AlienVault Installation Guide

AlienVault LC - 1901 S Bascom Avenue Suite 220 Campbell, CA, 95008 T +1 408 465-9989 info@AlienVault.com wwww.alienvault.com

Juan Manuel Lorenzo (jmlorenzo@alienvault.com)

Version 1.5

Table of Contents

Introduction 1
About this Installation Guide 1
AlienVault Professional SIEM 2
What is AlienVault Professional SIEM? 2
Basic Operation 3
Components 4
Detector 4
Collector 5
SIEM 5
Logger 5
Web interface 5
Before installing AlienVault 6
Installation Profiles 6
Sensor 6
Server 7
Framework 7
Database 7
All-in-one 7
Overview of the AlienVault installation procedure 8
Automated Installation 8
Custom Installation 8
What you will need 9
Professional Key 9
Role of the installed system 9
Network configuration for the Management Network card 9
Requirements 10
Hardware requirements 10
Network requirements 10
Obtaining AlienVault Installation Media 11
Downloading the installer from AlienVault Website 11
Creating a boot CD 11
Booting the installer 11

Automated Installation 12

Network configuration 12

Disk Partitioning 15

Set up users and passwords 16

Update the installation 17

Custom Installation 18

Selecting Localization Options 19

Profiles configuration 21

Network configuration 22

Time zone configuration 25

Disk Partitioning 26

Professional Key 29

AlienVault Configuration 30

Postfix configuration 31

AlienVault Plugins configuration 32

Custom installation - Server 34

Custom installation - Sensor 35

Custom installation - Framework 37

Custom installation - Database 38

Next Steps 39

How to administrate AlienVault Professional SIEM 39

Web Management interface 39

SSH 39

Passwords 39

Configuration 40

Basic System Configuration 40

Changing the keyboard layout 40

Setting the Current System Date and Time 40

Set the date and time via NTP 40

Changing the time zone 40

AlienVault Basic Configuration 41

Enable / Disable Plugins 41

Configure Plugins 41

Configure listening interfaces 41

Change the System Profile 42

VPN Configuration 43

Network Configuration 44

Setting the hostname 44

Setting up DNS 44

Setting up the IP address 44
Setting up a network card in promiscuous mode 44
Configure AlienVault local firewall 44
Setting the default Gateway 45
Network cards information 45
Network card statistics 45
Change the management IP address of the AlienVault Box 45

System Management 46

Upgrade the AlienVault System 46

Rsyslog Configuration 46

Rsyslog filtering 47

Log file rotation 48

Cron job management 50

Monit 50

Further reading and Information 51

Upgrade AlienVault Open Source SIEM to AlienVault Professional SIEM 51

Reporting Bugs 52

AlienVault 52

Website 52

Forums 52

IRC 52

Introduction

About this Installation Guide

This manual contains installation instructions for the AlienVault Professional SIEM 2.3. It also contains pointers for more information on how to start working with AlienVault Professional SIEM once it has been deployed.

Basic configuration and operation guidelines are contained in this document to assist you in implementing and using your AlienVault SIEM.

As the de facto standard in the world today, AlienVault has a large community of users with experience using AlienVault SIEM in virtually any type of application from compliance to operations, government to control systems, finance to manufacturing. This community of active developers and users communicate through the forums found on AlienVault's web site (http://AlienVault.com). We encourage our customers to engage with this rich source of tactical expertise.

Since AlienVault SIEM is a fully unified security management system you will find a great number of tools you are familiar with already integrated into the AlienVault technology you have acquired. These tools are not only manageable through the AlienVault interface they are also tightly integrated with the other functional components of the system. AlienVault will additionally integrate with external security tools of all sorts to allow you to create a unified solution to fit your specific needs.

AlienVault is proud of and stands behind the technology we create. As a company with roots in the Open Source community we understand the necessity for honesty and transparency. This is critically important when it comes to addressing the types of integration SIEM users undertake. The AlienVault team delivers the same level of commitment to its community that has led the technology to be adopted by more than half of all SIEM users worldwide.

If you have any comments or questions about AlienVault and its products please contact us at any time.

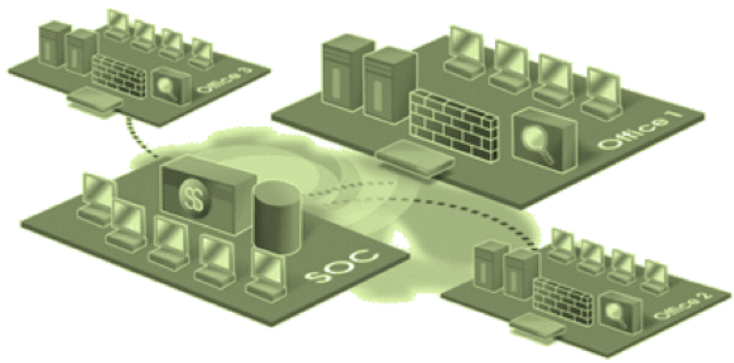
Welcome to the AlienVault community!

AlienVault Professional SIEM

What is AlienVault Professional SIEM?

AlienVault provides a Security and Event Management solution, and a framework that allows tight control over widely distributed enterprise networks from a single location.

This AlienVault professional SIEM is based in OSSIM, created and developed by AlienVault.



AlienVault SIEM Technology offers advanced intelligence, capable of synthesizing the underlying risks associated with complex distributed attacks on extensive networks..

The system considers the context of each threat and the importance of the assets involved, evaluates situational risk, discovers, and distinguishes actual threats from the thousands of false positives that are produced each day in each network.

