System iNtrusion Analysis & Reporting Environment

Release Notes for Snare for Linux v3.1.4

About this document

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

Snare for Linux Agent v3.1.4

Snare 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 Enterprise Snare for Linux agents only.

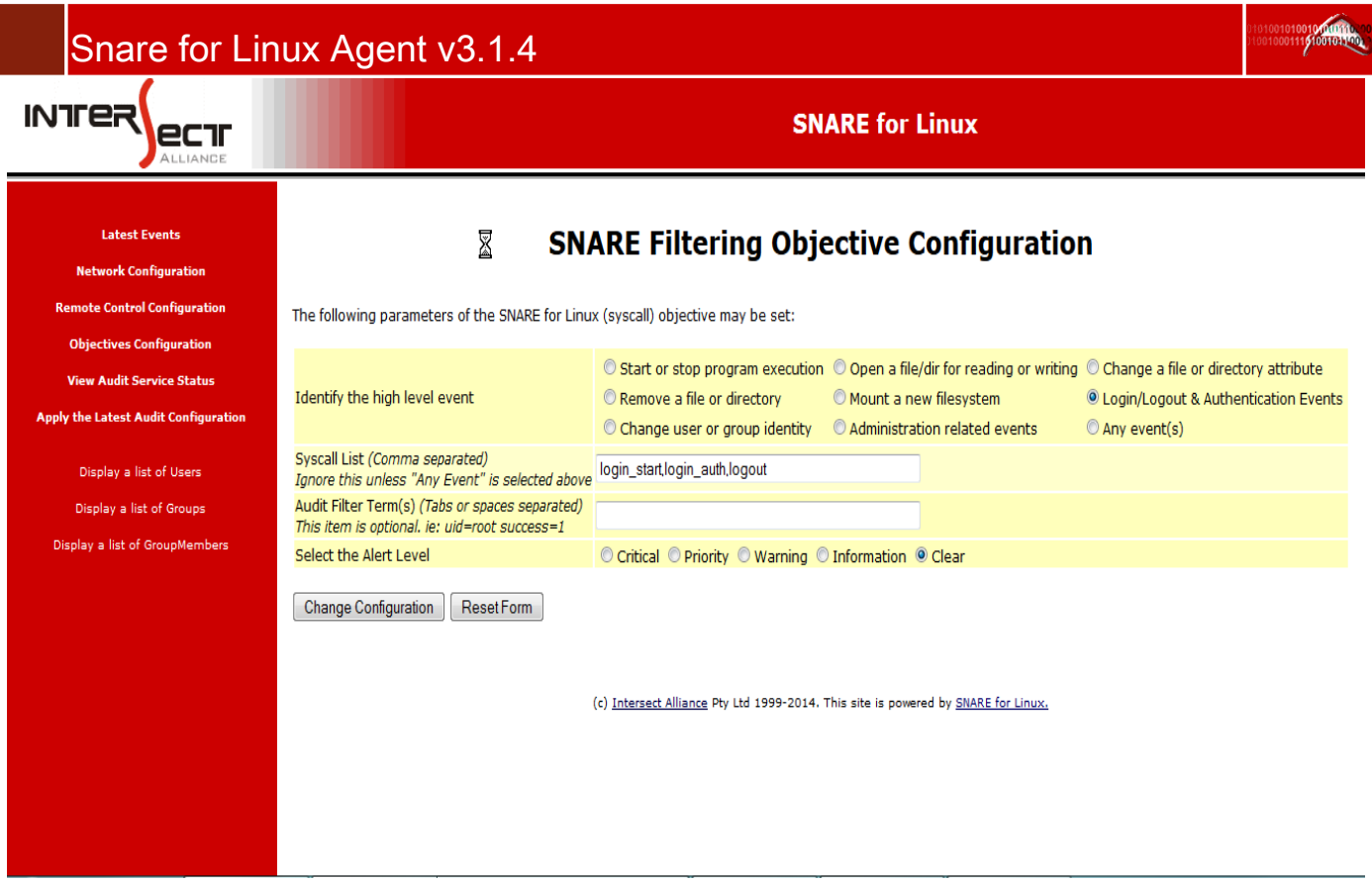
- **Login/Logout & Authentication Events Filtering**

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 cavet 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):

Snare for Linux Agent v3.1.4



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
```