ASA 8.2:使用ASDM配置系統日誌

目錄

簡介 必要條件 需求 採用元件 慣例 使用ASDM進行基本系統日誌配置 啟用日誌記錄 禁用日誌記錄 登入到電子郵件 登入到系統日誌伺服器 使用ASDM進行高級系統日誌配置 使用事件清單 使用日誌記錄過濾器 速率限制 記錄訪問規則的命中數 設定 組態 驗證 疑難排解 問題:連線丟失 — 系統日誌連線已終止 — 解決方案 無法檢視Cisco ASDM上的即時日誌 解決方案 相關資訊

<u>簡介</u>

本文提供有關如何使用自適應安全裝置管理器(ASDM)GUI在思科自適應安全裝置(ASA)8.x上配置系 統日誌的資訊。系統日誌消息是由Cisco ASA生成的消息,用於通知管理員配置的任何更改、網路 設定更改或裝置效能更改。通過分析系統日誌消息,管理員可以通過執行根本原因分析輕鬆排除錯 誤。

系統日誌消息主要根據其嚴重性級別來區分。

- 1. 嚴重性0 緊急消息 資源不可用
 2. 嚴重性1 警報消息 需要立即採取行動
 3. 嚴重級別2 嚴重消息 嚴重情況
- 4. 嚴重性3 錯誤消息 錯誤條件

5. 嚴重性4 — 警告消息 — 警告條件

6. 嚴重性5 — 通知消息 — 正常但重要的情況

7. 嚴重性6 — 資訊性消息 — 僅資訊性消息

8. 嚴重性7 — 調試消息 — 僅調試消息**注意:**最高嚴重性級別為緊急,最低嚴重性級別為調試。 Cisco ASA生成的示例系統日誌消息如下所示:

•%ASA-6-106012:拒絕從IP_address到IP_address的IP,IP選項十六進位制。

•%ASA-3-211001:記憶體分配錯誤

•%ASA-5-335003:NAC應用預設ACL, ACL:ACL-name - host-address

在「%ASA-X-YYYY:」中指定的數值X表示消息的嚴重性。例如,「%ASA-6-106012」是資訊性 消息,「%ASA-5-335003」是錯誤消息。

必要條件

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco ASA版本8.2
- Cisco ASDM版本6.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

使用ASDM進行基本系統日誌配置

請完成以下步驟:

1. 選擇*Configuration > Device Management > Logging > Logging Setup*,然後選中*Enable logging*選項。



 您可以通過指定緩衝區大小,將系統日誌消息記錄到內部緩衝區。您也可以通過按一下配置快 *閃記憶體使用情況*並定義快閃記憶體設定,選擇將緩衝區內容儲存到快閃記憶體。

🖾 Enable logging	F Enable logging on the failover standby unit	
F Send debug messages as syslogs	Send syslogs in EMBLEM format	
Logging to Internal Buffer	r to which syslogs will be saved. When the buffer fills up, it will be overw sytes ontents before the buffer is overwritten.	ritte
Save Buffer To: FTP Server	Configure FTP Settings Configure Flash Usage	
ASDM Logging		
Specify the size of the queue for sys Queue Size: 100	Incs Intended for viewon in ASDM. 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	h
	Minimum Free Space to Be Preserved: 3076 KB	

3. 緩衝日誌消息可以在被覆蓋之前傳送到FTP伺服器。按一下「*Configure FTP Settings*」,然 後指定FTP伺服器詳細資訊,如下所示

🔽 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 inter	nal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.
Buffer Size: 4096	bytes
ASDM Logging Specify the size of the queu	Configure Flash Usage
Queue Size: 100	Enable FTP client
	Server IP Address: 172,16.18.10
	Path:
	Username: testuser
	Password: ******
	Confirm Password: +++++++

