ASA 8.2: Syslog de la configuración usando el ASDM

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados **Convenciones** Configuración de syslog básica usando el ASDM Registro del permiso Registro de la neutralización Registro a un email Registro a un servidor de Syslog Configuración de syslog avanzada usando el ASDM Trabajo con las Listas de eventos Trabajo con los filtros del registro Límite de velocidad Registración de los golpes de una regla de acceso Configurar Configuraciones Verificación Troubleshooting Problema: Conexión perdida -- Conexión del Syslog terminada --Solución No puede ver el tiempo real abre una sesión el ASDM de Cisco Solución Información Relacionada

Introducción

Este documento proporciona la información sobre cómo configurar el Syslog en el dispositivo de seguridad adaptante de Cisco (ASA) 8.x usando el Administrador de dispositivos de seguridad adaptante (ASDM) GUI. Los mensajes del registro del sistema son los mensajes generados por Cisco ASA para notificar al administrador en cualquier cambio en la configuración, los cambios en configuración de la red, o los cambios en el funcionamiento del dispositivo. Analizando los mensajes del registro del sistema, un administrador puede resolver problemas fácilmente el error realizando una Análisis de la causa de raíz.

Los mensajes de Syslog principalmente se distinguen basados en su nivel de gravedad.

- 1. Gravedad 0 Mensajes de emergencia El recurso está inutilizable
- 2. Gravedad 1 Mensajes de alerta La acción inmediata es necesaria
- 3. Gravedad 2 Mensajes críticos Condiciones críticas
- 4. Gravedad 3 Mensajes de error Condiciones de error
- 5. Gravedad 4 Mensajes de advertencia Condiciones de advertencia
- 6. Gravedad 5 Mensajes de notificación Normal pero estados significativos
- 7. Gravedad 6 Mensajes de información Mensajes de información solamente
- 8. Gravedad 7 Mensajes de debugging Mensajes de debugging solamente**Nota:** El nivel de gravedad más alto es una emergencia y el nivel de gravedad más bajo está haciendo el debug de.

Los mensajes de Syslog de la muestra generados por Cisco ASA se muestran aquí:

- %ASA-6-106012: Niegue el IP de IP_address a IP_address, maleficio de las opciones IP.
- %ASA-3-211001: Error de asignación de memoria
- %ASA-5-335003: ACL predeterminado del NAC aplicado, ACL: ACL-nombre host address

El valor numérico X especificado en "%ASA-X-YYYYYY: ", denota la gravedad del mensaje. Por ejemplo, el "%ASA-6-106012" es un mensaje de información y el "%ASA-5-335003" es un mensaje de error.

prerrequisitos

Requisitos

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.

- Versión de ASA 8.2 de Cisco
- Cisco ASDM versión 6.2

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones sobre documentos.

Configuración de syslog básica usando el ASDM

Registro del permiso

Complete estos pasos:

1. Elija la *configuración > la Administración de dispositivos > el registro > el registro puesto* y la marca de tilde la *opción de registro del*

pe	rmiso.	
凾 (lisco ASDM 6.2 for ASA - 10.78.177.11	
File	View Tools Wizards Window Help	
G	Home 🍪 Configuration 🔗 Monitoring	I 🔜 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help
	Device Management 🗗 🖗 🗡	Configuration > Device Management > Logging > Logging Setup
Device Ust	Management Access Licensing System Image/Configuration Logging Logging Event Lists Rate Limit Syslog Servers Syslog Servers	Enable logging Enable logging on the failover standby unit Send debug messages as syslogs Send syslogs in EMBLEM format Logging to Internal Buffer Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten. Buffer Size: 4096 bytes You can choose to save the buffer contents before the buffer is overwritten. Save Buffer To: FTP Server Configure FTP Settings F Flash Configure Flash Usage ASDM Logging Specify the size of the queue for syslogs intended for viewing in ASDM. Queue Size:

2. Usted puede registrar los mensajes de Syslog a un búfer interno especificando el tamaño de almacén intermedio. Usted puede también elegir salvar el contenido del buffer a memoria flash haciendo clic el *uso de destello de la configuración* y definiendo las configuraciones de

