ASA 8.2: Configurazione di Syslog mediante ASDM

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Configurazione di syslog di base con ASDM Abilita registrazione Disabilita registrazione Accesso a un messaggio di posta elettronica Accesso a un server Syslog Configurazione syslog avanzata con ASDM Utilizzo degli elenchi di eventi Utilizzo dei filtri di registrazione Limite di velocità Registrazione dei riscontri di una regola di accesso Configurazione Configurazioni Verifica Risoluzione dei problemi Problema: Connessione interrotta — Connessione syslog terminata — Soluzione Impossibile visualizzare i log in tempo reale su Cisco ASDM Soluzione Informazioni correlate

Introduzione

In questo documento viene spiegato come configurare syslog su Cisco Adaptive Security Appliance (ASA) 8.x usando l'interfaccia utente di Adaptive Security Device Manager (ASDM). I messaggi del registro di sistema sono i messaggi generati dall'appliance Cisco ASA per notificare all'amministratore qualsiasi modifica apportata alla configurazione, alle impostazioni di rete o alle prestazioni del dispositivo. Analizzando i messaggi del registro eventi di sistema, un amministratore può risolvere facilmente l'errore eseguendo un'analisi della causa principale.

I messaggi Syslog vengono differenziati principalmente in base al livello di gravità.

1. Gravità 0 - Messaggi di emergenza - Risorsa inutilizzabile

- 2. Gravità 1 Messaggi di avviso È necessaria un'azione immediata
- 3. Gravità 2 Messaggi critici Condizioni critiche
- 4. Gravità 3 Messaggi di errore Condizioni di errore
- 5. Gravità 4 Messaggi di avviso Condizioni di avviso
- 6. Gravità 5 Messaggi di notifica Condizioni normali ma significative
- 7. Gravità 6 Messaggi informativi Solo messaggi informativi
- 8. Gravità 7 Messaggi di debug Solo messaggi di debug**Nota:** il livello di gravità più alto è quello di emergenza, mentre il livello più basso è quello di debug.

Di seguito sono riportati alcuni messaggi di syslog di esempio generati dall'appliance Cisco ASA:

- %ASA-6-106012: Nega IP da indirizzo_IP a indirizzo_IP, opzioni IP esadecimali.
- %ASA-3-211001: Errore di allocazione della memoria
- %ASA-5-35003: ACL predefinito NAC applicato, ACL:nome-ACL indirizzo-host

Il valore numerico X specificato in "%ASA-X-YYYY:" indica la gravità del messaggio. Ad esempio, "%ASA-6-106012" è un messaggio informativo e "%ASA-5-35003" è un messaggio di errore.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA versione 8.2
- Cisco ASDM versione 6.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione di syslog di base con ASDM

Abilita registrazione

Attenersi alla seguente procedura:

1. Scegliere *Configurazione > Gestione periferiche > Registrazione > Impostazione registrazione* e selezionare l'opzione *Abilita*

registrazione. É Cisco ASDM 6.2 for ASA - 10.78.177.11	
Home Configuration Monitor	ng 🔚 Save 🔇 Refresh 🔇 Back 🕥 Forward 🤗 Help
	Configuration > Device Management > Logging > Logging Setup Enable logging Enable logging Send debug messages as syslogs Send for Size: 4096 Vou can choose to save the buffer contents before the buffer is overwritten. Save Buffer To:

2. Èpossibile registrare i messaggi syslog in un buffer interno specificandone le dimensioni. Potete anche scegliere di salvare il contenuto del buffer nella memoria flash facendo clic su *Configura uso Flash* e definendo le impostazioni di

Configuration > Device Management > Logging > Logging Setup

F Enable logging	Enable logging on the failover standby unit
F Send debug messages as syslogs	F Send syslogs in EMBLEM format
igging 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 overwritte
Durrer Size:	byces
You can choose to save the buffer of	contents before the buffer is overwritten.
Save Buffer To: 🔲 FTP Server	Configure FTP Settings
(P Flash	Configure Flash Usage
SDM Logging	
Specify the size of the queue for sy	shos intended for viewing in ASDM.
Queue Size: 100	🕼 Conligure 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 France Source to Re Discounds 20076
	Parallal Processing and the served and the served and the

Flash.