<u>禁用日誌記錄</u>

您可以根據要求禁用特定系統日誌ID。

注意:通過為*Include timestamp in syslogs*選項選擇複選標籤,可以將作為欄位生成的日期和時間 新增到syslogs中。

infiguration > Device Management > Logging > Sysleg Setup			
slog Format Facility Code to Indude in Sysloge: 0.0CAL4(20)			
Trolude timestamp in syslogs			
slog ID Setup			
Show: All syslog IDs	×		and share a
Sysleg ID	Logging Level	Disabled	Edit
218001	Critical	No	
218002	Critical	No	Restore Defau
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	No	
302015	Informational	No	
302016	Informational	No	
302017	Informational	No	

2. 在Edit Syslog ID Settings視窗中, 選中Disable messages選項, 然後按一下OK。

	302015, 302016	
Syslog IDs:		
🔽 þisable m	essages	
ogging Leve	I: Informational	*

3. 通過在*Syslog ID Setup*下拉選單中選擇*Disabled syslog IDs*,可以在單獨的頁籤中檢視禁用的 系統日誌。

Configuration > Device Management > Logging > Syslog Setup			
Syslog Format			
Facility Code to Include in Syslogs: LOCAL4(20)			
🔽 Include timestamp in syslogs			
Syslog ID Setup			
Show: Disabled system IDs			
Syslog 10	Logging Level	Disabled	6
302015	Informational	Yes	

<u>登入到電子郵件</u>

使用ASDM完成以下步驟,以便將系統日誌傳送到電子郵件:

 選擇Configuration > Device Management > Logging > E-Mail Setup。Source E-Mail Address欄位有助於將電子郵件ID指定為系統日誌的源。指定源電子郵件地址。現在,按一下 Add新增電子郵件收件人。

	and a second
2.0.2	
syslog seventy	DDA
	Edit
	1 ACA200 1
	Syslog Severity

2. 指定目*的地電子郵件地址*並選擇嚴重*性級別*。根據嚴重性級別,您可以定義不同的電子郵件收件人。按一下*OK*返回到*E-Mail Setup*窗格。

Destination E-Mail Address:	monitorsyslog@example.com		
Filter the syslogs sent to thi severity filter used for this r severity selected below and recipients in Configuration> Filters.	is recipient by severity. The syst recipient will be the higher of the d the global filter set for all e-ma Properties>Logging>Logging	og i	
Syslog Severity:	Errors	<u> </u>	
ОК	Emergencies (Alerts		
	Critical		
	Errors		
	warnings Notifications		
	Informational		
	Debugging	一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	
onfiguration > Device Manage	ment > Logging > E-Mail Setup		
Enter the e-mail address that will b Source E-Mail Address: [test123@ Mail Peripients	ment > Logging > E-Mail Setup be used as the source address when sys Pexample.com	ogs are sent as e-mails.	
Enter the e-mail address that will b Source E-Mail Address: [test123@ -Mail Recipients	ment > Logging > E-Mail Setup be used as the source address when syst Dexample.com Destination E-Mail Address	ogs are sent as e-mails.	Syslog Severit
Enter the e-mail address that will b Source E-Mail Address: test123@ -Mail Recipients monitorsyslog@example.com	ment > Logging > E-Mail Setup be used as the source address when syst Pexample.com Destination E-Mail Address	ogs are sent as e-mails.	Syslog Severit Errors
Infiguration > Device Manage Enter the e-mail address that will b Source E-Mail Address: [test123@ -Mail Recipients monitorsyslog@example.com	ment > Logging > E-Mail Setup be used as the source address when syst Pexample.com Destination E-Mail Address Device: Setup > Logging	ogs are sent as e-mails. > SMTP	Syskog Severit Errors
Infiguration > Device Manage Enter the e-mail address that will b Source E-Mail Address: [test1230] -Mail Recipients Monitorsyslog@example.com 評審 Configuration > D onfiguration > Device N	ment > Logging > E-Mail Setup be used as the source address when syst Dexample.com Destination E-Mail Address Device Setup > Logging Management > Logging > S	ogs are sent as e-mails. <i>> SMTP</i> ,並指定SMTF	Syslog Severit Errors 2 伺服器。
Infiguration > Device Manage Enter the e-mail address that will the source E-Mail Address: [test123@ -Mail Recipients Monitorsyslog@example.com 持業 Configuration > Device Managements Configure the remote SM	ment > Logging > E-Mail Setup be used as the source address when syst Dexample.com Destination E-Mail Address Device Setup > Logging Management > Logging > S TP server IP address for sendin	ogs are sent as e-mails. <i>> SMTP</i> ,並指定SMTF MTP g email alerts and notifications	Syslog Severit Errors 2 伺服器。 in response to select events
Infiguration > Device Manage Enter the e-mail address that will the Source E-Mail Address: [test123@ -Mail Recipients Mail Re	ment > Logging > E-Mail Setup be used as the source address when syst Pexample.com Destination E-Mail Address Device Setup > Logging Management > Logging > S TP server IP address for sendin	ogs are sent as e-mails. <i>> SMTP</i> ,並指定SMTF MTP g email alerts and notifications	Syslog Severit Errors 2 伺服器。 in response to select events
Inter the e-mail address that will the source E-Mail Address: [test1230] Mail Recipients Mail Recipients	ment > Logging > E-Mail Setup be used as the source address when syst Pexample.com Destination E-Mail Address Device Setup > Logging Management > Logging > E TP server IP address for sendin ress: 172.18.10.20	ogs are sent as e-mails. <i>> SMTP</i> ,並指定SMTF MTP g email alerts and notifications	Sysiog Severit Errors 2何服器。 in response to select events
Inter the e-mail address that will the source E-Mail Address: [test1230] Mail Recipients Mail Recipients	ment > Logging > E-Mail Setup be used as the source address when syst Destination E-Mail Address Device Setup > Logging Management > Logging > E TP server IP address for sendin ress: 172.18.10.20 ddress: 172.18.10.20	ogs are sent as e-mails. <i>> SMTP</i> ,並指定SMTF MTP og email alerts and notifications (Optional)	Syslog Severit Errors 2 伺服器。 in response to select events

