



AlienVault Installation Guide and System Checking

Written by Billows



Automated Installation

此版本為 AlienVault 4.1

Start

「Automated Installation」將會安裝 AlienVault Open Source Version · 當安裝 完成後使用者可以自行手動升級成「AlienVault Professional version」。

而 OSSIM 這個安裝方式是以精靈的方式提供安裝指導,開機進入 OSSIM 的選單之後會有三個選項,請選擇第一個「Open Source Siem 4.1 (64 Bit) Automated Install」選項,按下「Enter」進入。





Go Back

Continue

Language Location and Keyboard Configuration

在開始安裝前,先選擇要在安裝的時候所顯示的語言以及系統預設語系,參考 「Figure 2」;接著,選擇你的位置將會用來設定「Time Zone 時區」,以及像是有 助於決定系統的「locale」參數,如果你的所在地沒有在列表中,請選擇 [other], 參考「Figure 3」、「Figure 4」、「Figure 5」、「Figure 6」;最後設定使用哪一種鍵盤 版面配置,參考「Figure 7」。



Screenshot

Figure 2 – 選擇語言





Bill	ows	
— j	竣 盟 科 5	を―

• •0	by AlienVault	
Select your location		
The selected location will be used to s this should be the country where you Select the continent or region to whic Continent or region:		select the system locale. Normally
Africa		
Antarctica		
Asia		
Atlantic Ocean		
Caribbean		
Central America		
Europe		
Indian Ocean		
North America		
Oceania		
South America		
Screenshot	Figure 4	Go Back Continue

• 0	by AlienVault	
Select your location		
The selected location will be used to s this should be the country where you	et your time zone and also for example to h live.	elp select the system locale. Normally
Listed are locations for: Asia. Use the listed.	<go back=""> option to select a different cont</go>	tinent or region if your location is not
Country, territory or area:		
Philippines		
Qatar		
Saudi Arabia		
Singapore		
Sri Lanka		
Svrian Arab Republic		
Taiwan 🕞		
lajikistan		
Thailand		
Timor-Leste		
Turkey		_
Turkmenistan		~
Screenshot	Figure 5	Go Back Continue



Configure locales	by AlienVault
preference from the column.	lefined for the combination of language and country you have selected. You can now select your e locales available for the selected language. The locale that will be used is listed in the second ofault locale settings on:
Botswana	- en BW.UTF-8
Canada	- en CA.UTF-8
Hong Kong	- en HK.UTF-8
India	- en IN
Ireland	- en IE.UTF-8
New Zealand	- en NZ.UTF-8
Nigeria	- en NG
Philippines	- en PH.UTF-8
Singapore	- en SG.UTF-8
South Africa	- en ZA.UTF-8
United Kingdom	- en GB.UTF-8
United States	- en US.UTF-8
Zimbabwe	- en ZW.UTF-8
	- en_ZW.UTF-8

Configure the keyboard	by Alien	n /ault	
Keymap to use:			
American English 🛛 📡			~
Belarusian			
Belgian			
Brazilian (ABNT2 layout)			
Brazilian (EUA layout)			
British English			
Bulgarian			
Bulgarian (phonetic layout)			
Canadian French			
Canadian Multilingual			
Croatian			
Czech			
Danish			
Dutch			
Datan			



Network configuration

這個是設定你的網路介面卡,填入可以上網的 IP address 讓這安裝的過程中可以透過網路抓取套件並安裝,輸入 IP address 然後選擇 [Continue]。

• •0	SIM by AlienVault	
Configure the network	by Aller Vault	
to use here, consult your network adm	uter and consists of four numbers separa inistrator.	ated by periods. If you don't know what
IP address:		
Screenshot	Figure 8	Go Back Continue

NetMask 是用來決定哪些機器是位於你的區域網路中,如果不確定,就使用 預設值 255.255.255.0;輸入這個 IP address 的網路遮罩後,選擇 [Continue]。