3. I messaggi di log nel buffer possono essere inviati a un server FTP prima di essere sovrascritti. Fare clic su *Configure FTP Settings* (Configura impostazioni FTP) e specificare i dettagli del server FTP, come mostrato di

Iv chable logging		Enable logging on t	the failover standby unit
F Send debug me	sages as syslogs	Send syslogs in EM	BLEM Format
Logging to Internal Bu	ffer		
Specify the size o	f the internal buffe	r to which syslogs will be	saved. When the buffer fills up, it will be over
Buffer Size:	4096 t	oytes	
You can choose to	save the buffer o	optents before the buffr	r is overwritten
Save Differ To:	ETP Source	Configure ETD Setting	~
Save burler 10.	- Fir Sarray	Configure Fife Second	P
	Flash	Configure Flash Usag	e
ASDM Logging		de e eme	-
Specify the size o	f the queue for s	te configure FTP Set	ungs
Queue Size: 100	â.	🔽 Enable FTP client	
		Server IP Address:	172,16,18.10
		Path:	[
		Username:	testuser
		Parsured	******
		Fashing.	
		Confirm Password:	

Disabilita registrazione

Èpossibile disabilitare gli ID syslog specifici in base alle proprie esigenze.

Nota: selezionando il segno di spunta per l'opzione *Includi indicatore orario nei syslog*, è possibile aggiungere la data e l'ora in cui sono stati generati come campo nei syslog.

1. Selezionare i syslog da disabilitare e fare clic su

onfiguration > Device Management > Logging > Syslog Setup				
yslog Format				
Facility Code to Include in Syslogs: 0.0CAL4(20)				
V Include timestame in suspec				
A THOMA CHIMAND AL STROAD				
yslog ID Setup				
Show: All sysing IDs	*			
Sysleg ID	Logging Level	Disabled		Edit
218001	Critical	No	1	
218002	Critical	No		Restore Defaults
218003	Critical	No.		
218004	Critical	No.		
219002	Errors	No		
302003	Informational	No	1.1	
302004	Informational	No	_	
302009	Informational	No.		
302010	Informational	No .		
302012	Informational	No		
302013	Informational	No		
302014	Informational	No		
302015	Informational	No		
302056	Informational	No		
302017	Informational	No,		
302018	Informational	No		

2. Dalla finestra Edit Syslog ID Settings, selezionare l'opzione Disable messages e fare clic su

	202015 202016	
Syslog IDs:	302013, 302010	
Dirable o		
Pisable I		

3. I syslog disattivati possono essere visualizzati in una scheda separata selezionando *ID syslog disattivati* dal menu a discesa *Syslog ID*

Disabled Disabled	E
onal Yes	
ional Yes	Poestone
at	g Level Disabled ational Yes ational Yes

Accesso a un messaggio di posta elettronica

Per inviare i syslog a un messaggio di posta elettronica, completare la procedura seguente utilizzando ASDM:

 Scegliere Configurazione > Gestione dispositivi > Registrazione > Configurazione posta elettronica. Il campo Indirizzo di posta elettronica di origine è utile per assegnare un ID di posta elettronica come origine per i syslog. Specificare l'indirizzo di posta elettronica di origine. Fare clic su Aggiungi per aggiungere i destinatari di posta elettronica.

onfiguration > 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.		
The state of the s		
Source E-Hai Address: Test12 specaripe.com		
Mail Recipients		
Mail Recipients Destination E-Nail Address	Syslog Severity	bbA
-Mail Recipients Destination E-Mail Address	Syslog Severity	bba
-Mail Recipients Destination E-Nail Address	Syslog Severity	Ede

2. Specificare l'*indirizzo e-mail di destinazione* e scegliere il *livello di gravità*. In base ai livelli di gravità, è possibile definire destinatari di posta elettronica diversi. Fare clic su *OK* per tornare al riquadro *Configurazione posta*

