ES-3124 Syslog Setting

情境說明:

當您有許多 ZyXEL 具備 Syslog 網管功能之設備(ex:網管型交換器或 ZyWall 防火牆)時,您可利用一 PC 安裝 Syslog Server 軟體來收集這各網路設備之訊息事件,而有哪些訊息嚴重程級可被收集,詳情請參閱交換器 ES-3124 的 3.70 英文版使用者手冊之第 29 章節 Syslog 篇,下載網址為

http://www.zyxel.com.tw/web/product_family_detail.php?PC1indexflag=2004052016 1143&CategoryGroupNo=9C21E61F-72C1-4DC8-BEC1-E67A6979B2D5

拓墣:



IP:192.168.1.x/24

交換器組態設定

第一部分: 啓動交換器 Syslog 功能

選擇欲進行紀錄 Syslog 日誌的交換器,然後點選 Management > Syslog 開始後續設定,設定方式如以下步驟:

步驟一:勾選 Active 設定並啓用 Syslog 功能項目。另外請自行勾選欲進行紀錄 之項目類別,在此範例為勾選「System」、「Interface」;每個 Syslog 訊息有各自 的嚴重程級,而 Facility 項目為決定您可在 Syslog Server 紀錄多少 Syslog 資訊, 此部份與您所使用的 Syslog Server 軟體有關,請自行查閱您所使用的軟體。設定 完成請點選 Apply 進行設定值套用

LyALL			🗉 Save
MENU Basic Setting	Syslog Setup		Syslog Server Setu
Advanced Application	Syslog	Active 🗹	
Management	25		
	1	A	Free 2044
Maintenance	Logging type	Active	Facility
Access Control	System		local use 5 💙
Diagnostic	Interface		local use 2 💙
Sysiog Cluster Management	Switch		local use 0 💙
MAC Table	Authentication		local use 0 💌
ARP Table	IP		local use 0 🗸
Configure Clone			

步驟二:請點選 Syslog Server Setup,開始設定 Syslog Server 相關資訊

2993 			🗉 Sav
MENU Basic Setting	🕘 Svslog Setup	-	Syslog Server Set
Advanced Application	Syslog	Active 🔽	1,11,1
Application Nanagement			
Maintenance	Logging type	Active	Facility
Access Control	System		local use 5 💌
Diagnostic	Interface	V	local use 2 🗙
Syslog	Switch		local use 0 🗸
Cluster Management	Authentication		local use 0 🗸
ARP Table	IP		local use 0 🗸
Danfarura Olana			

步驟三: 勾選 Active 設定並啓用 Syslog Server 功能項目,並填入該 Server 之 IP 位址,然後選擇 Log Level,請自行決定,最後點選 Add 進行套用

ZvXEL						
						Save
MENU Basic Setting	🔵 🔘 Sysla	g Server	Setup			Syslog Setup
Advanced Application	Acti	ve				
IP Application	Server A	ddress	192.168.1.33			
Management	Log L	evel	Level 0-7 V			
Maintenance						
Access Control			Add	Cancel Clear	7	
Diagnostic			, lud			
Syslog						
Cluster Management						D. I. I.
MAC Table	Index	Active		IP Address	Log Level	Delete
ARP Table	1	Yes	1	92.168.1.33	0-7	
Configure Clone						
			D	elete Cancel		

上述部分為完成交換器之 Syslog 相關組態設定,若要使 Syslog 功能能正常運作, 尚需安裝 Syslog Server 軟體並設定完成,進行 Syslog 接收

第二部分:設定安裝 Syslog Server

找尋任一 PC,並進行 Syslog Server 軟體安裝,由於提供此功能之軟體並非 唯一一種,故在此以 Kiwi 軟體為操作範例,而 Kiwi 軟體下載點為 <u>http://www.kiwisyslog.com/index.php</u>。