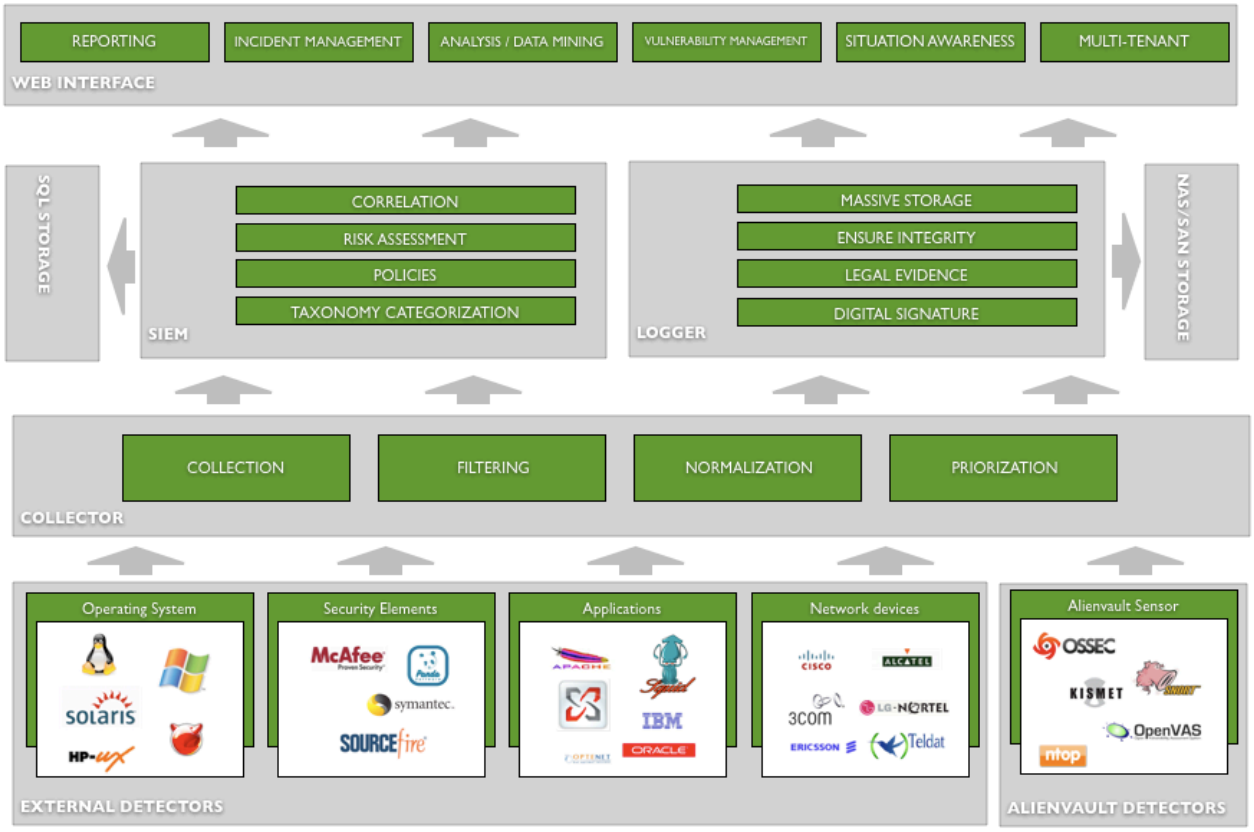
The solution features:

- Low level, real-time detection of known threats and anomalous activity (unknown threats)
- Compliance automation
- Network, host and policy auditing
- Network behavior analysis and situational behavior
- Log management
- Intelligence that enhances the accuracy of threat detection
- Risk oriented security analysis
- Executive and technical reports
- A scalable high performance architecture

Basic Operation

The following processes take place within AlienVault Professional SIEM:

- External applications and devices generate events (**External Detectors**)
- Applications shipped with AlienVault generate events (**AlienVault Detectors**)
- Events are collected and normalized before being sent to a central Server (**Collectors**)
- The AlienVault Server does the Risk Assessment, correlation and storage of the events in an SQL Database (**SIEM**)
- The AlienVault Server stores the events (Digitally signed) in a Massive Storage system, usually NAS or SAN (**Logger**)
- A web interfaces provides a reporting system, metrics, reports, Dashboards, a ticketing system, a vulnerability Management system and real-time information of the network. (**Web interface**)



Components

Detector

Any application or device that generates events within the network that is being monitored will be considered a Detector within the AlienVault deployment.

AlienVault includes a number of detectors using well-known Open Source Tools. From this moment we will use **Sensor** when referring to the detectors included by default when installing AlienVault Professional SIEM.

AlienVault Sensors have been designed for managed security. They feature an arsenal of technology into a single device, and introduce it into each remote network as if it were an “eye” detecting and surveilling remote, unauthorized activity. The combined effect of numerous detection and control points is global visibility, and compliance management.

AlienVault Sensors are installed on each network segment and inspect all traffic, detect attacks through various methods and collect information on attack context without affecting the performance.

These sensors utilize more than 10 expert systems that identify attacks along 5 different axes:

- Intrusion Detection
- Anomaly Detection
- Vulnerability Detection
- Discovery, Learning and Network Profiling systems
- Inventory systems

Detection systems locate in near real time, both known and unknown attacks through learning and anomaly reporting.

Vulnerability detection systems discover and identify latent network threats and can correct them before an attack occurs. This information, stored by the Management Server, is of vital importance when an attack is in progress. Prior knowledge of vulnerabilities in systems is vitally important when assessing the risk associated with an attack, prioritizing, alerting, and launching countermeasures.

The network information gathered by AlienVault probes also provides detailed information in near real time about network usage of each computer, and collects this data for analysis. The system automatically creates a highly detailed usage profile of each element on the network.

Collector

The Collectors gather the events generated by the AlienVault Sensors and any external system. Collectors classify and normalize the events before sending them to SIEM and Logger.

In order to support the maximum possible number of applications and devices, collector use Data Source connectors (also called Collection Plugins). Each DS connectors (Formerly OSSIM Plugins) defines the way events generated by each detector should be collected and normalized.

DS connectors can be configured easily using a simple configuration file and regular expressions to define the format of each type of event.

The Collector component can be deployed as a standalone system or included in the Sensor or SIEM appliance depending on the performance need.

SIEM

The SIEM component provides the system with Security Intelligence and Data Mining capacities, featuring:

- Risk assessment
- Correlation
- Risk metrics
- Vulnerability scanning
- Data mining for events
- Real-time monitoring

AlienVault SIEM uses a SQL database and stores information normalized allowing strong analysis and data mining capabilities.

AlienVault Professional SIEM is tuned for high performance and scalability of millions events per day.

Logger

PRO ONLY

The Logger component stores events in raw format in the file system. Events are digitally signed and stored en masse ensuring their admissibility as evidence in a court of law.

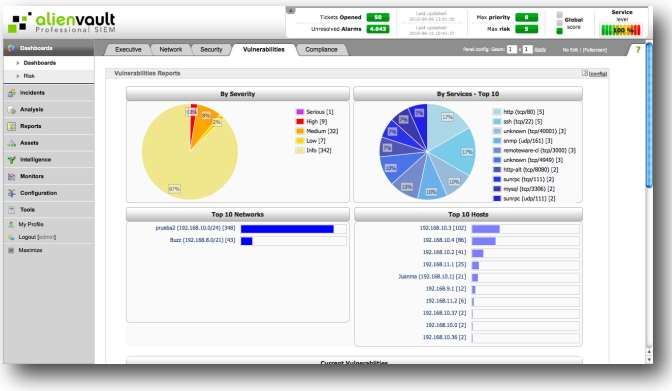
The logger component allows storage of an unlimited number of events with forensic purpose. For this purpose the logger is usually configured so that events are stored in a NAS / SAN network storage system.

Web interface

The Web interface provides access to all information collected and generated by the system as well as access to the configuration parameters.

The following tasks can be performed using the Web interface:

- Configuration changes
- Access to Dashboards and Metrics
- Multi-tenant and Multi-user management
- Access to Real-time information
- Reports generation
- Ticketing system
- Vulnerability Management
- Network Flows Management
- Responses configuration



Before installing AlienVault

Installation Profiles

Depending on the role of the new host within the AlienVault deployment it is possible to configure the profile in use. This can be configured during the installation process or after installation. By default the Automated Installation will enable all profiles in the same box.

Sensor

The Sensor Profile will enable both the AlienVault Detectors and the Collector.

