

SNARE

System iNtrusion Analysis & Reporting Environment

Guide to the SNARE BackLog

INTERSECT
ALLIANCE

Documentation History

Version No.	Date	Edits	By whom
0.9	28 December 2004	First draft for the Guide to the SNARE BackLog documentation.	George Cora
1.0	3 January 2005	Approved Version	George Cora
1.1	4 January 2005	Update for final release version of Snare Micro	Leigh Purdie
2.0	2 April 2005	Minor rewording	infofocus.com
2.1	30 November 2005	Formatting changes	George Cora
2.2	15 December 2006	Name change to BackLog	David Mohr

© 1999-2006 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 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 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.

About this guide

This guide introduces you to the functionality of the SNARE BackLog, a free Windows-based application that collects and stores log data sent from any SNARE agent (for example, Windows, Solaris, AIX, IRIX, Solaris, IIS Servers, ISA Servers, or Linux), as well as SYSLOG capable devices. The SNARE BackLog is the 'little brother' of the full 'SNARE Server' appliance provided by InterSect Alliance. SNARE Server is a full collection, analysis, reporting and archival capability, with a web-based interface, designed for those users who are serious about collecting, analyzing and processing events from a variety of SNARE agents or SYSLOG appliances.

Other guides that may be useful to read include:

- SNARE Server User's Guide.
- Installation Guide to the SNARE Server.
- SNARE Server Troubleshooting Guide.
- The SNARE Toolset - A White Paper.

Table of contents:

1 Introduction.....	4
2 Overview of SNARE BackLog.....	5
3 Installing and running SNARE BackLog.....	6
3.1 SNARE BackLog installation.....	6
3.2 Running SNARE.....	6
4 Setting the collection configuration.....	7
5 Management and display functions.....	9
6 SNARE Server - Commercial Version.....	10
7 About InterSect Alliance.....	11

1 INTRODUCTION



The team at InterSect Alliance have experience with auditing and intrusion detection on a wide range of platforms - Solaris, Windows NT, Linux, Windows 2000/2003/XP, Novell Netware, AIX, IRIX even MVS (ACF2/RACF); and within a wide range of IT security in businesses such as - National Security and Defence Agencies, Financial Service firms, Government Departments and Service Providers.

This background gives us a unique insight into how to effectively deploy host and network intrusion detection systems that support and enhance an organisation's business goals.

The 'SNARE BackLog' is a free Windows-based application that collects and stores log data sent from any SNARE agent (for example, Windows, Solaris, AIX, IRIX, Solaris, IIS Servers, ISA Servers, or Linux), as well as SYSLOG capable devices.

In the spirit of the release of the SNARE agents, the team at InterSect Alliance are proud to release SNARE BackLog as an open source initiative. Other event audit modules for Solaris, AIX, IRIX, Linux and other operating systems/services have also been released under the terms of the GNU Public License. The overall project is called 'SNARE' - **System iNtrusion Analysis and Reporting Environment**. The SNARE BackLog is the 'little brother' of the full 'SNARE Server' appliance provided by InterSect Alliance. SNARE Server is a full collection, analysis, reporting and archival capability, with a web-based interface, designed for those users who are serious about collecting, analysing and processing events from a variety of SNARE agents or SYSLOG appliances.

InterSect Alliance welcomes and values your support, comments, and contributions. Our contact details are available from our contact page at www.intersectalliance.com.

2 OVERVIEW OF SNARE BACKLOG

The SNARE BackLog operates through the actions of two complementary applications:

- The SNARE BackLog service based application (*snaresvr.exe*).
- The graphical configuration and reporting tool (*snaresvrgui.exe*)

The *snaresvr* service runs on a Windows host and listens for events on UDP port 6161 (native SNARE agent port), or UDP port 514 (native SYSLOG port). These events may be from any SNARE agent or SYSLOG appliance or software application that is able to send events via any of these two ports. The SNARE BackLog collection ports are fixed, and they may not be changed.

The *snaresvr* service collects events on the above mentioned ports and writes the data to a log file. The location and naming conventions of the log file can be specified by the user.

Since the above event log contains a great deal of information for the average user, and in a format which doesn't lend itself to interpretation, SNARE also incorporates a graphical front end (GUI) tool. The graphical tool allows for easy configuration of all the event logging parameters, as well as display of filtered event records. Note that only 1000 of the most recent collected events will be displayed on the GUI, although ALL events are written to the log files. Figure 1 shows the main window, which includes the main display.