步驟一:下載並點選 Kiwi 安裝執行檔進行安裝,在此以 Kiwi8.2.8 版本為例



步驟二:進行軟體 License 同意才可進行後續安裝,請點選 I Agree

Kiwi Syslog Da	emon 8.2.8 Installer	
	License Agreement	
KIWI	Please review the license terms before installing Kiwi Syslog Daemon 8.2.8 .	
Press Page Down	to see the rest of the agreement.	
Terms and Condi	tions of use:	^
You may use the having to registe list so you can be become available	free version of Kiwi Syslog Daemon for as long as you like without ever r. However, it is recommended that you join the Kiwi Software mailing e kept informed of bug reports, usage tips and new releases as they s.	
The free version enable additional key covers a sing need a unique se	of Kiwi Syslog Daemon (SOFTWARE PRODUCT) can be registered to features over and above those of the free product. Each registration le copy of the SOFTWARE PRODUCT installed on a single machine. You rial number and registration code for each copy of the program you	~
If you accept the agreement to inst	terms of the agreement, click I Agree to continue. You must accept the all Kiwi Syslog Daemon 8.2.8 .	
Kiwi Enterprises ——		el

步驟三:請選擇 Kiwi 是否要安裝成為 Windows 作業系統的一個服務,若是,則 只要該 PC 啓動,則 Kiwi 程式也一並啓動,請自行決定。在此範例為不選擇 Kiwi 安裝為 Windows 作業系統的服務。設定完畢請點選 Next 進行下一步驟設定

③ Kiwi Syslo	g Daemon 8.2.8 Installer	
Kiwi	Choose Operating Mode The program can be run as a Service or Application	
O Install K This option ir program to r installs the K	Xiwi Syslog Daemon as a Service Installs Kiwi Syslog Daemon as a Windows service, allowing the un without the need for a user to login to Windows. This option also iwi Syslog Daemon Manager which is used to control the service.	
Install K This option in requiring a u	Ciwi Syslog Daemon as an Application Installs Kiwi Syslog Daemon as a typical Windows application, ser to login to Windows before running the application.	
Kiwi Enterprises	< <u>B</u> ack Next >	Cancel

步驟四:選擇 Kiwi 安裝類別,請用預設值即可,完畢請點選 Next 進行下一步驟 設定

Siwi Syslog Daemon 8.2	2.8 Installer
KIWI	Choose Components Choose which features of Kiwi Syslog Daemon 8.2.8 you want to install.
This will install Kiwi Syslog Da	aemon version 8.2.8
Select the type of install:	Normal
Or, select the optional components you wish to install:	 Program files (required) Shortcuts apply to all users Add Start menu shortcut Add Desktop shortcut Add QuickLaunch shortcut Add Start-up shortcut
Space required: 27.0MB	Description Position your mouse over a component to see its description.
Kiwi Enterprises	< <u>Back</u> Next > Cancel

步驟五:選擇安裝路徑,請依照個人喜好設定,在此以預設值進行安裝,完畢請 點選 Install 進行下一步驟設定

Siwi Syslog Da	emon 8.2.8 Installer
KÎŴI	Choose Install Location Choose the folder in which to install Kiwi Syslog Daemon 8.2.8 .
Setup will install Ki folder, click Brows	wi Syslog Daemon 8.2.8 in the following folder. To install in a different e and select another folder. Click Install to start the installation.
Destination Fold	er es\Syslogd B <u>r</u> owse
Space required: 2	7.0MB
Space available: 6	.4GB
Kiwi Enterprises	
	< <u>B</u> ack Install Cancel

步驟六:Kiwi 軟體安裝過程,調棒跑完即安裝完成

③ Kiwi Syslog Da	emon 8.2.8 Installer	×
KIWI	Installing Please wait while Kiwi Syslog Daemon 8.2.8 is being installed.	
Registering: C:\W	INDOW5\system32\DartSnmp.dll	
Show <u>d</u> etails		
Kiwi Enterprises	< <u>B</u> ack <u>N</u> ext > Cancel	