The following detectors are enabled by default:

- Snort (Network Intrusion Detection System)
- Ntop (Network and usage Monitor)
- OpenVAS (Vulnerability Scanning)
- P0f (Passive operative system detection)
- Pads (Passive Asset Detection System)
- Arpwatch (Ethernet/Ip address parings monitor)
- OSSEC (Host Intrusion Detection System)
- Osiris (Host integrity Monitoring)
- Nagios (Availability Monitoring)
- OCS (Inventory)

Once the sensor profile has been enabled you can disable the detectors so that only the collection functionality remains enabled.

To get benefit of the detection capabilities of those tools we will have to configure networking in the OSSIM Sensor so that:

- It has access to the network that is being monitored:
  - Vulnerability Scanning, Availability monitoring, WMI Agent-less collection, Syslog collection

- It receives all the network traffic. A port mirroring, port span needs to be configured in your network devices, or a network tap could be used:
  - Snort, Ntop, Arpwatch, Flows generation, Pads, P0f...

The Sensor profile configures the system so that it is ready to receive events from remote hosts using the Syslog protocol. Each application or device will have an associated plugin (DS connector) that defines how to collect the events from the application or device as well as how events should be normalized before sending them to the central OSSIM Server.

An AlienVault deployment can have as many sensors as required, basically depending on the networks that are being monitored and on the geographical distribution of the organization that will be monitored using AlienVault. Usually a sensor per network will be required but installing more network cards in a single box and configuring network routing and port mirroring could reduce the number of required sensors monitoring more networks from a single Sensor.

Server

This installation profiles combines the SIEM and Logger component. The Sensors will connect to the OSSIM Server to send the normalized events.

Simple deployments will include a single Server in the deployment. More complex deployments could have more than one Server with different roles or in case it is required to deploy the OSSIM Server in high availability.

Framework

The Framework profile will install and configure the Web Management interface component. A single Web Management interface will be deployed on every AlienVault installation. More complex deployments with multiple AlienVault Servers may have more than one box with the Framework profile enabled.

The Framework is the installation profile that will use the lowest amount of memory and CPU. For this reason, the Framework is usually installed with the Server profile.

Database

The Database profile will enable a MySQL database to store configuration and events (If the SIEM functionality is in use). At least one Database is required in each deployment. Even if only the SIEM profile is enabled a database will be required to store the inventory information and the configuration parameters.

All-in-one

The All-in-one profile will enable all profiles in a single box. This is the default installation profile and it will be enabled if the user does an automated installation.

Overview of the AlienVault installation procedure

Here's a road map for the steps you will take during the installation process:

Automated Installation

1. Boot the installation system
2. Configure networking
3. Create and mount the partitions on which AlienVault will be installed
4. Watch the automatic download/install/setup/update of the base system.
5. Set up users and passwords
6. Load the newly installed system for the first time

Custom Installation

1. Boot the installation system
2. Select the installation language
3. Configure keyboard
4. Configure location
5. Select the installation AlienVault profiles for this installation
6. Configure networking
7. Create and mount the partitions on which AlienVault will be installed
8. Enter the professional license
9. Watch the automatic download/install/setup/update of the base system.
10. Set up users and passwords
11. Configure AlienVault components
12. Load the newly installed system for the first time

What you will need

Professional Key

You will need an AlienVault Professional license in order to install AlienVault Professional SIEM. Please note that your license is limited in the number of hosts in which it can be used. Misuse of that license may cause its cancellation. If you can not find your Professional Key please contact AlienVault Support.

Role of the installed system

Before installing you will need to know the role of this host within the AlienVault deployment. Please refer to the Installation Profiles section to get more information on AlienVault Profiles.

Network configuration for the Management Network card

During the installation process you will need internet connection from one of the network cards installed in the system. You will need an static IP address to be used during the installation process. This IP address can be changed once the system has been installed.

Installation or Management of the AlienVault Professional SIEM should never be done using an address assigned by your DHCP servers.

Requirements

Hardware requirements

The AlienVault hardware requirements will basically depend on the number of events per second and the throughput of the network that you want to secure.

As a minimum requirement is always advisable to have at least 4GB of ram. You may have to increase the available RAM memory based on the network throughput, the number of events that the AlienVault server is processing and the amount of data that needs to be stored in the database. In order to achieve maximum performance, it is essential to use only those applications and components that will be useful to you in each case.

The AlienVault Professional version will only run on 64 bit processors, so you should always try to choose 64-Bits architecture when buying new hardware. Most components of AlienVault support multithreading, so those using 64-Bits processors will also obtain a great improvement in performance.

When considering network cards, you should try to choose those supported by the e1000 driver. The Open Source development model of this driver ensures good compatibility of these cards with Debian GNU/Linux.

The worst network cards in your AlienVault box (Maybe the On board network cards) should be used to collect events from other devices or as the management interface.

Network requirements

In order to deploy AlienVault Detectors correctly you need to have a great knowledge of your network devices. You will have to configure port mirroring or use a network tap in those network devices that do not support port mirroring. To configure the port mirroring correctly you have to keep in mind avoiding these two situations:

- **Duplicated network traffic** : This happens when you are forwarding the same network traffic more than once in different network devices.
- **Encrypted network traffic** : In some cases it has no sense configuring a port mirroring in those devices that only show encrypted traffic (VPN, SSH…), as this traffic can not be easily analyzed by some applications.

Apart from the port mirroring, you need to have IP addresses for each AlienVault box. Those AlienVault boxes running a Sensor profile may require more than one network card as the Sensor will be require an IP address on each monitored network (Availability Monitoring, Vulnerability Scanning, Log collection, WMI...)

As an example, OpenVAS (Vulnerability Scanning) will have to be able to reach the target networks when the scan happens. When using OpenVAS, Nagios or Nmap you also have to make sure that your firewalls are configured correctly allowing access from your Sensors to the target networks or hosts.

As the events have to be normalized before being processed by the AlienVault Server, the AlienVault Sensor will require access to the DNS in your local network.

Obtaining AlienVault Installation Media

Downloading the installer from AlienVault Website

AlienVault is a constantly evolving product. For this reason you have to make sure you are using the latest version of the AlienVault installer. Newest versions are always available on the Project website http://www.AlienVault.com

You will need to download the 64 Bit version. The installer of the AlienVault Professional SIEM will be the same than the AlienVault Open Source SIEM.

If a professional key is used during the installation process, the installer will automatically upgrade your installation to the AlienVault Professional version

Creating a boot CD

Most CD recorders sold for Windows and Macintosh systems come with software that can burn ISO images to blank media. If yours does not, there are various no-cost applications that can do this for you:

- Windows 95 / 98 / Me / 2000 / XP / Server 2003 / Vista : http://infrarecorder.org
- Mac OS X: Disk Utility (Applications -> Utilities -> Disk Utility)
- Linux: k3b, Brasero

Booting the installer

Simply configure your system for booting off a CD, insert your burned CD, reboot, and proceed to the next chapter.

Note that certain CD drives may require special drivers, and thus be inaccessible in the early installation stages.

If you can not boot from your CD access your BIOS setup menus.