	Configuration > Device Manageme	nt > Logging > Logging Setup
	🖾 Enable logging	T Enable logging on the failover standby unit
	F Send debug messages as syslogs	☐ Send syslogs in EMBLEM format
	Logging to Internal Buffer Specify the size of the internal buff	er to which syslogs will be saved. When the buffer fills up, it will be overwritten.
	Buffer Size: (1096) You can choose to save the buffer	bytes contents before the buffer is overwritten.
	Save Buffer To: 🔲 FTP Server	Configure FTP Settings
	(Flash	Configure Flash Usage
	ASDM Logging	
	Specify the size of the queue for sy Queue Size: 100	ginos Intended for Viewon in ASDM. gin Configure Logging Flash Usage
		Specify the maximum space that logging can use on the flash.
		Maximum Flash to Be Used by Logging: 1024 KB
		Specify the minimum free space that logging will preserve on the flash.
		Minimum Free Space to Be Preserved: 3076 KB
destello.		

3. Los mensajes de registro guardado en memoria intermedia se pueden enviar a un servidor FTP antes de que estén sobregrabados. Haga clic las *configuraciones de la configuración FTP* y especifique a los detalles del servidor FTP como se muestra

Configuration > Device Management	nt > Logging > Logging Setup
🔽 Enable logging	Enable logging on the failover standby unit
F Send debug messages as syslogs	Send syslogs in EMBLEM Format
Logging to Internal Buffer	
Specify the size of the internal buffe	er to which syslogs will be saved. When the buffer fills up, it will be overwritten
Buffer Size: 4096	bytes
Filesh	Configure Flash Usage
Specify the size of the queue for sy	Configure FTP Settings
Quede Size: 1100	P Enable FTP clienc
	Server IP Address: 172,16,18,10
	Path:
	Username: testuser
	Password: ******
	Confirm Password: ++++++
	OK Cancel Help

Inhabilite el registro

Usted puede inhabilitar los ID de syslogs específicos basados en su requisito.

Nota: Seleccionando la marca de tilde para el *grupo fecha/hora del incluido en la* opción de los *Syslog*, usted puede agregar la fecha y hora que fueron generados como campo a los Syslog.

1. Seleccione los Syslog para inhabilitar y el tecleo

edita.			
Syslog Format Facility Code to Indude in Syslogs: COCAL4(20)			
F Include timestamp in syslops			
Syslog ID Setup			
Show: All syslog IDs	*		
Systeg ID	Logging Level	Disabled	Edit
218001	Critical	No	
218002	Critical	No	Restore Defaults
218003	Critical	No	
218004	Critical	No.	
219002	Errors	No	
302003	Informational	No	
302004	Informational	No	-
302009	Informational	No.	
302010	Informational	No .	
302012	Informational	No	
302013	Informational	No	
302014	Informational	Réo .	
302015	Informational	No	
302016	Informational	No	
302017	Informational	No	
302018	Informational	No	

2. *De la ventana de configuración del ID de syslog del editar*, marca de tilde la *AUTORIZACIÓN de la* opción y del tecleo de los *mensajes de la*

	302015, 302016	
yslog IDs:		
✓ Disable m	essages	
· Produce in		

neutralización.

3. Los Syslog discapacitados se pueden ver en una lengueta separada seleccionando los *ID de syslogs inhabilitados del* menú desplegable de la *configuración del ID de*

syslog.			
Configuration > Device Management > Logging > Syslog Setup			
Syslog Format			
Facility Code to Include in Syslogs: LOCAL4(20)			
☑ Include timestamp in syslogs			
Suba Di Cala			
Sysing to setup			
show. Described system into			
Syslog ID	Logging Level	Disabled	5
302015	Informational	Yes	and the second se
302016	Informational	Yes	Restore
302016	unrormational	Tes	

Registro a un email

Complete estos pasos usando el ASDM para enviar los Syslog a un email:

 Elija la configuración > la Administración de dispositivos > la configuración del registro > del email. El campo de la dirección de correo electrónico de la fuente es útil en la asignación de un email ID como la fuente para los Syslog. Especifique la dirección de correo electrónico de la fuente. Ahora, el tecleo agrega para agregar a los beneficiarios del email

Configuration > Device Management > Logging > E-Mail Setup		
Enter the e-mail address that will be used as the source address when syslogs are sent as e-mails.		
Source E-Mail Address:] [test123@example.com		
E-Mail Recipients		
Destination E-Mail Address	Syslog Severity	Add
		Ldr.
		Deterio

 Especifique la dirección de correo electrónico del destino y elija el nivel de gravedad. De acuerdo con los niveles de gravedad, usted puede definir a diversos beneficiarios del email. El Haga Click en OK a volver de nuevo al *email puso el*

Destination E-Mail Addre	ess: monitorsyslog@example.com	
Filter the syslogs sent to severity filter used for to severity selected below recipients in Configuration Filters.	o this recipient by severity. The syslog his recipient will be the higher of the and the global filter set for all e-mail on>Properties>Logging>Logging	
Syslog Severity:	Errors	
ОК	Alerts	
	Errors	
	Warnings	
	Warnings Notifications	

configuración:

nfiguration > Device Management > Logging > E-Mail Setup	
Enter the e-mail address that will be used as the source address when syslogs are sent as e-mails.	
Source Fulfail Addresses Teact 123/Revisionle com	
Hall Darbiante	
Mal Recipients	

3. Elija la *configuración > la configuración > el registro > el S TP de dispositivo* y especifique al servidor

SMTP. Configuration > Device Management > Log	Iging > SMTP
Configure the remote SMTP server IP address I	for sending email alerts and notifications in response to select events.
Remote SMTP Server	
Primary Server IP Address: 172.18.10.2	0
Secondary Server IP Address:	(Optional)
Secondary Server IF Hadress, 1	(optional)

Registro a un servidor de Syslog

Usted puede enviar todos los mensajes de Syslog a un servidor de Syslog dedicado. Realice estos pasos usando el ASDM:

 Elija la configuración > la Administración de dispositivos > el registro > a los servidores de Syslog y el tecleo agrega para agregar a un servidor de Syslog.

onfigurs	ation > Device Managemen	t > Logging > Syslog Servers				
specify	up to 16 syslog servers. Make :	sure logging is enabled in Configuration	> Device Management > Lopping > Lopping	j Setup.		
	Interface	IP Address	Protocol/Port	EMBLEM	Secure	Add
						Edit
						Oelits
						- Conterna

La ventana del servidor de Syslog del agregar aparece.

2. Especifique la interfaz que el servidor está asociado junto con a la dirección IP. Especifique el *protocolo* y a los *portes detailes* dependiendo de su configuración de la red. Entonces, *AUTORIZACIÓN del* tecleo.**Nota:** Aseegurese que usted tiene accesibilidad al servidor de

Address:	172.16.11.1	
otocol:	Стор	€ UDP
ort:	514	_
Log mes	sages in Cisco	EMBLEM format (UDP o

Syslog de Cisco ASA.

3. Ven al servidor de Syslog configurado como se muestra aquí. Las modificaciones se pueden hacer cuando usted selecciona este servidor, después hacen clic *editan*

172.16.11.100	UDP/514	No	No

Nota: Marca de tilde el *tráfico de usuarios de la permit a pasar cuando el servidor de Syslog TCP está abajo de* opción. Si no, las sesiones de usuario nuevo se niegan con el ASA. Esto es aplicable solamente cuando el Transport Protocol entre el ASA y el servidor de Syslog es TCP. Por abandono, las nuevas sesiones del acceso a la red son negadas por Cisco ASA cuando un servidor de Syslog está abajo por cualquier motivo.Para definir el tipo de mensajes de Syslog que deban ser enviados al servidor de Syslog, vea la sección del <u>filtro del registro</u>.