登入到系統日誌伺服器

可以將所有系統日誌消息傳送到專用系統日誌伺服器。使用ASDM執行以下步驟:

1. 選擇*Configuration > Device Management > Logging > Syslog Servers*,然後按一下*Add*以新 增syslog伺服器。

Interface	IP Address	Protocol/Port	EMOLEM	Secure	4

出現Add Syslog Server視窗。

指定伺服器與IP地址關聯的介面。根據網路設定指定協定和埠詳細資訊。然後,按一下OK。
 注意:確保可以從Cisco ASA訪問系統日誌伺服器。



3. 配置的系統日誌伺服器如下所示。選擇此伺服器,然後按一下編輯後,即可進行修改。

1140411000	IP Address	Protocol/Port	EMBLEM	Secure	Add
de	172.16.11.100	UDP/514	No	No	60
					Delet
fy the number of messages that	t are allowed to be queued when a syslog	server is busy. Use 0 to indicate unlimited o	ueue size.		
and the second se	in a state in the state of the st				
and a second sec					
Queue Size 512					

注意:選中Allow user traffic to pass when TCP syslog server is down選項。否則,新使用者 會話將通過ASA被拒絕。僅當ASA和syslog伺服器之間的傳輸協定為TCP時適用。預設情況下 ,Cisco ASA會在系統日誌伺服器因任何原因關閉時拒絕新的網路訪問會話。要定義要傳送到 系統日誌伺服器的系統日誌消息的型別,請參閱<u>日誌記錄過濾器</u>部分。

使用ASDM進行高級系統日誌配置

使用事件清單

事件清單使我們能夠建立自定義清單,其中包含要傳送到目標的系統日誌消息組。可以通過三種不同的方法建立事件清單:

- 消息ID或消息ID的範圍
- 消息嚴重性
- 消息類

消息ID或消息ID的範圍

請執行以下步驟:

1. 選擇*Configuration > Device Management > Logging > Event Lists*,然後按一下*Add*以建立新 的事件清單。