Automated Installation

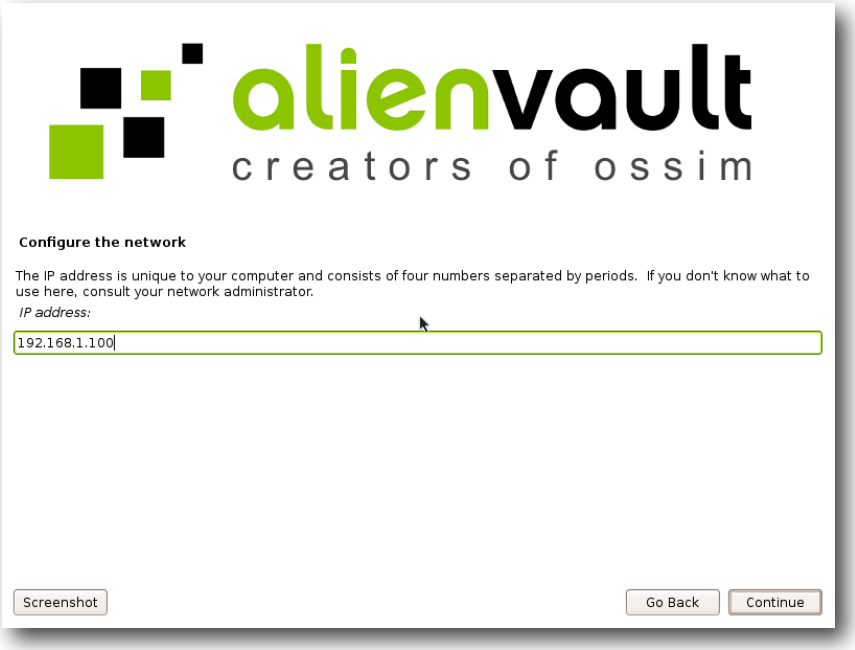
The automated installation will install AlienVault Open Source Version with the all-in-one profile enabled. Once installation is completed the user will upgrade manually to get the benefits of the AlienVault Professional version.

The installation is carried out with almost no user intervention. The automated installation will configure the US keymap and all texts will be in english.

Network configuration

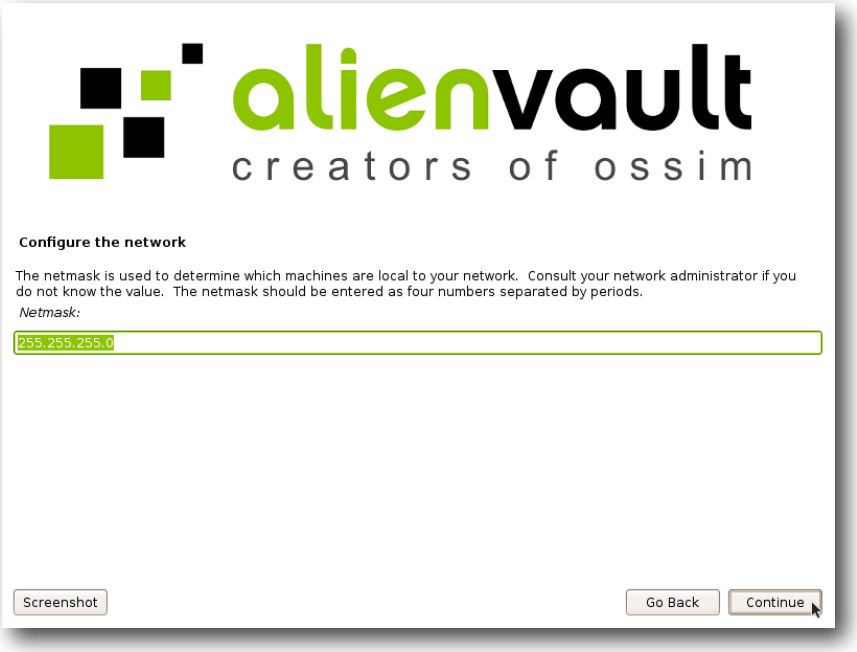
At this point you will have to configure your management network card. You should use an IP address with internet access during the installation process. This IP address will be used in the management interface.

Enter the IP address and select Continue.



The net mask to use with your network.

Enter the net mask and select Continue. If unsure leave the default 255.255.255.0



The IP address of the default gateway system you should route to, if your network has a gateway.

Enter the IP address of the default gateway and select Continue.

The system on your network that you should use as a DNS (Domain Name Service) server. If you have a local name server in your network it should be the first one in this configuration. You can enter as many name servers as you want.

Enter the IP addresses of the DNS (Separated by spaces) and select Continue.

Disk Partitioning

Now it is time for partitioning. Notice that this will delete any data stored in your hard disk.

Select “Guided: Use entire disk**”** and click on Continue.

If the Machine has multiple disks, select the disk in which AlienVault will be installed and click on Continue. In case the machine has a single disk just click on Continue.

Set up users and passwords

After the base system has been installed, the installer will allow you to set up the "root" account. Other user accounts can be created after the installation has been completed.

Any password you create should contain at least 6 characters, and should contain both upper- and lower-case characters, as well as punctuation characters. Take extra care when setting your root password, since it is such a powerful account. Avoid dictionary words or use of any personal information which could be guessed.

Enter the root password and select Continue.

Update the installation

The installation can connect to the AlienVault website to download the latest available version of every software package included in AlienVault Professional SIEM. This process may take up to 1 hour (Depending on your internet connection). Be patient and do not cancel this process.

Select “Yes” and click on Continue.

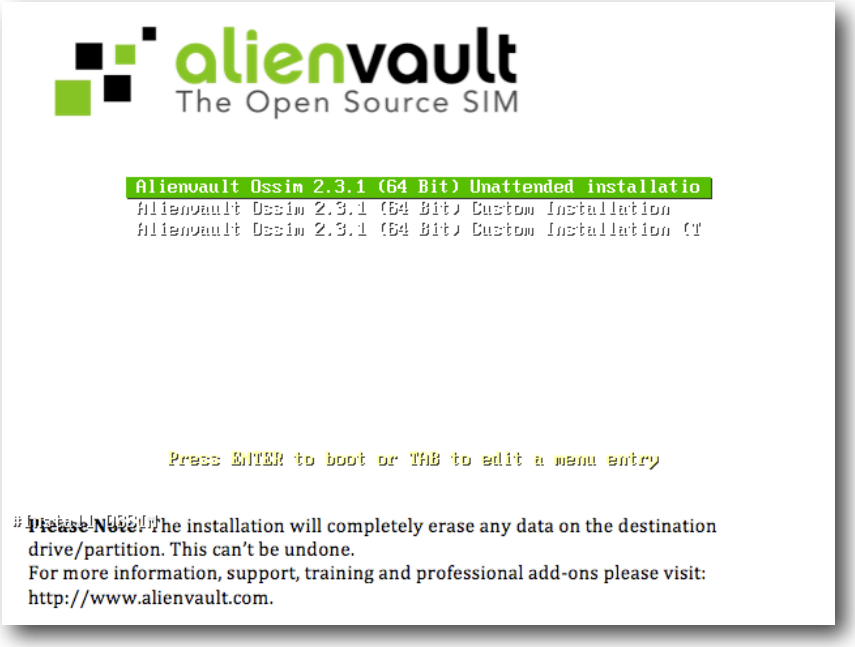
Once the installation has finished the system will be rebooted into your new AlienVault system.

