SNARE

System iNtrusion Analysis & Reporting Environment

Guide to
Snare for Linux
v4.1

INTERSECT ALLIANCE

About this guide

This guide introduces you to the functionality of the Snare Agent for the Linux operating system. Snare for Linux provides an event, auditing subsystem for the Linux operating system, and facilitates objective-based filtering, and remote audit event delivery. Snare for Linux will also allow a security administrator to fully remote control the application through a standard web browser if so desired. Snare has been designed in such a way as to allow the remote control functions to be easily effected manually, or by an automated process.

Other guides that may be useful to read include:

- Snare Overview
- The Snare Toolset - A White Paper

Table of contents:

1 Introduction

The team at InterSect Alliance have experience with auditing and intrusion detection on a wide range of platforms - Solaris, Windows, Android, AIX, even MVS (ACF2/RACF); and within a wide range of IT security in businesses such as National Security and Defence Agencies, Financial Service firms, Government Departments and Service Providers. This background gives us a unique insight into how to effectively deploy host and network intrusion detection systems that support and enhance an organization's business goals.

'Snare for Linux' allows event logs from the Linux audit subsystem to be collected from the operating system, and forwarded to a remote audit event collection facility after appropriate filtering. Snare for Linux will also allow a security administrator to fully remote control the application through a standard web browser if so desired. Snare has been designed in such a way as to allow the remote control functions to be easily effected manually, or by an automated process.

Other Snare agents are also available including Snare for Solaris, Linux, OSX, MSSQL, Epilog and Windows. The agents are capable of sending data to a wide variety of target collection systems, including our very own **'Snare Server'**. See *Chapter 5 Snare Server* for further details.

Welcome to **'Snare'** - **System iNtrusion Analysis & Reporting Environment**.

2 Overview of Snare for Linux

Snare operates through the actions of three complementary components:

- The native Linux audit subsystem
- The user-space audit daemon (auditd)
- The Snare 'dispatcher' applications.

The audit daemon, and kernel component act in concert to configure the underlying audit subsystem, and extract events of interest from the operating system.

Snare for Linux operates as an 'audit dispatcher' application that receives the audit log data, with Snare directing auditd what events to selectively filter out that you are not interested in, formats the resulting data into something that is more suited to follow-on processing, and delivers it to one or more remote systems over the network.

Snare formats the audit log data into a series of 'tokens'. Two different field separators are used in order to facilitate follow-on processing - TABS separate 'tokens', and COMMAS separate data within each token. This format is further discussed in *Appendix B-Event Output Format*. The result is that a raw event, as processed by Snare, may appear as follows:

```
localhost.localdomain LinuxKAudit 2 event,open,Jun 20 06:00:16
sequence,304390 uid,4294967295,unknown euid,0,root gid,0,root egid,0,root
process,,/opt/VBoxGuestAdditions-4.2.18/sbin/VBoxService return,4,yes
name,/var/run/utmp exe,/opt/VBoxGuestAdditions-4.2.18/sbin/VBoxService
success,yes return,4 syscall,5,open uid,unknown euid,root gid,root
egid,root arch, name,/var/run/utmp a0,b7ea7003 a1,2 a2,0 a3,b7ea7009
items,1 ppid,1 pid,2339 uid,0 suid,0 fsuid,0 sgid,0 fsgid,0 tty,none
comm,VBoxService key,obj-1-1 cwd,/ item,0 inode,67 dev,03:02 mode,0100664
ouid,0 ogid,5 rdev,00:00
```

Snare also incorporates a tiny embedded web server, the Remote Control Interface, which allows administrators to remotely control which events are collected and reported. The Remote Control Interface also provides information on users, groups, and group membership on the local machine, which can be used to satisfy various regulatory security requirements.

Snare for Linux is known to work on Red Hat Enterprise 5,6, CentOS 5,6, Fedora Core X, SuSE 10,11, Ubuntu 12,13,14, Debian 7.3.

3 Installing and running Snare

3.1 Snare installation

WHAT YOU NEED...

- An appropriate Linux Distribution
- The snarelinux package available for Enterprise customers from the Snare Secure Area at https://www.intersectalliance.com.

HOW TO... Install Snare for Linux binary RPM package.

1. To install the Snare package perform the following:
2. Download the required RPM or DEB
3. Logon as root user, i.e. at the command prompt enter the command `/bin/su` and enter the root password when prompted. Issue the command, as root as per your distribution:
   ```
   >rpm -Uvh filename.rpm
   E.g.  >rpm -Uvh snarelinux-supp-4.1.0-SLED-10.i686.rpm
   ```
   Or
   ```
   >dpkg -i filename.deb
   E.g.  >dpkg -i snarelinux-supp-4.1.0-Debian-7.3.x86_64.deb
   ```
4. This will install Snare for Linux and restart the audit daemon (auditd).

NOTE: **Red Hat** may have a conflict during install. If this occurs, use -force flag
```
E.g.  >rpm -Uvh --force snarelinux-supp-4.1.0-SLED-10.i686.rpm
```

HOW TO... Remove Snare for Linux binary RPM package (if required).

1. Query the RPM database to ensure Snare for Linux is installed
   ```
   >rpm -q snarelinux-supp
   ```
2. Remove the Snare for Linux package
   ```
   >rpm -e snarelinux-supp
   ```

Remove Snare for Linux binary DEB package (if required).

1. Remove the Snare for Linux package
   ```
   >dpkg -r snarelinux-supp
   ```

3.2 Audit configuration

The Snare configuration is stored as */etc/audit/snare.conf (SuSE 10 and 11 users the location is /etc/snare.conf)*. This file contains all the details required by Snare to configure the audit subsystem to successfully execute.

The configuration of */etc/audit/snare.conf* can be changed either:

- directly

  Care should be taken if manually editing the snare.conf configuration file to ensure that it conforms to the required format for the audit daemon. Also, any use of the Remote Control Interface to modify security objectives or selected events, may result in manual configuration file changes being overwritten. Details on the configuration file format can be viewed in *Appendix A - Configuration File Description*. Failure to specify a correct configuration file will prevent Snare from running.

- or by modifying the objectives via the Remote Control Interface

  The Remote Control Interface is the most effective and simplest way to configure */etc/audit/snare.conf* and operates completely in memory, with no reliance on any external files.

How to... Remote Audit Monitoring

The Remote Control Interface can be turned off by editing the default */etc/audit/snare.conf* file. You can either edit the */etc/audit/snare.conf* file directly, commenting the `allow=1` line under the `[Remote]` section, or by setting this value to `0`.

Be sure to restart the agent for the change to take effect. The agent can be restarted by:

```
>/etc/init.d/auditd restart
```

Note: For administrators, the system log files will be updated whenever settings are applied to the snare.conf, for example, /var/log/messages. This information may assist you when required.

4 The Remote Control Interface

The Remote Control Interface is accessible by entering http://localhost:6161 in the web browser as shown in Figure 1. The Remote Control Interface is turned on by default, and also password protected for security reasons. The default username and password are:

Username: snare
Password: snare

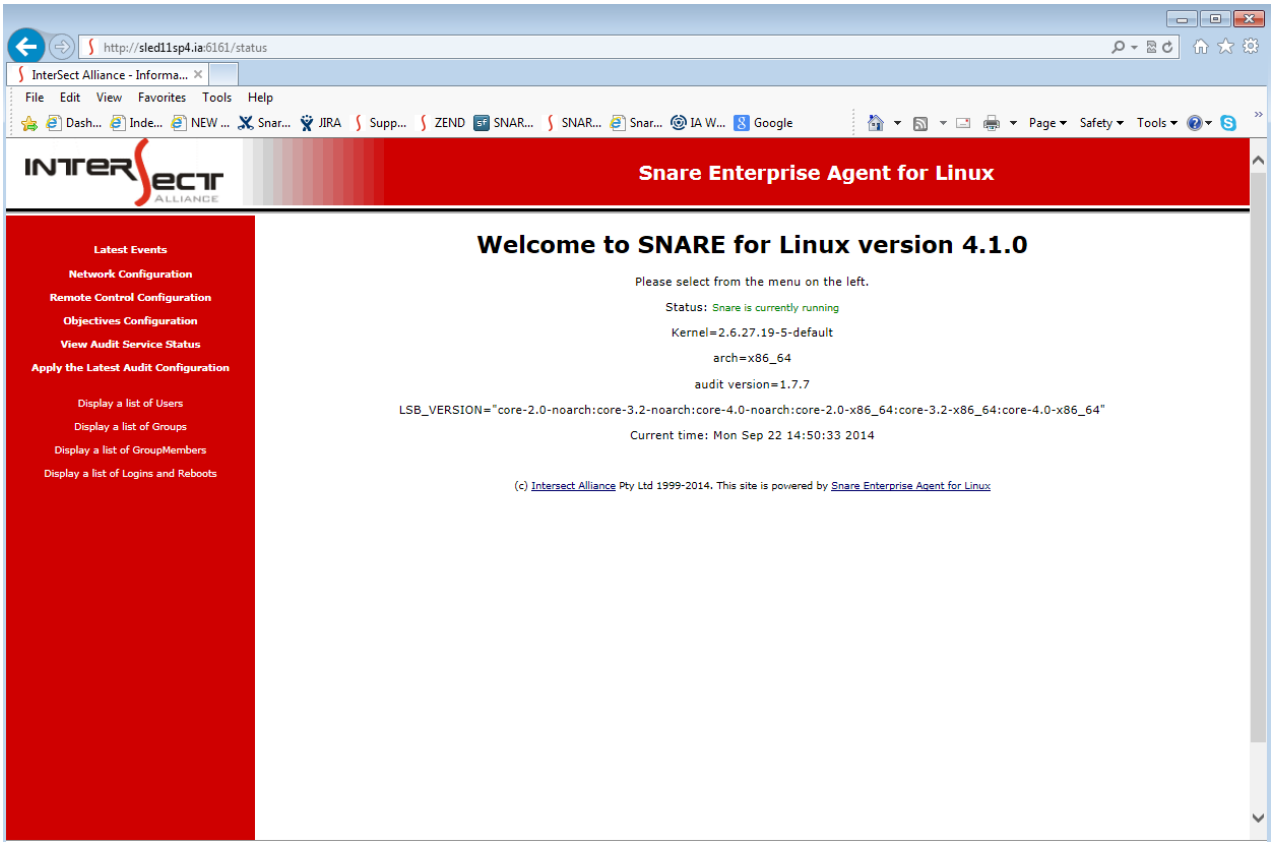
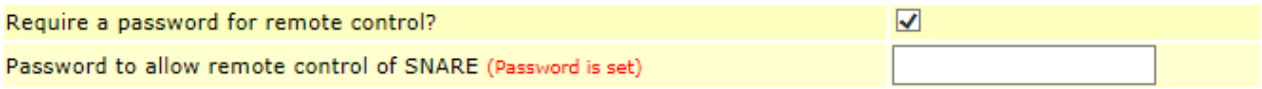


Figure 1: The Remote Control Interface-View Status

Note: The password is not encrypted at this time. Ensure you change the default Snare password immediately after installation so that it is encrypted, for security purposes. It is recommended you use a strong complex password of at least 12 characters. To update the password go to the Remote Control Configuration page and update the password.



Note: For Red Hat users to access the remote control interface, will need to ensure:

- the firewall rule allows access to the agent.
- to disable or set to permissive mode with SELinux.

The Remote Control Interface provides a number of capabilities including:

- Network Configuration
- Remote Control Configuration
- Objectives Configuration
- Viewing Recent Events
- Displaying User and Group metadata.

Please note that some options on these pages that are only available to users with the purchased Enterprise version. The OpenSource agents will not include any features that are new to this version of the Snare for Linux agent.

4.1 Network Configuration

To set the audit configuration parameters, select the 'Network Configuration' link.

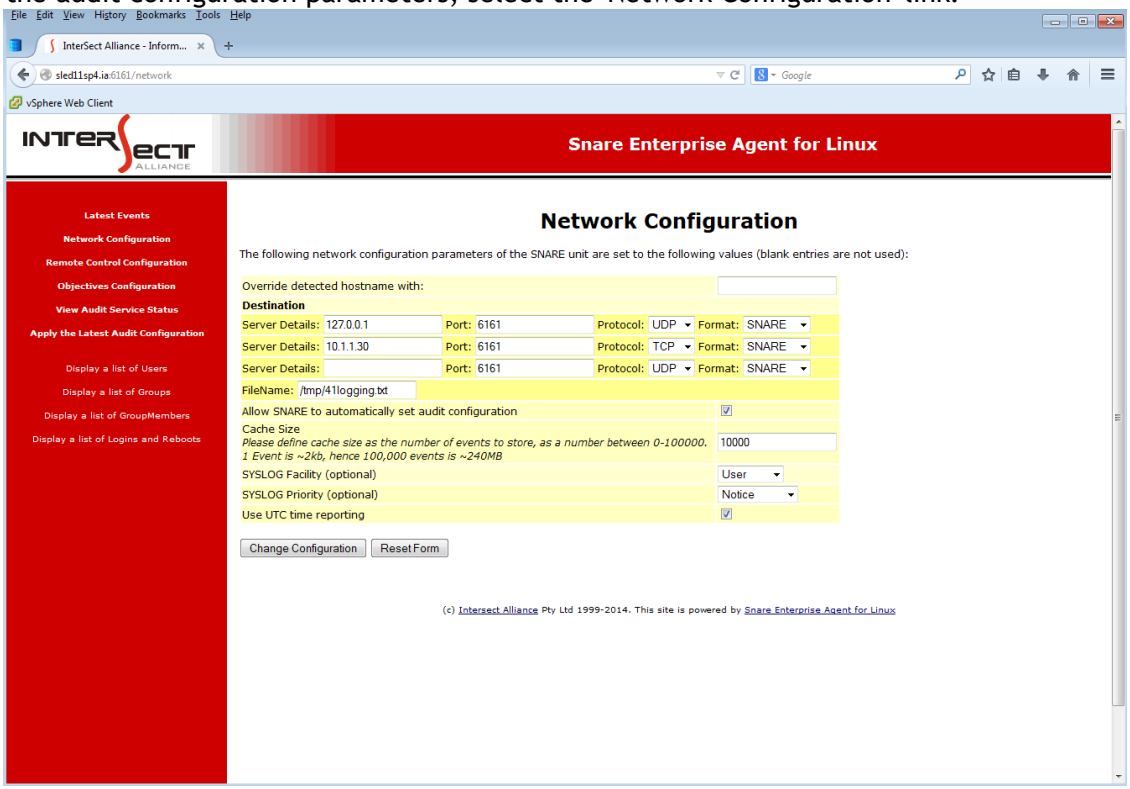


Figure 2: Configure the network settings

The configuration parameters available are as follows, as displayed in Figure 2:

- ***Override detected hostname with:*** Can be used to override the name that is given to the host. Unless a different name is required to be sent in the processed event log record, leave this field blank. The default is to use the fully qualified name for the machine.
- ***Destination:*** Snare can send audit events to one or more network destinations. Snare can send data either to a Snare-compatible server, or a SYSLOG compatible destination. Please be aware that most SYSLOG servers are incompatible with the extremely high volumes of data Snare is capable of generating.

  Server Details: Enter a DNS name, or IP address for each planned destination.

  Port: Select the port you would like Snare to use when sending events.

  Protocol: Select the protocol you would like Snare to use when sending events. Using TCP or SSL will guarantee message delivery. Using SSL will use an encrypted connection to the server.

Format: Select this option if the requirement is that the event records need to be in a specific format. This feature will allow the event log record to be formatted so it is accepted by a Syslog or a Snare server. Note: The agent will override the specified format in some cases. Specifying port 6161 will force the use of Snare format. Specifying a port of 514 will force the use of the Syslog format.

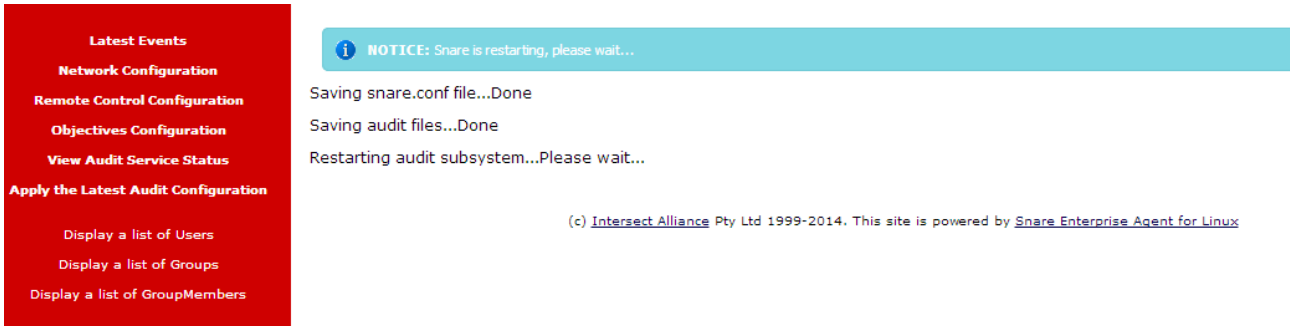
FileName: Log the output to disk as well as the network. If the file does not exist, it will be created.

