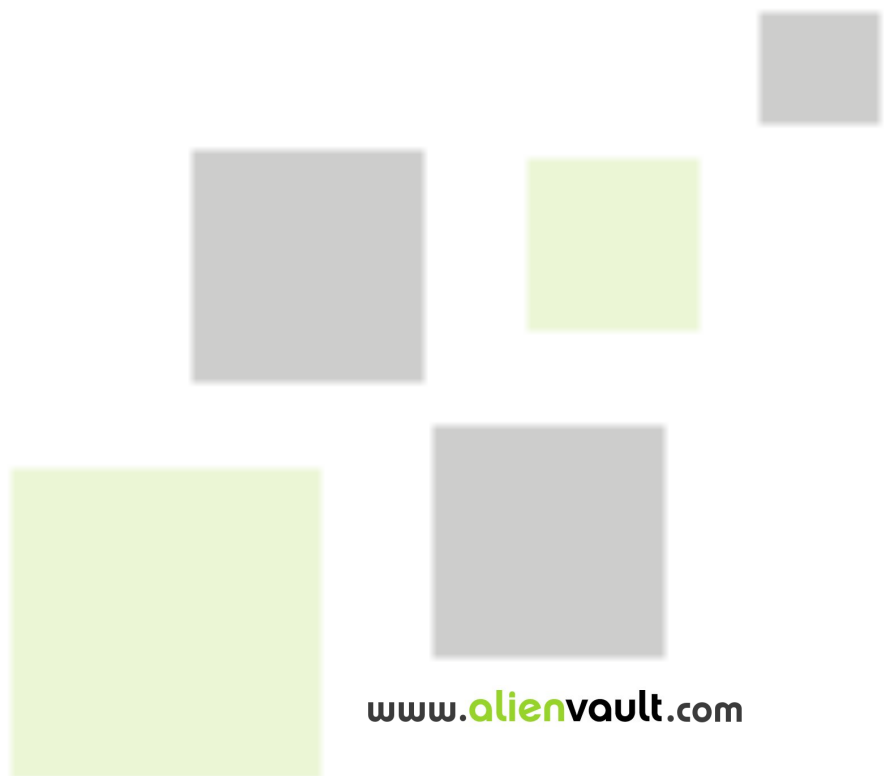


Collecting Windows logs using Snare



1 Introduction

This manual explains how to configure Snare to send Windows logs to AlienVault. A snare agent (installed in Windows machines) sends logs to the AlienVault Sensor which parses and forwards the events to the AlienVault Server (SIEM or Logger).

2 Download required software

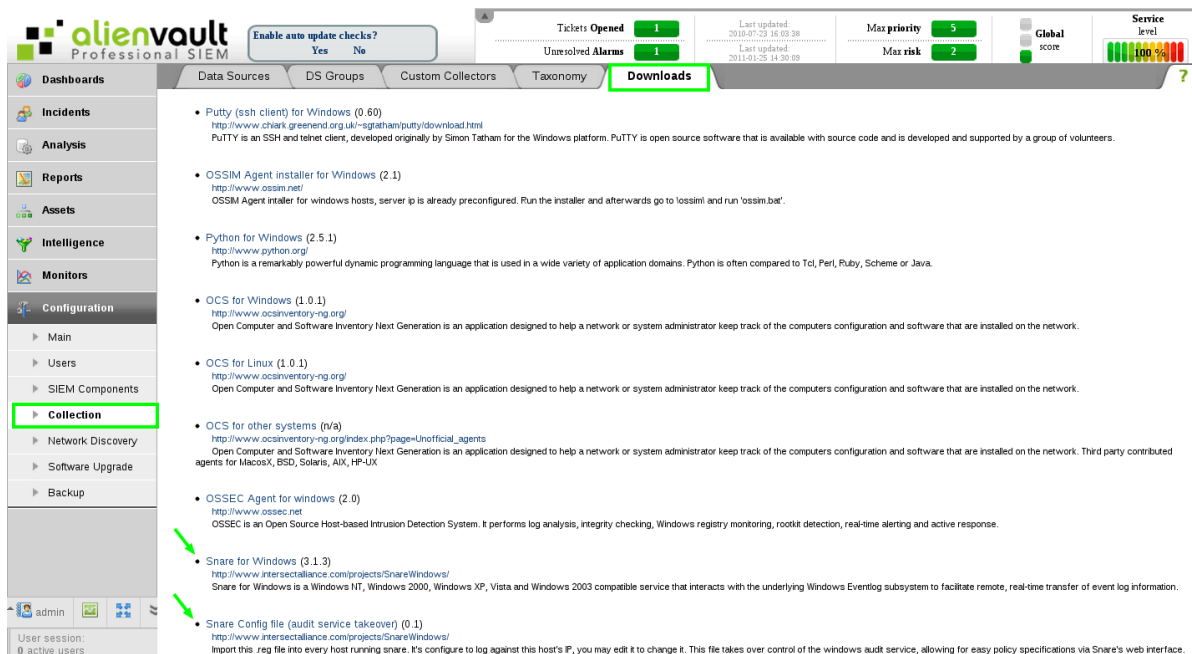
Download the Snare agent from the your AlienVault Web Interface (Version higher than 3.0)