步驟七:開啓 Kiwi 程式並執行相關設定,設定完畢即可開始收集 Syslog。首先 點選 File > Setup 設定 log 檔案存放位置

👫 Kiwi Syslog Daemon (Version 8.2.8)	
<u>File</u> Edit <u>V</u> iew <u>H</u> elp		
Setup , Ctrl+P Send jest Måssage to localhost Ctrl+T Purge Debug options Import settings from INI file Export settings to INI file Expit	Nessage	
	100% 0 MPH	17:39 06-20-2007

步驟八:依照預設, Syslog 檔案存放位置為

x:\Program Files\Syslogd\Logs\SyslogCatchAll.txt 該文字檔(x 為您的系統磁區)。若不進行變更請直接點選 OK 即可

🛃 Kiwi Syslog Daemon Setup			
	-	Action: Log to file	~
🖃 Rules 🔗	~		
□ 🖃 🗹 Default		Path and file name of log file: <u>Insert AutoSplit value</u>	
Filters		C:\Program Files\Syslogd\Logs\SyslogCatchAll.txt	
📮 Actions			
🗹 Display		Example of actual path and file name:	
Log to file		C:\Program Files\Syslogd\Logs\SyslogCatchAll.txt	
Archiving			
📮 Formatting		Log file format:	
Custom file formats		Kiwi format ISO yyyy-mm-dd (Tab delimited) 🛛 🛛 💌	
Custom DB formats			
DNS Resolution			
DNS Setup			
DNS Caching			
Modifiers			
Scripting			
Display			
Appearance			
E-mail			
📮 Alarms			
Min message count			
Max message count			
Disk space monitor			
	1		
	-	Test Setup	
I SNMP	20		
		Help OK Cancel	Annly

步驟九:若 Syslog Server 所記錄的交換器有事件觸發 Syslog 之發送(例如:網路線之插拔),則此時可清楚再此軟體上看見相關訊息,此即達成所有設定

🐕 Kiwi Sysl	og Daemon	(Version 8.2.8)			
<u>File E</u> dit <u>V</u>	iew <u>H</u> elp				
ə 🗹 📖	🔬 🔯 🛛	Display OO (Defa	ult) 🔽		
Date	Time	Priority	Hostname	Message	^
66-20-2007	17:51:06	Local2.Debug	192.168.1.1	Jan 1 0:28:59 ES-3124 interface: Port 12 link up	
06-20-2007	17:51:03	Local2.Debug	192.168.1.1	Jan 1 0:28:56 ES-3124 interface: Port 19 link down	
06-20-2007	17:51:01	Local2.Debug	192.168.1.1	Jan 1 0:28:55 ES-3124 interface: Port 19 link up	
06-20-2007	17:50:58	Local2.Debug	192.168.1.1	Jan 1 0:28:51 ES-3124 interface: Port 9 link down	
06-20-2007	17:50:56	Local2.Debug	192.168.1.1	Jan 1 0:28:50 ES-3124 interface: Port 9 link up	
06-20-2007	17:50:51	Local2.Debug	192.168.1.1	Jan 1 0:28:44 ES-3124 interface: Port 18 link down	
06-20-2007	17:50:50	Local2.Debug	192.168.1.1	Jan 1 0:28:43 ES-3124 interface: Port 18 link up	
06-20-2007	17:50:47	Local2.Debug	192.168.1.1	Jan 1 0:28:40 ES-3124 interface: Port 2 link down	
06-20-2007	17:50:46	Local2.Debug	192.168.1.1	Jan 1 0:28:39 ES-3124 interface: Port 2 link up	
06-20-2007	17:50:44	Local2.Debug	192.168.1.1	Jan 1 0:28:37 ES-3124 interface: Port 8 link down	
					~
				100% 10 MPH 17	51 06-20-2007