Custom Installation

The custom installations gives user more options during the installation process. This installation mode is recommended in case you want to enable only certain profiles in the new AlienVault host (Sensor only, Server + Database...). The custom installation can be performed in both text mode or graphical mode.

It is also the recommended installation method to perform an installation of the AlienVault Professional SIEM, as this will be installed directly in case of having internet access during the installation process. The Custom Installation will also configured a VPN Network to encrypt communications between all AlienVault Components.

The following screenshots will explain how to do a custom installation selecting all profiles while installing, just after that you will find the specific questions that will appear only when a single profile is selected while installing.



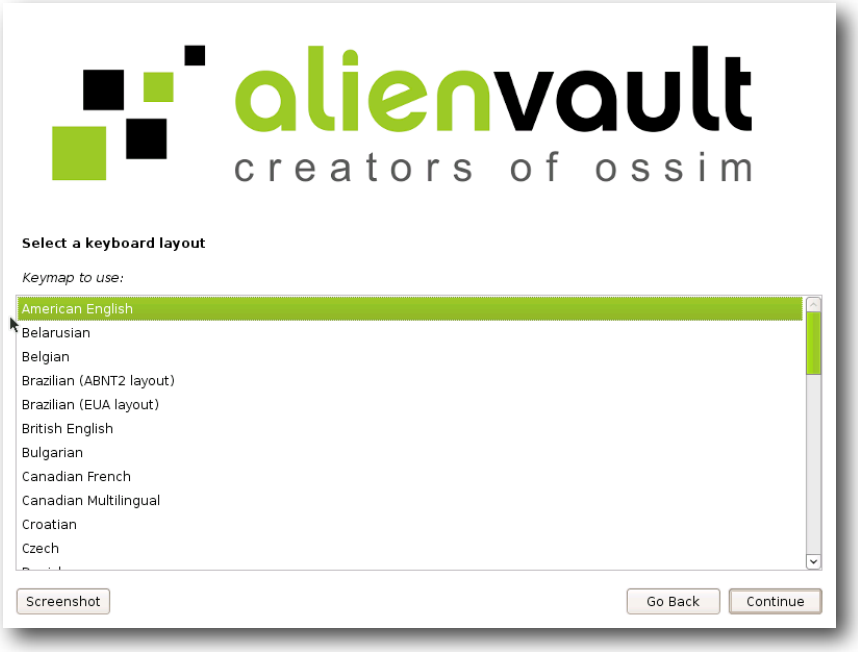
Selecting Localization Options

The first questions you will be asked concern the selection of localization options to be used both for the installation and for the installed system. The localization options consist of language, country and locales.

Choose the language used for the installation process and click on Continue.

Choose your country, territory or area and click on Continue.

Select your keyboard Layout and click on Continue. This can be changed once the system has been installed running 'dpkg-reconfigure console-data'



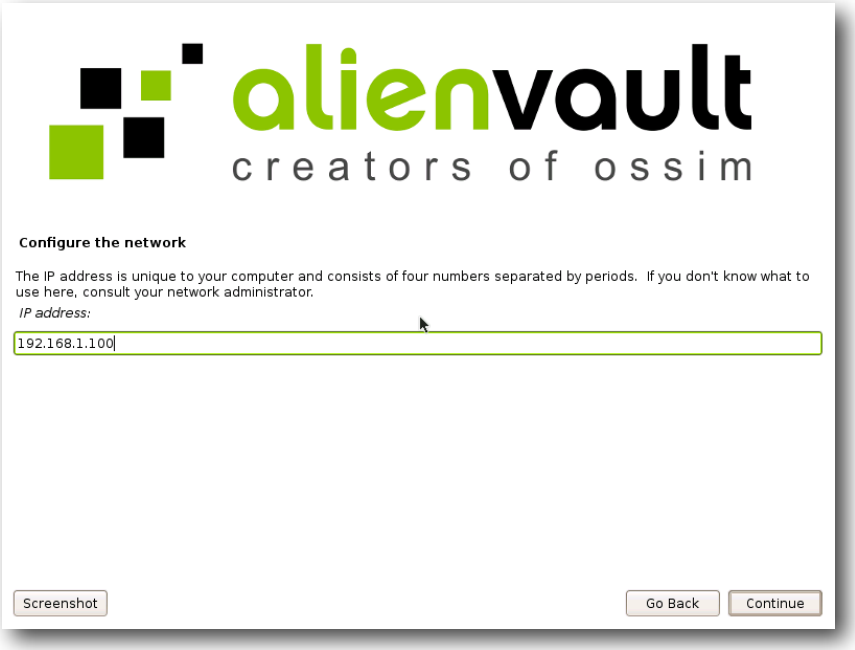
Profiles configuration

Select the profiles that you want to enable in this host. Depending on the chosen profile, you will get different questions during the rest of the installation process.

Network configuration

At this point you will have to configure your management network card. You should use an IP address with internet access during the installation process. This IP address will be used in the management interface.

Enter the IP address and select Continue.



The net mask to use with your network.

Enter the net mask and select Continue

The IP address of the default gateway system you should route to, if your network has a gateway.

Enter the IP address of the default gateway and select Continue.

The system on your network that you should use as a DNS (Domain Name Service) server. If you have a local name server in your network it should be the first one in this configuration. You can enter as many name servers as you want.

Enter the IP addresses of the DNS (Separated by spaces) and select Continue.

The name given to this host (hostname).

Enter the hostname and click on Continue.

Domain name in case there is one being used in your corporation.

Time zone configuration

Select your time zone and click on Continue.

Disk Partitioning

Now it is time for partitioning. Notice that this will delete any data stored in your hard disk.

Select “Guided: Use entire disk**”** and click on Continue.

If the Machine has multiple disks, select the disk in which AlienVault will be installed and click on Continue. In case the machine has a single disk just click on Continue.

Select your partitioning scheme. “All files in our partition” is the recommended option. In case you prefer configuring your own partitioning schema make sure you reserve enough space for the /var/ partition as most of the information in AlienVault will be stored in that folder.

Review the selected partitioning schema, select “Finish partitioning and write changes to disk” and click on Continue.

Select ‘Yes’ and click on ‘Continue’.

Professional Key

Enter the Professional Key and click on Continue. Installing the AlienVault Professional version will require internet connection.

In case you are using an invalid key, you will get the following screen. If you have any problem at this step please contact AlienVault Support team.

AlienVault Configuration

Select the network interfaces in promiscuous mode. All the AlienVault detectors that require collecting all network traffic will be configured to work on these network cards (Snort, Ntop, Fprobe, Pads...).

Select only those interfaces that are connected to a mirrored port, or to a network tap, as these applications will be useless if they are not analyzing all traffic in the network.

Enter your local networks (in CIDR format and separated by comma) that will be monitored by the AlienVault detectors: If unsure leave the default ones.

Postfix configuration

Postfix will be installed to send e-mails from the AlienVault box. You may need to change this configuration depending on how the e-mails can be sent from your network. In this case we are assuming that the AlienVault box can send e-mail and that it has internet connection.

Select 'Internet Site' and click on Continue:

Enter system mail name and click on Continue.