Configuration -> Collection -> Downloads

Or to (Previous versions):

Tools -> Downloads ->

And download the two files shown in the image below

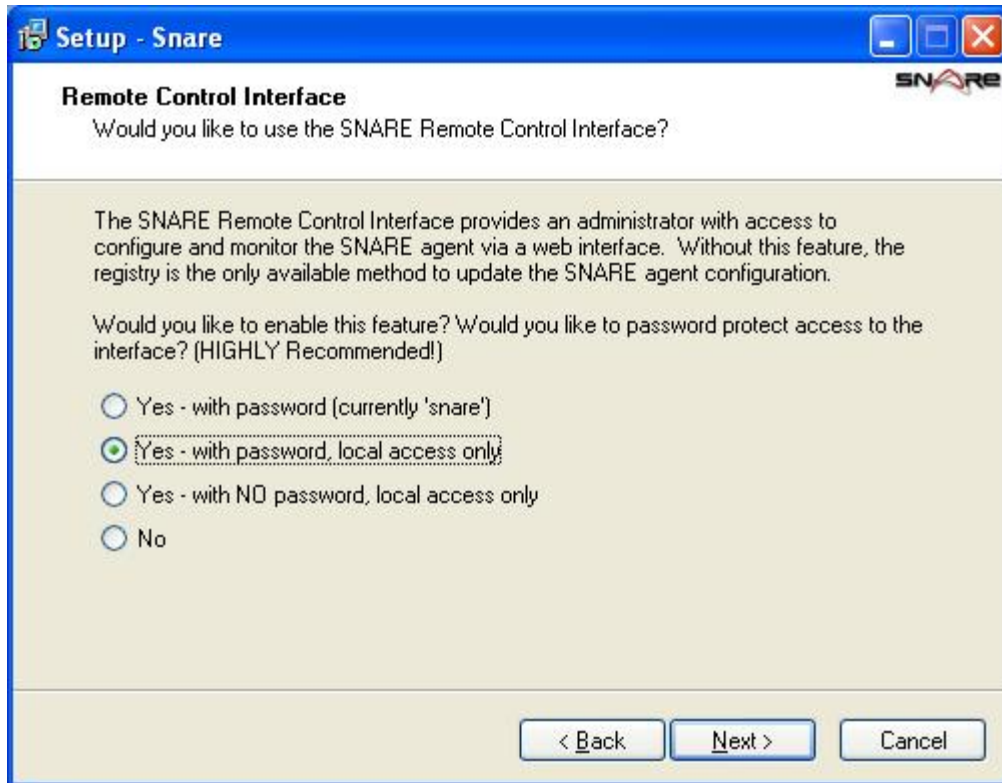


The screenshot shows the AlienVault Professional SIEM interface. The top navigation bar includes 'Downloads' which is highlighted. The left sidebar has 'Collection' highlighted. The main content area lists the following items:

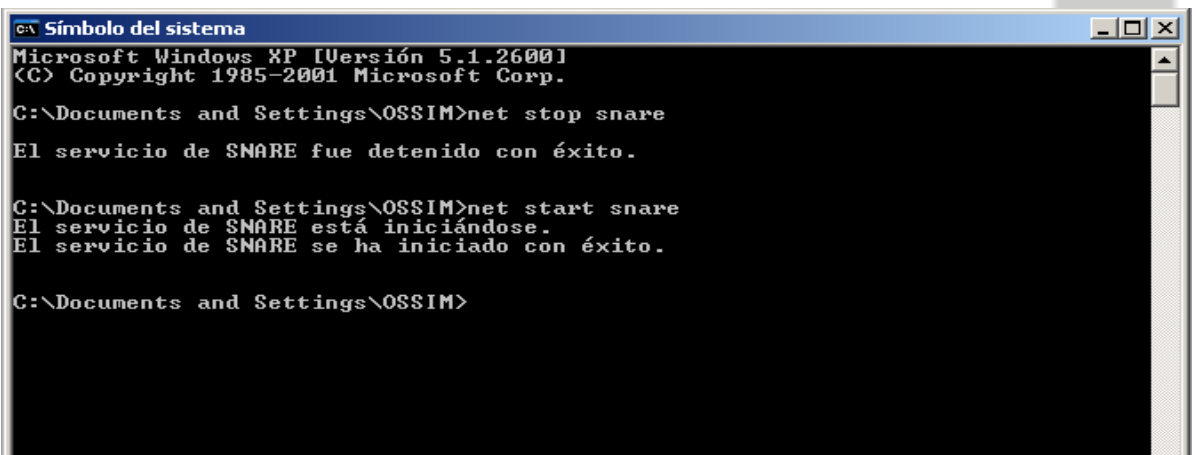
- Putty (ssh client) for Windows (0.60)
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
PUTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PUTTY is open source software that is available with source code and is developed and supported by a group of volunteers.
- OSSIM Agent installer for Windows (2.1)
<http://www.ossim.net/>
OSSIM Agent installer for windows hosts, server ip is already preconfigured. Run the installer and afterwards go to 'ossim!' and run 'ossim.bat'.
- Python for Windows (2.5.1)
<http://www.python.org/>
Python is a remarkably powerful dynamic programming language that is used in a wide variety of application domains. Python is often compared to Tcl, Perl, Ruby, Scheme or Java.
- OCS for Windows (1.0.1)
<http://www.ocsinventory-ng.org/>
Open Computer and Software Inventory Next Generation is an application designed to help a network or system administrator keep track of the computers configuration and software that are installed on the network.
- OCS for Linux (1.0.1)
<http://www.ocsinventory-ng.org/>
Open Computer and Software Inventory Next Generation is an application designed to help a network or system administrator keep track of the computers configuration and software that are installed on the network.
- OCS for other systems (n/a)
http://www.ocsinventory-ng.org/index.php?page=Unofficial_agents
Open Computer and Software Inventory Next Generation is an application designed to help a network or system administrator keep track of the computers configuration and software that are installed on the network. Third party contributed agents for MacOSX, BSD, Solaris, AIX, HP-UX.
- OSSEC Agent for windows (2.0)
<http://www.ossec.net>
OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response.
- Snare for Windows (3.1.3)
<http://www.intersectalliance.com/projects/SnareWindows/>
Snare for Windows is a Windows NT, Windows 2000, Windows XP, Vista and Windows 2003 compatible service that interacts with the underlying Windows Eventlog subsystem to facilitate remote, real-time transfer of event log information.
- Snare Config file (audit service takeover) (0.1)
<http://www.intersectalliance.com/projects/SnareWindows/>
Import this .reg file into every host running snare. It's configure to log against this host's IP, you may edit it to change it. This file takes over control of the windows audit service, allowing for easy policy specifications via Snare's web interface.

3 Installing software in windows

1. Execute the file *SnareSetup-3.1.3-MultiArch.exe* and follow the installer instructions. It is recommended to change the default option of Remote Control Interface to "Yes - with password, local access only". The password will be able to change later.



2. When the installation is completed you should edit *snare_takeover.reg* and check that Destination value is correct (it should be your ossim-server ip).
3. Execute *snare_takeover.reg*.
4. Restart `snare` service:



```
c:\ Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\OSSIM>net stop snare
El servicio de SNARE fue detenido con éxito.

C:\Documents and Settings\OSSIM>net start snare
El servicio de SNARE está iniciándose.
El servicio de SNARE se ha iniciado con éxito.

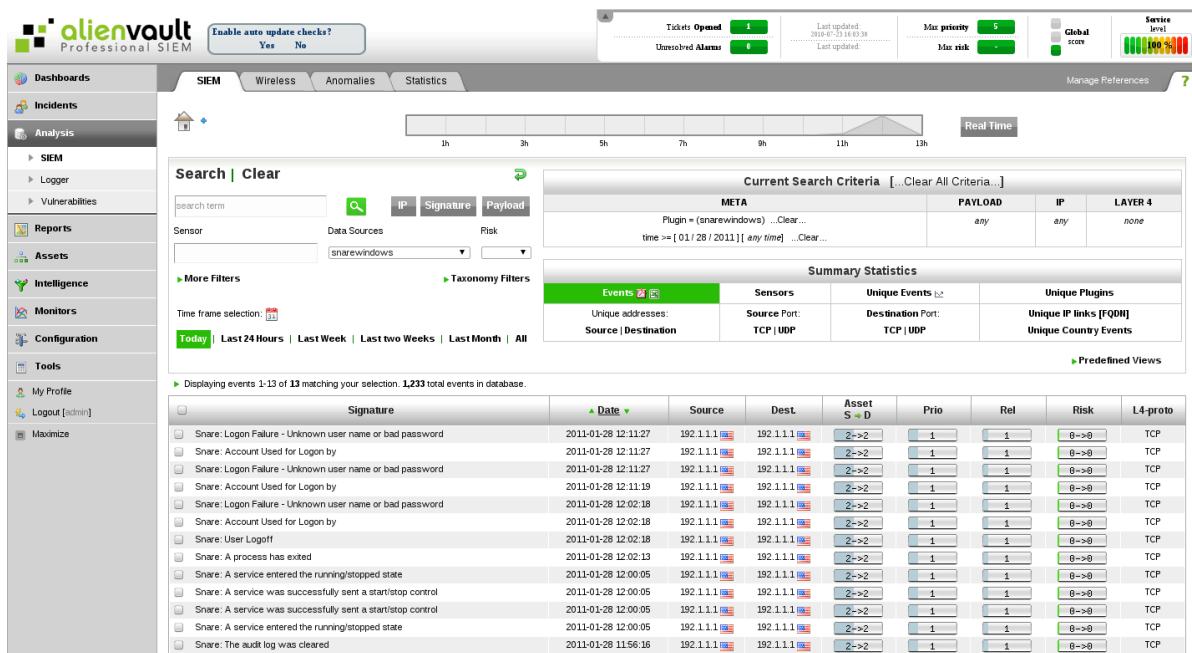
C:\Documents and Settings\OSSIM>
```