Destination F Mail Add	wasternales Terranels con
Destination E-Mail Add	ress: moncorsysiog@example.com
Filter the syslogs sent severity filter used for severity selected below recipients in Configural Filters.	to this recipient by severity. The sysk this recipient will be the higher of the w and the global filter set for all e-mail tion>Properties>Logging>Logging
Syslog Severity:	Errors
Syslog Severity:	Errors Emergencies
Syslog Severity: OK	Errors Emergencies Alerts
Syslog Severity: OK	Errors Emergencies Alerts Critical
Syslog Severity: OK	Errors Emergencies Alerts Critical Errors
Syslog Severity: OK	Errors Emergencies Alerts Critical Errors Warnings
Syslog Severity: OK	Errors Emergencies Alerts Critical Errors Warnings Notifications
Syslog Severity: OK	Errors Emergencies Alerts Critical Errors Warnings Notifications Informational

Il risultato è la seguente

configurazione:

onliguration > 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: Test 123@example.com	
-Mail Recipients	
-Mail Recipients Destination E-Mail Address	Syslog Severity

3. Scegliete *Configurazione > Configurazione dispositivo > Registrazione > SMTP* e specificate il server

SMTP.	
Configuration > Device Management > Loggi	ng > <u>SMTP</u>
Configure the remote SMTP server IP address for	sending email alerts and notifications in response to select events.
D L. CIND C.	
Remote SMTP Server	
Primary Server IP Address: 172.18.10.20	
Secondary Server IP Address:	(Optional)

Accesso a un server Syslog

Èpossibile inviare tutti i messaggi syslog a un server syslog dedicato. Eseguire i seguenti passaggi utilizzando ASDM:

 Scegliere Configurazione > Gestione dispositivi > Registrazione > Server syslog e fare clic su Aggiungi per aggiungere un server syslog.

Interface	IP Address	Protocol/Port	EMBLEM	Secure

Viene visualizzata la finestra Add Syslog Server.

2. Specificare l'interfaccia a cui è associato il server e l'indirizzo IP. Specificare i dettagli *Protocollo* e *Porta* a seconda dell'impostazione della rete. Quindi fare clic su *OK*.**Nota:** verificare di poter raggiungere il server syslog da Cisco

Interface:	linside	<u>×</u>
IP Address:	172.16.11.1	00
Protocol:	C TCP	UDP
Port:	514	_
Log mes	sages in Cisco	EMBLEM format (UD

3. Il server syslog configurato viene visualizzato come mostrato di seguito. Per apportare modifiche, selezionare il server e fare clic su

172.36.11.100 UDP/514 No	00 UDP/514 No. No.	100 UDP/514 No No

Nota: selezionare l'opzione *Consenti passaggio traffico utente quando il server syslog TCP è inattivo*. In caso contrario, le nuove sessioni utente vengono negate tramite l'appliance ASA. Questa opzione è applicabile solo quando il protocollo di trasporto tra l'ASA e il server syslog è TCP. Per impostazione predefinita, le nuove sessioni di accesso alla rete vengono negate da Cisco ASA quando un server syslog non è attivo per qualsiasi motivo.Per definire il tipo di messaggi syslog da inviare al server syslog, vedere la sezione <u>Filtro di registrazione</u>.

Configurazione syslog avanzata con ASDM

Utilizzo degli elenchi di eventi

Gli elenchi di eventi consentono di creare elenchi personalizzati contenenti il gruppo di messaggi syslog da inviare a una destinazione. Gli elenchi di eventi possono essere creati in tre modi diversi:

- ID messaggio o intervallo di ID messaggio
- Gravità messaggio
- Classe messaggio

ID messaggio o intervallo di ID messaggio

Attenersi alla procedura seguente:

1. Scegliere *Configurazione > Gestione dispositivi > Registrazione > Elenchi eventi* e fare clic su *Aggiungi* per creare un nuovo elenco di

onfiguration > Device Management > Logging	> Event Lists		
Use event lists to define a particular set of syslogs th	hat you are interested in. The event list can be used to filter syslogs sent	to a logging destination.	
Name	Event Class / Severity	Message IDs	Add
			and the second sec
			Edit

2. Specificare un nome nel campo *Nome*. Per creare un nuovo elenco di eventi, fare clic su *Aggiungi* nel riquadro *Filtri ID*

filters for the ents the maxi coecified level	e event list. You mum level for lo 1	can filter syslogs by t gging messages. The A	heir class and severity, or by their ID: ASA will filter system log messages wit	s. The severit h severity lev
Class/Severity	/ Filters		Message ID Filters	
ivent Class	Severity	Add	Message IDs	Add
		Edt		Edit
		Delete		Delete