AlienVault Plugins configuration

Now you will be asked to select enabled detector and monitor plugins. When you enable a plugin, the system will be ready to collect events generated by that application or device. Collecting events from certain applications or devices may require extra configuration.

Detector Plugins

They offer events (Snort, Firewalls, Antivirus, Web servers, OS events..). Detector plugins are constantly sending information to the Correlation Engine. Once the event has been generated by the collector, the OSSIM Collector will collect and normalize the event before sending it to the Correlation Engine.

Monitor Plugins

They offer indicators (Ntop, Tcptrack, Nmap, Webs, Compromise & Attack…). Monitor plugins offer information to the correlation engine in request by the OSSIM Server during the correlation process. This type of plugin will not generate events unless they are used in the correlation rules.

Select the detector plugins you want to enable and click on Continue:

Select the monitor plugins you want to enable and click on Continue:

Once the installation has finished the system will be rebooted into your new AlienVault system.

Custom installation - Server

When performing a custom installation selecting one or more profiles (But not all profiles), if the Server profile is selected the installation will show the following additional questions:

Enter the IP address of the AlienVault Box running the Database profile. Click on Continue.

Enter the password of the Database. This password can be found in the parameter 'pass' in the file /etc/ossim/ossim_setup.conf in the box running the Database profile. Click on Continue.

Custom installation - Sensor

When performing a custom installation selecting one or more profiles (But not all profiles), if the Sensor profile is selected the installation will show the following additional questions:

Every Sensor will send normalized events to a Server. Enter the IP address of the AlienVault Server this Sensor will send events to. Click on Continue.

The installer can automatically configure between the Sensor and the Server so communications to encrypt communication between the two components. Select 'Yes' and click on 'Continue':

Enter the password of the root user in the host running the Server profile and click on ‘Continue’:

The installer will show the IP addresses used within the VPN for both the Sensor and the Server. The range of addresses used within the VPN network can be modified in the file /etc/ossim/ossim_setup.conf

Custom installation - Framework

When performing a custom installation selecting one or more profiles (But not all profiles), if the Framework profile is selected the installation will show the following additional questions:

Enter the IP address of the host running the database profile and click on Continue. (You should have installed the Database profile first). Click on Continue.

Enter the password of the root user in the Database and click on 'Continue'. This password can be found in the 'pass' parameter in the file /etc/ossim/ossim_setup.conf in the host running the Database profile.

Custom installation - Database

When performing a custom installation selecting one or more profiles (But not all profiles), if the Database profile is selected the installation will show the following additional questions:

Enter the password to be used for the root user in the Database and click on Continue.

Enter the IP address of the host or hosts running the Server and Framework profiles. The installer will set the permissions in the Database to allow connections from the hosts running those profiles.

Next Steps

How to administrate AlienVault Professional SIEM

Web Management interface

In case you have installed a Server Profile or an all-in-one profile you will be able to connect to the AlienVault Management interface by pointing your favorite internet browser to the IP Address of your AlienVault system.

The default user and password is admin/admin. As soon as you log in you will be asked to change the password for the admin user.

SSH

You can use SSH to access any AlienVault box. SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

An SSH is included by default on every Linux distribution, *BSD and also in Mac OS X. Windows users can use Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) to connect to the AlienVault Box using SSH.

Putty can also be downloaded from the AlienVault Web Management interface in the section *Tools* -> *Downloads*.

Passwords

During the installation process a random password is generated. This password will be used as the root MySQL Password, ossim user within OpenVAS or Nessus and in every software that requires setting a password while it is being installed.

This password is stored in the password field in /etc/ossim/ossim_setup.conf. If you want to change this password, modify this file and then type the following command:

ossim-reconfig

Configuration

Basic System Configuration

Changing the keyboard layout

To change the keyboard layout simply type this command:

dpkg-reconfigure console-data

Setting the Current System Date and Time

To display the current system time, enter the **date** command:

```
AlienVaultsiem:~# date
Mon Jun 02 02:28:22 PDT 2009
```

To set the current system time, use the following form of the date command:

date MMDDhhmm[CC]YY[.ss]

The parts of the command argument have the following meanings:

- MM : A two-digit month, 01-12.
- DD: A two-digit day of month, 01-31.
- hh: A two-digit hour, 00-24.
- mm: A two-digit minute, 00-59.
- CC: An optional two-digit century; for example, 19 or 20.
- YY: A two-digit year; for example, 99 or 00.
- ss: An optional two-digit second, 00-59.

The command displays the time you enter and then sets the system time:

```
AlienVaultsiem:~# date 063010412009
Fri Jun 30 10:41:00 PDT 2009
```

Set the date and time via NTP

To set the date using an NTP server type the following command in the terminal

ntpdate pool.ntp.org

pool.ntp.org can be replaced by the NTP server in your corporation or by any other NTP server in the Internet.

Changing the time zone

To change the timezone just type this command:

dpkg-reconfigure tzdata

AlienVault Basic Configuration

To simplify the configuration of the large number of tools included in AlienVault, the configuration is centralized in a single file. Every time you modify this configuration you should run a command to update the configuration of every application based on the centralized configuration.

The centralized configuration is stored in the following file:

/etc/ossim/ossim_setup.conf

You can edit this file using any text editor (vim, nano, pico…). Inexperienced users should be using the following command to edit this file:

ossim-setup

To apply the centralized configuration on every configuration file you will have to run the following command:

ossim-reconfig

Enable / Disable Plugins

To select the enabled Plugins type the following command:

ossim-setup

Then select the Option 'Change Sensor Settings", and then 'Select detector plugins', you will get a list of enabled and disabled plugins, just click on space when over the name of the plugin to enable or disable that plugin. To apply changes select 'Save & Exit' in the main menu.

Configure Plugins

Once the plugin has been enabled you may need to configure some plugins. Plugin configuration files are stored in the directory /etc/ossim/agent/plugins. There you will find a .cfg file for each plugin.

You may need to edit the **location** parameter to point the AlienVault collector to the file in which the log of that application are being stored. If you modify the configuration file of one of your plugins type the following command to restart the OSSIM Agent (AlienVault Collector):

/etc/init.d/ossim-agent restart

Configure listening interfaces

The ossim-setup script allows configuring the network interfaces in promiscuous mode. All the AlienVault detectors that require analyzing all network traffic will be configured to work on these network cards (Snort, Ntop, Fprobe, Pads...).

Select only those interfaces that are connected to a mirrored port, or to a network tap, as these applications will be useless if they are not analyzing all traffic in the network.

To select the listening interfaces type the following command

ossim-setup

and then choose 'Change Sensor Settings' and then 'Select interfaces in promiscuous mode', then select 'Save & Exit' to apply changes.