¢C	by AlienVault	
Configure the network		
The netmask is used to determine w do not know the value. The netmask <i>Netmask:</i>	nich machines are local to your netw should be entered as four number:	work. Consult your network administrator if you s separated by periods.
255.255.255.0		
	Figure 9	
Screenshot		Go Back Continue



這設定是填入你網路卡 IP address 預設閘道路由器的 IP address · 可參考 「Figure 10」。; 接著是 Name Server 的設定是用來在網路上查詢主機名稱的 · 也 就是所謂的 DNS(Domain Name Server) · 如果不確定 · 請使用預設值 · 可參考「Figure 11」。

4 6 (DVIM		
· · · · · ·			
	by AlienVault		
Configure the network			
The gateway is an IP address (for	ur numbers separated by periods) that indicates the	gataway router, also l	nown as
the default router. All traffic that	goes outside your LAN (for instance, to the Internet e no router; in that case, you can leave this blank. I) is sent through this r	router. In
answer to this question, consult y		i you don't know the p	roper
Gateway:			
192.168.61.1			
	Figure 10		
	rigure 10		
Screenshot		Go Back	Continue
	DVIM		
	by AlienVault		
	by Aler Valie		
onfigure the network			
	k up host names on the network. Please enter the		
	by spaces. Do not use commas. The first name sen any name server, just leave this field blank.	ver in the list will be the	e first to be
Name server addresses:			
.92.168.61.1			
	Figure 11		
Screenshot		Go Back	Continue



Root password configuration

OSSIM 會要求你設定 root 的密碼,這個密碼是管理整個 OSSIM 伺服器的密碼,與實際上使用 OSSIM 管理介面時使用的密碼並不相同。

填入兩次相同的密碼之後,再按 [Continue]。

	lienVault	
Dy A Set up users and passwords	lienvauit	
You need to set a password for 'root', the syster access can have disastrous results, so you shou should not be a word found in dictionaries, or a	uld take care to choose a root	password that is not easy to guess. It
A good password will contain a mixture of letters	, numbers and punctuation ar	nd should be changed at regular intervals.
The root user should not have an empty passwo system's initial user account will be given the po		
Note that you will not be able to see the passwo <i>Root password:</i>	rd as you type it.	
•••••		
Please enter the same root password again to v <i>Re-enter password to verify:</i>	erify that you have typed it co	rrectly.
••••••		
Screenshot	Figure 12	Go Back Continue

Disk Partitioning – Use in Guide Mode

OSSIM 會要求配置硬碟分割,我們建議使用「LVM」的方式來,原因是 LVM 可以彈性的對 Partition 做管理。你可以把不同的實體 Partition,組成一個大的邏 輯硬碟。這個邏輯硬碟,可以隨時動態的加入或移除 Partition,所以邏輯硬碟,是 可以你想要變大就變大,想要變小就變小,彈性很大。

因此我們必須選擇第二個選項「Guided – use entire disk and set up LVM」·然 後選擇 [Continue] · 參考「Figure 13」;如果你這台機器有多個磁碟 · 請選擇要安 裝 AlienVault 的那顆磁碟 · 再按 [Continue] · 參考「Figure 14」;最後 · 就是確認 你是否要這樣切割磁區 · 若是確定就選擇「Yes」· 再按 [Continue] · 參考「Figure 15」、「Figure 16」



tire disk, you will next be asked which	disk should be	Go Back	
oted LVM		Go Back	
oted LVM		Go Back	
Figure 13		Go Back	
Figure 13		Go Back	
Figure 13		Go Back	
Figure 13		Go Back	
Figure 13		Go Back	
Figure 13		Go Back	
Figure 13		Go Back	
Figure 13		Go Back	_
Figure 13		Go Back	
Figure 13		GOBACK	
			Continue
7 II I I			
y AlienVault			
-			
·····	R		
ill be erased, but not before you nave	confirmed that	at you really v	want to make
ual disk			
	" ill be erased, but not before you have ual disk ual disk	ill be erased, but not before you have confirmed that ual disk ual disk	ill be erased, but not before you have confirmed that you really ual disk ual disk