Click Change Configuration to allow another destination to be added. Likewise, to remove a destination, then delete the entry in the *Server Details* and click Change Configuration.

- ***Allow SNARE to automatically set audit configuration:*** By default, Snare will take control and manage your audit event settings for you. Normally on a Unix system, you will need to modify the file */etc/audit/audit.rules* in order to establish a new monitored event. Snare has the capability to 'turn on' event auditing in response to the objectives you set within the Remote Control Interface. It is recommended that this parameter is enabled.
- ***Cache size:*** Allow Snare to store messages that could not be sent. Combined with the TCP or TLS this option will allow the agent to cache messages if there is a network failure or the Snare Server is otherwise unavailable. Any cached message is kept until it is sent or the size of the cache exceeds the specified allotment, in which case the oldest message is removed. If the agent is restarted, any cached messages are lost.
- ***SYSLOG Facility (optional):*** If you are sending your data to a SYSLOG server, specifies the subsystem that produced the message. The list displays default facility levels.
- ***SYSLOG Priority (optional):*** If you are sending your data to a SYSLOG server, the agent can be configured to use a static or dynamic priority level.
- ***Use UTC time reporting:*** Enables UTC (Coordinated Universal Time) timestamp format for events instead of local machine time zone format.

To save and set changes to these settings, and to ensure the audit daemon has received the new configuration, perform the following:

1. Click on Change Configuration to save any changes.
2. Click on the **Apply the Latest Audit Configuration** menu item. There will be a quick notice that Snare is restarting as displayed below.



4.2 Remote Control Configuration

The Snare for Linux agent can be controlled remotely by administrators, if required. Remote control is enabled by default. The remote control page is displayed in Figure 3.

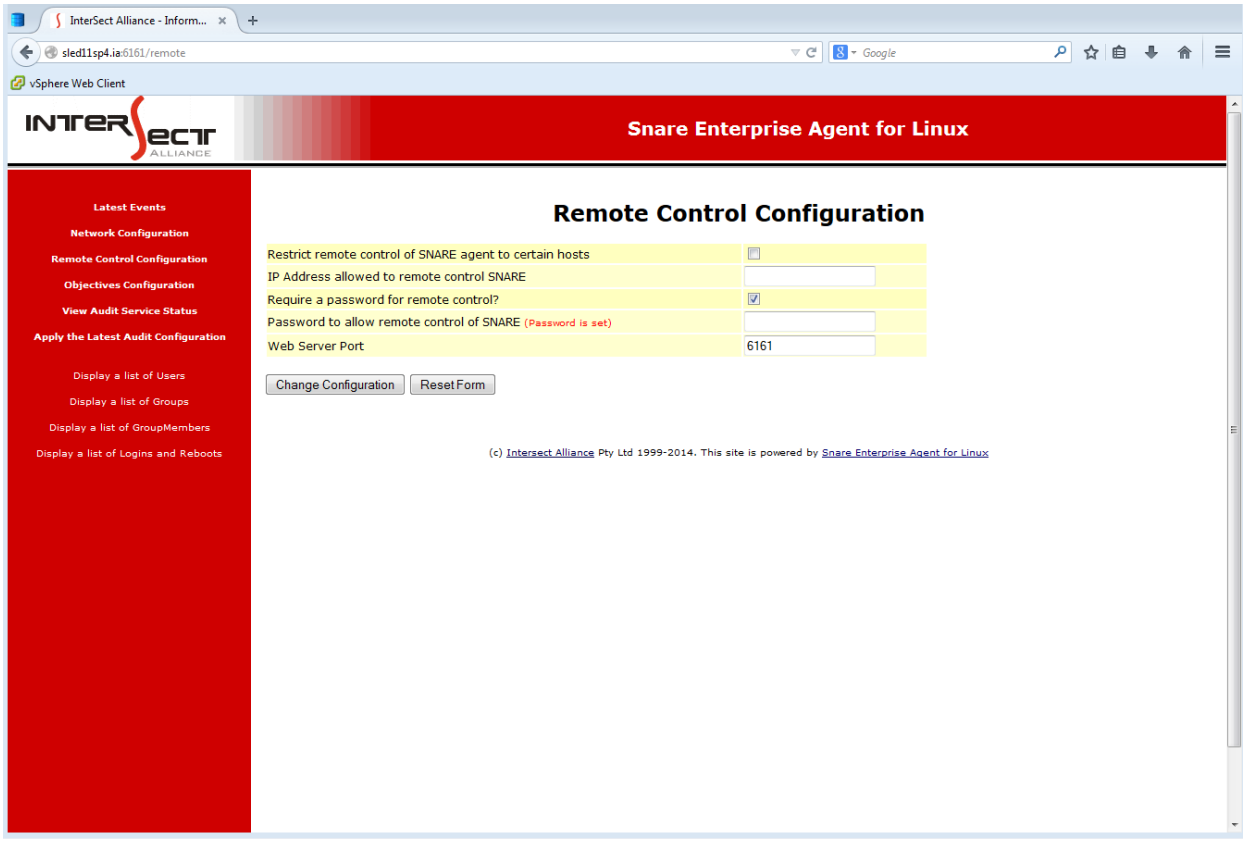


Figure 3: Configure the Remote Control

The parameters which may be set for remote control operation include:

- ***Restrict remote control of SNARE agent to certain hosts:*** By default Snare allows any IP address to connect to the remote control interface. Enabling this option restricts connections to the remote control interface to the IP given in the following option.
- ***IP Address allowed to remote control SNARE:*** Remote control actions may be limited to a given host. This host, entered as an IP address will only allow remote connections to be effected from the stated IP address. Application-level firewall capabilities are also available, which block users from accessing the Remote Control Interface from any IP address other than the one specified.
- ***Require a password for remote control?:*** Indicate whether a password will be set so that only authorised individuals may access the remote control functions. Highly recommended.
- ***Password to allow remote control of SNARE:*** If above checkbox is checked, password must be set. A password of appropriate strength should be set for the remote control facility.

- ***Web Server Port:*** An optional port that the Remote Control Interface listens on, can be specified. Users of the Snare Server should generally leave this as 6161, in order to take advantage of the Snare Server's user and group audit capabilities.

To save and set changes to these settings, and to ensure the audit daemon has received the new configuration, perform the following:

1. Click on Change Configuration to save any changes.
2. Click on the **Apply the Latest Audit Configuration** menu item.

4.3 Objectives configuration

Snare's ability to filter events is accomplished via the auditing 'objectives' capability. The term 'objective' is used within Snare Agents to describe an auditing goal. It is generally made up of events that Snare should watch for, a filter term containing a 'token' and a criticality level. See Figure 4.

The objective configuration page supplied as part of the web based remote control is intended as a way to enable users to commence audit functions reasonably quickly. For power users, a far more powerful and functional way is to manually control the */etc/audit/snare.conf* file. This is described in more detail in ***Appendix A***-Configuration File Description, and is intended for users who have a very detailed knowledge of Linux administration and security. It is NOT recommended for novice users.

