



System iNtrusion Analysis & Reporting Environment

Snare Server Version 4 Release Notes



Introduction

After every major Snare Server release, the team at InterSect Alliance, or our partners, will provide you with Snare Server updates as part of your support contract. This document provides information on all updates to Snare Server version 4.x series since the initial release (Snare Server v4.0). Note that all updates to the Snare Server are cumulative, meaning that applying an update incorporates all previous updates.

Version 4.0 - Released 22nd September 2007

Snare Server 4 represents a significant change from previous versions. The following points detail the key major features over the previous Snare Server versions. This is a significant change to the Snare Server. It is highly recommend that current users of Snare Server Versions 3.5.1 and below, read this carefully. Users who have installed Snare from the 'Version 4.0' release CD do not need to apply this update.

Changes between version 3.5.1 and 4.0 include:

- **Greater Storage Capability.** The Snare Server now stores event data in compressed flat-file archives, rather than a database. This change has resulted in the capability to store and query 15-25 times more data than previous versions. As an example, version 3.5 (using a database) could store a maximum of about 500 million records on a 300 gigabyte hard drive. Snare Server 4.0 can now store approximately 8 billion events on the same 300GB disk. A conversion process will assist users of Snare Server 3.5.1 and below to migrate to the new format. This process will occur in the background once the Snare Server has been upgraded, and may take several days, depending on the volume of log data currently stored. Over this time period, historical data will gradually be made available to query from the Snare Server web-based front-end.
- **Quicker Response.** Improvements in the search algorithms, combined with the elimination of the requirement to transfer data between a 'database' and nearline storage each night, has resulted in improved average objective run times. In addition, a "bytecode compiler" has been added to the Snare Server, which has proven effective at increasing the average objective generation speed.
- **Faster Collection Rates.** The Snare Server 4 sustained collection rates are over 3,500 events per second, per Snare Server. The Snare Server can also manage bursts of event data up to 50,000 events per second. Sustained collection rates may increase, if your Snare Server hardware has CPU, network bandwidth, or memory over and above the recommended minimum hardware configuration. Improvements have also been made to the Windows User and Group collection routines to improve multiple server collection rates.
- **Easier Configuration.** A configuration wizard has been included in Snare Server 4 to assist users to configure the software for normal use, or to meet regulatory requirements such as NISPOM, PCI Data Security Standard, or Sarbanes-Oxley. Many of the functions previously found in the "Snare General Configuration Items" objective, have been transferred to the Configuration Wizard.
- **Regulatory Compliance.** In regulatory compliance mode, set using the above mentioned configuration wizard, a new objective group appears on the top bar (right hand side). This group houses only those objectives which are geared to facilitate regulatory compliance.
- **Improved hardware compatibility.** The base operating system has been updated to facilitate better support for a greater range of hardware.

- **Advanced Remote Control.** Updated versions of the Snare agents will be released in the second half of 2007 which allow more advanced remote control features. Snare Server 4.0 now incorporates objectives to make use of this advanced remote control capability. In the "Snare Agents" category, a new objective has been created called "Check and Set Agent Configuration" which will control Windows and Solaris hosts. The "Data Retrieval" objectives, formally within the "Snare Server Configuration" category, have also moved to this category.
- **Better email reporting features.** Snare users can now have an email address associated with their account. As such, Snare users or groups can be specified as destination points for electronic mails generated by Snare scheduled tasks, rather than having to specify individual email addresses for each objective. An update to a users email address will therefore flow through to all objectives for which the user receives an email.
- **Performance graphs.** The "System Status" objective in the "Status and Statistics" category has been updated to include performance graphs on CPU, memory and other resource usage. These graphs can prove very useful in fault finding and capacity management for your Snare Server support team.
- **Statistics and Monitor Objectives.** A new objective has been created to report on the total events held in the new Snare data store. Also, an objective to monitor incoming data in real time has been created. These two objectives can be found in the "Status and Statistics" category. These objectives will replace the functionality previously offered by the Dynamic Data query front page. Another new feature is the "Surge Analysis" found in the Snare Health Checker. Snare will provide a variation analysis of the total number of events, the event source and originating agent to help identify trends in the incoming data.
- **IP Protection.** Snare Server 4 includes greater IP protection features. License keys will now be needed by ALL users of the Snare Server. Resellers will have access to the key request page, which can be accessed from the Intersect Alliance site, on request. You will need a userid/password to access the site. The license system works on the Snare Server generating a unique ID(s) based on the hardware configuration. Once a request has been submitted, IA will need to issue a license key. A temporary key can be used whilst the permanent key is being generated. Information on the current license key can be found in the Health Checker.
- **Improved data source flexibility.** Due to the increased flexibility of the backend datastore, creating and manipulating new types of eventlog, from new sources, has never been easier.
- **Database Process Management.** The data correlation objective and SQL process management functions have been removed.
- **Better diagnosis.** Some query management options have been added to the "Snare General Configuration Items" objective to allow greater control over query behavior.