4 Configuring AlienVault

1. Enable snare plugin using ossim-setup:
 - 1.1. Connect to your AlienVault Sensor using SSH
 - 1.2. Execute "ossim-setup"
 - 1.3. Go to "(5) Change Sensor Settings"
 - 1.4. Go to "(3) Select detector plugins"
 - 1.5. Select "Snare" and Accept
 - 1.6. Select "Save and exit"
2. Add the windows ip and host to /etc/hosts file
3. Restart ossim-agent:

```
root@ossim:~# /etc/init.d/ossim-agent restart
```

That's all. Now you can view the Windows events at the framework.



The screenshot shows the AlienVault Professional SIEM interface. The left sidebar contains navigation menus for Dashboards, Incidents, Analysis, Reports, Assets, Intelligence, Monitors, Configuration, Tools, My Profile, and Logout. The main content area is titled 'SIEM' and includes a search bar, filters, and a table of search results.

Current Search Criteria [...Clear All Criteria...]

META	PAYLOAD	IP	LAYER 4
Plugin = (snarewindows) ...Clear...	any	any	none
time == [01/28 / 2011] [any time] ...Clear...			

Summary Statistics

Events	Sensors	Unique Events	Unique Plugins
Unique addresses:	Source Port:	Destination Port:	Unique IP links [FQDN]
Source Destination	TCP UDP	TCP UDP	Unique Country Events

Displaying events 1-13 of 13 matching your selection. 1,233 total events in database.

<input type="checkbox"/>	Signature	Date	Source	Dest	Asset S → D	Prio	Rel	Risk	L4-proto
<input type="checkbox"/>	Snare: Logon Failure - Unknown user name or bad password	2011-01-28 12:11:27	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: Account Used for Logon by	2011-01-28 12:11:27	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: Logon Failure - Unknown user name or bad password	2011-01-28 12:11:27	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: Account Used for Logon by	2011-01-28 12:11:19	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: Logon Failure - Unknown user name or bad password	2011-01-28 12:02:18	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: Account Used for Logon by	2011-01-28 12:02:18	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: User Logoff	2011-01-28 12:02:18	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: A process has exited	2011-01-28 12:02:13	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: A service entered the running/stopped state	2011-01-28 12:00:05	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: A service was successfully sent a start/stop control	2011-01-28 12:00:05	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: A service was successfully sent a start/stop control	2011-01-28 12:00:05	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: A service entered the running/stopped state	2011-01-28 12:00:05	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP
<input type="checkbox"/>	Snare: The audit log was cleared	2011-01-28 11:56:16	192.1.1.1	192.1.1.1	2->2	1	1	8->8	TCP