Nane		Event Class / Severity	Message (Ds	
「夕孫、蜩侍中将	宁_ <i>佃</i> 夕瑶		ltoro容枚中拉	以建立新的建
百倍」 頒 区中 佰	<i>正 画</i> 石特。	TEMESSAGE ID FI	ile/S图伯中按 下Add,5	以建立利的有
Name: Itcn-copp-s	vsloa			
manes tep comins	7500			
Specify filters for t	he event list. You	can filter syslogs by thei	r class and severity, or by their ID	s. The severity i
represents the max to the specified law	kimum level for log el	gging messages. The ASA	will filter system log messages wi	th severity levels
co die specified lev	261			
Event Class/Severi	ty Filters		Message ID Filters	
Event Class/Severi	ty Filters	Add	Message ID Filters Message IDs	Add
Event Class/Severi Event Class	ty Filters Severity	Add	Message ID Filters Message IDs	Add
Event Class/Severi Event Class	ty Filters Severity	Add	Message ID Filters Message IDs	Add
Event Class/Severi Event Class	ty Filters Severity	Add Edt Delete	Message ID Filters Message IDs	Edit Delete
Event Class/Severi	ty Filters	Add Edt Delete	Message ID Filters Message IDs	Edit Delete
Event Class/Severi	ty Filters	Add Edt Delete	Message ID Filters Message IDs	Edit Delete
Event Class/Severi	ty Filters	Add Edt Delete	Message ID Filters Message IDs	Add Edit Delete
Event Class/Severi	ty Filters	Add Edt Delete	Message ID Filters Message IDs	Edit Delete
Event Class/Severi	ty Filters	Add Edit Delete	Message ID Filters Message IDs	Edit Delete
Event Class/Severi	ty Filters	Add Edt Delete OK Cance	Message ID Filters Message IDs Help	Edit Delete

presents the maximum the specified level.	n level for logging messages. The ASA will filter system log messages with	h severity levels up
ent Class/Severity Fi	Enter the oxieg message ID. Use humber to specify a same	
Event Class	of syslog IDs, for example, 101001-101010.	Add
	Message IDs: 302013-302018	Edit
		Delete
	OK Cancel Help	

4. 再次按一下OK以恢復到Event Lists視窗。

adon > Device Hanagement > Logging > Lyc	ncusts	
vent lists to define a particular set of syslogs that you	are interested in. The event list can be used to filter syslogs sent t	a logging destination.
Name	Event Class / Severity	Message IDs

消息嚴重性

1. 還可以根據消息嚴重性定義事件清單。按一下Add以建立單獨的事件清單。

Nane	Event Class / Seven	ky	Message IDs	
conn-syslog		302013-302	018	
之稻並按一下Add				
			VI	
dd Evenc Lisc				
ne: syslog-sev-error				
cify filters for the event list. Yo	u can filter syslogs by their class an	d severity, or by their ID	s. The severity level	
resents the maximum level for i be specified level.	ogging messages. The ASA will filter	r system log messagas w	th seventy levels up	
nt Class/Sevenity Filters	Message	ID Filters		
Funnt Class Security		Massage IDe	1 Mar 1	
Event class Deverky		message ups		
	Edit		Edt	
	Delete 1		Onlora	
	0.01010		001000	
1	or 1 carret 1	Heb		
	OK Cancel	Help		
[OK Cancel	Help		
	OK Cancel	Help	×	
	OK Cancel	Help y Filter	×	
	OK Cancel	Help y Filter	×	
	OK Cancel	Help y Filter	×	
	ОК Cancel Ca	Help y Filter	×1]	
	ОК Cancel Салсе! Са	Help y Filter	×1] ;	
	OK Cancel	Help y Filter ses		
	OK Cancel	Help y Filter ses	× [
	OK Cancel	Help y Filter ses		
	OK Cancel	Help y Filter		
	OK Cancel	Help y Filter		
	OK Cancel	Help y Filter		
	OK Cancel	Help y Filter ses		
	OK Cancel	Help y Filter ses		
	OK Cancel	Help y Filter ses		

4. 按一下「*OK*」(確定)。

resents the maxi the specified leve ent Class/Severity	mum level for lo I. / Filters	gging messages. The A	SA will filter system log messages wi Message ID Filters	th severity levels
Event Class	Severity	Add	Message IDs	Add
All	Errors	Edit		Edit
		Delete		Delete
				87