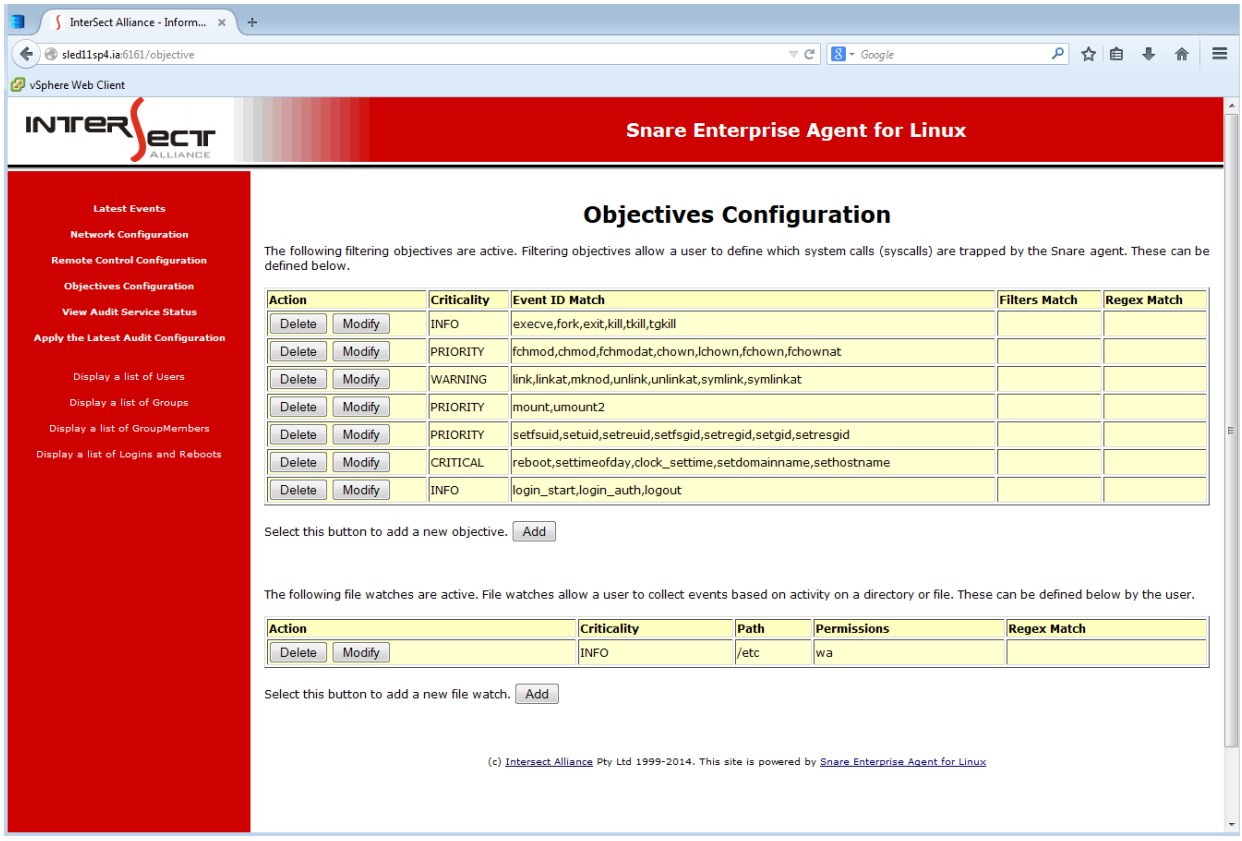


Figure 4: Display the Set objectives

Snare for Linux has two ways of auditing file-related events – event (syscall) objectives, and/or file watches. Either or both, can be employed depending on your requirements.

Event Objectives

Select 'Add' to insert an objective or 'Modify' to edit an objective. Generally the order of objectives is not important.

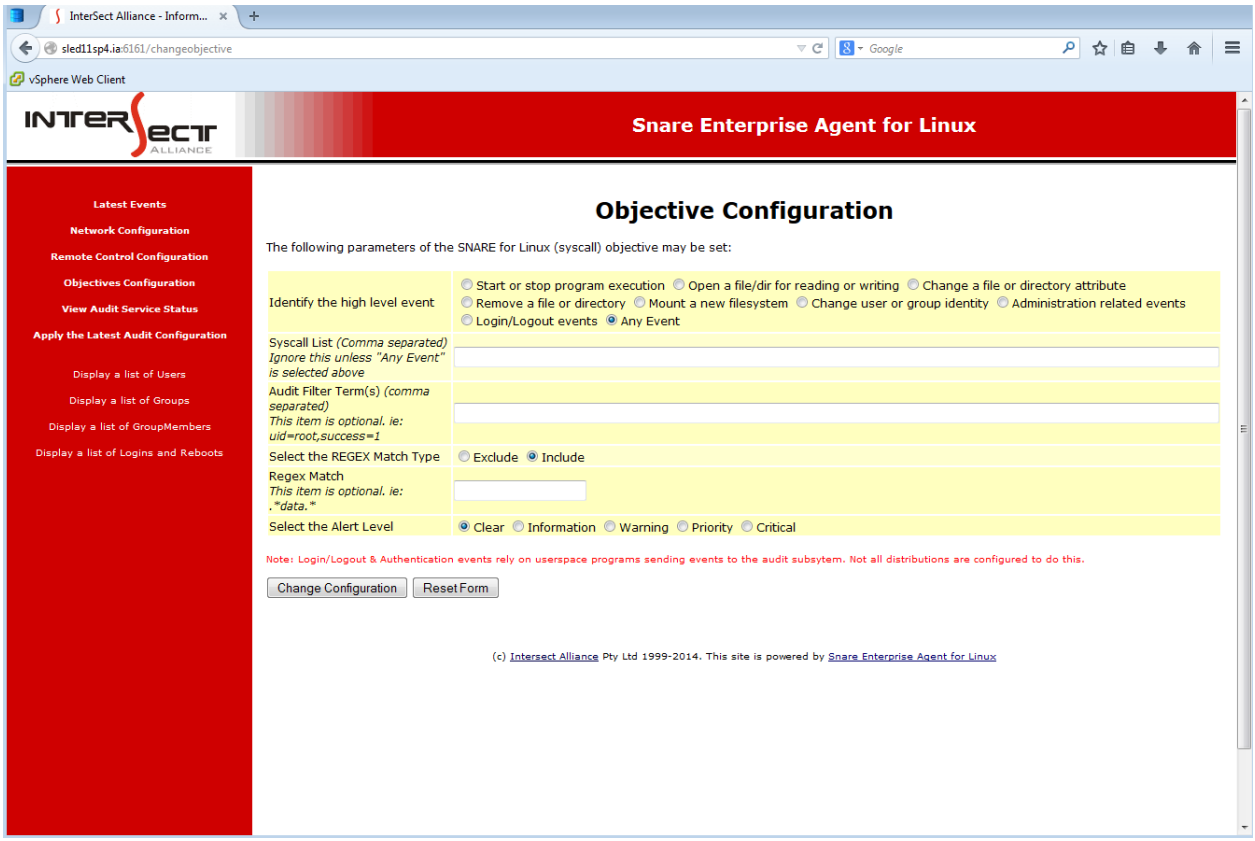


Figure 5: Adding/Modifying a Syscall Objective

The following parameters may be set as displayed in Figure 5:

- ***Identify the high level event:*** Each of the objectives provides a high level of control over which events are selected and reported. Events are selected from a group of high level requirements, and further refined using selected filters. Events are generally grouped into the following:
    - Start or stop program execution: execve,fork,exit,kill,tkill,tgkill
    - Open a file/dir for reading or writing: open,close
    - Change a file or directory attribute: fchmod,chmod,fchmodat,chown,lchown, fchown,fchownat
    - Remove a file or directory: rmdir, unlink
    - Mount a new filesystem: mount, umount2
    - Change user or group identity: setfsuid,setuid,setreuid,setfsgid,setregid,setgid,setresgid

- Administration Related Events: reboot,settimeofday,clock_settime,setdomainname, sethostname
- Login/Logout events: login_start,login_auth,logout

In addition, any event that can be generated by the audit subsystem can be specified (comma separated) by using the 'Any Event(s)' high level group.

Tip: Turning on file-related events can produce a very high volume of audit events on some systems, and therefore result in a considerable amount of CPU time being used by Snare and the audit subsystem.