LVM VG alienva LVM VG alienva	t, LV swap_1 la) tions are going to be formatted: t, LV root as ext3 t, LV swap_1 as swap CSI3 (0,0,0) (sda) as ext2
changes manuall The partition tab	s of the following devices are changed:
artition disks	by AlienVault
Screenshot	Figure 15
O No	
SCSI3 (0,0,0)	es of the following devices are changed: :da) <i>es to disks and configure LVM?</i>
After the Logica	annot be undone. volume Manager is configured, no additional changes to the partitioning scheme of disks containing are allowed during the installation. Please decide if you are satisfied with the current partitioning ontinuing.
	I Volume Manager can be configured, the current partitioning scheme has to be written to disk.
Partition disks	by AlienVault



最後,安裝完後重開機就能看到登入畫面了。



System Update

此版本為 AlienVault 4.1 · 若有升級的需求 · 請在登入系統後輸入下列 Command · (更新需耗費相當長的時間 · 請耐心等待)

alienvault-update



======================================	
== Connect to the AlienVault Web interface opening the following URL: == == https://192.168.61.141/	
You have new mail.	
alienvault:~# alienvault-update Use of uninitialized value \$vpn_ip in substitution (s///) at /usr/share/alienvault-cer figParser.pm line 851. Use of uninitialized value \$tun_iface in substitution (s///) at /usr/share/alienvault- ConfigParser.pm line 852. 2013-10-12 00:28:37 http://data.alienvault.com/RELEASES/alienvault4_update-script Resolving data.alienvault.com 70.38.37.7 Connecting to data.alienvault.com[70.38.37.7]:80 connected. HTTP request sent, awaiting response 200 OK Length: 37113 (36K) [text/plain] Saving to: `/usr/share/ossim-installer/temp/alienvault4_update-script' 100%[======>] 37,113 56.0K/s	-center/lib/AV/ : in 0.6s
2013–10–12 00:28:38 (56.0 KB/s) – `/usr/share/ossim–installer/temp/alienvault4_update- [37113/37113]	∙script' saved
## logging to /tmp/alienvault4_update−script−1381508918.log	Figure 18
-> checkabort_istrial_re_clean + checkabort_istrial_re_clean + echo '## checkabort_istrial_re_clean, code 0' + set +xv	
WARNING: PF_RING version should be >= 5.5.2, but 5.5.0 is loaded. Please, reboot your system (type: alienvault–setup (Maintenance –> Reboot Appliance))	
 You have new mail in ∕var/mail/root a∣ienvault:~#	Figure 19

接著,畫面會顯示你需要重新啟動系統,輸入下列 Command 進行重新開機。

reboot



Self-Check List

自我檢測也就是 System Checking · 主要是檢查你的 AlienVault 系統是不是處於正常的狀態 · 或者是檢查 Sensor 有沒有收到 Log · 檢查 Plugin 檔案有沒有 Configuration 檔案被載入 · 最後就是檢查 OSSIM 有沒有收到 log

Step One

一開始,請到能連上 AlienVault 的機器使用瀏覽器,在網址列輸入「AlienVault's IP address」,在這個例子當中就是 192.168.61.141;若是能連上系統,這就代表系統 在安裝後處於正常的狀態。

輸入機器 IP 位址後,網頁會先跳出一個視窗,這是憑證不被瀏覽器所信任才 跳出的警告視窗,點選 [Continue],參考「Figure 20」。回到網頁後,OSSIM 會需 要你先設定管理者帳號,請輸入 OSSIM 需要的資訊後,

S.			igure 20	再按[Start using AlienVault!] ,
a ya	he certificate for this wel website that is pretendi	ntity of the website "192.168.61.141". bsite is invalid. You might be connecti ng to be "192.168.61.141", which could tion at risk. Would you like to connect Cancel Show Certifica	ng to 1 put 1 to	參考 「Figure 21」。 最後,登入系統,參考 「Figure 22」。
Velcome Congratulations on cl	ILT OSSIM	gure 21		Figure 22
nformation Ne				
lease provide the fo	ollowing information. Don't we	orry, you can always change these lat	ST	User admin
Full Name	support the			Password
User Name	admin	(*) This will be your login to the AlienVault We	b interface	
Password	stronger			
	su onger			Login
Retype Password	stronger			
E-mail	Address for the second			
Company Name	(Hillion)	(*) Optional		
Location	Taiwan Hunan/JJ K. Jiangxi K. M	(*) Optional	 View Map 	
		Naha	Map Satellite	