Change the System Profile

You can change the profile using the ossim-setup script and selecting the second option (Change Profile Settings)

Based on the selected profile you will have to configure different configuration parameters:

all-in-one

- Choose interfaces: Enter those interfaces (Separated by comma) that are receiving all the traffic of the network.
- Profile Networks: Enter the networks (home networks) in CIDR format, and separated by comma, that the sensor will be able to see in its listening interface (e.g.: 192.168.0.0/24, 10.0.0.0/8)
- OSSIM Sensor Name: Name given to the sensor installed in this machine.
- Choose the plugins: Select those plugins that should be enabled in this Sensor. Monitor plugins are only enabled under request of the OSSIM Server during correlation. Detector plugins are collecting events in real time from files, databases, sockets..

sensor

- OSSIM Sensor Name: Name given to the sensor installed in this machine.
- Choose interfaces: Enter those interfaces (Separated by comma) that are receiving all the traffic of the network.
- Profile Networks: Enter the networks (home networks) in CIDR format, and separated by comma, that the sensor will be able to see in its listening interface (e.g.: 192.168.0.0/24, 10.0.0.0/8)
- OSSIM Server Ip Address: Enter the IP address where the OSSIM server is listening.
- Choose the plugins: Select those plugins that should be enabled in this Sensor. Monitor plugins are only enabled under request of the OSSIM Server during correlation. Detector plugins are collecting events in real time from files, databases, sockets..

server

- OSSIM MySQL Server IP Address: Enter the IP address of the AlienVault box that is running database profile. Make sure that you have the correct perms in the database to be able to connect from a remote machine.
- OSSIM MySQL Server Port: Listening for MySQL. (Default port is 3306)
- OSSIM MySQL Password: Password for root user in MySQL Server.

database

- OSSIM MySQL Password: Password for root user in MySQL Server.

If you only want to reconfigure the profile in use, select the profile in use and you will also be asked to enter the configuration parameters.

To apply changes have to select ‘Apply and save all changes’.

VPN Configuration

PRO ONLY

When performing a custom installation in different the installer will automatically configure a VPN Network to encrypt communication between the different AlienVault components. This feature has been implemented using OpenVPN.

The VPN Server will be configured in the machine running the Server Profile. If we want to include another AlienVault component in the VPN we have to run this command in the machine running the Server Profile. We will use in the following examples the IP address 192.168.0.200, as if it were a box running the Collector profile:

ossim-reconfig --add_vpnnode 192.168.0.200

This command will generate a compressed file containing all required files to configure the VPN network in the AlienVault component we want to put inside the VPN network. This file will be stored in the following directory:

/etc/openvpn/nodes/

Following the previous example, you will find a file like this:

/etc/openvpn/nodes/etc/openvpn/nodes/192.168.0.200.tar.gz

This file should be copied to the remote AlienVault component using SCP:

scp /etc/openvpn/nodes/192.168.0.200.tar.gz root@192.168.0.200:/etc/openvpn/

The file will be copied to the folder /etc/openvpn/. Now we will have to type the following commands in the remote Collector (192.168.0.200):

cd /etc/openvpn/

tar zxvf 192.168.0.200.tar.gz

/etc/init.d/openvpn restart

Network Configuration

Setting the hostname

To change the hostname, simply modify the value of the parameter hostname in the **/etc/ossim/ossim_setup.conf** and run the command:

ossim-reconfig

Setting up DNS

You can add hostname and IP addresses to the file /etc/hosts for static lookups.

To cause your machine to consult with a particular server for name lookups you simply add their addresses to/etc/resolv.conf.

For example a machine which should perform lookups from the DNS server at IP address 192.168.1.200 would have a resolv.conf file looking like this:

```
search my.domain
nameserver 192.168.1.1
```

Setting up the IP address

The IP addresses associated with any network cards you might have are read from the file /etc/network/interfaces. This file has documentation you can read with:

man interfaces

A sample entry for a machine with a static address (eth0) would look like this:

If you make changes to this file you can cause them to take effect by running:

/etc/init.d/networking restart

Setting up a network card in promiscuous mode

If a network is going to be used to analyze all traffic in the network, it should not have an assigned IP address. This will improve considerably the performance of the network card. To to this you will have to include a new entry in the file /etc/network/interfaces :

```
up ifconfig eth0 0.0.0.0 promisc -arp
```

Configure AlienVault local firewall

AlienVault configures a firewall during the installation process. If you want to disable or enable the firewall you can do that by typing:

ossim-setup

Select ‘Change General Settings’ and then select ‘Configure Firewall’. Then, in the main menu select ‘Save & Exit’.

If you want to add exceptions to that firewall write your own rules (iptables firewall rules) in the following file /etc/ossim/firewall_include and execute:

ossim-reconfig

Setting the default Gateway

The default route for a host with a static IP address can be set in/etc/network/interfaces.

If you wish to view your current default route/gateway then you can run:

netstat -nr

To change your default route you must first remove the current one:

/sbin/route del default gw 192.168.0.1

Network cards information

To display or change ethernet card settings execute ethtool followed by the name of the interface.

ethtool eth0

To see which network cards are connected to the Ethernet, and if so, at what speed, use:

mii-tool

Network card statistics

IPTraf is a console-based network statistics utility for Linux. It gathers a variety of figures such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts.

To run IPTraf simply execute the following command:

iptraf

Change the management IP address of the AlienVault Box

In case you change the management IP address of one your AlienVault boxes you have to do the following to make sure that all components using the old IP address are now using the new one.

To do that, once you will have modified /etc/network/interfaces and restarted networking you will need to edit the file /etc/ossim_setup.conf

In this file you could just do a search (Old IP Address) and replace (New IP Address) or take a look to the following parameters:

- admin_ip: Management IP (SSH and Web access)
- db_ip: IP address of the host running the Database Profile
- framework_ip: IP address of the host running the Web Management Interface
- server_ip: IP address of the host running the Server Profile

Once you have set the correct ip addresses you can generate all configuration files by running:

ossim-reconfig

System Management

Upgrade the AlienVault System

Package upgrades are a great success of the APT system. To upgrade an AlienVault Professional SIEM installation you will have to run the following commands:

apt-get update

This command looks for the package lists in the archives found in /etc/apt/sources.list

apt-get dist-upgrade

This command will upgrade all software packages to the newest available version.

ossim-reconfig

This command will generate all configuration files for the different AlienVault components. AlienVault has a complex system of package dependencies and preferences between the different packages as some of them will be available in different software repositories. For this reason the file /etc/apt/sources.list should never be modified. This could break the dependencies tree and make your system unstable.

Whenever a new Debian version is released wait for the instructions of AlienVault to upgrade to the new Debian stable version.

Rsyslog Configuration

Rsyslog is an open source program for forwarding log messages in an IP network for UNIX and Unix-like systems. It implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, flexible configuration options and adds important features such as using TCP for transport.

Rsyslog is the syslog implementation included by default when installing AlienVault Professional SIEM.

Rsyslog configuration files are:

- /etc/rsyslog.conf
- Any file inside the folder /etc/rsyslog.d/

During the installation process Rsyslog will be configured to accept information coming from a remote syslog daemon. Rsyslog will accept connections from any host in the listening port 514.

Rsyslog filtering

Rsyslog can be configured to store incoming events in different files depending on the host, application or device that is generating the events. This can be configured using four different types of “filter conditions”:

- BSD-style blocks
- "traditional" severity and facility based selectors
- property-based filters
- expression-based filters

This means that we can use the same syntax that we used to use in the Ksyslogd (Included in Debian install) and syslog-ng. Rsyslog expression-based filters will simplify a lot the process of filtering events and storing events in different files.