Configuración de syslog avanzada usando el ASDM

Trabajo con las Listas de eventos

Las Listas de eventos nos permiten para crear las listas personalizadas que contienen el grupo de mensajes de Syslog que deban ser enviados a un destino. Las Listas de eventos se pueden crear en tres maneras diferentes:

- ID del mensaje o rango de los ID del mensaje
- Gravedad del mensaje
- Clase de mensaje

ID del mensaje o rango de los ID del mensaje

Siga estos pasos:

1. Elija la *configuración > la Administración de dispositivos > el registro > las Listas de eventos* y el tecleo *agrega* para crear una lista del nuevo

Configuration > Device Management >	Logging > Event Lists						
Use event lists to define a particular set of	syslogs that you are interested in. The event list can be used to filter syslogs sent t	o a logging destination.					
Name	Event Class / Severity	Message IDs	Add I				
			Contraction in the local division of the loc				
			Edit				

2. Especifique un nombre en el *campo de nombre*. El tecleo *agrega* en el cristal de los *filtros del ID del mensaje* para crear una lista del nuevo evento

	T INCOLO	Fa 10	Message ID Filters	3.9
Event Class	Severity	Add	Message IDs	Add
		Edt		Edit
		Delete		Delete

 Especifique el rango del mensaje de Syslog ID. Aquí los mensajes de Syslog TCP han tomado por ejemplo. Haga Click en OK a completar.

acify filters for the ev resents the maximum the specified level.	ent list. You can filter syslogs by their class and severity, or by their IDs. level for logging messages. The ASA will filter system log messages with	The severity levels used to be a severity lev
ant Class/Severity Fil	Set the order records ID like human to credit a second	
Event Class	of syslog IDs, for example, 101001-101010.	Add
	Message IDs: 302013-302018	Edit
		Delete

4. Haga Click en OK otra vez para invertir de nuevo a la ventana de las *Listas de eventos*.

anfiguration > Device Management > Logging > Ever	nt Lists	
Use event lists to define a particular set of syslogs that you	are interested in. The event list can be used to filter syslo	gs sent to a logging destination.
None	Event Class / Severity	Message IDs

Gravedad del mensaje

1. Las Listas de eventos se pueden también definir sobre la base de la gravedad del mensaje. El tecleo *agrega* para crear una Lista de eventos

iouration > Device Management > Logging > Ev	ont Lists		
e event lists to define a particular set of sysiogs that yo	are interested in. The event list can be used to filter syslogs sent to	a logging destination.	
Nate	Event Class / Severity	Message IDs	Add
p-com-syslog		302013-302018	
			Edit

2. Especifique el nombre y el haga click en

Event Class Severity Add	Message IDs Add
Edt	Edt
Dolete	Delete
1	
1	
ok	Cancel Help
	de Add Class and Savarity Filter
	ge Add class and Sevency Filter
	Event Class: All
	Description All Europh Classon
	Description. Mil Event Classes
	Severity: Errors
	Severity: Errors Emergencies
	Severity: Errors Emergencies OK Alerts

- 3. Seleccione el nivel de gravedad como errores.
- 4. Haga clic en

epresents the max to the specified leve Event Class/Severit	imum level for log sl. y Filters	iging messages. The ASA	A will filter system log messages wi Message ID Filters	ith severity le
Event Class	Severity	Add	Message IDs	Add
All	Errors	Edit		Edit
		Delete		Deret

Clase de mensaje

Las Listas de eventos también se configuran sobre la base de la clase de mensaje. Una clase de

mensaje es un grupo de mensajes de Syslog relacionados con una característica del dispositivo de seguridad que le permita para especificar una clase entera de mensajes en vez de especificar una clase para cada mensaje individualmente. Por ejemplo, utilice la clase del auth para seleccionar todos los mensajes de Syslog que se relacionen con la autenticación de usuario. Algunas clases de mensajes disponibles se muestran aquí:

- Todos Todas las clases de evento
- auth Autenticación de usuario
- Bridge Firewall transparente
- Ca Autoridades de certificación PKI
- interfaz del comando config
- ha Conmutación por falla
- IPS Servicio de protección contra intrusos
- IP Pila IP
- NP Procesador de red
- OSPF OSPF Routing
- RIP El rutear del RIP
- sesión de usuario de sesión

Realice estos pasos para crear una clase de evento basada en la clase de mensaje de los vpnclient-*errores*. La clase de mensaje, *vpnc*, está disponible categorizar todos los mensajes de Syslog relacionados con el vpnclient. El nivel de gravedad para esta clase de mensaje se elige como "errores".

