System iNtrusion Analysis & Reporting Environment

Release Notes for Snare for Linux

About this document

This document provides release notes for the Snare Enterprise Agent for Linux.

Snare Enterprise Agent for Linux v4.1.6

Snare Enterprise Agent for Linux v4.1.6 was released on 4th September 2015

Bug Fixes

- **Agent website crashes in certain cases when a connection is severed**
  Fixed a potential crash of the agent when the web server component of the agent received many disconnect requests. This issue would not affect most customers as it would require a system to have hundreds or more network interfaces to manifest.
- **Linux agent does not allow deleting of options in filters field**
  Fix a bug where filters were not removed correctly from the rules setting when editing the objective configuration in the web interface.

Snare Enterprise Agent for Linux v4.1.5

Snare Enterprise Agent for Linux v4.1.5 was released on 31st July 2015

Bug Fixes

- **Snare Server getting strange fragments of logs from Linux agent**
  Fixed issue where multi-part audit events were being improperly parsed causing the tail of the event to be sent to the Generic Log queue.

- **Fix handling of subj_sen audit keyword**
  Fix issue where it was not possible to use the keyword subj_sen as a match condition in a objective rule. This keyword is now working correctly.

Snare Enterprise Agent for Linux v4.1.4

Snare Enterprise Agent for Linux v4.1.4 was released on 30th June 2015

Bug Fixes

- **Dropping leading zeroes in date and time formats in the logs**
  Fixed the log output where date/month/year was not being handled correctly. This could be in the file output or the syslog destination.

Snare Enterprise Agent for Linux v4.1.3

Snare Enterprise Agent for Linux v4.1.3 was released on 26th February 2015

Bug Fixes

- **Linux Agent does not work with DNS name in config file**
  Fixed the issue where a DNS name would not be resolved upon reload of the agent. The fix now both allows DNS names to be used but also validates that they resolve. Hence since the auditing process starts pre-network being brought up on some distributions, an entry in the /etc/hosts or equivalent should be added.

- **Clientname not honoured**
  A bug was identified where the clientname hostname override set in the network configuration page, was not always sent when events were generated. This bug has now been fixed.

- **Linux Agent Outputs the wrong date in Snare Format**
  Fix a bug where the date format of an event transmitted in SNARE format could potentially be wrong.

Snare Enterprise Agent for Linux v4.1.2

Snare Enterprise Agent for Linux v4.1.2 was released on 4th February 2015

Change Log

- **Issue with filtering login/logout events**
  Event processing has been updated so login/logout* events are correctly excluded if an exclude rule is active on the events.

- **Event processing to allow additional event names**
  Event processing has been updated allow the additional fields event names to be filtered:
  `acct_change` - A change in account has occurred (audit event id 1101)
  `cred_acq` - Additional credentials have been acquired, ie privilege upgrade via sudo (audit event id 1103)
  `cred_disp` - Obtained credentials have been disposed (ie drop sudo privileged)

  These event names can be used in either the Remote Control Interface or into the configuration file.

Snare Enterprise Agent for Linux v4.1.1

Snare Enterprise Agent for Linux v4.1.1 was released on 10th December 2014

Change Log

- **Syslog format difference between OpenSource and Enterprise version for Linux**
  A potential bug where a null character could appear in log output when SYSLOG format was selected has been fixed. Updating the agent will apply the change automatically.

- **Bug in regex Audit filter terms**
  A bug has been fixed in the parsing of audit filter terms. This bug was caused by incorrect parsing of the comma delimiter. As a results audit expressions such as auid=100,guid=100 would be be treated as a single term (ie auid = "100,guid=100"). This would in turn cause the audit.rules file to be written incorrectly. The fix corrects the parsing of the term. Updating the agent then reapplying the settings will fix and problems in the audit.rules file.

- **Gui session handling issue**
  When using the Snare Agent Remove Console with Internet Explorer 10, changes were not always possible, This would be reported as 'Your session has become invalid, please try again' when trying to change a setting. This session handling issue has been resolved for IE.