消息類

事件清單也會根據消息類進行配置。消息類是一組與安全裝置功能相關的系統日誌消息,通過該功 能,您可以指定整個消息類,而不是為每個消息單獨指定類。例如,使用auth類選擇與使用者身份 驗證相關的所有系統日誌消息。下面顯示了一些可用的消息類:

- All 所有事件類
- auth 使用者身份驗證
- bridge 透明防火牆
- ca PKI證書頒發機構
- config 命令介面
- ha 故障轉移
- ips 入侵防護服務
- ip IP堆疊
- np 網路處理器
- ospf OSPF路由
- rip RIP路由
- session 使用者會話

執行以下步驟,根據*vpnclient-errors*消息類建立事件類。消息類*vpnc*可用於對與vpnclient相關的所 有系統日誌消息進行分類。此消息類的嚴重性級別選擇為「錯誤」。

1. 按一下新增以建立新的事件清單。

Name	Event Class / Seventy	Message IDs	Add
p-conn-syslog		302013-302018	
dogisevierror	All / Errors		Edit

2. 指定要與所建立的消息類相關的名稱,然後按一下Add。

e specified lev t Class/Severi	ei. Ity Filters ——		Message ID	Fiters	
Event Class	Severity	Add		Message IDs	Add
		Edt			Edit
		Delete	-		Delete

3. 從下拉選單中選擇vpnc。

pecified level.	🚺 Add Class and Severity Filter	N .
vent Class S	ers Event Class: All and T	add
	Description: ssl *	Edit
	Severity: SYS	Defete
	OK vpdn	
		4

4. 選擇嚴重性級別為錯誤。此嚴重性級別僅適用於為此消息類記錄的消息。按一下OK以恢復到 ddd Event Li

represe	ints the maxim	num level l	for logging mes	sages. The ASA will filter	system log
to the s	specified level		📬 Add Class	and Severity Filter	
Event C	Jass/Seventy	Severi	Event Class:	vpnc	
	Terk Stars	Jeren	Description:	VPN Client	
			Severity:	Errors	2
			-	Emergencies	
			OK	Alerts	
				Errors	
				Warnings	

「新增事件清單」

5. 此處顯示事件類別/嚴重性。按一下OK完成配置「vpnclient-errors」事件清單。

ecify filters for the presents the maxi the specified leve	e event list. You mum level for log I.	can filter syslogs by thei Iging messages. The ASA	r class and severity, or by their ID will filter system log messages wit	s. The severity level h severity levels up	
ent Class/Severit; Event Class vpnc	y Filters Severity Errors	Edit Delete	Message ID Filters Message IDs	Add Edt Deete	
		OK Cancel	Help		

類相關的系統日誌消息,其嚴重性級別最高「警告」級別。註:在此處,「up」一詞非常重要 。指示嚴重性級別時,請記住,在該級別之前將記錄所有系統日誌消息。註:事件清單可以包 含多個事件類。通過按一下Edit並定義新的事件類「ssl/error」來修改「vpnclient-errors」事件 清單。

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 syslogs s	sent to a logging destination.
Name	Event Class / Severity	Message IDs
tcp-conn-syslog		302013-302018
syslog-sev-error	All / Errors	
vpnclient-errors	vpnc / Errors	

使用日誌記錄過濾器

日誌過濾器用於將系統日誌消息傳送到指定的目標。這些系統日誌消息可以基於「嚴重性」或「偶 數清單」。

以下是這些篩選條件適用的目的地型別:

- 內部緩衝區
- SNMP陷阱
- 電子郵件
- 主控台
- Telnet作業階段
- ASDM
- 系統日誌伺服器

請執行以下步驟:

 選擇Configuration > Device Management > Logging > Logging Filters, 然後選擇日誌記錄目 標。然後,按一下Edit修改設定。