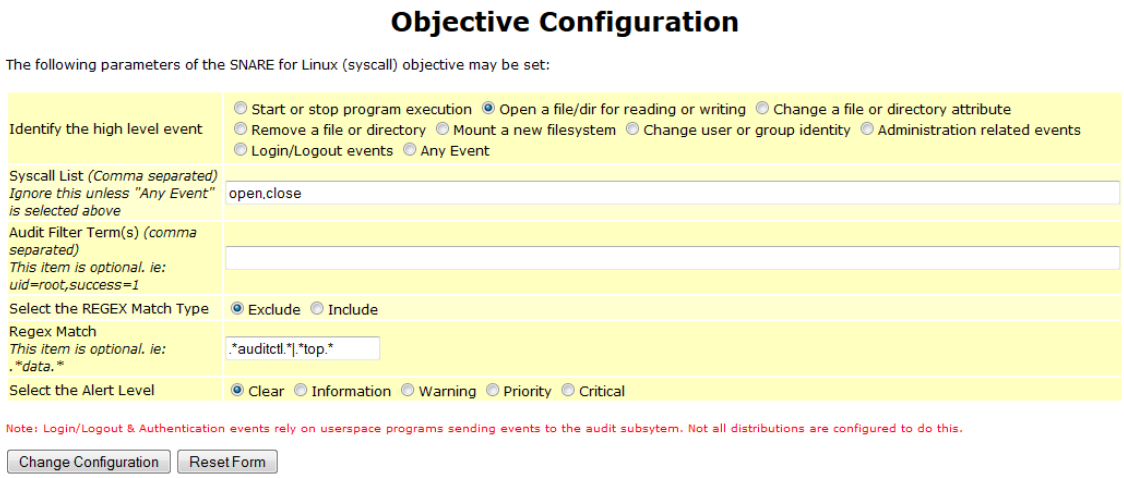
- ***Syscall List:*** If 'Any Event(s)' is selected as the high level event, then add a comma separated list of audit events to search for.
- ***Audit Filter Term(s):*** A filter term containing a 'token' which appears within the events of interest, and the search criteria that Snare should use to include or exclude the event. For example, a search term of: `/etc/.*` would match any event which mentions any file in `/etc`. Another example:

localhost.localdomain LinuxKAudit Criticality,2 event,execve,20130725 11:03:29 sequence,524 uid,500,george gid,500,george euid,500,george egid,500,george process,,"/bin/uname" return,0,yes name,"/bin/uname" 1374714209.448:524): arch,x86_64 syscall,59,execve success,yes return,0 a0,3190f70 a1,3191040 a2,318d4b0 a3,8 items,2 ppid,3214 pid,3236 ***auid,500,george*** *uid,500,george gid,500,george euid,500,george suid,500,george fsuid,500,george egid,500,george sgid,500,george fsgid,500,george tty,pts1 ses,1 comm,"uname" exe,"/bin/uname" key,"obj-2-0" argc,1 a0,"uname" cwd,"/home/george" item,0 name,"/bin/uname" inode,21430336 dev,fd:00 mode,0100755 ouid,0,root ogid,0,root rdev,00:00 item,1*

The token highlighted in red could be used to only select events where the “auid” (the 'audit' ID) is a certain value, in this case “audit,500,george” or a more general term, such as “george”.

- ***Select the REGEX Match Type:*** Select to either include the regex match in the search or exclude the regex match set below.
- ***Regex Match:*** A filter term the objective should match. For example .*data.* would cause the objective to match the word 'data' in the whole string. To use multiple matches use the virtual bar symbol which will act as the OR operator.

  Complex matches such as the following are possible. For example to include/exclude various commands from the log output use the following syntax:
  `.*/bin/grep.*|.*/bin/bash.*|.*/bin/sleep.*|.*/usr/bin/wc.*|.*/usr/bin/cut.*|.*/usr/bin/expr.*|.*/usr/bin/bc.*|.*/usr/bin/du.*|.*/usr/bin/tail.*|.*/usr/bin/head.*|.*/usr/bin/sum.*|.*/usr/bin/who.*`



  It is recommended to perform all the excludes for a particular high level event in one objective, for example to exclude events that contain either auditctl or top in the high level event open a file/directory for reading or writing, then select ***Exclude*** and in the Regex Match type ***.*auditctl.*|.*top.**** (as shown above).
- ***Select the Alert Level:*** The criticality levels are Critical, Priority, Warning, Information and Clear. These security levels are provided to enable the Snare user to map audit events to their most pressing business security objectives.

To save and set changes to these settings, and to ensure the audit daemon has received the new configuration, perform the following:

1. Click on Change Configuration to save any changes.
2. Click on the **Apply the Latest Audit Configuration** menu item.

File Watches

File watches are somewhat different to event filters. Rather than asking the kernel to report on all file activity, a 'file watch' will cause Snare to ask the kernel to 'tag' certain files, or directories, and only generate file-related events when activity associated with those particular files or directories, occur. This generally results in a spectacular drop in resource usage by the Snare and audit processes, as potentially thousands of file-related events-per-second no longer have to be discarded when they do not match a Snare agent objective. This method ***does not*** require that each targeted file or directory exist prior to Snare starting up. Where a directory is specified, Snare will also watch for the creation of new files and directories.

See Figure 6 for configuring a Snare file watch.

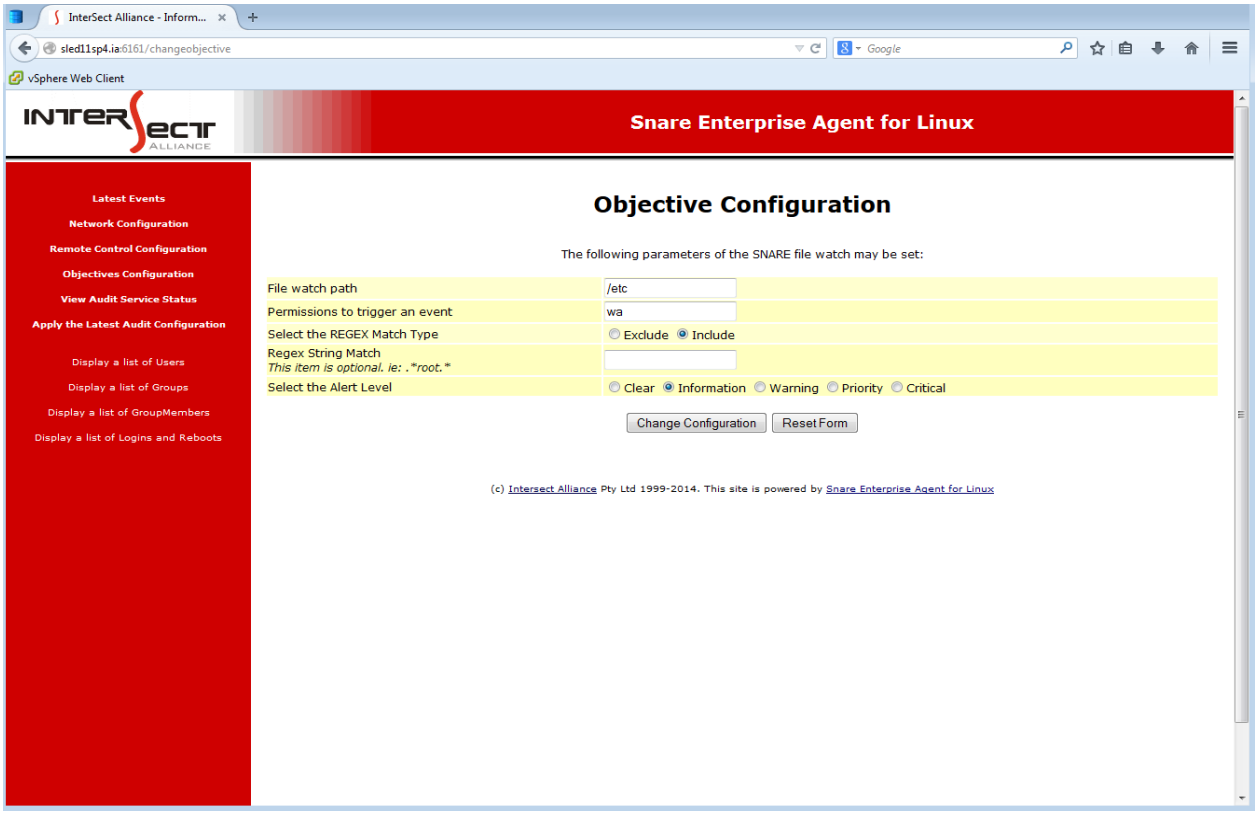


Figure 6: Adding/Modifying a File Watch Objective

The following parameters may be set:

- ***File watch path:*** Any file or directory, currently existing or not, can be specified. In order not to generate too many events, it is strongly recommended that file watches be set on the exact directory(ies) of choice, with as few permissions as possible. It is far more desirable to use file watches to monitor accesses to files and directories, than to use syscall/event filters.
- ***Permissions to trigger an event:*** A file watch is associated with monitoring four types of permissions, namely *rwxa*. These are read (r), write (w), execute (x) or attributes (a). A file MUST be specified with a minimum of 1 and a maximum of 4 permissions.

