Delete		Delete		

3. Elija All en la lista desplegable Event Class. Elija Crítico en la lista desplegable Gravedad. Haga clic en Aceptar cuando haya terminado.

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

4. Haga clic en Agregar bajo los Filtros de ID de mensaje si se requieren mensajes adicionales. En este caso, debe introducir mensajes con ID 611101-611323.

E	Add Event List				X
Na	ame: my_critical_	messages			
Sp re to Fv	ecify filters for th presents the max the specified leve rent Class/Severit	ne event list. You imum level for lo el. v Filters	ı can filter syslogs by gging messages. The	their class and severity, or by th ASA will filter system log messag Message ID Filters	neir IDs. The severity level ges with severity levels up
	Event Class	Severity	Add	Message IDs	Add
	All	Critical	Edit		Edit
			Delete		Delete
			OK Ca	ncel Help	

5. Coloque el rango de ID en el cuadro ID de mensaje y haga clic en Aceptar.

The state of the s
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. Vuelva al menú Logging Filters y elija Console como destino.
- 7. Elija my_critical_messages en la lista desplegable Use event list. Haga clic en Aceptar cuando haya terminado.

🔄 Edit Logging Filters	the local			×			
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							
Silter on severity Informational	Filter on severity Informational						
Use event list <u>my_critical_me</u>	O Use event list my_critical_messages → New						
Disable logging from all event class	ses						
Syslogs from Specific Event Classes —							
		Event Class	Severity				
Event Class: auth	Add >>						
Severity:	Delete						
Sevency.							
OK Cancel Help							

8. Haga clic en Apply después de volver a la ventana Logging Filters.

Cisco ASDM 7.1 for ASA - 10.106.44.1	144 - Transmitting Transmitting	Radio Talla				- 0 - X
File View Tools Waards Window	w Help				Pype topic to search	60
🕤 Hore 🖓 Configuration 🔀 Mone	toring 🔚 Sover 🔇 Rehesh 🔇 Ba	ask 🔘 Forward 💡 Help				cisco
Device List d1 0 ×	Configuration > Device Management	Lo Longing > Longing Filters				0
🗣 Add 📋 Delete 🖋 Correct	Configure systog filters for logging destin	nations.				
Find Gi						
5 10.2.6.2	Logging	Syslogs From		Syslogs From		Edit
10.105.44.144	Destination	All Event Classes		Specific Event Classes		
- 5 30.106.44.146	SNMP Trap	- Disabled				
10.108.44.078 ···	Internal Buffer	Disabled				
Device Management (P + P	E-Mol	- Cisased				
- Ranagement Sension Qut +	Conscie	- Deabled				
- <u>2,4</u> 59247	Telnet and SSH Sessions	- Ceased				
Management Access Rule	ASDM	Deathed				
E ad Libersing	System Servers	Eventus: re_pica_re	soyes			
The system stage, configuration						
D Loning						
- Dagging Setup						
St-Phul Setup						
Logging Filters						
Rate Link						
Synlog Servers						
4 10 9						
Device Setup						
🛃 Frend						
Remote Access WW						
Contraction State UPN						
A Trand Mark Contract Contracts						
These bible carderic Sectarch						
Centre Management						
·			Apply Reset			
-						
Configuration changes saved successfully.				0500 15	💷 🖉 📶 👘 🖉	10/28/06 9:19:10 AMUTC

Esto completa las configuraciones de ASDM con el uso de una lista de mensajes como se muestra en el Ejemplo 2.

Utilizar la clase de mensaje

Utilice la clase de mensaje para enviar todos los mensajes asociados con una clase a la ubicación de salida especificada. Cuando especifica un umbral de nivel de gravedad, puede limitar el número de mensajes enviados a la ubicación de salida.

```
<#root>
logging class
message_class destination | severity_level
```

Ejemplo 3

Ingrese este comando para enviar todos los mensajes de clase ca con un nivel de gravedad de emergencias o superior a la consola.

<#root>

```
logging class ca console emergencies
```

Configuración de ASDM

Este procedimiento muestra las configuraciones ASDM para el ejemplo 3 con el uso de la lista de mensajes.

- 1. Elija el menú Logging Filters y elija Console como el destino.
- 2. Haga clic en Deshabilitar el registro de todas las clases de eventos.
- 3. En Syslogs de Specific Event Classes, elija la clase de evento y la gravedad que desea agregar.