Expression based filters are indicated by the keyword "if" in column 1 of a new line. They have this format:

if expr then action-part-of-selector-line

"If" and "then" are fixed keywords that must be present. "expr" is a (potentially quite complex) expression.

Some examples:

```
if $syslogfacility-text == 'local0' and $msg startswith 'DEVNAME' and ($msg contains 'error1' or
$msg contains 'error0') then /var/log/somelog
```

This following entry will store all events generated in the host 192.168.1.100 containing the word ‘ACCEPT’ in the file /var/log/accept.log.

```
if $source == '192.168.1.100’ and $msg contains ‘ACCEPT’  then /var/log/accept.log
```

We can also forward certain events to a remote Syslog daemon using the following syntax:

```
if $source == '192.168.1.200’ and $msg contains ‘CISCO-PIX’ then
```

Filters are applied from top to bottom so they can match more than one filter. If we want to stop processing certain events we can use the next symbol “~”.

```
if $msg contains ‘error’ then /var/log/error.log
if $msg contains ‘error’ then ~
```

This way, in the previous example, logs containing the word error will be stored at /var/log/error.log, and with the second line we make sure that they will not match any other filtering rule.

Configuring Rsyslog filter may create new log files in your system. Make sure you configure a Log rotate policy for those files or the will grow without control.

Log file rotation

If you install new services or configure log forwarding in rsyslog this will produce log files which grow, and grow, and grow. If left unchecked this can leave your disk with no space available.

The process that is in charge of compressing and rotating these log files is called logrotate and it is executed once per day upon AlienVault installations.

Every day this script runs and examines two things:

- The configuration file /etc/logrotate.conf
- The configuration directory /etc/logrotate.d

The latter is where most of our packages are configured. This directory contains configuration files which other packages have installed.

A typical logrotate configuration file looks like this:

```
/var/log/apache/*.log {
        weekly
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                if [ -f /var/run/apache.pid ]; then
                        /etc/init.d/apache restart > /dev/null
                fi
        endscript
}
```

You can see several important things here. The most obvious is the list of files that will be matched by this configuration file:

```
/var/log/apache/*.log {
...
}
```

After this we have a collection of configuration terms, a different one on each line. In the example above we have:

- weekly
  - The files should be rotated every week. Opposite: daily
- rotate nn
  - We should keep no more than nn files.
- compress
  - Compress older files with gzip. Opposite: nocompress
- delaycompress
  - Don't compress yesterdays files. Opposite: compress
- notifempty
  - Don't do any rotation if the logfile is empty. Opposite: ifempty
- create xx user group
  - If we have to create the new file give it the given mode, owner, and group.
- sharedscripts
  - Run any given prerotate or postrotate script for each logfile individually. Opposite: nosharedscripts.
- postrotate + endscript
  - Anything between these is executed after the rotation process. Opposite : prerotate

If we wish to install a local service which creates a log file we can cause it to be rotated very easily, just by adding a new logrotate configuration file.

Cron job management

Any jobs under the purview of the system administrator should be in /etc, since they are configuration files. If you have a root cron job for daily, weekly, or monthly runs, put them in /etc/cron.{hourly,daily,weekly,monthly}. These are invoked from /etc/crontab, and will run in alphabetic order, which serializes them.

On the other hand, if you have a cron job that (a) needs to run as a special user, or (b) needs to run at a special time or frequency, you can use either /etc/crontab, or, better yet, /etc/cron.d/whatever. These particular files also have an extra field that allows you to stipulate the user account under which the cron job runs.

In either case, you just edit the files and cron will notice them automatically. There is no need to run a special command. For more information see cron(8), crontab(5), and /usr/share/doc/cron/README.Debian.

Monit

Monit is an application designed to monitor and manage your hosts and services, conduct automatic maintenance and repair and execute meaningful causal actions in error situations.

Monit is installed by default in AlienVault Professional SIEM, with a different configuration depending on the enabled installation profile.

The Monit configuration file can be found at:

/etc/monit/monitrc

Monit will be running in background all time so in case you want to stop some services momentarily so may need to stop Monit using the following command:

/etc/init.d/monit stop

To start Monit again use the following command:

/etc/init.d/monit start

Further reading and Information

Upgrade AlienVault Open Source SIEM to AlienVault Professional SIEM

If you have AlienVault Open Source version (64 Bits) installed there is no need to reinstall to upgrade to the professional version. This process will require internet connection. To upgrade your Open Source installation you will need to edit the file / etc/apt/sources.list

In this file you will find some lines that will be used by the system to retrieve software and updates:

```
deb http://data.AlienVault.com/debian/ binary/
deb http://www.ossim.net/download/ debian64/
deb http://data.AlienVault.com/debian_shared/ binary/
deb http://ftp.us.debian.org/debian/ lenny main contrib
deb-src http://ftp.us.debian.org/debian/ lenny main contrib
deb http://security.debian.org/ lenny/updates main contrib
deb-src http://security.debian.org/ lenny/updates main contrib
deb http://volatile.debian.org/debian-volatile lenny/volatile main
deb-src http://volatile.debian.org/debian-volatile lenny/volatile main
```

At the end of this file you include a new line with the following format

deb http://data.AlienVault.com/**YOUR_PROFESSIONAL_KEY**/ binary/

The /etc/apt/sources.list should look like this

```
deb http://data.AlienVault.com/debian/ binary/
deb http://www.ossim.net/download/ debian64/
deb http://data.AlienVault.com/debian_shared/ binary/
deb http://ftp.us.debian.org/debian/ lenny main contrib
deb-src http://ftp.us.debian.org/debian/ lenny main contrib
deb http://security.debian.org/ lenny/updates main contrib
deb-src http://security.debian.org/ lenny/updates main contrib
deb http://volatile.debian.org/debian-volatile lenny/volatile main
deb-src http://volatile.debian.org/debian-volatile lenny/volatile main
deb http://data.AlienVault.com/a12132this2is32not12a32key/ binary
```

Notice that there is an space before binary. Once this file has been edited type the following commands:

apt-get update

apt-get dist-upgrade

ossim-reconfig

Reporting Bugs

Reporting a bug with all required information will reduce the time required by the developer to fix it. When reporting a bug keep this in mind:

- Be precise
- Be clear
- Report every possible bugs, as small bugs may hide bigger bugs
- Read the documentation to make sure it is not the expected behavior
- Read what you wrote

You should always make sure that your are using the latest version available before filling the Bug Report. It will also be very helpful if you were including hardware information and a quick note about how is your deployment: Eg: Server only in one box and three remote Sensors).

Bugs must be filled in, in the following Web Site: https://www.assembla.com/spaces/os-sim/support/tickets

AlienVault

Website

The website http://www.AlienVault.com contains information of AlienVault, the company, as well as information about the AlienVault product, in both Professional and Open Source edition.

Forums

AlienVault forums are the perfect place to exchange experiences with AlienVault user community.

AlienVault forums can be accessed using the following URL: https://www.AlienVault.com/forum/

IRC

The AlienVault IRC channel is a dedicated chatroom ideal for getting real-time help from other users community users. The channel name is #ossim on irc.freenode.net