 Specificare l'intervallo degli ID dei messaggi syslog. Qui i messaggi syslog TCP hanno preso per esempio. Fare clic su *OK* per completare l'operazione.

ecify 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 lev severity levels u
ent Classi'Severity Fil	Add Syslog Message ID Hiter	
Event Class	Enter the syslog message ID. Use hyphen to specify a range	Add
LVCIA Class	of syslog IDs, for example, 101001-101010.	
	Message IDs: 302013-302018	Edit
		Delete
	OK Cancel Help	

4. Fare di nuovo clic su OK per tornare alla finestra Elenchi

eventi.		
Configuration > Device Management > Logging > Even	t Lists	
Use event lists to define a particular set of syslogs that you a	re interested in. The event list can be used to filter syslo	gs sent to a logging destination.
Nane	Event Class / Severity	Message IDs
tcp-conn-syslog		302013-302018

Gravità messaggio

1. Èinoltre possibile definire gli elenchi di eventi in base alla gravità del messaggio. Fare clic su Add per creare un elenco di eventi

19(3)		
interested in. The event list can be used to filter syslogs sent to a	a logging destination.	
Event Class / Severby	Message IDs	Add
	302013-302018	Liference and
		Edit
		Delate
	interested in. The event list can be used to filter syslogs sent to Event Class / Seventry	interested in. The event list can be used to filter syslogs sent to a logging destination. Event Class / Severity Message IDs 502019-302018

2. Specificare il nome e fare clic su

	🚰 Add Event List				×
	Name: syslog-sev-e Specify filters for the represents the maxi to the specified leve	eror e event list. You mum level for log I.	can filter syslogs ging messages. T	by their class and severity, or by their he ASA will filter system log messages v	IDs. The sevenity level with severity levels up
	Event Class/Severity	Filters		Message ID Filters	
	Event Class	Severity	Add	Message IDs	Add
			Edit		Edt
			Dalata		Delete
Aggiungi			ок]	Cancel Help	
			🔂 Add Cla	ss and Severity Filter	×
			Event Clas	s: All	-
			Description	All Event Classes	
			Severity:	From	-
				Emergencies	
			OK	Alerts	
			_	Critical	
				Warnings	
				Notifications	
			100	Informational	
2 Soloziona		rovità Erro	OK	Debugging	
J. JEIEZIUNA	ine il livello ul g		11.		

4. Fare clic su

epresents the max o the specified leve	e event list, rou imum level for log sl.	can filter syslogs by the iging messages. The AS/	r class and severity, or by their L A will filter system log messages w	th severity le
vent Class/Severit	y Filters		Message ID Filters	
Event Class	Severity	Add	Message IDs	Add
All	Errors	Edit		Edit
		Delete		Deret

Classe messaggio

Anche gli elenchi di eventi vengono configurati in base alla classe messaggio. Una classe

messaggio è un gruppo di messaggi syslog correlati a un accessorio di protezione che consente di specificare un'intera classe di messaggi anziché una classe per ogni singolo messaggio. Ad esempio, utilizzare la classe auth per selezionare tutti i messaggi syslog relativi all'autenticazione utente. Di seguito sono elencate alcune classi di messaggi disponibili:

- Tutte: tutte le classi di eventi
- auth Autenticazione utente
- bridge: firewall trasparente
- ca Autorità di certificazione PKI
- config—Command Interface
- ha Failover
- ips Servizio Intrusion Protection
- ip—Stack IP
- np—Network Processor
- ospf—Routing OSPF
- rip Routing RIP
- session Sessione utente

Eseguire la procedura seguente per creare una classe di evento basata sulla classe messaggio *vpnclient-errors*. La classe messaggio, *vpnc*, è disponibile per classificare tutti i messaggi syslog relativi al client vpnc. Il livello di gravità per questa classe messaggio è impostato su "errors".