- ***Select the REGEX Match Type:*** Select to either include the regex match in the search or exclude the regex match set below.
- ***Regex String Match:*** A filter term the objective should match. For example .*root.* would cause the objective to match the word 'root' in the whole string. The Regex format uses the same basic format as discussed in the objective section above.
- ***Select the Alert Level:*** The criticality levels are Critical, Priority, Warning, Information and Clear. These security levels are provided to enable the Snare user to map audit events to their most pressing business security objectives.

  Note: Depending on your Linux kernel there may be an issue with the creation/deletion of file watches. This bug in the kernel occurs if you create a file watch, and then do not apply the audit configuration, and then delete the file watch, with the result locking up your operating system. To prevent this issue ensure you set the audit configuration after creation.

4.4 Display of Latest Events / Destination Status

A small rotating cache of audit events is kept by the Snare for Linux web server. Clicking on the **Latest Events** menu item will display twenty of the most recent events as displayed in Figure 7.

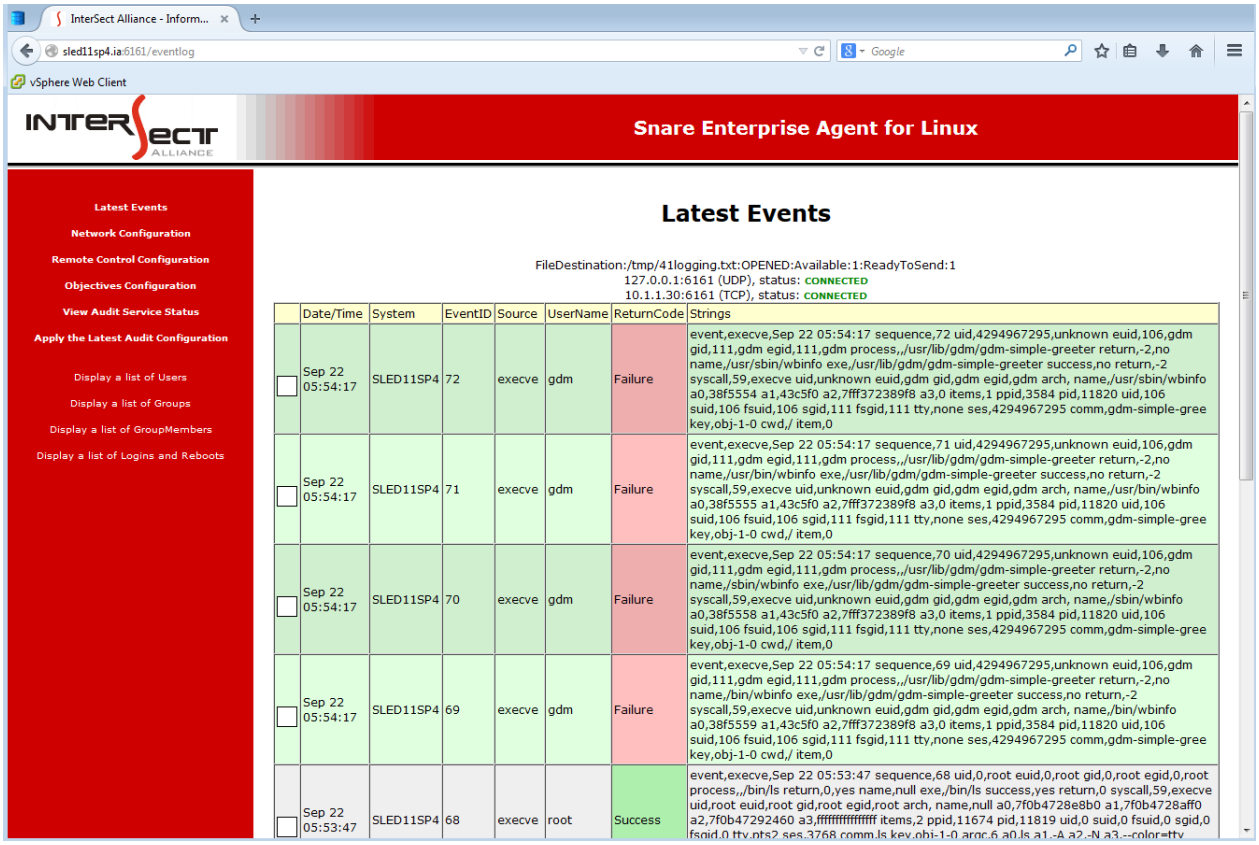


Figure 7: Display the latest events

Additionally this page shows the status for each Destination that was configured for logging. An example of this destination status is:

10.1.1.30:6161 (TCP), status: **CONNECTED**

This information can be used to help debug potential logging issues. The status can be explained as follows:

- **Host/Port:** e.g.: 10.1.1.30:6161
  The host ip/name and port that logs will be sent too.
- **Log destination Type:** e.g.: TCP
  The protocol of the remote connection. Possible values are TCP, UDP, SSL or File
- **The current State of the connection:** e.g.: CONNECTED
  This field indicates what snare is currently doing with the connection. You will see many different states including:

- INITIAL - The remote log location is about to begin setup
- RESOLVING - DNS resolution for a hostname is occurring
- RESOLVE_DELAY(x) - DNS resolution failed, a retry will occur in X seconds
- CONNECTING - Snare is trying to connect to the destination
- CONNECT_FAILED - The connection to the destination failed
- CONNECT_DELAY(x) - Connecting to the remote end failed, it will be retried again in X seconds
- CONNECTED - Snare has an active connection to the destination
- SENDING - Snare is currently sending logs to the destination
- DISCONNECTED - The destination has disconnected the snare agent.. a reconnection will occur automatically.
- HANDSHAKE - A SSL/TLS Handshake is in progress
- HANDSHAKE_FAILED - The SSL/TLS Handshake failed
- OPENING - Opening a a file destination is in progress
- WRITING - Writing is occurring to a file
- WRITE_FAILED - A write to file failed
- CLOSED - A file has been closed

Additionally two other statuses give instant feedback about what Snare is doing:

- ***Available***
  - Indicates if Snare can use the destination to send logs. A value of 1 indicates that logs can be sent. A value of 0 indicates logs can't be sent
- ***ReadyToSend***
  - Indicates if the destination is setup in a state where logs can be sent. For instance if Snare is already sending to the destination, ReadyToSend will be 0.

4.5 List Displays

A list of Users, Groups, Group Members, Logins and Reboots may be displayed by selecting on the appropriate link in the menu.

```
login   root        pts/2        Mon Sep 22 15:18        still logged in        sled11sp4.ia
login   root        pts/1        Mon Sep 22 15:17        still logged in        hydra.ia
login   root        pts/1        Mon Sep 22 14:10        15:16  (01:06)         hydra.ia
boot    runlevel    (to lvl 5)   Wed Aug 13 14:36        15:50 (40+01:13)       2.6.27.19-5-default
boot    reboot      system boot  Wed Aug 13 14:36              (40+01:13)       2.6.27.19-5-default
login   shutdown    system down  Wed Aug 13 14:36        15:50 (40+01:13)       2.6.27.19-5-default
boot    runlevel    (to lvl 6)   Wed Aug 13 14:36        14:36  (00:00)         2.6.27.19-5-default
boot    runlevel    (to lvl 5)   Tue Aug 12 16:48        14:36  (21:48)         2.6.27.19-5-default
boot    reboot      system boot  Tue Aug 12 16:47               (21:48)         2.6.27.19-5-default
boot    runlevel    (to lvl 5)   Tue Aug 12 16:41        16:48  (00:07)         2.6.27.19-5-default
boot    reboot      system boot  Tue Aug 12 16:40               (21:55)         2.6.27.19-5-default
boot    runlevel    (to lvl 5)   Thu Jun  5 15:59        16:41 (68+00:41)       2.6.27.19-5-default
boot    reboot      system boot  Thu Jun  5 15:59              (68+22:36)       2.6.27.19-5-default
boot    runlevel    (to lvl 5)   Thu Jun  5 15:01        15:59  (00:57)         2.6.27.19-5-default
boot    reboot      system boot  Thu Jun  5 15:01              (68+23:34)       2.6.27.19-5-default
boot    runlevel    (to lvl 5)   Thu Jun  5 14:52        15:01  (00:09)         2.6.27.19-5-default
boot    reboot      system boot  Thu Jun  5 14:52              (68+23:44)       2.6.27.19-5-default
```

```
HOST: SLED11SP4
at       25       Batch jobs daemon
bin      1        bin
daemon   2        Daemon
dnsmasq  107      dnsmasq
ftp      40       FTP account
games    12       Games account
gdm      106      Gnome Display Manager daemon
haldaemon         101      User for haldaemon
lp       4        Printing daemon
mail     8        Mailer daemon
man      13       Manual pages viewer
messagebus        100      User for D-Bus
news     9        News system
nobody   65534    nobody
ntp      74       NTP daemon
polkituser        103      PolicyKit
postfix  51       Postfix Daemon
pulse    104      PulseAudio daemon
root     0        root
sshd     71       SSH daemon
suse-ncc          105      Novell Customer Center User
uucp     10       Unix-to-Unix CoPy system
uuidd    102      User for uuidd
wwwrun   30       WWW daemon apache
snare    1000     Snare
vboxadd  108
```