1. El tecleo agrega para crear una lista del nuevo

iguration > Device Management > Log	aina > Event Lists		
se event lists to define a particular set of sysk	ogs that you are interested in. The event list can be used to filter syslogs sent to	e logging destination.	
Name	Event Class / Seventy	Message IDs	66A
cp-conn-syslog		302013-302018	
yslog-sev-error	All / Errors	R	Edit

2. Especifique el nombre para ser relevante a la clase de mensaje que usted crea y haga click

repr to t	resents the maxim he specified level	num level for log	ging messages. The /	ASA will filter system log messages w	ith severity
Eve	nt Class/Severity	Filters		Message ID Filters	
-	Event Class	Severky	Add	Message IDs	A
			Edt		Ec
			Delete		Del

3. Seleccione el vpnc de la lista

e specified leve t Class/Severity	l. / Filters	Add Class	and Severity Filter	×	
Event Class	Severi	Event Class:	·· All ··		Add
		Description:	ssi svc	-	Edit
		Sevency.	sys ym	22	Delete
		OK	vpdn		

desplegable.

4. Seleccione el nivel de gravedad como *errores*. Este nivel de gravedad es aplicable para esos mensajes que se registren para esta clase de mensaje solamente. Haga Click en OK a invertir de nuevo a la ventana de la Lista de eventos del

vent list.	Very ene filter		
	Tou can nicer	syslogs by their class and s	everity, o
in level f	or logging mes:	sages. The ASA will filter sy: and Sevenity Filter	stem log r 2
Severi	Event Class:	vpnc	*
20101	Description:	VPN Client	
	Severity:	Errors	*
		Emergencies	-
	ОК	Alerts	
12	_	Errors	
		Warnings Notifications Teformational	
	iters – Severi	iters - Severi Severi Description: Severity: OK	iters - Severi Severi Description: VPN Clent Severity: Errors Emergencies OK Alerts Critical Errors Warnings Notifications Informational

agregar.

5. La clase de evento/la gravedad se muestra aquí. Haga Click en OK a completar configurando la Lista de eventos de los "vpnclient-

resents the maxi	mum level for log	ging messages. The ASA	will filter system log messages wi	th severity levels up
he specified leve nt Class/Severity	d. v Filters ———		Message ID Filters	
Event Class	Severity	Add	Message IDs	Add
vpnc	Errors	Edit		Edit
		Delete		Deete
				1979 - 1979 A.

errores".

én se muestra en el tiro de siguiente pantalla que una lista del nuevo evento, el "usuarioauth-Syslog", se crea con una clase de mensaje como "auth" y el nivel de gravedad para los Syslog de esta clase de mensaje específica como "advertencias". Configurando esto, la Lista de eventos especifica todos los mensajes de Syslog que se relacionan con la clase de mensaje del "auth", con los niveles de gravedad **hasta el** nivel de las

"advertencias".**Nota:** Aquí, el término "hasta" está de significación. Al denotar el nivel de gravedad, tenga presente que todos los mensajes de Syslog serán registrados hasta que ese nivel.**Nota:** Una Lista de eventos puede contener las clases de eventos múltiples. La Lista de eventos de los "vpnclient-errores" es modificada haciendo clic **edita** y definiendo una clase de nuevo evento

"SSL/error".

infiguration > Device Management > Lo	iaina > Event Lists	
Use event lists to define a particular set of sys	logs that you are interested in. The event list can be used to filter sys	logs sent to a logging destination.
Name	Event Clare / Severity	Marcana IDr
Name	Event Class / Severky	Pressage tos
tcp-conn-syslog		302013-302018
syslog-sev-error.	All / Errors	
vpnclient-errors	vpnc / Errors	
user-auth-syslog	auth / Warnings	

Trabajo con los filtros del registro

Los filtros de registración se utilizan para enviar los mensajes de Syslog a un destino especificado. Estos mensajes de Syslog se pueden basar en la "gravedad" o "incluso enumera".