Snare Enterprise Agent for Linux v4.1.0

Snare Enterprise Agent for Linux v4.1.0 was released on 16th September 2014

Enhancements

- **Implement Exclude Rules in Linux agent***
  Audit Event Processing has been changed to support exclude matching. As a result of this change it is now possible to add rules which exclude specific events. Exclude changes are represented in the configuration file on an objective line as: match!="searchstring" and can be configured in the GUI. Existing event processing/configuration files are unaffected.

- **Last Logins Details**
  The webui has been updated to re-add the Last Logins screen which was present in the 2.x series agents but missing from the 3.x and 4.x agents prior to this release.

- **Various UI pages are formatted incorrectly**
  Remote UI has been changed to display the output with the mimetype text/plain for the User, Group, UserGroup and new LastLogin pages, . As a result of this change, this change should only be noticable if these pages are viewed in a web browser.

- **Config file permissions need modification**
  The agent has been changed to write out all files it touches (snare.conf, auditd.conf, audit.rules) with permissions of 0400. As a result of this change, programs that access these files as non root will no longer be able to access the files after applying changes in the GUI.

Change Log

- **.deb Installer doesn't rely on auditd correctly**
  The Snare for Linux installer has been changed to address a problem where it was possible to attempt an install without the auditd package installed on systems that use dpkg. As a result of this change, dpkg will now indicate the required dependancy of auditd is not yet installed before attempting the install of the Snare for Linux Agent.

Snare Enterprise Agent for Linux v4.0.1

Snare Enterprise Agent for Linux v4.0.1 was released on 7th July 2014

New Features

- **PCRE Regular Expression support for filtering objectives**
  When creating an objective, the ability to match a string search via regex is available. For example entering in the new Regex String Match field .*root.* would cause the objective to match the word 'root' in the whole string.
- **SSL support**
  Protocol can be selected in the Network Configuration settings of the Remote Control Interface. Using SSL will use an encrypted connection to the server.
- **Multi-threading**
  Improved multi-threading and general performance improvements.

Change Log

- **Remote Control Interface improved**
  The user interface layer includes subtle changes to the pages to include notices, warning and any errors. For example, when applying the latest audit configuration, a notice that Snare is restarting is displayed.
- **Event Destination Status Indicator**
  The Latest Events page now displays the status for each destination that was configured for logging as well as additional status information for each destination including the protocol, port and connection status.
- **Ability to adjust auditd buffer size**
  Available only via the configuration file for version 4.0, `audit_buffersize` may be adjusted if causing if there is a large number of events being generated by the system and the kernel audit load has difficultly in keeping up.
- **Improved caching capability when a destination server is down**
  The Cache Size parameter on the Network Configuration page, allows the agent to cache messages if there is a network failure or the destination server is 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.
- **UTC time support**
  Coordinated Universal Time timestamp format is available for events instead of local machine time zone format.

Snare Enterprise Agent for Linux v3.1.4

Snare Enterprise Agent for Linux v3.1.4 was released on 6th March 2014

Bug Fixes

- There was an issue where *execve* events may not always report the executable causing events.