Este procedimiento utiliza ca y Emergencias, respectivamente.

4. Haga clic en Agregar para agregar esto a la clase de mensaje y haga clic en Aceptar.

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: Console							
Syslogs from All Event Cl	lasses						
Filter on severity	Filter on severity Emergencies						
🔘 Use event list	─ 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 Ce	ertificate Add >>						
Severity: Emerg	gencies 👻						
OK Cancel Help							

5. Haga clic en Apply después de volver a la ventana Logging Filters. La consola ahora recopila el mensaje de clase ca con emergencias de nivel de gravedad como se muestra en la ventana Filtros de registro.

Cisco ASDM 7.3 for ASA - 10.306.44	144				- 0 - X -
File View Tools Wgards Winds	w Help			Pype topic to search	60 also de
🕤 Hone 🖓 Cantaguation 🛐 Mon	Roring 🔄 Sove 🔇 Refresh 🔇 Back (Differward 🦻 🚧			CISCO
Device List d ^p P ×	Configuration > Device Management > L	outing > Logging Filters			
Add Delete Connect. Find	Configure syslog filters for logging destination	15.			
	Logging Destination	Systops From All Event: Classes	Syslags Fran Specific Event Classes		t a
5 10.106.44.146 5 10.106.44.175	SMMP Trop Internal Buffer	O64595 Deabled			
Device Management d1 9	E-Mol	- Oisabled			
Printigement Semicon Co. Single Printigement Access Rule Printigement Access Rule	Tehet and S0H Sessions Attorn Syslog Servers	Disdied Disdied - Event List: Ing_pitical_messages			
Benche Access VPV Benche Access VPV Benche Ster UPN A Front More Cantent Security Device Screenert		Acoty	Reset		
Configuration changes saved successfully.			0500 15	💷 🔐 🔝	10,038/06 9127 50 AMUTC

Esto completa la configuración de ASDM para el ejemplo 3. Consulte <u>Mensajes Enumerados por</u> <u>Nivel de Gravedad</u> para obtener una lista de los niveles de gravedad de los mensajes de registro. Enviar mensajes de registro de depuración a un servidor Syslog

Para la resolución avanzada de problemas, se requieren registros de depuración específicos de funciones/protocolos. De forma predeterminada, estos mensajes de registro se muestran en el terminal (SSH/Telnet). Dependiendo del tipo de depuración y de la velocidad de mensajes de depuración generados, el uso de la CLI puede resultar difícil si se habilitan las depuraciones. Opcionalmente, los mensajes de depuración se pueden redirigir al proceso syslog y generarse como syslogs. Estos registros del sistema se pueden enviar a cualquier destino de registro del sistema como lo haría cualquier otro registro del sistema. Para desviar los debugs a syslogs, ingrese el comando logging debug-trace. Esta configuración envía la salida de depuración, como syslogs, a un servidor syslog.

logging trap debugging logging debug-trace logging host inside 172.22.1.5

Uso conjunto de listas de registro y clases de mensajes

Ingrese el comando logging list para capturar el syslog para los mensajes VPN IPsec de LAN a LAN y de acceso remoto solamente. Este ejemplo captura todos los mensajes de registro del sistema de clase VPN (IKE e IPsec) con nivel de depuración o superior.

Ejemplo:

<#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

Registro de Aciertos de ACL

Agregue log a cada elemento de la lista de acceso (ACE) que desee para registrar cuando se llegue a una lista de acceso. Utilice esta sintaxis:

<#root>

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

Ejemplo:

<#root>

ASAfirewall(config)#

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

Las ACL, de forma predeterminada, registran cada paquete denegado. No es necesario agregar la opción de registro para denegar ACL para generar registros del sistema para paquetes denegados. Cuando se especifica la opción log, genera el mensaje syslog 106100 para la ACE a la que se aplica. El mensaje de registro del sistema 106100 se genera para cada flujo ACE de permiso o denegación coincidente que pasa a través del firewall ASA. El flujo de la primera coincidencia se almacena en caché. Las coincidencias subsiguientes incrementan el conteo de aciertos que se muestra en el comando show access-list. El comportamiento predeterminado del registro de la lista de acceso, que es la palabra clave log no especificada, es que si se niega un paquete, se genera el mensaje 106023 y, si se permite un paquete, no se genera ningún mensaje syslog.