1. Fare clic su Aggiungi per creare un nuovo elenco di

enti. figuration > Device Management > Logo	inn > Fyrnk Licks		
ise event lists to define a particular set of syslo	gs that you are interested in. The event list can be used to filter syslogs	sent to a logging destination.	
Name	Event Class / Seventy	Message IDs	66A
tcp-conn-syslog		302013-302018	
syslog-sev-error	All / Errors		Edit
			Delete

2. Specificare il nome che si desidera assegnare alla classe messaggio creata e fare clic su

tot	the specified level and Class/Severity	indimieven for id / Filters	gging messages, me	Massage ID Filters	iur sevenity it
[Event Class	Severky	Add	Message IDs	Ad
			Edt		Edi
			Delete		Dels

3. Selezionare vpnc dall'elenco a

e specified leve t Class/Severity	l. / Filters –	🔂 Add Class	and Severity Filter	×	
Event Class	Severi	Event Class:	All		Add
		Description: Severity:	501 5VC	-	Edit
			sys vm		Delete
		OK_	vpdn		

discesa.

4. Selezionare il livello di gravità *Errori*. Questo livello di gravità è applicabile solo ai messaggi registrati per questa classe messaggio. Fare clic su *OK* per tornare alla finestra Aggiungi

. Inbilaterie en	rors			
y filters for the	e event list	You can filter	syslogs by their class and se	everity, c
specified leve	num level f I.	or logging mes	and Severity Filter	tem log i
Event Class	Severi	Event Class:	vpnc	*
		Description:	VPN Client	
		Severity:	Errors	
			Emergencies	
		OK	Alerts	
	1		Critical	
			Errors Warrings	
			Notifications	
			Informational	
		100		

elenco eventi.

5. Di seguito viene riportata la classe/gravità dell'evento. Fare clic su *OK* per completare la configurazione dell'elenco di eventi "vpnclient-

resents the maxim he specified level at Class Sources	e event list, rou mum level for log I.	can filter syslogs by their iging messages. The ASA	Class and severity, or by their IL will filter system log messages wi	ith severity levels up
Event Class	Severity	Add	Message ID Filters	Add
vpnc	Errors	Edit	-	Edit
		Delete		Deete

errors"

screenshot successivo viene inoltre mostrato come creare un nuovo elenco di eventi, "userauth-syslog", con una classe messaggio come "auth" e il livello di gravità per i syslog di questa classe messaggio specifica come "Warnings". Configurando questa opzione, l'elenco degli eventi specifica tutti i messaggi syslog correlati alla classe messaggio "auth", con livelli di gravità fino al livello "Warnings".Nota: qui, il termine "fino a" è di significato. Nel definire il livello di gravità, tenere presente che tutti i messaggi syslog verranno registrati fino a quel livello.Nota: un elenco di eventi può contenere più classi di eventi. L'elenco di eventi "vpnclient-errors" viene modificato facendo clic su Edit e definendo una nuova classe di eventi

"ssl/error".

figuration > Device Management > Log	ging > Event Lists	
Use event lists to define a particular set of sysk	ogs that you are interested in. The event list can be used to filter syslo	gs sent to a logging destination.
Name	Durat Class / Sauraha	Manager The
Name	Event Class / Severky	Pressage tos
tcp-conn-syslog		302013-302018
syslog-sev-error	All / Errors	
vpnclient-errors	vpnc / Errors	

Utilizzo dei filtri di registrazione

I filtri di registrazione vengono utilizzati per inviare i messaggi syslog a una destinazione specificata. I messaggi syslog possono essere basati sulla "gravità" o sugli "elenchi pari".

Di seguito sono riportati i tipi di destinazione a cui i filtri sono applicabili:

- Buffer interno
- Trap SNMP
- E-mail
- Console
- Sessioni Telnet
- ASDM
- Server Syslog

Attenersi alla procedura seguente:

1. Scegliere **Configurazione > Gestione dispositivi > Registrazione > Filtri di registrazione** e selezionare la destinazione di registrazione. Fare quindi clic su **Modifica** per modificare le impostazioni.

nfiguration > Device Management > Loggi	ing > Logging Filters		1
Configure syslog filters for logging destinations.			
Logging Destination	Sysilogs From All Event Clesses	Syslogs From Specific Event Classes	Edit
Internal Buffer	Disabled		
SNMP Trap	Disabled		
E-Mail	Disabled		
Console	Disabled		
Teinet and 55H Sessions	Disabled		
ASDM	Disabled		
Syslog Servers	Disabled'		