Logging	Systems From	Systegs From
kernal Buller	Disabled	Spear Ever Gasse
MMP Trap	Disabled	
(nail	Deabled	
einet and 55H Sessions	Disabled	
50M	Disabled	
yslog Servers	Disabled'	
コン根摅器舌性俥送系	统日誌消息 此處 Emerge	projes已選定為示例
り 次 仮 J家 敵 主 に 序 込 示) Edit Logging Filters	NILINO/FICIO ULME, LITTEIGE	
care cogging rivers		
onfigure logging filter settings.	The severity level represents the max with severity levels up to the specified	dmum level for logging messages. The ASA level
encrose system by messages i	nal severity levels up to the speared	IS YON
ogging Destination: Internal B.	lfer	
yslogs from All Event Classes		
· Filter on severity Emerg	jencies 💌	
C Use event list user-a	auth-syslog 💌 New	
C Disable logging from all av	ent classes	
· Double roughing moniton ev	010 000000	
urlage from Spacific Funct Clar		
ysings from specific Evenic clas	565	
	Fue	unt classe Severity
		an cruss serviny
Event Class: Jauth	× 1	
Event class. Jaddi	Add >>	
Description: User Authenti	cation	
	Doleto	
Severity: Emergencies	· · · · · · · · · · · · · · · · · · ·	
and the second second		
	OK Cancel	Help
ᆪᄵᇩᇉᆂᄮᆃᇣᅭᄮ		
引以医挥争什月早术拍。 Edit Looping Filters	正安停区到付 正日 惊的月尽到	空別。按一下「OK」(唯定)。
Late Logging Filters		
onfigure logging filter settings. The	severity level represents the maximum level	For logging messages. The ASA will
enerate system log messages with a	evenity levels up to the specified level.	
gging Destination: Internal Buffer		
igging Destination: Internal Buffer Islogs from All Event Classes		
oging Destination: Internal Buffer slogs from All Event Classes C Filter on severity Emergence	s	
oging Destination: Internal Buffer slogs from All Event Classes Filter on sevently Emergence Use event list user-auth-	syslog New	
oging Destination: Internal Buffer rslogs from All Event Classes Pilter on severity Emergence Use event list user-auth- C Disable logging from all event of	syslog 🚽 New	
oging Destination: Internal Buffer vslogs from All Event Classes C Elter on severity Emergence Use event list user-auth- C Disable logging from all event o	syslog 🚽 New	
Internal Buffer Internal Buffer Intern	syslog) New lasses	
Internal Buffer Internal Buffer Intern	syslog 🚽 New lasses Event Class	Seventy

Cancel

Help

OK

Emergencies 💌

Severity:

4. 驗證修改。

figuration > Device Management > Logg	ing > 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	
E-Mail	Disabled	
Console	Disabled	
Telnet and SSH Sessions	Disabled	
ASDM	Disabled	
Syslog Servers	Disabled	

以下是有關如何將一組郵件(根據其嚴重性級別)傳送到電子郵件伺服器的步驟。

1. 在Logging Destination欄位中選擇E-mail。然後按一下Edit。

infiguration > Device Management > Logg	ing > Logging Filters		
Configure syslog filters for logging destinations.			
Logging Destination	Syslogs From All Event: Classes	Syslags From Specific Event Classes	Edt
SNMP Trap	Disabled		
Internal Buffer	Event List: user-auth-syslog		
E-Mail	++ Disabled ++		
Console	Disabled		1
Telhet and SSH Sessions	Disabled		
ASDM	Disabled		
Syslog Servers	Disabled		

2. 選擇**按嚴重性過濾**選項並選擇所需的嚴重性級別。

gging Destination: E-M	tail			
slogs from All Event Cl Filter on severit Use event list Disable logging fro slogs from Specific Eve	Emergencies Emergencies Alerts Critical Errors Warnings Notifications	News	 Generity	
Event Class: auth Description: User A Severity: Emerg	uthentication pencies	Add >> Delete	Jordity	

此處,已選擇Alerts作為嚴重性級別。

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

您可以看到所有警報系統日誌消息都將傳送到已配置的電子郵件。

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
Internal Buffer	Event List: user-auth-syslog	
SNMP Trap	Disabled	
E-Mai	Severity: Alerts	
Console	Disabled	П
Telnet and SSH Sessions	Disabled	
ASDM	Disabled	
Syslog Servers	Disabled	