5 Snare Server

The Snare Server is a log collection, analysis, reporting, forensics, and storage appliance that helps your meet departmental, organisational, industry, and national security requirements and regulations. It integrates closely with the industry standard Snare agents, to provide a cohesive, end-to-end solution for your log-related security requirements.

The Snare Server, as shown in Figure 8 collects events and logs from a variety of operating systems, applications and appliances including, but not limited to: Windows (NT through 2012), Solaris, AIX, OSX, Irix, Linux, Tru64, ACF2, RACF, CISCO Routers, CISCO PIX Firewall, CyberGuard Firewall, Checkpoint Firewall1, Gauntlet Firewall, Netgear Firewall, IPTables Firewall, Microsoft ISA Server, Microsoft IIS Server, Lotus Notes, Microsoft Proxy Server, Apache, Squid, Snort Network Intrusion Detection Sensors, IBM SOCKS Server, and Generic Syslog Data of any variety.

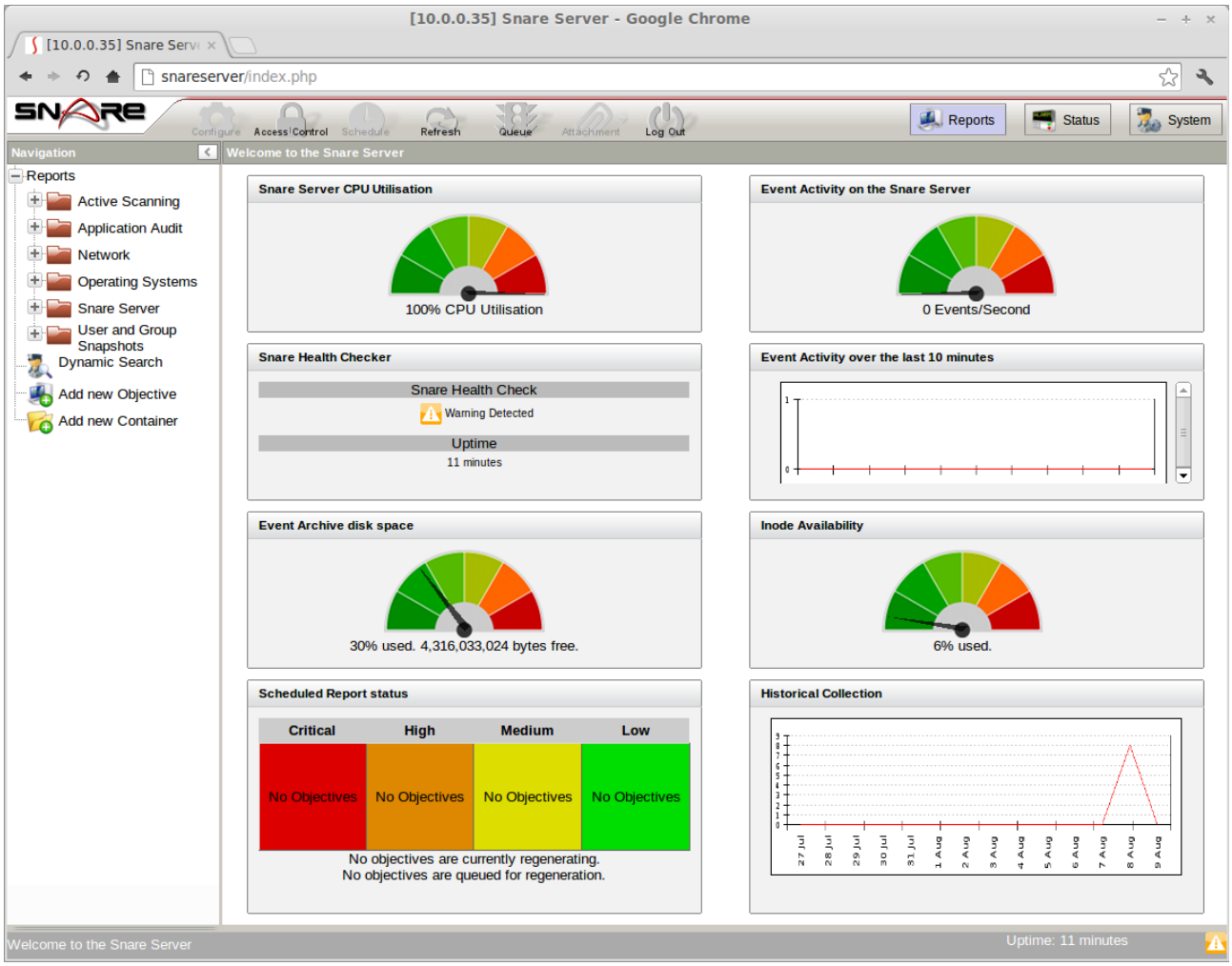


Figure 8 Welcome to the Snare Server

Some of the key features of the Snare Server include:

- Ability to collect any arbitrary log data, either via UDP or TCP
- Secure, encrypted channel for log data using TLS/SSL
- Proven technology that works seamlessly with the Snare agents
- Snare reflector technology that allows for all collected events to be sent, in real time, to a standby/backup Snare Server, or a third party collection system
- Ability to continuously collect large numbers of events. Snare Server collection rates exceed 60,000 events per minute using a low end, workstation class, Intel based PC on a 100Mbps network.
- Ability to drill down from top level reports. This reduces the amount of data "clutter" and allows a system administrator to fine tune the reporting objectives.
- Ability to 'clone' existing objectives in order to significantly tailor the reporting criteria. These reports, along with all Snare Server objectives, may be scheduled and emailed to designated staff.
- The Snare Server uses extensive discriminators for each objective, allowing system administrators to finely tune reporting based on inclusion or exclusion of a wide variety of parameters.
- Very simple download and installation
- Flexibility when dealing with unique customer requirements
- A strategic focus on low end hardware means that Snare can achieve outstanding results with minimal hardware cost outlay
- Snare gives you useful data, out of the box, with default objectives tuned for common organisational needs
- Ability to manage Enterprise Agents
- All future Snare Server versions and upgrades included as part of an annual maintenance fee.

The Snare Server is an appliance solution that comes packaged with a hardened, minimal version of the Linux operating system to provide baseline computing functionality, which means you do not need to purchase additional operating system licenses, database licenses, or install additional applications in order to get up and running. Like your android phone, or your home router, any operating-system level management and maintenance is either automated, or is available within the web-based interface.

For further information on the Snare Server refer to the *Snare Server User Guide* on the Intersect Alliance website.

6 About InterSect Alliance

Intersect Alliance, part of the Prophecy International Holdings Group, is a team of leading information technology security specialists. In particular, Intersect Alliance are noted leaders in key aspects of IT Security, including host intrusion detection. Our solutions have and continue to be used in the most sensitive areas of Government and business sectors.

Intersect Alliance intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying, abstracting and/or solving complex security problems.

Intersect Alliance welcomes and values your support, comments, and contributions.

For more information on the Enterprise Agents, Snare Server and other Snare products and licensing options, please contact us as follows:

The Americas +1 (800) 834 1060 Toll Free | +1 (303) 771 2666 Denver

Asia Pacific +61 8 8213 1200 Adelaide Australia

Europe and the UK +44 (797) 090 5011

Email intersect@intersectalliance.com

Visit www.intersectalliance.com

Appendix A - Configuration File Description

The purpose of this section is to discuss the parameter settings of the configuration file. The Snare configuration file is located at */etc/audit/snare.conf*, and this location may not be changed. If the configuration file does not exist, the audit daemon will not actively audit events until a correctly formatted configuration file is present.

