

System iNtrusion Analysis & Reporting Environment

Snare Server Benefits and Hardware Specification



Benefits of the Snare Server

The Snare Server collects events and logs from a variety of operating systems, applications and appliances including, but not limited to: Windows NT/2000/XP/2003/Vista, Solaris, AIX, 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 Logs or Syslog Data of any variety. In addition, the Snare Server 4 can now collect from any type of event.

In addition to the above, the benefits of purchasing the Snare Server include:

- Official support mechanism for the Snare open source agents. Note that official Snare agent support is currently not offered through **any** other channels.
- Ability to quickly and easily comply with **NISPOM, PCI, SOX** or other regulatory requirements.
- All future Snare Server versions and upgrades included as part of an annual maintenance fee.
- Ability to collect any arbitrary log data, either via UDP or TCP protocols.
- 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.
- Ability to continuously collect large numbers of events. Snare Server collection rates exceed 3,500 events per second using a low end, workstation class, Intel based PC on a 100Mbps network, with burst collection allowing over 50,000 events per second for a few minutes. Billions of events can be collected using the minimum recommended hardware.
- Automatic collection of events to compressed text format, suitable for offline forensics analysis.
- Ability to drill down from top level summary reports to raw log details. This reduces the amount of data “clutter” at the top level, and allows a system administrator to fine tune the reporting objectives.
- Ability to create “cloned” objectives that allow very specific reporting against any collection profile. 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 certain parameters.
- Very simple, single CD installation for those users not requiring a hardware based appliance.

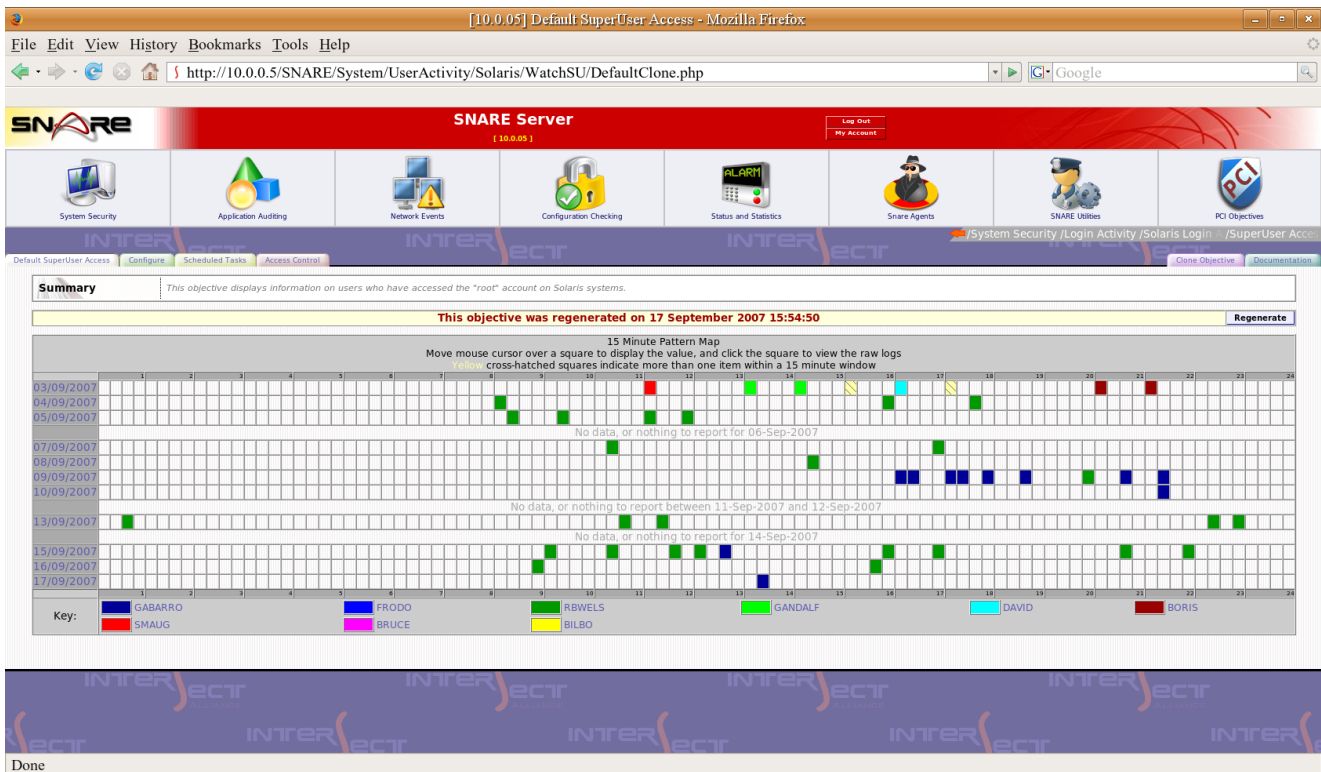
The Snare Server uses a hardened version of the Linux operating system base for stability, security, and hardware compatibility. A Snare Server user, however need not be concerned with managing a Linux server. The Snare Server, once installed, is a fully contained appliance, and does not require any system administrator level maintenance. The Snare Server will operate on commonly available Intel based PCs, with hardware specifications shown on the next page.

The Snare Server successfully builds on the freely available, open source Snare agents.

Snare Server Hardware Specification

Snare Server hardware requirements are significantly dependent on the predicted volume of audit, and the type and number of audit objectives defined. The following points should be considered minimal mandatory requirements for a functional Snare Server system:

- An x86 compatible CPU (eg: Pentium 4, AMD, AMD64) running at a processing capacity equivalent to, or better than a Pentium 4 - 3Ghz.
- 300GB hard disk or greater. Disk may be IDE, SCSI or SATA. The disk should either be one physical disk, or should appear as a single disk to the operating system, via a hardware RAID controller. Software RAID is not supported.
- 2 Gb RAM
- A 100 megabit, or (preferably) a 1000 megabit (1 Gigabit) network card.
- In general, the Snare Server operates on a hardened version of the 'Ubuntu Feisty' distribution of Linux. Any hardware supported out-of-the-box by Ubuntu Feisty, will also work on the Snare Server. In particular:
 - a. Some brands of Serial-Attached-SCSI may be supported.
 - b. Most modern CD/DVD ATAPI writers will operate correctly.
 - c. A majority of SATA/RAID cards will operate correctly.



Snare Server Screenshot

Snare Server 4.0 Release Features

Snare Server 4 represents a significant change from previous versions. The following points detail the key major features over the previous Snare Server versions.

- **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.
- **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.
- **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.
- **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.
- **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.

Email: sales@intersectalliance.com

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

Telephone: +61 402 03 3347

© 1999-2007 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. The Intersect Alliance logo and Snare logo are registered trademarks of Intersect Alliance Pty Ltd. Other trademarks and trade names are marks' 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.