5 Snare plugin

```

username={$username}
userdatal={$userdatal}

[z-snare-ossim-format-really-fallthrough]
#Feb 20 14:16:57 10.186.64.58 ^A MSWinEventLog;1;Security;466;Tue Feb 20 14:17:17
2007;538;Security;Administrador;User;Success Audit;QUICKSILVER-0JM08ZRD;Inicio/cierre de
sesióCierre de sesiõe usuario: ^INombre de usuario:^IAdministrador
^IDominio:^I^IQUICKSILVER-0JM08ZRD ^IId. de inicio de sesiõI^I(0x0,0x20E0FA) ^ITipo de
inicio de sesiõI7 ;61
event_type=event
regexp="(?(P<date>\w+\s+\d{1,2})\s\d\d:\d\d:\d\d)\s+(?(P<sensor>\S+)\s+.*MSWinEventLog(;|#011)\d
+(;|#011)\w+(;|#011)\d+(;|#011)(?(P<date2>\w+\s+\w+\s+\d{1,2})\s\d\d:\d\d:\d\d\s+\d+)(;|#011)(?P
<plugin_sid>\d+)(;|#011)[^(;|#011)]+(;|#011)(?P<username>[^(;|#011)]+)(;|#011)[^(;|#011)]+(;|#
011)[^(;|#011)]+(;|#011)[^(;|#011)]+(;|#011)[^(;|#011)]+(?P<userdatal>.*)$"
date={normalize_date($date)}
sensor={resolv($sensor)}
src_ip={resolv($sensor)}
dst_ip={resolv($sensor)}
plugin_id=1518
plugin_sid={$plugin_sid}
username={$username}
userdatal={$userdatal}

[snare-ossim-format-1]
#Feb 8 16:48:22 10.186.64.58 ^A MSWinEventLog;0;Security;4;Thu Feb 08 16:48:25
2007;592;Security;Administrador;User;Success Audit;QUICKSILVER-0JM08ZRD;Seguimiento
detallado;;Se ha creado un proceso: ^IId. de proceso:^I^I980 ^INombre de archivo de
imagen:^I\WINNT\system32\CMD.EXE ^IId. de proceso creador:^I^I984 ^INombre de
usuario:^I^I^IAdministrador ^IDominio:^I^I^IQUICKSILVER-0JM08ZRD ^IId. de inicio de
sesi\xf3n:^I^I(0x0,0xD237) ;1
event_type=event
regexp="(?(P<date>\w+\s+\d{1,2})\s\d\d:\d\d:\d\d)\s+(?(P<sensor>\S+)\s+.*MSWinEventLog(;|#011)\d
+(;|#011)\w+(;|#011)\d+(;|#011)(?(P<date2>\w+\s+\w+\s+\d{1,2})\s\d\d:\d\d:\d\d\s+\d+)(;|#011)(?P
<plugin_sid>\d+)(;|#011)[^(;|#011)]+(;|#011)(?P<username>[^(;|#011)]+)(;|#011)[^(;|#011)]+(;|#
011)[^(;|#011)]+(;|#011)[^(;|#011)]+(;|#011)[^(;|#011)]+(;|#011)(;|#011)[^:]+\s{4}[^:]+\D+(?
P<pid>\d+)\s{4}[^:]+:(?P<process_name>[^\\s{4}]+\s{4}[^:]+\D+(?P<ppid>\d+)\s{4}[^:]+:([^\s{4}
]+)\s{4}(.*))$"
date={normalize_date($date)}
sensor={resolv($sensor)}
src_ip={resolv($sensor)}
dst_ip={resolv($sensor)}
plugin_id=1518
plugin_sid={$plugin_sid}
username={$username}
filename={$process_name}
userdatal=date2:{$date2}
userdata2=pid:{$pid},ppid:{$ppid}

[snare-ossim-format-2]
#Feb 20 15:03:05 host_sample.int.whatever.corp.local host_samepl.int.whatever.corp.local
MSWinEventLog;1;System;1997;Tue Feb 20 15:04:08
2007;10;Print;SYSTEM;User;Information;AMRERSFP01;None;;Document 241, Sample file.pdf owned by
Kobi was printed on PRINTER1 via port JK82. Size in bytes: 7597 pages printed: 0 ;146
event_type=event