Version 4.1 - Released 1st January 2008

Snare Server 4.1 provides several functionality and usability upgrades over version 4.0, as well as optimising several functions to reduce server load. The following points detail the key major features over the previous Snare Server versions.

Changes between version 4.0 and 4.1 include:

- **New network vulnerability scanner / network mapper integration.** The functions of the network mapper, and network vulnerability scanner objectives have been merged into a new clonable objective, and a new configuration interface implemented. The program that handles vulnerability scanning has been upgraded, and now includes more comprehensive web server assessment functions.
- **Better metadata utilisation.** The new Snare Server storage mechanism offers many benefits over the old system, which relied on a database to contain event data. However, functions such as maintaining a list of current log sources, which were previously managed by the internal database metadata subsystem, are much more resource intensive under Snare Server 4.0. Version 4.1 increases the range of metadata collected by Snare internally, effectively speeding up several affected functions, and reducing the resource utilisation.
- **Linux logs.** The Linux 'iptables' firewall log collection subsystem has been enhanced to collect a wider range of log data, and the Linux audit collection capability has been modified to provide a more consistent approach to success/failure handling.
- **NetScreen firewall / Nortel VPN logs.** Two new log sources have been added to the Snare Server.
- **PIX firewall.** A bug in version 4.0 of the Snare Server resulted in the server not collecting logs from some newer PIX firewalls.
- **TCP collection truncation.** A bug in the tcp audit server, caused a very small percentage of events to be broken up over two lines, in circumstances where a network error was incorrectly handled.
- **Ports database.** The port 'number to description' database, used by Snare Server Firewall and Router objectives, has been upgraded with 3200 more port 'number to description' entries.
- **Date ranges.** Each objective that implements a time-based reporting range (eg: one week, one month, and so on), now includes the capability to specify an explicit date range.
- **More flexible regeneration.** Prior to version 4.1, as soon as an objective was queued for regeneration, data generated by a previous run, was not available to view. In version 4.1, the previously regenerated data will be viewable up until the time the objective is first in the objective generation queue.
- **Dynamic Query.** Both the standard Dynamic Query, and the Clonable Dynamic Query capabilities included a bug in version 4.0 which caused the 'next' and 'previous' links to not function correctly.

Version 4.2 - Released 28th March 2008

Snare Server 4.2 concentrates generally on core infrastructure changes, designed to streamline collection and analysis functions. The following points detail the key major features over the previous Snare Server versions.

Changes between version 4.1 and 4.2 include:

- **Optimising User and Group collection.** Through several back-end infrastructure changes, User and Group collection has been given a reasonable speed boost.
- **More efficient hardware utilisation.** Users with dual-core or SMP systems will notice significant objective regeneration speedups.
- **More network sources.** Logs from Netscreen firewalls, and Nortel VPN Routers can now be processed, and a range of appropriate objectives are now available on the Snare Server. Checkpoint Firewall 1 logs can now be received using the Snare Syslog collector. Updates to the snort collection capability have also been made, to reflect recent modifications to the snort reporting format.
- **Regulatory compliance updates.** Support for additional log sources in Snare's regulatory framework modules has been added.
- **New schedule options.** Quarterly, and hourly reports are now available. Reports that take significantly longer to generate than their schedule would normally allow, will be 'bumped' up to the next schedule option. For example, if an hourly report takes two hours to generate, the Snare Server will reconfigure the objective automatically, to run as a daily task.
- **Vista support.** Windows objectives have been modified to support those Windows Vista events that differ from previous versions of Windows.
- **More objectives cloneable.** Several existing objectives have been converted to 'clonable' objectives.
- **Better metadata utilisation.** The new Snare Server storage mechanism offers many benefits over the old system, which relied on a database to contain event data. However, functions such as maintaining a list of current log sources, which were previously managed by the internal database metadata subsystem, are much more resource intensive under Snare Server 4.0. Version 4.2 increases the range of metadata collected by Snare internally, effectively speeding up several affected functions, and reducing the resource utilisation.
- **Encryption.** The initial infrastructure required to support encrypted agent communications has been integrated into the Snare Server.
- **Tandem logs.** Initial support for Tandem log data is now available in the Snare Server.
- **PDF Support.** PDF generation is now available for Snare Server objectives.
- **Consolidation of infrastructure software.** Several areas of duplicated software have been consolidated, which means lower complexity, and therefore lower likelihood of bugs.
- **Agent Ordering.** Agents are now sorted alphabetically in the Agent configuration objective.