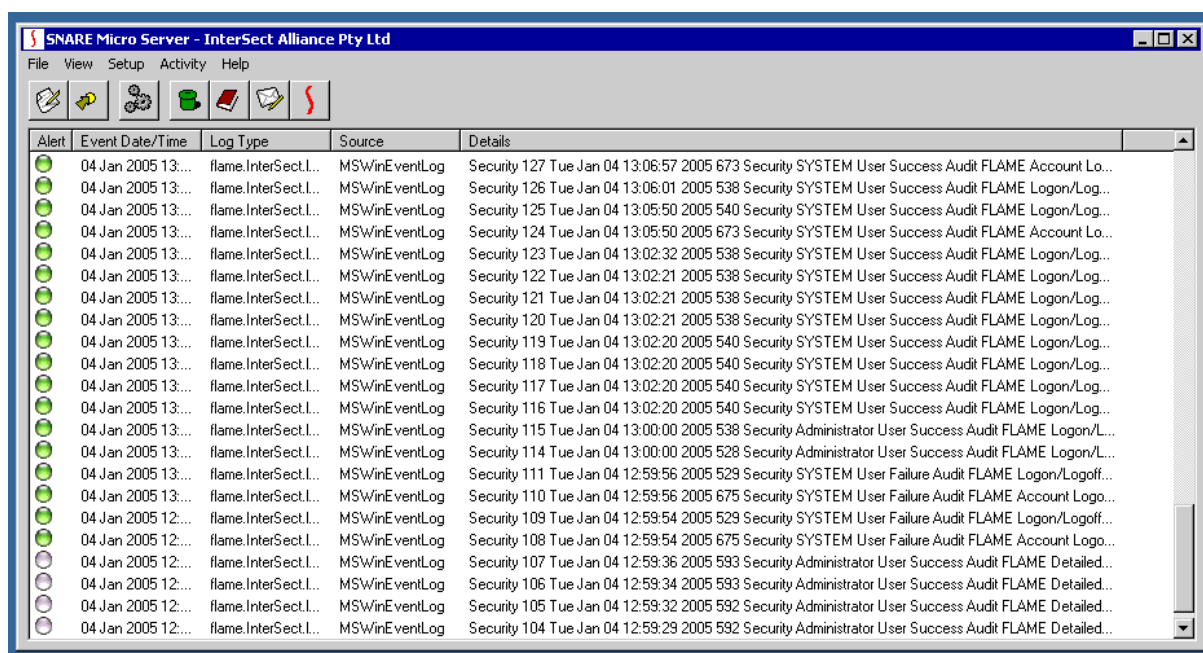


Figure 1 Main Window

3 INSTALLING AND RUNNING SNARE BACKLOG

3.1 SNARE BACKLOG INSTALLATION

SNARE is available in compressed format, and has been designed with an installation wizard to allow for easy installation and configuration of all critical components. The compressed file includes the two major components, namely:

- ***snaresvr.exe*** - The SNARE BackLog service is contained in the 'snaresvr.exe' binary. This binary contains all the programs to read the event log records, and write them to the specified log file. It also is able to communicate with the graphical user interface (GUI), when it is active.
- ***snaresvrgui.exe*** - This binary only contains the programs to provide for the SNARE BackLog front end (GUI) functions, as shown in Figure 1. However, the graphical user interface requires the *snaresvr* service to be installed and active.

Installation of the two main components (*snaresvr* and SNARE front end) is undertaken as follows:

1. Download the **setup.zip** file from the Intersect Alliance website.
2. Ensure you have administrator rights, then double click the **setup.zip** file. This is a self extracting archive, and will not require WinZip or other programs.
3. A series of screens will then be displayed, requesting that various parameters be set. Read these settings carefully, using this manual as a reference. Most of the settings are discussed later in this guide.

3.2 RUNNING SNARE

Upon installation of the SNARE BackLog front end, an 'Intersect Alliance' menu item is installed off the **Program** main Windows menu. The SNARE BackLog GUI front end launch menu is then available from **Programs->Intersect Alliance->Snare BackLog**.

For events to be passed to a remote host, the *snaresvr* service must be running. To verify that the *snaresvr* service is running, check the 'Services' item in Control Panel on older Windows NT hosts, or select 'Services' from the **Control Panel->Administrative Tools->Computer Management** options. The service must be running for events to be collected. If it is not, then select **Start and Automatic**, so that the service is started automatically when the host is rebooted.

4 SETTING THE COLLECTION CONFIGURATION

The configurations for the SNARE BackLog are stored in the system registry. The registry is a common storage location of configuration parameters for Windows programs, and other applications. The registry contains all the details required by the SNARE BackLog to successfully execute. Failure to specify a correct configuration will not 'crash' the *snare* service, but may result in events being logged in the wrong directory, or not at all.