Se puede especificar un nivel de syslog opcional (0 - 7) para los mensajes de syslog generados (106100). Si no se especifica ningún nivel, el nivel predeterminado es 6 (informativo) para una nueva ACE. Si la ACE ya existe, su nivel de registro actual permanece sin cambios. Si se especifica la opción log disable, el registro de la lista de acceso está completamente inhabilitado. No se genera ningún mensaje de registro del sistema, que incluye el mensaje 106023. La opción log default restaura el comportamiento de registro predeterminado de la lista de acceso.

Complete estos pasos para habilitar el mensaje syslog 106100 para verlo en el resultado de la consola:

- Ingrese el comando logging enable para habilitar la transmisión de mensajes del registro del sistema a todas las ubicaciones de salida. Debe establecer una ubicación de salida de registro para ver los registros.
- 2. Ingrese el comando logging message <message_number> level <severity_level> para establecer el nivel de gravedad de un mensaje de registro del sistema específico.

En este caso, ingrese el comando logging message 106100 para habilitar el mensaje 106100.

- Ingrese la lista de mensajes de la consola de registro | severity_level para permitir que los mensajes del registro del sistema se muestren en la consola del dispositivo de seguridad (tty) a medida que ocurran. Establezca severity_level de 1 a 7 o utilice el nombre del nivel. También puede especificar qué mensajes se envían con la variable message_list.
- 4. Ingrese el comando show logging message para mostrar una lista de mensajes de registro del sistema que se han modificado desde la configuración predeterminada, que son mensajes a los que se les ha asignado un nivel de gravedad diferente y mensajes que se han inhabilitado.

Este es un ejemplo de salida del 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
```

Bloqueo de la generación de syslog en un ASA en espera

Comience desde la versión 9.4.1 del software ASA en adelante y puede bloquear los registros del sistema específicos para que no se generen en una unidad en espera y utilice este comando:

no logging message syslog-id standby

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Si desea suprimir un mensaje syslog específico para enviarlo al servidor syslog, debe ingresar el comando como se muestra.

<#root>

hostname(config)#

<syslog_id>

Consulte el comando logging message para obtener más información.

%ASA-3-201008: no permitir nuevas conexiones

El mensaje de error %ASA-3-201008: No se permiten nuevas conexiones. Se ve cuando un ASA no puede comunicarse con el servidor syslog y no se permiten nuevas conexiones.

Solución

Este mensaje aparece cuando ha activado la mensajería de registro del sistema TCP y no se puede acceder al servidor syslog, o cuando utiliza Cisco ASA Syslog Server (PFSS) y el disco del sistema Windows NT está lleno. Complete estos pasos para resolver este mensaje de error:

- Desactive la mensajería de registro del sistema TCP si está activada.
- Si utiliza PFSS, libere espacio en el sistema Windows NT en el que reside PFSS.
- Asegúrese de que el servidor syslog esté activo y de que pueda hacer ping al host desde la consola de Cisco ASA.
- Reinicie el registro de mensajes del sistema TCP para permitir el tráfico.

Si el servidor syslog se desactiva y se configura el registro TCP, utilice el comando <u>logging</u> <u>permit-hostdown</u> o cambie al registro UDP.

Cisco ASDM 7.1 for ASA - 10.106.44	166						0 0
File View Tools Waards Winds	aw Help Roma 🕞 Sove 📿 Per	esh 🔿 Back 🕥 Forward 🧳 Help			Type topic to search	60	cisco
Device List d ¹ P ×	Configuration > Device?	Sanagement > Logging > Syslog Servers					
Device link 02 9 × Add Delete Correct Find 6 S 10.2.6.2 S 10.2.6.4.146 S 10.2.6.4.146 Device Management 01 # Period Management 01 # Device Management 01 #	Configuration > Device 1 Specify up to 16 syslopse Interface reste	Innovement > Locating > Soulog Servera invers. Hole sure logging is enabled in Configura IP Address 172.22115	tion > Device Management > Logging > Logging 5 Protocol/Port UC4/514	PHBLEM PHBLEM No	Secure No		Add Lot Delete
Center Setup C	Specify the number of me	mages that are also verifies be quested often a sy	ving server is bury. Use D to induste universel-up	ese áre.			
Device Management	Quaran Stor: 312	en when TCP systing earser is down	Apply Re	set			
Configuration changes saved successfully.				Cisto .	15 🔯 🌌 🚮	🙆 Q2	01UMA 50.64101 F39

Información Relacionada

- Referencias de Comandos de Cisco Secure PIX Firewall
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).