Éstos son los tipos de destinos a los cuales estos filtros sean aplicables:

- Búfer interno
- SNMP trap
- Correo electrónico
- Consola
- Sesiones telnets
- ASDM
- Servidores de Syslog

Siga estos pasos:

1. Elija la **configuración > la Administración de dispositivos > el registro > los filtros del registro** y seleccione el destino de registro. Entonces, el tecleo **edita** para modificar las

figuration > Device Management > Loggi	ng > Logging Filters		
Configure syslog filters for logging destinations.			
Logging Destination	Systeps From All Event Classes	Syslogs From Specific Event Classes	Edit
Internal Buffer	- Disabled		
SWMP Trap	Disabled		
e-real	Disabled		
Console	Disabled		
Teinet and SOH Sessions	Disabled		
ASDM	Disabled		
Curles Carbon	in Dicabled		

2. Usted puede enviar los mensajes de Syslog basados en la gravedad. Aquí, las **emergencias** se han seleccionado para mostrar como un ejemplo

ine and a parameters into	sages with seve	rity levels up to the	specified level.		
gging Destination: Int	ernal Buffer				
slogs from All Event Cl	asses Emergencies	+	5		
C Use event list	user-auth-sysl	ag 💌 New	2. 1		
C Disable logging fro	m all event class	es	_		
slogs from Specific Eve	int classes		Event Class	Severity	
Event Class: auth	÷	(
Description: User A	uthentication	Add >>			
	gencies 💌	Delete			
Severity: Emerg					

3. Una Lista de eventos se puede también seleccionar especificar qué tipo de mensaje debe ser enviado a un destino determinado. Haga clic en

generate system log me	ssages with sever	ity levels up to f	he specified level.		
Logging Destination: In	ernal Buffer				
Syslogs from All Event O	lasses				
C Filter on severity	Emergencies	+			
E Like event list	user-auth-syshi	New.			
C. C. Market		<u> </u>			
C Disable logging fro	m all event classe	8			
Syslogs from Specific Ev	ent Classes				
			Event Class	Severity	F.
121	-				
Event Class: auth	<u> </u>	Add >>	1		
Description: User a	Authentication	- Augusta			
Severity: Emer	gencies 💌				
Sectores of these	and the second				
		~	and I am		
		OK	Cancel Help		

figuration > Device Management > Loggi	ng > Logging Filters	
Configure syslog filters for logging destinations.		
Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classer
SNMP Trap	++ Disabled ++	
Internal Buffer	Event List: user-auth-syslog	
E-Mail	Disabled	(
Console	Disabled	
Telnet and SSH Sessions	Disabled	
ASDM	Disabled	
Syslog Servers	Disabled	

Éstos son los pasos en cómo enviar un grupo de mensajes (basados en su nivel de gravedad) al servidor del email.

1. Seleccione el **email** en el campo de destino de registro. Entonces, el tecleo

nfiguration > Device Management > Logg	na > Loaging Filters		
Configure syslog filters for logging destinations.			
Logging Destination	Syslags From All Event: Classes	Syslags From Specific Event Classes	[Ea
SNMP Trap	Disabled		
Internal Buffer	Event List: user-auth-syslog		
E-Mail	++ Disabled ++		
Cansole	Disabled		
Telhet and SSH Sessions	Disabled		
ASDM	Disabled		
Syslog Servers	Disabled		

2. Elija el **filtro en la** opción de la **gravedad** y seleccione el nivel de gravedad requerido.

ogging Destination: E-Mail				
ivslogs from All Event Classes	-			
Filter on severity) Emergencies Sevent list Disable logging from Critical Errors	New	J		
iyslogs from Specific Eve Warnings Notifications Informational Debugging	add so 1	Event Class	Severity	
Description: User Authentication	Delete			

quí, las **alertas** se han seleccionado como el nivel de

gravedad.