Note that manual editing of the registry location is possible, but care should be taken to ensure that it conforms to the required SNARE format. Also, any use of the graphical SNARE front end tool to modify selected configurations, may result in manual configuration changes being overwritten.

The most effective and simplest way to configure the SNARE BackLog is to use the graphical front end. The audit configuration window can be selected from the **Setup->Snare BackLog Configuration** menu, or directly from the associated toolbar button.

The SNARE BackLog is a very simple collection tool. The only configuration parameters to consider are:

- Location of the log file, and
- Naming convention for the log files.

These parameters are shown in the **SNARE BackLog Configuration** window, shown in Figure 2 below.

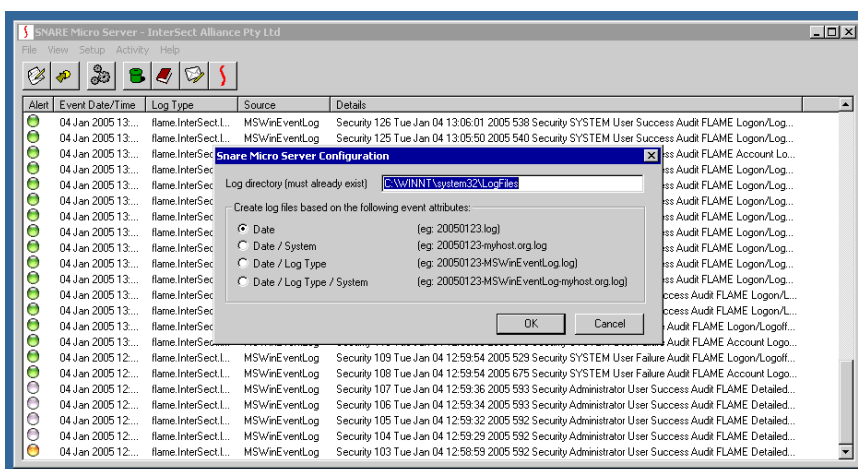


Figure 2 SNARE BackLog Configuration

The specific fields in the configuration window are described as follows:

- **Log Directory.** This is the location of the log files that will be maintained by the SNARE BackLog service. All logs collected via ports 514 or 6161 will be written to a log file located in this directory. The SNARE BackLog will default to the system32\LogFiles directory under the system root directory (usually *C:\WINNT\system32\LogFiles*) when first installed.

Please be aware, that the SNARE BackLog does not monitor this directory for disk space availability - you will need to ensure that files in this directory are appropriately managed, in order to ensure that your hard drive does not become full.

- **Create Log Files.** Log files will be created based on the selected naming convention. The choices are as follows:

- **Date only.** This will create a file based on the current date, that rotates at midnight. Format will be YYYYMMDD.log (eg. 20050123.log to signify 23rd January 2005). This is the default option, and represents the simplest, and least resource-intensive configuration.
- **Date and System.** This will create a file for each system that reports to the SNARE Server, combined with the current date. The format will be YYYYMMDD-system.dns.name.log (eg. 20050123-myhost.org.log, to signify 23rd January 2005 with events in the log file collected from the host 'myhost.org'). This option has a slightly higher performance impact than the default (Date Only) option, as the SNARE BackLog will need to perform some extra activity whenever it receives an event that has a different system source from the previous event that it received.
- **Date and Log Type.** This will create a file for each log type that is sent to the SNARE Server, combined with the current date. The format will be YYYYMMDD-LogType.log (eg. 20050123-MSWinEventLog.log to signify 23rd January 2005 with events in the file that contain Windows Event Log data). This option has a slightly higher performance impact than the default (Date Only) option, as the SNARE BackLog will need to perform some extra activity whenever it receives an event that has a different Log Type from the previous event that it received.
- **Date, System and Log Type.** This will create a file for each log type and system, combined with the current date. The format will be YYYYMMDD-LogType-system.dns.name.log (eg. 20050123-MSWinEventLog-myhost.org.log to signify 23rd January 2005, from myhost.org, containing events from the Windows logging sub-system. This option has a slightly higher performance impact than the default (Date Only) option, as the SNARE BackLog will need to perform some extra activity whenever it receives an event that has a different system source, or log type, from the previous event that it received.