Change Log

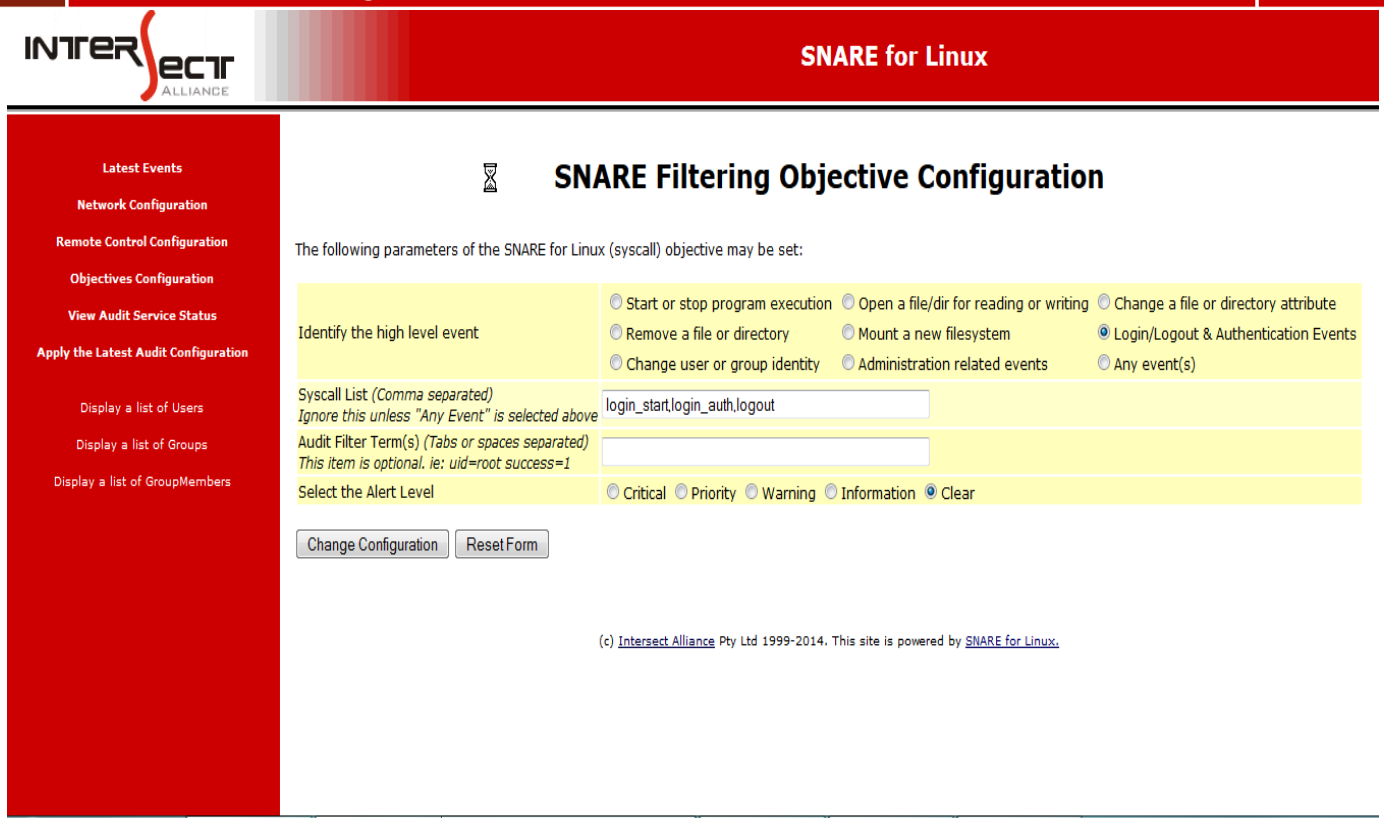
Restored Feature
Please note that the following features are now re-available for Snare Enterprise Agent for Linux only.

- **Login/Logout & Authentication Events Filtering**

In Snare For Linux 2.x, the ability to create objectives that monitored login/logout and Authentication events was available. This feature was removed in the 3.0.0 Agent. Due to multiple requests this feature has been restored in the 3.1.4 Linux Agent. However, the following caveat should be noted:

Under Linux login/logout/login_start events are generated by user-space applications (ie sshd). These events are sent to the kernel which then sends them to the audit subsystem. Snare is only capable of monitoring these events if the user-space applications actually sends them. Some distributions (such as Debian 7.3) have configured these user-space applications NOT to send events to the kernel, hence Snare is not able to monitor login/logout/login_start events for these distributions.

Login/Logout & Authentication event monitoring can be enabled using the remote configuration console (below):



Alternatively, Login/Logout & Authentication event monitoring can be enabled in the configuration file by defining an objective with one or more of the desired events:

- login_auth
  - This event is generated when an authentication event is attempted. It indicates success or failure of the authentication.
- login_start
  - This event is generated when a user successfully logs in to a session
- logout
  - This event is generated when the user logs out of a session

An example configuration file using these events is:

```
[Config]
        version=2
        use_criticality=0
        set_audit=1
        syslog_facility=local0
        syslog_priority=information

[Remote]
        allow=1
        listen_port=6161

[Output]
        network=127.0.0.1:6161

[Objectives]
        criticality=2   event=execve
        criticality=3   event=login_auth,login_start,logout
        criticality=1   event=login_auth
```