System iNtrusion Analysis & Reporting Environment

Release Notes for Snare for Solaris

About this document

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

Snare Enterprise Agent for Solaris v4.0.3

Snare Enterprise Agent for Solaris v4.0.3 was released on 19th February 2016

Change Log

- **The web interface may hang after long periods of time**
  Some Operating System socket error disconnect events could cause the agent's web UI to stop responding, however the rest of the agent continued as expected. This can also be manifested on systems with lots of network interfaces. This is now fixed.

Snare Enterprise Agent for Solaris v4.0.2

Snare Enterprise Agent for Solaris v4.0.2 was released on 4th September 2015

Change Log

- **Agent not using ALT syslog format correctly**
  On the network configuration page of the web interface, selecting SYSLOG Alternative for the format was not saving correctly. This is now resolved.
- **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.

Snare Enterprise Agent for Solaris v4.0.1

Snare Enterprise Agent for Solaris v4.0.1 was released on 30th June 2015

Enhancements

- **Solaris agent unable to parse event**
  Fixed an event parsing error on Solaris that occurred when using various versions of SSH. Previously connecting via SSH would result in erroneous errors 'Audit: Failed to parse/match audit event'.

Snare Enterprise Agent for Solaris v4.0.0

Snare Enterprise Agent for Solaris v4.0.0 was released on 10th December 2014

Enhancements

- **Use pragma No-Cache in the HTTP UI**
  The Web UI has been changed to use the 'Pragma: No Cache' header for all dynamically generated pages. As a result of this change the browser and any proxies will not cache dynamic pages. This reduces the likely hood of sensitive information being left on other systems.

New Features

- **Solaris 11 Support**
  Support for Solaris 11 has been added. As a result the Solaris Agent will now install itself as a auditd plugin rather than being a stand alone executable. This change was due to changes in Solaris which removed the required hooks to the audit subsystem that existed in Solaris 10 and below. Since Solaris 10 also supports the same methods as Solaris 11, in Solaris 10 this version 4 of the Snare agent will be installed as a auditd plugin.

- **Solaris 10 Agent needs native package**
  The way Snare for Solaris is installed has been changed to make use of the native package management system of Solaris. As a result of this change, tracking of which version of the software is much easier and can be done using:

  ```
  pkginfo -l SnareSolaris
  ```

  Please see the User Guide for more details.

- **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. (DES encryption support has been removed from the Solaris Agent in favour of SSL/TLS.)

- **Multi-threading**
  Improved multi-threading and general performance improvements.

Change Log

- **Path Validation Broken for Filenames under Unix in Core**
  Path Validation has been improved. As a result of this change when a path is entered in the GUI further validation that the path is valid, is a directory/file is performed to help prevent typos or mistakes.

- **Solaris Agent install conflict on system using LDOM management**
  The agents audit class handling has been changed to support a user modifiable audit mask. As a result of this change it is now possible to change the default audit mask Snare for Solaris Agent uses at install time.

  Traditionally the Snare for Solaris agent has create the following entry in /etc/security/audit_class 0x10000000:ia:intersect alliance snare. This registers the 'ia' class with the audit subsystem and the Snare for Solaris Agent uses this class to receive events. The 0x10000000 number indicates a mask that uniquely identifies the class. This mask must be unique. Due to multiple applications wanting to using the same mask, it has been impossible to use some tools together. Ie LDOM management tools and Snare for Solaris. To address this problem, the Snare for Solaris Agent now reads the audit_class file and looks for the mask value associated with the 'ia' class. This makes it possible to change the mask value upon a conflict. If a conflict arises, the mask value for the agent may be modified in /etc/security/audit_class. The audit_class file details the range of classes which are usable. Upon a restart of the audit deamon, the Snare for Solaris Agent will pickup the new mask value and use that for logging. It will not however deregister the previous mask used. Hence it is advised that if the mask value needs to be changed, a reboot is performed. The reboot will remove the previous mask settings from all active processes. Note: Due to this change, the 'ia' class MUST exists in the audit_class file. If it is removed the agent will fail to run and will log a message to syslog with the error message: Failed to initialize the agent: Audit: Unable to find 'ia' audit_class Snare for Solaris is not active. If the class is found, the agent will log the class value to syslog: Audit: Found audit_class definition:0x100000000000000:ia:intersect alliance snare

- **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.

- **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 when using TCP or SSL/TLS. 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.

- **Gui session handling issue**
  When using the Snare Agent Web Console with Internet Explorer 10, saving 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.