速率限制

這指定Cisco ASA在指定時間段內傳送到目標的系統日誌消息數。通常針對嚴重性級別進行定義。

選擇Configuration > Device Management > Logging > Rate Limit, 然後選擇所需的嚴重性級別。然後按一下Edit。

Velocitiquin urinited Addifications urinited Unergendes urinited Marrings urinited Unorganitation urinited Marrings urinited	Logging Level		No. of Messages	Interval (Seconds)	Edit
obfications uninited ninited uninited nergenciss uninited ornings uninited nors uninited formational uninited formational uninited	ebuşçing	uninited	and the second		
ritical urinited urinited encoded enco	oblications	unlimited			
rergendies urfinited urfin	Rical	unlimited			
arnings urinetd urinetd formational urinet of the second s	nergencies	unlimited			
rors urinited crimited crimite	amings	unlimited			
fornational orinated originates or the originate orinate originates or the	rors	unlinited			
arts	formational	unimited			
	larts	unimited			
of rate Lindbard Coulon Maryanay					

2. 指定隨時間間隔一起傳送的消息數。按一下「OK」(確定)。

To allow an unlimited	number of messages	keep both the	
Number of Messages	and Time Interval fiel	ds empty.	
Logging Level:	Debugging		
Number of Messages	600		
Number of Messages.			

的型別而異。修改的值如下所示

ign rate limits for all the syslog messages in a logging leve	as accion 3 induide alle to smarth sources massages	
	or assign it marvaciary to specific systed messages.	
Limits for Syslog Logging Levels		
Logging Level	No. of Messages	Interval (Seconds)
Logging Level	No. of Messages	Interval (Seconds) 86400
Logging Level Debugging Votifications	No. of Messages 600 unimited	Interval (Seconds) 86400

<u>記錄訪問規則的命中數</u>

您可以使用ASDM記錄訪問規則命中數。預設日誌記錄行為是向所有被拒絕的資料包傳送系統日誌 消息。對於允許的資料包,不會出現任何系統日誌消息,並且不會記錄這些消息。但是,您可以為 訪問規則定義自定義日誌記錄嚴重性級別,以跟蹤達到此訪問規則的資料包計數。

請執行以下步驟:

1. 選擇所需的訪問規則,然後按一下Edit。出現Edit the Access Rule視窗。

Interface:	inside
Action:	Permit C Deny
Source:	10.10.10.10
Destination	20.20.20.200
Service:	- v
Description:	
C Enable L	coging Level: Default
More Opt	ions Emergencies Alerts Critical OK Cancel Help
	Warnings Notifications

注意:在此映像中, Logging

*Level欄位中的Default*選項表示Cisco ASA的預設日誌記錄行為。有關此問題的詳細資訊,請 參閱<u>日誌記錄訪問清單活動</u>部分。

2. 選中標籤Enable logging選項並指定所需的嚴重性級別。然後,按一下OK。

	ss Rule		
Interface: Action:	inside I Permit C Deny		
Source:	10.10.10.10	-	
Destination	20.20.20.200		
Service:	ip.		
Description:			
C Enable L	evel: Errors		
More Opt	ons		*
Enable	Rule		
Traffic Dire	ction: C in C out		
Traffic Dire Source Ser	ction: Fin Cout		CP or UDP service only)
Traffic Dire Source Ser	rction: @ In C Out. vice: terval: 300 seconds		CP or UDP service only)

「*更多*選項」下拉標籤,您可以看到「記錄*間隔」*選項。僅當勾選上面的*Enable Logging*選項時,才會突出顯示此選項。此計時器的預設值為300秒。此設定可用於指定當該訪問規則沒有匹配項時要刪除的流統計資訊的超時值。如果有任何命中,則ASA將等待「日誌記錄間隔」時間,並將其傳送到系統日誌。