```

```
regex="^(?P<date>\w+\s\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<sensor>\S+)\s+.*MSWinEventLog(;\|#011)\d+
(;\|#011)[^\(;\|#011)]+(;\|#011)\d+(;\|#011)(?P<date2>\w+\s+\w+\s+\d{1,2}\s\d\d:\d\d:\d\d\s+\d+)(;\|#011)
(?P<plugin_sid>\d+)(;\|#011)[^\(;\|#011)]+(;\|#011)(?P<username>[^\(;\|#011)]+)(;\|#011)[^\(;\|#011)]+
(;\|#011)[^\(;\|#011)]+(;\|#011)[^\(;\|#011)]+(;\|#011)[^\(;\|#011)]+(;\|#011)(;\|#011)Document\s+(?
P<doc_number>\d+),\s+(?P<filename>.*)\s+owned by\s+(?P<owner_name>\S+).*was printed
on\s+(?P<printer_name>.*)\s+via port"
date={normalize_date($date)}
sensor={resolve($sensor)}
src_ip={resolve($sensor)}
dst_ip={resolve($printer_name)}
plugin_id=1518
plugin_sid={$plugin_sid}
username={$username}
filename={$filename}

[snare-ossim-format-3]
#Feb 20 15:03:05 host_sample.int.whatever.corp.local host_samepl.int.whatever.corp.local
MSWinEventLog;1;System;1997;Tue Feb 20 15:04:08
2007;10;Print;SYSTEM;User;Information;AMRERSFP01;None;;Document 241, Sample file.pdf owned by
DK (192.1682.44.31) was printed on PRINTER1 via port JK82. Size in bytes: 7597 pages
printed: 0 ;146
event_type=event
regex="^(?P<date>\w+\s\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<sensor>\S+)\s+.*MSWinEventLog(;\|#011)\d+
(;\|#011)[^\(;\|#011)]+(;\|#011)\d+(;\|#011)(?P<date2>\w+\s+\w+\s+\d{1,2}\s\d\d:\d\d:\d\d\s+\d+)(;\|#011)
(?P<plugin_sid>\d+)(;\|#011)[^\(;\|#011)]+(;\|#011)(?P<username>[^\(;\|#011)]+)(;\|#011)[^\(;\|#011)]+
(;\|#011)[^\(;\|#011)]+(;\|#011)[^\(;\|#011)]+(;\|#011)[^\(;\|#011)]+(;\|#011)(;\|#011)Document\s+(?
P<doc_number>\d+),\s+(?P<filename>.*)\s+owned
by\s+(?P<owner_name>\S+)\s+(?P<owner_ip>\S+)\s+was printed on\s+(?P<printer_name>.*)\s+via
port"
date={normalize_date($date)}
sensor={resolve($sensor)}
src_ip={resolve($owner_ip)}
dst_ip={resolve($printer_name)}
plugin_id=1518
plugin_sid={$plugin_sid}
username={$username}
filename={$filename}
```

6 How to configure Rsyslog to separate Snare logs

AlienVault uses Rsyslog to receive logs from other devices, Rsyslog can be configured to separate logs using filters and regular expressions.

In order to filter events coming from an application or device the best option would be creating a new file (With .conf extension) inside the following directory:

```
/etc/rsyslog.d/
```

The following properties can be used to create filters.

Property	Description
msg	The MSG part of the message
rawmsg	The message exactly as it was received from the socket. Should be useful for debugging.
hostname	Hostname from the message
fromhost-ip	The same as fromhost, but always as an IP address. Local inputs (like imklog) use 127.0.0.1 in this property.
programname	The "static" part of the tag, as defined by BSD syslogd. For example, when TAG is "named[12345]", programname is "named".

You can use the following comparators to make your filter

Comparator	Description
contains	Checks if the string provided in value is contained in the property. There must be an exact match, wildcards are not supported.
isempty	Checks if the property is empty. The value is discarded. This is especially useful when working with normalized data, where some fields may be populated based on normalization result.
isequal	Compares the "value" string provided and the property contents. These two values must be exactly equal to match. The difference to contains is that contains searches for the value anywhere inside the property value.
startswith	Checks if the value is found exactly at the beginning of the property value.
regex	Compares the property against the provided POSIX BRE regular expression.

To store Snare events in a different file, it is possible to use the property **fromhost-ip**,
E.g.:

1. Create the a new Rsyslog configuration file

```
root@ossim:~# vim /etc/rsyslog.d/snare.conf
```

2. Write your Snare filter:

```
if $fromhost-ip isequal <snare-ip> then -/var/log/snare.log  
& ~ # This line means discard after match
```

3. Reload rsyslog configuration:

```
root@ossim:~# /etc/init.d/rsyslog reload
```

Once the incoming Snare events are been stored in the new file, change the location property in the snare plugin configuration file

/etc/ossim/agent/plugins/snarewindows.cfg

```
location = /var/log/snare.log
```

7 Configure Log rotation

A Log rotation policy must be configured for every new log file, otherwise the size of the log files will grow indefinitely. AlienVault uses Logrotate to configure the Log rotation policies.