2. Èpossibile inviare i messaggi syslog in base alla gravità. In questo caso, **Emergenze** è stato selezionato come

sempio.				
🖆 Edit Logging Filters				
Configure logging filter so generate system log mes Logging Destination: Into Syslogs from All Event Cl	attings. The severity level repres sages with severity levels up to f arnal Buffer asses	ents the maximum level fo the specified level.	r logging messages. The	ASA will
Filter on severity	Emergencies •	\neg		
C Use event list	user-auth-syslog 💌 🛛 New.			
C Disable logging fro Syslogs from Specific Eve	m all event classes Int Classes	Event Class	Severity	
-		Even class	Jerony	
Event Class: Jauth	Add >>			
Description: User A	Uchentication Delete	1		
Severity: Emerg	jencies 💌 🛛	-		
	ОК	Cancel Help		

3. Èinoltre possibile selezionare un elenco di eventi per specificare il tipo di messaggi da inviare a una particolare destinazione. Fare clic su

	our prostriation is				
Syslogs from All I	Event Classes				
C Filter on se	werity Emergencies	÷			
Use event	list user-auth-sys	log - New	1		
C Disable log	ging from all event clas	ses			
	who found classes				
Systeps from Spe	COLLEVER Classes		Event Class	Severity	
	Law with		a torte scard		
Event Class	auth 🗾	Add >>			
Descriptions	User Authentication	Oriete			
Description.	and an other statements of the statement				

4. Verificare la

modifica.

nfiguration > Device Management > Loggi	ng > Logging Filters	
Configure syslog filters for logging destinations.		
Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	Disabled	
Internal Buffer	Event List: user-auth-syslog	12.
E-Mail	Disabled	
Console	Disabled	
Telnet and SSH Sessions	Disabled	
ASDM	Disabled	
Syslog Servers	Disabled	

Di seguito viene descritto come inviare un gruppo di messaggi al server di posta elettronica in base al livello di gravità.

1. Selezionare **E-mail** nel campo Destinazione registrazione. Fare quindi clic su **Modifica**.

onfiguration > Device Management > Logg	ing > Logging Filters		
Configure syslog filters for logging destinations.			
Logging Destination	Syslogs From All Event Classes	Syslegs From SpecFic Event Classes	[Edt
SNMP Trap	Disabled		
Internal Buffer	Event List: user-auth-syslog		
E-Mai	++ Disabled ++		
Cansale	Disabled		1
Telhet and SSH Sessions	Disabled		
ASDM	Disabled		
Syslog Servers	Disabled		

2. Scegliere l'opzione **Filtra in base alla gravità** e selezionare il livello di gravità richiesto.

Configure logging filter settings. The severity level repre- generate system log messages with severity levels up to Longing Destination: E-Mail	esents the maximum level fo o the specified level.	r logging messages. The A	ISA will
Syslogs from All Event Classes	9		
C Disable logging from Critical Errors Syslogs from Specific Eve Notifications Informational	Event Class	Severity	
Event Class: auth Debugging Add >> Description: User Authentication Delete Severity: Emergencies			
Severity: Emergencies	Cancel Help	1	

n questo caso, Alert è stato selezionato come livello di

gravità.

onfigure syslog filters for logging destinations.		
Logging Destination	Syslags From All Event: Classes	Syslogs From Specific Event Classes
INNP Trap	Disabled	
nternal Buffer	Event List: user-auth-syslog	
-14ai	Severity: Alerts	
ionsole	Disabled	
enet and SSH Sessions	Disabled	
SDM	Disabled	
yslog Servers	Disabled	

Tutti i messaggi del syslog di avviso devono essere inviati al messaggio di posta elettronica configurato.

anfigure syslog filters for logging destinations.		
Logging Destination	Syslogs From All Event: Classes	Syslogs From Specific Event Classes
Internal Buffer	Event List: user-auth-syslog	
SNMP Trap	Disabled	
E-Mail	Severity: Alarts	
Console	Disabled	П
Telnet and SSH Sessions	Disabled	U.
ASDM	Disabled	
System Servers	Disabled	

Limite di velocità

Questo valore specifica il numero di messaggi syslog che un'appliance Cisco ASA invia a una destinazione in un periodo di tempo specificato. In genere è definito per il livello di gravità.