Step Two

接著,就是要檢查 Log 有沒有進 Sensor 以及 Plugin 有沒有被載入。

我們來檢查你的 Log 是怎麼儲存的, 鍵入

#vim /etc/rsyslog.conf

到設定檔的「First some standard log files. Log by facility」的區塊,檢查一下 你的 Log 是怎麼分類的?儲存在哪裡?,若你有修改此設定檔,記得重起服務。 此例是根據 IP 來分 Log 的。

# # First some standard log fi #	les. Log by facility. Figure 23
<pre>#auth,authpriv.*</pre>	/var/log/auth.log
<pre>#*.*;auth,authpriv.none</pre>	-/var/log/syslog
<pre>\$template DynSyslogFile,"/va</pre>	r/log/rsyslog/%FROMHOST-IP%.log"
<pre>*.*;auth,authpriv.none</pre>	-?DynSyslogFile
<pre>*.*;auth,authpriv.none</pre>	~
#cron.*	/var/log/cron.log
daemon.*	<pre>-/var/log/daemon.log</pre>
kern.*	<pre>-/var/log/kern.log</pre>
lpr.*	<pre>-/var/log/lpr.log</pre>
mail.*	<pre>-/var/log/mail.log</pre>
user.*	-/var/log/user.log

在檢查設定檔後·再來就是檢查資料夾有沒有 Log 進來·如果仍然沒有的話· 請檢查設定檔·鍵入

ls -al /var/log/rsyslog

/檢查資料夾是否有 log 檔

tail -f [Log File Name]

/持續觀察 Log file 是否有資訊進來

drwxr-xr-x	2	root	root	4096	Oct	13	06:25	
drwxr-xr-x	28	root	root	4096	Oct	10	21:24	Figure 24
-rw-r	1	root	adm	257144	Oct	13	10:31	127.0.0.1.log
-rw-r	1	root	adm	2378798	Oct	13	06:25	127.0.0.1.log.1
-rw-r	1	root	adm	100198	Oct	12	06:25	127.0.0.1.log.2.gz
-rw-r	1	root	adm	142367	Oct	11	06:25	127.0.0.1.log.3.gz
-rw-r	1	root	adm	1313	Oct	10	21:25	127.0.0.1.log.4.gz
								127.0.0.1.log.5.gz
-rw-r	1	root	adm	8597	Oct	13	10:09	192.168.61.1.log
-rw-r	1	root	adm	31663	Oct	13	06:25	192.168.61.1.log.1
-rw-r	1	root	adm	4144	Oct	12	06:25	192.168.61.1.log.2.gz
-rw-r	1	root	adm	1186	Oct	11	06:25	192.168.61.1.log.3.gz
-rw-r	1	root	adm	628	Oct	10	21:24	192.168.61.1.log.4.gz
-rw-r	1	root	adm	2168	Oct	13	10:01	192.168.61.136.log
-rw-r	1	root	adm	20901	Oct	13	06:25	192.168.61.136.log.1
-rw-r	1	root	adm	2186	Oct	12	06:25	192.168.61.136.log.2.gz



檢查 Log 有沒有進 sensor 後,再來就是檢查你的 Plugin 有沒有被載入到設定 檔,你可以到 /etc/ossim/agent/config.cfg 裡面檢查,鍵入

vim /etc/ossim/agent/config.cfg



接下來,就是檢查 plugin 是否有讀到 log,拿 ssh 這個 plugin 來當例子,你要 先到這個 plugin 的檔案檢查兩個項目:1. 給 plugin 的 Source Log 路徑是否正確, 參考「Figure 26」 2. 這個 plugin 的正規表示法有沒有寫錯,參考「Figure 27」。