Version 4.2.1 - Released 1st May 2008

Snare Server 4.2.1 concentrates generally on problems reports since the release of version 4.2, however, some additional features are also available. The following points detail the key major features over the previous Snare Server versions.

Changes between version 4.2 and 4.2.1 include:

- **TCPAuditServer updates.** On some operating systems, the TCP/IP stack does not always grant Snare's request to use a single packet per event, and a single event per packet (where possible). In circumstances where the operating system 'squashes' three events, over two separate TCP packets, there is a risk that the middle event may arrive in the Snare data store, corrupted. An update to the TCP audit server, has implemented additional caching, at the cost of a small amount of memory, in order to compensate for 'squashed' events
- **SQLite error check.** A new sqlite database verification system runs nightly. If the sqlite database (which stores Snare's configuration settings) passes the verification check, a backup is made, just in case a future corruption renders the Snare server unusable. Note that this feature is in addition to the standard configuration settings archive that is saved to the first CD/DVD of any archive set.
- **OS400 updates.** Some minor changes have been made to the OS400 import process.
- **Older archive files.** Archive files in Snare Server 3.5 format, that are corrupted due to disk errors, will now be skipped, and left for optical archive. Previously, the Snare Server would reattempt these files every night, leading to duplicate data on some systems.
- **Metadata speedup.** The metadata collection system has been changed to regenerate metadata only for those directories that have had data added or removed since the last regeneration. All other metadata is saved off, and reloaded by any subsequent runs. This has reduced metadata run times by a significant (factor of 10+) amount.
- **Health Checker fix.** A bug in the Snare Server hourly run code, would update the 'end time' for the overnight cron run (rather than the daily). This means that the nightly run would appear to be running for much longer than it actually is, leading to a 'problem' report in the health checker.
- **User navigation mode.** User navigation mode is now configurable by the administrator on account creation, and can be turned on independently of regulatory compliance mode.
- **Query retry.** Transitory problems in sqlite when subjected to heavy query load, would cause a database level error to be returned on some queries. The same query, repeated seconds later, would succeed. The SnareDB module now attempts at least 10 retries of a query, if this database error appears, before notifying the Snare health checker of a potential problem.
- **Big Numbers.** The snare datastore interrogation module has been updated to handle numeric values over 4,294,967,296.
- **Unix privileged commands.** A new syslog 'sudo' scanner has been included in the standard syslog objective category.
- **Users and Groups.** A small bug in windows account retrieval has been found, and fixed.
- **Configuration checker.** The agent configuration checker now differentiates between non-contactable agents, and agents that do not support agent configuration checks.
- **Optical Archive.** The Snare archive capability can now write data to CD/DVD without removing the data afterwards.
- **Sidewinder Firewall.** A new module to collect sidewinder firewall logs has been integrated into Snare.

Version 4.3 - Released 1st September 2008

Snare Server 4.3 continues to build on the core infrastructure of Snare, by adding speed increases in several areas, in addition to providing several functionality enhancements. The following points detail the key major features over the previous Snare Server versions.

Changes between version 4.2.1 and 4.3 include:

- **IIS Web Server logging.** Some versions of IIS occasionally do not include a particular field element in event log information. The presence or absence is not predictable on a per-event basis, but Snare can work around it by evaluating the field count for each event. Snare Server 4.3 includes a small workaround to allow such events to be processed correctly.
- **Oracle Log collection - alpha test version.** A new oracle collection module has been added to the Snare Server. At present, this particular module is considered to be an alpha test version, and has been enabled only for a few interested clients. We intend to use this reference design as a basis for the development of a more administrator-friendly in upcoming versions of Snare.
- **ACF2 collection tweaks.** The ACF2 collection module has been updated to cope with a wider range of formatting for the existing ACF2 reports.
- **PDF output.** PDF output has been tweaked to make classification messages more obvious, and also to cope with extended table sizes.
- **Email classification.** The Snare Server configuration wizard has been updated to allow classification markings to be included at either the start, or end of a subject line.
- **Geolocation speed.** A small update to Snare's IP address geolocation capability, can significantly decrease the duration of lookups for an IP address that has already been queried recently.
- **Configuration database correction.** Transient errors in retrieving data from the Snare configuration database, have occasionally appeared on multi-processor systems. A small update to the query capability will now issue a retry when these circumstances occur.
- **Configuration layout.** A small layout change has been included in Snare's configuration settings page, in order to lay the foundation for upcoming feature enhancements in version 5.0.
- **Metadata collection optimisations.** A new system of metadata caching has decreased the amount of time that the Snare Server spends gathering information about collected events, in order to quickly display summary information back to the user on an interactive basis.
- **Query caching.** A new cache system has been implemented that can SIGNIFICANTLY speed up queries that are repeated often, with only slight variations to elements such as date or time.
- **Spreadsheet export.** Due to element length limitations of the excel spreadsheet file format (XLS), the excel spreadsheet export capability, found in Snares' dynamic query capability, has been shifted to a comma-separated-value (CSV) format instead. No significant functional differences should be noted when using CSV rather than XLS. This change will also allow users of alternative office products, such as OpenOffice, to access data in a more open format.
- **Monitoring SUDO.** A new objective under the 'Syslog Reports' category of the 'Applications' group, allows administrators to track SUDO access on posix systems.
- **Windows eventlog corruptions.** A new objective under the 'Applications' group, allows administrators to detect 'corrupted event' messages from windows systems.
- **Dynamic Query table additions.** OS400 and Oracle have been added as valid Dynamic Query log sources.
- **Data store integrity verification.** A new objective has been added to the "Status and Statistics" group, allowing you to display, and save, the cryptographic checksum of each Snare data store.
- **Data surge returns to the health checker.** A new data surge notification capability has been added to the health checker, providing a zero-configuration notification of significant increases or decreases to data collection on a per host basis.

Version 4.3.1 - Released 23rd September 2008

Snare Server 4.3.1 concentrates generally on problems reports since the release of version 4.3, however, some additional features are also available. The following points detail the key major features over the previous Snare Server versions.

Changes between version 4.3 and 4.3.1 include:

- **New SuperUsers group.** This group has been added to allow authenticated users access to “Administrator Only” objectives. This means that all administrative tasks on the Snare Server can be conducted without using the generic Administrator account.
- **Metadata collection optimisations.** An update to the system of metadata caching has decreased the amount of time that the Snare Server spends gathering information about collected events and addresses a race condition for heavily loaded machines.
- **Configuration Wizard.** All of the functions previously found in the “Snare General Configuration Items” objective, have been transferred to the Configuration Wizard. The Configuration Wizard is now located at Snare Utilities -> Snare Server Administrative Tools -> Configuration Wizard.
- **Attachment management.** The Snare Server configuration wizard has been updated to optionally allow only one attachment per objective, e.g. only the CSV attachment will be sent instead of both the HTML and CSV attachments.

Version 4.4 - Released 28th April 2009

Snare Server 4.4 provides another speed increase over the 4.3 series, with further tweaking of the cached query technology, to increase query performance. The following points detail the key major features over the previous Snare Server versions.

Changes between version 4.3.1 and 4.4 include:

- **Updated Metadata subsystem.** The new metadata subsystem will now respond better to old imported data, and should consume less resources.
- **Status Panel.** The Snare Server front page, which appears just after login, will now display the health checker summary, and also several other items, such as server uptime, and a summary of events received over the course of the last 24 hours.
- **Health Checker.** A more automated system of detecting systems that have received significant surges or drops in audit log collection volume, has returned to the health checker once more.
- **Objective Termination.** An objective regeneration can be terminated at the status-information page associated with each objective, if required.
- **Dynamic Query Capabilities.** The non-clonable dynamic query capability has been removed, and the clonable dynamic query facility has been enhanced to allow the user to selectively display information that appears as a component of a larger string element. Objectives that utilised the spreadsheet, or text output functionality, are also significantly faster to generate.
- **User and Group dynamic query.** A new objective has been created, to allow you to query Snare's User and Group database, which is collected daily from the Snare Agents.
- **Direct Data Removal.** Snare can now remove selected data, based on originating system, log type, or date range.
- **Administrative Super Users.** A "Super User" group has been established on the Snare Server, allowing you to give some administrators permissions that previously required explicit login with the "Administrator" user.
- **VMS Log Data.** The Snare Server can now collect logs from VMS systems.
- **Objective Control.** Global Objective access control, and scheduled task settings, have been amalgamated into a single objective.
- **Expanded Configuration Wizard.** The Snare Server configuration wizard has been enhanced to take over all functions of the old "Snare General Configuration Items" objective.
- **Limiting incorrect date information.** Clients that have incorrect dates set can clutter your log data. Snare now has the capability to ignore any log data that arrives at the Server, that is more than a preset number of days old. Data imports from optical media, is not affected by this setting.
- **Data Monitor.** The "Monitor Incoming Data" objective has been removed from the "Status and Statistics" group; reducing the complexity of the audit collection subsystem, which no longer needs to maintain a shared memory store to save off statistics.
- **Proactive file system monitoring.** The Snare Server collection subsystem will strangle incoming data, in response to extremely low disk space, or other file-related resource depletion (configurable on a per-site basis). Once disk space is made available, the collection subsystem will revert to normal once more.
- **SSH Keys.** Several packages have been upgraded, as part of InterSect Alliance's normal security support service. Of these, one that may affect some users, is an upgrade of SSH keys for some sites. Direct root-level ssh access has also been removed, in order to better meet PCI security requirements.
- **General Statistics.** The General Statistics objective has been upgraded to include more information, including average events per second.

Version 4.5 - Released 5th November 2009

Snare Server 4.5 concentrates generally on problems reports since the release of version 4.4, however, some additional features are also available. The following points detail the key major features over the previous Snare Server versions.

Changes between version 4.4 and 4.5 include:

- **File System.** For newly installed systems using 4.5, there will be twice the number of available files (inodes).
- **Data Restore.** The data restoration objectives were updated to ensure they bypass the “Discard Days” feature added in 4.4.
- **Collection speeds.** More optimizations have been applied to the network collection modules to increase their maximum collection rates, especially via TCP.
- **Snort Event IDs.** Snort.org have removed their SnortID lookup feature, so the Snort objectives have been updated to use snortid.com instead.
- **Windows Group Members.** The Windows Group Member functions have been optimized and now include recursion protection.
- **Archive Functions.** Small tweaks to the archive functions mean that Snare will create slightly fewer files on disk, for the same volume of data.
- **Query updates.** The main query engine has been updated to better handle years worth of data and many thousands of files.
- **Retrieve User/Group information.** OS400 and Windows objectives have been updated to allow them to handle a wider range of error situations. The Windows Retrieval objective now has a “Domain Suggestion” setting for use when more than one computer is being scanned, but all the machines are located in the same Domain.
- **Health Check.** In situations where hardware failures cause problems with Snare configuration files, the Snare Server is now capable of detecting and correcting inconsistencies.
- **Dynamic Query Capabilities.** Further extended to allow any number of user selected data columns (Tokens). Also, objectives now support post-query processing of token column data and attachments, such as CSVs, now accurately reflect report data (hidden and token columns).
- **Host-Based Time Zone Identification.** For hosts that are not in the same time zone as your Snare Server, you are now able to configure the correct time zone. Then, as each query is executed, or when results are returned by the Snare Server, for hosts that have had a time zone configured, the time zone offset will be added to the log date to align the date and time with the Snare Server's time zone.
- **Selective Data Removal.** Snare can now remove specific data from the data store based on a dynamic query.
- **Database Optimizations.** Additional indices have been added to the SQLite database to increase performance and updates have been made to the automated error correction feature.

Contacts:

Email: support@intersectalliance.com

Web: <http://www.intersectalliance.com>

© 1999-2009 Intersect Alliance Pty Ltd. All rights reserved worldwide.

Intersect Alliance Pty Ltd shall not be liable for errors contained herein or for direct, or indirect damages in connection with the use of this material. No part of this work may be reproduced or transmitted in any form or by any means except as expressly permitted by Intersect Alliance Pty Ltd. This does not include those documents and software programs developed under the terms of the open source General Public Licence, which covers the Snare agents and some other software.

The Intersect Alliance logo and Snare logo are registered trademarks of Intersect Alliance Pty Ltd. Other trademarks and trade names are marks¹ and names of their owners as may or may not be indicated. All trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications and content are subject to change without notice.