3. 此處顯示修改內容。或者,您可以按兩下特定訪問規則的Logging欄位,並在其中設定嚴重性級別。

Image: Structure (Sincoming rules) 1 Image: Structure (Sincoming rules) 2 Image: Structure (Sincoming rules) 3 Image: Structure (Sincoming rules) 4 Image: Structure (Sincoming rules) 5 Image: Structure (Sincoming rules) Image: Structure (Sincoming rules) Image: Structure (Sincoming rules)	4	Enabled	Source	Destination	Service	Action	Hits	Logging	Tir	ne
1 Image: Second sec	🥵 ins	side (S inco	ming rules)			111 - 51 - 50 - 10 - 11				
2 Image: Second s	1	V	. 10.10.10.10	20.20.20.200	I lo	🖌 Permit	0	Errors		1
3 ✓ ∰ 10.20.10.0/24 ∰ 20.20.20.200 mr ip © Deny 0 4 ✓ Д mside-network/26 mny mr 0 5 mny mny mr mr mr 3 √ mny mny mny mny mny 4 mny mny mny mny mny mny 5 mny mny mny mny mny mny mny model mny mny mny mny mny mny model mny mny mny mny mny mny model mny mny mny mny mny model mny mny mny mny	2	P	10.10.10.20	any	JP- iD	🖌 Permit	0			1
4 ✓ C= inside-network/26 Image: second seco	3		10.20.10.0/24	20.20.20.200	🥦 ip	🕲 Deny	0		1	
5 any any 20 ip 20 Deny Default Multiplicit r 5 provide (1 implicit incoming rules) Alerts Alerts Tracket	4		r inside-network/26	🤹 any	ID (p	💉 Permit	0	Default	2	K
Emergencies	5		🌍 any	any	JE- ip	3 Deny		Default	*	Implicit rule
Alerts Trackets	3 📮 au	utside (1 im	plicit incoming rules) 🦲					Emergencies		
T any any any Deny Deny	1		🥥 any	iany any	ar lo	🕴 Deny		Alerts		Implicit rule

注意:通過按兩下在同一Access Rules**窗格中指定**Logging Level的此替代方法僅適用於手動 建立的訪問規則條目,不適用於隱式規則。

<u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

本檔案會使用以下設定:

CiscoASA

```
: Saved
ASA Version 8.2(1)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
1
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
```



1

使用本節內容,確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

o

 您可以從ASDM檢視系統日誌。選擇Monitoring > Logging > Real Time Log Viewer。輸出示例 如下所示

f Real-1	lime Log Vier	ver - 10.7	8.177.11		1.4	Largest of Cold and		X
File To	ols Window	Help						
00 Paus	e Ma ⊆opy	🗐 Save 1	🔓 Cjear 🖞	Color Settings	Create Ru	le 📸 Show Rule	Show Details	🥐 Help
Alter By:		1	🕶 🏨 Filte	r 🔟 Show Al	Find:		e, i	
Severity	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 10.78.153.167/400*
1.6	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>4</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>i</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
<u>\$</u> 6	May 31 2011	10:24:31	302014	10.78.153.167	4008	10.78.177.11	443	Teardown TCP connection 135 for inside:
A 5	May 31 2011	10:24:31	111008					User 'test' executed the 'logging asdm Inf
								Sysleg Connection Lost

<u>疑難排解</u>

問題:連線丟失 — 系統日誌連線已終止 —

當嘗試在裝置控制面板上為任何情景啟用ASDM日誌記錄時,會收到此錯誤。

" - Syslog - "

當使用ASDM直接連線到管理情景並且那裡禁用了ADSM日誌記錄時,請切換到子情景並啟用 ASDM日誌記錄。收到錯誤,但syslog消息到達syslog伺服器時正常。

<u>解決方案</u>

這是Cisco ASDM的已知行為,記錄在Cisco錯誤ID <u>CSCsd1069</u>(僅限<u>註冊</u>客戶)。 作為解決方法 ,請在登入到管理情景時啟用asdm日誌記錄。

<u>無法檢視Cisco ASDM上的即時日誌</u>

一個問題是,無法在ASDM上檢視即時日誌。此配置如何?

<u>解決方案</u>

在Cisco ASA上配置以下內容:

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

相關資訊

- Cisco ASA 5500系列自適應安全裝置支援
- 技術支援與文件 Cisco Systems