To create a new logrotate configuration file follow the next steps:

1. Create a new logrotate file

```
root@ossim:~# vim /etc/logrotate.d/snare.conf
```

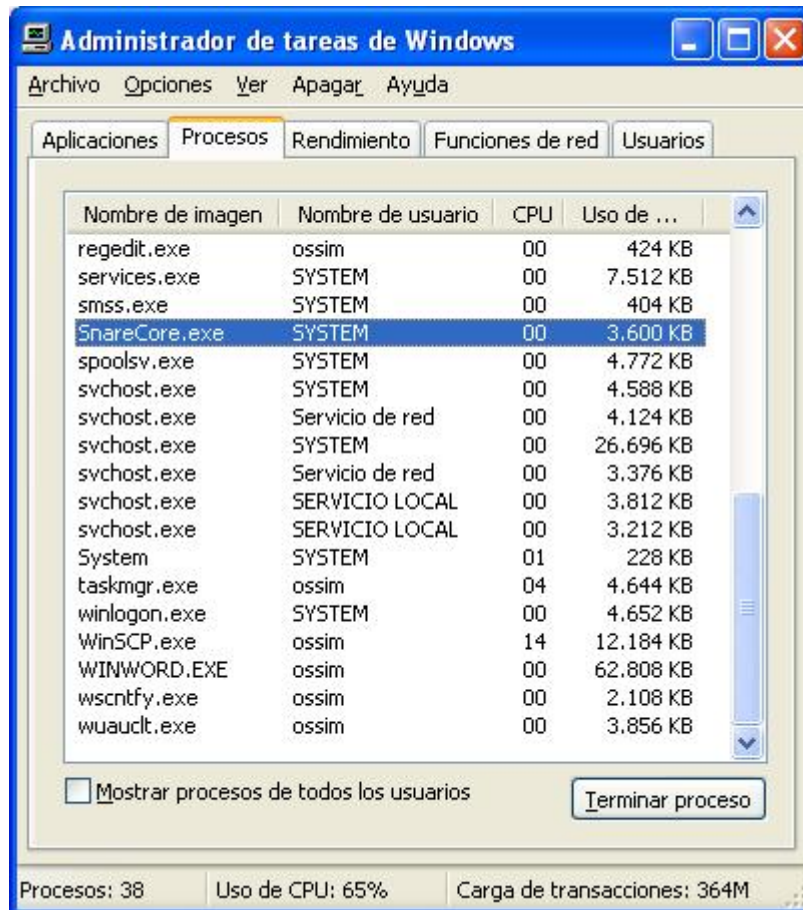
2. The file should look like as follows:

```
/var/log/snare.log {  
    daily                # rotate daily  
    missingok           # if file doesn't exist continue  
    rotate 7            # Save the last 7 logs  
    compress            # Compress the log  
    notifempty         # if log is empty, the log don't rotat  
}
```


8 Troubleshooting

8.1 Find out if your Snare is sending logs

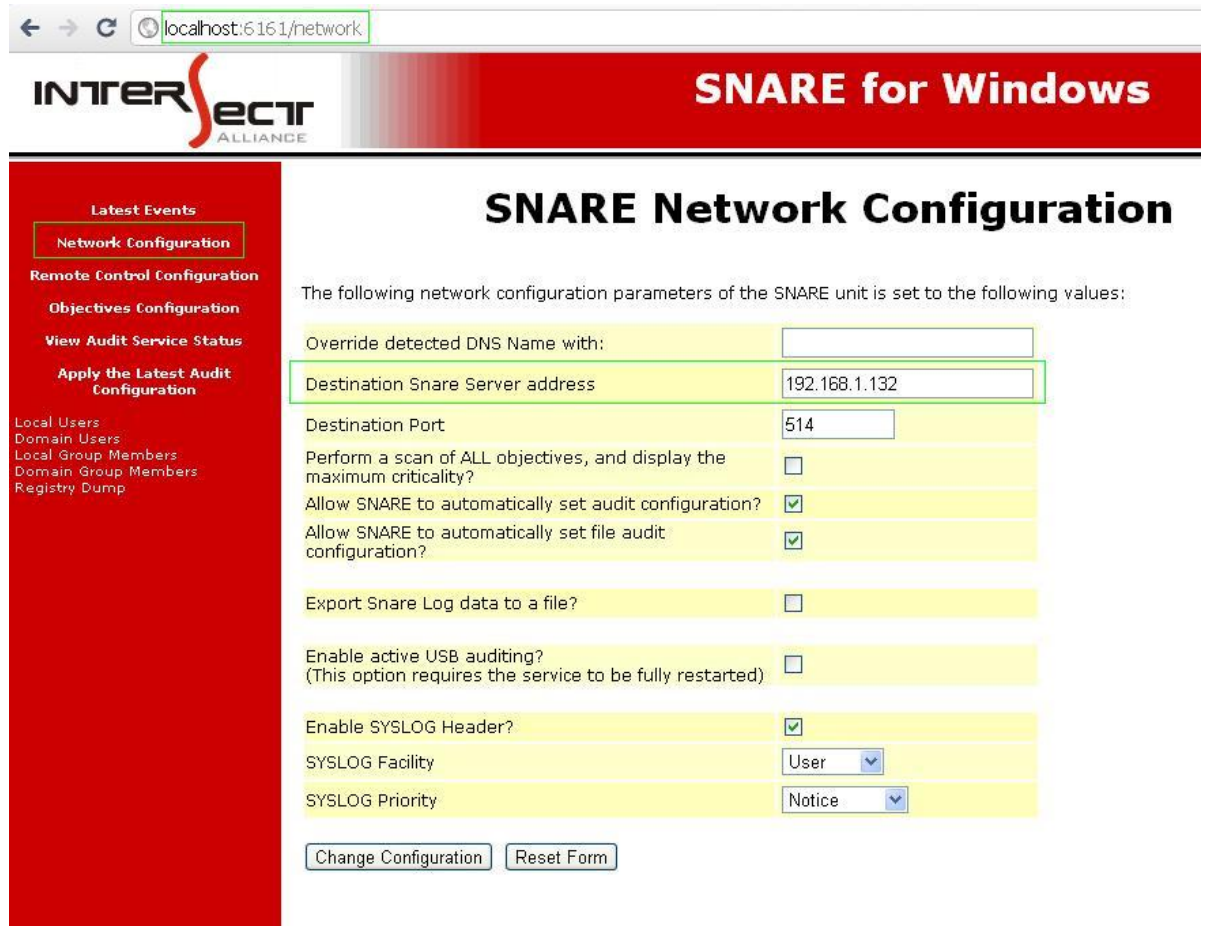
In your Windows box check that the SnareCore.exe process is running. To do that execute **taskmgr** , go to the Process tab and search it.