Snare can be configured in several different ways, namely:

a. Via the embedded web server (r*ecommended for novice users*), or
b. By manually editing the configuration file (r*ecommended for advanced users*).

The format of the **audit configuration file** is discussed below. Any line beginning with "#" will be treated as a comment line and ignored. Any number of tabs or spaces can be used. Major tokens such as `[Config]` must be surrounded by the square brackets.

`[Config]`	This section allows you to specify settings relating to the operation of the Snare agent.
`clientname=override`	The hostname of the client. If no hostname is set, the value of "hostname --fqdn" will be used
`set_audit=[1|0]`	This value determines if Snare should set the auditing configuration for the local machine.
`syslog_facility=facility`	The SYSLOG facility used when sending to a SYSLOG server.
`syslog_priority=priority`	The SYSLOG priority used when sending to a SYSLOG server.
`cache_size=(0 - 100000)`	This value determines the size of the event cache,ie; the number of events, that Snare should keep if it cannot reach at least one of the hosts. The value must be between 0 and 100000. This feature only appears in Enterprise Agents only.
`use_utc=1`	Enable UTC (Universal Coordinated Time). This feature only appears in Enterprise Agents only.
version=4	Future inclusion: Snare version for informational purposes.

[Remote]	This section allows you to specify settings relating to the Remote Control Interface used to control Snare.
allow=[1|0]	Turn the Remote Control Interface on or off.
listen_port=6161	Set a port that the Snare for Linux agent should listen on.
accesskey_enabled=on	Password is required to be set
accesskey=md5password	Md5 checksum of the password used to protect the embedded web server
restrict_ip_enabled=0	Restrict the Remote Control Interface to an IP.
restrict_ip=1.2.3.4	IP address of a system that is used to remotely control the agent. All requests from other systems will be dropped.

[Output]	By default, if no output section exists within the configuration file, the audit daemon will not send any data to anywhere. Otherwise, audit events will be sent to all valid destinations specified in the Output section. As such, events can be sent to one or all of a file, or to a remote network destination
file=/fully/qualified/file/name	The audit daemon will send data to the fully qualified filename. The *directory* must exist. The *file* will be created if it doesn't exist. E.g file=/var/log/filewatch.log
network=hostname:port:protocol:format	Data will be sent to the remote host, and network port specified here. Audit data can be sent to a remote system using the UDP or TCP protocol. SSL may also be used to indicate an encrypted TCP connection. Format may be either SNARE or SYSLOG. E.g networkOutput0=10.1.1.30:6161:TCP:SNARE

[Linux]	
audit_buffersize=360	Adjustment of audit buffers if required to avoid causing a too heavy audit load on your system. To be added to the Remote Control Interface as a setting in the future release of version 5.0 of the Snare for Linux agent.

`[Objectives]`	This section describes the format of the objectives. Objectives are composed of: 1. Criticality - an integer between 0 and 4 that indicates the severity of the event. 0 is 'clear', 4 is "critical". Any integer less than 0 will cause the line to be rejected. 2. The match function will either be include match="<value>" or exclude match!="<value>". The value follows standard regular expression format. 3. The event - this must either correspond to a valid syscall event, or a series of events separated by commas, and may be surrounded with round brackets (). Note that the embedded web server will convert the generic "groups" in the Audit Configuration window to the required events. For example, the abstracted group 'Administrative Events', will result in the event entry: 'event=(*reboot,settimeofday,clock_settime, setdomainname,sethostname*)' being written. 4. Audit Filter Term - The filter expressions to apply to the audit rule. It must match the filter expressions as documented in the auditctl Unix man page. Eg uid=root, success=1 5. Return - either Success, Failure or * to indicate both Success and Failure 6. Regex Match - An optional string to match. This can be a regular expression or .* to indicate all events. Eg .*/bin.* Note that whitespace will be trimmed from the start and end of items.

`criticality=1 match=".*/bin.*" event=execve uid=maria,sucess=1`
 	
`criticality=1 match!=".*/bin.*" event=execve uid=maria,success=1`
	Report at criticality level 1, whenever the user 'maria', attempts to execute a binary within /sbin,
	
	Using match!=".*/bin.*" will make an exclude rule to not send events that contain this string match.
	
	criticality=`0` for Clear (ordinary security level), `1` for Information, `2` for Warning, `3` for Priority, `4` for Critical.

Shown below is an example */etc/audit/snare.conf* file. It is an example file only, and should NOT be used for operational purposes. It has been included to demonstrate the key concepts of formulating a snare.conf file, as discussed above.

Example Version 4.1 snare.conf file

```
#This is a comment line with no leading spaces
# Snare configuration file
# Note: This file may be automatically updated by the Snare agent
# This file was generated by at: Mon Sep 22 15:22:26 2014

[Config]
use_criticality=1
encrypt_msg=0
clientname=
set_audit=1
cache_size=10000
use_utc=1
syslog_facility=1
syslog_priority=5

[Linux]
audit_buffersize=360

#TCP and multiple network entries only allowed by the Enterprise agent
[Output]
networkOutput0=10.1.1.30:514:UDP:SYSLOG
networkOutput1=10.1.1.46:6161:TCP:SNARE
fileOutput0=/tmp/41logging.txt

[Remote]
allow=1
accesskey_enabled=on
restrict_ip=
listen_port=6161
accesskey=snare
restrict_ip_enabled=0

[Objectives]
criticality=1   match=""        event=execve,fork,exit,kill,tkill,tgkill
criticality=3                                                   match=""
event=fchmod,chmod,fchmodat,chown,lchown,fchown,fchownat
criticality=2                                                   match=""
event=link,linkat,mknod,unlink,unlinkat,symlink,symlinkat
criticality=3   match=""        event=mount,umount2
criticality=3                                                   match=""
event=setfsuid,setuid,setreuid,setfsgid,setregid,setgid,setresgid
criticality=4                                                   match=""
event=reboot,settimeofday,clock_settime,setdomainname,sethostname
criticality=1   match=""        event=login_start,login_auth,logout

[Watch]
criticality=1   match=".*usesr01.*"        path=/etc       perms=waxr
```

Appendix B - Event Output Format

The Snare dispatcher receives data from the native Linux audit subsystem.

The native audit daemon reports data in such a way that:

- It is 'programmatically' difficult to determine how many 'lines' make up an audit event. Some lines can be repeated, with slightly different values.
- You can have multiple, identical tokens for an event (e.g. two “path=” tokens)
- Event lines may be interleaved (i.e. you might get two lines from event # 1000, then one line from event # 1001, then another line from event # 1000).
- Some filename characters are translated into their HEX equivalents which will make matching filenames difficult.

Snare for Linux uses an internal cache to amalgamate all lines relating to an individual event, into “one line per event” format, once appropriate filtering/event selection has taken place. An event will look like this once processed by Snare:

```
localhost.localdomain LinuxKAudit 2 event,execve,Jun 20 06:10:03
sequence,345199 uid,4294967295,unknown euid,0,root gid,0,root
egid,0,root process,,/sbin/auditctl return,0,yes name,null
exe,/sbin/auditctl success,yes return,0 syscall,11,execve uid,unknown
euid,root gid,root egid,root arch, name,null a0,80ca7f8 a1,80ca980
a2,80ca8a8 a3,0 items,2 ppid,24047 pid,24051 uid,0 suid,0 fsuid,0
sgid,0 fsgid,0 tty,none comm,auditctl key,obj-0-0 a0,/sbin/auditctl
a1,-v cwd,/ item,0 inode,37751 dev,03:02 mode,0100750 ouid,0 ogid,0
rdev,00:00 item,1 inode,17644 dev,03:02 mode,0100755 ouid,0 ogid,0
rdev,00:00
```

Snare for Linux presents the information in a series of token/data groups. Three different field separators are used in order to facilitate follow-on processing - TABS separate 'tokens', COMMAS separate data within each token. A 'token' is a group of related data, comprising a 'header', and a series of comma separated fields which make up data that relates to the header. Examples of tokens from the above event include:

- `syscall,11,execve`
- `/sbin/auditctl`