onfigure syslog filters for logging destinations.		
Logging Destination	Syslags From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	Disabled	
nternal Buffer	Event List: user-auth-syslog	
-Hal	Severity: Alerts	
ionsole	Disabled	
enet and SSH Sessions	Disabled	
SDM	Disabled	
iyslog Servers	Disabled	

Usted puede ver que todos los mensajes de Syslog alertas deben ser enviados al email configurado.

inFigure syslog filters for logging destinations.		
Logging Destination	Syslags From All Event: Classes	Syslogs From Specific Event Classes
Internal Buffer	Event List: user-auth-syslog	
5NMP Trap	Disabled	
E-Mail	Severity: Alerts	
Console	Disabled	Π
Teinet and SSH Sessions	Disabled	
ASDM	Disabled	
Sysing Servers	Disabled	

Límite de velocidad

Esto especifica el número de mensajes de Syslog que Cisco ASA envíe a un destino en un periodo de tiempo especificado. Se define generalmente para el nivel de gravedad.

1. Elija la configuración > la Administración de dispositivos > el registro > el límite de velocidad

y seleccione el nivel de gravedad requerido. Entonces, el tecleo **edita**.

Logging Level	No. of Messages	Interval (Seconds)	Edit
ebugging	urinited		
otifications	uninited		
Rical	unlimited		
mergencies	unimited		
anings	unimited		
rors	unlimited		
formational	unimited		
formational Jarts	unimited unimited		
rformational Narts	unimited		

2. Especifique el número de mensajes que se enviarán junto con el intervalo de tiempo. Haga

To allow an unlimited r Number of Messages (number of messages ke and Time Interval fields	ep both the empty.
Logging Level:	Debugging	
Number of Messages:	600	
Time Interval	86400	seconds

Nota: Estos números se

dan como un ejemplo. Éstos diferencian dependiendo del entorno del tipo de red.Los valores modificados se consideran

		,	
20			
au	u	Ι.	
	-		

Configuration > Device Management > Log	ning > 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)
Debugging	600	86400
Notifications	unimited	
Critical	unimited	

Registración de los golpes de una regla de acceso

Usted puede registrar los golpes de la regla de acceso usando el ASDM. El comportamiento predeterminado del registro es enviar un mensaje de Syslog para todos los paquetes negados. No habrá ningún mensaje de Syslog para los paquetes permitidos y éstos no serán registrados. Sin embargo, usted puede definir un nivel de gravedad de encargo del registro a la regla de acceso para seguir la cuenta de los paquetes que golpea esta regla de acceso.

Siga estos pasos:

1. Seleccione la regla de acceso requerida y el tecleo edita. El editar la ventana de la regla de

Interface:	inside	
Action:	(• Permit C Deny	
Source:	10.10.10 -	
Destination	20.20.200	
Service:	ip	
Description:		
🔽 Enable L	ogaing	
Logging I	Level: Default 👻	
	Default 🔺	
More Opt	ions Emergencies	
	Critical	1
	Errors OK Cancel Help	
	Warnings	
	END AND A DECOMP	

acceso aparece.

esta imagen, la *opción predeterminada* en el campo del *nivel de registro* indica el comportamiento predeterminado del registro de Cisco ASA. Para más información sobre esto, refiera a la sección de la <u>actividad de la lista de acceso del registro</u>.

2. La marca de tilde la *opción de registro del permiso* y especifica el nivel de gravedad requerido. Entonces, *AUTORIZACIÓN del*

Diterrate:	C	-			
Action:	(* Permit C	Deny			
Source:	10.10.10.10		-		
Destination	20.20.20.200		-		
Service;	ip		-		
Description:					
Frable L	, oging				
Logging I	evel: Errors				
More Opt	ons				C
🔽 Enable	Rule				and the second
Traffic Dire	ction: @ In	C or.			
Source Ser	vice:		- (10	P or UDP service	only)
Logging Ini	erval: 300	seconds			
Time Rang	e 🗌	·			

Nota: Haci

endo clic la *más* lengueta del descenso-abajo de las *opciones*, usted puede ver la opción del *intervalo del registro*. Se resalta esta opción solamente cuando se hace tictac la *opción de registro* antedicha del *permiso*. El valor predeterminado de este temporizador es 300

segundos. Esta configuración es útil en especificar el valor del time out para que las flujoestadísticas sean borradas cuando no hay coincidencia para esa regla de acceso. Si hay algunos golpes, después el ASA espera hasta la duración del intervalo del registro y envía eso al Syslog.