最後,檢查/var/ossim/logs 有沒有收到 log,在這個路徑底下存放的方式是以 「年」→「月」→「日」→「時」(以 UTC 表示)→「IP」→ 這個 IP 所有的 logs。

```
billows-avt:/var/ossim/logs/2013/10/13/01/192.168.61.134# ls
2013-10-13T01-02-48.820837Z.log count.total userdata.stats
2013-10-13T01-02-48.820837Z.log.count data.stats
2013-10-13T01-02-48.820837Z.log.sig index.inx
billows-avt:/var/ossim/logs/2013/10/13/01/192.168.61.134#
```

Step Three

此步驟主要目的是可以在偵測錯誤使用的一項工具·他可以觀測一些 log 看不 到的訊息。

- 1. 首先 · [Agent] 端進入 Debug Mode:
 - 用途:已經將 plugin 寫好並且已經將 sql 倒入系統,但還是不會 work 的情況下

用法:

//此指令可以將 watchdog 的 process,會將 shutdown 的 service 啟動

#/etc/init.d/monit stop

#/etc/init.d/ossim-agent stop

#/ossim-agent -vvv //進入 agent debug mode

- 2. 而進入 [Server] 端進入 Debug Mode:
 - 用途: 觀看其 Server 端是否有其他的 Error,在此處我們分成 4.3 前、後的版本來區分。

用法(4.3 版以前):

#/etc/init.d/monit stop

#/etc/init.d/ossim-server stop

#ossim-server -D 6 //進入 server debug mode



用法(4.3 版以後):

#start debug

#killall -47 ossim-server

#stop debug mode(method)

Method1 : killall -48 ossim-server

Method2 : /etc/init.d/ossim-server restart

[Log File] :

#/var/log/alienvault/idm/server.log

以上 Debug 完成後,記得將 Service 重新啟動

- 3. 透過自己的 Log 測試有沒有 Work · 千萬不要用「echo」的方式倒出 Log · 因 為沒有換行符號會出現問題 · 所以以下為解決方式:
 - a. 將 Log 檔先存入另一個檔案,例如:/root/test_log
 - b. 利用 cat 將 Log 倒入 source log
 - c. #/root/test_log >> /var/log/syslog
- 4. ossim-server restart 後先用

#tail -f /var/log/ossim/server.log

原因:資料量大的時候有時候他還沒結束你去 cat 他會無法正常運作

然後要看到類似以下畫面才可以繼續使用↓↓↓↓

₽ 192.168.61.135 [88x20]	
連線(C) 編輯(E) 檢視(Y) 視窗(W) 選項(O) 說明(H)	
alienvault-forward.log monit.log.5.gz server.log.external	~
alienvault-forward.log.1.gz nessus_cron.log update_db.log	
alienvault-forward.log.2.gz nessus_cron.log.1.gz update_db.log.1.gz	
alienvault-forward.log.3.gz nessus_cron.log.2.gz update_db.log.2.gz	
alienvault:/var/log/ossim# tail -f server.log	
2013-09-15 09:50:59 OSSIM-Message: Events in DB: 6122; Discarded events: 0	
2013-09-15 09:51:09 OSSIM-Message: Events in DB: 6124; Discarded events: 0	
2013-09-15 09:51:19 OSSIM-Message: Events in DB: 6124; Discarded events: 0	
2013-09-15 09:51:29 OSSIM-Message: Events in DB: 6124; Discarded events: 0	
2013-09-15 09:51:39 OSSIM-Message: Events in DB: 6124; Discarded events: 0	
2013-09-15 09:51:49 OSSIM-Message: Events in DB: 6124; Discarded events: 0	
2013-09-15 09:51:59 OSSIM-Message: Events in DB: 6131; Discarded events: 0	
2013-09-15 09:52:09 OSSIM-Message: Events in DB: 6140; Discarded events: 0	
2013-09-15 09:52:19 OSSIM-Message: Events in DB: 6140; Discarded events: O	
2013-09-15 09:52:29 OSSIM-Message: Events in DB: 6143; Discarded events: O	