6 SNARE SERVER – COMMERCIAL VERSION

The team at Intersect Alliance have produced software that enables remote control, collection, analysis and output from all SNARE agents, including Windows, Solaris, Linux and IRIX, as well as applications such as web servers and appliances that generate SYSLOG formatted events. This software is known as the SNARE Server, and full details are available from the Intersect Alliance web site (www.intersectalliance.com). The SNARE Server is proprietary software, and is not available as open source.

The SNARE Server is an Enterprise Audit Event Log analysis solution, comprising a central audit event collection, analysis, reporting and archive service, and security 'agents' for multiple operating systems and applications.

Full source code and documentation is provided with this service, allowing the Intersect Alliance partners, or internal security professionals, to quickly develop SNARE security objectives that are derived directly from your key organisational risk items. The SNARE Server also comes equipped by default with an array of security objectives that allows agencies to meet common security goals. A selected screen shot (Figure 4) of the SNARE Server is shown below. Full details on the SNARE Server, including more screen shots are available from the Intersect Alliance web site.

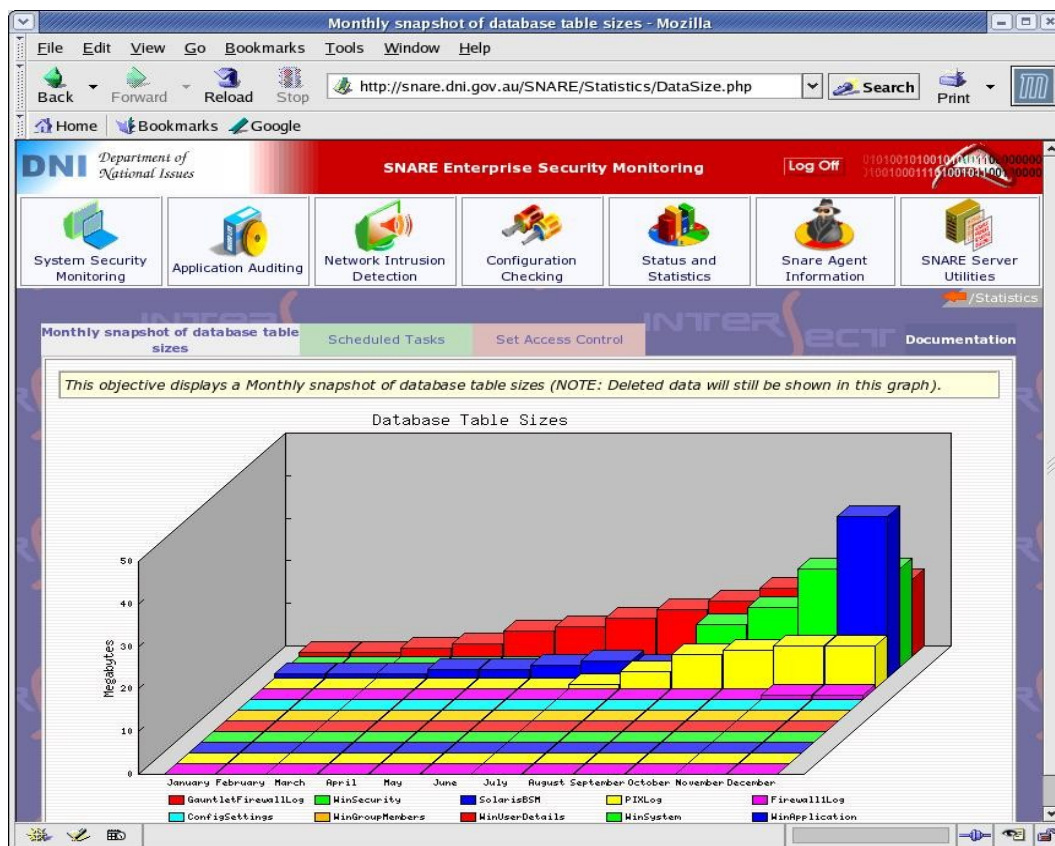


Figure 4 Screen shot from the SNARE Server

7 ABOUT INTERSECT ALLIANCE



InterSect Alliance is a team of leading information technology security specialists in both the 'technical' and 'policy' areas. In particular, Intersect Alliance are noted leaders in key aspects of IT Security, including host intrusion detection. Our solutions have and continue to be used in the most sensitive areas of Government and business sectors. Intersect Alliance consult and contract to a number of agencies in Australia and the Asia Pacific, for both the business and Government sectors.

The Intersect Alliance business strategy includes demonstrating our commitment and expertise in IT security by releasing open source products such as SNARE, and the proprietary SNARE Server. Intersect Alliance intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying, abstracting and/or solving complex security problems.

Visit the Intersect Alliance website for more information at www.intersectalliance.com.