3. Las modificaciones se muestran aquí. Alternativamente, usted puede hacer doble clic el campo del *registro de la* regla de acceso específica y fijar el nivel de gravedad allí.

4	Enabled	Source	Destination	Service	Action	Hits	Logging	10	Time
Ş\$ i	nside (5 inco	ming rules)			111-001-00	-1			
1	P	3 10.10.10.10	20.20.20.200	JE ID	🥩 Permit	0	Errors		1
2		10.10.10.20	any	JP ip	🖌 Permit	0			1
3		10.20.10.0/24	20.20.20.200	🧾 ip	3 Deny	0			
4		r inside-network/26	🔹 any	ID ID	Permit	0	Default		
5		any	any	ar ip	3 Deny		Default	*	Implicit rule
pi e	utside (1 im	plicit incoming rules)			- Comp.		mergencies	111	1/2000/10/10/10/00
1	any		🧇 any 📣 any 👥 ko 📢		3 Deny	1	Alerts		Implicit rule
							Errors Warnings Votifications Informational	-	

Nota: Este Método alternativo de especificar el *nivel de registro* en el mismo cristal de las *reglas de acceso* haciendo doble clic trabaja para solamente las entradas manualmente creadas de la regla de acceso, pero no a las reglas implícitas.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta <u>Command Lookup Tool</u> (<u>clientes registrados solamente</u>) para obtener más información sobre los comandos utilizados en esta sección.

Configuraciones

En este documento, se utilizan estas configuraciones:

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
1
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

 Usted puede ver los Syslog del ASDM. Elija la supervisión > el registro > Log Viewer en tiempo real. Aquí se muestra la salida de muestra:

estia.								
itoring >	Logging > Re	eal-Time I	og Viewer					
al-Time Log	Viewer							
😰 Real-1	lime Log Vier	ver - 10.7	8.177.11			Laparente de la		_DX
File To	ols Window	Help						
00 Paus	e Ma ⊆opy	Save 1	Clear	Color Settings	Create Ru	le 📷 Show Rule	Show Details	? Help
Ster Bu-		1	- EL Elta	t III stick Al	Find		a .	
actor 071			- altrais	C III SISTER	r inser [
Seventy	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	
6 🔔	May 31 2011	10:24:38	606003	10.78.153.167				ASDM logging session number 0 from 10.3
1.6	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*
<u>₹</u> 6	May 31 2011	10:24:38	725002	10.78.153.167	4009			Device completed SSL handshake with circ
<u>i</u> 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:
<u>\$</u> 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
<u>a</u> 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
4.6	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

Troubleshooting

Problema: Conexión perdida -- Conexión del Syslog terminada --

Se recibe este error al intentar habilitar el ASDM que registra en el panel del dispositivo para los contextos uces de los.

"Conexión perdida -- Conexión del Syslog terminada --"

Cuando el ASDM se utiliza para conectar directamente con el contexto admin y registro ADSM se inhabilita allí, después Switch a una registración del ASDM del subcontext y del permiso. Se reciben los errores, pero los mensajes de Syslog están alcanzando muy bien al servidor de Syslog.

Solución

Esto es un comportamiento sabido con el ASDM de Cisco y documentó en el Id. de bug Cisco <u>CSCsd10699</u> (clientes registrados solamente). Como solución alternativa, registro del asdm del permiso cuando está registrado en el contexto admin.

No puede ver el tiempo real abre una sesión el ASDM de Cisco

Un problema es que los registros en tiempo real no se pueden ver en el ASDM. ¿Cómo se configura esto?

Solución

Configure el siguiente en Cisco ASA:

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

Información Relacionada

- Soporte del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte Técnico y Documentación Cisco Systems