1. Scegliere Configurazione > Gestione dispositivi > Registrazione > Limite velocità e

selezionare il livello di gravità richiesto. Fare quindi clic su

Logging Level	No. of Messag	es Interval (Seconds)	Edk
ebuşging	urinited		
otifications	uninited		
rRical	unimited		
tergencies	unimited		
arnings	unimited		
rors	unlimited		
	and instantial		
formational	United		
rformational Jorts	unimited		
Informational Alanta	unimited		
s vella 8 ate i insteri flordon Messanes	urinited		

2. Specificare il numero di messaggi da inviare insieme all'intervallo di tempo. Fare clic su

To allow an unlimite Number of Message	d number of message as and Time Interval fi	s keep both the elds empty.
Logging Level:	Debugging	
Number of Message	es: 600	
	1 Same	(i)

Nota: questi numeri sono riportati

a titolo di esempio. Queste variano a seconda del tipo di ambiente di rete.l valori modificati sono visualizzati

ui:				
Configuration > Device Management	> Logging > Rate Limit			
Assign rate limits for all the syslog messa	ages in a logging level or assign it individ	ually to specific syslog messages.		
Rate Limits for Syslog Logging Levels				
Logging	Level	No. of Messages		Interval (Seconds)
Debugging	60	7	86400	
	000		00400	
Notifications	uni	imted	00400	

Registrazione dei riscontri di una regola di accesso

Èpossibile registrare i risultati della regola di accesso utilizzando ASDM. Il comportamento predefinito della registrazione consiste nell'inviare un messaggio syslog per tutti i pacchetti negati. Non verrà visualizzato alcun messaggio di syslog per i pacchetti consentiti che non verranno registrati. Tuttavia, è possibile definire un livello di gravità di registrazione personalizzato per la regola di accesso, in modo da tenere traccia del numero di pacchetti che raggiungono questa regola di accesso.

Attenersi alla procedura seguente:

1. Selezionare la regola di accesso richiesta e fare clic su Modifica. Verrà visualizzata la finestra Modifica regola di

	inside								
Action:	(* Pe	ermit C Den	γ.						
Source:	10.10	0.10.10							
Destination	20.20	20.20.200							
Service:	ip.		_		_	Ŀ]		
Description:									
🔽 Enable I	.coging								
Logging	Level:	Default	*						
More Opt	ions	Emergencies Alerts							

accesso.

Nota: in questa immagine, l'opzione Default nel campo Logging Level (Livello di registrazione) indica il comportamento di registrazione predefinito di Cisco ASA. Per ulteriori informazioni su questo

argomento, fare riferimento alla sezione Attività dell'elenco accessi alla registrazione.

2. Selezionare l'opzione Enable logging e specificare il livello di gravità richiesto. Quindi fare

ource:	10.10.10.10		1	-		
estination	20.20.20.20	0	1	-		
ervice;	ip			-		
escription: 7 Enable L	ogging					
Logging More Opt	Level: Errors					*
F Enable Traffic Dire	ection: @ in	C or.		- (TCP or L	DP service only)	
Logging In	iterval: 300	seconds			.,	

clic su OK.

facendo clic sulla scheda a discesa Altre opzioni, è possibile visualizzare l'opzione Intervallo di registrazione. Questa opzione è evidenziata solo quando l'opzione Abilita log sopra riportata è selezionata. Il valore predefinito del timer è 300 secondi. Questa impostazione è

utile per specificare il valore di timeout per le statistiche di flusso da eliminare quando non esiste una corrispondenza per la regola di accesso. In caso di riscontri, l'ASA attende l'intervallo di registrazione e lo invia al syslog.

3. Le modifiche sono illustrate di seguito. In alternativa, è possibile fare doppio clic sul campo *Registrazione* della regola di accesso specifica e impostare il livello di gravità.