Also check that Snare is sending events to the IP address of the AlienVault Sensor.

To check this point your browser to <http://localhost:6161>

In the configuration go to Network configuration and check the value of the field "Destination Snare Server address".



← → ↻ localhost:6161/network

INTERSECT **SNARE for Windows**
ALLIANCE

SNARE Network Configuration

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	<input type="text"/>
Destination Snare Server address	192.168.1.132
Destination Port	514
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input checked="" type="checkbox"/>
Export Snare Log data to a file?	<input type="checkbox"/>
Enable active USB auditing? (This option requires the service to be fully restarted)	<input type="checkbox"/>
Enable SYSLOG Header?	<input checked="" type="checkbox"/>
SYSLOG Facility	User
SYSLOG Priority	Notice

8.2 How to check if Syslog is receiving Snare events.

If you have not configured Rsyslog to save the events into a different file run the following command:

```
root@ossim:~# tail -f /var/log/syslog
```

If you have followed the previous steps to store the Snare events in a different file run the following command:

```
root@ossim:~# tail -f /var/log/snare.log
```

8.3 How to check if agent is receiving events.

The following commands shows the events that are being collected by the AlienVault Sensor

```
root@ossim:~# tail -f /var/log/ossim/agent.log
```

8.4 How to check if server is receiving events.

The following command shows the events that are being collected by the AlienVault Server

```
root@ossim:~# tail -f /var/log/ossim/server.log
```

8.5 How to check if Snare plug-in is enabled after ossim-reconfig running ossim-reconfig

You can run the following command to make sure that the plugin is enabled.

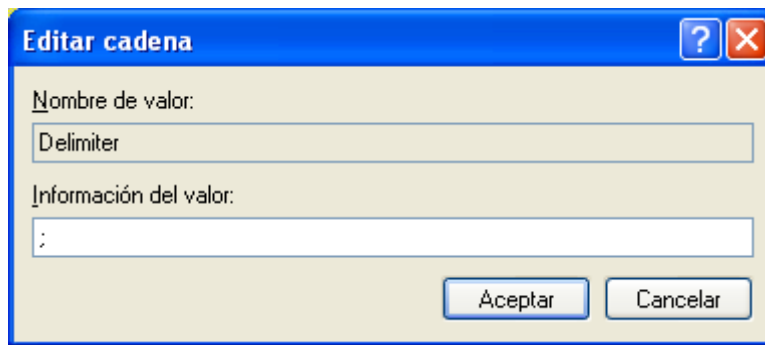
```
root@ossim:~# cat /etc/ossim/agent/config.cfg | grep snare  
snare=/etc/ossim/agent/plugins/snare.cfg
```

8.6 Windows logs delimiter

Windows uses by default the space character to separate the different fields in the log, you will need to change this delimiter and use ";" to allow AlienVault collecting events.

This delimiter can be changed in the Windows registry using the **regedit** tool.

```
HKEY_LOCAL_MACHINE/SOFTWARE/InterSect Alliance/AuditService/Config/Delimiter
```



After changing the delimiter you will need to restart the Snare Service.