Image: Sincorning rules) 1 Image: Sincorning rules) 2 Image: Sincorning rules) 3 Image: Sincorning rules) 4 Image: Sincorning rules) 5 Image: Sincorning rules) 1 Image: Sincorning rules) 2 Image: Sincorning rules) 3 Image: Sincorning rules) 4 Image: Sincorning rules) 5 Image: Sincorning rules) 5 Image: Sincorning rules)	
1 Image: Constraint of the second	
2 Image: Second s	
3 Image: Second s	1.0
4 ☑ p⊒ inside-network/26 ≪ any III> to ✓ Permit 0 Default II	
E Calendar C	
any any any ary ary	Implicit rule
Emergencies	1/2000 - 10 11 - 11 - 11 - 11 - 11 - 11 -
1 🥥 any 🖓 any 💷 lp 🔞 Deny Alerts	Implicit rule

Nota: questo metodo alternativo per specificare il *livello di log* nello stesso riquadro *Regole di accesso* facendo doppio clic funziona solo per le voci delle regole di accesso create manualmente, ma non per le regole implicite.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Configurazioni

Nel documento vengono usate queste configurazioni:

Cisco ASA
: 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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

 Èpossibile visualizzare i syslog da ASDM. Scegliere Monitoraggio > Log > Visualizzatore log in tempo reale. Di seguito è riportato un esempio di output⁻

itorina >	Logging > Re	eal-Time I	og Viewer					
al-Time Log	Viewer							
Real-1	lime Log Viel	ver - 10.7	8.177.11					=02
Fie To	ois Window	Help						C 7
00 Page	e Ma ⊆opy	Save 1	Clear	Color Settings	Create Ru	le 📷 Show Rule	Show Details	? Help
Alter By:		1	- B- Fite	r. III stick Al	Find:		a.	
						_	~	
Seventy	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	
<u>\$</u> 6	May 31 2011	10:24:38	606003	10.78.153.167				ASDM logging session number 0 from 10
1.6	May 31 2011	10:24:38	605005	10.78.153.167	4009	10.78.177.11	https	Login permitted from 10.78.153.167/40
1 6	May 31 2011	10:24:38	725002	10.78.153.167	4009			Device completed SSL handshake with c
<u>i</u> 6	May 31 2011	10:24:38	725003	10.78.153.167	4009			SSL client inside: 10.78.153.167/4009 re
6 🌜	May 31 2011	10:24:38	725001	10.78.153.167	4009			Starting SSL handshake with client inside
1.6	May 31 2011	10:24:38	302013	10.78.153.167	4009	10.78,177.11	443	Bult inbound TCP connection 136 for ins
1 6	May 31 2011	10:24:31	725007	10.78.153.167	4008			SSL session with client inside: 10.78.153
£ 6	May 31 2011	10:24:31	106015	10.78.153.167	4008	10.78.177.11	443	Deny TCP (no connection) from 10.78.1
<u>\$</u> 6	May 31 2011	10:24:31	302014	10.78.153.167	4006	10.78.177.11	443	Teardown TCP connection 135 for inside
R 5	May 31 2011	10:24:31	111008					User 'test' executed the 'logging asdm a
								Sysleg Connection Lost

Risoluzione dei problemi

Problema: Connessione interrotta — Connessione syslog terminata —

Questo errore viene visualizzato quando si tenta di abilitare la registrazione ASDM nel dashboard dei dispositivi per uno qualsiasi dei contesti.

"Connessione interrotta - Connessione syslog terminata -"

Quando ASDM viene utilizzato per connettersi direttamente al contesto di amministrazione e la registrazione ADSM è disabilitata in questo contesto, passare a un sottocontesto e abilitare la registrazione ASDM. Gli errori vengono ricevuti, ma i messaggi syslog stanno raggiungendo il server syslog.

Soluzione

Questo è un comportamento noto di Cisco ASDM e documentato nell'ID bug Cisco CSCsd10699

(solo utenti <u>registrati</u>). Per risolvere il problema, abilitare la registrazione asdm quando si è connessi al contesto di amministrazione.

Impossibile visualizzare i log in tempo reale su Cisco ASDM

Il problema è che i log in tempo reale non possono essere visualizzati su ASDM. Come viene configurato?

Soluzione

Configurare quanto segue sull'appliance Cisco ASA:

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

Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance Support</u>
- Documentazione e supporto tecnico Cisco Systems